

Protect Against CSCwi63113 During Upgrade to 7.2.6

Contents

[Introduction](#)

[Background](#)

[Disable SNMP before the upgrade](#)

[FMC Steps:](#)

[Step 1: Log into your FMC](#)

[Step 2: Navigate to Devices > Platform Settings](#)

[Step 3: Edit the policy associated with your FTD devices](#)

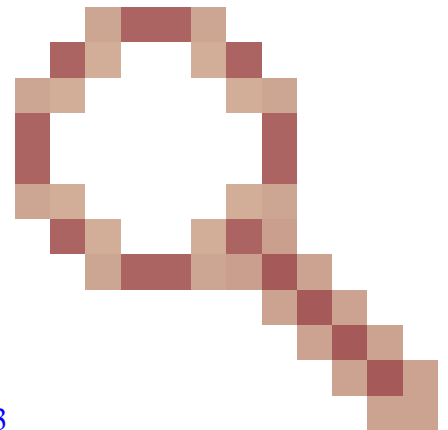
[Step 4: Select SNMP](#)

[Step 5: Disable SNMP Servers](#)

[Step 6: Save to policy and deploy](#)

[What to do if you have already upgraded and are experiencing a boot loop:](#)

Introduction



This document describes information related to Cisco bug ID [CSCwi63113](#) and how to prevent problems during the upgrade to FTD version 7.2.6.

Background

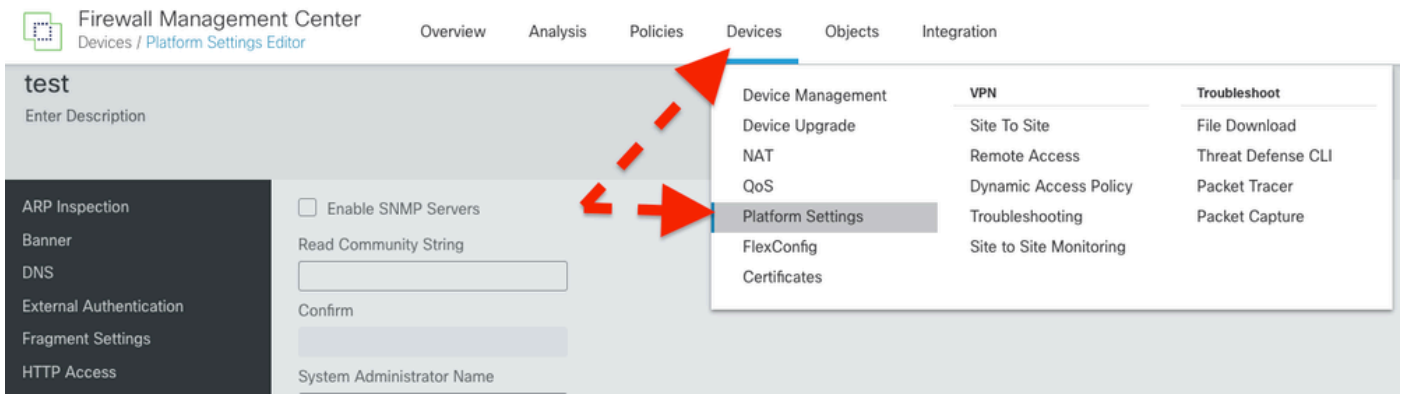
Cisco Firepower Threat Defense software version 7.2.6 contains Cisco bug ID [CSCwi63113](#), which prevents some devices from booting when SNMP is enabled. Before installing 7.2.6, please disable SNMP until you can upgrade to 7.2.7 or beyond. A fix for this is being prepared and will be released as 7.2.7 by 3 May 2024. Additionally, Cisco will be releasing 7.2.5.2 by 6 May 2024, which is 7.2.5.1 with only the fixes for CVE-2024-20353, CVE-2024-20359, and CVE-2024-20358.

Disable SNMP before the upgrade

FMC Steps:

Step 1: Log into your FMC

Step 2: Navigate to Devices > Platform Settings



The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is selected. A dropdown menu is open under 'Devices', with 'Platform Settings' highlighted. Red dashed arrows point from the 'Devices' tab to the dropdown menu and from the 'Platform Settings' option to the main content area.

test
Enter Description

ARP Inspection
Banner
DNS
External Authentication
Fragment Settings
HTTP Access

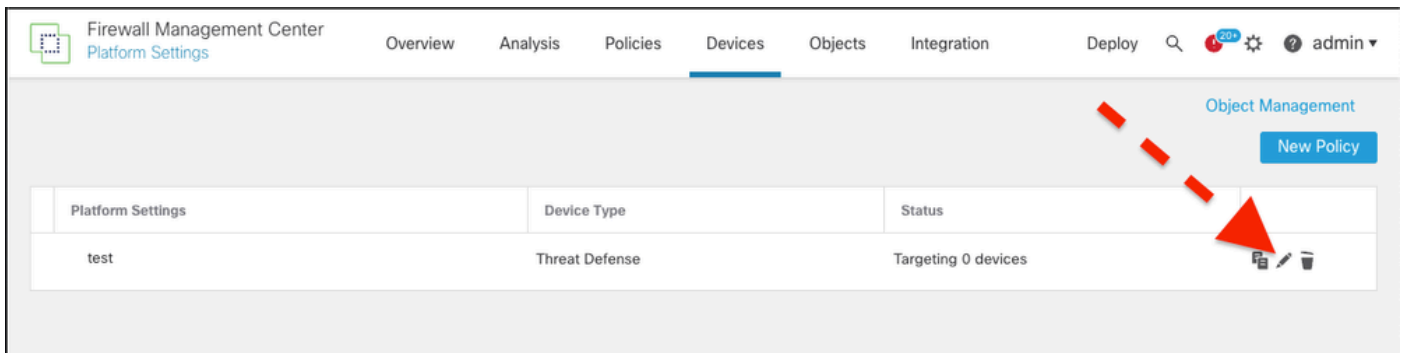
Enable SNMP Servers
Read Community String
Confirm
System Administrator Name

- Device Management
- Device Upgrade
- NAT
- QoS
- Platform Settings
- FlexConfig
- Certificates

- VPN
- Site To Site
- Remote Access
- Dynamic Access Policy
- Troubleshooting
- Site to Site Monitoring

- Troubleshoot
- File Download
- Threat Defense CLI
- Packet Tracer
- Packet Capture

Step 3: Edit the policy associated with your FTD devices



The screenshot shows the Firewall Management Center interface with the 'Devices' tab selected. A table lists policies. A red dashed arrow points from the 'Object Management' link to the edit icon in the table row.

Firewall Management Center
Platform Settings

Overview Analysis Policies Devices Objects Integration Deploy

Object Management
New Policy

Platform Settings	Device Type	Status
test	Threat Defense	Targeting 0 devices

Step 4: Select SNMP



test

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Listen Port

(1 - 65535)

Hosts

Users

SNMP Traps

Interface	Network	SNMP Version	Poll/Trap
Management	backup_c1	1	Poll,Trap

Step 5: Disable SNMP Servers



test

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Listen Port

(1 - 65535)

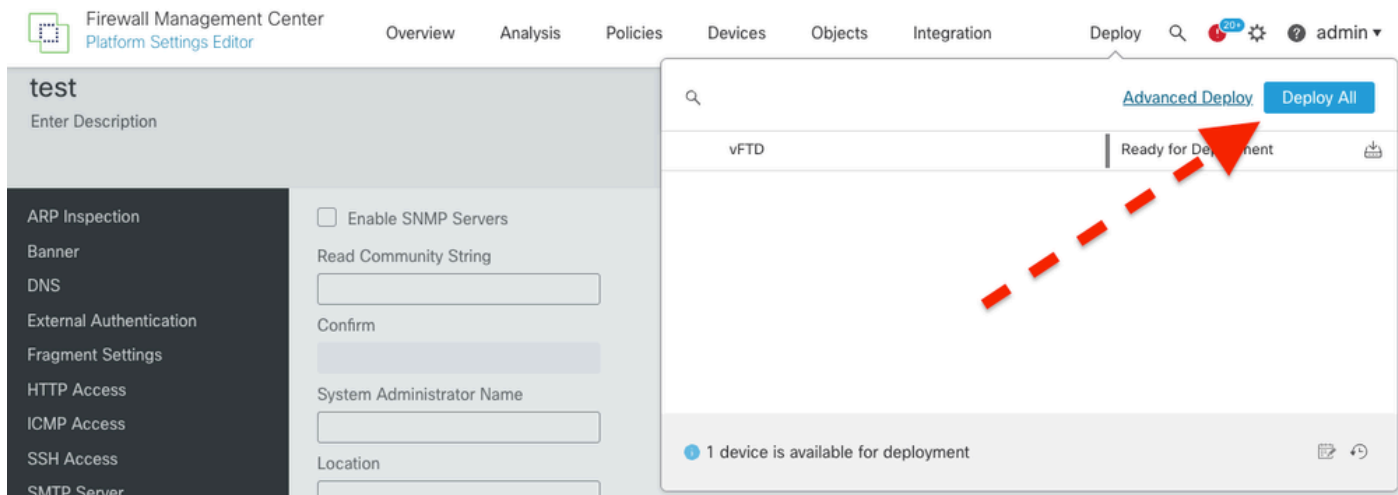
Hosts

Users

SNMP Traps

Interface	Network	SNMP Version
Management	backup_c1	1

Step 6: Save to policy and deploy



Please look at the defect for more up-to-date information: Cisco bug ID [CSCwi63113](#).

If you need any further information, please contact Cisco TAC ([support.cisco.com](#)) and reference Arcane Door (cisco-sa-asaftd-persist-rce-FLsNXF4h / CVE-2024-20359)

What to do If you have already upgraded and are experiencing a boot loop:

If you have already updated to 7.2.6 and are facing the effects of Cisco bug ID [CSCwi63113](#) please contact Cisco TAC ([support.cisco.com](#)).