



保証

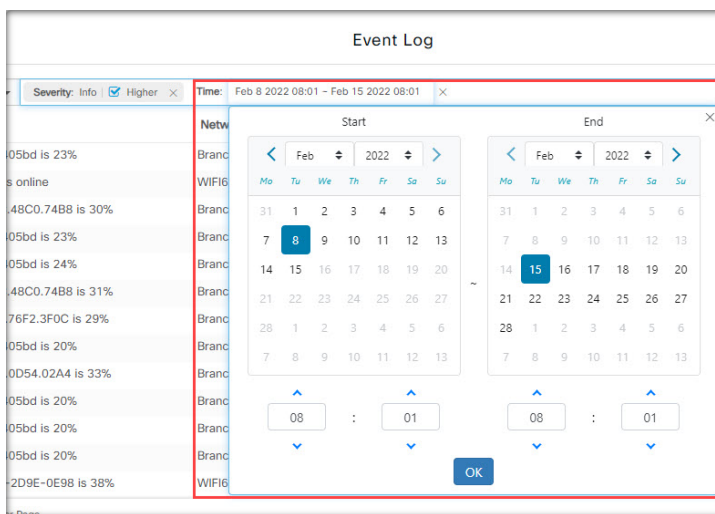
この項では、次のトピックを扱います。

- [イベントログについて](#) (1 ページ)
- [モニタリングのデフォルト値](#) (3 ページ)
- [モニタリングプロファイル](#) (4 ページ)
- [デバイスの完全性](#) (6 ページ)
- [通知](#) (6 ページ)

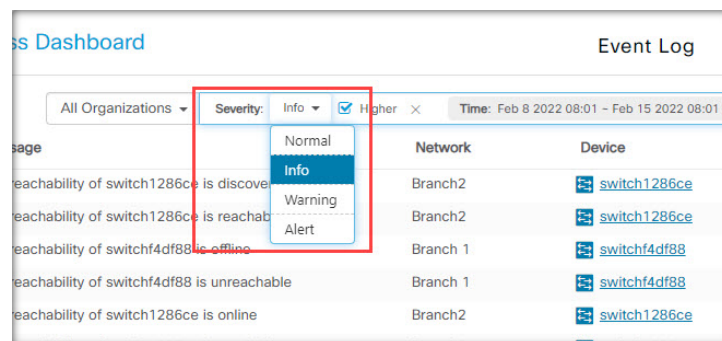
イベントログについて

[EventLog] 画面を開いて、ネットワーク全体で発生したイベントを検索します。この画面は、ネットワーク全体で生成されたイベントを検索およびソートできるインターフェイスを提供します。これらのイベントが最大500,000件、最大90日間保存されます。提供されるフィルタコントロールを使用して、次のパラメータの組み合わせに基づいて表示されたイベントを制限することができます。

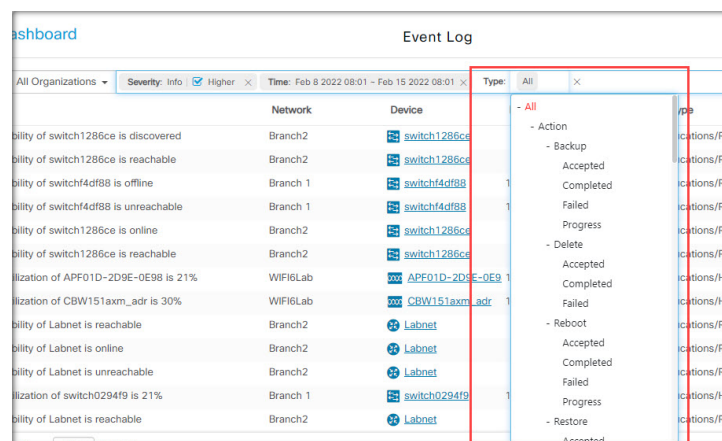
[Time] を追加し、目的の期間を示す開始時刻と終了時刻を指定します。この期間内に発生したイベントのみが表示されます。



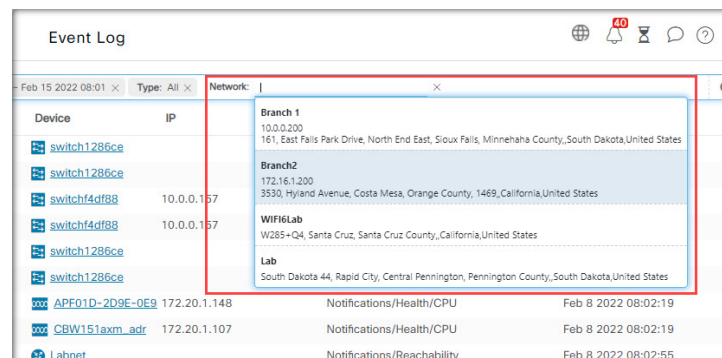
[Severity] フィルタを追加し、表示するイベントのレベルを選択します。[Higher] チェックボックスを選択して、より高いレベルの重大度のイベントを含めることもできます。



[Type] フィルタを追加し、表示するイベントタイプを1つ以上選択します。タイプはツリー構造で配置され、タイプを選択すると選択したタイプの下の子のすべてのイベントタイプが自動的にツリーに含まれます。



[Network] フィルタを使用して、1つ以上のネットワーク別にイベントを表示します。入力すると、一致したサイトが表示されます。



[Device] フィルタを使用して、1つ以上のデバイス別にイベントを表示します。入力すると、一致したデバイスが表示されます。名前、IPアドレス、またはMACアドレスでデバイスを指定することもできます。

Device	IP	Timestamp
AP5CE1.76F2.3F0C	172.16.1.164	5 2022 06:15
RV160W	172.16.1.2	5 2022 06:31
AP6C71.0D54.02A4	172.16.1.163	5 2022 05:05
AP5CE1.76F2.3F0C	172.16.1.164	5 2022 07:05
router44912C	172.16.1.60	5 2022 07:01
switch0294f9	10.0.0.110	5 2022 06:10
switch0294f9	10.0.0.110	5 2022 05:07

フィルタ条件に一致するイベントは、次の例のようなテーブルに表示されます。列見出しを使用して、テーブル内の情報を並べ替えることもできます。

Severity	Message	Network	Device	IP	Type	Timestamp
Warning	The CPU utilization of RV160W is 54%	Branch2	EV160W	172.16.1.2	Notifications/Health/CPU	Feb 15 2022 06:31:49
Warning	The CPU utilization of AP5CE1.76F2.3F0C is 22%	Branch2	AP5CE1.76F2.3F0C	172.16.1.164	Notifications/Health/CPU	Feb 15 2022 06:15:41
Alert	The CPU utilization of router44912C is 76%	Branch2	router44912C	172.16.1.60	Notifications/Health/CPU	Feb 15 2022 06:15:41
Alert	The CPU utilization of RV160W is 84%	Branch2	EV160W	172.16.1.2	Notifications/Health/CPU	Feb 15 2022 07:01:32
Warning	The CPU utilization of AP6A53.0E22.0A70 is 31%	Branch2	AP6A53.0E22.0A70	172.16.1.101	Notifications/Health/CPU	Feb 15 2022 07:05:41
Alert	The CPU utilization of RV160W is 80%	Branch2	EV160W	172.16.1.2	Notifications/Health/CPU	Feb 15 2022 04:46:30
Warning	The CPU utilization of AP5CE1.76F2.3F0C is 30%	Branch2	AP5CE1.76F2.3F0C	172.16.1.164	Notifications/Health/CPU	Feb 15 2022 07:05:41
Warning	The CPU utilization of AP5CE1.76F2.3F0C is 22%	Branch2	AP5CE1.76F2.3F0C	172.16.1.164	Notifications/Health/CPU	Feb 15 2022 03:55:41
Alert	The CPU utilization of RV160W is 74%	Branch2	EV160W	172.16.1.2	Notifications/Health/CPU	Feb 15 2022 07:45:50
Warning	The CPU utilization of AP6C71.0D54.02A4 is 26%	Branch2	AP6C71.0D54.02A4	172.16.1.163	Notifications/Health/CPU	Feb 15 2022 05:05:41
Warning	The CPU utilization of AP5CE1.76F2.3F0C is 20%	Branch2	AP5CE1.76F2.3F0C	172.16.1.164	Notifications/Health/CPU	Feb 15 2022 04:20:41

モニタリングのデフォルト値

モニタリングプロファイルを使用して、ネットワークで実行されるデバイスモニタリングを制御できます。モニタリングプロファイルは、組織レベルまたはシステムレベルで適用できます。システムレベルのモニタリングプロファイルの継承を選択した組織は、[Monitoring Defaults] ページで動作を制御します。

システム全体に適用される [Monitoring Profiles] を変更するには、以下の手順に従います。

1. [Assurance] > [Monitoring] > [Monitoring Defaults]に移動します。
2. ドロップダウンを使用して、対応するタイプのデバイスに適用する適切なモニタリングプロファイルを選択します。モニタリングプロファイルの作成の詳細については、「モニタリングプロファイルの管理」を参照してください。
3. [Save] をクリックします。

実行可能なモニタリングのタイプとその設定方法の詳細については、「[モニタリングプロファイル](#)」を参照してください。組織レベルでのモニタリング設定の変更に関する詳細については、[組織](#)を参照してください。

モニタリングプロファイル

モニタリングプロファイルは、デバイスから収集されるデータと生成される通知を制御します。プロファイルは、組織内またはシステム内のさまざまなタイプのデバイスに適用できます。たとえば、デバイスによっては、場所やセキュリティ要件に応じて異なる監視要件が必要になる場合があります。プロファイル内では、**通知モニタ**と**レポートモニタ**の2種類のモニタがサポートされています。

通知モニタは、通常、デバイスの状態の変化またはしきい値を超えるパラメータに起因して、通知およびアラートを生成します。通知には、情報、警告、およびアラートの重大度レベルがあり、次のチャンネルで配信されます。

- Web UI のポップアップ通知。
- 電子メール。これには、電子メール設定が正しく設定されている必要があります。詳細については、[電子メール設定の管理](#)を参照してください。
- ヘルプデスクチケット。これには、ヘルプデスクサービスを提供するアプリケーションとの統合が必要です。詳細については、[統合設定の管理](#)を参照してください。
- コラボレーションメッセージ。これには、コラボレーションアプリケーションとの統合が必要です。詳細については、[統合設定の管理](#)を参照してください。



(注) モニタリングプロファイルを設定して、チケットまたはコラボレーションメッセージの平均レートが1時間あたり60を超えないようにすることをお勧めします。外部アプリケーションと通信する場合、これを超えるレートが持続すると、APIの輻輳とイベントの損失が発生する可能性があります。

アクティブな通知は [Notification Center] にも表示され、デバイス情報ビューにも表示されます。通知の変更も [Event Log] に記録されます。

レポートモニタは、監視ダッシュボードのワイヤレスレポートおよびトラフィックグラフで使用されるデータを収集します。

複数のモニタリングプロファイルを作成し、システムレベルで、または組織ごとに、異なるデバイスタイプに異なるプロファイルを割り当てることができます。プロファイルへのテンプレートの割り当てに関する詳細については、[組織](#)と[モニタリングのデフォルト値 \(3 ページ\)](#)を参照してください。

新しいモニタリングプロファイルを追加

1. [Assurance] > [Monitoring] > [Monitoring Profiles]に移動します。
2. [+] (プラス) アイコンをクリックして新しいプロファイルを作成します。

3. プロファイルの名前と、プロファイルを関連付ける組織を指定します。ここで [All Organizations] を指定して、プロファイルを任意の組織で使用できるようにしたり、システムレベルのデフォルトとして使用したりすることもできます。
4. プロファイルの説明と、通知を受信する電子メールアドレスのカンマ区切りリストを指定することもできます。
5. [Save] をクリックします。
6. 画面が更新され、さまざまな通知モニタとレポートモニタが表示されます。用意されているコントロールを使用して、個々のモニターを有効または無効にすることができます。
7. 通知モニターには、[Edit] アイコンをクリックして変更できる追加の設定があります。設定はモニタによって異なりますが、生成される通知タイプ、通知のシビラティ（重大度）、通知をトリガーするしきい値が含まれます。

既存のモニタリングプロファイルをコピー

既存のモニタリングプロファイルをコピーするには、以下の手順に従います。

1. [Assurance] > [Monitoring] > [Monitoring Profiles] に移動します。
2. コピーするプロファイルの横にあるチェックボックスを選択し、[Save As] アイコンをクリックします。
3. 必要に応じてプロファイル名、説明、組織、電子メールアドレスを更新してから、[Save] をクリックします。
4. 必要に応じて、通知モニタとレポートモニタを変更します。[Reset to defaults] ボタンをクリックすると、モニター設定をデフォルトに戻すことができます。

モニタリングプロファイルを変更

既存のモニタリングプロファイルを変更するには、以下の手順に従います。

1. [Assurance] > [Monitoring] > [Monitoring Profiles] に移動します。
2. コピーするプロファイルの横にあるチェックボックスを選択し、[Edit] アイコンをクリックします。
3. 必要に応じてプロファイル設定と電子メールアドレスを更新してから、[Save] をクリックします。
4. 必要に応じて、通知モニタとレポートモニタを変更します。[Reset to defaults] ボタンをクリックすると、モニター設定をデフォルトに戻すことができます。

モニタリングプロファイルを削除

1. [Assurance] > [Monitoring] > [Monitoring Profiles] に移動します。

2. コピーするプロファイルの横にあるチェックボックスをオンにして、[Delete] アイコンをクリックします。



(注) プロファイルが組織レベルのモニタリングプロファイルとして使用されている場合は、対応する組織とデバイスタイプがシステムレベルの設定を継承するように更新されます。システムレベルのモニタリングプロファイルとして使用されているプロファイルは削除できません。プロファイルを削除する前に、そのプロファイルを [Assurance]>[Monitoring]>[Monitoring Defaults] ページから削除します。

デバイスの完全性

このサービスでは、シスコの Trustworthy 技術を搭載したシスコのソフトウェアおよびハードウェアの主要コンポーネントを検証して、お客様のシスコ製品の完全性を分析します。このセキュリティ技術は、偽造やソフトウェアの改ざんを防いで、シスコ製品が想定通りに動作するようシスコのネットワークングデバイスに組み込まれています。

The screenshot shows the 'Device Integrity' section of the Cisco Business Dashboard. It includes a 'Verify' button and a 'Start Over' button. The main content area displays the following information:

- Device Identification:**
 - Device Identified
 - SUDI Validation:
 - Cisco Root CA
 - Cisco SUDI Sub-CA
 - Cisco SUDI Device-CA
 - Cisco SUDI Signature
 - Integrity Check:
 - Output Signature
 - PCRP
 - Boot Loader
 - PCRS
 - Device OS
- Product:**
 - Product ID: C1300-16P-4X
 - Boot Loader: 1.0.76
 - Version:
 - Firmware: 4.0.0.91
 - Version:
- Certificate:**
 - Certificate: High Assurance SUDI CA
 - Issuer: Cisco
 - Valid From: 2022-12-29
 - Valid Thru: 2099-08-09

デバイスの完全性を確認する手順は、次のとおりです。

1. CLI コマンドをコピーします。
2. デバイスの CLI (コマンドラインインターフェイス) を開き、CLI コマンドを貼り付けて実行します。
3. CBD GUI で、CLI 出力を貼り付けるか、CLI 出力をファイルに保存してから、アップロードします。
4. [Verify] をクリックします。

通知

このセグメントには、次のセクションが含まれています。

通知について

Cisco Business ダッシュボードにより、Connectwise または Webex チームの統合通知など、ネットワークでさまざまなイベントが発生したときに通知が生成されます。通知は、電子メールか、ブラウザの右下隅に表示されるポップアップアラートを生成し、すべての通知は後で確認するためにログに記録されます。

通知は、関心がなくなったときに確認することもできます。デフォルトでは、これらの通知は [Notification Center] に表示されません。

サポートされる通知

次の表に、Cisco Business ダッシュボードでサポートされている通知のリストを示します

表 1: サポートされる通知

イベント	レベル	説明	自動的にクリアされるか
アクセスポイント、ルータ、IP 電話、およびスイッチのデバイス通知			
到達可能性/デバイスが検出されました	Information	ネットワーク上に新しいデバイスが検出されました。	はい。デバイス検出の5分後。
到達可能性/デバイスが検出されませんでした	Warning	デバイスは検出プロトコルを通じて認識されていますが、IP を使用して到達できません。	はい (IP を介してデバイスに再度到達可能になったとき)
到達可能性/デバイスがオフラインです	Alert	デバイスはネットワーク上で検出されなくなりました。	はい (デバイスが再検出されたとき)
クレデンシャルが必要です/SNMP	Warning	Probe は、認証エラーによりデバイスにアクセスできません。	はい (Probe が認証されたとき)
クレデンシャルが必要です/ユーザ ID	Warning	Probe は、認証エラーによりデバイスにアクセスできません。	はい (Probe が認証されたとき)
ログイン情報が必要/パスワードが期限切れ	Warning	デバイスの管理者ユーザーのパスワードの有効期限が切れています。	はい (デバイスのパスワードがリセットされたとき)。
コンフィギュレーションの不一致	Alert	現在のデバイス設定が、Cisco Business Dashboard の設定プロファイルおよびデバイス設定で指定された設定と一致しません。	はい (設定の不一致が解決されたとき)。

イベント	レベル	説明	自動的にクリアされるか
デバイスサービス/SNMP	Warning	SNMP がデバイスで無効になっています。	はい (SNMP が有効になったとき)
デバイス サービス/Web サービス	Warning	Web サービスがデバイスで無効になっています。	はい (web サービス API が有効化されているとき)
状態	Warning/Alert	デバイスの稼働レベルが警告またはアラートに変化しました。	はい (デバイスの稼働状態が正常に戻ったとき)
シスコサポート通知			
ファームウェア	Information	新しいバージョンのファームウェアが cisco.com で入手できます	はい (デバイスが最新版にアップデートされたとき)
サポート終了	Warning/Alert	デバイスのサポート終了製品速報が検出されたか、またはサポート終了のマイルストーンに到達しました。	なし
メンテナンス有効期限	Warning/Alert	デバイスは保証対象外である、または現在有効な保守契約が結ばれていない、あるいはその両方です。	はい (新しい保守契約が結ばれた場合)
デバイスの健全性通知			
CPU	Warning/Alert	デバイスの CPU 使用率が最大しきい値を超えています。	はい (CPU 使用率が通常のレベルに戻った場合)
稼働時間	Warning/Alert	デバイスの稼働時間が最小しきい値を下回っています。	はい (デバイスの稼働時間が最小レベルを超えた場合)
接続クライアント数	Warning/Alert	接続されているクライアントの数が最大しきい値を超えています。	はい (接続されているクライアントの数が許容レベルに戻ったとき)

現在のデバイスの通知の表示とフィルタリング

1つのデバイスまたはすべてのデバイスに対して現在有効な通知を表示するには、以下の手順を実行します。

ステップ 1 [Home] ウィンドウで、グローバルツールバーの右上隅にある [Notification Center] アイコンをクリックします。アイコンの番号バッジは未確認の通知の総数を示しており、バッジの色は現在未確認の最も高いシビラティ（重大度）を示しています。

現在未処理になっている通知は、[Notification Center] アイコンの下に表示されます。シビラティ（重大度）アイコンの数字は、以下の各カテゴリの通知の総数を示しています。

- 情報（緑色の円形のアイコン）
- 警告（オレンジ色の三角形のアイコン）
- アラート（赤い逆三角形のアイコン）

ステップ 2 [Notification Center] では、次のアクションを実行できます。

- 通知の確認：通知のチェックボックスをオンにして、通知を確認します。表示内のすべての通知を確認するには、[ACK All] チェックボックスをオンにします。
- 表示されている通知のフィルタリング：この操作の手順を以下に示します。

ステップ 3 フィルタボックスは、テーブルに表示される通知を制限します。デフォルトでは、すべてのタイプとすべてのシビラティ（重大度）レベルの通知が表示されます。既存のフィルタを変更するには、そのフィルタをダブルクリックして設定を変更します。新しいフィルタを追加するには、[Add Filter] ラベルをクリックし、ドロップダウンリストからフィルタを選択します。使用可能なフィルタは次のとおりです。

表 2: 使用可能なフィルタ

フィルタ	説明
Notification Type	表示する通知のタイプ。たとえば、オフラインのデバイスに対する通知を表示するには、ドロップダウンリストから [Device Offline] を選択します。
Severity	表示する通知のシビラティ（重大度）。次のいずれかを指定できます。 <ul style="list-style-type: none"> • Info • Warning • Alert [Higher] チェックボックスをオンにすると、高いレベルのシビラティ（重大度）を含めることができます。
Include Ack	確認応答済みの通知を含めます。
Network	指定したネットワークの通知を表示します。フィルタで入力を開始すると、一致するネットワークがドロップダウンに表示されます。該当するネットワークをクリックして選択します。 フィルタ内に複数のネットワークを含めることができます。

フィルタ	説明
Device	<p>指定したデバイスの通知を表示します。フィルタで入力を開始すると、一致するデバイスがドロップダウンに表示されます。目的のデバイスをクリックして選択します。</p> <p>フィルタ内に複数のデバイスを含めることができます。</p>

(注) 個々のデバイスに対する通知は、デバイスの [Basic Info] パネルと [Detailed Info] パネルで確認できます。

通知の受信方法を制御するには、組織レベルまたはシステム レベルで通知設定を変更します。

デバイスの履歴通知の表示とフィルタリング

通知の発生または状態の変化は、Dashboard にイベントとして記録され、[Event Log] でも表示されます。イベントログのサブセットは、次のパネルで表示できます。

[Basic Info] パネルまたは [Device Detail] パネルには、個々のデバイスが表示されます。

[Basic Info] パネルには、過去 24 時間分のイベントのみが表示されます。

[Device Detail] パネルには、使用可能なデバイスのすべての履歴データが表示されます。



(注) [Device Detail] パネルは、フィルタ処理することで関心のあるイベントを特定することができます。履歴イベントの表示とフィルタ処理に関する詳細については、「[イベントログについて](#)」を参照してください。

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。