

# Proteggi da CSCwi63113 durante l'aggiornamento alla versione 7.2.6

## Sommario

---

[Introduzione](#)

[Introduzione](#)

[Disabilitare il protocollo SNMP prima dell'aggiornamento](#)

[Fasi del CCP:](#)

[Passaggio 1: Accedere al CCP](#)

[Fase 2: Passare a Dispositivi > Impostazioni piattaforma](#)

[Passaggio 3: Modificare il criterio associato ai dispositivi FTD](#)

[Passaggio 4: Selezione di SNMP](#)

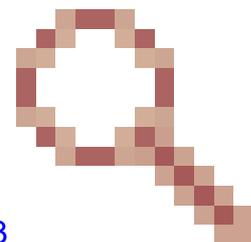
[Passaggio 5: disabilitare i server SNMP](#)

[Passaggio 6: Salvare nei criteri e distribuire](#)

[Cosa fare Se si è già eseguito l'aggiornamento e si verifica un loop di avvio:](#)

---

## Introduzione



Questo documento descrive le informazioni relative all'ID bug Cisco [CSCwi63113](#) e come prevenire i problemi durante l'aggiornamento alla versione 7.2.6 del FTD.

## Introduzione

Il software Cisco Firepower Threat Defense versione 7.2.6 contiene l'ID bug Cisco [CSCwi63113](#), che impedisce l'avvio di alcuni dispositivi quando SNMP è abilitato. Prima di installare la versione 7.2.6, disabilitare il protocollo SNMP fino a quando non è possibile eseguire l'aggiornamento alla versione 7.2.7 o successive. È in corso di preparazione una correzione che sarà pubblicata come 7.2.7 entro il 3 maggio 2024. Inoltre, Cisco rilascerà la versione 7.2.5.2 entro il 6 maggio 2024, ovvero la versione 7.2.5.1 con le sole correzioni per CVE-2024-20353, CVE-2024-20359 e CVE-2024-20358.

## Disabilitare il protocollo SNMP prima dell'aggiornamento

Fasi del CCP:

Passaggio 1: Accedere al CCP

## Fase 2: Passare a Dispositivi > Impostazioni piattaforma

The screenshot shows the 'Platform Settings Editor' for a device named 'test'. The navigation menu at the top includes Overview, Analysis, Policies, Devices, Objects, and Integration. The 'Devices' menu is expanded, showing options like Device Management, Device Upgrade, NAT, QoS, Platform Settings (highlighted), FlexConfig, and Certificates. Other categories include VPN (Site To Site, Remote Access, Dynamic Access Policy, Troubleshooting, Site to Site Monitoring) and Troubleshoot (File Download, Threat Defense CLI, Packet Tracer, Packet Capture). The main content area has a left sidebar with ARP Inspection, Banner, DNS, External Authentication, Fragment Settings, and HTTP Access. The main area contains a form with fields for 'Enable SNMP Servers', 'Read Community String', 'Confirm', and 'System Administrator Name'.

## Passaggio 3: Modificare il criterio associato ai dispositivi FTD

The screenshot shows the 'Platform Settings' table in the Firewall Management Center. The table has three columns: Platform Settings, Device Type, and Status. The first row shows 'test' under Platform Settings, 'Threat Defense' under Device Type, and 'Targeting 0 devices' under Status. A red dashed arrow points to the 'Object Management' icon in the rightmost column of the row. The top navigation bar includes Overview, Analysis, Policies, Devices, Objects, Integration, Deploy, and a user profile 'admin'.

Platform Settings	Device Type	Status	Object Management
test	Threat Defense	Targeting 0 devices	

## Passaggio 4: Selezione di 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

Passaggio 5: disabilitare i server 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)

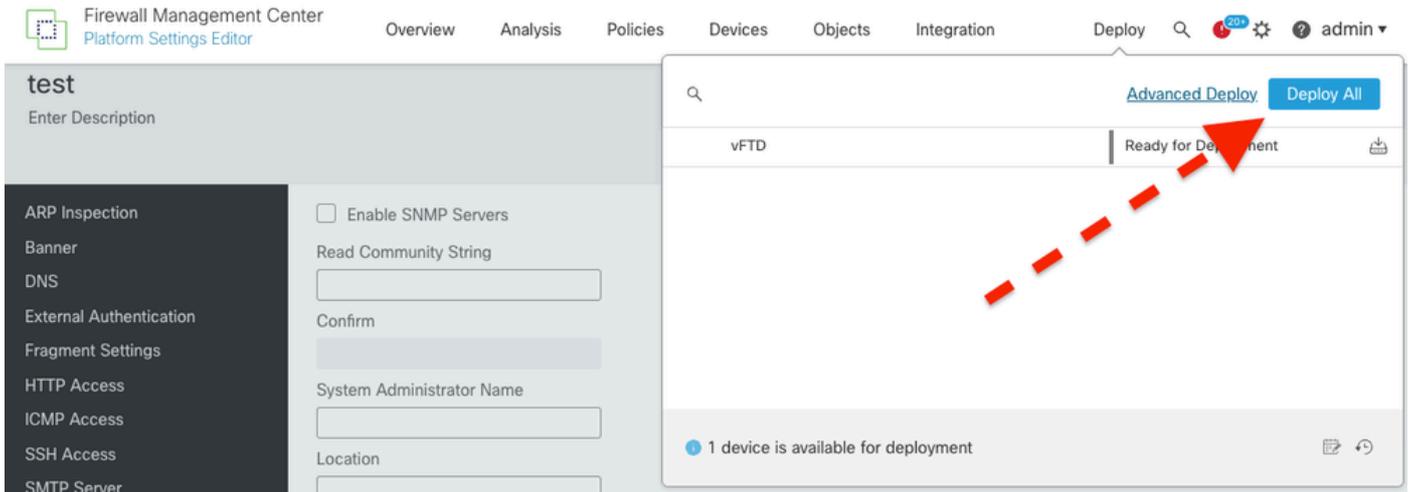
Hosts

Users

SNMP Traps

Interface	Network	SNMP Version
Management	backup_c1	1

Passaggio 6: Salvare nei criteri e distribuire



Controllare il difetto per informazioni più aggiornate: ID bug Cisco [CSCwi63113](#).

Per ulteriori informazioni, contattare Cisco TAC ([support.cisco.com](https://support.cisco.com)) e referenziare Arcane Door (cisco-sa-asaftd-persist-rce-FLsNXF4h / CVE-2024-20359)

**Cosa fare Se si è già eseguito l'aggiornamento e si verifica un loop di avvio:**

Se si è già eseguito l'aggiornamento alla versione 7.2.6 e si stanno riscontrando gli effetti dell'ID bug Cisco [CSCwi63113](#) contattare Cisco TAC ([support.cisco.com](https://support.cisco.com)).

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).