CISCO WSA Secure Network Analytics User Guide

Cisco Secure Network Analytics

Proxy Log Configuration Guide 7.5.3

Contents [hide]

Introduction

To collect user information from your network proxy servers for the Cisco Secure Network Analytics (formerly Stealthwatch) Proxy Log, you need to configure the proxy server logs. The Flow Collector receives the logs, and the Manager(formerly Stealthwatch Management Console) displays the information on the Flow Proxy Records page. This page provides URLs and application names of the traffic inside a network going through the proxy server.

Requirements

Before you start, confirm that you have met the following requirements:

- Cisco WSA (14-5-1-016), Blue Coat, McAfee, and Squid are supported for this configuration. Make sure your proxy server is configured and running as part of your network.
- Confirm that the Flow Collector and the proxy use the same NTP server (or receive time from a common source for flow and proxy records to be matched).
- Select the Flow Collector that collects data from the exporters and endpoints that you want to investigate in the proxy logs. You need the IP address for the configuration.
- There is no specific size limit on syslog proxy messages. However, we recommend that messages be kept shorter than the shortest Maximum Transmission Unit (MTU) along the path between the proxy and Flow Collector, usually 1500. This eliminates packet fragmentation and increases reliability.
- Proxy Log is not supported in High Availability (HA) mode.

Configuration Overview

Complete the following procedures:

1. Choose one of the following methods to configure your proxy server.
    - Configuring the Cisco Web Security Appliance (WSA) Proxy Logs
    - Configuring the Blue Coat Proxy Logs
    - Configuring the McAfee Proxy Logs
    - Configuring Squid Proxy Logs
2. Configuring the Flow Collector
3. Checking the Flows

Configuring the Cisco Web Security Appliance (WSA) Proxy Logs

Use this section to configure Cisco proxy logs to send to Secure Network Analytics.

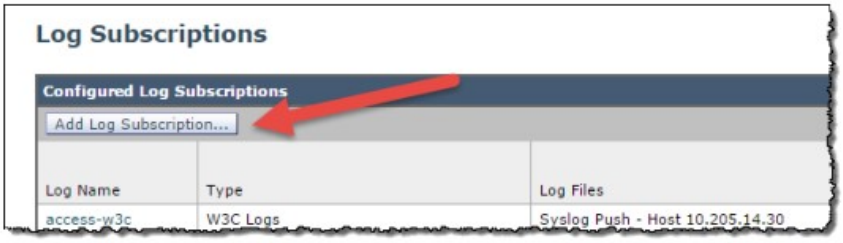
Cisco WSA proxy does not support Virtual IPs for adding the proxy device.

To set up the Cisco proxy log, complete the following steps:

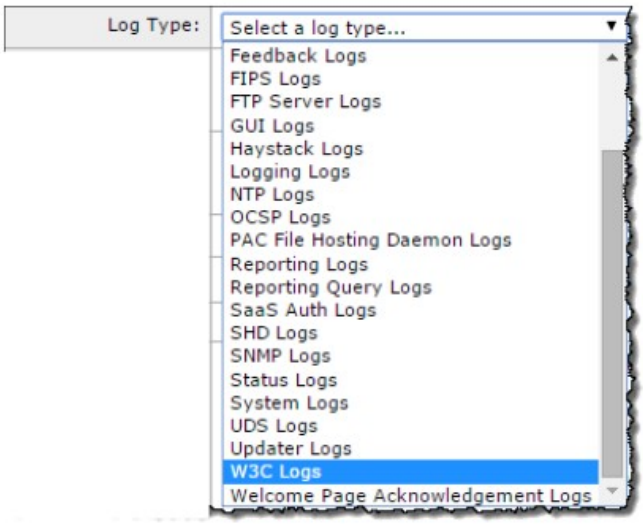
1. Log in to the Cisco proxy server.

2. On the main menu, click System Administration > Log Subscriptions. The Log Subscriptions page opens.

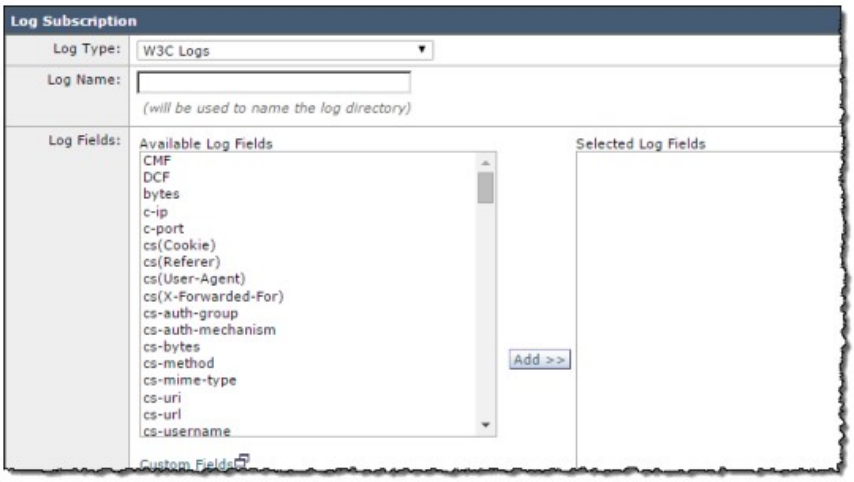
3. Click the Add Log Subscriptions button. The New Log Subscriptions page opens.



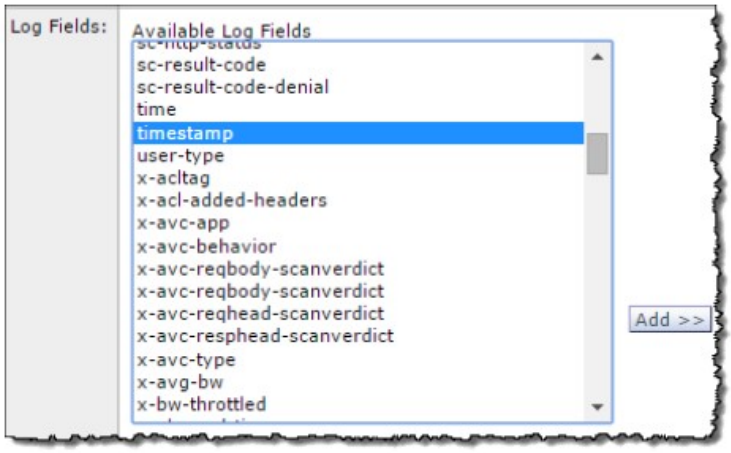
4. From the Log Type drop-down list, select W3C Logs. The available W3C Log fields appear.



5. In the Log Name field, type a name for the log that you will use.



6. From the Available Log Fields list, select Timestamp, and then click Add to move it the Select Log Fields list.



7. Repeat the previous step for the each of the following log fields in order:

a. timestamp

b. x-elapsed-time

c. c-ip

d. c-port

e. cs-bytes

f. s-ip

g. s-port

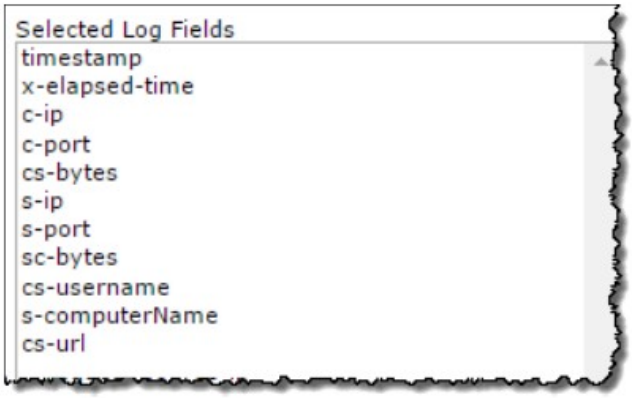
h. sc-bytes

i. cs-usernames

j. s-computerName

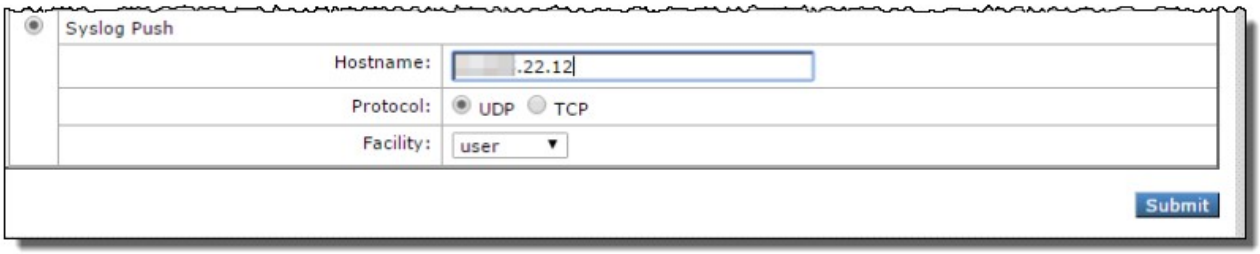
k. cs-url

The Selected Log Fields list should contain these fields as illustrated:



⚠ The Selected Log Fields list must be in the order above, with no other fields present.

8. Scroll to the bottom of the page, and then select the Syslog Push option.



9. In the Hostname field, type the Flow Collector IP address or its host name that the proxy sends logs to.

ℹ Make sure to select the Flow Collector that collects data from the exporters and end points that you want to investigate in the proxy logs.

10. Click Submit. The new log is added to the Log Subscription list.

11. Continue to the Configuring the Flow Collector section to set up your Flow Collector to receive syslog information.

Configuring the Blue Coat Proxy Logs

Use this section to configure Blue Coat proxy logs to send to Secure Network Analytics.

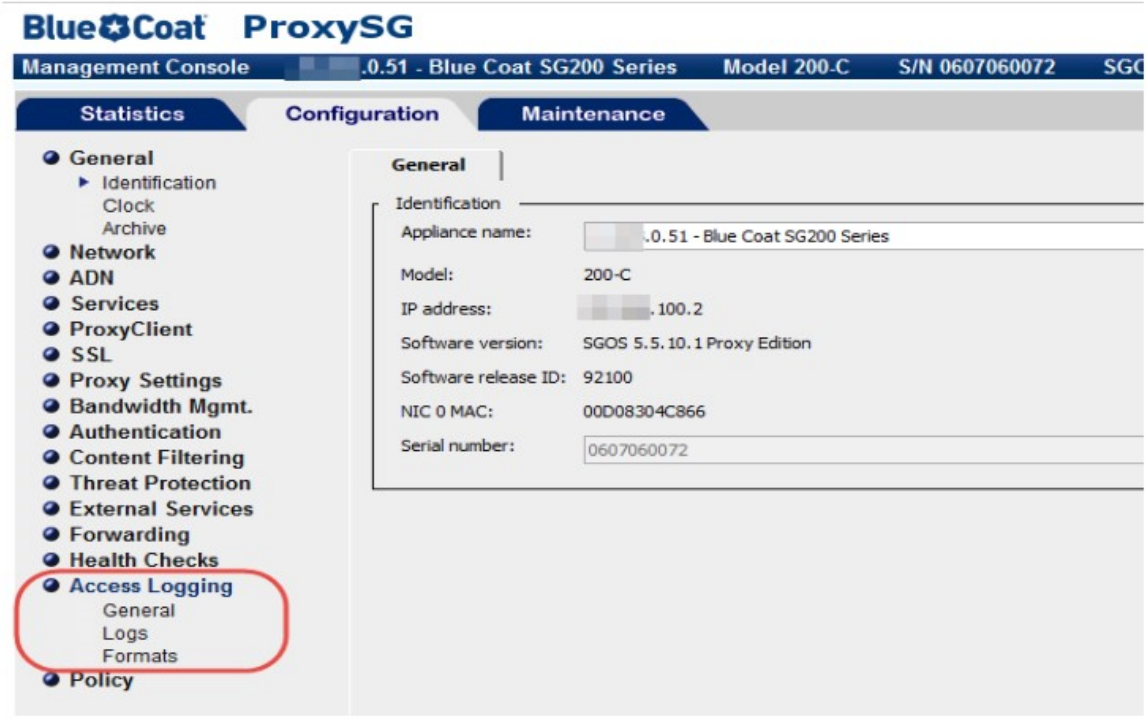
The Blue Coat proxy version used for testing was SG V100, SGOS 6.5.5.7 SWG Edition.

Creating the Format

To create a new log format, complete the following steps:

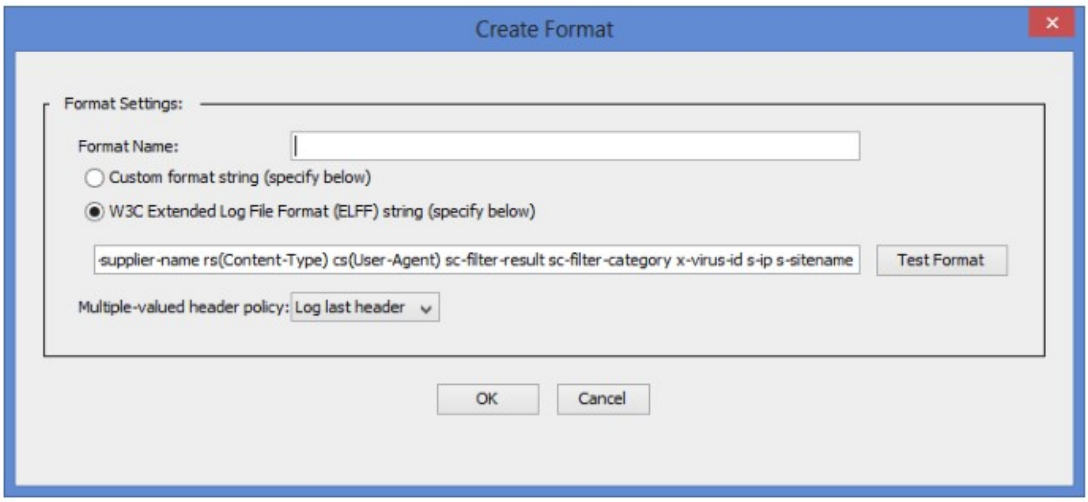
1. In your browser, access your Blue Coat proxy server.

2. Click the Configuration tab.



3. In the main menu of the Management Console, click Access Logging > Formats.

4. Click New at the bottom of the page. The Create Format page opens.



5. In the Format Name field, type a name for the new format.

6. Select the W3C Extended Log File Format (ELFF) option.

7. In the format field, type the following string:

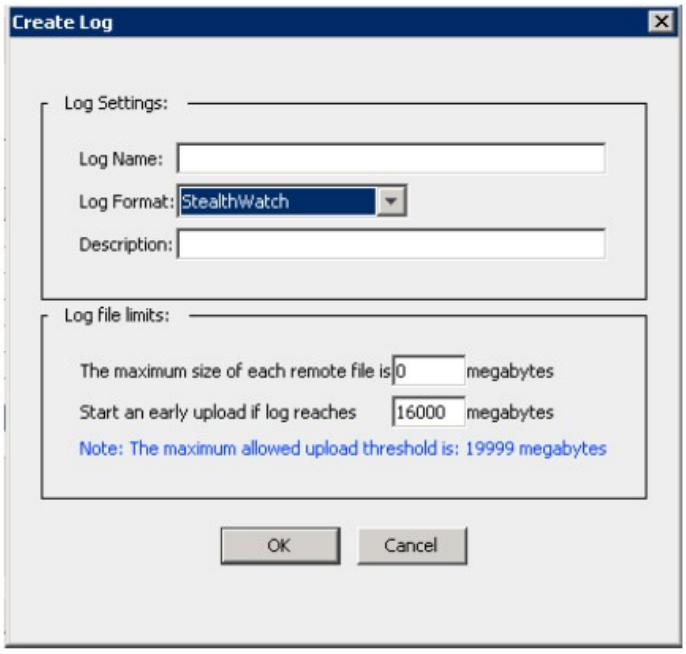
```
timestamp duration c-ip c-port r-ip r-port s-ip s-port cs-bytes sc-bytes
```

8. Click OK. Continue to the next section, Create a New Log

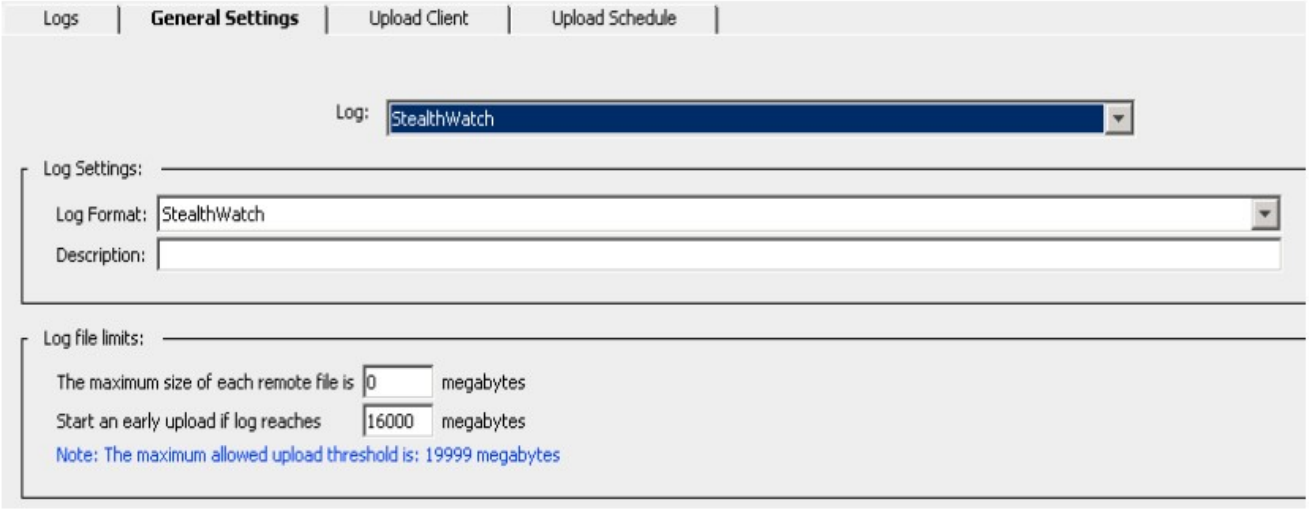
Create a New Log

To create the logs, complete the following steps:

1. In the main menu, click Access Logging > Logs, and then select the new log format. The Log page opens.



2. Click the General Settings tab.



3. From the Log Format drop-down list, select the log you created in Step 1.

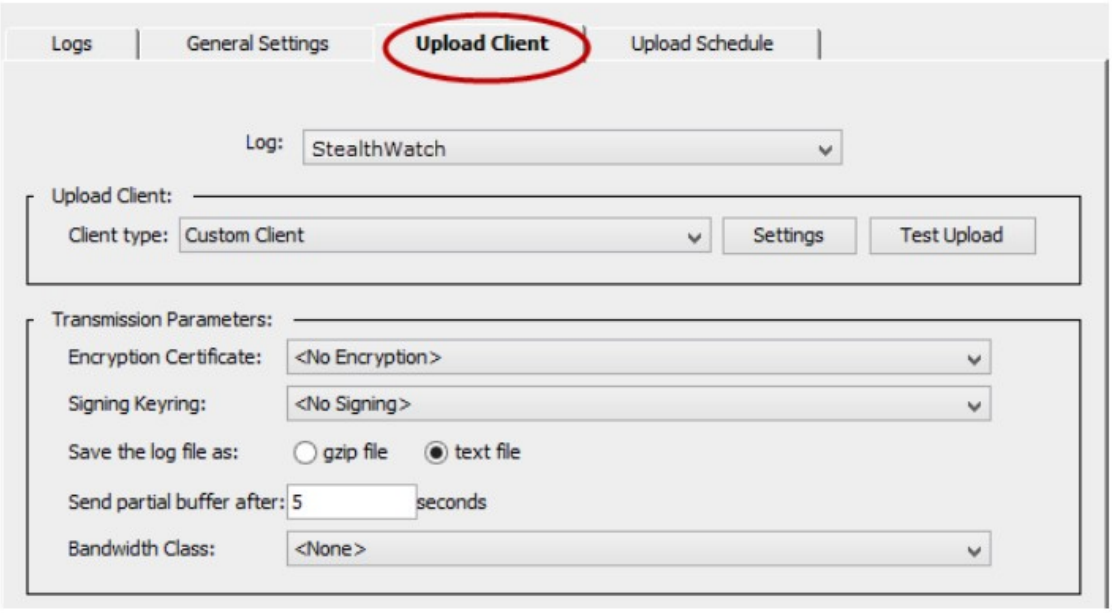
4. In the Description field, type a description for your new log.

5. Click the Apply button at the bottom of the page. Continue to the next section, Configure the Upload Client

Configure the Upload Client

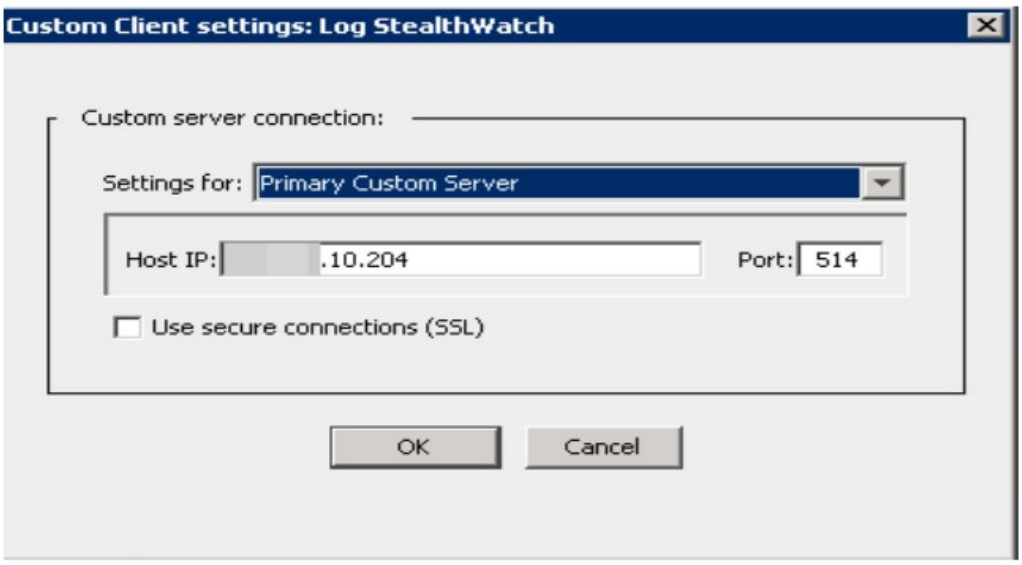
To configure the upload client, complete the following steps:

1. Click the Upload Client tab. The Upload Client page opens.



2. From the Client type drop-down list, select Custom Client.

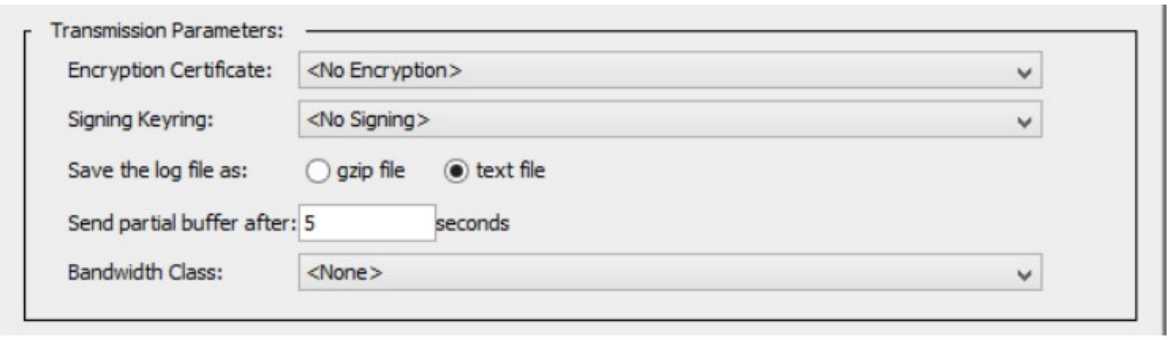
3. Click the Settings button. The Custom Client settings page opens.



4. In the appropriate fields, type the IP address of the Flow Collector and listening port of the proxy parser.

SSL is not supported at this time.

5. Click OK.



6. For the Transmission Parameters, complete these steps:

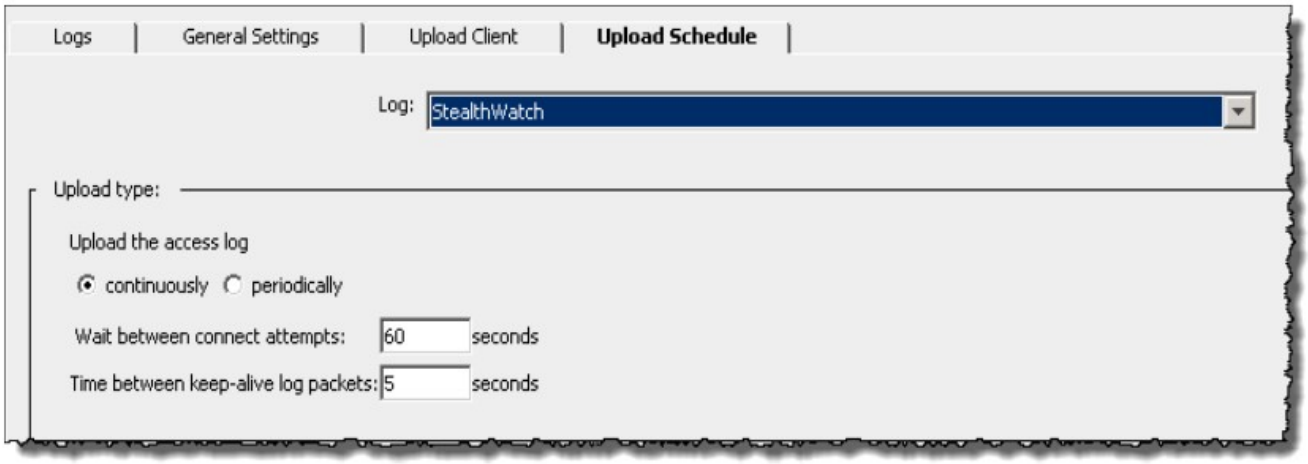
- a. For the Encryption Certificate, select No encryption.
- b. From the Signing Keyring drop-down list, select no signing.
- c. From “Save the log file as” select the Text file option.
- d. In the “Send partial buffer after” text box, type 5.
- e. Click the Upload Schedule tab, and select the continuously option for the Upload the access log.
- f. In the Wait between connect attempts field, type 60.
- g. In the Time between keep-alive log packets field, type 5.

7. Click the Apply button at the bottom of the page. Continue to the next section, Configuring the Upload Schedule.

Configuring the Upload Schedule

To configure the upload schedule, complete the following steps:

1. Click the Upload Schedule tab.



2. For the “Upload the access log,” select continuously.

3. Wait between correct attempts is 60 seconds.

4. Time between keep-alive log packet 5 seconds.

5. Click the Apply button at the bottom of the page.

This completes the configuration for the Blue Coat proxy logs for the Flow Collector.

Requirements

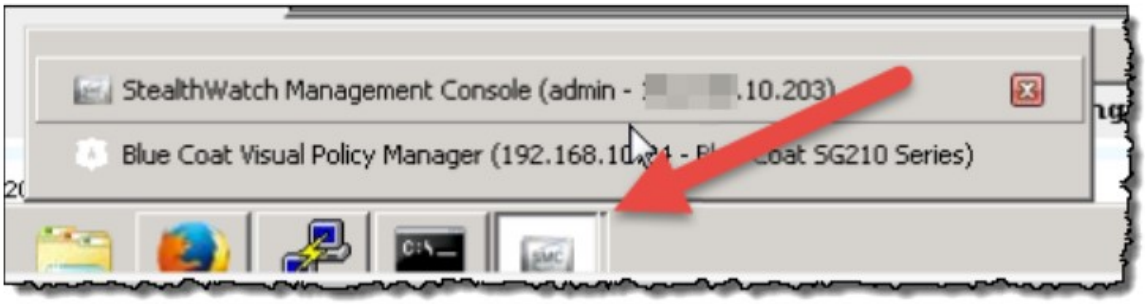
Further notes on configuration:

- Confirm that the Flow Collector and Proxy use the same NTP server (or receive time from a common source for flow and proxy records to be matched).
- Only one log output mechanism for the proxy is supported. If you are already exporting logs, you cannot capture and parse proxy records.
- The UDP Director High Availability is not supported.

Configuring the Visual Policy Manager

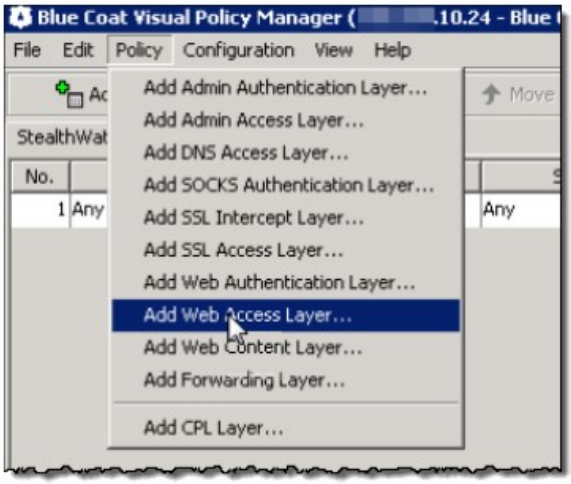
Configuration of the Visual Policy Manager enables you to check that the proxy log is being sent to the Flow Collector.

1. In the Configuration tab page in the main menu, click Policy > Visual Policy Manager. The Visual Policy Manager opens.



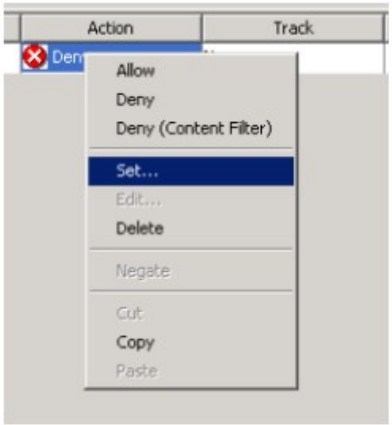
2. Click the Launch button at the bottom for your configured log. The Visual Policy Manager for the log window opens.

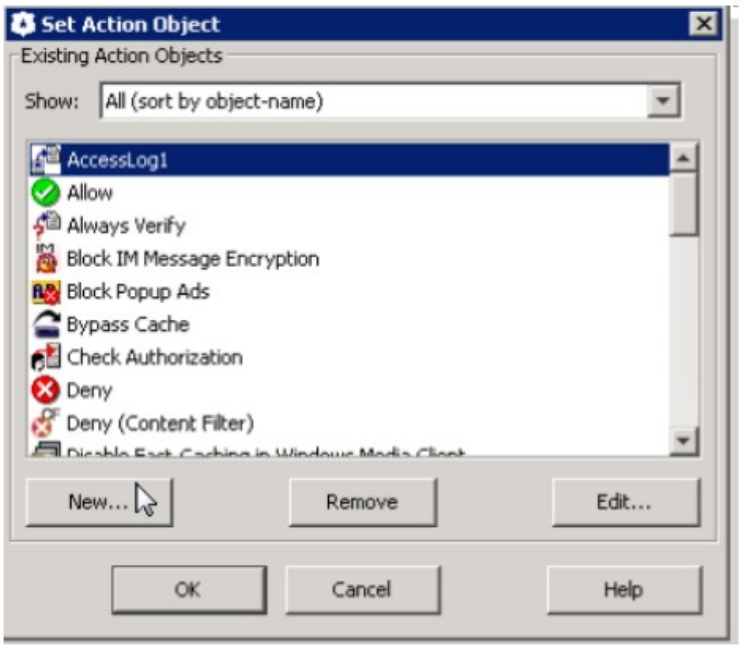
3. Click Policy > Add Web Access Layer. The Add New layer screen opens.



4. Type a name for the new layer, and then click OK.

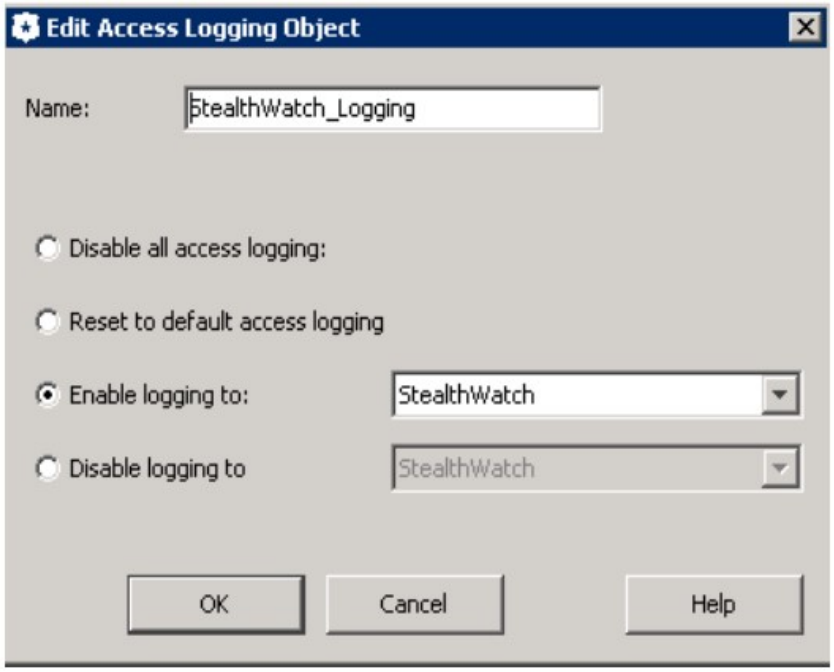
5. Right-click Deny in the Action column and then click Set. The Set Action Object dialog opens.





6. Click New and select Modify Access Logging. The Edit Access Logging Object dialog opens.

7. Click Enable logging to.

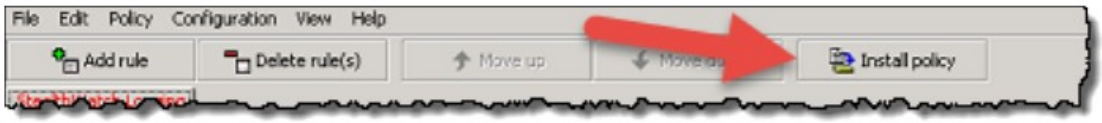


8. Type a name for your log and then select your log.

9. Click OK. The object is added.

10. In the Set Action Object dialog, click OK.

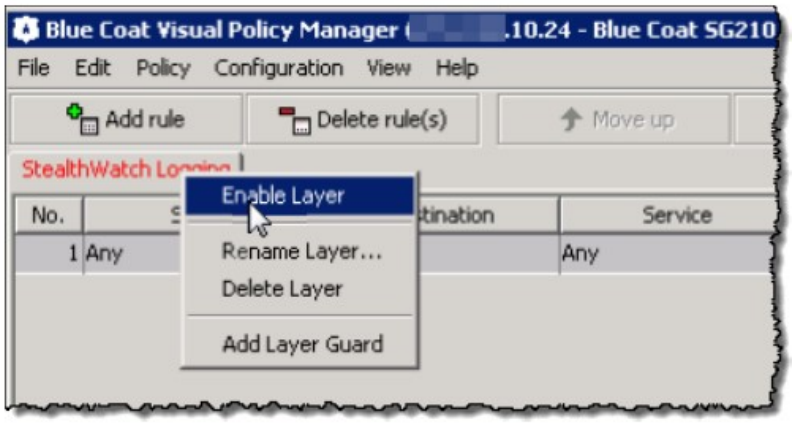
11. Click the Install policy button at the top right.



12. Click No and then OK for the following windows.

13. Launch the Blue Coat Visual Policy Manager again.

14. Right-click the logging tab and then select Enable Layer.

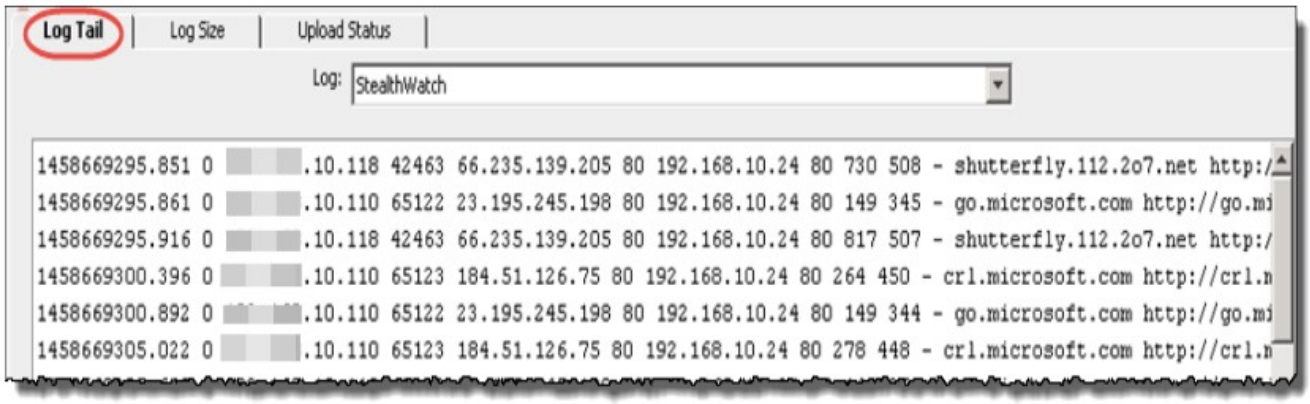


15. Click the Install Policy button. The Policy Installed opens.

16. Click OK.

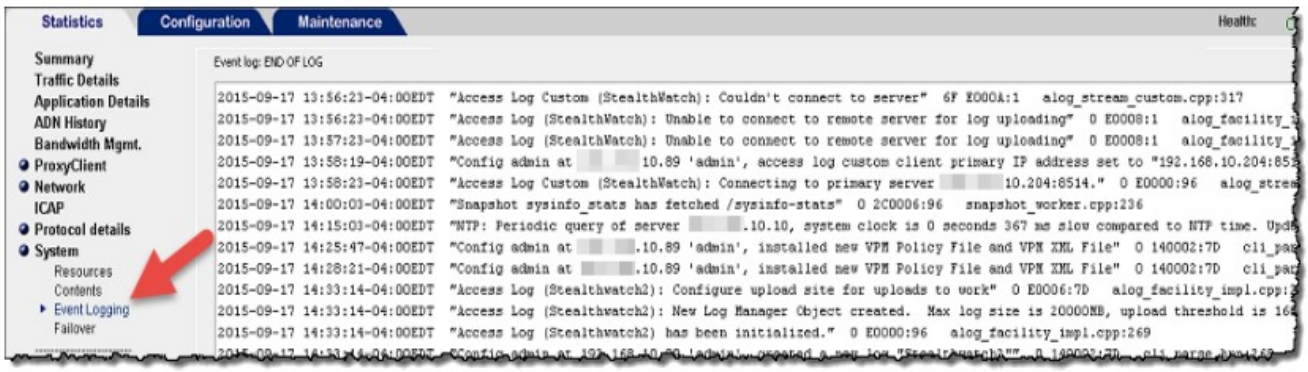
17. Click the Statistics tab, and in the log menu, select your log.

18. In the main menu, click Access Logging, and then click the Log Tail tab. The Log Tail window opens.



19. Click Start Tail button at the bottom of the page.

20. On the Statistics main menu, click System > Event Logging. This page will show if the log file is uploaded to the Flow Collector and the changes made. It shows whether the proxy is connected to the Flow Collector.



21. Continue to the Configuring the Flow Collector section to set up your Flow Collector to receive syslog information.

Configuring the McAfee Proxy Logs

Use this section to configure McAfee proxy logs from the McAfee Web Gateway to send to Secure Network Analytics.

- Make sure that you have downloaded the XML configuration file for the McAfee proxy. Go to Cisco Software Central to download the readme and Proxy Log XML configuration files.
- Log in to your Cisco Smart Account at https://software.cisco.com or contact your administrator.
- The McAfee proxy version used for testing was 7.4.2.6.0 – 18721.

To set up the McAfee proxy log, complete the following steps:

1. Download the XML file, FlowCollector_[date]_McAfee_Log_XML_Config_[v].xml, and then save it to your preferred location.

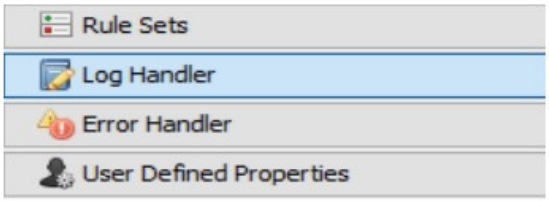
The "Date" indicates the date of the XML file, and "v" indicates the version of the McAfee proxy version. Select the XML file with the same version number as your McAfee proxy.

To download the file, complete the following steps:

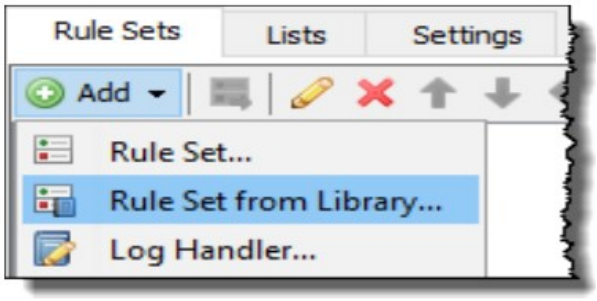
- a. Go to https://software.cisco.com, Cisco Software Central.
- b. In the Download and manage > Download and Upgrade section, select Access downloads.
- c. Scroll down to the select a Product field.
- d. Type Secure Network Analytics in the Select a Product field. Press Enter.
- e. Select Secure Network Analytics Virtual Flow Collector or another Flow Collector.
- f. Select Secure Network Analytics System Software > Configuration Files.

2. Log in to the McAfee proxy server.

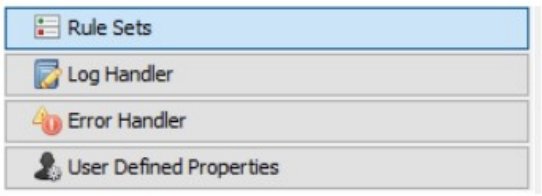
3. Click the Policy icon, and then click the Rule Sets tab.



4. Select Log Handler, and then select Default.



5. Click Add > Rule Set from the Library.



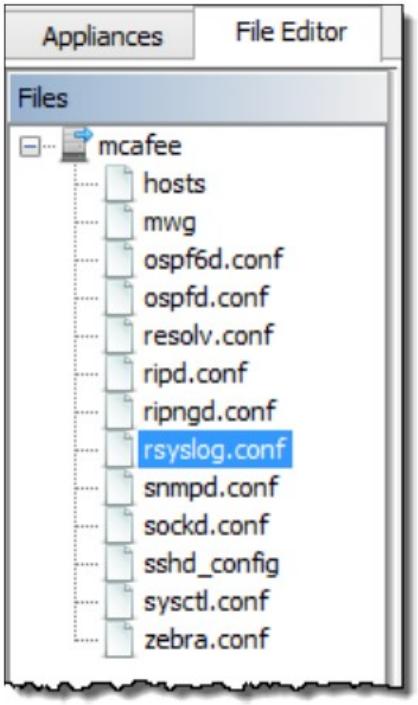
6. Click Import from file, and then select the XML file.

7. Select mcafeelancopelog in the log handler that was just imported.

Make sure the rule set and the rule “create access logline” and “send to syslog” is enabled.

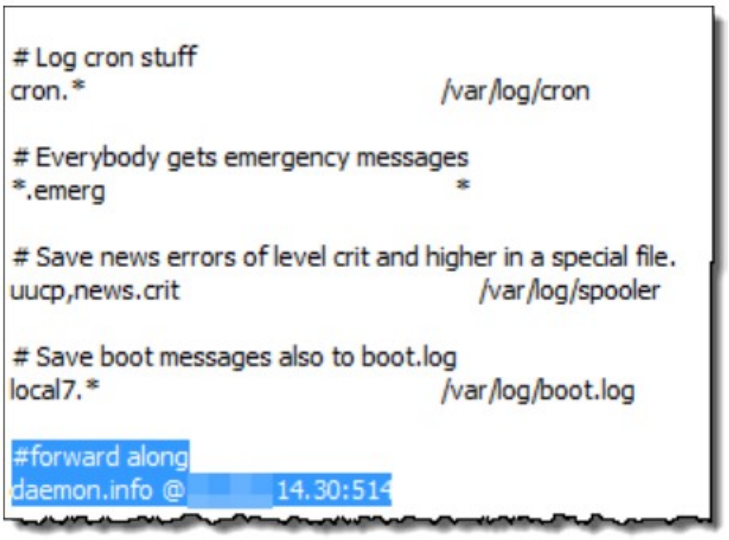
8. Click the Configuration icon at the top of the page.

9. At the left of the page, click the File Editor tab, and then select the rsyslog.conf file.



10. At the bottom of the text box (beside the list of files), type the following text:

```
daemon.info @[FlowCollector IP Address:514]
```



Make sure to select the Flow Collector that collects data from the exporters and end points that you want to investigate in the proxy logs.

11. Comment out this line:

```
*.info;mail.none;authpriv.none;cron.none.
```

12. Add this line:

```
*.info;daemon.!=info;mail.none;authpriv.none;cron.none - /var/log/messag
```

13. Click the Save Changes button at the top right of the page.

14. Continue to the Configuring the Flow Collector section to set up your Flow Collector to receive syslog information.

Configuring Squid Proxy Logs

Use this section to configure Squid proxy logs to send to Secure Network Analytics. You can edit the files on the proxy server using SSH.
To configure the Squid proxy logs, complete the following steps:

1. Log into a shell for the machine running Squid.

2. Go to the directory containing squid.conf (typically /etc/squid) and open it in an editor.

3. Add the following lines to squid.conf to configure logging:

```
logformat access_format %ts%03tu %<tt %>a %>p %>st %<A %<st %<la %<lp %l
access_log syslog:user.6 access_format
```

4. Restart squid using the following:

- For init based systems: /etc/init.d/squid3 restart
- For systemd based systems: systemctl restart squid

5. Configure the syslog service on the Squid server to forward logs to the Flow Collector. This is dependent on the Linux distribution/syslog service.

For syslog-ng, add the following to /etc/syslog-ng/syslog-ng.conf:

```
# Audit Log Facility BEGIN
filter bs_filter { filter(f_user) and level(info) };
destination udp_proxy { udp("10.205.14.15" port(514)); };
log {
source(s_all);
filter(bs_filter);
destination(udp_proxy);
};
# Audit Log Facility END
```

For rsyslog, add the following to /etc/rsyslog.conf:

```
:programname, contains, "squid" @10.205.14.15:514
```

Make sure to select the Flow Collector that collects data from the exporters and end points that you want to investigate in the proxy logs.

6. Then restart syslog service.

- For init based systems:
  /etc/init.d/syslog-ng restart (for syslog-ng)
  /etc/init.d/rsyslog restart (for rsyslog)
- For systemd based systems:
  systemctl restart syslog (for syslog-ng)
  systemctl restart rsyslog (for rsyslog)

7. Continue to the Configuring the Flow Collector section to receive syslog information.

Configuring the Flow Collector

After you have configured the proxy server, you need to configure the Flow Collector to accept the data.

To configure the Flow Collector to receive syslog information, complete the following steps:

1. Log in to your Manager.

2. Select Configure > Global > Central Management.

3. Click the (Ellipsis) icon for your Flow Collector, then click View Appliance Statistics.

4. Log in to the Flow Collector. The Flow Collector interface opens.

5. Click Configuration > Proxy Ingest. The Proxy Servers page opens.

6. Type the IP address of proxy server.

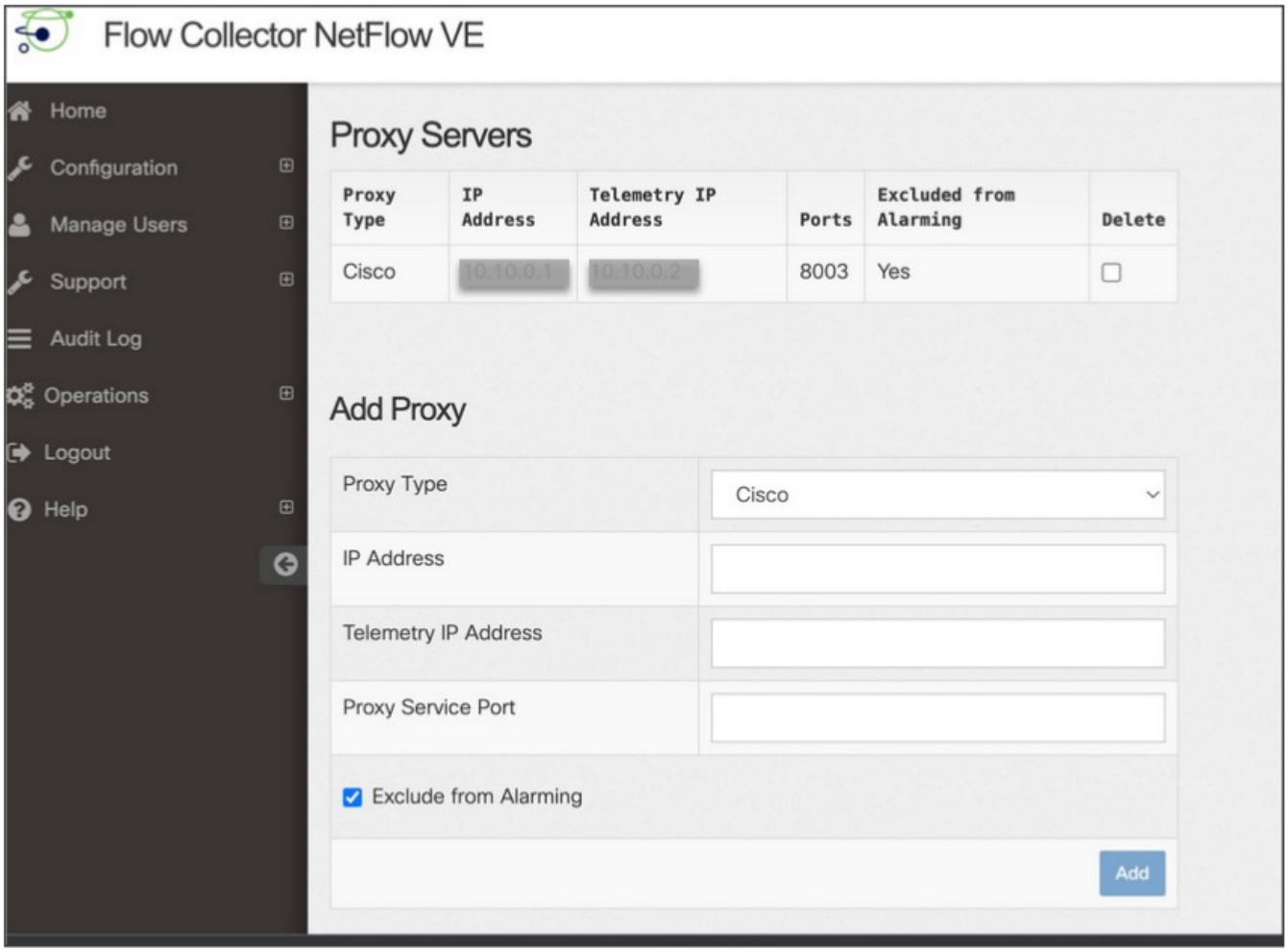
7. From the Proxy Type drop-down list, select your proxy server.

If your type of proxy server is not listed, you will not be able to use proxy logs at this time.

8. If the Proxy Server:

- has only one IP address, then type the IP address of the proxy server in the IP Address field. Leave the Telemetry IP Address field empty.
- has more IP addresses, then type the management IP address of the proxy server (syslog's message's source IP address) in the IP Address field. In the Telemetry IP Address field, type the telemetry IP address of the proxy server.

9. In the Proxy Service Port field, type the port number of the proxy server.



10. If you want the proxy server to trigger alarms, un-check the Exclude from Alarming check box.

11. Click Add.

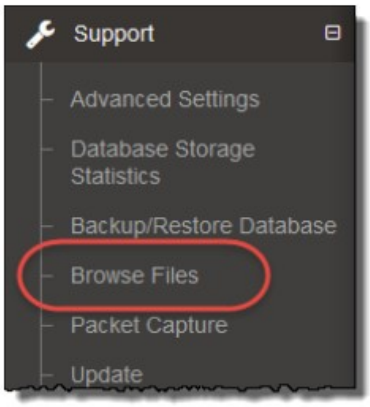
12. Click Apply. The proxy server appears in the Proxy Ingest table at the top of the page.

13. Continue to the Checking the Flows section.

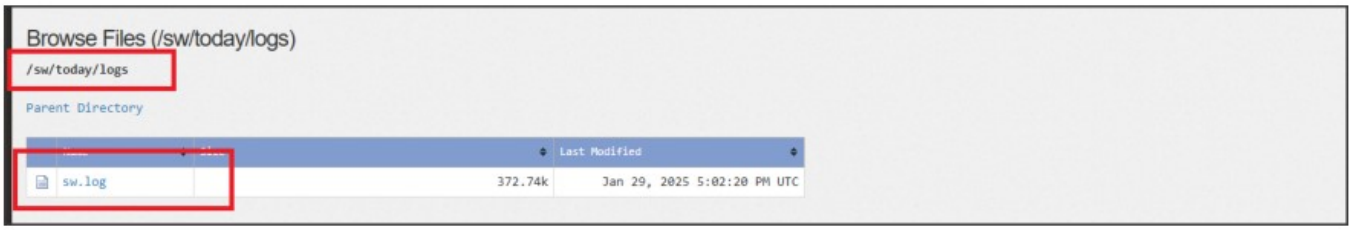
Checking the Flows

To check that you are receiving the flows, complete the following steps:

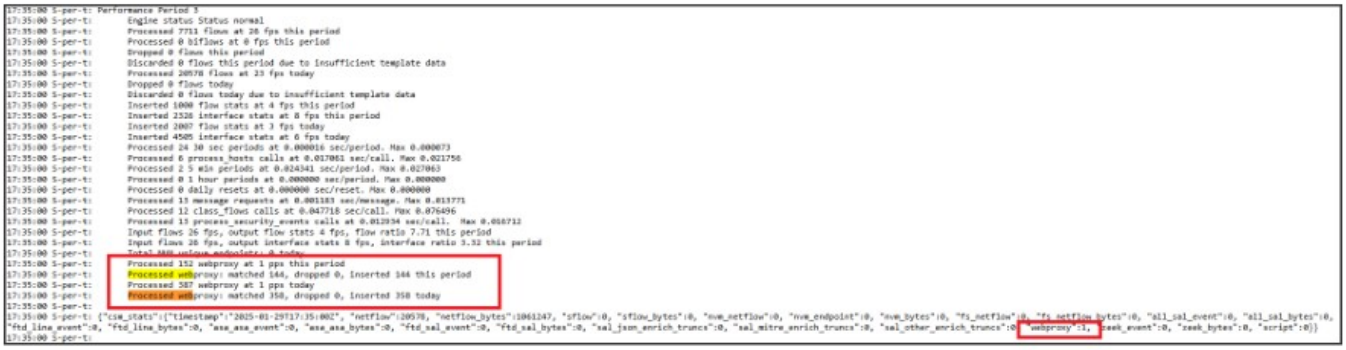
1. In the Flow Collector interface, click Support > Browse Files in the main menu. The Browse Files page opens.



2. Open the sw.log file.



3. Check that the webproxy is counting upwards to show that you are receiving data.



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
- 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

Change History

Document Version	Published Date	Description
1_0	August 7, 2025	Initial Version.

Copyright Information

Documents / Resources

	CISCO WSA Secure Network Analytics [pdf] User Guide WSA 14-5-1-016, Blue Coat, McAfee, Squid, WSA Secure Network Analytics, WSA, Secure Network Analytics, Network Analytics, Analytics

References

- User Manual

Cisco

Analytics, Blue Coat, Cisco, McAfee, Network Analytics, Secure Network Analytics, Squid, WSA, WSA 14-5-1-016, WSA Secure Network Analytics

Leave a comment

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search:

e.g. whirlpool wrf535swhz

Search