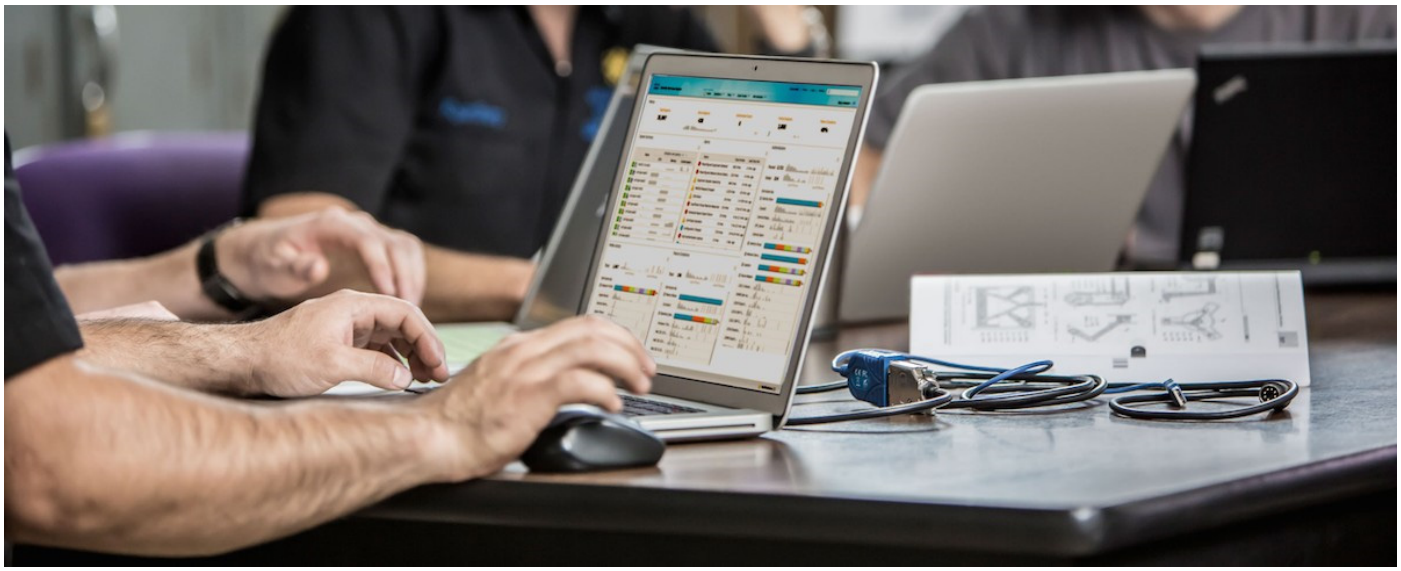


Cisco ISE の統合とモニタリング Splunk のユーザ デバイス コンテキスト

セキュア アクセスを実現するハウツー ガイド シリーズ

作成者：John Eppich

日付：2014 年 11 月

目次

はじめに

シスコ セキュア アクセスを実現するハウツー ガイドについて

シリーズのハウツー ドキュメントは、シスコ セキュア アクセスの導入におけるベスト プラクティスを説明するために、シスコ セキュア アクセス チームによって作成されています。このシリーズのドキュメントは相互に関連して作られており、シスコ セキュア アクセス ソリューションの導入を成功させるのに役立ちます。これらのドキュメントを参照することで、所定のパスに従ってシステム全体を展開したり、もしくは特定のニーズに合う個別の使用例を調べたりすることができます。

概要

このドキュメントは、ISE 用 Splunk アドオンを導入しているシスコのフィールド、パートナー、および顧客に向けて用意されています。このドキュメントでは、次に要約するように、すべてのダッシュボード、パネルおよび検索文字列フィールドについて詳しく説明します。ISE 管理者は、ISE 用の Splunk アドオンを使用して、以下のことを行います。

- 認証、ポスチャ、プロファイル済みデバイス、クライアント プロビジョニング、準拠/非準拠デバイス、ゲスト、ISE の正常性、ポスチャなどの、ISE 機能に関する詳細レポートを提供する。
- 企業のアイデンティティ セキュリティ ポリシーに準拠し、イベントに関するコンテキスト情報を提供する。
- ISE システム管理に操作ビューを提供する。

ISE と Splunk の統合により提供される使用例と機能の概要については、Cisco.com の「ISE Splunk At-a-Glance」のドキュメントを参照してください。

これは包括的なドキュメントで、全体をそのまま使用するか、あるいは ISE 向け Splunk アドオンの特定分野に関する参照資料として使用することもできます。ドキュメント内で最も関連性の高いセクションをすばやく見つけるには、目次を参照してください。

図 1.

EPS（エンドポイント保護サービス）のワークフロー アクションは、Splunk で作成されます。EPS ワークフローは特定のイベントに関連付けられています。これらのイベントは、IP アドレス別にデバイスを隔離し、MAC アドレス別にデバイスを隔離解除する際に、ISE REST API をトリガーします。

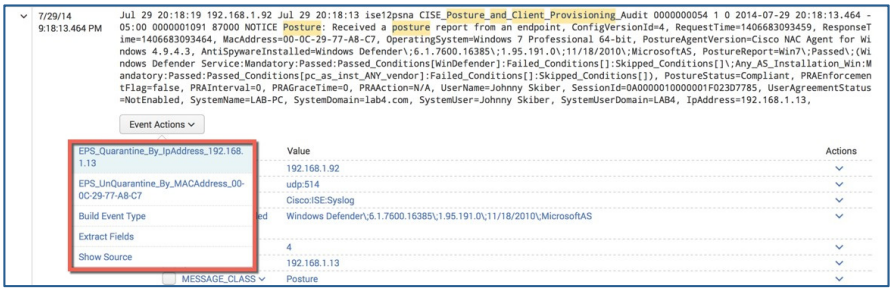


図 2.

読者は、Splunk と Cisco Identity Services Engine に精通している必要があります。

Splunk ISE モニタリング Syslog 番号は、有効な ISE ロギング カテゴリから推計される Splunk Syslog イベント数の推定値を表します。

要件

開始する前に、Splunk と ISE がインストールされていることを確認します。

要件は次のとおりです。

- Splunk Enterprise 6.1.2 以降
- 最新のパッチを含む ISE 1.2 ビルド 899 以降
- ISE バージョン 2.0.3 以降に対応した ISE 用 Splunk アドオン
- Splunk と ISE がインストール済みであることを前提としています。
- エンドポイント保護サービス（EPS）の有効な ISE Advanced ライセンス

Splunk の基礎

検索文字列フィールド

このセクションでは、このドキュメントで使用される検索文字列コマンドについて説明します。検索文字列コマンドはイベント フィールド情報を抽出し、ソース タイプを定義することから始まります。次にリストするソース タイプと、このドキュメント全体を通したソース タイプは eventtype です。eventtype は、分類された、またはタグ付けされたイベントです。この場合、eventtype は、syslog イベントを定義するさまざまな ISE MESSAGE コードで構成されます。ISE の eventtype と MESSAGE コードのリストには、ISE 用の Splunk アドオン（[設定（Settings）] -> [イベントタイプ（Event types）]）からアクセスできます。このリストのスクリーンショットは、「イベントタイプ」のセクションでも記載されています。

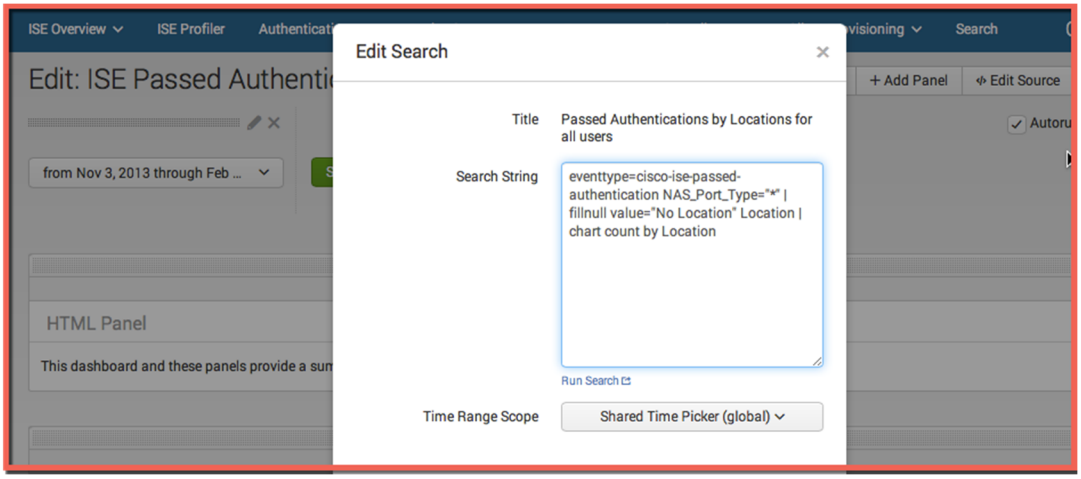


図 3.

また、eventtype を、CISE_Passed_Authentications や MESSAGE_code 5200 などの実際の ISE ロギング カテゴリに置き換えてテストすることもできます。

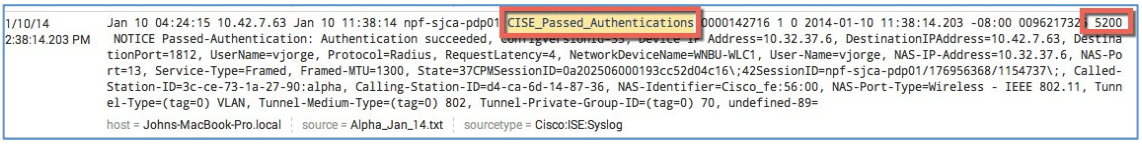


図 4.

Syslog イベントに基づいて、検索文字列フィールドを変更できます。

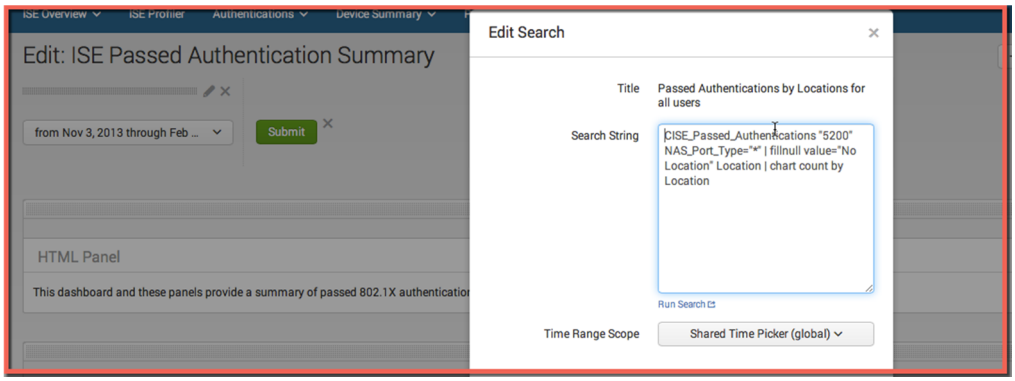


図 5.

表示される可能性があるその他の検索文字列記号とフィールドは次のとおりです。

- | パイプ バーは検索を構成する個々のコマンドを区切ります。
- **search** コマンドは、一連の結果にフィルタリングを適用します。たとえば、検索文字列 | **search NAS_Port_Type=”virtual”** は、**仮想ユーザ**についてのみ結果を取得します。
- **stats count by** コマンドは、イベント フィールドの統計数や集約数を提供します。円グラフと統計情報テーブル ビューも同じコマンドを使用して構築されます。これによって、検索結果を円グラフの割合として、または検索結果の数として視覚的に確認できます。たとえば、**| stats count by location** では、ロケーション フィールドに基づいて円グラフまたは統計情報テーブル ビューが提供されます。
- **fields** コマンドを使用すると、検索からフィールドを削除できます。たとえば、**| fields - _raw** を使用すると、検索から _raw フィールドが削除されます。また、検索でフィールドを保持することもできます。**| fields host** を使用すると、検索結果でホスト フィールドが保持されます。
- **rex** コマンドは、値が特定の正規表現と一致するフィールドを抽出します。たとえば、**rex "SystemUser=(?<SystemUser>.\w+)"** は、「.\w+」を使用して raw イベント SystemUser ユーザ フィールドを抽出します。これにより、単語に使用される文字が抽出されます。また、「.\w+」は「.*」に置き換えることができます。この場合には、IP アドレスを含んだフィールドの抽出に使用できる文字列全体が含まれます。

イベント タイプ

イベント タイプを使用して、イベントをイベント タイプにタグ付けしたり分類したりすることができます。

たとえば、eventtype の検索文字列 cisco-ise-provision-succeeded は、実際の検索文字列フィールド eventtype=cisco-ise “client provisioning succeeded” に対応します。

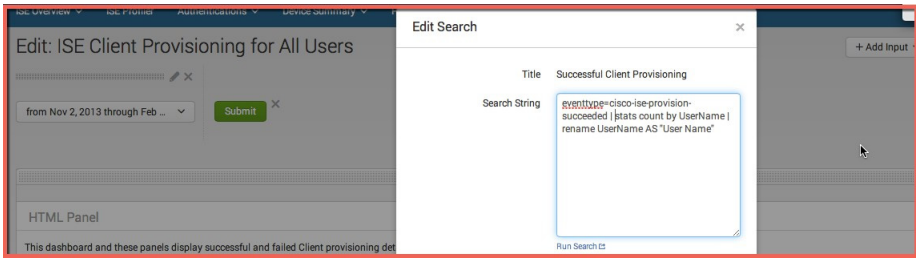
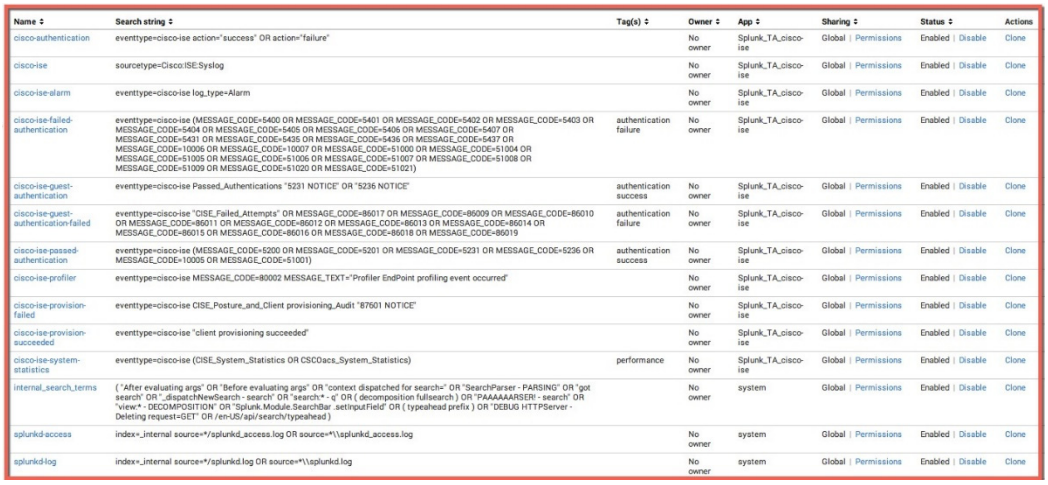


図 6.

Splunk/ISE 間のアドオンの完全なイベント タイプのリストを表示するには、[設定（settings）] -> [イベントタイプ（event types）] を選択します。



Name	Search string	Tag(s)	Owner	App	Sharing	Status	Actions
cisco-authentication	eventtype=cisco-ise action="success" OR action="failure"		No owner	Splunk_TA_cisco-ise	Global | Permissions	Enabled | Disable	Clone
cisco-ise	sourcetype=Cisco:ISE:Syslog		No owner	Splunk_TA_cisco-ise	Global | Permissions	Enabled | Disable	Clone
cisco-ise-alarm	eventtype=cisco-ise log_type=Alarm		No owner	Splunk_TA_cisco-ise	Global | Permissions	Enabled | Disable	Clone
cisco-ise-failed-authentication	eventtype=cisco-ise (MESSAGE_CODE=5400 OR MESSAGE_CODE=5401 OR MESSAGE_CODE=5402 OR MESSAGE_CODE=5403 OR MESSAGE_CODE=5404 OR MESSAGE_CODE=5405 OR MESSAGE_CODE=5406 OR MESSAGE_CODE=5407 OR MESSAGE_CODE=5431 OR MESSAGE_CODE=5435 OR MESSAGE_CODE=5436 OR MESSAGE_CODE=5437 OR MESSAGE_CODE=10006 OR MESSAGE_CODE=10007 OR MESSAGE_CODE=51000 OR MESSAGE_CODE=51004 OR MESSAGE_CODE=51005 OR MESSAGE_CODE=51006 OR MESSAGE_CODE=51007 OR MESSAGE_CODE=51008 OR MESSAGE_CODE=51009 OR MESSAGE_CODE=51020 OR MESSAGE_CODE=51021)	authentication failure	No owner	Splunk_TA_cisco-ise	Global | Permissions	Enabled | Disable	Clone
cisco-ise-guest-authentication	eventtype=cisco-ise Passed_Authentications "5231 NOTICE" OR "5236 NOTICE"	authentication success	No owner	Splunk_TA_cisco-ise	Global | Permissions	Enabled | Disable	Clone
cisco-ise-guest-authentication-failed	eventtype=cisco-ise "CISE_Failed_Attempts" OR MESSAGE_CODE=86017 OR MESSAGE_CODE=86009 OR MESSAGE_CODE=86010 OR MESSAGE_CODE=86011 OR MESSAGE_CODE=86012 OR MESSAGE_CODE=86013 OR MESSAGE_CODE=86014 OR MESSAGE_CODE=86015 OR MESSAGE_CODE=86016 OR MESSAGE_CODE=86018 OR MESSAGE_CODE=86019	authentication failure	No owner	Splunk_TA_cisco-ise	Global | Permissions	Enabled | Disable	Clone
cisco-ise-passed-authentication	eventtype=cisco-ise (MESSAGE_CODE=5200 OR MESSAGE_CODE=5201 OR MESSAGE_CODE=5231 OR MESSAGE_CODE=5236 OR MESSAGE_CODE=10005 OR MESSAGE_CODE=51001)	authentication success	No owner	Splunk_TA_cisco-ise	Global | Permissions	Enabled | Disable	Clone
cisco-ise-profiler	eventtype=cisco-ise MESSAGE_CODE=80002 MESSAGE_TEXT="Profiler EndPoint profiling event occurred"		No owner	Splunk_TA_cisco-ise	Global | Permissions	Enabled | Disable	Clone
cisco-ise-provision-failed	eventtype=cisco-ise CISE_Posture_and_Client provisioning_Audit "87501 NOTICE"		No owner	Splunk_TA_cisco-ise	Global | Permissions	Enabled | Disable	Clone
cisco-ise-provision-succeeded	eventtype=cisco-ise "client provisioning succeeded"		No owner	Splunk_TA_cisco-ise	Global | Permissions	Enabled | Disable	Clone
cisco-ise-system-statistics	eventtype=cisco-ise (CISE_System_Statistics OR CSCOacs_System_Statistics)	performance	No owner	Splunk_TA_cisco-ise	Global | Permissions	Enabled | Disable	Clone
internal_search_terms	("After evaluating args" OR "Before evaluating args" OR "context dispatched for search=" OR "SearchParser - PARSING" OR "got search" OR "_dispatchNewSearch - search" OR "search:* - q" OR (decomposition fullsearch) OR "PAAAAAARSER - search" OR "view:* - DECOMPOSITION" OR "Splunk.Module.SearchBar .setInputField" OR (typeahead prefix) OR "DEBUG HTTPServer - Deleting request=GET" OR /en-US/api/search/typeahead)		No owner	system	Global | Permissions	Enabled | Disable	Clone
splunkd-access	index=_internal source=*/splunkd_access.log OR source=*\\splunkd_access.log		No owner	system	Global | Permissions	Enabled | Disable	Clone
splunkd-log	index=_internal source=*/splunkd.log OR source=*\\splunkd.log		No owner	system	Global | Permissions	Enabled | Disable	Clone

図 7.

技術概要

pxGrid コントローラは、すべてのクライアント認証、承認、機能/トピックおよびそれらのサブスクリプション リストを管理します。pxGrid コントローラは、管理を含んだクライアント通信のすべての制御面のコントロールと、相互信頼と承認適用を伴うその他の参加クライアントの制御を行います。

pxGrid パブリッシャは、pxGrid サブスクライバまたは pxGrid クライアントが消費または「登録」する関心のあるトピックや機能を提供します。クライアントは、承認済みセッション、EPS（エンドポイント保護サービス）、または基本グループとして認証および承認のために pxGrid コントローラに登録します。これは相互認証を通じて発生します。クライアントは承認されると、これらの機能に登録して、pxGrid API スクリプトに基づいてコンテキスト情報を取得できます。

ほとんどの場合、クライアントはセッション グループまたは EPS グループに登録します。セッション グループでは、クライアントは異なる機能に登録できます。EPS グループはセッションへのスーパーセット グループであり、クライアントは EPS アクションを実行する EndpointProtectionService 機能に登録できます。基本グループでは、pxGrid 上でのいかなる操作の権限もクライアントに対して与えないので、承認済みセッションに配置可能にするには pxGrid 管理者からの手動承認が必要です。管理者グループは設定できず、MnT パブリッシャや PAP UI などの ISE ノード用に予約されています。また、他のグループから他のアクションを実行できます。

ISE 1.3 は、あらかじめ用意された機能付きで出荷されます。

- **SessionDirectory**：pxGrid セッション オブジェクトの ISE セッション ディレクトリ内にある既存の属性を公開します。
  - セッション状態、IP アドレス、ユーザ名、ユーザの AD ドメイン、MAC、NAS IP アドレス、Trustsec セキュリティ グループ名、エンドポイント プロファイル名、（ポリシー名のプロファイリング）、ポスチャ ステータス、監査セッション ID、アカウント セッション IP（RADIUS AV ペア内、最終更新日時）
- **EndointProfileMetadataCapability**：ISE のプロファイリング ポリシーを公開します。これらのポリシーの追加/削除/更新はこの機能を通じて通知されます。
  - id/name/fully-qualified name
- **TrustsecMetadataCapability**：ISE で設定された TrustSec セキュリティ グループ メタデータを公開します。
  - TrustSec タグ名、固有識別子、説明と値
- **EndpointProtectionService**：EPS 隔離/隔離解除 API を公開します。

pxGrid クライアントは Linux のホストで、ISE の pxGrid コントローラに接続および登録します。これは、ISE プライマリ ノードの pxGrid ペルソナとして有効になります。pxGrid クライアントが正常に登録されると、Java サンプル スクリプトは、認証されたユーザ セッションを対象とする Linux ホストからになります。これらのスクリプトによって pxGrid API が明らかになり、これらのスクリプトの結果はリアルタイムで通知として表示できます。これは pxGrid サンプル スクリプトとともにこのドキュメント全体で示されています。

ルックアップ アクション

Splunk のルックアップ機能では、イベント データのフィールドに一致する外部の .csv ファイルを、フィールドとして参照します。これは、ロケーション ベースのダッシュボードとパネルの中で使用されます。

ロケーションに固有のパネルが表示されていない場合は、[ナレッジ（Knowledge）] -> [検索とレポート（Searches and Reports）] -> [ルックアップ-ロケーション（Lookup-Locations）] -> [実行（Run）] と進み、関連付けられているパネルで「ロケーション」を選択できます。

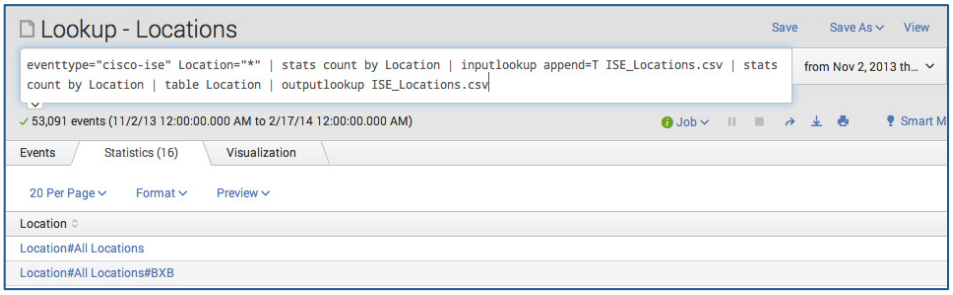


図 8.

折りたたみ式円グラフ

円グラフでその他（x）が表示される場合は、しきい値レベルを 0 に変更する必要があります。

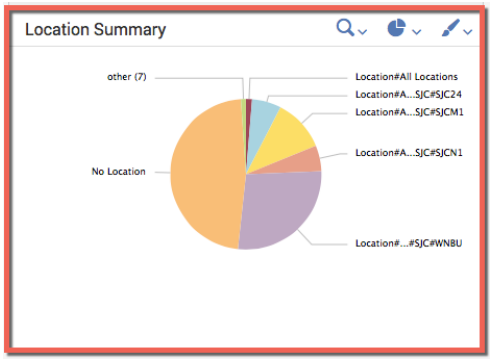


図 9.

ソース パネルを編集し、<option… “charting.chart.sliceCollapsingThreshold”>**0**</option> に変更する必要があります。

```
<chart>
  <title>Location Summary</title>
  <searchTemplate>eventtype=cisco-ise MESSAGE_CLASS="Passed-Authentication" | fillnull value="No Location" Location | stats cc
  <option name="charting.axisTitleX.visibility">visible</option>
  <option name="charting.axisTitleY.visibility">visible</option>
  <option name="charting.axisX.scale">linear</option>
  <option name="charting.axisY.scale">linear</option>
  <option name="charting.chart">pie</option>
  <option name="charting.chart.nullValueMode">gaps</option>
  <option name="charting.chart.sliceCollapsingThreshold">0</option>
  <option name="charting.chart.stackMode">default</option>
  <option name="charting.chart.style">shiny</option>
  <option name="charting.drilldown">all</option>
  <option name="charting.layout.splitSeries">0</option>
  <option name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</option>
  <option name="charting.legend.placement">right</option>
</chart>
```

図 10.

ISE の概要

この項では、ISE システムとユーザ認証の両面から日常業務の ISE メンテナンス ビューについて説明します。これには、ISE ノードの円滑な動作を確保するための、ISE アラーム イベントの受信や、CPU 使用率およびメモリ使用率などの ISE システムの正常性のモニタリングが含まれます。また、認証やプロトコル ルールの表示や、ロケーションごとの認証によって、成功および失敗したユーザ認証にも対応します。このセクションを通読することで、システム パフォーマンスおよびユーザ認証の問題が発生したときに、その問題を識別できるようになります。その後、特定のイベントにドリル ダウンしたり、別のダッシュボードを選択してより詳細な情報を取得したりすることができます。

ISE の概要は次のダッシュボードから構成されています。

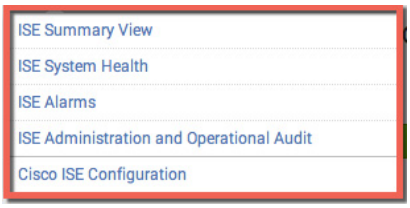


図 11.

- [ISE 概要ビュー(ISE summary View)]:ISE イベント、ロケーション別の成功した認証、プロトコル ルール別の成功/失敗した認証について、それぞれ要約が提供されます。
- [ISE システムの正常性(ISE System Health)]:ノードあたりの CPU 使用率、メモリ使用率、ディスク使用率の統計情報が提供されます。
- [ISE アラーム(ISE Alarms)]:MESSAGE コードによって決定される ISE アラーム情報が提供されます。
- [ISE の管理および操作の監査(ISE Administration and Operational Audit)]:詳細な管理および操作のメッセージが提供されます。
- [Cisco ISE の設定(Cisco ISE Configuration)]:Splunk と ISE の設定の手順を示します。これには、ISE カテゴリの有効化が含まれます。

[ISE 概要ビュー(ISE Summary View)] ダッシュボード

ISE の概要ダッシュボードは、[ISE イベント(ISE Events)]、[ロケーションサマリー(Location Summary)]、[プロトコルルール別の失敗(Failures by Protocol Rule)]、[プロトコルルール別の成功した認証(Passed Auths by Protocol Rule)]、[トップ アラーム(Top Alarms)]、[認証概要(Authentication Summary)] で構成されます。このダッシュボードは通常、ISE 日次イベントへのクイック操作ビューを提供するために、ISE 管理者によって使用されます。

ISE イベント(ISE Events)

[ISE イベント(ISE Events)] パネルでは、さまざまな MESSAGE コードに基づいて受信された ISE イベントのタイムチャートが示されます。

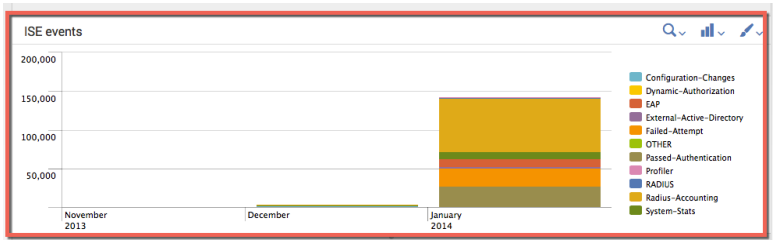


図 12.

検索文字列フィールド:

```
eventtype=cisco-ise | timechart usenull=f count by MESSAGE_CLASS
```

ロケーションサマリー(Location Summary)

この円グラフ ビューには、ロケーション別の成功した数と割合が示されます。このダッシュボードを使用して、ISE 管理者は、ユーザ認証の大部分がどのロケーションに由来しているかを認識できます。次の例では、ほとんどの認証が No Location ネットワーク グループに由来しています。No Location は、ネットワーク デバイスが ISE に追加された際に、ロケーションが選択されていないことに由来します。

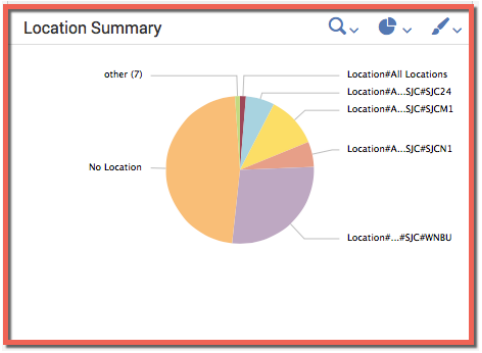


図 13.

検索文字列フィールドは次のとおりです。

```
eventtype=cisco-ise MESSAGE_CLASS="Passed-Authentication" | fillnull value="No Location" Location | stats
count by Location
```

プロトコルルール別の失敗(Failures by Protocol Rule)

[プロトコルルール別の失敗(Failures by Protocol Rule)] 横棒グラフには、認証ルール別に失敗した認証の上位 20 のイベントが表示されます。このダッシュボードは通常管理者によって使用され、ユーザ認証の失敗の診断に役立ちます。次のグラフでは、Dot1x ルールが認証失敗の主な原因です。管理者はこれらのイベントにドリルダウンして詳細を提供したり、これらの失敗へのユーザのコンテキスト情報を取得するために [失敗した試行(Failed Attempts)] ダッシュボードの選択を選んだりすることができます。

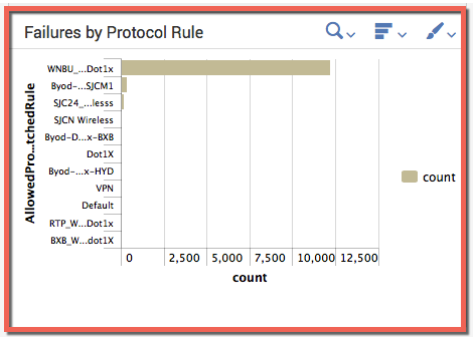


図 14.

検索文字列フィールド:

```
eventtype=cisco-ise MESSAGE_CLASS="Failed-Attempt"| top limit=20 AllowedProtocolMatchedRule
```

プロトコルルール別の成功した認証(Passed Authentications by Protocol Rule)

[プロトコルルール別の成功した認証(Passed Authentications by Protocol Rule)] 横棒グラフには、認証ルール別に成功した認証の上位 20 のイベントが表示されます。このダッシュボードは通常、認証プロトコル ルール別に成功した認証を識別または測定するために管理者によって使用されます。この例では、イベント数のほとんどが、次の DOT1x ルールで占められています。管理者はドリルダウンしてプロトコル ルールの詳細を取得したり、またはこれらのイベントに関するコンテキストデータを提供するために [成功した認証(Passed Authentications)] ダッシュボードの選択を選んだりすることができます。

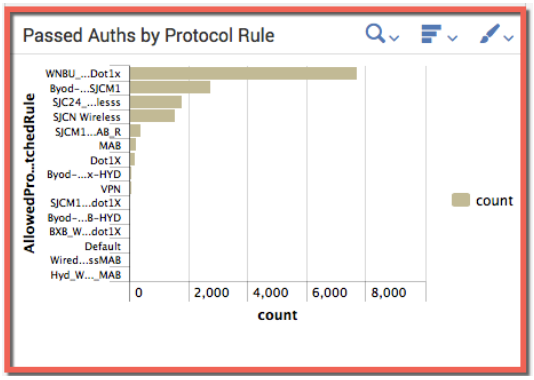


図 15.

検索文字列フィールド:

```
eventtype=cisco-ise MESSAGE_CLASS="Passed-Authentication"| stats count by AllowedProtocolMatchedRule | sort -
count
```

トップアラーム(Top Alarms)

[トップアラーム(Top Alarms)] 横棒グラフでは、ISE によって生成されたアラームにより生成されたイベント数のソートと表示が行われます。このダッシュボードは通常管理者によって使用され、ISE ノードまたはネットワーク環境の障害の診断に役立ちます。次の例では、NTP 同期障害にほとんどのイベントが含まれており、ISE と NTP サーバ間で時間同期エラーが発生したことを示しています。これによって ISE が AD ドメインに参加できなくなる場合があり、ユーザ認証の失敗が発生します。

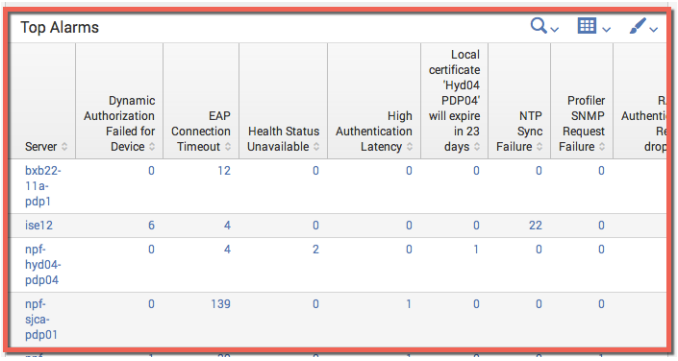


図 16.

検索文字列フィールド:

```
eventtype=cisco-ise vendor_action=Alarm | chart usenull=f count by Server, alarm_description | sort -count
```

認証概要（Authentication Summary）

[認証概要（Authentication Summary）] 縦棒グラフでは、成功/失敗した認証/承認ルールのビューが示されます。これは、ISE の [成功した認証（Passed Authentications）] および [失敗した試行（Failed Attempts）] カテゴリの MESSAGE コードに基づいています。このダッシュボードは通常、特定のイベントにドリルダウンすることによって認証エラーを診断するために、管理者によって使用されます。次の例では、管理者は認証に失敗したルールにドリルダウンできます。またはその後に [失敗した試行（Failed Attempts）] ダッシュボードを選択して、イベントに関するユーザのコンテキスト情報を提供し、失敗した認証への詳細な情報を入手することができます。

ISE ロギング カテゴリの説明については、[ISE の概要（ISE Overview）] -> [Cisco ISE の設定（Cisco ISE Configuration）] に移動します。

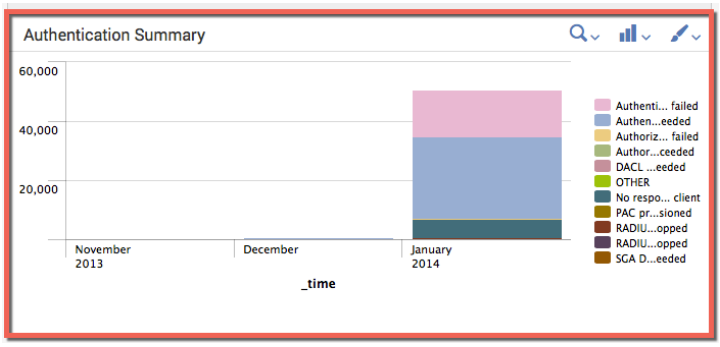


図 17.

検索文字列フィールド:

```
eventtype=cisco-ise MESSAGE_CLASS=Passed-Authentication OR MESSAGE_CLASS=Failed-Attempt | timechart count by
MESSAGE_TEXT
```

ISE システムの正常性（ISE System Health）

[システムの正常性（System Health）] ダッシュボードとパネルには、CPU 使用率、メモリ使用率、ディスク領域使用率、認証遅延、およびノードあたりの CPU 数に基づく ISE ノードのメンテナンス ビューが提供されます。このダッシュボードは通常、ISE ノード パフォーマンスを測定するために管理者によって使用されます。

CPU 使用率（CPU Utilization）

[CPU 使用率（CPU Utilization）] タイム チャートでは、ISE ノードあたりの CPU パフォーマンスがパーセンテージで測定されます。

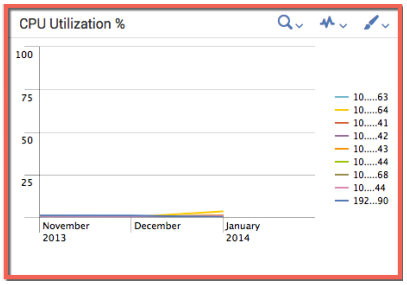


図 18.

検索文字列フィールド：

```
eventtype=cisco-ise MESSAGE_CLASS="System-Stats" ise_servername="$ise_server$" | timechart
avg(SysStatsUtilizationCpu) as "% Utilized" by ise_servername | rename ise_servername AS "ISE Server"
```

メモリ使用率（Memory Utilization）

[メモリ使用率（Memory Utilization）] タイム チャートでは、ISE ノードあたりのメモリ パフォーマンスがパーセンテージで測定されます。

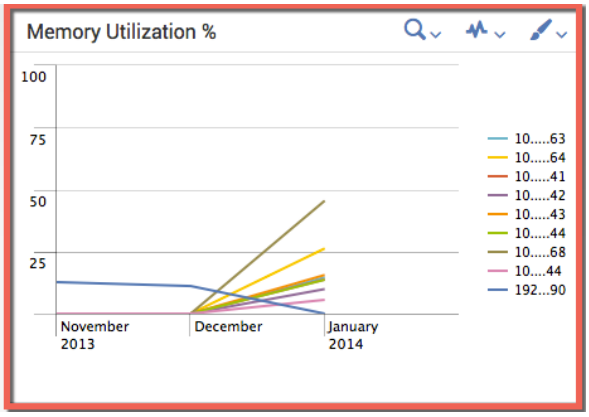


図 19.

検索文字列フィールド：

```
eventtype=cisco-ise MESSAGE_CLASS="System-Stats" ise_servername="$ise_server$" | timechart
avg(SysStatsUtilizationMemory) as "% Utilized" by ise_servername | rename ise_servername AS "ISE Server"
```

ディスク領域使用率（Disk Space Usage）

[ディスク領域使用率（Disk Space Usage）] タイム チャートでは、ISE ノードあたりのディスク使用率がパーセンテージで測定されます。

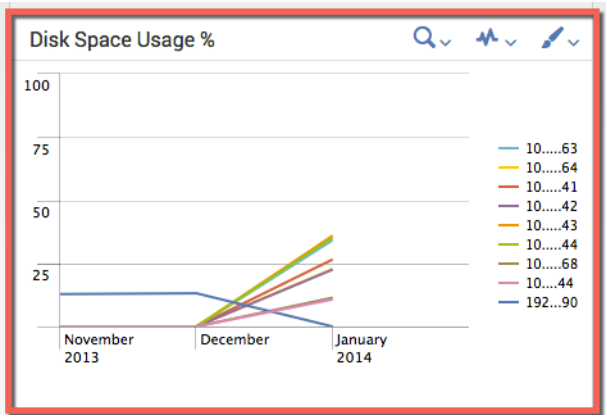


図 20.

検索文字列フィールド：

```
eventtype=cisco-ise MESSAGE_CLASS="System-Stats" ise_servername="$ise_server$" | timechart
avg(SysStatsUtilizationDiskSpace) as "% Utilized" by ise_servername | rename ise_servername AS "ISE Server"
```

認証遅延（Auth Latency）

[認証遅延（Auth Latency）] タイム チャートでは、ISE ノードあたりの平均 RADIUS 遅延が測定されます。このダッシュボードは通常、認証数やプロファイラ アクティビティなどの負担のかかるリソースを測定するために、ISE 管理者によって使用されます。

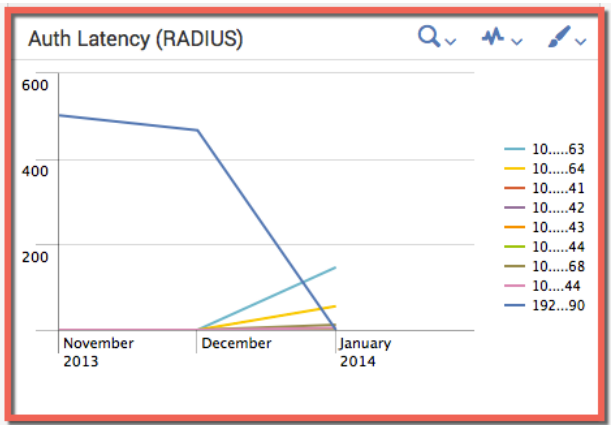


図 21.

検索文字列フィールド：

```
eventtype=cisco-ise MESSAGE_CLASS="System-Stats" ise_servername="$ise_server$" | timechart
avg(AverageRadiusRequestLatency) as Seconds by ise_servername | rename ise_servername AS "ISE Server"
```

認証遅延（Auth Latency）

TACACS の認証遅延は ISE には適用されません。

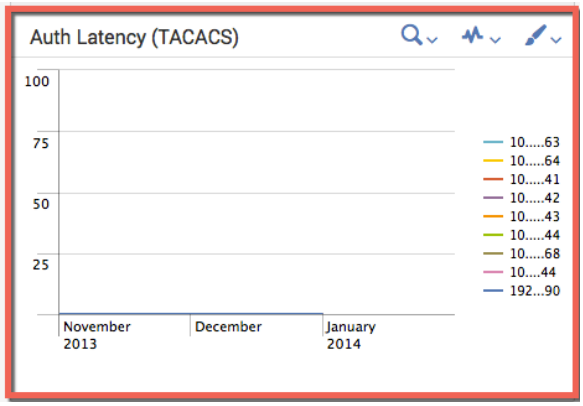


図 22.

検索文字列フィールド:

```
eventtype=cisco-ise MESSAGE_CLASS="System-Stats" ise_servername="$ise_server$" | timechart
avg(AverageTacacsRequestLatency) as Seconds by ise_servername | rename ise_servername AS "ISE Server"
```

ISE サーバあたりの CPU の数（Number of CPUs per ISE Server）

[ISE サーバあたりの CPU の数（Number of CPUs per ISE Server）] タイム チャートには、ISE ノードあたりの CPU 数が表示されます。このダッシュボードは通常、ISE に何らかのパフォーマンスの問題の可能性がある場合に CPU リソースをチェックするために、ISE 管理者によって使用されます。

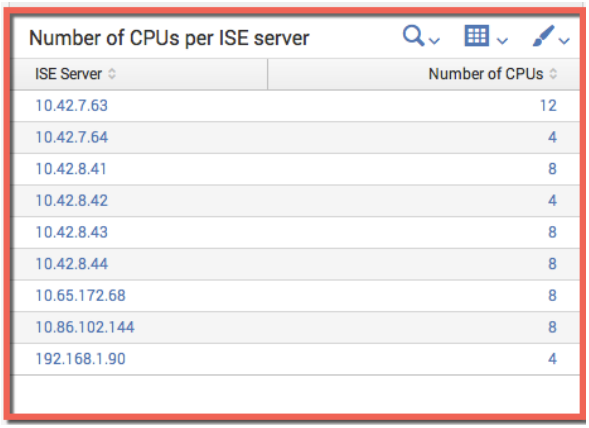


図 23.

検索文字列フィールド:

```
eventtype=cisco-ise MESSAGE_CLASS="System-Stats" SysStatsCpuCount="*" ise_servername="$ise_server$" | stats
max(SysStatsCpuCount) as "Number of CPUs" by ise_servername | rename ise_servername AS "ISE Server" | head 10
```

ISE アラーム(ISE Alarms)

[ISE アラーム(ISE Alarms)] ダッシュボードとパネルでは、[重要(CRITICAL)]、[情報(INFO)]、[警告(WARN)] の重大度に基づいてこれらのアラームの操作ビューが提供されます。

アラーム操作ビュー(Alarms Operational View)

[アラーム操作ビュー(Alarms Operational View)] 円グラフは、アラームの重大度の割合と数を表します。このダッシュボードは通常、ISE のパフォーマンスに影響を与える可能性がある重要なイベントを識別するために ISE 管理者によって使用されます。次の例では、[アラームの詳細(Alarm details)] ドロップダウンを選択することで、重要な詳細が取得されます。

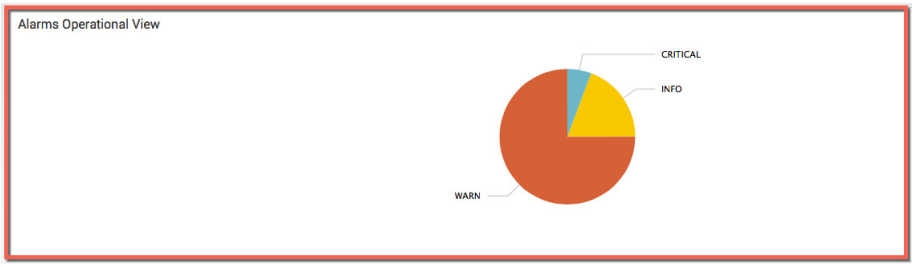


図 24.

検索文字列フィールド:

```
eventtype=cisco-ise-alarm |
        stats count by alarm_type |
        rename alarm_type AS "Alarm Type"
```

アラームの詳細(Alarm Details)

[アラームの詳細(Alarm Details)] ドロップダウン テーブルでは、これらの分類されたイベントのドリルダウンが提供されます。

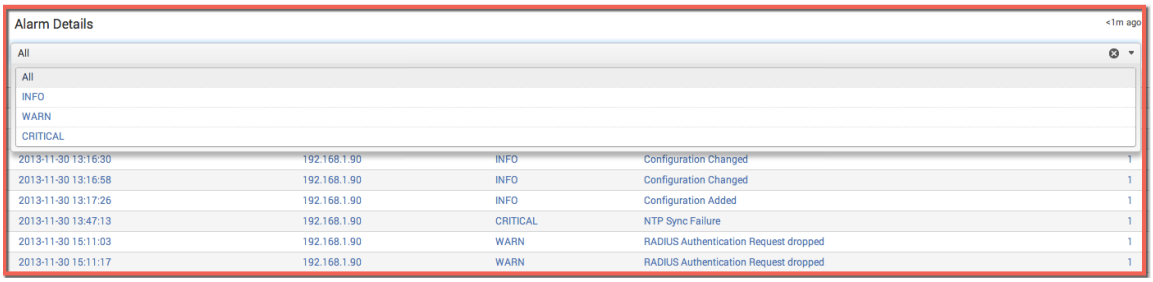


図 25.

検索文字列フィールド:

```
eventtype=cisco-ise-alarm alarm_type="$alarm_type$" |
stats count by _time ise_servername alarm_type alarm_description |
`format_field_names`
```

ISE 管理および操作の監査(ISE Administrational And Operational Audit)

[ISE 管理および操作の監査(ISE Administrational And Operational Audit)] ダッシュボードでは、ISE によって生成されるアラートへの操作ビューが提供されます。このダッシュボードは、通常、ISE の重要なシステム変更を識別するために ISE 管理者によって使用されます。重要なシステム変更には、ロックアウト/無効のアカウント、バックアップ/復元のエラーメッセージ、認証局(CA)サービス メッセージ、DNS 障害、MDM メッセージ、NTP サービス、パッチの成功/失敗、フィード サービス、ポスチャの更新などが含まれます。これにより、管理者は ISE の維持管理、起こり得る疑わしいアクティビティの有無の確認ができます。

システム管理操作ビュー(System Management Operational View)

[システム管理操作ビュー(System Management Operational View)] 円グラフは、ISE の管理および操作ロギング カテゴリに基づいて、ISE によって生成されるアラートの割合、数および説明を表示します。このダッシュボードは通常、すべてのイベントのクイックドリルダウンを提供し、起こり得る疑わしい動作に対する可視性を提供するために ISE 管理者によって使用されます。

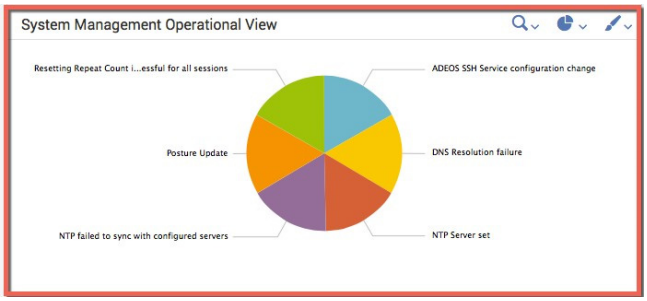


図 26.

検索文字列フィールド:

```
eventtype=cisco-ise log_type=Administrative_and_Operational_Audit System-management | stats count by
system_mgmt_desc MESSAGE_CODE
```

ホスト別の表示(View by Hosts)

[ホスト別の表示(View by Hosts)] 円グラフでは、ホスト別に生成された ISE アラートの割合と数が提供されます。

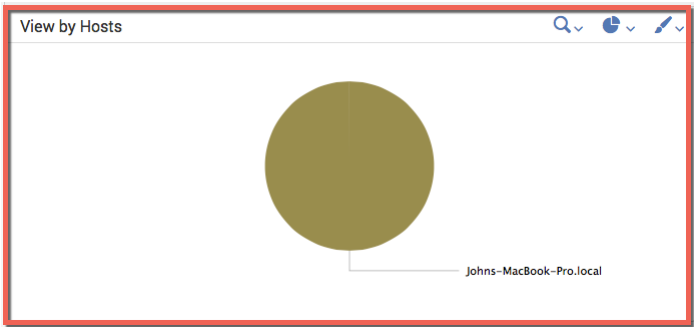


図 27.

検索文字列フィールド:

```
eventtype=cisco-ise log_type=Administrative_and_Operational_Audit System-management | stats count by host
```

システム管理操作の詳細（System Management Operational Details）

システム管理操作の統計情報テーブルでは、メッセージ コード、説明、操作メッセージなどの説明一式が提供されます。このダッシュボードは通常、イベントに関するコンテキストと、円グラフに表示されるシステム管理の説明を提供するために ISE 管理者によって使用されます。


System Management Operational Details

System Management Description	Message Code	Operational Message	host	Count
ADEOS SSH Service configuration change	60086	Service sshd configuration has been modified to ON	Johns-MacBook-Pro.local	6
DNS Resolution failure	60134	DNS resolution failed for the hostname bxb22-11a-pdp1.cisco.com against the currently configured name servers. Ensure that you have configured a reachable name server using the 'ip name-server <servername>' CLI	Johns-MacBook-Pro.local	2
DNS Resolution failure	60134	DNS resolution failed for the hostname ise12.lab4.com against the currently configured name servers. Ensure that you have configured a reachable name server using the 'ip name-server <servername>' CLI	Johns-MacBook-Pro.local	146
NTP Server set	58022	NTP	Johns-MacBook-Pro.local	6
NTP failed to sync with configured servers	60165	All	Johns-MacBook-Pro.local	143

図 28.

検索文字列フィールド:

```
eventtype=cisco-ise log_type=Administrative_and_Operational_Audit System-management | stats count by
system_mgmt_desc MESSAGE_CODE OperationMessageText host |`format_field_names`
```

Cisco ISE の設定

[Cisco ISE の設定（Cisco ISE Configuration）] ダッシュボードでは、ISE syslog の設定、ISE のロギング カテゴリ、Splunk sylog の設定に関する詳細が提供されます。詳細を表示するには、ダッシュボードに直接アクセスします。[Splunk]->[ISE の概要（ISE Overview）]->[Cisco ISE の設定（Cisco ISE Configuration）] を選択します。

ISE プロファイラ（ISE Profiler）

[ISE プロファイラ（ISE Profiler）] ダッシュボードとパネルでは、すべてのユーザの ISE によってプロファイリングされたデバイス、登録済みデバイスおよび未登録デバイスの組織に関するビューが提供されます。これらの syslog イベントは ISE プロファイラ カテゴリに由来します。このダッシュボードは通常、組織内のセキュリティ デバイスのコンプライアンスを提供するために、ISE 管理者によって使用されます。

すべてのユーザに対する組織のプロファイリングされたデバイスのビュー（Organizational Profiled Device View for All Users）

この円グラフでは、「EndPointMatchedPolicy」フィールドに基づいてプロファイリングされたエンドポイントの割合と数が提供されます。

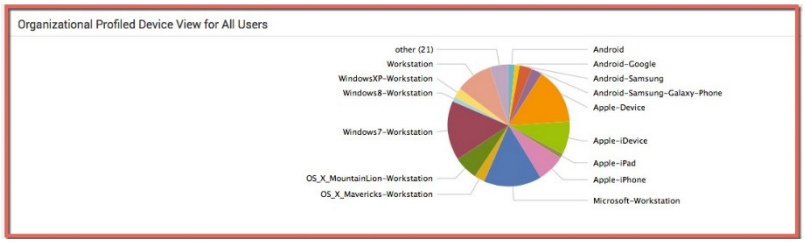


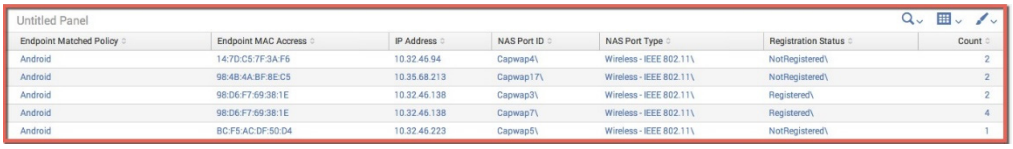
図 29.

検索文字列フィールド：

```
eventtype=cisco-ise-profiler | stats count by EndpointMatchedPolicy | rename EndpointMatchedPolicy AS
"Endpoint Matched Policy"
```

無題のパネルの統計情報パネルでは、[エンドポイントにマッチしたポリシー（Endpoint Matched Policy）]、[エンドポイントの MAC アドレス（Endpoint MAC Address）]、[エンドポイントの IP アドレス（Endpoint IP Address）]、[NAS ポート ID（NAS Port Id）]、[NAS ポートタイプ（NAS Port type）]、[デバイス登録ステータス（DeviceRegistration status）] が提供されます。ここでは、プロファイリングされたエンドポイントのコンテキスト情報が提供されます。

注：場合によっては「PortalUser」を使用できます。これは、取得したイベントに見つからなかった場合、結果に影響する可能性があります。


Untitled Panel

Endpoint Matched Policy	Endpoint MAC Accress	IP Address	NAS Port ID	NAS Port Type	Registration Status	Count
Android	14:7D:C5:7F:3A:F6	10.32.46.94	Capwap4\	Wireless - IEEE 802.11\	NotRegistered\	2
Android	98:4B:4A:BF:8E:C5	10.35.68.213	Capwap17\	Wireless - IEEE 802.11\	NotRegistered\	2
Android	98:D6:F7:69:38:1E	10.32.46.138	Capwap3\	Wireless - IEEE 802.11\	Registered\	2
Android	98:D6:F7:69:38:1E	10.32.46.138	Capwap7\	Wireless - IEEE 802.11\	Registered\	4
Android	BC:F5:AC:DF:50:D4	10.32.46.223	Capwap5\	Wireless - IEEE 802.11\	NotRegistered\	1

図 30.

検索文字列フィールド

```
eventtype=cisco-ise-profiler | stats count by EndpointMatchedPolicy EndpointMacAddress EndpointIPAddress
NAS_Port_Id NAS_Port_Type DeviceRegistrationStatus |`format_field_names`
```

登録済みデバイスを持つすべてのユーザのデバイス別プロファイル（Profiles by devices for all Users with Registered Devices）

この「円グラフ」では、「EndPointMatchedPolicy」および「DeviceRegistrationstatus=Registered\\」検索文字列フィールドに基づいてプロファイリングされたエンドポイントの割合と数が提供されます。このダッシュボードは通常、どのプロファイリングされたデバイスが登録されたかを示す内訳を提供するために ISE 管理者によって使用されます。これらのデバイスは企業の BYOD ポリシーに一致すると考えられ、推奨されたデバイスだけがネットワークにアクセスできます。

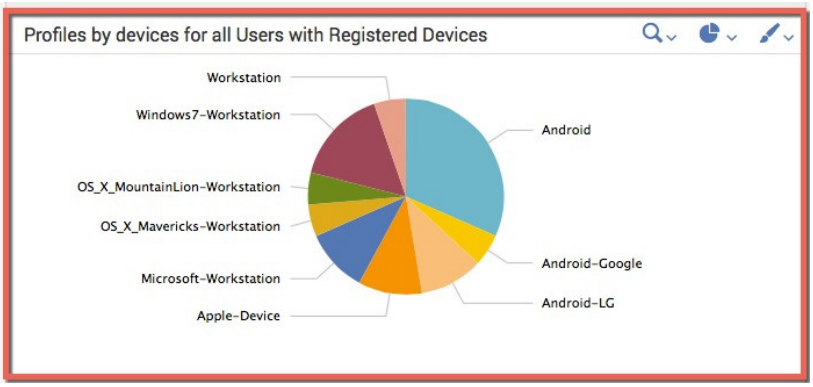


図 31.

検索文字列フィールド:

```
eventtype=cisco-ise-profiler DeviceRegistrationStatus="Registered\\" | stats count by EndpointPolicy |
rename EndpointPolicy AS "Endpoint Policy" count AS Count
```

無題のパネル「統計情報テーブル」では、登録済みデバイスの次のコンテキスト情報が提供されます:エンドポイント ポリシー、ポータル ユーザ、ホスト名、説明、エンドポイントの MAC アドレス、フレームド IP アドレス、エンドポイントの NAD アドレス、エンドポイント OUI、エンドポイント ソース イベント、dhcp_class 識別子、Nmapscancount、NmapsubnetScanID 情報。

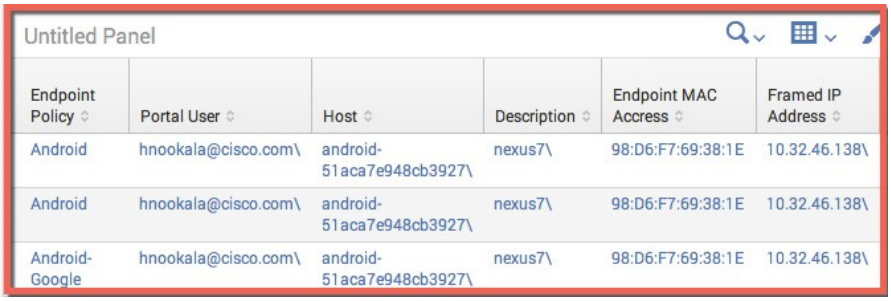


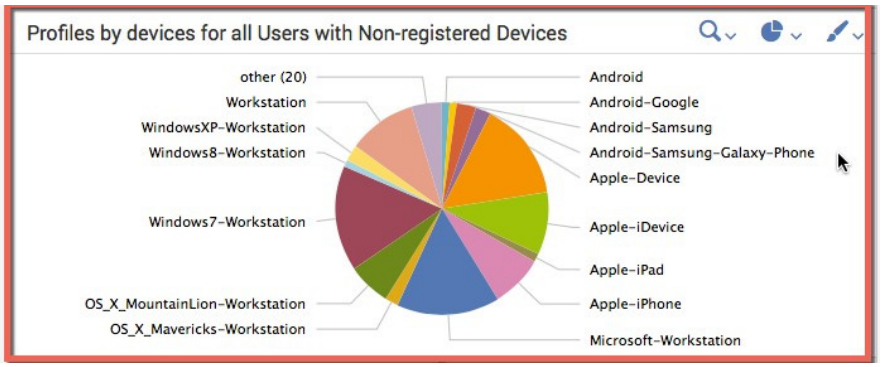
図 32.

検索文字列フィールド

```
eventtype=cisco-ise-profiler DeviceRegistrationStatus="Registered\\" | stats count by EndpointPolicy
PortalUser host_name Description EndpointMacAddress Framed_IP_Address EndpointNADAddress EndpointOUI
EndpointSourceEvent dhcp_class_identifier NmapScanCount NmapSubnetScanID | `format_field_names`
```

未登録デバイスを持つすべてのユーザのデバイス別プロファイル(Profiles by devices for all Users with Non-registered Devices)

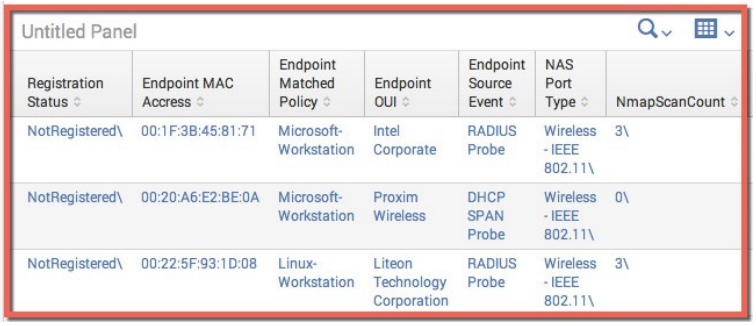
この「円グラフ」では、「EndPointMatchedPolicy」および「DeviceRegistrationstatus=NotRegistered\\」検索文字列フィールドに基づいて未登録デバイスの割合と数が提供されます。このダッシュボードは通常、どのプロファイリングされたデバイスが未登録かを示す内訳を提供するために ISE 管理者によって使用されます。これらのデバイスは企業の BYOD ポリシーに一致すると考えられ、非推奨のデバイスはネットワークにアクセスできません。



検索文字列フィールド:

```
eventtype=cisco-ise-profiler DeviceRegistrationStatus="NotRegistered\\" | stats count by EndpointPolicy |
rename EndpointPolicy AS "Endpoint Policy" count AS Count
```

無題のパネルの統計情報テーブルでは、未登録デバイスの次のコンテキスト情報が提供されます:エンドポイントにマッチしたポリシー、エンドポイントの MAC アドレス、エンドポイント OUI、NAS ポートタイプ、エンドポイント ソース イベント、NmapScanCount、NmapSubnetscanID。



Registration Status	Endpoint MAC Accress	Endpoint Matched Policy	Endpoint OUI	Endpoint Source Event	NAS Port Type	NmapScanCount
NotRegistered\	00:1F:3B:45:81:71	Microsoft-Workstation	Intel Corporate	RADIUS Probe	Wireless - IEEE 802.11\	3\
NotRegistered\	00:20:A6:E2:BE:0A	Microsoft-Workstation	Proxim Wireless	DHCP SPAN Probe	Wireless - IEEE 802.11\	0\
NotRegistered\	00:22:5F:93:1D:08	Linux-Workstation	Liteon Technology Corporation	RADIUS Probe	Wireless - IEEE 802.11\	3\

図 33.

検索文字列フィールド:

```
eventtype=cisco-ise-profiler DeviceRegistrationStatus="NotRegistered\\" | stats count by
DeviceRegistrationStatus EndpointMacAddress EndpointMatchedPolicy EndpointOUI EndpointSourceEvent
NAS_Port_Type NmapScanCount NmapSubnetScanID |`format_field_names`
```

認証（Authentications）

[認証（Authentications）] ダッシュボードでは、以下に示す追加のダッシュボードとパネルが提供されます。このダッシュボードは通常、特定のロケーションや、有線ユーザ、無線ユーザ、仮想ユーザなどの特定のネットワーク アクセス タイプ別に、認証や成功/失敗の試行に関して可視性を提供するために、ISE 管理者によって使用されます。これを使用して、管理者はドリルダウンを行い、特定の認証の詳細とコンテキスト ユーザ情報を取得することができます。管理者にはゲスト アクセスへの可視性もあります。

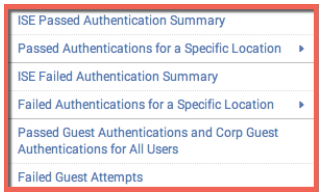


図 34.

- [ISE の成功した認証の概要（ISE Passed Authentication Summary）]：ロケーションや、有線ユーザ、無線ユーザ、仮想ユーザに基づく成功した認証の概要が提供されます。
- [特定のロケーションの成功した認証（Passed Authentications for a Specific Location）]：ロケーション別の、認証方式、802.1X の詳細、ユーザのコンテキスト情報などの成功した認証に関するドリルダウンが提供されます。 有線で成功した認証、無線で成功した認証、仮想で成功した認証に基づいた追加のダッシュボードがあります。
- [ISE の失敗した認証の概要（ISE Failed Authentication Summary）]：ロケーション、有線ユーザ、無線ユーザ、仮想ユーザなどに基づいた失敗した試行の概要が提供されます。
- [特定のロケーションの失敗した認証（Failed Authentications for a Specific Location）]：ロケーション別に、認証方式、802.1X の詳細、ユーザ コンテキスト情報などの失敗した試行に関するドリルダウンが提供されます。 有線で成功した認証、無線で成功した認証、仮想で成功した認証に基づいた追加のダッシュボードがあります。
- [すべてのユーザの成功したゲスト認証と企業ゲスト認証（Passed Guest Authentications and Corp Guest Authentications for All Users）]：ロケーション別のゲスト アクセスのビューが提供されます。
- [失敗したゲストの試行（Failed Guest Attempts）]：失敗したゲストの試行のビューが提供されます。

ISE の成功した認証の概要（ISE Passed Authentication Summary）

[ISE の成功した認証の概要（ISE Passed Authentication Summary）] ダッシュボードとパネルでは、ロケーション別のすべてのユーザの成功した 802.1X 認証の概要が提供されます。これには、有線ユーザ、無線ユーザ、および仮想ユーザ間の区別も含まれています。

すべてのユーザのロケーション別の成功した認証（Passed Authentications by Locations for all users）

[すべてのユーザのロケーション別の成功した認証（Passed Authentications by Locations for all users）] 円グラフは、「Location」および「NAS_PORT_Type」検索文字列フィールドによって定義されているように、異なるロケーションのすべてのユーザの成功した認証の割合と数を示します。各ロケーションの成功した認証の合計は、組織全体の成功した認証の総数を表します。

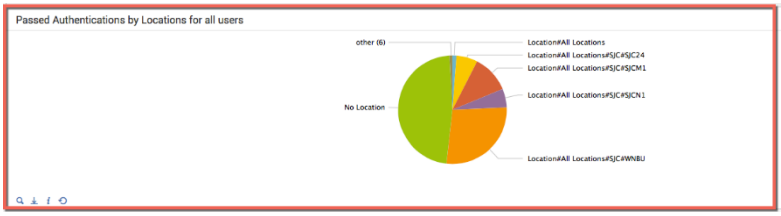


図 35.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication NAS_Port_Type="*" | fillnull value="No Location" Location | chart count by Location
```

ロケーション別有線ユーザ（Wired Users by Location）

この「円グラフ」は、「Location=”*”」および「NAS_PORT_Type=Ethernet」検索文字列フィールドによって定義されているように、すべてのロケーションの有線ユーザに対する成功した認証の割合と数を示します。各ロケーションの成功した認証の合計は、組織全体の有線エンドユーザの成功した認証の総数を表します。

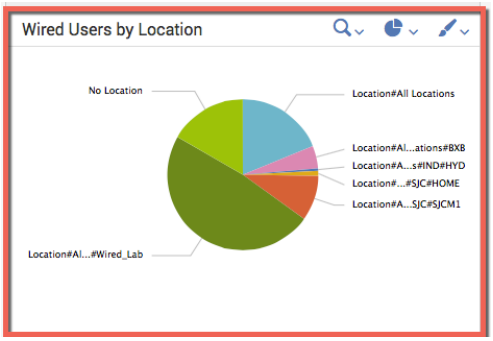


図 36.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication NAS_Port_Type="Ethernet" | fillnull value="No Location" Location | chart count by Location
```

ロケーション別無線ユーザ（Wireless Users by Location）

この「円グラフ」は、「Location=”*”」および「NAS_PORT_Type=Wireless-IEEE 802.11」検索文字列フィールドによって定義されているように、すべてのロケーションの無線ユーザに対する成功した認証の割合と数を示します。各ロケーションの成功した認証の合計は、組織全体の無線エンドユーザの成功した認証の総数を表します。

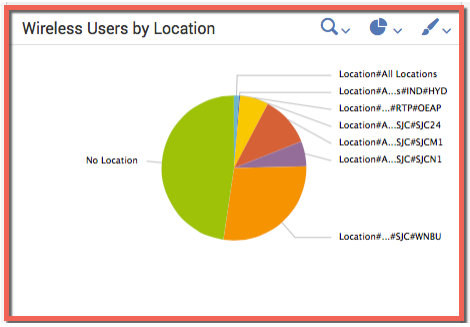


図 37.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication NAS_Port_Type="Wireless - IEEE 802.11" | fillnull value="No
Location" Location | chart count by Location
```

ロケーション別仮想、ASA ユーザ（Virtual, ASA users by Location）

この「円グラフ」は、「Location=”*”」および「NAS_PORT_Type=Virtual」検索文字列フィールドによって定義されているように、すべてのロケーションの仮想ユーザに対する成功した認証の割合と数を示します。各ロケーションの成功した認証の合計は、組織全体の仮想ユーザの成功した認証の総数を表します。これらのエンドユーザは、VPN トンネル経由で認証されている可能性があります。

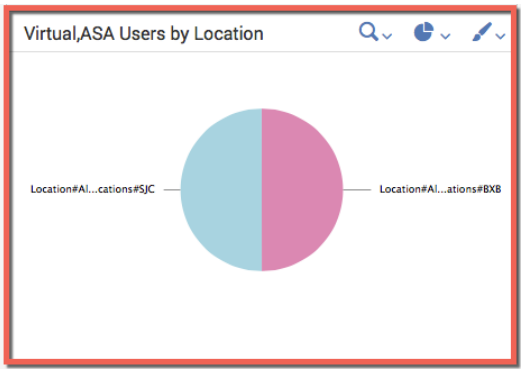


図 38.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication NAS_Port_Type="Virtual" | fillnull value="No Location" Location |
chart count by Location
```

特定のロケーションの成功した認証（Passed Authentications for a Specific Location）

[特定のロケーションの成功した認証（Passed Authentications for a Specific Location）] ダッシュボードとこれらのパネルには、特定のロケーション（この例では BXB ロケーション）からの有線ユーザの成功した 802.1X 認証が示されます。認証方式の詳細を表示するために複数のパネルが作成されました。これらの認証方式には、トンネル型 EAP 方式として EAP- FAST、EAP-TLS、内部メソッドとして MS-CHAPv2 を使用した EAP チェーンが含まれています。MAB も含まれています。

このダッシュボードは通常、特定のロケーション別の有線ユーザの成功した認証についてのコンテキストの詳細を提供するために、ISE 管理者によって使用されます。これがどのように使用されるかの例としては、特定のロケーションの有線ユーザが認証のためにより強力な EAP 方式を必要とするような、企業のセキュリティ アイデンティティ ポリシーが存在する場合などがあります。ISE 管理者はドリルダウンを行い、認証の詳細と、企業ポリシーに収まっているというユーザのコンテキスト情報を表示できます。

ISE の有線で成功した認証

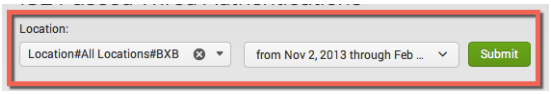


図 39.

有線で成功した認証：Locations#BXB の例

この「円グラフ」は、「Location=”BXB”」に基づく有線ユーザの成功した認証の割合と数を示します。「AuthenticationMethod=”*”」および「NAS_PORT_Type=Ethernet」検索文字列変数は、有線ユーザの認証方式と NAS ポート タイプを定義します。これらの成功した認証の合計は、正常に認証された有線ユーザの総数を表します。「AuthenticationMethod」は MSCHAPv2、x509_PKI、Lookup、PAP_ASCII などの認証方式を定義するだけであることに注意してください。さらなる認証の詳細については、外部またはトンネル型の EAP 方式と内部 EAP 方式（EAP-FAST（MSCHAPv2）など）を提供するために、「EapTunnel」および「EapAuthentication」が使用されます。これは、「802.1X 認証パネル」で確認できます。

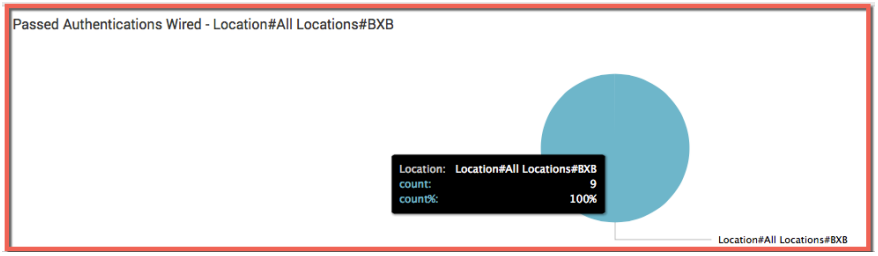


図 40.

検索文字列フィールド：

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Ethernet" | chart count by Location
```

成功した認証の合計（Passed Total Authentications）

この「統計情報テーブル」には、AuthenticationMethod タイプと成功した有線認証の数が表示されます。これは「円グラフ」とビューが異なるだけです。有線ユーザの成功した認証の合計数を容易に表示できます。また、円グラフを使用しようとしている場合は、正確な情報の表示にも役立ちます。Splunk の検索文字列変数は引き続き同じです。必要なのは「円グラフ」の代わりに「統計情報テーブル」のビューに変更することだけです。

図 41.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Ethernet" | stats count by
AuthenticationMethod | rename AuthenticationMethod AS "Authentication Method"
```

802.1X 認証（802.1X Authentications）

この「統計情報テーブル」には、EAP 認証方式とユーザのコンテキスト情報の詳細情報が表示されます。EapTunnel および EapAuthentication 検索文字列フィールドでは、トンネリング型 EAP 方式（この場合は PEAP）および内部方式（この場合は MS-CHAPv2）を抽出することで、より詳細な EAP 認証が提供されます。ユーザのコンテキスト情報には、ユーザ名、エンドポイントの MAC アドレス、エンドポイントで一致するプロファイル、およびホスト アイデンティティ グループの情報が含まれています。この場合、NAS IP アドレスも含まれています。

802.1X Authentications

Authentication Method	EAP Tunnel	EAP Authentication	User Name	MAC Address	Address	Matched Profile	Host Identity Group
Lookup	EAP-FAST	EAP-MSCHAPv2	anonymous	3C-97-0E-53-C8-2B	10.86.98.54	Windows7-Workstation	Endpoint Identity Groups:Profiled:Workstation
MSCHAPV2	EAP-FAST	EAP-MSCHAPv2	anonymous	3C-97-0E-53-C8-2B	10.86.98.54	Windows7-Workstation	Endpoint Identity Groups:Profiled:Workstation
MSCHAPV2	PEAP	EAP-MSCHAPv2	khvo	3C-07-54-21-A3-0C	10.86.98.55	OS_X_MountainLion-Workstation	Endpoint Identity Groups:Profiled:Workstation

図 42.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Ethernet" | fillnull
value="NULL" EapAuthentication | stats count by AuthenticationMethod EapTunnel EapAuthentication UserName
EndPointMACAddress Address EndPointMatchedProfile HostIdentityGroup |         `format_field_names`
```

EAP TLS

この「統計情報テーブル」には、x509_PKI 認証方式に関する詳細が表示され、ユーザのコンテキスト情報が提供されます。

EAP-TLS

No results found.

図 43.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Ethernet"
EapAuthentication="EAP-TLS" | stats count by AuthenticationMethod EapAuthentication UserName
EndPointMACAddress Address EndPointMatchedProfile |`format_field_names`
```

認証の詳細

認証の詳細には認証のコンテキスト情報が示されます。

図 44.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Ethernet" | stats count by
AuthenticationMethod EapTunnel EapAuthentication NetworkDeviceGroups NetworkDeviceName NAS_IP_Address
NAS_Port_Id Called_Station_ID EndPointMatchedProfile UserName |`format_field_names`
```

ISE の成功した無線認証(ISE Passed Wireless Authentications)

このダッシュボードとこれらのパネルには、特定のロケーション(この例では HYD ロケーション)から抽出した成功したワイヤレス 802.1X ユーザ認証情報が示されます。認証方式の詳細を表示するために複数のパネルが作成されました。これには、トンネル型 EAP 方式として EAP- FAST、EAP-TLS、内部メソッドとして MS-CHAPv2 を使用した EAP チェーンが含まれています。MAB も含まれています。

ロケーション:HYD の成功した認証(Passed Authentications Locations-HYD)

この「円グラフ」は、「Location=”*HYD”」に基づく無線ユーザに対する成功した認証の割合と数を示します。「AuthenticationMethod=”*”」および「NAS_PORT_Type=Wireless - IEEE -802.11」検索文字列フィールドは、認証方式と無線エンドユーザを定義します。これらの成功した認証の合計は、正常に認証された無線エンドユーザの総数を表します。「AuthenticationMethod」は MSCHAPv2、x509_PKI、Lookup などの認証方式を定義するだけであることに注意してください。認証の詳細については、802.1X 認証パネルで説明されているように、外部および内部の EAP 方式(EAP-FAST(MSCHAPv2) など)を提供するために、「EapTunnel」および「EapAuthentication」が使用されます。

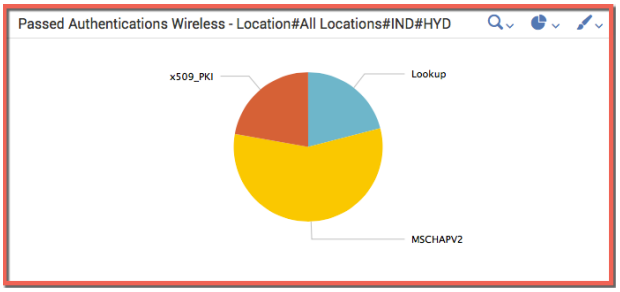


図 45.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Wireless - IEEE 802.11" |
chart count by AuthenticationMethod | rename AuthenticationMethod AS "Authentication Method"
```

成功した認証の合計(Passed Total Authentications)

この「統計情報テーブル」には、AuthenticationMethod タイプと成功した無線認証の数が示されます。これは「HYD の成功した認証」パネルの「円グラフ」とビューが異なるだけです。これによって、HYD ロケーションの無線エンドユーザの成功した認証の総数を容易に表示できます。また、円グラフに正しい情報が表示されているかを確認する際にも使用できます。Splunk の検索文字列フィールドは引き続き同じです。必要なのは「円グラフ」の代わりに「統計情報テーブル」のビューを変更することだけです。

図 46.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Wireless - IEEE 802.11" |
stats count by AuthenticationMethod | rename AuthenticationMethod AS "Authentication Method"
```

X 認証(X Authentications)

この「統計情報テーブル」には、EAP 認証方式とユーザのコンテキスト情報の詳細情報が表示されます。EapTunnel および EapAuthentication 検索文字列変数では、トンネリング型 EAP 方式(この場合は PEAP)および内部方式(この場合は MS-CHAPv2)を抽出することで、より詳細な EAP 認証が提供されます。ユーザのコンテキスト情報には、ユーザ名、エンドポイントの MAC アドレス、エンドポイントで一致するプロファイル、およびホスト アイデンティティ グループの情報が含まれています。この場合、NAS IP アドレスも含まれています。

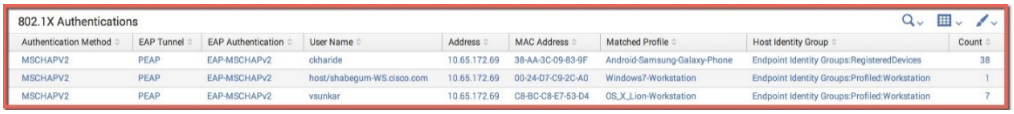


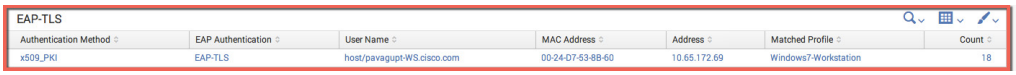
図 47.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Wireless - IEEE 802.11" |
fillnull value="NULL" EapAuthentication | stats count by AuthenticationMethod EapTunnel EapAuthentication
UserName Address EndPointMACAddress EndPointMatchedProfile HostIdentityGroup |          `format_field_names`
```

EAP-TLS

この「統計情報テーブル」には、x509_PKI 認証方式に関する詳細が表示され、ユーザのコンテキスト情報が提供されます。


EAP-TLS

Authentication Method	EAP Authentication	User Name	MAC Address	Address	Matched Profile	Count
x509_PKI	EAP-TLS	host/pavagupt-WS.cisco.com	00-24-D7-53-8B-60	10.65.172.69	Windows7-Workstation	18

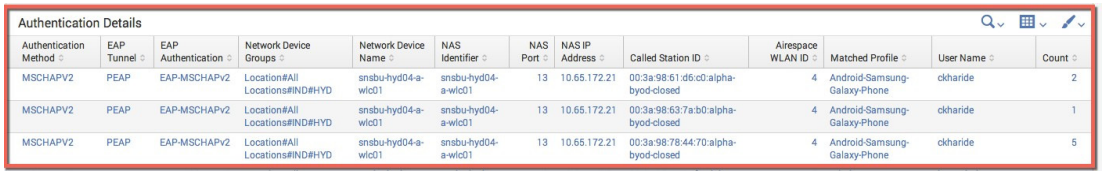
図 48.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Wireless - IEEE 802.11"
EapAuthentication="EAP-TLS" | stats count by AuthenticationMethod EapAuthentication UserName
EndPointMACAddress Address EndPointMatchedProfile | `format_field_names`
```

認証の詳細

この「統計情報テーブル」には、NAD デバイスのコンテキスト情報とユーザのコンテキスト情報が表示されます。NAD デバイスのコンテキスト情報と検索文字列フィールドは次から構成されます:ネットワーク デバイス グループ、「NetworkDeviceGroups」、ネットワーク デバイス名、「NetworkDeviceName」、NAS 識別子、「NAS_Identifier」、NAS ポート、「NAS_Port」、NAS の IP アドレス、「NAS_IP_Address」、着信ステーション ID、「Called_Station_ID」、および Airespace WLAN ID、「Airespace_Wlan_Id」。


Authentication Details

Authentication Method	EAP Tunnel	EAP Authentication	Network Device Groups	Network Device Name	NAS Identifier	NAS Port	NAS IP Address	Called Station ID	Airespace WLAN ID	Matched Profile	User Name	Count
MSCHAPV2	PEAP	EAP-MSCHAPv2	Location#All Locations#IND#HYD	snsbu-hyd04-a-wlc01	snsbu-hyd04-a-wlc01	13	10.65.172.21	00:3a:98:61:d6:c0:alpha-byod-closed	4	Android-Samsung-Galaxy-Phone	ckharide	2
MSCHAPV2	PEAP	EAP-MSCHAPv2	Location#All Locations#IND#HYD	snsbu-hyd04-a-wlc01	snsbu-hyd04-a-wlc01	13	10.65.172.21	00:3a:98:63:7a:b0:alpha-byod-closed	4	Android-Samsung-Galaxy-Phone	ckharide	1
MSCHAPV2	PEAP	EAP-MSCHAPv2	Location#All Locations#IND#HYD	snsbu-hyd04-a-wlc01	snsbu-hyd04-a-wlc01	13	10.65.172.21	00:3a:98:78:44:70:alpha-byod-closed	4	Android-Samsung-Galaxy-Phone	ckharide	5

図 49.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Wireless - IEEE 802.11" |
fillnull value="NULL" Called_Station_ID EapAuthentication NAS_Port | stats count by AuthenticationMethod
EapTunnel EapAuthentication NetworkDeviceGroups NetworkDeviceName NAS_Identifier NAS_Port NAS_IP_Address
Called_Station_ID Airespace_Wlan_Id EndPointMatchedProfile UserName | `format_field_names`
```

MAB

この「統計情報テーブル」では、MAB の詳細が提供されます。「AuthenticationMethod」変数は「ルックアップ」として MAB を表示することに注意してください。


MAB

Authentication Method	count
Lookup	17

図 50.

検索文字列フィールド:

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Wireless - IEEE 802.11"
AuthenticationMethod="Lookup" | stats count by AuthenticationMethod | rename AuthenticationMethod AS
"Authentication Method"
```

EAP チェーンの試行（EAP Chaining Attempts）

[EAP チェーンの試行（EAP Chaining Attempts）] は、イベントの EAPChainingResults を調べます。

図 51.

検索文字列フィールド：

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Wireless - IEEE 802.11" |
stats count by EapTunnel EapAuthentication UseCase EapChainingResult UserName EndPointMACAddress Address
EndPointMatchedProfile HostIdentityGroup |`format_field_names`
```

ISE の成功した仮想認証（ISE Passed Virtual Authentications）

このダッシュボードとこれらのパネルには、特定のロケーション（この例では BXB ロケーション）から抽出した成功した 802.1X 仮想ユーザ情報が示されます。認証方式を詳細に表示するために複数のパネルが作成されました。これには、トンネル型 EAP 方式として EAP- FAST、EAP-TLS、内部メソッドとして MS-CHAPv2 を使用した EAP チェーンが含まれています。MAB も含まれています。

成功した認証仮想（Passed Authentications Virtual）

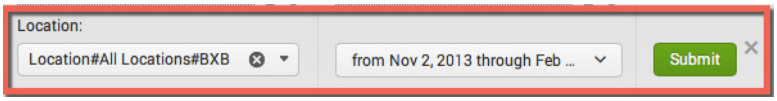


図 52.

この「円グラフ」は、「Location=”BXB”」に基づく仮想ユーザに対する成功した認証の割合と数を示します。「AuthenticationMethod=”*”」および「NAS_PORT_Type=”Virtual」検索文字列変数は、仮想ユーザの認証方式とポート タイプを定義します。これらの成功した認証の合計は、正常に認証された仮想ユーザの総数を表します。「AuthenticationMethod」は MSCHAPv2、x509_PKI、PAP_ASCII、Lookup などの認証方式を定義するだけであることに注意してください。この場合、PAP_ASCII は認証方式として定義されます。

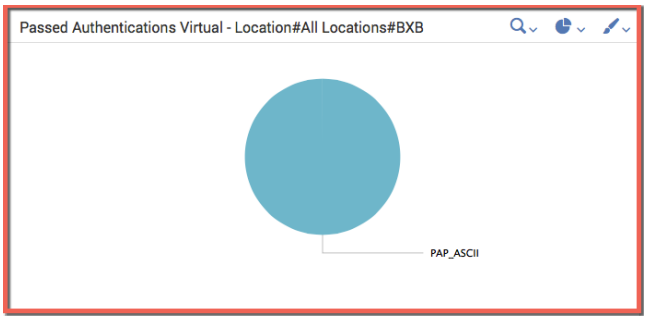


図 53.

検索文字列フィールド：

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Virtual" | chart count by
AuthenticationMethod | rename AuthenticationMethod AS "Authentication Method"
```

成功した認証の合計（Passed Total Authentications）

この「統計情報テーブル」には、AuthenticationMethod タイプと成功した仮想認証の数が表示されます。これは単に「円グラフ」の異なるビューです。仮想エンドユーザの成功した認証の合計数を容易に表示できます。また、円グラフに正確な情報を表示することができます。Splunk の検索文字列変数は引き続き同じです。必要なのは「円グラフ」の代わりに「統計情報テーブル」のビューに変更することだけです。

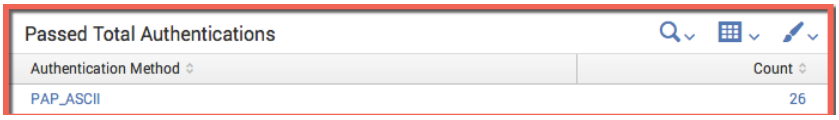


図 54.

検索文字列フィールド：

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Virtual" | stats count by
AuthenticationMethod | rename AuthenticationMethod AS "Authentication Method" count AS Count
```

認証済みユーザ（Authenticated Users）

この「統計情報テーブル」には、認証済みのユーザ名が表示されます。ユーザ名の検索文字列変数は「UserName」です。

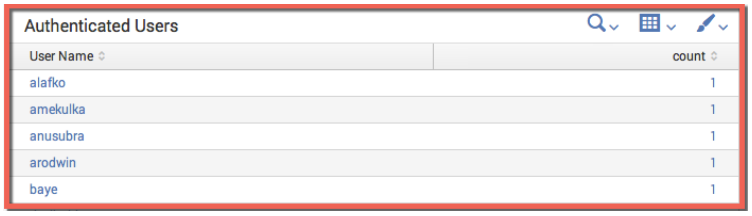


図 55.

検索文字列フィールド：

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Virtual" | stats count by
UserName | rename UserName AS "User Name"
```

認証済みユーザの概要（Authenticated Users Overview）

この「統計情報テーブル」には、関連する検索文字列変数（[ユーザ名（User Name）]、[発信側ステーション ID（Calling Station ID）]、[トンネルクライアントエンドポイント（Tunnel Client Endpoint）]、[PIX 7.x クライアントタイプ（PIX 7.x Client Type）]、[PIX 7.x トンネルグループ名（PIX 7.x Tunnel Group Name）]、[ネットワークデバイス名（Network Device Name）]）とともにユーザのコンテキスト情報が表示されます。

図 56.

検索文字列フィールド：

```
eventtype=cisco-ise-passed-authentication Location="$location$" NAS_Port_Type="Virtual" | stats count by
UserName Calling_Station_ID Tunnel_Client_Endpoint PIX7x_Client_Type PIX7x_Tunnel_Group_Name
NetworkDeviceName | `format_field_names`
```

すべてのユーザの成功したゲスト認証と企業ゲスト認証（Passed Guest Authentications and Corp Guest Authentications for all users）

[成功したゲスト認証（passed guest authentications）] ダッシュボードおよびパネルでは、ロケーション、ユーザ名別のロケーション ベースのゲスト アクセス ビューが提供され、ユーザのコンテキスト情報の詳細が含まれています。これは改訂されています。このダッシュボードは通常、ロケーション別のゲスト/ユーザの詳細への可視性を提供し、ゲスト/ユーザのコンテキスト情報を提供するために、ISE 管理者によって使用されます。

ロケーション別ゲストアクセス（Guest Access by Location）

この「円グラフ」には、すべてのユーザ（無線および有線）のすべてのロケーションからのゲスト ユーザの割合と数が表示されます。

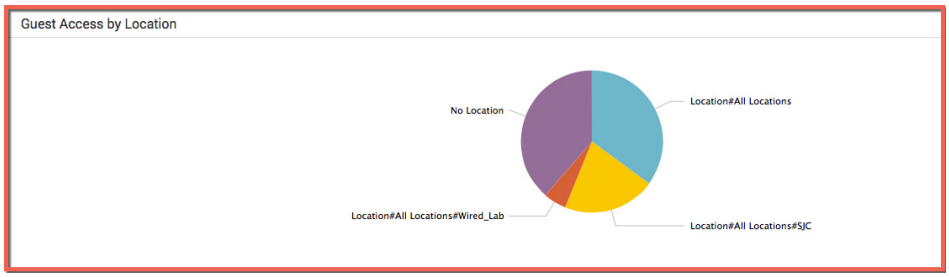


図 57.

検索文字列フィールド：

```
eventtype=cisco-ise-guest-authentication | fillnull value="No Location" Location | chart count by Location
```

ロケーション別ゲストユーザ名（Guest UserName by Locations）

この統計情報テーブル ビューには、ユーザ名とロケーションの内訳が示されます。

Guest UserName By Locations

UserName	Location	_time
jehyman	Location#All Locations#SJC	2014-01-10 12:38:05
skuthadi	Location#All Locations#SJC	2014-01-10 12:09:11
alafko	Location#All Locations#SJC	2014-01-10 11:57:56
thomas	Location#All Locations#SJC	2014-01-10 11:46:50
thomas	Location#All Locations#SJC	2014-01-10 11:22:07
martinf	Location#All Locations#SJC	2014-01-10 10:56:04
jjustins	Location#All Locations#SJC	2014-01-09 23:58:16

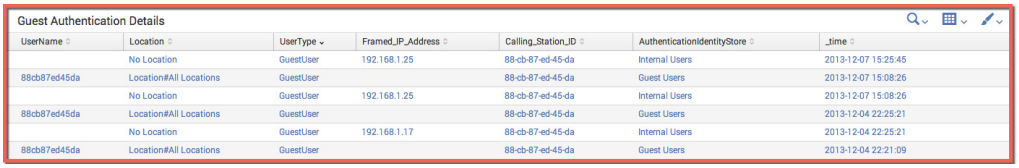
図 58.

検索文字列フィールド：

```
eventtype=cisco-ise-guest-authentication | fillnull value="No Location" Location | fields UserName Location
| fields - _raw
```

ゲスト認証の詳細（Guest Authentication Details）

この統計情報テーブル ビューには、ゲスト ユーザ名に関するコンテキスト情報が提供されます。


Guest Authentication Details

UserName	Location	UserType	Framed_IP_Address	Calling_Station_ID	AuthenticationIdentityStore	_time
	No Location	GuestUser	192.168.1.25	88-cb-87-ed-45-da	Internal Users	2013-12-07 15:25:45
88cb87ed45da	Location#All Locations	GuestUser		88-cb-87-ed-45-da	Guest Users	2013-12-07 15:08:26
	No Location	GuestUser	192.168.1.25	88-cb-87-ed-45-da	Internal Users	2013-12-07 15:08:26
88cb87ed45da	Location#All Locations	GuestUser		88-cb-87-ed-45-da	Guest Users	2013-12-04 22:25:21
	No Location	GuestUser	192.168.1.17	88-cb-87-ed-45-da	Internal Users	2013-12-04 22:25:21
88cb87ed45da	Location#All Locations	GuestUser		88-cb-87-ed-45-da	Guest Users	2013-12-04 22:21:09

図 59.

検索文字列フィールドは次のとおりです。

```
eventtype=cisco-ise-guest-authentication | fillnull value="No Location" Location | fields UserName Location
UserType Framed_IP_Address Calling_Station_ID AuthenticationIdentityStore | fields - _raw
```

企業ゲスト認証（Corp Guest Authentication）

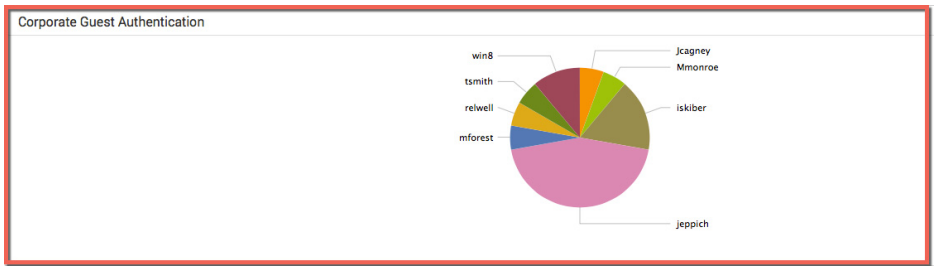
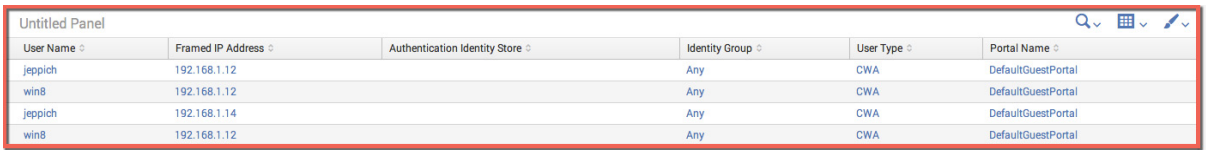


図 60.

```
"5231" UserType="CWA" UserName="*" | chart count by UserName | rename UserName AS "User Name"
```


Untitled Panel

User Name	Framed IP Address	Authentication Identity Store	Identity Group	User Type	Portal Name
jeppich	192.168.1.12		Any	CWA	DefaultGuestPortal
win8	192.168.1.12		Any	CWA	DefaultGuestPortal
jeppich	192.168.1.14		Any	CWA	DefaultGuestPortal
win8	192.168.1.12		Any	CWA	DefaultGuestPortal

図 61.

```
"5231" UserType="CWA" UserName="*" | fillnull value="NULL" Framed_IP_Address | table UserName
Framed_IP_Address AuthenticationIdentityStore IdentityGroup UserType PortalName |
`format_field_names`
```

失敗したゲストの試行（Failed Guest Attempts）

[失敗したゲスト（failed guest）] ダッシュボードとパネルには、説明とユーザ名情報によるゲストの失敗の詳細が提供されます。これは改訂されています。

ゲストの失敗（Guest Failures）

この円グラフには、FailureReason 別に失敗したゲストの試行の割合と数が示され、ユーザ情報が提供されます。「5418」メッセージコードはゲストの認証エラーを示していることに注意してください。

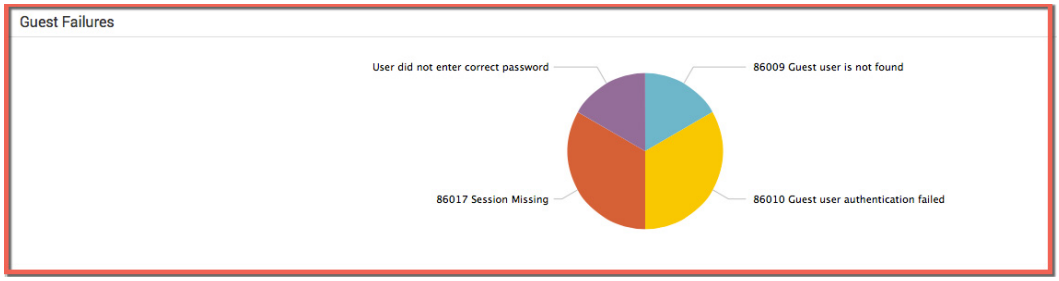


図 62.

検索文字列フィールド：

```
CISE_Failed_Attempts "5418" | stats count by FailureReason
```

無題パネル（Untitled Panel）

次の統計情報ビューには、ユーザ名と失敗の理由が示されます。


Untitled Panel

UserName	FailureReason	_time
	86009 Guest user is not found	2014-01-10 13:42:10
msanchez	User did not enter correct password	2013-12-07 15:06:46
ttebow02	86017 Session Missing	2013-12-07 14:54:53
rjones	86010 Guest user authentication failed	2013-12-07 14:00:37
jeppich	86017 Session Missing	2013-12-07 13:48:43
jdoe0001	86010 Guest user authentication failed	2013-12-04 22:39:09

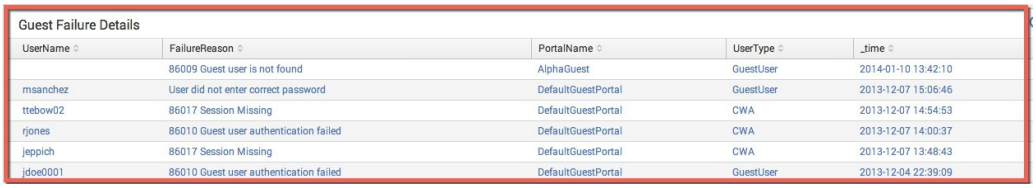
図 63.

検索文字列フィールド：

```
CISE_Failed_Attempts "5418" | fields UserName FailureReason | fields - _raw
```

ゲストの失敗の詳細（Guest Failure Details）

この統計情報ビューには、GuestUser を示す PortalName および UserType、または CWA を通過することで可能性のある企業ユーザを含めることで、UserName および FailureReason に関する追加のコンテキスト情報が提供されます。


Guest Failure Details

UserName	FailureReason	PortalName	UserType	_time
	86009 Guest user is not found	AlphaGuest	GuestUser	2014-01-10 13:42:10
msanchez	User did not enter correct password	DefaultGuestPortal	GuestUser	2013-12-07 15:06:46
ttebow02	86017 Session Missing	DefaultGuestPortal	CWA	2013-12-07 14:54:53
rjones	86010 Guest user authentication failed	DefaultGuestPortal	CWA	2013-12-07 14:00:37
jeppich	86017 Session Missing	DefaultGuestPortal	CWA	2013-12-07 13:48:43
jdoe0001	86010 Guest user authentication failed	DefaultGuestPortal	GuestUser	2013-12-04 22:39:09

図 64.

検索文字列フィールド:

```
CISE_Failed_Attempts "5418" | fields UserName FailureReason PortalName UserType | fields - _raw
```

ISE の失敗した認証の概要(ISE Failed Authentication Summary)

このダッシュボードとこれらのパネルには、ロケーション別のすべてのユーザの失敗した 802.1X 認証の概要が示され、有線ユーザ、無線ユーザおよび仮想ユーザの失敗した認証が含まれています。このダッシュボードは通常、可視性を提供し、失敗の理由のイベントとユーザのコンテキスト情報に基づいて失敗した認証の試行を診断するために、ISE 管理者によって使用されます。

すべてのユーザのロケーション別の失敗した認証(Failed Authentications by Locations for all users)

この「円グラフ」は、「Location」および「NAS_PORT_Type」検索文字列フィールドによって定義されているように、異なるロケーションに基づいてすべてのユーザの失敗した 802.1X 認証試行の割合と数を示します。各ロケーションの失敗した認証試行の合計は、組織全体のユーザの失敗した認証の総数を表します。

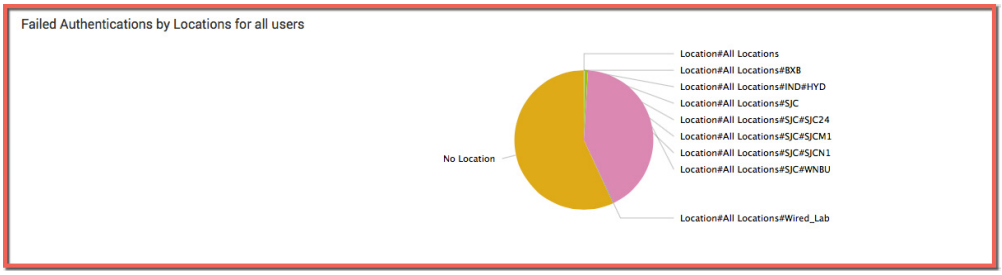


図 65.

検索文字列フィールド:

```
eventtype=cisco-ise-failed-authentication NAS_Port_Type="*" | fillnull value="No Location" Location | chart
count by Location
```

ロケーション別有線ユーザ(Wired Users by Location)

この「円グラフ」は、「Location=”*”」および「NAS_PORT_Type=Ethernet」検索文字列フィールドによって定義されているように、すべてのロケーションの有線ユーザの失敗した認証試行の割合と数を示します。各ロケーションの失敗した認証試行の合計は、組織全体の有線エンドユーザの失敗した認証の総数を表します。

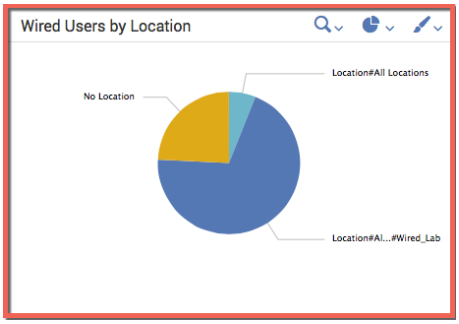


図 66.

検索文字列フィールド:

```
eventtype=cisco-ise-failed-authentication NAS_Port_Type="Ethernet" | fillnull value="No Location" Location |
chart count by Location
```

ロケーション別無線ユーザ（Wireless Users by Location）

この「円グラフ」は、「Location=”*”」および「NAS_PORT_Type=Wireless-IEEE-802.11」検索文字列フィールドによって定義されているように、すべてのロケーションの無線ユーザの失敗した認証試行の割合と数を示します。各ロケーションの失敗した認証試行の合計は、組織全体の無線エンドユーザの失敗した認証の総数を表します。

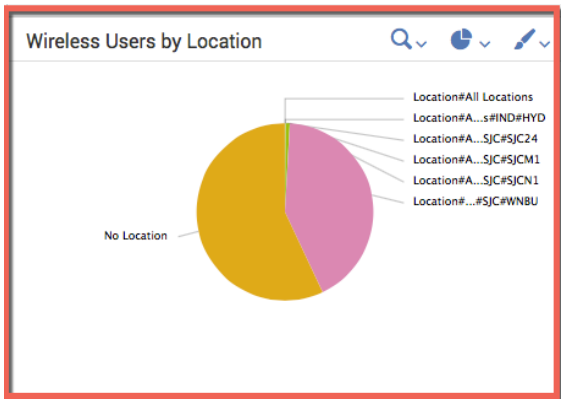


図 67.

検索文字列フィールド:

```
eventtype=cisco-ise-failed-authentication NAS_Port_Type="Wireless - IEEE 802.11" | fillnull value="No
Location" Location | chart count by Location
```

ロケーション別仮想、ASA ユーザ（Virtual, ASA Users by Locations）

この「円グラフ」は、「Location=”*”」および「NAS_PORT_Type=”Virtual」検索文字列フィールドによって定義されているように、すべてのロケーションの仮想ユーザの失敗した認証試行の割合と数を示します。各ロケーションの失敗した認証試行の合計は、組織全体の仮想エンドユーザの失敗した認証の総数を表します。これらのユーザは、VPN トンネル経由で認証される場合があります。

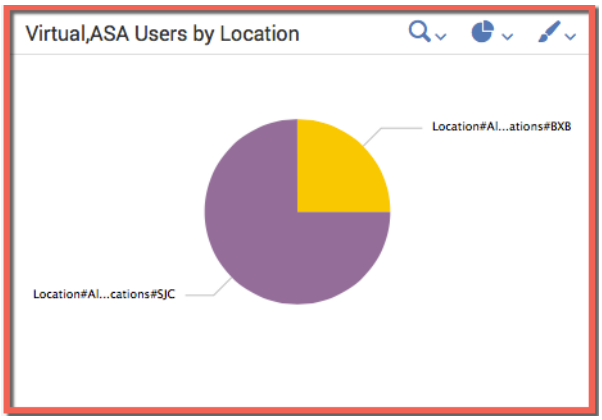


図 68.

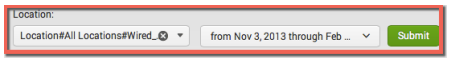
検索文字列フィールド:

```
eventtype=cisco-ise-failed-authentication NAS_Port_Type="Virtual" | fillnull value="No Location" Location |
chart count by Location
```

特定のロケーション別の失敗した認証(Failed Authentications by Specific Location)

このダッシュボードとこれらのパネルには、特定のロケーション(この例では WIREDLABS ロケーション)から抽出した、失敗した 802.1X 有線ユーザ情報が示されます。詳細な認証方式をサポートするために複数のパネルが作成されました。これには、トンネル型 EAP 方式として EAP- FAST、EAP-TLS、内部メソッドとして MS-CHAPv2 を使用した EAP チェーンが含まれています。MAB も含まれています。

ISE の失敗した有線認証



#WiredLab ロケーションの ISE の失敗した有線認証(ISE Failed Wired Authentications for #WiredLab Location)

この「円グラフ」は、「Location="*"」および「NAS_PORT_Type=Ethernet」検索文字列変数によって定義されているように、すべてのロケーションの有線ユーザの失敗した認証試行の割合と数を示します。各ロケーションの失敗した認証試行の合計は、組織全体の有線エンドユーザの失敗した認証の総数を表します。

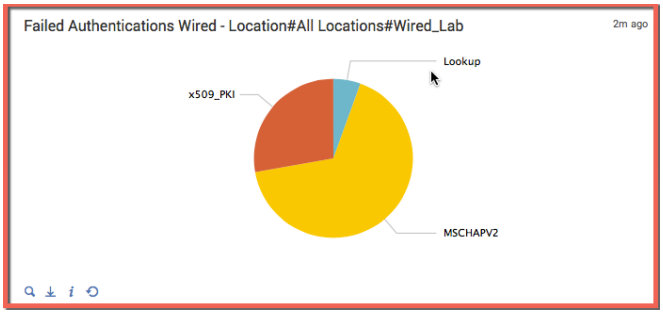


図 69.

検索文字列フィールド:

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Ethernet" | chart count by
AuthenticationMethod | rename AuthenticationMethod AS "Authentication Method"
```

失敗した理由（Failed Reason）

この円グラフには、失敗した有線 802.1X 試行の割合と数が示されます。

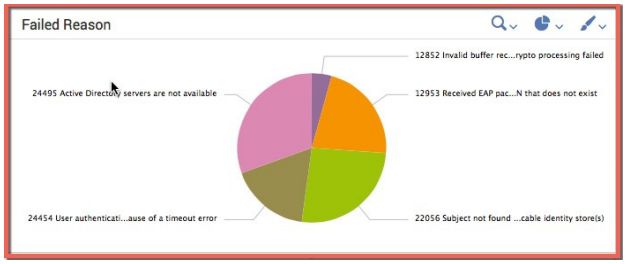


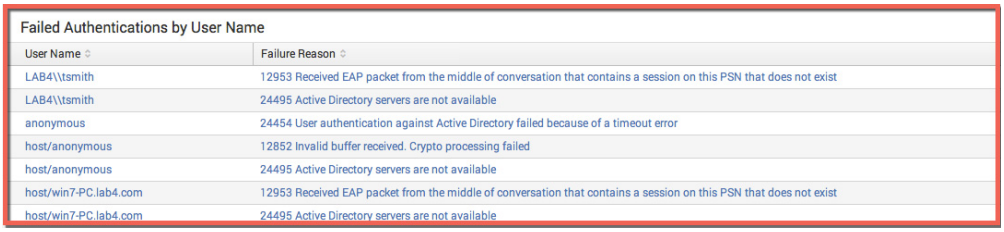
図 70.

検索文字列フィールド：

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Ethernet" | chart count by
FailureReason | rename FailureReason AS "Failure Reason"
```

ユーザ名別の失敗した認証（Failed Authentications by User Name）

この統計情報テーブル ビューには、802.1X 認証試行のユーザ名と失敗の理由が示されます。



Failed Authentications by User Name

User Name	Failure Reason
LAB4\\tsmith	12953 Received EAP packet from the middle of conversation that contains a session on this PSN that does not exist
LAB4\\tsmith	24495 Active Directory servers are not available
anonymous	24454 User authentication against Active Directory failed because of a timeout error
host/anonymous	12852 Invalid buffer received. Crypto processing failed
host/anonymous	24495 Active Directory servers are not available
host/win7-PC.lab4.com	12953 Received EAP packet from the middle of conversation that contains a session on this PSN that does not exist
host/win7-PC.lab4.com	24495 Active Directory servers are not available

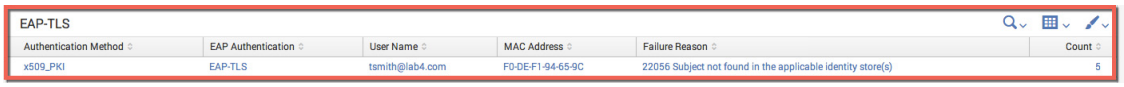
図 71.

検索文字列フィールド：

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Ethernet" | stats count by
UserName FailureReason |      table UserName FailureReason | rename UserName AS "User Name" FailureReason AS
"Failure Reason"
```

EAP-TLS

この統計情報テーブル ビューには、x509.PKI 認証方式の認証の詳細が示され、失敗の理由と認証方式のタイプを補完するために検索文字列変数（ユーザ名、「UserName」、エンドポイントの MAC アドレス、「EndPointMACAddress」）とともにユーザのコンテキスト情報が提供されます。


EAP-TLS

Authentication Method	EAP Authentication	User Name	MAC Address	Failure Reason	Count
x509_PKI	EAP-TLS	tsmith@lab4.com	F0-DE-F1-94-65-9C	22056 Subject not found in the applicable identity store(s)	5

図 72.

検索文字列フィールド:

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Ethernet"
EapAuthentication="EAP-TLS" | stats count by AuthenticationMethod EapAuthentication UserName
EndPointMACAddress FailureReason | `format_field_names`
```

EAP チェーンの試行(EAP Chaining Attempts)

この統計情報ビュー テーブルには、EapTunnel=EAP-FAST および EapChainingResult フィールドに基づいて EAP チェーンの詳細が提供されます。

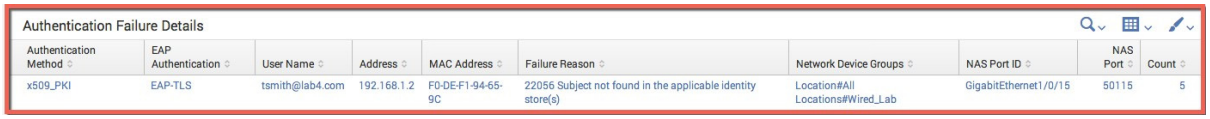
「統計情報テーブル」には EAP チェーンの詳細が表示されます。「統計情報テーブル」には EAP チェーンの失敗した認証試行が表示されます。追加の認証の詳細、および検索文字列変数 Eaptunnel、「EapTunnel」、EapAuthentication、「EapAuthentication」、UseCase、「UseCase」、EAP チェーン結果、「EapChainingResult」では、EAP チェーンの詳細が提供されます。ユーザのコンテキスト情報と検索文字列変数は次のとおりです:ユーザ名、「UserName」、エンドポイントの MAC アドレス、「EndpointMACAddress」。「Address」は NAS IP アドレスで、認証失敗パネルの NAS コンテキスト情報で定義されます。

検索文字列フィールド:

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Ethernet"
EapAuthentication="EAP-TLS" EapTunnel="EAP-FAST" | stats count by AuthenticationMethod EapAuthentication
EapTunnel UserName Address EndPointMACAddress FailureReason UseCase EapChainingResult |
```

認証失敗の詳細(Authentication Failure Details)

この統計情報テーブル ビューには、認証エラーの詳細が示されます。NAS コンテキスト情報と検索文字列変数 NetworkDeviceGroups、「NetworkDeviceGroups」、NAS ポート ID、「NAS_PORT_Id」、NAS ポート、「NAS_Port」はユーザのコンテキスト情報とともに追加されます。


Authentication Failure Details

Authentication Method	EAP Authentication	User Name	Address	MAC Address	Failure Reason	Network Device Groups	NAS Port ID	NAS Port	Count
x509_PKI	EAP-TLS	tsmith@lab4.com	192.168.1.2	F0-DE-F1-94-65-9C	22056 Subject not found in the applicable identity store(s)	Location#All Locations#Wired_Lab	GigabitEthernet1/0/15	50115	5

図 73.

検索文字列フィールド:

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Ethernet"
EapAuthentication="EAP-TLS" | stats count by AuthenticationMethod EapAuthentication UserName Address
EndPointMACAddress FailureReason NetworkDeviceGroups NAS_Port_Id NAS_Port | `format_field_names`
```

ISE の失敗した無線認証（ISE Failed Wireless Authentications）

このダッシュボードとこれらのパネルには、特定のロケーション（この例では HYD ロケーション）から抽出した、失敗した 802.1X 無線ユーザ情報が示されます。認証方式を詳細に表示するために複数のパネルが作成されました。これには、トンネル型 EAP 方式として EAP- FAST、EAP-TLS、内部メソッドとして MS-CHAPv2 を使用した EAP チェーンが含まれています。MAB も含まれています。

失敗した無線認証：Locations#ALL Locations#IND#HYD（Failed Authentications Wireless- Locations#ALL Locations#IND#HYD）

この「円グラフ」は、「Location=”*HYD”」に基づく無線エンドユーザの失敗した認証の割合と数を示します。「EapAuthentication」および「NAS_PORT_Type=Wireless - IEEE -802.11」検索文字列フィールドは、認証方式と無線エンドユーザを定義します。「AuthenticationMethod」の代わりに「EapAuthentication」が使用されていることに注目してください。これは AuthenticationMethod が使用できない場合に起こることがあります。デフォルトでは、EapAuthentication は内部方式の EAP 認証を提供します。これは通常、トンネル型 EAP 方式を提供する「EapTunnel」で使用されます。

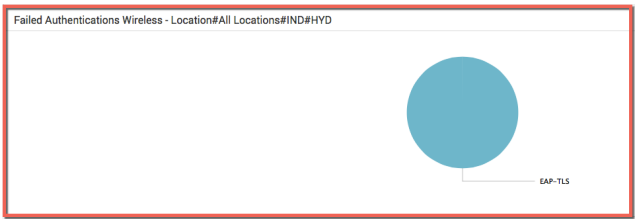


図 74.

検索文字列フィールド：

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Wireless - IEEE 802.11" |
chart count by EapAuthentication | rename AuthenticationMethod AS "Authentication Method"
```

ユーザ名別の失敗した認証（Failed Authentications by User Name）

この「統計情報テーブル」には、EAP 認証タイプと失敗した無線認証の数が表示されます。また、無線ユーザの失敗した認証試行のユーザ コンテキスト情報と検索文字列変数：ユーザ名、「UserName」、エンドポイントの MAC アドレス、「EndPointMACAddress」、さらに失敗の理由、「FailureReason」も示されます。

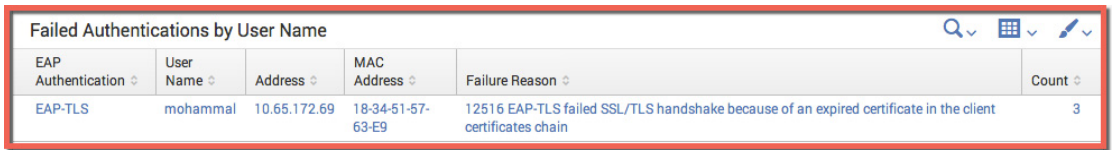


図 75.

検索文字列フィールド：

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Wireless - IEEE 802.11"
EapAuthentication="EAP-TLS" | stats count by EapAuthentication UserName Address EndPointMACAddress
FailureReason |`format_field_names`
```

認証失敗の詳細（Authentication Failure Details）

この「統計情報テーブル」には、ユーザのコンテキスト情報への追加の NAD デバイスのコンテキスト情報が表示されます。NAD デバイスのコンテキスト情報と検索文字列フィールドには次のものが含まれます：ネットワーク デバイス グループ、「NetworkDeviceGroups」、ネットワーク デバイス名、「NetworkDeviceName」、NAS 識別子、「NAS_Identifier」、NAS ポート、「NAS_Port」、NAS の IP アドレス、「NAS_IP_Address」、着信ステーション ID、「Called_Station_ID」、および Airespace WLAN ID、「Airespace_Wlan_Id」。

図 76.

検索文字列フィールド：

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Wireless - IEEE 802.11" |
fillnull value="NULL" Called_Station_ID EapAuthentication | stats count by EapAuthentication
NetworkDeviceGroups NetworkDeviceName NAS_Identifier NAS_Port NAS_IP_Address Called_Station_ID
Calling_Station_ID Airespace_Wlan_Id
```

ISE の失敗した仮想認証

Location#BXB

このダッシュボードとこれらのパネルには、特定のロケーション（この例では BXB ロケーション）から抽出した、失敗した 802.1X 仮想ユーザ情報が示されます。認証方式を詳細に表示するために複数のパネルが作成されました。これには、トンネル型 EAP 方式として EAP- FAST、EAP-TLS、内部メソッドとして MS-CHAPv2 を使用した EAP チェーンが含まれています。MAB も含まれています。

失敗した認証（Failed Authentications）

この「円グラフ」には、「Location=”*BXB”」に基づく仮想ユーザの失敗した認証の割合と数が表示されます。「AuthenticationMethod=”*”」および「NAS_PORT_Type=”Virtual」検索文字列フィールドは、認証方式と仮想エンドユーザを定義します。これらの失敗した認証の合計は、認証が失敗した仮想エンドユーザの総数を表します。「AuthenticationMethod」は MSCHAPv2、x509_PKI、PAP_ASCII などの認証方式を定義するだけであることに注意してください。この場合、PAP_ASCII は認証方式として定義されます。追加のユーザ コンテキスト情報と NAS 詳細用に他のパネルが作成されます。

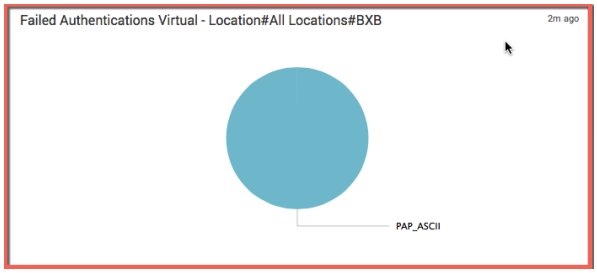


図 77.

検索文字列フィールド:

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Virtual" | chart count by
AuthenticationMethod | rename AuthenticationMethod AS "Authentication Method"
```

失敗した認証の合計(Failed Total Authentications)

この「統計情報テーブル」には、AuthenticationMethod タイプと失敗した仮想認証の数が示されます。これによって、円グラフを使用する代わりに失敗した認証の数を容易に表示できます。Splunk の検索文字列フィールドは引き続き同じです。必要なのは「円グラフ」の代わりに「統計情報テーブル」のビューを変更することだけです。このパネルでは、ユーザのコンテキスト情報と次の検索文字列変数が定義されます:ユーザ名、「UserName」、NAS IP アドレス、「Address」、発信側ステーション ID、「Calling_Station_ID」。失敗の理由、「FailureReason」も表示されます。

図 78.

検索文字列フィールド:

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Virtual" | chart count by
AuthenticationMethod | rename AuthenticationMethod AS "Authentication Method" count AS Count
```

失敗したユーザ認証(Failed User Authentications)

この「統計情報テーブル」には、AuthenticationMethod タイプと失敗した仮想認証の数が示されます。これによって、円グラフを使用する代わりに失敗した認証の数を容易に表示できます。Splunk の検索文字列フィールドは引き続き同じです。必要なのは「円グラフ」の代わりに「統計情報テーブル」のビューを変更することだけです。このパネルでは、ユーザのコンテキスト情報と次の検索文字列変数が定義されます:ユーザ名、「UserName」、NAS IP アドレス、「Address」、発信側ステーション ID、「Calling_Station_ID」。失敗の理由、「FailureReason」も表示されます。

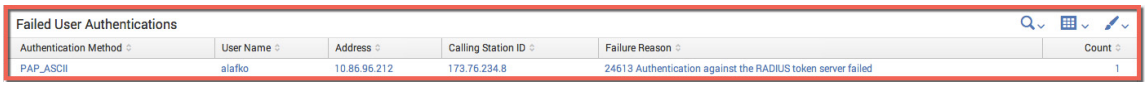


図 79.

検索文字列フィールド:

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Virtual" | stats count by
AuthenticationMethod UserName Address Calling_Station_ID FailureReason | `format
```

失敗した認証の概要(Failed Authentication Overview)

この「統計情報テーブル」には、ユーザのコンテキスト情報と次の検索文字列フィールドが表示されます:ユーザ名、「UserName」、発信側ステーション ID、「Calling_Station_ID」、トンネル クライアント エンドポイント、「Tunnel_Client_Endpoint」、PIX7x クライアント タイプ、「PIX7x_Client_Type」、PIX7x トンネル グループ名、「PIX7x_Tunnel_Group_Name」、ネットワーク デバイス名、「NetworkDeviceName」。また、失敗の理由が追加されます。

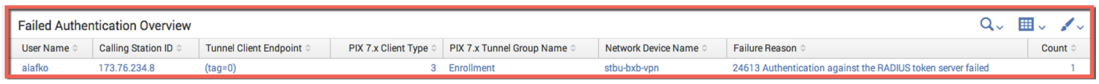


図 80.

検索文字列フィールド:

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Virtual" | stats count by
UserName Calling_Station_ID Tunnel_Client_Endpoint PIX7x_Client_Type PIX7x_Tunnel_Group_Name
NetworkDeviceName FailureReason | `format_field_names`
```

認証失敗の詳細(Authentication Failure Details)

この「統計情報テーブル」には、ユーザのコンテキスト情報を補完する NAS のコンテキスト情報が表示されます。NAS のコンテキスト情報と検索文字列フィールドは次のとおりです:ネットワーク デバイス グループ情報、「NetworkDeviceGroups」、ネットワーク デバイス タイプ、「Type」、NAS IP アドレス、「NAS_IP_Address」、NAS ポート、「NAS_port」。

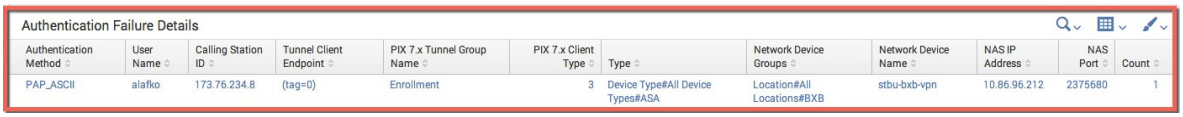


図 81.

検索文字列フィールド:

```
eventtype=cisco-ise-failed-authentication Location="$location$" NAS_Port_Type="Virtual" | stats count by
AuthenticationMethod UserName Calling_Station_ID Tunnel_Client_Endpoint PIX7x_Tunnel_Group_Name
PIX7x_Client_Type Type NetworkDeviceGroups NetworkDeviceName NAS_IP_Address NAS_Port |
`format_field_names`
```

デバイスの概要

デバイスの概要ビューは、すべてのロケーションのデバイスの概要、特定のロケーションのデバイスの概要、および特定のロケーションの不明なデバイスのダッシュボードから構成されます。これらのダッシュボードは通常、ロケーション別、およびネットワーク アクセス タイプ（有線ユーザ、無線ユーザ、仮想ユーザ）別のデバイスへの可視性を提供するために、ISE 管理者によって使用されます。たとえば、特定のロケーションごとに有線ユーザの推奨デバイスのみがネットワークに接続できるという企業ポリシーが存在する場合があります。HYD ロケーションの場合、有線ユーザはモバイル デバイスをネットワークに接続できません。[ISE 不明デバイス（ISE Unknown Devices）] ダッシュボードで、管理者はネットワークへの接続から ISE によって検出されていないデバイスを識別できます。

図 82.

- [ISE デバイスの概要-すべてのロケーション（ISE Device Summary- All Locations）]：組織全体の有線および無線ユーザのデバイスの概要が示されます。
- [ISE デバイスの概要-特定のロケーション（ISE Device Summary- Specific Location）]：ロケーション別のデバイスのサマリー情報が示されます。
- [ISE 不明デバイス-特定のロケーション（ISE Unknown Devices- Specific Location）]：ロケーション別の不明デバイスのサマリー情報が示されます。

すべてのロケーションの ISE デバイスの概要（ISE Device Summary for All Locations）

このダッシュボードとこれらのパネルには、すべてのユーザのロケーション別の組織全体からのデバイス情報が抽出されます。

組織全体のデバイスの概要（Device Summary across Organization）

この「円グラフ」には、「Location=”*”」、およびエンドポイントに一致したプロファイル、「EndPointMatchedProfile」検索文字列フィールドに基づいてすべてのロケーションのデバイスの概要が表示されます。これらのフィールドは、CISE_Passed_Authentication log_type に依存します。この情報を取得するには、エンドユーザが正常に ISE 認証に成功している必要があります。この「円グラフ」は、エンドポイント デバイスの割合とロケーション別のデバイスの数を表します。

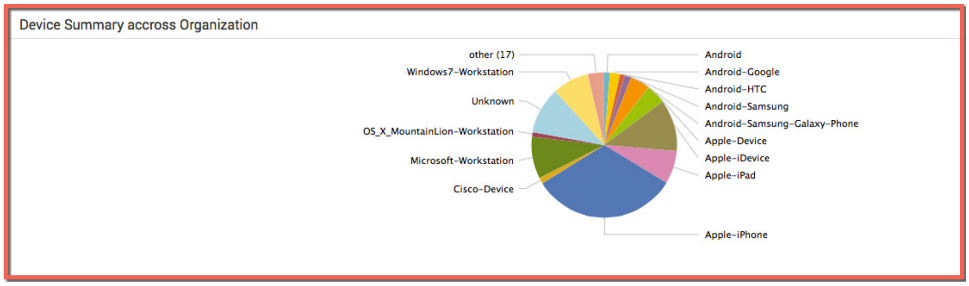


図 83.

検索文字列フィールド：

```
eventtype=cisco-ise NAS_Port_Type="*" | stats count by EndPointMatchedProfile | rename EndPointMatchedProfile
AS "Endpoint Matched Profile"
```

無線ユーザのデバイスの概要（Device Summary for Wireless Users）

この「円グラフ」には、「location=”*”」と一致したエンドポイント プロファイル、「EndPointMatchedProfile」に基づいて、組織全体のデバイスの概要が表示されます。無線ユーザは「NAS_Port_Type=Wireless- IEEE 802.11」変数によって定義されます。

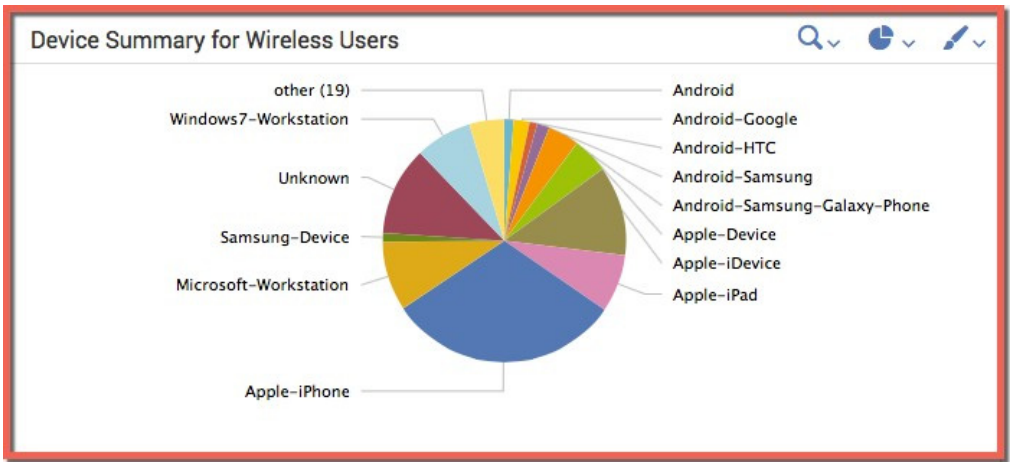


図 84.

検索文字列フィールド:

```
eventtype=cisco-ise NAS_Port_Type="Wireless - IEEE 802.11" | stats count by EndPointMatchedProfile |
rename EndPointMatchedProfile AS "Endpoint Matched Profile"
```

無題パネル（Untitled Panel）

この「統計情報テーブル」には、ロケーション別のデバイスのサマリー情報が示されます。この場合、統計情報テーブルには、ロケーション別のデバイス数へのさらなる可視性が提供されます。これらのロケーションの合計が組織内のデバイスの総数を構成します。

Untitled Panel

Matched Profile	Location	Count
Apple-iPhone	Location#All Locations#SJC#WNBU	2538
Unknown	Location#All Locations#SJC#WNBU	1661
Apple-iPhone	Location#All Locations#SJC#SJCM1	936
Windows7-Workstation	Location#All Locations#SJC#WNBU	897
Apple-iDevice	Location#All Locations#SJC#SJCM1	879
Apple-iPad	Location#All Locations#SJC#WNBU	705
Apple-iPhone	Location#All Locations#SJC#SJC24	589
Apple-iPhone	Location#All Locations#SJC#SJCN1	582
Microsoft-Workstation	Location#All Locations#SJC#WNBU	546
Apple-iDevice	Location#All Locations#SJC#WNBU	499

検索文字列フィールド:

```
eventtype=cisco-ise NAS_Port_Type="Wireless - IEEE 802.11" | fillnull value="No Location" Location |
stats count by EndPointMatchedProfile Location | sort -count | `format_field_names`
```

有線ユーザのデバイスの概要（Device Summary for Wired Users）

この「円グラフ」には、デバイス別のデバイスの割合と数が表示されます。

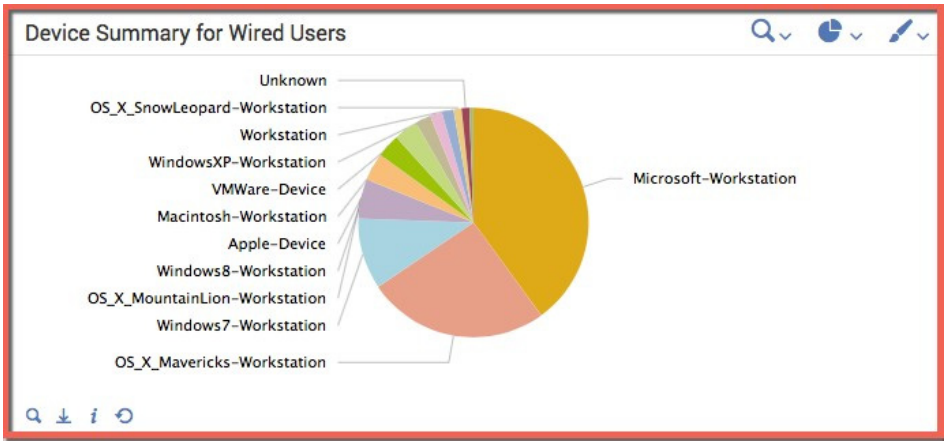


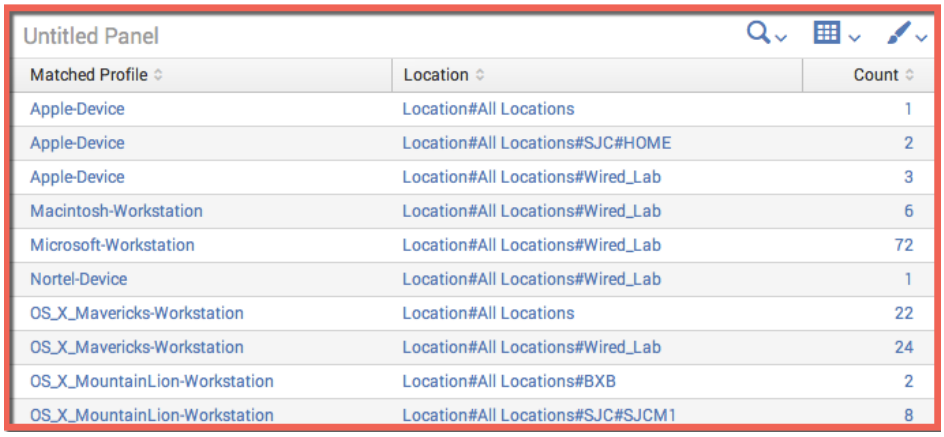
図 85.

検索文字列フィールド：

```
eventtype=cisco-ise NAS_Port_Type="Ethernet" | stats count by EndPointMatchedProfile | sort -count |
rename EndPointMatchedProfile AS "Endpoint Matched Profile"
```

無題パネル（Untitled Panel）

「統計情報テーブル」を使用した有線ユーザのデバイスの概要が示されます。このテーブルには、ロケーションおよび一致したエンドポイント プロファイル別のデバイスに基づくよりよい可視性の詳細が示されます。



Matched Profile	Location	Count
Apple-Device	Location#All Locations	1
Apple-Device	Location#All Locations#SJC#HOME	2
Apple-Device	Location#All Locations#Wired_Lab	3
Macintosh-Workstation	Location#All Locations#Wired_Lab	6
Microsoft-Workstation	Location#All Locations#Wired_Lab	72
Nortel-Device	Location#All Locations#Wired_Lab	1
OS_X_Mavericks-Workstation	Location#All Locations	22
OS_X_Mavericks-Workstation	Location#All Locations#Wired_Lab	24
OS_X_MountainLion-Workstation	Location#All Locations#BXB	2
OS_X_MountainLion-Workstation	Location#All Locations#SJC#SJCM1	8

図 86.

検索文字列フィールド：

```
eventtype=cisco-ise NAS_Port_Type="Ethernet" | fillnull value="No Location" Location | stats count by
EndPointMatchedProfile Location | `format_field_names`
```

デバイスの概要-特定のロケーション別（Device Summary- By Specific Location）

このダッシュボードとこれらのパネルには、すべてのユーザの HYD からデバイス情報が取得されます。有線および無線のユーザ タイプ用に個別のパネルが作成されました。

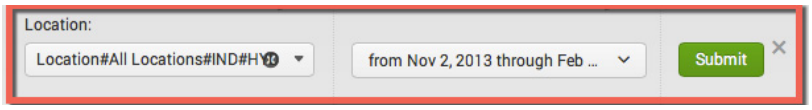


図 87.

Locations#HYD

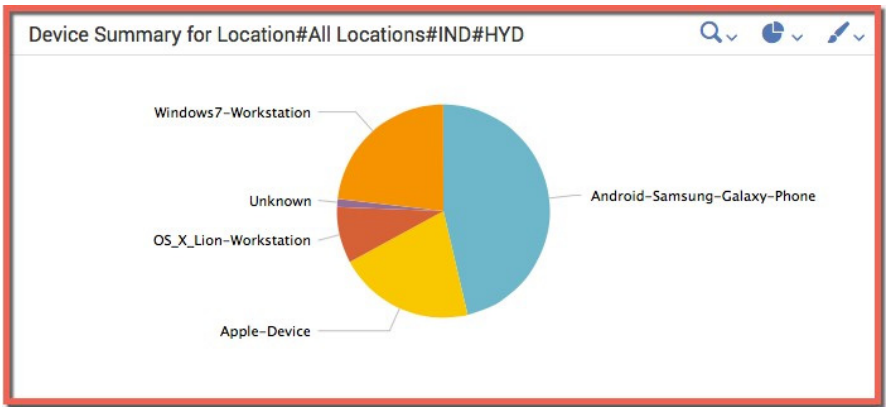


図 88.

検索文字列フィールド：

```
eventtype=cisco-ise Location="$location$" NAS_Port_Type="*" | stats count by EndPointMatchedProfile |
rename EndPointMatchedProfile AS "Endpoint Matched Profile"
```

デバイス数の内訳（Device Count Break Down）

この「統計情報テーブル」では、一致したエンドポイント プロファイル別のデバイスのデバイス数への可視性が提供されます。「EndPointMatchedProfile」、および「NAS_Port_Type=”*”」検索文字列変数は、すべてのユーザ タイプのデバイス情報を抽出します。

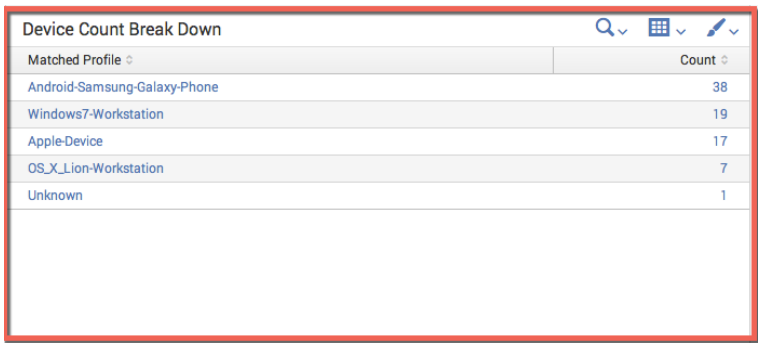


図 89.

検索文字列フィールド:

```
eventtype=cisco-ise Location="$location$" NAS_Port_Type="*" | stats count by EndPointMatchedProfile |
sort -count | `format_field_names`
```

有線ユーザのデバイス別操作ビュー(Operational View by Device for Wired Users)

この「円グラフ」には、「NAS_Port_Type=Ethernet」検索文字列変数で定義されているように、有線ユーザのみの一致したエンドポイント プロファイル別のデバイスの割合と数が示されます。

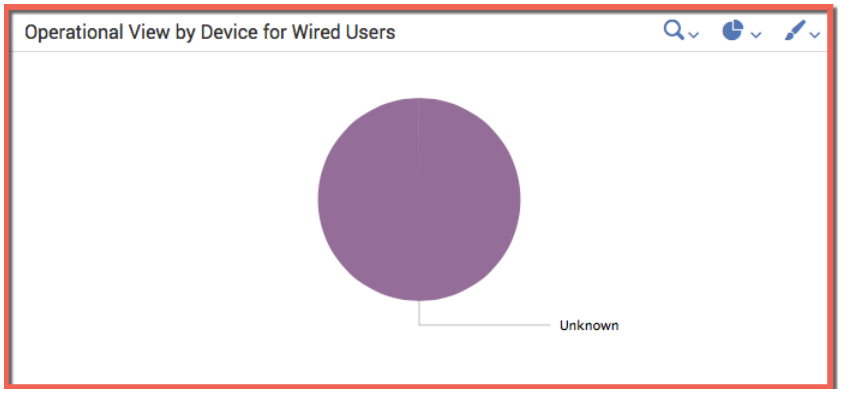


図 90.

検索文字列フィールド:

```
eventtype=cisco-ise Location="$location$" NAS_Port_Type="Ethernet" | stats count by EndPointMatchedProfile |
rename EndPointMatchedProfile AS "Endpoint Matched Profile"
```

有線ユーザのデバイスの詳細(Device Details for Wired Users)

この「統計情報テーブル」には、一致したエンドポイント プロファイルのユーザのコンテキスト情報が示されます。次に対する検索文字列変数:ユーザ名、「UserName」、エンドポイントの MAC アドレス、「EndPointMACAddress」、framed-ip-address、「Framed-IP- Address」。

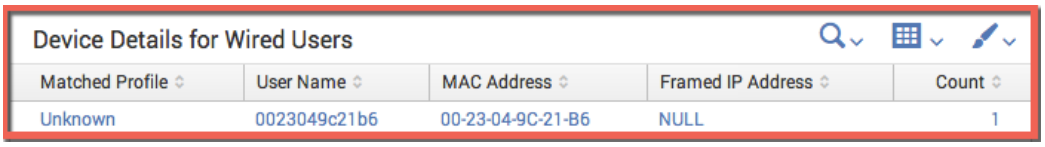


図 91.

検索文字列フィールド:

```
eventtype=cisco-ise Location="$location$" NAS_Port_Type="Ethernet" | fillnull value="NULL" Framed_IP_Address
| stats count by EndPointMatchedProfile UserName EndPointMACAddress Framed_IP_Address | sort -count |
`format_field_names`
```

無線ユーザのデバイス別操作ビュー（Operational View by Device for Wireless Users）

この「円グラフ」には、「NAS_Port_Type=Wireless - IEEE 802.11」検索文字列変数で定義されているように、無線ユーザのみの一致したエンドポイント プロファイル別のデバイスの割合と数が示されます。

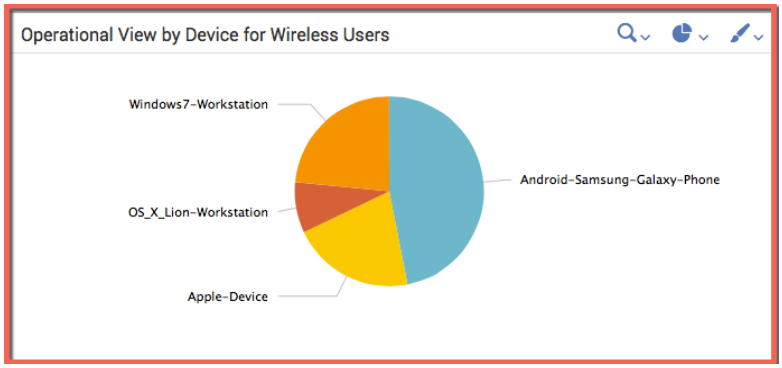


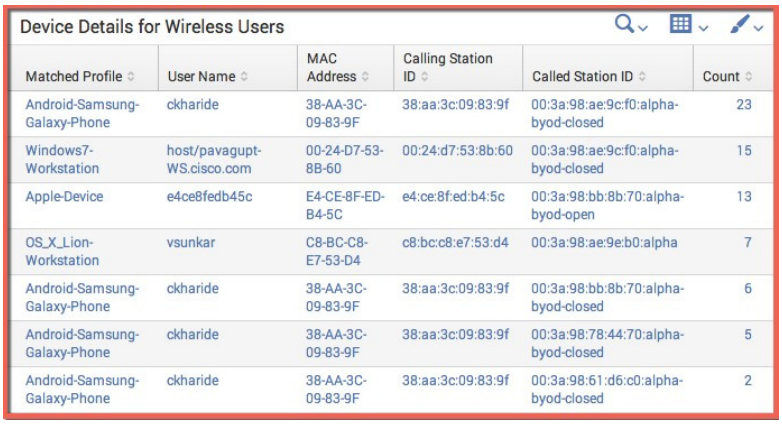
図 92.

検索文字列フィールド:

```
eventtype=cisco-ise Location="$location$" NAS_Port_Type="Wireless - IEEE 802.11" | stats count by
EndPointMatchedProfile | rename EndPointMatchedProfile AS "Endpoint Matched Profile"
```

無線ユーザのデバイスの詳細（Device Details for Wireless Users）

この「統計情報テーブル」には、追加の NAD コンテキスト情報、アイデンティティ グループ、および一致する承認条件ポリシー情報が示されます。NAD コンテキスト情報の検索文字列変数には、ネットワーク デバイス名、「NetworkDeviceName」、NAS_Port、「NAS_Port」が含まれます。IdentityGroup、「IdentityGroup」、認証 ID ストア「AuthenticationIdentityStore」、選択された承認プロファイル、「SelectedAuthorizationProfile」、承認ポリシーに一致したルール、「AuthorizationPolicyMatchedRule」もまた、より細かなデバイスの詳細を提供するために追加されました。


Device Details for Wireless Users

Matched Profile	User Name	MAC Address	Calling Station ID	Called Station ID	Count
Android-Samsung-Galaxy-Phone	ckharide	38-AA-3C-09-83-9F	38:aa:3c:09:83:9f	00:3a:98:ae:9c:f0:alpha-byod-closed	23
Windows7-Workstation	host/pavagupt-WS.cisco.com	00-24-D7-53-8B-60	00:24:d7:53:8b:60	00:3a:98:ae:9c:f0:alpha-byod-closed	15
Apple-Device	e4ce8fedb45c	E4-CE-8F-ED-B4-5C	e4:ce:8f:ed:b4:5c	00:3a:98:bb:8b:70:alpha-byod-open	13
OS_X_Lion-Workstation	vsunkar	C8-BC-C8-E7-53-D4	c8:bc:c8:e7:53:d4	00:3a:98:ae:9e:b0:alpha	7
Android-Samsung-Galaxy-Phone	ckharide	38-AA-3C-09-83-9F	38:aa:3c:09:83:9f	00:3a:98:bb:8b:70:alpha-byod-closed	6
Android-Samsung-Galaxy-Phone	ckharide	38-AA-3C-09-83-9F	38:aa:3c:09:83:9f	00:3a:98:78:44:70:alpha-byod-closed	5
Android-Samsung-Galaxy-Phone	ckharide	38-AA-3C-09-83-9F	38:aa:3c:09:83:9f	00:3a:98:61:d6:c0:alpha-byod-closed	2

図 93.

検索文字列フィールドは次のとおりです。

```
eventtype=cisco-ise Location="$location$" NAS_Port_Type="Wireless - IEEE 802.11" | fillnull value="NULL"
Called_Station_ID | stats count by EndPointMatchedProfile UserName EndPointMACAddress Calling_Station_ID
Called_Station_ID | sort -count | `format_field_names`
```

特定のロケーション別の不明デバイス

不明なデバイスには特記が必要です。この場合は、WNBU ロケーションの不明デバイスを調べます。これらのダッシュボードは通常 ISE 管理者によって使用され、ロケーション、IP アドレス、および認証情報別に不明デバイスを識別するのに役立ちます。

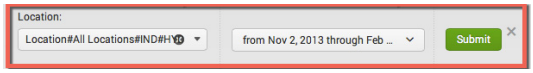


図 94.

Location#HYD

この「円グラフ」には、WNBU ロケーションの成功および失敗したユーザ認証の割合と不明デバイスの数が示されます。WNBU ロケーションの検索文字列変数は「Location=”*WNBU”」として定義され、不明デバイスは EndPointMatchedProfile=”Unknown” によって定義されます。

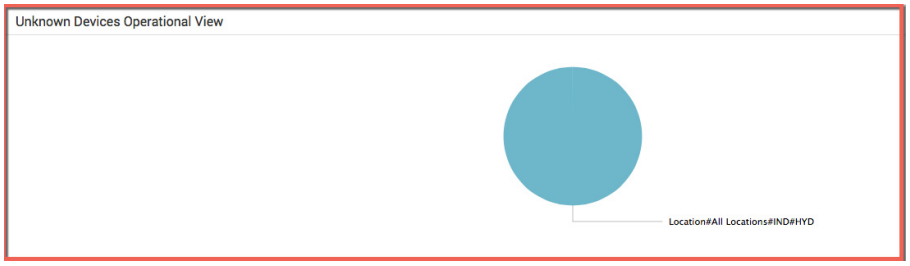


図 95.

検索文字列フィールド:

```
eventtype=cisco-ise EndPointMatchedProfile="Unknown" Location="$location$" | chart count by Location
```

不明デバイス-成功した認証（Unknown Devices- Passed Authentication）

この「円グラフ」には、検索文字列変数名「UserName」によって定義されているように、ユーザ名経由で成功したユーザ認証の割合と不明デバイスの数が示されます。

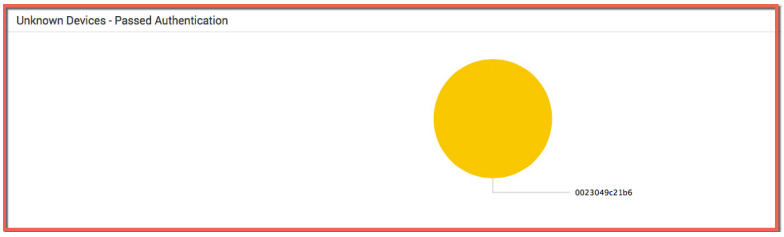


図 96.

検索文字列フィールド：

```
eventtype=cisco-ise-passed-authentication EndPointMatchedProfile="Unknown" Location="$location$" | chart
count by UserName
```

無題パネル（Untitled Panel）

この「統計情報テーブル」には、既知のデバイスの識別に役立つコンテキスト ユーザ情報、EAP 認証の詳細、および NAD コンテキスト情報が提供されます。ユーザのコンテキスト情報検索文字列変数には、ユーザ名、「UserName」、エンドポイントの MAC アドレス、「EndpointMACAddress」、IdentityGroup、「IdentityGroup」、ID ストア、「AuthenticationIdentityStore」が含まれています。

EAP 認証の詳細には、EAP 認証方式、「AuthenticationMethod」、EAP 認証、「EapAuthentication」が含まれています。

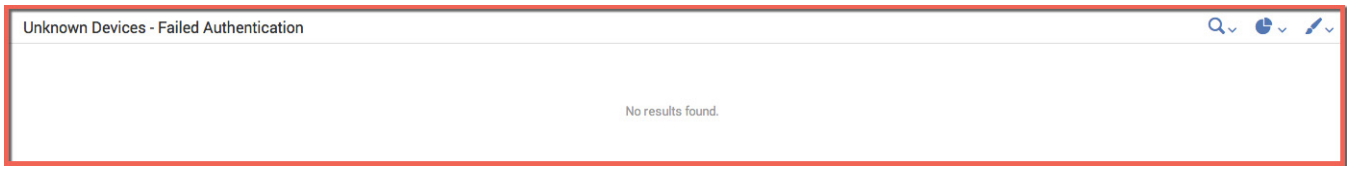
NAS コンテキスト情報には、NAS IP アドレス、「NAS_IP_Address」、NAS_Port、「NAS_Port」、ネットワーク デバイス名、「NetworkDeviceName」、ネットワーク デバイス グループ、「NetworkDeviceGroups」が含まれています。

検索文字列フィールドは次のとおりです。

```
eventtype=cisco-ise-passed-authentication EndPointMatchedProfile="Unknown" Location="$location$" | fillnull
value="NULL" EapAuthentication | stats count by EndPointMACAddress UserName IdentityGroup
AuthenticationMethod EapAuthentication NAS_IP_Address NAS_Port NetworkDeviceName NetworkDeviceGroups
```

不明デバイス-失敗した認証（Unknown Devices-Failed Authentication）

この「円グラフ」には、失敗した認証のユーザ試行の失敗の理由が示されます。これは、EAP 障害と関係があるかどうかを確認するために不明デバイスを識別するのに役立ちます。検索文字列変数は「FailureReason」です。



検索文字列フィールドは次のとおりです。

```
eventtype=cisco-ise-failed-authentication EndPointMatchedProfile="Unknown" Location="$location$" | chart
count by FailureReason
```

無題パネル（Untitled Panel）

この「統計情報テーブル」には、失敗の理由に関するユーザおよび NAS のコンテキスト情報が提供されます。

ユーザのコンテキスト情報には、次の検索文字列が含まれています：ユーザ名、「UserName」、エンドポイントの MAC アドレス、「EndPointMACAddress」、IdentityGroup、「IdentityGroup」。

NAS のコンテキスト情報には、次のものが含まれています：NAS_Identifier、「NAS_Identifier」、NAS_IP_Address、「NAS_IP_Address」、NAS_Port、「NAS_Port」、ネットワーク デバイス名、「NetworkDeviceName」。

EAP 認証の詳細には、認証方式、「AuthenticationMethod」、EAP 認証、「EapAuthentication」、EAP トンネル、「EapTunnel」が含まれています。

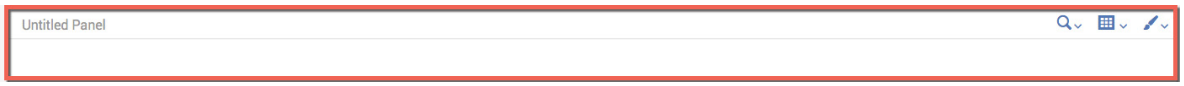


図 97.

検索文字列フィールドは次のとおりです。

```
eventtype=cisco-ise-failed-authentication EndPointMatchedProfile="Unknown" Location="$location$" | fillnull
value="NULL" EapAuthentication | stats count by FailureReason EndPointMACAddress UserName IdentityGroup
AuthenticationMethod EapAuthentication NAS_Identifier NAS_IP_Address NAS_Port NetworkDeviceName
NetworkDeviceGroups | `format_field_names`
```

ポスチャ（Posture）

ISE ポスチャウイルス対策（AV）（すべてのユーザ）（ISE Posture Antivirus (AV) (all Users)）

このダッシュボードとこれらのパネルには、インストール済み AV、準拠/非準拠のコンテキスト ユーザ情報およびポスチャ ポリシーの詳細が表示されます。これらのダッシュボードは通常、すべてのユーザに AV またはスパイウェア対策（AS）がインストールされている必要があるなどといった、企業のポスチャ セキュリティ ポリシーを順守するために、ISE 管理者によって使用されます。どのユーザが準拠していてどのユーザが準拠していないかは、失敗したポスチャのチェックと、配置されたポスチャ ポリシーに基づきます。

インストール済み AV（AV Installed）

この「円グラフ」は、「AntivirusInstalled」検索文字列変数に基づいてインストールされているウイルス対策の割合を表します。

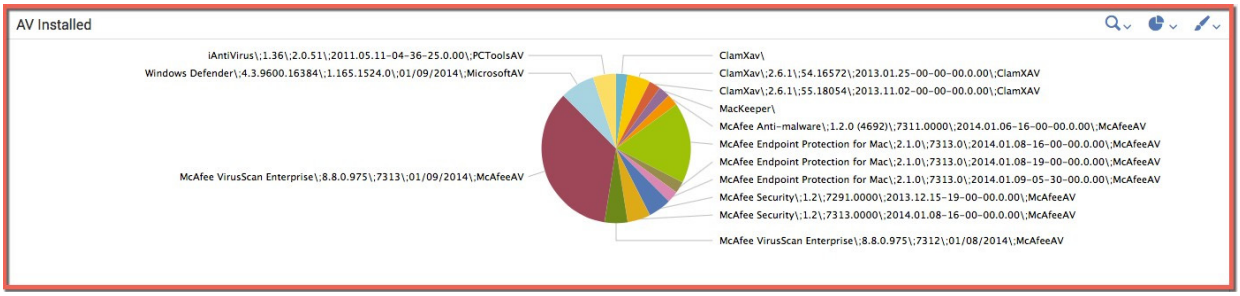


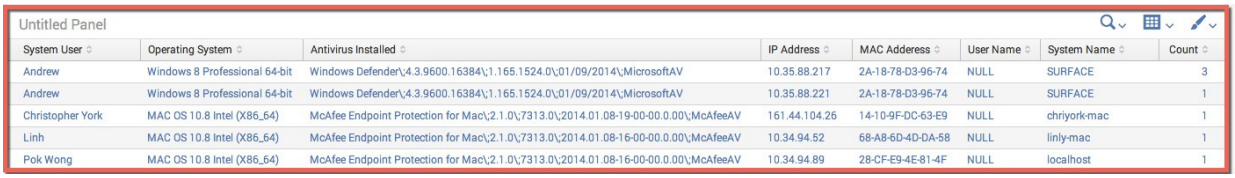
図 98.

検索文字列フィールド：

```
eventtype=cisco-ise | stats count by AntiVirusInstalled |rename AntiVirusInstalled AS "Antivirus Installed"
```

無題パネル（Untitled Panel）

この「統計情報テーブル」には、ユーザのコンテキスト情報と次の検索文字列変数が示されます：ユーザ名、「UserName」、システム名、「SystemName」、エンドポイントの MAC アドレス、「MACAddress」、オペレーティング システム、「OperatingSystem」、システム ユーザ、「SystemUser」情報。また、「AntivirusInstalled」および NAS IP アドレスに追加されます。


Untitled Panel

System User	Operating System	Antivirus Installed	IP Address	MAC Adderess	User Name	System Name	Count
Andrew	Windows 8 Professional 64-bit	Windows Defender\;4.3.9600.16384\;1.165.1524.0\;01/09/2014\;MicrosoftAV	10.35.88.217	2A-18-78-D3-96-74	NULL	SURFACE	3
Andrew	Windows 8 Professional 64-bit	Windows Defender\;4.3.9600.16384\;1.165.1524.0\;01/09/2014\;MicrosoftAV	10.35.88.221	2A-18-78-D3-96-74	NULL	SURFACE	1
Christopher York	MAC OS 10.8 Intel (X86_64)	McAfee Endpoint Protection for Mac\;2.1.0\;7313.0\;2014.01.08-19-00-00.0.00\;McAfeeAV	161.44.104.26	14-10-9F-DC-63-E9	NULL	chriyork-mac	1
Linh	MAC OS 10.8 Intel (X86_64)	McAfee Endpoint Protection for Mac\;2.1.0\;7313.0\;2014.01.08-16-00-00.0.00\;McAfeeAV	10.34.94.52	68-A8-6D-4D-DA-58	NULL	linly-mac	1
Pok Wong	MAC OS 10.8 Intel (X86_64)	McAfee Endpoint Protection for Mac\;2.1.0\;7313.0\;2014.01.08-16-00-00.0.00\;McAfeeAV	10.34.94.89	28-CF-E9-4E-81-4F	NULL	localhost	1

図 99.

検索文字列フィールド：

```
eventtype=cisco-ise AntiVirusInstalled="*" | fillnull value="NULL" UserName | stats count by SystemUser
OperatingSystem AntiVirusInstalled IpAddress MacAddress UserName SystemName |          `format_field_names`
```

コンプライアンス/コンプライアンス違反（Compliance/Non-Compliance）

この「円グラフ」は、ISE ポスチャ レポートの結果と「PostureStatus」変数に基づいて準拠/非準拠/不明ユーザの割合を表します。

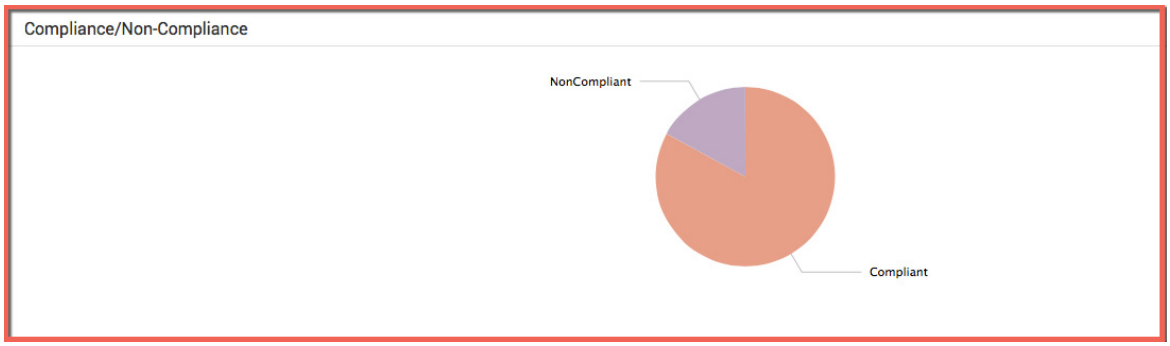


図 100.

検索文字列フィールド：

```
eventtype=cisco-ise cise_posture_and_client_provisioning_audit PostureStatus="*" | stats count by
PostureStatus | rename PostureStatus AS "Posture Status"
```

無題パネル（Untitled Panel）

この「統計情報テーブル」には、PostureReport の詳細とともにユーザのコンテキスト情報が表示されます。

Posture Status	User Name	IP Address	MAC Adderess	Posture Report	Antivirus Installed
NonCompliant	iskiber	192.168.1.18	10-DD-B1-C9-3C-39	MacTEST\;Failed\; (Any_AV_Installation_Mac:Mandatory:Failed:Passed_Conditions[]:Failed_Conditions[pc_av_mac_inst_ANY_vendor]:Skipped_Conditions[])	NULL
NonCompliant	jeppich	192.168.1.13	10-DD-B1-C9-3C-39	MacTEST\;Failed\; (Any_AV_Installation_Mac:Mandatory:Failed:Passed_Conditions[]:Failed_Conditions[pc_av_mac_inst_ANY_vendor]:Skipped_Conditions[])	NULL
NonCompliant	jeppich	192.168.1.14	10-DD-B1-C9-3C-39	MacTEST\;Failed\; (Any_AV_Installation_Mac:Mandatory:Failed:Passed_Conditions[]:Failed_Conditions[pc_av_mac_inst_ANY_vendor]:Skipped_Conditions[])	NULL
NonCompliant	jeppich	192.168.1.15	10-DD-B1-C9-3C-39	MacTEST\;Failed\; (Any_AV_Installation_Mac:Mandatory:Failed:Passed_Conditions[]:Failed_Conditions[pc_av_mac_inst_ANY_vendor]:Skipped_Conditions[])	NULL
NonCompliant	jeppich	192.168.1.18	10-DD-B1-C9-3C-39	MacTEST\;Failed\; (Any_AV_Installation_Mac:Mandatory:Failed:Passed_Conditions[]:Failed_Conditions[pc_av_mac_inst_ANY_vendor]:Skipped_Conditions[])	NULL
NonCompliant	relwell	192.168.1.13	10-DD-B1-C9-3C-39	MacTEST\;Failed\; (Any_AV_Installation_Mac:Mandatory:Failed:Passed_Conditions[]:Failed_Conditions[pc_av_mac_inst_ANY_vendor]:Skipped_Conditions[])	NULL
Compliant	CISCO\\saavula	10.34.94.41	24-77-03-3D-D2-FC	McAfee_AV_Installation_Win\;Passed\; (McAfee_AV_Installation_Win:Audit:Passed:Passed_Conditions[av_inst_ANY_of_McAfeeAV]:Failed_Conditions[]:Skipped_Conditions[])	McAfee VirusScan Enterprise\;8.8.0.975\;7313\;01/09/2014\;M
Compliant	CISCO\\tgong	161.44.64.247	F0-DE-F1-4E-0E-61	McAfee_AV_Installation_Win\;Passed\; (McAfee_AV_Installation_Win:Audit:Passed:Passed_Conditions[av_inst_ANY_of_McAfeeAV]:Failed_Conditions[]:Skipped_Conditions[])	McAfee VirusScan Enterprise\;8.8.0.975\;7313\;01/09/2014\;M

図 101.

検索文字列フィールド：

```
eventtype=cisco-ise cise_posture_and_client_provisioning_audit | fillnull value="NULL" UserName
AntiVirusInstalled | stats count by PostureStatus UserName IpAddress MacAddress PostureReport
AntiVirusInstalled | `format_field_names`
```

ポスチャポリシー（Posture Policies）

この「円グラフ」は、ポスチャ レポートに基づいて ISE のポスチャ ポリシーの割合を表します。

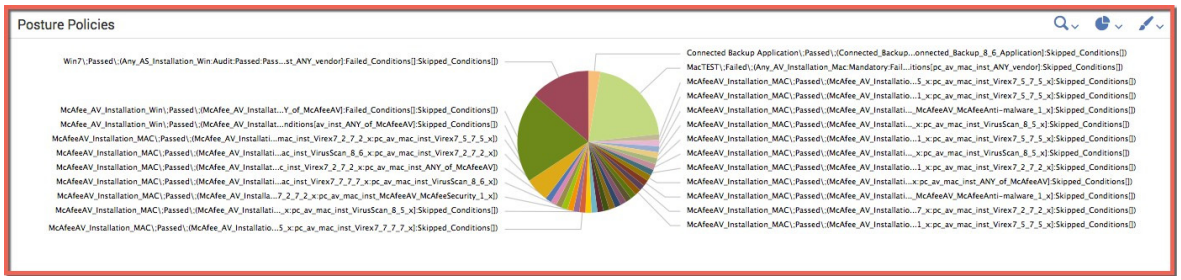


図 102.

検索文字列フィールド:

```
eventtype=cisco-ise cise_posture_and_client_provisioning_audit | stats count by PostureReport |
rename PostureReport AS "Posture Report"
```

ISE ポスチャスパイウェア対策(AS)(すべてのユーザ)(ISE Posture AntiSpyware (AS) (all Users))

このダッシュボードとこれらのパネルには、インストール済み AS、準拠/非準拠ユーザ情報と詳細が表示されます。これらのダッシュボードは通常、すべてのユーザに AV またはスパイウェア対策(AS)がインストールされている必要があるなどといった、企業のポスチャ セキュリティ ポリシーを順守するために、ISE 管理者によって使用されます。どのユーザが準拠していてどのユーザが準拠していないかは、失敗したポスチャのチェックと、配置されたポスチャ ポリシーに基づきます。

インストール済みスパイウェア対策(AntiSpyware Installed)

この「円グラフ」には、「AntispywareInstalled」検索文字列変数に基づいてインストール済みスパイウェア対策の割合と詳細が表示されます。

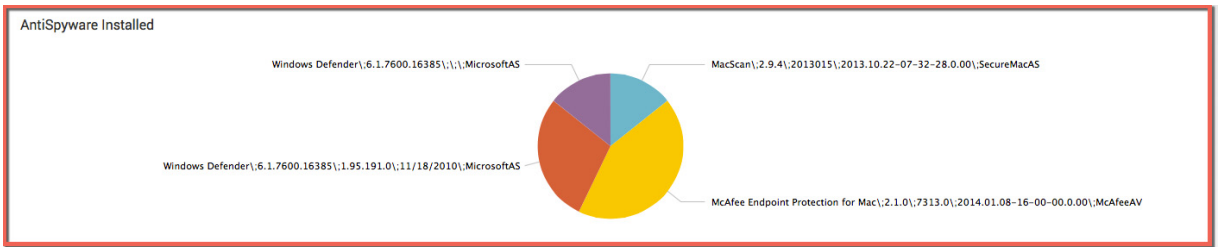


図 103.

検索文字列フィールド:

```
eventtype=cisco-ise | stats count by AntiSpywareInstalled | rename AntiSpywareInstalled AS "AntiSpyware
Installed"
```

無題パネル(Untitled Panel)

この「統計情報テーブル」には、ユーザのコンテキスト情報と次の検索文字列が示されます:ユーザ名、「UserName」、システム ユーザ、「SystemUser」、システム名、「SystemName」、エンドポイントの MAC アドレス、「MACAddress」、オペレーティング システム、「OperatingSystem」。また、インストール済み AS の詳細への NAS IP アドレスが含まれています。

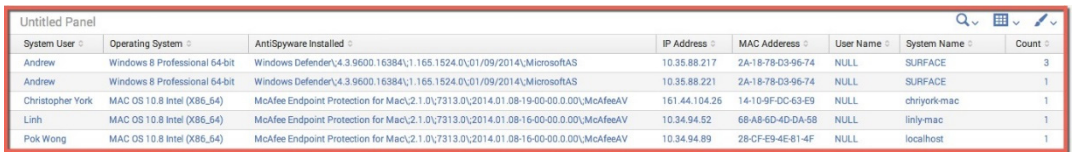


図 104.

検索文字列フィールド:

```
eventtype=cisco-ise AntiSpywareInstalled="*" | fillnull value="NULL" UserName | stats count by SystemUser
OperatingSystem AntiSpywareInstalled IpAddress MacAddress UserName SystemName |          `format_field_names`
```

準拠/非準拠（Compliant/Non-Compliant）

この「円グラフ」には、ISE ポスチャ レポートの結果と PostureStatus 検索文字列変数に基づいて準拠/非準拠/不明ユーザの割合が表示されます。

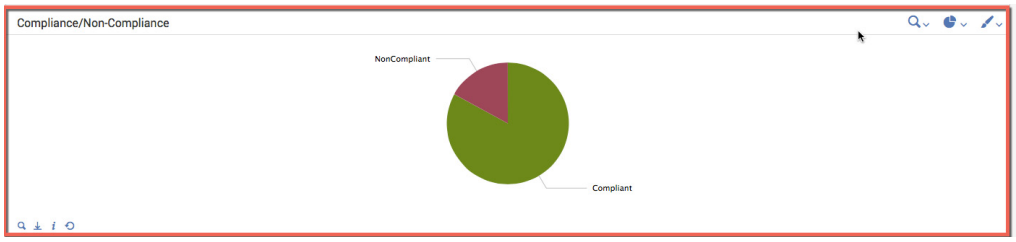


図 105.

検索文字列フィールド:

```
eventtype=cisco-ise cise_posture_and_client_provisioning_audit PostureStatus="*" | stats count
```

無題パネル（Untitled Panel）

この「統計情報テーブル」には、ポスチャ詳細へのユーザのコンテキスト情報が示されます。

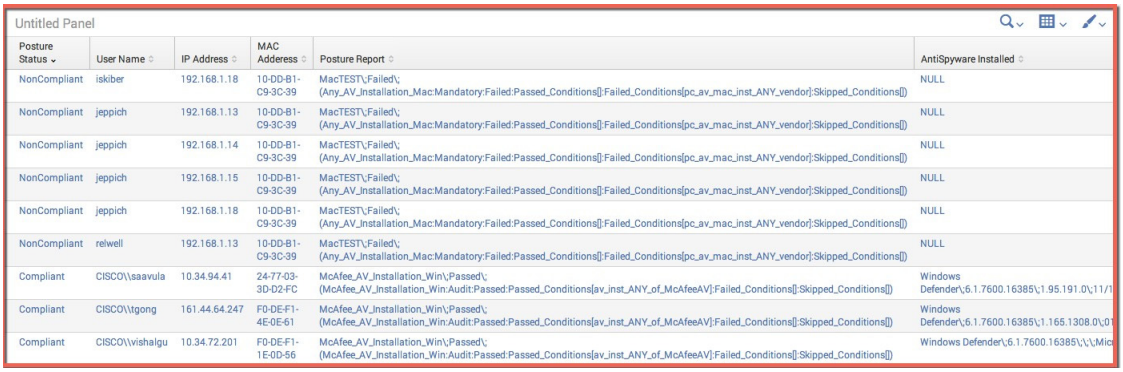


図 106.

検索文字列フィールド:

```
eventtype=cisco-ise cise_posture_and_client_provisioning_audit | fillnull value="NULL" UserName
AntiSpywareInstalled | stats count by PostureStatus UserName IpAddress MacAddress PostureReport
AntiSpywareInstalled | `format_field_names`
```

ポスチャポリシー（Posture Policies）

この「円グラフ」は、「PostureReport」検索文字列に基づくポスチャ レポートに基づいて ISE のポスチャ ポリシーの割合を表します。

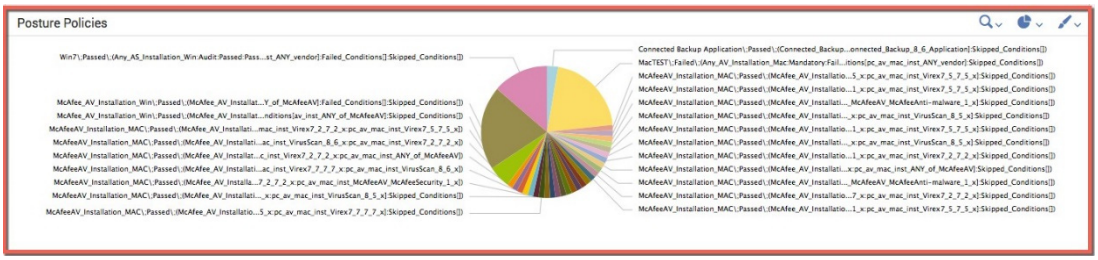


図 107.

検索文字列フィールド：

```
eventtype=cisco-ise cise_posture_and_client_provisioning_audit | stats count by PostureReport |
rename PostureReport AS "Posture Report"
```

クライアント プロビジョニング

[ISE クライアントプロビジョニング（ISE Client Provisioning）] ダッシュボードでは、ユーザのコンテキスト情報を含む成功/失敗したクライアント プロビジョニング パネルが提供されます。これらのダッシュボードは通常、ユーザ名別に成功したクライアント プロビジョニングへの可視性を提供し、失敗の理由のイベント別に失敗したクライアント プロビジョニングの試行を診断するために、ISE 管理者によって使用されます。

成功したクライアントプロビジョニング（Successful Client Provisioning）

このダッシュボードとこれらのパネルには、成功および失敗したクライアント プロビジョニングの詳細が表示されます。

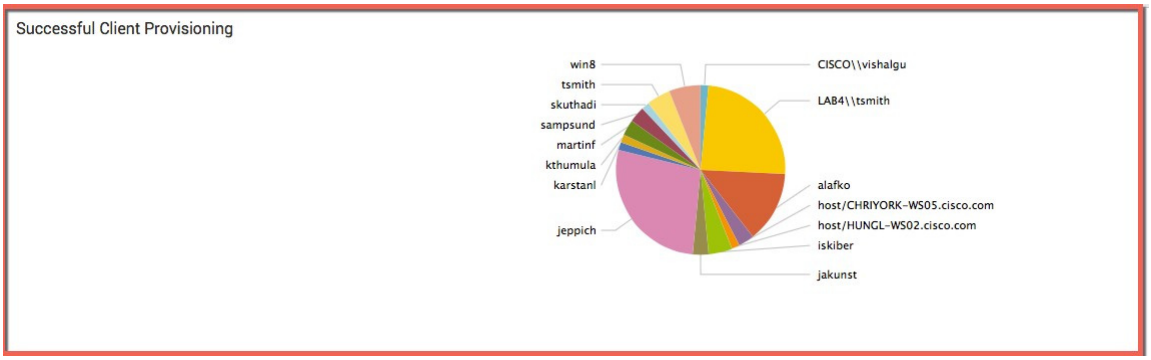


図 108.

検索文字列フィールドは次のとおりです。

```
eventtype=cisco-ise-provision-succeeded | stats count by UserName | rename UserName AS "User Name"
```

無題パネル（Untitled Panel）

この「統計情報テーブル」には、プロビジョニングの詳細に追加するための次のユーザのコンテキスト情報が表示されます：ユーザ名、エンドポイントの MAC アドレス、一致したポスチャ ポリシー、およびポスチャ エージェント バージョン。


Untitled Panel

User Name	IP Address	MAC Adderess	Posture Policy Matched	Posture Agent Version	Count
CISCO\\vishalgu	10.34.72.201	F0-DE-F1-1E-0D-56	SJCM1-WIN	NACAgent:4.9.0.1013	1
LAB4\\tsmith	192.168.1.17	F0-DE-F1-94-65-9C	Win81_revised	NACAgent:4.9.0.1009	10
host/CHRIYORK-WS05.cisco.com	161.44.104.29	24-77-03-36-EA-74	Win-CPP-BXB	NACAgent:4.9.0.1013	2
host/HUNGL-WS02.cisco.com	161.44.104.24	3C-A9-F4-21-4A-98	Win-CPP-BXB	NACAgent:4.9.0.1013	1
iskiber	192.168.1.18	10-DD-B1-C9-3C-39	Win81_revised	MacOsXAgent:4.9.0.1007	2
jakunst	10.81.4.11	7C-D1-C3-92-B6-6C	Android-CP-OEAP	MacOsXAgent:4.9.0.1007	2
jeppich	192.168.1.13	10-DD-B1-C9-3C-39	Win81	MacOsXAgent:4.9.0.1007	1
jeppich	192.168.1.15	10-DD-B1-C9-3C-39	Win81_revised	MacOsXAgent:4.9.0.1007	7

図 109.

検索文字列フィールド：

```
eventtype=cisco-ise-provision-succeeded | stats count by UserName IpAddress MacAddress PosturePolicyMatched
PostureAgentVersion | `format_field_names`
```

クライアントプロビジョニングの失敗（Client Provisioning Failures）

この「円グラフ」には、ユーザ名別の割合と失敗したクライアント プロビジョニングの試行が表示されます。

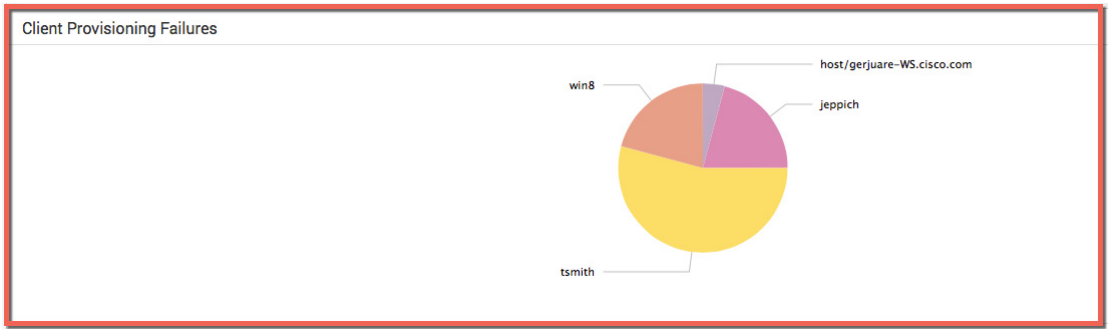


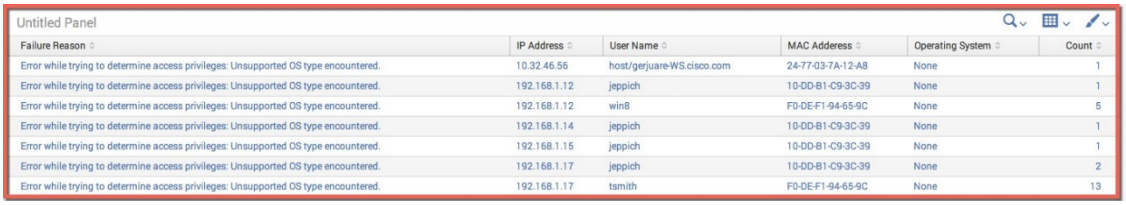
図 110.

検索文字列フィールド：

```
eventtype=cisco-ise-provision-failed | stats count by UserName | rename UserName AS "User Name"
```

無題パネル（Untitled Panel）

この「統計情報テーブル」には、失敗の理由に関するユーザのコンテキスト情報が表示されます。


Untitled Panel

Failure Reason	IP Address	User Name	MAC Address	Operating System	Count
Error while trying to determine access privileges: Unsupported OS type encountered.	10.32.46.56	host/gerjuare-WS.cisco.com	24-77-03-7A-12-A8	None	1
Error while trying to determine access privileges: Unsupported OS type encountered.	192.168.1.12	jeppich	10-DD-B1-C9-3C-39	None	1
Error while trying to determine access privileges: Unsupported OS type encountered.	192.168.1.12	win8	F0-DE-F1-94-65-9C	None	5
Error while trying to determine access privileges: Unsupported OS type encountered.	192.168.1.14	jeppich	10-DD-B1-C9-3C-39	None	1
Error while trying to determine access privileges: Unsupported OS type encountered.	192.168.1.15	jeppich	10-DD-B1-C9-3C-39	None	1
Error while trying to determine access privileges: Unsupported OS type encountered.	192.168.1.17	jeppich	10-DD-B1-C9-3C-39	None	2
Error while trying to determine access privileges: Unsupported OS type encountered.	192.168.1.17	tsmith	F0-DE-F1-94-65-9C	None	13

図 111.

検索文字列フィールド：

```
eventtype=cisco-ise-provision-failed | stats count by FailureReason IpAddress UserName MacAddress
OperatingSystem | `format_field_names`
```

コンプライアンス

コンプライアンス ビューは次のダッシュボードで構成されています。ISE 管理者はダッシュボードを使用して、ロケーション別の準拠/非準拠ユーザを可視化します。ダッシュボードには、すべてのユーザと特に無線ユーザの内訳も示されます。管理者は、企業のセキュリティ ポリシーに従うこともでき、どのロケーションおよびユーザが準拠しているか、または準拠していないかをメモできます。

図 112.

- [すべてのユーザのロケーション別の ISE コンプライアンスサマリー（ISE Compliance Summary by Location for All users）]：すべての有線ユーザ、無線ユーザ、仮想ユーザのロケーション別の詳細なユーザ コンプライアンス情報が提供されます。
- [無線ユーザのロケーション別の ISE コンプライアンスサマリー（ISE Compliance Summary by Location for Wireless Users）]：すべての無線ユーザのロケーション別の詳細なユーザ コンプライアンス情報が提供されます。

すべてのユーザのロケーション別の ISE コンプライアンスサマリー（ISE Compliance Summary By Location for All Users）

このダッシュボードとこれらのパネルには、すべてのユーザのロケーション別に、コンプライアンス サマリー イベントが表示され、コンプライアンス/コンプライアンス違反/不明な操作ビューが表示され、それらのビューに関するユーザのコンテキスト情報が示されます。

ロケーション別準拠ユーザ（Compliant Users by Location）

この「円グラフ」は、「PostureStatus=Compliant」および stats count by location を使用してロケーション別に準拠ユーザの割合を表します。

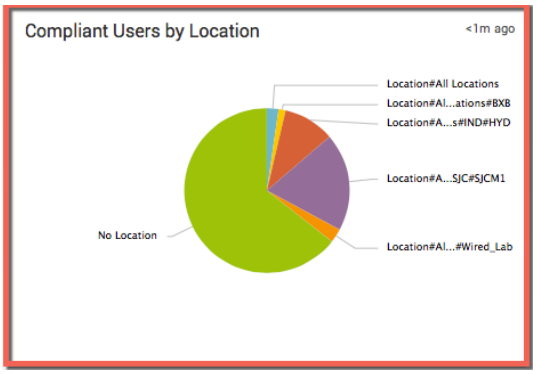


図 113.

検索文字列フィールド：

```
eventtype=cisco-ise PostureStatus="Compliant" | fillnull value="No Location" Location | stats count by Location
```

ロケーション別非準拠ユーザ（Non-Compliant Users by Location）

この「円グラフ」には、「PostureStatus=NonCompliant」および stats count by location 検索文字列変数によって定義されているように、ロケーション別に非準拠ユーザの割合と数が表示されます。

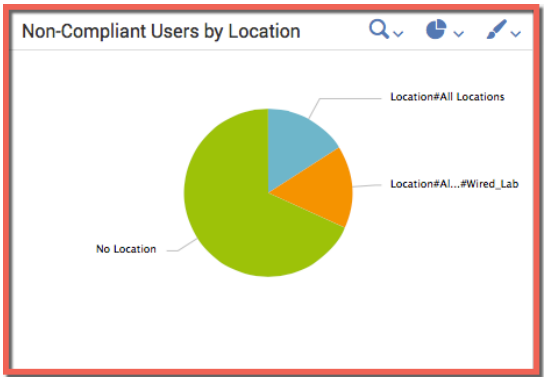


図 114.

検索文字列フィールド：

```
eventtype=cisco-ise PostureStatus="NonCompliant" | fillnull value="No Location" Location |        stats
count by Location
```

ロケーション別不明ユーザ（Unknown Users By Location）

この「統計情報テーブル」には、ロケーション別に不明ユーザ ポスチャ ステータスの割合と数が表示されます。

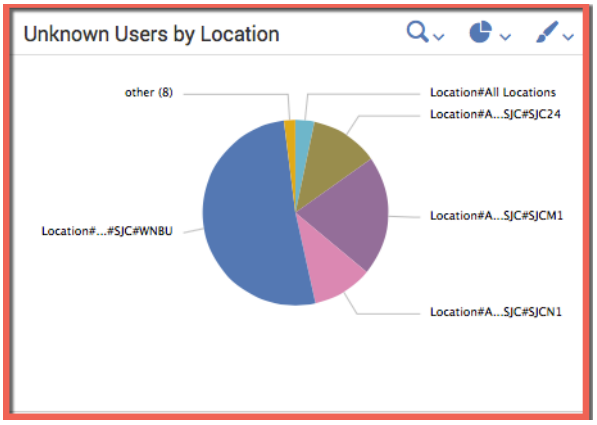


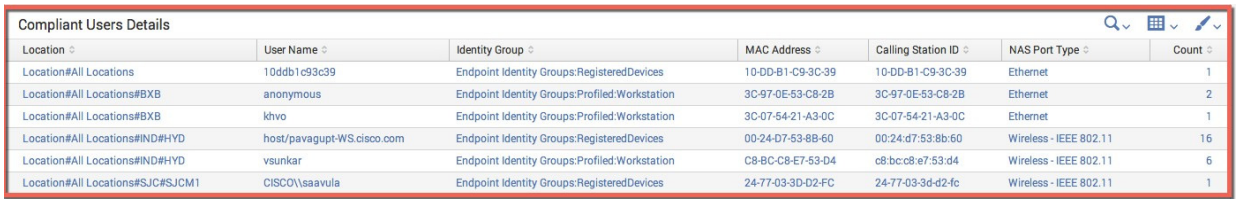
図 115.

検索文字列フィールドは次のとおりです。

```
eventtype=cisco-ise PostureStatus="Unknown" | fillnull value="No Location" Location |        stats count by
Location
```

準拠ユーザの詳細（Compliant Users Details）

この「統計情報テーブル」には、詳細なコンプライアンス情報に関する次のユーザのコンテキスト情報が表示されます：ユーザ名、エンドポイントの MAC アドレス、NAS IP アドレス、エンドポイントに一致したプロファイル。



Compliant Users Details

Location	User Name	Identity Group	MAC Address	Calling Station ID	NAS Port Type	Count
Location#All Locations	10ddb1c93c39	Endpoint Identity Groups:RegisteredDevices	10-DD-B1-C9-3C-39	10-DD-B1-C9-3C-39	Ethernet	1
Location#All Locations#BXB	anonymous	Endpoint Identity Groups:Profiled:Workstation	3C-97-0E-53-C8-2B	3C-97-0E-53-C8-2B	Ethernet	2
Location#All Locations#BXB	khvo	Endpoint Identity Groups:Profiled:Workstation	3C-07-54-21-A3-0C	3C-07-54-21-A3-0C	Ethernet	1
Location#All Locations#IND#HYD	host/pavagupt-WS.cisco.com	Endpoint Identity Groups:RegisteredDevices	00-24-D7-53-8B-60	00:24:d7:53:8b:60	Wireless - IEEE 802.11	16
Location#All Locations#IND#HYD	vsunkar	Endpoint Identity Groups:Profiled:Workstation	C8-BC-C8-E7-53-D4	c8:bc:c8:e7:53:d4	Wireless - IEEE 802.11	6
Location#All Locations#SJC#SJCM1	CISCO\\saavula	Endpoint Identity Groups:RegisteredDevices	24-77-03-3D-D2-FC	24-77-03-3d-d2-fc	Wireless - IEEE 802.11	1

図 116.

検索文字列フィールド：

```
eventtype=cisco-ise PostureStatus="Compliant" | fillnull value="No Location" Location           stats count
by Location UserName IdentityGroup EndPointMACAddress Calling Station ID NAS Port Type | `format field names`
```

非準拠ユーザの詳細（Non-Compliant Users Details）

Non-Compliant Users Details

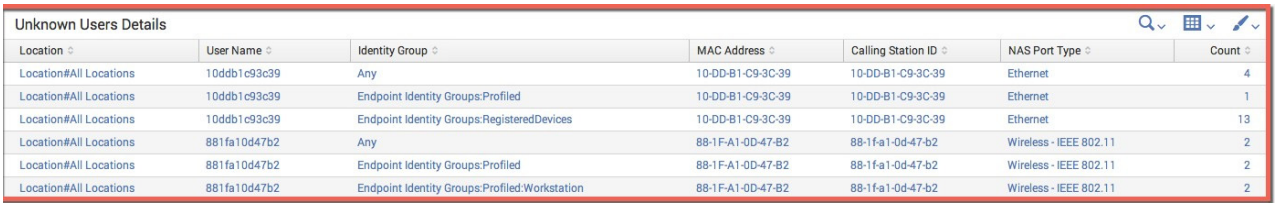
Location	User Name	Identity Group	MAC Address	Calling Station ID	NAS Port Type	Count
Location#All Locations	jeppich	Endpoint Identity Groups:RegisteredDevices	10-DD-B1-C9-3C-39	10-DD-B1-C9-3C-39	Ethernet	2
Location#All Locations#Wired_Lab	iskiber	Endpoint Identity Groups:RegisteredDevices	10-DD-B1-C9-3C-39	10-DD-B1-C9-3C-39	Ethernet	1
Location#All Locations#Wired_Lab	jeppich	Endpoint Identity Groups:Profiled:Workstation	10-DD-B1-C9-3C-39	10-DD-B1-C9-3C-39	Ethernet	5
Location#All Locations#Wired_Lab	relwell	Endpoint Identity Groups:Profiled:Workstation	10-DD-B1-C9-3C-39	10-DD-B1-C9-3C-39	Ethernet	1

図 117.

検索文字列フィールドは次のとおりです。

```
eventtype=cisco-ise PostureStatus="NonCompliant" | fillnull value="No Location" Location | stats count by
Location UserName IdentityGroup EndPointMACAddress Calling_Station_ID NAS_Port_Type | `format_field_names`
```

不明ユーザの詳細（Unknown Users Details）



Unknown Users Details

Location	User Name	Identity Group	MAC Address	Calling Station ID	NAS Port Type	Count
Location#All Locations	10ddb1c93c39	Any	10-DD-B1-C9-3C-39	10-DD-B1-C9-3C-39	Ethernet	4
Location#All Locations	10ddb1c93c39	Endpoint Identity Groups:Profiled	10-DD-B1-C9-3C-39	10-DD-B1-C9-3C-39	Ethernet	1
Location#All Locations	10ddb1c93c39	Endpoint Identity Groups:RegisteredDevices	10-DD-B1-C9-3C-39	10-DD-B1-C9-3C-39	Ethernet	13
Location#All Locations	881fa10d47b2	Any	88-1F-A1-0D-47-B2	88-1f-a1-0d-47-b2	Wireless - IEEE 802.11	2
Location#All Locations	881fa10d47b2	Endpoint Identity Groups:Profiled	88-1F-A1-0D-47-B2	88-1f-a1-0d-47-b2	Wireless - IEEE 802.11	2
Location#All Locations	881fa10d47b2	Endpoint Identity Groups:Profiled:Workstation	88-1F-A1-0D-47-B2	88-1f-a1-0d-47-b2	Wireless - IEEE 802.11	2

図 118.

検索文字列フィールドは次のとおりです。

```
eventtype=cisco-ise PostureStatus="Unknown" | fillnull value="No Location" Location |          stats count by
Location UserName IdentityGroup EndPointMACAddress Calling Station ID NAS Port Type | `format field names`
```

無線ユーザのロケーション別の ISE コンプライアンスサマリー（ISE Compliance Summary By Location for Wireless Users）

Location#HYD

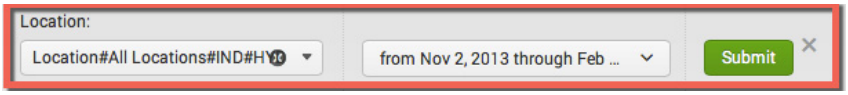


図 119.

コンプライアンスサマリー（Compliance Summary）

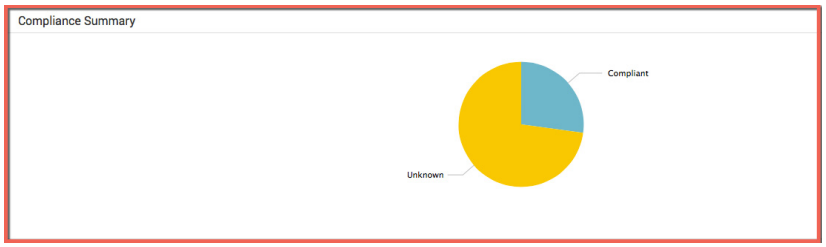
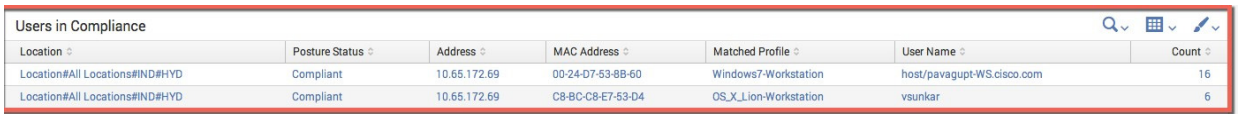


図 120.

検索文字列フィールド：

```
eventtype=cisco-ise Location="$location$" PostureStatus="*" NAS_Port_Type="Wireless - IEEE 802.11" | stats
count by PostureStatus | rename PostureStatus AS "Posture Status"
```

準拠しているユーザ（Users in Compliance）


Users in Compliance

Location	Posture Status	Address	MAC Address	Matched Profile	User Name	Count
Location#All Locations#IND#HYD	Compliant	10.65.172.69	00-24-D7-53-8B-60	Windows7-Workstation	host/pavagupt-WS.cisco.com	16
Location#All Locations#IND#HYD	Compliant	10.65.172.69	C8-BC-C8-E7-53-D4	OS_X_Lion-Workstation	vsunkar	6

図 121.

検索文字列フィールド：

```
eventtype=cisco-ise Location="$location$" PostureStatus="Compliant" NAS_Port_Type="Wireless - IEEE 802.11" |
stats count by Location PostureStatus Address EndPointMACAddress EndPointMatchedProfile UserName
|`format_field_names`
```

ポスチャステータス不明（Posture Status Unknown）

この「統計情報テーブル」には、ロケーション別の不明ユーザ ポスチャ ステータスの割合と数、および MAC アドレス、ユーザ名、およびデバイス（EndPointMatchedProfile に基づく）などのユーザのコンテキスト情報が表示されます。


Posture Status Unknown

Location	Posture Status	Address	MAC Address	Matched Profile	User Name	Count
Location#All Locations#IND#HYD	Unknown	10.65.172.69	00-24-D7-53-8B-60	Windows7-Workstation	host/pavagupt-WS.cisco.com	2
Location#All Locations#IND#HYD	Unknown	10.65.172.69	00-24-D7-C9-2C-A0	Windows7-Workstation	host/shabegum-WS.cisco.com	1
Location#All Locations#IND#HYD	Unknown	10.65.172.69	38-AA-3C-09-83-9F	Android-Samsung-Galaxy-Phone	ckharide	38
Location#All Locations#IND#HYD	Unknown	10.65.172.69	C8-BC-C8-E7-53-D4	OS_X_Lion-Workstation	vsunkar	1
Location#All Locations#IND#HYD	Unknown	10.65.172.69	E4-CE-8F-ED-B4-5C	Apple-Device	e4ce8fedb45c	17

図 122.

検索文字列フィールド:

```
eventtype=cisco-ise Location="$location$" PostureStatus="Unknown" NAS_Port_Type="Wireless - IEEE 802.11" |
stats count by Location PostureStatus Address EndPointMACAddress EndPointMatchedProfile UserName |
`format_field_names`
```

EPS(エンドポイント保護サービス)1.2 REST API

エンドポイント保護サービス(EPS)API

Cisco Identity Services Engine(ISE)は、Representational State Transfer(REST)API およびエンドポイント保護サービスの関連 API コールへのサポートを提供します。これらの REST API を使用することで、Splunk などのサードパーティ アプリケーションと ISE との統合が可能になり、これらのサードパーティが、セキュリティ イベントに反応してネットワーク上で ISE にユーザまたはデバイスの軽減を実行させることができます。これらの操作の例は、IP アドレス別にデバイスを隔離し、MAC アドレス別にデバイスを隔離解除することです。他の EPS 操作が可能です。このドキュメントでは特にこれらに焦点を当てます。EPS は通常、Splunk により警告された重大度の高いネットワーク セキュリティ イベントに基づいてユーザまたはデバイスで軽減措置を実行するために Splunk 管理者によって使用されます。

認証プロセスは、次のとおりです。

- Web サービスの URL は http://<mnt node>/ise/eps/… です。mnt ノードは ISE モニタリング ノードを表します。
- EPS REST API の実行には認証が必要です。ISE 管理者クレデンシャルを使用できます。
- ベーシック認証が使用されます。最初のコールの後、セッションは http から https に変換されます。
- 認証メカニズムは Cisco ISE 管理ユーザ インターフェイスへのアクセスに使用されるものと同様です。
- 認証はセッションごとに 1 回必要ですが、その後 JSessionID Cookie に保存されます。

EPS REST API は GET コールを利用します。

以下は、EPS REST API の隔離および隔離解除操作の形式です。

注:HTTP メソッドはすべて GET です。

- [MAC アドレス別隔離(Quarantine By MAC Address)]:エンドポイントの MAC アドレスを隔離します

```
https: //(MNT_node)/ise/eps/QuarantineByMAC/<mac_address>

where:

(MNT_node) is the IP address or FQDN of the ISE monitoring node

<mac_address> is MAC address of the endpoint
```

- [IP アドレス別隔離(Quarantine By IP Address)]:エンドポイントの IP アドレスを隔離します

```
https: //(MNT_node)/ise/eps/QuarantineByIP/<ip_address>

where:

(MNT_node) is the IP address or FQDN of the ISE monitoring node

<ip_address> is ip address of the endpoint
```

- [MAC アドレス別隔離解除(UnQuarantine By MAC Address)]:エンドポイントの MAC アドレスを隔離解除します

```
https: //(MNT_node)/ise/eps/UnQuarantineByMAC/<mac_address>
```

```
where:

(MNT_node) is the IP address or FQDN of the ISE node

<mac_address> is MAC address of the endpoint
```

- [IP アドレス別隔離解除(UnQuarantine By IpAddress)]:エンドポイントの IP アドレスを隔離解除します

```
https: //(MNT_node)/ise/eps/UnQuarantineByIP/<ip_address>

where:

(MNT_node) is the IP address or FQDN of the ISE node

<ip_address> is ip address of the endpoint
```

Splunk EPS ワークフローの基本操作

Splunk ワークフロー アクションによって、インデックス付きフィールドまたは抽出されたフィールドと他の Web リソース間のさまざまなインタラクションが可能になります。これらのワークフロー アクションによって、Splunk は ISE REST EPS API にアクセスするための URI リンクを使用して、IP アドレス別のデバイスの隔離や MAC アドレス別のデバイスの隔離解除などの EPS 操作を実行できます。

Splunk は、Framed_IP_Address、IpAddress、Calling_Station_ID、MACAddress フィールドに含まれている通りに、ISE から IP アドレスおよび MAC アドレスの syslog イベントを受信します。これらのフィールドは、ISE ロギング カテゴリに基づいています。

たとえば、ISE は [成功した認証(Passed Authentication)] カテゴリの Framed_IP_Address フィールドを送信します。これはエンドポイントの IP アドレスを表します。[ポスチャ(Posture)] や [クライアントプロビジョニング(Client Provisioning)] などの他の ISE カテゴリでは、IPAddress フィールドにエンドポイントの IP アドレスが含まれています。Calling_Station_ID および MACAddress についても同様です。これらのフィールドには、ISE カテゴリに基づいて、エンドポイントの MAC アドレスが含まれています。

Splunk でサードパーティ アプリケーションを使用する場合、EPS ワークフロー アクションを定義することができますが、エンドポイントの IP アドレスを変数として含め、エンドポイントは ISE で認証済みである必要があります。

これらの定義されたワークフロー アクションは、[イベント(Event)] および [アクション(Actions)] ドロップダウン メニューに表示され、関連フィールドが syslog イベントに存在する場合にのみ表示されます。これらのフィールドは、Framed_IP_Address、IpAddress、MacAddress、Calling_Station_ID です。

次の例では、ISE に対して認証しているエンドユーザは非準拠と見なされ、ポスチャ チェックが失敗します。Windows Defender サービスが停止しており、ポスチャ ポリシー ルールに違反しています。ISE は、Splunk に syslog イベントを送信します。Splunk 管理者はイベントを受信し、Splunk の [イベントアクション(Event Actions)] タブをクリックします。EPS_Quarantine_By_IpAddress が表示されます。Splunk 管理者はこのワークフロー アクションをクリックすることで、ISE への ISE EPS REST API リンクがトリガーされ、IP アドレス別にデバイスが隔離されます。

MAC アドレス別にデバイスを隔離解除するには、EPS_Unqurantine_BY_MACAddress が [Splunk イベント(Splunk Event)] ドロップダウンに表示されており、Splunk 管理者がこのワークフロー アクションをクリックすることで、ISE への ISE EPS REST API リンクがトリガーされ、MAC アドレス別にデバイスが隔離解除されます。

MAC アドレス別にデバイスを隔離解除するには、次の手順に従います。

ステップ 1 Splunk は ISE から syslog イベントを受信します。このイベントに基づいて、[ISE ポスチャ(ISE Posture)] および [クライアントプロビジョニング(Client provisioning)] カテゴリが有効になります。Splunk のワークフロー アクション **EPS_Quarantine_By_IpAddress _192.168.1.13**、**EPS_UnQuarantine_By_MACAddress_00-0C-29-77-A8-C7** はエンドポイントの IP アドレスと MAC アドレスを表します。

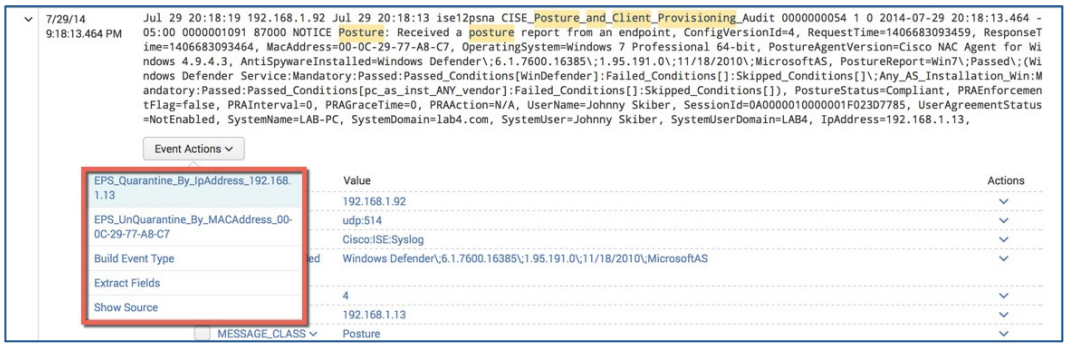
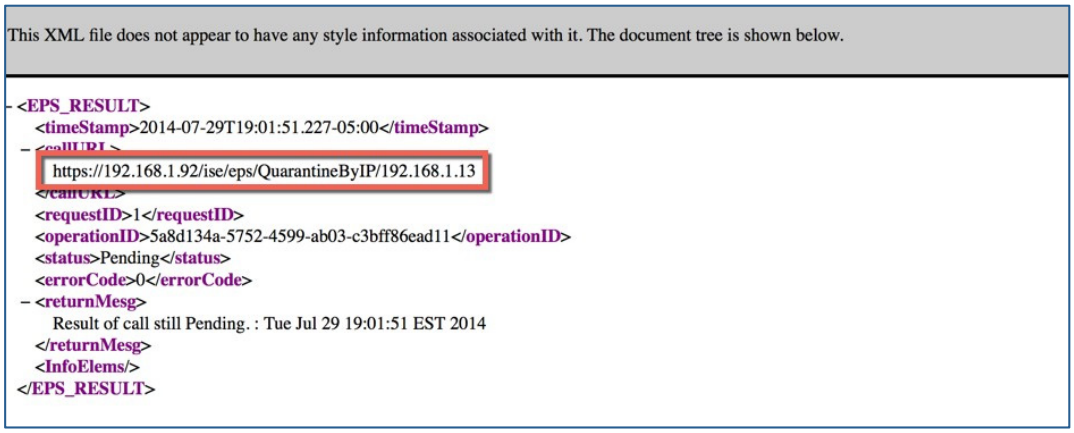


図 123.

ステップ 2 **EPS_Quarantine_By_IPAddress _192.168.1.13** ワークフロー アクションをクリックすると、ISE クレデンシャルの入力が求められます。

注:REST API を使用するには、サポート対象の Cisco ISE 管理ロール(Helpdesk Admin、Identity Admin、Monitoring Admin、Network Device Admin、Policy Admin、RBAC Admin、Super Admin、System Admin)のいずれかとしてログインする権限が必要です。

ステップ 3 認証されると、EPS REST API を含むコール URL が Splunk から ISE MnT ノードまたは ISE モニタリング ノードに送信されます。



ステップ 4 ISE の [操作認証(Operations Authentications)] ビューで、エンドポイントが隔離されていることを確認します。

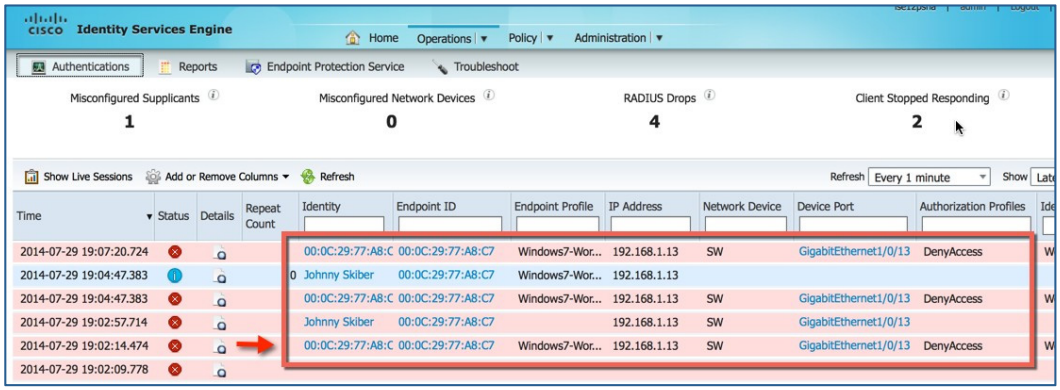


図 124.

ステップ 5 [詳細（Details）] ボタンをクリックすると、エンドポイントが承認ポリシー ルールに一致し、隔離されたことがわかります。

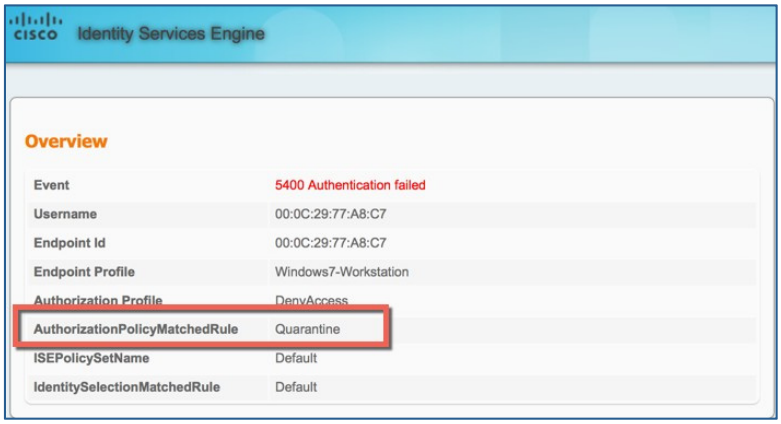


図 125.

ステップ 6 MAC アドレス別にデバイスを隔離解除するために、Splunk ワークフロー アクション **EPS_Unquarantine_BY_MacAddress-00-0C-29-77-A8-C7** をクリックすると、EPS 隔離解除 REST API が ISE MnT ノードに送信されます。

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
- <EPS_RESULT>
    <timeStamp>2014-07-29T19:44:55.403-05:00</timeStamp>
  - <callURL>
      https://192.168.1.92/ise/eps/UnQuarantineByMAC/00-0C-29-77-A8-C7
    </callURL>
    <requestID>2</requestID>
    <operationID>epsi--2932229668</operationID>
    <status>Success</status>
    <errorCode>0</errorCode>
  - <returnMesg>
      Request was Successful. : Tue Jul 29 19:44:55 EST 2014
    </returnMesg>
  - <InfoElems>
      <infoElem>0 : No Session found, but Unquarantine Permitted.</infoElem>
    </InfoElems>
</EPS_RESULT>
```


ステップ 7 ISE の [操作認証（Operations Authentications）] ビューで、エンドポイントにフル アクセスがあることを確認します。

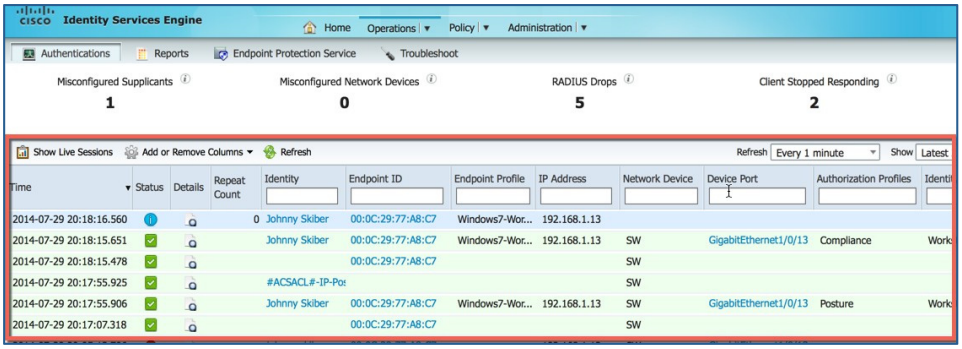


図 126.

ステップ 8 [詳細（Details）] ボタンをクリックすると、エンドポイントが承認プロファイルに一致したルール（デフォルトではネットワーク アクセスを許可するもの）に一致したことがわかります。

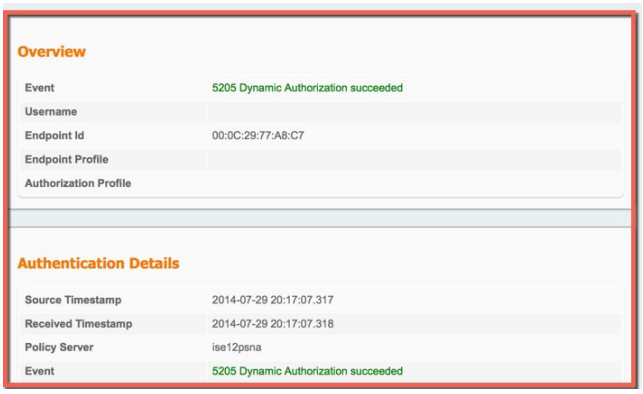


図 127.

EPS ワークフロー アクションの作成

次の EPS ワークフロー アクションは、Splunk で定義および作成され、個別にカバーされます。

- Framed_IP_Adddress 別 EPS 隔離
- Ip アドレス別 EPS 隔離
- MAC アドレス別 EPS 隔離
- MAC アドレス別 EPS 隔離解除
- IP アドレス別 EPS 隔離解除

Splunk Enterprise でワークフロー アクションを作成するには、次の手順を実行します。

ステップ 1 **[ナレッジ（Knowledge）] -> [フィールド（Fields）] -> [ワークフローアクション（WorkflowActions）] -> [新規（New）]** を選択します。

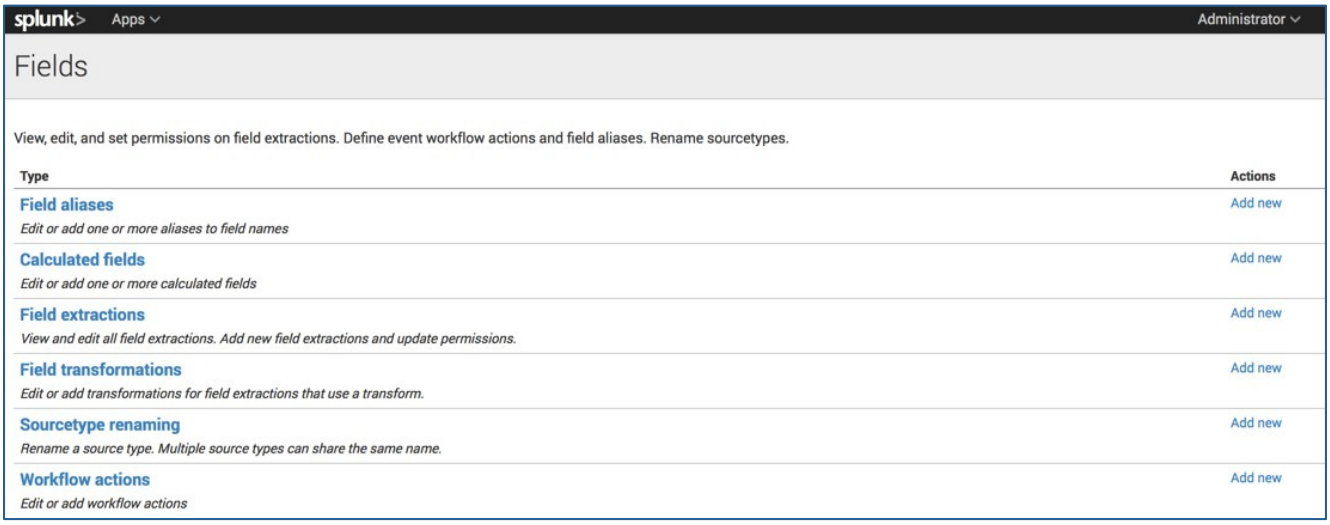


図 128.

ステップ 2 これらのワークフロー オブジェクトへの権限は [グローバル（global）] に設定する必要があり、これらのワークフロー アクションは、Splunk の ISE アドオン（インストールしている場合）に適用されます。

ステップ 3 目的のワークフロー アクションを選択し、[権限（Permissions）] をクリックします。

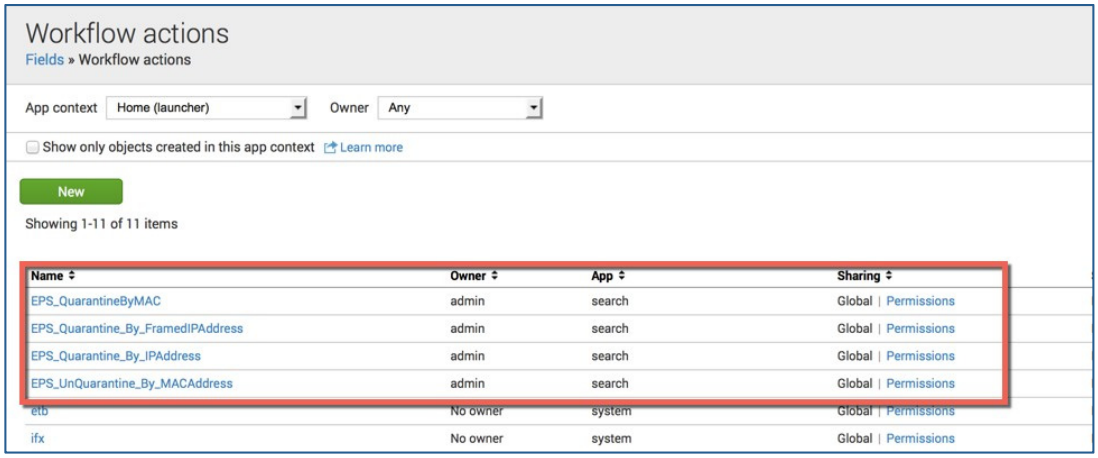


図 129.

ステップ 4 以下に EPS_Quarantine_By__IP アドレス ワークフロー アクションの例を示します。[すべてのアプリケーション（All apps）] を選択し、[保存（Save）] を選択します。

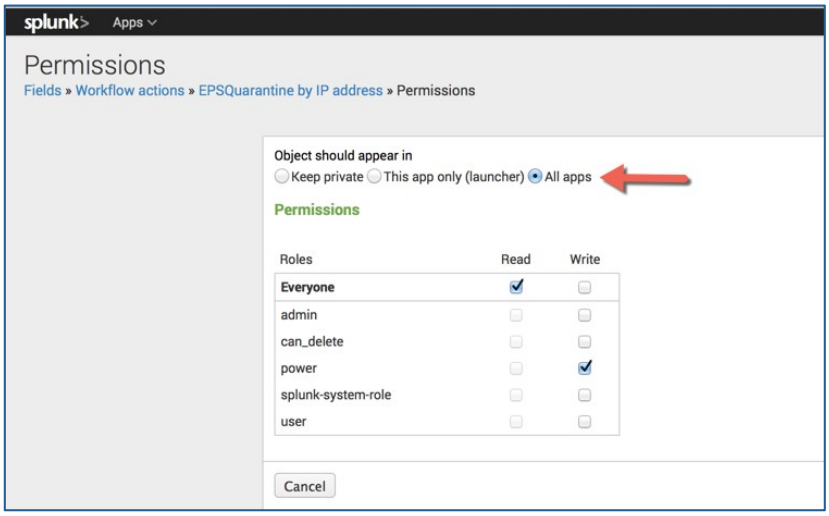


図 130.

注：これらはグローバル権限が与えられた場合のデフォルト設定です。

EPS_Quarantine_By_Framed_IP_Address

Framed_IP_Address フィールドには、次の ISE ロギング カテゴリから Splunk によって受信されたエンドポイントの IP アドレスが含まれています。

- 成功した認証（Passed Authentications）
- 失敗した試行（Failed Attempts）
- RADIUS アカウンティング（RADIUS Accounting）
- RADIUS 診断（RADIUS Diagnostics）
- プロファイラ（Profiler）

デバイス IP を隔離するときは、アクティブなユーザ セッションが存在する必要があるか、またはユーザが ISE に認証されていることに注意してください。

このワークフロー アクションの内容は次のとおりです。

Label: EPSQuarantine_By_FramedIpAddress_$Framed_IP_Address$

where:

Label defines the Workflow name. The $Framed_IP_Address$ variable contains the IP address in the Framed_IP_Address field

Apply only to the following fields: Framed_IP_Address

where:

Apply only to the following fields applies the worklow action to only exist when the Framed_IP_Address field is present

Show Action in Both: Both

where:

Show Action in Both defines where the workflow actions should appear.
Both: appear in both the Event and Action DropDown Menus.
Event: appears only in the Event DropDown menu.
Action: appears only in the Action DropDown menu.

Action Type: link

where:

Action Type either defines a link to the Web resource or search strings

URI: https://192.168.1.92/ise/eps/QuarantineByIP/$Framed_IP_Address$

where:

URI defines the REST API call, notice the $Framed_IP_Address$, this will contain the actual IP address contained in the Framed_IP_Address field.

Open Link In: New Window

where:

Open Link In defines if the Workflow action is opened up in the current window or in a new window.

Link Method: Get

where:

Link Method defines either the HTTP Get or HTTP Post method

以下は、EPS_Quarantine_By_FramedIPAddress の設定済みワークフロー アクションです。

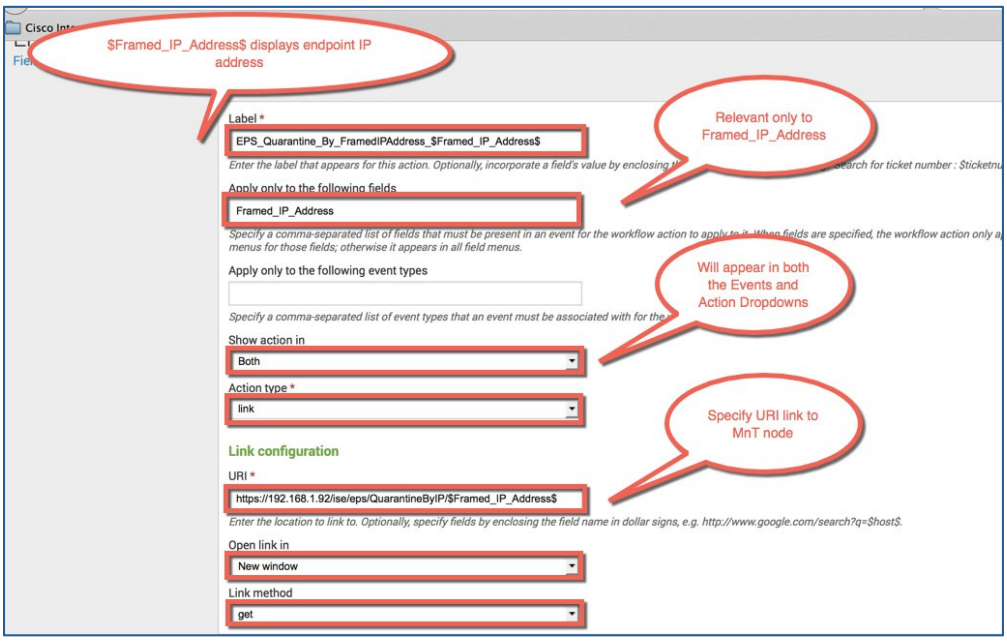


図 131.

EPS_QuarantineByIPAddress

[IP アドレス(IP Address)] フィールドには、次の ISE ロギング カテゴリから Splunk によって受信されたエンドポイントの IP アドレスが含まれています。

- ポスチャおよびクライアントプロビジョニング(Posture and Client Provisioning)
- 成功した認証(Passed Authentications)
- 失敗した試行(Failed Attempts)
- ゲスト(Guest)

ワークフロー アクションの作成時:

Label: EPSQuarantine_By_IpAddress_$IpAddress$

where:

Label defines the Workflow name, $IpAddress$ contains the IP address in the Framed_IP_Address field

Apply only to the following fields: IpAddress

where:

Apply only to the following fields applies the worklow action to only exist only when the IpAddress field is present

Show Action in Both: Both

where:

Show Action in Both defines where the workflow actions should appear.
Both: appear in both the Event and Action DropDown Menus.
Event: appears only in the Event DropDown menu.
Action: appears only in the Action DropDown menu.

Action Type: link

where:

Action Type either defines a link to the Web resource or search strings

URI: https://192.168.1.92/ise/eps/QuarantineByIP/$IpAddress$

where:

URI defines the REST API call, notice the $Framed_IP_Address$, this will contain the actual IP address contained in the Framed_IP_Address field.

Open Link In: New Window

where:

Open Link In defines if the Workflow action is opened up in the current window or in a new window.

Link Method: Get

```
where:

Link Method defines either the HTTP Get or HTTP Post method
```

以下は、EPS_Quarantine_By_IPAddress の設定済みワークフロー アクションです。

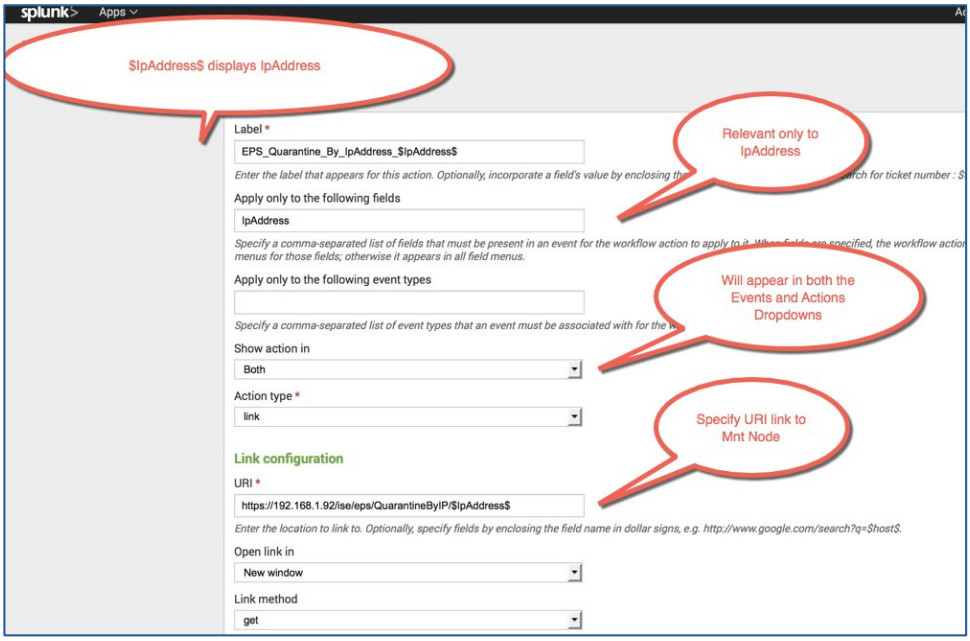


図 132.

EPS_QuarantineByMAC

Calling_Station_ID フィールドには、次の ISE ロギング カテゴリから Splunk によって受信されたエンドポイントの MAC アドレスが含まれています。

- RADIUS アカウンティング（RADIUS Accounting）
- 成功した認証（Passed Authentications）
- 失敗した試行（Failed Attempts）
- RADIUS 診断（RADIUS Diagnostics）
- プロファイラ（Profiler）

ワークフロー アクションの作成時：

```
Label: EPSQuarantine_By_MACAddress_$Calling_Station_ID$
```

where:

Label defines the Workflow name, $IpAddress$ contains the IP address in the Framed_IP_Address field

Apply only to the following fields: Calling_Station_ID

where:

Apply only to the following fields applies the worklow action to only exist only when the IpAddress field is present

Show Action in Both: Both

where:

Show Action in Both defines where the workflow actions should appear.
Both: appear in both the Event and Action DropDown Menus.
Event: appears only in the Event DropDown menu.
Action: appears only in the Action DropDown menu.

Action Type: link

where:

Action type either defines a link to the Web resource or search strings

URI: https://192.168.1.92/ise/eps/QuarantineByMAC/$Calling_Station_ID$

where:

URI defines the REST API call, notice the $Calling_Station_ID$, this will contain the actual MAC address contained in the Calling_Station_ID field.

Open Link In: New Window

where:

Open Link In defines if the Workflow action is opened up in the current window or in a new window.

```
Link Method: Get

where:

Link method defines either the HTTP Get or HTTP Post method
```

以下は、EPS_Quarantine_By_Calling_Station_ID の設定済みワークフロー アクションです。

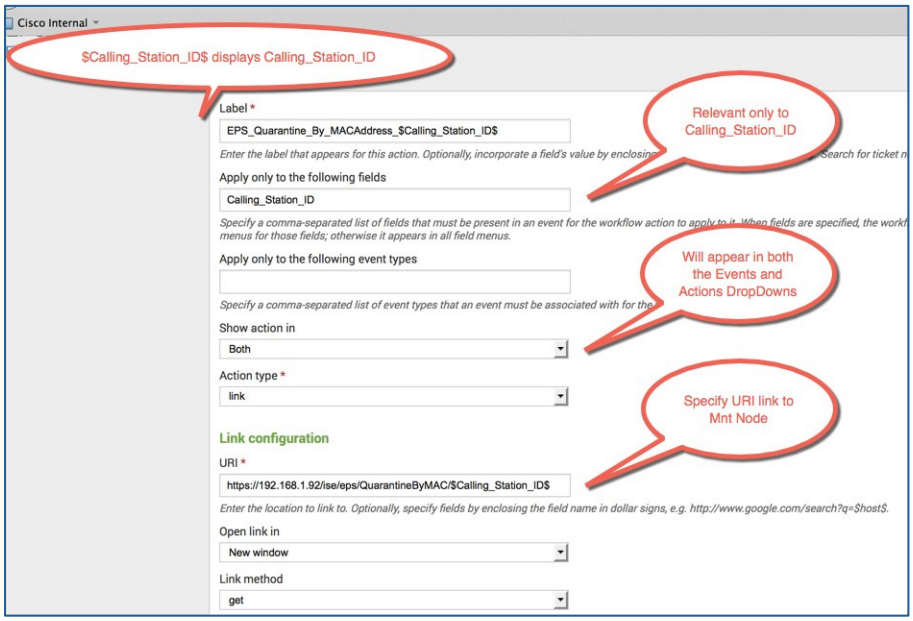


図 133.

EPS_UnquarantineByMAC

MacAddress フィールドには、次のロギング カテゴリから Splunk によって受信されたエンドポイントの MAC アドレスが含まれています。

- ポスチャおよびクライアントプロビジョニング（Posture and Client Provisioning）

- 管理および操作の監査（Administrative and Operational Audit）
- 成功した認証（Passed Authentications）
- 失敗した試行（Failed Attempts）
- ゲスト（Guest）
- プロファイラ（Profiler）

ワークフロー アクションの作成時：

```
Label: EPS_UnQuarantine_By_MACAddress_$MACAddress$

where:

Label defines the Workflow name, $IpAddress$ contains the IP address in the Framed_IP_Address field
```

```
Apply only to the following fields: MACAddress

where:

Apply only to the following fields applies the worklow action to only exist only when the IpAddress field
is present
```

```
Show Action in Both: Both

where:

Show Action in Both defines where the workflow actions should appear.
                      Both: appear in both the Event and Action DropDown Menus.
                      Event: appears only in the Event DropDown menu.
                      Action: appears only in the Action DropDown menu.
```

```
Action Type: link

where:

Action type either defines a link to the Web resource or search strings
```

```
https://192.168.1.92/ise/eps/UnQuarantineByMAC/$MACAddress$

where:
```

URI defines the REST API call, notice the $MACAddress$, this will contain the actual MAC address contained in the Calling_Station_ID field.

Open Link In: New Window

where:

Open Link In defines if the Workflow action is opened up in the current window or in a new window.

Link Method: Get

where:

Link method defines either the HTTP Get or HTTP Post method

以下は、EPS_Quarantine_By_MACAddress の設定済みワークフロー アクションです。

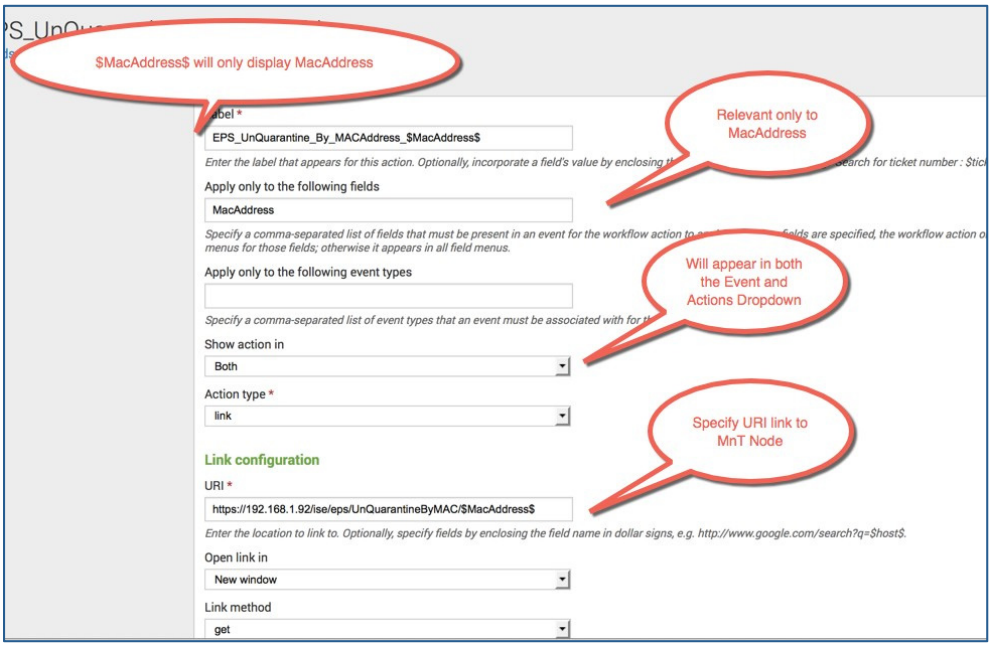


図 134.

ISE EPS 設定

このセクションでは、以下を ISE で設定する必要があります。

- REST API の有効化
- エンドポイント保護サービスの有効化
- 隔離承認プロファイルの作成
- 隔離用承認ポリシーの作成

REST API の有効化

REST API を有効にするには、次の手順を実行します。

ステップ 1 ISE VM コマンド ラインから、次のコマンドを実行します。

```
application configure ise
```

ステップ 2 以下が表示されます。

```
[1]Reset Active Directory settings to defaults
[2]Display Active Directory settings
[3]Configure Active Directory settings
[4]Restart/Apply Active Directory settings
[5]Clear Active Directory Trusts Cache and restart/apply Active Directory settings
[6]Enable/Disable External RESTful Services API
[7]Reset M&T Session Database
[8]Rebuild M&T Unusable Indexes
[9]Purge M&T Operational Data
[10]Reset M&T Database
```

```
[11]Refresh M&T Database Statistics
[12]Display Profiler Statistics
[13]Exit
```

ステップ 3 「6」と入力して ENTER を押します。

以下が表示されます。

```
Current External RESTful Services State: disabled
By proceeding, External RESTful Services port 9060 will be opened and External RESTful Services
API will be enabled
Are you sure you want to proceed? y/n [n]:
Enter "y" and press Enter
```

ステップ 4 以下が表示されます。

```
     Enabling External RESTful Services port 9060...
     External RESTful Services API enabled
```

ステップ 5 [外部 RESTful サービス SDK（External RESTful Services SDK）] ページにアクセスできることを確認し、次のように入力します。

```
https://<ipaddress>:9060/ers/sdk
```

注：SDK にアクセスするには、常にポート番号を 9600 として追加します。

エンドポイント保護サービスの有効化

ISE のエンドポイント保護サービスを有効にするには、次の手順を実行します。

ステップ 1 [管理（Administration）] -> [システム（System）] -> [設定（Settings）] -> [エンドポイント保護サービスの有効化（Enable Endpoint Protection Service）] を選択します。

隔離承認プロファイルの作成

承認プロファイルを作成するには、次の手順を実行します。

まず、承認プロファイルは、承認ポリシーで使用される隔離用に作成されます。

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

ステップ 2 プロファイルに **Quarantine** と名前をつけます。

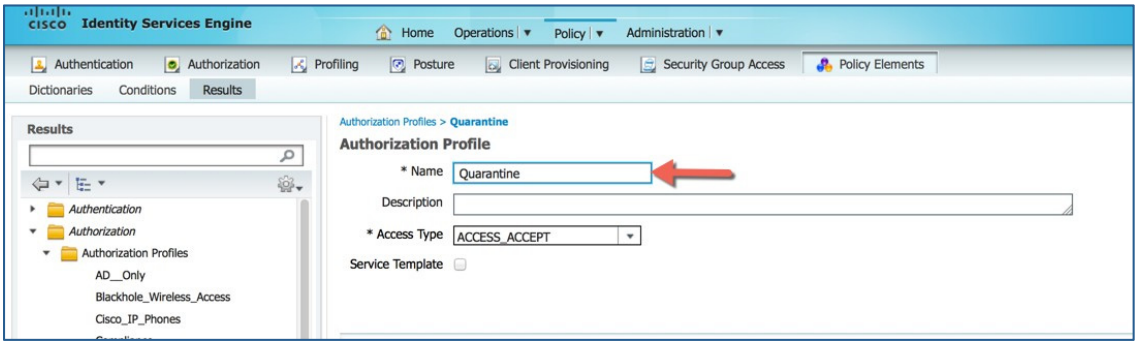


図 135.

ステップ 3 デフォルトのままにします。
ステップ 4 [送信(Submit)] を選択します。

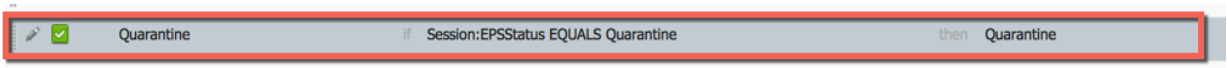
承認ポリシーを作成するには、次の手順を実行します。

ステップ 1 [ポリシー(Policy)] -> [承認ポリシー(Authorization Policy)] を選択します。
ステップ 2 [編集(Edit)] と [上に新規ルールを挿入(Insert New Rule Above)] をクリックします。

図 136.

ステップ 3 標準ルール 2 の名前を **Quarantine** に変更します。
ステップ 4 [属性の選択(Select Attribute)] の横にある + をクリックします。
ステップ 5 [新規条件の作成(Create New Condition)] をクリックします。
ステップ 6 [属性(Attribute)] -> [セッション:EPSTATUS は隔離に等しい(Session:EPSTATUS Equals Quarantine)] を選択します。
ステップ 7 [承認プロファイル(Authz Profile)] の横にある + をクリックします。
ステップ 8 ドロップダウンから、[標準(Standard)] -> [ポスチャプロファイル(Posture profile)] を選択します。

次のように表示されます。



ステップ 9 [保存(Save)] をクリックします。

ISE カテゴリの有効化

ここでは、ISE ロギング カテゴリを定義します。

ステップ 1 [管理(Administration)] -> [システム(System)] -> [ロギング(Logging)] -> [リモートロギングターゲット(Remote Logging Targets)] -> [追加(Add)] を選択します。
ステップ 2 リモート ログイン ターゲットとして Splunk を追加します。

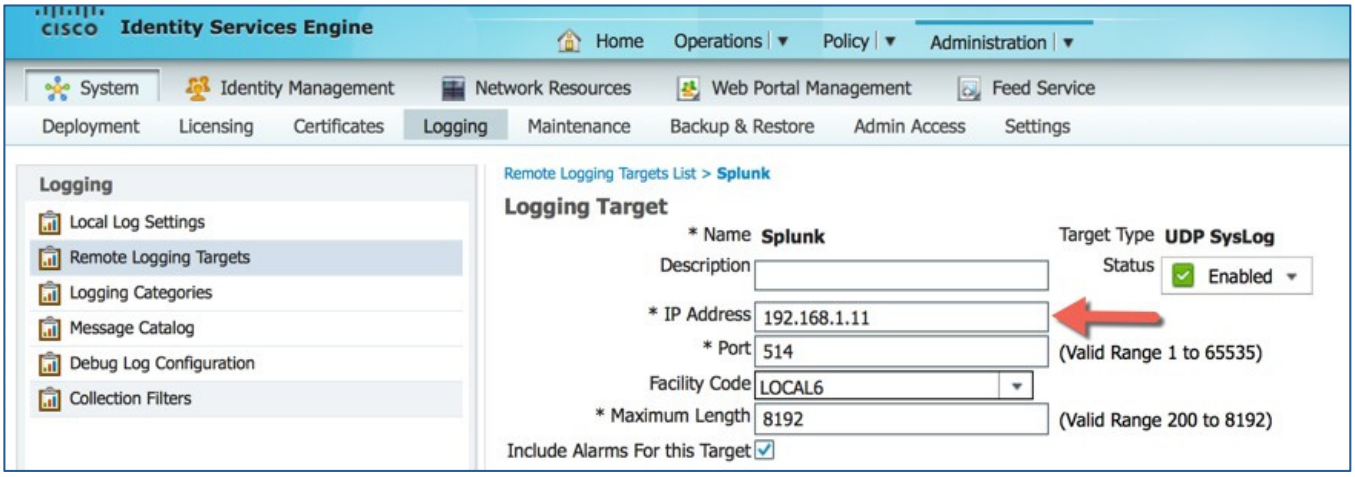


図 137.

注:最大長サイズは、1024 ～ 8192 に調整できます。

ステップ 3 目的の ISE ロギング カテゴリを選択します。

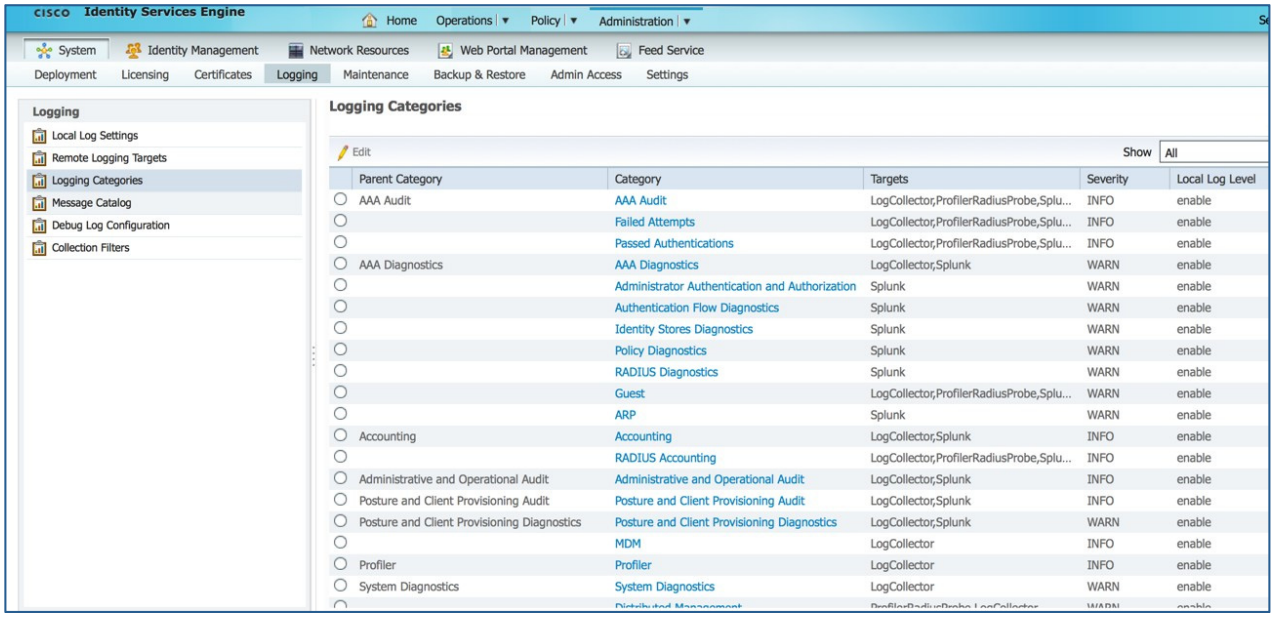


図 138.

注:カテゴリ選択は送信される syslog の量と Splunk のハードドライブの可用性に影響することに注意してください。

AAA 親カテゴリを選択し、目的のカテゴリに応じて追加できます。

EPS ポスチャの使用例

この EPS ポスチャは次の使用例を示します。

ユーザ Johnny Skiber は非準拠で、Antispyware Windows Defender サービスが実行されていません。EPS_Quarantine_By_IP ワークフロー アクションを使用して、デバイスが隔離されます。ユーザがサービスを有効にし、EPS_Unquarantine_By_MAC ワークフロー アクションが呼び出されます。ISE NAC エージェントがポスチャをチェックし、ユーザが準拠していると見なし、ネットワークへのフル アクセスが与えられます。

ステップ 1 NAC エージェントはユーザが非準拠と見なします。

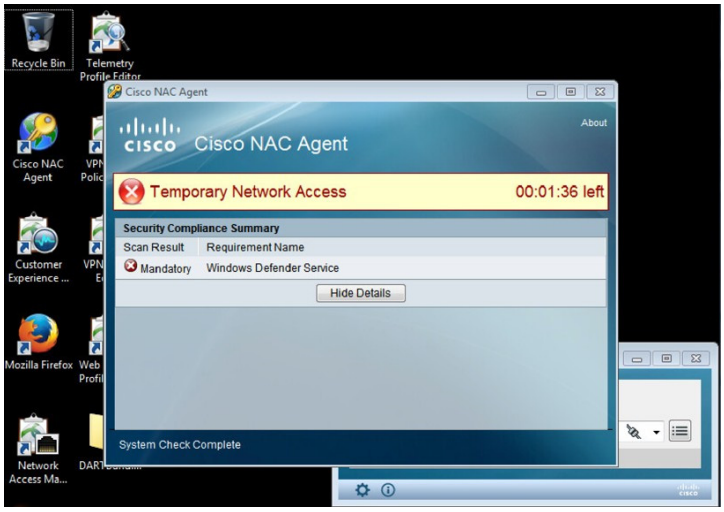


図 139.

ステップ 2 ISE の [操作認証（Operations Authentications）] ビューで、ユーザが非準拠になっています。

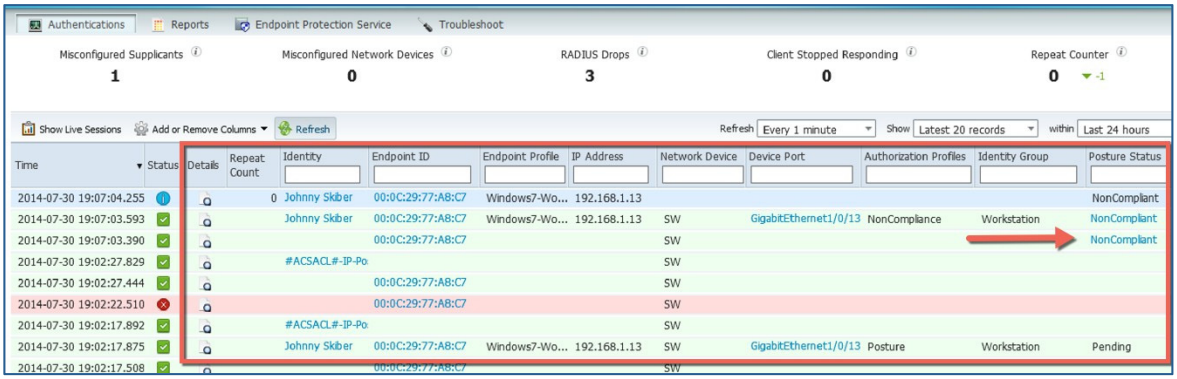


図 140.

ステップ 3 ISE ポスチャ スパイウェア対策（すべてのユーザ向け）ダッシュボードのアプリケーションで ISE アドオンの Splunk を確認します。

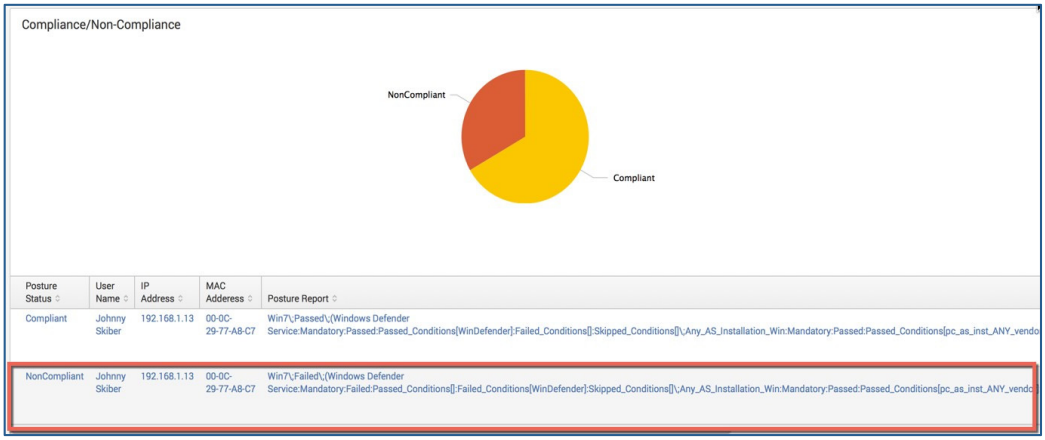


図 141.

エンドユーザが非準拠で、AS Windows Defender の必須チェックが失敗していることに注目してください。

ステップ 4 [NonCompliant] イベントをクリックします。これにより、syslog イベントに移動します。

ステップ 5 EPS_Quarantine_By_IpAddress_192.168.1.13 を選択します。

192.168.1.13 IpAddress がエンドポイントの IP アドレスであることに注意してください。

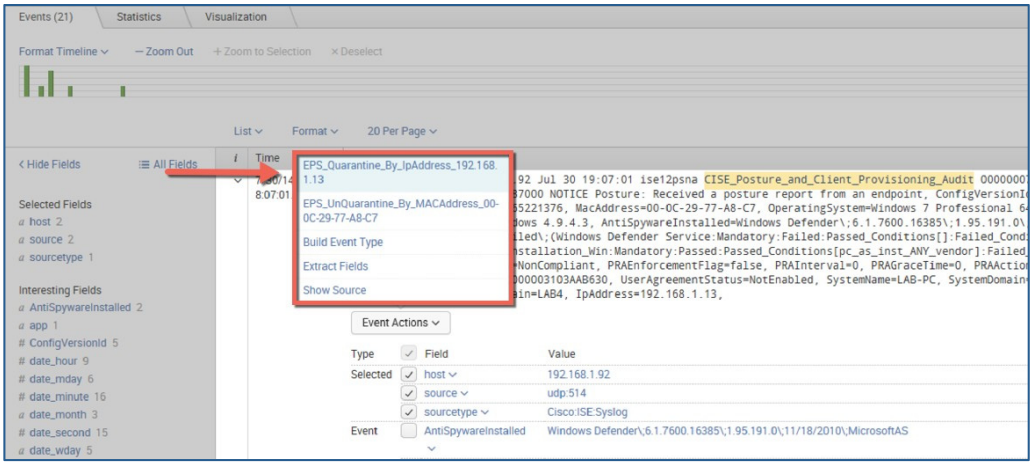


図 142.

ステップ 6 これにより URI REST EPS リンクが起動し、ISE 管理者クレデンシャルの入力が求められます。

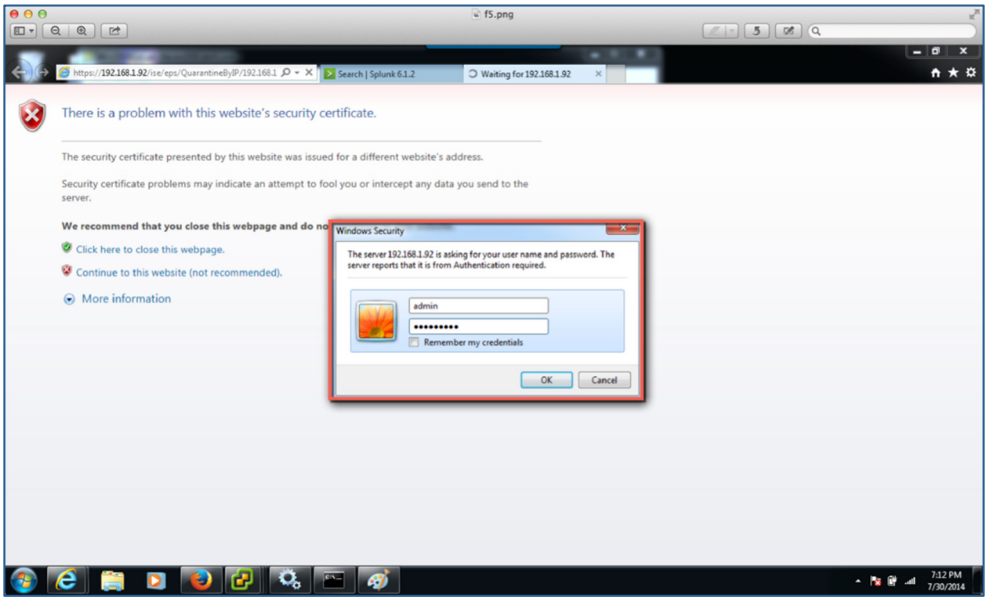


図 143.

REST API へのリンクが表示されます。

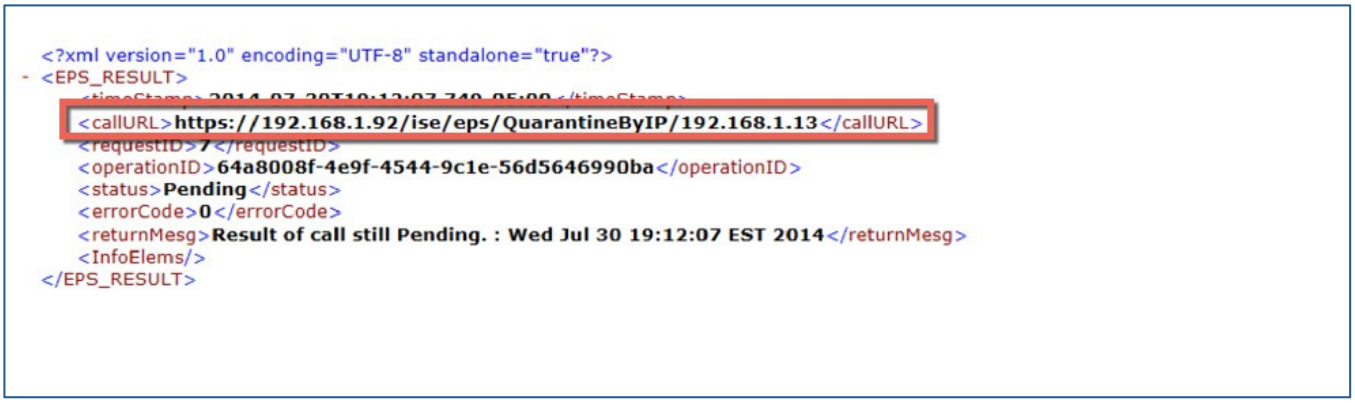


図 144.

[操作認証（Operations Authentications）] ビューでユーザが隔離されます。

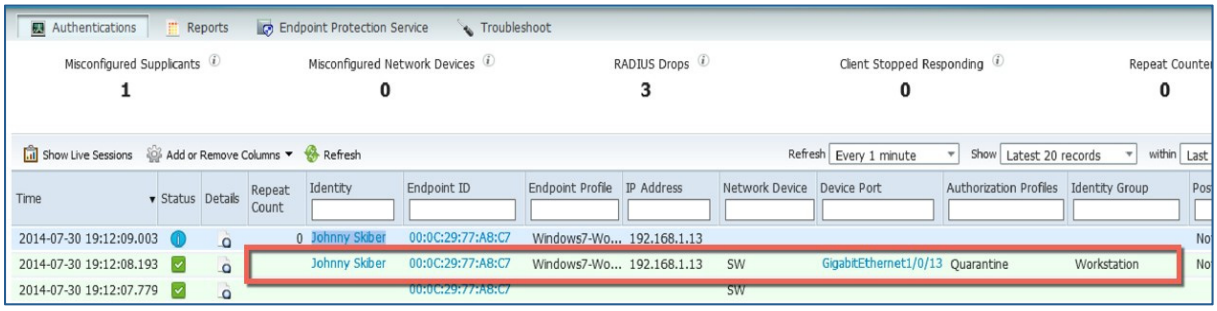


図 145.

ユーザは Windows Defender サービスを開始します。

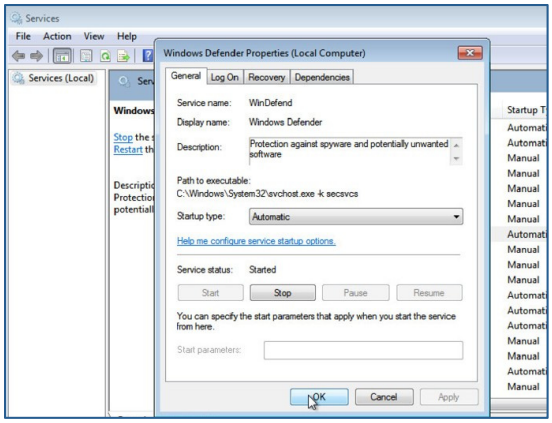


図 146.

ステップ 7 今度はイベントに戻り、**EPS_Unquarantine_By_MACAddress_00-0C-*29*-77-A8-C7** ワークフロー アクションを起動します。

これはエンドポイントの MAC アドレスであることに注意してください。

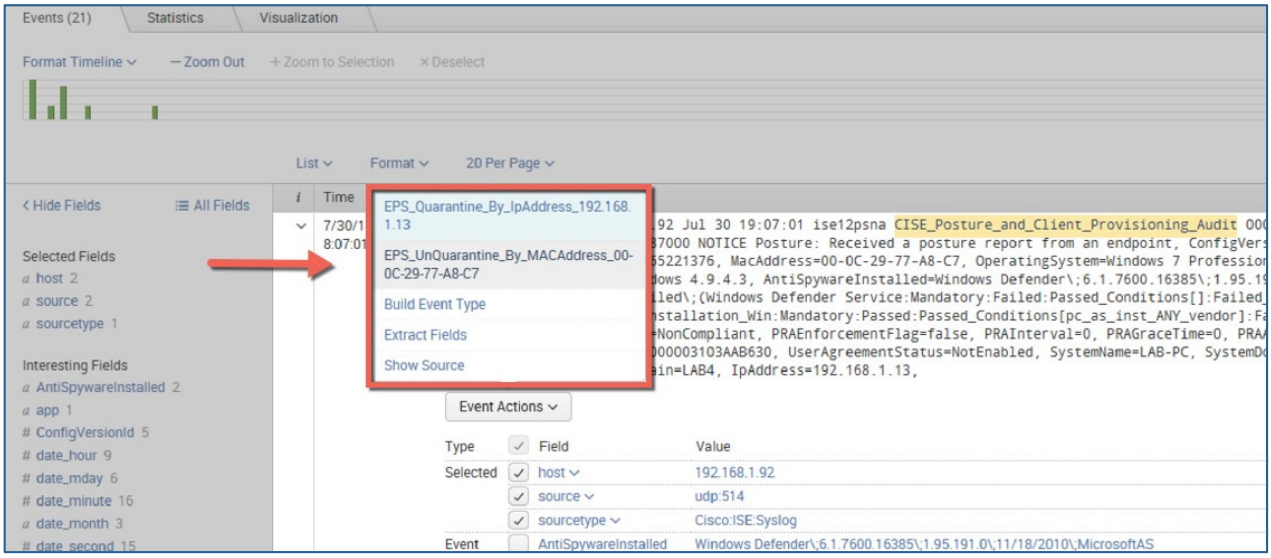


図 147.

ステップ 8 ISE モニタリング ノードを対象とした REST API リンクが表示されます。

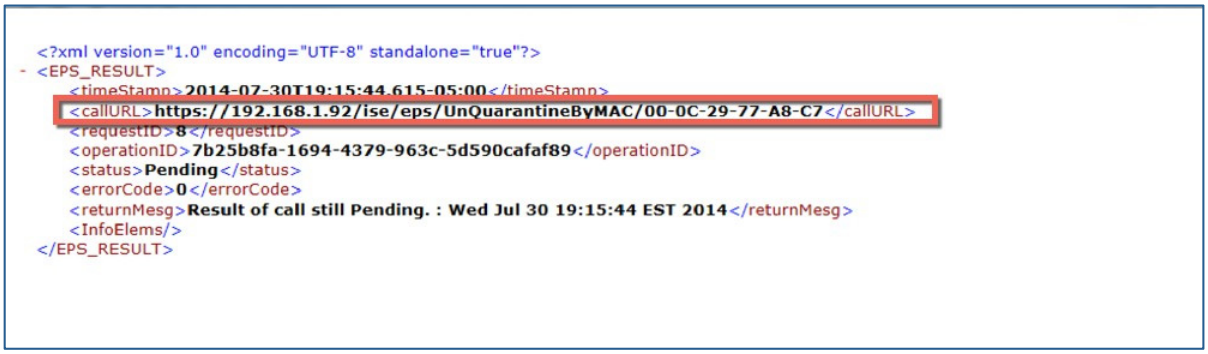


図 148.

[ISE 操作認証（ISE Operations Authentications）] ビューで、矢印はデバイスが隔離解除されたことを示します。

NAC エージェントがエンドポイントが準拠していると見なしていることに注意してください。

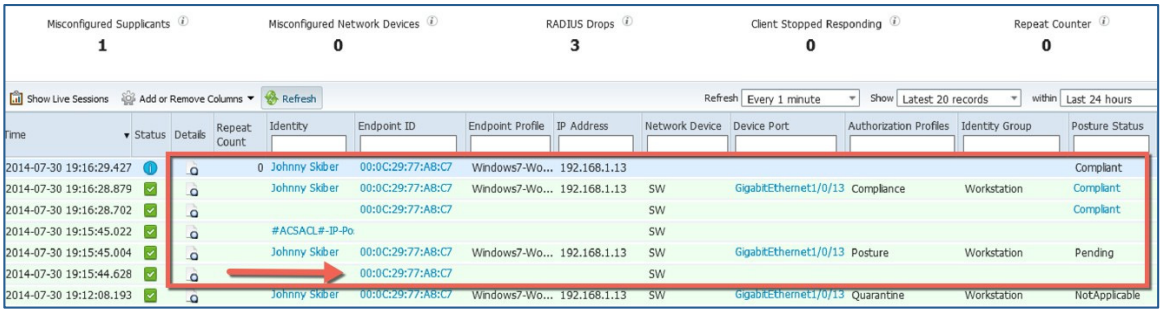


図 149.

AS ポスチャ ダッシュボードに準拠ユーザが表示されることに注意してください。

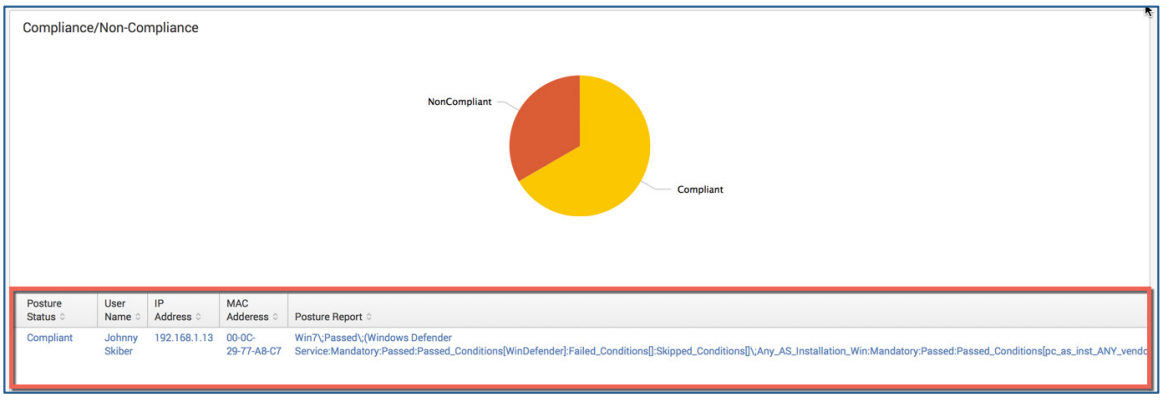


図 150.

また、AntiSpyware Windows Defender がインストールされていることにも注意してください。

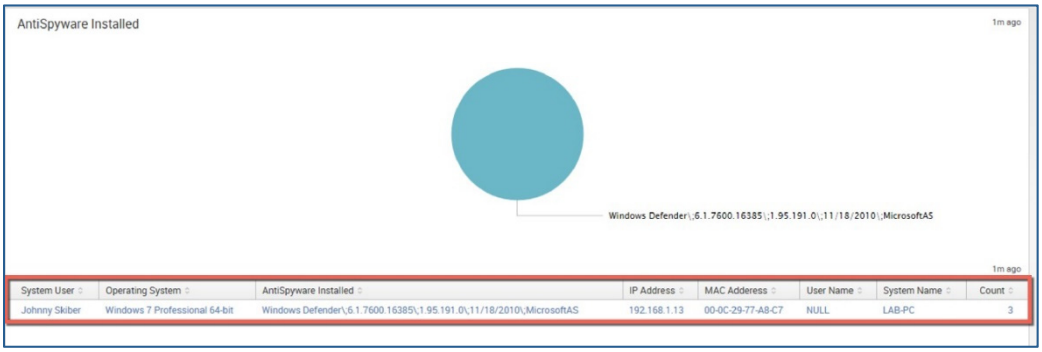

AntiSpyware Installed
1m ago
Windows Defender\,6.1.7600.16385\,1.95.191.0\,11/18/2010\,MicrosoftAS
1m ago
System User
Operating System
AntiSpyware Installed
IP Address
MAC Adderess
User Name
System Name
Count
Johnny Skiber
Windows 7 Professional 64-bit
Windows Defender\,6.1.7600.16385\,1.95.191.0\,11/18/2010\,MicrosoftAS
192.168.1.13
00-0C-29-77-A8-C7
NULL
LAB-PC
3

図 151.

EPS（エンドポイント保護サービス）1.3 REST API

エンドポイント保護サービス（EPS）1.3 REST API

Cisco Identity Services Engine（ISE）は、Representational State Transfer（REST）API およびエンドポイント保護サービスの関連 API コールへのサポートを提供します。これらの REST API を使用することで、Splunk などのサードパーティ アプリケーションと ISE との統合が可能になり、これらのサードパーティが、セキュリティ イベントに反応してネットワーク上で ISE にユーザまたはデバイスの軽減を実行させることができます。これらの操作の例は、IP アドレス別にデバイスを隔離し、MAC アドレス別にデバイスを隔離解除することです。他の EPS 操作が可能です。このドキュメントでは特にこれらに焦点を当てます。EPS は通常、Splunk により警告された重大度の高いネットワーク セキュリティ イベントに基づいてユーザまたはデバイスで軽減措置を実行するために Splunk 管理者によって使用されます。

注：ISE 1.3 パッチ 6 は同じ EPS 1.2 Rest API 構文を提供する必要があります。ISE 1.3 の構文の変更によって、ISE 1.2 Rest API コールに依存したアプリケーションでいくつかの問題が生じています。パッチ 6 は古い構文に戻ります。

認証プロセスは、次のとおりです。

- Web サービスの URL は http://<mnt node>/admin/API/eps/… です。mnt ノードは ISE モニタリング ノードを表します。
- EPS REST API の実行には認証が必要です。ISE 管理者クレデンシャルを使用できます。
- ベーシック認証が使用されます。最初のコールの後、セッションは http から https に変換されます。
- 認証メカニズムは Cisco ISE 管理ユーザ インターフェイスへのアクセスに使用されるものと同様です。
- 認証はセッションごとに 1 回必要ですが、その後 JSessionID Cookie に保存されます。

EPS REST API は GET コールを利用します。

以下は、EPS REST API の隔離および隔離解除操作の形式です。

注：HTTP メソッドはすべて GET です。

- [MAC アドレス別隔離（Quarantine By MAC Address）]：エンドポイントの MAC アドレスを隔離します。

```
https: //(MNT_node)/admin/API/eps/QuarantineByMAC/<mac_address>

where:

(MNT_node) is the IP address or FQDN of the ISE monitoring node

<mac_address> is MAC address of the endpoint
```

- [IP アドレス別隔離（Quarantine By IP Address）]：エンドポイントの IP アドレスを隔離します

```
https: //(MNT_node)/admin/API/eps/QuarantineByIP/<ip_address>

where:

(MNT_node) is the IP address or FQDN of the ISE monitoring node

<ip_address> is ip address of the endpoint
```

- [MAC アドレス別隔離解除（UnQuarantine By MAC Address）]：エンドポイントの MAC アドレスを隔離解除します

```
https: //(MNT_node)/admin/API/eps/UnQuarantineByMAC/<mac_address>

where:

(MNT_node) is the IP address or FQDN of the ISE node

<mac_address> is MAC address of the endpoint
```

- [IP アドレス別隔離解除(UnQuarantine By IpAddress)]:エンドポイントの IP アドレスを隔離解除します

```
https: //(MNT_node)/admin/API/eps/UnQuarantineByIP/<ip_address>

where:

(MNT_node) is the IP address or FQDN of the ISE node

<ip_address> is ip address of the endpoint
```

Splunk EPS ワークフローの基本操作

Splunk ワークフロー アクションによって、インデックス付きフィールドまたは抽出されたフィールドと他の Web リソース間のさまざまなインタラクションが可能になります。これらのワークフロー アクションによって、Splunk は ISE REST EPS API にアクセスするための URI リンクを使用して、IP アドレス別のデバイスの隔離や MAC アドレス別のデバイスの隔離解除などの EPS 操作を実行できます。

Splunk は、Framed_IP_Address、IpAddress、Calling_Station_ID、MACAddress フィールドに含まれている通りに、ISE から IP アドレスおよび MAC アドレスの syslog イベントを受信します。これらのフィールドは、ISE ロギング カテゴリに基づいています。

たとえば、ISE は [成功した認証(Passed Authentication)] カテゴリの Framed_IP_Address フィールドを送信します。これはエンドポイントの IP アドレスを表します。[ポスチャ(Posture)] や [クライアントプロビジョニング(Client Provisioning)] などの他の ISE カテゴリでは、IPAddress フィールドにエンドポイントの IP アドレスが含まれています。Calling_Station_ID および MACAddress についても同様です。これらのフィールドには、ISE カテゴリに基づいて、エンドポイントの MAC アドレスが含まれています。

Splunk でサードパーティ アプリケーションを使用する場合、EPS ワークフロー アクションを定義することができますが、エンドポイントの IP アドレスを変数として含め、エンドポイントは ISE で認証済みである必要があります。

これらの定義されたワークフロー アクションは、[イベント(Event)] および [アクション(Actions)] ドロップダウン メニューに表示され、関連フィールドが syslog イベントに存在する場合にのみ表示されます。これらのフィールドは、Framed_IP_Address、IpAddress、MacAddress、Calling_Station_ID です。

次の例では、ISE に対して認証しているエンドユーザは非準拠と見なされ、ポスチャ チェックが失敗します。Windows Defender サービスが停止しており、ポスチャ ポリシー ルールに違反しています。ISE は、Splunk に syslog イベントを送信します。Splunk 管理者はイベントを受信し、Splunk の [イベントアクション(Event Actions)] タブをクリックします。EPS_Quarantine_By_IpAddress が表示されます。Splunk 管理者はこのワークフロー アクションをクリックすることで、ISE への ISE EPS REST API リンクがトリガーされ、IP アドレス別にデバイスが隔離されます。

MAC アドレス別にデバイスを隔離解除するには、EPS_Unqurantine_BY_MACAddress が [Splunk イベント(Splunk Event)] ドロップダウンに表示されており、Splunk 管理者がこのワークフロー アクションをクリックすることで、ISE への ISE EPS REST API リンクがトリガーされ、MAC アドレス別にデバイスが隔離解除されます。

MAC アドレス別にデバイスを隔離解除するには、次の手順に従います。

ステップ 1 Splunk は ISE から syslog イベントを受信します。このイベントに基づいて、[ISE ポスチャ(ISE Posture)] および [クライアントプロビジョニング(Client provisioning)] カテゴリが有効になります。Splunk のワークフロー アクション **EPS_Quarantine_By_IpAddress _192.168.1.13**、**EPS_UnQuarantine_By_MACAddress_00-0C-*29*-77-A8-C7** はエンドポイントの IP アドレスと MAC アドレスを表します。

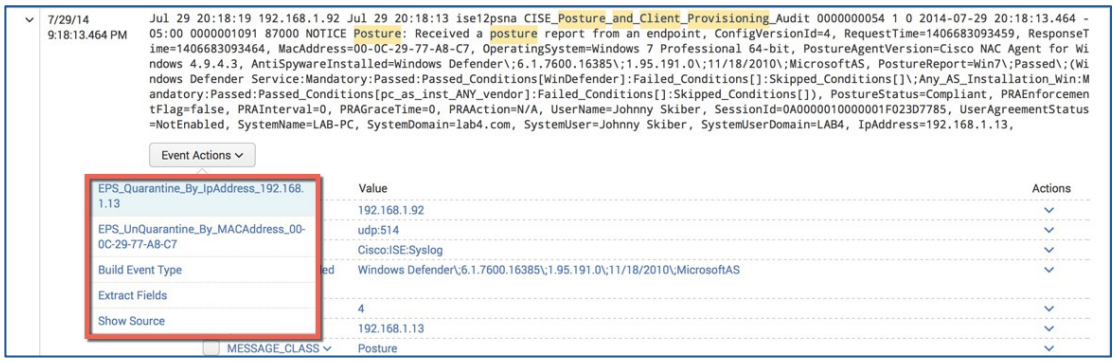


図 152.

EPS_Quarantine_By_IPAddress _192.168.1.13 ワークフロー アクションをクリックすると、ISE クレデンシャルの入力を求められます。

注:REST API を使用するには、サポート対象の Cisco ISE 管理ロール(Helpdesk Admin、Identity Admin、Monitoring Admin、Network Device Admin、Policy Admin、RBAC Admin、Super Admin、System Admin)のいずれかとしてログインする権限が必要です。

ステップ 2 認証されると、EPS REST API を含むコール URL が Splunk から ISE MnT ノードまたは ISE モニタリング ノードに送信されます。

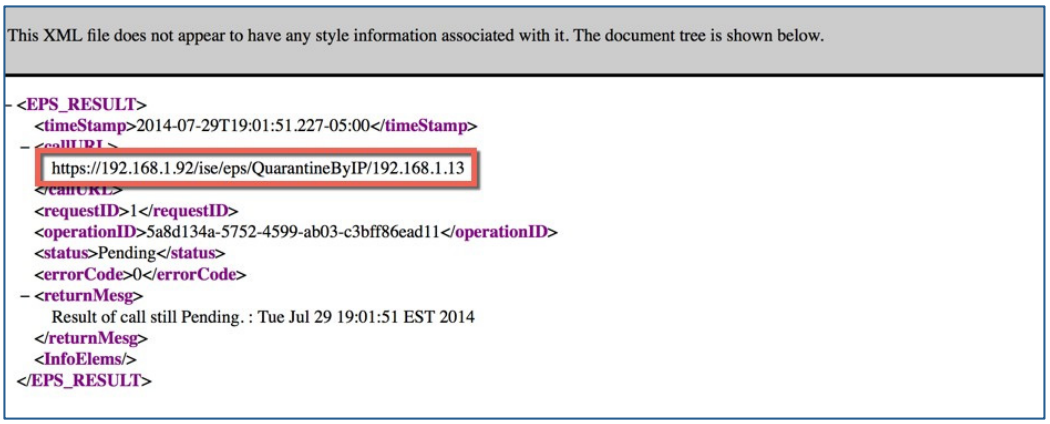


図 153.

ステップ 3 ISE の [操作認証（Operations Authentications）] ビューで、エンドポイントが隔離されていることを確認します。

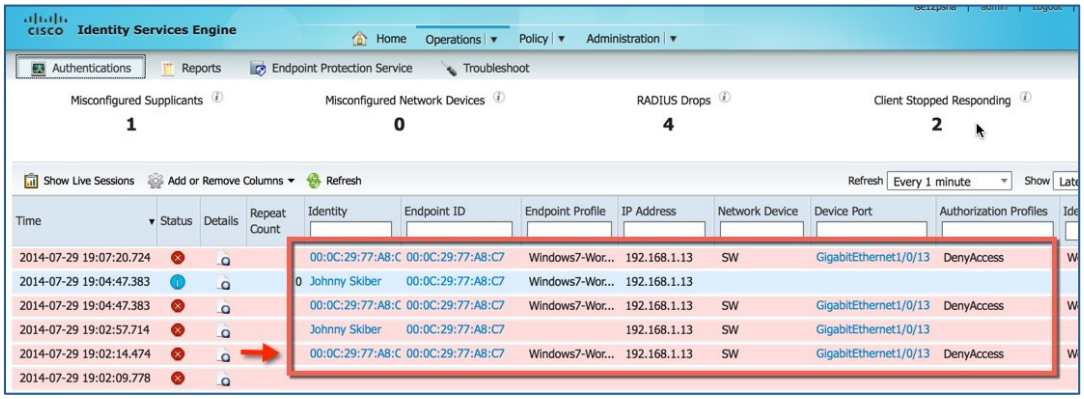


図 154.

ステップ 4 [詳細（Details）] ボタンをクリックします。 エンドポイントが承認ポリシー ルールに一致し、隔離されたことがわかります。

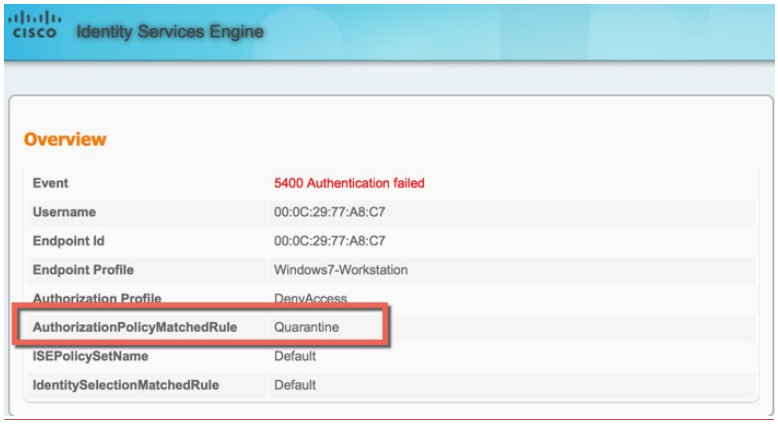


図 155.

ステップ 5 MAC アドレス別にデバイスを隔離解除するために、Splunk ワークフロー アクション **EPS_Unquarantine_BY_MacAddress-00-0C--77-77-A8-C7** をクリックすると、EPS 隔離解除 REST API が ISE MnT ノードに送信されます。

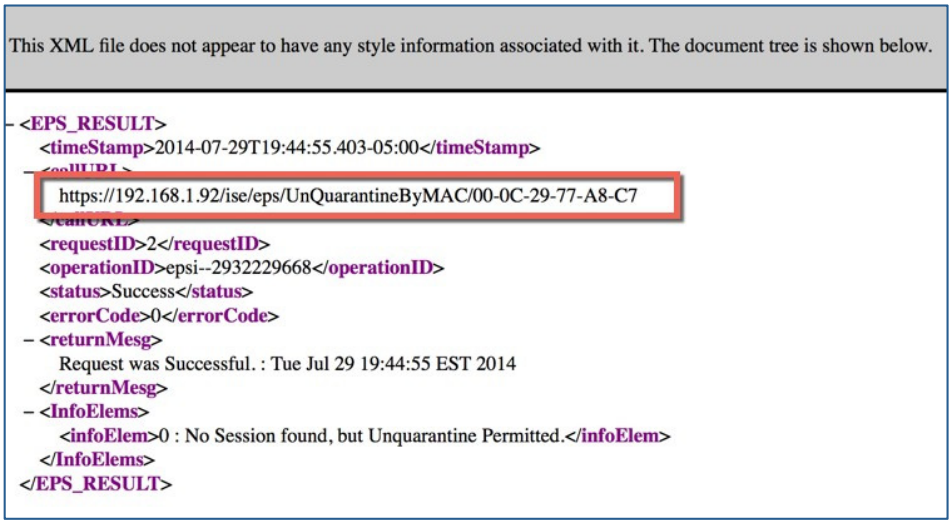


図 156.

手順 8：ISE の [操作認証（Operations Authentications）] ビューで、エンドポイントにフル アクセスがあることを確認します。

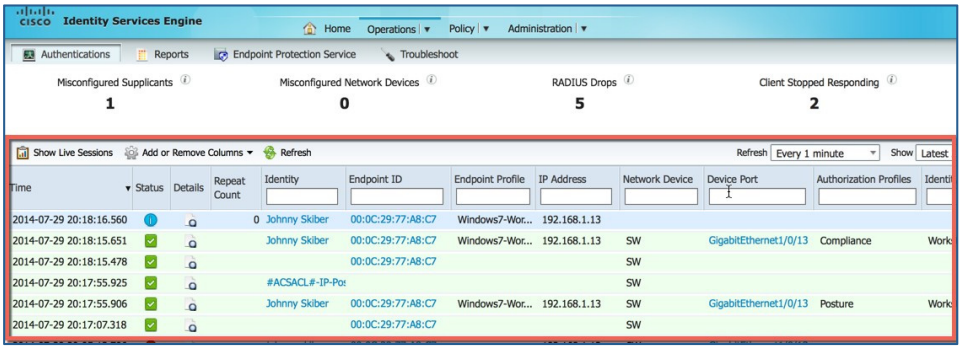


図 157.

ステップ 6 [詳細（Details）] ボタンをクリックすると、エンドポイントが承認プロファイルに一致したルール（デフォルトではネットワーク アクセスを許可するもの）に一致したことがわかります。

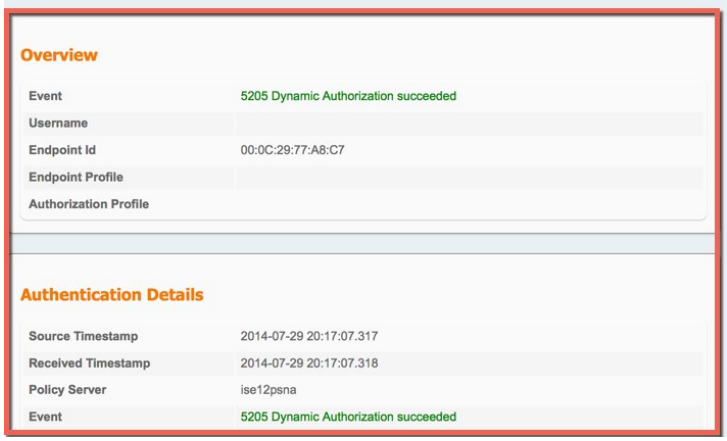


図 158.

EPS ワークフロー アクションの作成

次の EPS ワークフロー アクションは、Splunk で定義および作成され、個別にカバーされます。

- Framed_IP_Adddress 別 EPS 隔離
- Ip アドレス別 EPS 隔離
- MAC アドレス別 EPS 隔離
- MAC アドレス別 EPS 隔離解除
- IP アドレス別 EPS 隔離解除

Splunk Enterprise でワークフロー アクションを作成するには、次の手順を実行します。

ステップ 1 [ナレッジ（Knowledge）] -> [フィールド（Fields）] -> [ワークフローアクション（WorkflowActions）] -> [新規（New）] を選択します。

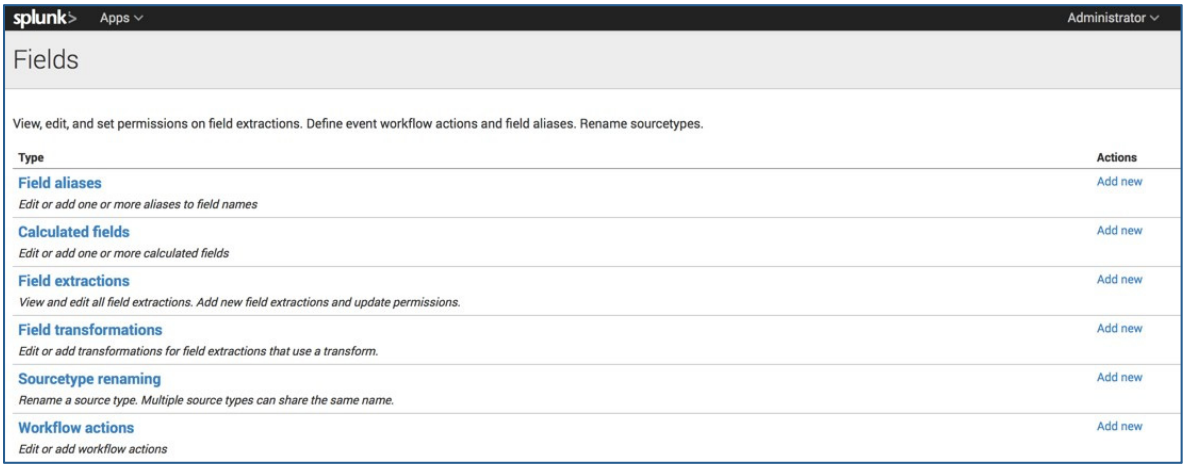


図 159.

これらのワークフロー オブジェクトへの権限は [グローバル（global）] に設定する必要があり、これらのワークフロー アクションは、Splunk の ISE アドオン（インストールしている場合）に適用されます。

ステップ 2 目的のワークフロー アクションを選択し、[権限（Permissions）] をクリックします。

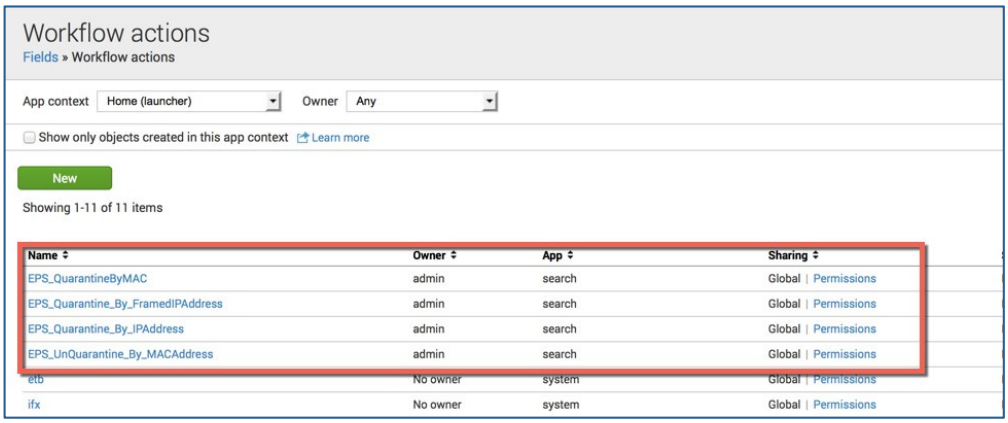


図 160.

ステップ 3 以下に EPS_Quarantine_By__IP アドレス ワークフロー アクションの例を示します。[すべてのアプリケーション（All apps）] を選択し、[保存（Save）] を選択します。

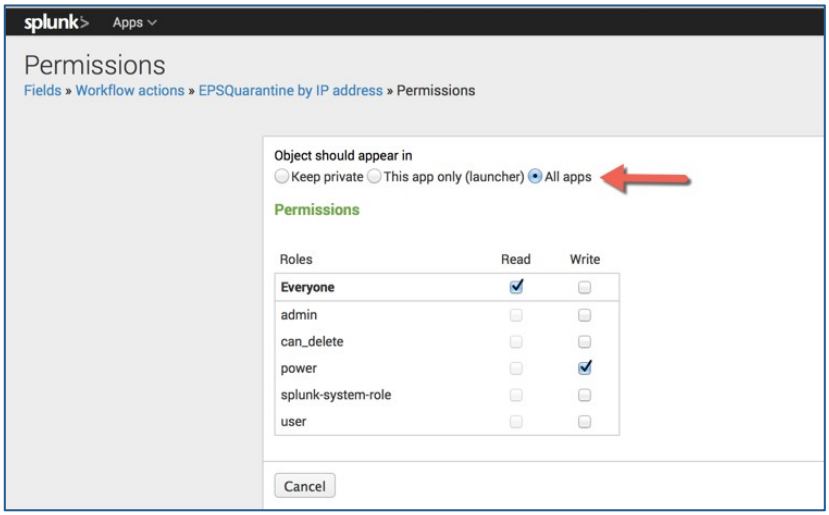


図 161.

注:これらはグローバル権限が与えられた場合のデフォルト設定です。

EPS_Quarantine_By_Framed_IP_Address

Framed_IP_Address フィールドには、次の ISE ロギング カテゴリから Splunk によって受信されたエンドポイントの IP アドレスが含まれています。

- 成功した認証(Passed Authentications)
- 失敗した試行(Failed Attempts)
- RADIUS アカウンティング(RADIUS Accounting)
- RADIUS 診断(RADIUS Diagnostics)
- プロファイラ(Profiler)

デバイス IP を隔離するときは、アクティブなユーザ セッションが存在する必要があるか、またはユーザが ISE に認証されていることに注意してください。

このワークフロー アクションの内容は次のとおりです。

```
Label: EPSQuarantine_By_FramedIpAddress_$Framed_IP_Address$

where:

Label defines the Workflow name. The $Framed_IP_Address$ variable contains the IP address in the
Framed_IP_Address field
```

```
Apply only to the following fields: Framed_IP_Address

where:

Apply only to the following fields applies the worklow action to only exist when the Framed_IP_Address
field is present
```

Show Action in Both: Both

where:

Show Action in Both defines where the workflow actions should appear.
Both: appear in both the Event and Action DropDown Menus.
Event: appears only in the Event DropDown menu.
Action: appears only in the Action DropDown menu.

Action Type: link

where:

Action Type either defines a link to the Web resource or search strings

URI: https://192.168.1.92/admin/API/eps/QuarantineByIP/$Framed_IP_Address$

where:

URI defines the REST API call, notice the $Framed_IP_Address$, this will contain the actual IP address contained in the Framed_IP_Address field.

Open Link In: New Window

where:

Open Link In defines if the Workflow action is opened up in the current window or in a new window.

Link Method: Get

where:

Link Method defines either the HTTP Get or HTTP Post method

以下は、EPS_Quarantine_By_FramedIPAddress の設定済みワークフロー アクションです。

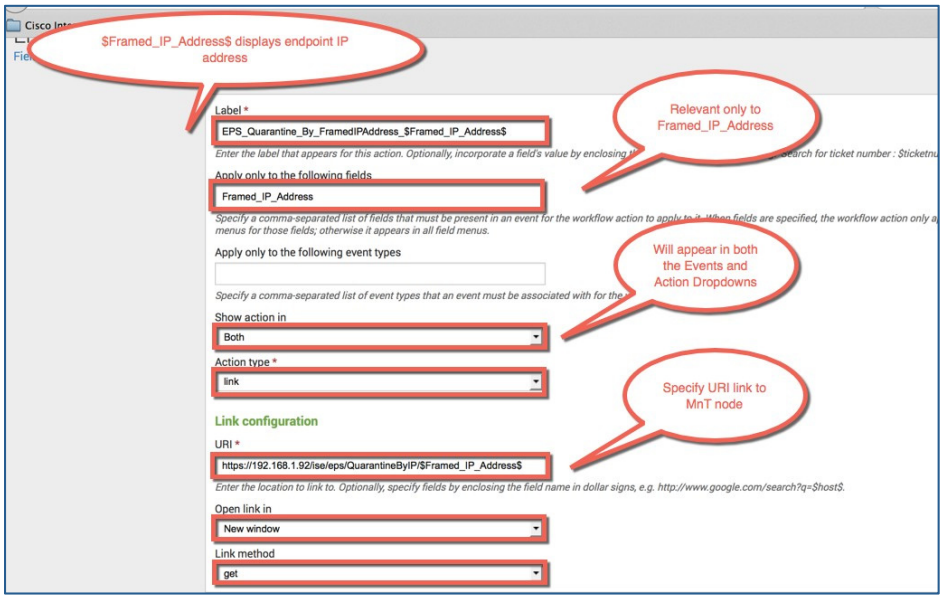


図 162.

EPS_QuarantineByIPAddress

[IP アドレス(IP Address)] フィールドには、次の ISE ロギング カテゴリから Splunk によって受信されたエンドポイントの IP アドレスが含まれています。

- ポスチャおよびクライアントプロビジョニング(Posture and Client Provisioning)
- 成功した認証(Passed Authentications)
- 失敗した試行(Failed Attempts)
- ゲスト(Guest)

ワークフロー アクションの作成時:

```
Label: EPSQuarantine_By_IpAddress_$IpAddress$

where:

Label defines the Workflow name, $IpAddress$ contains the IP address in the Framed_IP_Address field
```

```
Apply only to the following fields: IpAddress

where:

Apply only to the following fields applies the worklow action to only exist only when the IpAddress field
is present
Show Action in Both: Both
where:

Show Action in Both defines where the workflow actions should appear.
                      Both: appear in both the Event and Action DropDown Menus.
                      Event: appears only in the Event DropDown menu.
```

Action: appears only in the Action DropDown menu.

Action Type: link

where:

Action Type either defines a link to the Web resource or search strings

URI: https://192.168.1.92/admin/API/eps/QuarantineByIP/$IpAddress$

where:

URI defines the REST API call, notice the $Framed_IP_Address$, this will contain the actual IP address contained in the Framed_IP_Address field.

Open Link In: New Window

where:

Open Link In defines if the Workflow action is opened up in the current window or in a new window.

Link Method: Get

where:

Link Method defines either the HTTP Get or HTTP Post method

以下は、EPS_Quarantine_By_IPAddress の設定済みワークフロー アクションです。

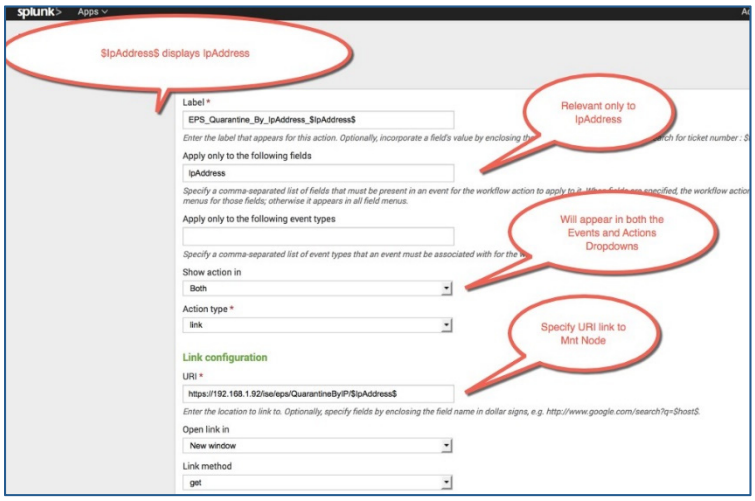


図 163.

EPS_QuarantineByMAC

Calling_Station_ID フィールドには、次の ISE ロギング カテゴリから Splunk によって受信されたエンドポイントの MAC アドレスが含まれています。

- RADIUS アカウンティング（RADIUS Accounting）
- 成功した認証（Passed Authentications）
- 失敗した試行（Failed Attempts）
- RADIUS 診断（RADIUS Diagnostics）
- プロファイラ（Profiler）

ワークフロー アクションの作成時：

```
Label: EPSQuarantine_By_MACAddress_$Calling_Station_ID$

where:

Label defines the Workflow name, $IpAddress$ contains the IP address in the Framed_IP_Address field
```

```
Apply only to the following fields: Calling_Station_ID

where:

Apply only to the following fields applies the worklow action to only exist only when the IpAddress field
is present
```

```
Show Action in Both: Both

where:
```

```
Show Action in Both defines where the workflow actions should appear.
                      Both: appear in both the Event and Action DropDown Menus.
                      Event: appears only in the Event DropDown menu.
                      Action: appears only in the Action DropDown menu.
Action Type: link

where:

Action type either defines a link to the Web resource or search strings
```

```
URI: https://192.168.1.92/admin/API/eps/QuarantineByMAC/$Calling_Station_ID$

where:

URI defines the REST API call, notice the $Calling_Station_ID$, this will contain the actual MAC address
contained in the Calling_Station_ID field.
```

```
Open Link In: New Window

where:

Open Link In defines if the Workflow action is opened up in the current window or in a new window.
```

```
Link Method: Get

where:

Link method defines either the HTTP Get or HTTP Post method
```

以下は、EPS_Quarantine_By_Calling_Station_ID の設定済みワークフロー アクションです。

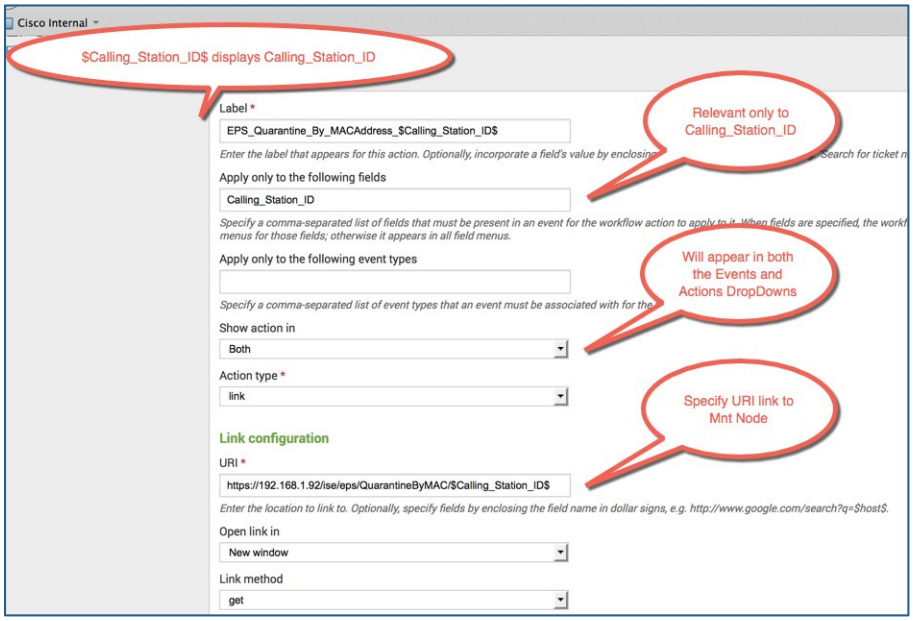


図 164.

EPS_UnquarantineByMAC

MacAddress フィールドには、次のロギング カテゴリから Splunk によって受信されたエンドポイントの MAC アドレスが含まれています。

- ポスチャおよびクライアントプロビジョニング（Posture and Client Provisioning）
- 管理および操作の監査（Administrative and Operational Audit）
- 成功した認証（Passed Authentications）
- 失敗した試行（Failed Attempts）
- ゲスト（Guest）
- プロファイラ（Profiler）

ワークフロー アクションの作成時：

```
Label: EPS_UnQuarantine_By_MACAddress_$MacAddress$

where:

Label defines the Workflow name, $IpAddress$ contains the IP address in the Framed_IP_Address field
```

```
Apply only to the following fields: MacAddress

where:

Apply only to the following fields applies the worklow action to only exist only when the IpAddress field
is present
```

Show Action in Both: Both

where:

Show Action in Both defines where the workflow actions should appear.
Both: appear in both the Event and Action DropDown Menus.
Event: appears only in the Event DropDown menu.
Action: appears only in the Action DropDown menu.

Action Type: link

where:

Action type either defines a link to the Web resource or search strings

https://192.168.1.92/admin/API/eps/UnQuarantineByMAC/$MacAddress$

where:

URI defines the REST API call, notice the $MACAddress$, this will contain the actual MAC address contained in the Calling_Station_ID field.

Open Link In: New Window

where:

Open Link In defines if the Workflow action is opened up in the current window or in a new window.

Link Method: Get

where:

Link method defines either the HTTP Get or HTTP Post method

以下は、EPS_Quarantine_By_MACAddress の設定済みワークフロー アクションです。

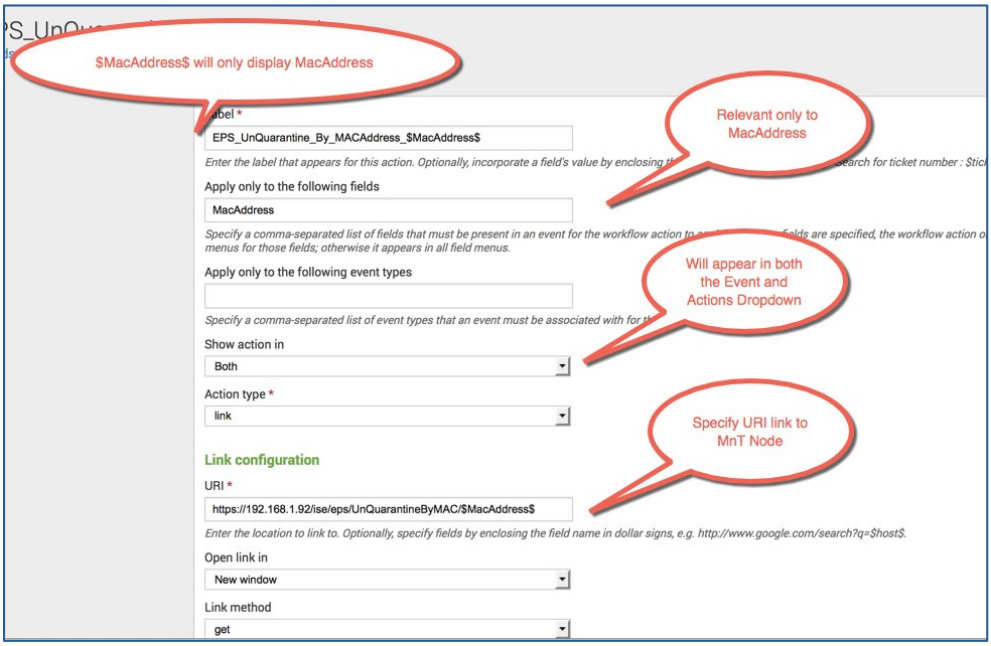


図 165.

ISE EPS 設定

このセクションでは、以下を ISE で設定する必要があります。

- エンドポイント保護サービスの有効化
- ERS 設定の有効化
- 隔離承認プロファイルの作成
- 隔離用承認ポリシーの作成

エンドポイント保護サービスの有効化

EPS サービスは EPS 操作用に ISE で有効にする必要があります。

エンドポイント保護サービスを有効にするには、次の手順を実行します。

ステップ 1 [管理(Administration)] -> [システム(System)] -> [設定(Settings)] -> [エンドポイント保護サービス(Endpoint Protection Service)] を選択します。

ステップ 2 [サービスステータス(Service Status)] ドロップダウンから、[有効(Enabled)] を選択します。

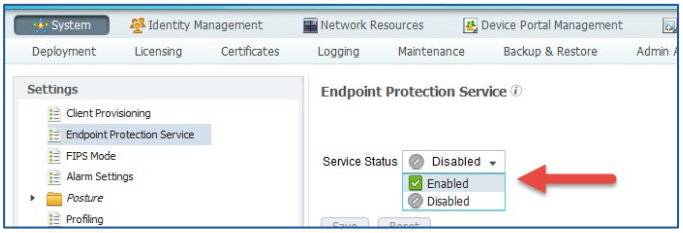


図 166.

ERS 設定の有効化

EPS 操作用に ISE で ERS（外部 Restful サービス）API を有効にします。

ERS 設定を有効にするには、次の手順を実行します。

ステップ 1 [管理（Administration）] -> [システム（System）] -> [設定（Settings）] -> [ERS 設定（ERS Settings）] を選択します。
ステップ 2 管理モードの [ERS 設定（ERS settings）] で、[読み書き用に ERS を有効にする（Enable ERS for Read/Write）] を選択します。
ステップ 3 [保存（Save）] を選択します。

隔離承認プロファイルの作成

まず、承認プロファイルは、承認ポリシーで使用される隔離用に作成されます。

承認プロファイルを作成するには、次の手順を実行します。

ステップ 1 [ポリシー（Policy）] -> [ポリシー要素（Policy Elements）] -> [結果（Results）] -> [承認（Authorization）] -> [承認プロファイル（Authorization Profiles）] -> [追加（Add）] を選択します。
ステップ 2 プロファイルに **Quarantine** と名前をつけます。

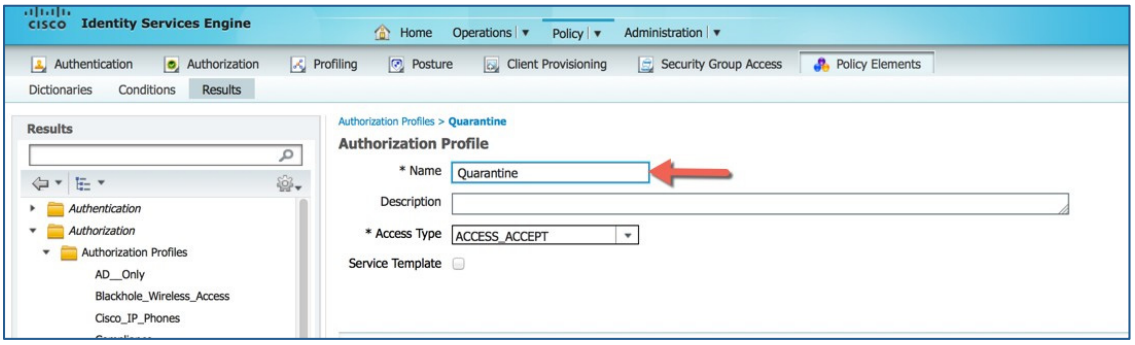


図 167.

ステップ 3 デフォルトのままにします。
ステップ 4 [送信（Submit）] を選択します。

承認ポリシーの作成

ステップ 1 [ポリシー（Policy）] -> [承認ポリシー（Authorization Policy）] を選択します。
ステップ 2 [編集（Edit）] と [上に新規ルールを挿入（Insert New Rule Above）] をクリックします。
ステップ 3 標準ルール 2 の名前を **Quarantine** に変更します。
ステップ 4 [属性の選択（Select Attribute）] の横にある + をクリックします。
ステップ 5 [新規条件の作成（Create New Condition）] をクリックします。
ステップ 6 [属性（Attribute）] -> [セッション：EPSTATUS は隔離に等しい（Session:EPSTATUS Equals Quarantine）] を選択します。
ステップ 7 [承認プロファイル（Authz Profile）] の横にある + をクリックします。
ステップ 8 ドロップダウンから、[標準（Standard）] -> [ポスチャプロファイル（Posture profile）] を選択します。

新しいポリシーが作成され、次の画面が表示されます。

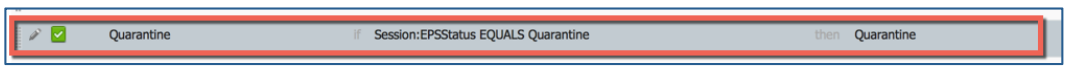


図 168.

ステップ 9 [保存（Save）] をクリックします。

ISE カテゴリの有効化

このセクションでは、ISE ロギング カテゴリを定義します。

ステップ 1 [管理（Administration）] -> [システム（System）] -> [ロギング（Logging）] -> [リモートロギングターゲット（Remote Logging Targets）] -> [追加（Add）] を選択します。

ステップ 2 リモート ログイン ターゲットとして Splunk を追加します。

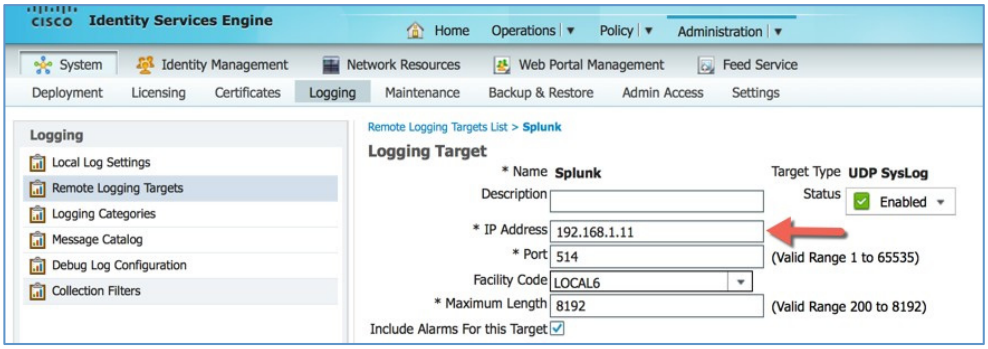


図 169.

注：最大長サイズは、1024 ～ 8192 に調整できます。

ステップ 3 目的の ISE ロギング カテゴリを選択します。

注：カテゴリ選択は送信される syslog の量と Splunk のハードドライブの可用性に影響することに注意してください。AAA 親カテゴリを選択し、目的のカテゴリに応じて追加できます。

EPS ポスチャの使用例

この EPS ポスチャは次の使用例を示します。

ユーザ Johnny Skiber は非準拠で、Antispyware Windows Defender サービスが実行されていません。**EPS_Quarantine_By_IP** ワークフロー アクションを使用して、デバイスが隔離されます。ユーザがサービスを有効にし、**EPS_Unquarantine_By_MAC** ワークフロー アクションが呼び出されます。ISE NAC エージェントがポスチャをチェックし、ユーザが準拠していると見なし、ネットワークへのフル アクセスが与えられます。

ステップ 1 NAC エージェントはユーザが非準拠と見なします。

図 170.

ISE の [操作認証（Operations Authentications）] ビューで、ユーザが非準拠になっています。

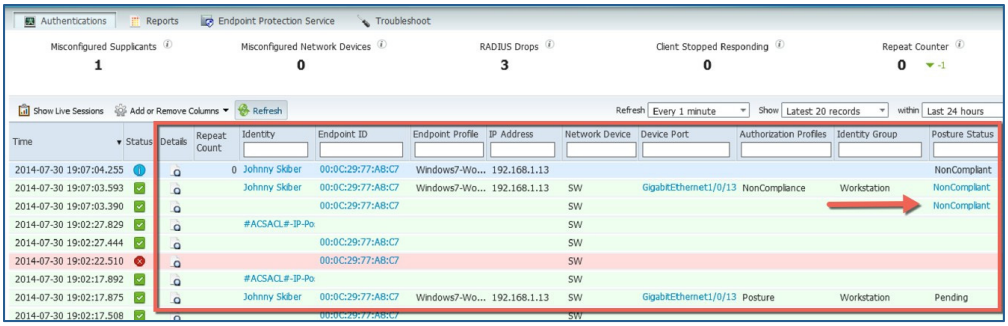


図 171.

ISE ポスチャ スパイウェア対策（すべてのユーザ向け）ダッシュボードのアプリケーションで ISE アドオンの Splunk を確認します。

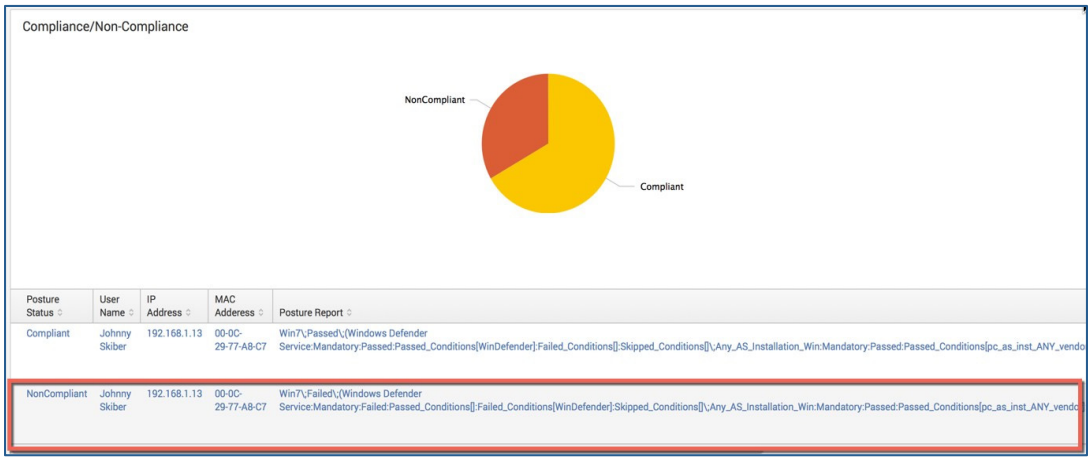


図 172.

エンドユーザが非準拠で、**AS Windows Defender** の必須チェックが失敗したことに注目してください。

ステップ 2 [NonCompliant] イベントをクリックします。

これにより、syslog イベントに移動します。

ステップ 3 **EPS_Quarantine_By_IpAddress_192.168.1.13** を選択します。

192.168.1.13 IP アドレスがエンドポイントの IP アドレスであることに注意してください。

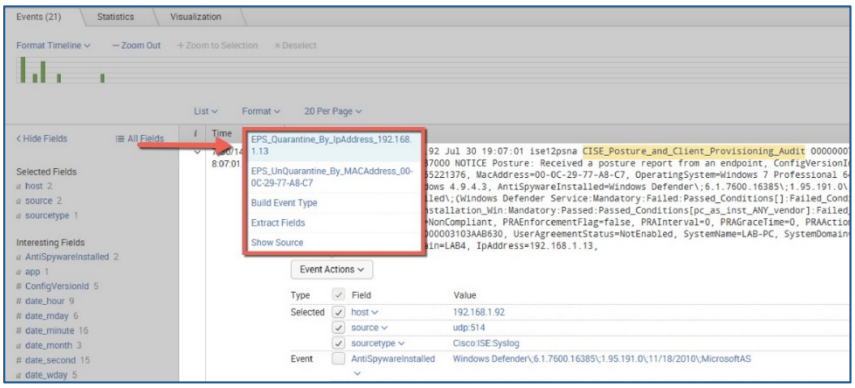


図 173.

これにより URI REST EPS リンクが起動し、ISE 管理者クレデンシャルの入力が求められます。

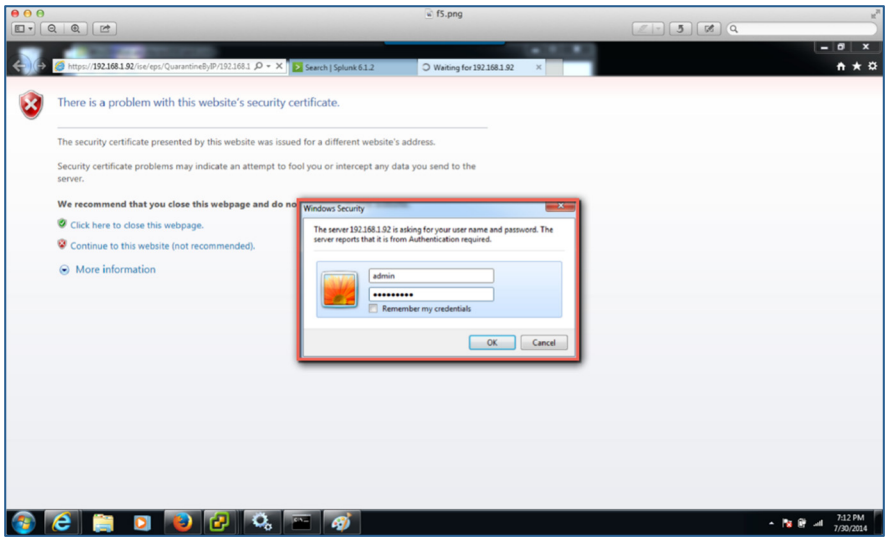


図 174.

REST API へのリンクが表示されます。

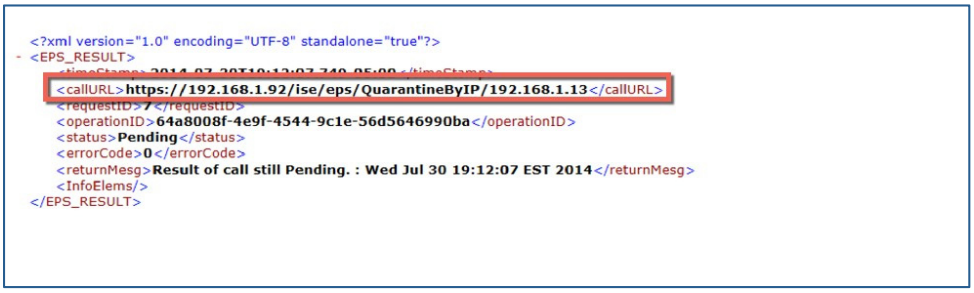


図 175.

[操作認証(Operations Authentications)] ビューでユーザが隔離されます。

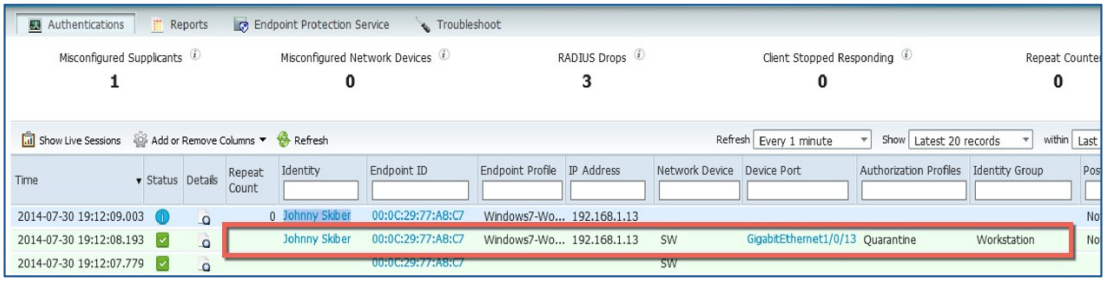


図 176.

ステップ 4 **Windows Defender** サービスを開始します。

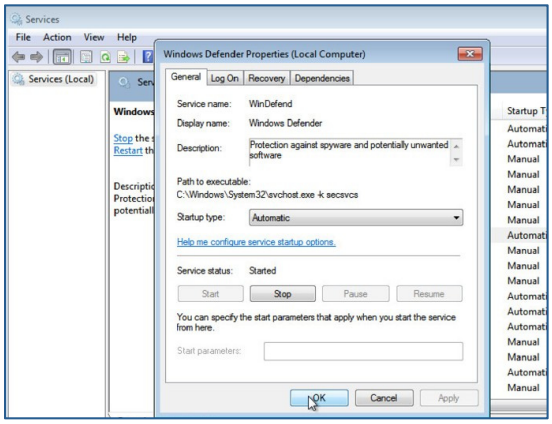


図 177.

ステップ 5 イベントに戻り、**EPS_Unquarantine_By_MACAddress_00-0C-29-77-A8-C7** ワークフロー アクションを起動します。

注:これはエンドポイントの MAC アドレスです。

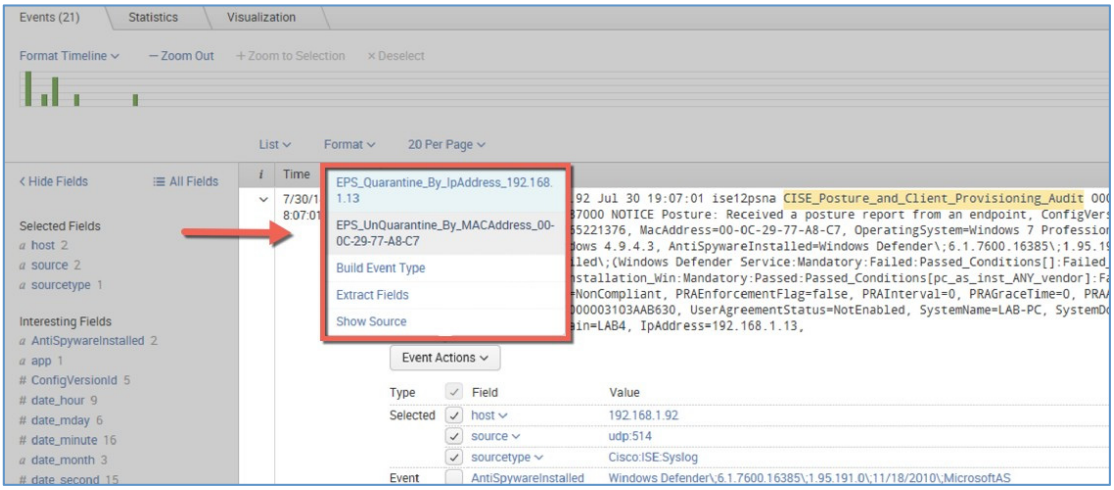


図 178.

ISE モニタリング ノードを対象とした REST API リンクが表示されます。

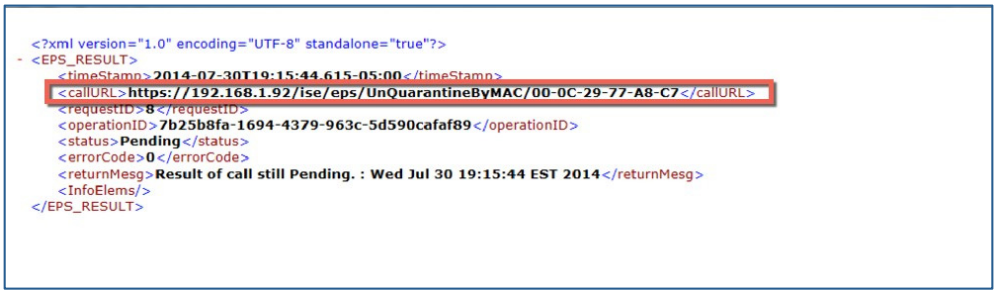


図 179.

[ISE 操作認証（ISE Operations Authentications）] ビューで、矢印はデバイスが隔離解除されたことを示します。

NAC エージェントがエンドポイントが準拠していると見なしていることに注意してください。

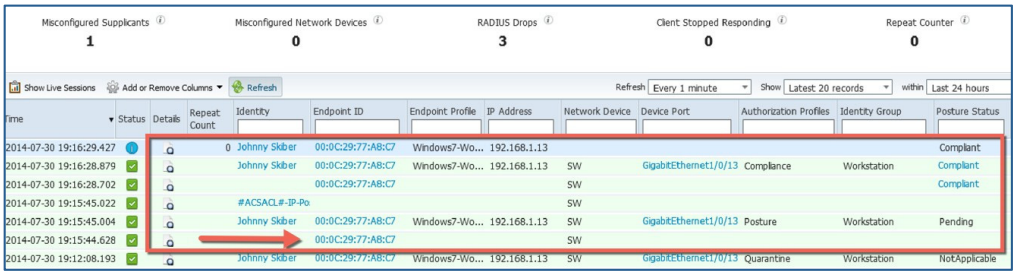


図 180.

AS ポスチャ ダッシュボードに準拠ユーザが表示されることに注意してください。

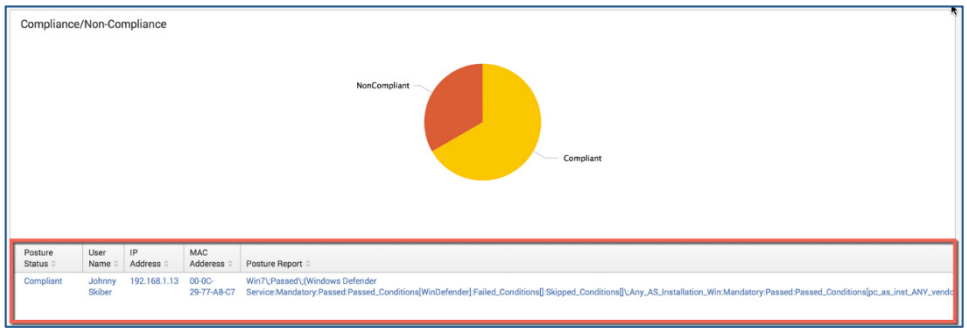


図 181.

AntiSpyware Windows Defender がインストールされていることに注意してください。

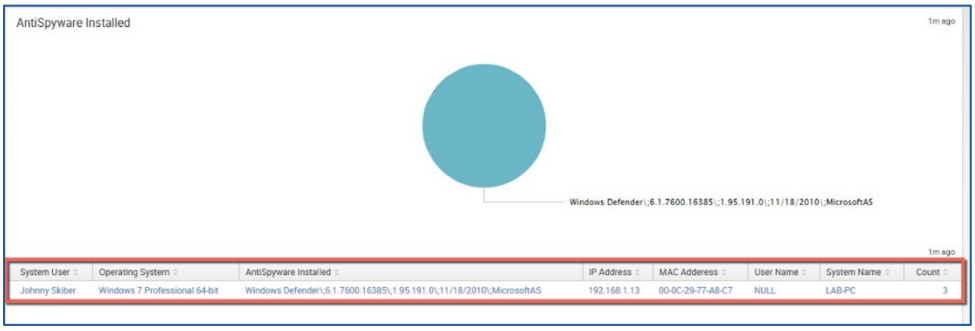


図 182.