Cisco Secure Network Analytics

Using the External Lookup Feature 7.4

Table of Contents

Managing External Lookup

The External Lookup feature allows you to launch a Web application (or internal asset database) to view additional information about an IP address. You can launch this Web application or database directly from the Desktop Client or the Web App.

You can also use the External Lookup feature to create shortcuts that enable you to jump quickly from the Desktop Client to the Web App.

Cisco Secure Network Analytics (formerly Stealthwatch) includes the following default Web applications (lookup options) for use with the External Lookup feature; you do not have to add them to your system:

- DShield.org
- Host Report
- OpenDNS Investigate
- Talos Reputation

Some examples of Web applications that the Admin (the default administrative user that is built into Secure Network Analytics and whose user name is *admin*) can add to view additional information about an IP address include the following:

- BigFix
- CiscoWorks
- Cisco Identity Services Engine (ISE)
- Splunk
- Tripwire
- Ziften

To add a non-default lookup option, you must use the External Lookup Configuration tool in the Web App. For more information about how to do this, refer to **Configuring External Lookup**.

Configuring External Lookup

Why you use this page

Use this page to do the following:

- View the lookup options you have added.
- Add, edit, delete, enable, or disable a lookup option.
- Configure the specific parameters that you want to send to a Web application. The parameters you configure are only sent if they are available for the IP address on which you are performing the lookup.

How to find this page

1. From the main menu, click the (**Global Settings**) icon .
2. Click **External Lookup Configuration**.

What you can do on this page

- DShield.org, Host Report, OpenDNS Investigate, and Talos Reputation and are included by default for use with the External Lookup feature; you do not have to add them to Secure Network Analytics. To use any other Web application with this feature, you must add it to Secure Network Analytics.

View lookup options

Do the following as they apply:

- View the list of Web applications (lookup options) to determine if this list contains the lookup options you need and that they are enabled for use with the External Lookup feature.
- To disable a lookup option so that it is not available for use with the External Lookup feature (but to retain its configuration for later use), click **Enabled** in the applicable row. The button toggles to show the status of *Disabled*. To enable this vendor in the future, click **Disabled**. The button toggles to show the status of *Enabled*.
- To edit or delete a lookup option, in the Actions column, click the (**Ellipsis**) icon to open the context menu, and then select the appropriate option.

Add lookup options and configure parameters

Click **Add External Lookup** in the upper right corner of the External Lookup section. Refer to the following for information about configuring parameters:

- To view information about internal IP addresses in a Web application, ensure you select the "Enable lookup of internal IP addresses" check box.
- The parameters you configure appear in a Web application only if they are available for the IP address on which you are performing the lookup.
- You can map up to 20 query parameters for each lookup option.
- If you want a parameter to be required when performing a lookup using a specific Web application, select the Required check box. Every parameter you designate to be required for a specific Web application must be available for the IP address on which you are performing a lookup. If one or more of the required parameters are not available for the relevant IP address, this lookup option will not be enabled in the pop-up menu.
- The URL script builder file contains the script that configures the query parameters into the URL format that the Web application requires in order to run a query.

> You can upload scripts that do not exceed 100 KB.

- If you do not upload a script builder file, Secure Network Analytics will use the default standard query parameters shown below.

  BaseURL?[ParameterName1]=[ParameterValue1]&[ParameterName2]=[ParameterValue2]&[ParameterName3]=[ParameterValue3] (and so on for each attribute you add)

- If your query parameters do not match the standard query parameters shown previously, then you must upload your customized script builder configuration. Below are some script examples to refer to when configuring a customized script builder file.

URL and script examples

Example 1

The following URL and script examples are used for Web applications that use values without parameter names (e.g., Splunk).

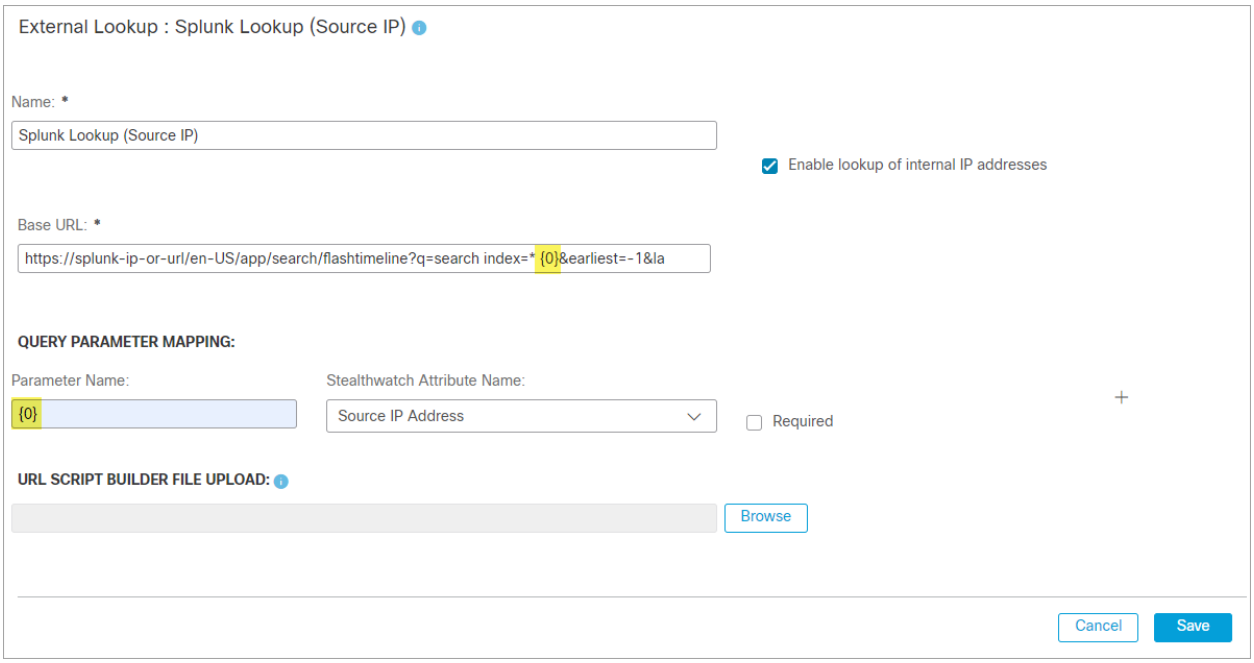
```
https://splunk-ip-or-url/en-US/app/search/flashtimeline
?q=search index=* {0}&earliest=-1d&latest=now
```

```
import java.util.ArrayList;
import java.util.List;
import java.text.*;

def List<String> values = new ArrayList<String>();

vendorValues.each { valueOperand ->
    values.add(valueOperand.getFromValue().toString());
};

MessageFormat messageFormat = new MessageFormat(baseUrl);
return messageFormat.format(values.toArray());
```

Click the following link to download a .txt file of the script shown in the previous image.

Splunk script

To build the script that configures the query parameters into the URL format shown previously in this example, use the Parameter Name field entry highlighted in the image below.



You can configure as many attributes as you need; however, ensure that you configure the same number of parameters.

Example 2

The following URL and script examples are used for Web applications that use rest-like parameters (e.g., Secure Network Analytics Host Report).

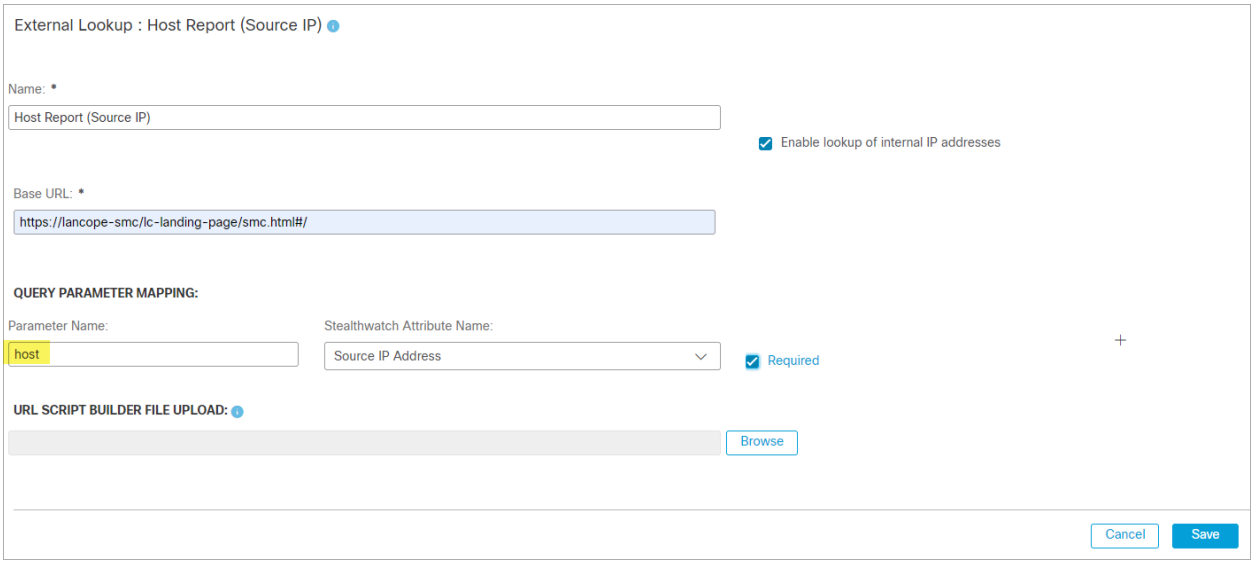
`https://lancope-smc/lc-landing-page/smc.html#/host/172.21.114.17`

```
def String query = "";

vendorValues.each { valueOperand ->


    query += valueOperand.getName() + "/";
    def String convertedStr = "";
    if (valueOperand.getFromValue() instanceof String || valueOperand.getFromValue() instanceof Integer) {
        convertedStr = valueOperand.getFromValue().toString();
    } else if (valueOperand.getFromValue() instanceof Date) {
        convertedStr = new SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss").format(valueOperand.getFromValue().time);
    }
    query += URLEncoder.encode(convertedStr,"UTF-8");
};

def char lastChar = baseUrl.charAt(baseUrl.length() - 1);
if (lastChar != '?' && lastChar != '/' && lastChar != '&') {
    baseUrl = baseUrl + "?";
};

query = baseUrl + query;
return query;
```

Click the following link to download a .txt file of the script shown in the previous image.

Secure Network Analytics Host Report script

To build the script that configures the query parameters into the URL format shown previously in this example, use the Parameter Name field entry highlighted in the image below.



What you can do next

To launch a vendor's Web application or internal asset database to view additional information about an IP address, perform an external lookup. For information about how to do this, see **Performing an External Lookup**.

Performing an External Lookup

Why you use this feature

Use this feature to query a Web application to view additional information about an IP address.

How to use this feature

1. Open any page in either the Web App or the Desktop Client that contains the relevant IP address. Do one of the following:
    - In the Web App, do one of the following to access the menu located on most pages throughout the Web App:
        - Click the (**Ellipsis**) icon beside the applicable IP address.
        - Click the **Ellipsis** icon in the Actions column of a data table or configuration table.
        - Click a point in a graph. (In the Traffic by Peer Host Group graph on the Host Report page and the Top Host Groups by Traffic graph on the Host Group Report page, you must click a host group, a column, or the line between two host groups.)
    - In the Desktop Client, right-click the relevant IP address (there are a few locations where you cannot access the External Lookup option from an IP address).
2. In the pop-up menu that appears, click **External Lookup**. A secondary pop-up menu appears.
3. Click the desired lookup option from the secondary pop-up menu that appears in step 3. The Web application for the lookup option you selected opens (you may be prompted to log in to the Web application) and displays the query results for the IP address on which you are performing the lookup.

    Every parameter you designate to be required for a specific Web application must be available for the IP address on which you are performing a lookup. If one or more of the required parameters are not available for the relevant IP address, that lookup option will not be enabled in the pop-up menu. For more information, see **Configuring External Lookup**.

What you can do next

Depending on the information that is returned by the vendor, you might want to do one or more of the following:

- Add this IP address to a specific host group for monitoring or isolation.
- Flag the IP for additional research by an analyst or investigator.
- Launch a mitigation action against the IP address. (You must configure Secure Network Analytics so that it can do this.)

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Copyright Information