

# Proteger contra CSCwi63113 durante la actualización a 7.2.6

## Contenido

---

[Introducción](#)

[Background](#)

[Desactivar SNMP antes de la actualización](#)

[Pasos del FMC:](#)

[Paso 1: Inicie sesión en el FMC](#)

[Paso 2: Vaya a Dispositivos > Configuración de plataforma](#)

[Paso 3: Editar la política asociada a sus dispositivos FTD](#)

[Paso 4: Seleccionar SNMP](#)

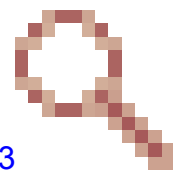
[Paso 5: Desactivar servidores SNMP](#)

[Paso 6: Guardar en la política e implementar](#)

[Qué hacer Si ya ha actualizado y está experimentando un loop de inicio:](#)

---

## Introducción



Este documento describe información relacionada con el ID de bug Cisco [CSCwi63113](#) y cómo prevenir problemas durante la actualización a la versión 7.2.6 de FTD.

## Background

La versión 7.2.6 del software Cisco Firepower Threat Defence contiene el ID de error de Cisco [CSCwi63113](#), que impide que algunos dispositivos se inicien cuando SNMP está activado. Antes de instalar 7.2.6, desactive SNMP hasta que pueda actualizar a 7.2.7 o posterior. Se está preparando una solución para este problema, que se publicará como 7.2.7 a más tardar el 3 de mayo de 2024. Además, Cisco publicará 7.2.5.2 el 6 de mayo de 2024, que es 7.2.5.1 con solo las correcciones para CVE-2024-20353, CVE-2024-20359 y CVE-2024-20358.

## Desactivar SNMP antes de la actualización

Pasos del FMC:

Paso 1: Inicie sesión en el FMC

Paso 2: Vaya a Dispositivos > Configuración de plataforma

Firewall Management Center  
Devices / Platform Settings Editor

Overview Analysis Policies **Devices** Objects Integration

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

### Paso 3: Editar la política asociada a sus dispositivos FTD

Firewall Management Center  
Platform Settings

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 20+ ⚙️ ? admin ▾

Object Management  
New Policy

| Platform Settings | Device Type    | Status              |  |
|-------------------|----------------|---------------------|--|
| test              | Threat Defense | Targeting 0 devices |  |

### Paso 4: Seleccionar 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 |

## Paso 5: Desactivar servidores 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)

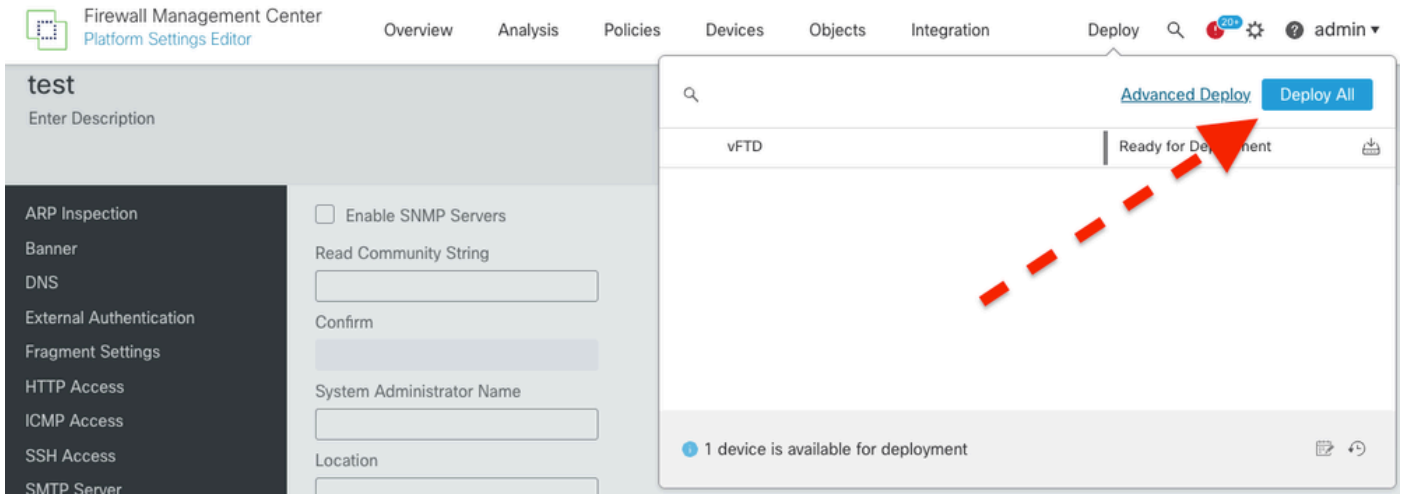
Hosts

Users

SNMP Traps

| Interface  | Network   | SNMP Version |
|------------|-----------|--------------|
| Management | backup_c1 | 1            |

Paso 6: Guardar en la política e implementar



Consulte el defecto para obtener información más actualizada: ID de error de Cisco [CSCwi63113](https://cisco.com/cisco/web/cisco-ids/cscwi63113).

Si necesita más información, póngase en contacto con Cisco TAC ([support.cisco.com](https://support.cisco.com)) y haga referencia a Arcane Door (cisco-sa-asaftd-persist-race-FLsNXF4h / CVE-2024-20359)

**Qué hacer Si ya ha actualizado y está experimentando un loop de inicio:**

Si ya ha actualizado a la versión 7.2.6 y se enfrenta a los efectos de la identificación de error de Cisco [CSCwi63113](https://cisco.com/cisco/web/cisco-ids/cscwi63113), póngase en contacto con Cisco TAC ([support.cisco.com](https://support.cisco.com)).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).