CHAPTER 5
仮想アプライアンスの設定

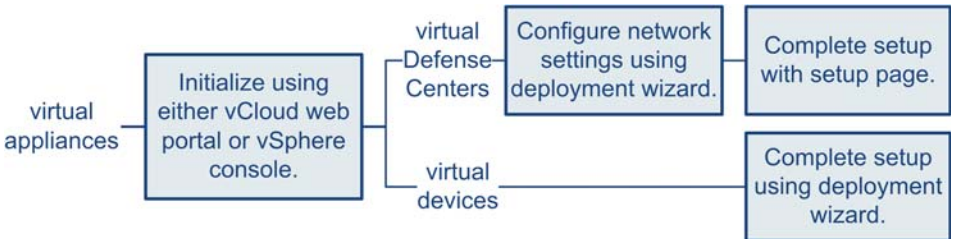
仮想アプライアンスをインストールしたら、設定プロセスを完了する必要があります。このプロセスにより、信頼された管理ネットワーク上で新しいアプライアンスが通信できるようになります。また、管理者パスワードを変更し、エンド ユーザ ライセンス契約（EULA）を承認する必要もあります。

設定プロセスにより、時間の設定、デバイスの登録とライセンシング、スケジュールの更新など、管理レベルの多数の初期タスクを実行することもできます。設定および登録時に選択したオプションにより、システムが作成および適用するデフォルトのインターフェイス、インライン セット、ゾーン、およびポリシーが決定されます。

これらの初期設定およびポリシーの目的は、すぐに使用できるエクスペリエンスを提供し、オプションを制限せずにユーザが展開を迅速に設定できるようにすることです。最初にデバイスをどのように設定するかに関係なく、防御センターを使用して設定を随時に変更することができます。つまり、設定時に検出モードまたはアクセス制御ポリシーを選択しても、ユーザが特定のデバイス ゾーンまたはポリシー設定には固定されることはありません。

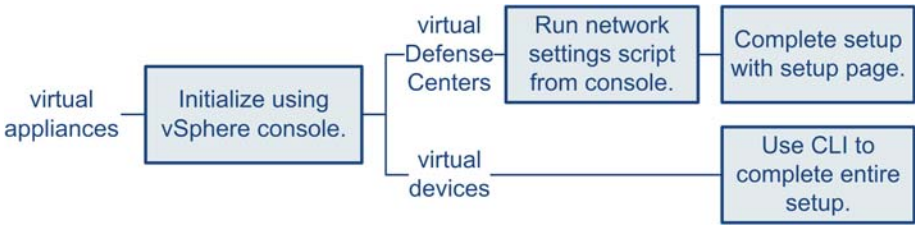
VI OVF テンプレートの展開

次の図は、VI OVF テンプレートを使用して展開する場合の、仮想防御センターおよび管理対象デバイスの設定の一般的なプロセスについて示しています。



ESXi OVF テンプレートの展開

次の図は、ESXi OVF テンプレートを使用して展開する場合の、仮想防御センターおよび管理対象デバイスの設定の一般的なプロセスについて示しています。



どのように展開する場合でも、最初に、初期化するアプライアンスの電源を入れてください。初期化が完了したら、VMware コンソールを使用してログインし、アプライアンスのタイプに応じて次のいずれかの方法で設定を完了します。

仮想デバイス

Web インターフェイスを持たない仮想デバイス。VI OVF テンプレートで展開すると、展開ウィザードを使用してデバイスを防御センターへ登録するなど、デバイスの初期設定を行うことができます。ESXi OVF テンプレートで展開する場合は、対話式のコマンドライン インターフェイス（CLI）を使用して初期設定を実行する必要があります。

仮想防御センター

VI OVF テンプレートで展開すると、展開でウィザードを使用してネットワークを設定することができます。セットアップ ウィザードを使用しない、または ESXi OVF テンプレートを使用して展開することを選択した場合は、スクリプトを使用してネットワークを設定します。ネットワークを設定した後で、管理ネットワーク上のコンピュータを使用して、防御センターの Web インターフェイスを参照するための設定プロセスを完了します。

ヒント! 複数のアプライアンスを展開する場合は、自身のデバイスを最初に設定し、次にそのデバイスを管理する防御センターを設定します。デバイスの初期設定プロセスにより、デバイスを事前に防御センターに登録することができ、防御センターの設定プロセスにより、事前に登録されていた管理対象デバイスを追加およびライセンス登録することができます。

詳細については、以下を参照してください。

- 「仮想アプライアンスの初期化」（P.74）
- 「CLI を使用した仮想デバイスの設定」（P.75）
- 「仮想防御センターの設定」（P.80）
- 「次の手順」（P.91）

仮想アプライアンスの初期化

仮想アプライアンスをインストールした後、仮想アプライアンスに初めて電源を入れると初期化が自動的に開始されます。

警告! 起動時間は、使用可能なサーバ リソース量など、いくつかの要因によって異なります。初期化が完了するまでに最大で 40 分かかることがあります。初期化は中断**しないで**ください。中断すると、アプライアンスを削除して、最初からやり直さなければならないことがあります。

仮想アプライアンスを初期化するには、次の手順を使用します。

仮想アプライアンスを初期化するには：

1. アプライアンスの電源をオンにします。
   - VMware vCloud Director の Web ポータルで、ディスプレイから [vApp] を選択して [Start] をクリックします。
   - vSphere Client で、インベントリ リストからインポートした仮想アプライアンスの名前を右クリックし、コンテキスト メニューで [Power] > [Power On] を選択します。

2. VMware コンソール タブで初期化を監視します。

   プロセスの最も長い 2 つの部分でメッセージが表示されます。プロセスが完了すると、ログイン プロンプトが表示されます。

次の手順は、アプライアンスのタイプと展開によって異なります。

VI OVF テンプレートを使用し、Sourcefire の必須設定を展開中に行った場合：

- 仮想防御センターについて、「仮想防御センターの設定」（P.80）に進んで設定を完了します。
- 仮想デバイスについては、これ以上設定することはありません。

ESXi OVF テンプレート使用している場合、または VI OVF テンプレートで展開したときに Sourcefire の必須設定を行っていない場合：

- 仮想防御センターについて、「仮想防御センターの設定」（P.80）に進み、スクリプトを使用してネットワークを設定し、仮想防御センターを設定します。
- 仮想デバイスについては、「CLI を使用した仮想デバイスの設定」（P.75）に進み、CLI を使用して仮想デバイスを設定します。

CLI を使用した仮想デバイスの設定

仮想デバイスには Web インターフェイスがないため、ESXi OVF テンプレートで展開した場合には、CLI を使用して仮想デバイスを設定する必要があります。VI OVF テンプレートで展開しており、展開時にセットアップ ウィザードを使用しなかった場合は、CLI を使用して、Sourcefire の必須設定を行うこともできます。

ヒント! VI OVF テンプレートで展開しており、セットアップ ウィザードを使用した場合は、仮想デバイスが設定されているため、これ以上の処理は必要ありません。

新しく設定されたデバイスに初めてログインするときに、EULA を読んで同意する必要があります。次に、セットアップ プロンプトに従って管理パスワードを変更し、デバイスのネットワーク設定および検出モードを設定します。

セットアップ プロンプトに従う場合に、複数の選択肢がある質問では、選択肢が `(y/n)` のように括弧で囲まれて示されます。デフォルトでは、`[y]` のように角括弧で囲まれています。選択を確定するには、Enter キーを押します。

CLI では、物理デバイスのセットアップ Web ページで要求される設定情報とほぼ同じ情報が要求されます。詳細については、『*Sourcefire 3D System Installation Guide*』を参照してください。

ヒント! 初期設定の完了後の仮想デバイスのこれらの設定を変更するには、CLI を使用します。詳細については、『*Sourcefire 3D System User Guide*』の「Command Line Reference」の章を参照してください。

デバイス ネットワークの設定について

Sourcefire 3D System には、IPv4 と IPv6 の両方の管理環境に対するデュアル スタックの実装が用意されています。ユーザは IPv4 または IPv6 の管理 IP アドレス、ネットマスクまたはプレフィクスの長さ、およびデフォルトのゲートウェイを設定する必要があります。また、デバイスに対してホスト名とドメインの他に、3 つまでの DNS サーバを指定することもできます。デバイスを再起動するまで、ホスト名は syslog に反映されないので注意してください。

検出モードについて

仮想デバイスに対して検出モードを選択すると、システムが最初にデバイス インターフェイスをどのように設定するか、およびこれらのインターフェイスがインライン セットとセキュリティ ゾーンのどちらに属するかが決定されます。検出モードはユーザが後から変更できない設定で、設定時にユーザが選択するだけのオプションです。このオプションの選択により、システムはデバイスの初期設定を調整して行うことができます。一般的には、デバイスがどのように展開されているかに基づいて検出モードを選択する必要があります。

パッシブ

デバイスが、侵入検知システム（IDS）としてパッシブに展開されている場合は、このモードを選択します。パッシブな展開では、仮想デバイスはネットワーク ディスカバリのほかに、ネットワークベースのファイルおよびマルウェアの検出、セキュリティ インテリジェンスの監視を行うことができます。

インライン

デバイスが、侵入防御システム（IPS）としてインラインで展開されている場合は、このモードを選択します。

重要! IPS 展開の一般的な方法はフェール オープンにし、一致しないトラフィックを許可することですが、仮想デバイスのインライン セットにはバイパス機能がありません。

ネットワーク ディスカバリ

デバイスが、ホスト、アプリケーション、およびユーザ ディスカバリのみを行うようパッシブに展開されている場合は、このモードを選択します。

次の表は、選択した検出モードごとに、システムが作成するインターフェイス、インライン セット、およびゾーンを示しています。

検出モードに基づいた初期設定

検出モード	セキュリティ ゾーン	インライン セット	インターフェイス
インライン	内部と外部	デフォルトのインライン セット	最初のペアはデフォルト インライン セットへ追加される（1 つは内部ゾーン、もう 1 つは外部ゾーンへ追加される）
パッシブ	パッシブ	なし	最初のペアはパッシブ ゾーンへ割り当てられる
ネットワーク ディスカバリ	パッシブ	なし	最初のペアはパッシブ ゾーンへ割り当てられる

セキュリティ ゾーンは防御センターレベルの設定であり、ユーザが実際にデバイスを防御センターに追加するまで作成されないことに注意してください。その時点で、防御センター上に適切なゾーン（内部、外部、またはパッシブ）がすでに存在している場合、システムは一覧で示されたインターフェイスを既存のゾーンに追加します。ゾーンが存在しない場合、システムはゾーンを作成してインターフェイスを追加します。インターフェイス、インライン セット、およびセキュリティ ゾーンの詳細については、『*Sourcefire 3D System User Guide*』を参照してください。

CLI を使用して仮想デバイスを設定するには：

アクセス： Admin

1. VMware コンソールで、ユーザ名として `admin`、および展開のセットアップ ウィザードで指定した新しい admin アカウント パスワードを使用して、仮想デバイスにログインします。

   ウィザードを使用してパスワードを変更していない場合、または ESXi OVF テンプレートを使用して展開している場合は、パスワードとして `Sourcefire` を使用します。

   デバイスでは、EULA を読むようすぐにプロンプトを表示します。

2. EULA を読んで同意します。

3. `admin` アカウントのパスワードを変更します。このアカウントには Configuration CLI アクセス レベルが付与されており、削除することはできません。

   Sourcefire は、大文字と小文字の両方、および少なくとも 1 つの数字を含む 8 文字以上の英数字の強力なパスワードを使用することを推奨しています。辞書に記載されている単語は使用しないでください。

4. デバイスのネットワーク設定を行います。

   最初に IPv4 の管理設定を行い（または無効にして）、次に IPv6 を設定します。手動でネットワークの設定を指定する場合は、次のようにする必要があります。

   - IPv4 のアドレスを、ドット付き 10 進法形式でネットマスクを含めて入力します。たとえば、255.255.0.0 のネットマスクを指定できます。
   - IPv6 のアドレスを、コロンで区切った 16 進数の形式で入力します。IPv6 プレフィックスについては、（プレフィックスの長さ 112 のように）ビットの数を指定します。

   VMware コンソールには、設定が実装されるときにメッセージが表示されることがあります。

5. デバイスをどのように展開したかに基づいて、検出モードを指定します。

   VMware コンソールには、設定が実装されるときにメッセージが表示されることがあります。完了すると、このデバイスを防御センターに登録するように要求され、CLI プロンプトが表示されます。

6. CLI を使用して、デバイスを管理する防御センターにそのデバイスを登録するには、次の項防御センターへの仮想デバイスの登録に進みます。

   防御センターを使用してデバイスを管理する必要があります。今はデバイスを登録しない場合は、デバイスを防御センターに追加する前に、後でログインしてデバイスを登録する必要があります。

防御センターへの仮想デバイスの登録

仮想デバイスには Web インターフェイスがないため、CLI を使用して仮想デバイスを防御センターに登録する必要があります（物理または仮想の両方）。デバイスの CLI にすでにログインしているため、初期設定のプロセスでデバイスを防御センターへ登録するのが最も簡単な方法です。

デバイスを登録するには、`configure manager add` コマンドを使用します。デバイスを防御センターへ登録するには、自己生成の一意の英数字登録キーが必ず必要です。これはユーザが指定する簡単なキーで、ライセンス キーとは異なります。

ほとんどの場合は、登録キーと一緒に防御センターの IP アドレスを指定する必要があります。たとえば次のようにします。

```
configure manager add XXX.XXX.XXX.XXX my_reg_key
```

XXX.XXX.XXX.XXX は、管理している防御センターの IP アドレスで、*my_reg_key* は、仮想デバイスに入力した登録キーです。

重要! vSphere Client を使用して仮想デバイスを防御センターへ登録する場合は、管理元の防御センターの（ホスト名ではなく）IP アドレスを使用する必要があります。

ただし、デバイスと防御センターがネットワーク アドレス変換（NAT）デバイスによって分けられている場合は、登録キーと一緒に一意の NAT ID を入力し、IP アドレスの代わりに `DONTRESOLVE` を指定します。たとえば次のようにします。

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

my_reg_key は仮想デバイスに入力した登録キーで、*my_nat_id* は NAT デバイスの NAT ID です。

防御センターへ仮想デバイスを登録するには：

アクセス： CLI の設定

1. CLI 設定（管理者）の権限を持つユーザとして仮想デバイスにログインします。
   - VMware コンソールから初期設定を実行している場合は、`admin` ユーザとしてすでにログインしています。このユーザは必要なアクセス レベルを持っています。
   - そうでない場合は、VMware コンソールを使用してデバイスにログインします。または、デバイスのネットワーク設定が完了している場合は、デバイスの管理 IP アドレスまたはホスト名に対する SSH を使用してログインします。
2. プロンプトで `configure manager add` コマンドを使用してデバイスを防御センターへ登録します。このコマンドの構文は次のとおりです。

   ```
   configure manager add {hostname | IPv4_address |
   IPv6_address | DONTRESOLVE} reg_key [nat_id]
   ```

   ここで、
   - {*hostname* | *IPv4_address* | *IPv6_address* | `DONTRESOLVE`} は、防御センターの IP アドレスを表します。防御センターを直接アドレス指定できない場合は、`DONTRESOLVE` を使用してください。
   - *reg_key* は、デバイスを防御センターへ登録するのに必要な一意の英数字による登録キーです。
   - *nat_id* はオプションの英数字による文字列で、防御センターとデバイス間の登録プロセスで使用されます。hostname が `DONTRESOLVE` に設定されている場合、これが必要です。
3. アプライアンスからログアウトします。

4. 管理元の防御センターをすでに設定しているかどうか、および防御センターのモデルによって、次の手順が異なります。
   - 防御センターをすでに設定している場合は、Web インターフェイスにログインし、[Device Management] ページ（[Devices] > [Device Management]）を使用してデバイスを追加します。詳細については、『*Sourcefire 3D System User Guide*』の「Managing Devices」の章を参照してください。
   - まだ防御センターを設定していない場合は、「仮想防御センターの設定」（P.80）で、仮想防御センターに関する説明を参照するか、または『*Sourcefire 3D System Installation Guide*』で、物理防御センターに関する説明を参照してください。

仮想防御センターの設定

仮想防御センターの設定に必要な手順は、VI OVF テンプレートまたは ESXi OVF テンプレートのいずれを使用して展開したかによって異なります。

- VI OVF テンプレートを使用して展開し、セットアップ ウィザードを使用した場合は、Sourcefire の必須設定を行ったときに指定したパスワードを使用して、仮想防御センターにログインし、Sourcefire 3D System を使用してローカル アプライアンスの設定、ライセンスとデバイスの追加、トラフィックを監視および管理するためのポリシーの適用を行います。詳細については、『*Sourcefire 3D System User Guide*』を参照してください。
- ESXi OVF テンプレートを使用して展開した場合、または VI OVF テンプレートを使用して展開したときに Sourcefire の必須設定を行っていない場合は、仮想防御センターの設定は 2 段階のプロセスになります。仮想防御センターを初期化した後で、VMware コンソールでスクリプトを実行します。これにより、管理ネットワーク上で通信するアプライアンスを設定できます。次に、管理ネットワーク上のコンピュータを使用して、アプライアンスの Web インターフェイスを参照するための設定プロセスを完了します。

> **ヒント!** ESXi OVF テンプレートを使用して仮想防御センターを展開し、VI OVF テンプレートを使用してすべての仮想デバイスを展開する場合は、1 ページのセットアップ ウィザードを使用して仮想防御センターへすべてのデバイスを同時に登録できます。詳細については、「初期設定ページ：仮想防御センター」（P.82）を参照してください。

詳細については、以下を参照してください。

- 「スクリプトを使用した仮想防御センター ネットワークの設定」（P.81）
- 「初期設定ページ：仮想防御センター」（P.82）

スクリプトを使用した仮想防御センター ネットワークの設定

新しい仮想防御センターを初期化した後で、管理ネットワーク上でアプライアンスが通信できるようにするための設定を行う必要があります。VMware コンソールでスクリプトを実行して、この手順を完了します。

Sourcefire 3D System には、IPv4 と IPv6 の両方の管理環境に対するデュアル スタックの実装が用意されています。最初に、スクリプトでは IPv4 の管理設定を行う（または無効にする）よう要求し、次に IPv6 について設定するよう要求します。IPv6 の展開については、ローカル ルータから設定を取得することができます。ユーザは IPv4 または IPv6 の管理 IP アドレス、ネットマスクまたはプレフィクスの長さ、およびデフォルトのゲートウェイを設定する必要があります。

スクリプトのプロンプトに従う場合に、複数の選択肢がある質問では、選択肢が `(y/n)` のように括弧で囲まれて示されます。デフォルトでは、`[y]` のように角括弧で囲まれています。選択を確定するには、Enter キーを押します。

スクリプトを使用して防御センターのネットワークを設定するには：

アクセス： Admin

1. 初期化プロセスが完了した後で、ユーザ名として `admin`、および VI OVF テンプレートを使用して展開したときにセットアップ ウィザードで指定した admin アカウントのパスワードを使用して、VMware コンソールで仮想防御センターにログインします。

   ウィザードを使用してパスワードを変更していない場合、または ESXi OVF テンプレートを使用して展開している場合は、パスワードとして `Sourcefire` を使用します。

2. admin プロンプトで `sudo su -` と入力してルート ユーザに切り替えて、要求された場合はもう一度パスワードを入力します。

3. root プロンプトで次のスクリプトを実行します。

   ```
   /usr/local/sf/bin/configure-network
   ```

4. スクリプトのプロンプトに従います。

   最初に IPv4 の管理設定を行い（または無効にして）、次に IPv6 を設定します。手動でネットワークの設定を指定する場合は、次のようにする必要があります。

   - IPv4 のアドレスを、ドット付き 10 進法形式でネットマスクを含めて入力します。たとえば、255.255.0.0 のネットマスクを指定できます。
   - IPv6 のアドレスを、コロンで区切った 16 進数の形式で入力します。IPv6 プレフィックスについては、（プレフィックスの長さ 112 のように）ビットの数を指定します。

5. 設定が正しいことを確認します。

   設定を誤って入力した場合は、プロンプトで n と入力して Enter キーを押します。ここで正しい情報を入力できます。VMware コンソールには、設定が実装されるときにメッセージが表示されることがあります。

6. アプライアンスからログアウトします。

7. 防御センターの Web インターフェイスを使用して設定を完了するには、「初期設定ページ：仮想防御センター」（P.82）に進みます。

初期設定ページ：仮想防御センター

仮想防御センターについて、防御センターの Web インターフェイスにログインし、セットアップ ページで初期設定のオプションを指定して、設定プロセスを完了する必要があります。管理者のパスワード変更と、ネットワーク設定の指定をまだ行っていない場合はこれらの 2 つを実行し、EULA に同意する必要があります。

設定プロセスでは、デバイスの登録およびライセンス付与を行うこともできます。デバイスを登録する前に、防御センターをリモート マネージャとして追加するだけでなく、そのデバイス自体の設定プロセスを完了する必要があります。完了していない場合、デバイスの登録が失敗します。

Web インターフェイスを使用して防御センターで初期設定を完了するには：

アクセス： Admin

1. 管理ネットワーク上のコンピュータから、サポートされているブラウザで `https://DC_name/` にアクセスします。ここで *DC_name* は、前の手順で防御センターの管理インターフェイスに割り当てたホスト名または IP アドレスです。

   ログイン ページが表示されます。

2. ユーザ名として `admin`、および VI OVF テンプレートによる展開でセットアップ ウィザードに指定した admin アカウントのパスワードを使用してログインします。ウィザードを使用してパスワードを変更していない場合は、パスワードとして `Sourcefire` を使用します。

   設定ページが表示されます。設定方法の詳細は、以下の項を参照してください。

   - 「パスワードの変更」（P.83）
   - 「ネットワーク設定」（P.84）
   - 「時間の設定」（P.85）
   - 「ルール更新の再帰的なインポート」（P.85）
   - 「地理情報の再帰的な更新」（P.86）
   - 「自動バックアップ」（P.87）
   - 「ライセンスの設定」（P.87）
   - 「デバイス登録」（P.88）
   - 「エンド ユーザ ライセンス契約」（P.91）

3. 完了したら、[Apply] をクリックします。

   選択した内容に従って防御センターが設定されます。中間のページが表示された後で、Administrator ロールを持つ `admin` ユーザとして、Web インターフェイスにログインします。

4. 初期設定が正常に終了したことを確認するには、[Task Status] ページ（[System] > [Monitoring] > [Task Status]）を使用します。

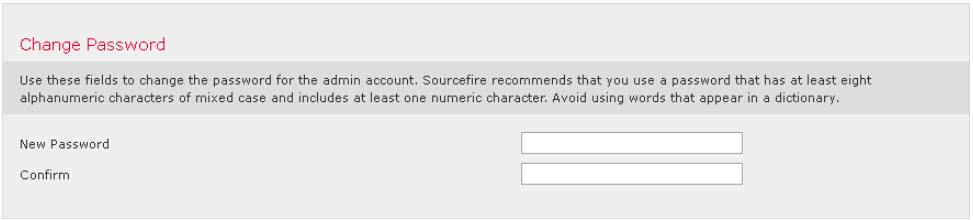
   ページは 10 秒ごとに自動的に更新されます。最初のデバイス登録およびポリシーの適用のタスクについて、[Completed] ステータスが表示されるまでページを監視します。設定の一部として、侵入ルールまたは位置情報の更新を設定した場合は、これらのタスクも監視することができます。

   これで防御センターを使用することができます。展開の設定についての詳細は、『*Sourcefire 3D System User Guide*』を参照してください。

5. 「次の手順」（P.91）に進みます。

パスワードの変更

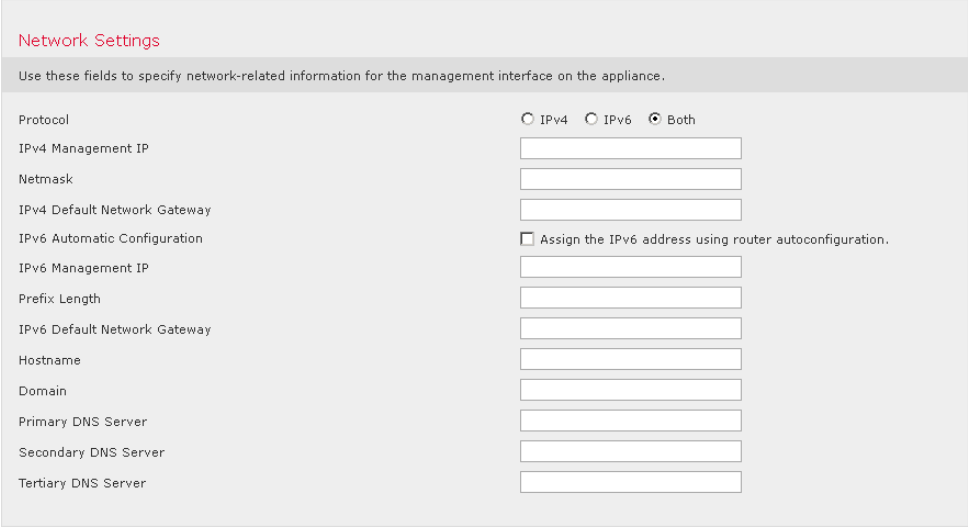
`admin` アカウントのパスワードを変更する必要があります。このアカウントには Administrator 権限が付与されており、削除することはできません。



Sourcefire は、大文字と小文字の両方、および少なくとも 1 つの数字を含む 8 文字以上の英数字の強力なパスワードを使用することを推奨しています。辞書に記載されている単語は使用しないでください。

ネットワーク設定

防御センターのネットワーク設定により、管理ネットワーク上で通信が可能になります。スクリプトを使用してすでにネットワークを設定しているため、ページのこの項には情報が設定されています。



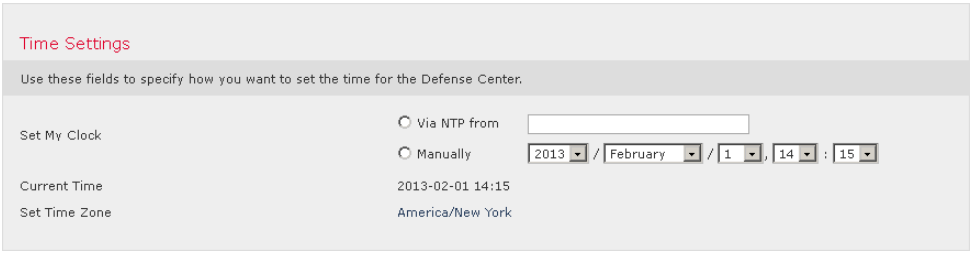
事前に指定されている設定を変更する場合は、Sourcefire 3D System には IPv4 と IPv6 の両方の管理環境についてデュアル スタックの実装が用意されていることに注意してください。管理ネットワーク プロトコル（[IPv4]、[IPv6]、または [Both]）を指定する必要があります。選択した内容に応じて、設定のページにはさまざまなフィールドが表示されます。ここで IPv4 または IPv6 の管理 IP アドレス、ネットマスクまたはプレフィックスの長さ、およびデフォルトのゲートウェイを設定する必要があります。

- IPv4 の場合は、アドレスとネットマスクをドット付き 10 進法の形式（255.255.0.0 のネットマスクなど）で設定する必要があります。
- IPv6 ネットワークの場合は、[Assign the IPv6 address using router autoconfiguration] チェックボックスをオンにして IPv6 のネットワーク設定を自動的に割り当てることができます。このチェックボックスをオンにしない場合は、コロンで区切った 16 進形式のアドレスと、プレフィックスのビット数を設定する必要があります（プレフィックスの長さ 112 など）。

また、デバイスに対してホスト名とドメインの他に、3 つまでの DNS サーバを指定することもできます。

時間の設定

防御センターに対して、手動で、またはネットワーク タイム プロトコル（NTP）を介して NTP サーバから時間を設定することができます。



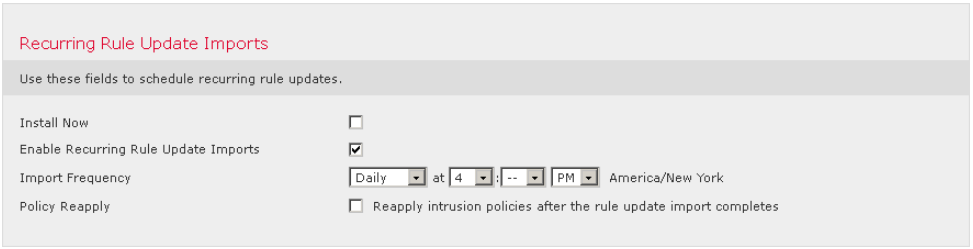
ローカル Web インターフェイスで `admin` アカウントに対して使用されるタイム ゾーンを指定することもできます。ポップアップ ウィンドウを使用してタイム ゾーンを変更するには、現在のタイム ゾーンをクリックします。

Sourcefire では、物理的な NTP サーバを使用して時間を設定することを推奨しています。

ルール更新の再帰的なインポート

新しい脆弱性が発見された場合、Sourcefire Vulnerability Research Team（VRT）は侵入ルールの更新を公開します。ルールの更新では、新しく見つかったおよび更新された侵入ルールおよびプリプロセッサ ルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が提供されます。ルールの更新では、ルールを削除して、新しいルール カテゴリおよびシステム変数を提供する場合もあります。

侵入検知および防御を実行するよう計画している場合、Sourcefire は、[Enable Recurring Rule Update Imports] を選択することを推奨しています。



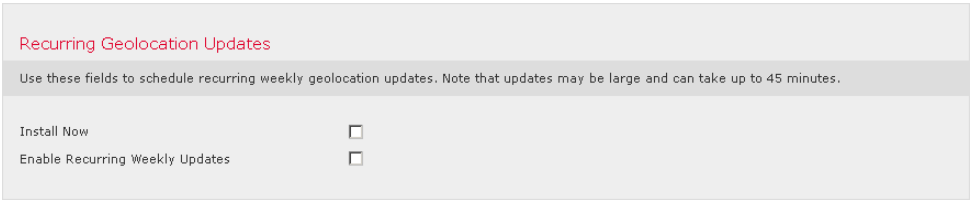
それぞれのルール更新の後で、システムが侵入についての [Policy Reapply] を実行するよう設定するだけでなく、[Import Frequency] も指定することができます。初期設定プロセスの一部としてルールの更新を実行するには、[Install Now] を選択します。

重要! ルールの更新には、新しいバイナリが含まれている場合があります。ルール更新のダウンロードおよびインストールのプロセスが、自身のセキュリティ ポリシーに適合していることを確認します。また、ルールの更新は量が多くなることがあるため、ルールのインポートはネットワークの使用量が少ないときに行うようにしてください。

地理情報の再帰的な更新

仮想防御センターを使用して、ダッシュボードおよび Context Explorer の地理情報統計を監視するだけでなく、システムで生成されたイベントに関連付けられているルーテッド IP アドレスの地理情報を表示することができます。

防御センターの地理情報データベース（GeoDB）には、IP アドレスに関連するインターネット サービス プロバイダ（ISP）、接続タイプ、プロキシ情報、正確な位置情報などの情報が含まれています。定期的な GeoDB の更新を有効にすることで、システムが常に最新の地理情報を使用するようにすることができます。展開で地理情報システムに関連する分析の実行を計画する場合、Sourcefire は [Enable Recurring Weekly Updates] を選択することを推奨しています。



GeoDB について、週次の更新頻度を指定できます。ポップアップ ウィンドウを使用してタイム ゾーンを変更するには、そのタイム ゾーンをクリックします。初期設定プロセスの一部としてデータベースをダウンロードするには、[Install Now] を選択します。

重要! GeoDB の更新は量が多くなることがあるため、ダウンロードの後のインストールに最大で 45 分かかることがあります。GeoDB は、ネットワークの使用量が少ないときに更新してください。

自動バックアップ

防御センターには、障害時に設定を復元できるように、データをアーカイブするためのしくみが用意されています。初期設定の一部として、[Enable Automatic Backups] を選択することができます。

この設定を有効にすると、スケジュールされたタスクが作成され、このタスクによって防御センターの設定のバックアップが週次に作成されます。

ライセンスの設定

組織に対して Sourcefire 3D System の最適な展開を実現するために、さまざまな機能についてライセンスを取得することができます。ホスト、アプリケーション、およびユーザ ディスカバリを行うには、防御センターに FireSIGHT のライセンスが必要です。モデル固有の追加ライセンスを取得すると、管理対象デバイスでさまざまな機能を実行することができます。アーキテクチャとリソースの制限により、すべての管理対象デバイスにすべてのライセンスが適用できるわけではありません。「仮想アプライアンスの機能について」（P.6）および「Sourcefire 仮想アプライアンスのライセンス」（P.9）を参照してください。

Sourcefire では、初期設定のページを使用して、組織で購入したライセンスを追加することを推奨しています。この時点でライセンスを追加しない場合、初期設定で登録するすべてのデバイスは、ライセンス未登録として防御センターに追加されるため、初期設定プロセスが終了した後で、個別にライセンスを付与する必要があります。

ヒント! 仮想防御センターを再作成した場合、および管理インターフェイスについて、削除したアプライアンスと同じ MAC アドレスを使用した場合は、以前のライセンスを使用できます。（動的に割り当てられたものなど）同じ MAC アドレスを使用できなかった場合は、新しいライセンスについて Sourcefire のサポートにお問い合わせください。

まだライセンスを取得していない場合は、リンクをクリックして `https://keyserver.sourcefire.com/` にナビゲートし、画面上の指示に従ってください。サポート契約に関連付けられている連絡先にメールで送信されたアクティベーション キーのほかに、（初期設定のページに示されている）ライセンス キーが必要です。

テキスト ボックスにライセンス キーをコピーし、[Submit License] をクリックしてライセンスを追加します。有効なライセンスを追加するとページが更新され、どのライセンスを追加したかを追跡することができます。ライセンスは一度に 1 つずつ追加します。

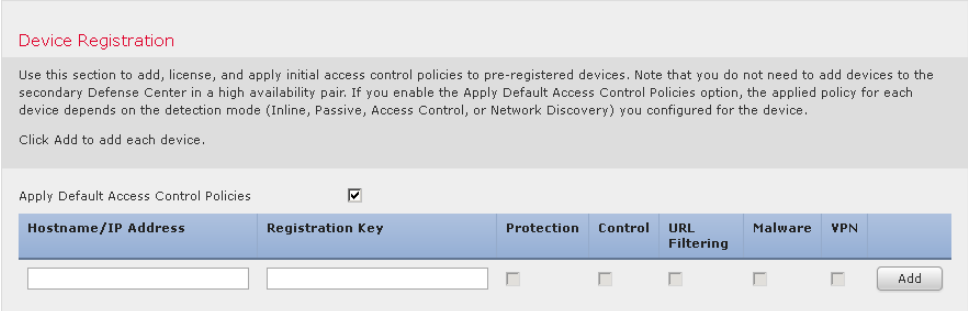
Maximum 3D8250 Licenses				
Protection	Control	URL Filtering	Malware	VPN
5	5	0	0	5
Maximum Virtual Device 64bit Licenses				
Protection	Control	URL Filtering	Malware	VPN
5	5	0	5	0
Maximum Virtual DC 64bit Licenses				
FireSIGHT Host	FireSIGHT User			
50000	50000			

Type	Description	Expires
3D8250	5 Protection License(s)	Never
3D8250	5 Control License(s)	Never
3D8250	5 VPN License(s)	Never
Virtual Device 64bit	5 Malware License(s)	2013-09-16 18:58:01
Virtual Device 64bit	5 Control License(s)	Never
Virtual Device 64bit	5 Protection License(s)	Never
Virtual DC 64bit	50000 FireSIGHT Host, 50000 FireSIGHT User License(s)	Never

デバイス登録

仮想防御センターは、Sourcefire 3D System が現在サポートしているすべての物理的および仮想的なデバイスを管理することができます。初期設定のプロセス中に、事前に登録したほとんどのデバイスを防御センターに追加できます。ただ

し、デバイスと防御センターが NAT デバイスによって分離されている場合は、設定プロセスが完了した後で、デバイスを追加する必要があります。



アクセス制御ポリシーを登録時にデバイスに適用する場合は、デバイスを登録するときに、[Apply Default Access Control Policies] チェックボックスをオンのままにします。防御センターが各デバイスに対してどのポリシーを適用するかは、選択できません。選択できるのはポリシーを適用するかどうかのみであることに注意してください。各デバイスに適用されるポリシーは、デバイスの設定時に選択した検出モードによって異なります。これを次の表に示します。

検出モードごとに適用されるデフォルトのアクセス制御ポリシー

検出モード	デフォルトのアクセス制御ポリシー
インライン	Default Intrusion Prevention
パッシブ	Default Intrusion Prevention
アクセス制御	Default Access Control
ネットワーク ディスカバリ	Default Network Discovery

防御センターを使用して以前にデバイスを管理しており、そのデバイスの最初のインターフェイス設定を変更すると、例外が発生します。このような場合、新しい防御センターのページによって適用されるポリシーは、変更した（現在の）デバイスの設定によって異なります。設定されたインターフェイスがある場合、防御センターは Default Intrusion Prevention ポリシーを適用します。そうでない場合、防御センターは Default Access Control ポリシーを適用します。

仮想デバイスの検出モードに関する詳細は、「CLI を使用した仮想デバイスの設定」（P.75）を参照してください。物理デバイスについては、『*Sourcefire 3D System Installation Guide*』を参照してください。

デバイスを追加するには、デバイスの登録時に指定した**登録キー**のほかに、**ホスト名**または **IP アドレス**を入力します。これは、ユーザが指定した単純なキーで、ライセンス キーとは異なりますので注意してください。

次に、チェックボックスを使用して、ライセンスが付与された機能をデバイスに追加します。すでに防御センターに追加したライセンスしか選択できないので注意してください。また、いくつかのライセンスについては、他の機能を有効にするまで、有効にできません。たとえば、最初に保護を有効にするまで、デバイス上で制御を有効にすることはできません。

アーキテクチャとリソースの制限により、すべての管理対象デバイスにすべてのライセンスが適用できるわけではありません。ただし、管理対象デバイスでサポートされていないライセンスを有効にしないようにする、モデル固有のライセンスを所有していない機能を有効にしないようにする、といったことは設定ページでは制御**できません**。これは、防御センターはこの時点ではデバイス モデルを決定していないためです。システムは無効なライセンスを有効にすることはできません。また、無効なライセンスを有効にしようとしても、ユーザが使用できるライセンス数は減少しません。詳細については、「仮想アプライアンスの機能について」（P.6）および「Sourcefire 仮想アプライアンスのライセンス」（P.9）を参照してください。

重要! [Apply Default Access Control Policies] を有効にした場合は、[Inline] または [Passive] 検出モードを選択したデバイス上で保護ライセンスを有効にする必要があります。また、設定されたインターフェイスを備えている、以前に管理していたデバイス上で保護を有効にする必要があります。有効にしない場合は、デフォルトのポリシー（この場合は保護が必要）の適用が失敗します。

ライセンスを有効にした後で [Add] をクリックしてデバイスの登録設定を保存します。必要に応じてデバイスを追加します。

Hostname/IP Address	Registration Key	Protection	Control	URL Filtering	Malware	VPN	
		☐	☐	☐	☐	☐	Add
bodhi.example.com	buddha	Enabled	Disabled	Disabled	Enabled	Disabled	Delete
yggdrasil.example.com	loki	Enabled	Enabled	Disabled	Disabled	Enabled	Delete

間違ったオプションを選択した場合、またはデバイス名を誤って入力した場合は、[Delete] をクリックして削除します。その後で、デバイスをもう一度追加できます。

エンド ユーザ ライセンス契約

EULA をよく読んで、規定に従う場合はチェックボックスをオンにします。指定した情報がすべて正しいことを確認して、[Apply] をクリックします。

選択した内容に従って防御センターが設定されます。中間のページが表示された後で、Administrator ロールを持つ `admin` ユーザとして、Web インターフェイスにログインします。防御センターの初期設定を完了するには、「初期設定ペー

ジ：仮想防御センター」（P.82）の手順 3 に進みます。

次の手順

仮想アプライアンスの初期設定プロセスが完了し、正常に終了したことが確認できたら、Sourcefire では、展開での管理を容易にするためのさまざまな管理タスクを完了することを推奨しています。また、デバイスの登録やライセンスの取得など、初期設定で省略したタスクも完了する必要があります。展開の設定をどのように始めるかについて、および以降の項に記載されているタスクの詳細については、『*Sourcefire 3D SystemUser Guide*』を参照してください。

個別のユーザ アカウント

初期設定を完了した状態では、システム上のユーザは `admin` ユーザのみです。このユーザは Administrator のロールおよびアクセス権を所有しています。このロールを所有しているユーザは、シェルまたは CLI を介したアクセスを含め、システムのすべてのメニューおよび設定にアクセスできます。セキュリティおよび監査上の理由から、Sourcefire では、`admin` アカウント（および Administrator ロール）の使用を制限することを推奨しています。

システムを使用する各ユーザに対して個別のアカウントを作成すると、各ユーザによって行われたアクションと変更を組織で監査できるほか、各ユーザに関連付けられたユーザ アクセス ロールを制限することができます。これは、ほとんどの設定および分析タスクを実行する防御センターで特に重要です。たとえば、アナリストはネットワークのセキュリティを分析するためにイベント データにアクセスする必要がありますが、展開の管理機能にアクセスする必要はありません。

システムには、さまざまな管理者およびアナリスト用に設計された 10 個の事前定義のユーザ ロールが用意されています。また、特別なアクセス権限を持つカスタム ユーザ ロールを作成することもできます。

ヘルス ポリシーとシステム ポリシー

デフォルトでは、すべてのアプライアンスにシステムの初期ポリシーが適用されます。システム ポリシーは、メール リレー ホストのプリファレンスや時間同期の設定など、展開内の複数のアプライアンスで共通している可能性が高い設定を管理します。Sourcefire では、防御センターを使用して、防御センター自身およびその管理対象デバイスすべてに同じシステム ポリシーを適用することを推奨しています。

デフォルトで、防御センターにはヘルス ポリシーも適用されます。ヘルス ポリシーは、ヘルス モニタリング機能の一部として、システムが展開環境内でアプライアンスのパフォーマンスを継続して監視するための基準を提供します。Sourcefire では、防御センターを使用して、その管理対象デバイスすべてにヘルス ポリシーを適用することを推奨しています。

ソフトウェアおよびデータベースの更新

展開を開始する前に、アプライアンス上でシステム ソフトウェアを更新する必要があります。Sourcefire では、展開環境内のすべてのアプライアンスが Sourcefire 3D System の最新のバージョンを実行することを推奨しています。展開環境でこれらのアプライアンスを使用する場合は、最新の侵入ルール更新、VDB、および GeoDB もインストールする必要があります。

警告! Sourcefire 3D System のいずれかの部分を更新する前に、更新に付属のリリース ノートまたはアドバイザリ テキストを読んでおく必要があります。リリース ノートには、サポートされるプラットフォーム、互換性、前提条件、警告、および特定のインストールとアンインストールの手順などの重要な情報が記載されています。