デバイス管理

TACACS+ デバイス管理

Cisco ISE は、ネットワークデバイスの設定の制御と監査を行うため、TACACS+ セキュリティ プロトコルを使用したデバイス管理をサポートしています。ネットワークデバイスは、デバイス管理者の操作の認証および許可のために Cisco ISE にクエリを行うために設定され、Cisco ISE のアカウンティングメッセージを送信して操作をログに記録します。これによって、どのネットワーク デバイスに誰がアクセスできて関連するネットワーク設定を変更できるかについて、きめ細かい制御が容易になります。Cisco ISE 管理者は、コマンドセットやシェルプロファイルなどの TACACS 結果をデバイス管理アクセスサービスの認証ポリシールールで選択できるようにするポリシーセットを作成できます。Cisco ISE モニタリングノードでは、デバイス管理に関する高度なレポートが提供されます。[ワークセンター（Work Center）] メニューには、すべてのデバイス管理ページが含まれており、ISE 管理者の単一の始点として機能します。

Cisco ISE には、TACACS+ を使用するためのデバイス管理ライセンスが必要です。

デバイス管理については 2 つのタイプの管理者がいます。

- デバイス管理者
- Cisco ISE 管理者

デバイス管理者は、管理対象デバイスの設定と保守を実行するために、（通常は SSH を介して）スイッチ、ワイヤレスアクセスポイント、ルータ、ゲートウェイなどのネットワークデバイスにログインするユーザーです。Cisco ISE 管理者は、デバイス管理者がログインするデバイスの設定と調整のために Cisco ISE にログインします。

Cisco ISE にログインしてデバイス管理者の操作を制御する設定を行う Cisco ISE 管理者がこのドキュメントの対象読者です。Cisco ISE 管理者は、デバイス管理機能（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work centers）] > [デバイス管理（Device Administration）]**）を使用して、ネットワークデバイスの構成を制御および監査します。デバイスは、TACACS のセキュリティプロトコルを使用して Cisco ISE サーバーにクエリを行うように設定できます。Cisco ISE モニタリングノードでは、デバイス管理に関する高度なレポートが提供されます。Cisco ISE 管理者は、次のタスクを実行できます。

- TACACS+ の詳細（共有秘密）によるネットワーク デバイスの設定。
- 内部ユーザーとしてのデバイス管理者の追加、および必要に応じてイネーブルパスワードの設定。
- コマンドセットやシェル プロファイルなどの TACACS 結果をデバイス管理アクセス サービスの許可ポリシー ルールで選択できるようにするポリシー セットの作成。
- デバイス管理者がポリシーセットに基づいてデバイスにアクセスできるようにするための Cisco ISE での TACACS サーバーの設定。

デバイス管理者は、Cisco ISE サーバーと通信するためのデバイスの設定タスクを実行します。デバイス管理者がデバイスにログインすると、デバイスは Cisco ISE サーバーにクエリを行い、次に内部または外部の ID ストアにクエリを行い、デバイス管理者の詳細を検証します。検証が Cisco ISE サーバーによって行われると、デバイスは、アカウンティングと監査の目的で、各セッションまたはコマンド許可操作の最終結果を Cisco ISE サーバーに通知します。

ISE 管理者は、TACACS および TACACS+ を使用してデバイスを管理できます。

（注） TACACS+ の操作を有効にするには、[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [全般設定（General Settings）] ページの [デバイス管理サービスの有効化（Enable Device Admin Service）] チェックボックスをオンにする必要があります。このオプションは展開内の各 PSN で必ず有効にしてください。

TACACS+ プロトコルの既知の制限により、スイッチまたはルータと Cisco ISE 間のセキュアな接続を確立するため、IP セキュリティプロトコルが二者間に展開されていることを確認してください。

ISE コミュニティ リソース

デバイス管理属性については、「ISE Device Administration Attributes」を参照してください。

ワイヤレス LAN コントローラ、Cisco IOS ネットワークデバイス、Cisco NX-OS ネットワークデバイス、およびネットワークデバイスの TACACS+ 設定については、「ISE Device Administration (TACACS+)」を参照してください。

デバイス管理ワーク センター

[ワークセンター（Work Center）] メニューには、すべてのデバイス管理ページが含まれており、Cisco ISE 管理者の単一の始点として機能します。ただし、ユーザー、ユーザー ID グループ、ネットワーク デバイス、デフォルト ネットワーク デバイス、ネットワーク デバイス グループ、認証および許可条件などのデバイス管理に固有ではないページは、[管理（Administration）] などの元のメニュー オプションから、アクセスすることができます。[ワークセンター（Work Centers）] オプションは、正しい TACACS+ ライセンスが取得され、インストールされている場合にのみ使用できます。

[デバイス管理（Device Administration）] メニューには、次のメニュー オプションが含まれています。[概要（Overview）]、[ID（Identities）]、[ユーザー ID グループ（User Identity Groups）]、[外部 ID ストア（Ext ID Stores）]、[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）]、[ポリシー要素（Policy Elements）]、[デバイス管理ポリシーセット（Device Admin Policy Sets）]、[レポート（Reports）] および [設定（Settings）]。

デバイス管理の展開設定

[デバイス管理の展開（Device Administration Deployment）] ページ（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [概要（Overview）] > [展開（Deployment）]**）では、Cisco ISE 管理者は [展開（deployment）] セクションで各ノードを確認することなく、デバイス管理システムを一元的に表示できます。

[デバイス管理の展開（Device Administration Deployment）] ページには、展開内の PSN が一覧表示されます。これにより、展開内の各 PSN でデバイス管理サービスを個別に有効にする作業が簡単になります。次のオプションを選択することで、多くの PSN に対するデバイス管理サービスを集合的に有効にできます。

表 *1 : [デバイス管理の展開（Device Administration Deployment）] ウィンドウのオプションリスト*

オプション	説明
なし（None）	デフォルトでは、デバイス管理サービスはすべてのノードで無効になっています。

オプション	説明
すべてのポリシーサービスノード（All Policy Service Nodes）	すべての PSN でデバイス管理サービスを有効にします。このオプションを使用すると、新しい PSN はデバイス管理のために追加されるときに自動的に有効になります。
特定のノード（Specific Nodes）	展開内のすべての PSN をリストしている [ISE ノード（ISE Nodes）] セクションが表示されます。デバイス管理サービスを有効にする必要があるノードを選択できます。

（注） 展開に TACACS+ のライセンスがない場合、上記のオプションは無効になります。

[TACACSポート（TACACS Ports）] フィールドでは、最大 4 つの TCP ポートをカンマ区切りで入力できます。ポート値の範囲は 1 ～ 65535 です。Cisco ISE ノードおよびそのインターフェイスは指定されたポートで TACACS+ 要求をリッスンします。指定されたポートが他のサービスで使用されないようにする必要があります。デフォルトの TACACS+ ポート値は 49 です。

[保存（Save）] をクリックすると、**[管理（Administration）] > [システム（System）] > [展開のリスト（Deployment Listing）]** ウィンドウで指定されたノードと変更が同期されます。

デバイス管理ポリシー セット

[デバイス管理ポリシーセット（Device Admin Policy Sets）] ウィンドウ（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシーセット（Device Admin Policy Sets）]**）には、Cisco ISE 管理者が TACACS+ デバイス管理者の認証と許可を制御するために管理するポリシーセットのリストが含まれています。各ポリシーでは、[通常（Regular）] および [プロキシシーケンス（Proxy Sequence）] の 2 つのモードのいずれかを使用できます。

通常のポリシー セットは認証ルール テーブルおよび許可ルール テーブルから成ります。認証ルールテーブルには、ネットワーク デバイスの認証に必要なアクションを選択する一連のルールが含まれています。

許可ルール テーブルは、承認ビジネス モデルを実装するために必要な特定の承認結果を選択するための一連のルールが含まれています。各許可ルールは、連動するようにルールに一致する必要がある 1 つ以上の条件と、許可プロセスを制御するために選択される一連のコマンド セット、および/またはシェル プロファイルで構成されます。各ルール テーブルには、特定の状況のルールを上書きするために使用できる例外ポリシーがあり、多くの場合、例外テーブルは一時的な状況に使用されます。

（注） TACACS + CHAP アウトバウンド認証はサポートされていません。

プロキシ シーケンス ポリシー セットには、単一の選択されたプロキシ シーケンスが含まれています。ポリシーセットがこのモードである場合、1 台以上のリモートプロキシサーバーが要求の処理に使用されます（ただし、ローカルアカウンティングがプロキシシーケンスで設定されている場合があります）。

デバイス管理ポリシー セットの作成

デバイス管理ポリシー セットを作成するには、次の手順を実行します。

始める前に

- [ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [概要（Overview）] > [展開（Deployment）] ウィンドウで、デバイス管理が TACACS+ 操作に対して有効になっていることを確認します。
- ポリシーに必要なユーザー ID グループ（たとえば、System_Admin、Helpdesk）が作成されていることを確認します。（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ユーザー ID グループ（User Identity Groups）]** ページ）。メンバーユーザー（たとえば、ABC、XYZ）が対応するグループに割り当てられていることを確認します。（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ID（Identities）] > [ユーザー（Users）] ウィンドウ）
- 管理しなければならないデバイスで TACACS 設定を行います。（デバイスが Cisco ISE にクエリを行いやすいようにするために、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 [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）] チェックボックスがイネーブルで、TACACS およびデバイスの共有秘密が同一になっています）
- デバイス タイプとロケーションに基づいたネットワーク デバイス グループが作成されていることを確認します。（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[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グループ（Network Device Groups）]** ウィンドウ）

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシーセット（Device Admin Policy Sets）]**。

ステップ 2 いずれかの行の [アクション（Actions）] 列から、歯車アイコンをクリックし、ドロップダウンリストから、必要に応じて、挿入オプションまたは複製オプションのいずれかを選択して新しいポリシー セットを挿入します。
[ポリシー セット（Policy Sets）] テーブルに新しい行が表示されます。

ステップ 3 ポリシー セットの名前と説明を入力します。

ステップ 4 必要であれば、[許可されているプロトコル/サーバー順序（Allowed Protocols/Server Sequence）] 列から、（+）記号をクリックし、次のいずれかを選択します。

a) 新しい許可されているプロトコルを作成（Create a New Allowed Protocol）
b) TACACS サーバー順序を作成（Create a TACACS Server Sequence）

ステップ 5 [条件（Conditions）] 列から、（+）記号をクリックします。

ステップ 6 [条件スタジオ（Conditions Studio）] ページで必要な条件を作成します。[エディタ（Editor）] セクションで、[クリックして属性を追加する（Click To Add an Attribute）] テキスト ボックスをクリックし、必要なディクショナリと属性（たとえば、Device-Location Equals Europe）を選択します。

ライブラリ条件を [クリックして属性を追加する（Click To Add An Attribute）] テキスト ボックスにドラッグ アンド ドロップできます。

ステップ 7 [使用（Use）] をクリックします。

ステップ 8 [表示（View）] 列から、 をクリックしてすべてのポリシーセットの詳細にアクセスし、認証および許可ポリシーとポリシー例外を作成します。

ステップ 9 必要な認証ポリシーを作成します（たとえば、Rule Name: ATN_Internal_Users、Conditions: DEVICE:Location EQUALS Location #All Locations#Europe：このポリシーは、ヨーロッパ内にあるデバイスにのみ一致します）。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 必要な許可ポリシーを作成します。

例 1：ルール名：Sys_Admin_rule、条件：if SysAdmin and TACACS User Equals ABC then cmd_Sys_Admin AND Profile_priv_8。この例で、ポリシーはユーザー名 ABC のシステム管理者を照合し、指定されたコマンドの実行を許可し、特権レベル 8 を割り当てます。

例 2：ルール名：HelpDesk AND TACACS User EQUALS XYZ then cmd_HDesk_show AND cmd_HDesk_ping AND Profile_priv_1。この例で、ポリシーはユーザー名 XYZ のシステム管理者を照合し、指定されたコマンドの実行を許可し、特権レベル 1 を割り当てます。

上記の例で、

- コマンドセット cmd_Sys_Admin と cmd_HDesk は、[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS コマンドセット（TACACS Command Sets）] > [追加（Add）] ウィンドウで作成されます。
- TACACS プロファイル Profile_Priv_1 と Profile_priv_8 は、[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS プロファイル（TACACS Profiles）] > [追加（Add）] ウィンドウで作成されます。

（注） 認証および許可ポリシーで使用される条件で、デバイス IP アドレス属性に IPv4 または IPv6 の単一アドレスを追加できます。

ステップ 12　[保存（Save）] をクリックします。

TACACS+ 認証設定と共有秘密

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）] ウィンドウ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）Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[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）Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[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。

フィールド名	使用上のガイドライン
共有秘密鍵（Shared Secret）	TACACS+ プロトコルが有効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。ユーザーは、ネットワーク デバイスによってユーザー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。ユーザー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。
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。

フィールド名	使用上のガイドライン
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。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[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。 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。 • [レガシーシスコデバイス（Legacy Cisco Devices）] • 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無効にすると、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。

要約すると、次のことができます。

- 廃止期間を日数として指定することで（範囲は 1 ～ 99 です）、古い共有秘密を廃止し、同時に新しい共有秘密を設定することができます。
- 廃止期間中は新旧の共有秘密を使用できます。
- 期限切れになる前に廃止期間を延長できます。
- 廃止期間の終了までは、古い共有秘密のみを使用できます。
- 期限切れになる前に廃止期間を終了できます（[終了（End）] をクリックしてから [送信（Submit）] をクリックします）。

（注） Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[TACACS+ 認証設定（TACACS+ Authentication Settings）] オプションにアクセスするには、**[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）]** > **[追加（Add）]** ウィンドウ。

デバイス管理：許可ポリシーの結果

Cisco ISE 管理者は、TACACS+ コマンドセットおよび TACACS+ プロファイル（ポリシー結果）を使用して、デバイス管理者に付与される権限およびコマンドを制御することができます。ポリシーはネットワークデバイスとともに動作するので、行われる可能性がある偶発的または悪意のある設定変更が回避されます。そのような変更が発生した場合は、デバイス管理の監査レポートを使用して、特定のコマンドを実行したデバイス管理者を追跡することができます。

TACACS+ デバイス管理を許可された FIPS および非 FIPS モードのプロトコル

ポリシーの結果を作成するための Cisco ISE が提供する多数の許可された認証プロトコル サービスがあります。ただし、TACACS+ プロトコルに適用される PAP/ASCII、CHAP および MS-CHAPv1 などの認証プロトコルサービスは、RADIUS の FIPS 対応 Cisco ISE アプライアンスで無効になります。その結果、FIPS 対応（**[管理（Administration）]** > **[システム設定（System Settings）]** > **[FIPSモード（FIPS Mode）]**）Cisco ISEアプライアンスを使用している場合は、デバイスの管理のために **[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可されているプロトコル（Allowed Protocols）]** ウィンドウでこれらのプロトコルを有効にすることはできません。

デバイス管理ポリシーの結果で PAP/ASCII、CHAP および MS-CHAPv1 プロトコルを設定するには、FIPS モードと非 FIPS モードのどちらの場合も、**[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可されているプロトコル（Allowed Protocols）]** ウィンドウに移動する必要があります。FIPS モードを有効にすると、デフォルト デバイス管理で許可されたプロトコル設定のみが使用できます。このオプションは、RADIUS では使用できません。

TACACS+ コマンド セット

コマンドセットは、デバイス管理者が実行できるコマンドの指定されたリストを適用します。デバイス管理者がネットワークデバイスに対して操作コマンドを発行すると、その管理者がこれらのコマンドの発行を認可されているかどうかを判定する問い合わせが Cisco ISE に行われます。これは、コマンド認可とも呼ばれます。

コマンド セットのワイルドカードと正規表現

コマンド ラインは、コマンドと 0 個以上の引数から成ります。Cisco ISE は、コマンド ライン（要求）を受信すると、次のさまざまな方法でコマンドおよび引数を処理します。

- ワイルドカード照合パラダイムを使用して、要求内のコマンドをコマンドセットのリストに指定されたコマンドと照合します。

  例：Sh?? または S*

- 正規表現（regex）照合パラダイムを使用して、要求内の引数をコマンドセットのリストに指定された引数と照合します。

  例：Show interface[1-4] port[1-9]:tty*

コマンド ラインおよびコマンド セットのリストの一致

要求されたコマンドラインをワイルドカードおよび正規表現を含むコマンドセットリストと照合するには、次の手順を実行します。

1. コマンド セットのリストを反復し、一致するコマンドを検出します。

   ワイルドカード照合では以下が許可されています。

   - 大文字小文字の区別なし。
   - コマンドセット内のコマンドの任意の文字を「?」にし、要求されたコマンドに存在する必要がある個別の文字に一致させることができます。
   - コマンドセット内のコマンドの任意の文字を「*」にし、要求されたコマンド内の 0 個以上の文字に一致させることができます。

     次に、例を示します。

要求	コマンド セット	一致	説明
show	show	Y	—
show	SHOW	Y	大文字小文字の区別なし
show	Sh??	Y	任意の文字と一致します
show	Sho??	N	2つ目の「?」は存在しない文字と交差します
show	S*	Y	「*」は任意の文字と一致します
show	S*w	Y	「*」は文字「ho」と一致します
show	S*p	N	文字「p」は対応しません

2. 一致する各コマンドに対し、Cisco ISE は引数を検証します。

   コマンドセットリストには、各コマンドのスペースで区切られた一連の引数が含まれています。

例：Show interface[1-4] port[1-9]:tty.*

このコマンドには、2 つの引数があります。

1. 引数 1：interface[1-4]

2. 引数 2：port[1-9]:tty.*

要求内のコマンド引数は、パケットに表示される位置が重要な順序で実行されます。コマンド定義内のすべての引数が要求内の引数に一致すると、このコマンドまたは引数は一致していると見なされます。要求内の無関係な引数はすべて無視されます。

（注） 引数には標準の Unix 正規表現を使用します。

複数のコマンド セットを持つルールの処理

1. コマンドセットにコマンドとその引数との一致が含まれる場合、その一致が Deny Always であると、Cisco ISE によってそのコマンドセットは Commandset-DenyAlways として指定されます。
2. コマンドセット内のコマンド一致に Deny Always が含まれていない場合は、Cisco ISE によって最初の一致が見つかるまで、コマンドセット内のすべてのコマンドが順番にチェックされます。
    1. 最初の一致が Permit である場合、Cisco ISE はそのコマンドセットを Commandset-Permit として指定します。
    2. 最初の一致が Deny である場合、Cisco ISE はそのコマンド セットを Commandset-Deny として指定します。
3. Cisco ISE は、すべてのコマンドセットを分析したあと、コマンドを次のように認可します。
    1. Cisco ISE がコマンドセットを Commandset-DenyAlways として指定した場合は、Cisco ISE はそのコマンドを拒否します。
    2. Commandset-DenyAlways がない場合、Cisco ISE はコマンドセットが Commandset-Permit であれば、そのコマンドを許可します。そうでない場合、そのコマンドを拒否します。唯一の例外は、[不一致（Unmatched）] チェックボックスがオンになっている場合です。

TACACS+ コマンド セットの作成

TACACS+ コマンドセットのポリシー結果を使用してポリシーセットを作成するには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS コマンドセット（TACACS Command Sets）]**。

[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシーセット（Device Admin Policy Sets）] ページで TACACS コマンドセットを設定することもできます。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 名前と説明を入力します。

ステップ 4 [追加（Add）] をクリックして、権限の付与、コマンドおよび引数を指定します。

ステップ 5 [付与（Grant）] ドロップダウンで、以下のいずれかを選択できます。

- [許可（Permit）]：指定したコマンドを許可する場合（たとえば、permit show、permit con* Argument terminal など）。
- [拒否（Deny）]：指定したコマンドを拒否する場合（たとえば、deny mtrace）。
- [常に拒否（Deny Always）]：他のコマンドセットで許可されているコマンドをオーバーライドする場合（たとえば、clear auditlogs）。

（注） [付与（Grant）]、[コマンド（Command）] および [引数（Argument）] フィールドの列幅を増やしたり減らしたりするには、アクション アイコンをクリックします。

ステップ 6 [下にリストされていないコマンドを許可（Permit any command that is not listed below）] チェックボックスをオンにして、[付与（Grant）] 列で [許可（Permit）]、[拒否（Deny）] または [常に拒否（Deny Always）] として指定されていないコマンドおよび引数を許可します。

TACACS+ プロファイル

TACACS+ プロファイルは、デバイス管理者の最初のログイン セッションを制御します。セッションは、個々の認証、許可、またはアカウンティングの要求を参照します。ネットワーク デバイスへのセッション認可要求により、Cisco ISE 応答が発生します。この応答には、ネットワークデバイスにより解釈されるトークンが含まれており、これはセッション期間中に実行できるコマンドを制限します。デバイス管理アクセス サービス用の許可ポリシーでは、単一のシェル プロファイルおよび複数のコマンド セットを含めることができます。TACACS+ プロファイル定義は、次の 2 つのコンポーネントに分けられています。

- 共通タスク
- カスタム属性

[TACACS+ プロファイル（TACACS+ Profiles）] ウィンドウ（Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS プロファイル（TACACS Profiles）]**）には、**[タスク属性（Task**

Attribute）] ビューと **[未処理（Raw）]** ビューの 2 つのビューがあります。共通タスクは [タスク属性（Task Attribute）] ビューを使用して入力でき、カスタム属性は [タスク属性（Task Attribute）] ビューおよび [未処理（Raw）] ビューで作成できます。

[共通タスク（Common Tasks）] セクションを使用すると、頻繁に使用されるプロファイルの属性を選択および設定できます。ここに含まれる属性は、TACACS+ プロトコル ドラフト仕様で定義された属性です。ただし、これらの値は、他のサービスからの要求の許可に使用される場合があります。[タスク属性（Task Attribute）] ビューでは、Cisco ISE 管理者はデバイス管理者に割り当てられる権限を設定できます。一般的なタスクのタイプは次のとおりです。

- Shell
- Cisco WLC
- Cisco Nexus
- 汎用

[カスタム属性（Custom Attributes）] セクションでは、追加の属性を設定できます。[共通タスク（Common Tasks）] セクションで認識されていない属性のリストも提供されます。各定義は、属性名、属性が必須であるか任意であるかの指定、および属性の値で構成されています。

（注） TACACS 対応ネットワークデバイスには、合計 24 個のタスク属性を定義できます。24 を超えるタスク属性を定義した場合、いずれの属性も TACACS 対応ネットワークデバイスに送信されません。

[未処理（Raw）] ビューでは、属性名とその値の間に等号（=）を使用して必須属性を入力でき、属性名とその値の間にアスタリスク（*）を使用して任意の属性を入力できます。[未処理（Raw）] ビューセクションで入力した属性は、[タスク属性（Task Attribute）] ビューの [カスタム属性（Custom Attributes）] セクションに反映され、その逆も同様です。[未処理（Raw）] ビューセクションは、クリップボードから属性リスト（たとえば、別の製品の属性リスト）を Cisco ISE にコピーアンドペーストするためにも使用されます。カスタム属性は、非シェル サービスに対して定義できます。

TACACS+ プロファイルの作成

TACACS+ プロファイルを作成するには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）]** > **[デバイス管理（Device Administration）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[TACACSプロファイル（TACACS Profiles）]**。

[ワークセンター（Work Centers）] > **[デバイス管理（Device Administration）]** > **[デバイス管理ポリシーセット（Device Admin Policy Sets）]** ページで TACACS コマンドセットを設定することもできます。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [TACACSプロファイル（TACACS Profile）] セクションで、名前と説明を入力します。

ステップ 4 [タスク属性ビュー（Task Attribute View）] タブで、必要な**共通タスク**を確認します。共通タスク設定 （14 ページ）ページを参照してください。

ステップ 5 [タスク属性ビュー（Task Attribute View）] タブの [カスタム属性（Custom Attributes）] セクションで、[追加（Add）] をクリックして必須属性を入力します。

共通タスク設定

共通タスクの設定ウィンドウを表示するには、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TACACS プロファイル（TACACS Profiles）] > [追加（Add）]**。一般的なタスクタイプは、Shell、Cisco WLC、Cisco Nexus および Generic です。

Shell

次のオプションは、Cisco ISE の管理者がデバイスの管理者権限を設定するために使用できます。

オプション	説明
デフォルトの権限（Default Privilege）	シェル認可のデバイス管理者のデフォルトの（最初の）権限レベルを有効にします。次のオプションのいずれかを選択します。 • 0 ～ 15 の範囲の値を選択します。 • 必要な ID ストア属性を選択します。
最大権限（Maximum Privilege）	イネーブル認証の最大権限レベルを有効にします。0 ～ 15 の範囲の値を選択できます。
アクセス コントロール リスト（Access Control List）	ASCII 文字列（1-251*）または必要な ID ストア属性を選択します。
自動コマンド（Auto Command）	ASCII 文字列（1-248*）または必要な ID ストア属性を選択します。
エスケープなし（No Escape）	エスケープ文字に、次のいずれかのオプションを選択します。 • [はい（True）]：エスケープ防止を有効にすることを指定します。 • [いいえ（False）]：エスケープ防止を有効にしないことを指定します。 • 必要な ID ストア属性を選択します。

オプション	説明
タイムアウト（Timeout）	0 ～ 9999 の範囲の値または必要な ID ストア属性を選択します。
アイドル時間（Idle Time）	0 ～ 9999 の範囲の値または必要な ID ストア属性を選択します。

Cisco WLC

次のオプションは、Cisco ISE の管理者がデバイス管理者による Cisco WLC アプリケーションのタブへのアクセスを制御するために使用できます。Cisco WLC アプリケーションには次のタブが含まれます。[WLAN]、[コントローラ（Controller）]、[ワイヤレス（Wireless）]、[セキュリティ（Security）]、[管理（Management）] および [コマンド（Commands）]。

オプション	説明
すべて（All）	デバイスの管理者はすべての Cisco WLC アプリケーションのタブにアクセスできます。
モニタ（Monitor）	デバイス管理者は Cisco WLC アプリケーションのタブへの読み取り専用アクセス権を持ちます。
ロビー（Lobby）	デバイス管理者は限定された設定の権限のみを持ちます。
選択（Selected）	デバイス管理者は次のチェックボックスから Cisco ISE 管理者がチェックしたタブにアクセスできます。[WLAN]、[コントローラ（Controller）]、[ワイヤレス（Wireless）]、[セキュリティ（Security）]、[管理（Management）] および [コマンド（Commands）]。

Nexus

次のオプションは、Cisco ISE の管理者がデバイス管理者による Cisco Nexus スイッチへのアクセスを制御するために使用できます。

オプション	説明
属性の設定（Set Attribute As）	Cisco ISE の管理者は、任意または必須として一般的なタスクによって生成された Nexus 属性を指定できます。

オプション	説明
ネットワークロール（Network Role）	Nexus が Cisco ISE を使用して認証するように設定されると、デバイス管理者は、デフォルトでは、読み取り専用アクセス権を持ちます。デバイス管理者は、これらのロールのいずれかに割り当てることができます。各ロールは許可された操作を定義します。 • [なし（None）]：権限はありません。 • [オペレータ（Operator）]（読み取り専用）：全NX-OSデバイスへの完全な読み取りアクセス権を持ちます。 • [管理者（Administrator）]（読み取り/書き込み）：全NX-OSデバイスへの完全な読み取り/書き込みアクセス権を持ちます。
仮想デバイスコンテキスト（VDC）（Virtual Device Context (VDC)）	[なし（None）]：権限はありません。 [オペレータ（Operator）]（読み取り専用）：VDC への限定された読み取りアクセス [管理者（Administrator）]（読み取り/書き込み）：VDCへの限定された読み取り/書き込みアクセス

汎用

Cisco ISE 管理者は、一般的なタスクでは使用できないカスタム属性を指定するオプションを使用します。

CLI によるイネーブルパスワードの変更

イネーブル パスワードを変更するには、次の手順を実行します。

始める前に

一部のコマンドは特権モードに割り当てられます。したがって、デバイスの管理者がこのモードに認証されているときしか実行できません。

そのデバイスの管理者が特権モードに入ろうとする際に、デバイスは特別なイネーブル認証タイプを送信します。Cisco ISE は、この特別なイネーブル認証タイプを検証するために別のイネーブル パスワードをサポートします。別のイネーブル パスワードはデバイスの管理者が内部 ID ストアに認証されているときに使用されます。外部 ID ストアとの認証では、同じパスワードが通常のログインに対して使用されます。

ステップ 1 スイッチにログインします。

ステップ 2 Enter を押して次のプロンプトを表示します。

```
Switch>
```

ステップ 3 次のコマンドを実行して、イネーブル パスワードを設定します。

```
Switch> enable
Password: (Press Enter to leave the password blank.)
Enter Old Password: (Enter the old password.)
Enter New Password: (Enter the new password.)
Enter New Password Confirmation: (Confirm the new password.)
```

（注） パスワードの有効期間がログイン パスワードおよびイネーブル パスワードに設定されている場合、パスワードが指定された時間期間内に変更されないと、ユーザー アカウントは無効になります。Cisco ISE が TACACS+ サーバーとして構成され、ネットワーク デバイスで [バイパスを有効にする（Enable Bypass）] オプションが設定されている場合、CLI から（telnet 経由で）イネーブル パスワードを変更できません。内部ユーザーの enable パスワードを変更するには、Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[管理（Administration）] > [ID 管理（Identity Management）] > [ID（Identities）] > [ユーザー（Users）]** 。

TACACS+ のグローバル設定

TACACS+ のグローバル設定を行うには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[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）] タブで、必須フィールドのデフォルト値を変更できます。

- [認証キャッシュタイムアウト（Authorization cache timeout）] フィールドで、内部ユーザーの特定の属性を最初の認証要求時にキャッシュ化するために存続可能時間（TTL）の値を設定できます。キャッシュ化された属性には、ユーザー名と、UserGroup などのユーザー固有の属性が含まれます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。**[システム管理（System Administration）] > [設定（Configuration）] > [ディクショナリ（Dictionaries）] > [ID（Identity）] > [内部ユーザー（Internal Users）]** で属性を作成します。デフォルト値は 0 です。つまり、認証キャッシュが無効になっています。
- 単一接続のサポート（Single Connect Support）：シングル接続モードを無効にすると、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。

ステップ 2 [パスワード変更制御（Password Change Control）] タブで、パスワードの更新を TACACS+ を介して許可するかどうかを制御するのに必要なフィールドを定義します。

[Telnetパスワード変更を有効にする（Enable Telnet Change Password）] セクションのプロンプトは、このオプションが選択されている場合にのみ有効です。選択されていない場合は、[Telnetパスワード変更を無効にする（Disable Telnet Change Password）] のプロンプトが有効になります。パスワード プロンプトはすべてカスタマイズ可能で、必要に応じて変更できます。

[パスワード ポリシー違反メッセージ（Password Policy Violation Message）] フィールドに、新しいパスワードが指定された条件と一致しない場合に、内部ユーザーが設定したパスワードに適したエラー メッセージを表示できます。

ステップ 3 [セッションキーの割り当て（Session Key Assignment）] タブで、セッションに TACACS+ 要求をリンクするために必要なフィールドを選択します。

セッション キーは、クライアントからの AAA 要求をリンクするためにモニタリング ノードによって使用されます。デフォルト設定では、[NASアドレス（NAS-Address）]、[ポート（Port）]、[リモートアドレス（Remote-Address）]、および [ユーザー（User）] フィールドが有効になっています。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

TACACS+ 認証設定と共有秘密 （7 ページ）

Cisco Secure ACS から Cisco ISE へのデータ移行

移行ツールを使用して、Cisco Secure ACS 5.5 以降からデータをインポートし、すべてのネットワークデバイスにデフォルトの TACACS+ 秘密を設定できます。**[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [概要（Overview）]**Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。[準備（Prepare）] セクションで、[ソフトウェアのダウンロード Web ページ（Download Software Webpage）] をクリックして移行ツールをダウンロードします。ツールを PC に保存し、[migTool] フォルダから migration.bat ファイルを実行し、移行プロセスを開始します。移行に関する詳細については、お使いのバージョンの Cisco ISE の『Migration Guide』を参照してください。

デバイス管理アクティビティのモニター

Cisco ISE では、TACACS+ で設定されたデバイスのアカウンティング、認証、承認、およびコマンドアカウンティングに関する情報を参照できる、さまざまなレポートおよびログが提供されます。オン デマンドまたはスケジュール ベースでこれらのレポートを実行できます。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[ワークセンター（Work Centers）] > [デバイス管理（Device Administration）] > [レポート（Reports）] > [レポート（Reports）]**。.

別の場所でレポートを表示することもできます。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[操作（Operations）]** > **[レポート（Reports）]** > **[レポート（Reports）]** ページを選択します。

ステップ 2 [レポート セレクタ（Report Selector）] で、[デバイス管理（Device Administration）] を展開し、[認証概要（Authentication Summary）]、[TACACS アカウンティング（TACACS Accounting）]、[TACACS 認証（TACACS Authentication）]、[TACACS 許可（TACACS Authorization）]、[TACACS コマンド アカウンティング（TACACS Command Accounting）]、[失敗の理由別上位 N の認証（Top N Authentication by Failure Reason）]、[ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device）]、[ユーザー別上位 N の認証（Top N Authentication by User）] レポートを表示します。

ステップ 3 レポートを選択し、[フィルタ（Filters）] ドロップダウン リストを使用して、検索するデータを選択します。

ステップ 4 データを表示する [時間範囲（Time Range）] を選択します。

ステップ 5 [実行（Run）] をクリックします。

TACACS ライブ ログ

次の表では、TACACS+ AAA の詳細を表示する [TACACS ライブログ（TACACS Live Logs）] ウィンドウのフィールドについて説明します。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして次を選択します。 **[操作（Operations）]** > **[TACACS]** > **[ライブログ（Live Logs）]**。TACACS ライブ ログはプライマリ PAN だけで表示されます。

表 *2 : TACACS* ライブ ログ

フィールド名	使用上のガイドライン
生成日時（Generated Time）	特定のイベントがトリガーされた時点に基づいて、syslog の生成日時を示します。
ログに記録された時刻（Logged Time）	syslog がモニタリング ノードによって処理され、保存された時刻を示します。このカラムは必須です。選択解除することはできません。
ステータス（Status）	認証の成功/失敗を表示します。このカラムは必須です。選択解除することはできません。緑色は認証が成功したことを示します。赤色は認証が失敗したことを示します。
詳細（Details）	虫眼鏡アイコンをクリックすると、選択した認証シナリオをドリルダウンし、詳細情報を確認できるレポートが表示されます。このカラムは必須です。選択解除することはできません。
セッションキー（Session Key）	ISE によってネットワーク デバイスに返される（EAP の成功メッセージまたはEAP の失敗メッセージにある）セッション キーを示します。

フィールド名	使用上のガイドライン
ユーザー名（**Username**）	デバイス管理者のユーザー名を示します。このカラムは必須です。選択解除することはできません。
タイプ（**Type**）	[認証（Authentication）] および [承認（Authorization）] の 2 つのタイプで構成されます。認証、承認、または両方を通過または失敗したユーザー名を表示します。このカラムは必須です。選択解除することはできません。
認証ポリシー（**Authentication policy**）	特定の認証に選択されているポリシーの名前を表示します。
許可ポリシー（**Authorization Policy**）	特定の許可に選択されているポリシーの名前を表示します。
ISEノード（**ISE Node**）	アクセス要求が処理される ISE ノードの名前を表示します。
ネットワークデバイス名（**Network Device Name**）	ネットワーク デバイスの名前を示します。
ネットワークデバイスIP（**Network Device IP**）	アクセス要求を処理するネットワークデバイスのIPアドレスを示します。
ネットワークデバイスグループ（**Network Device Groups**）	ネットワークデバイスが属する対応するネットワーク デバイス グループの名前を表示します。
デバイスタイプ（**Device Type**）	異なるネットワークデバイスからのアクセス要求の処理に使用されるデバイスタイプポリシーを示します。
ロケーション（**Location**）	ネットワークデバイスからのアクセス要求の処理に使用されるロケーションベースのポリシーを示します。
デバイスポート（**Device Port**）	アクセス要求が行われるデバイスのポート番号を示します。
失敗の理由（**Failure Reason**）	ネットワークデバイスによって行われたアクセス要求を拒否した理由を示します。
リモートアドレス（**Remote Address**）	エンドステーションを一意に識別するIPアドレス、MACアドレス、またはその他の任意の文字列を示します。

フィールド名	使用上のガイドライン
一致したコマンドセット（**Matched Command Set**）	MatchedCommandSet 属性値が存在する場合はその値を表示し、MatchedCommandSet 属性値が空の場合、または属性自体が syslog に存在しない場合は空の値を表示します。
シェルプロファイル（**Shell Profile**）	ネットワーク デバイスでコマンドを実行するためのデバイス管理者に付与された権限を示します。

[TACACSライブログ（TACACS Live Logs）] ウィンドウで、次の手順を実行できます。

- データを CSV または PDF 形式でエクスポートします。
- 要件に基づいて列を表示または非表示にします。
- 簡易またはカスタムフィルタを使用してデータをフィルタ処理します。後で使用するためにフィルタを保存することもできます。
- 列の順序を変更したり、列の幅を調整します。
- 列の値をソートします。

（注） ユーザーのカスタマイズはすべて、ユーザー設定として保存されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。