初期設定の完了

初期設定ワークフロー

設置したすべての Cisco DNA Center アプライアンスの設定が完了したら、次の表に一覧になっているタスクを実行し、本番環境での使用向けに Cisco DNA Center を準備する必要があります。

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。

表 *1 : Cisco DNA Center* アプライアンスの初期設定タスク

ステップ	説明
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を参照してください。

ステップ	説明
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 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 Web インターフェイスは、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する必要があります。

初めて管理者スーパーユーザ（ユーザ名は「admin」で、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。

新しいCisco DNA Centerユーザを作成する必要もあります。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。

- 「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」で必要とされている情報。

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 Cisco DNA Center GUI へのアクセスに使用するホスト IP アドレスを入力します。

HTTPS と、設定プロセスの最後に表示された Cisco DNA Center GUI の IP アドレスを使用します。

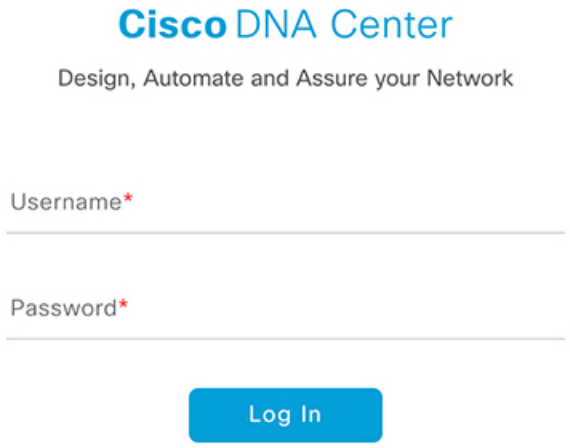
ステップ 3 ブラウザに IP アドレスを入力すると、「接続はプライベートではない」ことを示すメッセージが表示されます。

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

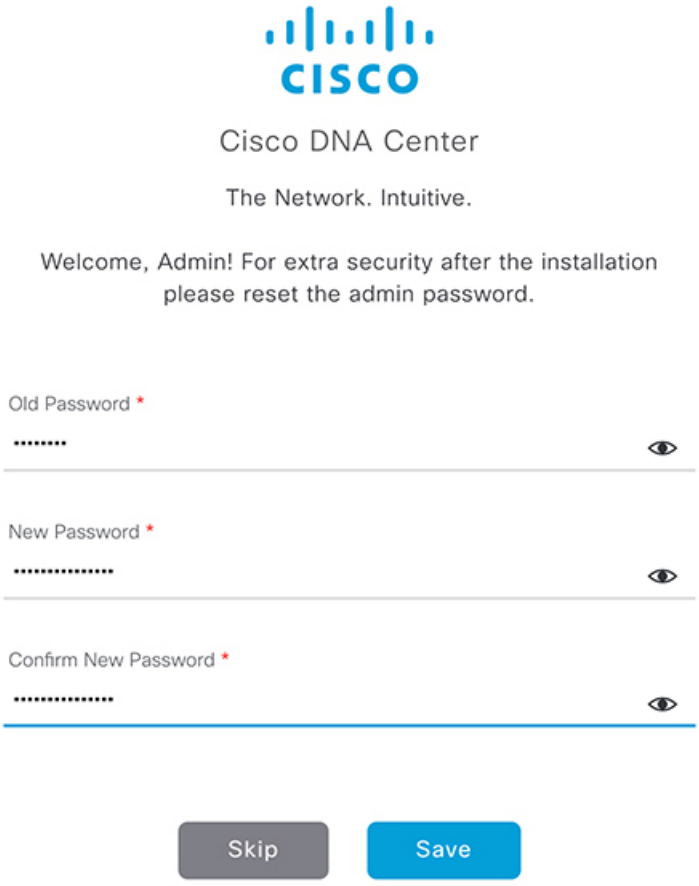
ステップ 4 サイトのセキュリティ証明書が信頼されていないことを示すメッセージが表示されます。

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。後ほど、Cisco DNA Center GUI を使用して信頼できる証明書をアップロードするオプションが表示されます。

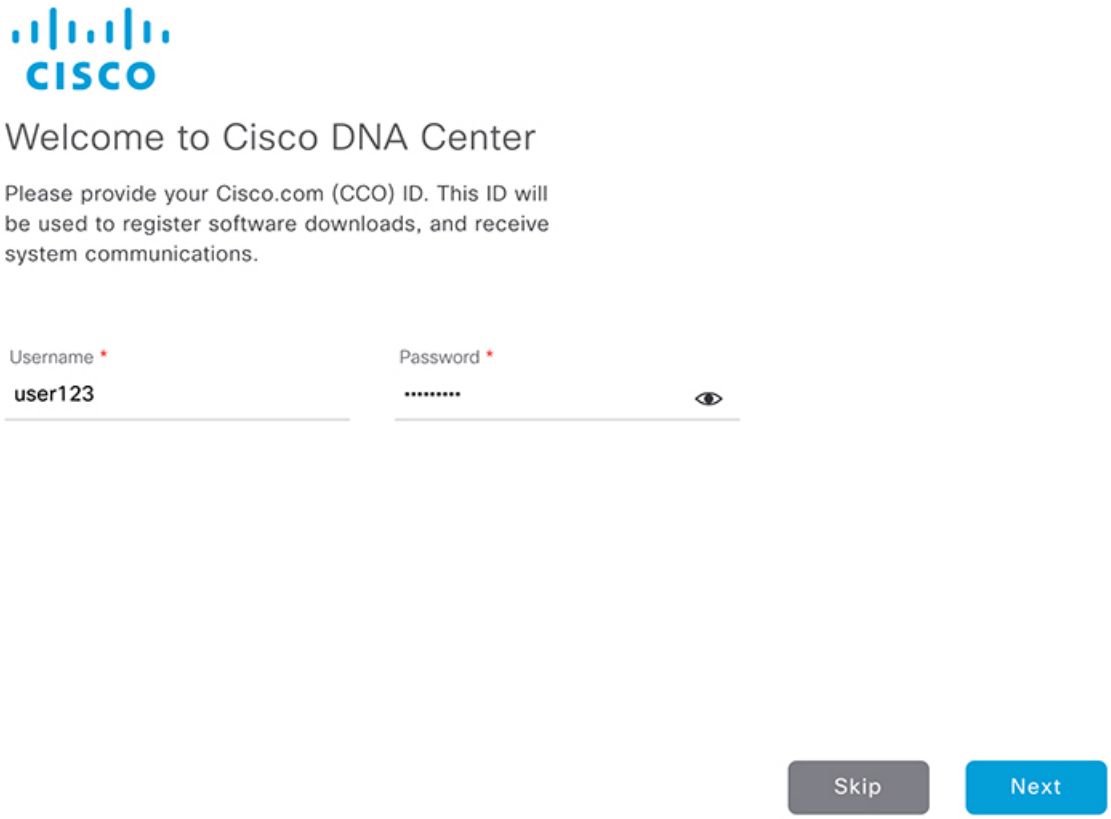
メッセージを無視して、ページの下部にあるリンクをクリックします。[ログイン（Login）]Cisco DNA Center ウィンドウが表示されます。



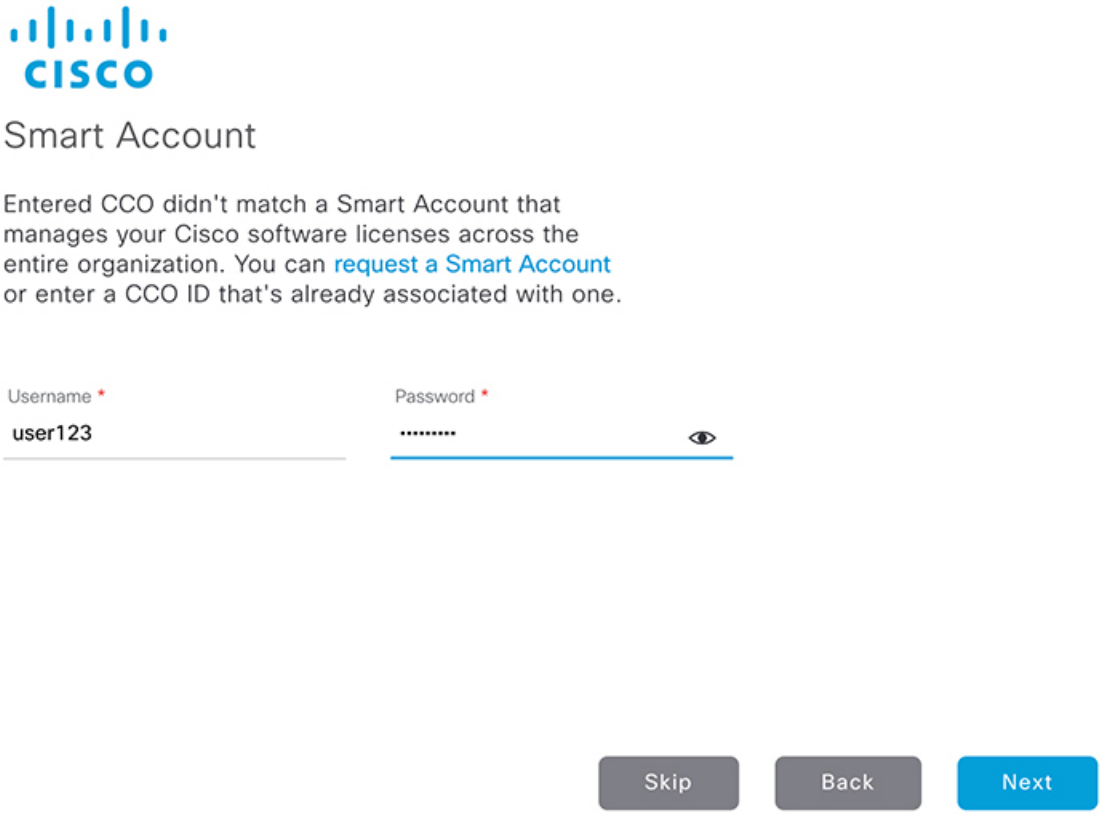
ステップ 5 [ログイン（Login）] ウィンドウで、Cisco DNA Center の設定時に設定した管理者ユーザ名（admin）とパスワードを入力します。入力後、[ログイン（Login）] をクリックします。**[ログインのリセット（Reset Login）]** ウィンドウが表示されます。



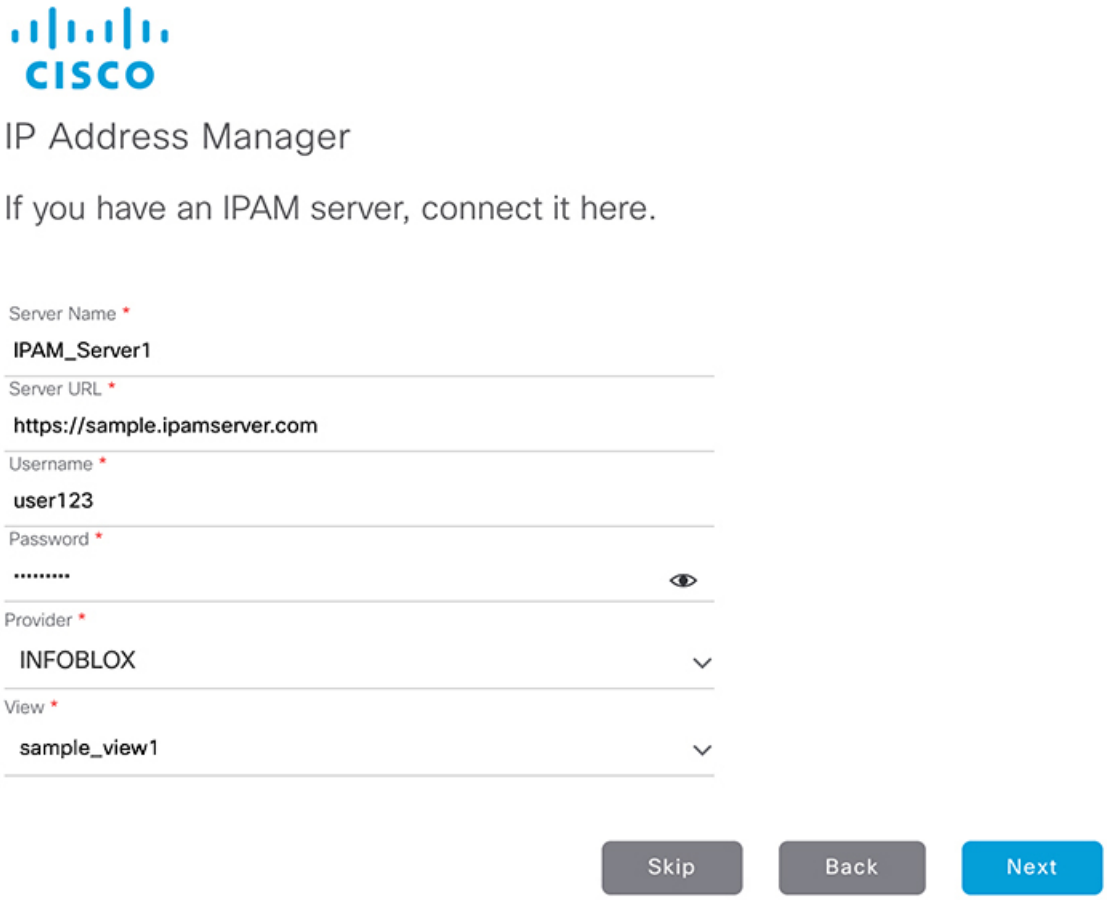
ステップ 6 古いパスワードを入力してから、管理者スーパーユーザの新しいパスワードを入力して確認します。次に、[保存（Save）] をクリックします。**[Cisco.com ID の入力（Enter Cisco.com ID）]** ウィンドウが表示されます。



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 Cisco スマート アカウント ユーザログインと一致しない場合には、**[スマートアカウント（Smart Account）]** ウィンドウが表示されます。



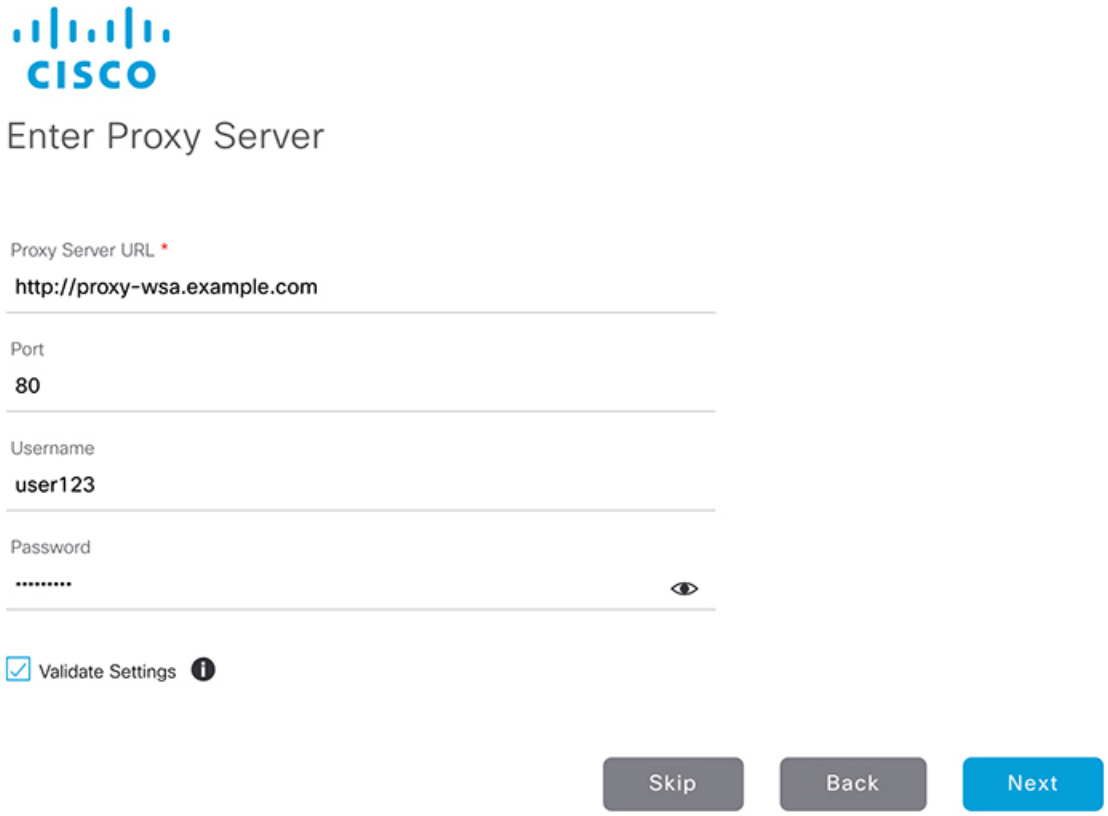
ステップ 8 [スマートアカウント（Smart Account）] ウィンドウが表示された場合には、組織のスマートアカウントのユーザ名とパスワードを入力するか、リンクをクリックして新しいスマートアカウントを開きます。確認したら、[次へ（Next）] をクリックします。**[IP アドレスマネージャ（IP Address Manager）]** ウィンドウが表示されます。



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。

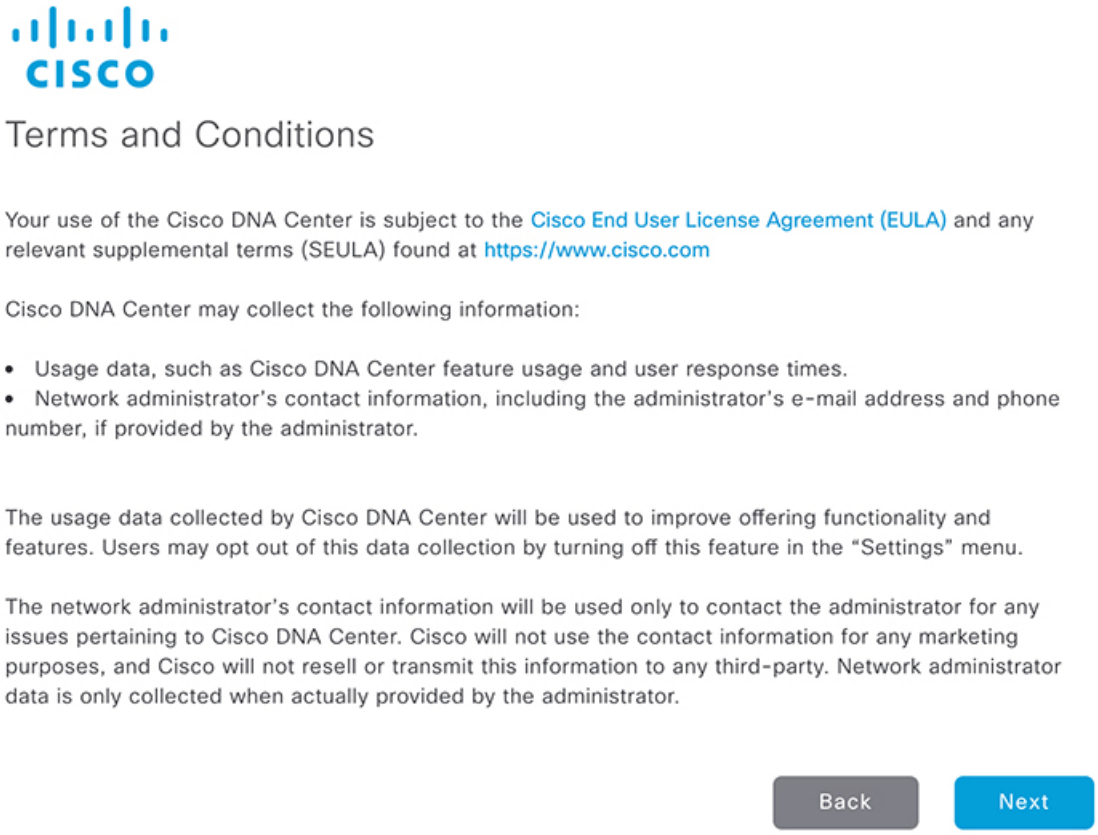
[プロキシサーバの入力（Enter Proxy Server）] ウィンドウが表示されます。



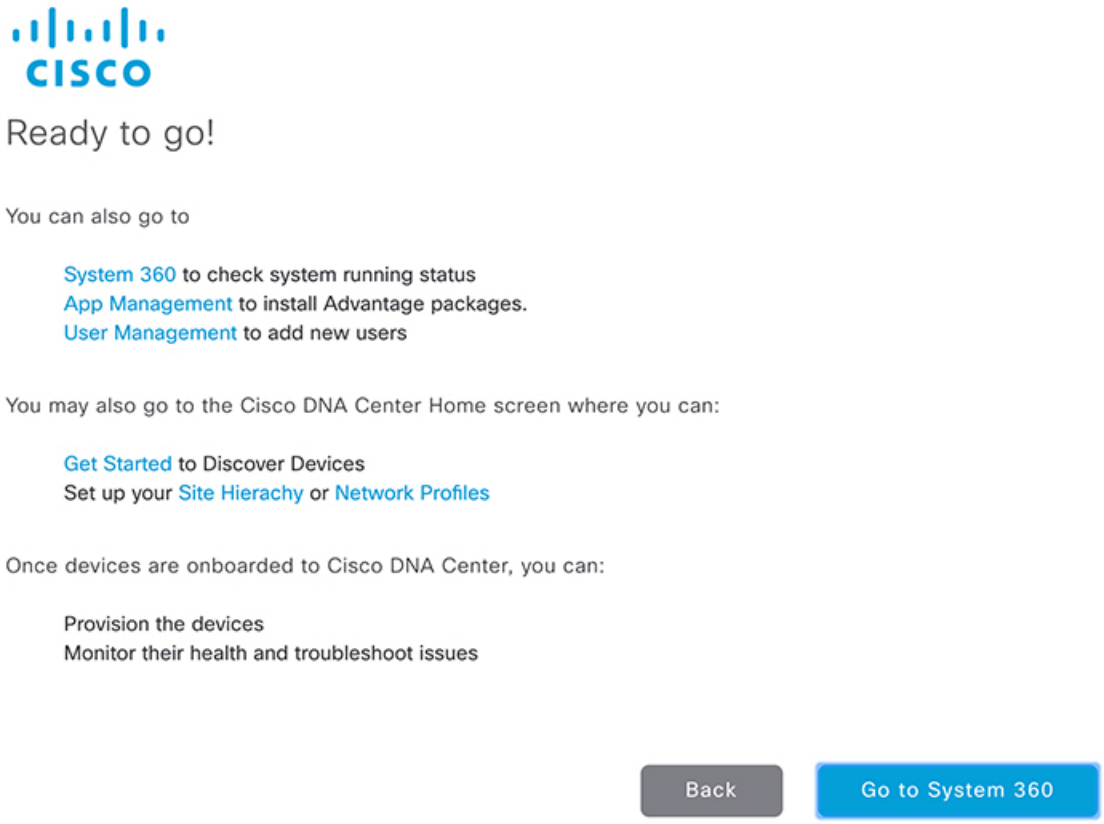
ステップ 10 組織が使用するプロキシサーバ情報を入力します。プロキシサーバに対するログインが必要な場合には、サーバのユーザ名とパスワードを含めます。

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。

確認したら、[次へ （Next）] をクリックします。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後、[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 Cisco DNA Center の統合
- 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 Cisco DNA Center の統合

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 の両方の機能をそれらに適用できます。これは、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。Cisco DNA Center および 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 のログイン情報、Cisco ISE 共有秘密情報など）はすべて、自動的に Cisco 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 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 インストールおよび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 Cisco ISE 展開環境がある場合は、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。

（注） Cisco ISE 2.4 以降では、pxGrid 2.0 および pxGrid 1.0 がサポートされています。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 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、プライマリ PAN で ERS を有効にする必要があります。また、セカンダリ PAN でも ERS を有効にする必要があります。Cisco ISE でプライマリ PAN のフェールオーバーが発生した場合に、セカンダリ PAN で ERS が有効になっていないと、Cisco DNA Center でセカンダリ PAN を使用できません。その結果、Cisco DNA Center と Cisco ISE の間の接続が影響を受けます。

（注） ベストプラクティスは、PAN を介して ERS を使用することです。ただしバックアップの場合は、ポリシーサービスノード（PSN）で ERS を有効化してください。

- 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。
- TrustSec/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 ISE のご使用のリリースに対応する管理者ワークフローのセグメンテーション ドキュメントを参照してください。

- 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 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。詳細および推奨される回避策については、『Cisco ISE Release Notes』を参照してください。

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 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) **[Administration]** > **[System]** > **[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) [**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 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) [Menu] アイコン（☰）をクリックし、**[System]** > **[System 360]** の順に選択します。

c) [Identity Services Engine（ISE）] ペインで、**[設定（Configure）]** リンクをクリックします。

d) [Authentication and Policy Servers] ウィンドウで、[Add] をクリックし、ドロップダウンリストから [ISE] を選択します。

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。
- 該当する Cisco ISE 管理ログイン情報を [Username] と [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。
- （任意）Cisco ISE 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**を入力します。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) [追加（Add）] をクリックします。

Cisco ISE との統合を初めて開始したときは、Cisco ISE からの証明書がまだ信頼されていないという通知が表示されます。

- 証明書を表示して詳細を確認できます。
- [Accept] を選択して証明書を信頼し、統合プロセスを続行します。証明書を信頼せずに統合プロセスを終了する場合は、[Decline] を選択します。

統合が正常に完了すると、確認メッセージが表示されます。

統合プロセスで問題が発生した場合は、問題の詳細を示すメッセージが表示されます。編集または再試行が可能な場合はそのオプションが表示されます。

- Cisco ISE 管理ログイン情報が無効であるというエラーメッセージが表示された場合は、[Edit] をクリックし、正しい情報を再入力します。
- 統合プロセスで証明書にエラーが見つかった場合は、Cisco ISE サーバエントリを削除し、証明書の問題が解決した後に統合を最初からやり直す必要があります。

ステップ 3 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確認します。

a) Cisco DNA Center GUI にログインします。
b) [Menu] アイコン（☰）をクリックし、**[System]** > **[System 360]** の順に選択します。
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。

ステップ 4 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 Identity Services Engine (ISE) Deployment] ウィンドウで pxGrid サーバとして表示されている Cisco ISE ノードにログインします。
b) **[Administration]** > **[pxGrid Services]** の順に選択し、[Web Clients] タブをクリックします。

Cisco DNA Center サーバの IP アドレスとともに 2 つの pxGrid クライアントがリストに表示されます。

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 および Cisco ISE が「Cisco ISE と 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 の共有秘密キーを定義することを含まれます。

- 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。

- [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）] の位置のままにして、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。

- [Cisco ISE]：サーバが Cisco ISE サーバかどうかを示す設定。[Cisco ISE] 設定をクリックして Cisco ISE を有効化します。
- [ユーザ名（Username）]：Cisco ISE コマンドライン インターフェイス（CLI）にログインするために使用する名前。

  （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 サーバの FQDN は、ise.cisco.com である可能性があります。

- [サブスクライバ名（Subscriber Name）]：Cisco ISE pxGrid サービス登録時の pxGrid クライアントを識別する一意のテキスト文字列（例：`acme`）。サブスクライバ名は Cisco DNA Center を Cisco ISE に統合するとき使用されます。

- [SSHキー（SSH Key）]：Cisco ISE と接続し、認証するために使用される Diffie-Hellman-Group14-SHA1 SSH キー。
- [仮想IPアドレス（Virtual IP address (es)）]：Cisco ISE ポリシーサービスノード（PSN）の前面にあ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 [View Advanced Settings] をクリックして、設定を構成します。

- [プロトコル（Protocol）]：TACACS または RADIUS。

  （注） グレー表示されるオプションは、選択したオプションです（デフォルトでは RADIUS）。TACACS オプションを選択するには、TACACS オプションを選択してから、RADIUS オプションの選択を手動で解除する必要があります。

- [Authentication Port]：AAA サーバへの認証メッセージのリレーに使用されるポート。デフォルト値は UDP ポート 1812 です。
- [Accounting Port]：AAA サーバ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。デフォルトの UDP ポートは 1813 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 1 回です。
- [Timeout]：接続の試行が中止される前に、デバイスが AAA サーバの応答を待機する時間。

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。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。

表 *2 : SNMP* のプロパティ

フィールド	説明
Retries	デバイスへ接続可能な試行回数。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）	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 [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。

サービスの再配布

Cisco DNA Center のハイアベイラビリティ（HA）の実装については、『*Cisco Digital Network Architecture Center Administrator Guide*』を参照してください。最初にこの情報を確認してから、実稼働環境に HA を展開するかどうかを決定するようお勧めします。展開を選択する場合は、次のとおりクラスタノード間でサービスを再配布することによって HA の動作を最適化します。

1. ⚙ をクリックして、[システム設定（System Settings）] を選択します。

   [システム360（System 360）] タブは、デフォルトで表示されます。

2. [ホスト（Hosts）] 領域で、[サービス配布の有効化（Enable Service Distribution）] をクリックします。

[サービス配布の有効化（Enable Service Distribution）]をクリックすると、Cisco DNA Center がメンテナンスモードになります。このモードではサービスの再配布が完了するまで Cisco DNA Center を使用できません。HA 展開のスケジュールを設定する場合は、このことを考慮する必要があります。

（注） Cisco DNA Center は、データベースの復元、システムアップグレード（パッケージアップグレードではない）の実行、HA のサービス再配布の有効化を実行するたび、（前述のとおり）メンテナンスモードになります。