エンドポイント保護サービスの設定

エンドポイント保護サービス（EPS）は、エンドポイントのネットワーク アクセスのモニタリングと制御に使用できる管理ノード上で実行されるサービスです。EPS は、有線とワイヤレス展開をサポートし、拡張ライセンスが必要です。

この章では、EPS を設定する方法について説明します。

エンドポイント保護サービスの設定

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。EPS は、手動で有効にする必要があり、管理者ポータルでサービスを手動で無効にするまで有効のままです。

Cisco ISE で EPS 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。

ステップ 1 [管理（Administration）] > [システム（System）] > [設定（Settings）] > [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 [サービス ステータス（Service Status）] ドロップダウン リストをクリックし、[有効（Enabled）] を選択します。

ステップ 3 [保存（Save）] をクリックします。

関連項目

- 「EPS によるネットワーク アクセス用の許可プロファイルの作成」（P.13-2）
- 「EPS によるネットワーク アクセス用の例外ポリシーの作成」（P.13-2）

EPS によるネットワーク アクセス用の許可プロファイルの作成

EPS で使用するために許可プロファイルを作成する必要があり、許可プロファイルは標準許可プロファイルのリストに表示されます。エンドポイントは、ネットワークで認証および許可できますが、ネットワークのアクセスが制限されています。

ステップ 1　[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）] を選択します。

ステップ 2　[追加（Add）] をクリックします。

ステップ 3　認可プロファイルの一意の名前と説明を入力し、アクセス タイプは **ACCESS_ACCEPT** のままにしておきます。

ステップ 4　[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_TRAFFIC] を選択します。

ステップ 5　[送信（Submit）] をクリックします。

関連項目

- 「EPS によるネットワーク アクセス用の例外ポリシーの作成」（P.13-2）
- 「ネットワーク アクセスの設定」（P.13-3）

EPS によるネットワーク アクセス用の例外ポリシーの作成

EPS 許可では、すべての標準許可ポリシー以前に処理される隔離例外ポリシーを作成する必要があります。例外許可ポリシーは、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。標準認可ポリシーは、安定し、ユーザの大規模なグループ、デバイス、および特権の共通セットを共有するグループに適用されることを目的としています。

はじめる前に

EPS で使用する標準許可プロファイルを作成している必要があります。

ステップ 1　[ポリシー（Policy）] > [許可（Authorization）] を選択し、[例外（Exceptions）] を展開します。

ステップ 2　[有効（Enabled）] または [無効（Disabled）]、あるいは [モニタのみ（Monitor Only）] オプションを選択します。

ステップ 3　ルールを [新規ルールを作成（Create a New）] をクリックします。

ステップ 4　例外ルール名を入力します。

ステップ 5　してプラス [+] 記号をクリックして、ID グループを選択します。

ステップ 6　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)）] を選択します。

ステップ 7　最初のフィールドの下矢印のアイコンをクリックしてディクショナリを表示し、[セッション（Session）] > [EPSStatus] を選択します。

ステップ 8　2 番めのフィールドのドロップダウン リストから [等しい（Equals）] を選択します。

ステップ 9　3 番めのフィールドのドロップダウン リストから [隔離（Quarantine）] を選択します。

ステップ 10　[保存（Save）] をクリックします。

関連項目

「ネットワーク アクセスの設定」（P.13-3）

ネットワーク アクセスの設定

エンドポイント保護サービス（EPS）を使用すると、エンドポイントのネットワーク アクセス ステータスをリセットし、ネットワーク アクセス ステータスによってネットワークへの許可を定義するポートを隔離、隔離解除、またはシャットダウンできます。

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、エンドポイントが接続されているネットワーク アクセス サーバ（NAS）のポートを隔離、隔離解除、またはシャットダウンできます。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。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、NAS ポートを閉じることができます。

はじめる前に

- EPS を有効にする必要があります。
- EPS の許可プロファイルおよび例外タイプの許可ポリシーを作成する必要があります。

ステップ 1　[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　エンドポイントの IP アドレスまたは MAC アドレスを入力します。

ステップ 3　[操作（Operations）] ドロップダウン リストをクリックして、次のいずれかのアクションを選択します。

- [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。
- [シャットダウン（Shutdown）] : エンドポイントが接続されている NAS ポートを閉じます。

ステップ 4　[送信（Submit）] をクリックします。

関連項目

- 「IP アドレスまたは MAC アドレスが見つからない場合 EPS 操作は失敗する」（P.13-4）
- 「外部認証された管理者は EPS 操作を実行できない」（P.13-4）
- 「EPS 隔離と隔離解除フロー」（P.13-5）
- 「EPS NAS ポートのシャットダウン フロー」（P.13-6）

IP アドレスまたは MAC アドレスが見つからない場合 EPS 操作は失敗する

エンドポイントのアクティブなセッションに IP アドレスに関する情報が含まれていない場合は、そのエンドポイントに対して実行する EPS 操作は失敗します。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。

- EPS によってエンドポイントの許可状態を変更する場合は、エンドポイントの IP アドレスまたは MAC アドレスを指定する必要があります。IP アドレスまたは MAC アドレスがエンドポイントのアクティブなセッションに見つからない場合、次のエラー メッセージが表示されます。この MAC アドレス、IP アドレスまたはセッション ID のアクティブなセッションは見つかりませんでした（No active session found for this MAC address, IP Address or Session ID）。

外部認証された管理者は EPS 操作を実行できない

外部認証された管理者がライブ セッションから CoA 隔離を発行すると、Cisco ISE は次のエラー メッセージを返します。

xx:xx:xx:xx:xx:xx に対する隔離の CoA アクションは開始できません（CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated）。（原因：内部にユーザが見つかりません。（(Cause:User not found internally.）サポートされていない外部認証されたユーザが使用している可能性があります（Possible use of unsupported externally authenticated user）

外部認証された管理者が Cisco ISE の管理者ポータルで [操作（Operations）] > [エンドポイント保護サービス（Endpoint Protection Service）] を選択し、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 EPS 処理を実行すると、Cisco ISE は次のエラー メッセージを返します。

サーバの障害 : 内部にユーザが見つかりません。（Server failure: User not found internally.）サポートされていない外部認証されたユーザが使用している可能性があります（Possible use of unsupported externally authenticated user）

エンドポイント保護サービス

エンドポイント保護サービス（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、許可状態を変更できます。EPS を使用すると、EPSStatus を確認してネットワーク アクセスを制限または拒否するように許可ポリシーが定義されている場合、確立された認可ポリシーの結果としてエンドポイントを隔離するときの許可状態を設定することができます。エンドポイントを隔離解除して、フル ネットワーク アクセスができるようにします。ネットワークからエンドポイントを接続解除する Network Attached System（NAS）上のポートをシャット ダウンすることもできます。

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。

EPS によってネットワーク アクセスをモニタおよび制御するには、次の操作を実行できます。

- 隔離：例外ポリシー（認可ポリシー）を使用して、ネットワークへのエンドポイント アクセスを制限または拒否することができます。EPS ステータスに応じて別々の許可プロファイル（権限）を割り当てるために、例外ポリシーを作成する必要があります。隔離状態に設定すると、基本的に、デフォルトの VLAN から指定した隔離 VLAN にエンドポイントが移動します。エンドポイントと同じ NAS でサポートされている隔離 VLAN をあらかじめ定義する必要があります。
- 隔離解除：エンドポイントのネットワークへのフル アクセスを許可し、エンドポイントを元の VLAN に戻す隔離ステータスを反転することができます。

- シャットダウン：NAS 上のポートを非アクティブ化し、エンドポイントをネットワークから接続解除することができます。一度エンドポイントが接続されている NAS 上のポートがシャットダウンされたら、エンドポイントがネットワークに接続できるようにするには、手動で NAS 上のポートを再度リセットする必要があります。ワイヤレス展開ではこれは使用できません。

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 レポートからトリガーできます。

（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。

関連項目

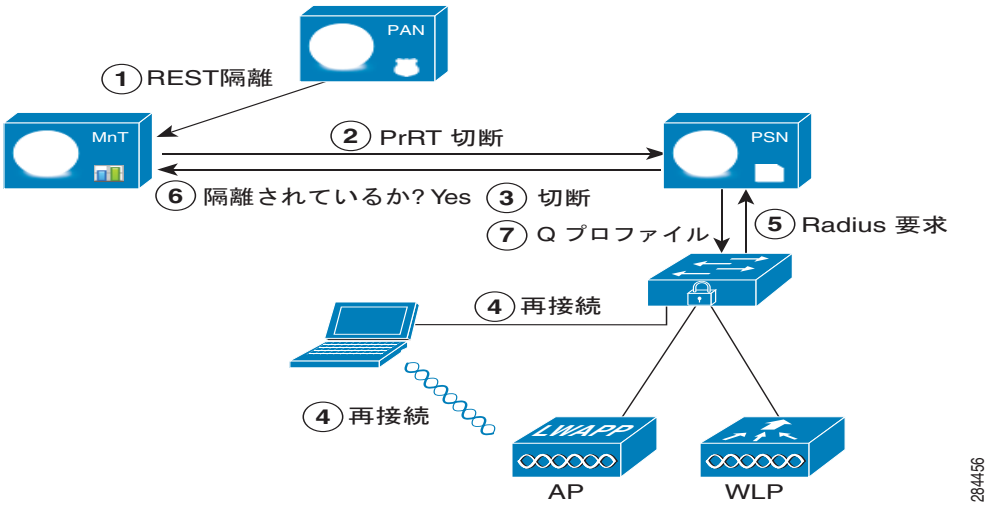
- 「ネットワーク アクセスの設定」（P.13-3）

EPS 隔離と隔離解除フロー

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。エンドポイントを隔離し、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例外許可ポリシーを作成できます。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許可ポリシーで定義す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。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。

図 13-1 は隔離フローを示していますが、許可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 13-1　EPS 隔離フロー



1. クライアント デバイスがワイヤレス 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 呼び出しが管理ノード（PAP）からモニタリング ノード（MnT）に発行されます。
2. 続いて、モニタリング ノードは、ポリシー サービス ISE ノード（PDP）を通じて PrRT をコールし、CoA を呼び出します。
3. クライアント デバイスが切断されます。
4. クライアント デバイスは再認証を行い、再接続されます。

5. クライアント デバイスに対する RADIUS 要求が、モニタリング ノードに返送されます。
6. チェックが行われている間、クライアント デバイスは隔離されます。
7. Q プロファイル許可ポリシーが適用され、クライアント デバイスの妥当性が確認されます。
8. クライアント デバイスの隔離が解除され、ネットワークにフル アクセスできるようになります。

EPS NAS ポートのシャットダウン フロー

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 NAS ポートをシャットダウンできます。

シャットダウンにより MAC アドレスに指定された IP アドレスに基づいて NAS ポートを閉じることができますが、エンドポイントをネットワークに戻すには手動でポートを再開する必要があります。この操作は、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

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。

図 13-2 に EPS シャットダウン フローを示します。

図のクライアント デバイスの場合、シャットダウン操作はクライアント デバイスがネットワークへのアクセスに使用する NAS で実行されます。

図 13-2　EPS シャットダウン フロー