



# FortiNAC

## Troubleshooting Device Detection Traps

Version: 8.7, 8.8

Date: October 13, 2020

Rev: A

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET KNOWLEDGE BASE**

<http://kb.fortinet.com>

**FORTINET BLOG**

<http://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<http://support.fortinet.com>

**FORTINET COOKBOOK**

<http://cookbook.fortinet.com>

**NSE INSTITUTE**

<http://training.fortinet.com>

**FORTIGUARD CENTER**

<http://fortiguard.com>

**FORTICAST**

<http://forticast.fortinet.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

# Contents

|                 |   |
|-----------------|---|
| Overview .....  | 4 |
| Procedure ..... | 4 |
| Debugging ..... | 5 |

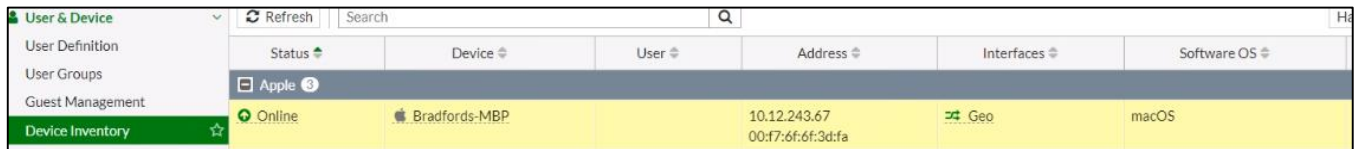
# Overview

This document provides steps to validate the receipt and processing of a Device Detection SNMP Trap sent by FortiGate.

For configuration details, refer to the [Fortigate Endpoint Management Integration](#) reference manuals in the FortiNAC Document Library:

## Procedure

1. Verify the appliance is running version 8.7.6, 8.8.2 or higher.
2. Verify the FortiGate is detecting the connected device. In the FortiGate UI, navigate to **User & Device > Device Inventory** confirm the device is listed.



| Status | Device         | User | Address                           | Interfaces | Software OS |
|--------|----------------|------|-----------------------------------|------------|-------------|
| Online | Bradford's-MBP |      | 10.12.243.67<br>00:f7:6f:6f:3d:fa | Geo        | macOS       |

3. Disconnect test device or admin down the switch port.
  4. Delete the device entry from Device Inventory. In FortiGate CLI type **Diagnose user device del <mac address xx:xx:xx:xx:xx>**
- ```
FGT-Branch # diagnose user device del 00:f7:6f:6f:3d:fa  
Removed host from vd 0
```
5. Run tcpdump on the FortiNAC to verify traps are received. In the FortiNAC CLI type **tcpdump -nni any port 162 and host <FGT IP address in FortiNAC>**
  6. Connect the device or admin up the port.
  7. In the FortiGate UI, confirm the device re-populates the Device Inventory.
  8. In the FortiNAC CLI, verify the trap is received.

```
FortiNAC FNMCA  
root@hercules:/root  
tcpdump -nni any portrange 161-163 and host 10.12.240.13  
tcpdump: verbose output suppressed, use -v or -w for full protocol decode  
listening on any, link-type LINUX_SLL (linux cooked), capture size 262144 bytes  
14:39:32.088182 IP 10.12.240.13.162 > 10.12.242.7.162: C="private" V2Trap(228) .1.3.6.1.2.1.1.3.0=190328859 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.4.1.12356.101.2.0.12  
01 .1.3.6.1.4.1.12356.100.1.1.1.0="FG81EPTK19001604" .1.3.6.1.2.1.1.5.0="FGT-Branch" .1.3.6.1.2.1.2.2.1.1.0=26 .1.3.6.1.4.1.12356.101.3.2.1.1.1.0=1 .1.3.6.1.4.1.1  
2356.101.18.1.2.0=5 .1.3.6.1.4.1.12356.101.18.1.3.0=0 .1.3.6.1.4.1.12356.101.18.1.1.0="00:f7:6f:6f:3d:fa"
```

9. Ctrl-C to stop tcpdump.

- In the FortiNAC UI, navigate to **Hosts > Host View** and search by MAC address for the connecting device. The host should now show online.



**Note:**

- If the host record has not yet been created, FortiNAC runs a L2 poll of the FortiGate after receiving the trap. Once poll completes, the host record is created.
- If host record already exists, the online status is updated upon receipt of the trap.
- Host record will display FortiGate as the location (since FortiNAC has no knowledge of the connecting switch).

## Debugging

If tcpdump shows the trap received but the host record connection status does not update, collect logs while reproducing the behavior.

In the FortiNAC CLI, enable debug. Type:  
**CampusMgrDebug -name DeviceInterface true**  
**CampusMgrDebug -name BridgeManager true**  
**CampusMgrDebug -name SnmpV1 true**

1. Disconnect test device or admin down the switch port.
2. Delete the device entry from Device Inventory. In FortiGate CLI type  
**Diagnose user device del <mac address xx:xx:xx:xx:xx>**
3. Run tcpdump on the FortiNAC to verify traps are received. In the FortiNAC CLI type  
**tcpdump -nni any port 162 and host <FGT IP address in FortiNAC>**
4. Open another FortiNAC CLI window and tail the logs. Save output to a file (DevDTrap\_master.txt). Type  
**tail -F /bsc/logs/output.master | tee DevDTrap\_master.txt**
5. Connect the device or admin up the port.

6. In the FortiGate UI, confirm the device re-populates the Device Inventory.
7. In the FortiNAC CLI tcpdump, verify the trap is received.
8. Ctrl-C to stop the tcpdump.
9. Save tcpdump output to a text file and save as DevDTraptcpdump.txt
10. Ctrl\_C to stop the tail.
11. Disable debug. Type  
**CampusMgrDebug -name DeviceInterface false**  
**CampusMgrDebug -name BridgeManager false**  
**CampusMgrDebug -name SnmpV1 false**
12. Use WinSCP or a similar application to download deviceDTrap\_master.txt to a computer (use SCP for the transfer protocol).
13. Open a support ticket and provide the following information:
  - Description of behavior
  - MAC address of the test device
  - Attach DevDTraptcpdump.txt
  - Attach DeviDTrap\_master.txt



**FORTINET®**



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.