# 管理のユーザ インターフェイスのリファレンス



# 展開とノードの設定

[展開ノード（Deployment Nodes）] ページを使用すると、Cisco ISE（管理、ポリシー サービス、およびモニタリング）ノードを設定し、展開を設定することができます。

## 展開ノードリストウィンドウ

次の表に、展開内の Cisco ISE ノードを設定するために使用できる [展開のノードリスト（Deployment Nodes List）] ページのフィールドを示します。このページへのナビゲーションパスは、**[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** です。

| フィールド名 | 使用上のガイドライン |
|---|---|
| **ホスト名（Hostname）** | ノードのホスト名を表示します。 |
| **ノード タイプ（Node Type）** | ノード タイプを表示します。次のいずれかを設定できます。<br>• Cisco ISE（管理、ポリシー サービス、およびモニタリング）ノード |

| フィールド名 | 使用上のガイドライン |
|---|---|
| ペルソナ（**Personas**） | （ノード タイプが Cisco ISE の場合にのみ表示）Cisco ISE ノードが担当してきたペルソナがリストされます。[管理（Administration）]、[ポリシー サービス（Policy Service）] などがあります。 |
| ロール（**Role**） | このノードで管理ペルソナまたはモニタリング ペルソナが有効になっている場合、これらのペルソナが担当しているロール（プライマリ、セカンダリ、またはスタンドアロン）が示されます。ロールは、次のうちの 1 つまたは複数にできます。<br>• [PRI（A）] : プライマリ PAN を意味します<br>• [SEC（A）] : セカンダリ PAN を意味します<br>• [PRI（M）] : プライマリ モニタリング ノードを意味します<br>• [SEC（M）] : セカンダリ モニタリング ノードを意味します |
| **Services** | （ポリシー サービス ペルソナが有効な場合にのみ表示）この Cisco ISE ノードで実行されているサービスがリストされます。サービスは次のいずれか 1 つとなります。<br>• セッション（Session）<br>• プロファイリング<br>• すべて（All） |

| フィールド名 | 使用上のガイドライン |
|---|---|
| ノード ステータス（**Node Status**） | データ レプリケーション用の展開内の各 ISE ノードのステータスを示します。<br>• [緑（接続）（Green（Connected））]：すでに展開に登録されている ISE ノードがプライマリ PAN と同期していることを示します。<br>• [赤（切断）（Red（Disconnected））]：ISE ノードに到達できないか、ISE ノードがダウンしているか、またはデータレプリケーションが行われていないことを示します。<br>• [オレンジ（進行中）（Orange（In Progress））]：ISE ノードがプライマリ PAN に新規に登録されているか、手動同期操作を実行したか、または ISE ノードがプライマリ PAN と同期していないことを示します。<br>詳細については、[ノード ステータス（Node Status）] カラムで各 ISE ノードのクイック ビュー アイコンをクリックします。 |

**関連トピック**

Cisco ISE 分散展開
Cisco ISE デプロイメントの用語
Cisco ISE ノードの設定
セカンダリ Cisco ISE ノードの登録

# ノードの一般設定

次の表で、Cisco ISE ノードの [全般設定 (General Settings)] ウィンドウのフィールドについて説明します。このウィンドウでは、ペルソナをノードに割り当て、そのサービスを実行するように設定できます。このタブのナビゲーションパスは、**[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** > **[展開ノード（Deployment Node）]** > **[編集（Edit）]** > **[全般設定（General Settings）]** です。

**表 *1:* ノードの一般設定**

| フィールド名 | 使用上のガイドライン |
|---|---|
| ホスト名（**Hostname**） | Cisco ISE ノードのホスト名を表示します。 |

| フィールド名 | 使用上のガイドライン |
|---|---|
| **FQDN** | Cisco ISE ノードの完全修飾ドメイン名を表示します。たとえば、ise1.cisco.com などです。 |
| **IP アドレス** | Cisco ISE ノードの IP アドレスを表示します。 |
| ノード タイプ（**Node Type**） | ノード タイプを表示します。 |
| ペルソナ（**Personas**） | |
| 管理（**Administration**） | Cisco ISE ノードに管理ペルソナを担当させる場合は、このチェックボックスをオンにします。管理ペルソナは、管理サービスを提供するようライセンスされているノードでのみ有効にできます。<br><br>ロール（Role）：管理ペルソナが展開で担当しているロールを表示します。[スタンドアロン（Standalone）]、[プライマリ（Primary）]、[セカンダリ（Secondary）] のいずれかの値になります。<br><br>プライマリにする（Make Primary）：ノードをプライマリ Cisco ISE ノードにする場合にこのボタンをクリックします。展開では 1 つのプライマリ Cisco ISE ノードのみを使用できます。このページのその他のオプションは、ノードをプライマリにした後にのみアクティブになります。展開では 2 つの管理ノードのみを使用できます。ノードにスタンドアロン ロールが割り当てられている場合、[プライマリにする（Make Primary）] ボタンがノードの横に表示されます。ノードにセカンダリ ロールが割り当てられている場合、[プライマリに昇格（Promote to Primary）] ボタンがノードの横に表示されます。ノードにプライマリ ロールがあり、そのノードを使用して登録されている他のノードがない場合は、ノードの横に [スタンドアロンにする（Make Standalone）] ボタンが表示されます。このボタンをクリックすると、プライマリ ノードをスタンドアロン ノードにすることができます。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| モニタリング | |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| | Cisco ISE ノードにモニタリング ペルソナを担当させ、ログ コレクタとして機能させる場合は、このチェックボックスをオンにします。分散展開内にモニタリング ノードが少なくとも 1 つ存在する必要があります。プライマリ PAN の設定時に、モニタリング ペルソナを有効にする必要があります。展開内のセカンダリ モニタリング ノードを登録した後、必要に応じてプライマリ PAN を編集したり、モニタリング ペルソナを無効にしたりできます。<br>VMware プラットフォームで Cisco ISE ノードをログ コレクタとして設定するには、次のガイドラインに従って最低限必要なディスク領域を決定します。1 日あたりネットワーク内のエンドポイント 1 つにつき 180 KB、1 日あたりネットワーク内の Cisco ISE ノード 1 つにつき 2.5 MB となります。<br><br>モニタリング ノードに何ヵ月分のデータを格納するかに応じて、必要な最大ディスク領域を計算します。展開にモニタリング ノードが 1 つしかない場合は、スタンドアロン ロールを担当します。展開に2つのモニタリング ノードがある場合は、Cisco ISE に、プライマリ-セカンダリ ロールを設定する他のモニタリング ノードの名前が表示されます。これらのロールを設定するには、次のいずれかを選択します。<br>• プライマリ（Primary）：現在のノードをプライマリ モニタリング ノードにする場合。<br>• セカンダリ（Secondary）：現在のノードをセカンダリ モニタリング ノードにする場合。<br>• なし（None）：モニタリングノードにプライマリ/セカンダリ ロールを担当させない場合。<br><br>モニタリング ノードの 1 つをプライマリまたはセカンダリとして設定すると、もう一方のモニタリング ノードが自動的にそれぞれセカンダリ ノードまたはプライマリ ノードになります。プライマリ モニタリング ノードおよび |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| | セカンダリ モニタリング ノードは、管理ログおよびポリシー サービス ログを受信します。1 つのモニタリングノードのロールを [なし（None）]に変更した場合、他方のモニタリングノードのロールも同様に [なし（None）] になり、それによって高可用性ペアがキャンセルされます。モニタリングノードとしてノードを指定すると、そのノードが **[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[リモートロギング ターゲット（Remote Logging Targets）]** ウィンドウで syslog ターゲットとして表示されます。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| ポリシー サービス（**Policy Service**） | |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| | 次のサービスの 1 つまたはすべてを有効にするには、このチェックボックスをオンにします。<br>• [セッションサービスの有効化（Enable Session Services）]：ネットワーク アクセス サービス、ポスチャサービス、ゲスト サービス、およびクライアント プロビジョニング サービスを有効にするには、このチェックボックスをオンにします。このポリシー サービス ノードが属するグループを、[ノードをノード グループに含める（Include Node in Node Group）] ドロップダウン リストから選択します。CA サービスと EST サービスは、セッション サービスが有効になっているポリシーサービスノードでのみ実行できることに注意してください。<br>[ノードをノードグループに含める（Include Node in Node Group）] については、このポリシーサービスモードをどのグループにも含めない場合は [なし（None）] を選択します。<br>同じノード グループ内のすべてのノードが、ネットワーク アクセス デバイス（NAD）で RADIUS クライアントとして設定され、CoA の許可を得る必要があります。これは、それらすべてのノードで、ノード グループ内の任意のノードを介して確立されたセッションに関する CoA 要求を発行できるためです。ロード バランサを使用していない場合、ノード グループ内のノードは、NAD で設定されている RADIUS サーバおよびクライアントと同じであるか、またはこれらのサブセットである必要があります。これらのノードは RADIUS サーバとしても設定できます。<br>多数の ISE ノード（RADIUS サーバおよび動的許可クライアントとして）を持つ単一の NAD を設定できますが、すべてのノードが同じノード グループに属している必要はありません。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| | ノード グループのメンバーは、ギガビット イーサネットなどの高速 LAN 接続を使用して相互に接続する必要があります。ノード グループのメンバーは L2 隣接関係である必要はありませんが、十分な帯域幅と到達可能性を確保するにはL2 隣接関係が強く推奨されます。詳細については、『』の「ポリシー サービス ノード グループの作成」のセクションポリシー サービス ノード グループの作成を参照してください。<br>• プロファイリング サービスの有効化（Enable Profiling Service）：プロファイラ サービスを有効にするには、このチェックボックスをオンにします。プロファイリング サービスを有効にする場合は、[Profiling Configuration（プロファイリング設定）] タブをクリックし、必要に応じて詳細を入力する必要があります。ポリシー サービス ノードで実行されるサービスを有効または無効にしたり、このノードを変更したりする場合は、そのサービスが実行されるアプリケーション サーバ プロセスを再起動します。これらのサービスが再起動されるまで遅延が発生します。ノードでアプリケーション サーバがいつ再起動したかを確認するには、CLI で show application status ise コマンドを使用します。<br>• 脅威中心型NACサービスの有効化（Enable Threat Centric NAC Service）：脅威中心型ネットワーク アクセス コントロール（TC-NAC）機能を有効にするには、このチェックボックスをオンにします。この機能では、脅威と脆弱性のアダプタから受信した脅威と脆弱性の属性に基づいて認証ポリシーを作成することができます。脅威の重大度レベルと脆弱性評価の結果は、エンドポイントまたはユーザのアクセス レベルを動的に制御するために使用できます。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| | • SXPサービスの有効化（Enable SXP Service）：ノードで SXP サービスを有効にするには、このチェックボックスをオンにします。また、SXP サービスに使用するインターフェイスを指定する必要があります。<br><br>NIC ボンディングまたはチーミングを設定している場合は、ボンディングされたインターフェイスも物理インターフェイスとともに [使用インターフェイス（Use Interface）] ドロップダウン リストに表示されます。<br><br>• デバイス管理サービスの有効化（Enable Device Admin Service）：TACACS ポリシーセット、ポリシー結果などを作成し、ネットワークデバイスの設定を制御および監査するには、このチェックボックスをオンにします。<br><br>• パッシブIDサービスの有効化（Enable Passive Identity Service）：ID マッピング機能を有効にするには、このチェックボックスをオンにします。この機能を使用すると、Cisco ISE ではなくドメイン コントローラ（DC）で認証されるユーザをモニタすることができます。Cisco ISE がユーザのネットワーク アクセスをアクティブには認証しないネットワークでは、ID マッピング機能を使用して、Active Directory（AD）ドメイン コントローラからユーザ認証情報を収集することができます。 |

| フィールド名 | 使用上のガイドライン |
|---|---|
| **pxGrid** | pxGridペルソナを有効にするには、このチェック ボックスをオンにします。Cisco pxGridは、Cisco ISE セッション ディレクトリからCisco Adaptive Security Appliance（ASA）などの他のポリシー ネットワーク システムへコンテキスト依存情報を共有するために使用されます。pxGrid フレームワークは、ポリシー データや設定データをノード間で交換するためにも使用できます（たとえば、ISEとサードパーティ ベンダー間でのタグやポリシー オブジェクトの共有）。また、脅威情報など、非 ISE 関連情報の交換用にも使用できます。 |

**関連トピック**

分散 Cisco ISE 展開のペルソナ
管理ノード
ポリシー サービス ノード
モニタリング ノード
pxGrid ノード
プライマリおよびセカンダリの Cisco ISE ノードの同期
ポリシー サービス ノード グループの作成
ISE pxGrid ノードの展開
ノード ペルソナとサービスの変更
自動フェールオーバー用のモニタリング ノードの設定

# プロファイリング ノードの設定

次の表では、プロファイラ サービスのプローブの設定に使用できる [プロファイリング設定（Profiling Configuration）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [ISE ノード（ISE Node）] > [編集（Edit）] > [プロファイリング設定（Profiling Configuration）]** です。

表 *2:* プロファイリング ノードの設定

| フィールド名 | 使用上のガイドライン |
|---|---|
| **NetFlow** | ルータから送信された NetFlow パケットを受信および解析するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとに NetFlow を有効にする場合は、このチェックボックスをオンにします。次のオプションを選択します。<br>• [インターフェイス（Interface）]：ISE ノード上のインターフェイスを選択します。<br>• [ポート（Port）]：NetFlow エクスポートがルータから受信した NetFlow リスナー ポート番号を入力します。デフォルト ポートは 9996 です。 |
| **DHCP** | IP ヘルパーから DHCP パケットをリッスンするために、ポリシーサービスペルソナを担当した Cisco ISE ノードごとに DHCP を有効にする場合は、このチェックボックスをオンにします。次のオプションを選択します。<br>• [ポート（Port）]：DHCP サーバの UDP ポート番号を入力します。デフォルト ポートは 67 です。<br>• [インターフェイス（Interface）]：ISE ノード上のインターフェイスを選択します。<br>• [ポート（Port）]：DHCP サーバの UDP ポート番号を入力します。デフォルト ポートは 67 です。 |
| **DHCP SPAN** | DHCP パケットを収集するために、ポリシー サービス ペルソナを担当した Cisco ISE ノードごとに DHCP SPAN を有効にする場合は、このチェックボックスをオンにします。<br>• [インターフェイス（Interface）]：ISE ノード上のインターフェイスを選択します。 |

| フィールド名 | 使用上のガイドライン |
|---|---|
| **HTTP** | HTTPパケットを受信および解析するために、ポリシー サービス ペルソナを担当したCisco ISEノードごとにHTTPを有効にする場合は、このチェックボックスをオンにします。<br>• [インターフェイス（Interface）]：ISEノード上のインターフェイスを選択します。 |
| 『**RADIUS**』 | IOSセンサー対応デバイスからRADIUSセッション属性、さらにCDP属性とLLDP属性を収集するために、ポリシーサービスペルソナを担当したISEノードごとにRADIUSを有効にする場合は、このチェックボックスをオンにします。 |
| **ネットワーク スキャン（NMAP）（Network Scan (NMAP)）** | NMAPプローブをイネーブルにするには、このボックスをオンにします。 |
| **DNS** | FQDNのDNSルックアップを実行するために、ポリシー サービス ペルソナを担当したISEノードごとにDNSを有効にする場合は、このチェックボックスをオンにします。秒単位でタイムアウト時間を入力します。<br>（注） DNSプローブを分散展開内の特定のCisco ISEノードで動作させるには、DHCP、DHCP SPAN、HTTP、RADIUS、SNMPのいずれかのプローブを有効にする必要があります。DNSルックアップの場合、上記のいずれかのプローブをDNSプローブとともに起動する必要があります。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| **SNMP クエリ（SNMP Query）** | 指定した間隔でネットワーク デバイスをポーリングするために、ポリシー サービス ペルソナを担当したISE ノードごとにSNMP クエリーを有効にする場合は、このチェックボックスをオンにします。[再試行（Retries）]、[タイムアウト（Timeout）]、[イベント タイムアウト（Event Timeout）]、任意の [説明（Description）] の各フィールドに値を入力します。<br>（注） SNMP クエリー プローブの設定に加えて、[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）] の場所にある他のSNMP設定も行う必要があります。ネットワーク デバイスで SNMP 設定を行う場合は、ネットワーク デバイスでシスコ デバイス プロトコル（CDP）およびLink Layer Discovery Protocol（LLDP）をグローバルに有効にしていることを確認します。 |

| フィールド名 | 使用上のガイドライン |
|---|---|
| **SNMP トラップ（SNMP Trap）** | ネットワーク デバイスから linkUp、linkDown、MAC 通知トラップを受信するために、ポリシー サービス ペルソナを担当した ISE ノードごとに SNMP トラップ プローブを有効にする場合は、このチェックボックスをオンにします。次のいずれかを選択します。<br>• [リンク トラップ クエリ（Link Trap Query）]：SNMP トラップを介して受信する linkup 通知と linkdown 通知を受信して解釈するには、このチェックボックスをオンにします。<br>• [MAC トラップ クエリ（MAC Trap Query）]：SNMP トラップを介して受信する MAC 通知を受信して解釈するには、このチェックボックスをオンにします。<br>• [インターフェイス（Interface）]：ISE ノードのインターフェイスを選択します。<br>• [ポート（Port）]：使用するホストの UDP ポートを入力します。デフォルト ポートは 162 です。 |
| **Active Directory** | 定義された Active Directory サーバをスキャンして、Windows ユーザに関する情報を探します。 |
| **pxGrid** | ISE で pxGrid を介してエンドポイント属性を収集（プロファイリング）できるようになります。 |

**関連トピック**

Cisco ISE プロファイリング サービス
プロファイリング サービスによって使用されるネットワーク プローブ
Cisco ISE ノードでのプロファイリング サービスの設定

# 証明書ストアの設定

[証明書ストア（Certificate Store）] ページでは、認証に使用できる証明書を Cisco ISE で設定することができます。

# 自己署名証明書の設定

次の表では、[自己署名証明書の生成（Generate Self Signed Certificate）] ページのフィールドについて説明します。このページでは、ノード間通信、EAP-TLS 認証、Cisco ISE Web ポータル、および pxGrid コントローラとの通信用のシステム証明書を作成できます。このページのナビゲーションパスは、**[管理（Administration）]**>**[システム（System）]**>**[証明書（Certificates）]**> **[システム証明書（System Certificates）]** > **[自己署名証明書の生成（Generate Self Signed Certificate）]** です。

**表 *3 :* 自己署名証明書の設定**

| フィールド名 | 使用上のガイドライン |
|---|---|
| **ノードの選択（Select Node）** | （必須）システム証明書を生成するノード。 |
| **Common Name（CN）** | （SAN を指定しない場合に必須）デフォルトでは、一般名は自己署名証明書を生成する ISE ノードの完全修飾ドメイン名です。 |
| **Organizational Unit（OU）** | 組織ユニット名。Engineering など。 |
| **組織（Organization）（O）** | 組織名。Cisco など。 |
| **都市（City）（L）** | （省略不可）都市名。San Jose など。 |
| **州（State）（ST）** | （省略不可）州名。California など。 |
| **Country（C）** | 国名。2 文字の ISO 国番号を入力する必要があります。US など。 |
| **サブジェクト代替名（Subject Alternative Name）（SAN）** | 証明書に関連付けられた IP アドレス、DNS 名、または Uniform Resource Identifier（URI）。 |
| **キー タイプ** | RSA または ECDSA の公開キーの作成に使用するアルゴリズムを指定します。 |

| フィールド名 | 使用上のガイドライン |
|---|---|
| キーの長さ（**Key Length**） | 公開キーのビット サイズを指定します。RSA には、次のオプションを使用できます。<br>• 512<br>• 1024<br>• 2048<br>• 4096<br><br>ECDSA には、次のオプションを使用できます。<br>• 256<br>• 384<br><br>（注） RSA および ECDSA の公開キーは、同じセキュリティ レベルで異なるキー長を持つことがあります。<br><br>パブリック CA 署名付き証明書を取得する場合、または FIPS 準拠ポリシー管理システムとして Cisco ISE を展開する場合は、2048 を選択します。 |
| 署名するダイジェスト（**Digest to Sign With**） | ハッシュ アルゴリズム SHA-1 または SHA-256 を選択します。 |
| 証明書ポリシー（**Certificate Policies**） | 証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。 |
| TTL 有効期限（**Expiration TTL**） | 証明書が失効するまでの日数を指定します。 |
| フレンドリ名（**Friendly Name**） | 証明書のフレンドリ名を入力します。名前を指定しない場合は、<common name> # <issuer> # <nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。 |
| ワイルドカード証明書の許可（**Allow Wildcard Certificates**） | 自己署名したワイルドカード証明書（サブジェクトの任意の一般名またはサブジェクト代替名の DNS 名、またはその両方にアスタリスク（*）が含まれている証明書）を生成する場合は、このチェックボックスをオンにします。たとえば、SAN に割り当てられている DNS 名が *.amer.cisco.com の場合です。 |

| フィールド名 | 使用上のガイドライン |
| --- | --- |
| **Usage** | このシステム証明書を使用する必要があるサービスを選択します。<br>• [管理者（Admin）]：管理者ポータルとの通信および展開内の ISE ノード間の通信の保護に使用されるサーバ証明書<br>• [EAP 認証（EAP Authentication）]：SSL/TLS トンネリングの EAP プロトコルを使用する認証に使用されるサーバ証明書<br>• [RADIUS DTLS]：RADIUS DTLS 認証に使用するサーバ証明書<br>• [pxGrid]：pxGrid クライアントとサーバの間の通信を保護するクライアントおよびサーバ証明書<br>• [SAML]：SAML ID プロバイダー（IdP）とのセキュア通信に使用するサーバ証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。<br>• [ポータル（Portal）]：すべての Cisco ISE Web ポータルとの通信を保護するために使用されるサーバ証明書 |

**関連トピック**

システム証明書
システム証明書の表示
自己署名証明書の生成

# 証明書署名要求の設定

Cisco ISE では、1 つの要求で、管理者ポータルから展開内のすべてのノードの CSR を生成することができます。また、展開内の単一ノードまたは複数両方のノードのどちらの CSR を生成するのか選択することもできます。単一ノードの CSR を生成する場合、ISE は証明書サブジェクトの [CN=] フィールドの特定ノードの完全修飾ドメイン名（FQDN）を自動的に置き換えます。証明書の [サブジェクト代替名（Subject Alternative Name (SAN)）] フィールドにエントリを含めることを選択した場合、他の SAN 属性に加えて ISE ノードの FQDN を入力する必要があります。展開内のすべてのノードの CSR を生成することを選択した場合は、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] チェックボックスをオンにして、[SAN] フィールド（DNS 名）にワイルドカード表記で FQDN を入力します（*.amer.example.com など）。EAP 認証に証明書を使用する場合は、[CN=] フィールドにワイルドカード値を入力しないでください。

ワイルドカード証明書を使用することにより、各 Cisco ISE ノードに固有の証明書を生成する必要がなくなります。また、証明書の警告を防ぐために、SAN フィールドに複数の FQDN 値を入力する必要もありません。SAN フィールドでアスタリスク（*）を使用すると、展開内の複数の両方のノードで単一の証明書を共有できるようになり、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書は、各 Cisco ISE ノードに固有のサーバ証明書を割り当てる場合よりも安全性が低いと見なされます。

次の表に、認証局（CA）が署名可能な証明書署名要求（CSR）の生成に使用できる [証明書署名要求（Certificate Signing Request）] ページのフィールドを示します。このページのナビゲーション パスは **[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書管理（Certificate Management）]** > **[証明書署名要求（Certificate Signing Request）]** です。

表 *4 :* 証明書署名要求の設定

| フィールド | 使用上のガイドライン |
| --- | --- |
| 証明書の用途（**Certificate(s) will be used for**） | |

| フィールド | 使用上のガイドライン |
| --- | --- |
| | 証明書を使用するサービスを選択します。<br>**Cisco ISE ID 証明書**<br>• [複数使用（Multi-Use）]：複数のサービス（管理者、EAP-TLS認証、pxGrid、およびポータル）に使用されます。複数使用の証明書は、クライアントとサーバ両方のキーの用途を使用します。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。<br>• [キーの用途（Key Usage）]：デジタル署名（署名）<br>• [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2）<br>• [管理者（Admin）]：サーバ認証に使用されます（管理者ポータルとの通信および展開内の ISE ノード間の通信を保護するため）。署名 CA の証明書テンプレートは、Webサーバ証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。<br>• [キーの用途（Key Usage）]：デジタル署名（署名）<br>• [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）<br>• [EAP 認証（EAP Authentication）]：サーバ認証に使用されます。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。<br>• [キーの用途（Key Usage）]：デジタル署名（署名）<br>• [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）<br>（注） EAP-TLS クライアント証明書にデジタル署名キー使用法を使用する必要があります。<br>• [RADIUS DTLS]：RADIUS DTLS サーバの認証に使用されます。このテンプレートには、次のプロパティがあります。<br>• [キーの用途（Key Usage）]：デジタル署名（署名）<br>• [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）<br>• [ポータル（Portal）]：サーバ認証に使用されます（すべての ISE Web |

| フィールド | 使用上のガイドライン |
| --- | --- |
| | ポータルとの通信を保護するため）。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。<br>• [キーの用途（Key Usage）]：デジタル署名（署名）<br>• [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）<br>• [pxGrid]：クライアント認証とサーバ認証の両方に使用されます（pxGrid クライアントとサーバ間の通信を保護するため）。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。<br>• [キーの用途（Key Usage）]：デジタル署名（署名）<br>• [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2）<br>• [SAML]：SAML ID プロバイダー（IdP）とのセキュア通信に使用するサーバ証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。<br>• [キーの用途（Key Usage）]：デジタル署名（署名）<br>• [キーの拡張用途（Extended Key Usage）]：TLS Web サーバ認証（1.3.6.1.5.5.7.3.1）<br>（注） 拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用しないことをお勧めします。拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用する場合、証明書は無効と見なされ、次のエラー メッセージが表示されます。<br>`source=local ; type=fatal ; message="unsupported certificate"`<br>**Cisco ISE 認証局証明書** |

| フィールド | 使用上のガイドライン |
|---|---|
| | • [ISE ルート CA（ISE Root CA）]：（内部 CA サービスにのみ適用可能）プライマリ PAN のルート CA および PSN の下位 CA を含む内部 CA 証明書チェーン全体を再生成するために使用されます。<br>• [ISE 中間 CA（ISE Intermediate）]：（ISE が外部 PKI の中間 CA として機能する場合に内部 CA サービスにのみ適用可能）プライマリ PAN の中間 CA 証明書および PSN の下位 CA 証明書の生成に使用されます。署名 CA の証明書テンプレートは、下位認証局と呼ばれます。このテンプレートには、次のプロパティがあります。<br>• [基本制約（Basic Constraints）]：重要、認証局<br>• [キーの用途（Key Usage）]：証明書の署名、デジタル署名<br>• [キーの拡張用途（Extended Key Usage）]：OCSP 署名（1.3.6.1.5.5.7.3.9）<br>• [ISE OCSP 応答側証明書の更新（Renew ISE OCSP Responder Certificates）]：（内部 CA サービスにのみ適用可能）展開全体の ISE OCSP 応答側証明書の更新に使用されます（証明書署名要求ではありません）。セキュリティ上の理由から、ISE OCSP 応答側証明書を 6 ヵ月ごとに更新することを推奨します。 |
| **ワイルドカード証明書の許可（Allow Wildcard Certificates）** | 証明書の [SAN] フィールドの CN/DNS 名にワイルドカード文字（*）を使用するには、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すると、展開内のすべてのノードが自動的に選択されます。左端のラベルの位置にアスタリスク（*）ワイルドカード文字を使用する必要があります。ワイルドカード証明書を使用する場合は、セキュリティを強化するためにドメイン領域を分割することを推奨します。たとえば、*.example.com の代わりに *.amer.example.com を使用して領域を分割することができます。ドメインを分割しないと、セキュリティ問題が発生する可能性があります。 |
| **これらのノードの CSR の生成（Generate CSRs for these Nodes）** | 証明書を生成するノードの隣のチェックボックスをオンにします。展開内の選択されたノードの CSR を生成するには、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオフにします。 |
| **Common Name（CN）** | デフォルトでは、一般名は CSR を生成する ISE ノードの FQDN です。$FQDN$ は ISE ノードの FQDN を意味します。展開内の複数ノードの CSR を生成すると、CSR の [一般名（Common Name）] フィールドは各 ISE ノードの FQDN に置き換えられます。 |
| **Organizational Unit（OU）** | 組織ユニット名。Engineering など。 |
| **Organization（O）** | 組織名。Cisco など。 |

| フィールド | 使用上のガイドライン |
|---|---|
| **都市（City）（L）** | （省略不可）都市名。San Jose など。 |
| **州（State）（ST）** | （省略不可）州名。California など。 |
| **Country（C）** | 国名。2 文字の ISO 国番号を入力する必要があります。US など。 |
| **サブジェクト代替名（Subject Alternative Name）（SAN）** | 証明書に関連付けられている IP アドレス、DNS 名、Uniform Resource Identifier（URI）、またはディレクトリ名。<br>• [DNS 名（DNS Name）]：DNS 名を選択した場合は、ISE ノードの完全修飾ドメイン名を入力します。[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオンにした場合は、ワイルドカード表記（ドメイン名の前にアスタリスクとピリオドを入力）を指定します。*.amer.example.com など。<br>• [IP アドレス（IP Address）]：証明書に関連付けられる ISE ノードの IP アドレス。<br>• [Uniform Resource Identifier]：証明書に関連付ける URI。<br>• [ディレクトリ名（Directory Name）]：RFC 2253 に従って定義される識別名（DN）の文字列表現。DN 間はカンマ（,）で区切ります。「dnQualifier」RDN の場合は、カンマをエスケープし、区切り文字としてバックスラッシュ カンマ「\,」を使用します。たとえば、CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL などです。 |
| **キー タイプ** | RSA または ECDSA の公開キーの作成に使用するアルゴリズムを指定します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| **キーの長さ（Key Length）** | 公開キーのビット サイズを指定します。<br>RSA には、次のオプションを使用できます。<br>• 512<br>• 1024<br>• 2048<br>• 4096<br>ECDSA には、次のオプションを使用できます。<br>• 256<br>• 384<br>（注） RSA および ECDSA の公開キーは、同じセキュリティ レベルで異なるキー長を持つことがあります。<br>パブリック CA の署名付き証明書を取得するか、FIPS 準拠ポリシー管理システムとして Cisco ISE を展開する場合は 2048 以上を選択します。 |
| **署名するダイジェスト（Digest to Sign With）** | ハッシュ アルゴリズム SHA-1 または SHA-256 を選択します。 |
| **証明書ポリシー（Certificate Policies）** | 証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。 |

**関連トピック**

証明書署名要求
証明書署名要求の作成と認証局への CSR の送信
CSR への CA 署名付き証明書のバインド

# 発行および失効した証明書

次の表で、[発行および失効した証明書の概要（Overview of Issued and Revoked Certificates）] ページのフィールドについて説明します。展開内の PSN ノードがエンドポイントに証明書を発行します。このページでは、展開内の各 PSN ノードが発行するエンドポイント証明書に関する情報を示します。このページへのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [概要（Overview）]** です。

表 *5:* 発行された証明書と失効した証明書

| フィールド | 使用上のガイドライン |
|---|---|
| ノード名 | 証明書を発行したポリシー サービス ノード（PSN）の名前。 |
| **[発行された証明書（Certificates Issued）]** | PSN ノードが発行したエンドポイント証明書の数。 |
| **[取り消された証明書（Certificates Revoked）]** | 失効したエンドポイント証明書（PSN ノードが発行した証明書）の数。 |
| **[証明書要求（Certificates Requests）]** | PSN ノードが処理した証明書ベースの認証要求の数。 |
| **[失敗した証明書（Certificates Failed）]** | PSN ノードが処理する失敗した認証要求の数。 |

関連トピック

- 発行された証明書
- ユーザおよびエンドポイントの証明書の更新
- 証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定
- ユーザによる証明書の更新を許可する Cisco ISE の設定
- エンドポイント証明書の失効

# 証明書のステータス（OCSP または CRL）の確認

Cisco ISE は、証明書失効リスト（CRL）を定期的にチェックします。このページを使用して、自動的にダウンロードされた CRL に対して進行中のセッションをチェックするように Cisco ISE を設定できます。OCSP または CRL のチェックを毎日開始する時刻と、OCSP サーバまたは CRL を再度チェックする前に Cisco ISE が待機する時間間隔を時間単位で指定できます。

次の表では、[証明書定期チェックの設定（Certificate Periodic Check Settings）] ページのフィールドについて説明します。このページを使用して、証明書（OCSP または CRL）のステータスをチェックする時間間隔を指定できます。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [証明書定期チェックの設定（Certificate Periodic Check Settings）]** です。

表 *6:* 証明書定期チェックの設定

| フィールド名 | 使用上のガイドライン |
|---|---|
| 証明書チェックの設定 | |

| フィールド名 | 使用上のガイドライン |
|---|---|
| 自動的に取得されたCRLに対する進行中のセッションのチェック（**Check ongoing sessions against automatically retrieved CRL**） | Cisco ISE が自動的にダウンロードされた CRL に対する進行中のセッションをチェックするようにするには、このチェックボックスをオンにします。 |
| **CRL/OCSP の定期的な証明書チェック** | |
| 最初のチェック時刻（**First check at**） | CRL または OCSP のチェックを毎日開始する時刻を指定します。00:00 ～ 23:59 の時間範囲の値を入力します。 |
| チェック間隔（**Check every**） | CRL または OCSP サーバを再度チェックする前に Cisco ISE が待機する時間間隔を時間単位で指定します。 |

関連トピック

OCSP サービス

OCSP クライアント プロファイルの追加

# システム証明書のインポート設定

次の表では、サーバ証明書をインポートするために使用できる [システム証明書のインポート（Import System Certificate）] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[管理（Administration）]** > > > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates）]** > **[インポート（Import）]** です。

表 *7:* システム証明書のインポート設定

| フィールド名 | 説明 |
|---|---|
| ノードの選択（**Select Node**） | （必須）システム証明書をインポートする Cisco ISE ノードを選択します。 |
| 証明書ファイル（**Certificate file**） | （必須）[参照（Browse）] をクリックして、ローカル システムから証明書ファイルを選択します。 |
| 秘密キー ファイル（**Private key file**） | （必須）[参照（Browse）] をクリックして、秘密キー ファイルを選択します。 |
| パスワード（**Password**） | （必須）秘密キー ファイルを復号化するためのパスワードを入力します。 |

| フィールド名 | 説明 |
|---|---|
| フレンドリ名（**Friendly Name**） | 証明書のフレンドリ名を入力します。名前を指定しない場合は、<common name> # <issuer> # <nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。 |
| ワイルドカード証明書の許可（**Allow Wildcard Certificates**） | ワイルドカード証明書（サブジェクトの任意の一般名またはサブジェクト代替名の DNS 名、またはその両方にアスタリスク（*）が含まれている証明書）をインポートする場合は、このチェックボックスをオンにします。たとえば、SAN に割り当てられている DNS 名が *.amer.cisco.com の場合です。このチェックボックスをオンにすると、Cisco ISE は展開内の他のすべてのノードにこの証明書をインポートします。 |
| 証明書の拡張の検証（**Validate Certificate Extensions**） | Cisco ISE に証明書の拡張の検証を許可する場合は、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、かつインポートする証明書に CA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。 |
| **Usage** | このシステム証明書を使用する必要があるサービスを選択します。<br>• [管理者（Admin）]：管理者ポータルとの通信および展開内の ISE ノード間の通信の保護に使用されるサーバ証明書<br>（注） プライマリ PAN 上の管理者ロール証明書の証明書を変更すると、他のすべてのノード上のサービスが再起動されます。<br>• [EAP 認証（EAP Authentication）]：SSL/TLS トンネリングの EAP プロトコルを使用する認証に使用されるサーバ証明書<br>• [RADIUS DTLS]：RADIUS DTLS 認証に使用するサーバ証明書<br>• [pxGrid]：pxGrid クライアントとサーバの間の通信を保護するクライアントおよびサーバ証明書<br>• [SAML]：SAML ID プロバイダー（IdP）とのセキュア通信に使用するサーバ証明書。SAML 用の使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。<br>• [ポータル（Portal）]：すべての Cisco ISE Web ポータルとの通信を保護するために使用されるサーバ証明書 |

### 関連トピック

システム証明書
システム証明書の表示
システム証明書のインポート

# [信頼できる証明書ストア（Trusted Certificate Store）] ページ

次の表では、管理ノードに追加された証明書を表示するために使用できる [信頼できる証明書ストア（Trusted Certificates Store）] ページのフィールドについて説明します。このページへのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** です。

表 *8:* 信頼できる証明書ページ

| フィールド名 | 使用上のガイドライン |
|---|---|
| フレンドリ名（**Friendly Name**） | 証明書の名前を表示します。 |
| **Status**（ステータス） | 有効または無効にします。[無効（Disabled）] の場合、ISEは信頼を確立するために証明書を使用しません。 |
| 信頼対象（**Trusted for**） | 証明書を使用するサービスを表示します。 |
| 発行先（**Issued To**） | 証明書のサブジェクトの一般名（CN）。 |
| 発行元（**Issued By**） | 証明書の発行元の一般名（CN）。 |
| 有効期限の開始（**Valid From**） | 「Not Before」証明書属性。 |
| **Expiration Date** | 「Not After」証明書属性。 |
| 有効期限ステータス（**Expiration Status**） | 証明書の有効期限のステータスに関する情報です。このコラムに表示される情報メッセージには5つのアイコンとカテゴリがあります。<br>• **緑色**：期限切れまで 91 日以上<br>• **青色**：期限切れまで 90 日以内<br>• **黄色**：期限切れまで 60 日以内<br>• **オレンジ色**：期限切れまで 30 日以内<br>• **赤色**: 期限切れ |

関連トピック

- 信頼できる証明書ストア
- 信頼できるストア証明書の表示
- 信頼できる証明書ストアの証明書のステータス変更
- 信頼できる証明書ストアへの証明書の追加

# 証明書設定の編集

次の表では、認証局（CA）証明書属性を編集するために使用できる [証明書ストアの証明書編集（Certificate Store Edit Certificate）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [証明書（Certificate）] > [編集（Edit）]** です。

**表 *9*：証明書ストア編集設定**

| フィールド名 | 使用上のガイドライン |
|---|---|
| 証明書発行元（Certificate Issuer） | |
| フレンドリ名（**Friendly Name**） | 証明書のフレンドリ名を入力します。 |
| **Status**（ステータス） | [有効（Enabled）] または [無効（Disabled）] を選択します。[無効（Disabled）] の場合、ISE は信頼を確立するために証明書を使用しません。 |
| 説明 | 任意で説明を入力します。 |
| 使用方法 | |
| **ISE 内の認証用に信頼する（Trust for authentication within ISE**） | この証明書で（他の ISE ノードまたは LDAP サーバから）サーバ証明書を検証する場合は、このチェックボックスをオンにします。 |
| クライアント認証および **syslog** 用に信頼する（**Trust for client authentication and Syslog**） | （[ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。<br>• EAP プロトコルを使用した ISE に接続するエンドポイントの認証<br>• syslog サーバの信頼 |
| シスコ サービスの認証用に信頼する（**Trust for authentication of Cisco Services**） | フィードサービスなどの外部シスコ サービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。 |

| フィールド名 | 使用上のガイドライン |
|---|---|
| 証明書ステータスの検証（**Certificate Status Validation**） | ISEは、特定のCAが発行するクライアントまたはサーバ証明書の失効ステータスをチェックする2とおりの方法をサポートしています。1つは、Online Certificate Status Protocol（OCSP）を使用して証明書を検証することです（OCSPは、CAによって保持されるOCSPサービスに要求を行います）。もう1つは、ISEにCAからダウンロードした証明書失効リスト（CRL）に対して証明書を検証することです。両方の方法は、OCSPを最初に使用し、ステータスを判断できないときに限りCRLを使用する場合に使用できます。 |
| **OCSP サービスに対して検証する（Validate Against OCSP Service）** | OCSP サービスに対して証明書を検証するには、このチェックボックスをオンにします。このボックスをオンにするには、まずOCSPサービスを作成する必要があります。 |
| **OCSP が不明なステータスを返した場合は要求を拒否する（Reject the request if OCSP returns UNKNOWN status）** | 認証ステータスがOCSPによって判別されなかった場合に要求を拒否するには、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た場合、OCSPサービスによって不明のステータス値が返されると、ISEは現在評価されているクライアントまたはサーバ証明書を拒否します。 |
| **OCSP応答側が到達不能な場合は要求を拒否する（Reject the request if OCSP Responder is unreachable）** | OCSP応答側が到達不能な場合にISEが要求を拒否するには、このチェックボックスをオンにします。 |
| **CRL のダウンロード（Download CRL）** | Cisco ISEでCRLをダウンロードするには、このチェックボックスをオンにします。 |
| **CRL 配信 URL（CRL Distribution URL）** | CA から CRL をダウンロードするための URL を入力します。認証局証明書で指定されている場合、このフィールドは自動的に読み込まれます。URL は「http」、「https」、または「ldap」で始まる必要があります。 |
| **CRL の取得（Retrieve CRL）** | CRL は、自動的または定期的にダウンロードできます。ダウンロードの時間間隔を設定します。 |
| **ダウンロードが失敗した場合は待機する（If download failed, wait）** | Cisco ISEがCRLを再度ダウンロードするまでに待機する時間間隔を設定します。 |

| フィールド名 | 使用上のガイドライン |
|---|---|
| **CRL を受信しない場合 CRL 検証をバイパスする（Bypass CRL Verification if CRL is not Received）** | このチェックボックスをオンにした場合、クライアント要求は CRL が受信される前に受け入れられます。このチェックボックスをオフにした場合、選択した CA によって署名された証明書を使用するすべてのクライアント要求は、Cisco ISE によって CRL ファイルが受信されるまで拒否されます。 |
| **CRL がまだ有効でないか、または期限切れの場合は無視する（Ignore that CRL is not yet valid or expired）** | Cisco ISE で開始日と期限日を無視し、まだアクティブでないかまたは期限切れの CRL を引き続き使用し、CRL の内容に基づいて EAP-TLS 認証を許可または拒否する場合は、このチェックボックスをオンにします。<br><br>Cisco ISE で [有効日（Effective Date）] フィールドの開始日と [次の更新（Next Update）] フィールドの期限日を CRL ファイルでチェックする場合は、このチェックボックスをオフにします。CRL がまだアクティブではないか、または期限切れの場合、その CA によって署名された証明書を使用するすべての認証は拒否されます。 |

関連トピック

信頼できる証明書ストア

信頼できる証明書の編集

# 信頼できる証明書のインポート設定

次の表では、認証局（CA）証明書を Cisco ISE に追加するために使用できる [信頼できる証明書のインポート（Trusted Certificate Import）] ページのフィールドについて説明します。このページへのナビゲーション パスは **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]** です。

表 *10 :* 信頼できる証明書のインポート設定

| フィールド | 説明 |
|---|---|
| **証明書ファイル（Certificate file）** | [参照（Browse）] をクリックして、ブラウザを実行しているコンピュータから証明書ファイルを選択します。 |

| フィールド | 説明 |
|---|---|
| フレンドリ名（**Friendly Name**） | 証明書のフレンドリ名を入力します。名前を指定しない場合は、Cisco ISE により <common name>#<issuer>#<nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。 |
| **ISE 内の認証用に信頼する（Trust for authentication within ISE）** | この証明書を（他の ISE ノードまたは LDAP サーバから）サーバ証明書の検証に使用する場合は、このチェックボックスをオンにします。 |
| **クライアント認証および syslog 用に信頼する（Trust for client authentication and Syslog）** | （[ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。<br>• EAP プロトコルを使用した ISE に接続するエンドポイントの認証<br>• syslog サーバの信頼 |
| **シスコ サービスの認証用に信頼する（Trust for authentication of Cisco Services）** | フィードサービスなどの外部シスコ サービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。 |
| **証明書の拡張の検証（Validate Certificate Extensions）** | （[クライアント認証用に信頼する（Trust for client authentication）] オプションと [証明書拡張の検証を有効にする（Enable Validation of Certificate Extensions）] オプションの両方をオンにした場合のみ）「keyUsage」拡張が存在し、「keyCertSign」ビットが設定されていることと、CA フラグが true に設定された基本制約拡張が存在することを確認します。 |
| **説明** | 任意で説明を入力します。 |

**関連トピック**

信頼できる証明書ストア
証明書チェーンのインポート
信頼できる証明書ストアへのルート証明書のインポート

# OCSP クライアント プロファイル設定

次の表では、OCSP クライアント プロファイル設定を行うために使用できる [OCSP クライアント プロファイル（OCSP Client Profile）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [OCSP クライアント プロファイル（OCSP Client Profile）]** です。

表 *11 : OCSP* クライアント プロファイル設定

| フィールド名 | 使用上のガイドライン |
|---|---|
| 名前（**Name**） | OCSP クライアント プロファイル名。 |
| 説明 | 任意で説明を入力します。 |
| **OCSP応答側の設定（Configure OCSP Responder）** | |
| セカンダリ サーバの有効化（**Enable Secondary Server**） | ハイ アベイラビリティのセカンダリ OCSP サーバを有効にするには、このチェックボックスをオンにします。 |
| 常にプライマリ サーバに最初にアクセスする（**Always Access Primary Server First**） | このオプションは、セカンダリ サーバへの移動を試行する前にプライマリ サーバをチェックする場合に使用します。プライマリが以前にチェックされ、応答しないことがわかっている場合にも、Cisco ISE はセカンダリ サーバに移動する前にプライマリ サーバへの要求の送信を試行します。 |
| [n 分経過後にプライマリ サーバにフォールバック（Fallback to Primary Server After Interval *n* Minutes）] | このオプションは、Cisco ISE がセカンダリ サーバに移動してから、再度プライマリ サーバにフォールバックする場合に使用します。この場合、その他の要求はすべてスキップされ、テキスト ボックスで設定した時間セカンダリ サーバが使用されます。許可される時間の範囲は 1 ～ 999 分です。 |
| **プライマリ サーバとセカンダリ サーバ（Primary and Secondary Servers）** | |
| **URL** | プライマリおよびセカンダリ OCSP サーバの URL を入力します。 |
| ナンス拡張サポートの有効化（**Enable Nonce Extension Support**） | ナンスが OCSP 要求の一部として送信されるように設定できます。ナンスには、OCSP 要求の疑似乱数が含まれます。応答で受信される数値は要求に含まれる数値と同じであることが検証されています。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。 |

| フィールド名 | 使用上のガイドライン |
|---|---|
| **応答の署名の検証（Validate Response Signature）** | OCSP レスポンダは、次のいずれかの証明書を使用して応答に署名します。<br>• CA 証明書<br>• CA 証明書とは別の証明書<br>Cisco ISE が応答の署名を検証するためには、OCSP 応答側が応答を証明書とともに送信する必要があります。そうでない場合、応答の検証は失敗し、証明書のステータスは利用できません。RFC に従い、OCSP は異なる証明書を使用して応答に署名できます。このことは、OCSP が Cisco ISE による検証用に応答に署名した証明書を送信する限り当てはまります。OCSP が Cisco ISE で設定されているものとは異なる証明書を使用して応答に署名した場合、応答の検証は失敗します。 |
| **Authority Information Access（AIA）に指定されたOCSP URLを使用する（Use OCSP URLs specified in Authority Information Access (AIA)）** | Authority Information Access の拡張で指定されている OCSP URL を使用するには、オプション ボタンをクリックします。 |
| **応答キャッシュ（Response Cache）** | |

| フィールド名 | 使用上のガイドライン |
|---|---|
| [キャッシュ エントリの存続可能時間 n 分(Cache Entry Time To Live *n* Minutes)] | キャッシュ エントリが期限切れになる時間を分単位で入力します。OCSP サーバからの各応答には nextUpdate 値が含まれています。この値は、証明書のステータスがサーバで次にいつ更新されるかを示します。OCSP 応答がキャッシュされるとき、2 つの値（1 つは設定から、もう 1 つは応答から）が比較され、この 2 つの最小値の時間だけ応答がキャッシュされます。nextUpdate 値が 0 の場合、応答はまったくキャッシュされません。Cisco ISE は設定された時間 OCSP 応答をキャッシュします。キャッシュは複製されず、永続的でもないため、Cisco ISE が再起動するとキャッシュはクリアされます。次の理由により、OCSP キャッシュは OCSP 応答を保持するために使用されます。<br>• 既知の証明書に関する OCSP サーバからのネットワーク トラフィックと負荷を低減するため<br>• 既知の証明書のステータスをキャッシュすることによって Cisco ISE のパフォーマンスを向上させるため<br><br>デフォルトでは、キャッシュは内部 CA OCSP クライアント プロファイルに対し 2 分に設定されています。エンドポイントが最初の認証から 2 分以内にもう一度認証すると、OCSP のキャッシュが使用され、OCSP レスポンダには問い合わせされません。エンドポイントの証明書がキャッシュ期間内に失効した場合、以前の OCSP のステータス [良好（Good）] が使用され、認証は成功します。キャッシュを 0 分に設定すると、応答はキャッシュされません。このオプションでは、セキュリティは向上しますが、認証のパフォーマンスは低下します。 |
| **キャッシュのクリア（Clear Cache）** | OCSP サービスに接続されているすべての認証局のエントリをクリアするには、[キャッシュのクリア（Clear Cache）] をクリックします。<br><br>展開内で、[キャッシュのクリア（Clear Cache）] はすべてのノードと相互作用して、処理を実行します。このメカニズムでは、展開内のすべてのノードが更新されます。 |

**関連トピック**

OCSP サービス
Cisco ISE CA サービスの Online Certificate Status Protocol レスポンダ
OCSP 証明書のステータスの値
OCSP ハイ アベイラビリティ
OCSP の障害
OCSP 統計情報カウンタ

OCSP クライアント プロファイルの追加

# 内部 CA の設定

次の表では、内部 CA の設定ページのフィールドについて説明します。内部 CA の設定を表示し、このページから内部 CA サービスを無効にできます。このページへのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [内部 CA の設定（Internal CA Settings）]** です。

表 *12 :* 内部 *CA* の設定

| フィールド名 | 使用上のガイドライン |
|---|---|
| **認証局の無効化（Disable Certificate Authority）** | 内部 CA サービスを無効にするには、このボタンをクリックします。 |
| **ホスト名（Host Name）** | CA サービスを実行している Cisco ISE ノードのホスト名。 |
| **ペルソナ（Personas）** | CA サービスを実行しているノードで有効な Cisco ISE ノードのペルソナ。たとえば、管理、ポリシー サービスなどです。 |
| **ロール（Role(s)）** | CA サービスを実行する Cisco ISE ノードが担当するロール。たとえば、スタンドアロンまたはプライマリまたはセカンダリです。 |
| **CA、EST、および OCSP 応答側のステータス（CA, EST & OCSP Responder Status）** | 有効または無効 |
| **OCSP 応答側 URL（OCSP Responder URL）** | OCSP サーバにアクセスするための Cisco ISE ノードの URL。 |
| **SCEP URL** | SCEP サーバにアクセスするための Cisco ISE ノードの URL。 |

**関連トピック**

Cisco ISE CA サービス

証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定

# 証明書テンプレートの設定

次の表に、クライアント プロビジョニング ポリシーで使用される SCEP RA プロファイルの定義に使用できる [CA 証明書テンプレート（CA Certificate Template）] ページのフィールドを示します。このページへのナビゲーションパスは、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > > **[証明書テンプレート（Certificate Templates）]** > **[追加（Add）]** です。

（注） 証明書テンプレート フィールド（[組織ユニット（Organizational Unit）]、[組織（Organization）]、[都市（City）]、[州（State）]、および [国（Country）]）の UTF-8 文字はサポートしていません。UTF-8 文字を証明書テンプレートで使用すると、証明書プロビジョニングが失敗します。

**表 *13*：証明書テンプレートの設定**

| フィールド名 | 使用上のガイドライン |
|---|---|
| **名前（Name）** | （必須）証明書テンプレートの名前を入力します。たとえば、Internal_CA_Template とします。 |
| **説明** | （任意）説明を入力します。 |
| **Common Name（CN）** | （表示のみ）一般名にはユーザ名が自動入力されます。 |
| **Organizational Unit（OU）** | 組織ユニット名。Engineering など。 |
| **Organization（O）** | 組織名。Cisco など。 |
| **都市（City）（L）** | （省略不可）都市名。San Jose など。 |
| **州（State）（ST）** | （省略不可）州名。California など。 |
| **国（Country）（C）** | 国名。2 文字の ISO 国番号を入力する必要があります。US など。 |
| **サブジェクト代替名（Subject Alternative Name）（SAN）** | （表示のみ）エンドポイントの MAC アドレス。 |
| **キー タイプ** | RSA または ECC |

| フィールド名 | 使用上のガイドライン |
|---|---|
| キー サイズ | （RSA を選択した場合にのみ適用可能）1024 以上のキー サイズを指定します。 |
| 曲線タイプ（**Curve Type**） | （ECC を選択した場合にのみ適用可能）曲線のタイプを指定します（デフォルトは P-384 です）。 |
| **SCEP RA プロファイル（SCEP RA Profile**） | ISE 内部 CA または作成した外部 SCEP RA プロファイルを選択します。 |
| 有効期限（**Valid Period**） | 証明書の期限が切れるまでの日数を入力します。 |
| 拡張キーの使用状況 | |
| クライアント認証 | クライアント認証にこの証明書を使用する場合は、このチェック ボックスをオンにします。 |
| サーバ認証（**Server Authentication**） | サーバ認証にこの証明書を使用する場合は、このチェック ボックスをオンにします。 |

関連トピック

- 証明書テンプレート
- 証明書テンプレート名の拡張子
- 証明書を使用してパーソナル デバイスを許可するための Cisco ISE の設定
- pxGrid コントローラ用の Cisco ISE CA 証明書の展開
- 許可ポリシー条件での証明書テンプレート名の使用

# ロギングの設定

次の各ページでは、デバッグ ログの重大度の設定、外部ログ ターゲットの作成が可能です。また、Cisco ISE がこれらの外部ログ ターゲットにログ メッセージを送信できるようにできます。

## リモート ロギング ターゲットの設定

次の表では、外部の場所（syslogサーバ）を作成してロギングメッセージを保存するために使用できる [リモート ロギング ターゲット（Remote Logging Targets）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）]** です。

表 *14*：リモート ロギング ターゲットの設定

| フィールド | 使用上のガイドライン |
|---|---|
| 名前（Name） | 新しいターゲットの名前を入力します。 |
| ターゲット タイプ（Target Type） | ターゲット タイプを選択します。デフォルトでは、[UDP Syslog] に設定されます。 |
| 説明 | 新しいターゲットの簡単な説明を入力します。 |
| [IPアドレス（IP Address）] | ログを格納する宛先マシンの IP アドレスまたはホスト名を入力します。ISEは、ロギング用に IPv4 と IPv6 形式をサポートします。 |
| [ポート（Port）] | 宛先マシンのポート番号を入力します。 |
| ファシリティ コード（Facility Code） | ロギングに使用する syslog ファシリティ コードを選択します。有効なオプションは、Local0 ～ Local7 です。 |
| 最大長（Maximum Length） | リモート ログ ターゲット メッセージの最大長を入力します。有効なオプションは200～1024バイトです。 |
| サーバダウン時のバッファ メッセージ（Buffer Message When Server Down） | TCP syslog ターゲットおよびセキュア syslog ターゲットが使用できないときに Cisco ISE に syslog メッセージをバッファするには、このチェックボックスをオンにします。ISEは、接続が再開されるとターゲットへのメッセージの送信を再試行します。接続が再開された後、メッセージは古いものから順に送信され、バッファ内のメッセージは常に新しいメッセージの前に送信されます。バッファがいっぱいになると、古いメッセージが廃棄されます。 |
| バッファ サイズ（MB）（Buffer Size (MB)） | 各ターゲットのバッファ サイズを設定します。デフォルトでは、100 MB に設定されます。バッファ サイズを変更するとバッファがクリアされ、特定のターゲットのバッファリングされた既存のすべてのメッセージが失われます。 |
| 再接続タイムアウト（秒）（Reconnect Timeout (Sec)） | サーバがダウンしている場合に TCP およびセキュア syslog を廃棄する前に保持する期間を秒単位で指定します。 |
| CA 証明書の選択（Select CA Certificate） | クライアント証明書を選択します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| サーバ証明書有効性を無視（Ignore Server Certificate validation） | ISE でサーバ証明書認証が無視されるようにして、syslog サーバを許可するには、このチェックボックスをオンにします。デフォルトでは、このオプションが無効になっているときにシステムが FIPS モードでない限り、このオプションはオフに設定されます。 |

**関連トピック**

- Cisco ISE ロギング メカニズム
- Cisco ISE システム ログ
- リモート syslog メッセージの形式
- Cisco ISE メッセージ カタログ
- 収集フィルタ
- イベント抑制バイパス フィルタ
- リモート syslog 収集場所の設定
- 収集フィルタの設定

# ロギング カテゴリの設定

次の表では、[ロギング カテゴリ（Logging Categories）]ページのフィールドについて説明します。これらのフィールドを使用して、ログの重大度レベルを設定し、選択したカテゴリのログが保存されるロギング ターゲットを選択できます。このページへのナビゲーション パスは、[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギングカテゴリ（Logging Categories）] です。

**表 *15:* ロギング カテゴリの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 名前（Name） | ロギング カテゴリの名前を表示します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| ログの重大度レベル（Log Severity Level） | 次のオプションから、診断ロギング カテゴリの重大度レベルを選択できます。<br>• [重大（FATAL）]：緊急事態。 このオプションは、Cisco ISE が使用できないため、緊急措置が必要であることを意味します<br>• [エラー（ERROR）]：このオプションは深刻な状態またはエラー状態を示します。<br>• [警告（WARN）]：このオプションは、通常の状態ではあるが重大な状態を示します。 これがデフォルトの条件です。<br>• [情報（INFO）]：このオプションは、情報メッセージを示します。<br>• [デバッグ（DEBUG）]：このオプションは、診断バグ メッセージを示します。 |
| ローカル ロギング（Local Logging） | ローカル ノードで上のこのカテゴリのロギング イベントを有効にするには、このチェックボックスをオンにします。 |
| ターゲット（Target） | 左アイコンと右アイコンを使用して[使用可能（Available）]と [選択済み（Selected）]のボックス間でターゲットを移動することによって、カテゴリのターゲットを変更できます。[使用可能（Available）]ボックスには、論理（事前定義済み）と外部（ユーザ定義）という両方の既存のロギング ターゲットが含まれています。最初は空の[選択済み（Selected）]ボックスには、特定のカテゴリの選択済みターゲットが含まれます。 |

**関連トピック**

リモート syslog メッセージの形式
Cisco ISE メッセージ コード
リモート syslog 収集場所の設定
メッセージ コードの重大度レベルの設定

# メンテナンスの設定

これらのページでは、バックアップ、復元、およびデータ消去機能を使用してデータを管理できます。

## リポジトリの設定

次の表では、リポジトリを作成してバックアップ ファイルを保存するために使用できる [リポジトリ リスト（Repository List）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[メンテナンス（Maintenance）]** > **[リポジトリ（Repository）]** です。

**表 *16 :* リポジトリの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| リポジトリ（Repository） | リポジトリの名前を入力します。最大 80 文字の英数字を使用できます。 |
| プロトコル | 使用する使用可能なプロトコルの 1 つを選択します。 |
| サーバ名（Server Name） | （TFTP、HTTP、HTTPS、FTP、SFTP、および NFS で必須）リポジトリの作成先サーバのホスト名または IP アドレス（IPv4 または IPv6）を入力します。<br>（注） IPv6 アドレスを使用してリポジトリを追加する場合は、IPv6 アドレスを使用して ISE eth0 インターフェイスが設定されていることを確認します。 |
| パス | リポジトリへのパスを入力します。このパスは、リポジトリの作成時に有効であり、存在している必要があります。<br>この値は、サーバのルート ディレクトリを示す 2 つのスラッシュ（//）または単一のスラッシュ（/）で開始できます。ただし、FTP プロトコルの場合は、単一のスラッシュ（/）はルートディレクトリではなく FTP ユーザのホームディレクトリを示します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| PKI 認証を有効にします。 | （オプション：SFTP リポジトリにのみ適用）SFTP リポジトリで RSA 公開キー認証を有効にするには、このチェック ボックスをオンにします。 |
| ユーザ名（User Name） | （FTP、SFTP で必須）指定されたサーバに対する書き込み権限を持つユーザ名を入力します。使用できる文字は英数字のみです。 |
| [パスワード（Password）] | （FTP、SFTP で必須）指定されたサーバへのアクセスに使用するパスワードを入力します。パスワードに使用できる文字は、0 ～ 9、a ～ z、A ～ Z、-、.、|、@、#、$、%、^、&、*、,、+、および = です。 |

**関連トピック**

バックアップ/復元リポジトリ
リポジトリの作成

# オンデマンド バックアップの設定

次の表では、バックアップを任意の時点で取得するために使用できる [オンデマンド バックアップ（On-Demand Backup）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[バックアップ/復元（Backup & Restore）]** です。

**表 *17*:オンデマンド バックアップの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| バックアップ名（Backup Name） | バックアップ ファイルの名前を入力します。 |
| リポジトリ名（Repository Name） | バックアップファイルを保存するリポジトリ。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。 |
| 暗号化キー（Encryption Key） | このキーは、バックアップ ファイルの暗号化および解読に使用されます。 |

**関連トピック**

バックアップ データのタイプ
オンデマンドおよびスケジュール バックアップ

# スケジュール バックアップの設定

次の表では、フル バックアップまたは差分バックアップの復元に使用できる [スケジュール バックアップ（Scheduled Backup）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[バックアップ/復元（Backup and Restore）]** です。

**表 *18* : スケジュール バックアップの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 名前（Name） | バックアップ ファイルの名前を入力します。任意の説明的な名前を入力できます。Cisco ISE は、バックアップ ファイル名にタイムスタンプを追加して、ファイルをリポジトリに格納します。一連のバックアップを設定しても、バックアップ ファイル名は一意になります。[スケジュール バックアップ（Scheduled Backup）] リスト ページでは、ファイルが **kron** occurrence ジョブであることを示すために、バックアップ ファイル名に「backup_occur」が付加されます。<br>. |
| 説明 | バックアップの説明を入力します。 |
| リポジトリ名（Repository Name） | バックアップ ファイルを保存するリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。 |
| 暗号化キー（Encryption Key） | バックアップ ファイルを暗号化および復号化するためのキーを入力します。 |
| スケジューリング オプション（Schedule Options） | スケジュール バックアップの頻度を選択し、適宜他のオプションに入力します。 |

関連トピック

- バックアップ データのタイプ
- オンデマンドおよびスケジュール バックアップ
- バックアップ履歴
- バックアップの失敗
- Cisco ISE 復元操作
- 認証および許可ポリシー設定のエクスポート
- 分散環境でのプライマリ ノードとセカンダリ ノードの同期
- CLI を使用したバックアップ
- バックアップのスケジュール

# ポリシーのエクスポート設定のスケジュール

次の表では、[ポリシーのエクスポートのスケジュール（Schedule Policy Export）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）] > [ポリシーのエクスポート（Policy Export）]** です。

表 *19* : ポリシーのエクスポート設定のスケジュール

| フィールド | 使用上のガイドライン |
|---|---|
| 暗号化（Encryption） | |
| 暗号化キー（Encryption Key） | エクスポート データを暗号化および復号化するためのキーを入力します。このフィールドは、[暗号キーを使用したエクスポート（Export with Encryption Key）] オプションを選択した場合にのみ有効になります。 |
| [接続先（Destination）] | |
| ローカル コンピュータにファイルをダウンロード（Download file to local computer） | ポリシー エクスポート ファイルをローカル システムにダウンロードできます。 |
| [ファイルをメールで送信（Email file to）] | 複数の電子メール アドレスをカンマで区切って入力します。 |
| リポジトリ（Repository） | エクスポート データを保存するリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。ポリシーのエクスポートのスケジュールを設定する前に、リポジトリを作成してください。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 今すぐエクスポート（Export Now） | 指定したリポジトリにデータをすぐにエクスポートするには、このオプションをクリックします。 |
| スケジュール | |
| スケジューリング オプション（Schedule Options） | エクスポートのスケジュールの頻度を選択し、それに応じてその他の詳細を入力します。 |

# 管理者アクセスの設定

これらのページにより、管理者のアクセス設定を行うことができます。

## 管理者パスワード ポリシーの設定

次の表に、管理者パスワードが満たす必要のある基準を定義するために使用できる [管理者パスワード ポリシー（Administrator Password Policy）] ページのフィールドを示します。このページのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[管理アクセス（Admin Access）]** > **[認証（Authentication）]** > **[パスワード ポリシー（Password Policy）]** です。

表 *20 :* 管理者パスワード ポリシーの設定

| フィールド | 使用上のガイドライン |
|---|---|
| 最小長（Minimum Length） | パスワードの最小長（文字数）を設定します。デフォルトは 6 文字です。 |

| フィールド | 使用上のガイドライン |
| --- | --- |
| パスワードに使用できない文字（Password may not contain） | [管理者名またはその文字の逆順は使用できません（Admin name or its characters in reverse order）]：このチェックボックスをオンにして、管理者ユーザ名またはその文字の逆順での使用を制限します。 |
| | [「cisco」またはその文字の逆順は使用できません（"cisco" or its characters in reverse order）]：このチェックボックスをオンにして、単語「cisco」またはその文字の逆順での使用を制限します。 |
| | [この単語またはその文字の逆順は使用できません（This word or its characters in reverse order）]：このチェックボックスをオンにして、定義したすべての単語またはその文字の逆順での使用を制限します。 |
| | [4 回以上連続する繰り返し文字は使用できません（Repeated characters four or more times consecutively）]：このチェックボックスをオンにして、4回以上連続する繰り返し文字の使用を制限します。 |

| フィールド | 使用上のガイドライン |
| --- | --- |
| | [辞書の単語、その文字の逆順、または文字の置き換えは使用できません（Dictionary words, their characters in reverse order or their letters replaced with other characters]：辞書の単語、単語の文字の逆順での使用、単語の文字の置き換えでの使用を制限します。<br><br>「s」を「$」、「a」を「@」、「o」を「0」、「l」を「1」、「i」を「!」、「e」を「3」に置き換えることはできません。たとえば Pa$$w0rd などです。<br><br>• [デフォルトの辞書（Default Dictionary）]：Cisco ISE でデフォルトの Linux 辞書を使用するには、このオプションを選択します。デフォルトの辞書には約 480,000 件の英単語が含まれています。<br><br>デフォルトでは、このオプションが選択されています。<br><br>• [カスタム辞書（Custom Dictionary]：カスタマイズした辞書を使用するには、このオプションを選択します。[ファイルの選択（Choose File）] をクリックし、カスタム辞書ファイルを選択します。このテキスト ファイルでは、単語が改行文字で区切られており、拡張子は .dic、サイズは 20 MB 以下である必要があります。 |
| 必須の文字（Required Characters） | 管理者パスワードに、次の選択肢から選択したタイプの文字が少なくとも 1 つ含まれている必要があることを指定します。<br><br>• 小文字の英文字<br><br>• 大文字の英文字<br><br>• 数字（Numeric characters）<br><br>• 英数字以外の文字（Non-alphanumeric characters） |

| フィールド | 使用上のガイドライン |
|---|---|
| パスワード履歴（Password History） | 同じパスワードが繰り返し使用されるのを防ぐために、新しいパスワードと異なっている必要がある以前のパスワードの数を指定します。<br>また、以前のパスワードと異なる必要がある文字数を指定します。<br>ユーザがパスワードを再使用できない日数を入力します。 |
| パスワードライフタイム（Password Lifetime） | 次のオプションを指定して、指定した期間後にパスワードを変更するようユーザに強制します。<br>• パスワードが変更されなかった場合に管理者アカウントを無効にするまでの時間（日数）（Time (in days) before the administrator account is disabled if the password is not changed.）（使用可能な範囲は 0 ～ 2,147,483,647 日です）。<br>• 管理者アカウントが無効になるまでのリマインダ（日数）。（Reminder (in days) before the administrator account is disabled.） |
| ネットワーク デバイスの機密データの表示 | |
| 管理者パスワードが必要（Require Admin Password） | 共有秘密やパスワードなどのネットワーク デバイスの機密データを表示するために管理者ユーザがログイン パスワードを入力するようにする場合には、このチェックボックスにマークを付けます。 |
| パスワードのキャッシュ期間（Password cached for） | 管理者ユーザによって入力されたパスワードは、この期間キャッシュされます。管理者ユーザはこの間、ネットワークデバイスの機密データを表示するためにパスワードの再入力を求められることはありません。有効な範囲は 1 ～ 60 分です。 |

**関連トピック**

Cisco ISE 管理者
新しい管理者の作成

# セッション タイムアウトおよびセッション情報の設定

次の表では、セッションタイムアウトを定義し、アクティブな管理セッションを終了するために使用できる[セッション（Session）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[管理者アクセス（Admin Access）]** > **[設定（Settings）]** > **[セッション（Session）]** です。

**表 *21* : セッション タイムアウトおよびセッション情報の設定**

| フィールド | 使用上のガイドライン |
|---|---|
| セッションのタイムアウト（Session Timeout） | |
| セッション アイドル タイムアウト（Session Idle Timeout） | アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間（分）を入力します。デフォルト値は 60 分です。有効な範囲は 6 ～ 100 分です。 |
| セッション情報（Session Info） | |
| 無効化（Invalidate） | 終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化（Invalidate）] をクリックします。 |

**関連トピック**

管理者アクセスの設定
管理者のセッション タイムアウトの設定
アクティブな管理セッションの終了

# 設定

これらのページでは、さまざまなサービスの全般設定を行うことができます。

# ポスチャの全般設定

次の表では、修復時間およびポスチャ ステータスなどの一般的なポスチャ設定を行うために使用できる [ポスチャの全般設定（Posture General Settings）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[全般設定（General Settings）]** です。

表 *22*：ポスチャの全般設定

| フィールド | 使用上のガイドライン |
|---|---|
| 修復タイマー（Remediation Timer） | 分単位で時間値を入力します。デフォルト値は 4 分です。有効な範囲は 1 ～ 300 分です。 |
| ネットワーク遷移遅延（Network Transition Delay） | 秒単位で時間値を入力します。デフォルト値は 3 秒です。有効な値の範囲は 2 ～ 30 秒です。 |
| デフォルトのポスチャ ステータス（Default Posture Status） | 準拠または非準拠を選択します。Linux のような非エージェント デバイスは、ネットワークに接続している間、このステータスを想定します。 |
| 一定時間（秒）経過後にログイン成功画面を自動的に閉じる（Automatically Close Login Success Screen After） | このチェックボックスをオンにすると、指定された時間後に、ログイン成功画面が自動的に閉じます。<br>チェックボックスの隣のフィールドに、時間値を秒単位で入力します。<br>0 ～ 300 秒にログイン画面が自動的に閉じるようにタイマーを設定できます。時間をゼロに設定した場合は、クライアント上のエージェントはログイン成功画面を表示しません。 |
| 連続モニタリング間隔（Continuous Monitoring Interval） | AnyConnect がモニタリング データの送信を開始するまでの時間間隔を指定します。アプリケーション条件の場合アプリケーションおよびハードウェア条件の場合、デフォルト値は 5 分です。 |
| ステルス モードでの利用規約（Acceptable Use Policy in Stealth Mode） | 会社のネットワーク使用条件が満たされていない場合、ステルス モードで [ブロック（Block）] を選択して、クライアントを非準拠ポスチャ ステータスに移行します。 |
| ポスチャのリース | |
| ユーザがネットワークに接続するたびにポスチャ評価を行う（Perform posture assessment every time a user connects to the network） | ユーザがネットワークに接続するたびにポスチャ評価を開始するには、このオプションを選択します。 |
| *n* 日おきにポスチャ評価を行う（Perform posture assessment every n days） | クライアントがすでにポスチャ準拠であるものの、指定された日数が経過したら、ポスチャ評価を開始する場合は、このオプションを選択します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 最後の既知の良い状態をキャッシュする（Cache Last Known Good State） | ポスチャ評価の結果をキャッシュするには、Cisco ISE のこのチェックボックスをオンにします。デフォルトでは、このフィールドは無効です。 |
| 最後の既知の良い状態（Last Known Good State） | [最後の既知の良い状態をキャッシュする（Cache Last Known Good State）] チェックボックスをオンにしている場合のみ該当します。Cisco ISE は、このフィールドに指定した期間にわたり、ポスチャ評価の結果をキャッシュします。有効な値は、1 ～ 30 日、1 ～ 720 時間、または 1 ～ 43200 分です。 |

**関連トピック**

- ポスチャ サービス
- ポスチャ管理の設定
- ポスチャのリース
- Cisco ISE でのポスチャ セッション サービスの有効化
- 指定した時間内で修復するためのクライアントの修復タイマーの設定
- クライアントの遷移のためのネットワーク遷移遅延タイマーの設定
- ログイン成功ウィンドウを自動的に閉じる設定
- 非エージェント デバイスへのポスチャ ステータスの設定

# ポスチャ再評価の構成設定

次の表では、ポスチャ再評価の設定に使用できる [ポスチャ再評価設定（Posture Reassessment Configurations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[再評価（Reassessments）]** です。

**表 *23* : ポスチャ再評価の構成設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 構成名 | PRA 設定の名前を入力します。 |
| 設定の説明（Configuration Description） | PRA 設定の説明を入力します。 |
| 再評価適用を使用?（Use Reassessment Enforcement?） | ユーザ ID グループの PRA 設定を適用するには、チェックボックスをオンにします。 |

| フィールド | 使用上のガイドライン |
| --- | --- |
| 適用タイプ（Enforcement Type） | 適用する次のアクションを選択します。<br>• [続行（Continue）]：ユーザはポスチャ要件に関係なくクライアントを修復できるようにユーザ介入なしの特権アクセスが引き続き提供されます。<br>• [ログオフ（Logoff）]：クライアントが非準拠の場合、ユーザを強制的にネットワークからログオフします。 クライアントが再度ログインしたときのコンプライアンス ステータスは不明です。<br>• [修復（Remediate）]：クライアントが非準拠の場合、エージェントは修復のために指定の期間待機します。 クライアントが修復された後、エージェントはポリシー サービス ノードにPRA レポートを送信します。修復がクライアントで無視された場合、エージェントはクライアントにネットワークからログオフすることを強制するために、ポリシー サービス ノードにログオフ要求を送信します。<br>ポスチャ要件が [必須（mandatory）] に設定されている場合、RADIUS セッションはPRA 障害アクションの結果としてクリアされ、クライアントを再びポスチャするには新しい RADIUS セッションを開始する必要があります。<br>ポスチャ要件が [任意（Optional）] に設定されている場合、クライアント上のエージェントではユーザがエージェントから [続行（Continue）] オプションをクリックできます。ユーザは、制限なしで現在のネットワークにとどまることができます。 |
| インターバル（Interval | 最初のログイン成功後にクライアントで PRA を開始する間隔を分単位で入力します。<br>デフォルト値は 240 分です。最小値は 60 分、最大値は 1440 分です。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 猶予時間（Grace time） | クライアントが修復を完了することのできる時間間隔を分単位で入力します。猶予時間をゼロにすることはできません。また、PRA 間隔より大きくする必要があります。デフォルトの最小間隔（5 分）から最小 PRA 間隔までの範囲にすることができます。<br>最小値は 5 分、最大値は 60 分です。<br>（注） 猶予時間は、クライアントがポスチャの再評価に失敗した後、適用タイプが修復アクションに設定されている場合にだけ有効です。 |
| ユーザ ID グループの選択（Select User Identity Groups） | PRA設定に対して一意のグループまたはグループの一意の組み合わせを選択します。 |
| PRA の設定（PRA configurations） | 既存の PRA 設定と PRA 設定に関連付けられたユーザ ID グループを表示します。 |

**関連トピック**

- ポスチャのリース
- 定期的再評価
- ポスチャ評価オプション
- ポスチャ修復オプション
- ポスチャのカスタム条件
- カスタム ポスチャ修復アクション
- 定期的再評価の設定

# ポスチャの利用規定の構成設定

次の表では、ポスチャのアクセプタブルユース ポリシーを設定するために使用できるポスチャの [利用規定設定（Acceptable Use Policy Configurations）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [利用規定（Acceptable Use Policy）]** です。

**表 *24 :* ポスチャ *AUP* の設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 構成名 | ユーザが作成する AUP 設定の名前を入力します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 設定の説明（Configuration Description） | ユーザが作成するAUP設定の説明を入力します。 |
| エージェントユーザへのAUPの表示（Windowsの場合のみ） | オンにした場合、[エージェントユーザへのAUPの表示（Show AUP to Agent users）]チェックボックスはユーザ（Windowsのみ）にネットワークの利用規約へのリンクを表示し、それをクリックすると、認証およびポスチャ評価が成功したときにAUPが表示されます。 |
| AUPメッセージのURLを使用（Use URL for AUP message）オプション ボタン | 選択した場合、認証およびポスチャ評価が成功したときにクライアントがアクセスする必要があるAUPメッセージへのURLをAUP URLに入力する必要があります。 |
| AUPメッセージのファイルを使用（Use file for AUP message）オプション ボタン | 選択した場合、場所を参照し、トップ レベルにindex.htmlを含むAUPファイルにジップ形式のファイルをアップロードします。<br>.zipファイルには、index.htmlファイルに加えて、他のファイルおよびサブディレクトリを含めることができます。これらのファイルは、HTMLタグを使用して相互に参照できます。 |
| AUP URL | クライアントは認証およびポスチャ評価が成功したときにアクセスする必要があるAUPへのURLを入力します。 |
| AUPファイル（AUP File） | [AUPファイル（AUP File）]で、ファイルを参照し、Cisco ISEサーバにアップロードします。これはzip形式のファイルで、zip形式のファイルではトップ レベルにindex.htmlファイルを含める必要があります。 |

| フィールド | 使用上のガイドライン |
|---|---|
| ユーザ ID グループの選択（Select User Identity Groups） | [ユーザ ID グループの選択（Select User Identity Groups）] ドロップダウン リストで、AUP 設定の一意のユーザ ID グループまたはユーザ ID グループの一意の組み合わせを選択します。<br><br>AUP 設定を作成する場合は、次の点に注意してください。<br><br>• ポスチャ AUP は、ゲスト フローには適用できません。<br><br>• 各設定には、一意のユーザ ID グループ、またはユーザ ID グループの一意の組み合わせが必要です。<br><br>• 2 つの設定が共通のユーザ ID グループを持つことはできません。<br><br>• ユーザ ID グループ「Any」で AUP 設定を作成する場合は、まず他のすべての AUP 設定を削除します。<br><br>• ユーザ ID グループ「Any」を使用して AUP 設定を作成した場合、一意のユーザ ID グループ、または複数のユーザ ID グループを使用して他の AUP 設定を作成することはできません。Any 以外のユーザ ID グループを使用して AUP 設定を作成するには、最初にユーザ ID グループ「Any」を使用した既存の AUP 設定を削除するか、ユーザ ID グループ「Any」を使用した既存の AUP 設定を一意のユーザ ID グループまたは複数のユーザの ID グループを使用して更新します。 |
| 利用規定設定 - 設定リスト（Acceptable use policy configurations—Configurations list） | 既存の AUP 設定と AUP 設定に関連付けられたエンドユーザ ID グループを一覧表示します。 |

**関連トピック**

ポスチャ サービス
ポスチャ評価の利用規定の設定

# EAP-FAST 設定

次の表に、EAP-FAST、EAP-TLS、およびPEAPプロトコルを設定するために使用できる[プロトコル設定（Protocol Settings）]ページのフィールドを示します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[EAP-FAST]** > **[EAP-FAST 設定（EAP-FAST Settings）]** です。

**表 *25 : EAP-FAST* の設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 機関識別情報の説明（Authority Identity Info Description） | クレデンシャルをクライアントに送信する Cisco ISE ノードを説明したわかりやすい文字列を入力します。クライアントは、この文字列をタイプ、長さ、および値（TLV）の Protected Access Credentials（PAC）情報で認識できます。デフォルト値は、Identity Services Engine です。 |
| マスター キー生成期間（Master Key Generation Period） | プライマリキー生成期間を、秒、分、時間、日、または週単位で指定します。値は、1 ～ 2147040000 秒の正の整数である必要があります。デフォルトは 604800 秒で、これは 1 週間と同等です。 |
| すべてのマスター キーおよび PAC の失効（Revoke all master keys and PACs） | すべてのプライマリキーと PAC を失効させるには、[失効（Revoke）] をクリックします。 |
| PAC なしセッション再開の有効化（Enable PAC-less Session Resume） | PAC ファイルなしで EAP-FAST を使用する場合は、このチェックボックスをオンにします。 |
| PAC なしセッションのタイムアウト（PAC-less Session Timeout） | PAC なしセッションの再開がタイムアウトするまでの時間を秒単位で指定します。デフォルトは 7200 秒です。 |

**関連トピック**

ポリシー セット プロトコルの設定
プロトコルとして EAP-FAST を使用するためのガイドライン
EAP-FAST の利点
EAP-FAST の設定

# PAC の設定

次の表では、[PAC の生成（Generate PAC）] ページ上のフィールドについて説明します。これらのフィールドを使用して、EAP-FAST 認証用の Protected Access Credentials を設定します。このページのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定**

（**Settings**）] > **[プロトコル（Protocols）]** > **[EAP-FAST]** > **[PAC の生成（Generate PAC）]** です。

表 *26 : EAP-FAST* の *PAC* の生成の設定

| フィールド | 使用上のガイドライン |
|---|---|
| トンネル PAC（Tunnel PAC） | トンネル PAC を生成するには、このオプション ボタンをクリックします。 |
| マシン PAC（Machine PAC） | マシン PAC を生成するには、このオプション ボタンをクリックします。 |
| TrustSec PAC | TrustSec PAC を生成するには、このオプション ボタンをクリックします。 |
| ID（Identity） | （トンネル PAC およびマシン PAC の ID フィールド用）EAP-FAST プロトコルによって「内部ユーザ名」として示されるユーザ名またはマシン名を指定します。ID 文字列がそのユーザ名と一致しない場合、認証は失敗します。これは、適応型セキュリティ アプライアンス（ASA）で定義されているホスト名です。ID 文字列は、ASA ホスト名に一致する必要があります。一致しない場合、ASA は生成された PAC ファイルをインポートできません。TrustSec PAC を生成する場合、[ID（Identity）] フィールドにより TrustSec ネットワーク デバイスのデバイス ID が指定され、EAP-FAST プロトコルによりイニシエータ ID とともに提供されます。ここに入力した ID 文字列がそのデバイス ID に一致しない場合、認証は失敗します。 |
| PAC 存続可能時間（PAC Time To Live） | （トンネル PAC およびマシン PAC 用）PAC の有効期限を指定する値を秒単位で入力します。デフォルトは 604800 秒で、これは 1 週間と同等です。この値は、1 ～ 157680000 秒の正の整数である必要があります。TrustSec PAC に対しては、日、週、月、または年単位で値を入力します。デフォルト値は 1 年です。最小値は 1 日、最大値は 10 年です。 |
| 暗号化キー（Encryption Key） | 暗号キーを入力します。キーの長さは 8 ～ 256 文字にする必要があります。キーはアルファベットの大文字または小文字、数字、または英数字の組み合わせを含むことができます。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 期限日（Expiration Date） | （TrustSec PAC のみ）有効期限は、PAC 存続可能時間に基づいて計算されます。 |

**関連トピック**

ポリシー セット プロトコルの設定
プロトコルとして EAP-FAST を使用するためのガイドライン
EAP-FAST の PAC の生成

# EAP-TTLS 設定

次の表では、[EAP-TTLS設定（EAP-TTLS Settings）]ページのフィールドについて説明します。このページへのナビゲーション パスは、[管理（Administration）]>[システム（System）]>[設定（Settings）]>[プロトコル（Protocols）]>[EAP-TTLS] です。

**表 *27 : EAP-TTLS* 設定**

| フィールド | 使用上のガイドライン |
|---|---|
| EAP-TTLSセッションの再開を有効にする（Enable EAP-TTLS Session Resume） | このチェックボックスをオンにすると、Cisco ISE はユーザが EAP-TTLS 認証のフェーズ 2 で正常に認証された場合に限り、EAP-TTLS 認証のフェーズ 1 で作成された TLS セッションをキャッシュします。ユーザが再接続しようとする場合、元の EAP-TTLS セッションがタイムアウトしていなければ、Cisco ISE はキャッシュされた TLS セッションを使用します。このため、EAP-TTLS のパフォーマンスが向上し、AAA サーバの負荷が軽減されます。<br>（注） EAP-TTLS セッションが再開されると、内部方式はスキップされます。 |
| EAP-TTLSセッションタイムアウト（EAP-TTLS Session Timeout） | EAP-TTLS セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。 |

**関連トピック**

ポリシー セット プロトコルの設定
認証プロトコルとしての EAP-TTLS の使用
EAP-TLS の設定

# EAP-TLS 設定

次の表に、EAP-TLS プロトコル設定を行うために使用できる [EAP-TLS 設定（EAP-TLS Settings）] ページのフィールドを示します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[EAP-TLS]** です。

表 *28 : EAP-TLS* 設定

| フィールド | 使用上のガイドライン |
|---|---|
| **EAP-TLS セッションの再開を有効にする（Enable EAP-TLS Session Resume）** | 完全な EAP-TLS 認証に成功したユーザの簡略化された再認証をサポートする場合にオンにします。この機能により、Secure Sockets Layer（SSL）ハンドシェイクのみでユーザの再認証が可能となり、証明書の適用が不要になります。EAP-TLS セッションは、タイムアウトしていない限り動作を再開します。 |
| **EAP-TLS セッション タイムアウト（EAP-TLS Session Timeout）** | EAP-TLS セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。 |
| **[ステートレス セッション再開（Stateless Session Resume）]** | |
| **マスター キー生成期間（Master Key Generation Period）** | プライマリキー再生成までの時間を入力します。この値により、プライマリキーがアクティブである期間が決定します。この値は秒、分、時、日数、または週数で入力できます。 |
| **[取り消し（Revoke）]** | これまでに生成されたすべてのプライマリキーとチケットをキャンセルするには、[取り消し（Revoke）] をクリックします。このオプションは、セカンダリ ノードでは無効です。 |

**関連トピック**

ポリシー セット プロトコルの設定

EAP-TLS の設定

# PEAP 設定

次の表では、PEAP プロトコル設定を行うために使用できる [PEAP 設定（PEAP Settings）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[プロトコル（Protocols）]** > **[PEAP]** です。

表 *29 : PEAP* 設定

| フィールド | 使用上のガイドライン |
|---|---|
| PEAP セッションの再開を有効にする（Enable PEAP Session Resume） | このチェックボックスをオンにすると、Cisco ISE はユーザが PEAP 認証のフェーズ 2 で正常に認証された場合に限り、PEAP 認証のフェーズ 1 で作成された TLS セッションをキャッシュします。ユーザが再接続しようとする場合、元の PEAP セッションがタイムアウトしていなければ、Cisco ISE はキャッシュされた TLS セッションを使用します。このため、PEAP のパフォーマンスが向上し、AAA サーバの負荷が軽減されます。PEAP セッション再開機能を動作させるには、PEAP セッション タイムアウト値を指定する必要があります。 |
| PEAP セッション タイムアウト（PEAP Session Timeout） | PEAP セッションがタイムアウトするまでの時間を秒単位で指定します。デフォルト値は 7200 秒です。 |
| 高速再接続を有効にする（Enable Fast Reconnect） | このチェックボックスをオンにすると、セッション再開機能が有効な場合に、ユーザ クレデンシャルを確認しないで PEAP セッションが Cisco ISE で再開することが許可されます。 |

**関連トピック**

ポリシー セット プロトコルの設定
PEAP の設定
PEAP の使用の利点
PEAP プロトコルでサポートされているサプリカント
PEAP プロトコルのフロー

# RADIUS 設定

次の表に、[RADIUS 設定（RADIUS Settings）] ページにある各フィールドの説明を示します。このページへのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [RADIUS]** です。

[繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）] オプションを有効にすると、認証が繰り返し失敗するクライアントは監査ログに出力されず、指定された期間にわたってこれらのクライアントからの要求が自動的に拒否されます。また、認証失敗回数を指定できます。失敗回数がこの回数を超えると、これらのクライアントからの要求は拒否されます。たとえばこの値を 5 に設定すると、クライアント認証が 5 回失敗した場合、指定された期間にわたってそのクライアントから受信する要求はすべて拒否されます。

（注） 認証失敗の原因が誤ったパスワードの入力である場合、クライアントは抑制されません。

**表 *30 : RADIUS* 設定**

| フィールド | 使用上のガイドライン |
|---|---|
| **[繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）]** | |
| [繰り返し失敗するクライアントの抑制（Suppress Repeated Failed Clients）] | 同じ理由で繰り返し認証に失敗するクライアントを抑止するには、このチェックボックスをオンにします。これらのクライアントは監査ログに出力されず、また [繰り返し失敗したクライアントからの RADIUS 要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）] オプションが有効な場合には、指定された期間にわたってこれらのクライアントからの要求が拒否されます。 |
| [2 回の失敗を検出する期間（Detect Two Failures Within）] | 分単位で時間間隔を入力します。クライアントがこの期間内に同じ理由で 2 回認証に失敗すると、監査ログに出力されず、また [繰り返し失敗したクライアントからの RADIUS 要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）] オプションが有効な場合には、指定された期間にわたってこのクライアントからの要求が拒否されます。 |
| [失敗を報告する間隔（Report Failures Once Every）] | 報告対象の認証失敗の時間間隔を分単位で入力します。たとえば、この値を 15 分に設定すると、繰り返し認証に失敗するクライアントが 15 分に 1 回だけ監査ログに報告されるため、報告の重複が防止されます。 |
| [繰り返し失敗したクライアントからの RADIUS 要求を拒否する（Reject RADIUS Requests from Clients with Repeated Failures）] | 認証が繰り返し失敗するクライアントからの RADIUS 要求を自動的に拒否するには、このチェック ボックスをオンにします。Cisco ISE による不要な処理を防ぎ、Denial of Service（DoS）攻撃から防御するには、このオプションを有効にします。 |

| フィールド | 使用上のガイドライン |
|---|---|
| [自動拒否前の失敗回数（Failures Prior to Automatic Rejection）] | 認証失敗回数を入力します。認証失敗回数がこの値を超えると、繰り返し失敗するクライアントからの要求は自動的に拒否されます。設定されている期間（[要求を拒否する期間（Continue Rejecting Requests for）] で指定）にわたり、これらのクライアントから受信する要求はすべて自動的に拒否されます。この期間が経過した後では、これらのクライアントからの認証要求が処理されます。 |
| [要求を拒否する期間（Continue Rejecting Requests for）] | 繰り返し失敗するクライアントからの要求を拒否する時間間隔を分単位で入力します。 |
| [繰り返し発生するアカウンティング更新を無視する期間（Ignore Repeated Accounting Updates Within）] | この期間内に繰り返し発生するアカウンティング更新は無視されます。 |
| **[成功レポートの抑制（Suppress Successful Reports）]** | |
| 繰り返される認証成功の抑制（Suppress Repeated Successful Authentications） | 直近の 24 時間で、ID、ネットワーク デバイス、および許可のコンテキストに変更がない認証要求成功が繰り返し報告されないようにするには、このチェックボックスをオンにします。 |
| **[認証の詳細（Authentications Details）]** | |
| [次よりも長いステップを強調表示（Highlight Steps Longer Than）] | ミリ秒単位で時間間隔を入力します。1つのステップの実行が指定のしきい値を超えると、認証詳細ページでそのステップがクロック アイコンでマークされます。 |
| **[高レートなRADIUS要求を検出する（Detect High Rate of RADIUS Requests）]** | |
| [定常的に高レートなRADIUS要求を検出する（Detect Steady High Rate of Radius Requests）] | [RADIUS要求の期間（Duration of RADIUS requests）] および [RADIUS要求の合計数（Total number of RADIUS requests）] フィールドで指定した上限を超える場合に、高レートな RADIUS 要求負荷のアラームを発生させる場合は、このチェックボックスをオンにします。 |
| [RADIUS要求の期間（Duration of RADIUS Requests）] | RADIUS のレートを計算するために使用する期間（秒単位）を入力します。デフォルトは 60 秒です。有効な範囲は 20 ～ 86400 秒です。 |

| フィールド | 使用上のガイドライン |
|---|---|
| [RADIUS要求の合計数（Total Number of RADIUS Requests）] | RADIUS のレートを計算するために使用される要求の上限を入力します。デフォルトの要求数は 72000 です。要求数の有効な範囲は 24000 ～ 103680000 で d す。 |
| **RADIUS UDP ポート** | |
| 認証ポート（Authentication Port） | RADIUS UDP の認証フローに使用するポートを指定します。最大 4 つのポート番号（カンマ区切り）を指定できます。デフォルトでは、ポート 1812 とポート 1645 が使用されます。値の範囲は 1024 ～ 65535 です。 |
| アカウンティング ポート（Accounting Port） | RADIUS UDP のアカウンティング フローに使用するポートを指定します。最大 4 つのポート番号（カンマ区切り）を指定できます。デフォルトでは、ポート 1813 とポート 1646 が使用されます。値の範囲は 1024 ～ 65535 です。<br>（注） これらのポートが他のサービスにより使用されていないことを確認します。 |
| **RADIUS DTLS** | |
| 認証およびアカウンティング ポート（Authentication and Accounting Port） | RADIUS DTLS の認証およびアカウンティング フローに使用するポートを指定します。デフォルトでは、ポート 2083 が使用されます。値の範囲は 1024 ～ 65535 です。<br>（注） このポートが他のサービスにより使用されていないことを確認します。 |
| アイドル タイムアウト | パケットがネットワーク デバイスから届かなかったら、TLS セッションを終了する前に、Cisco ISE を待機する時間を秒単位で入力します。デフォルト値は 120 秒です。有効な範囲は 60 ～ 600 秒です。 |

| フィールド | 使用上のガイドライン |
|---|---|
| RADIUS/DTLS クライアント ID 検証の有効化（Enable RADIUS/DTLS Client Identity Verification） | Cisco ISE が DTLS ハンドシェイク中に RADIUS/DTLS クライアントの ID を確認するようにする場合は、このチェックボックスをオンにします。クライアント ID が有効でない場合、Cisco ISE はハンドシェイクに失敗します。デフォルトのネットワーク デバイスが設定されている場合、ID チェックはスキップされます。ID チェックは次の順序で実行されます。<br>1. クライアント証明書にサブジェクト代替名（SAN）属性が含まれている場合：<br>• SAN に DNS 名が含まれている場合、証明書に指定されている DNS 名が Cisco ISE のネットワーク デバイスに設定されている DNS 名と比較されます。<br>• SAN に IP アドレスが含まれていて（DNS 名が含まれていない場合）、証明書で指定された IP アドレスが Cisco ISE で設定されているすべてのデバイス IP アドレスと比較されます。<br>2. 証明書に SAN が含まれていない場合、サブジェクト CN は Cisco ISE のネットワーク デバイスに設定されている DNS 名と比較されます。不一致の場合、Cisco ISE はハンドシェイクに失敗します。 |

**関連トピック**

ポリシー セット プロトコルの設定
Cisco ISE の RADIUS プロトコルのサポート
RADIUS の設定

# 一般 TrustSec の設定

Cisco ISE が TrustSec サーバとして機能したり、TrustSec サービスを提供したりするには、グローバル TrustSec 設定を定義します。次の表に、[TrustSec 設定（TrustSec Settings）] ウィンドウのフィールドの説明を示します（([ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [一般TrustSecの設定（General TrustSec Settings）]）。

### TrustSec 展開の確認

このオプションを選択すると、すべてのネットワークデバイスに最新のTrustSecポリシーが展開されているかどうかを確認できます。Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合は [アラーム（Alarms）] ダッシュレット（[ワークセンター（Work Centers）] > [TrustSec] > [ダッシュボード（Dashboard）] および [ホーム（Home）] > [サマリ（Summary）]）にアラームが表示されます。TrustSec ダッシュ ボードに、以下のアラームが表示されます。

- 検証プロセスが開始または完了するたびに、[情報（Info）] アイコンとともにアラームが表示されます。
- 新しい展開要求により検証プロセスがキャンセルされた場合は、[情報（Info）] アイコンとともにアラームが表示されます。
- 検証プロセスがエラーで失敗した場合は、[警告（Warning）] アイコンとともにアラームが表示されます。たとえば、ネットワーク デバイスとの SSH 接続を開けない場合やネットワーク デバイスが使用できない場合、あるいは Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合などです。

[展開の検証（Verify Deployment）] オプションは、次のウィンドウでも使用できます。

- **[ワーク センター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティ グループ（Security Groups）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ ACL（Security Group ACLs）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [送信元ツリー（Source Tree）]**
- **[ワーク センター（Work Centers）] > [TrustSec] > [TrustSec ポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）] > [宛先ツリー（Destination Tree）]**

[すべての展開後に自動検証（Automatic Verification After Every Deploy）]：それぞれの展開後に、Cisco ISE ですべてのネットワーク デバイス上の更新を検証するには、このチェックボックスをオンにします。展開プロセスが完了したら、[展開プロセス後の時間（Time after Deploy Process）] フィールドに指定した時間が経過した後に、検証プロセスが開始されます。

[展開プロセス後の時間（Time after Deploy Process）]：展開プロセスが完了した後、検証プロセスを開始する前に Cisco ISE に待機させる時間を指定します。有効な範囲は、10 ～ 60 分です。

待機期間中に新しい展開が要求された場合や別の検証が進行中の場合は、現在の検証プロセスはキャンセルされます。

[今すぐ検証（Verify Now）]：検証プロセスをすぐに開始するには、このオプションをクリックします。

### Protected Access Credential（PAC）

- [トンネル PAC の存続可能時間（Tunnel PAC Time to Live）]：

  PAC の有効期限を指定します。トンネル PAC は EAP-FAST プロトコル用のトンネルを生成します。時間を秒、分、時、日数、または週数で指定できます。デフォルト値は 90 日です。有効な範囲は次のとおりです。

  - 1 ～ 157680000 秒
  - 1 ～ 2628000 分
  - 1 ～ 43800 時間
  - 1 ～ 1825 日
  - 1 ～ 260 週間

- [プロアクティブ PAC 更新を次の後に実行する（Proactive PAC Update Will Occur After）]：Cisco ISE は、認証に成功した後、設定したパーセンテージのトンネル PAC TTL が残っているときに、新しい PAC をクライアントに予防的に提供します。PAC の期限が切れる前に最初の認証が正常に行われると、サーバはトンネル PAC の更新を開始します。このメカニズムにより、有効な PAC でクライアントが更新されます。デフォルト値は 10% です。

### セキュリティグループタグ番号の割り当て

- [システムで SGT 番号を割り当てる（System will Assign SGT Numbers）]：Cisco ISE に SGT 番号を自動生成させる場合は、このオプションを選択します。
- [範囲内の番号を除外する（Except Numbers In range）]：手動設定用に SGT 番号の範囲を予約する場合は、このオプションを選択します。Cisco ISE は、SGT の生成時にこの範囲の数値を使用しません。
- [ユーザが手動で SGT 番号を入力する（User Must Enter SGT Numbers Manually）]：SGT 番号を手動で定義する場合は、このオプションを選択します。

### APIC EPGのセキュリティグループタグのナンバリング（Security Group Tag Numbering for APIC EPGs）

[APIC EPG 用のセキュリティグループタグの番号付け（Security Group Tag Numbering for APIC EPGs）]：APIC から学習した EPG に基づいて SGT を作成する場合は、このチェックボックスをオンにし、使用する番号の範囲を指定します。

### セキュリティグループの自動作成

[認証ルールを作成するときにセキュリティグループを自動作成する（Auto Create Security Groups When Creating Authorization Rules）]：認可ポリシーのルールを作成する際に SGT を自動的に作成する場合は、このチェックボックスをオンにします。

このオプションを選択した場合は、[認可ポリシー（Authorization Policy）] ウィンドウの上部に、「 自動セキュリティグループの作成がオンです（Auto Security Group Creation is On）」というメッセージが表示されます。

自動作成された SGT は、ルール属性に基づいて命名されます。

（注） 自動作成された SGT は、それに対応する認可ポリシールールを削除しても削除されません。

デフォルトでは、新規インストールまたはアップグレードの後でこのオプションが無効になります。

- [自動命名オプション（Automatic Naming Options）]：自動作成される SGT の命名規則を定義するには、このオプションを使用します。

  （必須）[名前に次が含まれます（Name Will Include）]：次のオプションのいずれかを選択します。

  - **ルール名**
  - **SGT番号（SGT number）**
  - **ルール名およびSGT番号（Rule name and SGT number）**

  デフォルトでは、[ルール名（Rule name）] オプションが選択されます。

  オプションで、SGT 名に以下の情報を追加できます。

  - ポリシーセット名（Policy Set Name）（このオプションは [ポリシーセット（Policy Sets）] が有効な場合にのみ使用可能です）
  - プレフィックス（Prefix）（8 文字まで）
  - サフィックス（Suffix）（8 文字まで）

  Cisco ISE は、選択内容に応じて [サンプル名（Example Name）] フィールドにサンプル SGT 名を表示します。

  同じ名前の SGT が存在している場合、ISE は SGT 名に「*_x*」を付け加えます。*x* は（現在の名前に 1 が使用されていない場合は）1 から始まる最初の値です。新しい名前が 32 文字より長い場合、Cisco ISE によって最初の 32 文字に切り捨てられます。

### ホスト名の IP SGT 静的マッピング

[ホスト名の IP SGT 静的マッピング（IP SGT Static Mapping of Hostnames）]：FQDN とホスト名が使用される場合、Cisco ISE はマッピングを展開して展開状態を検査する際に、PAN および PSN ノード内の対応する IP アドレスを検索します。DNS クエリによって返される IP アドレス用に作成されるマッピングの数を指定する場合は、このオプションを使用します。次のいずれかのオプションを選択できます。

- **DNS クエリによって返されるすべての IP アドレスに対してマッピングを作成する（Create mappings for all IP addresses returned by a DNS query）**
- **DNSクエリによって返される最初のIPv4アドレスおよび最初のIPv6アドレスに対してのみマッピングを作成する（Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query）**

### 関連トピック

TrustSec アーキテクチャ
TrustSec のコンポーネント
TrustSec のグローバル設定

# TrustSec マトリックスの設定

次の表に、[TrustSecマトリックスの設定（TrustSec Matrix Settings）] ページにある各フィールドの説明を示します。このページへのナビゲーションパスは、[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [TrustSecマトリックスの設定（TrustSec Matrix Settings）] です。

**表 *31 : TrustSec* マトリックスの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 複数のSGACLを許可（Allow Multiple SGACLs） | セル内で複数のSGACLを許可するには、このチェックボックスをオンにします。このオプションが選択されていない場合、Cisco ISE はセル 1 つあたり 1 つの SGACL のみを許可します。<br>デフォルトでは、新たにインストールすると、このオプションはディセーブルになります。<br>アップグレード後、Cisco ISE は出力セルをスキャンし、複数の SGACL が割り当てられたセルを少なくとも 1 つ特定した場合、管理者に複数の SGACL をセルに追加することを許可します。それ以外の場合は、セル 1 つあたり 1 つの SGACL のみを許可します。<br>（注） 複数の SGACL を無効にする前に、複数の SGACL を含むセルを 1 つの SGACL のみを含めるように編集する必要があります。 |

| フィールド | 使用上のガイドライン |
|---|---|
| モニタリングの許可（Allow Monitoring） | マトリクス内のすべてのセルのモニタリングをイネーブルにする場合は、このチェックボックスをオンにします。モニタリングがディセーブルの場合、[セルの編集（Edit Cell）] ダイアログで、[すべてをモニタ（Monitor All）] アイコンはグレー表示され、[モニタ（Monitor）] オプションはディセーブルになります。<br>デフォルトでは、新たにインストールすると、モニタリングはディセーブルになります。<br>（注） マトリクス レベルでモニタリングをディセーブルにする前に、現在モニタされているセルのモニタリングをディセーブルにする必要があります。 |
| SGT番号の表示（Show SGT Numbers） | マトリクス セルの SGT 値（10 進数および 16 進数の両方）を表示または非表示にするには、このオプションを使用します。<br>デフォルトでは、SGT 値はセルに表示されます。 |
| アピアランス設定（Appearance Settings） | 次のオプションを使用できます。<br>• [カスタム設定（Custom settings）] : デフォルトのテーマ（パターンなしの色）が最初に表示されます。独自の色とパターンを設定できます。<br>• [デフォルト設定（Default settings）] : パターンなしの色の定義済みリスト（編集不可）。<br>• [アクセシビリティ設定（Accessibility settings）] : パターンありの色の定義済みリスト（編集不可）。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 色/パターン（Color/Pattern） | マトリックスを読み取りやすくするために、セルの内容に基づいて、マトリックスセルに色とパターンを適用できます。<br>使用可能な表示タイプは、次のとおりです。<br>• [IPを許可/IPログを許可（Permit IP/Permit IP Log）]：セル内に設定されます<br>• [IPを拒否/IPログを拒否（Deny IP/Deny IP Log）]：セル内に設定されます<br>• [SGACL（SGACLs）]：セル内に設定されている SGACL 用<br>• [IPを許可/IPログを許可（継承）（Permit IP/Permit IP Log (Inherited)）]：デフォルト ポリシーから取得されます（設定されていないセル用）<br>• [IPを拒否/IPログを拒否（継承）（Deny IP/Deny IP Log (Inherited)）]：デフォルト ポリシーから取得されます（設定されていないセル用）<br>• [SGACL（継承）（SGACLs (Inherited)）]：デフォルトポリシーから取得されます（設定されていないセル用） |

**関連トピック**

出力ポリシー
マトリクス ビュー
TrustSec マトリックスの設定

# SMS ゲートウェイ設定（SMS Gateway Settings）

電子メール サーバ経由でゲストとスポンサーに SMS メッセージを送信するように設定するには、次の設定を使用します。

表 *32 : SMS* 電子メール ゲートウェイの *SMS* ゲートウェイ設定

| フィールド | 使用上のガイドライン |
|---|---|
| SMS ゲートウェイ プロバイダー ドメイン（SMS Gateway Provider Domain） | プロバイダー ドメインと、ゲスト アカウントの携帯電話の番号を入力します。プロバイダーの SMS/MMS ゲートウェイにメッセージを送信するとき、前者が電子メール アドレスのホスト部として使用され、後者はユーザ部分として使用されます。 |
| プロバイダー アカウント アドレス（Provider account address） | （オプション）<br>アカウント アドレスを入力します。これは、電子メールの送信元アドレス（通常、アカウント アドレス）として使用され、**[ゲスト アクセス（Guest Access）] > [設定（Settings）]** の [デフォルトの電子メール アドレス（Default Email Address）] グローバル設定を上書きします。 |
| SMTP API 宛先アドレス（SMTP API destination address） | （オプション）<br>Clickatell SMTP API などの、特定のアカウント受信者アドレスを必要とする SMTP SMS API を使用する場合は、SMTP API 宛先アドレスを入力します。<br>これは、電子メールの送信先アドレスとして使用され、メッセージ本文のテンプレートはゲスト アカウントの携帯電話の番号に置き換えられます。 |
| SMTP API 本文テンプレート（SMTP API body template） | （オプション）<br>Clicketell SMTP API など、SMS の送信に特定の電子メール本文テンプレートを必要とする SMTP SMS API を使用する場合は、SMTP API 本文テンプレートを入力します。<br>サポートされる動的置換は $mobilenumber$、（形式 $YYYYMMDDHHHMISSmimi$ の）$timestamp$、および $message$ です。 URL に固有識別子が必要な SMS ゲートウェイには $timestamp$$mobilenumber$ を使用できます。 |

これらの設定へのナビゲーション パスは、**[ゲスト アクセス（Guest Access）] > [設定（Settings）] > [SMS ゲートウェイ（SMS Gateway）]** です。

HTTP API（GET 方式または POST 方式）でゲストとスポンサーに SMS メッセージを送信するように設定するには、次の設定を使用します。

**表 *33 : SMS HTTP API* 用の *SMS* ゲートウェイ設定（*SMS Gateway Settings for SMS HTTP API*）**

| フィールド | 使用上のガイドライン |
|---|---|
| URL | API の URL を入力します。<br>このフィールドは、符号化された URL ではありません。ゲスト アカウントの携帯電話の番号は、URL に置き換えられます。サポートされる動的置換は $mobilenumber$ および $message$ です。<br>HTTP API で HTTPS を使用した場合、HTTPS を URL 文字列に含め、Cisco ISE にプロバイダーの信頼できる証明書をアップロードします。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。 |
| データ（URL エンコード部分）（Data (Url encoded portion)） | GET 要求または POST 要求のデータ（URL エンコード部分）を入力します。<br>このフィールドは、符号化された URL です。デフォルトの GET 方式を使用している場合、データが上で指定した URL に付加されます。 |
| データ部分に HTTP POST 方式を使用（Use HTTP POST method for data portion） | POST 方式を使用する場合は、このオプションをオンにします。<br>上で指定したデータは、POST 要求の内容として使用されます。 |
| HTTP POST データ コンテンツ タイプ（HTTP POST data content type） | POST 方式を使用する場合は、「plain/text」や「application/xml」などのコンテンツ タイプを指定します。 |
| HTTPS ユーザ名（HTTPS Username）<br>HTTPS パスワード（HTTPS Password）<br>HTTPS ホスト名（HTTPS Host name）<br>HTTPS ポート番号（HTTPS Port number） | この情報を入力します。 |

## 関連トピック

SMS プロバイダーおよびサービス
ゲストに SMS 通知を送信するための SMS ゲートウェイの設定

# DHCP および DNS サービス

これらの設定のためのナビゲーション パスは、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [DHCP および DNS サービス（DHCP & DNS Services）]** です。

認証 VLAN URL リダイレクトのシミュレーションを有効にするために、これらの設定を使用して、DHCP、およびオプションの DNS を設定します。さまざまな ISE ノードに適用するために、複数のスコープを作成できます。1 つの ISE ノードに複数のスコープを適用する場合、同じネットワーク インターフェイスで設定する必要があります。

（注） プロファイリングのために、DHCP プローブを必要とすることがあります。ISE DHCP プローブは認証 VLAN DHCP サービスと同じ UDP ポート 67 を使用します。そのため、DHCP プローブは、異なるインターフェイスで設定される必要があるか、またはこの ISE ノードで無効にすることができます。DHCP プローブの詳細については、DHCP プローブを参照してください。

**表 *34 :* 認証 *VLAN URL* リダイレクトのシミュレーション用の *DHCP* と *DNS* サービスの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| スコープ名 | このスコープの目的を容易に記憶できる名前を入力します。 |
| ステータス | [有効（Enabled）] または [無効（Disabled）] を選択します。有効の場合、スコープは ISE ノードにのみ使用できます。 |
| ISE ノード（ISE Node） | DHCP/DNS サーバとして機能するように ISE ノードを適用します。ドロップダウン リストから、このスコープを使用する ISE ノードを選択します。認証 VLAN は ISE ノード/ネットワーク インターフェイスごとに設定され、2 つのインターフェイスまたは 2 つのノードが同じ VLAN を共有することはできません。 |

| フィールド | 使用上のガイドライン |
|---|---|
| ネットワーク インターフェイス（Network Interface） | 選択した ISE ノードで利用可能なネットワーク インターフェイスは、選択した ISE ノードに基づいて動的にこのドロップダウン リストに表示されます。認証 VLAN は ISE ノード/ネットワーク インターフェイスごとに設定され、2 つのインターフェイスまたは 2 つのノードが同じ VLAN を共有することはできません。DHCP/DNS サーバがリスニングするインターフェイスを選択します。NAD の VLAN IP ヘルパーを設定することによって、複数の VLAN が 1 つのネットワーク インターフェイス カードに接続される可能性があります。IP ヘルパーの設定の詳細については、デバイス用のアドミニストレーション ガイドの指示を参照してください。 |
| ドメイン名（Domain Name） | このスコープで使用する DHCP サーバのドメイン名を入力します。 |
| DHCP アドレス範囲 | ネットワーク定義に基づいて、このスコープに使用可能な DHCP アドレスの範囲を選択します。 |
| サブネット マスク（Subnet mask） | ネットワーク定義に基づいて、このスコープに使用するネットワーク マスクを選択します。 |
| ネットワーク ID（Network ID） | 入力した DHCP の属性に基づいて、Cisco ISE により自動的に決定されます。 |
| 除外アドレス範囲 | ネットワーク定義に基づいて、このスコープに使用すべきでない DHCP アドレスの範囲を選択します。 |
| デフォルト ゲートウェイ | デフォルト ゲートウェイの IP アドレスを入力します。 |
| DHCP リース期間 | DHCP リース期間を定義します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| [DHCP オプション（DHCP options）] | これはオプションのフィールドです。<br>DHCP オプションは、DHCP サーバが DHCP クライアントに渡すことができる追加の設定パラメータです。DHCP オプションにより、ネットワークにアクセスするため、または最終認証前にデバイスをブートストラップする手段として、オプション値に指定されている情報を必要とするデバイス（カメラ、アクセス ポイント、電話）がサポートされます。DHCP サーバは、DHCP 要求メッセージをクライアントから受信すると、(通常）DHCP ACK パケットをクライアントに送信することで応答します。この時点で、サーバは DHCP ACK パケットで設定されているすべてのオプションを転送します。<br>詳細については、次の表の後に続く「DHCP オプション」の項を参照してください。 |
| 外部 DNS サーバ | すべての企業ネットワークにアクセスするための認証を受ける前に、ユーザが認証 VLAN 外の外部ドメインにアクセスできるようにする場合、外部 DNS 名を解決するために DNS サーバの IP アドレスを入力します。 |
| 外部ドメイン | すべての企業ネットワークにアクセスするための認証を受ける前に、ユーザが特定のサイトにアクセスできるようにする場合、これらのフィールドにそれらのサイトのドメイン名を入力します。<br>親ドメインとは別に、ユーザがアクセスする必要があるすべての子ドメインの名前を入力します。 |

### DHCP オプション

ISE で DHCP サービスを設定すると、Auth VLAN に接続するクライアントに特定の DHCP オプションを割り当てることができます。定義する各範囲に複数の DHCP オプションを追加できます。

ドロップダウン リストで選択できるオプションは、RFC 2132 のものです。また、（RFC 2132 から）カスタマイズしたオプションを追加するには、ドロップダウン リストから [カスタム（Custom）] を選択し、オプション コードを入力します。

一般に、最もよく使用される DHCP オプションがいくつかあります。

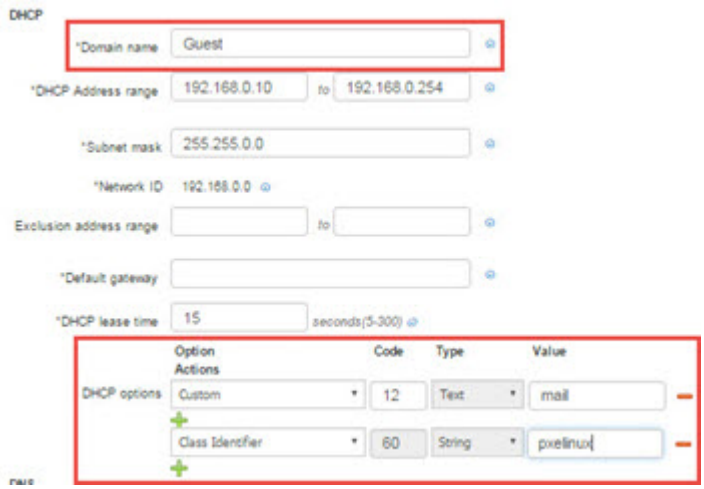
一般的なオプションとしては、次のようなものがあります。

- オプション12（ホスト名）：ノードの完全修飾ドメイン名の「ホスト名」部分を渡すために使用されます。たとえば mail.ise.com の「mail」です。
- オプション 42（NTP サーバ）：ネットワークで使用される NTP サーバを渡します。
- オプション 66（TFTP サーバ）：IP アドレスまたはホスト名を渡すために使用されます。このオプションは、ドロップダウンリストから選択できます。
- オプション 82（DHCP リレー エージェント）：サーバ側 DHCP リレー サーバ情報のその他のサブオプションを渡すために使用されます。

オプション値を定義するには、ドロップダウンリストからオプションを選択します。事前定義の**オプション**を選択すると、コードとタイプが自動的に取り込まれます。

[カスタム（Custom）] を選択して**コード**を入力すると、[タイプ（Type）] が自動的に更新されます。オプションの値を入力します。

**図 *1 : DHCP* オプション**




次に例を示します。

- ホスト名の設定：[オプション（Option）] から [カスタム（Custom）] を選択します。[コード（Code）] に 15 と入力します。[タイプ（Type）] が自動的に [テキスト（Text）] に更新されます。[値（Value）] にホスト名（mail.ise.com の「mail」など）を入力します。
- TFTP サーバ名の設定：[オプション（Option）] から [TFTP サーバ名（TFTP Server Name）] を選択します。[コード（Code）] と [タイプ（Type）] がそれぞれ自動的に更新されます。[値（Value）] に TFTP サーバのホスト名を入力します。

（注） 一部の DHCP オプションは、ISE に対して自動的に定義されているため、手動で入力できません。たとえばオプション 15（ドメイン名）はカスタム オプションとして定義できません。これは、DHCP ドメイン名は、この画面で必須フィールドとして定義されており、上書きできないためです。

複数のオプションを入力するには、[アクション（Actions）]の下のプラス記号をクリックします。

**関連トピック**

Cisco ISE でのサードパーティ ネットワーク デバイスのサポート
Cisco ISE でのサードパーティ製ネットワーク デバイスの設定
DHCP プローブ

# ID の管理

これらのページは、Cisco ISE の ID を設定し、管理することができます。

## エンドポイント

これらのページでは、ネットワークに接続するエンドポイントを設定および管理することができます。

### エンドポイント設定

次の表に、エンドポイントを作成し、エンドポイントにポリシーを割り当てるために使用できる [エンドポイント（Endpoints）] ページのフィールドを示します。このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** です。

**表 *35 :* エンドポイント設定**

| フィールド | 使用上のガイドライン |
|---|---|
| MAC アドレス（MAC Address） | エンドポイントを静的に作成するには、MAC アドレスを 16 進数形式で入力します。<br>MAC アドレスは、Cisco ISE 対応のネットワークに接続するインターフェイスのデバイス ID です。 |

| フィールド | 使用上のガイドライン |
| --- | --- |
| スタティック割り当て（Static Assignment） | [エンドポイント（Endpoints）] ページでエンドポイントを静的に作成する場合このチェックボックスをオンにすると、静的割り当てのステータスが static に設定されます。<br><br>エンドポイントのスタティック割り当てのステータスを静的から動的に、または動的から静的に切り替えできます。 |
| ポリシー割り当て | （スタティック割り当てが選択されていない限り、デフォルトで無効）[ポリシー割り当て（Policy Assignment）] ドロップダウン リストから一致するエンドポイント ポリシーを選択します。<br><br>次のいずれかを実行できます。<br><br>• 一致するエンドポイント ポリシーを選択しないで、デフォルトのエンドポイント ポリシーである不明を使用する場合、スタティック割り当てステータスはエンドポイントに対して動的に設定され、それにより、エンドポイントの動的プロファイリングが可能になります。<br><br>• 不明ではなく、一致するエンドポイント ポリシーを選択する場合、スタティック割り当てステータスはそのエンドポイントに対して静的に設定され、[スタティック割り当て（Static Assignment）] チェックボックスが自動的にオンにされます。 |

| フィールド | 使用上のガイドライン |
| --- | --- |
| スタティック グループ割り当て（Static Group Assignment） | （[スタティック グループ割り当て（Static Group Assignment）] が選択されていない限り、デフォルトで無効）エンドポイントを ID グループに静的に割り当てる場合、このチェックボックスをオンにします。<br><br>このチェックボックスをオンにした場合、プロファイリング サービスは、前に他のエンドポイント ID グループに動的に割り当てられたエンドポイントの次のエンドポイント ポリシーの評価時に、そのエンドポイント ID グループを変更しません。<br><br>このチェックボックスをオフにした場合、エンドポイント ID グループは、ポリシー設定に基づいて ISE プロファイラにより割り当てられたダイナミック グループです。[スタティック グループ割り当て（Static Group Assignment）] オプションを選択しない場合、エンドポイントは、エンドポイント ポリシーの次回評価時に一致する ID グループに自動的に割り当てられます。 |

| フィールド | 使用上のガイドライン |
|---|---|
| ID グループ割り当て | エンドポイントを割り当てるエンドポイント ID グループを選択します。<br><br>エンドポイントを静的に作成する場合、またはエンドポイントのエンドポイント ポリシーの評価時に [一致する ID グループの作成（Create Matching Identity Group）] オプションを使用しない場合は、エンドポイントを ID グループに割り当てることができます。<br><br>Cisco ISE には、次のシステムによって作成された次のエンドポイント ID グループがあります。<br>• ブラックリスト<br>• GuestEndpoints<br>• プロファイル済み<br>  • Cisco IP-Phone<br>  • ワークステーション<br>• RegisteredDevices<br>• 不明 |

**関連トピック**

識別されたエンドポイント
ポリシーおよび ID グループのスタティック割り当てによるエンドポイントの作成

## エンドポイントの LDAP からのインポートの設定

次の表では、LDAP サーバからのエンドポイントのインポートに使用できる [LDAP からのインポート（Import from LDAP）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[ワーク センター（Work Centers）]** > **[ネットワーク アクセス（Network Access）]** > **[ID（Identities）]** > **[エンドポイント（Endpoints）]** です。

**表 *36* : エンドポイントの *LDAP* からのインポートの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 接続の設定 | |
| ホスト | LDAP サーバのホスト名または IP アドレスを入力します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| [ポート（Port）] | LDAP サーバのポート番号を入力します。デフォルト ポート 389 を使用して LDAP サーバからインポートするか、デフォルト ポート 636 を使用して SSL を介して LDAP サーバからインポートできます。<br>（注） Cisco ISE では、任意の設定済みポート番号をサポートします。設定済みの値は、LDAP サーバ接続詳細に一致する必要があります。 |
| セキュア接続を有効にする（Enable Secure Connection） | SSL を介して LDAP サーバからインポートするには、[セキュア接続を有効にする（Enable Secure Connection）] チェックボックスをオンにします。 |
| ルート CA 証明書名 | ドロップダウン矢印をクリックして、信頼できる CA 証明書を表示します。<br>ルート CA 証明書名は、LDAP サーバに接続する場合に必要となる信頼できる CA 証明書を指します。Cisco ISE 内の CA 証明書は、追加（インポート）、編集、削除、およびエクスポートが可能です。 |
| 匿名バインド（Anonymous Bind） | 匿名バインドを有効にするには、[匿名バインド（Anonymous Bind）] チェックボックスをオンにします。<br>[匿名バインド（Anonymous Bind）] チェックボックスをオンにするか、または slapd.conf コンフィギュレーション ファイルの LDAP 管理者クレデンシャルを入力する必要があります。 |
| 管理者 DN（Admin DN） | slapd.conf コンフィギュレーション ファイルで LDAP 管理者に設定されている識別名（DN）を入力します。<br>管理者 DN フォーマット例：cn=Admin, dc=cisco.com, dc=com |
| [パスワード（Password）] | LDAP 管理者に設定されたパスワードを slapd.conf コンフィギュレーション ファイルに入力します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| ベース DN（Base DN） | 親エントリの認定者名を入力します。<br>ベース DN フォーマット例：dc=cisco.com, dc=com |
| クエリ設定（Query Settings） | |
| MAC アドレス objectClass（MAC Address objectClass） | MACアドレスのインポートに使用するクエリ フィルタを入力します。たとえば、ieee802Device です。 |
| MAC アドレス属性名（MAC Address Attribute Name） | インポートに対して返される属性名を入力します。たとえば、macAddress です。 |
| プロファイル属性名（Profile Attribute Name） | LDAP 属性の名前を入力します。この属性は、LDAP サーバで定義されている各エンドポイント エントリのポリシー名を保持します。<br>[プロファイル属性名（Profile Attribute Name）] フィールドを設定する場合は、次の点を考慮してください。<br>• [プロファイル属性名（Profile Attribute Name）] フィールドでこの LDAP 属性を指定しない場合、またはこの属性を誤って設定した場合、インポート操作時にエンドポイントは「不明」としてマークされ、これらのエンドポイントは一致するエンドポイント プロファイリング ポリシーに個別にプロファイリングされます。<br>• [プロファイル属性名（Profile Attribute Name）] フィールドで LDAP 属性を設定した場合、その属性値は、エンドポイント ポリシーが Cisco ISE 内の既存のポリシーに一致することを確認するために検証され、エンドポイントがインポートされます。エンドポイント ポリシーが既存のポリシーと一致しない場合、それらのエンドポイントはインポートされません。 |
| タイムアウト（秒）（Time Out [seconds]） | 時間を秒単位（1 ～ 60 秒）で入力します。 |

**関連トピック**

識別されたエンドポイント

LDAP サーバからのエンドポイントのインポート

# グループ

これらのページでは、エンドポイント ID グループを設定および管理することができます。

## エンドポイント ID グループの設定

次の表に、エンドポイント グループを作成するために使用できる [エンドポイント ID グループ（Endpoint Identity Groups）] ページのフィールドを示します。このページへのナビゲーション パスは、[管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）] です。

**表 *37 :* エンドポイント *ID* グループの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 名前（Name） | 作成するエンドポイント ID グループの名前を入力します。 |
| 説明 | 作成するエンドポイント ID グループの説明を入力します。 |
| 親グループ（Parent Group） | 新しく作成したエンドポイント ID グループを関連付けるエンドポイント ID グループを、[親グループ（Parent Group）] ドロップダウン リストから選択します。 |

**関連トピック**

識別されたエンドポイントの、エンドポイント ID グループでのグループ化
エンドポイント ID グループの作成

# 外部 ID ソース

これらのページでは、Cisco ISE が認証および認可に使用するユーザ データが含まれる外部 ID ソースを設定および管理することができます。

## LDAP ID ソースの設定

次の表では、[LDAP ID ソース（LDAP Identity Sources）] ページのフィールドについて説明します。これらのフィールドを使用して LDAP インスタンスを作成し、これに接続します。このページへのナビゲーション パスは、**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP]** です。

### LDAP 一般設定

以下の表では、[一般（General）] タブのフィールドについて説明します。

表 *38 : LDAP* 一般設定

| フィールド | 使用上のガイドライン |
|---|---|
| 名前（Name） | LDAP インスタンスの名前を入力します。この値は、サブジェクト DN および属性を取得するために検索で使用されます。この値は string 型で、最大長は 64 文字です。 |
| 説明（Description） | LDAP インスタンスの説明を入力します。この値は string 型で、最大長は 1024 文字です。 |
| スキーマ（Schema） | 次の組み込みのスキーマ タイプのいずれかを選択するか、カスタム スキーマを作成できます。<br>• Active Directory<br>• Sun Directory Server<br>• Novell eDirectory<br>[スキーマ（Schema）]の隣の矢印をクリックすると、スキーマの詳細を表示できます。<br>事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。 |
| （注）　次のフィールドは、カスタム スキーマを選択した場合にのみ編集できます。 | |
| サブジェクト オブジェクト クラス（Subject Objectclass） | サブジェクト DN および属性を取得するために検索で使用する値を入力します。この値は string 型で、最大長は 256 文字です。 |
| サブジェクト名属性（Subject Name Attribute） | 要求内のユーザ名を含む属性の名前を入力します。この値は string 型で、最大長は 256 文字です。 |
| グループ名属性（Group Name Attribute） | [グループ名属性（Group Name Attribute）] フィールドに CN または DN またはサポートされる属性を入力します。<br>• CN：共通名に基づいて LDAP ID ストア グループを取得します。<br>• DN：識別名に基づいて LDAP ID ストア グループを取得します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 証明書属性（Certificate Attribute） | 証明書定義を含む属性を入力します。証明書ベースの認証の場合、クライアントによって提示された証明書を検証するために、これらの定義が使用されます。 |
| グループ オブジェクト クラス（Group Objectclass） | グループとして認識されるオブジェクトを指定するために、検索に使用する値を入力します。この値は string 型で、最大長は 256 文字です。 |
| グループ マップ属性（Group Map Attribute） | マッピング情報を含む属性を指定します。この属性は、選択した参照方向に基づいて、ユーザまたはグループ属性を指定できます。 |
| サブジェクト オブジェクトにグループへの参照が含まれる（Subject Objects Contain Reference To Groups） | 所属するグループを指定する属性がサブジェクト オブジェクトに含まれている場合は、このオプション ボタンをクリックします。 |
| グループ オブジェクトにサブジェクトへの参照が含まれる（Group Objects Contain Reference To Subjects） | サブジェクトを指定する属性がグループ オブジェクトに含まれている場合は、このオプション ボタンをクリックします。この値はデフォルト値です。 |
| グループ内のサブジェクトをメンバー属性に保存（Subjects In Groups Are Stored In Member Attribute As） | （[グループ オブジェクトにサブジェクトへの参照が含まれる（Group Objects Contain Reference To Subjects）] オプション ボタンの選択時に限り使用可能）グループ メンバー属性にメンバーが供給される方法を指定します（デフォルトは DN）。 |

| フィールド | 使用上のガイドライン |
|---|---|
| ユーザ情報属性（User Info Attributes） | デフォルトでは、事前設定された属性が次の組み込みのスキーマタイプのユーザ情報（名、姓、電子メール、電話、地域など）を収集するために使用されます。<br>• Active Directory<br>• Sun Directory Server<br>• Novell eDirectory<br>事前定義されたスキーマの属性を編集すると、Cisco ISE が自動的にカスタム スキーマを作成します。<br>[スキーマ（Schema）] ドロップダウン リストから [カスタム（Custom）] オプションを選択し、要件に基づいてユーザ情報の属性を編集することもできます。 |

### LDAP の接続設定

以下の表では、[接続設定（Connection Settings）] タブのフィールドについて説明します。

**表 *39 : LDAP* の接続設定**

| フィールド | 使用上のガイドライン |
|---|---|
| セカンダリ サーバの有効化（Enable Secondary Server） | プライマリ LDAP サーバに障害が発生した場合にバックアップとして使用するセカンダリ LDAP サーバを有効にする場合は、このオプションをオンにします。このチェックボックスをオンにする場合は、セカンダリ LDAP サーバの設定パラメータを入力する必要があります。 |
| プライマリ サーバとセカンダリ サーバ（Primary and Secondary Servers） | |
| ホスト名/IP（Hostname/IP） | LDAP ソフトウェアを実行しているマシンの IP アドレスまたは DNS 名を入力します。ホスト名は 1 ～ 256 文字か、または文字列として表される有効な IP アドレスです。ホスト名の有効な文字は、英数字（a ～ z、A ～ Z、0 ～ 9）、ドット（.）、およびハイフン（-）だけです。 |

| フィールド | 使用上のガイドライン |
| --- | --- |
| ポート（Port） | LDAP サーバがリッスンしている TCP/IP ポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは、LDAP仕様の記述に従って 389 です。ポート番号が不明な場合は、LDAP サーバの管理者からポート番号を取得できます。 |
| 各 ISE ノードのサーバの指定（Specify server for each ISE node） | プライマリおよびセカンダリ LDAP サーバの hostnames/IP および各 PSN のポートを設定するには、このチェック ボックスをオンにします。<br>このオプションを有効にすると、導入のすべてのノードを表示するテーブルが表示されます。ノードを選択し、プライマリおよびセカンダリ LDAP サーバの hostname/IP および選択したノードのポートを設定する必要があります。 |
| アクセス（Access） | [匿名アクセス（Anonymous Access）]：LDAP ディレクトリの検索が匿名で行われるようにする場合にクリックします。サーバではクライアントが区別されず、認証されていないクライアントに対してアクセス可能に設定されているデータへの、クライアント読み取りアクセスが許可されます。認証情報をサーバに送信することを許可する特定のポリシーがない場合、クライアントは匿名接続を使用する必要があります。<br>[認証されたアクセス（Authenticated Access）]：LDAP ディレクトリの検索が管理クレデンシャルによって行われるようにする場合にクリックします。その場合、[管理者 DN（Admin DN）] および [パスワード（Password）] フィールドの情報を入力します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 管理者 DN（Admin DN） | 管理者の DN を入力します。管理者 DN は、[ユーザ ディレクトリ サブツリー（User Directory Subtree）] 下のすべての必要なユーザの検索およびグループの検索を行う権限を持つ LDAP アカウントです。指定した管理者に対して、検索でのグループ名属性の表示が許可されていない場合、該当 LDAP サーバで認証されたユーザのグループ マッピングは失敗します。 |
| パスワード（Password） | LDAP 管理者アカウントのパスワードを入力します。 |
| セキュアな認証（Secure Authentication） | SSL を使用して Cisco ISE とプライマリ LDAP サーバ間の通信を暗号化する場合にクリックします。[ポート（Port）] フィールドに LDAP サーバでの SSL に使用されるポート番号が入力されていることを確認します。このオプションを有効にした場合は、ルート CA を選択する必要があります。 |
| LDAP サーバのルート CA（LDAP Server Root CA） | ドロップダウン リスト ボックスから信頼できるルート認証局を選択して、証明書による安全な認証を有効にします。 |
| サーバ タイムアウト（Server timeout） | プライマリ LDAP サーバでの接続または認証が失敗したと判断する前に Cisco ISE がプライマリ LDAP サーバからの応答を待つ秒数を入力します。有効な値は 1 ～ 99 です。デフォルトは 10 です。 |
| 最大管理接続（Max. Admin Connections） | 特定の LDAP 設定に対して実行できる LDAP 管理者アカウント権限での同時接続の最大数（0 より大きい数）を入力します。これらの接続は、ユーザディレクトリ サブツリーおよびグループディレクトリ サブツリーの下にあるユーザおよびグループのディレクトリの検索に使用されます。有効な値は 1 ～ 99 です。デフォルトは 20 です。 |
| N 秒ごとに再接続（Force reconnect every N seconds） | このチェック ボックスをオンにし、2 つ目のテキスト ボックスに、サーバを指定された間隔で LDAP 接続を更新するための適切な値を入力します。有効な範囲は 1 ～ 60 分です。 |

| フィールド | 使用上のガイドライン |
|---|---|
| サーバへのバインドをテスト（Test Bind To Server） | LDAP サーバの詳細およびクレデンシャルが正常にバインドできることをテストおよび確認する場合にクリックします。テストが失敗した場合は、LDAP サーバの詳細を編集して再テストします。 |
| フェールオーバー | |
| 常にプライマリ サーバに最初にアクセスする（Always Access Primary Server First） | Cisco ISE の認証と認可のために常にプライマリ LDAP サーバに最初にアクセスするように設定するには、このオプションをクリックします。 |
| 経過後にプライマリ サーバにフェールバック（Failback to Primary Server After） | Cisco ISE で接続しようとしたプライマリ LDAP サーバが到達不可能な場合、Cisco ISE はセカンダリ LDAP サーバへの接続を試行します。Cisco ISE に再びプライマリ LDAP サーバを使用するように設定するには、このオプションをクリックし、テキスト ボックスに値を入力します。 |

### [LDAP] の [ディレクトリ構成（Directory Organization）] タブ

次の表では、[ディレクトリ構成（Directory Organization）] タブのフィールドについて説明します。

表 *40 : [LDAP]* の *[*ディレクトリ構成（*Directory Organization*）*]* タブ

| フィールド | 使用上のガイドライン |
|---|---|
| サブジェクト検索ベース（Subject Search Base） | すべてのサブジェクトを含むサブツリーの DN を入力します。次に例を示します。<br>o=corporation.com<br>サブジェクトを含むツリーがベース DN である場合は、LDAP 設定に応じて<br>o=corporation.com<br>または<br>dc=corporation,dc=com<br>と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。 |

| フィールド | 使用上のガイドライン |
| --- | --- |
| グループ検索ベース（Group Search Base） | すべてのグループを含むサブツリーの DN を入力します。次に例を示します。<br>ou = 組織ユニット、ou = 次の組織ユニット、o = corporation.com<br>グループを含むツリーがベース DN である場合は、LDAP 設定に応じて<br>o=corporation.com<br>または<br>dc=corporation,dc=com<br>と入力します。詳細については、LDAP データベースに関するドキュメントを参照してください。 |
| 形式での MAC アドレスの検索（Search for MAC Address in Format） | LDAPデータベースでの検索に使用する、Cisco ISE の MAC アドレス形式を入力します。内部 ID ソースの MAC アドレスは、xx-xx-xx-xx-xx-xx の形式で供給されます。LDAPデータベースのMACアドレスは、異なる形式で供給できます。ただし、Cisco ISE でホスト ルックアップ要求が受信されると、MACアドレスは内部形式からこのフィールドで指定した形式に変換されます。<br>ドロップダウン リストを使用して、特定の形式でのMACアドレスの検索を有効にします。<*format*> は次のいずれかです。<br>• xxxx.xxxx.xxxx<br>• xxxxxxxxxxxx<br>• xx-xx-xx-xx-xx-xx<br>• xx:xx:xx:xx:xx:xx<br>選択する形式は、LDAP サーバに供給されているMACアドレスの形式と一致している必要があります。 |

| フィールド | 使用上のガイドライン |
|---|---|
| サブジェクト名の先頭から最後に出現する区切り文字まで削除（Strip start of subject name up to the last occurrence of the separator） | ユーザ名からドメインプレフィックスを削除するための適切なテキストを入力します。<br><br>ユーザ名の中で、このフィールドに指定した区切り文字が Cisco ISE で検出されると、そのユーザ名の初めから区切り文字までのすべての文字が削除されます。ユーザ名に、<start_string> ボックスに指定した文字が複数含まれている場合は、Cisco ISE によって最後の区切り文字までの文字が削除されます。たとえば、区切り文字がバックスラッシュ（\）で、ユーザ名が DOMAIN\user1 である場合、Cisco ISE によって user1 が LDAP サーバに送信されます。<br><br>（注） <start_string> ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザ名にこれらの文字を使用できません。 |
| 最初に出現する区切り文字からサブジェクト名の末尾まで削除（Strip end of subject name from the first occurrence of the separator） | ユーザ名からドメイン サフィックスを削除するための適切なテキストを入力します。<br><br>ユーザ名の中で、このフィールドに指定した区切り文字が Cisco ISE で検出されると、その区切り文字からユーザ名の末尾までのすべての文字が削除されます。ユーザ名に、このフィールドに指定した文字が複数含まれている場合は、Cisco ISE によって最初の区切り文字から文字が削除されます。たとえば、区切り文字が@で、ユーザ名が *user1@domain* であれば、Cisco ISE は *user1* を LDAP サーバに送信します。<br><br>（注） <*end_string*> ボックスには、特殊文字であるシャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、右山カッコ（>）、および左山カッコ（<）を入力できません。Cisco ISE では、ユーザ名にこれらの文字を使用できません。 |

### LDAP グループ設定

**表 *41 : LDAP* グループ設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 追加（Add） | [追加（Add）] > [グループの追加（Add Group）] を選択して新しいグループを追加するか、[追加（Add）] > [ディレクトリからグループを選択（Select Groups From Directory）] を選択して LDAP ディレクトリからグループを選択します。<br><br>グループの追加を選択した場合は、新しいグループの名前を入力します。ディレクトリから選択する場合は、フィルタ基準を入力し、[グループの取得（Retrieve Groups）] をクリックします。選択するグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。選択したグループが [グループ（Groups）] ページに表示されます。 |

### LDAP 属性設定

**表 *42 : LDAP* 属性設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 追加（Add） | [追加（Add）] > [属性の追加（Add Attribute）] を選択して新しい属性を追加するか、[追加（Add）] > [ディレクトリから属性を選択（Select Attributes From Directory）] を選択して LDAP サーバから属性を選択します。<br><br>属性を追加する場合は、新しい属性の名前を入力します。ディレクトリから選択する場合は、ユーザ名を入力し、[属性の取得（Retrieve Attributes）] をクリックしてユーザの属性を取得します。選択する属性の隣にあるチェックボックスをオンにし、[OK] をクリックします。 |

### LDAP 詳細設定

以下の表では、[詳細設定（Advanced Settings）] タブのフィールドについて説明します。

表 *43 : LDAP* 詳細設定

| フィールド | 使用上のガイドライン |
|---|---|
| [パスワードの変更を有効にする（Enable password change）] | デバイス管理に PAP プロトコルを使用し、ネットワーク アクセスに RADIUS EAP-GTC プロトコルを使用している場合に、パスワードが期限切れになるか、またはパスワードがリセットされるときに、ユーザがパスワードを変更できるようにするには、このチェックボックスをオンにします。サポートされていないプロトコルでは、ユーザ認証が失敗します。このオプションでは、ユーザが次回のログイン時にパスワードを変更できるようにすることもできます。 |

**関連トピック**

LDAP ディレクトリ サービス
LDAP ユーザ認証
LDAP ユーザ ルックアップ
LDAP ID ソースの追加

## RADIUS トークン ID ソースの設定

次の表では、RADIUS 外部 ID ソースを設定し、それに接続するために使用できる [RADIUS トークン ID ソース（RADIUS Token Identity Sources）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RADIUS トークン（RADIUS Token）]** です。

表 *44 : RADIUS* トークン *ID* ソースの設定

| フィールド | 使用上のガイドライン |
|---|---|
| 名前（Name） | RADIUS トークンサーバの名前を入力します。許容最大文字数は 64 文字です。 |
| 説明 | RADIUS トークンサーバの説明を入力します。最大文字数は 1024 です。 |
| SafeWord サーバ（SafeWord Server） | RADIUS ID ソースが SafeWord サーバである場合はこのチェックボックスをオンにします。 |

| フィールド | 使用上のガイドライン |
|---|---|
| セカンダリ サーバの有効化（Enable Secondary Server） | プライマリに障害が発生した場合にバックアップとして使用する Cisco ISE のセカンダリ RADIUS トークン サーバを有効にするには、このチェックボックスをオンにします。このチェックボックスをオンにする場合は、セカンダリ RADIUS トークン サーバを設定する必要があります。 |
| 常にプライマリ サーバに最初にアクセスする（Always Access Primary Server First） | Cisco ISE が常にプライマリ サーバに最初にアクセスするには、このオプション ボタンをクリックします。 |
| 経過後にプライマリ サーバにフォールバック（Fallback to Primary Server after） | プライマリ サーバに到達できない場合に Cisco ISE がセカンダリ RADIUS トークン サーバを使用して認証できる時間（分単位）を指定するには、このオプション ボタンをクリックします。この時間を過ぎると、Cisco ISE はプライマリ サーバに対する認証を再試行します。 |
| **プライマリ サーバ（Primary Server）** | |
| ホスト名/アドレス（Host IP） | プライマリ RADIUS トークン サーバの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用できる文字は、数字とドット（.）です。 |
| 共有秘密鍵（Shared Secret） | この接続のプライマリ RADIUS トークン サーバで設定されている共有秘密を入力します。 |
| 認証ポート（Authentication Port） | プライマリ RADIUS トークン サーバが受信しているポート番号を入力します。 |
| サーバ タイムアウト（Server timeout） | プライマリ サーバがダウンしていると判断する前に Cisco ISE がプライマリ RADIUS トークン サーバからの応答を待つ時間（秒単位）を指定します。 |
| 接続試行回数（Connection Attempts） | セカンダリ サーバ（定義されている場合）に移動する前、またはセカンダリ サーバが定義されていない場合は要求をドロップする前に、Cisco ISE がプライマリ サーバへの再接続を試行する回数を指定します。 |
| **セカンダリ サーバ（Secondary Server）** | |

| フィールド | 使用上のガイドライン |
|---|---|
| ホスト名/アドレス（Host IP） | セカンダリ RADIUS トークン サーバの IP アドレスを入力します。このフィールドには、文字列として表される有効な IP アドレスを入力できます。このフィールドで使用できる文字は、数字とドット（.）です。 |
| 共有秘密鍵（Shared Secret） | この接続のセカンダリ RADIUS トークン サーバで設定されている共有秘密を入力します。 |
| 認証ポート（Authentication Port） | セカンダリ RADIUS トークン サーバが受信しているポート番号を入力します。有効な値は 1 ～ 65,535 です。デフォルトは 1812 です。 |
| サーバ タイムアウト（Server timeout） | セカンダリ サーバがダウンしていると判断する前に Cisco ISE がセカンダリ RADIUS トークン サーバからの応答を待つ時間（秒単位）を指定します。 |
| 接続試行回数（Connection Attempts） | 要求をドロップする前に Cisco ISE がセカンダリ サーバへの再接続を試行する回数を指定します。 |

**関連トピック**

RADIUS トークン ID ソース
RADIUS トークン サーバの追加

# RSA SecurID ID ソースの設定

次の表では、RSA SecurID ID ソースを作成し、それに接続するために使用できる [RSA SecurID ID ソース（RSA SecurID Identity Sources）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [RSA SecurID]** です。

## RSA プロンプトの設定

次の表では、[RSA プロンプト（RSA Prompts）] タブ内のフィールドについて説明します。

**表 *45 : RSA* プロンプトの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| パスコード プロンプトの入力（Enter Passcode Prompt） | パス コードを取得するテキスト文字列を入力します。 |
| 次のトークン コードの入力（Enter Next Token Code） | 次のトークンを要求するテキスト文字列を入力します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| PIN タイプの選択（Choose PIN Type） | PIN タイプを要求するテキスト文字列を入力します。 |
| システム PIN の受け入れ（Accept System PIN） | システム生成の PIN を受け付けるテキスト文字列を入力します。 |
| 英数字 PIN の入力（Enter Alphanumeric PIN） | 英数字 PIN を要求するテキスト文字列を入力します。 |
| 数値 PIN の入力（Enter Numeric PIN） | 数値 PIN を要求するテキスト文字列を入力します。 |
| PIN の再入力（Re-enter PIN） | ユーザに PIN の再入力を要求するテキスト文字列を入力します。 |

### RSA メッセージ設定（RSA Message Settings）

次の表では、[RSA メッセージ（RSA Messages）] タブ内のフィールドについて説明します。

**表 *46 : RSA* メッセージ設定（*RSA Messages Settings*）**

| フィールド | 使用上のガイドライン |
|---|---|
| システム PIN メッセージの表示（Display System PIN Message） | システム PIN メッセージのラベルにするテキスト文字列を入力します。 |
| システム PIN 通知の表示（Display System PIN Reminder） | ユーザに新しい PIN を覚えるように通知するテキスト文字列を入力します。 |
| 数字を入力する必要があるエラー（Must Enter Numeric Error） | PIN には数字のみを入力するようにユーザに指示するメッセージを入力します。 |
| 英数字を入力する必要があるエラー（Must Enter Alpha Error） | PIN には英数字のみを入力するようにユーザに指示するメッセージを入力します。 |
| PIN 受け入れメッセージ（PIN Accepted Message） | ユーザの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。 |
| PIN 拒否メッセージ（PIN Rejected Message） | ユーザの PIN がシステムによって拒否されたときに表示されるメッセージを入力します。 |
| ユーザの PIN が異なるエラー（User Pins Differ Error） | ユーザが不正な PIN を入力したときに表示されるメッセージを入力します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| システム PIN 受け入れメッセージ（System PIN Accepted Message） | ユーザの PIN がシステムによって受け入れられたときに表示されるメッセージを入力します。 |
| 不正パスワード長エラー（Bad Password Length Error） | ユーザが指定した PIN が、PIN 長ポリシーで指定されている範囲に収まらない場合に表示されるメッセージを入力します。 |

**関連トピック**

RSA ID ソース
Cisco ISE と RSA SecurID サーバの統合
RSA ID ソースの追加

# ネットワーク リソース

## ネットワーク デバイス

これらのページを使用すると、ネットワーク デバイスを追加し、管理することができます。

### ネットワーク デバイス定義の設定

次の表は、Cisco ISE のネットワーク アクセス デバイスを設定するために使用できる [ネットワーク デバイス（Network Devices）] ページのフィールドについて説明しています。このページへのナビゲーション パスは、**[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（Network Devices）]** です。

#### ネットワーク デバイスの設定

次の表に、[ネットワーク デバイス（Network Device）] セクションのフィールドを示します。

**表 *47*：ネットワーク デバイスの設定**

| フィールド | 説明 |
|---|---|
| **Name** | ネットワーク デバイスの名前を入力します。<br>ネットワーク デバイスに、デバイスのホスト名とは異なるわかりやすい名前を指定できます。デバイス名は論理識別子です。<br>（注） 一度設定したデバイスの名前は編集できません。 |
| **説明** | デバイスの説明を入力します。 |

| フィールド | 説明 |
|---|---|
| **IP アドレス/IP 範囲（IP Address/IP Ranges）** | 次のいずれかを実行します。<br>• [IP アドレス（IP Address）]：単一の IP アドレス（IPv4 または IPv6 アドレス）とサブネット マスクを入力します。<br>• [IP 範囲（IP Ranges）]：必要な IPv4 アドレス範囲を入力します。[除外（Exclude）] テキスト ボックスに IP アドレスまたは IP アドレス範囲を入力して、認証時に IP アドレスを除外することもできます。<br><br>IP アドレスとサブネットマスクまたは IP アドレス範囲を定義するときに従う必要があるガイドラインを次に示します。<br>• 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。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。<br>• すべてのオクテットの IP アドレス範囲を定義できます。IP アドレスの範囲を指定するときに、ハイフン（-）またはアスタリスク（*）をワイルドカードとして使用できます。たとえば、*.*.*.*、1-10.1-10.1-10.1-10 または 10-11.*.5.10-15 などです。<br>• サブセットがすでに追加されている場合には、設定された範囲からその IP アドレス範囲のサブセットを除外できます。たとえば、10.197.65.*/10.197.65.1 または 10.197.65.* exclude 10.197.65.1 などです。<br>• 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。<br>• 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。 |

| フィールド | 説明 |
|---|---|
| デバイスタイプ（**Device Type**） | ドロップダウン リストをクリックして、ネットワーク デバイスのベンダーを選択します。<br><br>ドロップダウン リストの横にあるツールのヒントを使用して、選択したベンダーのネットワーク デバイスがサポートしているフローおよびサービスと、デバイスで使用されている RADIUS CoA ポートと URL リダイレクトのタイプを表示できます。これらの属性は、デバイス タイプのネットワーク デバイス プロファイルで定義されます。 |
| モデル名（**Model Name**） | ドロップダウン リストをクリックして、デバイス モデルなどを選択します。<br><br>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あります。 |
| ソフトウェア バージョン（**Software Version**） | ドロップダウン リストをクリックして、ネットワーク デバイスで実行するソフトウェアのバージョンを選択します。<br><br>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 ディクショナリにあります。 |
| ネットワーク デバイス グループ（**Network Device Group**） | [ロケーション（Location）] および [デバイス タイプ（Device Type）] ドロップダウン リストをクリックし、ネットワーク デバイスに関連付けることができるロケーションとデバイス タイプを選択します。<br><br>グループを設定するときに、明確にデバイスをグループに割り当てないと、そのデバイスはデフォルトのデバイス グループ（ルート NDG）に含まれます。これにより、ロケーションはすべてのロケーション、デバイス タイプはすべてのデバイス タイプとなり、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。たとえば、すべてのロケーションとすべてのデバイス グループなどです。 |

### RADIUS 認証設定

次の表では、[RADIUS 認証設定（RADIUS Authentication Settings）] セクションのフィールドについて説明します。

表 *48 : RADIUS* 認証設定

| フィールド | 使用上のガイドライン |
|---|---|
| **RADIUS UDP の設定** | |
| **Protocol** | 選択したプロトコルとして RADIUS を表示します。 |
| **共有秘密鍵（Shared Secret）** | ネットワーク デバイスの共有秘密鍵を入力します。<br>共有秘密鍵は、**pac** オプションを指定した **radius-host** コマンドを使用してネットワーク デバイスに設定したキーです。<br>（注） 共有秘密鍵の長さは、[デバイスのセキュリティ設定（Device Security Settings）] ページの [RADIUS 共有秘密鍵の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定された値と同等以上である必要があります（[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）] > [デバイス セキュリティ設定（Device Security Settings）]）。<br>RADIUS サーバでのベスト プラクティスは、22 文字にすることです。新規インストールとアップグレードした展開の場合、デフォルトではこの値は 4 文字であることに注意してください。この値は[デバイスセキュリティ設定（Device Security Settings）] ページで変更できます。 |

| フィールド | 使用上のガイドライン |
| --- | --- |
| **2 番目の共有秘密の使用** | ネットワーク デバイスと Cisco ISE で使用される 2 つの共有秘密（鍵）を指定します。<br>（注） TrustSec デバイスには、デュアル共有秘密（鍵）の利点がありますが、Cisco ISE により送信される TrustSec CoA パケットは常に最初の共有秘密（鍵）を使用します。2 番目の共有秘密の使用を有効にするには、TrustSec デバイスに送信される必要のある TrustSec CoA パケットの送信元の ISE ノードを、**[ワークセンター（Work Centers）] > [デバイス管理（Device 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）] > [追加（Add）] > [TrustSecの詳細設定（Advanced TrustSec Settings）]** ページの [送信元（Send From）] ドロップダウン リストから選択する必要があります。PAN または PSN ノードを選択できます。選択した PSN ノードがダウンした場合、PAN を使用して TrustSec デバイスに TrustSec CoA パケットが送信されます。<br>（注） RADIUS アクセス要求の 2 番目の共有秘密機能は、Message-Authenticator フィールドを含むパケットに対してのみ機能します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| **CoA ポート（CoA Port）** | RADIUS CoA に使用するポートを指定します。<br>デバイスのデフォルトの CoA ポートはネットワーク デバイス プロファイルで定義されます。<br>（注） [RADIUS 認証設定（RADIUS Authentication Settings）] の [ネットワーク デバイス（Network Devices）] ページ（[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）]）で指定した CoA ポートを変更する場合は、[ネットワーク デバイス プロファイル（Network Device Profile）] ページ（[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 プロファイル（Network Device Profiles）]）で対応するプロファイルに同じ CoA ポートを指定します。 |
| **RADIUS DTLS の設定** | |
| **必要な DTLS** | このオプションを有効にすると、Cisco ISE ではこのデバイスからの DTLS 要求だけが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。<br>RADIUS DTLS は SSL トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。 |
| **共有秘密鍵（Shared Secret）** | RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、MD5 整合性チェックを計算するために使用されます。 |
| **CoA ポート（CoA Port）** | RADIUS DTLS CoA に使用するポートを指定します。 |
| **CoA の ISE 証明書の発行元 CA** | ドロップダウン リストから RADIUS DTLS CoA に使用する認証局を選択します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| **DNS 名** | ネットワーク デバイスの DNS 名を入力します。[RADIUS/DTLS クライアント ID 検証の有効化（Enable RADIUS/DTLS Client Identity Verification）] オプションが RADIUS 設定で有効になっている場合、Cisco ISE はこの DNS 名とクライアント証明書で指定されている DNS 名を比較して、ネットワーク デバイスの ID を確認します。 |
| **全般設定** | |
| KeyWrap の有効化（Enable KeyWrap） | ネットワーク デバイスでサポートされる場合にのみ、このチェックボックスをオンにします。これにより、AES KeyWrap アルゴリズムによって RADIUS のセキュリティが強化されます。<br>（注） FIPS モードで Cisco ISE を実行する場合は、ネットワーク デバイス上で KeyWrap を有効にする必要があります。 |
| **キー暗号キー（Key Encryption Key）** | （KeyWrap を有効にしている場合だけ表示されます）セッション暗号化（秘密）に使用される暗号キーを入力します。 |
| **メッセージ オーセンティケータ コード キー（Message Authenticator Code Key）** | （KeyWrap を有効にしている場合だけ表示されます）RADIUS メッセージのキー付き Hashed Message Authentication Code（HMAC）の計算に使用されるキーを入力します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| **キー入力形式（Key Input Format）** | 次の形式のいずれか 1 つを選択します。<br>• [ASCII]：キー暗号キーの長さは 16 文字（バイト）、メッセージ オーセンティケータ コード キーの長さは 20 文字（バイト）である必要があります。<br>• [16 進数（Hexadecimal）]：キー暗号キーの長さは 32 バイトであり、メッセージ オーセンティケータ コード キーの長さは 40 バイトである必要があります。<br><br>Cisco ISE FIPS 暗号キーの入力に使用するキー入力形式を指定します。これは、WLC の設定と一致する必要があります（指定する値はキーの正しい（全体の）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）。 |

### TACACS+ 認証設定

次の表では、ネットワーク デバイスの TACACS+ 認証を設定するために使用できる [ネットワークデバイス（Network Devices）] ページのフィールドについて説明します。ナビゲーション パスは次のとおりです。

- （ネットワーク デバイスの場合）**[ワークセンター（Work Centers）] > [デバイス管理（Device 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）] > [追加（Add）] > [TACACS認証設定（TACACS Authentication Settings）]**。
- （デフォルトのデバイスの場合）**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークリソース（Network Resources）] > [デフォルトのデバイス（Default Devices）] > [TACACS認証設定（TACACS Authentication Settings）]**。詳細については、「デフォルトのネットワーク デバイス定義」を参照してください。

| フィールド | 使用上のガイドライン |
|---|---|
| **共有秘密鍵（Shared Secret）** | TACACS+ プロトコルがイネーブルのときにネットワーク デバイスに割り当てられたテキストの文字列。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前にテキストを入力する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。これは必須フィールドではありません。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 廃止された共有秘密がアクティブです（**Retired Shared Secret is Active**） | リタイアメント期間がアクティブな場合に表示されます。 |
| 廃止（**Retire**） | 既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）] をクリックすると、メッセージ ボックスが表示されます。[はい（Yes）] または [いいえ（No）] をクリックできます。 |
| 残りの廃止期間（**Remaining Retired Period**） | （上のメッセージ ボックスで [はい（Yes）] を選択した場合にのみ利用可能）次のナビゲーション パスで指定されたデフォルト値が表示されます。**[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [設定（Settings）] > [接続設定（Connection Settings）] > [デフォルトの共有秘密リタイアメント期間（Default Shared Secret Retirement Period）]**。デフォルト値は変更することができます。<br><br>これにより、新しい共有秘密を入力でき、古い共有秘密は指定された日数にわたってアクティブなままになります。 |
| 終了（**End**） | （上のメッセージ ボックスで [はい（Yes）] を選択した場合にのみ利用可能）リタイアメント期間が終了し、古い共有秘密が終了します。 |
| シングル接続モードを有効にする（**Enable Single Connect Mode**） | ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを実行します。<br><br>• [レガシーシスコデバイス（Legacy Cisco Devices）]<br><br>• または、[TACACS+ドラフトコンプライアンスシングル接続のサポート（TACACS+ Draft Compliance Single Connect Support）]。シングル接続モードをディセーブルにすると、ISE はすべての TACACS+ 要求に対して新しい TCP 接続を使用します。 |

### SNMP 設定

次の表では、[SNMP 設定（SNMP Settings）] セクションのフィールドについて説明します。

表 *49 : SNMP* 設定

| フィールド | 使用上のガイドライン |
|---|---|
| **SNMP バージョン（SNMP Version）** | [バージョン（Version）] ドロップダウン リストから要求に使用される SNMP のバージョンを選択します。<br>次のバージョンがあります。<br>• 1：SNMPv1 は informs をサポートしていません。<br>• 2c<br>• 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。<br>（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 デバイスが SNMPv1 または SNMPv2c パラメータを使用して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 および 2c で選択された場合のみ）Cisco ISE にデバイスへの特定タイプのアクセスを提供する読み取り専用コミュニティ ストリングを入力します。<br>（注） キャレット記号（曲折アクセント付き^）を使用することはできません。 |

| フィールド | 使用上のガイドライン |
|---|---|
| **SNMP ユーザ名（SNMP Username）** | （SNMP バージョン 3 の場合のみ）SNMP ユーザ名を入力します。 |
| **セキュリティ レベル（Security Level）** | （SNMP バージョン 3 の場合のみ）次からセキュリティ レベルを選択します。<br>• [Auth]：Message Digest 5 またはセキュア ハッシュ アルゴリズム（SHA）パケット認証をイネーブルにします<br>• [No Auth]：認証なし、プライバシーなしのセキュリティ レベル。<br>• [Priv]：データ暗号規格（DES）パケットの暗号化をイネーブルにします |
| **認証プロトコル（Auth Protocol）** | （SNMP バージョン 3 でセキュリティ レベル Auth および Priv を選択した場合のみ）ネットワーク デバイスで使用する認証プロトコルを選択します。<br>認証プロトコルには、Auth および Priv のセキュリティ レベルに対して次のいずれかが含まれます。<br>• MD5<br>• SHA |
| **認証パスワード（Auth Password）** | （SNMP バージョン 3 でセキュリティ レベル Auth および Priv を選択した場合のみ）認証キーを入力します。このキーは 8 文字以上の長さにする必要があります。<br>デバイスにすでに設定されている認証パスワードを表示するには、[表示（Show）] をクリックします。<br>（注） キャレット記号（曲折アクセント付き ^）をパスワードで使用することはできません。 |

| フィールド | 使用上のガイドライン |
|---|---|
| プライバシー プロトコル（**Privacy Protocol**） | （SNMP バージョン 3 でセキュリティ レベル Priv を選択した場合のみ）ネットワーク デバイスで使用するプライバシー プロトコルを選択します。<br>プライバシープロトコルは次のいずれかです。<br>• DES<br>• AES128<br>• AES192<br>• AES256<br>• 3DES |
| プライバシー パスワード（**Privacy Password**） | （SNMP バージョン 3 でセキュリティ レベル Priv を選択した場合のみ）プライバシー キーを入力します。<br>デバイスにすでに設定されているプライバシー パスワードを表示するには、[表示（Show）] をクリックします。<br>（注） キャレット記号（曲折アクセント付き ^）をパスワードで使用することはできません。 |
| ポーリング間隔（**Polling Interval**） | ポーリング間隔を秒単位で入力します。デフォルトは 3600 秒です。 |
| リンク トラップ クエリー（**Link Trap Query**） | SNMP トラップを介して受信する linkup 通知と linkdown 通知を受信して解釈するには、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（**MAC Trap Query**） | SNMP トラップを介して受信する MAC 通知を受信して解釈するには、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 Service Node**） | SNMP データのポーリングに使用される ISE 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。 |

### 高度な TrustSec 設定

次の表は、[高度なTrustSec設定（Advanced TrustSec Settings）] セクションのフィールドについて説明しています。

**表 *50* : 高度な *TrustSec* 設定**

| フィールド | 使用上のガイドライン |
|---|---|
| **HTTP REST API の設定** | |
| **TrustSec デバイスの通知および更新の設定** | |
| **TrustSec ID にデバイス ID を使用（Use Device ID for TrustSec Identification）** | [デバイスID（Device ID）] フィールドにデバイスIDとしてデバイス名をリストするには、このチェックボックスをオンにします。 |
| **デバイスID （Device ID）** | [TrustSec IDにデバイスIDを使用（Use Device ID for TrustSec Identification）] チェックボックスがオンでない場合にのみ、このフィールドにデバイス ID を入力できます。 |
| **[パスワード（Password）]** | TrustSec デバイスを認証するために TrustSec デバイス CLI で設定したパスワードを入力します。<br>TrustSecデバイスの認証に使用されるパスワードを表示するには、[表示（Show）] をクリックします。 |
| **環境データのダウンロード間隔 <...>（Download Environment Data Every <...>）** | デバイスが Cisco ISE から環境データをダウンロードする必要がある時間間隔を指定します。時間を秒、分、時、日、または週で指定できます。デフォルト値は 1 日です。 |
| **ピア許可ポリシーのダウンロード間隔 <...>（Download Peer Authorization Policy Every <...>）** | デバイスが Cisco ISE からピア許可ポリシーをダウンロードする必要がある時間間隔を指定します。時間を秒、分、時、日、または週で指定できます。デフォルト値は 1 日です。 |
| **再認証間隔 <...>（Reauthentication Every <...>）** | 最初の認証後、デバイスが Cisco ISE に対して自身を再認証する時間間隔を指定します。時間を秒、分、時、日、または週で設定できます。たとえば1000秒と入力すると、デバイスは 1000 秒ごとに Cisco ISE に対して自身を認証します。デフォルト値は 1 日です。 |

| フィールド | 使用上のガイドライン |
|---|---|
| **SGACL リストのダウンロード間隔 <...>（Download SGACL Lists Every <...>）** | デバイスが Cisco ISE から SGACL をダウンロードする必要がある時間間隔を指定します。時間を秒、分、時、日、または週で設定できます。デフォルト値は 1 日です。 |
| **その他の TrustSec デバイスでこのデバイスを信頼する（信頼できる TrustSec）（Other TrustSec Devices to Trust This Device (TrustSec Trusted)）** | すべてのピア デバイスでこの TrustSec デバイスを信頼する場合は、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フにした場合、ピア デバイスはこのデバイスを信頼せず、このデバイスから到着したすべてのパケットが適宜色付けまたはタグ付けされます。 |
| **設定変更のデバイスへの送信（Send Configuration Changes to Device）** | Cisco ISE で CoA または CLI（SSH）を使用して TrustSec 設定変更を TrustSec デバイスに送信する場合は、このチェックボックスをオンにします。 |
| **CoA の使用（Using CoA）** | Cisco ISE で CoA を使用して設定変更を TrustSec デバイスに送信する場合は、このオプションを選択します。 |
| **送信元（Send From）** | 設定変更を TrustSec デバイスに送る必要がある送信元 ISE ノードを、このドロップダウンリストから選択します。PAN または PSN ノードを選択できます。選択した PSN ノードがダウンした場合、PSN を使用して TrustSec デバイスに設定変更が送信されます。 |
| **Test Connection** | TrustSec デバイスと選択した ISE ノード（PAN または PSN ノード）の間の接続をテストするには、このオプションを使用できます。 |
| **CLI（SSH）の使用（Using CLI (SSH)）** | Cisco ISE で CLI を使用（SSH 接続を使用）して設定の変更を TrustSec デバイスに送信するには、このオプションを選択します。詳細については、非 CoA サポート デバイスへの設定変更のプッシュを参照してください。 |

| フィールド | 使用上のガイドライン |
|---|---|
| **SSH キー（SSH Key）** | この機能を使用するには、Cisco ISE からネットワーク デバイスへの SSHv2 トンネルを開き、デバイスの CLI を使用して SSH キーを取得します。確認のために、このキーをコピーして [SSHキー（SSH Key）] フィールドに貼り付ける必要があります。詳細については、『』の「SSH キーの検証」のセクションSSH キーの検証を参照してください。 |
| **デバイス設定の展開設定** | |
| **セキュリティ グループ タグ マッピングの展開時にこのデバイスを含める（Include this device when deploying Security Group Tag Mapping Updates）** | この TrustSec デバイスで、デバイス インターフェイス クレデンシャルを使用して IP と SGT の間のマッピングを取得するには、このチェックボックスをオンにします。 |
| **EXEC モード ユーザ名（EXEC Mode Username）** | TrustSec デバイスへのログインに使用す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）** | （省略可能）特権モードで TrustSec デバイスの構成を編集するために使用する有効なパスワードを入力します。 |
| **アウト オブ バンド TrustSec PAC ディスプレイ（Out Of Band TrustSec PAC Display）** | |
| **発行日（Issue Date）** | この TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行日を表示します。 |
| **期限日（Expiration Date）** | この TrustSec デバイス用に Cisco ISE によって生成された最後の TrustSec PAC の有効期限を表示します。 |
| **発行元（Issued By）** | このデバイス用に Cisco ISE によって生成された最後の TrustSec PAC の発行者（TrustSec 管理者）の名前を表示します。 |
| **PAC の生成（Generate PAC）** | TrustSec デバイスのアウト オブ バンド TrustSec PAC を生成するには、このオプションをクリックします。 |

**関連トピック**

Cisco ISE でのネットワークデバイスの定義

Cisco ISE でのサードパーティ ネットワーク デバイスのサポート
ネットワーク デバイス グループ（Network Device Groups）
Cisco ISE でのネットワークデバイスの追加
Cisco ISE でのサードパーティ製ネットワーク デバイスの設定

# デフォルトのネットワーク デバイス定義の設定

次の表に、Cisco ISE が RADIUS または TACACS+ 認証に使用できる、デフォルトのネットワーク デバイスを設定できるようにする [デフォルトのネットワーク デバイス（Default Network device）]ページのフィールドを示します。次のいずれかのナビゲーション パスを選択します。

- **[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）] > [デフォルトのデバイス（Default Devices）]**
- **[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワーク リソース（Network Resources）] > [デフォルトのデバイス（Default Devices）]**

**表 *51* : デフォルトのネットワーク デバイス定義の設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 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） | 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 [有効化（Enable）] を選択します。<br>（注） デフォルトデバイスが有効になっている場合、RADIUS または TACACS+ で認証設定を有効にする必要があります。 |
| デバイス プロファイル | デフォルトのデバイス ベンダーとしてシスコを表示します。 |
| RADIUS 認証設定 | |
| RADIUS の有効化 | デバイスへの RADIUS 認証を有効にする場合は、このチェック ボックスをオンにします。 |
| RADIUS UDP の設定 | |

| フィールド | 使用上のガイドライン |
|---|---|
| 共有秘密鍵（Shared Secret） | 共有秘密を入力します。共有秘密情報の長さは、最大 127 文字です。<br><br>共有秘密鍵は、**pac** オプションを指定した **radius-host** コマンドを使用してネットワーク デバイスに設定したキーです。<br><br>（注） 共有秘密鍵の長さは、[デバイスのセキュリティ設定（Device Security Settings）] ページの [RADIUS 共有秘密鍵の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定された値と同等以上である必要があります（[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）] > [デバイス セキュリティ設定（Device Security Settings）]）。デフォルトでは、この値は新規インストールとアップグレードされた展開用は 4 文字です。RADIUS サーバでのベスト プラクティスは、22 文字にすることです。 |
| RADIUS DTLS の設定 | |
| 必要な DTLS | このオプションを有効にすると、Cisco ISE ではこのデバイスからの DTLS 要求だけが処理されます。このオプションを無効にすると、Cisco ISE ではこのデバイスからの UDP 要求と DTLS 要求の両方が処理されます。<br><br>RADIUS DTLS は SSL トンネルの確立および RADIUS の通信用に強化されたセキュリティを提供します。 |
| 共有秘密鍵（Shared Secret） | RADIUS DTLS に使用される共有秘密鍵が表示されます。この値は固定されており、MD5 整合性チェックを計算するために使用されます。 |
| CoA の ISE 証明書の発行元 CA | ドロップダウン リストから RADIUS DTLS CoA に使用する認証局を選択します。 |
| 全般設定 | |

| フィールド | 使用上のガイドライン |
|---|---|
| KeyWrap の有効化（Enable KeyWrap） | ネットワーク デバイスでサポートされる場合にのみ、このチェックボックスをオンにします。これにより、AES KeyWrap アルゴリズムによって RADIUS のセキュリティが強化されます。<br>FIPS モードで Cisco ISE を実行する場合は、ネットワーク デバイス上で KeyWrap を有効にする必要があります。 |
| キー暗号キー（Key Encryption Key） | KeyWrap を有効にしているときに、セッションの暗号化（秘密）に使用される暗号キーを入力します。 |
| メッセージ オーセンティケータ コード キー（Message Authenticator Code Key） | KeyWrap を有効にしているときに、RADIUS メッセージに対するキー付き Hashed Message Authentication Code（HMAC）の計算に使用されるキーを入力します。 |
| キー入力形式（Key Input Format） | 次の形式のいずれか 1 つを選択します。<br>• [ASCII]：キー暗号キーの長さは 16 文字（バイト）、メッセージ オーセンティケータ コード キーの長さは 20 文字（バイト）である必要があります。<br>• [16 進数（Hexadecimal）]：キー暗号キーの長さは 32 バイトであり、メッセージ オーセンティケータ コード キーの長さは 40 バイトである必要があります。<br>Cisco ISE FIPS 暗号キーの入力に使用するキー入力形式を指定します。これは、WLC の設定と一致する必要があります指定する値はキーの正しい（全体の）長さにする必要があります。それよりも短い値は許可されません。 |
| TACACS 認証設定 | |
| 共有秘密鍵（Shared Secret） | TACACS+ プロトコルがイネーブルのときにネットワーク デバイスに割り当てられたテキストの文字列。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証される前にテキストを入力する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 廃止された共有秘密がアクティブです（Retired Shared Secret is Active） | リタイアメント期間がアクティブな場合に表示されます。 |
| 廃止（Retire） | 既存の共有秘密を終了する代わりに廃止します。[廃止（Retire）] をクリックすると、メッセージ ボックスが表示されます。[はい（Yes）] または [いいえ（No）] をクリックできます。 |
| 残りの廃止期間（Remaining Retired Period） | （上のメッセージ ボックスで [はい（Yes）] を選択した場合にのみ利用可能）次のナビゲーション パスで指定されたデフォルト値が表示されます。**[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [設定（Settings）] > [接続設定（Connection Settings）] > [デフォルトの共有秘密リタイアメント期間（Default Shared Secret Retirement Period）]**。デフォルト値は変更することができます。<br>これにより、新しい共有秘密を入力でき、古い共有秘密は指定された日数にわたってアクティブなままになります。 |
| 終了（End） | （上のメッセージ ボックスで [はい（Yes）] を選択した場合にのみ利用可能）リタイアメント期間が終了し、古い共有秘密が終了します。 |
| シングル接続モードを有効にする（Enable Single Connect Mode） | ネットワーク デバイスとのすべての TACACS+ 通信に単一の TCP 接続を使用する場合にオンにします。次のいずれかを実行します。<br>• [レガシーシスコデバイス（Legacy Cisco Devices）]<br>• または、[TACACS+ドラフトコンプライアンスシングル接続のサポート（TACACS+ Draft Compliance Single Connect Support）]。このオプションをディセーブルにすると、すべての TACACS+ 要求に対して新しい TCP 接続が ISE で使用されます。 |

## デバイス セキュリティ設定

RADIUS 共有秘密の最小長を指定します。新規インストールとアップグレードした展開の場合、デフォルトではこの値は4文字になります。RADIUS サーバでのベストプラクティスは、22 文字にすることです。

（注） [ネットワーク デバイス（Network Devices）] ページに入力した共有秘密の長さは、[デバイス セキュリティ設定（Device Security Settings）] ページの [RADIUS 共有秘密の最小長（Minimum RADIUS Shared Secret Length）] フィールドで設定した値以上でなければなりません。

**関連トピック**

ネットワーク デバイス定義の設定 （100 ページ）

## ネットワーク デバイスのインポート設定

次の表では、ネットワークデバイスの詳細をCisco ISEにインポートするために使用する [ネットワーク デバイス インポート（Network Device Import）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[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（Network Devices）]** です。

**表 *52*：ネットワーク デバイスのインポート設定**

| フィールド | 使用上のガイドライン |
|---|---|
| テンプレートの生成（Generate a Template） | カンマ区切り形式（.csv）テンプレート ファイルを作成するには、このリンクをクリックします。<br>同じ形式のネットワーク デバイス情報でテンプレートを更新し、それらのネットワーク デバイスをCisco ISE展開にインポートするためにローカルで保存します。 |
| ファイル（File） | 作成したか、またはCisco ISE展開から以前にエクスポートしたカンマ区切り形式ファイルの場所を参照するには、[参照（Browse）] をクリックします。<br>インポートを使用して、新しい、更新されたネットワーク デバイス情報を含むネットワーク デバイスを別のCisco ISE展開にインポートできます。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 新しいデータで既存のデータを上書き（Overwrite existing data with new data） | Cisco 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。<br>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。重複エントリは無視されます。 |
| 最初のエラーでインポートを停止（Stop Import on First Error） | インポート中にエラーが発生したときに Cisco ISE にインポートを中止させる場合、このチェックボックスをオンにしますが、Cisco ISE はエラーのその時点までネットワーク デバイスをインポートします。<br>このチェックボックスがオフで、エラーが発生した場合は、エラーが報告され、Cisco ISE はデバイスを引き続きインポートします。 |

**関連トピック**

Cisco ISE でのネットワークデバイスの定義
Cisco ISE でのサードパーティ ネットワーク デバイスのサポート
Cisco ISE へのネットワーク デバイスのインポート

# ネットワーク デバイス グループ（Network Device Groups）

これらのページを使用すると、ネットワーク デバイス グループを設定し、管理することができます。

## ネットワーク デバイス グループの設定

次の表では、ネットワーク デバイス グループを作成するために使用できる [ネットワーク デバイス グループ（Network Device Groups）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[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）] > [グループ（Groups）]** です。

**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワークデバイスグループ（Network Device Groups）] > [グループ（Groups）]** ページでネットワーク デバイス グループを作成することもできます。

表 53 : ネットワーク デバイス グループの設定

| フィールド | 使用上のガイドライン |
|---|---|
| 名前（Name） | ルート ネットワーク デバイス グループ（NDG）の名前を入力します。ルート NDG の下の後続のすべての子ネットワーク デバイス グループに対して、新しいネットワーク デバイス グループの名前を入力します。<br>ルート ノードを含み、最大で 6 つのノードを NDG 階層に含めることができます。各 NDG 名は最大 32 文字です。 |
| 説明 | ルートまたは子のネットワーク デバイス グループの説明を入力します。 |
| 親グループ（Parent Group） | 親グループとして既存のグループを選択するか、ルートグループとして、この新しいグループを追加できます。 |

関連トピック

- ネットワーク デバイス グループ（Network Device Groups）
- ポリシー評価で Cisco ISE が使用するネットワーク デバイスの属性
- Cisco ISE でのネットワークデバイスの追加

## ネットワーク デバイス グループのインポート設定

次の表では、Cisco ISE にネットワーク デバイス グループをインポートするために使用できる [ネットワーク デバイス グループ インポート（Network Device Group Import）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[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）]** > **[グループ（Groups）]** です。

表 54 : ネットワーク デバイス グループのインポート設定

| フィールド | 使用上のガイドライン |
|---|---|
| テンプレートの生成（Generate a Template） | カンマ区切り形式（.csv）テンプレート ファイルを作成するには、このリンクをクリックします。<br>同じ形式のネットワーク デバイス グループ情報でテンプレートを更新し、それらのネットワーク デバイス グループを Cisco ISE 展開にインポートするためにローカルで保存します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| ファイル（File） | 作成したか、またはCisco ISE展開から以前にエクスポートしたカンマ区切り形式ファイルの場所を参照するには、[参照（Browse）] をクリックします。<br><br>インポートを使用して、新しい、更新されたネットワーク デバイス グループ情報を含むネットワーク デバイス グループを別の Cisco ISE 展開にインポートできます。 |
| 新しいデータで既存のデータを上書き（Overwrite existing data with new data） | Cisco 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。<br><br>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。重複エントリは無視されます。 |
| 最初のエラーでインポートを停止（Stop Import on First Error） | インポート中にエラーが発生すると、Cisco ISEにインポートを中止させる場合、このチェックボックスをオンにしますが、Cisco ISE はエラーのその時点までネットワーク デバイス グループをインポートします。<br><br>このチェックボックスがオフで、エラーが発生した場合は、エラーが報告され、Cisco ISE はデバイス グループを引き続きインポートします。 |

**関連トピック**

ネットワーク デバイス グループ（Network Device Groups）
ポリシー評価で Cisco ISE が使用するネットワーク デバイスの属性
Cisco ISE へのネットワーク デバイス グループのインポート

# セッション認識型ネットワーク（SAnet）のサポート

Cisco ISE は、セッション認識型ネットワーキング（SAnet）に対する限定的なサポートを提供します。SAnet は、多くのシスコスイッチで実行するセッション管理フレームワークです。SAnet は、可視性、認証、認可などのアクセスセッションを管理します。SAnet は、RADIUS 認可属性が含まれているサービステンプレートを使用します。Cisco ISE には、認証プロファイル内にサービステンプレートが含まれています。Cisco ISE は、プロファイルを「サービス

テンプレート」互換として識別するフラグを使用して認証プロファイルのサービステンプレートを識別します。

Cisco ISE 認証プロファイルには、属性のリストに変換される RADIUS 認可属性が含まれています。また、SAnet サービステンプレートには、RADIUS 認可属性も含まれていますが、これらの属性はリストに変換されません。

SAnetデバイスの場合、Cisco ISEはサービステンプレートの名前を送信します。キャッシュ内にそのコンテンツか、または静的に定義された設定が存在しない限り、デバイスはサービステンプレートのコンテンツをダウンロードします。サービステンプレートによってRADIUS属性が変更されると、Cisco ISE はデバイスに CoA 通知を送信します。

# ネットワーク デバイス プロファイル設定

次の表は、[ネットワーク デバイス プロファイル（Network Device Profiles）] ページのフィールドについての説明です。このページを使用して、プロトコル、リダイレクトURLおよびCoA設定に対するデバイスのサポートなど、特定のベンダーからのネットワークデバイスのタイプに対するデフォルト設定を構成することができます。その後、プロファイルを使用して特定のネットワーク デバイスを定義します。

このページへのナビゲーション パスは、**[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 プロファイル（Network Device Profiles）]** です。

### ネットワーク デバイス プロファイルの設定

次の表は、[ネットワークデバイスプロファイル（Network Device Profile）]セクションのフィールドについての説明です。

**表 *55 :* ネットワーク デバイス プロファイルの設定**

| フィールド | 説明 |
|---|---|
| 名前（Name）] | ネットワークデバイスプロファイルの名前を入力します。 |
| 説明 | ネットワークデバイスプロファイルの説明を入力します。 |
| アイコン（Icon） | ネットワークデバイスプロファイルに使用するアイコンを選択します。このアイコンには、選択したベンダーのアイコンがデフォルトで設定されます。<br>選択するアイコンは 16 X 16 の PNG ファイルである必要があります。 |

| フィールド | 説明 |
|---|---|
| ベンダー（Vendor） | ネットワーク デバイス プロファイルのベンダーを選択します。<br>選択可能なベンダーは、シスコ、Aruba、HP、Motorola、Brocade、Alcatel などです。 |
| サポートされるプロトコル | |
| RADIUS | このネットワーク デバイス プロファイルが RADIUS をサポートしている場合は、このチェックボックスをオンにします。 |
| TACACS+ | このネットワーク デバイス プロファイルが TACACS+ をサポートしている場合は、このチェックボックスをオンにします。 |
| TrustSec | このネットワーク デバイス プロファイルが TrustSec をサポートしている場合は、このチェックボックスをオンにします。 |
| RADIUS ディクショナリ（RADIUS Dictionaries） | このプロファイルでサポートされる 1 つ以上の RADIUS ディクショナリを選択します。プロファイルを作成する前に、ベンダー固有の RADIUSディクショナリをインポートします。 |

### 認証/許可テンプレートの設定

次の表は、[認証/許可（Authentication/Authorization）] セクションのフィールドについての説明です。

表 *56 :* 認証/許可の設定

| フィールド | 説明 |
|---|---|
| フロータイプの条件（Flow Type Conditions） | Cisco ISE では、802.1X、MAC 認証バイパス（MAB）、およびブラウザベースの Web 認証ログインが、有線ネットワークと無線ネットワークの両方を介した基本的なユーザ認証およびアクセスでサポートされます。<br>このタイプのネットワーク デバイスがサポートする認証ログインのチェックボックスをオンにします。次の 1 つ以上の項目を指定できます。<br>• 有線 MAC 認証バイパス（MAB）（Wired MAC authentication bypass (MAB)）<br>• 無線 MAB（Wireless MAB）<br>• 有線 802.1x（Wired 802.1X）<br>• 無線 802.1x（Wireless 802.1X）<br>• 有線 Web 認証（Wired Web Authentication）<br>• 無線 Web 認証（Wireless Web Authentication）<br>ネットワーク デバイス プロファイルでサポートされる認証ログインをオンにした後、ログインの条件を指定します。 |
| 属性エイリアシング（Attribute Aliasing） | ポリシー ルールのフレンドリ名としてデバイスのサービスセット識別子（SSID）を使用する場合は、[SSID] チェックボックスをオンにします。これにより、ポリシー ルールで使用する一貫した名前を作成でき、その名前は複数のデバイスに適用されます。 |
| ホスト ルックアップ（MAB） | |

| フィールド | 説明 |
|---|---|
| ホスト ルックアップの処理（Process Host Lookup） | ネットワーク デバイス プロファイルで使用されるホスト ルックアップ用のプロトコルを定義するには、このチェックボックスをオンにします。<br>さまざまなベンダーからのネットワーク デバイスは、MAB 認証を異なる方法で実行します。デバイス タイプに応じて、使用しているプロトコルの [パスワードを確認（Check Password）] チェックボックス、[Calling-Station-IdがMACアドレスと等しいかを確認（Checking Calling-Station-Id equals MAC Address）] チェックボックス、またはその両方をオンにします。 |
| PAP/ASCII 経由（Via PAP/ASCII） | ホスト ルックアップ要求としてネットワーク デバイス プロファイルからの PAP 要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。 |
| CHAP 経由（Via CHAP） | ホスト ルックアップ要求としてネットワーク デバイスからのこのタイプの要求を検出するように Cisco ISE を設定するには、このチェックボックスをオンにします。<br>このオプションによって、CHAP 認証が有効になります。CHAP は、パスワードの暗号化とともにチャレンジ/レスポンス方式を使用します。CHAP は、Microsoft Active Directory では使用できません。 |
| EAP-MD5 経由（EAP-MD5） | ネットワーク デバイス プロファイルに EAP ベースの MD5 ハッシュ認証を有効にするには、このチェックボックスをオンにします。 |

### 権限テンプレートの設定

このネットワーク デバイス プロファイルに使用される VLAN および ACL の権限を定義できます。プロファイルを保存すると、Cisco ISE は設定された各権限に対し許可プロファイルを自動的に生成します。次の表は、[権限（Permissions）] セクションのフィールドについての説明です。

表 *57* : 権限の設定

| フィールド | 説明 |
|---|---|
| VLAN の設定（Set VLAN） | このネットワーク デバイス プロファイルに VLAN権限を設定するには、このチェックボックスをオンにします。次のいずれかのオプションを選択します。<br>• IETF 802.1X 属性（IETF 802.1X Attributes）：Internet Engineering Task Force で定義されたデフォルトの RADIUS 属性のセットです。<br>• 一意の属性（Unique Attributes）：複数の RADIUS 属性値のペアを指定できます。 |
| ACL の設定（Set ACL） | RADIUS 属性をネットワーク デバイス プロファイルの ACL に設定する場合は、このチェックボックスをオンにします。 |

## 許可変更（CoA）テンプレートの設定

このテンプレートは、CoA がこのタイプのネットワーク デバイスにどのように送信されるかを定義します。次の表は、[許可変更（CoA）（Change of Authorization (CoA)）] セクションのフィールドについての説明です。

表 *58* : 許可変更（*CoA*）の設定

| フィールド | 定義（Definition） |
|---|---|
| 次による CoA（CoA by） | RADIUS により、または SNMP により、ネットワーク デバイス プロファイルに CoA パケットを送信するか、あるいはまったくしないかを選択します。 |
| RADIUS による CoA（CoA by RADIUS） | |
| デフォルトの CoA ポート（Default CoA Port） | RADIUS CoA を送信するポート。シスコ デバイスのデフォルト ポートは 1700 で、他のベンダーのデバイスでは 3799 です。<br>[ネットワークデバイス（Network Device）] ページでこれを上書きできます。 |
| タイムアウト間隔（Timeout Interval） | CoA の送信後に Cisco ISE が応答を待機する秒数。 |

| フィールド | 定義（Definition） |
|---|---|
| 再試行回数（Retry Count） | 最初のタイムアウト後に Cisco ISE が CoA の送信を試行する回数。 |
| 切断 | これらのデバイスに接続解除要求を送信する方法を選択します。<br>• RFC 5176（RFC 5176）：標準のセッション終了の場合はこのチェックボックスをオンにし、RFC 5176 に従って定義されているように、ポートを新しいセッション用に残しておきます。<br>• ポート バウンス（Port Bounce）：セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。<br>• ポートのシャットダウン（Port Shutdown）：セッションを終了して、ポートをシャットダウンするには、このチェックボックスをオンにします。 |
| 再認証（Re-authenticate） | ネットワーク デバイスに再認証要求を送信する方法を選択します。これは現在、シスコ デバイスのみでサポートされています。<br>• 基本（Basic）：標準のセッション再認証の場合はこのチェックボックスをオンにします。<br>• 再実行（Rerun）：認証方式によって最初から実行する場合は、このチェックボックスをオンにします。<br>• 最後（Last）：最後に成功した認証方式をセッションに使用します。 |
| CoA プッシュ（CoA Push） | ネットワーク デバイスがシスコの TrustSec CoA 機能をサポートしない場合は、このオプションを選択して、Cisco ISE が設定の変更をデバイスにプッシュできるようにします。 |
| SNMP による CoA（CoA by SNMP） | |
| タイムアウト間隔（Timeout Interval） | CoA の送信後に Cisco ISE が応答を待機する秒数。 |

| フィールド | 定義（Definition） |
|---|---|
| 再試行回数（Retry Count） | Cisco ISE が CoA の送信を試行する回数。 |
| NAD ポートの検出 | 関連する RADIUS 属性は、現時点での唯一のオプションです。 |
| 関連する RADIUS 属性 | NAD ポートを検出する方法を選択します。<br>• Nas-Port<br>• Nas-Port-ID |
| 切断 | これらのデバイスに接続解除要求を送信する方法を選択します。<br>• 再認証します。セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。<br>• ポート バウンス（Port Bounce）：セッションを終了して、ポートを再起動するには、このチェックボックスをオンにします。<br>• ポートのシャットダウン（Port Shutdown）：セッションを終了して、ポートをシャットダウンするには、このチェックボックスをオンにします。 |

### リダイレクト テンプレートの設定

ネットワークデバイスは、許可プロファイルで設定されている場合、クライアントのHTTP要求をリダイレクトできます。このテンプレートは、このネットワーク デバイス プロファイルがURLリダイレクトをサポートするかどうかを指定します。デバイス タイプに固有のURLパラメータ名を使用します。

次の表は、[リダイレクト（Redirect）] セクションのフィールドについての説明です。

表 *59:* リダイレクトの設定

| フィールド | 定義（Definition） |
|---|---|
| タイプ（Type） | ネットワーク デバイス プロファイルが静的または動的URL リダイレクトをサポートするかを選択します。<br>デバイスがどちらもサポートしていない場合、[未サポート（Not Supported）] を選択し、**[設定（Settings）] > [DHCPおよびDNSサービス（DHCP & DNS Services）]** から VLAN を設定します。 |
| リダイレクト URL パラメータ名 | |
| クライアント IP アドレス | ネットワーク デバイスがクライアントのIPアドレスに使用するパラメータ名を入力します。 |
| クライアントMACアドレス（Client MAC Address） | ネットワーク デバイスがクライアントのMACアドレスに使用するパラメータ名を入力します。 |
| 元の URL（Originating URL） | ネットワーク デバイスが元のURLに使用するパラメータ名を入力します。 |
| セッション ID | ネットワーク デバイスがセッション ID に使用するパラメータ名を入力します。 |
| SSID | ネットワーク デバイスがサービス セット識別子（SSID）に使用するパラメータ名を入力します。 |
| ダイナミック URL パラメータ | |
| パラメータ | 動的URL リダイレクトを選択する場合は、これらのネットワーク デバイスがリダイレクト URL を作成する方法を指定する必要があります。また、リダイレクトURLがセッションIDまたはクライアントのMACアドレスを使用するかを指定できます。 |

### 詳細設定（Advanced Settings）

ネットワーク デバイス プロファイルを使用して、ネットワーク デバイスをポリシー ルールで使いやすくするために、多数のポリシー要素を生成できます。これらの要素には、複合条件、許可プロファイル、および許可されているプロトコルが含まれています。

これらの要素を作成するには、[ポリシー要素の作成（Generate Policy Elements）] ボタンをクリックします。

**関連トピック**

ネットワーク デバイス プロファイル
Cisco ISE でのサードパーティ ネットワーク デバイスのサポート
ネットワーク デバイス プロファイルの作成

# 外部 RADIUS サーバの設定

次の表では、[外部 RADIUS サーバ（External RADIUS Server）] ページのフィールドについて説明します。これらのフィールドを使用して、RADIUS サーバを設定できます。Cisco ISE が RADIUS サーバとして機能するためには、このページで設定する必要があります。このページのナビゲーション パスは、**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [外部 RADIUS サーバ（External RADIUS Servers）]** です。

**表 *60* : 外部 *RADIUS* サーバの設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 名前（Name） | 外部 RADIUS サーバの名前を入力します。 |
| 説明 | 外部 RADIUS サーバの説明を入力します。 |
| ホスト名/アドレス（Host IP） | 外部 RADIUS サーバの IP アドレスを入力します。IPv4 アドレスを入力する場合は、範囲とサブネット マスクを使用できます。IPv6 では、範囲がサポートされていません。 |
| 共有秘密鍵（Shared Secret） | 外部 RADIUS サーバの認証に使用される、Cisco ISE と外部 RADIUS サーバの間の共有秘密を入力します。共有秘密情報は、予期されるテキスト文字列です。ユーザは、ネットワーク デバイスによってユーザ名およびパスワードが認証されるようにこれらの情報を提示する必要があります。ユーザが共有秘密情報を提示するまで、接続は拒否されます。共有秘密情報の長さは、最大 128 文字です。 |
| KeyWrap の有効化（Enable KeyWrap） | このオプションをオンにすると、Cisco ISE で FIPS 140-2 準拠が有効になり、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ます。 |

| フィールド | 使用上のガイドライン |
|---|---|
| キー暗号キー（Key Encryption Key） | （[keyWrap を有効にする（Enable keyWrap）] チェックボックスをオンにした場合のみ）セッション暗号化（秘密）に使用される暗号キーを入力します。 |
| メッセージ オーセンティケータ コード キー（Message Authenticator Code Key） | （[keyWrap を有効にする（Enable keyWrap）] チェックボックスをオンにした場合のみ）RADIUS メッセージ上のキー付き HMAC 計算に使用されるキーを入力します。 |
| キー入力形式（Key Input Format） | Cisco ISE 暗号キーの入力に使用する形式を指定します。これは、WLAN コントローラ上の設定と一致する必要があります。（指定する値の長さは、次に定義されているキーの最大長と正確に一致している必要があります。これより短い値は許可されません）。<br>• [ASCII]：キー暗号キーの長さは 16 文字（バイト）、メッセージ オーセンティケータ コード キーの長さは 20 文字（バイト）である必要があります。<br>• [16 進数（Hexadecimal）]：キー暗号キーの長さは 32 バイトであり、メッセージ オーセンティケータ コード キーの長さは 40 バイトである必要があります。 |
| 認証ポート（Authentication Port） | RADIUS 認証のポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 1812 です。 |
| アカウンティング ポート（Accounting Port） | RADIUS アカウンティングのポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 1813 です。 |
| サーバ タイムアウト（Server timeout） | Cisco ISE が外部 RADIUS サーバからの応答を待機する秒数を入力します。デフォルトは 5 秒です。有効な値は 5 ～ 120 です。 |
| 接続試行回数（Connection Attempts） | Cisco ISE が外部 RADIUS サーバへの接続を試行する回数を入力します。デフォルトは 3 回に設定されています。有効な値は 1 ～ 9 です。 |

| フィールド | 使用上のガイドライン |
|---|---|
| RADIUS プロキシ フェールオーバーの有効期限 | 接続に失敗してから、このサーバに再び接続を試みるまでの経過時間を入力します。有効値の範囲は 1 ～ 600 です。<br>サーバ タイムアウトをスキップし、フェールオーバーに直接移動するには、このパラメータを設定します。 |

**関連トピック**

RADIUS プロキシ サーバとして機能する CIsco ISE
外部 RADIUS サーバの設定

# RADIUS サーバ順序

次の表では、RADIUS サーバ順序を作成するために使用する [RADIUS サーバ順序（RADIUS Server Sequences）] ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [RADIUS サーバ順序（RADIUS Server Sequences）] > [追加（Add）]** です。

**表 *61 : RADIUS* サーバ順序**

| フィールド | 使用上のガイドライン |
|---|---|
| 名前（Name） | RADIUS サーバ順序の名前を入力します。 |
| 説明 | 任意で説明を入力します。 |
| ホスト名/アドレス（Host IP） | 外部 RADIUS サーバの IP アドレスを入力します。 |
| ユーザが選択したサービス タイプ（User Selected Service Type） | [使用可能（Available）] リスト ボックスで、ポリシー サーバとして使用する外部 RADIUS サーバを選択し、選択した外部 RADIUS サーバを [選択済み（Selected）] リスト ボックスに移動します。 |
| リモート アカウンティング（Remote Accounting） | リモート ポリシー サーバでアカウンティングを有効にするには、このチェックボックスをオンにします。 |
| ローカル アカウンティング（Local Accounting） | Cisco ISE でのアカウンティングを有効にするには、このチェックボックスをオンにします。 |
| 高度な属性設定（Advanced Attributes Settings） | |

| フィールド | 使用上のガイドライン |
| --- | --- |
| サブジェクト名の先頭から最後に出現する区切り文字まで削除（Strip Start of Subject Name up to the First Occurrence of the Separator） | プレフィクスからユーザ名を取り除くには、このチェックボックスをオンにします。たとえば、サブジェクト名が acme\userA、区切り文字が \ の場合、ユーザ名は userA になります。 |
| 最初に出現する区切り文字からサブジェクト名の末尾まで削除（Strip End of Subject Name from the Last Occurrence of the Separator） | サフィックスからユーザ名を取り除くには、このチェックボックスをオンにします。たとえば、サブジェクト名が userA@abc.com、区切り文字が @ の場合、ユーザ名は userA になります。<br>• NetBIOS または User Principle Name（UPN）フォーマットのユーザ名（user@domain.com または /domain/user）からユーザ名を抽出するには、これらのストリップ オプションを有効にする必要があります。RADIUS サーバでユーザを認証するために、ユーザ名だけがRADIUS サーバに渡されるためです。<br>• \ および @ の両方のストリップ機能をアクティブ化し、Cisco AnyConnect を使用している場合、Cisco ISE は最初に出現する \ を文字列から正確に取り除くことができません。ただし、各ストリップ機能は、Cisco AnyConnect を考慮して設計されているため、個別に使用する場合は動作します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 外部 RADIUS サーバへの要求に含まれる属性を変更する（Modify Attributes in the Request to the External RADIUS Server） | 認証済みの RADIUS サーバとの間で送受信する属性の操作を Cisco ISE に許可するには、このチェックボックスをオンにします。<br>次の属性操作が可能です。<br>• [追加（Add）]：RADIUS 要求/応答全体に属性を追加します。<br>• [更新（Update）]：属性値（固定または静的）を変更します。または属性を別の属性値（動的）で置き換えます。<br>• [削除（Remove）]：属性または属性と値のペアを削除します。<br>• [すべて削除（RemoveAny）]：存在するすべての属性を削除します。 |
| 認証ポリシーに進む（Continue to Authorization Policy） | ID ストア グループおよび属性の取得に基づいて、プロキシ フローを許可ポリシーの実行に誘導して、より詳細な意思決定を行うには、このチェックボックスをオンにします。このオプションを有効にすると、外部 RADIUS サーバからの応答に含まれる属性が、認証ポリシーの選択に使用されます。このコンテキストの既存の属性は、AAA サーバの受け入れ応答属性の適切な値で更新されます。 |
| Access-Accept の送信前に属性を変更する（Modify Attributes before send an Access-Accept） | 応答をデバイスに返送する直前に属性を変更するには、このチェックボックスをオンにします。 |

**関連トピック**

RADIUS プロキシ サーバとして機能する CIsco ISE
RADIUS サーバ順序の定義

# NAC マネージャの設定

次の表では、NAC マネージャを追加するために使用できる [新規 NAC Manager（New NAC Manager）]ページのフィールドについて説明します。このページへのナビゲーション パスは、**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [NAC Managers]** です。

表 *62 : NAC* マネージャの設定

| フィールド | 使用上のガイドライン |
|---|---|
| 名前（Name） | Cisco Access Manager（CAM）の名前を入力します。 |
| ステータス | CAM への接続を認証する Cisco ISE プロファイラからの REST API 通信を有効にする場合は、[ステータス（Status）] チェックボックスをオンにします。 |
| 説明 | CAM の説明を入力します。 |
| [IPアドレス（IP Address）] | CAM の IP アドレスを入力します。Cisco ISE で CAM を作成して保存した後、CAM の IP アドレスを編集することはできません。<br>0.0.0.0 と 255.255.255.255 は、Cisco ISE で CAM の IP アドレスを検証するときに除外され、CAM の [IP アドレス（IP Address）] フィールドで使用できる有効な IP アドレスではないため、使用できません。<br>（注） ハイ アベイラビリティ構成で CAM のペアが共有する仮想サービス IP アドレスを使用できます。これで、ハイ アベイラビリティ構成で CAM のフェールオーバーをサポートできます。 |
| [ユーザ名（Username）] | CAM のユーザインターフェイスにログオンできる CAM 管理者のユーザ名を入力します。 |
| [パスワード（Password）] | CAM のユーザインターフェイスにログオンできる CAM 管理者のパスワードを入力します。 |

## 関連トピック

Cisco NAC アプライアンスとの Cisco ISE 統合
Cisco Clean Access Manager の追加

# デバイス ポータルの管理

## デバイス ポータルの設定

### デバイス ポータルのグローバル設定

**[ワーク センター（Work Centers）] > [BYOD] > [設定（Settings）] > [従業員が登録するデバイス（Employee Registered Devices）]** または **[管理（Administration）] > [デバイス ポータルの管理（Device Portal Management）] > [設定（Settings）]** を選択します。

BYOD ポータルおよびデバイス ポータルの次の一般設定を設定できます。

- [従業員が登録するデバイス（Employee Registered Devices）]：[従業員を制限（Restrict employees to）] に、従業員が登録できるデバイスの最大数を入力します。デフォルトでは、この値は 5 デバイスに設定されています。
- [再試行 URL（Retry URL）]：デバイスを Cisco ISE にリダイレクトするために使用できる URL を [オンボードのための再試行 URL（Retry URL for onboarding）] に入力します。

これらの一般的な設定値を設定したら、これらの設定は会社に設定したすべて BYOD ポータルおよびデバイス ポータルに適用されます。

**関連トピック**

従業員が登録するパーソナル デバイス数の制限
BYOD 登録に再接続する URL の提供
分散環境のエンドユーザのデバイス ポータル

### デバイス ポータルのポータル ID 設定

これらの設定へのナビゲーションパスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [ブラックリスト ポータル（Blacklist Portal）]/[クライアント プロビジョニング ポータル（Client Provisioning Portals）]/[BYOD ポータル（BYOD Portals）]/[MDM ポータル（MDM Portals）]/[デバイス ポータル（My Device Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの設定およびカスタマイズ（Portals Settings and Customization）]** です。

- ポータル名（Portal Name）：このポータルにアクセスするための一意のポータル名を入力します。このポータル名を、その他のスポンサー、ゲスト、または非ゲストポータル（ブラックリスト、個人所有デバイス持ち込み（BYOD）、クライアントプロビジョニング、モバイルデバイス管理（MDM）、またはデバイスの各ポータル）に使用しないでください。

  この名前は、リダイレクションを選択するために、認証プロファイルポータルの選択に表示されます。これはポータルのリストに適用され、他のポータルとの間で簡単に識別できます。

- **説明（Description）**：任意項目です。
- ポータルテスト URL（Portal test URL）：[保存（Save）] をクリックした後にリンクとして表示されるシステムにより生成された URL。ポータルをテストするために使用します。

  リンクをクリックすると、このポータルの URL を表示する新しいブラウザ タブが開きます。ポリシーサービスを含むポリシーサービスノード（PSN）をオンにする必要があります。ポリシーサービスがオンになっていない場合、PSN は管理者用ポータルのみを表示します。

  （注） テストポータルは RADIUS セッションをサポートしていないため、すべてのポータルに対するポータルフローの全体は表示されません。BYOD およびクライアント プロビジョニングは RADIUS セッションに依存するポータルの例です。たとえば、外部 URL へのリダイレクションは機能しません。複数の PSN がある場合、ISE は最初のアクティブ PSN を選択します。

- 言語ファイル（Language File）：各ポータルタイプは、デフォルトで 15 種類の言語をサポートします。これらの言語は、個々のプロパティファイルとして使用できます。これらのファイルは、圧縮された単一の言語ファイル内にまとめてバンドルされています。ポータルで使用する圧縮言語ファイルをエクスポートまたはインポートします。圧縮言語ファイルには、ポータルのテキストを表示するために使用可能な個別の言語ファイルがすべて含まれています。

  言語ファイルには、その言語のポータル全体のすべての文字列設定に加え、特定のブラウザのロケール設定（例：フランス語の場合は fr、fr-fr、fr-ca）へのマッピングが含まれています。1 つの言語ファイルには、翻訳およびローカリゼーションの目的に容易に使用できるように、サポートされるすべての言語が含まれています。

  1 つの言語用のブラウザ ロケール設定を変更した場合、変更内容は他のすべてのエンドユーザ Web ポータルに適用されます。たとえば、ホットスポット ゲスト ポータルの French.properties ブラウザロケールを fr,fr-fr,fr-ca から fr,fr-fr に変更すると、この変更内容がデバイスポータルにも適用されます。

  [ポータルページのカスタマイズ（Portal Page Customizations）] タブでいずれかのテキストをカスタマイズすると、警告アイコンが表示されます。警告メッセージは、ポータルのカスタマイズ時に 1 つの言語で行った変更をすべてのサポート対象の言語プロパティファイルにも追加する必要があることを通知します。ドロップダウンリストのオプションを使用して、手動で警告アイコンが表示されないようにします。また、警告アイコンは、更新された圧縮言語ファイルのインポート後に自動的に表示されなくなります。

-

## 関連トピック

許可ポリシー ルールの作成
許可プロファイルの作成
パーソナル デバイス ポータル

# ブラックリスト ポータルのポータル設定

この設定のナビゲーション パスは、**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **[ブラックリスト ポータル（Blacklist Portal）]** > **[編集（Edit）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[ポータル設定（Portal Settings）]** です

これらの設定を使用して、ユーザ（状況に応じてゲスト、スポンサー、または従業員）に表示される特定のポータルページではなく、ポータル全体に適用される値を指定したり動作を定義したりします。

- [HTTPS ポート（HTTPS port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアント プロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

  同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストにインターフェイス 0 を使用することを推奨します。ポータル設定ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスを設定しようとします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
  - **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
    - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ（Certificate group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- **表示言語**
  - [ブラウザのロケールを使用する（Use browser locale）]：クライアント ブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。
  - [フォールバック言語（Fallback language）]：ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語が ISE でサポートされていない場合に使用する言語を選択します。
  - [常に使用（Always use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID（SSIDs available to sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID（セッション サービス識別子）を入力します。

**関連トピック**

ブラックリスト ポータルの編集
ブラックリスト ポータル
ブラックリスト ポータルの言語ファイルの HTML サポート

## BYOD と MDM ポータルのポータル設定

この設定のナビゲーションパスは、**[管理（Administration）]>[デバイス ポータル管理（Device Portal Management）] > [BYOD ポータルまたは MDM ポータル（BYOD Portals or MDM Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]** です。

これらを設定して、ポータル ページの動作を定義します。

- [HTTPS ポート（HTTPS port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアント プロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

- スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**
- 無効な組み合わせには次が含まれます。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストにインターフェイス 0 を使用することを推奨します。ポータル設定ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。
  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。こ

れは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。

- ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスを設定しようとします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
- **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
  - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ（Certificate group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- エンドポイント ID グループ（Endpoint identity group）：ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

  従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

- **表示言語**
  - [ブラウザのロケールを使用する（Use browser locale）]：クライアント ブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。

- [フォールバック言語（Fallback language）]：ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語が ISE でサポートされていない場合に使用する言語を選択します。

- [常に使用（Always use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID（SSIDs available to sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID（セッション サービス識別子）を入力します。

**関連トピック**

個人所有デバイスの持ち込みポータル
BYOD ポータルの作成
モバイル デバイス管理ポータル
MDM ポータルの作成
個人所有デバイスの持ち込みポータルの言語ファイルの HTML サポート
モバイル デバイス管理ポータルの言語ファイルの HTML サポート

## BYOD ポータルの BYOD 設定

この設定のナビゲーションパスは、**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **[BYOD ポータル（BYOD Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[BYOD 設定（BYOD Settings）]** です。

この設定を使用して、パーソナル デバイスを使用する従業員の個人所有デバイスの持ち込み（BYOD）機能を有効にし、企業ネットワークにアクセスできるようにします。

| フィールド | 使用上のガイドライン |
|---|---|
| AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)） | 会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、またはAUPテキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。 |
| 同意が必要（Require acceptance） | ユーザのアカウントが完全に有効になる前に、ユーザはAUPに同意する必要があります。[ログイン（Login）]ボタンは、ユーザが AUP を受け入れない場合は有効になりません。ユーザがAUPに同意しない場合、ネットワークにアクセスできません。 |

| フィールド | 使用上のガイドライン |
|---|---|
| AUP の最後までのスクロールが必要（Require scrolling to end of AUP） | このオプションは、[AUP をページに含める（Include an AUP on page）] が有効である場合のみ表示されます。<br><br>ユーザが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。 |
| 登録時にデバイス ID フィールドを表示する（Display Device ID field during registration） | 登録プロセス中に、デバイス ID をユーザに表示します。これは、デバイス ID が事前設定されており、BYOD ポータルを使用しているときに変更できない場合も含みます。 |
| 元の URL（Originating URL） | ネットワークへの認証に成功すると、可能な場合はユーザのブラウザを、ユーザがアクセスしようとしていた元の Web サイトにリダイレクトします。リダイレクトできない場合は、認証成功ページが表示されます。リダイレクト URL が NAD のアクセス コントロール リストとその NAD の ISE で設定された許可プロファイルにより、PSN のポート 8443 で動作することを確認します。<br><br>Windows、MAC、および Android デバイスの場合、制御はプロビジョニングを実行するセルフプロビジョニング ウィザード アプリケーションに渡されます。そのため、これらのデバイスは元の URL にリダイレクトされません。ただし、iOS（dot1X）およびサポート対象外のデバイス（ネットワーク アクセスが許可されている）では、この URL にリダイレクトされます。 |
| 成功ページ（Success page） | デバイスの登録が成功したことを示すページを表示します。 |
| URL | ネットワークへの認証に成功すると、ユーザのブラウザを指定された URL（会社の Web サイトなど）にリダイレクトします。 |

（注） 認証後に外部 URL にゲストをリダイレクトする場合、URL アドレスを解決して、セッションがリダイレクトされるまでに遅延が生じることがあります。

関連トピック

個人所有デバイスの持ち込みポータル
BYOD ポータルの作成
個人所有デバイスの持ち込みポータルの言語ファイルの HTML サポート

# 証明書プロビジョニング ポータルのポータル設定

これらの設定へのナビゲーション パスは、**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **[証明書プロビジョニング ポータル（Certificate Provisioning Portal）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[ポータル設定（Portal Settings）]** です。

- [HTTPS ポート（HTTPS port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアントプロビジョニング ポータルはポート 8905 および 8909 も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

  同じ HTTPS ポートに割り当てられたポータルは、同じギガビット イーサネット インターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループ タグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**

  - 無効な組み合わせには次が含まれます。
    - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
    - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストにインターフェイス 0 を使用することを推奨します。ポータル設定ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。
  - ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディングインターフェイスを設定しようとします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
  - **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
    - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ（Certificate group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- 認証方式（Authentication Method）IDソース順序（Identity source sequence）：ユーザ認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ISS は、ユーザ クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザ、内部ユーザ、Active Directory、LDAP ディレクトリ などがあります。

  Cisco ISE には、スポンサー ポータル Sponsor_Portal_Sequence 用のデフォルトのスポンサー ID ソース順序が含まれています。

  IdP を設定するには、**[管理（Administration）]** > **[IDの管理（Identity Management）]** > **[外部IDソース（External Identity Sources）]** > **[SAML ID プロバイダー（SAML Id Providers）]** の順に選択します。

  ID ソース順序を設定するには、[管理（Administration）] > [IDの管理（Identity Management）] > [IDソース順序（Identity Source Sequences）] の順に選択します。
- [承認済みグループの設定（Configure Authorized Groups）]：証明書を生成してそれを [選択済み（Chosen）] ボックスに移動するための権限を付与するユーザ ID グループを選択します。
- [完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]：スポンサーまたはデバイス ポータルに対応する 1 つの固有の FQDN またはホスト名を入力します。たとえば、**`sponsorportal.yourcompany.com,sponsor`** と入力することで、ユーザはブラウザにこれらのいずれかを入力すると、スポンサー ポータルが表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。

  デフォルトの FQDN を変更する場合は、次を実行します。

  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
  - 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバ証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。
- [アイドル タイムアウト（Idle timeout）]：ポータルでアクティビティがない場合にユーザをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

### ログイン ページの設定（Login Page Settings）

- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザ セッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウ

トは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。

- [AUPを含める（Include an AUP）]：フローに利用規約ページを追加します。AUP をページに追加したり、別のページへのリンクを設定することができます。これを追加すると、右側のフローの画像が変わります。
  - [同意が必要（require acceptance）]：フローを続行する前に、ユーザが AUP に同意するように強制します。
-

### 利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）

- [AUP ページを含める（Include an AUP page）]：会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [従業員に別の AUP を使用する（Use different AUP for employees）]：従業員専用に別の AUP およびネットワーク使用諸条件を表示します。このオプションを選択すると、[従業員用の AUP をスキップ（Skip AUP for employees）] は選択できません。
- [従業員用の AUP をスキップ（Skip AUP for employees）]：従業員は、ネットワークにアクセスする前に AUP に同意する必要はありません。このオプションを選択すると、[従業員に別の AUP を使用する（Use different AUP for employees）] は選択できません。
- [同意が必要（Require acceptance）]：ユーザのアカウントが完全に有効になる前に、ユーザは AUP に同意する必要があります。[ログイン（Login）] ボタンは、ユーザが AUP を受け入れない場合は有効になりません。ユーザが AUP に同意しない場合、ネットワークにアクセスできません。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：[AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。

  ユーザが AUP を最後まで読んだことを確認します。[同意（Accept）]ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。AUP がユーザに表示された場合に設定します。
  - [初回のログインのみ（On first login only）]：ユーザが初めてネットワークまたはポータルにログインしたときに AUP を表示します。
  - [ログインごと（On every login）]：ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。
  - [__ 日ごと（初回のログインから）（Every __ days (starting at first login)）]：ネットワークやポータルにユーザが初めてログインした後は、AUP を定期的に表示します。
-

### 関連トピック

証明書プロビジョニング ポータル

クライアント プロビジョニング ポータルの作成
証明書プロビジョニング ポータルの言語ファイルの HTML サポート

# クライアント プロビジョニング ポータルのポータル設定

これらの設定へのナビゲーション パスは、**[管理（Administration）]**>**[デバイス ポータル管理（Device Portal Management）]**>**[クライアント プロビジョニング ポータル（Client Provisioning Portals）]** > **[作成、編集、複製または削除（Create, Edit, Duplicate, or Delete）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** です。

### ポータル設定

- HTTPS ポート（HTTPS Port）：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合、この制限に従うようにポート設定を変更する必要があります。
- 使用可能インターフェイス（Allowed interfaces）：ポータルを実行できる PSN インターフェイスを選択します。PSN で使用可能なインターフェイスを備えた PSN のみがポータルを作成できます。物理およびボンディングされたインターフェイスの任意の組み合わせを設定できます。これは PSN 全体の設定です。すべてのポータルはこれらのインターフェイスでのみ動作し、このインターフェイス設定はすべての PSN に適用されます。
  - 異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。
  - ここで有効にするインターフェイスは、ポリシーサービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名は、インターフェイス IP に解決される必要があります。
  - ISE CLI の ip host x.x.x.x yyy.domain.com をセカンダリ インターフェイス IP と FQDN をマッピングするように設定します。これは証明書のサブジェクト名/サブジェクトの代替名を一致させるために使用されます。
  - ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスを設定しようとします。これが成功しない場合、その PSN にボンド セットがなかったことが原因である可能性があるので、PSN はエラーを記録して終了します。物理インターフェイスでポータルを開始しようとはしません。
  - **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。

- 物理NICと対応するボンディングされたNICの両方が設定されている場合：PSNがポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSNは物理インターフェイスでポータルを開始しようとします。

- 証明書グループ タグ（Certificate group tag）：ポータルの HTTPS トラフィックに使用する証明書グループのグループ タグを選択します。
- [認証方式（Authentication Method）]：ユーザ認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ISS は、ユーザ クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザ、内部ユーザ、Active Directory、LDAP などがあります。

  Cisco ISE には、クライアント プロビジョニング ポータル用のデフォルトのクライアント プロビジョニング ID ソース順序 Certificate_Portal_Sequence が含まれています。

- 完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）：クライアント プロビジョニング ポータル用に少なくとも 1 つの一意の FQDN、ホスト名、またはその両方を入力します。たとえば、「provisionportal.yourcompany.com」と入力した場合、ユーザはこれらのいずれかをブラウザに入力して証明書プロビジョニング ポータルに到達できます。

  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに確実に解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
  - 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバ証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。

  （注） URL リダイレクトなしのクライアント プロビジョニングの場合、[完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]フィールドに入力するポータル名は、DNS 設定で設定されている必要があります。URL リダイレクトなしのクライアント プロビジョニングを有効にするため、この URL をユーザに通知する必要があります。

- アイドル タイムアウト（Idle timeout）：ポータルでアクティビティがない場合にユーザをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

（注） クライアント プロビジョニング ポータルではポート番号と証明書を定義できます。これにより、ホストはクライアントプロビジョニングとポスチャに同じ証明書をダウンロードすることを許可します。ポータル証明書が正式な認証局により署名されている場合、セキュリティ警告は表示されません。自己署名証明書の場合、ポータルと Cisco AnyConnect Posture コンポーネントの両方でセキュリティ警告を受け取ります。

### ログイン ページの設定（Login Page Settings）

- [ログインの有効化（Enable Login）]：クライアント プロビジョニング ポータルのログイン手順を有効にするには、このチェック ボックスを選択します
- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：単一のブラウザ セッションからのログイン試行失敗回数を指定します。この回数を超過すると、Cisco ISE はログイン試行を実行できる頻度を意図的に低下させて、追加のログイン試行を防ぎます。ログイン失敗がこの回数に達した後のログイン試行の間隔は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で指定されます。
- [頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）]：[頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）] で定義された回数のログインの失敗後に、ユーザが再度ログインを試行するまでに待機する必要がある時間を分単位で設定します。
- [AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)）]：会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。
- [同意が必要（Require acceptance）]：ポータルにアクセスする前にユーザが AUP を受け入れることを要求します。[ログイン（Login）] ボタンは、ユーザが AUP を受け入れない場合は有効になりません。AUP を受け入れないユーザは、ポータルにアクセスできません。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：[AUP をページに含める（Include an AUP on page）] を有効にした場合にのみ、このオプションが表示されます。ユーザが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。

### 利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）

- [AUP を含める（Include an AUP）]：会社のネットワーク使用諸条件を、別のページでユーザに表示します。
- [AUP の最後までのスクロールが必要（Require scrolling to end of AUP）]：ユーザが AUP を完全に読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。

- [初回のログインのみ（On first login only）]：ユーザがネットワークまたはポータルに初めてログインしたときのみ、AUP を表示します。
- [ログインごと（On every login）]：ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。
- [_ 日ごと（初回のログインから）（Every _____ days (starting at first login)）]：ネットワークやポータルにユーザが初めてログインした後は、AUP を定期的に表示します。

### ポストログイン バナー ページ設定（Post-Login Banner Page Settings）

[ポストログイン バナー ページを含める（Include a Post-Login Banner page）]：ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。

### パスワード変更設定（Change Password Settings）

[内部ユーザに自身のパスワードの変更を許可する（Allow internal users to change their own passwords）]：従業員がクライアント プロビジョニング ポータルにログインして、自分のパスワードを変更できるようにします。これは、アカウントが Cisco ISE データベース保存されている従業員に適用され、Active Directory や LDAP などの外部データベースに保存されている場合には適用されません。

### 関連トピック

クライアント プロビジョニング ポータル
クライアント プロビジョニング ポータルの作成
クライアント プロビジョニング ポータルの言語ファイルの HTML サポート

## MDM ポータルの従業員のモバイル デバイス管理設定

これらの設定へのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [MDM ポータル（MDM Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [従業員のモバイル デバイス管理設定（Employee Mobile Device Management Settings）]** です。

これらの設定を使用して、MDM ポータルを使用する従業員のモバイルデバイス管理（MDM）機能を有効にし、AUP エクスペリエンスを定義します。

| フィールド | 使用上のガイドライン |
|---|---|
| AUP をページに含める/AUP をリンクとして含める（Include an AUP (on page/as link)） | 会社のネットワーク使用の諸条件を、現在ユーザに表示されるページ上のテキストとして、または AUP テキストが含まれる新しいタブまたはウィンドウを開くリンクとして表示します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 同意が必要（Require acceptance） | ユーザのアカウントが完全に有効になる前に、ユーザはAUPに同意する必要があります。[ログイン（Login）] ボタンは、ユーザが AUP を受け入れない場合は有効になりません。ユーザがAUPに同意しない場合、ネットワークにアクセスできません。 |
| AUPの最後までのスクロールが必要（Require scrolling to end of AUP） | このオプションは、[AUP をページに含める（Include an AUP on page）] が有効である場合のみ表示されます。<br>ユーザがAUPを最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。 |

**関連トピック**

モバイル デバイス管理ポータル
MDM ポータルの作成
Mobile Device Manager と Cisco ISE との相互運用性

## デバイス ポータルのポータル設定

これらの設定へのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポータル設定（Portal Settings）]** です。

- [HTTPS ポート（HTTPS port）]：8000 ～ 8999 の範囲のポート値を入力します。デフォルト値はすべてのデフォルト ポータルで 8443 です。ただし、ブラックリスト ポータルは 8444 です。この範囲外のポート値を使用してアップグレードした場合は、このページで変更を加えるまで維持されます。このページを変更する場合は、この制限に従うようにポート設定を更新します。

  ゲスト ポータルに非ゲスト ポータル（マイ デバイスなど）によって使用されるポートを割り当てると、エラー メッセージが表示されます。

  ポスチャ評価と修復についてのみ、クライアントプロビジョニングポータルはポート8905および8909も使用します。それ以外の場合は、ゲスト ポータルへの割り当てと同じポートを使用します。

  同じHTTPSポートに割り当てられたポータルは、同じギガビットイーサネットインターフェイスまたは別のインターフェイスを使用できます。これらのポータルが同じポートとインターフェイスの組み合わせを使用している場合、同じ証明書グループタグを使用する必要があります。次に例を示します。

  - スポンサー ポータルを例として使用した有効な組み合わせを次に示します。

- スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書タグ **A**、およびデバイス ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**
- スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：ポート **8445**、インターフェイス **0**、証明書グループ **B**
- スポンサー ポータル：ポート **8444**、インターフェイス **1**、証明書グループ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **B**

- 無効な組み合わせには次が含まれます。
  - スポンサー ポータル：ポート **8443**、インターフェイス **0**、証明書グループ **A**、およびデバイス ポータル：**8443**、インターフェイス **0**、証明書グループ **B**
  - スポンサー ポータル：ポート **8444**、インターフェイス **0**、証明書タグ **A**、およびブラックリスト ポータル：ポート **8444**、インターフェイス **0**、証明書グループ **A**

（注） 最適なパフォーマンスを得るには、ゲストにインターフェイス 0 を使用することを推奨します。ポータル設定ではインターフェイス 0 のみを設定できます。または、CLI コマンド **ip host** を使用して、ホスト名または FQDN をインターフェイス 0 の IP アドレスにマッピングすることもできます。

- [使用可能インターフェイス（Allowed interfaces）]：PAN がポータルの実行に使用できる PSN インターフェイスを選択します。ポータルを開く要求が PAN で行われると、PAN は PSN で使用可能なポートを探します。異なるサブネット上の IP アドレスを使用してイーサネット インターフェイスを設定する必要があります。

  これらのインターフェイスは、ポリシー サービスがオンになっているすべての PSN（VM ベースを含む）で使用可能である必要があります。これは、これらのすべての PSN がゲストセッションの開始時にリダイレクトに使用される可能性があるため、必須要件です。

  - イーサネット インターフェイスは、異なるサブネット上の IP アドレスを使用する必要があります。
  - ここで有効にするインターフェイスは、ポリシー サービスがオンになっているときの VM ベースのものを含む、すべての PSN で使用できるものでなければなりません。これは、これらのすべての PSN がゲスト セッションの開始時にリダイレクトに使用される可能性があるため必須です。
  - ポータルの証明書のサブジェクト名とサブジェクトの代替名はインターフェイス IP に解決する必要があります。

- ISE CLI で **ip host x.x.x.x yyy.domain.com** を設定して、セカンダリ インターフェイス IP を FQDN にマッピングします。これは、証明書のサブジェクト名とサブジェクトの代替名と一致させるために使用されます。
- ボンディングされた NIC のみが選択されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスを設定しようとします。これが成功しない場合、おそらくは、その PSN でボンディングが設定されていないために、PSN でエラーが記録されて終了します。PSN は物理インターフェイスでのポータルの開始を試みません。
- **NIC チーミング**またはボンディングは、高可用性（耐障害性）のために 2 つの個別の NIC を設定できる、O/S 設定オプションです。どちらかの NIC に障害が発生すると、ボンディングされた接続の一部であるもう一方の NIC は、接続を続行します。1 つの NIC がポータル設定に基づきポータルに対して選択されます。
  - 物理 NIC と対応するボンディングされた NIC の両方が設定されている場合：PSN がポータルを設定しようとすると、最初にボンディング インターフェイスへ接続しようとします。これが成功しない場合、その PSN にボンド セットアップがなかったことが原因である可能性があるので、PSN は物理インターフェイスでポータルを開始しようとします。

- [証明書グループ タグ（Certificate group tag）]：ポータルの HTTPS トラフィックに使用する証明書を指定する証明書グループ タグを選択します。
- [完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN)）]：スポンサーまたはデバイス ポータルに対応する 1 つの固有の FQDN またはホスト名を入力します。たとえば、**sponsorportal.yourcompany.com,sponsor** と入力することで、ユーザはブラウザにこれらのいずれかを入力すると、スポンサー ポータルが表示されます。カンマを使用して名前を区切りますが、エントリ間にスペースを挿入しないでください。

  デフォルトの FQDN を変更する場合は、次を実行します。
  - DNS を更新して、新しい URL の FQDN が有効なポリシー サービス ノード（PSN）の IP アドレスに解決するようにします。PSN のプールを提供するロード バランサの仮想 IP アドレスを指定することもできます。
  - 名前の不一致による証明書の警告メッセージを回避するために、Cisco ISE PSN のローカル サーバ証明書のサブジェクト代替名（SAN）属性に、カスタマイズされた URL の FQDN またはワイルドカードを含めます。

- 認証方式（Authentication Method）ID ソース順序（Identity source sequence）：ユーザ認証に使用する ID ソース順序（ISS）または ID プロバイダー（IdP）を選択します。ISS は、ユーザ クレデンシャルを確認するために順番に検索される ID ストアのリストです。たとえば、内部ゲスト ユーザ、内部ユーザ、Active Directory、LDAP ディレクトリ などがあります。

  Cisco ISE には、スポンサー ポータル Sponsor_Portal_Sequence 用のデフォルトのスポンサー ID ソース順序が含まれています。

IdP を設定するには、**[管理（Administration）]** > **[IDの管理（Identity Management）]** > **[外部IDソース（External Identity Sources）]** > **[SAML ID プロバイダー（SAML Id Providers）]** の順に選択します。

ID ソース順序を設定するには、[管理（Administration）] > [IDの管理（Identity Management）] > [IDソース順序（Identity Source Sequences）] の順に選択します。

- エンドポイント ID グループ（Endpoint identity group）：ゲストのデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **GuestEndpoints** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

  従業員のデバイスを追跡するためのエンドポイント ID グループを選択します。Cisco ISE はデフォルトとして使用する **RegisteredDevices** のエンドポイント ID グループを提供します。デフォルトを使用しない場合、追加のエンドポイント ID グループを作成することもできます。

- __日に達した場合にこの ID グループ内のエンドポイントを消去する（Purge endpoints in this identity group when they reach __ days）：Cisco ISE データベースから消去されるまでの、ユーザのデバイスの登録からの日数を変更します。消去は毎日実行され、消去アクティビティは全体的な消去タイミングと同期されます。変更は、このエンドポイント ID グループ全体に適用されます。

  その他のポリシー条件に基づいてエンドポイント消去ポリシーに変更が加えられた場合、この設定は使用できなくなります。

- [アイドル タイムアウト（Idle timeout）]：ポータルでアクティビティがない場合にユーザをログアウトするまでに Cisco ISE が待機する時間（分）を入力します。有効な範囲は 1 ～ 30 分です。

- **表示言語**

  - [ブラウザのロケールを使用する（Use browser locale）]：クライアント ブラウザのロケール設定で指定された言語をポータルの表示言語として使用します。ブラウザ ロケールの言語が ISE でサポートされていない場合は、フォールバック言語が言語ポータルとして使用されます。

  - [フォールバック言語（Fallback language）]：ブラウザ ロケールから言語を取得できない場合、またはブラウザ ロケール言語が ISE でサポートされていない場合に使用する言語を選択します。

  - [常に使用（Always use）]：ポータルに使用する表示言語を選択します。この設定は、ユーザのブラウザのロケール オプションを上書きします。

[スポンサーに使用可能な SSID（SSIDs available to sponsors）]：ゲストの訪問にあたり、スポンサーが正しい接続先ネットワークとしてゲストに通知できる、ネットワークの名前または SSID（セッション サービス識別子）を入力します。

関連トピック

デバイス ポータル

デバイス ポータルの作成

# デバイス ポータルのログイン ページ設定

### デバイス ポータルのログイン ページ設定

- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザ セッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。
- [頻度制限までの最大ログイン試行失敗数（Maximum failed login attempts before rate limiting）]：Cisco ISE がアカウントのスロットルを開始するまでの単一のブラウザ セッションからのログイン試行失敗回数を指定します。これにより、アカウントのロックアウトは起きません。スロットル率は、[頻度制限時のログイン試行間隔（Time between login attempts when rate limiting）] で設定されます。
- [AUPを含める（Include an AUP）]：フローに利用規約ページを追加します。AUP をページに追加したり、別のページへのリンクを設定することができます。これを追加すると、右側のフローの画像が変わります。
  - [同意が必要（require acceptance）]：フローを続行する前に、ユーザが AUP に同意するように強制します。
-

関連トピック

デバイス ポータル

デバイス ポータルの作成

デバイス ポータルおよびエンドポイント アクティビティのモニタ

# デバイス ポータルの利用規定ページ設定

このページへのナビゲーション パスは、**[ワーク センター（Work Centers）] > [管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [利用規定（AUP）ページ設定（Acceptable Use Policy (AUP) Page Settings）]** です。

これらの設定を使用して、ユーザ（状況に応じてゲスト、スポンサーまたは従業員）に対して AUP エクスペリエンスを定義します。

| フィールド | 使用上のガイドライン |
|---|---|
| AUP ページを含める（Include an AUP page） | 会社のネットワーク使用諸条件を、別のページでユーザに表示します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| AUP の最後までのスクロールが必要（Require scrolling to end of AUP） | ユーザが AUP を最後まで読んだことを確認します。[同意（Accept）] ボタンは、ユーザが AUP の最後までスクロールするとアクティブになります。 |
| 初回のログインのみ（On first login only） | ユーザがネットワークまたはポータルに初めてログインしたときのみ、AUPを表示します。 |
| ログインごと（On every login） | ユーザがネットワークまたはポータルにログインするごとに、AUP を表示します。 |
| __日ごと（初回のログインから）（Every __ days (starting at first login)） | ユーザがネットワークまたはポータルに初めてログインした後に、定期的に AUP を表示します。 |

**関連トピック**

デバイス ポータル

デバイス ポータルの作成

## デバイス ポータルのポストログイン バナー ページ設定

このページへのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [ポストログイン バナー ページ設定（Post-Login Banner Page Settings）]** です。

これらの設定を使用して、正常なログイン後にユーザ（状況に応じてゲスト、スポンサーまたは従業員）に追加情報を通知します。

| フィールド | 使用上のガイドライン |
|---|---|
| ポストログイン バナー ページを含める（Include a Post-Login Banner page） | ユーザが正常にログインした後、ネットワーク アクセスを付与される前に追加情報を表示します。 |

**関連トピック**

デバイス ポータル

デバイス ポータルの作成

## デバイス ポータルの従業員によるパスワード変更の設定

このページへのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）] > [従業員のパスワード変更設定（Employee Change Password Settings）]**

です。これらの設定を使用して、デバイス ポータルを使用している従業員のパスワード要件を定義します。

従業員のパスワード ポリシーを設定するには、**[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [ユーザ名パスワード ポリシー（Username Password Policy）]** を選択します。

| フィールド | 使用上のガイドライン |
|---|---|
| 内部ユーザにパスワードの変更を許可する（Allow internal users to change password） | 従業員が、デバイス ポータルにログインした後で、自分のパスワードを変更することを許可します。<br>これは、アカウントが Cisco ISE データベース保存されている従業員に適用され、Active Directory や LDAP などの外部データベースに保存されている場合には適用されません。 |

**関連トピック**

デバイス ポータルの作成

ポータルでの UTF-8 文字のサポート

## デバイス ポータルのデバイス管理設定

これらの設定へのナビゲーション パスは、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [デバイス ポータル（My Devices Portals）] > [作成、編集または複製（Create, Edit or Duplicate）] > [ポータル ページのカスタマイズ（Portal Page Customization）] > [デバイスの管理（Manage Device）]** です。

[ページのカスタマイズ（Page Customizations）] で、デバイス ポータルの [アカウントの管理（Manage Accounts）] タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

[設定（Settings）] では、このデバイス ポータルを使用する従業員が各自の登録されたパーソナル デバイスで実行可能なアクションを指定できます。

**表 *63 :* デバイス ポータルのデバイス管理設定**

| フィールド | 使用上のガイドライン |
|---|---|
| 紛失（Lost） | すべてのデバイス。<br>デバイスを紛失したことを従業員が示すことができるようにします。このアクションは、デバイス ポータルのデバイスのステータスを [紛失（Lost）] に更新し、ブラックリストのエンドポイントの ID グループにそのデバイスを追加します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| 復元（Reinstate） | すべてのデバイス。<br>このアクションでは、ブロックリストに記載されているか、紛失したか、または盗難されたデバイスを復元し、そのステータスを最後の既知の値にリセットします。このアクションでは、ネットワークに接続する前に追加プロビジョニングを実行する必要があるため、盗難デバイスのステータスを [未登録（Not Registered）] にリセットします。<br>ブロックリストに記載されているデバイスを従業員が復元できないようにする場合は、デバイスポータルでこのオプションを有効にしないでください。 |
| 削除（Delete） | すべてのデバイス。<br>登録済みデバイスの最大数に到達した場合、従業員が、登録されたデバイスをデバイス ポータルから削除したり、未使用のデバイスを削除して新しいデバイスを追加したりできるようにします。このアクションによって、デバイス ポータルに表示されるデバイス リストからデバイスが削除されますが、デバイスはCisco ISEデータベースに残り、エンドポイントのリストに表示されます。<br>BYOD またはデバイス ポータルを使用して従業員が登録できるパーソナル デバイスの最大数を定義するには、**[管理（Administration）] > [デバイス ポータル管理（Device Portal Management）] > [設定（Settings）] > [従業員登録済みデバイス（Employee Registered Devices）]** を選択します。<br>Cisco ISE データベースからデバイスを完全に削除するには、**[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）]** を選択します。 |
| 盗難（Stolen） | すべてのデバイス。<br>デバイスが盗まれたことを従業員が示すことができるようにします。このアクションは、デバイス ポータルのデバイスのステータスを [盗難（Stolen）] に更新し、ブラックリストのエンドポイントのIDグループにそのデバイスを追加し、証明書を削除します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| デバイス ロック | MDM 登録デバイスのみ。<br>デバイスの紛失または盗難が発生した場合、従業員がすぐにデバイス ポータルからリモートでデバイスをロックできるようにします。このアクションによって、デバイスの不正使用が防止されます。<br>ただし、デバイス ポータルでは PIN を設定できないため、従業員が事前にモバイル デバイスに設定しておく必要があります。 |
| 登録解除（Unenroll） | MDM 登録デバイスのみ。<br>職場でデバイスを使用する必要がなくなった場合に、従業員がこのオプションを選択できるようにします。このアクションでは、会社がインストールしているアプリケーションと設定のみが削除され、従業員のモバイルデバイス上の他のアプリケーションおよびデータは維持されます。 |
| 完全消去（Full wipe） | MDM 登録デバイスのみ。<br>デバイスを紛失したり、新しいものに交換したりした場合に、従業員がこのオプションを選択できるようにします。このアクションでは、従業員のモバイル デバイスを工場出荷時のデフォルト設定にリセットし、インストール済みのアプリケーションとデータを削除します。 |

**関連トピック**

従業員が追加するパーソナル デバイスの管理
デバイス ポータル

## デバイス ポータルのデバイス カスタマイズの追加、編集、および検索

これらの設定へのナビゲーション パスは、**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **[デバイス ポータル（My Devices Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータル ページのカスタマイズ（Portal Page Customization）]** > **[デバイスの追加、デバイスの編集またはデバイスの検索（Add Devices, Edit Devices or Locate Devices）]** です。

[ページのカスタマイズ（Page Customizations）] で、デバイス ポータルの [追加（Add）]、[編集（Edit）]、および [検索（Locate）] の各タブに表示される、メッセージ、タイトル、コンテンツ、手順、およびフィールドやボタンのラベルをカスタマイズできます。

**関連トピック**

デバイス ポータル

デバイス ポータルの作成

# デバイス ポータルのサポート情報ページの設定

この設定へのナビゲーションパスは、**[管理（Administration）]** > **[デバイス ポータル管理（Device Portal Management）]** > **[BYOD ポータル（BYOD Portals）]/[クライアント プロビジョニング ポータル（Client Provisioning Portals）]/[MDM ポータル（MDM Portals）]/[デバイス ポータル（My Device Portals）]** > **[作成、編集または複製（Create, Edit or Duplicate）]** > **[ポータルの動作およびフローの設定（Portal Behavior and Flow Settings）]** > **[サポート情報ページの設定（Support Information Page Settings）]** です。

これらの設定を使用して、ヘルプデスクがユーザ（状況に応じてゲスト、スポンサーまたは従業員）が体験したアクセスの問題をトラブルシューティングするために使用できる情報を表示します。

| フィールド | 使用上のガイドライン |
|---|---|
| サポート情報ページを含める（Include a Support Information Page） | 該当ポータルのすべての有効なページ上で、**問い合わせ先**などの情報へのリンクを表示します。 |
| MAC アドレス | [サポート情報（Support Information）] ページにデバイスの MAC アドレスを含めます。 |
| IP アドレス | [サポート情報（Support Information）] ページにデバイスの IP アドレスを含めます。 |
| ブラウザのユーザ エージェント（Browser user agent） | [サポート情報（Support Information）] ページに、要求の発信元のユーザ エージェントの製品名とバージョン、レイアウトエンジン、バージョンなど、ブラウザの詳細を含めます。 |
| ポリシー サーバ（Policy server） | [サポート情報（Support Information）] ページに、このポータルを提供している ISE ポリシー サービス ノード（PSN）の IP アドレスを含めます。 |
| 障害コード（Failure code） | 可能な場合は、ログ メッセージ カタログ内の対応する番号を含めます。メッセージ カタログにアクセスしてこれを表示するには、**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[メッセージ カタログ（Message Catalog）]** に移動します。 |

| フィールド | 使用上のガイドライン |
|---|---|
| フィールドを隠す（Hide field） | 含める情報が存在しない場合、[サポート情報（Support Information）] ページ上の該当するフィールドラベルを表示しません。たとえば、障害コードが不明であるために空白である場合、[障害コード（Failure code）] は、選択されている場合でも表示されません。 |
| 値のないラベルを表示（Display label with no value） | 含める情報が存在しない場合でも、選択されているすべてのフィールドのラベルを[サポート情報（Support Information）]ページに表示します。たとえば、障害コードが不明な場合、[障害コード（Failure code）] は空白であっても表示されます。 |
| デフォルト値でラベルを表示（Display label with default value） | [サポート情報（Support Information）] ページ上の選択されているフィールドに含まれる情報が存在しない場合、このテキストがこれらのすべてのフィールドに表示されます。たとえば、このフィールドに「Not Available」と入力した場合に障害コード不明が不明な場合は、[障害コード（Failure code）] に [使用できません（Not Available）] と表示されます。 |

**関連トピック**

デバイス ポータルおよびエンドポイント アクティビティのモニタ
デバイス ポータルへのアクセス