CHAPTER 6

ネットワーク デバイスの管理

この章では、ネットワーク内のデバイスを管理する方法について説明します。この章は、次の内容で構成されています。

- 「ネットワーク デバイスの管理」（P.6-1）
- 「ネットワーク デバイス グループの管理」（P.6-11）
- 「ネットワーク デバイスとネットワーク デバイス グループのインポート」（P.6-15）
- 「ネットワーク デバイスとネットワーク デバイス グループのエクスポート」（P.6-22）

ネットワーク デバイスの管理

ネットワーク デバイスは、AAA サービス要求の試行に使用される認証、許可、アカウンティング（AAA）クライアント（スイッチ、ルータなど）です。ネットワーク デバイスの定義により、Cisco Identity Services Engine（ISE）は設定されているネットワーク デバイスと対話できます。ISE に定義されていないネットワーク デバイスは、ISE から AAA サービスを受信できません。

特定の IP アドレスのデバイス定義が見つからない場合、ISE で使用できるデフォルトのネットワーク デバイスを定義することもできます。ISE では、RADIUS 認証のデフォルトのデバイス定義がサポートされています。この機能を使用すると、新しくプロビジョニングされたデバイスのデフォルトの RADIUS 共有秘密とアクセス レベルを定義できます。

ISE はネットワーク デバイスから RADIUS 要求を受信すると、対応するデバイス定義を探して設定されている共有秘密を取得します。デバイス定義が見つかった場合、デバイスに設定されている共有秘密を取得し、それを要求内の共有秘密と照合してアクセスを認証します。デバイス定義が見つからない場合、デフォルトのネットワーク デバイスから共有秘密を取得し、要求を処理します。共有秘密が一致した場合、ネットワーク アクセスは許可されます。成功した認証レポートが生成されます。一致しない場合は、拒否応答がデバイスに送信されます。失敗した認証レポートが生成され、失敗の理由が示されます。

ISE では、デバイス ディクショナリにあるデバイス タイプ、場所、モデル名などのデバイス属性に基づいて認証ポリシーと許可ポリシーを設定できます。新しいネットワーク デバイス グループ（NDG）を作成すると、ポリシー定義で使用できる新しいデバイス属性がディクショナリに追加されます。

ネットワーク デバイス定義には、次の設定を含める必要があります。

- デバイス名：デバイス名は、ネットワーク デバイスに指定できるわかりやすい名前です。デバイスのホスト名とは異なる名前にすることができます。デバイス名は論理識別子です。
- IP アドレスとサブネット マスク：IP アドレスとサブネット マスクを指定する必要があります。IP アドレスとサブネット マスクを定義するときに従う必要があるガイドラインの一部を次に示します。
  - 特定の IP アドレスを定義するか、サブネット マスクを使用して範囲を定義できます。

- 同じ IP アドレスを持つ 2 台のデバイスを定義することはできません。
- 同じ IP 範囲を持つ 2 台のデバイスを定義することはできません。IP 範囲は、一部または全部が重複することはできません。

（注）　デバイス A の IP アドレス範囲が定義されている場合、デバイス A に定義されている範囲の個別のアドレスを別のデバイス B に設定できます。

ISE は RADIUS 要求を受信し、その要求をネットワーク デバイスと照合しようとするときに、次の処理を実行します。

a. 要求内の IP アドレスに一致する特定の IP アドレスを探します。
b. 範囲を調べて、要求内の IP アドレスが指定された範囲内にあるかどうかを確認します。
c. これらの両方が失敗すると、要求の処理にデフォルトのデバイス定義（定義されている場合）が使用されます。

- ネットワーク デバイス グループ：NDG では、場所、タイプ、および他のグループに基づいてデバイスをグループ化し、これらのグループに基づいてポリシー条件を定義できます。設定時にグループに特定のデバイスを割り当てない場合、そのグループはデフォルトの [すべてのロケーション（All Locations）] および [すべてのデバイス タイプ（All Device Types）] デバイス グループに含まれます。詳細については、「ネットワーク デバイス グループの管理」（P.6-11）を参照してください。

次に、ネットワーク デバイスに定義できるオプション設定を示します。

- [モデル名（Model Name）]：モデル名によってネットワーク デバイスのモデルが識別されます。たとえば、CAT 6K、Nexus 7K などがあります。モデル名は、ルールベースのポリシーの条件をチェックするときに、パラメータの 1 つとして使用できます。この属性はデバイス ディクショナリに存在します。
- [ソフトウェア バージョン（Software Version）]：ネットワーク デバイスで実行されているソフトウェアのバージョン。たとえば、Cisco IOS Release 12.3、12.3 (2) などがあります。ソフトウェア バージョンは、ルールベースのポリシーの条件をチェックするときに、パラメータの 1 つとして使用できます。この属性はデバイス ディクショナリに存在します。

さらに、ネットワーク デバイスに次の設定を行うこともできます。

- 認証設定：RADIUS 認証に対してこの設定を行います。
- 簡易ネットワーク管理プロトコル（SNMP）設定：エンドポイントをプロファイリングするために、ISE でプロファイラ サービスに対してこの設定を行います。Cisco ISE プロファイラ サービスは、SNMP 設定が定義されているネットワーク デバイスと通信できます。プロファイラ サービスでは、これらの設定を使用してデバイスとの SNMP ベースの通信を開始し、モニタリングの目的でデバイス関連情報を取得します。
- セキュリティ グループ アクセス（SGA）設定：Cisco Security Group Access Solution に含めることができるデバイスの場合。SGA Solution は SGA デバイスです。たとえば、Nexus 7000 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、Catalyst 4000 シリーズ スイッチ、Catalyst 3000 シリーズ スイッチなどがあります。SGA デバイスは、SGA デバイスを追加するときに定義する必要がある SGA 設定を使用して認証されます。SGA 設定の詳細については、第 23 章「Cisco Security Group Access のポリシー」を参照してください。

  [PAC の生成（Generate PAC）] ボタンをクリックして、SGA PAC（Protected Access Credentials）を生成することもできます。詳細については、「[ネットワーク デバイス リスト（Network Devices List）] 画面からの SGA PAC の生成」（P.23-36）を参照してください。
- デバイス設定の詳細：ネットワーク デバイスの設定を編集するためのクレデンシャル。

これらのネットワーク デバイスを手動で設定するか、.csv ファイルを使用して一連のデバイスを ISE にインポートできます。

この項では、次のトピックを扱います。

- 「デバイスの追加と編集」（P.6-3）
- 「デバイスの削除」（P.6-7）
- 「[ネットワーク デバイス（Network Devices）] ページでのネットワーク デバイスのフィルタリング」（P.6-7）
- 「デフォルト デバイスの設定」（P.6-11）
- 「ネットワーク デバイスとネットワーク デバイス グループのインポート」（P.6-15）
- 「ネットワーク デバイスとネットワーク デバイス グループのエクスポート」（P.6-22）

デバイスの追加と編集

ISE サーバでデバイスを追加するか、デバイス定義を編集できます。

前提条件：

- この作業を開始する前に、ISE でのネットワーク デバイスおよびその管理方法の基礎を理解しておく必要があります。詳細については、「ネットワーク デバイスの管理」（P.6-1）を参照してください。
- 各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはネットワーク デバイス管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、「Cisco ISE 管理者グループのロールおよび役割」を参照してください。

デバイスを追加または編集するには、次の手順を実行します。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2　左側の [ネットワーク デバイス（Network Devices）] ナビゲーション ペインで、[ネットワーク デバイス（Network Devices）] をクリックします。

[ネットワーク デバイス（Network Devices）] ページが表示され、設定済みのデバイスのリストが示されます。

ステップ 3　[追加（Add）] をクリックするか、デバイスの隣にあるチェックボックスをオンにして編集のために [編集（Edit）] をクリックするか、[複製（Duplicate）] をクリックして重複するエントリを作成します。[ネットワーク デバイス（Network Devices）] ナビゲーション ペインでアクション アイコンをクリックして [新規デバイスの追加（Add new device）] を選択するか、リスト内のデバイス名をクリックして編集することもできます。

ステップ 4　右側のペインに、表 6-1 に説明されている値を入力します。

ステップ 5　[認証設定（Authentication Settings）] チェックボックスをオンにし、次の RADIUS 認証設定を定義します。

- [共有秘密（Shared Secret）]：共有秘密は、最大 128 文字の長さにすることができます。共有秘密は、**pac** オプションを指定した **radius-host** コマンドを使用してデバイスに設定したキーです。

- [KeyWrap を有効にする（Enable KeyWrap）] : このオプションを指定すると、AES KeyWrap アルゴリズムにより RADIUS プロトコルのセキュリティが強化され、Cisco ISE における FIPS 140-2 準拠に役立ちます。
- [キー暗号キー（Key Encryption Key）] : このキーはセッションの暗号化（秘密）に使用します。
- [メッセージ オーセンティケータ コード キー（Message Authenticator Code Key）] : このキーは、RADIUS メッセージに対するキー付き Hashed Message Authentication Code（HMAC）の計算に使用されます。
- [キー入力形式（Key Input Format）] : WLAN コントローラで使用できる設定と一致するように、Cisco ISE FIPS 暗号キーの入力に使用する形式を指定します。（指定する値は、次に定義されている正しい（全体）長さにする必要があり、それよりも短い値は許可されません）。
  - [ASCII] : [キー暗号キー（Key Encryption Key）] の長さは 16 文字（バイト）で、[メッセージ オーセンティケータ コード キー（Message Authenticator Code Key）] の長さは 20 文字（バイト）である必要があります。
  - [16 進（Hexadecimal）] : [キー暗号キー（Key Encryption Key）] の長さは 32 バイトで、[メッセージ オーセンティケータ コード キー（Message Authenticator Code Key）] の長さは 40 バイトである必要があります。

ステップ 6　[SNMP] チェックボックスをオンにして、デバイスの SNMP を設定します。これらの設定は ISE のプロファイラ サービスによって使用されます。表 6-2 に説明されているように値を入力します。

スイッチ関連の SNMP 設定の詳細については、以下を参照してください。

- 「SNMP トラップの有効化」（P.C-8）
- 「プロファイリング用の SNMP v3 クエリーの有効化」（P.C-8）

ステップ 7　[セキュリティ グループ アクセス（SGA）（Security Group Access (SGA)）] チェックボックスをオンにして、SGA デバイスを設定します。SGA デバイスでは IP アドレスは使用されません。代わりに、SGA デバイスが ISE と通信できるように、他の設定を定義する必要があります。表 23-4 に説明されているように値を入力します。

ステップ 8　[デバイス設定の展開（Device Configuration Deployment）] チェックボックスをオンにして、デバイスの設定を編集するためのユーザ クレデンシャルを入力します。表 6-3 に説明されているように値を入力します。

ステップ 9　[送信（Submit）] をクリックしてデバイス定義を保存します。

[ネットワーク デバイス（Network Devices）] ページ

表 6-1 に、[ネットワーク デバイス（Network Devices）] ページのフィールドとその説明を示します。

表 6-1　[ネットワーク デバイス（Network Devices）] ページ

フィールド	説明
名前（Name）	（必須）このフィールドはデバイスの名前です。 **（注）**　デバイスの名前は編集できません。
説明（Description）	このフィールドはデバイスの説明です。
IP アドレス（IP Address）	（必須）このフィールドには、デバイスに関連付けられている IP アドレスとサブネット マスクが含まれます。1 つのアドレスまたは範囲で、ルーティング可能な IP アドレスは、Cisco ISE アプライアンスが通信できるアドレスにする必要があります。

表 6-1　[ネットワーク デバイス（Network Devices）] ページ （続き）

フィールド	説明
モデル名（Model Name）	このフィールドは、Cisco Catalyst 6K、Cisco Nexus 7K などのデバイス モデルです。
ソフトウェア バージョン（Software version）	このフィールドは、Version 12.2、12.3 などのデバイス上のソフトウェアのバージョンです。
ネットワーク デバイス グループ（Network Device Group）	（必須）[場所（Location）] および [デバイス タイプ（Device Type）] ドロップダウン リストから、デバイスに関連付ける場所とデバイス タイプを選択します。 （注）　デバイス グループを選択しない場合は、デフォルトのデバイス グループ（ルート NDG）が割り当てられます。

[ネットワーク デバイス（Network Devices）] : [SNMP 設定（SNMP Settings）]

表 6-2 に、[ネットワーク デバイス（Network Devices）] ページの SNMP 設定とその説明を示します。

表 6-2　[ネットワーク デバイス（Network Devices）] リスト ページ : [SNMP 設定（SNMP Settings）]

フィールド	説明
SNMP バージョン（SNMP Version）	（必須）この設定は、要求に使用する SNMP のバージョンです。有効なオプションは次のとおりです。 • 1 : SNMPv1 は informs をサポートしていません。 • 2c • 3 : SNMPv3 は、[Priv] セキュリティ レベルを選択した場合にパケット暗号化が可能であるため、最もセキュアなモデルです。 （注）　ネットワーク デバイスに SNMPv3 パラメータを設定した場合、モニタリング サービス（[操作（Operations）] > [レポート（Reports）] > [カタログ（Catalog）] > [ネットワーク デバイス（Network Device）] > [セッション ステータス概要（Session Status Summary）]）によって提供されるネットワーク デバイス セッション ステータス概要レポートを生成できません。ネットワーク デバイスに SNMPv1 または SNMPv2c パラメータが設定されている場合は、このレポートを正常に生成できます。
SNMP RO コミュニティ（SNMP RO Community）	（SNMP バージョン 1 または 2c を選択した場合は必須）この設定は、読み取り専用のコミュニティ ストリングです。コミュニティ ストリングはパスワードに似ており、ISE にデバイスへの特定のタイプのアクセスを提供します。
SNMP ユーザ名（SNMP Username）	（SNMP バージョン 3 を選択した場合は必須）この設定は、SNMPv3 のユーザ名です。
セキュリティ レベル（Security Level）	（SNMP バージョン 3 を選択した場合は必須）SNMPv3 のセキュリティ レベルを選択します。有効なオプションは次のとおりです。 • [Auth] : MD5[1] または Secure Hash Algorithm（SHA）パケットの認証を有効にします。 • [No Auth] : 認証なし、プライバシーなしのセキュリティ レベル。 • [Priv] : DES[2] パケットの暗号化を有効にします。

表 6-2　[ネットワーク デバイス（Network Devices）] リスト ページ : [SNMP 設定（SNMP Settings）]（続き）

フィールド	説明
認証プロトコル（Auth Protocol）	この設定は、デバイスで使用する認証プロトコルです。有効なオプションは、[MD5] または [SHA1] です。
認証パスワード（Auth Password）	認証キーを入力します。認証キーは 8 文字以上の長さにする必要があります。
プライバシー プロトコル（Privacy Protocol）	この設定は、デバイスで使用するプライバシー プロトコルです。有効なオプションは [DES]、[AES128]、[AES192]、[AES256]、および [3DES] です。
プライバシー パスワード（Privacy Password）	プライバシー キーを入力します。
ポーリング間隔（Polling Interval）	この設定は、秒単位の SNMP ポーリング間隔です。デフォルトは 3600 秒です。
リンク トラップ クエリー（Link Trap Query）	プロファイラ サービスでデバイスに接続された NAD[3] からリンク トラップを受信する場合、デバイスに対してクエリーを実行するには、このチェックボックスをオンにします。
MAC トラップ クエリー（MAC Trap Query）	プロファイラ サービスでデバイスに接続された NAD から MAC トラップを受信する場合、デバイスに対してクエリーを実行するには、このチェックボックスをオンにします。
送信元ポリシー サービス ノード（Originating Policy Services Node）	この設定は、SNMP データのポーリングに使用するサーバを示します。デフォルトでは自動ですが、別の値を割り当てて設定を上書きできます。

1. MD5 = Message Digest 5。
2. DES = データ暗号規格。
3. NAD = ネットワーク アクセス デバイス

[ネットワーク デバイス（Network Devices）] : [デバイス設定の展開（Device Configuration Deployment）] の設定

表 6-3　[ネットワーク デバイス（Network Devices）] ページ : [デバイス設定の展開（Device Configuration Deployment）] の設定

フィールド	説明
EXEC モード ユーザ名（Exec Mode Username）	デバイス設定を編集する権限を持っているユーザ名を入力します。
EXEC モード パスワード（Exec Mode Password）	デバイス パスワードを入力します。
有効モード パスワード（Enable Mode Password）	デバイスの設定を編集するためのデバイスの有効パスワードを入力します。

詳細情報：

- 「ネットワーク デバイスの管理」（P.6-1）
- 「ネットワーク デバイス グループの管理」（P.6-11）
- 「ネットワーク デバイスとネットワーク デバイス グループのインポート」（P.6-15）
- 「ネットワーク デバイスとネットワーク デバイス グループのエクスポート」（P.6-22）

デバイスの削除

前提条件：

各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはネットワーク デバイス管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、「Cisco ISE 管理者グループのロールおよび役割」を参照してください。

ネットワーク デバイスを削除するには、次の手順を実行します。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2　左側の [ネットワーク デバイス（Network Devices）] ナビゲーション ペインで、[ネットワーク デバイス（Network Devices）] をクリックします。

[ネットワーク デバイス（Network Devices）] リスト ページが表示されます。

ステップ 3　削除するデバイスの隣にあるチェックボックスをオンにし、[削除（Delete）] > [選択済みの削除（Delete Selected）] を選択します。または、左側のナビゲーション ペインのリストからネットワーク デバイスを選択し、[操作（Action）] アイコン（  ）をクリックして [デバイスの削除（Delete device）] を選択します。

（注）　[削除（Delete）] > [すべて削除（Delete All）] をクリックして、定義されているすべてのデバイスを削除できます。

ダイアログボックスに次のメッセージが表示されます。

"*Device name*" を削除しますか？（Are you sure you want to delete "*Device name*"?）

ステップ 4　[OK] をクリックしてデバイスを削除します。

[ネットワーク デバイス（Network Devices）] ページでのネットワーク デバイスのフィルタリング

[ネットワーク デバイス（Network Devices）] ページで [表示（Show）] ドロップダウン リストを使用するか [フィルタ（Filter）] アイコンをクリックして、クイック フィルタを呼び出したり、閉じたりすることができます。クイック フィルタは、[ネットワーク デバイス（Network Devices）] ページで、ネットワーク デバイスの名前、説明、場所、タイプ、IP/マスクなどのフィールド説明に基づいてネットワーク デバイスをフィルタリングするために使用できる簡単なフィルタです。1 つの IP アドレスによるネットワーク デバイスのフィルタリングは排他的フィルタであり、クイック フィルタで他のすべてのフィルタ フィールドが無効になります。

[表示（Show）] ドロップダウン リストを使用して、拡張フィルタを呼び出すことができます。拡張フィルタは複雑なフィルタであり、[ネットワーク デバイス（Network Devices）] ページで結果とともに、後で使用したり取得したりするためにプリセットしておくことができます。拡張フィルタを使用すると、ネットワーク デバイスがフィールド説明に関連付けられた特定の値に基づいてフィルタリングされます。フィルタを追加または削除したり、一連のフィルタを組み合わせて 1 つの拡張フィルタにしたりすることができます。1 つの IP アドレスによるネットワーク デバイスのフィルタリングは排他的フィルタであり、拡張フィルタで他のフィールドをフィルタリングに同時に使用することはできません。

[プリセット フィルタの管理（Manage Preset Filters）] オプションを使用して、すべてのプリセット フィルタを表示できます。このオプションを使用してプリセット フィルタを管理できます。プリセット フィルタを作成して保存したら、[ネットワーク デバイス（Network Devices）] ページのフィルタリングされた結果のリストからプリセット フィルタを選択できます。プリセット フィルタにはセッション ライフタイムがあり、この間、[ネットワーク デバイス（Network Devices）] ページにフィルタリングされた結果が表示されます。プリセット フィルタを編集することも、プリセット フィルタ リストから削除することもできます。

ネットワーク デバイスをフィルタリングするには、次の手順を実行します。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）]（メニュー ウィンドウ）を選択します。

[ネットワーク デバイス（Network Devices）] メニューが表示されます。

ステップ 2　[ネットワーク デバイス（Network Devices）] メニュー ウィンドウで、[ネットワーク デバイス（Network Devices）] を選択します。

[ネットワーク デバイス（Network Devices）] ページに、すべてのネットワーク デバイスが表示されます。

ステップ 3　[ネットワーク デバイス（Network Devices）] ページで、[表示（Show）] ドロップダウン矢印をクリックしてフィルタ オプションを表示します。

ここでは、クイック フィルタ、フィルタリング用の拡張フィルタ、[プリセット フィルタの管理（Manage Preset Filters）] オプション（フィルタリング用のプリセット フィルタを管理できる）を選択できます。表 6-4 を参照してください。

詳細については、「クイック フィルタ オプションを使用してフィルタリングするには、次の手順を実行します。」（P.6-8）および「拡張フィルタ オプションを使用してフィルタリングするには、次の手順を実行します。」（P.6-9）を参照してください。

（注）　ネットワーク デバイス リストに戻るには、[表示（Show）] ドロップダウン リストから [すべて（All）] を選択します。フィルタリングなしですべてのネットワーク デバイスが表示されます。

クイック フィルタ オプションを使用してフィルタリングするには、次の手順を実行します。

クイック フィルタを使用すると、ネットワーク デバイスが [ネットワーク デバイス（Network Devices）] ページの [IP/マスク（IP/Mask）] フィールドを除く各フィールド説明に基づいてフィルタリングされます。いずれかのフィールドの内部をクリックし、フィールドに検索条件を入力すると、ページが更新されて結果が [ネットワーク デバイス（Network Devices）] ページに表示されます。フィールドをクリアすると、[ネットワーク デバイス（Network Devices）] ページにすべてのネットワーク デバイスのリストが表示されます。IP/マスクによるフィルタリングを使用すると、クイック フィルタで他のすべてのフィールドが無効になります。

ステップ 1　フィルタリングするには、各フィールドで [実行（Go）] ボタンをクリックします。ページが更新されて結果が [ネットワーク デバイス（Network Devices）] ページに表示されます。

ステップ 2　フィールドをクリアするには、各フィールドで [クリア（Clear）] ボタンをクリックします。

拡張フィルタ オプションを使用してフィルタリングするには、次の手順を実行します。

拡張フィルタでは、より複雑な変数を使用してネットワーク デバイスをフィルタリングできます。フィールド説明に一致する値に基づいてネットワーク デバイスをフィルタリングする 1 つ以上のフィルタが含まれています。1 行に 1 つのフィルタの場合、ネットワーク デバイスは各フィールド説明とフィルタに定義した値に基づいてフィルタリングされます。複数のフィルタを使用して値を照合し、ネットワーク デバイスのフィルタリングを行うには、1 つの拡張フィルタ内のフィルタのいずれかまたはすべてを使用します。IP/ マスクによるフィルタリングを使用すると、拡張フィルタで他のすべてのフィールドを同時に使用したフィルタリングが無効になります。

ステップ 1　フィールドの説明を表示および選択するには、ドロップダウン矢印をクリックします。

[IP/ マスク（IP/Mask）] を選択した場合、拡張フィルタで同時フィルタリングに他のフィルタを使用できません。

ステップ 2　演算子を表示および選択するには、ドロップダウン矢印をクリックします。

ステップ 3　選択したフィールドの説明の値を入力します。

ステップ 4　フィルタを追加するには [行の追加（Add Row）]（プラス [+] 記号）ボタンをクリックし、フィルタを削除するには [行の削除（Remove Row）]（マイナス [-] 記号）ボタンをクリックします。

ステップ 5　各フィルタの値に一致させるには [すべて（All）] をクリックし、いずれか 1 つのフィルタの値に一致させるには [任意（Any）] をクリックします。

ステップ 6　[実行（Go）] をクリックしてフィルタリングを開始します。

ステップ 7　[保存（Save）] アイコンをクリックしてフィルタを保存します。

[プリセット フィルタの保存（Save a Preset Filter）] ダイアログが表示されます。フィルタを保存するファイル名を入力し、[保存（Save）] をクリックします。作成するプリセット フィルタの名前にはスペースは使用できません。現在のフィルタを保存しないでフィルタをクリアするには、[キャンセル（Cancel）] をクリックします。

表 6-4 に、[ネットワーク デバイス（Network Devices）] ページでネットワーク デバイスのフィルタリングに使用できるフィールドを示します。

表 6-4　ネットワーク デバイスのフィルタリング

フィルタリング方法	フィルタリング フィールド	フィルタリング フィールドの説明
クイック フィルタ	名前（Name）	このフィールドを使用すると、ネットワーク デバイスの名前でネットワーク デバイスをフィルタリングできます。
	IP/マスク（IP/Mask）	このフィールドを使用すると、1 つの IP アドレスでネットワーク デバイスをフィルタリングできます。IP アドレスの一部によるフィルタリングでは、多くのレコードが生成され、結果にはその IP アドレスの一部を含むすべての IP アドレスが含まれます。
	場所（Location）	このフィールドを使用すると、ネットワーク デバイスの場所でネットワーク デバイスをフィルタリングできます。
	タイプ（Type）	このフィールドを使用すると、ネットワーク デバイスのタイプでネットワーク デバイスをフィルタリングできます。
	説明（Description）	このフィールドを使用すると、ネットワーク デバイスの説明でネットワーク デバイスをフィルタリングできます。
拡張フィルタ	次の中からフィールドの説明を選択します。 • 名前（Name） • IP/マスク（IP/Mask） • 場所（Location） • タイプ（Type） • 説明（Description）	ドロップダウン矢印をクリックしてフィールドの説明を選択します。
	演算子（Operator）	[演算子（Operator）] フィールドでドロップダウン矢印をクリックして、ネットワーク デバイスのフィルタリングに使用できる演算子を選択します。
	値（Value）	[値（Value）] フィールドで、選択したフィールド説明の値を選択します。この値に基づいてネットワーク デバイスがフィルタリングされます。

デフォルト デバイスの設定

RADIUS 要求に対して特定のデバイス定義が見つからない場合は、デフォルトのデバイス定義を使用できます。

前提条件：

各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはネットワーク デバイス管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、「Cisco ISE 管理者グループのロールおよび役割」を参照してください。

デフォルト デバイスを定義するには、次の手順を実行します。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2　左側の [ネットワーク デバイス（Network Devices）] ナビゲーション ペインで、[デフォルト デバイス（Default Device）] をクリックします。

[デフォルトのネットワーク デバイス（Default Network Device）] ページが表示されます。

ステップ 3　デフォルトのネットワーク デバイス定義を有効にするには、[デフォルトのネットワーク デバイスのステータス（Default Network Device Status）] ドロップダウン リストから [有効（Enable）] を選択します。

ステップ 4　RADIUS 共有秘密を入力します。

ステップ 5　[送信（Submit）] をクリックしてデフォルトのネットワーク デバイス定義を保存します。

結果：

ダイアログボックスに次のメッセージが表示されます。

設定は正常に保存されました。

詳細については、「ネットワーク デバイスの管理」（P.6-1）を参照してください。

ネットワーク デバイス グループの管理

デバイス グループは、ネットワーク デバイス グループ（NDG）が含まれた階層構造です。NDG では、デバイスが場所やデバイス タイプなどのさまざまな条件に基づいてグループ化されます。ルートの NDG ノードを作成する場合は、NDG の名前とタイプを指定する必要があります。後続のすべての子 NDG ノードについては、名前のみを指定する必要があります。タイプは親 NDG から継承されるため、ルート NDG の下にあるすべての子 NDG ノードは同じタイプになります。

ISE では、階層構造の NDG を作成できます。したがって、デバイスは、複数の NDG に属することができます。たとえば、デバイスは、次のような大陸、地域、および国でグループ化できます。

- アフリカ -> 南部 -> ナミビア
- アフリカ -> 南部 -> 南アフリカ
- アフリカ -> 南部 -> ボツワナ

次のようなデバイス タイプでデバイスをグループ化することもできます。

- アフリカ -> 南部 -> ボツワナ -> ファイアウォール

- アフリカ -> 南部 -> ボツワナ -> ルータ
- アフリカ -> 南部 -> ボツワナ -> スイッチ

ポリシー条件で NDG を使用できます。ISE には、事前定義された 2 つのルート NDG があります（[場所（Location）] および [デバイス タイプ（Device Type）])。事前定義された NDG の編集や削除を行うことはできません。デバイスは 1 つの NDG に割り当てることができます。作成した NDG は、ポリシーを定義するときに使用できます。新しいルート NDG を作成すると、新しいデバイス属性がディクショナリに追加されます。この属性を認証および許可ポリシーで使用できます。

（注）　ルート NDG のデバイス タイプは、デバイス ディクショナリで属性として使用できます。この属性に基づいて条件を定義できます。NDG の名前は、この属性が取得できる値のいずれかです。

この項では、次のトピックを扱います。

- 「ネットワーク デバイス グループの作成」（P.6-12）
- 「ネットワーク デバイス グループの編集」（P.6-13）
- 「ネットワーク デバイス グループの削除」（P.6-14）
- 「ISE へのネットワーク デバイス グループのインポート」（P.6-20）
- 「ネットワーク デバイス グループのエクスポート」（P.6-23）

ネットワーク デバイス グループの作成

前提条件：
各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはネットワーク デバイス管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、「Cisco ISE 管理者グループのロールおよび役割」を参照してください。

NDG を作成するには、次の手順を実行します。

（注）　デフォルトの NDG（[すべてのロケーション（All Locations）] および [すべてのデバイス タイプ（All Device Types）]）は編集できませんが、その下に新しいデバイス サブグループを追加することはできます。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] を選択します。

左側の [ネットワーク デバイス グループ（Network Device Groups）] ナビゲーション ペインで、[グループ（Groups）] をクリックします。

[ネットワーク デバイス グループ（Network Device Groups）] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- ルート NDG を作成するには、[追加（Add）] をクリックします。
- 子 NDG を作成するには、ナビゲーション ペインで、子 NDG を追加するグループをクリックし、[追加（Add）] をクリックします。

ステップ 3　[ネットワーク デバイス グループ（Network Device Groups）] ページで、次の情報を入力します。

- （必須）NDG の名前。この名前がナビゲーション ペインに表示されます。

NDG のフルネームは最大 100 文字です。たとえば、親グループ [Global] > [Asia] の下にサブグループ India を作成する場合、作成する NDG のフルネームは Global#Asia#India となり、このフルネームが 100 文字を超えてはなりません。NDG のフルネームが 100 文字を超える場合は、NDG の作成に失敗します。

- 任意の説明。
- （必須）NDG のタイプ。この NDG がルート NDG の場合、このデバイス タイプがデバイス ディクショナリで属性として使用できるようになります。この NDG が子 NDG の場合、親 NDG の名前がこのフィールドに表示されます。

ステップ 4　[保存（Save）] をクリックして NDG 設定を保存します。

結果：
NDG が正常に作成されると、ページの右下にポップアップ ダイアログが表示され、「*NDG_name* は正常に保存されました（NDG_name has been saved successfully）」というメッセージが表示されます。

関連項目
- 「ネットワーク デバイスの管理」（P.6-1）
- 「ネットワーク デバイス グループの編集」（P.6-13）
- 「ネットワーク デバイス グループの削除」（P.6-14）

ネットワーク デバイス グループの編集

前提条件：
各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはネットワーク デバイス管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、「Cisco ISE 管理者グループのロールおよび役割」を参照してください。

NDG を編集するには、次の手順を実行します。

（注）　事前定義された [場所（Location）] および [デバイス タイプ（Device Type）] NDG は編集できません。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] を選択します。

ステップ 2　左側のナビゲーション ペインで、[グループ タイプ（Group Types）] をクリックします。

[ネットワーク デバイス グループ（Network Device Groups）] リスト ページが表示されます。

ステップ 3　左側の [グループ タイプ（Group Types）] ナビゲーション ペインで、編集する子 NDG の親 NDG を選択します。

[ネットワーク デバイス グループ（Network Device Group）] リスト ページに子 NDG のリストが表示されます。

ステップ 4　編集する NDG の隣のチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 5　NDG の名前か説明、または両方を編集します。

NDG タイプは編集できません。

ステップ 6　[保存（Save）] をクリックして変更を保存します。

結果：
編集処理が正常に完了すると、ページの右下にポップアップ ダイアログが表示され、「*NDG_name* は正常に保存されました（NDG_name has been saved successfully）」というメッセージが表示されます。

関連項目

- 「ネットワーク デバイスの管理」（P.6-1）
- 「ネットワーク デバイス グループの作成」（P.6-12）
- 「ネットワーク デバイス グループの削除」（P.6-14）

ネットワーク デバイス グループの削除

前提条件：
各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはネットワーク デバイス管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、「Cisco ISE 管理者グループのロールおよび役割」を参照してください。

NDG を削除するには、次の手順を実行します。

（注）　下にサブグループがある NDG は削除できません。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] を選択します。

ステップ 2　左側のナビゲーション ペインで、[グループ タイプ（Group Types）] をクリックします。

[ネットワーク デバイス グループ（Network Device Groups）] リスト ページが表示されます。

ステップ 3　左側の [グループ タイプ（Group Types）] ナビゲーション ペインで、削除する子 NDG の親 NDG を選択します。

[ネットワーク デバイス グループ（Network Device Group）] リスト ページに子 NDG のリストが表示されます。

ステップ 4　削除する NDG の隣のチェックボックスをオンにして、[削除（Delete）] をクリックします。または、左側のナビゲーション ペインから削除する子 NDG を選択し、[操作（Action）] アイコンをクリックして [グループの削除（Delete Group）] を選択します。

ダイアログボックスに次のメッセージが表示されます。

削除してもよろしいですか？（Are you sure you want to delete?）

ステップ 5　NDG を削除するには、[OK] をクリックします。

結果：
削除処理が正常に完了すると、ページの右下にポップアップ ダイアログが表示され、「グループは正常に削除されました（Group was deleted successfully）」というメッセージが表示されます。

関連項目

- 「ネットワーク デバイスの管理」（P.6-1）
- 「ネットワーク デバイス グループの作成」（P.6-12）
- 「ネットワーク デバイス グループの編集」（P.6-13）

ネットワーク デバイスとネットワーク デバイス グループのインポート

ISE では、カンマ区切り形式（.csv）ファイルを使用して大量のネットワーク デバイスやネットワーク デバイス グループをインポートできます。デバイスとデバイス グループをインポートするときに、新しいレコードを作成したり、既存のレコードを更新したりできます。.csv インポート テンプレートを ISE ユーザ インターフェイスからダウンロードし、テンプレートにデバイスまたはデバイス グループの詳細を入力して、.csv ファイルとして保存できます。そのファイルを ISE にインポートできます。インポート ジョブを設定するときに、ISE で既存のデバイス定義を新しいデバイス定義で上書きするか、最初のエラーが検出されたときにインポート プロセスを中止するかを定義することもできます。

インポート ジョブが開始されたら、ISE ユーザ インターフェイスでジョブのステータスを確認できます。同じリソース タイプの 2 つのインポート ジョブを同時に実行することはできません。たとえば、2 つのインポート ジョブを同時に実行して、2 つの異なるインポート ファイルからネットワーク デバイスをインポートできません。

デバイスを ISE にインポートするには、次の作業を完了する必要があります。

1. 「インポート ファイル テンプレートのダウンロード」（P.6-15）
2. 「CSV インポート ファイルの作成」（P.6-16）
3. 「ISE へのデバイスのインポート」（P.6-19）または「ISE へのネットワーク デバイス グループのインポート」（P.6-20）

インポート ファイル テンプレートのダウンロード

前提条件：
各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはネットワーク デバイス管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、「Cisco ISE 管理者グループのロールおよび役割」を参照してください。

インポート ファイル テンプレートをダウンロードするには、次の手順を実行します。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2　左側の [ネットワーク デバイス（Network Devices）] ナビゲーション ペインで、[ネットワーク デバイス（Network Devices）] をクリックします。

[ネットワーク デバイス（Network Devices）] ページが表示されます。

（注）　ネットワーク デバイス グループのテンプレートをダウンロードする場合は、[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] を選択し、[グループ タイプ（Group Types）] をクリックします。

ステップ 3　[インポート（Import）] をクリックします。

[インポート（Import）] ページが表示されます。

ステップ 4　[テンプレートの生成（Generate a Template）] をクリックします。

ステップ 5　テンプレート ファイルをローカル ハード ディスクに保存します。

結果：

テンプレートがローカル ハード ディスクにダウンロードされます。

CSV インポート ファイルの作成

CSV インポート ファイルを ISE にインポートする前に、まず作成する必要があります。

前提条件：

各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはネットワーク デバイス管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、「Cisco ISE 管理者グループのロールおよび役割」を参照してください。

CSV インポート ファイルを作成するには、次の手順を実行します。

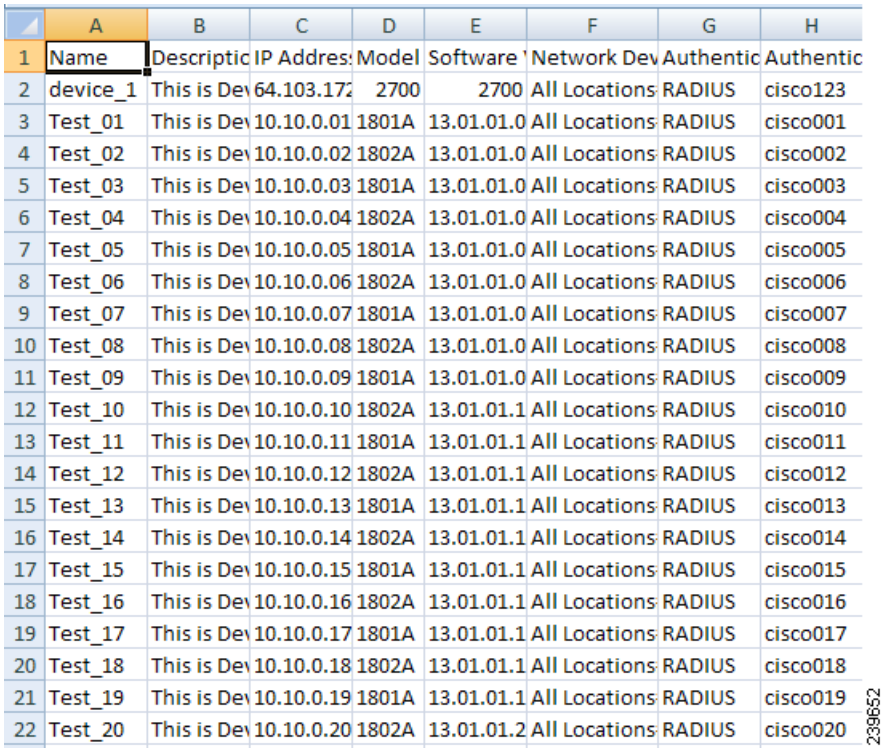
ステップ 1　Microsoft Excel または任意のスプレッドシート アプリケーションを使用して、ダウンロードした CSV テンプレートを開きます。

CSV テンプレートの最初の行はヘッダーで、ファイル内のフィールドの形式を定義します。このヘッダーは、編集しないでそのまま使用してください。

- 表 6-5 に、ヘッダーのフィールドとネットワーク デバイスの CSV ファイル テンプレートにおけるこれらのフィールドの説明を示します。
- 表 6-6 に、ヘッダーのフィールドとネットワーク デバイス グループの CSV ファイル テンプレートにおけるこれらのフィールドの説明を示します。

ステップ 2　図 6-1 に示すようにネットワーク デバイスのデータを入力するか、図 6-2 に示すようにネットワーク デバイス グループのデータを入力します。

図 6-1　ネットワーク デバイスをインポートするためのサンプル CSV ファイル



	A	B	C	D	E	F	G	H
1	Name	Descriptic	IP Addres	Model	Software	Network Dev	Authentic	Authentic
2	device_1	This is Dev	64.103.172	2700	2700	All Locations	RADIUS	cisco123
3	Test_01	This is Dev	10.10.0.01	1801A	13.01.01.0	All Locations	RADIUS	cisco001
4	Test_02	This is Dev	10.10.0.02	1802A	13.01.01.0	All Locations	RADIUS	cisco002
5	Test_03	This is Dev	10.10.0.03	1801A	13.01.01.0	All Locations	RADIUS	cisco003
6	Test_04	This is Dev	10.10.0.04	1802A	13.01.01.0	All Locations	RADIUS	cisco004
7	Test_05	This is Dev	10.10.0.05	1801A	13.01.01.0	All Locations	RADIUS	cisco005
8	Test_06	This is Dev	10.10.0.06	1802A	13.01.01.0	All Locations	RADIUS	cisco006
9	Test_07	This is Dev	10.10.0.07	1801A	13.01.01.0	All Locations	RADIUS	cisco007
10	Test_08	This is Dev	10.10.0.08	1802A	13.01.01.0	All Locations	RADIUS	cisco008
11	Test_09	This is Dev	10.10.0.09	1801A	13.01.01.0	All Locations	RADIUS	cisco009
12	Test_10	This is Dev	10.10.0.10	1802A	13.01.01.1	All Locations	RADIUS	cisco010
13	Test_11	This is Dev	10.10.0.11	1801A	13.01.01.1	All Locations	RADIUS	cisco011
14	Test_12	This is Dev	10.10.0.12	1802A	13.01.01.1	All Locations	RADIUS	cisco012
15	Test_13	This is Dev	10.10.0.13	1801A	13.01.01.1	All Locations	RADIUS	cisco013
16	Test_14	This is Dev	10.10.0.14	1802A	13.01.01.1	All Locations	RADIUS	cisco014
17	Test_15	This is Dev	10.10.0.15	1801A	13.01.01.1	All Locations	RADIUS	cisco015
18	Test_16	This is Dev	10.10.0.16	1802A	13.01.01.1	All Locations	RADIUS	cisco016
19	Test_17	This is Dev	10.10.0.17	1801A	13.01.01.1	All Locations	RADIUS	cisco017
20	Test_18	This is Dev	10.10.0.18	1802A	13.01.01.1	All Locations	RADIUS	cisco018
21	Test_19	This is Dev	10.10.0.19	1801A	13.01.01.1	All Locations	RADIUS	cisco019
22	Test_20	This is Dev	10.10.0.20	1802A	13.01.01.2	All Locations	RADIUS	cisco020

239652

ステップ 3　.csv ファイルを保存します。

ネットワーク デバイスの CSV テンプレートにおけるフィールドの説明

表 6-5　CSV テンプレートのフィールドと説明

フィールド	説明
Name:String(32):Required	（必須）このフィールドはネットワーク デバイスの名前です。最大 32 文字の英数字の文字列です。
Description:String(256)	このフィールドは、ネットワーク デバイスの任意の説明です。最大 256 文字の文字列です。
IP Address:Subnets(a.b.c.d/m|...):Required	（必須）このフィールドは、ネットワーク デバイスの IP アドレスとサブネット マスクです（パイプ「|」記号で複数の値を区切って指定できます）。
Model Name:String(32):Required	（必須）このフィールドはネットワーク デバイスのモデル名です。最大 32 文字の文字列です。
Software Version:String(32):Required	（必須）このフィールドはネットワーク デバイスのソフトウェア バージョンです。最大 32 文字の文字列です。
Network Device Groups:String(100):Required	（必須）このフィールドは、既存のネットワーク デバイス グループにする必要があります。サブグループを指定できますが、親グループとサブグループの両方をスペースで区切って含める必要があります。最大 100 文字の文字列（たとえば、Location#All Location#US）です。

表 6-5　CSV テンプレートのフィールドと説明 （続き）

フィールド	説明
Authentication:Protocol:String(6)	これはオプションのフィールドです。認証に使用するプロトコルです。唯一の有効な値は RADIUS です（大文字と小文字は区別されません）。
Authentication:Shared Secret:String(128)	（認証プロトコルのフィールドの値を入力した場合は必須）これは、最大 128 文字の文字列です。
SNMP:Version:Enumeration (1|2c|3)	これはオプションのフィールドで、プロファイラ サービスによって使用されます。SNMP プロトコルのバージョンです。有効な値は、1、2c、または 3 です。
SNMP:RO Community:String(32)	（SNMP バージョンのフィールドの値を入力した場合は必須）SNMP RO コミュニティ。最大 32 文字の文字列です。
SNMP:RW Community:String(32)	（SNMP バージョンのフィールドの値を入力した場合は必須）SNMP RW コミュニティ。最大 32 文字の文字列です。
SNMP:Username:String(32)	これはオプションのフィールドです。最大 32 文字の文字列です。
SNMP:Security Level:Enumeration(Auth|No Auth|Priv)	（SNMP バージョン 3 を選択した場合は必須）有効な値は、Auth、No Auth、Priv です。
SNMP:Authentication Protocol:Enumeration(MD5|SHA)	（SNMP セキュリティ レベルで Auth または Priv を入力した場合は必須）有効な値は、MD5 または SHA です。
SNMP:Authentication Password:String(32)	（SNMP セキュリティ レベルで Auth を入力した場合は必須）これは、最大 32 文字の文字列です。
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)	（SNMP セキュリティ レベルで Priv を入力した場合は必須）有効な値は、DES、AES128、AES192、AES256、または 3DES です。
SNMP:Privacy Password:String(32)	（SNMP セキュリティ レベルで Priv を入力した場合は必須）これは、最大 32 文字の文字列です。
SNMP:Polling Interval:Integer:600-86400 seconds	これはオプションのフィールドで、SNMP ポーリング間隔を設定します。有効な値は 600 ～ 86400 の整数です。
SNMP:Is Link Trap Query:Boolean(true|false)	これはオプションのフィールドで、SNMP リンク トラップを有効または無効にします。有効な値は true または false です。
SNMP:Is MAC Trap Query:Boolean(true|false)	これはオプションのフィールドで、SNMP MAC トラップを有効または無効にします。有効な値は true または false です。
SGA:Device Id:String(32)	これはオプションのフィールドです。セキュリティ グループ アクセス デバイス ID で、最大 32 文字の文字列です。
SGA:Device Password:String(256)	（SGA デバイス ID を入力した場合は必須）これはセキュリティ グループ アクセス デバイスのパスワードで、最大 256 文字の文字列です。
SGA:Environment Data Download Interval:Integer	これはオプションのフィールドです。セキュリティ グループ アクセス環境データのダウンロード間隔です。有効な値は 1 ～ 24850 の整数です。

表 6-5　CSV テンプレートのフィールドと説明 （続き）

フィールド	説明
SGA:Peer Authorization Policy Download Interval:Integer	これはオプションのフィールドです。セキュリティ グループ アクセス ピアの許可ポリシーのダウンロード間隔です。有効な値は 1 ～ 24850 の整数です。
SGA:Reauthentication Interval:Integer	これはオプションのフィールドです。セキュリティ グループ アクセスの再認証間隔です。有効な値は 1 ～ 24850 の整数です。
SGA:SGACL List Download Interval:Integer	これはオプションのフィールドです。セキュリティ グループ アクセスの SGACL リストのダウンロード間隔です。有効な値は 1 ～ 24850 の整数です。
SGA:Is Other SGA Devices Trusted:Boolean(true|false)	これはオプションのフィールドです。セキュリティ グループ アクセスを信頼できるかどうかを指定します。有効な値は true または false です。
SGA:Is Device Included on SGT Mapping:Boolean(true|false)	これはオプションのフィールドです。SGT に含まれているセキュリティ グループ アクセス デバイスです。有効な値は true または false です。
Deployment:Execution Mode Username:String(32)	これはオプションのフィールドです。デバイス設定を編集する権限を持っているユーザ名です。最大 32 文字の文字列です。
Deployment:Execution Mode Password:String(32)	これはオプションのフィールドです。デバイス パスワードで、最大 32 文字の文字列です。
Deployment:Enable Mode Password:String(32)	これはオプションのフィールドです。設定を編集するためのデバイスの有効パスワードで、最大 32 文字の文字列です。

これらの各フィールドの詳細については、表 6-1、表 6-2、表 23-4、および表 6-3 を参照してください。

結果：

.csv ファイルが作成され、インポート プロセスを開始できます。

関連項目

- 「ネットワーク デバイスとネットワーク デバイス グループのインポート」（P.6-15）
- 「ISE へのデバイスのインポート」（P.6-19）

ISE へのデバイスのインポート

前提条件：

各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはネットワーク デバイス管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、「Cisco ISE 管理者グループのロールおよび役割」を参照してください。

.csv インポート ファイルを作成したら、次の手順を実行します。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2　左側の [ネットワーク デバイス（Network Devices）] ナビゲーション ペインで、[ネットワーク デバイス（Network Devices）] をクリックします。

[ネットワーク デバイス（Network Devices）] ページが表示されます。

ステップ 3　[インポート（Import）] をクリックします。

[インポート（Import）] ページが表示されます。

ステップ 4　[参照（Browse）] をクリックして、クライアント ブラウザを実行しているシステムから .csv ファイルを選択します。

ステップ 5　次のオプションをオンまたはオフにします。

a. [既存のデータを新しいデータで上書き（Overwrite Existing Data with New Data）] : ISE で既存のネットワーク デバイスをインポート ファイル内のデバイスに置き換える場合は、このチェックボックスをオンにします。このチェックボックスをオンにしない場合、インポート ファイル内の新しいネットワーク デバイス定義がネットワーク デバイス リポジトリに追加されます。重複するエントリは無視されます。

b. [最初のエラー時にインポートを停止（Stop Import on First Error）] : インポート プロセスでエラーが発生したときに ISE でインポート プロセスを中止する場合は、このチェックボックスをオンにします。そのときまでに処理されたレコードがインポートされます。このチェックボックスがオフになっているときにエラーが発生した場合、エラーが報告されますが、ISE はインポート プロセスを続行します。

ステップ 6　[インポート（Import）] をクリックします。

[インポートの進行状況（Import Progress）] ページが表示され、インポート プロセスのステータスが示されます。インポートされたデバイスの数の概要とインポート プロセス中に見つかったエラーが報告されます。

ステップ 7　ナビゲーション ペインの [ネットワーク デバイス（Network Devices）] またはこのページの上部にある [ネットワーク デバイス リスト（Network Devices List）] リンクをクリックして、インポートされたデバイスを表示します。

結果：
インポート プロセスが正常に完了すると、ダイアログボックスに「インポートが完了しました（Import Completed）」というメッセージが表示されます。

ISE へのネットワーク デバイス グループのインポート

前提条件：
各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはネットワーク デバイス管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、「Cisco ISE 管理者グループのロールおよび役割」を参照してください。

NDG をインポートするには、次の手順を実行します。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] を選択します。

ステップ 2　左側のナビゲーション ペインで、[グループ タイプ（Group Types）] をクリックします。

[ネットワーク デバイス グループ（Network Device Groups）] ページが表示されます。

ステップ 3　[インポート（Import）] をクリックします。[操作（Action）] アイコンをクリックし、ナビゲーション ペインから [インポート（Import）] を選択することもできます。

[インポート（Import）] ページが表示されます。

ステップ 4　[テンプレートの生成（Generate a Template）] をクリックして、インポート ファイルを作成するためのテンプレートをダウンロードできます。

ステップ 5　テンプレートをローカル ハード ディスクに保存します。

ステップ 6　Microsoft Excel または任意のスプレッドシート アプリケーションでこのテンプレートを開きます。

CSV テンプレートの最初の行はヘッダーで、ファイル内のフィールドの形式を定義します。このヘッダーは、編集しないでそのまま使用してください。

ステップ 7　図 6-2 に示されているように詳細を入力します。

図 6-2　NDG インポート ファイル

	A	B	C	D	E	F	G	H
1	Name	Description	Type	Is Root				
2	Location#All Locations	All Locations	Location	TRUE				
3	Device Type#All Device Types	All Device Types	Device Type	TRUE				
4	Location#All Locations#WORLD		Location	FALSE				
5	Location#All Locations#ASIA		Location	FALSE				
6	DeviceGroup1#DeviceGroup1	THIS IS DEVICEGROUP 1	DeviceGroup1	TRUE				
7	DeviceGroup2#DeviceGroup2	THIS IS DEVICEGROUP 2	DeviceGroup2	TRUE				
8	DeviceGroup3#DeviceGroup3	THIS IS DEVICEGROUP 3	DeviceGroup3	TRUE				
9	DeviceGroup4#DeviceGroup4	THIS IS DEVICEGROUP 4	DeviceGroup4	TRUE				
10	DeviceGroup5#DeviceGroup5	THIS IS DEVICEGROUP 5	DeviceGroup5	TRUE				
11	DeviceGroup6#DeviceGroup6	THIS IS DEVICEGROUP 6	DeviceGroup6	TRUE				
12	DeviceGroup7#DeviceGroup7	THIS IS DEVICEGROUP 7	DeviceGroup7	TRUE				
13	DeviceGroup8#DeviceGroup8	THIS IS DEVICEGROUP 8	DeviceGroup8	TRUE				
14	DeviceGroup9#DeviceGroup9	THIS IS DEVICEGROUP 9	DeviceGroup9	TRUE				
15	DeviceGroup10#DeviceGroup10	THIS IS DEVICEGROUP 10	DeviceGroup10	TRUE				
16	DeviceGroup11#DeviceGroup11	THIS IS DEVICEGROUP 11	DeviceGroup11	TRUE				
17	DeviceGroup12#DeviceGroup12	THIS IS DEVICEGROUP 12	DeviceGroup12	TRUE				
18	DeviceGroup13#DeviceGroup13	THIS IS DEVICEGROUP 13	DeviceGroup13	TRUE				
19	DeviceGroup14#DeviceGroup14	THIS IS DEVICEGROUP 14	DeviceGroup14	TRUE				
20	DeviceGroup15#DeviceGroup15	THIS IS DEVICEGROUP 15	DeviceGroup15	TRUE				
21	DeviceGroup16#DeviceGroup16	THIS IS DEVICEGROUP 16	DeviceGroup16	TRUE				
22	DeviceGroup17#DeviceGroup17	THIS IS DEVICEGROUP 17	DeviceGroup17	TRUE				
23	DeviceGroup18#DeviceGroup18	THIS IS DEVICEGROUP 18	DeviceGroup18	TRUE				
24	DeviceGroup19#DeviceGroup19	THIS IS DEVICEGROUP 19	DeviceGroup19	TRUE				
25	DeviceGroup20#DeviceGroup20	THIS IS DEVICEGROUP 20	DeviceGroup20	TRUE				

239651

ステップ 8　インポート ファイルをローカル ハード ディスクに保存します。

ステップ 9　[インポート（Import）] ページの [参照（Browse）] をクリックして、インポート ファイルを選択します。

ステップ 10　次のオプションをオンまたはオフにします。

a.　[既存のデータを新しいデータで上書き（Overwrite Existing Data with New Data）] : ISE で既存のネットワーク デバイス グループをインポート ファイル内のデバイス グループに置き換える場合は、このチェックボックスをオンにします。このチェックボックスをオンにしない場合、インポート ファイル内の新しいネットワーク デバイス グループ定義がネットワーク デバイス グループ リポジトリに追加されます。重複するエントリは無視されます。

b.　[最初のエラー時にインポートを停止（Stop Import on First Error）] : インポート プロセスでエラーが発生したときに ISE でインポート プロセスを中止する場合は、このチェックボックスをオンにします。そのときまでに処理されたレコードがインポートされます。このチェックボックスがオフになっているときにエラーが発生した場合、エラーが報告されますが、ISE はインポート プロセスを続行します。

ステップ 11　[インポート（Import）] をクリックします。

ページにインポートの進行状況が表示され、インポート プロセスの終了時に結果が表示されます。

ネットワーク デバイス グループの CSV テンプレートにおけるフィールドの説明

表 6-6　ネットワーク デバイス グループの CSV テンプレートのフィールド

フィールド	説明
Name:String(100):Required	（必須）このフィールドはネットワーク デバイス グループの名前です。最大 100 文字の文字列です。NDG のフルネームは最大 100 文字です。たとえば、親グループ [Global] > [Asia] の下にサブグループ India を作成する場合、作成する NDG のフルネームは Global#Asia#India となり、このフルネームが 100 文字を超えてはなりません。NDG のフルネームが 100 文字を超える場合は、NDG の作成に失敗します。
Description:String(1024)	これは、オプションのネットワーク デバイス グループの説明です。最大 1024 文字の文字列です。
Type:String(64):Required	（必須）このフィールドはネットワーク デバイス グループのタイプです。最大 64 文字の文字列です。
Is Root:Boolean(true|false):Required	（必須）これは、特定のネットワーク デバイス グループがルート グループかどうかを示すフィールドです。有効な値は true または false です。

関連項目

- 「ネットワーク デバイスとネットワーク デバイス グループのインポート」（P.6-15）
- 「CSV インポート ファイルの作成」（P.6-16）

ネットワーク デバイスとネットワーク デバイス グループのエクスポート

Cisco ISE に設定されている一連のネットワーク デバイスとネットワーク デバイス グループを .csv ファイルの形式でエクスポートし、別の ISE ノードにインポートできます。

この項では、次のトピックを扱います。

- 「ネットワーク デバイスのエクスポート」（P.6-22）
- 「ネットワーク デバイス グループのエクスポート」（P.6-23）

ネットワーク デバイスのエクスポート

前提条件：

各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはネットワーク デバイス管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、「Cisco ISE 管理者グループのロールおよび役割」を参照してください。

ネットワーク デバイス設定をエクスポートするには、次の手順を実行します。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2　左側の [ネットワーク デバイス（Network Devices）] ナビゲーション ペインで、[ネットワーク デバイス（Network Devices）] をクリックします。

[ネットワーク デバイス（Network Devices）] ページが表示され、デバイス設定のリストが示されます。

ステップ 3　エクスポートするデバイスの隣にあるチェックボックスをオンにし、[エクスポート（Export）] > [選択済みをエクスポート（Export Selected）] を選択します。

（注）　定義されているすべてのネットワーク デバイスをエクスポートするには、[エクスポート（Export）] > [すべてエクスポート（Export All）] を選択します。

ステップ 4　export.csv ファイルをローカル ハード ディスクに保存します。

結果：

ネットワーク デバイス設定が別の ISE ノードにインポートできる .csv ファイルの形式で作成されます。

ネットワーク デバイス グループのエクスポート

前提条件：

各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、スーパー管理者またはネットワーク デバイス管理者のいずれかのロールを割り当てられている必要があります。さまざまな管理ロールの詳細と、各ロールに関連付けられている権限については、「Cisco ISE 管理者グループのロールおよび役割」を参照してください。

ネットワーク デバイス グループをエクスポートするには、次の手順を実行します。

ステップ 1　[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）] を選択します。

ステップ 2　左側のナビゲーション ペインで、[グループ タイプ（Group Types）] をクリックします。

[ネットワーク デバイス グループ（Network Device Groups）] ページが表示されます。

ステップ 3　[エクスポート（Export）] をクリックします。[操作（Action）] アイコンをクリックし、ナビゲーション ペインから [エクスポート（Export）] を選択することもできます。

ステップ 4　export.csv ファイルをローカル ハード ディスクに保存します。

ISE ノードからネットワーク デバイス グループ設定がエクスポートされ、別の ISE ノードにインポートできるようになりました。