システム設定

ここでは、[システム設定（System Settings）] ページでグループ化されているさまざまなシステム設定の設定方法について説明します。設定は、システムの機能全体を網羅しています。

- 管理アクセスの設定 （1 ページ）
- システム ロギングの設定 （4 ページ）
- DHCP サーバの設定 （10 ページ）
- DNS の設定 （12 ページ）
- 管理インターフェイスの設定 （17 ページ）
- デバイスのホスト名の設定 （19 ページ）
- Network Time Protocol（NTP）の設定 （20 ページ）
- URL フィルタリングの設定 （20 ページ）
- クラウド サービスの設定 （21 ページ）

管理アクセスの設定

管理アクセスとは、設定およびモニタ目的で FTD デバイスにログインする機能のことです。次の項目を設定できます。

- ユーザ アクセス認証に使用するアイデンティティ ソースを特定するための AAA。ローカル ユーザ データベースまたは外部 AAA サーバを使用することができます。管理ユーザの管理の詳細については、FDM および FTD ユーザ アクセスの管理を参照してください。
- 管理インターフェイスおよびデータ インターフェイスへのアクセス制御。これらのインターフェイスには個別のアクセス リストがあります。どの IP アドレスが HTTPS（Firepower Device Manager で使用）および SSH（CLI で使用）で許可されるかを決定できます。管理アクセス リストの設定 （2 ページ）を参照してください。
- Firepower Device Manager に接続するためにユーザが受け入れる必要がある管理 Web サーバ証明書。Web ブラウザで信頼される証明書をアップロードすることにより、ユーザが不明な証明書を信頼するように求められるのを回避できます。Firepower Device Manager Web サーバ証明書の設定 （4 ページ）を参照してください。

管理アクセス リストの設定

デフォルトでは、任意の IP アドレスから、デバイスの Firepower Device Manager ウェブまたは管理アドレスの CLI インターフェイスにアクセスできます。システム アクセスは、ユーザ名/パスワードのみで保護されています。ただし、特定の IP アドレスまたはサブネットのみからの接続を許可するようアクセス リストを設定し、さらにレベルの高い保護を提供できます。

また、データインターフェイスを開いて、Firepower Device Manager または SSH による CLI 接続を許可することもできます。これにより、管理アドレスを使用せずにデバイスを管理できます。たとえば、外部インターフェイスへの管理アクセスを許可し、デバイスをリモートで設定できます。ユーザ名/パスワードにより、不要な接続から保護します。デフォルトでは、データインターフェイスへの HTTPS 管理アクセスは内部インターフェイスで有効になっていますが、外部インターフェイスでは無効になっています。デフォルトの「内部」ブリッジグループを持つデバイス モデルの場合、ブリッジグループ内の任意のデータインターフェイスを介して、ブリッジグループ IP アドレス（デフォルトは 192.168.1.1）への Firepower Device Manager 接続が可能になります。管理接続は、デバイスに入るインターフェイス上でのみ開くことができます。

⚠

注意 特定のアドレスへのアクセスを制限すると、システムから簡単にロックアウトできます。現在使用している IP アドレスへのアクセスを削除し、「任意」のアドレスへのエントリが存在しない場合、ポリシーを展開した時点でシステムへのアクセスは失われます。アクセス リストを設定する場合は、特に注意してください。

始める前に

同じ TCP ポートの同じインターフェイスで Firepower Device Manager アクセス（HTTPS アクセス）、AnyConnect リモート アクセス SSL VPN の両方を構成することはできません。たとえば、外部インターフェイスにリモートアクセス SSL VPN を設定する場合、ポート 443 で HTTPS 接続用の外部インターフェイスも開くことはできません。Firepower Device Manager ではこれらの機能に使用されるポートを設定できないため、同じインターフェイスで両方の機能は設定できません。

手順

ステップ 1 [デバイス（Device）] をクリックします。 をクリックしてから、**[システム設定（System Settings）] > [管理アクセス（Management Access）]** の順にリンクをクリックします。

[システム設定（System Settings）] ページがすでに表示されている場合は、目次で [管理アクセス リスト（Management Access List）][管理アクセス（Management Access）] をクリックします。

このページで AAA を設定して、外部 AAA サーバで定義されたユーザの管理アクセスを許可することもできます。詳細は、FDM および FTD ユーザ アクセスの管理を参照してください。

ステップ 2 管理アドレスのルールを作成するには、以下の手順に従います。

a) [管理インターフェイス（Management Interface）] タブを選択します。

ルールのリストは、指定したポートへのアクセスが許可されるアドレスを定義します。Firepower Device Manager（HTTPS Web インターフェイス）の場合は 443、SSH CLI の場合は 22 です。

ルールは番号付きリストではありません。IP アドレスが要求されたポートの任意のルールと一致する場合、そのユーザはデバイスへのログイン試行が許可されます。

（注） ルールを削除するには、ルールの [ごみ箱（trash can）] アイコン（）をクリックします。すべてのプロトコルのルールを削除した場合は、誰もプロトコルを使用してそのインターフェイスのデバイスにアクセスすることはできません。

b) [+] をクリックし、次のオプションを入力します。

- [プロトコル（Protocol）]：ルールが HTTPS（ポート 443）または SSH（ポート 22）用かを選択します。
- [IPアドレス（IP Address）]：システムにアクセスできる IPv4 ネットワーク、IPv6 ネットワーク、またはホストを定義するネットワーク オブジェクトを選択します。「任意」のアドレスを指定するには、[any-ipv4] (0.0.0.0/0) および [any-ipv6] (::/0) を選択します。

c) [OK] をクリックします。

ステップ 3 データインターフェイスへのルールを作成するには、以下の手順に従います。

a) [データインターフェイス（Data Interfaces）] タブを選択します。

ルールのリストには、インターフェイス上の指定されたポート（Firepower Device Manager（HTTPS Web インターフェイス）の場合は 443、SSH CLI の場合は 22）へのアクセスが許可されるアドレスが定義されています。

ルールは番号付きリストではありません。IP アドレスが要求されたポートの任意のルールと一致する場合、そのユーザはデバイスへのログイン試行が許可されます。

（注） ルールを削除するには、ルールの [ごみ箱（trash can）] アイコン（）をクリックします。すべてのプロトコルのルールを削除した場合は、誰もプロトコルを使用してそのインターフェイスのデバイスにアクセスすることはできません。

b) [+] をクリックし、次のオプションを入力します。

- [インターフェイス（Interface）]：管理アクセスを許可するインターフェイスを選択します。
- [プロトコル（Protocols）]：ルールが HTTPS（ポート 443）または SSH（ポート 22）、またはその両方用かを選択します。外部インターフェイスがリモート アクセス VPN 接続プロファイルで使用されている場合、その外部インターフェイスに HTTPS ルールを設定することはできません。
- [許可されたネットワーク（Allowed Networks）]：システムにアクセスできる IPv4 ネットワーク、IPv6 ネットワーク、またはホストを定義するネットワーク オブジェクトを

選択します。「任意」のアドレスを指定するには、[any-ipv4] (0.0.0.0/0) および [any-ipv6] (::/0) を選択します。

c) [OK] をクリックします。

Firepower Device Manager Web サーバ証明書の設定

Web インターフェイスにログインするときに、システムはデジタル証明書を使用して HTTPS で通信を保護します。デフォルトの証明書はブラウザで信頼されていないため、Untrusted Authority という警告が表示され、証明書を信頼するかどうかを確認されます。ユーザは証明書を Trusted Root Certificate ストアに保存することもできますが、その代わりに信頼するようにブラウザがすでに設定されている新しい証明書をアップロードすることもできます。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）] > [管理アクセス（Management Access）]** リンクの順にクリックします。

[システム設定（System Settings）] ページがすでに表示されている場合は、目次で [管理アクセス（Management Access）] をクリックします。

ステップ 2 [管理Webサーバ（Management Web Server）] タブをクリックします。

ステップ 3 [Webサーバ証明書（Web Server Certificate）] で、Firepower Device Manager への HTTPS 接続をセキュリティ保護するために使用する内部証明書を選択します。

証明書をアップロードまたは作成していない場合、リストの下部にある [内部証明書の新規作成（Create New Internal Certificate）] リンクをクリックして作成します。

デフォルトは、事前に定義された DefaultWebserverCertificate オブジェクトです。

ステップ 4 [保存（Save）] をクリックします。

変更はすぐに適用され、システムが Web サーバを再起動します。設定を展開する必要はありません。

数分待って再起動が完了してから、ブラウザを更新します。

システム ロギングの設定

FTD デバイスのシステム ロギング（syslog）を有効にすることができます。情報をロギングすることで、ネットワークの問題またはデバイス設定の問題を特定して分離できます。syslog は、アクセス制御、侵入防御、およびファイルとマルウェアのロギングを含む診断ロギングおよび接続関連ロギングのために有効にすることができます。

診断ロギングは、デバイスおよびシステムの状態に関するイベントと、接続とは関係のないネットワーク設定に関するsyslogメッセージを提供します。個々のアクセスコントロールルール内に接続ロギングを設定します。

診断ロギングでは、データプレーン上で実行されている機能、つまり **show running-config** コマンドで表示できるCLI設定で定義されている機能に関するメッセージが生成されます。これには、ルーティング、VPN、データインターフェイス、DHCPサーバ、NATなどの機能が含まれます。

これらのメッセージの詳細については、『*Cisco Firepower Threat Defense Syslog Messages*』（https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html）を参照してください。

次のトピックでは、さまざまな出力場所に対するの診断メッセージやファイル/マルウェアメッセージのロギングを設定する方法について説明します。

重大度

次の表に、syslogメッセージの重大度の一覧を示します。

表 *1 : Syslog* メッセージの重大度

レベル番号	重大度	説明
0	**緊急**	システムが使用不可能な状態です。
1	**アラート**	すぐに措置する必要があります。
2	**重大**	深刻な状況です。
3	**エラー**	エラー状態です。
4	**警告**	警告状態です。
5	**通知**	正常ですが、注意を必要とする状況です。
6	**情報**	情報メッセージです。
7	**デバッグ**	デバッグ メッセージです。

（注） Firepower Threat Defenseは、重大度0（緊急）のsyslogメッセージを生成しません。

リモート syslog サーバのロギングの設定

システムを設定して、syslogのメッセージを外部syslogサーバに送信できます。これはシステムロギングの最適なオプションです。外部サーバを使用することでメッセージを保持する容量が増え、メッセージの表示、分析、およびアーカイブにサーバの施設を使用できます。

さらに、アクセス制御ルールでトラフィックにファイルポリシーを適用してファイルへのアクセスまたはマルウェア、あるいはその両方を制御する場合、外部 syslog サーバにファイル イベント メッセージを送信するようにシステムを設定できます。syslog サーバを設定しない場合、イベントは FDM イベント ビューアのみで使用できます。

次の手順では、診断（データ）ロギングおよびファイル/マルウェアのロギングのために syslog を有効にする方法について説明します。以下のために外部ロギングを設定することもできます。

- 接続イベント：個々のアクセス制御ルール、SSL 復号化ルール、またはセキュリティ インテリジェンス ポリシー設定で syslog サーバを選択します。
- 侵入イベント：侵入ポリシー設定で syslog サーバを選択します。

始める前に

ファイル/マルウェア イベントの syslog 設定は、脅威とマルウェアのライセンスを必要とするファイルまたはマルウェアのポリシーを適用する場合にのみ該当します。

さらに、ポリシーを適用するアクセス制御ルールで、**[ファイルイベント（File Events）]**>**[ファイルのロギング（Log Files）]** オプションが選択されていることを確認する必要があります。そうでない場合、syslog でもイベント ビューアでもイベントはまったく生成されません。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）]**>**[ログ設定（Logging Settings）]** リンクをクリックします。

[システム設定（System Settings）] ページをすでに開いている場合、目次の [ロギングの設定（Logging Settings）] をクリックします。

ステップ 2 [リモートサーバ（Remote Server）] の下の [データロギング（Data Logging）] スライダを [ON] にし、データプレーンで生成された診断メッセージの外部syslogサーバへのロギングを有効にするます。次に、以下のオプションを設定します。

- [Syslogサーバ（Syslog Server）]：[+] をクリックし、1 つまたは複数の syslog サーバ オブジェクトを選択して、[OK] をクリックします。オブジェクトが存在しない場合は、[Syslog サーバの追加（Add Syslog Server）] リンクをクリックして作成します。詳細については、Syslog サーバの設定を参照してください。
- [FXOSシャーシsyslogのフィルタリングの重大度レベル（Severity Level for Filtering FXOS Chassis Syslogs）]：FXOS を使用する特定のデバイス モデルの、基本の FXOS プラットフォームによって生成される syslog メッセージの重大度レベル。このオプションは、デバイスに該当する場合にのみ表示されます。重大度を選択します。このレベル以上のメッセージは、syslog サーバに送信されます。
- [Firepower Threat Defenseのメッセージフィルタリング（Message Filtering for Firepower Threat Defense）]：Firepower Threat Defense のオペレーティング システム用に生成されたメッセージを制御するには、次のオプションのいずれかを選択します。

- [すべてのイベントのフィルタリングの重大度レベル（Severity Level for Filtering All Events）]：重大度レベルを選択します。このレベル以上のメッセージは、syslog サーバに送信されます。
- [カスタムロギングフィルタ（Custom Logging Filter）]：関心のあるメッセージのみを取得するために追加のメッセージフィルタリングを行う場合、生成させたいメッセージを定義するイベント ログ フィルタを選択します。フィルタが存在しない場合は、[新しいイベントリストフィルタの作成（Create New Event List Filter）] をクリックして作成します。詳細については、イベント ログ フィルタの設定 （9 ページ）を参照してください。

ステップ 3 ファイルおよびマルウェアのイベントの外部 syslog サーバへのロギングを有効にするには、[ファイル/マルウェア（File/Malware）] スライダを [ON] にします。次に、ファイル/マルウェア ロギングのオプションを設定します。

- [Syslogサーバ（Syslog Server）]：syslog サーバ オブジェクトを選択します。オブジェクトが存在しない場合は、 [Syslogサーバの追加（Add Syslog Server）] リンクをクリックして作成します。
- [重大度レベルのログ（Log at Severity Level）]：ファイル/マルウェア イベントに割り当てる重大度レベルを選択します。すべてのファイル/マルウェア イベントが同じ重大度で生成されるため、フィルタリングは実行されません。選択したレベルに関係なく、すべてのイベントが表示されます。これがメッセージの重大度フィールドに表示されるレベルになります（つまり、FTD-x-<message_ID> の x）。ファイル イベントはメッセージ ID 430004 であり、マルウェア イベントは 430005 です。

ステップ 4 [保存（Save）] をクリックします。

内部バッファへのロギングの設定

システムを設定して、内部ロギング バッファへの syslog メッセージを保存できます。バッファの内容を表示するには、CLI または CLI コンソールで **show logging** コマンドを使用します。

新しいメッセージは、バッファの最後に追加されます。バッファがいっぱいになると、システムはバッファをクリアしてから、メッセージの追加を続行します。ログ バッファがいっぱいになると、システムが最も古いメッセージを削除して、バッファに新しいメッセージ用の領域を確保します。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）] > [ログ設定（Logging Settings）]** リンクをクリックします。

[システム設定（System Settings）] ページをすでに開いている場合、目次の [ロギングの設定（Logging Settings）] をクリックします。

ステップ 2 ロギングの宛先としてバッファを有効にするには、[内部バッファ（Internal Buffer）] スライダを [ON] にします。

ステップ 3 内部バッファ ロギングのオプションの設定。

- [すべてのイベントのフィルタリングの重大度レベル（Severity Level for Filtering All Events）]：重大度レベルを選択します。このレベル以上のメッセージは、内部バッファに送信されます。
- [カスタムロギングフィルタ（Custom Logging Filter）]：（オプション）関心のあるメッセージのみを取得するために追加のメッセージフィルタリングを行う場合、生成するメッセージを定義するイベント ログ フィルタを選択します。フィルタが存在しない場合は、[新しいイベントリストフィルタの作成（Create New Event List Filter）] をクリックして作成します。詳細については、イベント ログ フィルタの設定 （9 ページ）を参照してください。
- [バッファサイズ（Buffer Size）]：syslog メッセージを保存する内部ログ バッファのサイズを指定します。バッファが一杯になった場合は上書きされます。デフォルトは 4096 バイトです。指定できる範囲は 4096 ～ 52428800 です。

ステップ 4 [保存（Save）] をクリックします。

コンソールへのロギングの設定

コンソールにメッセージを送信するようにシステムを設定することができます。コンソール ポートの CLI にログインした時にこれらのメッセージが表示されます。さらに、**show console-output** コマンドを使用することで、他のインターフェイス（管理アドレスを含む）に対する SSH セッションでもこれらのログが表示されます。さらに、メイン CLI から **system support diagnostic-cli** と入力すると診断 CLI でリアルタイムでこれらのメッセージを表示できます。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）] > [ログ設定（Logging Settings）]** リンクをクリックします。

[システム設定（System Settings）] ページをすでに開いている場合、目次の [ロギングの設定（Logging Settings）] をクリックします。

ステップ 2 ロギングの宛先としてコンソールを有効にするには、[コンソールフィルタ（Console Filter）] スライダを [ON] にします。

ステップ 3 [重大度（Severity）] レベルを選択します。このレベル以上のメッセージがコンソールに送信されます。

ステップ 4 [保存（Save）] をクリックします。

イベント ログ フィルタの設定

イベント ログ フィルタの設定は、宛先に送信されるメッセージを制御するためにロギング宛先に適用するカスタム フィルタです。通常、重大度のみに基づいて接続先へのメッセージをフィルタリングしますが、フィルタを使用して、イベント クラス、重大度、およびメッセージ識別子（ID）の組み合わせに基づいて送信されるメッセージを微調整できます。

重大度レベル単独でメッセージを制限するだけでは目的を満たすのに不十分である場合は、フィルタを使用します。

次の手順では、[オブジェクト（Objects）]ページでフィルタを設定する方法について説明します。フィルタを使用できるロギング宛先の設定時にフィルタを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [**イベントログフィルタ（Event Log Filters**）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（  ）をクリックします。

ステップ 3 フィルタ プロパティを設定します。

- [名前（Name）]：フィルタ オブジェクトの名前。
- [説明（Description）]：（オプション）オブジェクトの説明。
- [重大度とログクラス（Severity and Log Class）]：メッセージクラスでフィルタリングする場合は、[+] をクリックしてクラス フィルタの重大度レベルを選択し、[OK] をクリックします。次に、重大度レベル内のドロップダウン矢印をクリックし、その重大度レベルでフィルタリングする 1 つまたは複数のクラスを選択し、[OK] をクリックします。

  システムは、指定されたクラスのメッセージがその重大度レベル以上の場合のみ、syslog メッセージを送信します。重大度レベルごとに最大で 1 行を追加することができます。

  特定の重大度レベルですべてのクラスをフィルタリングする場合は、重大度リストを空のままにし、その代わりに、ロギング宛先を有効にするときにグローバル重大度レベルを選択します。
- [Syslog範囲/メッセージID（Syslog Range/Message ID）]：syslog メッセージ ID でフィルタリングする場合は、単独のメッセージ ID、またはメッセージを生成する ID 番号の範囲を

入力します。範囲の開始番号と終了番号は、100000-200000 のようにハイフンで区切ります。ID は 6 桁の数字です。特定のメッセージ ID および関連するメッセージについては、『*Cisco Firepower Threat Defense Syslog Messages*』（https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html）を参照してください。

ステップ 4 [保存（Save）] をクリックします。

それを許可するロギング宛先のカスタム フィルタリング オプションで、このオブジェクトを選択できるようになりました。**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[ロギング設定（Logging Settings）]** に移動します。

DHCP サーバの設定

DHCP サーバは、IP アドレスなどのネットワーク構成パラメータを DHCP クライアントに提供します。接続されたネットワークで DHCP クライアントに構成パラメータを提供するように、インターフェイスで DHCP サーバを設定できます。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャスト アドレスよりもブロードキャストを使用します。DHCP クライアントは UDP ポート 68 でメッセージを待ちます。DHCP サーバは UDP ポート 67 でメッセージを待ちます。DHCP サーバは、BOOTP 要求をサポートしていません。

DHCP クライアントは、サーバが有効になっているインターフェイスと同じネットワークに属している必要があります。つまり、スイッチがあるとしても、サーバとクライアントの間にルータを介在させることはできません。

（注） すでに DHCP サーバが動作しているネットワークで DHCP サーバを設定しないでください。2 つのサーバが競合するため、結果は予測不可能になります。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]** > **[DHCPサーバ（DHCP Server）]** リンクをクリックします。

[システム設定（System Settings）] ページをすでに開いている場合、目次の [DHCPサーバ（DHCP Server）] をクリックします。

ページには 2 つのタブがあります。当初、[設定（Configuration）] タブには、グローバル パラメータが表示されます。

[DHCPサーバ（DHCP Servers）] タブには、DHCP サーバを設定したインターフェイスと、サーバが有効にされているかどうか、そしてサーバのアドレス プールが表示されます。

ステップ 2 [設定（Configuration）] タブで、自動設定およびグローバル設定を設定します。

DHCP 自動設定では、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバ、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。通常、外部インターフェイスで DHCP を使用してアドレスを取得する場合には自動設定を使用しますが、DHCP を介してアドレスを取得するインターフェイスを選択することもできます。自動設定を使用できない場合には、必要なオプションを手動で定義できます。

a) 自動設定を利用する場合、**[自動設定を有効にする（Enable Auto Configuration）] > [オン（On）]** をクリックしてから（スライダは右側に移動）、DHCP を介してアドレスを取得するインターフェイスを [次のインターフェイスから取得（From Interface）] で選択します。

b) 自動設定を有効にしない場合、または自動設定された設定を上書きするには、次のグローバル オプションを設定します。これらの設定は、DHCP サーバをホストするすべてのインターフェイスで DHCP クライアントに送信されます。

- [プライマリ WINS IP アドレス（Primary WINS IP Address）]、[セカンダリ WINS IP アドレス（Secondary WINS IP Address）]：Windows インターネット ネーム サービス（WINS）サーバ クライアントのアドレスは、NetBIOS の名前解決に使用されます。
- [プライマリ DNS IP アドレス（Primary DNS IP Address）]、[セカンダリ DNS IP アドレス（Secondary DNS IP Address）]：クライアントがドメイン名の解決に使用するドメイン ネーム システム（DNS）サーバのアドレス。OpenDNS パブリック DNS サーバを設定するには、[OpenDNSを使用する（Use OpenDNS）] をクリックします。ボタンをクリックすると、適切な IP アドレスがフィールドにロードされます。

c) [保存（Save）] をクリックします。

ステップ 3 [DHCPサーバ（DHCP Servers）] タブをクリックし、サーバを設定します。

a) 次のいずれかを実行します。

- まだリストされていないインターフェイスの DHCP サーバを設定するには、[+] をクリックします。
- 既存の DHCP サーバを編集するには、そのサーバの編集アイコン（  ）をクリックします。

サーバを削除するには、サーバのごみ箱アイコン（  ）をクリックします。

b) サーバ プロパティを設定します。

- [DHCPサーバを有効にする（Enable DHCP Server）]：サーバを有効にするかどうかを決定します。サーバを設定できますが、使用する準備が整うまでサーバは無効にしておきます。
- [インターフェイス（Interface）]：クライアントに DHCP アドレスを提供するインターフェイスを選択します。インターフェイスは静的 IP アドレスを持っている必要があります。インターフェイスで DHCP サーバを実行する場合、インターフェイス アドレスの取得に DHCP を使用することはできません。ブリッジ グループの場合、 メンバー

インターフェイスではなく、ブリッジ仮想インターフェイス（BVI）で DHCP サーバを設定します。そうすると、サーバはすべてのメンバーインターフェイスで有効になります。

診断インターフェイスで DHCP サーバを設定することはできません。**[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）]** ページの管理インターフェイスで設定します。

- [アドレスプール（Address Pool）]：アドレスを要求するクライアントにサーバが提供できる IP アドレスの最小から最大までの範囲。プールの開始アドレスと終了アドレスをハイフンで区切って指定します。たとえば、 10.100.10.12-10.100.10.250 のように指定します。

  IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自体の IP アドレス、ブロードキャスト アドレス、またはサブネット ネットワーク アドレスを含めることはできません。

  アドレス プールのサイズは、FTD デバイスでプールあたり 256 に制限されています。アドレス プールの範囲が 253 アドレスよりも大きい場合、FTD インターフェイスのネットマスクは、クラス C アドレス（たとえば、255.255.255.0）にはできないため、それよりいくらか大きく、たとえば、255.255.254.0 にする必要があります。

c) [OK] をクリックします。

DNS の設定

ドメイン ネーム システム（DNS）サーバは、IP アドレスのホスト名の解決に使用されます。初期システム セットアップ時に DNS サーバを設定します。それにより、これらのサーバがデータ インターフェイスと管理インターフェイスに適用されます。セットアップ後に変更することが可能です。また、データ インターフェイスと管理インターフェイスに個別のサーバ セットを使用できます。

少なくとも、管理インターフェイスの DNS を設定する必要があります。FQDN ベースのアクセス制御ルールを使用する場合や、**ping** などの CLI コマンドでホスト名を使用する場合は、データ インターフェイスの DNS も設定する必要があります。

DNS の設定は、DNS グループを設定し、インターフェイスで DNS を設定するという 2 手順のプロセスです。

ここでは、このプロセスについて詳しく説明します。

DNS グループの設定

DNS グループは、DNS サーバおよび関連付けられているいくつかの属性のリストを定義します。管理インターフェイスとデータ インターフェイスで別々に DNS を設定できます。

www.example.com などの完全修飾ドメイン名（FQDN）を IP アドレスに解決するのには、DNS サーバが必要です。

デバイス セットアップ ウィザードが完了した後、次のシステム定義 DNS グループの一方または両方を使用できます。

- CiscoUmbrellaDNSServerGroup：このグループには、Cisco Umbrella と使用できる DNS サーバの IP アドレスが含まれています。初期セットアップ時にこれらのサーバを選択した場合、これが唯一のシステム定義グループになります。このグループの名前またはサーバ リストを変更することはできませんが、他のプロパティは編集できます。
- CustomDNSServerGroup：デバイス セットアップ時に Umbrella サーバを選択していない場合、システムはサーバ リストを使用してこのグループを作成します。このグループのすべてのプロパティを編集できます。

手順

ステップ 1 [オブジェクト（Objects）] を選択して、目次から [DNSグループ（DNS Groups）] を選択します。

ステップ 2 次のいずれかを実行します。

- グループを作成するには、[グループの追加（Add Group）] ボタン（  ）をクリックします。
- グループを編集するには、そのグループの [編集（edit）] アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 3 次のプロパティを設定します。

- [名前（Name）]：DNS サーバ グループの名前。DefaultDNS という名前は予約済みで使用できません。
- [DNS IPアドレス（DNS IP Addresses）]：DNS サーバの IP アドレスを入力します。複数のサーバを設定するには、[別のDNS IPアドレスを追加（Add Another DNS IP Address）] をクリックします。サーバ アドレスを削除する場合は、アドレスの [削除（delete）] アイコン（  ）をクリックします。

  リストは優先順です。リストの最初のサーバが常に使用されます。後続のサーバは、上位のサーバから応答が受信されない場合にのみ使用されます。最大6台のサーバを設定できます。ただし、6台のサーバはデータ インターフェイスでのみサポートされます。管理インターフェイスでは、最初の 3 台のサーバのみが使用されます。
- [ドメイン検索名（Domain Search Name）]：ネットワークのドメイン名（example.com など）を入力します。このドメインは、完全修飾されていないホスト名（たとえば、

serverA.example.com ではなく serverA）に追加されます。名前は、データ インターフェイスのグループを使用するために 63 文字以下にする必要があります。

- [再試行（Retries）]：システムが応答を受信しない場合にDNSサーバのリストを再試行する回数（0 ～ 10 の範囲）。デフォルトは 2 です。この設定は、データ インターフェイスのみで使用される DNS グループに適用されます。
- [タイムアウト（Timeout）]：次の DNS サーバを試行する前に待機する秒数（1 ～ 30）。デフォルトは2秒です。システムがサーバのリストを再試行するたびに、このタイムアウトは2倍になります。この設定は、データインターフェイスのみで使用されるDNSグループに適用されます。

ステップ 4 [OK] をクリックします。

データと管理インターフェイスの DNS の設定

ドメイン ネーム システム（DNS）サーバは、IP アドレスのホスト名の解決に使用されます。まず、データおよび管理DNS設定は、デバイスセットアップ ウィザードで設定したDNSサーバに基づいています。次の手順を使用して、デフォルトを変更できます。

configure network dns servers および **configure network dns searchdomains** コマンドを使用して、CLI で管理 DNS の設定を変更することもできます。データ インターフェイスおよび管理インターフェイスが同じ DNS グループを使用していて、そのグループが更新され次の展開段階にある場合、データ インターフェイスにも変更が適用されます。

DNS 解決に関する問題が発生した場合は、次を参照してください。

- DNS の一般的な問題のトラブルシューティング （16 ページ）
- 管理インターフェイスの DNS のトラブルシューティング

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）] > [DNSサーバ（DNS Server）]** リンクをクリックします。

[システム設定（System Settings）] ページをすでに開いている場合、目次の [DNSサーバ（DNS Server）] をクリックします。

ステップ 2 データ インターフェイスの DNS を設定します。

a) （オプション）[+] をクリックし、DNSルックアップを実行するときに使用する [インターフェイス（Interfaces）] を選択します。

デフォルトおよび推奨される値は [任意（Any）] であるため、ルックアップを任意のインターフェイス（ルーティング テーブルに基づいた）で実行できます。これらのインターフェイスを介してDNSサーバにアクセスする必要があることがわかっている場合にのみ、

特定のインターフェイスを選択します。診断インターフェイスのIPアドレスを設定している場合にのみ、診断インターフェイスを選択します。サーバにトラフィックを転送するには既存のルートが不十分である場合、DNS サーバのスタティック ルートを設定する必要があることがあります。

b) データ インターフェイスで使用するサーバを定義する [DNSグループ（DNS Group）] を選択します。グループが存在していない場合は、[DNSグループの新規作成（Create New DNS Group）]をクリックし、すぐに作成します。データ インターフェイスでルックアップしないようにするには、[なし（None）] を選択します。

c) （オプション）アクセス制御ルールで FQDN ネットワーク オブジェクトを使用する場合は、[FQDN DNS設定（FQDN DNS Settings）] を設定します。

これらのオプションは、FQDN オブジェクトのみを解決する場合に使用されます。その他のタイプの DNS 解決では無視されます。

- [ポーリング時間（Poll Time）]：FQDN ネットワーク オブジェクトを IP アドレスに解決するために使用するポーリング サイクルの時間（分単位）。FQDN オブジェクトは、アクセス コントロール ポリシーで使用されている場合にのみ解決されます。タイマーによって、解決間隔の最大時間が決定されます。また、DNSエントリの存続可能時間（TTL）の値を使用しても、IP アドレス解決を更新するタイミングを決定できます。したがって、個々のFQDNがポーリング サイクルよりも頻繁に解決される可能性があります。デフォルトは 240（4 時間）です。指定できる範囲は 1 ～ 65535 分です。

- [有効期限（Expiry）]：DNS エントリの期限が切れる（DNS サーバから取得した TTL が経過する）分数。この分数が経過すると、エントリは DNS ルックアップ テーブルから削除されます。エントリを削除するとテーブルの再コンパイルが必要になります。このため、頻繁に削除するとデバイスの処理負荷が大きくなる可能性があります。DNSエントリによってはTTLが極端に短い（3秒程度）場合があるため、この設定を使用してTTLを実質的に延長できます。デフォルトは1分です（つまり、TTLが経過してから 1 分後にエントリが削除されます）。指定できる範囲は 1 ～ 65535 分です。

d) [保存（Save）] をクリックします。設定を展開して、デバイスに変更を適用する必要もあります。

ステップ 3 管理インターフェイスの DNS を設定します。

a) 管理インターフェイスで使用するサーバを定義する [DNSグループ（DNS Group）] を選択します。グループが存在していない場合は、[DNSグループの新規作成（Create New DNS Group）] をクリックし、すぐに作成します。

b) [保存（Save）] をクリックします。変更はすぐにデバイスに適用されます。この変更を適用するために展開ジョブは実行しません。

DNS の一般的な問題のトラブルシューティング

管理インターフェイスおよびデータ インターフェイスに個別に DNS サーバを設定する必要があります。一部の機能では、両方ではなくどちらか片方のタイプのインターフェイスで名前解決を行います。所定の機能では、用途に応じて異なる解決方法を使用することもあります。

たとえば、**ping** *hostname* コマンドと**ping interface** *interface_name hostname* コマンドはデータ インターフェイス DNS サーバを使用して名前解決を行い、**ping system** *hostname* コマンドは管理インターフェイス DNS サーバを使用します。これにより、特定のインターフェイスおよびルーティング テーブルを介した接続をテストできます。

ホスト名ルックアップに関する問題をトラブルシューティングする場合は、このことに留意してください。

管理インターフェイスの DNS をトラブルシューティングする場合は、管理インターフェイスの DNS のトラブルシューティングも参照してください。

名前解決しない場合

単純に名前解決が実行されない場合のトラブルシューティングに関するヒントは、次のとおりです。

- 管理インターフェイスとデータ インターフェイスの両方に DNS サーバを設定していることを確認します。データ インターフェイスでは、インターフェイスに [任意（Any）] を使用します。これらのインターフェイス経由で DNS サーバにアクセスする必要がある場合にのみ、インターフェイスを明示的に指定します。
- データ インターフェイスでのルックアップに診断インターフェイスを使用している場合、そのインターフェイスで IP アドレスを設定していることを確認します。ルックアップでは、インターフェイスに IP アドレスがある必要があります。
- 各 DNS サーバの IP アドレスに ping を実行して、到達可能であることを確認します。**system** および **interface** キーワードを使用して、特定のインターフェイスをテストします。ping が失敗した場合は、スタティック ルートとゲートウェイを確認します。サーバのスタティック ルートを追加する必要がある場合があります。
- ping が成功して名前解決が失敗する場合は、アクセス制御ルールを確認します。サーバから到達可能なインターフェイスの DNS トラフィック（UDP/53）を許可していることを確認します。このトラフィックは、システムと DNS サーバの間にあるデバイスによってブロックされる可能性もあるため、別の DNS サーバを使用する必要がある場合があります。
- ping が機能する場合は適切なルートが存在し、アクセス制御ルールに問題はありません。DNS サーバに FQDN のマッピングが存在しない可能性を考えます。別のサーバを使用する必要がある場合があります。

名前解決が正しくない場合

名前解決は実行されるが名前の IP アドレスが最新のものではない場合、キャッシュに問題がある可能性があります。この問題は、アクセス制御ルールで使用される FQDN ネットワーク オブジェクトなどのデータ インターフェイス ベースの機能にのみ影響します。

システムには、以前のルックアップで取得したDNS情報のローカル キャッシュが存在します。新しいルックアップが要求されると、システムは最初にローカル キャッシュを調べます。ローカル キャッシュに情報がある場合、結果の IP アドレスが戻されます。ローカル キャッシュで要求を解決できない場合、DNS サーバにDNS クエリが送信されます。外部 DNS サーバによって要求が解決された場合、結果の IP アドレスが、対応するホスト名とともにローカル キャッシュに格納されます。

各ルックアップにはDNS サーバによって定義される存続可能時間値が設定されており、キャッシュからのルックアップは自動的に期限切れになります。また、システムはアクセス制御ルールで使用される FQDN の値を定期的に更新します。この更新は、少なくともポーリング間隔（デフォルトでは4時間ごと）で実行されますが、エントリの存続可能時間値に基づいて、より頻繁に実行できます。

show dns-hosts コマンドおよび **show dns** コマンドを使用して、ローカル キャッシュを確認します。FQDN の IP アドレスが正しくない場合は、**dns update**[**host** *hostname*] コマンドを使用して情報を強制的に更新できます。ホストを指定せずにコマンドを使用すると、すべてのホスト名が更新されます。

clear dns[**host** *fqdn*] コマンドおよび **clear dns-hosts cache** コマンドを使用して、キャッシュ情報を削除できます。

管理インターフェイスの設定

管理インターフェイスは物理的な管理ポートに接続されている仮想インターフェイスです。物理ポートは診断インターフェイスと呼ばれ、他の物理ポートとともにインターフェイス ページで設定できます。Firepower Threat Defense Virtual では、両方のインターフェイスが仮想であってもこの二重性が維持されます。

管理インターフェイスには 2 つの使い方があります。

- IP アドレスへの Web および SSH 接続を開き、インターフェイスからデバイスを設定できます。
- システムはこの IP アドレスを使用してスマート ライセンスおよびデータベースの更新情報を取得します。

CLI セットアップ ウィザードを使用すると、システムの初期設定時にデバイスの管理アドレスとゲートウェイを設定します。Firepower Device Manager のセットアップ ウィザードを使用すると、管理アドレスとゲートウェイ アドレスはデフォルトのまま変更されません。

必要に応じて、Firepower Device Manager を通じてこれらのアドレスを変更できます。**configure network ipv4 manual** および **configure network ipv6 manual** コマンドを使用して、CLI で管理アドレスおよびゲートウェイを変更することもできます。

管理ネットワーク上の他のデバイスが DHCP サーバとして機能している場合、スタティックアドレスを定義するか、またはDHCPを介してアドレスを取得できます。デフォルトでは、管理アドレスが固定で、DHCP サーバはポートで実行されます（DHCP サーバのない Firepower Threat Defense Virtual を除く）。そのため、デバイスを管理ポートに直接接続し、ワークステーションのDHCPアドレスを取得できます。これにより、デバイスの接続と設定が容易になります。

⚠

注意 現在接続されているアドレスを変更した場合は、その変更がすぐに適用されるため、変更の保存と同時に、Firepower Device Manager（または CLI）にアクセスできなくなります。デバイスに接続し直す必要があります。新しいアドレスが管理ネットワークで使用できることを確認します。

手順

ステップ 1 [デバイス（Device）] をクリックし、次に **[システム設定（System Settings）]** > **[管理インターフェイス（Management Interface）]** リンクをクリックします。

すでにシステム設定ページを開いている場合、目次の [管理インターフェイス（Management Interface）] をクリックします。

ステップ 2 管理ゲートウェイの定義方法を選択します。

ゲートウェイは、システムがインターネット経由でスマートライセンスとデータベース更新（VDB、ルール、地理位置情報、URLなど）を取得し、管理 DNS サーバと NTP サーバに到達する方法を決定します。次のオプションから選択します。

- [データインターフェイスをゲートウェイとして使用（Use the Data Interfaces as the Gateway）]：物理管理インターフェイスに接続されている別の管理ネットワークがない場合、このオプションを選択します。トラフィックは、ルーティングテーブルに基づいてインターネットにルーティングされ、通常は、外部インターフェイスを通過します。これがデフォルトのオプションです。ただし、このオプションは Firepower Threat Defense Virtual デバイスではサポートされません。
- [IPアドレスに固有のゲートウェイを使用（Use Unique Gateways for the Management Interface）]：管理インターフェイスに接続されている別の管理ネットワークがある場合、IPv4 および IPv6 に固有のゲートウェイ（以下）を指定します。

ステップ 3 管理アドレス、サブネット マスクまたは IPv6 プレフィックス、および IPv4、IPv6、またはその両方のゲートウェイ（必要に応じて）を設定します。

少なくとも 1 組のプロパティを設定する必要があります。1 組は空白にし、そのアドレッシング方式を無効にします。

[タイプ（Type）] > **{DHCP]** を選択し、DHCP または IPv6 自動設定によってアドレスおよびゲートウェイを取得します。ただし、ゲートウェイとしてデータインターフェイスを使用して

いる場合、DHCPを使用することはできません。この場合はスタティックアドレスを使用する必要があります。

ステップ4 （オプション）スタティック IPv4 アドレスを設定する場合、ポート上で DHCP サーバを設定します。

管理ポート上でDHCPサーバを設定する場合、直接接続されているクライアント、または管理ネットワーク上のクライアントは、DHCPプールからそれぞれのアドレスを取得できます。このオプションは Firepower Threat Defense Virtual デバイスではサポートされません。

a) **[DHCPサーバを有効化（Enable DHCP Server）]** > **[オン（On）]** をクリックします。
b) サーバの [アドレスプール（Address Pool）] を入力します。

アドレスプールとは、アドレスを要求するクライアントに対してサーバが提供できる、最小から最大までの IP アドレスの範囲です。IP アドレスの範囲は管理アドレスと同じサブネット上にある必要があり、次のものを含めることはできません：インターフェイス自体のIPアドレス、ブロードキャストアドレス、またはサブネットのネットワークアドレス。プールに開始/終了アドレスをハイフンで区切って指定します。たとえば、192.168.45.46-192.168.45.254 などです。

ステップ5 [保存（Save）] をクリックして警告を読み、[OK] をクリックします。

デバイスのホスト名の設定

デバイス ホスト名を変更できます。

また、CLI で **configure network hostname** コマンドを使用してホスト名を変更することもできます。

⚠

注意 ホスト名を使用してシステムに接続しているときにホスト名を変更すると、変更はただちに適用されるため、変更を保存するときに Firepower Device Manager へのアクセスが失われます。デバイスに接続し直す必要があります。

手順

ステップ1 [デバイス（Device）] をクリックします。 をクリックし、**[システム設定（System Settings）]** > **[ホスト名（Hostname）]** リンクの順にクリックします。

すでにシステム設定ページを開いている場合、目次の [ホスト名（Hostname）] をクリックします。

ステップ2 新しいホスト名を入力します。
ステップ3 [保存（Save）] をクリックします。

ホスト名の変更は、いくつかのシステムプロセスにすぐに適用されます。ただし、すべてのシステムプロセスで同じ名前が使用されるため、更新を完了するには変更を展開する必要があります。

Network Time Protocol（NTP）の設定

システムの時刻を定義するには、Network Time Protocol（NTP）サーバを設定する必要があります。NTP サーバはシステムの初期設定時に設定しますが、次の手順を使用して変更できます。NTP 通信に関する問題が発生した場合は、NTP のトラブルシューティングを参照してください。

手順

ステップ 1 [デバイス（Device）] をクリックします。 をクリックし、**[システム設定（System Settings）]** > **[NTP]** リンクの順にクリックします。

すでに [システム設定（System Settings）] ページが表示されている場合は、目次の [NTP] をクリックします。

ステップ 2 [NTPタイムサーバ（NTP Time Server）] で、独自のタイム サーバとシスコのタイム サーバのどちらを使用するか選択します。

- [Cisco NTPタイムサーバ（Cisco NTP Time Server）][デフォルトNTPタイムサーバ（Default NTP Time Server）][デフォルトNTPサーバ（Default NTP Servers）]：このオプションを選択すると、NTP に使用するサーバ名がサーバ リストに表示されます。
- [手動入力（Manually Input）][ユーザ定義NTPサーバ（User-Defined NTP Servers）]：このオプションを選択する場合は、使用する NTP サーバの完全修飾ドメイン名または IP アドレスを入力します。例、ntp1.example.com または 10.100.10.10。複数の NTP サーバがある場合は、[別のNTPタイムサーバを追加（Add Another NTP Time Server）] をクリックしてアドレスを入力します。

ステップ 3 [保存（Save）] をクリックします。

URL フィルタリングの設定

URL カテゴリおよびレピュテーション データベースは Cisco Collective Security Intelligence（CSI）から取得されます。これらの設定により、データベースの更新とシステムが不明なカテゴリまたはレピュテーションの URL を処理する方法が制御されます。これらの設定を行うには、URL フィルタリング ライセンスを有効にする必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックします。 をクリックしてから、**[システム設定（System Settings）] > [URLフィルタリングの設定（URL Filtering Preferences）]** リンクの順にクリックします。

[システム設定（System Settings）] ページをすでに開いている場合、目次の [クラウドの基本設定（Cloud Preferences）]と [URLフィルタリングの基本設定（Filtering Preferences）] をクリックします。

ステップ 2 次のオプションを設定します。

- [自動更新の有効化（Enable Automatic Updates）]：カテゴリとレピュテーションを含む更新されたURLデータをチェックしてダウンロードすることをシステムに許可します。データは通常 1 日に 1 回更新されますが、システムは 30 分ごとに更新をチェックします。デフォルトでは、更新が有効になっています。このオプションを選択解除した状態でカテゴリとレピュテーションのフィルタリングを使用している場合、このオプションを周期的に有効にして新しい URL データを取得してください。
- [不明なURLに対するCisco CSIのクエリ （Query Cisco CSI for Unknown URLs）]：ローカル URL フィルタリング データベースのカテゴリおよびレピュテーションのデータを含まない URL の更新情報を Cisco CSI でチェックするかどうかを切り替えます。ルックアップが適度な制限時間内に更新情報を返した場合、その情報は、URL の状況に基づいてアクセス ルールを選択する際に使用されます。それ以外の場合、URL は分類されていないカテゴリと照合されます。メモリ制限によりインストールされる URL データベースが小さいローエンドのシステムでは、このオプションを選択することが重要です。
- [URL存続可能時間（URL Time to Live）]（[未知のURL用Cisco CSIのクエリ（Query Cisco CSI for Unknown URLs）]を選択している場合にのみ利用可能）：指定された URL のカテゴリおよびレピュテーション ルックアップ値を保持する時間。存続可能時間が経過すると、次に試行される URL のアクセスが新規のカテゴリ/レピュテーション ルックアップになります。時間が短いほどURLフィルタリングが正確になり、時間が長いほど未知のURLに対するパフォーマンスが向上します。TTL は 2、4、8、12、24、または 48 時間、1 週間、または [使用しない（Never）]（デフォルト）に設定できます。

ステップ 3 [保存（Save）] をクリックします。

クラウド サービスの設定

[クラウドサービス（Cloud Services）]ページを使用すると、デバイスによって使用されるクラウドベースのサービスをデバイス側から管理できます。特定のサービスを登録した後は、クラウドから管理する必要があります。

Cisco Smart Software Manager でデバイスを登録している場合（推奨される最初のステップです）、ページ上部の [クラウドサービスポータル（Cloud Services Portal）] リンクをクリックすると、Cisco Services Exchange に移動し、クラウドベースのサービスを管理できます。

ここでは、クラウド サービスのオプションについて説明します。

クラウド管理の設定（Cisco Defense Orchestrator）

Cisco Defense Orchestrator のクラウドベースのポータルを使用してデバイスを管理できます。Cisco Defense Orchestrator を使用すると、次のテクニックによりデバイス管理にアプローチできます。

- 初期設定のダウンロード：このアプローチでは、Cisco Defense Orchestrator からデバイスの初期設定をダウンロードしますが、その後 Firepower Device Manager を使用してデバイスをローカルで設定します。

（注） Firepower Device Manager を使用してデバイスを設定した後、代わりにクラウド経由でデバイスを管理することにした場合、クラウドベースの設定でローカルの変更を重複させるようにします。

- クラウドによるリモート設定管理：このアプローチでは、Cisco Defense Orchestrator を使用してデバイス設定を作成および更新します。このアプローチを使用する場合、ローカルで設定を変更しないでください。各クラウドの導入では、クラウドで定義した設定によりデバイスのローカル設定が置き換えられるためです。ローカルで変更した場合、変更を維持するには、クラウドベースの設定でも同じ設定を繰り返してください。

クラウド管理の仕組みの詳細については、Cisco Defense Orchestrator ポータル（http://www.cisco.com/go/cdo）を参照するか、共に作業している再販業者またはパートナーにお問い合わせください。

始める前に

Cisco Defense Orchestrator に登録するために推奨される方法は、最初に Cisco Smart Software Manager にデバイスを登録することです。その後、クラウドから Cisco Defense Orchestrator に登録します。すでにアカウントを持っている場合は、[有効化（Enable）] ボタンをクリックできます。デバイスを登録していない場合は、次の手順を使用します。

Cisco Defense Orchestrator の登録キーを取得します。

また、デバイスにインターネットへのルートがあることを確認します。

（注） ハイ アベイラビリティを設定する予定の場合、ハイ アベイラビリティ グループで使用する両方のデバイスを登録する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）] > [クラウドサービス（Cloud Services）]** リンクの順にクリックします。

すでに [システム設定（System Settings）] ページを表示している場合は、目次の[クラウド管理（Cloud Management）][クラウドサービス（Cloud Services）] をクリックします。

ステップ 2 [Cisco Defense Orchestrator] グループで、[始める（Get Started）] をクリックします。

ステップ 3 [登録キー（Registration Key）] にキーを貼り付け、[接続（Connect）] をクリックします。

登録要求がクラウドポータルに送信されます。キーが有効で、インターネットへのルートがある場合、デバイスはポータルに正常に登録されるはずです。その後、ポータルを使用してデバイスを管理できます。

クラウド管理を使用しない場合は、[無効化（Disable）] をクリックします。

（注） Cisco Smart Software Manager からデバイスの登録を解除する場合、または評価モードで評価期間の期限が切れる場合は自動的に登録解除されます。

Cisco Success Network への接続

デバイスを登録するときに、Cisco Success Network への接続を有効にするかどうかを決めます。デバイスの登録を参照してください。

Cisco Success Network を有効にすると、テクニカル サポートを提供するために不可欠な使用状況の情報と統計情報がシスコに提供されます。またこの情報により、シスコは製品を向上させ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。

接続を有効にすると、シスコから提供されているテクニカル サポート サービス、クラウド管理および監視サービスなどの追加サービスに参加できるように、デバイスで Cisco Cloud へのセキュアな接続が確立されます。お使いのデバイスは、いつでもこのセキュアな接続を確立して維持できます。クラウドから完全に切断する方法については、Cisco Security Services Exchange の登録の無効化 （24 ページ）を参照してください。

デバイスを登録した後で Cisco Success Network の設定を変更できます。

（注） システムがシスコにデータを送信する際に、タスク リストにテレメトリ ジョブが表示されます。

始める前に

Cisco Success Network を有効にするには、デバイスをクラウドに登録する必要があります。デバイスを登録するには、（[スマートライセンス（Smart Licensing）] ページで）Cisco Smart Software Manager にデバイスを登録するか、または登録キーを入力して Cisco Defense Orchestrator に登録します。

（注） ハイアベイラビリティ グループのアクティブ装置で Cisco Success Network を有効にする場合、スタンバイ装置での接続も有効にします。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）] > [クラウドサービス（Cloud Services）]** リンクの順にクリックします。

[システム設定（System Settings）] ページがすでに表示されている場合は、目次で [クラウドサービス（Cloud Services）] をクリックします。

ステップ 2 必要に応じて Cisco Success Network 機能の [有効化（Enable）]/[無効化（Disable）] コントロールをクリックして設定を変更します。

[サンプルデータ（sample data）] リンクをクリックするとシスコに送信される情報の種類を確認できます。

接続を有効にする場合、情報開示を読み、[同意（Accept）] をクリックします。

Cisco Security Services Exchange の登録の無効化

デバイスを Cisco Defense Orchestrator に登録するか、Cisco Success Network または Cisco Threat Response を有効にするか、、または Cisco Smart Software Manager にデバイスを登録すると、デバイスが Cisco Security Services Exchange に登録されます。すべてのクラウド サービスを無効にしても、デバイスは登録されたままになります。

接続を有効にすると、シスコから提供されているテクニカル サポート サービス、クラウド管理および監視サービスなどの追加サービスに参加できるように、デバイスで Cisco Security Services Exchange へのセキュアな接続が確立されます。お使いのデバイスは、いつでもこのセキュアな接続を確立して維持できます。

場合によっては、別のスマート ライセンシング アカウントに登録できるように、またはサービスからデバイスを削除するために、Cisco Security Services Exchange へのデバイスの登録を削除する必要があります。

手順

ステップ 1 **[デバイス（Device）] > [システム設定（System Settings）] > [クラウドサービス（Cloud Services）]** ページで、すべてのクラウド サービスを無効にします。

ステップ 2 **[デバイス（Device）] > [スマートライセンス（Smart License）]** を選択し、歯車ドロップダウン リストから [デバイスの登録解除（Unregister Device）] を選択します。

ステップ 3 デバイスをクラウドに再登録する場合は、次のいずれかを実行します。

- シスコ セキュリティ アカウントを使用する場合は、**[デバイス（Device）] > [システム設定（System Settings）] > [クラウドサービス（Cloud Services）]** を選択し、トークンを使用して Cisco Defense Orchestrator に再登録します。その後、**[デバイス（Device）] > [スマートライセンス（Smart License）]** に移動し、デバイスを再登録することができます。
- スマート ライセンス アカウントを使用する場合は、**[デバイス（Device）] > [スマートライセンス（Smart License）]** ページでデバイスを登録します。これで、[クラウドサービス（Cloud Services）] ページに戻り、必要なサービスを再度有効にすることができます。

Web 分析の有効化と無効化

Web分析を有効にすると、ページのヒット数に基づいて匿名の製品使用情報をシスコに提供できます。情報には、表示したページ、ページで費やした時間、ブラウザのバージョン、製品バージョン、デバイスのホスト名などが含まれます。この情報は、シスコが機能の使用状況パターンを確認し、製品を改善するのに使用されます。すべての使用状況データは匿名で、センシティブ データは送信されません。

Web 分析はデフォルトで有効になっています。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）] > [クラウドサービス（Cloud Services）]** リンクの順にクリックします。

[システム設定（System Settings）] ページがすでに表示されている場合は、目次で [クラウドサービス（Cloud Services）] をクリックします。

ステップ 2 必要に応じて [Web分析（Web Analytics）] 機能の [有効化（Enable）]/[無効化（Disable）] コントロールをクリックして設定を変更します。

Cisco Threat Response の有効化または無効化

Cisco Threat Response のクラウドベース アプリケーション（https://visibility.amp.cisco.com/）に侵入イベントおよび観察結果を送信することができます。その後、このサービスを利用してデバイスがクラウドに送信した脅威の分析および評価を実行できます。イベントをクラウドに送信するには、侵入ポリシーを少なくとも 1 つのアクセス制御ルールに適用する必要があります。

アプリケーションの使い方と利点についての動画は、YouTube でご視聴いただけます（http://cs.co/CTRvideos）。FTD での Cisco Threat Response の使い方の詳細については、『*Firepower And CTR Integration Guide*』を参照してください（https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html）。

スマート ライセンスの管理にサテライト サーバを使用している場合は、接続を有効にすることはできません。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]** > **[クラウドサービス（Cloud Services）]** リンクの順にクリックします。

[システム設定（System Settings）] ページがすでに表示されている場合は、目次で [クラウドサービス（Cloud Services）] をクリックします。

ステップ 2 必要に応じて **Cisco Threat Response** 機能の [有効化（Enable）]/[無効化（Disable）] コントロールをクリックして設定を変更します。

接続を有効にする場合、情報開示を読み、[同意（Accept）] をクリックします。