CSMへのセキュアなファイアウォールASAのプロビジョニング

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[背景説明](#)

[設定](#)

- [コンフィギュレーション](#)
  - [HTTPS管理のためのASAの設定](#)
  - [CSMへのセキュアなファイアウォールASAのプロビジョニング](#)

[確認](#)

はじめに

このドキュメントでは、Cisco Security Manager(CSM)にセキュアファイアウォール適応型セキュリティアプライアンス(ASA)をプロビジョニングするプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュアなファイアウォールASA
- CSM

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- セキュアファイアウォールASAバージョン9.18.3
- CSM バージョン 4.28

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

CSMは、一貫したポリシーの適用とセキュリティイベントの迅速なトラブルシューティングを可能にし、セキュリティ導入全体の要約レポートを提供します。一元化されたインターフェイスを使用して、組織は効率的に拡張し、可視性が向上したさまざまなシスコのセキュリティデバイスを管理できます。

設定

次の例では、仮想ASAがCSMにプロビジョニングされ、中央集中型管理が行われます。

コンフィギュレーション

HTTPS管理のためのASAの設定

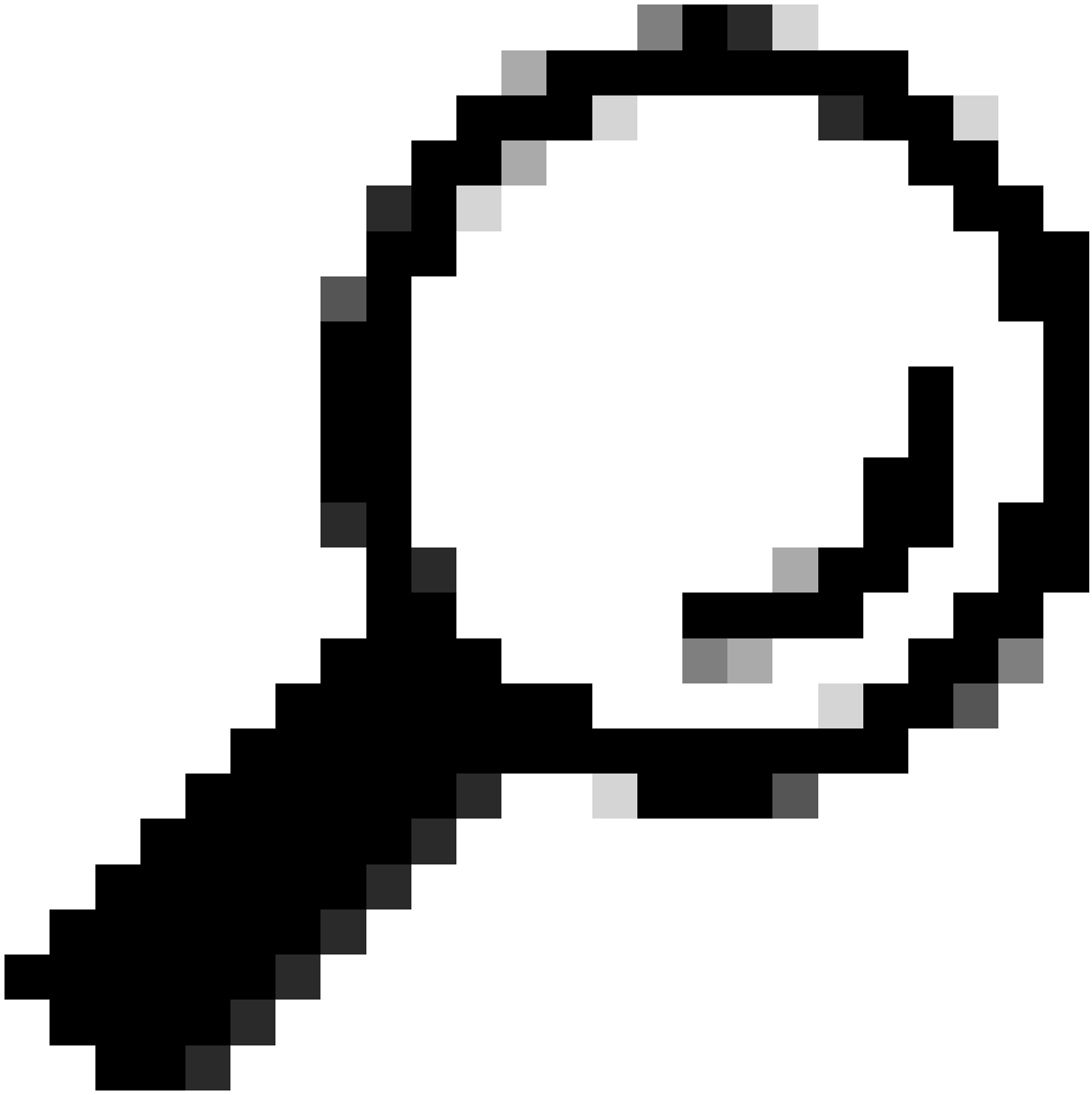
ステップ 1：すべての権限を持つユーザを作成します。

コマンドライン(CLI)構文：

```
configure terminal
username < user string > password < password > privilege < level number >
```

これは、次のコマンド例のユーザcsm-userとパスワードcisco123を意味します。

```
ciscoasa# configure terminal
ciscoasa(config)# username csm-user password cisco123 privilege 15
```



ヒント：この統合では、外部認証ユーザも受け入れられます。

ステップ 2：HTTPサーバを有効にします。

コマンドライン(CLI)構文：

```
configure terminal
http server enable
```

ステップ 3：CSMサーバのIPアドレスに対してHTTPSアクセスを許可します。

コマンドライン(CLI)構文：

```
configure terminal
http < hostname > < netmask > < interface name >
```

これは次のコマンド例の変換であり、任意のネットワークが外部インターフェイス(GigabitEthernet0/0)上のHTTPS経由でASAにアクセスできます。

```
ciscoasa# configure terminal
ciscoasa(config)# http 0.0.0.0 0.0.0.0 outside
```

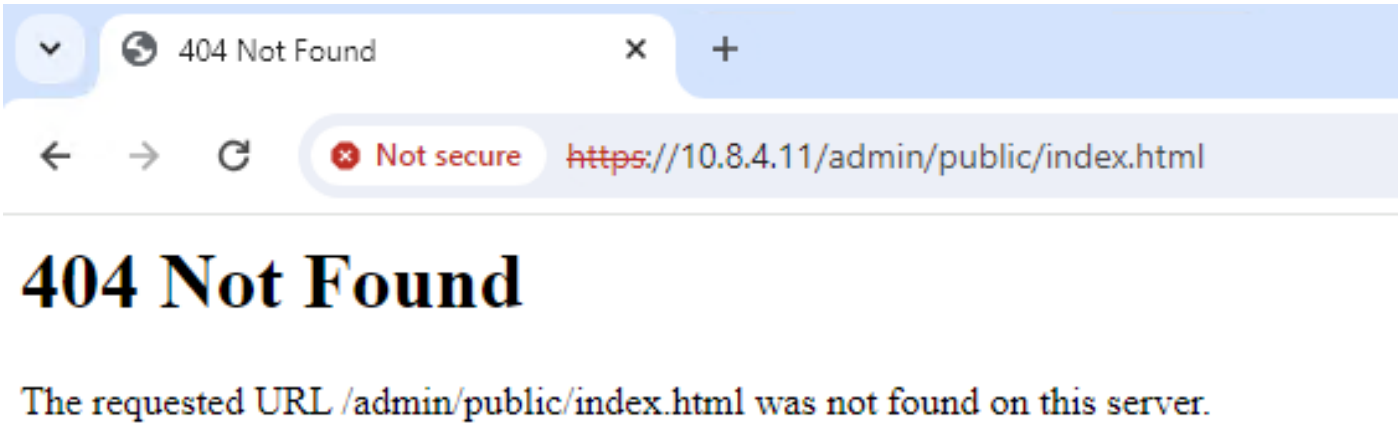
ステップ 4：CSMサーバからHTTPSに到達できることを確認します。

任意のWebブラウザを開き、次の構文を入力します。

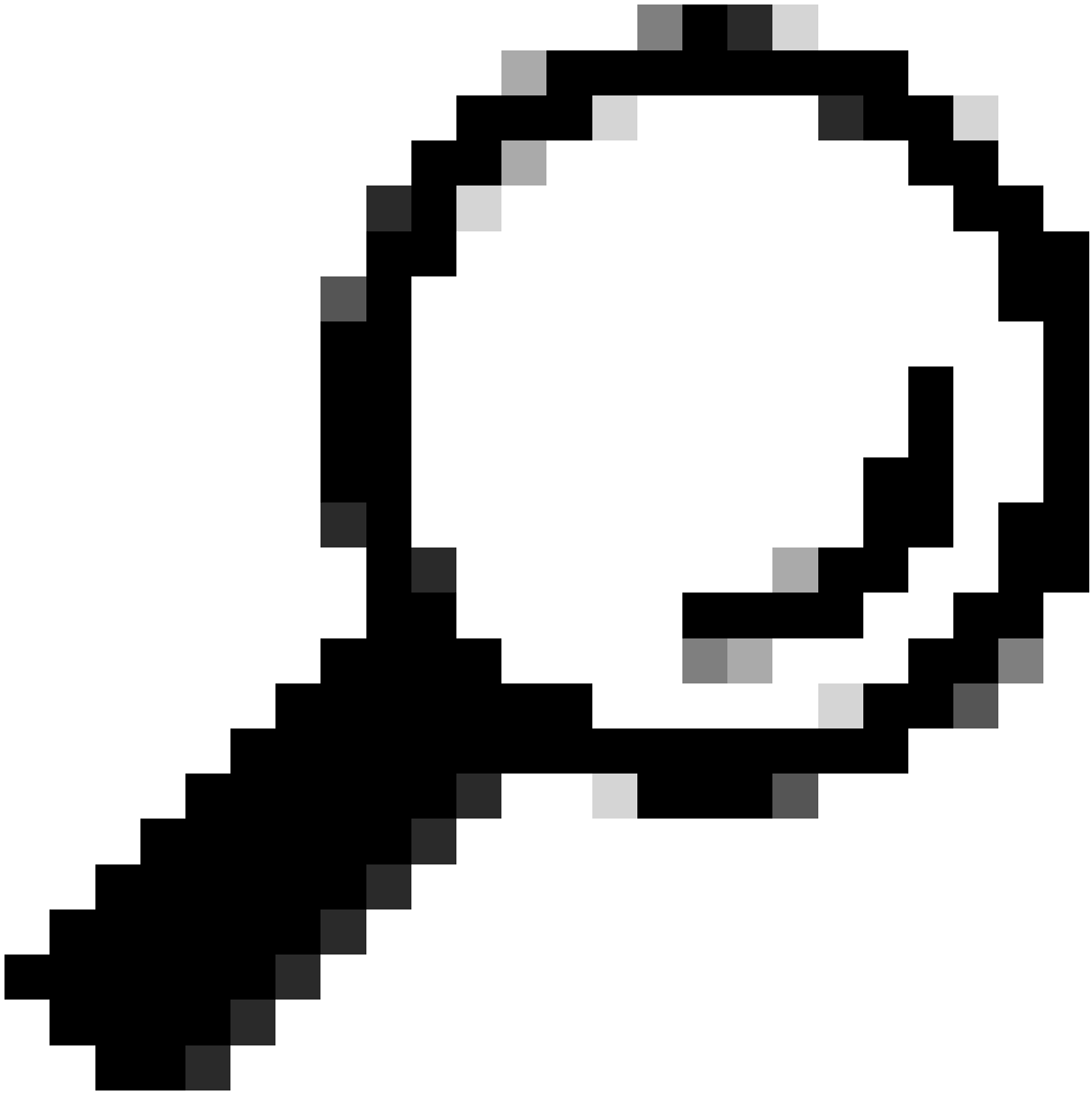
```
https://< ASA IP address >/
```

これは、前の手順でHTTPSアクセスに許可された外部インターフェイスのIPアドレスの次の例を示しています。

```
https://10.8.4.11/
```



ASAのHTTPS応答



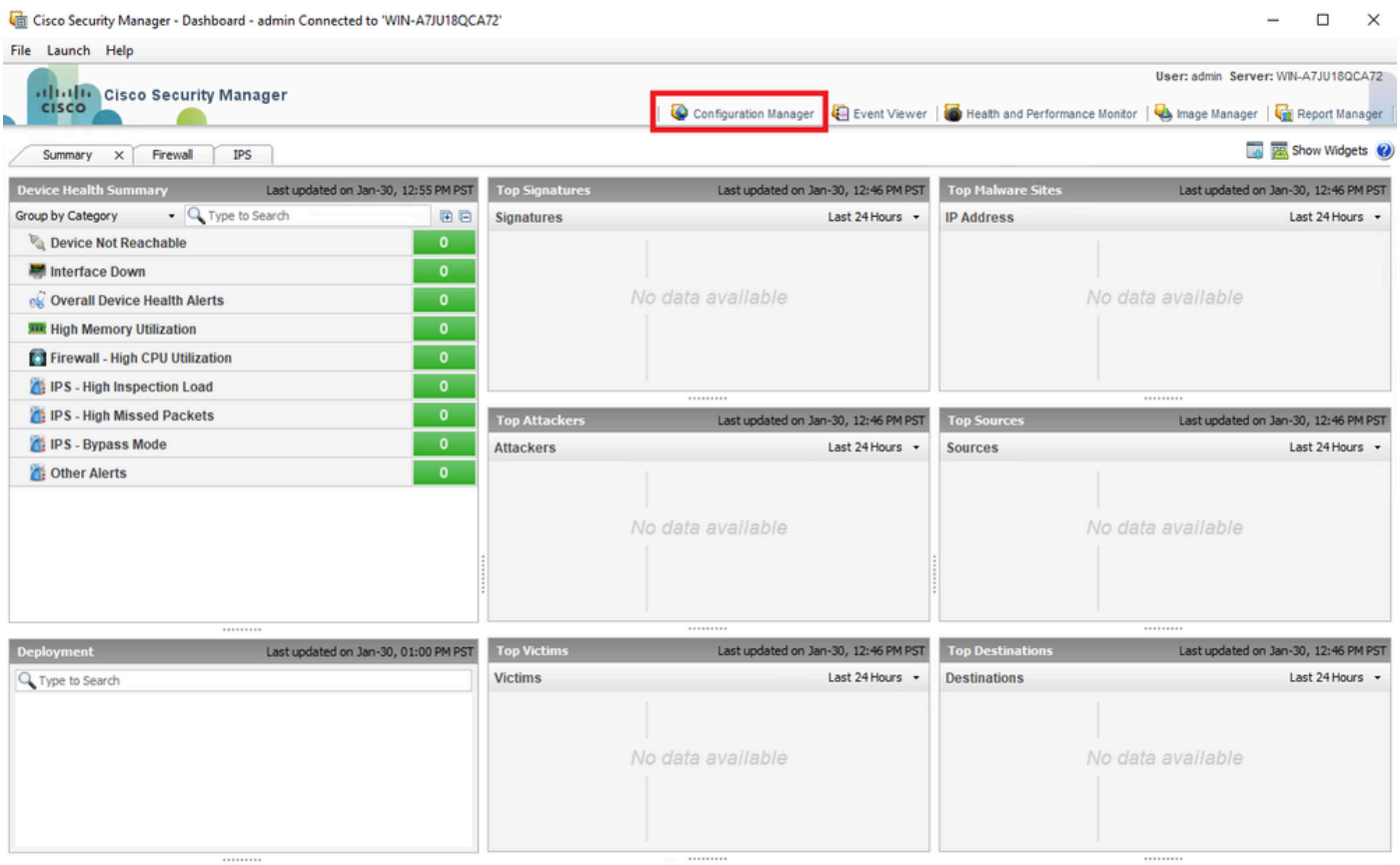
ヒント：このASAにはCisco Adaptive Security Device Manager(ASDM)がインストールされていないのに、ページがURL /admin/public/index.htmlにリダイレクトされるので、このステップではエラー404 Not Foundが予期されます。

CSMへのセキュアなファイアウォールASAのプロビジョニング

ステップ 1：CSMクライアントを開いてログインします。

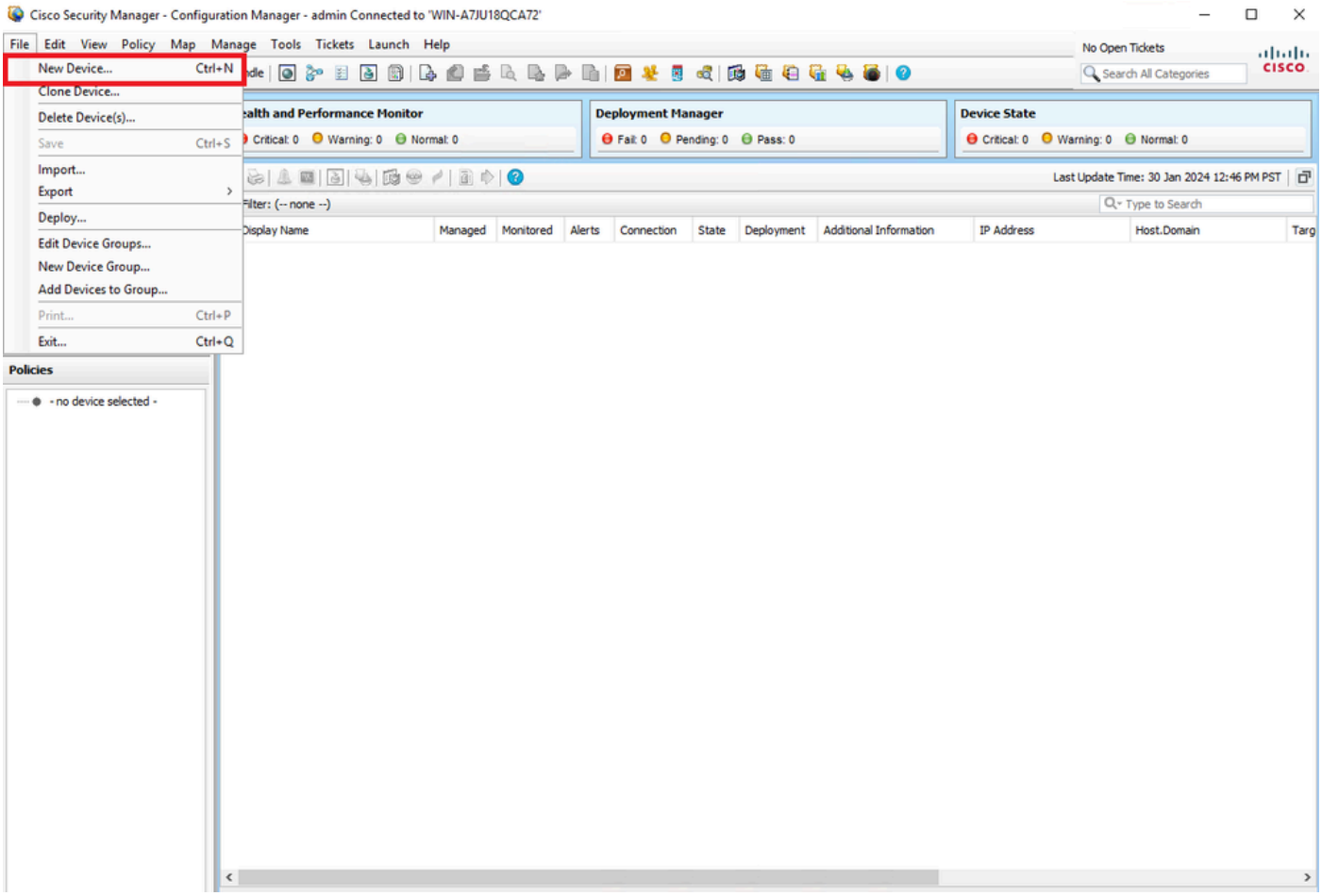
CSMクライアントログイン

ステップ 2：Configuration Managerを開きます。



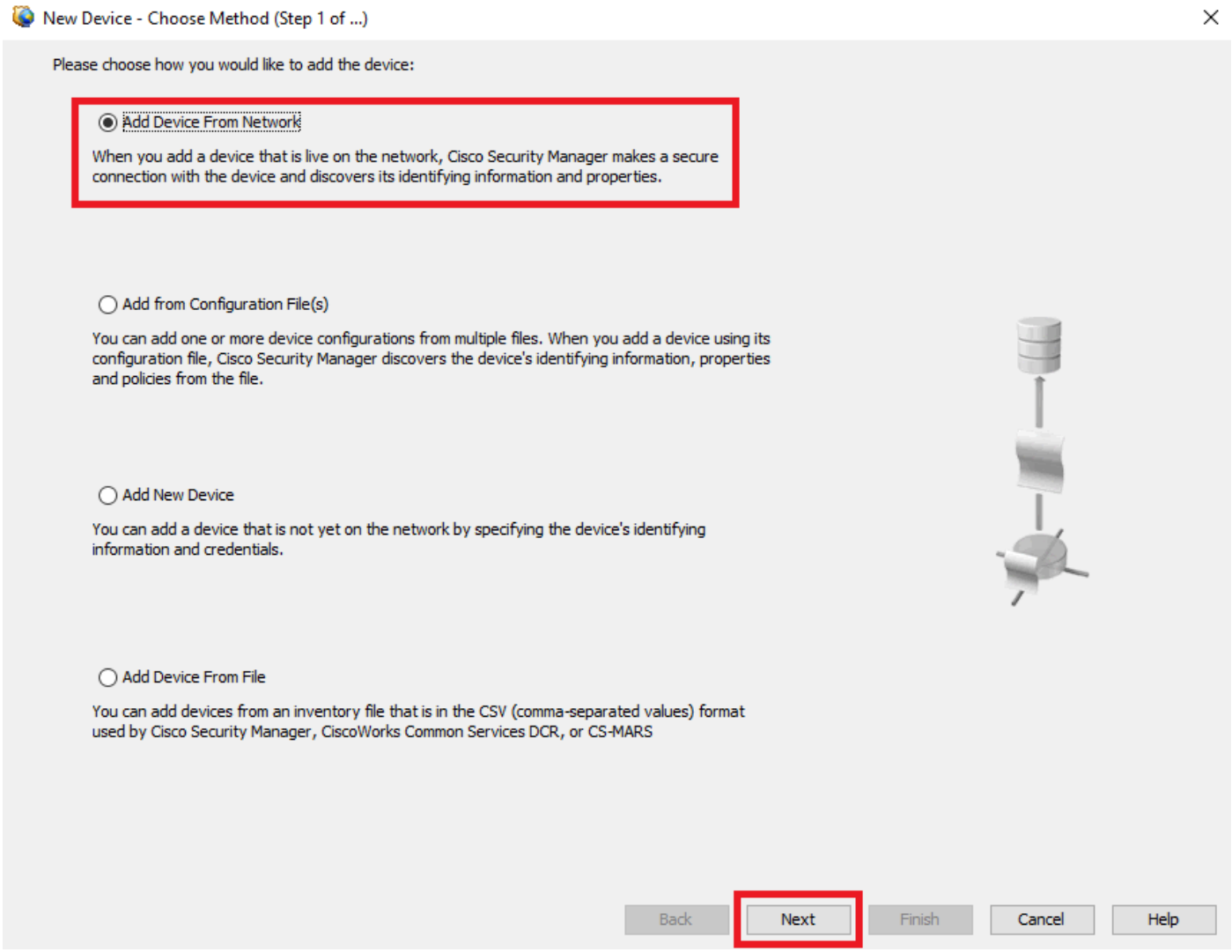
CSMクライアントダッシュボード

ステップ 3：Devices > New Deviceの順に移動します。



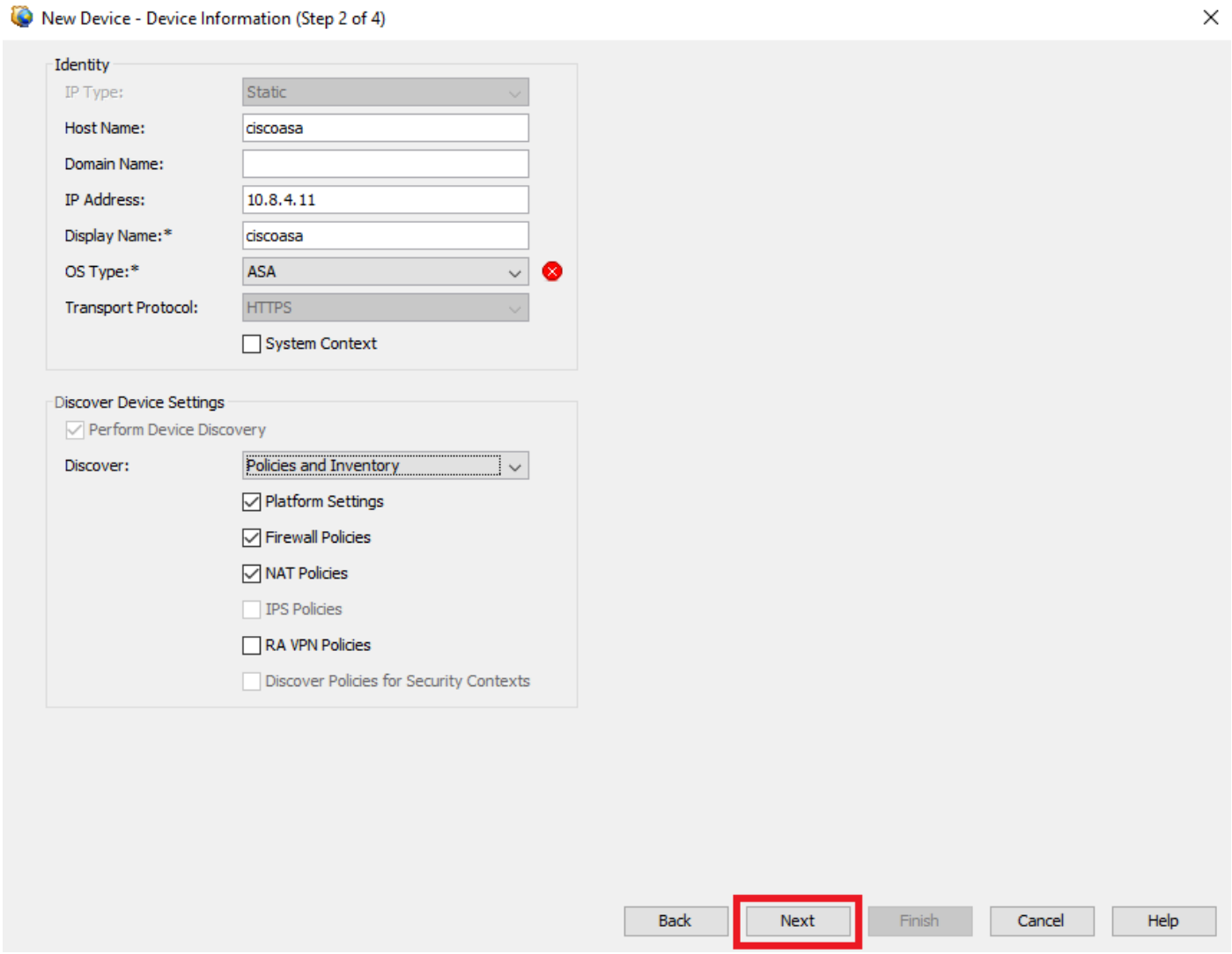
*CSM*コンフィギュレーションマネージャ

ステップ 4：目的の結果に応じて要件を満たす追加オプションを選択します。設定済みのASAがすでにネットワークに設定されているため、この例の最適なオプションは**Add Device From Network**であり、**Next**をクリックします。



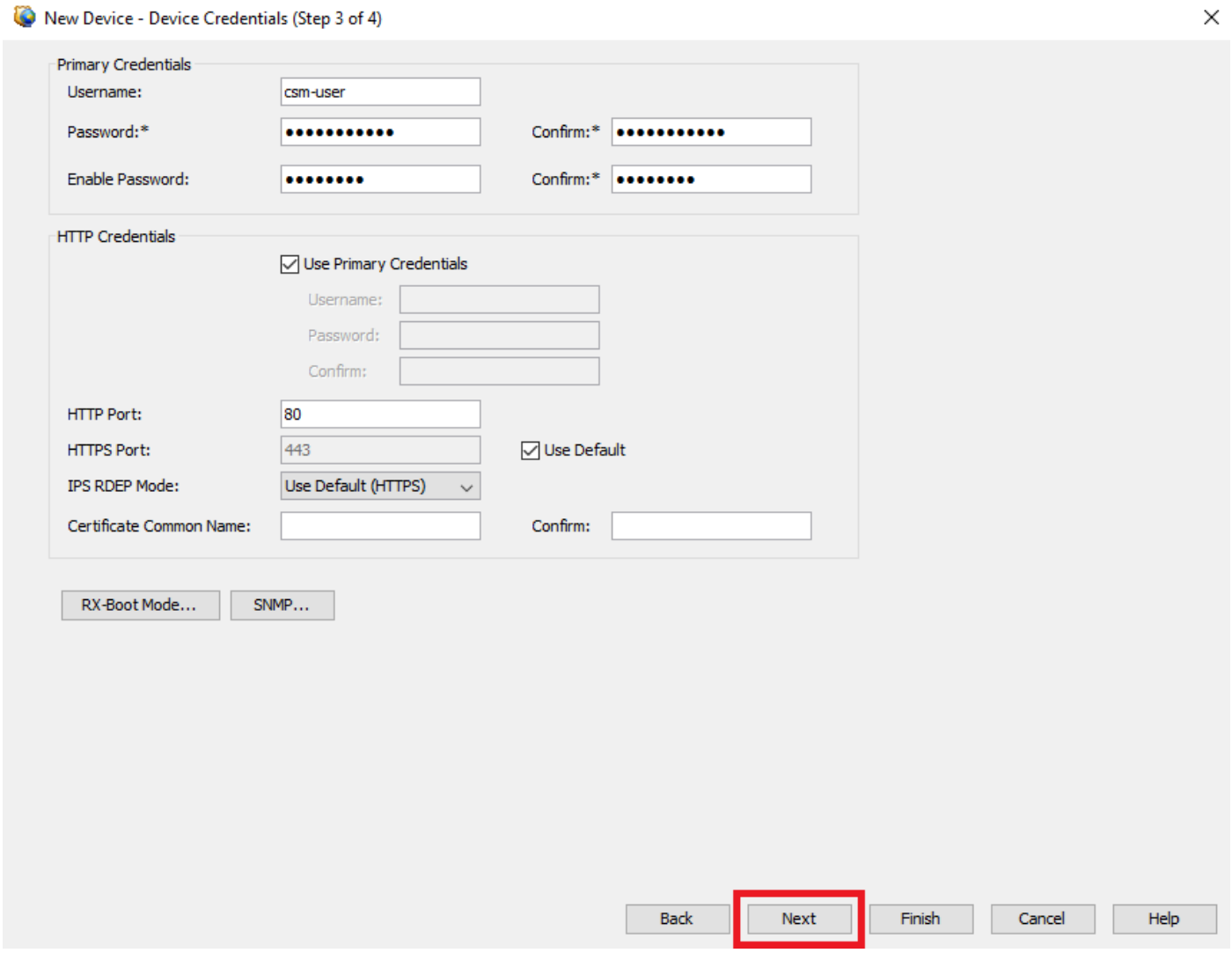
*Device Add*メソッド

ステップ 5：セキュアファイアウォールASAの設定とディスカバリ設定に従って、必要なデータを入力します。次に**Next**をクリックします。



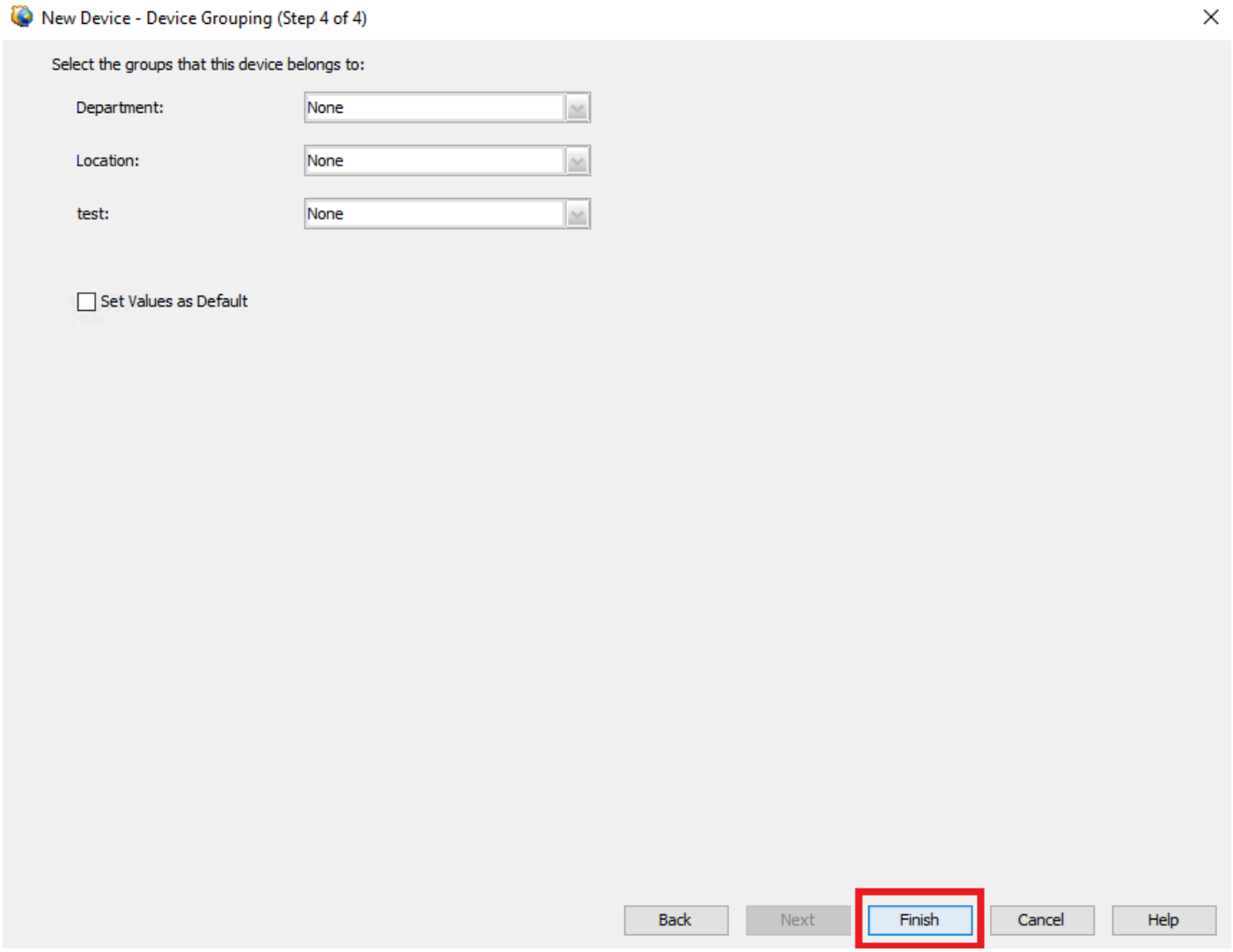
*ASA*の設定

手順 6：ASAで設定したCSMユーザと**enable**パスワードの両方から、必要なクレデンシャルを入力します。



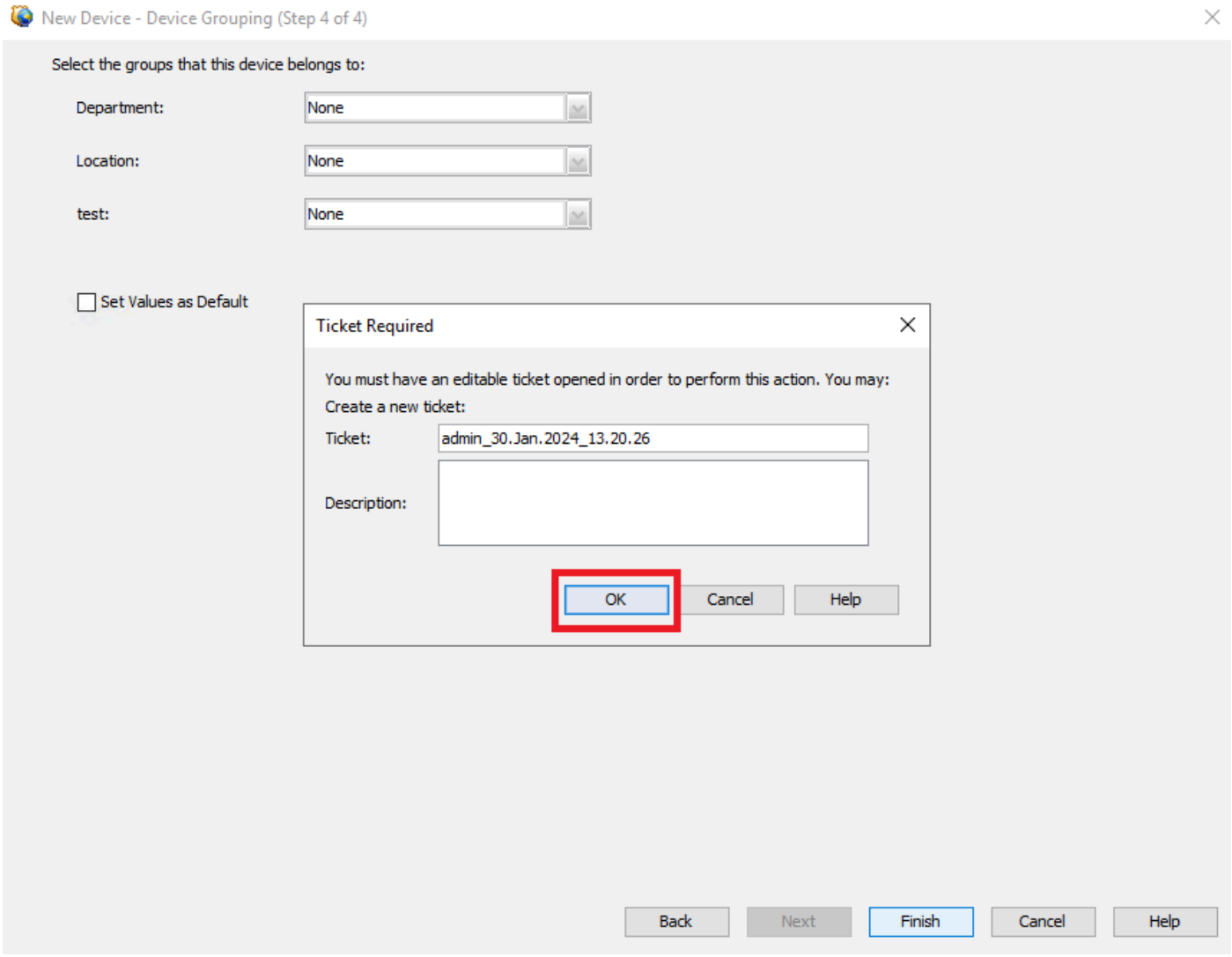
*ASA*クレデンシャル

手順 7：必要なグループを選択するか、不要な場合はこのステップを省略して、**Finish**をクリックします。



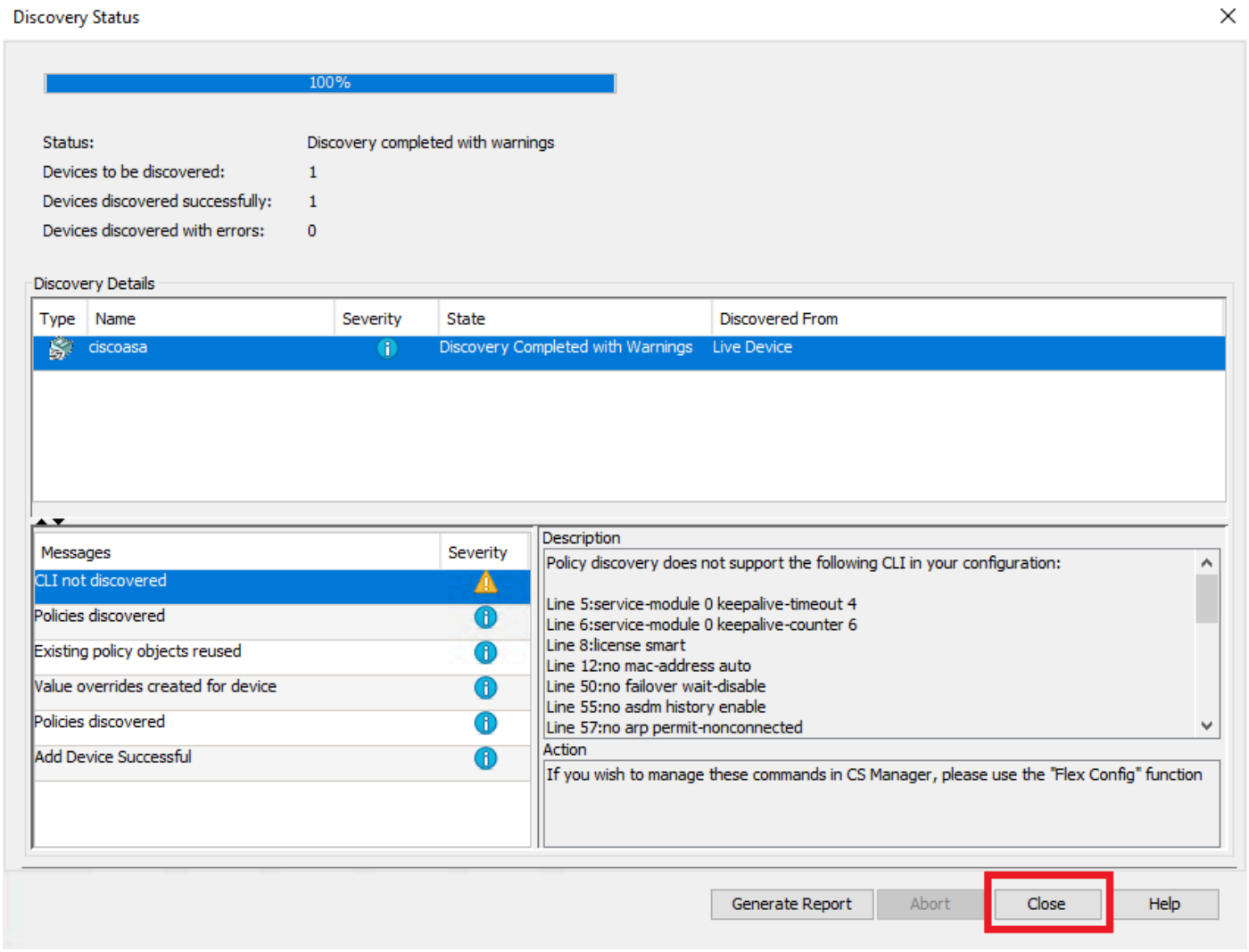
CSMグループの選択

ステップ 8：チケット要求が制御目的で生成された場合は、**OK**をクリックします。

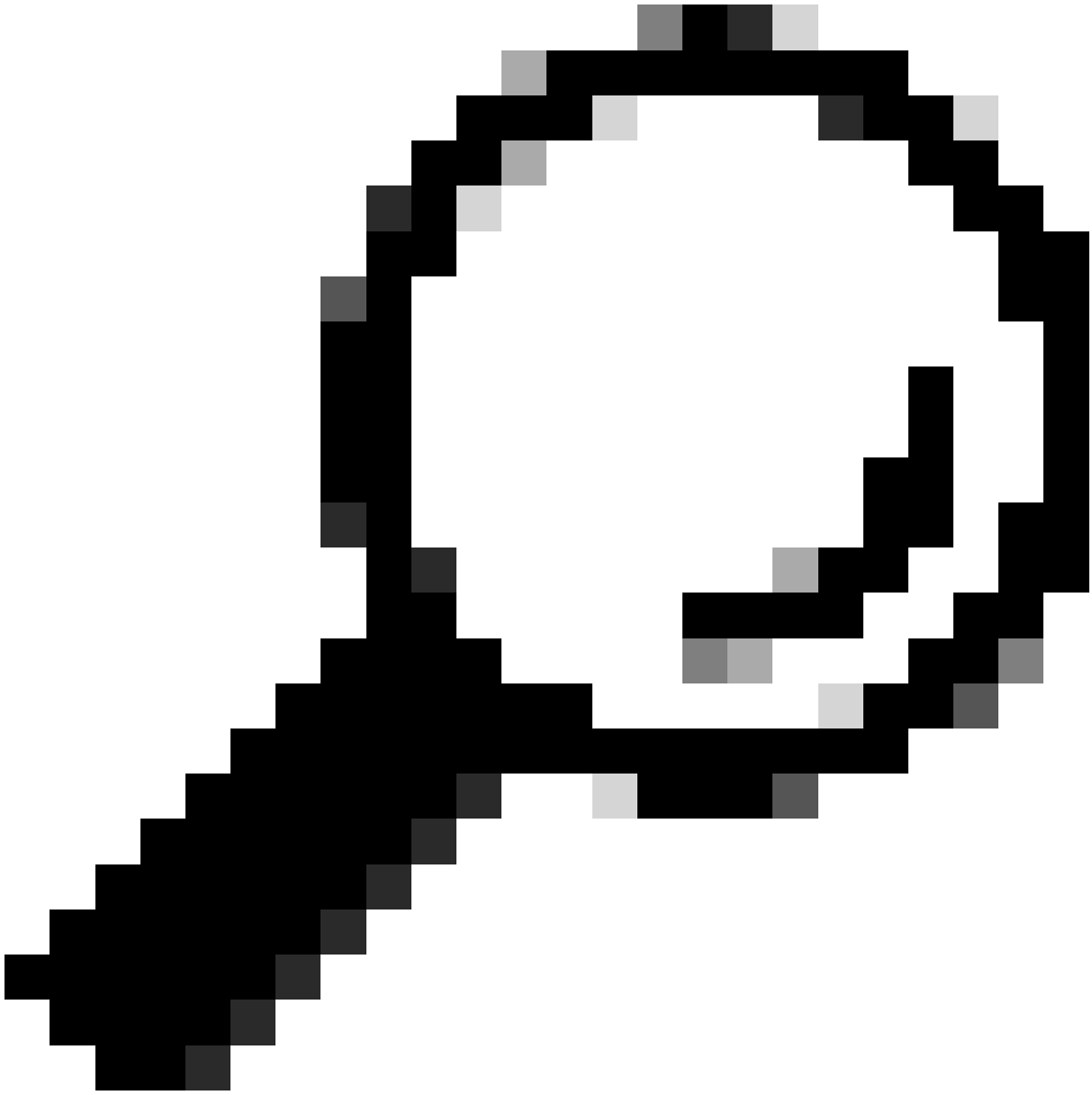


*CSM*チケットの作成

ステップ 9：検出がエラーなしで終了することを検証し、**Close**をクリックします。

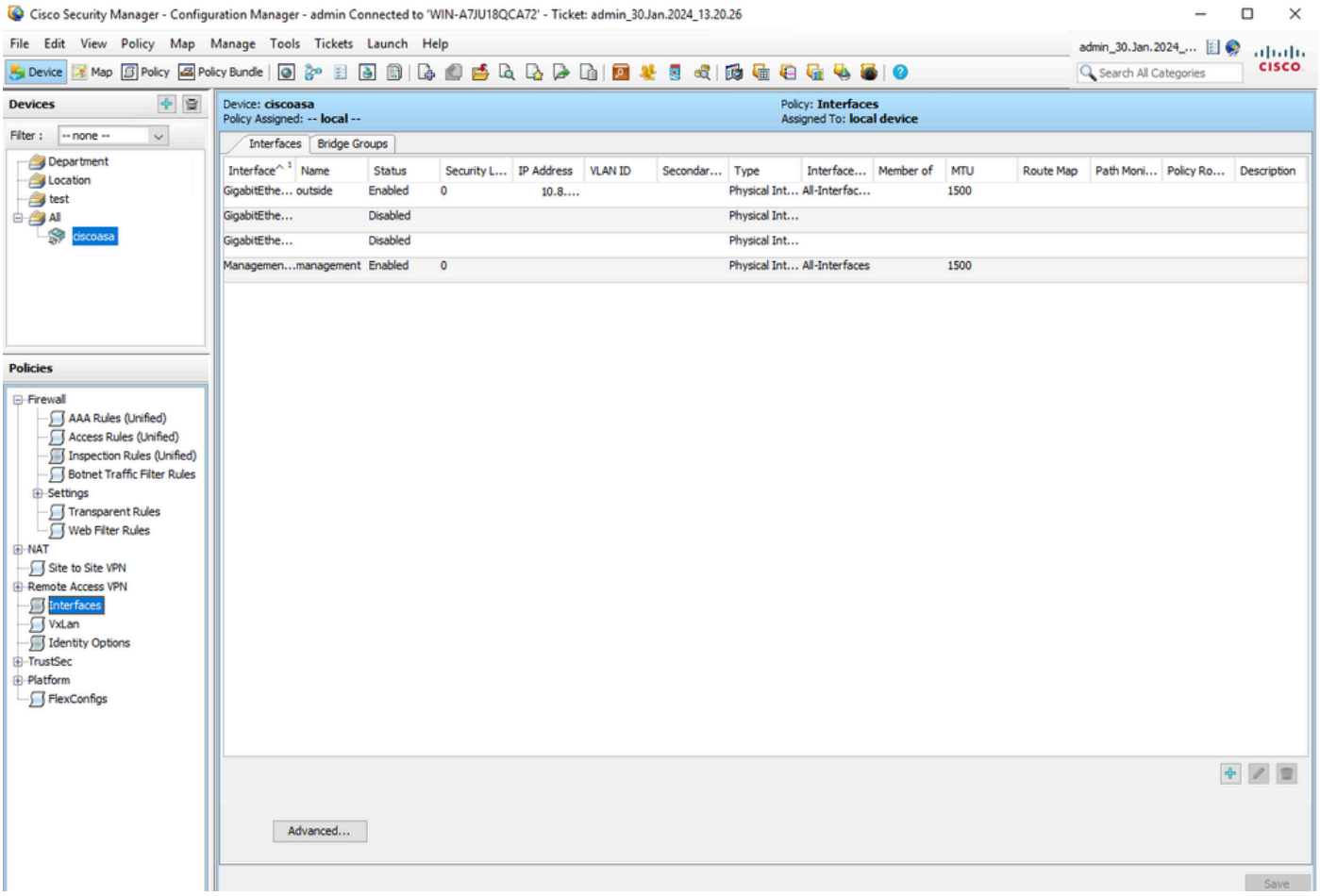

Discovery Status
100%
Status: Discovery completed with warnings
Devices to be discovered: 1
Devices discovered successfully: 1
Devices discovered with errors: 0
Discovery Details
Type Name Severity State Discovered From
ciscoasa Discovery Completed with Warnings Live Device
Messages Severity
CLI not discovered
Policies discovered
Existing policy objects reused
Value overrides created for device
Policies discovered
Add Device Successful
Description
Policy discovery does not support the following CLI in your configuration:
Line 5:service-module 0 keepalive-timeout 4
Line 6:service-module 0 keepalive-counter 6
Line 8:license smart
Line 12:no mac-address auto
Line 50:no failover wait-disable
Line 55:no asdm history enable
Line 57:no arp permit-nonconnected
Action
If you wish to manage these commands in CS Manager, please use the "Flex Config" function
Generate Report
Abort
Close
Help

ASAディスカバリ



ヒント:CSMではすべてのASA機能がサポートされているわけではないため、警告は正常な出力として受け入れられます。

ステップ 10：CSMクライアントでASAが登録済みとして表示され、正しい情報が表示されていることを確認します。



登録されたASA情報

確認

HTTPSデバッグは、トラブルシューティングの目的でASAで使用できます。次のコマンドを使用します。

```
debug http
```

CSM登録のデバッグが成功した例を次に示します。

```
ciscoasa# debug http debug http enabled at level 1. ciscoasa# HTTP: processing handoff to legacy admin
```

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。