

# Protection contre CSCwi63113 lors de la mise à niveau vers la version 7.2.6

## Table des matières

---

[Introduction](#)

[Fond](#)

[Désactiver SNMP avant la mise à niveau](#)

[Étapes FMC :](#)

[Étape 1 : Connectez-vous à votre FMC](#)

[Étape 2 : Accédez à Devices > Platform Settings](#)

[Étape 3 : Modifiez la stratégie associée à vos périphériques FTD](#)

[Étape 4 : sélectionnez SNMP](#)

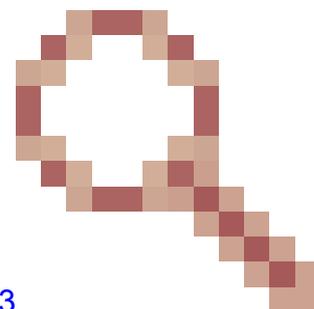
[Étape 5 : Désactivez les serveurs SNMP](#)

[Étape 6 : enregistrez dans la stratégie et déployez](#)

[Que faire Si vous avez déjà effectué une mise à niveau et que vous rencontrez une boucle de démarrage :](#)

---

## Introduction



Ce document décrit les informations liées à l'ID de bogue Cisco [CSCwi63113](#) et comment éviter les problèmes pendant la mise à niveau vers la version FTD 7.2.6.

## Fond

La version 7.2.6 du logiciel Cisco Firepower Threat Defense contient l'ID de bogue Cisco [CSCwi63113](#), qui empêche certains périphériques de démarrer lorsque le protocole SNMP est activé. Avant d'installer la version 7.2.6, désactivez SNMP jusqu'à ce que vous puissiez effectuer la mise à niveau vers la version 7.2.7 ou ultérieure. Un correctif est en cours de préparation et sera publié sous la forme 7.2.7 d'ici le 3 mai 2024. En outre, Cisco publiera 7.2.5.2 d'ici le 6 mai 2024, soit 7.2.5.1 avec uniquement les correctifs pour CVE-2024-20353, CVE-2024-20359 et CVE-2024-20358.

## Désactiver SNMP avant la mise à niveau

Étapes FMC :

Étape 1 : Connectez-vous à votre FMC

Étape 2 : Accédez à Devices > Platform Settings

The screenshot shows the Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' menu is open, showing options like 'Device Management', 'Device Upgrade', 'NAT', 'QoS', 'Platform Settings', 'FlexConfig', and 'Certificates'. The 'Platform Settings' option is highlighted. On the left, a sidebar lists various settings like 'ARP Inspection', 'Banner', 'DNS', etc. The main content area shows the 'Platform Settings Editor' for a device named 'test', with fields for 'Enable SNMP Servers', 'Read Community String', 'Confirm', and 'System Administrator Name'.

Étape 3 : Modifiez la stratégie associée à vos périphériques FTD

The screenshot shows the 'Platform Settings' page in the FMC. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'Integration', 'Deploy', and a search icon. The 'Devices' menu is open. The main content area shows a table with the following data:

Platform Settings	Device Type	Status
test	Threat Defense	Targeting 0 devices

There is a 'New Policy' button and an 'Object Management' link. A red dashed arrow points to the edit icon in the table row.

Étape 4 : sélectionnez 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

Étape 5 : Désactivez les serveurs 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

Étape 6 : enregistrez dans la stratégie et déployez

test  
Enter Description

ARP Inspection  
Banner  
DNS  
External Authentication  
Fragment Settings  
HTTP Access  
ICMP Access  
SSH Access  
SMTP Server

Enable SNMP Servers  
Read Community String  
Confirm  
System Administrator Name  
Location

vFTD | Ready for Deployment

Advanced Deploy Deploy All

1 device is available for deployment

Consultez le défaut pour obtenir des informations plus à jour : ID de bogue Cisco [CSCwi63113](https://cisco.com/cisco Bug ID CSCwi63113).

Pour plus d'informations, contactez le TAC Cisco ([support.cisco.com](https://support.cisco.com)) et la référence Arcane Door (cisco-sa-asaftd-persist-rce-FLsNXF4h / CVE-2024-20359)

**Que faire Si vous avez déjà effectué une mise à niveau et que vous rencontrez une boucle de démarrage :**

Si vous avez déjà effectué la mise à jour vers la version 7.2.6 et que vous rencontrez les effets du bogue Cisco ayant l'ID [CSCwi63113](https://cisco.com/cisco Bug ID CSCwi63113), contactez le TAC Cisco ([support.cisco.com](https://support.cisco.com)).

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.