Access Secure Web Appliance Logs

Contents

Introduction

This document describes the methods to view Secure Web Appliance (SWA) logs.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Physical or Virtual SWA Installed.
- License activated or installed.
- Secure Shell (SSH) Client.
- The setup wizard is completed.

- Administrative Access to the SWA.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

SWA Log Types

The Secure Web Appliance records its own system and traffic management activities by writing them to log files. Administrators can consult these log files to monitor and troubleshoot the appliance.

This table describes the Secure Web Appliance log file types.

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
Access Control Engine Logs	Records messages related to the Web Proxy ACL (access control list) evaluation engine.	No	No
Secure EndpointEngine Logs	Records information about file reputation scanning and file analysis (Secure Endpoint.)	Yes	Yes
Audit Logs	Records AAA (Authentication, Authorization, and Accounting) events. Records all user interaction with the application and command-line interfaces, and captures committed changes. Some of the audit log details are as follows: • User - Logon • User - Logon failed incorrect password • User - Logon failed unknown user name • User - Logon failed account expired • User - Logoff • User - Lockout • User - Activated • User - Password change • User - Password reset • User - Security settings/profile change • User - Created • User - Deleted/modified • Group/Role - Deletion / modified • Group /Role - Permissions change	Yes	Yes
Access Logs	Records Web Proxy client history.	Yes	Yes
ADC Engine Framework Logs	Records messages related to communication between the Web Proxy and the ADC engine.	No	No

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
ADC Engine Logs	Records debug messages from the ADC engine.	Yes	Yes
Authentication Framework Logs	Records authentication history and messages.	No	Yes
AVC Engine Framework Logs	Records messages related to communication between the Web Proxy and the AVC engine.	No	No
AVC Engine Logs	Records debug messages from the AVC engine.	Yes	Yes
CLI Audit Logs	Records a historical audit of command line interface activity.	Yes	Yes
Configuration Logs	Records messages related to the Web Proxy configuration management system.	No	No
Connection Management Logs	Records messages related to the Web Proxy connection management system.	No	No
Data Security Logs	Records client history for upload requests that are evaluated by the Cisco Data Security Filters.	Yes	Yes
Data Security Module Logs	Records messages related to the Cisco Data Security Filters.	No	No
DCA Engine Framework Logs (Dynamic Content Analysis)	Records messages related to communication between the Web Proxy and the Cisco Web Usage Controls Dynamic Content Analysis engine.	No	No
DCA Engine Logs (Dynamic Content Analysis)	Records messages related to the Cisco Web Usage Controls Dynamic Content Analysis engine.	Yes	Yes
Default Proxy Logs	Records errors related to the Web Proxy. This is the most basic of all Web Proxy related logs. To troubleshoot more specific aspects related to the Web Proxy,	Yes	Yes

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
	create a log subscription for the applicable Web Proxy module.		
Disk Manager Logs	Records Web Proxy messages related to writing to the cache on disk.	No	No
External Authentication Logs	Records messages related to using the external authentication feature, such as communication success or failure with the external authentication server. Even with external authentication is disabled, this log contains messages about local users successfully or failing logging in.	No	Yes
Feedback Logs	Records the web users reporting misclassified pages.	Yes	Yes
FTP Proxy Logs	Records error and warning messages related to the FTP Proxy.	No	No
FTP Server Logs	Records all files uploaded to and downloaded from theSecure Web Applianceusing FTP.	Yes	Yes
GUI Logs (Graphical User Interface)	Records history of page refreshes in the web interface. GUI logs also include information about SMTP transactions, for example information about scheduled reports emailed from the appliance.	Yes	Yes
Haystack Logs	Haystack logs record web transaction tracking data processing.	Yes	Yes
HTTPS Logs	Records Web Proxy messages specific to the HTTPS Proxy (when the HTTPS Proxy is enabled).	No	No
ISE Server Logs	Records ISE server(s) connection and operational information.	Yes	Yes
License Module Logs	Records messages related to the Web Proxy’s license and feature key handling system.	No	No

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
Logging Framework Logs	Records messages related to the Web Proxy's logging system.	No	No
Logging Logs	Records errors related to log management.	Yes	Yes
McAfee Integration Framework Logs	Records messages related to communication between the Web Proxy and the McAfee scanning engine.	No	No
McAfee Logs	Records the status of anti-malware scanning activity from the McAfee scanning engine.	Yes	Yes
Memory Manager Logs	Records Web Proxy messages related to managing all memory including the in-memory cache for the Web Proxy process.	No	No
Miscellaneous Proxy Modules Logs	Records Web Proxy messages that are mostly used by developers or customer support.	No	No
AnyConnect Secure Mobility Daemon Logs	Records the interaction between theSecure Web Applianceand the AnyConnect client, including the status check.	Yes	Yes
NTP Logs (Network Time Protocol)	Records changes to the system time made by the Network Time Protocol.	Yes	Yes
PAC File Hosting Daemon Logs	Records proxy auto-config (PAC) file usage by clients.	Yes	Yes
Proxy Bypass Logs	Records transactions that bypass the Web Proxy.	No	Yes
Reporting Logs	Records a history of report generation.	Yes	Yes
Reporting Query Logs	Records errors related to report generation.	Yes	Yes
Request Debug Logs	Records very detailed debug information on a specific HTTP	No	No

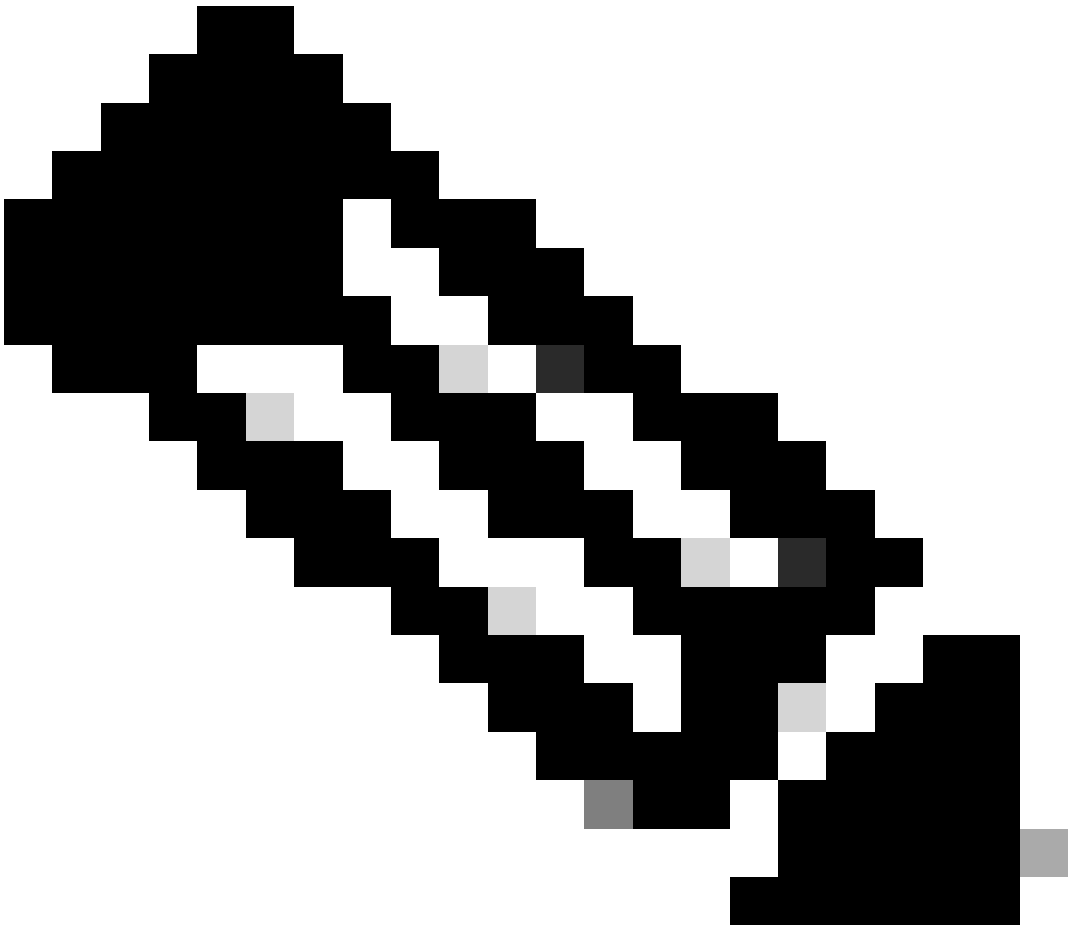
Log File Type	Description	Supports Syslog Push?	Enabled by Default?
	transaction from all Web Proxy module log types. It is advisable to create this log subscription to troubleshoot a proxy issue with a particular transaction without creating all other proxy log subscriptions. Note:You can create this log subscription in the CLI only.		
Auth Logs	Records messages related to the Access Control feature.	Yes	Yes
SHD Logs (System Health Daemon)	Records a history of the health of system services and a history of unexpected daemon restarts.	Yes	Yes
SNMP Logs	Records debug messages related to the SNMP network management engine.	Yes	Yes
SNMP Module Logs	Records Web Proxy messages related to interacting with the SNMP monitoring system.	No	No
Sophos Integration Framework Logs	Records messages related to communication between the Web Proxy and the Sophos scanning engine.	No	No
Sophos Logs	Records the status of anti-malware scanning activity from the Sophos scanning engine.	Yes	Yes
Status Logs	Records information related to the system, such as feature key downloads.	Yes	Yes
System Logs	Records DNS, error, and commit activity.	Yes	Yes
Traffic Monitor Error Logs	Records L4TM interface and capture errors.	Yes	Yes
Traffic Monitor Logs	Records sites added to the L4TM block and allow lists.	No	Yes
UDS Logs (User Discovery	Records data about how the Web Proxy discovers the user name without doing actual authentication. It includes information about interacting with the Cisco adaptive	Yes	Yes

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
Service)	security appliance for the Secure Mobility as well as integrating with the Novell eDirectory server for transparent user identification.		
Updater Logs	Records a history of WBRS and other updates.	Yes	Yes
W3C Logs	Records Web Proxy client history in a W3C compliant format. For more information.	Yes	No
WBNP Logs (SensorBase Network Participation)	Records a history of Cisco SensorBase Network participation uploads to the SensorBase network.	No	Yes
WBRS Framework Logs (Web Reputation Score)	Records messages related to communication between the Web Proxy and the Web Reputation Filters.	No	No
WCCP Module Logs	Records Web Proxy messages related to implementing WCCP.	No	No
Webcat Integration Framework Logs	Records messages related to communication between the Web Proxy and the URL filtering engine associated with Cisco Web Usage Controls.	No	No
Webroot Integration Framework Logs	Records messages related to communication between the Web Proxy and the Webroot scanning engine.	No	No
Webroot Logs	Records the status of anti-malware scanning activity from the Webroot scanning engine.	Yes	Yes
Welcome Page Acknowledgement Logs	Records a history of web clients who click the Accept button on the end-user acknowledgement page.	Yes	Yes

View Logs

By default, the logs are stored locally in the SWA, you can download the locally stored log files via GUI or view the logs from CLI.

Download Log Files via GUI



> **Note**: The FTP must be enabled on the appliance. To enable FTP please refer to Enable FTP on Secure Web Appliance in this article.

You can download the log files from GUI:

Step 1. Log in to GUI

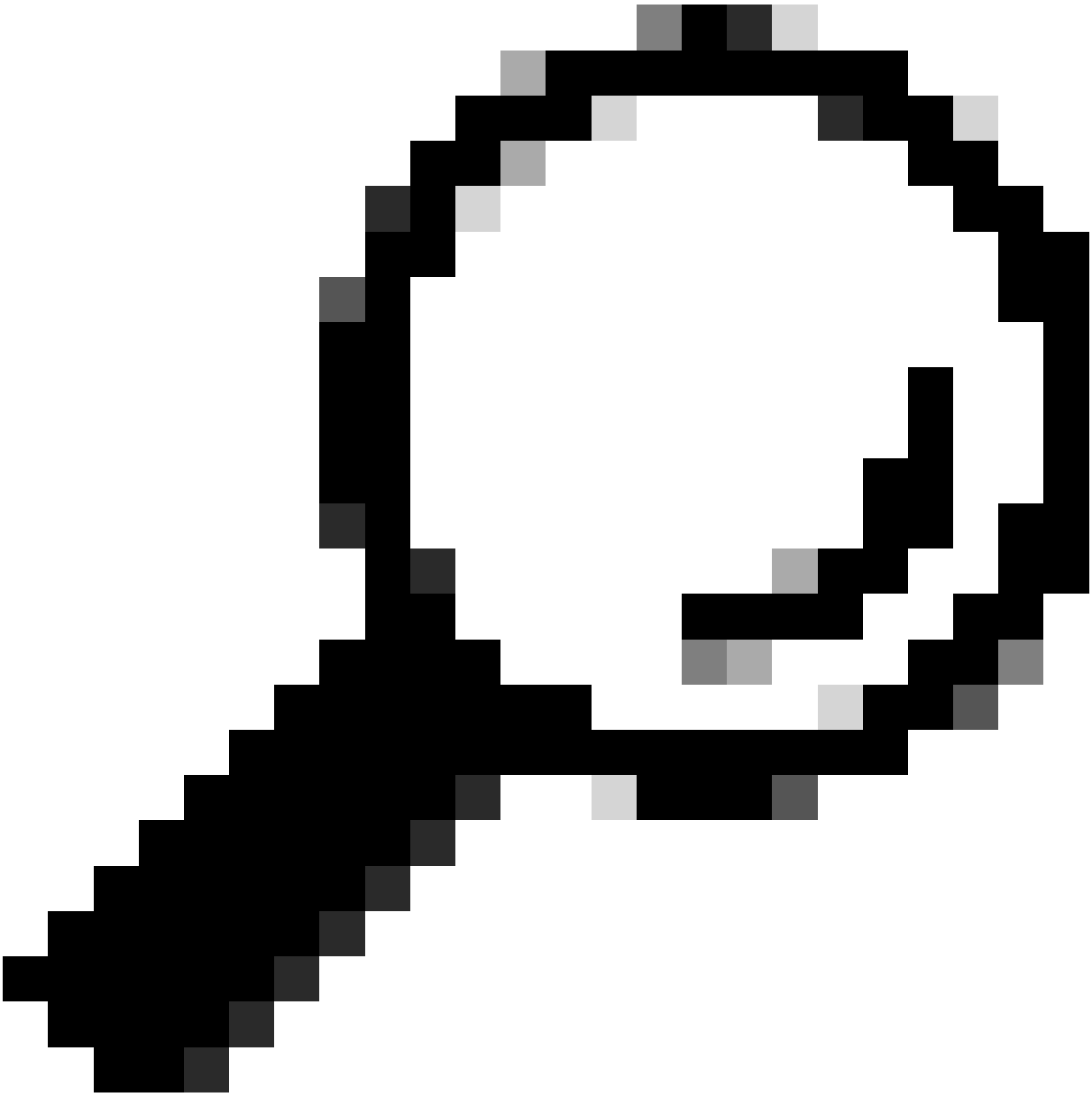
Step 2. Navigate to System Administration

Step 3. Choose Log Subscriptions

Step 4. Click the name of the log subscription in the Log Files column of the list of log subscriptions.

Step 5. When prompted, enter the administers username and password for accessing the appliance.

Step 6. When logged in, click one of the log files to view it in your browser or to save it to disk.



Tip: Refresh the browser for updated results.

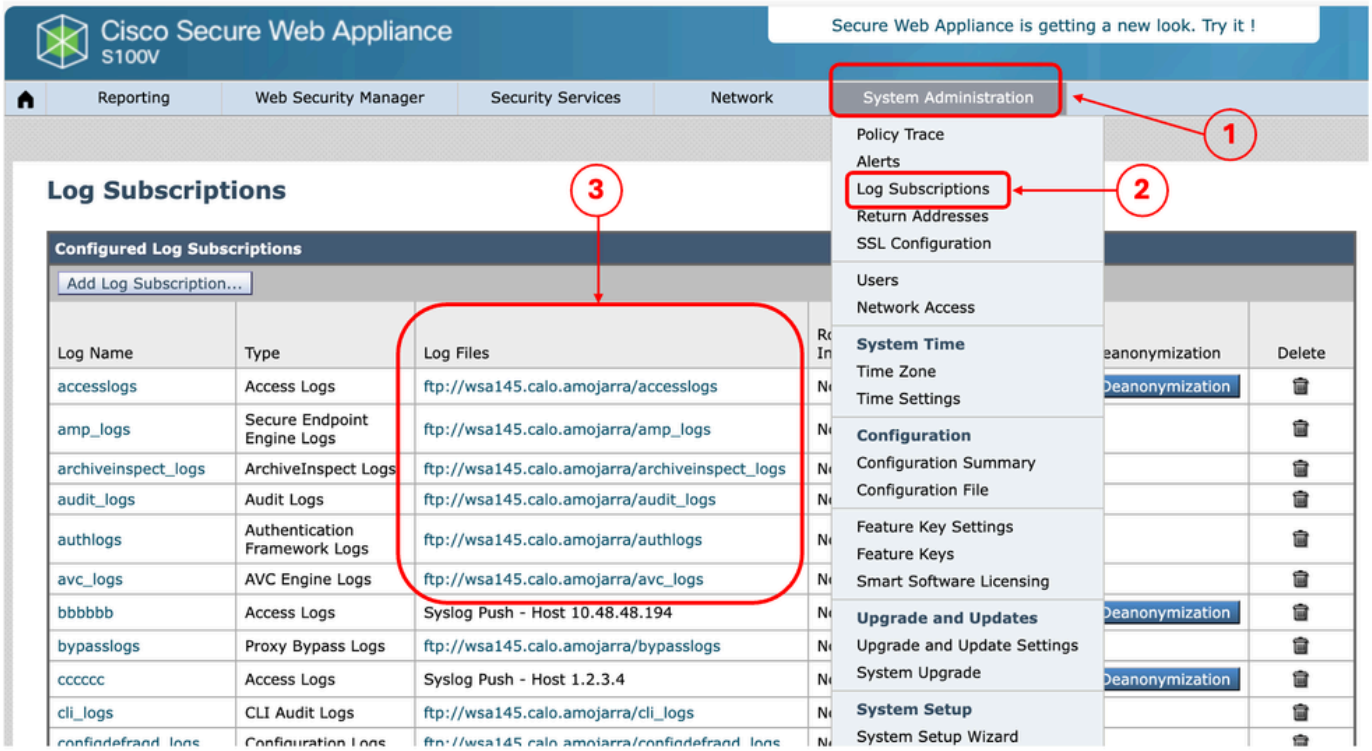
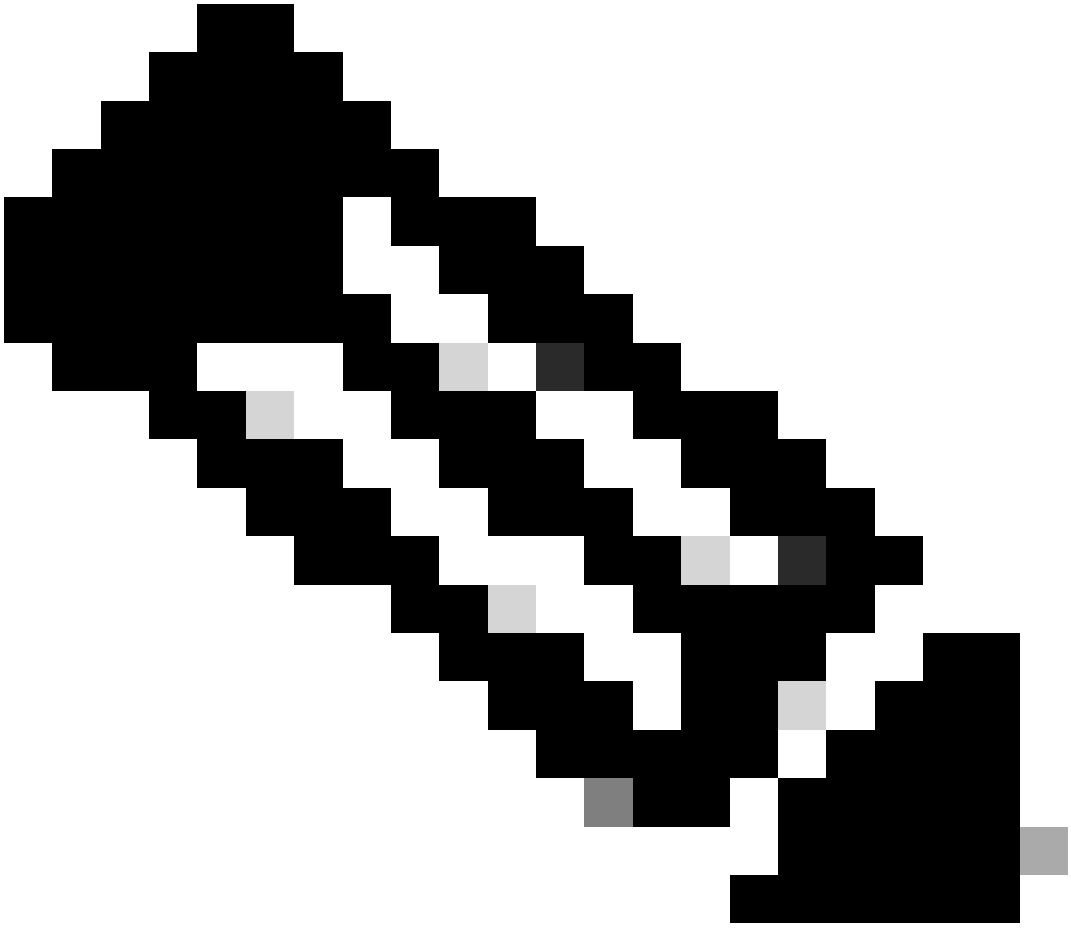


Image - Downlaod Log Files



Note: If a log subscription is compressed, download, decompress, and then open it.

View Logs From CLI

You can view the Logs from CLI. in this case, you can have access to live logs or filter for a keyword in the logs.

Step 1. Connect to CLI

Step 2. Type **grep** and press enter.

Step 3. Enter the number of the log you want to view

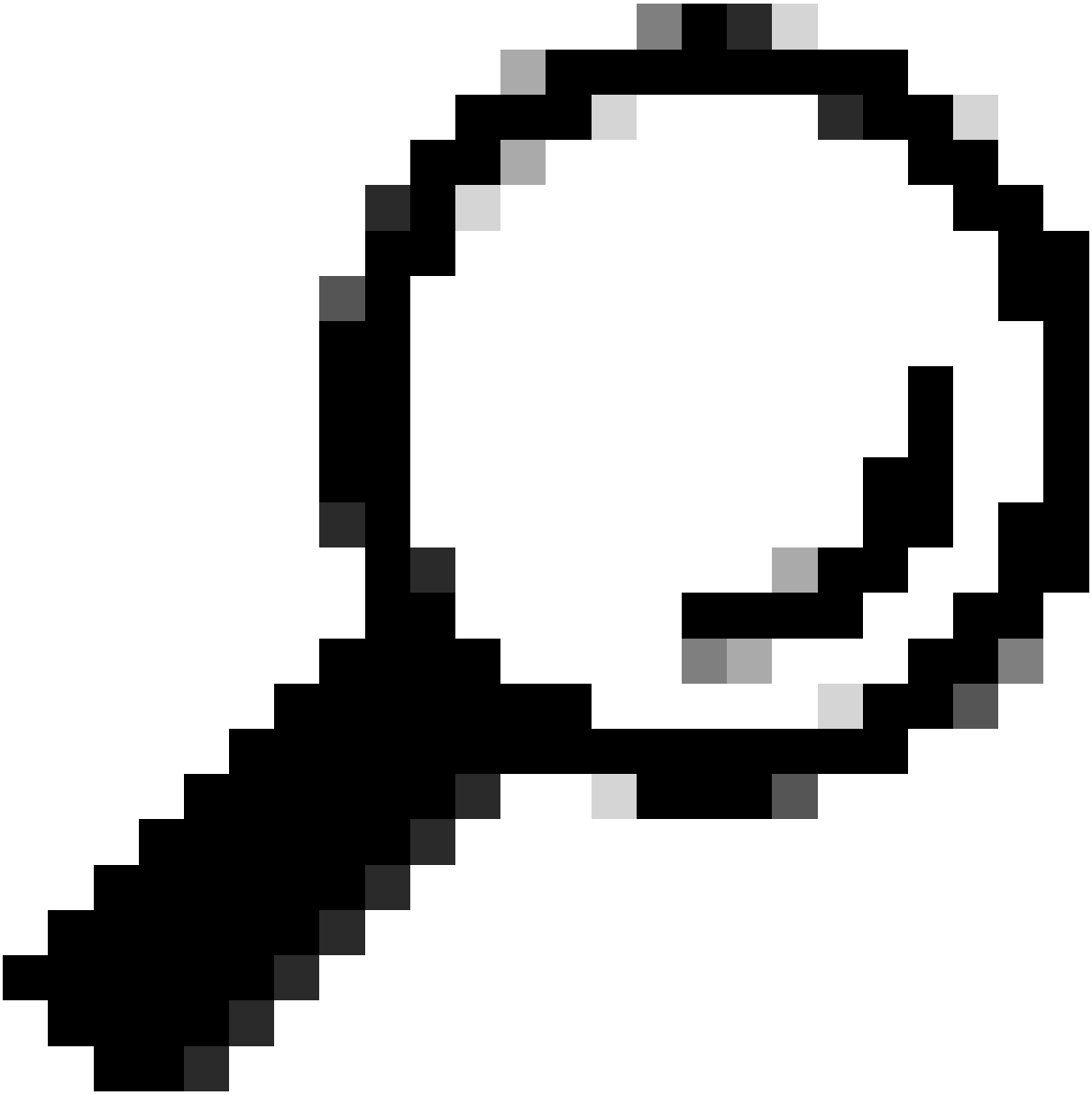
Step 4. (Optional) you can filter the output by defining a Regular Expression or a word, else press Enter

Step 5. If you need the search for the keyword entered in Step 4, to be case insensitive, press enter in "**Do you want this search to be case insensitive? [Y]>**" else type "N" and press Enter.

Step 6. If you need to exempt your keyword from search, type "Y" in "**Do you want to search for non-matching lines? [N]>**" else press Enter.

Step 7. If you need to view live logs, type "Y" in "**Do you want to tail the logs? [N]**>", else press Enter.

Step 8. If you want to paginate the logs to view them page by page type "Y" in "**Do you want to paginate the output? [N]**>" , else press Enter.



Tip: If you choose to paginate, you can exit the logs by pressing "**q**"

Here is a sample output shows all the lines which has "Warning" in them:

```
SWA_CLI> grep

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "Secure Endpoint Engine Logs" Retrieval: FTP Poll
3. "archiveinspect_logs" Type: "ArchiveInspect Logs" Retrieval: FTP Poll
4. "audit_logs" Type: "Audit Logs" Retrieval: FTP Poll
```

```
5. "authlogs" Type: "Authentication Framework Logs" Retrieval: FTP Poll
6. "avc_logs" Type: "AVC Engine Logs" Retrieval: FTP Poll
7. "bypasslogs" Type: "Proxy Bypass Logs" Retrieval: FTP Poll
8. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
...
45. "upgrade_logs" Type: "Upgrade Logs" Retrieval: FTP Poll
46. "wbnp_logs" Type: "WBNP Logs" Retrieval: FTP Poll
47. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
48. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
49. "webtapd_logs" Type: "Webtapd Logs" Retrieval: FTP Poll
50. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 40

Enter the regular expression to grep.
[]> Warning

Do you want this search to be case insensitive? [Y]>

Do you want to search for non-matching lines? [N]>

Do you want to tail the logs? [N]>

Do you want to paginate the output? [N]>
```

Enable FTP on Secure Web Appliance

By default FTP is not enabled on the SWA. To enable FTP:

Step 1. Log in to GUI

Step 2. Navigate to **Network**

Step 3. Choose **Interfaces**

Step 4. Click **Edit Settings**.

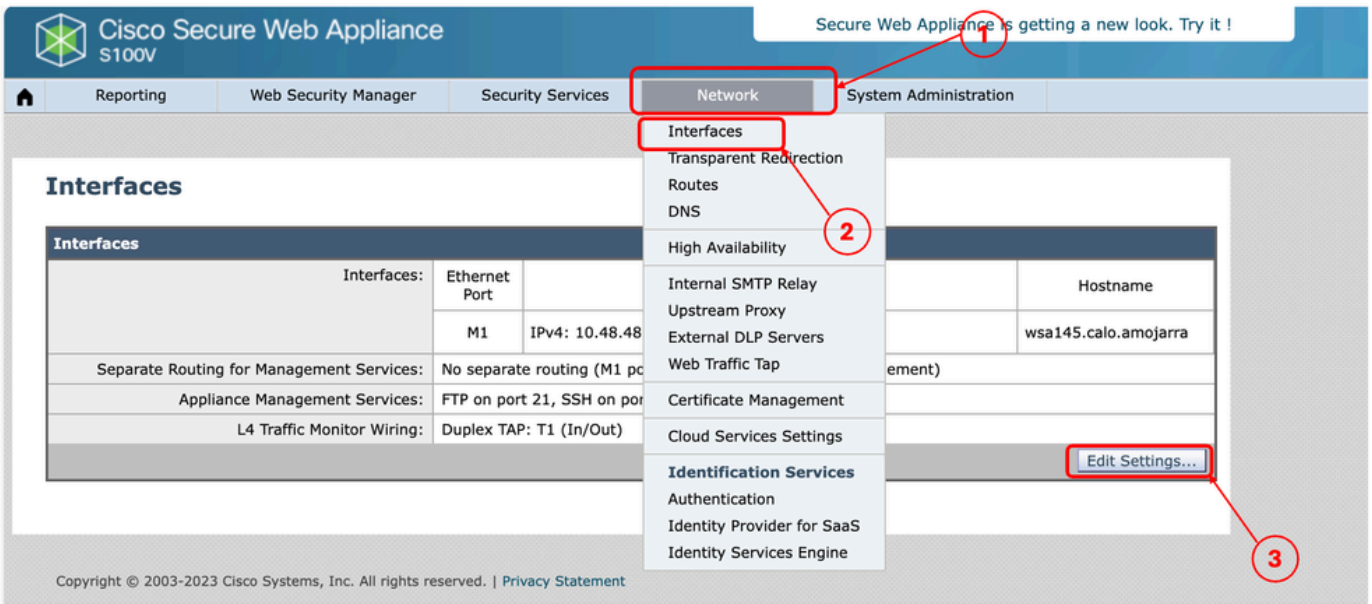


Image - Enable FTP on SWA

Step 5. Select the check box for FTP

Step 6. Provide the TCP Port number for FTP (Default FTP port is 21)

Step 7. Submit and **Commit** changes

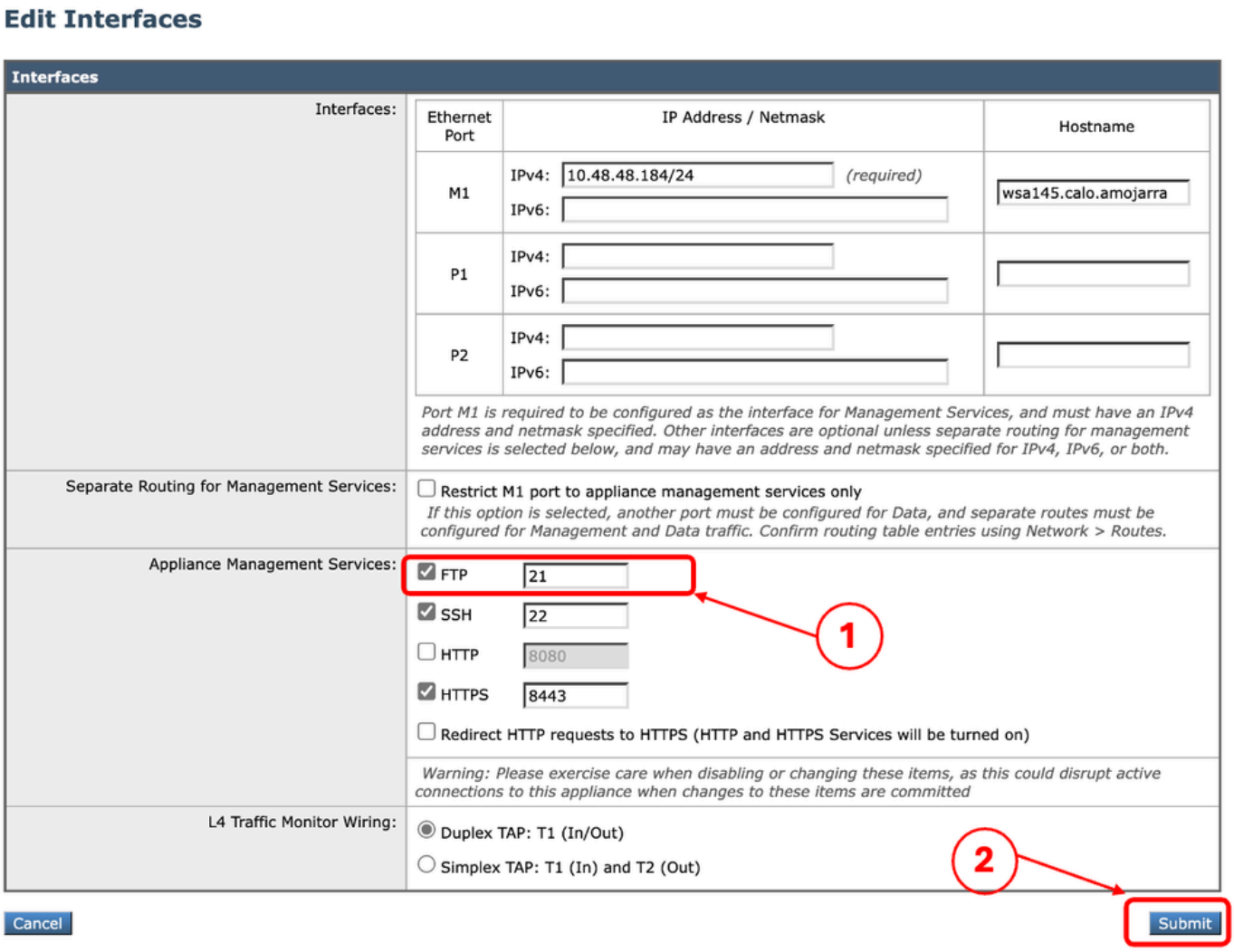


Image - Configure FTP Parameter in SWA

Related Information

- User Guide for AsyncOS 15.0 for Cisco Secure Web Appliance - LD (Limited Deployment) - Troubleshooti...
- Configure SCP Push Logs in Secure Web Appliance with Microsoft Server - Cisco