

SlashNext Phishing IR Integration Guide Swimlane SOAR

TABLE OF CONTENTS

1 INTRODUCTION	3
2 REQUIREMENTS	3
3 INSTALLATION	3
4 ACTIONS	8
SlashNext : Host Reputation	8
Inputs	8
Outputs	9
SlashNext : Host Report	10
Inputs	10
Outputs	11
SlashNext : Host URLs	12
Inputs	12
Outputs	12
SlashNext : URL Scan	13
Inputs	13
Outputs	14

TABLE OF CONTENTS

- SlashNext : URL Scan Sync 15
 - Inputs..... 15
 - Outputs..... 16
- SlashNext : Scan Report 17
 - Inputs..... 17
 - Outputs 18
- SlashNext : Download HTML 19
 - Inputs..... 19
 - Outputs..... 19
- SlashNext : Download Screenshot..... 20
 - Inputs..... 20
 - Outputs..... 20
- SlashNext : Download Text 21
 - Inputs..... 21
 - Outputs..... 21
- SlashNext : API Quota 22
 - Inputs..... 22
 - Outputs..... 23
- 5 | PLAYBOOKS** 24
 - Playbook - SlashNext Host Reputation 27
 - Outputs..... 27
 - Playbook - SlashNext URL Scan..... 28
 - Outputs..... 28

1 | INTRODUCTION

SlashNext Phishing Incident Response Integration for Swimlane SOAR platform is a bundle (swimbundle) which is a collection of Swimlane actions and assets that utilize SlashNext's On-demand Threat Intelligence (OTI) APIs to implement all the Phishing Incident Response (IR) actions.

2 | REQUIREMENTS

1. Swimlane Platform Version \geq **10.0.1**
2. Swimlane Server running
3. Swimlane Platform License
4. SlashNext Phishing Incident Response Plugin (swimbundle created using btb build server)
5. SlashNext On-demand Threat Intelligence (OTI) API Key provisioned by SlashNext to authenticate requests to SlashNext cloud

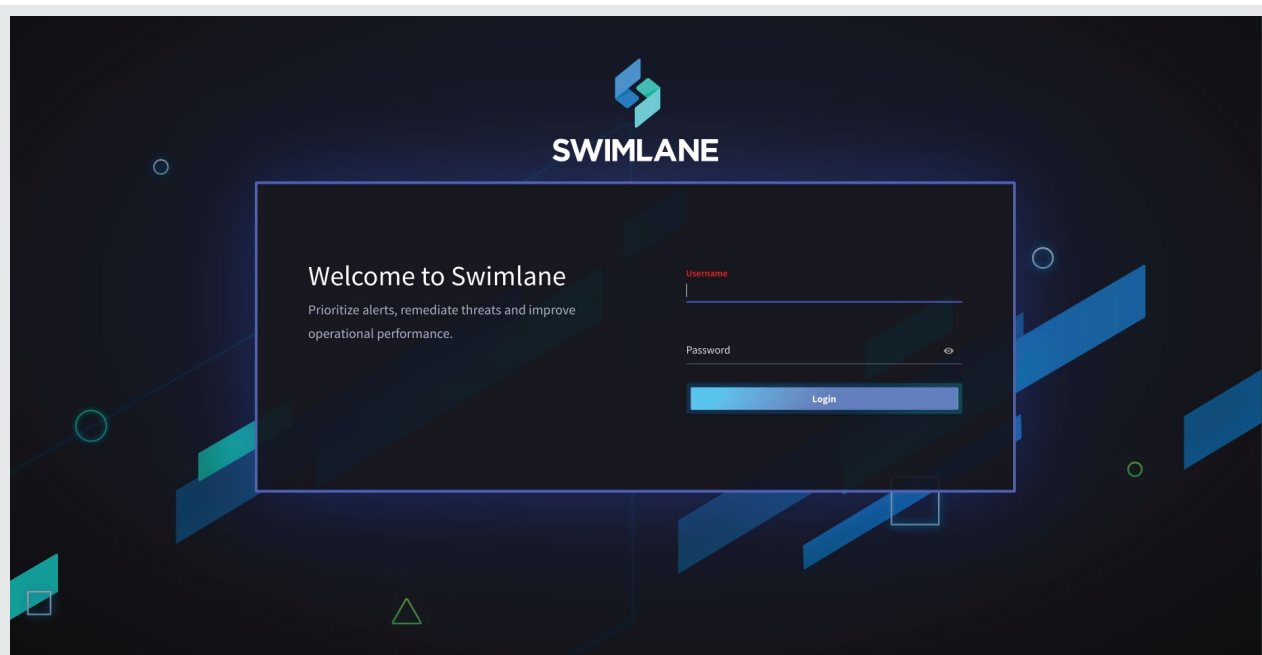
3 | INSTALLATION

To install SlashNext plugin into Swimlane platform, follow the steps below:

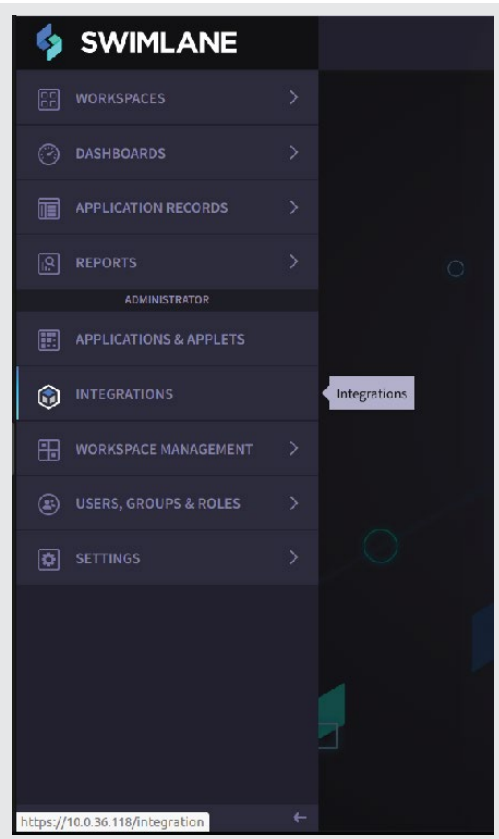
1. Log in to the Swimlane platform using the credentials created.

You can set up your Swimlane user profile by following the official docs at the following link:

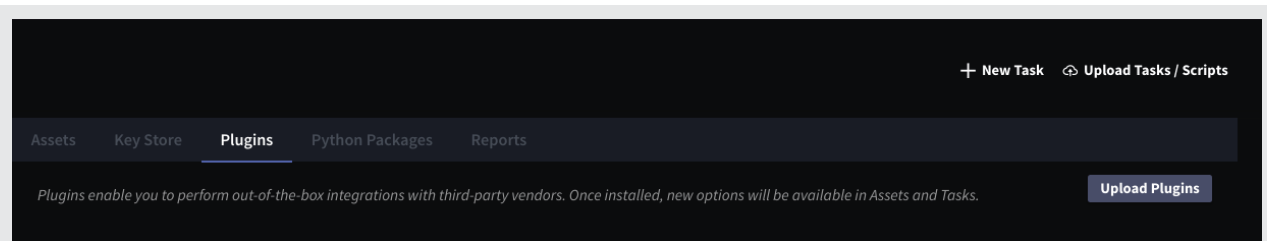
<https://swimlane.com/knowledge-center/docs/introduction/welcome-to-swimlane>



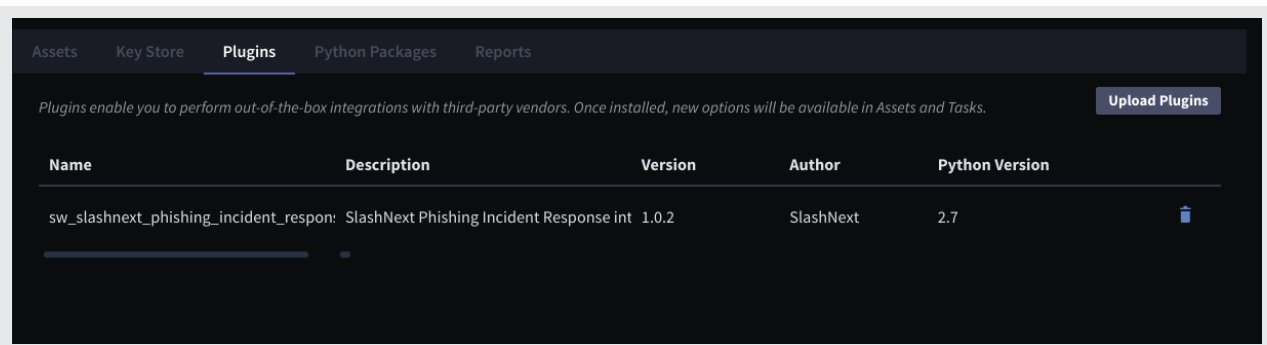
2. Once logged in and user profile is completed, go to the Integrations tab from the sidebar menu.



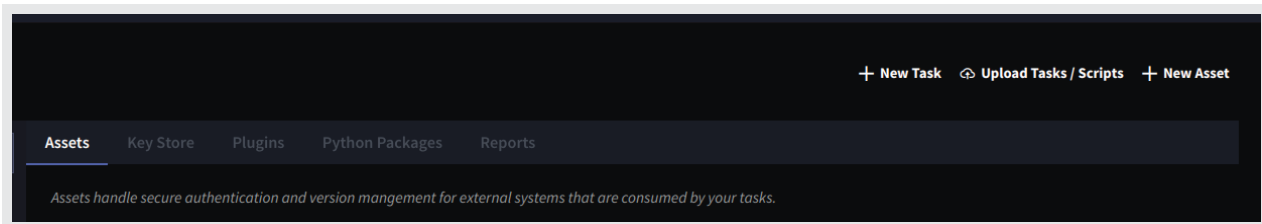
3. Then switch to the Plugins tab.



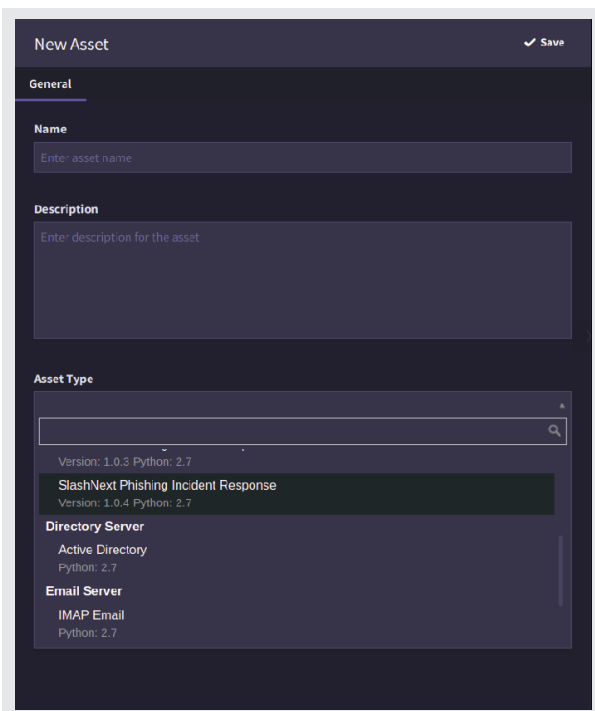
4. Click on Upload Plugins button and select the SlashNext plugin from the browse menu. Once successfully uploaded, the plugins tab would look something like this.



5. Next, go to the Assets tab and click on New Asset.

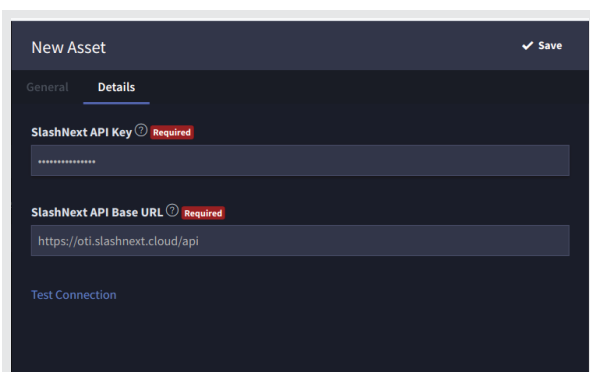


6. A new asset popup screen would open. From there, select the asset type **SlashNext Phishing Incident Response**.

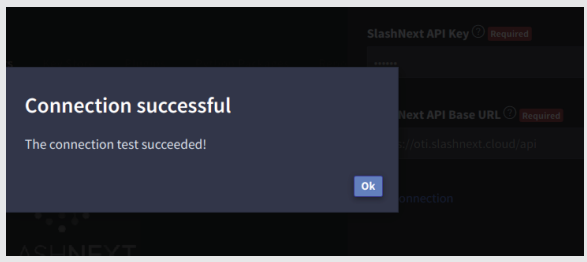


7. Next, click on the Details tab and enter the **SlashNext API Key** and **SlashNext API Base URL**.

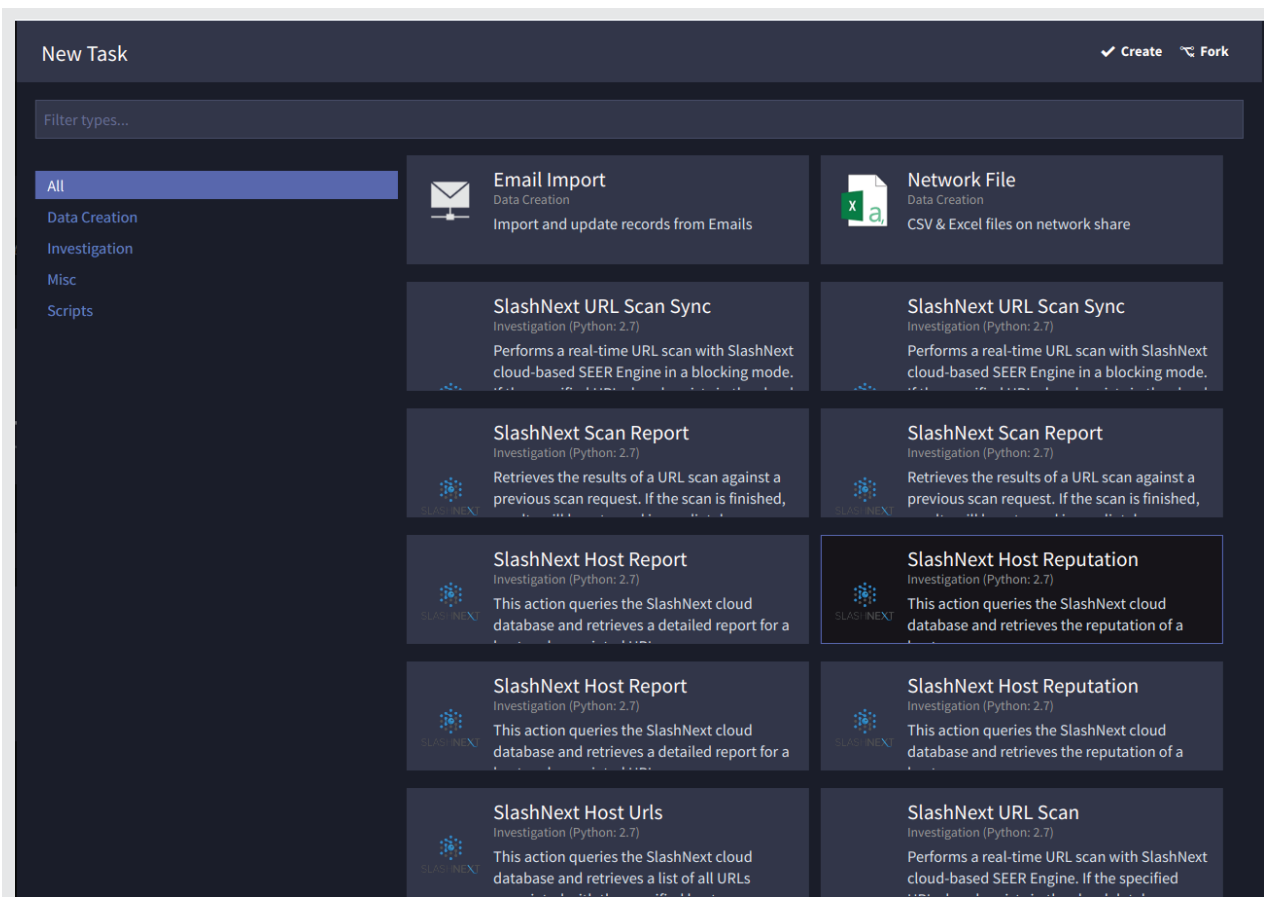
SlashNext API Base URL refers to the SlashNext endpoint URL. Do not changes its value from the default one until specified by SlashNext. Insert the SlashNext API key provided by SlashNext in the **SlashNext API Key** parameter.



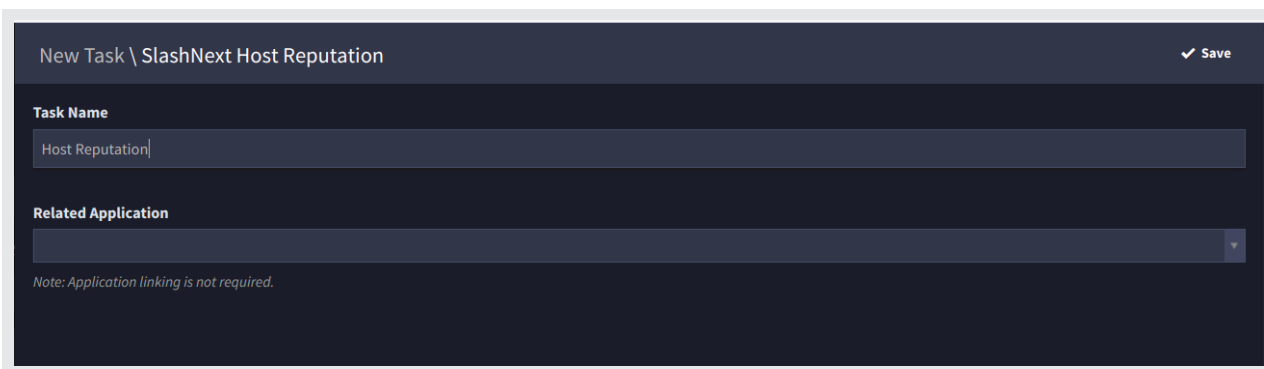
- Make sure that the entered values are correct. Then, click on Test Connection button. If you entered the values correctly, a success message will be shown. Otherwise, an error message will be shown.



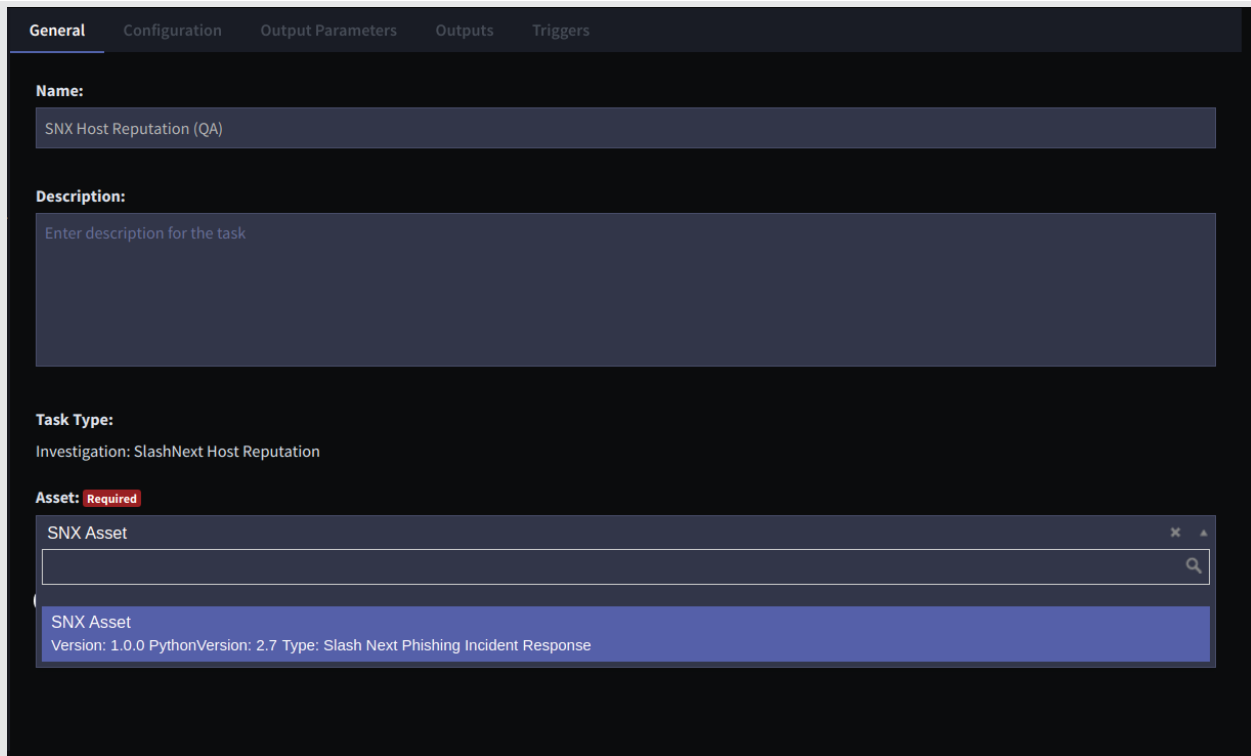
- Once the connection is successful, Click on the New Task button. Now you would see that the SlashNext actions are available. Click on any of the SlashNext Tasks from them and click on Create button at the top right.



- Select your related Swimlane application and click Save on the top right.



11. Then, from the General Tab, click on the Asset dropdown and select the SlashNext Asset that you created earlier.



The screenshot displays the configuration interface for a task in the SLASHNEXT system. The interface is divided into several sections:

- General Tab:** The active tab, showing the task name and description.
- Name:** A text input field containing "SNX Host Reputation (QA)".
- Description:** A large text area with the placeholder text "Enter description for the task".
- Task Type:** A dropdown menu currently set to "Investigation: SlashNext Host Reputation".
- Asset:** A dropdown menu with a red "Required" label. The dropdown is open, showing a search bar and a list of assets. The selected asset is "SNX Asset", with details: "Version: 1.0.0 PythonVersion: 2.7 Type: Slash Next Phishing Incident Response".

12. Save the task. Now you can add the Input Configurations, Outputs and Triggers based on your Application requirements.

4 | ACTIONS

SlashNext Integration Plugin for Swimlane contains the following actions as elaborated below:

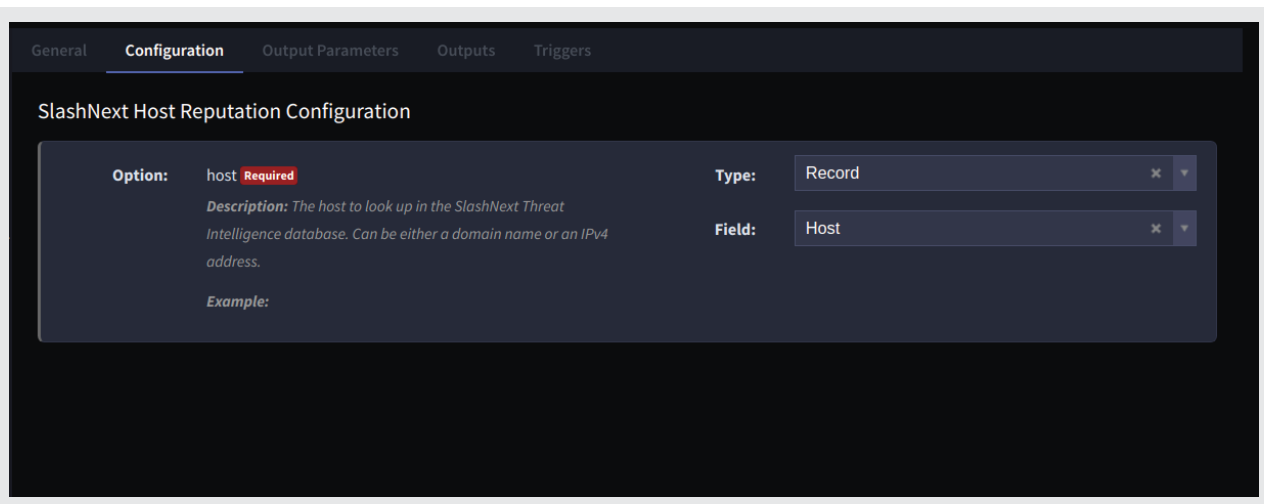
4.1 | SLASHNEXT : HOST REPUTATION

Host Reputation

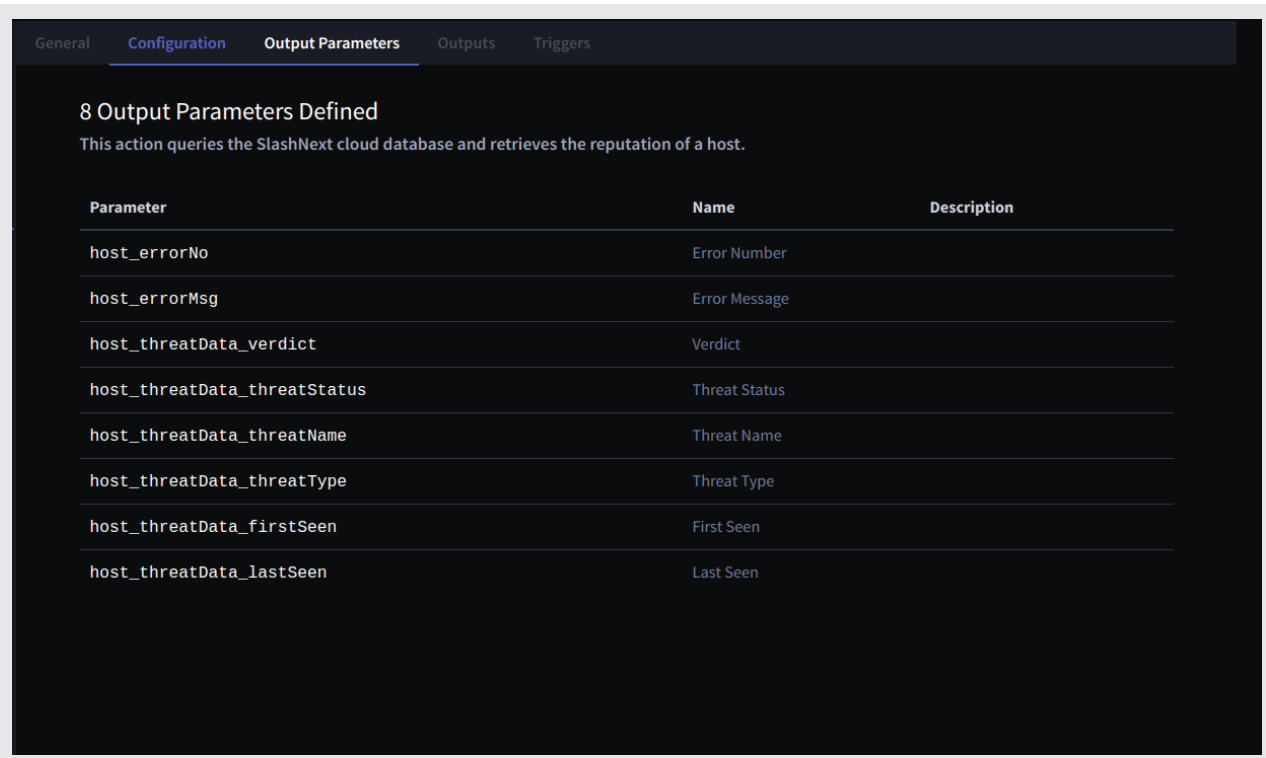
This action queries the SlashNext cloud database and retrieves the reputation of a host.

4.1.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
host	True	The host to look up in the SlashNext Threat Intelligence database. It can be either a domain name or an IPv4 address



4.1.2 | OUTPUT



General Configuration **Output Parameters** Outputs Triggers

8 Output Parameters Defined

This action queries the SlashNext cloud database and retrieves the reputation of a host.

Parameter	Name	Description
host_errorNo	Error Number	
host_errorMsg	Error Message	
host_threatData_verdict	Verdict	
host_threatData_threatStatus	Threat Status	
host_threatData_threatName	Threat Name	
host_threatData_threatType	Threat Type	
host_threatData_firstSeen	First Seen	
host_threatData_lastSeen	Last Seen	

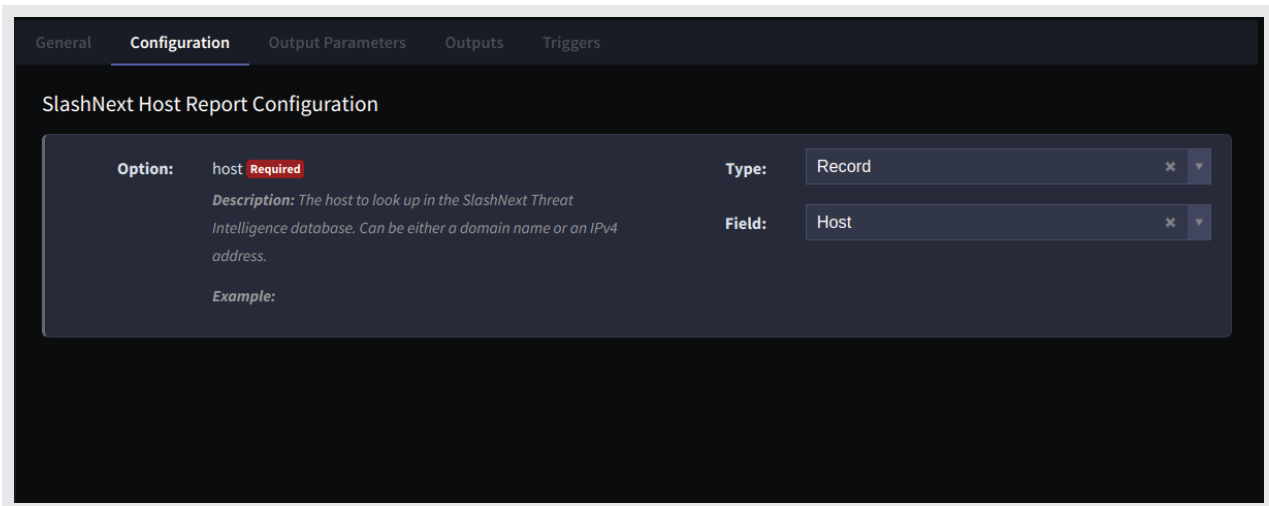
4.2 | SLASHNEXT : HOST REPORT

Host Report

This action queries the SlashNext cloud database and retrieves a detailed report for a host and associated URL.

4.2.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
host	True	The host to look up in the SlashNext Threat Intelligence database. It can be either a domain name or an IPv4 address



4.2.2 | OUTPUT

This function will report the threat information of the Host in the notes section. Additionally, it will show the threat information of the latest URL associated with that Host along with its webpage's forensics (Screenshot, HTML and Text), if available:

General Configuration **Output Parameters** Outputs Triggers

34 Output Parameters Defined
This action queries the SlashNext cloud database and retrieves a detailed report for a host and associated URL.

Parameter	Name	Description
host_errorNo	Host Error Number	
host_errorMsg	Host Error Message	
host_threatData_verdict	Host Verdict	
host_threatData_threatStatus	Host Threat Status	
host_threatData_threatName	Host Threat Name	
host_threatData_threatType	Host Threat Type	
host_threatData_firstSeen	Host First Seen	
host_threatData_lastSeen	Host Last Seen	
latestUri_errorNo	Latest URL Error Number	
latestUri_errorMsg	Latest URL Error Message	
latestUri_urIDataList_ur1	Latest URL Uri	
latestUri_urIDataList_scanId	Latest URL Scan ID	
latestUri_urIDataList_threatData_verdict	Latest URL Verdict	
latestUri_urIDataList_threatData_threatStatus	Latest URL Threat Status	
latestUri_urIDataList_threatData_threatName	Latest URL Threat Name	
latestUri_urIDataList_threatData_threatType	Latest URL Threat Type	
latestUri_urIDataList_threatData_firstSeen	Latest URL First Seen	
latestUri_urIDataList_threatData_lastSeen	Latest URL Last Seen	
latestUri_normalizeData_normalizeStatus	Latest URL Normalized Status	
latestUri_normalizeData_normalizeMessage	Latest URL Normalized Message	
screenshot_errorNo	Screenshot Error Number	
screenshot_errorMsg	Screenshot Error Message	
screenshot_scData_scName	Screenshot Name	
screenshot_scData_scContentType	Screenshot Content Type	
screenshot_scData_scBase64	Screenshot Base64	
html_errorNo	Html Error Number	
html_errorMsg	Html Error Message	
html_htmlData_htmlName	Html Name	
html_htmlData_htmlContentType	Html Content Type	
html_htmlData_htmlBase64	Html Base64	
text_errorNo	Text Error Number	
text_errorMsg	Text Error Message	
text_textData_textName	Text Name	
text_textData_textBase64	Text Base64	

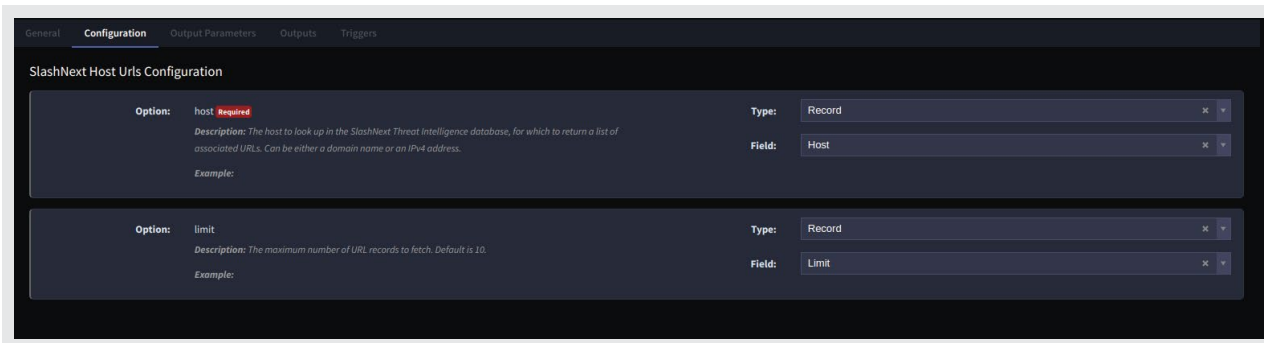
4.3 | SLASHNEXT : HOST URLS

Host URLs

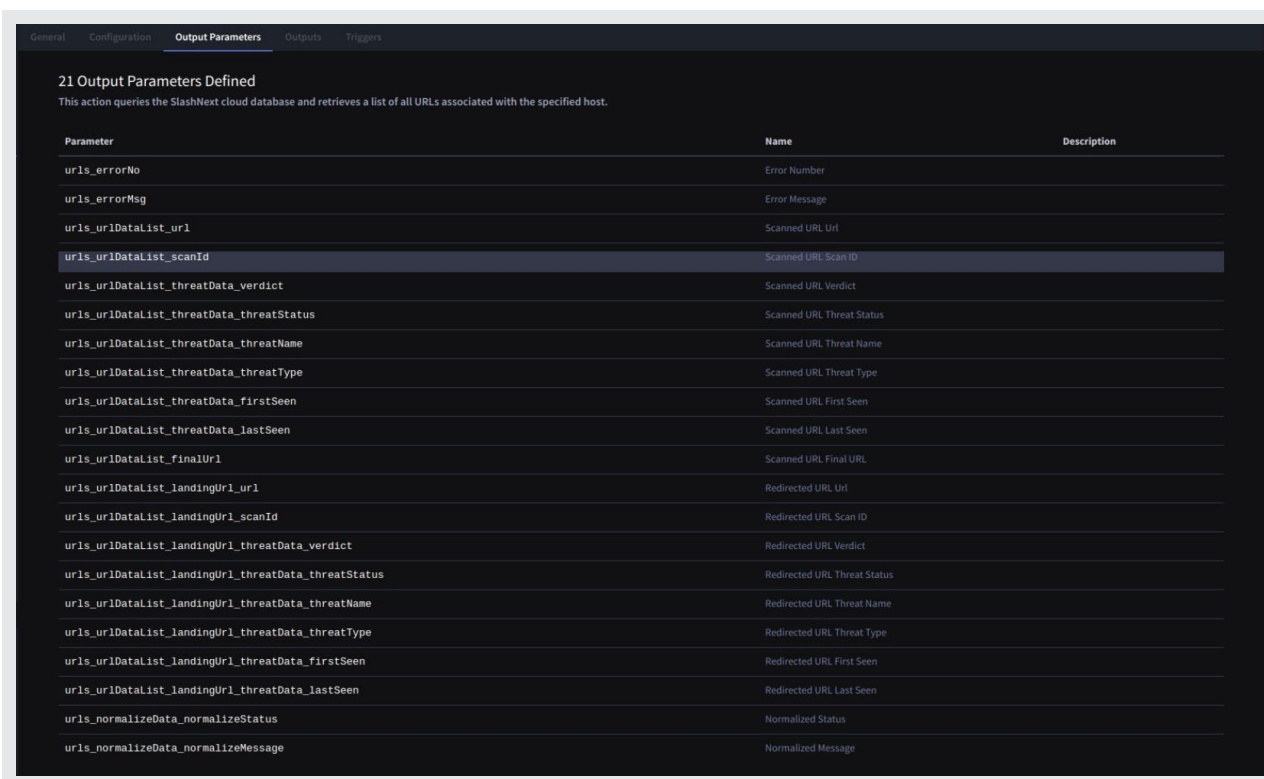
Search in SlashNext Cloud database and retrieve list of all URLs associated with the specified host.

4.3.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
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
limit	False	The maximum number of URL records to fetch. Default value is "10"



4.3.2 | OUTPUT



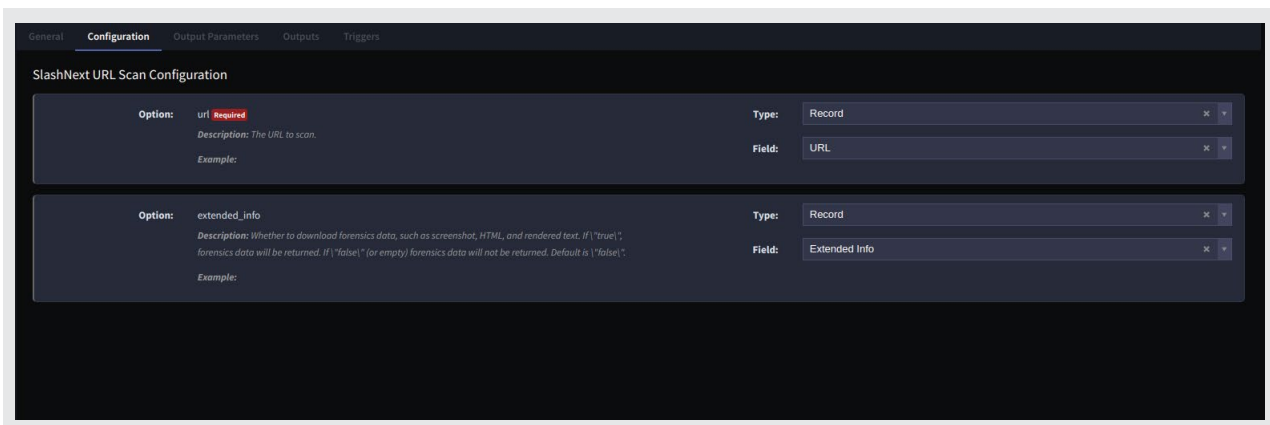
4.4 | SLASHNEXT : URL SCAN

URL Scan

Performs a real-time URL 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 action 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 "SlashNext Scan Report" anytime after 60 seconds using the returned Scan ID.

4.4.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
url	True	The URL that needs to be scanned.
extended_info	False	Whether to download forensics data, such as Screenshot, HTML, and rendered text. If "true", forensics data will be returned. If "false" (or empty) forensics data will not be returned.



4.4.2 | OUTPUT

34 Output Parameters Defined

Performs a real-time URL 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 action 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 "slashnext-scan-report" action anytime after 60 seconds using the returned Scan ID.

Parameter	Name	Description
url_errorNo	Error Number	
url_errorMsg	Error Message	
url_urldata_url	Scanned URL	
url_urldata_scanId	Scanned URL Scan ID	
url_urldata_threatData_verdict	Scanned URL Verdict	
url_urldata_threatData_threatStatus	Scanned URL Threat Status	
url_urldata_threatData_threatName	Scanned URL Threat Name	
url_urldata_threatData_threatType	Scanned URL Threat Type	
url_urldata_threatData_firstSeen	Scanned URL First Seen	
url_urldata_threatData_lastSeen	Scanned URL Last Seen	
url_urldata_landingUrl_url	Redirected URL Url	
url_urldata_landingUrl_scanId	Redirected URL Scan ID	
url_urldata_landingUrl_threatData_verdict	Redirected URL Verdict	
url_urldata_landingUrl_threatData_threatStatus	Redirected URL Threat Status	
url_urldata_landingUrl_threatData_threatType	Redirected URL Threat Type	
url_urldata_landingUrl_threatData_threatName	Redirected URL Threat Name	
url_urldata_landingUrl_threatData_firstSeen	Redirected URL First Seen	
url_urldata_landingUrl_threatData_lastSeen	Redirected URL Last Seen	
screenshot_errorNo	Screenshot Error Number	
screenshot_errorMsg	Screenshot Error Message	
screenshot_scData_scName	Screenshot Name	
screenshot_scData_scContentType	Screenshot Content Type	
screenshot_scData_scBase64	Screenshot Base64	
html_errorNo	Html Error Number	
html_errorMsg	Html Error Message	
html_htmlData_htmlName	Html Name	
html_htmlData_htmlContentType	Html Content Type	
html_htmlData_htmlBase64	Html Base64	
text_errorNo	Text Error Number	
text_errorMsg	Text Error Message	
text_textData_textName	Text Name	
text_textData_textBase64	Text Base64	
url_normalizeData_normalizeStatus	Normalized Status	
url_normalizeData_normalizeMessage	Normalized Message	

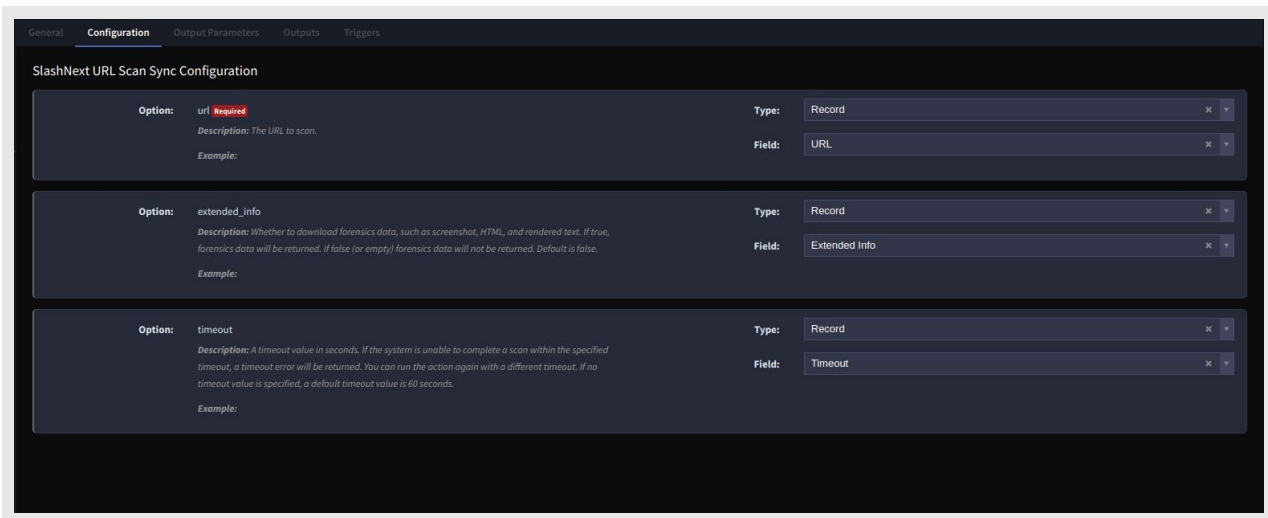
4.5 | SLASHNEXT : URL SCAN SYNC

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 action will submit a URL scan request and wait for the scan to finish. The scan may take up to 60 seconds to finish.

4.5.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
url	True	The URL that needs to be scanned.
extended_info	False	Whether to download forensics data, such as Screenshot, HTML, and rendered text. If "true", forensics data will be returned. If "false" (or empty) forensics data will not be returned.
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. The default timeout value is 60 seconds.



4.5.2 | OUTPUT

35 Output Parameters Defined

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 action will submit a URL scan request and wait for the scan to finish. The scan may take up to 60 seconds to finish.

Parameter	Name	Description
scan_sync_errorNo	Error Number	
scan_sync_errorMsg	Error Message	
scan_sync_urlData_url	Scanned URL	
scan_sync_urlData_scanId	Scanned URL Scan ID	
scan_sync_urlData_threatData_verdict	Scanned URL Verdict	
scan_sync_urlData_threatData_threatStatus	Scanned URL Threat Status	
scan_sync_urlData_threatData_threatName	Scanned URL Threat Name	
scan_sync_urlData_threatData_threatType	Scanned URL Threat Type	
scan_sync_urlData_threatData_firstSeen	Scanned URL First Seen	
scan_sync_urlData_threatData_lastSeen	Scanned URL Last Seen	
scan_sync_urlData_finalUrl	Final URL	
scan_sync_urlData_landingUrl_url	Redirected URL	
scan_sync_urlData_landingUrl_scanId	Redirected URL Scan ID	
scan_sync_urlData_landingUrl_threatData_verdict	Redirected URL Verdict	
scan_sync_urlData_landingUrl_threatData_threatStatus	Redirected URL Threat Status	
scan_sync_urlData_landingUrl_threatData_threatName	Redirected URL Threat Name	
scan_sync_urlData_landingUrl_threatData_threatType	Redirected URL Threat Type	
scan_sync_urlData_landingUrl_threatData_firstSeen	Redirected URL First Seen	
scan_sync_urlData_landingUrl_threatData_lastSeen	Redirected URL Last Seen	
screenshot_errorNo	Screenshot Error Number	
screenshot_errorMsg	Screenshot Error Message	
screenshot_scData_scName	Screenshot Name	
screenshot_scData_scContentType	Screenshot Content Type	
screenshot_scData_scBase64	Screenshot Base64	
html_errorNo	HTML Error Number	
html_errorMsg	HTML Error Message	
html_htmlData_htmlName	HTML Name	
html_htmlData_htmlContentType	HTML Content Type	
html_htmlData_htmlBase64	HTML Base64	
text_errorNo	Text Error Number	
text_errorMsg	Text Error Message	
text_textData_textName	Text Name	
text_textData_textBase64	Text Base64	
scan_sync_normalizeData_normalizeStatus	Normalized Status	
scan_sync_normalizeData_normalizeMessage	Normalized Message	

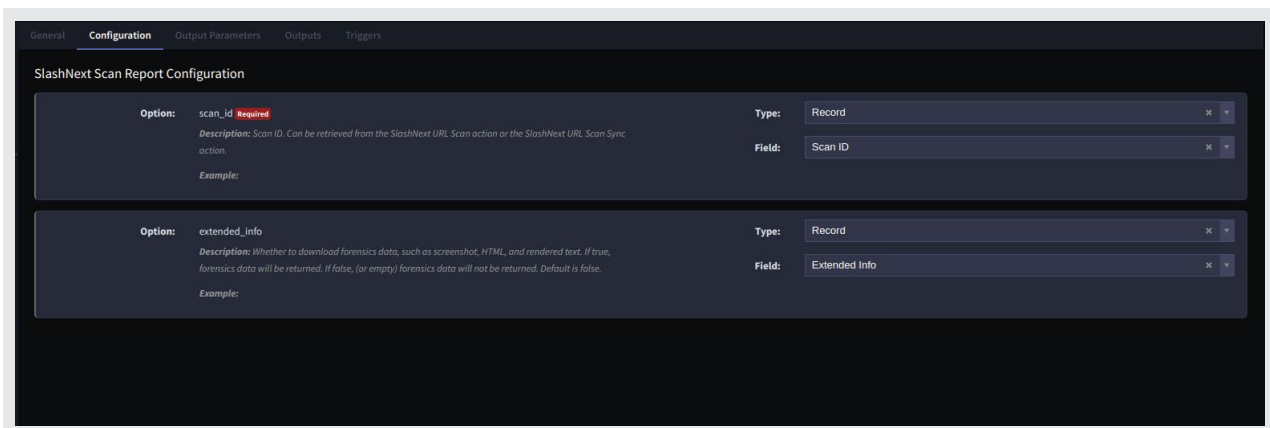
4.6 | SLASHNEXT : SCAN REPORT

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

4.6.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
scanid	True	Scan ID of the scan for which to get the report. It can be retrieved from the "URL Scan" function or "URL Scan Sync" function.
extended_info	False	Whether to download forensics data, such as Screenshot, HTML, and rendered text. If "true", forensics data will be returned. If "false" (or empty) forensics data will not be returned.



4.6.2 | OUTPUT

35 Output Parameters Defined

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 to check back later will be returned.

Parameter	Name	Description
scan_report_errorNo	Error Number	
scan_report_errorMsg	Error Message	
scan_report_urlData_url	Scanned URL	
scan_report_urlData_scanId	Scanned URL Scan ID	
scan_report_urlData_threatData_verdict	Scanned URL Verdict	
scan_report_urlData_threatData_threatStatus	Scanned URL Threat Status	
scan_report_urlData_threatData_threatName	Scanned URL Threat Name	
scan_report_urlData_threatData_threatType	Scanned URL Threat Type	
scan_report_urlData_threatData_firstSeen	Scanned URL First Seen	
scan_report_urlData_threatData_lastSeen	Scanned URL Last Seen	
scan_report_urlData_landingUrl_url	Redirected URL	
scan_report_urlData_landingUrl_scanId	Redirected URL Scan ID	
scan_report_urlData_landingUrl_threatData_verdict	Redirected URL Verdict	
scan_report_urlData_landingUrl_threatData_threatStatus	Redirected URL Threat Status	
scan_report_urlData_landingUrl_threatData_threatType	Redirected URL Threat Type	
scan_report_urlData_landingUrl_threatData_threatName	Redirected URL Threat Name	
scan_report_urlData_landingUrl_threatData_firstSeen	Redirected URL First Seen	
scan_report_urlData_landingUrl_threatData_lastSeen	Redirected URL Last Seen	
scan_report_urlData_finalUrl	Final URL	
scan_report_normalizeData_normalizeStatus	Normalized Status	
scan_report_normalizeData_normalizeMessage	Normalized Message	
screenshot_errorNo	Screenshot Error Number	
screenshot_errorMsg	Screenshot Error Message	
screenshot_scData_scName	Screenshot Name	
screenshot_scData_scContentType	Screenshot Content Type	
screenshot_scData_scBase64	Screenshot Base64	
html_errorNo	HTML Error Number	
html_errorMsg	HTML Error Message	
html_htmlData_htmlName	HTML Name	
html_htmlData_htmlContentType	HTML Content Type	
html_htmlData_htmlBase64	HTML Base64	
text_errorNo	Text Error Number	
text_errorMsg	Text Error Message	
text_textData_textName	Text Name	
text_textData_textBase64	Text Base64	

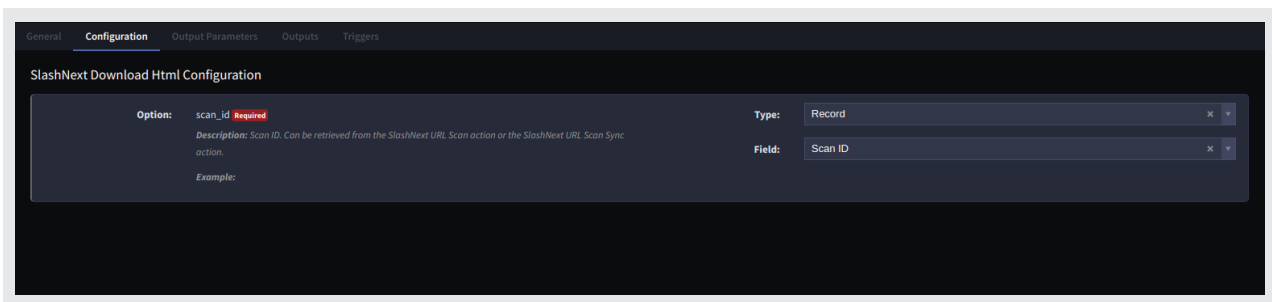
4.7 | SLASHNEXT : DOWNLOAD HTML

Download HTML

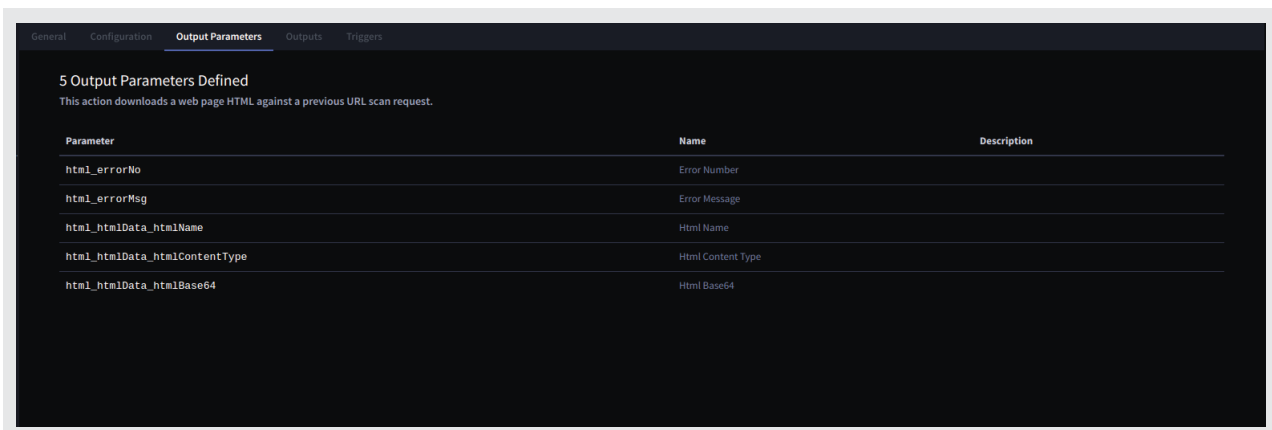
This action downloads a web page HTML against a previous URL scan request.

4.7.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
scanid	True	The Scan ID is a unique ID assigned by SlashNext Cloud to each scanning request and can be retrieved using the "URL Scan" or the "URL Scan Sync" functions.



4.7.2 | OUTPUT



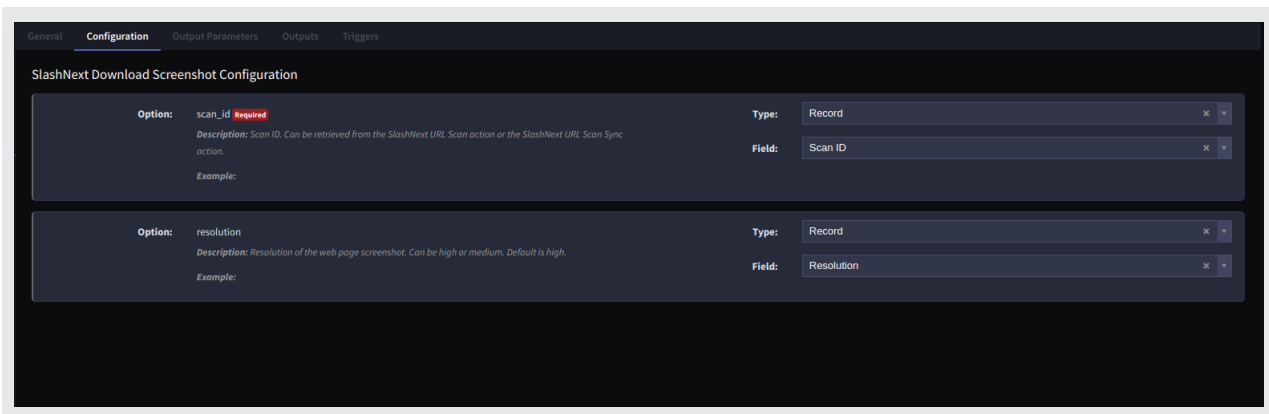
4.8 | SLASHNEXT : DOWNLOAD SCREENSHOT

Download Screenshot

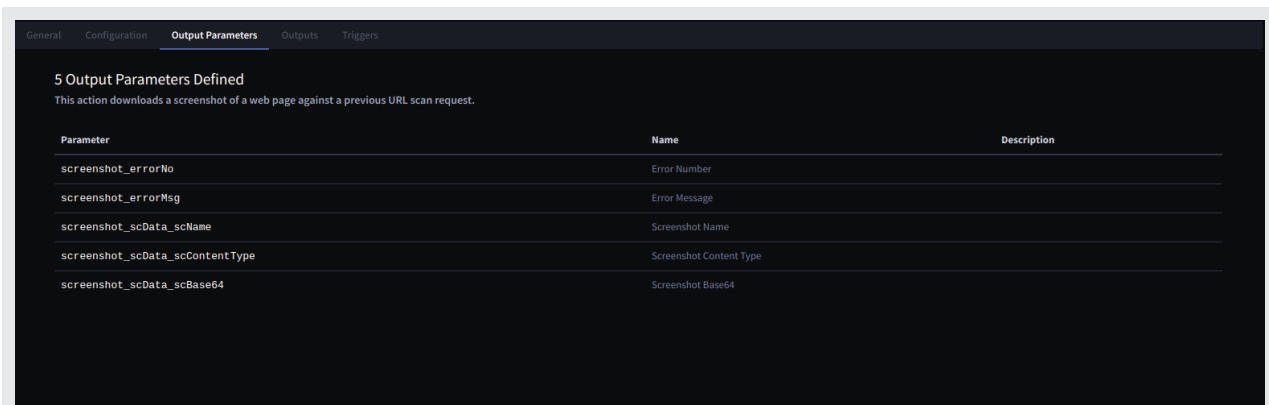
This action downloads a screenshot of a web page against a previous URL scan request.

4.8.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
scanid	True	The Scan ID is a unique ID assigned by SlashNext Cloud to each scanning request and can be retrieved using the "URL Scan" or the "URL Scan Sync" functions.
resolution	False	Resolution of the web page screenshot. Default value is "high".



5.8.2 | OUTPUT



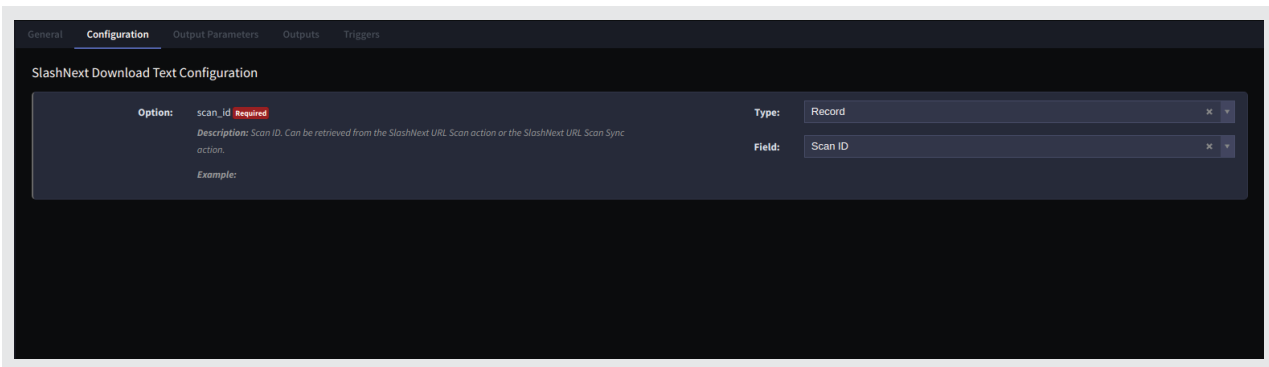
4.9 | SLASHNEXT : DOWNLOAD TEXT

Download Text

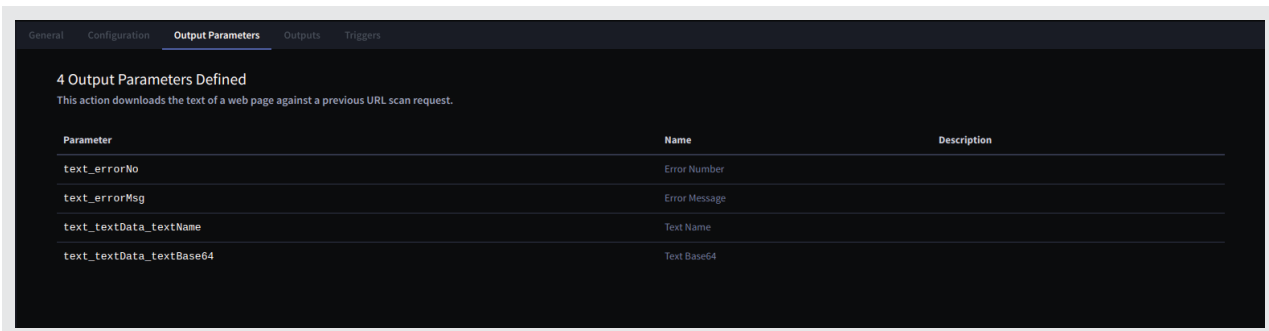
This action downloads the text of a web page against a previous URL scan request.

4.9.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
scanid	True	The Scan ID is a unique ID assigned by SlashNext Cloud to each scanning request and can be retrieved using the "URL Scan" or the "URL Scan Sync" functions.



4.9.2 | OUTPUT



4.10 | SLASHNEXT : API QUOTA

API Quota

This action queries the SlashNext cloud database and retrieves the details of API quota.

4.10.1 | INPUT

This action has no inputs. Instead, it uses the API Key defined in the asset to get the API quota details.

4.10.2 | OUTPUT

40 Output Parameters Defined

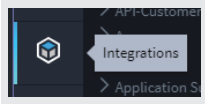
This action queries the SlashNext cloud database and retrieves the details of API quota.

Parameter	Name	Description
api_quota_errorNo	Error Number	
api_quota_errMsg	Error Message	
api_quota_quotaDetails_remainingQuota	Remaining Quota	
api_quota_quotaDetails_licensedQuota	Licensed Quota	
api_quota_quotaDetails_expiryDate	Expiry Date	
api_quota_quotaDetails_isExpired	Is Expired	
api_quota_quotaDetails_pointsConsumptionRate_hostReputation	Points ConsumptionRate Host Reputation	
api_quota_quotaDetails_pointsConsumptionRate_hostUrls	Points ConsumptionRate Host URLs	
api_quota_quotaDetails_pointsConsumptionRate_urlReputation	Points ConsumptionRate URL Reputation	
api_quota_quotaDetails_pointsConsumptionRate_urlScan	Points ConsumptionRate Url Scan	
api_quota_quotaDetails_pointsConsumptionRate_urlScanSync	Points ConsumptionRate Url Scan Sync	
api_quota_quotaDetails_pointsConsumptionRate_downloadScreenshot	Points ConsumptionRate Download Screenshot	
api_quota_quotaDetails_pointsConsumptionRate_downloadText	Points ConsumptionRate Download Text	
api_quota_quotaDetails_pointsConsumptionRate_downloadHTML	Points ConsumptionRate Download HTML	
api_quota_quotaDetails_pointsConsumptionRate_customerApiQuota	Points ConsumptionRate Customer Api Quota	
api_quota_quotaDetails_pointsConsumptionRate_urlScanWithScanId	Points ConsumptionRate Url Scan With Scan ID	
api_quota_quotaDetails_pointsConsumptionRate_urlScanSyncWithScanId	Points ConsumptionRate Url Scan Sync With Scan ID	
api_quota_quotaDetails_consumedAPIDetail_hostReputation	Consumed Api Post Reputation	
api_quota_quotaDetails_consumedAPIDetail_hostUrls	Consumed Api Post URLs	
api_quota_quotaDetails_consumedAPIDetail_urlReputation	Consumed Api Url Reputation	
api_quota_quotaDetails_consumedAPIDetail_urlScan	Consumed Api Url Scan	
api_quota_quotaDetails_consumedAPIDetail_urlScanSync	Consumed Api Url Scan Sync	
api_quota_quotaDetails_consumedAPIDetail_downloadScreenshot	Consumed Api Download Screenshot	
api_quota_quotaDetails_consumedAPIDetail_downloadText	Consumed Api Download Text	
api_quota_quotaDetails_consumedAPIDetail_downloadHTML	Consumed Api Download HTML	
api_quota_quotaDetails_consumedAPIDetail_customerApiQuota	Consumed Api Customer Api Quota	
api_quota_quotaDetails_consumedAPIDetail_scanReportWithScanId	Consumed Api Scan Report With Scan ID	
api_quota_quotaDetails_consumedAPIDetail_scanSyncReportWithScanId	Consumed Api Scan Sync Report With Scan ID	
api_quota_quotaDetails_consumedPointsDetail_hostReputation	Consumed Points Host Reputation	
api_quota_quotaDetails_consumedPointsDetail_hostUrls	Consumed Points Host URLs	
api_quota_quotaDetails_consumedPointsDetail_urlReputation	Consumed Points Url Reputation	
api_quota_quotaDetails_consumedPointsDetail_urlScan	Consumed Points Url Scan	
api_quota_quotaDetails_consumedPointsDetail_urlScanSync	Consumed Points Url Scan Sync	
api_quota_quotaDetails_consumedPointsDetail_downloadScreenshot	Consumed Points Download Screenshot	
api_quota_quotaDetails_consumedPointsDetail_downloadText	Consumed Points Download Text	
api_quota_quotaDetails_consumedPointsDetail_downloadHTML	Consumed Points Download HTML	
api_quota_quotaDetails_consumedPointsDetail_customerApiQuota	Consumed Points Customer Api Quota	
api_quota_quotaDetails_consumedPointsDetail_scanReportWithScanId	Consumed Points Scan Report With Scan ID	
api_quota_quotaDetails_consumedPointsDetail_scanSyncReportWithScanId	Consumed Points Scan Sync Report With Scan ID	
api_quota_quotaDetails_note	Quota Details Note	

5 | PLAYBOOKS

SlashNext Phishing Incident Response also provides two playbooks that defines the business logic to automate URL and Host scanning for an incoming email in Abuse Inbox.

- First, set up and IMAP Email Asset as described in the official [Swimlane documentation](#).
 1. Log in to Swimlane with your Chrome browser. From the global navigation menu, select Integrations.

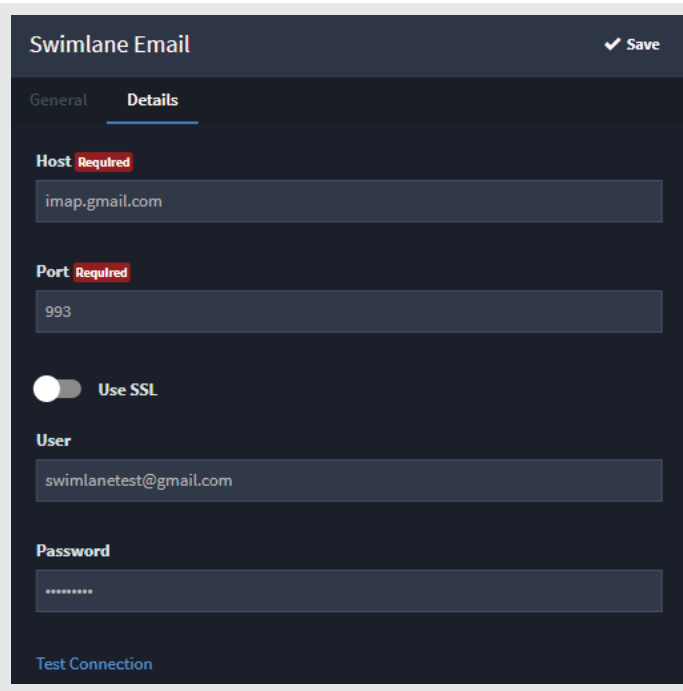


Important! Contact your Swimlane support or sales representative if you do not have log in credentials for Swimlane.

2. Select the **Assets** tab and then, from the Integrations taskbar, select **+ New Asset**.
3. On the New Asset, **General** tab, provide a name and description (optional) for your asset, and then select IMAP Email from the **Asset Type** pull-down field.

A screenshot of the 'Swimlane Email' asset configuration form in a dark theme. The form has a 'Save' button in the top right corner. It is divided into three sections: 'General', 'Description', and 'Asset Type'. The 'Name' field contains 'Swimlane Email'. The 'Description' field is empty with a placeholder 'Enter description for the asset'. The 'Asset Type' section shows a search bar and a list of options: 'McAfee Data Exchange Layer Asset' (Version: 1.0.0), 'Directory Server' (Active Directory), 'Email Server' (IMAP Email, POP3 Email, SMTP Email). The 'IMAP Email' option is selected and highlighted.

- Click the **Details** tab and fill out the required **Host** and **Port** fields. In addition, complete the **User** and **Password** fields and ensure that the **Use SSL** field is enabled.



Swimlane Email ✓ Save

General **Details**

Host Required
imap.gmail.com

Port Required
993

Use SSL

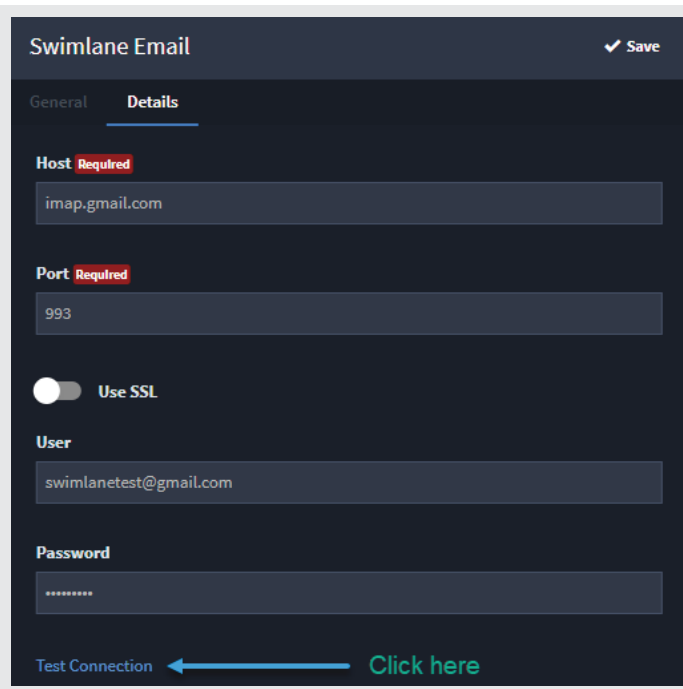
User
swimlanetest@gmail.com

Password

Test Connection

Note: The User and Password you use here need to be real assets that you have access to!

- Next, click **Test Connection**.



Swimlane Email ✓ Save

General **Details**

Host Required
imap.gmail.com

Port Required
993

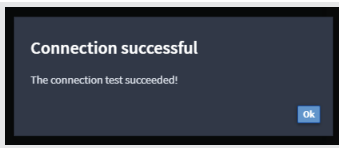
Use SSL

User
swimlanetest@gmail.com

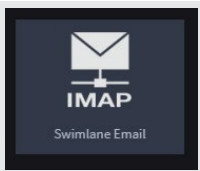
Password

Test Connection ← Click here

6. Once you receive a message that the connection test has succeeded, click **Ok**, and then click **Save** to save your new asset.



You can now see your asset listed under the Assets tab.



- After creating an Email Asset, go on to create a related Email task which uses the Asset created in the first step by following the official Swimlane documentation [here](#).

The details for both playbooks are mentioned below:

5.1 | PLAYBOOK - SLASHNEXT HOST REPUTATION

This section demonstrates the complete business logic to scan Hosts (IPv4/Domain) from an incoming email in Swimlane platform via SlashNext Phishing Incident Response playbook application.

A new Swimlane record is created for each of the host present in the email body.

5.1.1 | OUTPUT

SE-1155
Delete

HOST REPORT SECTION

<p>Scanned Host: estelasplantrental.com</p> <p>Host Verdict: Malicious</p> <p>Host Threat Status: No Longer Active</p> <p>Host Threat Type: Phishing & Social Engineering</p> <p>Host Last Seen: 03-20-2020 22:14:52 UTC</p> <p>Latest URL: http://estelasplantrental.com/amexx/login</p> <p>Latest URL Scan ID: 1d5e0b40-0cbe-40d2-9cc4-9ad973e9b67f</p> <p>Latest URL Threat Status: No Longer Active</p> <p>Latest URL Threat Type: Phishing & Social Engineering</p> <p>Latest URL Last Seen: 03-19-2020 23:51:24 UTC</p> <p>Latest URL Normalized Message:</p> <p>Host Screenshot: Name 658195936CAC622B201F10C62462060F1FD5D9B1759E158294B00B3044595C5F</p> <p>Host Html File: Name A34F3CC26CD9F644981749272DDA95649F52FBC389AC321223F371AE88495517</p> <p>Host Text File: Name 16A5DE2FD7212587DDFD804F4E90DE50B15E81BC3069A4B46D16F7F439975C72</p>	<p>Host Threat Name: Fake Login Page</p> <p>Host First Seen: 03-10-2020 12:38:56 UTC</p> <p>Latest URL Verdict: Malicious</p> <p>Latest URL Threat Name: Fake Login Page</p> <p>Latest URL First Seen: 03-16-2020 12:38:45 UTC</p> <p>Latest URL Normalized Status: 0</p>
--	---

5.2 | PLAYBOOK - SLASHNEXT URL SCAN

This section demonstrates the complete business logic to scan URLs from an incoming email in Swimlane platform via Slash-Next Phishing Incident Response playbook application.

A new Swimlane record is created for each of the URLs found in the email body.

5.2.1 | OUTPUT

