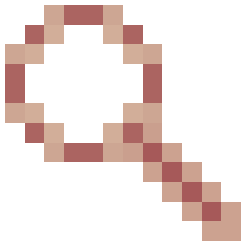
# Proteggi da CSCwi63113 durante l'aggiornamento alla versione 7.2.6

## Sommario



## 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

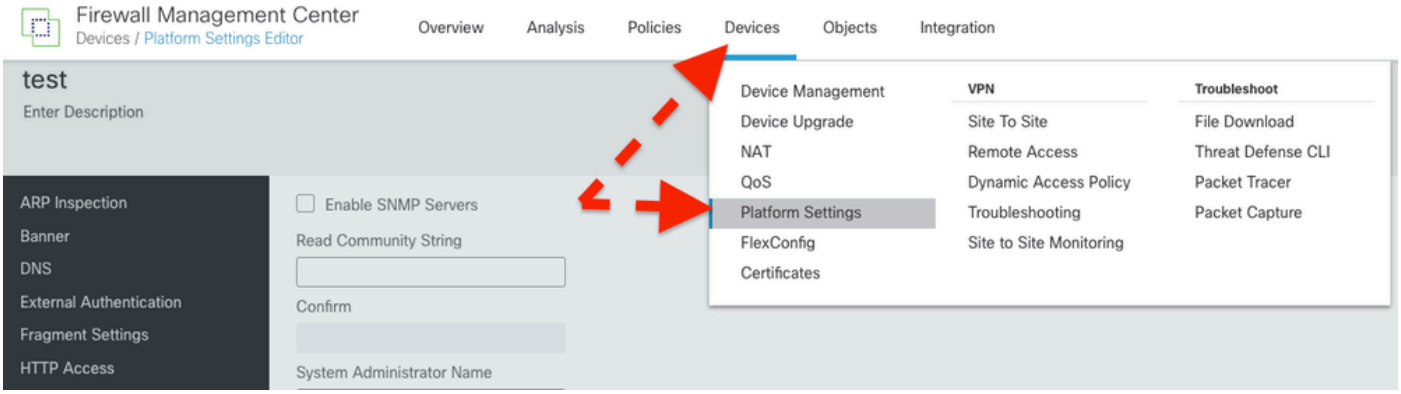
Il software Cisco Firepower Threat Defense versione 7.2.6 contiene l'ID bug Cisco CSCwi63113, che impedisce l'avvio di alcuni dispositivi quando SNMP è abilitato. Prima di installare la versione 7.2.6, disabilitare il protocollo SNMP fino a quando non è possibile eseguire l'aggiornamento alla versione 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

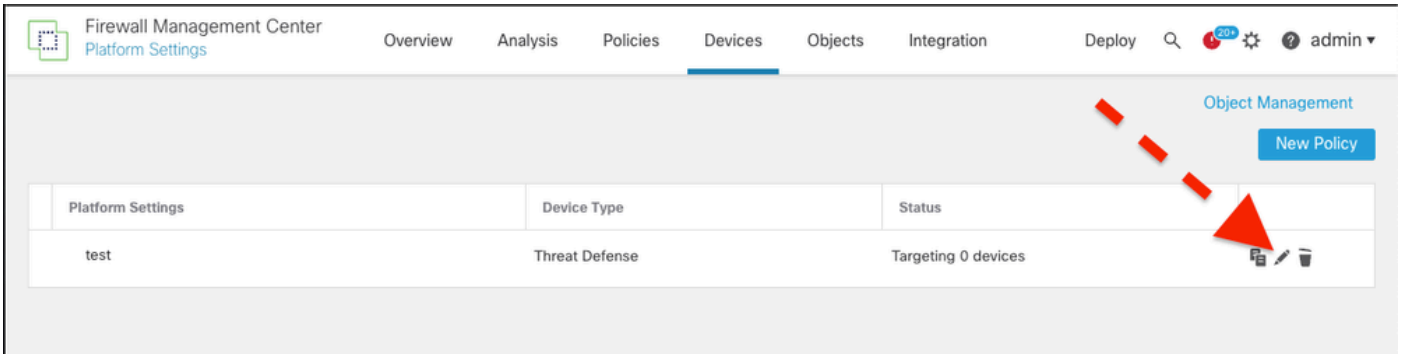
### Fasi del CCP:

Passaggio 1: Accedere al CCP

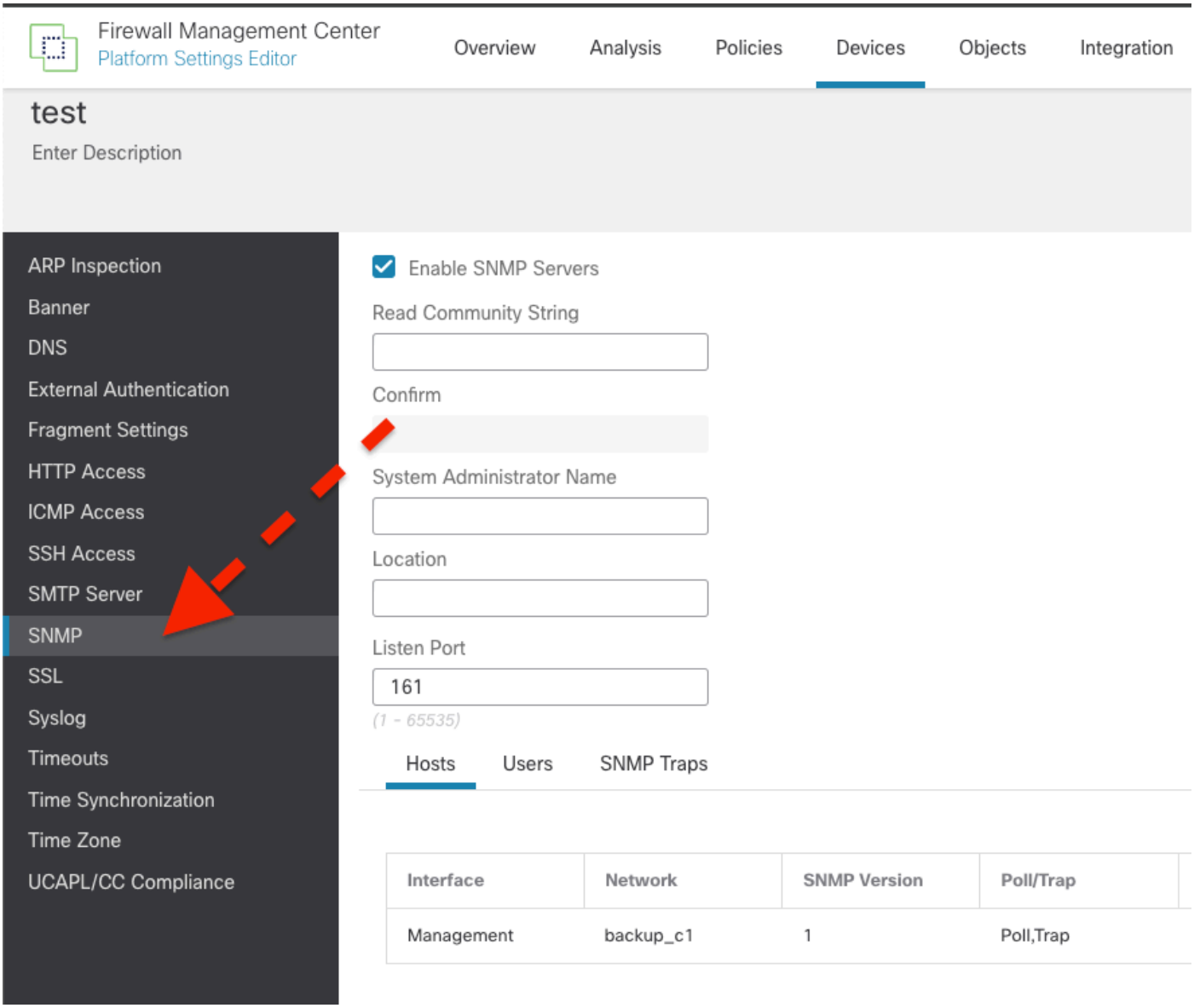
Fase 2: Passare a Dispositivi > Impostazioni piattaforma



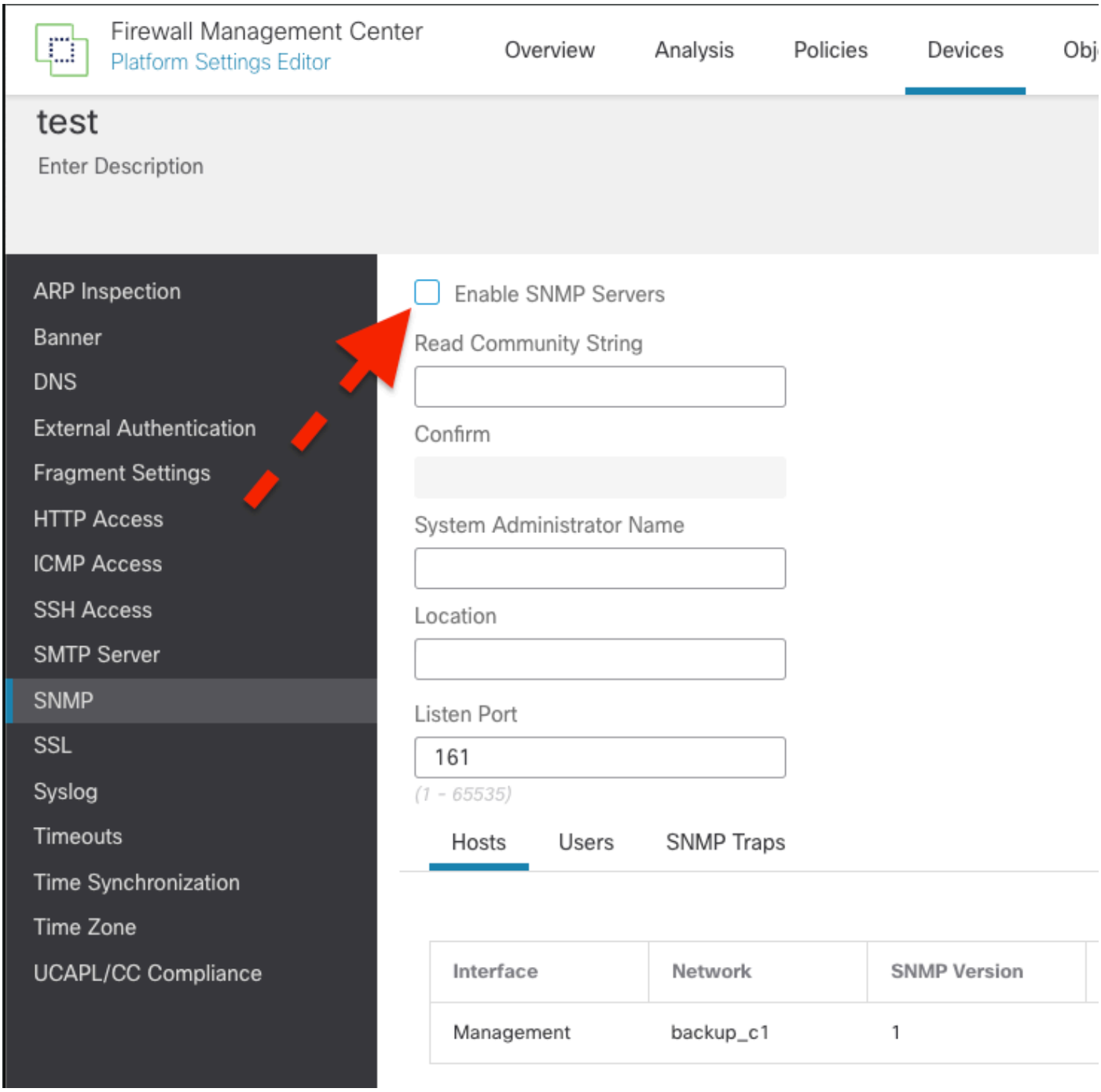

Passaggio 3: Modificare il criterio associato ai dispositivi FTD



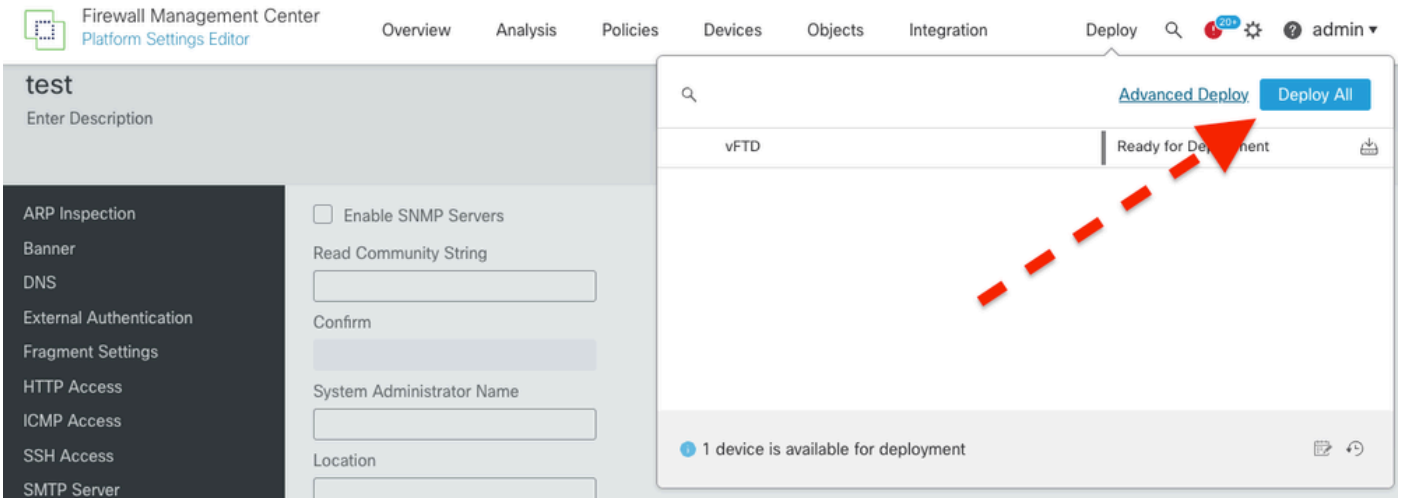

Passaggio 4: Selezione di SNMP




Passaggio 5: disabilitare i server SNMP




Passaggio 6: Salvare nei criteri e distribuire




Controllare il difetto per informazioni più aggiornate: ID bug Cisco CSCwi63113.

Per ulteriori informazioni, contattare Cisco TAC (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 CSCwi63113contattare Cisco TAC (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).