

Configure and Troubleshoot NTP Settings on Firepower Appliances

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[NTP on FPR 41xx/9300](#)

[NTP on FPR 1xxx/2100](#)

[Configure the NTP on FPR 1xxx/2100/41xx/9300 Appliances](#)

[Verify](#)

[Verify the NTP Synchronization on FPR41xx/9300 Appliances](#)

[Verify the NTP Configuration on FPR41xx/9300 Appliances](#)

[Verify the NTP Synchronization Between MIO and Logical Device \(Blade\) on FPR41xx/9300 Appliances](#)

[Verify the NTP Configuration on FPR1xxx/2100 Appliances](#)

[Troubleshoot Common Issues](#)

[1. FXOS not Able to Resolve the NTP Server Hostname](#)

[2. Connectivity Issues Between FXOS - NTP Server on UDP Port 123](#)

[3. Intermittent Connectivity Issues Between FXOS and NTP Server](#)

[Related Defects](#)

[Related Information](#)

Introduction

This document describes how to configure, verify and troubleshoot Network Time Protocol (NTP) on Firepower FXOS Appliances.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

- FPR4140 that runs FXOS 2.3(1.130) and 2.8(1.105)

- FPR2110 that runs ASA platform mode
- FPR1140 that runs ASA appliance mode

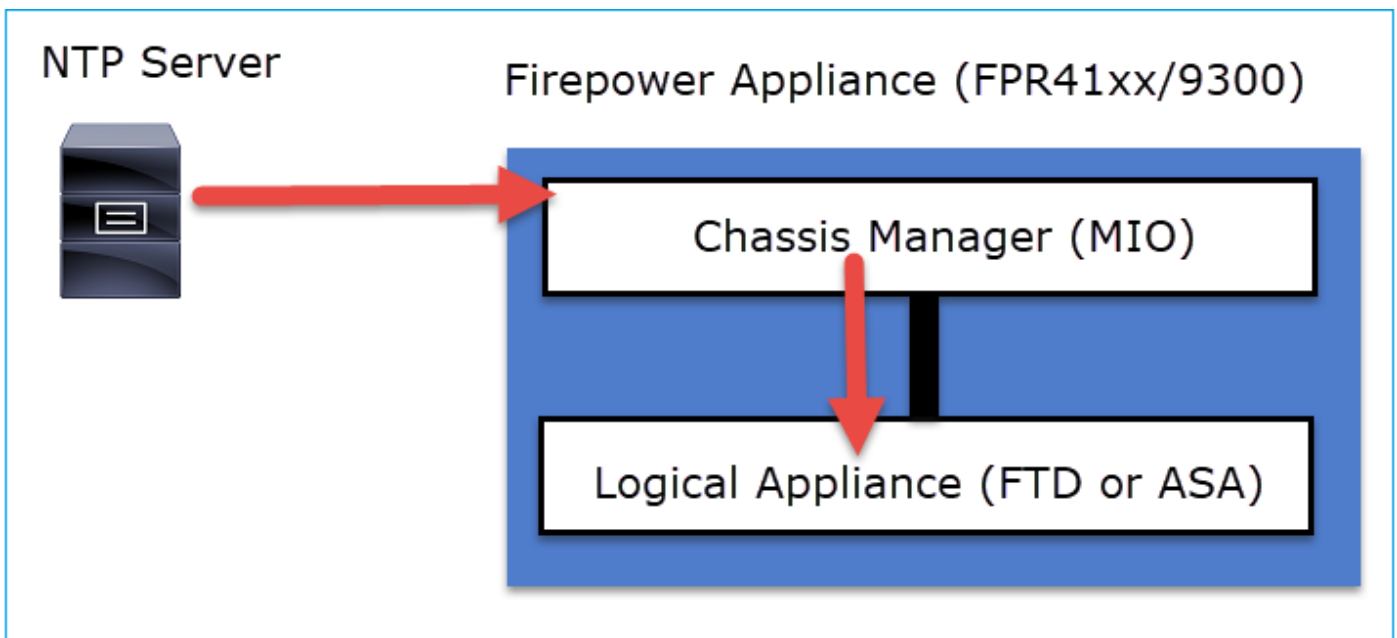
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

On Firepower, the NTP operation depends on the platform.

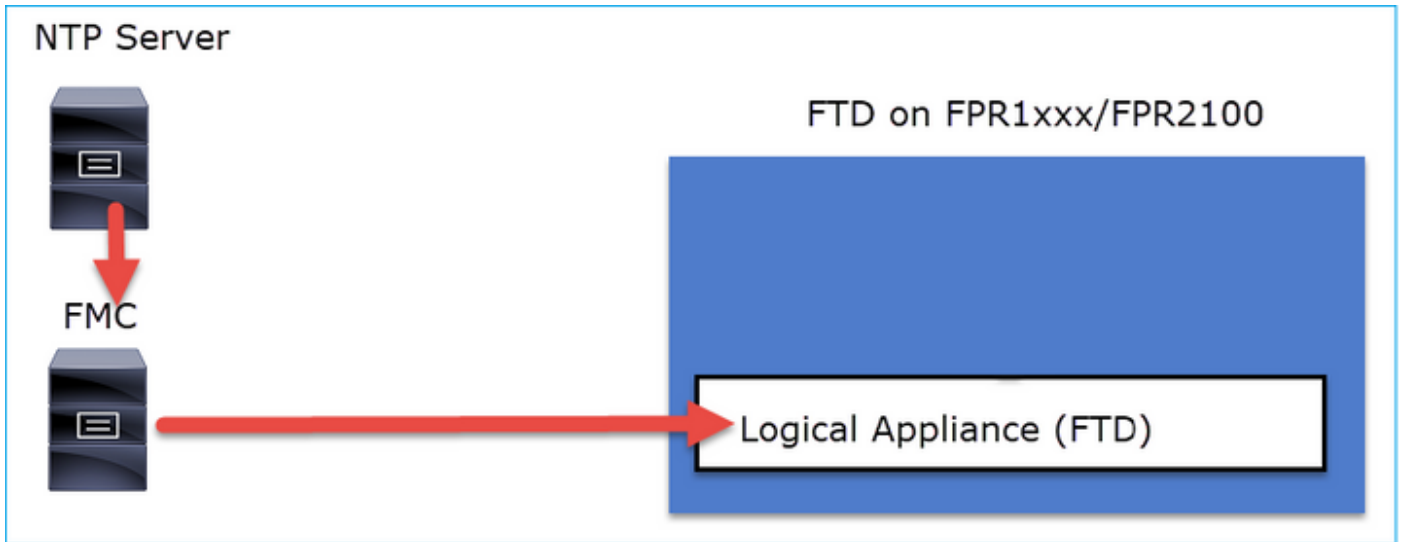
FPR41xx/FPR9300

The ASA or FTD time is taken from the chassis Firepower Chassis Manager (FCM) Management Input/Output (MIO). MIO is the supervisor of the Firepower chassis.



FPR1xxx/FPR2100

On FTD, the time is taken from the FMC:



For this deployment, check these documents:

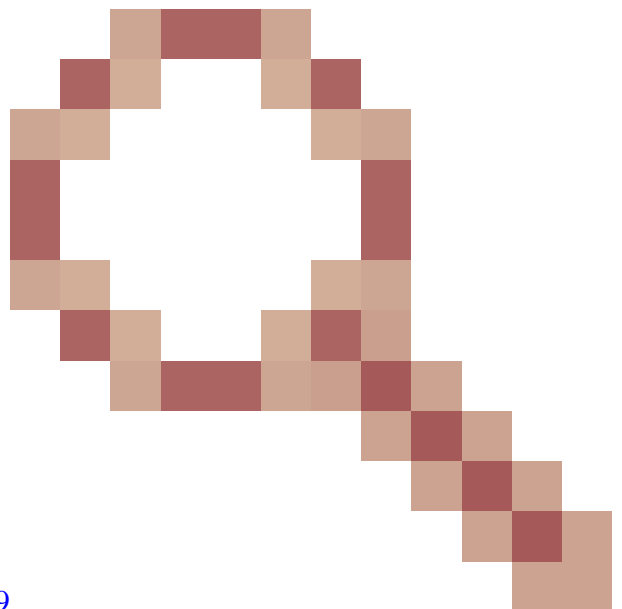
- [Configure NTP Time Synchronization for Threat Defense](#)
- [Troubleshoot Issues with Network Time Protocol \(NTP\) on Firepower Systems](#)

Additional Information

NTP is used for time synchronization. NTP uses as a transport the UDP port number 123.

Supported NTP versions on FXOS:

- FXOS 10.2.2.7 and later use NTP version 3
- Older FXOS than 10.2.2.7 use NTP version 2



Supported version changed due to Cisco bug ID [CSCve58269](#)

- NTP: change v2 to v3



Note: NTP version 4 is not officially supported. NTP version 4 is backwards compatible to NTP version 3.

Configure


NTP on FPR 41xx/9300

Key Points

- To configure NTP on a Firepower 41xx/9300 appliance, log in to FCM and navigate to the **Platform Settings** tab.
- The NTP on the logical devices (ASA or FTD) is synchronized with the MIO.
- Currently, there is no possibility to synchronize NTP on FTD with Firepower Management Center (FMC), even if you choose that option, NTP on FTD is synchronized with MIO. Thus, it is highly recommended that FMC and FCM use the same NTP server.
- The FMC is not a full-blown NTP server. It can just provide time settings to its managed devices through the sftunnel. Thus, it cannot be used as the NTP server for the Firepower 41xx/9300 chassis.
- Proper NTP configuration is required for a successful Smart License installation.

NTP on FPR 1xxx/2100

- To configure NTP on a Firepower 1xxx/2100 appliance, navigate to the **Platform Settings** tab from the Firepower Chassis Manager (FCM), Firepower for ASA in Platform mode.
- In case of an ASA in Platform mode, the NTP on the logical device is synchronized with the MIO.
- Configure the NTP settings on the logical application itself. The ASA in Appliance mode or in case of FTD on-box management from the Firepower Device Manager (FDM).
- In case the FTD is managed by FMC (off-box management), configure the NTP on the FMC.

 Note: On post-9.13(1) versions you can run the Firepower 1xxx/2100 for ASA in these modes: Appliance mode (the default) and Platform mode. Appliance mode allows you to configure all settings, that includes NTP, on the ASA. Only advanced troubleshoot commands are available from the FXOS CLI. On the other hand, in Platform mode, you must configure basic settings (including NTP) and hardware interface settings in chassis manager (FCM).

Configure the NTP on FPR 1xxx/2100/41xx/9300 Appliances

Step1. Log in into the Firepower Chassis Manager GUI with the Local user credentials and navigate to **Platform Settings > NTP**. Select the **Add** button:

Overview Interfaces Logical Devices Security Engine **Platform Settings** 1

NTP 2

SSH
SNMP
HTTPS
AAA
Syslog
DNS
FIPS and Common Criteria
Access List

Time Synchronization Current Time

Set Time Source

Set Time Manually

Date: 11/26/2017 (mm/dd/yyyy)

Time: 8 47 PM (hh:mm)

Get System Time

NTP Server Authentication: Enable

Use NTP Server

3

Add

NTP Server Server Sta Actions

Step 2. Specify the NTP server IP address or hostname (If you use a hostname for the NTP server, you must configure a DNS server).


Add NTP Server ? X

NTP Server * 172.16.38.66

Authentication Key

Authentication Value



Add Cancel


 Note: You can configure up to 4 NTP Servers

Verify

Verify the NTP Synchronization on FPR41xx/9300 Appliances

Monitor the Server Status.

Server Status	Actions
Synchronization in progress	 

Server Status	Actions
Synchronized	 

Server Status reference

- Not available: The default status shown immediately after the NTP server configuration.
- Unreachable/Invalid: Shown in these scenarios:
 - When the NTP server IP address or host name is unreachable by the NTP protocol.
 - When the NTP server IP address or host name is reachable, but the remote host is not an NTP server.
 - Other internal failures such as when the query fails to execute, exception thrown, undefined time sync status is encountered, and so on.
- Synchronization in progress: The server is reachable and supports the NTP protocol, the initial time converge is still going on and has not completed yet.
- Synchronized: The host is declared as the system sync peer and the time clock is in synchronization with it.
- Candidate: The host is the candidate (standby) peer. A candidate NTP server means it is a valid one and has successfully communicated with the Firepower appliance, but the module has been synchronized with another NTP server so it is the standby one. It can be elected as the next in-sync peer if the current one is deleted.
- Outlier: An NTP server that is discarded due to big difference (time offset and round-trip delay) compared to the rest of the NTP servers.

Verify the NTP Configuration on FPR41xx/9300 Appliances

Verify the NTP peer status:

```
FPR4100-8-A# connect fxos
FPR4100-8-A(fxos)# show ntp peer-status
Total peers : 4
* - selected for sync, + - peer mode(active),
- - peer mode(passive), = - polled in client mode
remote          local          st  poll  reach delay
-----
```

```

=172.16.38.66          10.62.148.196          1 1024          17  0.20996
*172.31.201.67        10.62.148.196          1 1024          377 0.03035
=172.16.38.65         10.62.148.196          1 1024          377 0.19914
=172.31.20.115        10.62.148.196          1 1024          377 0.02905

```

Verify the NTP server configuration and synchronization:

```

FPR4100-8-A# scope system
FPR4100-8-A /system # scope services
FPR4100-8-A /system/services # show ntp-server detail
NTP server hostname:
  Name: 172.16.38.65 Time Sync Status: Candidate
  NTP SHA-1 key id: 0
  Error Msg:

  Name: 172.16.38.66
  Time Sync Status: Time Sync In Progress
  NTP SHA-1 key id: 0
  Error Msg:

  Name: 172.31.20.115
  Time Sync Status: Candidate
  NTP SHA-1 key id: 0
  Error Msg:

  Name: 172.31.201.67
  Time Sync Status: Time Synchronized
  NTP SHA-1 key id: 0
  Error Msg:

```

Verify the NTP association:

```

FPR4100-8-A# connect module 1 console
Firepower-module1>show ntp association

```

```

      remote          refid          st t when poll reach  delay  offset  jitter
=====
*203.0.113.126  172.31.201.67  2 u  39  64  370  0.070  0.445  0.210

ind assid status  conf reach auth condition  last_event cnt
=====
  1 16696 961a  yes  yes  none  sys.peer  sys_peer  1

```

```

associd=16696 status=961a conf, reach, sel_sys.peer, 1 event, sys_peer,
srcadr=203.0.113.126, srcport=123, dstadr=203.0.113.1, dstport=123,
leap=00, stratum=2, precision=-21, rootdelay=29.053, rootdisp=70.496,
refid=172.31.201.67,
reftime=e24d4bd9.3b680f6d Fri, Apr 24 2020 11:28:25.232,
rec=e24d4d34.170bd724 Fri, Apr 24 2020 11:34:12.090, reach=370,
unreach=0, hmode=3, pmode=4, hpoll=6, ppoll=6, headway=0,
flash=20 pkt_stratum, keyid=0, offset=0.445, delay=0.070,
dispersion=2.152, jitter=0.210, xleave=0.017,

```

```
filtdelay= 0.08 0.11 0.08 0.10 0.07 0.08 0.09 0.07,
filtoffset= 0.17 0.18 0.29 0.29 0.45 0.45 0.69 0.69,
filtdisp= 0.00 0.03 0.99 1.02 2.03 2.06 3.03 3.06
```

```
associd=16696 status=961a conf, reach, sel_sys.peer, 1 event, sys_peer,
remote host: 203.0.113.126:123
local address: 203.0.113.1:123
time last received: 39
time until next send: 26
reachability change: 170025
packets sent: 5048
packets received: 5048
bad authentication: 0
bogus origin: 0
duplicate: 0
bad dispersion: 27
bad reference time: 0
```

Verify the NTP sysinfo:

```
FPR4100-8-A# connect module 1 console
Firepower-module1>show ntp sysinfo
associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
version="ntpd 4.2.8p11@1.3728-o Sat Dec 8 06:11:47 UTC 2018 (2)",
processor="x86_64", system="Linux/3.10.62-ltsi-WR10.0.0.29_standard",
leap=00, stratum=3, precision=-24, rootdelay=29.129, rootdisp=24.276,
refid=203.0.113.126,
reftime=e24dd3bf.170a6210 Fri, Apr 24 2020 21:08:15.090,
clock=e24dd437.59b86104 Fri, Apr 24 2020 21:10:15.350, peer=16696, tc=6,
mintc=3, offset=0.009911, frequency=7.499, sys_jitter=0.023550,
clk_jitter=0.004, clk_wander=0.001
```

```
associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
system peer: 203.0.113.126:123
system peer mode: client
leap indicator: 00
stratum: 3
log2 precision: -24
root delay: 29.129
root dispersion: 24.276
reference ID: 203.0.113.126
reference time: e24dd3bf.170a6210 Fri, Apr 24 2020 21:08:15.090
system jitter: 0.023550
clock jitter: 0.004
clock wander: 0.001
broadcast delay: -50.000
symm. auth. delay: 0.000
```

```
uptime: 204908
sysstats reset: 204908
packets received: 19928
current version: 6069
older version: 0
bad length or format: 0
authentication failed: 0
declined: 0
restricted: 0
rate limited: 0
```



```

KoD responses:          0
processed for time:    6040

associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
pll offset:            0.006196
pll frequency:        7.49899
maximum error:        0.097039
estimated error:      3e-06
kernel status:        pll nano
pll time constant:    6
precision:            1e-06
frequency tolerance:  500
pps frequency:        0
pps stability:        0
pps jitter:           0
calibration interval  0
calibration cycles:   0
jitter exceeded:     0
stability exceeded:   0
calibration errors:   0

time since reset:     204908
receive buffers:      10
free receive buffers: 9
used receive buffers: 0
low water refills:   1
dropped packets:     0
ignored packets:     0
received packets:    19930
packets sent:        26811
packet send failures: 0
input wakeups:       224931
useful input wakeups: 20034

```

Verify the NTP Synchronization Between MIO and Logical Device (Blade) on FPR41xx/9300 Appliances

On FPR41xx/9300 the NTP settings are pushed to FTD via the MIO (chassis). The NTP configuration from the FTD CLI or the FMC UI is not possible.


Each FTD blade uses an internal reference-id: 203.0.113.126 to communicate with the MIO for time sync and based on that, it shows whether it is synchronized or not. The FTD CLI reflects this. The NTP IP in this example is the internal ref-id, not the actual NTP Server IP. A change of the NTP server IP in the FCM does not affect this output since the reference-id is always the same:

```

> show ntp
NTP Server          : 203.0.113.126
Status              : Being Used
Offset              : -0.078 (milliseconds)
Last Update         : 43 (seconds)

```

Verify the NTP Configuration on FPR1xxx/2100 Appliances

 **Caution:** This is only applicable on FPR1xxx/2100 appliances for ASA in Platform mode.

```
firepower-2140# scope system
firepower-2140 /system # scope services
firepower-2140 /system/services # show ntp-server detail
```




```
NTP server hostname:
Name: 172.31.201.67
Time Sync Status: Time Synchronized
Error Msg:
```

```
Name: ntp.esl.cisco.com
Time Sync Status: Candidate
Error Msg:
```

Troubleshoot Common Issues

1. FXOS not Able to Resolve the NTP Server Hostname

The FCM UI shows:

NTP Server	Server Status	Actions
ntp.esl.cisco.com	Unreachable/Invalid 	 

Recommended Action

Use the ping command to verify the NTP server hostname resolution




```
KSEC-FPR4100-8-A(local-mgmt)# ping ntp.esl.cisco.com
Invalid Host Name.
```

Possible Causes


- The DNS Server is not configured.
- The DNS Server is not able to resolve the hostname.

2. Connectivity Issues Between FXOS - NTP Server on UDP Port 123

The FCM UI shows:

+ Add		
NTP Server	Server Status	Actions
cisco.com	Unreachable/Invalid 	 

Recommended Action

 **Caution:** Ethanalyzer capture on chassis management interface is only available on FPR41xx/9300 appliances.

Take captures on the chassis management interface and verify the bidirectional communication on UDP port 123:

<#root>




```
KSEC- FPR4100-8-A(fxos)# ethanalyzer local interface mgmt capture-filter "udp port 123"
Capturing on 'eth0'
1 2020-04-30 20:09:54.150237760 10.62.148.196 → 172.16.4.161 NTP 90 NTP Version 3, client
2 2020-04-30 20:14:14.150172804 10.62.148.196 → 172.16.4.161 NTP 90 NTP Version 3, client
3 2020-04-30 20:23:13.150171682 10.62.148.196 → 172.16.4.161 NTP 90 NTP Version 3, client
```

Possible Causes

- The configured server is not an NTP Server.
- A device in the path (for example, firewall) blocks or modifies the traffic.

3. Intermittent Connectivity Issues Between FXOS and NTP Server

The FCM UI shows:

+ Add		
NTP Server	Server Status	Actions
ntp.esl.cisco.com	Unreachable/Invalid 	 

Recommended Actions

 **Caution:** Only for FPR41xx/9300 appliances.

Initiate the NTP synchronization process from the FXOS CLI

```
FPR4100-8-A# connect fxos
FPR4100-8-A(fxos)# ntp sync-retry
```

Take captures on chassis management interface with **ethalyzer** CLI command tool.

Possible Cause

- Intermittent connectivity issues between FXOS - NTP Server

Related Defects

Check the Release Notes for known/fixed defects.

Related Information

- [FXOS Configuration Guides](#)
- [Troubleshoot Issues with Network Time Protocol \(NTP\) on Firepower Systems](#)