



初期設定の完了

- [初期設定ワークフロー](#) (1 ページ)
- [互換性のあるブラウザ](#) (2 ページ)
- [初回ログイン](#) (2 ページ)
- [Cisco ISE との統合 Cisco DNA Center](#) (5 ページ)
- [認証サーバとポリシーサーバの設定](#) (8 ページ)
- [SNMP プロパティの設定](#) (10 ページ)

初期設定ワークフロー

インストールしたすべての Cisco DNA Center アプライアンスの設定が完了したら、次のタスクを実行して、Cisco DNA Center を実稼働に使用する準備をします。



(注) この作業を完了するために必要なパラメータ情報については「[必要な初期設定情報](#)」を参照してください。

1. 互換性のあるブラウザを使用して、Cisco DNA Center にアクセスしていることを確認してください。

互換性のあるブラウザの一覧については、インストールしている Cisco DNA Center のバージョンに対応する [リリースノートドキュメント](#) を参照してください。
2. 最初に管理者として Cisco DNA Center GUI にログインします。最初の管理ログイン中、次のプロンプトが表示されます。
 1. 管理スーパーユーザーの新規パスワードを提供します。
 2. ソフトウェアイメージをダウンロードし、シスコから電子メール通信を受信するために組織が使用する `cisco.com` ユーザ名とパスワードを入力します。
 3. 組織がスマートアカウントライセンスを管理するために使用する `cisco.com` ユーザ名とパスワードを入力します。

4. Cisco DNA Center で使用する予定の IP アドレスマネージャ (IPAM) サーバを設定します。

これらのタスクの詳細については、「[初回ログイン](#)」を参照してください。

3. Cisco DNA Center を Cisco Identity Services Engine (ISE) と一緒に使用する予定の場合は、2つが適切に統合されていることを確認してください：[Cisco ISE との統合 Cisco DNA Center の統合](#)
4. Cisco DNA Center にポリシーおよび AAA サーバ (ISE を含む) を接続します：[認証サーバとポリシーサーバの設定](#)
5. 基本的な SNMP の再試行およびポーリングパラメータを設定します：[SNMP プロパティの設定](#)
6. HA 動作を最適化するために、クラスタノード間でサービスを再配布します：[サービスの再配布](#)
7. 初回設定を完了したら：[ログアウト](#)

互換性のあるブラウザ

Cisco DNA Center の GUI は次の HTTPS 対応ブラウザと互換性があります。

- Google Chrome : バージョン 62.0 以降。
- Mozilla Firefox : バージョン 54.0 以降。

Cisco DNA Center へのログインに使用するクライアント システムは、64 ビット オペレーティング システムとブラウザを装備していることが推奨されます。

初回ログイン

Cisco DNA Center アプライアンスをインストールして設定した後、Web ベースの GUI にログインできます。Cisco DNA Center にアクセスする際には、互換性のある HTTPS 対応ブラウザを使用してください。

スーパーユーザ権限を持つ管理者 (admin というユーザ名、スーパー管理者ロール (SUPER-ADMIN-ROLE) が割り当てられている) として初めてログインする場合、システムセキュリティを強化し、基本的なセットアップタスクを完了するのに役立つ、初回セットアップウィザードを完了するように求められます。ウィザードの各ステップを省略することは可能ですが、システムをできるだけ早く使用できるようにするため、指示どおりにすべてのステップを完了することをお勧めします。

また、新しいCisco DNA Centerユーザを作成する必要があります。毎日の操作で使用する追加のユーザアカウントを少なくとも1つ作成し、このユーザアカウントにネットワーク管理者ロール (NETWORK-ADMIN-ROLE) を割り当てることをお勧めします。

始める前に

Cisco DNA Center にログインして初回セットアップウィザードを完了するには、次の情報が必要です。

- 「[Maglev ウィザードを使用したマスタノードの設定](#)」の手順に従って指定した「管理者」スーパーユーザのユーザ名とパスワード。
- [\[必要な初期設定情報 \(Required First-Time Setup Information\)\]](#) に記載されている必要な情報。

ステップ 1 Cisco DNA Center アプライアンスのリブートが完了したら、ブラウザを起動します。

ステップ 2 **HTTPS://** と設定プロセスの最後に表示された Cisco DNA Center GUI の IP アドレスを使用して、Cisco DNA Center GUI にアクセスするホスト IP アドレスを入力します。

IP アドレスを入力すると、次のいずれかのメッセージが表示されます（使用しているブラウザによって異なります）。

- Google Chrome：接続のプライバシーは保護されません
- Mozilla Firefox：警告：今後セキュリティリスクが見つかる潜在的可能性があります

ステップ 3 メッセージを無視して **[詳細設定 (Advanced)]** をクリックします。

サイトのセキュリティ証明書が信頼されていないことを示すメッセージが表示されます。このメッセージが表示されるのは、コントローラが自己署名証明書を使用しているためです。Cisco DNA Center での証明書の使用方法については、『[Cisco Digital Network Architecture Center 管理者ガイド](#)』の「証明書と秘密キーのサポート」の項を参照してください。

ステップ 4 メッセージを無視して、ウィンドウの下部にあるリンクをクリックします。

[ログイン (Login)] Cisco DNA Center ウィンドウが表示されます。

ステップ 5 **[ログイン (Login)]** ウィンドウで Cisco DNA Center の設定時に設定した管理ユーザ名 (admin) とパスワードを入力し、**[ログイン (Log In)]** をクリックします。

[ログインのリセット (Reset Login)] ウィンドウが表示されます。

ステップ 6 古いパスワードを入力してから、スーパーユーザ権限を持つ管理者の新しいパスワードを入力して確認し、**[保存 (Save)]** をクリックします。

[Cisco.com IDの入力 (Enter Cisco.com ID)] ウィンドウが表示されます。

ステップ 7 Cisco.com ユーザのユーザ名とパスワードを入力してから **[次へ (Next)]** をクリックします。

cisco.com ユーザログインが既知のどの Cisco Smart Account ユーザログインとも一致しない場合は、**[Smart Account]** ウィンドウが表示されます。

ステップ 8 **[スマートアカウント (Smart Account)]** ウィンドウが表示された場合には、組織のスマートアカウントのユーザ名とパスワードを入力するか、対応するリンクをクリックして新しいスマートアカウントを開きます。完了したら **[次へ (Next)]** をクリックします。

[IPアドレスマネージャ (IP Address Manager)] ウィンドウが表示されます。

ステップ 9 組織が外部 IP アドレスマネージャ (IPAM) を使用している場合には、次の手順を実行してから [次へ (Next)] をクリックします。

- IPAM サーバの名前と URL を入力します。
- サーバへのアクセスに必要なユーザ名とパスワードを入力します。
- 使用中の IPAM プロバイダー (Infoblox など) を選択します。
- Cisco DNA Center で使用する利用可能な IP アドレスの特定のビューを IPAM サーバデータベースで選択します。

[プロキシサーバの入力 (Enter Proxy Server)] ウィンドウが表示されます。

ステップ 10 組織が使用するプロキシサーバ情報を入力し、[次へ (Next)] をクリックします。

- プロキシサーバに対するログインが必要な場合には、サーバのユーザ名とパスワードを含めます。
- 続行する前にこの情報を検証する (推奨) 場合には、[設定の検証 (Validate Settings)] チェックボックスがオンになっていることを確認します。

ソフトウェアの [EULA] ウィンドウが表示されます。

ステップ 11 [次へ (Next)] をクリックして、ソフトウェアのエンドユーザライセンス契約書に同意します。

[準備完了 (Ready to go!)] ウィンドウが表示されます。

ステップ 12 このウィンドウでいずれかのリンクをクリックするか、[システム360に移動 (Go To System 360)] をクリックして [システム360 (System 360)] ダッシュボードを表示することにより、Cisco DNA Center の使用を開始できます。

シスコでは、[ユーザ管理 (User Management)] リンクをクリックして、[ユーザ管理 (User Management)] ウィンドウを表示することを推奨しています。[追加 (Add)] をクリックして、新しい Cisco DNA Center ユーザの追加を開始します。新しいユーザの名前とパスワードを入力し、ユーザのロールを選択したら、[保存 (Save)] をクリックして新しいユーザを作成します。初期展開の新しいユーザすべてが追加されるまで、必要に応じてこの手順を繰り返します。ネットワーク管理者ロール (NETWORK-ADMIN-ROLE) を持つユーザを少なくとも 1 人作成してください。

次のタスク

残りの管理設定タスクを任意の順序で実行します。

- [Cisco ISE との統合 Cisco DNA Center](#)
- [認証サーバとポリシー サーバの設定](#)
- [SNMP プロパティの設定](#)

Cisco ISE との統合 Cisco DNA Center

このリリースの Cisco DNA Center は、Cisco ISE と信頼された通信リンクを作成するメカニズムを備えており、Cisco DNA Center は安全な方法で Cisco ISE とデータを共有できます。Cisco ISE が Cisco DNA Center に登録されると、Cisco DNA Center が検出するすべてのデバイスが、関連する設定データやその他のデータとともに Cisco ISE にプッシュされます。ユーザは Cisco DNA Center を使用してデバイスを検出し、Cisco DNA Center と Cisco ISE の両方の機能を検出したデバイスに適用できます。この理由はこれらのデバイスが両方のアプリケーションに公開されるためです。また Cisco DNA Center デバイスと Cisco ISE デバイスはすべてデバイス名で一意に識別されます。

Cisco DNA Center デバイスは Cisco DNA Center サイト階層内の特定のサイトにプロビジョニングされて所属すると、即座に Cisco ISE にプッシュされます。Cisco DNA Center デバイスのアップデート (IP アドレス、SNMP または CLI のクレデンシャル、Cisco ISE 共有秘密情報など) はすべて、自動的に ISE 上の対応するデバイスインスタンスに使用されます。Cisco DNA Center デバイスが削除される場合は、Cisco ISE から削除されます。Cisco DNA Center デバイスが Cisco ISE にプッシュされるのは、Cisco ISE が AAA サーバとして設定されている特定のサイトにそれらのデバイスが関連付けられている場合に限ることに注意してください。

始める前に

Cisco ISE を Cisco DNA Center と統合する前に、次の前提条件を満たしていることを確認します。

- ネットワークに 1 つ以上の Cisco ISE バージョン 2.3 (以降) のホストを展開済みであること。Cisco ISE のインストールについては、[Cisco Identity Services Engine のインストールガイド、アップグレードガイド](#) (バージョン 2.3 以降用) を参照してください。
- スタンドアロン ISE 導入環境がある場合は、Cisco ISE ノード上で pxGrid サービスおよび ERS と統合し、これらを有効化する必要があります。
- 分散型 Cisco ISE 展開がある場合：
 - Cisco DNA Center を Cisco ISE 管理ノード、プライマリポリシー管理ノード (PAN) と統合し、ERS を有効にする必要があります。



(注) PAN を介した ERS 使用がベストプラクティスです。ただしバックアップの場合は、PSN で発信をイネーブルにします。

- 単一ノードの導入環境と同様に、分散型の導入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。分散型の導入環境では、他の任意の Cisco ISE ノード上で pxGrid を有効化できます。

- ポート 22、443、5222、8910、9060 で Cisco DNA Center と Cisco ISE の通信が有効になっています。
- 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 ノードでは SSH が有効化されます。
- Cisco ISE 管理ノード証明書のサブジェクト名または SAN のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれます。
- Cisco DNA Center システム証明書の [サブジェクト代替名 (SAN) (Subject Alternative Name (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。


Cisco DNA Center に対応した Cisco ISE の設定の詳細については、『[Cisco ISE Administrators Guide](#)』の「*Integration with Cisco DNA Center*」を参照してください。

ステップ 1 次のように Cisco ISE の pxGrid サービスと ERS を有効化します。

- a) Cisco ISE のプライマリ管理ノードにログインします。
- b) **[管理 (Administration)] > [システム (System)] > [展開 (Deployment)]** を選択します。
[展開設定 (Deployment Configuration)] ウィンドウが開きます。
- c) pxGrid サービスを有効化する Cisco ISE ノードのホスト名をクリックします。
分散型展開の場合、これは展開環境内の任意の Cisco ISE ノードです。
[ノードの編集 (Edit Node)] ウィンドウが開き、**[General Settings (一般設定)]** タブがデフォルトで選択されています。
- d) **[PxGrid]** チェックボックスがオンになっていることを確認してから、**[保存 (Save)]** をクリックします。
- e) **[管理 (Administration)] > [システム (System)] > [設定 (Settings)]** の順に選択します。
- f) 左側のナビゲーションウィンドウで **[設定 (Settings)]** をクリックして、**[設定 (Settings)]** ウィンドウを開きます。
- g) **[読み取り/書き込み用にERSを有効化 (Enable ERS for Read/Write)]** オプションボタンをクリックし、通知プロンプトで **[OK]** をクリックします。
- h) **[保存 (Save)]** をクリックします。

ステップ 2 次のように Cisco ISE ノードを AAA サーバとして Cisco DNA Center に追加します。



- a) Cisco DNA Center GUI にログインします。
- b) **メニューアイコン (☰)** をクリックし、**[システム (System)] > [システム360 (System 360)]** を選択します。
- c) **[Identity Services Engine (ISE)]** ペインで、**[設定 (Configure)]** リンクをクリックします。

- d) [認証サーバとポリシーサーバ (Authentication And Policy Servers)] ウィンドウで [ Add] をクリックします。
- e) [AAA/ISEサーバの追加 (Add AAA/ISE server)] スライドインペインで、次のタスクを実行します。
- [サーバIPアドレス (Server IP address)] フィールドに、Cisco ISE 管理 IP アドレスを入力します。
 - ネットワークデバイスと Cisco ISE の通信を保護するために使用する [共有秘密 (Shared Secret)] を入力します。
 - [Cisco ISEサーバ (Cisco ISE Server)] スライダをクリックして、すべての Cisco ISE 関連フィールドが表示されていることを確認します。
 - 該当する Cisco ISE 管理者の CLI クレデンシャルを [ユーザ名 (Username)] と [パスワード (Password)] フィールドに入力します。
 - Cisco ISE ノードの FQDN を入力します。
 - [サブスクライバ名 (Subscriber Name)] を入力します (例: cdnacenter)。
 - (任意) Cisco ISE への接続に使用する Group14-SHA1 SSH キーを入力します。
 - (任意) 仮想 IP アドレス (Virtual IP Address) : Cisco ISE ポリシーサービスノード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ポリシーサービス ノード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。
- f) [保存 (Save)] をクリックし、サーバのステータスが [アクティブ (Active)] になるまで待ちます。

ステップ 3 次のように Cisco ISE が Cisco DNA Center に接続され、接続にサブスクライバがあることを確認します。

- a) Cisco DNA Center を統合した Cisco ISE ノードにログインします。
- b) [管理 (Administration)] > [pxGrid サービス (pxGrid Services)] を選択します。
- 現在のステータスが [オフライン (Offline)] の pxGrid サービスサブスクライバが、ユーザの入力した名前 (cdnacenter など) で表示されます。デフォルトでは、サブスクライバのステータスは **オフライン** のままであることに注意してください。

ステップ 4 Cisco DNA Center が Cisco ISE に接続していること、Cisco ISE SGT グループとデバイスが Cisco DNA Center にプッシュされることを次の手順で確認します。

- a) Cisco DNA Center GUI にログインします。
- b)  をクリックし、[システム (System)] > [システム360 (System 360)] を選択します。
- c) [Identity Services Engine (ISE)] ペインで、[Update (更新)] リンクをクリックします。
- d) [認証サーバとポリシーサーバ (Authentication And Policy Servers)] ウィンドウで、Cisco ISE AAA サーバのステータスがまだ [アクティブ (Active)] であることを確認します。
- e)  をクリックし、[ポリシー (Policy)] > [グループベースアクセスコントロール (Group Based Access Control)] を選択します。


ISE SGT グループは [スケーラブルグループ] 表に表示されます。

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 と Cisco ISE が「[Cisco ISE との統合 Cisco DNA Center の統合](#)」の説明に従って統合されたことを確認します。
- 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 サーバで Cisco DNA Center を登録します。これには、AAA サーバと 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。

ステップ 1 Cisco DNA Center のホームページで、 > [System Settings] > [Settings] > [Authentication and Policy Servers] 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 次の情報を入力して、プライマリ AAA サーバを設定します。

- **サーバの IP アドレス (Server IP Address)** : AAA サーバの IP アドレス。
- **共有秘密 (Shared Secret)** : デバイス認証キー。共有秘密情報の長さは、最大 128 文字です。

ステップ 4 AAA サーバ (Cisco ISE 以外) を設定するには、[Cisco ISE サーバ (Cisco ISE Server)] ボタンを [オフ (Off)] 位置のままにして、次の手順に進みます。

Cisco ISE サーバを設定するには、[Cisco ISE サーバ (Cisco ISE server)] ボタンをクリックして [オン (On)] の位置に合わせ、次のフィールドに情報を入力します。

- **ユーザ名 (Username)** : Cisco ISE CLI へのログインに使用する名前です。
(注) このユーザにはスーパーユーザの管理権限が必要です。
- **パスワード (Password)** : Cisco ISE CLI ユーザ名のパスワード。
- **FQDN** - Cisco ISE サーバの FQDN。

- (注)
- Cisco ISE ([管理 (Administration)] > [展開 (Deployment)] > [展開ノード (Deployment Nodes)] > [リスト (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す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、ホスト名とドメイン名の 2 つのパートで構成されています。

hostname.domainname.com。

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

- **サブスクリバ名 (Subscriber Name)** : Cisco ISE pxGrid サービスに登録するとき pxGrid クライアントを識別する一意のテキスト文字列 (acme など)。サブスクリバ名は Cisco DNA Center を Cisco ISE に統合するとき使用されます。
 - (任意) **SSH キー** : Cisco ISE への接続に使用される Diffie-Hellman-Group14-SHA1 SSH キー。
 - (任意) **仮想 IP アドレス** : Cisco ISE ポリシーサービスノード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ポリシーサービス ノード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。
- (注) 設定された ISE サーバのステータスがパスワードの変更により [失敗 (FAILED)] になっている場合は、[再試行 (Retry)] をクリックし、パスワードを更新して ISE 接続を再同期します。

ステップ 5 [詳細設定の表示 (View Advanced Settings)] をクリックして、設定を構成します。

(注) 必要な設定は、サーバのプロトコル設定によって異なります。

- **プロトコル (Protocol)** : [RADIUS] はデフォルトで設定されていますが、代わりに [TACACS] を選択するか、両方のプロトコルを選択することもできます。
注目 Cisco ISE サーバに [TACAS] を選択しない場合、Cisco ISE ノードの設定には使用できません。
- **認証ポート (Authentication Port)** : RADIUS が AAA サーバに認証メッセージを中継するために使用されるポート。デフォルト値は UDP ポート 1812 です。
- **アカウントングポート (Accounting Port)** : RADIUS が AAA サーバに重要なイベントを中継するために使用するポート。これらのイベントの情報は、セキュリティおよび請求目的で使用されます。デフォルトの UDP ポートは 1813 です。
- **ポート (Port)** : TACACS が AAA サーバとの通信に使用するポート。デフォルトポートは 49 です。
- **再試行 (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。
- **タイムアウト (Timeout)** : 接続の試行が中止される前に、デバイスが AAA サーバの応答を待機する時間。デフォルトのタイムアウトは 4 秒です。

ステップ 6 [適用 (Apply)] をクリックします。

ステップ7 セカンダリサーバを追加するには、ステップ2～6を繰り返します。

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。詳細については、[Cisco Digital Network Architecture Center 管理者ガイド](#)を参照してください。

ステップ1 Cisco DNA Center のホームページで、歯車のアイコン (⚙️) をクリックし、[システムの設定 (System Settings)] > [設定 (Settings)] > [SNMP プロパティ (SNMP Properties)] 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。
- **タイムアウト (秒数) (Timeout (in Seconds))** : 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秒の範囲内です。デフォルトは5秒です。

ステップ3 [適用 (Apply)] をクリックします。

(注) デフォルト設定に戻すには、[デフォルトに戻す (Revert to Defaults)] をクリックします。
