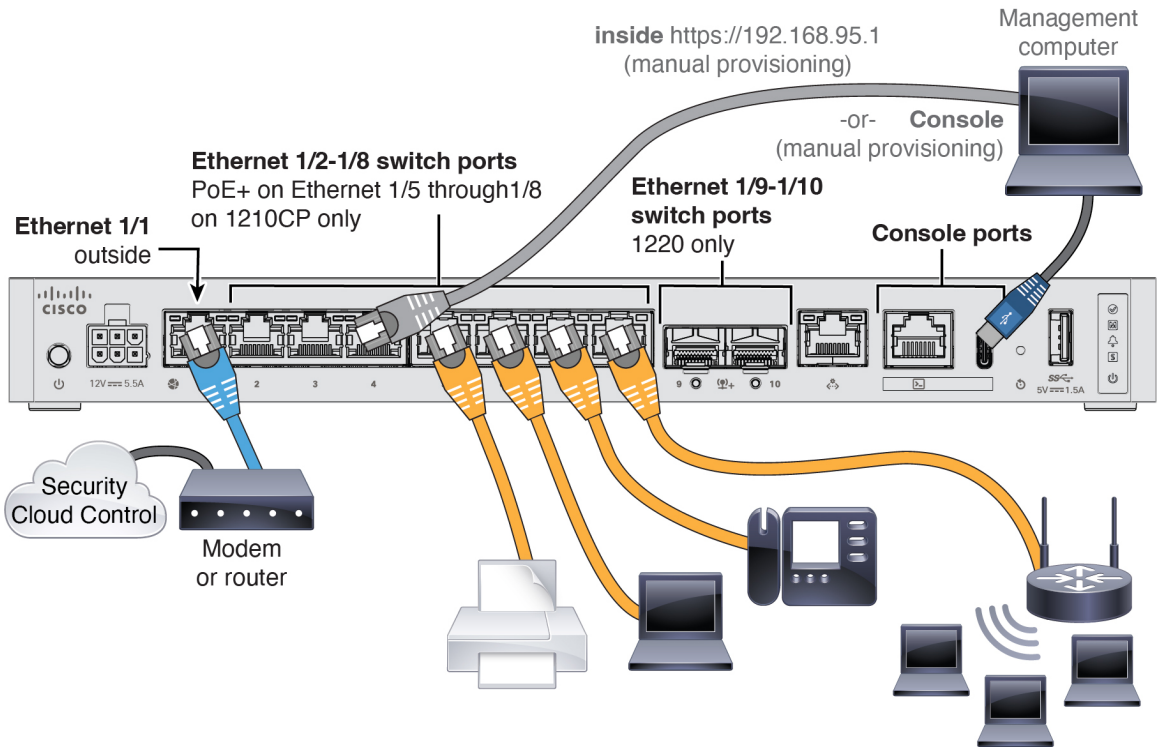
ファイアウォールのケーブル接続とオンボード

ファイアウォールをケーブル接続し、Security Cloud Control にオンボードします。

ファイアウォールのケーブル接続

- Cisco Secure Firewall 1220 の場合は、SFP をイーサネット 1/9 および 1/10 ポートに取り付けます。このポートは、SFP/SFP+ モジュールを必要とする 1/10 Gb SFP+ ポートです。
- 詳細については、ハードウェア設置ガイドを参照してください。
- ゼロタッチプロビジョニングで高可用性を使用する場合を除き、管理インターフェイスをケーブル接続しないでください。この場合は、Cisco Security Cloud Control のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理を参照してください。このガイドでは、ゼロタッチプロビジョニングの外部インターフェイスについてのみ説明します。



ファイアウォールの Security Cloud Control へのオンボード

ゼロタッチプロビジョニングまたは手動プロビジョニングを使用してファイアウォールをオンボードします。

ゼロタッチプロビジョニングによるファイアウォールをオンボード

ゼロタッチプロビジョニング とデバイスのシリアル番号を使用して Threat Defense を導入準備します。

手順

ステップ 1 Security Cloud Control のナビゲーションウィンドウで **セキュリティデバイス** をクリックし、青色のプラスボタン（ ）をクリックしてデバイスを [オンボード（Onboard）] します。

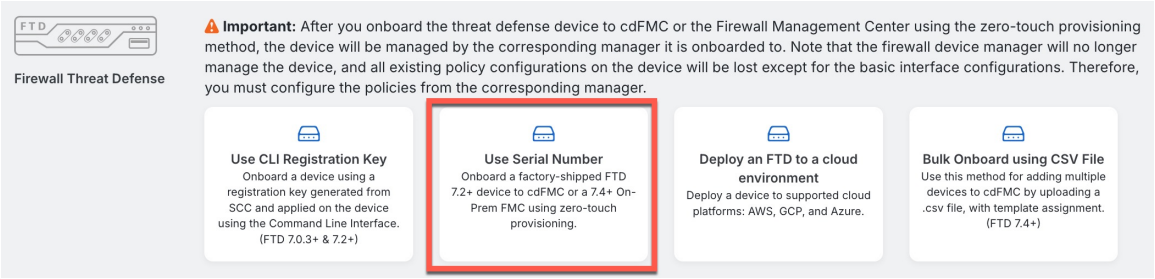
ステップ 2 [FTD] タイルを選択します。

ステップ 3 [管理モード] で、[FTD] が選択されていることを確認します。

管理モードとして [FTD] を選択した後はいつでも、[スマートライセンスの管理] をクリックして、デバイスで使用可能な既存のスマートライセンスに登録または変更できます。使用可能なライセンスについては、ライセンスを取得する を参照してください。

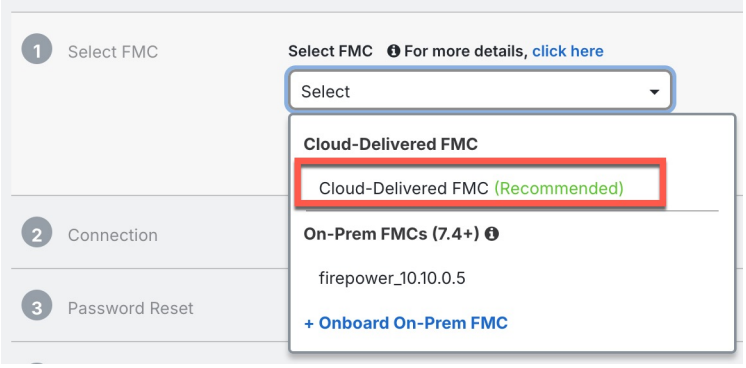
ステップ 4 オンボーディング方法として [シリアル番号を使用（Use Serial Number）] を選択します。

図 *1* : シリアル番号を使用



ステップ 5 [FMCの選択（Select FMC）] で、リストから [クラウド提供型FMC（Cloud-Delivered FMC）]、[Firewall Management Center] の順に選択し、[次へ（Next）] をクリックします。 >

図 *2* : *FMC*の選択



ステップ 6 [接続（Connection）]エリアで、[デバイスのシリアル番号（Device Serial Number）] と [デバイス名（Device Serial Number）] を入力し、[次へ（Next）] をクリックします。

図 *3* : 接続

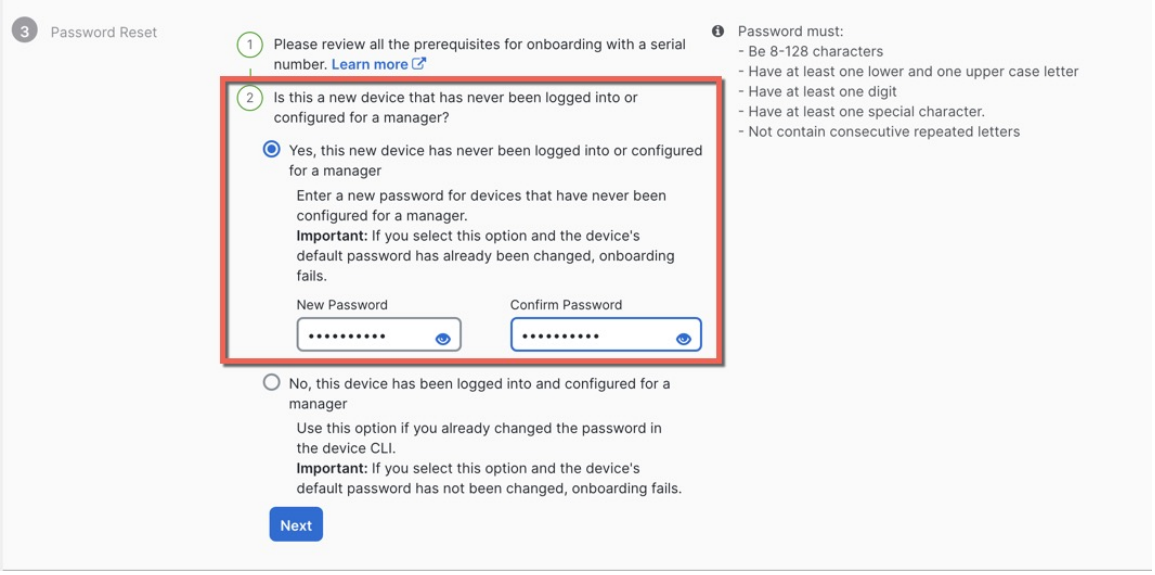
ステップ 7 **[パスワードのリセット（Password Reset）]** で、**[はい...（Yes...）]** をクリックします。デバイスの新しいパスワードを入力し、この新しいパスワードを確認して、[次へ（Next）] をクリックします。

ゼロタッチプロビジョニング の場合、デバイスは新規であるか、再イメージ化されている必要があります。

（注）

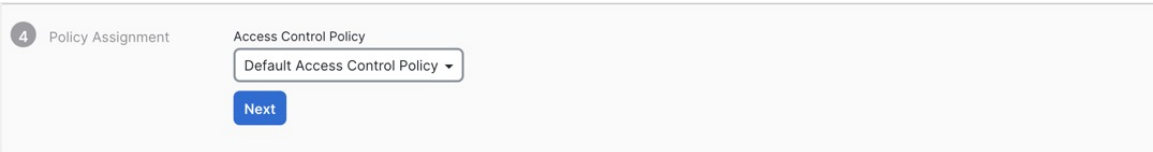
デバイスにログインしてパスワードをリセットし、ゼロタッチプロビジョニング を無効にするように設定を変更しなかった場合は、[いいえ...（No...）]オプションを選択する必要があります。ゼロタッチプロビジョニングプロビジョニングを無効にする設定は多数あるため、再イメージ化などの必要がある場合を除き、デバイスにログインすることは推奨されません。

図 *4:* パスワードのリセット



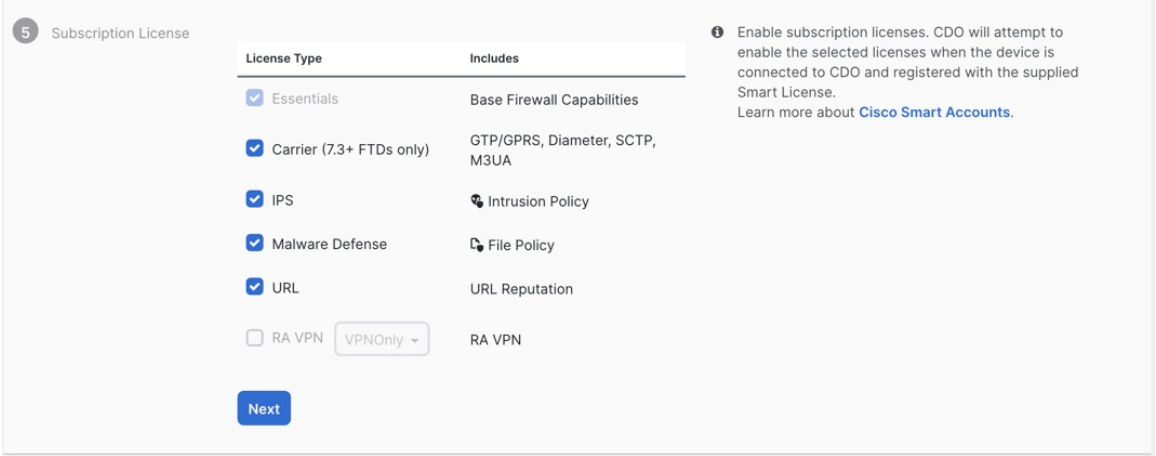
ステップ 8 [ポリシー割り当て（Policy Assignment）]については、ドロップダウンメニューを使用して、デバイスのアクセス コントロール ポリシーを選択します。ポリシーが設定されていない場合は、[デフォルトのアクセスコントロールポリシー（Default Access Control Policy）] を選択します。

図 *5:* ポリシー割り当て



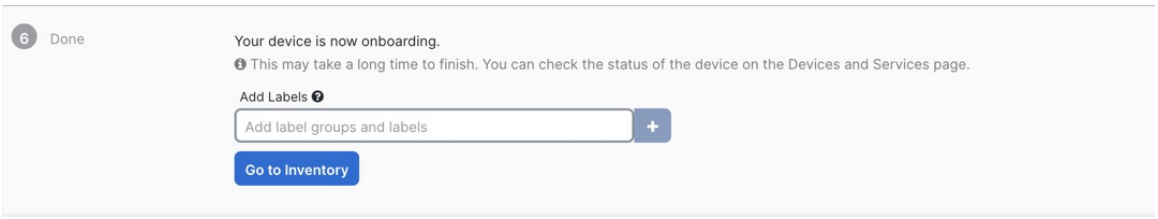
ステップ 9 [サブスクリプションライセンス（Subscription License）] については、有効にする各機能ライセンスをチェックします。[Next] をクリックします。

図 *6*:サブスクリプションライセンス



ステップ 10 （任意）[セキュリティデバイス（Security Devices）] ページの並べ替えとフィルタ処理に役立つラベルをデバイスに追加します。ラベルを入力し、青いプラスボタン（ ）を選択します。ラベルは、Security Cloud Control への導入準備後にデバイスに適用されます。

図 *7*:終了



次のタスク

[セキュリティデバイス（Security Devices）] ページから、導入準備したばかりのデバイスを選択し、右側にある [管理（Management）] ペインに一覧表示されているオプションのいずれかを選択します。

手動プロビジョニングによるファイアウォールをオンボード

CLI 登録キーを使用してファイアウォールをオンボードします。

手順

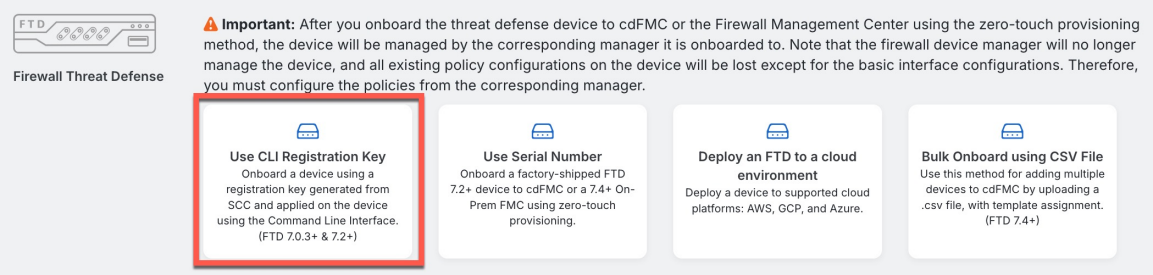
ステップ 1 Security Cloud Control のナビゲーションウィンドウで **セキュリティデバイス** をクリックし、青色のプラスボタン（ ）をクリックしてデバイスを [オンボード（Onboard）] します。

ステップ 2 [FTD] タイルをクリックします。

ステップ 3 [管理モード] で、[FTD] が選択されていることを確認します。

ステップ 4 オンボーディング方法として [CLI登録キーを使用（Use CLI Registration Key）] を選択します。

図 *8 : CLI* 登録キーを使用

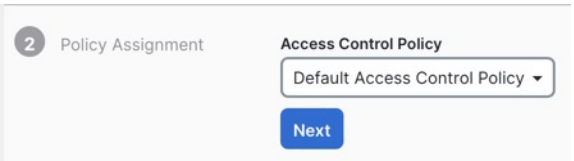


ステップ 5 [デバイス名（Device Name）] を入力して、[次へ（Next）] をクリックします。

図 *9 :* デバイス名

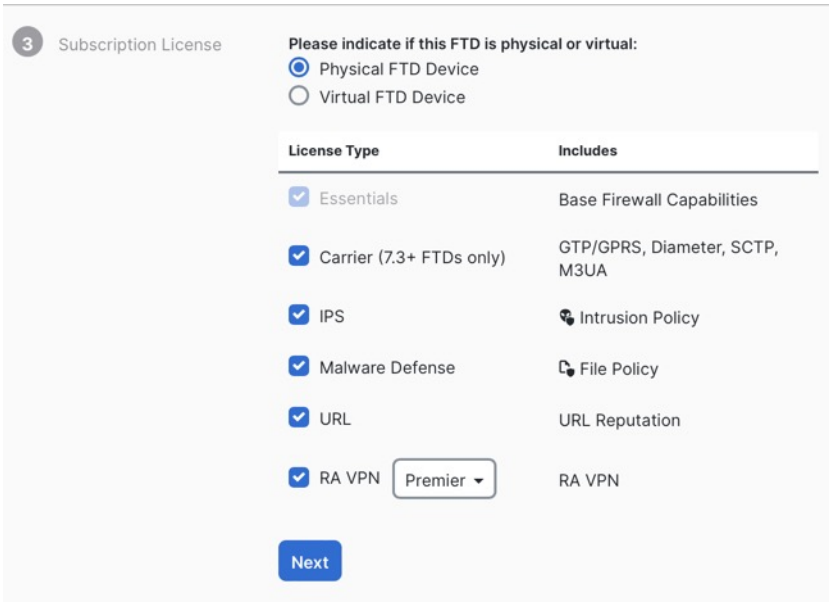
ステップ 6 [ポリシー割り当て（Policy Assignment）] については、ドロップダウンメニューを使用して、デバイスのアクセス コントロール ポリシーを選択します。ポリシーが設定されていない場合は、[デフォルトのアクセスコントロールポリシー（Default Access Control Policy）] を選択します。

図 *10 :* アクセス コントロール ポリシー



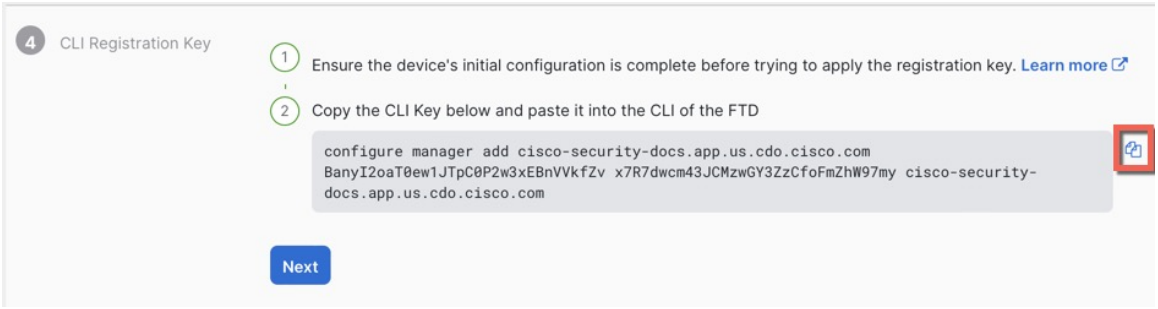
ステップ 7 [サブスクリプションライセンス（Subscription License）] については、[物理 FTD デバイス（Physical FTD Device）] ラジオ ボタンをクリックし、有効にする各機能ライセンスをチェックします。[Next] をクリックします。

図 *11* : サブスクリプションライセンス



ステップ 8 [CLI登録キー（CLI Registration Key）] については、Security Cloud Control は、登録キーとその他のパラメータを使用してコマンドを生成します。このコマンドをコピーして、Threat Defense の初期設定で使用する必要があります。

図 *12* : *CLI* 登録キー



configure manager add Security Cloud Control_*hostname registration_key nat_id display_name*

CLI での、または Device Manager を使用した初期設定の完了

- 初期設定：CLI （15 ページ） ：スタートアップスクリプトを完了した後、Threat Defense CLI でこのコマンドをコピーします。
- 初期設定：デバイスマネージャ （8 ページ） ：コマンドの *scc_hostname*、*registration_key*、および *nat_id* の部分を、[Management Center/Security Cloud Controlのホスト名/IPアドレス（Management Center/Security Cloud Control Hostname/IP Address）]、[Management Center/Security Cloud Controlの登録キー（Management Center/Security Cloud Control Registration Key）]、および [NAT ID] フィールドにコピーします。

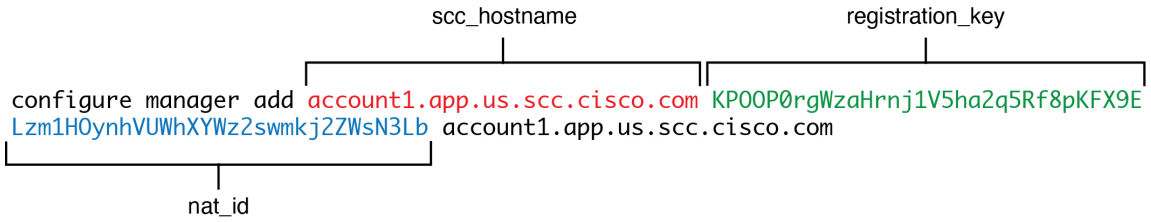
例：

CLI セットアップのサンプルコマンド:

```
configure manager add account1.app.us.scc.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.scc.cisco.com
```

GUI セットアップのサンプル コマンド コンポーネント：

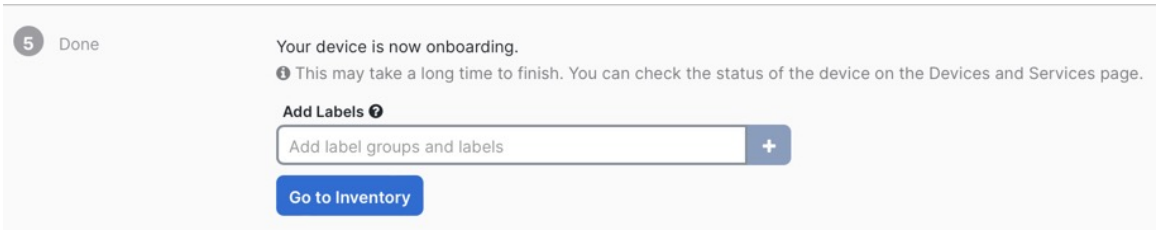
図 *13 : configure manager add* コマンドコンポーネント



ステップ 9 オンボーディングウィザードで [次へ（Next）] をクリックして、デバイスの登録を開始します。

ステップ 10 （任意） [セキュリティデバイス（Security Devices）] ページの並べ替えとフィルタ処理に役立つラベルをデバイスに追加します。ラベルを入力し、青いプラスボタン（+）を選択します。ラベルは、Security Cloud Control への導入準備後にデバイスに適用されます。

図 *14 :* 終了



初期設定の実行（手動プロビジョニング）

手動でプロビジョニングを行う場合は、Secure Firewall Device Manager または CLI を使用して、ファイアウォールの初期設定を実行します。

初期設定：デバイスマネージャ

この方法を使用すると、ファイアウォールを登録した後、管理インターフェイスに加えて次のインターフェイスが事前設定されます。

- イーサネット 1/1：「外部」、DHCP からの IP アドレス、IPv6 自動設定
- VLAN1：「内部」、192.168.95.1/24
- デフォルトルート：外部インターフェイスで DHCP を介して取得

- 追加インターフェイス：Device Manager からのインターフェイス設定はすべて保持されます。

他の設定（内部の DHCP サーバー、アクセス コントロール ポリシー、セキュリティゾーンなど）は保持されません。

手順

ステップ 1 コンピュータを内部インターフェイス（Ethernet 1/2 ～ 1/8 または Cisco Secure Firewall 1220 の場合は 1/2 ～ 1/10）に接続します。

ステップ 2 Device Manager にログインします。

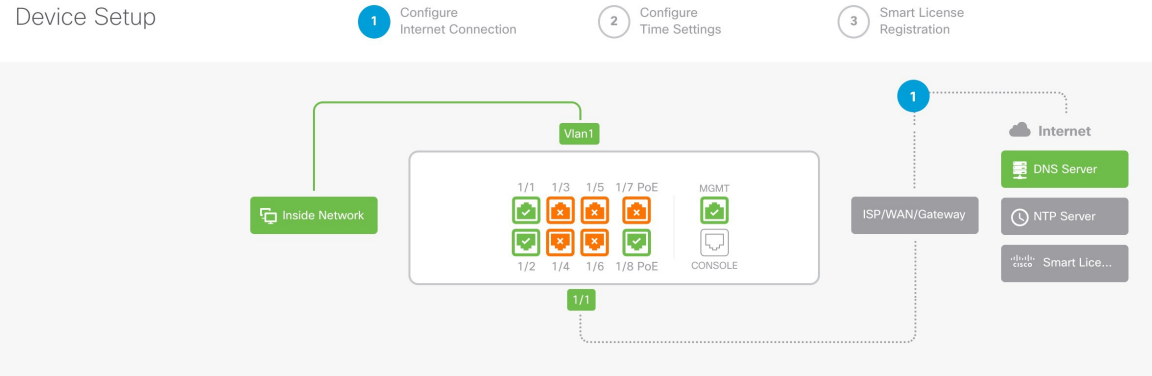
a) https://192.168.95.1に進みます。

b) ユーザー名 **admin** とデフォルトパスワード **Admin123** を使用してログインします。

c) 一般規約を読んで同意し、管理者パスワードを変更するように求められます。

ステップ 3 セットアップウィザードを使用します。

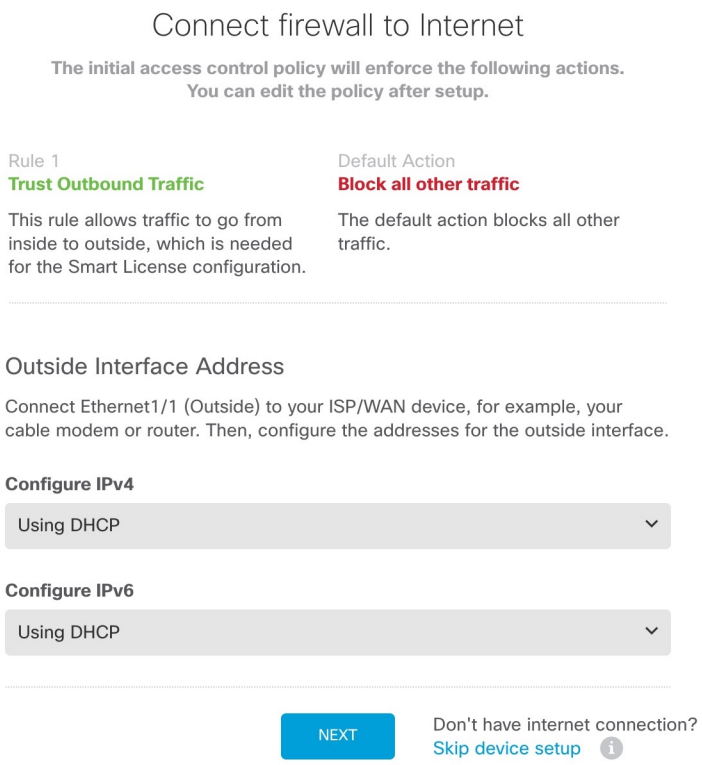
図 *15 : [デバイスの設定（Device Setup）]*



（注）
正確なポート設定は、モデルによって異なります。

a) 外部インターフェイスと管理インターフェイスを設定します。

図 *16*：インターネットへのファイアウォールの接続



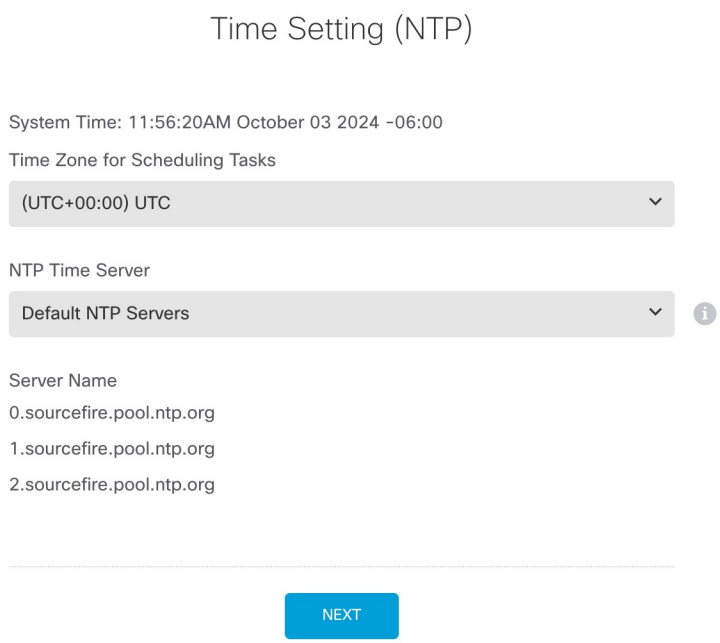
1. [外部インターフェイスアドレス（Outside Interface Address）]：高可用性の実装を予定している場合は、静的 IP アドレスを使用します。セットアップウィザードを使用して PPPoE を設定することはできません。ウィザードの完了後に PPPoE を設定できます。
2. [管理インターフェイス（Management Interface）]：外部インターフェイスでマネージャアクセスを使用している場合でも、管理インターフェイスの設定が使用されます。たとえば、外部インターフェイスを介してバックプレーン経由で回送される管理トラフィックは、外部インターフェイスの DNS サーバーではなく、これらの管理インターフェイスの DNS サーバーを使用して FQDN を解決します。

   [DNSサーバ（DNS Servers）]：システムの管理アドレス用の DNS サーバ。デフォルトは OpenDNS パブリック DNS サーバです。これらは、両方とも外部インターフェイスからアクセスされるため、後で設定する外部インターフェイスの DNS サーバーと一致する可能性があります。

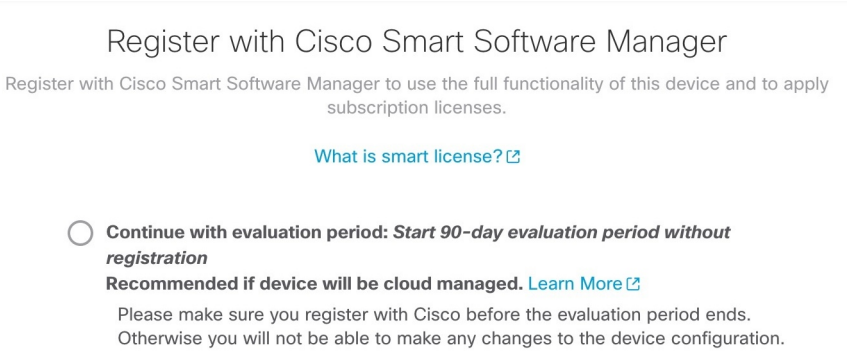
   ファイアウォールのホスト名

b) [時刻設定（NTP）（Time Setting (NTP)）] を設定し、[次へ（Next）] をクリックします。

図 *17*：時刻設定（***NTP***）



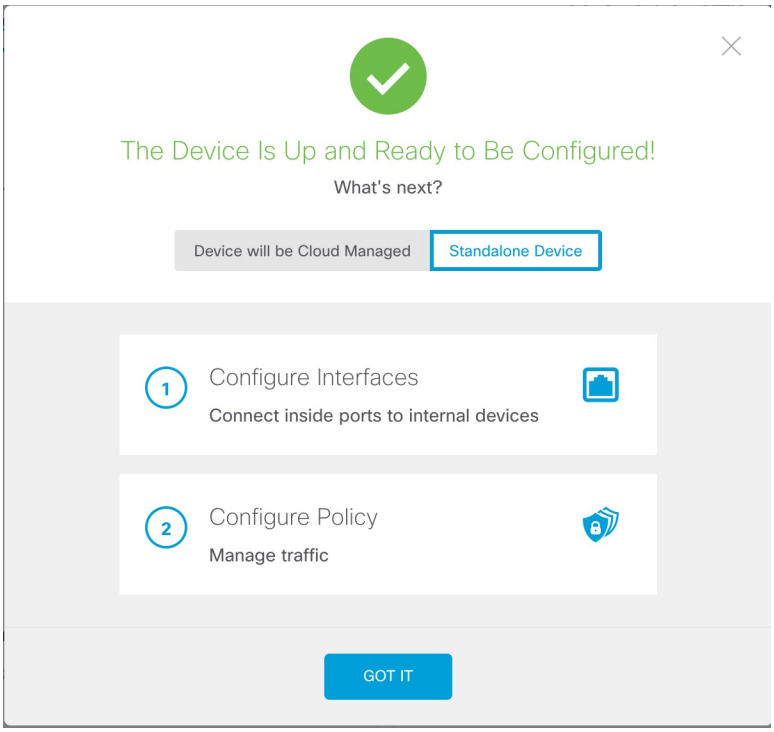
c) [登録せずに 90 日間の評価期間を開始（Start 90 day evaluation period without registration）] を選択します。



Threat Defense を Smart Software Manager に登録「しない」でください。すべてのライセンスは Security Cloud Control で実行されます。

d) [終了（Finish）] をクリックします。

図 *18*：次のステップ



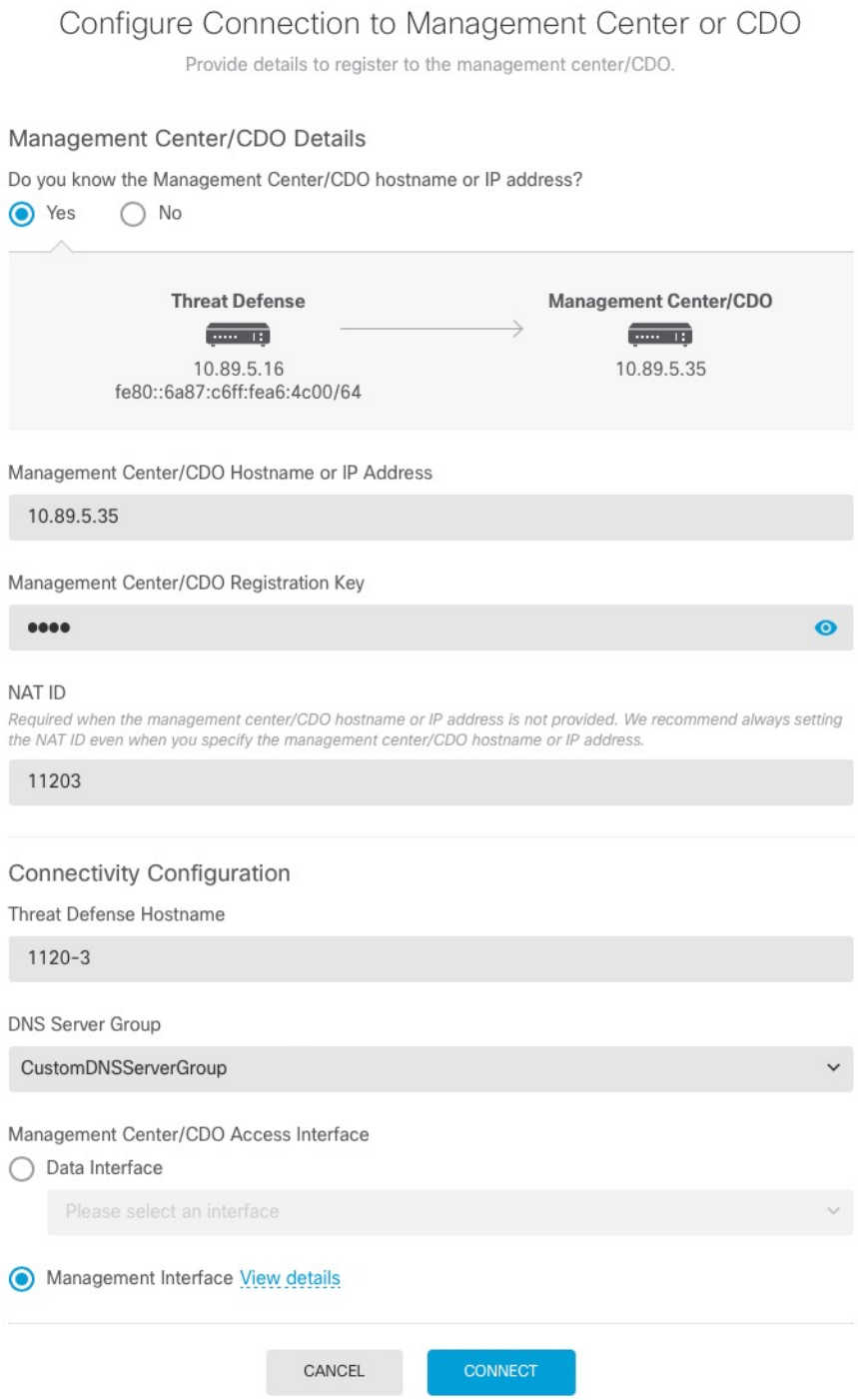
e) [スタンドアロンデバイス（Standalone Device）] を選択し、[了解（Got It）] を選択します。

ステップ 4 追加のインターフェイスを設定する場合は、[デバイス（Device）] を選択し、[インターフェイス（Interface）] のサマリーにあるリンクをクリックします。

ステップ 5 **[デバイス（Device）] > [システム設定（System Settings）] > [集中管理（Central Management）]** の順に選択し、[続行（Proceed）] をクリックして Security Cloud Control に登録します。

[Management Center/CDOの詳細（Management Center/Security Cloud Control Details）] を設定します。

図 *19 : Management Center/Security Cloud Control* の詳細



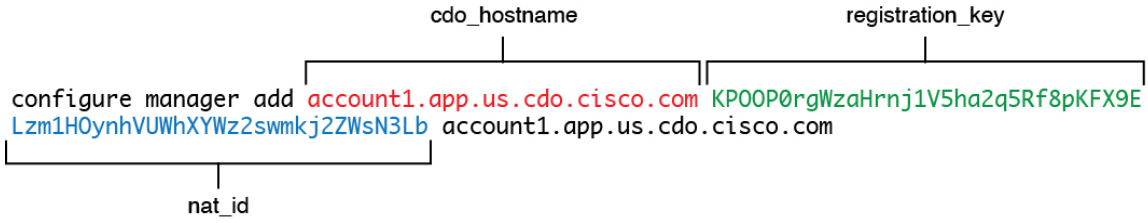
a) [Management Center/CDOのホスト名またはIPアドレスを知っていますか（Do you know the Management Center/Security Cloud Control hostname or IP address）] で、[はい（Yes）] をクリックします。

Security Cloud Control は **configure manager add** コマンドを生成します。コマンドの生成については、手動プロビジョニングによるファイアウォールをオンボード （5 ページ） を参照してください。

configure manager add *_hostname registration_key nat_id display_name*

例：

図 ***20 : configure manager add*** コマンドコンポーネント



b) コマンドの *cdo_hostname*、*registration_key*、*nat_id* の部分を [Management Center/CDOのホスト名/IPアドレス（Management Center/CDO Hostname/IP Address）]、[Management Center/CDOの登録キー（Management Center/CDO Registration Key）]、[NAT ID（NAT ID）] フィールドにコピーします。

ステップ 6 [接続の設定（Connectivity Configuration）] を設定します。

a) [Threat Defenseのホスト名（Threat Defense Hostname）] を指定します。

この FQDN は外部インターフェイスに使用されます。

b) [DNSサーバーグループ（DNS Server Group）] を指定します。

既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは **CiscoUmbrellaDNSServerGroup** と呼ばれ、OpenDNS サーバーが含まれます。

登録後に外部 DNS サーバー設定を保持するには、Management Center で DNS プラットフォーム設定を再設定する必要があります。

c) [Management Center/CDOアクセスインターフェイス（Management Center/CDO Access Interface）] については、[データインターフェイス（Data Interface）] をクリックし、[外部（outside）] を選択します。

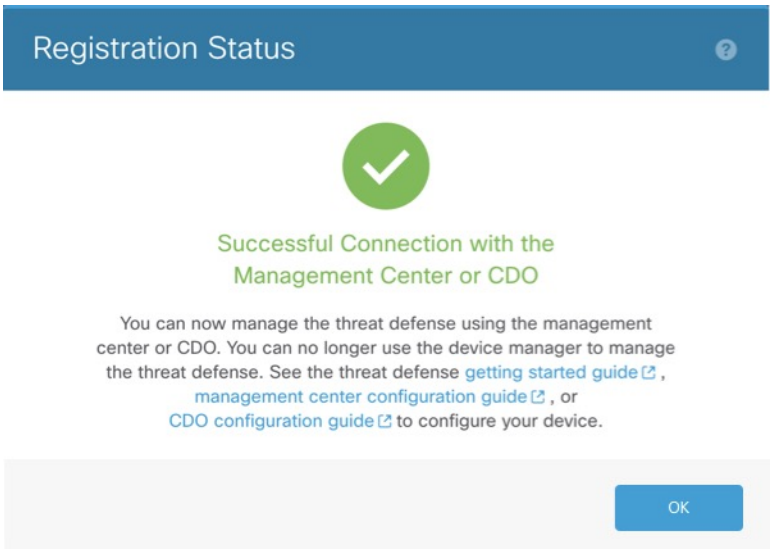
ステップ 7 （任意）[ダイナミックDNS（DDNS）方式の追加（Add a Dynamic DNS (DDNS) method）] をクリックします。

DDNS は、Threat Defense の IP アドレスが変更された場合に Management Center が FQDN で Threat Defense に到達できるようにします。

ステップ 8 [接続（Connect）] をクリックします。

[登録ステータス（Registration Status）] ダイアログボックスに、Security Cloud Control 登録の現在のステータスが表示されます。

図 *21* : 正常接続



ステップ 9 ステータス画面で [Management Center/CDO登録設定の保存（Saving Management Center/Security Cloud Control Registration Settings）] 手順を実行したら、Security Cloud Control に移動し、ファイアウォールを追加します。手動プロビジョニングによるファイアウォールをオンボード （5 ページ）を参照してください。

初期設定：CLI

CLIセットアップスクリプトを使用して、専用の管理IPアドレス、ゲートウェイ、およびその他の基本ネットワーク設定を行います。

手順

ステップ 1 コンソールポートに接続して Threat Defense CLI にアクセスします。Threat Defense CLI へのアクセスを参照してください。

ステップ 2 管理インターフェイスの設定用の CLI セットアップスクリプトを完了します。

（注）
設定をクリア（たとえば、イメージを再作成することにより）しないかぎり、CLI セットアップスクリプトを繰り返すことはできません。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]
```

```
Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
```

ガイダンス：これらのタイプのアドレスの少なくとも 1 つについて **y** を入力します。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどのIPアドレスを設定する必要があります。

```
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
```

ガイダンス：[手動（manual）] を選択します。マネージャアクセスに外部インターフェイスを使用する場合、DHCPはサポートされません。ルーティングの問題を防ぐために、このインターフェイスがマネージャアクセス インターフェイスとは異なるサブネット上にあることを確認してください。

```
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
```

ガイダンス：ゲートウェイを **data-interfaces** に設定します。この設定は、外部インターフェイスを通じてルーティングできるように、バックプレーンを介して管理トラフィックを転送します。

```
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
```

ガイダンス：管理インターフェイスのDNSサーバーを設定します。これらは、両方とも外部インターフェイスからアクセスされるため、後で設定する外部インターフェイスのDNSサーバーと一致する可能性があります。

```
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
```

ガイダンス：Management Center を使用する場合は、**no** と入力します。

```
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

ガイダンス：**routed**と入力します。外部マネージャアクセスは、ルーテッドファイアウォールモードでのみサポートされています。

```
Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
    - add device configuration
```

```
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

ステップ 3 マネージャアクセス用の外部インターフェイスを設定します。

configure network management-data-interface

その後、外部インターフェイスの基本的なネットワーク設定を行うように求めるプロンプトが表示されます。

手動 IP アドレス

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
```

ガイダンス：登録後に外部 DNS サーバーを保持するには、Management Center で DNS プラットフォーム設定を再設定する必要があります。

```
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to change the
 manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

DHCP からの IP アドレス

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
```

```
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to change the
 manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

ステップ 4 Security Cloud Control が生成した **configure manager add** コマンドを使用して、この Threat Defense を管理する Security Cloud Control を識別します。コマンドの生成については、手動プロビジョニングによるファイアウォールをオンボード （5 ページ） を参照してください。

例：

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

ステップ 5 デバイスをリモート支社に送信できるように Threat Defense をシャットダウンします。

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたり、電源スイッチを押したりすると、重大なファイル システムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されており、電源プラグを抜いたり、電源を切断したりすると、システムをグレースフルシャットダウンできないことを覚えておいてください。

a) **shutdown** コマンドを入力します。
b) 電源 LED とステータス LED を観察して、シャーシの電源が切断されていることを確認します（LED が消灯）。
c) シャーシの電源が正常に切断されたら、必要に応じて電源プラグを抜き、シャーシから物理的に電源を取り外すことができます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。