Configure Cisco Secure Web Appliance to Upload Log Files to Cisco Global Threat Alerts

Last updated: July 12, 2021

Contents

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution: Means *reader be careful.* In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning: IMPORTANT SAFETY INSTRUCTIONS

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Introduction

This document describes how to configure a Cisco Secure Web Appliance (formerly Web Security Appliance or WSA) to upload its log files to Cisco, where cloud-based machine learning analyzes the data and reports its findings in the global threat alerts (formerly Cognitive Intelligence or Cognitive Threat Analytics) portal.

Prerequisites

Requirements

Cisco ScanCenter is the administration portal into Cisco Cloud Web Security. You must first create a device account in Cisco ScanCenter for your Secure Web Appliance.

- Log in to Cisco ScanCenter
- Click the **Threats** tab
- Click the global settings menu icon in the upper-right corner of the page
- Click **Device Accounts**
- Choose **Automatic** upload method

For more information, see Proxy Device Uploads.

Once the device account is created, copy this information from the Add Device Account page in Cisco ScanCenter to paste into your Secure Web Appliance configuration:

- SCP host: `etr.cloudsec.sco.cisco.com`
- Device username generated for your proxy device, case sensitive, different per proxy device

For your Secure Web Appliance, you need:

- Hostname or IP address of your Secure Web Appliance
- Admin user password of your Secure Web Appliance (default password is `ironport`)
- Secure Web Appliance must be connected directly to the Internet without any additional proxy upstream
- Must be network connectivity between the Secure Web Appliance management interface and SCP host `etr.cloudsec.sco.cisco.com` using port `22`: firewall rules may need adjustment to allow this connection

Caution: The information in this document was created from devices in a lab environment. If your network is live, understand the potential impact of any configuration command.

Components Used

The information in this document was tested on these software versions:

- WSA 8.5.1 GD
- WSA 8.0.8
- WSA 7.7.5

The information in this document was tested on this hardware:

- WSA S100V
- WSA S160
- WSA S300V

Configure

Configure the Proxy

1. Point your web browser to your Secure Web Appliance: http://wsa_*hostname*:8080/
2. If needed, accept the insecure HTTPS certificate to proceed.
3. Log in as admin.
4. Navigate to **System Administration** > **Log Subscriptions**.
5. Click **Add Log Subscription**.
6. In the **Log Type** pull-down, select **W3C Logs**.
7. In the **Log Name** field, enter a descriptive name for the log directory.
8. Remove the pre-selected Log Fields by selecting all items in the **Selected Log Fields** box and clicking **Remove**.
9. In the **Custom Fields** box, enter the following items, using line breaks to separate them:
```
timestamp
x-elapsed-time
c-ip
cs-username
c-port
s-ip
s-port
cs-url
cs-bytes
sc-bytes
sc-body-size
cs(User-Agent)
cs-mime-type
cs-method
sc-http-status
cs(Referer)
sc(Location)
sc-result-code
x-amp-sha
x-amp-verdict
```

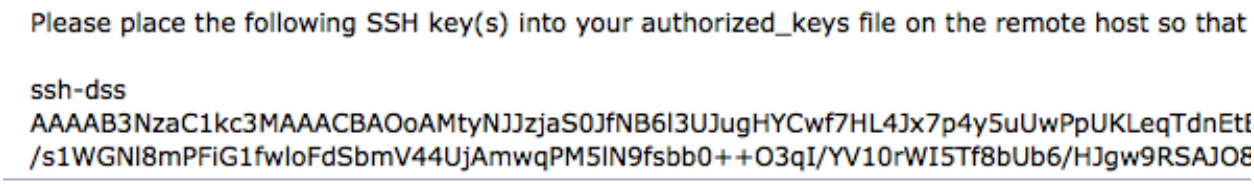
`x-amp-malware-name`
`x-amp-score`

Note: On WSA version 7.7.5, AMP is not supported, so do not add the four "`x-amp`" fields.

10. Once all items are entered, click **Add >>**.
11. In the **Rollover by File Size** field, enter `500M`.
12. In the **Rollover by Time** pull-down, select **Custom Time Interval**.
13. In the **Rollover every** field, enter for example `55m`.

Number of Users Behind Proxy	Recommended Upload Period
Unknown or less than 2000	55 minutes
2000 to 4000	30 minutes
4000 to 6000	20 minutes
More than 6000	10 minutes

14. In the **File Name** field, enter `w3c_log`.
15. Enable compression by checking **Log Compression**.
16. For **Retrieval Method**, select **SCP on Remote Server**.
17. In the **SCP Host** field, enter the SCP host provided in Cisco ScanCenter; for example: `etr.cloudsec.sco.cisco.com`
18. In the **SCP Port** field, enter `22`.
19. In the **Directory** field, enter `/upload`.
20. In the **Username** field, enter the username generated for your device in Cisco ScanCenter. The device username is case sensitive and different for each proxy device.
21. Select the **Enable Host Key Checking** check box, and select the **Automatically Scan** radio button.
22. Click **Submit**.
23. The Secure Web Appliance Management Console displays a public SSH key. Copy and paste the whole key, including the "ssh-dss" at the beginning, into the device account in Cisco ScanCenter. Successful authentication between your proxy device and global threat alerts will allow log files from your proxy device to be uploaded to Cisco for analysis.



24. Click **Commit Changes**.

    Caution: In order to process these changes, the proxy process will restart after you commit changes. This will cause a brief interruption in service. Additionally, the authentication cache will be cleared, which might require some users to authenticate again. We recommended you configure the Secure Web Appliance during an off-hour maintenance window to avoid impacting users during production hours.

New Log Subscription

Log Subscription

Log Type:	W3C Logs
Log Name:	w3clogs *(will be used to name the log directory)*
Log Fields:	Available Log Fields: CMF, DCF, bytes, c-ip, c-port, cs(Cookie), cs(Referer), cs(User-Agent), cs(X-Forwarded-For), cs-auth-group, cs-auth-mechanism, cs-bytes, cs-method, cs-mime-type, cs-uri, cs-url Add >> Selected Log Fields: timestamp, x-elapsed-time, c-ip, cs-username, c-port, s-ip, s-port, cs-url, cs-bytes, sc-bytes, sc-body-size, cs(User-Agent), cs-mime-type, cs-method, sc-http-status, cs(Referer), sc(Location), x-amp-sha, x-amp-verdict, x-amp-malware-name, x-amp-score Custom Fields *(Use line breaks to separate multiple entries)*
Rollover by File Size:	500M Maximum *(Add a trailing K or M to indicate size units)*
Rollover by Time:	Custom Time Interval Rollover every: 55m *(Example: 120s, 5m 30s, 4h, 2d)*
File Name:	w3c_log
Log Compression:	☑ Enable
Log Exclusions (Optional):	*(Enter the HTTP status codes of transactions that should not be included in the W3C Log)*
Retrieval Method:	○ FTP on prg5-wsa-s160.cisco.com Maximum Number of Files: 100 ○ FTP on Remote Server FTP Host: Directory: Username: Password: ◉ SCP on Remote Server SCP Host: etr.cloudsec.sco.cisco.com SCP Port: 22 Directory: /upload Username: d111... ☑ Enable Host Key Checking ◉ Automatically Scan ○ Enter Manually

Connect to Active Directory to Resolve Usernames

Setting up an Active Directory is not required for creating a log subscription, and you may already have it configured, but this helps in identifying affected devices. To see usernames in global threat alerts, the Secure Web Appliance needs to be able to authenticate all users. This can be accomplished by using the Transparent User Identification feature. For additional information, see Chapter 5 "Acquire End-User Credentials" in the Cisco Web Security Appliances User Guide.

1. Navigate to **Network** > **Authentication**.
2. Add a Realm connecting to your Active Directory:
    a. **Active Directory Server** is the name of your domain, not the hostname.
    b. **Active Directory Domain** is the name of your domain in capitalized letters.
    c. After clicking **Join Domain**, enter the credentials of a user with domain administrator rights; the Secure Web Appliance will create its own user in the Active Directory.
    d. Check **Enable Transparent User Identification using Active Directory** agent. There must be a Cisco Active Directory agent running and able to connect to Active Directory. Enter its server hostname and shared secret.
3. Navigate to **Web Security Manager** > **Identities**.
4. Edit **Global Identity Policy**. Set **Identification and Authentication to Identify Users Transparently** and pick the realm created in the previous step.
5. In **Network Authentication Global Authentication Settings** click on **Edit Global Settings** and set the **Action if Authentication Service Unavailable** to **Block all traffic if authentication fails**. This will prevent the addition of "*" in the **userid access** log field, which is added for non-authenticated users.

Using Secure Email and Web Manager to Configure Multiple Secure Web Appliances

The Cisco Secure Email and Web Manager (formerly Content Security Management Appliance or SMA) centralizes management functions across multiple Secure Web Appliances. However, the Secure Email and Web Manager does not help when setting up log uploading. Since configuration settings vary between Secure Web Appliances, and the Secure Email and Web Manager does not support W3C logs, each Secure Web Appliance must be configured individually.

Deployment Scenarios

Single Secure Web Appliance, Explicit or Transparent Mode, Single Routing Table

- Ensure you can reach the global threat alerts server on port 22.
- Control the interface to be used for the logs by the routing table.

Single Secure Web Appliance, Explicit Mode, Separate Routing Tables for DATA and MGMT Traffic

- Ensure you can reach the global threat alerts server on port 22 over the MGMT interface.
- SCP traffic is considered MGMT traffic and is sent out the MGMT port. Ensure the MGMT port can reach the global threat alerts server on port 22.

Upstream and Downstream Proxy

Typical configuration:

- Downstream proxy responsibilities: authentication, URL filtering
- Upstream proxy responsibilities: anti-malware scanning
- Client → Downstream → Upstream → Internet
- Separate routing tables for data and management (MGMT) traffic

In this scenario, the downstream proxy has username and client IP address, but not the destination IP address, which is a required field. Destination IP address is always known to the upstream proxy, but username is only seen by the downstream proxy.

In this case, activate the XFF (X-Forwarded-For) header on the downstream proxy and evaluate it on the upstream proxy. This way the upstream proxy knowns the client IP address. Configure the upstream proxy to send HTTP logs to the global threat alerts server via the MGMT interface.

Next Steps

From within Cisco ScanCenter, select the device account and enter the public SSH key. For more information, see Proxy Device Uploads.

Q&A

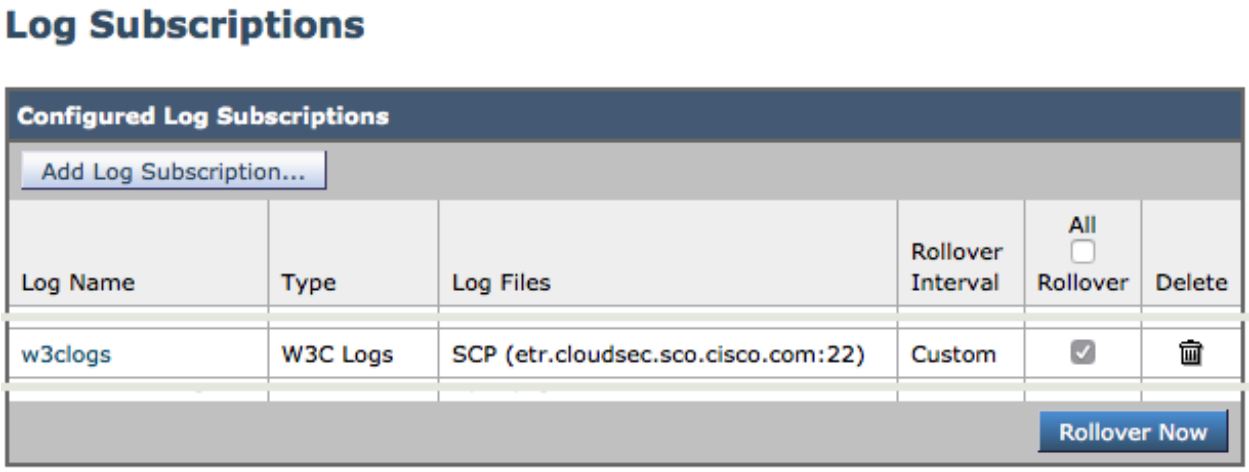
Can I anonymize the logs before sending?

Yes. Username and client IP are mandatory fields and can be anonymized. Usernames can be hashed and the mapping stored in a translation table for future reference. Valid IP addresses (client only) can also be anonymized.

Troubleshooting

To test your connection, force the Secure Web Appliance to attempt an immediate upload.

1. Navigate to the **Log Subscriptions** page.
2. For the subscription you want to test, select the **Rollover** check box.
3. Click the **Rollover Now** button.



Check Connectivity

Follow these steps to check connectivity:

1. Log in to the CLI of the Secure Web Appliance.
2. Enter the **logconfig** command.
3. Enter the **hostkeyconfig** command.
4. Enter the **scan** command.
5. Enter the global threat alerts server hostname: `etr.cloudsec.sco.cisco.com`
6. Choose **All** when asked for the SSH protocol type.
7. Enter **Y** when asked whether the host key should be added.

No RSA host key is known for etr.cloudsec.sco.cisco.com

If your telemetry data did not upload, check the Secure Web Appliance log. If you received this message:

"No RSA host key is known for etr.cloudsec.sco.cisco.com and you have requested strict checking. Host key verification failed. Lost connection."

Follow these steps to resolve:

1. Log in to the CLI of the Secure Web Appliance.
2. Enter the **logconfig** command.
3. Enter the **hostkeyconfig** command.
4. Delete the host key.
5. Press the Enter key to return to the main CLI.
6. Enter the **commit** command.
7. Repeat the configuration steps to add a log subscription. Ensure you select the **Enable Host Key Checking** check box, and select the **Automatically Scan** radio button.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.