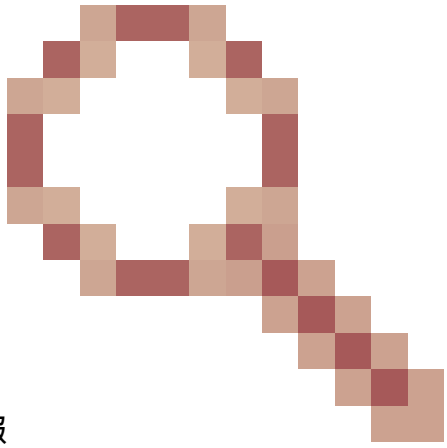
7.2.6へのアップグレード中のCSCwi63113からの保護

内容

はじめに



このドキュメントでは、Cisco Bug ID CSCwi63113に関連する情報
、およびFTDバージョン7.2.6へのアップグレード中の問題を回避する方法について説明します。

背景

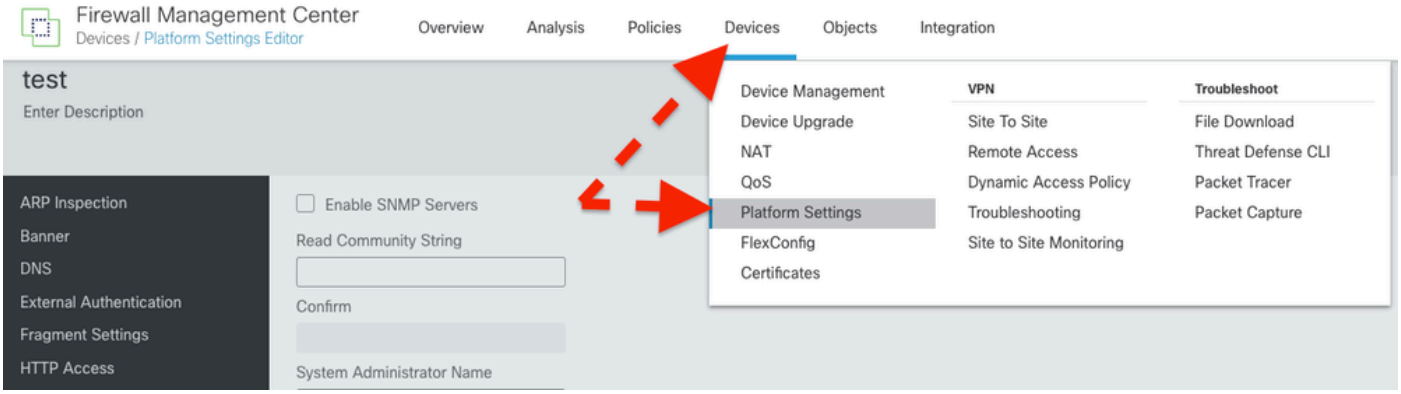
Cisco Firepower Threat Defense(FTD)ソフトウェアバージョン7.2.6には、Cisco Bug ID CSCwi63113が含まれており、SNMPが有効な場合に一部のデバイスでのブートが妨げられています。7.2.6をインストールする前に、7.2.7以降にアップグレードできるまでSNMPをディセーブルにしてください。この問題の修正は現在準備中です。2024年5月3日までに7.2.7としてリリースされる予定です。さらに、シスコは2024年5月6日までに7.2.5.2をリリースする予定です。これは、CVE-2024-20353、CVE-2024-20359、およびCVE-2024-20358の修正のみによる7.2.5.1です。

アップグレードの前にSNMPを無効にする

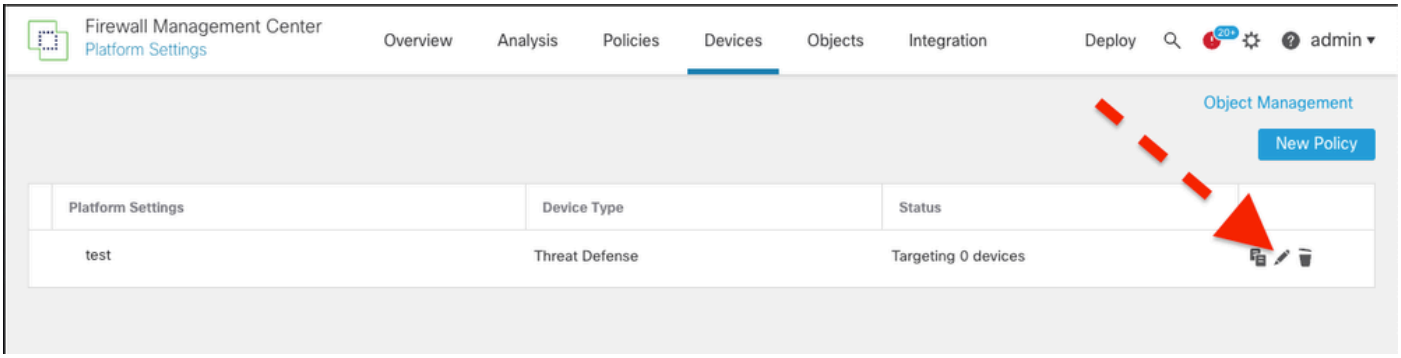
FMCの手順：

ステップ1:FMCにログインします。

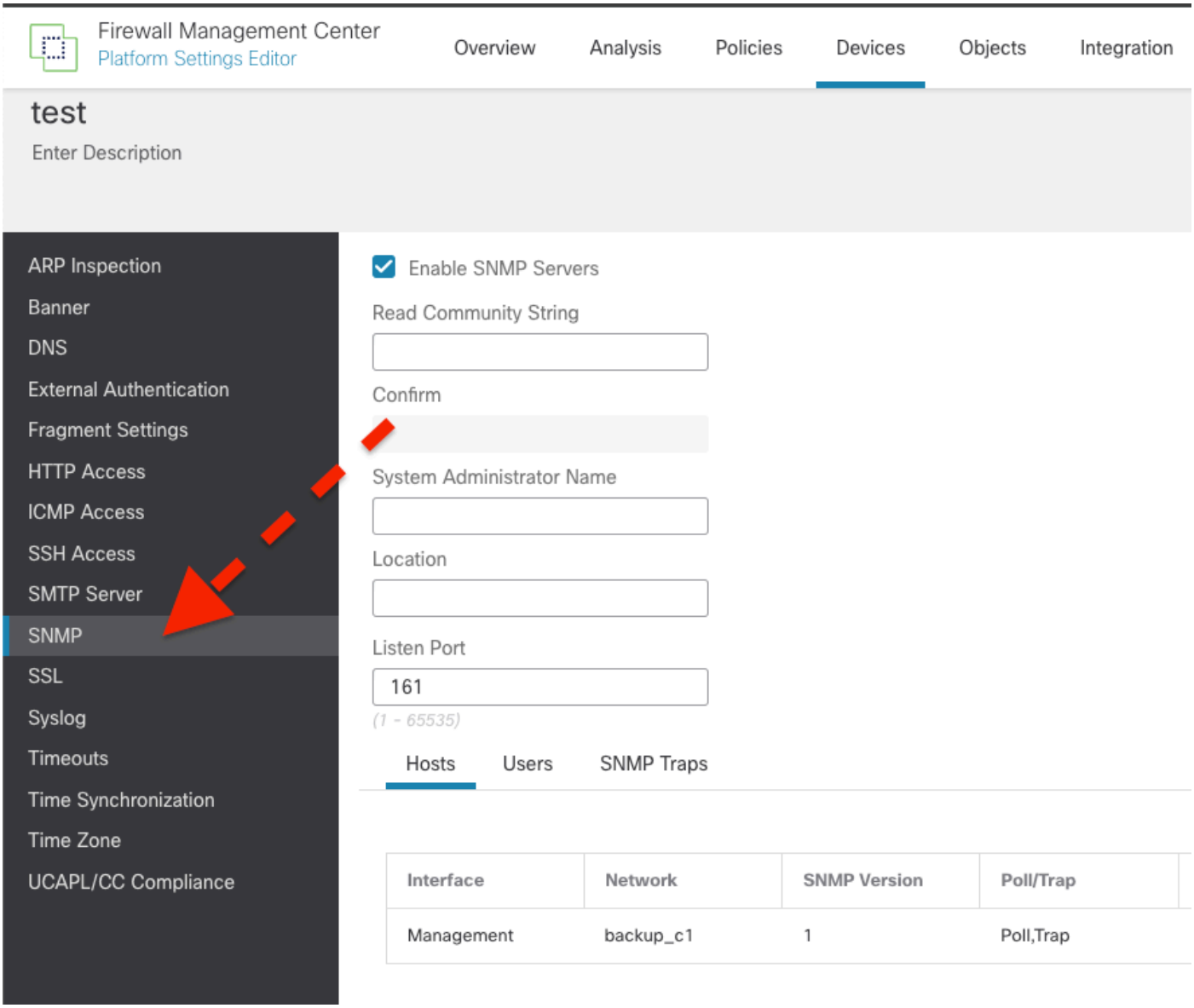
ステップ2：デバイス>プラットフォーム設定に移動します



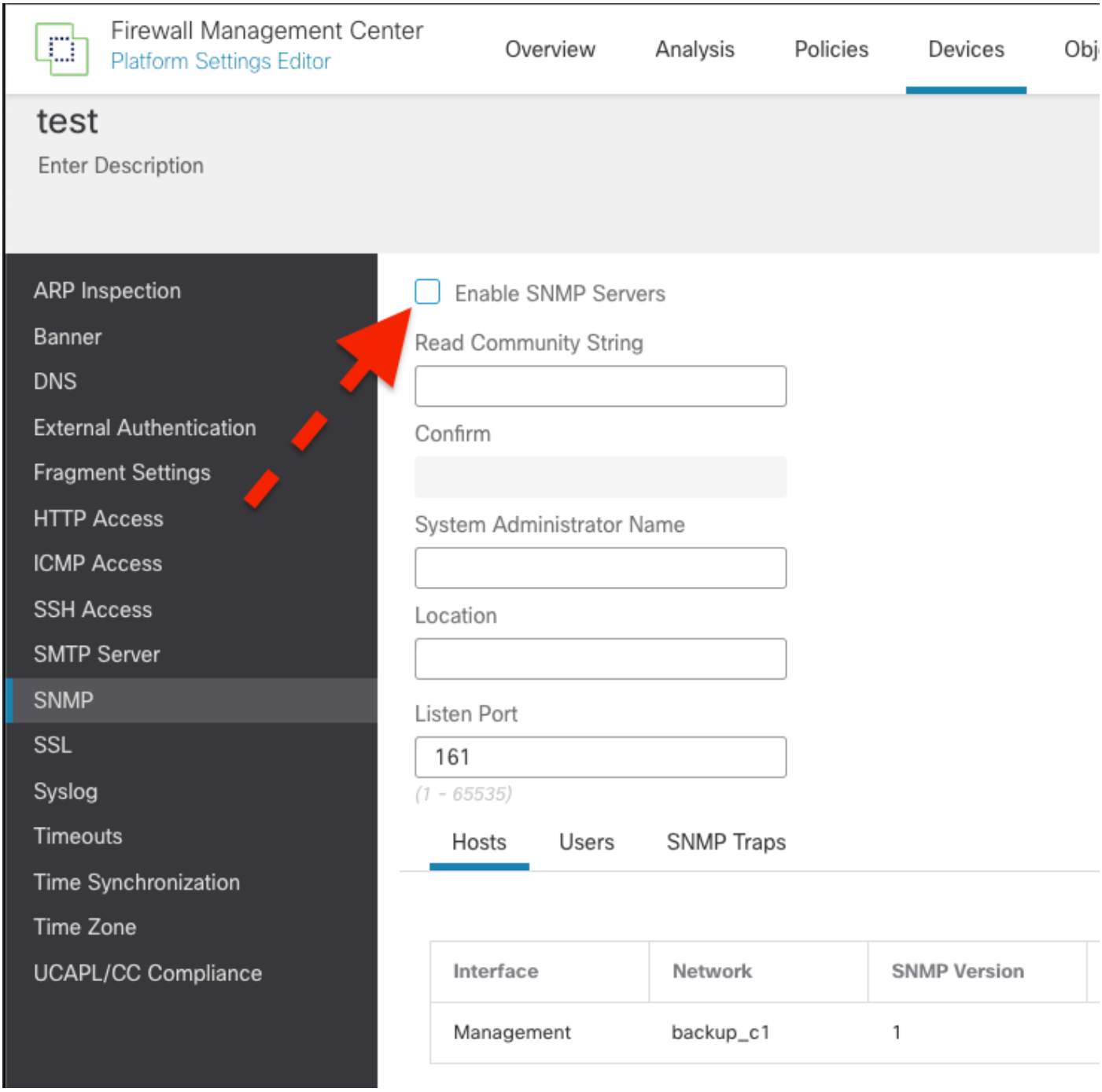
ステップ3:FTDデバイスに関連付けられたポリシーを編集します。



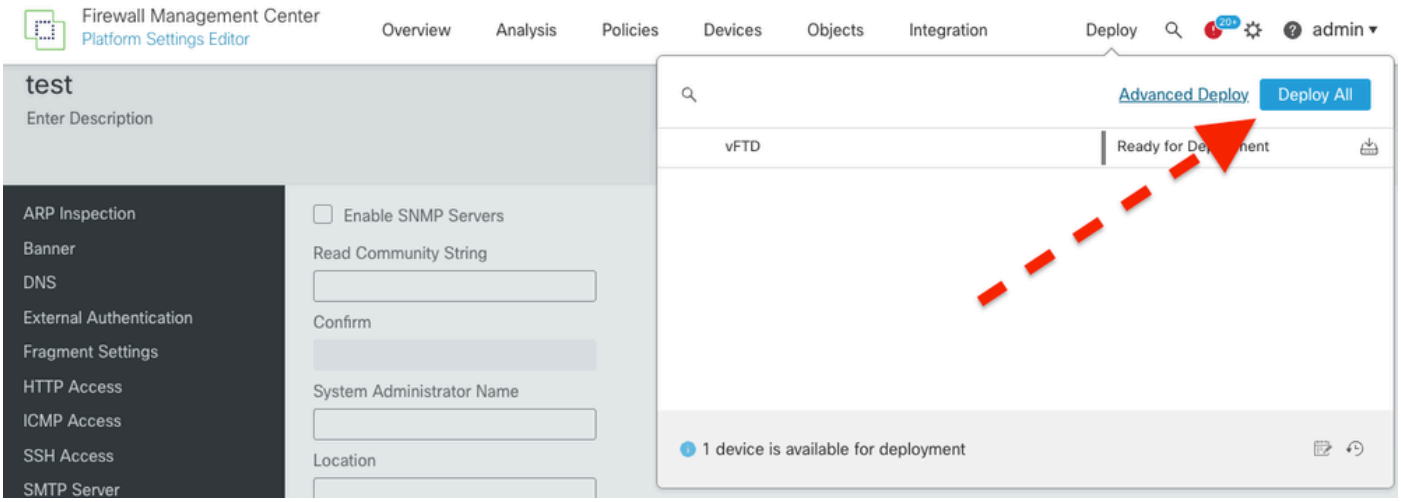
ステップ4:SNMPの選択



ステップ5:SNMPサーバを無効にする



ステップ6：ポリシーに保存して展開します。



最新不具合については、Cisco Bug ID CSCwi63113を参照してください。

詳細については、Cisco TAC(support.cisco.com)に問い合わせ、Arcane Door(cisco-sa-asaftd-persist-rce-FLsNXF4h / CVE-2024-20359)を参照してください

アップグレード済みで、ブートループが発生している場合の対処法：

すでに7.2.6にアップデートしていて、Cisco Bug ID CSCwi63113の影響を受ける場合は、Cisco TAC(support.cisco.com)にお問い合せください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。