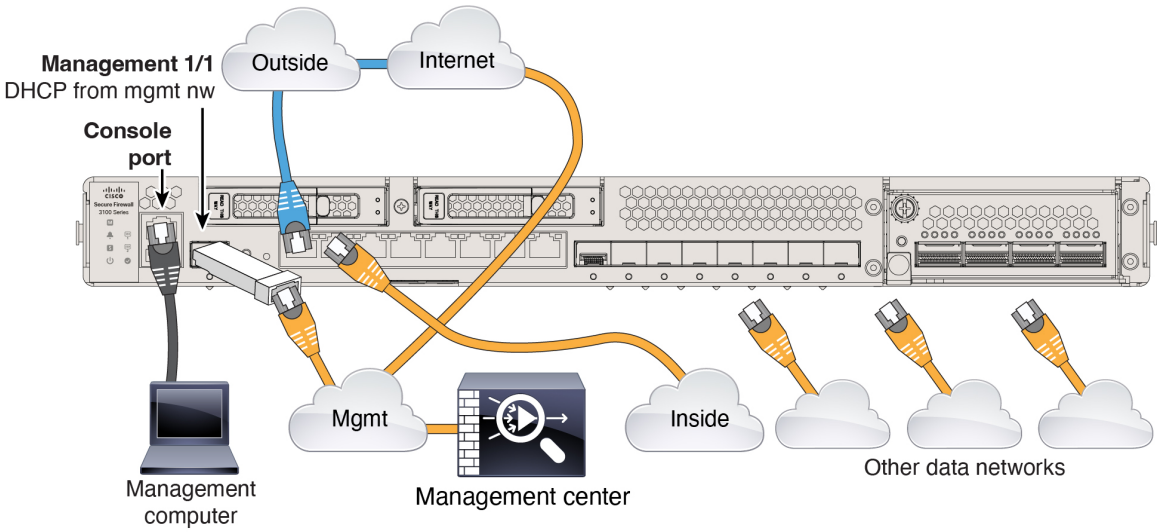
ファイアウォールのケーブル接続と登録

ファイアウォールをケーブル接続し、ファイアウォールを Firewall Management Center に登録します。

ファイアウォールのケーブル接続

Firewall Management Center を専用の管理 1/1 インターフェイスに接続します。管理ネットワークには、更新のためのインターネットへのアクセスが必要です。たとえば、ファイアウォール自体を介して（たとえば、内部ネットワークに接続することによって）管理ネットワークをインターネットに接続できます。

- コンソールアダプタの取得：Cisco Secure Firewall 3100 には DB-9 to RJ-45 シリアルケーブルが付属しているため、接続するにはサードパーティの DB-9-to-USB シリアルケーブルの購入が必要になる場合があります。
- SFP をイーサネット 1/9 以降のポートに取り付けます。
- 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。



初期設定の実行

Cisco 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
- イーサネット 1/2：「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：Firewall 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）に接続します。

ステップ 2 Firewall Device Manager にログインします。

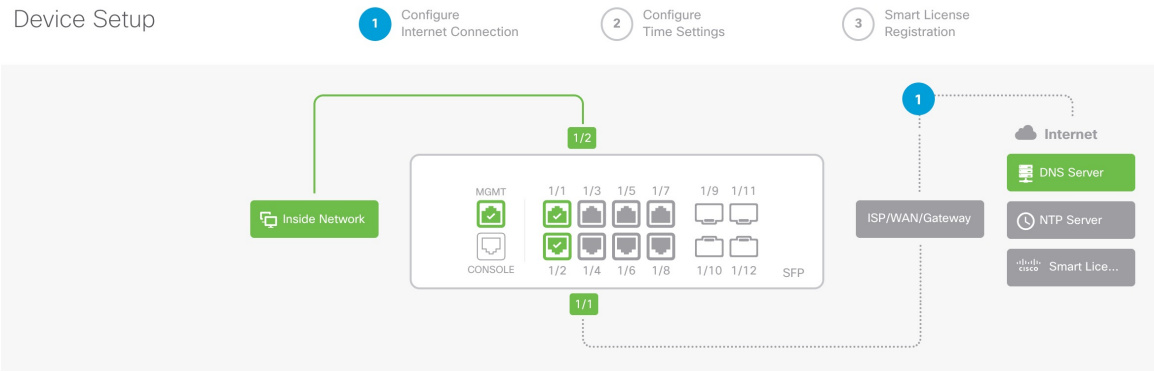
a) https://192.168.95.1に進みます。

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。

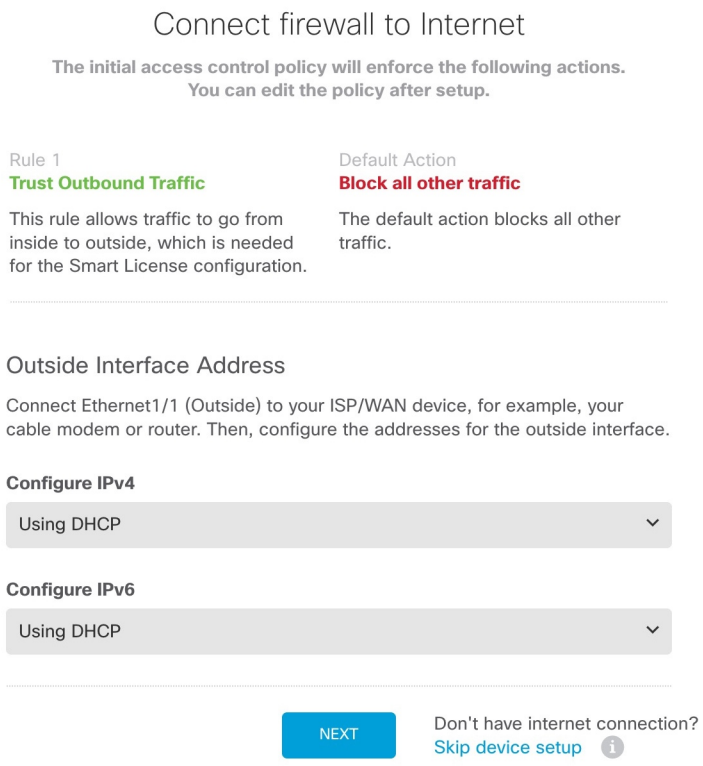
図 *1*：[デバイスの設定（*Device Setup*）]



（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 *2*：インターネットへのファイアウォールの接続



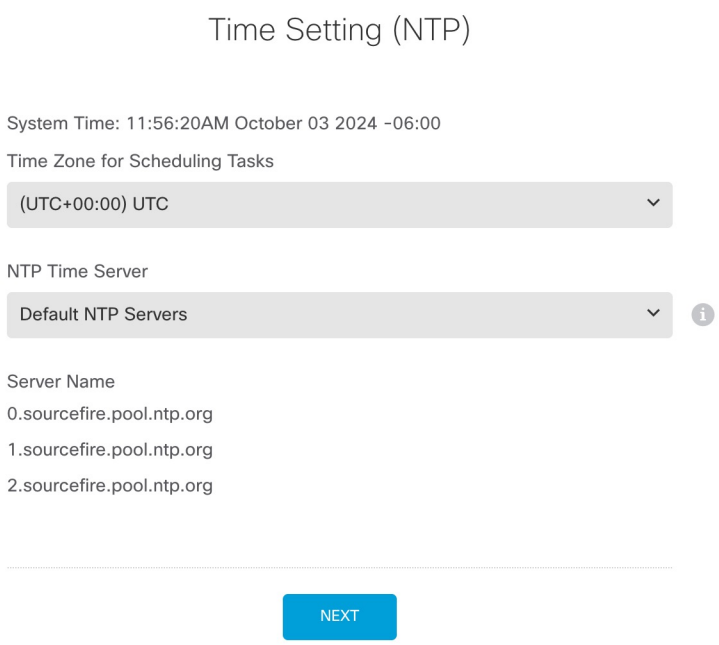
1. [外部インターフェイスアドレス（Outside Interface Address）]：高可用性の実装を予定している場合は、静的 IP アドレスを使用します。セットアップウィザードを使用して PPPoE を設定することはできません。ウィザードの完了後に PPPoE を設定できます。
2. [管理インターフェイス（Management Interface）]：管理インターフェイスの IP アドレスの設定はセットアップウィザードに含まれませんが、次のオプションを設定できます。静的 IP アドレスを使用する必要がある場合は、手順 ステップ 4 （5 ページ） を参照してください。

   [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。

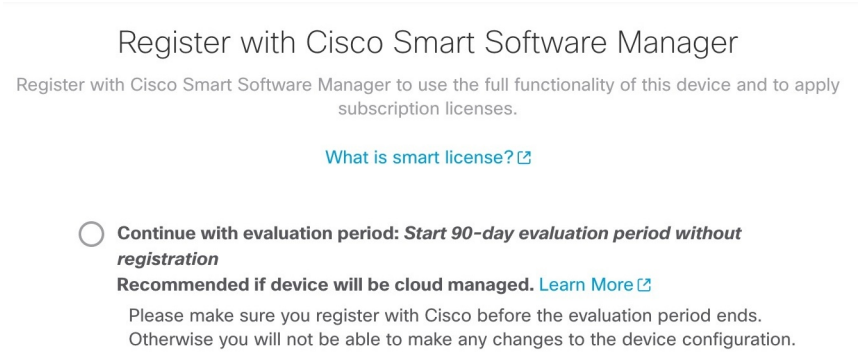
   ファイアウォールのホスト名

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 *3*：時刻設定（*NTP*）



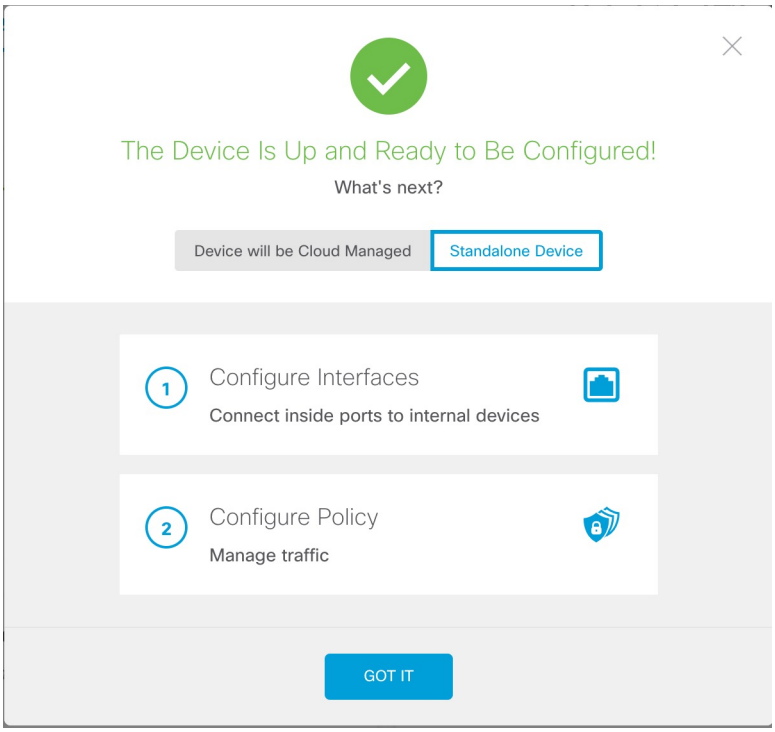
c) [登録せずに 90 日間の評価期間を開始（Start 90 day evaluation period without registration）] を選択します。



Firewall 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 Firewall Management CenterCDO で実行されます。

d) [終了（Finish）] をクリックします。

図 *4:* 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 （任意） 管理インターフェイスに静的 IP アドレスを設定します。[デバイス（Device）]>[インターフェイス（Interfaces）] の管理インターフェイスを参照してください。

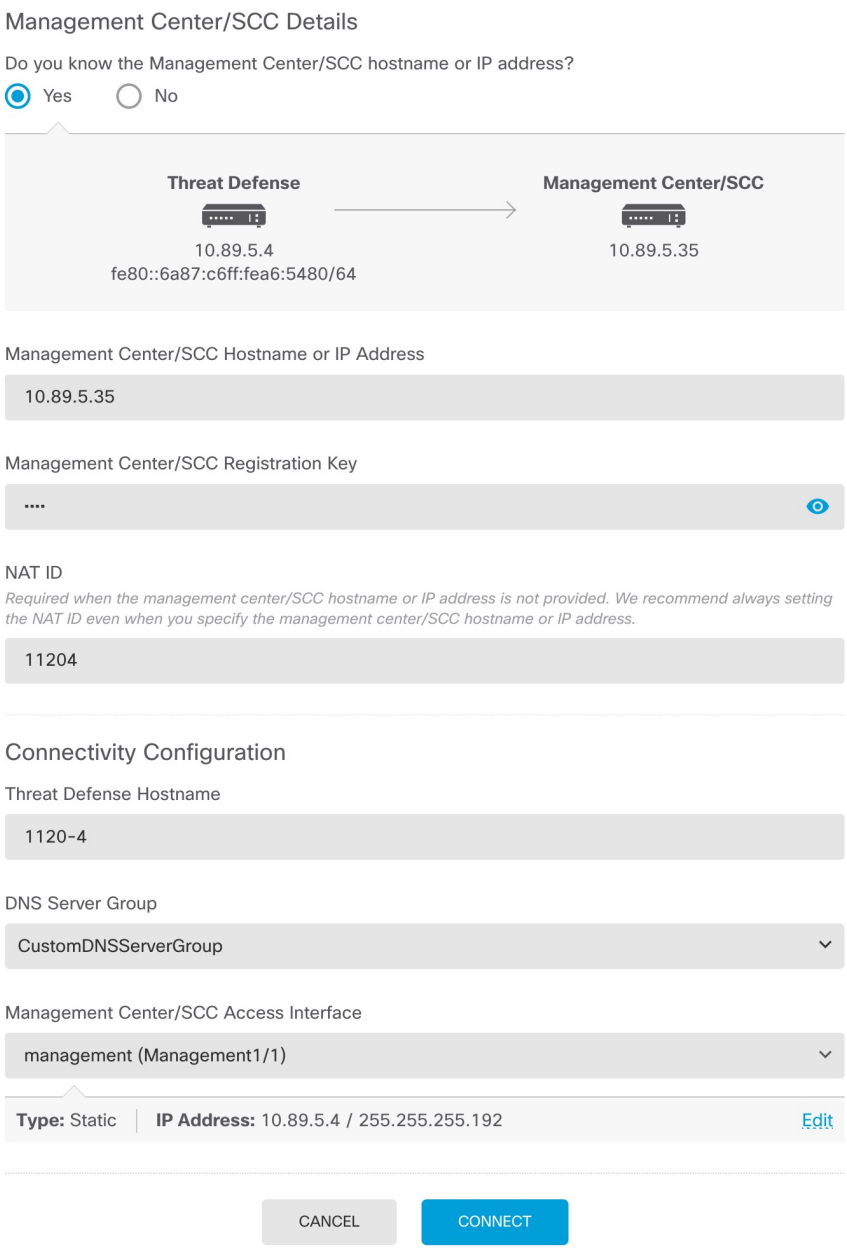
ステップ 5 追加のインターフェイスを設定する場合は、[デバイス（Device）] を選択し、[インターフェイス（Interface）] のサマリーにあるリンクをクリックします。

ステップ 6 **[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 Firewall Management CenterCDO に登録します。

[**Management Center/SCC/Details**] を設定します。

（注）
古いバージョンでは、「SCC」の代わりに「CDO」と表示されることがあります。

図 *5 : Management Center/SCC* の詳細



a) [**Do you know the Management Center/SCC Hostname or IP address**] に対し、IP アドレスまたはホスト名を使用して Firewall Management Center に到達できる場合は [**Yes**] を、Firewall Management Center が NAT の内側にあるか、パブリック IP アドレスまたはホスト名がない場合は [**No**] をクリックします。

b) [**Yes**] を選択した場合は、[**Management Center/SCC Hostname/IP Address**] に入力します。

c) [**Management Center/SCC Registration Key**] を指定します。

このキーは、ファイアウォールを登録するときに Firewall Management Center でも指定する任意の 1 回限りの登録キーです。登録キーは 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Firewall Management Center に登録する複数のファイアウォールに使用できます。

d) [NAT ID] を指定します。

この識別子は、Firewall Management Center でも指定する任意の 1 回限りの文字列です。両方のデバイスの IP アドレスがわかっている場合でも、NAT ID を指定することを推奨します。NAT ID は 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Firewall Management Center に登録する他のファイアウォールには使用「できません」。NAT ID は、正しいデバイスからの接続であることを確認するために IP アドレスと組み合わせて使用されます。 IP アドレス/NAT ID の認証後にのみ、登録キーがチェックされます。

ステップ 7 [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。

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

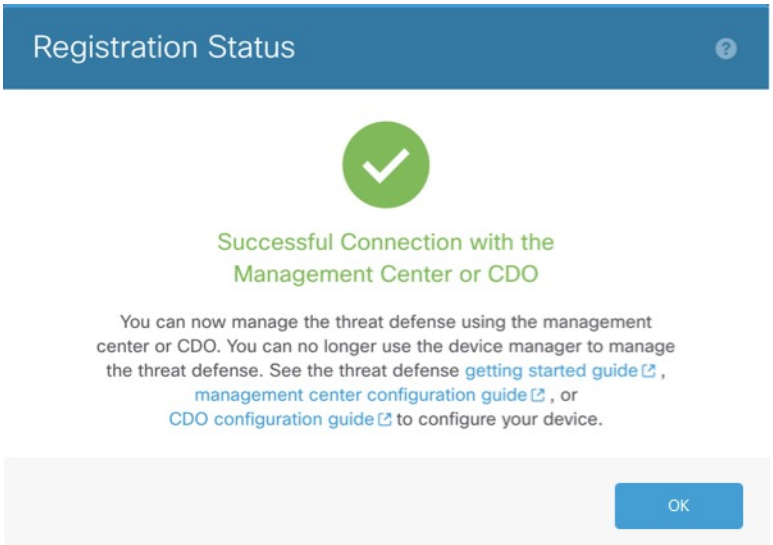
これはすでに設定していますが、既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは **CiscoUmbrellaDNSServerGroup** と呼ばれ、OpenDNS サーバーが含まれます。

c) [**Management Center/SCC Access Interface**] で [**Management Interface**] をクリックします。

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、Firewall Management CenterCDO 登録の現在のステータスが表示されます。

図 *6*：正常接続



ステップ 9 ステータス画面で [**Saving Management Center/ Registration Settings**] の手順を実行したら Firewall Management CenterCDO に移動し、ファイアウォールを追加します。Management Center へのファイアウォールの登録（10 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 Firewall Threat Defense CLI にアクセスします。Firewall 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。

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

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]: 10.10.10.1

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
```

```
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：Firewall 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'

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 Firewall Management Center を指定します。

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key nat_id*

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the Firewall Management Center.Firewall Management Center を直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。この場合は、ファイアウォールが、到達可能な IP アドレスまたはホスト名を持っている必要があります。
- reg_key：Firewall Threat Defense を登録するときに Firewall Management Center でも指定する任意のワンタイム登録キーを指定します。登録キーは 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。

- nat_id：Firewall Management Center でも指定する、任意で一意の 1 回限りの文字列を指定します。NAT ID は 2 ～ 36 文字である必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Firewall Management Center に登録する他のデバイスには使用できません。

例：

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

Management Center へのファイアウォールの登録

ファイアウォールを Firewall Management Center に登録します。

手順

ステップ 1 Firewall Management Center にログインします。

a) 次の URL を入力します。

https://*fmc_ip_address*

b) ユーザー名とパスワードを入力します。

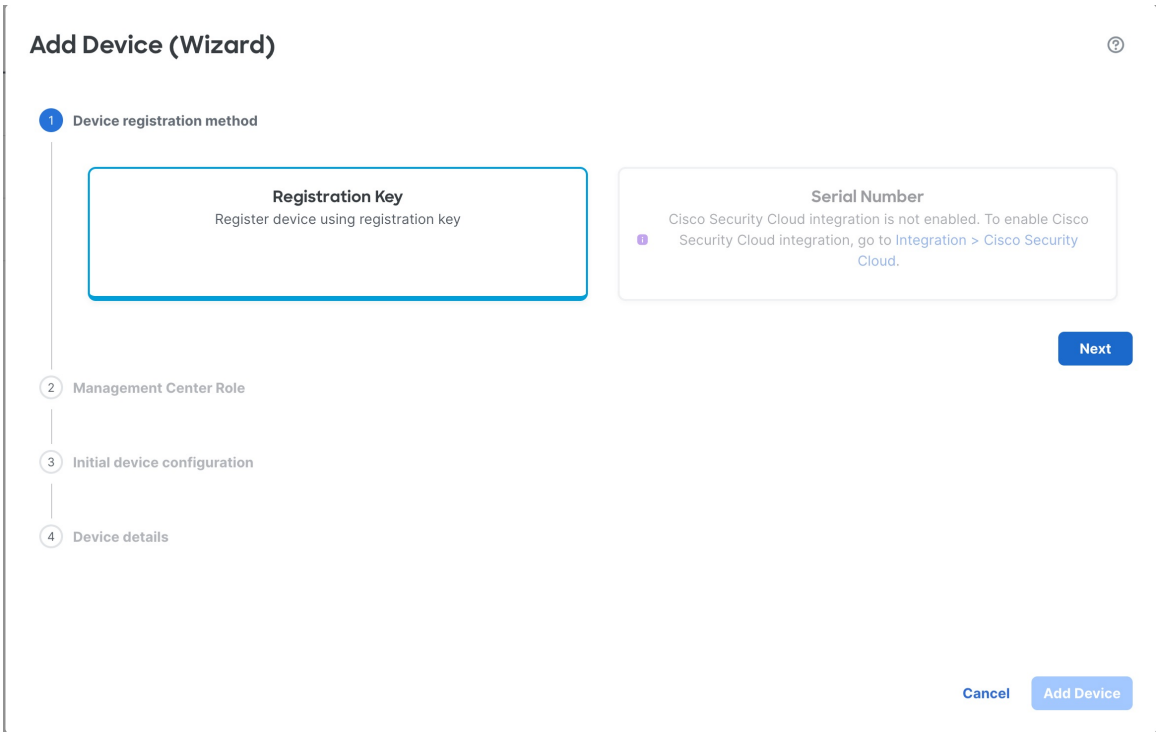
c) [ログイン（Log In）] をクリックします。

ステップ 2 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。

ステップ 3 [**Add**] ドロップダウンメニューから、[][**Device (Wizard)**] を選択します。

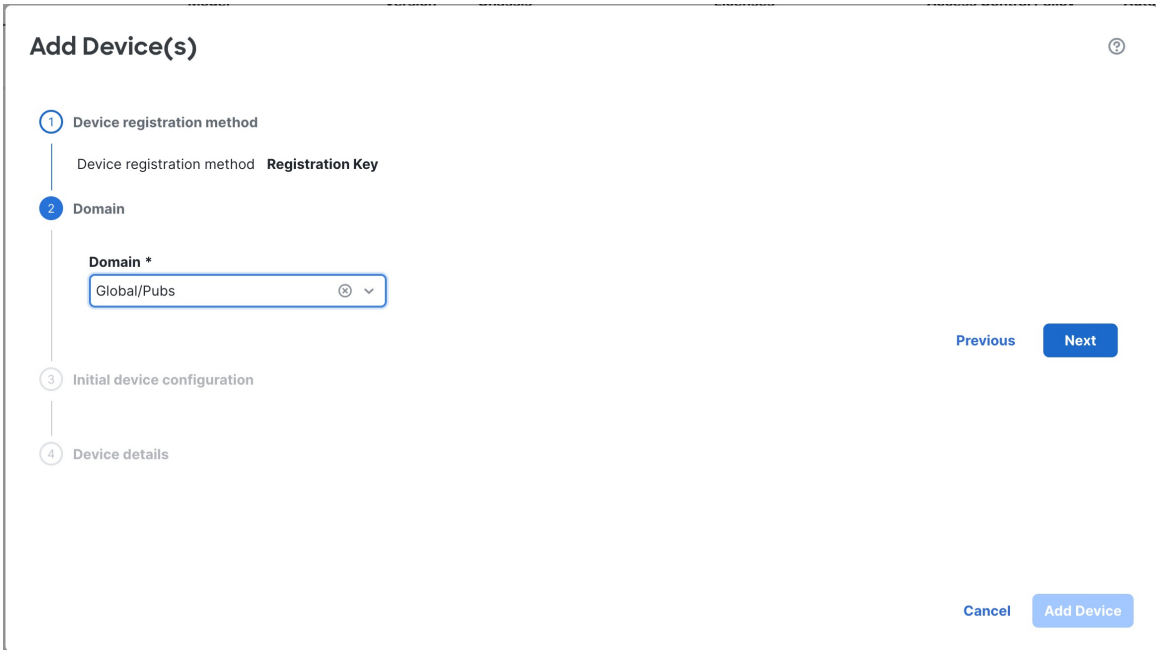
ステップ 4 [登録キー（Registration Key）] をクリックし、[次へ（Next）] をクリックします。

図 *7*: デバイスの登録方法



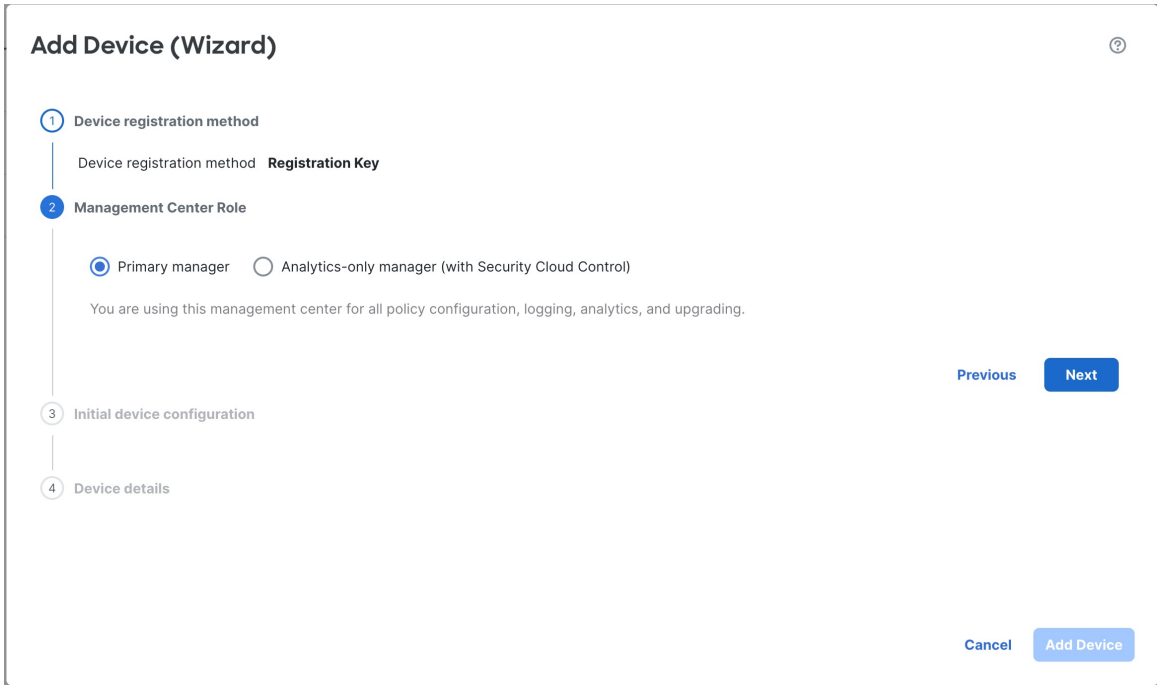
ステップ 5 マルチドメイン環境では、ドロップダウンリストから [ドメイン（Domain）] を選択し、[次へ（Next）] をクリックします。

図 *8*: ドメイン



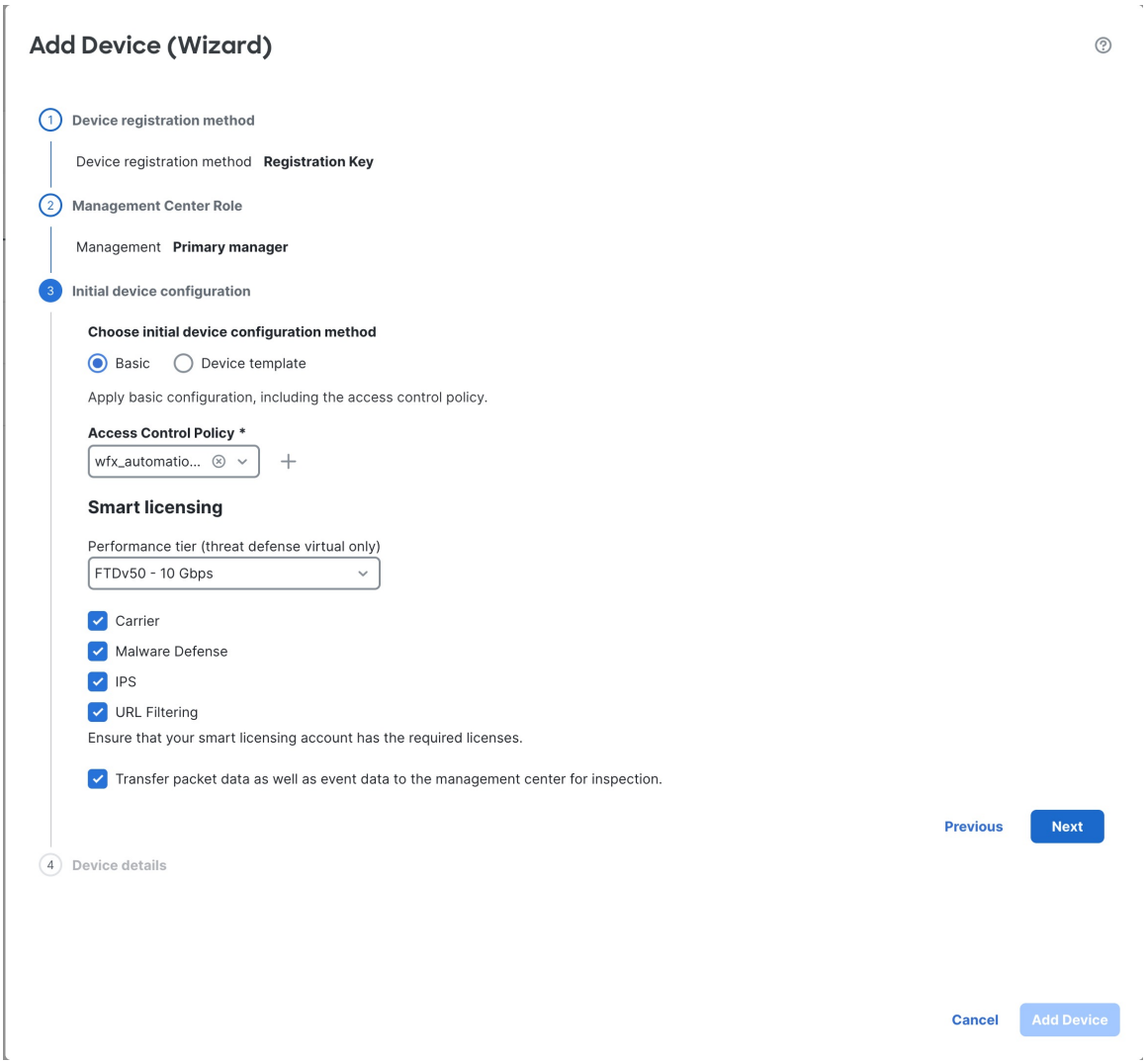
ステップ 6 通常の管理の場合は [プライマリマネージャ（Primary manager）] をクリックし、クラウド提供型 Firewall Management Center で管理されているデバイスの場合は [分析専用マネージャ（Analytics-only manager）] をクリックします。。

図 *9 : Management Center* のロール



ステップ 7 [デバイスの初期設定（Initial Device Configuration）] で、[基本（Basic）] をクリックします。

図 *10* : デバイスの初期設定



a) 登録時にデバイスに展開する最初の [アクセスコントロールポリシー（Access Control Policy）] を選択するか、新しいポリシーを作成します。使用する必要があることがわかっているカスタマイズ済みのポリシーがすでにある場合を除いて、[新しいポリシーの作成（Create new policy）] を選択し、[すべてのトラフィックをブロック（Block all traffic）] を選択します。後でこれを変更してトラフィックを許可することができます。「アクセス制御ルールの設定」を参照してください。

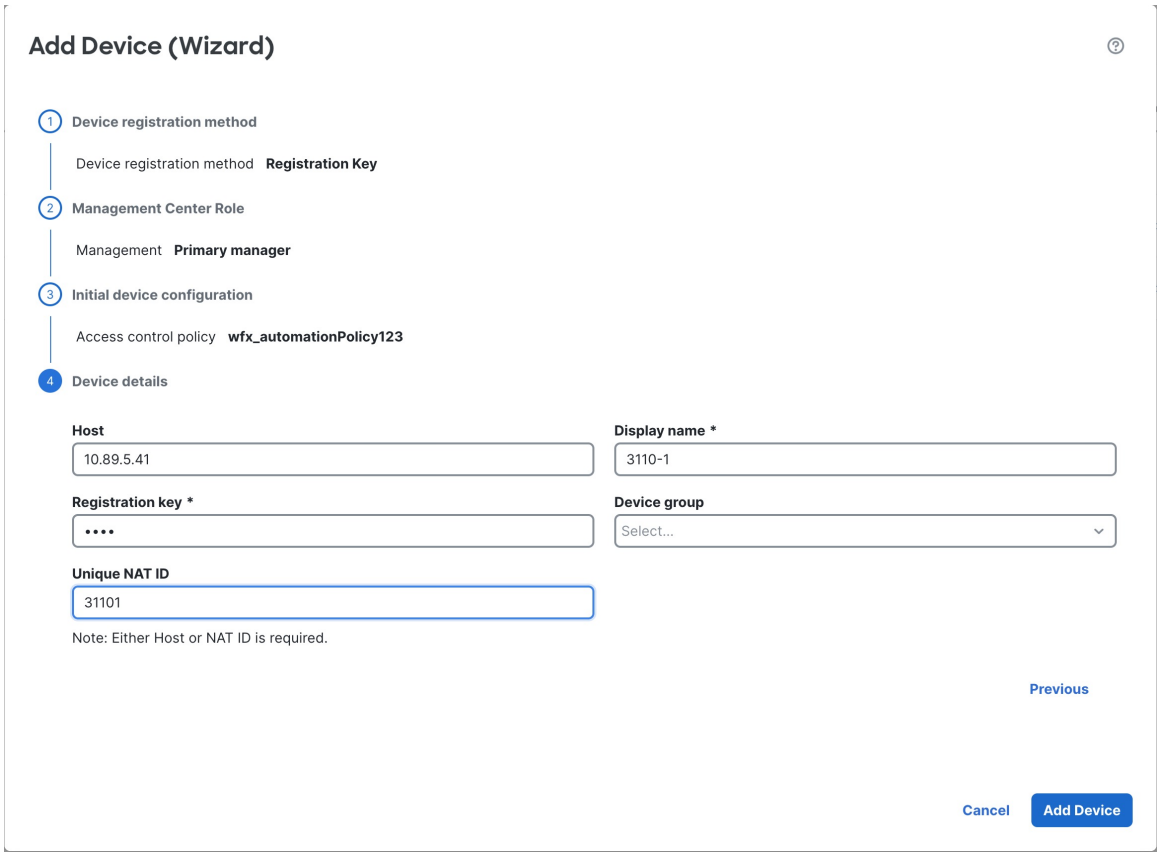
b) デバイスに適用する [スマートライセンス（Smart Licensing）] ライセンスを選択します。

[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] ページから、デバイスを追加した後にライセンスを適用することもできます（セキュアクライアント リモートアクセス VPN ライセンスを含む）。

c) [次へ（Next）] をクリックします。

ステップ 8 [デバイスの詳細（Device details）] を指定します。

図 *11* : デバイスの詳細（***Device Details***）



a) [ホスト（Host）] には、追加デバイスの IP アドレスまたはホスト名を入力します。デバイスの IP アドレスが不明な場合（NAT の背後にある場合など）は、このフィールドを空白のままにします。

b) [表示名（Display name）] フィールドに、Firewall Management Center でのデバイスの表示名を入力します。この名前は変更できません。

c) [登録キー（Registration key）] には、初期設定と同じ登録キーを入力します。

d) （任意） デバイスを [デバイスグループ（Device group）] に追加します。

e) [一意のNAT ID（Unique NAT ID）] には、初期設定と同じ ID を入力します。

f) [パケットの転送（Transfer Packets）] チェックボックスをオンにして、侵入イベントが発生するたびに、デバイスが検査のためにパケットを Firewall Management Center に転送するようにします。

侵入イベントごとに、デバイスは、イベント情報とイベントをトリガーしたパケットを検査のために Firewall Management Center に送信します。このオプションを無効にした場合は、イベント情報だけが Firewall Management Center に送信され、パケットは送信されません。

ステップ 9 [Add Device] をクリックします。

Firewall Management Center がデバイスのハートビートを確認して通信を確立するまでに、最大 2 分かかる場合があります。登録が成功すると、デバイスがリストに追加されます。失敗した場合は、エラーメッセージが表示されます。デバイスの登録に失敗した場合は、次の項目を確認してください。

- ping：デバイスの CLI にアクセスし、次のコマンドを使用して Firewall Management Center の IP アドレスへの ping を実行します。

  ping system *ip_address*

  ping が成功しない場合は、**show network** コマンドを使用してネットワーク設定を確認します。デバイスの IP アドレスを変更する必要がある場合は、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを使用します。

- 登録キー、NAT ID、および Firewall Management Center IP アドレス：両方のデバイスで同じ登録キーを使用していることを確認し、使用している場合はNAT IDを使用していることを確認します。**configure manager add** コマンドを使用して、デバイスで登録キーと NAT ID を設定することができます。

トラブルシューティングの詳細については、https://cisco.com/go/fmc-reg-error を参照してください。

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。