

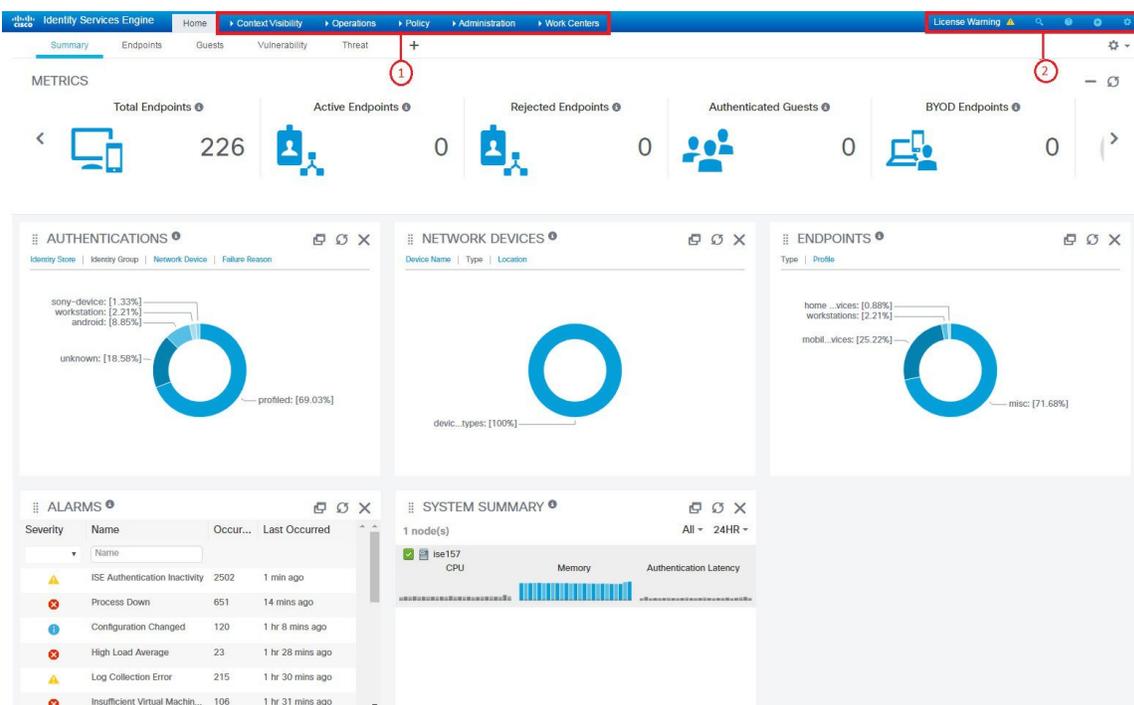


管理者ポータルでの移動

- 管理者ポータル (1 ページ)
- Cisco ISE 国際化およびローカリゼーション (19 ページ)
- MAC アドレスの正規化 (27 ページ)

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要要素を示します。



1	メニューのドロップダウン	<ul style="list-style-type: none"> • [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、ISE コミュニティへのリンク、ポータル ビルダーなどのオンライン 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。

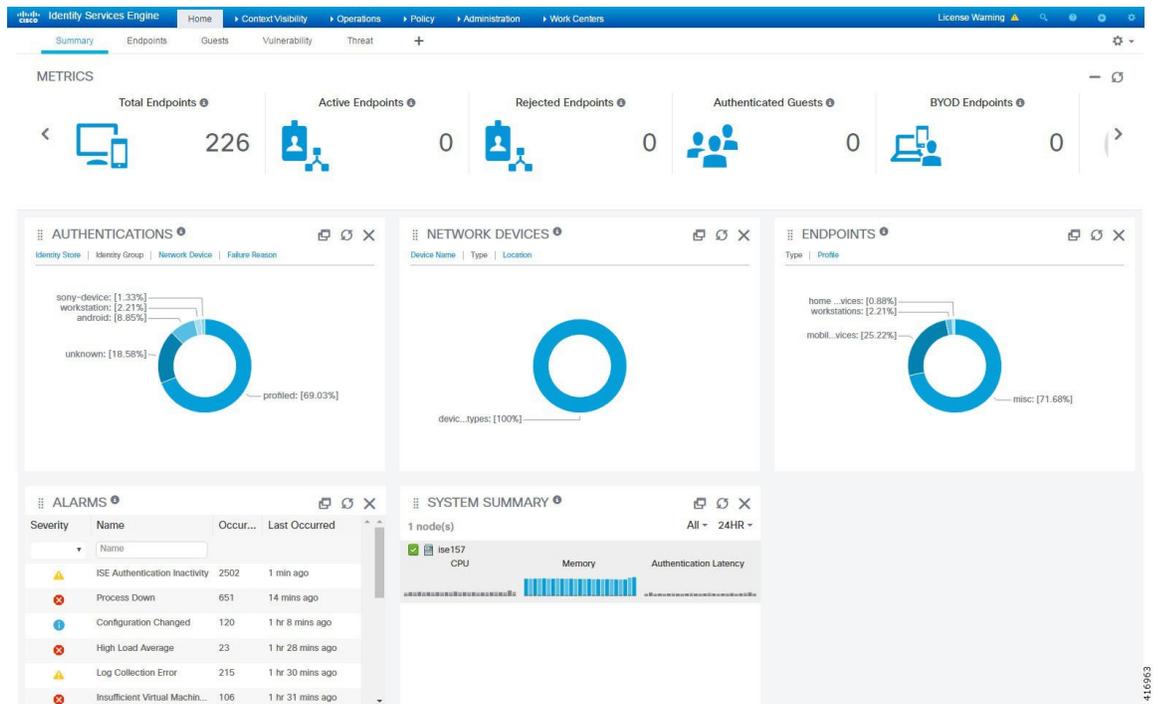
- **[可視性セットアップ (Visibility Setup)]** : **[可視性セットアップ (Visibility Setup)]** オプションは、アプリケーション、ハードウェアインベントリ、USB ステータス、ファイアウォール ステータス、Windows エンドポイントの全般的なコンプライアンス ステータスなどのエンドポイントデータを収集して Cisco ISE に送信する、価値の実証 (PoV) サービスです。ISE の **[可視性セットアップ (Visibility Setup)]** ウィザードを起動すると、IP アドレス範囲を指定して、ネットワークの特定セグメントまた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

		<p>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。</p> <ul style="list-style-type: none">• C:\WINDOWS\systemwow64\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) <p>• [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。</p> <ul style="list-style-type: none">•  オンライン ヘルプの起動とアカウント設定の指定を含む、システム アクティビティ。 アカウント設定
--	--	---

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。



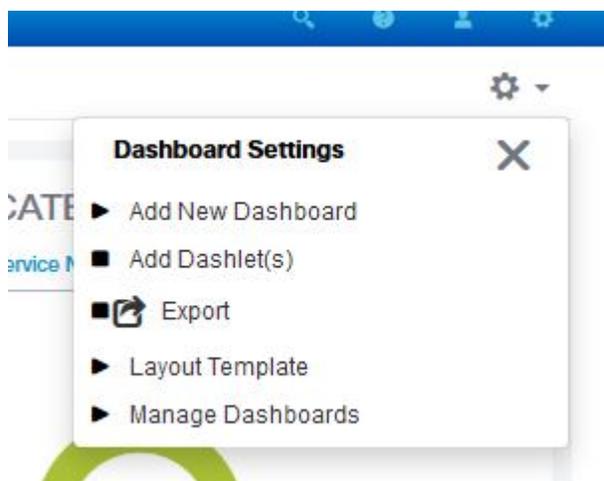
[ホーム (Home)] ページには、ISE データのビューを表示する 5 つのデフォルト ダッシュボードがあります。

- [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ることで実行します。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。詳細については、「[ハードウェアダッシュボード \(13 ページ\)](#)」の項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。



(注) ネットワーク デバイスに SNMPv3 パラメータを設定した場合、モニタリングサービス ([操作 (Operations)]>[レポート (Reports)]>[カタログ (Catalog)]>[ネットワーク デバイス (Network Device)]>[セッション ステータス概要 (Session Status Summary)]) によって提供されるネットワーク デバイスセッション ステータス概要レポートを生成できません。ネットワーク デバイスが SNMPv1 または SNMPv2c パラメータを使用して設定されている場合は、このレポートを正常に生成できます。

- [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。

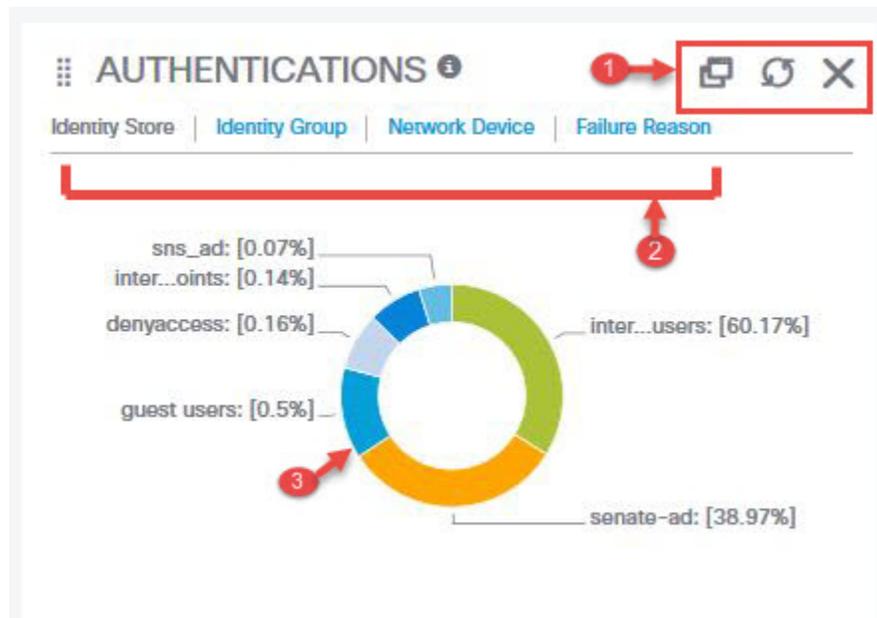
[コンテキストの可視性 (Context Visibility)] を使用してエンドポイント データを検索する方法の詳細については、Cisco YouTube ビデオを参照してください。このビデオでは ISE 2.1 <https://www.youtube.com/watch?v=HvonGhrydfg> を使用しています。

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

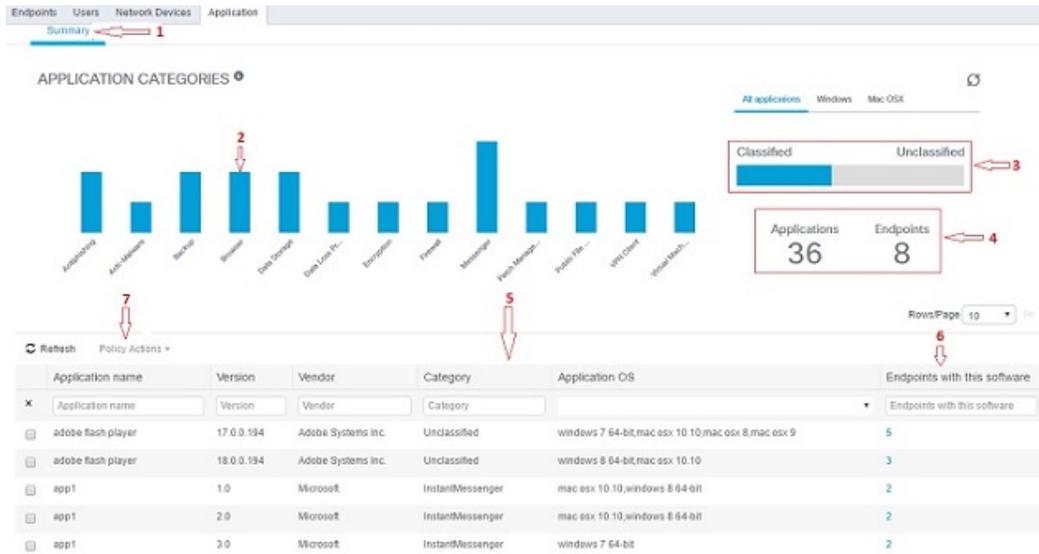
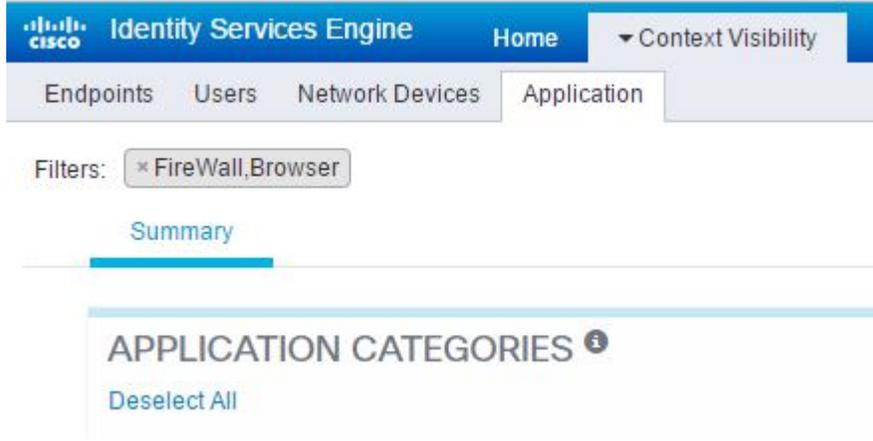


表 1: アプリケーション ダッシュボードの説明

ラベル	説明
1	<p>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。</p> <p>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)]、[メッセージング (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。</p>
2	<p>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。</p>
3	<p>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。</p>

ラベル	説明																								
4	<p>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。</p> 																								
5	<p>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。</p> <table border="1" data-bbox="483 1003 1485 1711"> <thead> <tr> <th>アプリケーション</th> <th>Version</th> <th>Vendor</th> <th>カテゴリ</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> </thead> <tbody> <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> </tbody> </table>	アプリケーション	Version	Vendor	カテゴリ	アプリケーション OS	このソフトウェアで使用するエンドポイント	Gatekeeper	9.9.5	Apple Inc.	マルウェア対策	windows 7 64ビット、mac osx 10.10、mac osx 8、mac osx 9	5	Gatekeeper	10.9.5	Apple Inc.	マルウェア対策	windows 8 64ビット、mac osx 10.10	3	ソフトウェア更新	2.3	Apple Inc.	パッチ管理	windows 7 64ビット、mac osx 10.10、mac osx 8、mac osx 9	5
アプリケーション	Version	Vendor	カテゴリ	アプリケーション OS	このソフトウェアで使用するエンドポイント																				
Gatekeeper	9.9.5	Apple Inc.	マルウェア対策	windows 7 64ビット、mac osx 10.10、mac osx 8、mac osx 9	5																				
Gatekeeper	10.9.5	Apple Inc.	マルウェア対策	windows 8 64ビット、mac osx 10.10	3																				
ソフトウェア更新	2.3	Apple Inc.	パッチ管理	windows 7 64ビット、mac osx 10.10、mac osx 8、mac osx 9	5																				
[6]	<p>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。</p>																								

ラベル	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。



- (注)
- [ハードウェアの可視性 (Hardware Visibility)] ページのクイック フィルタには、3 文字以上入力する必要があります。クイックフィルタを効率的に機能させるには、文字の入力後に他のカラム属性のフィルタをクリックする方法もあります。
 - 次の表はハードウェアに関連した属性に基づいたフィルタリングにのみ使用されるため、一部のカラム属性はグレー表示されています。
 - オペレーティングシステムのフィルタは、[製造元 (Manufacturers)] チャートにのみ適用されます。これは、次の表には関連しません。

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
- BIOS 製造元
- BIOS シリアル番号
- BIOS モデル
- 接続デバイス
- CPU 名
- CPU 速度 (GHz)
- CPU 使用率 (%)
- コア数
- プロセッサ数
- メモリ サイズ (GB)
- メモリ使用率 (%)
- 内部ディスクの合計サイズ (GB)
- 内部ディスクの合計フリー サイズ (GB)
- 内部ディスクの合計使用率 (%)
- 内部ディスク数
- NAD ポート ID
- ステータス
- ネットワークデバイス名
- 参照先

- UDID
- IPv4 アドレス
- ユーザ名
- ホストネーム
- OS タイプ
- 異常な動作
- エンドポイント プロファイル
- 説明
- エンドポイント タイプ
- ID グループ
- 登録日
- 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。

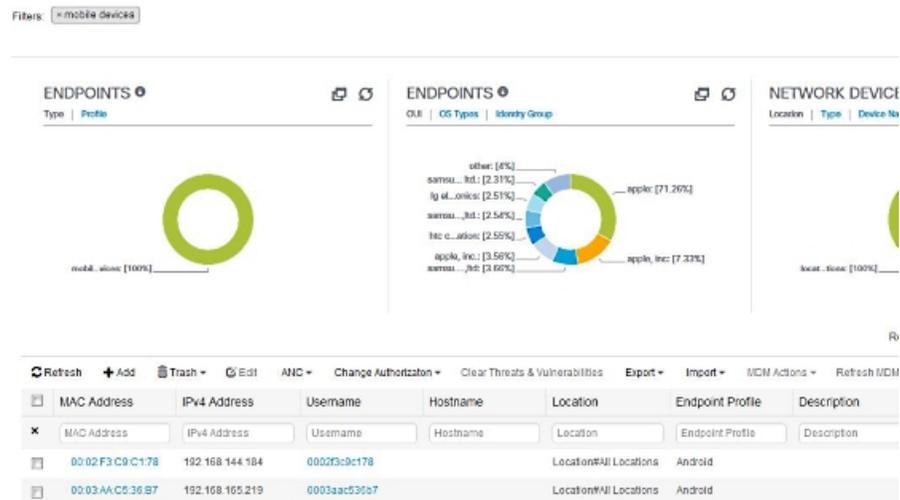
ハードウェア インベントリ データの収集間隔は、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [全般設定 (General Settings)] ページで制御できます。デフォルトの間隔は 5 分です。

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。



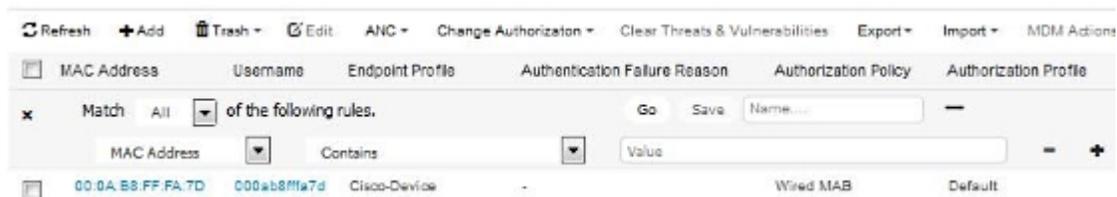
[エンドポイント (Endpoints)]ダッシュレットで[mobil...vices]をクリックすると、ページが再表示され、2つの[エンドポイント (Endpoints)]ダッシュレット、[ネットワークデバイス (Network Devices)]ダッシュレット、およびデータのリストが表示されます。次の例に示すように、ダッシュレットとリストにはモバイルデバイスのデータが表示されます。



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。

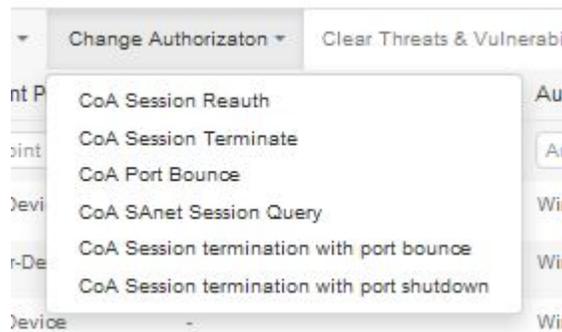


カスタムフィルタは保存できます。

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、の「Cisco ISE での適応型ネットワーク制御の有効化」のセクションを参照してください [Cisco ISE での適応型ネットワーク制御の有効化](#)。

- 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	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
オランダ語	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
韓国語	ko-kr
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 またはサブリカント、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ブリカントに依存します。一部の Windows ネイティブサブリカントでは、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トチャ評価

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。

ポストチャ要件を、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）。

サブ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、サブ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、サブリカントによって、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 サブリカントでは、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、サブ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。エンドユーザのサブ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のユーザ名と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	<ul style="list-style-type: none"> • [ユーザ名 (User name)] ユーザ名には、大文字と小文字、数字、スペース、特殊文字 (、%、^、;、:、[、{、 、}、]、\、'、"、=、<、>、?、!)、制御文字を除く) を自由に組み合わせて使用できます。スペースのみのユーザ名も許可されません。 • [名 (First name)] • [姓 (Last name)] • [電子メール (e-mail)]
ユーザリスト	<ul style="list-style-type: none"> • 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

管理者ポータル要素	UTF-8 フィールド
<p>ユーザ パスワード ポリシー</p>	<p>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せんが、制御文字は使用できません。</p> <p>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。</p> <ul style="list-style-type: none"> • 小文字の英文字 (Lowercase alphabetic characters) • 大文字の英文字
<p>管理者リスト</p>	<ul style="list-style-type: none"> • 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
<p>管理者ログイン ページ</p>	<ul style="list-style-type: none"> • [ユーザ名 (User name)]
<p>RSA</p>	<ul style="list-style-type: none"> • メッセージ • プロンプト
<p>RADIUS トークン</p>	<ul style="list-style-type: none"> • [認証 (Authentication)] タブ > [プロンプト (Prompt)]

管理者ポータル要素	UTF-8 フィールド
ポストチャ要件	<ul style="list-style-type: none"> • [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
ポストチャ条件	<ul style="list-style-type: none"> • [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	<ul style="list-style-type: none"> • [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	<ul style="list-style-type: none"> • [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)]
[操作 (Operations)]>[アラーム (Alarms)]>[ルール (Rule)]	<ul style="list-style-type: none"> • [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)]

管理者ポータル要素	UTF-8 フィールド
[操作 (Operations)]>[レポート (Reports)]	<ul style="list-style-type: none"> • [操作 (Operations)]>[ライブ認証 (Live Authentications)]>[フィルタ (Filter)] 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 (Report filter)] フィールド
[操作 (Operations)]>[トラブルシューティング (Troubleshoot)]	<ul style="list-style-type: none"> • [一般ツール (General Tools)]>[RADIUS 認証トラブルシューティング (RADIUS Authentication Troubleshooting)]>[ユーザー名 (Username)]
ポリシー	<ul style="list-style-type: none"> • [認証 (Authentication)]>ポリシー条件内での av 式の値 • [許可 (Authorization)]/[ポストチャ (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	<ul style="list-style-type: none"> • [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。ACS から ISE への移行についての詳細は、お使いの ISE バージョンの『[Cisco Secure ACS to Cisco ISE Migration Tool](#)』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 ユーザー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。