

Schutz vor CSCwi63113 beim Upgrade auf 7.2.6

Inhalt

[Einleitung](#)

[Hintergrund](#)

[SNMP vor dem Upgrade deaktivieren](#)

[FMC-Schritte:](#)

[Schritt 1: Melden Sie sich bei Ihrem FMC an](#)

[Schritt 2: Navigieren Sie zu Geräte > Plattformeinstellungen.](#)

[Schritt 3: Bearbeiten Sie die Richtlinie für Ihre FTD-Geräte.](#)

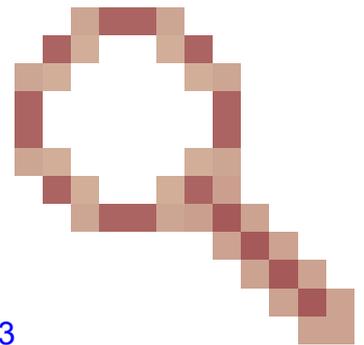
[Schritt 4: SNMP auswählen](#)

[Schritt 5: Deaktivieren von SNMP-Servern](#)

[Schritt 6: Speichern Sie bei Richtlinien, und stellen Sie sie bereit](#)

[Vorgehensweise Wenn Sie bereits ein Upgrade durchgeführt haben und eine Boot-Schleife vorhanden ist:](#)

Einleitung



In diesem Dokument werden Informationen zur Cisco Bug-ID [CSCwi63113](#) und zur Vermeidung von Problemen während des Upgrades auf FTD-Version 7.2.6 beschrieben.

Hintergrund

Die Cisco Firepower Threat Defense-Software Version 7.2.6 enthält die Cisco Bug-ID [CSCwi63113](#), die verhindert, dass einige Geräte starten, wenn SNMP aktiviert ist. Vor der Installation von 7.2.6 deaktivieren Sie SNMP, bis Sie ein Upgrade auf Version 7.2.7 oder höher durchführen können. Ein Fix dafür wird vorbereitet und wird bis zum 3. Mai 2024 als 7.2.7 veröffentlicht. Darüber hinaus wird Cisco 7.2.5.2 bis zum 6. Mai 2024 veröffentlichen. Dies entspricht 7.2.5.1, wobei nur die Korrekturen für CVE-2024-20353, CVE-2024-20359 und CVE-2024-20358 vorliegen.

SNMP vor dem Upgrade deaktivieren

FMC-Schritte:

Schritt 1: Melden Sie sich bei Ihrem FMC an

Schritt 2: Navigieren Sie zu Geräte > Plattformeinstellungen.

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, showing options: Device Management, Device Upgrade, NAT, QoS, Platform Settings (highlighted), FlexConfig, and Certificates. A red dashed arrow points from the 'Devices' tab to the dropdown menu, and another red dashed arrow points 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

Schritt 3: Bearbeiten Sie die Richtlinie für Ihre FTD-Geräte.

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'Integration', 'Deploy', a search icon, a gear icon, and 'admin'. The 'Devices' tab is selected. A table displays the Platform Settings for a device named 'test'. A red dashed arrow points from the 'Object Management' link to the table, and another red dashed arrow points from the 'New Policy' button to the table.

Platform Settings
Device Type
Status

test
Threat Defense
Targeting 0 devices

Object Management
New Policy

Schritt 4: SNMP auswählen



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

Schritt 5: Deaktivieren von SNMP-Servern



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)

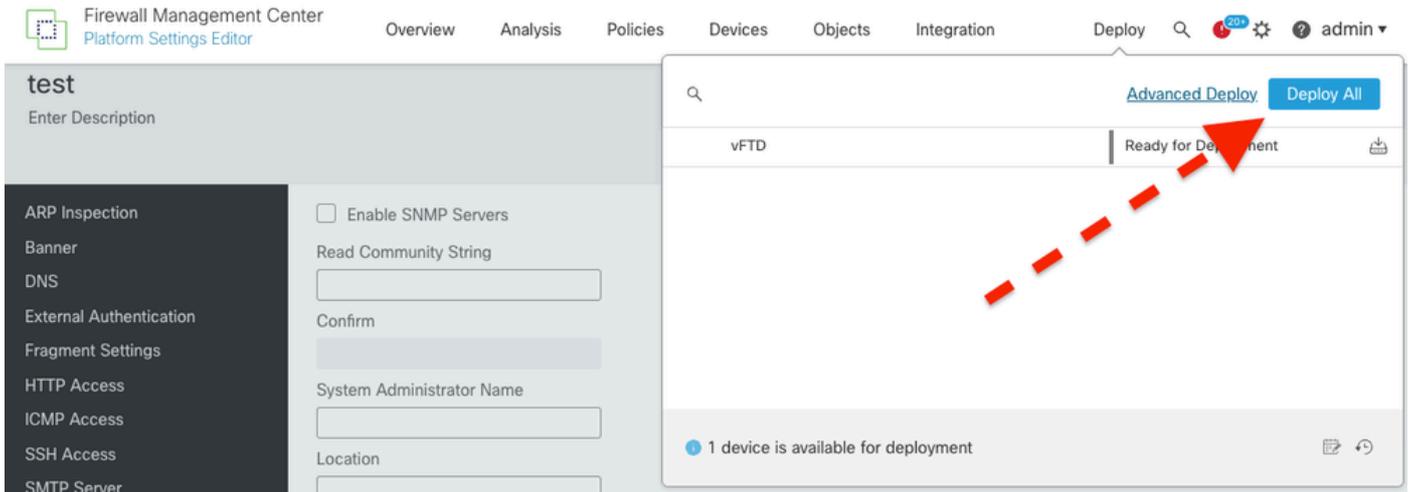
Hosts

Users

SNMP Traps

Interface	Network	SNMP Version
Management	backup_c1	1

Schritt 6: Sparen Sie bei Richtlinien, und stellen Sie sie bereit



Bitte sehen Sie sich den Defekt an, um weitere aktuelle Informationen zu erhalten: Cisco Bug-ID [CSCwi63113](#).

Wenn Sie weitere Informationen benötigen, wenden Sie sich an das Cisco TAC (support.cisco.com) und an Arcane Door (cisco-sa-asaftd-persist-rce-FLsNXF4h / CVE-2024-20359).

Vorgehensweise Wenn Sie bereits ein Upgrade durchgeführt haben und eine Boot-Schleife vorhanden ist:

Wenn Sie bereits ein Update auf Version 7.2.6 durchgeführt haben und die Auswirkungen des Cisco Bug ID [CSCwi63113](#) haben, wenden Sie sich an das Cisco TAC (support.cisco.com).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.