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 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 [管理アクセスリスト（Management Access List）][管理アクセス（Management Access）] をクリックします。

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。

診断ロギングの設定

診断ロギングは、接続に関係していないイベントの 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。次の手順では、診断メッセージのロギングの設定方法について説明します。

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）] > [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 **[診断ログの設定（Diagnostic Log Settings）] > [オン（On）]** をクリックします。

このページの残りのフィールドを設定しても、この設定を有効にしなければ診断ログ メッセージは生成されません。

ステップ 3 診断ログ メッセージを確認したい各場所のスライダを [オン（On）] に切り替えて、最低の重大度レベルを選択します。

メッセージは次の場所に記録できます。

- [コンソール（Console）]：メッセージは、コンソール ポートの CLI にログインすると表示されます。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。
- [Syslog]：メッセージは、指定する外部の syslog サーバに送信されます。[+] をクリックして syslog サーバ オブジェクトを選択し、ポップアップ ダイアログボックスで [OK] をクリックします。サーバのオブジェクトがまだ存在していない場合は、[Syslogサーバの追加（Add Syslog Server）] をクリックして作成します。

ステップ 4 [保存（Save）] をクリックします。

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。

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、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。これらのサーバは管理インターフェイスによって使用されます。DNS サーバは初期システム設定の際に設定しますが、次のプロシージャを使用して設定を変更できます。

configure network dns servers および **configure network dns searchdomains** コマンドを使用して、CLI で DNS の設定を変更することもできます。

DNS解決に関する問題が発生した場合は、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）]** > **[DNSサーバ（DNS Server）]** 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 [DNSサーバ（DNS Server）] をクリックします。

ステップ 2 [プライマリ、セカンダリ、ターシャリDNS IPアドレス（Primary, Secondary, Tertiary DNS IP address）] に、DNS サーバの IP アドレスを優先順位に従って 3 つまで入力します。

使用していたプライマリ DNS サーバからの応答がなくなると、セカンダリが使用され、最後にターシャリが使用されます。

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。

ステップ 3 [ドメイン検索名（Domain Search Name）] に、example.com などのネットワークのドメイン名を入力します。

このドメインは、完全修飾されていないホスト名に追加されます（たとえばserverA.example.comではなく serverA のようなホスト名）。

ステップ 4 [保存（Save）] をクリックします。

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、管理アドレスは静的であり、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 は除く）。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、**[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。

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、**[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。

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。

ページの上部にある [クラウドサービスポータル (Cloud Services Portal）] リンクをクリックして、[シスコ クラウドサービス（Cisco Cloud Services）] 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 の登録キーを取得します。

デバイスを Cisco Smart Software Manager（CSSM）にすでに登録している場合は、最初に [スマートライセンシング（Smart Licensing）] ページからデバイスを登録解除することを強く推奨します。トークンを使用して Cisco Defense Orchestrator を有効にした後で再登録できます。

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。

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。

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。

この接続は、Cisco Success Network および Cisco Defense Orchestrator の両方を無効にすることで、いつでもオフにできます。両方を無効にすると、デバイスがクラウドから切断されます。切断しても更新の受信やスマートライセンス機能の操作には影響せず、正常に動作を継続します。

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。

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。