



**Symantec Endpoint Protection Integration Guide v1.0**

Security Orchestration, Automation and Response Platform

Licensed Materials – Property of IBM

© Copyright IBM Corp. 2010, 2019.  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 | July 2019 | Initial publication. |

Table of Contents

[Table of Contents 3](#_Toc13739621)

[1. Overview 5](#_Toc13739622)

[1.1. Use cases 6](#_Toc13739623)

[2. Installation 7](#_Toc13739624)

[2.1. Configuring Generic Email Parsing Script 7](#_Toc13739625)

[2.2. Useful links 7](#_Toc13739626)

[3. Package contents 8](#_Toc13739627)

[4. Custom layout 11](#_Toc13739628)

[5. Function descriptions 13](#_Toc13739629)

[5.1. SEP - Scan Endpoints 13](#_Toc13739630)

[5.2. SEP - Upload File to SEPM 16](#_Toc13739631)

[5.3. SEP - Get File Content as Base64 17](#_Toc13739632)

[5.4. SEP - Get Computers 18](#_Toc13739633)

[5.5. SEP - Move Endpoint 21](#_Toc13739634)

[5.6. SEP - Quarantine Endpoints 22](#_Toc13739635)

[5.7. SEP - Get Fingerprint List 25](#_Toc13739636)

[5.8. SEP - Add Fingerprint List 26](#_Toc13739637)

[5.9. SEP - Update Fingerprint List 27](#_Toc13739638)

[5.10. SEP - Get Groups 28](#_Toc13739639)

[5.11. SEP - Assign Fingerprint List to Group 29](#_Toc13739640)

[5.12. SEP - Delete Fingerprint List 30](#_Toc13739641)

[5.13. SEP - Get Command Status 31](#_Toc13739642)

[5.14. SEP - Get Domains 35](#_Toc13739643)

[6. Script description 36](#_Toc13739644)

[7. Notifications description 37](#_Toc13739645)

[7.1. Parsing Notifications of critical events 37](#_Toc13739646)

[7.2. Generic email script 37](#_Toc13739647)

[7.3. Script – scr\_sep\_parse\_email\_notification 38](#_Toc13739648)

[8. Configuring Symantec Endpoint Protection 39](#_Toc13739649)

[9. Inform Resilient Users 39](#_Toc13739650)

# 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 Symantec Endpoint Protection environment:

* Remediate (delete) 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 or delete an md5 hash value to 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 also has two user defined settings:

* Results limit

The EOC scan query can return a total number of results which can overwhelm the Resilient platforms ability to process them. The integration has a user defined parameter to limit the amount of results that are returned by the function.

* The integration configuration parameter sep\_result\_limit, can be used to limit the amount of results send back to the Resilient platform.
* If the results returned is over the limit, the results sent to the Resilient platform is truncated to the results limit and the total results are also 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.

## 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 Evidence of Compromise (EOC) scan for the artifact in the SEP environment using rule/workflow “Example: SEP - Initiate EOC Scan for Artifact”.
2. A match is discovered, and a row is added to data table “Symantec SEP - EOC scan results”.
3. If the file is an executable upload the file to the SEPM server using rule/workflow “Example: SEP - Upload file to SEPM server” which is enabled for the matching data table row from step 2.
4. To delete the file on matching endpoint or all matching endpoints, use rule/workflow “Example: SEP - Remediate Artifact on Endpoint” which is enabled for the matching data table row from step 2.
5. Use the rule/workflow “Example: SEP - Get File Content as Base64 string”, which is enabled for the matching data table row from step 2, 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 rule/workflow “Example: SEP - Get Endpoint Details for artifact”.

or

Get information on an endpoint from a match in the data table “Symantec SEP - EOC scan results” using rule/workflow “Example: SEP - Get Endpoint Details”.

When a matching endpoint name is discovered, a row is added to data table “Symantec SEP - Endpoint details”.

1. Move the endpoint to a quarantine group using rule/workflow “Example: SEP - Move Endpoint” which is enabled for the data table row from step 1.
2. Add the endpoint to network quarantine using rule/workflow “Example: SEP - Quarantine Endpoint” which is enabled for the data table row from step 1.

* An MD5 hash value of a suspicious file is added as an artifact value to a Resilient incident.

1. See if the hash exists in a blacklist in a target SEP domain use rule/workflow “Blacklist Example: SEP - Get Blacklist information”.

A row is added to data table “Symantec SEP - Fingerprint lists” if the blacklist is found.

1. 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”.
2. Get a list of SEP group information for the SEP domain using rule/workflow “Example: SEP - Get Groups information”.
3. Information on each SEP group is added as a row to data table “Example: SEP - Get Groups information”.
4. Assign the blacklist to a group for system lockdown using rule/workflow “Example: SEP - Assign Blacklist to lockdown group”.
5. If the MD5 hash is no longer considered suspicious, delete the hash from the blacklist using workflow “Example: SEP - Delete Blacklist”.
6. Delete the blacklist using rule/workflow Example: SEP - Delete Blacklist.

# Installation

You download the function package to a Resilient integration server, and from there you deploy the functions and components to a Resilient platform. These procedures are provided in the [Resilient Integration Server Guide (PDF)](https://github.com/ibmresilient/resilient-reference/blob/master/developer_guides/Integration%20Server%20Guide.pdf).

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.

After installing the package, Resilient Circuits creates a new section, *fn\_sep*, in the app.config file. You need to edit the following settings in that section.

[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>

# Limit result sent to Resilient, add full result as an attachment.

sep\_results\_limit=200

# Period of time to wait for all endpoints to return a scan result.  
sep\_scan\_timeout=1800

## Configuring Generic Email Parsing Script

Refer to the Generic Email Parsing Script package for setup instructions. You need to configure the Symantec Endpoint Protection Manager (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

# Add entries to these lists to whitelist the entries without disrupting the standard set above

# Whitelist SEPM server ip addresses

customIPv4WhiteList = [CIDR("192.168.194.93")]

customIPv6WhiteList = [CIDR("2002:835:c36d::946:c25d")]

# Standard domain whitelist

# Whitelist SEPM domain

domainWhiteList=[Domain("\*.sepmdomain.com")]

# Customer-specific domain whitelist

# Whitelist SEPM hostname

## Useful links

More information is available at: [Symantec Endpoint Protection 14 documentation](https://support.symantec.com/us/en/article.howto124729.html#sep14)

And more specifically for the API: [Symantec Endpoint Protection REST API documentation](https://apidocs.symantec.com/home/saep)

Setting up SEPM quarantine policy: [Creating a Quarantine policy for a failed Host Integrity check](https://support.symantec.com/us/en/article.howto101741.html)

Setting up SEPM for system lockdown: [Running system lockdown in blacklist mode](https://support.symantec.com/us/en/article.HOWTO81100.html#v69910011)

Setting up SEPM for email notifications: [How to Configure Symantec Endpoint Protection Manager to Send Email Alerts](https://support.symantec.com/us/en/article.tech104394.html)

# 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** |
| SEP - Scan Endpoints | Example: SEP - Initiate EOC Scan for Artifact | Example: SEP - Initiate EOC Scan for Artifact |
| Example: SEP - Remediate Artifact on Endpoint | Example: SEP - Remediate Artifact on Endpoint |
| SEP - Upload File to SEPM | Example: SEP - Upload file to SEPM server | Example: SEP - Upload file to SEPM server |
| SEP - Get File Content as Base64 | Example: SEP - Get File Content as Base64 string | Example: SEP - Get File Content as Base64 string |

**Endpoint related functions**

|  |  |  |
| --- | --- | --- |
| **Function** | **Workflow** | **Rule** |
| SEP - Get Computers | Example: SEP - Get Endpoint Details | Example: SEP - Get Endpoint Details |
| Example: SEP - Get Endpoints status | Example: SEP - Get Endpoints status |
| Example: SEP - Get Endpoints status (refresh) | Example: SEP - Get Endpoints status (refresh) |
| Example: SEP - Get Non-Compliant Endpoints status details | Example: SEP - Get Non-Compliant Endpoints status details |
| SEP - Move endpoint | Example: SEP - Move Endpoint | Example: SEP - Move Endpoint |
| SEP - Quarantine Endpoints | Example: SEP - Quarantine Endpoint | Example: SEP - Quarantine Endpoint |

**Fingerprint list related functions**

|  |  |  |
| --- | --- | --- |
| **Function** | **Workflow** | **Rule** |
| 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 |
| SEP - Update Fingerprint List | Example: SEP - Add Hash to Blacklist | Example: SEP - Add Hash to Blacklist |
| Example: SEP - Delete Hash from Blacklist | Example: SEP - Delete Hash from Blacklist |
| 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 |
| SEP - Delete Fingerprint List | Example: SEP - Delete Blacklist | Example: SEP - Delete Blacklist |

**Support functions**

|  |  |  |
| --- | --- | --- |
| **Function** | **Workflow** | **Rule** |
| SEP - Get Command Status | Example: SEP - Get Scan results | Example: SEP - Get Scan results |
| Example: SEP - Get Remediation status | Example: SEP - Get Remediation status |
| Example: SEP - Get Upload status | Example: SEP - Get Upload status |
| Example: SEP - Get Quarantine status | Example: SEP - Get Quarantine status |
| 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**: Functions 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

# 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:

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

# Function descriptions

## SEP - Scan Endpoints

Use the function to initiate an Evidence of Compromise (EOC) scan against a list of endpoints or groups. The function can also be used to complete a remediation delete action on a sha256 hash value in conjunction with a scan. 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 | No | 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.

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**.**A screenshot of a cell phone

   Description automatically generated**

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”.

A screenshot of a cell phone

Description automatically generated

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](#_SEP_-_Get) for more information on rule/workflow “Example: SEP - Get Scan results”.

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

A screenshot of a cell phone

Description automatically generated

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

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 (delete) 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”.

A screenshot of a cell phone

Description automatically generated

This invokes the “Example: SEP - Remediate Artifact on Endpoint” workflow, which calls the “SEP - Scan Endpoints” function. This workflow initiates a remediation or delete 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](#_SEP_-_Get) for more information on rule/workflow “Example: SEP - Get Remediation status”.

**NOTE**: When a remediation action is successful on an endpoint, it deletes 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 deleted on the endpoint.

## 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 a value from selected data table row.
* sep\_file\_path is mapped to value from selected data table row.
* sep\_sha256 is mapped to value from selected data table row.
* sep\_sha1 is mapped to value from selected data table row.
* sep\_md5 is mapped to value from selected data table row.
* sep\_source is selected from value in an activity field drop-down list.

**NOTE**: Only one of md5, sha1 or sha256 is mapped to an artifact value for each execution.

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.**

A screenshot of a cell phone

Description automatically generated

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

A screenshot of a cell phone

Description automatically generated

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](#_SEP_-_Get) for more information on rule/workflow “Example: SEP - Get Upload status”.

## SEP - Get File Content as Base64

Use the function to get the binary file content for a given file ID. 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 is mapped to value from 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.**

A screenshot of a cell phone

Description automatically generated

## 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**.

A screenshot of a cell phone

Description automatically generated

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**

**A screenshot of a social media post

Description automatically generated**

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.

A screenshot of a social media post

Description automatically generated

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”.

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

A screenshot of a cell phone

Description automatically generated

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

A screenshot of a social media post

Description automatically generated

Once a match has been found, two actions are enabled for the matching row including “Example: SEP - Get Endpoints status (refresh)” and “Example: SEP - Get Non-Compliant Endpoints status details”.

A screenshot of a social media post

Description automatically generated

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”.

A screenshot of a cell phone

Description automatically generated

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

## 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**.

A screenshot of a cell phone

Description automatically generated

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

A screenshot of a cell phone

Description automatically generated

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.

A screenshot of a cell phone

Description automatically generated

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

## SEP - Quarantine Endpoints

Use the function to quarantine or un-quarantine Symantec Endpoint Protection 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 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 status” is set to “Available”.

A screenshot of a cell phone

Description automatically generated

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](#_SEP_-_Get) 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 status” is transitioned to “Quarantined”.

A screenshot of a cell phone

Description automatically generated

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 status” is set to “Quarantined”.

A screenshot of a cell phone

Description automatically generated

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](#_SEP_-_Get) 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” is transitioned to “Available”.

A screenshot of a cell phone

Description automatically generated

## SEP - Get Fingerprint List

Use the function to get the file 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**.

A screenshot of a cell phone

Description automatically generated

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.

A screenshot of a cell phone

Description automatically generated

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.

A screenshot of a social media post

Description automatically generated

## 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**.

**A screenshot of a cell phone

Description automatically generated**

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.

A screenshot of a cell phone

Description automatically generated

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.

## SEP - Update Fingerprint List

Use the function to update an existing fingerprint list with a set of hash values. 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\_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](#_SEP_-_Add) for details.

## 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**.

A screenshot of a cell phone

Description automatically generated

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

A screenshot of a cell phone

Description automatically generated

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.

A screenshot of a social media post

Description automatically generated

## 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.

**A screenshot of a cell phone

Description automatically generated**

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.

**A screenshot of a cell phone

Description automatically generated**

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 already 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.

## SEP - Delete Fingerprint List

Use the function to delete a file 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 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**.

A screenshot of a social media post

Description automatically generated

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.

## 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”, “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**.

A screenshot of a social media post

Description automatically generated

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

A screenshot of a cell phone

Description automatically generated

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.

A screenshot of a social media post

Description automatically generated

**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**.

A screenshot of a cell phone

Description automatically generated

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

A screenshot of a social media post

Description automatically generated

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**.

A screenshot of a cell phone

Description automatically generated

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.

A screenshot of a social media post

Description automatically generated

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**.

A screenshot of a cell phone

Description automatically generated

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

## 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”.

# 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**.

A screenshot of a cell phone

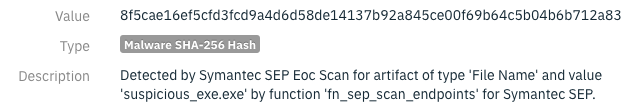
Description automatically generated

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 screenshot of a cell phone

Description automatically generated

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



# Notifications description

## Parsing Notifications of critical events

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 Symantec Endpoint Protection manager. An incident is generated from the notification event which includes artifacts for suspect files and endpoint names.

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

A screenshot of a cell phone

Description automatically generated

## 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 screenshot of a cell phone

Description automatically generated

A new incident is generated for the notification event.

## 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.

A screenshot of a cell phone

Description automatically generated

These artifacts can be used to initiate lookups, scans, and remedial actions in the Symantec Endpoint Protection environment.

# Configuring Symantec Endpoint Protection

Access to the Symantec Endpoint Protection Manager (SEPM) 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.

# Inform Resilient Users

The target audience for this guide is the Resilient playbook designer. These users configure the incident response aspect of the Resilient platform, including rules, functions, workflows, data tables, custom fields, and so on. Provide any helpful advice to help them get the maximum benefit of the integration in their environments.

The Resilient platform has another class of users, incident responders. These responders can be analysts, IT, and Support. With them in mind, provide any helpful advice about how to best use this integration in the context of an incident. For example, your integration may populate a data table which also allows a user to perform an action on your product directly from the data table.

To better understand these users, see the *User Guide* and *Platform Playbook Designer Guide*. You can find these documents in the Resilient platform’s Help/Contact menu, or online in the [IBM Knowledge Center](https://www.ibm.com/support/knowledgecenter/SSBRUQ).