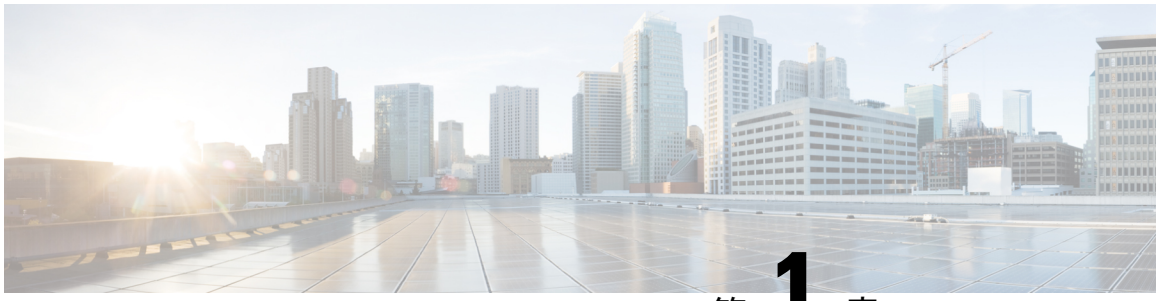
ESXi 上の Cisco DNA Center 2.3.7.3 管理者ガイド

初版：2023 年 10 月 30 日

最終更新：2024 年 2 月 29 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

システム設定の構成

システム設定について

Cisco DNA Center の使用を開始するには、最初にシステム設定を構成して、サーバーがネットワークの外部と通信し、セキュアな通信の確保やユーザーの認証といった主要なタスクを実行できるようにする必要があります。システム設定を構成するには、この章で説明されている手順を使用します。

（注）

- プロキシサーバー設定の変更など、Cisco DNA Center の構成を変更する場合、すべて Cisco DNA Center GUI で実行する必要があります。
- IP アドレス、静的ルート、DNS サーバー、または **maglev** ユーザーパスワードの変更は、CLI から `sudo maglev-config update` コマンドを使用して実行する必要があります。
- デフォルトでは、Cisco DNA Center システムのタイムゾーンは UTC に設定されています。Cisco DNA Center の GUI はブラウザのタイムゾーンで動作するため、設定でこのタイムゾーンを変更しないでください。

ユーザープロファイルの役割および権限

Cisco DNA Center は、ロールベース アクセス コントロール（RBAC）をサポートします。ユーザープロファイルに割り当てられたロールは、ユーザーが実行する権限を持つ機能を定義します。Cisco DNA Center には、次の 3 つの主要なデフォルトユーザーロールがあります。

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE

• OBSERVER-ROLE

SUPER-ADMIN-ROLE は、ユーザーに幅広い機能を提供し、カスタムロールの作成やユーザープロファイルへの割り当てなど、Cisco DNA Center GUI ですべてのアクションを実行できるようにします。NETWORK-ADMIN-ROLE と OBSERVER-ROLE は、Cisco DNA Center GUI での機能が制限されます。

Cisco DNA Center でアクションを実行できない場合、それを許可しないロールがユーザープロファイルに割り当てられていることが原因である可能性があります。詳細については、システム管理者に確認するか、または*Cisco DNA Center* 管理者ガイドを参照してください。

システム 360 の使用

[System 360] タブには、Cisco DNA Center に関する一目でわかる情報が表示されます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[System 360]** の順に選択します。

ステップ 2 [System 360] ダッシュボードで、表示される次のデータメトリックを確認します。

[Cluster]

- [Hosts]：Cisco DNA Center ホストに関する情報を表示します。表示される情報には、ホストの IP アドレスと、ホストで実行されているサービスに関する詳細なデータが含まれます。ホストで実行されているサービスに関する詳細なデータを表示するには、[View Services] リンクをクリックします。

  （注） ホスト IP アドレスの横には、カラーバッジが付きます。緑色のバッジは、ホストが正常であることを示します。赤色のバッジは、ホストが正常でないことを示します。

  側面パネルには、次の情報が表示されます。

  - [Node Status]：ノードのヘルスステータスが表示されます。

    ノードヘルスが**正常でない**場合は、ステータスにカーソルを合わせると、トラブルシューティングのための追加情報が表示されます。

  - [Services Status]：サービスのヘルスステータスが表示されます。1 つでもサービスがダウンしていると、ステータスは [Unhealthy] になります。

  - [Name]：サービス名。

  - [Appstack]：アプリケーションスタック名。

    アプリケーションスタックは、疎結合されたサービスの集合です。この環境でのサービスは、要求が増えると自身のインスタンスを追加し、要求が減ると自身のインスタンスを解放する、水平方向にスケーラブルなアプリケーションです。

  - [Health]：サービスのステータス。

  - [Version]：サービスのバージョン。

- [Tools]：サービスのメトリックとログを表示します。Grafana でサービスモニターリングデータを表示するには、[Metrics] リンクをクリックします。Grafanaは、オープンソースのメトリック分析および可視化スイートです。サービスモニターリングデータを調べることで、問題をトラブルシューティングすることができます。Grafana の詳細については、https://grafana.com/ を参照してください。[Logs] リンクをクリックすると、Kibana でサービスログが表示されます。Kibana は、オープンソースの分析および可視化プラットフォームです。サービスログを調べることで、問題をトラブルシューティングすることができます。Kibana の詳細については、https://www.elastic.co/products/kibana を参照してください。
- [Actions]：サービスを再起動するために使用できるオプション。一部の内部サービスおよびシステム固有のサービスでは、[Actions] オプションが無効になっています。

- [High Availability]：VMware vSphere によって提供されるため、HA のステータスは ESXi 上の Cisco DNA Center では使用できません。詳細については、ハイ アベイラビリティ （41 ページ）を参照してください。
- [Cluster Tools]：次のツールにアクセスできます。
  - [Monitoring]：オープンソースメトリック分析および可視化スイートである Grafana を使用して、Cisco DNA Center コンポーネントの複数のダッシュボードにアクセスします。[Monitoring] ツールを使用して、メモリおよび CPU 使用率などの主要な Cisco DNA Center メトリックを確認および分析します。Grafana の詳細については、https://grafana.com/ を参照してください。

    （注） マルチホスト Cisco DNA Center 環境では、複数のホストによる Grafana データの重複が予想されます。

  - [Log Explorer]：Kibana を使用して Cisco DNA Center のアクティビティログとシステムログにアクセスします。Kibana は Elasticsearch と連動するように設計されたオープンソースの分析および可視化を実行するプラットフォームです。[Log Explorer] ツールを使用して、詳細なアクティビティログおよびシステムログを確認します。Kibana の左側にあるナビゲーションウィンドウで、[Dashboard] をクリックします。次に、[System Overview] をクリックしてすべてのシステムログを表示します。Kibana の詳細については、https://www.elastic.co/guide/en/kibana/current/index.htmlを参照してください。Elasticsearch の詳細については、「https://www.elastic.co/guide/index.html」を参照してください。

    （注） デフォルトでは、Cisco DNA Center のロギングはすべて有効です。

システム管理

- [Software Updates]：インストールされているバージョンのステータスとシステムアップデートに関する情報が表示されます。[View] リンクをクリックすると、更新の詳細が表示されます。ダッシュレットは、エアギャップモードが有効になると通知します。

  （注） 更新には、その横にカラーバッジが付きます。緑色のバッジは、更新または更新に関連するアクションが正常に完了したことを示します。黄色のバッジは、使用可能な更新があることを示します。

- [Backups]：最新のバックアップのステータスが表示されます。[View] リンクをクリックすると、すべてのバックアップの詳細が表示されます。

  さらに、次のスケジュールバックアップのステータスも表示されます（またはスケジュールされているバックアップがないことを示します）。エアギャップモードが有効になっている場合、バックアップ設定は見つかりません。

  （注） バックアップには、その横にカラーバッジが付きます。緑色のバッジは、バックアップが正常に完了したことをタイムスタンプとともに示します。黄色のバッジは、次のバックアップがまだスケジュールされていないことを示します。

Cisco DNA Center と Cisco ISE の統合

Cisco ISE には、Cisco DNA Center に関して次の 3 つの使用例があります。

1. Cisco ISE はユーザー、デバイス、クライアント認証用の AAA（「トリプル A」と発音）サーバーとして使用できます。アクセス コントロール ポリシーを使用していない場合、または Cisco ISE をデバイス認証用の AAA サーバーとして使用していない場合は、Cisco ISE のインストールおよび設定は不要です。
2. アクセス コントロール ポリシーは Cisco ISE を使用してアクセス制御を適用します。アクセス コントロール ポリシーを作成および使用する前に、Cisco DNA Center と Cisco ISE を統合します。このプロセスでは、特定のサービスを用いて Cisco ISE をインストールして設定し、Cisco DNA Center で Cisco ISE の設定を行う必要があります。Cisco DNA Center を用いた Cisco ISE のインストールと設定の詳細については、*Cisco DNA Center* 設置ガイドを参照してください。
3. ネットワークでのユーザー認証に Cisco ISE を使用している場合、Cisco ISE を統合するためにアシュアランスを設定します。この統合により、有線クライアントの詳細（ユーザー名やオペレーティングシステムなど）を アシュアランス で確認できるようになります。詳細については、*Cisco DNA Assurance* ユーザガイド の「Cisco DNA Center の Cisco ISE 設定について」を参照してください。

データの匿名化

Cisco DNA Center では、有線エンドポイントとワイヤレスエンドポイントのデータを匿名化できます。ユーザー ID やデバイスのホスト名など、有線エンドポイントとワイヤレスエンドポイントの個人を特定できる情報をスクランブル化できます。

[Discovery] を実行する前に、匿名化が有効になっていることを確認します。[Discovery] を実行した後にデータを匿名化した場合、システムに入ってくる新しいデータは匿名化されますが、既存のデータは匿名化されません。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Anonymize Data]** の順に選択します。

ステップ 2 [Anonymize Data] ウィンドウで、[Enable Anonymization] チェックボックスをオンにします。

ステップ 3 [Save] をクリックします。
匿名化を有効にすると、デバイス検索時に、MAC アドレス、IP アドレスなどの匿名以外の情報しか指定できなくなります。

認証サーバとポリシー サーバの設定

Cisco DNA Center は AAA サーバをユーザ認証に使用し、Cisco ISE をユーザ認証とアクセス制御の両方に使用します。この手順を使って Cisco ISE を含む AAA サーバを設定します。

始める前に

- Cisco ISE を使用してポリシーと AAA 機能の両方を実行する場合、Cisco DNA Center および Cisco ISE が統合されていることを確認します。
- 他の製品（Cisco ISE 以外）で AAA 機能を使用している場合、以下に注意してください。
  - AAA サーバーで Cisco DNA Center を登録します。これには、AAA サーバーと Cisco DNA Center の共有秘密を定義することが含まれます。
  - AAA サーバーで Cisco DNA Center の属性名を定義します。
  - Cisco DNA Center マルチホストクラスタの設定の場合は、AAA サーバーのマルチホストクラスタに、すべての個別のホスト IP アドレスと仮想 IP アドレスを定義します。
- Cisco ISE を設定する前に、以下の点を確認してください。
  - Cisco ISE をネットワークに展開していること。サポートされている Cisco ISE バージョンの詳細については、『Cisco DNA Center Compatibility Matrix』を参照してください。Cisco ISE のインストールについては、Cisco Identity Services Engine インストールおよびアップグレードガイド [英語] を参照してください。
  - スタンドアロン ISE 展開環境がある場合は、Cisco DNA Center を Cisco ISE ノードと統合し、そのノード上で pxGrid サービスと外部 RESTful サービス（ERS）を有効にする必要があります。

（注） pxGrid 2.0 では Cisco ISE の展開で最大 4 つの pxGrid ノードを使用できますが、Cisco DNA Center 2.2.1.x 以前のリリースは 2 つを超える pxGrid ノードをサポートしていません。

- 分散型 Cisco ISE 展開がある場合：

- Cisco DNA Center をプライマリポリシー管理ノード（PAN）と統合し、PAN 上で ERS を有効にする必要があります。

（注） PAN 経由で ERS を使用することを推奨します。ただし、バックアップの場合は、PSN 上で ERS を有効にできます。

  - 分散型展開環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。PAN 上で pxGrid サービスを有効化することを選択できますが、必須ではありません。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。
  - TrustSec または SD-Access のコンテンツと PAC を処理するように Cisco ISE で設定する PSN は、**[Work Centers]** > **[Trustsec]** > **[Trustsec Servers]** > **[Trustsec AAA Servers]** でも定義する必要があります。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

- ポート 443、5222、8910、9060 で Cisco DNA Center と Cisco ISE の通信を有効にする必要があります。
- pxGrid が有効化されている Cisco ISE ホストには、Cisco ISE eth0 インターフェイスの IP アドレス上の Cisco DNA Center から到達できる必要があります。
- Cisco ISE ノードは、アプライアンス NIC 経由でファブリック アンダーレイ ネットワークに到達できます。
- Cisco ISE 管理ノード証明書のサブジェクト名またはサブジェクト代替名（SAN）のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれている必要があります。
- Cisco DNA Center システム証明書の SAN フィールドに、Cisco DNA Center アプライアンスの IP アドレスと FQDN の両方がリストされている必要があります。

（注） Cisco ISE 2.4 パッチ 13、2.6 パッチ 7、および 2.7 パッチ 3 では、pxGrid 証明書に Cisco ISE のデフォルトの自己署名証明書を使用している場合、証明書が Cisco ISE によって拒否されることがあります。これは、その証明書の古いバージョンに、SSL サーバとして指定された Netscape Cert Type 拡張があるためです。これは、クライアント証明書が必要なため失敗します。

この問題は Cisco ISE 3.0 以降では発生しません。詳細については、Cisco Cloud APIC リリースノート [英語] を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]**。

ステップ 2 [Add] ドロップダウンリストから、[AAA] または [ISE] を選択します。

ステップ 3 プライマリ AAA サーバーを設定するには、次の情報を入力します。

- [Server IP Address]：AAA サーバの IP アドレス。
- [Shared Secret]：デバイス認証のキー。共有秘密の長さは、最大 100 文字です。

（注） 既存の Cisco ISE クラスタの一部である PSN をプライマリ AAA サーバーに設定しないでください。

ステップ 4 Cisco ISE サーバーを設定するには、次の詳細情報を入力します。

- [Server IP Address]：Cisco ISE サーバーの IP アドレス。
- [Shared Secret]：デバイス認証のキー。
- [Username]：Cisco ISE に HTTPS 経由でログインするために使用するユーザー名。
- [Password]：Cisco ISE HTTPS ユーザー名のパスワード。

（注） ユーザー名とパスワードは、ネットワーク管理者に属する ISE 管理者アカウントである必要があります。

- [FQDN]：Cisco ISE サーバーの完全修飾ドメイン名（FQDN）。

（注）
- Cisco ISE（**[Administration]** > **[Deployment]** > **[Deployment Nodes]** > **[List]**）で定義されている FQDN をコピーして、このフィールドに直接貼り付けることをお勧めします。
- 入力した FQDN は、Cisco ISE 証明書で定義されている FQDN、共通名（CN）または Subject Alternative Name（SAN）と一致する必要があります。

FQDN は、次の形式で、ホスト名およびドメイン名の 2 つのパートで構成されています。

hostname.domainname.com

たとえば、Cisco ISE サーバーの FQDN は ise.cisco.com である可能性があります。

- [Virtual IP Address（es）]：Cisco ISE ポリシーサービスノード（PSN）が背後に配置されているロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数の PSN ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

ステップ 5 [Advanced Settings] をクリックして、設定を構成します。

- [Connect to pxGrid]：pxGrid 接続を有効にするには、このチェックボックスをオンにします。

  Cisco DNA Center システム証明書を pxGrid クライアント証明書として使用する場合（pxGrid クライアントとして Cisco DNA Center システムを認証するために Cisco ISE に送信）、[Use Cisco DNA Center Certificate for pxGrid] チェックボックスをオンにします。動作環境で使用されるすべての証明書を同じ

CA で生成する必要がある場合は、このオプションを使用できます。このオプションを無効にすると、Cisco DNA Center は、システムが使用する pxGrid クライアント証明書を生成するための要求を Cisco ISE に送信します。

このオプションを有効にする場合は、次のことを確認してください。

- Cisco DNA Center 証明書が、Cisco ISE で使用中の CA と同じ認証局（CA）によって生成されていること（そうでない場合、pxGrid 認証は失敗します）。
- [Certificate Extended Key Use（EKU）] フィールドに「クライアント認証」が含まれていること。

- [Protocol]：[TACACS] と [RADIUS]（デフォルト）。両方のプロトコルを選択できます。

  注目 ここで Cisco ISE サーバーの TACAS を有効にしない場合は、ネットワークデバイス認証用に AAA サーバーを設定するときに、**[Design]** > **[Network Settings]** > **[Network]** で Cisco ISE サーバーを TACAS サーバーとして設定できません。

- [Authentication Port]：AAA サーバーへの認証メッセージのリレーに使用されるポート。デフォルトの UDP ポートは 1812 です。
- [Accounting Port]：AAA サーバーへの重要なイベントのリレーに使用されるポート。デフォルトの UDP ポートは 1813 です。
- [Port]：デフォルトの TACACS ポートは 49 です。
- [Retries]：接続の試行が中止される前に、Cisco DNA Center が AAA サーバへの接続を試みた回数。デフォルトの試行回数は 3 回です。
- [Timeout]：接続の試行が中止される前に、デバイスが AAA サーバーの応答を待機するタイムアウト期間。デフォルトのタイムアウトは 4 秒です。

（注） 必要な情報を入力すると、Cisco ISE は 2 つのフェーズを経て Cisco DNA Center と統合されます。統合が完了するまでには数分かかります。フェーズごとの統合ステータスは、[Authentication and Policy Servers] ウィンドウと [System 360] ウィンドウに表示されます。

Cisco ISE サーバー登録フェーズ：

- [Authentication and Policy Servers] ウィンドウ：「進行中」
- [System 360] ウィンドウ：「プライマリ使用可能」

pxGrid サブスクリプション登録フェーズ：

- [Authentication and Policy Servers] ウィンドウ：「アクティブ」
- [System 360] ウィンドウ：「プライマリ使用可能」および「pxGrid 使用可能」

設定された Cisco ISE サーバーのステータスがパスワードの変更により [FAILED] と表示されている場合は、[Retry] をクリックし、パスワードを更新して Cisco ISE 接続を再同期します。

ステップ 6 [Add] をクリックします。

ステップ 7 セカンダリサーバーを追加するには、前述の手順を繰り返します。

Cisco AI Network Analytics の設定

この手順で、Cisco AI Analytics 機能を有効にして、ネットワークデバイスとインベントリ、サイト階層、トロポジデータからネットワークイベントのデータを Cisco AI Cloud にエクスポートします。

始める前に

- Cisco DNA Center 用の Cisco DNA Advantage ソフトウェアライセンスを保有していることを確認してください。**AI ネットワーク分析** アプリケーションは、Cisco DNA Advantage ソフトウェアライセンスに含まれています。
- AI Network Analytics アプリケーションの最新バージョンがインストールされていることを確認してください。
- ネットワークまたは HTTP プロキシが、次のクラウドホストへのアウトバウンド HTTPS（TCP 443）アクセスを許可するように設定されていることを確認します。
  - [api.use1.prd.kairos.ciscolabs.com]（米国東部地域）
  - [api.euc1.prd.kairos.ciscolabs.com]（EU 中央地域）

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] までスクロールし、[Cisco AI Analytics] を選択します。
AI ネットワーク分析 ウィンドウが開きます。

ステップ 3 次のいずれかを実行します。

- アプライアンスに以前のバージョンの Cisco AI Network Analytics がインストールされている場合は、次の手順を実行します。
  1. [Recover from a config file] をクリックします。

     [Restore] AI ネットワーク分析ウィンドウが開きます。
  2. 表示されたエリアにコンフィギュレーション ファイルをドラッグアンドドロップするか、ファイルシステムからファイルを選択します。
  3. [Restore] をクリックします。

     Cisco AI Network Analytics の復元には数分かかる場合があり、その後、[Success] ダイアログボックスが表示されます。

- Cisco AI Network Analyticsを初めて構成する場合、次の手順を実行します。
  1. [Configure] をクリックします。

2. [Where should we securely store your data?] 領域で、データを保存する場所を選択します。[Europe (Germany)] または [US East (North Virginia)] を選択できます。

   [Testing cloud connectivity...] タブで示されているように、システムはクラウド接続のテストを開始します。クラウド接続のテストが完了すると、[Testing cloud connectivity...] タブが [Cloud connection verified] に変わります。

3. [Next] をクリックします。

   [Terms and Conditions] ウィンドウが表示されます。

4. [Accept Cisco Universal Cloud Agreement] チェックボックスをオンにして契約条件に同意してから、[Enable] をクリックします。

   Cisco AI Network Analytics が有効になるまでに数分かかる場合があり、その後、[Success] ダイアログボックスが表示されます。

ステップ 4 [Success] ダイアログボックスで [Okay] をクリックします。
AI ネットワーク分析 ウィンドウが表示され、[Enable AI Network Analytics] トグルボタンが表示されます。

ステップ 5 （推奨）**AI ネットワーク分析** ウィンドウで、[Download Configuration] ファイルをクリックします。

クライアント証明書の更新

AI エージェントは、X.509 クライアント証明書を使用して AI クラウドへの認証を実行します。証明書は、AI クラウドへのテナントのオンボーディング時に AI クラウド CA によって作成および署名され、3 年間有効です（2021 年 8 月に 1 年に短縮）。有効期限が切れる前に、クラウド接続が失われないようにクライアント証明書を更新する必要があります。証明書の自動更新メカニズムが導入されています。このメカニズムでは、更新後に証明書を手動でバックアップする必要があります。新しい Cisco DNA Center を復元または移行する場合は、バックアップが必要です。

更新後、すべての AI 分析ウィンドウ（ピア比較、ヒートマップ、ネットワーク比較、トレンドおよびインサイト）に通知が表示され、新しい AI ネットワーク分析構成をバックアップするように指示されます。

Cisco AI Network Analytics の無効化

Cisco AI Network Analytics のデータ収集を無効にするには、次のように AI Network Analytics 機能を無効にする必要があります。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] までスクロールし、[Cisco AI Analytics] を選択します。

各機能のチェックマーク（  ）は、その機能が有効になっていることを示します。チェックボックスがオフの場合（  ）、機能は無効になっています。

ステップ 3 [AI Network Analytics] 領域で、[Enable AI Network Analytics] トグルボタンをクリックしてオフにします（  ）。

ステップ 4 [Update] をクリックします。

ステップ 5 Cisco AI Network Analytics クラウドからネットワークデータを削除するには、Cisco Technical Response Center（TAC）に連絡してサポートリクエストをオープンします。

ステップ 6 以前の設定が間違って配置されている場合は、[Download configuration file] をクリックします。

機械推論ナレッジベースの更新

機械推論ナレッジパックは、機械推論エンジン（MRE）がセキュリティの問題を特定し、根本原因の自動分析を改善するために使用する、段階的なワークフローです。これらのナレッジパックは、より多くの情報を受信しながら継続的に更新されます。機械推論ナレッジベースは、これらのナレッジパック（ワークフロー）のリポジトリです。最新のナレッジパックは、機械推論ナレッジベースが毎日自動で更新されるようCisco DNA Centerを設定するか、手動で更新することで入手できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] まで下にスクロールし、[Machine Reasoning Knowledge Base]を選択します。
[Machine Reasoning Knowledge Base] ウィンドウには、次の情報が表示されます。

- [INSTALLED]：インストールされている機械推論ナレッジベースパッケージのバージョンとインストール日が表示されます。

機械推論ナレッジベースに新しいアップデートがある場合は、[Machine Reasoning Knowledge Base] ウィンドウに [AVAILABLE UPDATE] が表示され、アップデートの [Version] と [Details] が示されます。

- [AUTO UPDATE] ：機械推論ナレッジベースが Cisco DNA Center で自動的に毎日更新されます。
- [CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER, SECURITY ADVISORY, FIELD NOTICES AND EOX]：自動構成を実行できる CX Cloud と Cisco DNA Center を統合します。この統合により、Cisco DNA Centerのセキュリティ アドバイザリ ツールから直接デバイスの脆弱性を検出する機能が更に強化されました。

ステップ 3 （推奨）[AUTO UPDATE] チェックボックスをオンにして、機械推論ナレッジベースを自動的に更新します。
[Next Attempt] 領域に、次回の更新の日付と時刻が表示されます。

自動更新は、Cisco DNA Center がクラウドの機械推論エンジンに正常に接続されている場合にのみ実行できます。

ステップ 4 機械推論ナレッジベースを Cisco DNA Center で手動で更新するには 、次のいずれかを実行します。

- [AVAILABLE UPDATES] の下にある [Update] をクリックします。[Success] ポップアップウィンドウが表示され、更新のステータスが表示されます。
- 機械推論ナレッジベースをローカルマシンに手動でダウンロードして Cisco DNA Center にインポートします。次の手順を実行します。

  1. [Download] をクリックします。

     [Opening mre_workflow_signed] ダイアログボックスが表示されます。

  2. ダウンロードしたファイルを開くか、ローカルマシンの目的の場所に保存して、[OK] をクリックします。

  3. [Import] をクリックして、ダウンロードした機械推論ナレッジベースをローカルマシンから Cisco DNA Center にインポートします。

ステップ 5 [CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY] チェックボックスをオンにして、ネットワークバグ ID およびセキュリティアドバイザリとの Cisco CX Cloud の連携を有効にします。

ステップ 6 [Security Advisories Settings] エリアで、[RECURRING SCAN] トグルボタンをクリックして、毎週の定期的なスキャンを有効または無効にします。

ステップ 7 [CISCO CX CLOUD] トグルボタンをクリックして、Cisco CX Cloud を有効または無効にします。

シスコのクレデンシャルの設定

Cisco DNA Center の Cisco のクレデンシャルを設定できます。Cisco のクレデンシャルは、シスコの顧客またはパートナーとして制限付きの場所にアクセスするために、シスコの Web サイトのログインに使用するユーザー名とパスワードです。

（注） 次の手順を使用して、Cisco DNA Center 用に設定された Cisco のクレデンシャルは、ソフトウェア イメージや更新プログラムをダウンロードするために使用されます。Cisco のクレデンシャルはまた、セキュリティのために、このプロセスによって暗号化されます。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Cisco Accounts]** > **[Cisco.com Credentials]** の順に選択します。

ステップ 2 シスコユーザー名およびパスワードを入力してください。

ステップ 3 **[Save]** をクリックします。

cisco.com のログイン情報がソフトウェアとサービスに対して設定されます。

シスコのクレデンシャルのクリア

Cisco DNA Center に対して現在設定されている cisco.com のログイン情報を削除するには、次の手順を実行します。

（注）
- ソフトウェアのダウンロードやデバイスのプロビジョニングに関連するタスクを実行する際、cisco.com のログイン情報が設定されていないと、タスクの開始前にログイン情報を入力するように求められます。入力したログイン情報を保存して Cisco DNA Center 全体で使用するには、表示されたダイアログボックスで [Save for Later] チェックボックスをオンにします。それ以外の場合は、これらのタスクを実行するたびにログイン情報を入力する必要があります。
- この手順を完了すると、エンドユーザーライセンス契約（EULA）の承認が取り消されます。EULA の承認を再入力する方法については、ライセンス契約書の受諾 （22 ページ）を参照してください。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザーのみがこの手順を実行することができます。詳細については、ユーザ ロールの概要 （77 ページ）を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Cisco Accounts]** > **[Cisco.com Credentials]** の順に選択します。

ステップ 2 [Clear] をクリックします。

ステップ 3 表示されたダイアログボックスで、[Continue] をクリックして操作を確定します。

接続モードの設定

接続モードは、Cisco DNA Center と連携するネットワーク内のスマート対応デバイスと Cisco Smart Software Manager（SSM）の間の接続を管理します。異なる接続モードを設定するには、SUPER-ADMIN アクセス権限が必要です。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Cisco Accounts]** > **[SSM Connection Mode]** の順に選択します。

次の接続モードを使用できます。

- 直接
- オンプレミス CSSM
- スマートプロキシ

ステップ 2 Cisco SSM クラウドへの直接接続を有効にするには、[Direct] を選択します。

ステップ 3 組織のセキュリティを高める必要がある場合は、[On-Prem CSSM] を選択します。オンプレミスオプションでは、Cisco SSM クラウドでライセンスを管理する際に、インターネットで直接接続する代わりに Cisco SSM 機能のサブセットにアクセスできます。

a) [On-Prem CSSM] を有効にする前に、サテライトがネットワークサイトに展開されて稼働していることを確認してください。

サテライトが FQDN で設定されている場合、サテライト FQDN の Call Home 設定が IP アドレスの代わりにプッシュされます。

b) [On-Prem CSSM Host]、[Smart Account Name]、[Client ID]、および [Client Secret] の詳細を入力します。

[Smart Account] フィールドに、1 つの SSM オンプレミスアカウント名のみを入力します。スペースやアンダースコアは使用できません。

クライアント ID とクライアントシークレットを取得する方法については、『*Cisco Smart Software Manager On-Prem User Guide*』を参照してください。

c) [Test Connection] をクリックして Cisco SSM 接続を検証します。

d) [Save] をクリックしてから [Confirm] をクリックします。

e) 変更した SSM で再登録が必要なデバイスがある場合は、[Need to Re-Register Devices] ダイアログボックスが表示されます。ダイアログ ボックスで [OK] をクリックします。

f) **[Tools]** > **[License Manager]** > **[Devices]** ウィンドウで、再度登録するデバイスを選択し、[Sync Connection Mode] をクリックします。

（注） このようなデバイスには、「接続モードが同期していない（Connection Mode out of sync）」旨のタグまたはメッセージが表示されます。

g) [Resync Devices] ダイアログボックスで、次の手順を実行します。

- [Smart Account] を入力します。
- [Virtual Account] を入力します。
- [Now] をクリックしてすぐに再同期を開始するか、[Later] をクリックして特定の時間に再同期をスケジュールします。
- [Resync] をクリックします。

[Recent Tasks] ウィンドウには、デバイスの再同期ステータスが表示されます。

ステップ 4 [Smart Proxy] を選択し、Cisco DNA Center を介して Cisco SSM クラウドにスマート対応デバイスを登録します。このモードでは、デバイスを Cisco SSM クラウドに直接接続する必要はありません。Cisco DNA Center は、デバイスからの要求を自身を介して Cisco SSM クラウドにプロキシします。

Call Home 設定をデバイスにプロビジョニングするときに、サテライトが FQDN で設定されている場合、IP アドレスの代わりにサテライトの FQDN がプッシュされます。

プラグアンドプレイの登録

Cisco DNA Center を、Cisco Plug and Play（PnP）Connect のコントローラとして、リダイレクトサービス用に Cisco スマートアカウントに登録できます。これにより、Cisco PnP Connect クラウドポータルから Cisco DNA Center の PnP に、デバイスインベントリを同期することができます。

始める前に

SUPER-ADMIN-ROLE またはシステム管理権限を持つ **CUSTOM-ROLE** のユーザーのみがこの手順を実行することができます。

スマートアカウントで、特定の機能の実行を許可するロールがユーザーに割り当てられます。

- スマートアカウント管理者ユーザーは、すべてのバーチャルアカウントにアクセスできます。
- ユーザーは、割り当てられたバーチャルアカウントにのみアクセスできます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Cisco Accounts]** > **[PnP Connect]** の順に選択します。

PnP 接続プロファイルのテーブルが表示されます。

ステップ 2 [Register] をクリックして、バーチャルアカウントを登録します。

ステップ 3 [Register Virtual Account] ウィンドウで、設定したスマートアカウントが [Select Smart Account] ドロップダウンリストに表示されます。[Select Virtual Account] ドロップダウンリストからアカウントを選択できます。

ステップ 4 必要な [IP] または [FQDN] オプションボタンをクリックします。

ステップ 5 コントローラの IP アドレスまたは FQDN（完全修飾ドメイン名）を入力します。

ステップ 6 プロファイル名を入力します。指定した設定を使用して、選択したバーチャルアカウントのプロファイルが作成されます。

ステップ 7 [Use as Default Controller Profile] チェックボックスをオンにして、この Cisco DNA Center コントローラを Cisco PnP Connect クラウドポータルにデフォルトコントローラとして登録します。

ステップ 8 [Register] をクリックします。

PnP イベント通知の作成

イベント通知を作成することで、プラグアンドプレイ（PnP）イベントが Cisco DNA Center で発生するたびに通知を受け取ります。サポートされているチャネルを設定し、イベント通知を作成する方法については、『Cisco DNA Center Platform User Guide』の「Work with Event Notifications」トピックを参照してください。

次の PnP イベントのイベント通知を作成してください。

イベント名	イベント ID	説明
デバイスの追加に失敗しました。	NETWORK-TASK_FAILURE-3-008	デバイスは、単一または一括インポートでは追加されません。単一または一括インポートによってデバイスを追加すると、エラーが発生します。
デバイスの追加に成功しました。	NETWORK-TASK_COMPLETE-4-007	単一または一括インポートによってデバイスが正常に追加されました。
デバイスはエラー状態です。	NETWORK-ERROR_1-002	デバイスは**エラー**状態になります。
デバイスはプロビジョニング状態です。	NETWORK-INFO_4-003	デバイスは**プロビジョニング**状態になります。
デバイスがオンボーディング状態でスタックします。	NETWORK-TASK_PROGRESS-2-006	デバイスが 15 分以上オンボーディング状態でスタックしています。
デバイスが請求を待っています。	NETWORK-INFO_2-001	デバイスは**未請求**の状態になり、プロビジョニングの準備ができています。
スマートアカウントの同期に失敗しました。	NETWORK-TASK_FAILURE-1-005	一部のデバイスでスマートアカウントの同期に失敗しました。
スマートアカウントの同期に成功しました。	NETWORK-TASK_COMPLETE-4-004	一部のデバイスで、スマートアカウントの同期に成功しました。

スマートアカウントの設定

シスコスマートアカウントのログイン情報は、スマート ライセンス アカウントに接続する目的で使用されます。ライセンスマネージャツールは、権限付与とライセンス管理のために、このスマートアカウントの詳細なライセンス情報を使用します。

始める前に

SUPER-ADMIN-ROLE 権限を取得しておきます。

ステップ 1 [System]左上隅にあるメニューアイコンをクリックして、>[Settings]>[Cisco Accounts]>[Smart Account]。

ステップ 2 [Add] ボタンをクリックします。スマートアカウントのログイン情報を入力するように求められます。

a) スマート アカウントのユーザー名およびパスワードを入力します。

b) **[Save]** をクリックします。
スマートアカウントが設定されます。

ステップ 3 選択したスマートアカウントの名前を変更するには、[Change] をクリックします。Cisco SSM クラウドでスマート ライセンス アカウントへの接続に使用されるスマートアカウントを選択するように促されます。

a) ドロップダウンリストから [Smart Account] を選択します。

b) **[Save]** をクリックします。

ステップ 4 [View all virtual accounts] をクリックし、そのスマートアカウントに関連付けられているすべてのバーチャルアカウントを表示します。

（注） シスコ アカウントは複数のスマートアカウントとバーチャルアカウントをサポートしています。

ステップ 5 （オプション）スマートライセンス対応デバイスをバーチャルアカウントに自動登録する場合、[Auto register smart license enabled devices] チェックボックスをオンにします。スマートアカウントに関連付けられているバーチャルアカウントのリストが表示されます。

ステップ 6 必要なバーチャルアカウントを選択します。スマートライセンス対応デバイスがインベントリに追加されるたびに、選択したバーチャルアカウントに自動的に登録されます。

ステップ 7 ライセンスを取得したスマートアカウントユーザーとそれに関連する履歴データを削除する場合は、[Delete historical information] をクリックします。

[Delete Historical Data] スライドインペインには、ライセンスを取得したスマートアカウントユーザーが表示されます。また、Cisco DNA Center に現在存在していない既存のスマートアカウントも表示されますが、それらの履歴データは引き続き利用できます。

ステップ 8 [Smart Account list] エリアで、削除するスマートアカウントの横にあるチェックボックスをオンにします。

ステップ 9 [Delete] をクリックします。

ステップ 10 次の確認ウィンドウで、[Delete] をクリックします。

ステップ 11 [Delete the associated license historical information] チェックボックスをオンにして、関連するライセンスの履歴情報を削除します。

スマートライセンス

シスコ スマート ライセンシングを使用すると、Cisco SSM に Cisco DNA Center を登録できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（software.cisco.com）。

シスコライセンスの詳細については、cisco.com/go/licensingguide を参照してください。

始める前に

- スマートライセンスを有効にするには、Cisco クレデンシャルを設定し（「シスコのクレデンシャルの設定 （13 ページ）」を参照）、Cisco SSM で Cisco DNA Center ライセンス規則をアップロードする必要があります。
- スマートライセンスを有効にするには、**[System]** > **[Settings]** > **[Cisco Accounts]** > **[Smart Account]** でスマートアカウントを追加する必要があります。詳細については、スマートアカウントの設定 （17 ページ）を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Cisco Accounts]** > **[Smart Licensing]** の順に選択します。

デフォルトでは、[Smart Account] の詳細が表示されます。

ステップ 2 登録するバーチャルアカウントを [Search Virtual Account] ドロップダウンリストから選択します。

ステップ 3 [Register] をクリックします。

ステップ 4 登録が正常に完了したら、[View Available Licenses] リンクをクリックして、Cisco DNA Center の使用可能なライセンスを確認します。

デバイスの可制御性

デバイスの可制御性とは、Cisco DNA Center におけるいくつかのデバイス層機能の同期状態を徹底するシステムレベルのプロセスです。この目的は、Cisco DNA Center がデバイスを管理するのに必要なネットワーク設定の導入を支援することです。ディスカバリを実行したり、インベントリにデバイスを追加したり、デバイスをサイトに割り当てたりすると、ネットワークデバイスに変更が加えられます。

デバイスにプッシュされる設定を表示するには、**[Provision]** > **[Inventory]** に移動し、**[Focus]** ドロップダウンリストから **[Provision]** を選択します。[Provision Status] 列の [See Details] をクリックします。

（注） Cisco DNA Centerによりデバイスが設定または更新されると、トランザクションが監査ログにキャプチャされ、変更の追跡と問題のトラブルシューティングに使用できます。

下記のデバイス設定がデバイスの可制御性の一部として有効になります。

- **デバイス検出**

- [SNMP Credentials]
- [NETCONF Credentials]

- **インベントリへのデバイスの追加**

  Cisco TrustSec（CTS）クレデンシャル

（注） [Global] サイトが Cisco ISE で AAA として設定されている場合にのみ、Cisco TrustSec（CTS）クレデンシャルがインベントリ中にプッシュされます。それ以外の場合は、CTS が Cisco ISE で AAA として設定されている場合に「サイトへの割り当て」中にデバイスにプッシュされます。

- **デバイスのサイトへの割り当て**
  - コントローラ証明書

（注） Cisco IOS デバイスの場合、PKCS 証明書の有効期限の処理で問題が発生しないように、デバイスの UI コンソールからタイムゾーンを設定することを推奨します。

  - SNMP トラップサーバ定義
  - Syslog サーバ定義
  - NetFlow サーバ定義
  - Wireless Service Assurance（WSA）
  - IPDT の有効化

デバイスの可制御性はデフォルトで有効です。デバイスの可制御性を有効にしたくない場合は、手動で無効にします。詳細については、デバイスの可制御性の設定 （22 ページ）を参照してください。

デバイスの可制御性が無効の場合、ディスカバリ実行時やデバイスのサイトへの割り当て時に、上述のクレデンシャルや機能が Cisco DNA Center で設定されることはありません。

次のような状況により、デバイスの可制御性によってデバイスにネットワーク設定が適用されるかどうかが決まります。

- **デバイス検出**：SNMP と NETCONF クレデンシャルがまだデバイスに存在しない場合は、この設定が検出プロセス中に適用されます。
- **インベントリ内のデバイス（Device in Inventory）**：初期インベントリ収集が正常に終了すると、IPDT がデバイスで設定されます。

以前のリリースでは、次の IPDT コマンドが設定されていました。

```
ip device tracking
ip device tracking probe delay 60
ip device tracking probe use-svi
```

インターフェイスごとに、次の手順を実行します。

```
interface $physicalInterface
ip device tracking maximum 65535
```

現在のリリースでは、新しく検出されたデバイスに対して次の IPDT コマンドが設定されます。

```
device-tracking tracking
device-tracking policy IPDT_POLICY
tracking enable
```

インターフェイスごとに、次の手順を実行します。

```
interface $physicalInterface
device-tracking attach-policy IPDT_POLICY
```

- **グローバルサイト内のデバイス**：デバイスが正常に追加、インポート、または検出されると、Cisco DNA Center はデフォルトでデバイスを [Managed] 状態にして [Global] サイトに割り当てます。**グローバル** サイト用の SNMP サーバ、Syslog サーバ、および NetFlow コレクタ設定が定義済みの場合でも、デバイス上のこれらの設定を変更 Cisco DNA Center しません。
- **サイトに移動されたデバイス（Device Moved to Site）**：デバイスを [グローバル（Global）] サイトから、SNMP サーバ、Syslog サーバ、NetFlow コレクタ設定が定義済みの新しいサイトに移動させると、Cisco DNA Center ではデバイスのこれらの設定が新しいサイト用に定義された設定に変更されます。
- **サイトから削除されたデバイス（Device Removed from Site）**：デバイスをサイトから削除する場合、Cisco DNA Center ではデバイスの SNMP サーバ、Syslog サーバ、NetFlow コレクタ設定が削除されません。
- **削除されるデバイスCisco DNA Center**：デバイスを Cisco DNA Center から削除し、[Configuration Clean-up] チェックボックスがオンにすると、 SNMP サーバ、Syslog サーバ、および NetFlow コレクタ設定はデバイスから削除されます。
- **別のサイトに移動したデバイス（Device Moved from Site to Site）**：たとえばサイト A からサイト B にデバイスを移動させると、Cisco DNA Center ではデバイスの SNMP サーバ、Syslog サーバ、NetFlow コレクタ設定が、サイト B に割り当てられた設定に置き換えられます。
- **サイトテレメトリの変更の更新**：デバイスの可制御性の範囲内にある設定に対する変更は、デバイスのプロビジョニング中、または**テレメトリ設定の更新**アクションの実行時にネットワークデバイスに適用されます。

デバイスの制御可能性が有効になっている場合、Cisco DNA Centerがユーザーが提供した SNMP 資格情報を介してデバイスに接続できず、デバイス情報を収集できない場合、Cisco DNA Center がユーザーが提供した SNMP 資格情報をデバイスにプッシュします。 SNMPv3 の場合、ユーザーは [Default] グループの下に作成されます。

（注） Cisco AireOS デバイスの場合、ユーザ指定の SNMPv3 パスフレーズには 12 ～ 31 文字が含まれている必要があります。

デバイスの可制御性の設定

デバイスの可制御性は、Cisco DNA Centerでデバイスを管理するために必要なネットワーク設定の展開を支援します。

（注） デバイスの可制御性を無効にすると、[Device Controllability] ページに記載されているログイン情報または機能は、ディスカバリ時または実行時にデバイスに設定されません。

デバイスの可制御性はデフォルトで有効です。デバイスの可制御性を手動で無効にするには、次の手順を実行します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[Device Controllability]**。

ステップ 2 [Enable Device Controllability] チェックボックスをオフにします。

ステップ 3 [Save] をクリックします。

ライセンス契約書の受諾

ソフトウェアをダウンロードする前、またはデバイスをプロビジョニングする前に、エンドユーザーライセンス契約（EULA）に同意する必要があります。

（注） cisco.com のログイン情報をまだ設定していない場合は、先に進む前に、[Device EULA Acceptance] ウィンドウで設定するように求められます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[Device EULA Acceptance]** の順に選択します。

ステップ 2 [Cisco End User License Agreement] リンクをクリックし、EULA を読みます。

ステップ 3 [I have read and accept the Device EULA] チェックボックスをオンにします。

ステップ 4 [Save] をクリックします。

SNMP プロパティの設定

SNMP の再試行とタイムアウトの値を設定することができます。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[SNMP]** の順に選択します。

ステップ 2 次のフィールドを設定します。

- **再試行回数（Retries）**：許容されるデバイス接続の最大試行回数。有効な値は 1 ～ 3 です。デフォルトは 3 です。
- [Timeout]：タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Cisco DNA Center が待機する秒数。有効な値は、5 秒間隔で 1 ～ 300 秒です。デフォルトは 5 秒です。

ステップ 3 **[保存（Save）]** をクリックします。

ステップ 4 （オプション）デフォルトの設定に戻すには、[Reset] をクリックしてから [Save] をクリックします。

ICMP ping のイネーブル化

Internet Control Message Protocol（ICMP）ping が有効になっていて、FlexConnect モードで到達不能なアクセスポイントがある場合、Cisco DNA Center は ICMP を使用して 5 分ごとにそれらのアクセスポイントに ping を実行し、到達可能性を強化します。

次の手順では、ICMP ping を有効にする方法について説明します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[ICMP Ping]** の順に選択します。

ステップ 2 [Enable ICMP ping for unreachable access Points in FlexConnect mode] チェックボックスをオンにします。

ステップ 3 [Save] をクリックします。

PnP 導入準備用の AP ロケーションの設定

Cisco DNA Center では、PnP 導入準備の AP の場所として、PnP 要求中に割り当てられたサイトを使用できます。[Configure AP Location] チェックボックスをオンにすると、Cisco DNA Center

は割り当てられたサイトを PnP 導入準備用の AP の場所として設定します。チェックボックスをオフにした場合は [Configure Access Points] ワークフローを使用して、PnP 導入準備用の AP の場所を設定します。詳細については、『*Cisco DNA Center User Guide*』の「AP Configuration in Cisco DNA Center」を参照してください。

（注） これらの設定は、Day-N 運用中には適用されません。Day-N 運用の AP の場所を設定するには、[Configure Access Points] ワークフローを使用します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[PnP AP Location]** の順に選択します。

ステップ 2 [Configure AP Location] チェックボックスをオンにします。

ステップ 3 [Save] をクリックします。

イメージ配信サーバの設定

イメージ配信サーバーは、ソフトウェアイメージの保管と配信に役立ちます。ソフトウェアイメージを配信するように最大 3 つの外部イメージ配信サーバーを設定できます。また、新しく追加されたイメージ配信サーバーに 1 つ以上のプロトコルを設定できます。

サポートされているサーバーの詳細については、*Cisco DNA Center* 管理者ガイド のトピック「バックアップサーバーの要件」にある「自動化データバックアップのサーバー要件」セクションを参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[Image Distribution Servers]**。

ステップ 2 [Image Distribution Servers] ウィンドウで、[Servers] をクリックします。

[Image Distribution Servers] テーブルには、イメージ配信サーバーのホスト、ユーザー名、SFTP、SCP、および接続に関する詳細が表示されます。

ステップ 3 [Add] をクリックして新しいイメージ配信サーバを追加します。

[Add a New Image Distribution Server]slide-in pane が表示されます。

ステップ 4 イメージ配信サーバについて、次の項目を設定します。

- [Host]：イメージ配信サーバーのホスト名または IP アドレスを入力します。
- [Root Location] ：ファイル転送用の作業ルートディレクトリ。

（注） Cisco AireOS ワイヤレスコントローラ の場合、設定されたパスが 16 文字を超えると、イメージの配信は失敗します。

- [Username]：イメージ配信サーバーへのログインに使用されるユーザー名を入力します。ユーザー名には、サーバーの作業ルートディレクトリに対する読み取り/書き込み権限が必要です。
- [Password]：イメージ配信サーバーへのログインに使用されるパスワード。
- [ポート番号]：イメージ配信サーバーが実行されているポート番号を入力します。

ステップ 5 [**Save**] をクリックします。

ステップ 6 一部のワイヤレスコントローラの旧バージョンのソフトウェアでは、SFTP の暗号方式として弱い暗号方式（SHA1 ベースの暗号など）しかサポートされていないため、Cisco DNA Center でソフトウェアイメージの管理やワイヤレスアシュアランスの設定を行うには、ワイヤレスコントローラからの SFTP 接続に対して SFTP 互換モードを有効にする必要があります。Cisco DNA Center の SFTP サーバーでは、弱い暗号方式のサポートを最大 90 日間まで一時的に有効にすることができます。弱い暗号を許可するには、以下を実行します。

a) SFTP サーバーの IP アドレスの横にある [i] アイコンにカーソルを合わせ、[Click here] をクリックします。
b) [Compatibility Mode] slide-in paneで [Compatibility Mode] チェックボックスをオンにして期間（1 分～ 90 日）を入力します。
c) [Save] をクリックします。

ステップ 7 （任意） 設定を編集するには、対応するイメージ配信サーバーの横にある [Edit] アイコンをクリックし、必要な変更を行って [Save] をクリックします。

ステップ 8 （任意） イメージ配信サーバーを削除するには、イメージ配信サーバーの横にある [Delete] アイコンをクリックし、[Delete] をクリックします。

PnP デバイス許可の有効化

次の手順では、デバイスで許可を有効にする方法について説明します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Device Settings]** の順に選択します。

ステップ 2 [Device Settings] ドロップダウンリストから [PnP Device Authorization] を選択します。

（注） デフォルトでは、デバイスは自動的に許可されます。

ステップ 3 [Device Authorization] チェックボックスをオンにしてデバイスで許可を有効にします。

ステップ 4 [Save] をクリックします。

デバイスプロンプトの構成

Cisco DNA Center ではユーザー名とパスワードのカスタムプロンプトを作成できます。カスタムプロンプトを使用してデバイスに関する情報を収集するように、ネットワーク内のデバイスを構成できます。

カスタムプロンプトの作成

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[Device Prompts]** の順に選択します。

[Device Prompts] ウィンドウが開きます。

ステップ 2 [Create Custom Prompt] をクリックします。

[Create Custom Prompt] スライドインペインが開きます。

ステップ 3 ユーザー名のカスタムプロンプトを作成するには、次の手順を実行します。

1. [Prompt Type] ドロップダウンリストから、[username] を選択します。
2. [Prompt Text] フィールドに、正規表現（Regex）でテキストを入力します。
3. [Save] をクリックします。

ステップ 4 パスワードのカスタムプロンプトを作成するには、次の手順を実行します。

1. [Prompt Type] ドロップダウンリストから、[password] を選択します。
2. [Prompt Text] フィールドに、正規表現（Regex）でテキストを入力します。
3. [Save] をクリックします。

（注） [Device Prompts] ウィンドウにカスタムプロンプトが表示されます。ユーザー名とパスワードのカスタムプロンプトを 8 つまで作成できます。

ステップ 5 カスタムプロンプトを必要な順序でドラッグアンドドロップします。

（注） Cisco DNA Center は、カスタムプロンプトの順序を維持し、プロンプトをコンマ区切り値としてデバイスに渡します。最上位のカスタムプロンプトの優先度が高くなります。

ステップ 6 編集アイコンをクリックして、カスタムプロンプトを編集します。

ステップ 7 カスタムプロンプトを削除するには、削除アイコンをクリックします。

（注） ユーザー名のプロンプトとパスワードのプロンプトには、一意の正規表現が必要です。同じまたは類似の正規表現を作成すると、デバイスで認証の問題が発生します。

デバイス構成のバックアップ設定の構成

Cisco DNA Center は、デバイスの実行構成の定期的なバックアップを実行します。バックアップの日時と、デバイスごとに保存できる構成ドリフトの合計数を選択できます。

（注）
- [Daily Backup]：Cisco DNA Center は、毎日午後 11:00（UTC タイムゾーン）に実行するようにスケジュールされた自動設定バックアップを実行します。このプロセス中、Cisco DNA Centerは、最後にデバイス構成の収集が行われた時点のタイムスタンプと、デバイス構成がアーカイブされた時点のタイムスタンプを比較します。この差が30分を超える場合は、デバイス構成のアーカイブが実行されます。

  日次バックアップは、週次バックアップがスケジュールされている日には実行されません。
- [Weekly Backup]：Cisco DNA Center は、毎週日曜日の午後 11:30（UTC タイムゾーン）に実行するようにスケジュールされた自動設定バックアップを実行します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[System]** > **[Settings]** > **[Configuration Archive]** を選択します。

ステップ 2 [Configuration Archive] ウィンドウで、[Internal] タブをクリックします。

ステップ 3 [Number of config drift per device] ドロップダウンリストをクリックし、デバイスごとに保存する構成ドリフトの数を選択します。

デバイスごとに 7 ～ 50 の構成ドリフトを保存できます。保存される構成ドリフトの合計には、デバイスのすべてのラベル付き構成が含まれます。

（注） デフォルトでは、デバイスごとに保存される構成ドリフトの数は 15 です。

ステップ 4 バックアップの日時を選択します。

選択したバックアップの日時は、ネットワークに展開された Cisco DNA Center クラスタのタイムゾーンに基づきます。

ステップ 5 [Save] をクリックします。

バックアップは、スケジュールした後にアクティビティセンターで表示できます。

ステップ 6 [External] タブをクリックして、デバイス構成をアーカイブするための外部サーバーを構成します。詳細については、アーカイブデバイス構成用の外部サーバーの構成 （28 ページ）を参照してください。

アーカイブデバイス構成用の外部サーバーの構成

デバイスの実行コンフィギュレーションをアーカイブするための外部 SFTP サーバーを構成できます。

始める前に

外部サーバーで SSH、SFTP、SCP が有効になっていることを確認します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[System]** > **[Settings]** > **[Configuration Archive]** を選択します。

ステップ 2 [Configuration Archive] ウィンドウで、[External] タブをクリックします。

ステップ 3 [Add] をクリックして、[External Repository] を追加します。

（注） 追加できる SFTP サーバーは 1 つだけです。

ステップ 4 [Add New External Repository] スライドインペインで、次の詳細を入力します。

a) [Host]：ホストの IP アドレスを入力します。

b) [Root Location]：ルートフォルダの場所を入力します。

（注）
- ルートの場所のパスが相対パスではなく絶対パスであることを確認します。
- 外部サーバーのルートの場所は空である必要があります。

c) [Server Protocol]：SFTP サーバーのユーザー名、パスワード、ポート番号を入力します。

d) [Backup Format] を選択します。

- [RAW]：実行コンフィギュレーションがすべて公開されます。すべての機密設定とプライベート設定は、バックアップデータでマスク解除されます。パスワードを入力して、バックアップファイルをロックします。

  （注） ファイルのパスワードは Cisco DNA Center に保存されません。SFTP サーバー上のファイルにアクセスするには、パスワードを覚えておく必要があります。

- [Sanitized (Masked)]：実行コンフィギュレーションの機密設定とプライベート設定の詳細がマスクされます。

  パスワードは、RAW バックアップ形式を選択した場合にのみ適用されます。

e) バックアップサイクルをスケジュールします。

バックアップの日付、時刻、タイムゾーン、およびバックアップの繰り返し間隔を入力します。

ステップ 5 [Save] をクリックします。

ステップ 6 SFTP サーバーの詳細を編集するには、[Action] 列の編集ボタンをクリックします。

ステップ 7 SFTP サーバーを削除するには、[Action] 列の下にある削除ボタンをクリックします。

整合性検証

整合性検証（IV）では、主要なデバイスデータに対する、デバイス侵害の可能性を示す予期しない変更または無効な値を監視します（該当する場合）。この目的は、シスコデバイスに対する不正な変更の検出時間を大幅に短縮することで、侵害の影響を最小限に抑えることにあります。

（注） このリリースでは、IV で Cisco DNA Center にアップロードされたソフトウェアイメージの整合性検証チェックを実行します。整合性検証チェックを実行するために、IV サービスは、Known Good Value（KGV）ファイルをアップロードする必要があります。

KGV ファイルのアップロード

セキュリティの整合性を提供するために、真正かつ有効なソフトウェアを実行しているものとしてシスコデバイスを検証する必要があります。現在、シスコデバイスには、真正なシスコソフトウェアを実行しているかどうかを判別するための参照ポイントがありません。IV では、収集されたイメージ整合性データをシスコソフトウェアの KGV と比較するためのシステムを使用します。

シスコは、その多くの製品の KGV が含まれる KGV データファイルを生成および発行しています。この KGV ファイルは標準の JSON 形式であり、シスコによって署名され、他のファイルとともに単一の KGV ファイルにバンドルされ、シスコの Web サイトから入手できます。KGV ファイルは、次の場所に掲載されています。

https://tools.cisco.com/cscrdr/security/center/files/trust/Cisco_KnownGoodValues.tar

KGV ファイルは IV にインポートされ、ネットワークデバイスから取得した整合性の測定を検証するために使用されます。

（注） デバイス整合性の測定値は IV に提供され、IV 内で完全に使用されます。IV と cisco.com の間の接続は必要ありません。KGV ファイルを保護された環境にエアギャップ転送し、IV にロードできます。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Integrity Verification]** の順に選択します。

ステップ 2 現在の KGV ファイル情報を確認します。

- [File Name]：KGV tar ファイルの名前。
- [Imported By]：KGV ファイルをインポートした Cisco DNA Center ユーザー。自動的にダウンロードされる場合、値は [System] です。
- [Imported Time]：KGV ファイルがインポートされた時刻。
- [Imported Mode]：ローカルまたはリモートのインポートモード。
- [Records]：処理されたレコード。
- [File Hash]：KGV ファイルのファイルハッシュ。
- [Published]：KGV ファイルの発行日。

ステップ 3 KGV ファイルをインポートするには、次のいずれかの手順を実行します。

- KGV ファイルをローカルにインポートするには、[Import New from Local] をクリックします。
- KGV ファイルを cisco.com からインポートするには、[Import Latest from Cisco] をクリックします。

（注） [Import Latest from Cisco] オプションでは、ファイアウォール設定は必要ありません。ただし、ファイアウォールがすでに設定されている場合は、https://tools.cisco.com への接続のみを開く必要があります。

ステップ 4 [Import Latest from Cisco] をクリックした場合は、cisco.com への接続が行われ、最新の KGV ファイルが自動的に Cisco DNA Center にインポートされます。

（注） https://tools.cisco.com へのセキュアな接続は、Cisco DNA Center とそのプロキシ（初回セットアップ時に設定された場合）に追加された証明書を使用して行われます。

ステップ 5 [Import New from Local] をクリックした場合は、[Import KGV] ウィンドウが表示されます。

ステップ 6 次の手順のいずれかを実行してローカルにインポートします。

- ローカル KGV ファイルを [Import KGV] フィールドにドラッグアンドドロップします。
- [Click here to select a KGV file from your computer] をクリックして、ご使用のコンピュータ上のフォルダから KGV ファイルを選択します。
- [Latest KGV file] リンクをクリックし、最新の KGV ファイルをダウンロードしてから、そのファイルを [Import KGV] フィールドにドラッグアンドドロップします。

ステップ 7 [Import] をクリックします。

KGV ファイルが Cisco DNA Center にインポートされます。

ステップ 8 インポートが完了したら、GUI で現在の KGV ファイル情報を検証し、ファイルが更新されたことを確認します。

IV は、Cisco DNA Center が展開されてから 7 日後に最新の KGV ファイルを cisco.com からシステムに自動的にダウンロードします。自動ダウンロードは 7 日ごとに継続されます。KGV ファイルをローカルシステムに手動でダウンロードして、Cisco DNA Center にインポートすることもできます。たとえば、金曜日に新しい KGV ファイルが使用可能になり、自動ダウンロードが 7 日ごと（月曜日）に行われる場合は、手動でダウンロードできます。

次の KGV 自動ダウンロード情報が表示されます。

- [Frequency]：自動ダウンロードの頻度。
- [Last Attempt]：KGV スケジューラが最後にトリガーされた時間。
- [Status]：KGV スケジューラの最後の試行のステータス。
- [Message]：ステータスメッセージ。

（注） 最新の KGV ファイルをインポートするときにエラーが見つかった場合は、エラーメッセージが表示されます。このエラーメッセージは複数の言語に翻訳されるようになりました。

次のタスク

最新の KGV ファイルをインポートしたら、**[Design]** > **[Image Repository]** を選択して、インポートされたイメージの整合性を表示します。

（注） すでにインポートされたイメージが検証不能ステータス（物理または仮想）である場合は、KGV ファイルをインポートした効果を [Image Repository] ウィンドウで確認できます。さらに、将来のイメージインポートでも、新しくアップロードした KGV を検証のために参照します（該当する場合）。

IP アドレスマネージャの設定

Cisco DNA Center を外部 IP アドレスマネージャ（IPAM）と通信するように設定できます。Cisco DNA Center を使用して、IP アドレスプールの作成、予約、または削除を行うと、Cisco DNA Center はその情報を外部 IPAM に伝達します。

始める前に

外部 IP アドレスマネージャがセットアップされ、機能していることを確認します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[External Services]** > **[IP Address Manager]** の順に選択します。

ステップ 2 [Server Name] フィールドに、IPAM サーバーの名前を入力します。

ステップ 3 [Server URL] フィールドに、IPAM サーバーの URL または IP アドレスを入力します。

証明書がこのサーバーに対して信頼されていないことを示す警告アイコンとメッセージが表示されます。信頼証明書を IPAM から直接インポートするには、次の手順を実行します。

a) 警告アイコンをクリックします。

[Certificate Warning] ダイアログボックスが表示されます。

b) 証明書の発行者、シリアル番号、および有効期限を確認します。
c) 情報が正しい場合は、チェックボックスをクリックして Cisco DNA Center による IP アドレスへのアクセスを許可し、信頼できない証明書を信頼できる証明書に追加します。
d) [許可（Allowed）] をクリックします。

ステップ 4 [Username] および [Password] フィールドに、IPAM ログイン情報を入力します。

ステップ 5 [Provider] ロップダウンリストからプロバイダーを選択します。

（注） [BlueCat] をプロバイダとして選択した場合は、自分のユーザーに、BlueCat アドレスマネージャの API アクセスが許可されていることを確認します。1 人または複数のユーザーの API アクセスを設定する方法に関する詳細については、**BlueCat** のマニュアルを参照してください。

Cisco DNA Center を連邦情報処理標準（FIPS）モードの BlueCat と統合するには、BlueCat 9.3.0 を使用します。

ステップ 6 [View] ドロップダウンリストから、デフォルトの IPAM ネットワークビューを選択します。専用ビューが 1 つ設定されている場合、[default] のみがドロップダウンリストに表示されます。ネットワークビューが IPAM で作成され、IP アドレスプールのコンテナとして使用されます。

ステップ 7 [**保存（Save**）] をクリックします。

次のタスク

証明書が正常に追加されたことを確認するには、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Trusted Certificates]** に移動します。

（注） 信頼できる証明書では、証明書はサードパーティの信頼できる証明書として参照されます。

[System] > **[System 360]**に移動し、外部 IP アドレスマネージャ設定が正常に完了したことを確認します。

Webex 統合の設定

Cisco DNA Center はクライアント 360 の Webex 会議セッション情報を提供します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Webex Integration]** の順に選択します。

ステップ 2 [Authenticate to Webex] をクリックします。

ステップ 3 [Cisco Webex] ポップアップウィンドウで、電子メールアドレスを入力し、[Sign In] をクリックします。

ステップ 4 パスワードを入力し、[Sign In] をクリックします。

Webex 認証が正常に完了します。

ステップ 5 [Default Email Domain for Webex Meetings Sign-In] で、Webex ユーザーの電子メールドメインを入力し、[Save] をクリックします。

Webex ドメインは組織全体に適用され、ドメインを使用するすべてのユーザーが会議を主催したり会議に参加したりできます。

ステップ 6 （任意） [Authentication Token] で、[Delete] をクリックして Webex 認証を削除します。

AppX MS-Teams 統合の構成

アクティブ化すると、Cisco DNA Center のアプリケーション 360 ダッシュボードとクライアント 360 ダッシュボードに通話品質メトリック情報が表示されます。

始める前に

管理者権限を付与された Microsoft Teams アカウントが必要です。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[System]** > **[Settings]** > **[External Services]** > **[Cisco DNA - Cloud]** の順に選択します。

ステップ 2 [Region] ドロップダウンリストから目的の地域を選択します。

ステップ 3 アイコンをクリックし、名前で検索して、[AppX MS-Teams] を見つけます。

ステップ 4 [Activate] をクリックします。

[Cisco DNA - Cloud] ウィンドウにリダイレクトされます。

ステップ 5 [Cisco DNA - Cloud] ウィンドウで、次の手順を実行します。

a) cisco.com ログイン情報を使用して [Cisco DNA - Cloud]https://dna.cisco.com/にログインします。

cisco.com ログイン情報がない場合は、作成することができます。

b) [Activate application on your product] ウィンドウで、同意フローリンクをクリックして、次の手順を実行します。

- [Sign in to your account] ウィンドウで、Microsoft 管理者のユーザー名とパスワードを入力し、[Sign In] をクリックします。

- [承認（Accept）] をクリックします。

c) [Activate application on your product] ウィンドウで、アクティブ化する製品を選択し、[Next] をクリックします。

新しい製品を登録するには、**こちら**のリンクをクリックして、次の手順を実行します。

- [Host name/IP] フィールドに、製品の IP アドレスを入力します。
- [Product Name] フィールドに、製品の名前を入力します。
- [Type] フィールドに、製品のタイプを入力します。
- [Register] をクリックします。

d) Cisco DNA - Cloud が Cisco DNA Center と自動的に同期します。その後、[Choose the Scope for your Cisco DNA Center] ウィンドウにリダイレクトされます。 [Next] をクリックします。

e) [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

f) [Activate] をクリックします。
Cisco DNA Center に再びリダイレクトされます。

（注） 製品を非アクティブ化するか、AppX MS-Teams アプリケーションから接続解除する場合は、Cisco DNA - Cloud を使用した AppX MS-Teams 統合の構成 （34 ページ）を参照してください。

Cisco DNA - Cloud を使用した AppX MS-Teams 統合の構成

次の手順を使用して、Cisco DNA - Cloud サービスを介したデバイスでの MS-Teams 統合のステータスをアクティブ化、非アクティブ化、またはチェックします。

始める前に

管理者権限を付与された Microsoft Teams アカウントが必要です。

ステップ 1 cisco.com ログイン情報を使用して [Cisco DNA - Cloud]https://dna.cisco.com/にログインします。

cisco.com ログイン情報がない場合は、作成することができます。

ステップ 2 左上隅にあるメニューアイコンをクリックして、**アプリケーションと製品**。

ステップ 3 [Region] ドロップダウンリストから目的の地域を選択します。

ステップ 4 🔍 アイコンをクリックし、名前で検索して、[AppX MS-Teams] を見つけます。

ステップ 5 [AppX MS-Teams] タイルで、[Activate] をクリックします。詳細については、AppX MS-Teams 統合の構成（33 ページ）を参照してください。

ステップ 6 製品がアクティブ化されたら、[Exit] をクリックします。

ステップ 7 [Applications] ウィンドウにリダイレクトされます。

ステップ 8 [AppX MS-Team] タイルをクリックして、[App 360] ウィンドウに詳細を表示します。

ステップ 9 （オプション）[App 360] ウィンドウから製品をアクティブ化するには、次の手順を実行します。

a) [Product Activations] テーブルで、[Add] をクリックします。

b) アクティブ化する製品を選択し、[Next] をクリックします。

（注） 一度に複数の製品を選択することはできません。

c) [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。それ以外の場合は、[Activate] をクリックします。

ステップ 10 （オプション）製品を非アクティブ化するには、次の手順を実行します。

a) [AppX MS-Teams] タイルをクリックします。

b) [Product Activations] テーブルで、非アクティブ化する製品の横にあるチェックボックスをオンにします。

c) [More Action] ドロップダウンリストから、[Deactivate] を選択します。

d) 確認ウィンドウで、[Deactivate] をクリックします。

ステップ 11 （オプション）AppX MS-Teams アプリケーションから製品の接続を解除するには、次の手順を実行します。

a) [AppX MS-Teams] タイルをクリックして、[App 360] ウィンドウに詳細を表示します。

b) 上部のメニューバーで、[View all details] をクリックします。
[Details] slide-in pane が表示されます。

c) [Disconnect now] をクリックします。

ThousandEyes の統合の構成

外部 ThousandEyes API エージェントと通信するように Cisco DNA Center を構成して、認証トークンを使用して ThousandEyes の統合を有効にできます。統合後、Cisco DNA Center はアプリケーション ヘルス ダッシュボードに ThousandEyes エージェントのテストデータを提供します。

ThousandEyes 統合を機能させるには、デバイスに ThousandEyes エージェントを展開する際に、[Provision] > [Network Devices] > [Inventory] テーブルの [Device Name] と同様のエージェントホスト名を設定する必要があります。

始める前に

Cisco Catalyst 9300 および 9400 シリーズスイッチをサポートするアプリケーション ホスティングを介して ThousandEyes エージェントを展開したことを確認します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[External Services]** > **[ThousandEyes Integration]** の順に選択します。

ステップ 2 [Insert new token here] フィールドに、認証トークンを入力します。

（注） OAuth ベアラートークンを受け取るには、[ThousandEyes] ページに移動します。https://app.thousandeyes.com/

ステップ 3 [Save] をクリックします。

ThousandEyes が有効になっています。

ステップ 4 （オプション）[Delete] をクリックして、OAuth ベアラートークンを削除します。

デバッグログの設定

サービスの問題のトラブルシューティングに役立てるために、Cisco DNA Center サービスのログレベルを変更できます。

ログレベルによって、ログファイルでキャプチャされるデータ量が違います。各ログレベルは累積的です。つまり、各レベルには、指定されたレベル以上のレベルで生成されたデータがあれば、すべて含まれます。たとえば、ログレベルを [Info] に設定すると、[Warn] および [Error] ログもキャプチャされます。より多くのデータをキャプチャして、問題のトラブルシューティングに役立つようにログレベルを調整することをお勧めします。たとえば、ログレベルを調整することで、より多くのデータをキャプチャし、根本原因分析または RCA サポートファイルで確認できるようになります。

サービスのデフォルトのログレベルには情報提供（[Info]）が含まれています。情報提供からのログレベルを、さまざまなログレベル（[Debug] または [Trace]）に変更して、より詳細な情報をキャプチャできます。

注意 開示される可能性がある情報のタイプによっては、[Debug] レベル以上で収集されたログでアクセスを制限する必要があります。

（注） ログファイルが作成されると Cisco DNA Center ホストの一元的な場所に保存され、GUI で表示されます。この場所から、Cisco DNA Center は、GUI（**[System]** > **[System 360]** > **[Log Explorer]**）でログを照会して表示できます。ログは、過去 2 日間のクエリにのみ使用できます。2 日以上経過したログは、この場所から自動的に消去されます。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[System Configuration]** > **[Debugging Logs]** の順に選択します。

[Debugging Logs] ウィンドウが表示されます。

ステップ 2 [Service] ドロップダウンリストからサービスを選択し、そのログレベルを調節します。

[Service] ドロップダウンリストには、現在 Cisco DNA Center に設定され、実行中のサービスが表示されます。

ステップ 3 [Logger Name] を入力します。

これは、ロギングフレームワークにメッセージを出力するソフトウェアコンポーネントを制御するために追加された高度な機能です。この機能を使用する際は、十分注意してください。この機能を誤用すると、テクニカルサポートのために必要な情報が失われる可能性があります。ログメッセージは、ここで指定されたロガー（パッケージ）に対してのみ書き込まれます。デフォルトでは、ロガー名には *com.cisco* で始まるパッケージが含まれています。追加のパッケージ名はカンマ区切り値として入力できます。明示的に指示されていない限り、デフォルト値は削除しないでください。* を使用すると、すべてのパッケージがログに記録されます。

ステップ 4 [Logging Level] ドロップダウンリストで、サービスの新しいログレベルを選択します。

Cisco DNA Center では次のログレベルがサポートされています（詳細は以下、降順）。

- [Trace]：トレースメッセージ
- [Debug]：デバッグメッセージ
- [Info]：正常だが重要な状態メッセージ
- [Warn]：警告状態メッセージ
- [Error]：エラー状態メッセージ

ステップ 5 [Time Out] フィールドで、ログレベルの期間を選択します。

ログレベルの期間を 15 分単位で設定します（～無制限）。期間を無制限に指定する場合、トラブルシューティング作業が完了するたびに、デフォルトのログレベルをリセットする必要があります。

ステップ 6 選択内容を確認し、[Save] をクリックします。

ネットワークの再同期間隔の設定

[System] > **[Settings]** > **[Network Resync Interval]** の順に選択すると、グローバルレベルですべてのデバイスのポーリング間隔を更新できます。また、[Device Inventory] を選択すると、デバイスレベルで特定のデバイスのポーリング間隔を更新できます。[Network Resync Interval] を使用してポーリング間隔を設定すると、その値が [Device Inventory] ポーリング間隔値よりも優先されます。

始める前に

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

- インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[Network Resync Interval]** の順に選択します。

ステップ 2 [Resync Interval] フィールドに、新しい時間値（分）を入力します。

ステップ 3 （オプション）すべてのデバイスに対して設定された既存のポーリング間隔をオーバーライドする場合は、[Override for all devices] チェックボックスをオンにします。

ステップ 4 [Save] をクリックします。

監査ログの表示

監査ログは、Cisco DNA Centerで実行されているさまざまなアプリケーションに関する情報を取得します。さらに、監査ログは、デバイス Public Key Infrastructure（PKI）通知についての情報も取得します。これらの監査ログの情報は、アプリケーションまたはデバイス CA 証明書に関連する問題（ある場合）のトラブルシューティングを支援するために使用できます。

監査ログは、発生したシステムイベント、発生した場所、開始したユーザーを記録するシステムでもあります。監査ログを使用すると、監査用の別のログファイルにシステムの設定変更が記録されます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Activities]** > **[Audit Logs]** の順に選択します。

[Audit Logs] ウィンドウが開きます。このウィンドウで、ネットワーク内の現在のポリシーに関するログを表示できます。これらのポリシーは、Cisco DNA Center にインストールされているアプリケーションによってネットワークデバイスに適用されます。

ステップ 2 タイムラインスライダをクリックして、ウィンドウに表示するデータの時間範囲を次のとおり指定します。

1. [Time Range] 領域で、[Last 2 Weeks]、[Last 7 Days]、[Last 24 Hours]、または [Last 3 Hours] の時間範囲を選択します。
2. カスタム範囲を指定するには、[日付（By date）] をクリックし、開始日時と終了日時を指定します。
3. [Apply] をクリックします。

ステップ 3 対応する子監査ログを表示するには、監査ログの横にある矢印をクリックします。

各監査ログは、いくつかの子監査ログの親になることができます。矢印をクリックすると、一連の追加の子監査ログを表示できます。

（注） 監査ログは、Cisco DNA Center によって実行されたタスクに関するデータをキャプチャします。子監査ログは、Cisco DNA Center によって実行されたタスクのサブタスクです。

ステップ 4 （任意）左側のペインに表示された監査ログのリストで特定の監査ログメッセージをクリックします。右側のペインで **[イベント ID（Event ID）]** > **[イベント ID をクリップボードにコピー（Copy Event ID to Clipboard）]** をクリックします。コピーされた ID を API で使用すると、イベント ID に基づく監査ログメッセージを取得できます。

監査ログの右側のペインに各ポリシーの **[説明（Description）]**、**[ユーザー（User）]**、**[インターフェイス（Interface）]**、**[宛先（Destination）]** が表示されます。

（注） 監査ログには、ペイロード情報を含むPOST、DELETE、PUTなどのノースバウンド操作の詳細と、デバイスにプッシュされた設定などのサウスバウンド操作の詳細が表示されます。Cisco DevNet の API の詳細については、『CISCO DNA Center PlatformIntent APIs』を参照してください。

ステップ 5 （任意）[Filter] をクリックして、[User ID]、[Log ID]、または [Description] でログをフィルタリングします。

ステップ 6 [Subscribe] をクリックして監査ログイベントを登録します。

syslog サーバーのリストが表示されます。

ステップ 7 登録する syslog サーバーのチェックボックスをオンにし、[Save] をクリックします。

（注） 監査ログイベントの登録を解除するには、syslog サーバーのチェックボックスをオフにして [Save] をクリックします。

ステップ 8 右側のペインで、[Search] フィールドを使用して、ログメッセージ内の特定のテキストを検索します。

ステップ 9 左上隅にあるメニューアイコンをクリックして、**[Activities]** > **[Scheduled Tasks]** で、OS の更新やデバイスの交換などの予定、進行中、完了および失敗の管理タスクを確認します。

ステップ 10 左上隅にあるメニューアイコンをクリックして、**[Activities]** > **[Work Items]** タブで、進行中、完了、および失敗の作業項目を確認します。

Syslog サーバーへの監査ログのエクスポート

セキュリティに関する推奨事項：より安全で簡単なログモニタリングのために、監査ログを Cisco DNA Center からネットワーク内のリモート Syslog サーバーにエクスポートすることを強く推奨します。

syslog サーバーを複数登録することで、監査ログを Cisco DNA Center から複数の syslog サーバーにエクスポートできます。

始める前に

[System] > **[Settings]** > **[External Services]** > **[Destinations]** > **[Syslog]** 領域で syslog サーバーを設定します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Activities]** > **[Audit Logs]** の順に選択します。

ステップ 2 [**Subscribe**] をクリックします。

ステップ 3 登録する syslog サーバーを選択し、[Save] をクリックします。

ステップ 4 （任意） 登録を解除するには、syslog サーバーの選択を解除し、[Save] をクリックします。

API を使用した Syslog サーバーでの監査ログの表示

Cisco DNA Center プラットフォーム では、API を使用して Syslog サーバーの監査ログを表示できます。[Developer Toolkit] の [Create Syslog Event Subscription] API を使用して、監査ログイベントの syslog サブスクリプションを作成できます。

監査ログイベントが発生するたびに、Syslog サーバーで監査ログイベントがリストされます。

設定の可視性と制御の有効化

[Visibility and Control of Configurations] 機能は、計画したネットワーク構成をデバイスに展開する前にセキュリティを強化するソリューションを提供します。優れた可視化機能により、デバイス構成を展開する前にプレビューできます（CLI および NETCONF コマンドを使用）。可視化機能はデフォルトで有効になっています。可視化機能が有効になっている場合は、確認するまでデバイス設定を展開できません。強化された制御により、計画されたネットワーク設定を IT サービス管理（ITSM）に送信して承認できます。制御が有効になっている場合は、IT 管理者が承認するまで設定を展開できません。

（注） タスク展開のスケジュール時に次のバナーメッセージが表示される場合、ワークフローで可視性と制御がサポートされます。

このワークフローでは、ネットワーク管理者などのユーザーがネットワークデバイスにワークフローを展開する前に、設定をプレビューできます。ワークフローを設定するには、**[System]** > **[Settings]** > **[Visibility and Control of Configurations]** に移動します。

始める前に

[ITSM Approval] を有効にできるように、Cisco DNA Center で ITSM が有効になっており、かつ設定されていることを確認します。ITSM を有効にし、設定する方法については、『*Cisco DNA Center ITSM Integration Guide*』の「Configure the Cisco DNA Center Automation Events for ITSM (ServiceNow) Bundle」を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[System]** > **[Settings]** > **[System Configuration]** > **[Visibility and Control of Configurations]** の順に選択します。

ステップ 2 [Configuration Preview] トグルボタンをクリックして、可視性を有効または無効にします。

可視性を有効にした場合、デバイス設定を展開する前にプレビューする必要があります。

可視性を無効にした場合、デバイス設定を展開する前にプレビューを強制されなくなります。可視性が無効になっている場合は、プレビューの要否にかかわらず設定をスケジュールして展開できます。

ステップ 3 （任意） [ITSM Approval] トグルボタンをクリックして制御を有効または無効にします。

制御を有効にした場合、計画したネットワーク構成を展開する前に、ITSM管理者に送信して承認を受ける必要があります。

制御を無効にした場合、計画したネットワーク構成を展開する前の ITSM の承認が不要になります。制御が無効になっている場合、ITSM の承認なしで設定を展開できます。

タスクと作業項目の表示

Cisco DNA Center で、実行中のタスクと作業項目、完了したタスクと作業項目、および失敗したタスクと作業項目に関する情報を表示できます。

タスクは、ユーザーまたはシステムがスケジュール設定した操作であり、繰り返される可能性があります。タスクがある場合、これは、スケジュールどおりに展開するために完了する必要がある対応する作業項目がないことを意味します。

ハイ アベイラビリティ

VMware vSphere 高可用性（HA）は、同じ vSphere クラスタ内の仮想マシンとそのホストをリンクすることで、ESXi 上の Cisco DNA Center に高可用性を提供します。vSphere HA が機能するには、共有ストレージが必要です。ホストに障害が発生すると、仮想マシンが代替ホストで再起動します。vSphere HA はその設定に基づいて障害に対応し、vSphere HA は次のレベルで障害を検出します。

- ホストレベル
- 仮想マシン（VM）レベル
- アプリケーションレベル

現在のリリースでは、Cisco DNA Center はホストレベルの障害に対する高可用性のみをサポートします。

ホストレベルの障害に対する VMware vSphere の設定

ホストレベルの障害に対して vSphere HA を設定するには、次の手順を実行します。

始める前に

Cisco DNA Center 仮想アプライアンスが、障害が発生したホストを引き継ぐには、少なくとも 2 つのホストに、*ESXi 上の Cisco DNA Center リリースノート* で説明されている未予約の CPU/メモリリソースが必要です。

（注） Cisco DNA Center 仮想アプライアンスに、障害が発生したホストを引き継ぐための十分なリソースを確保するために、適切な設定で**HA アドミッションコントロール**を有効にします。この設定では、システムに影響を与えることなく仮想アプライアンスを別のホストで再起動できるようにする必要があります。必要なリソースが予約されていない場合、リソース不足のために、フェールオーバーホストで再起動した仮想アプライアンスに障害が発生する可能性があります。

ステップ 1 vSphere クライアントにログインします。

ステップ 2 デバイスメニューで適切な Cisco DNA Center クラスタを選択します。

ステップ 3 クラスタを設定するには、**[Configure]** > **[Services]** > **[vSphere Availability]** を選択します。

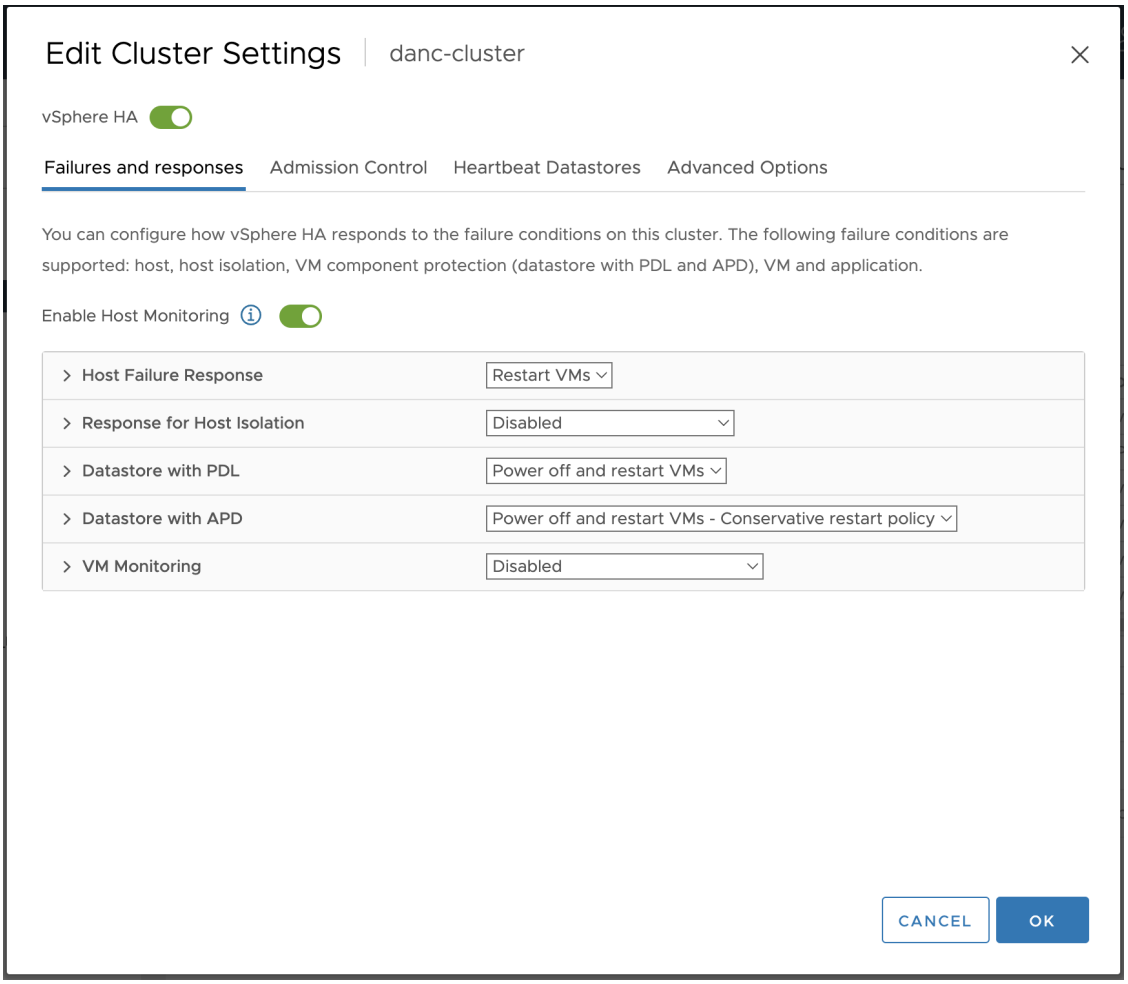
ステップ 4 右上隅の [Edit] をクリックします。

ステップ 5 トグルボタンをクリックして **vSphere HA** を有効にします。

ステップ 6 [Failures and responses] を選択し、次の設定を指定します。

a) トグルボタンをクリックして**ホストモニタリング**を有効にします。

b) [Host Failure Response] ドロップダウンリストに移動し、[Restart VMs] を選択します。



ステップ 7 [OK] をクリックします。

ESXi 上の Cisco DNA Center 仮想マシンの優先再起動の設定

ホスト障害時に ESXi 上の Cisco DNA Center 仮想アプライアンスが優先的に再起動するようにするには、次の手順を実行します。

ステップ 1 vSphere クライアントにログインします。

ステップ 2 デバイスメニューで適切な ESXi 上の Cisco DNA Center クラスタを選択します。

ステップ 3 クラスタを設定するには、**[Configure]** > **[VM Overrides]** > **[ADD]** を選択します。

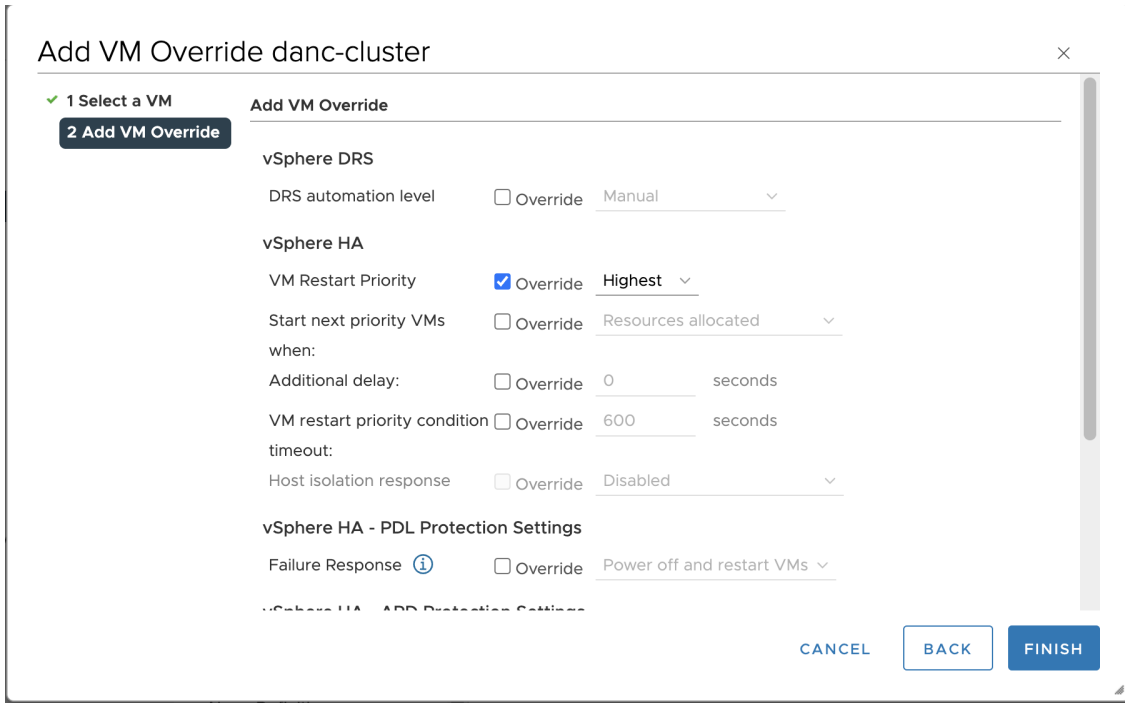
ステップ 4 [Select a VM] ウィンドウで、展開済みの ESXi 上の Cisco DNA Center 仮想マシンを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 [Add VM Override] ウィンドウで、**[vSphere HA]** > **[VM Restart Priority]** に移動し、次の設定を指定します。

a) [Override] チェックボックスにマークを付けます。

b) ドロップダウンリストから、[Highest] を選択します。



ステップ 7 [FINISH] をクリックします。

VMware vSphere 製品に関する資料

ESXi 上の Cisco DNA Center は、 VMware vSphere HA 機能を通じて高可用性をサポートします。vSphere HA クラスタを作成および使用するための VMware vSphere の実装と要件については、次の VMware vSphere 製品ドキュメント を参照してください。

- VMware High Availability の製品データシート（PDF）
- 『VMware Infrastructure: Automating High Availability (HA) Services with VMware HA』（PDF）
- 「How vSphere HA Works」（HTML）
- 「vSphere HA Checklist」（HTML）

統合設定の設定

ファイアウォールなどのルールが、Cisco DNA Center と Cisco DNA Center プラットフォーム と通信する必要があるサードパーティ製アプリケーションの間に存在する場合は、[Integration Settings] を設定する必要があります。Cisco DNA Center の IP アドレスが、インターネットや外部ネットワークに接続する別の IP アドレスに内部的にマッピングされる場合には、このような事例が発生します。

重要 Cisco DNA Center のバックアップおよび復元後、[Integration Settings] ページにアクセスし、（必要に応じて）次の手順を使用して [Callback URL Host Name] または [IP Address] を更新する必要があります。

始める前に

Cisco DNA Center プラットフォーム をインストールしておきます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[System]** > **[設定]** > **[Integration Settings]** の順に選択します。

ステップ 2 サードパーティ製アプリケーションが Cisco DNA Center プラットフォームと通信するときに接続する必要がある [Callback URL Host Name] または [IP Address] を入力します。

（注） [Callback URL Host Name] または [IP Address] は、Cisco DNA Center に内部的にマッピングされている外部向けホスト名または IP アドレスです。3 ノードクラスタセットアップの VIP アドレスを設定します。

ステップ 3 [Apply] をクリックします。

ログインメッセージの設定

Cisco DNA Center にログインしたすべてのユーザーに表示されるメッセージを設定できます。

始める前に

SUPER-ADMIN-ROLE またはシステム管理権限を持つ **CUSTOM-ROLE** のユーザーのみがこの手順を実行することができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[System Configuration]** > **[Login Message]** の順に選択します。

ステップ 2 [Login Message] テキストボックスにメッセージを入力します。

ステップ 3 [保存（**Save**）] をクリックします。

このメッセージは、Cisco DNA Center ログインページの [Log In] ボタンの下に表示されます。

後でこのメッセージを削除する場合は、次の手順を実行します。

1. [Login Message Settings] ページに戻ります。

2. [Clear] をクリックし、[Save] をクリックします。

プロキシの設定

ESXi 上の Cisco DNA Center と管理しているネットワークデバイスとの間の仲介として設定されているプロキシサーバーがある場合は、プロキシサーバーへのアクセスを設定する必要があります。

（注） ESXi 上の Cisco DNA Center は、Windows New Technology LAN Manager（NTLM）認証を使用するプロキシサーバーをサポートしていません。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザーのみがこの手順を実行することができます。詳細については、ユーザ ロールの概要 （77 ページ）を参照してください。

ステップ 1 **[System]** > **[Settings]** > **[System Configuration]** 左上隅にあるメニューアイコンをクリックして、。

ステップ 2 [System Configuration] ドロップダウンリストから、**[Proxy]** > **[Outgoing Proxy]**を選択します。

ステップ 3 プロキシ サーバーの URL アドレスを入力します。

ステップ 4 プロキシサーバーのポート番号を入力します。

（注）
- HTTP の場合、ポート番号は通常 80 です。
- ポート番号の範囲は 0 ～ 65535 です。

ステップ 5 （オプション）プロキシサーバーが認証を必要とする場合、[Update] をクリックして、プロキシサーバーにアクセスするためのユーザー名とパスワードを入力します。

ステップ 6 [Validate Settings] チェックボックスをオンにし、適用時に ESXi 上の Cisco DNA Center でプロキシ構成時の設定が検証されるようにします。

ステップ 7 選択内容を確認し、[Save] をクリックします。

選択内容をキャンセルするには、[Reset] をクリックします。既存のプロキシ設定を削除するには、[Delete] をクリックします。

プロキシを設定した後、[Proxy] ウィンドウに設定を表示できます。

重要 ESXi 上の Cisco DNA Center サービスがプロキシサーバーの設定で更新されるまでに最大 5 分かかることがあります。

セキュリティに関する推奨事項

Cisco DNA Centerは、それ自体とモニターおよび管理対象のホスト/ネットワークデバイス用の多数のセキュリティ機能を提供します。セキュリティ機能は、明確に理解して、正しく設定する必要があります。次のセキュリティに関する推奨事項に従うことを強く推奨します。

- Cisco DNA Center は、プライベート内部ネットワーク内、およびインターネットなどの信頼できないネットワークに対して Cisco DNA Center を開いていないファイアウォールの背後に導入してください。
- 管理ネットワークとエンタープライズネットワークが個別にある場合は、Cisco DNA Center の管理インターフェイスとエンタープライズインターフェイスをそれぞれ管理ネットワークとエンタープライズ ネットワークに接続してください。これにより、Cisco DNA Center の管理に使用されるサービスと、ネットワークデバイスとの通信および管理に使用されるサービスとの間で確実にネットワーク分離が行われます。
- 3 ノードクラスタセットアップで Cisco DNA Center を展開する場合は、クラスタインターフェイスが分離されたネットワークに接続されていることを確認してください。
- パッチのアナウンス後できる限り早急に、セキュリティパッチを含む重要なアップグレードで Cisco DNA Center をアップグレードしてください。詳細については、『Cisco DNA CenterUpgrade Guide』を参照してください。
- HTTPS プロキシサーバーを使用する Cisco DNA Center によってアクセスされるリモート URL を制限してください。Cisco DNA Center は、インターネット経由でアクセスして、ソフトウェアアップデート、ライセンス、デバイスソフトウェアをダウンロードしたり、最新のマップ情報、ユーザーフィードバックなどを提供したりするように設定されています。これらの目的でインターネット接続を提供することは必須要件です。ただし、HTTPS プロキシサーバーを介して安全な接続を提供します。
- 既知の IP アドレスおよび範囲のみを許可し、未使用のポートへのネットワーク接続をブロックすることにより、ファイアウォールを使用した Cisco DNA Center への入力および出力管理とエンタープライズ ネットワーク接続を制限してください。
- Cisco DNA Center の自己署名サーバー証明書を、内部認証局（CA）によって署名された証明書に置き換えてください。
- 使用しているネットワーク環境で可能な場合は、SFTP 互換モードを無効にします。このモードでは、レガシー ネットワーク デバイスが古い暗号スイートを使用して Cisco DNA Center に接続できます。
- ブラウザベースのアプライアンス設定ウィザードを無効にします。このウィザードには、自己署名証明書が付属しています。

プロキシ証明書の設定

ネットワーク構成によっては、プロキシゲートウェイは、Cisco DNA Center と管理するリモートネットワーク（さまざまなネットワークデバイスを含む）の間に存在する可能性があります。80 や 443 などの一般的なポートは DMZ のゲートウェイプロキシを通過します。このため、Cisco DNA Center 用に設定されたネットワークデバイスからの SSL セッションは、プロキシゲートウェイで終了することになります。したがって、これらのリモートネットワーク内にあるネットワークデバイスは、プロキシゲートウェイ経由でのみ Cisco DNA Center と通信できます。ネットワークデバイスが Cisco DNA Center または、（存在する場合は）プロキシゲートウェイと安全で信頼できる接続を確立するため、ネットワークデバイスは、関連する CA ルート証明書で、または特定の状況ではサーバー独自の証明書を使って、適切にプロビジョニングされた PKI トラストストアを保有する必要があります。

PnP 検出/サービスによってデバイスのオンボード中にそのようなプロキシが配置されている場合は、ネットワークデバイスが安全に Cisco DNA Center を信頼および認証できるように、プロキシと Cisco DNA Center サーバー証明書を同一にすることを推奨します。

プロキシゲートウェイが Cisco DNA Center と管理対象のリモートネットワークの間に存在するネットワークトポロジでは、次の手順を実行してプロキシゲートウェイ証明書を Cisco DNA Center にインポートします。

始める前に

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。
- Cisco DNA Center とそのサービスに到達するプロキシゲートウェイの IP アドレスを使用する必要があります。
- プロキシゲートウェイで現在使用されている証明書ファイルを持っている必要があります。証明書ファイルの内容は、次のいずれかで構成されている必要があります。
  - PEM または DER 形式のプロキシゲートウェイの証明書、および自己署名された証明書。
  - PEM または DER 形式のプロキシ ゲートウェイの証明書、および有効な既知の CA によって発行された証明書。
  - PEM または DER 形式のプロキシ ゲートウェイの証明書とそのチェーン。

デバイスとプロキシゲートウェイで使用される証明書は、次の手順に従って、Cisco DNA Center にインポートする必要があります。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[System Configuration]**の順に選択します。

ステップ 2 [System Configuration] ドロップダウンリストから、**[Proxy]** > **[Incoming Proxy]** を選択します。

ステップ 3 [Proxy Certificate] ウィンドウで、（存在する場合は）現在のプロキシゲートウェイ証明書のデータを表示します。

（注） [Expiration Date and Time] は、グリニッジ標準時（GMT）値で表示されます。証明書有効期限の 2 ヵ月前に、Cisco DNA Center の GUI にシステム通知が表示されます。

ステップ 4 プロキシゲートウェイ証明書を追加するには、自己署名証明書または CA 証明書を [Drag and Drop Here] 領域にドラッグアンドドロップします。

（注） PEM または DER ファイル（公開キー暗号化標準のファイル形式）だけが、この領域を使用して Cisco DNA Center にインポートできます。さらに、この手順には秘密キーは必要ではなく、Cisco DNA Center にアップロードもされません。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 [Proxy Certificate] ウィンドウを更新し、更新されたプロキシゲートウェイ証明書のデータを表示します。[Proxy Certificate] ウィンドウに表示された情報は、新しい証明書名、発行者、および証明機関を反映するように変更する必要があります。

ステップ 7 プロキシゲートウェイ証明書の機能を有効にするには、[Enable] ボタンをクリックします。

[Enable] ボタンをクリックすると、プロキシゲートウェイからの要求時にコントローラがインポートされたプロキシゲートウェイ証明書を返します。[Enabled] ボタンをクリックしない場合、コントローラは独自の自己署名証明書またはインポートされた CA 証明書をプロキシゲートウェイに返します。

プロキシゲートウェイ証明書の機能が使用されている場合、[Enable] ボタンはグレー表示されます。

SSL インターセプトプロキシ証明書のアップロード

Cisco DNA Center とソフトウェアアップデートのダウンロード元である Cisco Cloud との間に設定されたプロキシサーバーで SSL 復号が有効になっている場合、正式な認証局から発行された証明書を使用してプロキシが構成されていることを確認してください。プライベート証明書を使用している場合は、次の手順を実行します。

（注） セキュリティを強化するため、ルートシェルへのアクセスは Cisco DNA Center で無効になっています。制限付きシェルでは、ユーザーは基礎となるオペレーティングシステムとファイルシステムにアクセスできないため、運用上のリスクが軽減されます。ただし、このセクションのコマンドを使用するには、Cisco TACに連絡して、ルートシェルに一時的にアクセスする必要があります。 制限付きシェルについて （64 ページ）を参照してください。

ステップ 1 プロキシサーバーの証明書（.pem 形式）を Cisco DNA Center サーバーのディレクトリに転送します。

ステップ 2 maglev ユーザーとして Cisco DNA Center サーバーに SSH で接続し、次のコマンドを入力します。<*directory*> は証明書ファイルの場所、<*proxy.pem*> はプロキシサーバーの TLS/SSL 証明書ファイルです。

```
$ sudo /usr/local/bin/update_cacerts.sh -v -a /<directory>/<proxy.pem>
```

このコマンドは、次のような出力を返します。

```
Reading CA cert from file /tmp/sdn.pem
Adding certificate import_1E:94:6D:2C:81:22:BB:B2:2E:24:BD:72:57:AE:35:AD:EC:5E:71:44.crt
Updating /etc/ca-certificates.conf
Updating certificates in /etc/ssl/certs…
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d…
done.
Deleting tempfiles /tmp/file0PpQxV /temp/filePtmQ8U /tmp/filercR3cV
```

ステップ 3 コマンド出力で、「1 added」の行を探し、追加された数がゼロでないことを確認します。チェーン内の証明書に基づき、この数は 1 または 1 を超える場合があります。

ステップ 4 次のコマンドを入力して、docker およびカタログサーバーを再起動します。

```
sudo systemctl restart docker
magctl service restart -d catalogserver
```

ステップ 5 Cisco DNA Center GUI にログインし、次の手順を実行します。

a) **[System]** > **[Settings]** > **[Trust & Privacy]** > **[Trusted Certificates]** に移動し、同じ証明書をアップロードします。詳細については、信頼できる証明書の設定 （63 ページ）を参照してください。

b) クラウド接続とC MX/Spaces 接続を確認します。

証明書および秘密キーのサポート

Cisco DNA Center は、セッション（HTTPS）の認証に使用される認証局管理機能をサポートしています。これらのセッションでは、CA と呼ばれる一般に認められた信頼されたエージェントを使用します。Cisco DNA Center は、認証局管理機能を使用して、内部 CA から X.509 証明書をインポートして保存し、管理します。インポートされた証明書は Cisco DNA Center のアイデンティティ証明書になり、Cisco DNA Center は認証のためにこの証明書をクライアントに提示します。クライアントは、ノースバウンド API アプリケーションとネットワークデバイスです。

Cisco DNA Center GUI を使用して次のファイルを（PEM または PKCS ファイル形式で）インポートできます。

- X.509 証明書
- 秘密キー（Private key）

（注） 秘密キーについては、Cisco DNA Center で RSA キーのインポートをサポートしています。ユーザー自身のキー管理システムで秘密キーを保護してください。秘密キーのモジュラスサイズは最小でも 2048 ビット必要です。

Cisco DNA Center 2.3.4.x 以前の場合、DSA、DH、ECDH、および ECDSA キータイプはサポートされていないため、インポートしないでください。Cisco DNA Center 2.3.4.x 以前では、証明書チェーンに関連付けられたリーフ証明書を含む ECDH および ECDSA の形式はサポートされません。

Cisco DNA Center 2.3.5 以降では、すべてのキータイプがサポートされます。

インポートする前に、内部 CA で発行された有効な X.509 証明書と秘密キーを取得する必要があります。証明書は所有する秘密キーに対応している必要があります。インポートすると、X.509 証明書と秘密キーに基づくセキュリティ機能が自動的にアクティブ化されます。Cisco DNA Center は証明書を、要求するデバイスまたはアプリケーションに提示します。ノースバウンド API アプリケーションとネットワークデバイスでは、これらのログイン情報を使用して Cisco DNA Center との信頼関係を確立できます。

（注） 自己署名証明書を使用したり、Cisco DNA Center にインポートしたりすることは推奨されません。内部 CA から有効な X.509 証明書をインポートすることをお勧めします。さらに、プラグアンドプレイ機能を正常に動作させるには、自己署名証明書（デフォルトで Cisco DNA Center にインストールされている）を、内部 CA によって署名された証明書に置き換える必要があります。

Cisco DNA Center は一度に 1 つのインポート済み X.509 証明書および秘密キーだけをサポートします。2 つ目の証明書および秘密キーをインポートすると、最初の（既存の）インポート済み証明書および秘密キーの値が上書きされます。

証明書チェーンのサポート

Cisco DNA Center では、GUI を介して証明書と秘密キーをインポートできます。Cisco DNA Center にインポートされる証明書（署名された証明書）につながる証明書チェーンに含まれる下位証明書がある場合は、それらの下位証明書とそれらの下位 CA のルート証明書が一緒に、インポートされる単一のファイルに追加される必要があります。これらの証明書を追加する場合は、認定の実際のチェーンと同じ順序で追加する必要があります。

次の証明書は、単一の PEM ファイルに一緒に貼り付ける必要があります。証明書のサブジェクト名と発行元を調べて、正しい証明書がインポートされ、正しい順序が維持されていることを確認してください。また、チェーンに含まれるすべての証明書が一緒に貼り付けられていることを確認してください。

- [Signed Cisco DNA Center certificate]：件名フィールドに CN=<*FQDN of Cisco DNA Center*> が含まれていて、発行元が発行機関の CN を持っている。

（注） 内部認証局（CA）による署名入りの証明書をインストールする場合は、Cisco DNA Center へのアクセスに使用するすべての DNS 名（Cisco DNA Center の FQDN を含む）が証明書の **alt_names** セクションで指定されていることを確認してください。詳細については、『Cisco DNA Center Security Best Practices Guide』の「Generate a Certificate Request Using Open SSL」を参照してください。

- [Issuing (subordinate) CA certificate that issues the Cisco DNA Center certificate]：件名フィールドに Cisco DNA Center の証明書を発行する（下位）CA の CN が含まれていて、発行元がルート CA の CN である。

- [Next issuing (root/subordinate CA) certificate that issues the subordinate CA certificate]：件名フィールドがルート CA で、発行元が件名フィールドと同じ値である。それらが同じ値でない場合は、その次の発行元を追加していきます。

Cisco DNA Center のサーバー証明書の更新

Cisco DNA Center は、X.509 証明書と秘密キーの Cisco DNA Center へのインポートとストレージをサポートします。インポートをすると、証明書と秘密キーを使用して、Cisco DNA Center、ノースバウンド API アプリケーション、およびネットワーク デバイスの間に安全で信頼できる環境を作成することができます。

GUI の [Certificates] ウィンドウを使用して、証明書と秘密キーをインポートできます。

始める前に

内部認証局によって発行された有効な X.509 証明書を取得します。証明書は、所有している秘密キーに対応している必要があります。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 > **[System]** > **[Settings]** > **[Trust & Privacy]** > **[System Certificate]** の順に選択します。

ステップ 2 [System] タブで、現在の証明書データを確認します。

このウィンドウを最初に表示したときに現在の証明書として表示されるのは、Cisco DNA Center の自己署名証明書のデータです。自己署名証明書の有効期限は、数年先に設定されています。

（注） 有効期限の日時は、グリニッジ標準時（GMT）値で表示されます。証明書有効期限の 2 か月前に、Cisco DNA Center の GUI にシステム通知が表示されます。

[System] タブには次のフィールドが表示されます。

- [Current Certificate Name]：現在の証明書の名前。
- [Issuer]：証明書に署名し、証明書を発行したエンティティの名前。
- [Expires]：証明書の有効期限。

ステップ 3 [System Certificate] ウィンドウで、[Replace Certificate] をクリックします。

初めて CSR を生成する場合、[Generate New CSR] リンクが表示されます。

それ以外の場合は、[Download existing CSR] リンクが表示されます。既存の CSR をダウンロードしてプロバイダーに送信し、証明書を生成できます。既存の CSR を使用しない場合は、[Delete existing CSR] をクリックし、次の [Confirmation] ウィンドウで [Accept] をクリックします。[Generate New CSR] リンクが表示されます。

ステップ 4 [Generate New CSR] リンクをクリックします。

ステップ 5 [Certificate Signing Request Generator] ウィンドウで、必須フィールドに情報を入力します。

ステップ 6 [新規 CSR の生成（Generate New CSR）] をクリックします。

生成された新しい CSR は自動的にダウンロードされます。

[Certificate Signing] ウィンドウには、CSR のプロパティが表示され、次のことができます。

- CSR プロパティをプレーンテキストでコピーします。
- Base64 をコピーし、任意の認証局に貼り付けます。たとえば、Base64 を Microsoft 認証局に貼り付けることができます。
- Base64 をダウンロードします。

ステップ 7 Cisco DNA Center にインポートする証明書のファイル形式タイプを選択します。

- [PEM]：プライバシー強化メールファイル形式
- [PKCS]：公開キー暗号化標準ファイル形式

（注） [Generate New CSR] オプションを選択して証明書を要求した場合、[PKCS] ファイルタイプは無効になります。

ステップ 8 証明書発行元から p7b で証明書の完全なチェーン（サーバーおよびCA）が提供されていることを確認します。不明な場合は、次の手順を実行し、チェーンを確認して組み立てます。

a) p7b バンドルを DER 形式でダウンロードし、dnac-chain.p7b として保存します。
b) dnac-chain.p7b 証明書を Cisco DNA Center クラスタに SSH を介してコピーします。
c) 次のコマンドを入力します。

```
openssl pkcs7 -in dnac-chain.p7b -inform DER -out dnac-chain.pem -print_certs
```

d) すべての証明書が出力に記載され、発行者と Cisco DNA Center 証明書が含まれていることを確認します。PEM としてアップロードを続行します。証明書がルーズファイルにある場合は、次の手順を実行して、個々のファイルをダウンロードして組み立てます。

ステップ 9 証明書発行元からルーズファイルで証明書とその発行元 CA チェーンが提供された場合は、次の手順を実行します。

a) PEM（base64）ファイルを収集するか、openssl を使用して DER を PEM に変換します。
b) 証明書とその発行元 CA を連結し、証明書から下位 CA に続いてルート CA までを dnac-chain.pem ファイルに出力します。次に例を示します。

```
cat certificate.pem subCA.pem rootCA.pem > dnac-chain.pem
```

c) PEM としてアップロードを続行します。

ステップ 10 [PEM] ファイルの場合、次のタスクを実行します。

- [Drag and Drop] 領域にファイルをドラッグアンドドロップして、 [PEM] ファイルをインポートします。

（注） PEM ファイルには、有効な PEM 形式の拡張子（.pem）が必須です。証明書の最大ファイルサイズは 10 MB です。

アップロードに成功すると、システム証明書が検証されます。

- [Drag and Drop] 領域にファイルをドラッグアンドドロップして、[Private Key] をインポートします。

（注） 秘密キーには、有効な秘密キー形式の拡張子（.key）が必須です。秘密キーの最大ファイルサイズは 10 MB です。

アップロードに成功すると、秘密キーが検証されます。

- 秘密キーの [Encrypted] 領域から、暗号化オプションを選択します。
- 暗号化を選択した場合、[Password] フィールドに秘密キーのパスワードを入力します。

ステップ 11 [PKCS] ファイルの場合、次のタスクを実行します。

- [Drag and Drop] 領域にファイルをドラッグアンドドロップして、[PKCS] ファイルをインポートします。

（注） PKCS ファイルには、有効な PKCS 形式の拡張子（.pfx または .p12）が必須です。証明書の最大ファイルサイズは 10 MB です。

アップロードに成功すると、システム証明書が検証されます。

- [Password] フィールドで証明書用のパスフレーズを入力します。

（注） PKCS の場合は、インポートした証明書もパスフレーズを必要とします。

- [秘密キー（Private Key）] フィールドについては、秘密キーの暗号化オプションを選択します。
- [Private Key] フィールドで、暗号化を選択した場合は、[Password] フィールドに秘密キーのパスワードを入力します。

ステップ 12 **[Save]** をクリックします。

（注） Cisco DNA Center サーバーの SSL 証明書が置き換えられると、自動的にログアウトされるため、再度ログインする必要があります。

ステップ 13 [Certificates] ウィンドウに戻り、更新された証明書データを確認します。
[System] タブに表示される情報が更新され、新しい証明書名、発行者、および認証局が反映されます。

外部 SCEP ブローカーの使用

Cisco DNA Center では、ネットワークデバイスへの証明書の登録とプロビジョニングに Simple Certificate Enrollment Protocol（SCEP）が使用されます。独自の SCEP ブローカと証明書サービスを使用したり、外部の SCEP ブローカを使用したりできます。外部 SCEP ブローカをセットアップするには、以下の手順を実行します。

（注） SCEP の詳細については、「Simple Certificate Enrollment Protocol Overview」を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[System]** > **[Settings]** > **[Trust & Privacy]** > **[Certificate Authority]**。

ステップ 2 [Certificate Authority] ウィンドウで、[Use external SCEP broker] オプションボタンをクリックします。

ステップ 3 外部証明書をアップロードするには、次のいずれかのオプションを使用します。

- ファイルを選択する
- ドラッグアンドドロップしてアップロードする

（注） .pem、.crt、.cer などのファイルタイプのみ使用できます。ファイルサイズは 1 MB を超えることはできません。

ステップ 4 [Upload] をクリックします。

ステップ 5 デフォルトでは、[Manages Device Trustpoint] が有効になっています。つまり、デバイスで sdn-network-infra-iwan トラストポイントが設定されます。Cisco DNA Center次の手順を実行してください。

a) デバイスが SCEP 経由で証明書を要求する登録 URL を入力します。

b) （任意）証明書で使用される任意のサブジェクトフィールド（国、地域、州、組織、組織単位など）を入力します。共通名（CN）は、デバイスのプラットフォーム ID とデバイスのシリアル番号を使用して Cisco DNA Center によって自動的に設定されます。

c) [Revocation Check] フィールドで、ドロップダウンリストをクリックし、適切な失効チェックオプションを選択します。

d) （任意）[Auto Renew] チェックボックスをオンにして、自動登録の割合を入力します。

[Manages Device Trustpoint] が無効になっている場合、デバイスが有線およびワイヤレスのアシュアランステレメトリを Cisco DNA Center に送信するようにするため、デバイスに手動で sdn-network-infra-iwan トラストポイントを設定し、証明書をインポートする必要があります。「デバイス証明書トラストポイントの設定」を参照してください。

ステップ 6 [保存（**Save**）] をクリックします。

外部 CA 証明書がアップロードされます。

アップロードされた外部証明書を置き換える場合は、[Replace Certificate] をクリックし、必要な詳細を入力します。

内部認証局への切り替え

外部証明書をアップロードした後、内部証明書に切り替える場合は、次の手順を実行します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[System]** > **[Settings]** > **[Trust & Privacy]** > **[Certificate Authority]**。

ステップ 2 [Certificate Authority] ウィンドウで、[Use Cisco DNA Center] オプションボタンをクリックします。

ステップ 3 [Switching back to Internal Certificate Authority] アラートで、[Apply] をクリックします。

[Settings have been updated] メッセージが表示されます。詳細については、認証局のロールをルートから下位に変更 （57 ページ）を参照してください。

Cisco DNA Center 認証局のエクスポート

Cisco DNA Center では、デバイスを認証するための AAA サーバーまたは Cisco ISE サーバーなどの外部エンティティの設定に必要なデバイス証明書をダウンロードできます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[System]** > **[Settings]** > **[Trust & Privacy]** > **[Certificate Authority]**。

ステップ 2 [Download] をクリックして、デバイス CA をエクスポートし、信頼できる CA として外部エンティティに追加します。

証明書の管理

デバイス証明書の管理

管理対象デバイスがデバイスを認証および識別するために Cisco DNA Center によって発行された証明書を表示および管理できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Device Certificate]** の順に選択します。

[Device Certificate] ウィンドウには、発行された証明書のステータスが個別のステータスタブに表示されます。

- [Expired] ステータスタブ：有効期限が切れた証明書のリストを表示します。
- [Expiring] ステータスタブ：有効期限が近づいている証明書のリストを昇順で表示します。
- [All] ステータスタブ：有効な証明書、期限切れの証明書、および期限切れ間近の証明書のリストを表示します。
- [Revoked] ステータスタブ：取り消された証明書を表示します。

ステップ 2 [Device Name] と [Issue To] の値に基づいて、証明書をフィルタリングできます。

ステップ 3 有効な証明書を取り消す場合は、次の手順を実行します。

a) [All] ステータスタブをクリックします。
b) [Actions] 列で、取り消す証明書に対応する [Revoke] アイコンをクリックします。
c) 確認ウィンドウで、[OK] をクリックします。

ステップ 4 証明書の詳細をエクスポートする場合は、[Export] をクリックします。

証明書の詳細が CSV 形式でエクスポートされます。

デバイス証明書の有効期間の設定

Cisco DNA Center では、Cisco DNA Center のプライベート（内部）CA で管理および監視しているネットワークデバイスの証明書の有効期間を変更できます。Cisco DNA Center での証明書の有効期間のデフォルト値は 365 日です。Cisco DNA Center GUI を使用して証明書の有効期間を変更すると、それ以降に Cisco DNA Center に対して証明書を要求するネットワークデバイスにその有効期間の値が割り当てられます。

（注） デバイス証明書のライフタイム値を CA 証明書のライフタイム値より大きくすることはできません。さらに、CA 証明書の残りの有効期間が設定されたデバイスの証明書の有効期間より短い場合、デバイス証明書の有効期間の値は CA 証明書の残りの有効期間と同じになります。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Device Certificate]** の順に選択します。

ステップ 2 デバイス証明書と現在のデバイス証明書の有効期間を確認します。

ステップ 3 [Device Certificate] ウィンドウで、[Modify] をクリックします。

ステップ 4 [Device Certificate Lifetime] ダイアログボックスに、新しい値を入力します（日数）。

ステップ 5 [Save] をクリックします。

認証局のロールをルートから下位に変更

デバイス CA は Cisco DNA Center のプライベート CA であり、サーバーとクライアントの間の接続の確立と保護に使用される証明書やキーを管理します。デバイス CA のロールをルート CA から下位 CA に変更するには、次の手順を実行します。

[Certificate Authority Management] ウィンドウの GUI を使用して、プライベート（内部）Cisco DNA Center CA のロールをルート CA から下位 CA に変更できます。このロールを変更する際は、次の手順を実行します。

- Cisco DNA Center が下位 CA の役割を果たすようにする場合、すでにルート CA（たとえば Microsoft CA）があり、Cisco DNA Center を下位 CA として認めているものと見なされます。
- 下位 CA が完全に設定されていない限り、Cisco DNA Center は内部ルート CA としての役割を継続します。
- Cisco DNA Center 用の証明書署名要求ファイルを生成し（次の手順の記述に従う）、手動で外部ルート CA に署名させる必要があります。

（注） Cisco DNA Center は、この期間中は内部ルート CA として実行し続けます。

- 証明書署名要求が外部ルート CA によって署名された後、GUI を使用してこの署名ファイルを Cisco DNA Center にインポートし直す必要があります（次の手順の記述に従う）。

  インポート後、Cisco DNA Center は下位 CA として自身を初期化し、下位 CA の既存機能をすべて提供します。

- 内部ルート CA から下位 CA への切り替え前にデバイスの制御可能性が有効になっている場合（デフォルト）、新しいデバイス証明書は自動的に更新されます。

- GUI に表示されている下位 CA 証明書有効期間は、証明書から読み取られたもので、システム時刻を使って計算されたものではありません。したがって今日、証明書を有効期間 1 年でインストールして来年の同じ時間に GUI で見ると、証明書の有効期間は 1 年間と表示されます。

- 下位 CA 証明書として PEM または DER 形式のみを使用できます。

- 下位 CA は上位の CA と連携しないため、上位レベルの証明書がある場合は、その失効に注意してください。このため、下位 CA からネットワークデバイスに対して、証明書の失効に関する情報が通知されることもありません。下位 CA にはこの情報がないため、すべてのネットワークデバイスは下位 CA を Cisco Discovery Protocol（CDP）送信元としてのみ使用します。

始める前に

ルート CA 証明書のコピーが必要です。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[System]** > **[Settings]** > **[Certificate Authority]** の順に選択します。

ステップ 2 [CA Management] タブをクリックします。

ステップ 3 GUI で既存のルートまたは下位 CA 証明書の設定情報を確認します。

- [Root CA Certificate]：現在のルート CA 証明書（外部または内部）を表示します。
- [Root CA Certificate Lifetime]：現在のルート CA 証明書の最新の有効期間を表示します（日数）。
- [Current CA Mode]：現在の CA モードを表示します（ルート CA または下位 CA）。
- [Sub CA mode]：ルート CA から下位 CA に変更できます。

ステップ 4 [CA Management] タブで、[Sub CA Mode] チェックボックスをオンにします。

ステップ 5 [Next] をクリックします。

ステップ 6 表示される警告内容を確認します。

次に例を示します。

- ルート CA から下位 CA に変更するプロセスは元に戻すことができません。
- ルート CA モードで登録された、または証明書が発行されたネットワーク デバイスがないことを確認する必要があります。ネットワークデバイスを誤ってルート CA モードで登録した場合は、ルート CA から下位 CA に変更する前に、取り消しをする必要があります。
- 下位 CA の設定プロセスが終了しなければ、ネットワークデバイスをオンラインにできません。

ステップ 7 [OK] をクリックして続行します。

[Certificate Authority Management] ウィンドウに、[Import External Root CA Certificate] フィールドが表示されます。

ステップ 8 [Import External Root CA Certificate] フィールドにルート CA 証明書をドラッグ アンド ドロップして、[Upload] をクリックします。

ルート CA 証明書が Cisco DNA Center にアップロードされ、証明書署名要求の生成に使用されます。

アップロードプロセスが完了すると、「Certificate Uploaded Successfully」というメッセージが表示されます。

ステップ 9 [Next] をクリックします。

Cisco DNA Center で証明書署名要求が生成されて表示されます。

ステップ 10 Cisco DNA Center で生成された証明書署名要求を GUI で確認し、次のアクションのいずれかを実行します。

- [Download] リンクをクリックして、証明書署名要求ファイルのローカルコピーをダウンロードします。

  その後、この証明書署名要求ファイルを電子メールに添付して、ルート CA に送信することができます。

- [Copy to the Clipboard] リンクをクリックして、証明書署名要求ファイルの内容をコピーします。

  その後、この証明書署名要求の内容を電子メールに貼り付けるか、電子メールに添付ファイルとして添付して、ルート CA に送信することができます。

ステップ 11 証明書署名要求ファイルをルート CA に送信します。

ルート CA から下位 CA ファイルが返されます。このファイルを Cisco DNA Center にインポートし直す必要があります。

ステップ 12 ルート CA から下位 CA ファイルを受信した後、Cisco DNA Center の GUI に再度アクセスし、[Certificate Authority Management] ウィンドウに戻ります。

ステップ 13 [CA Management] タブをクリックします。

ステップ 14 [Change CA mode] ボタンの [Yes] をクリックします。

[Yes] をクリックすると、GUI に証明書署名要求が表示されます。

ステップ 15 [Next] をクリックします。

[Certificate Authority Management] ウィンドウに、[Import Sub CA Certificate] フィールドが表示されます。

ステップ 16 [Import Sub CA Certificate] フィールドに下位 CA 証明書をドラッグ アンド ドロップして、[Apply] をクリックします。

下位 CA 証明書が Cisco DNA Center にアップロードされます。

アップロードが完了すると、GUI の [CA Management] タブに、下位 CA モードが表示されます。

ステップ 17 [CA Management] タブのフィールドを確認します。

- [Sub CA Certificate]：現在の下位 CA 証明書を表示します。
- [External Root CA Certificate]：ルート CA 証明書を表示します。
- [Sub CA Certificate Lifetime]：下位 CA 証明書の有効期間を表示します（日数）。
- [Current CA Mode]：SubCA モードを表示します。

ロールオーバー下位 CA 証明書のプロビジョニング

Cisco DNA Center では、既存の下位 CA の有効期間が 70% 以上経過している場合に、ユーザーがロールオーバー下位 CA として下位証明書を適用することができます。

始める前に

- 下位 CA ロールオーバー プロビジョニングを開始するには、認証局のロールを下位 CA モードに変更しておく必要があります。認証局のロールをルートから下位に変更（57 ページ）を参照してください。
- 現在の下位 CA 証明書の有効期限が 70 % 以上経過していることが必要です。この状態になると、Cisco DNA Center の [CA Management] タブの下に [Renew] ボタンが表示されます。
- ロールオーバー下位 CA の署名付き証明書のコピーが必要です。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[System]** > **[Settings]** > **[Trust & Privacy]** > **[Certificate Authority]**。

ステップ 2 [CA Management] タブをクリックします。

ステップ 3 CA 証明書の設定情報を確認します。

- [Subordinate CA Certificate]：現在の下位 CA 証明書を表示します。
- [External Root CA Certificate]：ルート CA 証明書を表示します。
- [Subordinate CA Certificate Lifetime]：現在の下位 CA 証明書の有効期間（日数）を表示します。

- [Current CA Mode]：SubCA モードを表示します。

ステップ 4 [Renew] をクリックします。

Cisco DNA Center は既存の下位 CA を使用して、ロールオーバー下位 CA の証明書署名要求を生成し、表示します。

ステップ 5 生成された証明書署名要求を GUI で確認し、次のアクションのいずれかを実行します。

- [Download] リンクをクリックして、証明書署名要求ファイルのローカルコピーをダウンロードします。

  その後、この証明書署名要求ファイルを電子メールに添付して、ルート CA に送信することができます。

- [Copy to the Clipboard] リンクをクリックして、証明書署名要求ファイルの内容をコピーします。

  その後、この証明書署名要求の内容を電子メールに貼り付けるか、電子メールに添付ファイルとして添付して、ルート CA に送信することができます。

ステップ 6 証明書署名要求ファイルをルート CA に送信します。

次にルート CA がロールオーバー下位 CA ファイルを返送してくると、それを Cisco DNA Center にインポートし直す必要があります。

下位 CA ロールオーバーの証明書署名要求は、RootCA モードから SubCA モードに切り替えた際にインポートした下位 CA に署名したルート CA と同じルート CA によって署名される必要があります。

ステップ 7 ルート CA からロールオーバー下位 CA ファイルを受信した後、[Certificate Authority Management] ウィンドウに戻ります。

ステップ 8 [CA Management] タブをクリックします。

ステップ 9 証明書署名要求が表示されている GUI で [Next] をクリックします。

[Certificate Authority Management] ウィンドウに、[Import Sub CA Certificate] フィールドが表示されます。

ステップ 10 下位ロールオーバー CA 証明書を [Import Sub CA Certificate] フィールドにドラッグアンドドロップし、[Apply] をクリックします。

ロールオーバー下位 CA 証明書が Cisco DNA Center にアップロードされます。

アップロードが終了すると、GUI が変更され、[CA Management] タブの [Renew] ボタンが無効になります。

デバイス証明書トラストポイントの設定

Cisco DNA Center で [Manages Device Trustpoint] が無効になっている場合、デバイスが有線およびワイヤレス アシュアランス テレメトリを Cisco DNA Center に送信するようにするため、デバイスに手動で sdn-network-infra-iwan トラストポイントを設定し、証明書をインポートする必要があります。

SCEP を介して外部 CA から登録するには、次の手動設定が必要です。

ステップ 1 次のコマンドを入力します。

```
crypto pki trustpoint sdn-network-infra-iwan
  enrollment url http://<SCEP_enrollment_URL_to_external_CA>
  fqdn <device_FQDN>
  subject-name CN=<device_platform_ID>_<device_serial_number>_sdn-network-infra-iwan
  revocation-check <crl, crl none, or none>  # to perform revocation check with CRL, CRL fallback
to no check, or no check
  rsakeypair sdn-network-infra-iwan
  fingerprint <CA_fingerprint> # to verify that the CA at the url connection matches the fingerprint
 given
```

ステップ 2 （任意、ただし推奨）証明書を自動的に更新し、証明書の有効期限を回避します。

```
auto-enroll 80 regenerate
```

ステップ 3 （任意）登録 URL に到達可能なインターフェイスを指定します。それ以外の場合、http サービスの送信元インターフェイスがデフォルトで設定されます。

```
source interface <interface>
```

証明書の更新

Cisco DNA Center は、Kubernetes によって生成された証明書や、Kong および資格情報マネージャサービスが使用する証明書など、多数の証明書を使用します。これらの証明書は1年間有効です。証明書はクラスタをインストールするとすぐに開始され、期限切れに設定される前に Cisco DNA Center によって 1 年自動的に更新されます。

- 期限切れになる前に証明書を更新することを推奨します。
- 今から 100 日間の間に期限切れになるように設定されている証明書のみを更新できます。この手順では、それ以降に期限切れになる証明書については何も実行されません。
- このスクリプトでは、サードパーティ/認証局（CA）署名付き証明書ではなく、自己署名証明書のみを更新します。サードパーティ/CA 署名付き証明書の場合、スクリプトは Kubernetes と資格情報マネージャによって使用される内部証明書を更新します。
- 自己署名証明書の場合、更新プロセスではルート CA が変更されないため、証明書をデバイスにプッシュする必要はありません。
- クラスタという用語は、単一ノードと 3 ノード Cisco DNA Center 設定の両方に適用されます。

ステップ 1 各クラスタノードが正常であり、問題が発生していないことを確認します。

ステップ 2 そのノードで現在使用されている証明書のリストとそれらの有効期限を表示するには、次のコマンドを入力します。

```
sudo maglev-config certs info
```

ステップ 3 次のコマンドを入力して、すぐに期限切れになるように設定されている証明書を更新します。

```
sudo maglev-config certs refresh
```

ステップ 4 他のクラスタノードに対して上記の手順を繰り返します。

ステップ 5 ユーティリティのヘルプを表示するには、次のように入力します。

```
$ sudo maglev-config certs --help
Usage: maglev-config certs [OPTIONS] COMMAND [ARGS]...

Options:
  --help  Show this message and exit.

Commands:
  info
  refresh
```

信頼できる証明書の設定

Cisco DNA Center には、事前インストールされているシスコの信頼できる証明書バンドル（シスコが信頼する外部ルートバンドル）が含まれています。Cisco DNA Center は、シスコからの更新された信頼できる証明書バンドルのインポートとストレージもサポートしています。信頼できる証明書バンドルは、Cisco DNA Center およびそのアプリケーションとの信頼関係を確立するために、サポートされるシスコ ネットワーキング デバイスによって使用されます。

（注） シスコの信頼できる証明書バンドルは、サポートされているシスコデバイスのみをアンバンドルして使用できる、ios.p7b と呼ばれるファイルです。この ios.p7b ファイルには、シスコを含む有効な認証局のルート証明書が含まれています。このシスコの信頼できる証明書バンドルは、Cisco cloud（Cisco InfoSec）で使用できます。リンクは https://www.cisco.com/security/pki/ にあります。

この信頼できる証明書バンドルは、同じ CA を使用してすべてのネットワークデバイスの証明書および Cisco DNA Center の証明書を管理する、安全で便利な方法を提供します。信頼できる証明書バンドルは Cisco DNA Center によって使用され、自身の証明書およびプロキシゲートウェイ証明書（存在する場合）を検証し、それが有効な CA 署名付き証明書かを判断します。さらに、PnP ワークフローの開始時にネットワーク PnP 対応デバイスにアップロードできるように、また、その後の HTTPS ベースの接続で Cisco DNA Center を信頼できるように、信頼できる証明書バンドルを使用できます。

GUI の [Trusted Certificates] ウィンドウを使用して、シスコ トラストプール バンドルをインポートします。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[System]** > **[Settings]** > **[Trust & Privacy]** > **[Trusted Certificates]** の順に選択します。

ステップ 2 [Trusted Certificates] ウィンドウで、[Update] ボタンをクリックして信頼できる証明書バンドルの新規ダウンロードおよびインストールを開始します。

[Update] ボタンは、ios.p7b ファイルの更新バージョンが使用可能で、インターネットアクセスが可能なときにのみアクティブになります。

Cisco DNA Center に新しい信頼できる証明書バンドルがダウンロードおよびインストールされると、Cisco DNA Center はシスコのデバイスのダウンロードをサポートするよう、この信頼できる証明書バンドルを使用可能にします。

ステップ 3 新しい証明書ファイルをインポートする場合は、[Import] をクリックしてローカルシステムから有効な証明書ファイルを選択し、[Import Certificate] ウィンドウで [Import] をクリックします。

ステップ 4 [Export] をクリックして、証明書の詳細を CSV 形式でエクスポートします。

制限付きシェルについて

セキュリティを強化するため、ルートシェルへのアクセスは無効になっています。Shell コマンドへのアクセスが制限されることで、ユーザーは基礎となるオペレーティングシステムとファイルシステムにアクセスできなくなるため、運用上のリスクが軽減されます。

セキュリティ上の理由から、Shell コマンドへのアクセスが制限されています。ただし、root shell に一時的にアクセスしたい場合は、Cisco TAC にお問い合わせください。

必要に応じて、次の限定されたリストのコマンドを使用できます。

```
$ help
Help:
  cat                  concatenate and print files in restricted mode
  clear                clear the terminal screen
  date                 display the current time in the given FORMAT, or set the system
date
  debug                enable console debug logs
  df                   file system information
  dmesg                print or control the kernel ring buffer.
  du                   summarize disk usage of the set of FILEs, recursively for
directories.
  free                 quick summary of memory usage
  history              enable shell commands history
  htop                 interactive process viewer.
  ip                   print routing, network devices, interfaces and tunnels.
  kubectl              Interact with Kubernetes Cluster in a restricted manner.
  last                 show a listing of last logged in users.
  ls                   restricted file system view chrooted to maglev Home
  lscpu                print information about the CPU architecture.
  magctl               tool to manage a Maglev deployment
  maglev-config        tool to configure a Maglev deployment
  manufacture_check    tool to perform manufacturing checks
  netstat              print networking information.
  nslookup             query Internet name servers interactively.
  ntpq                 standard NTP query program.
  ping                 send ICMP ECHO_REQUEST to network hosts.
  ps                   check status of active processes in the system
  rca                  root cause analysis collection utilities
  reboot               Reboot the machine
  rm                   delete files in restricted mode
```

```
route                print the IP routing table.
runonce              Execute runonce scripts
scp                  restricted secure copy
sftp                 secure file transfer
shutdown             Shutdown the machine
ssh                  OpenSSH SSH client.
tail                 Print the last 10 lines of each FILE to standard output
top                  display sorted list of system processes
traceroute           print the route packets trace to network host.
uname                print system information.
uptime               tell how long the system has been running.
vi                   text editor
w                    show who is logged on and what they are doing.
```

製品使用状況テレメトリの収集について

Cisco DNA Center ではデフォルトでテレメトリデータが収集されますが、一部のデータ収集をオプトアウトできます。データ収集は、製品機能の開発を支援し、運用上の問題に対処して、より優れた価値と投資回収率（ROI）を実現することを目的としています。シスコが収集するデータの種類は、Cisco.com ID、システム、機能の使用状況、ネットワークデバイスインベントリ、およびソフトウェア利用資格です。収集されるデータの詳しいリストについては、「Cisco DNA Center のデータシート」を参照してください。一部のデータ収集をオプトアウトするには、シスコのアカウント担当者および Cisco Technical Assistance Center（TAC）にお問い合わせください。

左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Terms and Conditions]** > **[Telemetry Collection]** の順に選択します。[Telemetry Collection] ウィンドウから、ライセンス契約、プライバシーポリシー、プライバシーデータシートを確認できます。

テレメトリコレクションの設定

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System Settings]** > **[Settings]** > **[Telemetry Collection]** の順に選択します。

ステップ 2 テレメトリコレクションの契約を確認するには、[End User License Agreement] をクリックします。

ステップ 3 （任意）テレメトリコレクションを無効にするには、[Telemetry Collection] チェックボックスをオフにして [Update] をクリックします。

vManage プロパティの設定

Cisco DNA Center は、統合 vManage 設定を使用して Cisco vEdge 展開をサポートします。vEdge トポロジをプロビジョニングする前に、[Settings] ウィンドウで vManage の詳細を保存できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[External Services]** > **[vManage]** の順に選択します。

ステップ 2 vManage プロパティを設定します。

- [Host Name/IP Address]：vManage の IP アドレス。
- [Username]：vManage にログインするために使用される名前。
- [Password]：vManage にログインするために使用されるパスワード。
- [Port Number]：vManage にログインするために使用されるポート。
- [vBond Host Name/IP Address]：vBond の IP アドレス。vManage を使用して NFV を管理する場合に必要です。
- [Organization Name]：組織の名前。vManage を使用して NFV を管理する場合に必要です。

ステップ 3 vManage 証明書をアップロードするには、[Select a file from your computer] をクリックします。

ステップ 4 [Save] をクリックします。

アカウントのロックアウト

アカウント ロックアウト ポリシーを設定して、ユーザーによるログインの試行、アカウントのロックアウト期間、ログインの再試行回数を管理できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Account Lockout]** の順に選択します。

ステップ 2 [Enforce Account Lockout] トグルボタンをクリックして、チェックマークが表示された状態にします。

ステップ 3 [Enforce Account Lockout] の次のパラメータの値を入力します。

- Maximum Login Retries
- Lockout Effective Periods (minutes)
- Reset Login Retries after (minutes)

（注） [Info] にカーソルを合わせると、各パラメータの詳細が表示されます。

ステップ 4 ドロップダウンリストから [Idle Session Timeout] の値を選択します。

ステップ 5 [保存（**Save**）] をクリックします。

セッションをアイドル状態のままにすると、セッションタイムアウトの 5 分前に [Session Timeout] ダイアログボックスが表示されます。セッションを続行する場合は、[Stay signed in] をクリックします。[Sign out] をクリックすると、すぐにセッションを終了できます。

パスワードの有効期限切れ

パスワード有効期限ポリシーを設定して、以下を管理できます。

- パスワードの有効期限の通知間隔。
- パスワードが期限切れになる前にユーザーに通知が表示される日数。
- 猶予期間。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Password Expiry]** の順に選択します。

ステップ 2 [Enforce Password Expiry] トグルボタンをクリックして、チェックマークが表示された状態にします。

ステップ 3 次の [Enforce Password Expiry] パラメータの値を入力します。

- パスワード期限（日）
- パスワードの期限の警告（日）
- 猶予期間（日）

（注） [Info] にカーソルを合わせると、各パラメータの詳細が表示されます。

ステップ 4 [Save] をクリックして、パスワード有効期限設定を保存します。

IP アクセス制御

IP アクセス制御を使用すると、ホストまたはネットワークの IP アドレスに基づいて Cisco DNA Center へのアクセスを制御できます。Cisco DNA Center では、IP アクセス制御に次のオプションがあります。

- すべての IP アドレスに Cisco DNA Center へのアクセスを許可します。デフォルトでは、すべての IP アドレスが Cisco DNA Center にアクセスできます。
- 選択した IP アドレスのみに Cisco DNA Center へのアクセスを許可します。

IP アクセス制御の構成

IP アクセス制御を構成し、選択した IP アドレスのみに Cisco DNA Center へのアクセスを許可するには、次の手順を実行します。

1. IP アクセス制御の有効化 （68 ページ）
2. IP アクセスリストへの IP アドレスの追加 （68 ページ）
3. （任意） IP アクセスリストからの IP アドレスの削除 （69 ページ）

IP アクセス制御の有効化

始める前に

- SUPER-ADMIN-ROLE 権限を取得しておきます。
- Cisco DNA Center サービスサブネット、クラスタサービスサブネット、およびクラスタインターフェイス サブネットを許可サブネットのリストに追加します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[IP Access Control]** の順に選択します。

ステップ 2 [リストされている IP アドレスのみに接続を許可する（Allow only listed IP addresses to connect）] オプションボタンをクリックします。

ステップ 3 [Add IP List] をクリックします。

ステップ 4 [Add IP] スライドインペインの [IP Address] フィールドに、IPv4 アドレスを入力します。

（注） IP アドレスを IP アクセスリストに追加しないと、Cisco DNA Center にアクセスできなくなる可能性があります。

ステップ 5 [Subnet Mask] フィールドにサブネット マスクを入力します。

サブネットマスクの有効範囲は 0 ～ 32 です。

ステップ 6 [Save] をクリックします。

IP アクセスリストへの IP アドレスの追加

IP アクセスリストに IP アドレスを追加するには、次の手順を実行します。

始める前に

IP アクセス制御が有効になっていることを確認してください。詳細については、IP アクセス制御の有効化 （68 ページ）を参照してください。

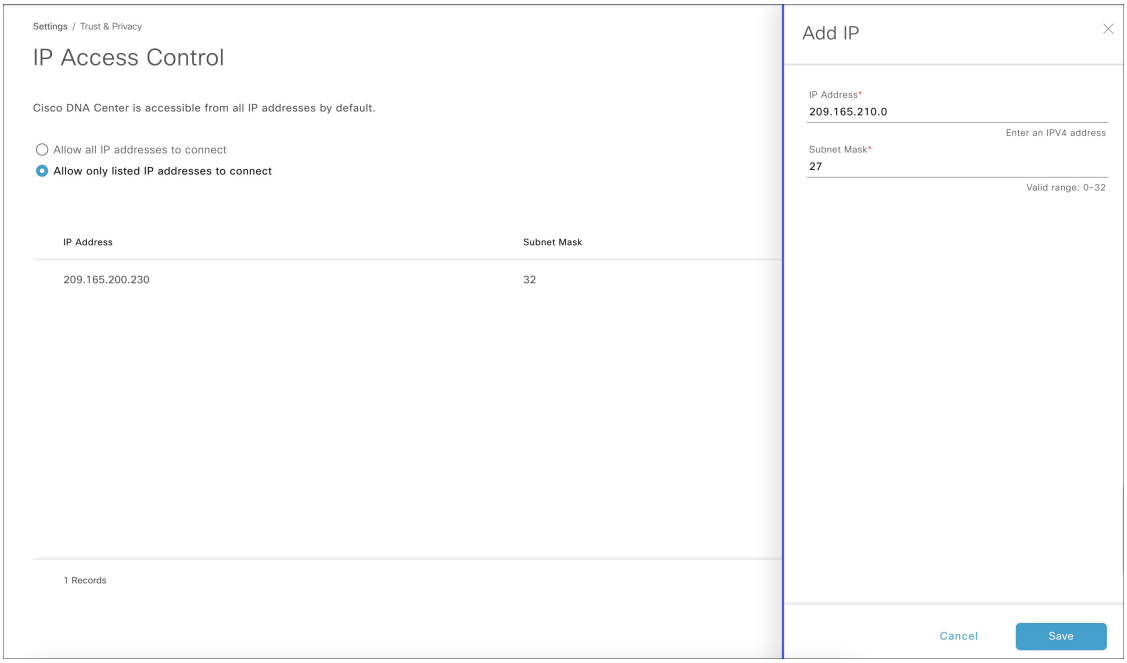
ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[IP Access Control]** の順に選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [Add IP] スライドインペインの [IP Address] フィールドに、ホストまたはネットワークの IPv4 アドレスを入力します。

ステップ 4 [Subnet Mask] フィールドにサブネット マスクを入力します。

サブネットマスクの有効範囲は 0 ～ 32 です。



ステップ 5 [Save] をクリックします。

IP アクセスリストからの IP アドレスの削除

IP アクセスリストから IP アドレスを削除して Cisco DNA Center へのアクセスを無効にするには、以下の手順を実行します。

始める前に

IP アクセスコントロールを有効にして、IP アドレスを IP アクセスリストに追加したことを確認します。詳細については、IP アクセス制御の有効化 （68 ページ）およびIP アクセスリストへの IP アドレスの追加 （68 ページ）を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[IP Access Control]** の順に選択します。

ステップ 2 [Action] 列で、対応する IP アドレスの [Action] アイコンをクリックします。

ステップ 3 [Delete] をクリックします。

IP アクセス制御の無効化

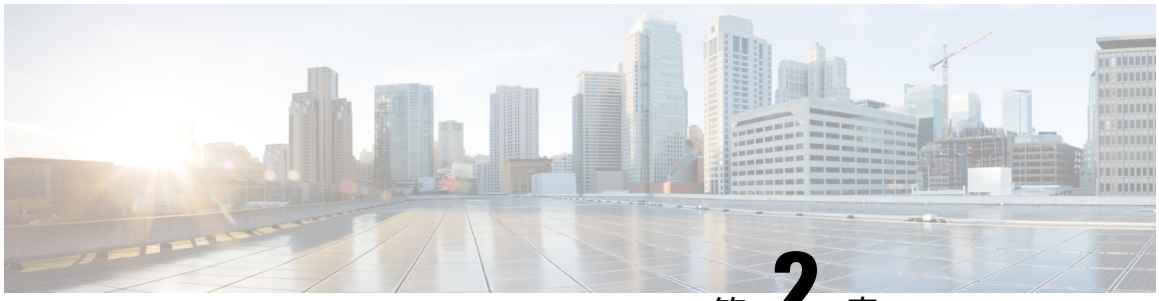
IP アクセス制御を無効化し、すべての IP アドレスに Cisco DNA Center へのアクセスを許可するには、次の手順を実行します。

始める前に

SUPER-ADMIN-ROLE 権限を取得しておきます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[IP Access Control]** の順に選択します。

ステップ 2 [Allow all IP addresses to connect] オプションボタンをクリックします。



第 2 章

アプリケーションの管理

アプリケーション管理

Cisco DNA Center はその多くの機能を、コアインフラストラクチャとは別にパッケージ化された個別のアプリケーションとして扱います。このため、ユーザーは設定に応じて、必要なアプリケーションをインストールして実行し、使用していないアプリケーションをアンインストールできます。

[Software Management] ウィンドウに表示されるアプリケーションパッケージの数とタイプは、Cisco DNA Center のバージョンおよび Cisco DNA Center のライセンスレベルによって異なります。使用可能なアプリケーションパッケージはすべて、現在インストールされているかどうかに関係なく表示されます。

一部のアプリケーションは基本的なアプリケーションなので、ほぼすべての Cisco DNA Center の導入で必要になります。パッケージの説明については、[Currently Installed Applications] リンクをクリックし、その名前の上にカーソルを置きます。

各 Cisco DNA Center アプリケーションパッケージは、サービスバンドル、メタデータファイル、およびスクリプトで構成されています。

（注） アプリケーション管理手順はすべて、Cisco DNA Center GUI から実行します。これらの手順の多くは、シェルにログイン後 CLI を使用して実行することもできますが、この方法はお勧めしません。特に、CLI を使用してパッケージを導入またはアップグレードする場合、**maglev package status** コマンドの結果に、すべてのパッケージが NOT_DEPLOYED、DEPLOYED、または DEPLOYMENT_ERROR と表示されている場合を除き、**deploy** または **upgrade** コマンドが入力されていないことを確認する必要があります。その他の状態はすべて、対応するアクティビティが進行中であることを示しています。また、パラレル導入やアップグレードはサポートされていません。

最新のシステムバージョンのダウンロードとインストール

[Software Management] ウィンドウには、最新の Cisco DNA Center バージョンが利用可能であるかが示されます。

最新バージョンをダウンロードしてインストールするには、次の手順を実行します。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Software Management]** の順に選択します。

（注） この時点で、Cisco DNA Center によって接続性チェックが実行されます。接続に問題がある場合、[Software Management] ウィンドウに、現在利用可能なシステムアップデートは表示されません。

ステップ 2 システムアップデートが利用可能であることがウィンドウに示されている場合は、次のいずれかをクリックします。

1. [Upgrade] をクリックすると最新バージョンがダウンロードされ、システムが今すぐアップグレードされます。

   [Upgrade Release] ダイアログボックスで、次の手順を実行します。

   1. ダイアログボックスに、使用可能なアプリケーションパッケージが一覧表示されます。アプリケーションをインストールするには、アプリケーションの横にあるチェックボックスをオンにします。
   2. [Install] をクリックします。

2. [Download] をクリックして今すぐダウンロードし、アップグレードを後からスケジュールします。

   [Schedule Upgrade] ダイアログボックスで、次の手順を実行します。

   1. アップグレードする日時をスケジュールします。

2. ダイアログボックスに、使用可能なアプリケーションが一覧表示されます。アプリケーションをインストールするには、アプリケーションの横にあるチェックボックスをオンにします。
3. [Download] をクリックします。

（注） アップグレード中、Cisco DNA Center はメンテナンスモードになり、システムアップデートが実行されている間は使用できません。アップデートが完了したら、Cisco DNA Center に再度ログインします。

システムアップグレードが完了すると、ウィンドウの上部にあるメッセージにシステムが最新であることが表示されます。

ステップ 3 [ソフトウェア管理（Software Management）] ウィンドウで、[アクティビティ（Activities）] をクリックして、システムに加えられた変更のリストを表示します。システムのアップグレードまたはダウンロードの詳細、インストールまたはアンインストールされたアプリケーション、およびアクティビティのタイムスタンプを表示できます。

ステップ 4 [アクション（Actions）] 列で省略記号をクリックすると、アクティビティの実行中に発生したタスクを表示できます。

エアギャップモードでの最新のシステムバージョンのダウンロードとインストール

システムのアップグレードは、インターネットに接続し、オンライン更新プロセスを使用することによって完了します。ただし、場合によっては、アップグレードが内部ネットワーク内（つまり、エアギャップ環境）内で厳密に維持されます。このアップグレードは、追加のセキュリティまたは法的規制をサポートするために必要な場合があります。

（注） エアギャップモードを有効にすると、次のことが可能になります。

- プライベート IP サブネットのみと通信します。
- 提供されている API を使用して、エアギャップ環境を通過する IP アドレス範囲を追加できます。
- エアギャップモードとクラウドモードを切り替えます。

始める前に

クラスタでエアギャップモードが有効になっている必要があります。エアギャップモードを有効にする方法については、『Cisco DNA Center Air Gap Deployment Guide』を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Software Management]** の順に選択します。

ステップ 2 制限付きシェルのエアギャップディレクトリにアクセスし、次の SCP コマンドを使用して、所定の場所からエアギャップ tarball をコピーします。

```
scp -P 2222 <airgap tar file> maglev@<cluster_ip>:airgap/
```

3 ノードクラスタの場合は、任意のノードにファイルをコピーできます。

ステップ 3 [Software Management] ウィンドウの右上隅にある [Scan] をクリックして、使用可能な最新のソフトウェアリリースを表示します。

ステップ 4 ファイルをダウンロードし、アップグレードを後で実行するようにスケジュールするには、次の手順を実行します。

a) [PreLoad] をクリックします。

b) [Schedule Upgrade] ダイアログボックスで、システムアップグレードをスケジュールし、[PreLoad] をクリックします。

送信が成功すると、ウィンドウの上部にあるバナーメッセージに、システムアップグレードのスケジュールされた日時が表示されます。

c) スケジュールされたシステムアップグレードを編集または削除するには、バナーメッセージの末尾にある省略記号をクリックします。スケジュールをすぐにアップグレードすることもできます。

ステップ 5 最新バージョンをダウンロードしてシステムをすぐにアップグレードするには、次の手順を実行します。

a) **[Upgrade]** をクリックします。

b) ダイアログボックスで、一覧表示されている使用可能なパッケージアプリケーションから、アプリケーションの横にあるチェックボックスをオンにしてアプリケーションをインストールします。

c) [Install] をクリックします。

（注） アップグレード中、Cisco DNA Center はメンテナンスモードになり、システムアップデートが実行されている間は使用できません。

システムアップグレードが完了すると、ウィンドウの上部にあるメッセージにシステムが最新であることが表示されます。

（注）
- エアギャップモードが有効になっているときにシステムが外部クラウドに接続できる場合は、次のコマンドを使用してネットワークポリシーを確認します。

```
sudo calicoctl get gnp allow-outbound-external -o yaml
```

- ALM のネットワークモードがエアギャップかどうかを確認するには、次のコマンドを使用します。

```
kc get po -n maglev-control-plane alm-agent-8469679dfb-nvkxk -o yaml | grep -A1
NETWORK_MODE
```

- スキャンのステータスとログを取得するには、次のコマンドを使用します。

```
kc get po -n maglev-control-plane | grep ef-airgap-seed
```

- プリロードのステータスとログを取得するには、次のコマンドを使用します。

```
kc get po -n maglev-control-plane | grep ef-airgap-scan
```

アプリケーションの更新のダウンロードとインストール

Cisco DNA Center 個々のアプリケーションはコアインフラストラクチャから独立して扱われます。具体的には、アプリケーションの個別のパッケージをインストールして、Cisco DNA Center 上で実行できます。

アプリケーションのパッケージは、インストールと展開に時間がかかる場合があります。そのため、ネットワークのメンテナンス期間中にパッケージをインストールしてください。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Software Management]** の順に選択します。

（注） この時点で、Cisco DNA Center によって接続性チェックが実行されます。接続に問題がある場合、[ソフトウェア管理（Software Management）] ウィンドウに、現在利用可能なシステムアップデートは表示されません。

ステップ 2 アプリケーション更新が利用可能な場合は、ウィンドウの下部に表示されます。次のいずれかを実行します。

1. 利用可能なすべてのシステムアップデートをインストールするには、[Select All] リンクをクリックします。
2. 個々のアプリケーション更新をインストールするには、該当するチェックボックスをオンにします。

システムアップグレードの実行中に、使用可能なアプリケーションをインストールすることもできます。詳細については、最新のシステムバージョンのダウンロードとインストール （72 ページ）を参照してください。

ステップ 3 [Install] をクリックします。

（注） インストール中に依存関係がチェックされ、自動的にインストールされます。

更新中の各アプリケーションの進行状況バーがウィンドウに表示されます。

ステップ 4 [Currently Installed Applications] リンクをクリックし、選択したアプリケーションが更新されていることを確認します。

ステップ 5 [ソフトウェア管理（Software Management）] ウィンドウで、[アクティビティ（Activities）] をクリックして、システムに加えられた変更のリストを表示します。システムのアップグレードまたはダウンロードの詳細、インストールまたはアンインストールされたアプリケーション、およびアクティビティのタイムスタンプを表示できます。

ステップ 6 [アクション（Actions）] 列で省略記号をクリックすると、アクティビティの実行中に発生したタスクを表示できます。

アプリケーションのアンインストール

Cisco DNA Center 個々のアプリケーションはコアインフラストラクチャから独立して扱われます。具体的には、Cisco DNA Center からアプリケーションの個々のパッケージをアンインストールすることができます。

アンインストールできるのはシステムに必須でないアプリケーションのパッケージのみです。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

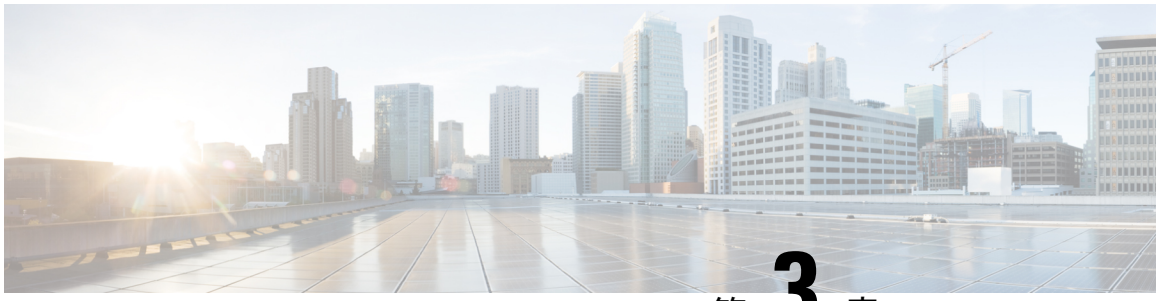
ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Software Management]** の順に選択します。

ステップ 2 [Currently Installed Applications] リンクをクリックして、Cisco DNA Center アプライアンスにインストールされているすべてのアプリケーションを表示します。

ステップ 3 削除するパッケージのチェックボックスをチェックし、[Uninstall] をクリックします。

（注） 同時に複数のパッケージをアンインストールすることはできません。

Cisco DNA Center はアプリケーションが削除された後にメッセージを表示します。



第 3 章

ユーザの管理

ユーザー プロファイルについて

ユーザープロファイルで、ユーザーのログイン、パスワード、およびロール（権限）を定義します。

ユーザーの内部プロファイルと外部プロファイルの両方を設定できます。内部ユーザープロファイルは Cisco DNA Center に配置され、外部ユーザープロファイルは外部 AAA サーバーに配置されます。

Cisco DNA Center をインストールすると、SUPER-ADMIN-ROLE 権限を持つデフォルトのユーザープロファイルが作成されます。

ユーザ ロールの概要

実行できる機能を指定する次のユーザロールがユーザに割り当てられます。

- **管理者（SUPER-ADMIN-ROLE）**：このロールを持つユーザは、Cisco DNA Center のすべての機能へのフルアクセスが可能です。管理者は、SUPER-ADMIN-ROLE を含むさまざまなロールを持つ他のユーザプロファイルを作成できます。
- **ネットワーク管理者（NETWORK-ADMIN-ROLE）**：このロールを持つユーザは、Cisco DNA Center のすべてのネットワーク関連機能へのフルアクセスが可能です。ただし、バックアップと復元など、システム関連の機能へのアクセス権はありません。
- **オブザーバ（OBSERVER-ROLE）**：このロールを持つユーザは、Cisco DNA Center の機能への表示専用アクセスが可能です。オブザーバロールを持つユーザは、Cisco DNA Center やそれが管理するデバイスを設定または制御する機能にはアクセスできません。

内部ユーザーの作成

ユーザーを作成し、このユーザーにロールを割り当てることができます。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[User Management]** の順に選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 新しいユーザーの姓、名、電子メールアドレス、およびユーザー名を入力します。

電子メールアドレスは、標準の Apache EmailValidator クラスの要件を満たしている必要があります。

ステップ 4 [Role List] で、SUPER-ADMIN-ROLE、NETWORK-ADMIN-ROLE、または OBSERVER-ROLE のいずれかのロールを選択します。

ステップ 5 パスワードを入力し、確認します。パスワードの要件：

- 最低 8 文字
- 次のカテゴリのうち少なくとも 3 つのカテゴリに属する文字：
  - 小文字の英字
  - 大文字の英字
  - 番号（Number）
  - 特殊文字

ステップ 6 [Save] をクリックします。

ユーザーの編集

一部のユーザープロパティは編集できますが、ユーザー名は編集できません。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[User Management]** の順に選択します。

ステップ 2 編集するユーザーの横にあるオプションボタンをクリックします。

ステップ 3 [Edit] をクリックします。

ステップ 4 必要に応じて、姓名または電子メールアドレスを編集します。

ステップ 5 [Role List] で、必要に応じて新しいロール（[SUPER-ADMIN-ROLE]、[NETWORK-ADMIN-ROLE]、または [OBSERVER-ROLE]）を選択します。

ステップ 6 [Save] をクリックします。

ユーザーの削除

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[User Management]** の順に選択します。

ステップ 2 削除するユーザーの横にあるオプションボタンをクリックします。

ステップ 3 [Delete] をクリックします。

ステップ 4 確認のプロンプトで、[Continue] をクリックします。

ユーザーパスワードのリセット

別のユーザーのパスワードをリセットできます。

セキュリティ上の理由から、パスワードは、どのユーザーに対しても（管理者権限を持つユーザーに対しても）表示されません。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[User Management]** の順に選択します。

ステップ 2 パスワードをリセットするユーザーの横にあるオプションボタンをクリックします。

ステップ 3 [Reset Password] をクリックします。

ステップ 4 パスワードを入力し、確認します。新しいパスワードの要件：

- 最低 8 文字
- 次のカテゴリのうち少なくとも 3 つのカテゴリに属する文字：
  - 小文字の英字
  - 大文字の英字
  - 番号（Number）
  - 特殊文字

ステップ 5 [Save] をクリックします。

自身のユーザーパスワードの変更

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、「ユーザ ロールの概要」を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[Change Password]** の順にクリックします。

ステップ 2 必要なフィールドに情報を入力します。

ステップ 3 [更新（Update）] をクリックします。

管理者権限なしでのユーザーパスワードの変更

次の手順では、管理者権限なしでパスワードを変更する方法について説明します。

ステップ 1 右上隅で、表示されたユーザー名をクリックし、**[My Profile and Settings]** > **[My Account]** の順に選択します。

ステップ 2 [Password] フィールドで、[Update Password] をクリックします。

ステップ 3 [Update Password] ダイアログボックスで、現在のパスワードと新しいパスワードを入力し、新しいパスワードを確認します。

ステップ 4 [更新（Update）] をクリックします。

思い出せないパスワードのリセット

パスワードを忘れた場合は、Cisco Technical Assistance Center（TAC）に連絡してパスワードをリセットしてください。

ロールベース アクセス コントロールの設定

Cisco DNA Center は、ロールベース アクセス コントロール（RBAC）をサポートしています。これにより、SUPER-ADMIN-ROLE 権限を持つユーザーは、特定の Cisco DNA Center 機能へのユーザーアクセスを許可または制限するカスタムロールを定義できます。

カスタムロールを定義し、定義したロールにユーザーを割り当てるには、次の手順を実行します。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 カスタムロールを定義します。

a) 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[Role Based Access Control]** の順に選択します。

b) [Create a New Role] をクリックします。
[Create a Role] ウィンドウが表示されます。これが RBAC の最初のイテレーションである場合、新しいロールを作成した後に、ユーザーを新しいロールに割り当てるように求められます。

c) タスクの概要ウィンドウが開いたら、[Let's do it] をクリックして、ワークフローに直接移動します。
[Create a New Role] ウィンドウが開きます。

d) ロール名を入力し、[Next] をクリックします。
[Define the Access] ウィンドウが開き、オプションのリストが表示されます。デフォルトでは、Cisco DNA Center のすべての機能に対してオブザーバロールが設定されています。

e) 目的の機能に対応する [>] アイコンをクリックして、関連付けられている機能を表示します。

f) それぞれの機能の権限レベルを必要に応じて [Deny]、[Read]、または [Write] に設定します。

機能の権限レベルを [Deny] に設定すると、このロールを割り当てられたユーザーは該当する機能を GUI で表示できなくなります。

g) [Next] をクリックします。
[Summary] ウィンドウが開きます。
h) [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。
[Done, Role-Name] ウィンドウが開きます。

ステップ 2 作成したカスタムロールにユーザーを割り当てるには、[Add Users] をクリックします。

[User Management] > **[Internal Users]** ウィンドウが開きます。このウィンドウでは、カスタムロールを既存のユーザーまたは新規ユーザーに割り当てることができます。

- 既存のユーザーにカスタムロールを割り当てるには、次の手順を実行します。
  1. [Internal Users] ウィンドウで、カスタムロールを割り当てるユーザーの横にあるオプションボタンをクリックし、次に [Edit] をクリックします。
     [Update Internal User] スライドインペインが開きます。
  2. [Role List] ドロップダウンリストから、カスタムロールを選択し、[Save] をクリックします。
- カスタムロールを新規ユーザーに割り当てるには、次の手順を実行します。
  1. [Add] をクリックします。
     [Create Internal User] スライドインペインが開きます。
  2. 表示されるフィールドに氏名とユーザー名を入力します。
  3. [Role List] ドロップダウンリストから、新規ユーザーに割り当てるカスタムロールを選択します。
  4. 新しいパスワードを入力し、確認のために再度入力します。
  5. [Save] をクリックします。

ステップ 3 既存のユーザーのログイン中に管理者がそのユーザーのアクセス権限を更新した場合、新しい権限設定を有効にするには、ユーザーが Cisco DNA Center からログアウトして、ログインし直す必要があります。

Cisco DNA Center ユーザー ロール権限

表 *1 : Cisco DNA Center* ユーザー ロール権限

機能	説明
アシュアランス	ネットワークのあらゆる側面を完全に可視化して一貫したサービスレベルを維持できます。

機能	説明
モニターリングおよびトラブルシューティング	問題のトラブルシューティングと修復、プロアクティブなネットワークモニタリング、および AI ネットワーク分析 から得られるインサイトにより、ネットワークの正常性のモニタリングと管理を行います。 このロールでは次のことが可能です。 • 問題の解決、クローズ、無視。 • 機械推論エンジン（MRE）のワークフローの実行。 • トレンドとインサイトの分析。 • パストレース、センサーダッシュボード、不正管理などの問題のトラブルシューティング。 • 不正および Cisco Advanced Wireless Intrusion Prevention System（aWIPS）のワークフローの実行。これらのワークフローには、AP 許可リスト、ベンダー許可リスト、aWIPS プロファイルの作成、aWIPS プロファイルの割り当てなどが含まれます。
モニターリングの設定（Monitoring Settings）	問題の設定と管理を行います。ネットワーク、クライアント、およびアプリケーションの正常性のしきい値を更新します。 注：[Monitoring and Troubleshooting] に対する読み取りアクセス許可が最低限必要です。
トラブルシューティング ツール	センサーテストの作成と管理を行います。クライアントのトラブルシューティングのためのオンデマンドのフォレンジック パケット キャプチャ（インテリジェント キャプチャ）をスケジュールします。 注：[Monitoring and Troubleshooting] に対する読み取りアクセス許可が最低限必要です。
ネットワーク分析	ネットワーク分析関連のコンポーネントを管理します。
データアクセス	クエリエンジン API へのアクセスを有効にします。グローバル検索、不正管理、aWIPS などの制御機能。 注：許可を [Deny] に設定すると、検索と アシュアランス 機能に影響します。
ネットワーク設計	ネットワーク階層の設定、ソフトウェア イメージ リポジトリの更新、サイトやネットワークデバイスの管理に使用するネットワークプロファイルと設定の構成を行います。

機能	説明
詳細ネットワーク設定	• グローバルデバイスログイン情報、認証サーバーとポリシーサーバー、証明書、信頼できる証明書、クラウドアクセスキー、Stealthwatch、Umbrella、データ匿名化などのネットワーク設定を更新します。 • デバイスインベントリとそのクレデンシャルをエクスポートします。 注：このタスクを完了するには、[Network Settings] に対する書き込み権限が必要です。
イメージリポジトリ	ソフトウェアイメージを管理し、物理および仮想ネットワークエンティティのアップグレードと更新を促進します。
ネットワーク階層	サイト、ビルディング、フロア、およびエリアのネットワーク階層を地理的な場所に基づいて定義および作成します。このロールを持つユーザーは、**[System]** > **[Settings]** で CMX サーバーを追加することもできます。
ネットワーク プロファイル	ルーティング、スイッチング、およびワイヤレスのネットワークプロファイルを作成します。サイトへプロファイルを割り当てます。このロールには、テンプレートハブ、タギング、モデル設定エディタ、および認証テンプレートが含まれます。 注：SSID を作成するには、[Network Settings] に対する書き込み権限が必要です。
ネットワーク設定	AAA、NTP、DHCP、DNS、Syslog、SNMP、テレメトリなど、サイト全体の共通のネットワーク設定。このロールを持つユーザーは、**[System]** > **[Settings]** で SFTP サーバーの追加とネットワーク再同期間隔の変更が可能です。 注：ワイヤレスプロファイルを作成するには、[Network Profiles] に対する書き込み権限が必要です。CMX サーバーをサイト、ビルディング、またはフロアに割り当てるには、[Network Hierarchy] に対する書き込み権限が必要です。
仮想ネットワーク	仮想ネットワーク（VN）を管理します。トラフィックの分離や VN 間通信の制御のために、物理ネットワークを複数の論理ネットワークにセグメント化します。
ネットワーク プロビジョニング	ネットワークデバイスの設定、アップグレード、プロビジョニング、および管理を行います。
コンプライアンス	コンプライアンス プロビジョニングを管理します。
EoX	ネットワーク内のハードウェアおよびソフトウェアの [End of Life]、[End of Sales]、または [End of Support] に関連する公開情報の詳細について、ネットワークをスキャンします。 注：EoX スキャンを表示するには、[Compliance] に対する読み取り権限が必要です。EoX スキャンを実行するには、[Compliance] に対する書き込み権限が必要です。
イメージの更新	完全なアップグレードライフサイクルの後で、ゴールデンイメージ設定に一致しないデバイスのソフトウェアイメージをアップグレードします。

機能	説明
インベントリ管理	ネットワーク上のデバイスの検出、追加、置換、削除、およびデバイス属性と設定プロパティの管理を行います。 注：デバイスを交換するには、**[Network Provision]** > **[PnP]** に対する書き込み権限が必要です。
[Inventory Management] > [Device Configuration]	デバイス設定：デバイスの実行構成を表示します。
[Inventory Management] > [Discovery]	ディスカバリ：ネットワーク内の新しいデバイスを検出します。
[Inventory Management] > [Network Device]	ネットワークデバイス：インベントリからデバイスを追加し、デバイスの詳細を表示し、デバイスレベルのアクションを実行します。
	インベントリインサイト：速度/デュプレックス設定の不一致やVLANの不一致などのデバイスの問題や、各問題が発生した回数を表示します。問題を解決するためにユーザーが実行する詳細なアクションを提供します。この情報には、可能な設定変更を含むアクションが必要であるため、読み取り専用ロールのユーザーには表示されません。
[Inventory Management] > [Port Management]	ポート管理：デバイスでポートアクションを許可します。
[Inventory Management] > [Topology]	トポロジ：ネットワークデバイスとリンク接続を表示します。デバイスロールの管理、デバイスのタグ付け、表示のカスタマイズ、およびカスタムトポロジレイアウトの保存を行います。 注：[SD-Access Fabric] ウィンドウを表示するには、少なくとも**[Network Provision]** > **[Inventory Management]** > **[Topology]**に対する読み取りアクセス許可が必要です。
ライセンス	ソフトウェア資産やネットワーク資産のライセンス使用状況とコンプライアンスに関する情報を一元管理します。このロールは、cisco.com、シスコのクレデンシャル、デバイスの EULA、およびスマートアカウントの権限も管理します。
ネットワークテレメトリ	デバイスからのアプリケーションテレメトリの収集を有効または無効にします。サイトテレメトリレシーバ、ワイヤレスサービスアシュアランス、コントローラ証明書などの関連設定をデバイスに展開します。 注：アプリケーションテレメトリの収集を有効または無効にするには、[Provision] に対する書き込み権限が必要です。
PnP	新しいデバイスを自動的にオンボードしてサイトに割り当て、サイト固有のコンテキスト設定に基づいて設定します。

機能	説明
プロビジョニング	サイト固有の設定とネットワークに対して設定されたポリシーを使用してデバイスをプロビジョニングします。このロールには、ファブリック、アプリケーションポリシー、アプリケーションの可視性、クラウド、サイト間 VPN、ネットワーク/アプリケーションテレメトリ、Stealthwatch、同期開始と実行設定、および Umbrella プロビジョニングが含まれます。 不正および aWIPS のメインダッシュボードでは、不正封じ込めなどの特定のアクションを有効または無効にできます。 デバイスをプロビジョニングするには、[Network Design] と [Network Provisioning] に対する書き込み権限が必要です。
ネットワーク サービス	基本的なネットワーク接続とアクセスの枠を超えたネットワークの追加機能を設定します。
アプリケーション ホスティング	ネットワークデバイスで実行される仮想化されたコンテナベースのアプリケーションを展開、管理、およびモニターします。
Bonjour	ポリシーベースのサービス検出を有効にするために、ネットワーク全体で Wide Area Bonjour サービスを有効にします。
Stealthwatch	暗号化されたトラフィックに含まれる脅威も検出して軽減できるようにするために、ネットワーク要素から Cisco Stealthwatch にデータを送信するように設定します。 Stealthwatch をプロビジョニングするには、次のコンポーネントに対する書き込み権限が必要です。 • **[Network Design] > [Network Settings]** • **[Network Provision] > [Provision]** • **[Network Services] > [Stealthwatch]** • **[Network Design] > [Advanced Settings]**
Umbrella	サイバーセキュリティの脅威に対する最前線の防御策として、ネットワーク要素で Cisco Umbrella を使用するように設定します。 Umbrella をプロビジョニングするには、次のコンポーネントに対する書き込み権限が必要です。 • **[Network Design] > [Network Settings]** • **[Network Provision] > [Provision]** • **[Network Provision] > [Scheduler]** • **[Network Services] > [Umbrella]** また、[Advanced Network Settings] に対する読み取り権限も必要です。

機能	説明
プラットフォーム	アクセス可能なインテントベースのワークフロー、データ交換、通知、統合の設定、およびサードパーティ製アプリケーションの統合に使用できるオープンなプラットフォーム。
API	Cisco DNA Center に REST API を使用してアクセスできます。
バンドル	生産性の向上のために、ITSM との統合用に事前設定されたバンドルを設定およびアクティブ化します。
イベント	ネットワークやシステムの関心があるイベントに登録することで、それらのイベントについての通知をほぼリアルタイムで受け取り、修正処置を開始できます。 電子メールおよび Syslog ログの設定は、**[System]** > **[Settings]** > **[Destinations]** で設定できます。
レポート	事前定義されたレポーティングテンプレートを使用して、ネットワークのあらゆる側面についてのレポートを生成できます。 不正デバイスおよび aWIPS のレポートを生成します。 ウェブフックは、**[System]** > **[Settings]** > **[Destinations]** で設定できます。
セキュリティ	ネットワークへのセキュアなアクセスを管理および制御します。
グループベース ポリシー	シスコのセキュリティグループタグに基づいてネットワークのセグメンテーションとアクセス制御を適用するグループベースポリシーを管理します。このロールには、エンドポイント分析が含まれます。
IP ベースのアクセス制御	IP アドレスに基づいてネットワークのセグメンテーションを適用する IP ベースのアクセス制御リストを管理します。
セキュリティ アドバイザリ	ネットワークをスキャンしてセキュリティアドバイザリを検索します。シスコが公開しているセキュリティアドバイザリでネットワークに影響する可能性がある情報を確認および把握できます。
システム	Cisco DNA Center の構成管理、ネットワーク接続、ソフトウェアアップグレードなどを一元管理します。
機械推論	セキュリティの脆弱性を迅速に特定して問題の自動分析を改善するために、機械推論ナレッジベースの自動更新を設定します。
システム管理	システムのコア機能と接続の設定を管理します。ユーザーロールを管理し、外部認証を設定します。 このロールには、整合性検証、HA、ディザスタリカバリ、デバッグログ、テレメトリコレクション、システムの EULA、IPAM、vManage サーバー、Cisco AI Analytics、バックアップと復元、およびデータプラットフォームが含まれます。

機能	説明
ユーティリティ	広く使用されているトラブルシューティング ツールやサービスなど、生産性に役立つ情報がまとめられています。
監査ログ	UI または API インターフェイスを通じてネットワークデバイスや Cisco DNA Center に加えられた変更の詳細なログ。
イベント ビューア	トラブルシューティングのためのネットワークデバイスおよびクライアントイベントの表示。
ネットワーク推論機能	ネットワーク分野の専門家の知識に基づく、ネットワークの問題についての自動化された論理的なトラブルシューティングを開始します。
リモートデバイスのサポート	シスコサポートチームが Cisco DNA Center によって管理されているネットワークデバイスをリモートでトラブルシューティングできるようにします。このロールを有効にすると、Cisco Technical Assistance Center（TAC）のエンジニアは、トラブルシューティングのためにお客様の Cisco DNA Center のセットアップにリモートで接続できます。
スケジューラ	他のバックエンドサービスと統合されたスケジューラを使用して、ポリシーの展開、プロビジョニング、ネットワークのアップグレードなどのタスクやアクティビティの実行、スケジュール、および監視が行えます。 不正封じ込めをスケジュールすることもできます。
検索	サイト、ネットワークデバイス、クライアント、アプリケーション、ポリシー、設定、タグ、メニュー項目など、Cisco DNA Center のさまざまなオブジェクトを検索します。

ロールベース アクセス コントロール統計の表示

各ユーザーロールに属しているユーザーの数を示す統計を表示できます。ドリルダウンして、選択したロールを持つユーザーのリストを表示することもできます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[Role Based Access Control]** の順に選択します。

デフォルトのすべてのユーザーロールとカスタムロールが表示されます。

ステップ 2 各ユーザーロールに対応する番号をクリックすると、そのロールを持つユーザーのリストが表示されます。

外部認証の設定

外部ユーザーの認証と許可に外部サーバーを使用している場合、Cisco DNA Center で外部認証を有効にする必要があります。

始める前に

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。
- 少なくとも 1 つの認証サーバーを設定する必要があります。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[External Authentication]** の順に選択します。

ステップ 2 Cisco DNA Center で外部認証を有効にするには、[Enable External User] チェックボックスをオンにします。

ステップ 3 （任意） AAA 属性を設定します。

TACACS 認証では、次の AAA 属性がサポートされています。

Cisco DNA Center	TACACS
Empty	cisco-av-pair
cisco-av-pair	cisco-av-pair
Cisco-AVPair	Cisco-AVPair

RADIUS 認証では、次の AAA 属性がサポートされています。

Cisco DNA Center	RADIUS
Empty	cisco-av-pair
Cisco-AVPair	cisco-av-pair

a) 前の表で説明されているように、[AAA Attribute] フィールドに、ユースケースに適した属性を入力します。[AAA Attribute] フィールドのデフォルト値は Null です。

b) [更新（Update）] をクリックします。

ステップ 4 （任意） AAA サーバーを設定します。

これらの設定は、現在のプライマリ AAA サーバーとセカンダリ AAA サーバーを交換したり、異なる AAA サーバーを定義したりする場合にのみ行います。左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]** の順に選択して **[Authentication and Policy Servers]** ウィンドウを開きます。

a) [Primary AAA Server IP Address] ドロップダウンリストで、事前設定されたいずれかの AAA サーバーの IP アドレスを選択します。

b) [Secondary AAA Server IP Address] ドロップダウンリストで、事前設定されたいずれかの AAA サーバーの IP アドレスを選択します。

c) （任意） Cisco ISE サーバーを使用している場合は、必要に応じて設定を更新できます。

Cisco ISE ポリシーの詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「Configure and Manage Policies」を参照してください。

表 *2 : Cisco ISE*サーバーの設定

名前	説明
Shared Secret	デバイスの認証キー。共有秘密の長さは、最大 100 文字です。 AAA アドレスを更新する前に、共有秘密を指定する必要があります。
Username	Cisco ISE CLI にログインするために使用する名前。
Password	Cisco ISE CLI ユーザー名のパスワード。
FQDN	Cisco ISE サーバーの完全修飾ドメイン名（FQDN）。FQDN は、次の形式で、ホスト名およびドメイン名の 2 つのパートで構成されています。 *hostname.domainname.com* たとえば Cisco ISE サーバーの FQDN は、ise.cisco.com である可能性があります。
Subscriber Name	一意のテキスト文字列（`acme` など）。これは Cisco DNA Center から Cisco ISE への統合中に、Cisco ISE に新しい pxGrid クライアントを設定するために使用されます。
Virtual IP Address	Cisco ISE ポリシーサービスノード（PSN）が背後に配置されているロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数の PSN ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

d) （任意） 詳細設定を更新するには、[View Advanced Settings] をクリックして、必要に応じて設定を更新します。

表 *3 : AAA* サーバー詳細設定

名前	説明
Protocol	TACACS または RADIUS。
Authentication Port	AAA サーバーへの認証メッセージのリレーに使用されるポート。 • RADIUS の場合、デフォルトは UDP ポート 1812 です。 • TACACS の場合、ポートは 49 であり、変更できません。

名前	説明
Accounting Port	AAA サーバーへの重要なイベントのリレーに使用されるポート。これらのイベントの情報は、セキュリティと請求の目的で使用されます。 • RADIUS の場合、デフォルトの UDP ポートは 1813 です。 • TACACS の場合、ポートは 49 であり、変更できません。
Retries	Cisco DNA Center が Cisco ISE との接続を試行できる回数。
Timeout	Cisco DNA Center が Cisco ISE からの応答を待機する時間の長さ。タイムアウトの最大値は 60 秒です。

e) [更新（Update）] をクリックします。

二要素認証

二要素認証（2FA）は、ユーザー名とパスワードに加えて識別子手法を使用することで、ユーザー認証のセキュリティを強化するものです。識別子手法は、一般に、実際の対象ユーザーだけが所持し（スマホアプリやキーフォブなど）、元のログイン方法と意図的に異なるものを使用します。

Cisco DNA Center の二要素認証の実装では、トークンクライアント（適切な PIN が入力された後に使い捨てトークンコードを生成）、トークンサーバー（トークンコードを検証）、およびユーザーのアクセスを管理する認証サーバーを使用できます。認証処理には、RADIUS または TACACS+ プロトコルが使用されます。

二要素認証の前提条件

Cisco DNA Center で使用する二要素認証を設定するには、次の前提条件を満たしている必要があります。

- 認証された Cisco DNA Center ユーザーの RBAC ロール認可を伝達する属性値ペアを返すことができる認証サーバー。この例では、Cisco Identity Services Engine（Cisco ISE）2.3 パッチ 1 を使用しています。
- 認証サーバーと統合する二要素トークンサーバー。この例では、RSA Authentication Manager 7.2 を使用しています。
- ソフトウェアトークンを生成するクライアントのマシン上のトークン カード アプリケーション。この例では、RSA SecurID ソフトウェアトークンを使用しています。

二要素認証のワークフロー

以下に、二要素認証が設定されている Cisco DNA Center アプライアンスにユーザーがログインしたときの動作の概要を示します。

1. RSA SecurID トークンクライアントでは、ユーザーは PIN を入力してトークンコードを取得します。
2. Cisco DNA Center ログインページでは、ユーザー名とトークンコードを入力します。
3. Cisco DNA Center では、Cisco ISE へのログイン要求の送信に、RADIUS または TACACS+ プロトコルを使用します。
4. Cisco ISE RSA Authentication Manager サーバーに要求を送信します。
5. RSA Authentication Manager でトークンコードを検証し、ユーザーが正常に認証されたかどうかを Cisco ISE に通知します。
6. ユーザーが認証されている場合、Cisco ISE は認証されたユーザーと設定済みの認可プロファイルを照合し、**role=NETWORK-ADMIN-ROLE** 属性値ペアを返します。
7. Cisco DNA Center ユーザーのロールベース アクセス コントロール（RBAC）ロールに関連付けられている機能およびページへのアクセス権を付与します。

二要素認証の設定

Cisco DNA Center アプライアンスで二要素認証を設定するには、次の手順を実行します。

ステップ 1 RSA Authentication Manager を Cisco ISE と統合します。

a) RSA Authentication Manager で、2 つのユーザー、すなわち **cdnac_admin**（管理者ユーザーロール用）と **cdnac_observer**（オブザーバロール用）を作成します。

詳細については、RSA Self-Service Console Help の「Add a User to the Internal Database」のトピックを参照してください。このトピックにアクセスするには、次の手順を実行します。

1. *RSA Self-Service Console Help* を開きます。
2. [Search help] フィールドで、「**Add a User To the Internal Database**」と入力して、[Search help] をクリックします。

b) 新しい認証エージェントを作成します。

詳細については、*RSA Self-Service Console Help* の「Add an Authentication Agent」のトピックを参照してください。

c) 認証マネージャエージェント設定ファイル（sdconf.rec）を生成します。

1. RSA セキュリティコンソールで、**[Access]** > **[Authentication Agents]** > **[Generate Configuration File]** の順に選択します。

[Configure Agent Timeout And Retries] タブが開きます。

2. [Maximum Retries] と [Maximum Time Between Each Retry] フィールドについては、デフォルト値を使用します。
3. [Generate Configuration File] をクリックします。

   [Download Configuration File] タブが開きます。
4. [Download Now] リンクをクリックします。
5. 画面に指示が表示されたら、[Save to Disk] をクリックして、zip ファイルのローカルコピーを保存します。
6. ファイルを解凍し、このバージョンの sdconf.rec ファイルを使用して、エージェントに現在インストールされているバージョンを上書きします。

d) 手順 1a で作成した **cdnac_admin** ユーザーと **cdnac_observer** ユーザーの PIN を生成します。

詳細については、*RSA Self-Service Console Help* の「Create My On-Demand Authentication PIN」のトピックを参照してください。

e) Cisco ISE を開始するには、**[Administration]** > **[Identity Management]** > **[External Identity Sources]** > **[RSA SecurID]** の順に選択して、[Add] を選択します。

f) [RSA SecurID Identity Sources] ページで、[Browse] をクリックし、ダウンロードした sdconf.rec ファイルを選択して、[Open] をクリックします。

g) [Reauthenticate on Change PIN] チェックボックスをオンにして、[Submit] をクリックします。

ステップ 2 2 つの許可プロファイルを作成します。1 つは Admin ユーザーロール用、もう 1 つは オブザーバユーザーロール用です。

a) Cisco ISE で、**[Policy]** > **[Policy Elements]** > **[Results]** > **[Authorization]** > **[Authorization Profiles]** を選択します。

b) 両方のプロファイルについて、次の情報を入力します。

- [Name]：プロファイル名を入力します。
- [Access Type]：[ACCESS_ACCEPT] を選択します。
- [Advanced Attributes Settings] 領域：最初のドロップダウンリストから [Cisco:cisco-av-pair] を選択します。

  Admin ユーザーロールの認証プロファイルを作成する場合は、2 番目のドロップダウンリストから [Role=NETWORK-ADMIN-ROLE] を選択します。

  オブザーバユーザーロールの認証プロファイルを作成する場合は、2 番目のドロップダウンリストから [Role=OBSERVER-ROLE] を選択します。

ステップ 3 Cisco DNA Center アプライアンスの認証ポリシーを作成します。

『*Cisco Identity Services Engine Administrator Guide*』の「Configure Authentication Policies」のトピックを参照してください。

ステップ 4 2 つの許可ポリシーを作成します。1 つは Admin ユーザーロール用、もう 1 つは オブザーバユーザーロール用です。

『*Cisco Identity Services Engine Administrator Guide*』の「Configure Authorization Policies」のトピックを参照してください。

ステップ 5 RSA Authentication Manager セキュリティコンソールで、ソフトウェアトークンが両方のユーザーに割り当てられていることを確認します。

詳細については、*RSA Self-Service Console Help* の「View a Token」のトピックを参照してください。

（注） トークンを割り当てる必要がある場合は、「Assign a Software Token to a User」のトピックで説明されている手順を実行します。

RADIUS を使用した二要素認証の有効化

RADIUS 用に設定された Cisco ISE サーバーを使用する二要素認証を有効にするには、次の手順を実行します。

ステップ 1 Cisco ISE と Cisco DNA Center を連動させます。

『*Cisco DNA Center Installation Guide*』の「Integrate Cisco ISE with Cisco DNA Center」を参照してください。

ステップ 2 認証に Cisco ISE サーバーを使用するよう Cisco DNA Center を設定します。

「外部認証の設定」を参照してください。

重要 Cisco ISE と Cisco DNA Center の両方に同じ共有秘密を指定していることを確認します。

TACACS+ を使用した二要素認証の有効化

TACACS+ が設定された Cisco ISE サーバーを使用する二要素認証を有効にするには、次の手順を実行します。

ステップ 1 Cisco ISE で、**[Administration]** > **[Network Resources]** > **[Network Devices]** の順に選択すると、[Network Devices] ウィンドウが開きます。

ステップ 2 [TACACS Authentication Settings] をクリックして、その内容を表示します。以前に追加した Cisco DNA Center デバイスに対して共有秘密がすでに設定されていることを確認します。

ステップ 3 **[Work Centers]** > **[Device Administration]** > **[Policy Elements]** を選択すると、[TACACS Profiles] ウィンドウが開きます。

ステップ 4 cdnac_admin および cdnac_observer ユーザーロールの TACACS+ プロファイルを作成します。

a) [Add] をクリックします。

b) 次のタスクを実行します。

- プロファイル名を入力します。
- [Raw View] タブをクリックした後、[Profile Attributes] テキストボックスに次のテキストを入力します。
  - cdnac_admin ユーザーロールの場合は、**Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE** と入力します。
  - cdnac_observer ユーザーロールの場合は、**Cisco-AVPair=ROLE=OBSERVER-ROLE** と入力します。

c) **[保存（Save）]** をクリックします。

ステップ 5 Cisco ISE と Cisco DNA Center を連動させます。

『*Cisco DNA Center Installation Guide*』の「Integrate Cisco ISE with Cisco DNA Center」を参照してください。

ステップ 6 認証に Cisco ISE サーバーを使用するよう Cisco DNA Center を設定します。

「外部認証の設定」を参照してください。

重要 Cisco ISE と Cisco DNA Center の両方に同じ共有秘密を指定していることを確認します。

二要素認証を使用したログイン

二要素認証を使用して Cisco DNA Center にログインするには、次の手順を実行します。

ステップ 1 Cisco DNA Center のログインページで、適切なユーザー名を入力します。

ステップ 2 RSA SecurID トークンクライアントを開き、以前設定した PIN を入力して使い捨てトークンを生成します。

ステップ 3 このトークンをコピーして、Cisco DNA Center のログインページの [Password] フィールドに貼り付けます。

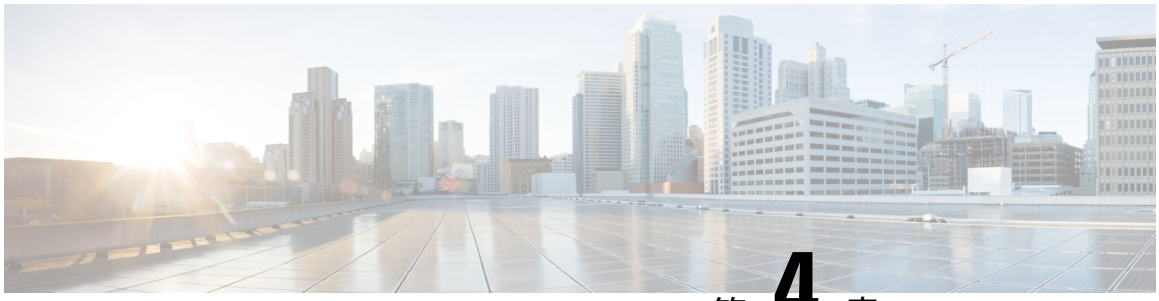
ステップ 4 [Log In] をクリックします。

外部ユーザーの表示

RADIUS/TACACS を使用して初めてログインした外部ユーザーのリストを表示できます。表示される情報には、ユーザー名とロールが含まれます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Users & Roles]** > **[External Authentication]** の順に選択します。

ステップ 2 ウィンドウの下部までスクロールします。[External Users] 領域に外部ユーザーのリストが表示されます。



第 4 章

ライセンスの管理

ライセンスマネージャの概要

Cisco DNA Center ライセンス マネージャ機能は、スマート アカウント ライセンスを含む、シスコ製品のすべてのライセンスの可視化と管理に役立ちます。左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[License Manager]** の順に選択します。[License Manager] ウィンドウには、次の情報のタブが含まれています。

- [Overview]：
  - [Switch]：すべてのスイッチのライセンスの購入情報と使用情報が表示されます。
  - [Router]：すべてのルータのライセンスの購入情報と使用情報が表示されます。

- [Wireless]：すべてのワイヤレスコントローラとアクセスポイントについて、ライセンスの購入情報と使用情報が表示されます。
- [ISE]：Cisco Identity Services Engine（ISE）によって管理されているデバイスのライセンスの購入情報と使用情報が表示されます。

- [Licenses]：[License Summary] には、すべてのシスコデバイスにわたるすべてのタイプのライセンスについて、Cisco Smart Software Management（CSSM）から購入したライセンスの総数、期限切れ間近のライセンスの数、コンプライアンス違反の詳細が表示されます。
- [Devices]：[Devices] テーブルには、ライセンスタイプ、ライセンスの有効期限、ライセンスモード、仮想アカウント、サイト、および Cisco DNA Center による管理対象の各デバイスの登録ステータスが表示されます。
- [Reporting]：[Smart License Compliance] カードを使用すると、[Smart License Update] ワークフローを開始できます。
- [Sync Status]：スマートライセンスポリシー（SLP）に関するコンプライアンスの表には、Cisco DNA Center から CSSM に送信されるライセンス使用状況レポートのデバイスおよびタイムライングラフが表示されます。ステータスに基づいてデバイスをフィルタリングし、コンプライアンスレポートを CSV または PDF 形式でエクスポートできます。

ライセンスを管理するには、各タブに一覧表示されているテーブルの上部にあるコントロールを使用できます。次の表では、各コントロールについて説明します。

（注） すべてのタブですべてのコントロールを使用できるわけではありません。

表 *4*：ライセンス管理のコントロール

制御	説明
Filter	[Filter] をクリックして 1 つ以上のフィルタ値を指定し、[Apply] をクリックします。複数のフィルタを適用することができます。フィルタを削除するには、対応するフィルタ値の横にある **x** アイコンをクリックします。
Change Cisco DNA License	1 つ以上のライセンスを選択し、**[Actions]** > **[Change Cisco DNA License]** の順に選択して、選択した Cisco DNA Center ライセンスのレベルを Essential または Advantage に変更します。このコントロールを使用して Cisco DNA Center ライセンスを削除することもできます。詳細については、ライセンスレベルの変更 （106 ページ）を参照してください。
Change Virtual Account	1 つ以上のライセンスを選択し、**[Actions]** > **[Change Virtual Account]** の順に選択して、ライセンスの管理に使用されるバーチャルアカウントを指定します。
[Manage Smart License] > **[Register]**	スマートライセンスが有効になっているデバイスを 1 つ以上選択し、**[Actions]** > **[Manage Smart License]** > **[Register]** の順に選択して、スマートライセンスが有効になっているデバイスを登録します。

制御	説明
[Manage Smart License] > [Deregister]	スマートライセンスが有効になっているデバイスを 1 つ以上選択し、**[Actions]** > **[Manage Smart License]** > **[Deregister]** の順に選択して、スマートライセンスが有効になっているデバイスを登録解除します。
[Manage License Reservation] > [Enable License Reservation]	特定ライセンス予約（SLR）または永久ライセンス予約（PLR）を適用するデバイスを選択し、**[Actions]** > **[Manage License Reservation]** > **[Enable License Reservation]** の順に選択します。
[Manage License Reservation] > [Update License Reservation]	デバイスが SLR 登録済みの状態である必要があります。 ワイヤレスデバイスまたはスイッチに適用されている SLR を、ワイヤレス コントローラ パッケージで更新できます。 SLR を更新するデバイスを選択し、**[Actions]** > **[Manage License Reservation]** > **[Update License Reservation]** の順に選択します。
[Manage License Reservation] > [Cancel/Return License Reservation]	デバイスを選択し、**[Actions]** > **[Manage License Reservation]** > **[Cancel/Return License Reservation]** の順に選択して、デバイスに適用された SLR または PLR を取り消すか、返却します。
[Manage License Reservation] > [Factory License Reservation]	デバイスを選択し、**[Actions]** > **[Manage License Reservation]** > **[Factory License Reservation]** の順に選択して、工場出荷時にデバイスにインストールされている SLR を有効にします。
Recent Tasks	[Recent Tasks] をクリックして、最近実行された 50 件すべての Cisco DNA Center タスクを表示します。ドロップダウンを使用してリストをフィルタリングし、ステータスが [Success]、[Failure]、または [In Progress] のタスクのみを表示します。
License Usage	[License Usage] をクリックすると、すべてのタイプのライセンスについて、ライセンス使用率が表示されます。
Refresh	[Refresh] をクリックすると、現在のデータを使用してウィンドウがリロードされます。
Find	[Find] フィールドに検索用語を入力し、いずれかの列にその用語が含まれている、リスト内のライセンスをすべて検索します。検索文字列の任意の場所で、ワイルドカードとしてアスタリスク（*）を使用します。
Show Records	テーブルの各ページに表示するレコードの総数を選択します。

ライセンステーブルには、各デバイスに表示される情報が表示されます。すべての列はソートに対応しています。列ヘッダーをクリックすると、行が昇順にソートされます。列ヘッダーをもう一度クリックすると、行が降順にソートされます。

（注） すべてのタブですべての列が使用されるわけではありません。また一部の列は、デフォルトの列ビュー設定で非表示になります。非表示の列を表示するには、歯車アイコンをクリックし、[Edit Table Columns] で、テーブルに表示する列を選択します。

表 5: ライセンスの使用状況情報

カラム	説明
Device Type: Device Series	デバイスの製品シリーズの名前（例：Catalyst 3850 シリーズ イーサネット スタッカブル スイッチ）。詳細については、ライセンス詳細の表示 （105 ページ）を参照してください。
Device Type: Total Devices	Cisco DNA Center によってアクティブに管理されている、この製品シリーズのデバイスの総数。
Purchased Licenses	この製品シリーズのデバイスの購入済み Cisco DNA Center サブスクリプション ライセンスの総数。
Purchased Licenses: Network/Legacy	この製品シリーズのデバイスの購入済みネットワーク（またはレガシー）永久ライセンスの総数。
Used Licenses	この製品シリーズのデバイスに適用された Cisco DNA Center サブスクリプション ライセンスの総数。
Used Licenses: Network/Legacy	この製品シリーズのデバイスのネットワーク永久ライセンスの総数。
Feature Licenses (applicable only for Routers)	セキュリティ、AVC などの特定機能のために購入したライセンスの数。

表 6: すべてのライセンス情報

カラム	説明
Device Name	デバイスの名前。詳細については、ライセンス詳細の表示 （105 ページ）を参照してください。
Device Family	スイッチやハブなど、Cisco DNA Center で定義されているデバイスのカテゴリ。
IP Address	デバイスの IP アドレス。
Device Series	表示されているデバイスが属しているシスコ製品シリーズの正式名称（例：Cisco Catalyst 3850 シリーズ イーサネット スタッカブル スイッチ）。
Cisco DNA License	Cisco DNA Center のライセンスレベル。
Cisco DNA License Expiry	Cisco DNA Center ライセンスの有効期限。
License Mode	Cisco DNA Center のライセンスモード。

カラム	説明
Network License	ネットワークライセンスの種類。
Virtual Account	デバイスのライセンスを管理しているシスコバーチャルアカウントの名前。 バーチャルアカウントとサイト階層は別個のエンティティであり、相互接続されていません。
Site	デバイスが設置されている Cisco DNA Center サイト。
Registration Status	デバイスの登録ステータス。
Authorization Status	デバイスの認証ステータス。
Reservation Status	デバイスの予約ステータス。
Last Updated Time	テーブル内のこのエントリが最後に更新された時刻。
MAC Address	ライセンスデバイスの MAC アドレス。
Term	Cisco DNA Center サブスクリプション ライセンスが有効である合計期間。
Days to Expiry	Cisco DNA Center ライセンス期間が期限切れになるまでの残りの日数。
Software Version	デバイスで現在実行されているネットワーク オペレーティング システムのバージョン。

Cisco スマート アカウントとの統合

Cisco DNA Centerは、簡素化された柔軟性のある自動ソフトウェア、組織全体のデバイス ライセンスの購入、展開、および管理を提供するCisco スマート アカウント、オンラインのシスコ サービスをサポートしています。複数のシスコ スマート アカウントを追加できます。

複数のシスコ スマート アカウントがある場合、1 つのアカウントがデフォルトとして指定され、ライセンスマネージャで可視化およびライセンス操作（登録、ライセンスレベルの変更など）に使用します。

バーチャルアカウントは、Cisco スマートアカウント内の下位区分として機能し、スマートアカウントに関連付けられたライセンスと権限付与の制御を強化します。バーチャルアカウントとサイト階層は別個のエンティティであり、相互接続されていません。

デフォルトのシスコ スマート アカウントを変更した後、CSSM からデータを取得し、[License Manager Overview] および [All License] ウィンドウに表示するまでに数分かかります。

デフォルトアカウントを除くすべてのシスコ スマート アカウントを削除できます。

Cisco スマート アカウントをすでに保有している場合、Cisco DNA Center を使用して次のことができます。

- ライセンスの使用量と有効期限を追跡する
- 人が介入せずに、新しいライセンスを適用および有効にする
- Essentials から Advantage（あるいはその逆）に各デバイスのライセンス レベルを上げ、新たに変更された機能ライセンスのレベルでデバイスをリブートする
- 未使用ライセンスを特定して再適用する

これらの操作は、Cisco DNA Center を離れることなく自動的に実行できます。

ライセンス マネージャのセット アップ

Cisco DNA Center ライセンスマネージャツールを使用する前に、Cisco スマートアカウントへのアクセスを設定する必要があります。

始める前に

- この手順を実行するには、SUPER-ADMIN-ROLE 権限と、適切な RBAC 範囲があることを確認します。
- スマート アカウントの Cisco ユーザー ID とパスワードを収集します。
- スマートアカウントが複数ある場合：Cisco DNA Center で使用するスマートアカウントを選択し、そのアカウントのユーザー ID とパスワードを収集します。
- スマートアカウントを有効にするには、Cisco DNA Center が tools.cisco.com に到達できる必要があります。
- Cisco DNA Center のデバイスにライセンスを適用するには、デバイスがインベントリに存在し、デバイスにサイトが割り当てられている必要があります。また、tools.cisco.com に到達できる必要があります。
- 任意のファイアウォールまたはプロキシで、『*Cisco DNA Center* 設置ガイド』に記載されているすべての使用可能なポート、FQDN、および URL が許可されていることを確認します。

ステップ 1 Cisco DNA Center システム管理者のユーザー名とパスワードを使用してログインします。

ステップ 2 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Cisco.com Credentials]** の順に選択します。

ステップ 3 [Cisco.com Credentials] に、cisco.com アカウントのユーザー名とパスワードを入力します。

ステップ 4 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Smart Account]** の順に選択します。

ステップ 5 [Smart Account] で [Add] をクリックし、スマートアカウントのユーザー名とパスワードを入力します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 スマートアカウントが複数ある場合は、[Add] をクリックして追加のアカウントを入力します。

ステップ 8 スマートアカウントが複数ある場合は、デフォルトのアカウントを 1 つ選択します。ライセンスマネージャは、可視化およびライセンス操作にデフォルトのアカウントを使用します。デフォルトのスマートアカウントを変更するには、次の手順を実行します。

a) 選択したスマートアカウントの横にある [Change] をクリックします。
b) アクティブなスマートアカウントを変更し、デフォルトに設定するスマートアカウントを選択します。
c) [Apply] をクリックします。
デフォルトのアカウントを変更した後、CSSM からデータを取得し、[License Manager Overview] ウィンドウと [All License] ウィンドウに表示するまでに数分かかります。

ステップ 9 スマートアカウントを編集するには、[Actions] 列にある三点リーダーをクリックし、[Edit] を選択します。

ステップ 10 デフォルト以外のスマートアカウントを削除するには、[Actions] 列にある三点リーダーをクリックし、[Delete] を選択します。

ステップ 11 仮想または下位のスマートアカウント名とパスワードを使用してスマートアカウントにアクセスするには、[スマート アカウントのリンク（Link Your Smart Account）] 配下で次のいずれかを選択します。

- [Use Cisco.com user ID]：Cisco.com とスマートアカウントのログイン情報が同じ場合。
- [Use different credentials]：Cisco.com とスマートアカウントのログイン情報が異なる場合は、スマートアカウントのログイン情報を入力します。

ステップ 12 [View all virtual accounts] をクリックし、すべての仮想スマート ライセンス アカウントを表示します。

次のタスク

Cisco DNA Center を、Cisco Plug and Play Connect のコントローラとして、リダイレクト サービス用に Cisco スマート アカウントに登録します。これにより、Cisco Plug and Play Connect クラウドポータルから Cisco DNA Center のネットワーク プラグアンドプレイに、デバイスインベントリを同期することができます。詳細については、『Cisco DNA Center User Guide』の「」を参照してください。

ライセンスの使用状況と有効期限の可視化

Cisco DNA Center では、購入済みのライセンスのグラフィカル表示、使用中のライセンス数（デバイスに割り当てられている数）、およびその期間を表示できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[License Manager]** の順に選択します。

ステップ 2 ライセンスの使用状況を確認するデバイスカテゴリのタイプを選択します。タイプは [Switches]、[Routers]、[Wireless]、[ISE]、[Licenses]、または [Reporting] のいずれかです。

ウィンドウの上部の [License Usage] 円グラフには、購入済みのライセンスの総数と選択したデバイスカテゴリで現在使用中のライセンスの数が表示されます。また、グラフには各合計内での Essentials ライセンスと Advantage ライセンスの割合も示されます。

グラフの下の [License Usage] テーブルには、使用されているライセンスと未使用のライセンスの小計が、製品ファミリ名別にアルファベット順でリストされます。

ステップ 3 特定の製品ファミリの詳細な比較を表示するには、[Device Series] 列で目的の製品ファミリの名前をクリックします。

Cisco DNA Center に、選択した製品ファミリに関する詳細が表示されます。

ステップ 4 ライセンス期間のグラフィカル表示を確認するには、[License Timeline] セクションまでスクロールダウンします。各製品ファミリのタイムライングラフは、その製品ファミリに対して設定したスマートアカウントのライセンスが期限切れになるまでのビジュアル表示です。

ライセンス使用量の履歴傾向の表示

Cisco DNA Center では、CSSM で購入および使用されたすべてのライセンス使用量の履歴傾向を、日次、週次、および月次で表示できます。CSSM には、最大 1 年間の履歴情報が保存されます。

始める前に

Cisco DNA Center を CSSM の特定のスマートアカウントに登録する必要があります。詳細については、Cisco スマート アカウントとの統合 （101 ページ）を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[Tools]** > **[License Manager]** > **[Licenses]** の順に選択します。

- [License Summary] エリアには、CSSM から購入した Cisco DNA Center サブスクリプション ライセンスの総数が表示されます。
- [Smart Account] エリアには、スマートアカウントに関する詳細が表示されます。
- [ESSENTIALS]、[ADVANTAGE]、および [PREMIER] エリアでは、[Total Licenses]、[About to Expire]、および [Out of Compliance] の Cisco DNA Center サブスクリプション ライセンスの数を分類します。
- [License] ウィンドウのテーブルは、[Focus] ドロップダウンリストからの次のビューに基づいて、検出されたデバイスとそのライセンスをフィルタ処理します。
  - バーチャルアカウントビュー
  - ライセンスビュー
  - デバイスシリーズビュー
  - デバイスタイプビュー

• ライセンスタイプビュー

ステップ 2 選択したライセンスの履歴情報を表示するには、そのデバイスの行にあるライセンスリンクをクリックします。

ライセンス詳細 slide-in pane に、選択したデバイスの完全なライセンスの詳細とライセンスの履歴が表示されます。

（注） ライセンス詳細 slide-in pane のタイトルが、選択したデバイスのタイトルと一致します。

ステップ 3 ライセンス詳細 slide-in pane で、[Frequency] ドロップダウンリストから履歴情報の頻度を選択します。

使用可能な頻度は次のとおりです。

• [Daily]：最初の日におけるライセンスデータのスナップショットを表示します。

• [Weekly]：月曜日のライセンスデータのスナップショットを表示します。

• [Monthly]：その月の 1 日におけるライセンスデータのスナップショットを表示します。

頻度の選択に応じて、[Purchased]、[In Use]、および [Balance] のライセンスに基づいたライセンスデータを示すグラフが表示されます。

[License History] テーブルは、頻度の選択に応じて、[Date]、[Purchased]、[In Use]、および [Balance] に基づいてライセンス履歴情報をフィルタ処理します。

（注） CSSM は以前のデータからこの情報を提供するため、ライセンス履歴情報は常に 1 日前のデータです。Cisco DNA Center は、CSSM からライセンスの履歴情報を毎日定期的に取得します。

ライセンス詳細の表示

Cisco DNA Center でライセンス詳細を検索して表示するには、さまざまな方法があります。たとえば、[License Manager] ウィンドウの [Switches]、[Routers]、[Wireless]、[ISE]、または [Devices] タブに表示されたライセンスの使用状況や期間のグラフをクリックできます。各グラフに、各製品ファミリのライセンスについての集約された情報を示すポップアップが表示されます。

次に、[License Manager] の [Devices] テーブルを使用して 1 つのデバイスに関する包括的なライセンスの詳細を取得する方法について説明します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[License Manager]** > **[Devices]** の順に選択します。

[License Manager] ウィンドウには、検出されたすべてのデバイスと、それらのライセンスの一覧を示すテーブルが表示されます。テーブルの情報には、デバイスの種類やライセンスの有効期限など、基本的なデバイスおよびライセンスの情報のみが含まれます。

ステップ 2 必要なライセンス詳細のデバイスを見つけるには、テーブルをスクロールします。必要なデバイスを見つけられない場合、次の操作を行います。

- [Filter]：▽をクリックして、該当するフィールドにフィルタ条件を入力します。（たとえば、[Device Name] フィールドにデバイス名の全体または一部を入力）。フィルタ条件を複数のフィールドに入力することができます。[Apply] をクリックすると、テーブルにはフィルタ条件に一致する情報を表示する行のみが表示されます。

  特定のサイトに属するデバイスを表示する場合は、左側のペインでそのサイトまで移動してクリックします。フィルタ処理されて該当するデバイスが表示されます。サイト階層を示すサイトマーカーがページの上部に表示されます。

- [Find]：[Find] フィールドをクリックし、テーブルの列のいずれかに検索するテキストを入力します。**Enter** を押すと、テーブルは [Find] フィールドの入力に一致するテキストが含まれる最初の行にスクロールします。

- [Customize]：歯車アイコンをクリックし、[Edit Table Columns] で、テーブルに表示する列を選択します。たとえば、[Device Series] を選択解除するか、[Days to Expiry] を選択します。[Apply] をクリックすると、テーブルに選択した列のみが表示されます。

ステップ 3 必要なデバイスが見つかったら、該当するデバイスの行の [Device Name] リンクをクリックします。

Cisco DNA Center に [License Details] slide-in pane が表示され、選択したデバイスのすべてのライセンス詳細情報とライセンス履歴が示されます。[Actions] には、デバイスまたはそのライセンスで実行できるアクションが表示されます。

完了したら ✖ をクリックし、[License Details] slide-in pane を閉じます。

ライセンスレベルの変更

デバイスライセンスの機能レベルを、アップグレードまたはダウングレードすることができます。これは、Cisco DNA Center（サブスクリプション）ライセンスで行うことができます。機能レベルの選択内容は、基本的な Essentials レベルか包括的な Advantage レベルのいずれかです（ネットワークライセンス変換は、Cisco Catalyst 9000 デバイスファミリの製品でのみ使用可能です。Cisco DNA Center ライセンスレベルが変更になると、ネットワークライセンス変換が暗黙のうちに処理されることに注意してください）。

デバイスのライセンスレベルを変更するたびに、Cisco DNA Center は、スマートアカウントを使用して、内部で自動的にライセンスをダウンロードして適用します。

ライセンスレベルの変更を適用するにはデバイスのリブートが必要になるため、License Manager からユーザーに、ライセンスレベルの変更が完了した後にデバイスをリブートするかどうかの確認があります。ライセンスの変更時にリブートしないようにも選択できますが、その場合は後でリブートをスケジュールする必要があります。リブートしなければ、ライセンスレベルの変更は適用されません。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[License Manager]** > **[Devices]** の順に選択します。

[License Manager] ウィンドウには、検出されたすべてのデバイスと、それらのライセンスの一覧を示すテーブルが表示されます。

ステップ 2 [Find] を使用するか、テーブルをスクロールして、ライセンスレベルを変更するデバイスを検索します。デバイスの検索で問題が発生したり、複数のデバイスを選択したりする場合は、ライセンス詳細の表示（105 ページ）のヒントに従ってテーブルを変更し、必要なデバイスだけを表示します。

ステップ 3 ライセンスレベルを変更する各デバイスの横にあるチェックボックスをオンにし、**[Actions]** > **[Change License]** > **[Change Cisco DNA License]** の順に選択します。

Cisco DNA Center は、変更するライセンスタイプの [Change Cisco DNA License Level] ウィンドウを表示します。

ステップ 4 これらのデバイスに必要なライセンスレベル（[Essentials] または [Advantage]）をクリックします。デバイスからライセンスを削除するには、[Remove] をクリックします。

ステップ 5 [Continue] をクリックします。Cisco DNA Center が、変更をすぐに適用するか、後で適用をするかを確認します。また、そのライセンスのステータスを更新すると、デバイスを再起動するかどうかを選択する必要があります。

続行するには、次の操作を行います。

- 変更する準備ができていない場合は、[Back] をクリックしてライセンスレベルの選択を変更するか、 をクリックし、ウィンドウを閉じて変更をキャンセルします。
- すぐに変更する準備ができている場合は、[Now] をクリックし、次に [Confirm] をクリックします。変更が適用されると、このライセンスを使用するデバイスがリブートされます。
- 後で変更を適用する場合は、[Later] をクリックして、スケジュール済みのタスクの名前を入力し、変更を適用する日時を指定します。デバイスが設置されているサイトのタイムゾーンのスケジュールに従って変更を行う場合は、[Site Settings] をクリックします。スケジュールのパラメータの指定が終わったら、[Confirm] をクリックします。

スマートライセンス対応デバイスの自動登録

スマートライセンス（SL）が有効なデバイスの自動登録を有効化することができます。自動登録を有効化すると、Cisco DNA Center に追加される SL が有効なデバイスは、選択したバーチャルアカウントに自動登録されます。

（注） この機能は、Cisco IOS-XE ソフトウェアバージョン 17.3.1 で動作する Smart Licensing Using Policy（SLUP）対応デバイスをサポートしていません。

ステップ 1 Cisco DNA Center システム管理者のユーザー名とパスワードを使用してログインします。

ステップ 2 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Cisco Accounts]** > **[Smart Account]** の順に選択します。

ステップ 3 [License] をクリックします。

ステップ 4 [Auto register smart license enabled device] チェックボックスをオンにします。

ステップ 5 仮想アカウントを選択します。

ステップ 6 [Apply] をクリックします。

スマートライセンス対応デバイスのデイゼロ設定

自動登録を有効にする前に Cisco DNA Center に追加されたデバイスは、自動登録されません。登録されていないスマートライセンス対応デバイスは、[All License] ページで確認できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[License Manager]** > **[Devices]** の順に選択します。

[License Manager] ウィンドウには、自動登録されていない SL 対応デバイスの数と、検出されたデバイスとそのライセンスの一覧が表示されたテーブルのバナーメッセージが、自動登録を設定するリンクとともに表示されます。

また、[Registration Status] 列を使用して、未登録のデバイスをフィルタリングすることもできます。

ステップ 2 登録する SL 対応デバイスを選択し、**[Actions]** > **[Manage Smart License]** > **[Register]** の順に選択します。

ステップ 3 仮想アカウントを選択して [Continue] をクリックします。

ステップ 4 デバイスを登録するには、次のいずれかを実行します。

- すぐにデバイスを登録する場合は、[Now] を選択し、[Confirm] をクリックします。
- 後でデバイスを登録する場合は、[Later] を選択し、日時を指定します。スケジュールのパラメータの指定が終わったら、[Confirm] をクリックします。

デバイスへの特定ライセンス予約またはパーマネントライセンス予約の適用

スマートライセンスでは、スマートデバイスのインスタンスによって Cisco Smart Software Management（CSSM）と定期的に同期して、ライセンスステータスの最新化とコンプライアンスの報告が行われるようにする必要があります。一部のお客様は、インターネットアクセスが制限された高度に保護されたネットワーク内にあるデバイスを使用しています。このようなタ

イプのネットワークでは、デバイスは定期的にCSSMと同期してコンプライアンス違反を表示することができません。このようなお客様の環境をサポートするため、特定ライセンス予約（SLR）およびパーマネントライセンス予約（PLR）が導入されました。Cisco DNA Center のお客様は、ライセンスマネージャで API ベースのワークフローを使用して CSSM から安全にライセンスを予約できます。Cisco DNA Center では、ステージング環境で CSSM に一度接続すれば、デバイスから SLR モードまたは PLR モードでシスコに接続する必要はありません。CSSMへの接続やステージングが実行できない場合は、CSSMで利用できる手動SLR/PLRワークフローが使用できます。

SLRによってお客様は、製品インスタンスにノードロック ライセンス ファイル（SLR承認コード）をインストールできます。このライセンスファイルによって、個別の（特定の）ライセンス（権限付与タグ）が有効化されます。

PLRによってお客様は、製品にすべてのライセンス済み機能を有効化する承認コードをインストールできます。

SLR と PLR の両方に、スマートアカウントのレベルでの事前承認が必要です。サポートが必要な場合は、licensing@cisco.com にご連絡ください。

デバイスと Cisco DNA Center の両方が CSSM に接続されている場合に SLR または PLR を有効にする方法については、デバイスと Cisco DNA Center が CSSM に接続されている場合の SLR/PLR の有効化 （109 ページ） を参照してください。

デバイスと Cisco DNA Center が CSSM に接続されていない場合に SLR または PLR を有効にする方法については、デバイスと Cisco DNA Center が CSSM に接続されていない場合の SLR/PLR の有効化 （110 ページ） を参照してください。

デバイスと Cisco DNA Center が CSSM に接続されている場合の SLR/PLR の有効化

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[License Manager]** > **[Devices]** の順に選択します。

ステップ 2 SLR または PLR を適用するデバイスを選択して、**[Actions]** > **[Manage License Reservation]** > **[Enable License Reservation]** の順にクリックします。

ステップ 3 [Specific License Reservation (SLR)] または [Permanent License Reservation (PLR)] を選択し、[Continue] をクリックして選択したデバイスの要求コードを取得します。

ステップ 4 選択したデバイスの要求コードが生成されたら、[Continue] をクリックします。

ステップ 5 ライセンスを予約するバーチャルアカウントを選択し、[Continue] をクリックして選択したデバイスの承認コードを生成します。

ステップ 6 承認コードが生成されたら、次のいずれかを実行します。

- SLR をすぐに適用する場合は、デバイスを選択して、[Continue] をクリックします。
- 後で SLR を適用する場合は、[Apply Later] をクリックします。

ステップ 7 [Confirm] をクリックして、SLR/PLR を選択したデバイスに適用します。

[All Licenses] ウィンドウの [Reservation Status] に、更新された最新のデバイスのステータスを表示できるようになりました。

デバイスとCiscoDNACenterがCSSMに接続されていない場合のSLR/PLRの有効化

CSSM に接続されていないデバイスの SLR/PLR を有効にするには、次の手順を実行します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[License Manager]** > **[Devices]** の順に選択します。

ステップ 2 SLR または PLR を適用するデバイスを選択して、**[Actions]** > **[Manage License Reservation]** > **[Enable License Reservation]** の順にクリックします。

ステップ 3 [Specific License Reservation (SLR)] または [Permanent License Reservation (PLR)] を選択し、[Continue] をクリックして選択したデバイスの要求コードを取得します。

Telnet を介してデバイスに接続し、要求コードを取得することもできます。

ステップ 4 選択したデバイスの要求コードが生成されたら、[Export] をクリックします。これにより、requestcodes.csv ファイルがダウンロードされます。このファイルには、IP アドレス、デバイスのシリアル番号、および要求コードが含まれています。

ステップ 5 任意の場所にファイルを保存します。

ステップ 6 CSSM から各デバイスの承認コードを取得し、CSV ファイル内で更新します。「CSSM からの承認コードの生成」を参照してください。

ステップ 7 [Upload CSV] リンクをクリックします。

ステップ 8 [Select a file from your computer] リンクをクリックして、保存した CSV ファイルを選択します。

ステップ 9 [Continue] をクリックします。

ステップ 10 ライセンスを予約するバーチャルアカウントを選択し、[Continue] をクリックします。選択したデバイスに SLR または PLR が適用されます。

[All Licenses] ウィンドウの [Reservation Status] に、更新された最新のデバイスのステータスを表示できるようになりました。

CSSM からの承認コードの生成

始める前に

CSSM にログインするには、スマートアカウントのクレデンシャルが必要です。

ステップ 1 **CSSM** にログインします。

ステップ 2 **[Inventory]** > **[Licenses]** > **[License Reservation]** を選択します。[Smart License Reservation] ウィザードが表示されます。

[Licenses] タブの [License Reservation] ボタンは、自分のスマートアカウントで特定ライセンス予約（SLR）を有効にした場合にのみ表示されます。

ステップ 3 [Step 1: Enter Request Code] タブで、[Reservation Request Code] フィールドに要求コードを入力して、[Next] をクリックします。

ステップ 4 [Step 2: Select Licenses] タブで、[Reserve a specific license] チェックボックスをオンにします。

ステップ 5 [Quantity to Reserve] フィールドに、予約するライセンスの数を入力し、[Next] をクリックします。

ステップ 6 [Step 3: Review and Confirm] タブで [Generate Authorization Code] をクリックします。

ステップ 7 [Step 4: Authorize Code] タブで承認コードを取得します。

デバイスに適用された SLR または PLR をキャンセル

デバイスに適用されている SLR または PLR をキャンセルまたは返すことができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[Tools]** > **[License Manager]** > **[Licenses]** の順に選択します。

ステップ 2 デバイスをクリックし、**[Actions]** > **[Manage License Reservation]** > **[Cancel/Return License Reservation]** の順に選択します。

ステップ 3 [Cancel] をクリックしてライセンスを返却します。

[All Licenses] ウィンドウの [Reservation Status] に、更新された最新のデバイスのステータスを表示できるようになりました。

承認コードをインストールし、高セキュリティライセンスを有効にする

シスコでは、デフォルトで250 Mbpsのスループットを提供しています。デバイスのスループットを 250 Mbps 超に増やすには、シスコから承認コードを取得する必要があります。必要に応じて、単一のワークフローまたは個別のワークフローで承認コードをインストールし、高セキュリティ（HSEC）ライセンスを有効にできます。

始める前に

デバイスで Cisco IOS XE リリース 17.3.2 以降が実行されていることを確認します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[License Manager]** > **[Reporting]** の順に選択します。

または、**[Workflows]** > **[Smart License Compliance]** を使用できます。

ステップ 2 [Smart License Compliance] カードをクリックします。

ステップ 3 [Smart License Update] ウィンドウで、[Let's Do It] をクリックします。

今後このウィンドウをスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 4 [Select Smart Account] ウィンドウで、ドロップダウンリストから [Smart Account] と [Virtual Account] を選択します。

ステップ 5 [Next] をクリックします。

ステップ 6 [Choose Sites and Devices] ウィンドウで、承認コードをインストールするデバイスを選択し、[Next] をクリックします。

ステップ 7 [Policy Settings] ウィンドウで、CSSM ポリシーを確認し、[Next] をクリックします。

ステップ 8 [Choose Device Features] ウィンドウで、次の手順を実行します。

a) デバイスを選択します。
b) [Auth Codes] ドロップダウンリストから、[Install] を選択します。
c) [HSEC] ドロップダウンリストから、[Enable] を選択します。
d) [Next] をクリックします。

ステップ 9 [Review Device Features]ウィンドウで、[Next]をクリックします。

ステップ 10 [Installing Device Features] ウィンドウで、承認コードと HSEC インストールステータスを確認し、[Next] をクリックします。

ステップ 11 [Sync Data with Cisco] ウィンドウで [Next] をクリックします。

ステップ 12 [Summary] ウィンドウで承認コードと HSEC インストールステータスを確認したら、[Finish] をクリックします。

高セキュリティライセンスの無効化

HSEC ライセンスを不必要に消費しないように、デバイスの HSEC ライセンスを無効にすることができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[License Manager]** > **[Reporting]** の順に選択します。

ステップ 2 [Smart License Compliance] カードをクリックします。

ステップ 3 [Smart License Update] ウィンドウで、[Let's Do It] をクリックします。

今後このウィンドウをスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 4 [Select Smart Account] ウィンドウで、ドロップダウンリストから [Smart Account] と [Virtual Account] を選択します。

ステップ 5 [Next] をクリックします。

ステップ 6 [Choose Sites and Devices] ウィンドウで、HSEC ライセンスを無効にするデバイスを選択し、[Next] をクリックします。

ステップ 7 [Policy Settings] ウィンドウで、[Next] をクリックします。

ステップ 8 [Choose Device Features] ウィンドウで、次の手順を実行します。

a) デバイスを選択します。

b) [HSEC] ドロップダウンリストから、[Disable] を選択します。

c) [Next] をクリックします。

ステップ 9 [Review Device Features]ウィンドウで、[Next]をクリックします。

ステップ 10 [Installing Device Features] ウィンドウで、 HSEC 無効化操作のステータスを確認し、[Next] をクリックします。

ステップ 11 [Sync Data with Cisco] ウィンドウで [Next] をクリックします。

ステップ 12 [Summary] ウィンドウで [Finish] をクリックします。

CSSM へのリソース使用率の詳細のアップロード

リソース使用率の詳細を CSSM に即座にアップロードしたり、アップロードイベントをスケジュールすることができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[Tools]** > **[License Manager]** > **[Reporting]** の順に選択します。

ステップ 2 [Smart License Compliance] カードをクリックします。

ステップ 3 [Smart License Update] ウィンドウで、[Let's Do It] をクリックします。

今後このウィンドウをスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 4 [Select Smart Account] ウィンドウで、ドロップダウンリストから [Smart Account] と [Virtual Account] を選択します。

ステップ 5 [Next] をクリックします。

ステップ 6 [Choose Sites and Devices] ウィンドウで、リソース使用率の詳細を取得するデバイスを選択し、[Next] をクリックします。

ステップ 7 リソース使用率の詳細を即座にアップロードするには、[Modify Policy] ウィンドウで [Next] をクリックします。定期レポートの頻度を変更するには、次の手順を実行します。

a) [Policy Settings] で、[Reporting Interval] フィールドに対応する [Modify] をクリックします。

b) [Change Reporting Interval] ウィンドウで、値を入力します。

レポート間隔（日数）は、Cisco DNA Center から CSSM へのリソース使用率の詳細の定期的なアップロードの頻度を示します。アップロードの頻度は増やすことができますが、最小レポート頻度未満に減らすことはできません。

c) [保存（**Save**）] をクリックします。

ステップ 8 [Sync Data with Cisco] ウィンドウで [Next] をクリックします。

ステップ 9 [Summary] ウィンドウで [Finish] をクリックします。

CSSM とのデータの同期が成功すると、Cisco DNA Center が確認応答をデバイスに送信します。

次のタスク

ライセンス使用状況レポートが失敗したデバイスの数は、別の [Smart License Compliance] カードに [Retry] オプションとともに表示されます。[Smart License Compliance] カードをクリックし、上記の手順をやり直して、失敗したデバイスから CSSM にライセンス使用状況レポートを送信します。

デバイスのスループットの変更

スマートライセンス対応ルータのスループットを変更できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[License Manager]** > **[Reporting]** の順に選択します。

ステップ 2 変更するデバイスを選択します。

ステップ 3 [More Actions] をクリックし、[Change Throughput] を選択します。

ステップ 4 [Choose Throughput] ウィンドウでスループット値を選択し、[Next] をクリックします。

ステップ 5 [Apply Throughput] ウィンドウで [Next] をクリックします。

ステップ 6 [Recent Tasks] リンクをクリックして、[Recent Tasks] ウィンドウを起動します。

[Recent Task] ウィンドウで [Change Throughput] タスクのステータスを確認できます。

バーチャルアカウント間のライセンスの転送

バーチャルアカウント間でライセンスを転送できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[License Manager]** > **[Licenses]** の順に選択します。

ステップ 2 転送するライセンスを選択し、[Transfer Licenses] をクリックします。

ステップ 3 [Transfer Licenses] ウィンドウで、バーチャルアカウントを選択します。

ステップ 4 選択した各ライセンスの [Transfer License Count] を入力し、[Transfer] をクリックします。

ステップ 5 [Recent Tasks] リンクをクリックして、[Recent Tasks] ウィンドウを起動します。

[Recent Task] ウィンドウで [License Transfer] タスクのステータスを確認できます。

スマートライセンス対応デバイスでの顧客タグの管理

スマートライセンス対応デバイスに最大4つの顧客タグを追加して、製品インスタンスのテレメトリデータの識別を容易にすることができます。顧客タグを更新および削除することもできます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[License Manager]** > **[Reporting]** の順に選択します。

ステップ 2 顧客タグを追加するデバイスを選択します。

ステップ 3 [More Actions] をクリックし、[Manage Free Form Fields] を選択して、顧客タグを追加、更新、または削除します。

ステップ 4 顧客タグを追加または更新するには、[Free Form Fields] ウィンドウで次の手順を実行します。

a) 顧客タグを入力します。

b) [**保存**（**Save**）] をクリックします。

ステップ 5 顧客タグを削除するには、[Free Form Fields] ウィンドウで次の手順を実行します。

a) 削除する顧客タグの削除アイコンをクリックします。

b) [**保存**（**Save**）] をクリックします。

c) [Warning] ウィンドウで [Continue] をクリックします。

ステップ 6 [Recent Tasks] リンクをクリックして、[Recent Tasks] ウィンドウを起動します。

[Recent Task] ウィンドウで [Manage Customer Tags] タスクのステータスを確認できます。

ライセンスポリシーの変更

ネットワークデバイスが CSSM に機能の使用状況を報告するレポート間隔を変更できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[Tools]** > **[License Manager]** > **[Reporting]** の順に選択します。

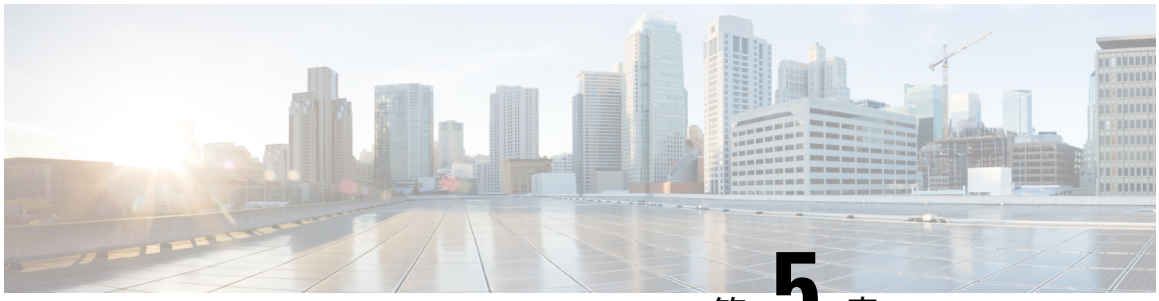
ステップ 2 [Smart License] テーブルで、[Modify Policy] をクリックします。

[Modify Policy] ウィンドウに、ポリシー設定と CSSM ポリシーの詳細が表示されます。

ステップ 3 [Policy Settings] で、[Modify] をクリックします。

ステップ 4 [Change Reporting Interval] ウィンドウで、レポート間隔の値を入力します。

ステップ 5 [Save] をクリックします。



第 5 章

バックアップと復元

バックアップと復元について

バックアップおよび復元機能を使用して、バックアップファイルを作成し、同じ仮想アプライアンスまたは別の仮想アプライアンスに復元できます（ネットワーク構成に必要な場合）。

自動化と アシュアランス データは、単一のデータストレージデバイスを使用するように統合されます。データは、仮想マシンに接続されている物理ディスクまたはリモートのネットワークファイルシステム（NFS）サーバーに保存できます。

Backup

自動化データと アシュアランス データの両方をバックアップできます。

自動化データは、Cisco DNA Center データベース、クレデンシャル、ファイルシステム、およびファイルで構成されています。自動化バックアップは常に完全バックアップです。

アシュアランスデータは、ネットワークアシュアランスと分析データで構成されています。アシュアランスデータの最初のバックアップは完全バックアップで、その後は増分バックアップです。

（注） バックアップファイルは変更しないでください。変更すると、バックアップファイルを Cisco DNA Center に復元できない場合があります。

Cisco DNA Center はバックアップファイルを作成して、物理ディスクまたは NFS サーバーにポストします。

バックアップ用に複数の物理ディスクを追加できます。以前のバックアップディスクのディスク容量が不足している場合は、他の追加されたディスクをバックアップに使用できます。物理ディスクの追加方法については、「バックアップと復元用の物理ディスクの追加 （122 ページ）」を参照してください。新しいディスクをバックアップの場所として使用するには、**[System]** > **[Settings]** > **[Backup Configuration]** ウィンドウでディスクを変更し、変更を保存する必要があります。物理ディスクの変更方法については、「バックアップファイルを保存する場所の設定 （126 ページ）」を参照してください。

複数の NFS サーバーをバックアップ用に追加することもできます。NFS サーバーの追加方法については、「NFS サーバーの追加 （125 ページ）」を参照してください。新しい NFS サーバーをバックアップの場所として使用するには、**[System]** > **[Settings]** > **[Backup Configuration]** ウィンドウで NFS サーバーを変更し、変更を保存する必要があります。NFS サーバーの変更方法については、「バックアップファイルを保存する場所の設定 （126ページ）」を参照してください。

（注） 一度に 1 つのバックアップのみ実行できます。一度に複数のバックアップを実行することはできません。

バックアップの実行中は、バックアップサーバーにアップロードされたファイルを削除することはできず、ファイルに加えた変更はバックアッププロセスによってキャプチャされないことがあります。

次の点を推奨します。

- データベースとファイルの現在のバージョンを維持するために毎日バックアップを実行する。
- 設定に変更を加えた後はバックアップを実行する（デバイスで新しいポリシーを作成または変更した場合など）。
- バックアップは影響の少ない時間帯かメンテナンス時間にのみ実行する。

週の特定日の時刻に週単位のバックアップをスケジュールできます。

Restore

Cisco DNA Center を使用して物理ディスクまたは NFS サーバーからバックアップファイルを復元できます。

ESXi 上の Cisco DNA Center はバージョン間のバックアップと復元をサポートします。つまり、ESXi 上の Cisco DNA Center の 1 つのバージョンでバックアップを作成し、ESXi 上の Cisco DNA Center の別のバージョンに復元できます。現在、ESXi 上の Cisco DNA Center のバージョン 2.3.7.0-75530 のバックアップは、 ESXi 上の Cisco DNA Center のバージョン 2.3.7.3-75176 に復元できます。

（注） 仮想マシンで作成されたバックアップは、同じまたはそれ以降のソフトウェアバージョンの仮想マシンでのみ復元できます。

バックアップファイルを復元すると、Cisco DNA Center によって既存のデータベースとファイルが削除され、バックアップデータベースとファイルで置き換えられます。復元を実行している間、Cisco DNA Center は使用できません。

故障または障害が発生した仮想アプライアンスのバックアップファイルを復元できます。詳細については、障害が発生した仮想アプライアンスの物理ディスクからのデータの復元（132ページ）および障害が発生した仮想アプライアンスのNFSサーバーからのデータの復元（138ページ）を参照してください。

バックアップは、別の IP アドレスを持つ Cisco DNA Center アプライアンスに復元することもできます。

（注） Cisco DNA Center のバックアップおよび復元後、[Integration Settings] ウィンドウにアクセスし、（必要に応じて）[Callback URL Host Name] または [IP Address] を更新する必要があります。

バックアップと復元のイベント通知

バックアップまたは復元イベントが発生するたびに通知を受信できます。これらの通知を設定およびサブスクライブするには、『*Cisco DNA Center Platform User Guide*』の「Work with Event Notifications」トピックで説明されている手順を実行してください。この手順を完了したら、[SYSTEM-BACKUP]イベントと [SYSTEM-RESTORE]イベントを選択し、サブスクライブしていることを確認します。

動作	イベント
バックアップ	システムのバックアップファイルを作成するプロセスが開始された。
	システムのバックアップファイルを作成できなかった。 • このイベントは通常、必要なディスク容量がリモートストレージにないために発生します。 • システムでバックアップファイルを作成中に、接続の問題や遅延が発生しました。

動作	イベント
復元	バックアップファイルを復元するプロセスが開始された。
	バックアップファイルの復元に失敗した。 • このイベントは通常、バックアップファイルが破損しているために発生します。 • システムでバックアップファイルを作成中に、接続の問題や遅延が発生しました。

NFS バックアップサーバーの要件

NFS サーバーのデータバックアップをサポートするには、サーバーが次の要件を満たす Linux ベースの NFS サーバーである必要があります。

- NFS v4 および NFS v3 をサポートしている（このサポートを確認するには、サーバーから **nfsstat -s** を入力します）。
- NFS エクスポートディレクトリに対する読み取り/書き込み権限がある。
- ESXi 上の Cisco DNA Center と NFS サーバー間のネットワーク接続が安定している。
- ESXi 上の Cisco DNA Center と NFS サーバー間のネットワーク速度が十分速い。

（注） NFS 搭載ディレクトリを ESXi 上の Cisco DNA Center のバックアップ サーバー ディレクトリとして使用することはできません。カスケードされた NFS マウントは遅延の層が増えるため、サポートされません。

複数の ESXi 上の Cisco DNA Center を展開するための要件

ネットワークに複数の Cisco DNA Center クラスタが含まれている場合、次の設定例は、NFS サーバーのバックアップディレクトリ構造に名前を付ける方法を示しています。

リソース	設定例
ESXi 上の Cisco DNA Center クラスタ	1. *cluster1* 2. *cluster2*
自動化と アシュアランス のバックアップをホストするバックアップサーバー	例示したディレクトリは `/data/` で、両方のタイプのバックアップをホストする十分なスペースがあります。

NFS エクスポート設定	/etc/exports ファイルの内容：
	`/data/cluster1 *(rw,sync,no_subtree_check,all_squash)`
	`/data/cluster2 *(rw,sync,no_subtree_check,all_squash)`

バックアップ物理ディスクの名称

バックアップに物理ディスクを使用するには、仮想マシンに物理ディスクを追加する必要があります。バックアップ用の物理ディスクを容易に識別するために、UUID が使用されます。

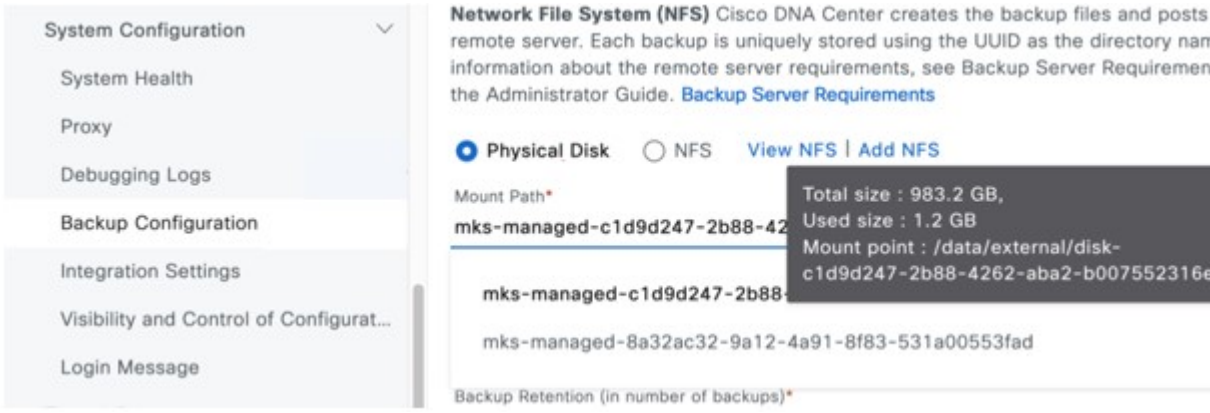
UUIDは、ディスクに関連付けられている一意の識別子であり、再起動しても変更されません。削除されて別のクラスタに追加されたディスクは、再度フォーマットされない限り、同じUUIDを持ちます。

ディスクは `mks-managed` として明示的にラベル付けされます。

バックアップに使用可能な物理ディスクは、**[System]** > **[Settings]** > **[Backup Configuration]** ウィンドウの [Mount Path] ドロップダウンリストで確認できます。

[i]アイコンにマウスのカーソルを合わせると、その物理ディスクの名称が次の形式で表示されます。

```
/data/external/disk-<uuid>
```



バックアップ ストレージ要件

ESXi 上の Cisco DNA Center は、 アシュアランス のバックアップコピーと自動化データを、仮想マシンまたはリモート NFS サーバーに接続されている物理ディスクに保存します。バックアップには、必要な保存期間をカバーするのに十分な外部ストレージを割り当てる必要があります。次のストレージを推奨します。

仮想アプライアンス	アシュアランスデータストレージ（14日単位で増分）	自動化データストレージ（日次でフル）	物理ディスク/NFSサーバー（アシュアランスおよび自動化）ストレージ
DN-SW-APL	1.75 TB	50 GB	1.75 TB + 50 GB

補足事項：

- 上記の表は、各アプライアンスのアクセスポイントとネットワークデバイスの最大数をサポートする、フル装備の仮想アプライアンス構成を前提としています。
- 自動バックアップの量は、1日1回のバックアップで見積もられます。バックアップを保持する日数を追加する場合は、必要なストレージ容量 x 追加する日数で算出します。たとえば、DN-SW-APL 仮想アプライアンスがあり、1日1回生成される自動化データバックアップのコピーを 5 つ保存する場合、必要なストレージの合計は 5 x 50 GB = 250 GB です。
- バックアップ時間の合計は、毎日のデータロードと保持する履歴データの量によって異なります。
- Cisco DNA Center への書き込みパスは、 Cisco DNA Center から NFS サーバーへのネットワークスループットによって異なります。NFSサーバーのスループットは、少なくとも 100 MB/秒である必要があります。
- 他のITサービスと同様に、最適なパフォーマンスを確保するには、NFSのパフォーマンスをモニタリングする必要があります。

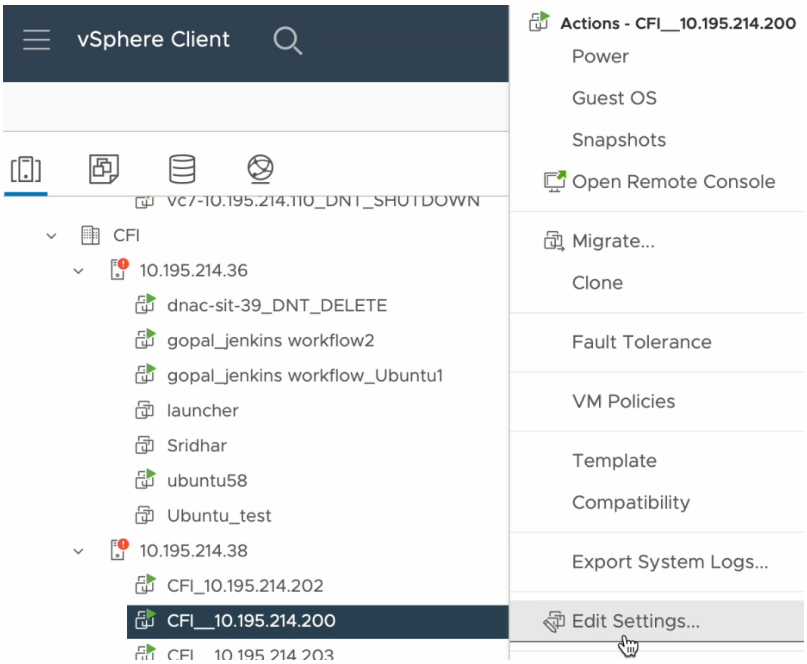
バックアップと復元用の物理ディスクの追加

バックアップと復元操作に使用できる物理ディスクを追加するには、次の手順を実行します。

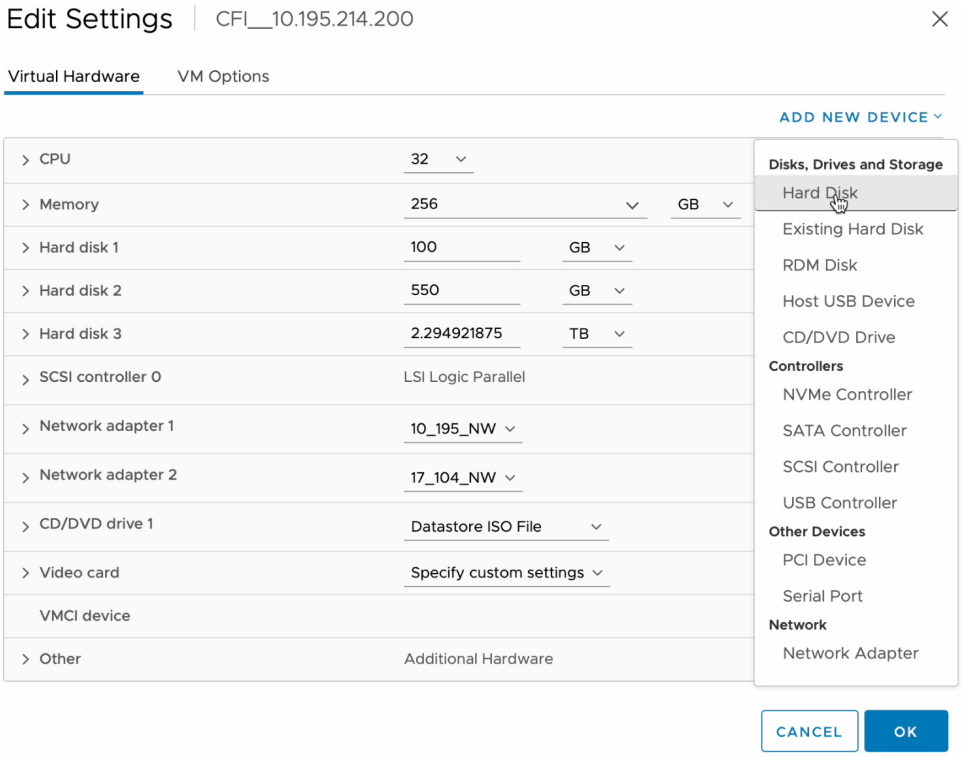
ステップ 1 ESXi 上の Cisco DNA Centerをホストしているマシンでアプライアンスが実行されている場合は、アプライアンスの仮想マシンの電源をオフにします。

ステップ 2 VMware vSphere にログインします。

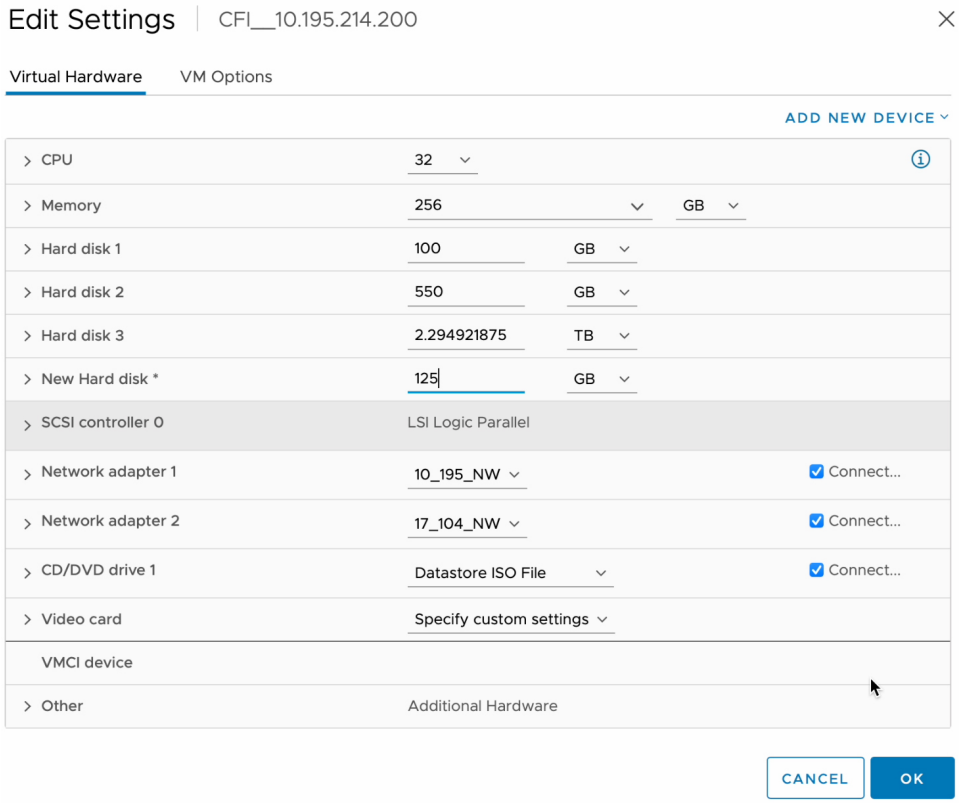
ステップ 3 vSphere クライアントの左側のペインで、ESXi ホストを右クリックし、[Edit Settings] を選択します。



ステップ 4 [Edit Settings] ダイアログボックスで [Add New Device] をクリックし、[Hard Disk] を選択します。



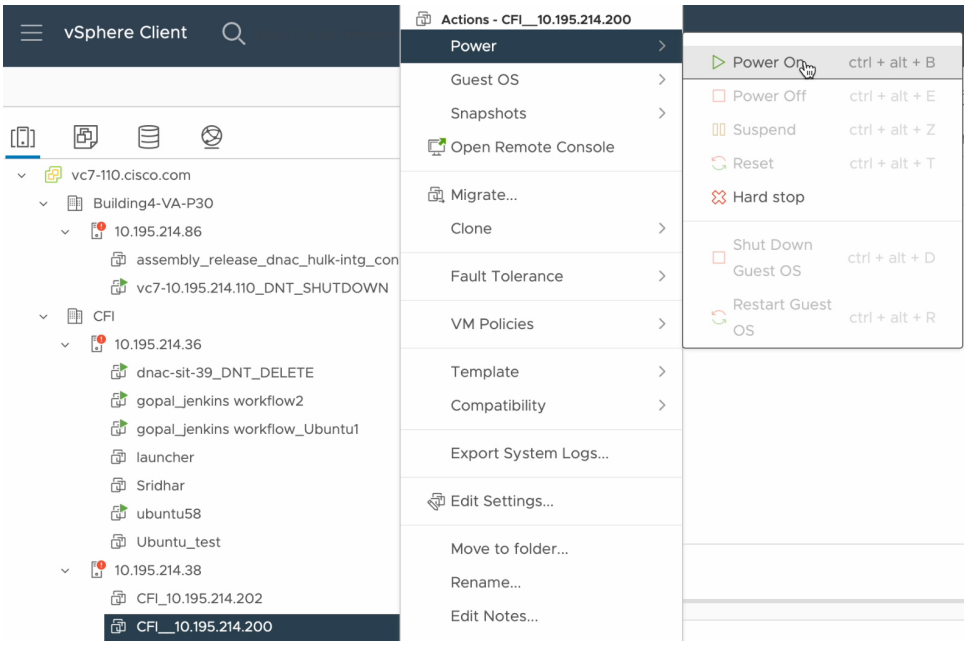
ステップ 5 [New Hard disk] フィールドに、目的のストレージサイズを入力します。



（注） バックアップに推奨されるストレージ容量の詳細については、「バックアップストレージ要件（121 ページ）」を参照してください。

ステップ 6 [OK] をクリックします。

ステップ 7 アプライアンスの仮想マシンの電源をオンにします。



次のタスク

追加した物理ディスクをバックアップ用に設定できます。物理ディスクの設定方法については、「バックアップファイルを保存する場所の設定 （126 ページ）」を参照してください。

NFS サーバーの追加

Cisco DNA Center では、バックアップ用に複数の NFS サーバーを追加できます。バックアップ操作に使用できる NFS サーバーを追加するには、次の手順を実行します。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Settings]** > **[Backup Configuration]** の順に選択します。

ステップ 2 [Add NFS] リンクをクリックします。

ステップ 3 [Add NFS slide-in pane] で次の手順を実行します。

a) それぞれのフィールドに [Server Host] と [Source Path] を入力します。

b) ドロップダウンリストから [NFS Version] を選択します。

c) [Port] はデフォルトで追加されます。このフィールドは空のままにもできます。

d) [Port Mapper] 番号を入力します。

e) [Save] をクリックします。

ステップ 4 [View NFS] をクリックして、使用可能な NFS サーバーを表示します。[NFS slide-in pane] には、NFS サーバーのリストが詳細とともに表示されます。

ステップ 5 [NFS slide-in pane] で [Actions] の下にある省略記号をクリックして、NFS サーバーを削除します。

（注）　進行中のバックアップジョブがない場合にのみ、NFS サーバーを削除できます。

次のタスク

バックアップ用に追加した NFS サーバーを設定します。詳細については、バックアップファイルを保存する場所の設定 （126 ページ）を参照してください。

バックアップファイルを保存する場所の設定

Cisco DNA Center では、自動化と アシュアランス データのバックアップを設定できます。

バックアップファイルの保存場所を設定するには、次の手順を実行します。

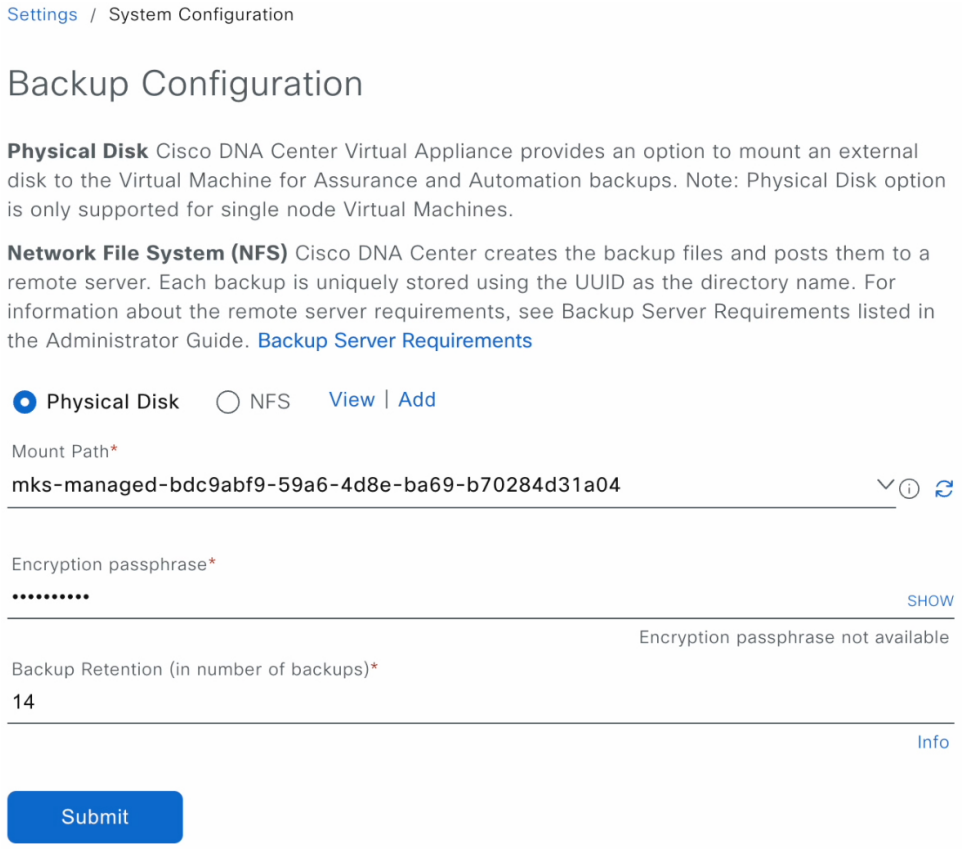
始める前に

次の要件が満たされていることを確認します。

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。
- データバックアップサーバーがNFS バックアップサーバーの要件 （120 ページ）で説明されている要件を満たしている。

ステップ 1　左上隅にあるメニューアイコンをクリックして、 **[System]** > **[Settings]** > **[System Configuration]** > **[Backup Configuration]** の順に選択します。

物理ディスクまたは NFS サーバーをバックアップの場所として選択できます。



ステップ 2 [Physical Disk]： Cisco DNA Center は、アシュアランス のバックアップコピーと自動化データを保存するため、外部ディスクを仮想マシンにマウントするオプションを提供します。物理ディスクを設定するには、[Physical Disk] ラジオボタンをクリックし、次の設定を定義します。

（注） 物理ディスクオプションは、単一ノード仮想マシンでのみサポートされます。

フィールド	説明
マウント パス	外部ディスクの場所。
Encryption Passphrase	バックアップのセキュリティの影響を受けやすいコンポーネントを暗号化するために使用するパスフレーズ。これらのセキュリティに影響を受けやすいコンポーネントには、証明書とクレデンシャルが含まれます。 このパスフレーズは必須で、バックアップファイルを復元するときに入力を求められます。このパスフレーズがなければ、バックアップファイルは復元されません。
バックアップの保持	データを保持するバックアップ数。 指定したバックアップ数より古いデータは削除されます。

ステップ 3 [NFS]： Cisco DNA Center はバックアップファイルを作成して、リモート NFS サーバーにポストします。リモートサーバーの要件の詳細については、NFS バックアップサーバーの要件 （120 ページ）を参照して

ください。NFS バックアップサーバーを設定するには、[NFS] ラジオボタンをクリックして次の設定を定義します。

フィールド	説明
マウント パス	リモートサーバーの場所。
Encryption Passphrase	バックアップのセキュリティの影響を受けやすいコンポーネントを暗号化するために使用するパスフレーズ。これらのセキュリティに影響を受けやすいコンポーネントには、証明書とクレデンシャルが含まれます。 このパスフレーズは必須で、バックアップファイルを復元するときに入力を求められます。このパスフレーズがなければ、バックアップファイルは復元されません。
バックアップの保持	データを保持するバックアップ数。 指定したバックアップ数より古いデータは削除されます。

ステップ 4 [Submit] をクリックします。`

要求が送信されると、**[System]** > **[Backup & Restore]** で、設定された物理ディスクまたは NFS サーバーを表示できます。

バックアップの作成

仮想アプライアンスのバックアップを作成するには、次の手順を使用します。

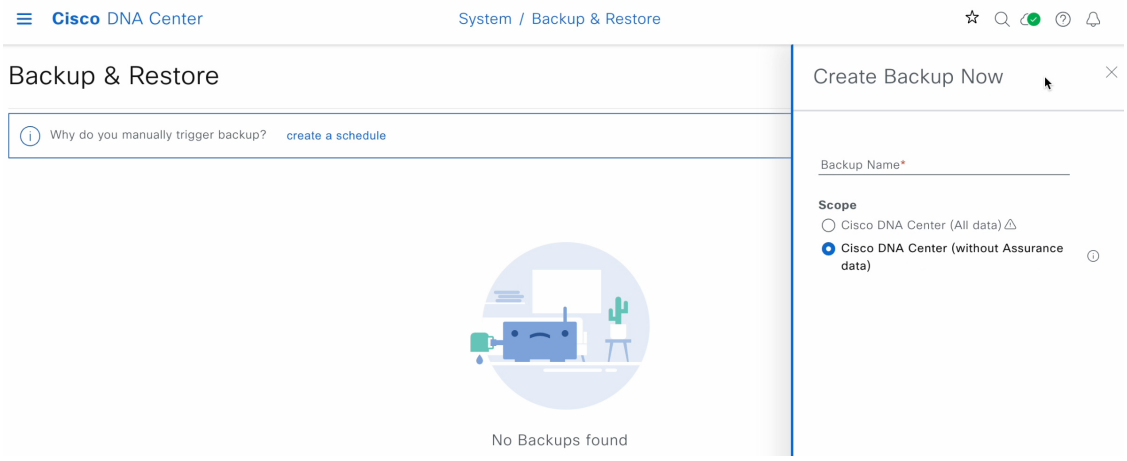
始める前に

バックアップの場所を設定する必要があります。詳細については、バックアップファイルを保存する場所の設定 （126 ページ）を参照してください。

ステップ 1 ESXi 上の Cisco DNA Center メニューから **[System]** > **[Backup & Restore]** を選択します。

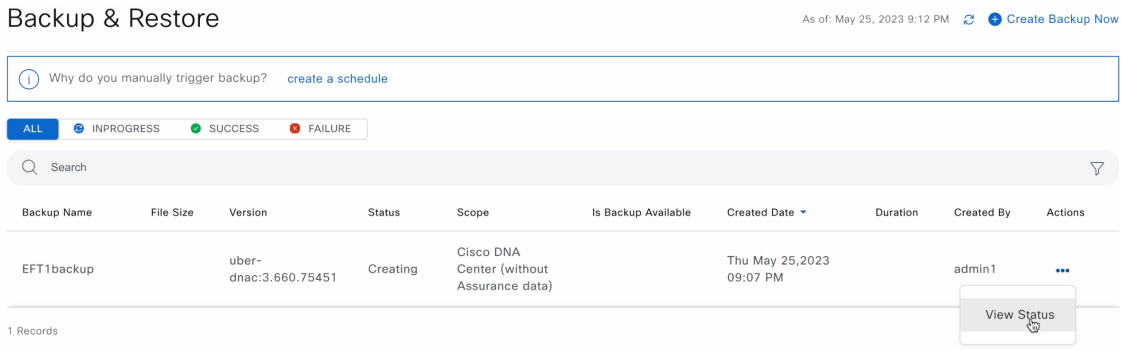
ステップ 2 [Create Backup Now] をクリックします。

[Create Backup Now] スライドインペインが表示されます。



ステップ 3 バックアップの一意の名前を入力し、[Save] をクリックします。

ESXi 上の Cisco DNA Center がバックアッププロセスを開始します。バックアップのエントリが [Backup & Restore] ウィンドウのテーブルに追加されます。バックアップのステータスに関する詳細を表示するには、省略記号をクリックし、[View Status] を選択します。



バックアップが完了すると、ステータスが [Creating] から [Success] に変わります。

バックアップからデータを復元

仮想アプライアンスからバックアップデータを復元するには、この手順を使用します。故障または障害が発生した仮想アプライアンスからバックアップファイルを復元する場合は、障害が発生した仮想アプライアンスの物理ディスクからのデータの復元（132 ページ）を参照してください。

⚠

注意 Cisco DNA Center の復元プロセスでは、データベースとファイルのみ復元します。復元プロセスでは、ネットワークの状態や、最後のバックアップ以降に加えられた変更は復元されません。これには、新しいネットワークポリシーやパスワード、証明書、トラストプールバンドル、または更新されたこれらのものが含まれます。

始める前に

次の要件が満たされていることを確認します。

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。
- データを復元する元となるバックアップがあること。

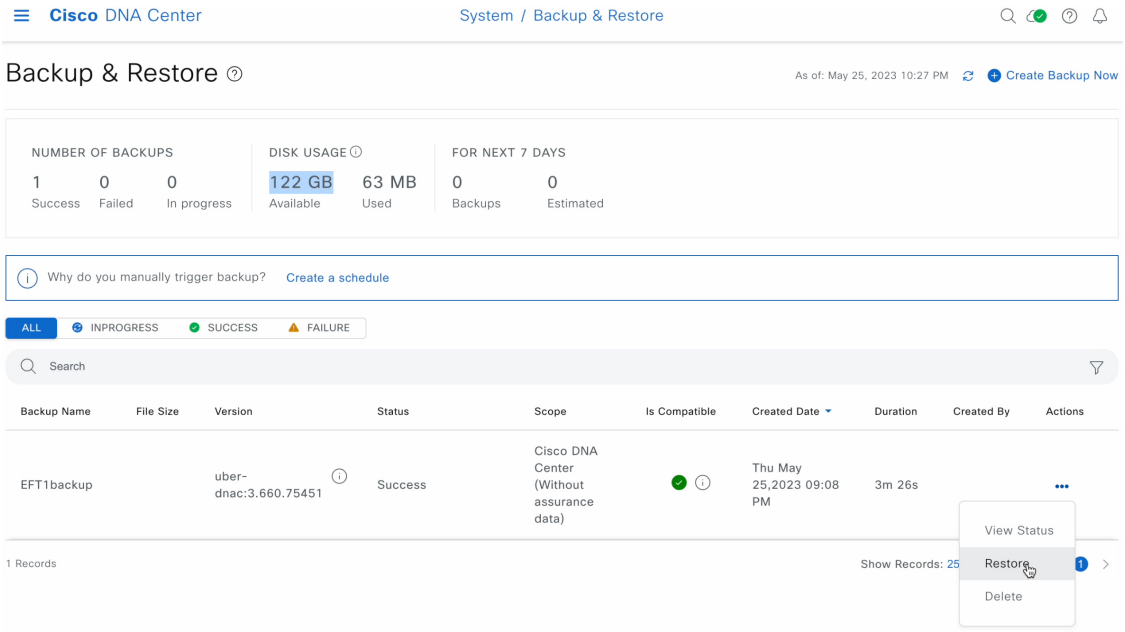
データを復元する場合、ESXi 上の Cisco DNA Center はメンテナンスモードに入り、復元プロセスが終わるまで使用できません。ESXi 上の Cisco DNA Center を使用不可にできるときにデータを復元してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、**[System]** > **[Backup & Restore]** の順に選択します。

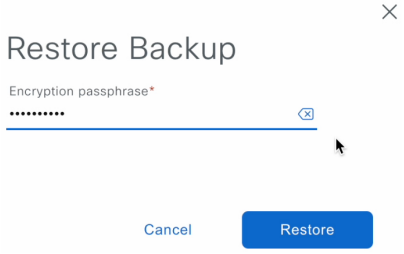
作成したバックアップは、[Backup & Restore] ウィンドウに表示されます。

ステップ 2 [Backup Name] 列で、復元するバックアップを特定します。

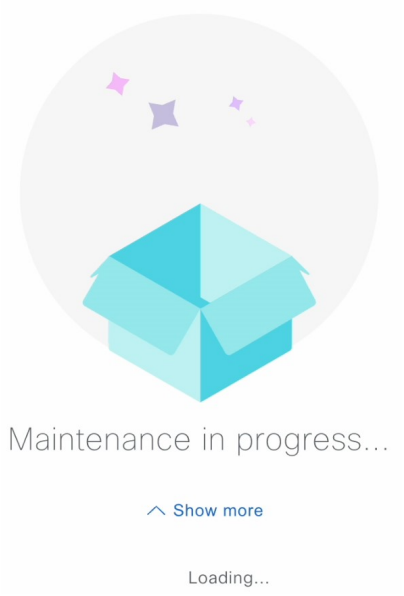
ステップ 3 [Actions] 列で、省略記号をクリックし、[Restore] を選択します。



ステップ 4 [Restore Backup] ダイアログボックスで、バックアップ場所の設定時に使用した**暗号化パスフレーズ**を入力し、[Restore] をクリックします。

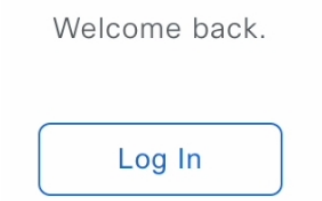


アプライアンスがメンテナンスモードになり、復元プロセスを開始します。

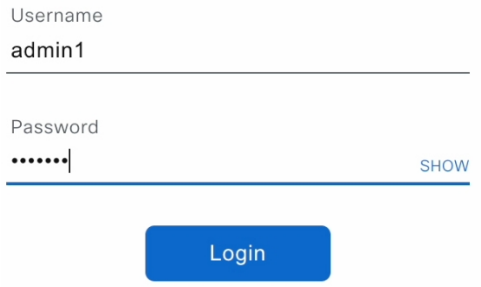


復元操作が完了すると、[Backup & Restore] ウィンドウのテーブルのステータスが [Success] に変更されます。

ステップ 5 復元操作が完了したら、[Log In] をクリックして ESXi 上の Cisco DNA Centerに再度ログインします。



ステップ 6 管理者ユーザーのユーザー名とパスワードを入力して、[Login] をクリックします。

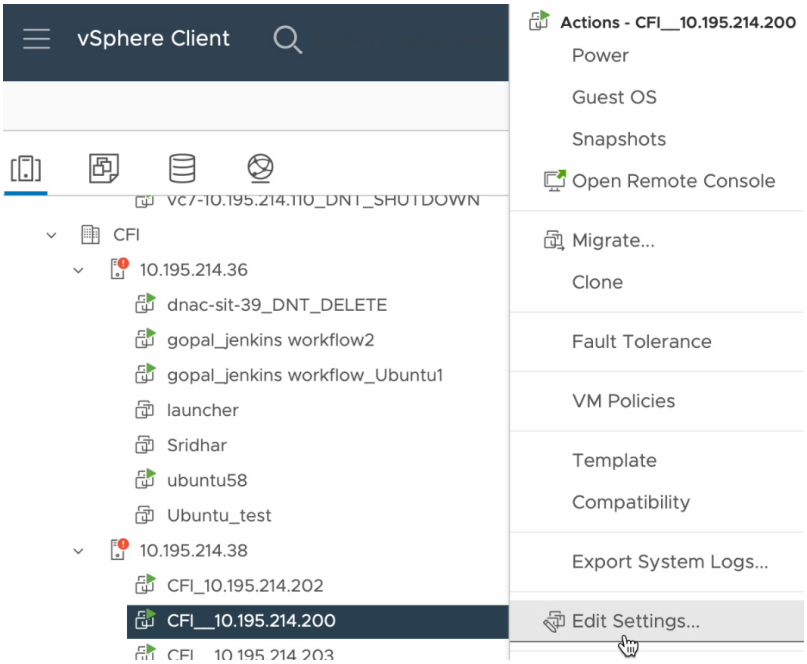


障害が発生した仮想アプライアンスの物理ディスクからのデータの復元

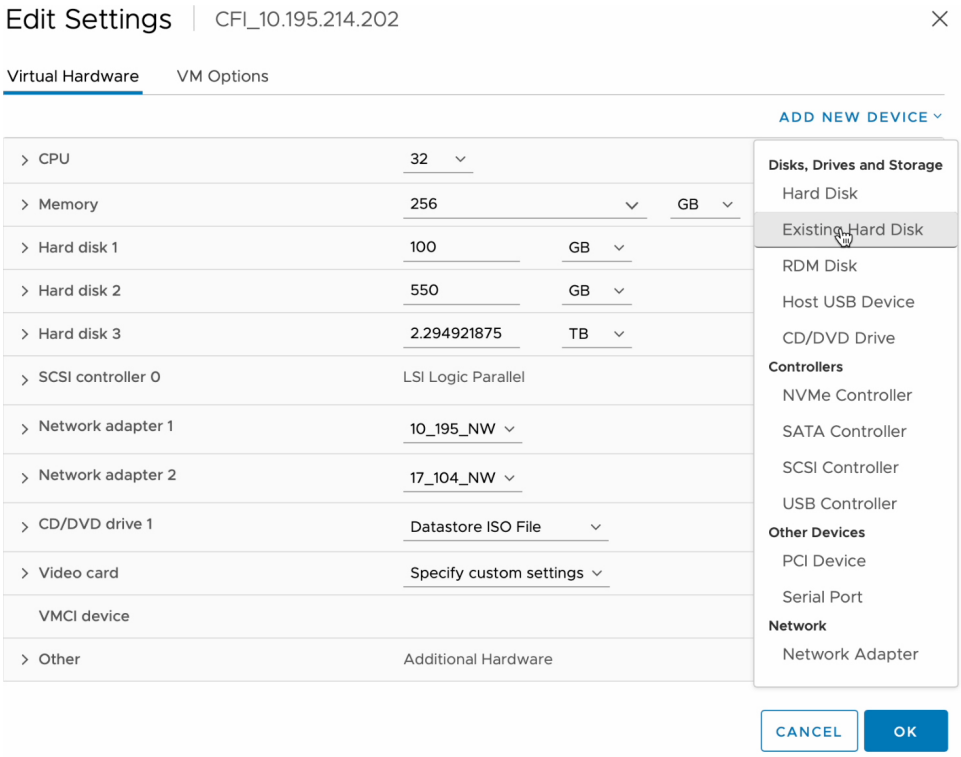
故障または障害が発生した仮想アプライアンスの物理ディスクからデータを復元するには、次の手順を実行します。

ステップ 1 新しい仮想アプライアンスで、障害のある仮想アプライアンス用に設定したストレージディスクを使用するように ESXi 上の Cisco DNA Center を設定するには、次の手順を実行します。

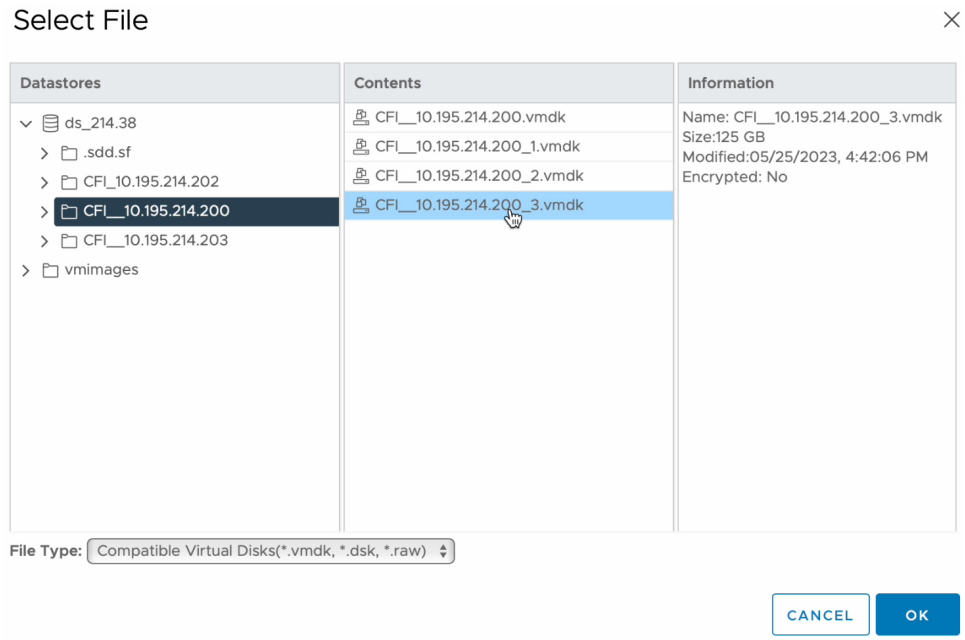
1. アプライアンスの仮想マシンの電源をオフにします。
2. vSphere Client を開き、左ペインの ESXi 上の Cisco DNA Center 仮想マシンを右クリックして [Edit Settings] を選択します。



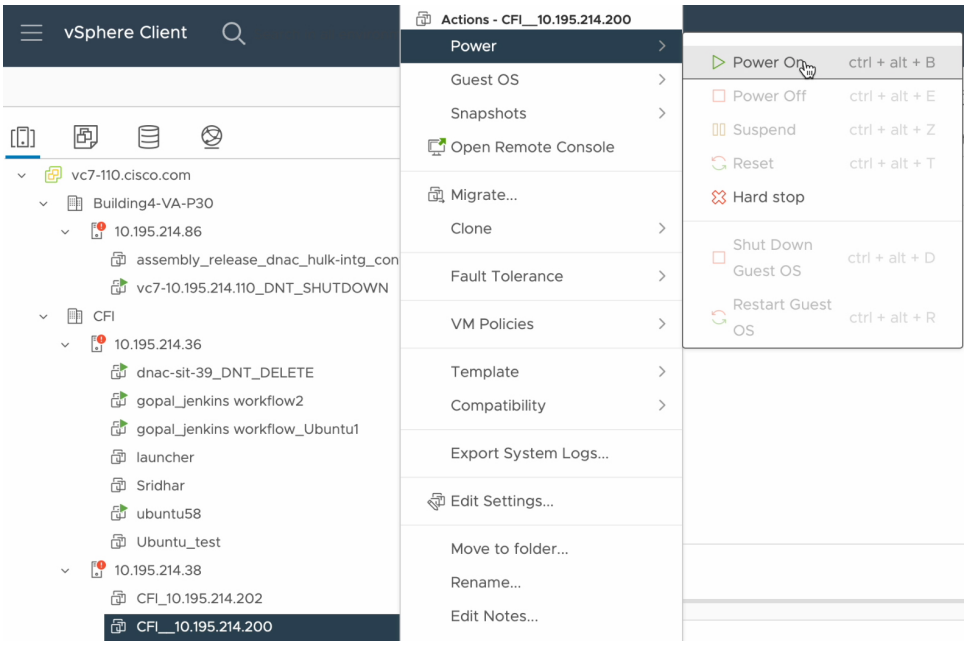
3. [Edit Settings] ダイアログボックスで [Add New Device] をクリックし、[Existing Hard Disk] を選択します。



4. [Select File] ダイアログボックスで ESXi ホストをクリックし、作成したストレージディスク（.vmdk）をクリックして [OK] を選択します。



5. アプライアンスの仮想マシンの電源をオンにします。



すべてのサーバーが再起動するには約 45 分かかります。

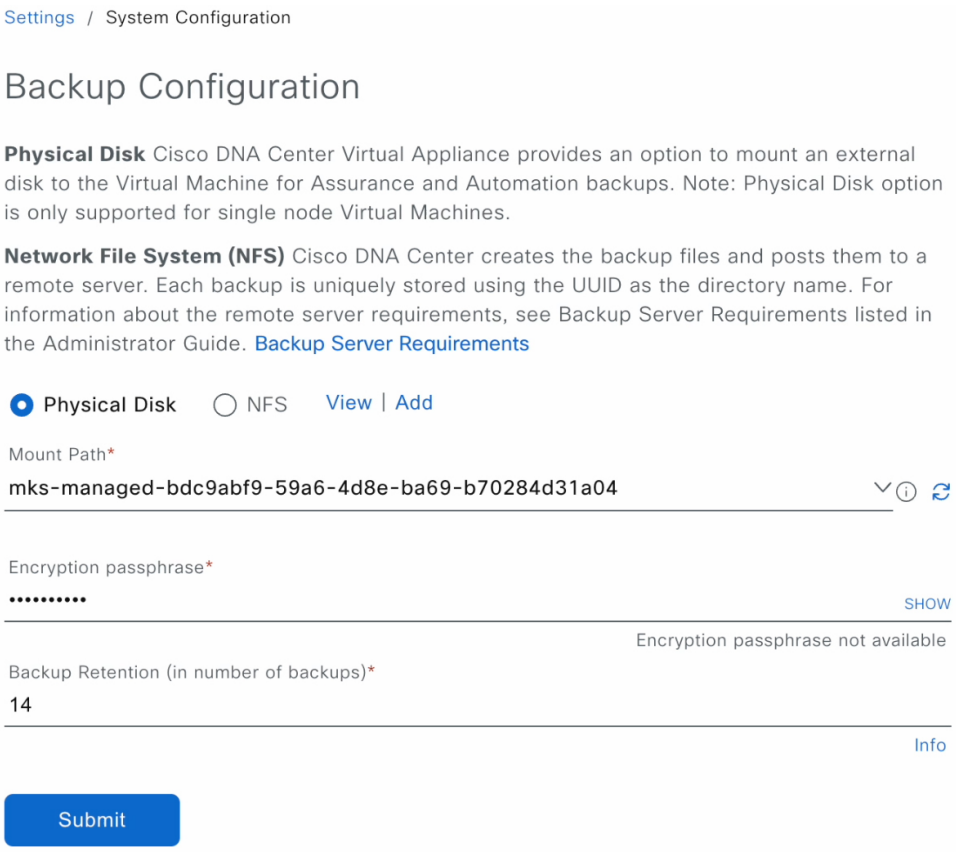
（注） 仮想マシンが復旧したら、**magctl appstack status** コマンドを実行してサービスが実行されていることを確認します。

ステップ 2 バックアップの保存場所を設定するには、次の手順を実行します。

a) ESXi 上の Cisco DNA Center メニューから、**[System]** > **[Settings]** > **[System Configuration]** > **[Backup Configuration]** の順に選択します。

b) [Physical Disk] ラジオボタンをクリックします。

c) [Mount Path] ドロップダウンリストから物理ディスクを選択します。



d) バックアップのセキュリティが重要なコンポーネント（証明書やログイン情報など）の暗号化に使用するパスフレーズを入力します。

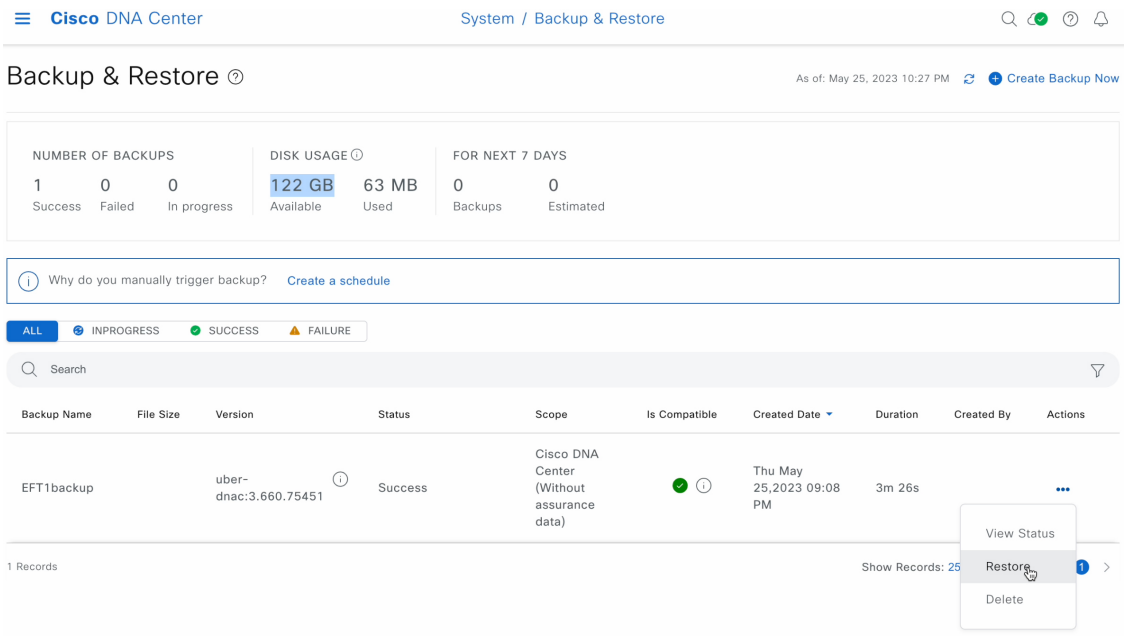
重要 このパスフレーズを忘れないようにしてください。後続の手順でパスフレーズを入力する必要があり、パスフレーズを忘れた場合は作成対象のバックアップを復元することはできません。

e) バックアップファイルが削除されるまでの保持期間を設定します。

f) [Submit] をクリックします。`

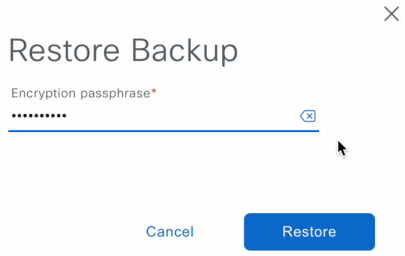
ステップ 3 バックアップを復元するには、次の手順を実行します。

a) ESXi 上の Cisco DNA Center メニューから **[System]** > **[Backup & Restore]** を選択します。

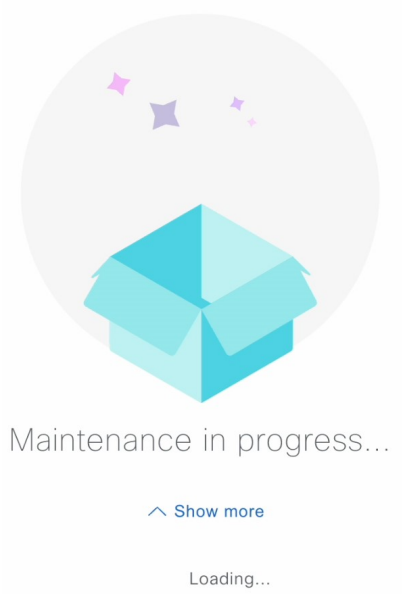


b) [Backup & Restore] ウィンドウのテーブルでバックアップを見つけ、[Actions] 列の下にある省略記号をクリックして [Restore] を選択します。

c) 前の手順で入力したものと同じ暗号化パスフレーズを入力し、[Restore] をクリックします。

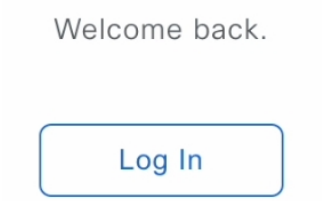


アプライアンスがメンテナンスモードになり、復元プロセスを開始します。

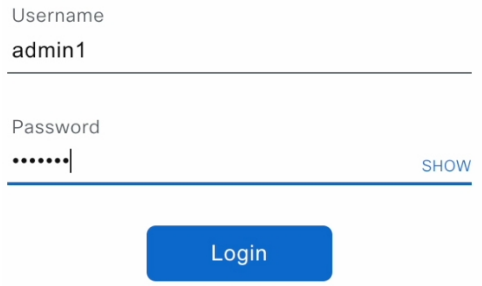


復元操作が完了すると、[Backup & Restore] ウィンドウのテーブルのステータスが [Success] に変更されます。

d) 復元操作が完了したら、[Log In] をクリックして ESXi 上の Cisco DNA Centerに再度ログインします。



e) 管理者ユーザーのユーザー名とパスワードを入力して、[Login] をクリックします。



障害が発生した仮想アプライアンスの NFS サーバーからのデータの復元

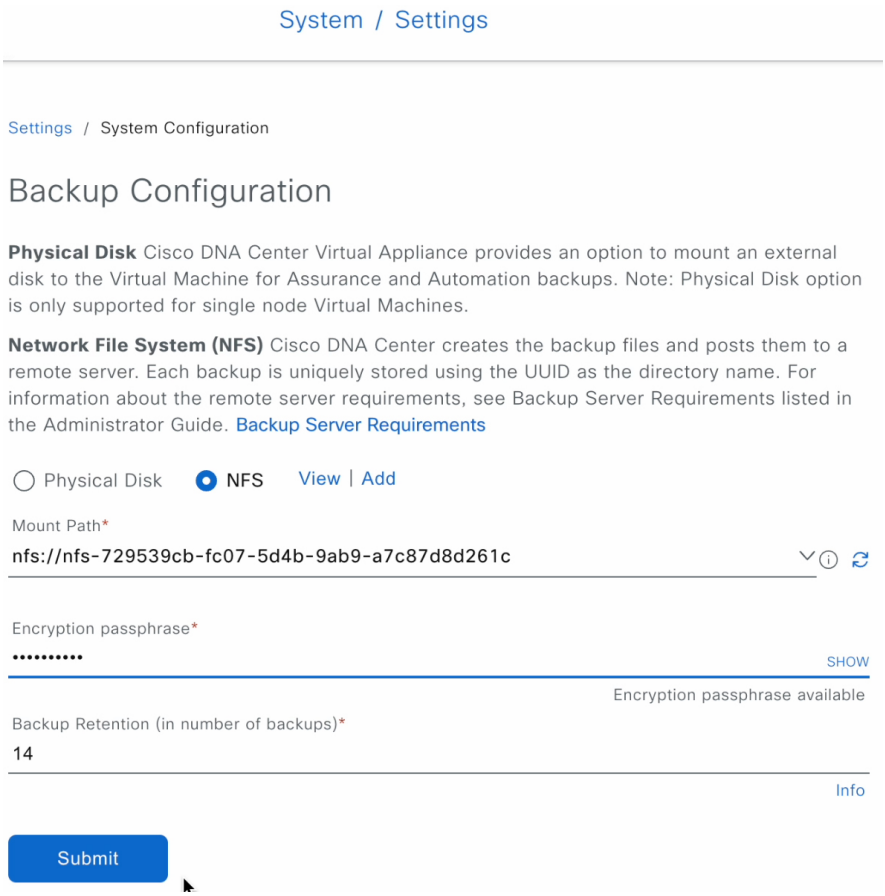
故障または障害が発生した仮想アプライアンスの NFS サーバーからデータを復元するには、次の手順を実行します。

ステップ 1 新しい仮想アプライアンスで、障害のある仮想アプライアンス用に設定した NFS サーバーを使用するように ESXi 上の Cisco DNA Center を設定するには、次の手順を実行します。

a) ESXi 上の Cisco DNA Center メニューから、**[System]** > **[Settings]** > **[System Configuration]** > **[Backup Configuration]** の順に選択します。

b) [NFS] ラジオボタンをクリックします。

c) [Mount Path] ドロップダウンリストから NFS サーバーを選択します。



d) バックアップのセキュリティが重要なコンポーネント（証明書やログイン情報など）の暗号化に使用するパスフレーズを入力します。

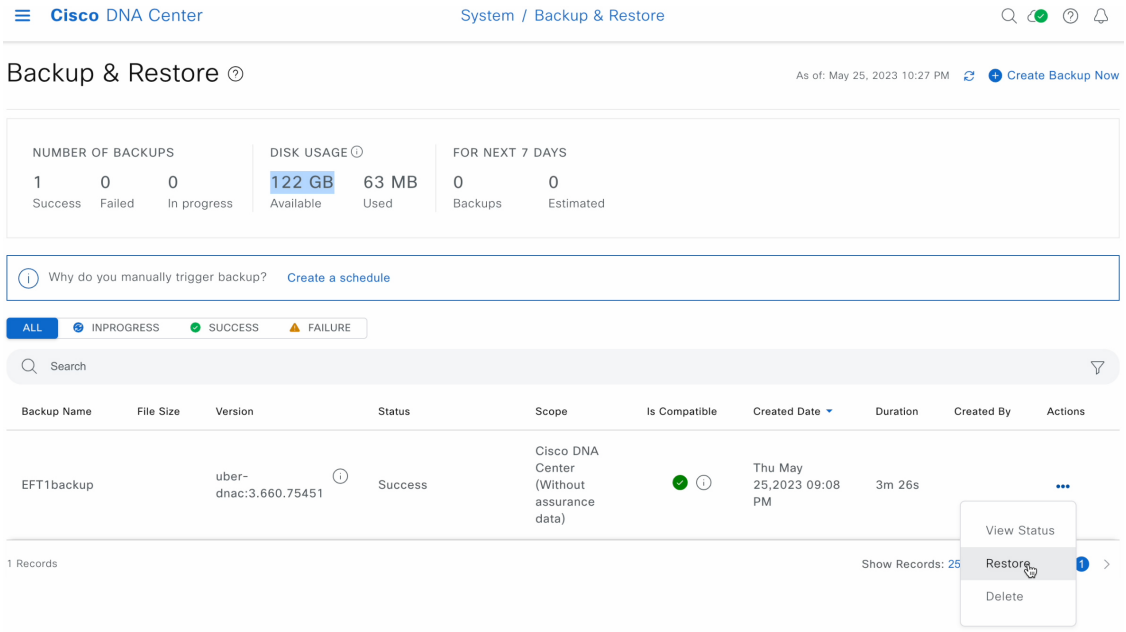
重要 このパスフレーズを忘れないようにしてください。後続の手順でパスフレーズを入力する必要があり、パスフレーズを忘れた場合は作成対象のバックアップを復元することはできません。

e) バックアップファイルが削除されるまでの保持期間を設定します。

f) [Submit] をクリックします。`

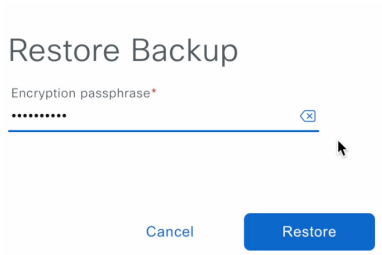
ステップ 2 バックアップを復元するには、次の手順を実行します。

a) ESXi 上の Cisco DNA Center メニューから **[System]** > **[Backup & Restore]** を選択します。

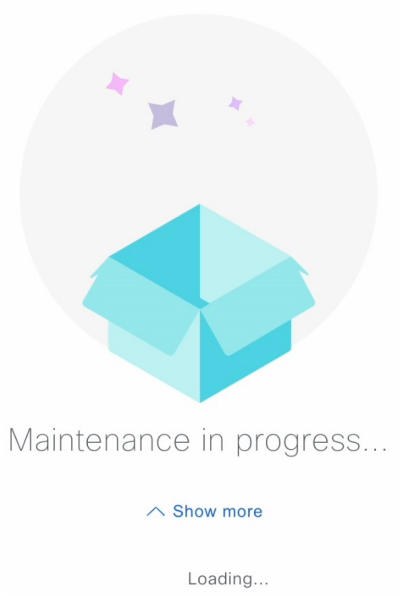


b) [Backup & Restore] ウィンドウのテーブルでバックアップを見つけ、[Actions] 列の下にある省略記号をクリックして [Restore] を選択します。

c) 前の手順で入力したものと同じ暗号化パスフレーズを入力し、[Restore] をクリックします。

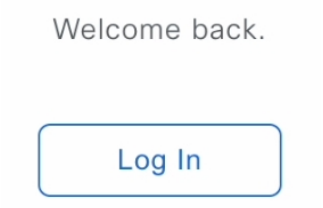


アプライアンスがメンテナンスモードになり、復元プロセスを開始します。

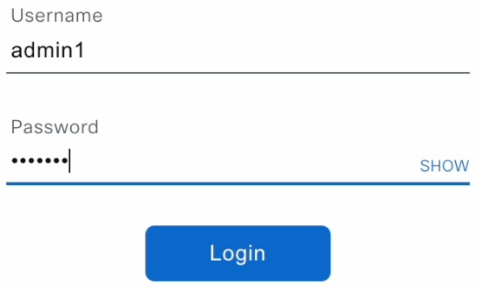


復元操作が完了すると、[Backup & Restore] ウィンドウのテーブルのステータスが [Success] に変更されます。

d) 復元操作が完了したら、[Log In] をクリックして ESXi 上の Cisco DNA Centerに再度ログインします。



e) 管理者ユーザーのユーザー名とパスワードを入力して、[Login] をクリックします。



データのバックアップスケジュール

定期的なバックアップをスケジュールし、実行する曜日と時間を定義することができます。

始める前に

次の要件が満たされていることを確認します。

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。
- データバックアップサーバーがNFS バックアップサーバーの要件 （120 ページ）で説明されている要件を満たしている。
- バックアップサーバーが Cisco DNA Center で設定されている。詳細については、バックアップファイルを保存する場所の設定 （126 ページ）を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして、 **[System]** > **[Backup & Restore]** の順に選択します。[Backup & Restore] ウィンドウが表示されます。

ステップ 2 [Create Schedule] リンクをクリックします。

（注） 進行中のバックアップジョブがない場合にのみ、新しいバックアップをスケジュールできます。

ステップ 3 [Create Schedule] slide-in paneで、次の手順を実行します。

1. [Backup Name] フィールドで、バックアップの一意の名前を入力します。
2. スケジュールオプションを選択します。
   - [Schedule Daily]：バックアップジョブを毎日スケジュールするには、バックアップを実行する時刻を選択します。
   - [Schedule Weekly]：バックアップジョブを毎週スケジュールするには、バックアップを実行する曜日と時刻を選択します。
3. バックアップの範囲を定義します。
   - [Cisco DNA Center (All data)]：このオプションを使用すると、システム管理者は自動化、アシュアランス、システム固有のセットのバックアップを作成できます。
   - [Cisco DNA Center (without Assurance data)]：このオプションを使用すると、管理者は自動化およびシステム固有のセットのバックアップを作成できます。
4. [Save] をクリックします。

[Backup & Restore] ウィンドウには、バックアップがスケジュールされている日時を示すバナーメッセージが表示されます。

ステップ 4 （任意） バナーメッセージの末尾にある省略記号をクリックすると、次の操作を実行できます。

1. [Edit] をクリックすると、スケジュールを編集できます。
2. [Upcoming Schedules] をクリックすると、今後のスケジュールを変更できます。slide-in pane の [Upcoming Schedules] でスケジュールされた日時にバックアップを実行しない場合は、トグルボタンをクリックして特定のスケジュールを無効にします。
3. スケジュールを削除するには、[Delete] をクリックします。

ステップ 5 バックアップが開始されると、[Backup & Restore] ウィンドウにバックアップが表示されます。実行されたステップのリストを表示するには、[Actions] の下にある省略記号をクリックし、[View Status] を選択します。

[Status] 列でバックアップのステータスを確認することもできます。

ステップ 6 [Backup & Restore] ウィンドウで [In Progress]、[Success]、または [Failure] タブをクリックすると、バックアップのリストをステータスが [In Progress]、[Success]、または [Failure] のタスクのみをフィルタリングして表示できます。

バックアッププロセス中は、Cisco DNA Center によりバックアップデータベースおよびファイルが作成されます。バックアップファイルは指定された場所に保存されます。バックアップファイルは単一のセットに限らず、一意の名前で識別される複数のバックアップファイルを作成できます。プロセスが完了すると、バックアップジョブのステータスが [In Progress] から [Success] に変わります。

（注） バックアッププロセスが失敗しても、アプライアンスまたはそのデータベースへの影響はありません。バックアップの失敗の最も一般的な原因は、ディスク領域の不足です。バックアッププロセスが失敗した場合は、リモートサーバーに十分なディスク容量があるかどうかを確認し、別のバックアップを試行します。

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。