CHAPTER 11

エンドポイント保護サービスの設定

この章では、エンドポイント保護サービス（EPS）の設定方法について説明します。内容は次のとおりです。

エンドポイント保護サービスについて

エンドポイント保護サービス（EPS）は、Cisco Identity Services Engine 管理ノードで実行されるサービスで、エンドポイントのモニタリングおよび制御の機能を拡張します。EPS を使用すると、システムの全体的な許可ポリシーを変更せずに、エンドポイントの許可状態をモニタおよび変更できます。EPS では、有線とワイヤレスの両方の展開をサポートしています。

（注） EPS は、ISE ADVANCED ライセンスでのみ使用できます。ISE ADVANCED ライセンスがインストールされていない場合は、EPS 機能を使用できません。詳細については、第 12 章「ライセンスの管理」を参照してください。

EPS 機能の概要

ここでは、Cisco ISE の EPS の機能面について概要を説明します。EPS 操作は、有線とワイヤレスの両方の展開でサポートされています。

EPS では、次の操作を通じて管理者がエンドポイントを管理できます。

- 隔離：ポリシーを使用して、ネットワークへのエンドポイント アクセスを禁止するか、またはそのアクセスを制限します。ポリシーを作成すると、ステータスに応じて別々の許可プロファイルを割り当てることができます。
- 隔離解除：隔離ステータスを無効にし、ネットワークへのフル アクセスをエンドポイントに許可します。

- シャットダウン：Network Attached System（NAS）のポートを非アクティブにします。ポートがいったんシャットダウンされると、ポートの手動リセットが必要になります。

（注） 手動でポートをリセットする必要があるため、シャットダウン操作はワイヤレス アクセスおよびデバイスには使用できません。

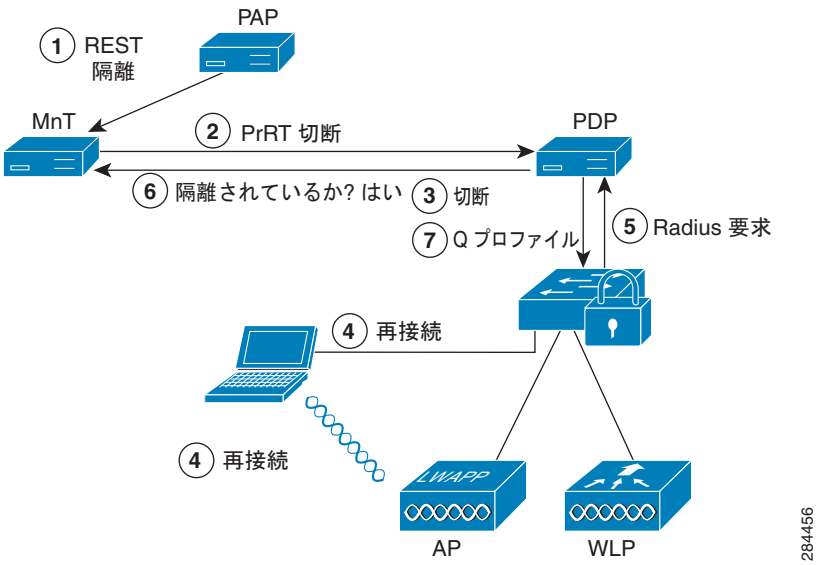
隔離および隔離解除

エンドポイント保護ステータスを隔離に設定し、エンドポイントのステータスに応じてそれぞれ異なる許可プロファイルを割り当てるポリシーを作成できます。

隔離は、基本的に、デフォルトの VLAN から指定した隔離 VLAN にエンドポイントを移動します。隔離 VLAN は、ネットワーク管理者によってあらかじめ定義されている必要があり、また、エンドポイントと同じ NAS でサポートされている必要があります。隔離解除は隔離操作を無効にし、エンドポイントを元の VLAN に戻します。

隔離および隔離解除操作は、EPSStatus を確認するために定義されている作成済み許可ルールの結果として実行されます。図 11-1 の隔離フローでは、ルールが設定済みであり、また EPS セッションが確立済みであることを前提としています。

図 11-1　EPS 隔離フロー



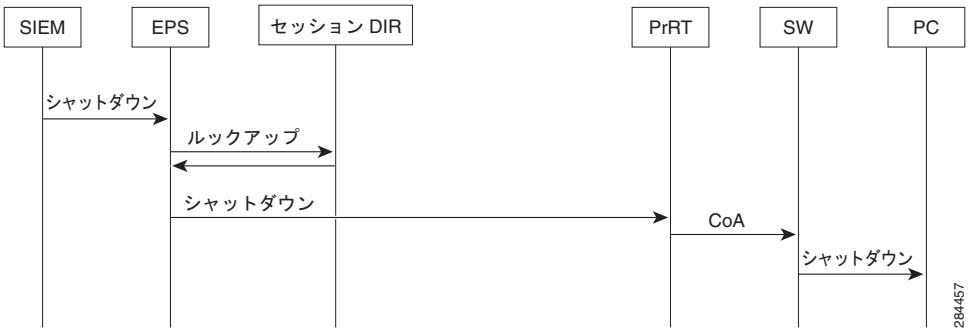
1. PC エンドポイントがワイヤレス デバイス（WLC）を通じてネットワークにログインし、隔離の REST API 呼び出しが管理 ISE ノードからモニタリング ISE ノードに発行されます。
2. 続いて、モニタリング ISE ノードは、ポリシー サービス ISE ノードを通じて PrRT をコールし、CoA を呼び出します。
3. PC エンドポイントが切断されます。
4. PC は再認証を行い、再接続されます。
5. PC エンドポイントに対する RADIUS 要求が、モニタリング ISE ノードに返送されます。
6. チェックが行われている間、PC エンドポイントは隔離されます。
7. Q プロファイル許可ポリシーが適用され、エンドポイントの妥当性が確認されます。

8. PC エンドポイントの隔離が解除され、ネットワークにフル アクセスできるようになります。

シャットダウン

シャットダウン機能により、管理者は指定した MAC アドレスの IP アドレスに基づいて、ポートをクローズできます。この機能はすべてのデバイスでサポートされているわけではありません。図 11-2 に EPS シャットダウン フローを示します。

図 11-2　EPS シャットダウン フロー



図の PC の場合、シャットダウン操作は PC がネットワークへのアクセスに使用するスイッチで実行されます。

警告　この方法でポートをシャットダウンする場合は、ポートを手動でリセットして再度アクティブにする必要があります。

EPS の有効化および無効化

エンドポイント保護サービス（EPS）は、デフォルトでは無効になっています。次の手順に示すとおり、サービスを有効にするにはスーパー管理者またはポリシー管理者のロール権限が必要です。

（注） EPS は、ISE ADVANCED ライセンスでのみ使用できます。ISE ADVANCED ライセンスがインストールされていない場合は、EPS 機能を使用できません。詳細については、第 12 章「ライセンスの管理」を参照してください。

EPS を有効または無効にするには、次の手順を実行します。

ステップ 1　ISE 管理ダッシュボードで、[管理（Administration）] > [システム（System）] > [設定（Settings）] を選択します。

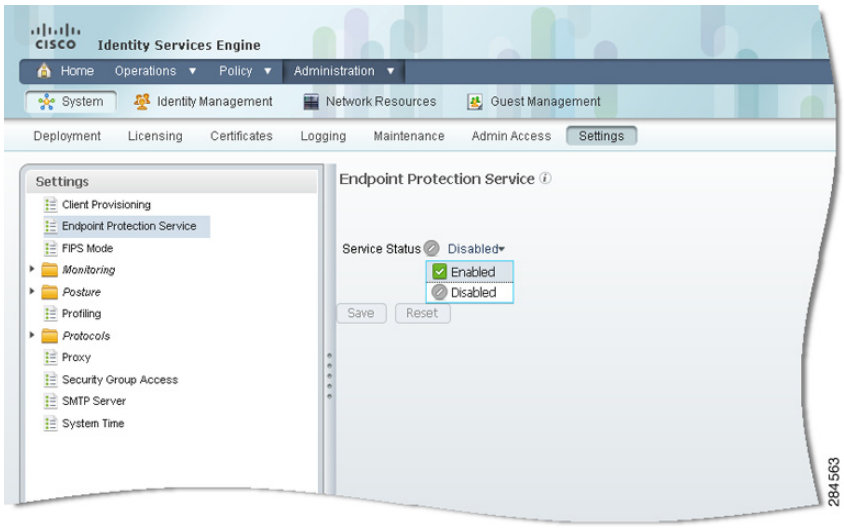
ステップ 2　左側にある [設定（Settings）] パネルで、[エンドポイント保護サービス（Endpoint Protection Service）] を選択します。

ステップ 3　EPS を有効にするには、[サービス ステータス（Service Status）] ドロップダウン メニューから [有効（Enabled）] を選択し、[保存（Save）] をクリックします。

サービスは、手動で無効にするまで有効のままになります。

ステップ 4　EPS を無効にするには、[サービス ステータス（Service Status）] ドロップダウン メニューから [無効（Disabled）] を選択し、[保存（Save）] をクリックします。

図 11-3　　EPS の有効化および無効化



コマンドライン インターフェイス（CLI）を使用して EPS が有効か無効かを確認する方法については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x*』を参照してください。

EPS 許可

EPS では、エンドポイントのアクセス ステータスを隔離、隔離解除、またはシャットダウンにリセットできます。これを行うには、EPS 許可プロファイルおよびポリシー ルールを作成する必要があります。

ここでは、次のトピックについて取り上げます。

- 「隔離許可プロファイルの作成」（P.11-4）
- 「EPS ポリシーおよびルールの作成」（P.11-5）

隔離許可プロファイルの作成

許可プロファイルは、指定したネットワーク サービスへのアクセスを許可するために定義される権限のコンテナとして機能します。許可が完了すると、ネットワーク アクセス要求に権限が付与されます。詳細については、「Cisco ISE 許可ポリシーおよびプロファイル」（P.17-5）を参照してください。

ここでは、隔離許可プロファイルを作成して EPS で使用する方法の例を示します。

隔離許可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 管理ユーザ インターフェイスで、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] に移動します。

ステップ 2　左側にある [結果（Results）] パネルで、[許可（Authorization）] > [許可プロファイル（Authorization Profiles）] を選択します。

右側に [標準許可プロファイル（Standard Authorization Profiles）] パネルが表示されます。

ステップ 3　[標準許可プロファイル（Standard Authorization Profiles）] パネルで、[追加（Add）] をクリックします。

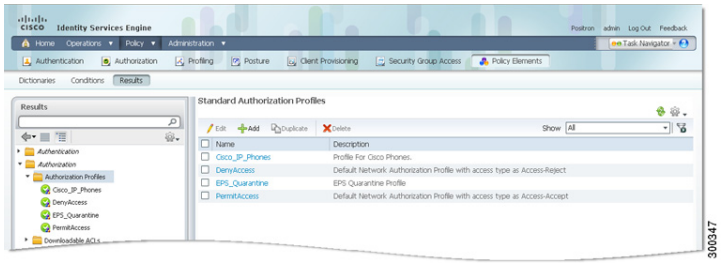
ステップ 4　一意の**名前**および**説明**を入力し、アクセス タイプは ACCESS_ACCEPT のままにしておきます。

ステップ 5　[DACL 名（DACL Name）] チェックボックスをオンにし、ドロップダウン リストから [DENY_ALL_ACCESS] を選択します。

ステップ 6　[保存（Save）] をクリックします。

図 11-4 に示すように、[標準許可プロファイル（Standard Authorization Profiles）] のリストに隔離プロファイルが表示されます。

図 11-4　EPS 隔離プロファイル



EPS ポリシーおよびルールの作成

標準および例外の 2 つのタイプの許可ポリシーがあります。標準ポリシーは不変であり、共通の権限セットを共有するユーザ、デバイス、およびグループの大規模なグループに適用されます。

一方、例外ポリシーは、標準ポリシーの例外として機能します。例外ポリシーは、特別な条件や権限、または緊急の要件を満たすために制限付きアクセスを許可することを目的としています。

EPS 許可では、標準ポリシーの処理以前に処理される隔離ステータス例外ルールを作成しておくことを推奨します。これら両方のタイプのポリシーについては、「許可ポリシーについて」（P.17-1）を参照してください。

前提条件

「隔離許可プロファイルの作成」（P.11-4）を正常に完了している必要があります。

EPS 例外ポリシーおよびルールを作成するには、次の手順を実行します。

ステップ 1　ISE 管理ダッシュボードで、[ポリシー（Policy）] > [許可（Authorization）] を選択し、[例外（Exceptions）] パネルを展開します。

ステップ 2　[新しいルールの作成（Create New Rule）] をクリックし、テキスト フィールドに EPS Exception Rule などのルール名を入力します。

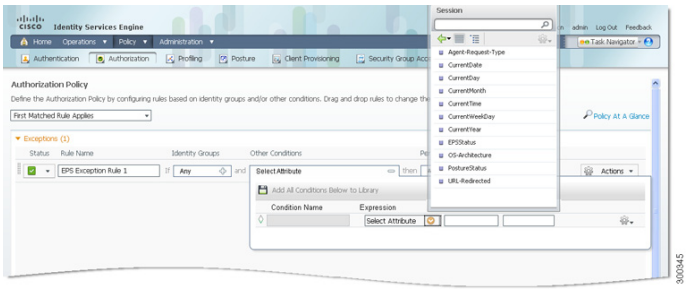
ステップ 3　必要に応じて、[ID グループ（Identity Group）] のプラス記号（[+]）をクリックして ID グループを選択するか、デフォルトの [任意（Any）] のままにします。

ステップ 4　[条件（Conditions）] のプラス記号（[+]）をクリックし、[新しい条件の作成（高度なオプション）（Create New Condition (Advanced Option)）] をクリックします。

ステップ 5　[式（Expression）] で [属性の選択（Select Attribute）] をクリックし、[ディクショナリ（Dictionaries）] リストから [セッション（Session）] を選択します。

ステップ 6　[セッション（Session）] リストから [EPSStatus] を選択して、右側にある 1 つ目のドロップダウン リストから [等しい（Equals）] を選択し、2 つ目のドロップダウン リストから [隔離（Quarantine）] を選択します。

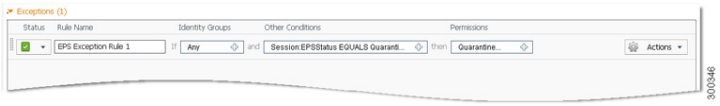
図 11-5　EPSStatus の設定



ステップ 7　下へスクロールして、[保存（Save）] をクリックします。

図 11-6 に示すように、EPS 例外ルールが [例外（Exception）] リストに表示されます。

図 11-6　EPS 例外ルール



エンドポイントの制御

選択したエンドポイントのネットワークへのアクセスを制限するために、EPS を使用してこれらを隔離できます。エンドポイントの妥当性が認められた場合には、エンドポイントの隔離を解除してネットワークへのフル アクセスを許可できます。ネットワーク上に悪意のあるエンドポイントを見つけた場合は、EPS を使用してそのエンドポイントのアクセスをシャットダウンし、ポートを閉じることができます。

（注）　シャットダウンはすべてのデバイスでサポートされているわけではありません。ただし、大部分のスイッチでシャットダウン コマンドがサポートされています。getResult() コマンドを使用すると、シャットダウンが正常に実行されたかどうかを確認できます。

エンドポイントの隔離および隔離解除

エンドポイント IP アドレスまたは MAC アドレスを使用して、エンドポイントを隔離および隔離解除できます。

前提条件

- 「EPS の有効化および無効化」（P.11-3）で説明されているように、EPS が有効になっている必要があります。
- 「EPS 許可」（P.11-4）の作成が完了している必要があります。

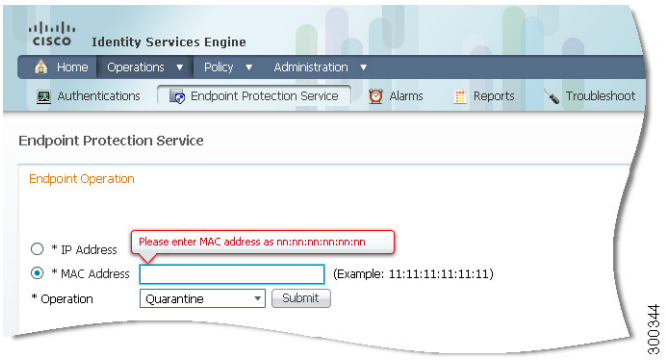
エンドポイントを隔離および隔離解除するには、次の手順を実行します。

ステップ 1　ISE 管理ダッシュボードで、[操作（Operations）] > [エンドポイント保護サービス（Endpoint Protection Service）] を選択します。

ステップ 2　[IP アドレス（IP Address）] または [MAC アドレス（MAC address）] オプション ボタンをクリックし、指定された形式に従って、テキスト フィールドにエンドポイントのアドレスを入力します。

（注）　アクティブ セッションにエンドポイントの IP アドレスに関する情報が含まれていない場合、Cisco ISE では、その IP アドレスを使用した EPS 操作に失敗します。このことは、そのエンドポイントの MAC アドレスおよびセッション ID にも適用されます。Cisco ISE によって、「EPS 操作が IP アドレス、MAC アドレス、またはセッション ID を使用して実行されたときに、この IP アドレス、MAC アドレス、またはセッション ID のアクティブ セッションが見つかりませんでした。（No active session found for this MAC address, IP Address, or Session ID when an EPS operation is performed with that IP address, MAC address, or session ID not found in the active session.）」というエラー メッセージが表示されます。

図 11-7　　エンドポイントの操作



ステップ 3　[操作（Operation）] ドロップダウン メニューから、次のいずれかを選択します。

- [隔離（Quarantine）] : エンドポイントを隔離して、ネットワークへのアクセスを制限します。
- [隔離解除（Unquarantine）] : 隔離プロセスを無効にし、ネットワークへのフル アクセスを許可します。

（注）　Cisco ISE では、同時に実行しない限り、同じエンドポイントに複数回、隔離操作および隔離解除操作を実行できます。

ステップ 4　[送信（Submit）] をクリックします。

ポートのシャットダウン

エンドポイントの IP アドレスまたは MAC アドレスを使用して、エンドポイントの接続先のスイッチ ポートをシャットダウンできます。

警告　**シャットダウン操作によって、スイッチ ポートが閉じます。これを行った場合、エンドポイントを再度ネットワークに接続するには、ポートを手動で再開する必要があります。**

シャットダウン操作は、有線メディアを介して接続されているエンドポイントにのみ有効です。

エンドポイントをシャットダウンするには、次の手順を実行します。

ステップ 1　ISE 管理ダッシュボードで、[操作（Operations）] > [エンドポイント保護サービス（Endpoint Protection Service）] を選択します。

ステップ 2　[IP アドレス（IP Address）] または [MAC アドレス（MAC address）] オプション ボタンをクリックし、指定された形式に従って、テキスト フィールドにエンドポイントのアドレスを入力します。

ステップ 3　[操作（Operation）] ドロップダウン メニューから、[シャットダウン（Shutdown）] を選択します。

ステップ 4　[送信（Submit）] をクリックします。

（注）　CLI で getResult() コマンドを使用して、ポートがシャットダウンされたかどうかを確認することもできます。詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x*』を参照してください。

EPS データのモニタリング

次の形式で EPS データを表示できます。

- エンドポイント保護サービス レポート
- セッション ディレクトリ レポート

ここでは、これらの各レポートの実行プロセスについて説明します。Cisco ISE レポートの詳細については、第 25 章「レポート」を参照してください。

エンドポイント保護サービス レポート

EPS レポート データを表示するには、次の手順を実行します。

ステップ 1　ISE 管理ダッシュボードで、[操作（Operations）] > [レポート（Reports）] > [カタログ（Catalog）] を選択します。

ステップ 2　[レポート（Reports）] リストで、[エンドポイント保護サービス（Endpoint Protection Services）] を選択します。

ステップ 3　右側の [レポート（Reports）] パネルで、[エンドポイント操作履歴（Endpoint Operations History）] チェックボックスをオンにします。

ステップ 4　[実行（Run）] ドロップダウン メニューで、レポート データを収集する期間を選択します。

- 直近の 30 分（Last 30 minutes）
- 直近の 1 時間（Last hour）
- 直近の 12 時間（Last 12 hours）
- 今日（Today）
- 昨日（Yesterday）
- 直近 7 日間（Last 7 days）
- 直近 30 日間（Last 30 days）
- クエリーおよび実行（Query and Run）

期間を選択した時点でレポートが実行され、エンドポイント操作履歴データが表示されます。

セッション ディレクトリ レポート

アクティブ エンドポイントに対する隔離および隔離解除操作は、セッション ディレクトリ レポートからもトリガーできます。

RADIUS セッション ディレクトリ レポートは、EPS データの追跡にも使用できます。一度に隔離できるユーザの数に制限はなく、また隔離期間の長さにも制限はありません。

（注）　隔離されていたセッションが隔離解除された場合、新たに隔離解除されたセッションの開始方法は、スイッチ設定で指定されている認証方法によって決まります。

セッション ディレクトリ レポートを使用して EPS データを追跡するには、次の手順を実行します。

ステップ 1　ISE 管理ダッシュボードで、[操作（Operations）] > [レポート（Reports）] > [カタログ（Catalog）] を選択します。

ステップ 2　[レポート（Reports）] リストで、[セッション ディレクトリ（Session Directory）] を選択します。

ステップ 3　右側の [レポート（Reports）] パネルで、次のいずれかのオプション ボタンをクリックします。

- [RADIUS アクティブ セッション（RADIUS Active Sessions）] : RADIUS で認証、許可、および開始されたセッションの情報が提供されます。
- [RADIUS セッション履歴（RADIUS Session History）] : 選択された期間における、認証されたセッションおよび終了されたセッションの合計数や、セッションの継続時間とスループットの合計および平均などの、RADIUS セッション履歴の概要が提供されます。
- [RADIUS 中断セッション（RADIUS Terminated Sessions）] : 選択された期間における、すべての終了された RADIUS セッションの情報が提供されます。

ステップ 4　[実行（Run）] ドロップダウン メニューで、レポート データを収集する期間を選択します。

- 直近の 30 分（Last 30 minutes）
- 直近の 1 時間（Last hour）
- 直近の 12 時間（Last 12 hours）
- 今日（Today）
- 昨日（Yesterday）
- 直近 7 日間（Last 7 days）
- 直近 30 日間（Last 30 days）
- クエリーおよび実行（Query and Run）

期間を選択した時点でレポートが実行され、レポート データが表示されます。