



Device Manager での Threat Defense の展開

この章の対象読者

この章では、Device Manager の Web ベースのデバイスセットアップ ウィザードを使用して、脅威に対する防御 デバイスの初期セットアップと設定を完了する方法について説明します。

Device Manager では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの Device Manager デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

多数のデバイスを管理している場合、または 脅威に対する防御 で許可される、より複雑な機能や設定を使用する場合は、代わりに Management Center を使用します。

ISA 3000 ハードウェアでは、脅威に対する防御 ソフトウェアまたは ASA ソフトウェアを実行できます。脅威に対する防御 と ASA の間で切り替えを行う際には、デバイスの再イメージ化が必要になります。「Cisco ASA および Firepower Threat Defense 再イメージ化ガイド」を参照してください。

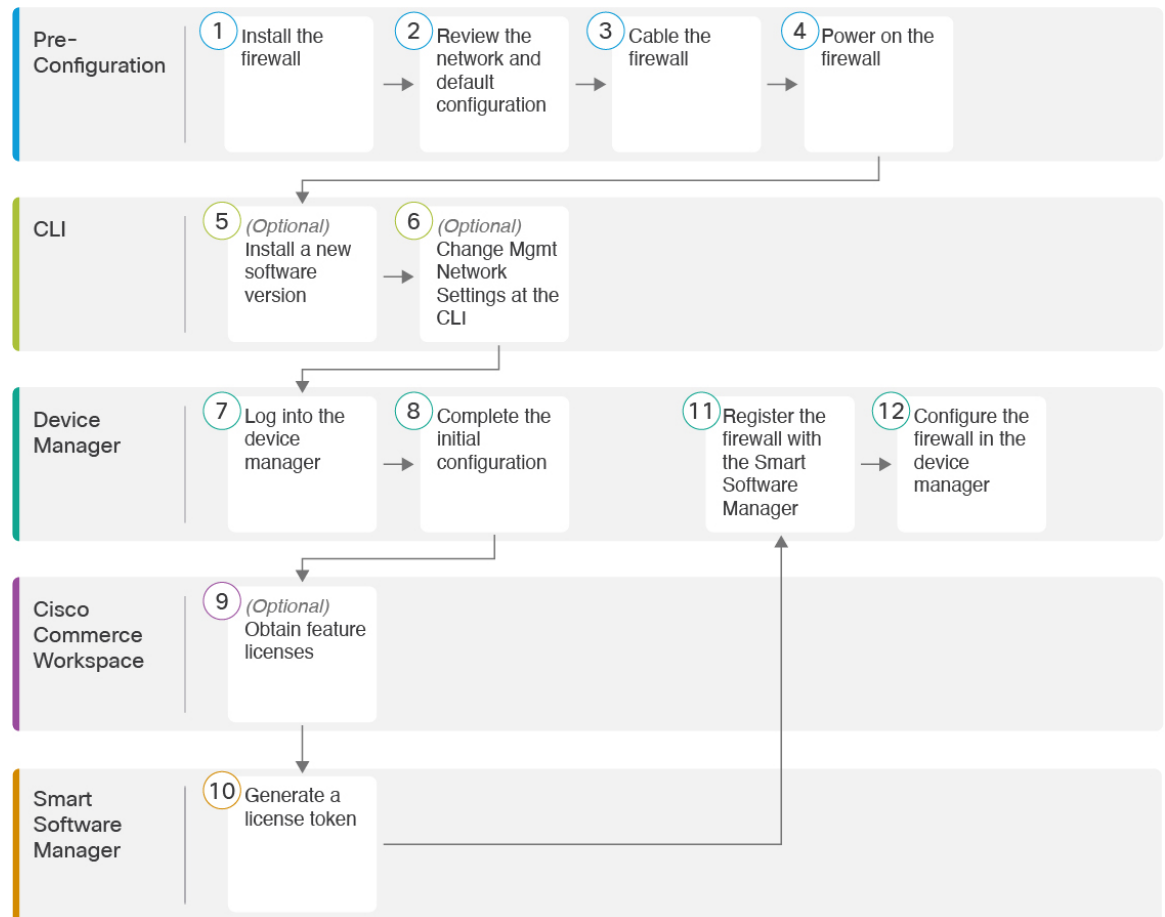
プライバシー収集ステートメント : Firepower 1100 シリーズには個人識別情報は不要で、積極的に収集することはありません。ただし、ユーザー名などの設定では、個人識別情報を使用できます。この場合、設定作業時や SNMP の使用時に、管理者が個人識別情報を確認できる場合があります。

- [エンドツーエンドの手順 \(2 ページ\)](#)
- [ネットワーク配置とデフォルト設定の確認 \(3 ページ\)](#)
- [デバイスのケーブル接続 \(6.5 以降\) \(7 ページ\)](#)
- [デバイスの配線 \(6.4 以降\) \(8 ページ\)](#)
- [デバイスの電源投入 \(9 ページ\)](#)
- [\(任意\) CLI での管理ネットワーク設定の変更 \(10 ページ\)](#)
- [へのログイン Device Manager \(11 ページ\)](#)
- [初期設定の完了 \(6.5 以降\) \(12 ページ\)](#)
- [初期設定の完了 \(6.4 以前\) \(17 ページ\)](#)
- [ライセンスの設定 \(19 ページ\)](#)
- [Device Manager \(6.5 以降\) でのデバイスの設定 \(24 ページ\)](#)
- [Device Manager \(6.4 以前\) でのファイアウォールの設定 \(26 ページ\)](#)

- [Threat Defense CLI へのアクセス](#) (31 ページ)
- [ファイアウォールの電源の切断](#) (32 ページ)
- [次のステップ](#) (34 ページ)

エンドツーエンドの手順

シャーシで Device Manager を使用して脅威に対する防御を展開するには、次のタスクを参照してください。



①	事前設定	ネットワーク配置とデフォルト設定の確認 (3 ページ)。
②	事前設定	<ul style="list-style-type: none"> • デバイスのケーブル接続 (6.5 以降) (7 ページ)。 • デバイスの配線 (6.4 以降) (8 ページ)
③	事前設定	デバイスの電源投入 (9 ページ)。

4	Threat Defense CLI	(任意) CLI での管理ネットワーク設定の変更 (10 ページ)。
5	Device Manager	へのログイン Device Manager (11 ページ)。
6	Device Manager	<ul style="list-style-type: none"> 初期設定の完了 (6.5 以降) (12 ページ) 初期設定の完了 (6.4 以前) (17 ページ)。
7	Cisco Commerce Workspace	ライセンスの設定 (19 ページ) : ライセンス機能を取得します。
8	Smart Software Manager	ライセンスの設定 (19 ページ) : ライセンス トークンを生成します。
9	Device Manager	ライセンスの設定 (19 ページ) : スマート ライセンシング サーバーにデバイスを登録します。
10	Device Manager	<ul style="list-style-type: none"> Device Manager (6.5 以降) でのデバイスの設定 (24 ページ) Device Manager (6.4 以前) でのファイアウォールの設定 (26 ページ)。

ネットワーク配置とデフォルト設定の確認

次の図は、バージョン 6.5 以降およびバージョン 6.4 以前の ISA 3000 における推奨されるネットワーク配置を示しています。デフォルト設定はバージョン 6.5 で変更されました。



- (注) デフォルトの管理 IP アドレスを使用できない場合 (たとえば、デバイスを既存のネットワークに追加する場合)、コンソールポートに接続して、CLI で初期セットアップ (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の指定など) を実行できます。 (任意) [CLI での管理ネットワーク設定の変更](#) (10 ページ) を参照してください。

図 1: 6.5以降 : 推奨されるネットワーク展開

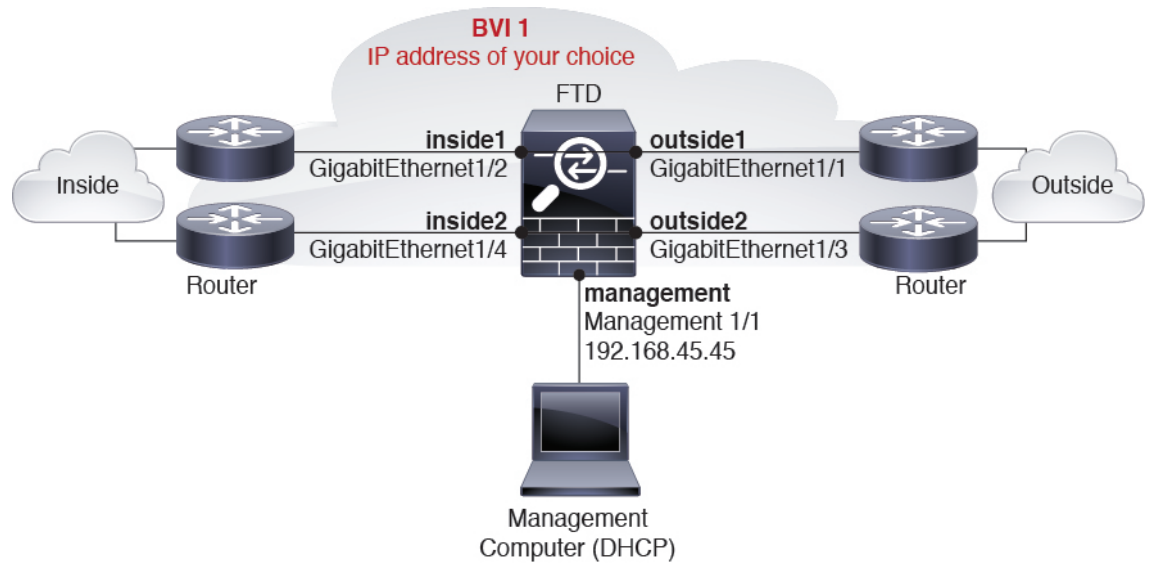
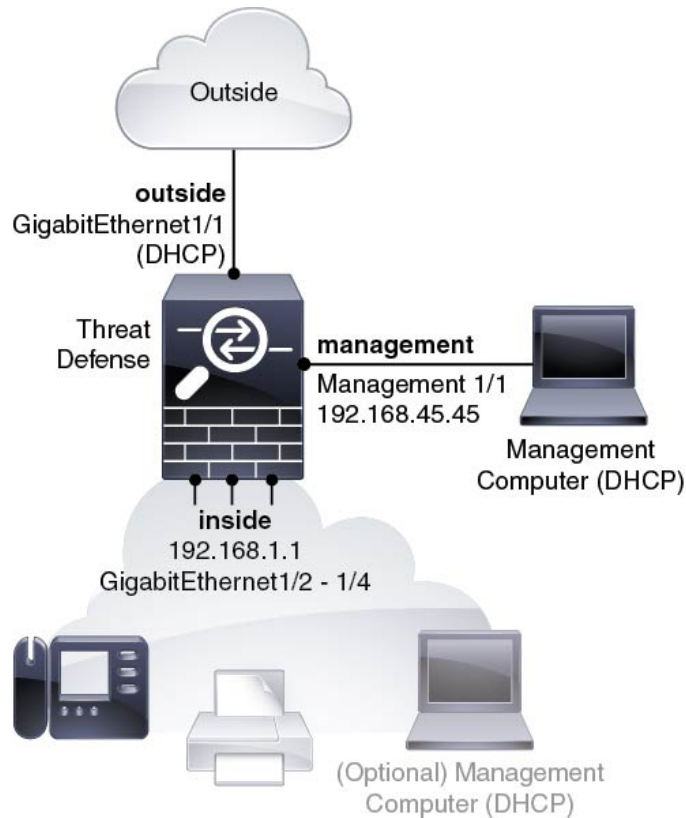


図 2: 6.4以前 : 推奨されるネットワーク展開



デフォルト設定 (6.5 以降)

出荷前に特別なデフォルト設定が適用されている ISA 3000 の設定には、以下が含まれます。

- BVI 1 : すべてのメンバーインターフェイスは同じネットワーク内に存在しています (IP アドレスは事前設定されていません。ネットワークと一致するように設定する必要があります) : GigabitEthernet 1/1 (outside1)、GigabitEthernet 1/2 (inside1)、GigabitEthernet 1/3 (outside2)、GigabitEthernet 1/4 (inside2)
- 内部→外部トラフィックフローすべてのインターフェイスは相互通信できます。
- 管理 : Management 1/1 (管理)、IP アドレス 192.168.45.45



(注) Management 1/1 インターフェイスは、管理論理インターフェイスと診断論理インターフェイスの間で共有できます。『[FDM コンフィギュレーションガイド](#)』を参照してください。

- 管理用の DNS サーバー : OpenDNS: 208.67.222.222, 208.67.220.220
- NTP : Cisco NTP サーバー : 0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org
- デフォルトルート
 - 管理インターフェイス : 192.168.45.1 への管理インターフェイス経由。
 - データインターフェイス : なし。
- FDM アクセス : 管理ホストが許可されます。
- ハードウェアバイパス : 次のインターフェイスペアで有効になっています。GigabitEthernet 1/1 および 1/2。GigabitEthernet 1/3 および 1/4



(注) ISA 3000 への電源が切断され、ハードウェア バイパス モードに移行すると、通信できるのは上記のインターフェイスペアのみになります。inside1 と inside2 および outside1 と outside2 は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。電源が再投入されると、脅威に対する防御 がフローを引き継ぐため、接続が短時間中断されます。

デフォルト設定 (6.4 以前)

初期セットアップ後の ISA 3000 の設定には、次のものが含まれます。

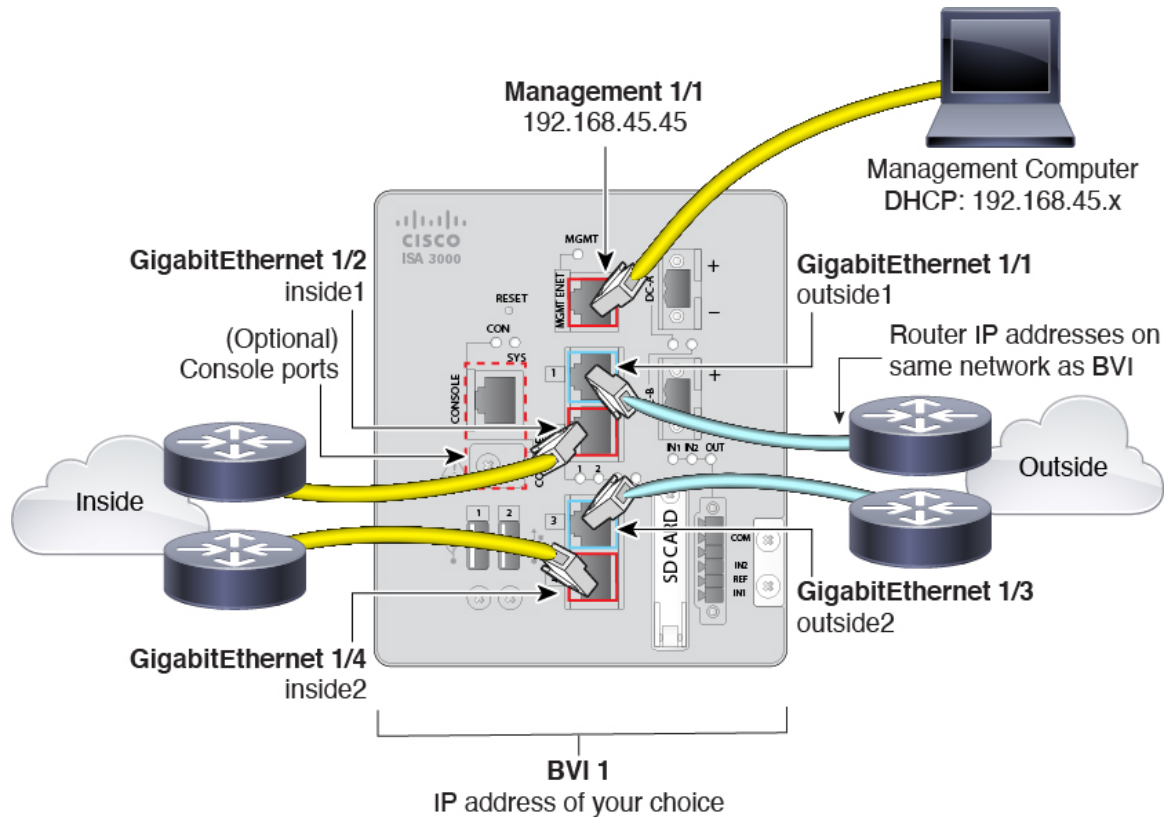
- 内部 : GigabitEthernet 1/2 ~ 1/4 は、□ブリッジグループ インターフェイス (BVI) 1、IP アドレス 192.168.1.1 に属します。
- 外部 : GigabitEthernet 1/1、DHCP からの IP アドレス、またはセットアップ時に指定したアドレス
- 内部→外部トラフィックフロー
- 管理 : Management 1/1 (管理)、IP アドレス 192.168.45.45



(注) Management 1/1 インターフェイスは、管理論理インターフェイスと診断論理インターフェイスの間で共有できます。『[FDM コンフィギュレーションガイド](#)』を参照してください。

- [管理用のDNSサーバー (DNS server for management)] : OpenDNS : 208.67.222.222、208.67.220.220、またはセットアップ時に指定したサーバー。
- NTP : Cisco NTP サーバー : 0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org、またはセットアップ時に指定したサーバー
- デフォルトルート
 - データインターフェイス : 外部DHCPから取得したもの、またはセットアップ時に指定したゲートウェイ IP アドレス
 - 管理インターフェイス : バックプレーンを介しデータインターフェイスを経由脅威に対する防御 には、ライセンスおよびアップデート用のインターネットアクセスが必要です。
- 内部インターフェイスの **DHCP サーバー**、管理インターフェイス
- **FDM アクセス** : 管理ホストと内部ホストに許可されます
- **NAT** : 内部から外部へのすべてのトラフィック用のインターフェイス PAT

デバイスのケーブル接続 (6.5 以降)



Management 1/1 インターフェイスで ISA 3000 を管理します。

手順

ステップ 1 GigabitEthernet 1/1 を外部ルータに接続し、GigabitEthernet 1/2 を内部ルータに接続します。

これらのインターフェイスによってハードウェアバイパスペアが形成されます。

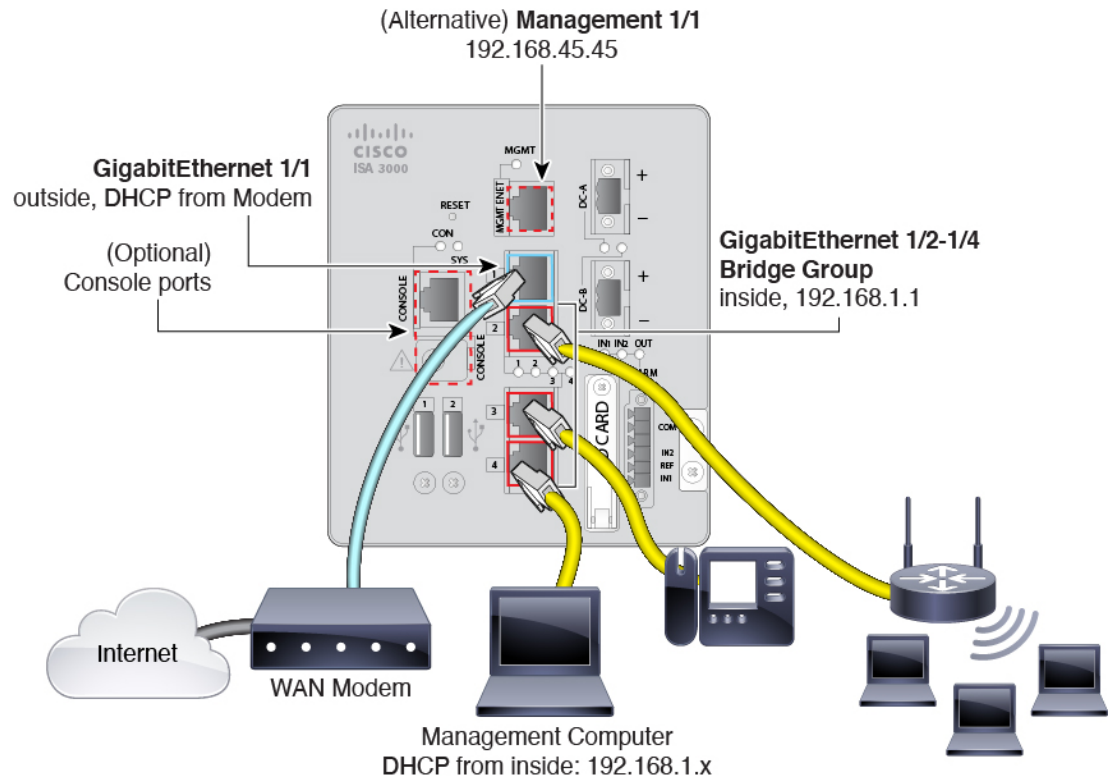
ステップ 2 GigabitEthernet 1/3 を冗長外部ルータに接続し、GigabitEthernet 1/4 を冗長内部ルータに接続します。

これらのインターフェイスによってハードウェアバイパスペアが形成されます。これらのインターフェイスは、他方のペアで障害が発生した場合に冗長ネットワークパスを提供します。これら 4 つのデータインターフェイスはすべて、選択した同じネットワーク上に存在します。BVI 1 の IP アドレスを、内部ルータおよび外部ルータと同じネットワーク上に配置するように設定する必要があります。

ステップ 3 Management 1/1 を管理 PC (またはネットワーク) に接続します。

Management 1/1 の IP アドレスをデフォルトから変更する必要がある場合は、管理 PC をコンソールポートにケーブル接続する必要もあります（ケーブル接続は表示されていません）。
 「(任意) CLI での管理ネットワーク設定の変更 (10 ページ)」を参照してください。

デバイスの配線 (6.4 以降)



Management 1/1 または GigabitEthernet 1/2 ~ 1/4 のいずれかで ISA 3000 を管理します。デフォルト設定でも、GigabitEthernet 1/1 は外部として設定されています。

手順

ステップ 1 管理コンピュータを次のいずれかのインターフェイスに接続します。

- GigabitEthernet 1/2 ~ 1/4 : 管理コンピュータをいずれかの内部ポート（イーサネット 1/2 ~ 1/4）に直接接続します。内部にはデフォルトの IP アドレス（192.168.1.1）があり、クライアントに IP アドレスを提供するために DHCP サーバーも実行されます（管理コンピュータを含む）。したがって、これらの設定が既存の内部ネットワーク設定と競合しないようにしてください（[デフォルト設定 \(6.4 以前\) \(5 ページ\)](#) を参照）。

- **Management 1/1** : 管理コンピュータを Management 1/1 に直接接続します。または、Management 1/1 を管理ネットワークに接続します。管理 1/1 にはデフォルトの IP アドレス (192.168.45.45) があり、クライアント (管理コンピュータを含む) に IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の管理ネットワークの設定と競合しないようにしてください ([デフォルト設定 \(6.4 以前\)](#) ([5 ページ](#)) を参照)。

Management 1/1 の IP アドレスをデフォルトから変更する必要がある場合は、管理 PC をコンソールポートにケーブル接続する必要もあります (ケーブル接続は表示されていません)。(任意) [CLI での管理ネットワーク設定の変更 \(10 ページ\)](#) を参照してください。

ステップ 2 外部ネットワークを GigabitEthernet 1/1 インターフェイスに接続します。

デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティックアドレスを設定することもできます。

ステップ 3 内部デバイスを残りのポート (GigabitEthernet 1/2 ~ 1/8) に接続します。

デバイスの電源投入

システムの電源は DC 電源で制御されます。電源ボタンはありません。

始める前に

デバイスに対して信頼性の高い電力を供給することが重要です (たとえば、無停電電源装置 (UPS) を使用)。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。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いて、電力が失われると、システムをグレースフルシャットダウンできません。

手順

ステップ 1 電源プラグは DC 電源に配線した後に ISA 3000 に接続します。

電源プラグの正しい配線手順については、『[ハードウェア設定ガイド](#)』の「[DC 電源への接続](#)」を参照してください。

ステップ 2 ISA 3000 デバイスの前面にあるシステム LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。緑色に点滅している場合、デバイスはブートアップフェーズおよび POST (電源投入時自己診断テスト) の状態です。

すべてのデバイスが ISA 3000 に正しく接続されているか確認するには、『[ハードウェア設置ガイド](#)』の「[接続の確認](#)」を参照してください。

(任意) CLI での管理ネットワーク設定の変更

デフォルトの IP アドレスを使用できない場合（たとえば、デバイスを既存のネットワークに追加する場合）、コンソールポートに接続して、CLI で初期セットアップ（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の指定など）を実行できます。管理インターフェイスのみを設定できます。内部インターフェイスや外部インターフェイスは設定できません。これらは後で GUI を使用して設定できます。



(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。

手順

ステップ 1 脅威に対する防御 コンソールポートに接続します。詳細については、[Threat Defense CLI へのアクセス \(31 ページ\)](#) を参照してください。

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

(注) パスワードがすでに変更されていて、パスワードがわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。手順については、『[Cisco ASA and Firepower Threat Defense Device Reimage Guide](#)』を参照してください。

ステップ 2 Threat Defense に初めてログインすると、エンドユーザーライセンス契約 (EULA) に同意して管理者パスワードを変更するように求められます。その後、CLI セットアップスクリプトが表示されます。

デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

次のガイドラインを参照してください。

- [管理インターフェイスの IPv4 デフォルトゲートウェイを入力します (Enter the IPv4 default gateway for the management interface)] : 手動 IP アドレスを設定した場合は、「**data-interfaces**」またはゲートウェイルータの IP アドレスのいずれかを入力します。**data-interfaces** を設定すると、アウトバウンド管理トラフィックがバックプレーン経由で送信され、データインターフェイスが終了します。この設定は、インターネットにアクセスできる個別の管理ネットワークがない場合に役立ちます。管理インターフェイスから発信されるトラフィックには、インターネットアクセスを必要とするライセンス登録とデータベースの更新が含まれます。**data-interfaces** を使用する場合、管理ネットワークに直接接続していれば管理インターフェイスで Device Manager（または SSH）を引き続き使用できますが、特定のネットワークまたはホストのリモート管理の場合は、**configure network**

static-routes コマンドを使用して静的ルートを追加する必要があります。データインターフェイスでの Device Manager の管理は、この設定の影響を受けないことに注意してください。DHCPを使用する場合、システムはDHCPによって提供されるゲートウェイを使用します。DHCP がゲートウェイを提供しない場合は、フォールバックメソッドとして **data-interfaces** を使用します。

- [ネットワーク情報が変更された場合は再接続が必要になります (If your networking information has changed, you will need to reconnect)] : SSH でデフォルトの IP アドレスに接続しているのに、初期セットアップでその IP アドレスを変更すると、接続が切断されます。新しい IP アドレスとパスワードで再接続してください。コンソール接続は影響を受けません。
- [デバイスをローカルで管理しますか (Manage the device locally?)] : または Device Manager を使用するには [はい (yes)] を入力します。[いいえ (no)] と応えると、Management Center デバイスの管理にはオンプレミスまたはクラウド配信を使用することになります。

例 :

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

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

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: *****
Confirm new password: *****
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
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]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

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

>
```

ステップ3 新しい管理 IP アドレスで Device Manager にログインしてください。

へのログインDevice Manager

Device Manager にログインして 脅威に対する防衛 を設定します。

始める前に

- Firefox、Chrome、Safari、Edge、または Internet Explorer の最新バージョンを使用します。

手順

ステップ 1 ブラウザに次の URL を入力します。

- 管理 : <https://192.168.45.45>。CLI セットアップで管理 IP アドレスを変更した場合は、そのアドレスを入力します。
- (6.4 以前のみ) 内部 : <https://192.168.1.1>。任意の内部 BVI インターフェイス (Ethernet1/2 から 1/4) の内部アドレスに接続できます。6.5 以降の場合、デフォルト設定ではデータインターフェイスの管理が事前設定されません。

ステップ 2 ユーザー名 **admin**、デフォルトパスワード **Admin123** を使用してログインします。

次のタスク

- 6.4 以前の場合 : Device Manager セットアップウィザードを実行します。 [初期設定の完了 \(6.4 以前\) \(17 ページ\)](#) を参照してください。 6.5 以降の場合 : ISA 3000 はセットアップウィザードをサポートしていません。出荷前に特別なデフォルト設定が適用されます。FTD を手動で設定するには、 [初期設定の完了 \(6.5 以降\) \(12 ページ\)](#) を参照してください。

初期設定の完了 (6.5 以降)

ここでは、次の重要設定を設定する方法について説明します。

- BVI 1 IP アドレス : ブリッジグループ メンバー インターフェイス間でトラフィックが流れるには、BVI 1 IP アドレスを設定する必要があります。
- デバイスで発信されるトラフィックのデフォルトルート : すべてのインターフェイスはブリッジグループの一部であり、トラフィック転送に MAC アドレスルックアップを使用します。ただし、デバイスで発信されるトラフィックの場合は、デフォルトルートが必要です。管理ゲートウェイをデータインターフェイスに変更すると、このルートは管理インターフェイストラフィックにも使用されます。

手順

ステップ 1 CLI セットアップスクリプト ([\(任意\) CLI での管理ネットワーク設定の変更 \(10 ページ\)](#)) を使用していない場合、この接続が最初の接続であれば、次のプロンプトが表示されます。

- エンドユーザーライセンス契約書を確認して、内容に同意します。
- admin パスワードを変更します。
- 90 日間の評価ライセンスに同意します

ステップ2 BVI1 IP アドレスを設定します。

ブリッジグループメンバー インターフェイス間でトラフィックが流れるには、BVI1 IP アドレスを設定する必要があります。

- a) [デバイス (Device)] ページで、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックし、[ブリッジグループ (Bridge Groups)] をクリックします。
- b) BVI1 ブリッジグループの編集アイコン (🔗) をクリックします。
- c) [IPv4アドレス (IPv4 Address)] タブをクリックして、IPv4 アドレスを設定します。

[タイプ (Type)] フィールドから次のいずれかのオプションを選択します。

- [スタティック (Static)] : 変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。ブリッジグループの IP アドレスとサブネットマスクを入力します。接続されているエンドポイントはすべて、このネットワーク上に存在することになります。このアドレスがネットワーク上ですでに使用されていないことを確認します。

高可用性を設定し、このインターフェイスの HA をモニターしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイアドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブ ユニッツはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。

- [DHCP] : ネットワーク上の DHCP サーバーからアドレスを取得する場合は、このオプションを選択します。これはブリッジグループの一般的なオプションではありませんが、必要に応じて設定できます。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。

- [DHCPを使用してデフォルトルートを取得 (Obtain Default Route Using DHCP)] : デフォルトルートを DHCP サーバーから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。

- d) [IPv6アドレス (IPv6 Address)] タブをクリックして、IPv6 アドレスを設定します。

- [状態 (State)] : グローバルアドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、スライダをクリックして有効にします (🔘)。リンクローカルアドレスはインターフェイスの MAC アドレス (*Modified EUI-64* 形式) に基づいて生成されます。

(注) IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [スタティックアドレスとプレフィックス (Static Address/Prefix)]: ステータス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワークプレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。
- [RAを抑制 (Suppress RA)]: ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、脅威に対する防御はルータアドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ (ICMPv6 Type 134) は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

ルータ アドバタイズメントもルータ要請メッセージ (ICMPv6 Type 133) に応答して送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定できます。

脅威に対する防御 デバイスで IPv6 プレフィックスを提供する必要がないインターフェイス (外部インターフェイスなど) では、これらのメッセージを抑制できます。

- [スタンバイ IP アドレス (Standby IP Address)]: 高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイアドレスは、スタンバイデバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。

e) [OK] をクリックします。

ステップ 3 デバイスで発信されるトラフィックのデフォルトルートを設定します。

すべてのインターフェイスはブリッジグループの一部であり、トラフィック転送に MAC アドレスルックアップを使用します。ただし、デバイスで発信されるトラフィックの場合は、デフォルトルートが必要です。管理ゲートウェイをデータインターフェイス (デフォルト) のままにすると、このルートは管理インターフェイス トラフィックにも使用されます。

- a) [デバイス (Device)] をクリックしてから、[ルーティング (Routing)] サマリーにあるリンクをクリックします。

[スタティックルーティング (Static Routing)] ページが表示されます。


- b) **+** または [スタティックルートの作成 (Create Static Route)] をクリックします。
- c) デフォルトルートのプロパティを設定します。

The screenshot shows a dialog box titled "Add Static Route". It contains the following fields and options:

- Name:** default
- Description:** (empty text area)
- Protocol:** IPv4 (selected), IPv6
- Gateway:** gateway
- Interface:** bvi1 (BV11)
- Metric:** 1
- Networks:** + any-ipv4
- SLA Monitor:** Please select an SLA Monitor

Buttons: CANCEL, OK

1. [名前 (Name)]を入力します。たとえば「default」とします。
2. [IPv4] または [IPv6] ラジオボタンをクリックします。
IPv4 と IPv6 に対して個別のデフォルトルートを作成する必要があります。
3. [ゲートウェイ (Gateway)]をクリックしてから [新しいネットワークの作成 (Create New Network)]をクリックして、ゲートウェイ IP アドレスをホストオブジェクトとして追加します。[OK] をクリックしてオブジェクトを追加します。

4. [インターフェイス (Interface)] で [BVI1] を選択します。
5. [ネットワーク (Network)]  アイコンをクリックし、IPv4 デフォルトルートの場合は [any-ipv4]、IPv6 デフォルトルートの場合は [any-ipv6] を選択します。
- d) [OK] をクリックします。
- e) [OK] をクリックします。

ステップ 4 (任意) CLI での管理ネットワーク設定の変更 (10 ページ) を使用して新しい管理 IP アドレスとゲートウェイを設定していない場合は、[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] ページで IP アドレスとゲートウェイを変更できます。ブラウザを使用して新しいアドレスに再接続する必要があります。

ステップ 5 Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。

このアイコンは、展開されていない変更がある場合にドットマークで強調表示されます。



[保留中の変更 (Pending Changes)] ウィンドウには、設定の展開バージョンと保留中の変更との比較が表示されます。それらの変更は、削除された要素、追加された要素、または編集された要素を示すために色分けされています。色の説明については、ウィンドウの凡例を参照してください。

ステップ 6 変更内容に問題がない場合は、[今すぐ展開 (Deploy Now)] をクリックして、ジョブをすぐに開始できます。

ウィンドウに展開が進行中であることが示されます。ウィンドウを閉じるか、または展開が完了するまで待機できます。展開が進行中の間にウィンドウを閉じて、ジョブは停止しません。結果は、タスクリストや監査ログで確認できます。ウィンドウを開いたままにした場合、[展開履歴 (Deployment History)] リンクをクリックすると結果が表示されます。

次のタスク

- 評価ライセンスを引き続き使用することもできますが、デバイスを登録してライセンスを取得することをお勧めします。[ライセンスの設定 \(19 ページ\)](#) を参照してください。
- また、デバイスの設定を選択することもできます。[Device Manager \(6.5 以降\) でのデバイスの設定 \(24 ページ\)](#) を参照してください。

初期設定の完了 (6.4 以前)

初期設定を完了するには、最初に Device Manager にログインしたときにセットアップウィザードを使用します。セットアップウィザードの完了後、いくつかの基本ポリシーが適切に設定された機能しているデバイスが必要です。

- 外部 (GigabitEthernet1/1) および内部インターフェイス。GigabitEthernet1/2 ~ 1/4 は、ブリッジグループメンバー内にあります。
- 内部インターフェイスと外部インターフェイスのセキュリティゾーン。
- 内部から外部へのすべてのトラフィックを信頼するアクセスルール。
- 内部から外部へのすべてのトラフィックを外部インターフェイスの IP アドレスの固有のポートへ変換するインターフェイス NAT ルール。
- 内部インターフェイスで実行されている DHCP サーバー。



(注) [\(任意\) CLI での管理ネットワーク設定の変更 \(10 ページ\)](#) の手順を実行した場合は、これらのタスクの一部、具体的には管理者パスワードの変更、および外部インターフェイスと管理インターフェイスの設定がすでに完了しているはずです。

手順

ステップ 1 エンドユーザー ライセンス契約書を読んで同意し、管理者パスワードを変更するように求められます。

続行するには、これらの手順を完了する必要があります。

ステップ 2 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ (Next)]をクリックします。

(注) [次へ (Next)]をクリックすると、設定がデバイスに展開されます。インターフェイスの名前は「外部」となり、「outside_zone」セキュリティゾーンに追加されます。設定値が正しいことを確認します。

- a) [外部インターフェイス (Outside Interface)]: これは、ゲートウェイ ルータに接続するためのデータポートです。デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータインターフェイスがデフォルトの外部インターフェイスです。

[IPv4の設定 (Configure IPv4)]: 外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ (Off)]を選択して、IPv4 アドレスを設定しないという選択肢もあります。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。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。

[IPv6の設定 (Configure IPv6)]: 外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ (Off)]を選択して、IPv6 アドレスを設定しないという選択肢もあります。

- b) [管理インターフェイス (Management Interface)]

[DNSサーバ (DNS Servers)]: システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻りたい場合は、[OpenDNSを使用 (Use OpenDNS)]をクリックすると、フィールドに適切な IP アドレスがリロードされます。

[ファイアウォールホスト名 (Firewall Hostname)]: システムの管理アドレスのホスト名です。

ステップ 3 システム時刻を設定し、[次へ (Next)]をクリックします。

- a) [タイムゾーン (Time Zone)]: システムのタイムゾーンを選択します。
- b) [NTPタイムサーバ (NTP Time Server)]: デフォルトの NTP サーバを使用するか、使用している NTP サーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。

ステップ 4 (任意) システムのスマートライセンスを設定します。

Threat Defense デバイスを購入すると、自動的に基本ライセンスが付いてきます。すべての追加ライセンスはオプションです。

スマートライセンスのアカウントを取得し、システムが必要とするライセンスを適用する必要があります。最初は 90 日間の評価ライセンスを使用し、後でスマートライセンスを設定できます。

デバイスを今すぐ登録するには、リンクをクリックして Smart Software Manager のアカウントにログインします。[ライセンスの設定 \(19 ページ\)](#) を参照してください。

評価ライセンスを使用するには、[登録せずに90日間の評価期間を開始する (Start 90 day evaluation period without registration)] を選択します。

ステップ 5 [終了 (Finish)] をクリックします。

次のタスク

- 評価ライセンスを引き続き使用することもできますが、デバイスを登録し、ライセンスを取得することをお勧めします。を参照してください[ライセンスの設定 \(19 ページ\)](#)。
- Device Manager を使用してデバイスを設定することもできます。「[Device Manager \(6.4 以前\) でのファイアウォールの設定 \(26 ページ\)](#)」を参照してください。

ライセンスの設定

脅威に対する防御 は、ライセンスの購入およびライセンス プールの一元管理が可能なシスコ スマート ソフトウェア ライセンシングを使用します。

シャーシを登録すると、License Authority によって シャーシと License Authority 間の通信に使用される ID 証明書が発行されます。また、適切な仮想アカウントにシャーシが割り当てられます。

基本ライセンスは自動的に含まれます。スマート ライセンシングでは、まだ購入していない製品機能を使用することはできませんが、次のオプション機能ライセンスを購入して準拠する必要があります。

- **Cisco Secure Firewall Threat Defense の IPS** : セキュリティ インテリジェンスと Cisco Secure IPS
- **Cisco Secure Firewall Threat Defense のマルウェア防御** : マルウェア防御
- **Cisco Secure Firewall Threat Defense の URL フィルタリング** : URL フィルタリング
- **RA VPN** : AnyConnect Plus、AnyConnect Apex、または AnyConnect VPN 専用。

上記のライセンスに加えて、1、3、または5年のアップデートにアクセスするため、該当するサブスクリプションを購入する必要があります。

システムのライセンシングの詳細については、『[FDM コンフィグレーション ガイド](#)』を参照してください。

始める前に

- [Cisco Smart Software Manager](#) にマスター アカウントを持ちます。

まだアカウントをお持ちでない場合は、リンクをクリックして[新しいアカウントを設定](#)してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

- (輸出コンプライアンスフラグを使用して有効化される) 機能を使用するには、ご使用のシスコ スマート ソフトウェア ライセンシング アカウントで強力な暗号化 (3DES/AES) ライセンスを使用できる必要があります。

手順

ステップ 1 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

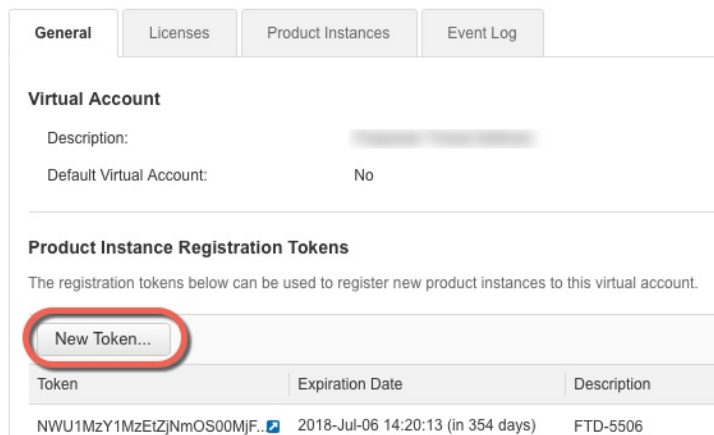
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマートソフトウェアライセンス アカウントにリンクされています。

ステップ 2 [Smart Software Manager](#) で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。



b) [General] タブで、[New Token] をクリックします。



c) [登録トークンを作成 (Create Registration Token)] ダイアログボックスで、以下の設定値を入力してから [トークンを作成 (Create Token)] をクリックします。

Create Registration Token

This dialog will generate the token required to register your product instances with your Smart Account.

Virtual Account: [Redacted]

Description: [Empty text box]

* Expire After: [30] Days

Enter the value between 1 and 365, but Cisco recommends a maximum of 30 days.

Allow export-controlled functionality on the products registered with this token

[Create Token] [Cancel]

• [説明 (Description)]

• [有効期限 (Expire After)] : 推奨値は 30 日です。

• [このトークンに登録された製品で輸出管理機能を許可する (Allow export-controlled functionality on the products registered with this token)] : 高度暗号化が許可されている国の場合は輸出コンプライアンスフラグを有効にします。

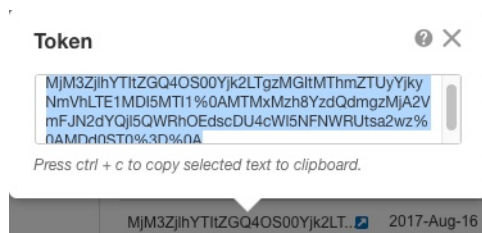
トークンはインベントリに追加されます。

- d) トークンの右側にある矢印アイコンをクリックして [トークン (Token)] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。脅威に対する防御の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 3: トークンの表示

Token	Expiration Date	Description	Export-Controlled	Created By	Actions
MjM3ZjhhYTIzGQ4OS00Yjk2LT...	2017-Aug-16 19:41:53 (in 30 days)	ASA FP 2110 1	Allowed	[Redacted]	[Copy icon] Actions

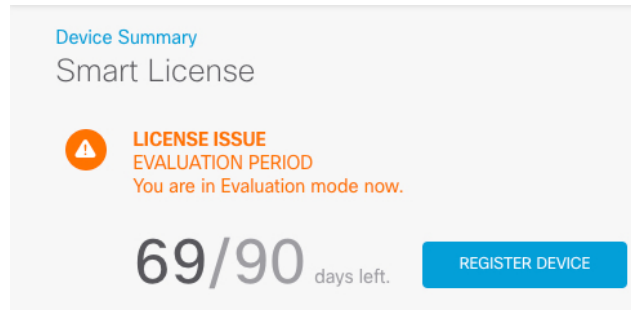
図 4: トークンのコピー



ステップ 3 Device Manager で [デバイス (Device)] をクリックし、 [スマートライセンス (Smart License)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

[スマートライセンス (Smart License)] ページが表示されます。

ステップ 4 [デバイスの登録 (Register Device)] をクリックします。



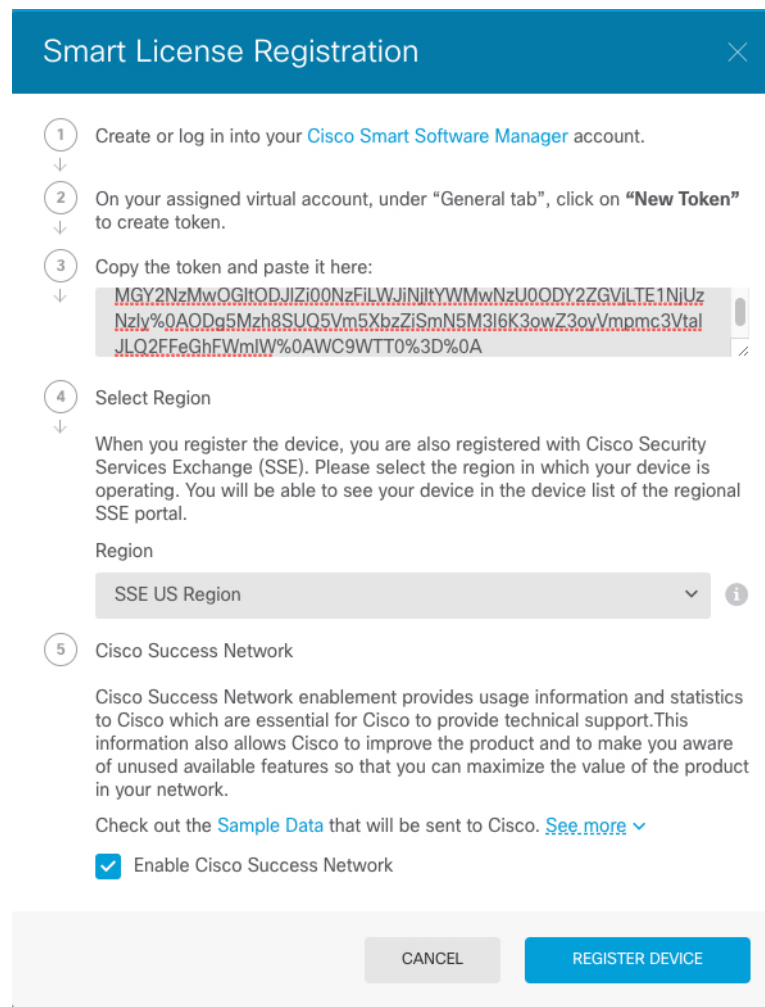
Device Summary
Smart License

LICENSE ISSUE
EVALUATION PERIOD
You are in Evaluation mode now.

69/90 days left.

REGISTER DEVICE

次に、 [スマートライセンス登録 (Smart License Registration)] ダイアログボックスの指示に従って、トークンに貼り付けます。



Smart License Registration

- Create or log in into your [Cisco Smart Software Manager](#) account.
- On your assigned virtual account, under "General tab", click on "New Token" to create token.
- Copy the token and paste it here:

```
MGY2Nz-MwOGItODJIZi00NzFiLWJiNitYWMwNzU0ODY2ZGVlTE1NIUz
Nzly%QAODq5Mzh8SUQ5Vm5XbzZiSmN5M3I6K3owZ3ovVmpmc3Vtal
JLQ2FFeGhFWmIW%0AWC9WTT0%3D%0A
```
- Select Region
 When you register the device, you are also registered with Cisco Security Services Exchange (SSE). Please select the region in which your device is operating. You will be able to see your device in the device list of the regional SSE portal.
 Region
 SSE US Region
- Cisco Success Network
 Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.
 Check out the [Sample Data](#) that will be sent to Cisco. [See more](#)
 - Enable Cisco Success Network

CANCEL REGISTER DEVICE

ステップ 5 [デバイスの登録 (Register Device)] をクリックします。

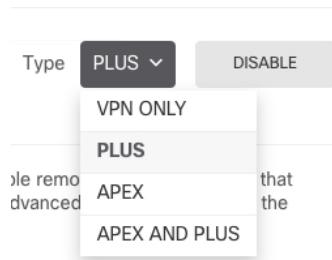
[スマートライセンス (Smart License)] ページに戻ります。デバイス登録中は次のメッセージが表示されます。

Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in Task List. Refresh this page to see the updated status.

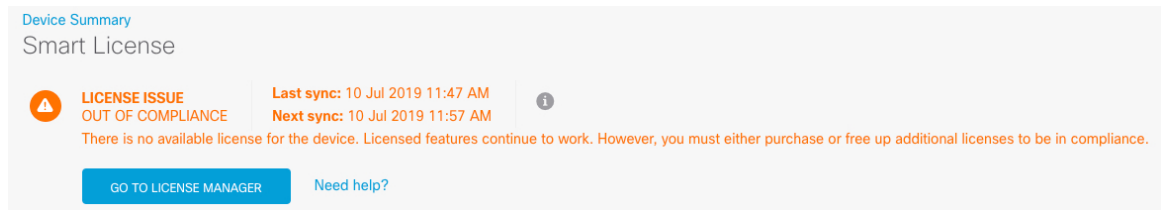
デバイスが正常に登録され、ページが更新されると、次のように表示されます。

ステップ 6 必要に応じて、それぞれのオプションライセンスの [有効化/無効化 (Enable/Disable)] コントロールをクリックします。

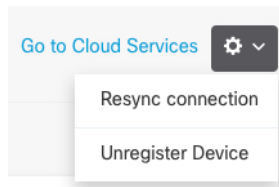
- [有効化 (Enable)] : Cisco Smart Software Manager アカウントにライセンスを登録し、制御された機能が有効になります。ライセンスによって制御されるポリシーを設定し、展開できます。
- [無効化 (Disable)] : Cisco Smart Software Manager アカウントのライセンスを登録解除し、制御された機能が無効になります。新しいポリシーの機能の設定も、その機能を使用するポリシーの展開もできません。
- **RA VPN** ライセンスを有効にした場合は、使用するライセンスのタイプ ([Plus]、[Apex]、[VPN 専用 (VPN Only)]、または [Plus と Apex (Plus and Apex)]) を選択します。



機能を有効にすると、アカウントにライセンスがない場合はページを更新した後に次の非準拠メッセージが表示されます。



ステップ 7 歯車ドロップダウンリストから [接続の再同期 (Resync Connection)] を選択して、Cisco Smart Software Manager とライセンス情報を同期させます。



Device Manager (6.5 以降) でのデバイスの設定

次の手順では、追加機能の設定の概要を説明します。各手順について詳細な情報を表示するには、ページのヘルプ ボタン (?) をクリックしてください。

手順

ステップ 1 ブリッジグループ インターフェイスを変換する場合は、[デバイス (Device)] を選択し、[インターフェイス (Interfaces)] の概要のリンクをクリックします。

各インターフェイスの編集アイコン (🔗) をクリックしてモードを設定し、IP アドレスなどの設定を定義します。

次の例では、Web サーバーなどのパブリックアクセス可能な資産を配置する「緩衝地帯」(DMZ) として使用するためのインターフェイスを構成します。完了したら [保存 (Save)] をクリックします。

図 5: インターフェイスの編集

Interface Name: dmz Status:

Description:

IPv4 Address IPv6 Address Advanced Options

Type: Static

IP Address and Subnet Mask: 192.168.6.1 / 24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

ステップ 2 [ポリシー (Policies)] を選択してネットワークのセキュリティポリシーを構成します。

デフォルトでは、すべてのインターフェイス間ですべてのトラフィックが許可されます。他のセキュリティゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。さらに、組織が必要とする結果を得るために、その他のポリシーを設定して、追加サービスの提供や、アクセスルールを微調整できます。次のポリシーを設定できます。

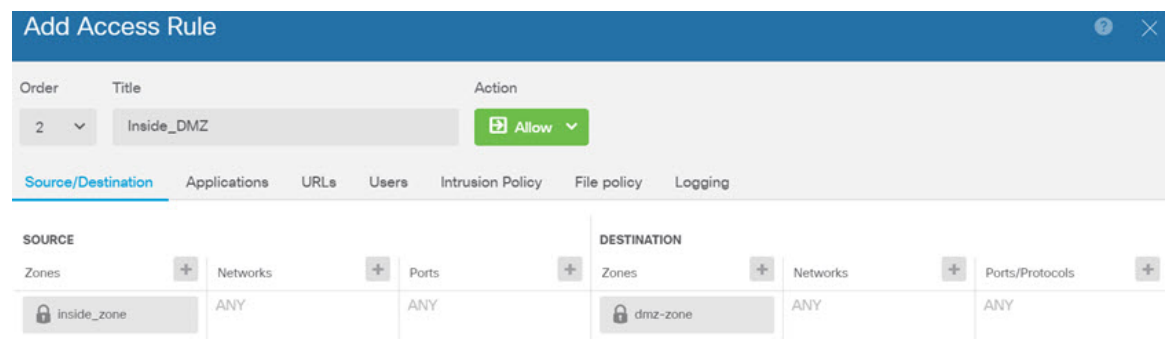
- [SSL復号 (SSL Decryption)] : 侵入、マルウェアなどについて暗号化された接続 (HTTPS など) を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するには SSL 復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。
- [アイデンティティ (Identity)] : 個々のユーザーにネットワークアクティビティを関連付ける、またはユーザーまたはユーザーグループのメンバーシップに基づいてネットワークアクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザーを判定するためにアイデンティティポリシーを使用します。
- [セキュリティインテリジェンス (Security Intelligence)] : ブラックリスト登録済みの IP アドレスまたは URL の接続をただちにドロップするには、セキュリティインテリジェンスポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセスコントロールポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティインテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスや URL の定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。
- [NAT] (ネットワークアドレス変換) : 内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。
- [アクセス制御 (Access Control)] : ネットワーク上で許可する接続の決定にアクセスコントロールポリシーを使用します。セキュリティゾーン、IP アドレス、プロトコル、ポー

ト、アプリケーション、URL、ユーザーまたはユーザーグループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル（マルウェア）ポリシーを適用します。このポリシーを使用して URL フィルタリングを実装します。

- [侵入 (Intrusion)]: 侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。

次の例では、アクセス制御ポリシーで内部ゾーンと DMZ ゾーンの間でのトラフィックを許可する方法を示します。この例では、[接続の最後で (At End of Connection)] が選択されている場合、[ロギング (Logging)] を除いて他のいずれのタブでもオプションは設定されません。

図 6: アクセスコントロールポリシー



ステップ 3 [デバイス (Device)] を選択してから、[更新 (Updates)] グループで [設定の表示 (View Configuration)] をクリックし、システムデータベースの更新スケジュールを設定します。

侵入ポリシーを使用している場合は、ルールと VDB のデータベースを定期的な更新を設定します。セキュリティ情報フィードを使用する場合は、それらの更新スケジュールを設定します。一致基準としてセキュリティポリシーで地理位置情報を使用する場合は、そのデータベースの更新スケジュールを設定します。

ステップ 4 メニューの [導入 (Deploy)] ボタンをクリックし、[今すぐ導入する (Deploy Now)] ボタン



() をクリックして、変更内容をデバイスに展開します。

変更は、それらを展開するまでデバイスで有効になりません。

Device Manager (6.4 以前) でのファイアウォールの設定

次の手順では、追加機能の設定の概要を説明します。各手順について詳細な情報を表示するには、ページのヘルプ ボタン (?) をクリックしてください。

手順

- ステップ 1** □ブリッジグループ インターフェイスを変換する場合は、[デバイス (Device)] を選択して [インターフェイス (Interfaces)] の概要のリンクをクリックします。

各インターフェイスの編集アイコン (🔗) をクリックしてモードを設定し、IP アドレスなどの設定を定義します。

次の例では、Web サーバーなどのパブリックアクセス可能な資産を配置する「緩衝地帯」(DMZ) として使用するためのインターフェイスを構成します。完了したら [保存 (Save)] をクリックします。

図 7: インターフェイスの編集

The screenshot shows the 'Edit Physical Interface' configuration page. At the top, there is a blue header with the title 'Edit Physical Interface'. Below the header, there are two main sections: 'Interface Name' and 'Status'. The 'Interface Name' field contains the text 'dmz'. The 'Status' section has a toggle switch that is currently turned on (blue). Below these is a 'Description' field, which is currently empty. Underneath the description field are three tabs: 'IPv4 Address' (which is selected and highlighted in blue), 'IPv6 Address', and 'Advanced Options'. Below the tabs, there is a 'Type' dropdown menu set to 'Static'. Below that is the 'IP Address and Subnet Mask' section, which contains two input fields: the first contains '192.168.6.1' and the second contains '24'. At the bottom of this section, there is a small note: 'e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0'.

- ステップ 2** 新しいインターフェイスを構成する場合は、[オブジェクト (Objects)] を選択し、目次から [セキュリティゾーン (Security Zones)] を選択します。

編集または必要に応じて新しいゾーンを作成します。インターフェイスではなく、セキュリティゾーンに基づいてポリシーを構成するため、各インターフェイスはゾーンに属している必要があります。インターフェイスを構成する場合、ゾーンにインターフェイスを置くことはできません。このため、新しいインターフェイスを作成した後、または既存のインターフェイスの目的を変更した後は常にゾーンオブジェクトを編集する必要があります。

次の例では、DMZインターフェイスのために新しいDMZゾーンを作成する方法を示します。

図 8: セキュリティゾーンオブジェクト

ステップ 3 内部クライアントで DHCP を使用してデバイスから IP アドレスを取得する場合は、[デバイス (Device)] > [システム設定 (System Settings)] > [DHCPサーバー (DHCP Server)] を選択してから、[DHCPサーバー (DHCP Servers)] タブを選択します。

すでに内部インターフェイス用に構成されている DHCP サーバーがありますが、アドレスプールを編集したり、それを削除したりすることができます。他の内部インターフェイスを構成した場合は、それらのインターフェイス上に DHCP サーバーをセットアップするのがごく一般的です。[+] をクリックして各内部インターフェイスのサーバーとアドレスプールを構成します。

[構成 (Configuration)] タブでクライアントに提供される WINS および DNS のリストを微調整することもできます。次の例では、アドレスプールの 192.168.4.50 ~ 192.168.4.240 で inside2 インターフェイス上の DHCP サーバーを設定する方法を示しています。

図 9: DHCPサーバー

ステップ 4 [デバイス (Device)] を選択してから、[ルーティング (Routing)] グループで [設定の表示 (View Configuration)] (または [最初のスタティックルートを作成 (Create First Static Route)]) をクリックし、デフォルトルートを構成します。

デフォルトルートは通常、外部インターフェイス以外に存在するアップストリームまたは ISP ルータを指しています。デフォルトの IPv4 ルートは任意の ipv4 (0.0.0.0/0)、デフォルトの IPv6 ルートは任意の ipv6 (:::0/0) です。使用する IP バージョンごとにルートを作成します。

外部インターフェイスのアドレスの取得に DHCP を使用する場合、必要なデフォルトルートをすでに持っていることがあります。

(注) このページで定義したルートは、データ インターフェイス用のみです。管理インターフェイスには影響しません。[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] で管理ゲートウェイを設定します。

次の例に、IPv4 のデフォルトルートを示します。この例では、isp ゲートウェイは ISP ゲートウェイの IP アドレスを識別するネットワーク オブジェクトです (アドレスは ISP から取得する必要があります)。[ゲートウェイ (Gateway)] の下部の [新しいネットワークを作成する (Create New Network)] ドロップダウンリストをクリックしてこのオブジェクトを作成することができます。

図 10: デフォルトルート

The screenshot shows the 'Add Static Route' configuration interface. It includes the following fields and options:

- Protocol:** Radio buttons for IPv4 (selected) and IPv6.
- Gateway:** A text input field containing 'isp-gateway'.
- Interface:** A text input field containing 'outside'.
- Metric:** A text input field containing '1'.
- Networks:** A dropdown menu with a plus sign and a selected item 'amy-ipv4'.

ステップ 5 [ポリシー (Policies)] を選択してネットワークのセキュリティ ポリシーを構成します。

デバイス セットアップ ウィザードは、内部ゾーンと外部ゾーンの間でのトラフィック フローを有効にします。また、外部インターフェイスを使用する場合に、全インターフェイスに対するインターフェイス NAT も有効にします。新しいインターフェイスを構成した場合でも、内部ゾーンオブジェクトに追加する場合はそれらにアクセス制御ルールが自動的に適用されます。

ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィックフローを許可するアクセス制御ルールが必要です。他のセキュリティゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。これらは最低限の変更になります。

さらに、組織が必要とする結果を得るために、その他のポリシーを設定して、追加サービスの提供や、NAT およびアクセス ルールを微調整できます。次のポリシーを設定できます。

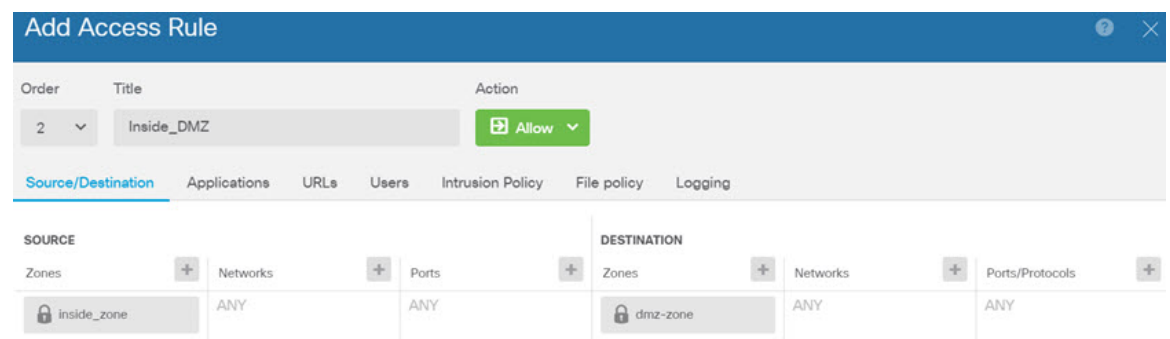
- [SSL 復号 (SSL Decryption)]: 侵入、マルウェアなどについて暗号化された接続 (HTTPS など) を検査する場合は、接続を復号化する必要があります。どの接続を復号化する必要があります。

あるかを判断するには SSL 復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。

- [アイデンティティ (Identity)] : 個々のユーザーにネットワークアクティビティを関連付ける、またはユーザーまたはユーザーグループのメンバーシップに基づいてネットワークアクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザーを判定するためにアイデンティティポリシーを使用します。
- [セキュリティインテリジェンス (Security Intelligence)] : ブラックリスト登録済みの IP アドレスまたは URL の接続をただちにドロップするには、セキュリティインテリジェンスポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセスコントロールポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティインテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスや URL の定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。
- [NAT] (ネットワークアドレス変換) : 内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。
- [アクセス制御 (Access Control)] : ネットワーク上で許可する接続の決定にアクセスコントロールポリシーを使用します。セキュリティゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザーまたはユーザーグループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル (マルウェア) ポリシーを適用します。このポリシーを使用して URL フィルタリングを実装します。
- [侵入 (Intrusion)] : 侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。

次の例では、アクセス制御ポリシーで内部ゾーンと DMZ ゾーンの間でのトラフィックを許可する方法を示します。この例では、[接続の最後で (At End of Connection)] が選択されている場合、[ロギング (Logging)] を除いて他のいずれのタブでもオプションは設定されません。

図 11: アクセスコントロールポリシー



- ステップ 6** [デバイス (Device)] を選択してから、[更新 (Updates)] グループで [設定の表示 (View Configuration)] をクリックし、システムデータベースの更新スケジュールを設定します。

侵入ポリシーを使用している場合は、ルールと VDB のデータベースを定期的な更新を設定します。セキュリティ情報フィードを使用する場合は、それらの更新スケジュールを設定します。一致基準としてセキュリティポリシーで地理位置情報を使用する場合は、そのデータベースの更新スケジュールを設定します。

ステップ 7 メニューの [導入 (Deploy)] ボタンをクリックし、[今すぐ導入する (Deploy Now)] ボタン



をクリックして、変更内容をデバイスに展開します。

変更は、それらを展開するまでデバイスで有効になりません。

Threat Defense CLI へのアクセス

コマンドラインインターフェイス (CLI) を使用してシステムのセットアップを行い、基本的なシステムのトラブルシューティングを行います。CLI セッションからポリシーを設定することはできません。CLI には、コンソールポートに接続してアクセスできます。

脅威に対する防御 デバイスの管理インターフェイスに SSH で接続できます。SSH 接続用のインターフェイスを開いている場合、データインターフェイス上のアドレスにも接続できます。データインターフェイスへの SSH アクセスはデフォルトで無効になっています。

手順

ステップ 1 CLI にログインして、管理コンピュータをコンソールポート、RJ-45 ポート、ミニ USB ポートのいずれかに接続します。ご使用のオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

ステップ 2 ユーザー名 **admin**、および初期セットアップ時に設定したパスワードを使用して脅威に対する防御 CLI にログインします (デフォルトは **Admin123**)。

ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用法の詳細については、『[Cisco Firepower Threat Defense Command Reference](#)』を参照してください。

ファイアウォールの電源の切断

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、ファイアウォール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。

ISA 3000 シャーシには、外部電源スイッチはありません。Device Manager を使用してファイアウォールの電源を切断するか、CLI を使用できます。

Device Manager を使用したファイアウォールの電源の切断

Device Manager を使用してシステムを適切にシャットダウンできます。



(注) シャットダウンは 7.0.2+/7.2+ でサポートされています。

手順

ステップ 1 Device Manager を使用してファイアウォールをシャットダウンします。

- a) [デバイス (Device)] をクリックしてから、[システム設定 (System Settings)] > [再起動/シャットダウン (Reboot/Shutdown)] リンクをクリックします。
- b) [シャットダウン (Shut Down)] をクリックします。

ステップ 2 シャットダウンプロセスをモニターします。デバイスを監視できない場合は、約 3 分間待ってシステムがシャットダウンしたことを確認します。

- コンソール：コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.  
It is safe to power off now.  
  
To restart the device, you must Power cycle to the device.
```

ステップ 3 必要に応じて電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

CLI におけるファイアウォールの電源の切断

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。ISA 3000 シャーシには、外部電源スイッチはありません。



(注) シャットダウンは 7.0.2+/7.2+ でサポートされています。

手順

ステップ 1 コンソールポートに接続して脅威に対する防御 CLI にアクセスし、脅威に対する防御 をシャットダウンします。

shutdown

例：

```
> shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense.....ok
Shutting down sfid... [ OK ]
Clearing static routes
Unconfiguring default route [ OK ]
Unconfiguring address on br1 [ OK ]
Unconfiguring IPv6 [ OK ]
Downing interface [ OK ]
Stopping xinetd:
Stopping nsd... [ OK ]
Stopping system log daemon... [ OK ]
Stopping Threat Defense ...
Stopping system message bus: dbus. [ OK ]
Un-mounting disk partitions ...
device-mapper: remove ioctl on root failed: Device or resource busy
[...]
mdadm: Cannot get exclusive access to /dev/md0:Perhaps a running process, mounted
filesystem or active volume group?
Stopping OpenBSD Secure Shell server: sshd
stopped /usr/sbin/sshd (pid 3520)
done.
Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid
3525)
acpid.
Stopping system message bus: dbus.
Stopping internet superserver: xinetd.
no /etc/sysconfig/kdump.conf
Deconfiguring network interfaces... ifdown: interface br1 not configured
done.
SSP-Security-Module is shutting down ...
Sending ALL processes the TERM signal ...
acpid: exiting
Sending ALL processes the KILL signal ...
Deactivating swap...
Unmounting local filesystems...

Firepower Threat Defense stopped.
It is safe to power off now.
```

To restart the device, you must Power cycle to the device.

ステップ 2 脅威に対する防御 がシャットダウンし、コンソールに「今すぐに電源をオフにする」と表示された場合は、必要に応じて電源を抜いてシャーシから電源を物理的に取り外します。

次のステップ

Threat Defense の設定を続行するには、「[Cisco Firepower ドキュメント一覧](#)」にあるお使いのソフトウェアバージョンのマニュアルを参照してください。

Device Manager の使用に関する情報については、「[『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』](#)」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。