システム ステータス

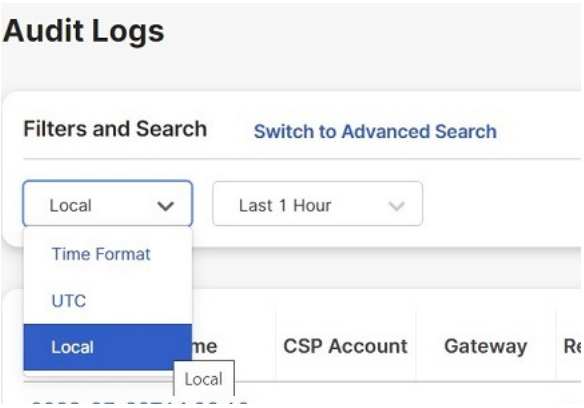
監査ログ

監査ログには、ユーザーが実行したアクションの詳細が含まれます。これには、ログイン/ログアウトアクティビティ、プロファイル、ルール、ゲートウェイの作成、削除、更新、有効化、無効化などのアクション、または Multicloud Defense ソリューションの設定および運用に関連するユーザーアクティビティが含まれますが、これらに限定されません。

[時間フォーマット（Time Format）]

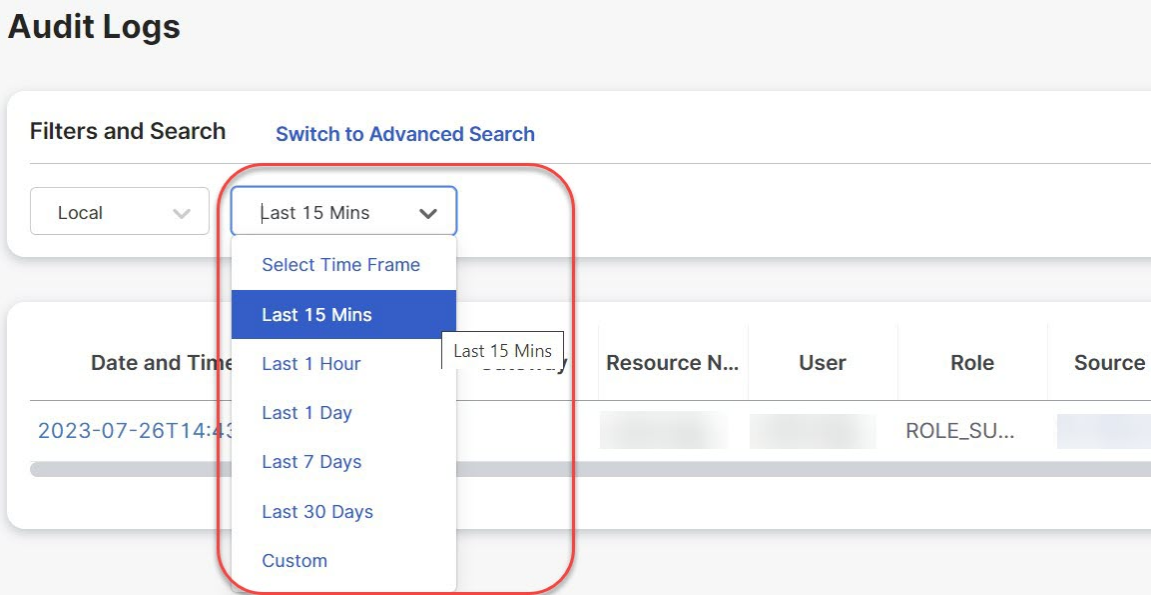
ログは、UTC（協定世界時）または現地時間の形式で表示できます。[ローカル（Local）]は、設定されたユーザーのタイムゾーンを意味します。たとえば、米国/太平洋時間です。ログの日付と時刻は ISO 8601 形式で表示されます（省略なしの日付、時、分、秒、および小数点以下の秒数：YYYY-MM-DD T HH:MM:SS:S）。例：`2020-11-22T10:58:46.820`

異なる時間形式を選択または切り替えるには、次に示すようにオプションボタンをクリックします。



タイムフレーム（Timeframe）

ログは、15 分から 30 日の増分オプション、またはカスタムタイムフレームで表示できます。タイムフレームを選択または切り替えるには、次に示すようにドロップダウンメニューをクリックしてタイムフレームを選択します。



カスタムタイムフレームの場合は、[カスタム（Custom）] を選択し、カレンダーオブジェクトをクリックして [開始（Start）]、[終了（End）] の日付または時刻を選択してから、[保存（Save）] をクリックします。

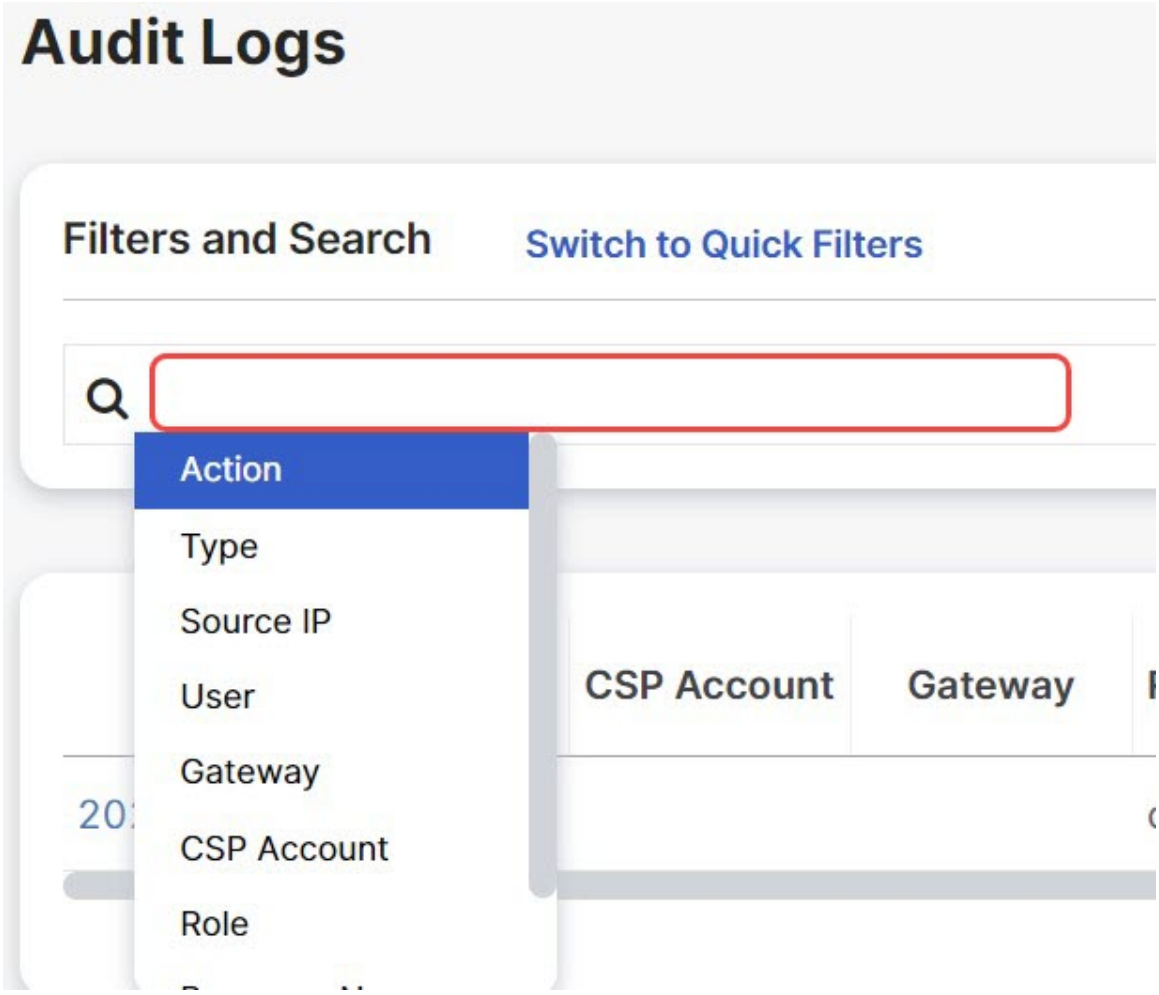
Search Filter

ログは、検索機能と監査ログフィールドを使用してフィルタ処理できます。監査ログフィールドは、[アクション（Action）]、[タイプ（Type）]、[送信元IP（Source IP）]、[ユーザー（User）]、[ゲートウェイ（Gateway）]、[CSPアカウント（CSP Account）]、[ロール（Role）] です。

1 つまたは複数のフィールドで監査ログをフィルタリングするには、次の手順を実行します。

手順

ステップ 1 [検索（Search）] フィールドを左クリックして、プルダウンメニューにアクセスします。



ステップ 2 フィールドを選択します。

ステップ 3 目的の検索文字列を入力します。

ステップ 4 必要に応じて、検索条件にフィールドを追加します。

例：「**DELETE**」でフィルタリングされ、実行したユーザーに「**steve**」という文字列が含まれるアクションが、フィルタ条件と結果に表示されます。

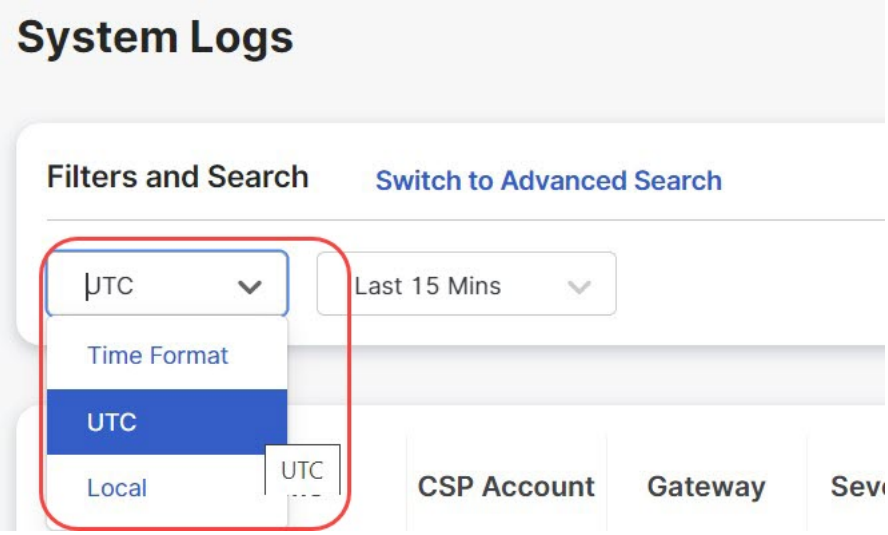
システム ログ

システムログには、Multicloud Defense ソリューションが実行するアクションの詳細が含まれています。これには、システムメッセージ、ゲートウェイイベント、インスタンスの作成または削除、Multicloud Defense ソリューションのその他の設定と操作の変更が含まれます。これらのログは 1 年間保存されます。

[時間フォーマット（Time Format）]

ログは UTC（協定世界時）または現地時間の形式で表示されます。[ローカル（Local）] は、設定されたユーザーのタイムゾーンを意味します。たとえば、米国/太平洋時間です。ログの日付と時刻は ISO 8601 形式で表示されます（省略なしの日付、時、分、秒、および小数点以下の秒数：YYYY-MM-DD T HH:MM:SS:S）。例：`2020-11-22T10:58:46.820`

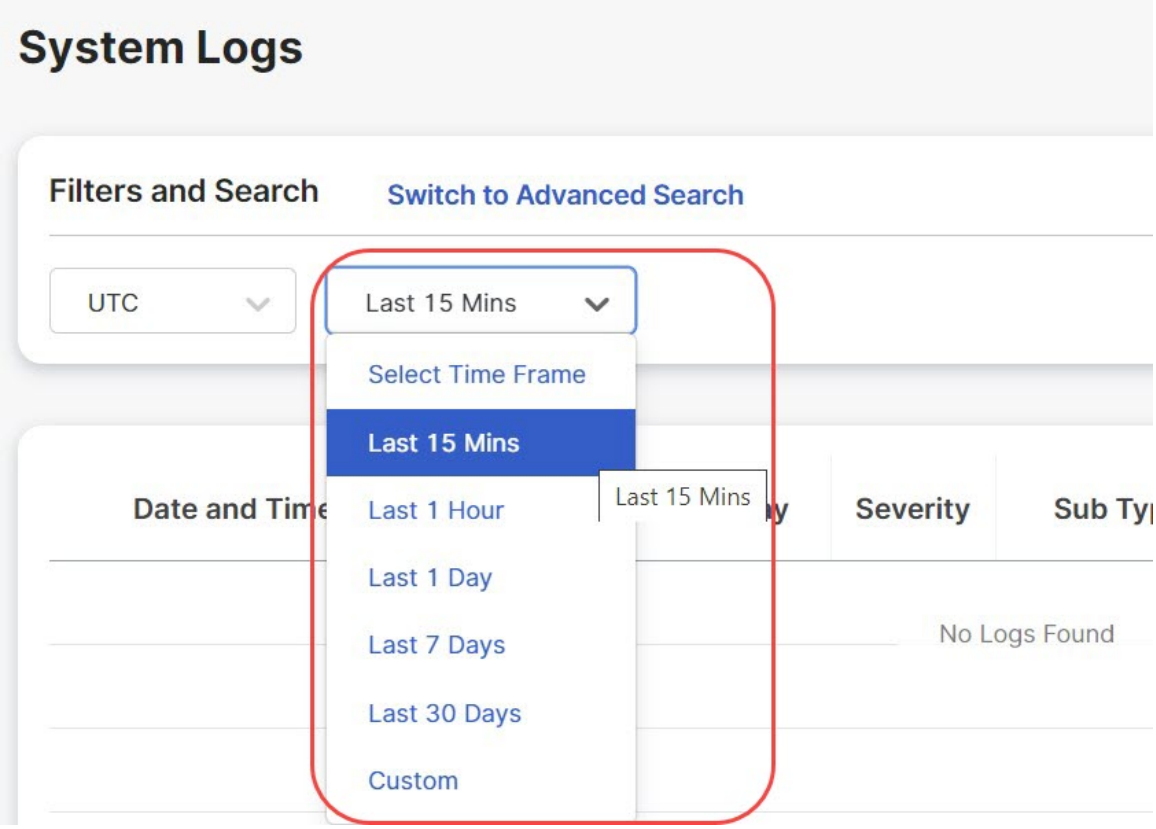
異なる時間形式を選択または切り替えるには、次に示すようにオプションボタンをクリックします。



タイムフレーム（Timeframe）

ログは、15 分から 30 日の増分オプション、またはカスタムタイムフレームで表示できます。

タイムフレームを選択または切り替えるには、次に示すようにドロップダウンをクリックしてタイムフレームを選択します。



カスタムタイムフレームの場合は、[カスタム（Custom）]を選択し、カレンダーオブジェクトをクリックして [開始（Start）]、[終了（End）] の日付または時刻を選択してから、[保存（Save）] をクリックします。

重大度

システムログの重大度は次のとおりです。

- [情報（Info）]：サインイン、サインアウト、パスワードの変更、設定の変更などの参考情報の詳細。ここには、他の重大度レベルに当てはまらないイベントが含まれます。
- [警告（Warning）]：考えられるシステムアクションまたは変更（パスワードの更新など）を通知します。
- [中（Medium）]：パッケージのアップグレードなど、重大度が中程度の問題。
- [高（High）]：外部デバイスとのネットワーク接続の切断などの重大な問題。
- [重大（Critical）]：ハードウェア障害など、本質的に重大な深刻な問題。

Search Filter

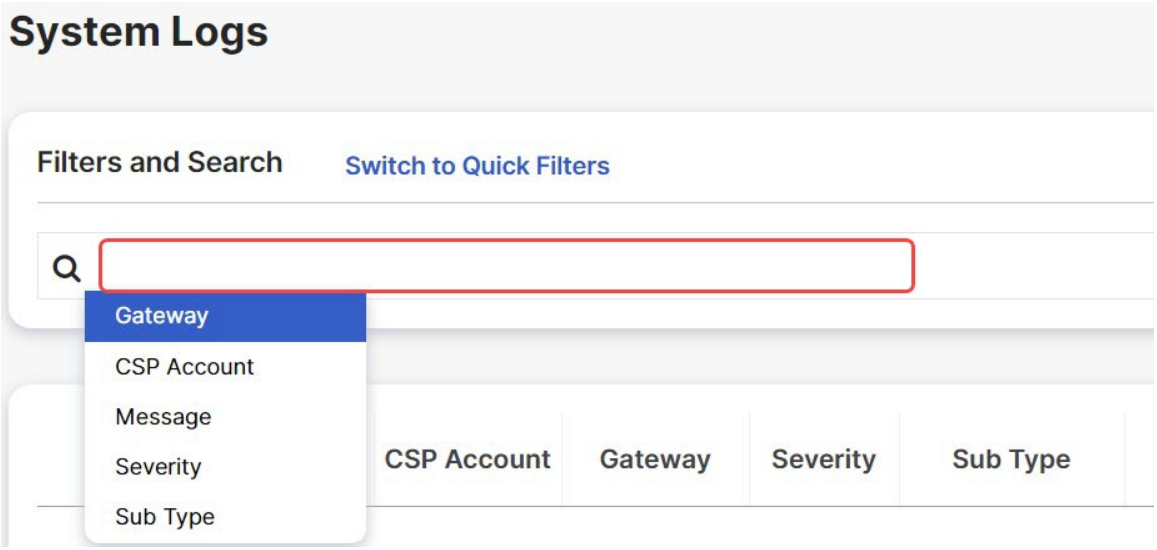
ログは、検索機能とシステムログフィールドを使用してフィルタ処理できます。

システムログフィールドは、[ゲートウェイ（Gateway）]、[CSPアカウント（CSP Account）]、[メッセージ（Message）] です。

1 つまたは複数のフィールドでシステムログをフィルタリングするには、次の手順を実行します。

手順

ステップ 1 [検索（Search）] フィールドを左クリックして、プルダウンメニューにアクセスします。



ステップ 2 [ゲートウェイ（Gateway）] などのフィールドを選択します。

ステップ 3 目的の検索文字列を入力します（例：`ingress`）。

ステップ 4 必要に応じて、検索条件にフィールドを追加します。

例：「**ingress**」でフィルタリングされたゲートウェイと、「**created**」を含むメッセージが、フィルタ条件と結果に表示されます。

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。