Cisco AI エンドポイント分析

- Cisco AI エンドポイント分析の概要 （1 ページ）
- Cisco AI エンドポイント分析の主な機能 （2 ページ）
- FIPS Compliance （3 ページ）
- Cisco DNA Center での Cisco AI エンドポイント分析のセットアップ （4 ページ）
- [Cisco AI Endpoint Analytics Overview] ウィンドウ （9 ページ）
- [Cisco AI Endpoint Analytics Overview] ウィンドウ （13 ページ）
- Endpoint Inventory （21 ページ）
- 信頼得点 （27 ページ）
- プロファイリングルール （46 ページ）
- スマートグループ化のための Cisco AI ルール （52 ページ）
- 階層 （61 ページ）

Cisco AI エンドポイント分析の概要

可視性は、エンドポイントを保護するための最初のステップです。Cisco AI エンドポイント分析は、エンドポイントと Internet of Things（IoT）デバイスの識別とプロファイリングに役立つエンドポイント可視性ソリューションです。Cisco AI エンドポイント分析エンジンを使用すると、さまざまなソースからネットワーク経由で受信したテレメトリ情報を使用して、エンドポイントにラベルを割り当てることができます。

Cisco AI エンドポイント分析で使用できるプロファイリングラベルは、エンドポイントタイプ、ハードウェアモデル、製造元、およびオペレーティング システム タイプです。これは多要素分類と呼ばれます。

Cisco AI エンドポイント分析は、潜在的に危険なエンドポイントやデバイスを特定して対処することを可能にする信頼スコアなどの機能により、ネットワークにおける繊細な可視化と処置を実現します。Cisco AI エンドポイント分析の GUI から Cisco ISE を介して ANC ポリシーを適用することにより、潜在的なリスクを管理することもできます。Cisco AI エンドポイント分析でエンドポイントのランダムおよび変更 MAC アドレスの問題をモニターして回避し、MAC アドレスの代わりに「DUID」と呼ばれる一意の属性を使用してエンドポイントを正確に識別することができます。

Cisco AI エンドポイント分析は、さまざまなソースからエンドポイントテレメトリを収集するのに役立ちます。主要なソースは、Network-Based Application Recognition（NBAR）メカニズムです。NBAR メカニズムは、Cisco Catalyst 9000 シリーズ スイッチ（アクセスデバイス）に組み込まれていて、ディープ パケット インスペクション（DPI）を実行します。Cisco AI エンドポイント分析は、Cisco DNA トラフィック テレメトリ アプライアンスからテレメトリを受信することもできます。

Cisco ISE、自己登録型ポータル、ServiceNow のような構成管理データベース（CMDB）ソフトウェアなど、さまざまなソースからエンドポイントコンテキスト情報を収集できます。

Cisco AI エンドポイント分析を使用すると、さまざまなネットワークデバイスからのデータインフローが可能になり、エンドポイントをより高い精度で容易に識別してプロファイリングし、異常に対処する機能が拡張されます。Cisco AI エンドポイント分析では、さまざまなエンドポイント情報を集約し、そのデータを使用してエンドポイントをプロファイリングできます。エンドポイントのプロファイリング後、AI と機械学習アルゴリズムを使用して、さまざまな方法を直感的に活用することで不明なエンドポイントの数を減らすこともできます。

Cisco AI エンドポイント分析の主な機能

- **Cisco AI エンドポイント分析ダッシュボード**

  Cisco AI エンドポイント分析ダッシュボードでは、ネットワークに接続されているエンドポイントの全体像を確認できます。既知のエンドポイント、不明なエンドポイント、プロファイリングされたエンドポイント、プロファイリングされていないエンドポイント、信頼スコアが低いエンドポイント、およびランダム MAC アドレスを使用するエンドポイントの数を表示できます。[AI Proposals] ダッシュレットには、エンドポイントのプロファイリングと管理を強化するためのインテリジェントなプロファイリングの提案が表示されます。

- **潜在的に危険なエンドポイントにフラグを付ける信頼スコア**

  Cisco AI エンドポイント分析は、エンドポイントに信頼スコアを割り当てます。これにより、ネットワーク内の潜在的に危険なエンドポイントを簡単にモニタして対処することができます。異常な動作がモニタおよび追跡され、追跡された異常の数と頻度に基づいて信頼スコアが割り当てられます。エンドポイントの信頼スコア （28 ページ）を参照してください。

- **ランダム MAC アドレスを使用するエンドポイントの検出**

  Cisco AI エンドポイント分析を使用すると、Cisco ISE から「DUID」と呼ばれる（Cisco ISE では「GUID」とも呼ばれます）一意のエンドポイント識別子を受信することにより、ランダムおよび変更 MAC アドレスの問題を処理できます。Cisco AI エンドポイント分析は、MAC アドレスの代わりに、エンドポイントの識別子として DUID を使用します。

- **機械学習機能を使用したネット内の不明なエンドポイントの削減**

  Cisco AI エンドポイント分析では、エンドポイントのグループ化で学習した情報に基づいてプロファイリング提案が提供されます。このような提案を使用して、ネットワーク内の

不明なエンドポイントやプロファイリングされていないエンドポイントの数を減らすことができます。

- **システムルールおよびカスタム プロファイリング ルールによるエンドポイントの管理**

  ネットワークに接続されたエンドポイントを確実にプロファイリングおよび管理するには、シスコが提供するシステムルールと自分で設計したカスタムルールを使用します。

- **Cisco AI エンドポイント分析によるエンドポイントの登録**

  Cisco AI エンドポイント分析を使用して、エンドポイントをオンボードおよびプロファイリングできます。この登録プロセスでエンドポイント属性データが収集されて、エンドポイントのプロファイリングに使用されます。

- **外部ソースを使用したエンドポイントの登録**

  構成管理データベース（CMDB）などエンドポイントデータの外部ソースの中には、Cisco AI エンドポイント分析に接続できるものがあります。これにより、ネットワーク内のエンドポイントを簡単に登録、管理、およびプロファイリングできます。

- **定義された非アクティブ期間後のエンドポイントのパージ**

  定義された時間にわたって非アクティブだったエンドポイントをネットワークから削除するには、エンドポイント パージ ポリシーを定義します。エンドポイントを削除する必要があるまでの非アクティブ期間を定義できます。また、プロファイリング属性に基づいて特定のエンドポイントのセットに作用するようにパージポリシーをカスタマイズすることもできます。

FIPS Compliance

Cisco DNA Center は米国の連邦情報処理標準（FIPS）をサポートしています。FIPS は、Cisco DNA Center イメージのインストール時に有効にできるオプションのモードです。デフォルトでは、FIPS モードはディセーブルです。

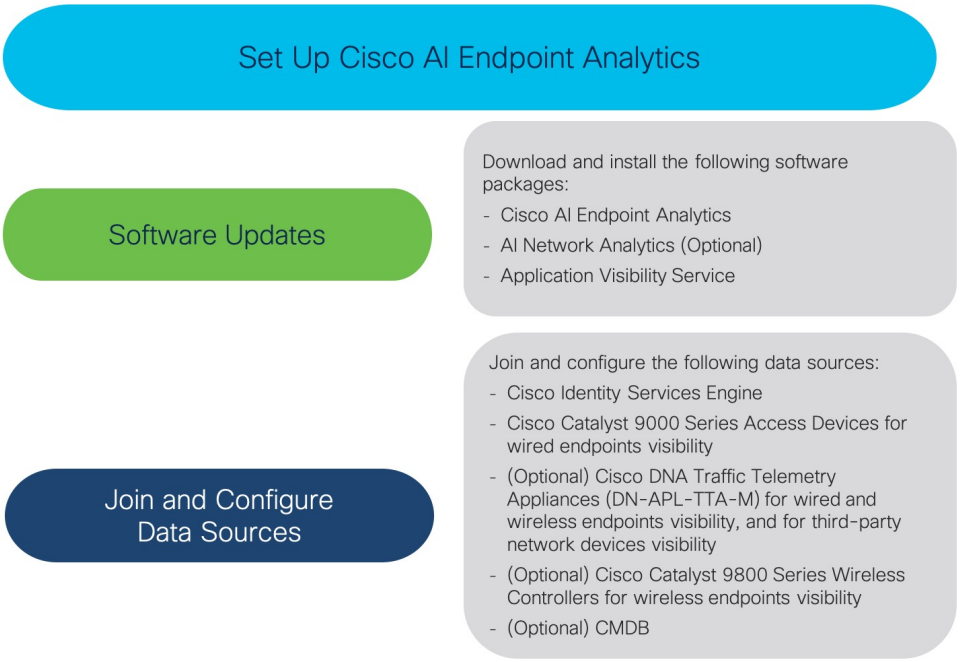
Cisco DNA Center で FIPS モードが有効になっている場合、Cisco DNA Center GUI の次の機能は使用できません。

- [AI Endpoint Analytics Setup] の [Optional Configurations] セクションにある [Enable AI Network Analytics] ダッシュレット。
- **[Policy]** > **[AI Endpoint Analytics]** > **[Overview]**の [AI Proposals] ダッシュレット。
- **[Policy]** > **[AI Endpoint Analytics]** > **[Overview]** > **[Configuration]** の [Profile Rule Settings] タブ。
- **[Policy]** > **[AI Endpoint Analytics]** > **[Overview]** > **[Configuration]** > **[Trust Analytics]** の [AI Spoofing Detection] セクション。
- [Policy] > [AI Endpoint Analytics] > [Endpoint Inventory] の特定のエンドポイントの [Trust Score] の詳細の下にある [Endpoint Anomaly Detection] の [AI Spoofing Detection] セクション。

- **[Policy]** > **[AI Endpoint Analytics]** > **[Endpoint Inventory]** > **[Focus as Trust Score]** の [AI Spoofing Detection] 列。

（注） FIPS が有効になっている場合、Talos IP レピュテーションはサポートされません。

Cisco DNA Center での Cisco AI エンドポイント分析のセットアップ



ソフトウェア アップデートのインストール

次の手順で説明するように、Cisco AI エンドポイント分析を使用するためのソフトウェアアップデートを Cisco DNA Center にインストールします。

ステップ 1 Cisco DNA Center にログインします。

ステップ 2 メニューアイコン（☰）をクリックして、**[System]** > **[Software Management]** の順に選択します。

ステップ 3 [Updates] タブで、[Cisco AI Endpoint Analytics]、[AI Network Analytics]、および [Application Visibility Service] が [Application Updates] セクションにリストされているかどうかを確認してください。これらのアプリケーション更新が表示されている場合は、[Install All] をクリックします。

- Cisco DNA Center でエンドポイント プロファイリング ソリューションにアクセスするには、[Cisco AI Endpoint Analytics] 更新をインストールします。
- 機械学習と AI の機能を使用してインテリジェントなプロファイリング提案を受け取るには、[AI Network Analytics] 更新をインストールします。
- NBAR およびコントローラベースのアプリケーション認識（CBAR）の技術を使用してエンドポイント プロファイリングを通知するには、[Application Visibility Service] 更新をインストールします。

ステップ 4 これらの更新が [Updates] タブにリストされていない場合は、[Installed Apps] タブをクリックして、更新がすでにインストールされ、使用可能であるかどうかを確認してください。[Currently Installed Applications] タブでは、ソフトウェアインストールが正常に完了しているかどうかも確認できます。

データソースの接続と有効化

Cisco AI エンドポイント分析が使用するデータソースは、すでに Cisco DNA Center に接続されている可能性があります。データソースが接続されている場合は、次の手順を参照して、Cisco AI エンドポイント分析でデータソースを使用できることを確認します。

Cisco AI エンドポイント分析が結果を提供できるようにするには、Cisco ISE または Catalyst 9000 シリーズ アクセスデバイスを Cisco DNA Center に追加する必要があります。

ステップ 1 Cisco ISE を Cisco DNA Center に接続します。

『Cisco DNA Center Appliance Installation Guide』の「Complete First-Time Setup」にある「Integrate Cisco ISE with Cisco DNA Center」セクションを参照してください。

次の Cisco ISE リリースが Cisco AI エンドポイント分析をサポートします。

- 2.4 パッチ 11 以降
- 2.6 パッチ 5 以降
- 2.7 パッチ 1 以降
- 3.0 以降

Cisco ISE リリース 3.1 以降の場合、Cisco ISE 管理ポータルで次の手順を実行します。

a) **[Work Centers]** > **[Profiler]** > **[Settings]** の順に選択します。
b) [Endpoint Analytics Settings] エリアで、次のチェックボックスをオンにします。
   - [Publish Endpoint Attributes to AI Endpoint Analytics]
   - [Consume Endpoint Profiles from AI Endpoint Analytics]

   Cisco ISE が 802.1X または MAB 認証方式でエンドポイントを認証すると、収集されたエンドポイント属性が Cisco AI エンドポイント分析で使用可能になります。Cisco ISE はまた Cisco AI エンドポイント分析とテレメトリデータを共有します。

Cisco ISE リリース 2.4、2.6、および 3.0 の場合、Cisco ISE 管理ポータルで次の手順を実行します。

a) **[Work Centers]** > **[Profiler]** > **[Settings]** の順に選択します。
b) [Enable Probe Data Publisher] オプションを選択します。
c) [Save] をクリックします。

ステップ 2 有線エンドポイントが表示されるように、Cisco 9000 シリーズ アクセスデバイスを Cisco DNA Center に接続します。

『*Cisco DNA Center User Guide*』の「Discover Your Network」を参照してください。

Cisco AI エンドポイント分析機能を有効にするには、Cisco 9000 シリーズアクセスデバイスを Cisco IOS-XE リリース 17.6 以降にアップグレードします。

必要なアクセスデバイスの CBAR を有効にするには、

a) Cisco DNA Center GUI でメニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。
b) データが必要な Cisco Catalyst 9000 アクセスデバイスを選択します。[Site Devices] セクションのデバイス名の横にあるチェックボックスをオンにします。
c) [Enable CBAR] をクリックします。
d) 表示される確認ウィンドウで、[Yes] をクリックします。
e) [Enable CBAR] slide-in paneで、サポートされている SSID タイプの横にあるチェックボックスをオンにします。
f) [Enable] をクリックします。

ステップ 3 （任意）ワイヤレスエンドポイントを可視化するには、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラを Cisco DNA Center に接続します。

次の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ モデルは Cisco AI エンドポイント分析によりサポートされます。

- 9800-CL
- 9800-40
- 9800-80
- 9800-L

Cisco DNA Center リリース 2.3.2 以降は、Cisco IOS XE リリース 17.7.1 以降を搭載した Cisco Catalyst 9800 シリーズ ワイヤレスコントローラで FlexConnect をサポートします。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要 で Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定およびプロビジョニングするには、Cisco DNA Centerを参照してください。

ステップ 4 （オプション）Cisco Catalyst IE9300 高耐久性シリーズ スイッチを Cisco DNA Center に接続します。

Cisco Catalyst IE9300 高耐久性シリーズ スイッチは Cisco AI エンドポイント分析でサポートされます。

『Cisco DNA Center User Guide』の「Discover Your Network」を参照してください。

ステップ 5 （任意）有線およびワイヤレスエンドポイントを可視化し、サードパーティのネットワークデバイスを可視化するには、Cisco DNA トラフィック テレメトリ アプライアンスを Cisco DNA Center に接続します。

Cisco DNA トラフィック テレメトリ アプライアンス（DN-APL-TTA-M）は、ミラーリングされたネットワークトラフィックからテレメトリを生成してエンドポイントを分析できるようにします。このアプライアンスでは、Network-Based Application Recognition ベース（NBAR ベース）のプロトコル検査、およびエンドポイント属性の抽出が可能です。

テレメトリアプライアンスで収集されたエンドポイント属性を Cisco AI エンドポイント分析で受信するには、Cisco ISE と Cisco DNA Center を統合する必要があります。

Cisco DNA Center でのアプライアンスのインストール、接続の構成、およびアプライアンスの管理については、『Cisco DNA Traffic Telemetry Appliances』を参照してください。

Cisco DNA トラフィック テレメトリ アプライアンスに接続されたアクセススイッチのスイッチドポートアナライザ（SPAN）受信ポートで CBAR を有効にするには、次のコマンドを使用します。

```
ip nbar protocol-discovery
```

テレメトリアプライアンスに接続されているすべてのエンドポイントが Cisco AI エンドポイント分析に表示されるわけではありません。Cisco DNA アシュアランス で管理されるネットワーク アクセス デバイス（NAD）にも接続されているエンドポイントのみが、Cisco AI エンドポイント分析 に表示されます。

ステップ 6 （任意）Cisco DNA Center で ServiceNow を有効にします。

a) ServiceNow を Cisco DNA Center に接続した後に、メニューアイコン（☰）をクリックして、**[Platform]** > **[Manage]** > **[Bundles]** の順に選択します。

b) バンドル [Endpoint Attribute Retrieval with ITSM (ServiceNow)] の [Status] が [New] の場合は、バンドルの [Enable] をクリックします。

ステップ 7 （任意）Cisco DNA Center で Cisco AI 分析を有効にします。

AI ベースのエンドポイントグループ化、カスタム プロファイリング ルール自動化、およびエンドポイントラベルに関する提案を受け取るには、また、ネットワーク内のスプーフィングされている可能性のあるデバイスを検出するには、[Cisco AI Analytics] ウィンドウで、必要な設定を有効にする必要があります。

これらの AI ベースの提案を受け取るには、AI ネットワーク分析ソフトウェアをインストールする必要があります。

a) メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Cisco AI Analytics]** の順に選択します。

b) 有効にする次の各サービスのトグルボタンをクリックします。

- **AI エンドポイント分析**：AI ネットワーク分析は、機械学習を利用してネットワークのインテリジェンスを推進し、ネットワークパフォーマンスを効果的に改善して問題解決を加速できるようにします。AI ネットワーク分析は、ネットワークの動作を分析し、ネットワーク環境に適応することで、ノイズや誤検出を大幅に削減します。

- **エンドポイントスマートグループ化**：エンドポイントスマートグループ化は、AI と機械学習を使用して、AI ベースのエンドポイントグループ化、自動化されたカスタム プロファイリング ルール、クラウドソーシングされたエンドポイントラベルを提供することにより、ネットワーク内の不明なエンドポイントの数を減らします。

- **AI スプーフィング検出**：AI スプーフィング検出は、事前トレーニング動作モデルに基づいてスプーフィングされているエンドポイントを識別します。 [Enable AI Spoofing Detection] トグルボタ

ンを有効にすると、Cisco DNA Centerはこれらの動作モデルとネットワークデバイスによって提供されるフロー情報を使用して、スプーフィングされたエンドポイントを検出できます。参加しているお客様から収集されたフロー情報を使用して、いくつかの行動モデルが構築され、集中的にトレーニングされます。

- クラウドでスプーフィングの検出が実行されたら、Cisco DNA Centerからクラウドに匿名化されたデータをエクスポートする必要があります。その後、Cisco DNA Centerはスプーフィング検出のためにクラウドをポーリングします。
- この機能を使用するには、中断のないインターネット接続が必要です。
- 最新リリースへのアップグレード中に、以前のバージョンでデータエクスポートが無効になっていた場合、アップグレードのときにデータエクスポートが無効になっていることを示す警告がユーザーに表示されます。スプーフィング検出は、ユーザーが再度有効にする必要があります。

エンドポイント テレメトリ ソース

Cisco AI エンドポイント分析は、次の方法でテレメトリデータを受信します。

- **ディープ パケット インスペクション**

  ディープ パケット インスペクションは、Cisco Catalyst 9000 シリーズ アクセス デバイスによって実行される高度なパケット分析方法です。これらのアクセスデバイスは、NBARを実行します。NBAR は、アプリケーション トラフィックを検査し、プロトコル分析を実行して、精度の高いエンドポイントを検出および識別し、プロファイリングします。

  ディープ パケット インスペクションのプロファイリングは、ネットワークへのエンドポイントトラフィックから収集されたさまざまな属性に基づいています。これらの属性は、パケットヘッダーレイヤ 4 ～ 7 から複数のプロトコルにわたって収集されます。

- **構成管理データベース接続**

  Cisco AI エンドポイント分析は、エンドポイント プロファイリングの精度を高めるために、構成管理データベース（CMDB）接続からエンドポイントデータを受信します。ServiceNow との接続により、CMDB から Cisco AI エンドポイント分析への情報を受信できます。

- **機械学習機能**

  プロファイリング用に収集されたデータは、匿名化されて、Cisco Cloudでデバイスデータレイクとして機能する場所に送信されます。ここでは、機械学習アルゴリズムで使用可能なデータを分析し、必要に応じて評価して適用できるプロファイリングルールを作成します。エンドポイント プロファイリングと管理を簡素化かつ効率化できるように、Cisco AI エンドポイント分析によってスマート プロファイリング ルールが提案されます。既存のルールも評価され、この継続学習に基づいて改善提案が提供されます。

[Cisco AI Endpoint Analytics Overview] ウィンドウ

メニューアイコン（☰）をクリックして、**[Policy]** > **[AI Endpoint Analytics]**の順に選択します。

[Overview] ウィンドウに次のダッシュレットが表示されます。

- **合計エンドポイント数**

  このダッシュレットでは、ネットワーク内のエンドポイントの合計数が [Fully Profiled] と [Partially Profiled] の 2 つのグループに分かれて表示されます。Cisco AI エンドポイント分析は、エンドポイントタイプ、OS タイプ、ハードウェアモデル、およびハードウェア製造元の 4 つの要因に基づいてエンドポイントをプロファイリングします。エンドポイントにこれらの要因の 1 つ以上が欠落している場合は、[Partially Profiled] グループにプロファイリングされます。

  [Partially Profiled Labels] をクリックすると、ネットワーク内のプロファイルが欠落しているエンドポイントの数が、プロファイルラベルタイプで分類されて表示されます。特定のプロファイルラベルが欠落しているエンドポイントを確認するには、プロファイルラベルの横にある数字をクリックします。[Endpoint Inventory] タブが、対応するエンドポイントのリストとともに表示されます。

- **AI 提案**

  Cisco AI エンドポイント分析は、スマートグループ化アルゴリズムを使用して、ネットワーク内で類似するプロファイリングデータを持つ不明なエンドポイントをグループ化します。AI エンドポイント分析を有効にした場合、次のタイプのルール提案が表示されます。これらのルール提案は、次のようにエンドポイントクラスタから学習した内容に基づいています。

  - 類似している可能性があるエンドポイントをプロファイリングするための新しいルール。
  - 以前に受け入れられていたルールの変更提案。
  - 不要になったプロファイリングルールの確認。

  詳細については、スマートグループ化のための Cisco AI ルール （52 ページ）を参照してください。

- **信頼スコア**

  [Trust Scores] ダッシュレットには、ネットワーク内のエンドポイントに割り当てられている信頼スコアの全体像が示されます。エンドポイントの信頼スコア （28 ページ）を参照してください。

- **設定**

  [Overview] エリアの右上隅にある [Configuration] リンクをクリックすると、次の設定にアクセスできます。

- [Profile Rule Settings]：システムプロファイルルールの自動更新をスケジュールします。エンドポイント プロファイリング用の自動システムルール更新 （48 ページ）を参照してください。
- [ISE Integration]：Cisco ISE への許可属性の公開 （15 ページ）を参照してください。
- [**Trust Analytics**]：信頼スコアのソースを有効または無効にするには、このトグルボタンをクリックします。[Authentication Method] ソースを無効にすることはできません。アクティブな Cisco ISE 統合が設定されている場合、エンドポイントが使用する認証方式およびそのポスチャステータスによって、エンドポイントの信頼スコアが通知されます。[AI Spoofing Detection]、[Changed Profile Labels]、[Endpoint Attribute Conflict]、[NAT Mode Detection]、[Concurrent MAC Addresses]、[Security Sensor] などの信頼スコアデータのその他のソースは、有効または無効にすることができます。

  「エンドポイントの信頼スコア （28 ページ）」を参照してください。
- [Endpoint Purge Policy]：エンドポイント パージ ポリシー （19 ページ）を参照してください。
- [Endpoint Subnet Inspection]：エンドポイントサブネット検査の設定 （20 ページ）を参照してください。

- **エンドポイント MAC ランダム化**

  [Endpoint MAC Randomization] には、ネットワーク内の静的 MAC アドレスとランダムおよび変更 MAC アドレスの数が表示されます。ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコア （35 ページ）を参照してください。

Cisco AI エンドポイント分析とTalos インテリジェンスの統合

Talos インテリジェンス [英語] は、包括的な脅威検出ネットワークです。Talos インテリジェンスは、脅威検出アナリストと、Web リクエスト、電子メール、マルウェアサンプル、オープンソースデータセット、エンドポイントインテリジェンス、ネットワーク侵入に及ぶリアルタイムの自動検出システムで構成されています。Cisco AI エンドポイント分析 を Talos と統合して、信頼できない IP アドレスに到達するネットワーク接続にフラグを立て、それらを隔離し、最も一般的なサイバー脅威からネットワークを保護します。

Cisco DNA Cloud は Talos インテリジェンス クラウド サービスと通信して、更新された IP のレピュテーションデータを 30 分ごとに取得します。IP のレピュテーションデータのこの更新は、すべての登録済みの Cisco DNA Center デバイスにプッシュされます。

Cisco DNA Center デバイスで Talos Intelligence をセットアップするには、次の手順を実行します。

始める前に

Cisco AI エンドポイント分析 を Talos インテリジェンスと統合するための前提条件は次のとおりです。

- Cisco DNA Center は Cisco DNA Cloud に登録する必要があります。

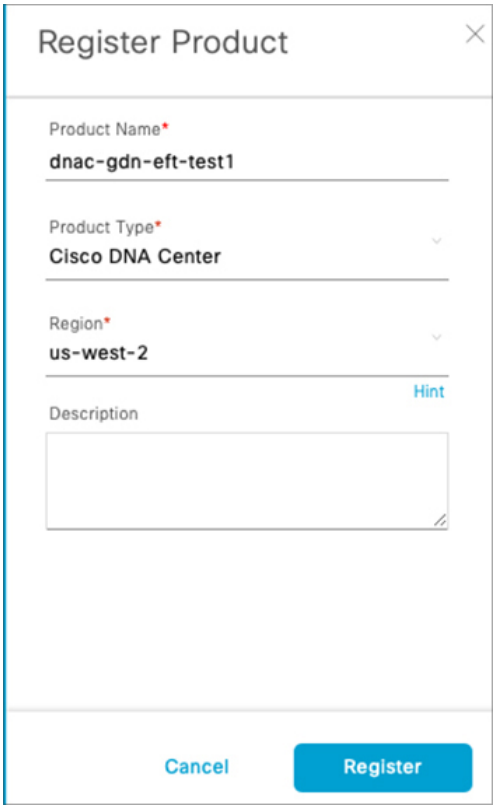
（注） ユーザーが Cisco DNA Cloud に登録されていない場合、Cisco DNA Center GUI の [Talos IP Reputation] 設定の下にあるトグルボタンの横に警告が表示されます。

- アカウントは、Cisco DNA Cloud の Talos オファーに登録されている必要があります。
- Talos IP レピュテーション機能がスムーズに動作するには、アプリケーションテレメトリを有効にして、NetFlow コレクタとして Cisco DNA Center を選択します。

ステップ 1 Cisco DNA Center GUI でメニューアイコン（≡）をクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Cloud Authentication]** の順に選択します。

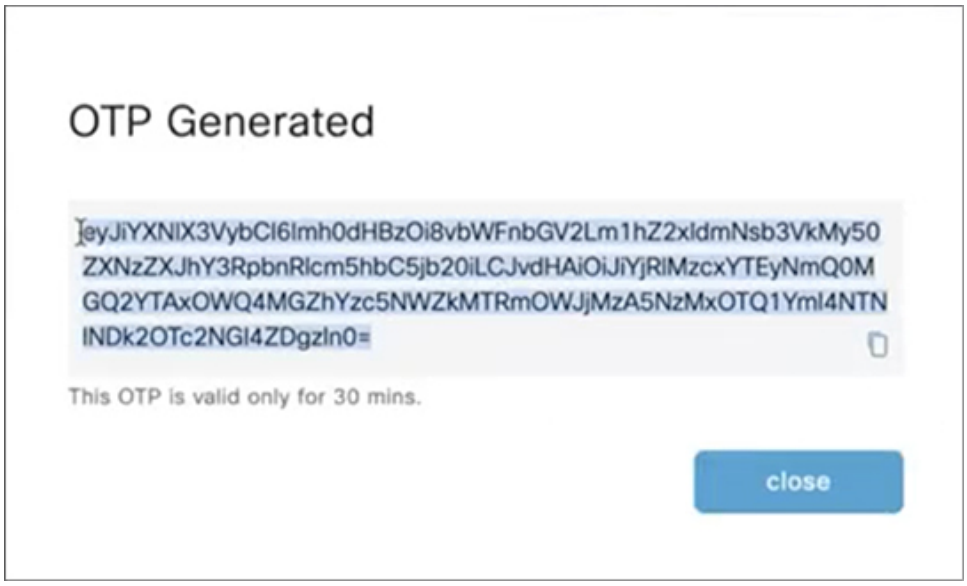
ステップ 2 [dna.cisco.com] リンクをクリックして、Cisco DNA Cloud アカウントを作成します。Cisco DNA Cloud で、Talos オファー登録し、適切な Cisco DNA Center リージョンを選択します。

図 *1 : Talos* オファーへの登録



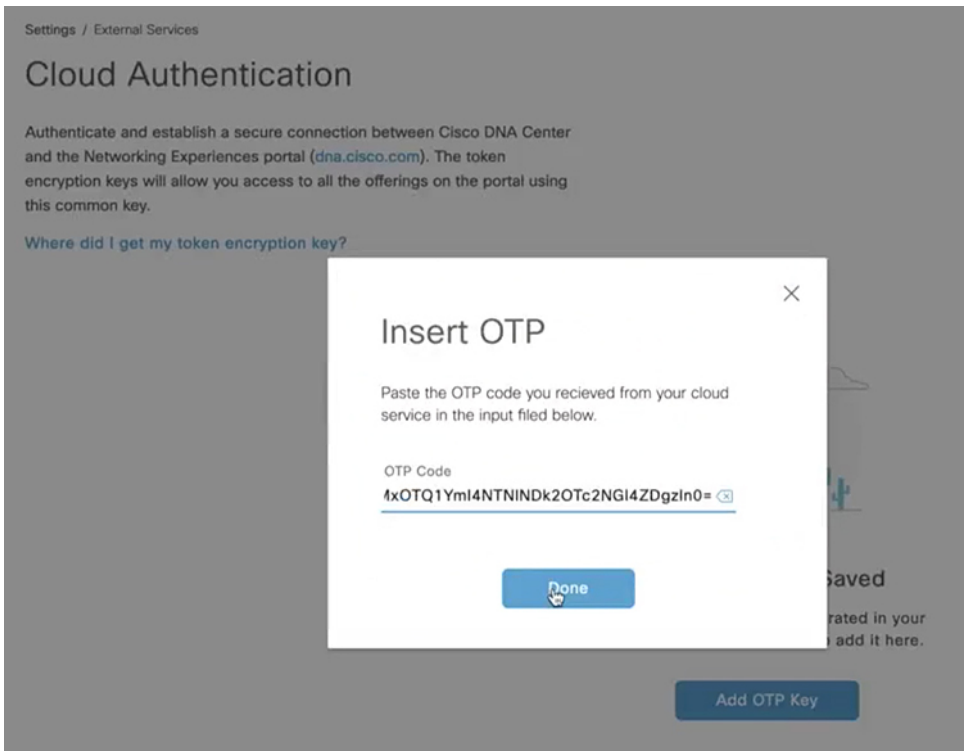
ステップ 3 [On-prem Connections] で Cisco DNA Center デバイスを登録します。ワンタイムパスワード（OTP）がデバイスに送信されます。この OTP は 30 分間有効です。

図 *2:* デバイスに送信される *OTP*



ステップ 4 Cisco DNA Center ホームページで、クラウド認証の OTP を使用して Cisco DNA Center デバイスを Cisco DNA Cloud に登録します（**[System-Settings]** > **[Cloud Authentication]**）。

図 *3 : Cisco DNA Cloud* への *Cisco DNA Center* の登録



（注） Cisco DNA Center デバイスを Cisco DNA Cloud に登録したら、3 分待ってからステップ 4 に進みます。

ステップ 5 [Cisco DNA Center AI Endpoint Analytics] ウィンドウ（**[AI Endpoint Analytics]** > **[Configurations]** > **[Trust Analytics]**）で、[Talos IP Reputation] トグルボタンをクリックして有効にします。[Trust Score] ウィンドウまたは [Cisco DNA Center System Settings] ウィンドウから [Talos IP Reputation] を有効にできます。
[Talos IP Reputation] を有効にすると、Cisco DNA Center は更新された IP のレピュテーションデータが利用可能になるたびにそのデータを受信します。ネットワーク内のエンドポイントが信頼できない IP アドレスにアクセスしようとすると、フラグが設定され、エンドポイントの [Trust Score] ビューの Talos IP レピュテーションに対して、「Detected」という警告メッセージが表示されます。この警告により、エンドポイントの全体的な信頼スコアが低下します。Talos IP レピュテーション機能により、アクセスされた信頼できない IP アドレスと、エンドポイントによるアクセス試行回数に関する情報が保存されます。この情報は、ネットワークのセキュリティを強化することを決定するときに役立ちます。

[Talos Reputation] ウィンドウ（**[Cisco DNA Center System Settings]** > **[Talos IP Reputation]**）には、Talos から受信したさまざまなファイルの最新バージョンが表示されます。これらのファイルを受信した時刻も表示されます。IPv4 および IPv6 ファイルは Talos IP レピュテーション データ ファイルであり、通常 1 日に 1 回更新されます。ただし、Threat Level ファイルはメタデータであり、このファイルが変更されることはほとんどありません。

[Cisco AI Endpoint Analytics Overview] ウィンドウ

メニューアイコン（☰）をクリックして、**[Policy]** > **[AI Endpoint Analytics]**の順に選択します。

[Overview] ウィンドウに次のダッシュレットが表示されます。

- **合計エンドポイント数**

  このダッシュレットでは、ネットワーク内のエンドポイントの合計数が [Fully Profiled] と [Partially Profiled] の 2 つのグループに分かれて表示されます。Cisco AI エンドポイント分析は、エンドポイントタイプ、OS タイプ、ハードウェアモデル、およびハードウェア製造元の 4 つの要因に基づいてエンドポイントをプロファイリングします。エンドポイントにこれらの要因の 1 つ以上が欠落している場合は、[Partially Profiled] グループにプロファイリングされます。

  [Partially Profiled Labels] をクリックすると、ネットワーク内のプロファイルが欠落しているエンドポイントの数が、プロファイルラベルタイプで分類されて表示されます。特定のプロファイルラベルが欠落しているエンドポイントを確認するには、プロファイルラベルの横にある数字をクリックします。[Endpoint Inventory] タブが、対応するエンドポイントのリストとともに表示されます。

- **AI 提案**

  Cisco AI エンドポイント分析は、スマートグループ化アルゴリズムを使用して、ネットワーク内で類似するプロファイリングデータを持つ不明なエンドポイントをグループ化します。AI エンドポイント分析を有効にした場合、次のタイプのルール提案が表示されます。これらのルール提案は、次のようにエンドポイントクラスタから学習した内容に基づいています。

- 類似している可能性があるエンドポイントをプロファイリングするための新しいルール。
- 以前に受け入れられていたルールの変更提案。
- 不要になったプロファイリングルールの確認。

詳細については、スマートグループ化のための Cisco AI ルール （52 ページ）を参照してください。

- **信頼スコア**

  [Trust Scores] ダッシュレットには、ネットワーク内のエンドポイントに割り当てられている信頼スコアの全体像が示されます。エンドポイントの信頼スコア （28 ページ）を参照してください。

- **設定**

  [Overview] エリアの右上隅にある [Configuration] リンクをクリックすると、次の設定にアクセスできます。

  - [Profile Rule Settings]：システムプロファイルルールの自動更新をスケジュールします。エンドポイント プロファイリング用の自動システムルール更新 （48 ページ）を参照してください。
  - [ISE Integration]：Cisco ISE への許可属性の公開 （15 ページ）を参照してください。
  - [**Trust Analytics**]：信頼スコアのソースを有効または無効にするには、このトグルボタンをクリックします。[Authentication Method] ソースを無効にすることはできません。アクティブな Cisco ISE 統合が設定されている場合、エンドポイントが使用する認証方式およびそのポスチャステータスによって、エンドポイントの信頼スコアが通知されます。[AI Spoofing Detection]、[Changed Profile Labels]、[Endpoint Attribute Conflict]、[NAT Mode Detection]、[Concurrent MAC Addresses]、[Security Sensor] などの信頼スコアデータのその他のソースは、有効または無効にすることができます。

    「エンドポイントの信頼スコア （28 ページ）」を参照してください。
  - [Endpoint Purge Policy]：エンドポイント パージ ポリシー （19 ページ）を参照してください。
  - [Endpoint Subnet Inspection]：エンドポイントサブネット検査の設定 （20 ページ）を参照してください。

- **エンドポイント MAC ランダム化**

  [Endpoint MAC Randomization] には、ネットワーク内の静的 MAC アドレスとランダムおよび変更 MAC アドレスの数が表示されます。ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコア （35 ページ）を参照してください。

Cisco ISE への許可属性の公開

ネットワークへのエンドポイントアクセスを承認し、エンドポイントを制御するために、Cisco ISE へ AI エンドポイント分析プロファイルデータを公開します。Cisco AI エンドポイント分析によって共有される属性情報には、AI エンドポイント分析ディクショナリを介して Cisco ISE 管理者が簡単にアクセスできるようになります。Cisco ISE 管理者は、Cisco ISE で許可ポリシーを簡単に作成できます。次の属性が Cisco ISE と共有されます。

1. 全体的な信頼スコアと、記録された各異常スコア。
2. CMDB 属性。
3. 多要素プロファイリング属性：ハードウェア製造元、ハードウェアモデル、オペレーティングシステム、およびエンドポイントタイプ。

Cisco DNA Center が Cisco ISE リリース 3.1 以降とアクティブに統合されており、認証属性を Cisco ISE に公開する必要がある場合は、次のタスクを実行します。

ステップ 1 Cisco DNA Center で属性共有を有効にするには、次の手順を実行します。

a) Cisco AI エンドポイント分析の [Overview] ウィンドウで、[Configurations] をクリックします。
b) 左側のパネルから [ISE Integration] をクリックします。
c) [Enable Profile Publishing to ISE] トグルボタンをクリックしてこの機能を有効にします。
d) 属性情報を Cisco ISE に公開するために使用するトピックのタイプに応じて、[Asset Topic Based Integration] チェックボックスと [Enhanced Authorization Integration] チェックボックスのいずれかまたは両方をオンにします。
e) **[Save]** をクリックします。

ステップ 2 Cisco ISE で pxGrid サブスクリプションを有効にするには、次の手順を実行します。

a) Cisco ISE GUI でメニューアイコンをクリックし、**[Work Center]** > **[Profiler]** > **[Settings]** の順に選択します。
b) Cisco ISE Release 3.1 に接続している場合、[Endpoint Analytics Settings] 領域で、次のチェックボックスをオンにします。
   - [Publish Endpoint Attributes to AI Endpoint Analytics]
   - [Consume Endpoint Profiles from AI Endpoint Analytics]

次のタスク

サブスクリプションを検証するには、Cisco ISE メインメニューから、**[Administration]** > **[pxGrid Services]** > **[Diagnostics]** > **[WebSocket]** > **[Clients]** の順に選択します。新しく作成された「`com.cisco.ea.data.ise-<Cisco ISE node>`」を含むサブスクリプションが、PSN ノードの [Subscription] 列に表示されます。

Cisco ISE の **[Policy]** > **[Policy Sets]** ウィンドウで、[Conditions Studio] に「**Endpoint-Analytics**」という名前の新しいディクショナリが表示されます。

Cisco ISE の **[Context Visibility]** > **[Endpoints]** ウィンドウで、エンドポイントの詳細情報の [MAC Address] をクリックします。その詳細情報の属性エリアに、Cisco AI エンドポイント分析から受信された属性の「EA-」というプレフィックスを含む属性が表示されます。

Trust Analytics

[Trust Analytics] ウィンドウでは、さまざまな信頼スコアソースが表示されます。また、一定期間非アクティブになった後にこれらのソースで発生したアラートを手動または自動でリセットしたり、エンドポイントの全体的な信頼スコアを正確に測定するために各信頼スコアソースの影響度を設定したりすることもできます。

信頼スコアは、Zero Trust の成果を達成できるように、ネットワーク上の特定のエンドポイントの信頼性を評価します。値は、1（低信頼度）から 10（高信頼度）の範囲で、複数のソースを使用して計算されます。

- [Endpoint Context]：このカテゴリのソースは、エンドポイントで使用される認証方法とエンドポイントのポスチャステータスに基づいて、エンドポイントの信頼性に関する情報を提供します。
- [Threat and vulnerability Context]：このカテゴリのソースは、エンドポイントに関連する各種の脅威に基づいて、エンドポイントがどの程度脆弱であるかに関する情報を提供します。
- [Network Context]：このカテゴリのソースは、エンドポイントからネットワークへのアクセス方法に関する情報を提供します。

信頼スコアの影響度により、異常が発生した場合のエンドポイントの信頼スコアを制御できます。次の影響度を使用できます。

- [Low]：ネットワークでの異常の重要度が低いとわかっている場合は、その影響度を [Low] に設定して、信頼スコアへの影響を小さくすることができます。影響度をこのように設定した後で同様の異常が再度検出されると、異常が検出されたエンドポイントの信頼スコアはゆっくりと 1 に低下します（システム生成の影響度が合計信頼スコアの 50% 上がります）。
- [Critical]：ネットワークでの異常の重要度が高いとわかっている場合は、その影響レベルを [Critical] に設定して、信頼スコアに非常に大きな影響を与えるようにすることができます。影響度をこのように設定した後で同様の異常が再度検出されると、異常が検出されたエンドポイントの信頼スコアはすぐに 1 に低下します（システム生成の影響度が合計信頼スコアの 50% 下がります）。
- [No Impact]：異常が検出されますが、全体的な信頼スコアには影響しません。このオプションを使用すると、全体的な信頼スコアを変更せずに異常をテストして表示できます。
- [System Default]：デフォルトのシステム生成の信頼スコア。

ソースの影響度をカスタマイズする方法については、「影響度のカスタマイズ」を参照してください。

異常や脆弱性が原因で逸脱が発生した場合、またはエンドポイント接続やインターフェイスに弱点が見つかった場合にアラートが表示されます。アラートは、対処後に手動でリセットできます。対処する必要がないアラートを手動でリセットすることもできます。または、リセットタイマーを設定して、アラートを自動的にリセットすることもできます。一定期間非アクティブになった後、このアラートはエンドポイントで検出されません。

ソースのアラートをリセットする方法については、「アラートのリセットの構成」を参照してください。

影響度のカスタマイズ

エンドポイントについて把握している影響度を設定することにより、エンドポイントの信頼スコアをカスタマイズできるようになりました。ソースに対して設定した影響度に基づいて、エンドポイントの全体的な信頼スコアが再計算されます。これにより、ある異常について、システム生成の信頼スコアに関係なく、ユーザーがその信頼度を決定できます。

（注） 認証方式 EAT-TLS およびポスチャ非準拠エンドポイントの場合、影響度を変更しても、信頼度は同じままです。信頼度は、MAB 認証の場合にのみ変更されます。

（注） 使用する認証方式によって得られる高い信頼スコアは、その認証方式の影響度を変更しても低下しません。認証方式の影響度が増大した場合、エンドポイントでは、その新しいセッションが受信されない限り、現在の信頼スコアを保持し続けます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[AI Endpoint Analytics]** > **[Overview]** > **[Manage Sources]** の順に選択します。
[Trust Analytics] ウィンドウが開きます。

ステップ 2 [Customize Impact Level] をクリックします。

ステップ 3 [Let's Do It] をクリックします。
[Customize Trust Score Sources] ワークフローが開始されます。ワークフローウィンドウの下部にある [Exit] オプションをクリックすると、いつでもワークフローを終了できます。

ステップ 4 影響度を変更するソースの横にあるチェックボックスをオンにします。

ステップ 5 [More Actions] ドロップダウンリストから [New Impact Level] を選択します。

ステップ 6 [Next] をクリックします。

次のウィンドウでは、個々のエンドポイントに対する信頼スコアのカスタマイズの影響を示す、以前の信頼スコアと新しい信頼スコアの比較調査が提供されます。この円グラフには、ソースの影響レベルの変化による影響を受けたかどうかに関係なく、ネットワーク内のすべてのエンドポイントが含まれています。

下の [Endpoints (After)] テーブルには、影響度構成の変更の結果として影響を受けた各エンドポイントの新しい信頼スコアが表示されます。

ステップ 7 [Next] をクリックします。

各ソースの新しい影響度を示す概要が表示されます。結果に満足できない場合は、[Edit] をクリックしてワークフローに戻り、信頼スコアの影響度を編集します。

ステップ 8 [Next] をクリックします。

エンドポイントの信頼スコアが更新され、Cisco ISE にも送信されます。これにより、Cisco ISE が信頼スコアベースの認証ポリシーを使用している場合、該当するエンドポイントの認可変更が生じる可能性があります。

次のタスク

[Policy] > [AI Endpoint Analytics] > [Trust Score] で、エンドポイントの新しい信頼スコアを確認します。

アラートのリセットの構成

一定期間非アクティブになった後にアラートを手動または自動でリセットできます。デフォルトでは、サポートされているすべてのソースのリセットアクションは手動に設定されています。ここで説明されているグローバル構成ワークフローを使用して、アラートをリセットするように構成できます。

ステップ 1 メニューアイコン（≡）をクリックして、**[Policy]** > **[AI Endpoint Analytics]** > **[Manage Sources]** の順に選択します。

[Trust Analytics] ウィンドウが開きます。

ステップ 2 [Alert Configuration] をクリックします。

ステップ 3 [Choose Reset Alert Type] ウィンドウで、[Let's Do It] をクリックします。

ワークフローウィンドウの下部にある [Exit] オプションをクリックすると、いつでもワークフローを終了できます。

ステップ 4 [Reset Alert Type] ドロップダウンリストから、[Manual] または [Customize reset timer after alert inactivity] を選択します。

ステップ 5 [Customize reset timer after alert inactivity] を選択した場合は、非アクティブなときにアラートをリセットするまでの日数（0 ～ 365 日）または時間数（0 ～ 24 時間）を入力します。

ANC ポリシーを削除するか、保持するかを選択できます。複数の信頼スコアソースからの信頼値がエンドポイントにある場合、[Remove ANC Policy] チェックボックスがオンになっていても、ANC ポリシーは削除されません。

ステップ 6 [Next] をクリックします。

ステップ 7 手順 4 で選択した設定を適用するすべてのソースの横にあるチェックボックスをオンにします。

ステップ 8 [Apply] をクリックします。

[Trust Analytics] ウィンドウからローカルでアラートをリセットするように構成することもできます。アラートのリセットを構成するソースを選択します。右側のスライドインウィンドウで、適切な設定を選択し、[Save] をクリックします。アラートのリセット構成オプションは、すべてのソースで使用できるわけではないことに注意してください。アラートがリセットされると、同じ情報が Cisco ISE に伝達されます。

アラートは、更新のために 30 分ごとにチェックされます。また、チェック中に、アラートのリセット構成で設定された期間が経過した場合、その異常について信頼スコアがリセットされます。アラートのリセットのステータスは、監査ログに表示されます。

エンドポイント パージ ポリシー

定義された時間にわたって非アクティブだったエンドポイントをネットワークから削除するには、エンドポイント パージ ポリシーを定義します。エンドポイントを削除する必要があるまでの非アクティブ期間を定義できます。また、プロファイリング属性に基づいて特定のエンドポイントのセットに作用するようにパージポリシーをカスタマイズすることもできます。パージポリシーは毎日午前2時（サーバー時間）に実行され、定義されたパージ要件を満たすエンドポイントがネットワークから削除されます。

Cisco AI エンドポイント分析にインポートされた登録済みエンドポイントおよび静的エンドポイントは、エンドポイント パージ ポリシーの影響を受けません。

Cisco DNA Center のバックアップ/復元操作、およびエンドポイント パージ アクティビティを同時に実行することはできません。バックアップ/復元操作が午前 2 時に進行中の場合、パージアクティビティは開始されません。エンドポイント アクティビティの進行中にバックアップ/復元操作が開始されると、エンドポイントパージの実行は停止され、パージアクティビティは未完了のままになります。残りのエンドポイントは、次のパージが翌日の午前 2 時（サーバー時間）に実行されるまで処理されません。

エンドポイントパージポリシーを表示、編集、または追加するには、メニューアイコン（☰）をクリックし、**[Policy]** > **[AI Endpoint Analytics]** > **[Configurations]** > **[Endpoint Purge Policy]** を選択します。デフォルトでは、次のポリシーを使用できます。

- **Default**
- **Random MAC Default**

これらのデフォルトポリシーは編集できません。有効または無効にすることだけが可能です。

[Purge Now] オプションを使用すると、午前 2 時まで待つのではなく、すぐにパージポリシーを実行できます。[Purge Now] オプションを使用するには、次の 2 つの方法があります。

- すぐに実行する必要があるパージポリシーを選択し、[More Actions] ドロップダウンリストから [Purge Now] を選択します。
- すぐに実行する必要があるパージポリシーの [Actions] 列の下にあるアイコンをクリックし、[Purge Now] を選択します。

パージポリシーの作成

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[AI Endpoint Analytics]** > **[Configurations]** > **[Endpoint Purge Policy]**の順に選択します。

ステップ 2 [Add Endpoint Purge Policy] をクリックします。

ステップ 3 [Add Endpoint Purge Policy] ダイアログボックスで、[Let's Do It] をクリックしてワークフローに直接移動します。

ステップ 4 [Define Policy Details] ウィンドウで、次の手順を実行します。

1. ポリシーの名前を [Rule Name] フィールドに入力します。
2. [Select Status] ドロップダウンリストで [Enabled] または [Disabled] を選択します。
3. エンドポイントがパージされるまでの非アクティブ時間を定義します。[Elapsed Greater than or Equal to] フィールドに値（日単位）を入力してください。有効な値の範囲は 5 ー 180 日です。

ステップ 5 （オプション）[Define Additional Policy Conditions] ウィンドウで、このパージポリシーの影響を受けるエンドポイントをフィルタ処理するためのプロファイリング属性を選択します。選択する属性の横にあるチェックボックスをオンにして、その属性に関して表示されるドロップダウンリストで必要な値を選択してください。

ステップ 6 [Summary] ウィンドウに、パージポリシーの設定が表示されます。表示される詳細情報を確認し、[Done] をクリックしてポリシーを作成します。

次のタスク

エンドポイント パージ アクティビティの監査ログ

エンドポイント パージ ポリシーを有効にして、パージアクティビティが実行された後に、監査ログを確認することができます。詳細については、『Cisco DNA Center Administrator Guide』の「**View Audit Logs**」を参照してください。

エンドポイントサブネット検査の設定

展開内では、アクセスレイヤにあるデバイスとアクセスレイヤよりも上にあるデバイスの IP サブネットが異なります。シスコの TTA デバイスの場合、エンドポイント プロファイリングの精度は、Cisco AI エンドポイント分析によってサウスバウンドトラフィックのみが分析される場合に最大になります。エンドポイントプロファイリングを向上させるには、Cisco AI エンドポイント分析 で分析する必要がある特定の IP サブネットまたはサブネット範囲を設定します。

その後、このフィルタ処理されたサブネットに関する設定は、Cisco SD-AVC サーバーと共有されます。この設定は、Cisco SD-AVC サーバーを介して Cisco TTA デバイスに適用されます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[AI Endpoint Analytics]** > **[Configurations]** > **[Endpoint Subnet Inspection]**の順に選択します。

ステップ 2 [IP Subnet] フィールドに必要な値を入力します。

ステップ 3 [+] をクリックして IP サブネットを追加します。このウィンドウでは、複数のサブネットまたはサブネット範囲を追加できます。

Endpoint Inventory

[Endpoint Inventory] タブには、設定されたデータソースを介して Cisco AI エンドポイント分析に接続されているエンドポイントの詳細が表示されます。このビューには、接続されているすべてのエンドポイントのプロファイリング情報が表示されます。

表示するエンドポイントのプロファイリング情報を選択するには、テーブルの右上隅にある垂直省略記号アイコンをクリックします。次のプロファイリング情報セットのいずれかを選択し、[Apply] をクリックします。

- [All]：使用可能なすべてのプロファイリング情報が表示されます。このセットは編集できません。
- [General]：これを選択すると、エンドポイントの全体図を確認できるプロファイリング情報が表示されます。これは、デフォルトで表示される列のセットです。このセットは編集できません。
- [Detailed]：これを選択すると、エンドポイントを深く洞察できるプロファイリング情報が表示されます。このセットは編集できません。
- [Custom]：これは編集可能な唯一のセットです。[Endpoint Inventory] ウィンドウに表示するプロファイリング情報をオンまたはオフにします。

必要な [View Known Profiles] ボタンをクリックして、[All Endpoints] ビューに表示されるエンドポイントのリストをフィルタ処理することもできます。**エンドポイントタイプ**、**ハードウェア製造元**、**ハードウェアモデル**、および **OS タイプ**でエンドポイントのリストをフィルタ処理できます。

表示されるエンドポイント インベントリ テーブルを編集またはカスタマイズするには、テーブルの上部の右隅にある歯車アイコンをクリックします。表示されるペインには、[Table Appearance]、[Edit Table Columns]、および [Edit Custom Views] メニューが含まれており、テーブルビューやテーブルに表示する情報を選択したり、カスタムビューを作成したりできます。

[Apply] をクリックして変更を保存するか、[Reset All Settings] をクリックしてエンドポイント インベントリ テーブルのデフォルト設定を適用します。

要件に基づいて一連のエンドポイントを簡単にフィルタ処理できます。テーブルの上部にある検索バーを使用すると、フィルタパラメータを簡単に見つけることができます。入力して検索

支援機能を使用するか、表示されるドロップダウンをスクロールして必要なパラメータを見つけて選択することができます。

ほとんどの列にはクイックフィルタが含まれています。一部のフィルタでは値を選択できるドロップダウンメニューが表示され、一部のフィルタは入力可能なテキストフィールドです。

エンドポイントを登録したり、登録済みのエンドポイントを編集、削除、およびプロファイリングしたりできます。単一または複数のエンドポイントを選択するには、MAC アドレスの横にあるチェックボックスをオンにします。これにより、選択したエンドポイントに対して、[Actions] ドロップダウンリストから特定のアクションをフィルタリングして実行することができます。

登録済みのエンドポイント、未登録のエンドポイント、および他のソースから学習したエンドポイントも削除できます。エンドポイントを選択すると、テーブル内のすべての行を選択できるバナー行が表示されます。バナーをクリックすると、バナー行でテーブル内のすべての行をクリアできるようになりました。すべてのエンドポイントを削除するには、バナーをクリックするか、[More Actions] ドロップダウンリストから [Delete] オプションを選択します。

エンドポイントのプロファイリングの完全な詳細を表示するには、エンドポイントの [MAC Address] をクリックします。表示されるスライドインダイアログボックスには、ユーザーの詳細、エンドポイントの詳細、およびエンドポイントの属性の詳細が含まれます。

Cisco DNA Center リリース 2.2.2 以降では、[Details] タブに次の新しいフィールドが表示され、Cisco ISE から受信した詳細が示されます。

- [Authentication Status]：このフィールドには、エンドポイントが Cisco ISE で認証された場合は [Started]、そうでない場合は [Disconnected] と表示されます。
- [Authorization Profile]：Cisco ISE のエンドポイントに設定されている認証ポリシーがここに表示されます。
- [Security Group Tag]：Cisco ISE でエンドポイントに設定されたセキュリティグループタグがここに表示されます。

これらの属性の詳細については、使用する Cisco ISE リリースの Cisco ISE 管理者ガイド [英語] を参照してください。

Cisco DNA Center 2.2.2 以降では、エンドポイントの詳細を示すスライドイン ダイアログボックスに [Trust Score] タブがあります。このタブには、エンドポイントの信頼スコアを示すさまざまな要因の詳細が表示されます。エンドポイントの信頼スコア （28 ページ）を参照してください。

Cisco DNA Center 2.2.3 以降では、[Details] タブに [Previous MAC Addresses] エリアがあり、MAC ランダム化機能が有効になっているエンドポイントで使用された MAC アドレスが表示されます。ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコア （35 ページ）を参照してください。

Cisco AI エンドポイント分析データのエクスポート

このウィンドウからエンドポイントとエンドポイントの詳細のリストをエクスポートするには、[Export] をクリックします。[Endpoint Inventory] ウィンドウでフィルタを適用すると、フィルタ処理されたエンドポイントのみがエクスポート用に処理されます。すべてのエンドポイントの詳細をエクスポートするには、フィルタが適用されていないことを確認して、[Export] をクリックします。

[Export] をクリックすると、[Reports] ウィンドウで新しいタブが開きます。[Generated Reports] ウィンドウには、開始されたエクスポートのリストが表示され、リストの一番上に最新のエクスポート要求が表示されます。[Endpoint Inventory] ウィンドウから生成されたレポートの [Template Category] 列に [AI Endpoint Analytics] が含まれています。レポートの生成には数分かかります。レポートのダウンロード準備ができると、[Last Run] 列の値が [Not Initiated] から、その横にダウンロードアイコンがあるタイムスタンプに変わります。タイムスタンプは、エクスポートリストが生成された時刻を示します。ダウンロードアイコンをクリックして、エンドポイントのリストの CSV ファイルをシステムにダウンロードします。

次の手順で、[Reports] ウィンドウから Cisco AI エンドポイント分析データをエクスポートすることもできます。

（注） エンドポイントの AI エンドポイント分析データの最初のエクスポートは [Endpoint Inventory] ウィンドウから実行する必要があります。その後、[Reports] ウィンドウから直接 AI エンドポイント分析レポートを生成できます。

ステップ 1 メニューアイコン（≡）をクリックして、**[Reports]** > **[Report Templates]** > **[AI Endpoint Analytics]** の順に選択します。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

（注） 今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 3 [Select Report Template] ウィンドウでは、[Endpoint Profiling] テンプレートがデフォルトで適用されています。

ステップ 4 [Setup Report Scope] ウィンドウで、次の手順を実行します。

a) [Report Name] フィールドに名前を入力します。
b) [Endpoint Inventory] ウィンドウからエクスポートするエンドポイントのリストに適用するフィルタを定義します。
c) すべてのエンドポイントの詳細をエクスポートするには、[Scope]エリアで値を選択しないでください。

ステップ 5 [Select File Type] ウィンドウの [Client Details] エリアで、選択したパラメータを確認できます。関連するフィールドの横にあるチェックボックスをオンまたはオフにして、エクスポートする情報を編集します。

ステップ 6 [Schedule Report] ウィンドウで、[Run Now]、[Run Later]（[One-Time] または [Run Recurring]）オプションボタンをクリックします。

（注） [Run Later] の [One-Time] および [Run Recurring] オプションには、エクスポートの時間を定義するスケジューリングフィールドが表示されます。

ステップ 7 [Delivery and Notification] ウィンドウでは、[Email Report] チェックボックスをオンにしないでください。

ステップ 8 [Summary] ウィンドウで、すべての設定を確認します。変更するには、[Edit] をクリックします。

ステップ 9 生成されたレポートのリストを表示するには、このウィンドウの [View Reports] リンクをクリックします。レポートが生成され、このウィンドウに表示されるまでに数分かかります。

エンドポイントのフィルタ処理

この手順を使用して、プロファイリングデータ、プライマリ プロファイリング ラベル、既知のプロファイル、および正常性ステータスに基づいてエンドポイントをフィルタ処理します。

ステップ 1 [Endpoint Inventory] ウィンドウで、[Filter] をクリックします。

ステップ 2 必要に応じて、対応するドロップダウンリストから値を選択するか、必要な値のオプションボタンをクリックするか、特定のフィールドの必要な値の横にあるチェックボックスをオンにして、次のフィルタを定義します。

- **Profile Status Condition**
- **Mac Address**
- **Is Random Mac**
- **信頼得点**
- [IP Address]
- **Last Seen**
- **ホスト名（Host Name）**
- **エンドポイント タイプ**
- **OS Type**
- **ハードウェア モデル**
- **ハードウェア製造元**
- **Registered**

ステップ 3 [Apply] をクリックします。

また、4 つのプライマリ プロファイリング ラベルで表示されるプロファイリング済みのエンドポイントをフィルタ処理することもできます。[View Known Profiles] セクションで 1 つ以上のラベルをクリックします。

エンドポイントの正常性ステータスは 5 分ごとに更新されます。

属性用語集

属性用語集は、Cisco ISE プローブデータから使用可能なすべてのプロファイリング属性のリストです。

すべてのプロファイリング属性を表示するには、次の手順を実行します。

ステップ 1 [Endpoint Inventory] ウィンドウで、エンドポイントの MAC アドレスをクリックします。

ステップ 2 右側に表示される新しい領域で、[View Attribute Glossary] をクリックします。

[Attribute Glossary] ウィンドウに、属性ごとに次の情報が表示されます。

- **キープロファイリング属性**
- **説明**
- **関連付けられたプロファイルラベル**
- **[Source]**
- **Dictionary**
- **ディスカバリの方法**

用語集では、すべてのプロファイリング属性の詳細ビューが表示されます。プロファイリング属性がプロファイルラベルの作成に頻繁に使用される場合は、そのラベルが [Associated Profile Labels] 列に一覧表示されます。

また、ルールの論理条件の作成中に、[Choose Attribute Condition] ウィンドウに属性用語集を表示することもできます。詳細については、「カスタムルールの作成」を参照してください。

エンドポイントの登録

新しいエンドポイントをオンボードおよびプロファイリングするには、そのエンドポイントを Cisco AI エンドポイント分析に登録します。エンドポイントのプロファイリング情報は、分類のための信頼できる情報源です。また、[Register Endpoint] オプションを使用して、登録済みのエンドポイントの新しいプロファイル情報を更新することもできます。

ステップ 1 **[Actions]** > **[Register Endpoints]** の順に選択します。

ステップ 2 [Single] または [Bulk] のいずれかのオプションボタンをクリックして、単一のエンドポイントまたは複数のエンドポイントを登録するかどうかを選択します。

a) [Single] オプションボタンをクリックしたら、エンドポイントの [MAC Address]、[Endpoint Type]、[Hardware Model]、および [Hardware Manufacturer] を入力します。
b) [Bulk] オプションボタンをクリックしたら、次の手順を実行します。
   1. [Download .csv Template] オプションをクリックして、.csv テンプレートをダウンロードします。
   2. ダウンロードした .csv ファイルに、登録する必要がある各エンドポイントの詳細を入力します。具体的には、MAC アドレス、エンドポイントタイプ、ハードウェアモデル、およびハードウェア製造元です。このファイルを保存します。
   3. [Choose a File] オプションを使用して .csv ファイルをアップロードします。

   [Bulk] オプションを使用すると、一度に最大 500 個のエンドポイントを登録できます。

ステップ 3 [Review Endpoint] ウィンドウでエンドポイントの詳細を確認します。変更するには、[Edit] をクリックします。

（注） 既存のエンドポイントの登録中は、エンドポイントのプロファイルラベルの変更が紫色で反映され、編集できます。

ステップ 4 [Next] をクリックして、登録プロセスを続行します。

ステップ 5 [登録（Register）] をクリックします。

登録済みのエンドポイントの編集

登録済みのエンドポイントのプロファイリング情報は、[Endpoint Inventory] ウィンドウから更新できます。

ステップ 1 編集するエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックします。

ステップ 3 [Edit Endpoint] をクリックします。

ステップ 4 [Endpoint Type]、[Hardware Model]、[Hardware Manufacturer] に詳細を入力します。

ステップ 5 [Save] をクリックします。

登録済みのエンドポイントの削除

登録済みのエンドポイントがネットワークの一部ではなくなった場合は、Cisco AI エンドポイント分析から削除できます。

ステップ 1 削除するエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックします。

ステップ 3 [Delete Endpoint] をクリックします。

次のメッセージが表示されます。

「Do you really want to delete the selected endpoint(s)?」

ステップ 4 [Yes] をクリックして、Cisco AI エンドポイント分析からエンドポイントを完全に削除します。

信頼得点

[Trust Score] ウィンドウは、次の 2 つの表形式のセクションで構成されています。

[Alerts]：

異常や脆弱性が原因で逸脱が発生した場合、またはエンドポイント接続やインターフェイスに弱点が見つかった場合にアラートが表示されます。これらのアラートは、信頼スコアに悪影響を与える検出（MAC アドレスの同時検出、NAT モード、またはその他の信頼できない変更など）があったことを表しています。アラートを監視することで、ネットワーク内の最も緊急のリスクに迅速に対処できます。

[Alerts] タブには、ネットワーク内のエンドポイントが受信したさまざまなアラートが表示されます。以前は、エンドポイントが受信したアラートのタイプを確認するために各エンドポイントの詳細を個別に確認する必要があり、他のどのエンドポイントが同じアラートを受信したかを知る方法はありませんでした。今では、特定のタイプのアラートを受信したすべてのエンドポイントがわかるようになりました。アラートをクリックすると、このアラートを受信したエンドポイントのリストを表示できます。さらに各エンドポイントをクリックすれば、詳細を表示できます。アラートは、次の 3 つの状態のいずれかになります。

- [Open]：エンドポイントで最初に検出されたアラートはオープン状態であり、解決または後で対処するためのユーザーによるアクションが必要になります。
- [Disabled]：オープンアラートに対してアクションを実行しない場合は、アラートを無効状態に移行できます。アラートを任意の期間、さらには無期限に無効にすることができます。この期間中は、このアラートで新しいエンドポイントが検出されても、アラートは無効状態のままです。
- [Reset]：アラートに対してすぐにアクションを実行しない場合は、アラートをリセット状態に移行できます。リセット後に別のエンドポイントでこのアラートが検出されると、アラートはオープン状態に戻ります。

[Endpoint]：

このビューには、エンドポイントの全体的な信頼スコアを示すさまざまな要因の列が表示されます。信頼スコアは、動作異常が検出されたエンドポイントを特定するために役立ちます。これにより、エンドポイントの詳細情報を調べて、必要な修復アクションを実行することができます。低い信頼スコアを管理するためにエンドポイントに ANC ポリシーを適用する場合、[Trust Score] ビューには、適用された ANC ポリシーの名前とポリシーが適用された日時も表示されます。エンドポイントの信頼スコア （28 ページ）を参照してください。

オプションの [Reset Trust Score] を使用すると、一度に複数のエンドポイントをリセットできるようになりました。ただし、パフォーマンスの問題を避けるために、最大 10 個のエンドポイントまでという上限があります。エンドポイントのリセット時には、監査目的で、アクションの正当化が必要になります。エンドポイントがリセットされると、そのエンドポイントの信頼スコアとそのエンドポイントに適用されていた ANC ポリシーがクリアされます。

エンドポイントの信頼スコア

Cisco AI エンドポイント分析は、エンドポイントに信頼スコアを割り当てます。これにより、ネットワーク内の潜在的に危険なエンドポイントを簡単にモニターして対処することができます。異常な動作がモニタおよび追跡され、追跡された異常の数と頻度に基づいて信頼スコアが割り当てられます。

信頼スコアの計算に含める必要があるソースを選択するには、Cisco AI エンドポイント分析の [Overview] ウィンドウで、**[Configuration]** > **[Trust Analytics]** を選択します。ソースをクリックすると、スライドイン構成ウィンドウが右側に表示されます。トグルボタンをクリックしてソースを有効にします。

Cisco AI エンドポイント分析 は、次の要因に基づいて履歴信頼スコアを生成します。

- エンドポイントに関連付けられた異常の履歴（このエンドポイントに関して検出された異常の数）。
- エンドポイントで検出された各異常の重大度。

Cisco DNA Center リリース 2.2.3 以降では、エンドポイントの全体的な信頼スコア計算に次の異常が考慮され、検出された異常ごとにスコアが表示されます（対応するソースが有効になっている場合）。

- **AI スプーフィング検出**

  Cisco AI エンドポイント分析 は、NetFlow テレメトリデータ、および Cisco ISE デバイスと SD-AVC デバイスからのネットワークプローブデータを分析して、スプーフィングされたエンドポイントを検出します。NetFlow コレクタサーバーの構成方法の詳細については、テレメトリを使用した Syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定を参照してください。Cisco DNA Center 2.3.2 以降では、Cisco DNA トラフィック テレメトリ アプライアンスからのプローブおよび NetFlow データ（DN-APL-TTA-M）も分析されます。Cisco DNA トラフィック テレメトリ アプライアンスへのトラフィックの受信スパンを構成して、Cisco AI エンドポイント分析でエンドポイント トラフィック データを スプーフィング検出に使用できるようにします。

  各エンドポイントタイプには、機械学習アルゴリズムを使用して開発された動作モデルがあります。エンドポイントに対して受信されたデータに基づき、エンドポイントの動作がエンドポイント タイプ プロファイルで予期されていない動作の場合、エンドポイントには [AI Spoofing Detection] 領域で低い信頼スコアが割り当てられます。エンドポイントで使用されるアプリケーションおよびサーバーポートは、このスプーフィング検出プロセスで分析されます。たとえば、プリンタとしてプロファイリングされたエンドポイントがビデオ通話アプリケーションを使用する場合、スプーフィングされたエンドポイントとして識別され、信頼スコアが割り当てられます。

エンドポイントは、Cisco DNA Center の管理対象スイッチの MAC アドレスによって識別されます。NAT の使用、仮想マシンまたはコンテナの実行など、単一の MAC アドレスを使用する複数のエンドポイントは、Cisco AI エンドポイント分析でサポートされている構成ではありません。

AI スプーフィング検出は現在、次のデバイスタイプをカバーしています。

- IP 電話
- プリンタ
- カメラ
- 次のハードウェアモデル属性を持つビルディングオートメーションデバイス：
  - Automated-Logic-Device
  - Honeywell-Device
  - Johnson-Controls-Device
  - Rockwell-Automation-Device
  - Schneider-Electric-Device
  - Siemens-Automation-Device
  - Siemens-Building-Device
  - Trane-Device
- TelePresence：
  - 次のいずれかのハードウェアモデルを持つエンドポイント：
    - Cisco-Tandberg-Device
    - Cisco-TelePresence
    - Cisco TelePresence SX80
    - Cisco Telepresence SX20
    - Cisco-Collaboration-Room-Endpoint
    - Poly-Device
  - デバイスタイプがビデオ会議のエンドポイント

- **エンドポイント属性の競合**

  デバイスがネットワークに参加し、デバイスがアクティブであるときに定期的にプローブを実行すると、エンドポイントのプロファイリングデータが継続的にモニタされ、更新されます。エンドポイントから受信したプロファイリングデータにおける特定の変化は、Cisco AI エンドポイント分析 で異常としてフラグが付けられます。たとえば、エンドポイントが最初に Linux デバイスとしてプロファイルされ、その後で macOS デバイスとして

プロファイルされた場合、これは重大度の高い異常としてフラグが付けられます。エンドポイントの [Endpoint Attribute Conflict] 列にスコアが割り当てられ、エンドポイントの全体的な信頼スコアもこの変化を反映して更新されます。

ただし、macOS のバージョンに変化があり、エンドポイントが新しいリリースから古いリリースにダウングレードされたように見える場合、そのような変化は優先順位の低い異常としてフラグが付けられ、対応するスコアがそれに応じて更新されます。

- **NAT モード検出**

  ネットワーク内に NAT 対応ルータがある場合、NAT ルータに接続されたエンドポイントは、特定のエンドポイントの IP アドレスまたは MAC アドレスではなくルータの IP アドレスまたは MAC アドレスによって認識されます。NAT 対応ルータに関する情報は、接続先の Cisco Catalyst 9000 シリーズ デバイスから収集されます。

- **同時 MAC アドレス**

  同じ MAC アドレスを共有し、Cisco Catalyst 9000シリーズ デバイスに接続されているエンドポイントを特定してください。共有 MAC アドレスを持つエンドポイントには、同時 MAC アドレススコアが割り当てられます。これにより、容易に、それらのエンドポイントを識別して詳細情報を調べることができます。

- **セキュリティ センサー**

  セキュリティ センサー スキャン機能を使用すると、特定の Cisco Catalyst 9000 シリーズ スイッチにアクティブプローブをインストールし、開いていると想定されていないのに開いているポート、クレデンシャルの脆弱性、またはその両方についてエンドポイントをスキャンするように Cisco AI エンドポイント分析 を設定できます。

エンドポイントの信頼スコアは、Cisco ISE から収集される次のイベントによっても通知されます。Cisco ISE を介して認証するすべてのエンドポイントは、次のイベントに基づいて初期信頼スコアを受け取ります。

- **認証方式**
- **ポスチャ**

（注） Cisco Catalyst 9000 シリーズ デバイスからデータを受信する信頼スコアソースの場合、デバイスで CBAR を有効にし、デバイスを Cisco IOS-XE リリース 17.6 以降にアップグレードする必要があります。

[Endpoint Inventory] ウィンドウに表示される信頼スコアは、エンドポイントの異常の履歴と重大度を考慮した全体的な信頼スコアです。[MAC Address] をクリックすると、エンドポイントに割り当てられた信頼スコアの原因の詳細情報が表示されます。たとえば、エンドポイントに関して低レベルの異常が検出され、これが異常の唯一のインスタンスである場合、エンドポイントの全体的な信頼スコアは 9 になります。

複数の低レベルの異常が検出された場合は、異常の数を考慮して全体的な信頼スコアがさらに低下します。

割り当てられる信頼スコアの範囲は 1 ー 10 で、次のように分類されます。

信頼スコアカテゴリ	範囲	エンドポイントの脅威レベル
低	1 ～ 3	高
中規模	4 ～ 6	中程度
高	7 ～ 10	低

その後、Cisco ISE から適応型ネットワーク制御（ANC）ポリシーを適用して、エンドポイントで適切な修復アクションを実施することができます。*Cisco ISE* の管理者ガイドで「Maintain and Monitor」の章にある「Adaptive Network Control」を参照してください。

ANC ポリシーは、Cisco ISE で定義され、選択したエンドポイントに修復アクションを適用することを可能にします。ANC ポリシーを適用して、エンドポイントを隔離またはシャットダウンしたり、エンドポイントのポートをバウンスしたり、エンドポイントの再認証を強制的に実行することができます。Cisco AI エンドポイント分析で望ましくない信頼スコアを持つエンドポイントに ANC ポリシーを適用すると、認可変更（CoA）が Cisco ISE からそのエンドポイントに送信されます。

エンドポイントは、MAC アドレスによって識別されます。Cisco ISE は、ANC 適用時点で識別された MAC アドレスに関してアクティブセッションを保持しているエンドポイントに CoA を送信します。その時点で Cisco ISE においてアクティブセッションを持たない、同じ MAC アドレスのエンドポイントは、新しいセッションが開始されたときに、または設定された再認証タイマーの終了時に再認証する必要がある場合に、ANC ポリシーと照合されます。

ANC ポリシーが適用されているエンドポイントを確認するには、Cisco ISE 管理ポータルにログインします。メインメニューから、**[Operations]** > **[RADIUS]** > **[Live Sessions]** の順に選択します。[Endpoint ID] 列に、スプーフィングされたエンドポイントの MAC アドレスを入力します。これにより、同じ MAC アドレスを共有し、現在 Cisco ISE でライブセッションを持つエンドポイントがフィルタ処理されます。これらが、ANC ポリシーの影響を受けるエンドポイントです。

Cisco ISE で RADIUS セッションの履歴ログを表示するには、メインメニューから、**[Operations]** > **[Reports]** > **[Reports]** > **[Endpoints and Users]** > **[RADIUS Authentications]** の順に選択します。

Cisco ISE でエンドポイントへの ANC ポリシーの適用を表示または変更するには、メインメニューから、**[Context Visibility]** > **[Endpoints]** の順に選択します。必要に応じて、エンドポイントの MAC アドレスの横にあるチェックボックスをオンにして、リストの上部に表示されるオプションをクリックしてください。

前提条件

エンドポイントの信頼スコアを受信するための前提条件：

- Cisco DNA Center がリリース 2.2.2 以降にアップグレードされている。

- Cisco ISE がオンプレミス Cisco DNA Center に接続されている。
- ネットワーク アクセス デバイスが、Cisco DNA アシュアランス と Cisco ISE の両方によって管理されている。

（注） Cisco DNA アシュアランス では 500 台の NetFlow エクスポータのみサポートされるため、エンドポイント スプーフィング検出機能は、NetFlow エクスポートフローで最大 500 台のネットワーク アクセス デバイスをサポートします。

- ネットワーク アクセス デバイスに接続されているエンドポイントが、Cisco ISE を介して認証されている。
- [Trust Score Sources] ウィンドウ（**[Policy]** > **[AI Endpoint Analytics]** > **[Configurations]** > **[Trust Analytics]**）で、信頼スコアの計算に必要なソースが有効になっている。

エンドポイント属性の競合

Cisco AI エンドポイント分析では、エンドポイントの正確なプロファイルラベルを取得するために、さまざまなソースから複数のプローブのデータが継続的に収集されます。Cisco AI エンドポイント分析では、次のソースから、次のデータが収集されます。

Cisco ISE から：

- RADIUS プローブ
- ディレクトリからのユーザーの詳細情報
- VPN の詳細情報（AnyConnect の可用性などの）
- オプションで、ポートフォワーディングが設定されている場合のその他のデータ（DHCP の詳細情報など）

スイッチから：

- デバイス接続メッセージ（DHCP メッセージや NetBIOS メッセージなど）
- ディープ パッケージ インスペクション
- スイッチテレメトリ

Cisco AI エンドポイント分析では、これらのソースから受信した情報に基づいてシステムルールが作成されます。デバイスがネットワークに参加し、デバイスがアクティブであるときに定期的にプローブを実行すると、エンドポイントのプロファイリングデータが継続的にモニタされ、更新されます。

エンドポイントから受信したプロファイリングデータにおける特定の変化は、Cisco AI エンドポイント分析で異常としてフラグが付けられます。たとえば、エンドポイントが最初に Linux デバイスとしてプロファイルされ、その後でmacOSデバイスとしてプロファイルされた場合、

これは重大度の高い異常としてフラグが付けられます。エンドポイントの [Endpoint Attribute Conflict] 列にスコアが割り当てられ、エンドポイントの全体的な信頼スコアもこの変化を反映して更新されます。

ただし、macOS のサブバージョンに変化があり、エンドポイントが新しいリリースから古いリリースにダウングレードされたように見える場合、そのような変化は優先順位の低い異常としてフラグが付けられ、対応するスコアがそれに応じて更新されます。

[Endpoint Inventory] ウィンドウで、**[Endpoint Attribute Conflict]** スコアを持つエンドポイントの MAC アドレスをクリックすると、記録されたプロファイリングデータの変化を確認できます。ここにはエンドポイントの新旧のプロファイルが表示されます。プロファイリングの変化が何らかの理由で問題ないと判断できる場合、または検出されたプロファイリングの変化に誤りがあると思われる場合は、エンドポイントの詳細情報の **[Endpoint Attribute Conflict]** エリアで対応するボタンをクリックしてスコアをリセットします。

エンドポイントの詳細情報の [Endpoint Attribute Conflict] エリアにあるトグルボタンをクリックすることにより、特定のエンドポイントに関してエンドポイント属性の競合の検出を無効にすることもできます。

影響を受けるエンドポイントが Cisco ISE に接続されている場合は、この異常に関するデータが Cisco ISE に送信されます。このデータは、Cisco ISE 管理者がポリシーを定義するために簡単に使用できるエンドポイント分析ディクショナリ属性として使用できます。

エンドポイント属性の競合の検出は、カスタムルールが適用されているエンドポイントには使用できません。

NAT モード検出

ネットワークアドレス変換（NAT）は、登録されていない IP アドレスを使用してインターネットへ接続するプライベート IP インターネットワークを可能にします。NAT は、ネットワーク全体で 1 つだけのアドレスを外部にアドバタイズするように設定できます。ネットワーク内に NAT 対応ルータがある場合、NAT ルータに接続されたエンドポイントは、特定のエンドポイントの IP アドレスまたは MAC アドレスではなくルータの IP アドレスまたは MAC アドレスによって認識されます。NAT 対応ルータに関する情報は、接続先の Cisco Catalyst 9000 シリーズ デバイスから収集されます。

NAC 対応ルータとして機能するデバイスは、不正なエンドポイントをネットワークに接続させる可能性があるため、NAT 検出が信頼スコアの計算に含まれます。NAT モード検出スコアが割り当てられているエンドポイントの場合は、[Endpoint Inventory] タブで MAC アドレスをクリックすると、スライドインウィンドウにエンドポイントの詳細情報が表示されます。エンドポイントのアイデンティティがネットワーク内の NAT 対応ルータに対応していることが確実な場合は、次の手順を実行します。

1. 詳細情報のスライドインウィンドウの [Trust Score] タブで、[NAT Mode Detection] をクリックします。
2. トグルボタンをクリックして、この特定エンドポイントの NAT 検出を無効にします。

Cisco Catalyst 9000 シリーズ デバイスに接続された同時 MAC アドレスを持つエンドポイント

同じ MAC アドレスを共有し、Cisco Catalyst 9000 シリーズ デバイスに接続されているエンドポイントを特定してください。同時 MAC アドレスを持つエンドポイントの問題は、有線環境と、有線展開およびワイヤレス展開を含むハイブリッド環境で発生します。ワイヤレス環境では、常時、特定の MAC アドレスを持つエンドポイントは 1 つしかネットワークにアクセスできないため、同時 MAC アドレスは発生しません。

Cisco AI エンドポイント分析では、同時 MAC アドレススコアをエンドポイントに割り当てることにより、同時 MAC アドレスを持つエンドポイントを特定することができます。ネットワーク内で共有 MAC アドレスを持つエンドポイントを検出するには、接続されている Cisco Catalyst 9000 シリーズ デバイスで CBAR を有効にする必要があります。

同じ MAC アドレスを持つデバイスが Cisco Catalyst 9000 シリーズ デバイスに接続すると、それらのエンドポイントは同時エンドポイントとして認識され、その MAC アドレスに低いスコアが割り当てられます。同時 MAC アドレスを持つエンドポイントは、次のデバイスに接続できます。

- 異なる VLAN から同じ Cisco Catalyst 9000 シリーズ デバイス
- 異なる Cisco Catalyst 9000 シリーズ デバイス

表 *1:* 同時 *MAC* アドレスの問題が発生する環境

展開 1	展開 2	ネットワークで同時 MAC アドレスが発生するか	この環境での同時 MAC アドレス検出のサポート
有線	有線	対応	対応
有線	ワイヤレス	対応	対応
ワイヤレス	有線	対応	対応
ワイヤレス	ワイヤレス	非対応	非対応

Cisco DNA Center リリース 2.2.3 以降では、[Endpoint Inventory] タブの [Trust Scores] ビューに [Concurrent MAC Address] 列があります。共有 MAC アドレスは異常として検出され、[Concurrent MAC Address] 列に低いスコアが割り当てられます。[MAC Address] をクリックすると、スライドインウィンドウが表示され、その MAC アドレスの詳細情報が示されます。[Concurrent MAC Address] をクリックすると、フィールドが展開され、MAC アドレスのさまざまな送信元に関する情報が表示されます。

[Concurrent MAC Address] エリアの [Network Device Name] 列には、エンドポイントが接続されている Cisco Catalyst 9000 シリーズ デバイスの名前が表示されます。[Interface] 列と [VLAN] 列

には対応する値が表示され、エンドポイントがネットワークにどのように接続されているのかを特定するために役立ちます。

Cisco ISE からのポスチャおよび認証値を使用した初期信頼スコアアセスメント

エンドポイントが Cisco ISE を介して認証されると、認証およびポスチャの詳細情報に基づいて、エンドポイントに信頼スコアがただちに割り当てられます。認証方式スコアはデフォルトで割り当てられ、このスコアを無効にすることも、このスコアに対処することもできません。[Configurations] ウィンドウからグローバルレベルで、または [Endpoint Inventory] タブで特定のエンドポイントについて、ポスチャベースのスコアを有効または無効にすることができます。認証方式およびポスチャ値に基づいて割り当てられた信頼スコアが、エンドポイントの初期信頼スコアになります。

その後、このエンドポイントで検出されたその他の異常な動作は、この初期信頼スコアに影響を与え、異常の重大度と数に基づいて信頼スコアを低下させます。

[Endpoint Inventory] タブのエンドポイントの詳細情報に表示される**認証方式**スコアは、使用される認証方式の認識されたセキュリティレベルに基づいています。たとえば、「HTTPS を介した Web 認証」、「証明書ベースの認証」、「セキュアトンネルを使用した認証」などは、高い信頼スコアを得ます。

ポスチャスコアは、接続エンドポイントがポスチャに準拠しているかどうかに基づきます。

エンドポイントの信頼スコアが認証方式スコアのみで構成されている場合、[Reset Trust Score] ボタンは非アクティブになります。認証方式以外の信頼スコアソースにスコアが表示されている場合は、リセットオプションを使用できます。

ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコア

プライバシー対策として、モバイルデバイスでは接続先の SSID ごとにランダムおよび変更 MAC アドレスを使用することが増えています。一部のデスクトップ オペレーティング システムは、ユーザーが定期的に MAC アドレスをランダム化する機能も提供しています。つまり、エンドポイントは、異なる SSID に接続するたびに異なる MAC アドレスを提示します。

Cisco AI エンドポイント分析を使用すると、Cisco ISE から「DUID」と呼ばれる（Cisco ISE では「GUID」とも呼ばれます）一意のエンドポイント識別子を受信することにより、ランダムおよび変更 MAC アドレスの問題を処理できます。Cisco AI エンドポイント分析は、MAC アドレスの代わりに、エンドポイントの識別子として DUID を使用します。Cisco ISE での GUID の割り当て方法の詳細については、Cisco ISE の管理者ガイド（リリース 3.1）を参照してください。

Cisco AI エンドポイント分析の [Overview] ウィンドウの [Endpoint MAC Randomization] ダッシュレットには、ネットワーク内のランダムおよび変更 MAC アドレスを使用しているエンドポイントの数がグラフィカルに表示されます。

Cisco ISE に接続され、DUID 情報を使用可能なエンドポイントの場合、この情報は Cisco AI エンドポイント分析にも表示されます。次の列には、Cisco AI エンドポイント分析の [Endpoint Inventory] ウィンドウで必要になる情報が表示されます。

- [DUID]：エンドポイントの DUID 値。

- [Previous MAC Addresses]：エンドポイントが以前にネットワークへの接続に使用していたランダムおよび変更 MAC アドレス。

DUID 値を使用することで、Cisco AI エンドポイント分析では、エンドポイントを確実に識別し、エンドポイントが以前に使用していたさまざまな MAC アドレスを追跡することが可能になっています。これは、ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコアも高精度であることを意味します。以前の MAC アドレスでのエンドポイントの信頼スコアは、エンドポイントが提示している現在の MAC アドレスに引き継がれ、同じエンドポイントに関して受信されたプローブデータの影響を受け続けます。

デバイスで [Private Address] 設定が有効になっている場合、このデバイスの [Is MAC Random] 列に [Yes] という値が表示されます。つまり、このデバイスは、ランダムおよび変更 MAC アドレスとして認識されます。ただし、このデバイスに関して DUID 値を使用できるかどうかは、エンドポイントが Cisco ISE を介して認証されているかどうかと、Cisco ISE でこのエンドポイントの GUID が生成されているかどうかに依存します。

オープンポートと資格情報の脆弱性を確認するためのセンサースキャン

アクティブなプローブコンテナをインストールして、ネットワーク内のエンドポイントに関する詳細情報を取得します。セキュリティ センサー スキャンを有効にすると、エンドポイントに割り当てられるトラストスコアは、開いているポートとエンドポイントのログイン情報の異常を考慮します。

センサースキャン機能は、次のスイッチでサポートされています。

- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ

（注） Cisco Catalyst 9800 シリーズ ワイヤレスコントローラは、センサースキャン機能をサポートしていません。

Cisco AI エンドポイント分析は、スイッチで利用可能なアプリケーション ホスティング機能を使用して、開いているポートと弱いログイン情報のスキャンを有効にします。

センサースキャンの有効化と監視

始める前に

- スキャン結果に基づいてエンドポイントポリシーを適用する場合は、Cisco ISE リリース 3.1 以降のリリースに接続します。
- Cisco Catalyst 9300 または 9400 シリーズ デバイスに接続します。
- スイッチが Cisco IOS XE リリース 17.7.1 以降のリリースにアップグレードされていることを確認します。

ステップ 1 Cisco DNA Center にログインします。

ステップ 2 メインメニューから **[ポリシー（Policy）]** > **[AI エンドポイント分析（AI Endpoint Analytics）]** を選択します。

ステップ 3 表示される [Overview] ウィンドウで、[Configurations] をクリックします。

ステップ 4 左ペインから、[**Trust Analytics**] を選択します。

ステップ 5 [Security Sensor] 領域には、センサース キャン機能を使用して、開いているポートと脆弱なエンドポイントのクレデンシャルを識別するための前提条件が表示されます。この領域で対応するリンクをクリックして、次のタスクを実行します。

1. Cisco Catalyst 9000 シリーズ デバイスのリリースノートで、サポートされている Cisco DNA Center および Cisco IOS-XE リリースを確認します。関連する Cisco Catalyst 9000 シリーズ デバイスのセキュリティ センサー コンテナを software.cisco.com からダウンロードします。.tar ファイルがシステムにダウンロードされます。
2. Cisco DNA Center にアプリケーション ホスティングをインストールします。手順については、アプリケーション ホスティングを参照してください。
3. Cisco DNA Center アプリケーション ホスティングウィンドウに .tar ファイルをアップロードします。[Security Sensor] 領域にアプリケーション ホスティング ウィンドウへのリンクが表示されます。
4. センサースキャンを有効にする Cisco Catalyst 9000 シリーズデバイスごとに、.tar ファイルをインストールして有効にします。

   Cisco DNA Center アプリケーションのホスティングウィンドウで、.tar ファイルを有効にした少なくとも 1 つの Cisco Catalyst 9000 シリーズ デバイスの [App Hosting Status] がアクティブであることを確認します。

ステップ 6 前の手順で説明したようにアクティブプローブコンテナをインストールして有効にした後、[Security Sensor] 領域で、Cisco AI エンドポイント分析の信頼スコア設定を構成して、Cisco ISE に接続されているエンドポイントと、アクティブなプローブアプリケーションが有効になっている Cisco Catalyst デバイスで、開いているポートと、脆弱なクレデンシャルをスキャンできます。

- [Open Port Scan] トグルボタンをクリックして、Cisco AI エンドポイント分析がポートスキャンをプロアクティブに実行して、ネットワーク上の定義済みエンドポイントで考えられる脆弱性を検出して解決できるようにします。
- [Credential Vulnerability Scan] トグルボタンをクリックして、ネットワーク上のエンドポイントが脆弱なクレデンシャルを使用している場合に、Cisco AI エンドポイント分析がプロアクティブに検出できるようにして、悪意のあるアクティビティを防止します。

ステップ 7 （任意） 開いているポートのスキャンを有効にすることを選択した場合は、[Open Port Scan] 領域の [Scan Configuration] をクリックしてスキャンを定義できます。

a) [Scan Configuration] ウィンドウの [Defined Scans] タブで、[Define Scan] ボタンをクリックします。
b) ポートのスキャンの範囲を定義できるダイアログボックスが表示されます。

- エンドポイントの登録時に各エンドポイントをスキャンするには、[On enrollment, scan all endpoints] オプションボタンを選択します。
- サブネット、プロファイル属性などにより、開いているポートのスキャンの範囲を定義するには、[Create a Custom Scan] オプションボタンを選択します。

どちらのタイプのポートのスキャンでも、許可されていないポートのリストを定義して、常に閉じておく必要があるポートを指定します。このリストにより、Cisco AI エンドポイント分析はエンドポイントの異常なポートアクティビティを認識し、低い信頼スコアを割り当てることができます。どちらのタイプのポートのスキャンでも、設定できるスキャンの最小頻度は 12 時間です。

c) [Scan Configuration] ウィンドウの [Open Ports List] タブで、スキャンする必要があるポートのタイプと範囲、または個々のポートを指定します。

d) [Scan Configuration] ウィンドウの [Unauthorized Ports] タブで、ネットワーク内の許可されていないポートをポート番号とポートタイプで定義します。Cisco AI エンドポイント分析がこれらのポートをアクティブとして検出した場合、エンドポイントには、許可されていないポートがアクティブである異常に対して低い信頼スコアが与えられます。

ステップ 8 （任意） 脆弱なクレデンシャルの検出を有効にすることを選択した場合は、[Credential Vulnerability Scan] 領域の [Scan Configuration] をクリックしてスキャンを定義できます。この機能では、SSH および TELNET プロトコルがサポートされています。

a) [Credential Vulnerability Scan] ウィンドウの [Scan] タブで、脆弱なクレデンシャルとして識別するクレデンシャルのリストを定義します。企業の要件に従って、脆弱であると見なされるユーザー名とパスワードのリストを定義します。

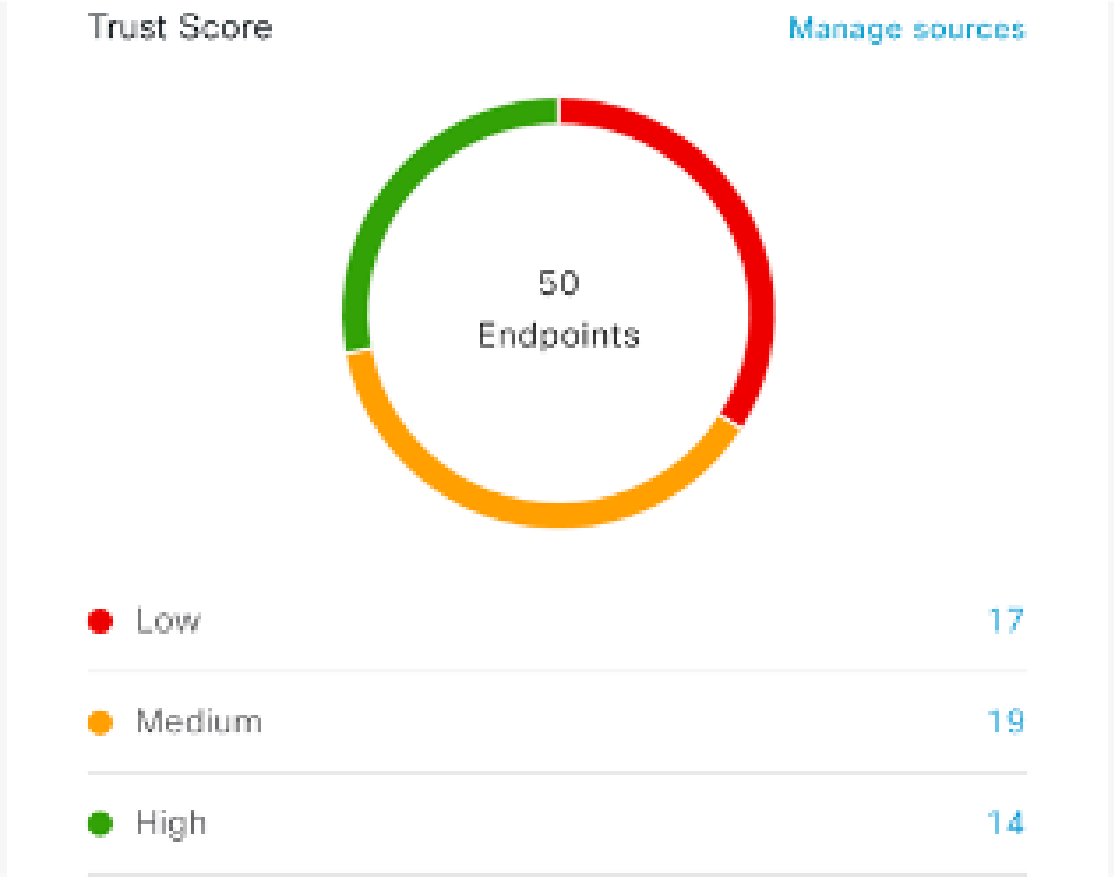
b) [Credentials] タブでは、デフォルトで、3500 を超える脆弱なクレデンシャルのデフォルトリストが利用可能です。このデフォルトリストを使用して、クレデンシャルの脆弱性スキャンを作成できます。脆弱なクレデンシャルの新しいリストを追加するには、[Create New List] をクリックします。

クレデンシャル脆弱性スキャンの設定可能な最小頻度は 12 時間です。

ステップ 9 [Security Sensor] で有効にしたスキャンでは、関連するエンドポイントがスキャンされ、開いているポートまたはクレデンシャルの確認で異常が検出された場合、これらのエンドポイントの信頼スコアがそれに応じて調整されます。[Endpoint Inventory] タブ（該当する場合）では、エンドポイントの [Trust Score] タブに、エンドポイントで開いている許可されていないポート、脆弱なユーザー名、またはその両方のリストが表示されます。

エンドポイントの信頼スコアの表示と管理

図 *4 : [Cisco AI Endpoint Analytics Overview]* タブの *[Trust Score]* ダッシュレット



Cisco DNA Center をアップグレードし、必要な信頼スコアのソースを有効にすると、Cisco AI エンドポイント分析の [Overview] タブ（メインメニュー > **[Policy]** > **[AI Endpoint Analytics]**）に [Trust Scores] ダッシュレットが表示されます。このダッシュレットには、次の情報が含まれます。

- 信頼スコアが割り当てられているエンドポイントの総数。
- 信頼スコアが低、中、および高のエンドポイントの数に関するドーナツグラフおよびリスト。

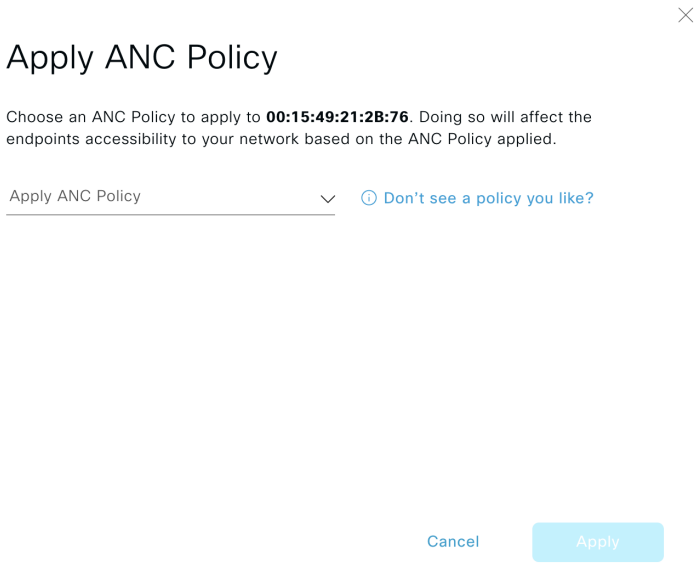
信頼スコアカテゴリのエンドポイントの詳細を表示するには、[Trust Scores] ダッシュレットでエンドポイント数をクリックします。[Endpoint Inventory] タブの [Trust Score] ビューが、適切なフィルタが適用されて表示されます。

次の 2 つの方法で信頼スコアを持つエンドポイントを表示できます。

- [Trust Score] タブで、[Endpoints] タブを選択して、信頼スコアが割り当てられているすべてのエンドポイントを表示します。
- [Endpoint Inventory] タブで、表示される警告メッセージの [View endpoints in Trust Score View] をクリックすると、低スコアと中スコアのエンドポイントが表示されます。

信頼スコアのあるエンドポイントでは、次のアクションを実行できます。

- **ANC ポリシーの適用**

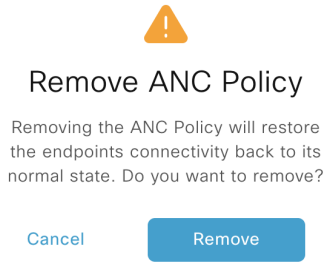


[Apply ANC Policy] ボタンをクリックして、エンドポイントに適用する ANC ポリシーを選択します。ネットワークへのエンドポイントのアクセスは、ポリシーに応じて変更されます。ANC ポリシーは Cisco ISE からインポートされ、表示されるポップアップウィンドウのドロップダウンリストに表示されます。

- **ANC ポリシーの置換**

[Change ANC Policy] ボタンをクリックして、エンドポイントの既存の ANC ポリシーを別の ANC ポリシーに置き換えます。表示されるポップアップウィンドウで、[Change ANC Policy] ドロップダウンリストから適用する新しいポリシーを選択します。

- **ANC ポリシーの削除**



適用された ANC ポリシーをエンドポイントから削除するには、[Remove ANC Policy] ボタンをクリックします。表示されるポップアップウィンドウで、[Remove] をクリックします。これにより、エンドポイントに適用された修復ポリシーが削除され、エンドポイントがネットワークに正常に接続できるようになります。

- **信頼スコアのリセット**

図 *5 : ANC* ポリシーを使用しないエンドポイントの信頼スコアのリセット

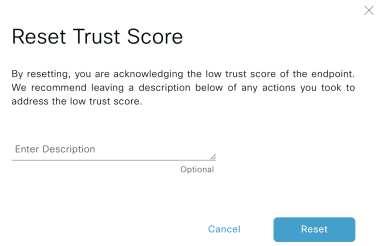
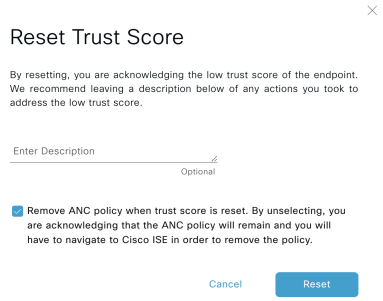


図 *6 : ANC* ポリシーを使用したエンドポイントの信頼スコアのリセット



信頼スコアインベントリからエンドポイントを削除するには、[Reset Trust Score] ボタンをクリックします。表示されるポップアップウィンドウで、[Reset] をクリックします。

ANC ポリシーの適用後にエンドポイントに対してこのオプションを選択した場合、このエンドポイントは信頼スコアインベントリに再度表示されません。この場合、このようなエンドポイントの ANC ポリシーを変更するには、Cisco ISE からポリシーを削除する必要があります。

ANC ポリシーを適用せずにエンドポイントのスコアをリセットした場合、信頼スコアデータの次回の自動更新時に、エンドポイントが信頼スコアインベントリに再度表示されることがあります。

各アクションのボタンは、[Endpoint Inventory] タブの 2 つの場所に表示されます。アクションは、単一のエンドポイントまたは複数のエンドポイントで実行できます。

- **単一エンドポイントの信頼スコアの管理**

図 *7 : ANC* ポリシーを使用しないエンドポイントの信頼スコアオプション

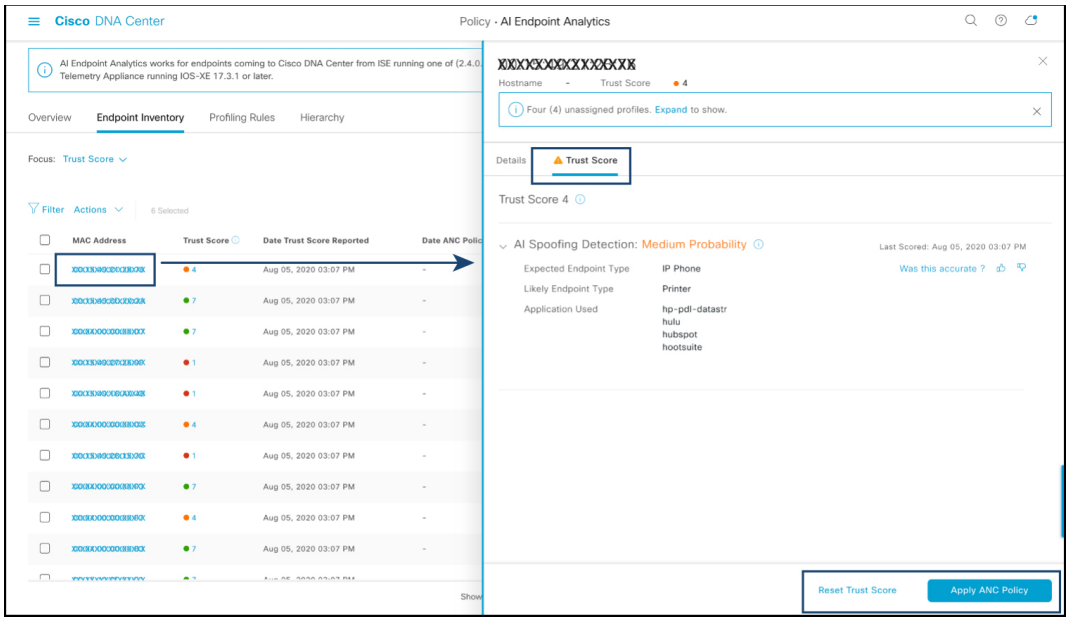
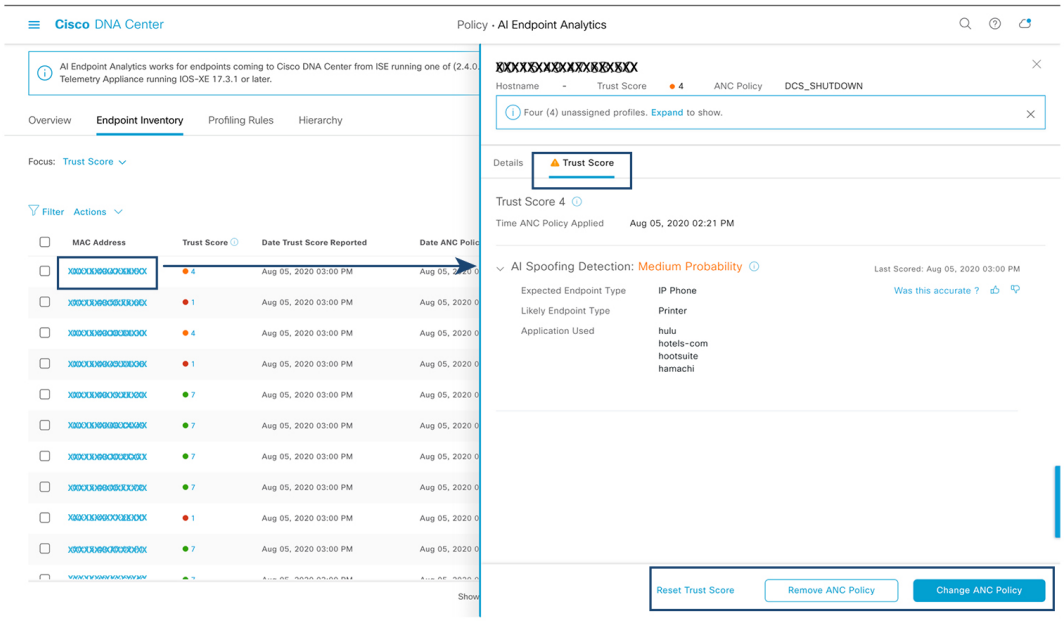


図 *8 : ANC* ポリシーを使用したエンドポイントの信頼スコアオプション



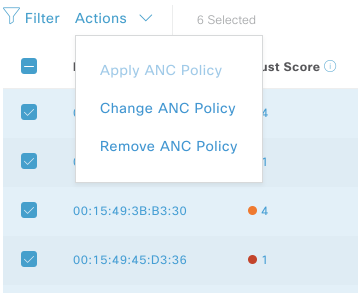
信頼スコアのあるエンドポイントのリストから、管理するエンドポイントの MAC アドレスをクリックします。表示されるエンドポイントの詳細ペインで、[Trust Score] タブをクリックします。

ここには、**[Expected Endpoint Type]** の値が表示されます。[Applications Used] フィールドには、エンドポイントで使用されるアプリケーションが一覧表示されます。

このペインには、ANC ポリシーの受け入れと削除のワークフローを開始し、信頼スコアをリセットするためのボタンがあります。目的のタスクのボタンをクリックします。

または、[Endpoint Inventory] ウィンドウで個々のエンドポイントのチェックボックスをオンにし、[Actions] をクリックして、ドロップダウンリストから必要なオプションを選択します。

- **複数のエンドポイントの信頼スコアの管理**



[Endpoint Inventory] タブで、特定のアクションを実行する必要があるすべてのエンドポイントのチェックボックスをオンにします。[Actions] をクリックし、ドロップダウンリストから必要なアクションを選択します。

エンドポイント スプーフィングの制御

同時 MAC アドレス検出とは、同じ MAC アドレスを持つ 2 つのエンドポイントがネットワークにアクセスしてトラフィックを生成していることが検出されることを意味します。次に、実際のエンドポイントとスプーフィングされたエンドポイントを区別し、スプーフィングされたエンドポイントに対して必要な修復アクションを実行することが不可欠になります。

コントロール エンドポイント スプーフィング機能は、エンドポイントの MAC アドレス以外のネットワーク情報を提供することにより、詳細なポリシーコントロールを提供します。ネットワーク情報には、サイト情報、ネットワークデバイスの IP アドレス、ネットワークデバイスポート、最初に承認されたタイムスタンプ、最後に承認されたタイムスタンプ、およびエンドポイントがネットワークで使用可能であった期間が含まれます。従来のように MAC アドレスでエントリを区別するか、MAC アドレスと提供されたネットワーク情報の両方を使用してエントリを区別するかを選択できます。MAC アドレスと接続（ネットワーク情報）で区別することを選択した場合、スプーフィングされたエンドポイントを検出するための選択が自動的に行われます。自動選択を使用するか、スプーフィングされたエンドポイントであると思われるものを選択して、そのエンドポイントに適切な修復アクションを適用することができます。使用可能な修復アクションは、Cisco ISE で設定された適応型ネットワーク制御（ANC）ポリシーです。

これはポリシーを適用する詳細な方法であるため、**[Operations] > [Adaptive Network Control] > [Endpoint Assignment]** にこのポリシーのリストは表示されません。

同時MACアドレス検出がなく、NATモード検出のみのエンドポイントの場合、ANCポリシーは「エンドポイントの信頼スコアの表示と管理 （39 ページ）」で説明されているように適用

されます。このようなシナリオでは、エンドポイントは Cisco ISE の [Endpoint Assignment] の下にリストされます。

同時 MAC アドレスと NAT モードの両方の検出があるエンドポイントの場合、詳細なポリシー制御が優先されます。したがって、[Apply ANC Policy] をクリックすると、エントリを区別する 2 つのオプションがある新しい [Apply ANC Policy] ウィンドウが表示されます。

また、いつでもエンドポイントの ANC ポリシーを変更することを選択できます。ANC ポリシーの変更中に、ANC ポリシーを適用できる複数のエントリを選択するオプションがあります。

（注） 修復アクションとして [Shutdown] を選択し、アクションを変更する場合、エンドポイントはアクションの変更後に自動的に再起動されません。エンドポイントが接続されているスイッチのインターフェイスを手動でオンにする必要があります。

ANC ポリシーはいつでも削除できます。

始める前に

ダイナミック認証を、ネットワークデバイスで設定する必要があります。Cisco DNA Center から AAA 設定を使用してネットワークデバイスをプロビジョニングすることをお勧めします。

ステップ 1 Cisco DNA Center の GUI から、**[Policy]** > **[AI Endpoint Analytics]** > **[Endpoint Inventory]** > **[View endpoints in trust score view]** の順に選択します。

ステップ 2 確認するエンドポイントをクリックして、ANC ポリシーを適用します。

ステップ 3 [Trust Score] > [Concurrent MAC Address] を選択します。

ステップ 4 [Apply ANC Policy] をクリックします。

ステップ 5 [Apply ANC Policy] ウィンドウで、[Based on MAC address] または [Based on MAC address and connectivity] を選択します。

ステップ 6 [Apply ANC Policy] ドロップダウンリストから適切な修復アクションを選択します。

ステップ 7 [Apply ANC Policy] をクリックします。

このタスクを完了した後、そのエンドポイントの [Trust Score] ビューに戻ると、ANC ポリシー名と、ポリシーが適用されたネットワークデバイスの IP アドレスと、ANC ポリシーが適用された時刻を確認できます。

設定を確認するには、Cisco ISE の GUI で、**[Operation]** > **[RADIUS]** > **[Live logs]** の順に選択します。[Identity] 列をエンドポイントの MAC アドレスでフィルタリングできます。

このエンドポイントの Cisco ISE から開始された CoA アクションのエントリが一覧表示されます。詳細を確認すると、エンドポイントに適用した ANC ポリシーが [CoA Reason] に表示されます。

プロファイリングルール

Cisco AI エンドポイント分析のプロファイリングルールを使用すると、共通の属性を組み合わせてエンドポイントをグループ化できます。これらの属性により、エンドポイントタイプ、OS タイプ、ハードウェアモデル、およびハードウェア製造元でエンドポイントを識別できます。プロファイリングルールを使用すると、多くのエンドポイントを簡単に管理できます。

Cisco AI エンドポイント分析は、DPI、メディアプロトコル、医療業界のプロトコルなどを介してネットワークデバイスからプロファイリングデータを受信します。Cisco ISE からのプロファイリングデータは、pxGrid を介して通信されます。これらのプロファイリング属性をデバイスディクショナリで使用してプロファイルルールを作成できます。

プロファイリングルールは、Cisco AI エンドポイント分析の [Profiling Rules] タブで確認できます。このタブの下に表示されるテーブルで、[Rule Name] エントリをクリックすると、割り当てられたプロファイルと使用される属性が表示されます。

Cisco AI エンドポイント分析でエンドポイントをプロファイリングするために使用されるプロファイリングルールは次のとおりです。

- システムルール
- シスコの規則
- Cisco AI ルール

ルールの優先順位付け

Cisco AI エンドポイント分析のプロファイリングルールには優先順位があります。プロファイリングルールの実行は、このルールの優先順位に従って、精度の高いエンドポイントをプロファイリングします。

Cisco AI エンドポイント分析ではユーザー入力がプライマリであるため、プロファイリングルールの優先順位は次のようになります。

- 管理者が作成した静的プロファイル（たとえば、[Register Endpoints] オプションを使用して追加したプロファイル）。
- 管理者が作成したカスタムルール。
- デフォルトで使用可能なシスコ提供のシステムルール。
- 機械学習対応のスマートグループ化ワークフローによって自動生成されたルール。

ルールに設定された優先順位を表示するには、[Profiling Rules] ウィンドウで [Rule priorityitization] をクリックします。

登録済みのエンドポイントは、さまざまなプロファイリングラベルの複数の Cisco AI エンドポイント分析ルールによってプロファイリングできます。次の表に、2 つのエンドポイントに対するプロファイリングルールの設計を示します。

エンドポイント 1	エンドポイント 2
システムルールによってプロファイリングされたハードウェアモデル Cisco AI ルールによってプロファイリングされた OS タイプ カスタムルールによってプロファイリングされたハードウェア製造元	システムルールによってプロファイリングされたハードウェアモデル カスタムルールによってプロファイリングされたハードウェアモデル Cisco AI ルールによってプロファイリングされたハードウェアモデル

エンドポイント 2 のルール優先順位では、カスタムルールが他のルールよりも優先されます。エンドポイント 2 のハードウェアモデルラベルは、カスタムルールによってプロファイリングされます。

エンドポイント 1 の場合、ルールごとに異なるプロファイルラベルが定義され、それに応じて各ラベルがプロファイリングされます。

プロファイリングルールのフィルタ処理

ステップ 1 [Profiling Rules] ウィンドウで、[Filter] をクリックします。

ステップ 2 [Rule Name] フィールドに、名前を入力します。

ステップ 3 対応するドロップダウンリストからエンドポイント属性の値を選択して、一連のエンドポイントをフィルタ処理します。

ステップ 4 [Apply] をクリックします。

更新されたプロファイリングルールの表示

ステップ 1 [Endpoint Inventory] ウィンドウに移動します。

ステップ 2 エンドポイントの MAC アドレスの横にあるチェックボックスをクリックして、エンドポイントのプロファイリングの詳細を表示します。

ステップ 3 プロファイルラベルの横にある情報アイコンをクリックし、ルール名をクリックして、割り当てられたプロファイルと属性の詳細を表示します。

システムルール

Cisco AI エンドポイント分析には、エンドポイントをプロファイリングするためのシステムルールと呼ばれる事前定義済みのルールが用意されています。Cisco AI エンドポイント分析を導入すると、特定のルールを設定することなく、エンドポイントのゼロデイ可視性を実現できます。

新しくオンボーディングされたエンドポイントは、デフォルトでシステムルールを使用してプロファイリングされます。

ネットワークデバイスは、Cisco DNA Center の **[Provision]** > **[Network Devices]** > **[Inventory]** ウィンドウで管理されます。

これらのネットワークデバイスは、システムルールによってプロファイリングされ、Cisco AI エンドポイント分析の [Endpoint Inventory] ウィンドウには表示されません。ただし、カスタムルールでプロファイリングされたエンドポイントは、カスタムルールがネットワークデバイスを [Device Type] として作成されるため表示できます。

エンドポイント プロファイリング用の自動システムルール更新

Cisco AI エンドポイント分析でエンドポイントプロファイリングに使用されるシステムルールは、プロファイリングの精度を高めるために定期的に更新されます。シスコからのエンドポイント プロファイリング システム ルールの更新を受信するように自動更新をスケジュールします。Cisco DNA Center が設定された時間に更新を受信し、変更内容が Cisco AI エンドポイント分析に適用されます。[Profiling Rules] ウィンドウ（**[Policy]** > **[AI Endpoint Analytics]** > **[Profiling Rules]**）で、エンドポイントプロファイルの変更の詳細を確認し、システムルールの更新を承認または拒否します。

承認されたシステムルールの更新によってエンドポイントのハードウェアモデルの値が変更された場合、[Endpoint Inventory] タブでエンドポイントの詳細を表示すると、[Hardware Model] フィールドにシステムルールの更新の名前があります。

始める前に

NBAR クラウドを設定し、有効にします。「NBAR クラウドコネクタの設定」を参照してください。

NBAR クラウドのステータスを確認するには、**[Policy]** > **[AI Endpoint Analytics]** > **[Overview]** の順に選択し、[Configuration] をクリックします。

ステップ 1 メインメニューから、**[System]** > **[Settings]** > **[Cisco Accounts]** > **[Profile Rule Settings]** の順に選択します。

[Schedule Automatic Updates] エリアの [Enabled] トグルボタンは、デフォルトでアクティブに設定されています。

ステップ 2 更新をスケジュールする曜日のボタンをクリックします。複数の日を選択できます。次に、[Time Slot] テキストフィールドを使用して、更新の時間を選択します。Cisco DNA Center によって更新が受信されるまでに 30 分かかります。2 番目のタイムスロット領域は編集できず、スケジュールされた更新が完了すると予想される時間が表示されます。

ステップ 3 Cisco DNA Center がシステムルールの更新を受信すると、[Profiling Rules] ウィンドウ（**[Policy]** > **[AI Endpoint Analytics]** > **[Profiling Rules]**）に通知が表示されます。ダイアログボックスで [Expand] をクリックすると、次の通知が表示されます。

最新バージョン（最新バージョンの名前）に更新され、最近のシスコプロファイリングルールによって一部のエンドポイントのプロファイルが変更されています。更新を確認します。

[Review Update] をクリックします。

ステップ 4 [Endpoint Profile Update Review] ダイアログボックスが表示されます。このダイアログボックスには、現在適用されている安定版の更新、受信した最新の更新などの情報が表示されます。また、クリックして、関連するエンドポイントプロファイルの更新を表示できる次のセクションも含まれています。

1. [Major Updates]：Linux エンドポイントとして現在記録されている Windows エンドポイントなど、プロファイルに大きな変更があったエンドポイントが一覧表示されます。
2. [Minor Updates]：Windows OS の更新バージョンなど、プロファイルにマイナーな変更があったエンドポイントが一覧表示されます。
3. [Newly Profiled]：以前にプロファイル解除され、現在プロファイル情報が割り当てられているエンドポイントが一覧表示されます。

ステップ 5 エンドポイントプロファイルの変更を確認した後、プロファイルの更新を受け入れるには、[Endpoint Profile Update Review] ダイアログボックスで [Mark As Approved Version] をクリックします。エンドポイントプロファイルの変更に同意しない場合は、[Rollback] をクリックします。

ロールバックを選択する場合、対応するオプションをクリックして、最後の実行バージョンにロールバックするか、最後に承認されたバージョンにロールバックするかを選択する必要があります。

また、[AI Endpoint Analytics] > [Overview] > [Configuration] ウィンドウから、承認およびロールバックアクションを実行することもできます。

ステップ 6 [x] をクリックして、ダイアログボックスを閉じます。

シスコの規則

システムルールのほかに、エンドポイント属性を組み合わせて、エンドポイントをプロファイリングするためのカスタムルールを作成することもできます。カスタムルールは、Cisco AI エンドポイント分析の他のエンドポイント プロファイリング ルールよりも優先されます。

プロファイリングルールの論理と条件

[Endpoint Inventory] ウィンドウでカスタム プロファイリング ルールを作成できます。カスタム プロファイリングルールを作成するには、エンドポイントの属性と値に基づいて論理条件を作成する必要があります。これらの属性は、ネットワークプローブデータから収集され、[Attribute Glossary] ウィンドウで使用できる分類属性とは異なります。

値は、エンドポイントグループを一意に識別するユーザー入力です。次の演算子を使用して、属性と値から正規表現が作成されます。

演算子	説明
次の文字列を含む	属性は、選択した値を持ちます。
イコール	属性は、選択した値に厳密にマッピングされます。

演算子	説明
一致する	属性は、選択した値の正規表現パターンと一致する必要があります。
Starts With	属性は、選択した値で始まる必要があります。

（注） Contains、Equals、および Starts With は、大文字と小文字を区別する演算子です。大文字と小文字を区別しない値の場合は、Matches 演算子を使用します。

論理（[AND] および [OR]）によってこれらの条件をさらに組み合わせて、ネストされたルールを作成できます。

論理条件の作成と編集

論理条件を作成するには、次の手順に従います。

ステップ 1 [Choose Attribute Conditions] ウィンドウで、更新する [Attribute] の横にあるチェックボックスをオンにします。

ステップ 2 [Operator] ドロップダウンリストからオプションを選択します。

ステップ 3 [Value] フィールドに値を入力します。

ステップ 4 [Next] をクリックします。

ステップ 5 表示される [Add Logic to Conditions] ウィンドウで、条件間の [AND] ロジックまたは [OR] ロジックをドラッグアンドドロップして、カスタムルールの条件の論理シーケンスを作成します。

（注） 条件の横にある垂直省略記号を使用して、[Add Logical Conditions] ウィンドウで属性条件を追加または編集することもできます。

ステップ 6 [Next] をクリックします。

カスタムルールの作成

ステップ 1 [Endpoint Inventory] ウィンドウで、プロファイリングするエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Profile with Custom Rules] を選択します。

ステップ 3 表示される [Name Rule and Type] ウィンドウの [Rule Name] フィールドにルールの名前を入力し、[Profile Label] ドロップダウンリストからラベルを選択します。

[Profile Label] ドロップダウンリストから選択した内容に応じて、対応するフィールドが表示され、その名前は動的に更新されます。たとえば、[Endpoint Type] を選択すると、[Endpoint Type] フィールドが表示されます。

ステップ 4 表示される新しいフィールドに値を入力します。情報の入力を開始すると、一致するオプションが表示されます。要件に一致するオプションがあれば、そのオプションを選択します。なければ、タイプ名全体を入力します。

ステップ 5 [Next] をクリックします。

ステップ 6 表示される [Choose Attribute Conditions] ウィンドウで、論理条件を作成します。

詳細については、「プロファイリングルールの論理と条件」を参照してください。

ステップ 7 [Review Rule] ウィンドウで、このカスタムルールでプロファイリングされるエンドポイントのリストを確認します。

ステップ 8 [Next] をクリックします。

ステップ 9 [Profiles] をクリックします。

カスタムルールの編集

ステップ 1 [Profiling Rules] ウィンドウで、編集する管理ルールの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Edit] を選択します。

ステップ 3 表示される [Edit] ウィンドウの [Rule Name] フィールドにルールの名前を入力し、ルールの作成時に選択した [Profile Label] に基づいてプロファイルの詳細を選択または入力します。

ステップ 4 [Logic and Conditions] セクションで、垂直省略記号をクリックし、[Edit] を選択して、プロファイリングルールの論理と条件を更新します。詳細については、「プロファイリングルールの論理と条件」を参照してください。

ステップ 5 **[次へ (Next)]** をクリックします。

ステップ 6 **[適用 (Apply)]** をクリックします。
既存のルールが新しいプロファイリングの詳細で更新されると、そのルールでプロファイリングされたエンドポイントが新しいプロファイリングの詳細で更新されます。

カスタムルールの削除

ステップ 1 [Profiling Rules] ウィンドウで、削除するルールの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Delete] を選択します。

次のメッセージが表示されます。

「Do you really want to delete the selected Rule(s)?」

ステップ 3 [Yes] をクリックして、Cisco AI エンドポイント分析からルールを完全に削除します。
カスタムルールが削除されると、このルールでプロファイリングされたエンドポイントがシステムルールで更新されます。

展開間での API を使用したカスタム プロファイリング ルールのエクスポートとインポート

Cisco DNA Center には、カスタム プロファイリング ルールのインポート、エクスポート、編集、および削除に使用できる Cisco AI エンドポイント分析 API が含まれています。

Cisco AI エンドポイント分析 API バンドルを有効にするには、次の手順を実行します。

1. メニューアイコン（☰）をクリックして、**[Platform]** > **[Manage]** > **[Bundles]** の順に選択します。
2. [AI Endpoint Analytics] という名前のバンドルを見つけ、[Enable] をクリックします。
3. [Status] 列の値が [Disabled] から [Active] に更新され、API のリストが表示されます。各 API の予期される要求および応答ペイロードを確認することもできます。
4. API バンドルを有効にすると、Cisco AI エンドポイント分析 API が Cisco DNA Center 開発者用ツールキットに追加されます。その後、[Developer Toolkit] ウィンドウ（**[Platform]** > **[Developer Toolkit]**）から API にアクセスできます。

[Bundles] ウィンドウと [Developer Toolkit] ウィンドウの両方から、次の操作を実行できます。

- コードプレビューを生成して、API を実行する別のツールで使用できる API コードを表示します。
- [Try It] をクリックして、Cisco DNA Center GUI から API を実行します。JSON 応答を受信し、それを任意のテキストエディタにコピーアンドペーストして作業を続行できます。

スマートグループ化のための Cisco AI ルール

Cisco AI エンドポイント分析の AI アルゴリズムは、展開全体のエンドポイント プロファイリング ラベルとグループに関するデータを分析し、スマートなプロファイリングルールの提案を提供します。

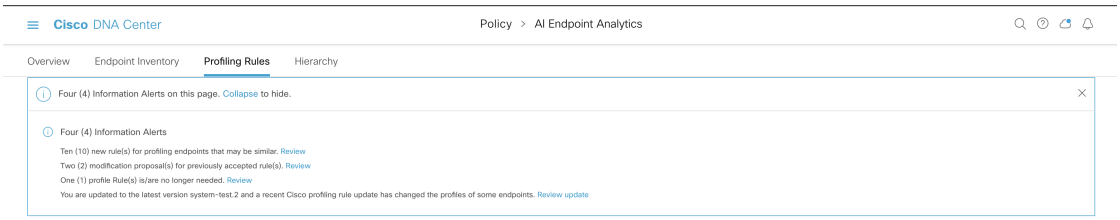
Cisco AI エンドポイント分析の [Overview] タブの [AI Proposal] ダッシュレットには、エンドポイントクラスタからの学習に基づいた次のルールの提案が表示されます。

- ネットワーク内のプロファイルされていない、またはラベル付けされていないエンドポイントの新しいプロファイリングルール。詳細については、ネットワーク内の類似のエンドポイントに対する新しいプロファイリングの提案 （53 ページ）を参照してください。
- AI アルゴリズムが展開全体で学習したエンドポイント プロファイリング データの変更に基づいた、ネットワーク内の既存のプロファイリングルールの変更提案。詳細については、エンドポイント プロファイリング ルールに対するスマート変更の提案 （56 ページ）を参照してください。
- AI アルゴリズムが展開全体で学習したエンドポイント プロファイリング データの変更に基づいた、不適切なラベルを含むプロファイリングルールの削除提案。ルールの削除を受け入れると、影響を受けるエンドポイントから不適切なプロファイリングラベルが削除さ

れます。エンドポイントのプロファイリングタイプの値は空になるか、以前に割り当てられたラベルに戻ります。詳細については、プロファイリングルールを削除するためのスマート提案 （58 ページ）を参照してください。

また、ワークフローを開始して、Cisco AI エンドポイント分析の [Profiling Rules] タブから、エンドポイントプロファイリングルールへの変更の提案を確認および適用することもできます。[Profiling Rules] は、情報アラートを含むダイアログボックスを表示します。情報アラートのダイアログボックスで、[Expand] をクリックして、エンドポイント プロファイリング ルールの変更に関する利用可能な提案を表示します。調査する情報アラートの横にある [Review] をクリックして、対応するワークフローを開始します。

図 *9 : [Profiling Rules]* タブの情報アラート

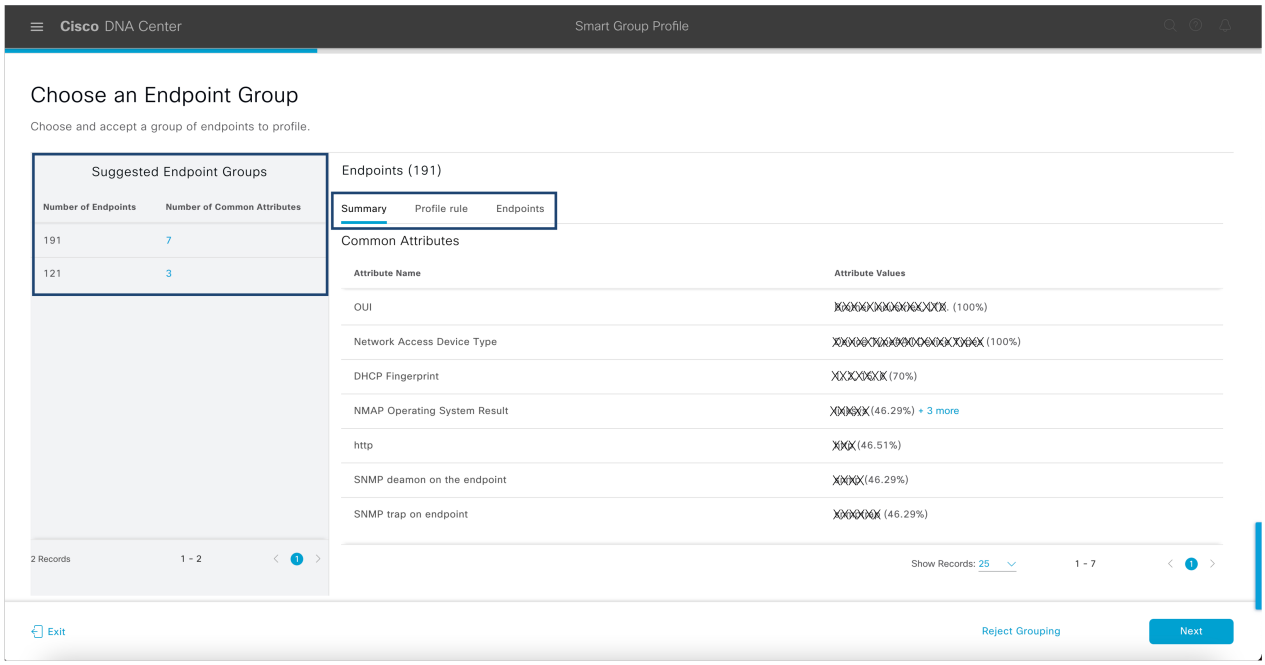


ネットワーク内の類似のエンドポイントに対する新しいプロファイリングの提案

ステップ 1 [AI Proposals] ダッシュレットで、[New rule(s) for profiling endpoints that may be similar] の横にある [Review] ボタンをクリックします。
[Smart Group Profile] ワークフローが起動されます。

ステップ 2 表示される [Choose an Endpoint Group] ウィンドウには、左側のペインに新しいプロファイリングルールの提案のリストが含まれています。リスト内のエントリをクリックして、右側のペインにプロファイリングルールの詳細を表示します。

図 *10 : [Smart Group Profile]* ワークフローの *[Choose an Endpoint Group]* ウィンドウ

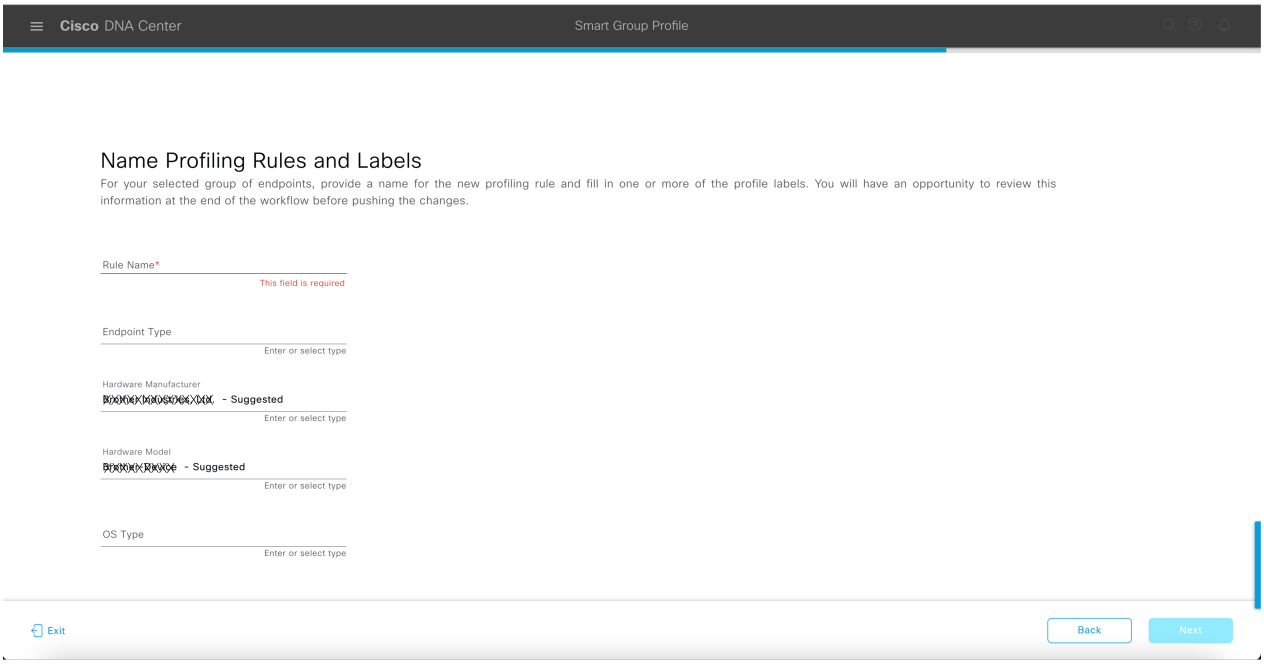


右側のペインには、[Summary]、[Profile Rule]、および [Endpoints] タブが含まれており、提案されたプロファイリングルールの詳細を簡単に表示できます。

ステップ 3 [Next] をクリックして、推奨されるプロファイリングルールを作成します。

ステップ 4 表示される [Name Profiling Rules and Labels] ウィンドウの [Rule Name] フィールドにルールの名前を入力します。

図 *11 : [Smart Group Profile]* ワークフローの *[Name Profiling Rules and Labels]* ウィンドウ



ステップ 5 次の 1 つ以上のフィールドに、必要な値を入力します。次の手順に進むには、少なくとも 1 つのフィールドに値を入力する必要があります。

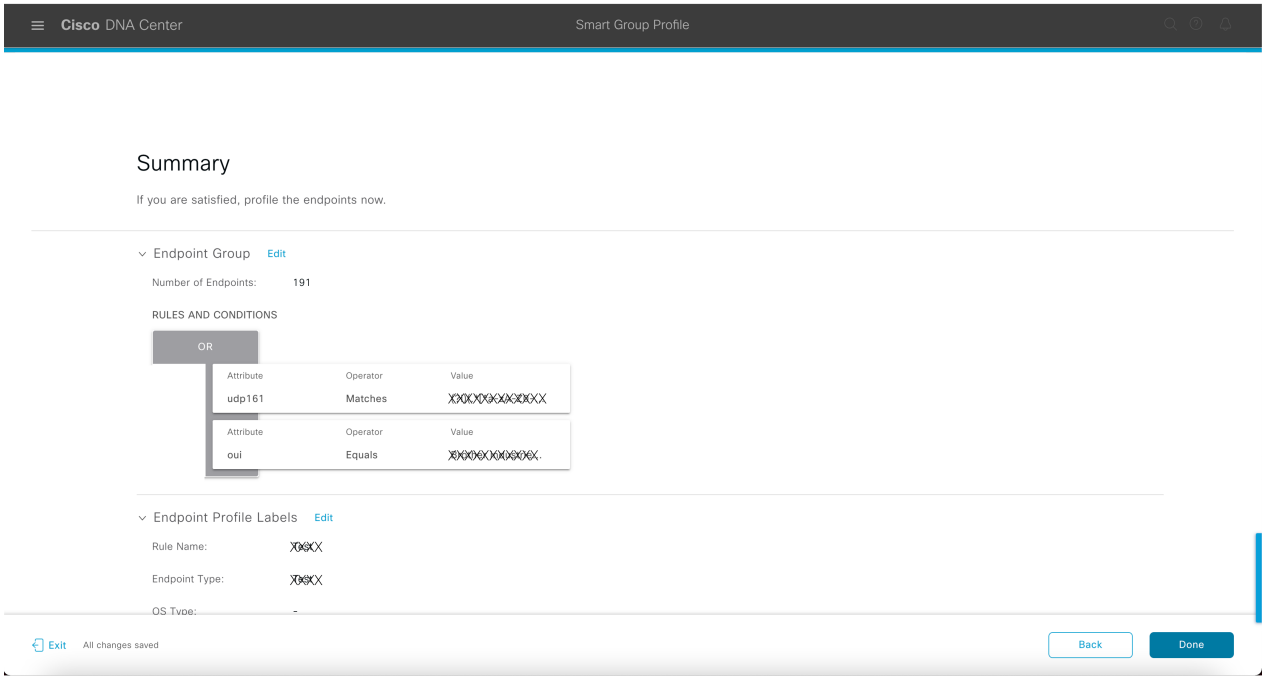
- **エンドポイント タイプ**
- **Hardware Manufacturer**
- **ハードウェア モデル**
- **OS Type**

AI アルゴリズムがエンドポイントのプロファイリングラベルを識別した場合、そのラベルは対応するフィールドに提案として表示されます。提案されたラベルで続行するか、別のラベルを選択するかを選択できます。

ステップ 6 [次へ（**Next**）] をクリックして続行します。

ステップ 7 [Summary] ウィンドウで、プロファイリングルールの詳細を確認します。変更するには、[Edit] をクリックします。

図 *12 : [Smart Group Profile]* ワークフローの *[Summary]* ウィンドウ



ステップ 8 プロファイリングルールを作成するには、[Done] をクリックします。

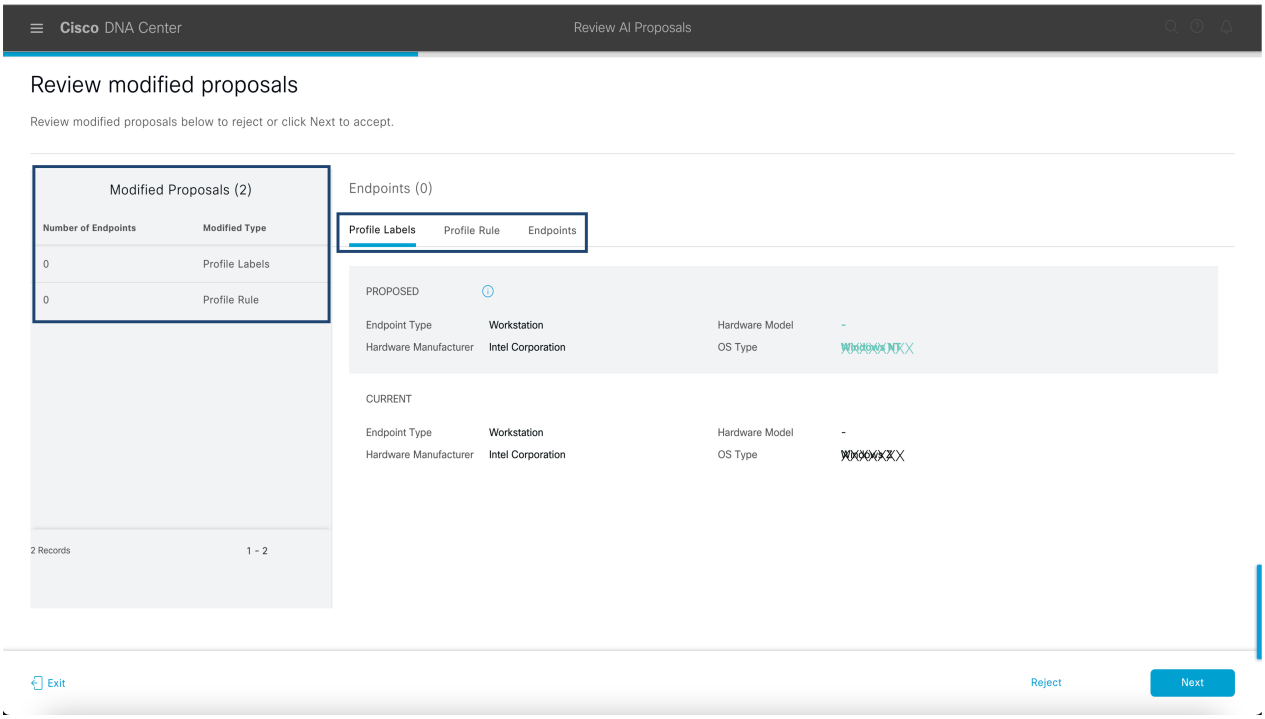
エンドポイント プロファイリング ルールに対するスマート変更の提案

ステップ 1 [AI Proposals] ダッシュレットで、[Modification proposal(s) for previously accepted rule(s)] の横にある [Review] ボタンをクリックします。

[Smart Group Profile] ワークフローが起動されます。

ステップ 2 表示される [Review modified proposals] ウィンドウには、既存のプロファイリングルールの変更提案のリストが含まれています。リスト内のエントリをクリックして、右側のペインに変更提案の詳細を表示します。

図 *13 : Review AI Proposals]* ワークフローの *[Review Modified Proposals]* ウィンドウ

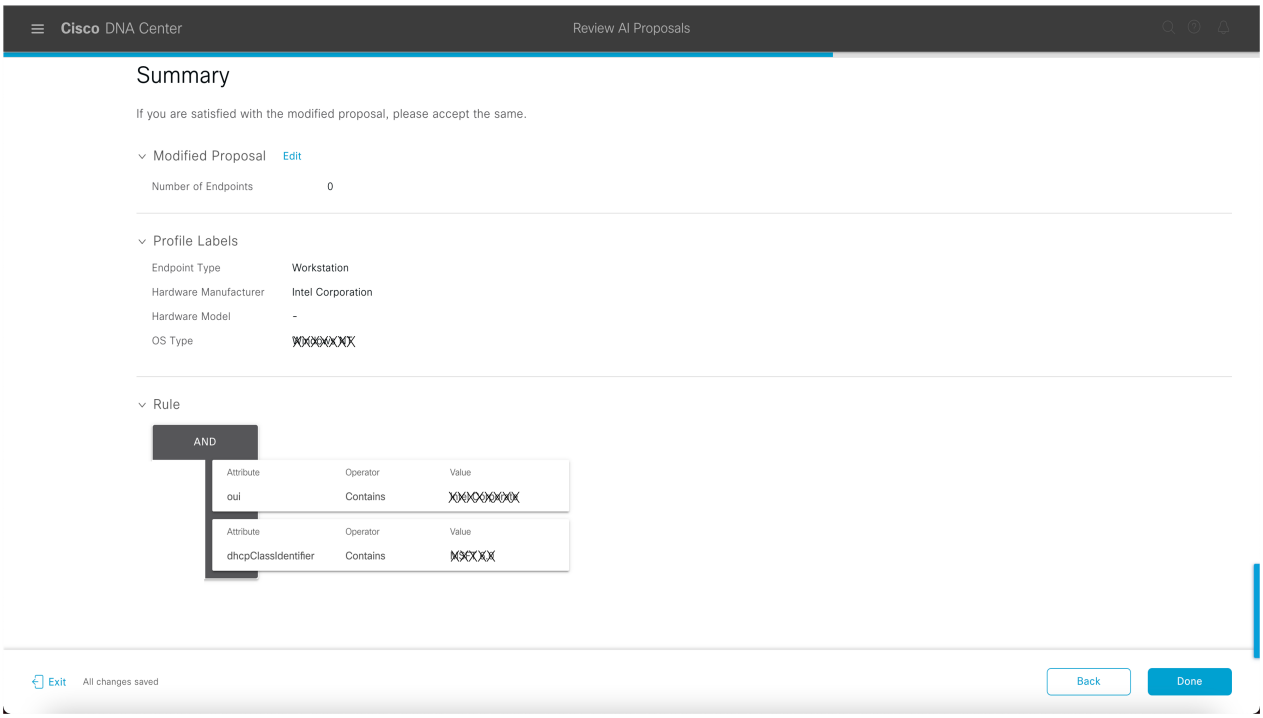


右側のペインには、[Profile Labels]、[Profile Rule]、および [Endpoints] タブが含まれており、提案された変更済みプロファイリングルールの詳細を簡単に表示できます。

ステップ 3 [Next] をクリックして、プロファイリングルールを提案どおりに更新します。

ステップ 4 [Summary] ウィンドウで、プロファイリングルールの詳細を確認します。変更するには、[Edit] をクリックします。

図 *14 : [Review AI Proposals]* ワークフローの *[Summary]* ウィンドウ



ステップ 5 プロファイリングルールを更新するには、[Done] をクリックします。

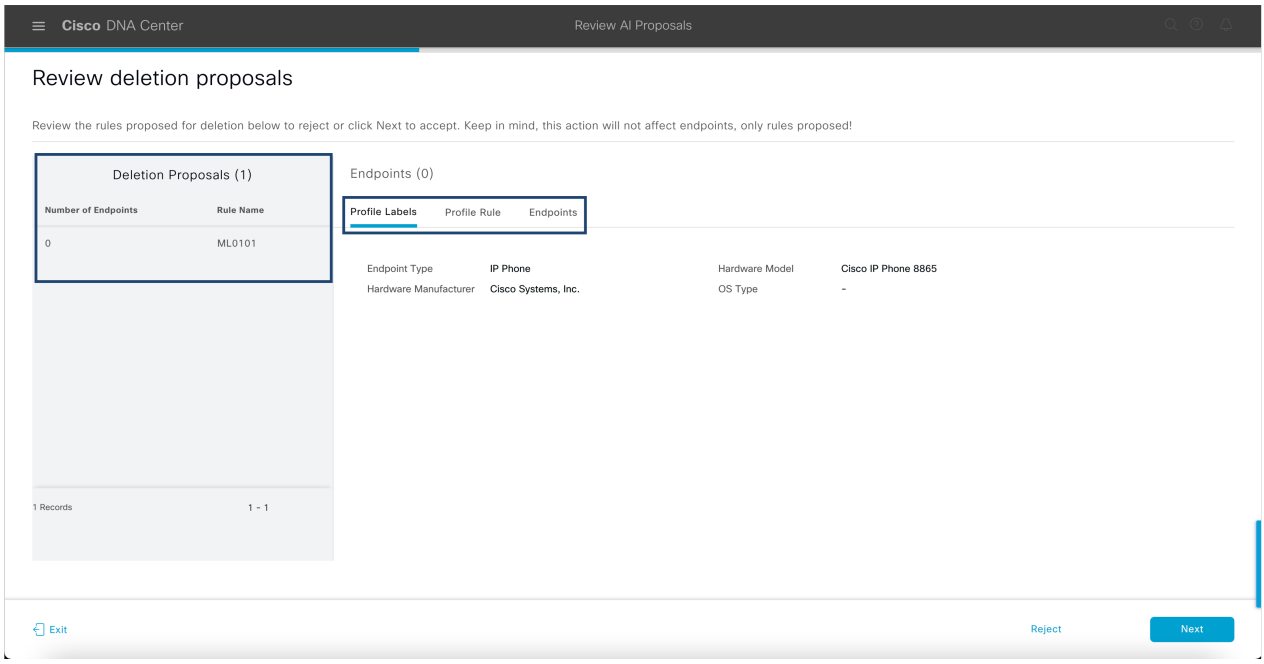
プロファイリングルールを削除するためのスマート提案

ステップ 1 [AI Proposals] ダッシュレットで、[Profiling Rules(s) is/are no longer needed] の横にある [Review] ボタンをクリックします。

[Review AI Proposals]ワークフローが開始されます。

ステップ 2 表示される [Review deletion proposals] ウィンドウには、既存のプロファイリングルールの削除提案のリストが含まれています。リスト内のエントリをクリックして、右側のペインに削除提案の詳細を表示します。

図 *15 : [Review AI Proposals]* ワークフローの *[Review Deletion Proposals]* ウィンドウ

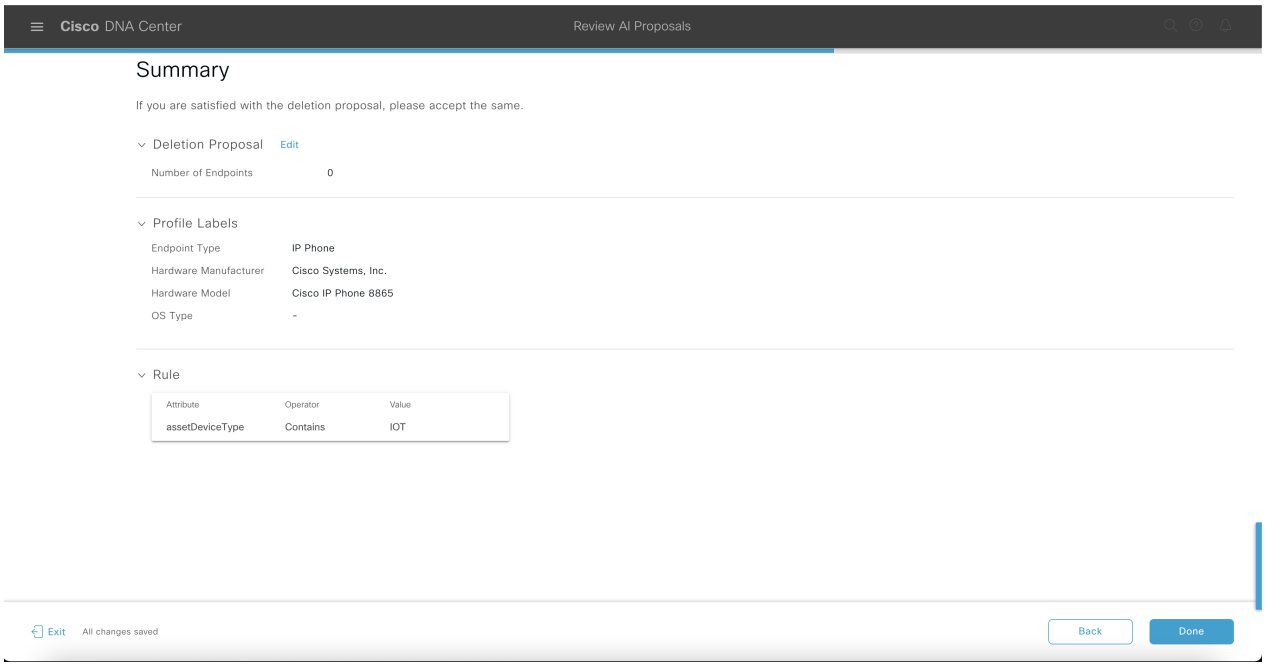


右側のペインには、[Profile Labels]、[Profile Rule]、および [Endpoints] タブが含まれており、提案された変更済みプロファイリングルールの詳細を簡単に表示できます。

ステップ 3 [Next] をクリックして、プロファイリングルールを提案どおりに更新します。

ステップ 4 [Summary] ウィンドウで、プロファイリングルールの詳細を確認します。変更するには、[Edit] をクリックします。

図 *16 : [Review AI Proposals]* ワークフローの *[Summary]* ウィンドウ



ステップ 5 [Done] をクリックして、削除提案を受け入れます。

プロファイリングルールのインポート

カスタムプロファイリングルールと Cisco AI ルールを移行するには、.json ファイルをインポートします。

ステップ 1 [Profiling Rule] ウィンドウで、[Actions] をクリックします。
ステップ 2 [Import Profiling Rules] を選択します。
ステップ 3 [Choose a file] をクリックし、システムの .json ファイルを参照します。
ステップ 4 [OK] をクリックします。

プロファイリングルールのエクスポート

Cisco AI エンドポイント分析からカスタムルールおよび Cisco AI プロファイリングルールをエクスポートしてバックアップできます。[Export Profiling Rules] オプションは、使用可能なすべてのカスタムルールと Cisco AI プロファイリングルールをエクスポートします。ルールを選択してエクスポートすることはできません。

ステップ 1 [Profiling Rules] ウィンドウで、[Actions] をクリックします。

ステップ 2 [Export Profiling Rules] を選択します。

ステップ 3 [Yes] をクリックして、すべてのカスタムルールと ML プロファイリングルールをエクスポートします。終了するには、[No] をクリックします。

（注） 同じファイルを Cisco AI エンドポイント分析に再度インポートできます。

階層

Cisco AI エンドポイント分析階層は、エンドポイントタイプに基づいてエンドポイントの論理グループを作成するのに役立ちます。エンドポイントのカテゴリとサブカテゴリを作成すると、エンドポイントの可視性に焦点が当てられ、許可プロセスが簡素化されます。

デフォルトの [All Endpoints] 親カテゴリからカテゴリを作成できます。エンドポイントの総数、エンドポイントタイプ、サブカテゴリなどのカテゴリの詳細が [Hierarchy] ウィンドウの個々のボックス内に表示されます。

カテゴリを作成、編集、および削除して、階層を並べ替えることができます。

カテゴリとサブカテゴリの作成

ステップ 1 [Hierarchy] ウィンドウで、親カテゴリの水平省略記号をクリックします。

ステップ 2 [Create Category] をクリックします。

ステップ 3 カテゴリ名を入力します。

ステップ 4 Enter キーを押します。

次のタスク

カテゴリを作成したら、[Endpoint Type] ウィンドウからエンドポイントタイプをドラッグアンドドロップするか、カテゴリを編集してエンドポイントを追加できます。

カテゴリまたはサブカテゴリの編集

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。

ステップ 2 [Edit] をクリックします。

ステップ 3 表示される [Edit] ウィンドウで、[Category Name] に値を入力します。

ステップ 4 カテゴリを再割り当てする場合は、ドロップダウンメニューから [Parent Category] を入力します。
ステップ 5 [Endpoint Type] タブをクリックします。
ステップ 6 [Actions] をクリックし、[Add Endpoint Type] を選択します。
ステップ 7 [Search Dropdown] リストからエンドポイントタイプを選択します。
ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

[Endpoint Type] ウィンドウで、[All]、[Available]、および [Assigned] でエンドポイントタイプをフィルタ処理できます。

カテゴリからのエンドポイントタイプの削除

ステップ 1 [Hierarchy] ウィンドウで、削除するカテゴリの水平省略記号をクリックします。
ステップ 2 [Edit] をクリックします。
ステップ 3 [Edit] ウィンドウで、[Endpoint Type] タブをクリックします。
ステップ 4 削除するエンドポイントタイプの横にあるチェックボックスをオンにします。
ステップ 5 [Actions] をクリックし、[Remove From Category] を選択します。

次のメッセージが表示されます。

「Are you sure you want to delete this category?」

ステップ 6 カテゴリからエンドポイントを削除するには、[Yes] をクリックします。終了するには、[No] をクリックします。

カテゴリからのエンドポイントタイプの再割り当て

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。
ステップ 2 [Edit] をクリックします。
ステップ 3 [Edit] ウィンドウで、[Endpoint Type] タブをクリックします。
ステップ 4 再割り当てするエンドポイントタイプの横にあるチェックボックスをオンにします。
ステップ 5 [Actions] をクリックし、[Re-assign to existing category] または [Re-assign to a new category] を選択します。

オプション	手順
既存のカテゴリへの再割り当て	1. [Reassign] ウィンドウで、[Category] ドロップダウンリストから既存のカテゴリを選択します。 2. **[保存（Save）]** をクリックします。

オプション	手順
新しいカテゴリへの再割り当て	1. [Reassign] ウィンドウで、[Category] ドロップダウンリストから [New Category] を選択します。 2. [Parent Category] ドロップダウンリストから親カテゴリを選択します。 3. [New Category] フィールドにカテゴリ名を入力します。 4. [Save] をクリックします。

カテゴリの削除

始める前に

親カテゴリを削除する前に、そのサブカテゴリを確認します。サブカテゴリを別の既存のカテゴリまたは新しいカテゴリに再割り当てできます。そうしないと、すべてのサブカテゴリが親カテゴリとともに削除されます。カテゴリの削除中にサブカテゴリを再割り当てすることもできます。

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。

ステップ 2 [削除（Delete）] をクリックします。

サブカテゴリが割り当てられているカテゴリを削除する場合には、[Reassign Relationships] ダイアログボックスが表示されます。次のいずれかのオプションを選択します。

オプション	条件	手順
既存のカテゴリへの再割り当て	既存のカテゴリにサブカテゴリを再割り当てします。	1. [Category] ドロップダウンリストからカテゴリを選択します。 2. [Reassign] をクリックします。 親カテゴリが削除され、選択したカテゴリにサブカテゴリが再割り当てされます。

オプション	条件	手順
新しいカテゴリへの再割り当て	既存のカテゴリにサブカテゴリを再割り当てします。	**1.** [Parent Category] ドロップダウンリストからカテゴリを選択します。 **2.** [New Category] フィールドにカテゴリ名を入力します。 **3.** [Reassign] をクリックします。 親カテゴリが削除され、新しいカテゴリにサブカテゴリが再割り当てされます。
カテゴリからの削除	親カテゴリとともにサブカテゴリを削除します。	[Reassign] をクリックします。 親カテゴリとそのサブカテゴリが削除されます。

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。