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

管理アクセスとは、設定およびモニター目的で 脅威に対する防御 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。

- ユーザー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。ローカルユーザーデータベースまたは外部AAAサーバーを使用することができます。管理ユーザーの管理の詳細については、Device Manager および Threat Defense ユーザー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（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。

- Device Manager に接続するためにユーザーが受け入れる必要がある管理 Web サーバー証明書。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、ユーザー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。Threat Defense Web サーバー証明書の設定 （5 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、デバイスの管理アドレス上の Device Manager Web または 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、Device Manager または SSH から CLI への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」ブリッジグループが設定されている Firepower 1010 の場合、この設定は、ブリッジグループに含まれる任意のデータインターフェイスを使用して Device Manager をブリッジグループ IP アドレス（デフォルトは 192.168.95.1）に接続できることを意味します。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は、Device Manager アクセス（HTTPS アクセス）とリモートアクセス SSL VPN の両方を設定できません。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。同じインターフェイスで両方の機能を設定する場合は、競合を回避するために、必ず、これらのサービスの少なくとも 1 つの HTTPS ポートを変更してください。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[System Settings]** > **[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（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、Device Manager および Threat Defense ユーザー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、指定され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。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。あるプロトコルのルールをすべて削除した場合、そのプロトコルを使用して該当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なくなります。

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。

ルールのリストは、インターフェイス上の指定され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。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。あるプロトコルのルールをすべて削除した場合、そのプロトコルを使用して該当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なくなります。

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) （任意）HTTPS データポート番号を変更する場合は、番号をクリックし、新しいポートを入力します。データインターフェイスでの管理アクセス用の HTTPS ポートの設定 （4 ページ）を参照してください。

d) [OK] をクリックします。

データインターフェイスでの管理アクセス用の HTTPS ポートの設定

デフォルトでは、Device Manager または Threat Defense API のいずれかで管理のためにデバイスにアクセスする場合、ポート TCP/443 を経由します。データインターフェイスの管理アクセスポートは変更できます。

ポートを変更すると、ユーザは、システムにアクセスするための URL にカスタムポートを含める必要があります。たとえば、データインターフェイスが ftd.example.com であり、ポートを 4443 に変更した場合、ユーザは URL を https://ftd.example.com:4443 に変更する必要があります。

すべてのデータインターフェイスで同じポートが使用されます。インターフェイスごとに異なるポートを設定することはできません。

（注） 管理インターフェイスの管理アクセスポートは変更できません。管理インターフェイスでは常にポート 443 が使用されます。

手順

ステップ 1 [Device] をクリックしてから、**[System Settings]** > **[Management Access]** リンクの順にクリックします。

[System Settings] ページがすでに表示されている場合は、目次で [Management Access] をクリックします。

ステップ 2 [Data Interfaces] タブをクリックします。

ステップ 3 [HTTPS Data Port] 番号をクリックします。

ステップ 4 [Data Interfaces Setting] ダイアログボックスで [HTTPS Data Port] を、使用するポートに変更します。

次の番号は指定できません。

- 22：このポートは SSH 接続に使用されます。
- リモートアクセス VPN に使用するポート（管理アクセスも許可されているインターフェイス用に設定されている場合）：リモートアクセス VPN はデフォルトではポート 443 を使用しますが、カスタムポートを設定できます。
- アイデンティティポリシーでアクティブ認証に使用するポート：デフォルトは 885 です。

ステップ 5 [OK] をクリックします。

Threat Defense Web サーバー証明書の設定

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。ユーザーは証明書を Trusted Root Certificate ストアに保存することもできますが、その代わりにブラウザが信頼するよう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。

[System Settings] ページがすでに表示されている場合は、目次で [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、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 証明書が自己署名されていない場合は、完全な信頼チェーン内のすべての中間証明書とルート証明書を信頼チェーンリストに追加します。

チェーンには最大 10 個の証明書を追加できます。[+] をクリックして各中間証明書を追加し、最後にルート証明書を追加します。[保存（Save）] をクリックし（Webサーバの再起動を警告するダイアログで [続行（Proceed）] をクリックすると）、証明書がない場合は、欠落しているチェーン内の次の証明書の共通名を含むエラーメッセージが表示されます。チェーンに含まれていない証明書を追加した場合も、エラーが表示されます。これらのメッセージを慎重に調べて、追加または削除する必要がある証明書を特定してください。

ここから証明書をアップロードするには、[+] をクリックした後に、[新規信頼CA証明書の作成（Create New Trusted CA Certificate）] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

変更はすぐに適用され、システムは Web サーバーを再起動します。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

Threat Defense 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、デバイスとシステムの正常性に関連するイベントと、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、https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html にある『*Cisco Threat Defense Syslog Messages*』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。

シビラティ（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	**emergencies**	システムが使用不可能な状態です。
1	**alert**	すぐに措置する必要があります。
2	**critical**	深刻な状況です。
3	**error**	エラー状態です。
4	**warning**	警告状態です。
5	**Notification（通告）**	正常ですが、注意を必要とする状況です。
6	**informational**	情報メッセージです。
7	**debugging**	デバッグ メッセージです。 問題をデバッグするときに、このレベルで一時的にのみログに記録します。このログレベルでは、非常に多くのメッセージが生成される可能性があるため、システムパフォーマンスに影響を与える可能性があります。

（注） ASA および 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 サーバーのロギングの設定

syslog のメッセージを外部 syslog サーバーに送信するようにシステムを設定できます。これはシステムロギングの最適なオプションです。外部サーバーを使用すると、メッセージを保持するためのスペースを確保し、サーバーの施設を使用してメッセージを表示、分析、およびアーカイブできます。

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サーバー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 サーバーを設定しない場合、イベントは Device Manager イベントビューアのみに表示されます。

次の手順では、診断（データ）ロギングとファイル/マルウェアロギング用に Syslog をイネーブルにする方法について説明します。次のイベント用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 サーバーを選択します。
- 侵入イベントの場合は、侵入ポリシーの設定で syslog サーバーを選択します。

始める前に

ファイル/マルウェアイベントの syslog 設定は、IPS およびマルウェア防御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 [ロギングの設定（Logging Settings）] をクリックします。

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

- [Syslogサーバー（Syslog Server）]：[+] をクリックし、1 つまたは複数の syslog サーバー 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 サーバーの追加（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 サーバーの設定」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、デバイスに関連している場合にのみ表示されます。重大度のレベルを選択します。このレベル以上のメッセージが syslog サーバーに送信されます。
- [メッセージフィルタリング（Message Filtering）]：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が syslog サーバーに送信されます。
  - [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リストフィルタを選択します。この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 リスト フィルタの設定 （10 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サーバー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「オン」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サーバー（Syslog Server）]：syslog サーバー 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サーバーの追加（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。これは、メッセージの [シビラティ（重大度）（severity）] 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に syslog メッセージを保存できます。この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。バッファの空きがなくなると、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。ログバッファに空きがなくなると、システムは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 [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「オン」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が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 リスト フィルタを選択します。この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 リスト フィルタの設定 （10 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できます。コンソールポートの CLI にログインしたとき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 [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「オン」にします。

ステップ 3 **重大度**の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 リスト フィルタの設定

[イベントリストフィルタ（event list filter）] 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できるカスタムフィルタです。通常は、シビラティ（重大度）のみに基

づいて宛先へのメッセージをフィルタ処理しますが、カスタムフィルタを使用すると、イベントクラス、シビラティ（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、送信するメッセージを微調整できます。

シビラティ（重大度）レベル単独でのメッセージの制限では目的を十分に果たせない場合は、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 **[イベントリストフィルタ（Event List 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（trash can）] アイコン（  ）をクリックします。

ステップ 3 フィルタの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、シビラティ（重大度）レベル内のドロップダウン矢印をクリックして、そのシビラティ（重大度）レベルでフィルタ処理する 1 つ以上のクラスを選択し、[OK] をクリックします。

  システムは、そのシビラティ（重大度）レベル以上のメッセージがある場合にのみ、指定されたメッセージクラスの syslog メッセージを送信します。各シビラティ（重大度）レベルには、最大で 1 つの行を追加できます。

  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そのロギング宛先の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。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、https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html の『*Cisco Threat Defense Syslog Messages*』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。

これで、[カスタムフィルタリング（custom filtering）] オプションでこのオブジェクトを選択して、そのオブジェクトを許可する宛先をロギングできます。**[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 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。インターフェイス上の DHCP サーバーを設定して、接続されたネットワーク上の DHCP クライアントに設定パラメータを提供するか、またはインターフェイス上の DHCP リレーを有効にして、ネットワーク内の別のデバイスで動作している外部 DHCP サーバーに要求を転送できます。

これらの機能は相互に排他的です。いずれか一方のみ設定でき、両方は設定できません。

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。

（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。

始める前に

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。

複数のネットワークをサポートする必要があり、各インターフェイスで DHCP サーバを設定したくない場合は、代わりに DHCP リレーを設定して、一つのネットワークから別のネットワークに存在する DHCP サーバに DHCP 要求を転送できます。この場合、DHCP サーバはネットワーク内の別のデバイス上に存在する必要があります。一つのインターフェイスで DHCP サーバを設定し、同じデバイスの別のインターフェイスで DHCP リレーを設定することはできません。DHCP リレーを使用する場合は、DHCP サーバが管理する各ネットワークアドレス空間のアドレスプールを DHCP サーバに設定してください。

DHCP リレーを設定する方法については、DHCP リレーの設定 （15 ページ）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、**[システム設定（System Settings）]** > **[DHCP サーバー/リレー（DHCP Server / Relay）]** リンクをクリックします。

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 [DHCPサーバー（DHCP Server）] **[DHCP]** > **[DHCPサーバー（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。

仮想ルータを設定する場合、DHCP サーバの自動設定は、グローバル仮想ルータのインターフェイスのみで使用できます。自動設定は、ユーザ定義の仮想ルータに割り当てられているインターフェイスではサポートされていません。

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。

  この画面で Management インターフェイス上に DHCP サーバーを設定することはできません。その代わりに、**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** ページで、管理インターフェイス上に DHCP サーバーを設定します。
- [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、脅威に対する防御 デバイス上のプールあたり 256 アドレス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、脅威に対する防御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。

DHCP リレーの設定

インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。

DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワーク セグメントにクライアントがある場合、脅威に対する防御 デバイスはブロードキャスト トラフィックを転送しないため、UDP ブロードキャストは通常転送されません。DHCP リレーエージェントを使用して、ブロードキャストを受信している脅威に対する防御デバイスのインターフェイスを、別のインターフェイスを介して利用可能な DHCP サーバに DHCP 要求を転送するように設定できます。

そのため、DHCP サーバをホストしていないサブネット上のクライアントでも、別のサブネットに存在する DHCP サーバから IP アドレスリースを取得できます。

始める前に

- 追加するサブネットごとに、アドレスプールを使用して DHCP サーバを設定します。たとえば、アドレスが 192.168.1.1/24 のインターフェイスで DHCP リレークライアントを有効にする場合、192.168.1.0/24 ネットワーク上のクライアントをサポートするには、DHCP サーバが 192.168.1.0/24 サブネットの IP アドレス（192.168.1.2 ～ 192.168.1.254 など）を提供できる必要があります。
- DHCP サーバごとに、サーバの IP アドレスを指定して、ホスト ネットワーク オブジェクトを作成します。
- **[DHCP]** > **[DHCPサーバ（DHCP Servers）]** ページで、すべてのサーバが削除または無効化されていることを確認します。いずれかのインターフェイスで DHCP リレーが有効になっている場合は、どのインターフェイスでも（異なるインターフェイスであっても）DHCP サーバをホストできません。
- インターフェイスに関する制限：インターフェイスには、サーバまたはエージェントのいずれかに使用される名前が必要です。また、次の点に注意してください。
  - インターフェイスをルーティング ECMP トラフィックゾーンのメンバーにすることはできません。
  - インターフェイスは DHCP を使用してアドレスを取得できません。
  - DHCP サーバと DHCP リレーの両方を、物理インターフェイス、サブインターフェイス、VLAN インターフェイス、および EtherChannel で設定できます（それらのメンバーでは設定できない）。
  - 仮想トンネルインターフェイス（VTI）で DHCP リレーサーバを設定することもできます。
  - どちらのサービスも、管理インターフェイス、またはブリッジグループとそのメンバーをサポートしません。

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）] > [DHCPサーバ/リレー（DHCP Server / Relay）]** リンクをクリックして、目次の **[DHCP] > [DHCPリレー（DHCP Relay）]** 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は、目次の **[DHCP] > [DHCPリレー（DHCP Relay）]** をクリックします。

ステップ 2 （任意）必要に応じて、[IPv4リレータイムアウト（IPv4 Relay Timeout）] と [IPv6リレータイムアウト（IPv6 Relay Timeout）] の設定を調整します。

これらのタイムアウトにより、特定の IP バージョンの DHCP リレー アドレス ネゴシエーションで許可される秒数が設定されます。デフォルトは 60 秒（1 分）ですが、1 ー 3600 秒の範囲で異なるタイムアウトを設定できます。サブネットと DHCP サーバの間に大きな遅延がある場合は、タイムアウトを長くすることが適切である可能性があります。

ステップ 3 **DHCP リレーサーバ**を設定します。

DHCP リレーサーバは、DHCP リレー要求を処理するネットワーク内の DHCP サーバです。これらの DHCP サーバは、ネットワーク内の設定しているデバイスとは異なるデバイス上に存在します。

a) [+] をクリックし、DHCP サーバの IP アドレスを持つホストネットワークオブジェクトを選択して、[OK] をクリックします。

オブジェクトがまだ存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックして、今すぐ作成します。追加した DHCP サーバを使用する必要がなくなった場合は、サーバのエントリの右側にある [X] をクリックして削除します。

b) 追加した DHCP サーバのエントリをクリックし、その DHCP サーバに到達できるインターフェイスを選択します。

ステップ 4 DHCP リレーエージェントを設定します。

DHCP リレーエージェントはインターフェイス上で動作します。これらは、ネットワークセグメント上のクライアントからの DHCP 要求を DHCP サーバに転送してから、応答をクライアントに返します。

a) [+] をクリックし、DHCP リレーエージェントを実行するインターフェイスを選択して、[OK] をクリックします。

インターフェイスで DHCP リレーエージェントを実行する必要がなくなった場合は、サーバのエントリの右側にある [X] をクリックして削除します。必要に応じて、テーブルからインターフェイスを削除せず、単にすべての DHCP リレーサービスを無効にすることができます。

b) 追加したインターフェイスエントリをクリックし、エージェントが提供する DHCP サービスを選択して、[OK] をクリックします。

- [IPv4 を有効にする（Enable IPv4）]：IPv4 アドレス要求を DHCP サーバに転送します。このオプションを選択しない場合、IPv4 アドレス要求は無視され、クライアントは IPv4 アドレスを取得できません。
- [ルート設定（Set Route）]（IPv4 のみ）：DHCP サーバーから送信されるパケットにある最初のデフォルトルータアドレスを、DHCP リレーエージェントを実行している脅威に対する防御デバイスインターフェイスのアドレスに変更します。このアクションを行うと、クライアントは、自分のデフォルトルートを設定して、DHCP サーバで異なるルータが指定されている場合でも、脅威に対する防御デバイスをポイントすることができます。パケット内にデフォルトのルータオプションがなければ、DHCP リレーエージェントは、そのインターフェイスのアドレスを含んでいるデフォルトルータを追加します。
- [IPv6 を有効にする（Enable IPv6）]：IPv6 アドレス要求を DHCP サーバに転送します。このオプションを選択しない場合、IPv6 アドレス要求は無視され、クライアントは IPv6 アドレスを取得できません。

ステップ 5 [保存（Save）] をクリックします。

ダイナミック DNS（DDNS）の設定

Web 更新方式を使用してダイナミック ドメイン ネーム システム（DDNS）の変更をダイナミック DNS サービスに送信するようにシステムを設定できます。これらのサービスは、完全修飾ドメイン名（FQDN）に関連付けられた新しい IP アドレスを使用するように DNS サーバを更新します。これにより、ユーザがホスト名を使用してシステムにアクセスしようとしたときに、DNS によって名前が正しい IP アドレスに解決されます。

DDNS を使用すると、システムのインターフェイスに定義された FQDN が常に正しい IP アドレスに解決されるようになります。これは、DHCP を使用してインターフェイスのアドレスを取得するように設定する場合に特に重要です。また、スタティック IP アドレスに使用しても効果的です。DNS サーバに正しいアドレスが保持され、スタティックアドレスを変更した場合に簡単に更新できるようになります。

選択した DDNS サービスプロバイダーのグループを使用するように DDNS を設定できるほか、カスタムオプションを使用すると Web 更新をサポートする他の DDNS プロバイダーに更新を送信できます。インターフェイスに指定する FQDN をこれらのサービスプロバイダーに登録する必要があります。

（注） Device Manager を使用して設定できるのは Web 更新の DDNS のみです。IETF RFC 2136 で定義されている方式の DDNS は設定できません。

始める前に

プロバイダーの証明書を検証する信頼できる CA 証明書が必要です。この証明書がシステムにないと、DDNS 接続は成功しません。証明書はサービスプロバイダーのサイトからダウンロードできます。適切な証明書がアップロードされて展開されていることを確認してください。また、アップロードした証明書の [検証の使用（Validation Usage）] が SSL サーバーを含むように設定されていることを確認します。「信頼できる CA 証明書のアップロード」を参照してください。

手順

ステップ 1 [Device] をクリックし、**[System Settings]** > **[DDNS Service]** リンクをクリックします。

[System Settings] ページをすでに開いている場合、目次の [DDNS Service] をクリックします。

このページには、サービスプロバイダー、インターフェイス、インターフェイスの完全修飾ドメイン名（FQDN）、DNS サーバーで FQDN の IP アドレスの変更を更新する頻度など、DDNS 更新方式のリストが表示されます。エントリの [ステータスの表示（Show Status）] リンクをクリックすると、エントリが正しく機能しているかどうかを確認できます。

ステップ 2 次のいずれかを実行します。

- 新しいダイナミック DNS 更新方式を作成するには、[+] または [Create DDNS Service] ボタンをクリックします。
- 既存のダイナミック DNS 更新方式を編集するには、その方式の編集アイコン（）をクリックします。

方式を削除するには、その方式のごみ箱アイコン（）をクリックします。

ステップ 3 ダイナミック DNS サービスのプロパティを設定します。

- [Name]：サービスの名前。
- [Web Type Update]：DDNS サービスプロバイダーでサポートされる内容に基づいて、更新するアドレスのタイプを選択します。デフォルトは [All Addresses] で、IPv4 と IPv6 の両方のすべてのアドレスが更新されます。代わりに [IPv4 Address]、[IPv4 and One IPv6 Address]、[One IPv6 Address]、または [All IPv6 Addresses] を選択すると、該当するアドレスを更新できます。

  IPv6 アドレスについては、次の点に注意してください。

  - 更新されるのはグローバルアドレスのみです。リンクローカルアドレスは更新されません。
  - Device Manager では各インターフェイスに設定できる IPv6 アドレスは 1 つだけであるため、1 つの IPv6 アドレスのみが更新されます。
- [Service Provider]：ダイナミック DNS 更新を受信して処理するサービスプロバイダーを選択します。次のサービスプロバイダーを使用できます。

- [No-IP]：No-IP DDNS サービスプロバイダー（https://www.noip.com/）。
- [Dynamic DNS]：Oracle Dynamic DNS サービスプロバイダー（https://account.dyn.com/）。
- [Google]：Google Domains サービスプロバイダー（https://domains.google.com）。
- [Custom URL]：その他の DDNS サービスプロバイダー。選択したプロバイダーに必要な URL（ユーザ名とパスワードを含む）を [Web URL] フィールドに入力する必要があります。DDNS サービスは、https://help.dyn.com/remote-access-api/ で説明されている標準に従う必要があります。

- [Username] と [Password]（[Custom URL] 以外の方式）：ダイナミック DNS 更新を送信するときに使用するユーザ名とパスワード（サービスプロバイダーのプラットフォームで定義）。

  注：

  - ユーザ名にスペースや@および:を含めることはできません。これらの文字はデリミタとして使用されます。
  - パスワードにスペースや @ を含めることはできません。この文字はデリミタとして使用されます。最初の : から @ までの間にある : は、パスワードの一部と見なされます。

- [Web URL]（[Custom URL] 方式）：サービスプロバイダーとしてカスタム URL を選択した場合、ダイナミック DNS サービスの URL を入力します。URL は次の形式にする必要があり、511 文字までに制限されます。

  http(s)://username:password@provider-domain/xyz?hostname=<h> &myip=<a>

  https://username:password@domain-provider/xyz?hostname=%3Ch%3E&myip=%3Ca%3E

- [Interfaces and Fully-Qualified Domain Name]：このサービスプロバイダーで DNS レコードを更新するインターフェイスを選択し、各インターフェイスの完全修飾ドメイン名を入力します。たとえば、interface.example.com のようになります。インターフェイスには次の制限があります。
  - 名前付きの物理インターフェイスとサブインターフェイスのみを選択できます。
  - 管理、BVI/EtherChannel またはそのメンバー、VLAN、仮想トンネルインターフェイス（VTI）のタイプのインターフェイスは選択できません。
  - 各インターフェイスは 1 つの DDNS 更新方式でのみ選択できます。同じ DDNS 更新オブジェクトでサービスプロバイダーを使用するすべてのインターフェイスを選択できます。

- [Update Interval]：ダイナミック DNS 更新を送信する頻度。デフォルトは [On Change] で、インターフェイスの IP アドレスが変更されるたびに更新が送信されます。ほかに、[Hourly]、[Daily]、または [Monthly] を選択できます。更新を毎日送信する場合は時刻を設定し、毎月送信する場合は時刻と日付を設定します。

ステップ 4 [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）サーバーは、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 サーバー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 サーバーが必要です。

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。サーバー 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 サーバー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 サーバーを試行する前に待機する秒数（1 ～ 30）。デフォルト値は 2 秒です。システムがサーバー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。

データおよび管理トラフィック用の DNS の設定

ドメイン ネーム システム（DNS）サーバーは、IP アドレスのホスト名の解決に使用されます。2 つの DNS サーバー設定があり、異なるタイプのトラフィック（データトラフィックと特別な管理トラフィック）に適用されます。データトラフィックには、アクセスコントロールルールやリモートアクセス VPN など、DNS ルックアップが必要な FQDN を使用するサービスが含ま

れます。特別な管理トラフィックには、スマートライセンスやデータベースの更新など、管理インターフェイスで発生するトラフィックが含まれます。

CLI セットアップウィザードを使用する場合、システムの初期設定で管理 DNS サーバーを設定します。Device Manager セットアップウィザードでデータおよび管理 DNS サーバーを設定することもできます。次の手順を使用して、DNS サーバーの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 サーバー通信の正しいインターフェイスを決定するために、Threat Defense はルーティングルックアップを使用しますが、どのルーティングテーブルが使用されるかは、DNS をイネーブルにするインターフェイスによって異なります。詳細については、以下のインターフェイス設定を参照してください。

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 （24 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

始める前に

- DNS サーバグループを作成していることを確認します。この説明については、DNS グループの設定 （20 ページ） を参照してください。
- Threat Defense に、DNS サーバーにアクセスするための適切なスタティックルートまたはダイナミックルートがあ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、**[システム設定（System Settings）] > [DNSサーバー（DNS Server）]** リンクをクリックします。

すでに [システム設定（System Settings）] ページを表示している場合は、コンテンツテーブルの [DNSサーバー（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) すべてのインターフェイスまたは特定のインターフェイスで DNS ルックアップを有効にします。これらの選択は、使用されるルーティングテーブルにも影響します。

インターフェイスで DNS ルックアップを有効にすることは、ルックアップの送信元インターフェイスを指定することとは異なるので注意してください。デバイスは、常にルートルックアップを使用して送信元インターフェイスを決定します。

- [すべて（ANY）]（どのインターフェースも選択しない）：すべてのインターフェイスで、DNSルックアップを有効にします。デバイスはデータルーティングテーブルのみ。
- [Managementインターフェイスまたは管理専用インターフェイス以外の選択したインターフェイス（Interfaces selected but not the Diagnostic interface or a management）]：指定したインターフェイスでDNSルックアップを有効にします。デバイスはデータルーティングテーブルのみチェックします。
- [選択したインターフェイスとManagementインターフェイスまたは管理専用インターフェイス（Interfaces selected plus the Diagnostic interface or a management-only interface）]：指定したインターフェイスで DNS ルックアップを有効にします。デバイスはデータルーティングテーブルをチェックし、ルートが見つからない場合、管理専用ルーティングテーブルにフォールバックします。
- [選択されたManagementインターフェイスまたは管理専用インターフェイス（Only the Diagnostic interface or a management-only interface selected）]：Managementインターフェイスまたは管理専用インターフェイスで DNS ルックアップを有効にします。デバイスは管理専用ルーティングテーブルのみチェックします。

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ーを定義する [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。管理DNSサーバーを更新するには、変更を展開する必要があります。

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。一部のインターフェイスで DNS を許可しない場合にのみ、インターフェイスを明示的に指定します。
- Managementインターフェイスまたは管理専用インターフェイスManagementインターフェイスを使用する場合は、そのインターフェイスのみが選択されていることを確認します。
- 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** キーワードおよび **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。

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 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、**[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）サーバーを設定する必要があります。NTP サーバー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。

Threat Defense デバイスは NTPv4 をサポートします。

（注） Firepower 4100/9300 の場合は、Device Manager を介して NTP を設定しません。FXOS で NTP を設定してください。

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）]** > **[タイムサービス（Time Services）]** リンクの順にクリックします。

[システム設定（System Settings）] ページをすでに表示している場合は、目次で [タイムサービス（Time Services）] をクリックします。

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

- **[デフォルトNTPサーバー（Default NTP Servers）]**：このオプションを選択すると、NTP に使用するサーバー名がサーバー リストに表示されます。

- **[ユーザー定義NTPサーバー（User-Defined NTP Servers）]**：このオプションを選択する場合は、使用する NTP サーバーの完全修飾ドメイン名か IPv4 または IPv6 アドレスを入力します。例、ntp1.example.com または 10.100.10.10。NTP サーバは最大 3 つまで追加できます。

ステップ 3 [保存（Save）] をクリックします。

Precision Time Protocol の設定（ISA 3000）

高精度時間プロトコル（PTP）は、パケットベース ネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。それらのデバイスクロックは、一般的に精度と安定性が異なります。このプロトコルは、産業用のネットワーク化された測定および制御システム向けに特別に設計されており、最小限の帯域幅とわずかな処理オーバーヘッドしか必要としないため、分散システムでの使用に最適です。

PTP システムは、PTP デバイスと非 PTP デバイスの組み合わせによる、分散型のネットワークシステムです。PTP デバイスには、オーディナリ クロック、境界クロック、およびトランスペアレント クロックが含まれます。非 PTP デバイスには、ネットワーク スイッチやルータなどのインフラストラクチャ デバイスが含まれます。

Threat Defense デバイスは、トランスペアレントクロックとして設定できます。Threat Defense デバイスは、自身のクロックを PTP クロックと同期しません。Threat Defense デバイスは、PTP クロックで定義されている PTP のデフォルトプロファイルを使用します。

PTP デバイスを設定するときは、連携させるデバイスのドメイン番号を定義します。したがって、複数の PTP ドメインを設定した後、1 つの特定のドメインに PTP クロックを使用するように各非 PTP デバイスを設定できます。

始める前に

デバイスが使用する PTP クロックに設定されているドメイン番号を確認します。また、システムがドメイン内の PTP クロックに到達できるインターフェイスを決定します。

以下に、PTP の設定に関するガイドラインを示します。

- この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。
- Cisco PTP は、マルチキャスト PTP メッセージのみをサポートしています。
- PTP は IPv6 ネットワークではなく、IPv4 ネットワークでのみ使用できます。
- PTP 設定は、ルーテッドかブリッジグループメンバーかを問わず、物理イーサネット データ インターフェイスでサポートされます。管理インターフェイス、サブインターフェイス、Etherchannel、ブリッジ仮想インターフェイス（BVI）、またはその他の仮想インターフェイスではサポートされません。
- VLAN サブインターフェイスでの PTP フローは、適切な PTP 設定が親インターフェイス上に存在する場合にサポートされます。

- PTP パケットが確実にデバイスを通過できるようにする必要があります。PTP トラフィックは UDP 宛先ポート 319 と 320、および宛先 IP アドレス 224.0.1.129 によって識別されます。そのため、このトラフィックを許可するアクセスコントロールルールはすべて動作します。
- ルーティングされたインターフェイス間で PTP パケットが転送される場合は、マルチキャストルーティングを有効にするとともに、各インターフェイスが 224.0.1.129 IGMP マルチキャストグループに参加する必要があります。同じブリッジグループ内のインターフェイス間で PTP パケットが転送される場合は、マルチキャストルーティングを有効にして IGMP グループを設定する必要はありません。

手順

ステップ 1 PTP クロック側インターフェイスの設定を確認します。

デフォルト設定では、すべてのインターフェイスが同じブリッジグループに配置されますが、ブリッジグループからインターフェイスを削除できます。マルチキャスト IGMP グループの場合とは異なる方法で設定する必要があるため、インターフェイスがルーテッドなのかブリッジグループメンバーなのかを決定することが重要です。

次の手順では、ブリッジグループに含まれているインターフェイスの確認方法について説明します。PTP 用に設定するインターフェイスがブリッジ グループ メンバーかどうかを確認します。

a) FDM で、**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** の [すべてのインターフェイスを表示（View All Interfaces）] をクリックします。
b) リストでインターフェイスを検索し、[モード（Mode）]列を確認します。BridgeGroupMember はブリッジ グループの一部であることを意味します。それ以外の場合はルーテッドです。

ステップ 2 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]** > **[タイムサービス（Time Services）]** リンクの順にクリックします。

[システム設定（System Settings）] ページをすでに表示している場合は、目次で [タイムサービス（Time Services）] をクリックします。

ステップ 3 PTP の設定を行います。

- [ドメイン番号（Domain Number）]: ネットワーク内の PTP デバイスに設定されているドメイン番号（0 ～ 255）。異なるドメインで受信されたパケットは、通常のマルチキャストパケットのように扱われるため、PTP 処理は行われません。
- [クロックモード（Clock Mode）] : [エンドツーエンドトランスペアレント（End To End Transparent）] を選択します。デバイスを PTP トランスペアレントクロックとしてのみ動作させることができます。

  [転送（Forward）] を選択することもできますが、これは PTP を設定しない場合と基本的に同じです。ドメイン番号は無視されます。PTP パケットは、マルチキャストトラフィックのルーティングテーブルに基づいてデバイスを通過します。これは、デフォルトの PTP 設定です。

- [インターフェイス（Interface）]：システムがネットワーク内の PTP クロックに接続できるインターフェイスをすべて選択します。PTPは、これらのインターフェイスでのみ有効になります。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 選択したインターフェイスのいずれかがルーテッドモードである場合、つまりブリッジグループメンバーではない場合は、FlexConfig を使用してマルチキャストルーティングを有効にし、ルーテッドインターフェイスを正しい IGMP グループに参加させる必要があります。

選択したすべてのインターフェイスがブリッジグループメンバーである場合は、この手順を完了しないでください。ブリッジグループメンバーでIGMPを設定しようとすると、展開に失敗します。

a) **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

b) 詳細設定の目次で **[FlexConfig]** > **[FlexConfig オブジェクト（FlexConfig Objects）]** をクリックします。

c) マルチキャストルーティングを有効にし、ルーテッドインターフェイスの IGMP 参加を設定するために、必要なオブジェクトを作成します。

次に、オブジェクトの基本テンプレートを示します。この例では、GigabitEthernet1/2 は、PTP を有効にするルーテッドインターフェイスの 1 つです。必要に応じてインターフェイスのハードウェア名を変更します。また、複数のルーテッドインターフェイスがある場合は、追加のインターフェイスごとに **interface** コマンドと **igmp** コマンドを繰り返します。

コマンド **igmp** では、224.0.1.129 IGMP グループに参加します。これは、ネットワークアドレスに関係なく、すべてのインターフェイスの正しい IP アドレスです。

```
multicast-routing
interface GigabitEthernet1/2
 igmp join-group 224.0.1.129
```

ルーテッドインターフェイスのネゲートテンプレートは、次のようになります。

```
no multicast-routing
interface GigabitEthernet1/2
 no igmp join-group 224.0.1.129
```

d) 目次の [FlexConfigポリシー（FlexConfig Policy）] をクリックして、FlexConfig ポリシーにこのオブジェクトを追加し、[保存（Save）] をクリックします。

プレビューに、オブジェクトからの期待されるコマンドが表示されていることを確認します。

次のタスク

変更を展開した後に、PTP の設定を確認できます。Device Manager CLI コンソール、または SSH またはコンソールセッションから、さまざまな **show ptp** コマンドを発行します。たとえ

ば、GigabitEthernet1/2 のみでドメイン 10 の PTP を設定している場合、出力は次のようになります。

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/4
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 4
  PTP version: 2
  Port state: Disabled
```

管理接続用 HTTP プロキシの設定

システムとインターネットの間に直接接続がない場合は、管理インターフェイスのHTTPプロキシを設定できます。システムは、Device Manager への接続やデータベース更新をダウンロードするためのシステムからシスコへの接続など、すべての管理接続にプロキシを使用します。

また、Threat Defense CLI で **configure network http-proxy** コマンドを使用して、HTTP プロキシを設定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、**[システム設定（System Settings）]** > **[HTTPプロキシ（HTTP Proxy）]** リンクをクリックします。

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 [HTTPプロキシ（HTTP Proxy）] をクリックします。

ステップ 2 トグルをクリックしてプロキシを有効にしてから、プロキシ設定を指定します。

- [HTTPプロキシ（HTTP proxy）]：プロキシサーバーの IP アドレス。
- [Port（ポート）]：HTTP接続をリッスンするためにプロキシサーバーに設定するポート番号。
- [プロキシ認証を使用（Use Proxy Authentication）]：プロキシ接続に認証を要求するようサーバーが設定されている場合は、このオプションを選択します。このオプションを選択した場合は、プロキシサーバーにログインできるアカウントの[ユーザー名（Username）]と [パスワード（Password）] も入力します。

ステップ 3 [保存（Save）] をクリックし、変更を確定します。

変更はすぐに適用されます。展開ジョブは必要ありません。

システムの管理接続完了方法を変更しようとしているため、Device Manager への接続が失われます。変更が完了するまで数分待って、ブラウザウィンドウを更新してからもう一度ログインしてください。

クラウド サービスの設定

クラウドサービスに登録すると、CDO、Cisco Threat Response、Cisco Success Network など、さまざまなクラウドベースのアプリケーションを使用できます。

クラウドに登録すると、ページには登録ステータスとテナンシーのタイプ、およびデバイス登録で使用されたアカウント名が表示されます。

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。

デバイスが登録されていない場合、このページに Cisco Cloud に登録するための登録方法が表示されます。クラウドに登録すると、個々のクラウドサービスを有効または無効にできます。

ステップ 2 （評価モードのとき、またはクラウドサービスからの登録解除後に）Cisco Cloud に登録するには、次のいずれかのオプションを選択します。

- [セキュリティ/CDOアカウント（Security/CDO Account）]：次のいずれかの方法を使用できます。
  - [Cisco Defense Orchestratorのテナンシーへの自動登録（Auto-enroll with Tenancy from Cisco Defense Orchestrator）]（Firepower 1000、2100、Cisco Secure Firewall 3100 のみ）。登録キーを取得する代わりに、自動登録を使用できます。最初に CDO に移動し、デ

バイスのシリアル番号を使用してデバイスを追加します。次に、Device Manager でこのチェックボックスをオンにして登録を開始します。デバイスのシャーシまたは梱包明細からシリアル番号を取得します。FXOS の場合は、FXOS CLI に移動して **show chassis detail** コマンドを実行することにより、シリアル番号（SN）というラベルが付いた正しいシリアル番号が表示されます。Threat Defense コマンドの **show serial-number** では異なるシリアル番号が表示されることに注意してください。これは CDO 登録には推奨されません。この方式は、CDO のレガシー デバイス マネージャ モードだけでなく、CDO のクラウド提供型 Management Center でも機能します。

（注） デバイスマネージャモードは、このモードを使用して Threat Defense をすでに管理している既存のユーザーのみが使用できます。

- CDO またはその他のセキュリティアカウントにログインし、登録キーを生成します。このページに戻り、[クラウドサービスのリージョン（Cloud Services Region）] を選択して、[登録キー（Registration Key）] に貼り付けます。この方式は、CDO のレガシー デバイス マネージャ モードでのみ機能します。CDO のクラウド提供型の管理センターについては、Device Manager から Management Center、または CDO への切り替え（38 ページ）を参照してください。

  （注） デバイスマネージャモードは、このモードを使用して Threat Defense をすでに管理している既存のユーザーのみが使用できます。

  この時点で、**Cisco Defense Orchestrator** と **Cisco Success Network** を有効にすることもできます。これらはデフォルトで有効になっています。

- [スマートライセンス（Smart License）]：（CDO を使用しない場合のみ）リンクをクリックして [スマートライセンシング（Smart Licensing）] ページに移動し、CSSM に登録します。CSSM に登録すると、デバイスがクラウドサービスにも登録されます。

  （注） クラウドサービスから登録解除した場合、スマートライセンスの登録アプローチではいくつかの追加手順が必要です。この場合、[クラウドサービスのリージョン（Cloud Services Region）] を選択してから [登録（Register）] をクリックします。開示内容を読み、[承認（Accept）] をクリックします。

ステップ 3 クラウドサービスに登録したら、必要に応じて機能を有効または無効にできます。次のトピックを参照してください。

- CDO の有効化または無効化（レガシー デバイス マネージャ モード） （33 ページ）
- Cisco Success Network への接続 （33 ページ）
- Cisco Cloud へのイベントの送信 （35 ページ）
- クラウドサービスの登録解除 （36 ページ）

CDO の有効化または無効化（レガシー デバイス マネージャ モード）

（注） このセクションは、クラウド提供型の管理センターではなく、CDO のレガシー デバイス マネージャ モードにのみ適用されます。

クラウド サービスの設定 （31 ページ） の推奨に従い、CDO の登録キーを使用してクラウド サービスに登録した場合、デバイスはすでに CDO に登録されています。その後、必要に応じて接続を無効にしたり、再度有効にしたりできます。

デバイスがスマートライセンスを使用してクラウドサービスに登録されている場合、CDO を有効にすると問題が発生します。デバイスは CDO インベントリに表示されません。最初にクラウドサービスからデバイスの登録を解除しておくことを強くお勧めします。歯車（⚙）ドロップダウンリストから [クラウドサービスの登録解除（Unregister Cloud Services）] を選択します。登録解除後、「クラウド サービスの設定 （31 ページ）」で説明されているとおりに、CDO から登録トークンを取得し、トークンとセキュリティアカウントを使用して再登録します。

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

始める前に

高可用性を設定する予定の場合、高可用性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、CDO 機能の [有効化（Enable）]/[無効化（Disable）] ボタンをクリックして設定を変更します。

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、デバイスが Cisco Cloud へのセキュアな接続を確立し、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なります。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、クラウドサービスの登録解除（36 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 にデバイスを登録し、登録中に [Cisco Success Network] オプションを選択するか、または登録キーを入力して CDO に登録します（CDO のレガシーデバイス マネージャ モードのみ）。

（注） 高可用性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 Cloud へのイベントの送信

Cisco Cloud サーバーにイベントを送信できます。このサーバーから、各種のシスコ クラウド サービスがイベントにアクセスできます。次に、クラウドアプリケーションを使用して、イベントを分析したり、デバイスが遭遇した可能性のある脅威を評価したりできます。

クラウドツールは、送信したイベントを使用するかどうかを決定します。ツールのマニュアルを参照するかイベントデータを調べ、未使用のイベントをクラウドに送信して帯域幅とストレージ領域の両方を無駄にしていないことを確認します。ツールは同じソースからイベントを取り込むため、最も制限の厳しいツールだけでなく、使用するすべてのツールを選択する必要があります。次に例を示します。

- CDO のセキュリティ分析およびロギングツールは、すべての接続イベントを使用できます。
- Threat Response は優先順位の高い接続イベントのみを使用するため、すべての接続イベントをクラウドに送信する必要がありません。またこれは、セキュリティインテリジェンスの優先順位の高いイベントのみを使用します。

始める前に

このサービスを有効にするには、事前にクラウドサービスにデバイスを登録する必要があります。

米国地域では https://visibility.amp.cisco.com/ で、EU 地域では https://visibility.eu.amp.cisco.com で、APJC 地域では https://visibility.apjc.amp.cisco.com で、Threat Response に接続できます。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）。詳細については、https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html にある『*Cisco Secure Firewall Threat Defense and SecureX Threat Response Integration guide*』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 Cloudにイベントを送信（Send Events to the Cisco Cloud）]** オプションの [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。

ステップ 3 サービスを有効にすると、クラウドに送信するイベントを選択するように求められます。後で、選択したイベントのリストの横にある [編集（Edit）] をクリックして、これらの選択を変更できます。送信するイベントのタイプを選択し、[OK] をクリックします。

- [ファイル/マルウェア（File/Malware）]：任意のアクセスコントロールルールで適用した任意のファイルポリシー用。

- [侵入（Intrusion）]：任意のアクセスコントロールルールで適用した任意の侵入ポリシー用。
- [接続（Connection）]：ロギングを有効にしたアクセスコントロールルール用。このオプションを選択すると、すべての接続イベントを送信するか、優先度の高い接続イベントのみを送信するかを選択することも可能です。優先度の高い接続イベントとは、侵入、ファイル、またはマルウェアイベントをトリガーする接続、またはセキュリティインテリジェンス ブロッキング ポリシーに一致する接続に関連するイベントです。

クラウドサービスの登録解除

クラウドサービスを使用しなくなった場合は、クラウドからそのデバイスの登録を解除できます。デバイスをサービスから削除する場合、またはサービスの使用を停止する場合、登録を解除する必要があります。クラウドサービスのリージョンを変更する必要がある場合は、登録を解除してから、再登録時に新しいリージョンを選択します。

この手順を使用してクラウドから登録を解除しても、スマートライセンシングの登録には影響しません。

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 歯車（⚙）のドロップダウンリストから、[クラウドサービスの登録解除（Unregister Cloud Services）] を選択します。

ステップ 3 警告を確認してから、[登録解除（Unregister）] をクリックします。

有効にしたクラウドサービスは自動的に無効になり、それらを再度有効にすることはできなくなります。ただし、クラウドに登録するためのコントロールが表示されるため、再登録は可能です。

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、**[システム設定（System Settings）]** > **[Web分析（Web Analytics）]** リンクをクリックします。

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 [Web分析（Web Analytics）] 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。

URL フィルタリングの設定

システムは Cisco Collective Security Intelligence（csi）（Cisco Talos Intelligence Group（Talos））から URL カテゴリおよびレピュテーションデータベースを取得します。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。
- [URLクエリソース（URL Query Source）]：URL のカテゴリとレピュテーションを取得するためにクエリを実行するソース。
  - [ローカルデータベースのみ（Local Database Only）]：ローカル URL フィルタリングデータベースでのみカテゴリとレピュテーションを検索します。一致するものがない

場合、URLはレピュテーションなしの未分類になります。この方式は、特にローエンドシステムにおいてストレージが限られているためにURLフィルタリングデータベースが小さい場合には、限定的なものになる可能性があります。

- [ローカルデータベースおよびCisco Cloud（Local Database and Cisco Cloud）]：これは推奨されるオプションです。ローカルデータベースに一致するものがない場合、更新されたカテゴリ/レピュテーション情報に関して Cisco Cloud に対するクエリが実行されます。規定された時間内に応答が受信された場合は、それが照合に使用されます。それ以外の場合、および一致するものがない場合、URLはレピュテーションなしの未分類になります。
- [Cisco Cloudのみ（Cisco Cloud Only）]：カテゴリおよびレピュテーション情報に関して、常に、Cisco Cloud に対するクエリが実行されます。ローカル URL データベースは使用されません。

- [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 必要に応じて、**URL のカテゴリを確認**できます。

特定の URL のカテゴリとレピュテーションを確認できます。[確認するURL（URL to Check）] ボックスに URL を入力し、[移動（Go）] をクリックします。結果を表示するには、外部の Webサイトに移動します。分類に同意しない場合は、[URLカテゴリの異議を送信する（Submit a URL Category Dispute）] リンクをクリックしてお知らせください。

ステップ 4 [保存（Save）] をクリックします。

Device Manager から Management Center、または CDO への切り替え

Device Manager から切り替える場合は、Threat Defense デバイスを Management Center または CDO に接続するように設定して管理できます。

（注） CDOは、クラウド提供型の管理センターを使用してThreat Defense デバイスを管理できます。CDOの簡素化されたデバイスマネージャ機能は、このモードでThreat Defense をすでに管理している既存のユーザーのみが使用できます。この手順は、クラウド提供型の管理センターにのみ適用されます。

Device Manager を使用して Management Center/CDO セットアップを実行すると、管理インターフェイスおよびマネージャ アクセス インターフェイスの設定に加えて、管理のために Management Center/CDO に切り替えたときに、Device Manager で完了したすべてのインターフェイス構成が保持されます。アクセス コントロール ポリシーやセキュリティゾーンなどの他のデフォルト設定は保持されないことに注意してください。Management Center/CDO の初期設定に Threat Defense CLI を使用する場合、管理インターフェイスとマネージャアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス設定は保持されません）。

Management Center/CDO に切り替えると、Device Manager を使用して Threat Defense デバイスを管理できなくなります。

始める前に

ファイアウォールが高可用性用に設定されている場合は、まず、Device Manager （可能な場合）または **configure high-availability disable** コマンドを使用して、高可用性設定を中断する必要があります。アクティブなユニットから高可用性を中断することをお勧めします

手順

ステップ 1 Cisco Smart Software Manager にファイアウォールを登録した場合は、マネージャを切り替える前に登録を解除する必要があります。デバイスの登録解除を参照してください。

ファイアウォールを登録解除すると、基本ライセンスとすべての機能ライセンスが解放されます。ファイアウォールを登録解除しないと、それらのライセンスは Cisco Smart Software Manager のファイアウォールに割り当てられたままになります。

ステップ 2 （必要に応じて）管理インターフェイスを設定します。管理インターフェイスの設定を参照してください。

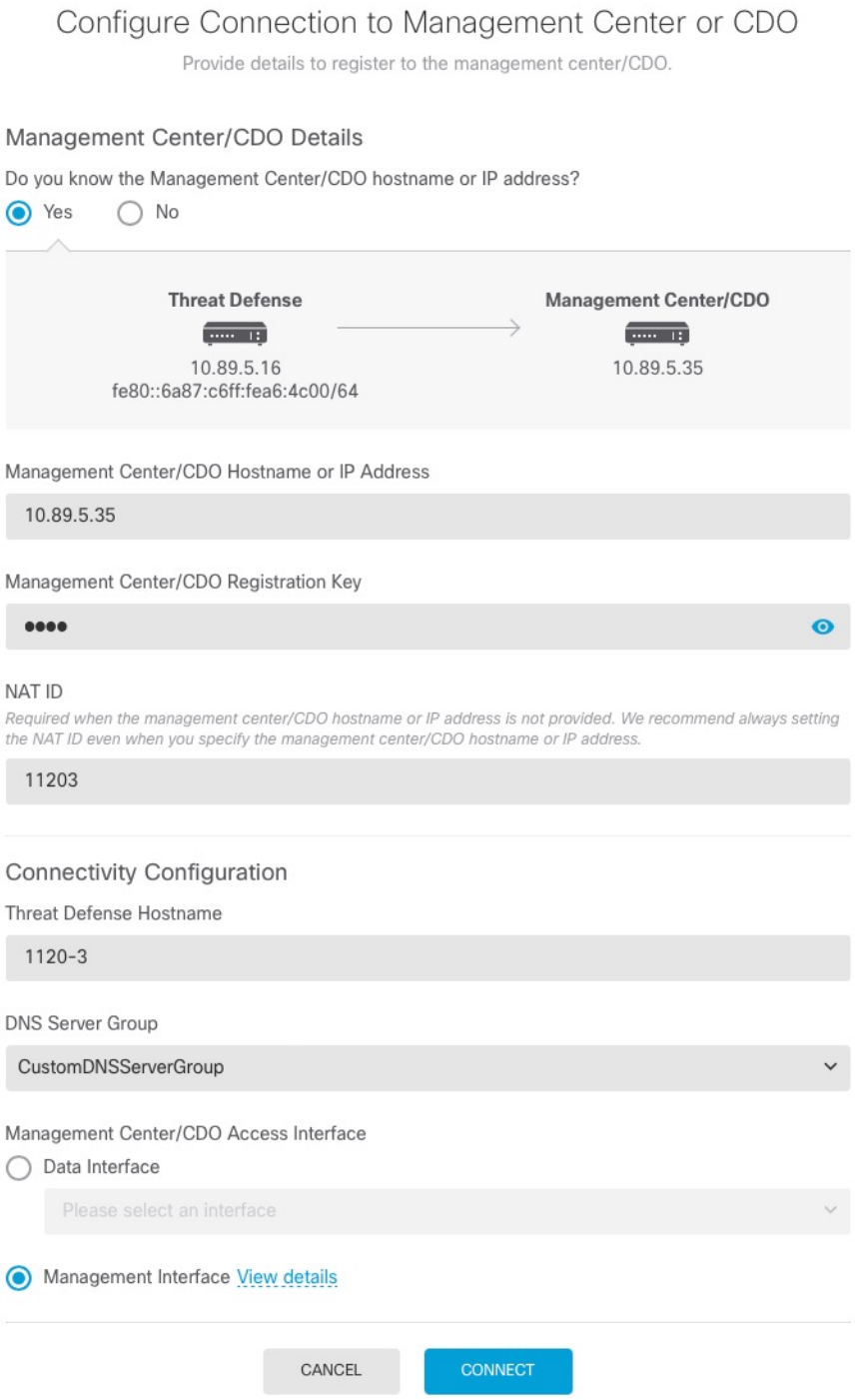
マネージャアクセスにデータインターフェイスを使用する場合でも、管理インターフェイスの設定を変更する必要がある場合があります。Device Manager 接続に管理インターフェイスを使用していた場合は、Device Manager に再接続する必要があります。

- マネージャアクセス用のデータインターフェイス：管理インターフェイスには、データインターフェイスに設定されたゲートウェイが必要です。デフォルトでは、管理インターフェイスは DHCP から IP アドレスとゲートウェイを受信します。DHCP からゲートウェイを受信しない場合（たとえば、管理インターフェイスをネットワークに接続していない場合）、ゲートウェイはデフォルトでデータインターフェイスになり、何も設定する必要はありません。DHCP からゲートウェイを受信した場合は、代わりに管理インターフェイスに静的 IP アドレスを設定し、ゲートウェイをデータインターフェイスに設定する必要があります。
- マネージャアクセス用の管理インターフェイス：静的 IP アドレスを設定する場合は、デフォルトゲートウェイもデータインターフェイスではなく一意のゲートウェイに設定してください。DHCP を使用する場合は、DHCP からゲートウェイを正常に取得できると仮定して、何も設定する必要はありません。

ステップ 3 **[デバイス（Device）] > [システム設定（Device System Settings）] > [中央管理（Central Management）]** の順に選択し、[続行（Proceed）] をクリックして Management Center/CDO の管理を設定します。

ステップ 4 **[Management Center/CDOの詳細（Management Center/CDO Details）]** を設定します。

図 *1 : Management Center/CDO* の詳細



a) **[Management Center/CDOのホスト名またはIPアドレスを知っていますか（Do you know the FMC hostname or IP address）]** で、IP アドレスまたはホスト名を使用して Management Center/CDO に到達できる場合は [はい（Yes）] をクリックし、Management Center/CDO が NAT の背後にあるか、パブリック IP アドレスまたはホスト名がない場合は[いいえ（No）] をクリックします。

双方向の TLS-1.3 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくても 1 台以上のデバイス（Management Center/CDO または Threat Defense デバイス）に到達可能な IP アドレスが必要です。

b) [はい（Yes）] を選択した場合は、**管理センター/CDO のホスト名/IP アドレス**を入力します。

c) **Management Center/CDO 登録キー**を指定します。

このキーは、Threat Defense デバイスを登録するときに Management Center/CDO でも指定する任意の 1 回限りの登録キーです。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Management Center/CDO に登録する複数のデバイスに使用できます。

d) [NAT ID] を指定します。

この ID は、Management Center/CDO でも指定する任意の 1 回限りの文字列です。いずれかのデバイスの IP アドレスのみを指定する場合、このフィールドは必須です。両方のデバイスの IP アドレスがわかっている場合でも、NAT ID を指定することを推奨します。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Management Center/CDO に登録する他のデバイスには使用できません。NAT ID は、正しいデバイスからの接続であることを確認するために IP アドレスと組み合わせて使用されます。 IP アドレス/NAT ID の認証後にのみ、登録キーがチェックされます。

ステップ 5 [接続の設定（Connectivity Configuration）] を設定します。

a) [FTDホスト名（FTD Hostname）] を指定します。

Management Center/CDO アクセスインターフェイスのアクセスにデータインターフェイスを使用する場合、この FQDN がこのインターフェイスに使用されます。

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

既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは **CiscoUmbrellaDNSServerGroup** と呼ばれ、OpenDNS サーバーが含まれます。

Management Center/CDO アクセスインターフェイスにデータインターフェイスを選択する場合は、この設定でデータインターフェイス DNS サーバーを設定します。セットアップウィザードで設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。管理トラフィックとデータトラフィックの両方が外部インターフェイス経由で DNS サーバーに到達するため、管理に使用したものと同じ DNS サーバーグループを選択する可能性があります。

Management Center/CDO では、この Threat Defense デバイスに割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center/CDO に Threat Defense デバイスを追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Threat Defense デバイスに後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Management Center/CDO と Threat Defense デバイスを同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center/CDO で保持されます。

Management Center/CDO アクセスインターフェイスに管理インターフェイスを選択する場合は、この設定で管理 DNS サーバーを構成します。

c) **Management Center/CDO アクセスインターフェイス**については、任意の構成済みインターフェイスを選択してください。

管理インターフェイスは、Threat Defense デバイスを Management Center/CDO に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。

ステップ 6 （任意）外部インターフェイスではないデータインターフェイスを選択した場合は、デフォルトルートを追加します。

インターフェイスを通過するデフォルトルートがあることを確認するように求めるメッセージが表示されます。外部を選択した場合は、セットアップウィザードの一環としてこのルートがすでに設定されています。別のインターフェイスを選択した場合は、Management Center/CDO に接続する前にデフォルトルートを手動で設定する必要があります。スタティックルートの設定の詳細については、「スタティック ルートの設定」を参照してください。

管理インターフェイスを選択した場合は、この画面に進む前に、ゲートウェイを一意のゲートウェイとして設定する必要があります。 管理インターフェイスの設定を参照してください。

ステップ 7 （任意） データインターフェイスを選択した場合は、[ダイナミックDNS（DDNS）方式の追加（Add a Dynamic DNS (DDNS) method）] をクリックします。

DDNS は、 IP アドレスが変更された場合に Management Center/CDO が完全修飾ドメイン名（FQDN）で Threat Defense デバイスに到達できるようにします。[デバイス（Device）] > [システム設定（System Settings）] > [DDNSサービス（DDNS Service）] を参照して DDNS を設定します。

Management Center/CDO に Threat Defense デバイスを追加する前に DDNS を設定すると、Threat Defense デバイスは、Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加し、Threat Defense デバイスが HTTPS 接続のために DDNS サーバー証明書を検証できるようにします。 Threat Defense は、DynDNS リモート API 仕様（https://help.dyn.com/remote-access-api/）を使用するすべての DDNS サーバーをサポートします。

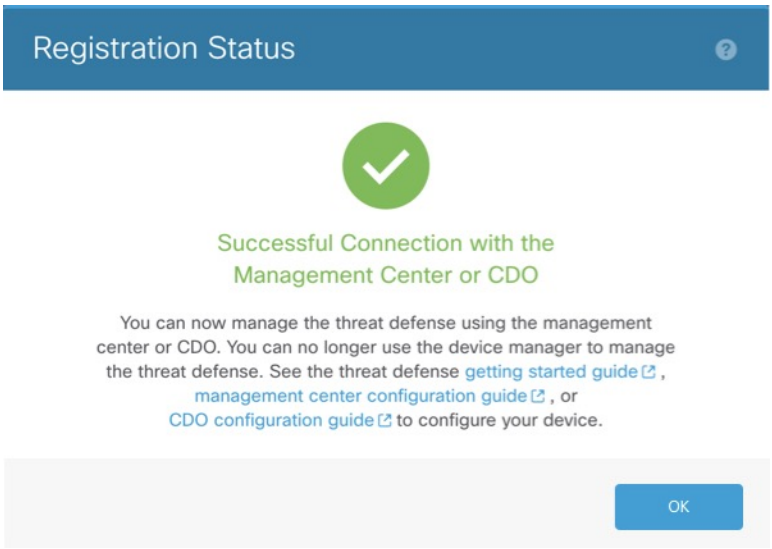
マネージャアクセスに管理インターフェイスを使用する場合、DDNSはサポートされません。

ステップ 8 [接続（Connect）] をクリックします。**[登録ステータス（Registration Status）]** ダイアログボックスには、Management Center/CDO への切り替えに関する現在のステータスが表示されます。**[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）]** のステップの後、Management Center/CDO に移動してファイアウォールを追加します。

Management Center/CDO への切り替えをキャンセルする場合は、[登録のキャンセル（Cancel Registration）] をクリックします。キャンセルしない場合は、**[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）]** のステップが完了するまで Device Manager のブラウザウィンドウを閉じないでください。閉じた場合、プロセスは一時停止し、Device Manager に再接続した場合のみ再開されます。

[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）] のステップの後に Device Manager に接続したままにする場合、その後 **[Management CenterまたはCDOとの正常接続（Successful Connection with Management Center or CDO）]** ダイアログボックスが表示され、Device Manager から切断されます。

図 *2 :* 正常接続



Management Center または CDO から Device Manager に切り替える

代わりにDevice Managerを使用するように、オンプレミスまたはクラウド提供型のManagement Centerによって現在管理されている Threat Defense デバイスを設定できます。

ソフトウェアを再インストールすることなく、Management CenterからDevice Managerに切り替えることができます。Management CenterからDevice Managerに切り替える前に、Device Managerがすべての設定要件を満たしていることを確認します。Device Manager から Management Center

に切り替える場合は、Device Manager から Management Center、または CDO への切り替え （38 ページ） を参照してください。

注意 Device Manager に切り替えると、デバイスの設定は削除され、システムはデフォルト設定に戻ります。ただし、管理 IP アドレスとホスト名は維持されます。

手順

ステップ 1 Management Center で、[デバイス（Devices）] > [デバイス管理（Device Management）] ページからファイアウォールを削除します。

ステップ 2 SSH またはコンソールポートを使用して、Threat Defense CLI に接続します。SSH の場合、管理 IP アドレスへの接続を開き、admin ユーザー名（または管理者権限を持つ他のユーザー）で Threat Defense CLI にログインします。

（Firepower モデル）コンソールポートはデフォルトで FXOS CLI になります。**connect ftd** コマンドを使用して、Threat Defense CLI に接続します。SSH セッションは Threat Defense CLI に直接接続します。

管理 IP アドレスに接続できない場合は、次のいずれかを実行します。

- 管理物理ポートが、機能しているネットワークに接続されていることを確認します。
- 管理ネットワークに管理 IP アドレスとゲートウェイが設定されていることを確認します。**configure network ipv4/ipv6 manual** コマンドを使用します。

ステップ 3 現在リモート管理モードになっていることを確認します。

show managers

例：

```
> show managers
Type                    : Manager
Host                    : 10.89.5.35
Display name            : 10.89.5.35
Identifier              : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration            : Completed
```

ステップ 4 リモート マネージャを削除すると、マネージャなしのモードになります。

configure manager delete *uuid*

リモート管理からローカル管理に直接移行することはできません。複数のマネージャが定義されている場合は、識別子（UUID とも呼ばれます。**show managers** コマンドを参照）を指定する必要があります。各マネージャ エントリを個別に削除します。

例：

```
> configure manager delete
```

```
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

ステップ 5 ローカル マネージャを設定します。

configure manager local

これで、Web ブラウザで **https://***management-IP-address* にアクセスしてローカル マネージャを開くことができるようになりました。

例：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

TLS/SSL 暗号設定の設定

SSL 暗号設定は、デバイスへの TLS/SSL 接続に許可される TLS バージョンと暗号化暗号スイートを制御します。具体的には、これらの設定は、リモートアクセス VPN 接続を確立するときにクライアントが使用できる暗号を制御します。

通常、設定する暗号スイートには、使用可能な複数の暗号化暗号スイートが必要です。システムは、クライアントと Threat Defense デバイスの両方がサポートする最高の TLS バージョンを決定し、その TLS バージョンと互換性のある両方をサポートする暗号スイートを選択します。システムは、両方のエンドポイントでサポートされている最も強力な TLS バージョンと暗号スイートを選択して、許可する暗号の中で最も安全な接続を確保します。

始める前に

デフォルトでは、システムは DefaultSSLCipher オブジェクトを使用して、許可される暗号スイートを定義します。このオブジェクトに含まれる暗号は、スマート ライセンス アカウントが輸出規制機能に対して有効になっているかどうかによって異なります。このデフォルトでは、できるだけ多くのクライアントが接続を完了できるように、低セキュリティ レベルが設定されます。デフォルトの Diffie-Hellman グループもあります。これらの設定は、デフォルトが要件に適合しない場合にのみ設定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）] > [SSL設定（SSL Settings）]** リンクの順にクリックします。

ステップ 2 次のオプションを設定します。

- [暗号（Ciphers）]：許可されるTLSバージョンと暗号化アルゴリズムを定義するSSL暗号オブジェクトを選択します。DefaultSSLCipher オブジェクトでは、低セキュリティレベルが設定されます。このオブジェクトをCiscoRecommendedCipher、または独自のカスタム暗号オブジェクトに置き換えて、より高い要件を実装します。理想的には、すべておよび許可する TLS バージョンと暗号のみを含む単一のオブジェクトを作成します。

  オブジェクトを今すぐ作成する必要がある場合は、リストの下部にある [新しい暗号の作成（Create New Cipher）] をクリックします。

- [一時的なDiffie-Hellmanグループ（Ephemeral Diffie-Hellman Group）]：一時的な暗号化アルゴリズムに使用する DH グループ。DH グループの説明については、使用する Diffie-Hellman 係数グループの決定を参照してください。デフォルトは 14 です。

- [楕円曲線DHグループ（Elliptical Curve DH Group）]：楕円曲線暗号化アルゴリズムに使用する DH グループ。デフォルトは 19 です。

ステップ 3 [保存（Save）] をクリックします。

TLS/SSL 暗号オブジェクトの設定

SSL 暗号オブジェクトでは、Threat Defense デバイスへの SSL 接続を確立するときに使用できるセキュリティレベル、TLS/DTLS プロトコルバージョン、および暗号化アルゴリズムの組み合わせを定義します。ボックスへのSSL接続を確立するユーザーのセキュリティ要件を定義するには、**[デバイス（Device）] > [システム設定（System Settings）] > [SSL設定（SSL Settings）]** で次のオブジェクトを使用します。

選択できる TLS のバージョンと暗号は、スマート ライセンス アカウントによって制御されます。輸出コンプライアンス要件を満たしている場合は、オプションの任意の組み合わせを選択できます。ライセンスが輸出要件に準拠していない場合は、TLSv1.0 および DES-CDC-SHA に制限されます。これらは最も低いセキュリティオプションです。評価モードは非準拠モードと見なされるため、システムのライセンスを取得するまではオプションが制限されます。

システムには、事前定義されたオブジェクトがいくつか含まれています。事前定義されたオブジェクトがセキュリティ要件に適合しない場合にのみ、新しいオブジェクトを作成する必要があります。オブジェクトは次のとおりです。

- DefaultSSLCipher：これは低セキュリティレベルのグループです。これは、できるだけ多くのクライアントがシステムへの接続を完了できるようにするために、SSL設定で使用されるデフォルトです。システムでサポートされるすべてのプロトコルバージョンと暗号が含まれます。

- CiscoRecommendedCipher：これは、最も安全な暗号と TLS バージョンのみを含む、高セキュリティレベルのグループです。このグループは最高のセキュリティを提供しますが、各クライアントが一致する暗号を使用できるようにする必要があります。暗号の不一致の問題によって、一部のクライアントが接続を完了できない可能性が高くなります。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [SSL暗号（SSL Ciphers）] 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（trash can）] アイコン（）をクリックします。

ステップ 3 オブジェクトの名前を入力し、任意で説明を入力します。

ステップ 4 次のオプションを設定します。

- [セキュリティレベル（Security Level）]：オブジェクトの相対的なセキュリティレベル。セキュリティレベルを選択した後にプロトコルバージョンまたは暗号スイートリストを編集すると、オブジェクトによって提供される実際のセキュリティレベルが選択したセキュリティレベルと一致しない場合があることに注意してください。次のいずれかを実行します。
  - [すべて（All）]：低セキュリティから高セキュリティまで、すべての TLS レベルと暗号スイートをオブジェクトに含めます。
  - [低（Low）]：すべての TLS バージョンと暗号が含まれます。この場合、ユーザーは最も安全性の低い暗号で接続を完了できます。非輸出準拠ライセンスの場合は、TLSv1.0 および DES-CBC-SHA が含まれます。
  - [中（Medium）]：すべての TLS バージョンが含まれますが、一部の比較的安全でない暗号は削除されます。このオプションと [低（Low）] および [すべて（All）] オプションの違いはごくわずかです。このオプションは、非輸出準拠ライセンスでは使用できません。
  - [高（High）]：最新の DTLS および TLS バージョンのみ、およびこれらのバージョンで動作する暗号を許可します。このオプションは、現在使用可能な最も安全な暗号に接続を制限します。このオプションは、非輸出準拠ライセンスでは使用できません。
  - [カスタム（Custom）]：TLS バージョンと暗号を個別に選択する場合は、このオプションを選択します。選択するオプションによって、定義するセキュリティ暗号化設定の高低が決まります。カスタムオブジェクトにはデフォルトはありませんが、[カスタム（Custom）] を選択する前に別のレベルを選択した場合は、前に表示されたオプションが選択したままになります。

- [プロトコルバージョン（Protocol Versions）]：クライアントが Threat Defense デバイスへの TLS/SSL 接続を確立するときに使用できる TLS/DTLS バージョン。カスタムオブジェクトの場合は、サポートするバージョンを選択します。他のセキュリティレベルの場合は、リストを編集しないことが理想的ですが、必要に応じてバージョンを追加または削除できます。
- [使用可能な暗号スイート（Applicable Cipher Suites）]：クライアントが使用できる暗号化アルゴリズム。新しいスイートを追加する場合は [+] をクリックします。スイートを削除する場合はそのスイートの [x] をクリックします。

  選択したプロトコルバージョンによって、このリストで使用可能なスイートが制御されます。プロトコルバージョンを変更すると、選択したバージョンで動作しなくなった選択済みのスイートにフラグが付けられます。それらのスイートは削除するか、必要なプロトコルバージョンを再度追加する必要があります。

ステップ 5 [OK] をクリックします。

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。