# **Configure FMC to Send Audit Logs to a Syslog Server**

# Contents

Introduction Prerequisites Requirements Components Used Background Information Configure Step 1. Enabled Audit Logs to Syslog Step 2. Configure Syslog Information Verify Troubleshoot Related Information

# Introduction

This document describes how to configure Secure Firewall Management Center Audit Logs to be sent to a Syslog server.

# Prerequisites

#### Requirements

Cisco recommends that you have knowledge of these topics:

- Basic Usability of the Cisco Firewall Management Center (FMC)
- Understanding of Syslog protocol

#### **Components Used**

The information in this document is based on these software and hardware versions:

- Cisco Firewall Management Center Virtual v7.4.0
- Third Party Syslog Server

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.

# **Background Information**

The Secure Firewall Management Center records user activity in read-only audit logs. Starting Firepower version 7.4.0, you can stream configuration changes as part of audit log data to syslog by specifying the configuration data format and the hosts. Streaming audit logs to an external server allows you to conserve

space on the management center, as well, it is useful when you need to provide audit trail of configuration changes.

In case of high availability, only the active management center sends the configuration changes syslog to the external syslog servers. The log file is synchronized between the HA pairs so that during a failover or switchover, the new active management center would resume sending the change logs. In case the HA pair is working in split-brain mode, both management centers in the pair sends the config change syslog to the external servers.

# Configure

#### Step 1. Enabled Audit Logs to Syslog

To enable so FMC sends audit logs to a syslog server, navigate to **System > Configuration > Audit Log > Send Audit Log to Syslog > Enabled.** 

This image shows how to enable the Send Audit Log to Syslog feature:



The FMC can stream audit log data to a maximum of five syslog servers.

#### **Step 2. Configure Syslog Information**

After the service have been enabled, you can configure the syslog information. To configure the syslog information, navigate to **System > Configuration > Audit Log.** 

Depending on your requirements, select Send Configuration Changes, Hosts, Facility, Severity

This image shows the parameters to configure Syslog Server for Audit Logs:

Firewall Management Center System / Configuration	Overview A	Analysis	Policies	Devices	Objects	Integration
Access List						
Access Control Preferences						
Audit Log	Send Audit Log to	Syslog	Enabled		•	
Audit Log Certificate	cond riddit Log to	cyclog [	Lindbied	0	<u> </u>	
Change Management	Send Configuration Cl	hanges	Send as JSON	1	•	
Change Reconciliation	Hosts (U	lp to 5)	172.16.10.11			
DNS Cache		Facility	USER		•	
Dashboard	S	Severity	INFO		•	
Database	Tag (or	otional)				
Email Notification	Tag (0)					
External Database Access	Send Audit Log to HTTP	Server	Disabled		•	
HTTPS Certificate	URL to Pos	st Audit				
Information			ſ	Test Syslog	Server	
Intrusion Policy Preferences						

# Verify

To verify if the parameters are correctly configured, select **System > Configuration > Audit Log > Test Syslog Server.** 

This image shows a successful Syslog Server Test:

Firewall Management Center System / Configuration	Overview	Analysis	Policies	Devices	Objects	Integration
Access List						
Access Control Preferences						
Audit Log	Send Audit Loa	to Syslog	Enabled		•	
Audit Log Certificate		0				
Change Management	Send Configuration	Changes	Send as JSO	N	•	
Change Reconciliation	Hosts	(Up to 5)	172.16.10.11			
DNS Cache		Facility	USER		•	
Dashboard		Severity	INFO		•	
Database	Tag	(optional)	[		1	
Email Notification		TDO	Disabled			
External Database Access	send Audit Log to HI	IP Server	Disabled		•	
HTTPS Certificate	URL to F	Post Audit				
Information		Syslog	server has beer	reached.	Test Syslog	Server
Intrusion Policy Preferences	27		1/2			

Another way to verify that syslog is working, check the syslog interface to confirm the audit logs are being received.

This image shows some examples of the audit logs received by Syslog Server:

Date	Isne	Priority	Hostname	Message
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [neta sequenceId="1933"][19129] situnneld:stream. File [INFO] AFTER FOUND COMPL TASK ON SRC.: File copy 100 % completed, 40 bytes of file copied out of 40
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 1:5021 firepower 5F4K5[10117] [insta respanced="1327"[13123] itumedit stream, file [INF0] AFTER FOUND COMPL TASK ON SRC: cur_read=40, cur_mite=40, total_byter=40, thream_id_utc=0, thream_id_dest=204, terc_it_end_est=204, terc_it_end_
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-INS[10417]: [meta sequenceld="1931"][19129] sftunneld: stream_file [INF0] FILE /var/sf/sidns_download/7cb124a4-4c0e-11ee b245-a2990cdac7a0
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 Eirepower SF-INS[10417]: [meta sequenceId="1930"][19129] sflueneId:stream_life [INFO] ADDED INIT confirmation to be SRC:: File copy 0 % completed, 0 bytes of file copied out of 0
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50 21 fierpower 57 WS[10417] [nets requenced="1937"][1173] situanedi stream_ide [INFO] ADDED INIT confination to be SRC: cur_read=0, cur_wite=0, total_bytes=0, stream_id_stc=0, stream_id_dest-204, ste_id_stc=0, stream_id_stc=0, stream_is
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="1928"][19129] sftunneld:stream_file [INFO] Adding SRC Task on Request, key: 0:204
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 Sirepower SF-IMS[10417]: [meta sequenceld="1927"][19129] situmend: stream_life [INFO] Creating task on SRC for incoming task.: File copy 0 % completed, 0 bytes of file copied out of 0
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50 21 finepower 57:W5[10417] [intext sequenced="1925"[19123] intermedia thream_lide [INFO] Creating task on SRC for incoming task: cur_read=0, cur_write=0, total_bytes=0, stream_id_set=204, seq_id_urc=0, req_id_det=0 atale=5tated_trated2023 09 28:17:50 21 UIC, supresse 2023 09 28:200 21 UIC
03-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="1925"][19129] sthumeld:stream_life [INFO] SRC TASK for KEY 0:204 was not found
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 Sirepower SF-INS[10417]: [meta sequenceld="1924"][19129] strunneld:stream_life [INFO] ELASTIC/FSTREAM request DoNotBlockList validation passed for: /var/st/sidns_download/7cb124a4-4c0e-11ee-b245-a2990cdac7a0
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 20 21:50:21 Sirepower SF-IMS(9765); [meta sequenceld="1923"]run_hm(19200]; Sending message at /usz/local/st//Bib/pet//5.32.1/SF/HealthMon.pm line 579.
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 20 21:50:20 firepower SF-INS[10417]: [meta sequenceld="1922"][19129] situmedd:titeam_file [INFO] AFTER FOUND COMPL TASK ON SRC:: File copy 100 % completed, 42 bytes of file copied out of 42
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50 20 finepower 57 HX5[10417]; [and sequenceld-119217]]19123] informedia stream, file [INF0] AFTER FOUND COMPL TASK ON SRC: cur_read-42, cur_mite=42, total_bytes=42, stream_id_stre=0, stream_id_stre=10, stream_id
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 20 21:50:20 firepower SF-IMS(10417): [meta sequenceld="1920"][19129] situnneld: stream_file [INFO] FILE /var/sf/sidns_download/7cb2ta4a-4c0e-11ee-b245-a2990cdac7a0
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta requenceId="1919"][19123] sthunneld: stream_file [INFO] ADDED INIT confirmation to be SRC:: File copy 0 % completed, 0 bytes of file copied out of 0
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50 20 (incipones 57:MS[10417]; [incl srequenceld="1918"][19123] situanedi stream_ide [INFO] ADDED INIT confirmation to be SRC: cur_read=0, cur_mite=0, total_bytes=0, stream_id_strc=0, stream_id_dest=282, steid_stre=0, stream_id_stre=282, steid_stre=28, steam_id_stre=28, steam_id_stre
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]; [meta requenceId="1917"][19129] sltunneld: stream_life [INFO] Adding SRC Task on Request, key: 0:202
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-INS[10417]: [meta sequenceld="1916"][19129] situnneld:stream_life [INFO] Creating task on SRC for incoming task:: File copy 0 % completed, 0 bytes of file copied out of 0
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50 20 (incposer 5F:MS[10417] [and sequenceld-"1915"][19123] sthumedi stream_life [INF0] Creating task on SRC for incoming task: cur_read-0, cur_write-0, total_bytes-0, stream_id_est-2022, seq_id_strc-0, stream_id_est-2022, ses_id_strc-0, stream_id_est-2022, seq_id_strc-0, stream_id_est-2022, seq_id_strc-0, stream_id_est-2022, seq_id_strc-0, stream_id_est-2022, seq_id_strc-0, stream_id_est-2022, stream_id_straam_id_stream_id_strd-0, stream_id_straam_id_straa
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS(10417): [meta sequence(d="1914")[19129] situnneld:stream_life (INFO) SRC TASK for KEY 0:202 was not found
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [neta sequenceId="1913"][19129] sltunneld: stream_life [INFO] ELASTIC/FSTREAM request DoNotBlockList validation passed for: /var/sl/sidns_download/?cb21a4a-4c0e-11ee-b245-a2990cdac?a0
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[9765] [meta sequenceId+"1912"]Sexhat[10441]; 169593782010.06(1.82)4.31)0.94(7814.92)4815.22)0.00(0.004,79)1.60(142.39)00(0.00)0000.02)0.06(0)25510.00(0.000)000.02)0.04(0)16(2.39)0.00.000000.02)0.04(0)16(2.39)0.0000000.02)0.04(0)16(2.39)0.00000000.02)0.04(0)16(2.39)0.0000000000000000000000000000000000
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 filepower SF-IMS[9765]: [meta sequenceId="1911"]Evenids[10442]: 16959378201211221175(0)60
09-28-2023	21:50:07	Local7.Debug	172.16.10.2	Sep 28 21:50:12 firepower SF-IMS[9765]: [meta sequenceId="1910"]sshd_monitor[9974]: sshd is running with 2046 4005 3992 2046
09-28-2023	21:50:05	Local7.Debug	172.16.10.2	Sep 28 21:50:10 firepower SF-IMS[9765]; [meta sequenceld="1909"]Seshat[10441]; 1695937810[1.0295.73]32:5011.92110021.906635:9010.0000.0011.71[1.60367.20]15278]0.0000.000000.0380.050025500.0000.0000001.5113.512.10.0
09-28-2023	21:50:05	Local7.Debug	172.16.10.2	Sep 28 21:50:10 firepower SF-IMS[9765]; [meta sequenceId="1908"]Eventds[10442]; 1695937810[2]122[1175]00
09-28-2023	21:49:58	User.Info	172.16.10.2	Sep 28 21:50:03 firepower: platformSettingEdit.cgi: admin@10.152.201.95, System > Configuration > /platinum/platformSettingEdit.cgi?type=AuditLog, Page View
09-28-2023	21:49.57	User.Info	172.16.10.2	Sep 28 21:50:02 firepower: ActionQueueScrape.pt. csm_processes@Default User IP, Login, Login Success
09-28-2023	21:49:57	Local7.Debug	172.16.10.2	Sep 28 21:50:02 firepower SF-IMS[9765]: [meta sequenceId="1907"]sshd_monitor[9974]: sshd is running with 2046 4005 3992 2046
09-28-2023	21:49.57	Local7.Debug	172.16.10.2	Sep 28 21:50:02 firepower store_allowlist_history: [meta sequenceld="1906"]store_allowlist_history finished successfully.
09-28-2023	21:49:56	Local7.Debug	172.16.10.2	Sep 28 21:50:01 firepower store_allowfist_history: [meta sequenceId="1905"]Invoking '/uur/local/sf/bin/store_allowfist_history:pf.
09-28-2023	21:49:56	Local7.Debug	172.16.10.2	Sep 28 21:50:01 lirepower CR0ND[6894]; [meta sequenceld="1904"](root) CMD (/usr/hibexec/sa/sa1 1 1)
09-28-2023	21:49:56	Local7.Debug	172.16.10.2	Sep 28 21:50:01 [irepower CR0ND[6893]; [meta sequenceld="1903"[ireoi] CMD [ //usr/local/s1/bin/run parts-cron /etc/cron.5min]
09-28-2023	21:49.56	User.Info	172.16.10.2	Sep 28 21:50:01 firepower: ActionQueueScrape.pt: admin@localhost, Task Queue, Policy Deployment to FTD - SUCCESS
09-28-2023	21:49.55	Local7.Debug	172.16.10.2	Sep 28 21:50:00 firepower SF-IMS[9765]; [meta sequenceld="1902"]Sexhal[10441]; 169593780010.592:46[11.31]0.867731.67[5066.81]0.0010.00916010.0010.0010.000]000.0010.010.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.00000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.0000000.0310.04002550.0000.000000000000000000000000
09-28-2023	21:49:55	Local7.Debug	172.16.10.2	Sep 28 21:50:00 firepower SF-IMS(9765); [meta sequenceld="1901")Eventds[10442]; 16353378000(2)12211175000
09.20.2023	21-49-52	Here Info	172 16 10 2	San 20 21-49-57 European and cast coi: admin@10.152.201.95. Sustem \ Configuration \ Configura

Here are some examples of the configuration changes you can received in your syslog server:

2023-09-29 16:12:18 localhost 172.16.10.2 Sep 29 16:12:23 firepower: [FMC-AUDIT] mojo\_server.pl: admin@ 2023-09-29 16:12:20 localhost 172.16.10.2 Sep 29 16:12:25 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1. 2023-09-29 16:12:23 localhost 172.16.10.2 Sep 29 16:12:28 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1. 2023-09-29 16:13:39 localhost 172.16.10.2 Sep 29 16:13:44 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1. 2023-09-29 16:14:32 localhost 172.16.10.2 Sep 29 16:14:37 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1. 2023-09-29 16:14:32 localhost 172.16.10.2 Sep 29 16:14:37 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1. 2023-09-29 16:14:54 localhost 172.16.10.2 Sep 29 16:14:59 firepower: [FMC-AUDIT] ActionQueueScrape.pl: 2023-09-29 16:14:55 localhost 172.16.10.2 Sep 29 16:15:00 firepower: [FMC-AUDIT] ActionQueueScrape.pl:

#### Troubleshoot

After the configuration has been applied, make sure the FMC can communicate with syslog server.

The system uses ICMP/ARP and TCP SYN packets to verify that the syslog server is reachable. Then, the system by default uses port 514/UDP to stream audit logs and TCP port 1470 if you secure the channel.

To configure a packet capture on FMC, apply these commands:

• tcpdump. This command captures the traffic on the network

```
> expert
admin@firepower:~$ sudo su
Password:
root@firepower:/Volume/home/admin# tcpdump -i eth0 host 172.16.10.11 and port 514
```

Additionally, to test ICMP reachability, apply this command:

• **ping.** This command helps to confirm if a device is reachable or not and to know the latency of the connection.

```
> expert
admin@firepower:~$ sudo su
Password:
root@firepower:/Volume/home/admin#ping 172.16.10.11
PING 172.16.10.11 (172.16.10.11) 56(84) bytes of data.
64 bytes from 172.16.10.11: icmp_seq=1 ttl=128 time=3.07 ms
64 bytes from 172.16.10.11: icmp_seq=2 ttl=128 time=2.06 ms
64 bytes from 172.16.10.11: icmp_seq=3 ttl=128 time=2.04 ms
64 bytes from 172.16.10.11: icmp_seq=4 ttl=128 time=0.632 ms
```

#### **Related Information**

- <u>Technical Support & Documentation Cisco Systems</u>
- <u>Cisco Secure Firewall Management Center Administration Guide</u>