SLASHNEXT

USER GUIDE V1.0

SlashNext Phishing Incident Response Guide for ThreatConnect

TABLE OF CONTENTS

TABLE OF CONTENTS

1 | INTRODUCTION

This document outlines the process to install the Phishing Incident Response Application provided by SlashNext into the ThreatConnect platform and also provides details on how to efficiently use the integrated action commands for on-demand threat intelligence APIs to request reputation and real-time scan of specific IoCs.

SlashNext Phishing Incident Response Playbook app enables ThreatConnect users to fully automate analysis of suspicious URLs. For example, IR teams responsible for abuse inbox management can extract links or domains out of suspicious emails and automatically analyze them with the SlashNext SEER™ threat detection cloud to get definitive, binary verdicts (malicious or benign) along with IOCs, screenshots, and more. Automating URL analysis can save IR teams hundreds of hours versus manually triaging these emails or checking URLs and domains against less accurate phishing databases and domain reputation services.

SlashNext threat detection uses browsers in a purpose-built cloud to dynamically inspect page contents and site behavior in real-time. This method enables SlashNext to follow URL re-directs and multi-stage attacks to more thoroughly analyze the final page(s) and make a much more accurate, binary determination with near-zero false positives. It also detects all six major categories of phishing and social engineering sites. These include credential stealing, rogue software / malware sites, scare-ware, phishing exploits (sites hosting weaponized documents, etc.), and social engineering scams (fake deals, giveaways, etc.).

SlashNext not only provides accurate, binary verdicts (rather than threat scores), it provides IoC metadata and screen-shots of detected phishing pages. These enable easier classification and reporting. Screen-shots can be used as an aid in on-going employee phishing awareness training and testing.

2 | CONFIGURATION

2.1 | REQUIREMENT

The following requirements must be met to use **SlashNext Phishing Incident Response** app in your ThreatConnect Playbooks:

- Access to ThreatConnect instance
- Access to execute ThreatConnect Playbooks
- SlashNext API Key provisioned by SlashNext to authenticate requests to SlashNext cloud
- **SlashNext Phishing Incident Response** app installed in ThreatConnect Instance. (See **App Installation** section)

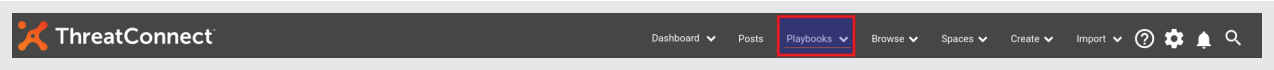
2.2 | APP INSTALLATION

SlashNext Phishing Incident Response app for ThreatConnect is available on Github at: Github Link. Download the app package with tcx extension and install it in your instance. To install the app in your ThreatConnect instance, refer to the ThreatConnect System Administration Guide (Install an App) for more information or contact your ThreatConnect Customer Success Engineer.

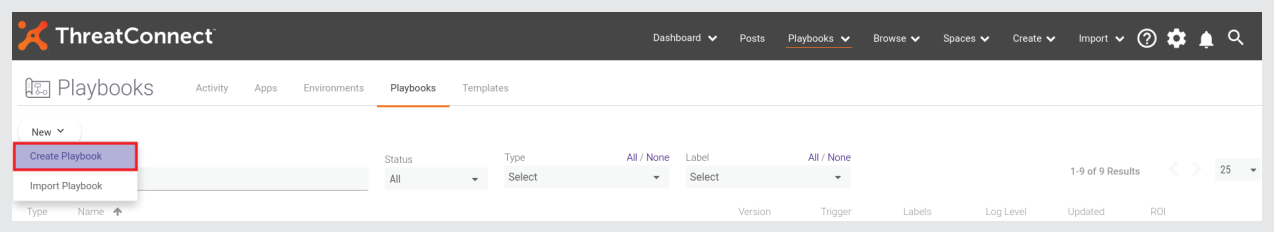
2.3 | APP CONFIGURATION

In order to demonstrate configuration of **SlashNext Phishing Incident Reponse** app in ThreatConnect's Playbook editor, let us create a sample Playbook as below:

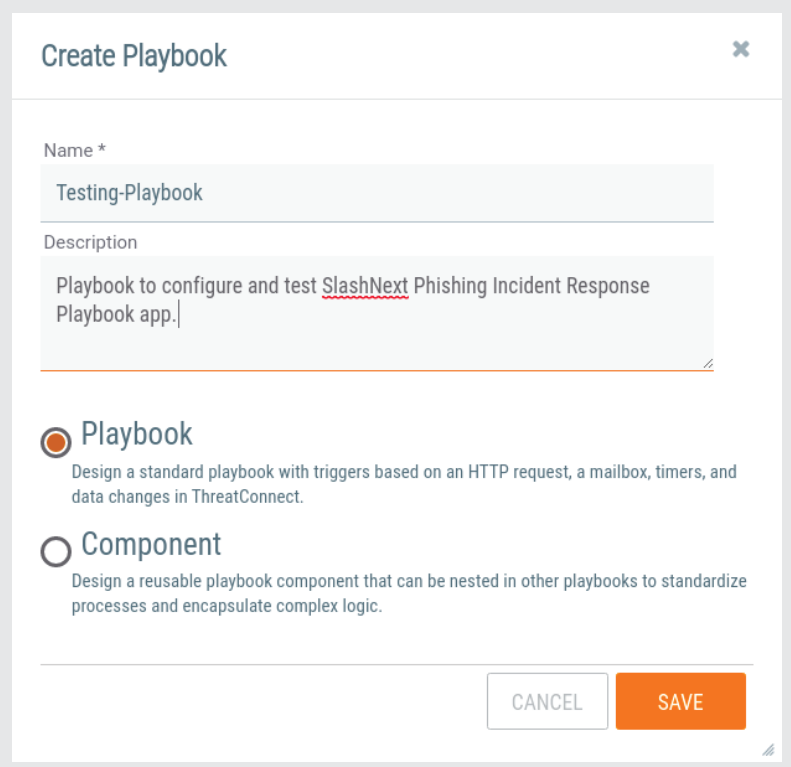
1. Click on **Playbooks** button on the top menu-bar to go to the Playbooks page.



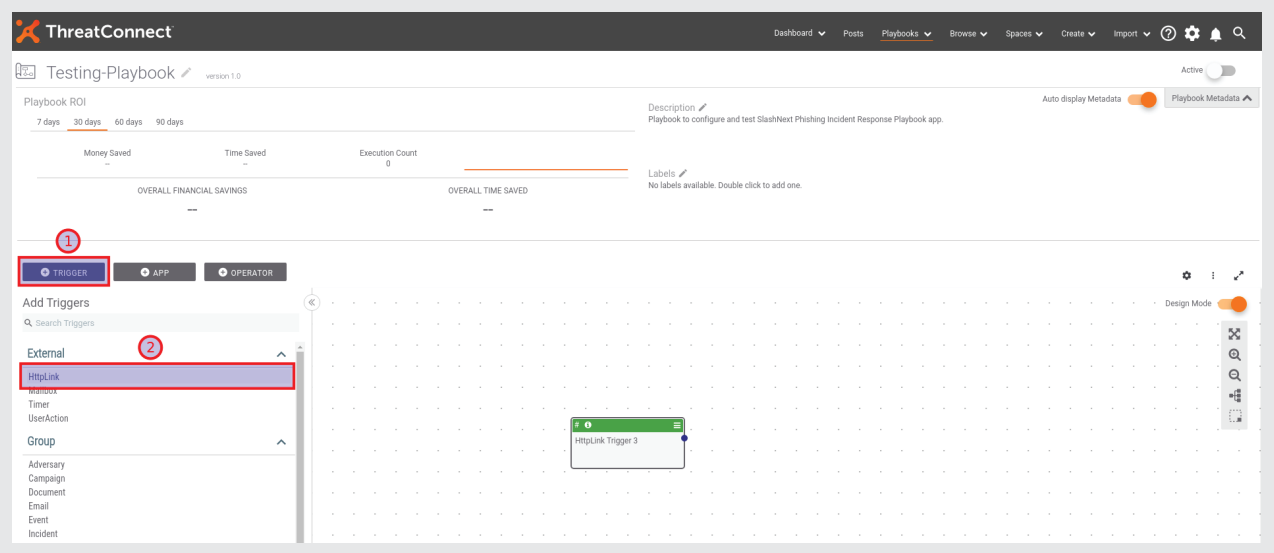
2. Hover the cursor over the **New** button on the left side of the page and click on **Create Playbook** from the drop-down menu.



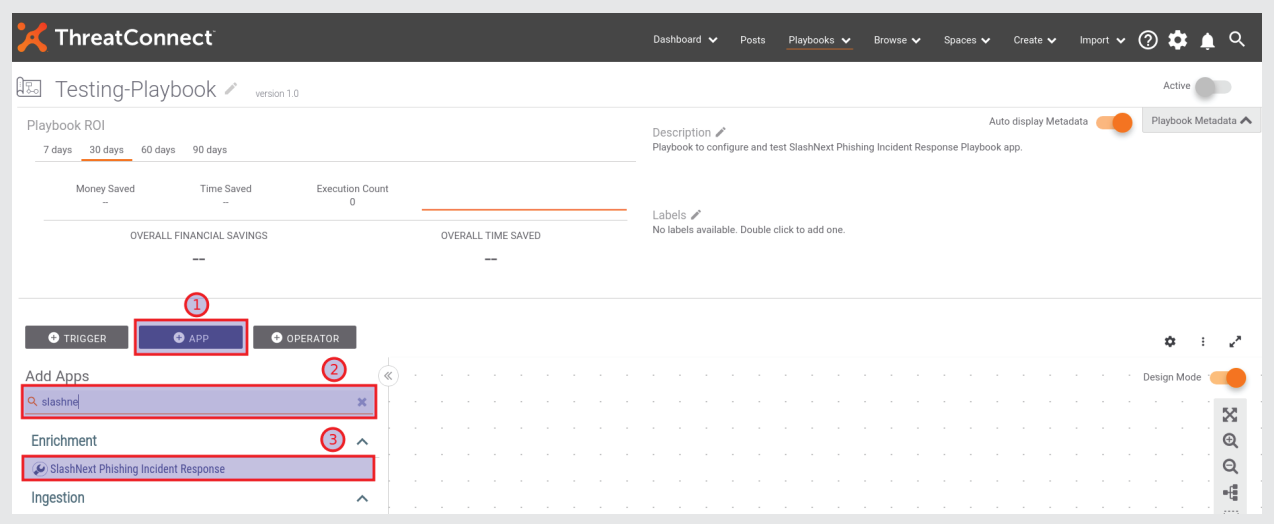
3. The **Create Playbook** dialog box will appear. Choose a suitable **Name** and **Description** for the sample Playbook and click **Save**. The page will then automatically redirect you to the Playbook editor.



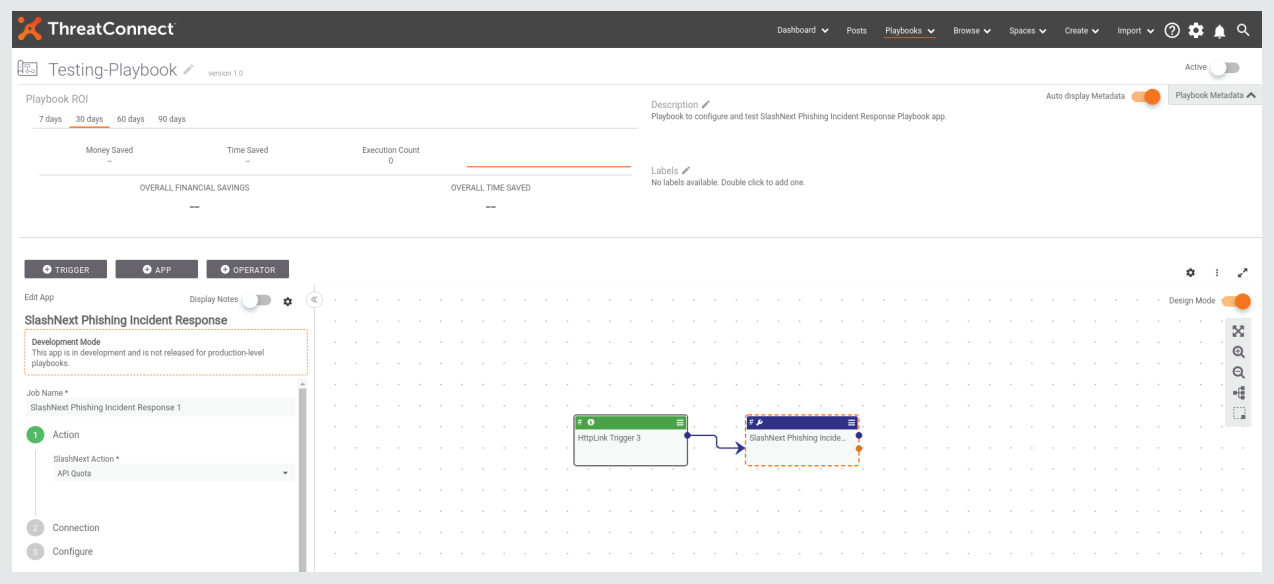
4. In order to test the running of the app, you will a Trigger block to trigger the app to run. Click on + **TRIGGER** button and select **HttpLink**. This will provide you with an endpoint URL to signal the Playbook to run.



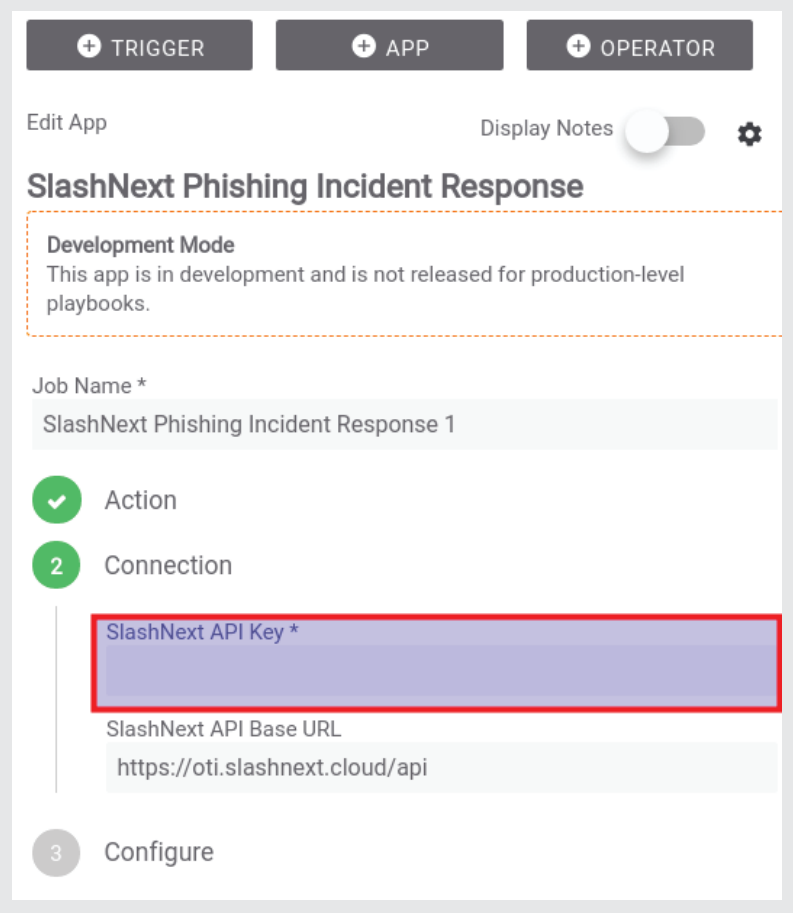
5. In the Playbook editor page, click on + **APP** button to select the ThreatConnect app to be imported into the Playbook. Next search for **"slashnext"** to filter out all of SlashNext's apps in the ThreatConnect Platform and choose the **SlashNext Phishing Incident Response** app.



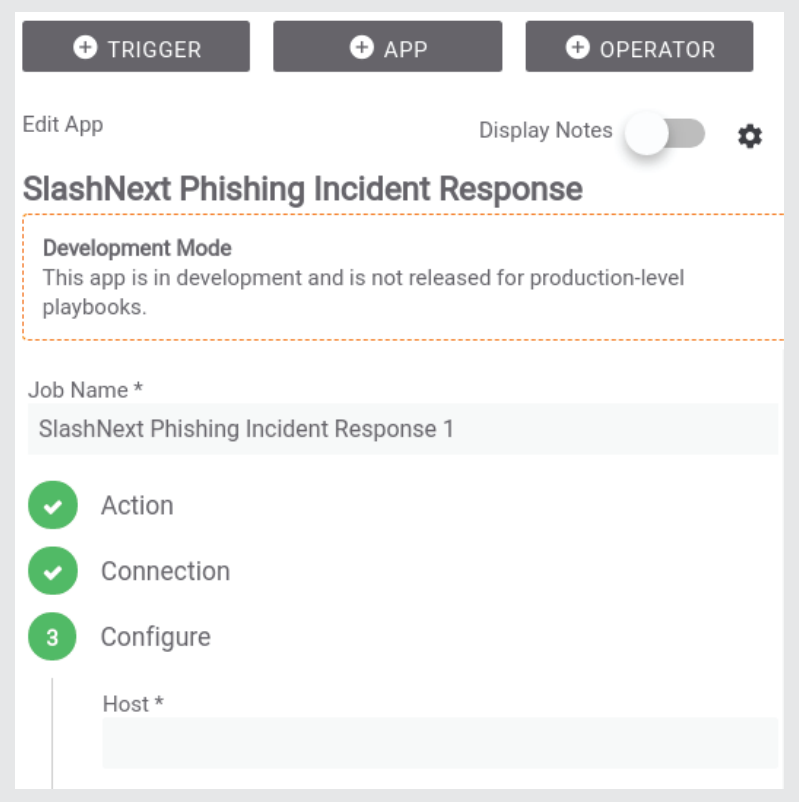
6. Once you click on the app, it will appear in the Playbook editor as shown below. Connect the output of the trigger block to the app block as shown in the figure below. Double click on the app block to view the **Edit App** panel on the left side. The **SlashNext Phishing Incident Response** app has three configurations steps. The **Action** step is used to select one of the SlashNext Actions (For detailed information on all of the available app actions, please refer to **Actions** section) to be performed.



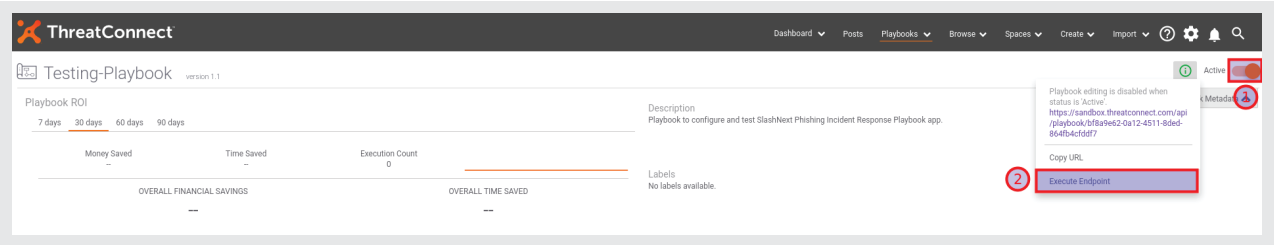
7. Click on **Next** to see the second step **Connection**, which is used to configure the connectivity between the app and Slash-Next's back-end cloud. In this step, enter the API key provided to you by SlashNext in the **SlashNext API Key** text-box. For **SlashNext API Base URL** parameter, use the default value until or unless another value is provided by **SlashNext, Inc**.



8. The final step, **Configure** is used to set the input action parameters to the app according to each specific action. For a detailed overview of parameters required for each action, please refer to **Actions** section. Click on Save to finish the app configuration settings. At this point, the **SlashNext Phishing Incident Response** app block's configuration is complete and is ready to be used with other objects of the Playbook as required by the user.



9. To run the Playbook, toogle the **Active** button on the top-right corner of the Playbook editor. A green exclamation symbol will appear on its left if all the apps in the Playbook have been configured properly. Click on the green exclamation and it will show the endpoint URL that you need to hit in order to trigger the Playbook to run. Optionally, you can click on **Execute Endpoint** menu-item to do this automatically.



3 | ACTIONS

SlashNext Phishing Incident Response integration app's supported actions and outputs are listed below.

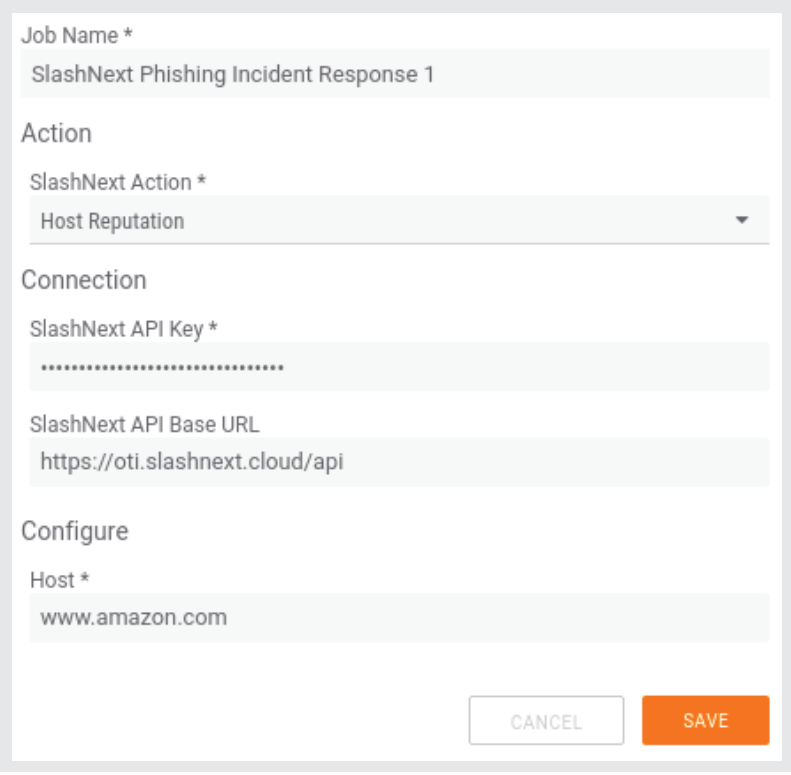
1. **Host Reputation** - Queries the SlashNext Cloud database and retrieves the reputation of a host.
2. **Host Report** - Queries the SlashNext Cloud database and retrieves a detailed report.
3. **Host URLs** - Queries the SlashNext Cloud database and retrieves a list of all URLs.
4. **URL Scan** - Performs a real-time URL reputation scan with SlashNext cloud-based SEER Engine
5. **URL Scan Sync** - Performs a real-time URL scan with SlashNext cloud-based SEER Engine in a blocking mode.
6. **Scan Report** - Retrieves URL scan results against a previous Scan request.
7. **Download Screenshot** - Downloads a screenshot of a web page against a previous URL Scan request.
8. **Download HTML** - Downloads a web page HTML against a previous URL Scan request.
9. **Download Text** - Downloads the text of a web page against a previous URL Scan request.
10. **API Quota** - Finds information about your API quota, like current usage, quota left etc.

3.1 | HOST REPUTATION

Queries the SlashNext Cloud database and retrieves the reputation of a host.

3.1.1 | ACTION PARAMETERS

PARAMETER	REQUIRED	DESCRIPTION	THREAT CONNECT TYPE	CONTAINS
Host	True	The host to look up in the SlashNext Threat Intelligence database. It can be either a domain name or an IPv4 address	String	Domain/IP



3.1.2 | ACTION OUTPUTS

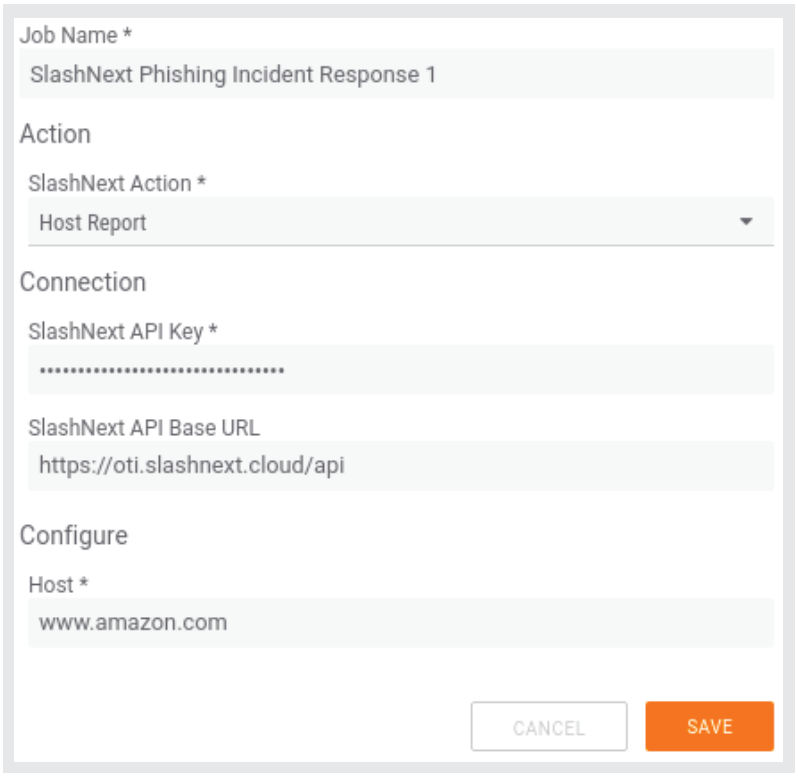
OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.host.reputation.parameters.host	The Host value input to the Host Reputation action echoed back as an output	String
#snx.host.reputation.threatStatus	Status of threat posed by Host ("Active"/"No Longer Active" etc)	String
#snx.host.reputation.threatName	Name of threat posed by Host ("Fake Login Page"/"Scareware" etc)	String
#snx.host.reputation.threatType	Type of threat posed by Host ("Malware & Exploit"/"Phishing & Social Engineering" etc)	String
#snx.host.reputation.firstSeen	Threat first observed time in UTC ("mm-dd-yyyy hh:mm:ss UTC" etc)	String
#snx.host.reputation.verdict	Verdict of the Host reputation execution ("Malicious"/"Benign" etc)	String
#snx.host.reputation.lastSeen	Threat last observed time in UTC ("mm-dd-yyyy hh:mm:ss UTC" etc)	String
#snx.host.reputation.rawJSON	Raw JSON response from Host Reputation SlashNext API for debugging purposes	String
#snx.action.summary	Summary of Host Reputation action execution	String
#snx.action.errorNo	Error Number returned by SlashNext Cloud in case of any error (0 for successful execution)	String
#snx.action.errorMsg	Error Message returned by SlashNext Cloud in case of any error ("Success" for successful execution)	String

3.2 | HOST REPORT

Queries the SlashNext Cloud database and retrieves a detailed report for a host and associated URL.

3.2.1 | ACTION PARAMETERS

PARAMETER	REQUIRED	DESCRIPTION	THREAT CONNECT TYPE	CONTAINS
Host	True	The host to look up in the SlashNext Threat Intelligence database. Can be either a domain name or an IPv4 address	String	Domain/IP



3.2.2 | ACTION OUTPUTS

OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.host.report.parameters.host	The Host value input to the Host Report action echoed back as an output	String
#snx.host.report.reputation.threatStatus	Status of threat posed by Host ("Active"/"No Longer Active" etc)	String
#snx.host.report.reputation.threatName	Name of threat posed by Host ("Fake Login Page"/"Scareware" etc)	String
#snx.host.report.reputation.threatType	Type of threat posed by Host ("Malware & Exploit"/"Phishing & Social Engineering" etc)	String
#snx.host.report.reputation.firstSeen	Threat first observed time in UTC ("mm-dd-yyyy hh:mm:ss UTC" etc)	String
#snx.host.report.reputation.verdict	Verdict of the Host Reputation execution ("Malicious"/"Benign" etc)	String
#snx.host.report.reputation.lastSeen	Threat last observed time in UTC ("mm-dd-yyyy hh:mm:ss UTC" etc)	String
#snx.host.report.reputation.rawJSON	Raw JSON response of the Host reputation SlashNext API for debugging purposes	KeyValue
#snx.host.report.latestURL	The latest scanned URL of the Host	String
#snx.host.report.latestURL.scanID	The scan ID assigned by SlashNext to the latest scanned URL of the Host	String
#snx.host.report.latestURL.threatStatus	Status of threat posed by Host's latest URL ("Active"/"No Longer Active" etc)	String
#snx.host.report.latestURL.threatName	Name of threat posed by Host's latest URL ("Fake Login Page"/"Scareware" etc)	String
#snx.host.report.latestURL.threatType	Type of threat posed by Host's latest URL ("Malware & Exploit"/"Phishing & Social Engineering" etc)	String
#snx.host.report.latestURL.firstSeen	Latest URL's threat first observed time in UTC ("mm-dd-yyyy hh:mm:ss UTC" etc)	String
#snx.host.report.latestURL.verdict	Verdict of the latest URL of the Host ("Malicious"/"Benign" etc)	String
#snx.host.report.latestURL.lastSeen	Latest URL's threat last observed time in UTC ("mm-dd-yyyy hh:mm:ss UTC" etc)	String
#snx.host.report.latestURL.rawJSON	Raw JSON response of the latest URL SlashNext API for debugging purposes	KeyValue
#snx.host.report.latestURL.redirectedURL	Redirected URL (if exists) of the latest URL of the Host	String

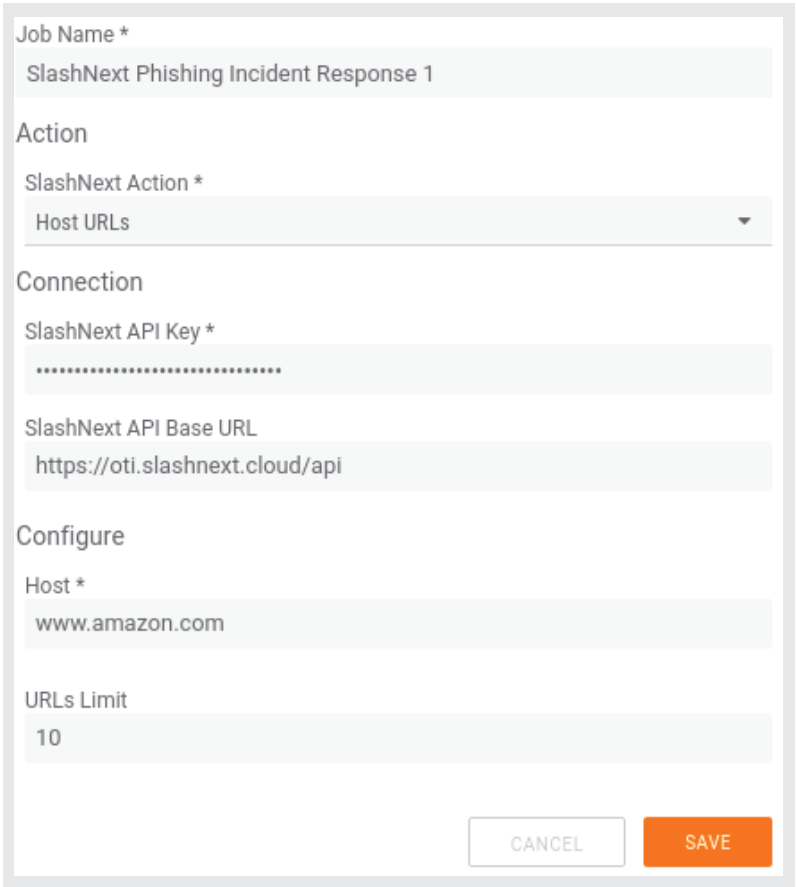
OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.host.report.latestURL.redirectedURL.scanID	Scan ID assigned to the redirected URL (if exists) of the latest URL of the Host	String
#snx.host.report.latestURL.redirectedURL.threatStatus	Threat status of the redirected URL (if exists) of the latest URL of the Host	String
#snx.host.report.latestURL.redirectedURL.threatName	Threat name of the redirected URL (if exists) of the latest URL of the Host	String
#snx.host.report.latestURL.redirectedURL.threatType	Threat type of the redirected URL (if exists) of the latest URL of the Host	String
#snx.host.report.latestURL.redirectedURL.firstSeen	Redirected URL's (if exists) threat first observed time in UTC	String
#snx.host.report.latestURL.redirectedURL.verdict	Verdict of the redirected URL (if exists) of the host's latest URL	String
#snx.host.report.latestURL.redirectedURL.lastSeen	Redirected URL's (if exists) threat last observed time in UTC	String
#snx.host.report.latestURL.scData.scBase64	Raw screenshot data of latest URL (JPEG type) encoded in Base64 format	String
#snx.host.report.latestURL.htmlData.htmlBase64	Raw HTML data of the latest URL in Base64 format	String
#snx.host.report.latestURL.textData.textBase64	Raw Text data of the latest URL in Base64 format	String
#snx.action.summary	Summary of Host Report action execution	String
#snx.action.errorNo	Error Number returned by SlashNext Cloud in case of any error (0 for successful execution)	String
#snx.action.errorMsg	Error Message returned by SlashNext Cloud in case of any error ("Success" for successful execution)	String

3.3 | HOST URLs

Queries the SlashNext Cloud database and retrieves a list of all URLs associated with the specified host.

3.3.1 | ACTION PARAMETERS

PARAMETER	REQUIRED	DESCRIPTION	THREAT CONNECT TYPE	CONTAINS
Host	True	The Host to look up in the SlashNext Threat Intelligence database, for which to return a list of associated URLs. It can either be a domain name or an IPv4 address	String	Domain/IP
Limit	False	The maximum number of URL records to fetch. Default is "10"	String	Integer



3.3.2 | ACTION OUTPUTS

OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.host.urls.parameters.host	The Host value input to the Host URLs action echoed back as an output	String
#snx.host.urls.parameters.urls_limit	The Limit value input to the Host URLs actions echoed back as an output	String
#snx.host.urls	Array containing all the URLs fetched for the required Host	StringArray
#snx.host.urls.threatStatus	Array containing Threat Statuses of all the fetched URLs in 1-to-1 correspondence	StringArray
#snx.host.urls.threatName	Array containing Threat Names of all the fetched URLs in 1-to-1 correspondence	StringArray
#snx.host.urls.threatType	Array containing Threat Types of all the fetched URLs in 1-to-1 correspondence	StringArray
#snx.host.urls.firstSeen	Array containing Threat's first seen UTC time of all the fetched URLs in 1-to-1 correspondence	StringArray
#snx.host.urls.verdict	Array containing verdicts on all the fetched URLs in 1-to-1 correspondence	StringArray
#snx.host.urls.lastSeen	Array containing Threat's last seen UTC time of all the fetched URLs in 1-to-1 correspondence	StringArray
#snx.host.urls.scanID	Array containing Scan IDs assigned to all the fetched URLs in 1-to-1 correspondence (A value of "N/A" indicates that the URL is not yet scanned and has to be manually scanned by the user by using "URL Scan" or "URL Scan Sync" actions)	StringArray
#snx.host.urls.rawJSON	Raw JSON response from SlashNext API for debugging purposes	KeyValue
#snx.host.urls.redirectedURLs	Array containing the redirected URL (if exists) of all the fetched URLs in 1-to-1 correspondence	StringArray
#snx.host.urls.redirectedURLs.threatStatus	Array containing the Threat Status of redirected URL (if exists) of all the fetched URLs in 1-to-1 correspondence	StringArray
#snx.host.urls.redirectedURLs.threatName	Array containing the Threat Name of redirected URL (if exists) of all the fetched URLs in 1-to-1 correspondence	StringArray
#snx.host.urls.redirectedURLs.threatType	Array containing the Threat Type of redirected URL (if exists) of all the fetched URLs in 1-to-1 correspondence	StringArray
#snx.host.urls.redirectedURLs.firstSeen	Array containing the Threat's first seen UTC time of redirected URL (if exists) of all the fetched URLs in 1-to-1 correspondence	StringArray

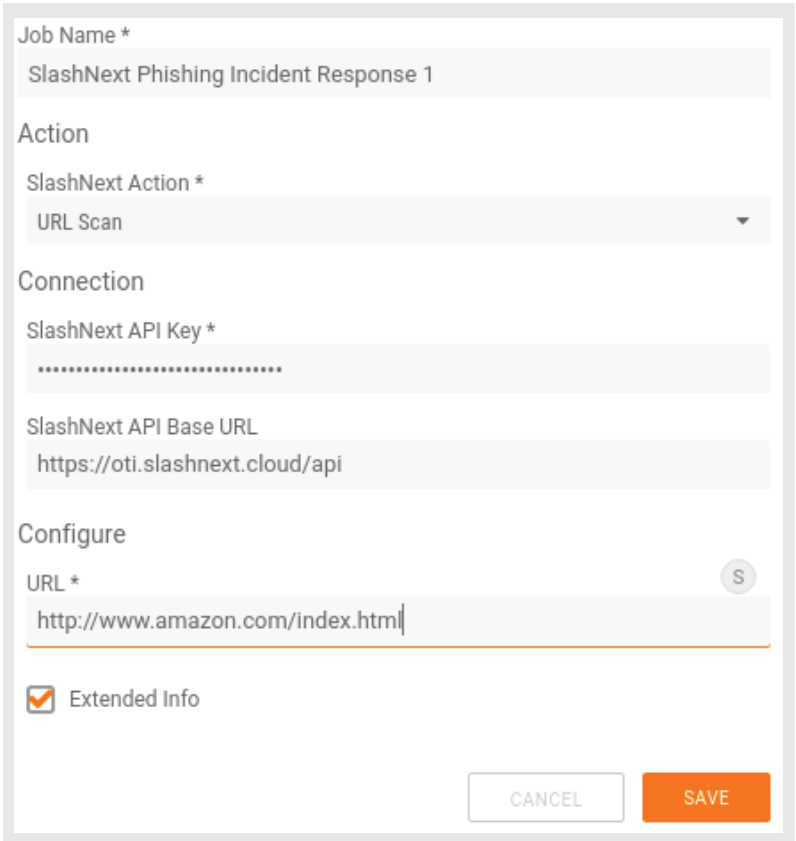
OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.host.urls.redirectedURLs.verdict	Array containing the verdict of redirected URL (if exists) of all the fetched URLs in 1-to-1 correspondence	StringArray
#snx.host.urls.redirectedURLs.lastSeen	Array containing the Threat's last seen UTC time of redirected URL (if exists) of all the fetched URLs in 1-to-1 correspondence	StringArray
#snx.host.urls.redirectedURLs.scanID	Array containing Scan IDs assigned to the redirected URL (if exists) of all the fetched URLs in 1-to-1 correspondence	StringArray
#snx.action.summary	Summary of Host URLs action execution	String
#snx.action.errorNo	Error Number returned by SlashNext Cloud in case of any error (0 for successful execution)	String
#snx.action.errorMsg	Error Message returned by SlashNext Cloud in case of any error ("Success" for successful execution)	String

3.4 | URL SCAN

Performs a real-time URL reputation scan with SlashNext cloud-based SEER Engine. If the specified URL already exists in the cloud database, scan results will be returned immediately. If not, this command will submit a URL scan request and return with the message "check back later" and include a unique Scan ID. You can check the results of this scan using the "Scan Report" action anytime after 60 seconds using the returned Scan ID.

3.4.1 | ACTION PARAMETERS

PARAMETER	REQUIRED	DESCRIPTION	THREAT CONNECT TYPE	CONTAINS
URL	True	The URL that needs to be scanned.	String	URL
Extended Info	False	Whether to download forensics data, such as Screenshot, HTML, and rendered text. If "checked", forensics data will be returned. If "unchecked" (or empty) forensics data will not be returned.	Binary	Boolean (True/False)



3.4.2 | ACTION OUTPUTS

OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.url.scan.parameters.url	The URL value input to the URL Scan action echoed back as an output	String
#snx.url.scan.parameters.extended_info	The Extended Info value input to the URL Scan action echoed back as an output	Binary
#snx.url.scan.scannedURL	The complete submitted URL to the SlashNext Cloud	String
#snx.url.scan.scannedURL.scanID	The scan ID assigned by SlashNext to the scanned URL	String
#snx.url.scan.scannedURL.threatStatus	Status of the threat posed by the scanned URL ("Active"/"No Longer Active" etc)	String
#snx.url.scan.scannedURL.threatName	Name of threat posed by the scanned URL ("Fake Login Page"/"Scareware" etc)	String
#snx.url.scan.scannedURL.threatType	Type of threat posed by the scanned URL ("Malware & Exploit"/"Phishing & Social Engineering" etc)	String
#snx.url.scan.scannedURL.firstSeen	Scanned URL's threat first observed time in UTC ("mm-dd-yyyy hh:mm:ss UTC" etc)	String
#snx.url.scan.scannedURL.verdict	Verdict of the scanned URL ("Malicious"/"Benign" etc)	String
#snx.url.scan.scannedURL.lastSeen	Scanned URL's threat last observed time in UTC ("mm-dd-yyyy hh:mm:ss UTC" etc)	String
#snx.url.scan.rawJSON	Raw JSON response of the URL Scan SlashNext API for debugging purposes	KeyValue
#snx.url.scan.scannedURL.redirectedURL	Redirected URL (if exists) of the Scanned URL	String
#snx.url.scan.scannedURL.redirectedURL.scanID	Scan ID assigned to the redirected URL (if exists) of the scanned URL	String
#snx.url.scan.scannedURL.redirectedURL.threatStatus	Threat status of the redirected URL (if exists) of the scanned URL	String
#snx.url.scan.scannedURL.redirectedURL.threatName	Threat name of the redirected URL (if exists) of the scanned URL	String
#snx.url.scan.scannedURL.redirectedURL.threatType	Threat type of the redirected URL (if exists) of the scanned URL	String
#snx.url.scan.scannedURL.redirectedURL.firstSeen	Redirected URL's (if exists) threat first observed time in UTC	String
#snx.url.scan.scannedURL.redirectedURL.verdict	Verdict of the redirected URL (if exists) of the scanned URL	String

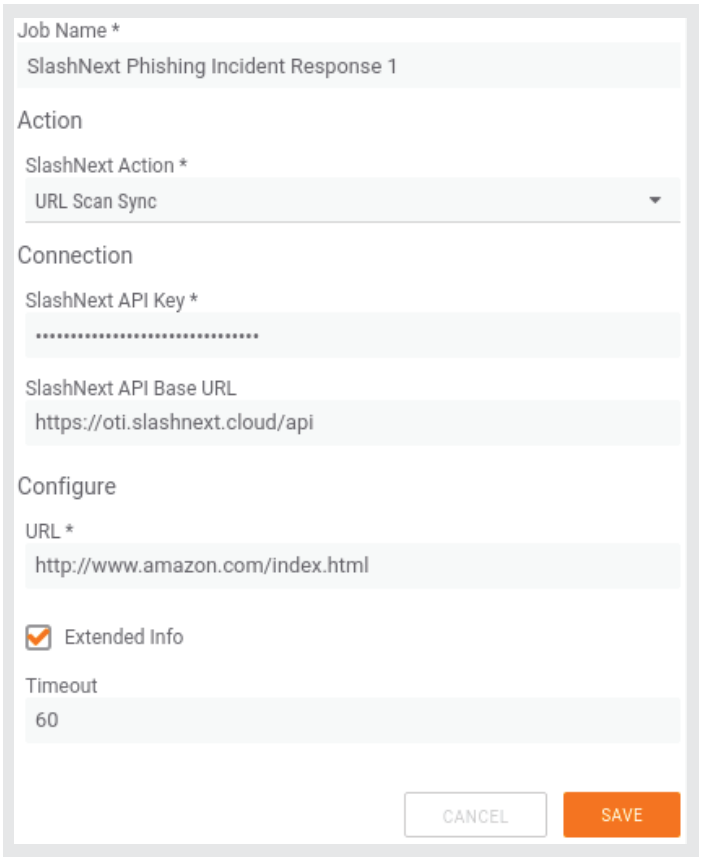
OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.url.scan.scannedURL.redirectedURL.lastSeen	Redirected URL's (if exists) threat last observed time in UTC	String
#snx.url.scan.scannedURL.scData.scBase64	Raw screenshot data (JPEG type) of scanned URL encoded in Base64 format (If "Extended Info" is True)	String
#snx.url.scan.scannedURL.htmlData.htmlBase64	Raw HTML data of the scanned URL in Base64 format (If "Extended Info" is True)	String
#snx.url.scan.scannedURL.textData.textBase64	Raw Text data of the scanned URL in Base64 format (If "Extended Info" is True)	String
#snx.action.summary	Summary of URL Scan action execution	String
#snx.action.errorNo	Error Number returned by SlashNext Cloud in case of any error (0 for successful execution)	String
#snx.action.errorMsg	Error Message returned by SlashNext Cloud in case of any error ("Success" for successful execution)	String

3.5 | URL SCAN SYNC

Performs a real-time URL scan with SlashNext cloud-based SEER Engine in a blocking mode. If the specified URL already exists in the cloud database, scan result will be returned immediately. If not, this command will submit a URL scan request and wait for the scan to finish. The scan may take up to 60 seconds to finish.

3.5.1 | ACTION PARAMETERS

PARAMETER	REQUIRED	DESCRIPTION	THREAT CONNECT TYPE	CONTAINS
URL	True	The URL that needs to be scanned.	String	URL
Extended Info	False	Whether to download forensics data, such as Screenshot, HTML, and rendered text. If "checked", forensics data will be returned. If "unchecked" (or empty) forensics data will not be returned.	Binary	Boolean (True/False)
Timeout	False	A timeout value in seconds. If the system is unable to complete a scan within the specified timeout, a timeout error will be returned. You can run the command again with a different timeout. If no timeout value is specified, a default timeout value is 60 seconds.	String	Integer



3.5.2 | ACTION OUTPUTS

OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.url.scansync.parameters.url	The URL value input to the URL Scan Sync action echoed back as an output	String
#snx.url.scansync.parameters.extended_info	The Extended Info value input to the URL Scan Sync action echoed back as an output	Binary
#snx.url.scansync.parameters.timeout	The Timeout value input to the URL Scan Sync action echoed back as an output	String
#snx.url.scansync.scannedURL	The complete submitted URL to the SlashNext Cloud	String
#snx.url.scansync.scannedURL.scanID	The scan ID assigned by SlashNext to the scanned URL	String
#snx.url.scansync.scannedURL.threatStatus	Status of the threat posed by the scanned URL ("Active"/"No Longer Active" etc)	String
#snx.url.scansync.scannedURL.threatName	Name of threat posed by the scanned URL ("Fake Login Page"/"Scareware" etc)	String
#snx.url.scansync.scannedURL.threatType	Type of threat posed by the scanned URL ("Malware & Exploit"/"Phishing & Social Engineering" etc)	String
#snx.url.scansync.scannedURL.firstSeen	Scanned URL's threat first observed time in UTC ("mm-dd-yyyy hh:mm:ss UTC" etc)	String
#snx.url.scansync.scannedURL.verdict	Verdict of the scanned URL ("Malicious"/"Benign" etc)	String
#snx.url.scansync.scannedURL.lastSeen	Scanned URL's threat last observed time in UTC ("mm-dd-yyyy hh:mm:ss UTC" etc)	String
#snx.url.scansync.rawJSON	Raw JSON response of the URL Scan Sync SlashNext API for debugging purposes	KeyValue
#snx.url.scansync.scannedURL.redirectedURL	Redirected URL (if exists) of the Scanned URL	String
#snx.url.scansync.scannedURL.redirectedURL.scanID	Scan ID assigned to the redirected URL (if exists) of the scanned URL	String
#snx.url.scansync.scannedURL.redirectedURL.threatStatus	Threat status of the redirected URL (if exists) of the scanned URL	String
#snx.url.scansync.scannedURL.redirectedURL.threatName	Threat name of the redirected URL (if exists) of the scanned URL	String
#snx.url.scansync.scannedURL.redirectedURL.threatType	Threat type of the redirected URL (if exists) of the scanned URL	String
#snx.url.scansync.scannedURL.redirectedURL.firstSeen	Redirected URL's (if exists) threat first observed time in UTC	String

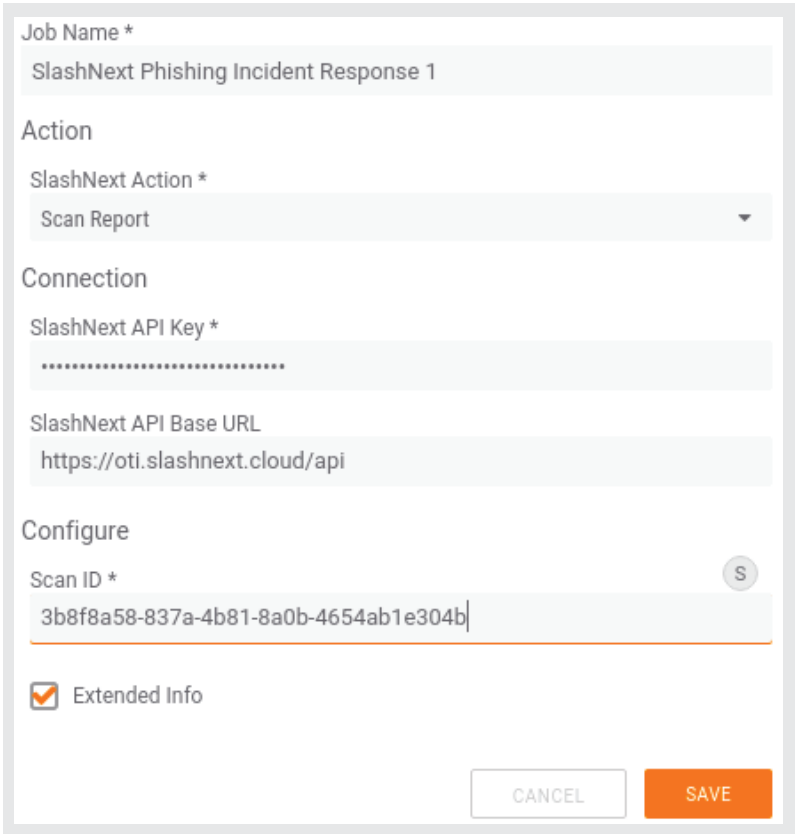
OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.url.scansync.scannedURL.redirectedURL.verdict	Verdict of the redirected URL (if exists) of the scanned URL	String
#snx.url.scansync.scannedURL.redirectedURL.lastSeen	Redirected URL's (if exists) threat last observed time in UTC	String
#snx.url.scansync.scannedURL.scData.scBase64	Raw screenshot data (JPEG type) of scanned URL encoded in Base64 format (If "Extended Info" is True)	String
#snx.url.scansync.scannedURL.htmlData.htmlBase64	Raw HTML data of the scanned URL in Base64 format (If "Extended Info" is True)	String
#snx.url.scansync.scannedURL.textData.textBase64	Raw Text data of the scanned URL in Base64 format (If "Extended Info" is True)	String
#snx.action.summary	Summary of URL Scan Sync action execution	String
#snx.action.errorNo	Error Number returned by SlashNext Cloud in case of any error (0 for successful execution)	String
#snx.action.errorMsg	Error Message returned by SlashNext Cloud in case of any error ("Success" for successful execution)	String

3.6 | SCAN REPORT

Retrieves the results of a URL scan against a previous scan request. If the scan is finished, results will be returned immediately; otherwise the message "check back later" will be returned

3.6.1 | ACTION PARAMETERS

PARAMETER	REQUIRED	DESCRIPTION	THREAT CONNECT TYPE	CONTAINS
Scan ID	True	Scan ID of the scan for which to get the report. It can be retrieved from the "URL Scan" action or "URL Scan Sync" action.	String	URL
Extended Info	False	Whether to download forensics data, such as Screenshot, HTML, and rendered text. If "checked", forensics data will be returned. If "unchecked" (or empty) forensics data will not be returned.	Binary	Boolean (True/False)



3.6.2 | ACTION OUTPUTS

OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.url.scanreport.parameters.scanID	The Scan ID value input to the Scan Report action echoed back as an output	String
#snx.url.scanreport.parameters.extended_info	The Extended Info value input to the Scan Report action echoed back as an output	Binary
#snx.scanID.scanreport.scannedURL	The complete URL scanned by the SlashNext Cloud	String
#snx.scanID.scanreport.scannedURL.scanID	The scan ID assigned by SlashNext to the scanned URL	String
#snx.scanID.scanreport.scannedURL.threatStatus	Status of the threat posed by the scanned URL ("Active"/"No Longer Active" etc)	String
#snx.scanID.scanreport.scannedURL.threatName	Name of threat posed by the scanned URL ("Fake Login Page"/"Scareware" etc)	String
#snx.scanID.scanreport.scannedURL.threatType	Type of threat posed by the scanned URL ("Malware & Exploit"/"Phishing & Social Engineering" etc)	String
#snx.scanID.scanreport.scannedURL.firstSeen	Scanned URL's threat first observed time in UTC ("mm-dd-yyyy hh:mm:ss UTC" etc)	String
#snx.scanID.scanreport.scannedURL.verdict	Verdict of the scanned URL ("Malicious"/"Benign" etc)	String
#snx.scanID.scanreport.scannedURL.lastSeen	Scanned URL's threat last observed time in UTC ("mm-dd-yyyy hh:mm:ss UTC" etc)	String
#snx.scanID.scanreport.rawJSON	Raw JSON response of the URL Scan SlashNext API for debugging purposes	KeyValue
#snx.scanID.scanreport.scannedURL.redirectedURL	Redirected URL (if exists) of the Scanned URL	KeyValue
#snx.scanID.scanreport.scannedURL.redirectedURL.scanID	Scan ID assigned to the redirected URL (if exists) of the scanned URL	String
#snx.scanID.scanreport.scannedURL.redirectedURL.threatStatus	Threat status of the redirected URL (if exists) of the scanned URL	String
#snx.scanID.scanreport.scannedURL.redirectedURL.threatName	Threat name of the redirected URL (if exists) of the scanned URL	String
#snx.scanID.scanreport.scannedURL.redirectedURL.threatType	Threat type of the redirected URL (if exists) of the scanned URL	String
#snx.scanID.scanreport.scannedURL.redirectedURL.firstSeen	Redirected URL's (if exists) threat first observed time in UTC	String
#snx.scanID.scanreport.scannedURL.redirectedURL.verdict	Verdict of the redirected URL (if exists) of the scanned URL	String

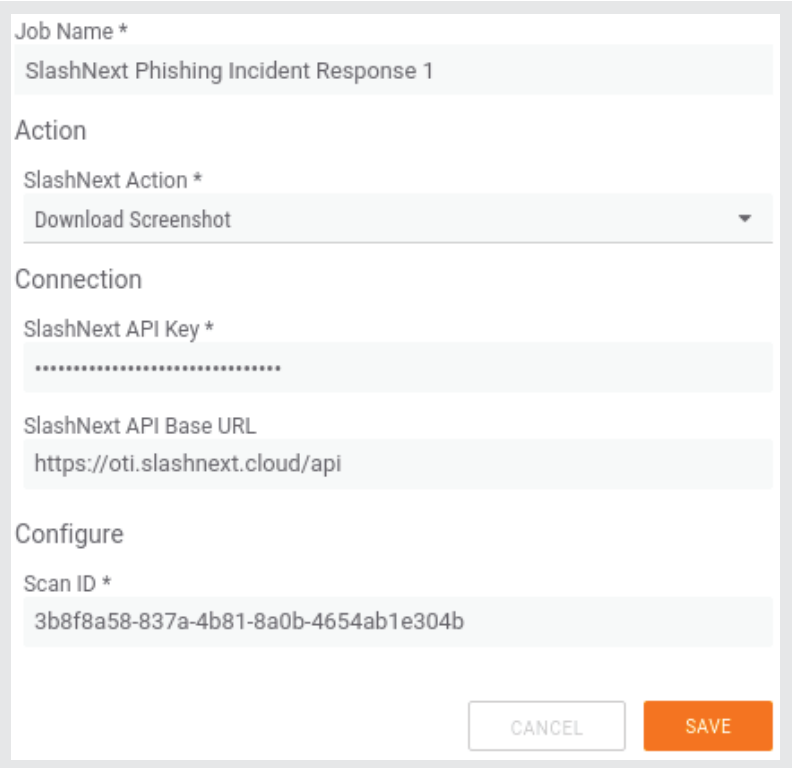
OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.scanID.scanreport.scannedURL.redirected URL.lastSeen	Redirected URL's (if exists) threat last observed time in UTC	String
#snx.scanID.scanreport.scannedURL.scData. scBase64	Raw screenshot data (JPEG type) of the scanned URL in Base64 format (If "Extended Info" is True)	Binary
#snx.scanID.scanreport.scannedURL.htmlData. htmlBase64	Raw HTML data of the scanned URL in Base64 format (If "Extended Info" is True)	String
#snx.scanID.scanreport.scannedURL.textData. textBase64	Raw Text data of the scanned URL in Base64 format (If "Extended Info" is True)	String
#snx.action.summary	Summary of Scan Report action execution	String
#snx.action.errorNo	Error Number returned by SlashNext Cloud in case of any error (0 for successful execution)	String
#snx.action.errorMsg	Error Message returned by SlashNext Cloud in case of any error ("Success" for successful execution)	String

3.7 | DOWNLOAD SCREENSHOT

Downloads a screenshot of a web page against a previous URL scan request.

3.7.1 | ACTION PARAMETERS

PARAMETER	REQUIRED	DESCRIPTION	THREAT CONNECT TYPE	CONTAINS
Scan ID	True	The Scan ID is a unique ID assigned by SlashNext Cloud to each scanning request and can be retrieved from the SlashNext "URL Scan" or the "URL Scan Sync" actions.	String	SlashNext Scan ID



3.7.2 | ACTION OUTPUTS

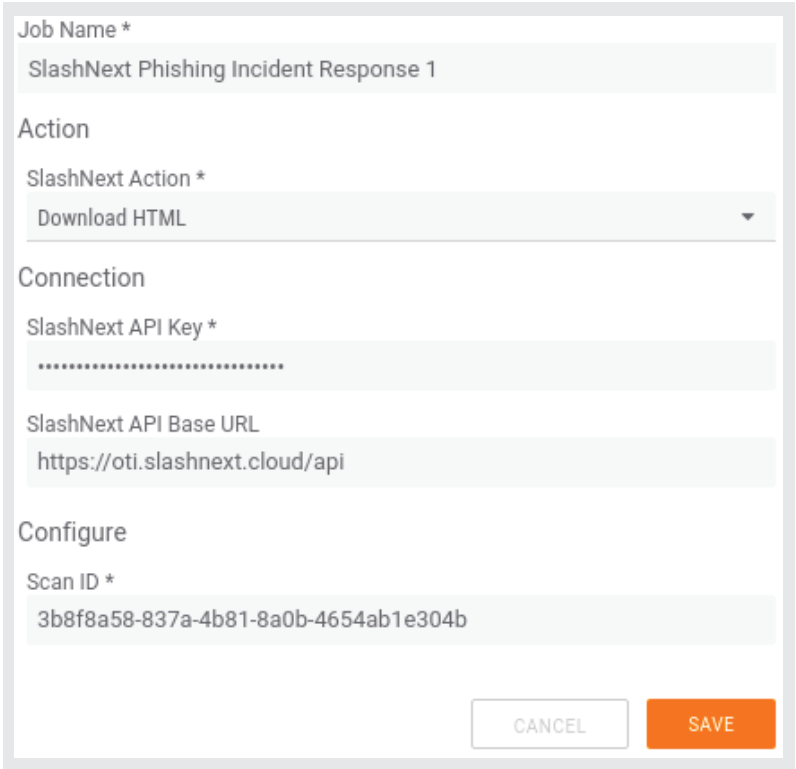
OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.download.screenshot.parameters.scanID	The Scan ID value input to the Download Screenshot action echoed back as an output	String
#snx.download.screenshot.scData.scBase64	Raw screenshot data (JPEG type) encoded in Base64 format	String
#snx.download.screenshot.rawJSON	Raw JSON response of Download Screenshot SlashNext API for debugging purposes	KeyValue
#snx.action.summary	Summary of Download Screenshot action execution	String
#snx.action.errorNo	Error Number returned by SlashNext Cloud in case of any error (0 for successful execution)	String
#snx.action.errorMsg	Error Message returned by SlashNext Cloud in case of any error ("Success" for successful execution)	String

3.8 | DOWNLOAD HTML

Downloads a web page HTML against a previous URL scan request.

3.8.1 | ACTION PARAMETERS

PARAMETER	REQUIRED	DESCRIPTION	THREAT CONNECT TYPE	CONTAINS
Scan ID	True	The Scan ID is a unique ID assigned by SlashNext Cloud to each scanning request#snx.url.scan.scannedURL and can be retrieved from the SlashNext "URL Scan" or the "URL Scan Sync" actions.	String	SlashNext Scan ID



3.8.2 | ACTION OUTPUTS

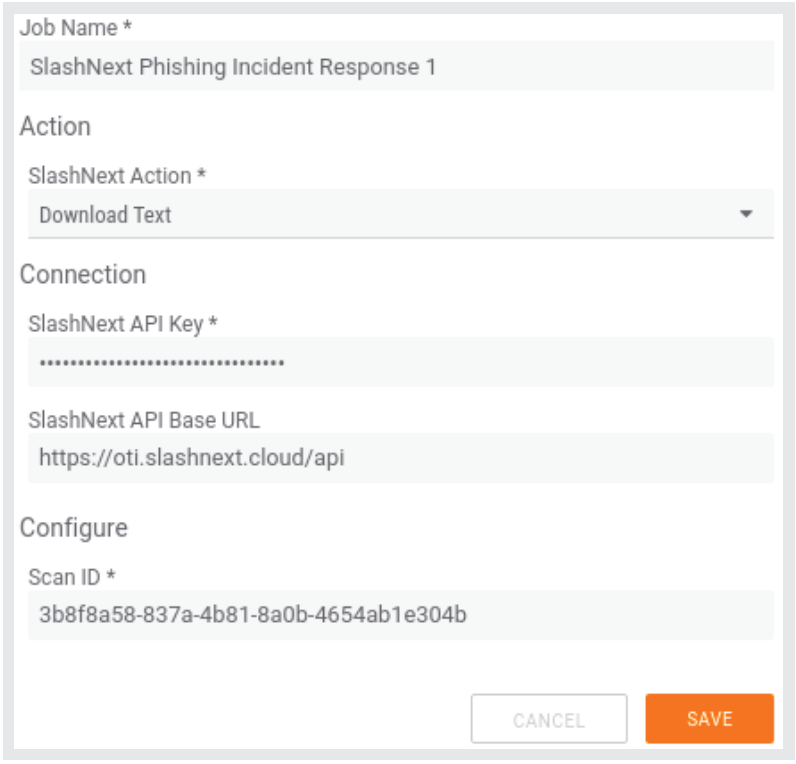
OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.download.html.parameters.scanID	The Scan ID value input to the Download HTML action echoed back as an output	String
#snx.download.html.htmlData.htmlBase64	Raw HTML data of the scanned URL in Base64 format	String
#snx.download.html.rawJSON	Raw JSON response of Download HTML SlashNext API for debugging purposes	KeyValue
#snx.action.summary	Summary of Download HTML action execution	String
#snx.action.errorNo	Error Number returned by SlashNext Cloud in case of any error (0 for successful execution)	String
#snx.action.errorMsg	Error Message returned by SlashNext Cloud in case of any error ("Success" for successful execution)	String

3.9 | DOWNLOAD TEXT

Downloads the text of a web page against a previous URL scan request.

3.9.1 | ACTION PARAMETERS

PARAMETER	REQUIRED	DESCRIPTION	THREAT CONNECT TYPE	CONTAINS
Scan ID	True	The Scan ID is a unique ID assigned by SlashNext Cloud to each scanning request and can be retrieved from the SlashNext "URL Scan" or the "URL Scan Sync" actions.	String	SlashNext Scan ID



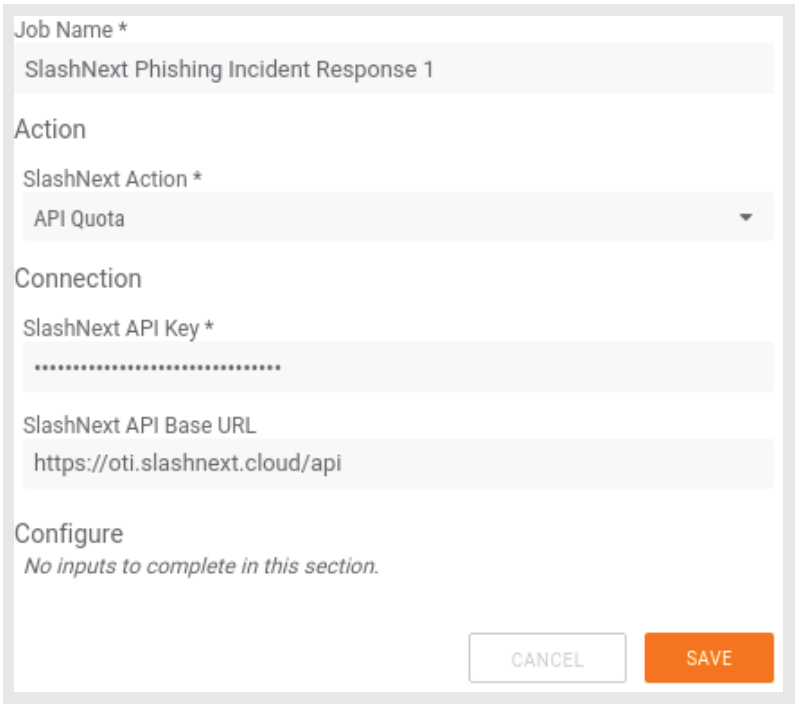
3.9.2 | ACTION OUTPUTS

OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.download.text.parameters.scanID	The Scan ID value input to the Download Text action echoed back as an output	String
#snx.download.text.textData.textBase64	Raw Text data of the scanned URL in Base64 format	String
#snx.download.text.rawJSON	Raw JSON response of Download Text SlashNext API for debugging purposes	KeyValue
#snx.action.summary	Summary of Download Text action execution	String
#snx.action.errorNo	Error Number returned by SlashNext Cloud in case of any error (0 for successful execution)	String
#snx.action.errorMsg	Error Message returned by SlashNext Cloud in case of any error ("Success" for successful execution)	String

3.10 | API QUOTA

3.10.1 | ACTION PARAMETERS

No Input parameters are required for this action



3.10.2 | ACTION OUTPUTS

OUTPUT	DESCRIPTION	THREATCONNECT TYPE
#snx.action.summary	Summary of API Quota action execution	String
#snx.action.errorNo	Error Number returned by SlashNext Cloud in case of any error (0 for successful execution)	String
#snx.action.errorMsg	Error Message returned by SlashNext Cloud in case of any error ("Success" for successful execution)	String