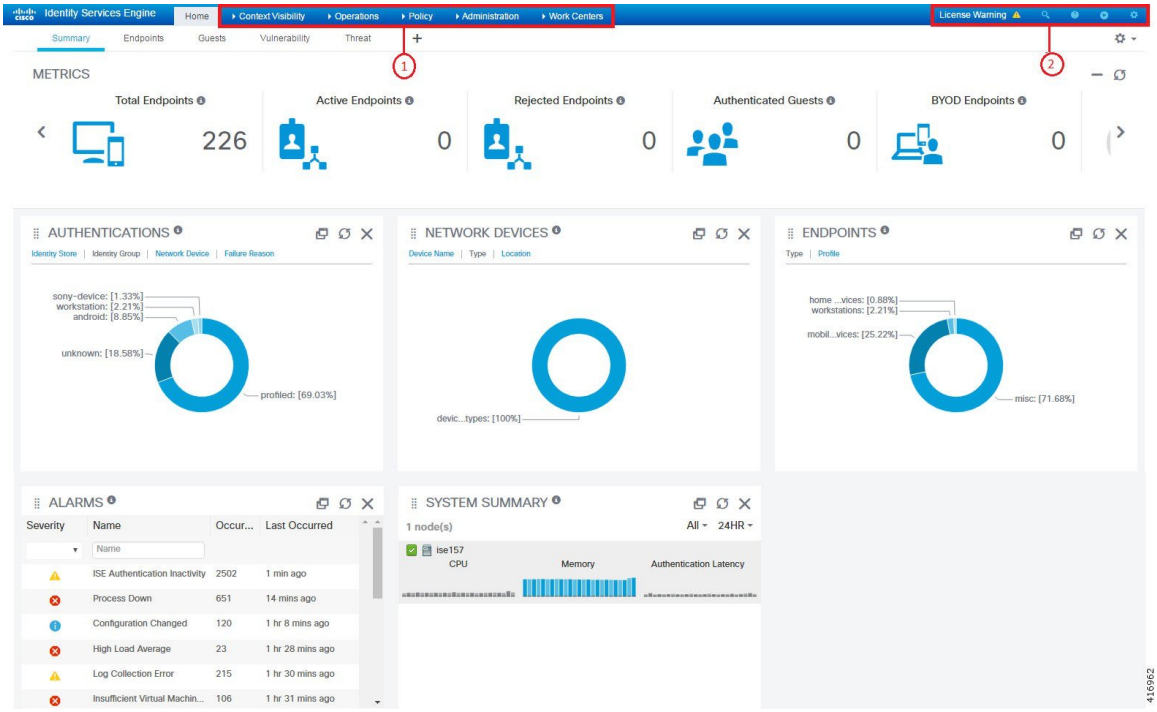
管理者ポータルでの移動

管理者ポータル

管理者ポータルでは、ISE の設定およびレポートにアクセスできます。次の図に、このポータルのメニュー バーの主な要素を示します。



1	メニューのドロップダウン	• [コンテキストの可視性（Context Visibility）]：これらのメニューでは、エンドポイント、ユーザ、NAD に関する情報が表示されます。情報は、ライセンスに応じて、機能、アプリケーション、BYOD、その他のカテゴリ別にセグメント化できます。コンテキスト メニューは中央データベースを使用して、データベース テーブル、キャッシュ、およびバッファから情報を収集し、それにより、コンテキストダッシュレットおよびリストの内容が非常に高速に更新されます。コンテキスト メニューは上部のダッシュレットおよび下部の情報のリストから構成されます。リストのカラム属性を変更することによってデータをフィルタすると、変更したコンテンツを示すためにダッシュレットが更新されます。 • [ポリシー（Policy）]：認証、許可、プロファイリング、ポスチャ、クライアントプロビジョニングの領域でネットワーク セキュリティを管理するためのツールにアクセスします。 • [管理（Administration）]：Cisco ISE ノード、ライセンス、証明書、ネットワーク デバイス、ユーザ、エンドポイント、およびゲスト サービスを管理するためのツールにアクセスします。

2	右上のメニュー	

- 

  エンドポイントを検索し、プロファイル、障害、IDストア、ロケーション、デバイス タイプ別にそれらの分布を表示します。

- 

  現在表示されているページのヘルプにアクセスします。

- 

  次のオプションにアクセスします。

  - [PassiveIDセットアップ（PassiveID Setup）]：[PassiveIDセットアップ（PassiveID Setup）]オプションでは、Active Directory を使用してパッシブ ID をセットアップする [PassiveIDセットアップ（PassiveID Setup）] ウィザードが起動されます。外部認証サーバからユーザ ID と IP アドレスを収集し、認証済み IP アドレスを対応するサブスクライバに配信するように、サーバを設定することができます。

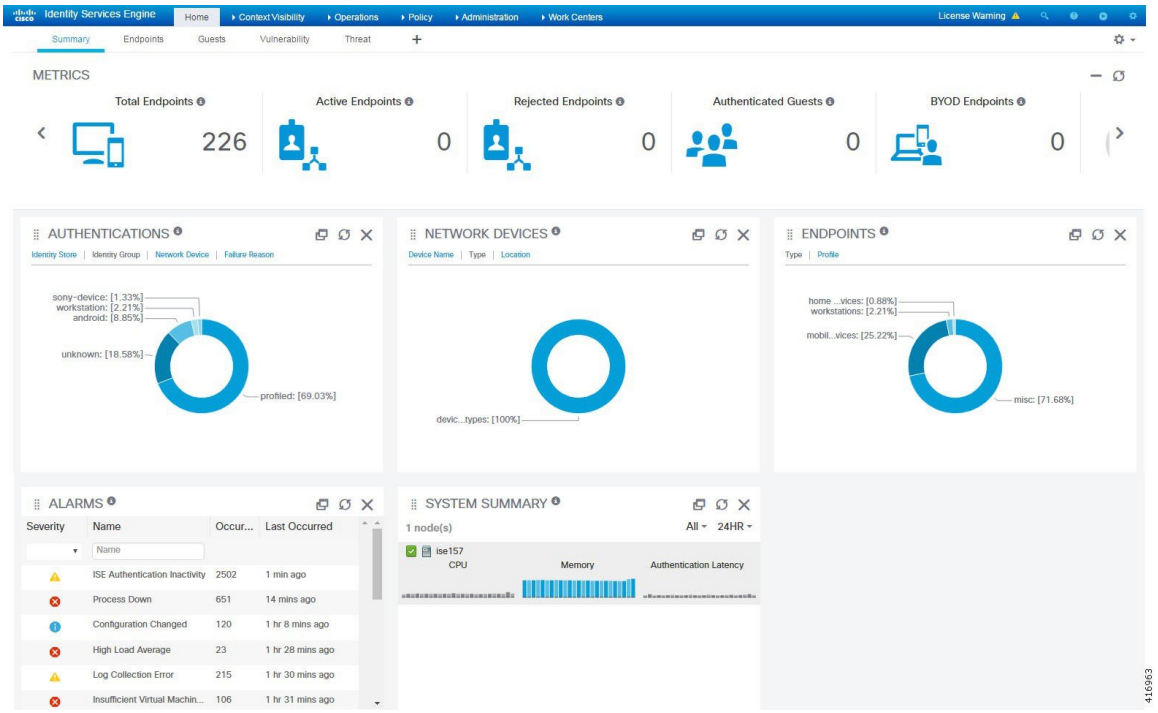
  - [可視性セットアップ（Visibility Setup）]：[可視性セットアップ（Visibility Setup）] オプションは、アプリケーション、ハードウェアインベントリ、USB ステータス、ファイアウォール ステータス、Windows エンドポイントの全般的なコンプライアンス ステータスなどのエンドポイント データを収集して Cisco ISE に送信する、価値の実証（PoV）サービスです。ISE の [可視性セットアップ（Visibility Setup）] ウィザードを起動すると、IP アドレス範囲を指定して、ネットワークの特定セグメントまたはエンドポイント グループに対してエンドポイント検出を実行できます。

    PoV サービスは Cisco Stealth Temporal エージェントを使用して、エンドポイント ポスチャ データを収集します。Cisco ISE は、管理者アカウント タイプで Windows を実行しているコンピュータに Cisco Stealth Temporal エージェントをプッシュし、一時的な実行可能ファイルを自動実行してコンテキストを収集し、エージェントが自動的に削除されます。Cisco Stealth Temporal エージェントのオプション デバッグ機能を使用するには、[エンドポイントロギング（Endpoint Logging）]チェックボックス（[可視性セットアップ（Visibility Setup）] > [ポスチャ（Posture）]）をチェックして、1 つまたは複数のエンドポイントにデバッグ ログを保存します。ログは、次のいずれかの場所で参照できます。

		• C:\WINDOWS\syswow64\config\systemprofile\（64 ビット オペレーティング システム） • C:\WINDOWS\system32\config\systemprofile\（32 ビット オペレーティング システム） • [ワイヤレスのセットアップ（ベータ）（Wireless Setup（BETA））]：[ワイヤレスのセットアップ（ベータ）（Wireless Setup（BETA））] オプションでは、802.1x、ゲスト、および個人所有デバイス持ち込み（BYOD）のワイヤレス フローを容易にセットアップできます。また、このオプションには、ゲストおよび BYOD 向けの各ポータルを設定してカスタマイズするためのワークフローも用意されています。 •  システム アクティビティ。

ISE ホーム ダッシュボード

Cisco ISE ダッシュボードには、効果的なモニタリングおよびトラブルシューティングに必要不可欠な、統合された相関性のあるライブ統計データが表示されます。特に指定がない限り、ダッシュボード要素によってアクティビティは 24 時間表示されます。次の図に、Cisco ISE ダッシュボードで使用できる情報の一部を示します。Cisco ISE ダッシュボード データはプライマリ管理ノード（PAN）でのみ表示されます。



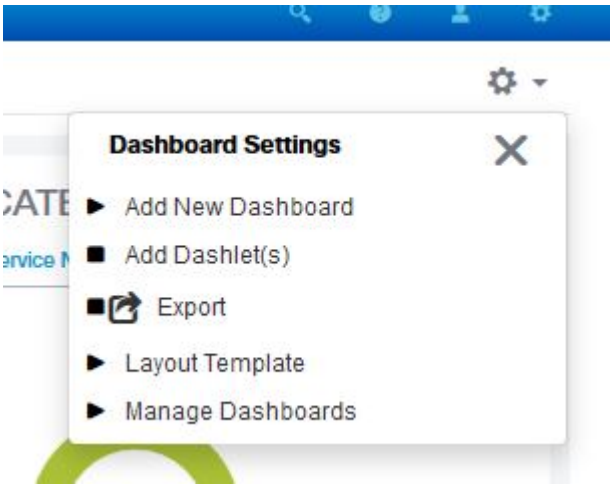
[ホーム（Home）]ページには、ISEデータのビューを表示する5つのデフォルトダッシュボードがあります。

- [概要（Summary）]：このビューには、線形の[メトリック（Metrics）]ダッシュレット、円グラフ ダッシュレット、およびリスト ダッシュレットが表示されます。[メトリック（Metrics）]ダッシュレットは設定できません。
- [エンドポイント（Endpoints）]：ステータス、エンドポイント、エンドポイント カテゴリ、ネットワーク デバイス。
- [ゲスト（Guests）]：ゲスト ユーザ タイプ、ログイン失敗、ロケーション。
- [脆弱性（Vulnerability）]：脆弱性サーバにより ISE に報告される情報。
- [脅威（Threat）]：脅威サーバにより ISE に報告される情報。

これらの各ダッシュボードには、複数の事前定義ダッシュレットがあります。たとえば[概要（Summary）]ダッシュボードには[ステータス（Status）]、[エンドポイント（Endpoints）]、[エンドポイント カテゴリ（Endpoint Categories）]、および[ネットワーク デバイス（Network Devices）]があります。

ホーム ダッシュボードの設定

ホーム ページ ダッシュボードをカスタマイズするには、ページの右上隅にある歯車アイコンをクリックします。



- [エクスポート（Export）] は、現在選択されているホーム ビューを PDF に保存します。
- [レイアウト テンプレート（Layout Template）] は、このビューに表示される列の数を設定します。
- [ダッシュボードの管理（Manage Dashboards）] では、現在のダッシュボードをデフォルト（[ホーム（Home）] を選択すると表示されるダッシュボード）に設定するか、またはすべてのダッシュボードをリセットする（すべてのホーム ダッシュボードの設定を削除する）ことができます。

[コンテキストの可視性（Context Visibility）] のビュー

[コンテキストの可視性（Context Visibility）] ページの構造はホーム ページに似ていますが、[コンテキストの可視性（Context Visibility）] ページでは次の点が異なります。

- 表示データをフィルタリングするときに、現在のコンテキストを維持する（ブラウザ ウィンドウ）。
- より細かなカスタマイズが可能である
- エンドポイント データを中心としている

コンテキストの可視性データはプライマリ管理ノード（PAN）にのみ表示されます。

[コンテキスト（Context）] ページのダッシュレットには、エンドポイントと、エンドポイントからNADへの接続に関する情報が表示されます。現在表示されている情報は、各ページのダッシュレットの下にあるデータ リストの内容に基づいています。各ページには、タブの名前に基づいてエンドポイント データのビューが表示されます。データをフィルタリングすると、リストとダッシュレットの両方が更新されます。データをフィルタリングするには、1 つ以上の円グラフの特定部分をクリックするか、表で行をフィルタリングするか、またはこれらの操作を組み合わせて実行します。複数のフィルタを選択した場合、フィルタ結果は加算的になります。これはカスケード フィルタと呼ばれます。これにより、ドリルダウンして特定のデータを

見つけることができます。また、リストでエンドポイントをクリックして、そのエンドポイントの詳細ビューを表示することもできます。

[コンテキストの可視性（Context Visibility）] には 4 つのメイン ビューがあります。

- [エンドポイント（Endpoints）]：デバイス タイプ、コンプライアンス ステータス、認証タイプ、ハードウェア インベントリなどに基づいて表示するエンドポイントを選択できます。詳しくは、ハードウェア ダッシュボード （13 ページ） を参照してください。

（注） アカウンティングの開始および更新情報が Cisco ISE に確実に送信されるように、NAD でアカウンティングの設定を有効にすることを推奨します。

Cisco ISE では、アカウンティングが有効な場合にのみ、最新の IP アドレス、セッションのステータス（接続 [Connected]、切断 [Disconnected]、または拒否 [Rejected]）、エンドポイントの非アクティブな日数などのアカウンティング情報を収集できます。この情報は、[ライブ ログ（Live Logs）]、[ライブ セッション（Live Sessions）] および [コンテキストの可視性（Context Visibility）] ページに表示されます。NAD でアカウンティングが無効にされている場合、[ライブ セッション（Live Sessions）]、[ライブ ログ（Live Logs）] および [コンテキストの可視性（Context Visibility）] ページ間でアカウンティング情報が欠落しているか、間違っているか、一致していない可能性があります。

（注） [可視性セットアップ（Visibility Setup）] ウィザードでは、エンドポイントを検出するため IP アドレス範囲のリストを追加できます。このウィザードの設定後に、Cisco ISE はエンドポイントを認証しますが、設定された IP アドレス範囲に含まれないエンドポイントは、[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] タブと、[エンドポイント（Endpoints）] リスト ページ（[ワーク センター（Work Centers）] > [ネットワーク アクセス（Network Access）] > [ID（Identities）] > [エンドポイント（Endpoints）] の下）には表示されません。

- [ユーザベース（User-Based）]：ユーザ ID ソースからのユーザ情報を表示します。

  このビューを使用する際には次の点に注意してください。

  1. ユーザ名属性またはパスワード属性が変更されると、認証ステータスが変更された時点でこのページに変更が即時に反映されます。
  2. Active Directory でユーザ名以外の属性が変更されると、再認証から 24 時間後に、更新された属性が表示されます。

3. Active Directory でユーザ名とその他の属性が変更されると、再認証後即時に最新の変更が表示されます。

- [ネットワーク デバイス（Network Devices）]：エンドポイントに接続している NAD のリスト。NAD のエンドポイント数（右端の列）をクリックすると、その NAD に基づいてフィルタリングされたすべてのデバイスが [コンテキストの可視性（Context Visibility）] 画面にリストされます。
- [アプリケーション（Application）]：[アプリケーション（Application）] ビューは、指定されたアプリケーションがインストールされているエンドポイントの数を識別するために使用されます。結果は、グラフ形式と表形式で表示されます。グラフ表示は、比較分析に役立ちます。たとえば、Google Chrome ソフトウェアを使用してエンドポイントの数をバージョン、ベンダー、カテゴリ（フィッシング詐欺対策、ブラウザなど）と共に、表や棒グラフで確認することができます。詳細については、「アプリケーション ダッシュボード」の項を参照してください。

フィルタリング処理を追加する目的で、[コンテキストの可視性（Context Visibility）] の下に新しいビューを作成し、カスタム リストを作成できます。このリリースでは、カスタム ビューでダッシュレットがサポートされていません。

ダッシュレットの円グラフの特定部分をクリックすると、新しいページが開き、そのダッシュレットからフィルタリングされたデータが [コンテキストの可視性（Context Visibility）] モードで表示されます。この新しいページから、表示されているデータをさらにフィルタリングできます。これについてはビューに表示するデータのフィルタリング （15 ページ）で説明します。

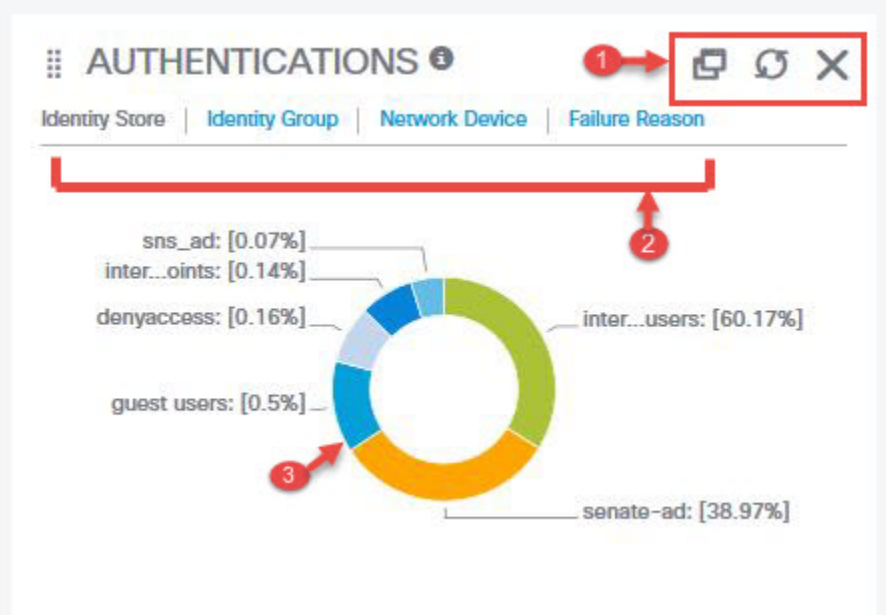
[コンテキストの可視性（Context Visibility）] を使用してエンドポイント データを検索する方法の詳細については、Cisco YouTube ビデオを参照してください。このビデオでは ISE 2.1 https://www.youtube.com/watch?v=HvonGhrydfg を使用しています。

関連トピック

ハードウェア ダッシュボード （13 ページ）

ダッシュレット

次に、ダッシュレットの例を示します。



1. ウィンドウが重なり合ったシンボルは、このダッシュレットを「切り離し」ます。つまり、新しいブラウザ ウィンドウでこのダッシュレットを開きます。円形のシンボルは更新を実行します。Xはこのダッシュレットを削除します。このシンボルはホームページでのみ使用可能です。[コンテキストの可視性（Context Visibility）] でダッシュレットを削除するには、画面右上隅にある歯車のシンボルを使用します。
2. 一部のダッシュレットには異なるカテゴリのデータが表示されます。リンクをクリックすると、そのデータ セットの円グラフが表示されます。
3. 円グラフには、選択したデータが表示されます。円グラフの 1 つのセグメントをクリックすると、[コンテキストの可視性（Context Visibility）] で新しいタブが開き、円グラフ セグメントに基づいてフィルタリングされたデータが表示されます。

ホーム ダッシュボードで円グラフのセクションをクリックすると、新しいブラウザ ウィンドウが開き、円グラフでクリックしたセクションに基づいてフィルタリングされたデータが表示されます。

[コンテキスト（Context）] ビューで円グラフのセクションをクリックすると、表示されているデータがフィルタリングされますが、コンテキストは変更されず、フィルタリングされたデータは同じブラウザ ウィンドウに表示されます。

アプリケーション ダッシュボード

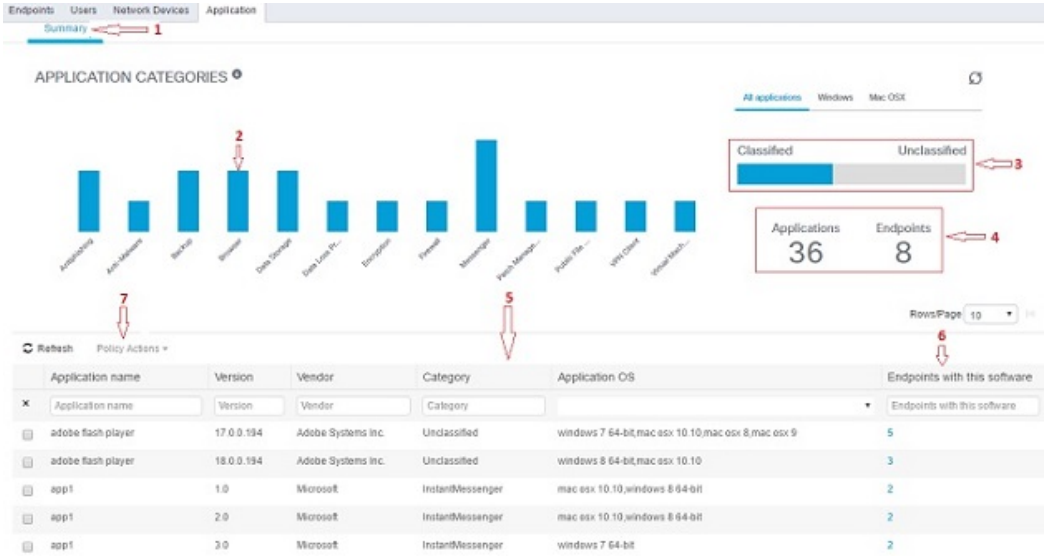
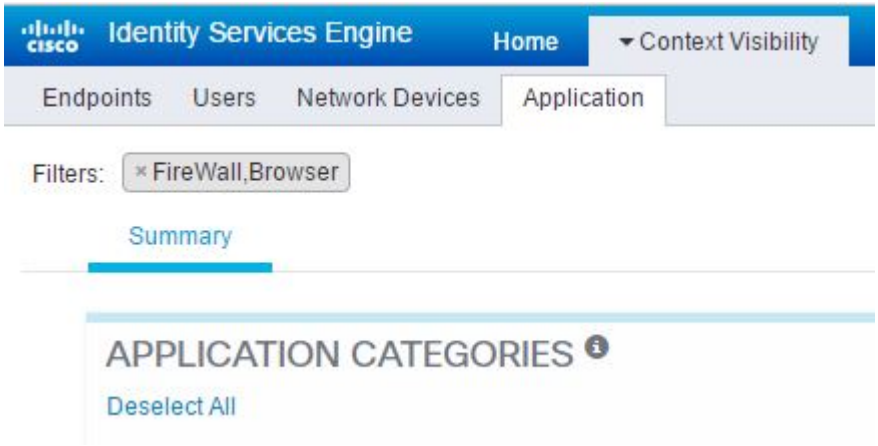


表 *1:* アプリケーション ダッシュボードの説明

ラベル（Label）	説明
1	デフォルトで[概要（Summary）]タブが選択されています。棒グラフを含む[アプリケーション カテゴリ（Application Categories）] ダッシュレットが表示されます。アプリケーションは13のカテゴリに分類されます。これらのカテゴリに属さないアプリケーションは、「未分類（Unclassified）」と呼ばれます。 利用可能なカテゴリは、[マルウェア対策（Anti-Malware）]、[フィッシング対策（Antiphishing）]、[バックアップ（Backup）]、[ブラウザ（Browser）]、[データ漏洩防止（Data Loss Prevention）]、[データ ストレージ（Data Storage）]、[暗号化（Encryption）]、[ファイアウォール（Firewall）]、[メッセンジャ（Messenger）]、[パッチ管理（Patch Management）]、[パブリック ファイル共有（Public File Sharing）]、[仮想マシン（Virtual Machine）]、[VPN クライアント（VPN Client）] です。
2	各バーは、分類されたカテゴリに対応します。各バーの上にマウスを置くと、選択したアプリケーション カテゴリに対応するアプリケーションとエンドポイントの合計数を表示できます。
3	分類されたカテゴリに該当するアプリケーションとエンドポイントは青色で表示されます。未分類のアプリケーションとエンドポイントはグレーで表示されます。分類されたカテゴリ バーまたは分類されていないカテゴリ バーの上にマウスを置くと、そのカテゴリに属するアプリケーションとエンドポイントの合計数を表示できます。[分類済み（Classified）]をクリックして、棒グラフと表（5）で結果を表示できます。[未分類（Unclassified）]をクリックすると、棒グラフが無効になり（グレー表示）、結果が表（5）に表示されます。

<table>
<tr><th>ラベル（Label）</th><th>説明</th></tr>
<tr><td>4</td><td>アプリケーションとエンドポイントは、選択されたフィルタに基づいて表示されます。異なるフィルタをクリックすると、パンくずリストを表示できます。[すべて選択解除（Deselect All）] をクリックして、すべてのフィルタを削除できます。
 
</td></tr>
<tr><td>5</td><td>複数のバーをクリックすると、対応する分類されたアプリケーションとエンドポイントが表に表示されます。たとえば、[マルウェア対策（Antimalware）]および[パッチ管理（Patch Management）] カテゴリを選択すると、次の結果が表示されます。
<table>
<tr><th>アプリケーション</th><th>バージョン（Version）</th><th>ベンダー（Vendor）</th><th>カテゴリ（Category）</th><th>アプリケーション OS</th><th>このソフトウェアで使用するエンドポイント</th></tr>
<tr><td>Gatekeeper</td><td>9.9.5</td><td>Apple Inc.</td><td>マルウェア対策</td><td>windows 7 64 ビット、mac osx 10.10、mac osx 8、mac osx 9</td><td>5</td></tr>
<tr><td>Gatekeeper</td><td>10.9.5</td><td>Apple Inc.</td><td>マルウェア対策</td><td>windows 8 64 ビット、mac osx 10.10</td><td>3</td></tr>
<tr><td>ソフトウェア更新</td><td>2.3</td><td>Apple Inc.</td><td>パッチ管理</td><td>windows 7 64 ビット、mac osx 10.10、mac osx 8、mac osx 9</td><td>5</td></tr>
</table></td></tr>
<tr><td>[6]</td><td>表の [このソフトウェアで使用するエンドポイント（Endpoints With This Software）] 列のエンドポイントをクリックして、Mac アドレス、NAD IP アドレス、NAD ポート ID/SSID、IPv4 アドレスなどのエンドポイントの詳細を表示します。</td></tr>
</table>

ラベル（Label）	説明
7	アプリケーションのコンプライアンス条件と修復を作成するには、アプリケーション名を選択し、[ポリシー アクション（Policy Actions）] ドロップダウンリストから [アプリケーション コンプライアンスの作成（Create App Compliance）] オプションを選択します。

ハードウェア ダッシュボード

[コンテキストの可視性（context visibility）] の下の [エンドポイント ハードウェア（endpoint hardware）] タブは、短期間にエンドポイント ハードウェア インベントリ情報を収集、分析、およびレポートするのに役立ちます。メモリ容量が小さいエンドポイントの検出や、エンドポイントのBIOSモデル/バージョンの検出など、情報を収集することができます。これらの結果に基づいて、メモリ容量を増やしたり、BIOS バージョンをアップグレードすることができます。アセットの購入を計画する前に、要件を評価することができます。リソースを適時に交換することができます。モジュールをインストールしたりエンドポイントとやりとりすることなく、この情報を収集できます。要約すると、アセットのライフサイクルを効果的に管理できます。

[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [ハードウェア（Hardware）] ページには、[製造者（Manufacturers）] および [エンドポイント使用率（Endpoint Utilizations）] ダッシュレットが表示されます。これらのダッシュレットは、選択されたフィルタに基づく変更を反映します。[製造者（Manufacturers）] ダッシュレットには、Windows および Mac OS が搭載されたエンドポイントのハードウェア インベントリの詳細が表示されます。[エンドポイント使用率（Endpoint Utilizations）] ダッシュレットには、エンドポイントの CPU、メモリ、およびディスク使用率が表示されます。3 つのオプションのいずれかを選択すると、利用率をパーセンテージで表示できます。

- CPU 使用率が n% を超えるデバイス（Devices With Over n% CPU Usage）
- メモリ使用率が n% を超えるデバイス（Devices With Over n% Memory Usage）
- ディスク使用率が n% を超えるデバイス（Devices With Over n% Disk Usage）

（注） ハードウェア インベントリ データは、ISE GUI に表示されるまでに 120 秒かかります。ハードウェア インベントリ データは、ポスチャ準拠および非準拠の状態について収集されます。

エンドポイントとその接続された外部デバイスのハードウェア属性は表形式で表示されます。次のハードウェア属性が表示されます。

- MAC アドレス（MAC Address）
- BIOS 製造元（BIOS Manufacturer）
- BIOS シリアル番号（BIOS Serial Number）

- BIOS モデル（BIOS Model）
- 接続デバイス（Attached Devices）
- CPU 名（CPU Name）
- CPU 速度（GHz）（CPU Speed (GHz)）
- CPU 使用率（%）（CPU Usage (%)）
- コア数
- プロセッサ数（Number of Processors）
- メモリ サイズ（GB）（Memory Size (GB)）
- メモリ使用率（%）（Memory Usage (%)）
- 内部ディスクの合計サイズ（GB）（Total Internal Disk(s) Size (GB)）
- 内部ディスクの合計フリー サイズ（GB）（Total Internal Disk(s) Free Size (GB)）
- 内部ディスクの合計使用率（%）（Total Internal Disk(s) Usage (%)）
- 内部ディスク数（Number of Internal Disks）
- NAD ポート ID（NAD Port ID）
- ステータス
- ネットワークデバイス名（Network Device Name）
- 参照先
- UDID
- IPv4 アドレス（IPv4 Address）
- [ユーザ名（Username）]
- ホストネーム
- OS タイプ（OS Types）
- 異常な動作（Anomalous Behavior）
- エンドポイント プロファイル（Endpoint Profile）
- 説明
- [エンドポイント タイプ（Endpoint Type）]
- ID グループ
- 登録日（Registration Date）
- ID ストア

- 許可プロファイル

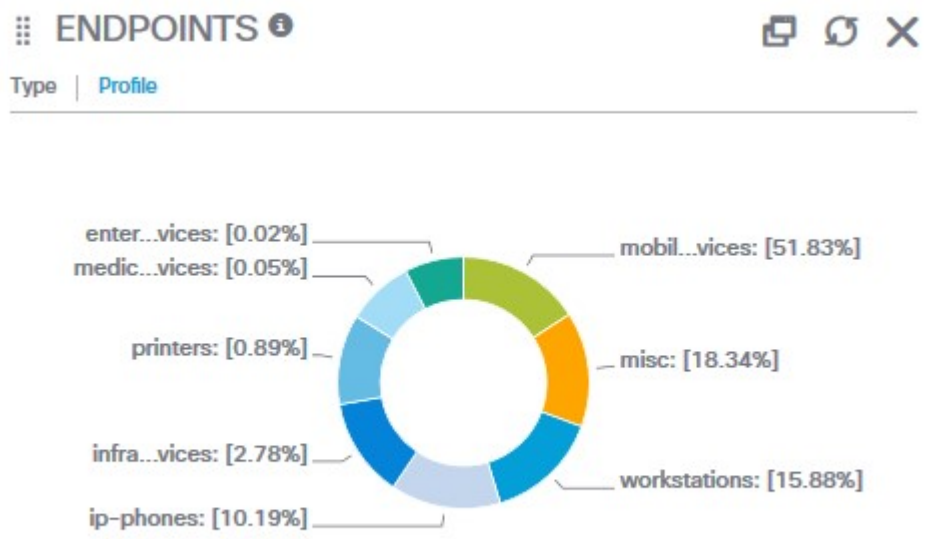
エンドポイントに対応する [接続デバイス（Attached Devices）] 列の番号をクリックすると、現在エンドポイントに接続されている USB デバイスの名前、カテゴリ、製造元、タイプ、製品 ID、およびベンダー ID を表示できます。

（注） Cisco ISE はクライアントのシステムのハードウェア属性をプロファイリングしますが、Cisco ISE がプロファイリングしないハードウェア属性がいくつか存在することがあります。これらのハードウェア属性は、[ハードウェア コンテキストの可視性（Hardware Context Visibility）] ページに表示されないことがあります。

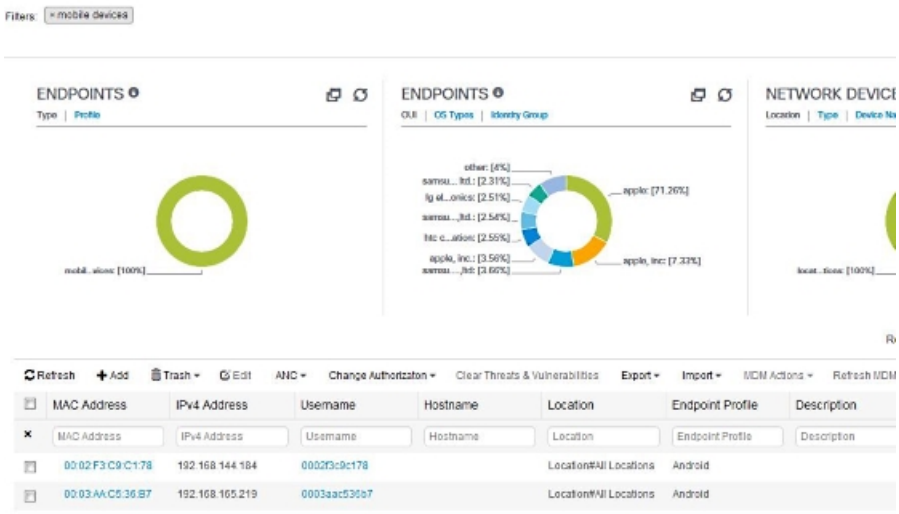
ハードウェア インベントリ データの収集間隔は、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）]** ページで制御できます。デフォルトの間隔は 5 分です。

ビューに表示するデータのフィルタリング

[コンテキストの可視性（Context Visibility）] ページでいずれかのダッシュレットをクリックすると、クリックしたアイテムに基づいて表示されるデータ（円グラフの一部分など）がフィルタリングされます。

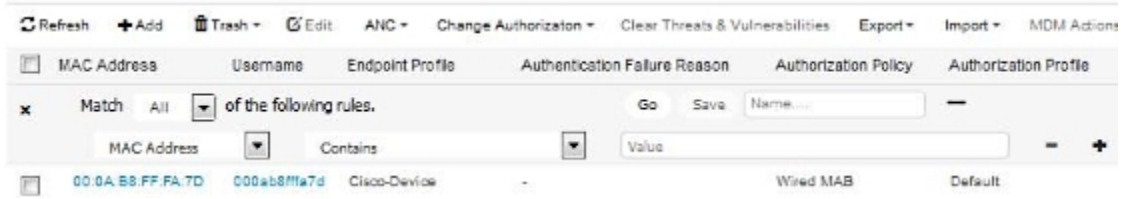


[エンドポイント（Endpoints）] ダッシュレットで [mobil…vices] をクリックすると、ページが再表示され、2 つの [エンドポイント（Endpoints）] ダッシュレット、[ネットワーク デバイス（Network Devices）] ダッシュレット、およびデータのリストが表示されます。次の例に示すように、ダッシュレットとリストにはモバイル デバイスのデータが表示されます。



さらにデータをフィルタリングするには、円グラフの他のセクションをクリックするか、またはデータ リストのコントロールを使用します。

1. 歯車アイコンにより、表示列がフィルタリングされます。ドロップダウンでは、このダッシュボードのリストに表示する列を選択できます。
2. デフォルトではクイック フィルタが表示されます。ボックス（ラベル番号 3）に文字を入力すると、結果に基づいてリストがフィルタリングされます。カスタム フィルタでは、次に示すようにより細かく設定できるフィルタが表示されます。

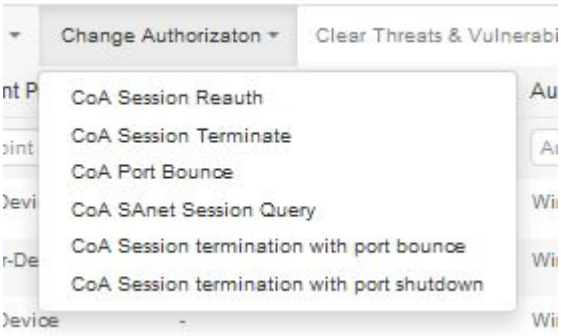


カスタム フィルタは保存できます。

ビューのリストでのエンドポイント アクション

リスト上部にあるツールバーから、リストで選択したエンドポイントに対してアクションを実行できます。すべてのリストですべてのアクションが有効になっているわけではありません。一部のアクションは、使用可能な機能に基づいています。次のリストに、使用する前にISEで有効にする必要がある2つのエンドポイント アクションを示します。

- 適応型ネットワーク制御（ANC）が有効な場合、リストでエンドポイントを選択して、ネットワーク アクセスを割り当てるかまたは取り消すことができます。認可変更（CoA）も発行できます。



ANC（エンドポイント保護サービス）は、ISEの[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）]>[適応型ネットワーク制御（Adaptive Network Control）]で有効にします。詳細については、Cisco ISE での適応型ネットワーク制御の有効化を参照してください。

- MDMがインストールされている場合は、選択したエンドポイントに対してMDMアクションを実行できます。

コンテキストの可視性の属性

コンテキストの可視性の属性を提供するシステムとサービスでは、同じ属性名に異なる値を使用していることがよくあります。次にいくつかの例を示します。

オペレーティング システム

- *OperatingSystem*：ポスチャ オペレーティング システム
- *operating-system*：NMAP オペレーティング システム
- *operating-system-result*：プロファイラ統合オペレーティング システム

ポータル名

- *Portal.Name*：デバイス登録が有効な場合のゲスト ポータル名。
- *PortalName*：デバイス登録が無効な場合のゲスト ポータル名。

ポータル ユーザ

- *User-Name*：RADIUS 認証のユーザ名
- *GuestUserName*：ゲスト ユーザ
- *PortalUser*：ポータル ユーザ

Cisco ISE 国際化およびローカリゼーション

Cisco ISE 国際化では、サポートされる言語にユーザ インターフェイスを合わせます。ユーザ インターフェイスのローカリゼーションでは、ロケール固有のコンポーネントおよび翻訳されたテキストが組み込まれます。Windows、MAC OSX、および Android デバイスの場合、ネイティブ サプリカント プロビジョニング ウィザードは、次のサポートされている言語のいずれかで使用できます。

Cisco ISE の国際化およびローカリゼーションのサポートでは、ポータルに接するエンドユーザに対してUTF-8符号化で英語以外のテキストをサポートすること、および管理者ポータルの選択的フィールドに重点を置いています。

サポートされる言語

Cisco ISE では、次の言語とブラウザ ロケールのローカリゼーションおよび国際化がサポートされます。

[言語（Language）]	ブラウザ ロケール
中国語（繁体字）	zh-tw
中国語（簡体字）	zh-cn
チェコ語	cs-cz
Dutch	nl-nl
英語	en
フランス語	fr-fr
ドイツ語	de-de
ハンガリー語	hu-hu
イタリア語	it-it
日本語	ja-jp
Korean	ko-kr

[言語（Language）]	ブラウザ ロケール
ポーランド語	pl-pl
ポルトガル語（ブラジル）	pt-br
ロシア語	ru-ru
スペイン語	es-es

エンドユーザ Web ポータルのローカリゼーション

ゲスト、スポンサー、デバイスおよびクライアントプロビジョニングの各ポータルは、サポートされているすべての言語およびロケールにローカライズされています。ローカライズには、テキスト ラベル、メッセージ、フィールド名およびボタン ラベルが含まれます。クライアント ブラウザが Cisco ISE テンプレートにマッピングされていないロケールを要求した場合、ポータルは英語のテンプレートを使用して内容を表示します。

管理者ポータルを使用して、各言語のゲスト、スポンサー、デバイスの各ポータルで使用されるフィールドを個別に変更できます。また、言語を追加することも可能です。現在、クライアントプロビジョニング ポータルについては、これらのフィールドはカスタマイズできません。

HTML ページを Cisco ISE にアップロードすることによって、ゲスト ポータルを詳細にカスタマイズできます。カスタマイズしたページをアップロードする場合は、展開に対する適切なローカリゼーション サポートに責任を負います。Cisco ISE では、サンプル HTML ページを含むローカリゼーション サポート例が提供されており、これをガイドとして使用できます。Cisco ISE には、国際化されたカスタム HTML ページをアップロード、格納、および表示する機能があります。

（注） NAC および MAC エージェントのインストーラおよび WebAgent ページはローカライズされていません。

UTF-8 文字データ エントリのサポート

エンドユーザに（Cisco NAC Agent またはサプリカント、あるいはスポンサー、ゲスト、デバイス、クライアント プロビジョニングの各ポータルを介して）公開される Cisco ISE フィールドは、すべての言語の UTF-8 文字セットをサポートします。UTF-8 は、Unicode 文字セット用のマルチバイト文字エンコーディングであり、ヘブライ語、サンスクリット語、アラビア語など、多数の異なる言語文字セットがあります。

文字の値は、管理設定データベースに UTF-8 で格納され、UTF-8 文字はレポートおよびユーザ インターフェイス コンポーネントで正しく表示されます。

UTF-8 クレデンシャル認証

ネットワーク アクセス認証では、UTF-8ユーザ名およびパスワードのクレデンシャルがサポートされます。これには、RADIUS、EAP、RADIUS プロキシ、RADIUS トークン、ゲストおよび管理ポータルのログイン認証からのWeb認証が含まれます。ユーザ名とパスワードのUTF-8サポートは、ローカル ID ストアおよび外部 ID ストアに対する認証に適用されます。

UTF-8認証は、ネットワーク ログインに使用されるクライアント サプリカントに依存します。一部のWindowsネイティブ サプリカントでは、UTF-8 クレデンシャルはサポートされません。

（注） RSA では UTF-8 ユーザはサポートされないため、RSA を使用した UTF-8 認証はサポートされません。同様に、Cisco ISE と互換性がある RSA サーバでも UTF-8 がサポートされません。

UTF-8 ポリシーおよびポスチャ評価

属性値に基づいて決定される Cisco ISE のポリシー ルールに、UTF-8 テキストが含まれている場合があります。UTF-8 属性値はルール評価でサポートされます。また、管理ポータルでUTF-8の値を使用して条件を設定できます。

ポスチャ要件を、UTF-8 文字セットに基づくファイル、アプリケーション、およびサービス条件として変更できます。これには、UTF-8 要件の値を NAC エージェントに送信することが含まれます。NAC エージェントはそれに応じてエンドポイントを評価し、UTF-8 の値を報告します（該当する場合）。

Cisco NAC および MAC エージェントの UTF-8 サポート

Cisco NAC エージェントでは、テキスト、メッセージ、および Cisco ISE と交換される任意のUTF-8データの国際化がサポートされます。これには、要件メッセージ、要件名、および条件で使用されるファイル名およびプロセス名が含まれます。

次の制限が適用されます。

- UTF-8 サポートは、Windows ベースの NAC エージェントにのみ適用されます。
- Cisco NAC および MAC エージェントのインターフェイスでは、現在、ローカリゼーションはサポートされていません。
- WebAgent では、UTF-8 ベースのルールおよび要件はサポートされません。
- 利用規定（AUP）が設定されている場合は、ブラウザ ロケールと設定で指定された言語セットに基づいて、ポリシーのページがクライアント側で提供されます。ローカライズされた AUP バンドルまたはサイト URL の提供は、ユーザの責任です。

サプリカントに送信されるメッセージの UTF-8 サポート

RSA プロンプトおよびメッセージは、RADIUS 属性 REPLY-MESSAGE を使用して、または EAP データ内で、サプリカントに転送されます。テキストに UTF-8 データが含まれている場合は、サプリカントによって、クライアントのローカル オペレーティング システムの言語サ

ポートに基づいて表示されます。一部の Windows ネイティブ サプリカントでは、UTF-8 クレデンシャルはサポートされません。

Cisco ISE プロンプトおよびメッセージは、サプリカントが実行されているクライアントのオペレーティング システムのロケールと同期していない場合があります。エンドユーザのサプリカントのロケールを Cisco ISE によってサポートされている言語に合わせる必要があります。

レポートおよびアラートの UTF-8 サポート

モニタリングおよびトラブルシューティングのレポートおよびアラートでは、Cisco ISE でサポートされる言語について、次のように関連属性の UTF-8 の値がサポートされます。

- ライブ認証の表示
- レポート レコードの詳細ページの表示
- レポートのエクスポートと保存
- Cisco ISE ダッシュボードの表示
- アラート情報の表示
- tcpdump データの表示

ポータルでの UTF-8 文字のサポート

Cisco ISE フィールド（UTF-8）では、ポータルおよびエンドユーザ メッセージでローカリゼーション用に現在サポートされているよりも、多くの文字セットがサポートされます。たとえば、Cisco ISE では、ヘブライ語やアラビア語などの右から左へ記述する言語はサポートされていません（文字セット自体はサポートされています）。

次の表に、データの入力および表示に UTF-8 文字をサポートする管理者ポータルおよびエンドユーザ ポータルのフィールドを示します。次の制限があります。

- Cisco ISE では、UTF-8 文字を使用したゲスト パスワードはサポートされません。
- Cisco ISE では、証明書で UTF-8 文字を使用することはできません。

表 *2 :* 管理者ポータルの *UTF-8* 文字フィールド

管理者ポータル要素	UTF-8 フィールド
ネットワーク アクセスのユーザ設定	• ユーザ名（User name） • 名（First name） • 姓（Last name） • 電子メール（e-mail）

管理者ポータル要素	UTF-8 フィールド
ユーザ リスト	• すべてのフィルタ フィールド • [ユーザ リスト（User List）] ページに表示される値 • 左側のナビゲーション クイック ビューに表示される値
ユーザ パスワード ポリシー	パスワードには、大文字と小文字、数字、特殊文字（「!」、「@」、「#」、「$」、「%」、「^」、「&」、「*」、「(」、「)」など）を自由に組み合わせて使用できます。[パスワード（Password）] フィールドでは、UTF-8 文字を含むあらゆる文字を使用できますが、制御文字は使用できません。 言語の中には大文字または小文字のアルファベットがないものがあります。ユーザパスワード ポリシーでユーザに大文字または小文字でパスワードを入力することを求め、ユーザの言語がこれらの文字をサポートしていない場合、ユーザはパスワードを設定できません。ユーザ パスワード フィールドで UTF-8 文字をサポートするには、ユーザ パスワード ポリシー ページ（**[管理（Administration）] > [IDの管理（Identity Management）] > [設定（Settings）] > [ユーザ パスワード ポリシー（User Password Policy）]**）で次のオプションをオフにする必要があります。 • 小文字の英文字（Lowercase alphabetic characters） • 大文字の英文字（Uppercase alphabetic characters）
管理者リスト	• すべてのフィルタ フィールド • [管理者リスト（Administrator List）] ページに表示される値 • 左側のナビゲーション クイック ビューに表示される値
管理者ログイン ページ	• ユーザ名（User name）

管理者ポータル要素	UTF-8 フィールド
RSA	• メッセージ • プロンプト
RADIUS トークン	• [認証（Authentication）] タブ > [プロンプト（Prompt）]
ポスチャ要件	• [名前（Name）] • [修復アクション（Remediation action）] > エージェント ユーザに表示されるメッセージ • 要件リスト表示
ポスチャ条件	• [ファイル条件（File condition）]>[ファイル パス（File path）] • [アプリケーション条件（Application condition）] > [プロセス名（Process name）] • [サービス条件（Service condition）]>[サービス名（Service name）] • 条件リスト表示
ゲストおよびデバイスの設定	• [スポンサー（Sponsor）] > [言語テンプレート（Language Template）] : サポートされているすべての言語、すべてのフィールド • [ゲスト（Guest）] > [言語テンプレート（Language Template）] : サポートされているすべての言語、すべてのフィールド • [デバイス（My Devices）] > [言語テンプレート（Language Template）] : サポートされているすべての言語、すべてのフィールド
システム設定	• [SMTP サーバ（SMTP Server）] > [デフォルトの電子メール アドレス（Default e-mail address）]

管理者ポータル要素	UTF-8 フィールド
[操作（Operations）]>[アラーム（Alarms）]>[ルール（Rule）]	• [基準（Criteria）] > [ユーザ（User）] • [通知（Notification）] > [電子メール通知ユーザ リスト（e-mail Notification user list）]
[操作（Operations）] > [レポート（Reports）]	• [操作（Operations）] > [ライブ認証（Live Authentications）] > フィルタ フィールド • [操作（Operations）] > [レポート（Reports）] > [カタログ（Catalog）] > レポート フィルタ フィールド
[操作（Operations）]>[トラブルシューティング（Troubleshoot）]	• [一般ツール（General Tools）] > [RADIUS 認証トラブルシューティング（RADIUS Authentication Troubleshooting）] > [ユーザ名（Username）]
ポリシー	• [認証（Authentication）]>ポリシー条件内での av 式の値 • [許可（Authorization）]/[ポスチャ（Posture）]/[クライアント プロビジョニング（Client Provisioning）] > [その他の条件（Other Conditions）] > ポリシー条件内での av 式の値

管理者ポータル要素	UTF-8 フィールド
ポリシー ライブラリ条件の属性値	• [認証（Authentication）] > [単純条件/複合条件（Simple Condition/Compound Condition）] > av 式の値 • [認証（Authentication）]> 単純条件リスト表示 • [認証（Authentication）]> 単純条件リスト > 左のナビゲーション クイック ビュー表示 • [許可（Authorization）] > [単純条件/複合条件（Simple Condition/Compound Condition）] > av 式の値 • [許可（Authorization）] > 単純条件リスト > 左のナビゲーション クイック ビュー表示 • [ポスチャ（Posture）] > [ディクショナリ単純条件/ディクショナリ複合条件（Dictionary Simple Condition/Dictionary Compound Condition）] > av 式の値 • [ゲスト（Guest）] > [単純条件/複合条件（Simple Condition/Compound Condition）] > av 式の値

ユーザ インターフェイス外での UTF-8 サポート

この項では、Cisco ISE ユーザ インターフェイス外で UTF-8 がサポートされる領域について説明します。

デバッグ ログおよび CLI 関連の UTF-8 サポート

一部のデバッグ ログには、属性値およびポスチャ条件の詳細が表示されます。そのため、すべてのデバッグ ログで UTF-8 の値が受け入れられます。raw UTF-8 データを含むデバッグ ログをダウンロードして、UTF-8 対応ビューアで表示できます。

ACS 移行の UTF-8 サポート

Cisco ISE では、ACS UTF-8 設定オブジェクトおよび値の移行が可能です。一部の UTF-8 オブジェクトの移行は、Cisco ISE UTF-8 言語でサポートされない場合があります。そのため、移行中に提供される UTF-8 データの一部は、管理ポータルまたはレポート方式を使用して読み取れない表示になる場合があります。（ACS から移行された）読み取り不可能な UTF-8 値は ASCII テキストに変換する必要があります。ACE から ISE への移行の詳細については、『ISE Migration

Guide』（http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/migration_guide/b_ise_MigrationGuide21.html）を参照してください。

UTF-8 の値のインポートおよびエクスポートのサポート

管理者ポータルおよびスポンサー ポータルは、ユーザ アカウントの詳細をインポートするときに使用される UTF-8 値のプレーン テキストおよび .csv ファイルをサポートします。エクスポートされたファイルは csv ファイルとして提供されます。

REST での UTF-8 サポート

UTF-8 の値は、外部 REST 通信でサポートされます。これは、admin 認証を除き、Cisco ISE ユーザ インターフェイスの UTF-8 がサポートされる設定可能項目に適用されます。REST での admin 認証には、ログインのために ASCII テキスト クレデンシャルが必要です。

ID ストアの許可データの UTF-8 サポート

Cisco ISE では、Active Directory および LDAP がポリシー処理のために許可ポリシーで UTF- 8 データを使用できます。

MAC アドレスの正規化

ISE は次のいずれかの形式で入力された MAC アドレスの正規化をサポートします。

- 00-11-22-33-44-55
- 0011.2233.4455
- 00:11:22:33:44:55
- 001122334455
- 001122-334455

次の ISE ウィンドウでは、完全または部分的な MAC アドレスを指定できます。

- [ポリシー（Policy）] > [ポリシー セット（Policy Sets）]
- [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [許可（Authorization）]
- [認証（Authentications）] > [フィルタ（Filters）]（エンドポイント カラムおよび ID カラム）
- [グローバル検索（Global Search）]
- [操作（Operations）] > [レポート（Reports）] > [レポート フィルタ（Reports Filters）]
- [操作（Operations）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [エンドポイントのデバッグ（Endpoint Debug）]

次のISEウィンドウでは、完全なMACアドレスを指定する必要があります（「:」または「-」または「.」で区切られた6オクテット）。

- [操作（Operations）]>[エンドポイント保護サービス（Endpoint Protection Services）適応型ネットワーク制御（Adaptive Network Control）]
- [操作（Operations）]>[トラブルシューティング（Troubleshooting）]>[診断ツール（Diagnostic Tools）]>[一般ツール（General Tools）]>[RADIUS認証トラブルシューティング（RADIUS Authentication Troubleshooting）]
- [操作（Operations）]>[トラブルシューティング（Troubleshooting）]>[診断ツール（Diagnostic Tools）]>[一般ツール（General Tools）]>[ポスチャのトラブルシューティング（Posture Troubleshooting）]
- [管理（Administration）]>[ID（Identities）]>[エンドポイント（Endpoints）]
- [管理（Administration）]>[システム（System）]>[展開（Deployment）]
- [管理（Administration）]>[ロギング（Logging）]>[収集フィルタ（Collection Filter）]

REST APIでも、完全なMACアドレスの正規化がサポートされます。

有効なオクテットには0～9、a～f、またはA～Fのみ含めることができます。

ロールベース アクセス コントロール ポリシーによって制限されている管理者機能

Cisco ISEでは、管理権限を制限することでセキュリティを確保するロールベース アクセス コントロール（RBAC）ポリシーが提供されます。RBACポリシーは、ロールおよび権限を定義するためにデフォルトの管理者グループに関連付けられています。標準的な権限セット（メニューおよびデータアクセス）が、事前定義された管理者グループそれぞれとペアになっており、それによって、関連付けられたロールおよび職務機能と整合性がとられています。

ユーザインターフェイスにある一部の機能には、使用するために特定の権限が必要です。ある機能が使用できない場合、または特定のタスクの実行が許可されない場合、その機能を利用するタスクを実行するのに必要な権限が自分の管理者グループにない場合があります。

アクセス レベルに関係なく、すべての管理者アカウントは、管理者がアクセスできるすべてのページの、権限を持つオブジェクトを変更または削除できます。