イベントの表示と管理

イベントダッシュボードの概要

イベントダッシュボードは、デバイス（ルーター、スイッチ、ワイヤレスコントローラ、AP）およびエンドポイント（有線およびワイヤレス）のイベントのコンテキストビューを提供します。イベントに関連する他のデバイスに接続されているデバイスによってトリガーされたイベントを検索する代わりに、アシュアランス がこれらの詳細を提供します。

デフォルトでは、**イベント**ダッシュボードにはタイムラインチャートとリストビューが表示されます。

タイムラインチャートは、一定期間に発生したデバイスタイプ別のイベント数を色で表現します。

リストビューには、イベントのテーブルが表示されます。最大 10,000 のイベントが表示できますが、それ以上のイベントがログに記録されている場合があります。最大 5000 件のイベントを CSV ファイルにエクスポートできます。ただし、5000 を超えるイベントがある場合、エクスポート機能は無効になります。

リストビューからイベントをクリックして、接続されたデバイスによってトリガーされたイベントなどの詳細を表示できます。イベントの時間の範囲は、15 分刻みで最大 1 時間（+/- 15 分、+/- 30 分、+/- 45 分、+/- 1 時間）設定できます。

複数のイベントを選択すると、イベントの詳細を含む複数のカードを表示できます。複数のイベントカードが表示されている場合、カードを最小化、最大化、および閉じることができます。たとえば、あるイベントについて接続デバイスイベントテーブルを表示するには、そのイベントカードを最大化します。複数のカードビューに戻るには、 カードを最小化します。

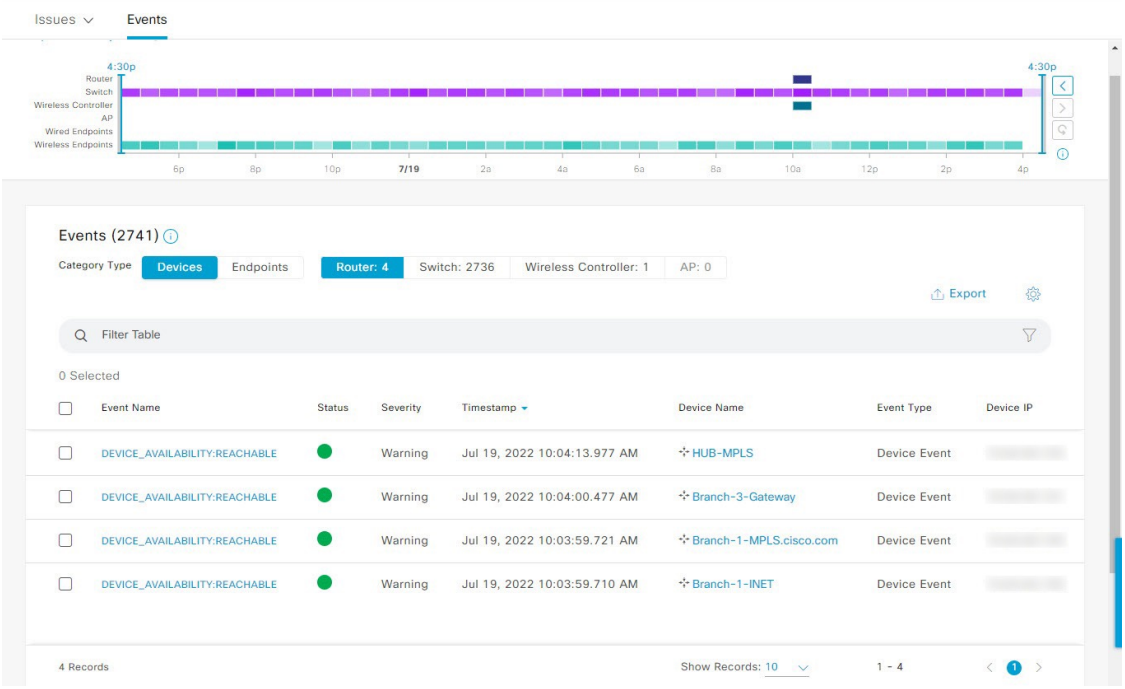
デバイスイベントの表示

この手順を使用して、ルータ、スイッチ、ワイヤレスコントローラ、およびAPによって生成されたイベントを表示します。

ステップ1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Assurance]** > **[Dashboards]** > **[Issues and Events]** の順に選択します。

デフォルトで [Category Type] として [Device] が選択された状態で [Events] ダッシュボードが開きます。

図 *1 : Device Events* ダッシュボード



Device Events ダッシュボード	
アイテム	説明
Global	• 上部のメニューバーで Global をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 • [location] アイコンの横にある をクリックし、[Site Details] を選択して、各サイトのイベントカウントを表示します。 • ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択した項目に基づいて、テーブルが更新されます。 • [Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのイベントのみが表示されます。
[Time Range] の設定	選択した時間範囲に基づく情報をウィンドウに表示できます。デフォルトは [24 Hours] です。次の手順を実行します。 **1.** [24 Hours] ドロップダウン リストで、時間範囲（[3 hours]、[24 Hours]、または [7 days]）を選択します。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。 これにより、タイムラインの範囲が設定されます。
タイムラインスライダ	より詳細な時間範囲を指定できます。時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。 色は、デバイスの種類を表します。 ：ルータ ：スイッチ ：ワイヤレスコントローラ ：AP 色の明度は重要性（そのデバイスで発生したイベント数の多寡）を示します。たとえば、薄い青色は、濃い青色よりもルーターのイベントが少ないことを示します。
Total Events	特定の時間範囲におけるすべてのデバイスタイプのイベントの総数。

ステップ 2 [Events] の [Category Type] で、[Router] タブ、[Switch] タブ、[Wireless Controller] タブ、または [AP] タブをクリックして、そのデバイスタイプのイベントのリストをテーブルに表示します。

イベントの表	
アイテム	説明
Event Name	イベントの名前。 イベント名をクリックすると、イベントの詳細が表示されたslide-in paneが開きます。
Status	デバイスのステータスです。 色はイベントの重大度を表します。 ●：エラー。 ●：警告。 ●：情報。 ●：使用できるデータがありません。
重大度	イベントの重大度：Critical 以上（Emergency および Alert）と、Critical レベルよりも低い重大度（Error、Warning、Notice、Info）。
Timestamp	イベントが発生した日付と時刻。
Device Name	イベントの影響を受けたデバイス名。 デバイス名をクリックして、[Device 360] ウィンドウを開きます。
イベント タイプ	イベントのカテゴリ: Syslog、トラップ、イベント、または AP イベント。
デバイス IP	デバイスの IP アドレス。

ステップ 3 複数のイベントを表示するには、表示する各イベントの横にあるチェックボックスをオンにして、[Show Selected Events] をクリックします。

[Multiple Events] slide-in paneが開き、各イベントが個別のカードに表示されます。

カードの中から、次のことができます。

- カードを最小化、最大化、および閉じます。
- 下矢印をクリックして詳細を表示します。
- ハイパーリンクをクリックして、それぞれの [Device 360] ウィンドウを起動します。

カードを最大化すると、接続されているデバイスのイベントがすべて表示されます。

ステップ 4 [Multiple Events] slide-in paneで、リストビューアイコン をクリックすると、リスト内のすべてのサブイベントを集めたものが順番に表示されます。

カードビューに戻るには、カードビューアイコン をクリックします。

エンドポイントイベントの表示

この手順を使用して、有線およびワイヤレスエンドポイントによって生成されたイベントを表示します。

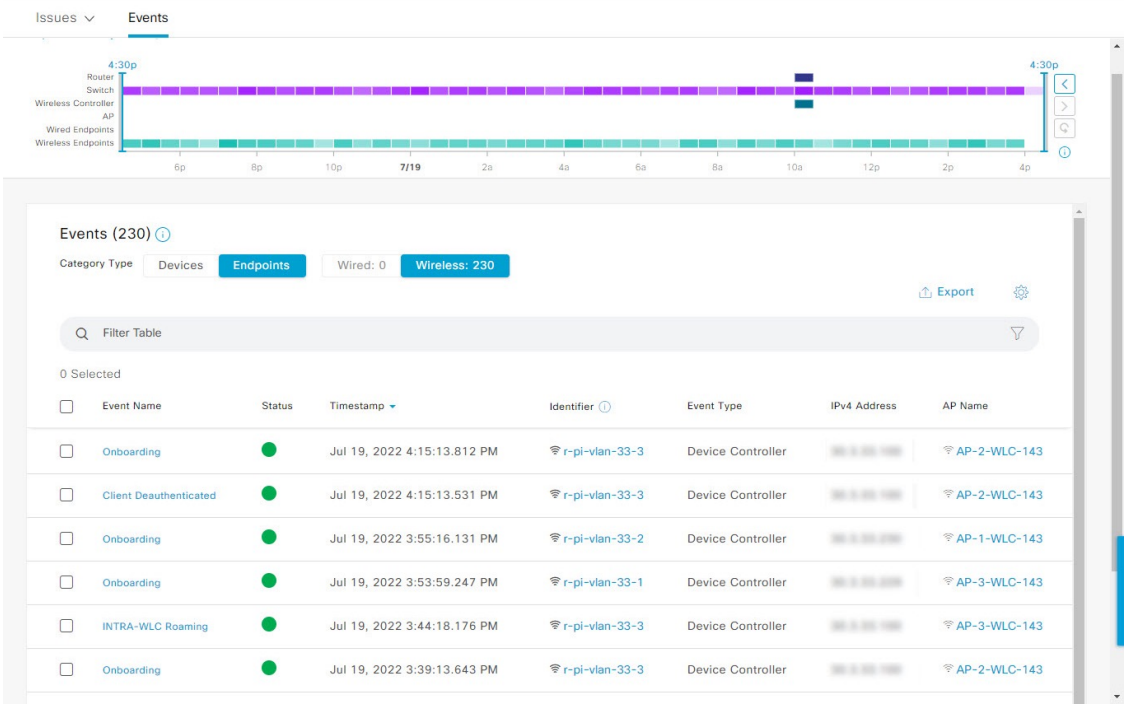
ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Assurance]** > **[Dashboards]** > **[Issues and Events]** の順に選択します。

ステップ 2 [Events] タブをクリックします。

[Events] ダッシュボードが開きます。

ステップ 3 [Category Type] で、[Endpoints] タブをクリックします。

図 *2 : Endpoint Events* ダッシュボード



Device Events ダッシュボード	
アイテム	説明
Global	• 上部のメニューバーで Global をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 • [location] アイコンの横にある をクリックし、[Site Details] を選択して、各サイトのイベントカウントを表示します。 • ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択した項目に基づいて、テーブルが更新されます。 • [Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのイベントのみが表示されます。
[Time Range] の設定	選択した時間範囲に基づく情報をウィンドウに表示できます。デフォルトは [24 Hours] です。次の手順を実行します。 **1.** [24 Hours] ドロップダウン リストで、時間範囲（[3 hours]、[24 Hours]、または [7 days]）を選択します。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。 これにより、タイムラインの範囲が設定されます。
タイムラインスライダ	より詳細な時間範囲を指定できます。時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。 色は、エンドポイントの種類を表します。 ：有線 ：ワイヤレス 色の明度は重要性（そのデバイスで発生したイベント数の多寡）を示します。たとえば、薄い紫色は、濃い紫色よりもエンドポイントのイベントが少ないことを示します。
Total Events	特定の時間範囲におけるすべてのエンドポイントタイプのイベントの総数。

ステップ 4 [Wired] または [Wireless] タブをクリックして、テーブル内のそのエンドポイントタイプのイベントのリストを表示します。

イベントの表	
アイテム	**説明**
Event Name	イベントの名前。 イベント名をクリックすると、その詳細が表示されたslide-in paneが開きます。
Status（有線エンドポイントのみ）	色はイベントの重大度を表します。 ●：エラー。 ●：警告。 ●：情報。 ●：使用できるデータがありません。
Severity（有線エンドポイントのみ）	イベントのシビラティ（重大度）です。重大度は、Critical 以上（Emergency、Alert）、およびこれより低い重大度（Error、Warning、Notice、Info）の場合があります。
Timestamp	イベントが発生した日付と時刻。
[Identifier]	エンドポイントの識別子。これは、その順序での可用性に応じて、ユーザー ID、ホスト名、IP アドレス、MAC アドレスのいずれかになります。 識別子をクリックすると、その詳細が表示されたslide-in paneが開きます。
イベント タイプ	イベントのカテゴリ: Syslog、トラップ、イベント、または AP イベント。
IPv4 アドレス（IPv4 Address）	エンドポイントに接続されているデバイスの IPv4 アドレス。
AP Name（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントに接続されている AP の名前。 AP 名をクリックして、[Device 360] ウィンドウを開きます。
Switch（有線エンドポイントのみ）	有線エンドポイントに接続されているスイッチの名前。 スイッチ名をクリックして、[Device 360] ウィンドウを開きます。
[MAC Address]	エンドポイントに接続されているデバイスの MAC アドレス。
Port（有線エンドポイントのみ）	有線エンドポイントに接続されているスイッチポート。
VLAN ID（有線エンドポイントのみ）	有線エンドポイントに接続されているスイッチポートの VLAN ID。
Switch IP Address（有線エンドポイントのみ）	有線エンドポイントに接続されているスイッチの IP アドレス。
AP MAC（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントに接続されている AP の MAC アドレス。

イベントの表	
アイテム	説明
SSID（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントが使用している SSID。
UserID（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントのユーザー ID。
Wireless Controller Name（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントに接続されているワイヤレスコントローラの名前。
Band（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントが使用している無線帯域。
DHCP Server（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントが使用している DHCP サーバー。

ステップ 5 複数のイベントを表示するには、表示する各イベントの横にあるチェックボックスをオンにして、[Show Selected Events] をクリックします。

[Multiple Events] slide-in paneが開き、各イベントが個別のカードに表示されます。

カードの中から、次のことができます。

- カードを最小化、最大化、および閉じます。
- 下矢印をクリックして詳細を表示します。
- ハイパーリンクされたデータをクリックします。

カードを最大化すると、接続されているデバイスのイベントがすべて表示されます。

ステップ 6 [Multiple Events] slide-in paneで、リストビューアイコン をクリックすると、リスト内のすべてのサブイベントを集めたものが順番に表示されます。

カードビューに戻るには、カードビューアイコン をクリックします。

イベント分析の表示：ダッシュボードのプレビュー

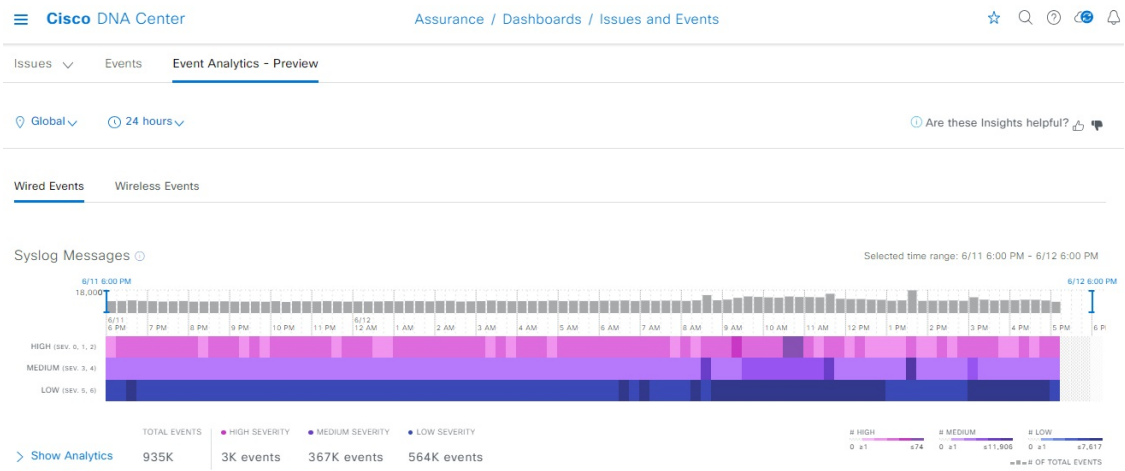
[Events Analytics - Preview] ダッシュボードには、さまざまなタイプのネットワークイベントであるsyslogメッセージが可視化されるため、ユーザーは異なるデータソース間のトレンドを識別し、イベントを関連付けられます。

この手順を使用して、syslog メッセージの数と有線およびワイヤレス ネットワーク イベントの到達可能性の遷移を表示するヒートマップとして表される分析とインサイトを表示します。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Assurance]** > **[Dashboards]** > **[Issues and Events]** の順に選択します。

ステップ 2 [Event Analytics - Preview] タブをクリックすると、イベント分析ダッシュボードが開き、有線イベントが表示されます。

図 *3 : [Event Analytics - Preview]* ダッシュボード



[Event Analytics - Preview] ダッシュボード	
アイテム	**説明**
Global	上部のメニューバーでこのアイコンをクリックして、[Select a location] スライドインペインからサイト階層のサイト、建物、またはフロアを選択します。.
[Time Range] の設定	選択した時間範囲に基づく情報をウィンドウに表示できます。デフォルトは [24 Hours] です。次の手順を実行します。 **1.** [24 Hours] ドロップダウンリストで、時間範囲（[24 hours]、[7 days]、[14 days]、[30 days]、または [60 days]）を選択します。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。 これにより、タイムラインの範囲が設定されます。

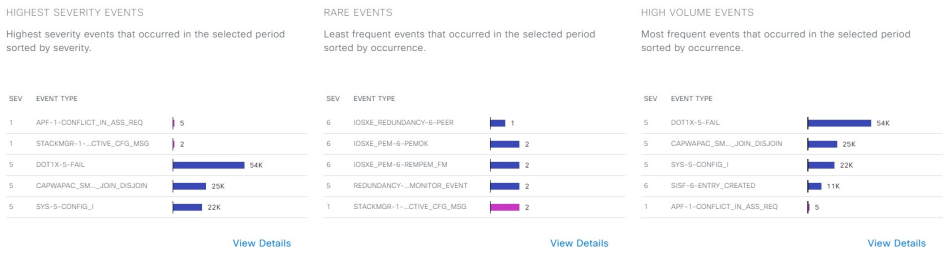
ステップ 3 [Wired Events] をクリックして、syslog メッセージの数と有線デバイスからの到達可能性の遷移を表示するヒートマップを表示します。これには、最大 24 時間の期間に対して 15 分単位のメッセージ重大度データの内訳が含まれます。7 日の場合は 4 時間単位、14 日および 30 日の場合は 12 時間単位、60 日の場合は 24 時間単位となります。

Syslog メッセージ：

- ヒートマップの上部にあるタイムスライダを使用して syslog メッセージのヒートマップに特定の期間を設定し、イベントの合計数、高、中、低に分類されたメッセージ重大度の数を表示できます。
- インサイトと分析データの syslog メッセージを表示するには、[Show Analytics] をクリックします。さまざまな可視化を備えた一連のカードには、syslog メッセージまたはデバイスの数が異なる分析基準に基づいた順序で表示されます。現在サポートされている syslog メッセージの分析は、次のとおりです。
  - 重大度が最も高いイベント：選択した期間に発生した重大度が最も高いイベントです（重大度別）。

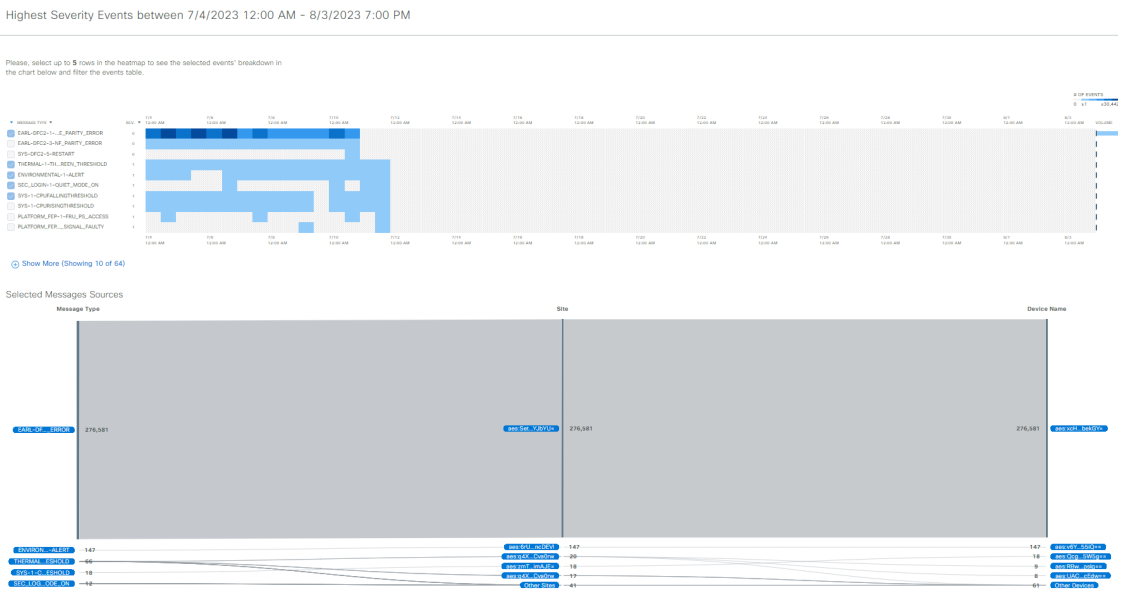
    .
  - 頻度の低いイベント：選択した期間に発生した最も頻度の低いイベントです（発生回数別）。
  - 大量のイベント：選択した期間に発生した最も頻度の高いイベントです（発生回数別）。
  - メッセージ量の増加：選択した期間内で増加量が最も高いイベントです（変動量別）。
  - メッセージ量の減少：選択した期間内で減少量が最も高いイベントです（変動量別）。
  - 新規イベント：選択した期間の終わりの時点で発生が開始されていたイベントです（発生回数別）。
  - 最もアクティブなデバイス：選択した期間に最も多くのイベントを生成したデバイスです（生成量別）。

図 *4 : syslog* メッセージの分析



- [View Details] をクリックしてスライドインペインを開き、各イベントタイプのイベント数に関する詳細なヒートマップを時系列で表示します。ヒートマップで最大 5 つの syslog メッセージタイプを選択して Sankey チャートをフィルタ処理し、選択したイベントタイプの分布を表示して、特定のサイトおよびデバイス生成イベントについて学習できます。

図 *5 : Sankey* チャートを使用した *syslog* イベントヒートマップ



- Sankey チャートでメッセージタイプ、サイト、またはデバイスを選択し、チャートの下にあるイベントテーブルをフィルタ処理してデータを表示できます。イベントテーブルには、最大 10,000 のイベントを表示できます。ユーザー定義の問題を作成するには、イベントテーブルの [messages] をクリックし、[Confirm] をクリックします。

到達可能性の遷移：

- ヒートマップの上部にあるタイムスライダを使用してヒートマップで特定の期間を設定し、イベント、到達不能イベント、到達可能イベント、および ping 到達可能イベントの合計数を表示できます。
- 別のカードに表示された有線デバイスからの各到達可能性の遷移（上位ステータス遷移、イベント別上位デバイス）のインサイトと分析データを表示するには、[Show Analytics] をクリックします。
- [View Details] をクリックしてスライドインペインを開き、各イベントタイプのイベント数に関する詳細なヒートマップを時系列で表示します。ヒートマップで最大 5 つのイベントを選択して Sankey チャートをフィルタ処理し、選択したイベントタイプの分布を表示して、特定のサイトおよびデバイス生成イベントについて学習できます。
- Sankey チャートで From イベント、To イベント、サイト、またはデバイスを選択し、イベントテーブルをフィルタ処理して、各イベントの到達可能性の遷移を表示できます。イベントテーブルには、最大 10,000 のイベントを表示できます。

ステップ 4 [Wireless Events] をクリックして、syslog メッセージの数と有線デバイスからの到達可能性の遷移を表示するヒートマップを表示します。これには、15 分単位のメッセージ重大度データの内訳が含まれます。

syslog メッセージ：

- ヒートマップの上部にあるタイムスライダを使用して syslog メッセージのヒートマップに特定の期間を設定し、イベントの合計数、高、中、低に分類されたメッセージ重大度の数を表示できます。

- 別のカードに表示される各syslogメッセージのインサイトと分析データを表示するには、[Show Analytics] をクリックします。使用可能な syslog メッセージの分析カードが、重大度とイベントタイプとともに表示されます。
- [View Details] をクリックしてスライドインペインを開き、各イベントタイプのイベント数に関する詳細なヒートマップを時系列で表示します。ヒートマップで最大 5 つの syslog メッセージタイプを選択してSankeyチャートをフィルタ処理し、選択したイベントタイプの分布を表示して、特定のサイトおよびデバイス生成イベントについて学習できます。
- Sankey チャートでメッセージタイプ、サイト、またはデバイスを選択し、イベントテーブルをフィルタ処理して syslog メッセージを表示できます。イベントテーブルには、最大 10,000 のイベントを表示できます。

到達可能性の遷移：

- ヒートマップの上部にあるタイムスライダを使用してヒートマップで特定の期間を設定し、イベント、到達不能イベント、到達可能イベント、および ping 到達可能イベントの合計数を表示できます。
- 別のカードに表示されたワイヤレスデバイスからの各到達可能性の遷移（上位ステータス遷移、イベント別上位デバイス）のインサイトと分析データを表示するには、[Show Analytics] をクリックします。
- [View Details] をクリックしてスライドインペインを開き、各イベントタイプのイベント数に関する詳細なヒートマップを時系列で表示します。ヒートマップで最大5つのイベントを選択してSankeyチャートをフィルタ処理し、選択したイベントタイプの分布を表示して、特定のサイトおよびデバイス生成イベントについて学習できます。
- Sankey チャートで From イベント、To イベント、サイト、またはデバイスを選択し、イベントテーブルをフィルタ処理して、各イベントの到達可能性の遷移を表示できます。イベントテーブルには、最大 10,000 のイベントを表示できます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。