



Cisco Secure Network Analytics

Proxy Log Configuration Guide 7.5.1



Table of Contents

Introduction	3
Requirements	3
Configuration Overview	4
Configuring the Cisco Web Security Appliance (WSA) Proxy Logs	5
Configuring the Blue Coat Proxy Logs	9
Creating the Format	9
Create a New Log	10
Configure the Upload Client	11
Configuring the Upload Schedule	14
Requirements	14
Configuring the Visual Policy Manager	14
Configuring the McAfee Proxy Logs	20
Configuring Squid Proxy Logs	24
Configuring the Flow Collector	26
Checking the Flows	28
Contacting Support	30
Change History	31

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:

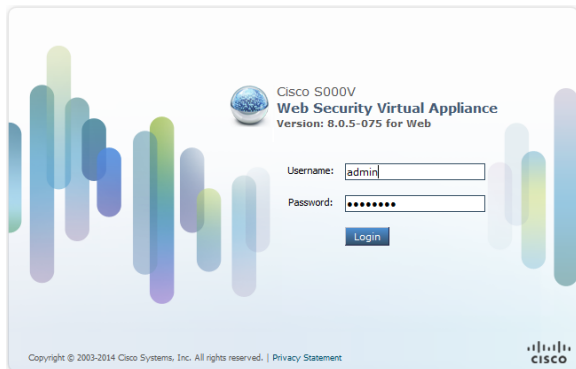
1. Choose one of the following methods to configure your proxy server.
 - [Configuring the Cisco Web Security Appliance \(WSA\) Proxy Logs](#)
 - [Configuring the Blue Coat Proxy Logs](#)
 - [Configuring the McAfee Proxy Logs](#)
 - [Configuring Squid Proxy Logs](#)
2. [Configuring the Flow Collector](#)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

Configuring the Cisco Web Security Appliance (WSA) Proxy Logs

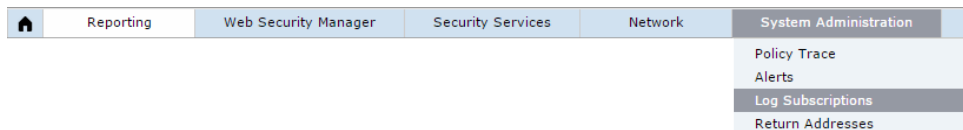
Use this section to configure Cisco proxy logs to send to Secure Network Analytics.

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

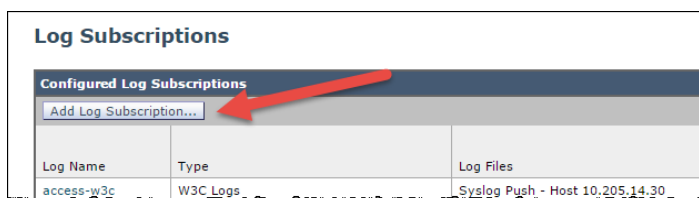
To set up the Cisco proxy log, complete the following steps:



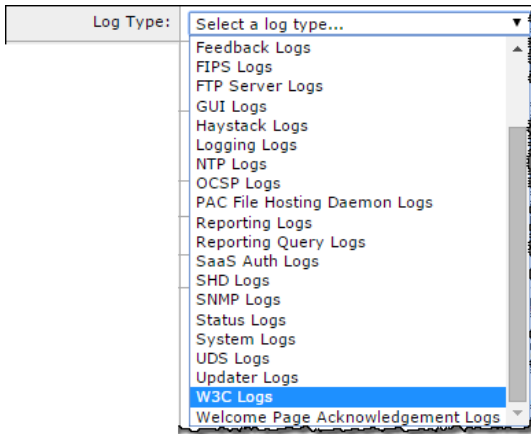
1. Log in to the Cisco proxy server.



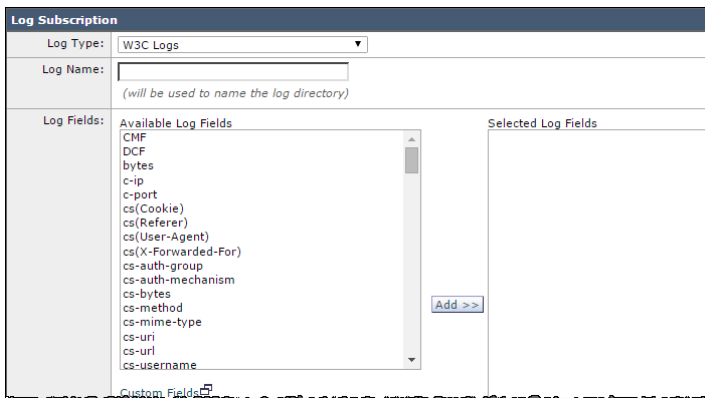
2. On the main menu, click **System Administration > Log Subscriptions**. The Log Subscriptions page opens.



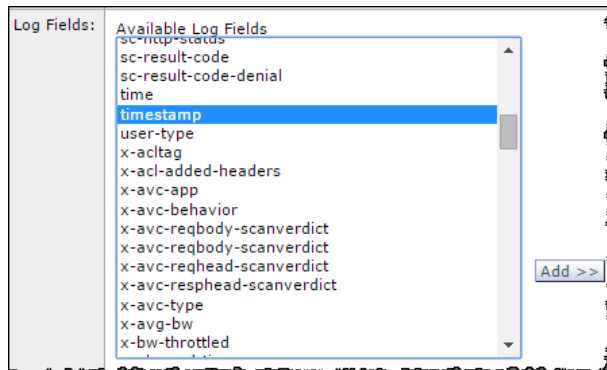
3. Click the **Add Log Subscriptions** button. The New Log Subscriptions page opens.



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

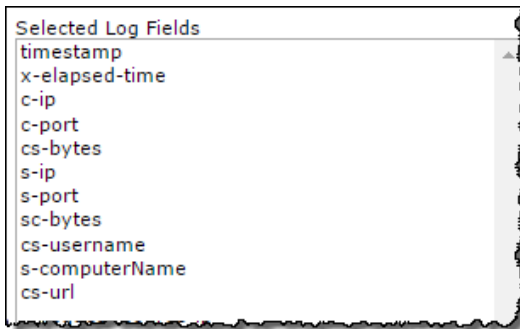


5. In the Log Name field, type a name for the log that you will use.
6. From the Available Log Fields list, select **Timestamp**, and then click **Add** to move it the Select Log Fields list.



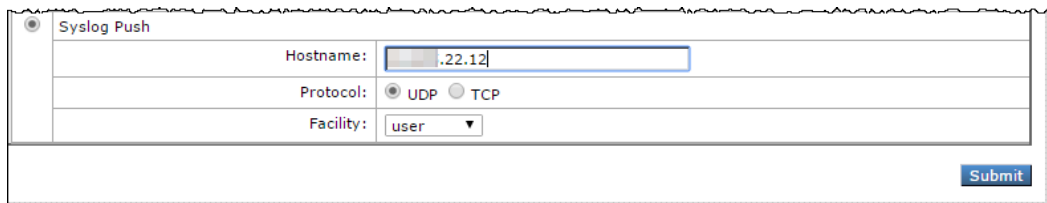
7. Repeat the previous step for the each of the following log fields in order:
 - a. timestamp
 - b. x-elapsed-time
 - c. c-ip
 - d. c-port
 - e. cs-bytes
 - f. s-ip
 - g. s-port
 - h. sc-bytes
 - i. cs-username
 - j. s-computerName
 - k. cs-url

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.



Syslog Push

Hostname:

Protocol: UDP TCP

Facility:

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



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.

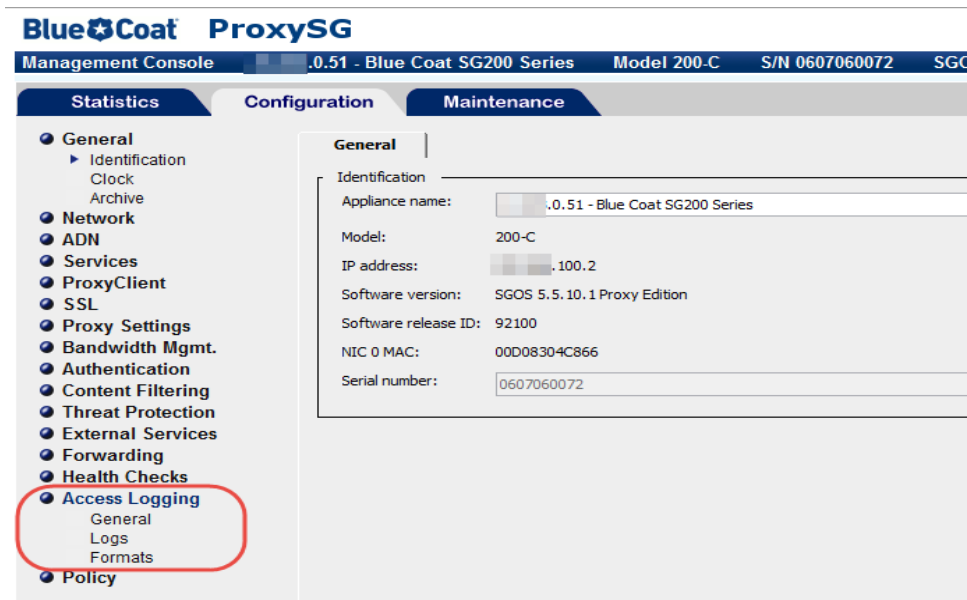


The Blue Coat proxy version used for testing was SG V100, SGOS 6.5.5.7 SWG Edition.

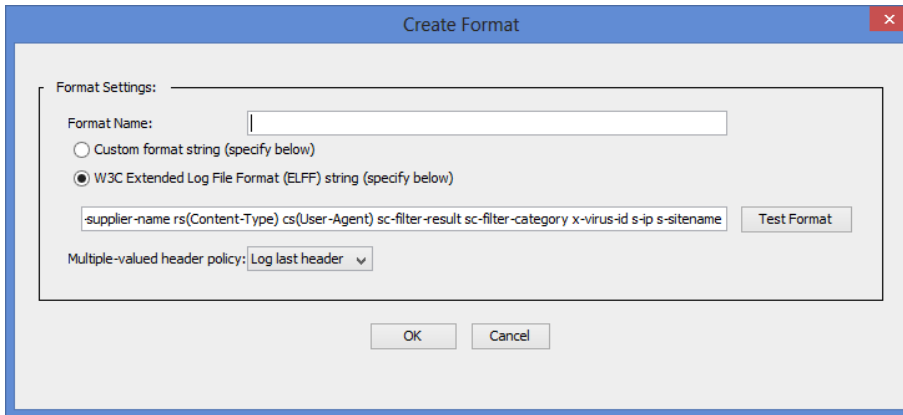
Creating the Format

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:

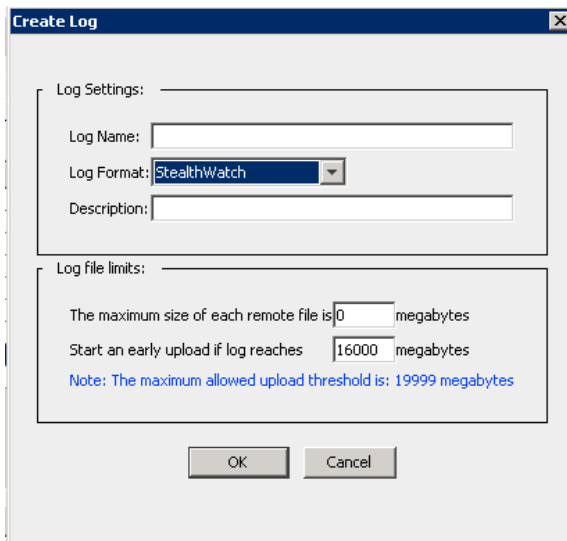
```
timestamp duration c-ip c-port r-ip r-port s-ip s-port cs-bytes
sc-bytes cs-user cs-host cs-uri
```

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.

Logs | **General Settings** | Upload Client | Upload Schedule

Log: StealthWatch

Log Settings:

Log Format: StealthWatch

Description:

Log file limits:

The maximum size of each remote file is 0 megabytes

Start an early upload if log reaches 16000 megabytes

Note: The maximum allowed upload threshold is: 19999 megabytes

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.

Logs | General Settings | **Upload Client** | Upload Schedule

Log: StealthWatch

Upload Client:

Client type: Custom Client Settings Test Upload

Transmission Parameters:

Encryption Certificate: <No Encryption>

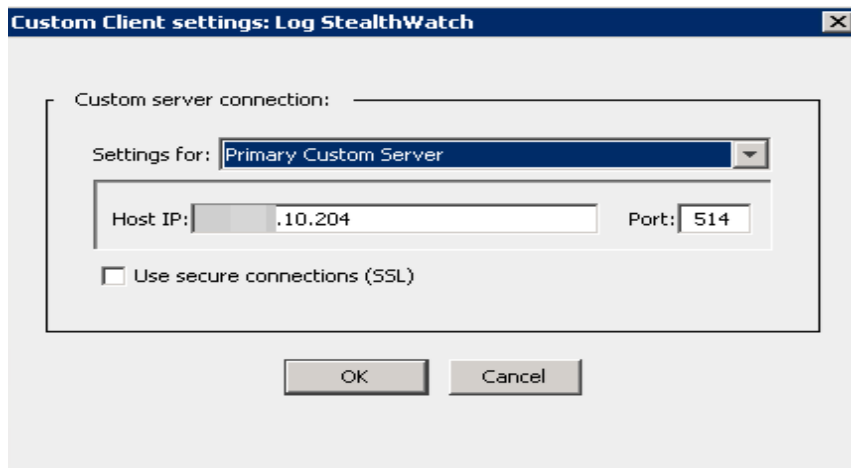
Signing Keyring: <No Signing>

Save the log file as: gzip file text file

Send partial buffer after: 5 seconds

Bandwidth Class: <None>

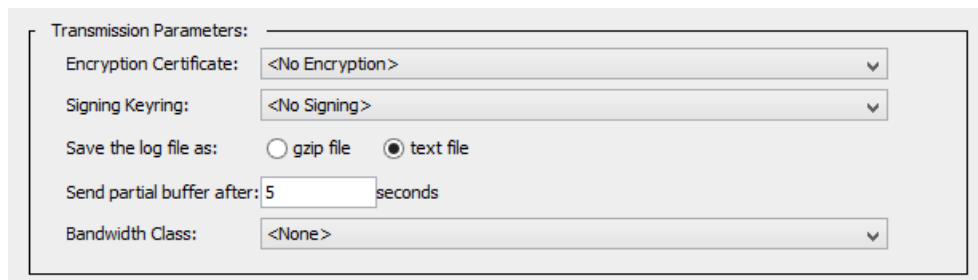
2. From the Client type drop-down list, select **Custom Client**.
3. Click the **Settings** button. The Custom Client settings page opens.



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

i 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.

The screenshot shows a web interface with four tabs: 'Logs', 'General Settings', 'Upload Client', and 'Upload Schedule'. The 'Upload Schedule' tab is active. Below the tabs, there is a 'Log:' dropdown menu with 'StealthWatch' selected. Underneath, there is a section for 'Upload type:'. It includes a heading 'Upload the access log' and two radio buttons: 'continuously' (which is selected) and 'periodically'. Below these are two input fields: 'Wait between connect attempts:' with a value of '60' and 'seconds', and 'Time between keep-alive log packets:' with a value of '5' and 'seconds'.

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:

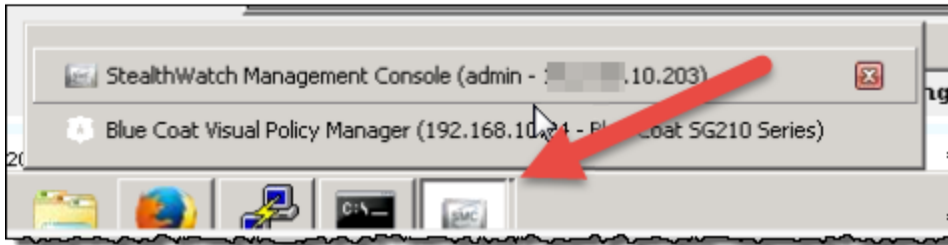
- Confirm that the Flow Collector and Proxy use the same NTP server (or receive time from a common source for flow and proxy records to be matched).
- Only one log output mechanism for the proxy is supported. If you are already exporting logs, you cannot capture and parse proxy records.
- The UDP Director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

Configuring the Visual Policy Manager

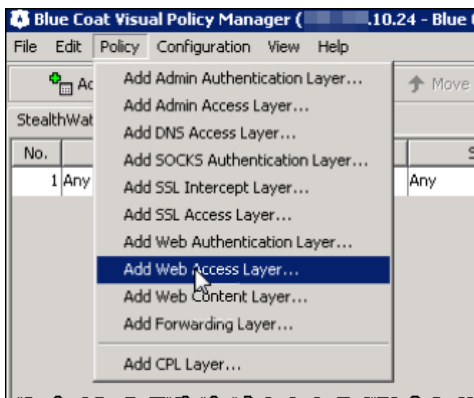
Configuration of the Visual Policy Manager enables you to check that the proxy log is being sent to the Flow Collector.



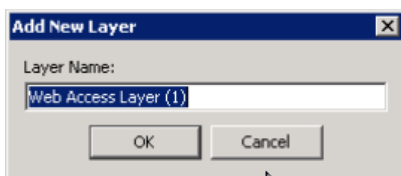
1. In the Configuration tab page in the main menu, click **Policy > Visual Policy Manager**. The Visual Policy Manager opens.



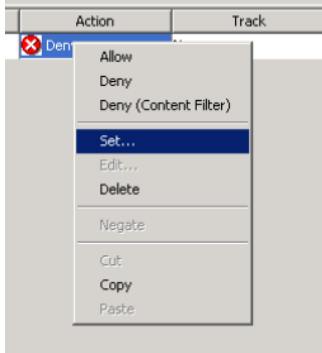
2. Click the Launch button at the bottom for your configured log. The Visual Policy Manager for the log window opens.



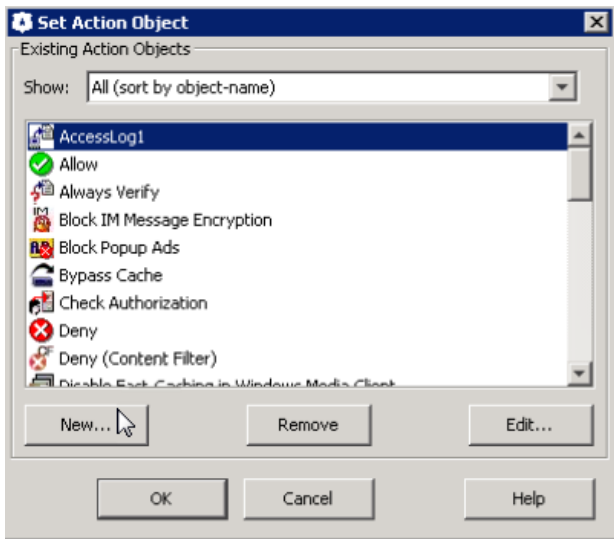
3. Click **Policy > Add Web Access Layer**. The Add New layer screen opens.



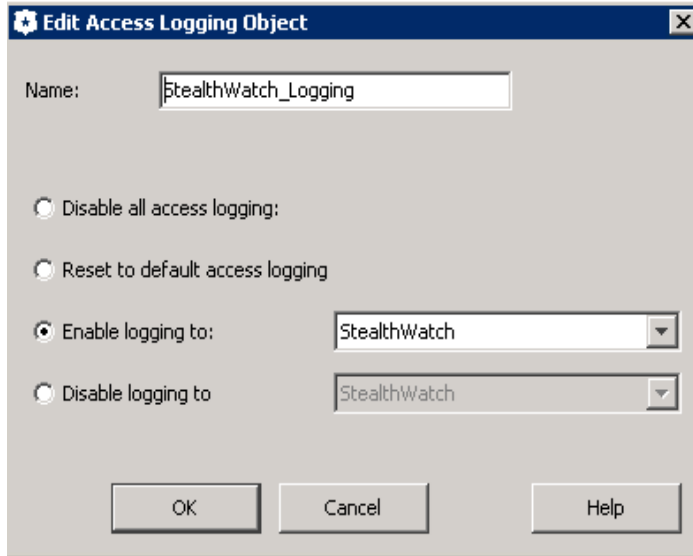
4. Type a name for the new layer, and then click **OK**.



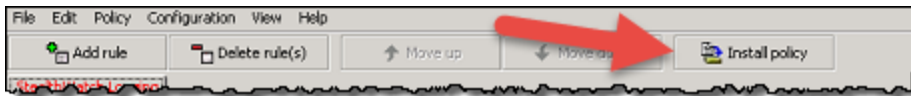
5. Right-click **Deny** in the Action column and then click **Set**. The Set Action Object dialog opens.



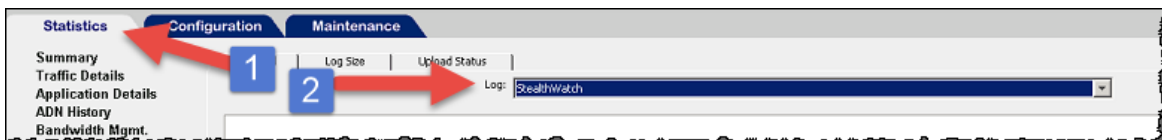
6. Click **New** and select **Modify Access Logging**. The Edit Access Logging Object dialog opens.



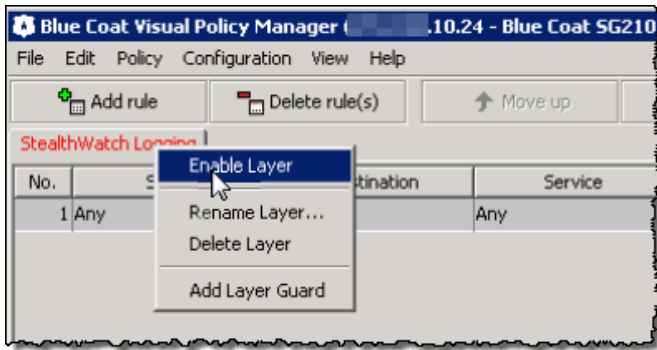
7. Click **Enable logging to**.
8. Type a name for your log and then select your log.
9. Click **OK**. The object is added.
10. In the Set Action Object dialog, click **OK**.



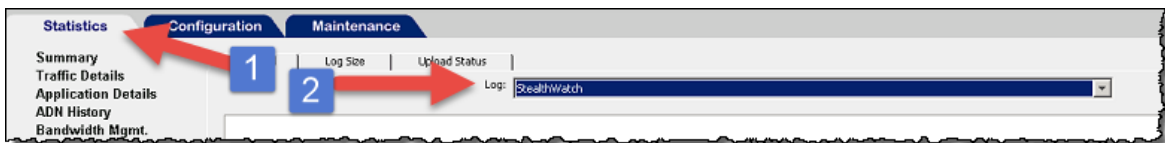
11. Click the **Install policy** button at the top right.
12. Click **No** and then **OK** for the following windows.



13. Launch the Blue Coat Visual Policy Manager again.



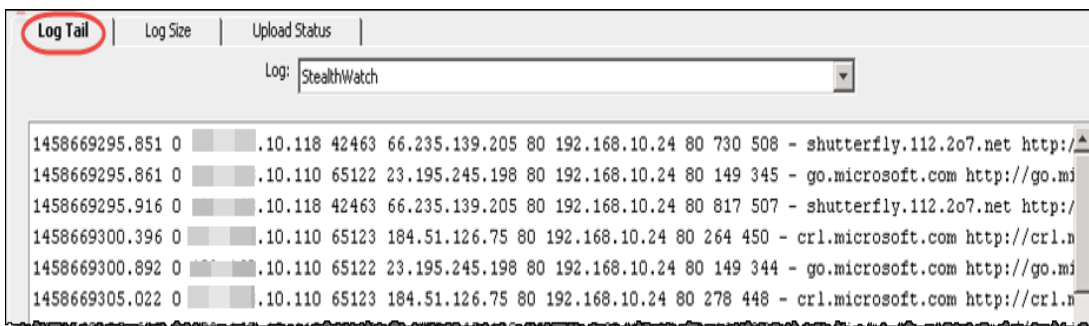
14. Right-click the logging tab and then select **Enable Layer**.
15. Click the Install Policy button. The Policy Installed opens.
16. Click **OK**.



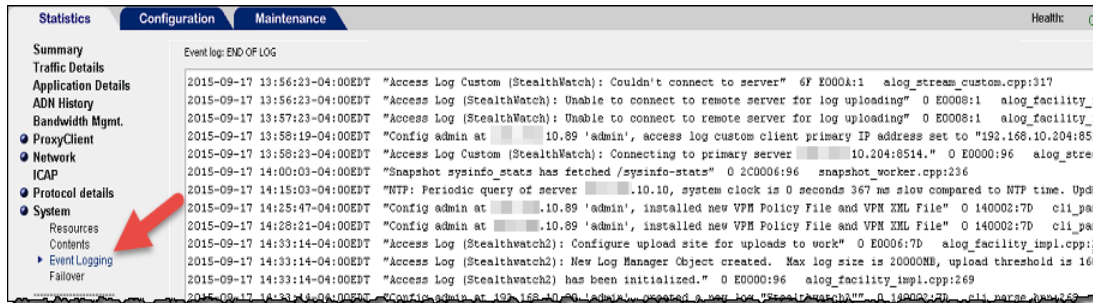
17. Click the **Statistics** tab, and in the log menu, select your log.



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:

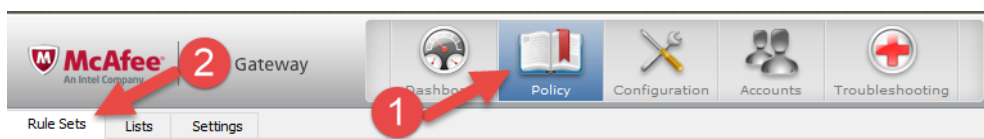
1. Download the XML file, FlowCollector_[date]_McAfee_Log_XML_Config_[v].xml, and then save it to your preferred location.



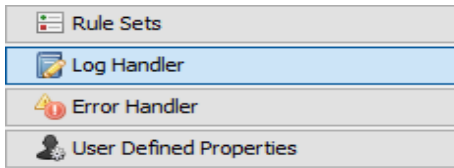
The "Date" indicates the date of the XML file, and "v" indicates the version of the McAfee proxy version. Select the XML file with the same version number as your McAfee proxy.

To download the file, complete the following steps:

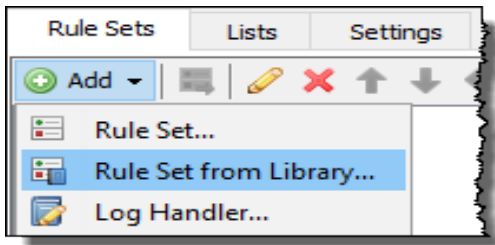
- a. Go to <https://software.cisco.com>, **Cisco Software Central**.
 - b. In the **Download and manage > Download and Upgrade** section, select **Access** downloads.
 - c. Scroll down to the select a **Product** field.
 - d. Type **Secure Network Analytics** in the **Select a Product** field. Press **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.



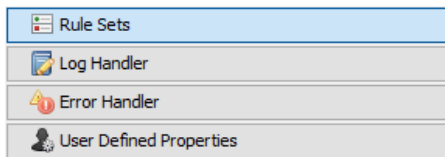
- Click the Policy icon, and then click the **Rule Sets** tab.



- Select **Log Handler**, and then select **Default**.



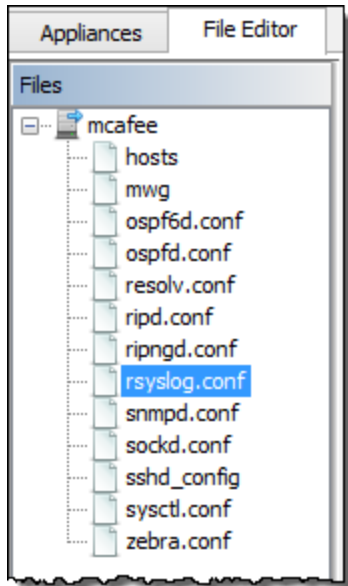
- Click **Add > Rule Set from the Library**.



- Click **Import from file**, and then select the XML file.
- Select **mcafeelancopelog** in the log handler that was just imported.

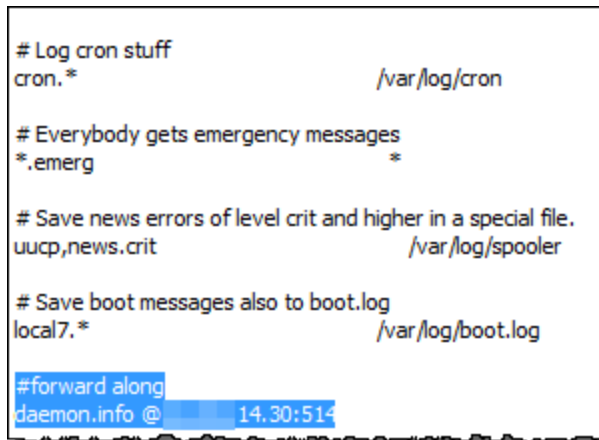
i Make sure the rule set and the rule “create access logline” and “send to syslog” is enabled.

- Click the Configuration icon at the top of the page.
- 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/messages`.
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 %la %lp %un %ru  
  
access_log syslog:user.6 access_format
```

4. Restart squid using the following:

```
/etc/init.d/squid3 restart
```

5. Configure the syslog service on the Squid server to forward logs to the Flow Collector. This is dependent on the Linux distribution, but for `syslog-ng` you would add the following to `/etc/syslog-ng`:

```
# 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
```



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-ng` with `/etc/init.d/syslog-ng restart`.
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.

The screenshot shows the 'Flow Collector NetFlow VE' interface. On the left is a navigation menu with options: Home, Configuration, Manage Users, Support, Audit Log, Operations, Logout, and Help. The main content area is titled 'Proxy Servers' and contains a table with the following data:

Proxy Type	IP Address	Telemetry IP Address	Ports	Excluded from Alarming	Delete
Cisco	10.10.0.1	10.10.0.2	8003	Yes	<input type="checkbox"/>

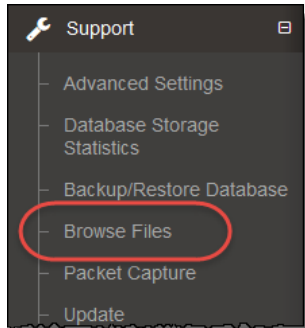
Below the table is the 'Add Proxy' form with the following fields:

- Proxy Type: Cisco (dropdown menu)
- IP Address: [text input field]
- Telemetry IP Address: [text input field]
- Proxy Service Port: [text input field]
- Exclude from Alarming: (checked)
- Add: [button]

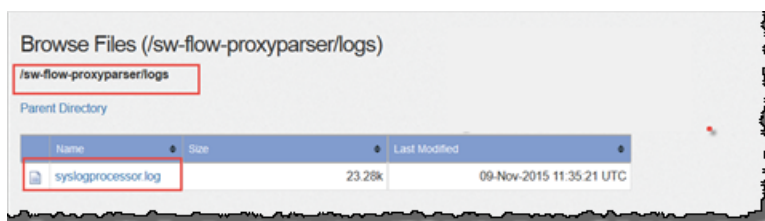
10. If you want the proxy server to trigger alarms, un-check the **Exclude from Alarming** check box.
11. Click **Add**.
12. Click **Apply**. The proxy server appears in the Proxy Ingest table at the top of the page.
13. Continue to the [Checking the Flows](#) section.

Checking the Flows

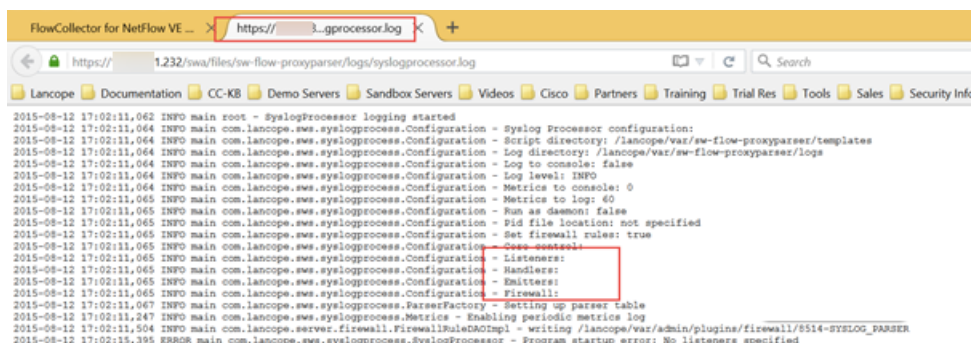
To check that you are receiving the flows, complete the following steps:



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



2. Open the syslog file.



3. Check that the marked files are not blank. If there are then, there is an issue.
 - Listeners has the number of the proxies.
 - Handlers is only one that parses out the data.
 - Emitters take parsed data from the handler and convert it into a format the engine

is looking for.

- Firewall

```

2015-11-11 16:04:26,354 INFO main com.lancope.ses.syslogprocess.Configuration - Syslog Processor configuration.
2015-11-11 16:04:26,354 INFO main com.lancope.ses.syslogprocess.Configuration - Script directory: /lancope/var/ra-flow-prongparser/complete
2015-11-11 16:04:26,354 INFO main com.lancope.ses.syslogprocess.Configuration - Log directory: /lancope/var/ra-flow-prongparser/imp
2015-11-11 16:04:26,354 INFO main com.lancope.ses.syslogprocess.Configuration - Log to console: false
2015-11-11 16:04:26,354 INFO main com.lancope.ses.syslogprocess.Configuration - Log Level: INFO
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - Metrics to console: 0
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - Metrics to log: 0
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - Run as daemon: false
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - PID file location: not specified
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - Set firewall rules: true
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - Core control:
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - Listeners:
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - @ syslog: port=8514
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - @ headers:
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - @ proxy: sourceip=10.205.14.14 emitter=prongengine pa
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - @ filters:
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - @ @psmp/prongengine:
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - @ @RECONNECT: iface=eth0 protocol=udp destport=8514 srcport=1
2015-11-11 16:04:26,355 INFO main com.lancope.ses.syslogprocess.Configuration - @ @ @ port=8514 protocol=udp exporter=true ip=10.205.14.14
2015-11-11 16:04:26,357 INFO main com.lancope.ses.syslogprocess.ParserFactory - Setting up parser table
2015-11-11 16:04:26,428 INFO main com.lancope.ses.syslogprocess.Metric - Enabling periodic metric log
2015-11-11 16:04:26,568 INFO main com.lancope.ses.syslogprocess.core.FirewallRuleManager - writing /lancope/var/ra-flow-prongparser/firewall/8514-8514
2015-11-11 16:04:27,791 INFO main com.lancope.ses.syslogprocess.core.DisruptorCore - Core configuration started
2015-11-11 16:04:27,791 INFO main com.lancope.ses.syslogprocess.core.DisruptorCore - Core configuration: single producer, blocking wait st
2015-11-11 16:04:27,881 INFO main com.lancope.ses.syslogprocess.SyslogProcessor - Starting metric log job
2015-11-11 16:04:27,886 INFO pool-2-thread-1 com.lancope.ses.syslogprocess.Metric - Listeners: c@ rates: @ rate1: @ rate1: @ rate1: @
2015-11-11 16:04:27,886 INFO pool-2-thread-2 com.lancope.ses.syslogprocess.Metric - Listeners: c@ rates: @ rate1: @ rate1: @
2015-11-11 16:04:27,886 INFO pool-2-thread-1 com.lancope.ses.syslogprocess.Metric - Listeners: c@ rates: @ rate1: @ rate1: @
2015-11-11 16:04:27,886 INFO pool-2-thread-1 com.lancope.ses.syslogprocess.Metric - Listeners: c@
2015-11-11 16:04:27,887 INFO pool-2-thread-1 com.lancope.ses.syslogprocess.Metric - Listeners: c@ rates: @ rate1: @ rate1: @ rate1: @
2015-11-11 16:04:27,891 INFO pool-2-thread-1 com.lancope.ses.syslogprocess.Metric - Listeners: c@ rates: @ rate1: @ rate1: @
    
```

The C is the count. These should go up when logs going through.

4. Check that the count 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>
- 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>

Change History

Document Version	Published Date	Description
1_0	August 16, 2024	Initial Version.

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

