



仮想アプライアンスの設定

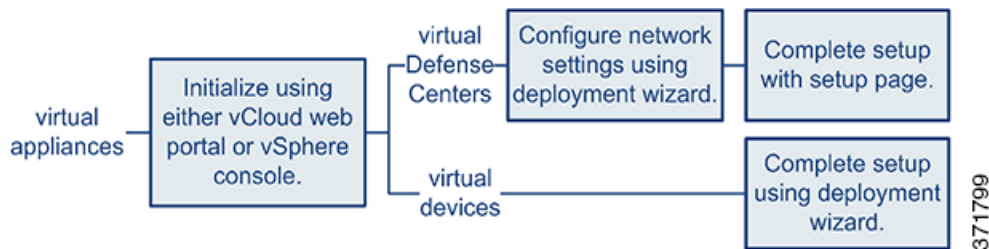
仮想アプライアンスをインストールしたら、設定プロセスを完了する必要があります。このプロセスにより、信頼された管理ネットワーク上で新しいアプライアンスが通信できるようになります。また、管理者パスワードを変更し、エンドユーザ ライセンス契約書(EULA)に同意する必要があります。

設定プロセスを使用すると、時間の設定、デバイスの登録とライセンス認証、更新のスケジュールリングなどのさまざまな管理レベル タスクを実行することもできます。設定と登録中に選択されたオプションによって、システムで作成され、適用されるデフォルト 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。

これらの初期設定とポリシーの目的は、オプションを制限することではなく、アウトオブザボックス エクスペリエンスを提供し、短時間で展開を設定できるようにすることです。デバイスをどのように初期設定したかに関係なく、その設定はいつでも防御センターを使用して変更できます。つまり、たとえば、設定中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、特定のデバイス、ゾーン、またはポリシー設定に固定されません。

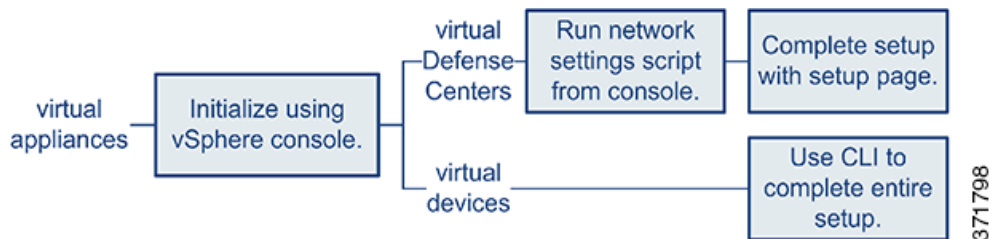
VI OVF テンプレートの展開

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している場合は、先にデバイスを設定してから、管理元の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を使用すれば、デバイスを防御センターに事前登録できます。防御センターの設定プロセスを使用すれば、事前登録した管理対象デバイスを追加してライセンス認証できます。

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.5-2)
- 「CLI を使用した仮想デバイスの設定」(P.5-3)
- 「仮想防御センターの設定」(P.5-7)
- 「VMware ツールの有効化」(P.5-13)
- 「次の手順」(P.5-14)

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。



注意

起動時間は、サーバリソースの可用性など、さまざまな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:

ステップ 1 以下のようにして、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 クライアントで、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。

ステップ 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、FireSIGHT システム 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.5-7)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 テンプレートを使用している場合、または VI OVF テンプレートで展開したときに FireSIGHT システム 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.5-7)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.5-3)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 テンプレートを使用して展開し、かつ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、CLI を使用して FireSIGHT システムで必要な設定を行うことができます。



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。デフォルト値は、[y] のように大カッコ内に列挙されます。Enter キーを押して、選択を確定します。

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、『*FireSIGHT 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、『*FireSIGHT System User Guide*』の「コマンドライン リファレンス」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

FireSIGHT システムは、IPv4 と IPv6 の両方の管理環境にデュアル スタック実装を提供します。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。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

デバイスがパッシブ展開されている場合は、このモードを侵入検知システム (IDS) として選択します。パッシブ展開では、仮想デバイスは、ネットワーク ベース ファイルとマルウェアの検出、セキュリティ インテリジェンス モニタリング、およびネットワーク 検出を実行できます。

インライン

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



(注)

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

デバイスがパッシブ展開されている場合は、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実行するためにこのモードを選択します。

次の表に、選択された検出モードに基づいて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ます。

表 5-1 検出モードに基づく初期設定

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 インライン セット	デフォルト インライン セットに追加された最初のペア: 内部ゾーン向けの 1 つと外部ゾーン向けの 1 つ
パッシブ	パッシブ	なし	パッシブ ゾーンに割り当てられた最初のペア
ネットワーク ディスカバリ	パッシブ	なし	パッシブ ゾーンに割り当てられた最初のペア

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は、システムがそれ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、『*FireSIGHT 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

-
- ステップ 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 사용하여展開している場合は、パスワードとして `Cisco` を使用します。
- 直後に、デバイスから EULA を読むように要求されます。
- ステップ 2** EULA を読んで同意します。
- ステップ 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。
- シスコ では、大文字と小文字が混在する 8 文字以上の英数字で、1 つ以上の数字を含む強力なパスワードを使用することを推奨しています。辞書に掲載されている単語の使用は避けてください。
- ステップ 4** デバイスのネットワーク設定を構成します。
- 最初に IPv4 管理設定を構成(または無効に)してから、IPv6 に移ります。ネットワーク設定を手動で指定する場合は、次の手順を実行する必要があります。
- ネットマスクを含む IPv4 アドレスをドット付き 10 進形式で入力します。たとえば、`255.255.0.0` のネットマスクを指定できます。
 - IPv6 アドレスをコロン区切りの 16 進形式で入力します。IPv6 プレフィックスの場合、ビット数を指定します(たとえば、`112` のプレフィックス長)。
- 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。
- ステップ 5** デバイスの展開方法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。完了したら、このデバイスを防御センターに登録するよう要求され、CLI プロンプトが表示されます。
- ステップ 6** CLI を使用して、デバイスを管理元の防御センターに登録するには、次の項(「[防御センターへの仮想デバイスの登録](#)」(P.5-5))に進みます。
- デバイスは防御センターを使用して管理する必要があります。今すぐデバイスを登録しない場合は、後でデバイスにログインしてそれを登録するまで防御センターに追加できません。
-

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)。初期設定プロセス中にデバイスを防御センターに登録する方が簡単です。これは、すでにデバイスの CLI にログインしているためです。

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。



(注) vSphere クライアント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。

仮想デバイスを防御センターに登録するには:

アクセス: CLI Configuration

ステップ 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。

ステップ 2 プロンプトで、次のような構文の configure manager add コマンドを使用してデバイスを防御センターに登録します。

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

値は次のとおりです。

- {hostname | IPv4_address | IPv6_address | DONTRESOLVE} は、防御センターの IP アドレスを表します。防御センターが直接アドレス指定できない場合は、DONTRESOLVE を使用します。
- 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、防御センターとデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。ホスト名が DONTRESOLVE に設定されている場合に必須です。

ステップ 3 アプライアンスからログアウトします。

ステップ 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、『FireSIGHT System User Guide』の「デバイスの管理」の章を参照してください。
- 防御センターをまだ設定していない場合、仮想防御センターについては、「[仮想防御センターの設定](#)」(P.5-7)を参照してください。物理防御センターについては、『FireSIGHT System Installation Guide』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か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、FireSIGHT システム 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、FireSIGHT システム 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、『*FireSIGHT 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 FireSIGHT システム 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。
- 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.5-8)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。

- 「[仮想防御センター ネットワーク設定の自動化](#)」(P.5-7)
- 「[初期設定ページ: 仮想防御センター](#)」(P.5-8)

仮想防御センター ネットワーク設定の自動化

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。

FireSIGHT システム は、IPv4 と IPv6 の両方の管理環境にデュアル スタック実装を提供します。最初に、スクリプトから IPv4 管理設定を構成(または無効に)するように要求されてから、IPv6 に移ります。IPv6 展開では、ローカル ルータから設定値を取得できます。IPv4 または IPv6 管理 IP アドレス、ネットマスクまたはプレフィックス長、およびデフォルト ゲートウェイを指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。デフォルト値は、[y] のように大カッコ内に列挙されます。Enter キーを押して、選択を確定します。

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

- ステップ 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 Cisco を使用します。

ステップ 2 admin プロンプトで、次のスクリプトを実行します。

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

ステップ 3 スクリプトのプロンプトに従ってください。

最初に IPv4 管理設定を構成(または無効に)してから、IPv6 に移ります。ネットワーク設定を手動で指定する場合は、次の手順を実行する必要があります。

- ネットマスクを含む IPv4 アドレスをドット付き 10 進形式で入力します。たとえば、255.255.0.0 のネットマスクを指定できます。
- IPv6 アドレスをコロン区切りの 16 進形式で入力します。IPv6 プレフィックスの場合、ビット数を指定します(たとえば、112 のプレフィックス長)。

ステップ 4 設定値が正しいことを確認します。

設定値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。その後、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。

ステップ 5 アプライアンスからログアウトします。

ステップ 6 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.5-8)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。管理者パスワードを変更して、まだの場合はネットワーク設定を指定し、EULA に同意します。

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上で初期設定を完了するには:

アクセス: Admin

ステップ 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。

ステップ 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 `Cisco` を使用します。

設定ページが表示されます。設定の完了方法については、次の項を参照してください。

- 「[パスワードの変更](#)」(P.5-9)
- 「[ネットワーク設定](#)」(P.5-9)
- 「[時間設定](#)」(P.5-10)
- 「[ルール更新の定期インポート](#)」(P.5-10)
- 「[地理情報の定期的な更新](#)」(P.5-10)

- 「自動バックアップ」(P.5-11)
- 「ライセンス設定」(P.5-11)
- 「デバイス登録」(P.5-11)
- 「VMware ツールの有効化」(P.5-13)
- 「End User License Agreement」(P.5-13)

ステップ 3 完了したら、[Apply] をクリックします。

防御センターが選択内容に従って設定されます。中間ページが表示されたら、管理者ロールを持つ admin ユーザとして Web インターフェイスにログインします。

ステップ 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。

防御センターを使用する準備が整いました。展開の設定の詳細については、『FireSIGHT System User Guide』を参照してください。

ステップ 5 「次の手順」(P.5-14)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。このアカウントは管理者特権が付与されているため、削除できません。シスコでは、大文字と小文字が混在する 8 文字以上の英数字で、1 つ以上の数字を含む強力なパスワードを使用することを推奨しています。辞書に掲載されている単語の使用は避けてください。

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って、それが管理ネットワーク上で通信できるようになります。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。

事前入力された設定を変更する場合は、FireSIGHT システムによって IPv4 と IPv6 の両方の管理環境にデュアルスタック実装が提供され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、ドット付き 10 進表記でアドレスおよびネットマスクを設定する必要があります(例:255.255.0.0 のネットマスク)。
- 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選択しない場合は、コロンで区切られた 16 進表記のアドレスおよびプレフィックス内のビット数(たとえば、112 のプレフィックス長)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。

時間設定

防御センターの時刻は、手動で設定することも、ネットワーク タイム プロトコル(NTP)サーバから NTP 経由で設定することもできます。

また、admin アカウント用のローカル Web インターフェイスで使用されるタイムゾーンを指定することもできます。現在のタイムゾーンをクリックして、ポップアップ ウィンドウを使用してそれを変更します。

シスコ 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。

ルール更新の定期インポート

新しい脆弱性が発見された場合、Cisco の脆弱性調査チーム(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、シスコ 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。



(注)

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。

地理情報の定期的な更新

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なります。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、シスコ 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。



(注)

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、**自動バックアップを有効に**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。

ライセンス設定

組織に対して FireSIGHT システム 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.1-3) および「**仮想アプライアンスのライセンス**」(P.1-12)を参照してください。

シスコでは、初期設定ページを使用して、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。同じ MAC アドレスを使用できない(たとえば、動的に割り当てられた)場合、新しいライセンスについて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。

デバイス登録

仮想防御センターは、FireSIGHT システム 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。

防御センターに管理対象デバイスを登録する際、登録時にアクセス制御ポリシーを自動的にデバイスに適用する場合は、[Apply Default Access Control Policies] チェックボックスをオンのままにしておきます。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。

表 5-2 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 コントロール	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の詳細については、「[CLI を使用した仮想デバイスの設定](#)」(P.5-3)を参照してください。物理デバイスについては、『*FireSIGHT System Installation Guide*』を参照してください。



(注)

デバイスがアクセス制御ポリシーに適合していない場合は、ポリシーの適用に失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。最初のアクセス制御ポリシーが失敗すると、最初のネットワーク ディスカバリ ポリシーの適用も失敗します。障害の原因となる問題を解決した後は、アクセス制御ポリシーおよびネットワーク ディスカバリ ポリシーを手動でデバイスに適用する必要があります。アクセス制御ポリシー適用失敗の原因となる可能性のある問題についての詳細は、『*FireSIGHT System User 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 Control 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ですべてのライセンスがサポートされるわけではありません。ただし、セットアップ ページでは、管理対象デバイスでサポートされていないライセンスの有効化は可能な状態です。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.1-3)および「[仮想アプライアンスのライセンス](#)」(P.1-12)を参照してください。

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。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。

End User License Agreement

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。

防御センターが選択内容に従って設定されます。中間ページが表示されたら、管理者ロールを持つ 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.5-8)の手順 3 に進みます。

VMware ツールの有効化

VMware Tools は仮想マシンのオペレーティング システム上にインストールされるユーティリティのスイートで、仮想マシンのパフォーマンスを強化し、VMware 製品で使い勝手のよい多数の機能を実現します。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

VMware ツールのサポートされるプラグインおよびすべての機能の詳細については、VMware Web サイト (<http://www.vmware.com/>) を参照してください。

仮想アプライアンスをセットアップした後、管理対象デバイスでコマンドライン インターフェイス (CLI) を使用するか、または仮想防御センターでブラウザを使用して、仮想アプライアンスの VMware ツールを有効にできます。詳細については、次の項を参照してください。

- 「[仮想デバイスでの VMware ツールの設定](#)」(P.5-13)
- 「[仮想防御センターでの VMware ツールの設定](#)」(P.5-14)

仮想デバイスでの VMware ツールの設定

仮想デバイスにログインし、次のコマンドの 1 つ以上を入力できます。

- `show vmware-tools` は、VMware ツールがシステム上で実行されているかどうかを表示します。
- `configure vmware-tools enable` は、仮想デバイスで VMware ツールを有効にします。
- `configure vmware-tools disable` は、仮想デバイスで VMware ツールを無効にします。

仮想デバイスで VMware ツールを有効にするには:

アクセス: Admin

- ステップ 1** コンソールで仮想デバイスにログインし、CLI プロンプトで、VMware ツールを有効または無効にするコマンド、あるいは、VMware ツールが有効であるかどうかを表示するコマンドを入力して、**Enter** を押します。

VMware ツールが実行中、有効、無効のいずれであるかを示すメッセージが、コンソールに表示されます。

仮想防御センターでの VMware ツールの設定

Web インターフェイスを使用して [Configuration] メニューのチェックボックスをオンまたはオフにできます。CLI を使用して仮想防御センターで VMware ツールを有効にすることはできません。

仮想防御センターで VMware ツールを有効または無効にするには:

アクセス:Admin

- ステップ 1** Web ブラウザを使用して、防御センターにログインし、[System] > [Local] > [Configuration] > [VMware Tools] を選択します。それから、[VMware Tools] チェック ボックスをオンまたはオフにし、[Save] をクリックします。

変更が正常に実行されたことを示すメッセージが表示されます。

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、シスコでは、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。以下のセクションで説明するタスクの詳細、および展開の設定を開始する方法の詳細については、『*FireSIGHT System User Guide*』を参照してください。

個別のユーザアカウント

初期セットアップが完了した時点で、システム上の唯一のユーザは、管理者ロールとアクセス権を持つ admin ユーザです。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、シスコでは、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。シスコでは、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。シスコでは、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。

ソフトウェアと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。シスコでは、展開環境内のすべてのアプライアンスが FireSIGHT システム 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。



注意

FireSIGHT システム 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ー 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。

■ 次の手順