Citrix Analytics for Security

Machine translated content

Disclaimer

Contents

新機能

June 18, 2024

Citrix の目標は、Citrix Analytics のお客様に新機能や製品アップデートを提供することです。新しいリリースでは、より便利な機能をご利用いただけます。今すぐ更新してください。

このプロセスは、お客様向けのわかりやすいものになっています。最初の更新は、Citrix 内部サイトのみに適用され、その後徐々にお客様の環境に適用されます。アップデートを段階的に配信することで、製品の品質を確保し、可用性を最大限に高めることができます。

2024 年 **4** 月 **15** 日

新しいエグゼクティブサマリーレポート

複数のレポートを単一のエグゼクティブレポートに統合して、必要な期間にスケジュールを設定できるようになりました。この新機能では、必要なグラフィック情報のみを視聴者に提供できます。詳細については、「エグゼクティブサマリーレポート」を参照してください。

2024 年 **1** 月 **29** 日

Workspace アプリステータスフィールドの更新

- セルフサービス検索: **Citrix Apps and Desktops** データソースに新しく導入された Workspace アプリステータスフィールドを利用して、クエリを実行して **Workspace** アプリバージョンのサポートステータスを確認できるようになりました。
- ユーザー: **Workspace** アプリのステータス列は削除されました。

詳しくは、「アプリとデスクトップのセルフサービス検索」を参照してください。

2024 年 **1** 月 **25** 日

CAS UI の矛盾が解消されました

Apps and Desktops データソースのセルフサービス検索機能で、以下の問題が解決されました:

- 以前はセッション内で順序どおりに表示されていなかったイベントが正しく表示されるようになりました。
- 既定の列が更新されました。

2024 年 1 月 24 日

SIEM 環境でのユーザープロファイルイベントの強化

SIEM 環境にエクスポートされるユーザープロファイルイベントには次のものが含まれるようになりました:

- IP アドレスに関する洞察
- Citrix Virtual Apps and Desktops と Citrix DaaS（旧 Citrix Virtual Apps and Desktops サービス）のロケーションインサイト

これらの新しい拡張機能により、組織のデータへのアクセスに使用されるクライアントの IP アドレスを特定し、Citrix Virtual Apps and Desktops、および Citrix DaaS の両方からユーザーの位置情報を収集できます。

詳細については、「SIEM のリスクインサイトデータ」を参照してください。

2023 年 12 月 1 日

週次メールと **SIEM** アラートの管理者メール設定ページ

新しい管理者メール設定機能では、システムアラートのカスタム配布リスト受信者を設定できます。この機能強化により、管理者は自分に関連するシステムアラートのみを受信できるようになります。

詳細については、「管理者メール設定」を参照してください。

ユーザーダッシュボード-アクティブユーザー数の時間フィルターが新しくなり、概要セクションが更新されました

ユーザーダッシュボードの新しい時間フィルターを使用すると、Citrix Analytics を有効にしたデータソースを考慮して、特定の期間の組織内のアクティブユーザーの総数を表示および変更できます。

ユーザーダッシュボードの強化された概要セクションには、組織内のユーザーの総数と、現在ログオンしているアクティブユーザーと非アクティブユーザーの数が表示されます。

詳細については、「ユーザーダッシュボード」を参照してください。

カスタムレポートの強化

- Citrix Analytics for Security で利用できるイベントとインサイトを使用して、カスタムレポートを作成およびスケジュールできるようになりました。カスタムレポートを使用すると、特定の関心のある情報を抽出し、データをグラフィカルに整理できます。
- Self-Service Search のクエリベースのレポート、テンプレート、より優れた視覚化、すべてのデータソースと指標の網羅性、レポートのスケジュール設定、PDF のエクスポートなど、強化されたカスタムレポートプラットフォーム機能を使用できるようになりました。

詳細については、「カスタムレポート」を参照してください。

2023 年 11 月 30 日

Citrix Analytics のすべての **ShareFile** 機能の削除

次の ShareFile 検出機能が削除されました:

- リンクを共有する
- 関連リスク指標
- ポリシーとその発生回数
- Content Collaboration データエクスポート設定
- Content Collaboration レポート
- 検索での Content Collaboration データソース
- Content Collaboration 保存済み検索
- Content Collaboration データソース。

これらの機能を削除すると、リスクスコアとユーザータイムラインが一時的に不一致になる可能性があります。Citrix Analytics の他の機能はすべて同じままです。

ShareFile がShareFile.com から直接セキュリティコントロールに簡単にアクセスできるようにする方法をご覧ください。

2023 年 9 月 22 日

カスタムインジケータの **Citrix Secure Browser** データソース

Citrix Secure Browser データソースのリスク指標を作成して、セキュアブラウザでのユーザーのアクティビティを追跡できるようになりました。詳細については、「カスタムインディケータ」を参照してください。

SIEM データエクスポートによる週次メールの強化

ウィークリーメールが強化され、SIEM データのエクスポートが可能になり、組織のセキュリティ体制をより深く把握できるようになりました。より多くのデータソースをオンボーディングしてアクティブ化し、ユーザーを取り巻くさまざまなイベントを発見できるようになりました。毎週のメールには、次の新しい追加事項が含まれています:

- データ概要セクションには、SIEM 環境でのデータ消費状況が表示されます。
- データエクスポートの消費状況に基づくデータエクスポートの推奨事項

詳細については、「毎週の電子メール通知」を参照してください。

メールでのカスタム管理者の通知設定の使用

Citrix Analytics for Security は、Citrix Cloud のカスタム管理者が設定した通知設定を引き継ぐようになりました。この機能強化により、カスタム管理者は通知設定をより柔軟に管理できます。この設定は、週次メール、管理者への通知アクションメール、データエクスポートのアラートなどの通知メールを送信する際にも使用されます。

詳細については、「セキュリティアナリティクスの管理者ロールの管理」を参照してください。

2023 年 **7** 月 **4** 日

セルフサービス検索とカスタムインジケーターでの **OR** オペレーターのサポート

OR** 演算子がセルフサービス検索とカスタムリスク指標機能で利用できるようになりました ** 。**OR** 演算子は、セルフサービス検索やカスタムインジケータクエリなどの検索ビューで使用できます。

詳細については、「検索クエリでサポートされる演算子」を参照してください。

2023 年 **6** 月 **15** 日

VDA クリップボードテレメトリを有効にする

Citrix Apps and Desktops でクリップボード操作を開始すると、VDA.Clipboard というイベントがトリガーされます。これらのクリップボードログには、VDA 名、クリップボードサイズ、クリップボード形式タイプ、クライアント IP、クリップボード操作、クリップボード操作の方向、クリップボード操作が許可されたかどうかなどの重要な情報が含まれます。VDA クリップボードのイベント属性は、セルフサービス検索およびカスタムリスク指標ワークフローでも使用できます。

- セルフサービス検索：レポートの生成、クエリの保存、VDA.Clipboard イベントとそのすべての属性の詳細の確認ができます。
- カスタムリスク指標：VDA クリップボードイベントの属性は、カスタムインジケーターワークフローで使用できます。これらのイベントキーと値のペアを使用して、カスタムインジケータートリガーを設定したり、アクション付きの自動ポリシーを設定したりできます。

セキュリティ監視ポリシーのクリップボードプレースメタデータコレクションを使用して、クリップボードテレメトリを有効にし、クリップボードログを **Citrix Analytics for** Security に送信できます。デフォルトでは、このポリシーは有効になっています。無効にするには、ポリシーページに移動して無効にし、VDA からのデータ収集を停止します。

詳しくは、「Citrix DaaS のクリップボードテレメトリの有効化」を参照してください。

2023 年 6 月 14 日

Citrix Analytics for Security での **Session Recording** アプリのライフサイクルイベントとレジストリイベントの可用性

SessionRecording** の以下のアプリケーションライフサイクルイベントとレジストリイベントが ** 、Citrix Analytics for Security で利用できるようになりました。

- Citrix. イベントモニター. レジストリ変更
- Citrix. イベントモニター. セッション起動
- Citrix. イベントモニター. セッション終了
- Citrix. イベントモニター. クリップボード
- Citrix. イベントモニター. ファイル転送

これらのイベントを表示したり、カスタムインジケーターを作成したり、これらのイベントを SIEM 環境にエクスポートしたりできます。

詳細については、「イベントタイプとサポートされているフィールド」を参照してください。

2023 年 6 月 8 日

解決された問題

- Citrix Analytics for Security に送信される一部のセッションログオンイベントには、ユーザー名がありません。この結果、セルフサービス検索およびアクセス保証ユーザーログオンページの一部のイベントで、ユーザー名列が「**NA** 」と表示されます。過去 1 時間や過去 **1** 日などの短い時間範囲のデータを表示すると、Access Assurance IP Registration Organizations グラフの合計ログオン数が 0 以外であるにもかかわらず、ユニークユーザー数がゼロになることもあります。この問題は修正されました。[CAS-70954]
- アプリとデスクトップのセルフサービス検索、Session.Logon および Session.end ユーザーイベントの場合、検索クエリの App-Name ディメンションに、起動されたアプリケーションまたはデスクトップの名前ではなく、デリバリーグループ名が入力されるため、管理者の誤解を招く可能性があります。App-Name ディメンションは、起動中のアプリケーションを指すため、App.Start/App.End イベントのクエリに便利です。詳細については、「アプリとデスクトップのセルフサービス検索」を参照してください。この問題は現在修正されています。[CAS-67968]
- 組織がアジア太平洋地域の **Citrix** Cloud にオンボーディングされている場合、Content Collaboration イベントは Citrix Analytics テナントに表示されません。この問題は現在修正されています。[CAS-62317]
- Citrix Workspace アプリおよび Citrix Receiver クライアントのいくつかのバージョンでは、特定のイベントが Citrix Analytics に送信されません。したがって、Citrix Analytics は、これらのイベントに関する洞察を提供したり、リスク指標を生成したりすることはできません。この問題は現在修正されています。詳細については、「チェック 6: 仮想アプリとデスクトップのイベントは Analytics に送信されていますか?」を参照してください。。[CAS-16151]

2023 年 5 月 29 日

Splunk 向け **Citrix Analytics** アドオンが **Splunk** クラウドプラットフォームで利用可能に

Splunk Integration for Citrix Analytics は、Splunk 向け Citrix Analytics アドオンを利用して分析環境に接続し、ビジネスに不可欠なデータを Splunk 環境に取り込みます。

以前は、アドオンは Splunk Enterprise レイヤーへのインストールについてのみ Splunk によって審査され、お客様はオンプレミスの Splunk 環境内でアドオンを構成する責任を負っていました。2.1.2 の最新バージョンでは、アドオンには Splunk プラットフォームと Splunk Cloud との互換性が追加されています。クラシックインスタンスを IDM インスタンスまたは **Victoria** インスタンスとともに使用しているお客様は、このプラットフォーム互換性拡張機能を利用できます。これで、お客様は Splunk Enterprise と Splunk Cloud のどちらかを柔軟に選択できるようになり、Splunk の統合を促進するアドオンの導入を検討できるようになりました。

詳細については、「Splunk インテグレーション」を参照してください。

SIEM のセッション記録イベント

Session Recording イベントを、** アプリとデスクトップのリスクインサイトイベントとデータソースイベントの形式で **SIEM** にエクスポートできるようになりました ** 。新しく追加されたイベントタイプは、データエクスポートページのエクスポート用データイベントステージにあります。

詳細については、「ポリシーとアクション」を参照してください。

2023 年 5 月 24 日

エンドユーザーへのグローバルアクションを通知

Citrix **Analytics** のポリシーとアクション機能が、組み込みまたはカスタムのリスク指標トリガーと組み合わせることができる **Notify End User** グローバルアクションをサポートするようになりました。管理者は、「エンドユーザーへの通知」アクションを使用して、エンドユーザーのみに電子メール通知を生成するポリシーを作成できます。このアクションは、許可されていないアプリケーションの使用についてユーザーに通知したり、Citrix アカウントで不審な動作が発生したときに中断を伴うアクションを実行せずに警告したりするなど、さまざまなコンプライアンス用途に使用できます。管理者は、特定のシナリオに応じてメールメッセージの本文と件名をカスタマイズできます。

詳細については、「エンドユーザーへの通知」を参照してください。

2023 年 5 月 4 日

テストイベント生成

テストイベント生成機能は、お客様が Citrix Analytics-SIEM パイプラインを迅速にテストできるように作成されています。以前は、管理者がこの統合をテストする必要がある場合、イベントが Citrix Analytics によって生成され、

SIEM 環境で受信されているかどうかを確認するために、データソースのオンボーディングとユーザーのアクティビティを待つ必要がありました。これはもはや必要ではありません。「テストデータを送信」ボタンをクリックするだけで、SIEM 環境にダミーイベントを送信し、提供されたクエリを使用して Citrix Analytics SIEM インテグレーションが期待どおりに設定されているかどうかを確認できます。これは、障害箇所の特定に役立つため、中断されたデータフローをデバッグしようとしている管理者にとっても有効です。

詳細については、「テストイベントの生成」を参照してください。

SIEM メールアラート生成

SIEM E メールアラート生成機能により、データエクスポートのトラブルシューティングがこれまでになく簡単になります。Citrix Analytics は、SIEM データフローの中断につながる、または SIEM データフローの中断を示す可能性のあるアクティビティについてシステムアラートを送信します。メールは、Citrix Cloud 管理者、セキュリティ担当管理者、セキュリティ読み取り専用管理者、およびセキュリティとパフォーマンスの読み取り専用管理者に配布されます。送信されるアラートの種類は次のとおりです。

1. **SIEM** データエクスポートアラート**-**パスワードがリセットされました

   このメールは、データエクスポートページからアカウントパスワードがリセットされるたびにトリガーされます。Citrix Analytics for Security GUI でのみ実行すると、データフローが中断する可能性があります。このアラートにはパスワードのリセットが実行された時刻が含まれるため、正常なデータフローに簡単に戻ることができます。

2. **SIEM** データエクスポートアラート**-**データフローが停止しました

このメールは、顧客がデータフローの中断フォームに直面したときにトリガーされます。

- **24** 時間以上 -アラート内の役立つトラブルシューティングのヒントを使用するか、クイックガイドの [データエクスポートの概要**]** タブを活用して、迅速に正常なデータフローに戻るための重要な時間です。
- **7** 日以上 -Kakfa の保持ポリシーは、お客様のトピックごとに 7 日間となっています。つまり、セキュリティ対策の対象となっているデータの一部が期限切れになっている可能性があります。SIEM へのデータフローを元に戻すには、トラブルシューティングツールを使用することが不可欠です。
- **30** 日以上 -つまり、お客様はセキュリティを重視するデータに悩まされており、Citrix Analytics から SIEM 環境へのデータフローの復元に早急に対応する必要があるということです。

詳細については、「SIEM メールアラート生成」を参照してください。

2023 年 **4** 月 **13** 日

修正された問題

Windows Citrix Workspace アプリは、バージョン 2203 以降の Citrix Workspace アプリから空のファイル名、パス、およびフォーマットのプロパティを送信します。その結果、Citrix Analytics for Security GUI では、「ダウ

ンロードファイル名」、「ダウンロードファイルパス」、「ダウンロードファイル形式」列の NA 値が表示されます。この問題は現在修正されています。[CAS-73498]

2023 年 **3** 月 **31** 日

Citrix Analytics for Security のセッション記録イベント

Citrix Apps and Desktops では、セッション記録に基づくイベントの識別と評価に役立つ 2 つの新しいイベントタイプが追加されました。

- Citrix.EventMonitor.RDPConnection
- Citrix.EventMonitor.UserAccountModification

管理者は潜在的なセキュリティリスクを簡単に特定して評価できるようになりました。これらのイベントを使用して、プロセス ID、宛先 IP アドレス、ユーザーアカウント操作の説明などの重要なデータに関する情報を収集できます。さらに、**** これらのイベントはカスタムリスク指標ページとセルフサービス検索ページにも表示されます **** 。

- セルフサービス検索: これらのイベントとその属性の詳細を表示できます。
- カスタムリスク指標: これらのイベントタイプを使用して任意のカスタム指標を設定できます。
  詳細については、「イベントタイプとサポートされているフィールド」を参照してください。

セルフサービス検索のアプリ保護イベント

Citrix Apps and Desktops データソースで保護されたセッション中にスクリーンショットをキャプチャしようとすると、**AppProtection.ScreenCapture** という新しいイベントがトリガーされます。**AppProtection.ScreenCapture****** イベントは、セルフサービス検索ページとデータエクスポートページでも確認できます。**

- セルフサービス検索: **AppProtection.ScreenCapture** の結果とそのすべての属性の詳細を表示できます。
- データエクスポート: **AppProtection.ScreenCapture** イベントタイプは、データエクスポートセクションで確認できます。[設定**] > [**データエクスポート**] > [**設定**] > [**エクスポート用データイベント] に移動し、[データソースイベント (オプション)] カテゴリから [アプリとデスクトップ] を選択します。

Session.Logon イベントのアプリ保護ポリシーという新しい属性も表示できます。

詳細については、「イベントタイプとサポートされているフィールド」を参照してください。

2023 年 **3** 月 **30** 日

カスタムロールのサポート

管理者は、Active Directory または Azure AActive Directory Directory のグループを使用するか、Citrix Analytics for Security の Okta インテグレーションをセットアップすることで、カスタムロールに追加できます。この統合に

より、すべてのグループ管理者のサービスアクセス権限を効率的に管理できます。

管理者を Active Directory または Azure Active Directory に正常に追加すると、管理者はグループを作成し、特定のグループにカスタムロールを割り当てることができます。管理者が両方のメンバーである場合は、個々の権限がグループ権限よりも優先されます。

詳細については、「カスタムロールのサポート」を参照してください。

SIEM UI のトラブルシューティングパネル

データエクスポートの UI は、以下の変更により強化されました。

- **[サマリ]** タブ:[サマリ] タブには、次のシナリオにおける SIEM イベントの指標、データソースのオンボーディングステータス、およびデータ消費ステータスが表示されます。
  - **Citrix Analytics** で利用可能なデータ: さまざまなデータソースのオンボーディングステータスが表示されます。
  - **SIEM** を利用できるイベント:SIEM 環境に送信されるインサイトの数が表示されます。
  - **SIEM** によるデータ消費量: データ消費状況が表示されます。
- 設定タブ: 設定タブには、アカウント設定、SIEM 環境設定、データイベントの選択に関する情報が含まれています。
- データエクスポートクイックガイド: 管理者はクイックガイドを利用できるようになりました。これにより、SIEM 統合の設定と保守がより簡単になります。「データエクスポートクイックガイド」リンクには、「概要」タブと「構成」タブの両方からアクセスできます。

詳細については、「データエクスポートのトラブルシューティング」を参照してください。

2023 年 **3** 月 **24** 日

ユーザープロフィールビューの変更

アプリケーション、ロケーション、デバイス、および ShareFile のデータ使用量に関連するユーザーのプロファイルデータは、ユーザーのタイムラインのユーザー情報ページには表示されません。Active Directory から取得された次のユーザー情報は引き続き利用できます-

- ジョブタイトル
- アドレス
- メール
- 電話
- 位置情報
- 組織

SIEM にエクスポートされるユーザープロファイルデータには変更はありません。詳細については、「ユーザープロファイル」を参照してください。

すべての検索ビューからの動的自動候補の削除

テナントの履歴データに基づくディメンションの自動提案機能は、次のページでは廃止されました。

- セルフサービス検索
- カスタムリスク指標

ただし、** イベントタイプやクリップボード操作などのディメンションの静的候補は引き続き検索ボックスに表示されます ** 。

詳細については、「セルフサービス検索の使用方法」を参照してください。

2023 年 3 月 21 日

オンプレミス **StoreFront** データソースの導入に役立つ推奨パネル

** データソースページに新しいレコメンデーションパネルが導入されました。** データソースページの推奨パネルでは ** 、オンプレミスの StoreFront データソースをオンボーディングすることの重要性をユーザーに伝えます。これにより、ユーザーはオンプレミスの StoreFront データソースを簡単にオンボーディングできます。また、利用可能なすべてのデータソースを確認してオンボーディングを確認するオプションも提供されます。

詳しくは、「StoreFront デプロイへの接続」を参照してください。

2023 年 2 月 23 日

解決された問題

Citrix Apps and Desktop のバージョンが 1912 より前のオンプレミスの Citrix Apps および Desktop 展開では、アクションが失敗しています。この問題は、手動アクションとポリシーベースアクションの両方で発生しています。この問題は現在修正されています。[CAS-69098]

[アプリとデスクトップのセルフサービス検索] ページには、仮想アプリケーションが 1 回だけ起動されると、複数のアプリ開始イベントとアプリ終了イベントが表示されます。この問題は、Linux 向け Citrix Workspace アプリのクライアントバージョンで発生します。この問題は現在修正されています。[CAS-36236]

2022 年 4 月 4 日以降から 2022 年 5 月末までのセキュアプライベートアクセスサービスのユーザーイベントは、Citrix Analytics テナントでは利用できない場合があります。この問題は現在修正されています。[CAS-66897]

2023 年 2 月 22 日

毎週のメール通知の強化

Citrix Analytics では、組織のセキュリティリスクを要約するのに役立つ電子メール通知を毎週送信します。毎週のメール通知が次の更新により改善されました。

- ユーザーのリスク分布 (検出されたユーザーの総数、リスクのあるユーザー、リスクのあるユーザー、およびリスクのないユーザー) を 1 週間で表示します。
- 1 週間に処理されたイベントの総数
- 1 週間でトリガーされた指標の合計数
- 1 週間に実行されたアクションの合計数
- データ処理が有効になっているデータソースの合計数

詳細については、「毎週のメール通知」を参照してください。

App.Saas.File.Download イベントタイプに「ダウンロードファイル形式」フィールドを追加しました

アプリとデスクトップのデータソースのセルフサービス検索ページに、app.Saas.File.Download イベントタイプ用の新しいダウンロードファイル形式のフィールドが追加されました。この変更により、**Download File Format** フィールドのカスタムリスク指標を設定できるようになりました。また、このフィールドを CSV 形式にエクスポートすることもできます。

詳しくは、「アプリとデスクトップのセルフサービス検索」を参照してください。

ブラウザから派生したフィールドの変更

以前は、セルフサービス検索ページには、ブラウザの名前とバージョンを表す **[**ブラウザ**]**、**[**ブラウザのメジャーバージョン**]**、**[**ブラウザのマイナーバージョン] の各フィールドがありました。ただし、明確さと正確さを確保するために、セルフサービス検索、カスタム指標テンプレート、アプリとデスクトップのデータソースの CSV ダウンロードでは、これら 3 つのフィールドは廃止され、**** ブラウザ名とブラウザバージョンに置き換えられました ** 。

詳しくは、「アプリとデスクトップのセルフサービス検索」を参照してください。

2023 年 2 月 16 日

修正された問題

一部の EU および APS のお客様では、テナントのユーザー名マスキングステータスを取得する際に、毎週のメールが影響を受けます。その結果、例外が発生したため、管理者は毎週 10 通の同一のメールを受信しています。例外が発生すると、後続のテナントには毎週のメールが届きませんでした。この問題は修正されました。[CAS-76138]

2023 年 2 月 3 日

欧州連合（**EU**）およびアジア太平洋南部地域で利用可能な **Citrix Secure Private Access**・サービスの分析サポート

Citrix Analytics for Security は、欧州連合地域およびアジア太平洋南部地域で利用可能な Citrix Secure Private Access からのユーザーイベントを処理するようになりました。組織が欧州連合地域またはアジア太平洋南部地域から Citrix Cloud にオンボーディングしている場合は、Secure Private Access サービスを使用しているユーザーのリスクインサイトを表示できます。

詳細については、「データソース」を参照してください。

2023 年 1 月 11 日

Secure Private Access からの **Web** フィルタリング機能の削除

Web フィルタリング機能は、Secure Private Access カテゴリから削除されました。Secure Private Access によるカテゴリベースの Web フィルタリングの廃止により、Citrix Analytics for Security の以下の機能が影響を受けます。

1. カテゴリグループ、カテゴリ、URL のレピュテーションなどのデータフィールドは、Citrix Analytics for Security ダッシュボードでは使用できなくなりました。
2. 同じデータに依存する危険な Web サイトアクセスインジケーターも廃止され、お客様には表示されなくなりました。
3. データフィールド (カテゴリグループ、カテゴリ、URL のレピュテーション) とそれに関連するポリシーを使用する既存のカスタムリスク指標はトリガーされなくなりました。
4. [ユーザーアクセス] タブと [アプリアクセス] タブ。
5. SIEM エクスポートには、しばらくの間 urlcategory、urlcategorygroup、urlcategoryGroup、urlcategoryReputation の各属性が次のダミー値とともに表示され続けます。
    - カテゴリとカテゴリグループの場合は 99999
    - 0 (評判)

詳細については、「Secure Private Access のセルフサービス検索」を参照してください。

2022 年 12 月 27 日

セルフサービス検索のデータソースドロップダウンの変更

データソースリストは、セルフサービス検索ページのアプリとデスクトップではなく、デフォルトでセッションを反映するように変更されています。また、パフォーマンスデータソースが表示されなかったため、パフォーマンスセク

ションが一番上に移動し、次にセキュリティセクションが続きます。

詳細については、「セルフサービス検索」を参照してください。

2022 年 12 月 13 日

ユーザーダッシュボードの強化

ユーザーダッシュボードが刷新され、管理者が組織のセキュリティ体制を監視しやすくなるように、概要とグラフが追加されました。このビューには、検出されたユーザー、トリガーされたリスク指標、適用されたアクションの詳細が表示されるだけでなく、重要な指標の時間ベースの傾向線も表示されるため、リスクをより適切に評価できます。管理者は関心のあるデータを掘り下げて適切なコンテキストの関連ダッシュボードに移動できるため、リスク分析を迅速に行うことができます。

詳細については、「ユーザーダッシュボード」を参照してください。

2022 年 12 月 5 日

アクセス保証ダッシュボード-ログオンネットワーク

ログオンネットワークセクションが新しく追加され、以下のユーザー情報が表示されます。

- ユーザーがログオンした IP アドレスに関連する組織。
- ユーザーがログオンしたユニークパブリックサブネットとプライベートサブネットの合計。
- ユーザーがプロキシとプライベート VPN サービスを使用してログオンした詳細。

これらの追加情報を使用して、管理者はユーザーログオンの詳細を検証し、ユーザーログオンが組織のセキュリティ要件の範囲内であることを確認できます。

詳細については、「アクセス保証ダッシュボード」を参照してください。

2022 年 11 月 18 日

修正された問題

- ソースイベントなしで誤ってトリガーされたジオフェンスインジケーターが修正されました。[CAS-73222]

2022 年 11 月 8 日

アクションの名前を変更

Citrix Analytics for Security で使用されるアクションの一部は、わかりやすいように名前が変更されています。それらのアクションは以下のとおりです。

- 管理者に通知 -管理者に通知
- ユーザーをロック -ユーザーアカウントをロック
- ユーザーをログオフ -アクティブなセッションをログオフする
- ユーザーのロック解除 -ユーザーアカウントのロック解除
- ユーザーを無効化 -ユーザーアカウントを無効にする

詳細については、「アクションとは」を参照してください。

解決された問題

- タイムラインのアクションドロップダウンからオプションを選択すると、「クリア」ボタンと「適用」ボタンが表示されないため、手動アクションはトリガーできません。この状態は最新の Firefox バージョンで発生します。この問題は現在修正されています。[CAS-72051]
- ****App and Desktops** データソースのセルフサービス検索の **[**ダウンロードデバイスタイプ**]** フィールドでは、****** ハードドライブ、ハードドライブ、および ****HDD** の各カテゴリが 1 つのカテゴリにまとめられ、ハードディスクドライブとしてまとめられます。** [CAS-67188]
- Microsoft Graph から同じアラート ID の通知が重複して受信され、そのためにリスクイベントが重複して作成されることがあります。この問題を防ぐため、アプリケーションには重複排除メカニズムが実装されています。[CAS-66731]

2022 年 10 月 19 日

日付ソースイベントの選択とエクスポート

新しいデータイベントエクスポートワークフローを活用して、機械学習によって生成されたリスクインサイトイベントと関連データに加えて、データソースイベントをエクスポートできるようになりました。

これにより、セキュリティおよびセキュリティオペレーション (SOC) 管理者は次のことが可能になります。

- Citrix Analytics のデータを、セキュリティ情報およびイベント管理（SIEM）で集約された他のデータソースイベントと関連付ける
- どのデータイベントが SIEM に流れるかを制御してストレージコストを最適化する

データイベントは、既存の SIEM インテグレーションとデータコネクタに配信され、セルフサービスのイベント検索ビューに表示されるものと同等に配信されます。

詳しくは、「Citrix Analytics for Security から SIEM サービスにエクスポートされるデータイベント」を参照してください。

2022 年 10 月 18 日

管理者が **Citrix DaaS** サイトで動的セッション記録アクションを実行できるようにする

管理者は、Citrix DaaS サイトで動的セッション記録アクションを実行したり、ユーザーの仮想セッションを動的に記録したりできるようになりました。特定のユーザーによる危険なアクティビティが Citrix Analytics for Security によって検出された場合に、ユーザーセッションの記録を自動的に開始するポリシーを使用してアクションを構成できます。

詳細については、「アクションとは」を参照してください。

2022 年 10 月 14 日

ユーザーリスク指標へのフィードバックを提供する

Citrix Analytics for Security 管理者は、指標の詳細パネルでフィードバックを提供することで、ユーザーのリスク指標を有用または役に立たないものとして報告できるようになりました。この機能により、管理者は誤検知を報告したり、頻繁にトリガーされるインジケーターのノイズを減らしたり、他の管理者と追加のコンテキストを共有したりできます。さらに、役に立たないリスク指標がユーザーのタイムラインから隠され、ユーザーのリスクスコアが再調整されます。

詳細については、「ユーザーリスク指標へのフィードバックの提供」を参照してください。

2022 年 9 月 26 日

ジオフェンスブロックリストをサポートするアクセス保証

ジオフェンス設定の下に [安全な場所] タブと [危険な場所] タブが追加されました。

- 安全なロケーションジオフェンシングは、ジオフェンスされたエリア外へのアクセスを識別して制限するのに役立ちます。
- 危険なロケーションジオフェンシングは、組織の既知の行動に基づいて危険なユーザーアクセスを検出して絞り込むのに役立ちます。

安全なジオフェンシングと危険なジオフェンシングはどちらも、独自の事前設定されたカスタムリスク指標によって支えられています。

詳細については、「ジオフェンシングを有効にする」を参照してください。

解決された問題

- 電子メール本文に顧客名を表示するための **Citrix** Cloud API。これで、メールはニックネームを使用して、管理者に送信されるメール本文に顧客名を表示するようになりました。[CAS-65350]
- NetScaler Gateway データソースカードは、**Citrix Analytics for Security** と **CitrixAnalytics for Performance** データ処理は、Citrix Analytics for Security エンドポイントを絶えず呼び出していましたが、**Citrix Analytics for Performance** の資格しか持たない顧客では正常に動作しませんでした。[CAS-70817]
- Citrix Cloud から複数の資格メッセージを同時に受信すると、Redis Cache の更新中に競合状態が発生します。このようなシナリオでは、1 つのエンタイトルメントメッセージがキャッシュに更新され、残りは失われます。この問題は修正され、キャッシュ内のすべてのエンタイトルメントメッセージが更新されるようになりました。[CAS-70823]

2022 年 **9** 月 **13** 日

シェアリンクダッシュボードの強化

Sharelink ダッシュボードが改良され、概要と詳細ビューが追加されました。概要ビューは、上位のアクティブな共有と上位リスクの高い共有で構成されます。詳細ビューでは、作成者、アクティビティ数、認証タイプ、権限、共有タイプ、コンテンツなどの詳細情報が管理者に表示されます。管理者は必要に応じてドリルダウンしてさらに絞り込み、時間枠を変更/提供して関心のあるデータを表示できます。

詳細については、「共有リンク」ダッシュボードを参照してください。

2022 年 **9** 月 **9** 日

インポッシブルトラベル **RI** 強化

インポッシブル・トラベル・リスク指標が拡張され、クライアントの IP アドレスの登録組織とルーティング・タイプを報告できるようになりました。これらの新しいフィールドは、ユーザータイムラインのインジケーター詳細ビューと SIEM に送信されたインジケーター詳細の両方で使用できます。

デフォルトポリシーの詳細については、次の記事を参照してください。

- 継続的なリスク評価。
- ポリシーとアクション

2022 年 8 月 19 日

VDA Print テレメトリを有効にする

Citrix Apps and Desktops で印刷ジョブが開始されると、VDA.Print というイベントがトリガーされます。VDA Print イベントは、セルフサービス検索ページとカスタムリスク指標ページでも確認できます。

- セルフサービス検索：VDA.print の結果とそのすべての属性の詳細を表示できます。
- カスタムリスク指標：VDA 印刷テレメトリ用の新しいイベントが EventHub 経由で提供され、カスタム指標でも利用できます。これらのイベントキーと値のペアを使用して、カスタムインディケータートリガーを設定できます。

印刷テレメトリを有効にし、Citrix Analytics for Security に印刷ログを送信できるようにするには、レジストリキーを作成して VDA を構成する必要があります。これらの印刷ログには、プリンタ名、印刷ファイル名、印刷部数など、印刷処理に関する重要な情報が含まれます。セキュリティ管理者は、これらのログを使用してリスクを分析し、ユーザーを調査できます。

詳しくは、「Citrix DaaS 印刷テレメトリーの有効化」を参照してください。

2022 年 8 月 18 日

修正された問題

- アプリとデスクトップのセルフサービス検索とアクセス保証ロケーションダッシュボードの「ユーザーログオン」ページでは、ダウンロードした CSV ファイルに Workspace アプリのバージョン値が **NA**（使用不可）として入力されていましたが、ページビューでは表示されていました。この問題は修正されました。[CAS-70361]

2022 年 8 月 17 日

ポリシーごとにエンドユーザーの **E** メールをカスタマイズ

エンドユーザーに送信されるメールの内容をポリシーごとにカスタマイズできるようになりました。具体的には、「エンドユーザー応答のリクエスト」アクション、またはユーザーのアカウントに対する破壊的なアクション（「ユーザーのログオフ」や「ユーザーのロック」など）を使用してポリシーを作成する場合、ポリシーの適用時にエンドユーザーに送信される電子メールコンテンツはカスタマイズ可能です。

ポリシーごとにエンドユーザメールをカスタマイズする方法の詳細については、「ポリシーとアクション」を参照してください。

2022 年 8 月 11 日

アクセス保証-ジオロケーションに関する新しい質問が **FAQ** の記事に追加されました。詳細については、FAQを参照してください。

修正された問題

- [すべての通知を表示] ボタンにより、管理者はタイプミスのある毎週のhttps://citrix.cloud.com/notifications電子メールリンクにリダイレクトされました。[CAS-69236]

2022 年 6 月 17 日

データ処理は、新しい有料資格に対してデフォルトで有効になっています

以前は、Citrix Analytics for Security の新しい有料資格を持つ顧客は、特定のデータソースのサイトカードで [データ処理] をオンにして、それらのデータソースのデータ処理を開始する必要がありました。

今回のリリースでは、Citrix Analytics for Security の新しい有料資格がプロビジョニングされると、以下の Citrix Cloud サービスのデータ処理がデフォルトでオンになります。

- Citrix Secure Private Access
- Citrix Content Collaboration
- Citrix DaaS

詳しくは、「はじめに」を参照してください。

2022 年 6 月 9 日

修正された問題

- Azure AD ID 保護および Microsoft Defender for Endpoint によって生成された Microsoft Graph リスク指標は、セキュリティ分析で複数回表示される場合があります。この問題は修正されました。[CAS-66593,CAS-66731]

2022 年 6 月 2 日

解決された問題

- ポリシーのセルフサービス検索で、イベントをフィルタリングするために検索クエリで **Policy-Name** ディメンションを選択すると、Security Analytics の有効なポリシーとともに無効なポリシーのリストが提案されました。[CAS-66838]

- Windows Citrix **Receiver** からの **File.Download** イベントのダウンロードファイルサイズがセルフサービス検索で正しく表示されない。この問題は、実際の値が KB 単位であり、UI が値をバイトとして扱い、誤った値がユーザーに表示されたために発生しました。[CAS-67105]

2022 年 **5** 月 **24** 日

Content Collaboration、**Citrix DaaS**、**Citrix Virtual Apps and Desktops**、**Gateway** データソースに関する不可能な移動リスク指標の紹介

ユーザーが離れすぎて経過時間内に移動できない 2 つの場所からログオンした場合、Citrix Analytics はこのアクティビティを不可能な移動シナリオとして検出し、不可能な移動リスク指標をトリガーします。インポッシブル・トラベル・リスク指標の詳細については、次の記事を参照してください。

- Citrix Content Collaboration のリスク指標
- NetScaler Gateway リスク指標
- Citrix Virtual Apps and Desktops および Citrix DaaS リスク指標

2022 年 **5** 月 **17** 日

Virtual Apps and Desktops] の名前が **[**アプリとデスクトップ**]** に変更されました

Security Analytics のダッシュボードとレポート、および Security Analytics から SIEM サービスに送信されるデータで、すべての [Virtual Apps and Desktops] ラベルが [アプリとデスクトップ] として更新され、ブランド名が変更された製品名に合わせられるようになりました。

たとえば、[データソース] ページでは、[Virtual Apps and Desktops] ラベルの名前が [アプリとデスクトップ] に変更されます。

[アプリとデスクトップ] ラベルは、組織内の Citrix オンプレミスの Citrix Virtual Apps and Desktops 、および Citrix DaaS （以前の Citrix Virtual Apps and Desktops サービス）の両方を表します。

解決された問題

Citrix Analytics は、Citrix Cloud アカウントに関連付けられている Citrix DaaS クラウドモニターまたは Director サイトを自動的に検出しません。[CAS-66801]

2022 年 4 月 5 日

新機能

「Secure Workspace Access」が「Secure Private Access」に改名

Analytics ダッシュボードとレポートで、すべての **Secure Workspace Access** ラベルが、ブランド変更された製品名に合わせて **Secure Private Access** として更新されるようになりました。

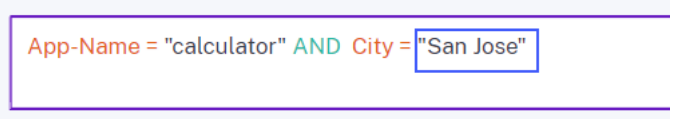
たとえば、[データソース] ページと [セルフサービス検索] ページでは、**[Secure Workspace Access]** ラベルの名前が [**Secure Private Access**] に変更されます。

2022 年 3 月 21 日

修正された問題

- **[**リスク指標の作成] ページで、検索クエリの前の条件にスペースで区切られたディメンション値が含まれている場合、ディメンションと演算子の自動候補は機能しません。

  たとえば、次のクエリでは、都市を`San Jose`として選択すると、自動候補が機能しなくなります。この問題は修正されました。[CAS-64126]

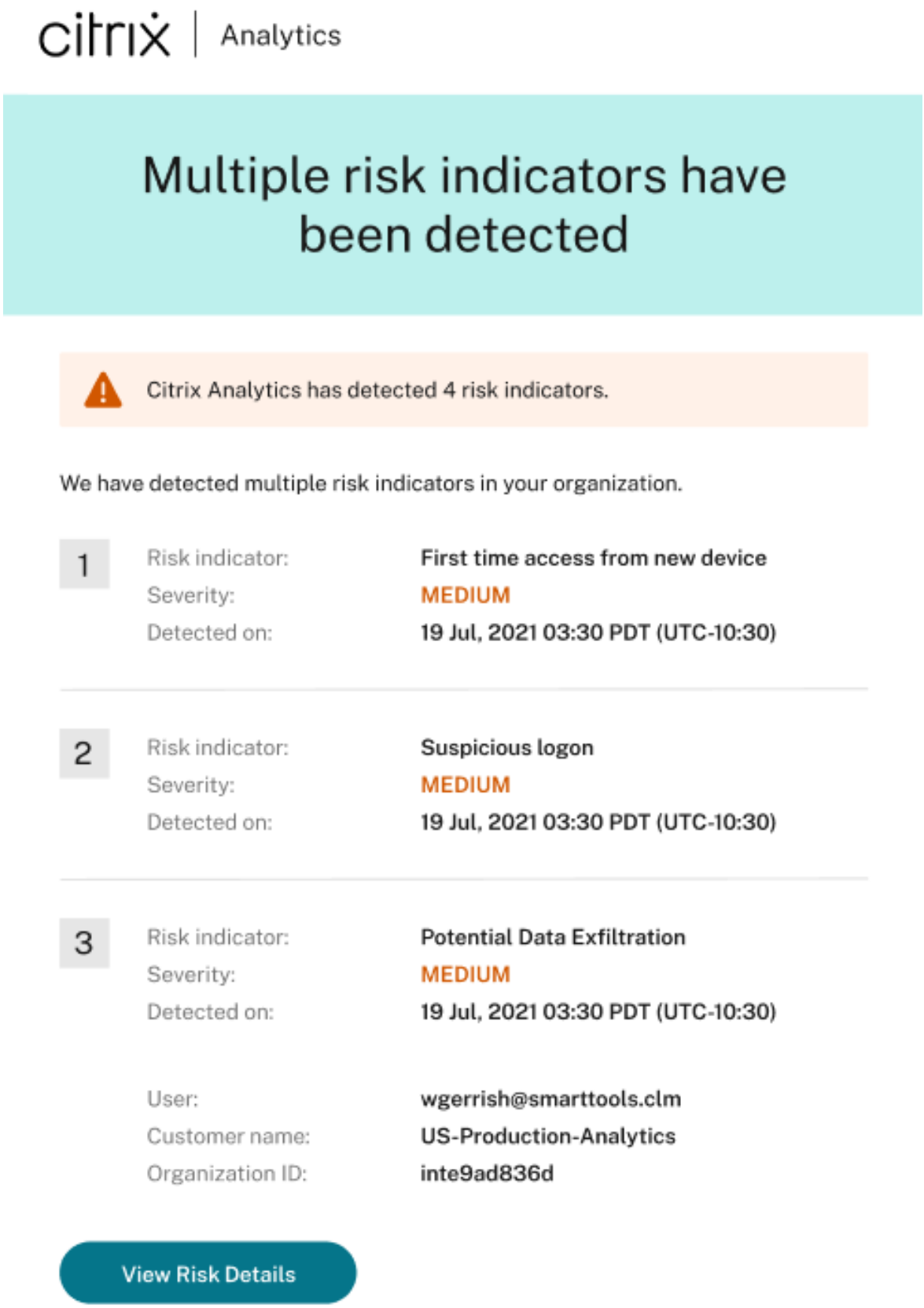
  

2022 年 3 月 10 日

新機能

管理者への通知メールの機能拡張

- [管理者に通知] アクションの電子メール通知で、トリガーされたポリシーに関連付けられた複数のリスク指標の詳細が提供されるようになりました。
- ポリシーに関連付けられている各リスク指標の名前、重大度、およびトリガー日を表示できます。
- [リスクの詳細の表示] をクリックすると、Citrix Analytics でユーザータイムラインページが開き、ポリシーをトリガーした最新のリスク指標が表示されます。ユーザータイムラインページでは、ユーザーに対してトリガーされたすべてのリスク指標を表示することもできます。



「管理者に通知」操作について詳しくは、「ポリシーと操作」を参照してください。

修正された問題

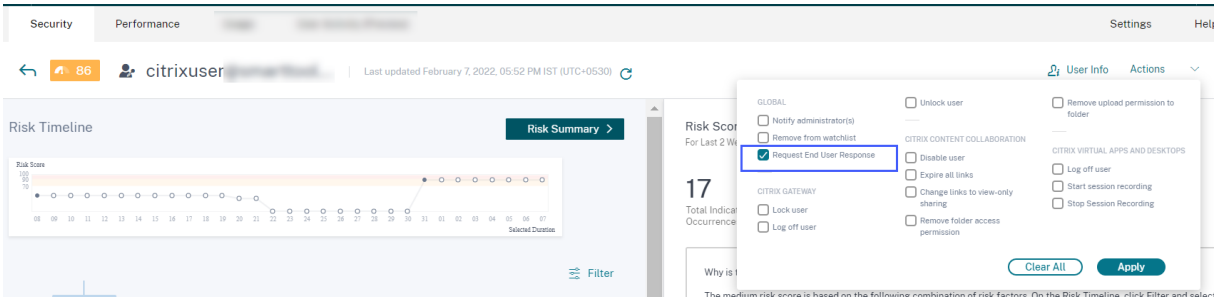
Citrix Analytics が、Secure Workspace Access データソースからユーザーイベントを受信できません。そのため、対応するセルフサービス検索ページにはユーザーイベントは表示されません。また、Secure Workspace Access データソースのカスタムリスク指標を作成することもできません。[CAS-64619]

2022 年 3 月 3 日

新機能

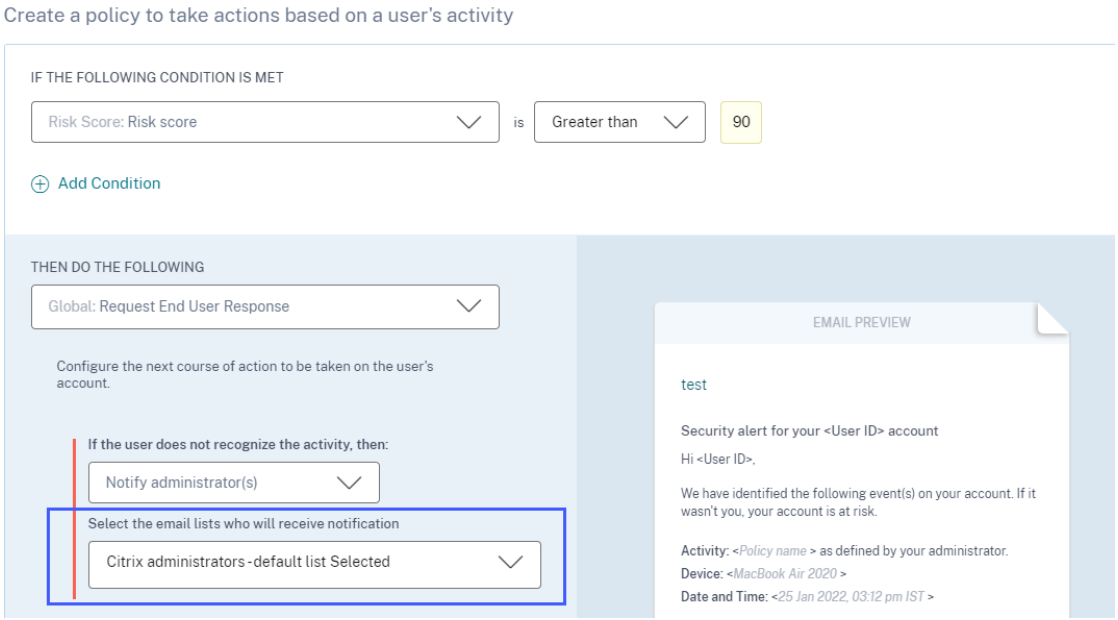
エンドユーザー応答のリクエストを手動で適用する　以前は、ポリシーを作成することによってのみ、ユーザーアカウントに「エンドユーザーレスポンスを要求」アクションを適用できました。
今回のリリースでは、ユーザータイムラインの [アクション] リストからアクションを選択し、このアクションをリスク指標に手動で適用できます。

アクションの詳細と、アクションを手動で適用する方法については、「ポリシーとアクション」を参照してください。

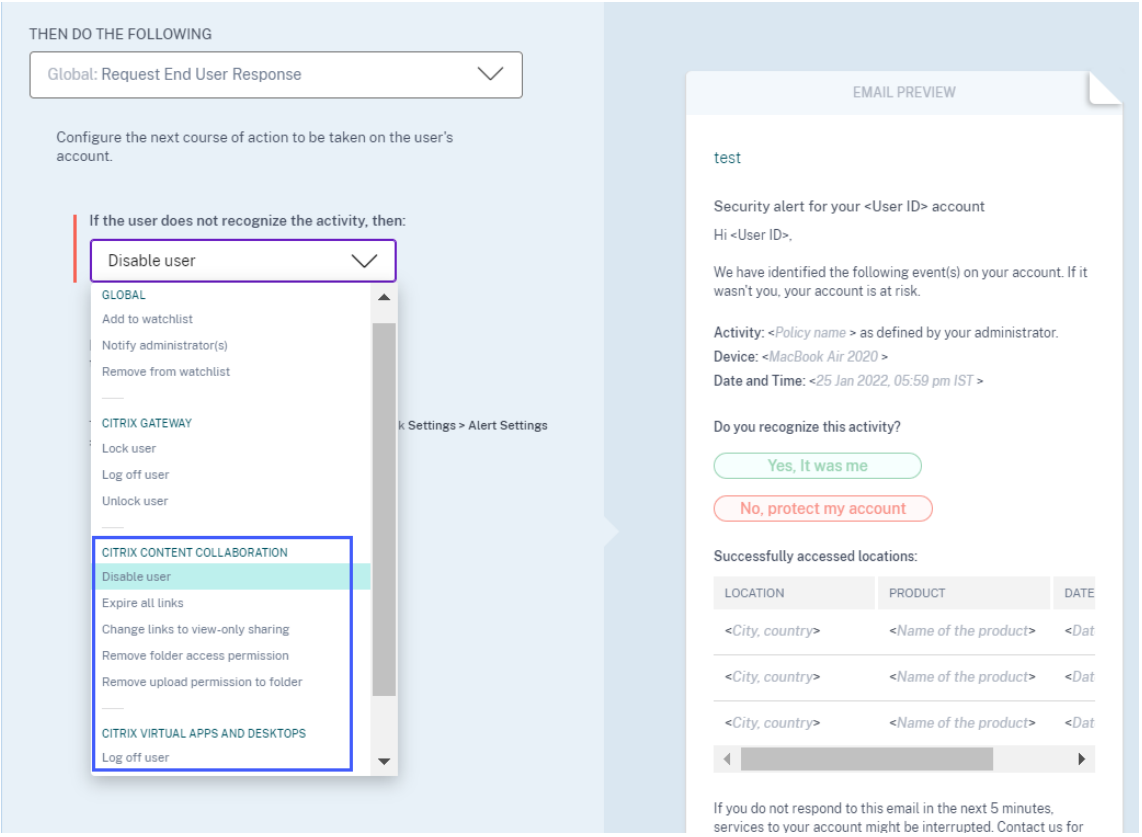


ポリシーに対するエンドユーザー応答の拡張をリクエストする　「エンドユーザーレスポンスのリクエスト」アクションを使用してポリシーを作成すると、次の拡張機能が表示されます。

- 次のアクションとして [管理者に通知] を選択すると、既定の電子メール配布リストと、選択した電子メール配布リストが表示されます。



- これで、次のアクションとして、「Citrix Content Collaboration」または「Citrix Virtual Apps and Desktops」と「Citrix DaaS」のいずれかのアクションを選択できます。以前は、グローバルアクションまたは NetScaler Gateway アクションのうち 1 つしか選択できませんでした。



アクションの詳細については、「ポリシーとアクション」を参照してください。

2022 年 **2** 月 **23** 日

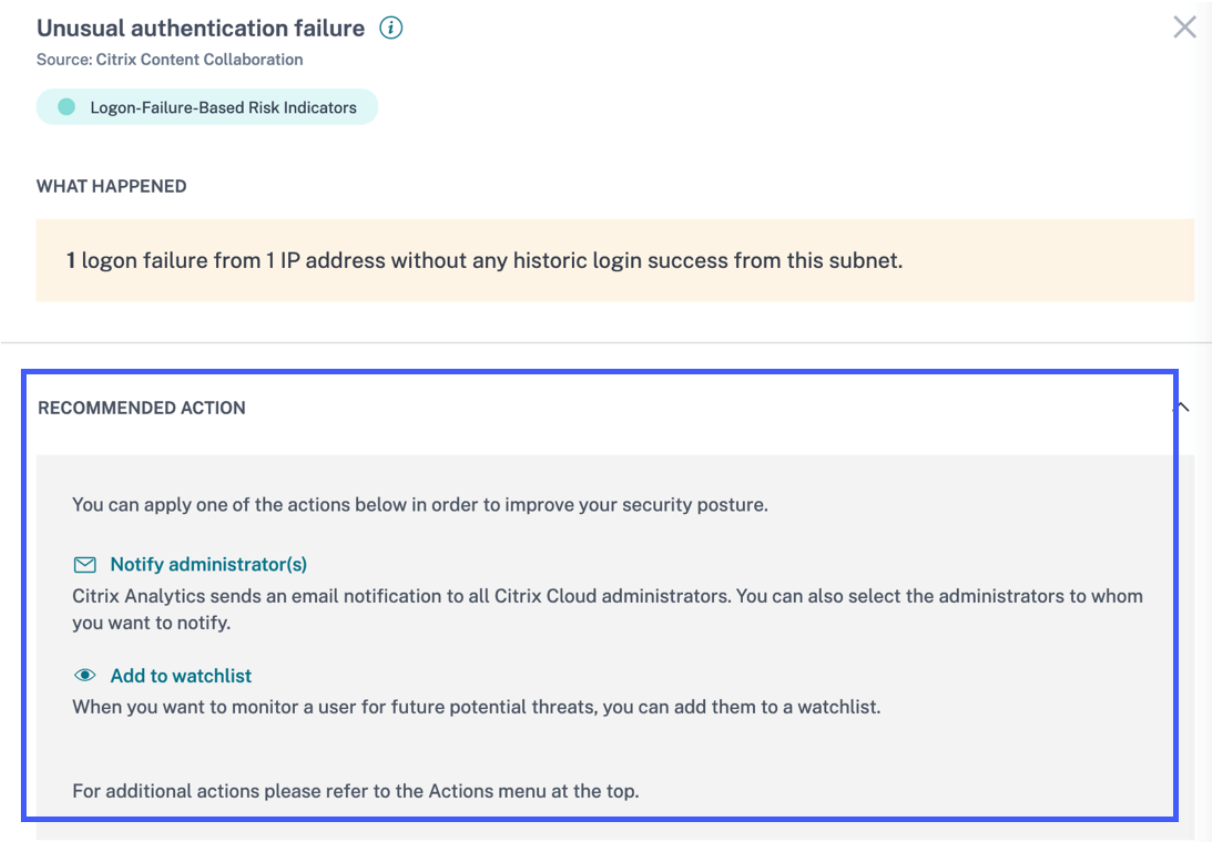
新機能

リスク指標に推奨されるアクション　Citrix Analytics では、ユーザーに対して次のリスク指標がトリガーされたときに、**[**** 管理者に通知**]**、[ウォッチリストに追加]、**[**** ポリシーの作成] などのアクションを適用することをお勧めします。

- 異常な認証エラー (Content Collaboration データソース)
- 異常な認証失敗 (Gateway データソース)
- 不審なログオン (Citrix Virtual Apps and Desktops、Citrix DaaS データソース)

ユーザータイムラインに移動してリスク指標を選択すると、[推奨アクション] セクションで推奨されるアクションをすべて表示できます。

たとえば、異常な認証失敗リスク指標では、次の推奨アクションを表示できます。



この機能は、ユーザーがもたらすリスクの重大度に応じて実行できるアクションを選択するためのガイダンスを提供します。ただし、リスク分析によっては、推奨リストに含まれない適切なアクションを実行することもできます。

修正された問題

- 組織がアジア太平洋地域の **Citrix** Cloud にオンボーディングされている場合、Citrix Analytics が認証データソースからユーザーイベントを受信しないことがあります。そのため、対応するセルフサービス検索ページにユーザーイベントが表示されないことがあります。この問題は修正されました。[CAS-62300]

2022 年 **2** 月 **17** 日

新機能

Citrix Virtual Apps and Desktops および **Citrix DaaS** データソースのデータ収集とレポート機能の向上　今回のリリースでは、次の変更点が見られます。

- Citrix Workspace アプリクライアントと Citrix Monitor サービスからのイベントのデータ収集、相関、およびレポート作成が改善されました。
- セルフサービス検索、カスタムリスク指標、および全体的なリスク検出に使用できる、ユーザーおよびクライアントバージョンから受信するイベントの品質が向上しました。

Content Collaboration のセッションイベントとアプリイベント用のコンテキストテンプレートのサポート　セルフサービス検索ページでは、ファイル、フォルダ、セッション、共有、およびユーザーイベントに関連付けられた関連フィールドのみの詳細を表示できるようになりました。イベントに該当しないフィールドは削除されます。

たとえば、次のような`File.Copy`イベントの詳細を表示できます。

- ファイル ID
- ファイルコピー ID
- [ファイルパス]
- デスティネーションファイルパス
- ストリーム ID
- ゾーン ID

これらの詳細は、リスクのある行動に関連するユーザーアカウントのリスク調査と分析を行う際に役立ちます。リスクが高いと思われるイベントの特定の属性にドリルダウンできます。

フィールドの詳細については、「Content Collaboration のセルフサービス検索」を参照してください。

2022 年 2 月 10 日

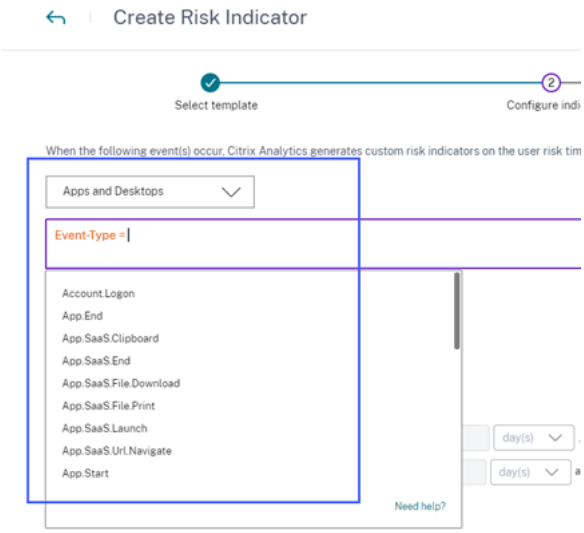
新機能

カスタムリスク指標のディメンションの自動推奨値　カスタムリスク指標ページで、条件バーでディメンションと有効な演算子を選択すると、ディメンションの値が自動的に表示されます。自動推奨リストから値を選択するか、ユースケースに応じて手動で値を入力します。値を入力すると、レコード内の一致する値が自動的に候補として表示されます。

ディメンションに推奨される値のリストは、データベースで事前定義されている (既知の値) か、履歴イベントに基づいています。

たとえば、ディメンションEvent-Typeと代入演算子を選択すると、既知の値が自動的に推奨されます。要件に応じて値を選択できます。

詳細については、「カスタムリスク指標」を参照してください。



2022 年 2 月 9 日

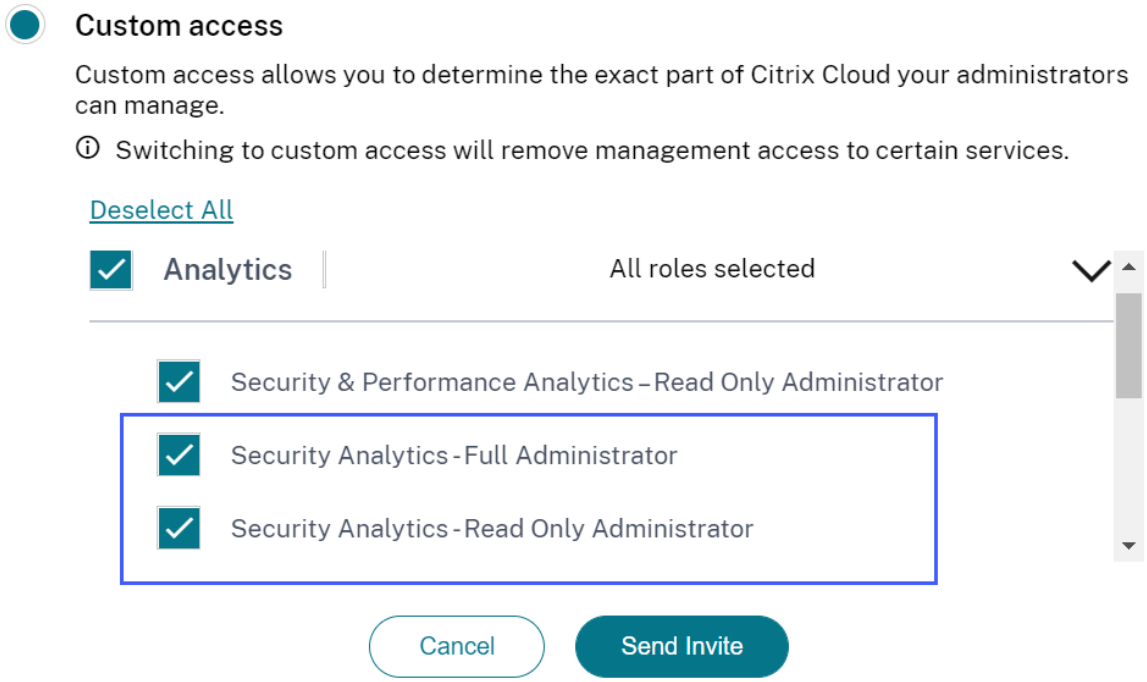
新機能

管理者用の新しいカスタムロール　フルアクセス権を持つ Citrix Cloud 管理者は、組織内のセキュリティ分析を管理するよう他の管理者を招待できます。招待された管理者に次のカスタムロールを割り当てることができるようになりました。

- セキュリティ分析-すべての管理者
- セキュリティ分析-読み取り専用管理者

カスタムロールを使用すると、管理者に読み取り専用またはフルアクセス権限を付与して、Security Analytics のさまざまな機能の管理を許可できます。

これらのカスタムロールのアクセス権限の詳細については、Security Analytics の管理者ロールの管理を参照してください。



カスタムアクセス管理者向けの電子メール通知のサポート　Citrix Cloud 管理者で、Security Analytics を管理するためのカスタムアクセス（読み取り専用またはフルアクセス）権限を持つ場合、次の通知が表示されるようになりました。

- 組織で検出されたセキュリティリスクについて毎週通知します。詳細については、「毎週の電子メール通知」を参照してください。
- [管理者に通知] アクションが手動で適用された場合や、ポリシーによってトリガーされた場合のリスク指標に関する通知。詳細については、「ポリシーとアクション」を参照してください。

2022 年 1 月 28 日

新機能

Content Collaboration と **Gateway** データソースに対する不審なログオンのリスク指標の導入　Citrix Analytics for Security は、次のような複数のコンテキスト要因に基づいて、本質的に疑わしいユーザーログオンを検出するようになりました。

- 場所は、ユーザーおよび組織履歴に関して通常とは違うと見なされます
- デバイスはユーザーおよび組織履歴に関して異常であるとみなされます

- ユーザーおよび組織の履歴に関して、ネットワークが異常と見なされる
- IP アドレスは、IP 脅威インテリジェンスフィードに基づいて疑わしいと見なされます。

これらの要因の組み合わせに基づいて疑わしいコンテキストからユーザーがログオンすると、リスク指標がトリガーされます。

このリスク指標は、Citrix Content Collaboration および NetScaler Gateway データソースに関連付けられている［通常とは異なる場所からのアクセス］リスク指標を置き換えます。[異常な場所からのアクセス] リスク指標に基づく既存のポリシーは、新しいリスク指標である [疑わしいログオン] に自動的にリンクされます。

リスク指標の詳細については、「疑わしいログオン-Content Collaboration」および「疑わしいログオン- ゲートウェイ」を参照してください。

リスク指標のスキーマについて詳しくは、SIEM 用の Citrix Analytics データ形式を参照してください。

2022 年 1 月 20 日

新機能

Microsoft Azure Active Directory 統合　Azure Active Directory をセキュリティ向け Citrix Analytics クスと接続して、次のことが可能になりました。

- 組織のドメインから Citrix Analytics for Security にユーザーの詳細とユーザーグループをインポートします。
- 役職、組織、オフィスの所在地、電子メール、連絡先情報などの追加情報でユーザープロファイルを強化し、リスク調査や分析の際に役立ちます。

詳細については、「Azure Active Directory との統合」を参照してください。

2022 年 1 月 18 日

新機能

すべての **Content Collaboration** リスク指標に対する共有リンクアクションのサポート　以前は、Content Collaboration サービスに関連付けられた次の共有リンクベースのリスク指標で、共有リンクアクション **([**すべてのリンクを期限切れにする**]** および **[**リンクを表示のみの共有に変更]) を適用できました。

- 匿名の機密共有リンクのダウンロード
- 共有リンクのダウンロードが多すぎる
- 過剰なファイル共有

このリリースでは、Content Collaboration サービスに関連付けられた次のユーザーベースのリスク指標に共有リンクアクションを適用できるようになりました。

- 通常の場所以外からのアクセス
- 機密ファイルへの過剰なアクセス
- 過剰なファイルのアップロード
- 過剰なファイルのダウンロード
- ファイルまたはフォルダの過剰な削除
- マルウェアファイルが検出されました
- ランサムウェアのアクティビティの疑い
- 異常な認証失敗

Content Collaboration サービスに関連付けられたカスタムリスク指標に共有リンクアクションを適用することもできます。

アクションとリスク指標の詳細については、次の記事を参照してください。

- ポリシーとアクション
- Content Collaboration のリスク指標
- カスタムリスク指標

SIEM との統合が一般提供される　Citrix Analytics for Security をセキュリティ情報およびイベント管理（SIEM）サービスと統合し、ユーザーのデータを Citrix IT 環境から SIEM にエクスポートできます。この統合により、さまざまなソースから収集されたデータを相互に関連付け、組織のセキュリティを全体的に把握できます。

現在、Citrix Analytics for Security を次のサービスと統合できます。

- Splunk
- Microsoft Sentinel
- Elasticsearch
- Kafka または Logstash ベースのデータコネクターを使用するその他の SIEM サービス

詳細については、「セキュリティ情報とイベント管理 (SIEM) の統合」を参照してください。

2021 年 **12** 月 **23** 日

新機能

共有リンクのリスク指標の拡張　次の機能強化が行われました。

- 匿名の機密共有リンクダウンロードリスク指標を使用してポリシーを作成できるようになりました。

- 匿名の機密共有ダウンロードリスク指標は、共有リンクのリスク指標と区別するために、匿名の機密共有リンクのダウンロードに名前が変更されました。
- 過剰ダウンロードリスク指標は、共有リンクのリスク指標と区別し、ユーザーベースの過剰なファイルダウンロードリスク指標と区別するために、「過剰な共有リンクのダウンロード」に名前が変更されました。

詳しくは、「Citrix 共有リンクのリスク指標」を参照してください。

2021 年 12 月 21 日

新機能

リスク指標に関する通知を **Citrix Cloud** 管理者以外に送信する　組織内の Citrix Cloud 管理者以外に、[管理者に通知] アクションを使用して通知できるようになりました。

これらの管理者に通知するには、電子メール配布リストを作成します。Citrix Cloud に接続されている外部ドメインから、または電子メールアドレスを直接使用して、電子メール配布リストで管理者を選択します。[管理者に通知] アクションを適用する場合は、**Citrix Cloud** 管理者以外の管理者が含まれるメール配布リストを選択します。

詳細については、「電子メール配布リスト」を参照してください。

2021 年 12 月 20 日

新機能

Content Collaboration ユーザにユーザ応答通知を送信する　Active Directory ユーザーに加えて、Content Collaboration ユーザーに [エンドユーザー応答の要求] アクションを適用できるようになりました。

この操作により、Citrix Analytics がユーザーの Citrix アカウントで異常なアクティビティを検出すると、ユーザーに電子メール通知が送信されます。「エンドユーザーレスポンスをリクエスト」アクションの詳細については、「ポリシーとアクション」を参照してください。

アクセス制御の名前が「**Secure Workspace Access**」に変更されました　**Security** Analytics ダッシュボードとレポートでは、すべてのアクセス制御ラベルが **Secure Workspace Access** として更新され、ブランド変更された製品名に合わせられるようになりました。

たとえば、[データソース] ページ、[セルフサービス検索] ページ、および [ポリシー] ページでは、[アクセス制御] ラベルの名前が [Secure Workspace Access] に変更されます。

修正された問題

- Apps and Desktops データソースの場合、検索レポートを CSV ファイルとしてダウンロードすると、CSV ファイル内の一部のフィールド値は、値は使用できますが、使用不可 (N/A) と表示されます。たとえば、

`Download File Name`、`Session Launch Type`、`Workspace App Version`などのフィールドの値は [セルフサービス検索] ページに表示されますが、ダウンロードされた CSV ファイルでは、これらの値は利用できません (N/A) と表示されます。この問題は修正されました。[CAS-62299]

2021 年 **12** 月 **9** 日

新機能

テンプレートを使用してカスタムリスク指標を簡単に作成　ユースケースに基づいてテンプレートを選択し、カスタムリスク指標を作成できるようになりました。テンプレートには、定義済みのクエリとパラメーターが用意されています。これにより、カスタムリスク指標を作成する際の作業が楽になります。

詳細については、「カスタムリスク指標」を参照してください。

2021 年 **12** 月 **7** 日

修正された問題

- Citrix Analytics for Security では、2021 年 9 月にリリースされた Citrix Secure Browser を使用しているユーザーのイベントは受信されません。この問題は、2021 年 9 月以降のリリースである Citrix Secure Browser でホスト名追跡ポリシーが表示されないため、Citrix Analytics for Security との統合を有効にできないためです。この問題は修正されました。[CAS-62254]

2021 年 **12** 月 **2** 日

新機能

マルウェアファイルが検出されたリスク指標　Content Collaboration でユーザが感染ファイルをアップロードしたときにアラートを受信できるようになりました。

リスク指標は、トロイの木馬、ウイルス、その他の悪意のある脅威などのマルウェアに感染しているファイルを検出します。これにより、ファイルの所有者、ウイルス名、ファイルの場所など、悪意のあるファイルの詳細を可視化できます。

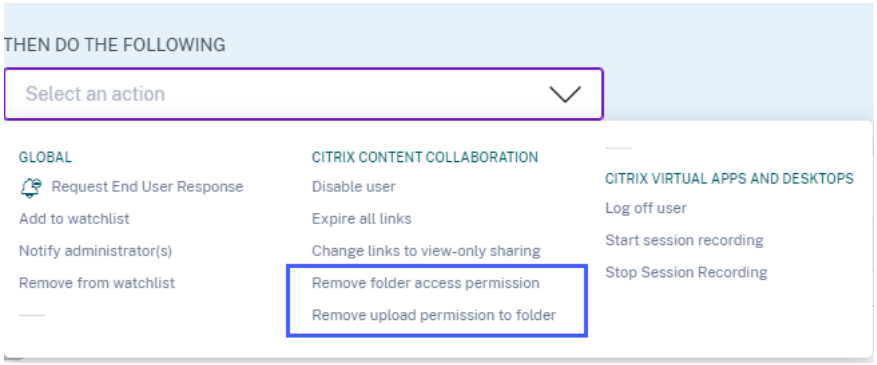
マルウェアファイルが検出されたリスク指標に関連するリスク要因は、ファイルベースのリスク指標です。

リスク指標と適用できるアクションの詳細については、「マルウェアファイルが検出されたリスク指標」を参照してください。

Content Collaboration データソースの新しいアクション　マルウェアファイルが検出されたリスク指標がユーザーに対してトリガーされると、次のアクションを適用できます。

- フォルダのアクセス権限を削除する。感染ファイルをアップロードしたユーザーのアクセス権をブロックできます。ユーザーは、感染ファイルがアップロードされたフォルダーにアクセスできません。
- フォルダへのアップロード権限を削除する。感染ファイルをアップロードしたユーザーのアップロード権限をブロックできます。ユーザーは、感染ファイルがアップロードされたフォルダーにファイルをアップロードできません。

Content Collaboration のアクションの詳細については、「ポリシーとアクション」を参照してください。

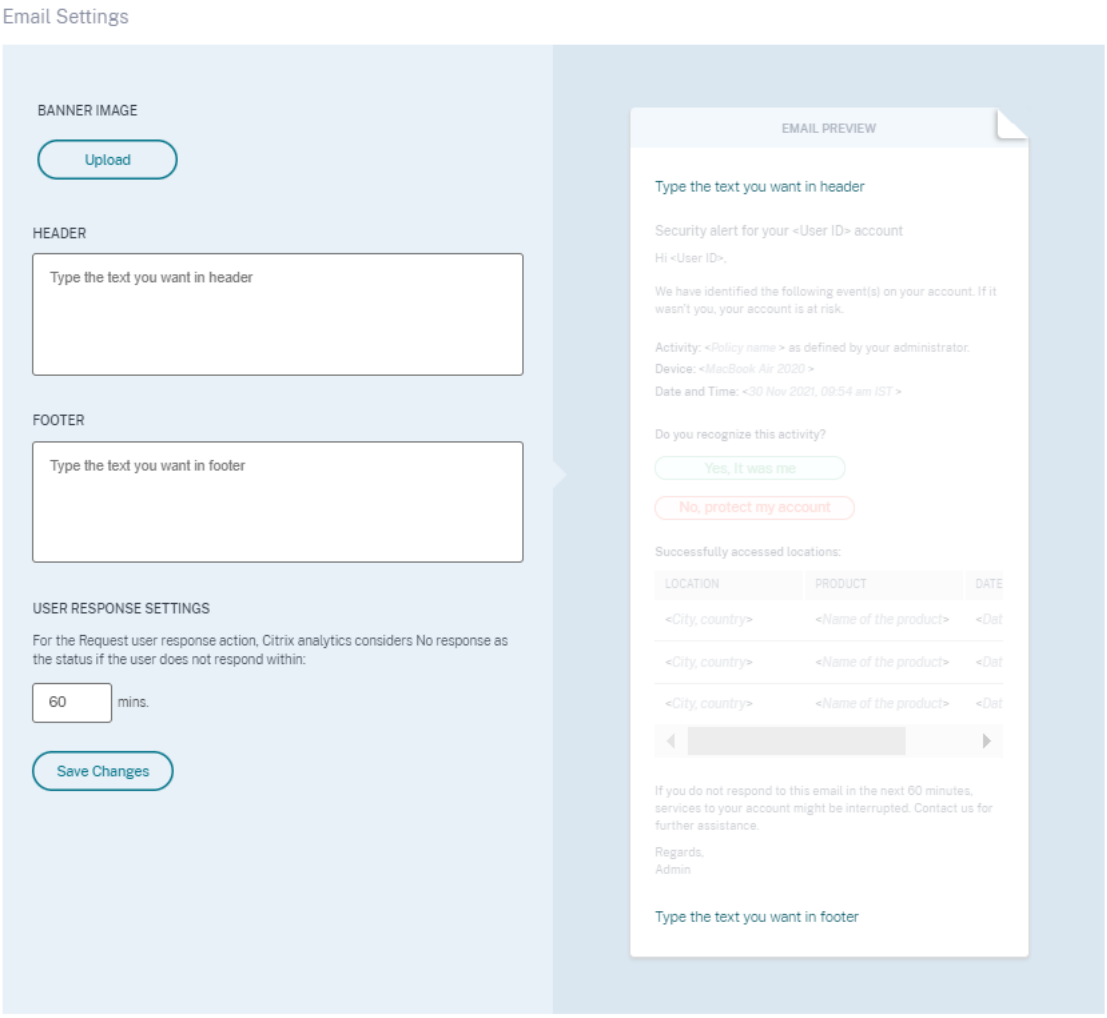


2021 年 11 月 29 日

新機能

ユーザー通知のメール設定の強化　管理者は、ユーザー返信メールテンプレートにバナー画像、ヘッダー、フッターのテキストを追加できるようになりました。これらのフィールドはメールの正当性を高め、ユーザーのメールに対する関心と反応を高めます。

詳細については、「エンドユーザーのメール設定」を参照してください。

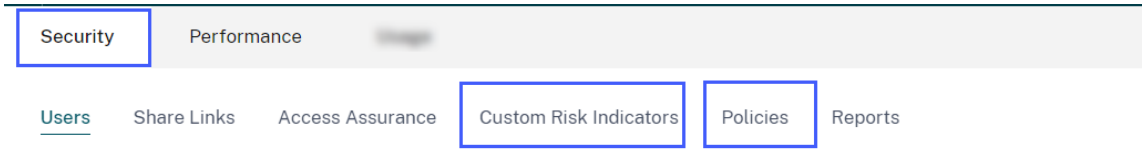


2021 年 11 月 26 日

新機能

カスタムリスク指標とポリシーメニューの変更　次の機能のナビゲーションリンクが更新されました。

- カスタムリスク指標: この機能を使用するには、[セキュリティ] > [カスタムリスク指標] をクリックします。
- ポリシー: この機能を使用するには、[セキュリティ] > [ポリシー] をクリックします。



2021 年 11 月 25 日

新機能

セキュリティ情報およびイベント管理 **(SIEM)** 統合の強化

> 注
>
> このインテグレーションはプレビュー版です。

Citrix Analytics for Security を次の SIEM サービスと統合できるようになりました。

- Microsoft Sentinel
- Kibana などの可視化サービスと logryThm などの SIEM サービスを備えた Elasticsearch
- Logstash データ収集エンジンを使用するその他の SIEM サービス

ビジネスニーズに応じて、Citrix Analytics for Security から SIEM サービスにユーザーのデータをインポートします。この統合により、セキュリティ運用チームは組織内の SIEM サービス内のさまざまなログからデータを関連付け、分析、検索できるようになり、セキュリティリスクを特定して迅速に修正できるようになります。

詳細については、「セキュリティ情報とイベント管理 (SIEM) の統合」を参照してください。

2021 年 11 月 9 日

修正された問題

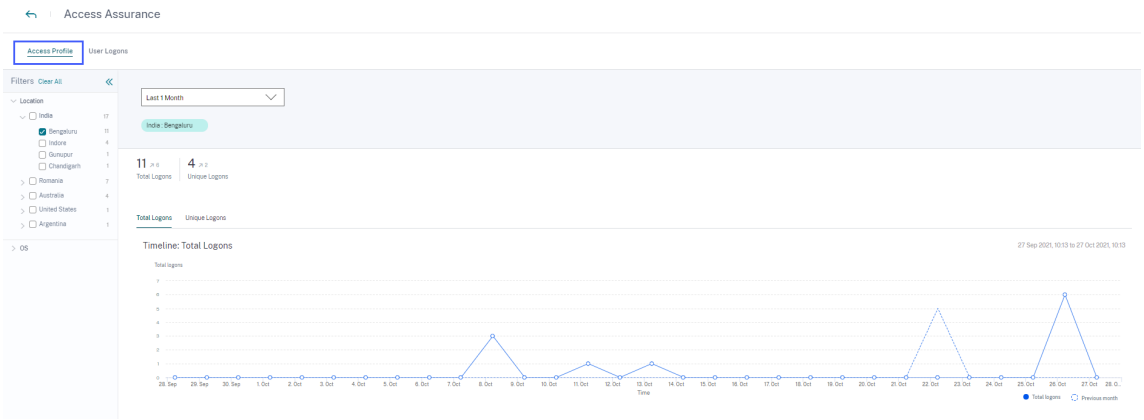
- 一部のテナントでは、ユーザーポリシーが機能していません。この問題は、仮想アプリケーションのアラートにドメインの文字列値が空である場合に発生しました。この問題は修正されました。[CAS-60920]

2021 年 11 月 2 日

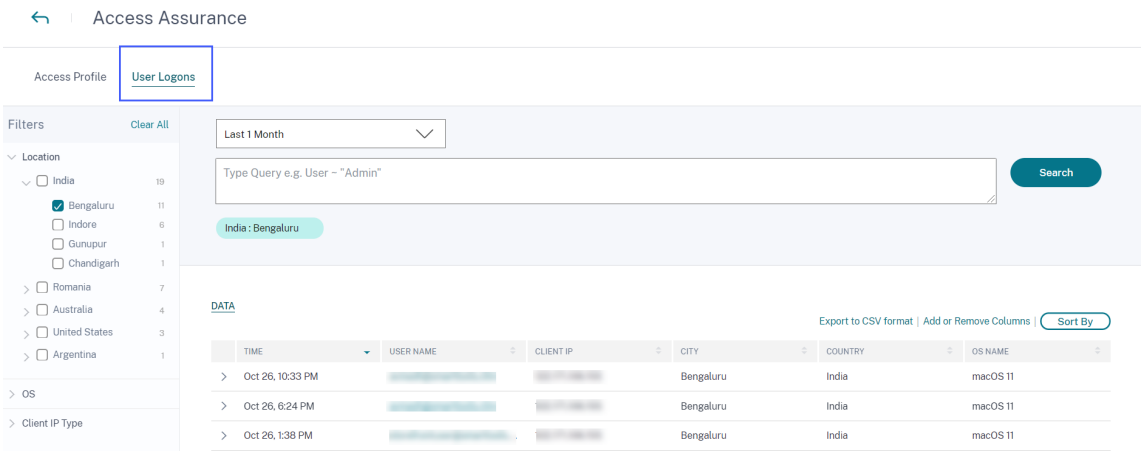
新機能

Citrix Virtual Apps and Desktops、および **Citrix DaaS** ユーザーのアクセスプロファイルとログオンの詳細を表示する [**Access Assurance Location**] ダッシュボードでは、仮想アプリケーションおよび仮想デスクトップにログオンしたユーザーのアクセスプロファイルとログオン詳細を表示できます。この情報は、脅威の調査と分析を行う際に役立ちます。

- [**Access Profile**] ページには、選択した場所からのユーザーアクセスの概要が表示されます。合計ユーザー数と個別ユーザーログオン数の傾向分析と上位アクセスイベントを表示できます。



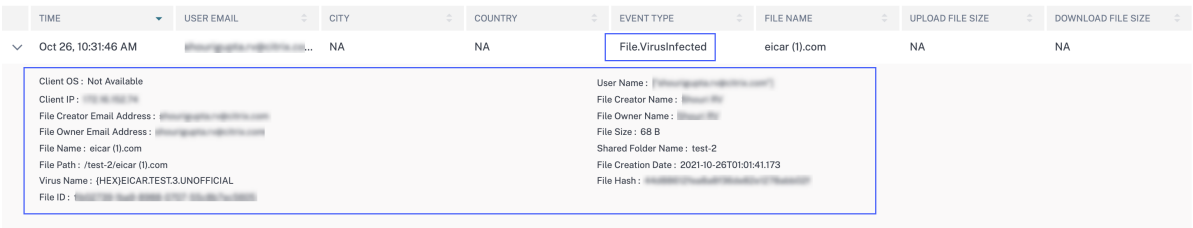
- [ユーザーログオン] ページには、選択した場所から仮想アプリケーションおよび仮想デスクトップへのユーザーログオンの詳細が表示されます。



詳細については、「アクセス保証ロケーション」ダッシュボードを参照してください。

Content Collaboration のセルフサービス検索ページでマルウェアログを表示する　Content Collaboration のセルフサービスページで、マルウェアイベント`File.VirusInfected`とそれに関連するログを表示できるようになりました。このイベントは、Content Collaboration ユーザーがマルウェアに感染したファイルをアップロードしたときにトリガーされます。

詳細については、「Content Collaboration のセルフサービス検索」を参照してください。



修正された問題

- Citrix Analytics でイベントを処理しているときに、一部の Content Collaboration ユーザーが誤って非従業員として設定されます。そのため、ユーザーは [検出されたユーザー] として識別されません。この問題は修正されました。[CAS-59608]

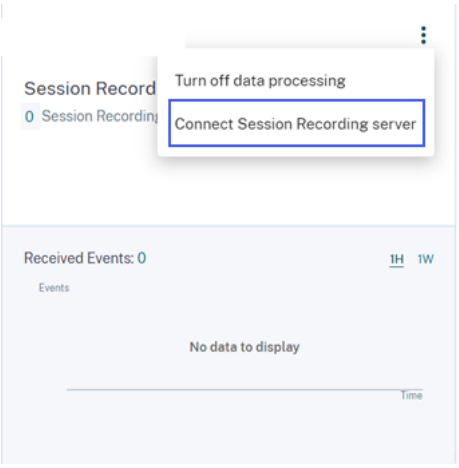
2021 年 10 月 20 日

新機能

Session Recording サーバー統合　Citrix Virtual Apps and Desktops Citrix DaaS 環境では、セキュリティのためにユーザーイベントを Citrix Analytics に送信するように Session Recording サーバーを構成できるようになりました。これらのユーザーイベントは、ユーザーの行動に関する実用的なインサイトを提供するために処理されます。

[データソース] **>** [セキュリティ] ページで、[**Virtual Apps and Desktops**] サイトカードに移動します。**Session Recording** サイトカードで、縦の省略記号 (⋮) をクリックし、[**Session Recording** サーバーの接続] を選択します。

詳しくは、「Session Recording 展開に接続する」を参照してください。



2021 年 10 月 19 日

新機能

管理者への通知メールテンプレートの機能拡張　「管理者に通知」アクションを適用した後に管理者が受け取る電子メール通知が拡張され、ユーザーのリスクの高いイベントをより的確に把握できるようになりました。

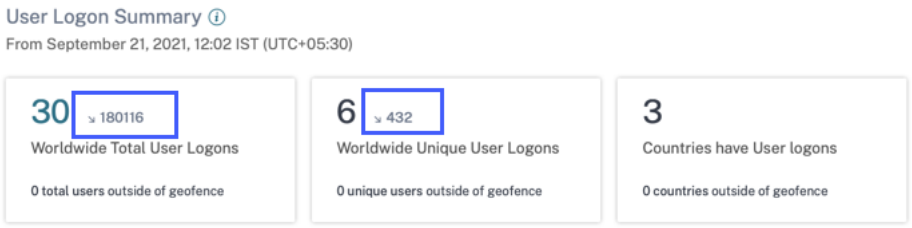
- 通知には、トリガーされたリスク指標または適用されたポリシーに関する詳細情報が表示されるようになりました。たとえば、既定のリスク指標とカスタムリスク指標の重大度とトリガーされた時間を表示できます。コンテンツ構造が改善され、読みやすくなります。

- 管理者は、電子メール通知からユーザーのタイムラインに直接アクセスして、危険なイベントに関する詳細を表示できるようになりました。
- 通知にフィードバックオプションが追加されました。このオプションは、管理者からの応答を収集し、応答に基づいて通知の内容を継続的に改善するのに役立ちます。

「管理者に通知」操作について詳しくは、「ポリシーと操作」を参照してください。

ユーザーログオンサマリーの機能強化

- 世界規模の合計ユーザーログオン数と世界規模のユニークユーザーログオン数について、ユーザーログオン数の増加傾向または減少傾向を確認できるようになりました。



- [一意のログオン場所] テーブルの **[** 偏差] 列には、特定の場所に対する一意のユーザーログオンが上向きまたは下向きに変化したことがわかります ** 。

これらの指標は、ユーザーログオンが前期からどのように変化したか（正または負）を把握するのに役立ちます。これにより、Citrix Virtual Apps and Desktops Citrix DaaS 環境でのユーザーインタラクションを可視化できます。

詳細については、「アクセス保証ロケーションダッシュボード」を参照してください。

修正された問題

- ジオフェンスエリア外からログオンするユーザーがいないと、**[**Access Assurance Location**] ダッシュボードの [User Logon Summary**] カードにユーザーログオンメトリック (ワールドワイド合計ユーザーログオン数、ワールドワイドユニークユーザーログオン数、およびユーザーログオンがある国) が表示されません。この問題は修正されました。[CAS-59595]

2021 年 **10** 月 **1** 日

新機能

Content Collaboration のセルフサービス検索に関する監査ログの表示　Content Collaboration のセルフサービス検索で、監査ログを表示できるようになりました。これらのログは、Content Collaboration 管理者がユーザーアカウントに適用した権限とアクションに関する洞察を提供します。これらのデータを使用して、Content Collaboration 管理者がユーザーアカウントに対して有効なアクションを実行したかどうかを確認できます。セキュリティ管理者は、リスクの調査と分析の際に役立ちます。

監査ログの詳細については、「Content Collaboration のセルフサービス検索」を参照してください。

修正された問題

Azure AD を使用して Citrix Cloud にログオンする管理者は、以前の期限切れのセッション ID が新しいセッション ID と共に来ると、Citrix Analytics サービスにアクセスできません。この問題は修正されました。[CAS-59385]

2021 年 **9** 月 **29** 日

新機能

アクセス保証ロケーションダッシュボードが一般公開されました　ダッシュボードには、Citrix Virtual Apps and Desktops Citrix DaaS ユーザーの場所が表示されます。ジオフェンシングを有効にすることで、場所が異常なユーザーを特定し、脅威を防ぐための適切なアクションを適用できます。

ダッシュボードを表示するには、[セキュリティ**] > [**アクセス保証] の順にクリックします。ロケーションの詳細を表示する期間を選択します。

詳細については、「アクセス保証ロケーションダッシュボード」を参照してください。

2021 年 **9** 月 **15** 日

新機能

カスタムリスク指標の機能強化

- カスタムリスク指標がトリガーされると、すぐにユーザータイムラインに表示されます 。ただし、ユーザーのリスクサマリーとリスクスコアは数分（約 15 ～20 分）後に更新されます。
- 既存のカスタムリスク指標の条件、リスクカテゴリ、重大度、名前などの属性をユーザータイムラインで変更しても、そのユーザーに対してトリガーされたカスタムリスク指標（古い属性を含む）の以前の発生を表示できます。
- カスタムリスク指標を削除しても、ユーザータイムラインで、そのユーザーに対してトリガーされたカスタムリスク指標の以前の発生を表示できます。

詳細については、「カスタムリスク指標」を参照してください。

2021 年 **9** 月 **14** 日

新機能

疑わしいログオンリスクインジケータの導入　Citrix Analytics for Security は、次のような複数のコンテキスト要因に基づいて、本質的に疑わしいユーザーログオンを検出するようになりました。

- 場所は、ユーザーおよび組織履歴に関して通常とは違うと見なされます
- デバイスはユーザーおよび組織履歴に関して異常であるとみなされます
- ユーザーおよび組織の履歴に関して、ネットワークが異常と見なされる
- IP アドレスは、IP 脅威インテリジェンスフィードに基づいて疑わしいと見なされます。

Citrix Virtual Apps and Desktops および Citrix DaaS ユーザーが、これらの要因の組み合わせに基づいて疑わしいコンテキストからログオンすると、リスク指標がトリガーされます。

このリスク指標は、Citrix Virtual Apps and **Desktops** データソースに関連付けられた異常な場所からのアクセスのリスク指標を置き換えます。[異常な場所からのアクセス] リスク指標に基づく既存のポリシーは、新しいリスク指標である [疑わしいログオン] に自動的にリンクされます。

リスク指標について詳しくは、「Citrix Virtual Apps and Desktops」および「Citrix DaaS リスク指標」を参照してください。

SIEM メッセージの機能強化　Citrix Analytics for Security は、疑わしいログオンリスク指標のスキーマの詳細を **SIEM** サービスに送信するようになりました。指標の概要のスキーマと、疑わしいログオンリスク指標のイベントの詳細を表示できます。詳しくは、「SIEM 用の Citrix Analytics データ形式」を参照してください。

修正された問題

- アプリとデスクトップのセルフサービス検索では、ダウンロードした CSV ファイルにクライアント IP 値がありません。この問題は修正されました。[CAS-58426]

2021 年 **8** 月 **19** 日

新機能

Splunk 向け **Citrix Analytics** アプリの紹介

> 注
>
> アプリはプレビューです。

Splunk 向け Citrix Analytics アプリを使用すると、セキュリティ向け Citrix Analytics から収集されたデータを、洞察に満ちたダッシュボードの形式で Splunk に表示できます。ダッシュボードは、ユーザーの危険なイベントに関するインサイトを提供します。また、Citrix Analytics データを、他のさまざまなデータソースから収集されたログと関連付けることもできます。相関関係は、イベント間の関係を見つけ、IT 環境を保護するためのタイムリーなアクションを実行するのに役立ちます。

アプリをダウンロードするには、Splunkbaseにアクセスしてください。Splunk 検索ヘッドにアプリをインストールします。

詳しくは、「Splunk 用 Citrix Analytics アプリ」を参照してください。

SIEM のカスタムリスク指標スキーマ　SIEM サービスで、Citrix Virtual Apps and Desktops Citrix DaaS 用に作成されたカスタムリスク指標のスキーマを表示できるようになりました。このデータは、組織のセキュリティリスク状況に関する洞察を得るのに役立ちます。

カスタムリスク指標スキーマについて詳しくは、「SIEM の Citrix Analytics データ形式」を参照してください。

データソースとしての **Citrix Director** のサポート　Citrix Director でオンプレミスサイトを構成して、セキュリティ分析にイベントを送信できるようになりました。これらのイベントは、Security Analytics に接続しているユーザーを検出し、ユーザーのデバイスにインストールされている Workspace アプリのバージョンを判断するために使用されます。

デフォルトでは、サイトの検出後にデータ処理が有効になります。[監視] カードでは、接続されているすべてのサイトを表示できます。

Director でサイトを構成する方法について詳しくは、「Citrix Virtual Apps and Desktops」および「Citrix DaaS データソース」を参照してください。

アクセス保証ロケーションダッシュボードでのジオフェンスのサポート　ダッシュボードの [ジオフェンス設定] を使用して、ジオフェンスエリアを選択して有効にできるようになりました。ジオフェンスを有効にすると、マップにジオフェンスエリア（国）が表示され、ジオフェンスの外側と内側からユーザーがログオンします。この機能は、ジオフェンスのリスク指標の外で開始された **CVAD** セッションを使用して、ユーザーのログオンを監視します。

詳細については、「アクセス保証ロケーションダッシュボード」を参照してください。

[ユーザー] ページの **Workspace** アプリのステータス　［ユーザー］ページで、Citrix Analytics でサポートされている Citrix Workspace アプリクライアントのステータスを表示できるようになりました。このページには、次のステータスが表示されます。

- サポート対象
- 部分的にサポートされている
- サポートされません
- 利用できない
- 非アクティブ

このステータスは、ユーザが使用するサポートされていないクライアントバージョンを特定し、クライアントをサポート対象バージョンにアップグレードするようにユーザに推奨するのに役立ちます。サポートされているクライアントバージョンは、ユーザーイベントを Citrix Analytics に送信します。

> 注
>
> Citrix Workspace アプリのステータスを表示するには、Citrix Director データソースを起動する必要があります。それ以外の場合、すべての Citrix Virtual Apps and Desktops Citrix DaaS ユーザーのステータスは「非アクティブ」と表示されます。

詳細については、[ユーザー] ダッシュボードを参照してください。

IS EMPTY 演算子のサポート　カスタムリスク指標の作成中に、条件で IS **EMPTY** 演算子を使用して NULL または空のディメンションをチェックできるようになりました。

> 注**:**
>
> この演算子は、App-Name、Browser、Country などの文字列タイプのディメンションでのみ機能します。

詳細については、「カスタムリスク指標」を参照してください。

リスクスコアリングの向上　ユーザーのタイムラインで、ユーザーのリスクサマリーを表示できるようになりました。リスクサマリーは、ユーザーイベントに関連するリスク要因に関する情報を提供します。リスクファクターは、ユーザーイベントの異常のタイプを識別するのに役立ち、リスクスコアも決定します。リスク要因は次のとおりです。

- デバイスベースのリスク指標
- ロケーションベースのリスク指標
- IP ベースのリスク指標
- ログオン失敗ベースのリスク指標
- データベースのリスク指標
- ファイルベースのリスク指標

- カスタムリスク指標
- その他のリスク指標

ユーザーのタイムラインで、フィルターを適用して、リスク要因に基づいてユーザーイベントを表示できるようになりました。

詳しくは、次のトピックを参照してください:

- Citrix ユーザーリスク指標
- ユーザーリスクのタイムラインとプロファイル

2021 年 7 月 29 日

非推奨の機能

Citrix Endpoint Management に関連付けられている非推奨のアクション　以下のアクションは、Citrix Endpoint Management データソースから削除されます。これらのアクションをリスク指標に適用したり、これらのアクションを使用してポリシーを作成したりすることはできなくなりました。

- デバイスのロック
- Endpoint Management 管理者に通知する
- ユーザーに通知
- デバイスの取り消し
- デバイスのワイプ

既存のポリシーでは、これらのアクションがすでに使用されている場合は、自動的に [ウォッチリストに追加] アクションに置き換えられます。そして、ウォッチリストからそのようなユーザーを監視することができます。

2021 年 7 月 14 日

新機能

IS NOT EMPTY 演算子のサポート　カスタムリスク指標の作成時に、条件で IS NOT **EMPTY** 演算子を使用して、ディメンションが空ではない (空白ではない) かどうかを確認できるようになりました。

> 注:
>
> この演算子は、App-Name、Browser、Country などの文字列タイプのディメンションでのみ機能します。

たとえば、次の条件は、country 値が NULL でないすべての国のユーザーログオンイベントを検出します。つまり、国名が指定されます。


```
Event-Type = “Session.logon” AND Country IS NOT EMPTY
```

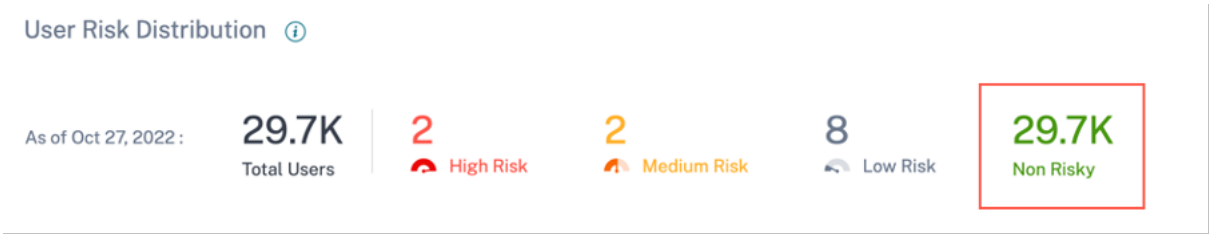
詳細については、「カスタムリスク指標」を参照してください。

2021 年 7 月 06 日放送分

新機能

ユーザーダッシュボードでリスクのないユーザーを表示する　[ユーザー] ダッシュボードで、選択した期間のリスクのないユーザーの数を表示できるようになりました。検出されたこれらのユーザーは、選択した期間のゼロリスクスコアに基づいて、非リスクとして識別されます。[**Non Risky Users**] カードをクリックすると、リスクスコアがゼロのすべてのユーザーが表示されます。

詳細については、「ユーザーダッシュボード」を参照してください。



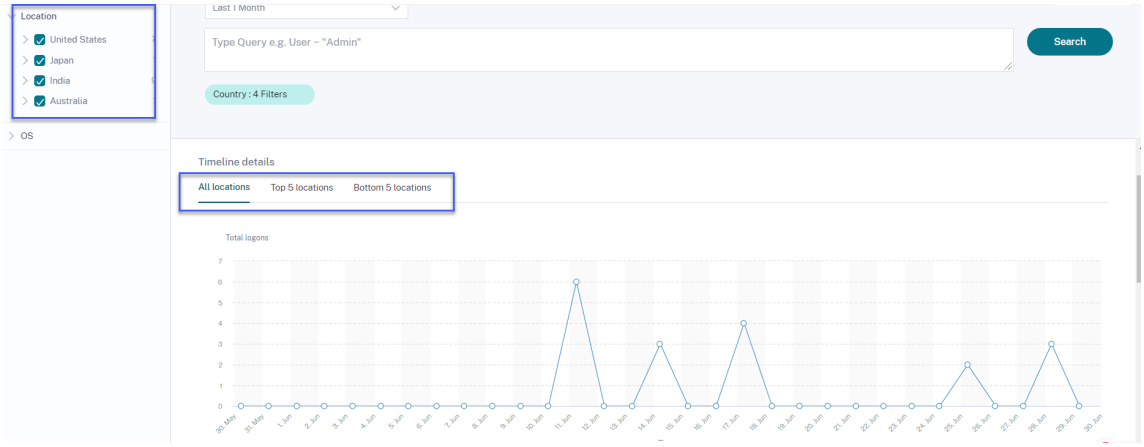
2021 年 7 月 01 日

新機能

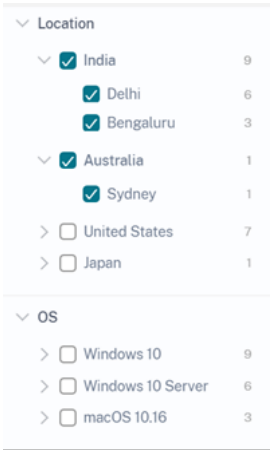
アクセス保証ロケーションダッシュボードの機能強化

- [一意のログオンの場所の上位 **10**] テーブルでは、不明な場所からの一意のユーザーログオンの数を表示できます。このリストは、一意のログオン場所の上位 10 のサブセットです。また、場所が不明である理由と、ユーザーの位置情報を取得する方法もわかります。

- [アクセス場所] ページで、複数の場所を選択した場合、すべての場所、上位 5 つの場所、および下位 5 つの場所からのユーザーログオンのタイムラインの詳細を表示および比較できます。

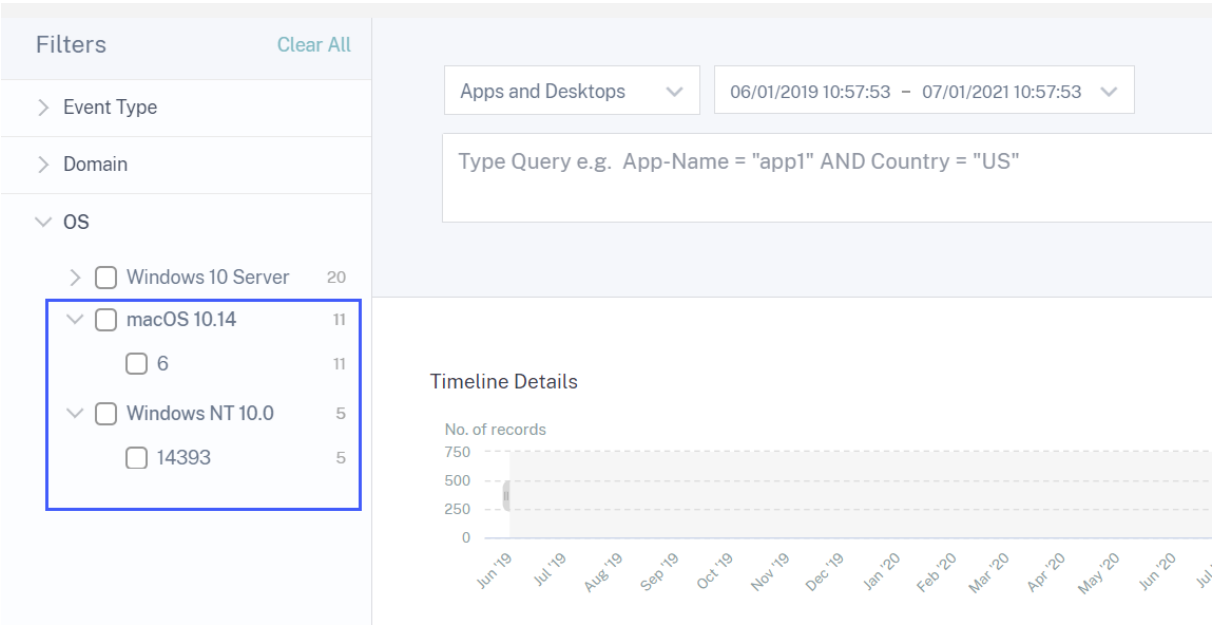


- [アクセス場所] ページでは、国とその都市、オペレーティングシステム (メジャーバージョンとマイナーバージョンなど) のネストされたファセットを使用できます。これらのファセットを使用すると、イベントを細かくフィルタリングできます。



詳細については、アクセス保証の場所を参照してください。

Virtual Apps and Desktops のセルフサービス検索の **OS** ファセットを更新しました　ネストされた OS ファセットを使用して、Apps および Desktops イベントをフィルタリングできるようになりました。オペレーティングシステムに関連付けられているメジャーバージョンとマイナーバージョンを選択し、詳細な方法でイベントをフィルタリングします。詳しくは、「アプリとデスクトップのセルフサービス検索」を参照してください。



2021 年 6 月 30 日

新機能

アプリとデスクトップのカスタムリスク指標条件に **Workspace** アプリのバージョンを追加　アプリとデスクトップデータソースでは、**Workspace-App-Version** ディメンションを使用して、カスタムリスク指標の作成中に条件を定義できるようになりました。ディメンションの詳細については、「アプリとデスクトップのセルフサービス検索」を参照してください。

2021 年 6 月 23 日

新機能

SIEM メッセージの機能強化　次のフィールドがリスク指標のスキーマに追加されました。

- `indicator_vector_name`-リスク指標に関連付けられたリスクベクトルを示します。リスクベクトルは、デバイスベースのリスク指標、ロケーションベースのリスク指標、ログオン失敗ベースのリスク指標、IP ベースのリスク指標、データベースのリスク指標、ファイルベースのリスク指標、およびその他のリスク指標です。
- `indicator_vector_id`-リスクベクトルに関連付けられた ID。ID 1 = デバイスベースのリスク指標、ID 2 = ロケーションベースのリスク指標、ID 3 = ログオン失敗ベースのリスク指標、ID 4 = IP ベースのリスク指標、ID 5 = IP ベースのリスク指標、ID 6 = データベースのリスク指標、ID 7 = その他のリスクインジケータ、ID 999 = 利用できません。

詳しくは、「SIEM 用の Citrix Analytics データ形式」を参照してください。

2021 年 6 月 07 日

新機能

管理者に通知アクションの機能強化　[管理者に通知] アクションをリスクインジケータに適用したり、アクションでポリシーを作成したりするときに、ユーザーの危険な動作に関する通知を受け取る管理者を選択できるようになりました。アクションの詳細については、「ポリシーとアクション」を参照してください。

表示専用共有アクションのサポートが追加されました　ユーザーがファイルを過度に共有すると、Citrix Analytics は過剰なファイル共有のリスクインジケータをトリガーします。ユーザーのリスクタイムラインから、[表示のみの共有にリンクを変更] アクションを **[**** 過剰なファイル共有リスク **] インジケータに適用できるようになりました。共有リンクリスクタイムライン上の特定の共有リンクにアクションを適用することもできます。この操作により、他のユーザーが共有リンクに関連付けられているファイルをダウンロードしたり、コピーしたり、印刷したりできなくなります。アクションの詳細については、「ポリシーとアクション」を参照してください。

2021 年 5 月 18 日

新機能

デフォルトのリスク指標をカスタムリスク指標に移行する　次のデフォルトリスク指標は、事前設定されたカスタムリスク指標に移行されます。

デフォルトのリスクインジケータ	データソース	事前構成されたカスタムリスクインジケータ
新しいデバイスからの初回アクセス	Citrix Virtual Apps and Desktops および Citrix DaaS	CVAD-新しいデバイスからの初回アクセス
新しい IP からの初回アクセス	Citrix Gateway	新しい IP からのゲートウェイファーストタイムアクセス

このカスタムリスク指標への移行により、デフォルトのリスク指標と関連する機械学習アルゴリズムは廃止されます。

対応するカスタムリスク指標は、次の事前設定された条件に基づいてトリガーされます。

- ユーザーが新しいデバイスから初めてアクセスしたとき、または最低 90 日間使用されていない既存のデバイスからアクセスした場合。
- ユーザーが新しい IP アドレス、または最低 90 日間使用されていない既存の IP アドレスからサインインしたとき。

事前構成された条件に加えて、これらのカスタムリスク指標に独自の条件を追加して、Citrix 環境内の脅威を特定できるようになりました。このオプションを使用すると、セキュリティのニーズに基づいてカスタムリスク指標を柔軟に設定できます。また、これらのカスタムリスク指標によって検出されたリスクのあるイベントにアクションを適用するポリシーを作成することもできます。

ただし、ユーザーのタイムラインでは、以前にトリガーされたデフォルトのリスク指標とそのイベントは引き続き表示できます。

これらのデフォルトリスク指標に関連付けられているポリシーは、対応する事前設定されたカスタムリスク指標に自動的にリンクされます。

詳細については、「事前構成されたカスタムリスク指標とポリシー」を参照してください。

Gateway のセルフサービス検索の機能強化

- イベントタイプフィルタの名前が [レコードタイプ] に変更されました。次のいずれかのレコードタイプを選択して、イベントをフィルタリングします。VPN_AI、VPN_IF、および VPN_ST。
- **DATA** テーブルで、ユーザーイベントの行を展開して、対応するイベントタイプを表示します。イベントタイプは、認証、ICA ファイル、またはセッションログアウトのいずれかです。

次の表では、レコードタイプとイベントタイプの相関関係について説明します。

レコードタイプ	イベントの種類
VPN_AI	認証

レコードタイプ	イベントの種類
VPN_IF	ICA ファイル
VPN_ST	セッションログアウト

詳細については、「Gateway のセルフサービス検索」を参照してください。

修正された問題

- カスタムリスク指標は、条件値の大文字と小文字の区別に基づいてトリガーされます。たとえば、許可リストにデバイス ID を含むユーザイベントでは、次の動作が表示されます。
  - Device-ID ディメンションの値を小文字で入力すると、カスタムインジケータがトリガーされます。

    ```
    Event-Type = Session.Logon AND Device-ID NOTIN ( “1621d2cb-f598-5ef7-a5bf-81747496ed2e” )
    ```

  - 同じデバイスのDevice-IDディメンションの値を大文字で入力すると、カスタムインジケータはトリガーされません。

    ```
    Event-Type = Session.Logon AND Device-ID NOTIN ( “1621D2CB-F598-5EF7-A5BF-81747496ED2E” )
    ```

  この問題は修正され、条件付き値の大文字と小文字の区別に関係なく、カスタムリスク指標がトリガーされます。

  [CAS-50153]

2021 年 4 月 29 日

新機能

カスタムリスク指標のイベント詳細　ユーザーのリスクタイムラインページで、カスタムリスク指標をトリガーしたイベントを表示できるようになりました。以前は、カスタムリスク指標の定義済みの条件、説明、およびトリガー頻度のみを表示できました。[イベント検索] をクリックして、ユーザーとリスク指標に関連付けられているイベントの詳細を表示します。
詳細については、「カスタムリスク指標」を参照してください。

修正された問題

- 管理者は、アクセス権限が読み取り専用管理者から完全管理者に変更された後でも、カスタムリスク指標を作成できません。[CAS-49628]

2021 年 4 月 16 日

新機能

SIEM メッセージの機能強化　リスク指標スキーマ形式について、次の機能強化を表示できます。

- クライアント IP アドレスが、すべてのバッチリスク指標のスキーマで利用可能になりました。以前は、クライアント IP アドレスは、いくつかのバッチリスク指標でのみ使用可能でした。
  - EPA スキャンの失敗
  - 過剰な認証失敗
  - 疑わしい IP からのログオン
  - 通常の場所以外からのアクセス
  - 異常な認証の失敗
  - 匿名の機密共有ダウンロード
  - データ流出の可能性
- 整数データ型のフィールド値が使用できない場合、割り当てられる値は **-999** です。例：`"latitide"`=−999。
- 文字列データ型のフィールド値が使用できない場合、割り当てられる値は **NA** になります。例：`"city"`=`"NA"`。

詳しくは、「SIEM 用の Citrix Analytics データ形式」を参照してください。

2021 年 3 月 26 日

新機能

SIEM メッセージの制限　Citrix Analytics は、リスク指標の発生ごとに最大 1000 個のイベントの詳細を SIEM サービスに送信します。これらのイベントは、発生時順に送信されます。詳しくは、「SIEM 用の Citrix Analytics データ形式」を参照してください。

SIEM メッセージにデータソース **ID** フィールドとインジケータカテゴリ **ID** フィールドを追加しました　インジケータサマリスキーマとインジケータイベント詳細スキーマには、次のフィールドが追加されます。

フィールド	説明
data_source_id	データソースに関連付けられた ID。ID 0 = Citrix Content Collaboration、ID 1 = NetScaler Gateway、ID 2 = Citrix Endpoint Management、ID 3 = Citrix Virtual Apps and Desktops、ID 4 = Citrix アクセスコントロール
indicator_category_id	リスク指標カテゴリに関連付けられた ID。ID 1 = データの漏出し、ID 2 = 内部者の脅威、ID 3 = 侵害されたユーザー

詳しくは、「SIEM 用の Citrix Analytics データ形式」を参照してください。

2021 年 3 月 18 日

新機能

アシュアランスロケーションダッシュボードにアクセスする

> 注
>
> この機能はプレビューです。

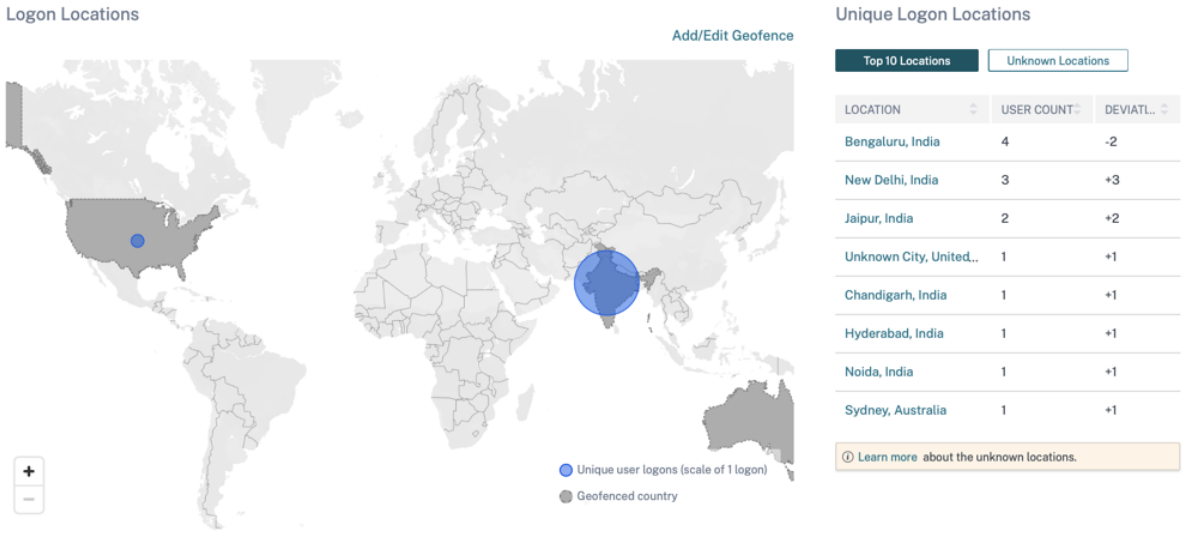
アクセス保証ロケーションダッシュボードには、Citrix Virtual Apps and Desktops と Citrix DaaS ユーザーが選択した期間にログオンした場所の概要が表示されます。Citrix Analytics は、ユーザーのデバイスにインストールされている Citrix Workspace アプリからこれらのユーザーログオンイベントを受信します。

ダッシュボードを表示するには、[セキュリティ] **>** [アクセス保証] の順にクリックします。

選択した期間について、次の情報を表示できます。

- 特定の場所およびロケーション間のユーザーログオンの合計数。
- ロケーション全体の一意のユーザーログオンの総数。
- ユーザーがログオンした国の総数。
- 一意のユーザーログオンがある上位 10 の場所。

詳細については、アクセス保証の場所を参照してください。



NOT LIKE (!~) 演算子のサポート　セルフサービス検索クエリとカスタムリスク指標条件では、NOT LIKE (!~) 演算子。オペレータは、指定したマッチングパターンのユーザイベントをチェックします。これは、イベント文字列内の指定されたパターンを含まないイベントを返します。

たとえば、クエリ`User-Name !~ "John"`では、John、John Smith、または一致する名前「John」を含むユーザー以外のユーザーのイベントが表示されます。

詳細については、「セルフサービス検索」を参照してください。

翻訳されたオペレーティングシステムのバージョン　Citrix Virtual Apps and Desktops と Citrix DaaS データソースでは、プラットフォームディメンションが **OS** メジャーバージョン、****OS** マイナーバージョン、および ****OS** エクストラディテールディメンションに変換されるようになりました。Citrix Analytics では、ユーザーのオペレーティングシステムの詳細に基づいて、セルフサービス検索ページにこれらのディメンションが表示されます。

これらのディメンションを使用して、カスタムリスク指標の条件を定義できます。

以前に作成したカスタムリスク指標について、プラットフォームディメンションを条件として使用している場合、Citrix Analytics はプラットフォームディメンションを **OS** メジャーバージョン、**OS** マイナーバージョン、**OS-Extra-Details** に自動的に置き換えます。この更新は、定義した条件の整合性には影響しません。

新しいディメンションについて詳しくは、Virtual Apps and Desktops のセルフサービス検索を参照してください。

アプリとデスクトップのデータフィールドが更新されました　アプリとデスクトップのセルフサービス検索で、コンテキストテンプレートに基づいて更新されたデータフィールドを表示します。

詳しくは、「アプリとデスクトップのセルフサービス検索」を参照してください。

非推奨の機能

セルフサービス検索ページから **VPN_AF** イベントと **VPN_SU** イベントを削除しました　NetScaler Gateway データソースのセルフサービス検索ページで、次のレコードタイプが削除されました。

レコードタイプ	レコード名
VPN_SU	セッション更新レコード
VPN_AF	アプリケーションの起動失敗レコード

そのため、これらのレコードタイプに基づいてイベントをフィルタリングして表示することはできません。これらのレコードタイプに基づくカスタムリスク指標は機能しなくなります。

詳細については、「Gateway のセルフサービス検索」を参照してください。

2021 年 **3** 月 **11** 日

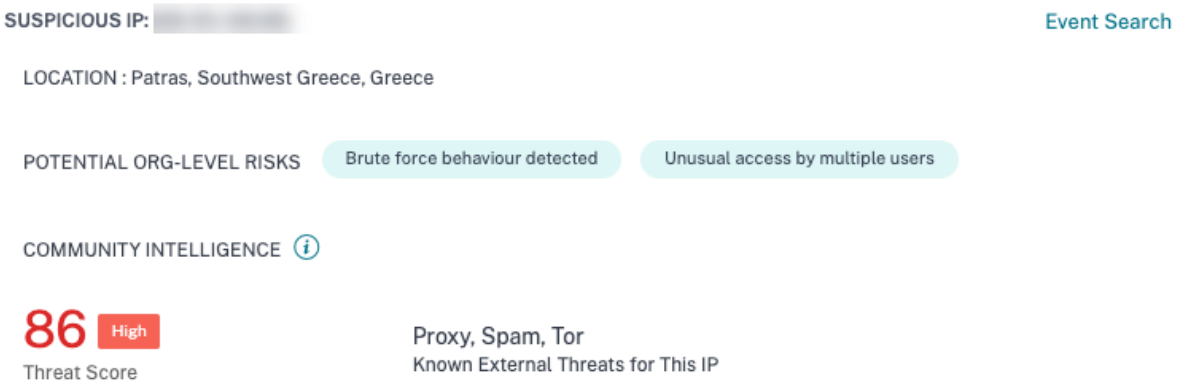
新機能

ユーザリスクスコアスキーマの現在のタイムスタンプ　ユーザリスクスコアスキーマ形式で新しいフィールド`last_update_timestamp`が追加されます。このフィールドは、リスクスコアが最後に更新された時刻を示します。スキーマ形式の詳細については、「ユーザーリスクスコアスキーマ」を参照してください。

2021 年 **3** 月 **03** 日

新機能

疑わしい **IP** リスク指標からのログオンの機能強化　ユーザーのリスクタイムラインページに、[疑わしい **IP** からのログオン**]** リスクインジケータの新しいセクション **[**疑わしい **IP**] が表示されます。このセクションでは、次の内容について説明します：



- 疑わしいサインインアクティビティが検出される IP アドレス。
- ユーザーの場所。
- Citrix Analytics が組織で最近検出した疑わしい IP アクティビティのパターン。
- コミュニティレベルのインテリジェンスは、IP アドレスについてフィードします。

詳細については、疑わしい IP からのログオンリスク指標を参照してください 。

異常な場所からのアクセスリスク指標の機能強化

- Citrix Content Collaboration の［異常な場所からのアクセス］リスクインジケータで、イベントテーブルに［ツール名］列を追加しました。イベントテーブルから **DEVICE BROWSER** 列を削除しました。詳しくは、「Citrix Content Collaboration のリスク指標」を参照してください。
- Citrix Virtual Apps and Desktops と Citrix DaaS の「異常な位置情報からのアクセス」リスク指標で、イベントテーブルに「デバイス **ID** 」列と「受信者タイプ」列を追加しました。詳しくは、「Citrix Virtual Apps and Desktops のリスク指標」を参照してください。

Citrix Analytics の **SIEM** 用のデータ形式　この記事では 、SIEM サービス用に Citrix Analytics によって生成される処理されたデータのスキーマについて説明します。

修正された問題

- Content Collaboration ユーザーの場合、`Is Employee<!--NeedCopy-->` 値が null のユーザーは検出されたユーザーリストに表示されません。[CAS-47815]

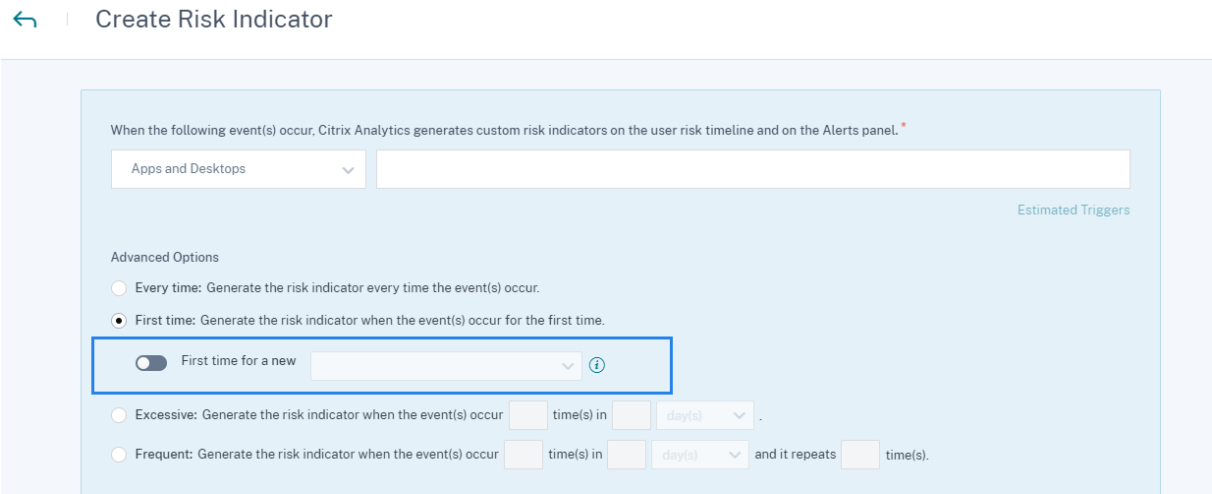
2021 年 **2** 月 **18** 日

新機能

カスタムリスク指標の新しいエンティティからの初回アクセスのサポート　Citrix Analytics が新しいエンティティから初めてイベントを受信したときにトリガーされるリスク指標を作成できるようになりました。エンティティの例としては、クライアント IP、都市、国などがあります。

[インジケータの作成] ページで、[初回] オプションをクリックします。[初めて新規作成] ボタンを有効にし、データソースに基づいてリストから有効なエンティティを選択します。エンティティに特定の値を割り当てる必要はありません。たとえば、リストから［都市］を選択すると、ユーザーが新しい都市から初めてサインインするたびに、Citrix Analytics によってリスク指標がトリガーされます。

詳細については、「カスタムリスク指標の作成」を参照してください。



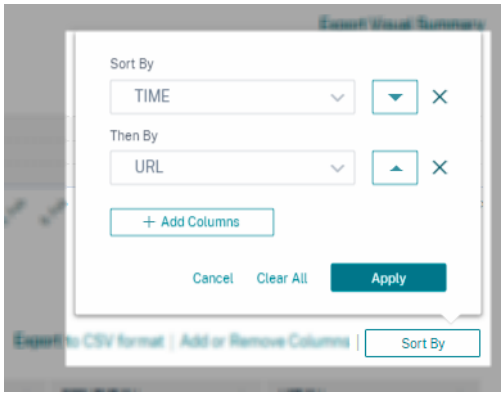
カスタムリスク指標を作成するための上限　最大 50 のカスタムリスク指標を作成できるようになりました。この上限に達した場合は、既存のカスタムリスク指標を削除または編集して、カスタムリスク指標を作成する必要があります。

詳細については、「カスタムリスク指標」を参照してください。

Citrix Virtual Apps and Desktops および **Citrix DaaS** からのユーザーの位置情報データ　ユーザー情報ページに、Citrix Analytics が Citrix Virtual Apps and Desktops と Citrix DaaS データソースからユーザーの場所を表示するようになりました。

ユーザーの場所の詳細については、「ユーザープロファイル」を参照してください。

複数列の並べ替え　セルフサービス検索ページで、ユーザーイベントを複数の列で並べ替えることができるようになりました。[並べ替え] をクリックし、列と並べ替え順序を追加します。[**Apply**] をクリックして、ユーザーイベントを並べ替えます。最大 6 つの列を追加して、複数列の並べ替えを実行できます。



詳細については、「セルフサービス検索」を参照してください。

廃止された機能

過剰な認証失敗リスク指標は非推奨　NetScaler Gateway リスクインジケータ- 過剰な承認失敗は廃止されました。このインジケーターに関連する履歴データのみを表示できます。

この非推奨の一部として、次の変更が適用されます。

- Citrix Analytics はこれらのリスク指標を生成しなくなりました。
- Citrix Analytics は、これらのリスク指標を条件として持つポリシーを生成しなくなりました。
- これらのリスク指標を条件とするデフォルトのポリシーは有効になりません。

詳しくは、「NetScaler Gateway リスク指標」を参照してください。

2021 年 1 月 27 日

新機能

異常な場所からのアクセスリスク指標の強化　Citrix Content Collaboration、NetScaler Gateway、および Citrix Virtual Apps and Desktops では、ユーザーが新しい国に関連付けられた IP アドレス、または以前のサインインから異常に離れた新しい都市からサインインすると、異常な場所からのアクセスリスクインジケータがトリガーされるようになりました ロケーション。その他の要因には、ユーザーの全体的なモビリティレベルや、組織内のすべてのユーザーの都市からのログインの相対的な頻度などがあります。すべての場合において、ユーザーのロケーション履歴は、過去 30 日間のサインインアクティビティに基づいています。

リスク指標の詳細については、次のトピックを参照してください。

- Citrix Content Collaboration のリスク指標
- NetScaler Gateway リスク指標
- Citrix Virtual Apps and Desktops および Citrix DaaS リスク指標

2021 年 1 月 20 日

修正された問題

- オンプレミスの StoreFront を使用するアプリとデスクトップのデータソースでは、StoreFront 展開環境は正常に接続されていますが、データ処理は失敗します。

  [CAS-46656]

2021 年 1 月 19 日

修正された問題

- カスタムリスク指標ページで、検索フィールドの無効な条件を修正した後、[**Estimate Trigger**] リンクが応答しません。

  たとえば、クライアント *IP = 10.10.10.10* という無効な条件を入力するとします。この条件を修正し、*client-IP =”10.10.10.10*”と入力すると、[トリガーの推定] リンクが応答しません。

  回避策：カスタムインジケータページを更新し、有効な条件でカスタムインジケータを作成します。

  [CAS-46316]

2021 年 1 月 13 日

新機能

Splunk 向けの **Citrix Analytics** アドオンの新しいバージョンが利用可能になりました　Splunk の Citrix Analytics アドオンバージョン 2.1.0 が利用可能になりました。ダウンロードページに移動して 、ファイルをダウンロードします。

Splunk クラウド入力データマネージャー **(IDM)** と **Splunk 8.1 64** ビットのサポートを追加　セキュリティ向け Citrix Analytics を Splunk クラウド IDM および Splunk 8.1 64 ビットと統合できるようになりました。詳細については、「Splunk 統合」を参照してください。

非推奨のサポート

Splunk 7.1 64 ビットのサポートを削除しました　セキュリティ向け Citrix Analytics を Splunk 7.1 64 ビットと統合できなくなりました。サポートされている Splunk のバージョンについては、「Splunk 統合」を参照してください。

2021 年 1 月 11 日

修正された問題

- [Virtual Apps and Desktops] サイトカードで、ラベル [サポートされているクライアントユーザー] の名前が [ユーザーから受信したイベント] に変更されます。「サポートされていないクライアントユーザー」というラベルの名前が「ユーザーからのイベントを受信できません」に変更されます。

  [CAS-44773]

2020 年 12 月 17 日

新機能

事前構成されたカスタムリスク指標とポリシーを使用して、異常な場所からのアクセスをブロックする（ジオフェンシング） Citrix は、事前構成されたカスタムリスク指標のリストと、Citrix インフラストラクチャのセキュリティを監視するのに役立つポリシーを提供します。これらのインジケーターとポリシーを使用すると、通常の運用国以外の国からのユーザーアクセスをブロックできます。デフォルトでは、国は「米国」に設定されています。ジオフェンシングに必要な国を設定できます。

以下は、事前構成されたカスタムリスク指標とポリシーです。

- CVAD-セッションがジオフェンスの外で開始されました
- GW-ジオフェンスクロッシング
- CCC-ジオフェンス交差点
- ジオフェンス外でのセッション開始

詳細については、「事前構成されたカスタムリスク指標とポリシー」を参照してください。

アクセスした場所をユーザー応答メールで表示する ユーザーデバイスの IP アドレスの代わりに、ユーザー応答メールには、過去 15 分間にユーザーがアクセスしたすべての場所が表示されるようになりました。場所は、<City>,<Country><!--NeedCopy--> の形式で表示されます。都市または国が利用できない場合、対応する値は「不明」と表示されます。

詳細については、「ユーザー応答のリクエスト」を参照してください。

名前が変更された **Content Collaboration** リスク指標-新しい場所からの初回アクセス Citrix Content Collaboration リスク指標の［新しい場所からの初回アクセス］は、［異常な場所からのアクセス］という名前に変更されます。

詳細については、「異常な場所からのアクセス」を参照してください。

廃止された機能

リスク指標のフィードバック　リスク指標フィードバックメカニズムが削除されます。Content Collaboration のリスクインジケータ-異常な場所からのアクセスが誤ってトリガーされた場合、それを誤検知として報告してフィードバックを提供することはできなくなります。

2020 年 12 月 7 日

新機能

潜在的なデータ漏洩リスク指標の改善　リスク指標には、次の機能強化が加えられています。

- **WHAT HAPPENED** セクションの情報が更新されます。時刻形式は、一貫性を維持するために更新されます。
- デバイスの位置情報がイベントリストに表示されます。

リスク指標の詳細については、「データの漏洩の可能性」を参照してください。

Content Collaboration リスク指標の改善-新しい場所からの初回アクセス　ユーザーリスクタイムラインで、[新しい場所からの初回アクセス] を選択して、次の情報を表示します。

- サインイン場所: ユーザーがサインインした通常の場所と通常とは異なる場所の地理的マップビューを表示します。
- 通常の場所からのサインイン数-過去 **30** 日間: ユーザーが過去 30 日間にサインインした通常の場所の上位 6 つの円グラフビューを表示します。また、これらの場所からのサインインイベントの数も表示されます。
- 異常な場所のイベントの詳細: ユーザーの異常な場所からのサインインイベントのリストを提供します。

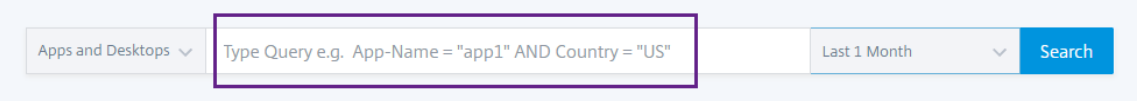
リスク指標の詳細については、「新しい場所からの初回アクセス」を参照してください。

2020 年 11 月 30 日

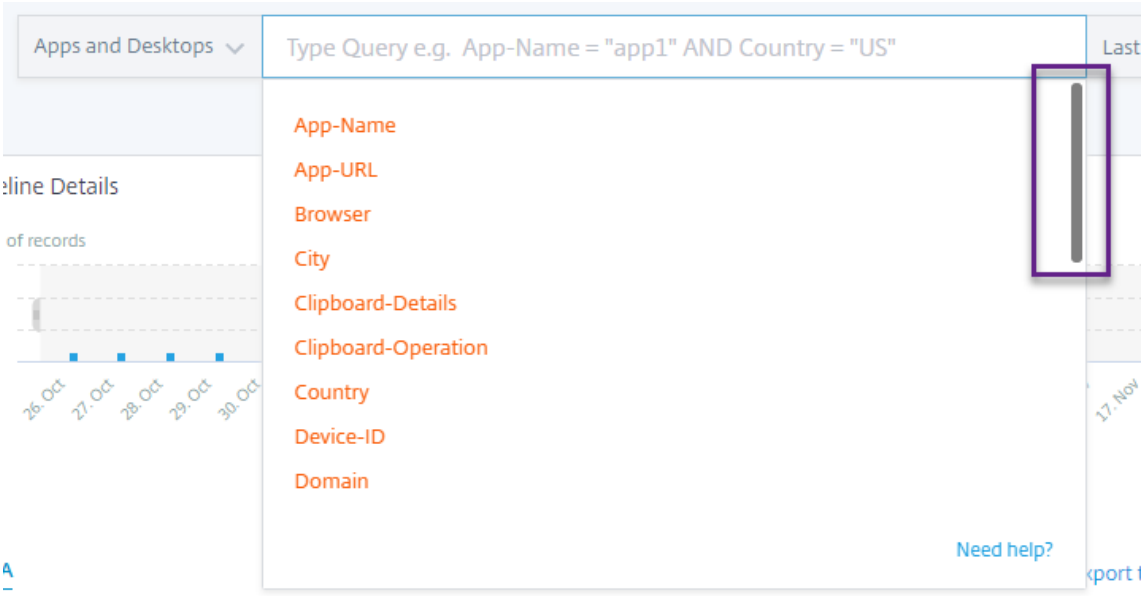
新機能

セルフサービス検索ページの改善　セルフサービス検索ページの使いやすさを向上させるために、次の改善が行われました。

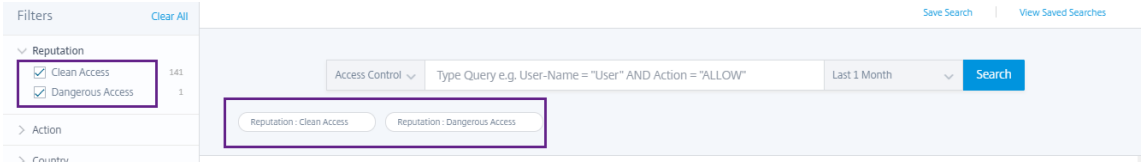
- 検索ボックスには、独自のクエリの入力方法を示すクエリの例が表示されます。



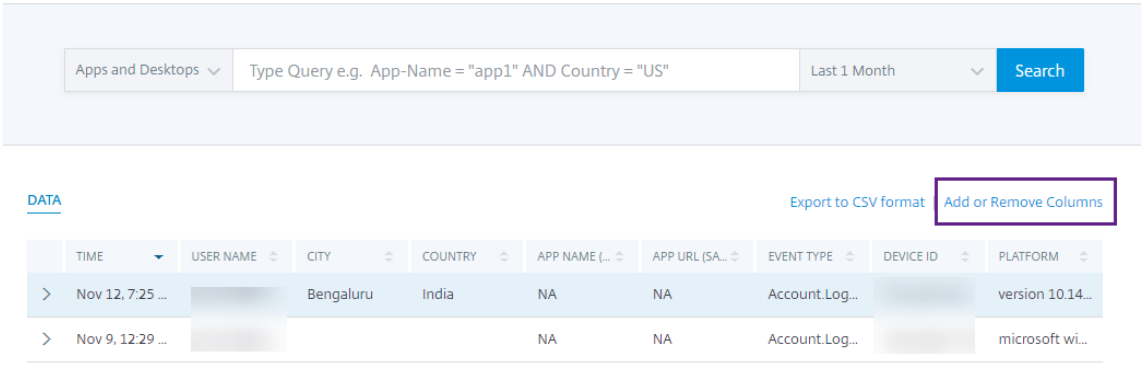
- macOS では、寸法リストのスクロールバーがデフォルトで表示されるようになりました。



- 適用されたフィルターがチップとして表示されるようになりました。



- [列の追加または削除] ラベルが [**+**] アイコンに置き換わります。



詳細については、「セルフサービス検索」を参照してください。

ポリシーの改善　［ポリシー］ページに、正常に検出され、Citrix Analytics に接続されたデータソースに関連付けられたポリシーが表示されます。このページには、未検出のデータソースに対して条件が定義されているポリシーは表示されません。すでに接続されているデータソースのデータ処理をオフにしても、**[**ポリシー**]** ページの既存のポリシーには影響しません。

詳細については、「ポリシーとアクションの構成」を参照してください。

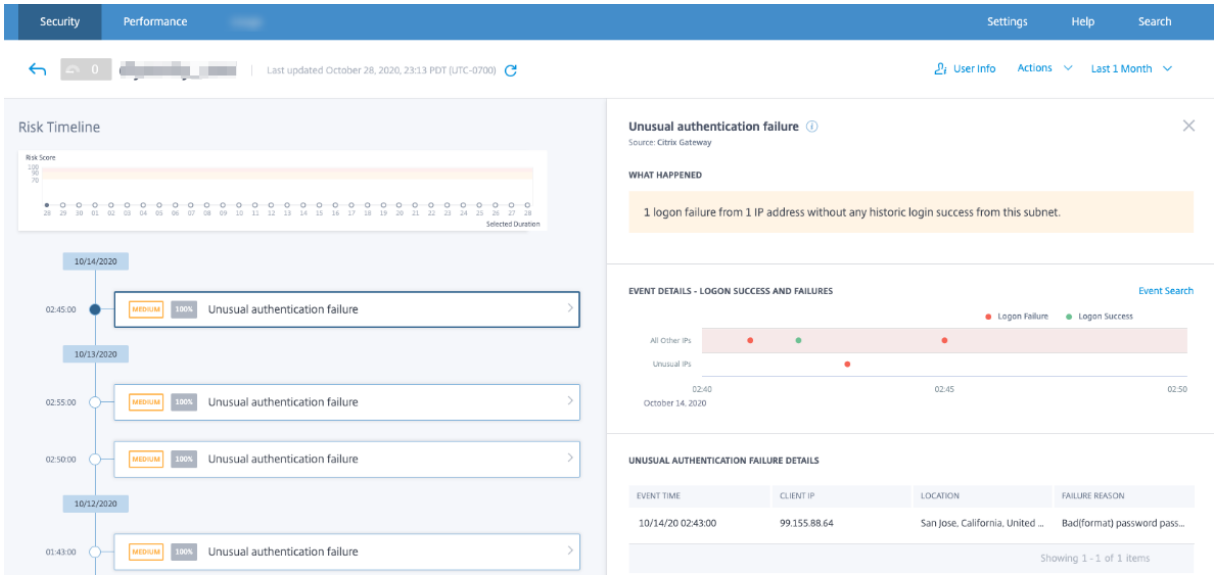
2020 年 11 月 04 日

新機能

異常な認証失敗**-NetScaler Gateway** リスク指標　Citrix Analytics は、ユーザーが異常な IP アドレスからのログオンに失敗したときにアクセスベースの脅威を検出し、異常な認証失敗リスク指標をトリガーします。

このリスク指標は、組織内のユーザーが通常の動作に反する異常な IP アドレスからのログオンに失敗したときにトリガーされます。

詳しくは、「NetScaler Gateway リスク指標」を参照してください。



2020 年 10 月 20 日

修正された問題

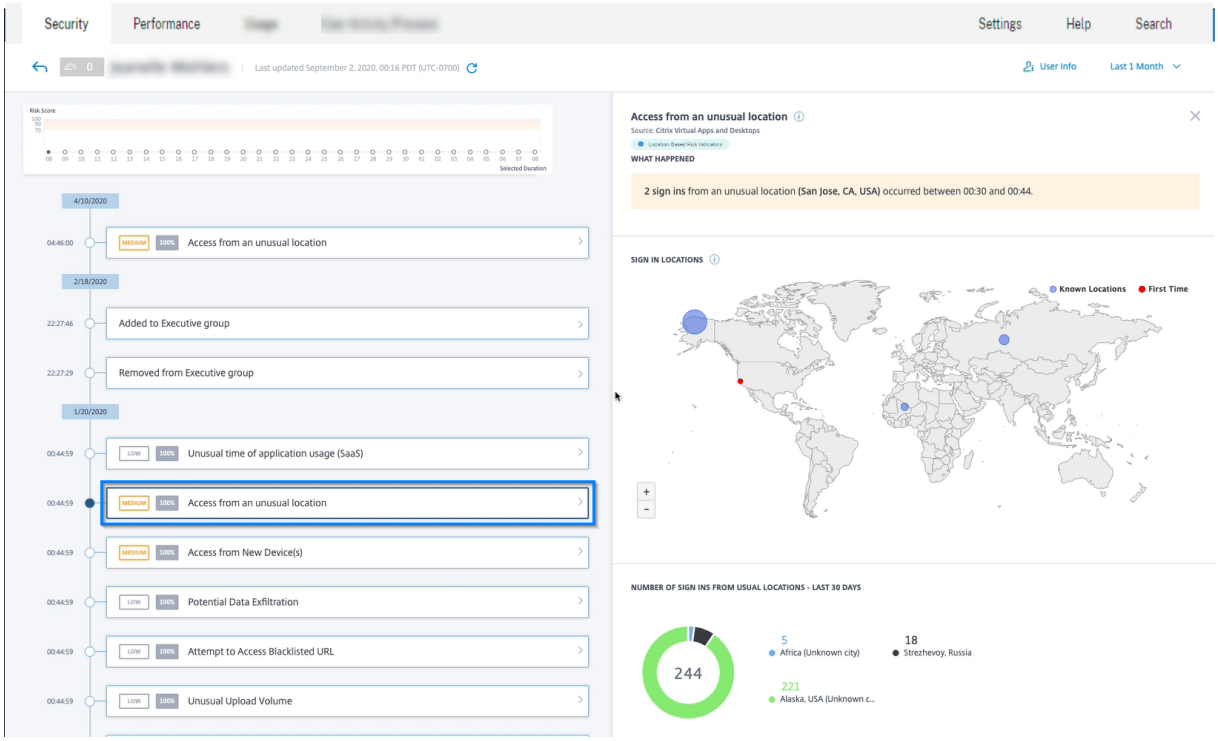
- リスクインジケータ [ログオフ] ** ユーザーアクションが適用された新しいデバイスからの初回アクセスが期待どおりに機能しません ** 。

  [CAS-40743]

2020 年 10 月 15 日

新機能

異常な場所からのアクセス—**Citrix Virtual Apps and Desktops** および **Citrix DaaS** リスク指標　Citrix Analytics は、Citrix Workspace からの異常なサインインに基づいてアクセスベースの脅威を検出し、対応するリスク指標をトリガーします。



詳しくは、「Citrix Virtual Apps and Desktops」および「Citrix DaaS リスク指標」を参照してください。

共有リンクダッシュボードの機能強化

- [共有 URL] 列は、[共有 ID] 列に置き換えられました。各共有 URL は、共有 ID で識別されるようになりました。
- ダッシュボード上の時間選択が削除されます。このダッシュボードには、選択した期間ではなく、アクティブな状態から期限切れの状態までのすべての共有リンクが表示されます。
- すべての共有リンクは、最初にアクティブなリンク、次に期限切れのリンクの順にソートされます。既定では、リスク指標の数が最も高い共有リンクがリストの一番上に表示されます。
- 危険なリンクには、危険な動作を持つアクティブなリンクが表示されるようになりました。期限切れのリンクは表示されません。既定では、リスク指標の数が最も高い危険なリンクがリストの一番上に表示されます。
- [危険な共有リンク] カードと [すべての共有リンク] カードのトレンドビューが削除されます。

詳細については、「共有リンク」ダッシュボードを参照してください。

リンクのリスクタイムラインの拡張機能の共有　リスクタイムラインに、共有 URL の代わりに共有 ID が表示されるようになりました。詳細については、「リンクのリスクタイムラインを共有する」を参照してください。

廃止された機能

サポートされていないオペレーティングシステム **(OS)** リスク指標を持つデバイスからのアクセスは非推奨　Citrix Virtual Apps and Desktops のリスク指標- サポートされていないオペレーティングシステム（**OS**）を搭載したデバイスからのアクセスは廃止されました。このインジケーターに関連する履歴データのみを表示できます。

この非推奨の一部として、次の変更が適用されます。

- Analytics はこれらのリスク指標を生成しなくなりました。
- Analytics は、これらのリスク指標を条件とするポリシーを生成しなくなりました。
- これらのリスク指標を条件とするデフォルトのポリシーは有効になりません。

詳しくは、「Citrix Virtual Apps and Desktops」および「Citrix DaaS リスク指標」を参照してください。

2020 年 **9** 月 **10** 日

新機能

StoreFront のチェックリスト　Citrix Analytics で、StoreFront 構成ファイルをダウンロードする前に満たす必要のある前提条件の一覧が表示されるようになりました。チェックリストを確認し、すべての最小要件が選択されていることを確認します。最小要件が選択されていない場合、設定ファイルをダウンロードできません。詳しくは、「Citrix Virtual Apps and Desktops のデータソース」を参照してください。

セルフサービス検索**-NOT EQUAL (!=)** 演算子のサポート　これで、次の機能のクエリの演算子で NOT EQUAL (!=) 演算子を使用できます (!=)：

- カスタムリスクインジケータ
- セルフサービス検索

この演算子は、次の条件で使用できます。

データソース	ディメンション
Content Collaboration	国、都市、クライアント OS
アクセス制御	国、都市、アクション、URL、URL、カテゴリ、レピュテーション、ブラウザ、OS、デバイス
アプリケーションとデスクトップ	国、都市、アプリ名、クリップボード操作、ブラウザ、OS
Gateway	認証段階、クライアント IP

演算子を使用して、「Country!= XYZ」を選択し、ユーザーのリストを表示します。次に、[ウォッチリストに追加]、[管理者に通知]、[ユーザーを無効にする] などのアクションを適用するポリシーを作成します。

また、指定したデータソースのセルフサービス検索で、オペレータを使用して、ユーザーイベントをフィルタリングすることもできます。

クエリのディメンションの値を入力する際には、データソースのセルフサービス検索ページに表示されている正確な値を使用します。寸法値では、大文字と小文字が区別されます。

2020 年 **9** 月 **08** 日

新機能

ユーザー相関関係　Analytics は、さまざまなデータソースから検出されたユーザーを関連付けるようになりました。このメカニズムにより、検出されたユーザーのリストから重複するユーザーのほとんどが排除されます。Analytics で検出されたユーザーは、データソースとリスク指標とともに一意のユーザーのリストを表示するようになりました。

たとえば、ユーザー「Joe Smith」は、データソースに基づいて複数のユーザー識別子 (JosephSM < joe.smith@citrix.com > と joe.smith) を持つことができます。Analytics は、このユーザーを一意の識別子名で識別するようになりました。その他すべてのユーザー ID は相関しており、さまざまなデータソースから Joe Smith に対して受信されたイベントは、この一意の名前にリンクされます。
詳細については、「検出されたユーザー」を参照してください。

修正された問題

「アクション」 (Actions) リストで、アクションオプションを選択して「適用」**(Apply**) をクリックすると、エラーメッセージが表示されます。

[CAS-39914]

2020 年 **8** 月 **11** 日

解決された問題

- Microsoft Graph セキュリティを Citrix Analytics 統合することはできません。この問題は、Microsoft ポータルが Citrix Analytics にリダイレクトできなかったために発生しました。

[CAS-38021]

2020 年 7 月 31 日

解決された問題

- カスタムリスク指標の [**Estimated Triggers**] オプションは、過去 1 日のカスタムリスク指標インスタンスを予測しません。

[CAS-38129]

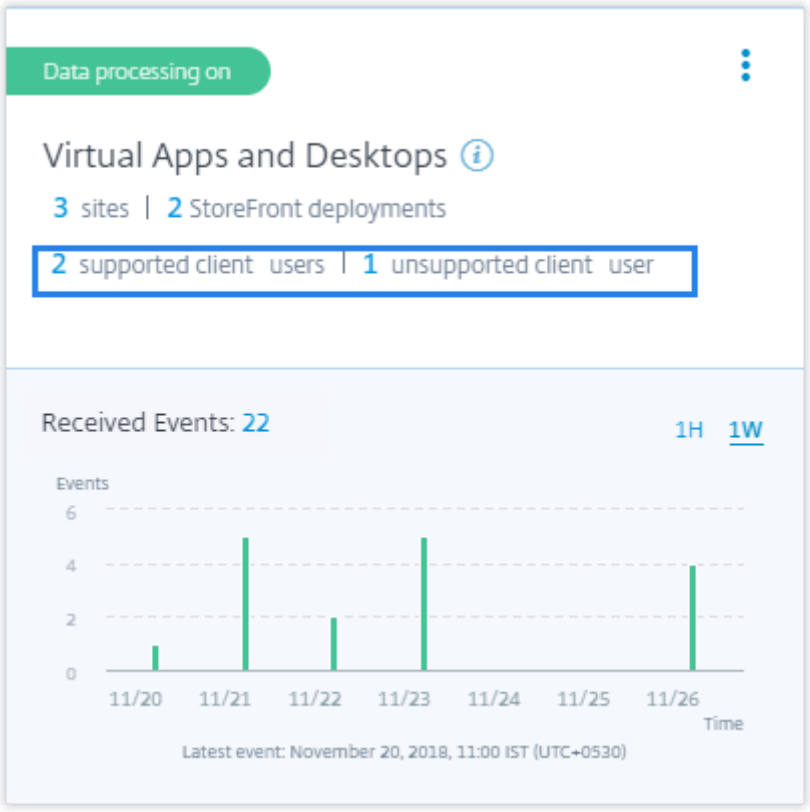
2020 年 7 月 09 日

新機能

Virtual Apps and Desktops のサイトカードには、サポートされているクライアントとサポートされていないクライアントを持つユーザーが表示されます　サイトカードで、エンドポイントで Citrix Workspace アプリまたは Citrix Receiver クライアントのサポートされているバージョンとサポートされていないバージョンを使用しているユーザーの数を表示できるようになりました。

- サポートされているクライアントのユーザ数をクリックして、検出されたすべてのユーザを表示する [ユーザ（**User** ）] ページを表示します。
- サポートされていないクライアントのユーザー数をクリックして、CSV ファイルをダウンロードします。このファイルには、ユーザーとそのサポートされていないクライアントバージョンが一覧表示されます。Analytics は、サポートされていないクライアントからユーザーイベントを受信しないため、検出されたユーザーとしてユーザーを追加しません。CSV ファイルを使用して、Analytics が動作に関するセキュリティ上の洞察を提供できるように、クライアントをサポートバージョンにアップグレードする必要があるユーザーを特定します。

サポートされているクライアントの一覧を表示するには、「Citrix Virtual Apps and Desktops」および「Citrix DaaS データソース」を参照してください。



異常なロケーションリスク指標からのアクセス

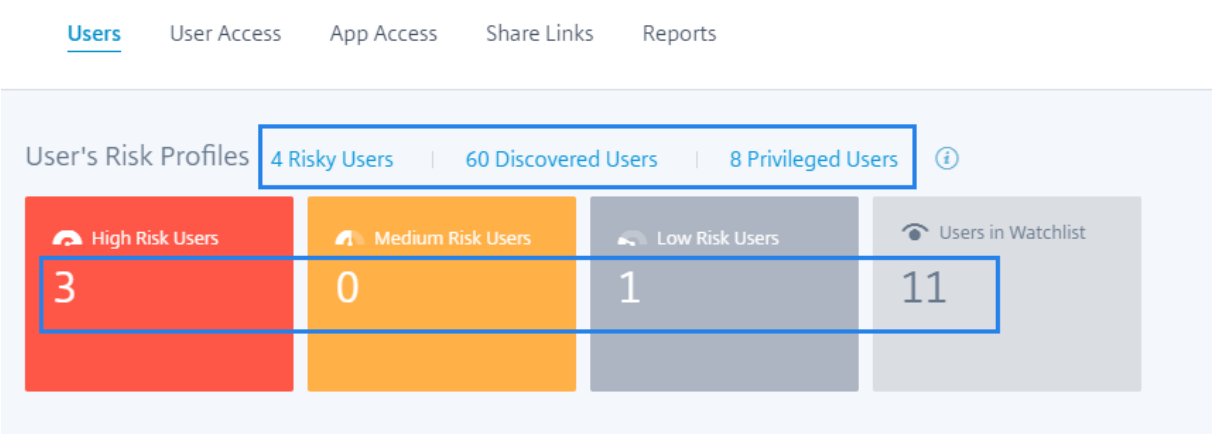
- NetScaler Gateway リスク指標新しい場所からの初回アクセスは、異常な場所からのアクセスという名前に変更されます **。
- ユーザーリスクのタイムラインでは、地理的なマップと円グラフがイベントの詳細セクションに導入されています。
  - サインイン場所: このセクションには、ユーザーの通常および異常な場所の地理的マップビューが表示されます。通常の場所と通常とは異なる場所は、ジオマップの右上のセクションにカラーコードで示されます。Geo マップをズームして、位置を詳しく見ることができます。

- 通常の場所-過去 **30** 日間: このセクションには、ユーザーがサインインした通常の場所の上位 6 つを示す円グラフが表示されます。各場所には異なるカラーコードが付いています。セクションを場所順に並べ替えて、選択した場所の詳細を表示することができます。

詳細については、「異常な場所からのアクセス」を参照してください。

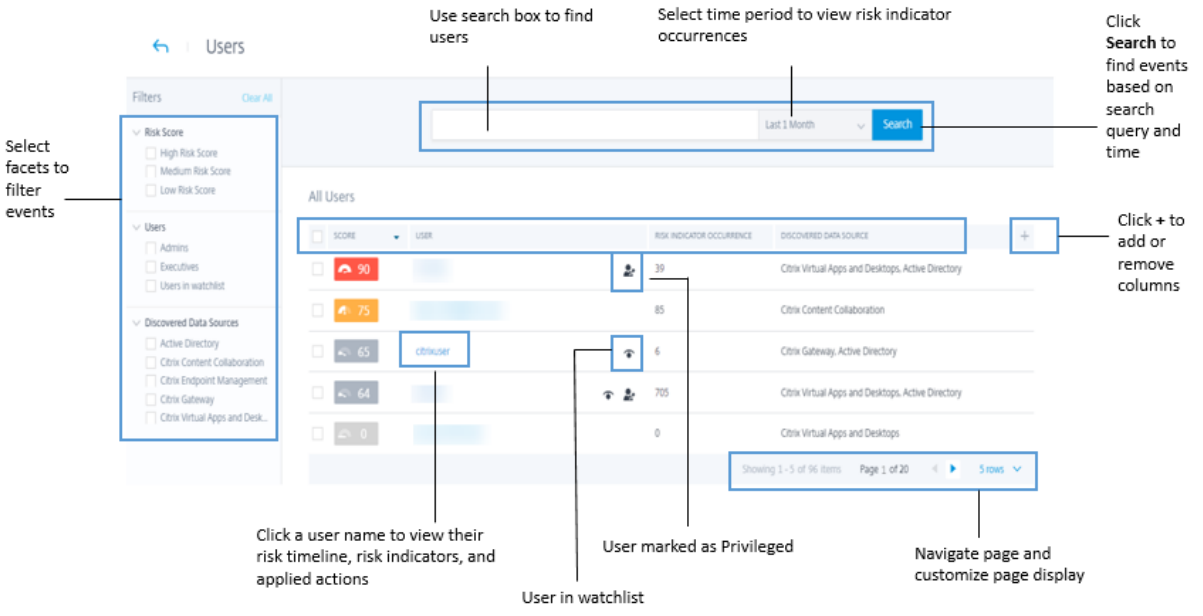
ユーザーダッシュボードデータ　[ユーザー] ダッシュボードおよび [ユーザー] ページで選択した期間に関係なく、過去 13 か月間の危険なユーザー、検出されたユーザー、特権ユーザー、およびウォッチリスト内のユーザーの数が表示されます。期間を選択すると、リスク指標の発生が変化します。

詳細については、「ユーザーダッシュボード」を参照してください。



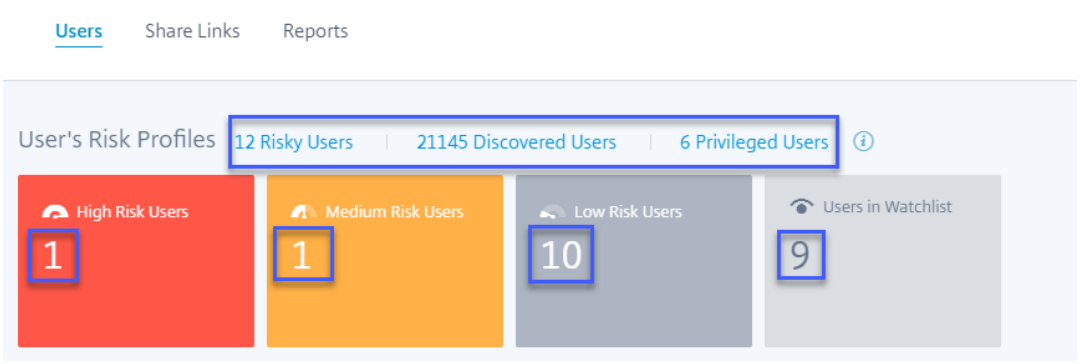
再設計された **[ユーザー]** ページ　[ユーザー] ページが強化され、ユーザーエクスペリエンスが向上しました。ユーザーリスクスコア、データソース、およびユーザータイプに基づいて、ユーザーイベントの統合サマリーを提供します。

より焦点を絞った検索をサポートするために、[ユーザー] ページの左ペインに [フィルター] セクションがあり、上部に検索バーがあります。事前設定された時間またはカスタマイズされた時間範囲のユーザイベントを検索できます。



[ユーザー] ページを表示するには、次の手順に従います。

- [セキュリティ] **>** **[ユーザー]** に移動して [ユーザー] ダッシュボードを表示し、次の操作を行います。
  - 次のリンクまたはカードのいずれかをクリックします。

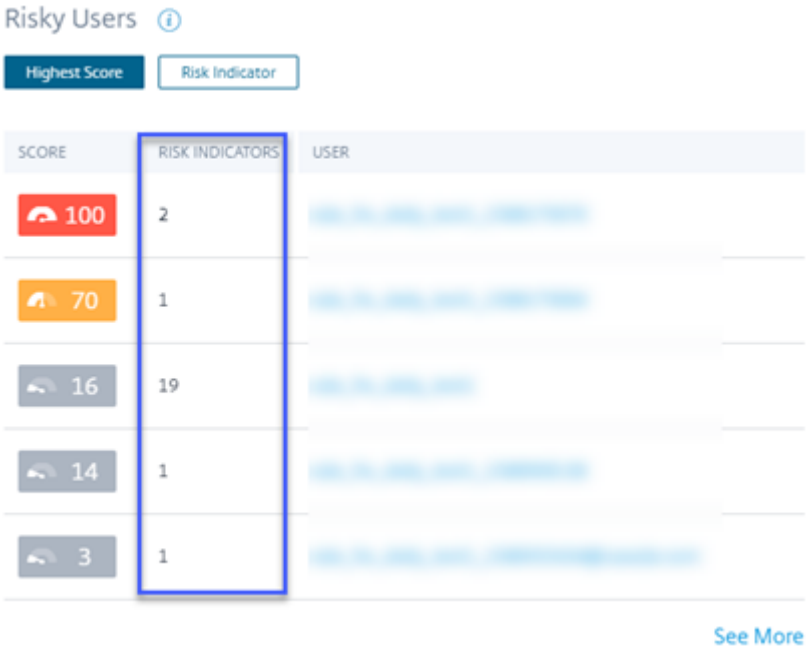


  - [危険なユーザー] ウィンドウで、[詳細を表示] をクリックします。
  - [ウォッチリストのユーザー] ペインで、[詳細を表示] をクリックします。
  - [管理者ユーザー] ペインで、[詳細を表示] をクリックします。
- **[設定] > [データソース] > [セキュリティ]** に移動します。任意のデータソースサイトカード上のユーザー数をクリックします。

詳細については、「ユーザーダッシュボード」を参照してください。

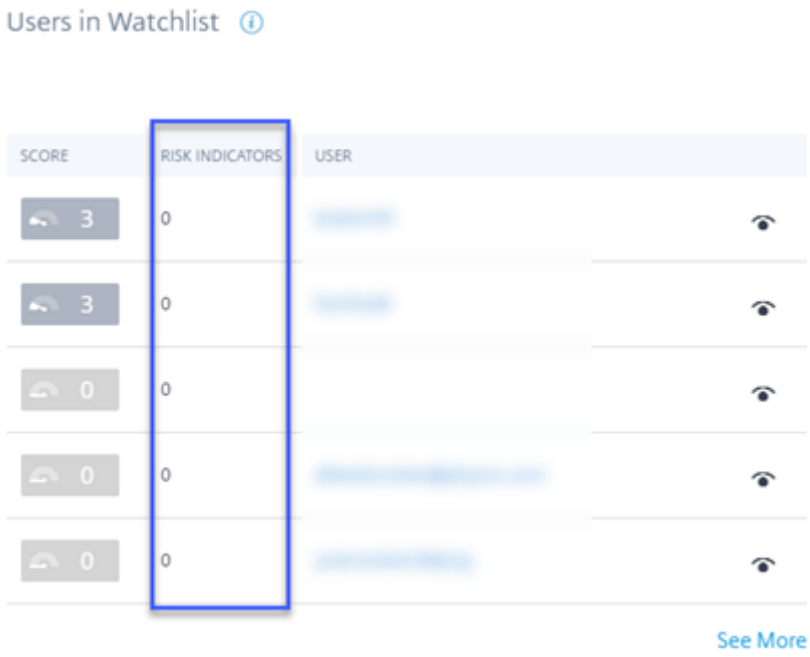
[危険なユーザー] ペインの機能強化　[変更] 列が [リスク指標] 列に置き換えられます。[リスク指標] 列には、特定の期間におけるユーザーのリスク指標の発生総数が表示されます。

詳細については、「危険なユーザー」を参照してください。



[ウォッチリスト] ペインのユーザーの機能強化　[変更] 列が [リスク指標] 列に置き換えられます。[リスク指標] 列には、特定の期間におけるユーザーのリスク指標の発生総数が表示されます。

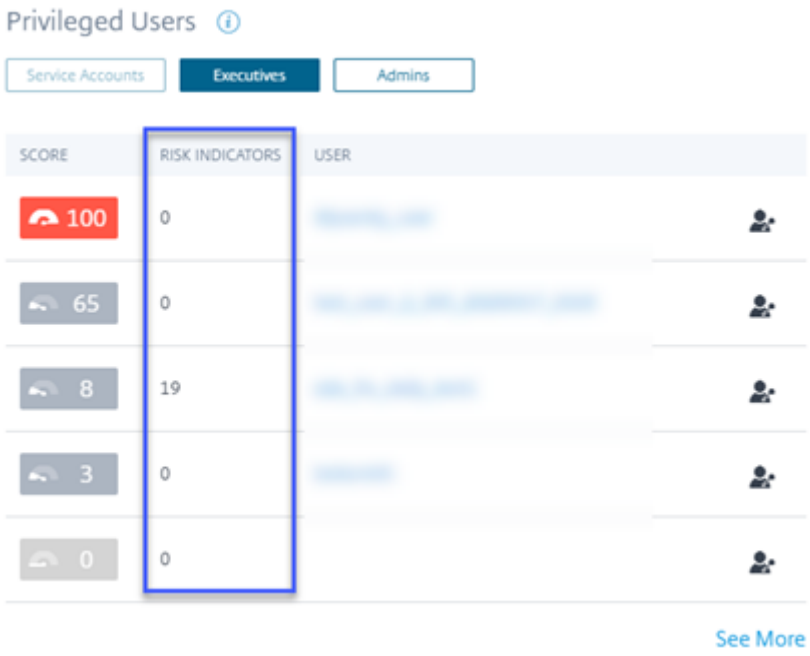
詳細については、ウォッチリスト内のユーザーを参照してください。



[特権ユーザー**]** ペインの強化

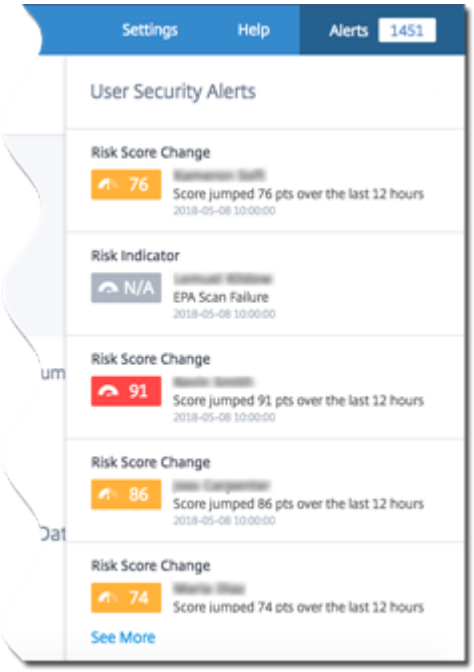
- [変更] 列が [リスク指標] 列に置き換えられます。[リスク指標] 列には、特定の期間におけるユーザーのリスク指標の発生総数が表示されます。
- [詳細を表示] をクリックして、[ユーザー] ページを表示します。管理者およびエグゼクティブ特権ユーザのリストを表示する [ユーザ（Users）] ページ。このページでは、ユーザーを特権ユーザーとして追加または削除できます。

詳細については、「特権ユーザー」を参照してください。



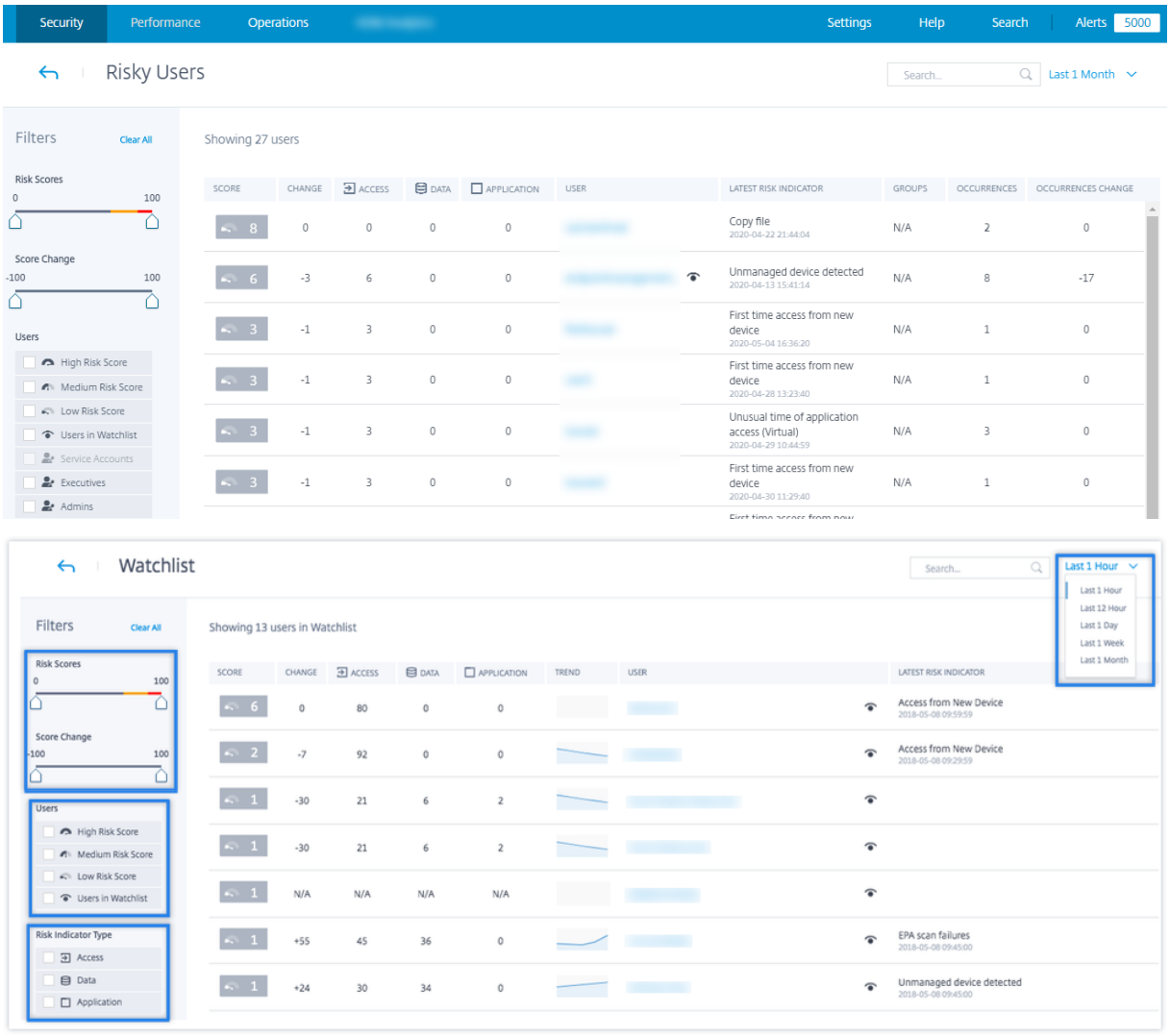
廃止された機能

アラート　アラート機能は廃止され、Analytics ユーザーインターフェイスでは使用できなくなりました。

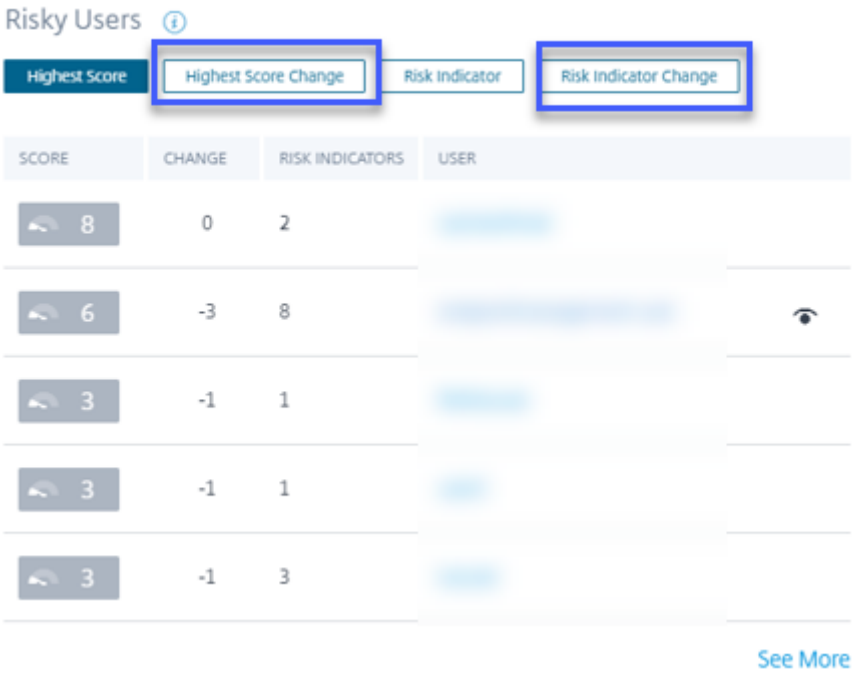


危険なユーザーとウォッチリストのページ　** 危険なユーザーページとウォッチリストページは廃止されました **。これらは、すべての危険なユーザーイベントとウォッチリスト内のユーザーをまとめたユーザーページに置き換え

られます。

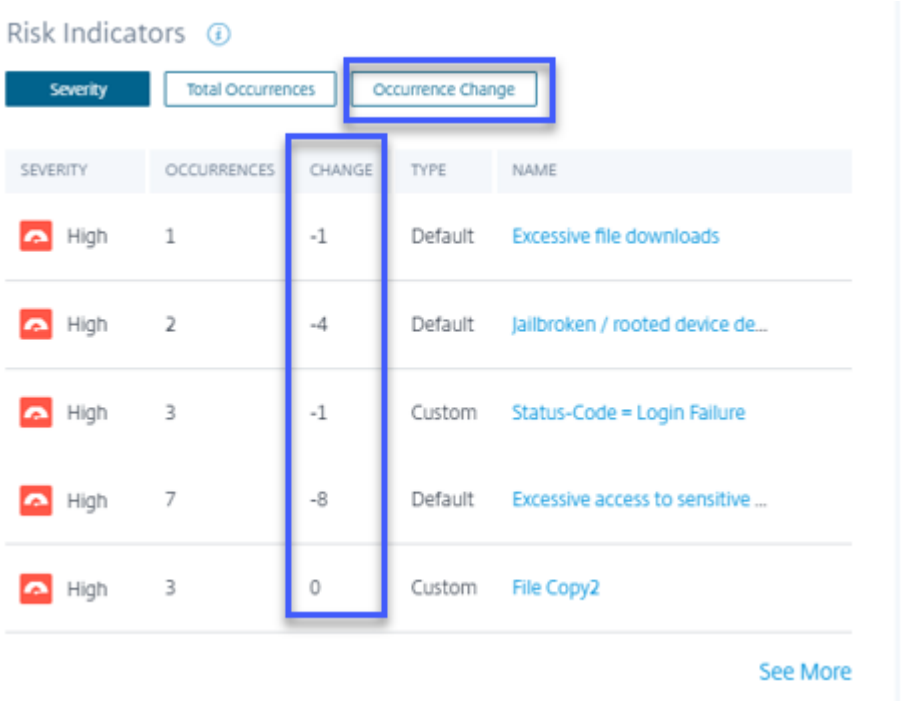


[危険なユーザー] ペイン　[最高スコアの変更] タブと [リスク指標の変更] タブが [危険なユーザー] ペインから削除されます。

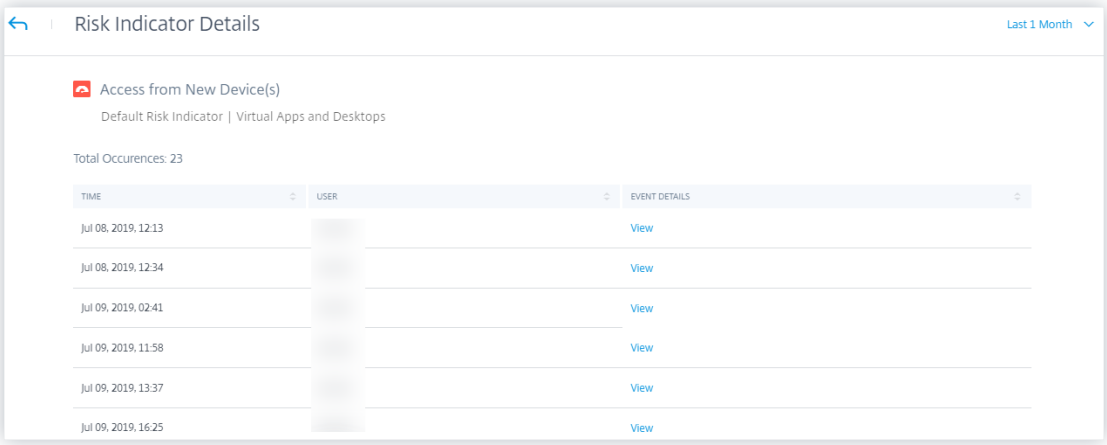


[リスク指標**]** ペイン

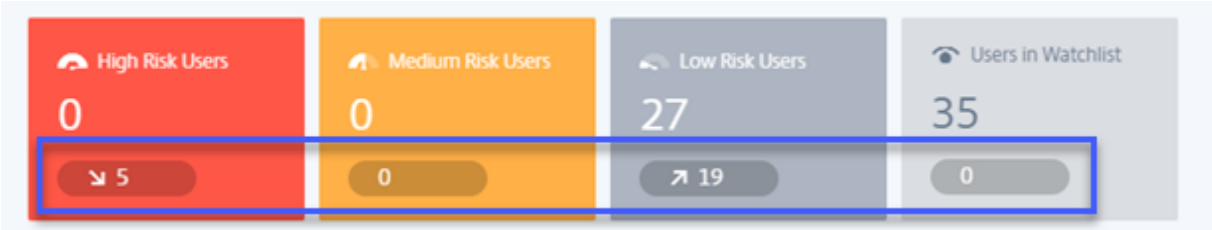
- [オカレンスの変更] タブと [変更] 列が削除されます。



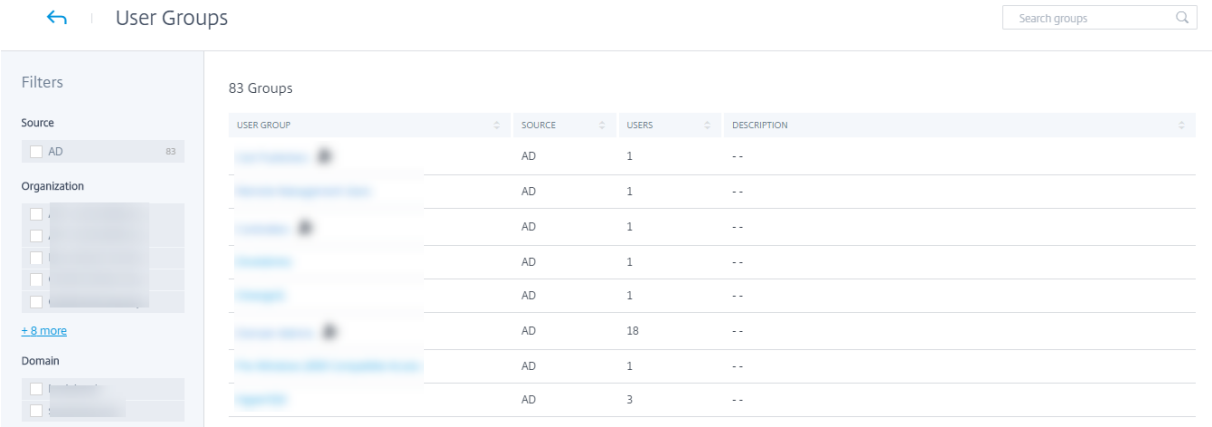
- [リスク指標の詳細] ページは廃止されました。以前は、このページは、[リスク指標] ウィンドウまたは [リスク指標の概要**]** ページでリスク指標を選択したときに表示されていました。



トレンドビュー　[ユーザー] ダッシュボードで、ユーザー数のトレンドビューが、[高リスクユーザー]、[中リスクユーザー]、[** 低リスクユーザー]、および **[ウォッチリストのユーザー] カードから削除されます。



[ユーザーグループ] ページ　[設定] オプションの下の [ユーザーグループ] ページは廃止されました。ユーザーグループを特権グループとして追加または削除できなくなりました。ただし、個々のユーザーを特権ユーザーとして追加または削除できます。詳細については、「特権ユーザー」を参照してください。



2020 年 6 月 26 日

廃止された機能

アプリケーションアクセスの異常な時間 **(**仮想**/SaaS)** リスク指標は非推奨　Citrix Virtual Apps and Desktops のリスク指標- アプリケーションアクセスの異常時間（仮想）および異常なアプリケーションアクセス時間（**SaaS**）は廃止されました。これらの指標に関連する履歴データのみを表示できます。

この非推奨の一部として、次の変更が適用されます。

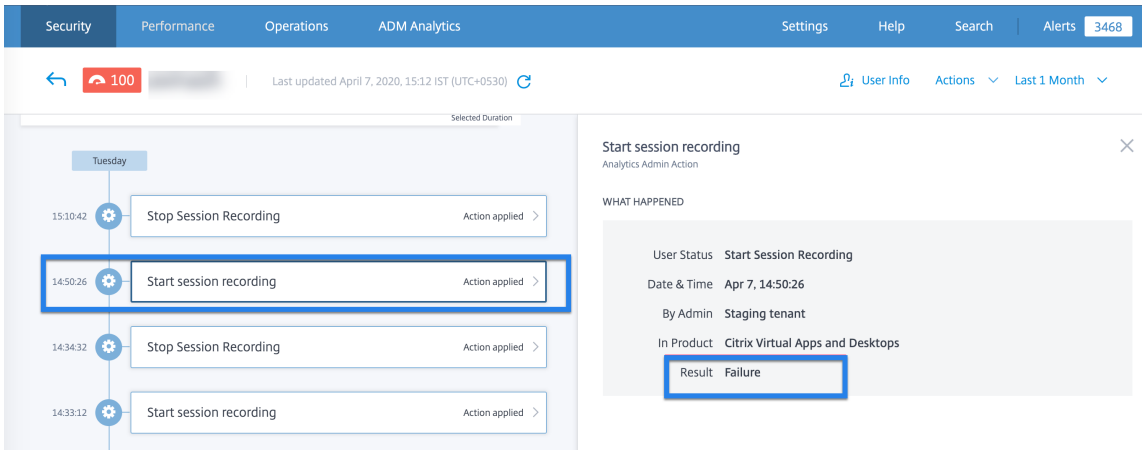
- Analytics はこれらのリスク指標を生成しなくなりました。
- Analytics は、これらのリスク指標を条件とするポリシーを生成しなくなりました。
- これらのリスク指標を条件とするデフォルトのポリシーは有効になりません。

詳しくは、「Citrix Virtual Apps and Desktops」および「Citrix DaaS リスク指標」を参照してください。

2020 年 6 月 02 日

解決された問題

- ユーザーリスクタイムラインでは、Virtual Apps and Desktops のアクションのステータス（ポリシーベースまたは手動で適用）は、アクションがユーザーアカウントに正常に適用された場合でも「失敗」と表示されます。たとえば、[セッションの録画の開始] アクションはユーザーアカウントに正常に適用されますが、結果は「失敗」と表示されます。[CAS-32773]



2020 年 5 月 11 日

解決された問題

- 一部のユーザーの場合、ポリシーベースのアクションはトリガーされず、ポリシー強制モードを適用できません。この問題は、顧客 ID が小文字でない場合に発生します。

[CAS-34209], [CAS-34141]

- 一部のユーザーのカスタムリスク指標を作成できません。この問題は、顧客 ID が小文字でない場合に発生します。

  [CAS-34139]

2020 年 4 月 29 日

解決された問題

- Citrix Virtual Apps and Desktops のリスク指標に適用されたアクションは有効になりませんが、Analytics はアクションが正常に適用されたことを示すメッセージを表示します。この問題は、Citrix Virtual Apps and Desktops 7 1912 バージョンで観察されます。

  [CAS-31544]

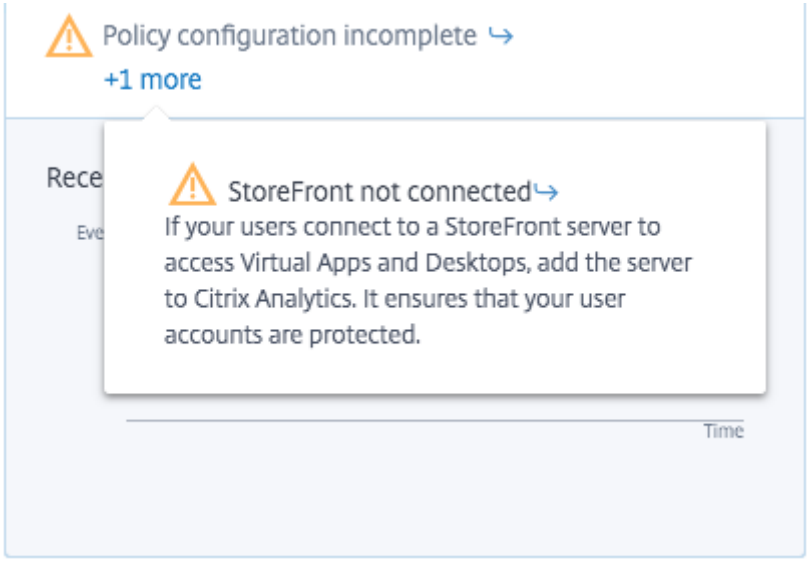
2020 年 4 月 02 日

新機能

StoreFront が追加されていない場合はデータ処理を無効にする　StoreFront をオンボーディングしていない場合、［設定］>［データソース］>［セキュリティ］>［**Virtual Apps and Desktops** ］データソースサイトカードで、［データ処理を有効にする］ボタンが有効になりません。サイトカードに **StoreFront** が接続されていないという警告メッセージが表示されます。Analytics でデータを受信するアクティブなオンプレミスサイトがある場合は、StoreFront を Citrix Analytics にオンボーディングしたことを確認する必要があります。これにより、ユーザーアカウントが確実に保護されます。

［**Virtual Apps and Desktops** ］サイトカードで、縦方向の省略記号（⊠）を選択し、［**StoreFront** 展開環境の接続］をクリックします。表示される画面で、指示に従って StoreFront の構成を完了します。

詳しくは、「StoreFront を使用した Citrix Virtual Apps and Desktops のオンプレミスサイトのオンボード」を参照してください。



解決された問題

- Citrix Content Collaboration ユーザーの場合、ポリシーベースのアクションは、次の条件下で有効になりません。
  - カスタムリスク指標の条件が定義されている場合
  - ユーザーのリスク指標が生成されるまで

  [CAS-29226]

2020 年 **3** 月 **04** 日

解決された問題

- Gateway ユーザーが初めて Analytics にオンボードすると、**NetScaler ADC** が応答しないか、資格情報が正しくないというエラーが表示されます。再試行すると、「この **IP** アドレスのデバイスは既に存在します」というエラーが表示されます。

[CAS-31180]

2020 年 **2** 月 **20** 日

新機能

セキュリティ向け **Citrix Analytics** オファ　セキュリティ向け Citrix Analytics が個別のサブスクリプションで利用できるようになりました。

セキュリティ向け Citrix Analytics をサブスクライブして、このオファリングに固有のインサイトを取得できます。詳しくは、「導入」を参照してください。

リスクカテゴリダッシュボード　Citrix Analytics では、組織のセキュリティ側面に同様の影響を与えるリスクに基づいて、リスク指標の分類が導入されています。このダッシュボードには、直ちに対処する必要があるリスクエクスポージャーと重大なリスクの包括的なビューが表示されます。デフォルトのリスク指標の場合、Analytics はリスクエクスポージャーに基づいてリスクカテゴリを自動的に割り当てます。カスタムリスク指標の場合は、リスクエクスポージャーに基づいて適切なリスクカテゴリを選択する必要があります。

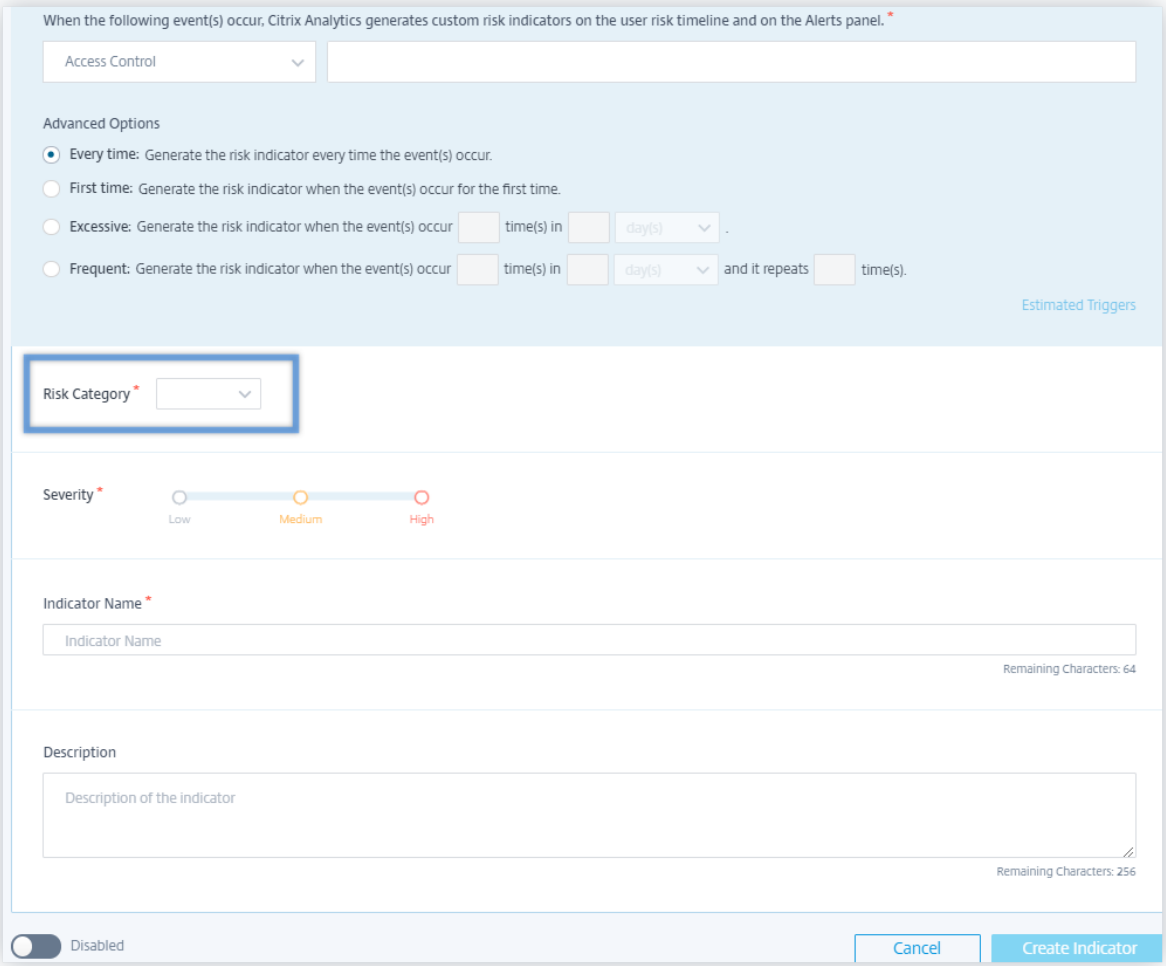
Analytics では、次のリスクカテゴリがサポートされています。

- データ流出
- インサイダーの脅威
- 侵害されたユーザー
- 侵害されたエンドポイント

詳細については、「リスクカテゴリ」を参照してください。

[カスタムインジケータ] ページの **[リスクカテゴリ]** 列　[リスクカテゴリ] 列は、[カスタムリスク指標] ページに導入されます。リスクエクスポージャーのタイプに基づいて、カスタムリスク指標のリスクカテゴリを選択できます。以前に作成したカスタムリスク指標は、リスクカテゴリを選択して変更すると、[リスクカテゴリ] ダッシュボードに表示されます。

詳細については、「カスタムリスク指標」を参照してください。



リスク指標名の変更　次のリスク指標名が変更されました。

[データソース]	旧名	新名称
Citrix Virtual Apps and Desktops および Citrix DaaS	異常なアプリケーション使用 (仮想)	アプリケーションアクセスの異常な時間 (仮想)
Citrix Virtual Apps and Desktops および Citrix DaaS	異常なアプリケーション使用 (SaaS)	アプリケーションアクセスの異常な時間 (SaaS)
Citrix Content Collaboration	過剰なログオン失敗	過剰な認証失敗
Citrix Content Collaboration	異常なログオンアクセス	新しい場所からの初回アクセス
Citrix Access Control	異常なダウンロードボリューム	過剰なデータのダウンロード
Citrix Gateway	ログオンの失敗	過剰な認証失敗
Citrix Gateway	認証の失敗	過度の認証の失敗

[データソース]	旧名	新名称
Citrix Gateway	異常なログオンアクセス	新しい場所からの初回アクセス

詳細については、「リスク指標」を参照してください。

解決された問題

- 一部のユーザーの場合、データソースが正常にオンボーディングされ、StoreFront が有効になっていても、Citrix Analytics は Virtual Apps and Desktops からデータを受信できません。[CAS-24134]
- Citrix Analytics は、Citrix Content Collaboration からダウンロードイベントを受信できません。したがって、次のリスク指標はトリガーされません。
  - 匿名の機密共有ダウンロード
  - 共有リンクのダウンロードが多すぎる
  - 機密ファイルへの過剰なアクセス
  - 過剰なファイルのダウンロード

  [CAS-29207]
- 新しくオンボーディングされたユーザーの場合、NetScaler Gateway リスク指標に適用される手動およびポリシーベースのアクションは有効になりません。[CAS-29029]
- 一部のユーザーは、[データソース] ページでサイトカードを表示できません。この問題は、キャッシュを再設定することで解決されます。[CAS-28781]

2020 年 **1** 月 **09** 日

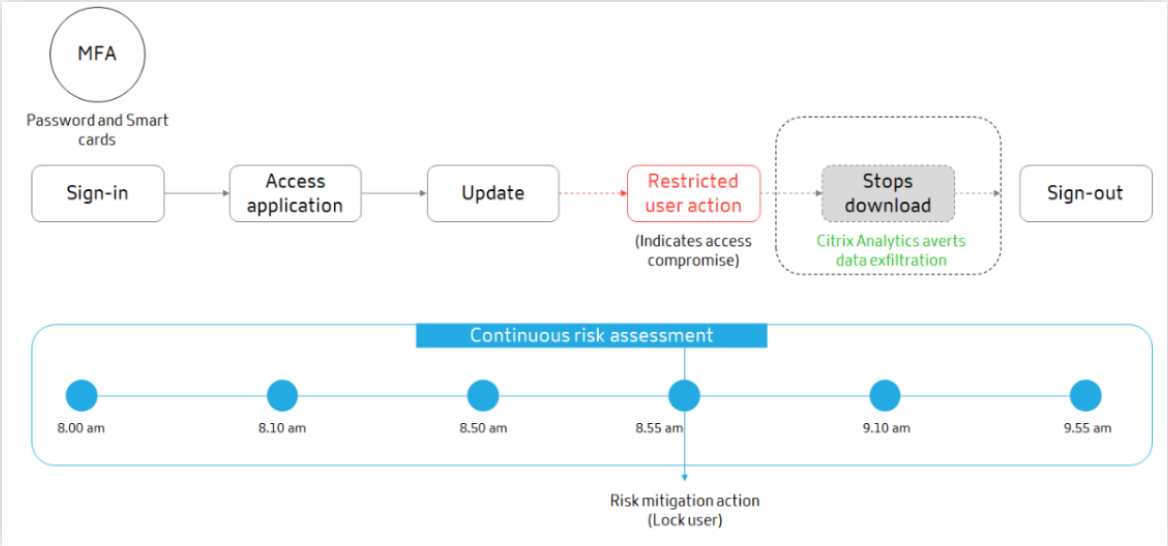
新機能

継続的なリスク評価　Citrix Workspace ユーザーが直面するいくつかの課題は、リモートアクセスは、データの漏洩、盗難、破壊行為、サービスの中断などのサイバー犯罪行為を通じて、機密データをセキュリティリスクにさらすことです。組織内の従業員もこの被害の一因になりそうです。

これらのリスクに対処するいくつかの方法は、多要素認証を実装し、短いサインインタイムアウトを強制することなどです。これらのリスクアセスメント手法は、より高いレベルのセキュリティを保証しますが、最初の検証後に完全なセキュリティを提供することはできません。

セキュリティの側面を強化し、ユーザーエクスペリエンスを向上させるために、Citrix Analytics は継続的なリスク評価のソリューションを導入しています。このソリューションは、ユーザープロファイルを継続的に監視し、危険なイベントが検出されたときにさまざまなアクションを実行するのに役立ちます。

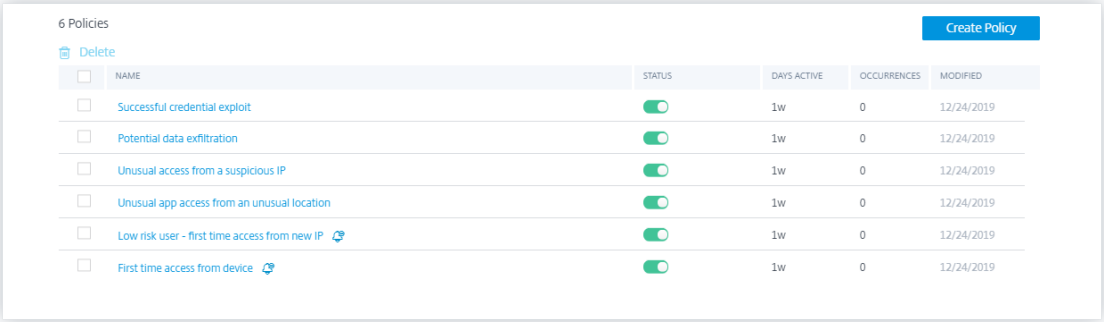
詳細については、「継続的なリスク評価」を参照してください。



ポリシー設定　Citrix Analytics は、ポリシー構成をより効率的に管理するのに役立ちます。次の機能を使用して、悪意のある攻撃からユーザーアカウントを保護できます。

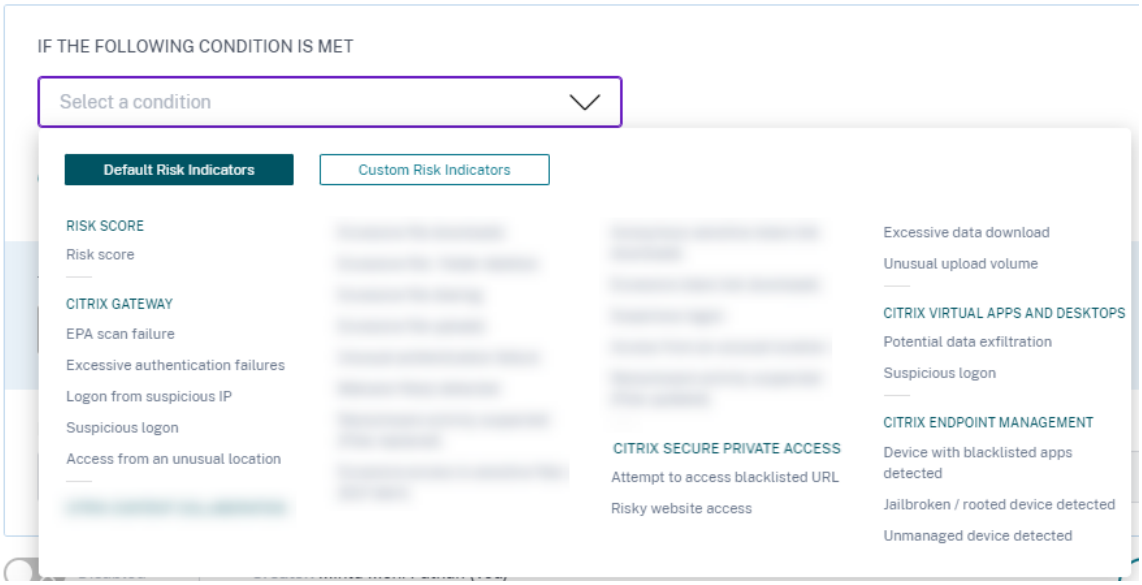
- デフォルトポリシー: Citrix Analytics は次のデフォルトポリシーをサポートしています。
  - 認証情報の不正利用の成功
  - データ流出の可能性
  - 疑わしい IP からの異常なアクセス
  - 通常の場所以外からの異常なアプリアクセス
  - 低リスクユーザー-新しい IP からの初回アクセス
  - デバイスからの初回アクセス

  デフォルトのポリシーは、要件に基づいて変更できます。

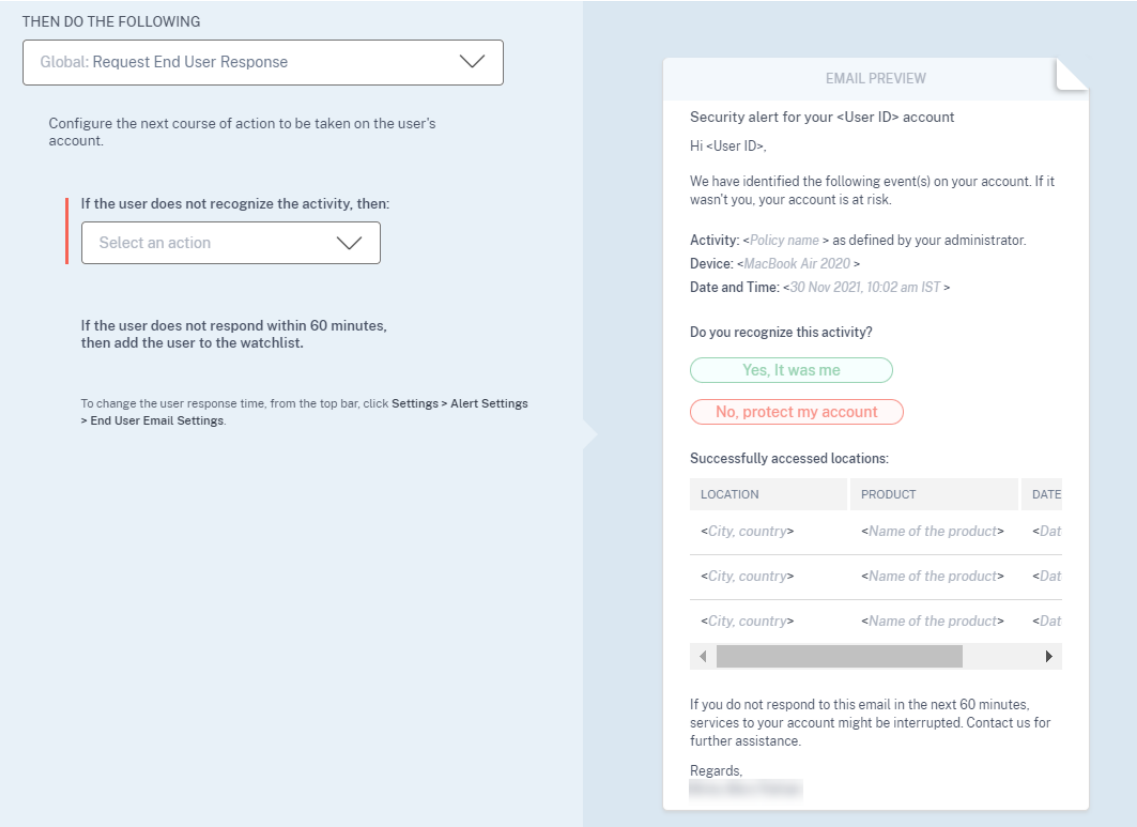


- 複数の条件: ポリシーには最大 4 つの条件を含めることができます。条件は、リスクスコアとリスク指標、またはその両方を組み合わせて設定できます。

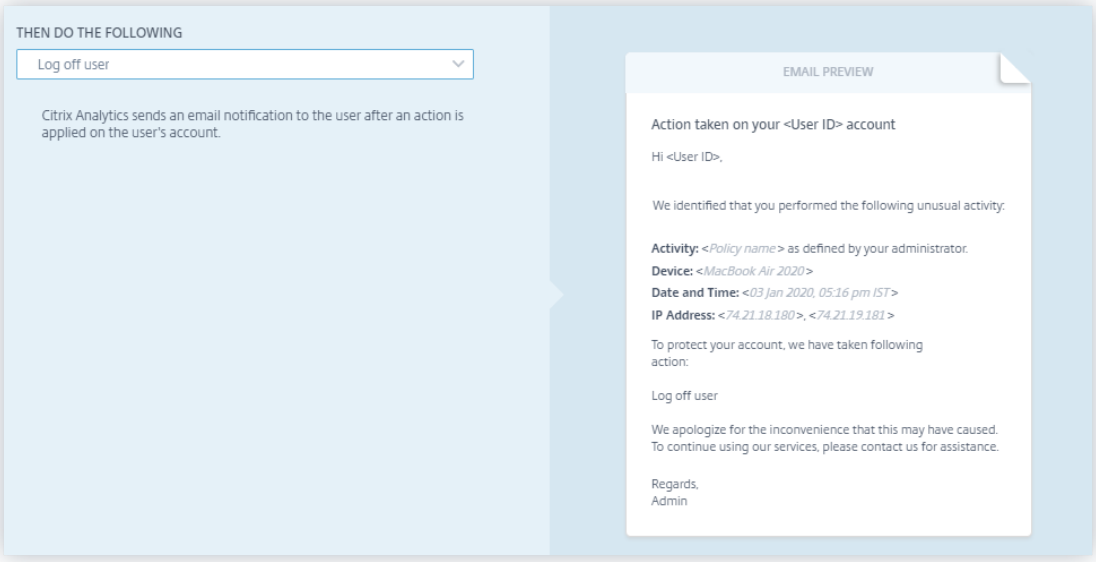
- デフォルトリスク指標とカスタムリスク指標：[ポリシーの作成] ページの条件メニューは、デフォルトリスク指標とカスタムリスク指標に基づいて分離されるようになりました。ポリシーを作成するときに、デフォルトのリスク指標タブとカスタムリスク指標タブを切り替え、リスク指標の条件を設定できます。



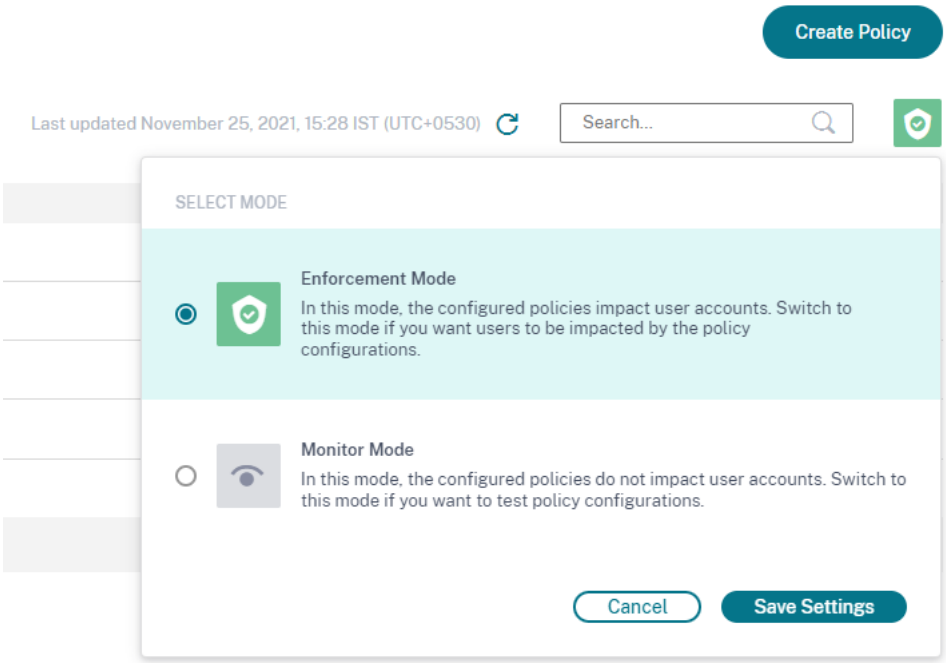
- エンドユーザー応答の要求：Citrix Analytics では、「エンドユーザー応答を要求」このアクションを使用して、検出された危険なアクティビティに関する電子メール通知をユーザーに送信できます。ユーザーがアクティビティについて応答したら、アカウントで実行する次のアクションを決定できます。ユーザーの応答時間を設定することもできます。応答が受信されない場合、Citrix Analytics はステータスとして応答なしと見なします。



- 中断アクションの適用: ユーザーのログオフやユーザーのロックなどの中断を伴うアクションが適用されたときに、ユーザーに通知できます。アクティビティの詳細と適用されたアクションを含む通知がユーザーに送信されます。この操作により、ユーザーのアカウントへのサービスが一時的に中断され、さらなる誤用が防止されます。アカウントへのアクセスを続行するには、管理者に問い合わせる必要があります。



- 強制モードと監視モード: ポリシーに適用モードまたは監視モードを設定できます。



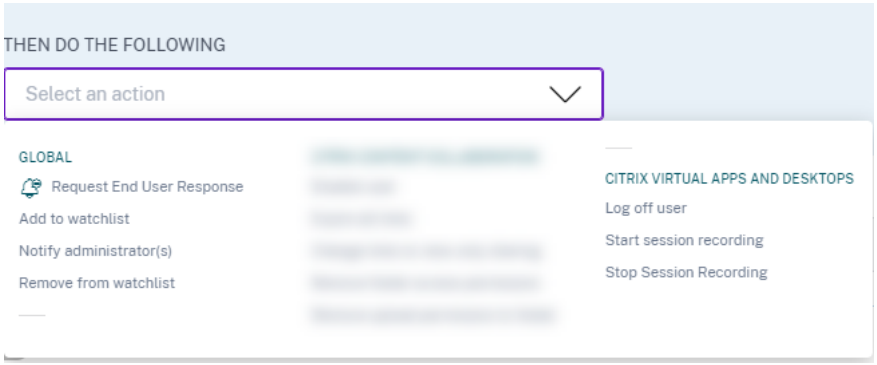
ポリシーの拡張について詳しくは、「ポリシーとアクション」を参照してください。

ユーザーのロックとユーザーアクションのロック解除　Citrix Analytics では、次のゲートウェイアクションが導入されています。

- ユーザーのロック
- ユーザーのロック解除

これらのアクションは、手動で、またはポリシーを構成するときに適用できます。

詳細については、「アクションとは」を参照してください。

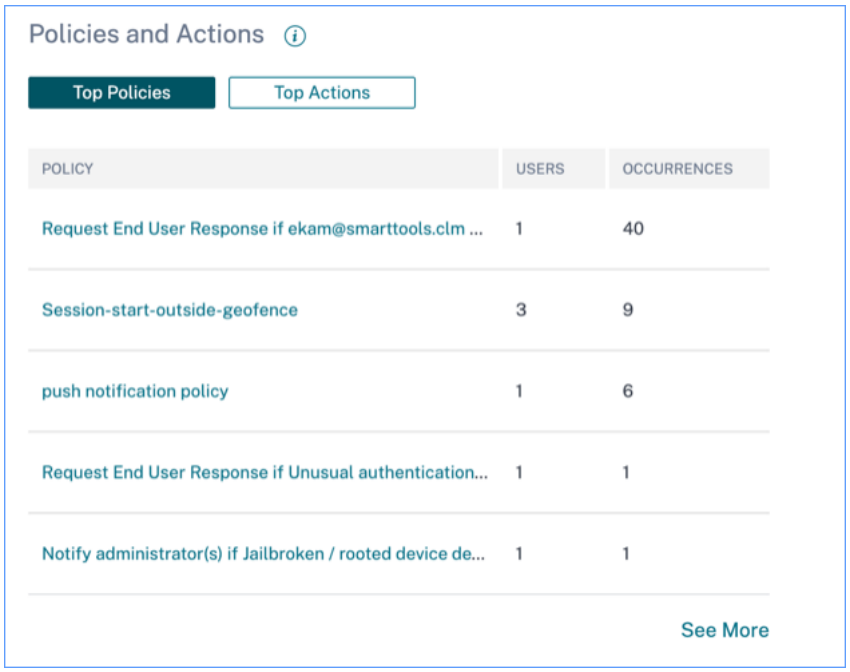


概要ダッシュボードにアクセスする　Citrix Analytics の［ユーザー］ダッシュボードに［アクセスの概要］パネルが導入されました。このレポートには、組織内のリソースへのアクセスをユーザーが試行した合計回数が要約されます。

詳細については、「アクセスの概要」を参照してください。

ポリシーとアクションダッシュボード　Citrix Analytics では、ユーザーダッシュボードに［ポリシーとアクション］パネルが導入されています。ユーザープロファイルに適用されている上位 5 つのポリシーとアクションが表示されます。選択した期間の上位ポリシーと上位アクションに基づいてデータをソートできます。

詳細については、「ポリシーとアクション」を参照してください。



ポリシーのセルフサービス検索　セルフサービス検索を使用して、定義したポリシーを満たすユーザーイベントを表示します。また、アナリティクスがこれらの異常イベントに適用したアクションを表示することもできます。ファセットと検索ボックスを使用して、必要なイベントを検索します。

イベントを表示するには、検索ボックスで、リストから [ポリシー] を選択し、期間を選択して、[検索] をクリックします。

詳細については、ポリシーのセルフサービス検索を参照してください。

廃止された機能

リスクスコアの変更ポリシーベースの条件が削除されました　ポリシーを設定すると、リスクスコアの変更ポリシーベースの条件を使用できなくなります。Citrix Analytics はこの条件をサポートしていません。

詳細については、「ポリシーとアクション」を参照してください。

複数のポリシーベースのアクションが削除されました　ポリシーを設定すると、複数のアクションを適用できなくなります。Citrix Analytics は、各ポリシーに対して 1 つのアクションのみをサポートします。

詳細については、「ポリシーとアクション」を参照してください。

解決された問題

- 委任された読み取り専用管理者が [ユーザーアクセス] および [アプリケーションアクセス] ダッシュボードにアクセスしているときにエラーが発生します。[CAS-16297]

2019 年 12 月 12 日

新機能

Splunk バージョンのサポート　Citrix Analytics は、以下のバージョンの Splunk をサポートしています。

- **Splunk 8.0 64** ビット
- **Splunk 7.3 64** ビット

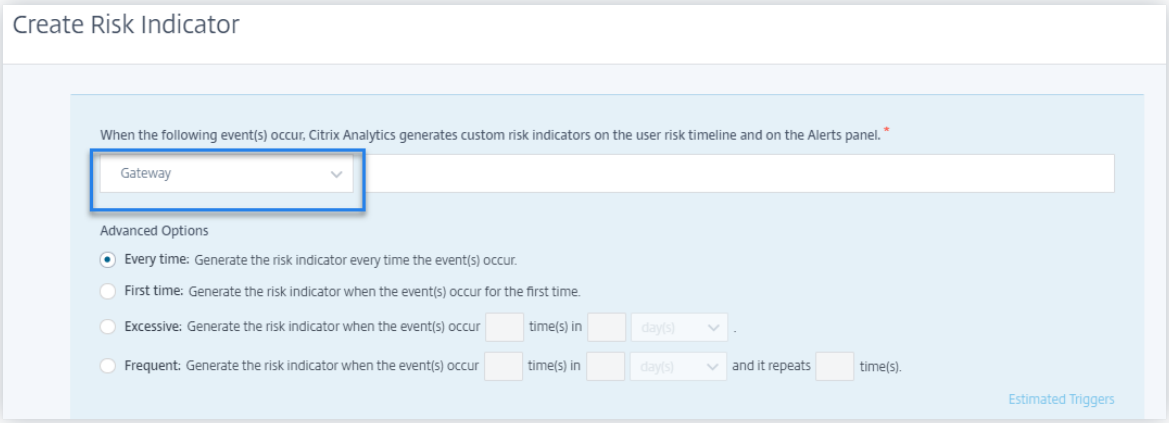
Splunk 統合のセキュリティ上の利点を最大限に活用するには、ダウンロードページから Splunk アドオンアプリの最新バージョンにアップグレードしてください。

サポートされている Splunk バージョンの詳細については、「サポートされているバージョン」を参照してください。

2019 年 12 月 04 日

新機能

NetScaler Gateway のカスタムリスクインジケータ　カスタムリスク指標を使用して、NetScaler Gateway イベントのリスク指標をトリガーするための条件と頻度を定義できるようになりました。ユーザーイベントが条件を満たすと、Analytics はリスク指標をトリガーします。カスタムリスク指標の作成方法の詳細については、「カスタムリスク指標」を参照してください。

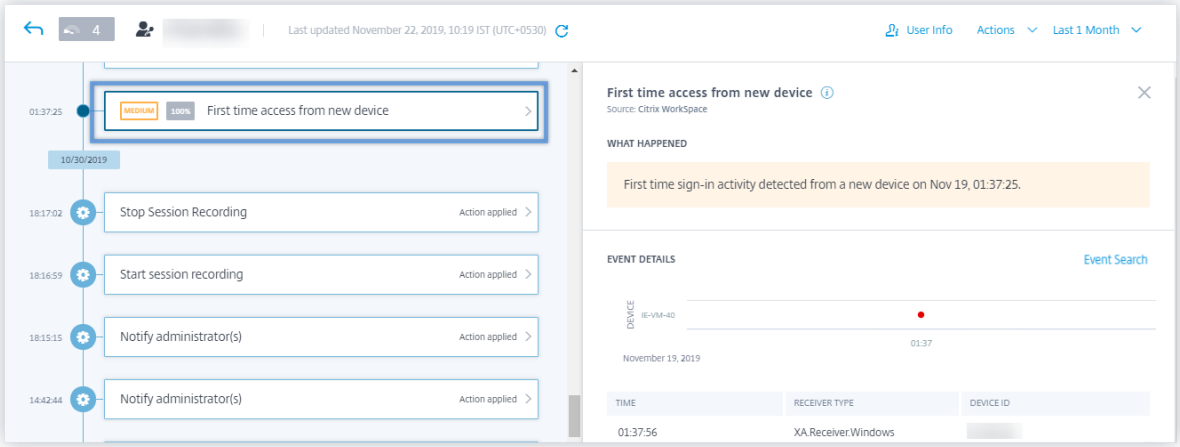


2019 年 11 月 22 日

新機能

新しいデバイスからの初回アクセス—**Citrix Virtual Apps and Desktops** のリスクインジケータ　Citrix Analytics は、新しいデバイスからのアクセスに基づいてアクセスの脅威を検出し、対応するリスク指標をトリガーします。

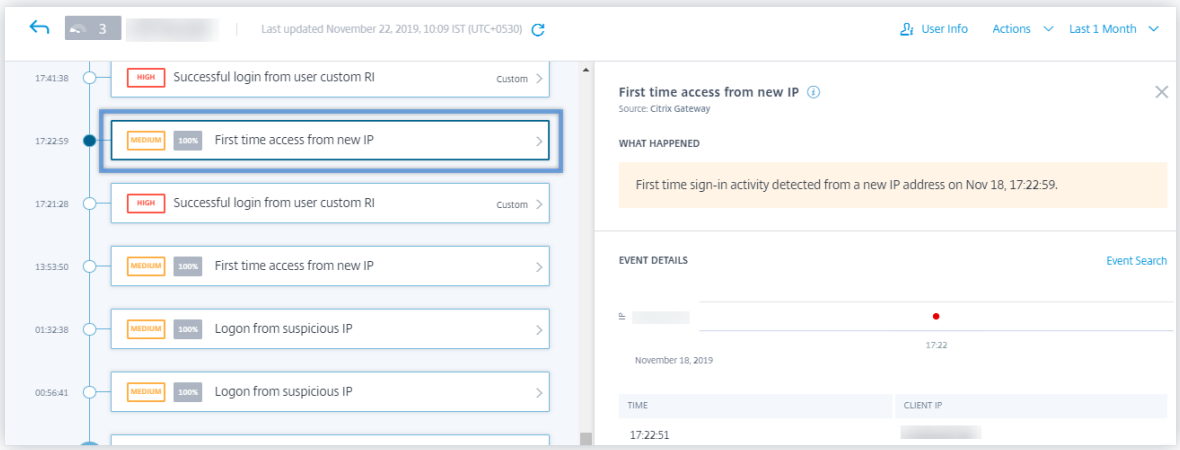
新しいデバイスからの初回アクセスリスク指標は、ユーザーが 90 日後にデバイスからサインインしたときにトリガーされます。このイベントは、Citrix Receiver がこの新しいデバイスまたは不慣れなデバイスからのサインインレコードを過去 90 日間保持していないためにトリガーされます。詳しくは、「Citrix Virtual Apps and Desktops」および「Citrix DaaS リスク指標」を参照してください。



新しい **IP** からの初回アクセス**-NetScaler Gateway** リスクインジケータ　Citrix Analytics は、新しい IP アドレスからのアクセスに基づいてアクセスの脅威を検出し、対応するリスク指標をトリガーします。

新しい **IP** からの初回アクセスリスク指標は、ユーザーが 90 日後に IP アドレスからサインインしたときにトリガーされます。このイベントは、Citrix Receiver に過去 90 日間に新しい IP アドレスまたは不慣れな IP アドレスからのサインインレコードがないためにトリガーされます。

詳しくは、「NetScaler Gateway リスク指標」を参照してください。



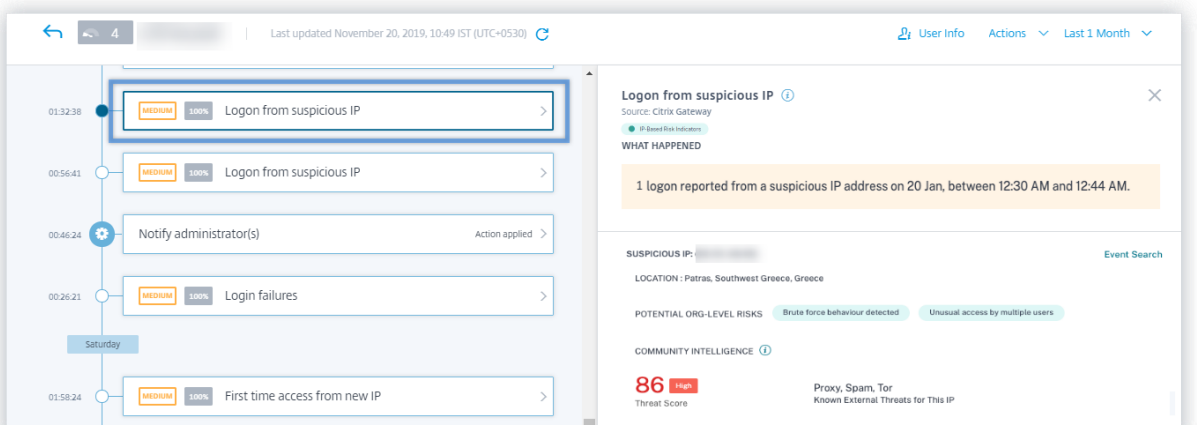
疑わしい **IP** からのログオン**-NetScaler Gateway** リスクインジケータ　Citrix Analytics は、疑わしい IP サインインアクティビティに基づいてユーザーアクセスの脅威を検出し、疑わしい **IP** からのログオンリスク指標をトリガーします。

このリスクインジケータは、ユーザーが疑わしい IP アドレスからネットワークにアクセスしようとしたときにトリガーされます。Analytics では、次のいずれかの条件に基づいて、IP アドレスが疑わしいと見なされます。

- 外部 IP 脅威インテリジェンスフィードにリストされている

- 異常な場所から複数のユーザーサインインレコードがある
- 過剰なログイン試行が失敗し、ブルートフォース攻撃を示す可能性があります。

詳しくは、「NetScaler Gateway リスク指標」を参照してください。



NetScaler Gateway イベントのセルフサービス検索　セルフサービス検索機能を使用して、NetScaler Gateway データソースから受信したユーザーイベントに関する洞察を取得します。Citrix Analytics は、NetScaler Gateway ユーザーの認証ステージ、承認タイプ、VPN セッションコード、VPN セッション状態などのイベントを受信します。ファセットと検索ボックスを使用して、必要なイベントを検索し、基礎となるデータを調べます。

イベントを表示するには、検索ボックスで、リストから [ゲートウェイ] を選択し、期間を選択して、[検索] をクリックします。

詳細については、「Gateway のセルフサービス検索」を参照してください。

Citrix Remote Browser Isolation イベントのセルフサービス検索　セルフサービス検索機能を使用すると、Citrix Remote Browser Isolation Service から受信したブラウジングイベントを把握できます。Citrix Analytics は、ユーザー接続ごとに、セッション接続、セッション起動、公開アプリケーション、削除されたアプリケーションなどのイベントを受信します。検索ボックスを使用して、必要なイベントを検索し、参照元データを調べます。

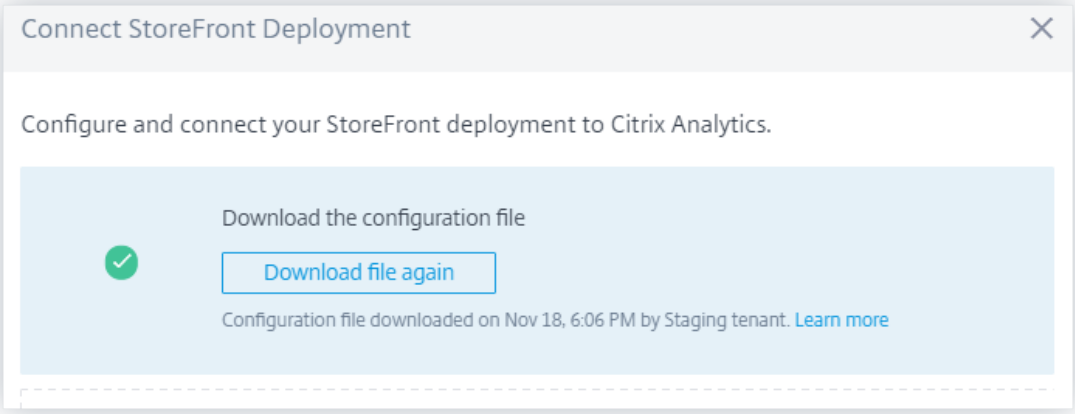
イベントを表示するには、検索ボックスで、リストから「**Remote Browser Isolation** 」を選択し、期間を選択して、「検索」をクリックします。

詳細については、「Remote Browser Isolation のセルフサービス検索」を参照してください。

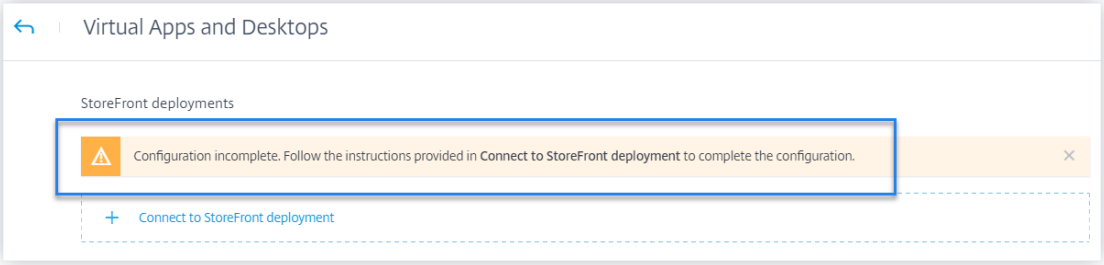
ウォッチリストから削除アクション　ウォッチリストからユーザを削除するには、手動方式を適用するか、ポリシーベースの方式を適用します。詳細については、「ウォッチリスト」を参照してください。

StoreFront 展開環境を構成する際のオンボーディングメッセージの改善　Citrix Analytics では、StoreFront 展開環境の構成に役立つ次のメッセージが表示されるようになりました。

- 設定ファイルをダウンロードすると、ダウンロードの日時とユーザー名を示すメッセージが表示されます。このページを更新すると、[ファイルのダウンロード] ボタンがもう一度 [ファイルのダウンロード] に変わります。



- StoreFront の構成が不完全な場合は、構成手順に従って StoreFront 展開環境を Analytics に接続するように指示する警告メッセージが表示されます。



StoreFront 展開環境を構成する方法について詳しくは、「StoreFront を使用した Citrix Virtual Apps and Desktops のオンプレミスサイトのオンボード」を参照してください。

廃止された機能

リスクインジケータ-新しいデバイスからのアクセス削除　Citrix Analytics が［新しいデバイスからのアクセス］リスク指標をトリガーしなくなりました。ただし、ユーザーダッシュボード、ユーザータイムライン、およびポリシーダッシュボードでは、このリスク指標に関連する履歴データを表示できます。

新しいデバイスからのアクセスに基づいて以前に作成したポリシーの場合、ポリシーを変更するか、新しいリスク指標の新しいデバイスからの初回アクセスでポリシーを作成する必要があります。

解決された問題

- 認証のセルフサービス検索で、イベントが表示されない。[CAS-24959]

2019 年 11 月 08 日

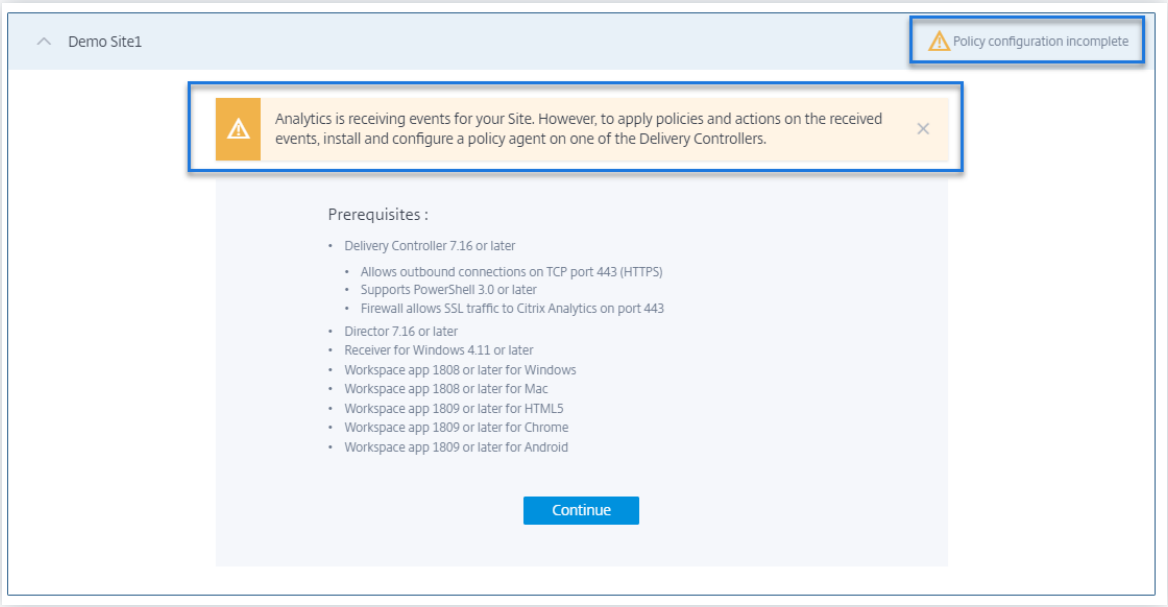
解決された問題

- Citrix Content Collaboration のリスク指標の場合、ユーザーはリスクタイムラインにアクションを適用できません。[CAS-24844]
- バージョン 1911 より前の Chrome 向け Citrix Workspace アプリは、イベントの詳細を Citrix Analytics 送信できません。[CAS-24938]

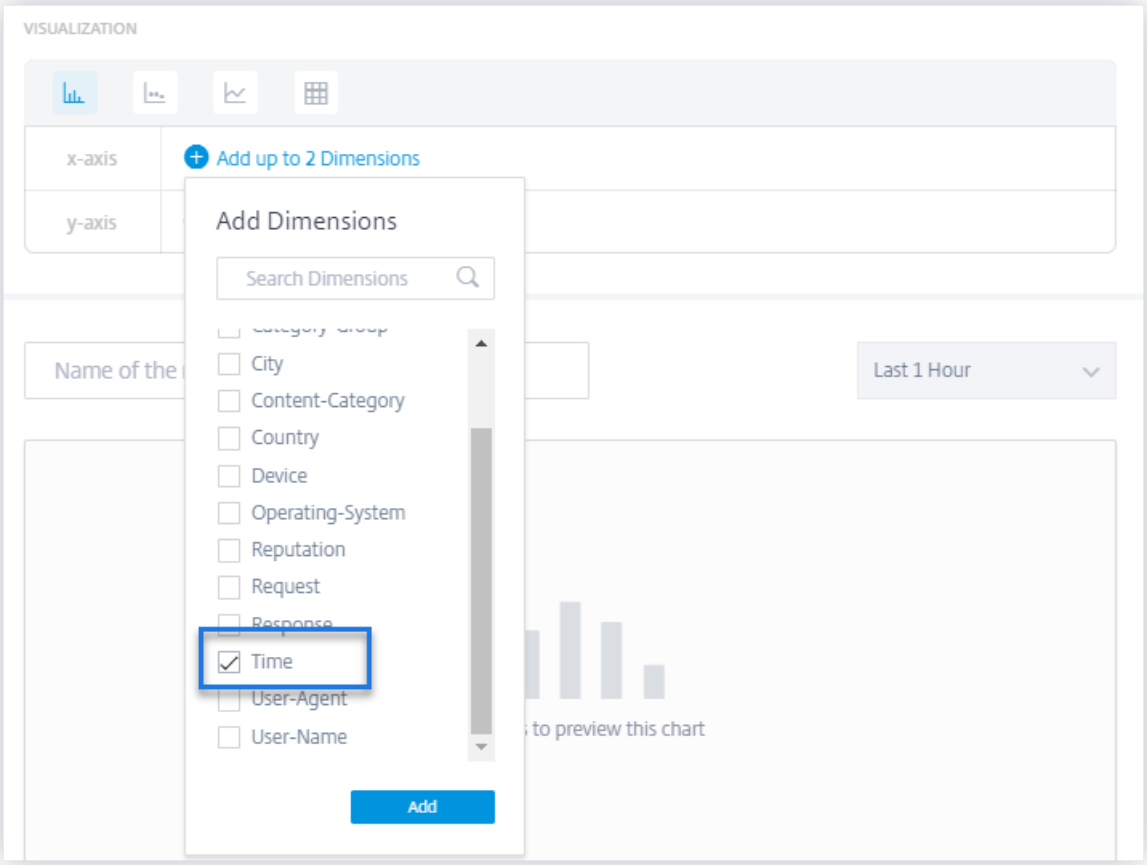
2019 年 10 月 21 日

新機能

分析エージェントの名前を変更しました　エージェント名は、ユーザーインターフェイスで **Analytics** ポリシーエージェントとして表示され、そのロールを示します。オンプレミスの Citrix Virtual Apps and Desktops データソースをオンボーディングすると、Citrix Analytics は、サイトのポリシーとアクションを構成するためだけにポリシーエージェントが必要であることを明確に通知します。このエージェントは、データソースからデータを送信する役割はありません。詳しくは、「Citrix Virtual Apps and Desktops」および「Citrix DaaS データソース」を参照してください。



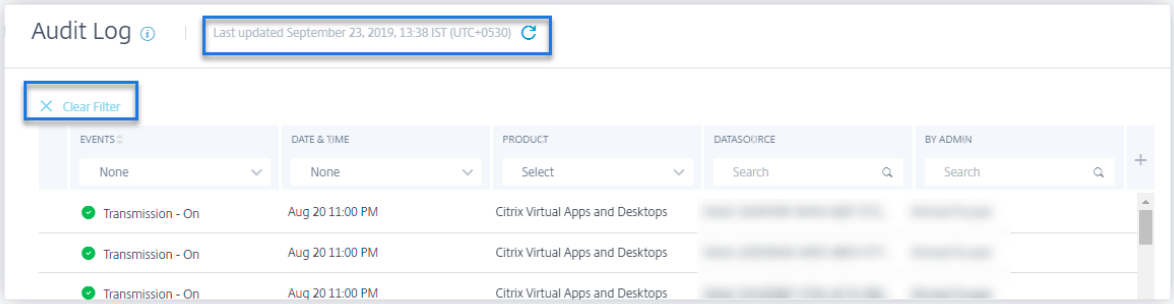
カスタムレポートの時間ディメンションのサポート　X 軸の [時間] ディメンションを選択して、時間に基づいてイベントをグループ化できるようになりました。レポートには、選択した期間の時間間隔に基づいて、受信したイベントの合計が表示されます。レポートの作成方法の詳細については、「カスタムレポート」を参照してください。



監査ログの機能強化　[監査ログ] ページのユーザーエクスペリエンスが強化されました。

- 監査ログページが最後に更新された日時の詳細を表示し、ページを更新して最新の監査ログを表示できます。
- 監査ログに適用されたすべてのフィルタをクリアできます。

監査データの詳細については、監査ログを参照してください。



解決された問題

- Citrix Analytics は、Microsoft Graph セキュリティが正常にオンボーディングされても、匿名 **IP** アドレスのリスク指標を生成できません。[CAS-21329]
- バージョン 1910 より前の HTML5 向け Citrix Workspace アプリは、イベントの詳細を Citrix Analytics 送信できません。[CAS-24938]

2019 年 **9** 月 **23** 日

解決された問題

- データソースのサイトカードで、[最新のイベント] フィールドに誤った日付と時刻の情報が表示されます。[CAS-24087]

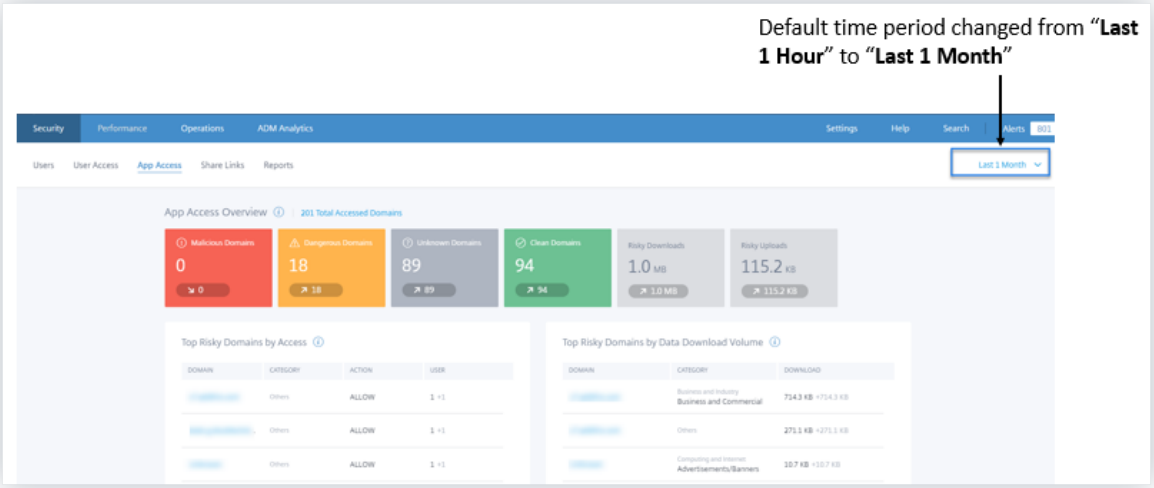
2019 年 **8** 月 **30** 日

新機能

ダッシュボード全体のデフォルト期間の変更　次のダッシュボードのデフォルトの期間が [過去 **1** 時間**]** から **[**過去 **1** か月] に変更されました。

- ユーザー
- リスクタイムライン
- ユーザーアクセス
- アプリアクセス
- リンクを共有する
- アラート履歴

ダッシュボードには、デフォルトで、過去 1 か月間のイベントが表示されます。これらのダッシュボードを使用すると、より魅力的なエクスペリエンスが得られます。たとえば、**App Access** ダッシュボードを開くと、ダッシュボードにはデフォルトで、過去 1 か月間のアプリケーションアクセスイベントが表示されます。



解決された問題

- Content Collaboration のリスク指標の場合、[ユーザーポリシーベースの無効化] アクションを正常に適用できません。[CAS-17304]
- Citrix Analytics は、NetScaler Gateway 13.0 からのイベントを処理できません。この問題は、NetScaler Gateway 13.0 が Citrix Analytics に送信されるログオンイベントでユーザー名を提供できないために発生します。[CAS-21339]

2019 年 **8** 月 **20** 日

新機能

セルフサービス検索の機能強化

- セルフサービスページのユーザーエクスペリエンスが強化されました。ユーザーリスクタイムラインとセルフサービス検索ページをシームレスに切り替えることができるようになりました。
- イベントを時間順に並べ替えることができるようになりました。デフォルトでは、最新のイベントがイベントテーブルの最初に表示されます。[時間（TIME）] 列の並べ替えアイコンをクリックして、イベントを最新時刻または最早時刻に基づいて並べ替えます。

セルフサービス検索の使用方法の詳細については、「セルフサービス検索」を参照してください。

カスタムレポートの機能強化

- [アクセス制御]、[Content Collaboration]、[アプリとデスクトップ] の各データソースに新しいディメンションが追加されました。これらのディメンションを選択してレポートを作成できます。次のディメンションがデータソースに追加されます。

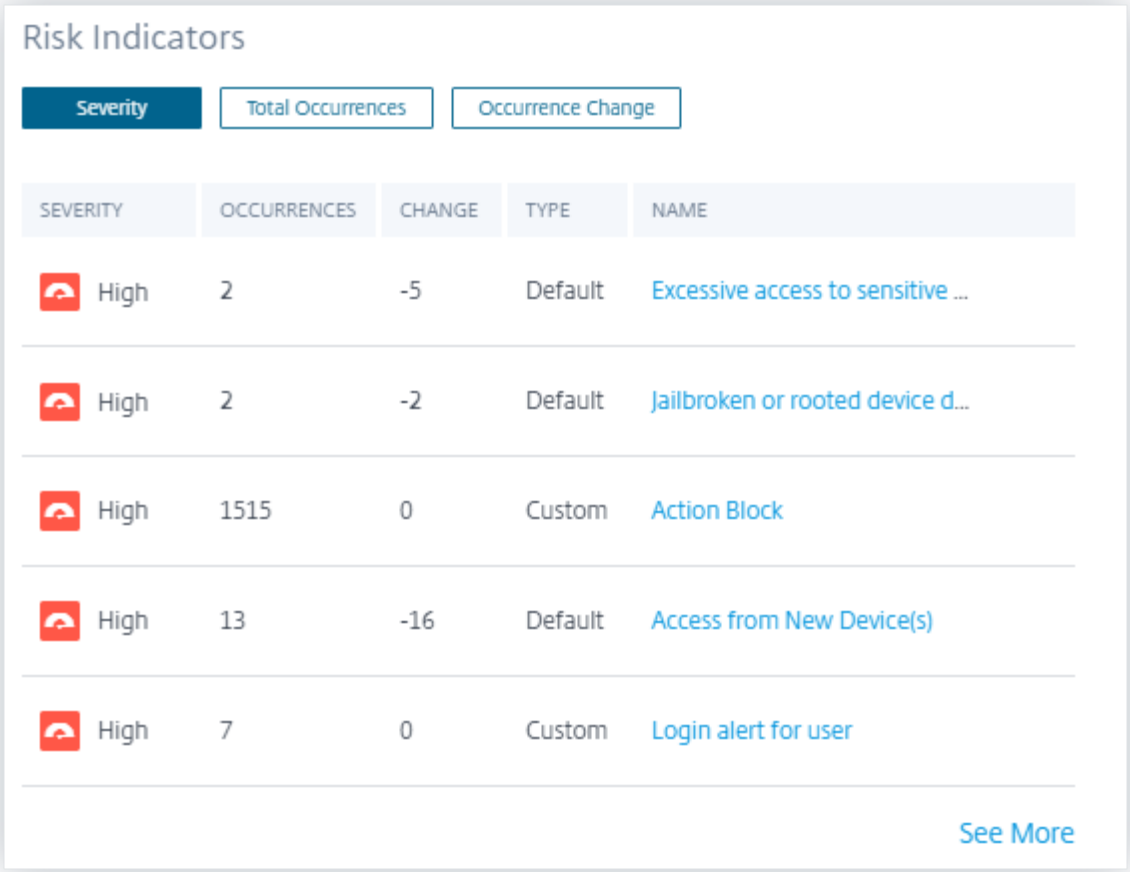
  - アクセス制御: ユーザーエージェント、ユーザー名
  - **Content Collaboration**: ユーザーの電子メール、ユーザー名、作成者、アカウント ID、OAuth クライアント ID、イベント ID、フォルダー ID、フォルダー名、リソース ID、フォーム ID、クライアント IP
  - アプリとデスクトップ: ユーザー名、IP アドレス、デバイス ID、Jail Broken、セッション起動タイプ、セッションサーバー名、セッションユーザー名、ダウンロードファイル名、ダウンロードファイルパス、プリンター名の印刷、印刷ジョブ詳細ファイル名、SaaS アプリ起動 URL、クリップボード操作、クリップボード詳細結果

- カスタムレポートのユーザーインターフェイスは、ページネーションのサポートと、フィルターの [すべてクリア] オプションによって強化されました。

これらのディメンションを使用してカスタムレポートを作成する方法について詳しくは、「カスタムレポート」を参照してください。

リスク指標ダッシュボード　リスク指標ダッシュボードは、[ユーザー] ページに導入されています。これは、ユーザーのデフォルトリスク指標とカスタムリスク指標の上位 5 つをまとめたものです。[詳細を表示] リンクをクリックすると、[リスク指標の概要] ページにリダイレクトされます。このページには、選択した期間に生成されたリスク指標に関する詳細情報が表示されます。

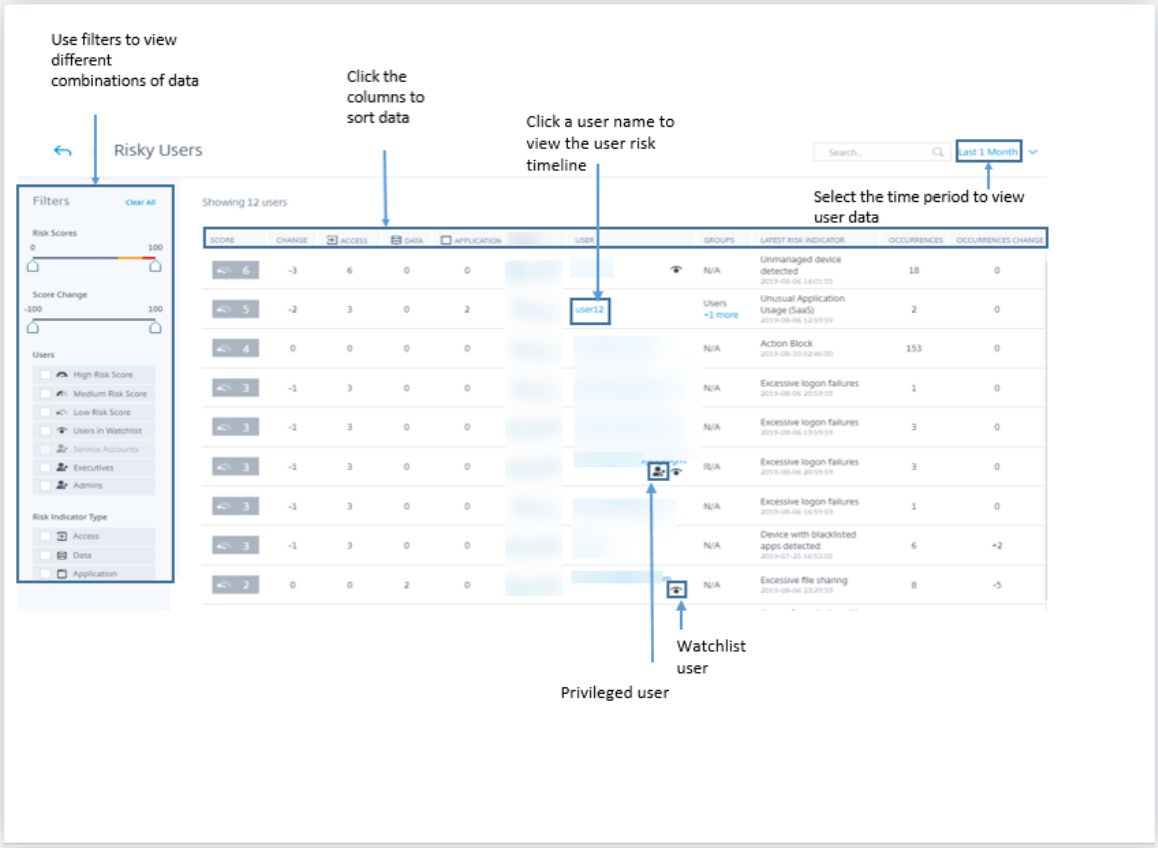
詳細については、「ユーザーダッシュボード」を参照してください。



リスクの高いユーザーのダッシュボードの機能強化　Citrix Analytics では、[** リスクユーザー **] ダッシュボードの［リスク指標］タブと［リスク指標の変更］タブが導入されています。これらのタブに基づいて、リスクの高い上位 5 人のユーザーを表示できます。ダッシュボードには、[リスク指標] 列も表示されます。ユーザーのリスク指標の数を示します。

危険なユーザー] ページには、[発生回数] 列と [発生回数の変更] 列が表示されます。これらの列には、カスタムおよびデフォルトのリスク指標の発生総数と発生数の変化が要約されます。

詳細については、「ユーザーダッシュボード」を参照してください。



リンクのリスク指標を共有する-過剰なダウンロード　Citrix Analytics は、共有リンクでの過剰なダウンロードに基づいてアクセスの脅威を検出し、過剰ダウンロードリスク指標をトリガーします。以前の動作に基づいて、過剰なダウンロードを含む共有リンクを特定することで、潜在的な攻撃の共有リンクを監視できます。このリスク指標は、過剰なファイルのダウンロードアクティビティを識別するのに役立ちます。

詳細については、「過剰なダウンロード」を参照してください。

認証データのセルフサービス検索　セルフサービス検索を使用して、認証イベントに関するインサイトを取得します。Citrix Analytics は、ユーザーログイン、ユーザーログオフ、クライアント更新などの認証イベントを、Citrix Cloud の ID およびアクセス管理サービスから受信します。この検索では、認証イベントに関する詳細なレポートが提供され、認証の問題の特定とトラブルシューティングに役立ちます。検索クエリを定義して、定義した条件に一致するイベントを取得することもできます。

イベントを表示するには、リストから [認証] を選択し、期間を選択して、[検索] をクリックします。

詳細については、「認証のセルフサービス検索」を参照してください。

2019 年 7 月 11 日

新機能

カスタムリスク指標　Citrix Analytics が生成するデフォルトのリスク指標は、機械学習アルゴリズムに基づいています。Citrix Analytics でカスタムリスク指標を作成できるようになりました。ユーザーイベントに基づいて、条件を定義し、カスタムリスク指標を作成できます。

定義された条件が満たされると、Citrix Analytics はデフォルトのリスク指標と同様のカスタムリスク指標を生成し、ユーザーのリスクタイムラインに表示します。カスタムリスク指標は、ユーザーのリスクタイムラインにラベルで示されます。

詳細については、「カスタムリスク指標」を参照してください。

リスクタイムラインの特権ステータス

ユーザーリスクタイムラインには、ユーザーの管理者またはエグゼクティブ権限ステータスに変更があるたびに、次のイベントが表示されます。

- エグゼクティブグループに追加されました
- エグゼクティブグループから削除されました
- 特権が管理者に昇格されました
- 管理者権限が削除されました

ユーザーに対してリスク指標がトリガーされると、その指標を指定された特権ステータス変更イベントに関連付けることができます。必要に応じて、ユーザープロファイルに適切なアクションを適用できます。

詳細については、「ユーザーリスクのタイムライン」を参照してください。

共有リンクアクションの有効期限切れ

Citrix Analytics では、共有リンクのリスク指標にアクションを適用できます。現在、サポートされているアクションは [共有リンクを期限切れ] です。

詳しくは、「Citrix 共有リンクのリスク指標」を参照してください。

セルフサービス検索の機能強化

- 検索クエリでのワイルドカード文字 * のサポート：検索クエリでアスタリスク（*）文字を使用して、任意の文字を 0 回以上一致させます。たとえば、検索クエリ UserName =「John*」では、John で始まるすべてのユーザー名のイベントが表示されます。

- ファセットに「すべてクリア」**(Clear All)** オプションが追加されました。選択したファセットを一度にすべて削除するには、「すべて クリア」**(Clear All)** をクリックします。
- イベントリストに非表示の列データを表示する: イベントテーブルから列を削除すると、対応するデータをユーザーイベントリストに表示できます。ユーザーのイベント行を展開し、データを表示します。

詳細については、「セルフサービス検索」を参照してください。

サイトカードのデータエラーステータス

Citrix Analytics がデータソースから過去 **1** 時間イベントを受信しない場合、サイトカードには「データを受信していません」ラベルが赤で表示されます。また、受信したイベントの数も表示され、対応するセルフサービス検索ページにリンクされています。この機能は、セルフサービス検索ページで対応するイベントを表示し、データ転送の問題がないかどうかをチェックするのに役立ちます。

> 注
>
> 現在、セルフサービス検索は、Access、Content Collaboration、および Apps and Desktop データソースでのみ使用できます。

詳しくは、「Citrix データソースでの分析の有効化」を参照してください。

解決された問題

- アクセス制御データソースの場合、サイトカード上のイベントの数がセルフサービスの検索結果と一致しません。[CAS-18286]

2019 年 **6** 月 **19** 日

解決された問題

- [監査ログ] ページには、Active Directory データソースが検出されるたびに、データ転送のオンまたはオフの状態が表示されます。[CAS-17575]
- [ユーザー] ダッシュボードの [期間] メニューが正確に読み込まれません。タイムアウトエラーメッセージが表示されます。[CAS-19467]
- ユーザーが Splunk からテナントに接続しているときに、Citrix Analytics でエラーメッセージが表示されます。新しいデータソースのオンボーディングが失敗することがあります。[CAS-19429]

2019 年 6 月 17 日

新機能

StoreFront の構成

組織でオンプレミスの StoreFront を使用している場合、Citrix Analytics に接続するように StoreFront t を構成できるようになりました。構成は、Citrix Analytics からインポートされた構成ファイルを使用して実行されます。構成が成功すると、Citrix Workspace アプリはユーザーイベントを Citrix Analytics に送信して、ユーザーの行動に関する実用的な洞察を生成します。インサイトは、異常なユーザー行動を検出し、組織内のセキュリティの脅威をプロアクティブに処理するのに役立ちます。詳しくは、「StoreFront を使用した Citrix Virtual Apps and Desktops のオンプレミスサイトのオンボード」を参照してください。

2019 年 5 月 30 日

新機能

過剰なログオン失敗

Citrix Analytics は、過剰なログオンアクティビティに基づいてアクセスの脅威を検出し、過剰なログオン失敗のリスク指標をトリガーします。このリスク指標は、ユーザーが Content Collaboration にアクセスしようとして複数のログオンに失敗したときにトリガーされます。以前の動作に基づいて、過剰なログオンに失敗したユーザーを特定することで、管理者はユーザーのアカウントを監視してブルートフォース攻撃を受けることができます。

> 注
>
> 過剰なログオン失敗は、過剰な認証失敗の名前に変更されました。

解決された問題

- Citrix Workspace アプリによって送信される一部のユーザーイベントでは、データソースが Citrix Virtual Apps and Desktops ではなく、Endpoint Management として誤って識別されます。

  [CAS-17323]

- [ユーザー] ダッシュボードは、過去 **1** か月間の読み込みに時間がかかります。この問題は、ユーザー数が多い場合に発生します。場合によっては、601 エラーに遭遇することさえあります。

  [CAS-16300]

- Citrix Cloud 上のサービスにサブスクライブしているユーザーもいますが、Citrix Content Collaboration はデータソースとして検出されません。

  [CAS-16299]

2019 年 **5** 月 **09** 日

新機能

カスタムレポートの作成

運用要件に基づいてカスタムレポートを作成できるようになりました。Citrix Analytics には、選択したデータソースに応じたディメンションと指標のリストが表示されます。必要なパラメーターと、棒グラフ、イベントチャート、折れ線グラフ、テーブルなどの可視化タイプを選択して、レポートを作成します。レポートを作成すると、データをグラフィカルに整理して分析できます。

カスタムレポートを作成するには、[セキュリティ] タブで、[レポート] > [****** レポートの作成**]** の順にクリックします。以前に作成したレポートを表示するには、**[**** セキュリティ] タブの [レポート] をクリックします。詳細については、「カスタムレポート」を参照してください。

特権ユーザーの監視

Citrix Analytics を使用すると、組織内の特権ユーザーの動作の異常を詳細に監視できます。特権ユーザーはセキュリティ上の脅威に対して非常に脆弱であり、日常的なアクティビティと悪意のあるアクティビティを区別することが困難になります。したがって、特権ユーザーの悪意のある活動は、長い間検出されないままです。この機能を使用すると、このようなアクティビティをプロアクティブに監視し、適切なユーザーアカウントに対して適切なアクションを実行できます。特権ユーザーは、[ユーザー] ダッシュボードにアイコンで表示されます。

Citrix Analytics では、次の種類の特権ユーザーの監視がサポートされています。

- 管理者 -それぞれの Citrix サービスによって管理者権限が割り当てられているユーザー。現在、Citrix Analytics は、Content Collaboration サービスで管理者権限を持つユーザーの特権ユーザー監視をサポートしています。
- エグゼクティブ -Citrix Analytics では、AD グループをエグゼクティブグループとしてマークできます。AD グループを Executive グループとしてマークすると、そのグループ内のすべてのユーザーが特権ユーザーになります。AD グループ内のユーザーの動作異常をさらにサポートする必要がない場合は、そのグループを Executive グループとして削除できます。

詳細については、「特権ユーザー」を参照してください。

週次 **E** メール要約

Citrix Analytics は、組織の IT 環境におけるセキュリティリスクのエクスポージャーを要約したメールを毎週管理者に送信します。メール通知は毎週火曜日に管理者に送信され、前週に発生したセキュリティイベントが強調表示されます。このメールにより、Citrix Analytics にサインインすることなく、セキュリティリスクのエクスポージャーについて管理者に通知されます。詳細については、「週次メールの概要」を参照してください。

2019 年 4 月 26 日

新機能

委任管理者

Citrix Analytics は、委任された管理者の役割をサポートするようになりました。この機能を使用すると、他の管理者を Citrix Cloud アカウントに招待して、組織の Citrix Analytics を管理できます。フルアクセス権限を持つ Citrix Analytics 管理者の場合は、他の管理者を Citrix Cloud アカウントに追加できます。これらの追加の管理者は、委任管理者と呼ばれます。現在、委任された管理者に読み取り専用アクセスを割り当てることができます。詳細については、「委任された管理者」を参照してください。

解決された問題

データストリーミングを使用するデータソースのリスク指標は、アラートを生成しないものはほとんどありません。次のリスク指標のいずれかがトリガーされた場合、アラート通知は取得されず、ポリシーベースのアクションは自動的に適用されません。

- **Citrix Endpoint Management** リスク指標 -管理対象外のデバイス、ジェイルブレイクまたは Root 化されたデバイス、および禁止リストに登録されたアプリを搭載したデバイス。
- **Citrix Virtual Apps and Desktops** のリスクインジケータ -サポートされていないオペレーティングシステム（OS）を搭載したデバイスからのアクセス。
- **Citrix Content Collaboration** のリスクインジケータ -機密ファイルへの過剰なアクセス。

[CAS-14590]

2019 年 2 月 19 日

新機能

Splunk 統合

Citrix Analytics は Splunk と統合され、セキュリティインシデントの監視とトラブルシューティングのエクスペリエンスを強化します。この統合により、リスク指標、リスクスコア、ユーザープロファイルなど、Citrix Analytics for Security のリスク分析機能とインテリジェンスにより、既存のデータソースが強化されます。Citrix Analytics はリスク分析情報をチャンネルにエクスポートします。Splunk はこのチャンネルから同じものを引き出します。

Splunk の統合には、Citrix Analytics での構成、**Splunk** アプリ向け **Citrix Analytics** アドオンのインストール、およびアプリケーションの構成が含まれます。少なくとも 1 つのデータソースのデータ処理をオンにしてください。これは、Citrix Analytics が Splunk 統合プロセスを開始するのに役立ちます。

詳細については、「Splunk 統合」を参照してください。

動的なセッションの録画　Citrix Analytics では、ユーザーの現在の Virtual Apps and Desktops セッションでセッション記録を動的にトリガーする機能が導入されます。リスク分析に必要な証拠を把握し、セッションの切断やユーザーのブロックなど、適切なインシデント対応アクションを実行するのに役立ちます。

詳細については、「ポリシーとアクション」を参照してください。

リンクダッシュボードとリスク指標の共有　Citrix Analytics は、Citrix Content Collaboration から収集されたデータに基づいて、共有リンクのリスク可視性を導入します。これは、共有リンクがトリガーするリスク指標を通じて、共有リンクのリスクエクスポージャーを理解するのに役立ちます。

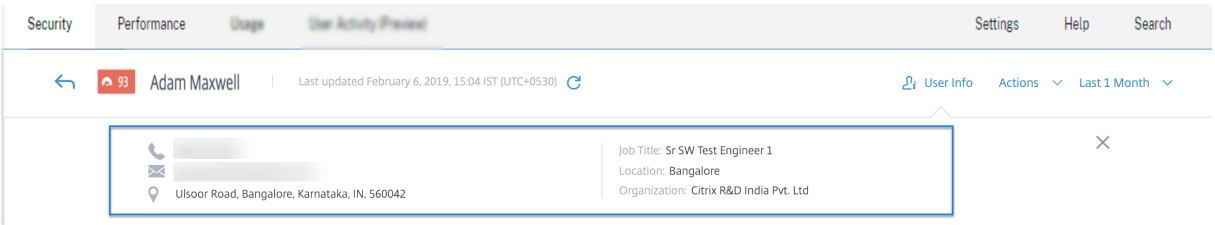
詳細については、「共有リンク」ダッシュボードを参照してください。

現在、匿名の機密共有ダウンロードリスク指標は、共有リンクに対してトリガーされます。Content Collaboration によってこの危険な動作が検出されると、Citrix Analytics がイベントを受け取ります。[アラート] パネルに通知され、匿名の機密共有ダウンロードリスク指標が共有リンクのリスクタイムラインに追加されます。

詳しくは、「共有リンクのリスクタイムライン」および「Citrix Share Link リスク指標」を参照してください。

Microsoft Active Directory 統合　Microsoft Active Directory と Citrix Analytics 統合できるようになりました。この統合により、役職、組織、オフィスの場所、電子メール、連絡先の詳細などの追加情報を使用して、リスクの高いユーザーのコンテキストが強化されます。Citrix Analytics のユーザープロファイルページで、ユーザーの可視性を高めることができます。

詳細については、「分析と Microsoft Active Directory の統合」を参照してください。



2019 年 **1** 月 **04** 日

新機能

既存のリスク指標の **SOURCE** 列の追加　**SOURCE** 列は、次のリスク指標の [**EVENT DETAILS**] セクションに導入されました。

- 過剰なファイルのアップロード
- 過剰なファイルのダウンロード
- 過剰なファイル共有
- ファイルまたはフォルダの過剰な削除

詳しくは、「Citrix Content Collaboration のリスク指標」を参照してください。

高度なユーザープロファイル　ユーザプロファイルの [ユーザ情報（**User Info**）] ビューが拡張されました。[アプリケーション]、[デバイス]、[データ使用量] セクションの右上隅に［トレンドビュー］リンクが追加されました。**[マップビュー]** リンクが **[場所]** セクションの右上隅に導入されました。これらのリンクは、特定の期間におけるユーザーの過去の行動に関するグラフィック表現を提供します。ユーザーのリスクタイムラインまたは **[データソース]** ページから **[ユーザー情報]** に移動できます。

> 注:
>
> 現在、認証データとドメインデータは、ユーザー情報プロファイルでは使用できません。

詳細については、「ユーザーリスクのタイムラインとプロファイル」を参照してください。

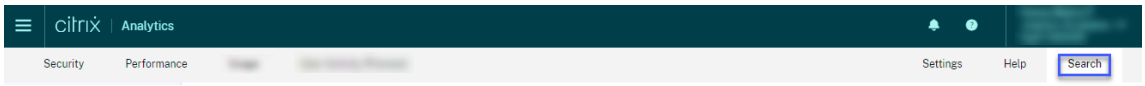
Microsoft Graph セキュリティリスク指標　オンボーディングされた Microsoft Graph セキュリティは、次のいずれかのセキュリティプロバイダーからリスク指標の詳細を受信し、Citrix Analytics に転送できます。

- Azure AD Identity Protection
- エンドポイント向け Microsoft Defender

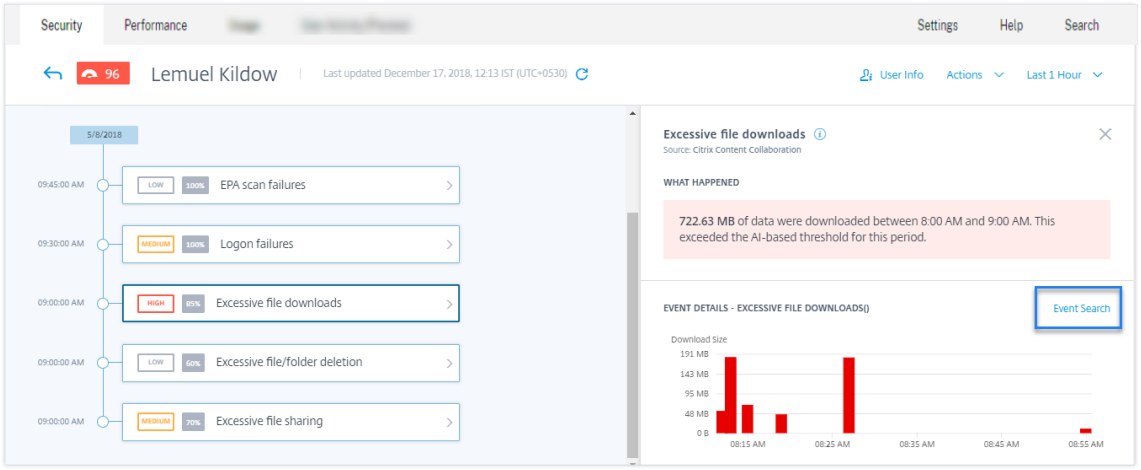
詳細については、「Microsoft Graph セキュリティリスク指標」を参照してください。

セルフサービス検索ページに入る方法　次のオプションを使用して、セルフサービス検索ページにアクセスできるようになりました。

- トップバー: トップバーの [検索] をクリックして、検索ページに直接アクセスします。



- ユーザープロファイルページのリスクタイムライン:[イベント検索] をクリックして、検索ページにアクセスし、特定のユーザーのリスク指標とデータソースに対応するイベントを表示します。詳細については、「セルフサービス検索」を参照してください。



Content Collaboration のセルフサービス検索　セルフサービス検索を使用して、Content Collaboration データソースに関連付けられたイベントに関するインサイトを取得します。イベントを表示するには、リストから [**Content Collaboration**] を選択し、期間を選択して、[検索] をクリックします。
詳細については、「Content Collaboration のセルフサービス検索」を参照してください。

アプリとデスクトップのセルフサービス検索　セルフサービス検索を使用して、Apps and Desktops データソースに関連付けられているイベントに関するインサイトを取得します。イベントを表示するには、リストから [アプリとデスクトップ] を選択し、期間を選択して、[検索] をクリックします。詳しくは、「アプリとデスクトップのセルフサービス検索」を参照してください。

セルフサービス検索イベントを **CSV** ファイルにエクスポートする　セルフサービス検索イベントを CSV ファイルにエクスポートし、将来使用するためにファイルをダウンロードできるようになりました。詳細については、「セルフサービス検索」を参照してください。

Citrix Virtual Apps and Desktops のオンボーディングの向上　Citrix Virtual Apps and Desktops データソースのオンボーディングプロセスが改善され、ユーザーエクスペリエンスが向上しました。サイトカードと搭乗手順が変更されました。詳しくは、「Citrix Virtual Apps and Desktops」および「Citrix DaaS データソース」を参照してください。

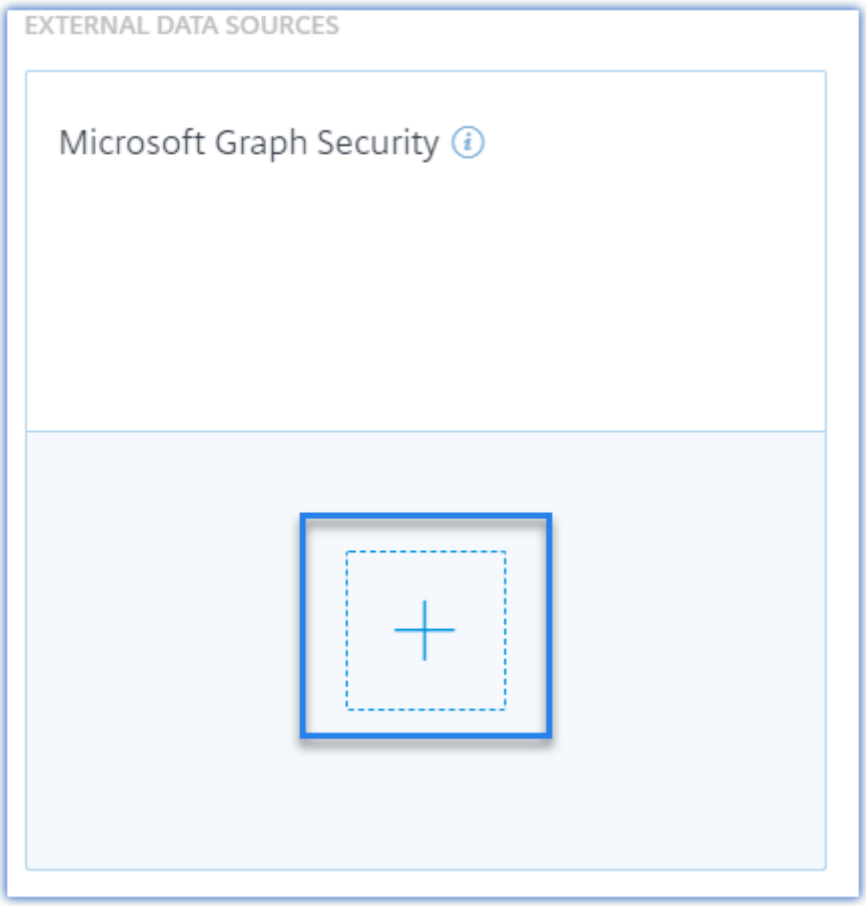
2018 年 **11** 月 **29** 日

新機能

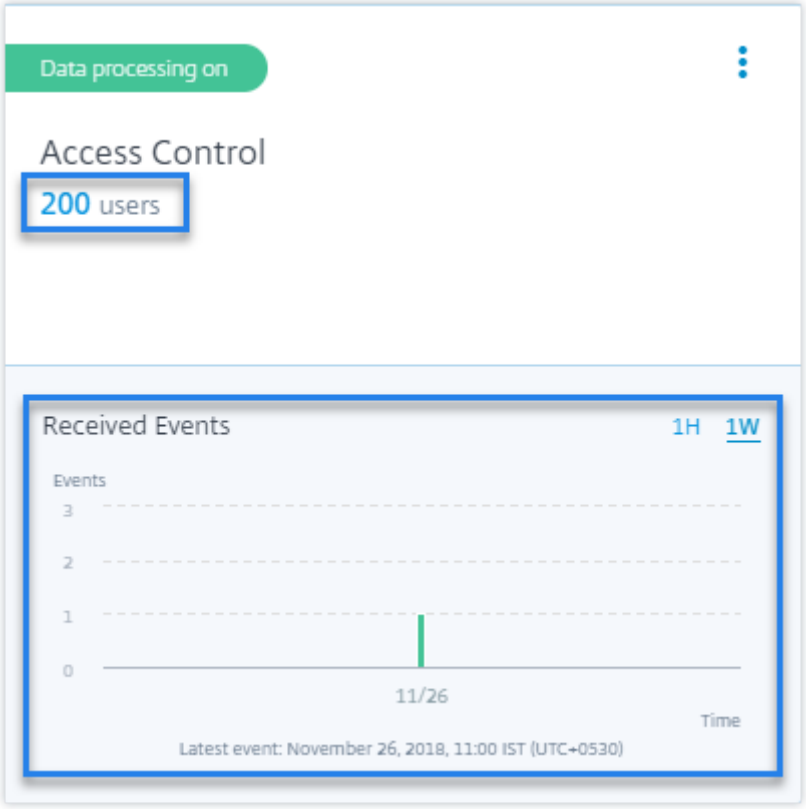
Microsoft セキュリティグラフデータソース　Microsoft Graph セキュリティは 、複数のセキュリティプロバイダのデータを集約する外部データソースです。また、ユーザインベントリデータへのアクセスも提供します。

Citrix Analytics は現在、このデータソースに関連付けられている **Azure AD** アイデンティティ保護およびエンドポイント向けセキュリティプロバイダー向け **Microsoft Defender** をサポートしています。

このデータソースをオンボードするには、Microsoft ID プラットフォームからアクセス許可を取得する必要があります。詳細については、「Microsoft Graph セキュリティ」を参照してください。



データソースのサイトカードでイベントの詳細と検出されたユーザーの表示　データソースのサイトカードには、イベントの詳細とユーザー数が表示されます。たとえば、サイトカードでアクセス制御のイベントの詳細とユーザーを表示できます。詳細については、「データソースでの Analytics の有効化」を参照してください。



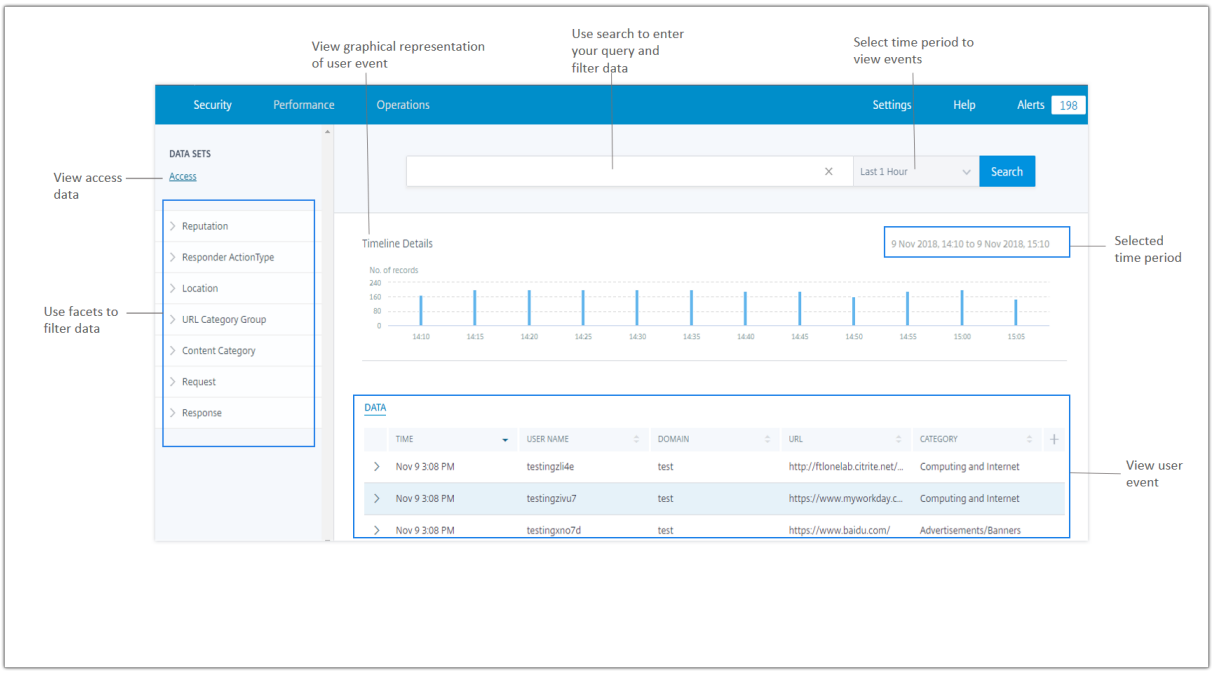
2018 年 **11** 月 **16** 日

新機能

アクセスデータのセルフサービス検索　セルフサービス検索を使用すると、企業内のユーザーのアクセス詳細を把握できます。Citrix Analytics は、Citrix アクセス制御サービスからユーザーのアクセス詳細を収集します。ファセットと検索クエリを使用して、検索結果を絞り込みます。

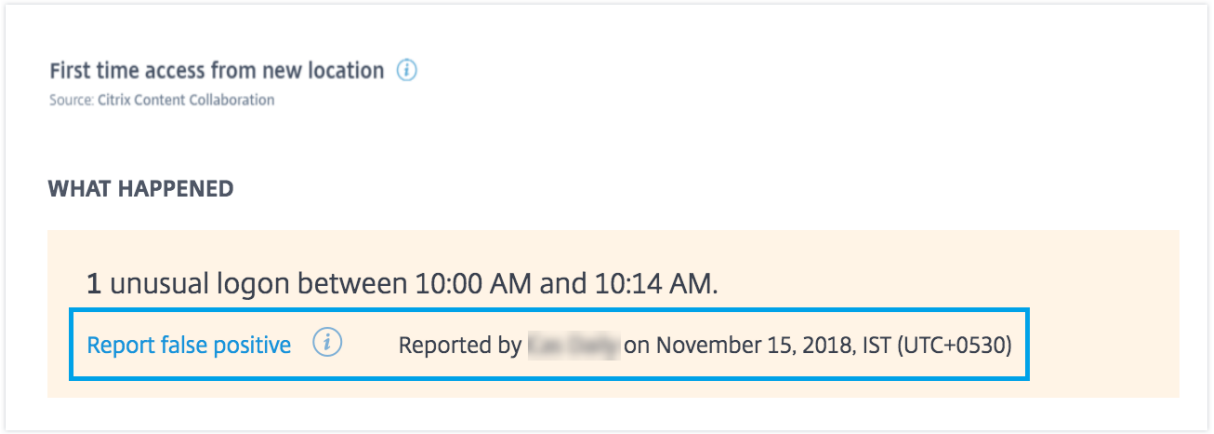
セルフサービス検索ページを使用するには、［セキュリティ］タブの［イベント検索］をクリックします。

詳細については、「Access のセルフサービス検索」を参照してください。



リスク指標のフィードバック　Citrix Analytics のリスク指標フィードバック機能を使用すると、リスク指標に関するフィードバックを提供できます。フィードバックは、報告されたセキュリティインシデントが正確であるかどうかを確認するのに役立ちます。

現在、この機能は Content Collaboration データソースによってトリガーされる異常なログオンアクセスのリスク指標でサポートされています。トリガーされたこのリスク指標が正しくない場合は、偽陽性として報告し、フィードバックを提供できます。以前に送信したフィードバックを編集することもできます。Citrix Analytics はフィードバックをキャプチャし、予測された情報を検証して、異常な動作検出を最適化します。



解決された問題

- Internet Explorer 11.0 を使用して Citrix Analytics にアクセスしている場合、ポリシーを編集および保存することはできません。

既知の問題

December 7, 2023

セキュリティ向け Citrix Analytics には、次の既知の問題があります。

- Linux 向け Citrix Workspace アプリは、アプリとデスクトップを Web ブラウザーで開き、ネイティブクライアント上の ICA から起動すると、Citrix Analytics に印刷イベントを送信できません。[CAS-36238]

  > 注:
  >
  > すべてのプラットフォームでの Citrix Workspace kspace アプリおよび Citrix Receiver のライフサイクル期間とライフサイクルのフェーズ（一般提供、メンテナンス終了、およびサポート終了）について詳しくは、「Citrix Workspace アプリおよび Citrix Receiver のライフサイクルマイルストーン」を参照してください。

Citrix Analytics オファリング

December 7, 2023

Citrix Analytics for Security

セキュアプライベートアクセス、Citrix Virtual Apps and Desktops、Citrix DaaS サイト、NetScaler Gateway など、顧客の接続されたデータソースから収集されたユーザーとアプリケーションの行動を照合して可視化します。行動のあらゆる側面を追跡でき、高度な機械学習アルゴリズムを活用することで、通常の行動と悪意のある攻撃者を区別できます。これにより、内部および外部の脅威をプロアクティブに特定して管理できます。

詳細：Citrix Analytics for Security

Citrix Analytics for Performance

Citrix Virtual Apps and Desktops Citrix DaaS サイトのハイブリッド展開全体にわたる包括的なエンドツーエンドの可視性を提供します。パフォーマンスはユーザーエクスペリエンススコアによって示されます。ユーザーエクスペリエンススコアは、シトリックスが提供する公開アプリケーション、公開デスクトップ、またはリモート PC を使用したときのユーザーエクスペリエンスを定義する履歴要因とメトリックを定量化したものです。

詳細：パフォーマンス向け Citrix Analytics

シトリックスアナリティクス-使用状況（サポート終了）

> 注
>
> :Citrix Usage Analytics のサポートが終了したため、ユーザーは利用できなくなりました。

データソース

April 12, 2024

データソースは、Citrix Analytics にデータを送信するクラウドサービスとオンプレミス製品です。

Citrix データソース

次の表は、Citrix Analytics for Security でサポートされているさまざまな Citrix データソースの一覧です。詳しくは、「はじめに」を参照してください。

[データソース]	展開の種類	必要なエージェント	製品コンポーネントとバージョン
Citrix Endpoint Management	サービス	-	Citrix Endpoint Management
Gateway	オンプレミス	アプリケーション配信管理エージェント	NetScaler Gateway 12.0.56.16 以降
Citrix ID プロバイダー	サービス	-	Citrix ID およびアクセス管理
Citrix Secure Private Access	サービス	(該当なし) N/A	Citrix Secure Private Access
Citrix Remote Browser Isolation	サービス	-	Citrix Remote Browser Isolation

[データソース]	展開の種類	必要なエージェント	製品コンポーネントとバージョン
Citrix DaaS（旧称 Virtual Apps and Desktops サービス）	サービス	-	Windows 向け Citrix Workspace アプリ 1907 以降用、Mac 向け Citrix Workspace アプリ 1910.2 以降、HTML5 向け Citrix Workspace アプリ 2007 以降、Chrome 向け Citrix Workspace アプリ-Chrome Web Store で入手可能な最新バージョン、Android 向け Citrix Workspace アプリ-Google Play で利用可能な最新バージョン、iOS 向け Citrix Workspace アプリ Apple App Store で入手可能な最新バージョン、Linux 向け Citrix Workspace アプリ 2006 以降
Citrix Virtual Apps and Desktops	オンプレミス	Virtual Apps and Desktops エージェント	Citrix Virtual Apps and Desktops 7 1808、Citrix XenApp および XenDesktop 7.16 以降

[データソース]	展開の種類	必要なエージェント	製品コンポーネントとバージョン
		アクションなどの高度な機能にはエージェントが必要です。	Windows 向け Citrix Workspace アプリ 1907 以降用、Mac 向け Citrix Workspace アプリ 1910.2 以降、HTML5 向け Citrix Workspace アプリ 2007 以降、Chrome 向け Citrix Workspace アプリ-Chrome Web Store で入手可能な最新バージョン、Android 向け Citrix Workspace アプリ-Google Play で利用可能な最新バージョン、iOS 向け Citrix Workspace アプリ Apple App Store で入手可能な最新バージョン、Linux 向け Citrix Workspace アプリ 2006 以降 Citrix Director 7.16 以降 **Workspace** ユーザーの場合:Virtual Apps and Desktops オンプレミスサイトは、サイト集約を使用して Workspace に追加する必要があります。

[データソース]	展開の種類	必要なエージェント	製品コンポーネントとバージョン
			StoreFront ユーザーの場合：StoreFront 展開バージョンは StorFront 1906 以降である必要があります。StoreFront にアクセスするには、HTML5 互換ブラウザーの Citrix Receiver for Web サイト、Windows 向け Citrix Workspace アプリ 1907 以降、Linux 向け Citrix Workspace アプリ 2006 以降、Mac 向け Citrix Workspace アプリ 2006 以降のいずれかを使用してアクセスする必要があります。 **LTSR** のサポート: Citrix Virtual Apps and Desktops 7 1912 LTSR の場合、サポートされる StoreFront バージョンは 1912 です。

> 注
>
> Citrix 製品とそのサブスクリプションについては、Citrix Cloud サービスを参照してください 。

外部データソース

次の表に、Citrix Analytics for Security でサポートされている外部データソース（サードパーティ製品）を示します。

データソース	展開の種類	必要なエージェント
Microsoft Graph Security	サービス	-

データソース	展開の種類	必要なエージェント
Microsoft Active Directory	オンプレミス	Citrix Cloud Connector

サポートされているホームリージョン

Citrix Analytics for Security は、次のホームリージョンでサポートされています。

- 米国（米国）
- 欧州連合 (EU)
- アジア太平洋南部 (APS)

組織の場所に応じて、いずれかのホームリージョンの Citrix Cloud にオンボーディングできます。

データソースがサポートされていないホームリージョンで組織が Citrix Cloud にオンボーディングされている場合、データソースからユーザーイベントは取得されません。

次の表を使用して、データソースとそれらがサポートされているリージョンを表示します。

データソース	米国リージョンでのサポート	EU リージョンでのサポート	APS リージョンでサポートされています
Citrix Endpoint Management	はい	はい	はい
NetScaler Gateway (オンプレミス)	はい	はい	はい
Citrix ID プロバイダー	はい	はい	はい
Citrix Secure Private Access	はい	はい	はい
Citrix Remote Browser Isolation	はい	はい	はい
Citrix DaaS（旧称: Citrix Virtual Apps and Desktops サービス）	はい	はい	はい
Citrix Virtual Apps and Desktops オンプレミス	はい	はい	はい
Microsoft Active Directory	はい	はい	はい
Microsoft Graph Security	はい	はい	はい

Citrix Workspace アプリのバージョンマトリックス

このセクションには、すべてのテレメトリを送信し、必要なすべての重大なバグ修正を含む Citrix Workspace アプリのサポート対象バージョンを示します。

次の表は、Citrix Workspace アプリでサポートされているバージョンとサポートされていないバージョンを示しています。

プラットフォーム	サポートされるバージョン
Windows	CU3 以降のすべての LTSR 2203 リリース 23.0.3.0 またはそれ以上
HTML5	21.5.0.0 またはそれ以上
Macintosh	21.0.4.0 またはそれ以上
Linux	21.4.0.0 またはそれ以上
Chrome	21.5.0.0 またはそれ以上
iOS	21.4.0.0 またはそれ以上
Android	21.5.0.0 またはそれ以上

次の表は、オペレーティングシステムが Citrix Analytics for Security で以下のユーザーイベント属性を受信するために必要な Citrix Workspace アプリの最小バージョンを示しています。

イベント属性	関連フィーチャー	Windows	Mac	Linux	HTML5	Chrome	iOS	Android
都市、国	アクセス保証の場所、セルフサービス検索-アプリケーションとデスクトップ	2008 以降	2006 以降	2104 またはそれ以上	2007 以降	Chrome Web Store で利用可能な最新バージョン	Apple App Store で最新バージョンが入手可能	Google Play で利用できる最新バージョン

イベント属性	関連フィーチャー	Windows	Mac	Linux	HTML5	Chrome	iOS	Android
クライアント IP	セルフサービス検索-アプリケーションとデスクトップ	2008 以降	2006 以降	2104 またはそれ以上	2007 以降	Chrome Web Store で利用可能な最新バージョン	Apple App Store で最新バージョンが入手可能	Google Play で利用できる最新バージョン
OS 名、OS バージョン、OS 追加情報	セルフサービス検索-アプリケーションとデスクトップ	2109 またはそれ以上	2108 またはそれ以上	2104 またはそれ以上	2007 以降	Chrome Web Store で利用可能な最新バージョン	Apple App Store で最新バージョンが入手可能	Google Play で利用できる最新バージョン
プリンタ名	セルフサービス検索-アプリケーションとデスクトップ	2106 またはそれ以降	1809 またはそれ以降	2006 以降	1911 以降	Chrome Web Store で利用可能な最新バージョン	Apple App Store で最新バージョンが入手可能	Google Play で利用できる最新バージョン
Web 起動のすべてのユーザーイベント	セルフサービス検索-アプリケーションとデスクトップ	2008 以降	2006 以降	2006 以降	該当なし	未サポート	Apple App Store で最新バージョンが入手可能	Google Play で利用できる最新バージョン

データガバナンス

December 7, 2023

このセクションでは、Citrix Analytics サービスによるログの収集、保存、および保持に関する情報を提供します。「定義 」セクションで定義されていない大文字の用語は、Citrix エンドユーザーサービス契約で指定された意味を持ちます。

Citrix Analytics は、Citrix コンピューティング環境でのアクティビティに関する洞察を顧客に提供するように設計されています。Citrix Analytics を使用すると、セキュリティ管理者は、監視するログを選択し、ログに記録されたアクティビティに基づいて指示されたアクションを実行できます。これらのインサイトは、セキュリティ管理者がコ

ンピューティング環境へのアクセスを管理し、お客様のコンピューティング環境にあるカスタマーコンテンツを保護するのに役立ちます。

データ所在地

Citrix Analytics ログはデータソースとは別に保持され、米国、欧州連合、およびアジア太平洋南部地域にある複数の Microsoft Azure Cloud 環境に集約されます。ログのストレージは、Citrix Cloud 管理者が組織を Citrix Cloud にオンボーディングするときに選択したホームリージョンによって異なります。たとえば、組織を Citrix Cloud にオンボーディングするときにヨーロッパリージョンを選択した場合、Citrix Analytics ログは欧州連合の Microsoft Azure 環境に格納されます。

詳しくは、「Citrix Cloud Services の顧客コンテンツとログの処理 」および「地理的考慮事項」を参照してください。

データ収集

Citrix Cloud サービスは、ログを Citrix Analytics に送信するようにインストルメントされています。ログは、次のデータソースから収集されます。

- NetScaler ADC（オンプレミス）と NetScaler Application Delivery Management サブスクリプション
- Citrix Endpoint Management
- NetScaler Gateway (オンプレミス)
- Citrix ID プロバイダー
- Citrix Secure Browser
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS （旧 Citrix Virtual Apps and Desktops サービス）
- Microsoft Active Directory
- Microsoft Graph Security

データ送信

Citrix Cloud のログは、Citrix Analytics に安全に送信されます。顧客環境の管理者が Citrix Analytics を明示的に有効にすると、これらのログが分析され、顧客データベースに保存されます。Citrix Workspace Citrix Virtual Apps and Desktops
が構成されているデータソースにも同じことが当てはまります。

NetScaler ADC データソースの場合、ログ転送は、管理者が特定のデータソースに対して明示的に Citrix Analytics を有効にする場合にのみ開始されます。

データ管理

Citrix Analytics に送信されるログは、管理者がいつでもオンまたはオフにすることができます。

NetScaler ADC オンプレミスデータソースに対してオフにすると、特定の ADC データソースと Citrix Analytics 間の通信が停止します。

他のデータソースですべてオフにすると、特定のデータソースのログは分析されなくなり、Citrix Analytics に保存されなくなります。

データ保持

Citrix Analytics ログは、最大 13 か月または 396 日間、識別可能な形式で保持されます。すべてのログおよび関連する分析データ（ユーザーリスクプロファイル、ユーザーリスクスコアの詳細、ユーザーリスクイベントの詳細、ユーザーウォッチリスト、ユーザーアクション、ユーザープロファイルなど）は、この期間保持されます。

たとえば、2021 年 1 月 1 日にデータソースでアナリティクスを有効にした場合、デフォルトでは、2021 年 1 月 1 日に収集されたデータは、2022 年 1 月 31 日まで Citrix Analytics に保持されます。同様に、2021 年 1 月 15 日に収集されたデータは、2022 年 2 月 15 日まで保持されます。

このデータは、データソースのデータ処理をオフにした後や、Citrix Analytics からデータソースを削除した後でも、デフォルトのデータ保持期間にわたって保存されます。

Citrix Analytics は、サブスクリプションの有効期限または試用期間の 90 日後にすべてのカスタマーコンテンツを削除します。

データのエクスポート

このセクションでは、セキュリティのための Citrix Analytics とパフォーマンスのための Citrix Analytics からエクスポートされたデータについて説明します。

Citrix Analytics for Performance は、データソースからパフォーマンスメトリックを収集して分析します。

セルフサービス検索ページから CSV ファイルとしてデータをダウンロードできます。

Citrix Analytics for Security は、さまざまな製品（データソース）からユーザーイベントを収集します。これらのイベントは、ユーザーの危険で異常な動作を可視化するために処理されます。ユーザーのリスクインサイトとユーザーのイベントに関連するこれらの処理済みデータを、システム情報およびイベント管理 (SIEM) サービスにエクスポートできます。

現在、データは Citrix Analytics for Security から次の 2 つの方法でエクスポートできます。

- Citrix Analytics for Security を SIEM サービスと統合する
- セルフサービス検索ページからデータを CSV ファイルとしてダウンロードします。

Citrix Analytics for Security を SIEM サービスと統合すると、北行きの Kafka トピックまたは Logstash ベースのデータコネクタのいずれかを使用して、データが SIEM サービスに送信されます。

現在、次の SIEM サービスと統合できます。

- Splunk（Citrix Analytics アドオンを介して接続することにより）
- Elasticsearch や Microsoft Azure Sentinel などの Kafka トピックまたは Logstash ベースのデータコネクタをサポートする SIEM サービス

CSV ファイルを使用して SIEM サービスにデータをエクスポートすることもできます。[セルフサービス検索] ページでは、データソースのデータ (ユーザーイベント) を表示し、そのデータを CSV ファイルとしてダウンロードできます。CSV ファイルの詳細については、「セルフサービス検索」を参照してください。

> 重要
>
> SIEM サービスにデータがエクスポートされると、Citrix はエクスポートされたデータのセキュリティ、ストレージ、管理、および SIEM 環境での使用について責任を負いません。

Citrix Analytics for Security から SIEM サービスへのデータ転送をオンまたはオフにできます。

処理されたデータと SIEM 統合について詳しくは、「SIEM （セキュリティ情報およびイベント管理）の統合」および「SIEMの Citrix Analytics データ形式」を参照してください。

Citrix Services Security Exhibit

アクセスと認証、セキュリティプログラム管理、ビジネス継続性、インシデント管理など、Citrix Analytics に適用されるセキュリティ制御に関する詳細情報は、Citrix Services のセキュリティに関する展示会に含まれています。

定義

顧客コンテンツとは、Citrix がサービスを実行するためのアクセスを提供されているお客様の環境におけるストレージまたはデータのためにお客様のアカウントにアップロードされるデータを意味します。

ログ：パフォーマンス、安定性、使用状況、セキュリティ、およびサポートを測定するレコードを含む、サービスに関連するイベントのレコードを意味します。

サービスとは、Citrix Analytics の目的で上記に概説した Citrix Cloud クラウドサービスを意味します。

データ収集契約

お客様のデータを Citrix Analytics にアップロードし、Citrix Analytics の機能を使用することにより、お客様は、Citrix がお客様の Citrix 製品およびサービスに関する技術情報、ユーザー情報、または関連情報を収集、保存、送信、維持、処理、および使用することに同意し、同意するものとします。

Citrix は、受信した情報を常に Citrix プライバシーポリシーに従って取り扱います。

付録**:** 収集されたログ

- セキュリティログの Citrix Analytics
- パフォーマンス向け Citrix Analytics ログ

セキュリティログの **Citrix Analytics**

一般ログ

一般に、Citrix Analytics ログには次のヘッダー識別データポイントが含まれます。

- ヘッダーキー
- デバイス識別
- 識別
- IP アドレス
- 組織
- Product
- 製品バージョン
- システム時刻
- テナントの識別
- 種類
- ユーザー: 電子メール、ID、SAM アカウント名、ドメイン、UPN
- バージョン

Citrix Endpoint Management サービスログ

Citrix Endpoint Management サービスのログには、次のデータポイントが含まれています。

- コンプライアンス
- 企業所有
- デバイス ID
- デバイスモデル
- デバイスの種類
- 地理緯度
- 地理経度
- ホスト名
- IMEI
- IP アドレス
- ジェイル・ブロークン
- 前回のアクティビティ
- 管理モード
- オペレーティングシステム
- オペレーティングシステムバージョン
- プラットフォーム情報
- 理由
- シリアル番号
- 監視対象

Citrix Secure Private Access ログ

- AAA ユーザ名
- 認証ポリシーアクション名
- 認証セッション ID
- リクエスト URL
- URL カテゴリポリシー名
- VPN セッション ID
- 仮想サーバー IP
- AAA ユーザの電子メール ID

- 実際のテンプレートコード
- アプリ FQDN
- アプリ名
- アプリケーション名 Vserver LS
- アプリケーションフラグ
- 認証の種類
- 認証ステージ
- 認証ステータスコード
- バックエンドサーバー DST IPv4 アドレス
- バックエンドサーバー IPv4 アドレス
- バックエンドサーバー IPv6 アドレス
- カテゴリドメイン名
- カテゴリドメインソース
- クライアント IP
- クライアント MSS
- クライアント高速レトックスカウント
- クライアント TCP ジッター
- 再送信されたクライアント TCP パケット
- クライアント TCP RTO カウント
- クライアント TCP ゼロウィンドウカウント
- Clt フローフラグ Rx
- Clt フローフラグ Tx
- Clt TCP フラグ Rx
- Clt TCP フラグ Tx
- 接続チェーンホップカウント
- 接続チェーン ID
- 出力インターフェイス
- プロセス ID をエクスポート中
- フローフラグ Rx

- フローフラグ Tx
- HTTP コンテンツタイプ
- HTTP ドメイン名
- HTTP 要求認証
- HTTP 要求クッキー
- HTTP Req Forw FB
- HTTP Req Forw LB
- HTTP 要求ホスト
- HTTP 要求メソッド
- HTTP Req Rcv FB
- HTTP Req Rcv LB
- HTTP 要求リファラー
- HTTP リクエストの URL
- HTTP Req XForwarded For
- HTTP RES Forw FB
- HTTP Res Forw LB
- HTTP 解像度ロケーション
- HTTP 解像度 Rcv FB
- HTTP Res Rcv LB
- HTTP 解像度セットクッキー
- HTTP Rsp Len
- HTTP Rsp Status
- HTTP トランザクション終了時刻
- HTTP トランザクション ID
- IC Cont Grp Name
- IC フラグ
- IC ストアフラグなし
- IC ポリシー名
- Ingress インターフェイスクライアント

- NetScaler Gateway Service アプリ ID
- NetScaler Gateway Service アプリ名
- NetScaler Gateway Service アプリの種類
- NetScaler パーティション ID
- 観測ドメイン ID
- 観測ポイント ID
- 原点解像度ステータス
- オリジン Rsp レン
- プロトコル識別子
- レート制限識別子の名前
- レコードタイプ
- レスポンダーアクションタイプ
- レスポンスメディアタイプ
- Srv フローフラグ Rx
- Srv フローフラグ Tx
- サーブ高速レトックスカウント
- サーバー TCP ジッター
- 再送信されたサーバ TCP パケット
- サーバー TCP Rot カウント
- サーバー TCP ゼロウィンドウカウント
- SSL 暗号値 BE
- SSL 暗号値 FE
- SSL クライアント証明書サイズ BE
- SSL クライアント証明書サイズ FE
- SSL Clnt Cert Sig Hash BE
- SSL Clnt Cert Sig Hash FE
- SSL エラーアプリ名
- SSL エラーフラグ
- SSL フラグ

- SSL フラグ FE
- SSL ハンドシェイクエラーメッセージ
- SSL サーバ証明書サイズ BE
- SSL サーバ証明書サイズ FE
- SSL Session ID BE
- SSL セッション ID FE
- SSL Sig Hash Alg BE
- SSL Sig Hash Alg FE
- SSL Srvr Cert Sig Hash BE
- SSL Srvr Cert Sig Hash FE
- SSL iDomain Category
- SSL iDomain カテゴリグループ
- SSL ID ドメイン名
- SSL IDomain レピュテーション
- SSL i 実行アクション
- SSL iPolicy アクション
- SSL iReason for アクション
- SSL iURL セットが一致しました
- SSL iURL セットプライベート
- 加入者識別子
- Svr Tcp フラグ Rx
- Svr Tcp フラグ Tx
- テナント名
- Req 親スパン ID のトレース
- Req スパン ID のトレース
- トレーストレース ID
- トランスコルトダスト IPv4 アドレス
- トランスコルトダスト IPv6 アドレス
- トランス Clt Dst ポート

- トランス Clt フローエンドユーザーレックス
- トランス Clt フローエンドユーザー税
- トランス Clt フロー開始 Usec Rx
- トランス Clt フロー開始使用税
- トランス Clt IPv4 アドレス
- トランス Clt IPv6 アドレス
- トランスコルトパケット Tox Cnt Rex
- トランスコルトパケットトート Cnt Tx
- トランス・コルト RTT
- トランス Clt Src ポート
- トランス・コルト・トット・レックス 10 月 Cnt
- トランスコルトトート税 10 月 Cnt
- トランス情報
- トランスサーブ Dst ポート
- トランスサーブパケットトート Cnt Rx
- トランスサーブパケットトート Cnt Tx
- トランス Srv Src ポート
- トランス Svr フローエンドユーザー Rx
- Trans Svr フローエンドユーザー Tx
- Trans Svr Flow Start Usec Rx
- Trans Svr Flow Start Usec Tx
- Trans Svr RTT
- Trans Svr Tot Rx Oct Cnt
- Trans Svr Tot Tx Oct Cnt
- トランザクション ID
- URL カテゴリ
- URL カテゴリグループ
- URL カテゴリレピュテーション
- URL カテゴリアクションの理由

- 一致した URL セット
- URL セットプライベート
- URL オブジェクト ID
- VLAN 番号

Citrix Virtual Apps and Desktops および **Citrix DaaS** ログ

Citrix Virtual Apps and Desktops、および Citrix DaaS ログには、次のデータポイントが含まれます。

- アプリ名
- ブラウザー
- カスタマー ID
- 詳細: フォーマットサイズ、フォーマットタイプ、イニシエータ、結果
- デバイス ID
- デバイスの種類
- フィードバック
- フィードバック ID
- ファイル名
- [ファイルパス]
- ファイルサイズ
- Is like
- ジェイル・ブロークン
- ジョブの詳細: ファイル名、フォーマット、サイズ
- 位置: 推定、緯度、経度

  > 注
  >
  > 位置情報は都市レベルおよび国レベルで提供され、正確な地理的位置情報を表すものではありません。

- 長い CMD ライン
- モジュールファイルパス
- 操作
- オペレーティングシステム
- プラットフォームの追加情報

- プリンタ名
- 質問
- 質問 ID
- SaaS アプリケーション名
- セッションドメイン
- セッションサーバー名
- セッションユーザー名
- セッション GUID
- Timestamp
- タイムゾーン: バイアス、DST、名前
- 印刷部数の総数
- 総印刷ページ数
- 種類
- URL
- ユーザー エージェント

NetScaler ADC ログ

NetScaler ADC ログには、次のデータポイントが含まれています。

- コンテナ
- ファイル
- 形式
- 種類

Azure ログ用 **Citrix DaaS** スタンダード

Azure 向け Citrix DaaS Standard ログには、次のデータポイントが含まれています。

- アプリ名
- ブラウザー
- 詳細: フォーマットサイズ、フォーマットタイプ、イニシエータ、結果
- デバイス ID

- デバイスの種類
- ファイル名
- [ファイルパス]
- ファイルサイズ
- ジェイル・ブロークン
- ジョブの詳細: ファイル名、フォーマット、サイズ
- 位置: 推定、緯度、経度

  > 注
  >
  > 位置情報は都市レベルおよび国レベルで提供され、正確な地理的位置情報を表すものではありません。

- 長い CMD ライン
- モジュールファイルパス
- 操作
- オペレーティングシステム
- プラットフォームの追加情報
- プリンタ名
- SaaS アプリケーション名
- セッションドメイン
- セッションサーバー名
- セッションユーザー名
- セッション GUID
- Timestamp
- タイムゾーン: バイアス、DST、名前
- 種類
- URL
- ユーザー エージェント

Citrix アイデンティティプロバイダーのログ

- ユーザーログイン:
  - 認証ドメイン: 名前、製品、IdP タイプ、IdP 表示名

        * IdP プロパティ: アプリケーション、認証タイプ、顧客 ID、クライアント ID、ディレクトリ、発行者、ロゴ、リソース、TID
        * 拡張機能:
            - ワークスペース: 背景色、ヘッダーロゴ、ログオンロゴ、リンクの色、テキストの色、StoreFront ドメイン
            - ShareFile: カスタマー ID、カスタマージオ
            - 長寿命トークン: 有効、有効期限タイプ、絶対有効期限秒、スライディング有効期限秒
    - 認証結果: ユーザー名、エラーメッセージ
    - サインインメッセージ: クライアント ID、クライアント名
    - ユーザーの要求:AMR、アクセストークンハッシュ、Aud、認証時間、CIP Cred、認証エイリアス、認証ドメイン、グループ、製品、システムエイリアス、電子メール、
      検証済み E メール、Exp、ファミリー名、指定された名前、IAT、IdP、ISS、ロケール、名前、NBF、SID、サブ
        * 認証エイリアスの要求: 名前、値
        * ディレクトリコンテキスト: ドメイン、フォレスト、ID プロバイダ、テナント ID
        * ユーザー: 顧客、電子メール、OID、SID、UPN
        * IdP エクストラフィールド:Azure AD OID、Azure AD TID
- ユーザーログオフ: クライアント ID、クライアント名、ナンス、サブ
- クライアントアップデート: アクション、クライアント ID、クライアント名

NetScaler Gateway ログ

- トランザクションイベント:
    - ICA アプリケーション: レコードタイプ、実際のテンプレートコード、観測ドメイン ID、観測ポイント ID、エクスポートプロセス ID、ICA セッション GUID、MSI クライアント Cookie、フロー ID Rx、ICA フラグ、接続 ID、パディングオクテット 2、ICA デバイスシリアル番号、IP バージョン 4、プロトコル識別子、送信元 IPv4 アドレス Rx、宛先 IPv4 アドレス Rx、ソーストランスポートポート Rx、宛先トランスポートポート Rx、ICA アプリケーションの起動期間、ICA 起動メカニズム、ICA アプリケーションの起動時間、ICA プロセス ID の起動、ICA アプリケーション名、ICA アプリケーションモジュールパス、ICA アプリケーションの終了タイプ、ICA アプリケーションの終了時間、アプリケーション名アプリケーション ID、ICA アプリケーションプロセス ID 終了、ICA アプリケーション
    - ICA イベント: レコードタイプ、実際のテンプレートコード、ソース IPv4 アドレス Rx、宛先 IPv4 アドレス Rx、ICA セッション GUID、MSI クライアント Cookie、接続チェーン ID、ICA クライアントバー

ジョン、ICA クライアントホスト名、ICA ユーザー名、ICA ドメイン名、ログオンチケットの設定、サーバー名、サーバーバージョン、フロー Id Rx、ICA フラグ、観察ポイント ID、エクスポートプロセス ID、監視ドメイン ID、接続 ID、ICA デバイスのシリアル番号、ICA セッションのセットアップ時間、ICA クライアント IP、NS ICA セッション状態のセットアップ、ソーストランスポートポート Rx、送信先トランスポートポート Rx、ICA クライアント起動ツール、ICA クライアントの種類、ICA 接続の優先度のセットアップ、NS ICA セッションサーバーポート、NS ICA セッションサーバ IP アドレス、IPv4、プロトコル識別子、接続チェーンホップカウント、アクセスタイプ

- ICA 更新: レコードタイプ、実際のテンプレートコード、観測ドメイン ID、観測ポイント ID、エクスポートプロセス ID、ICA セッション GUID、MSI クライアント Cookie、フロー ID Rx、ICA フラグ、接続 ID、ICA デバイスシリアル番号、IPv4、プロトコル識別子、パディングオクテット 2、ICA RTT、クライアント側の RX バイト、クライアント側パケット再送信、サーバー側パケット再送信、クライアント側 RTT、クライアント側ジッター、サーバー側ジッター、ICA ネットワーク更新開始時刻、ICA ネットワーク更新終了時刻、クライアント側 SRTT、サーバー側遅延、サーバー側遅延、ホスト遅延、クライアント側ゼロウィンドウ数、サーバー側ゼロウィンドウ数、クライアントサイド RTO カウント、サーバー側 RTO カウント、L7 クライアント遅延、L7 サーバー遅延、アプリケーション名アプリケーション ID、テナント名、ICA セッション更新開始秒、ICA セッション更新終了秒、ICA チャネル ID 1、ICA チャネル ID 2、ICA チャネル ID 2 バイト、ICA チャネル ID 3 バイト、ICA チャネル ID 3 バイト、ICA チャネル ID 4 バイト、ICA チャネル ID 5、ICA チャネル ID 5 バイト
- AppFlow 構成: レコードタイプ、実際のテンプレートコード、観測ドメイン ID、観測ポイント ID、エクスポートプロセス ID、システムルールフラグ 1、システム安全性インデックス、AppFlow プロファイル緩和フラグ、AppFlow プロファイルブロックフラグ、AppFlow プロファイルログフラグ、AppFlow プロファイル学習フラグ、AppFlow プロファイル統計フラグ、AppFlow プロファイル統計フラグ、AppFlow プロファイルなしフラグ、AppFlow アプリケーション名 ID、AppFlow プロファイル記号無効、AppFlow プロファイル符号ブロック数、AppFlow プロファイル符号ログ数、AppFlow プロファイル記号統計数、AppFlow 化身番号、AppFlow シーケンス番号、AppFlow プロファイル記号自動更新、AppFlow 安全性インデックス、AppFlow アプリケーション安全性インデックス、AppFlow プロファイル秒チェック安全性インデックス、AppFlow プロファイルタイプ、Iprep アプリケーション安全性インデックス、AppFlow プロファイル名、AppFlow シグネーム、AppFlow アプリケーション名 Ls、AppFlow シグルール ID1、AppFlow シグルール ID2、AppFlow シグルール ID3、AppFlow シグルール ID4、AppFlow シグルール ID5、AppFlow シグルール有効フラグ、AppFlow シグルールログフラグ、AppFlow シグルールファイル名、AppFlow シグルールカテゴリ 1、AppFlow シグルール Logstring1、AppFlow シグルールカテゴリ 2、AppFlow シグルール LogString2、AppFlow シグルールカテゴリ 3、AppFlow シグルールカテゴリ 4、AppFlow シグルール Logstring4、AppFlow シグルールカテゴリ 5、AppFlow Sig ルール logString5
- AppFlow: 実際のテンプレートコード、観測ドメイン ID、観測ポイント ID、エクスポートプロセス ID、トランザクション ID、Appfw 違反発生時間、アプリ名アプリ ID、appfw 違反の重大度、appfw 違反タイプ、appfw 違反場所、appfw 違反脅威インデックス、appfw NS 経度、appfw NS 緯度、ソース IPv4 アドレス Rx、appfw Http メソッド、Appfw アプリケーション脅威インデックス、appfw ブロックフラグ、appfw 変換フラグ、appfw 違反プロファイル名、appfw セッション ID、appfw Req

URL、appfw 地理ロケーション、appfw 違反タイプ名 1、appfw 違反名の値 1、appfw シグカテゴリ 1、appfw 違反タイプ名 2、appfw 違反名前値 2、appfw シグカテゴリ 2、appfw 違反タイプ名 3、appfw 違反名の値 3、appfw シグカテゴリ 3、Appfw 要望 X 転送対用、Appfw アプリケーション名 Ls、アプリケーション名 Ps、Iprep カテゴリ、iprep 攻撃時間、Iprep レピュテーションスコア、Iprep NS 経度、Iprep NS 緯度、Iprep 重大度、Iprep HTTP メソッド、Iprep アプリ脅威インデックス、iprep 地理ロケーション、Tcp Syn 攻撃センター、Tcp 低速リスクセンター、TCP ゼロウィンドウセンター、Appfw ログ Expr 名、Appfw ログ Expr 値、Appfw Log Expr コメント

- VPN: 実際のテンプレートコード、観測ドメイン ID、アクセスインサイトフラグ、観測ポイント ID、エクスポートプロセス ID、アクセスインサイトステータスコード、アクセスインサイトのタイムスタンプ、認証期間、デバイスタイプ、デバイス ID、デバイスの場所、アプリ名アプリ ID、アプリ名アプリ Id、アプリ名アプリ Id1、ソーストランスポートポート Rx、宛先トランスポートポート Rx、認証ステージ、認証タイプ、VPN セッション ID、EPA ID、AAA ユーザ名、ポリシー名、認証エージェント名、グループ名、仮想サーバ FQDN、Csec 式、送信元 IPv4 アドレス Rx、宛先 IPv4 アドレス Rx、CUR ファクタポリシーラベル、次の要素ポリシーラベル、アプリケーション名 Ls、アプリケーション名 1 Ls、AAA ユーザ電子メール ID、ゲートウェイ IP、ゲートウェイポート、アプリケーションバイト数、VPN セッション状態、VPN セッションモード、SSO 認証方式、IIP アドレス、VPN 要求 URL、SSO 要求 URL、バックエンドサーバ名、VPN セッションログアウトモード、ログオンチケットファイル情報、STA チケット、セッション共有キー、リソース名、SNIP アドレス、一時 VPN セッション ID
- HTTP: 実際のテンプレートコード, HTTP 要求メソッド, HTTP 要求 URL, HTTP 要求ユーザエージェント, HTTP コンテンツタイプ, HTTP 要求ホスト, HTTP 要求承認, HTTP 要求クッキー, HTTP 要求リファラ, HTTP 解像度セットクッキー, IC 続き GRP 名, IC フラグ, IC Nostore フラグ, IC ポリシー名, 応答メディアタイプ, 入力インターフェイスクライアント, オリジン解像度ステータス、オリジン Rsp Len、Srv フローフラグ Rx、Srv フローフラグ Tx、フローフラグ Tx、フローフラグ Tx、アプリケーション名、観測ポイント ID、エクスポートプロセス ID、観測ドメイン ID、Http トランス終了時刻、トランザクション ID、Http Rsp ステータス、トランス clt Ipv4 アドレス、トランス clt dst Ipv4 アドレス、バックエンド Svr Ipv4 アドレス, Http Rsp Len, Trans Svr RTT, Trans Clt RTT, Http Req Rcv FB, Http Req Rcv LB, Http Res Rcv LB, Http Req Forw LB, Http Req Forw LB, Http Req X Forw 転送先、Http ドメイン名、HTTP Res ロケーション、プロトコル識別子、出力インターフェイス、バックエンド保存 IPv6 アドレス、SSL フラグ BE、SSL フラグ FE、SSL セッション IDBE、SSL セッション IDBE、SSL 暗号値 FE、SSL 暗号値 BE、SSL 署名ハッシュアルグ BE、SSL サーバー証明書署名ハッシュ BE、SSL サーバー証明書署名ハッシュ FE、SSL クライアント証明書署名ハッシュ FE、SSL クライアント証明書署名ハッシュ FE、SSL クライアント証明書署名ハッシュ BE、SSL サーバー証明書サイズ FE、SSL サーバー証明書サイズ BE、SSL クライアント証明書サイズ FE、SSL クライアント証明書サイズ BE、SSL エラーアプリケーション名、SSL エラーフラグ、SSL ハンドシェイクエラーメッセージ、クライアント IP、仮想サーバー IP、接続チェーン ID、接続チェーンホップカウント、トランス clt TotT Rx Oct Cnt、トランス clt TotTx Oct Cnt、トランス clt Src ポート、トランス Srv Src ポート、トランス Srv Dst ポート、VLAN 番号、クライアント mss、トランス情報、トランス Clt フロー終了使用 Rx、トランス CLT フロー終了 Usec Tx、トランス clt フロー開始使用 Rx、トランス clt フロー開始使用 Tx、トランス Svr フロー終了使用 Rx、トランス Svr フロー終了使用 Tx、トランス Svr フロー開始 Usec、

Trans Svr フロー開始 Usec Tx、Trans Svr Tot Rx Oct CNT、TransSvr Tit Tx Oct Cnt, clt フローフラグ Tx, clt フローフラグ Rx, トランス clt IPv6 アドレス, トランス CLT DST IPv6 アドレス, サブスクライバ識別子, SSLi ドメイン名, SSLi ドメインカテゴリ, SSLi ドメインカテゴリグループ, SSLI ドメインレピュテーション, SSLI ポリシーアクション, SSLI 実行アクション, SSLI アクションの理由, SSLI URL セット一致,SSLi URL セットプライベート、URL カテゴリ、URL カテゴリグループ、URL カテゴリレピュテーション、レスポンダアクションタイプ、一致した URL セット、URL セットプライベート、カテゴリドメイン名、カテゴリドメインソース、AAA ユーザ名、VPN セッション ID、テナント名

- メトリクスイベント:
  - vServer LB：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、表現、スキーマタイプ、時間、CPU、GSLB サーバー、GSLB 仮想サーバー、インターフェイス、メモリプール、サーバーサービスグループ、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer Cs、vServer LB：RATE Si Tet 要求バイト、RATE SiTot レスポンスバイト, RATE Si Tot レスポンス, RATE Si TotT clt Ttlb トランザクション, RATE Si Tott clt ttlb Pkt Rcvd, RATE Si TotT clt Pkt Sent, RATE Vsvr TotT Hits, Si Cur クライアント, Si Cur Conn 確立, Si Cur サーバ, Si Cur State, Si Tot リクエストバイト, Si Tot レスポンス, Si Tot レスポンス, Si Tott clt ttlb、Si Tott clt ttlb トランザクション、Si TotPkt Rcvd、Si TotPkt Sent Sent、Si TottLb イライラするトランザクション、Si TottTtlb 許容トランザクション、VSVR アクティブ SVC、VSVR TotTot ヒット、Vsvr TotReq Resp 無効、Vsvr TottReq Resp 無効なドロップ
  - CPU：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、表現、スキーマタイプ、時間、Cc CPU 使用 GSLB サーバー、GSLB 仮想サーバー、インターフェイス、メモリプール、NetScaler、サーバーサービスグループ、サーバー SVC Cfg、vServer Authn、vServer Cr、vServer CS、vServer Lb、vServer SSL、仮想サーバーユーザー
  - サーバーサービスグループ: バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、表現、スキーマタイプ、時間、Cc CPU 使用率、GSLB サーバー、GSLB 仮想サーバー、インターフェイス、メモリプール、NetScaler、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer CS、vServer Lb、vServer SSL、vServer ユーザー、サーバーサービスグループ：RATE Si Tot リクエストバイト, RATE Si Tot_Response バイト, RATE Si Tot_Response バイト, RATE Si Tott clt ttlb, RATE Si Tott clt Ttlb トランザクション, RATE Si Tott Si Tt SV ttfb トランザクション, RATE Si Tott Si Tvr ttfb トランザクション, RATE Si Tott Si Ttlb トランザクションイライラするトランザクション、RATE Si Tott Ttlb 許容トランザクション, Si Cur 状態, Si Tot リクエストバイト, Si Tot リクエスト, Si Tot レスポンスバイト, Si TotT clt Ttlb, Si TottClt Ttlb トランザクション, Si TotSvr ttfb, Si TotSvr Ttfb トランザクション, Si Tott Svr Ttlb トランザクション, Si Tott Svr Ttlb トランザクション, Si Tott Svr Ttlb トランザクション, Si Tots Svr Ttlb TotTtlb イライラするトランザクション、Si Totttlb 許容するトランザクション
  - サーバー SVC CFG：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、表現、スキーマタイプ、時間、CPU 使用率、GSLB サーバー、GSLB 仮想サーバー、インターフェイス、メモリプール、NetScaler、vServer Authn、vServer Cr、vServer CS、vServer Lb、vServer SSL、vServer ユーザー、サーバー SVC Cfg：RATE Si Totot 要求バイト、RATESi Tot 要求, RATE Si

Tot 応答バイト, RATE Si Tot 応答, Si Tott clt ttlb, RATE Si Tott Pkt rcvd, RATE Si Tott Pkt Si Pkt Si Tkt Sd, RATE Si Tott SVR Busy Err, RATE Si Tott SVR Tfb, RATE Si Tott Si Ttr Ttlb, RATE Si Tott svr ttlb Transactions, RATE SiTotTtlb イライラするトランザクション, RATE Si Tott ttlb 許容トランザクション, Si Cur 状態, Si Cur トランスポート, Si Tot リクエストバイト, Si Tot リクエスト, Si Tot レスポンスバイト, Si Tott clt ttlb, Si Tott clt Ttlb トランザクション, Si TotPkt Rcvd, Si Tott Pkt Sent Svr ビジーえーーーーーーーーーーーーーーーーーーーーーーーー Svr Ttfb トランザクション, Si TottSvr Ttlb, Si TotSvr Ttlb トランザクション, Si TottTtlb イライラするトランザクション, Si TottTtlb 許容トランザクション

- NetScaler：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、表現、スキーマタイプ、時間、GSLB サーバー、GSLB 仮想サーバー、インターフェイス、メモリプール、サーバーサービスグループ、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer CS、vServer Lb、vServer SSL、vServer ユーザー、NetScaler：RATE すべてニックトット Rx メガビット、RATE すべて NIC トット Rx メガビット、レート Dns トットクエリ、レート Dns トット Nxdmn エントリ、レート Http トット Gets、レート Http トットその他、レート Http トット投稿、レート Http トットリクエスト、レート Http トットリクエスト 1.0、レート Http トットリクエスト 1.1、レート Http トットリクエスト、レート Http トットリクエスト Rx レスポンスバイト、RATE Ip Tt Rx Mbit、RATE Ip TotT Rx バイト、RATE Ip Tt Rx Pits、RATE Ip Tt Tx バイト、RATE Ip Tt Tx バイト、RATE SSL Tt Dec バイト、RATE SSL TotT End バイト、RATE SSL Tt SSL 情報セッションヒット、RATE SSL トット SSL 情報合計送信カウント、レート Tcp エラー Rst、RATE Tcp Top クライアントオープン、レート Tcp Tt サーバーオープン、レート Tcp トット Rx バイト、レート Tcp トット Rx ポート、レート Tcp トット Syn、レート Tcp トット Tx バイト、レート Tcp トット Tx バイト、レート UDP トット Rx バイト、レート UDP トット Rx バイト、レート UDP トット Tx バイト、レート UDP トット Tx バイト、レート UDP トット Tx バイト、すべて NIC トット送信メガビット、CPU 使用、DNS トットクエリ、DNS トットネグ Nxdmn エントリ、Http トット取得, Http トットその他, Http トット投稿, Http トットリクエスト, Http トット Requests1.0, Http トットレスポンス, Http トット受信リクエストバイト, Http トット受信レスポンスバイト, IP トット受信メガビット, IP トット受信バイト, IP トット Rx Pkts, IP トット送信バイト, IP トット Pkt TS, Mem cur フリーサイズ, Mem Cur Free 実際のサイズ、メモリ CUR 使用サイズ、使用可能なメモリトット、管理追加 CPU 使用、管理 CPU 使用、管理 CPU 使用、SSL トット Dec バイト、SSL トット Enc バイト、SSL トット SSL 情報セッションヒット、SSL トット SSL 情報合計送信回数、システム CPU、Tcp Cur クライアントコネクト、TCP CUR クライアント接続終了、TCP CUR クライアント接続終了、TCP CUR クライアント接続テスト、TCP Cur サーバーコネン、TCP CUR サーバー接続終了、TCP CUR サーバー接続テスト、TCP エラー最初、TCP おっとクライアントオープン、TCP トットサーバーオープン、TCP トット受信バイト、TCP トット受信ピクツ、TCP トット同列、TCP トット Tx バイト、Tcp トット送信バイト、Tcp トット Tx Pkts、Ucp トット受信バイト、Udp トット送信バイト、Udp トット送信バイト
- メモリプール：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、スキーマタイプ、時間、CPU、Gslb サーバー、Gslb 仮想サーバー、インターフェイス、NetScaler、サーバーサービスグループ、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer CS、vServer Lb、vServer SSL、vServer ユーザー、メモリプール：メモリコア割り当てサイズ、メモリエラーの割り当

てに失敗しました。メモリメモリが使用可能

- 監視サービスバインド：バインドエンティティ名、エンティティ名、NetScalerId、schemaType、時間、CPU、Gslb サーバー、Gslb 仮想サーバー、インターフェイス、メモリプール、NetScaler、サーバーサービスグループ、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer CS、Vserver Lb、vServer SSL、vServer ユーザー、月サービスバインディング：レート月 Toto プローブ、月トットプローブ
- インターフェイス：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler Id、スキーマタイプ、時間、CPU、Gslb サーバー、Gslb 仮想サーバー、メモリプール、NetScaler、サーバーサービスグループ、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer Cs、Vserver Lb、vServer SSL、仮想サーバーユーザー、インターフェイス：レート NIC 合計受信バイト、RATE NIC tot 受信パケット、RATE NIC tot Tx バイト、RATE NIC tot Tx パケット、NIC tot Rx バイト、NIC ToT Rx パケット、NIC ToT Tx バイト、NIC ToT Tx パケット
- vServer CS：バインドエンティティ名、エンティティ名、月サービスバインド、NetScaler ID、スキーマタイプ、時間、CPU、Gslb サーバー、Gslb 仮想サーバー、メモリプール、NetScaler、サーバーサービスグループ、サーバー Svc Cfg、vServer Authn、vServer Cr、vServer CS、vServer Lb、vServer SSL、vServer ユーザー、vServer CS：RATE Si Totot 要求バイト、RATESi Tot リクエスト, RATE Si Tot レスポンスバイト, RATE Si Tot レスポンス, RATE Si Tott clt ttlb トランザクション, RATE Si Tott Pkt rcvd, RATE Si Tott Pkt Si Pkt 送信, RATE Si Tott ttlb イライラするトランザクション, RATE Si Tott ttlb 許容トランザクション, RATE Vsvr Tott Hits, Si Cur State, Si トット要求バイト数、SiTot リクエスト、Si Tot レスポンスバイト、Si Tot レスポンス、Si TotClt Ttlb トランザクション、Si TotPkt Rvd、Si TotPkt Sent、Si TottPit イライラするトランザクション、Si TottTlb 許容トランザクション、VSVR TotTotReq、VSVR TottReq Resp 無効ドロップされました

セキュリティで保護されたブラウザログ

- アプリケーションポスト:
  - 公開アプリケーションの前のログ: 認証、ブラウザ、ID の変更、作成済み、顧客名、宛先 URL、E-Tag、ゲートウェイサービス製品 ID、セッション ID、レガシーアイコン、アプリケーション名、ポリシー、公開アプリケーション ID、リージョン、リソースゾーン、リソースゾーン ID、サブスクリプション、セッションアイドルタイムアウト、セッションアイドルタイムアウト警告、ウォーターマーク、外部ホワイトリスト、ホワイトリスト内部、ホワイトリトリダイレクト
  - 公開アプリケーションの後のログ: 認証、ブラウザ、ID の変更、作成済み、顧客名、宛先、E-Tag、ゲートウェイサービス製品 ID、セッション ID、レガシーアイコン、アプリケーション名、ポリシー、公開アプリケーション ID、リージョン、リソースゾーン、リソースゾーン ID、サブスクリプション、セッションアイドルタイムアウト、セッションアイドルタイムアウト警告、ウォーターマーク、ホワイトリスト外部 URL、ホワイトリスト内部 URL、ホワイトリトリダイレクト URL
- アプリケーションの削除:

  - 公開アプリケーションの前のログ: 認証、ブラウザ、ID の変更、作成済み、顧客名、宛先 URL、E-Tag、ゲートウェイサービス製品 ID、セッション ID、レガシーアイコン、アプリケーション名、ポリシー、公開アプリケーション ID、リージョン、リソースゾーン、リソースゾーン ID、サブスクリプション、セッションアイドルタイムアウト、セッションアイドルタイムアウト警告、ウォーターマーク、外部ホワイトリスト、ホワイトリスト内部、ホワイトリトリダイレクト
  - 公開アプリケーションの後のログ: 認証、ブラウザ、ID の変更、作成済み、顧客名、宛先、E-Tag、ゲートウェイサービス製品 ID、セッション ID、レガシーアイコン、アプリケーション名、ポリシー、公開アプリケーション ID、リージョン、リソースゾーン、リソースゾーン ID、サブスクリプション、セッションアイドルタイムアウト、セッションアイドルタイムアウト警告、ウォーターマーク、ホワイトリスト外部 URL、ホワイトリスト内部 URL、ホワイトリトリダイレクト URL

- アプリケーションの更新:

  - 公開アプリケーションの前のログ: 認証、ブラウザ、ID の変更、作成済み、顧客名、宛先 URL、E-Tag、ゲートウェイサービス製品 ID、セッション ID、レガシーアイコン、アプリケーション名、ポリシー、公開アプリケーション ID、リージョン、リソースゾーン、リソースゾーン ID、サブスクリプション、セッションアイドルタイムアウト、セッションアイドルタイムアウト警告、ウォーターマーク、外部ホワイトリスト、ホワイトリスト内部、ホワイトリトリダイレクト
  - 公開アプリケーションの後のログ: 認証、ブラウザ、ID の変更、作成済み、顧客名、宛先、E-Tag、ゲートウェイサービス製品 ID、セッション ID、レガシーアイコン、アプリケーション名、ポリシー、公開アプリケーション ID、リージョン、リソースゾーン、リソースゾーン ID、サブスクリプション、セッションアイドルタイムアウト、セッションアイドルタイムアウト警告、ウォーターマーク、ホワイトリスト外部 URL、ホワイトリスト内部 URL、ホワイトリトリダイレクト URL

- エンタイトルメントの作成:

  - エンタイトルメント作成前のログ: 承認済み、顧客 ID、データ保持日数、終了日、猶予期間日数、セッション ID、製品 SKU、数量、シリアル番号、開始日、状態、タイプ
  - エンタイトルメント作成後のログ: 承認済み、顧客 ID、データ保持日数、終了日、猶予期間日数、セッション ID、製品 SKU、数量、シリアル番号、開始日、状態、タイプ

- エンタイトルメントの更新:

  - エンタイトルメント更新前のログ: 承認済み、顧客 ID、データ保持日数、終了日、猶予期間日数、セッション ID、製品 SKU、数量、シリアル番号、開始日、状態、タイプ
  - エンタイトルメント更新後のログ: 承認済み、顧客 ID、データ保持日数、終了日、猶予期間日数、セッション ID、製品 SKU、数量、シリアル番号、開始日、状態、タイプ

- セッションアクセスホスト： ホスト、クライアント IP、日時、ホスト、セッション、ユーザー名を受け入れる
- セッション接続:

  - セッション接続前のログ: アプリケーション ID、アプリケーション名、ブラウザ、作成済み、顧客 ID、期間、セッション ID、IP アドレス、最終更新日、起動ソース、ユーザー名
  - セッション接続後のログ: アプリケーション ID、アプリケーション名、ブラウザ、作成済み、顧客 ID、期間、セッション ID、IP アドレス、最終更新日、起動ソース、ユーザー名

- セッションの起動:
  - セッション起動前のログ: アプリケーション ID、アプリケーション名、ブラウザ、作成済み、顧客 ID、期間、セッション ID、IP アドレス、最終更新日、起動ソース、ユーザー名
  - セッション起動後のログ: アプリケーション ID、アプリケーション名、ブラウザ、作成済み、顧客 ID、期間、セッション ID、IP アドレス、最終更新日、起動ソース、ユーザー名
- セッションティック:
  - セッションティック前のログ: アプリケーション ID、アプリケーション名、ブラウザ、作成済み、顧客 ID、期間、セッション ID、IP アドレス、最終更新日、起動ソース、ユーザー名
  - セッションティック後のログ: アプリケーション ID、アプリケーション名、ブラウザ、作成済み、顧客 ID、期間、セッション ID、IP アドレス、最終更新日、起動ソース、ユーザー名

Microsoft Graph セキュリティログ

- テナント ID
- ユーザー ID
- インジケータ ID
- インジケータ UUID
- イベント時間
- 時間を作成
- アラートのカテゴリ
- ログオンの場所
- ログオン IP
- ログオンの種類
- ユーザーアカウントタイプ
- ベンダー情報
- ベンダープロバイダ情報
- 脆弱性の状態
- 脆弱性の重大度

Microsoft Active Directory ログ

- テナント ID
- 時間を集める
- 種類
- ディレクトリコンテキスト
- グループ
- ユーザー情報
- ユーザーの種類
- アカウント名
- 不正なパスワードカウント
- 市区町村
- コモンネーム
- 会社
- 国
- パスワードの有効期限までの日数
- 部署
- 説明
- 表示名
- 識別名
- メール
- ファックス番号
- 名
- グループカテゴリ
- グループスコープ
- 自宅電話
- イニシャル
- IP フォン
- アカウントは有効になっていますか
- アカウントはロックされていか

- セキュリティグループか
- 姓
- マネージャー
- のメンバー
- 携帯電話
- ポケベル
- パスワードは期限切れにならない
- 物理的な配達所名
- 私書箱
- 郵便番号
- プライマリグループ ID
- 状態
- 番地
- 役職
- ユーザーアカウント制御
- ユーザーグループリスト
- ユーザー プリンシパル名
- 勤務先の電話番号

パフォーマンス向け **Citrix Analytics** ログ

- actionid
- actionreason
- actiontype
- adminfolder
- agentversion
- allocationtype
- applicationid
- applicationname
- applicationpath

- applicationtype
- applicationversion
- associateduserfullnames
- associatedusername
- associatedusernames
- associateduserupns
- authenticationduration
- autoreconnectcount
- autoreconnecttype
- AvgendPoint スループット受信バイト数
- AvgendPoint スループットバイトが送信されました
- blobcontainer
- blobendpoint
- blobpath
- brokerapplicationchanged
- brokerapplicationcreated
- brokerapplicationdeleted
- brokeringdate
- brokeringduration
- brokerloadindex
- brokerregistrationstarted
- browsername
- catalogchangeevent
- catalogcreatedevent
- catalogdeletedevent
- catalogid
- catalogname
- catalogsync
- clientaddress

- clientname
- clientplatform
- clientsessionvalidatedate
- clientversion
- collecteddate
- connectedviahostname
- connectedviaipaddress
- connectionid
- connectioninfo
- connectionstate
- connectiontype
- controllerdnsname
- cpu
- cpuindex
- createddate
- currentloadindexid
- currentpowerstate
- currentregistrationstate
- currentsessioncount
- datetime
- deliverygroupadded
- deliverygroupchanged
- deliverygroupdeleted
- deliverygroupid
- deliverygroupmaintenancemodechanged
- deliverygroupname
- deliverygroupsync
- deliverytype
- deregistrationreason

- desktopgroupdeletedevent
- desktopgroupid
- desktopgroupname
- desktopkind
- disconnectcode
- disconnectreason
- disk
- diskindex
- dnsname
- domainname
- effectiveloadindex
- enddate
- errormessage
- establishmentdate
- eventreporteddate
- eventtime
- exitcode
- failurecategory
- failurecode
- failuredata
- failuredate
- failurereason
- failuretype
- faultstate
- functionallevel
- gpoenddate
- gpostartdate
- hdxenddate
- hdxstartdate

- host
- hostedmachineid
- hostedmachinename
- hostingservername
- hypervisorconnectionchangedevent
- hypervisorconnectioncreatedevent
- hypervisorid
- hypervisorname
- hypervisorsync
- icartt
- icarttms
- id
- idletime
- inputbandwidthavailable
- inputbandwidthused
- instancecount
- interactiveenddate
- interactivestartdate
- ipaddress
- isassigned
- isinmaintenancemode
- ismachinephysical
- ispendingupdate
- ispreparing
- isremotepc
- issecureica
- lastderegisteredcode
- launchedviahostname
- launchedviaipaddress

- lifecyclestate
- linkSpeed
- logonduration
- logonenddate
- logonscriptsenddate
- logonscriptsstartdate
- logonstartdate
- long
- machineaddedtodesktopgroupevent
- machineassignedchanged
- machinecatalogchangedevent
- machinecreatedevent
- machinedeletedevent
- machinederegistrationevent
- machinednsname
- machinefaultstatechangeevent
- machinehardregistrationevent
- machineid
- machinemaintenancemodechangeevent
- machinename
- machinepvdstatechanged
- machineregistrationendedevent
- machineremovedfromdesktopgroupevent
- machinerole
- machinesid
- machineupdatedevent
- machinewindowsconnectionsettingchanged
- memory
- memoryindex

- modifieddate
- NGSConnector.ICAConnection.Start
- ngsConnector.ngs シンセティックメトリック
- ngsConnector.ngspassive メトリック
- ngsConnector.ngs システムメトリック
- network
- networkindex
- networklatency
- networkinfoperiodic
- ネットワークインターフェースタイプ
- ostype
- outputbandwidthavailable
- 使用された出力帯域幅
- path
- percentcpu
- persistentuserchanges
- powerstate
- processname
- profileloadenddate
- profileloadstartdate
- protocol
- provisioningschemeid
- provisioningtype
- publishedname
- registrationstate
- serversessionvalidatedate
- sessioncount
- sessionend
- sessionfailure

- sessionid
- sessionidlesince
- sessionindex
- sessionkey
- sessionstart
- sessionstate
- sessionsupport
- sessiontermination
- sessiontype
- sid
- 信号強度
- siteid
- sitename
- startdate
- totalmemory
- triggerinterval
- triggerlevel
- triggerperiod
- triggervalue
- usedmemory
- userid
- userinputdelay
- username
- usersid
- vdalogonDuration
- vdaprocessdata
- vdaresourceData
- version
- vmstartenddate

- vmstartstartdate
- windowsconnectionsetting
- xd.sessionStart

システム要件

April 12, 2024

Citrix Analytics for Security の使用を開始する前に、次の要件を確認してください。

セキュリティ向け **Citrix Analytics** サブスクリプ

この Analytics 製品はサブスクリプションベースのサービスです。Security Analytics を使用するには、有効なサブスクリプションが必要です。詳細については、製品概要ページを参照してください 。

データソース要件

Citrix Analytics for Security はさまざまなデータソースからイベントを受信します。Analytics を正しく機能させるには、Analytics のデータソースとして機能する以下の製品の少なくとも 1 つを使用するには、有効なサブスクリプションが必要です。

- NetScaler ADC（オンプレミス）と NetScaler Application Delivery Managementサブスクリプション
- Citrix Endpoint Management サービス
- NetScaler Gateway (オンプレミス)
- Citrix ID プロバイダー
- Citrix Remote Browser Isolation
- Citrix Secure Private Access サービス
- Citrix Virtual Apps and Desktops または Citrix DaaS（旧 Citrix Virtual Apps and Desktops サービス）

- Microsoft Active Directory
- Microsoft Graph Security

サポートされているブラウザー

Analytics にアクセスするには、ワークステーションに次のサポートされている Web ブラウザがインストールされている必要があります。

- 最新バージョンの Google Chrome
- 最新バージョンの Mozilla Firefox
- 最新バージョンの Microsoft Edge
- 最新バージョンの Apple Safari

セキュリティ分析の管理者ロールを管理する

December 7, 2023

フルアクセス権限を持つ Citrix Cloud 管理者は、他の管理者を招待して Security Analytics オファリングを管理し、次のカスタムロールのいずれかを割り当てることができます。

- セキュリティ分析-すべての管理者
- セキュリティ分析-読み取り専用管理者

新しい管理者を 2 つの方法で追加できます。1 つはユーザーとして個別に追加する方法と、Azure Active Directory グループを使用する方法です。新しい管理者の追加の詳細については、「管理者ロールの管理」を参照してください。

> 注:
> ユーザーにユーザーとして直接、または Azure Active Directory グループを通じてアクセス権を付与した場合、そのユーザーに個別に付与されたアクセスが有効になります。

カスタムロールの権限

Security Analytics-すべての管理者の役割を持つ管理者は、Security Analytics オファリングのすべての機能にアクセスできます。組織の要件に従って、フィーチャを使用および変更できます。たとえば、完全な管理者は、カスタムリスク指標の作成、ジオフェンスの有効化、ポリシーの作成を行うことができます。

Security Analytics-Read Only Administrator ロールを持つ管理者は、セキュリティダッシュボード (ユーザー、ユーザーアクセス、アプリケーションアクセス、アクセス保証、レポート) にのみアクセスして表示できます。ユーザーの行動を監視し、これらのダッシュボードでユーザーイベントを表示できます。ただし、次のような重要なタスクを実行することはできません。

- データソースのデータ処理をオンまたはオフにする

- ポリシーとアクションを作成または削除する
- ユーザーリスクタイムラインに表示されるリスク指標に手動でアクションを適用する
- カスタムリスク指標を作成、変更、または削除する
- カスタムレポートの作成
- 別の管理者ユーザーの追加、変更、削除
- アクセス保証ロケーションのジオフェンスの追加または変更

管理者へのセキュリティ警告通知

フルアクセス権限を持つ Citrix Cloud 管理者と同様に、カスタムの役割（フルアクセスおよび読み取り専用アクセス）を持つ管理者は、Security Analytics から電子メール通知を受信します。

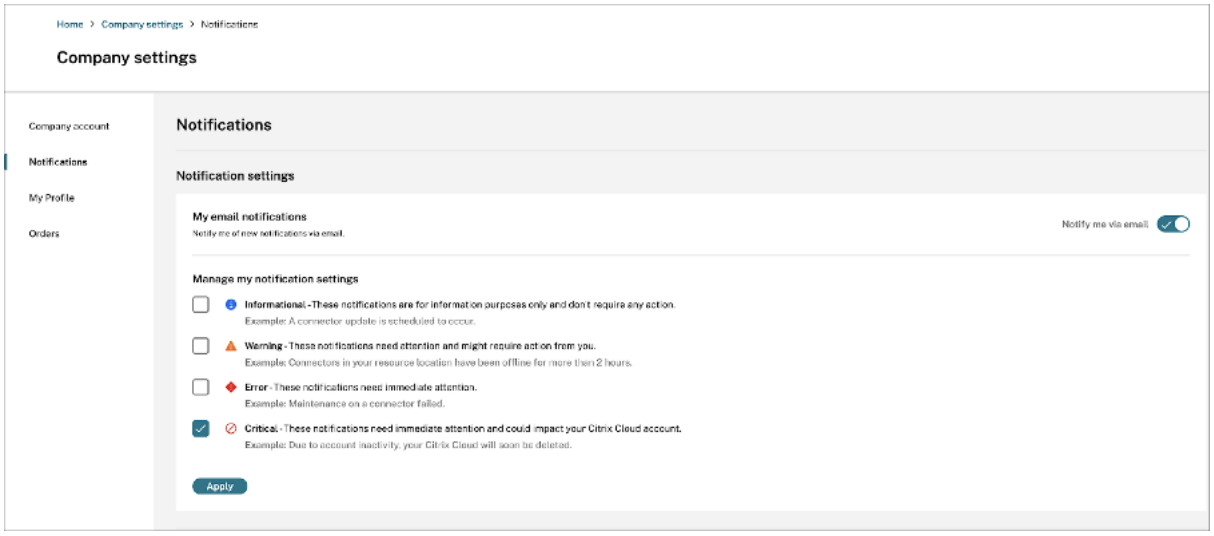
管理者は次の 2 種類の電子メール通知を受け取ります：

- 組織内の Security Insight に関する毎週の通知。詳細については、「毎週の電子メール通知」を参照してください。
- 管理者への通知アクションに基づく通知。詳細については、「ポリシーとアクション」を参照してください。

フルアクセス権限またはカスタムアクセス権を持つ Citrix Cloud 管理者の場合、メール通知は Citrix Cloud アカウントでデフォルトで無効になっています。Citrix Analytics などの Citrix Cloud サービスから電子メール通知を受信するには、Citrix Cloud で通知オプションを有効にします。詳細については、「受信した電子メール通知」を参照してください。Active Directory/Azure AD グループを通じて追加された管理者は、通知設定を使用できません。

通知設定は、毎週の電子メール、管理者への通知アクション電子メール、データエクスポートのアラートなどの通知を送信する際に利用されます。メール通知では、メールの受信を停止したい場合は、Security Analytics へのフルアクセス権を持つ管理者があなたを配布リストから削除する必要があります。配布リストの詳細については、「電子メール配布リスト」を参照してください。

> 注：
>
> Citrix Cloud 管理者（フルアクセス権限またはカスタムアクセス権）は、通知設定を利用する他の **Citrix Cloud** サービスからの通知を受信しません。



詳しくは、「Citrix Analytics の管理者の管理」を参照してください。

はじめに

December 7, 2023

このドキュメントでは、Citrix Analytics for Security を初めて使用する方法について説明します。

ステップ **1**：**Citrix Cloud** にサインインする

Citrix Analytics for Security を使用するには、Citrix Cloud アカウントが必要です。https://citrix.cloud.com にアクセスし、既存の Citrix Cloud アカウントでサインインします。

Citrix Cloud アカウントをお持ちでない場合は、最初に Citrix Cloud アカウントを作成するか、組織内の他のユーザーが作成した既存のアカウントに参加する必要があります。詳細なプロセスと手順については、「Citrix Cloud へのサインアップ」を参照してください。

ステップ **2:** セキュリティ分析にアクセスする

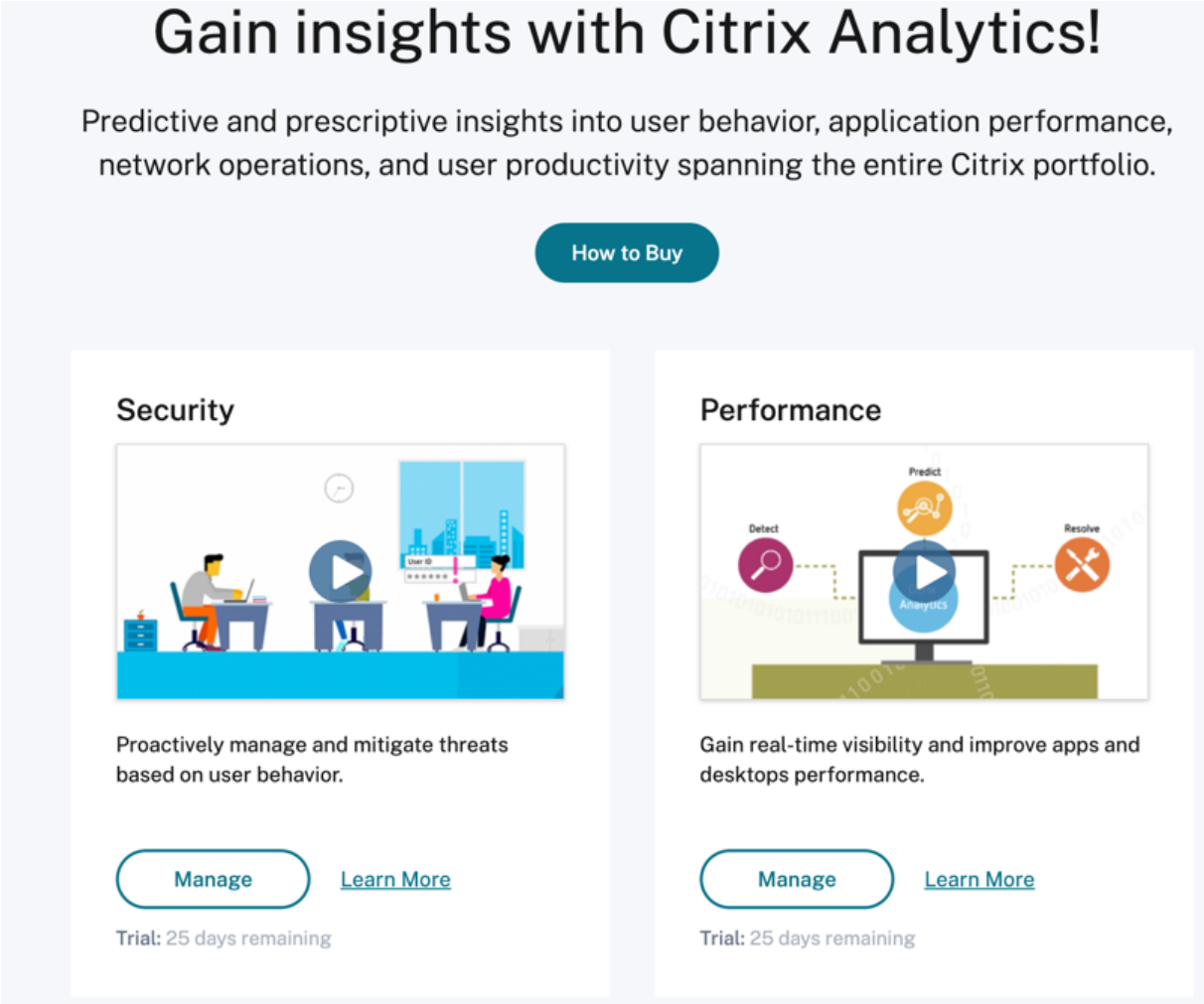
Citrix Analytics for Security には、次のいずれかの方法でアクセスできます。

- セキュリティ向け **Citrix Analytics** トライアルをリクエストします。Citrix Cloud にサインインしたら、次の操作を行います。
  1. [利用可能なサービス] セクションで、[アナリティクス] タイルの [管理] をクリックします。Analytics の概要ページにリダイレクトされます。
  2. セキュリティタイルで、「トライアルをリクエスト」をクリックするか、シトリックスアカウントまたは Citrix Partner に直接連絡してください。
- セキュリティ向け **Citrix Analytics** に登録します。Citrix Analytics for Security サブスクリプションを購入するには、https://www.citrix.com/en-in/products/citrix-analytics/form/inquiry/ にアクセスして、サポート Citrix Analytics エキスパートにお問い合わせください。

> 注
>
> - 2023 年 3 月 8 日以降、セキュリティ向けシトリックスアナリティクスは ShareFile/Citrix Content Collaboration のスタンドアロン製品として購入できなくなります。ShareFile/Citrix Content Collaboration 向けの Citrix Analytics Service スタンドアロンアドオンの販売終了（EOS）および更新終了（EOR）をお知らせします。お客様の Citrix Analytics for Security の既存の資格は、サブスクリプションの有効期限が切れるまで有効です。ただし、Sharefile/Citrix Content Collaboration の統合では、試用版、更新、および新規購入はサポートされません。他のシトリックス製品との Citrix Analytics Service 統合は、既存の Citrix DaaS プラン、Citrix Virtual Apps and Desktops デプロイメント、および Citrix Workspace デプロイメントとのスタンドアロンまたはバンドルオファリングとして引き続き提供されます。
> - 2020 年 2 月 3 日から Citrix Analytics for Security は、ワークスペースプレミアムおよびワークスペースプレミアムプラスのサブスクリプションには含まれなくなりました。2020 年 2 月 3 日より前に Workspace プレミアムまたは Workspace プレミアムプラスのサブスクリプションを購入したお客様は、サブスクリプションの有効期限が切れるまで、Workspace サブスクリプションの一部として Citrix Analytics for Security にアクセスできます。Citrix Analytics for Security は、Citrix Workspace パッケージ（ワークスペーススタンダード、ワークスペースプレミアム、ワークスペースプレミアムプラス）でアドオンサービスとして提供されるようになりました。詳しくは、「Citrix Cloud サービス」を参照してください。

ステップ **3:** セキュリティ分析を管理する

必要なサブスクリプションを取得するか、トライアルにアクセスする権限が付与されると、Analytics の概要ページで、セキュリティ製品の [トライアルをリクエスト] ボタンが [管理] に変わります。[**Manage**] をクリックして、ユーザダッシュボードを表示します。



Analytics では、Citrix [データソースと外部データソースの両方がサポートされます](/ja-jp/security-analytics/data-sources.html#external-data-sources)。Citrix Cloud アカウントに関連付けられている Citrix データソースを自動的に検出します。外部データソースからデータを受け取るには、外部データソースを Analytics と統合する必要があります。検出されたデータソースを表示するには、[設定] **>** [データソース] **>** [セキュリティ] をクリックします。

次の操作

- Citrix Analytics for Security の資格が承認されると、次のクラウドサービスのデータ処理が有効になります:
  - Citrix データソース
    - Citrix Secure Private Access
    - Citrix Virtual Apps and Desktops および Citrix DaaS
- データ処理のステータスを確認する、または手動でオンにする方法を知るには、次の記事を参照してください。

  - Citrix データソース:
    * Citrix Endpoint Management
    * Citrix Gateway
  - 外部データソース:
    * Microsoft Graph Security
    * Microsoft Active Directory

- 処理済みデータを Analytics から次の製品にエクスポートします。
  - Splunk
  - Microsoft Azure Sentinel
  - Elasticsearch
  - Kafka または Logstash ベースのデータコネクタを使用する他の SIEM

- [ユーザー] ダッシュボードを使用して 、検出されたユーザーとそのセキュリティリスクプロファイルを表示します。ユーザーダッシュボードは、ユーザーの行動分析と脅威防止の出発点です。

  > 注
  >
  > Analytics を初めて使用する場合、ユーザーリスクプロファイルがダッシュボードに表示されるまでに時間がかかります。Analytics では、機械学習を使用してユーザーイベントにおける危険なパターンや異常を特定し、リスクの重大度に基づいて、ユーザープロファイルを高リスク、中リスク、低リスクとして識別します。

- セルフサービス検索機能を使用して 、データソースから受信したユーザーイベント (生データ) を表示してフィルタリングします。

Citrix Endpoint Management データソース

December 6, 2021

Endpoint Management データソースは、Citrix Cloud アカウントに関連付けられている Citrix Endpoint Management サービスを表します。ユーザーがこのサービスを使用すると、Citrix Analytics はユーザーのエンドポイントとそのアクティビティに関連するユーザーイベントをリアルタイムで受信します 。ユーザーイベントは、セキュリティ上の脅威を検出するために処理されます。

前提条件

- Citrix Cloud で提供される Citrix Endpoint Management を購読します。Endpoint Management サービスのセットアップ方法については、「オンボーディングとリソースのセットアップ」を参照してください。
- クラウドサイトとエンタープライズディレクトリのセットアップ。Cloud Connector をインストールするために、Windows 2012 R2 または Windows 2016 サーバーを実行しているコンピューターが 2 台あることを確認します。
- **Cloud Connector** がインストールされました。Active Directory の一部である仮想マシンに Cloud Connector をダウンロードしてインストールします。
- システム要件を確認し 、ご使用の環境が要件を満たしていることを確認します。

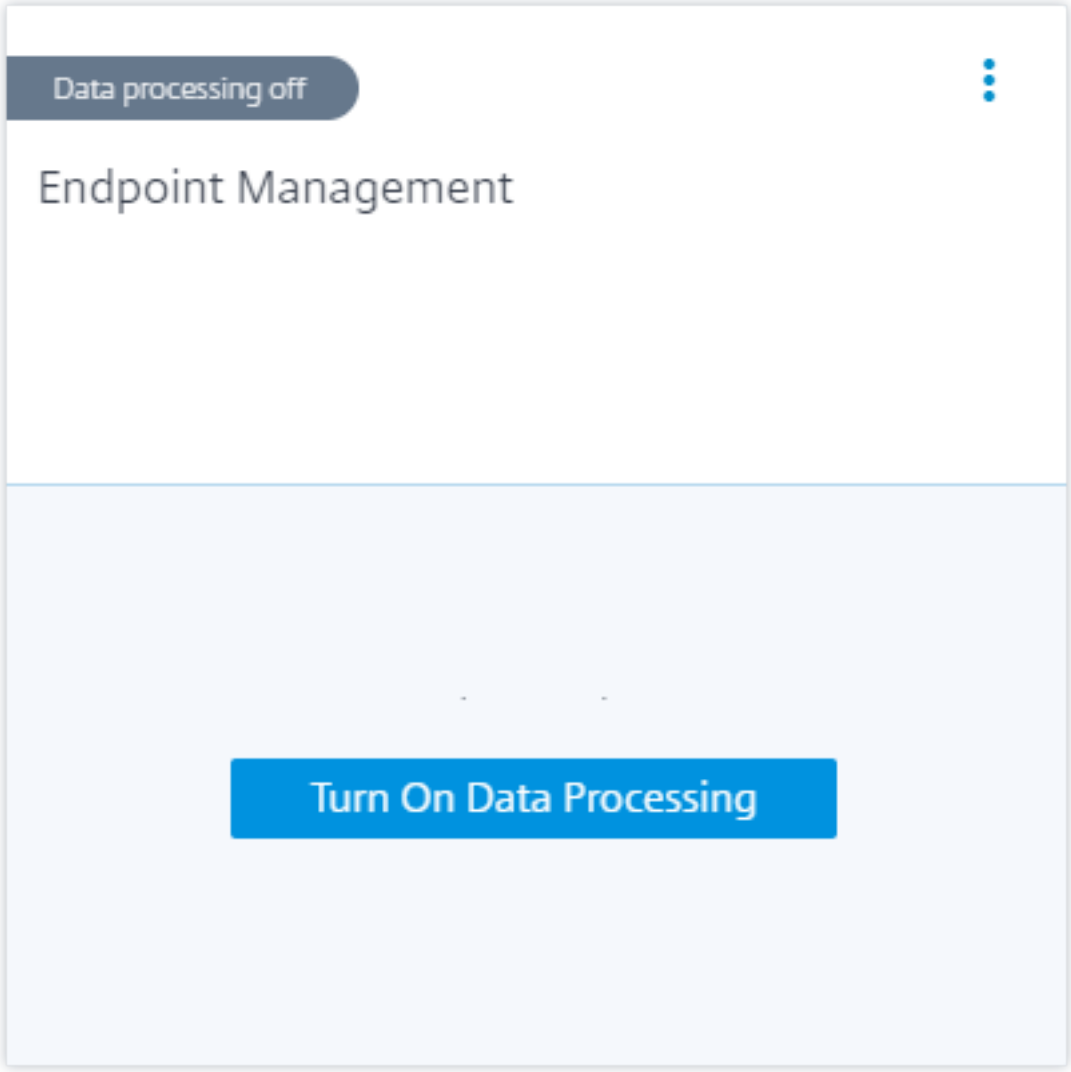
データソースを表示してデータ処理を有効にする

Citrix Analytics は、Citrix Cloud アカウントに関連付けられているすべての Endpoint Management データソースを自動的に検出します。

データソースを表示するには、次の手順を実行します。

トップバーで、[設定] > [データソース] > [セキュリティ] をクリックします。

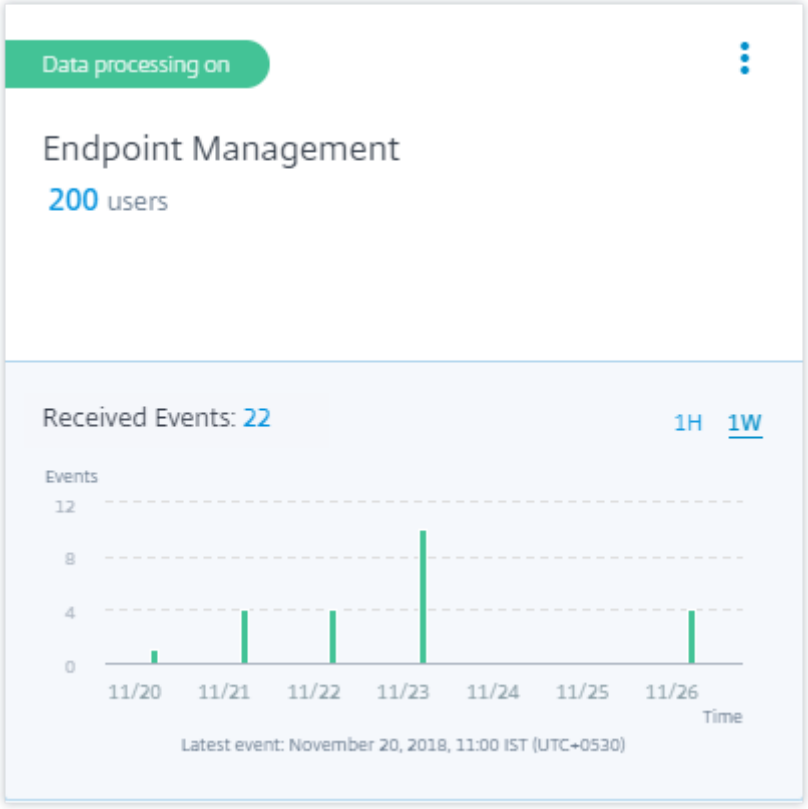
Endpoint Management データソースのサイトカードが［データソース］ページに表示されます。Citrix Analytics がこのデータソースのデータの処理を開始できるようにするには、［データ処理を有効にする］をクリックします。



ユーザーと受信したイベントの表示

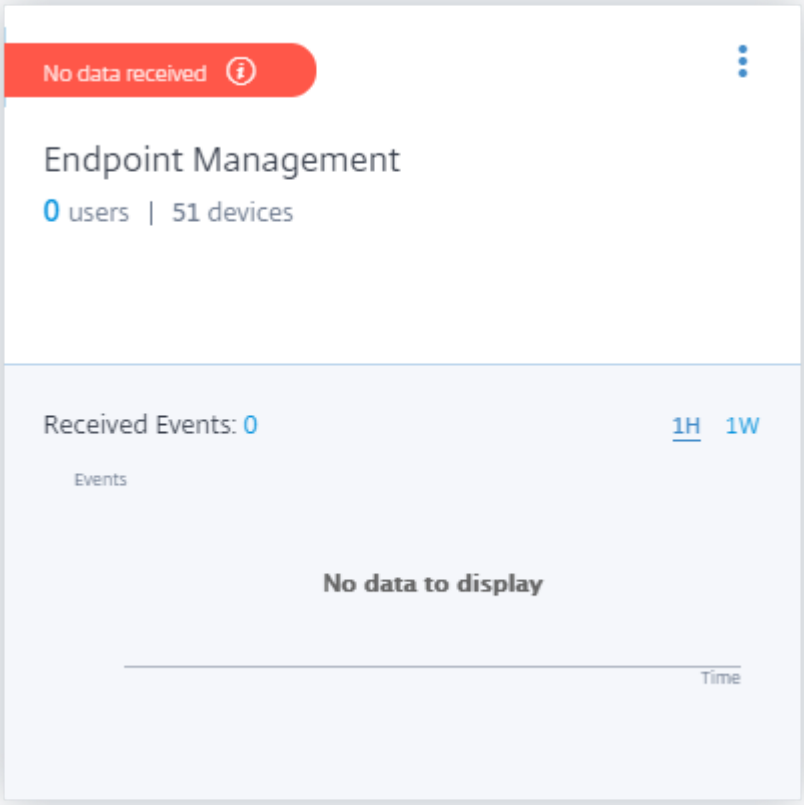
サイトカードには、Endpoint Management のユーザー、デバイス、および過去 1 時間に受信したイベントの数が表示されます。これはデフォルトの時間選択です。また、1 週 (**1W**) を選択してデータを表示することもできます。

ユーザー数をクリックすると、**[Users]** ページにユーザーの詳細が表示されます。



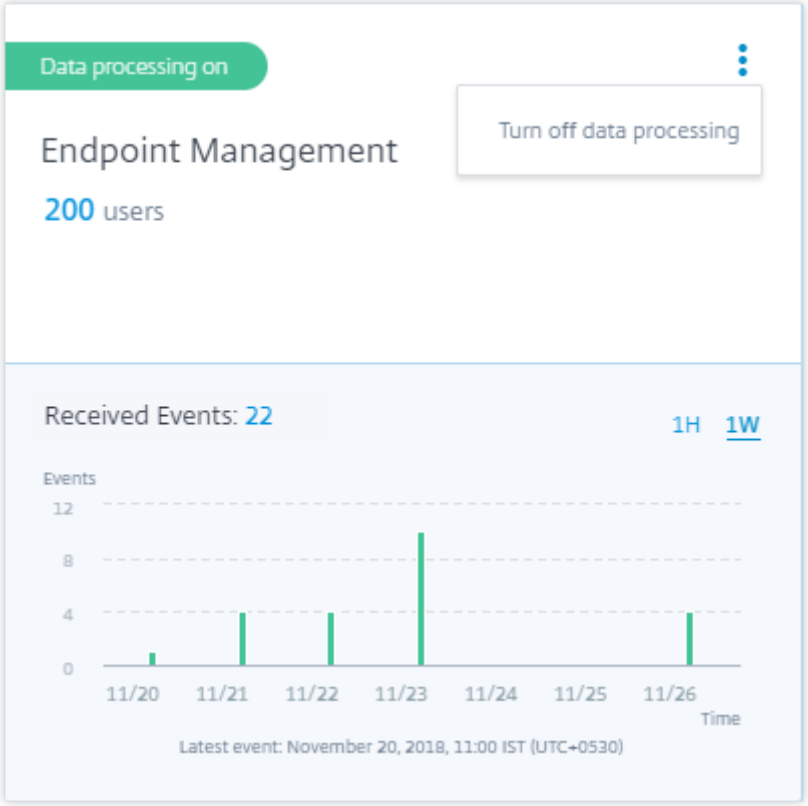
データ処理を有効にすると、サイトカードに [データを受信していません] ステータスが表示される場合があります。このステータスは、次の 2 つの理由で表示されます。

1. データ処理を初めて有効にした場合は、イベントが Citrix Analytics のイベントハブに到達するまでに時間がかかります。Citrix Analytics がイベントを受信すると、ステータスは［データ処理オン］に変わります。しばらくしてもステータスが変わらない場合は、[データソース] ページを更新します。
2. アナリティクスは、過去 1 時間の間にデータソースからイベントを受信していません。

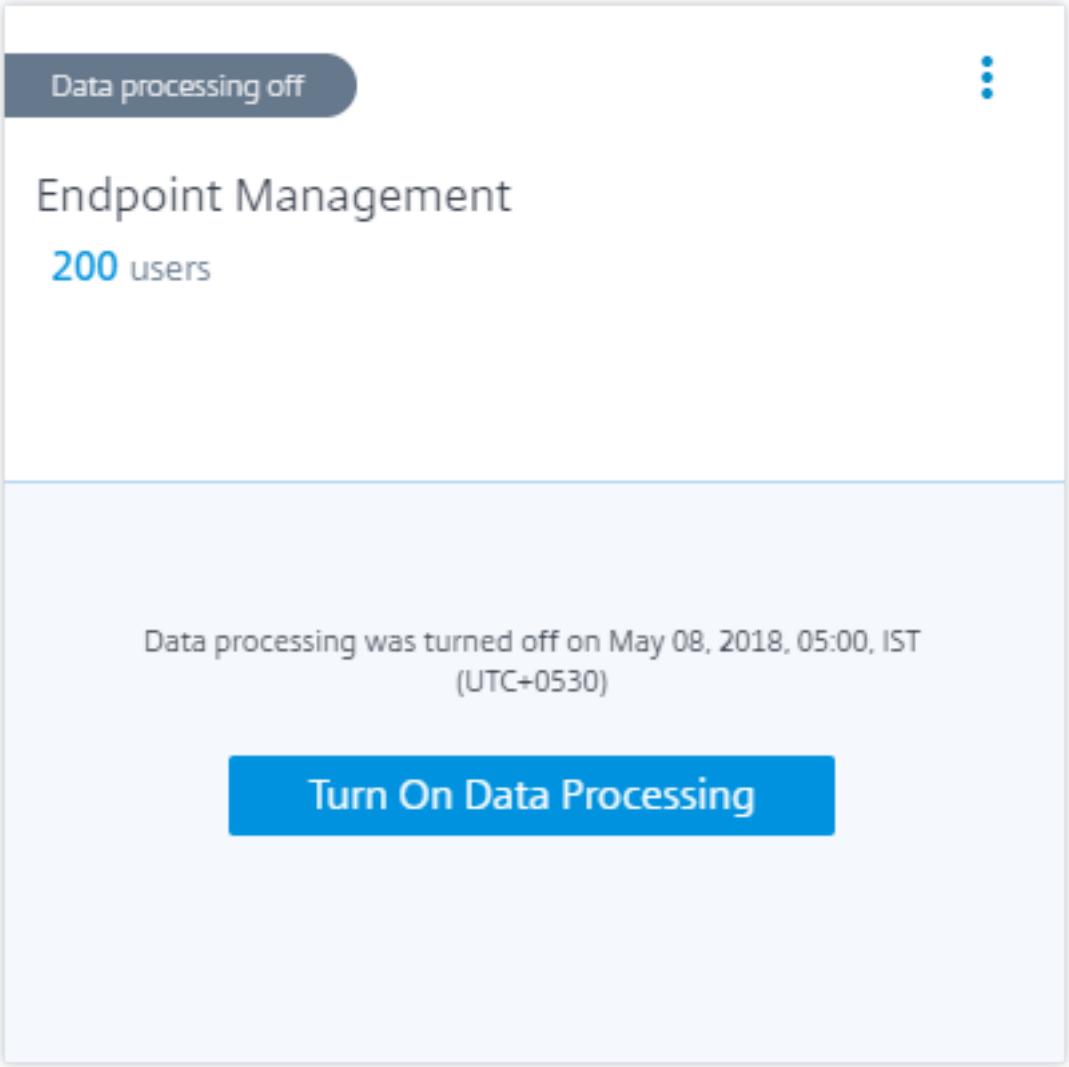


データ処理のオンとオフを切り替える

データ処理を停止するには、サイトカードの縦の省略記号 (⊠) をクリックし、[データ処理をオフにする] をクリックします。Citrix Analytics は、このデータソースに対するデータの処理を停止します。



データ処理を再度有効にするには、[データ処理をオンにする] をクリックします。



Citrix Gateway（オンプレミス）データソース

April 12, 2024

Gateway データソースは、環境内のオンプレミスの Citrix Gateway インスタンスを表します。Citrix Analytics は、Citrix ADM サービスに追加された Citrix Application Delivery Management（ADM）エージェントと Gateway インスタンスを自動的に検出します。

ユーザーが Gateway 経由でサービスまたはアプリケーションにアクセスすると、Citrix Analytics はユーザーアクセスイベントをリアルタイムで受信します 。ユーザーイベントは、セキュリティ上の脅威を検出するために処理されます。

前提条件とオンボーディング手順については、Citrix Analytics プラットフォームのドキュメントの「Citrix

Gateway データソース」の記事を参照してください。

Citrix Remote Browser Isolation データソース

March 27, 2023

シトリックスの Remote Browser Isolation サービスは 、Web ブラウジングを隔離して、ブラウザベースの攻撃から企業ネットワークを保護します。ユーザーデバイスを構成する必要なく、インターネットでホストされた Web アプリケーションに一貫してセキュアにリモートアクセスすることができます。

Citrix Analytics for Security では、公開されている Remote Browser Isolation セッションのユーザーイベントを表示できます。ユーザーイベントの詳細については、「Remote Browser Isolation のセルフサービス検索」を参照してください。

公開されている Remote Browser Isolation セッションからユーザーイベントを受信するには、**Remote Browser Isolation** でホスト名追跡ポリシーを有効にします。デフォルトでは、このポリシーは無効になっています。

ホスト名追跡ポリシーを有効にすると、Remote Browser Isolation により、ユーザーセッション中に使用されたホスト名が Citrix Analytics for Security に送信されます。
詳細については、「公開されている Remote Browser Isolation の管理」を参照してください。

Citrix Secure Private Access データソース

April 12, 2024

セキュアプライベートアクセスデータソースは、Citrix Cloud Citrix Secure Private Access アカウントに関連付けられているサービスを表します。ユーザーがこのサービスを使用すると、Citrix Analytics はユーザーアクセスイベント （ログ）をリアルタイムで受信します。ユーザーイベントは、セキュリティ上の脅威を検出するために処理されます。

前提条件

- Citrix Cloud Citrix Secure Private Access で提供されるサービスに登録します。開始方法については、「セキュアプライベートアクセスサービス」を参照してください。
- システム要件を確認し 、ご使用の環境が要件を満たしていることを確認します。

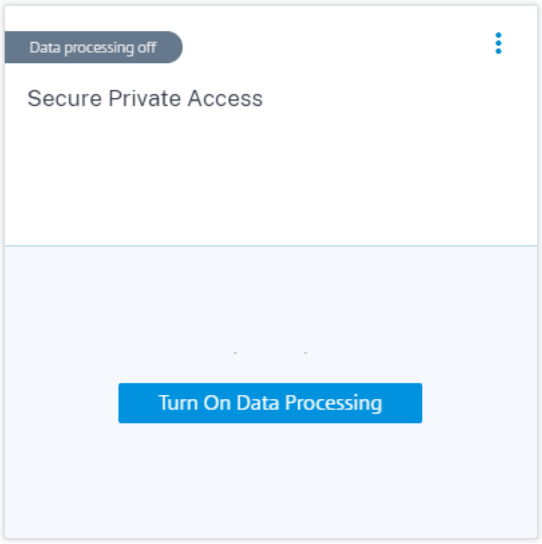
データソースを表示してデータ処理を有効にする

Citrix Analytics は、Citrix Cloud アカウントに関連付けられているセキュアプライベートアクセスデータソースを自動的に検出します。

データソースを表示するには、次の操作を行います。

トップバーで、[設定] > [データソース] > [セキュリティ] をクリックします。

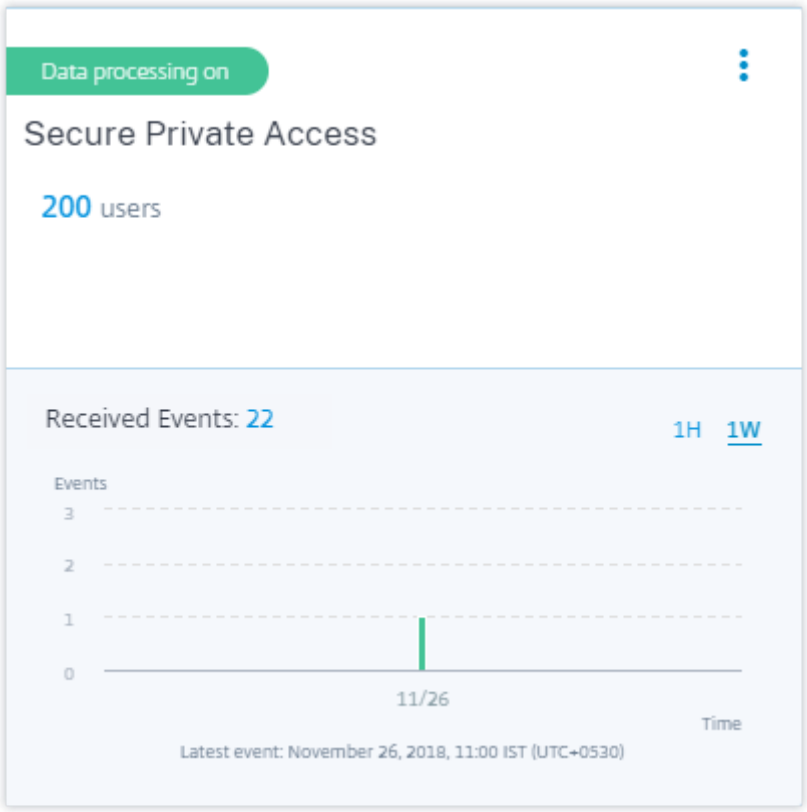
Secure Private Access データソースのサイトカードが [データソース] ページに表示されます。Citrix Analytics がこのデータソースのデータの処理を開始できるようにするには、［データ処理を有効にする］をクリックします。



ユーザーと受信したイベントの表示

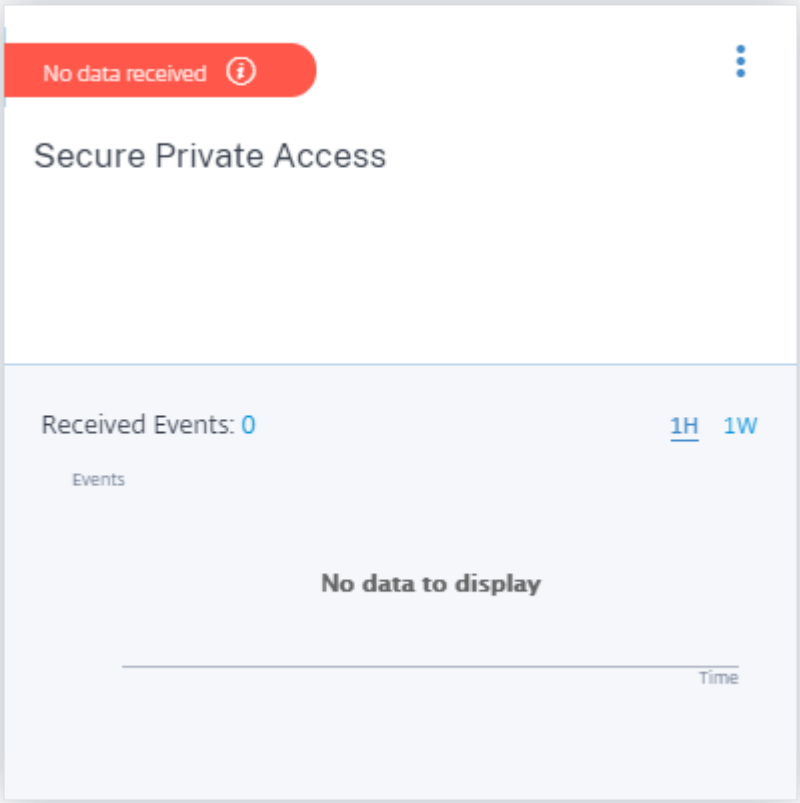
サイトカードには、アクティブなユーザーの数と、過去 1 時間にデータソースから受信したイベントが表示されます。これは既定の時間選択です。また、1 週間 (1 W) を選択してデータを表示することもできます。

ユーザー数をクリックすると、**[Users]** ページにユーザーの詳細が表示されます。受信したイベントの数をクリックすると、セルフサービス検索ページにイベントの詳細が表示されます 。



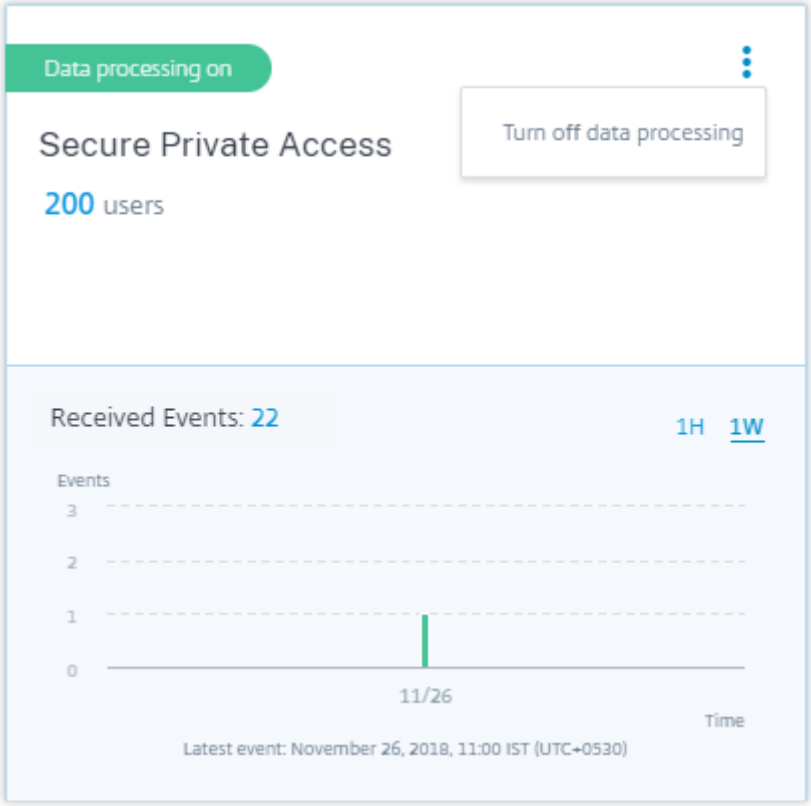
データ処理を有効にすると、サイトカードに [データを受信していません] ステータスが表示される場合があります。このステータスは、次の 2 つの理由で表示されます:

1. 初めてデータ処理をオンにした場合、イベントが Citrix Analytics のイベントハブに到達するまでに時間がかかります。Citrix Analytics がイベントを受信すると、ステータスが **Data processing on** に変わります。しばらくしてもステータスが変わらない場合は、[データソース] ページを更新します。
2. アナリティクスは、過去 1 時間の間にデータソースからイベントを受信していません。

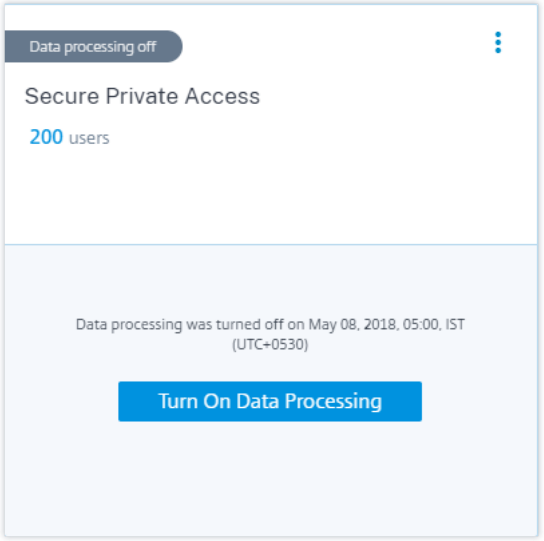


データ処理のオンとオフを切り替える

データ処理を停止するには、サイトカードの縦の省略記号 (⊠) をクリックし、[データ処理をオフにする] をクリックします。Citrix Analytics は、このデータソースに対するデータの処理を停止します。



データ処理を再度有効にするには、[データ処理をオンにする] をクリックします。



Citrix Virtual Apps and Desktops および Citrix DaaS データソース

April 12, 2024

アプリとデスクトップのデータソースは、組織内のオンプレミスの Citrix Virtual Apps and Desktops Citrix DaaS（旧 Citrix Virtual Apps and Desktops サービス）を表します。

Citrix Analytics for Security は、オファリングとデータソースからのユーザーイベントの受信の両方をサポートしています。この記事では、両方のサービスで Analytics を有効にするための前提条件と手順について説明します。

Citrix Analytics for Security は、Citrix Virtual Apps and Desktops の次のコンポーネントと Citrix DaaS データソースからユーザーイベントを受信します。

- ユーザーデバイスにインストールされた Citrix Workspace アプリ
- オンプレミス展開向け Citrix Director
- Citrix モニターサービス
- Session Recording サーバー

ユーザーが仮想アプリまたは仮想デスクトップを使用すると、Citrix Analytics for Security でユーザーイベントがリアルタイムで受信されます。

サポートされているクライアントバージョン

Citrix Analytics は、サポートされているクライアントバージョンがユーザーエンドポイントで使用されている場合にユーザーイベントを受信します。サポートされていないクライアントバージョンを使用している場合は、クライアントを次のバージョンのいずれかにアップグレードする必要があります。

- Windows 1907 以降向けの Citrix Workspace アプリ
- Mac 用 Citrix Workspace アプリ 1910.2 以降の場合
- HTML5 2007 またはそれ以降の Citrix Workspace アプリ
- Chrome 向け Citrix Workspace アプリ-Chrome Web Store で最新バージョンが利用可能
- Android 向け Citrix Workspace アプリ-Google Play で利用可能な最新バージョン
- iOS 向け Citrix Workspace アプリ-Apple App Store で最新バージョンが利用可能
- Linux 2006 以降向け Citrix Workspace アプリ

Citrix DaaS で分析を有効にする

前提条件

- Citrix Cloud で提供される Citrix DaaS を購読してください。Citrix DaaS を使い始める方法については、「インストールと構成」を参照してください。
- 「システム要件 」セクションを確認し、要件を満たしていることを確認します。

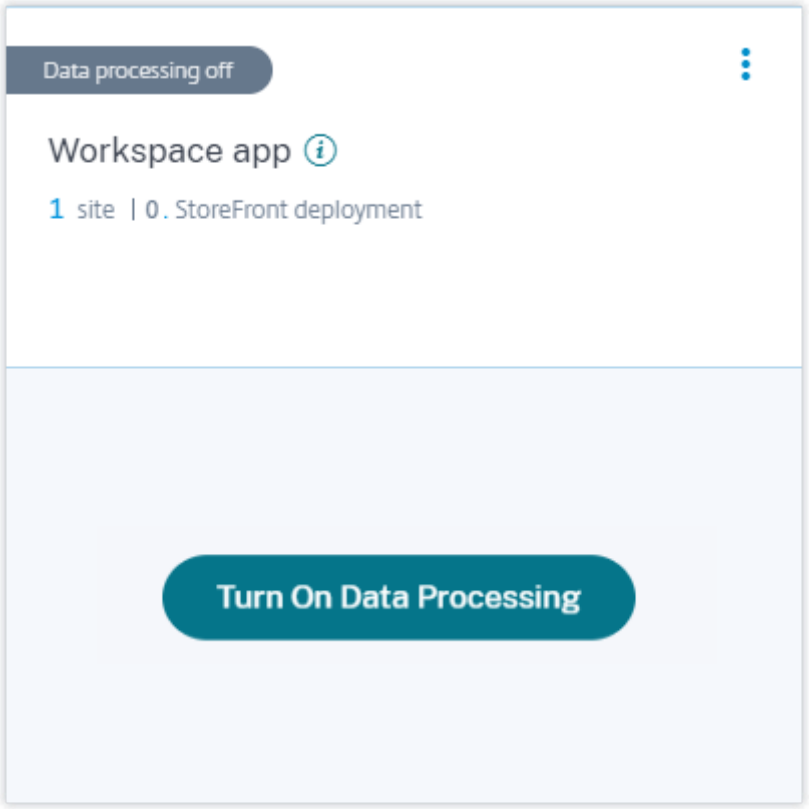
データソースを表示し、データ処理をオンにする

Citrix Analytics は、Citrix Cloud アカウントに関連付けられている Citrix DaaS を自動的に検出します。

データソースを表示するには:

トップバーで、[設定] > [データソース] > [セキュリティ] をクリックします。

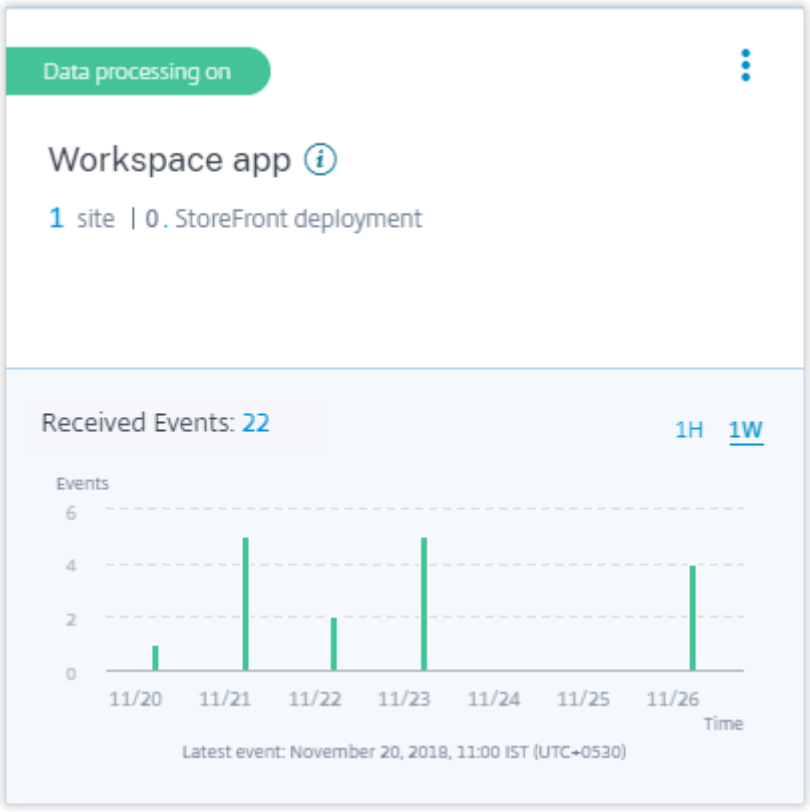
[アプリとデスクトップ**-Workspace** アプリ] サイトカードが [データソース] ページに表示されます。Citrix Analytics がこのデータソースのデータの処理を開始できるようにするには、[データ処理を有効にする] をクリックします。



クラウドサイト、ユーザー、受信したイベントの表示

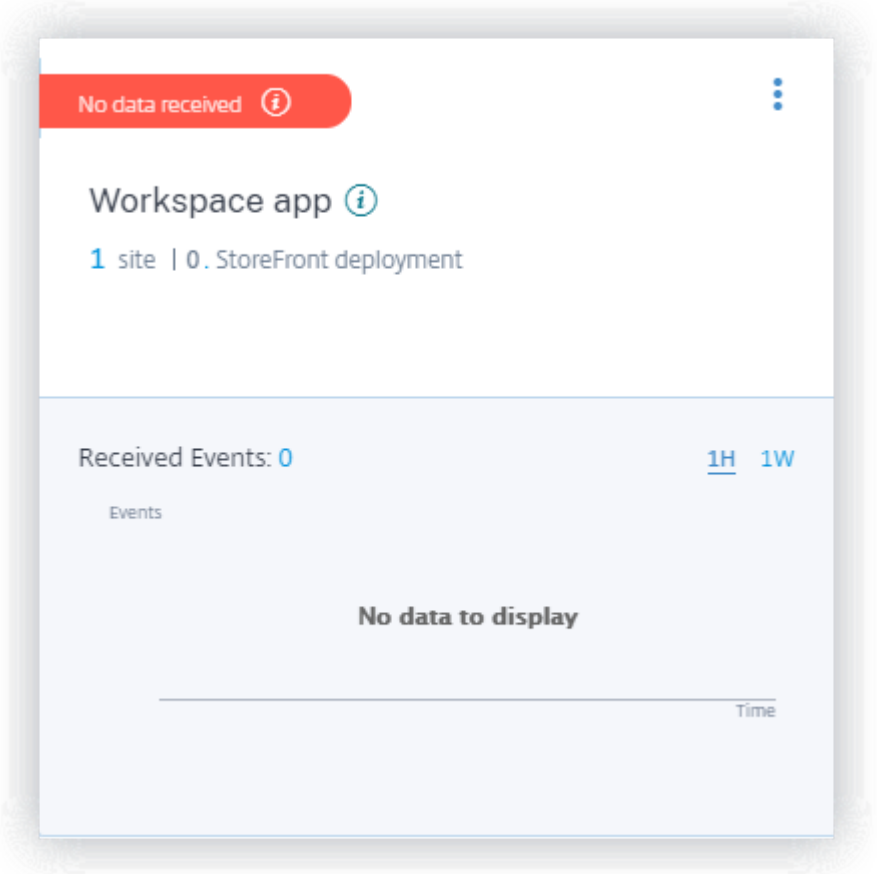
サイトカードには、アプリとデスクトップのユーザー数、検出されたクラウドサイト、過去 1 時間に受信したイベントが表示されます。これはデフォルトの時間選択です。1 週間（1 W）を選択して、データを表示することもできます。

受信したイベントの数をクリックすると、セルフサービス検索ページにイベントが表示されます 。



データ処理を有効にすると、サイトカードに [データを受信していません] ステータスが表示される場合があります。このステータスは、次の 2 つの理由で表示されます:

1. 初めてデータ処理をオンにした場合、イベントが Citrix Analytics のイベントハブに到達するまでに時間がかかります。Citrix Analytics がイベントを受信すると、ステータスが **Data processing on** に変わります。しばらくしてもステータスが変わらない場合は、[データソース] ページを更新します。
2. アナリティクスは、過去 1 時間の間にデータソースからイベントを受信していません。



オンプレミスの **Citrix Virtual Apps and Desktops** で **Analytics** を有効にする

Citrix Analytics は、Workspace に追加されたオンプレミスサイトおよび StoreFront 展開環境からアクセスされるサイトからユーザーイベントを受信します

組織でオンプレミスサイトを使用している場合、Analytics がサイトを検出できるように、次のいずれかの方法を使用してサイトをオンボーディングする必要があります:

- StoreFront を使用したオンプレミスサイトのオンボーディング
- Workspace を使用してオンプレミスサイトをオンボーディングする

前提条件

- Citrix Virtual Apps and Desktops のオンプレミスソリューションを使用するには、ライセンスが必要です。Citrix Virtual Apps and Desktops をオンプレミスで使い始める方法については、「インストールと構成」を参照してください。
- 「システム要件 」セクションを確認し、要件を満たしていることを確認します。

- Director のバージョンは 1912 CU2 以降です。詳しくは、「機能の互換性マトリックス」を参照してください。
- **Citrix Workspace** へのサブスクリプション。Citrix Workspace にサイトを追加する場合は、Workspace サブスクリプションが必要です。

  Citrix Workspace サブスクリプションを購入するには、https://www.citrix.com/products/citrix-workspace/get-started.html にアクセスし、Citrix Workspace のエキスパートにお問い合わせください。
- ワークスペースに追加されたサイト。Citrix Analytics は、Citrix Workspace に追加されたサイトを自動的に検出します。Citrix Analytics のオンボーディングに進む前に、Citrix Workspace にサイトを追加してください。このプロセスは、サイトアグリゲーションと呼ばれます。

  サイトアグリゲーションでは、Cloud Connector をインストールし、Workspace リソースへの内部および外部接続用に NetScaler Gateway STA サーバーを構成してから、サイトを Workspace に追加する必要があります。サイトアグリゲーションの詳細な手順については、「ワークスペースでのオンプレミスの仮想アプリケーションとデスクトップの集約」を参照してください。
- **StoreFront** バージョン。サイトで StoreFront 展開環境を使用している場合は、StoreFront のバージョンが 1906 以降であることを確認します。

StoreFront を使用した **Citrix Virtual Apps and Desktops** のオンプレミスサイトのオンボーディング

前提条件とオンボーディング手順については、Citrix Analytics プラットフォームのドキュメントの「Citrix Virtual Apps and Desktops」データソースの記事を参照してください 。

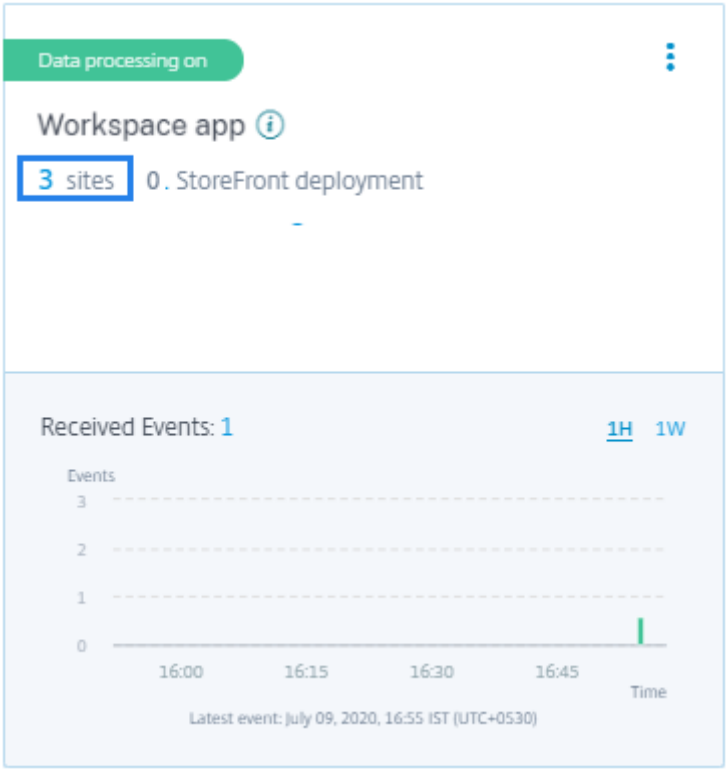
Workspace を使用した **Citrix Virtual Apps and Desktops** のオンプレミスサイトのオンボーディング

Citrix Workspace にすでに追加されているサイト　Citrix Analytics は、Citrix Workspace に既に追加されているオンプレミスサイトを自動的に検出し、データソースサイトカードに表示します。

データソースを表示するには**:**

トップバーで、[設定] > [データソース] > [セキュリティ] をクリックします。

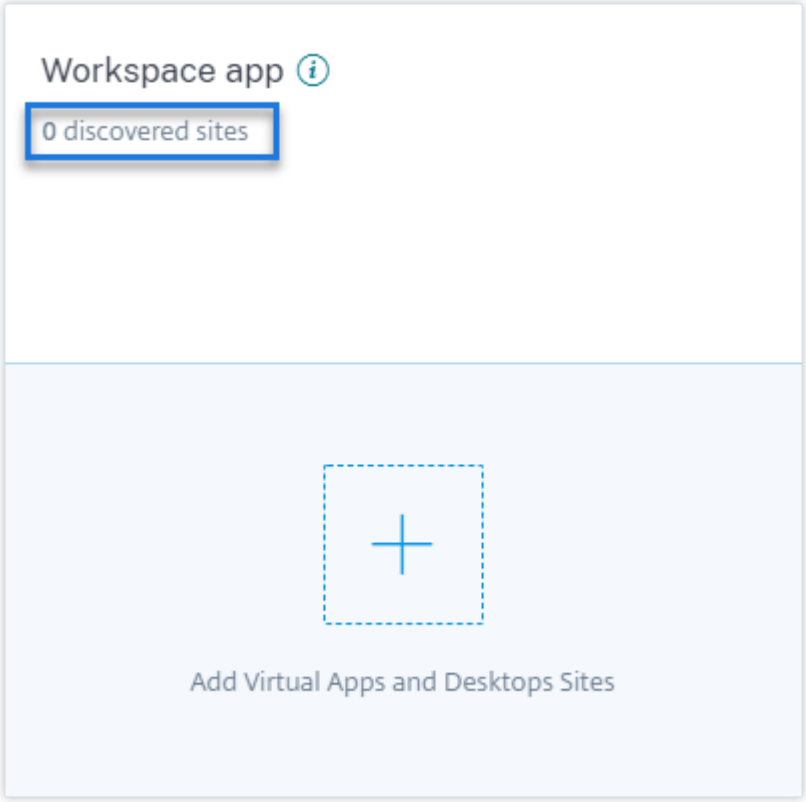
[アプリとデスクトップ] サイトカードには、Workspace に追加されたサイトの数と、これらのサイトに接続しているユーザーが表示されます。サイト数をクリックすると、検出されたサイトが表示されます。ユーザ数をクリックすると、検出されたユーザが **[**ユーザ（**Users**）**]** ページに表示されます。



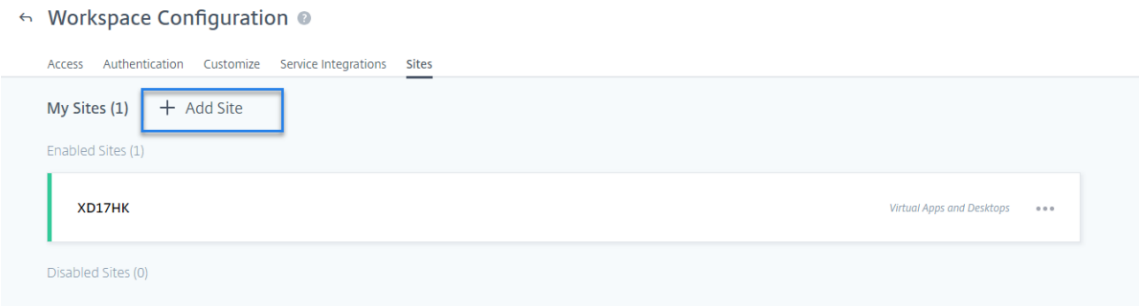
Citrix Workspace に追加されていないサイト　オンプレミスサイトを Workspace にまだ追加していない場合、Analytics はサイトを検出できません。サイトカードには、検出されたサイトが **0** 件表示されます。

Workspace にサイトを追加するには**:**

1. サイトカードの [+] をクリックします。



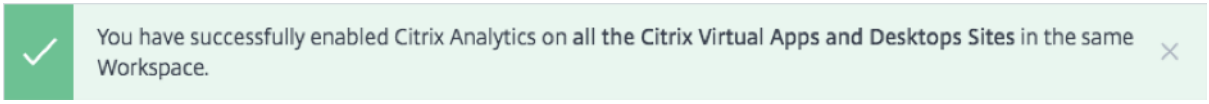
2. 「ワークスペース構成」ページで、「**+** サイトを追加」をクリックします。



3. 画面の指示に従って、サイトを追加します。詳細については、「ワークスペースでのオンプレミスの仮想アプリケーションおよびデスクトップの集約」を参照してください。
4. サイトを追加したら、Citrix Analytics に再度ログインし、[データソース] ページを更新して、サイトカードに最近追加したサイトを表示します。

データ処理をオンにして、受信したイベントを表示する　検出されたサイトのデータ処理を Analytics が開始できるようにするには、サイトカードの [データ処理を有効にする] をクリックし、画面の指示に従います。

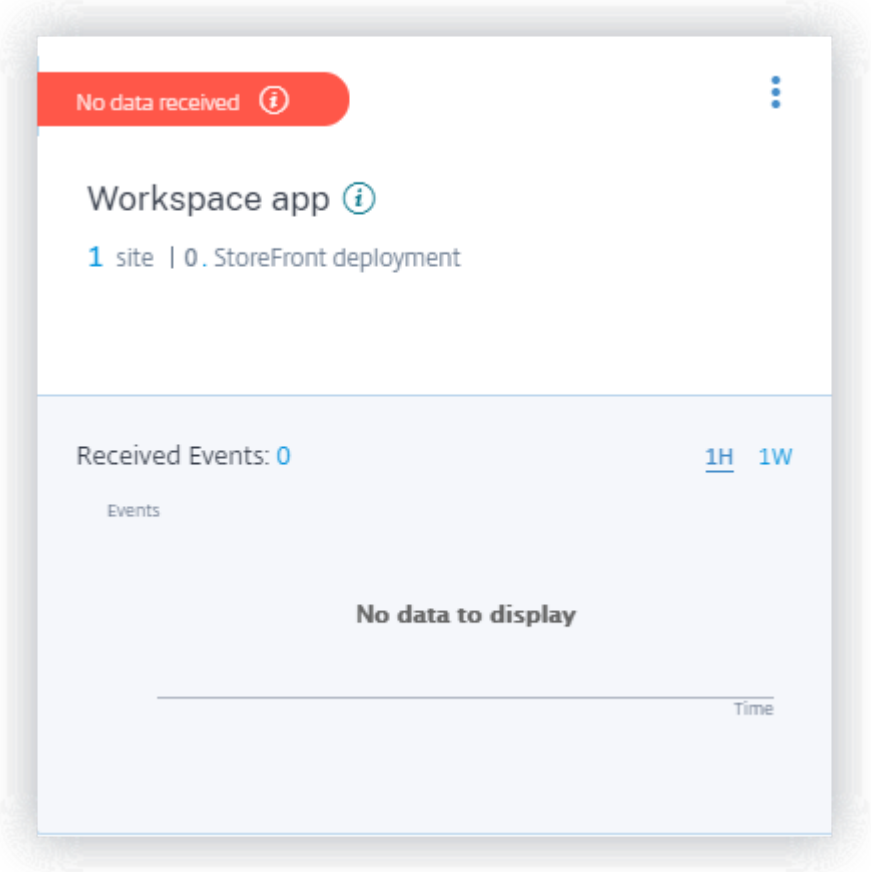
同じ Workspace に複数のサイトを追加した場合、Analytics はワークスペース内のすべてのサイトのデータを処理して保存します。すべてのサイトで Analytics が正常に有効になると、成功メッセージが表示されます。



サイトカードには、過去 1 時間の受信イベントが表示されます。これはデフォルトの時間選択です。1 週間（1 W）を選択して、データを表示することもできます。受信したイベントの数をクリックすると、対応するセルフサービス検索ページでイベントが表示されます 。

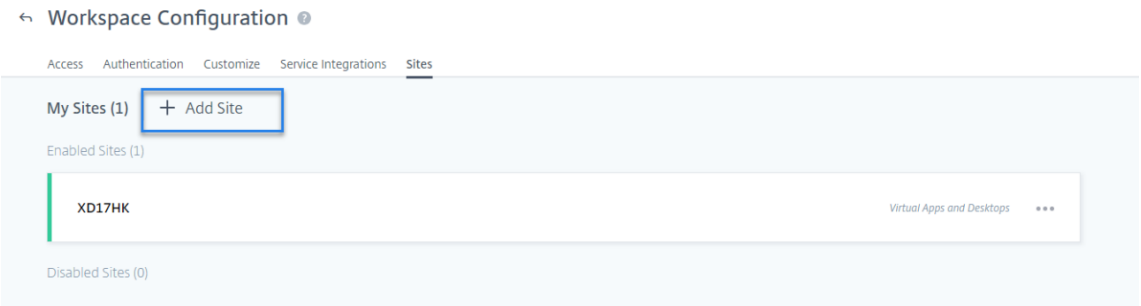
データ処理を有効にすると、サイトカードに [データを受信していません] ステータスが表示される場合があります。このステータスは、次の 2 つの理由で表示されます:

1. 初めてデータ処理をオンにした場合、イベントが Citrix Analytics のイベントハブに到達するまでに時間がかかります。Citrix Analytics がイベントを受信すると、ステータスが **Data processing on** に変わります。しばらくしてもステータスが変わらない場合は、[データソース] ページを更新します。
2. アナリティクスは、過去 1 時間の間にデータソースからイベントを受信していません。



サイトの追加　別のオンプレミスサイトを Workspace に追加する場合は、Analytics から追加できます:

1.「ワークスペース構成」ページで、「**+** サイトを追加」をクリックします。



2. 画面の指示に従って、サイトを追加します。詳細については、「ワークスペースでのオンプレミスの仮想アプリケーションおよびデスクトップの集約」を参照してください。
3. サイトを追加したら、Citrix Analytics に移動し、［データソース］ページを更新して、サイトカードに最近追加したサイトを表示します。

オンプレミスサイトの **Citrix Director** に接続する

Citrix Director は 、Citrix Virtual Apps and Desktops 用の監視およびトラブルシューティングコンソールです。Director を使用して、オンプレミスのサイトをセキュリティ向け Citrix Analytics（セキュリティ分析）用に構成できます。サイトが構成されると、Director は監視イベントをセキュリティ分析に送信します。

Citrix DaaS を使用している場合、Citrix Monitor サービスはクラウドサイトからセキュリティアナリティクスにイベントを送信します。

クラウド展開とオンプレミス展開の両方が存在するハイブリッド環境では、Security Analytics は Citrix Monitor サービスおよび Citrix Director にオンボーディングされたサイトからイベントを受信します。

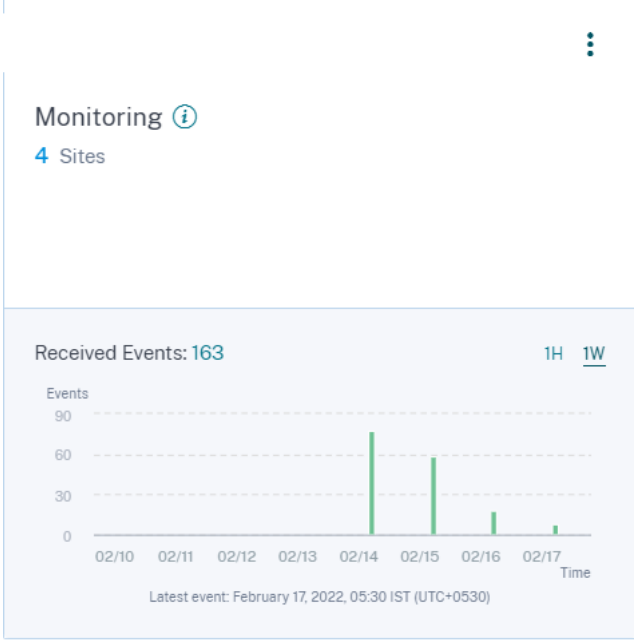
前提条件と設定手順

> メモ
>
> - 現在、Director ユーザーインターフェイスには、パフォーマンス向け Citrix Analytics（パフォーマンス分析）に関連する構成手順が表示されます。これらの構成手順は、セキュリティ向け Citrix Analytics（セキュリティ分析）にも適用されます。セキュリティ分析のアクティブな Citrix Cloud 資格がある場合は、以下の手順に従って Citrix Director に接続できます。
> - Citrix Cloud アカウントにセキュリティ分析とパフォーマンス分析の両方の有効な資格があり、すでにパフォーマンス分析用にサイトを構成している場合は、セキュリティ分析用に Director を再度構成する必要はありません。

前提条件と構成手順について詳しくは、パフォーマンス向け Citrix Analytics のドキュメントを参照してください。

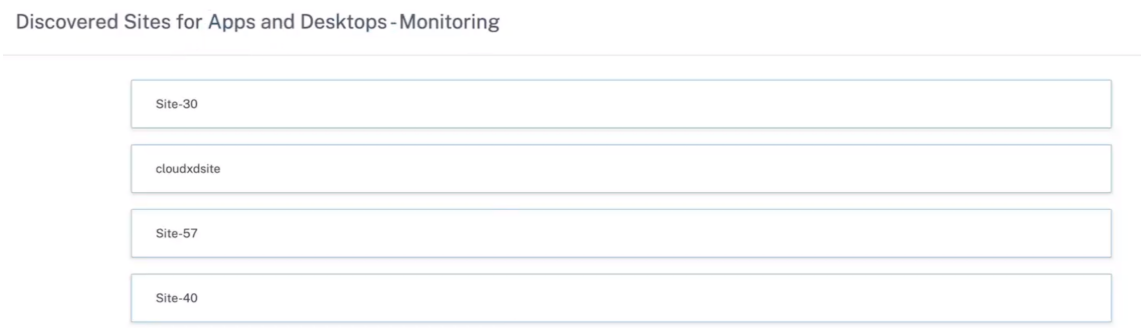
接続したサイトと受信したイベントを表示する

1. Citrix Analytics で、［データソース］ページに移動します。
2. ［セキュリティ］タブをクリックします。
3. [アプリとデスクトップ-監視] サイトカードでは、オンプレミスサイトまたはクラウドサイト (該当する方) を表示できます。また、サイトから受信したイベントも表示します。



> メモ
>
> - Director でオンプレミスサイトを初めて構成する場合、サイトからのイベントの処理にしばらく時間がかかり（約 1 時間）、接続されているサイトが［アプリとデスクトップ-監視］サイトカードに表示されるのが遅れることがあります。
> - [監視] サイトカードでは、Monitor サービスまたは Director データソースのデータ処理が既定で有効になっています。必要に応じて、データ処理をオフにすることもできます。ただし、Security Analytics のメリットを最大限に引き出すには、データ処理を継続することをお勧めします。

4. サイトをクリックすると詳細が表示されます。



Session Recording デプロイメント

Session Recording を使用すると 、Citrix Virtual Apps and Desktops Citrix DaaS での任意のユーザーセッションの画面上のアクティビティを記録できます。ユーザーイベントを Citrix Analytics for Security に送信するように、Session Recording サーバーを構成できます。ユーザーイベントは、ユーザーの危険な行動に関する実用的なインサイトを提供するために処理されます。

前提条件

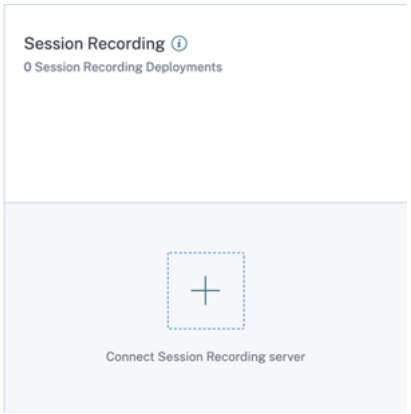
開始する前に、次のことを確認してください。

- Session Recording サーバーと VDA エージェントは 2103 以降である必要があります。
- Session Recording サーバーは、必要なアドレスに接続できる必要があります。URL の詳細については、「ネットワーク要件」を参照してください。
- Session Recording 展開では、送信インターネット接続用にポート 443 を解放する必要があります。ネットワーク上のすべてのプロキシサーバーは、この Citrix Analytics for Security との通信を許可する必要があります。
- Citrix Virtual Apps and Desktops 7 1912 LTSR を使用している場合、サポートされている Session Recording のバージョンは 2103 以降です。

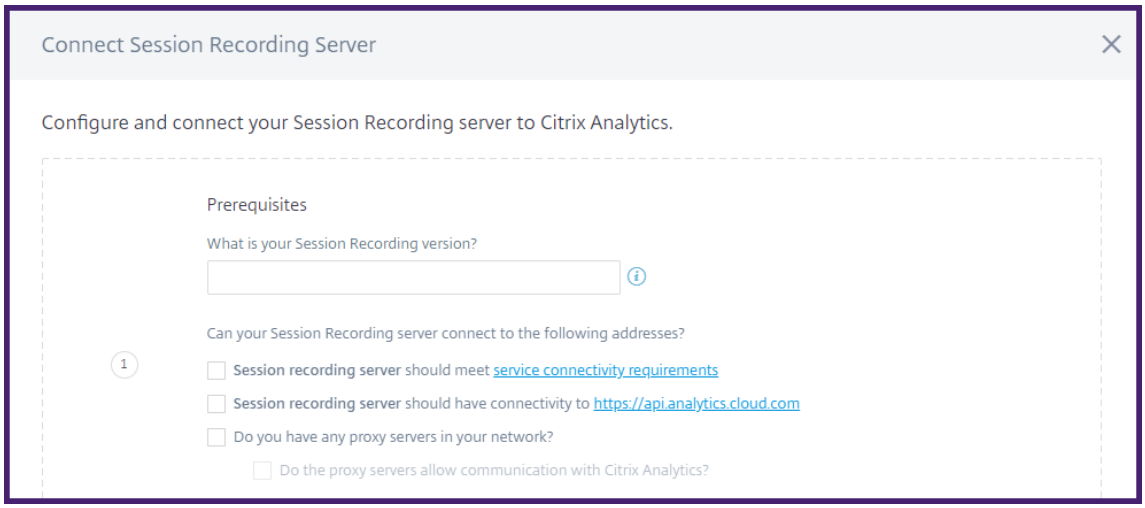
> 注:
>
> **Session Recording** サービスを使用する際は、追加の接続要件を必ず確認してください 。

Session Recording サーバーを設定する

1. アプリとデスクトップ**-Session Recording** サイトカードで、[**Session Recording** サーバーの接続] をクリックします



2. [**Connect Session Recording Server**] ページで、チェックリストを確認し、すべての必須要件を選択します。必須要件を選択しない場合、[ファイルのダウンロード] オプションは無効になります。



3. ネットワークにプロキシサーバーがある場合は、Session Recording サーバーの *ssrecStorageAnager.exe.config* ファイルにプロキシアドレスを入力します。

   構成ファイルは次の場所にあります: <Session Recording Server installation path>\bin\SsRecStorageManager.exe.config

   たとえば、次のようになります: C:\Program Files\Citrix\SessionRecording\Server\Bin\SsRecStorageManager.exe.config

4. [ファイルのダウンロード] をクリックして、*SessionRecordingConfigurationFile.json* ファイルをダウンロードします。

   > 注
   >
   > このファイルには機密情報が含まれています。ファイルを安全な場所に保存します。

5. Citrix Analytics for Security に接続する Session Recording サーバーにファイルをコピーします。

6. 展開に複数の Session Recording サーバーがある場合は、接続する各サーバーにファイルをコピーし、手順に従って各サーバーを構成する必要があります。
7. Session Recording サーバーで、次のコマンドを実行して設定をインポートします:

```
<Session Recording Server installation path>\bin\SsRecUtils.exe -Import_SRCasConfigurations <configuration file path>
```

例:

```
C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.exe -Import_SRCasConfigurations C:\Users\administrator \Downloads\SessionRecordingConfigurationFile.json
```

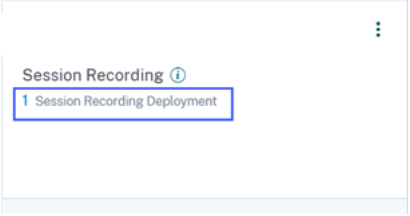
8. 次のサービスを再起動します:
   - Citrix Session Recording Analytics サービス
   - Citrix Session Recording ストレージマネージャー
9. 構成が正常に完了したら、Citrix Analytics for Security に移動して、接続されている Session Recording サーバーを表示します。[データ処理をオンにする] をクリックして、Citrix Analytics for Security でデータを処理できるようにします。

> 注
>
> Session Recording サーバーバージョン 2103 または 2104 を使用している場合は、まずアプリとデスクトップセッションを起動して、接続されている Session Recording サーバーを Citrix Analytics for Security で表示する必要があります。こうしないと、接続されている Session Recording サーバーが表示されません。この要件は、Session Recording サーバーバージョン 2106 以降には適用されません。

接続された展開を表示する

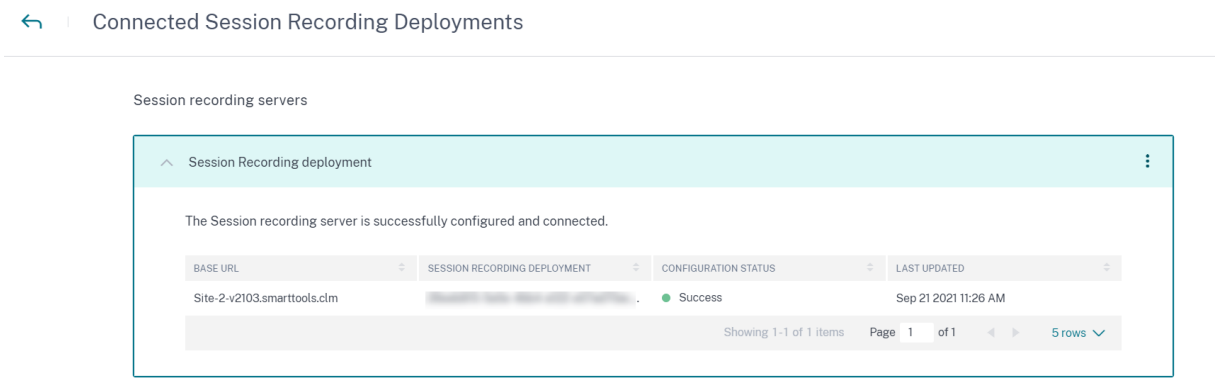
サーバーの展開は、構成が成功した場合にのみ Session Recording サイトカードに表示されます。サイトカードには、Citrix Analytics for Security との接続を確立した構成済みサーバーの数が表示されます。

設定が完了しても Session Recording サーバーが表示されない場合は、「トラブルシューティング」の記事を参照してください。



サイトカードで、展開の数をクリックして、Citrix Analytics for Security で接続されているサーバーグループを表示します。たとえば、**1 Session Recording Deployment** をクリックして、接続されている 1 つまたは複数のサ

ーバーグループを表示します。各 Session Recording サーバーは、ベース URL と ServerGroupID で表示されます。



受信したイベントを表示する

サイトカードには、接続された Session Recording 展開と、これらの展開から過去 1 時間に受信したイベントが表示されます。これは、デフォルトの時間の選択肢です。1 週間（1 W）を選択して、データを表示することもできます。受信したイベントの数をクリックして、セルフサービス検索ページにイベントを表示します。

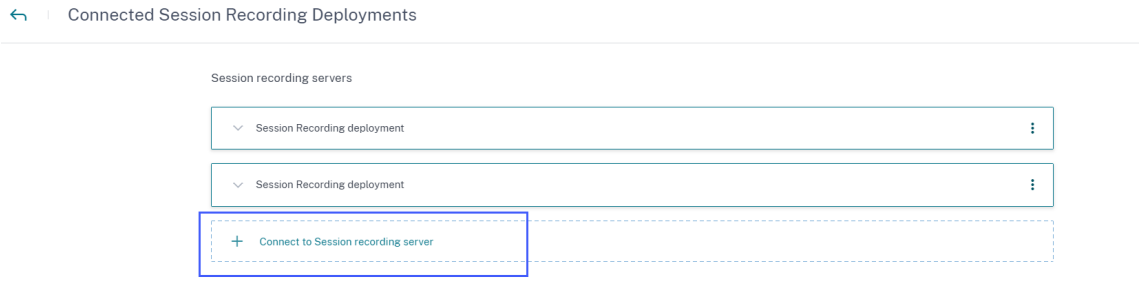
データ処理を有効にすると、サイトカードに **No data received** ステータスが表示される場合があります。このステータスは、次の 2 つの理由で表示されます:

1. 初めてデータ処理をオンにした場合、イベントが Citrix Analytics のイベントハブに到達するまでに時間がかかります。Citrix Analytics がイベントを受信すると、ステータスが **Data processing on** に変わります。しばらく経ってもステータスが変わらない場合は、[Data Sources] ページを更新してください。
2. Citrix Analytics は、過去 1 時間にデータソースからイベントを受信していません。

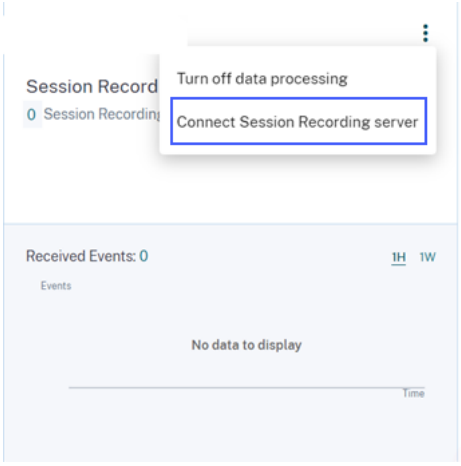
Session Recording サーバーを追加する

Session Recording サーバーを追加するには、次のいずれかを実行します:

- [**Connected Session Recording Deployments**] ページで、[**Session Recording Server** への接続] をクリックします。



- ［アプリとデスクトップ-**Session Recording** ］サイトカードで、縦方向の省略記号（⊠）をクリックし、［**Session Recording** サーバーの接続］を選択します。

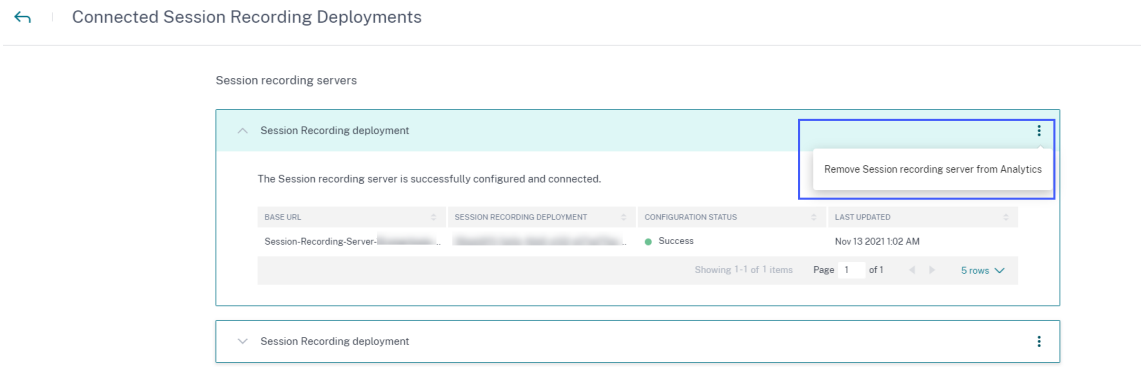


手順に従って構成ファイルをダウンロードし、Session Recording サーバーを構成します。

Session Recording サーバーを削除する

Session Recording サーバーを削除するには：

1. Citrix Analytics for Security で、［**Connected Session Recording Deployments**］ページに移動し、削除するサーバー展開を選択します。
2. 縦の省略記号（⊠）をクリックし、［**Remove Session Recording server from Analytics**］を選択します。



3. Citrix Analytics から削除した Session Recording サーバーで、次のコマンドを実行します：

```
<Session Recording Server installation path>\bin\SsRecUtils.exe -
    Remove_SRCasConfigurations
```

例：

```
C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.
exe -Remove_SRCasConfigurations
```


Citrix DaaS の印刷テレメトリを有効にする

ユーザーが Citrix DaaS（以前の Citrix Virtual Apps and Desktops サービス）で印刷ジョブを実行すると、Citrix Analytics for Security でこれらの印刷ジョブに関連するログを表示できます。これらの印刷ログは、プリンタ名、印刷ファイル名、印刷部数など、印刷アクティビティに関する重要な情報を提供します。

> 注
>
> この機能は Citrix DaaS でのみサポートされています。

Citrix Analytics for **Security** の検索ページで、アプリとデスクトップのデータソースを選択して印刷ログを表示できます。セキュリティ管理者は、これらのログをユーザーのリスク分析と調査に使用できます。

デフォルトでは、これらの印刷ログの収集と送信である印刷テレメトリ機能は、仮想配信エージェント（VDA）では無効になっています。

印刷テレメトリを有効にし、Citrix Analytics for Security に印刷ログを送信できるようにするには、レジストリキーを作成して VDA を構成する必要があります。

> 重要
>
> : この構成は、Windows VDA にのみ適用されます。

前提条件

- VDA のバージョンは、Citrix Virtual Apps and Desktops 7 2203 LTSR 以降のベースラインバージョンと同じである必要があります。詳しくは、「Citrix Virtual Apps and Desktops 7 2203 ベースラインコンポーネント」を参照してください。
- レジストリキーの更新を実行するには、フルアクセス権限が必要です。

電源管理されたマシンで印刷テレメトリを有効にする

電源管理されたマシンには、次のシナリオの仮想マシンまたはブレード PC が含まれます。

- 既存のマスターイメージ
- 新しいマスターイメージ

VDA のバージョンが **Citrix Virtual Apps and Desktops 7 2203 LTSR** よりも低い既存のマスターイメージの印刷テレメトリを有効にする

1. マスター VDA マシンにログインし、現在の状態のスナップショットを作成します。
2. 次のレジストリキーを追加して、印刷サービスログを有効にします。
    - Microsoft-Windows-プリントサービス/オペレーショナル

- イベントログに役職を表示する

レジストリキーの詳細については、「レジストリキーの作成」を参照してください。

3. VDA を Citrix Virtual Apps and Desktops 7 2203 LTSR 以降のベースラインバージョンにアップグレードします。詳しくは、「Citrix Virtual Apps and Desktops 7 2203 ベースラインコンポーネント」を参照してください。
4. マシンの電源を切り、最新の状態のスナップショットを作成します。
5. Citrix Cloud にログインします。マシンカタログを選択し、［マシンの更新］をクリックして、画面の指示に従います。詳しくは、「マシンカタログの作成」を参照してください。
6. 24 時間待ちます。設定は 24 時間以内に自動的にプッシュされます。構成が既に完了している場合は、待つ必要はありません。
7. Citrix Workspace アプリを使用してデスクトップセッションを開始します。クライアントプリンターを使用してトリガーされたすべての印刷イベントは、Citrix Analytics for **Security** の検索ページに表示されます。

VDA バージョンが **Citrix Virtual Apps and Desktops 7 2203 LTSR** 以降と同じである既存のマスターイメージの印刷テレメトリを有効にする　オプション **1**: マスター VDA に印刷レジストリキーを追加し、仮想デスクトップを更新します。

1. マスター VDA マシンにログインし、現在の状態のスナップショットを作成します。
2. 次のレジストリキーを追加して、印刷サービスログを有効にします。

   - Microsoft-Windows-プリントサービス/オペレーショナル
   - イベントログに役職を表示する

   レジストリキーの詳細については、「レジストリキーの作成」を参照してください。
3. VDA マシンの電源を切り、最新の状態のスナップショットを作成します。
4. Citrix Cloud にログインし、マシンカタログを選択し、［マシンの更新］をクリックして、画面上の指示に従います。
5. Citrix Workspace アプリを使用してデスクトップセッションを開始します。クライアントプリンターを使用してトリガーされたすべての印刷イベントは、Citrix Analytics for **Security** の検索ページに表示されます。

オプション **2**: 仮想デスクトップを組織単位 (OU) に移動し、GPO を使用してレジストリキーを作成する

> 注**:**
>
> オプション 2 の方法は、スタティックマシンでのみ機能します。ランダムマシンの場合は、オプション 1 の方法（前述のとおり）に従う必要があります。

1. ドメインコントローラーマシンにログインします。
2. 次のレジストリキーを追加して、印刷サービスログを有効にします。

- Microsoft-Windows-プリントサービス/オペレーショナル
- イベントログに役職を表示する

レジストリキーの詳細については、「レジストリキーの作成」を参照してください。

> 注:
>
> どのドメインコントローラーでも、レジストリキーの作成は 1 回限りのタスクです。

1. Citrix Cloud から VDA マシンを再起動します。
2. Citrix Workspace アプリを使用してデスクトップセッションを開始します。クライアントプリンターを使用してトリガーされたすべての印刷イベントは、Citrix Analytics for **Security** の検索ページに表示されます。

新しいマスターイメージで印刷テレメトリを有効にする

1. ハイパーバイザーの管理ツールを使用して仮想マシン (VM) を作成します。この仮想マシンはマスター VDA として扱われます。
2. マスター VDA が必要なドメインに追加されていることを確認します。
3. マスター VDA にログインし、次のレジストリキーを追加して印刷サービスログを有効にします。

   - Microsoft-Windows-プリントサービス/オペレーショナル
   - イベントログに役職を表示する

   詳細については、「レジストリキーの作成」を参照してください。
4. Citrix Virtual Apps and Desktops 7 2203 LTSR 以降の VDA バージョンをインストールします。VDA のインストール中に、マスターイメージオプションを選択します。詳しくは、「Citrix Virtual Apps and Desktops 7 2203 ベースラインコンポーネント」を参照してください。
5. ホスティング接続が Citrix Cloud に追加されていることを確認します。詳しくは、「マシンカタログの作成」を参照してください。
6. マスターイメージを使用してマシンカタログを作成します。詳しくは、「マシンカタログの作成」を参照してください。
7. デリバリーグループを作成し、マシンカタログを追加します。詳しくは、「デリバリーグループの作成」を参照してください。
8. 24 時間待ちます。設定は、グループポリシーエンジンによって 24 時間以内に自動的にプッシュされます。
9. Citrix Workspace アプリを使用してデスクトップセッションを開始します。クライアントプリンターを使用してトリガーされたすべての印刷イベントは、Citrix Analytics for **Security** の検索ページに表示されます。

電源管理されていないマシンで印刷テレメトリを有効にする

電源管理対象外のマシンには、次のシナリオの物理コンピューターが含まれます。

- 既存の物理 VDA
- 新しい物理 VDA

VDA のバージョンが **Citrix Virtual Apps and Desktops 7 2203 LTSR** よりも低い既存の物理 **VDA** の印刷テレメトリを有効にする

1. 次のレジストリキーを追加して、印刷サービスログを有効にします:

   - Microsoft-Windows-プリントサービス/オペレーショナル
   - イベントログに役職を表示する

   詳細については、「レジストリキーの作成」を参照してください。

2. VDA を Citrix Virtual Apps and Desktops 7 2203 LTSR 以降のベースラインバージョンにアップグレードします。詳しくは、「Citrix Virtual Apps and Desktops 7 2203 ベースラインコンポーネント」を参照してください。
3. 24 時間待ちます。設定は 24 時間以内に自動的にプッシュされます。設定が既に完了している場合は、待つ必要はありません。
4. Citrix Workspace アプリを使用してデスクトップセッションを開始します。クライアントプリンターを使用してトリガーされたすべての印刷イベントは、Citrix Analytics for **Security** の検索ページに表示されます。

新しい物理 **VDA** の印刷テレメトリを有効にする

1. 物理 VM を作成し、ドメインを必要なドメイン名に変更します。
2. 仮想マシンにログインし、次のレジストリキーを追加して印刷サービスログを有効にします。

   - Microsoft-Windows-プリントサービス/オペレーショナル
   - イベントログに役職を表示する

   詳細については、「レジストリキーの作成」を参照してください。

3. Citrix Virtual Apps and Desktops 7 2203 LTSR リリース以降の VDA バージョンをインストールします。VDA のインストール中に、［リモート PC アクセス］オプションを選択します。
4. マシンカタログを作成します。詳しくは、「マシンカタログの作成」を参照してください。

   > **注:**
   >
   > マシン管理は、電源管理されていないマシン (物理マシンなど) として選択する必要があります。

5. デリバリーグループを作成し、マシンカタログを追加します。詳しくは、「デリバリーグループの作成」を参照してください。
6. 24 時間待ちます。設定は、グループポリシーエンジンによって 24 時間以内に自動的にプッシュされます。

7. Citrix Workspace アプリを使用してデスクトップセッションを開始します。クライアントプリンターを使用してトリガーされたすべての印刷イベントは、Citrix Analytics for **Security** の検索ページに表示されます。

レジストリキーを作成する

VDA で、次のいずれかのオプションを実行します。

- レジストリキーを手動で作成します。この方法は、マスター VDA と、展開環境内の物理 VDA の数が少ない場合に使用します。
- グループポリシーオブジェクト (GPO) を使用してレジストリキーを作成します。導入環境に物理 VDA マシンの数が多く、すべてのマシンで印刷テレメトリを有効にする必要がある場合に、この方法を使用してください。

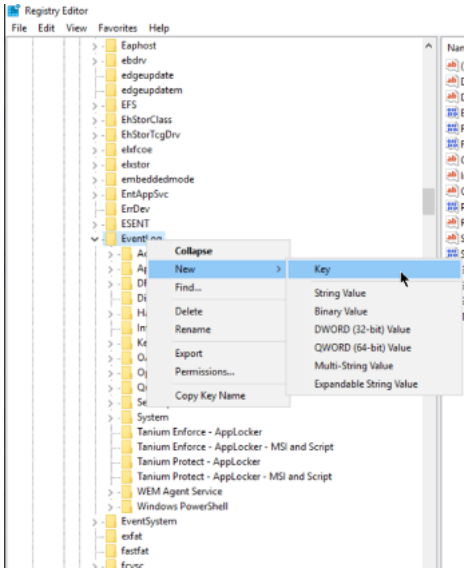
レジストリキーの詳細

SL	レジストリキー名	鍵の目的	レジストリの詳細
1	Microsoft-Windows-プリントサービス/オペレーショナル	イベントビューアでサービスログの印刷を有効にします。	レジストリパス:HKLM:\SYSTEM\CurrentControlSet\Serv
2	イベントログに役職を表示する	印刷ジョブ名を印刷イベントログに含めるかどうかを制御します。含めない場合、汎用ジョブ名は「Print Document」とみなされます。	レジストリハイブ:**HKEY_LOCAL_MACHINE** レジストリパス: Software\Policies\Microsoft\Windows NT\Printers 値名:showjobTitleEventLogs 値の種類:REG_DWORD バリュー:1

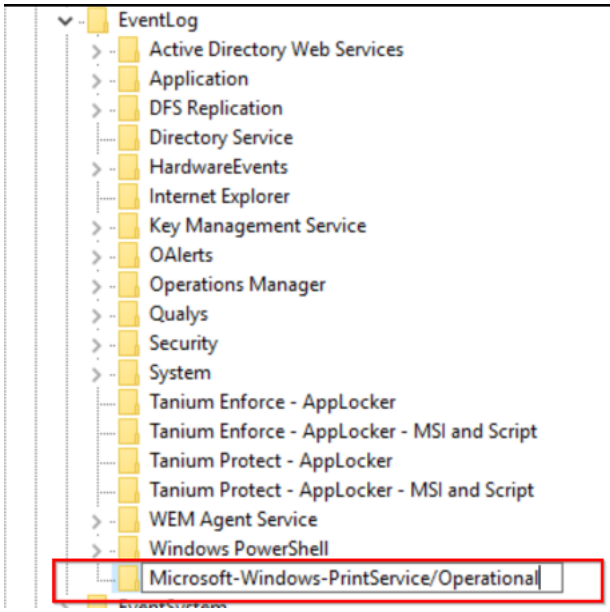
VDA マシンでレジストリキーを手動で作成する　この方法を使用して、VDA マスターイメージにレジストリキーを作成します。マスターイメージにキーを追加すると、マスターイメージを使用して作成されるすべてのタイプの VDA でキーを永続的に保つことができます。

1. VDA マスターマシンにサインインします。

2. ファイル名を指定して実行を開き、Regedit と入力して Windows レジストリを開きます。
3. 場所 HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet \Services\EventLog に移動します
4. **EventLog** を右クリックし、[新規**] > [**キー] を選択します。



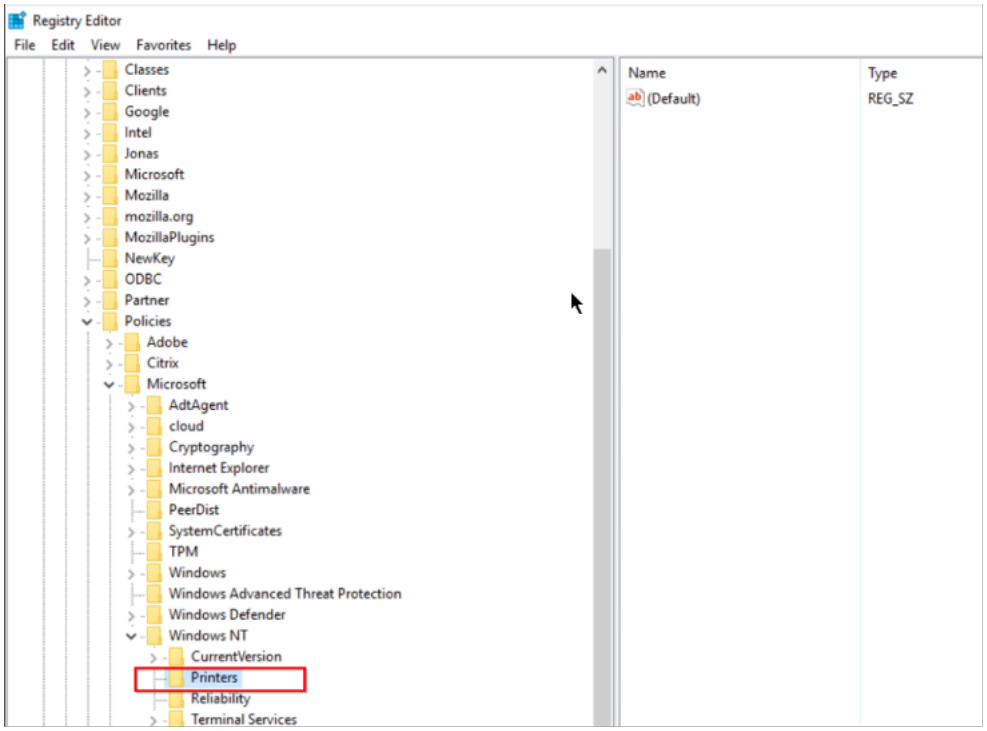
5. **Microsoft-Windows-Print** サービス/オペレーショナルという名前のキーを作成します。このキーは、印刷サービスログを有効にします。



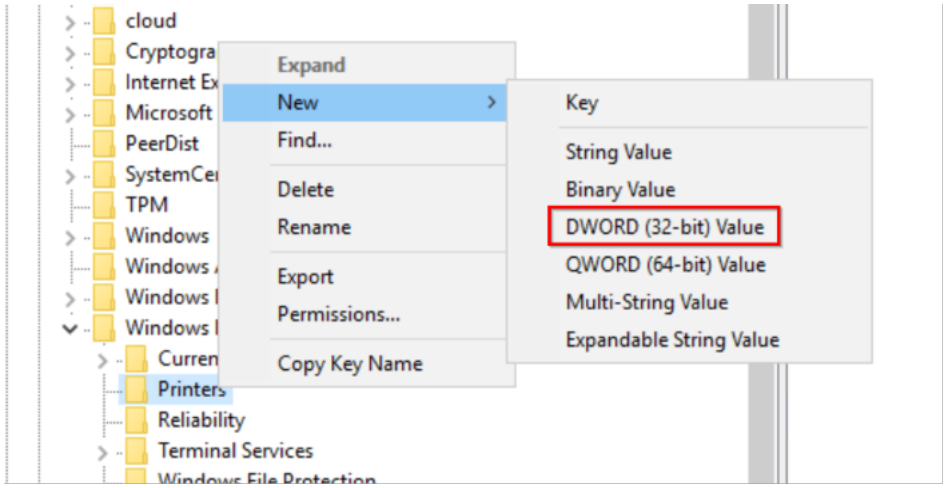
6. **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers** の場所に移動します。

> 注:
>
> [プリンタ] フォルダが使用できない場合は、Windows NT フォルダに Printers という名前のキーを作

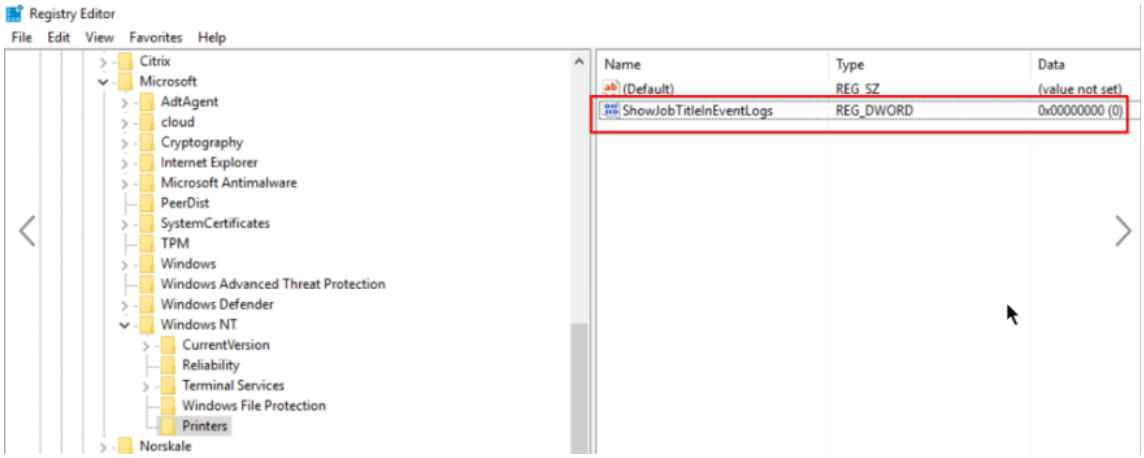
成します。



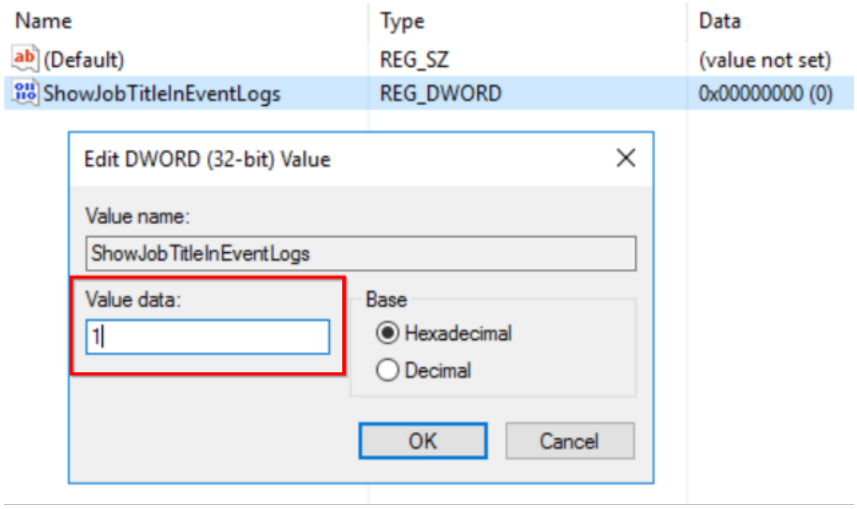
7. [プリンタ] フォルダを右クリックし、[新規] **> [DWORD (32** ビット**)** 値] を選択します。



8. **ShowJobTitleInEventLogs** という名前の値を作成します。



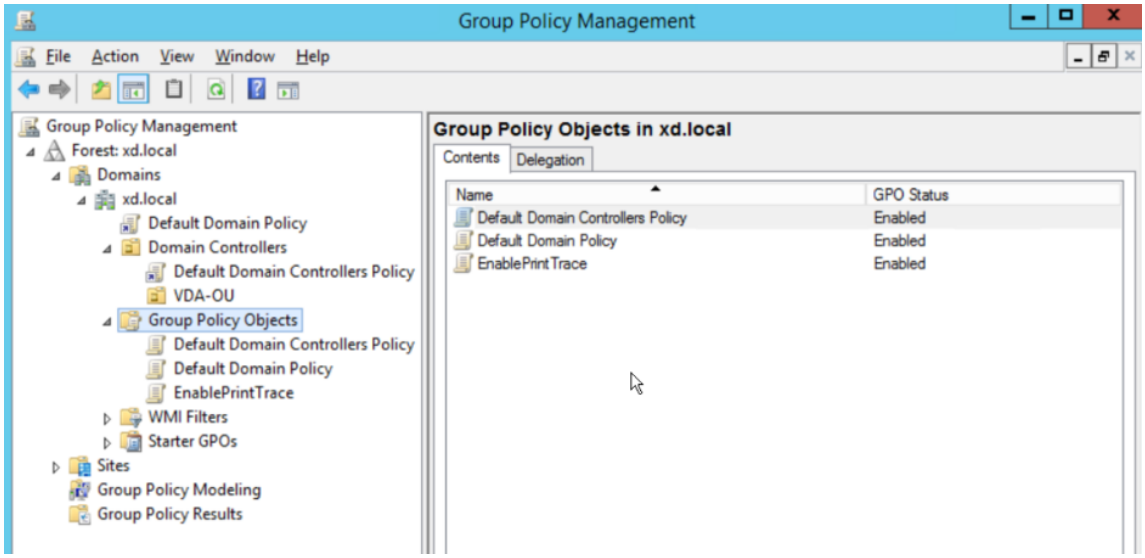
9. **ShowJobTitleInEventLogs** を右クリックして、変更を選択します。値データに 1 を入力して、「**OK**」をクリックします。



GPO を使用して複数の **VDA** にレジストリキーを作成する　このアプローチは永続 VDA でのみ機能し、レジストリキーの作成後に VDA を再起動する必要があります。永続 VDA は、再起動後もその状態を維持するマシンです。再起動後、ユーザーのデータは失われません。

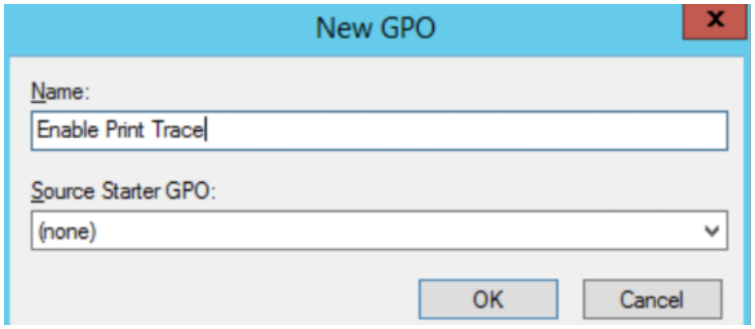
レジストリキーを使用してレジストリ **GPO** を作成する

1. [グループポリシー管理] を開き、[グループポリシーオブジェクト] を右クリックします。

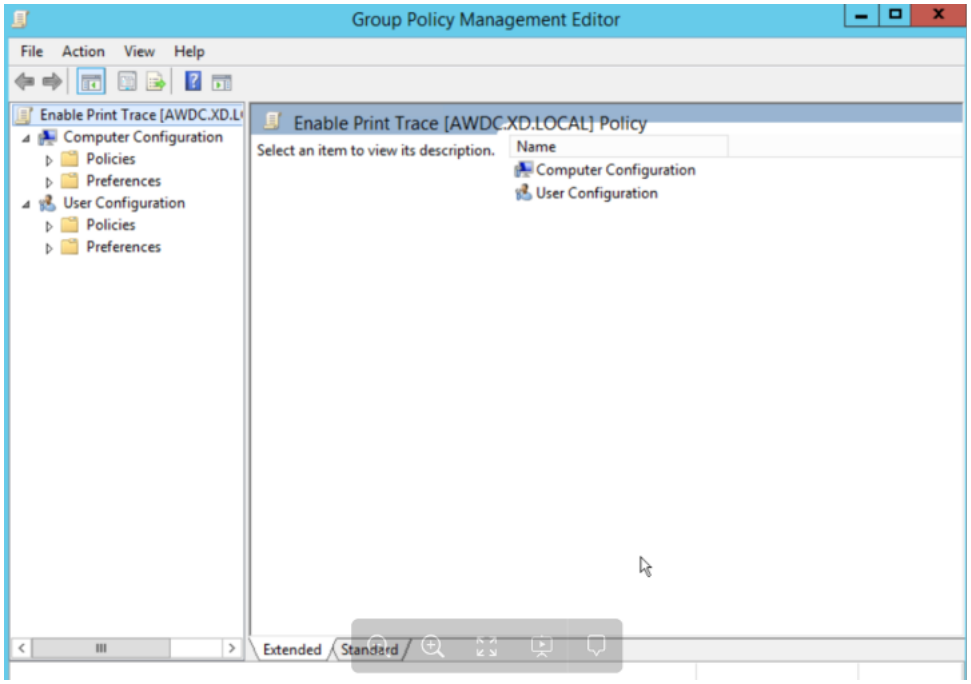


2. 「新規 **GPO** 」ウィンドウで、次のフィールドに値を入力します。

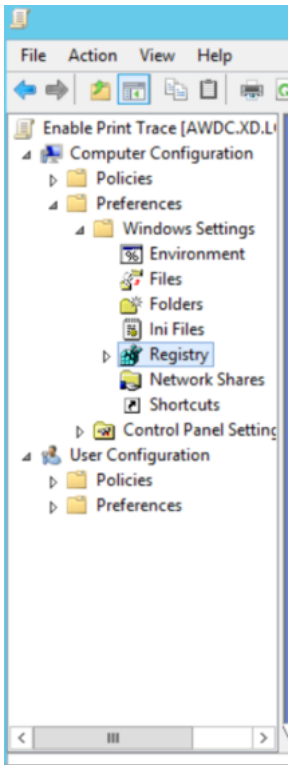
   - 名前: 印刷トレースを有効にする
   - ソーススターター GPO: (なし)



3. [**OK**] を選択します。
4. 作成した [印刷トレースの有効化] オブジェクトを右クリックし、[編集] を選択します。



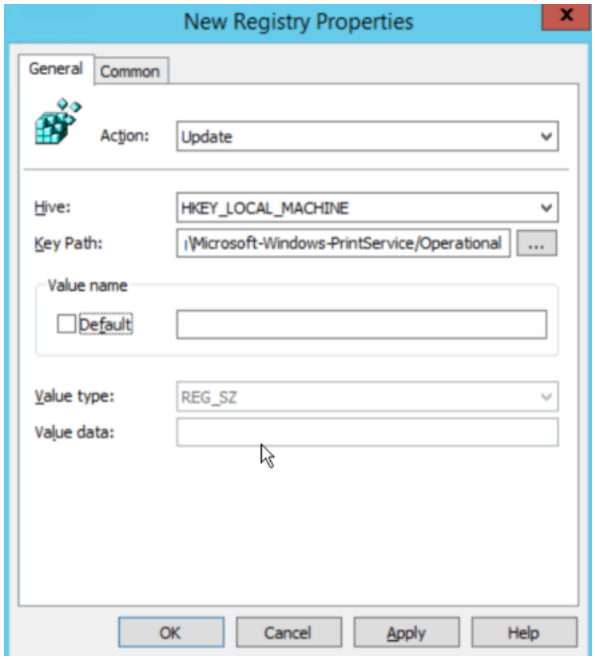
5. [コンピュータの構成] リストで、[環境設定**] > [Windows** の設定**]** を選択します。



6. [レジストリ] を右クリックし、[新規**] > [**レジストリ] を選択します。印刷ログを有効にするには、次のプロパティを入力します。

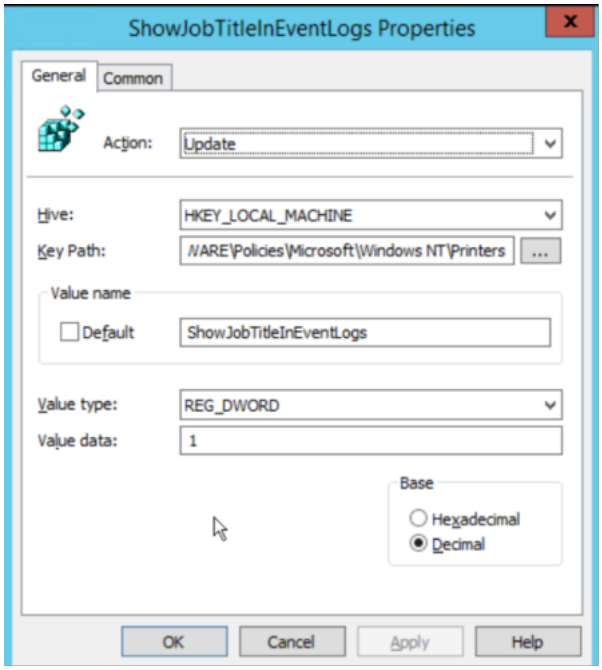
   - アクション: 更新

- Hive: HKEY_LOCAL_MACHINE
- キーパス:SYSTEM\ CurrentControlSet\ サービス\ イベントログ\ Microsoft-Windows-印刷サービス/運用



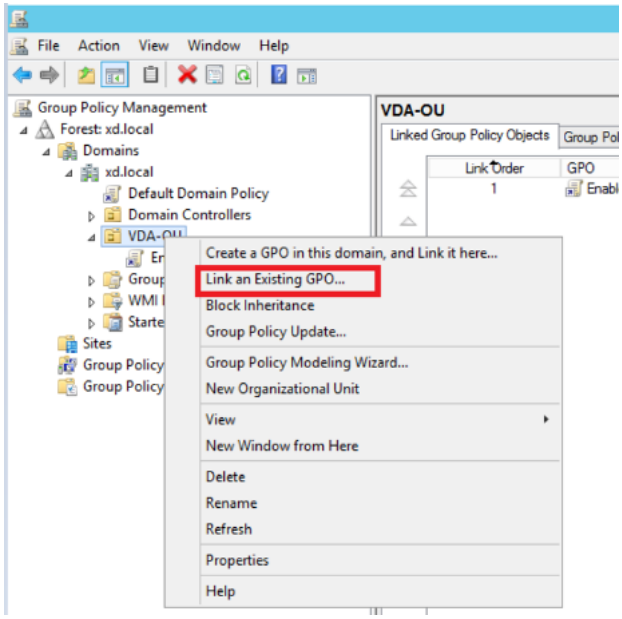
7. 「適用」を選択し、「**OK**」を選択します。
8. 再度、レジストリを右クリックし、[新規**] > [**レジストリ項目] を選択します印刷ジョブ名を有効にするには、次のプロパティを入力します。

   - アクション: 更新
   - Hive: HKEY_LOCAL_MACHINE
   - キーパス： SOFTWARE\Policies\Microsoft\Windows NT\Printers
   - 値名:showjobTitleEventLogs
   - 値の種類:REG_DWORD
   - バリューデータ:1
   - ベース: 十進表記

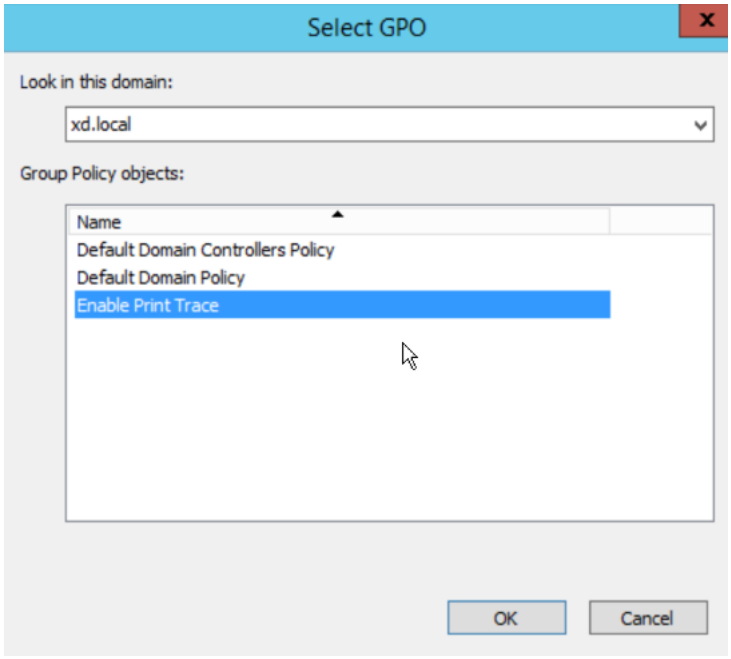


組織単位の印刷トレースを有効にする

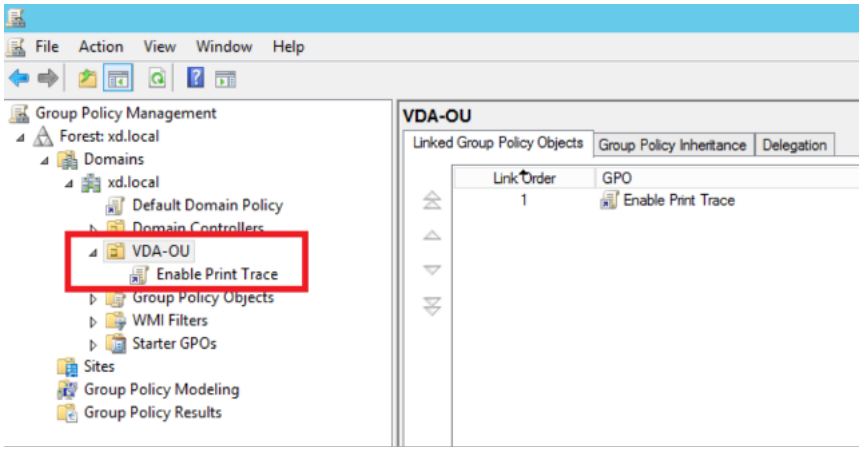
1. グループポリシー管理を開き、ドメイン（例：xd.local）を選択するか、VDA がその一部である場合は OU（VDA-OU など）を選択します。
2. ドメイン (xd.local) または OU (VDA-OU) を右クリックし、[既存の **GPO** をリンクする] を選択します。



3. [**GPO** の選択] ダイアログボックスで、[印刷トレースを有効にする] を選択し、[**OK**] を選択します。



4. 印刷トレースの有効化 **GPO** が **OU** にリンクされていることを確認します。



> 注
>
> - VDA を再起動すると、キュー内のイベントはすべて失われ、Citrix Analytics で使用できなくなります。
> - この再起動は、一度に 1 つのセッションしかアクティブにできないため、単一セッション VDA への影響は小さく、したがってイベントの数は少なくなります。
> - この再起動は、再起動中にすべてのアクティブセッションが終了し、キュー内のイベントが失われるため、マルチセッション VDA に大きな影響を与えます。

Citrix DaaS のクリップボードテレメトリを有効にする

Citrix DaaS（以前は Citrix Virtual Apps and Desktops サービスと呼ばれていました）を使用すると、ユーザーはクリップボード操作を実行でき、関連するログは Citrix Analytics for Security で表示できます。これらのクリッ

プボードログには、VDA 名、クリップボードサイズ、クリップボード形式の種類、クライアント IP、クリップボード操作、クリップボード操作の方向、クリップボード操作が許可されたかどうかなどの貴重な情報が含まれます。

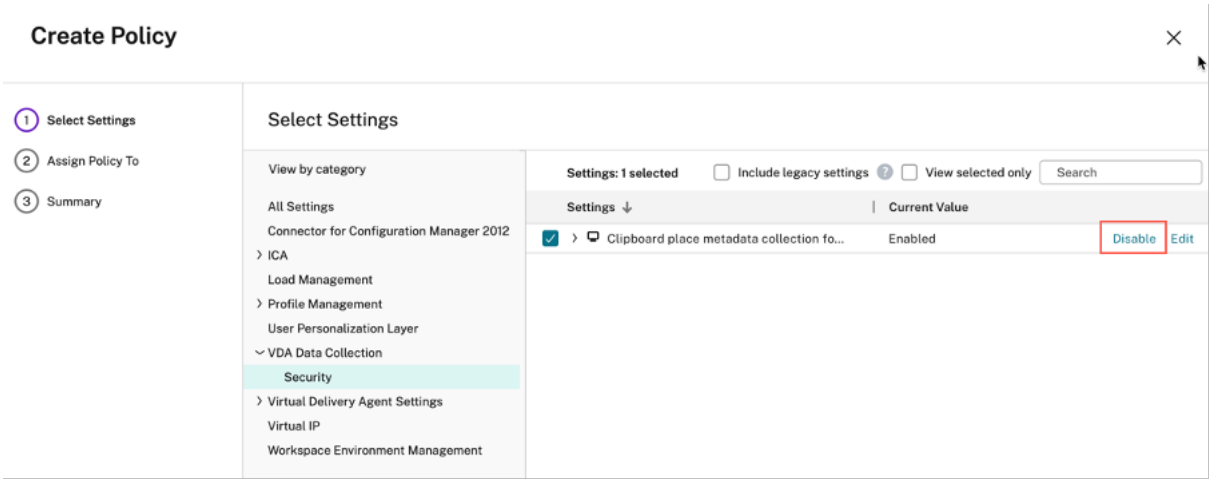
セキュリティ管理者は、Citrix Analytics for **Security の検索ページでアプリとデスクトップのデータソースを選択することで ** 、これらのログをリスク分析や調査に使用できます。

> 注
>
> - デフォルトでは、これらのクリップボードログの収集と送信は仮想配信エージェント（VDA）で有効になっています。
> - この構成は Windows VDA にのみ適用されます。

前提条件

- VDA のバージョンは、Citrix Virtual Apps and Desktops 7 2305 以降のベースラインバージョンと同じである必要があります。詳しくは、「Citrix Virtual Apps and Desktops 7 2305」を参照してください。
- **Web**Studio ポリシーページのクライアントクリップボードリダイレクト設定が禁止状態に設定されていないことを確認します ** 。詳しくは、「クライアントクリップボードリダイレクト」を参照してください。

セキュリティ監視ポリシーのクリップボードプレースメタデータコレクションを使用して、クリップボードテレメトリを有効または無効にできます。デフォルトでは、このポリシーは有効になっています。無効にするには、[ポリシー] ページに移動し、[**VDA** データコレクション] で [セキュリティ] を選択し、ポリシーを確認して [無効化] をクリックする必要があります。



詳細については、「セキュリティ監視のためのクリップボードプレースメタデータの収集」を参照してください。

データソースのデータ処理をオンまたはオフにする

特定のデータソース（Director および Workspace アプリ）のデータ処理はいつでも停止できます。データソースサイトカードで、縦方向の省略記号 **(⋮) > [**データ処理をオフにする] をクリックします。Citrix Analytics は、そのデ

ータソースのデータの処理を停止します。アプリとデスクトップのサイトカードからデータ処理を停止することもできます。このオプションは、Director と Workspace アプリの両方のデータソースで使用できます。

データ処理を再度有効にするには、[データ処理をオンにする] をクリックします。

Microsoft Active Directory と Azure Active Directory の統合

May 10, 2022

AcActive Directory または Azure Active Directory を接続し、組織のドメインから Citrix Analytics for Security にユーザーの詳細とユーザーグループをインポートします。

この統合により、Citrix Analytics for Security のユーザープロファイルが、役職、組織、オフィスの場所、電子メール、連絡先などのユーザー ID の詳細で強化されます。[ユーザープロファイル] ページでは、リスクの調査と分析に役立つこれらのユーザー詳細を表示できます。

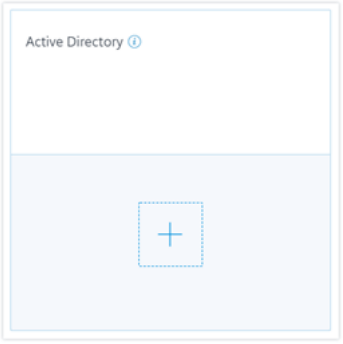
前提条件

- セキュリティのために Active Directory を Citrix Analytics スと接続する場合は、まず Active Directory が Citrix Cloud アカウントに接続されていることを確認してください。詳しくは、「Active Directory を Citrix Cloud に接続する」を参照してください。
- セキュリティのために Azure Active Directory を Citrix Analytics に接続する場合は、Azure Active Directory がまず Citrix Cloud アカウントに接続されていることを確認してください。詳しくは、「Azure Active Directory を Citrix Cloud に接続する」を参照してください。

Microsoft Active Directory に接続

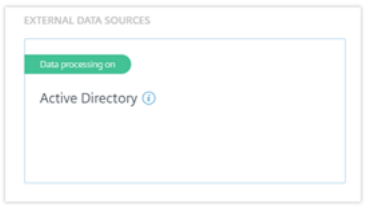
Active Directory をセキュリティのために Citrix Analytics に接続するには、次の手順に従います。

1. [設定] > [データソース] > [セキュリティ] に移動し、[外部データソース] セクションに移動します。
2. **Active Directory** サイトカードで、プラス記号 **(+)** をクリックします。



3. Active Directory を Citrix Analytics Citrix Cloud アカウントに接続するように求めるプロンプトが表示されます。詳細については、「前提条件」を参照してください。

Active Directory を Citrix Cloud アカウントに接続すると、この新しいデータソースが自動的に検出されます。[データソース] ページの Active Directory サイトカードに [データ処理中] と表示されます。

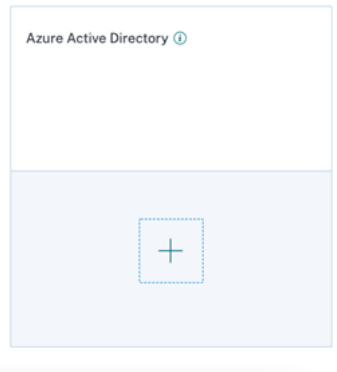


[データ処理中] ステータスは、Active Directory が検出され、ユーザー情報が Active Directory からフェッチされていることを示します。

Microsoft Azure Active Directory を接続します

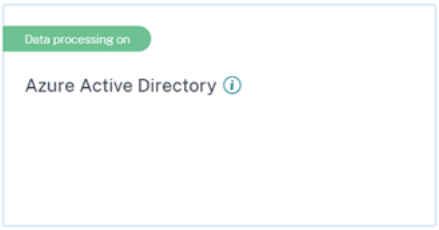
Azure Active Directory を Citrix Analytics に接続するには、次の手順を実行します。

1. **[**設定**] > [**データソース**] > [**セキュリティ] に移動し、[外部データソース] セクションに移動します。
2. **Azure Active Directory** サイトカードで、プラス記号 (+) をクリックします。



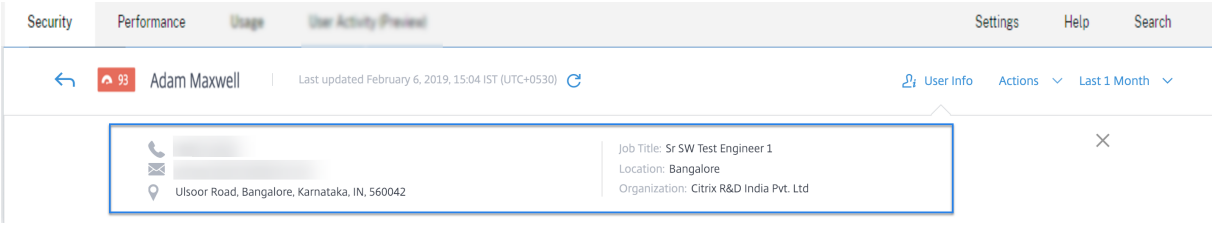
3. Azure Active Directory を Citrix Cloud アカウントに接続するように求めるメッセージが表示されます。詳しくは、「Azure Active Directory を Citrix Cloud に接続する」を参照してください。

Azure Active Directory を Citrix Cloud アカウントに接続すると、Citrix Analytics クスはこの新しいデータソースを自動的に検出します。[データソース] ページの **Azure Active Directory** サイトカードに [データ処理オン] と表示されます。このステータスは、Azure Active Directory が検出され、ユーザー情報が Azure Active Directory からフェッチされていることを示します。



ユーザー情報の表示

[セキュリティ] タブで、危険なユーザーをクリックしてユーザープロファイルページを表示します。ユーザーが Active Directory または Azure Active Directory で使用可能な場合は、ユーザープロファイルページで役職、組織、電子メール、および連絡先番号を表示できます。



Microsoft Graph Security の統合

June 24, 2021

Microsoft Graph Securityは、複数のセキュリティプロバイダからのデータを集約する外部データソースです。また、ユーザインベントリデータへのアクセスも提供します。

Citrix Analytics は現在、Microsoft Graph Security から以下のセキュリティプロバイダーをサポートしています。

- Azure AD Identity Protection
- Microsoft Defender for Endpoint

セキュリティプロバイダーについて詳しくは、次のリンクを参照してください。

- **Azure AD Identity Protection** の場合：https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events
- **Microsoft Defender for Endpoint** の場合：https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection

Microsoft Graph Security データソースをオンボードするには、テナントに代わって必要なアクセス許可を Microsoft ID プラットフォームから取得する必要があります。

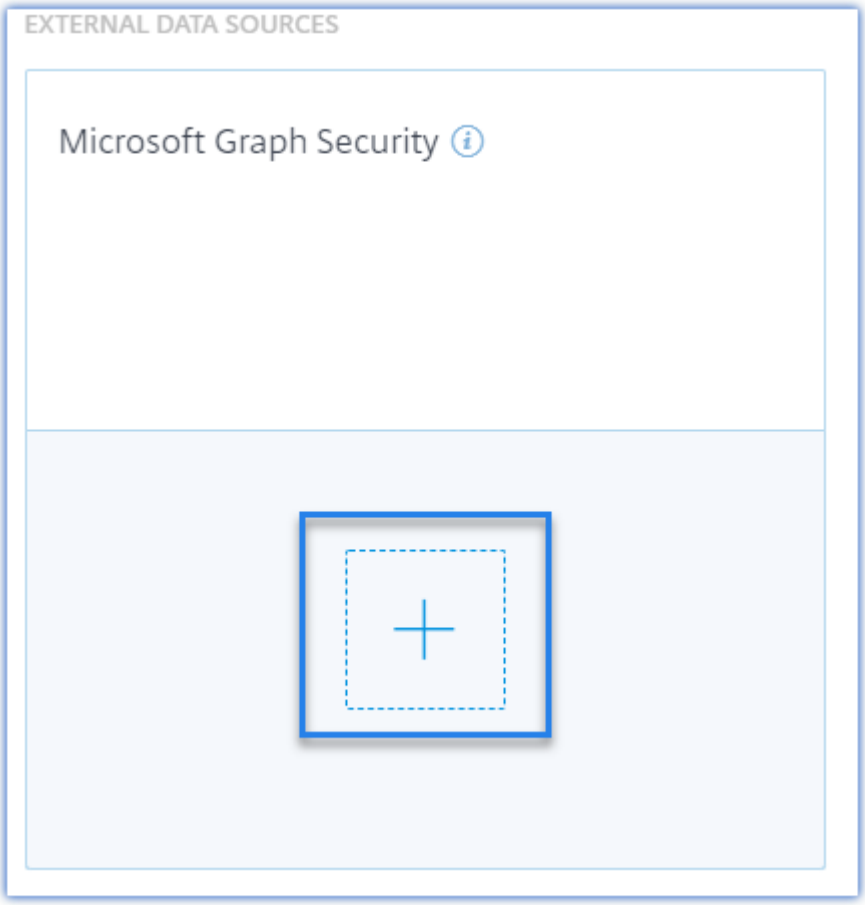
前提条件

Microsoft Graph Security データソースのオンボーディングを開始する前に、次のことを確認してください。

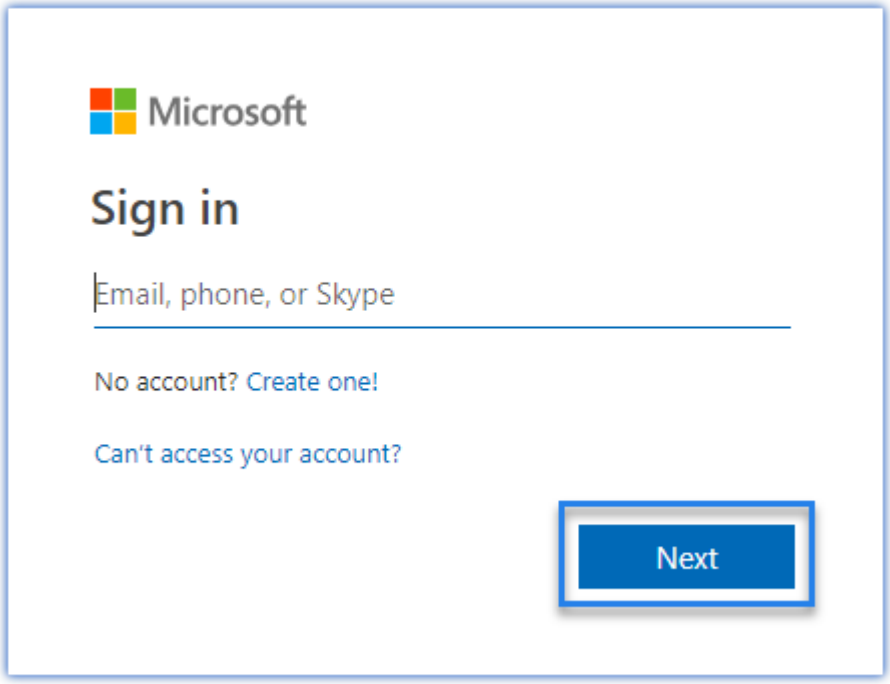
- 管理者は、Azure AD Identity Protection（Azure AD Premium P2 の一部）セキュリティプロバイダーを使用しています。
- エンドユーザーは、職場または学校のアカウントを使用して Microsoft Store にサインインしています。

Microsoft Graph Security インスタンスのオンボーディング

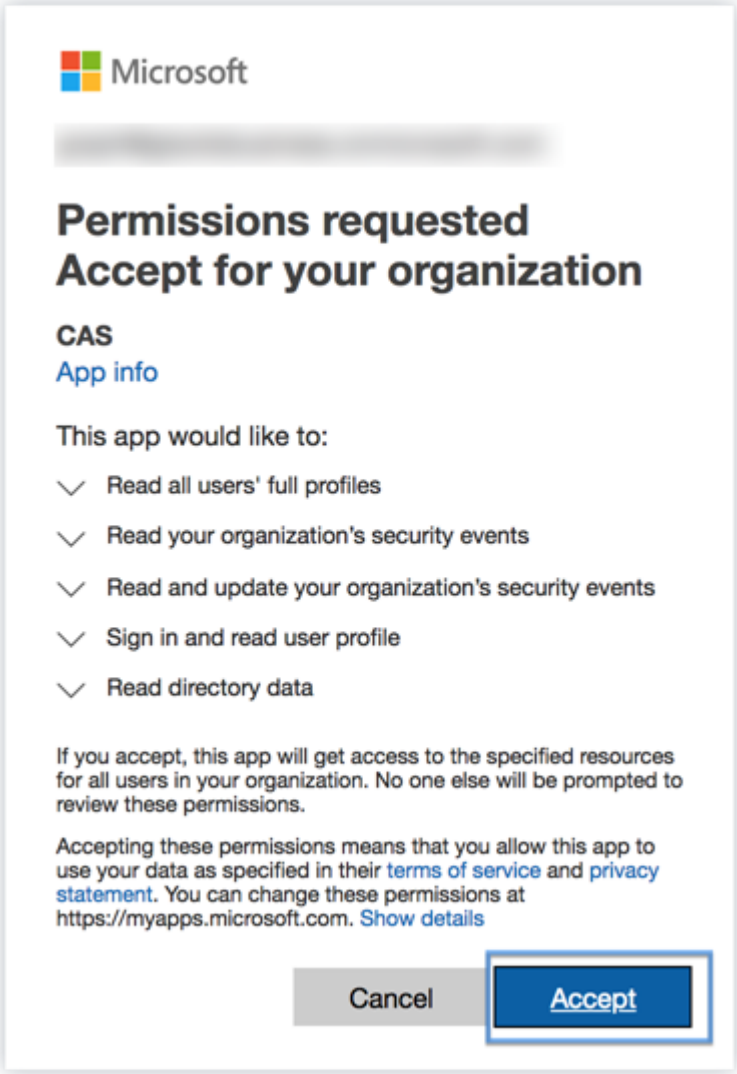
1. **[設定]** > **[データソース]** > **[セキュリティ]** にアクセスし、**[外部データソース]** セクションに移動します。
2. Microsoft Graph Security サイトカードのプラス記号 (**+**) をクリックします。認証エンドポイントにリダイレクトされます。



3. **Microsoft** ウィンドウで、Azure ログオン資格情報を使用してサインインし、アカウントを登録します。または、既存のアカウントを選択します。
4. ［次へ］をクリックします。



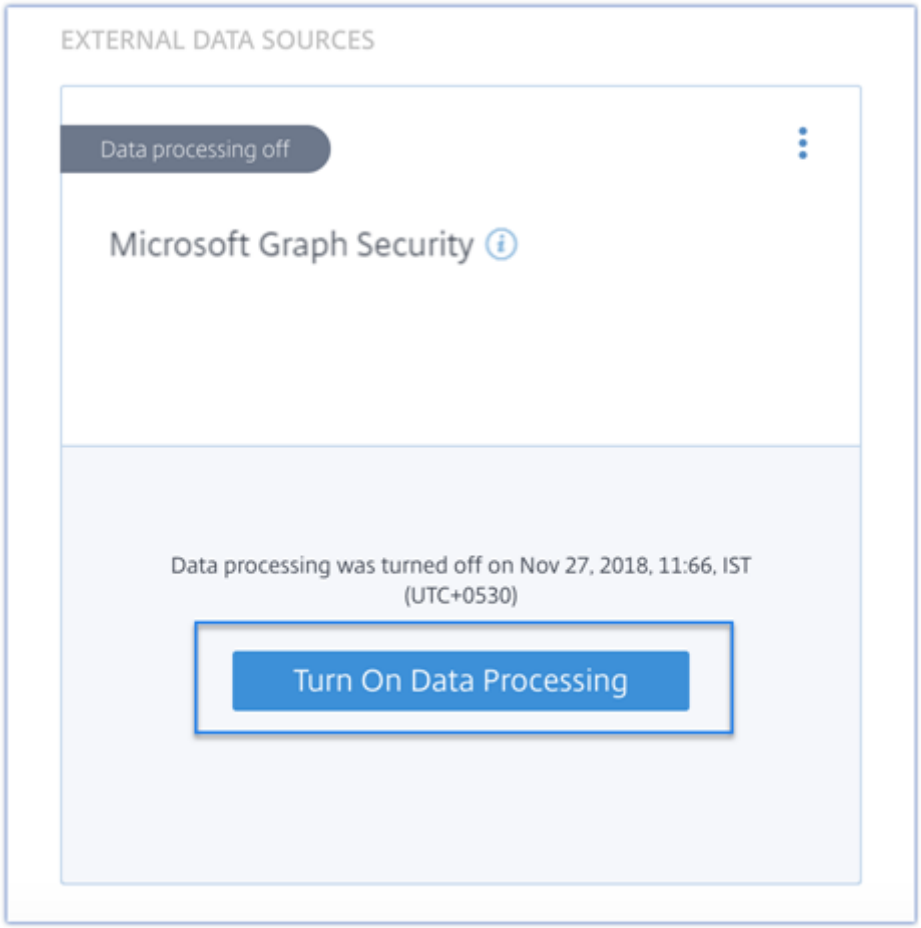
5. [受け入れ] をクリックします。[データソース] ページにリダイレクトされます。これで、Microsoft Graph Security データソースが Citrix Cloud アカウントにリンクされます。



データ処理のオンとオフを切り替える

データ処理を無効にするには、サイトカードの縦の省略記号（⊠）をクリックして、[データ処理をオフにする] を選択します。Citrix Analytics がこのデータソースのデータ処理を停止します。

サイトカード で [データ処理を有効にする] を選択すると、データ処理 を再度有効にすることができます。



Microsoft Graph Security リスク指標について詳しくは、「Microsoft Graph Security のリスク指標」を参照してください。

セキュリティ情報およびイベント管理 **(SIEM)** の統合

December 7, 2023

> 注
>
> < CAS-PM-Ext@cloud.com >SIEM 統合、SIEM へのデータのエクスポート、フィードバックの提供に関するサポートをリクエストするには、お問い合わせください。

Citrix Analytics for Security を SIEM サービスと統合し、ユーザーのデータを Citrix IT 環境から SIEM にエクスポートします。エクスポートしたデータを SIEM で使用可能なデータに関連付けて、組織のセキュリティ体制についてより深い洞察を得ることができます。

この統合により、Citrix Analytics for Security と SIEM の両方の価値が高まります。

メリット

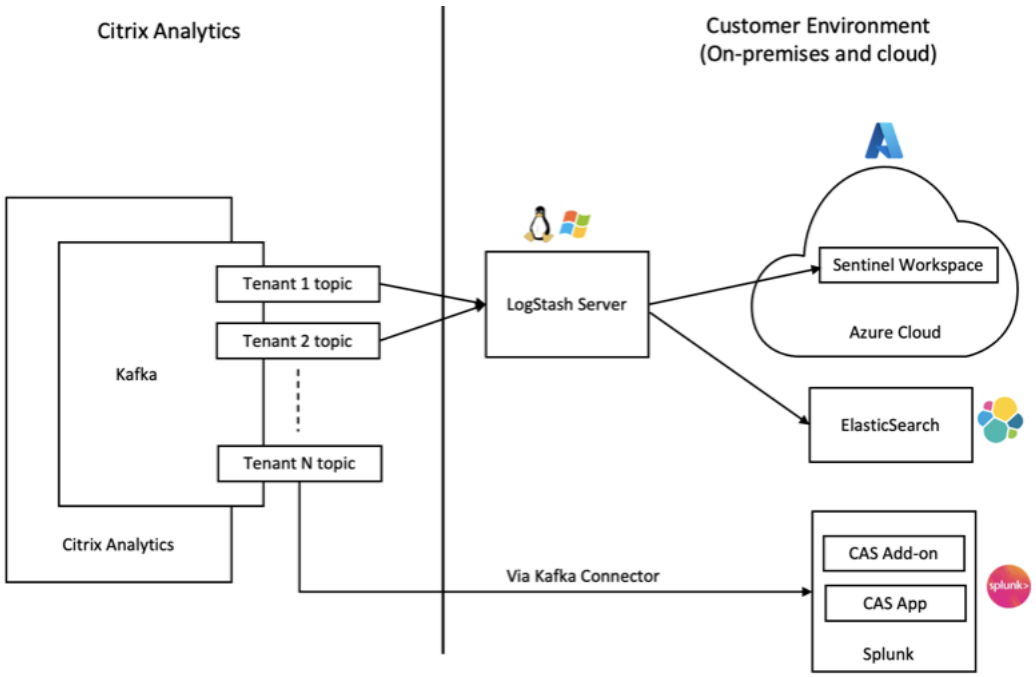
- セキュリティ運用チームは、異なるログのデータを相互に関連付け、分析、検索できます。
- セキュリティ運用チームがセキュリティリスクを特定し、迅速に修正できるよう支援します。
- セキュリティアラートを一元的に可視化。
- リスク指標、ユーザープロファイル、リスクスコアなどの組織のリスク分析機能のための潜在的なセキュリティ脅威を検出する一元的なアプローチ。
- ユーザーアカウントの Citrix Analytics リスクインテリジェンス情報を、SIEM 内で接続された外部データソースと結合して相関させる機能。

SIEM 統合アーキテクチャ

SIEM インテグレーションは、Citrix Analytics for Security クラウドにデプロイされたノースバウンドの Kafka に接続します。これは次の 2 つの方法で実現できます。

- **Kafka** エンドポイント: SIEM が Kafka エンドポイントをサポートしている場合は、Logstash 構成ファイルで提供されるパラメーターと、JKS ファイルまたは PEM ファイルの証明書の詳細を使用して、SIEM を Citrix Analytics for Security と統合します。Kafka エンドポイントを使用すると、選択した SIEM にデータを接続してプルできます。
- **Logstash** エンジン: お使いの SIEM が Kafka エンドポイントをサポートしていない場合は、Logstash データ収集エンジンを使用できます。Citrix Analytics for Security からのリスクインサイトデータを、Logstash がサポートする出力プラグインのいずれかに送信できます 。

Citrix Analytics for Security から SIEM サービスにデータがどのように流れるかを理解するには、次の SIEM ソリューションのアーキテクチャ図を参照してください。

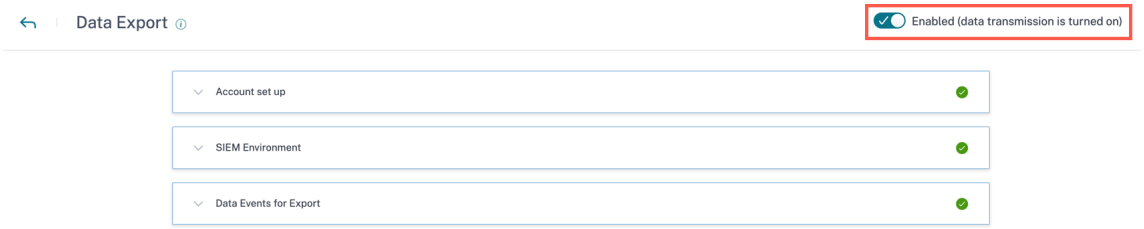


データ伝送をオンまたはオフにする

セキュリティ向け Citrix Analytics からのデータの送信を停止するには:

1. **[設定] > [データエクスポート]** に移動します。
2. トグルボタンをオフにしてデータ転送を無効にします。

> 注:
> デフォルトでは、SIEM のデータ転送は常にオン/有効になっています。



データ転送を再度有効にするには、トグルボタンをオンにします。

SIEM 環境のセットアップ

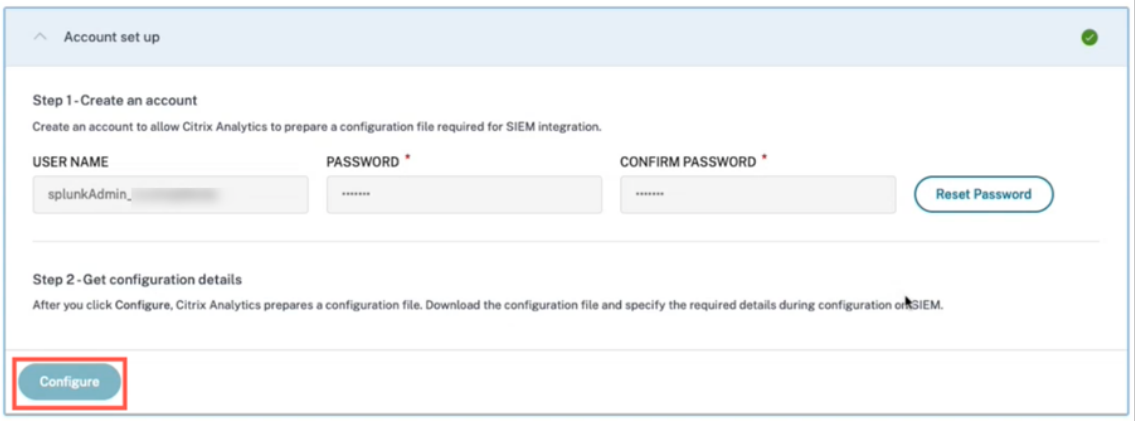
データを SIEM にエクスポートするには、次のアクションを実行する必要があります。

- Kafka アカウントと認証情報を設定する

- 事前に入力された設定をダウンロードし、SIEM 環境をセットアップします
- エクスポート用のデータイベント

SIEM エクスポートアカウントの設定

1. アカウントを設定するには、[設定] > [データエクスポート] に移動し、[アカウント設定] を展開します。ユーザー名とパスワードを指定してアカウントを作成します。アカウントを設定すると、Kafka の詳細が生成されます。これらの詳細は、構成ファイルの生成時に自動的に埋め込まれます。

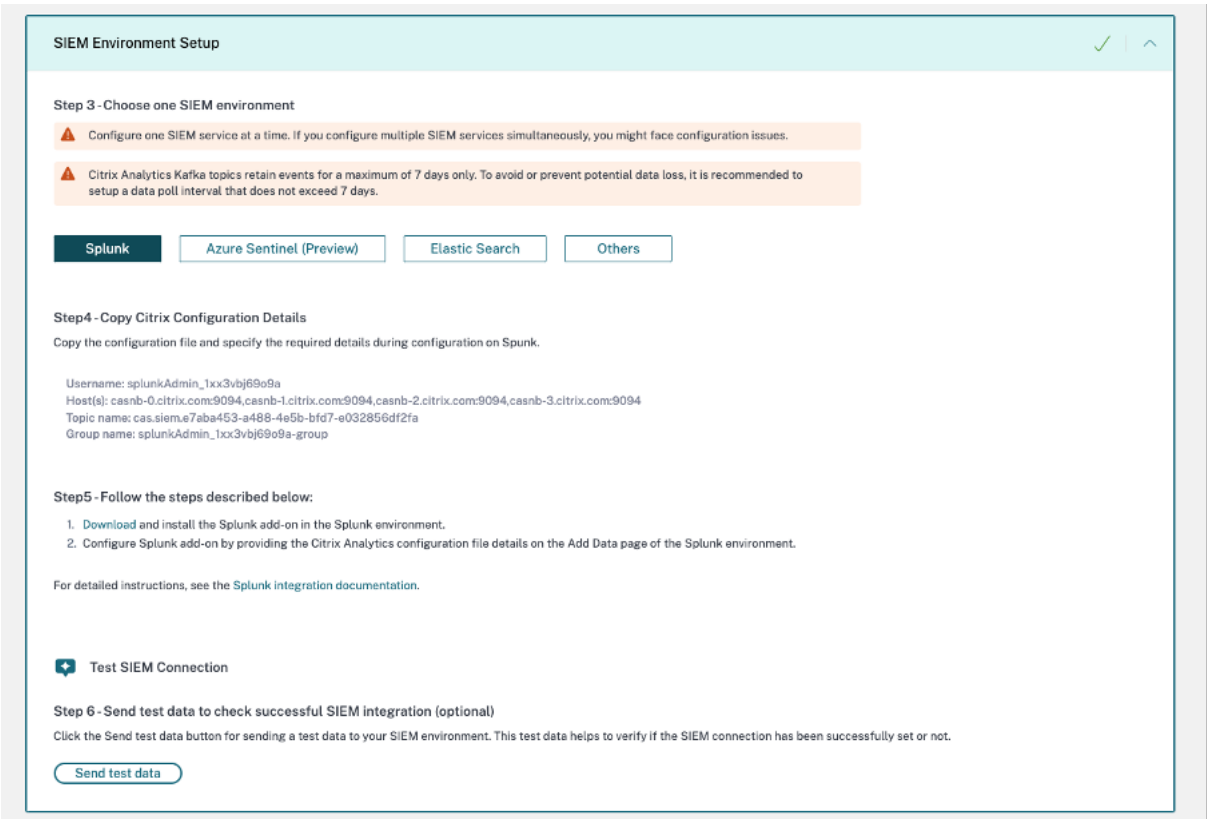


2. 「構成」をクリックして構成ファイルを生成します。設定ファイルには、Kafka エンドポイント、特定のサブスクリプショントピック、グループ ID などの詳細が含まれています。また、認証とデータフローを完了するために必要な Kafka 属性と SSL 属性が事前に設定されています。

SIEM の構成と環境のセットアップ

必要に応じて SIEM 環境を選択します。Citrix Analytics for Security を次のサービスと統合できます。詳細情報と SIEM 固有の設定については、次のリンクを参照してください。

- Splunk
- Microsoft Sentinel
- Elasticsearch
- Kafka または Logstash ベースのデータコネクタを使用する他の SIEM



Citrix Analytics for Security から **SIEM** サービスにエクスポートされたデータイベント

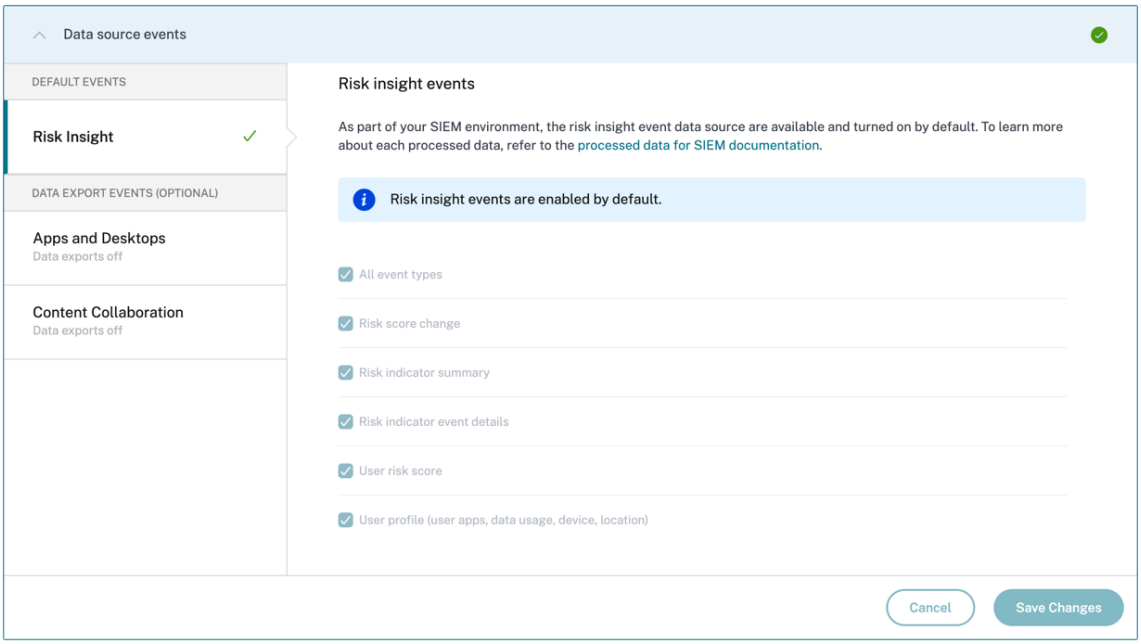
SIEM エクスポートの一部として、次の 2 種類のデータセットがあります。

1. リスクインサイトイベント **(**デフォルトエクスポート**)** —アカウント設定と SIEM 設定が完了すると、デフォルトデータ (リスクインサイトイベント) が SIEM デプロイメントに流れ始めます。リスクインサイトデータには、ユーザーリスクスコア、ユーザープロファイル、およびリスク指標アラートが含まれます。これらは、Citrix Analytics の機械学習アルゴリズム、ユーザー行動分析によって生成され、ユーザーイベントに基づいて生成されます。利用可能なイベントタイプ、メタデータ、スキーマについては、「SIEM のリスクインサイトデータ」を参照してください。
2. データソースイベント（オプションのエクスポート） -さらに、Citrix Analytics for Security 対応製品のデータソースからユーザーイベントをエクスポートするようにデータエクスポート機能を構成できます。Citrix 環境で何らかのアクティビティを実行すると、データソースイベントが生成されます。エクスポートされたイベントは、セルフサービスビューで利用できる未処理のリアルタイムのユーザーおよび製品使用データです。これらのイベントに含まれるメタデータは、さらに詳細な脅威分析や新しいダッシュボードの作成に使用したり、セキュリティや IT インフラストラクチャ全体で Citrix 以外のデータソースイベントと連携させたりすることができます。

   現在、Citrix Analytics for Security は、CitrixVirtual Apps and Desktops データソースのユーザーイベントを SIEM に送信しています。

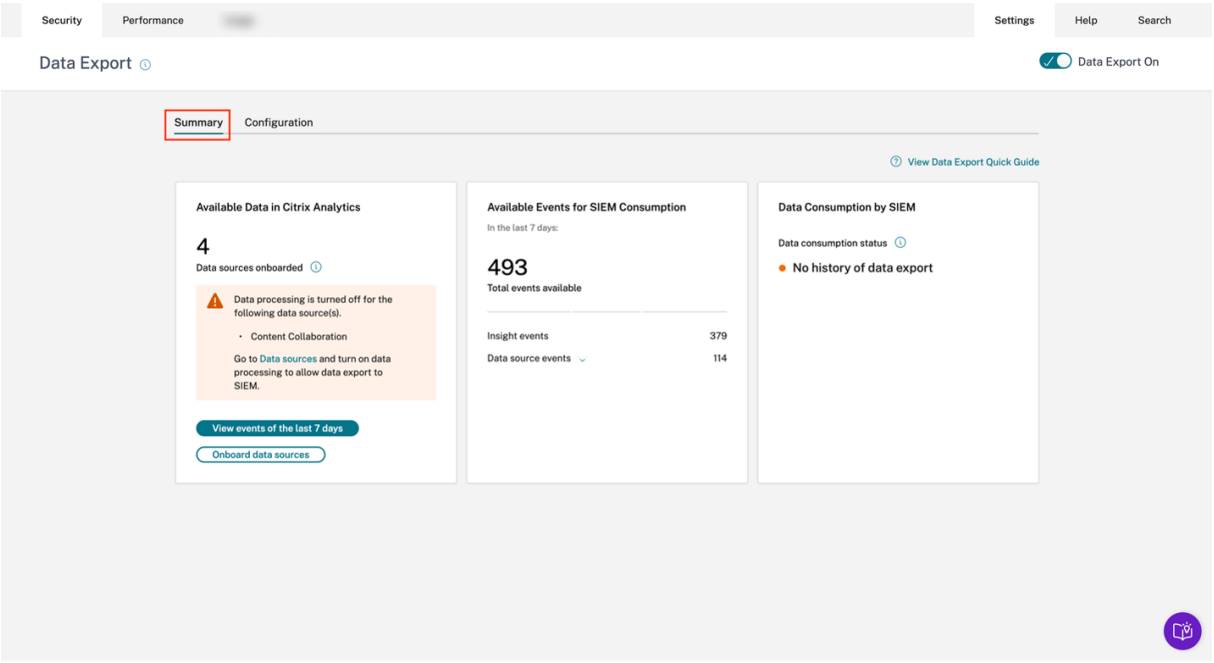
利用可能なイベントタイプ、メタデータ、スキーマについては、「データソースイベント」を参照してください。

> 注
>
> Logstash データブローカーを使用しているお客様は、最新の構成ファイルを Citrix Analytics for Security ポータルからダウンロードし 、Logstash サービスの展開時に更新することをお勧めします。これにより、正しいデータソースイベントテーブルが作成され、イベントが SIEM インデックスで使用できるようになります。



SIEM 統合のトラブルシューティング

セキュリティ用データエクスポートビューには、管理者が SIEM と Citrix **Analytics** 統合のトラブルシューティングに役立つサマリータブが含まれています。概要ダッシュボードでは、トラブルシューティングプロセスに役立つチェックポイントを通すことで、データの状態とフローを可視化できます。



この機能の詳細については、「データエクスポートのトラブルシューティング」を参照してください。

Splunk 統合

November 26, 2023

Citrix Analytics for Security を Splunk と統合すると、ユーザーのデータを Citrix IT 環境から Splunk にエクスポートして相互に関連付けることができ 、組織のセキュリティ体制についてより深い洞察を得ることができます。

統合の利点と、SIEM に送信される処理済みデータの種類の詳細については、セキュリティ情報とイベント管理の統合を参照してください。

Splunk の導入方法論を包括的に理解し、効果的な計画を行うための戦略を採用するには、Splunk でホストされている Citrix
Analytics アプリケーションを含む Splunk アーキテクチャのドキュメントを参照してください 。

セキュリティのための **Citrix Analytics** と **Splunk** の統合

Citrix Analytics for Security と Splunk を統合するには、前述のガイドラインに従ってください。

- データのエクスポート。Citrix Analytics for Security は、Kafka チャネルを作成し、リスクインサイトとデータソースイベントをエクスポートします。Splunk は、チャネルからこのリスクインテリジェンスを取得します。

- Citrix Analytics 構成を取得します。認証用の事前定義されたアカウントのパスワードを作成します。セキュリティ向け Citrix Analytics は、Splunk の Citrix Analytics アドオンを構成するために必要な構成ファイルを準備します。
- Splunk 用 Citrix Analytics アドオンをダウンロードしてインストールします。Splunkbase または Splunk Cloud のいずれかを使用して **Splunk** 用 **Citrix Analytics** アドオンをダウンロードし、インストールプロセスを完了してください。
- Splunk 用の Citrix Analytics アドオンを構成します。セキュリティ向け Citrix Analytics が提供する構成の詳細を使用してデータ入力を設定し、Splunk 用の Citrix Analytics アドオンを構成します。

Citrix Analytics 構成ファイルが準備されたら、以下を参照してください。

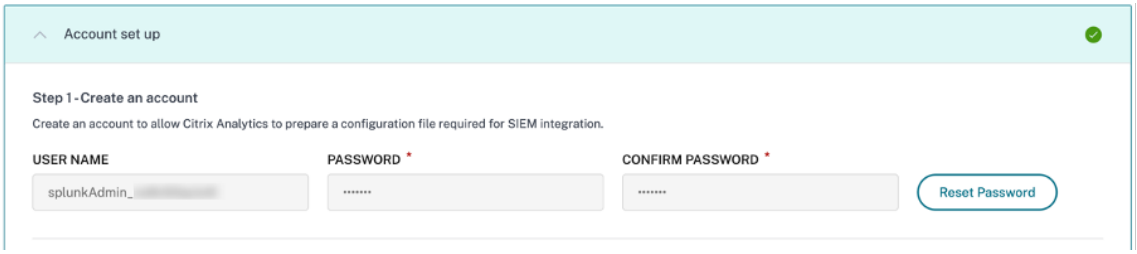
- パスワードリセット機能
- データ伝送をオンまたはオフにする

Splunk 用の Citrix Analytics アドオンを構成したら、以下を参照してください。

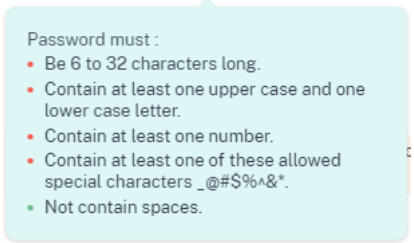
- Splunk 環境でのイベントの利用方法
- Splunk 用に Citrix Analytics アプリを構成する方法

データのエクスポート

1. **[設定] > [**** データエクスポート]** に移動します。
2. アカウント設定セクションで、ユーザー名とパスワードを指定してアカウントを作成します。このアカウントは、統合に必要な設定ファイルの準備に使用されます。

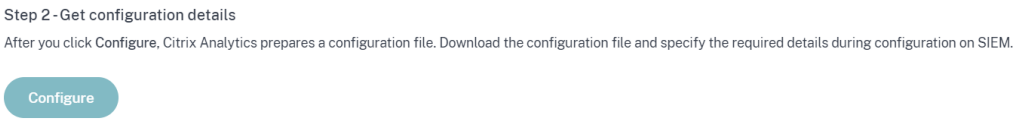


3. パスワードが次の条件を満たしていることを確認します。



4. [構成] を選択します。

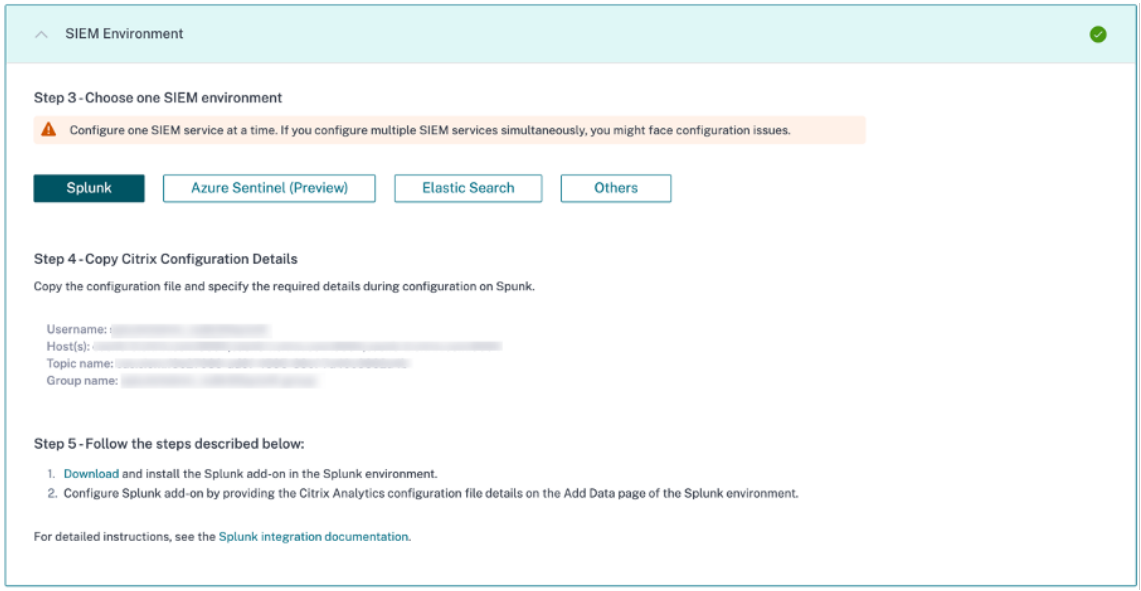
   Citrix Analytics for Security は、Splunk の統合に必要な構成の詳細を準備します。



5. [**Splunk**] を選択します。
6. ユーザー名、ホスト、Kafka トピック名、グループ名などの設定の詳細をコピーします。

   以降の手順で SSplunk 用 Citrix Analytics アドオンを構成するには、これらの詳細が必要です。

   > 重要
   >
   > これらの情報は機密情報であるため、安全な場所に保存する必要があります。

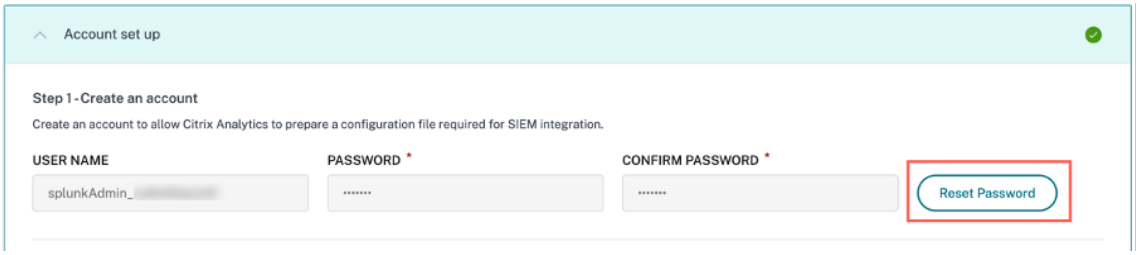


Splunk Integration の候補データを生成するには、
少なくとも 1 つのデータソースのデータ処理をオンにするか、テストイベント生成機能を使用してください。Citrix Analytics
for Security が Splunk の統合プロセスを開始するのに役立ちます。

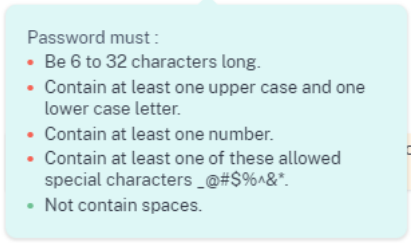
パスワードリセット機能

Citrix Analytics for Security で構成パスワードをリセットする場合は、次の手順に従います。

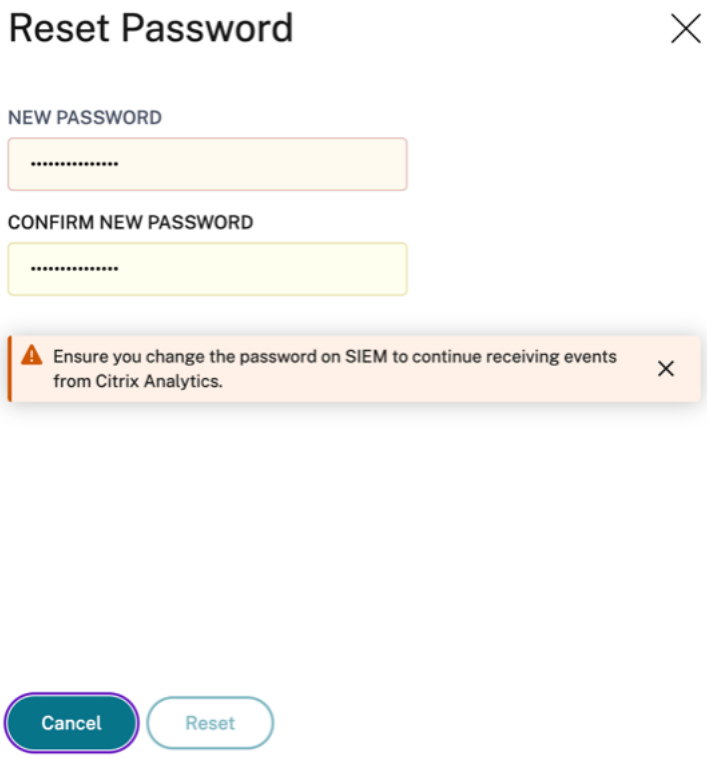
1. アカウント設定ページで、「パスワードのリセット」をクリックします。



2. ［パスワードのリセット］ウィンドウで、［新しいパスワード］フィールドと［新しいパスワードの確認］フィールドに、更新されたパスワードを指定します。表示されるパスワードルールに従います。



3. [リセット] をクリックします。設定ファイルの準備が開始されます。



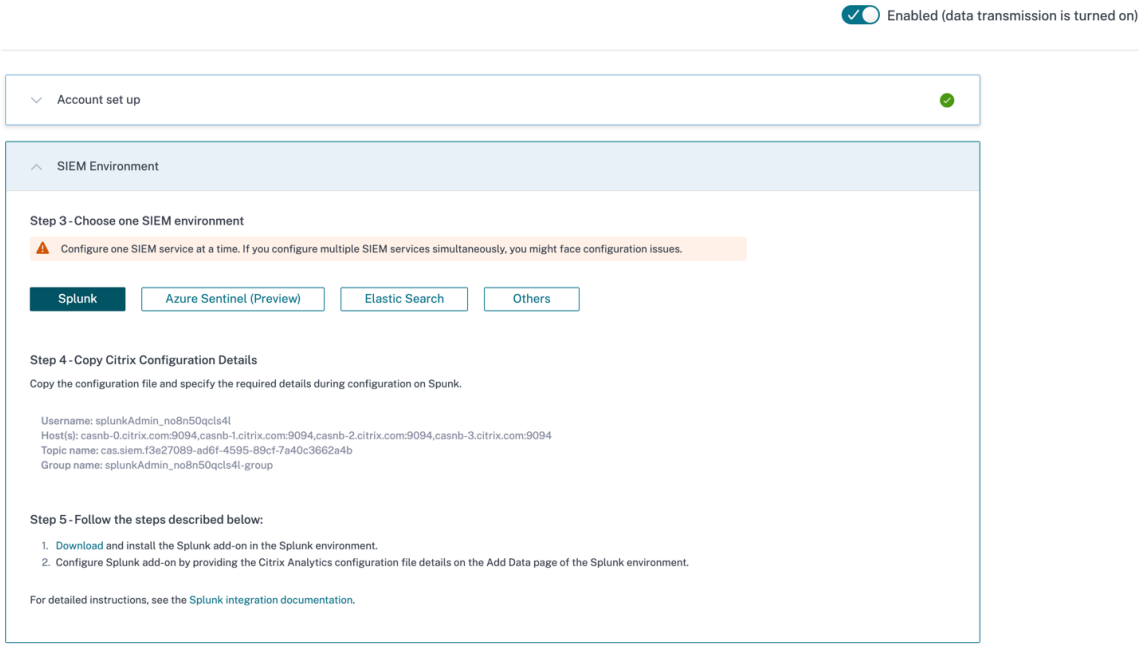
> 注:
>
> 設定パスワードをリセットしたら、Splunk 環境の **[Add Data]** ページでデータ入力を設定するときに、必ず新しいパスワードを更新してください。Citrix Analytics for Security は、Splunk にデータを送信し続けるのに役立ちます。

データ伝送をオンまたはオフにする

Citrix Analytics からの Splunk データエクスポートのデータ転送は、デフォルトでオンになっています。

セキュリティ向け Citrix Analytics からのデータの送信を停止するには:

1. **[設定] > [データエクスポート]** に移動します。
2. トグルボタンをオフにしてデータ転送を無効にします。



データ転送を再度有効にするには、トグルボタンをオンにします。

Splunk 向け Citrix Analytics アドオン

アドオンアプリケーションは次のいずれかのプラットフォームにインストールできます。

- Splunk エンタープライズ (ヘビーフォワーダー)
- Splunk Cloud

Splunk 向け Citrix Analytics アドオン（オンプレミス/エンタープライズ）

サポートされるバージョン

Citrix Analytics for Security は、次のオペレーティングシステムで Splunk 統合をサポートしています。

- CentOS Linux 7 以降
- Debian GNU/Linux 10.0 以降

- Red Hat エンタープライズ Linux サーバー 7.0 以降
- Ubuntu 18.04 LTS 以降

> 注
>
> - Citrix では、
>   前述のオペレーティングシステムの最新バージョンまたは各ベンダーのサポートを受けているバージョンを使用することをお勧めします。
> - Linux カーネル (64 ビット) オペレーティングシステムの場合は、Splunk
>   がサポートしているカーネルバージョンを使用してください。詳細については、Splunk のドキュメントを参照してください。

当社の Splunk インテグレーションは、Splunk 8.1
(64 ビット) 以降の Splunk バージョンで設定できます。

前提条件

- **Splunk** 用の **Citrix Analytics** アドオンは、セキュリティ向け Citrix Analytics の以下のエンドポイントに接続します。エンドポイントがネットワークの許可リストに含まれていることを確認します。

エンドポイント	米国リージョン	欧州連合地域	アジア太平洋南部リージョン
Kafka ブローカー	casnb-0.citrix.com:9094 casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-0.citrix.com:9094 casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-0.citrix.com:9094 casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

> 注:
>
> IP アドレスではなくエンドポイント名を使用してみてください。エンドポイントのパブリック IP アドレスは変更される可能性があります。

Splunk 用 **Citrix Analytics** アドオンをダウンロードしてインストールする

アドオンは、「ファイルからアプリをインストール」を使用してインストールするか、
Splunk 環境内からインストールするかを選択できます。

ファイルからアプリをインストールする

1. Splunkbaseに移動
2. Splunk 用 Citrix Analytics アドオンファイルをダウンロードします。
3. Splunk Web ホームページで、[アプリ] の横にある歯車アイコンをクリックします。
4. [ファイルからアプリをインストール] をクリックします。
5. ダウンロードしたファイルを探し、[アップロード] をクリックします。

   > メモ
   >
   > - 古いバージョンのアドオンを使用している場合は、[アプリのアップグレード] を選択して上書きします。
   > - **Citrix Analytics Splunk for Splunk** を **2.0.0** より前のバージョンからアップグレードする場合は、アドオンインストールフォルダーの */bin* フォルダー内にある以下のファイルとフォルダーを削除し、Splunk Forwarder または Splunk スタンドアロン環境を再起動する必要があります。
   >
   > ```
   > - cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin
   > - rm -rf splunklib
   > - rm -rf mac
   > - rm -rf linux_x64
   > - rm CARoot.pem
   > - rm certificate.pem
   > ```

6. アプリが **[アプリ]** リストに表示されていることを確認します。

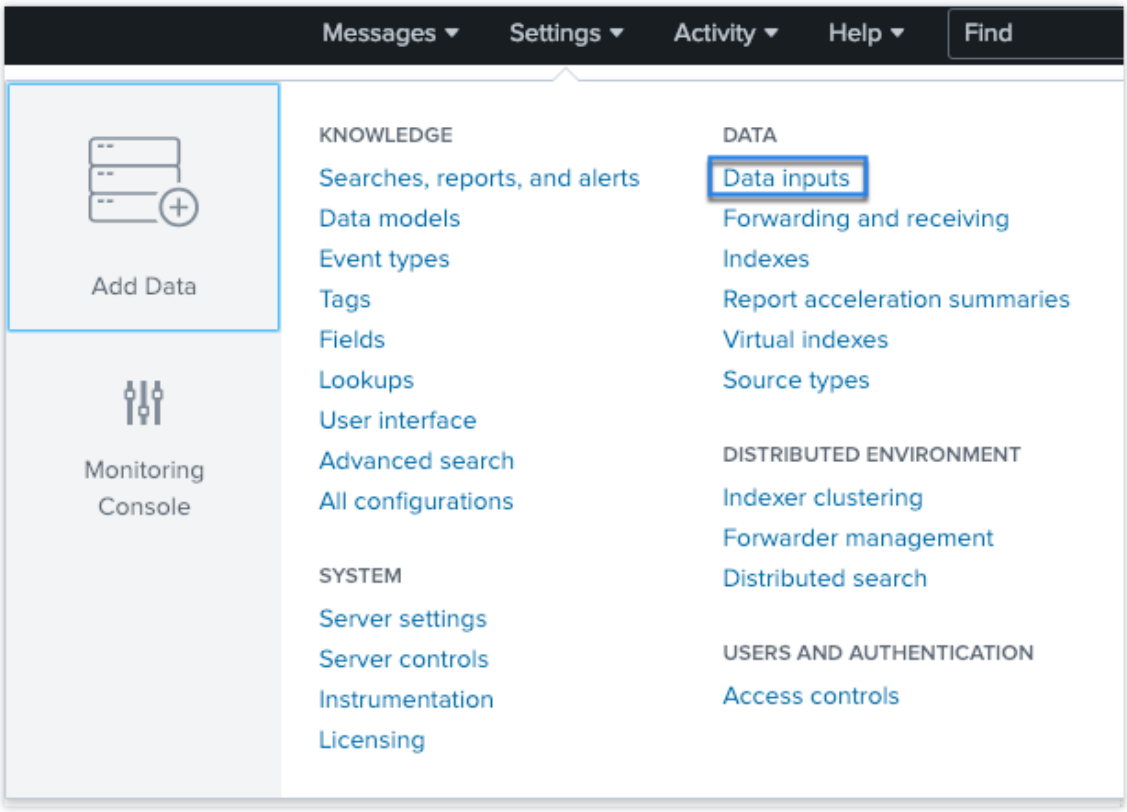
Splunk 内からアプリをインストールする

1. Splunk Web ホームページから、[**+** その他のアプリを検索] をクリックします。
2. ［その他のアプリの参照］ページで、［**Splunk**］の［**Citrix Analytics** アドオン］を検索します。
3. アプリの横にある [インストール] をクリックします。
4. アプリが **[アプリ]** リストに表示されていることを確認します。

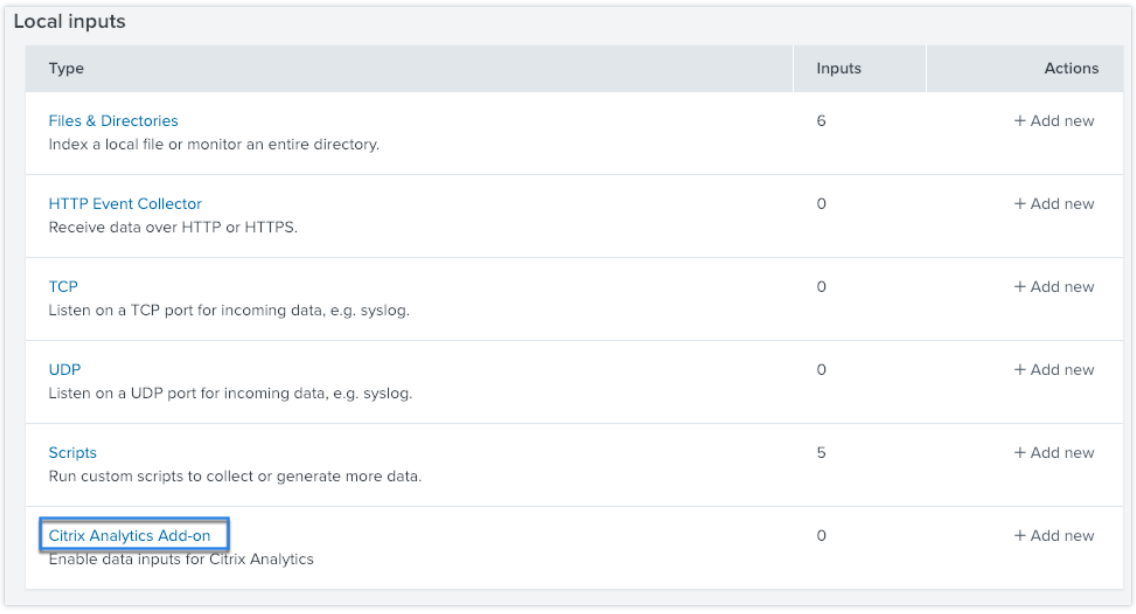
Splunk 用の **Citrix Analytics** アドオンを構成する

Citrix Analytics for Security が提供する構成の詳細を使用して、Splunk の Citrix Analytics アドオンを構成します。アドオンが正常に構成されると、Splunk は Citrix Analytics for Security からイベントの消費を開始します。

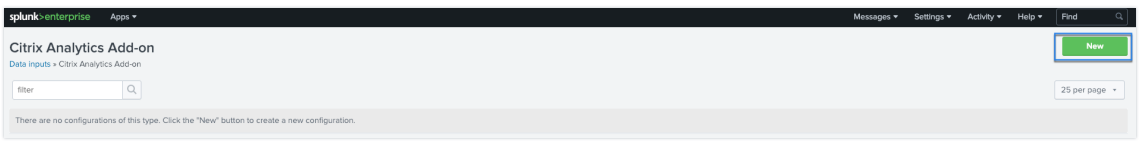
1. Splunk のホームページで、[設定**] > [**データ入力] の順に選択します。



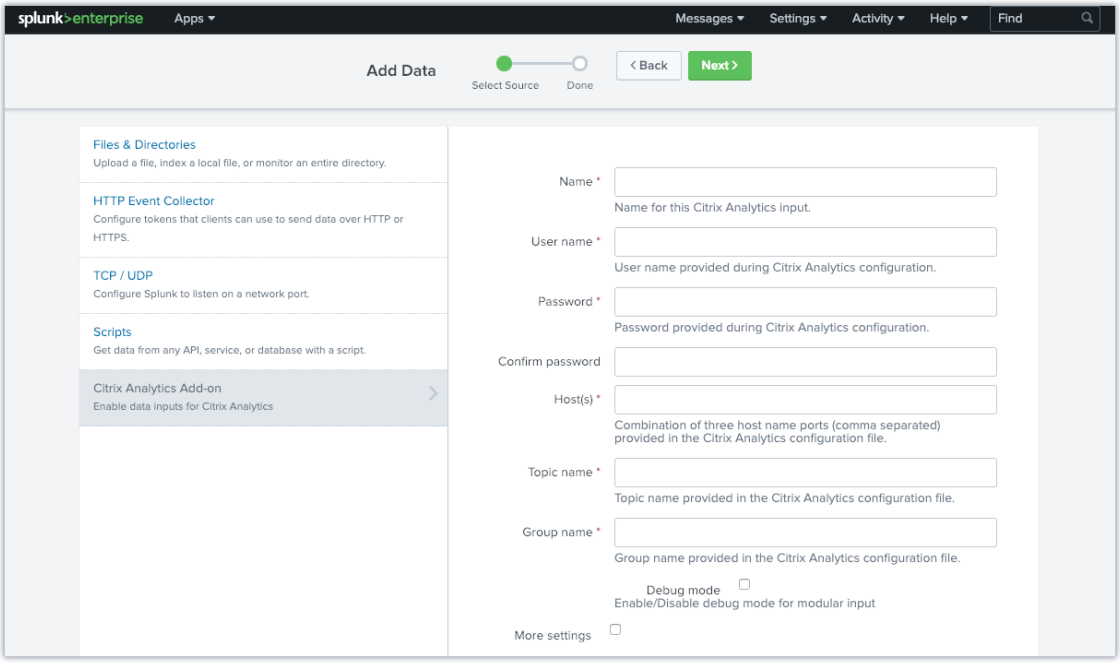
2. ［ローカル入力］セクションで、［**Citrix Analytics** アドオン］をクリックします。



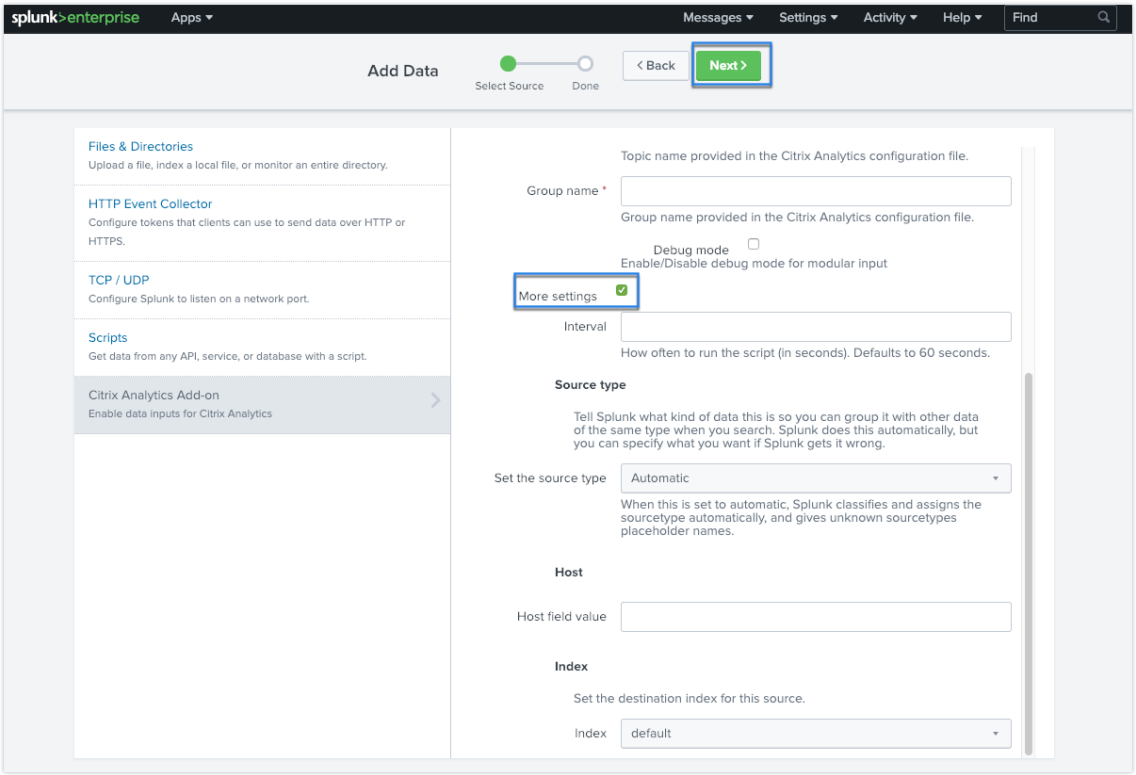
3. ［**New**］をクリックします。



4. ［データの追加］ページで、Citrix Analytics 構成ファイルに記載されている詳細を入力します。



5. デフォルト設定をカスタマイズするには、[詳細設定] をクリックしてデータ入力を設定します。独自の Splunk インデックス、ホスト名、ソースタイプを定義できます。



6. ［次へ］をクリックします。Citrix Analytics データ入力が作成され、Splunk 用の Citrix Analytics アドオン

が正常に構成されました。

Splunk 向け Citrix Analytics アドオン (クラウド)

Splunk インテグレーションは、次の Splunk バージョン (Splunk 8.1 以降) で設定できます。

前提条件

Splunk 向け Citrix Analytics アドオンは、次の IP とアウトバウンドポートに接続して、セキュリティ向け Citrix 分析に接続します。次の IP と送信ポート（Citrix Cloud の地域によって異なります）がネットワークの許可リストに含まれていることを確認してください。これらの IP と送信ポートを構成するには、「管理構成サービス（**ACS**）を使用して **Citrix Analytics IP** と送信ポートを **Splunk Cloud** 許可リストに追加する」セクションを参照してください。

米国リージョン	IP	アウトバウンドポート	欧州連合地域	IP	アウトバウンドポート	アジア太平洋南部リージョン	IP	アウトバウンドポート
casnb-0 Citrix ドットコム	20.242.21.84	9094	casnb-eu-0 Citrix.com	20.229.150.91	9094	casnb-aps-0 citrix.com	20.211.0.219	9094
casnb-1.citrix.com	20.98.232.69	9094	casnb-eu-1.citrix.com	20.107.97.59	9094	casnb-aps-1 citrix.com	20.211.38.102	9094
casnb-2.citrix.com	20.242.21.108	9094	casnb-eu-2.citrix.com	51.124.223.102	9094	casnb-aps-2 citrix.com	20.211.36.180	9094
casnb-3.citrix.com	20.242.57.14	9094						

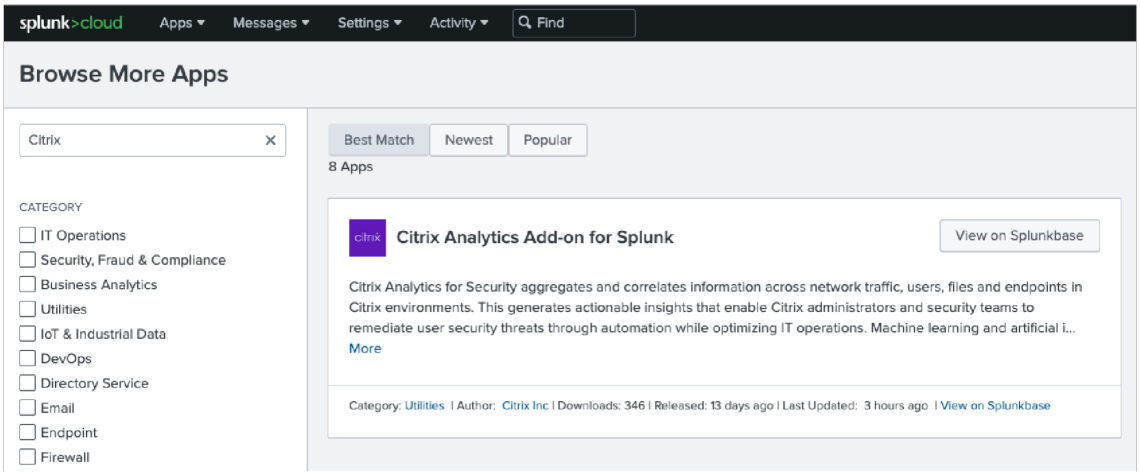
> 注:
>
> これらの IP はローテーションの対象となります。上記のように、IP 許可リストが最新の IP で更新されていることを確認してください。

管理者構成サービス（**ACS**）を使用して **Citrix Analytics IP** とアウトバウンドポートを **Splunk Cloud** の許可リストに追加する

1. Citrix Cloud の地域によっては、IP をゼロインで許可リストに追加する必要があります。
2. Splunk クラウドプラットフォームで管理設定サービス (ACS) を有効にします。
3. 管理者権限を持つローカルアカウントを使用して、許可リストのトークンを作成します。
4. cURL GET および POST コマンドを実行して 、サブネットをそれぞれのポートの許可リストに追加し、正常に追加されたかどうかを検証します。
5. cURL の GET および POST コマンドを実行して 、送信ポートを許可リストに追加し、正常に追加されたかどうかを確認します。

Splunk 用 **Citrix Analytics** アドオンをダウンロードしてインストールする

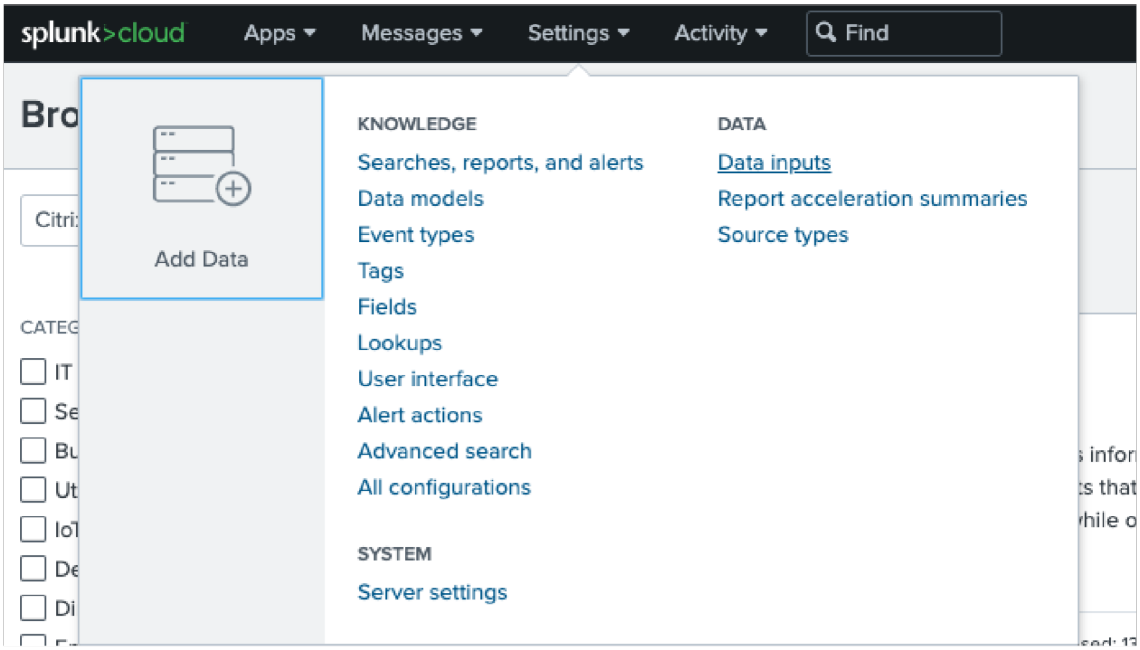
1. [アプリ] **>** [その他のアプリを探す] **>** [**Splunk** 向け **Citrix Analytics** アドオンを検索する] に移動します。



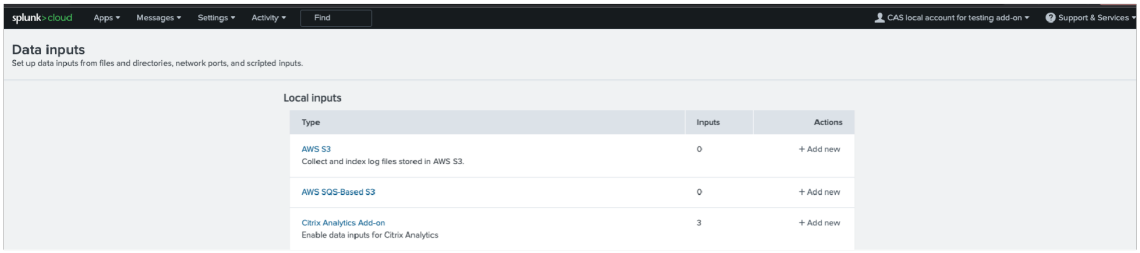
2. アプリをインストールします。
3. アプリが [アプリ] リストに表示されていることを確認します。

Splunk 用の **Citrix Analytics** アドオンを構成する

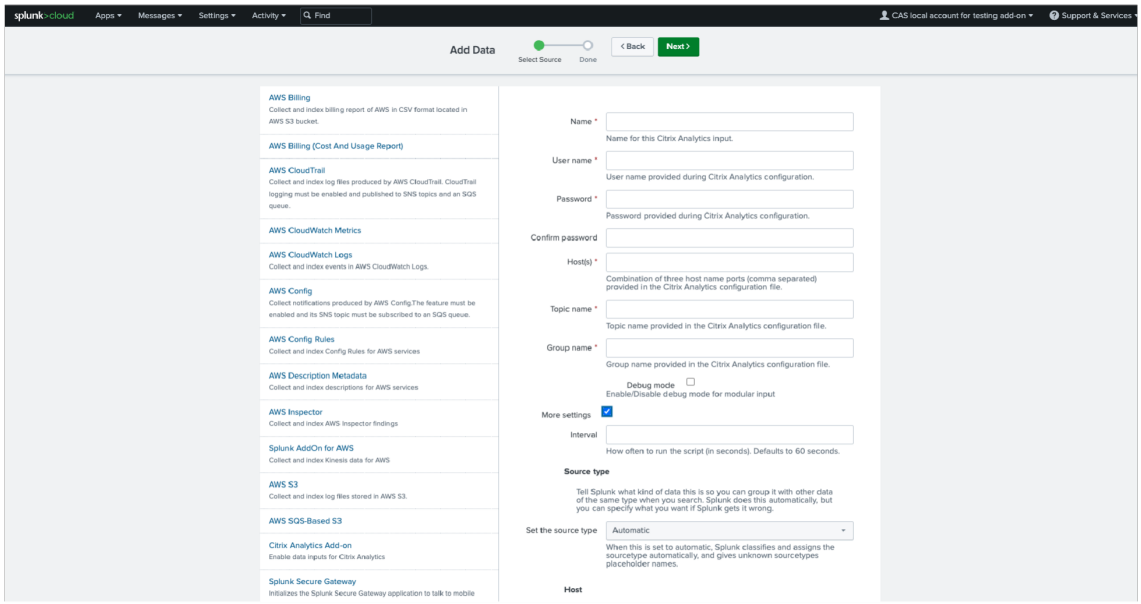
1. [設定] **>** [データ入力] **>** [**Citrix Analytics** アドオン] に移動します。



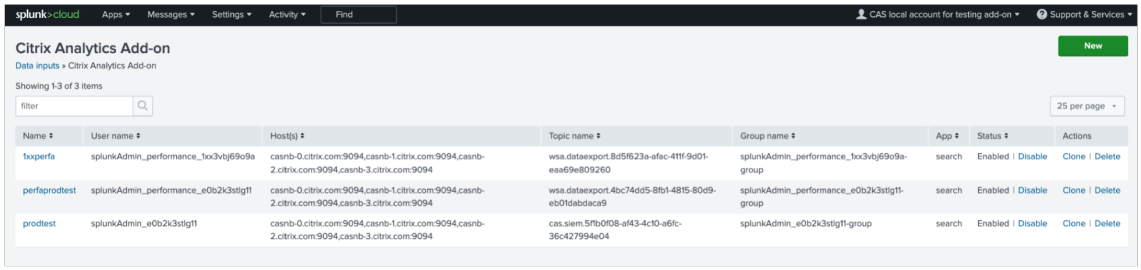
入力を追加:Splunk インテグレーション	Citrix Analytics for Security。［新規追加］をクリックします。

2. 

3. **Citrix Analytics** データエクスポートページで構成された詳細を入力して、データ入力を構成します。



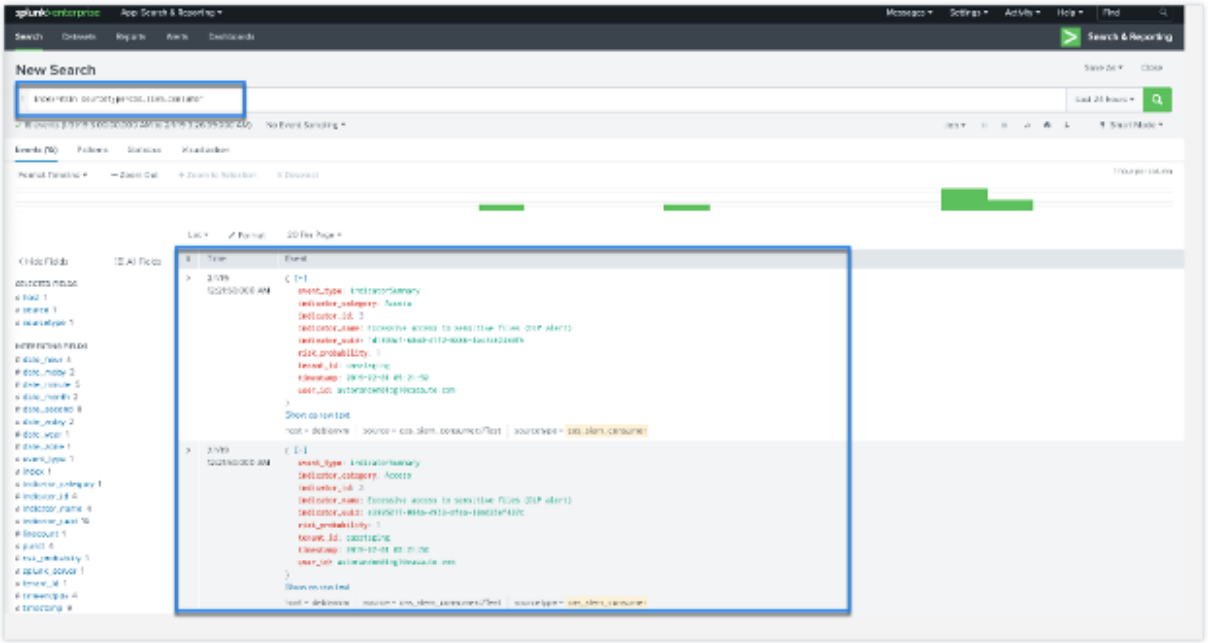
4. データ入力が正常に追加されたかどうかを確認してください。



Splunk 環境でイベントを利用する方法

アドオンの構成後、Splunk はセキュリティ向け Citrix Analytics からリスクインテリジェンスの取得を開始します。設定済みのデータ入力に基づいて Splunk 検索ヘッドから組織のイベントを検索することができます。

検索結果は次の形式で表示されます。



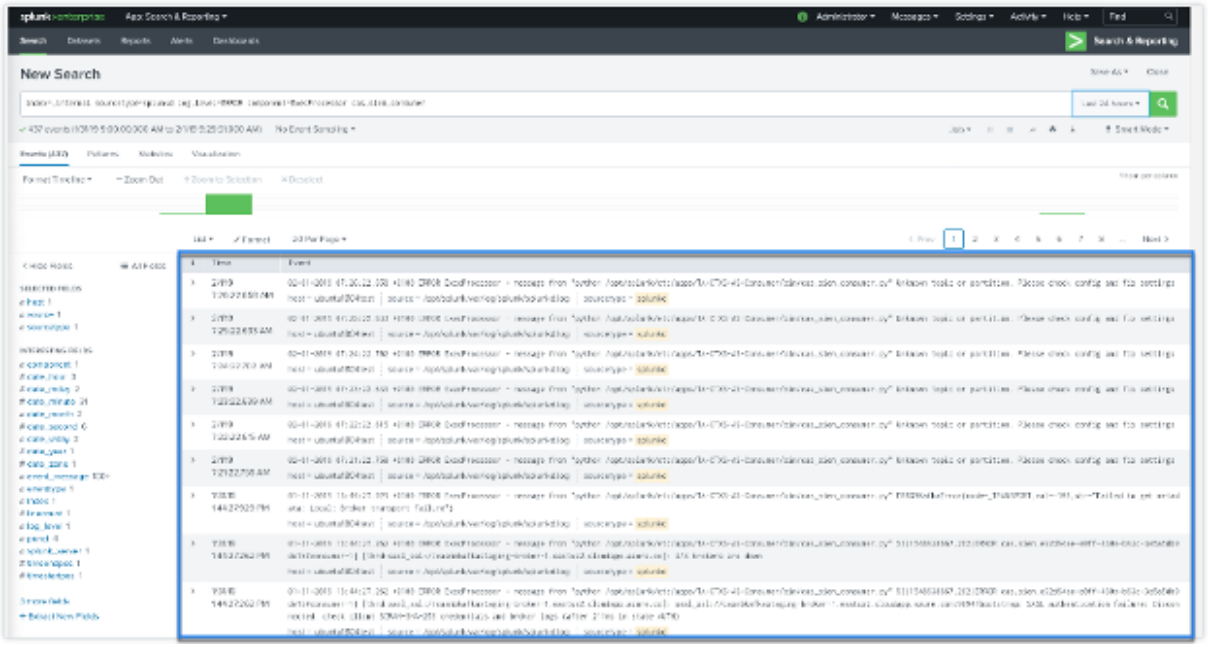
出力例:

```
{"event_type": "indicatorSummary", "indicator_category": "Access",
"indicator_id": 200, "indicator_name": "Jailbroken / Rooted Device
Detected", "indicator_uuid": "1b97c3be-0000-000-0000-0000000000",
"risk_probability": 1.0, "tenant_id": "notcloud", "timestamp": "2017-11-16
23:59:59", "user_id": "testuser00001"}
```

アドオンの問題を検索してデバッグするには、次の検索クエリを使用します。

```
index=_internal sourcetype=splunkd log_level=ERROR component=ExecProcessor
cas_siem_consumer
```

結果は次の形式で表示されます。



データ形式について詳しくは、「SIEM 用の Citrix Analytics データ形式」を参照してください。

Splunk 用 Citrix Analytics アドオンのトラブルシューティング

Splunk ダッシュボードにデータが表示されない場合や、Splunk 用の Citrix Analytics アドオンの構成中に問題が発生した場合は、デバッグ手順を実行して問題を修正します。詳しくは、「Splunk 用 Citrix Analytics アドオンの構成に関する問題」を参照してください。

> 注
>
> < CAS-PM-Ext@cloud.com >Splunk の統合、Splunk へのデータのエクスポート、またはフィードバックの提供に関するサポートをリクエストするには、お問い合わせください。

Splunk 向け Citrix Analytics アプリ

> 注
>
> このアプリはプレビュー版です。

Splunk 向けの Citrix Analytics アプリを使用すると、Splunk エンタープライズ管理者は、セキュリティ向け Citrix Analytics から収集されたユーザーデータを、Splunk 上の洞察力に富んだ実用的なダッシュボードの形式で表示できます。これらのダッシュボードを使用すると、組織内のユーザーのリスクの高い行動を詳細に把握し、内部からの脅威を軽減するためにタイムリーな措置を講じることができます。また、セキュリティ向け Citrix Analytics から収集されたデータを、Splunk で構成された他のデータソースと関連付けることもできます。この相関関係により、複数のソースからのユーザーの危険なアクティビティを可視化し、IT 環境を保護するための対策を講じることができます。

サポートされている **Splunk** バージョン

Splunk 向け Citrix Analytics アプリは、次のバージョンの Splunk で実行されます。

- Splunk 9.0 64 ビット
- Splunk 8.2 64 ビット
- Splunk 8.1 64 ビット

Splunk 用 **Citrix Analytics** アプリケーションの前提条件

- Splunk 用 Citrix Analytics アドオンをインストールします 。
- Splunk 用 Citrix Analytics アドオンの前提条件が既に満たされていることを確認します 。
- データがセキュリティ向け Citrix Analytics から Splunk に流れていることを確認します。

インストールと構成

アプリをインストールする場所はどこですか　Splunk 検索ヘッド

アプリをインストールして設定する方法は　Splunk 用 Citrix Analytics アプリをインストールするには、Splunkbase からダウンロードするか、Splunk 内からインストールします。

ファイルからアプリをインストールする

1. Splunkbaseに移動
2. Splunk 用 Citrix Analytics アプリファイルをダウンロードします。
3. Splunk Web ホームページで、[アプリ] の横にある歯車アイコンをクリックします。
4. [ファイルからアプリをインストール] をクリックします。
5. ダウンロードしたファイルを探し、[アップロード] をクリックします。

   > 注
   >
   > 古いバージョンのアプリを使用している場合は、[アプリのアップグレード] を選択して上書きします。

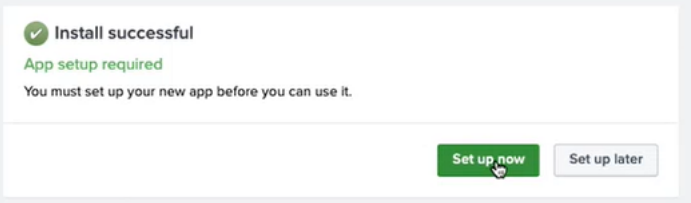
6. アプリが **[**アプリ**]** リストに表示されていることを確認します。

Splunk 内からアプリをインストールする

1. Splunk Web ホームページから、[**+** その他のアプリを検索] をクリックします。
2. ［その他のアプリの参照］ページで、**Citrix Analytics** アプリで **Splunk** を検索します。
3. アプリの横にある [インストール] をクリックします。

インデックスとソースタイプを設定してデータを関連付ける

1. アプリをインストールしたら、[今すぐ設定] をクリックします。

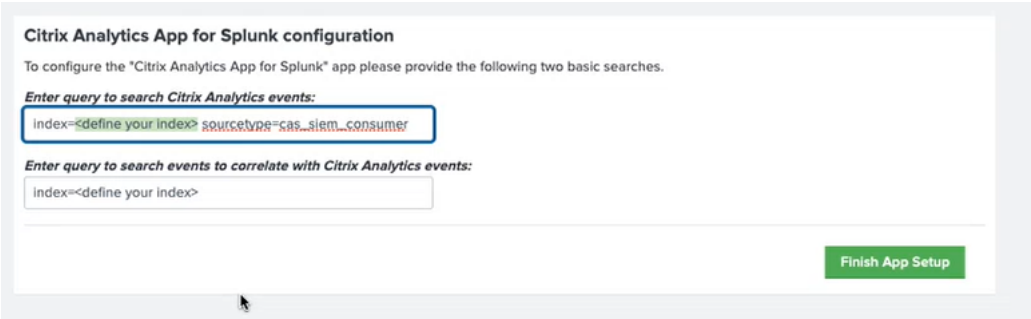


2. 次のクエリを入力します。

   - Citrix Analytics for Security のデータが保存されるインデックスとソースタイプ。

     > 注
     >
     > これらのクエリ値は、Splunk の Citrix Analytics アドオンで指定されている値と同じである必要があります。詳しくは、「Splunk 用の Citrix Analytics アドオンを構成する」を参照してください。

   - データとセキュリティ向け Citrix Analytics を関連付けるインデックスです。



3. [アプリのセットアップを終了] をクリックして、構成を完了します。

SSplunk 用の Citrix Analytics アプリを構成してセットアップしたら、Citrix Analytics ダッシュボードを使用して 、SSplunk のユーザーイベントを表示します。

Splunk 統合の詳細については、次のリンクを参照してください。

- Citrix Analytics と Splunk の
- Splunk 用の Citrix Analytics アプリ、Splunkbase に登場

Citrix Analytics のアドオンアプリケーションを使用した **Splunk** アーキテクチャ

February 14, 2023

Splunk は、次の 3 つの階層で構成されるアーキテクチャを採用しています。

- コレクション
- インデックス作成
- 検索中

Splunk は、データを簡単に Splunk に取り込むことができるさまざまなデータ収集メカニズムをサポートしています。これにより、データをインデックス化して検索できるようになります。この階層は、ヘビーフォワーダーまたはユニバーサルフォワーダーに他なりません。

アドオンアプリケーションは、ユニバーサルフォワーダーレイヤーではなくヘビーフォワーダーレイヤーにインストールする必要があります。なぜなら、よく構造化されたデータ (json、csv、tsv など) を除いて、ユニバーサルフォワーダーはログソースを解析してイベントを生成しないため、ログの形式を理解する必要があるアクションを実行できないためです。

また、Python の簡略化されたバージョンも付属しているため、機能するために Splunk スタック全体を必要とするモジュラー入力アプリケーションとは互換性がありません。ヘビーフォワーダーはコレクション階層に他なりません。

ユニバーサルフォワーダーとヘビーフォワーダーの主な違いは、ヘビーフォワーダーには完全な解析パイプラインが含まれており、実際にディスクにイベントを書き込んだりインデックスしたりしなくても、インデクサーが実行するのと同じ機能を実行することです。これにより、ヘビーフォワーダーは、データのマスキング、フィルタリング、イベントデータに基づくルーティングなどの個々のイベントを理解して処理できます。アドオンアプリケーションには Splunk Enterprise が完全にインストールされているため、適切なデータ収集のために完全な Python スタックを必要とするモジュラー入力をホストすることも、Splunk HTTP イベントコレクター（HEC）のエンドポイントとして機能させることもできます。

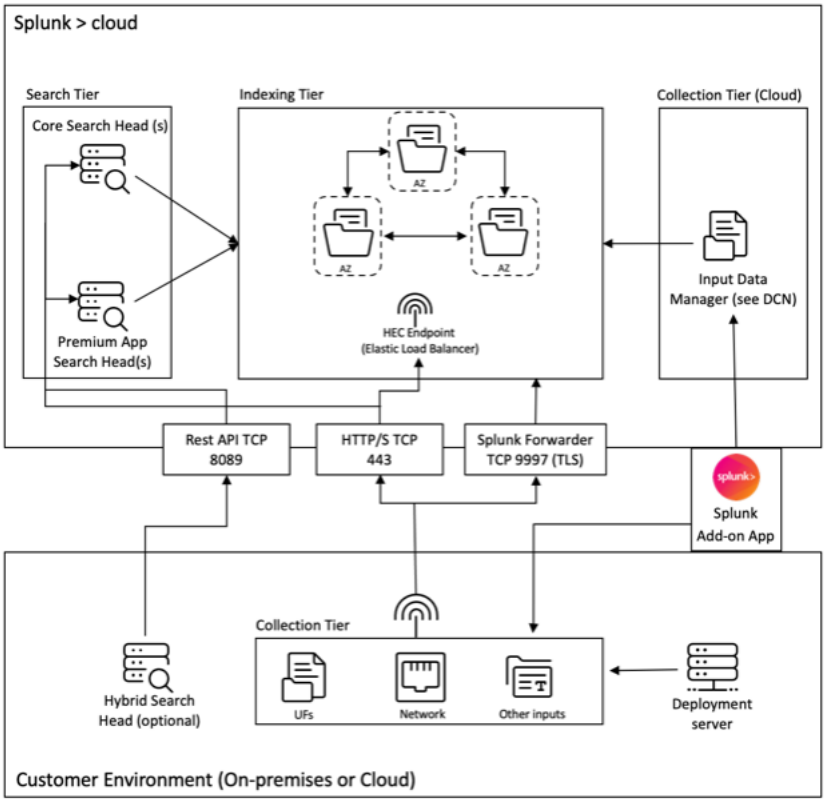
データが収集されると、インデックス化または処理され、検索可能な方法で保存されます。

顧客がデータを探索する主な方法は検索です。検索はレポートとして保存し、ダッシュボードパネルに追加できます。検索は、データから情報を抽出したものです。

一般に、Splunk アドオンアプリケーションはコレクション層（Splunk エンタープライズレベル）にデプロイされ、ダッシュボードアプリケーションは検索レイヤー（Splunk Cloud レベル）にデプロイされます。シンプルなオンプレミス設定では、これら 3 つの階層すべてを 1 台の Splunk ホストに配置できます (シングルサーバーデプロイメントと呼ばれます)。

Splunk のアドオンアプリケーションを使用するには、コレクション階層の方がはるかに優れています。アドオンアプリケーションをインストールするには 2 つの方法があります。お客様の環境のコレクション階層にインストールすることも、**Splunk Cloud** インスタンスの入力データマネージャーにインストールすることもできます。

アドオンアプリケーションでの Splunk の導入アーキテクチャを理解するには、次の図を参照してください。



前述の図に示されている入力データマネージャー (IDM) は、Splunk Cloud が管理するデータ収集ノード (DCN) の実装で、スクリプト入力とモジュラー入力のみをサポートします。それ以上のデータ収集が必要な場合は、Splunk ヘビーフォワーダーを使用して環境内に DCN をデプロイして管理できます。

Splunk では、さまざまなソースからデータを収集、インデックス化、検索できます。データを収集する 1 つの方法は、Splunk が他のシステムやアプリケーションに保存されているデータにアクセスできるようにする API を使用することです。これらの API には、クエリメカニズムとして REST、Web サービス、JMS、または JDBC を含めることができます。Splunk やサードパーティの開発者は、Splunk のモジュラー型入力フレームワークを通じて API インタラクションを可能にするさまざまなアプリケーションを提供しています。これらのアプリケーションを正しく機能させるには、通常、Splunk Enterprise ソフトウェアを完全にインストールする必要があります。

API によるデータ収集を容易にするために、ヘビーフォワーダーを DCN としてデプロイするのが一般的です。ヘビーフォワーダーは、完全な解析パイプラインを備えており、個々のイベントを理解して処理できるため、ユニバーサルフォワーダーよりも強力なエージェントです。これにより、API を使用してデータを収集し、Splunk インスタンスに転送してインデックス化する前に処理できます。

Splunk Cloud デプロイのアーキテクチャの概要について詳しくは、「Splunk 検証済みアーキテクチャ」を参照してください。

Splunk 向け Citrix Analytics ダッシュボード

December 7, 2023

> ** 注注意 **
>
> : シトリックスの Content Collaboration と ShareFile はサポート終了となり、ユーザーは使用できなくなります。
>
> この機能はプレビュー段階です。

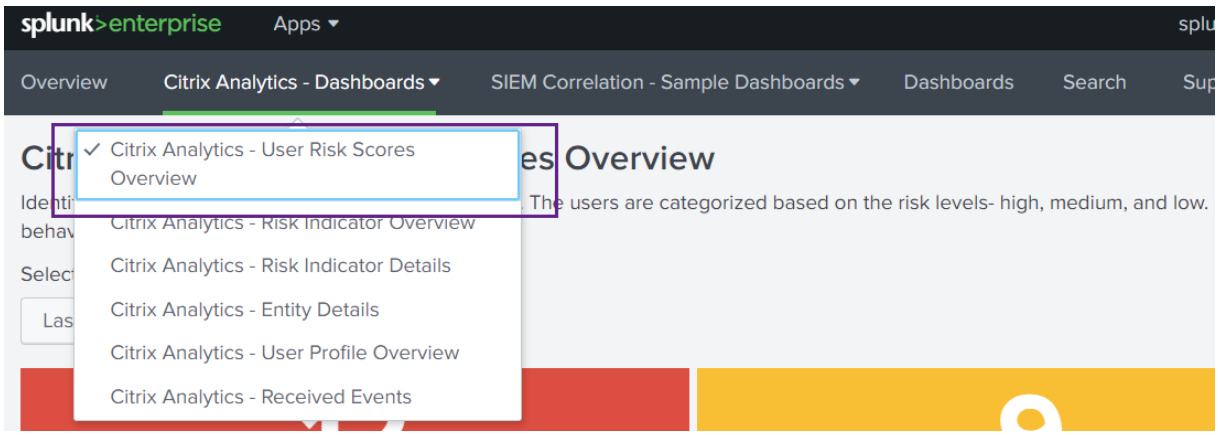
前提条件

次の Citrix Analytics ダッシュボードを使用するには、SSplunk 用の Citrix Analytics アプリが構成およびセットアップ済みであることを確認します。

ユーザーリスクスコアの概要

このダッシュボードには、組織内のリスクの高いユーザーの統合ビューが表示されます。ユーザーは、リスクレベル（高、中、低）によって分類されます。リスクレベルはユーザーアクティビティの異常に基づいており、したがってリスクスコアが割り当てられます。リスクの高いユーザーのタイプの詳細については、「ユーザー」ダッシュボードを参照してください。

このダッシュボードを表示するには、［**Citrix Analytics-**ダッシュボード］**>**［**Citrix Analytics-**ユーザーリスクスコアの概要］をクリックします。



プリセットされた時間範囲またはカスタムの時間範囲を選択して、危険なユーザーのタイムラインとその詳細を表示します。

Risky Users テーブルには、次の情報が表示されます。

- ユーザー: ユーザー名を示します。ユーザー名をクリックすると、［Citrix Analytics-エンティティの詳細］ダッシュボードでユーザーの危険な動作に関する詳細が表示されます。
- 侵害されたエンドポイントのリスクが見つかりました：侵害されたエンドポイントのリスクカテゴリに属するユーザーによってトリガーされたリスク指標の数を示します。
- 侵害されたユーザーのリスクが見つかりました：侵害されたユーザーのリスクカテゴリに属するユーザーによってトリガーされたリスク指標の数を示します。
- データ漏洩リスクが見つかりました：データ漏洩リスクカテゴリに属するユーザーによってトリガーされたリスク指標の数を示します。
- 内部脅威リスクが見つかりました: 内部脅威リスクカテゴリに属するユーザーによってトリガーされるリスク指標の数を示します。
- リスクスコア: ユーザーのリスクスコアを示します。

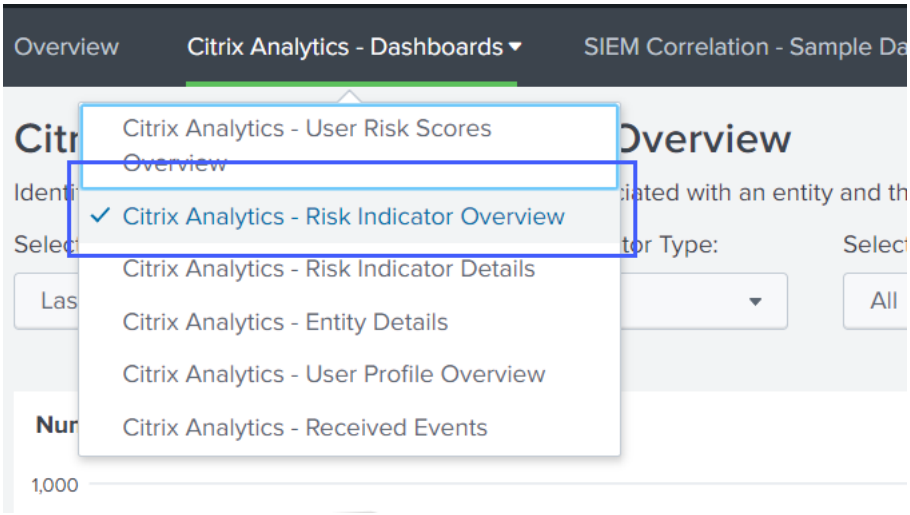
また、ユーザー名でユーザーを検索し、必要な詳細を取得することもできます。

詳細については、「リスクカテゴリ」を参照してください。

リスク指標の概要

ダッシュボードには、組織内のユーザーによってトリガーされたリスク指標の統合ビューが表示されます。

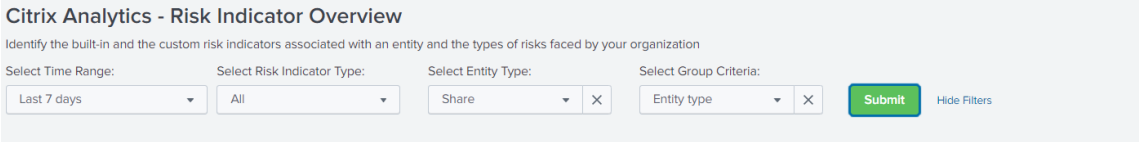
ダッシュボードを表示するには、[**Citrix Analytics**-ダッシュボード] **>** [**Citrix Analytics**-リスク指標の概要] をクリックします。



レポートを表示するカテゴリを選択

1 つ以上のカテゴリを選択して、リスク指標を検索します。

- 時間範囲: 事前設定された時間範囲またはカスタム時間範囲を選択して、その期間のトリガーされたリスク指標を表示します。
- リスク指標の種類: リスク指標の種類として、組み込みまたはカスタムを選択します。
- エンティティタイプ: ユーザーを選択すると、関連するリスク指標が表示されます。
- グループ: データソース、指標カテゴリ、指標名、指標タイプ、またはエンティティタイプ別にユーザーイベントをグループ化し、関連するリスク指標を表示するための条件を選択します。

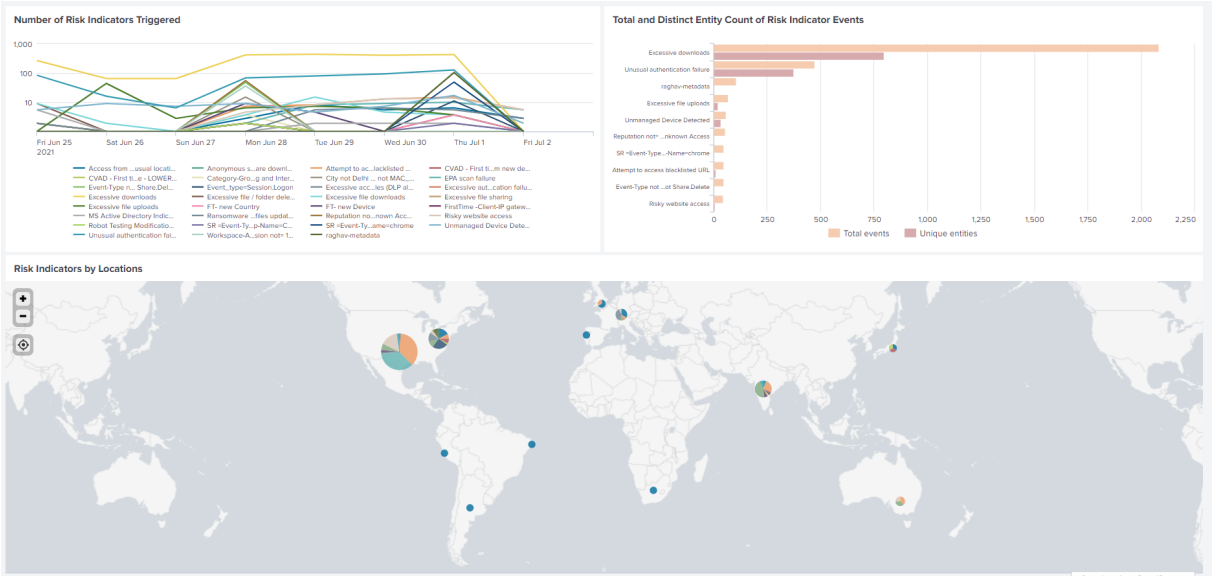


レポートを表示

次のレポートを使用して、1 つ以上のカテゴリを選択してリスク指標の詳細を表示します。

- トリガーされたリスク指標の数: 選択した期間にトリガーされたリスク指標の数が表示されます。このレポートを使用して、危険な活動のパターンと領域を特定します。また、組織内でリスクの高いアクティビティを特定します。

- リスク指標イベントの合計および個別エンティティ数**:** リスク指標に対応するイベントの合計と一意のイベントを表示します。このレポートを使用して、組織内の各リスク指標の発生状況と上位のリスク指標を特定します。また、特定のリスク指標をトリガーしたユニークユーザーの数を特定し、そのリスク指標がより大きなユーザーグループによってトリガーされたのか、より小さなユーザーグループによってトリガーされたのかを確認することもできます。
- 場所別のリスク指標**:** 場所間でユーザーによってトリガーされたリスク指標の数を表示します。このレポートを使用して、よりリスクの高い活動を示す事業所を特定し、事業所が組織の業務領域外にあるかどうかを確認します。
- リスク指標の詳細: 関連するデータソース、指標カテゴリ、指標の種類、発生回数など、リスク指標の詳細を表示します。



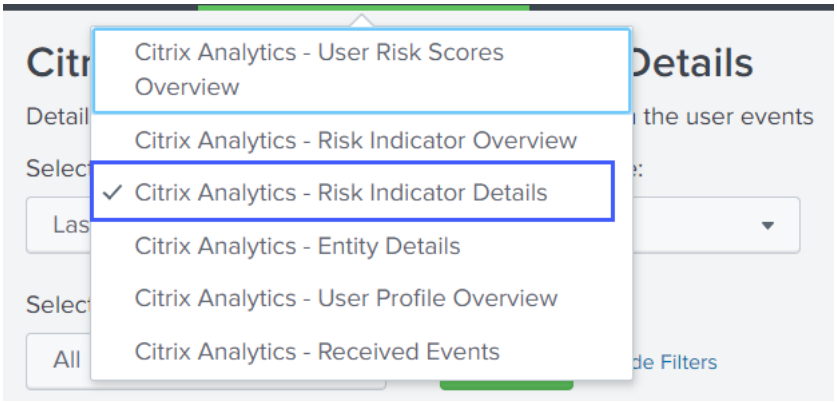
Risk Indicator Details

Data source	Indicator category	Indicator type	Indicator name	Number of Risk Indicator Events
Citrix Content Collaboration	Data exfiltration	builtin	Excessive downloads	2084
Citrix Content Collaboration	Compromised users	builtin	Unusual authentication failure	473
Citrix Virtual Apps and Desktops	Data exfiltration	custom	raghav-metadata	104
Citrix Content Collaboration	Insider threats	builtin	Excessive file uploads	68
Citrix Endpoint Management	Compromised endpoints	builtin	Unmanaged Device Detected	59
Citrix Access Control	Compromised users	custom	Reputation not= Clean Access AND Reputation not= Unknown Access	55
Citrix Virtual Apps and Desktops	Compromised users	custom	SR =Event-Type=Citrix.EventMonitor.AppStart AND App-Name=chrome	49
Citrix Access Control	Insider threats	builtin	Attempt to access blacklisted URL	48
Citrix Content Collaboration	Compromised users	custom	Event-Type not Share.Create AND Event-Type not Share.Delete	48
Citrix Access Control	Insider threats	builtin	Risky website access	44

リスク指標の詳細

ダッシュボードには、ユーザーによってトリガーされた組み込みおよびカスタムリスク指標に関する詳細情報が表示されます。詳しくは、「Citrix ユーザーリスク指標 」および「カスタムリスク指標」を参照してください。

ダッシュボードを表示するには、［**Citrix Analytics-**ダッシュボード］**>** ［**Citrix Analytics**］**-** ［リスク指標の詳細］をクリックします。



カテゴリを選択してレポートを表示します

1 つ以上のカテゴリを選択して、リスク指標の詳細を表示します。

- 時間範囲: 事前設定された時間範囲またはカスタム時間範囲を選択して、その期間のトリガーされたリスク指標の詳細を表示します。
- エンティティタイプ: ユーザーを選択すると、関連するリスク指標の詳細が表示されます。
- リスク指標タイプ-詳細を表示するには、組み込みまたはカスタムのリスク指標の種類を選択します。
- データソース-データソースを選択して、関連するリスク指標の詳細を表示します。
- リスク指標カテゴリ-関連するリスク指標の詳細を表示するには、リスクカテゴリを選択します。
- リスクインジケータ-詳細を表示するリスクインジケータを選択します。

レポートの表示

たとえば、[リスク指標の選択] リストから、[異常な認証失敗 (**Citrix Content Collaboration**)] を選択し、[送信] をクリックして、次の情報を表示します。

- リスク指標に関連する上位 10 人のユーザー
- 次のようなリスク指標の詳細
  - トリガーの日時
  - 関連付けられたデータソース
  - 関連リスクカテゴリ
  - 関連エンティティ ID とユーザーエンティティタイプ
  - リスクの重大度-高、中、低
  - ユーザーイベントのリスク確率

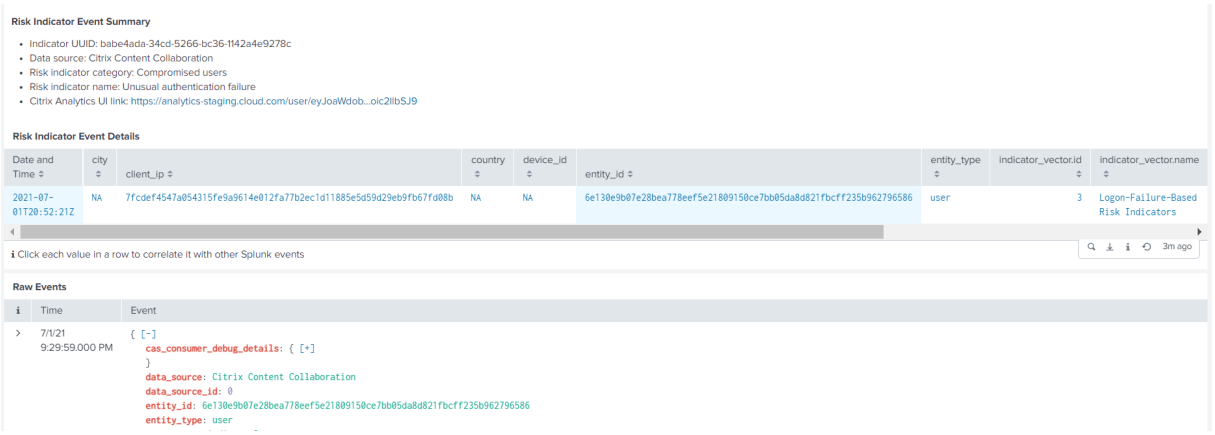
- リスク指標の一意のアイデンティティ (UUID)

「リスク指標別上位 **10** エンティティ」で、エンティティをクリックして、**Citrix Analytics-**エンティティの詳細ダッシュボードで詳細を表示します。

リスク指標詳細表の各行をクリックすると、選択したリスク指標のイベント概要、イベント詳細、および未処理イベントが表示されます。

[リスク指標イベントの概要] セクションで、[**Citrix Analytics UI**] リンクをクリックして、SSplunk からセキュリティのための Citrix Analytics のユーザータイムラインに直接移動します。ユーザータイムラインで、リスク指標、関連するイベント、およびユーザーに適用されたアクションを表示します。

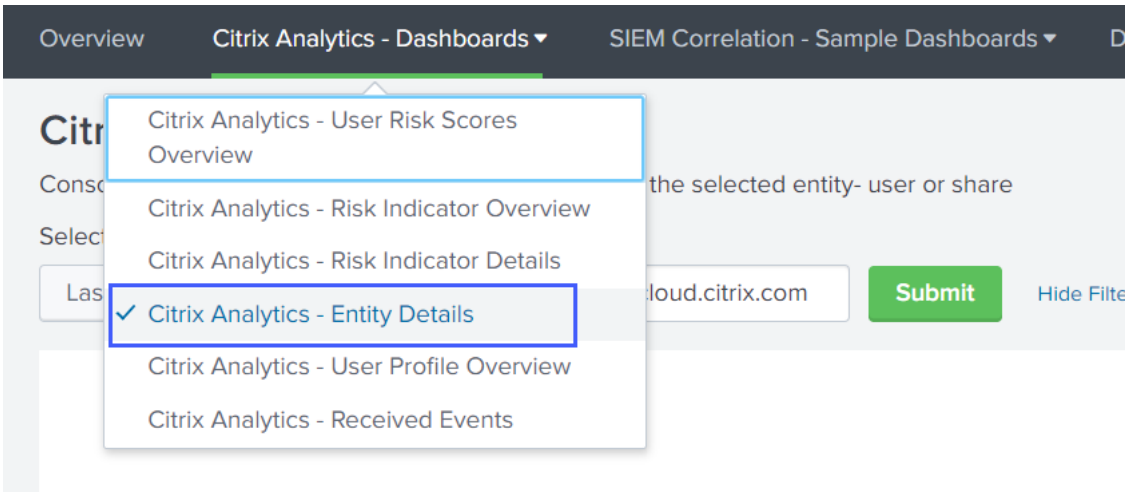
イベントの概要とイベントの詳細について詳しくは、「SIEM の Citrix Analytics データ形式」を参照してください。



エンティティの詳細

ダッシュボードを使用して、ユーザーエンティティユーザーとその危険な行動に関する詳細を表示します。

ダッシュボードを表示するには、[**Citrix Analytics**] **-** [ダッシュボード] **>** [**Citrix Analytics-**エンティティの詳細] をクリックします。

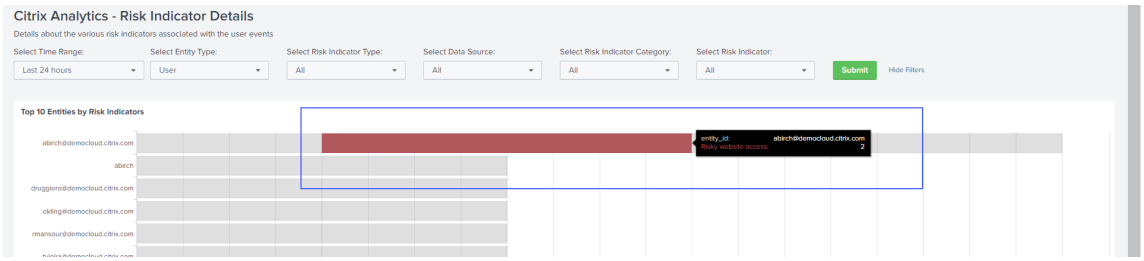


レポートを表示する

時間範囲とエンティティ (ユーザー名) を入力し、[**Submit**] をクリックして詳細情報を表示します。

または、次のダッシュボードからエンティティに関する詳細情報を表示することもできます。

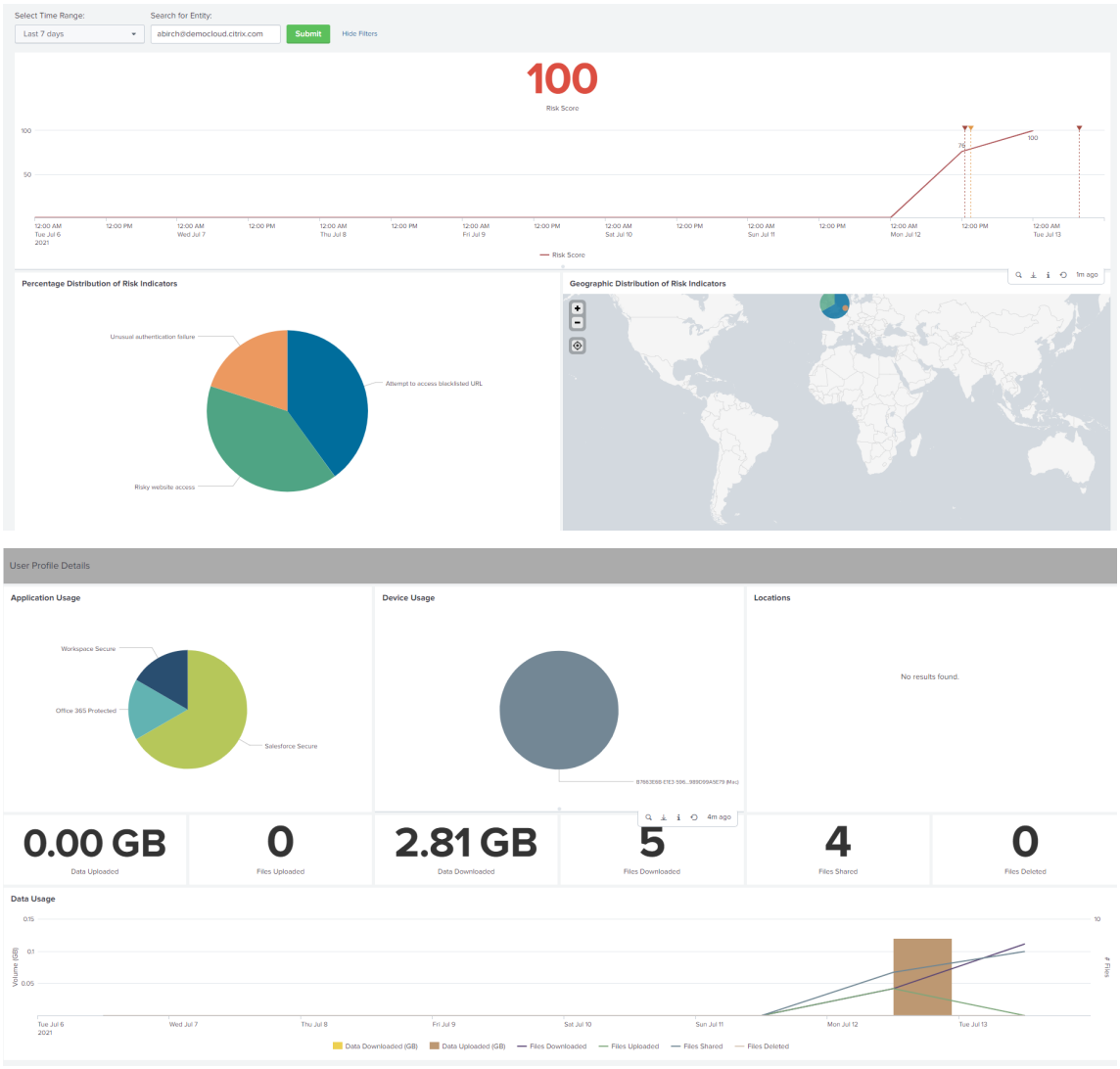
- 「**Citrix Analytics-**リスク指標の詳細」で、「リスク指標別上位 **10** エンティティ」に移動し、エンティティをクリックします。



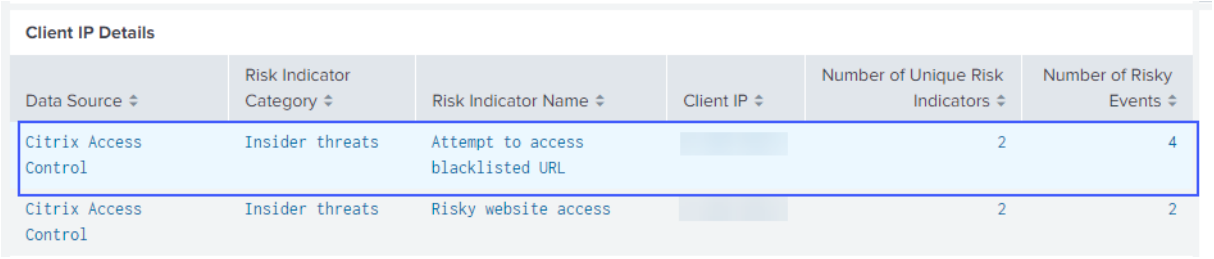
- **Citrix Analytics-**リスクスコアの概要で、「危険なユーザー」に移動し、ユーザー名をクリックします。

次の詳細情報が表示されます。

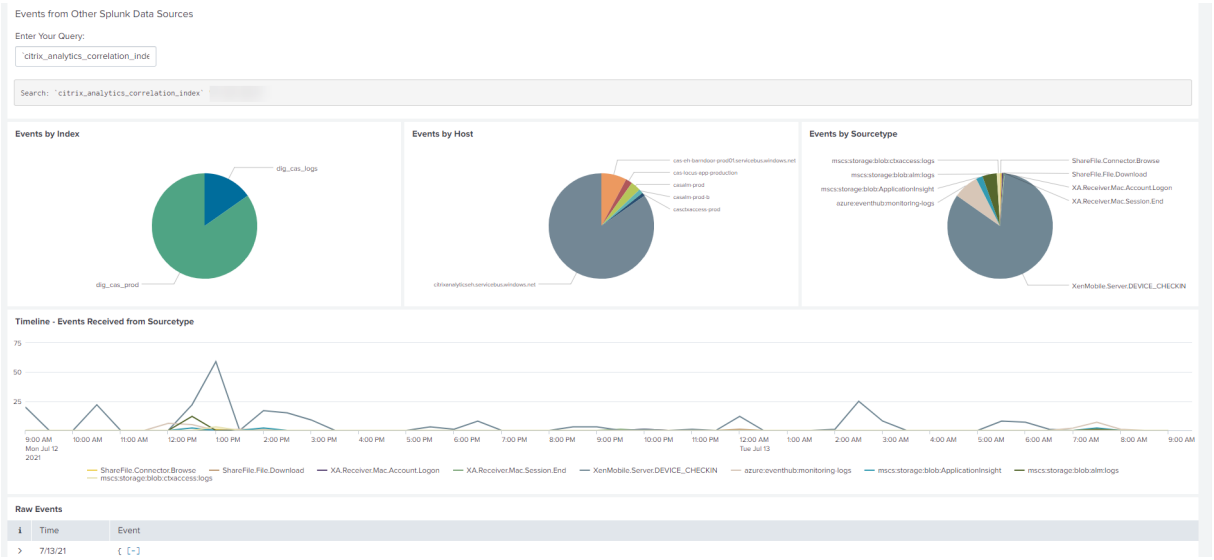
- 選択した期間における現在のリスクスコアとリスクスコアのタイムライン。
- リスク指標の割合分布。エンティティの危険なアクティビティのパターンを分析するのに役立ちます。
- リスク指標の地理的分布。珍しい場所やリスクの高い場所を特定するのに役立ちます。
- リスクの高いアクティビティに関連するクライアント IP の詳細。
- 危険なアクティビティに関連付けられているユーザーデバイスの詳細。
- 関連するデータソース、リスクカテゴリ、リスクの重大度などのリスク指標の詳細。



危険なアクティビティに関連するクライアント IP とユーザーデバイスを、Splunk に接続されている他のセキュリティソースから収集されたイベントと関連付けます。たとえば、[クライアント **IP** の詳細] テーブルの行をクリックします。



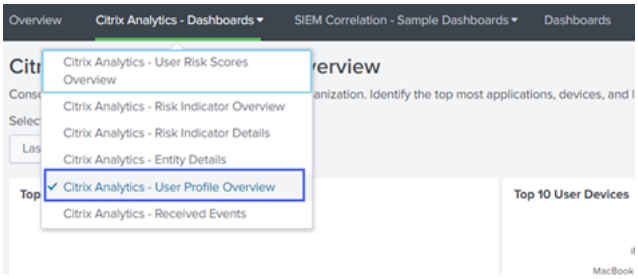
Citrix Analytics イベント相関ダッシュボードでは、（インデックスとソースタイプに基づいて）他のセキュリティデータソースと相関する、選択したクライアント IP に関連付けられたイベントを表示できます。これらのイベントは、クライアント IP に関連する悪意のあるアクティビティに関するより深い洞察を提供します。



ユーザープロファイルの概要

ダッシュボードを使用して、組織内のユーザーに関連付けられているイベントメトリックを表示します。

ダッシュボードを表示するには、[**Citrix Analytics**] - [ダッシュボード] > [**Citrix Analytics**] - [ユーザープロファイルの概要] をクリックします。

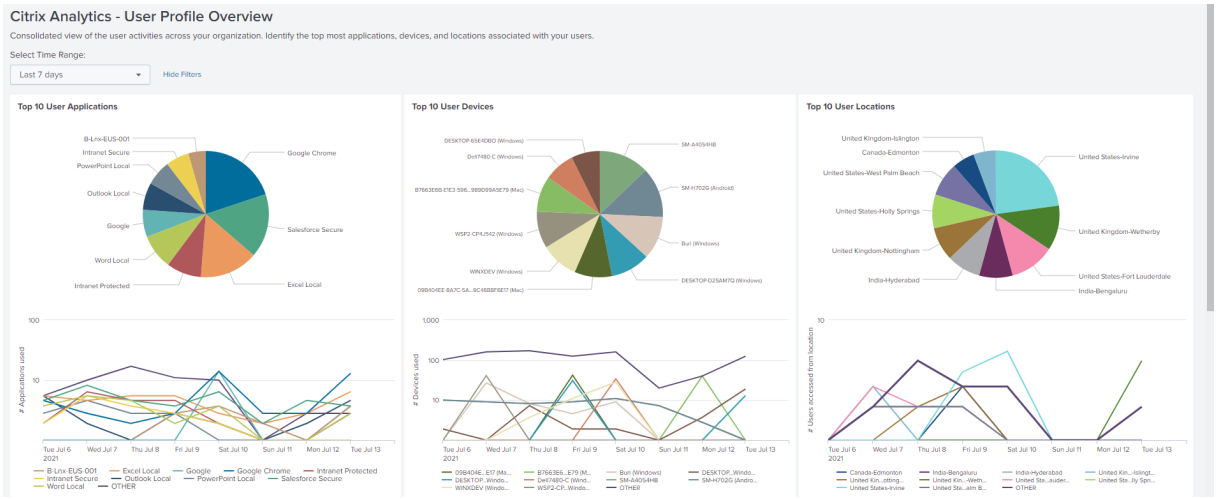


イベントを表示する

時間範囲を選択し、次のメトリックを表示します。

- ユーザーが使用するアプリケーションの上位 10
- ユーザーが使用しているデバイスの上位 10
- ユーザーが使用する上位 10 の場所
- 使用されている Web アプリケーションと SaaS アプリケーションの数
- 使用されたデバイスの数
- 複数のロケーションでアクセスしたユーザーの数
- アップロード、ダウンロード、共有ファイルなどのデータ使用量メトリクス

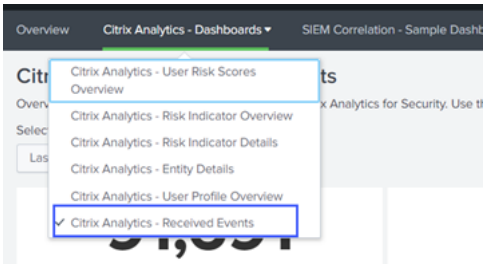
これらの指標は、組織内のユーザーアクティビティに関するインサイトを提供します。最上位のアプリケーションとデバイス、使用パターン、非準拠のデバイスとアプリケーション、異常な場所、危険なアクセス、および異常なファイルアクティビティを特定できます。



受信したイベント

ダッシュボードを使用して、Citrix Analytics for Security から受信したイベントを表示します。イベントは、ユーザアクティビティのタイプを示します。

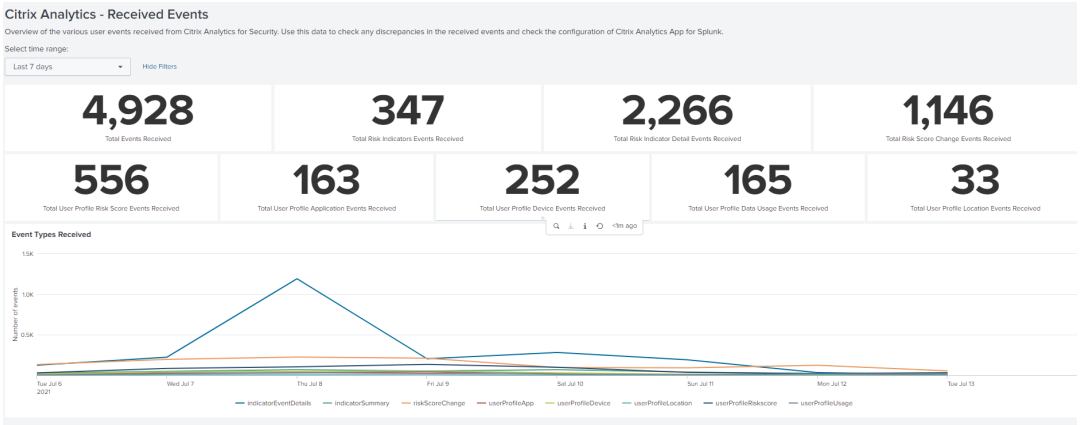
ダッシュボードを表示するには、[**Citrix Analytics**] **-** [ダッシュボード] **>** [**Citrix Analytics-**受信イベント] をクリックします。



レポートの表示

受信したさまざまなタイプのイベントを表示および比較するには、時間範囲を選択します。ダッシュボードには、次の情報が表示されます。

- 受信したイベントの総数：Citrix Analytics for Security から受信した次のイベントを含むすべてのイベントの合計です。
  - リスク指標イベントの合計: ユーザーによってトリガーされたリスク指標に関連付けられたイベントを示します。
  - リスク指標の詳細イベントの合計: トリガーされたリスク指標の詳細に関連付けられたイベントを示します。
  - 総リスクスコア変更イベント: ユーザーのリスクスコア変更に関連するイベントを示します。
  - ユーザープロファイルのリスクスコアイベントの合計: ユーザーのリスクスコアに関連付けられたイベントを示します。
  - ユーザープロファイルアプリケーションイベントの合計：ユーザーが使用するアプリケーションに関連付けられているイベントを示します。
  - ユーザープロファイルデバイスイベントの合計：ユーザーが使用するデバイスに関連付けられているイベントを示します。
  - ユーザープロファイルデータ使用イベント合計：ユーザーのデータ使用量に関連するイベントを示します。
  - ユーザプロファイルロケーションイベントの合計：ユーザがアクセスしたロケーションに関連付けられたイベントを示します。

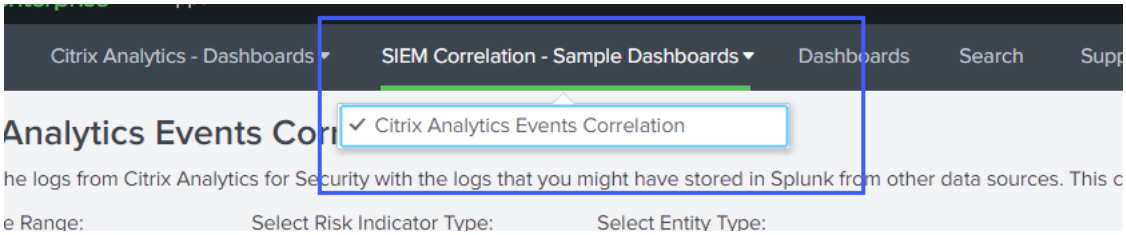


イベント相関の例

ダッシュボードを使用して、Citrix Analytics for Security から受信したイベントを、SSplunk で構成された他のセキュリティデータソースから収集されたイベントと関連付けます。複数のデータソースから収集されたユーザーの

リスクの高いアクティビティについてより深い洞察を得て、イベント間の関係を見つけ、脅威を特定します。

ダッシュボードを表示するには、[**SIEM** 相関**-**サンプルダッシュボード**] > [Citrix Analytics** イベントの相関] をクリックします。



前提条件

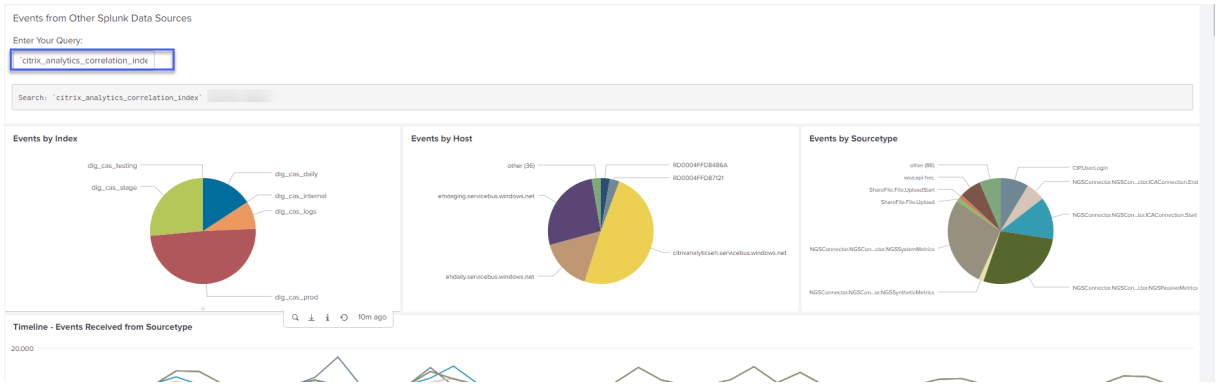
相関関係を実行するには、次のことを確認します。

- 関連付けを行うには、他のセキュリティデータソースからのイベントが必要です。たとえば、Splunk で設定されている他のデータソースから受信したユーザ、デバイス、クライアント IP アドレスに関連付けられたイベントなどです。
- 構成時に相関インデックスがすでに定義されている必要があります。

イベントの関連付け

Citrix Analytics for Security によって検出されたリスクの高いエンティティとリスクの高い IP アドレスを表示できます。これらのイベントを他のデータソース (インデックスとソースタイプで定義) に関連付けるには、テーブルからエンティティまたは IP アドレスをクリックします。

クエリフィールドに表示されるインデックス値は、アプリの設定時に定義されます。要件に応じて、インデックス値を別のセキュリティデータソースに変更できます。

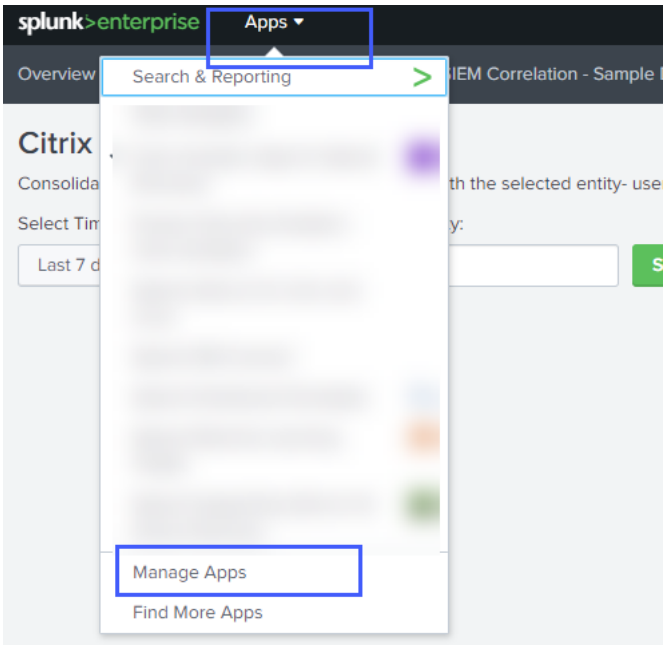


イベントがない場合のトラブルシューティング

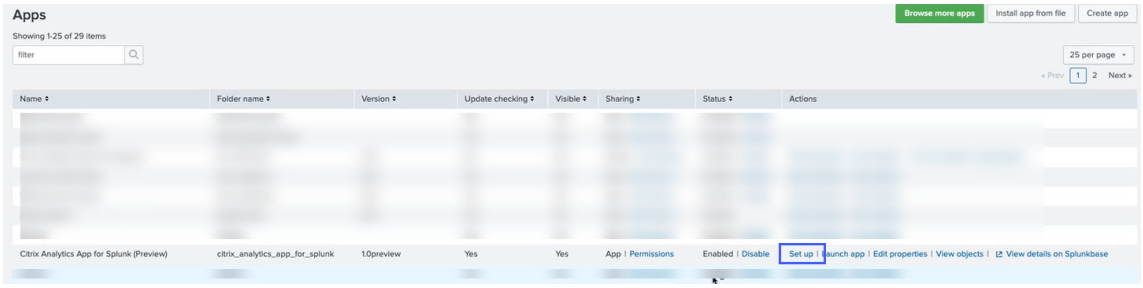
すべてのダッシュボードでイベントが見つからない場合は、Splunk 向け Citrix Analytics アプリおよび SSplunk 用の Citrix AnCitrix Analytics アドオンの構成の問題が原因である可能性があります。このようなシナリオでは、インデックス値とソースタイプの値を確認します。インデックスとソースタイプの値が、アプリとアドオンの両方で同じであることを確認してください。

Splunk 用 Citrix Analytics アプリケーションの構成設定を表示するには:

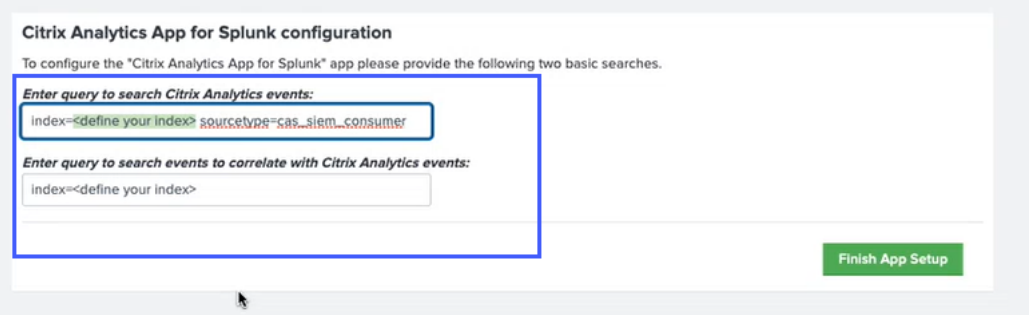
1. [アプリ] **>** [アプリの管理] をクリックします。



2. リストから Splunk 向け Citrix Analytics アプリを探します。[セットアップ] をクリックします。

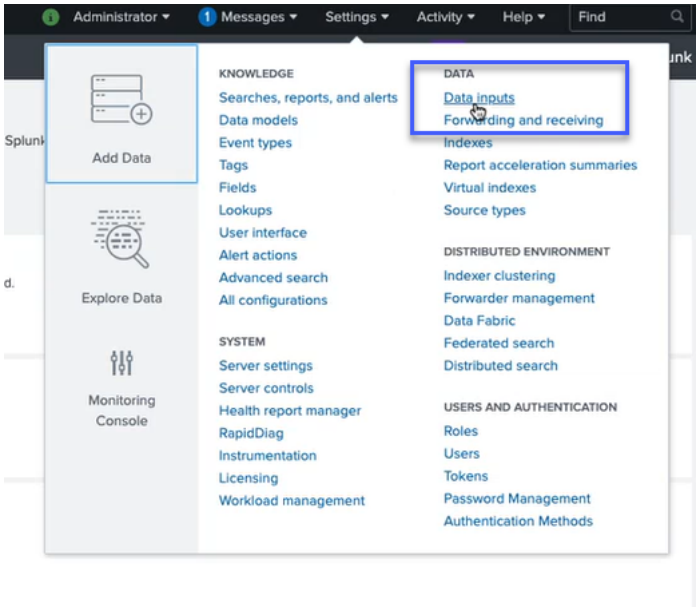


3. ソースタイプとインデックスを確認します。

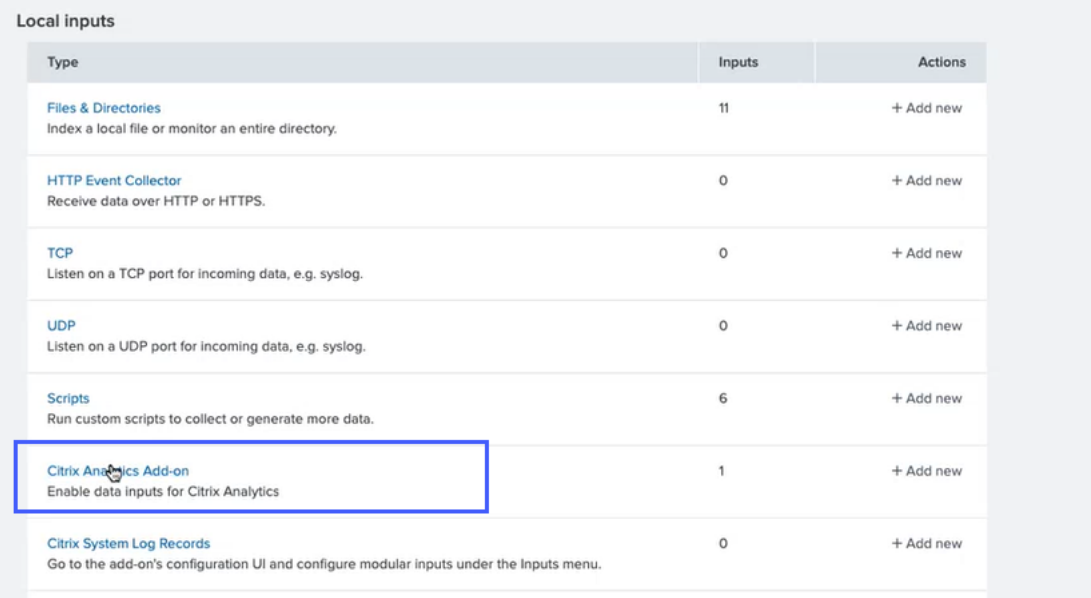


Splunk 向け Citrix Analytics アドオンの構成設定を表示するには:

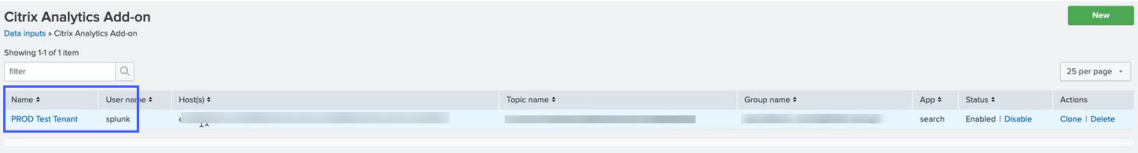
1. [設定] **>** [データ入力] をクリックします。



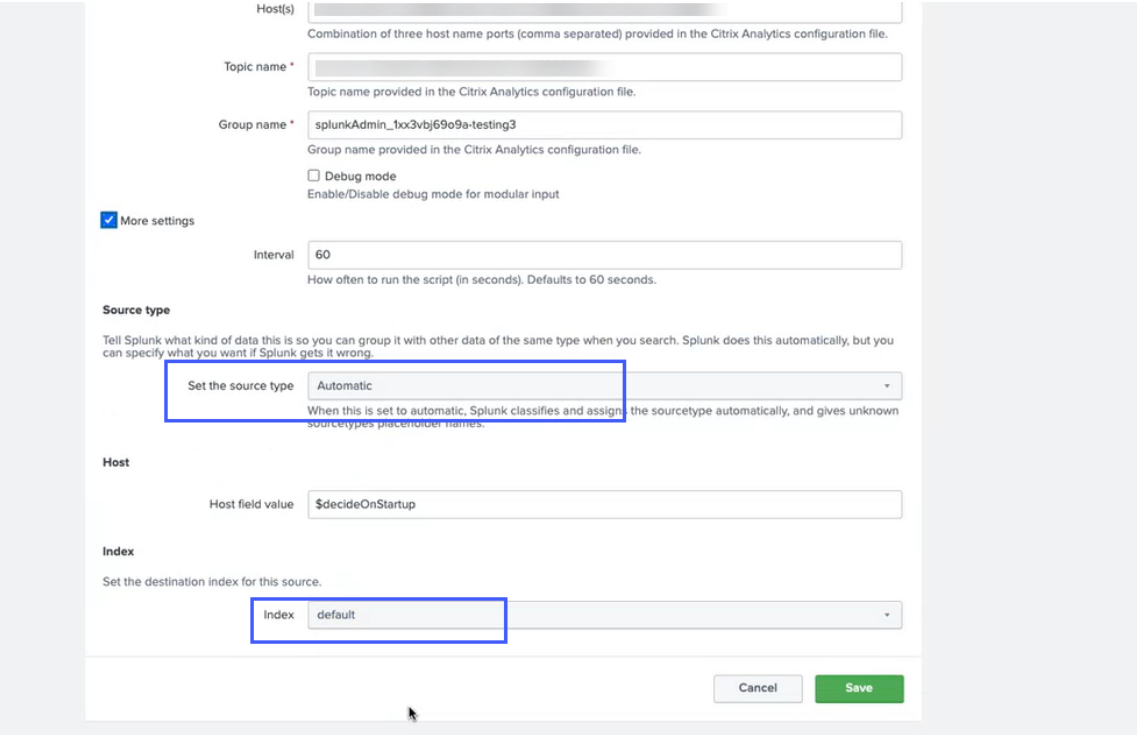
2. [**Citrix Analytics** アドオン] をクリックします。



3. イベントを取得するテナントをクリックします。
4. [その他の設定] を選択します。



5. ソースタイプとインデックスを確認します。



構成について詳しくは、「Splunk 用の Citrix Analytics アドオンを構成する」を参照してください。

Splunk 用 Citrix Analytics アドオンの設定に関する問題

July 15, 2022

Citrix Analytics アドオン設定を使用できません

Splunk Forwarder または Splunk スタンドアロン環境に Splunk 用 Citrix **Analytics** アドオンをインストールした後、**[設定] > [データ入力]** に **[Citrix Analytics** アドオン**]** 設定が表示されません。

理由

この問題は、サポートされていない Splunk 環境に Splunk 用 Citrix Analytics アドオンをインストールすると発生します。

解決された問題

サポートされている Splunk 環境に Splunk 用 Citrix Analytics アドオンをインストールします。サポートされるバージョンの詳細については、「Splunk 統合」を参照してください。

Splunk ダッシュボードにはデータがありません

Splunk Forwarder または Splunk スタンドアロン環境に Splunk 用 Citrix Analytics アドオンをインストールして構成すると、Splunk ダッシュボードにシトリックスアナリティクスからのデータが表示されません。

チェック

この問題のトラブルシューティングを行うには、Splunk Forwarder または Splunk スタンドアロン環境で以下を確認します。

1. Splunk 統合の前提条件が満たされていることを確認します 。
2. ［設定］**>** ［データ入力］**>** ［**Citrix Analytics** アドオン］Citrix Analytics の構成の詳細が利用可能であることを確認します 。
3. 構成の詳細が利用できる場合は、次のクエリを実行して、SSplunk 向け Citrix Analytics アドオンに関連するエラーがないかログを確認します。


```
index=_internal sourcetype=splunkd log_level=ERROR component=
    ExecProcessor cas_siem_consumer
```

4. エラーが見つからない場合、SSplunk 向け Citrix Analytics アドオンは期待どおりに動作しています。ログにエラーが見つかった場合は、次のいずれかの原因が考えられます。

   - Splunk 環境と Citrix Analytics Kafka エンドポイント間の接続を確立できませんでした。この問題は、ファイアウォールの設定が原因である可能性があります。

     修正方法: この問題を解決するには、ネットワーク管理者に問い合わせてください。

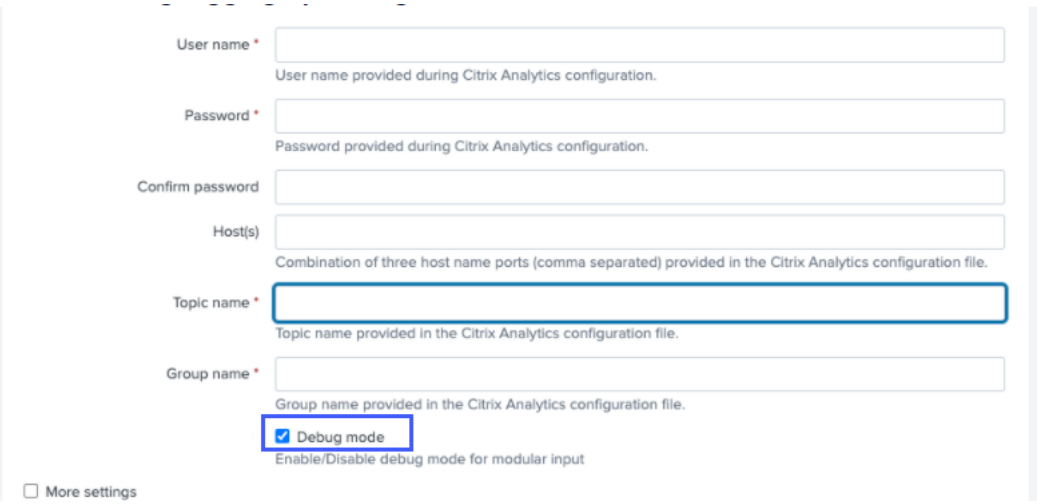
   - ［設定］**>**［データ入力］**>**［**Citrix Analytics** アドオン］の構成の詳細

     修正：ユーザー名、パスワード、ホストエンドポイント、トピック、コンシューマーグループなどの Citrix Analytics 構成の詳細が、Citrix Analytics 構成ファイルに従って正しく入力されていることを確認します。詳しくは、「Splunk 用の Citrix Analytics アドオンを構成する」を参照してください。

5. 前述のログから問題の原因が見つからず、さらに調査する場合は、次の手順を実行します。

   a) 設定］**>**［データ入力］**>**［**Citrix Analytics** アドオン］でデバッグモードを有効にします

   > 注
   >
   > デフォルトでは、**Debug** モードは無効になっています。このモードを有効にすると、生成されるログが多すぎます。したがって、このオプションは必要な場合にのみ使用し、デバッグタスクが完了したら無効にしてください。



   b) 生成されたデバッグログを次の場所で探し、エラーがないか確認します。

```
$SPLUNK_HOME$/var/log/splunk.Filename
    splunk_citrix_analytics_add_on_debug_connection.log
```

   c) (オプション)Splunk 用 Citrix Analytics `splunk cmd python cas_siem_consumer_debug.py` アドオンで使用できるデバッグスクリプトを使用します。このスクリプトは、Splunk 環境と接続

チェックの詳細を含むログファイルを生成します。この詳細を使用して、問題をデバッグできます。以下のコマンドを使用してスクリプトを実行します。

```
cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin/; /opt/splunk/bin/
    splunk cmd python cas_siem_consumer_debug.py
```

エラーメッセージ

Splunk 用 Citrix Analytics アドオンに関連するログに、次のエラーが表示される場合があります。

```
ERRORKafkaError{ code=_TRANSPORT,val=-195,str="Failed to get metadata
: Local: Broker transport failure"}
```

このエラーは、ネットワーク接続の問題または認証の問題が原因で発生します。

この問題をデバッグするには、次の手順を実行します。

1. Splunk Forwarder または Splunk スタンドアロン環境で、デバッグモードを有効にしてデバッグログを取得します。前のステップ 5.a を参照してください。
2. 次のクエリを実行して、デバッグログで認証の問題を検出します。

   ```
   index=_internal source="*
       splunk_citrix_analytics_add_on_debug_connection.log*" "
       Authentication failure"
   ```

3. デバッグログに認証の問題が見つからない場合、エラーはネットワーク接続の問題が原因です。
4. telnet または前のステップ 5.c で説明したデバッグスクリプトを使用して、問題を検出して解決します。

2.0.0 より前のバージョンからのアドオンのアップグレードが失敗する

Splunk Forwarder または Splunk スタンドアロン環境で、Splunk 用 Citrix Analytics アドオンを 2.0.0 より前のバージョンから最新バージョンにアップグレードすると 、アップグレードが失敗します。

解決された問題

1. Citrix Analytics Splunk /bin アドオンインストールフォルダーのフォルダー内にある以下のファイルとフォルダーを削除します。
   - cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin
   - rm -rf splunklib
   - rm -rf mac
   - rm -rf linux_x64

- `rm CARoot.pem`
- `rm certificate.pem`

2. Splunk フォワーダまたは Splunk スタンドアロン環境を再起動します。

Microsoft Sentinel との統合

November 26, 2023

> メモ
>
> - Microsoft Sentinel < CAS-PM-Ext@cloud.com > の統合、Microsoft Sentinel へのデータのエクスポートに関するサポートの依頼、またはフィードバックの提供については、お問い合わせください。
> - Logstash エンジンを使用した Microsoft Sentinel へのデータエクスポートはプレビュー中です。この機能はサービスレベルアグリーメントなしで提供され、本番環境のワークロードには推奨されません。詳細については、Microsoft Sentinel のドキュメントを参照してください 。

Logstash エンジンを使用して、Citrix Analytics for Security を Microsoft Sentinel と統合します。

この統合により、Citrix IT 環境から Microsoft Sentinel にユーザーのデータをエクスポートして関連付け、組織のセキュリティ体制に関するより深い洞察を得ることができます。SSplunk k 環境内の Citrix Analytics for Security に固有の洞察に満ちたダッシュボードを表示します。セキュリティ要件に基づいてカスタムビューを作成することもできます。

統合の利点と、SIEM に送信される処理済みデータの種類の詳細については、セキュリティ情報とイベント管理の統合を参照してください。

前提条件

- 少なくとも 1 つのデータソースのデータ処理を有効にします。これは、Citrix Analytics for Security が Microsoft Sentinel 統合プロセスを開始するのに役立ちます。
- ネットワークの許可リストに次のエンドポイントがあることを確認します。

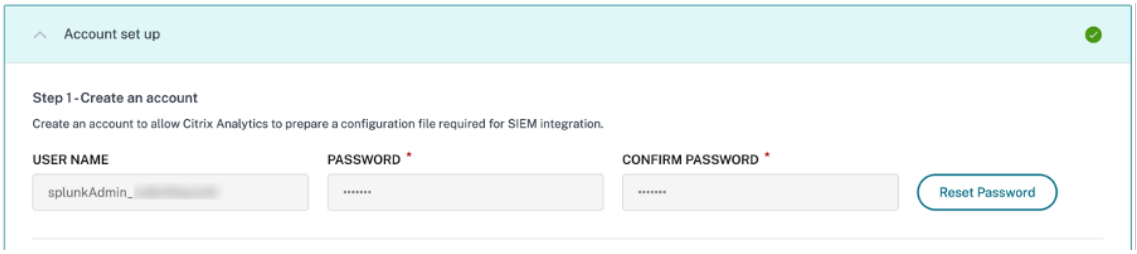
エンドポイント	米国リージョン	欧州連合地域	アジア太平洋南部リージョン
Kafka ブローカー	`casnb-0.citrix.com:9094`	`casnb-eu-0.citrix.com:9094`	`casnb-aps-0.citrix.com:9094`

エンドポイント	米国リージョン	欧州連合地域	アジア太平洋南部リージョン
	casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

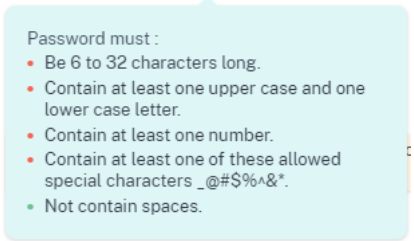
- Logstash 用の Microsoft Sentinel 出力プラグインを備えた Logstash バージョン 7.17.7 以降（セキュリティ向け Citrix Analytics との互換性がテストされたバージョン：v7.17.7 および v8.5.3）を必ず使用してください。

Microsoft Sentinel との統合

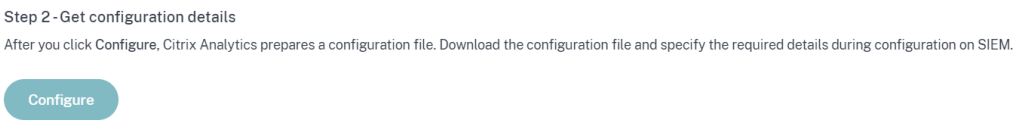
1. **[設定] > [データエクスポート]** に移動します。
2. アカウント設定セクションで、ユーザー名とパスワードを指定してアカウントを作成します。このアカウントは、統合に必要な設定ファイルの準備に使用されます。



3. パスワードが次の条件を満たしていることを確認します。



4. [**Configure**] をクリックして Logstash 設定ファイルを生成します。



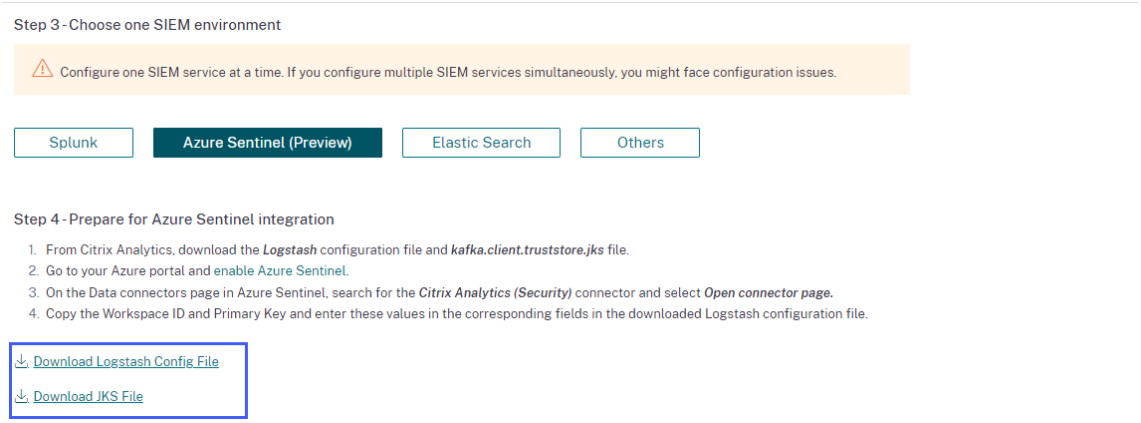
5. Azure Sentinel (プレビュー) タブを選択して構成ファイルをダウンロードします。

   - **Logstash** 構成ファイル: Logstash データ収集エンジンを使用して Citrix Analytics for Security から Microsoft Sentinel にイベントを送信するための構成データ（入力、フィルター、および出力セクション）が含まれます。

     Logstash の設定ファイルの構造については、Logstash のドキュメントを参照してください。

   - **JKS** ファイル:SSL 接続に必要な証明書が含まれます。

   > 注
   >
   > これらのファイルには機密情報が含まれています。安全な場所に保管してください。



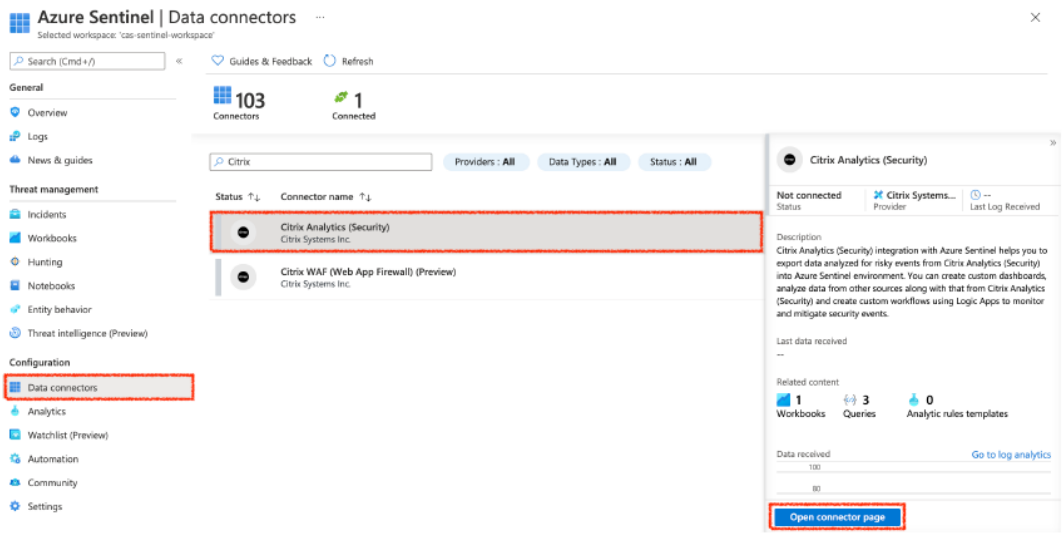
6. Azure Sentinel インテグレーションを準備します。

   a) Azure ポータルで、Microsoft Sentinelを有効にします。ワークスペースを作成することも、既存のワークスペースを使用して Microsoft Sentinel を実行することもできます。

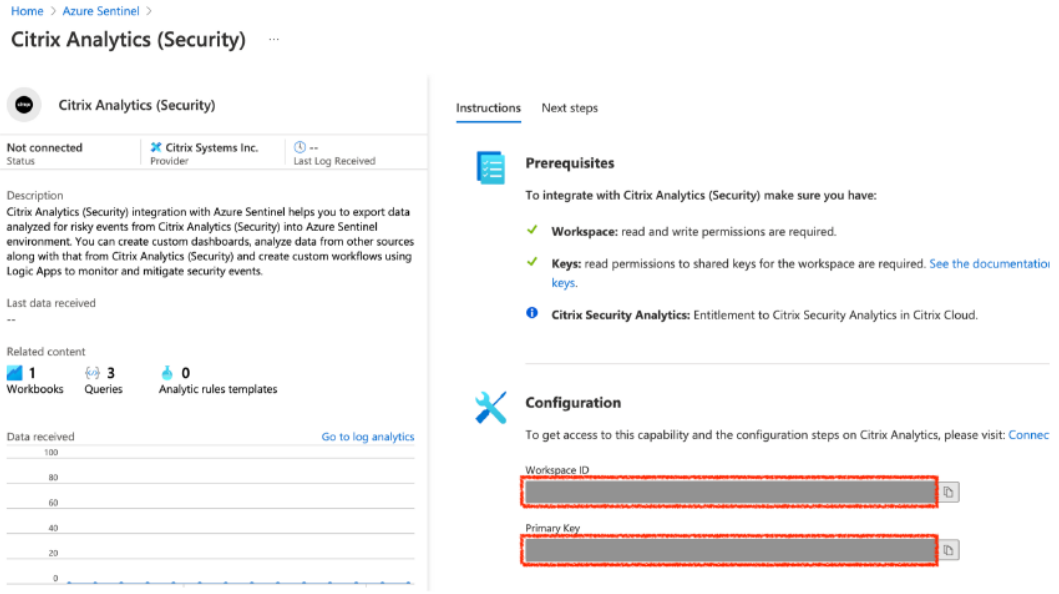
   b) メインメニューから [データコネクタ] を選択し、[データコネクタ] ギャラリーを開きます。

   c)「**Citrix Analytics**（セキュリティ）」を検索します。

   d) **Citrix Analytics**（セキュリティ）］を選択し、［コネクタページを開く］を選択します。



e) **Citrix Analytics**（セキュリティ）］ページから、［ワークスペース **ID** ］と［主キー］をコピーします。この情報は、以降の手順で Logstash 設定ファイルに入力する必要があります。



f) ホストマシンで Logstash を設定します。

i. Linux または Windows ホストマシンで、Logstash 用の Logstashおよび Microsoft Sentinel 出力プラグインをインストールします。

ii. Logstash をインストールしたホストマシンで、次のファイルを指定したディレクトリに配置します。

ホストマシンタイプ	ファイル名	ディレクトリパス
Linux	CAS_AzureSentinel_LogStash_Config.conf	Debian パッケージと RPM パッケージの場合: /etc/logstash/conf.d/ .zip および.tar.gz アーカイブの場合: { extract.path } / config
	kafka.client.truststore.jks	Debian パッケージと RPM パッケージの場合: /etc/logstash/ssl/ .zip および.tar.gz アーカイブの場合: { extract.path } /ssl
Windows	CAS_AzureSentinel_LogStash_Config.conf	C:\logstash-7.xx.x\config
	kafka.client.truststore.jks	

Logstash インストールパッケージのデフォルトのディレクトリ構造については、Logstash のドキュメントを参照してください。

iii. Logstash 設定ファイルを開き、次の操作を行います。

A. ファイルの input セクションに、次のように入力します。

- パスワード: Citrix Analytics for Security で構成ファイルを準備するために作成したアカウントのパスワード。
- **SSL** トラストストアの場所:SSL クライアント証明書の場所。これは、ホストマシンの kafka.client.truststore.jks ファイルの場所です。

```
input {
  kafka {
    bootstrap_servers => "
    topics => ["
    group_id => "
    session_timeout_ms => 60000
    auto_offset_reset => "earliest"
    security_protocol => "SASL_SSL"
    sasl_mechanism => "SCRAM-SHA-256"
    ssl_endpoint_identification_algorithm => ""
    sasl_jaas_config => "org.apache.kafka.common.security.scram.ScramLoginModule required username='
    ssl_truststore_location => "/etc/logstash/ssl/kafka.client.truststore.jks"
  }
}
```

B. ファイルの出力セクションで、ファイルの出力セクションにワークスペース **ID** とプライマリキー (Microsoft Sentinel からコピーしたもの) を入力します。


```
output {
  if [event_type] == "indicatorSummary" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_indicatorSummary"
          time_generated_field => "timestamp"
    }
  } else if [event_type] == "indicatorEventDetails" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_indicatorEventDetails"
          time_generated_field => "timestamp"
    }
  }else if [event_type] == "riskScoreChange" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_riskScoreChange"
          time_generated_field => "timestamp"
    }
  } else if [event_type] =~ "userProfile.+" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_userProfile"
          time_generated_field => "timestamp"
    }
  } else {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_misc"
          time_generated_field => "timestamp"
    }
```

iv. Logstash ホストマシンを再起動して、Citrix Analytics for Security から Microsoft Sentinel に処理済みのデータを送信します。

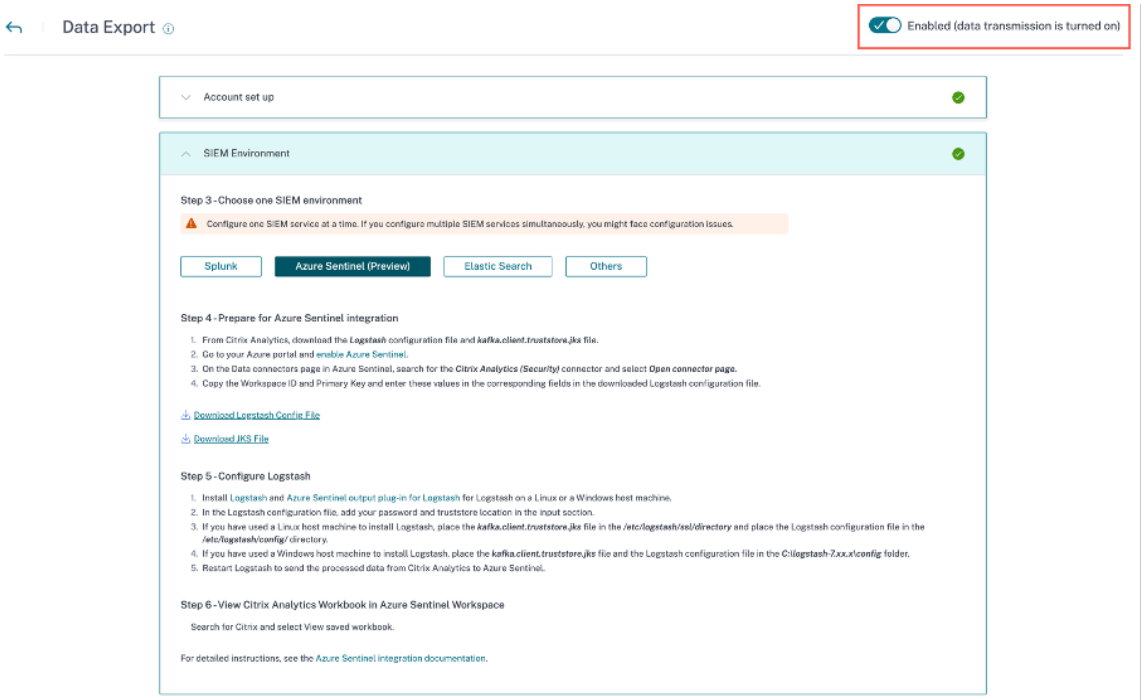
g) Microsoft Sentinel ワークスペースに移動し、Citrix Analytics ワークブックのデータを表示します。

データ伝送をオンまたはオフにする

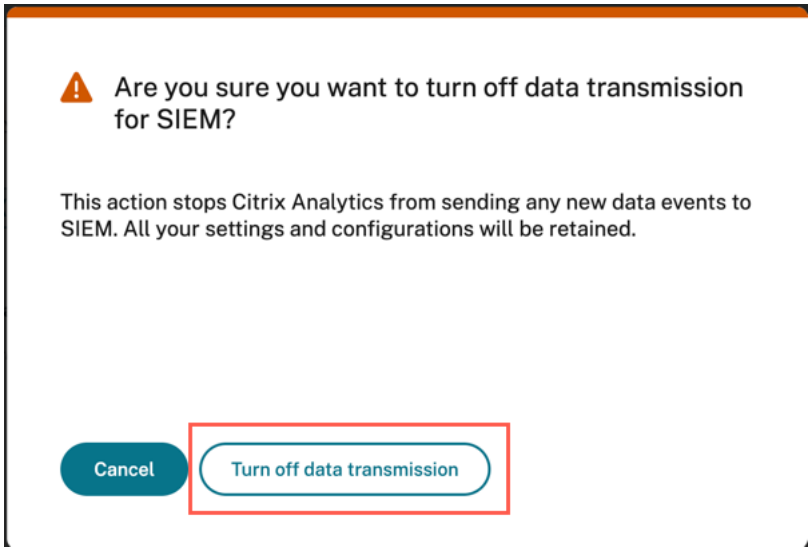
Citrix Analytics for Security が構成ファイルを準備すると、Microsoft Sentinel のデータ転送がオンになります。

セキュリティ向け Citrix Analytics からのデータの送信を停止するには:

1. **[設定] > [データエクスポート]** に移動します。
2. トグルボタンをオフにしてデータ転送を無効にします。デフォルトでは、データ転送は常に有効になっています。



確認用の警告ウィンドウが表示されます。データ転送を停止するには、[データ転送をオフにする] ボタンをクリックします。



データ転送を再度有効にするには、トグルボタンをオンにします。

Microsoft Sentinel 統合の詳細については、次のリンクを参照してください。

- Citrix Analytics と Microsoft Sentinel の統合
- Citrix Analytics for Security と Microsoft Sentinel で脅威ハンティングゲームを盛り上げましょう

Microsoft Sentinel 向け Citrix Analytics ワークブック

December 7, 2023

> 注
>
> この機能はプレビュー段階です。

この記事では、Microsoft Sentinel ワークスペースで使用できる Citrix Analytics ワークブックについて説明します。

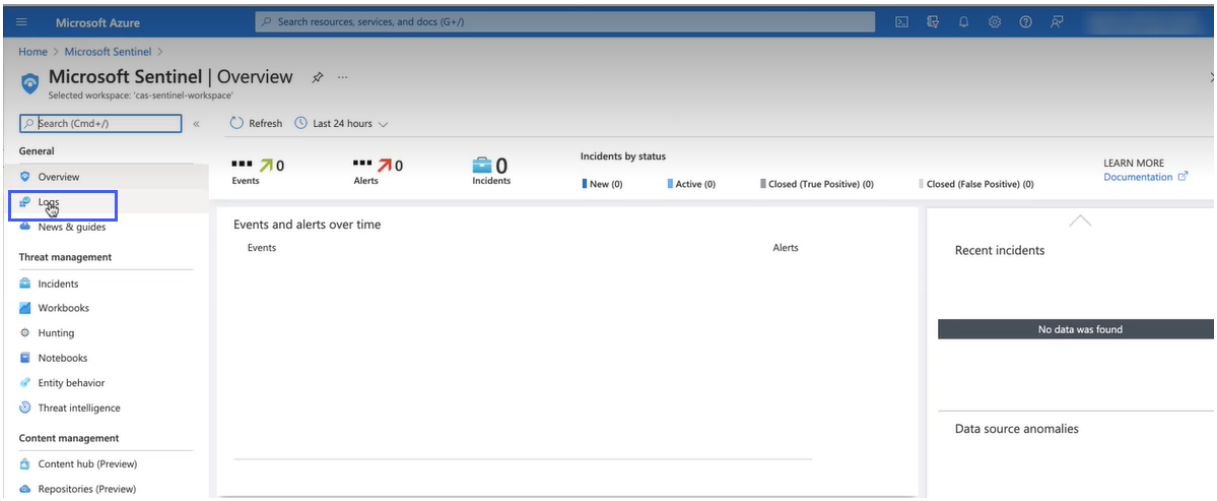
前提条件

Citrix Analytics ワークブックを使用するには、Microsoft Sentinel と Citrix Analytics for Security が既に統合されていることを確認してください。詳細については、「Microsoft Sentinel の統合」を参照してください。

Citrix Analytics イベントを表示する

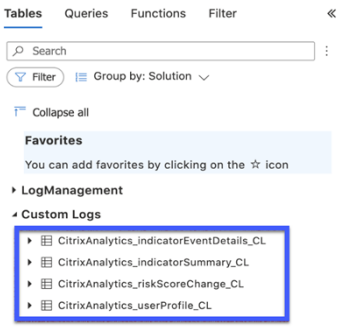
Citrix Analytics for Security を Microsoft Sentinel と統合すると、Logstash コネクタは Citrix Analytics for Security から Microsoft Sentinel ワークスペースへのイベントのプッシュを開始します。**Azure** ポータルで、統合に使用した Microsoft Sentinel ワークスペースを開きます。

Microsoft Sentinel が Citrix Analytics for Security からイベントを受信していることを確認するには、［ログ］**>** ［カスタムログ］を選択します。



［カスタムログ］セクションでは、Citrix Analytics for Security から受信したイベントを保存するために自動的に作成されるログテーブルを表示できます。これらのログテーブルは、Citrix Analytics ワークブックのダッシュボードのソースとして機能します。

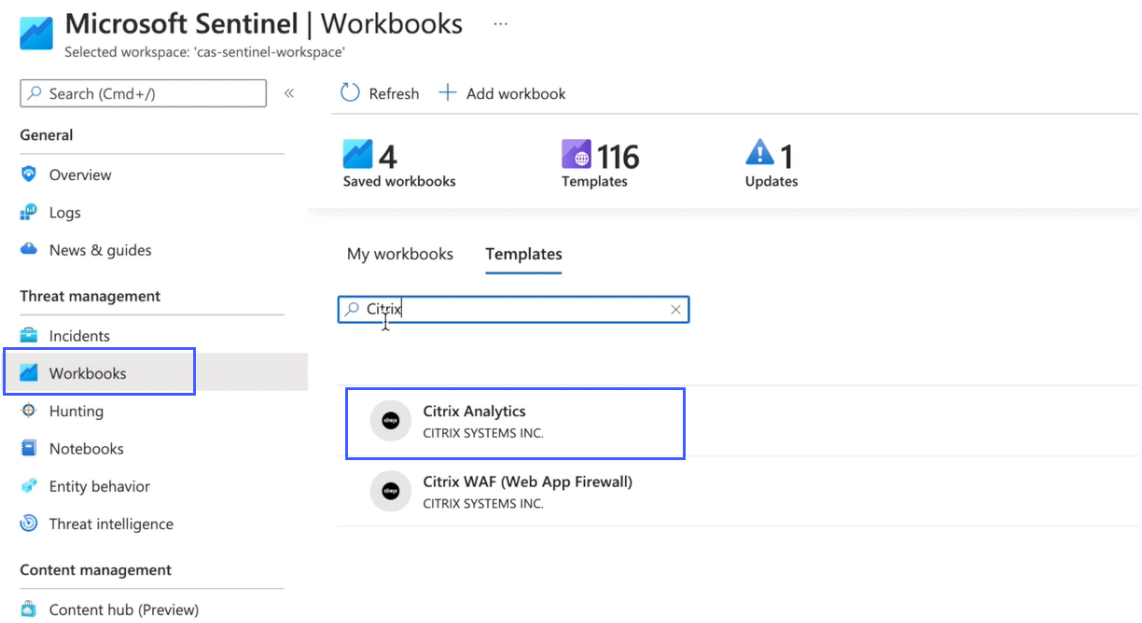
> 注
>
> Citrix Analytics for Security から送信されたイベントが、Microsoft Sentinel ワークスペースに表示されるまでに数時間かかる場合があります。そのため、イベントのログテーブルの作成に遅延が生じることがあります。



Citrix Analytics ワークブックを表示する

ログテーブルが正常に作成されたら、次の操作を実行します。

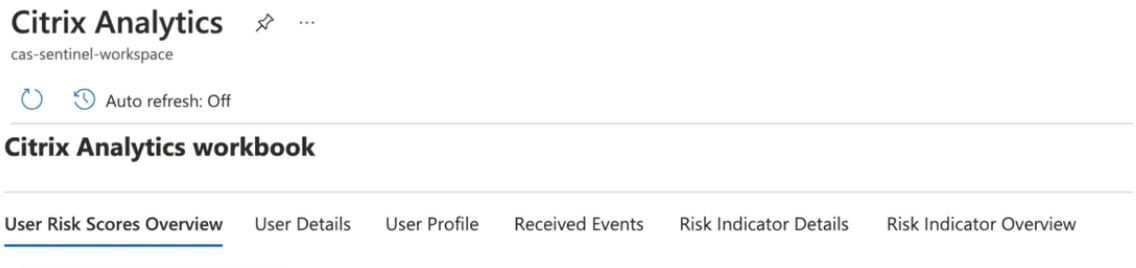
1. ワークブック］を選択して［**Citrix Analytics**］を検索します。［**Citrix Analytics**］



2. ［テンプレートの表示］を選択して、Citrix Analytics ワークブックを開きます。

Citrix Analytics ワークブックでは、次のダッシュボードでユーザーイベントを表示できます。

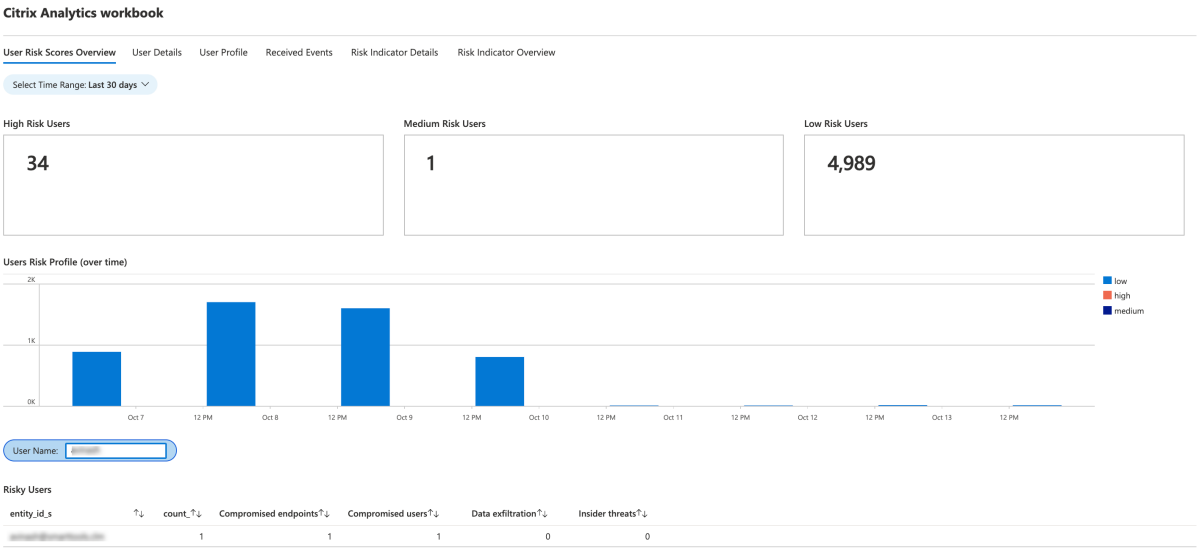
- ユーザーリスクスコアの概要: 組織内のリスクの高いユーザーを統合して表示します。
- ユーザーの詳細: ユーザーとその危険な行動の詳細が表示されます。
- ユーザープロファイル: ユーザーに関連付けられたイベントメトリクスを提供します。
- 受信したイベント： Citrix Analytics for Security から受信したイベントを提供します。
- リスク指標の詳細: ユーザーによってトリガーされた組み込みリスク指標とカスタムリスク指標に関する詳細を提供します。
- リスク指標の概要: ユーザーによってトリガーされたリスク指標をまとめて表示します。



ユーザーリスクスコアの概要

このダッシュボードには、組織内のリスクの高いユーザーの統合ビューが表示されます。ユーザーは、リスクレベル（高、中、低）によって分類されます。リスクレベルはユーザーアクティビティの異常に基づいており、したがってリスクスコアが割り当てられます。リスクの高いユーザーのタイプの詳細については、「ユーザー」ダッシュボードを参照してください。

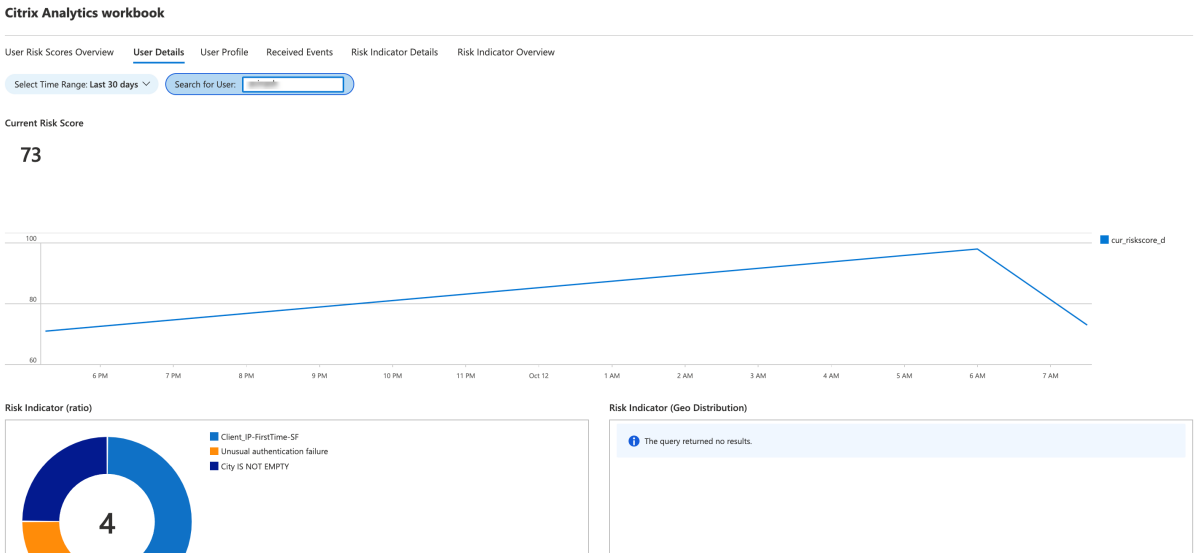
期間を選択して、組織内のリスクの高いユーザーを表示します。



ユーザーの詳細

このダッシュボードには、ユーザーに関連付けられたリスクスコアとリスク指標が表示されます。

ユーザーを検索し、組織に脅威を与える可能性のある危険なアクティビティを表示します。脅威を軽減するために、リスクの重大度に基づいてユーザーアカウントに対して適切なアクションを実行できます。



ユーザープロフィール

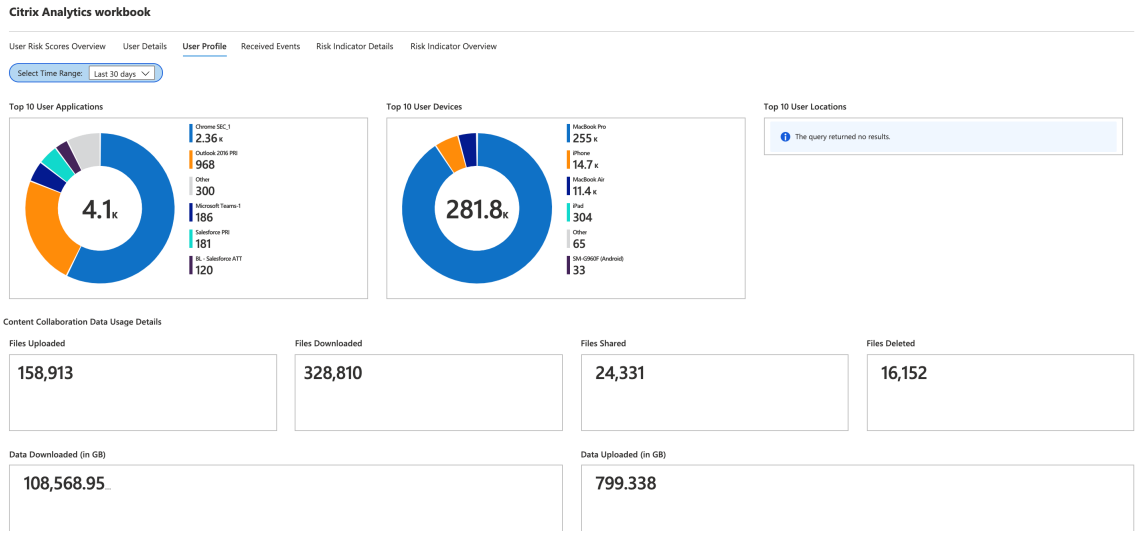
このダッシュボードには、選択した期間におけるユーザーに関連付けられたイベントメトリックの詳細が表示されます。メトリクスは、次のようなユーザーアクティビティに関するインサイトを提供します。

- ユーザーが使用するアプリケーションの上位 10

- ユーザーが使用しているデバイスの上位 10
- ユーザーがログオンした場所の上位 10 か所

このレポートを使用すると、次のことができます。

- ユーザーの使用傾向を特定する
- リソースへのアクセスに使用されている非準拠デバイスを検出します。
- ユーザーからの潜在的に危険なアクセスがないか確認する



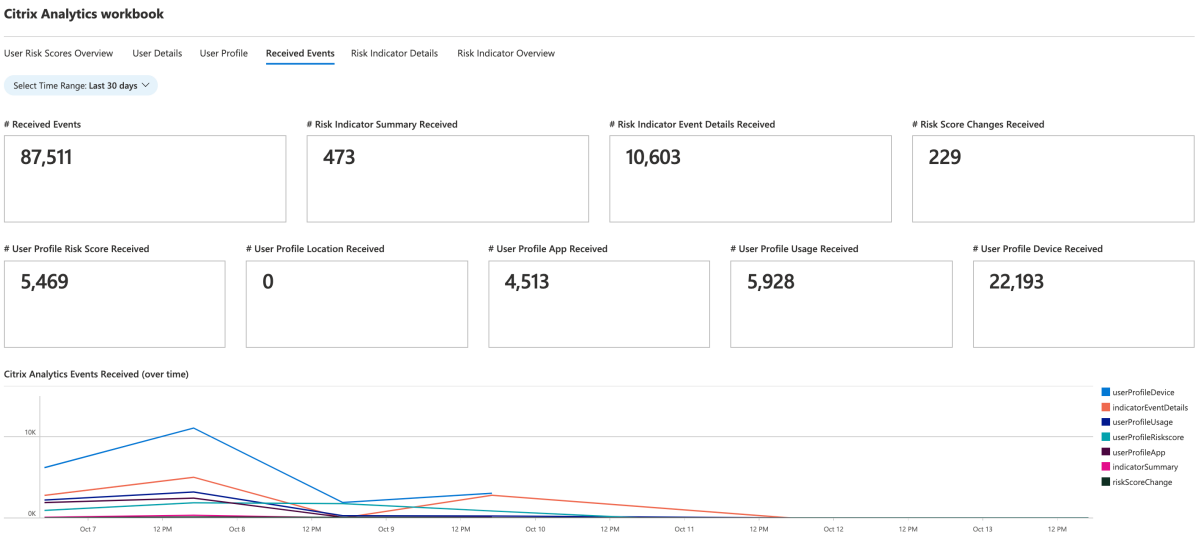
受信したイベント

選択した期間について、Citrix Analytics for Security から受信したイベントの総数を表示できます。受信したイベントの総数には次のものが含まれます。

- リスク指標サマリー: ユーザーリスク指標のサマリーに関連付けられているイベントを示します。さまざまなリスク指標サマリーイベントの詳細については、「リスク指標スキーマ」を参照してください。
- リスク指標イベントの詳細: ユーザーリスク指標の詳細に関連付けられたイベントを示します。さまざまなリスク指標詳細イベントについては、「リスク指標スキーマ」を参照してください。
- ユーザープロファイルリスクスコア: ユーザーのリスクスコアに関連付けられたイベントを示します。詳細については、「ユーザーダッシュボード」を参照してください。
- リスクスコアの変更: ユーザーのリスクスコアの変更に関連するイベントを示します。詳細については、「ユーザーダッシュボード」を参照してください。
- ユーザープロファイルの場所: ユーザーがログオンした場所に関連付けられているイベントを示します。
- ユーザープロファイルアプリ: ユーザーが使用するアプリケーションに関連付けられているイベントを示します。

- ユーザープロファイルの使用状況: ユーザーのデータ使用量に関連するイベントを示します。
- ユーザープロファイルデバイス: ユーザーが使用するデバイスに関連付けられているイベントを示します。

ダッシュボードを定期的に確認することで、Microsoft Sentinel ワークスペースにイベントが適切に流れているかどうかを確認できます。受信したイベントの合計に不一致がある場合は、Citrix Analytics for Security との統合の問題を示している可能性があります。問題のデバッグに必要な手順を実行できます。

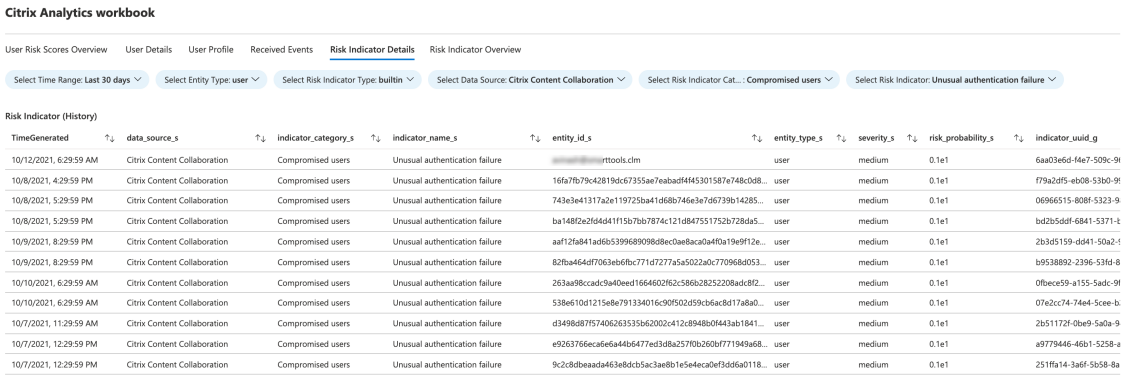


リスク指標の詳細

このダッシュボードには、ユーザーによってトリガーされたリスク指標の詳細が表示されます。

リスク指標の詳細は、1 つ以上のカテゴリを選択して表示できます。

- 時間範囲: 期間中にトリガーされたリスク指標の詳細を表示する時間範囲を選択します。
- エンティティタイプ: ユーザーを選択すると、関連するリスク指標の詳細が表示されます。
- リスク指標タイプ: [組み込みまたはカスタムのリスク指標を選択して](/ja-jp/security-analytics/custom-risk-indicators.html) 、詳細を表示します。
- データソース: データソースを選択して 、関連するリスク指標を表示します。
- リスク指標カテゴリ: 関連するリスク指標を表示するリスクカテゴリを選択します 。
- リスク指標: リスク指標を名前で選択し、その詳細を表示します。

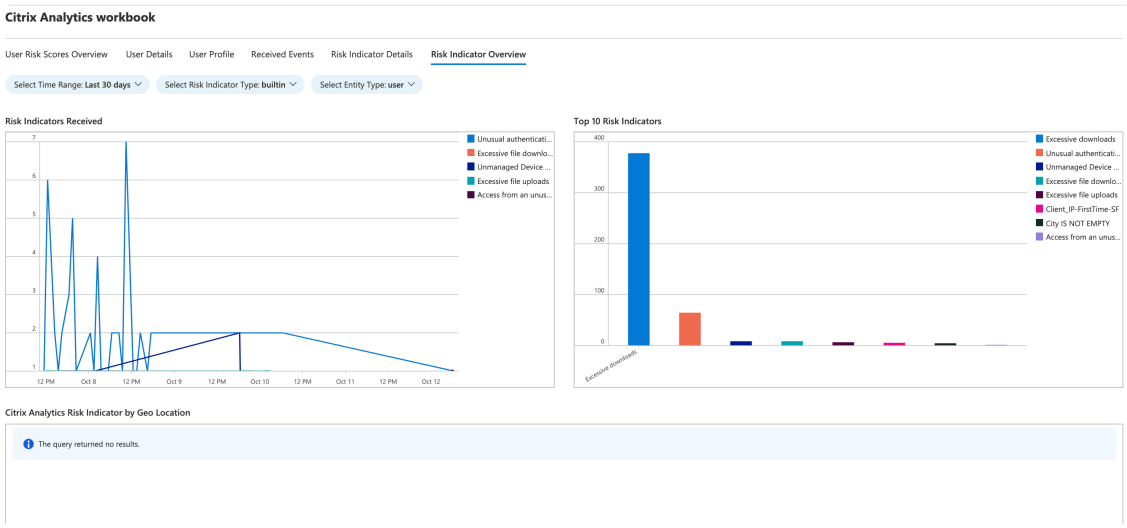


リスク指標の概要

このダッシュボードには、ユーザーによってトリガーされたすべてのリスク指標が統合されたビューが表示されます。

リスク指標を表示するには、1 つ以上のカテゴリを選択します。

- 時間範囲: 期間を選択して、その期間中にトリガーされるリスク指標を表示します。
- リスク指標タイプ: [組み込みまたはカスタムのいずれかを選択して](/ja-jp/security-analytics/custom-risk-indicators.html) 、関連するリスク指標を表示します。
- エンティティタイプ: いずれかのユーザーを選択すると、関連するリスク指標が表示されます。



Logstash による **Sentinel** インテグレーションのトラブルシューティングガイダンス

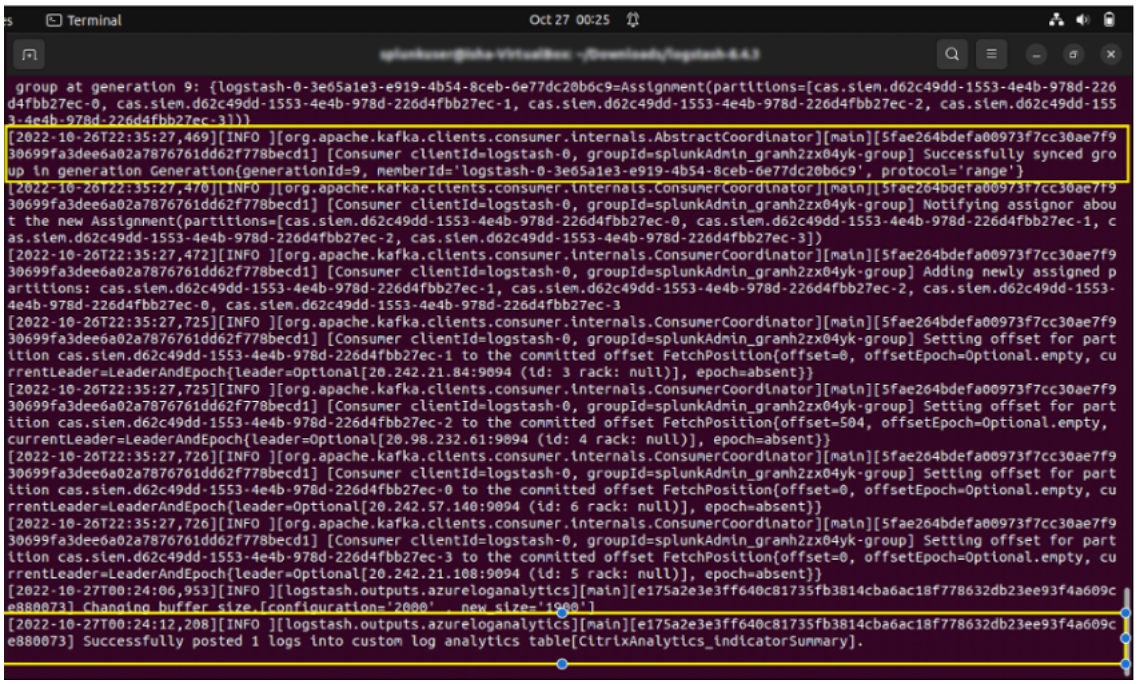
May 9, 2023

この記事では、Logstash を使用して Microsoft Sentinel を Citrix Analytics と統合する際に発生する可能性のある問題を解決するためのヒントを紹介します。詳細については、Kafka または Logstash ベースのデータコネクタを使用した SIEM 統合を参照してください。

Logstash サーバーのログをチェック

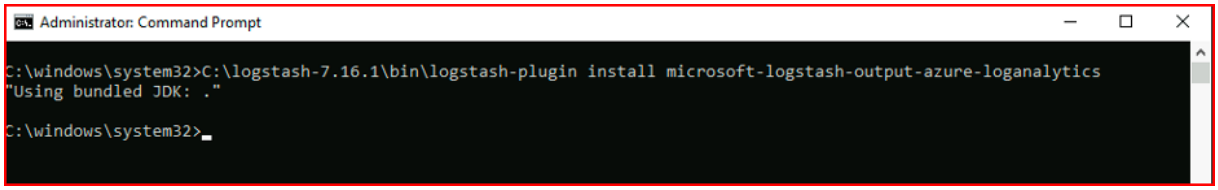
ターミナルウィンドウに表示される Logstash サーバーのログを確認して、データが Sentinel ワークスペースのカスタムログテーブルに正しく取り込まれたかどうかを確認できます。

1. ログの詳細を表示するには、[設定] > [データエクスポート**] > [**設定**]** タブ ****** [**SIEM** 環境の拡張] から Logstash 設定ファイルをダウンロードする必要があります。****Azure Sentinel (**プレビュー**)** で、「**Logstash** 設定ファイルのダウンロード」をクリックします。
2. 設定ファイルを使用して Logstash サーバーを起動すると、同じターミナルウィンドウに、Microsoft Azure がホストする Log Analytics ワークスペースとの接続が成功したことを示す次のログが表示されます。

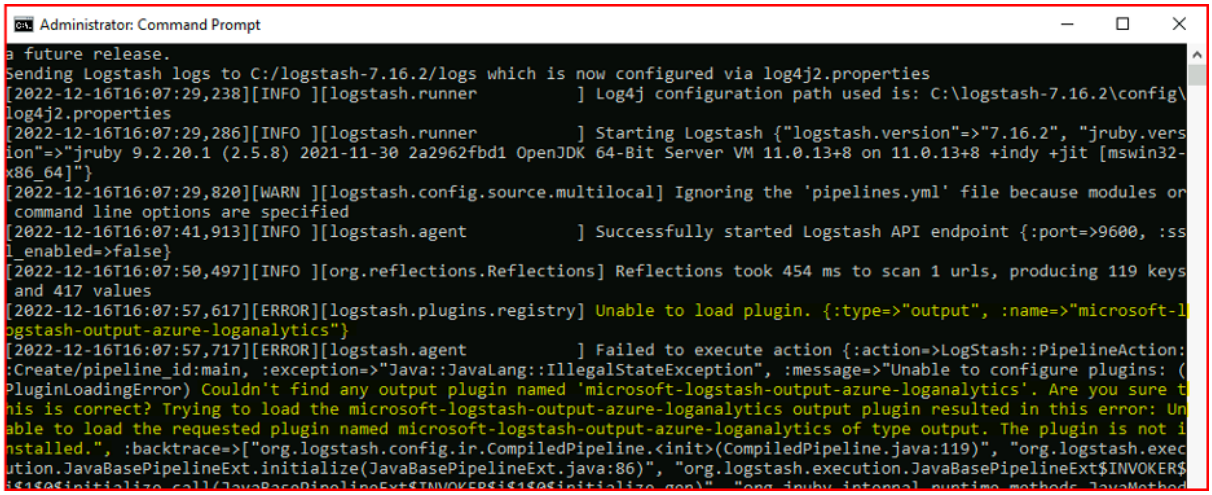


よくあるエラー**:** バンドルされた **JDK** を使用する

Microsoft ログ分析プラグインをインストールしようとすると、一般的に次のようなエラーが報告されます。



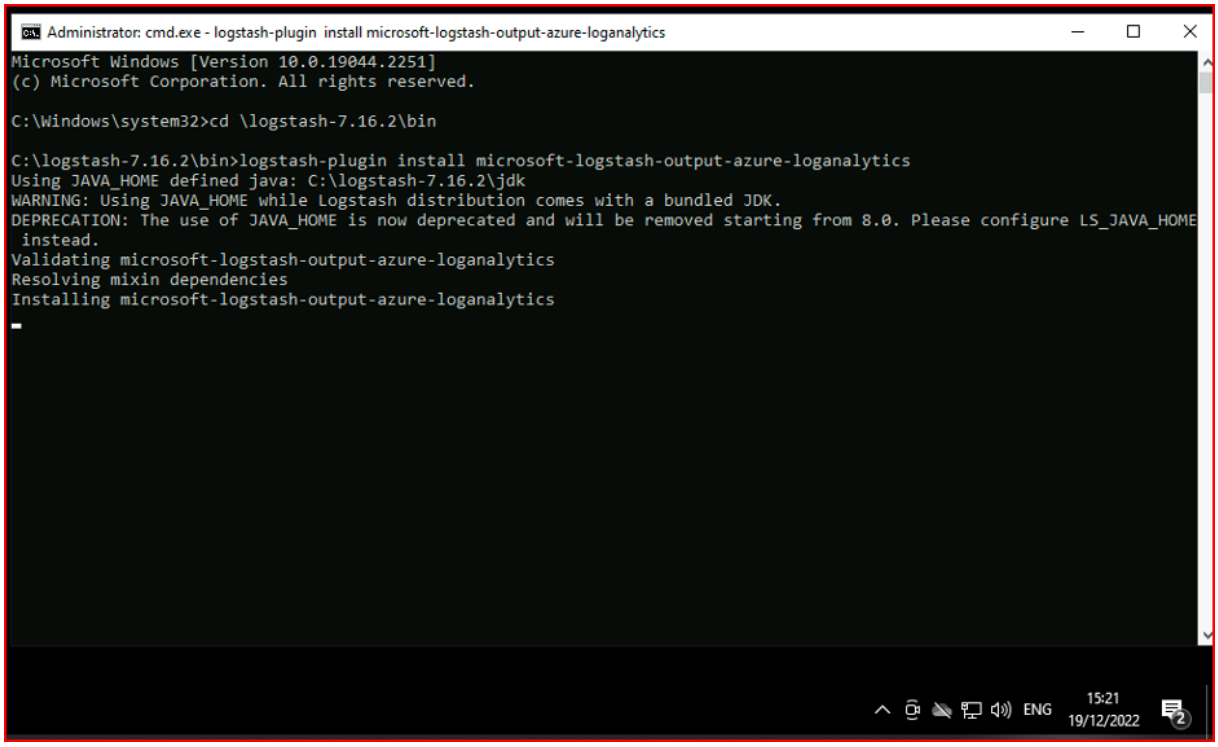
その後、Logstash サーバーを実行しようとすると、次のエラーが表示されることがあります。



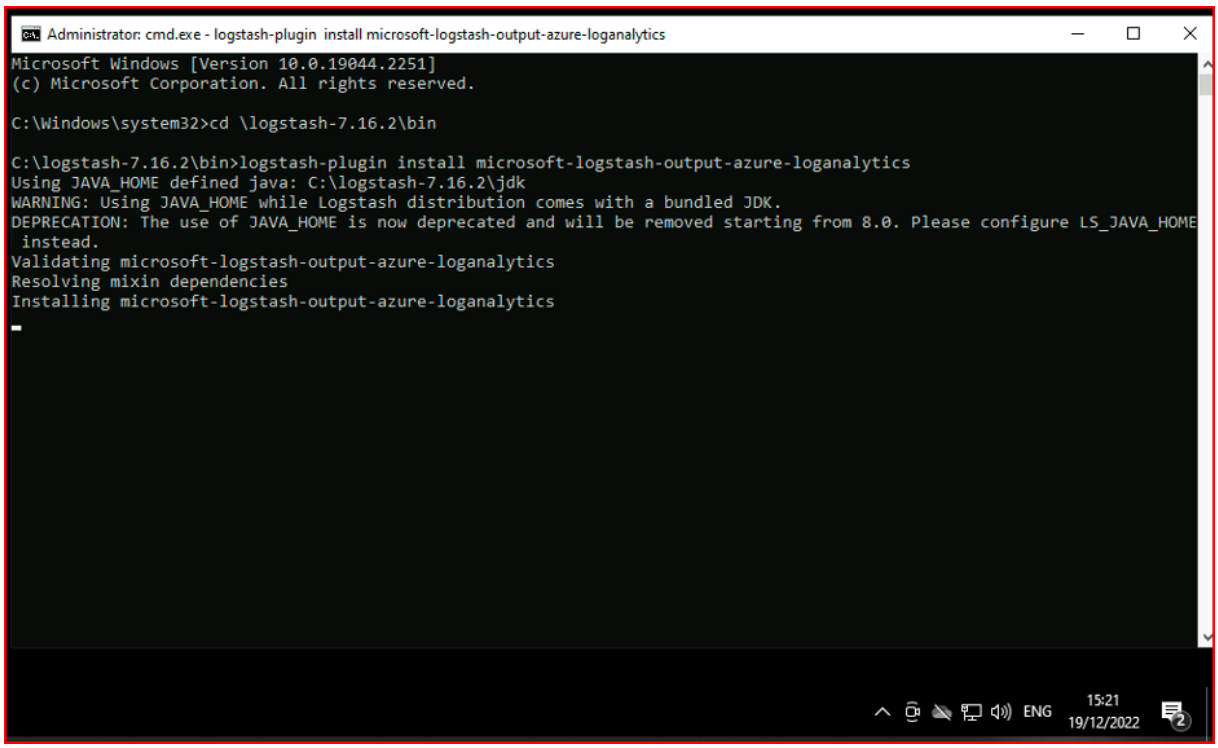
これを解決するには、JAVA_HOME をバンドルされている JDK に設定します。

1. Windows 環境変数に移動
2.「JAVA_HOME」という名前の新しいシステム変数を作成します。
3. < path_to_logstash > バンドルされている Logstash JDK (/Logstash-X.x.x/JDK) にパスを追加してください。

上記の手順を実行した後、プラグインを再インストールしようとすると、次の画面が表示されます。

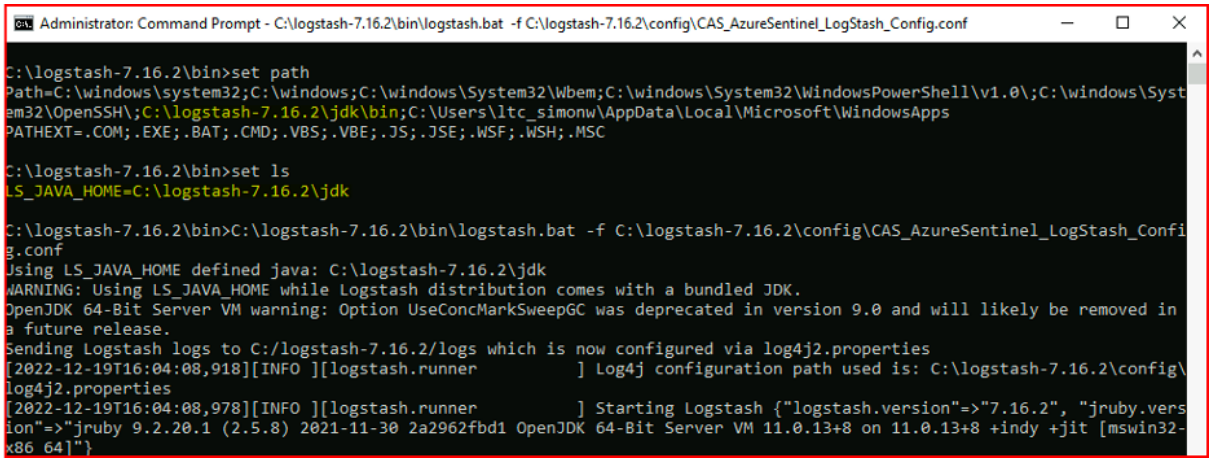


LS_JAVA_HOME を使用する場合は **(JAVA_HOME** は廃止されているため**)**、バンドルされている **JDK** の場所もシステムの **PATH** 変数に指定する必要があります。また、このパスは **(LS_JAVA_HOME** 変数とは異なり**) jdk\bin** フォルダーを指している必要があります。



LS_JAVA_HOME を使用する場合は **(JAVA_HOME** は廃止されているため**)**、バンドルされている **JDK** の場所も

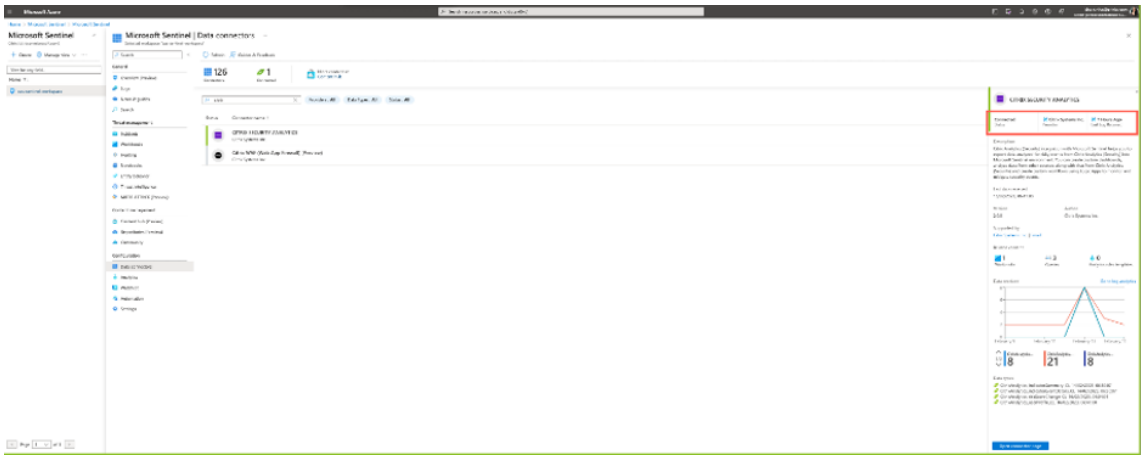
システムの **PATH** 変数に指定する必要があります。また、このパスは **(LS_JAVA_HOME** 変数とは異なり**) jdk\bin** フォルダーを指している必要があります。



Microsoft Sentinel Workbook をチェック

Citrix Analytics から送信されたデータが、ログ分析ワークスペースの適切なカスタムログテーブルに正常に入力されたかどうかを確認するには（Microsoft Sentinel と Citrix Analytics の統合について詳しくは、「Microsoft Sentinel の統合」を参照してください）。

1. **Azure** ポータル **> Microsoft Sentinel >** 適切なワークスペースを選択 **>** データコネクタに移動し、**Citrix SecurityAnalytics** を選択してクリックします。
2. トップバーをチェックして、接続状態を確認します。

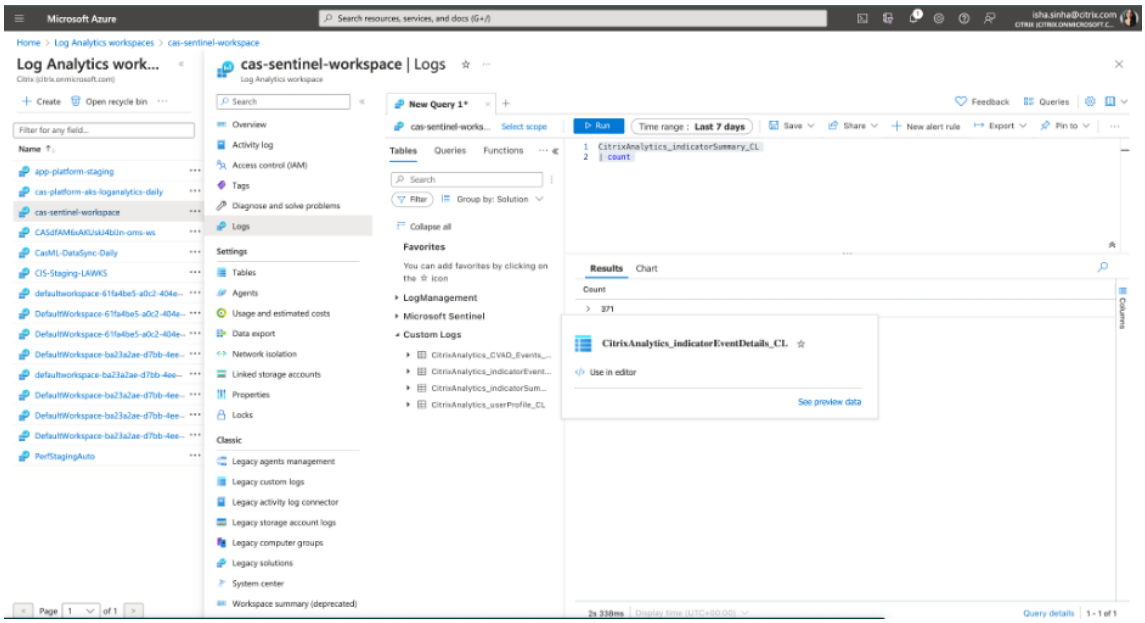


3. ワークブックでは、直感的なフィルターを使用してデータをさらに掘り下げてリスク指標情報を取得できます。情報を取得するには、**Azure** ポータル **> Microsoft Sentinel >** データコネクタ **> CITRIX SECURITY ANALYTICS** ワークブックに移動します。

KQL を使用してログ分析ワークスペースのログを確認する

また、それぞれのカスタムログテーブルで KQL クエリを実行して、正しいデータが LogAnalytics ワークスペースに届いたかどうかを確認することもできます。

1. **Azure** ポータル **> Log Analytics** ワークスペースに移動し、適切なワークスペースを検索します。
2. 左側のパネルで [ログ] を選択し、[テーブル] タブでカスタムログ分析テーブルを検索します。
3. カスタムログ分析テーブルを選択し、[エディターで使用] をクリックします。(ログ分析ワークスペースでの KQL クエリのガイダンスについては、ログ分析チュートリアルを参照してください)。
4. [実行] をクリックします。



Elasticsearch インテグレーション

November 26, 2023

> 注
>
> < CAS-PM-Ext@cloud.com >Elasticsearch の統合、Elasticsearch へのデータのエクスポートに関するサポートのリクエスト、またはフィードバックの提供については、お問い合わせください。

Logstash エンジンを使用して、Citrix Analytics for Security を Elasticsearch と統合します。この統合により、ユーザーのデータを Citrix IT 環境から Elasticsearch にエクスポートして関連付け、組織のセキュリティ体制についてより深い洞察を得ることができます。また、Elasticsearch は、ビジュアライゼーションサービスや Kibana や LogrHhythm などの SIEM でそれぞれ使用できます。

統合の利点と、SIEM に送信される処理済みデータの種類の詳細については、セキュリティ情報とイベント管理の統合を参照してください。

前提条件

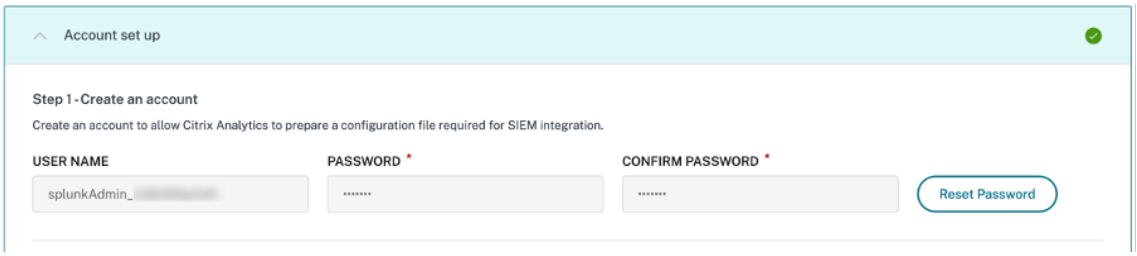
- 少なくとも 1 つのデータソースのデータ処理を有効にします。これは、Citrix Analytics for Security が Elasticsearch 統合プロセスを開始するのに役立ちます。
- ネットワークの許可リストに次のエンドポイントがあることを確認します。

エンドポイント	米国リージョン	欧州連合地域	アジア太平洋南部リージョン
Kafka ブローカー	casnb-0.citrix.com:9094 casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-0.citrix.com:9094 casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-0.citrix.com:9094 casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

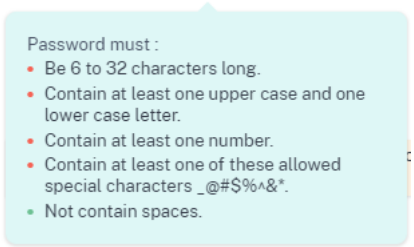
Elasticsearch との統合

1. **[設定] > [データエクスポート]** に移動します。

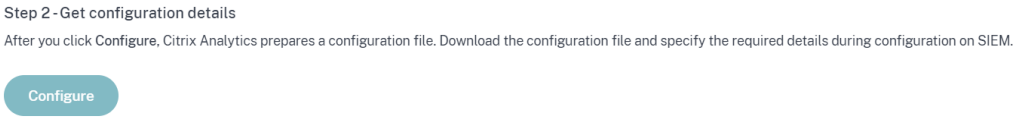
2. アカウント設定セクションで、ユーザー名とパスワードを指定してアカウントを作成します。このアカウントは、統合に必要な設定ファイルの準備に使用されます。



3. パスワードが次の条件を満たしていることを確認します。



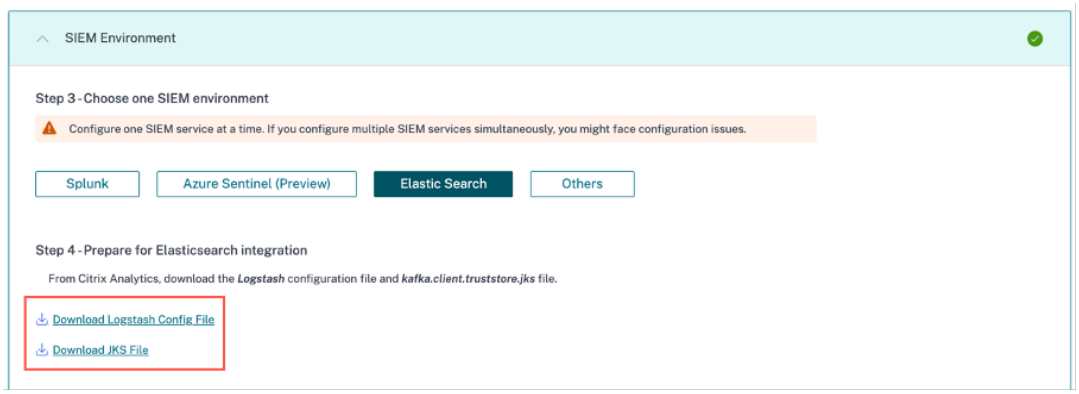
4. [**Configure**] をクリックして Logstash 設定ファイルを生成します。



5. SIEM 環境セクションから **Elastic Search** タブを選択し、設定ファイルをダウンロードします。

   - **Logstash** 構成ファイル: Logstash データ収集エンジンを使用して Citrix Analytics for Security から Elasticsearch にイベントを送信するための構成データ（入力、フィルター、および出力セクション）が含まれています。Logstash の設定ファイルの構造については、Logstash のドキュメントを参照してください。
   - **JKS** ファイル:SSL 接続に必要な証明書が含まれます。

     > 注
     >
     > これらのファイルには機密情報が含まれています。安全な場所に保管してください。



6. Logstash を設定します。

   a) Linux または Windows ホストマシンに Logstashをインストールします。既存の Logstash インスタンスを使用することもできます。

   b) Logstash をインストールしたホストマシンで、次のファイルを指定したディレクトリに配置します。

ホストマシンタイプ	ファイル名	ディレクトリパス
Linux	CAS_Elasticsearch_LogStash_Config.conf	Debian パッケージと RPM パッケージの場合: `/etc/logstash/conf.d/` .zip および.tar.gz アーカイブの場合: `{ extract.path } /config`
	kafka.client.truststore.jks	Debian パッケージと RPM パッケージの場合: `/etc/logstash/ssl/` .zip および.tar.gz アーカイブの場合: `{ extract.path } /ssl`
Windows	CAS_Elasticsearch_LogStash_Config.conf	`C:\Logstash-7.xx.x\config`
	kafka.client.truststore.jks	

   Logstash インストールパッケージのデフォルトディレクトリ構造については、Logstash のドキュメントを参照してください。

   c) Logstash 設定ファイルを開き、次の操作を行います。

      i. ファイルの input セクションに、次の情報を入力します。

- パスワード：Citrix Analytics for Security で構成ファイルを準備するために作成したアカウントのパスワード。
- **SSL** トラストストアの場所:SSL クライアント証明書の場所。これは、ホストマシンの kafka.client.truststore.jks ファイルの場所です。

```
input {
  kafka {
    bootstrap_servers => "
    topics => [
    group_id =>
    session_timeout_ms => 60000
    auto_offset_reset => "earliest"
    security_protocol => "SASL_SSL"
    sasl_mechanism => "SCRAM-SHA-256"
    ssl_endpoint_identification_algorithm => ""
    sasl_jaas_config => "org.apache.kafka.common.security.scram.ScramLoginModule required username='
    ssl_truststore_location => "/etc/logstash/ssl/kafka.client.truststore.jks"
  }
`
```

ii. ファイルの出力セクションに、Elasticsearch が実行されているホストマシンまたはクラスターのアドレスを入力します。

```
}
output {
  elasticsearch {
    hosts => ["<your logstash host : port>"]
    index => "citrixanalytics-%{+YYYY.MM.dd}"
  }
}
```

d) ホストマシンを再起動して、処理されたデータを Citrix Analytics for Security から Elasticsearch に送信します。

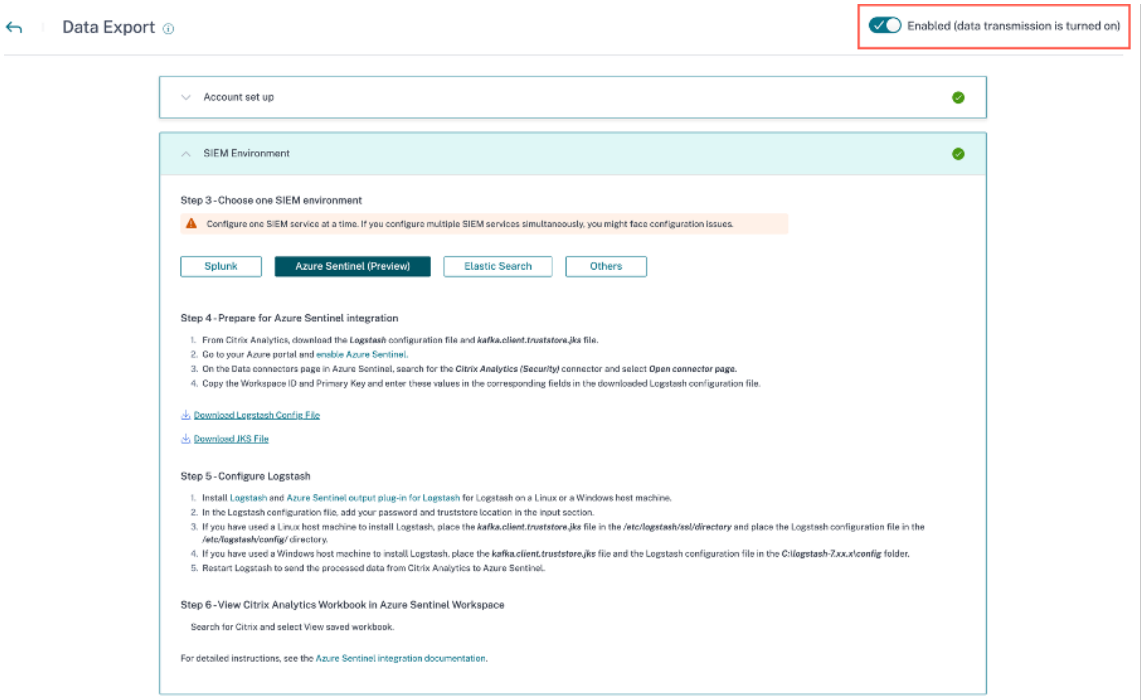
構成が完了したら、Elasticsearch で Citrix Analytics データを表示できることを確認します。

データ伝送をオンまたはオフにする

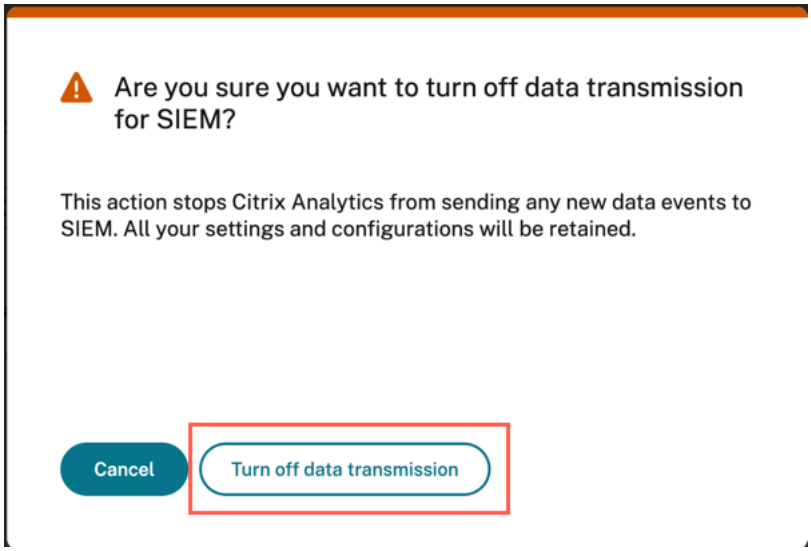
Citrix Analytics for Security が構成ファイルを準備すると、Elasticsearch のデータ転送がオンになります。

セキュリティ向け Citrix Analytics からのデータの送信を停止するには：

1. **[**設定**] > [**データエクスポート**]** に移動します。
2. トグルボタンをオフにしてデータ転送を無効にします。デフォルトでは、データ転送は常に有効になっています。



確認用の警告ウィンドウが表示されます。データ転送を停止するには、[データ転送をオフにする] ボタンをクリックします。



データ転送を再度有効にするには、トグルボタンをオンにします。

Kafka または **Logstash** ベースのデータコネクタを使用した **SIEM** 統合

November 26, 2023

Citrix Analytics for Security SIEM の統合により、ユーザーのデータを Citrix Analytics から SIEM 環境にエクスポートして関連付けることができ、組織のセキュリティ体制についてより深い洞察を得ることができます。

統合の利点と、SIEM に送信されるデータイベントの種類 (リスクインサイトとデータソースイベント) の詳細については、「セキュリティ情報とイベント管理の統合」を参照してください。

Citrix Analytics for Security を SIEM ソリューションと統合するには、次の 2 つのメカニズム（SIEM と IT の導入環境によってサポートされている）を使用します。

1. Kafka エンドポイント経由で接続
2. Kafka ベースのインジェスト機能を備えた Logstash データブローカー経由で接続

前提条件

- 少なくとも 1 つのデータソースのデータ処理を有効にします。これは、Citrix Analytics for Security が SIEM ツールとの統合を開始するのに役立ちます。
- ネットワークの許可リストに次のエンドポイントがあることを確認します。

エンドポイント	米国リージョン	欧州連合地域	アジア太平洋南部リージョン
Kafka ブローカー	casnb-0.citrix.com:9094 casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-0.citrix.com:9094 casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-0.citrix.com:9094 casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

Kafka を使用して **SIEM** サービスと統合する

Kafka はオープンソースソフトウェアで、データのリアルタイムストリーミングに使用されます。Kafka を使用すると、リアルタイムデータを分析してより迅速に洞察を得ることができます。ほとんどの場合、適切なデータを扱う大規模な組織は Kafka を使用しています。

Northbound Kafka は、Citrix Analytics が Kafka エンドポイントを通じてリアルタイムのデータフィードを SIEM のお客様と共有できるようにする内部中間レイヤーです。SIEM が Kafka エンドポイントをサポートしている場合は、Logstash 構成ファイルで提供されるパラメーターと、JKS ファイルまたは PEM ファイルの証明書の詳細を使用して、SIEM を Citrix Analytics for Security に統合します。

Kafka を使用して統合するには、以下のパラメーターが必要です。

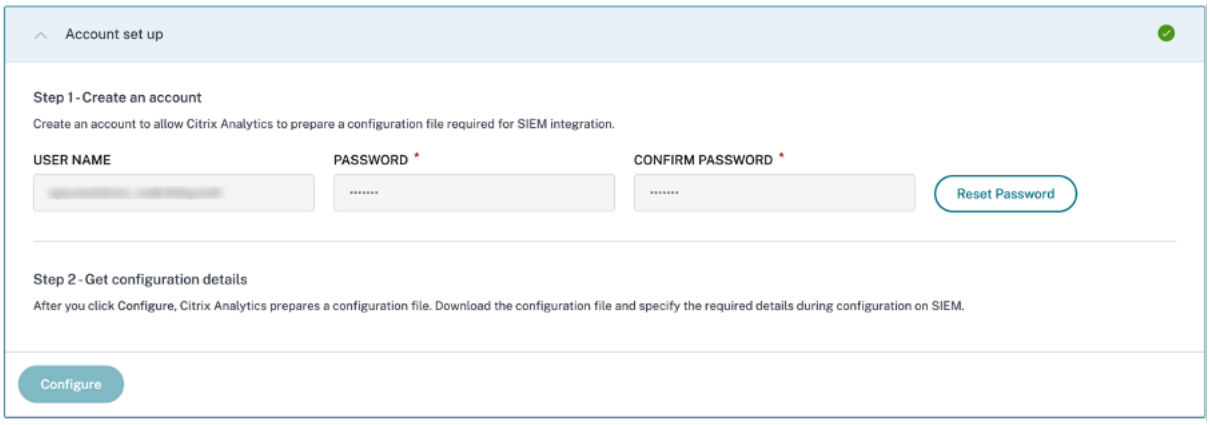
属性名	説明	設定データサンプル
ユーザー名	Kafka から提供されたユーザー名。	`'sasl.username': cas_siem_user_name,`
ホスト	接続する Kafka サーバーのホスト名。	`'bootstrap.servers': cas_siem_host,`
トピック名/クライアント ID	各テナントに割り当てられたクライアント ID。	`'client.id': cas_siem_topic,`
グループ名/ID	コンシューマーが共有するメッセージを読むために必要なグループ名。	`'group.id': cas_siem_group_id,`
セキュリティプロトコル	セキュリティプロトコルの名前。	`'security.protocol': 'SASL_SSL',`
SASL メカニズム	安全な認証を実装するための暗号化に一般的に使用される認証メカニズム。	`'sasl.mechanisms': 'SCRAM-SHA-256',`
SSL トラストストアの場所	証明書ファイルを保存できる場所。クライアントのトラストストアのパスワードはオプションで、空白のままにしておく必要があります。	`'ssl.ca.location': ca_location`
セッションのタイムアウト	Kafka 使用中のクライアント障害の検出に使用されるセッションタイムアウト。	`'session.timeout.ms': 60000,`
自動オフセットリセット	初期オフセットがない場合にトピックパーティションからデータを消費するときの動作を定義します。「最新」、「最新」、「最新」、「なし」などの値を設定できます。	`'auto.offset.reset': 'earliest',`

次に、設定出力の例を示します。

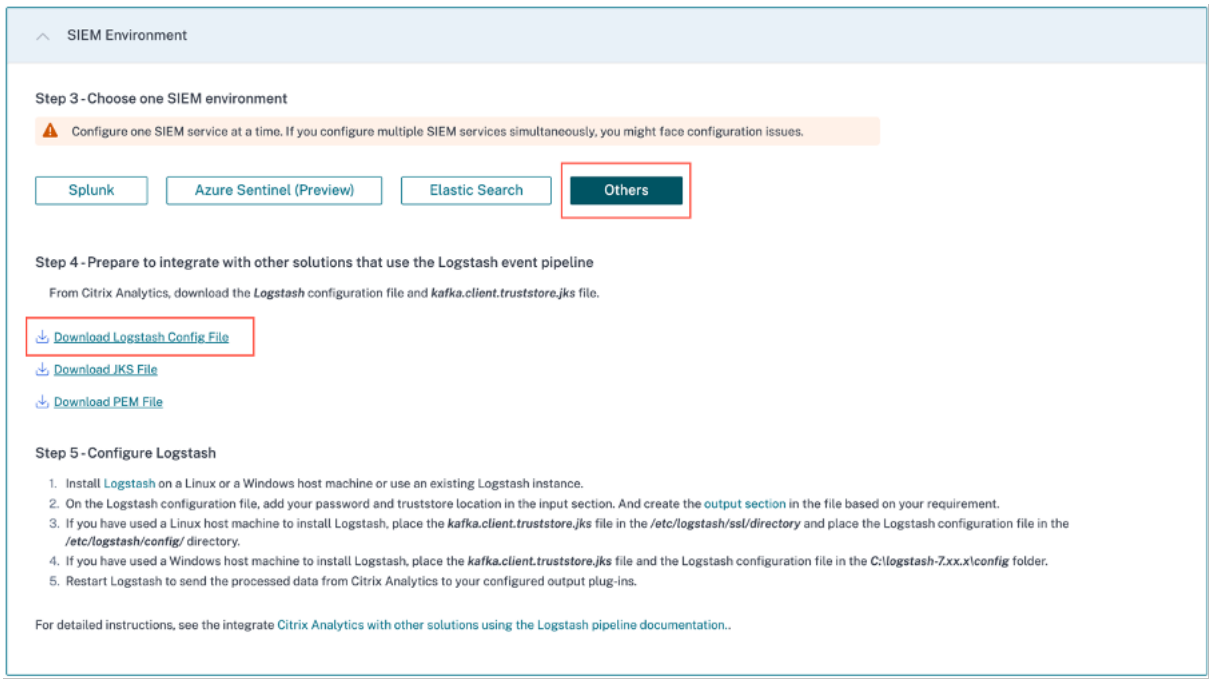
```
{
 'bootstrap.servers': cas_siem_host,
                      'client.id': cas_siem_topic,
                      'group.id': cas_siem_group_id,
                      'session.timeout.ms': 60000,
                      'auto.offset.reset': 'earliest',
                      'security.protocol': 'SASL_SSL',
                      'sasl.mechanisms': 'SCRAM-SHA-256',
                      'sasl.username': cas_siem_user_name,
```



```
                    'sasl.password': self.CLEAR_PASSWORD,
                    'ssl.ca.location': ca_location
                }


<!--NeedCopy-->
```



前述のパラメータは Logstash 設定ファイルにあります。設定ファイルをダウンロードするには、[設定] **> [**データエクスポート**] > [SIEM** 環境] に移動し、[その他] タブを選択し、[**Logstash** 設定ファイルのダウンロード] をクリックします。



設定値についての理解/詳細については、「設定」を参照してください。

データフロー

認証データ通信は、Kafka サーバー側のブローカー（セキュリティクラウド向け Citrix Analytics）と Kafka クライアントの間で行われます。すべてのブローカー/外部クライアントの通信は、有効化された SASL_SSL セキュリティプロトコルとパブリックアクセス用のターゲット 9094 ポートを使用します。

Apache Kafka には、SSL 暗号化を使用して送信中のデータを暗号化するセキュリティコンポーネントがあります。暗号化が有効で SSL 証明書が設定されている場合、ネットワーク上のデータ送信は暗号化され、保護されます。SSL 経由で送信されるパケットを復号化できるのは、最初と最後のマシンだけです。

[認証**]**

認証には、次の 2 つのレベルがあります。

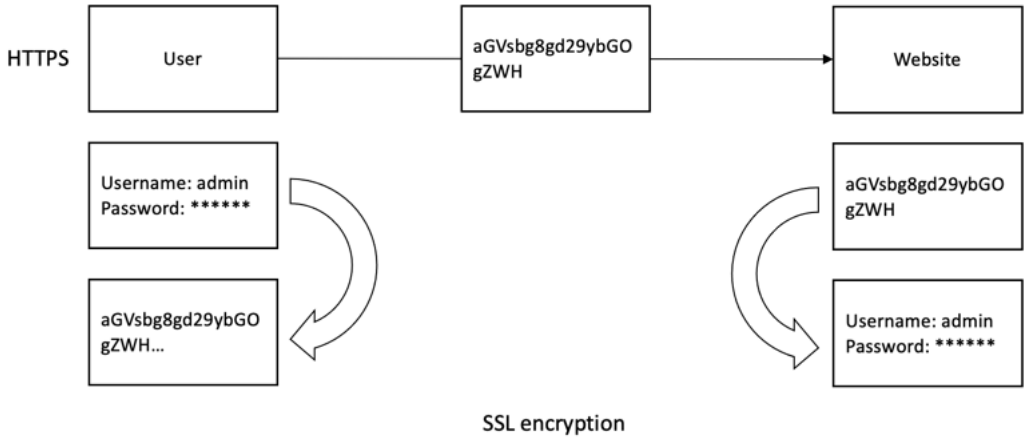
1. TLS/クライアントとサーバー間。
    - クライアントとサーバー間の TLS 認証交換用のサーバー証明書 (公開鍵)。
    - クライアントベースの認証または双方向認証はサポートされていません (クライアントの秘密鍵証明書が必要です)。
2. トピック/エンドポイントへのアクセス制御用のユーザー名/パスワード
    - 特定のクライアントが特定の顧客トピックのみを読むことができるようにする
    - ユーザー名/パスワード認証メカニズムには SASL/SCRAM と TLS 暗号化を使用して安全な認証を実装します。

SSL による暗号化と **SASL/SSL&SASL/**プレーンテキストによる認証

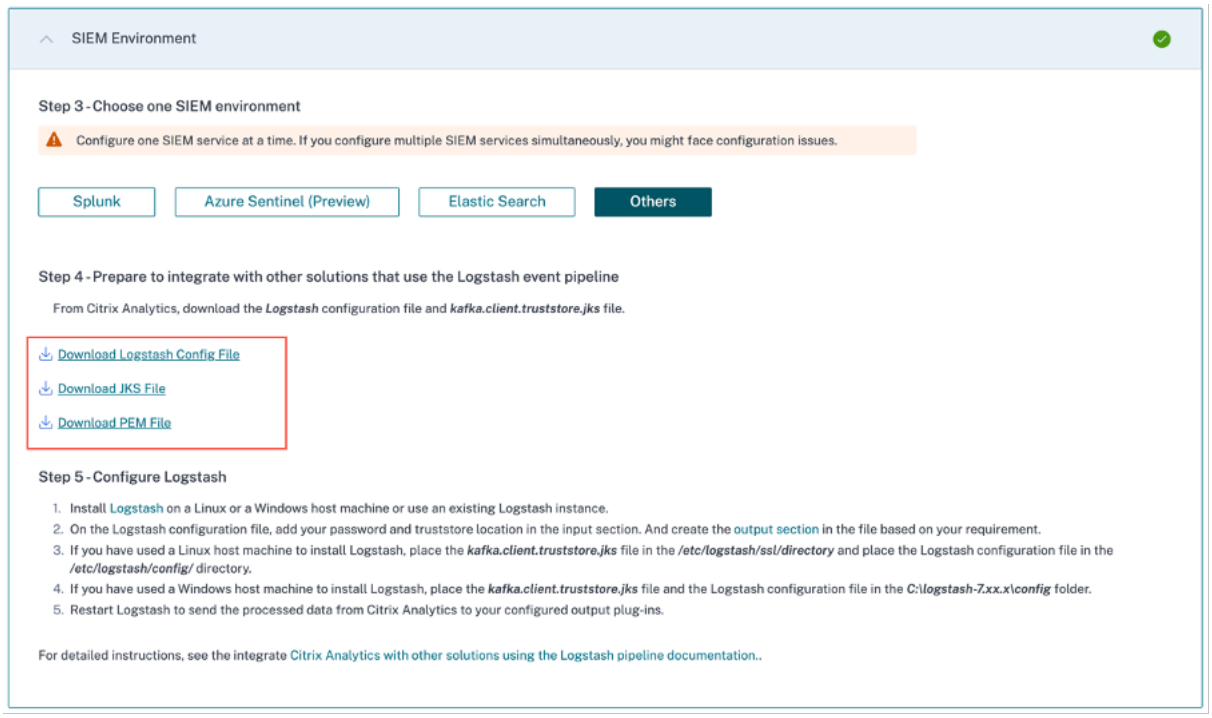
デフォルトでは、Apache Kafka はプレーンテキストで通信します。プレーンテキストでは、すべてのデータが平文で送信され、どのルーターもデータコンテンツを読み取ることができます。Apache Kafka には、SSL 暗号化を使用して送信中のデータを暗号化するセキュリティコンポーネントがあります。暗号化を有効にし、SSL 証明書を慎重に設定すると、データが暗号化され、ネットワーク上で安全に転送されるようになりました。SSL 暗号化では、送信されるパケットを復号化できるのは、最初と最後のマシンだけです。

双方向 SSL 暗号化が使用されているため、ユーザー名/パスワードによるログインは外部通信にとって安全です。

暗号化は実行中のみで、データは暗号化されずにブローカーのディスクに残ります。



クライアント構成では、クライアントのトラストストア JKS ファイルと (トラストストア jks ファイルから変換された) PEM ファイルが必要です。これらのファイルは、次のスクリーンショットに示すように、Citrix Analytics for Security GUI からダウンロードできます。



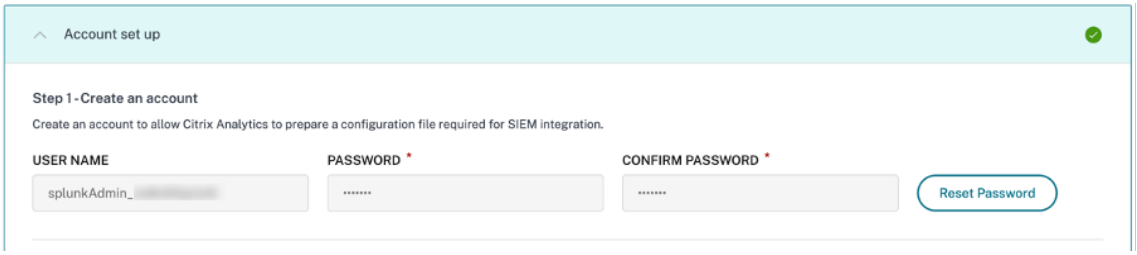
ログスタッシュを使った **SIEM** インテグレーション

SIEM が Kafka エンドポイントをサポートしていない場合は、**Logstash** データ収集エンジンを使用できます。Citrix Analytics for Security のデータイベントを、Logstash がサポートする出力プラグインのいずれかに送信できます 。

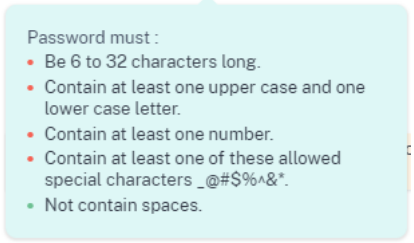
以下のセクションでは、Logstash を使用して SIEM を Citrix Analytics for Security と統合するために実行する必要のある手順について説明します。

Logstash を使用して **SIEM** サービスと統合する

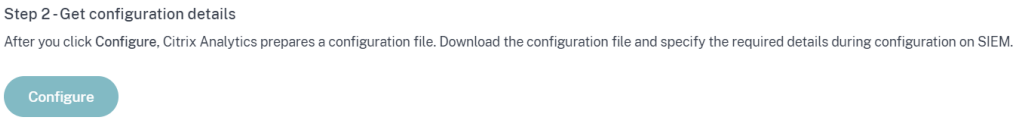
1. **[設定] > [データエクスポート]** に移動します。
2. アカウント設定ページで、ユーザー名とパスワードを指定してアカウントを作成します。このアカウントは、統合に必要な設定ファイルの準備に使用されます。



3. パスワードが次の条件を満たしていることを確認します。



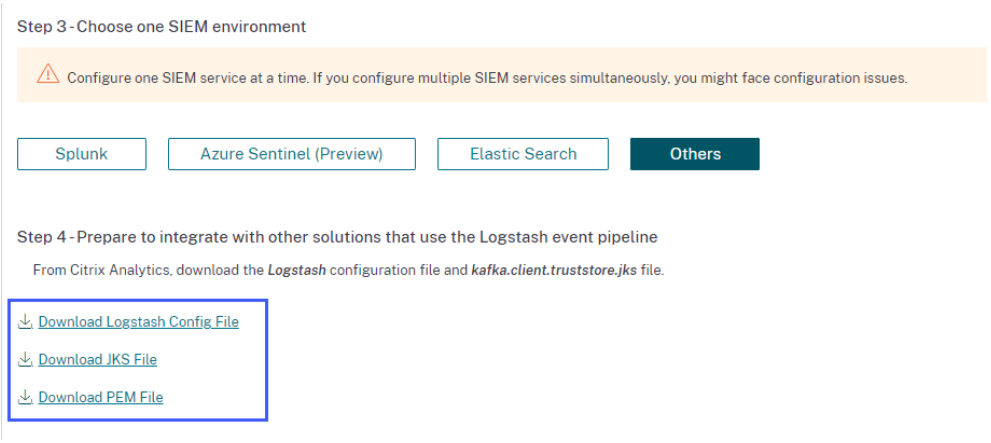
4. [**Configure**] を選択して Logstash 設定ファイルを生成します。



5. [**Others**] タブを選択して、設定ファイルをダウンロードします。

   - **Logstash** 構成ファイル: このファイルには、Logstash データ収集エンジンを使用して Citrix Analytics for Security からイベントを送信するための構成データ（入力、フィルター、および出力セクション）が含まれます。Logstash の設定ファイルの構造については、Logstash のドキュメントを参照してください。
   - **JKS** ファイル: このファイルには、SSL 接続に必要な証明書が含まれています。このファイルは、Logstash を使用して SIEM を統合する場合に必要です。
   - **PEM** ファイル: このファイルには、SSL 接続に必要な証明書が含まれています。このファイルは、Kafka を使用して SIEM を統合する場合に必要です。

     > 注
     >
     > これらのファイルには機密情報が含まれています。安全な場所に保管してください。



6. Logstash を設定します。

   a) Linux または Windows のホストマシンに、Logstash をインストールします （Citrix Analytics for Security との互換性がテストされたバージョン: v7.17.7 および v8.5.3)。既存の Logstash インスタンスを使用することもできます。

   b) Logstash をインストールしたホストマシンで、次のファイルを指定したディレクトリに配置します。

ホストマシンタイプ	ファイル名	ディレクトリパス
Linux	CAS_Others_LogStash_Config.config	Debian パッケージと RPM パッケージの場合: `/etc/logstash/conf.d/` .zip および.tar.gz アーカイブの場合: `{ extract.path } /config`
	kafka.client.truststore.jks	Debian パッケージと RPM パッケージの場合: `/etc/logstash/ssl/` .zip および.tar.gz アーカイブの場合: `{ extract.path } /ssl`
Windows	CAS_Others_LogStash_Config.config	`C:\logstash-7.xx.x\config`
	kafka.client.truststore.jks	`C:\logstash-7.xx.x\config`

   c) Logstash 設定ファイルには、Kafka 認証情報、LogAnalytics ワークスペース ID、プライマリキーなどの機密情報が含まれています。これらの機密認証情報はプレーンテキストとして保存しないことをお

勧めします。統合を確実にするために、Logstash キーストアを使用してキーにそれぞれの値を追加し、そのキーを設定ファイル内のキー名を使用して参照できます。Logstash キーストアの詳細と、これによって設定のセキュリティがどのように強化されるかについては、「Secrets キーストアによる安全な設定」を参照してください。

d) Logstash 設定ファイルを開き、次の操作を行います。

ファイルの input セクションに、次の情報を入力します。

- パスワード: Citrix Analytics for Security で構成ファイルを準備するために作成したアカウントのパスワード。
- **SSL** トラストストアの場所:SSL クライアント証明書の場所。これは、ホストマシンの kafka.client.truststore.jks ファイルの場所です。

```
input {
  kafka {
    bootstrap_servers => "
    topics => ["
    group_id => "
    session_timeout_ms => 60000
    auto_offset_reset => "earliest"
    security_protocol => "SASL_SSL"
    sasl_mechanism => "SCRAM-SHA-256"
    ssl_endpoint_identification_algorithm => ""
    sasl_jaas_config => "org.apache.kafka.common.security.scram.ScramLoginModule required username='
    ssl_truststore_location => "/etc/logstash/ssl/kafka.client.truststore.jks"
  }
}
```

ファイルの出力セクションに、データを送信する宛先パスまたは詳細を入力します。出力プラグインについては、Logstash のドキュメントを参照してください。

次のスニペットは、出力がローカルログファイルに書き込まれることを示しています。

```
output {
        file {
        path => "./citrixanalytics-%{+YYYY.MM.dd}.log"
    }
}
```

e) ホストマシンを再起動して、処理されたデータを Citrix Analytics for Security から SIEM サービスに送信します。

構成が完了したら、SIEM サービスにログインし、SIEM の Citrix Analytics データを確認します。

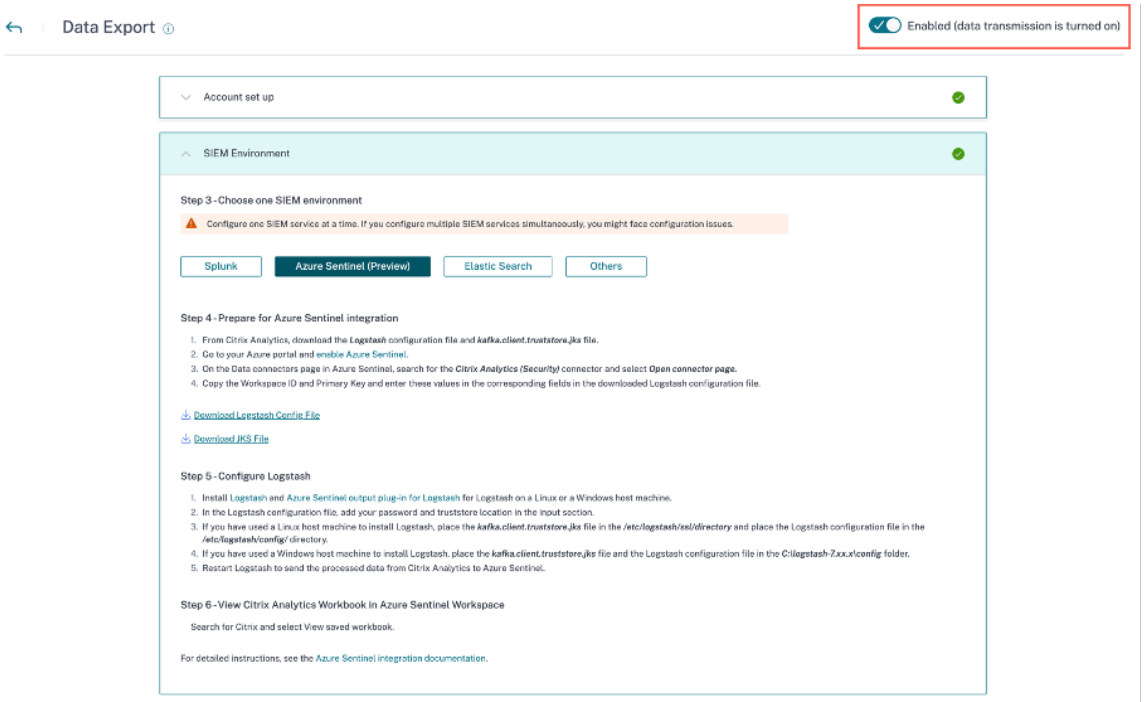
データ伝送をオンまたはオフにする

Citrix Analytics for Security が構成ファイルを準備すると、SIEM のデータ転送がオンになります。

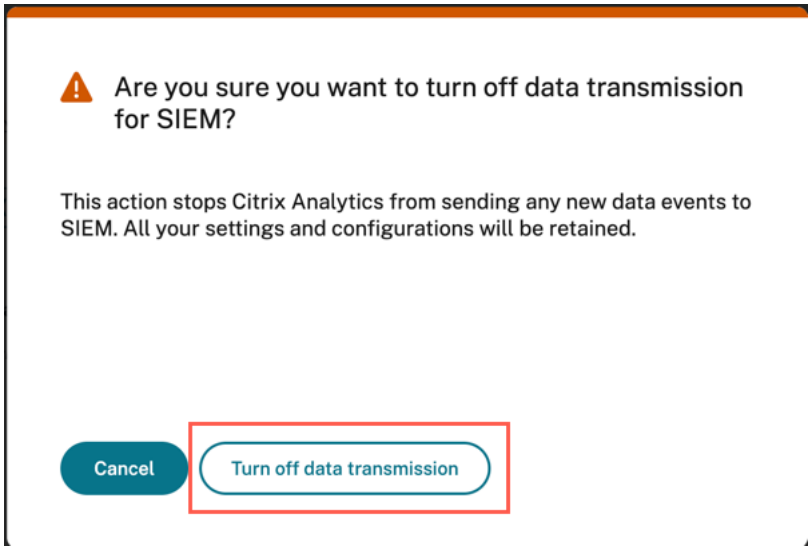
セキュリティ向け Citrix Analytics からのデータの送信を停止するには:

1. **[設定] > [データエクスポート]** に移動します。

2. トグルボタンをオフにしてデータ転送を無効にします。デフォルトでは、データ転送は常に有効になっています。



確認用の警告ウィンドウが表示されます。データ送信を停止するには、[データ送信をオフにする] ボタンをクリックします。



データ転送を再度有効にするには、トグルボタンをオンにします。

> 注
>
> < CAS-PM-Ext@cloud.com >SIEM 統合、SIEM へのデータのエクスポートに関するサポートの依頼、またはフィードバックの提供については、お問い合わせください。

SIEM 用の Citrix Analytics データエクスポート形式

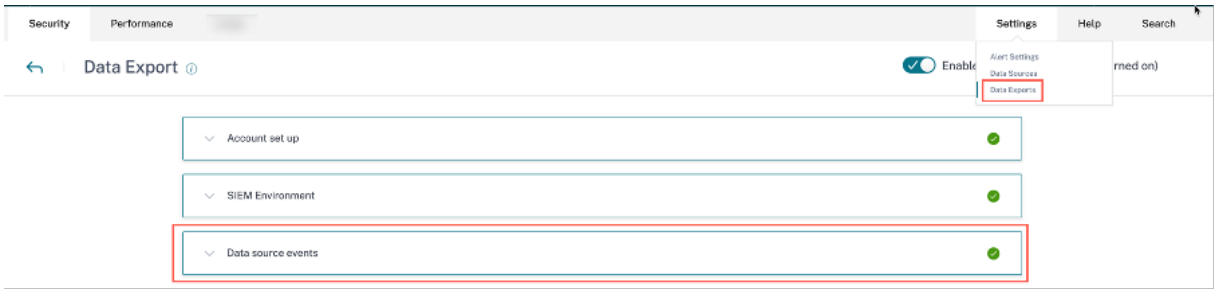
February 14, 2024

Citrix Analytics for Security では、セキュリティ情報およびイベント管理（SIEM）サービスと統合できます。この統合により、Citrix Analytics for Security は SIEM サービスにデータを送信できるようになり、組織のセキュリティリスク状況に関する洞察を得るのに役立ちます。

現在、セキュリティ向け Citrix Analytics を次の SIEM サービスと統合できます。

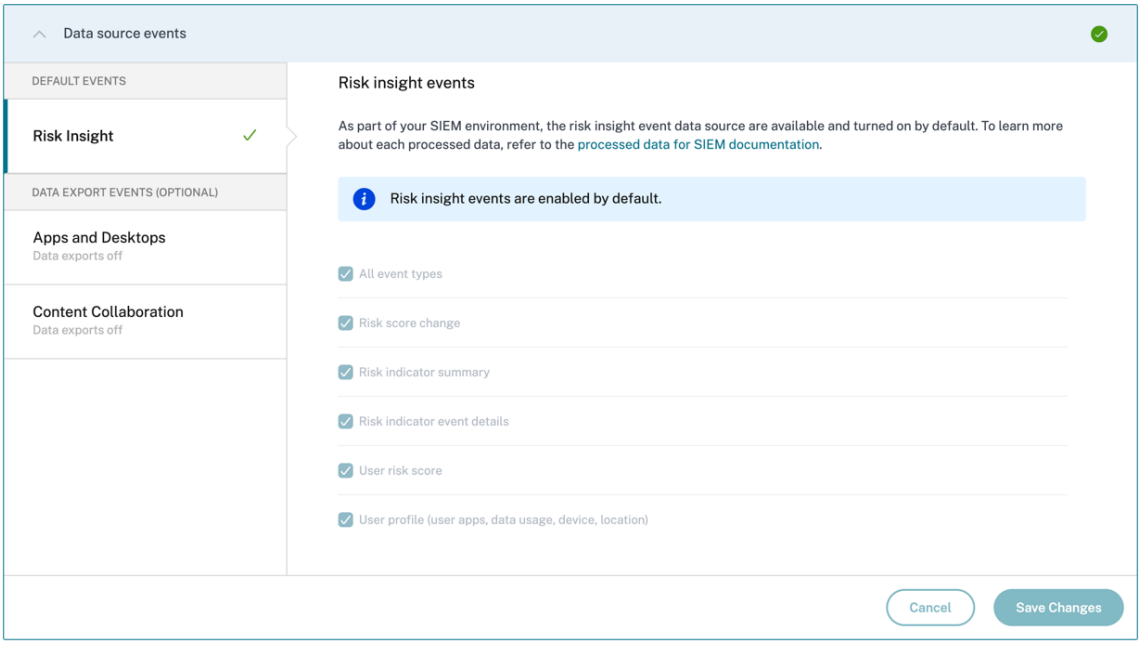
- Splunk
- Microsoft Azure Sentinel
- Elasticsearch
- Kafka または Logstash ベースのデータコネクタを使用する他の SIEM

[データエクスポート] オプションが **[**設定**]** でグローバルに利用できるようになりました。データソースイベントを表示するには、[設定**] > [**データエクスポート**] > [**データソースイベント] に移動します。



Citrix Analytics for Security から SIEM サービスに送信されるリスクインサイトデータには、次の 2 つのタイプがあります。

- リスクインサイトイベント (デフォルトエクスポート)
- データソースイベント (オプションのエクスポート)



SIEM のリスクインサイトデータ

アカウント設定と SIEM 設定が完了すると、デフォルトのデータセット（リスクインサイトイベント）が SIEM デプロイメントに流れ始めます。リスクインサイトデータセットには、ユーザーリスクスコアイベント、ユーザープロファイルイベント、およびリスク指標アラートが含まれます。これらは、Citrix Analytics の機械学習アルゴリズムとユーザー行動分析によって、ユーザーイベントを活用して生成されます。

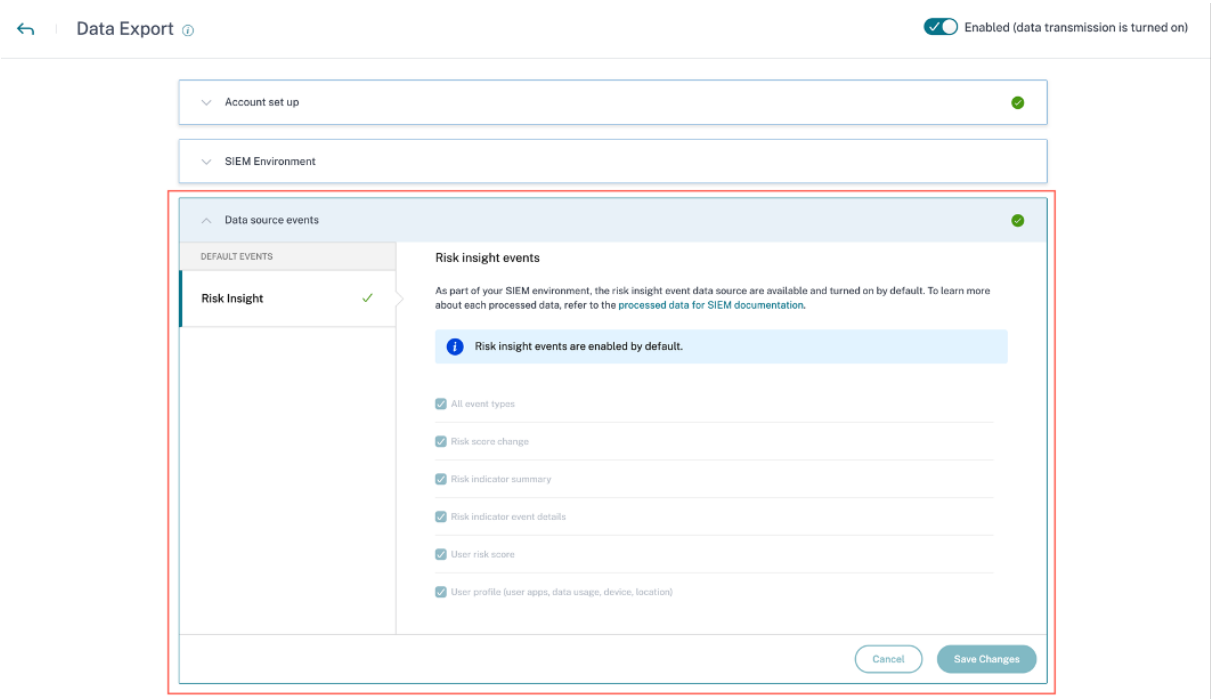
ユーザーのリスクインサイトデータセットには次のものが含まれます:

- リスクスコアの変更: ユーザーのリスクスコアの変化を示します。ユーザーのリスクスコアの変化が 3 以上で、この変化が何らかの割合で増加するか、10%以上低下した場合、データは SIEM サービスに送信されます。
- リスク指標の概要: ユーザーに対してトリガーされたリスク指標の詳細。
- リスク指標イベントの詳細: リスク指標に関連するユーザーイベント。Citrix Analytics は、リスク指標の発生ごとに最大 1000 個のイベント詳細を SIEM サービスに送信します。これらのイベントは発生順に送信されます。
- ユーザーリスクスコアイベント**:** ユーザーの現在のリスクスコア。Citrix Analytics for Security は、このデータを 12 時間ごとに SIEM サービスに送信します。
- ユーザープロファイル: ユーザープロファイルデータは次のように分類できます:
  - ユーザーアプリ: ユーザーが起動して使用したアプリケーション。Citrix Analytics for Security は、このデータを Citrix Virtual Apps から取得し、12 時間ごとに SIEM サービスに送信します。
  - ユーザーデバイス: ユーザーに関連付けられているデバイス。Citrix Analytics for Security は、Citrix Virtual Apps と Citrix Endpoint Management からこのデータを取得し、12 時間ごとに SIEM サービスに送信します。

- ユーザーの所在地: ユーザーが最後に検出された都市。Citrix Analytics for Security は、このデータを Citrix Virtual Apps and Desktops および Citrix DaaS（旧 Citrix Virtual Apps and Desktops サービス）から取得します。Citrix Analytics for Security は、この情報を 12 時間ごとに SIEM サービスに送信します。
- ユーザークライアント **IP**: ユーザーデバイスのクライアント IP アドレス。Citrix Analytics for Security は、このデータを Citrix Virtual Apps and Desktops および Citrix DaaS（以前の Citrix Virtual Apps and Desktops サービス）から取得し、この情報を 12 時間ごとに SIEM サービスに送信します。

データソースのイベントプリファレンスを表示することはできるが、設定できない場合は、必要な管理者権限がありません。
詳細については、「セキュリティアナリティクスの管理者ロールの管理」を参照してください。

次の例では、[変更を保存] ボタンが無効になっています。リスクインサイトイベントはデフォルトで有効になっています。



リスクインサイトイベントのスキーマ詳細

次のセクションでは、Citrix Analytics for Security によって生成される処理されたデータのスキーマについて説明します。

> 注
>
> 以下のスキーマサンプルに示されているフィールド値は、表現のみを目的としています。実際のフィールドの値は、ユーザープロファイル、ユーザーイベント、およびリスク指標によって異なります。

次の表では、すべてのユーザープロファイルデータ、ユーザーリスクスコア、およびリスクスコアの変更について、スキーマ全体で共通するフィールド名を示します。

フィールド名	説明
entity_id	エンティティに関連付けられている ID。この場合、エンティティはユーザーです。
entity_type	リスクにさらされているエンティティ。この場合、エンティティはユーザーです。
event_type	SIEM サービスに送信されるデータのタイプ。たとえば、ユーザーの場所、ユーザーのデータ使用状況、ユーザーのデバイスアクセス情報などです。
tenant_id	顧客の一意のアイデンティティ。
timestamp	最近のユーザーアクティビティの日時。
version	処理されたデータのスキーマのバージョン。現在のスキーマのバージョンは 2 です。

ユーザープロファイルデータスキーマ

ユーザーロケーションスキーマ

```
{

  "tenant_id": "demo_tenant", "entity_id": "demo_user", "entity_type":
     "user", "timestamp": "2021-02-10T15:00:00Z", "event_type": "
     userProfileLocation", "country": "India", "city": "Bengaluru", "
     cnt": 4, "version": 2
   }


<!--NeedCopy-->
```

ユーザーロケーションのフィールドの説明

フィールド名	説明
event_type	SIEM サービスに送信されるデータのタイプ。この場合、イベントタイプはユーザーのロケーションです。
country	ユーザーがログインした国。
city	ユーザーがログインした市区町村。
cnt	過去 12 時間内にロケーションにアクセスされた回数。

ユーザークライアント **IP** スキーマ


```
{

  "client_ip": "149.147.136.10",
  "cnt": 3,
  "entity_id": "r2_up_user_1",
  "entity_type": "user",
  "event_type": "userProfileClientIps",
  "tenant_id": "xaxddaily1",
  "timestamp": "2023-09-18T10:45:00Z",
  "version": 2
 }



<!--NeedCopy-->
```

クライアント IP のフィールド説明

フィールド名	説明
client_ip	ユーザーデバイスの IP アドレス。
cnt	過去 12 時間にユーザーがデバイスにアクセスした回数。
entity_id	エンティティに関連付けられている ID。この場合、エンティティはユーザーです。
entity_type	リスクにさらされているエンティティ。この場合、イベントタイプはユーザーのクライアント IP です。
event_type	SIEM サービスに送信されるデータのタイプ。例: ユーザーの位置情報、ユーザーのデータ使用量、ユーザーのデバイスアクセス情報。
tenant_id	顧客の一意のアイデンティティ。
timestamp	最近のユーザーアクティビティの日付と時刻。
version	処理されたデータのスキーマのバージョン。現在のスキーマのバージョンは 2 です。

ユーザーデータ使用スキーマ

```
{

  "data_usage_bytes": 87555255, "deleted_file_cnt": 0, "
     downloaded_bytes": 87555255, "downloaded_file_cnt": 5, "entity_id"
     : "demo@demo.com", "entity_type": "user", "event_type": "
     userProfileUsage", "shared_file_cnt": 0, "tenant_id": "demo_tenant
     ", "timestamp": "2021-02-10T21:00:00Z", "uploaded_bytes": 0, "
     uploaded_file_cnt": 0, "version": 2
   }



```



```
<!--NeedCopy-->
```

ユーザーデータの使用に関するフィールドの説明

フィールド名	説明
data_usage_bytes	ユーザーが使用するデータの量 (バイト単位)。これは、ユーザーのダウンロードおよびアップロードされたボリュームの集合体です。
deleted_file_cnt	ユーザーが削除したファイルの数。
downloaded_bytes	ユーザーがダウンロードしたデータの量。
downloaded_file_count	ユーザーがダウンロードしたファイルの数。
event_type	SIEM サービスに送信されるデータのタイプ。この場合、イベントタイプはユーザーの使用プロファイルです。
shared_file_count	ユーザーが共有するファイルの数。
uploaded_bytes	ユーザーがアップロードしたデータの量。
uploaded_file_cnt	ユーザーがアップロードしたファイルの数。

ユーザーデバイススキーマ

```
{

  "cnt": 2, "device": "user1612978536 (Windows)", "entity_id": "demo",
     "entity_type": "user", "event_type": "userProfileDevice", "
     tenant_id": "demo_tenant", "timestamp": "2021-02-10T21:00:00Z", "
     version": 2
   }


<!--NeedCopy-->
```

ユーザーデバイスのフィールドの説明。

フィールド名	説明
cnt	過去 12 時間以内にデバイスにアクセスされた回数。
device	デバイスの名前。
event_type	SIEM サービスに送信されるデータのタイプ。この場合、イベントタイプはユーザーのデバイスアクセス情報です。

ユーザーアプリスキーマ

```
{

```



```
3    "tenant_id": "demo_tenant", "entity_id": "demo", "entity_type": "user
        ", "timestamp": "2021-02-10T21:00:00Z", "event_type": "
        userProfileApp", "version": 2, "session_domain": "99
        e38d488136f62f828d4823edd120b4f32d724396a7410e6dd1b0", "
        user_samaccountname": "testnameeikragz779", "app": "
        Chromeeikragz779", "cnt": 189
4     }
5
6
7  <!--NeedCopy-->
```

ユーザーアプリのフィールドの説明。

フィールド名	説明
event_type	SIEM サービスに送信されるデータのタイプ。この場合、イベントタイプはユーザーのデバイスアクセス情報です。
session_domain	ユーザーがログオンしたセッションの ID。
user_samaccountname	Windows NT 4.0、Windows 95、Windows 98、および LAN マネージャなど、以前のバージョンの Windows からのクライアントおよびサーバのログオン名。この名前は、Citrix StoreFront にログオンし、リモートの Windows マシンにもログオンするために使用されます。
app	ユーザーがアクセスするアプリケーションの名前。
cnt	過去 12 時間内にアプリケーションにアクセスされた回数。

ユーザリスクスコアスキーマ

```
1  {
2
3    "cur_riskscore": 7, "entity_id": "demo", "entity_type": "user", "
        event_type": "userProfileRiskscore", "last_update_timestamp": "
        2021-01-21T16:14:29Z", "tenant_id": "demo_tenant", "timestamp": "
        2021-02-10T20:45:00Z", "version": 2
4     }
5
6
7  <!--NeedCopy-->
```

ユーザーリスクスコアのフィールドの説明。

フィールド名	説明
cur_riskscore	ユーザーに割り当てられている現在のリスクスコア。リスクスコアは、ユーザーのアクティビティに関連する脅威の重要度に応じて、0 ～100 の範囲で変化します。
event_type	SIEM サービスに送信されるデータのタイプ。この場合、イベントタイプはユーザーのリスクスコアです。
last_update_timestamp	ユーザーのリスクスコアが最後に更新された時刻。
timestamp	ユーザーリスクスコアイベントが収集され、SIEM サービスに送信される時刻。このイベントは 12 時間ごとに SIEM サービスに送信されます。

リスクスコア変更スキーマ

サンプル **1**:

```
{

  "alert_message": "Large risk score drop percent since last check", "
     alert_type": "riskscore_large_drop_pct", "alert_value": -21.73913,
      "cur_riskscore": 18, "entity_id": "demo_user", "entity_type": "
     user", "event_type": "riskScoreChange", "tenant_id": "demo_tenant"
     , "timestamp": "2021-02-11T05:45:00Z", "version": 2
   }


<!--NeedCopy-->
```

サンプル **2**:

```
{

  "alert_message": "Risk score increase since last check", "alert_type"
     : "riskscore_increase", "alert_value": 39.0, "cur_riskscore": 76,
     "entity_id": "demo_user", "entity_type": "user", "event_type": "
     riskScoreChange", "tenant_id": "demo_tenant", "timestamp": "
     2021-02-11T03:45:00Z", "version": 2
   }


<!--NeedCopy-->
```

リスクスコア変更のフィールドの説明。

フィールド名	説明
alert_message	リスクスコアの変更に対して表示されるメッセージ。
alert_type	アラートがリスクスコアの増加またはリスクスコアの割合の大幅な低下を示すかどうかを示します。ユーザーのリスクスコアの変更が 3 以上で、この変更が任意の割合で増加するか 10% を超えると、データは SIEM サービスに送信されます。
alert_value	リスクスコアの変更に割り当てられる数値。リスクスコアの変更は、ユーザーの現在のリスクスコアと以前のリスクスコアの差です。アラートの値は -100 から 100 まで変化します。
cur_riskscore	ユーザーに割り当てられている現在のリスクスコア。リスクスコアは、ユーザーのアクティビティに関連する脅威の重要度に応じて、0 ～100 の範囲で変化します。
event_type	SIEM サービスに送信されるデータのタイプ。この場合、イベントタイプはユーザーのリスクスコアの変化です。
timestamp	ユーザーのリスクスコアの最新の変化が検出された日時。

リスク指標スキーマ

リスク指標スキーマは、指標概要スキーマと指標イベント詳細スキーマの 2 つの部分で構成されています。リスク指標に基づいて、スキーマのフィールドとその値がそれに応じて変化します。

次の表に、すべてのインディケータサマリースキーマに共通するフィールド名を示します。

フィールド名	説明
data source	Citrix Analytics のセキュリティにデータを送信する製品。例：Citrix Secure Private Access、NetScaler Gateway、および Citrix アプリとデスクトップ。
data_source_id	データソースに関連付けられた ID。ID 1 = Citrix Gateway、ID 2 = Citrix Endpoint Management、ID 3 = Citrix Apps and Desktops、ID 4 = Citrix Secure Private Access
entity_type	リスクにさらされているエンティティ。ユーザーでもかまいません。
entity_id	リスクのあるエンティティに関連付けられている ID。

フィールド名	説明
event_type	SIEM サービスに送信されるデータのタイプ。この場合、イベントタイプはリスク指標の要約です。
indicator_category	リスク指標のカテゴリを示します。リスク指標は、侵害されたエンドポイント、侵害されたユーザー、データの漏えい、またはインサイダー脅威などのリスクカテゴリに分類されます。
indicator_id	リスク指標に関連付けられている一意の ID。
indicator_category_id	リスク指標カテゴリに関連付けられた ID。ID 1 = データの漏出し、ID 2 = 内部者の脅威、ID 3 = 侵害されたユーザー、ID 4 = 侵害されたエンドポイント
indicator_name	リスク指標の名前。カスタムリスク指標の場合、この名前は指標の作成時に定義されます。
indicator_type	リスク指標がデフォルト（組み込み）かカスタムかを示します。
indicator_uuid	リスク指標インスタンスに関連付けられている一意の ID。
indicator_vector_name	リスク指標に関連付けられているリスクベクトルを示します。リスクベクトルは、デバイスベースのリスク指標、ロケーションベースのリスク指標、ログオン失敗ベースのリスク指標、IP ベースのリスク指標、データベースのリスク指標、ファイルベースのリスク指標、およびその他のリスク指標です。
indicator_vector_id	リスクベクトルに関連付けられた ID。ID 1 = デバイスベースのリスク指標、ID 2 = ロケーションベースのリスク指標、ID 3 = ログオン失敗ベースのリスク指標、ID 4 = IP ベースのリスク指標、ID 5 = データベースのリスク指標、ID 6 = ファイルベースのリスク指標、ID 7 = その他のリスクインジケータ、ID 999 = 利用できない
occurrence_details	リスク指標のトリガー条件に関する詳細。
risk_probability	ユーザーイベントに関連するリスクの可能性を示します。値は 0 から 1.0 まで変化します。カスタムリスク指標の場合、risk_probablabity はポリシーベースの指標であるため、常に 1.0 になります。
severity	リスクの重大度を示します。低、中、高のいずれかになります。
tenant_id	顧客の一意のアイデンティティ。
timestamp	リスク指標がトリガーされる日付と時刻。

フィールド名	説明
ui_link	Citrix Analytics ユーザーインターフェイスのユーザータイムラインビューへのリンク。
observation_start_time	Citrix Analytics がユーザーアクティビティの監視を開始してからタイムスタンプまでの時間。この期間に異常行動が検出された場合、リスク指標がトリガーされます。

次の表では、すべてのインジケータイベントの詳細スキーマに共通するフィールド名を示します。

フィールド名	説明
data_source_id	データソースに関連付けられた ID。ID 1 = Citrix Gateway、ID 2 = Citrix Endpoint Management、ID 3 = Citrix Apps and Desktops、ID 4 = Citrix Secure Private Access
indicator_category_id	リスク指標カテゴリに関連付けられた ID。ID 1 = データの漏出し、ID 2 = 内部者の脅威、ID 3 = 侵害されたユーザー、ID 4 = 侵害されたエンドポイント
entity_id	リスクのあるエンティティに関連付けられている ID。
entity_type	リスクにさらされているエンティティ。ユーザーでもかまいません。
event_type	SIEM サービスに送信されるデータのタイプ。この場合、イベントタイプはリスク指標イベントの詳細です。
indicator_id	リスク指標に関連付けられている一意の ID。
indicator_uuid	リスク指標インスタンスに関連付けられている一意の ID。
indicator_vector_name	リスク指標に関連付けられているリスクベクトルを示します。リスクベクトルは、デバイスベースのリスク指標、ロケーションベースのリスク指標、ログオン失敗ベースのリスク指標、IP ベースのリスク指標、データベースのリスク指標、ファイルベースのリスク指標、およびその他のリスク指標です。
indicator_vector_id	リスクベクトルに関連付けられた ID。ID 1 = デバイスベースのリスク指標、ID 2 = ロケーションベースのリスク指標、ID 3 = ログオン失敗ベースのリスク指標、ID 4 = IP ベースのリスク指標、ID 5 = データベースのリスク指標、ID 6 = ファイルベースのリスク指標、ID 7 = その他のリスクインジケータ、ID 999 = 利用できない

フィールド名	説明
tenant_id	顧客の一意のアイデンティティ。
timestamp	リスク指標がトリガーされる日付と時刻。
version	処理されたデータのスキーマのバージョン。現在のスキーマのバージョンは 2 です。
client_ip	ユーザーのデバイスの IP アドレス。

> 注
>
> - 整数データ型のフィールド値が使用できない場合、割り当てられる値は -999 です。たとえば、"latitude": -999、"longitude": -999。
> - 文字列データ型のフィールド値が使用できない場合、割り当てられる値は NA になります。たとえば、"city": "NA"、"region": "NA"。

Citrix Secure Private Access リスク指標スキーマ

禁止リストに登録された **URL** リスクインジケータスキーマにアクセスしようとしました

インジケータサマリースキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 401,
  "indicator_uuid": "8f2a39bd-c7c2-5555-a86a-5cfe5b64dfef",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-15T10:59:58Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Attempt to access blacklisted URL",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {
```



```
26
27      "observation_start_time": "2018-03-15T10:44:59Z",
28      "relevant_event_type": "Blacklisted External Resource Access"
29     }
30
31   }
32
33
34  <!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": 401,
5    "indicator_uuid": "c421f3f8-33d8-59b9-ad47-715b9d4f65f4",
6    "indicator_category_id": 2,
7    "indicator_vector": {
8
9      "name": "Other Risk Indicators",
10     "id": 7  }
11  ,
12   "data_source_id": 4,
13   "timestamp": "2018-03-15T10:57:21Z",
14   "event_type": "indicatorEventDetails",
15   "entity_type": "user",
16   "entity_id": "demo_user",
17   "version": 2,
18   "domain_name": "googleads.g.doubleclick.net",
19   "executed_action": "blocked",
20   "reason_for_action": "URL Category match",
21   "client_ip": "157.xx.xxx.xxx"
22  }
23
24
25  <!--NeedCopy-->
```

次の表では、禁止リストに登録された URL にアクセスしようとする場合の概要スキーマとイベント詳細スキーマに固有のフィールド名について説明します。

フィールド名	説明
observation_start_time	Citrix Analytics がユーザーアクティビティの監視を開始してからタイムスタンプまでの時間。この期間に異常行動が検出された場合、リスク指標がトリガーされます。
executed_action	禁止リストに登録された URL に適用されるアクション。アクションには [許可] と [ブロック] が含まれます。
reason_for_action	URL のアクションを適用する理由。

過剰なデータダウンロードリスク指標スキーマ

インジケータサマリースキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 403,
  "indicator_uuid": "67d21b81-a89a-531e-af0b-c5688c2e9d40",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Excessive data download",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2018-03-16T10:00:00Z",
    "data_volume_in_bytes": 24000,
    "relevant_event_type": "External Resource Access"
   }

 }


<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 403,
  "indicator_uuid": "67d21b81-a89a-531e-af0b-c5688c2e9d40",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
```



```
  "timestamp": "2018-03-16T10:30:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "domain_name": "www.facebook.com",
  "client_ip": "157.xx.xxx.xxx",
  "downloaded_bytes": 24000
 }


<!--NeedCopy-->
```

次の表では、過剰なデータダウンロードのサマリスキーマおよびイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
observation_start_time	Citrix Analytics がユーザーアクティビティの監視を開始してからタイムスタンプまでの時間。この期間に異常行動が検出された場合、リスク指標がトリガーされます。
data_volume_in_bytes	ダウンロードされるデータの量 (バイト単位)。
relevant_event_type	ユーザーイベントのタイプを示します。
domain_name	データのダウンロード元のドメインの名前。
downloaded_bytes	ダウンロードされるデータの量 (バイト単位)。

異常なアップロードボリュームリスク指標スキーマ

インジケータサマリースキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 402,
  "indicator_uuid": "4f2a249c-9d05-5409-9c5f-f4c764f50e67",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
```



```
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Unusual upload volume",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2018-03-16T10:00:00Z",
    "data_volume_in_bytes": 24000,
    "relevant_event_type": "External Resource Access"
   }

 }


<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 402,
  "indicator_uuid": "c6abf40c-9b62-5db4-84bc-5b2cd2c0ca5f",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }

 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:30:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "domain_name": "www.facebook.com",
  "client_ip": "157.xx.xxx.xxx",
  "uploaded_bytes": 24000
 }


<!--NeedCopy-->
```

次の表では、異常なアップロードボリュームのサマリスキーマおよびイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
observation_start_time	Citrix Analytics がユーザーアクティビティの監視を開始してからタイムスタンプまでの時間。この期間に異常行動が検出された場合、リスク指標がトリガーされます。
data_volume_in_bytes	アップロードされるデータの量 (バイト単位)。
relevant_event_type	ユーザーイベントのタイプを示します。
domain_name	データがアップロードされるドメインの名前。
uploaded_bytes	アップロードされるデータの量 (バイト単位)。

Citrix Endpoint Management のリスク指標スキーマ

ジェイルブレイクまたはルートデバイス検出インジケータースキーマ

インジケータサマリースキーマ

```
{

  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 200,
  "indicator_name": "Jailbroken / Rooted Device Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "aa872f86-a991-4219-ad01-2a070b6e633d",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-13T17:49:05Z",
  "ui_link": "https://analytics.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```


インジケータイベント詳細スキーマ

```
{

  "indicator_id": 200,
  "client_ip": "122.xx.xx.xxx",
  "data_source_id": 2,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_uuid": "9aaaa9e1-39ad-4daf-ae8b-2fa2caa60732",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T17:50:35Z",
  "version": 2
 }


<!--NeedCopy-->
```

禁止リストに登録されたアプリが検出されたデバイス

インジケータサマリースキーマ

```
{

  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 201,
  "indicator_name": "Device with Blacklisted Apps Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "3ff7bd54-4319-46b6-8b98-58a9a50ae9a7",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-13T17:49:23Z",
```



```
  "ui_link": "https://analytics.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

  "indicator_id": 201,
  "client_ip": "122.xx.xx.xxx",
  "data_source_id": 2,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_uuid": "743cd13a-2596-4323-8da9-1ac279232894",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T17:50:39Z",
  "version": 2
 }


<!--NeedCopy-->
```

管理対象外のデバイスが検出されました

インジケータサマリースキーマ

```
{

  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 203,
  "indicator_name": "Unmanaged Device Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_type": "builtin",
```



```
  "indicator_uuid": "e28b8186-496b-44ff-9ddc-ae50e87bd757",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-13T12:56:30Z",
  "ui_link": "https://analytics.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

  "indicator_id": 203,
  "client_ip": "127.xx.xx.xxx",
  "data_source_id": 2,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_uuid": "dd280122-04f2-42b4-b9fc-92a715c907a0",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T18:41:30Z",
  "version": 2
 }


<!--NeedCopy-->
```

NetScaler Gateway リスク指標スキー

EPA スキャン失敗リスク指標スキーマ

インジケータサマリースキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 100,
  "indicator_uuid": "3c17454c-86f5-588a-a4ac-0342693d8a70",
  "indicator_category_id": 3,
```



```
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "EPA scan failure",
  "severity": "low",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "event_description": "Post auth failed, no quarantine",
    "observation_start_time": "2017-12-21T07:00:00Z",
    "relevant_event_type": "EPA Scan Failure at Logon"
   }

 }


<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 100,
  "indicator_uuid": "3c17454c-86f5-588a-a4ac-0342693d8a70",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:12:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "event_description": "Post auth failed, no quarantine",
  "gateway_domain_name": "10.102.xx.xx",
  "gateway_ip": "56.xx.xxx.xx",
  "policy_name": "postauth_act_1",
  "client_ip": "210.91.xx.xxx",
```



```
23    "country": "United States",
24    "city": "San Jose",
25    "region": "California",
26    "cs_vserver_name": "demo_vserver",
27    "device_os": "Windows OS",
28    "security_expression": "CLIENT.OS(Win12) EXISTS",
29    "vpn_vserver_name": "demo_vpn_vserver",
30    "vserver_fqdn": "10.xxx.xx.xx"
31   }
32
33  <!--NeedCopy-->
```

次の表に、EPA スキャン障害リスクインジケータのサマリスキーマおよびイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
event_description	ポスト認証が失敗し、検疫グループがないなど、EPA スキャンが失敗した理由について説明します。
relevant_event_type	EPA スキャン失敗イベントのタイプを示します。
gateway_domain_name	NetScaler Gateway のドメイン名。
gateway_ip	NetScaler Gateway の IP アドレス。
policy_name	NetScaler Gateway で構成された EPA スキャンポリシー名。
country	ユーザーアクティビティが検出された国。
city	ユーザーアクティビティが検出された市区町村。
region	ユーザーアクティビティが検出されたリージョン。
cs_vserver_name	コンテンツスイッチ仮想サーバの名前。
device_os	ユーザーのデバイスのオペレーティングシステム。
security_expression	NetScaler Gateway で構成されたセキュリティ式。
vpn_vserver_name	NetScaler Gateway 仮想サーバーの名前。
vserver_fqdn	NetScaler Gateway 仮想サーバーの FQDN。

過剰な認証失敗リスクインジケータスキーマ

インジケータサマリースキーマ

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": 101,
5    "indicator_uuid": "4bc0f759-93e0-5eea-9967-ed69de9dd09a",
```



```
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Excessive authentication failures",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/” ,
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2017-12-21T07:00:00Z",
    "relevant_event_type": "Logon Failure"
   }

 }

<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 101,
  "indicator_uuid": "a391cd1a-d298-57c3-a17b-01f159b26b99",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:10:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo-user",
  "version": 2,
  "event_description": "Bad (format) password passed to nsaaad",
  "authentication_stage": "Secondary",
  "authentication_type": "LDAP",
  "auth_server_ip": "10.xxx.x.xx",
  "client_ip": "24.xxx.xxx.xx",
  "gateway_ip": "24.xxx.xxx.xx",
```



```
  "vserver_fqdn": "demo-fqdn.citrix.com",
  "vpn_vserver_name": "demo_vpn_vserver",
  "cs_vserver_name": "demo_cs_vserver",
  "gateway_domain_name": "xyz",
  "country": "United States",
  "region": "California",
  "city": "San Jose",
  "nth_failure": 5
 }


<!--NeedCopy-->
```

次の表では、過剰な認証失敗のサマリスキーマおよびイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
relevant_event_type	ログオン失敗などのイベントのタイプを示します。
event_description	パスワードの誤りなど、認証エラーが頻繁に発生した理由について説明します。
authentication_stage	認証ステージがプライマリ、セカンダリ、ターシャリのどちらであるかを示します。
authentication_type	LDAP、ローカル、OAuth などの認証のタイプを示します。
auth_server_ip	認証サーバの IP アドレス。
gateway_domain_name	NetScaler Gateway のドメイン名。
gateway_ip	NetScaler Gateway の IP アドレス。
cs_vserver_name	コンテンツスイッチ仮想サーバの名前。
vpn_vserver_name	NetScaler Gateway 仮想サーバーの名前。
vserver_fqdn	NetScaler Gateway 仮想サーバーの FQDN。
nth_failure	ユーザー認証が失敗した回数。
country	ユーザーアクティビティが検出された国。
city	ユーザーアクティビティが検出された市区町村。
region	ユーザーアクティビティが検出されたリージョン。

あり得ない移動リスクインジケータ

インジケータサマリースキーマ

```
{

```



```
  "tenant_id": "demo_tenant",
  "indicator_id": "111",
  "indicator_uuid": "83d68a6d-6588-5b77-9118-8a9e6a5b462b",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Location-Based Risk Indicators",
    "id": 2
   }
 ,
  "data_source_id": 1,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Impossible travel",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Impossible travel",
    "distance": 7480.44718,
    "observation_start_time": "2020-06-06T12:00:00Z",
    "historical_logon_locations": "[{
 "country":"United States","region":"Florida","city":"Miami","latitude"
    :25.7617,"longitude":-80.191,"count":28 }
 ,{
 "country":"United States","latitude":37.0902,"longitude":-95.7129,"
    count":2 }
 ]",
    "historical_observation_period_in_days": 30
   }

 }


<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "111",
  "indicator_uuid": "83d68a6d-6588-5b77-9118-8a9e6a5b462b",
  "pair_id": 2,
  "indicator_category_id": 3,
  "indicator_vector": {

```



```
10      "name": "Location-Based Risk Indicators",
11      "id": 2
12     }
13   ,
14    "data_source_id": 1,
15    "timestamp": "2020-06-06T05:05:00Z",
16    "event_type": "indicatorEventDetails",
17    "entity_type": "user",
18    "entity_id": "demo_user",
19    "version": 2,
20    "client_ip": "95.xxx.xx.xx",
21     “ip_organization” :  “global telecom ltd” ,
22     “ip_routing_type” :  “mobile gateway” ,
23    "country": "Norway",
24    "region": "Oslo",
25    "city": "Oslo",
26    "latitude": 59.9139,
27    "longitude": 10.7522,
28    "device_os": "Linux OS",
29    "device_browser": "Chrome 62.0.3202.94"
30   }
31
32
33  <!--NeedCopy-->
```

次の表に、インポッシブルトラベルのサマリースキーマとイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
distance	あり得ない移動に関連するイベント間の距離 (km)。
historical_logon_locations	ユーザーがアクセスした場所と、観測期間中に各場所にアクセスした回数。
historical_observation_period_in_days	各場所は 30 日間監視されます。
relevant_event_type	ログオンなどのイベントのタイプを示します。
observation_start_time	Citrix Analytics がユーザーアクティビティの監視を開始してからタイムスタンプまでの時間。この期間に異常行動が検出された場合、リスク指標がトリガーされます。
country	ユーザーがログオンした国。
city	ユーザーがログオンした市区町村。
region	ユーザーがログオンしたリージョンを示します。
latitude	ユーザーがログオンした場所の緯度を示します。
longitude	ユーザーがログオンした場所の経度を示します。
device_browser	ユーザーが使用する Web ブラウザ。

フィールド名	説明
device_os	ユーザーのデバイスのオペレーティングシステム。
ip_organization	クライアント IP アドレスの組織を登録する
ip_routing_type	クライアント IP ルーティングタイプ

疑わしい **IP** リスク指標スキーマからログオン

インジケータサマリースキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 102,
  "indicator_uuid": "0100e910-561a-5ff3-b2a8-fc556d199ba5",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "data_source_id": 1,
  "timestamp": "2019-10-10T10:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 0.91,
  "indicator_category": "Compromised users",
  "indicator_name": "Logon from suspicious IP",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Logon",
    "client_ip": "1.0.xxx.xx",
    "observation_start_time": "2019-10-10T10:00:00Z",
    "suspicion_reasons": "brute_force|external_threat"
   }

 }

<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

```



```
  "tenant_id": "demo_tenant",
  "indicator_id": 102,
  "indicator_uuid": "4ba77b6c-bac0-5ad0-9b4a-c459a3e2ec33",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "data_source_id": 1,
  "timestamp": "2019-10-10T10:11:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "suspicion_reasons": "external_threat",
  "gateway_ip": "gIP1",
  "client_ip": "128.0.xxx.xxx",
  "country": "Sweden",
  "city": "Stockholm",
  "region": "Stockholm",
  "webroot_reputation": 14,
  "webroot_threat_categories": "Windows Exploits|Botnets|Proxy",
  "device_os": "Windows OS",
  "device_browser": "Chrome"
 }


<!--NeedCopy-->
```

次の表は、不審な IP からのログインのサマリスキーマとイベント詳細スキーマに固有のフィールド名を示しています。

フィールド名	説明
suspicious_reasons	IP アドレスが疑わしいと識別される理由。
webroot_reputation	脅威インテリジェンスプロバイダ Webroot によって提供される IP レピュテーションインデックス。
webroot_threat_categories	脅威インテリジェンスプロバイダ Webroot によって疑わしい IP で識別される脅威カテゴリ。
device_os	ユーザーデバイスのオペレーティングシステム。
device_browser	使用した Web ブラウザ。
country	ユーザーアクティビティが検出された国。
city	ユーザーアクティビティが検出された市区町村。
region	ユーザーアクティビティが検出されたリージョン。

異常な認証失敗リスクインジケータスキーマ

インジケータサマリースキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 109,
  "indicator_uuid": "dc0174c9-247a-5e48-a2ab-d5f92cd83d0f",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2020-04-01T06:44:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Unusual authentication failure",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Logon Failure",
    "observation_start_time": "2020-04-01T05:45:00Z"
   }

 }


<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 109,
  "indicator_uuid": "ef4b9830-39d6-5b41-bdf3-84873a77ea9a",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2020-04-01T06:42:00Z",
```



```
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "event_description": "Success",
  "authentication_stage": "Secondary",
  "authentication_type": "LDAP",
  "client_ip": "99.xxx.xx.xx",
  "country": "United States",
  "city": "San Jose",
  "region": "California",
  "device_os": "Windows OS ",
  "device_browser": "Chrome",
  "is_risky": "false"
 }


<!--NeedCopy-->
```

次の表に、異常な認証失敗のサマリスキーマおよびイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
relevant_event_type	ログオン失敗などのイベントのタイプを示します。
event_description	ログオンが成功したか失敗したかを示します
authentication_stage	認証ステージがプライマリ、セカンダリ、ターシャリのどちらであるかを示します。
authentication_type	LDAP、ローカル、OAuth などの認証のタイプを示します。
is_risky	ログオンが成功した場合、is_risky の値は false になります。ログオンに失敗した場合、is_risky の値は true になります。
device_os	ユーザーデバイスのオペレーティングシステム。
device_browser	ユーザーが使用する Web ブラウザ。
country	ユーザーアクティビティが検出された国。
city	ユーザーアクティビティが検出された市区町村。
region	ユーザーアクティビティが検出されたリージョン。

不審なログオンリスク指標

インジケータサマリースキーマ

```
{

```



```
  "tenant_id": "demo_tenant",
  "indicator_id": "110",
  "indicator_uuid": "67fd935-a6a3-5397-b596-636aa1588c",
  "indicator_category_id": 3,
  "indicator_vector": [
    {

      "name": "Location-Based Risk Indicators",
      "id": 2
     }
,
    {

      "name": "IP-Based Risk Indicators",
      "id": 4
     }
,
    {

      "name": "Other Risk Indicators",
      "id": 7
     }

  ],
  "data_source_id": 1,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 0.71,
  "indicator_category": "Compromised users",
  "indicator_name": "Suspicious logon",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2020-06-06T12:00:00Z",
    "relevant_event_type": "Logon",
    "event_count": 1,
    "historical_observation_period_in_days": 30,
    "country": "United States",
    "region": "Florida",
    "city": "Miami",
    "historical_logon_locations": "[{
"country":"United States","region":"New York","city":"New York City","
    latitude":40.7128,"longitude":-74.0060,"count":9 }
]",
    "user_location_risk": 75,
    "device_id": "",
    "device_os": "Windows OS",
```



```
    "device_browser": "Chrome",
    "user_device_risk": 0,
    "client_ip": "99.xxx.xx.xx",
    "user_network_risk": 75,
    "webroot_threat_categories": "Phishing",
    "suspicious_network_risk": 89
   }

 }



<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "110",
  "indicator_uuid": "67fd6935-a6a3-5397-b596-63856aa1588c",
  "indicator_category_id": 3,
  "indicator_vector": [
    {

      "name": "Location-Based Risk Indicators",
      "id": 2
     }
 ,
    {

      "name": "IP-Based Risk Indicators",
      "id": 4
     }
 ,
    {

      "name": "Other Risk Indicators",
      "id": 7
     }

  ],
  "data_source_id": 1,
  "timestamp": "2020-06-06T12:08:40Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "country": "United States",
  "region": "Florida",
  "city": "Miami",
  "latitude": 25.7617,
  "longitude": -80.1918,
  "device_browser": "Chrome",
```



```
39    "device_os": "Windows OS",
40    "device_id": "NA",
41    "client_ip": "99.xxx.xx.xx"
42   }
43
44
45  <!--NeedCopy-->
```

次の表に、不審なログオンのサマリスキーマとイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
historical_logon_locations	ユーザーがアクセスした場所と、観測期間中に各場所にアクセスした回数。
historical_observation_period_in_days	各場所は 30 日間監視されます。
relevant_event_type	ログオンなどのイベントのタイプを示します。
observation_start_time	Citrix Analytics がユーザーアクティビティの監視を開始してからタイムスタンプまでの時間。この期間に異常行動が検出された場合、リスク指標がトリガーされます。
occurrence_event_type	アカウントログオンなどのユーザーイベントタイプを示します。
country	ユーザーがログオンした国。
city	ユーザーがログオンした市区町村。
region	ユーザーがログオンしたリージョンを示します。
latitude	ユーザーがログオンした場所の緯度を示します。
longitude	ユーザーがログオンした場所の経度を示します。
device_browser	ユーザーが使用する Web ブラウザ。
device_os	ユーザーのデバイスのオペレーティングシステム。
device_id	ユーザーが使用するデバイスの名前。
user_location_risk	ユーザーがログオンした場所の疑わしいレベルを示します。低い疑いレベル:0—69、中程度の疑いレベル:70—89、高い疑いレベル:90—100
user_device_risk	ユーザーがログオンしたデバイスの疑いレベルを示します。低い疑いレベル:0—69、中程度の疑いレベル:70—89、高い疑いレベル:90—100
user_network_risk	ユーザーがログオンしたネットワークまたはサブネットの疑いレベルを示します。低い疑いレベル:0—69、中程度の疑いレベル:70—89、高い疑いレベル:90—100

フィールド名	説明
suspicious_network_risk	Webroot IP 脅威インテリジェンスフィードに基づく IP 脅威レベルを示します。低脅威レベル:0—69、中脅威レベル:70—89、高脅威レベル:90—100
webroot_threat_categories	Webroot IP 脅威インテリジェンスフィードに基づいて、IP アドレスから検出された脅威のタイプを示します。脅威カテゴリには、スパムソース、Windows エクスプロイト、Web 攻撃、ボットネット、スキャナ、サービス拒否、レピュテーション、フィッシング、プロキシ、不特定、モバイル脅威、Tor プロキシがあります。

Citrix DaaS と **Citrix Virtual Apps and Desktops** のリスク指標スキーマ

あり得ない移動リスクインジケータ

インジケータサマリースキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "313",
  "indicator_uuid": "c78d1dd4-5e70-5642-ba6f-1cdf31bc6ab2",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Location-Based Risk Indicators",
    "id": 2
   }
 ,
  "data_source_id": 3,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Impossible travel",
  "severity": "medium",
  "data_source": "Apps and Desktops",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Impossible travel",
    "distance": 7480.44718,
    "observation_start_time": "2020-06-06T12:00:00Z",
```



```
    "historical_logon_locations": "[{
 "country":"United States","region":"Florida","city":"Miami","latitude"
    :25.7617,"longitude":-80.191,"count":28 }
 ,{
 "country":"United States","latitude":37.0902,"longitude":-95.7129,"
    count":2 }
 ]",
    "historical_observation_period_in_days": 30
   }

 }


<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "313",
  "indicator_uuid": "c78d1dd4-5e70-5642-ba6f-1cdf31bc6ab2",
  "pair_id": 2,
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Location-Based Risk Indicators",
    "id": 2
   }
 ,
  "data_source_id": 3,
  "timestamp": "2020-06-06T05:05:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "occurrence_event_type": "Account.Logon",
  "client_ip": "95.xxx.xx.xx",
   “ip_organization” : “global telecom ltd” ,
   “ip_routing_type” : “mobile gateway” ,
  "country": "Norway",
  "region": "Oslo",
  "city": "Oslo",
  "latitude": 59.9139,
  "longitude": 10.7522,
  "device_id": "device1",
  "receiver_type": "XA.Receiver.Linux",
  "os": "Linux OS",
  "browser": "Chrome 62.0.3202.94"
 }


<!--NeedCopy-->
```


次の表に、インポッシブルトラベルのサマリースキーマとイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
distance	あり得ない移動に関連するイベント間の距離 (km)。
historical_logon_locations	ユーザーがアクセスした場所と、観測期間中に各場所にアクセスした回数。
historical_observation_period_in_days	各場所は 30 日間監視されます。
relevant_event_type	ログオンなどのイベントのタイプを示します。
observation_start_time	Citrix Analytics がユーザーアクティビティの監視を開始してからタイムスタンプまでの時間。この期間に異常行動が検出された場合、リスク指標がトリガーされます。
country	ユーザーがログオンした国。
city	ユーザーがログオンした市区町村。
region	ユーザーがログオンしたリージョンを示します。
latitude	ユーザーがログオンした場所の緯度を示します。
longitude	ユーザーがログオンした場所の経度を示します。
browser	ユーザーが使用する Web ブラウザ。
os	ユーザーのデバイスのオペレーティングシステム。
device_id	ユーザーが使用するデバイスの名前。
receiver_type	ユーザーのデバイスにインストールされている Citrix Workspace アプリまたは Citrix Receiver タイプ。
ip_organization	クライアント IP アドレスの組織を登録する
ip_routing_type	クライアント IP ルーティングタイプ

潜在的なデータ漏洩リスク指標

インジケータサマリースキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 303,
  "indicator_uuid": "fb649ff7-5b09-5f48-8a04-12836b9eed85",
  "indicator_category_id": 1,
  "indicator_vector": {

    "name": "Data-Based Risk Indicators",
```



```
    "id": 5  }
 ,
  "data_source_id": 3,
  "timestamp": "2018-04-02T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Data exfiltration",
  "indicator_name": "Potential data exfiltration",
  "severity": "low",
  "data_source": "Citrix Apps and Desktops",
  "ui_link": "https://analytics.cloud.com/user/ ",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Download/Print/Copy",
    "observation_start_time": "2018-04-02T10:00:00Z",
    "exfil_data_volume_in_bytes": 1172000
   }

 }


<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 303,
  "indicator_uuid": "fb649ff7-5b09-5f48-8a04-12836b9eed85",
  "indicator_category_id": 1,
  "indicator_vector": {

    "name": "Data-Based Risk Indicators",
    "id": 5  }
 ,
  "data_source_id": 3,
  "timestamp": "2018-04-02T10:57:36Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "occurrence_event_type": "App.SaaS.Clipboard",
  "file_size_in_bytes": 98000,
  "file_type": "text",
  "device_id": "dvc5",
  "receiver_type": "XA.Receiver.Windows",
  "app_url": "https://www.citrix.com",
  "client_ip": "10.xxx.xx.xxx",
  "entity_time_zone": "Pacific Standard Time"
```



```
 }


<!--NeedCopy-->
```

次の表では、潜在的なデータ漏出のサマリースキーマおよびイベント詳細スキーマに固有のフィールドについて説明します。

フィールド名	説明
observation_start_time	Citrix Analytics がユーザーアクティビティの監視を開始してからタイムスタンプまでの時間。この期間に異常行動が検出された場合、リスク指標がトリガーされます。
relevant_event_type	データのダウンロード、印刷、コピーなどのユーザーアクティビティを示します。
exfil_data_volume_in_bytes	データの流出量。
occurrence_event_type	SaaS アプリでのクリップボード操作など、データの流出がどのように発生したかを示します。
file_size_in_bytes	ファイルのサイズ。
file_type	ファイルのタイプ。
device_id	ユーザーデバイスの ID。
receiver_type	ユーザーデバイスにインストールされている Citrix Workspace アプリまたは Citrix Receiver です。
app_url	ユーザーがアクセスするアプリケーションの URL。
entity_time_zone	ユーザーのタイムゾーン。

疑わしいログオンリスク指標スキーマ

インジケータサマリースキーマ

```
{

  "tenant_id": "tenant_1",
  "indicator_id": "312",
  "indicator_uuid": "1b97c3be-abcd-efgh-ijkl-1234567890",
  "indicator_category_id": 3,
  "indicator_vector":
  [
    {

      "name": "Other Risk Indicators",
      "id": 7
     }
 ,
```



```
    {

      "name":"Location-Based Risk Indicators",
      "id":2
     }
,
    {

      "name":"IP-Based Risk Indicators",
      "id":4
     }
,
    {

      "name": "Device-Based Risk Indicators",
      "id": 1
     }
,
 ],
 "data_source_id": 3,
 "timestamp": "2020-06-06T12:14:59Z",
 "event_type": "indicatorSummary",
 "entity_type": "user",
 "entity_id": "user2",
 "version": 2,
 "risk_probability": 0.78,
 "indicator_category": "Compromised users",
 "indicator_name": "Suspicious logon",
 "severity": "medium",
 "data_source": "Citrix Apps and Desktops",
 "ui_link": "https://analytics.cloud.com/user/ ",
 "indicator_type": "builtin",
 "occurrence_details":
 {

   "user_location_risk": 0,
   "city": "Some_city",
   "observation_start_time": "2020-06-06T12:00:00Z",
   "event_count": 1,
   "user_device_risk": 75,
   "country": "United States",
   "device_id": "device2",
   "region": "Some_Region",
   "client_ip": "99.xx.xx.xx",
   "webroot_threat_categories": "'Spam Sources', 'Windows Exploits', '
      Web Attacks', 'Botnets', 'Scanners', 'Denial of Service'",
   "historical_logon_locations": "[{
"country":"United States","latitude":45.0,"longitude":45.0,"count":12
    }
,{
"country":"United States","region":"Some_Region_A","city":"Some_City_A
   ","latitude":0.0,"longitude":0.0,"count":8 }
]",
```



```
    "relevant_event_type": "Logon",
    "user_network_risk": 100,
    "historical_observation_period_in_days": 30,
    "suspicious_network_risk": 0
   }

 }


<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

  "tenant_id": "tenant_1",
  "indicator_id": "312",
  "indicator_uuid": "1b97c3be-abcd-efgh-ijkl-1234567890",
  "indicator_category_id": 3,
  "indicator_vector":
  [
    {

      "name": "Other Risk Indicators",
      "id": 7
     }
 ,
    {

      "name":"Location-Based Risk Indicators",
      "id":2
     }
 ,
    {

      "name":"IP-Based Risk Indicators",
      "id":4
     }
 ,
    {

      "name": "Device-Based Risk Indicators",
      "id": 1
     }
 ,
  ],
  "data_source_id": 3,
  "timestamp": "2020-06-06 12:02:30",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "user2",
  "version": 2,
  "occurrence_event_type": "Account.Logon",
  "city": "Some_city",
```



```
  "country": "United States",
  "region": "Some_Region",
  "latitude": 37.751,
  "longitude": -97.822,
  "browser": "Firefox 1.3",
  "os": "Windows OS",
  "device_id": "device2",
  "receiver_type": "XA.Receiver.Chrome",
  "client_ip": "99.xxx.xx.xx"
 }


<!--NeedCopy-->
```

次の表に、不審なログオンのサマリスキーマとイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
historical_logon_locations	ユーザーがアクセスした場所と、観測期間中に各場所にアクセスした回数。
historical_observation_period_in_days	各場所は 30 日間監視されます。
relevant_event_type	ログオンなどのイベントのタイプを示します。
observation_start_time	Citrix Analytics がユーザーアクティビティの監視を開始してからタイムスタンプまでの時間。この期間に異常行動が検出された場合、リスク指標がトリガーされます。
occurrence_event_type	アカウントログオンなどのユーザーイベントタイプを示します。
country	ユーザーがログオンした国。
city	ユーザーがログオンした市区町村。
region	ユーザーがログオンしたリージョンを示します。
latitude	ユーザーがログオンした場所の緯度を示します。
longitude	ユーザーがログオンした場所の経度を示します。
browser	ユーザーが使用する Web ブラウザ。
os	ユーザーのデバイスのオペレーティングシステム。
device_id	ユーザーが使用するデバイスの名前。
receiver_type	ユーザーのデバイスにインストールされている Citrix Workspace アプリまたは Citrix Receiver タイプ。
user_location_risk	ユーザーがログオンした場所の疑わしいレベルを示します。低い疑いレベル:0—69、中程度の疑いレベル:70—89、高い疑いレベル:90—100

フィールド名	説明
user_device_risk	ユーザーがログオンしたデバイスの疑いレベルを示します。低い疑いレベル:0—69、中程度の疑いレベル:70—89、高い疑いレベル:90—100
user_network_risk	ユーザーがログオンしたネットワークまたはサブネットの疑いレベルを示します。低い疑いレベル:0—69、中程度の疑いレベル:70—89、高い疑いレベル:90—100
suspicious_network_risk	Webroot IP 脅威インテリジェンスフィードに基づく IP 脅威レベルを示します。低脅威レベル:0—69、中脅威レベル:70—89、高脅威レベル:90—100
webroot_threat_categories	Webroot IP 脅威インテリジェンスフィードに基づいて、IP アドレスから検出された脅威のタイプを示します。脅威カテゴリには、スパムソース、Windows エクスプロイト、Web 攻撃、ボットネット、スキャナ、サービス拒否、レピュテーション、フィッシング、プロキシ、不特定、モバイル脅威、Tor プロキシがあります。

Microsoft Active Directory インジケータ

インジケータサマリースキーマ

```
{

  "data_source": "Microsoft Graph Security",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised users",
  "indicator_id": 1000,
  "indicator_name": "MS Active Directory Indicator",
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "9880f479-9fbe-4ab0-8348-a613f9de5eba",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-01-27T16:03:46Z",
  "ui_link": "https://analytics-daily.cloud.com/user/",
  "version": 2
 }
```



```
<!--NeedCopy-->
```

インジケータイベント詳細スキーマ

```
{

  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_id": 1000,
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "indicator_uuid": "9880f479-9fbe-4ab0-8348-a613f9de5eba",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-01-27T16:03:46Z",
  "version": 2
 }


<!--NeedCopy-->
```

カスタムリスク指標スキーマ

次のセクションでは、カスタムリスク指標のスキーマについて説明します。

> 注
>
> 現在、Citrix Analytics は、Citrix DaaS および Citrix Virtual Apps and Desktops のカスタムリスク指標に関連するデータを SIEM サービスに送信します。

次の表に、カスタムリスク指標サマリスキーマのフィールド名を示します。

フィールド名	説明
data source	Citrix Analytics のセキュリティにデータを送信する製品。例：Citrix Secure Private Access、NetScaler Gateway、および Citrix アプリとデスクトップ。
data_source_id	データソースに関連付けられた ID。ID 1 = Citrix Gateway、ID 2 = Citrix Endpoint Management、ID 3 = Citrix Apps and Desktops、ID 4 = Citrix Secure Private Access
entity_id	リスクのあるエンティティに関連付けられている ID。

フィールド名	説明
entity_type	リスクにさらされているエンティティ。この場合、エンティティはユーザーです。
event_type	SIEM サービスに送信されるデータのタイプ。この場合、イベントタイプはリスク指標の要約です。
indicator_category	リスク指標のカテゴリを示します。リスク指標は、侵害されたエンドポイント、侵害されたユーザー、データの漏えい、またはインサイダー脅威などのリスクカテゴリに分類されます。
indicator_id	リスク指標に関連付けられている一意の ID。
indicator_category_id	リスク指標カテゴリに関連付けられた ID。ID 1 = データ流出、ID 2 = インサイダーの脅威、ID 3 = 侵害されたユーザー、ID 4 = 侵害されたエンドポイント
indicator_name	リスク指標の名前。カスタムリスク指標の場合、この名前は指標の作成時に定義されます。
indicator_type	リスク指標がデフォルト（組み込み）かカスタムかを示します。
indicator_uuid	リスク指標インスタンスに関連付けられている一意の ID。
occurrence_details	リスク指標のトリガー条件に関する詳細。
pre_configured	カスタムリスク指標が事前構成されているかどうかを示します。
risk_probability	ユーザーイベントに関連するリスクの可能性を示します。値は 0 から 1.0 まで変化します。カスタムリスク指標の場合、risk_probablabity はポリシーベースの指標であるため、常に 1.0 になります。
severity	リスクの重大度を示します。低、中、高のいずれかになります。
tenant_id	顧客の一意のアイデンティティ。
timestamp	リスク指標がトリガーされる日付と時刻。
ui_link	Citrix Analytics ユーザーインターフェイスのユーザータイムラインビューへのリンク。
version	処理されたデータのスキーマのバージョン。現在のスキーマのバージョンは 2 です。

次の表に、カスタムリスク指標イベント詳細スキーマで共通のフィールド名を示します。

フィールド名	説明
data_source_id	データソースに関連付けられた ID。ID 1 = Citrix Gateway、ID 2 = Citrix Endpoint Management、ID 3 = Citrix Apps and Desktops、ID 4 = Citrix Secure Private Access
indicator_category_id	リスク指標カテゴリに関連付けられた ID。ID 1 = データ流出、ID 2 = インサイダーの脅威、ID 3 = 侵害されたユーザー、ID 4 = 侵害されたエンドポイント
event_type	SIEM サービスに送信されるデータのタイプ。この場合、イベントタイプはリスク指標イベントの詳細です。
tenant_id	顧客の一意のアイデンティティ。
entity_id	リスクのあるエンティティに関連付けられている ID。
entity_type	リスクにさらされているエンティティ。この場合は、ユーザーです。
indicator_id	リスク指標に関連付けられている一意の ID。
indicator_uuid	リスク指標インスタンスに関連付けられている一意の ID。
timestamp	リスク指標がトリガーされる日付と時刻。
version	処理されたデータのスキーマのバージョン。現在のスキーマのバージョンは 2 です。
event_id	ユーザーイベントに関連付けられた ID。
occurrence_event_type	セッションログオン、セッション起動、アカウントログオンなど、ユーザーイベントの種類を示します。
product	Windows 向け Citrix Workspace アプリなど、Citrix Workspace アプリの種類を示します。
client_ip	ユーザーのデバイスの IP アドレス。
session_user_name	Citrix Apps and Desktops セッションに関連付けられたユーザー名。
city	ユーザーアクティビティが検出された都市の名前。
country	ユーザーアクティビティが検出された国の名前。
device_id	ユーザーが使用するデバイスの名前。
os_name	ユーザーのデバイスにインストールされているオペレーティングシステム。詳しくは、「アプリとデスクトップのセルフサービス検索」を参照してください。

フィールド名	説明
os_version	ユーザーのデバイスにインストールされているオペレーティングシステムのバージョン。詳しくは、「アプリとデスクトップのセルフサービス検索」を参照してください。
os_extra_info	ユーザーのデバイスにインストールされているオペレーティングシステムに関連する追加情報。詳しくは、「アプリとデスクトップのセルフサービス検索」を参照してください。

Citrix DaaS および **Citrix Virtual Apps and Desktops** のカスタムリスクインジケータ

インジケータサマリースキーマ

```
{

  "data_source": " Citrix Apps and Desktops",
  "data_source_id": 3,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised users",
  "indicator_category_id": 3,
  "indicator_id": "ca97a656ab0442b78f3514052d595936",
  "indicator_name": "Demo_user_usage",
  "indicator_type": "custom",
  "indicator_uuid": "8e680e29-d742-4e09-9a40-78d1d9730ea5",
  "occurrence_details": {

    "condition": "User-Name ~ demo_user", "happen": 0, "new_entities":
       "", "repeat": 0, "time_quantity": 0, "time_unit": "", "type": "
       everyTime" }
 ,
  "pre_configured": "N",
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-02-10T14:47:25Z",
  "ui_link": "https://analytics.cloud.com/user/ ",
  "version": 2
 }


<!--NeedCopy-->
```

セッションログオンイベントのインジケータイベント詳細スキーマ

```
{

  "event_type": "indicatorEventDetails",
```



```
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.Logon",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "SYD04-MS1-S102",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
 }


<!--NeedCopy-->
```

次の表に、セッションログオンイベントのイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
app_name	起動されたアプリケーションまたはデスクトップの名前。
launch_type	アプリケーションまたはデスクトップのいずれかを示します。
domain	リクエストを送信したサーバーのドメイン名。
server_name	サーバーの名前。
session_guid	アクティブなセッションの GUID。

セッション起動イベントのインジケータイベント詳細スキーマ

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
```



```
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.Launch",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
 }


<!--NeedCopy-->
```

次の表に、セッション起動イベントのイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
app_name	起動されたアプリケーションまたはデスクトップの名前。
launch_type	アプリケーションまたはデスクトップのいずれかを示します。

アカウントログオンイベントのインジケータイベント詳細スキーマ

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Account.Logon",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
```



```
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
 }


<!--NeedCopy-->
```

次の表では、アカウントログオンイベントのイベント詳細スキーマに固有のフィールド名について説明します。

フィールド名	説明
app_name	起動されたアプリケーションまたはデスクトップの名前。

セッション終了イベントのインジケータイベント詳細スキーマ

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
 }


<!--NeedCopy-->
```


次の表に、セッション終了イベントのイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
app_name	起動されたアプリケーションまたはデスクトップの名前。
launch_type	アプリケーションまたはデスクトップのいずれかを示します。
domain	リクエストを送信したサーバーのドメイン名。
server_name	サーバーの名前。
session_guid	アクティブなセッションの GUID。

アプリ開始イベントのインジケーターイベントの詳細スキーマ

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.Start",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "module_file_path": "/root/folder1/folder2/folder3"
 }


<!--NeedCopy-->
```

次の表に、アプリ開始イベントのイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
app_name	起動されたアプリケーションまたはデスクトップの名前。
launch_type	アプリケーションまたはデスクトップのいずれかを示します。
domain	リクエストを送信したサーバーのドメイン名。
server_name	サーバーの名前。
session_guid	アクティブなセッションの GUID。
module_file_path	使用されているアプリケーションのパス。

アプリ終了イベントのインジケータイベント詳細スキーマ

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "module_file_path": "/root/folder1/folder2/folder3"
 }


<!--NeedCopy-->
```

次の表に、アプリ終了イベントのイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
app_name	起動されたアプリケーションまたはデスクトップの名前。
launch_type	アプリケーションまたはデスクトップのいずれかを示します。
domain	リクエストを送信したサーバーのドメイン名。
server_name	サーバーの名前。
session_guid	アクティブなセッションの GUID。
module_file_path	使用されているアプリケーションのパス。

Indicator イベントの詳細ファイルダウンロードイベントのスキーマ

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "File.Download",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "file_download_file_name": "File5.txt",
  "file_download_file_path": "/root/folder1/folder2/folder3",
  "file_size_in_bytes": 278,
  "launch_type": "Desktop",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "device_type": "USB"
 }


<!--NeedCopy-->
```

次の表に、ファイルダウンロードイベントのイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
file_download_file_name	ダウンロードファイルの名前。
file_download_file_path	ファイルがダウンロードされる宛先パス。
launch_type	アプリケーションまたはデスクトップのいずれかを示します。
domain	リクエストを送信したサーバーのドメイン名。
server_name	サーバーの名前。
session_guid	アクティブなセッションの GUID。
device_type	ファイルがダウンロードされるデバイスのタイプを示します。

印刷イベントのインジケータイベント詳細スキーマ

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Printing",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "printer_name": "Test-printer",
  "launch_type": "Desktop",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "job_details_size_in_bytes": 454,
  "job_details_filename": "file1.pdf",
  "job_details_format": "PDF"
 }


```



```
<!--NeedCopy-->
```

次の表に、印刷イベントのイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
printer_name	印刷ジョブに使用されるプリンタの名前。
launch_type	アプリケーションまたはデスクトップのいずれかを示します。
domain	リクエストを送信したサーバーのドメイン名。
server_name	サーバーの名前。
session_guid	アクティブなセッションの GUID。
job_details_size_in_bytes	ファイルやフォルダなどの印刷ジョブのサイズ。
job_details_filename	印刷されるファイルの名前。
job_details_format	印刷ジョブの形式。

アプリの **SaaS** 起動イベントのインジケータイベント詳細スキーマ

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.SaaS.Launch",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "launch_type": "Desktop",
 }


<!--NeedCopy-->
```


次の表に、アプリの SaaS 起動イベントのイベント詳細スキーマに固有のフィールド名を示します。

フィールド名	説明
launch_type	アプリケーションまたはデスクトップのいずれかを示します。

アプリの **SaaS** 終了イベントのインジケータイベント詳細スキーマ

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.SaaS.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "launch_type": "Desktop",
 }


<!--NeedCopy-->
```

次の表では、App SaaS 終了イベントのイベント詳細スキーマに固有のフィールド名について説明します。

フィールド名	説明
launch_type	アプリケーションまたはデスクトップのいずれかを示します。

データソースイベント

さらに、データエクスポート機能を構成して、Citrix Analytics for Security 対応の製品データソースからユーザーイベントをエクスポートできます。Citrix 環境で何らかのアクティビティを実行すると、データソースイベントが生

成されます。エクスポートされたイベントは、セルフサービスビューで確認できる未処理のリアルタイムユーザーおよび製品使用データです。これらのイベントに含まれるメタデータは、さらに詳細な脅威分析、新しいダッシュボードの作成、セキュリティや IT インフラストラクチャ全体にわたる Citrix 以外の他のデータソースイベントとの関連付けにも使用できます。

現在、Citrix Analytics for Security は、Citrix Virtual Apps and Desktops データソースのユーザーイベントを SIEM に送信しています。

データソースイベントのスキーマ詳細

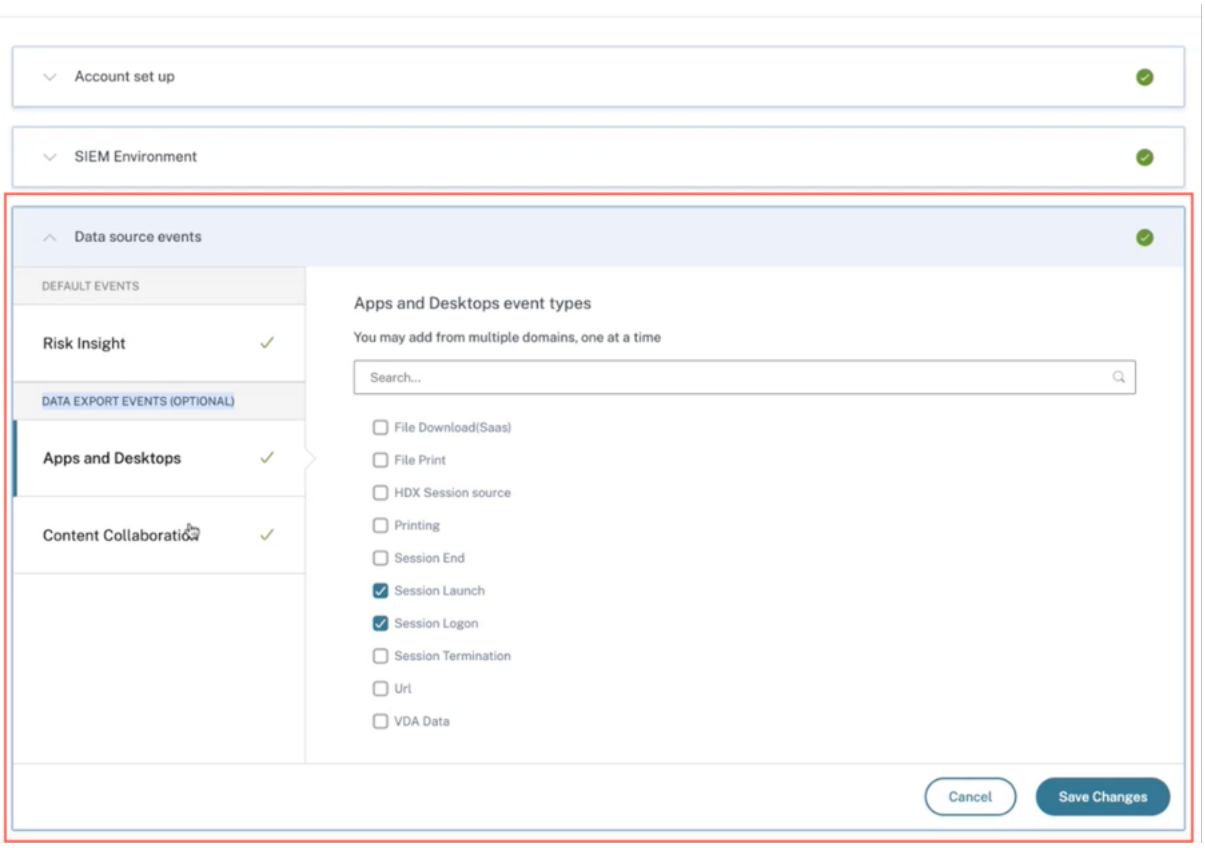
CitrixVirtual Apps and Desktops イベント

ユーザーイベントは、ユーザーが仮想アプリまたは仮想デスクトップを使用するときに、Citrix Analytics for Security でリアルタイムで受信されます。詳しくは、「Citrix Virtual Apps and Desktops」および「Citrix DaaS データソース」を参照してください。SIEM では、Citrix Virtual Apps and Desktops に関連する次のユーザーイベントを表示できます。

- すべてのイベントタイプ
- アカウントログオン
- アプリ (開始、起動、終了)
- クリップボード
- ファイル (印刷、ダウンロード)
- ファイルダウンロード (SaaS)
- HDX セッションソース
- 印刷
- セッション (ログオン、起動、終了、終了)
- Url
- VDA データ
- VDA プロセス作成

イベントとその属性の詳細については、「Virtual Apps and Desktops のセルフサービス検索」を参照してください。

どのイベントタイプが有効で SIEM に流れているかを確認できます。テナントに適用できるイベントタイプを設定または削除し、[変更を保存] ボタンをクリックして設定を保存できます。



脅威分析とデータ相関のための **Citrix Analytics SIEM** データモデルの活用

June 19, 2023

この記事では、お客様の SIEM 環境に送信されるイベントによって示されるエンティティデータの関係について説明します。これを理解するために、クライアント IP と OS という属性が焦点となる脅威ハンティングのシナリオを例にとってみましょう。上記の属性をユーザーに関連付ける次の方法について説明します。

- カスタムリスク指標インサイトの使用
- データソースイベントの使用

Splunk は、次の例で紹介する SIEM 環境として選ばれました。同様のデータ相関は、Citrix Analytics のワークブックテンプレートを使用して Sentinel で実行することもできます。これについてさらに詳しく調べるには、Microsoft Sentinel 用の Citrix Analytics ワークブックを参照してください。

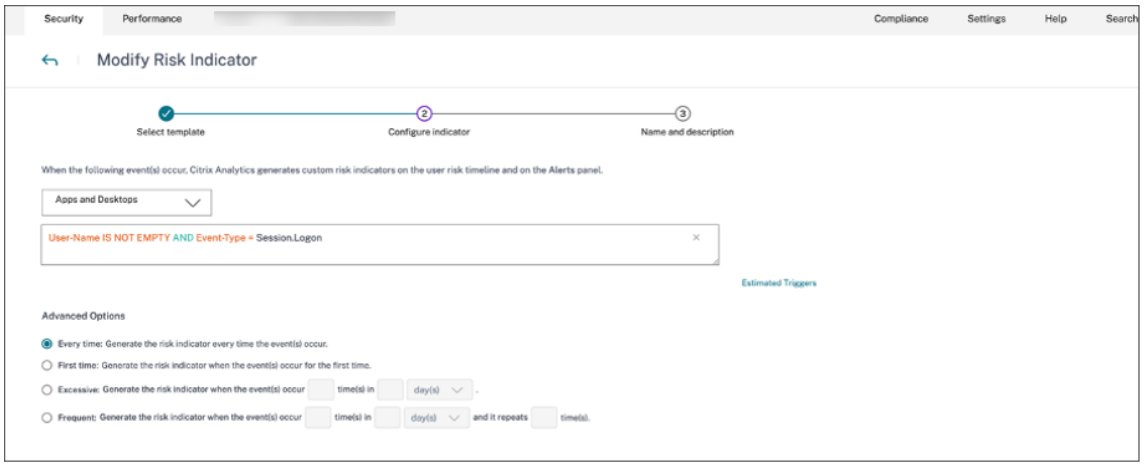
カスタムリスク指標インサイト

SIEM の Citrix Analytics データエクスポート形式で説明したように、指標の概要とイベントの詳細のインサイトはデフォルトのリスクインサイトデータセットの一部です。Citrix Virtual Apps and Desktops インジケーターデー

タセットの場合、クライアント IP と OS はデフォルトでエクスポートされます。したがって、管理者がこれらのフィールドを含む条件付きまたは条件なしのカスタムインジケーターを設定すると、そのデータポイントが Splunk 環境に流れ込みます。

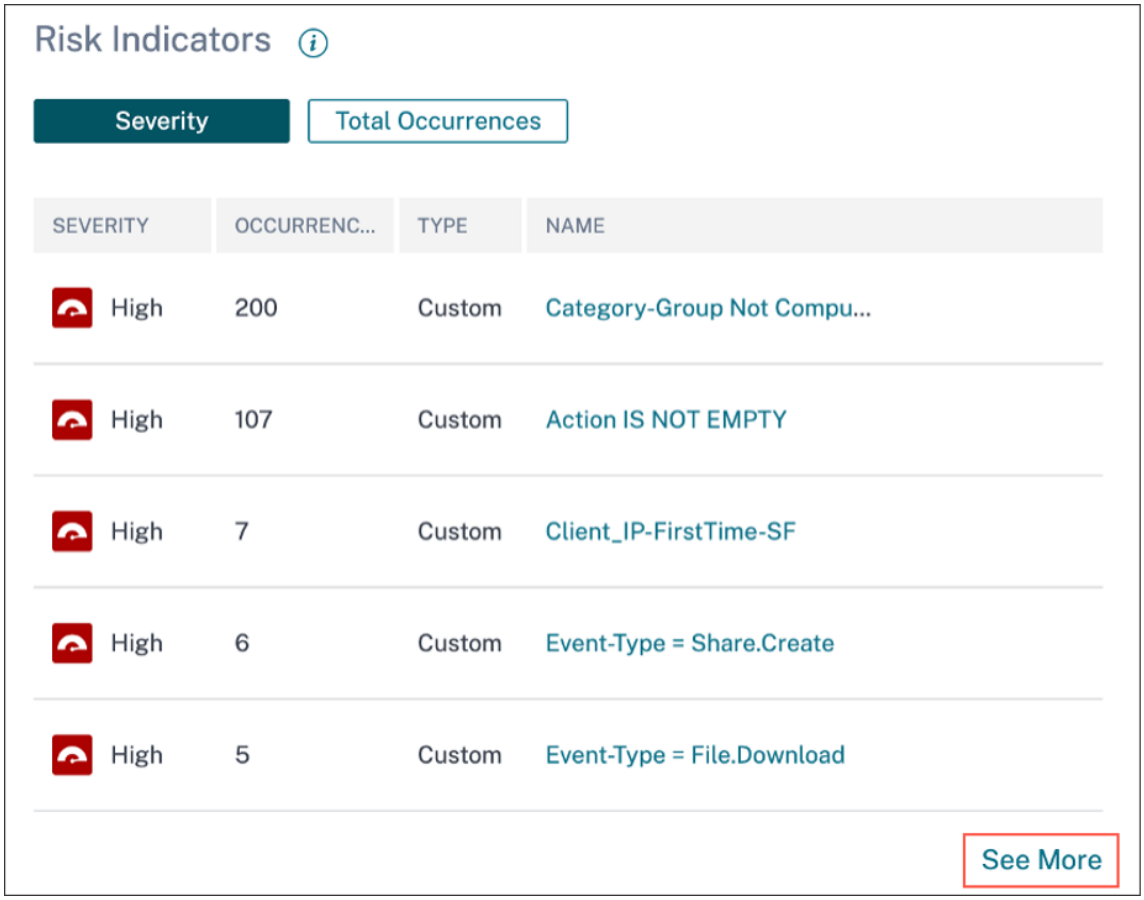
Citrix Analytics でのカスタムリスク指標の設定

1. **Citrix Analytics for Security** ダッシュボード **>** カスタムリスク指標 **>** 指標の作成に移動します。ユーザーの行動を監視するのに役立つ任意の条件でカスタムリスク指標を作成できます。カスタムインジケーターを設定すると、関連する条件をトリガーしたすべてのユーザーが Splunk 環境に表示されます。

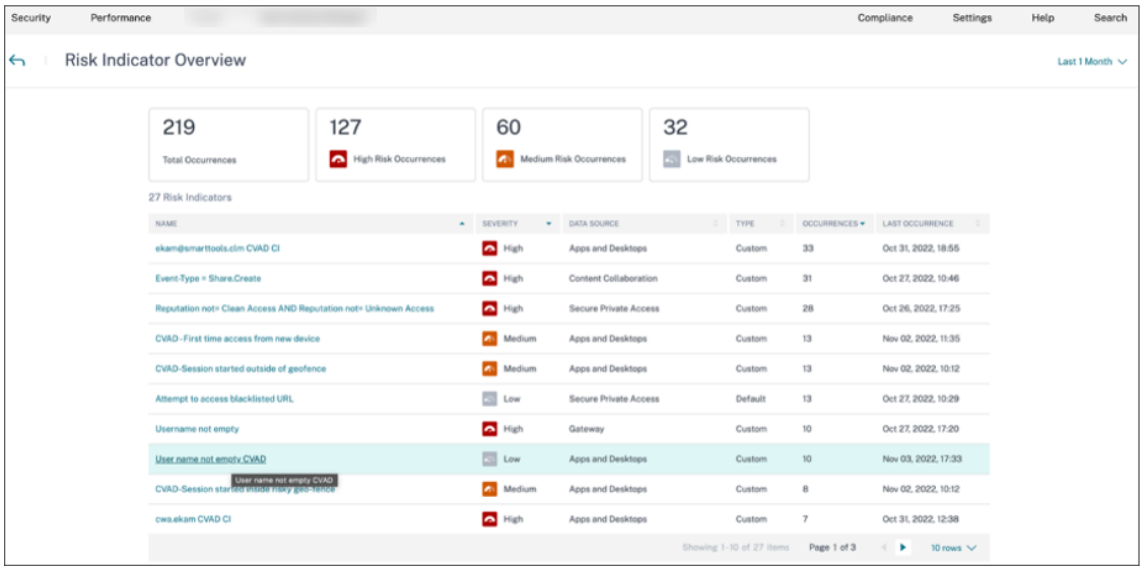


2. 作成したリスク指標のオカレンスを Citrix Analytics for Security で表示するには、［セキュリティ］>［ユーザー］に移動します。ページの一番下に移動し、プラス **(+)** アイコンをクリックします。

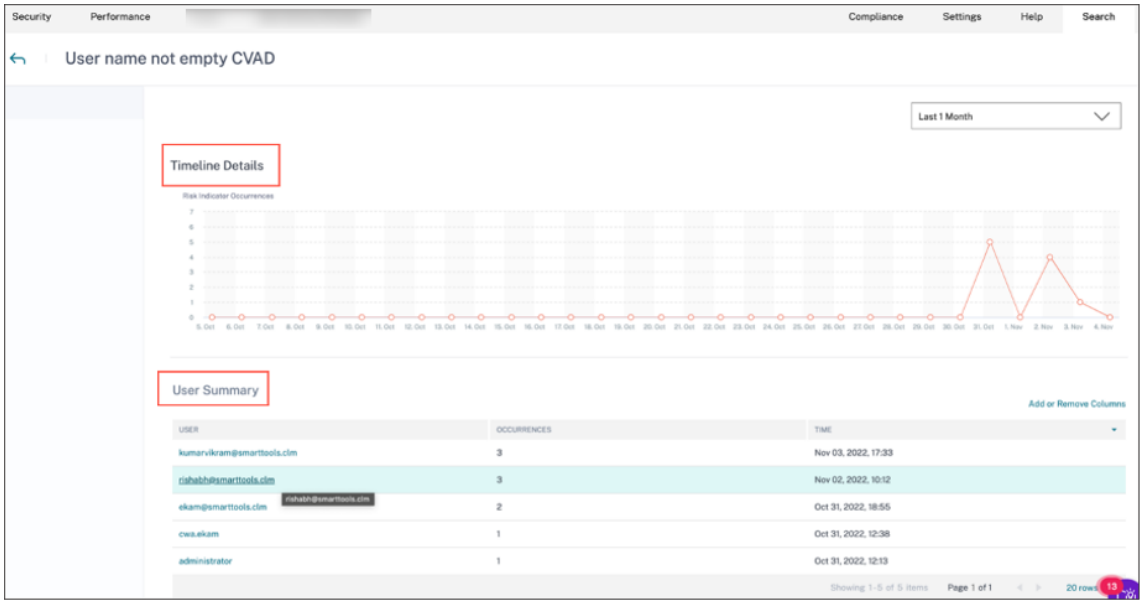
リスク指標カードが表示されます。リスク指標、重要度、発生率の詳細を表示できます。



3. 「もっと見る」をクリックします。リスク指標の概要ページが表示されます。



リスク指標の概要ページでは、指標をトリガーしたユーザーの詳細を、詳細なタイムラインビューとユーザー概要で表示できます。タイムラインの詳細については、「ユーザーリスクタイムラインとプロファイル」を参照してください。

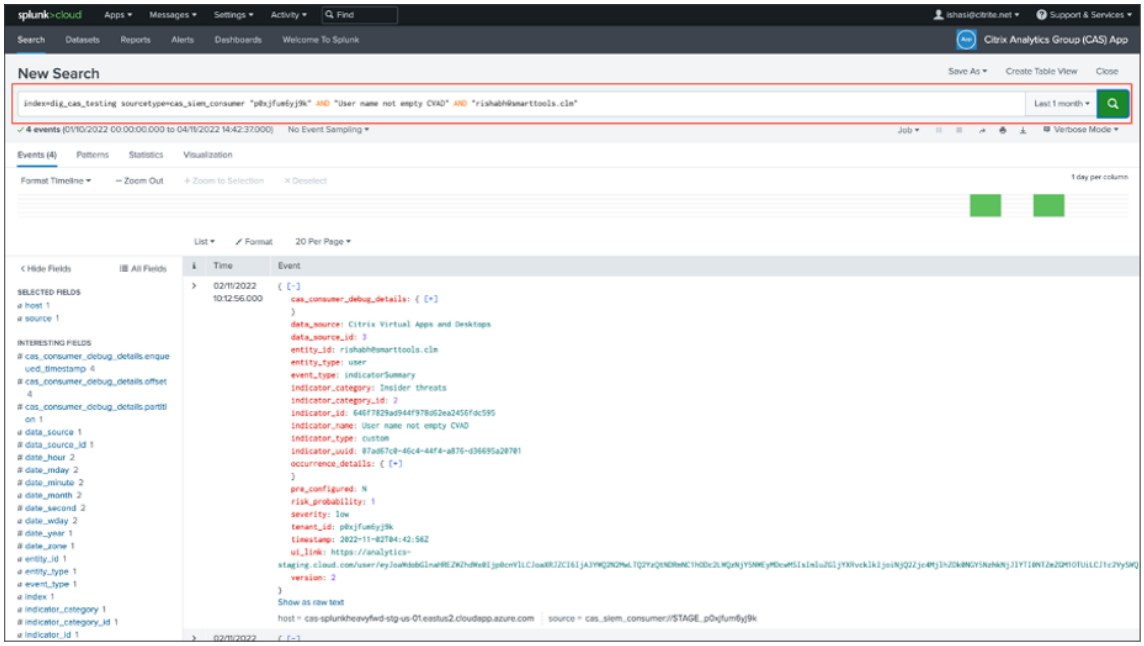


Splunk でのリスク指標の発生-未処理クエリ

また、Splunk Enterprise for Citrix Analytics for Security Add-on でデータ入力を設定する際に使用したインデックスとソースタイプを使用して、クライアントの IP と OS の情報を取得することもできます。

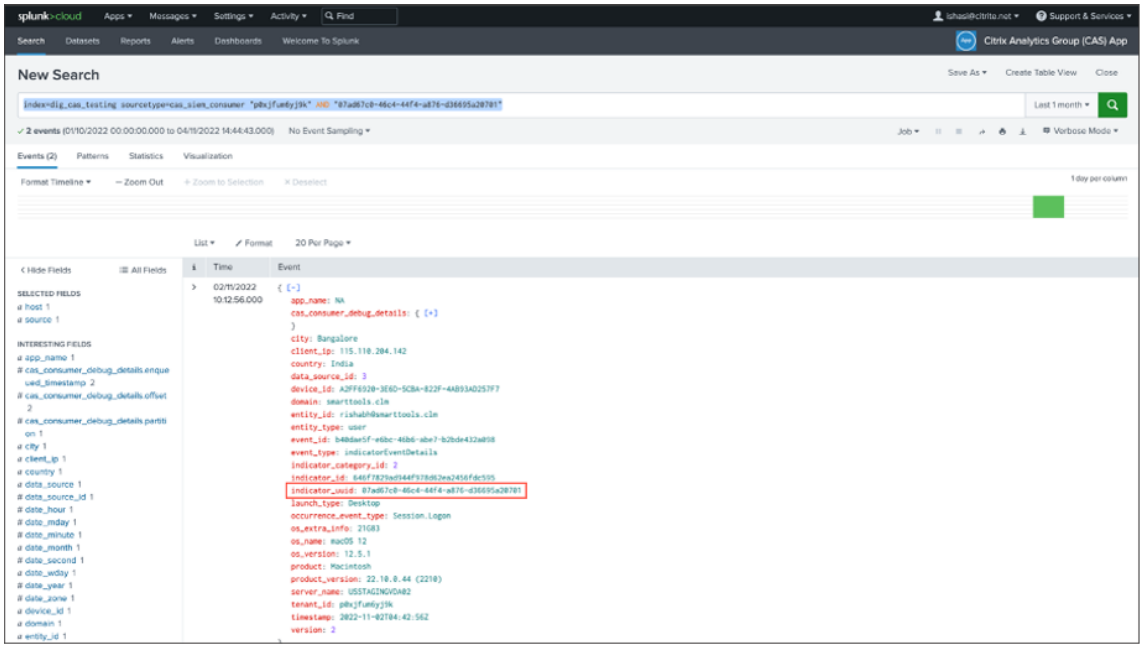
1. [**Splunk] > [**新規検索] に移動します。検索クエリで、次のクエリを入力して実行します。

```
index=<index configured by you> sourcetype=<sourcetype configured
    by you> AND "<tenant_id>" AND "<indicator name configured by
    you on CAS>" AND "<user you are interested in>"

<!--NeedCopy-->
```

2. indicator_uuid を取得して、次のクエリを実行します。

```
index=<index configured by you> sourcetype=<sourcetype configured
    by you> "<tenant_id>" AND "<indicator_uuid>"

<!--NeedCopy-->
```



イベント結果には、** インジケーターイベントの概要とインジケーターイベントの詳細 ** （インジケーターによってトリガーされるアクティビティ）が含まれます。イベントの詳細には、クライアント **IP** と **OS** の情報 (名前、バージョン、追加情報) が含まれます。

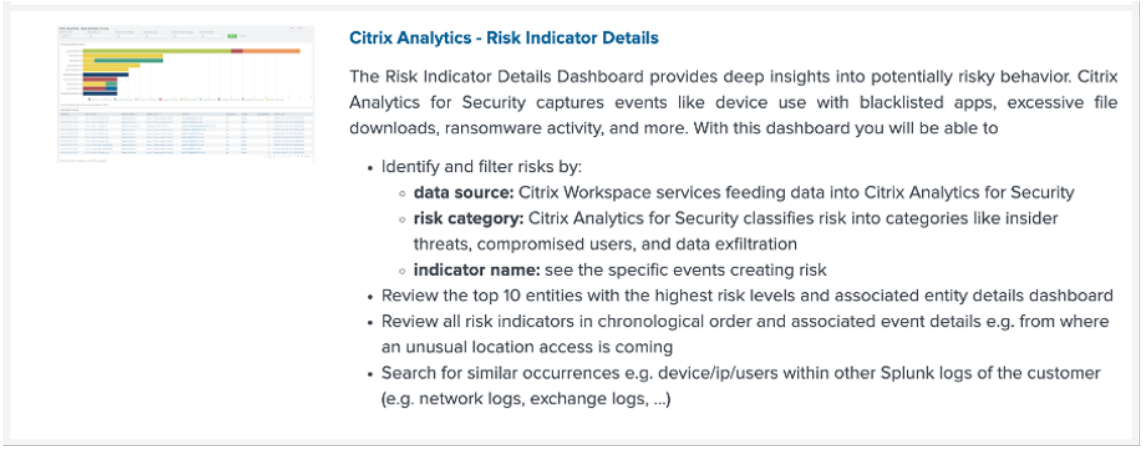
データ形式の詳細については、「Citrix Analytics SIEM 用データエクスポート形式」を参照してください。

Splunk でのリスク指標の発生-ダッシュボードアプリ

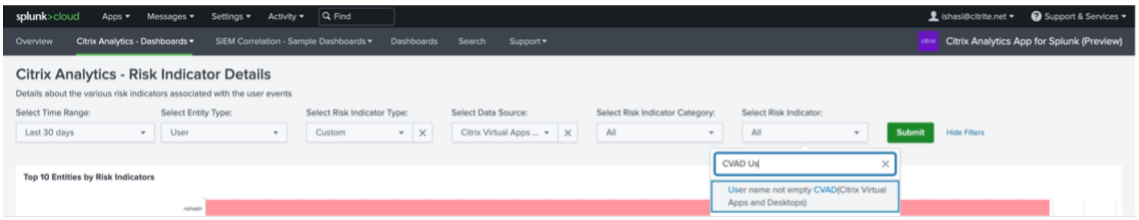
Splunk 向け Citrix Analytics アプリのインストール方法に関するガイダンスについては、以下の記事を参照してください。

- Splunk 向け Citrix Analytics アプリ
- Splunk 向け Citrix Analytics ダッシュボード

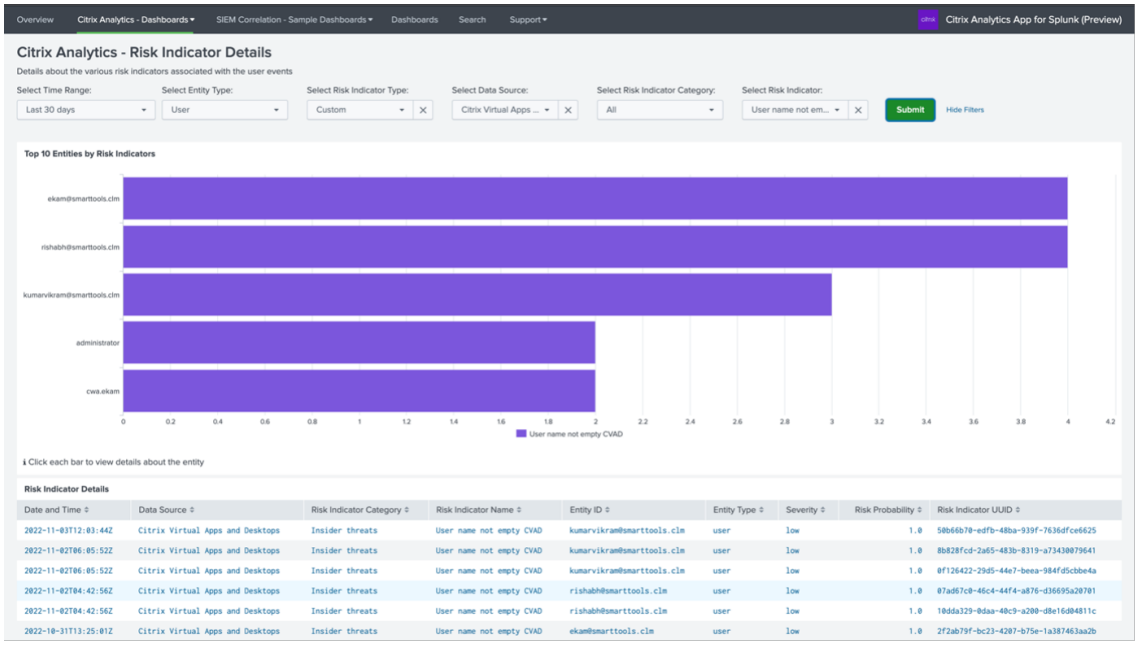
1. **Citrix Analytics** —ダッシュボードタブをクリックし、ドロップダウンリストから「リスク指標の詳細」オプションを選択します。



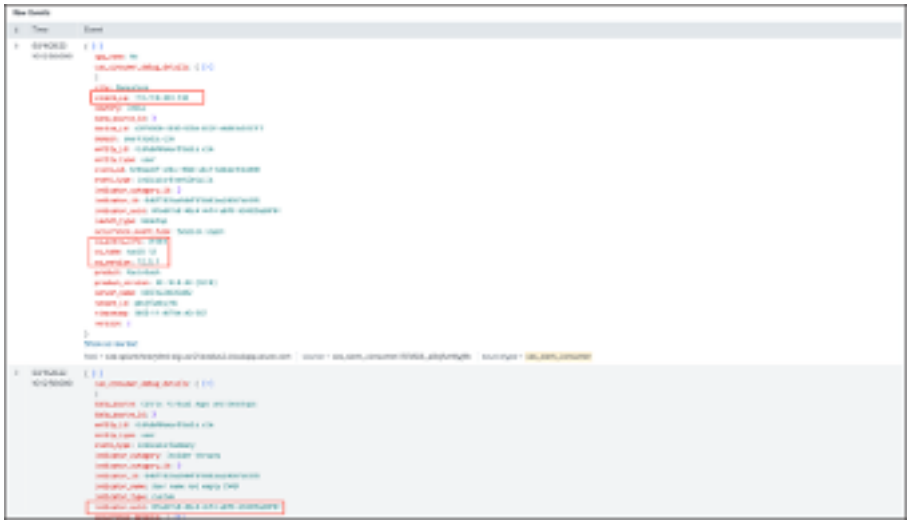
2. ドロップダウンリストからコンテンツを適切にフィルタリングし、[送信] をクリックします。



3. ユーザーインスタンスをクリックすると、詳細が表示されます。



4. クライアント **IP** と **OS** の情報 (名前、バージョン、追加情報) は、このページの下部に表示されます。

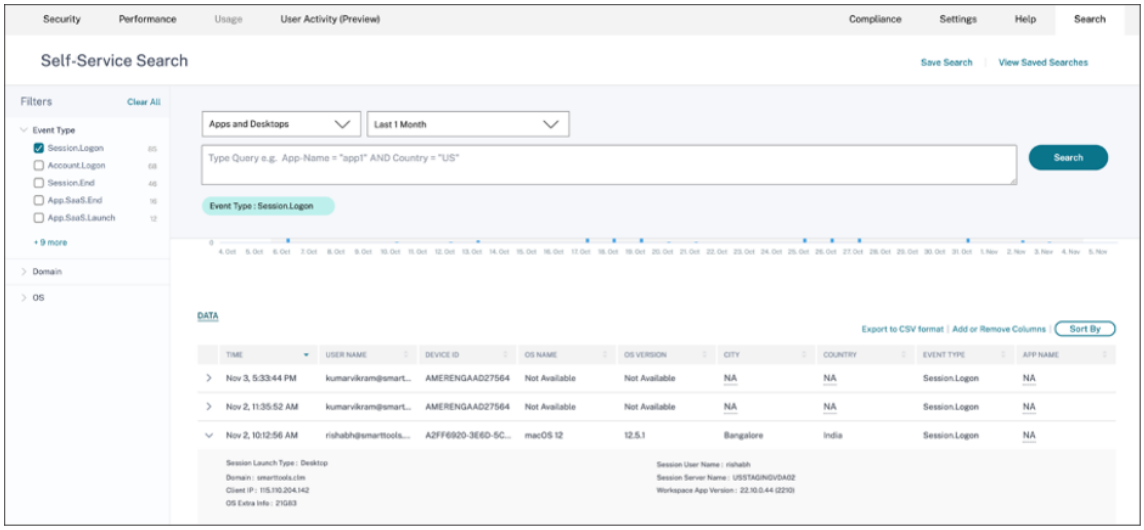


データソースイベント

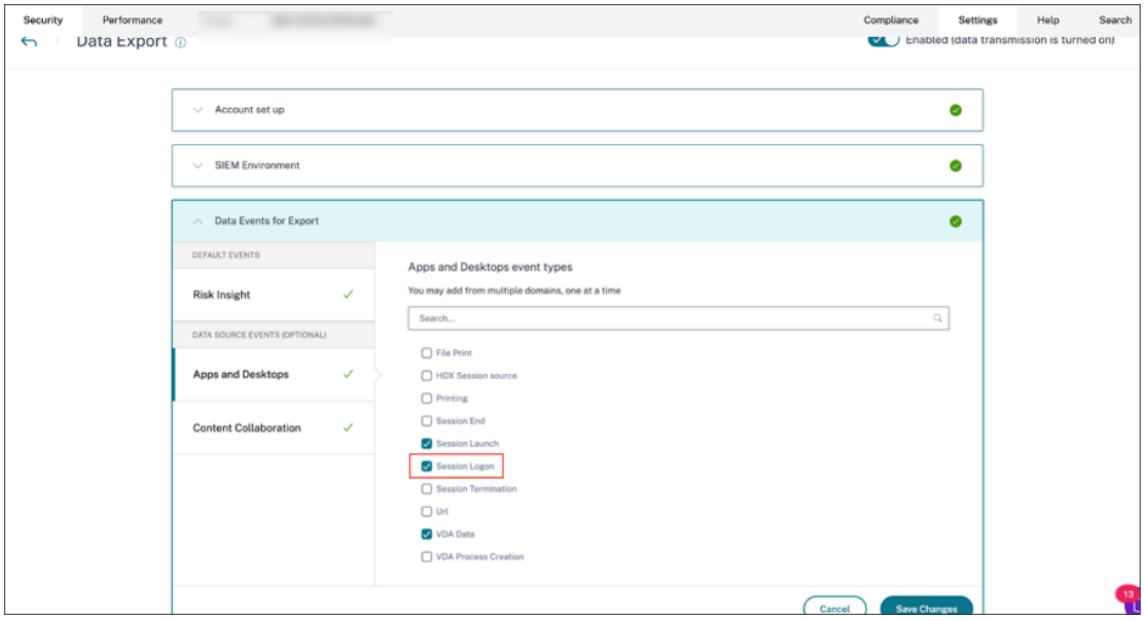
Splunk 環境のクライアント IP と OS の詳細を取得するもう 1 つの方法は、エクスポート用のデータソースイベントを設定することです。この機能により、Self-Service Search ビューに表示されているイベントを Splunk 環境に直接送信できます。SIEM にエクスポートする Virtual Apps and Desktops のイベントタイプを設定する方法の詳細については、次の記事を参照してください。

- Citrix Analytics for Security から SIEM サービスにエクスポートされたデータイベント。
- データソースイベント

1. **Citrix Analytic for** セキュリティダッシュボード **>** 検索に移動します。このセルフサービス検索ページでは、すべてのイベントタイプと関連情報が表示されます。次のスクリーンショットの例として、**Session.Logon** イベントタイプを確認できます。



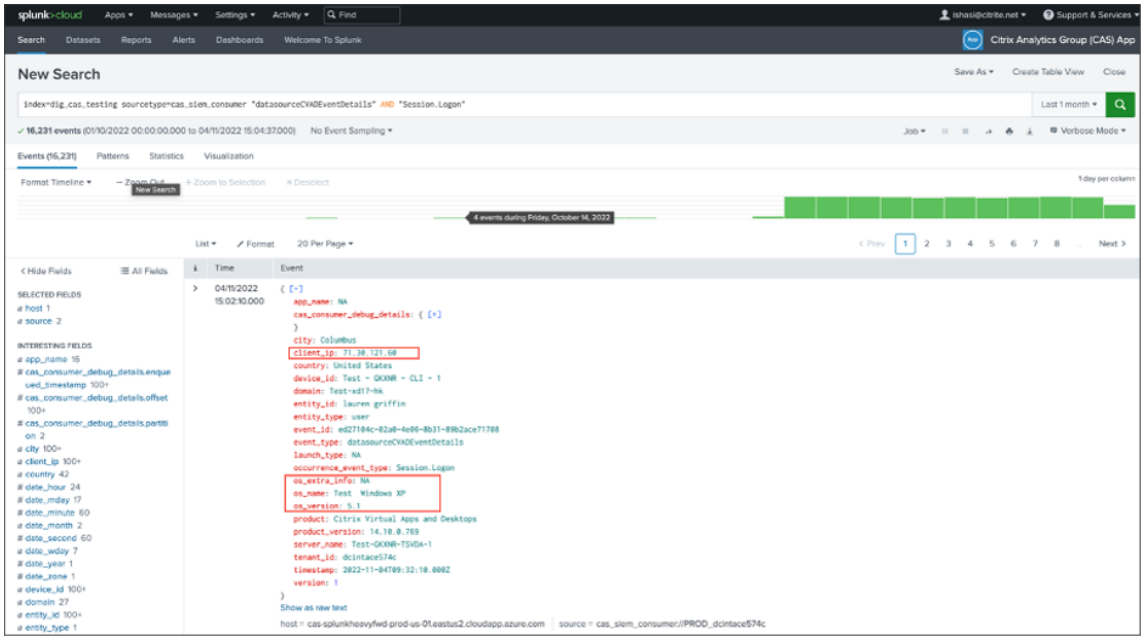
2. **Session.Logon** をエクスポート用のデータソースイベントに設定し、保存を押して **Splunk** 環境にフローさせます。



3. Splunk に移動し、次のクエリを入力して実行します。

```
index="<index you configured>" sourcetype="<sourcetype you
    configured>" "<tenant_id>" AND "datasourceCVADEventDetails" AND
     "Session.Logon"  AND "<user you' re interested in>"

<!--NeedCopy-->
```

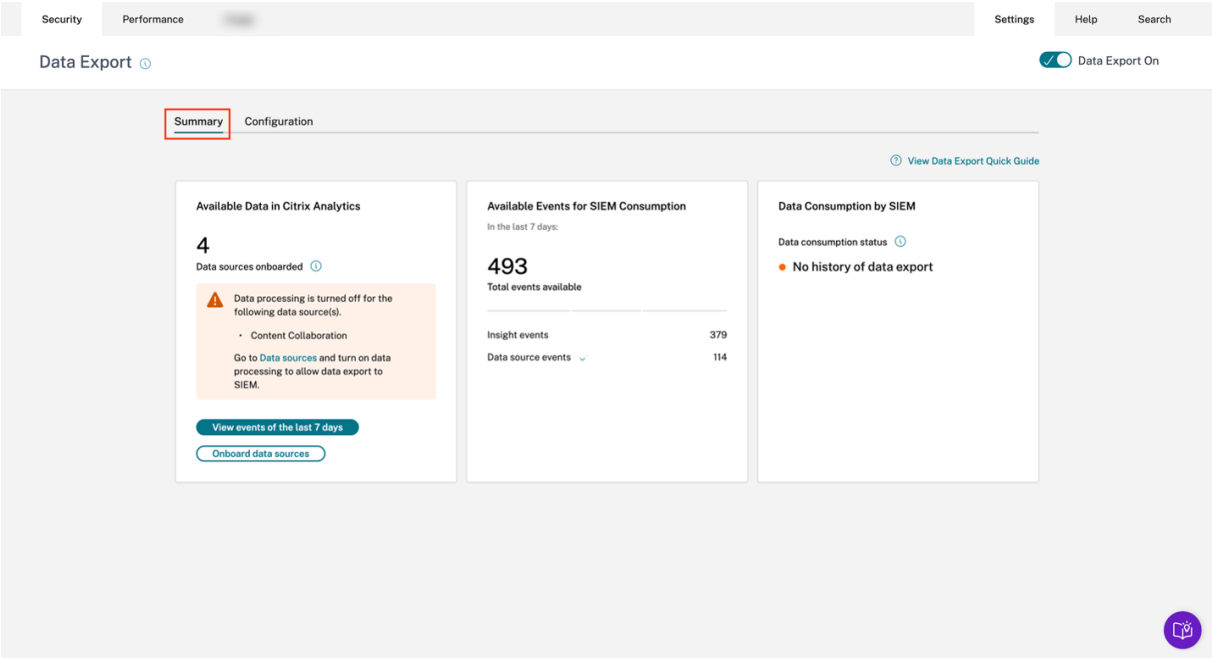
クライアント IP と OS に関連するフィールドが強調表示されます。



データエクスポートのトラブルシューティング

December 7, 2023

セキュリティ用データエクスポートビューには、管理者が SIEM と Citrix **Analytics** 統合のトラブルシューティングに役立つサマリータブが含まれています。概要ダッシュボードでは、トラブルシューティングプロセスに役立つチェックポイントを通すことで、データの状態とフローを可視化できます。

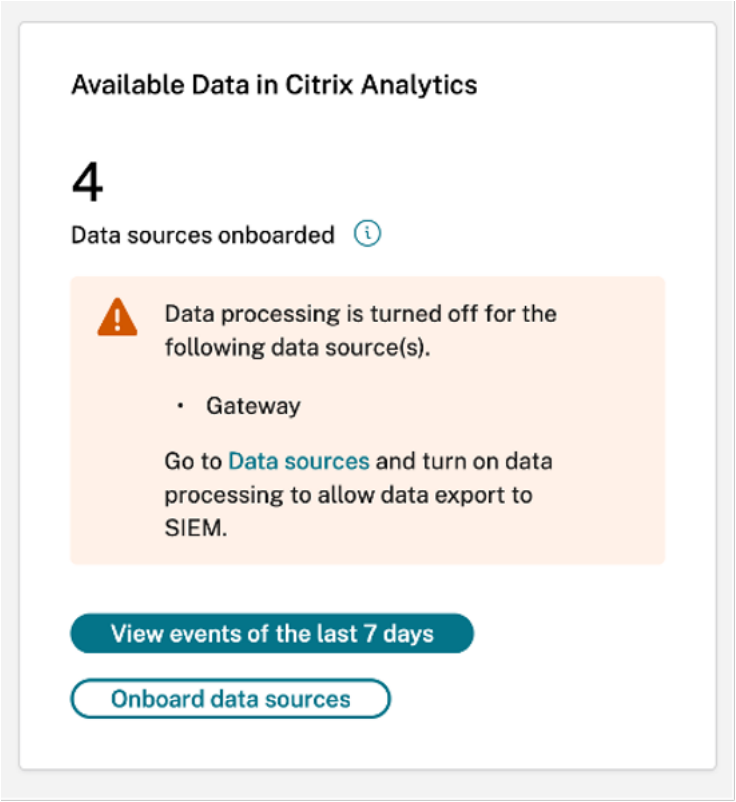


「概要」タブ

「サマリ」タブは、「データエクスポート」ビューのセルフ・サービス・トラブルシューティング・ワークフローの基礎となります。以下の 3 つのカードを使用して SIEM を設定する方法について説明します。

- **Citrix Analytics** で利用可能なデータ: このカードには、データソース構成の状態が表示されます。
- **SIEM** で使用可能なイベント: このカードには、ご使用の SIEM 環境で処理できるイベントの数が表示されます。
- **SIEM** によるデータ消費量: このカードには、SIEM 環境のデータフローの状態が表示されます。

Citrix Analytics で利用可能なデータ

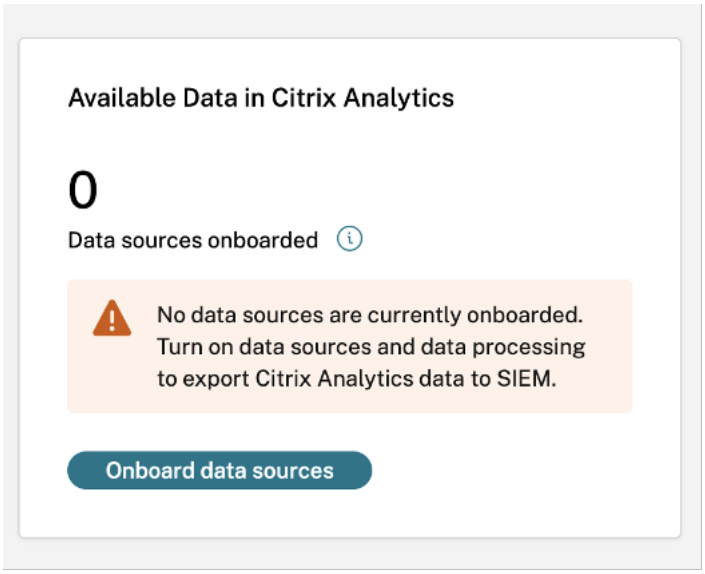


Citrix Analytics で利用可能なデータカードには、Citrix Analytics for Security に組み込まれたデータの中で、最終的に SIEM のインサイトに貢献できるデータソースの数が表示されます。現在、データエクスポートでは、アプリとデスクトップ、ゲートウェイ、セキュアプライベートアクセスの 3 つのデータソースがサポートされています。これらのデータソースがオンボードされていても、データ処理がオフになっているデータソースのデータエクスポートは機能しません。このようなデータソースが検出されると、上の画像のような適切な警告メッセージが表示されます。

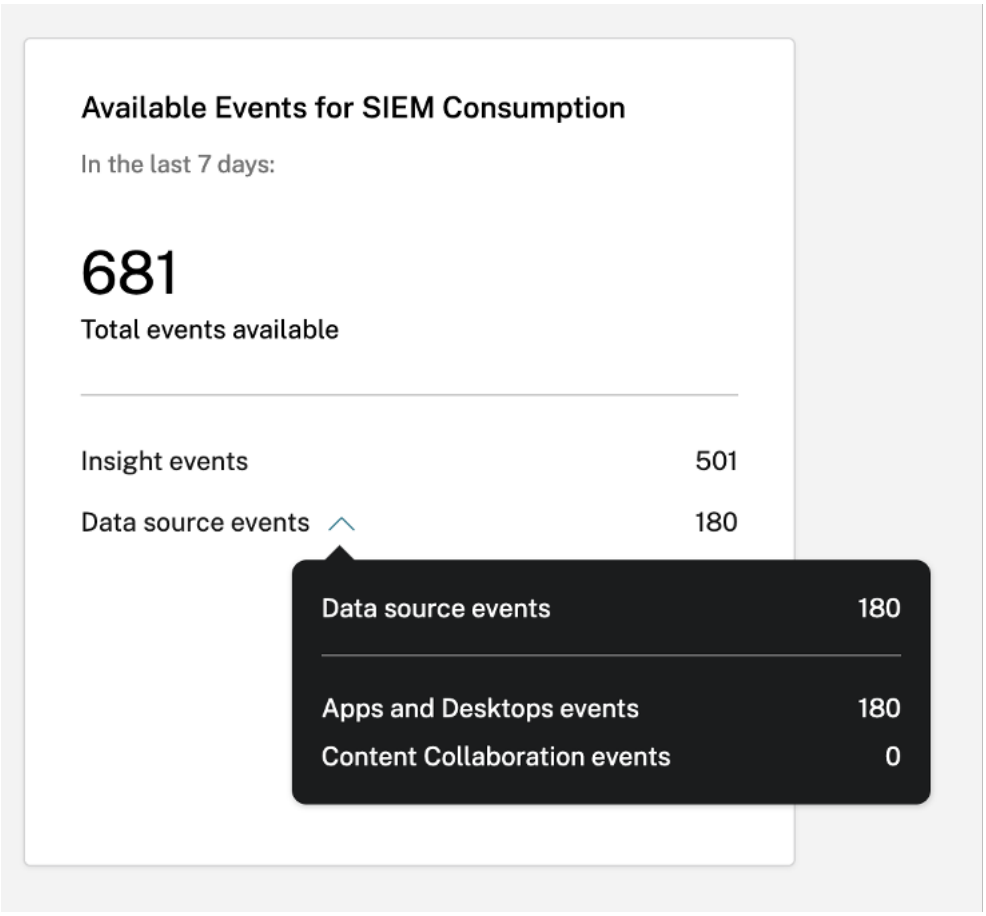
「過去 **7** 日間のイベントを表示」ボタンをクリックすると、管理者はセルフサービス検索ビューにリダイレクトされます。管理者はこのビューを使用して、イベントが Citrix Analytics for Security に流入したことを確認できます。オ

ンボードデータソースボタンはデータソースビューにリダイレクトされ、オンボーディングプロセスを詳しく説明できます。

オンボードされたデータソースがない場合は、次のスクリーンショットのように適切な警告メッセージが表示されます。



SIEM で使用できるイベント



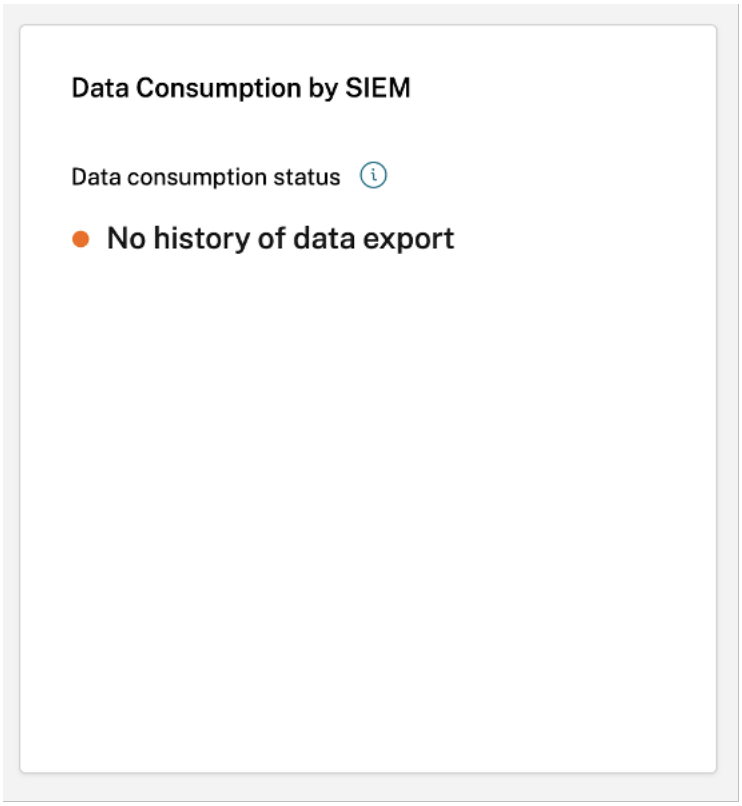
「**SIEM** 消費で利用可能なイベント」カードには、SIEM 環境に流入すると予想されるインサイトイベントとデータソースイベントの数とその内訳が表示されます。拡張すると、エクスポート用の各タイプのデータイベントの詳細も表示されます。

SIEM によるデータ消費

SIEM ごとのデータ消費量カードは、Citrix Analytics によって準備されたデータの SIEM 環境へのフローの状態を示しています。データ消費状況は、**Kafka** トピック内のオフセットの動きに基づいています。使用可能な場合、カードには最後にデータ消費が成功したときのタイムスタンプも表示されます。データ消費ステータスとタイムスタンプの両方が 10 分ごとに更新されます。Kafka コンシューマーグループ/オフセット管理の詳細については、ここをクリックしてください 。

データ消費状況は次のような状態になります。

1. 非アクティブ消費
    - データエクスポートの履歴なし：この状態はオレンジ色の点で表されます。これは、Citrix Analytics で作成されたデータが SIEM 環境に正常に転送されたことがないことを示します。



これには以下の原因が考えられます-

- データソースの設定が正しくないか不完全です。**Citrix Analytics** の「利用可能なデータ」カードを使用して、データソースが十分にあるかどうか、およびそれらのデータソースのデータ処理がエクスポート可能になっているかどうかを確認できます。
- ユーザーアクティビティの欠如。**Citrix Analytics** カードの［利用可能なデータ］の［過去 **7** 日間のイベントを表示］ボタンを使用して、ユーザーアクティビティがないことを確認できます。さらに、「**SIEM** 消費対象イベント」カードを使用して、Citrix Analytics が SIEM に送る準備が整っているインサイトまたはデータソースイベントがあるかどうかを確認できます。
- SIEM の設定が正しくないか不完全です。「構成」タブのアカウント設定ステージが正常に完了したことを確認します。設定が完了すると、アカウント設定段階で緑色のチェックマークが表示されます。

  アカウントの設定が正常に完了しても状態が変わらない場合は、次の点を確認してさらにトラブルシューティングを行います。

  * ファイアウォールの問題または SIEM 設定の誤り—「SIEM 環境のセットアップ」を参照してください。
  * Kafka アカウントの設定や SIEM 環境に関する認証情報の問題—Kafka を使用した SIEM 統合を参照してください。

- アクティブな消費が検出されない：この状態は、少なくとも過去 10 分間、データが SIEM 環境に正常

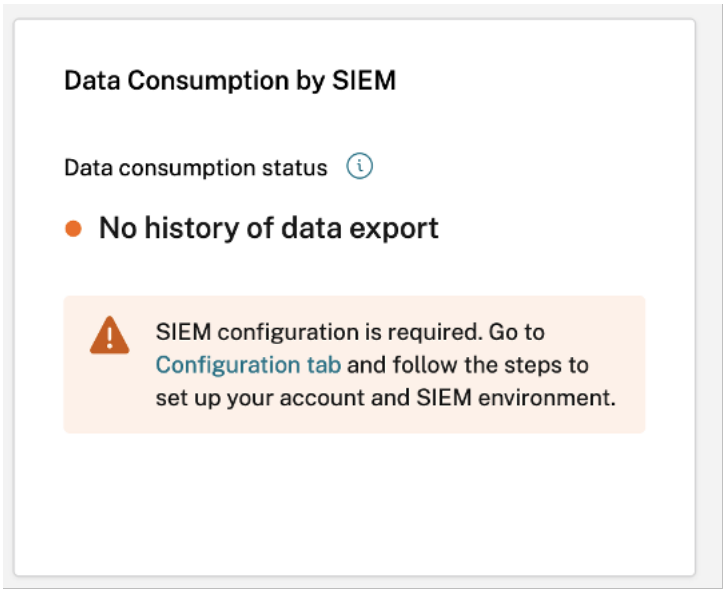
に送信されなかったことを示します。カードには、最後に成功したデータ移動のタイムスタンプも表示されます。「データエクスポートの履歴なし」と同様に、**Citrix Analytics** の「使用可能なデータ」と「SIEM 消費カードで利用可能なイベント **」を使用してこの問題を解決できます。ユーザーアクティビティが十分にあり、利用可能なイベント数が増えている場合は、最後に成功したタイムスタンプに注目して、そのタイムスタンプ以降にファイアウォールの変更やパスワードのローテーションが行われていないかを確認するとよいでしょう。

- エクスポートから **7** 日以上前：この状態は、SIEM でのアクティブな消費が最後に検出されたのが 1 週間以上前であることを示しています。上記の 2 つの状態と同様に、データ消費状態が検出された場合は、「**Citrix Analytics** で利用可能なデータ」と「**SIEM** 消費カードで利用できるイベント」を使用して、SIEM 設定のトラブルシューティングを行います。

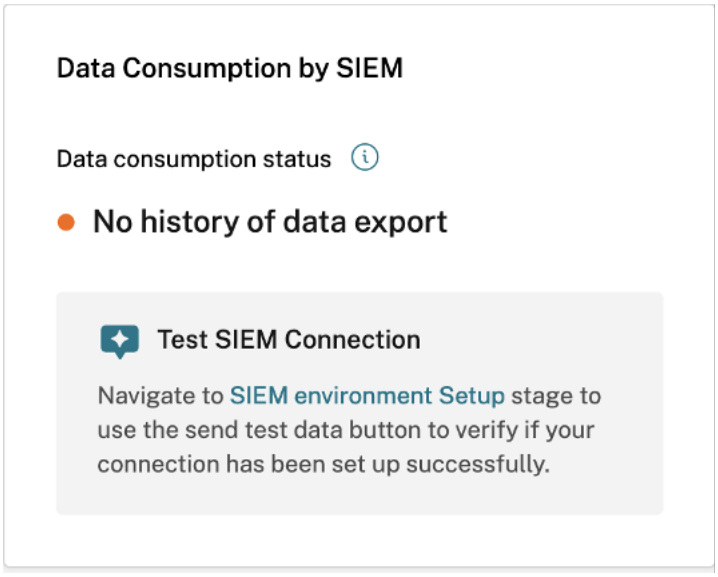
> 注
>
> **Kafka** 保持ポリシー：Citrix Analytics Kafka トピックは、最大 7 日間のみイベントを保持します。潜在的なデータ損失を回避または防止するために、データポーリング間隔を 7 日を超えないように設定することをお勧めします。

使用頻度の低い状態では、トラブルシューティングプロセスを進めるのに役立つ次の警告メッセージが表示されます。

データエクスポートの履歴がないケースで強調したように、SIEM の設定が完了していないと、データが SIEM 環境に流れ込むことはありません。したがって、次のスクリーンショットに示すように、ユーザーは [設定] タブにリダイレクトされ、アカウントの設定を完了します。

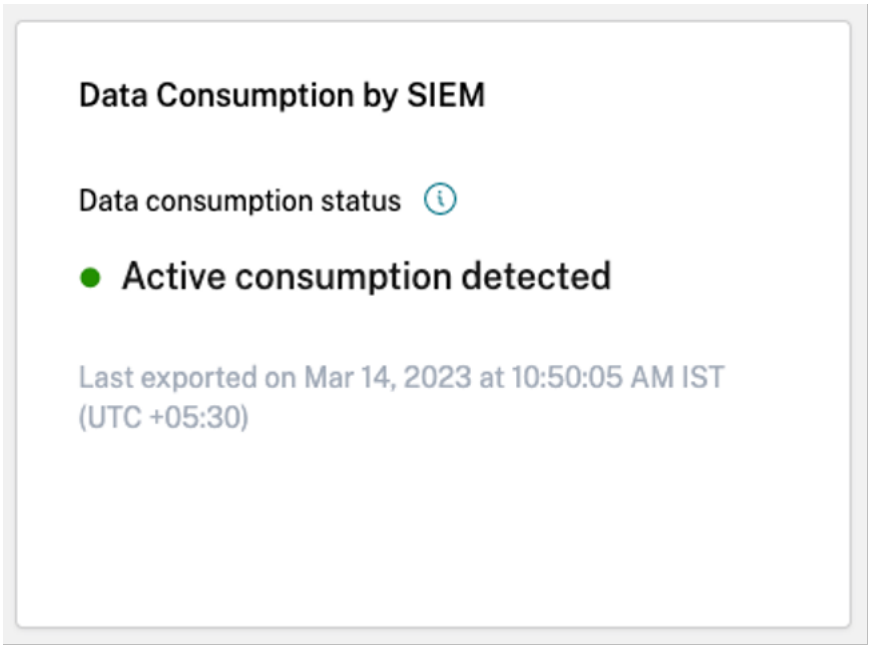


SIEM のセットアップが完了しても、「アクティブな消費量が検出されていない、または 7 日以上前にエクスポートされていない」状態に示されているように、データがアクティブに流れていない場合があります。そのため、次の警告メッセージで強調表示されているように、ユーザーはテストイベント生成セクションに移動して SIEM 接続をテストするように求められます。



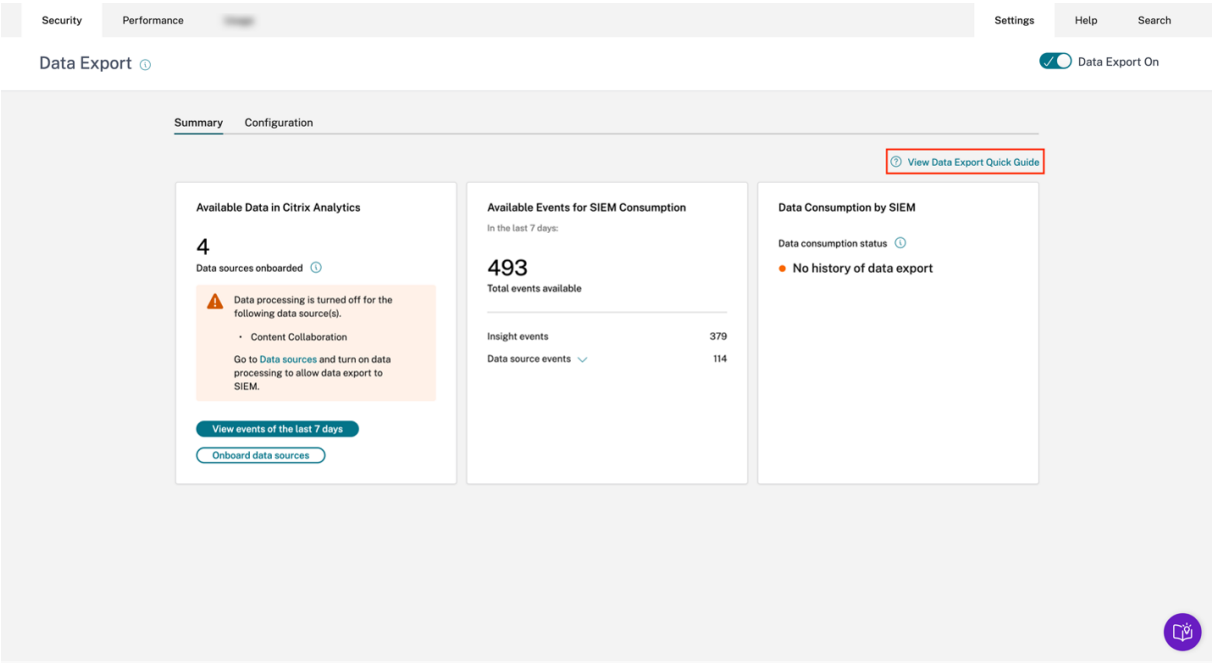
2. アクティブ消費

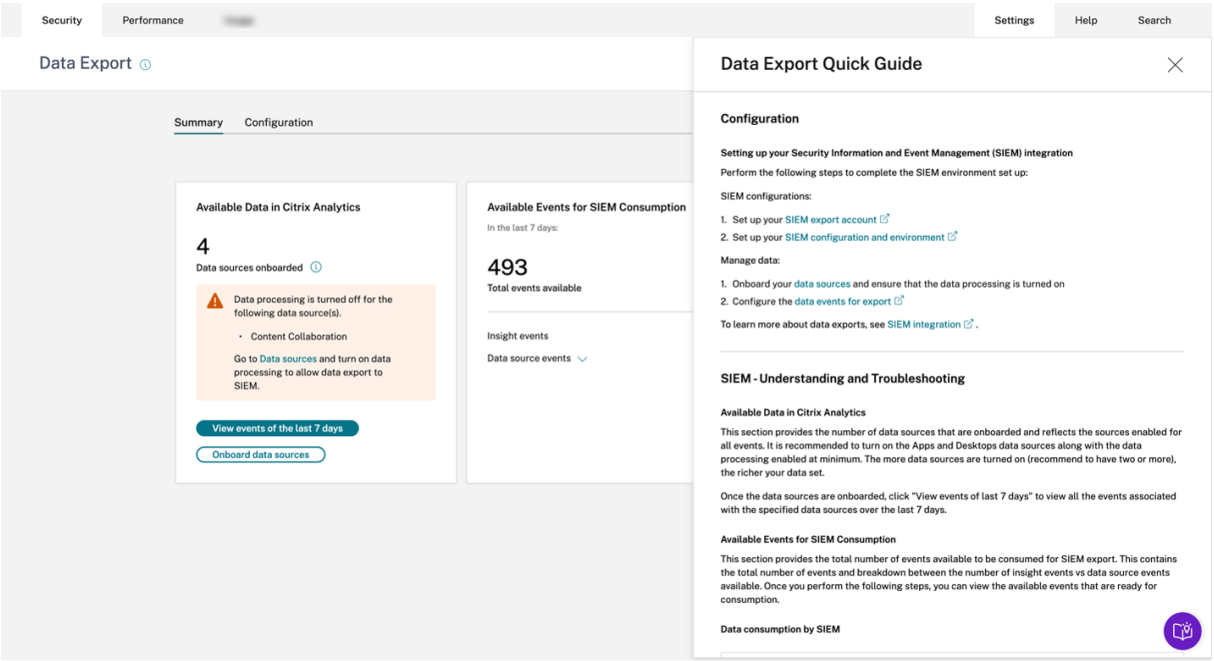
   - アクティブ消費が検出されました: この状態は、SIEM でアクティブ消費が検出されたことを示します。

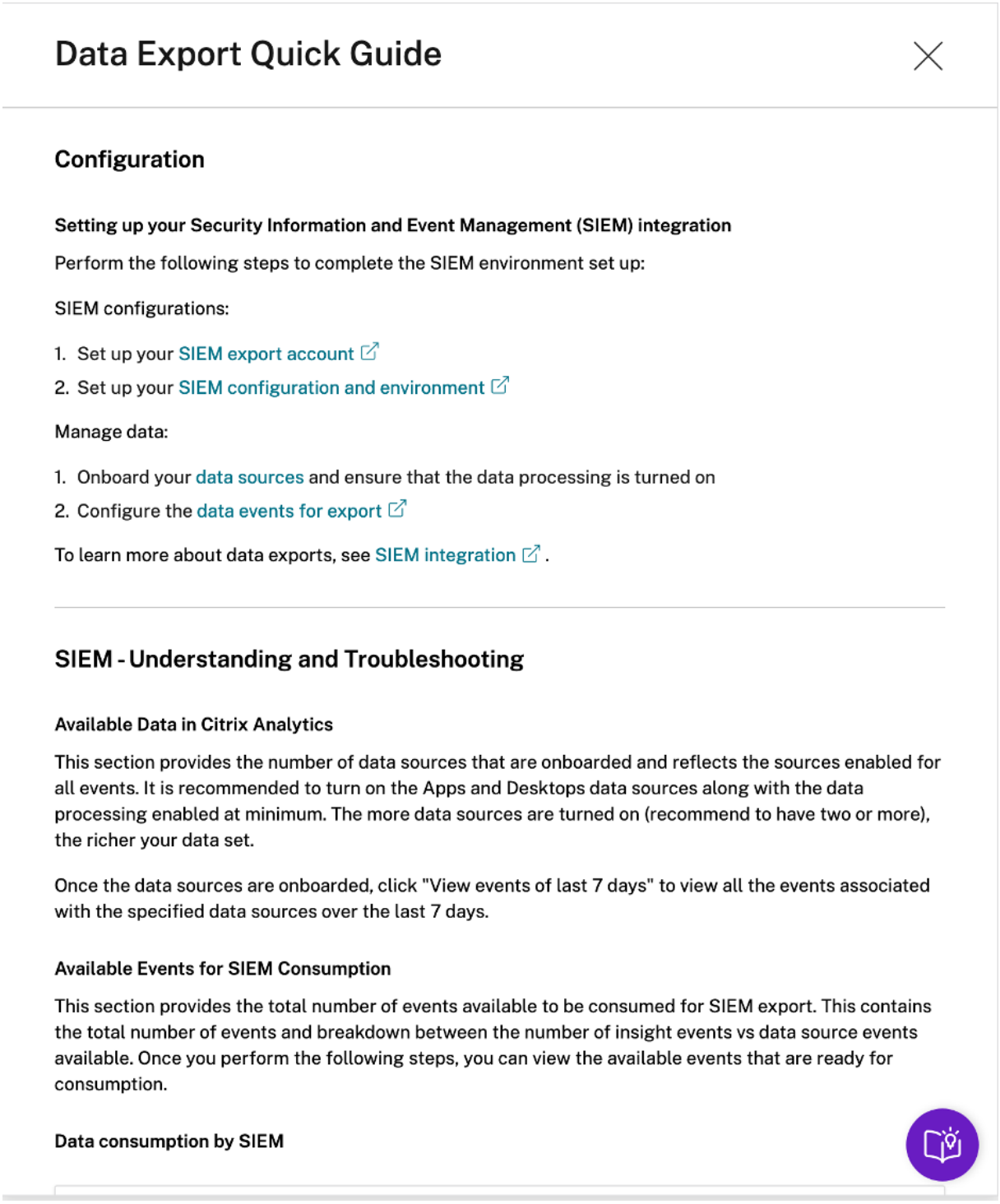


データエクスポートクイックガイド

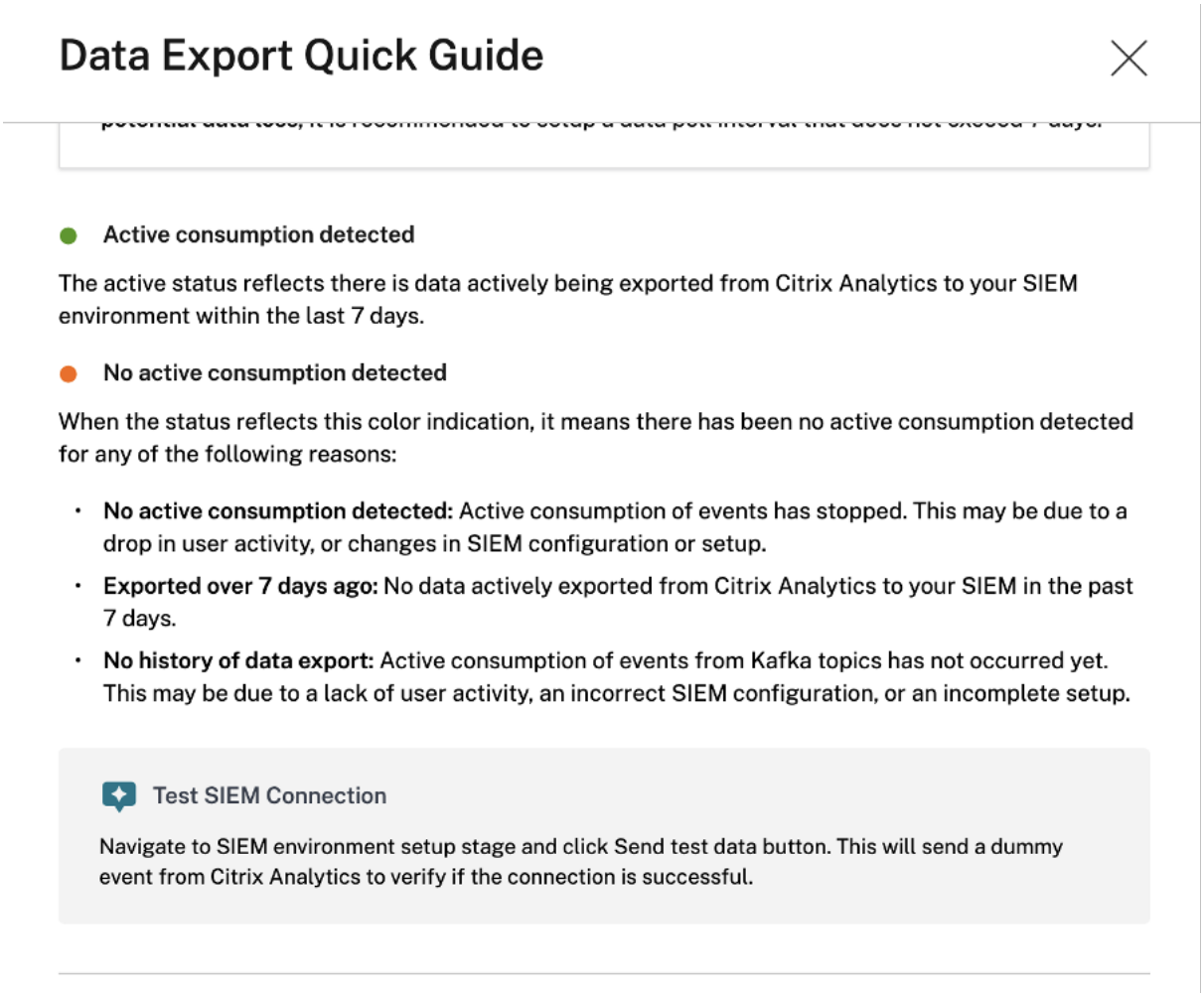
「サマリ」タブには、SIEM 設定の導入、管理、トラブルシューティングを容易にするデータエクスポートクイックガイドブレードが追加されています。クイックガイドには、セキュリティビュー用のデータエクスポートに関する包括的なガイドのほかに、関連するドキュメントへのリンクが掲載されており、SIEM 環境の設定と管理方法に関する役立つヒントも含まれています。





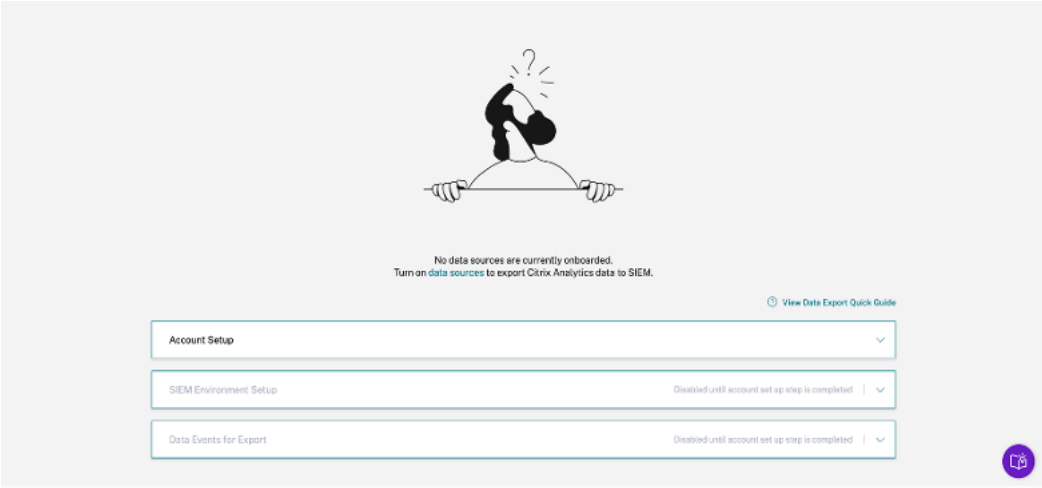


クイックガイドブレードには、ユーザーを **SIEM** 環境設定段階内の **SIEM** 接続テスト段階にリダイレクトするテスト **SIEM** 接続セクションもあります。これにより、ユーザーは SIEM 統合自体が壊れているかどうかを調査できるため、Citrix Analytics for Security がイベントを処理する際に問題が発生する可能性を排除できます。その後、ユーザーは SIEM 接続を修正してデータフローを有効にできます。

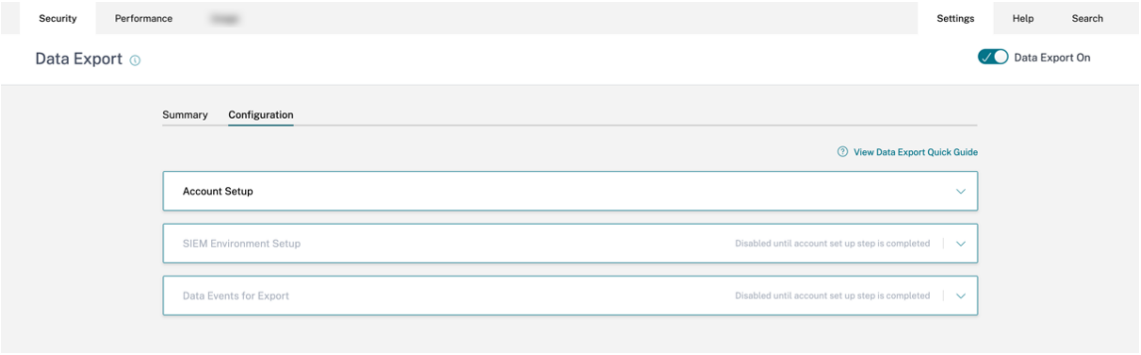


「構成」タブは、導入セットアップのガイドとなると同時に、管理者が SIEM をセットアップする際に役立つヒント、警告メッセージ、よくある落とし穴を知るのにも役立ちます。次の場合に適切な警告が表示されます。

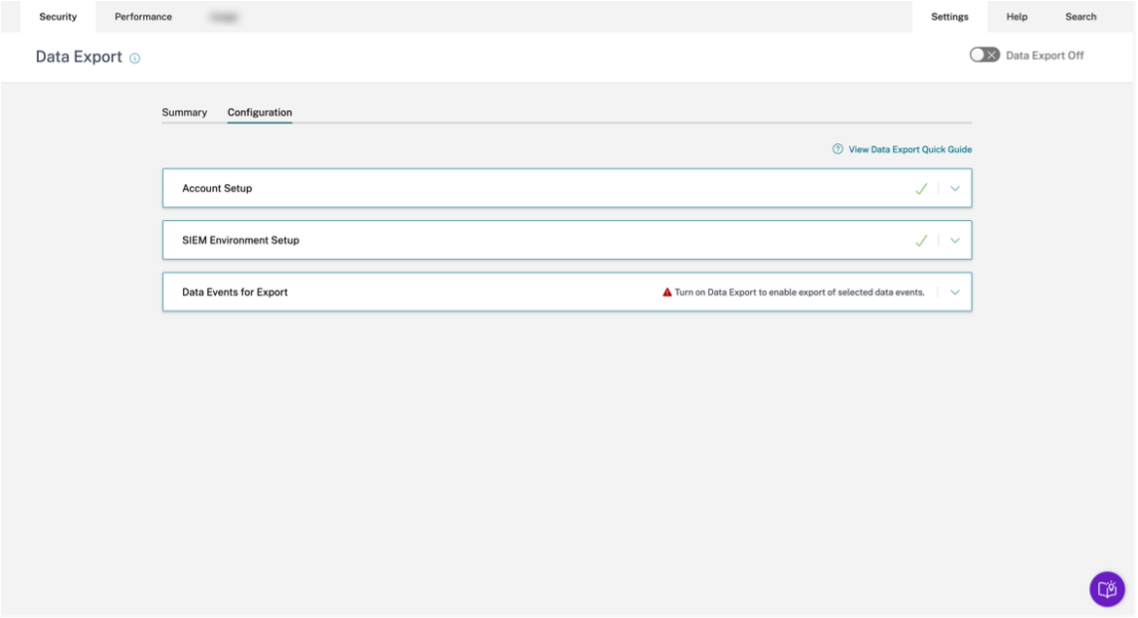
- Citrix Analytics は、データソースがオンボードされていないことを検出します。ユーザーアクティビティに基づいてテレメトリを収集するには、Apps and Desktops をオンボーディングすることをお勧めします。データソースがオンボードされていない場合、SIEM の設定は正常に完了したとしても、データフローは観察されません。



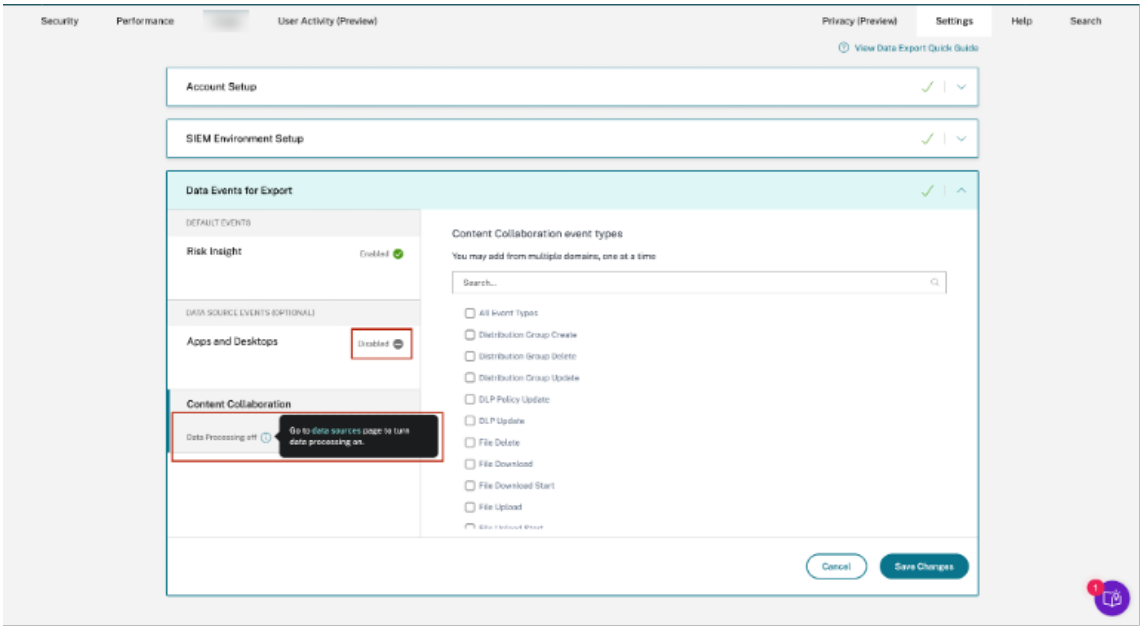
- 次の図に示すように、SIEM Environment Setup と Export ステージのデータイベントは、アカウントの設定が正常に完了するまで無効になります。



- データエクスポートはオフになっています。Data Events for Export ステージの警告は、データエクスポートで何らかの変更が反映されるよう促すものです。



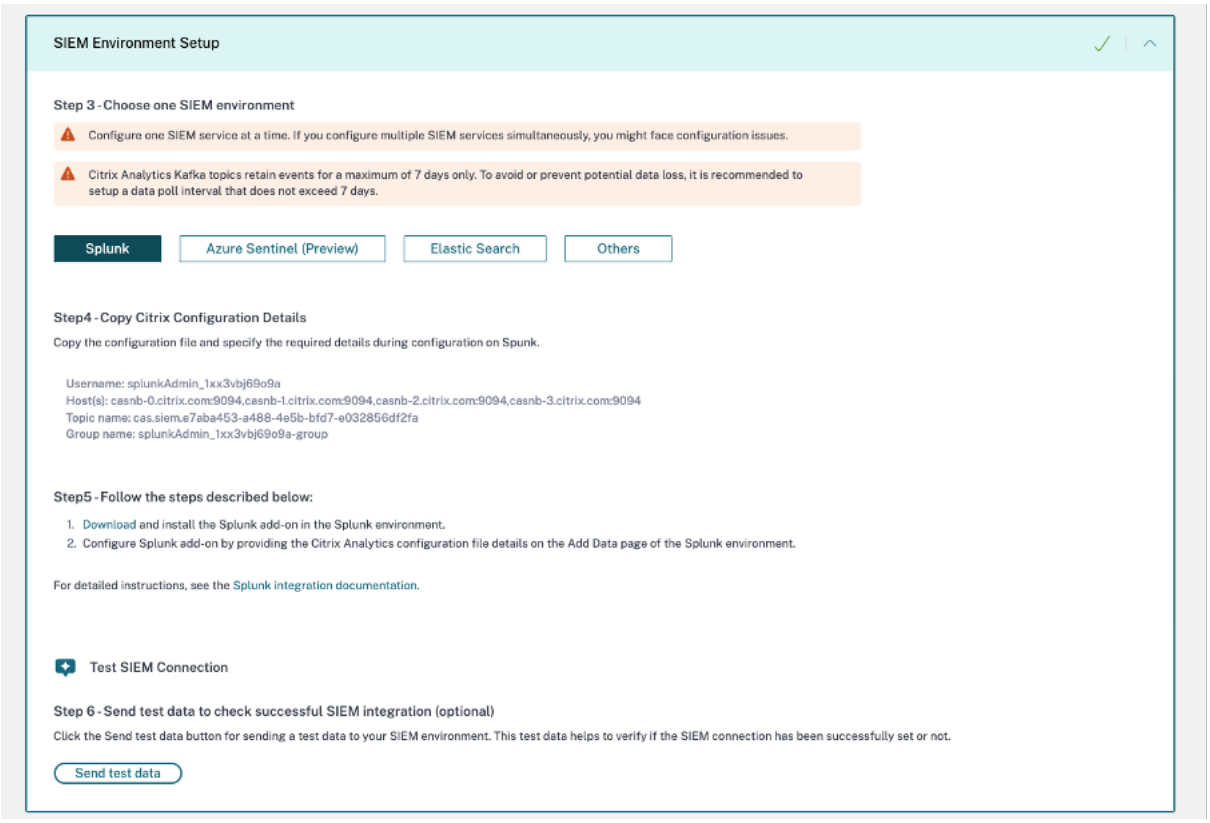
- Data Events for Export ステージでは、特定のデータソースのデータエクスポートが無効になっている場合、データソースイベントは SIEM に流れません。これを有効にするには、目的のデータソースイベントタイプを設定および選択する必要があります。さらに、データが Citrix Analytics に確実に届くように、それぞれのデータソースのデータ処理が有効になっていることを確認してください。



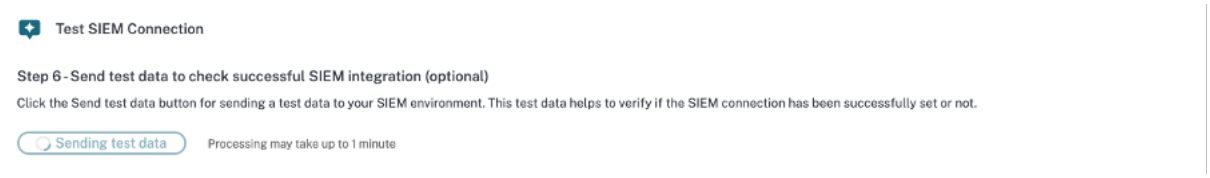
テストイベント生成

テストイベントの生成は、**SIEM** 環境設定段階の一部として提供され、トラブルシューティングのしやすさを向上させます。ユーザーが SIEM の設定を完了すると、テストイベントの生成により、テストイベントを顧客の SIEM データエクスポート Kafka トピックに直接送信することで、SIEM 接続をすばやくテストできます。

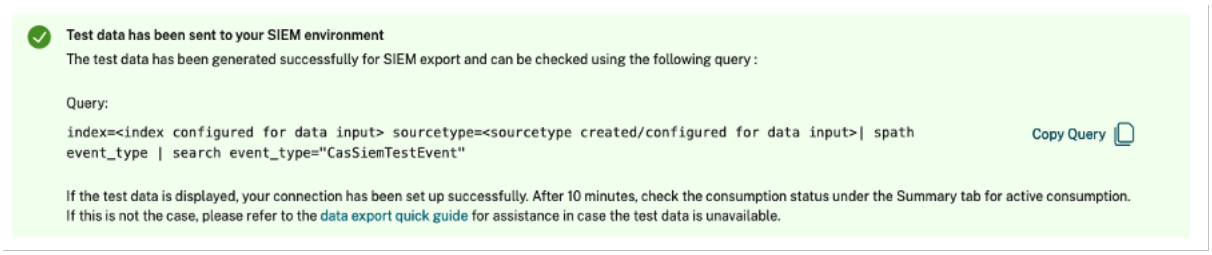
また、新規ユーザーは、新しいデータソースを明示的にオンボーディングしてユーザーアクティビティを生成しなくても、Citrix Analytics との SIEM 統合を迅速にテストできます。

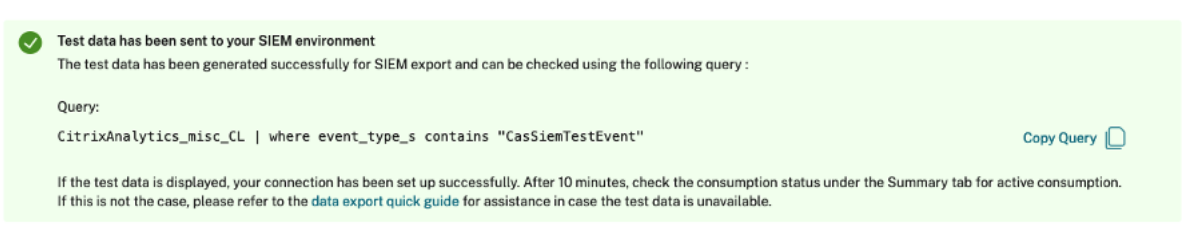


この機能をテストするには、ユーザーは [テストデータの送信] ボタンをクリックする必要があります。これによりダミーのテストイベントが生成され、顧客の SIEM データエクスポート Kafka トピックに送信されます。次のスクリーンショットに示すように、このテストイベント生成プロセスには最大 1 分かかる場合があります。

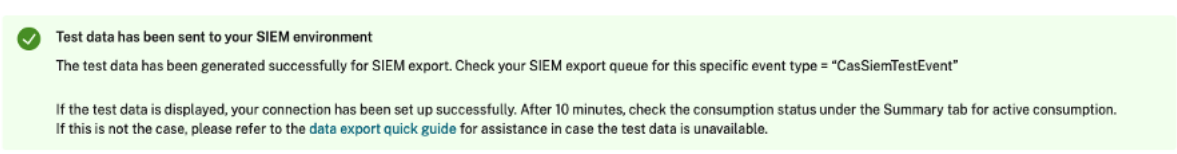


テストイベントデータが顧客の Kafka トピックに正常に書き込まれると、SIEM 接続が成功したことを示す成功メッセージが表示されます。選択した環境（Splunk と Sentinel）に応じて、管理者はクエリをコピーして、テストイベントの SIEM 環境を確認できます。

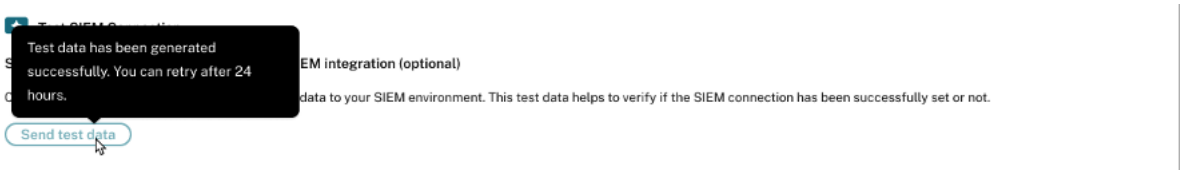




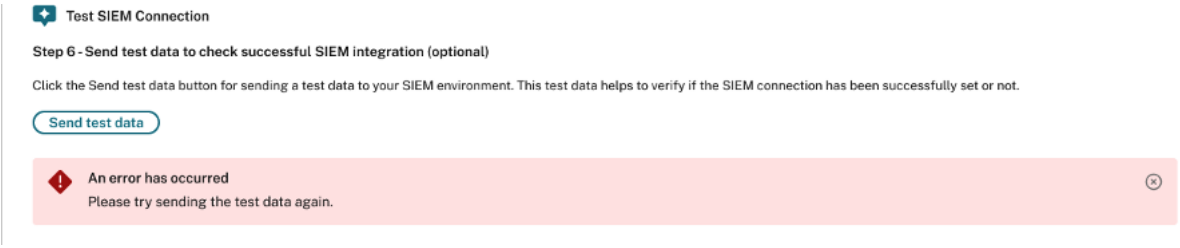
Elasticsearch およびその他の環境では、次の成功メッセージが表示されます。



> 注:
>
> テストイベントが生成されると、[テストデータの送信] ボタンは 24 時間は無効になり、ボタンにカーソルを合わせると次のポップアップが表示されます。最新の成功タイムスタンプから 24 時間が経過すると、ボタンが有効になり、ユーザーが機能を再度テストできるようになります。



テストイベントデータが顧客の Kafka トピックに正常に書き込まれなかった場合、次のスクリーンショットに示すように失敗メッセージが表示されます。ユーザーはデータを再送信して接続をテストできます。



SIEM メールアラート

Citrix Analytics は、SIEM 環境へのデータフローの中断につながる可能性のあるシナリオを管理者に通知する電子メールアラートを送信します。これには、一時的または永続的なセキュリティ対策によるデータ損失につながる可能性のあるアクティビティに関する状況情報が含まれています。また、SIEM データエクスポートのセルフサービスによるトラブルシューティングの進め方にも役立ちます。

この一連のメールアラートには、受信トレイから同じものを見つけるのに役立つ重要なプロパティがいくつかあります。

- メールは、Citrix Cloud 管理者、セキュリティフル管理者、セキュリティ読み取り専用管理者、およびセキュリティとパフォーマンスの読み取り専用管理者に配信されます。
- < donotreplynotifications@citrix.com > 送信者は Citrix Cloud ** です。
- 件名は以下のとおりです：
  - **SIEM** データエクスポートアラート**-**パスワードリセットメールアラートのパスワードがリセットされました。
  - **SIEM** データエクスポートアラート**-**データフロー中断の電子メールアラートでデータフローが停止しました。

メール通知を有効にするにはどうすればいいですか

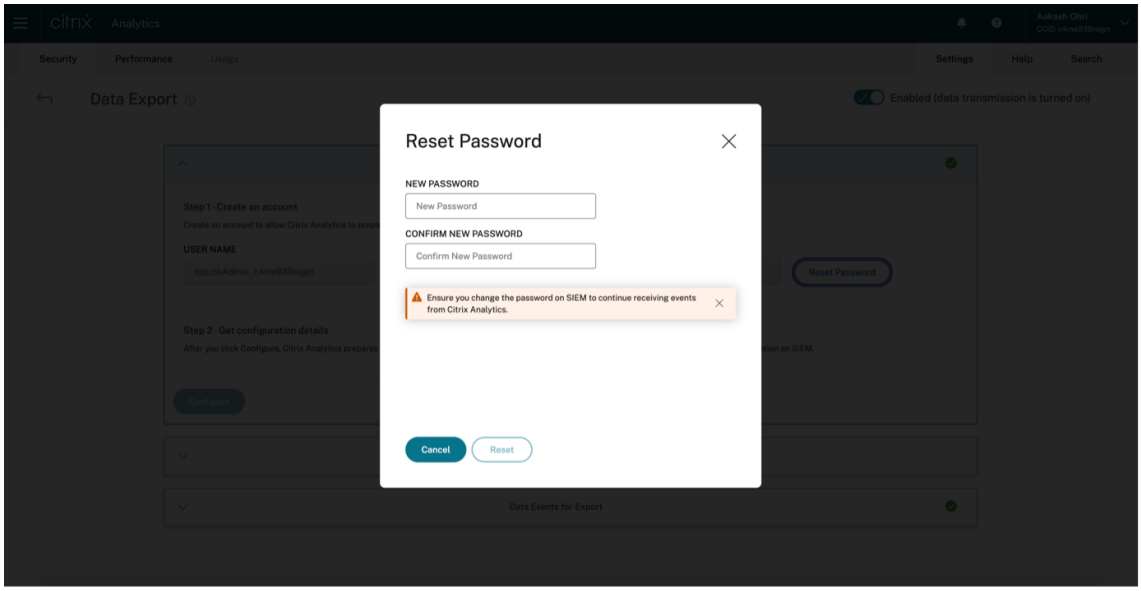
セキュリティ分析を管理するためのカスタムアクセス権（セキュリティフル管理者、セキュリティ読み取り専用管理者、セキュリティ、パフォーマンス読み取り専用）を持つ Citrix Cloud 管理者の場合、メール通知は常に Citrix Cloud アカウントで有効になります。デフォルトでは、毎週のメール通知は Citrix セキュリティ管理者（デフォルトリスト）に送信されます。このアラートを受け取る配布リストを変更することもできます。詳細については、「」を参照してください。

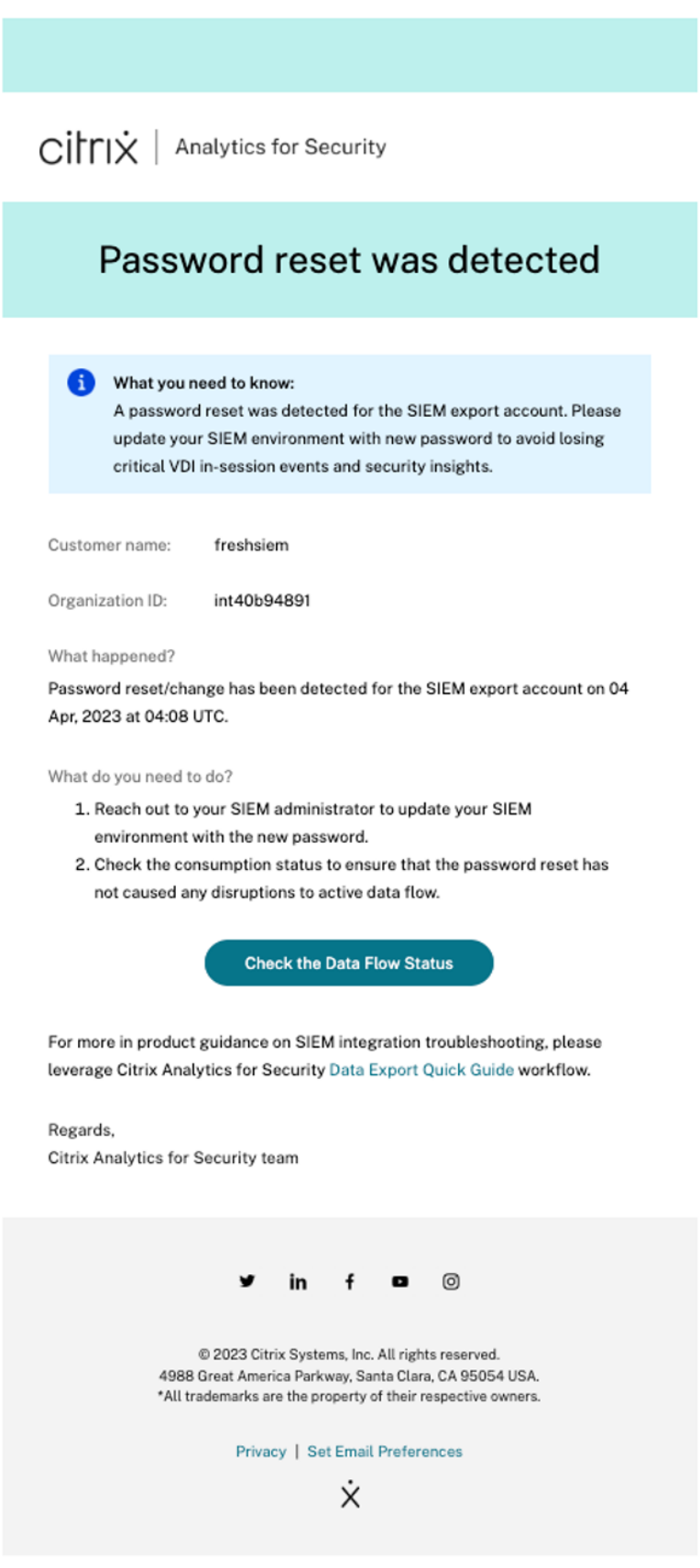
セキュリティ分析を管理するためのカスタムアクセス権限（セキュリティフル管理者、セキュリティ読み取り専用管理者、セキュリティとパフォーマンス読み取り専用）を持つ Citrix Cloud 管理者の場合、電子メール通知は Citrix Cloud アカウントで常に有効になります。

SIEM メールアラートの種類

1. **SIEM** パスワードリセットメールアラート

   SIEM パスワードリセットアラートメールは、データエクスポートページでアカウントパスワードがリセットされたときに受信されます。Citrix Analytics UI だけで SIEM パスワードをリセットすると、SIEM で構成されているものとパスワードが一致しなくなる可能性があります。これはデータフローの中断につながります。このメールアラートには、パスワードがリセットされた時刻が含まれています。データフローが停止した場合は、[概要] タブに移動し、「最終エクスポート日」のタイムスタンプがパスワードリセットのタイムスタンプに近いかどうかを確認して、必要なパスワード変更を中継できます。これにより、デバッグプロセスが短縮され、SIEM 環境への正常なデータフローをすぐに戻すことができます。





citrix | Analytics for Security

Password reset was detected

What you need to know:
A password reset was detected for the SIEM export account. Please update your SIEM environment with new password to avoid losing critical VDI in-session events and security insights.

Customer name: freshsiem

Organization ID: int40b94891

What happened?

Password reset/change has been detected for the SIEM export account on 04 Apr, 2023 at 04:08 UTC.

What do you need to do?

1. Reach out to your SIEM administrator to update your SIEM environment with the new password.
2. Check the consumption status to ensure that the password reset has not caused any disruptions to active data flow.

Check the Data Flow Status

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

Regards,
Citrix Analytics for Security team

2. **24** 時間のデータフロー中断メールアラート

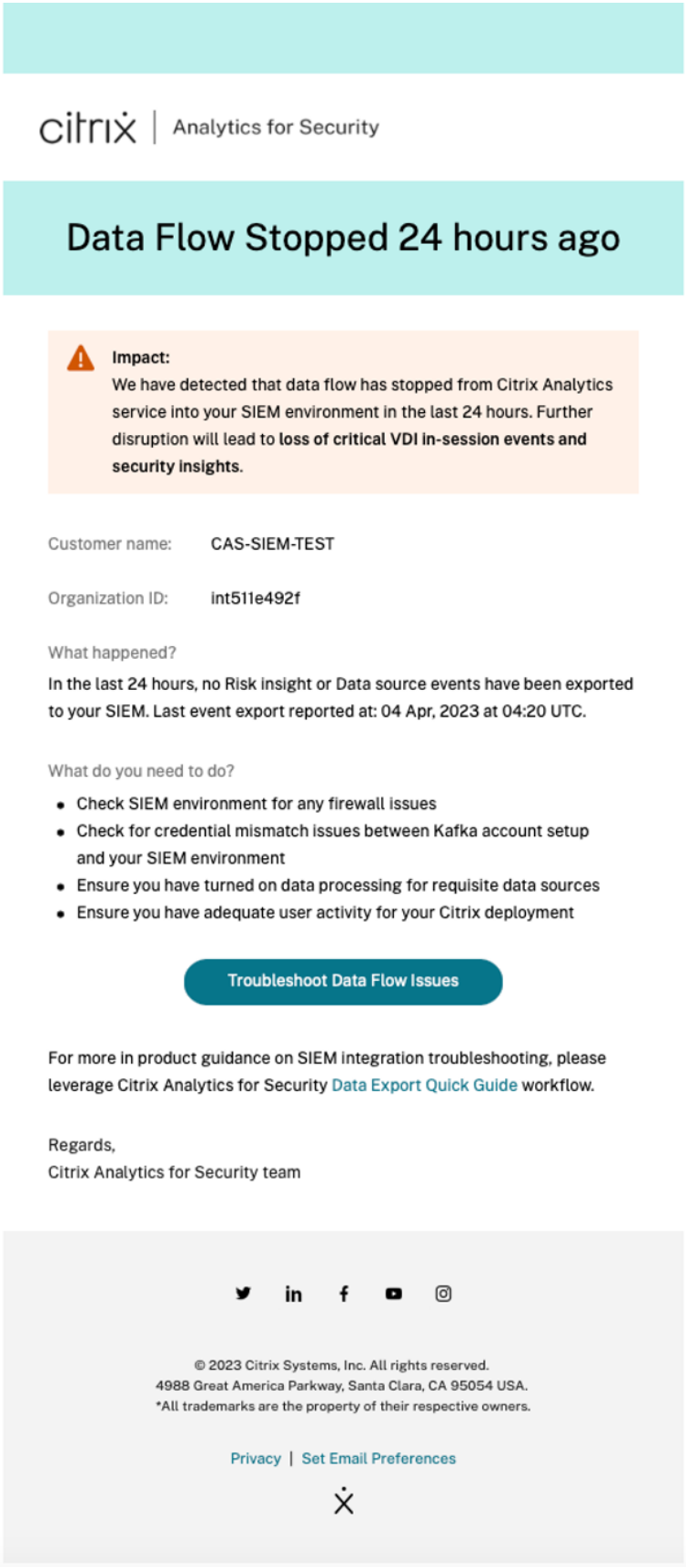
   このメールアラートは、Citrix Analytics サービスから SIEM 環境へのデータフローが 24 時間以上中断されたときに送信されます。メールには、最後のイベントがエクスポートされた時刻と、データフローを元に戻すために実行できるトラブルシューティングに役立つクイックヒントが記載されています。今こそ、セキュリティ対策が施されたデータを失わないように、データフローを迅速に回復させる適切なタイミングです。

3. **7** 日間のデータフロー中断メールアラート

   このメールアラートは、Citrix Analytics サービスから SIEM 環境へのデータフローが 7 日以上中断された場合に送信されます。お客様の Kafka トピックの保存期間は 7 日間であるため、トラブルシューティングのヒントに従い、データエクスポートページにあるクイックガイドを参考にして、これ以上データを失わないようにすることが重要です。このメールは、セキュリティ対策の情報が永久に失われる状況を警告するものです。

4. **30** 日間のデータフロー中断メールアラート

   このメールアラートは、Citrix Analytics サービスから SIEM 環境へのデータフローが 30 日間以上中断された場合に送信されます。今では、お客様はセキュリティ対策済みのデータを失ってしまったため、トラブルシューティング機能を使用してできるだけ早くフローを回復することが不可欠です。



citrix | Analytics for Security

Data Flow Stopped 24 hours ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in the last 24 hours. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 24 hours, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 04 Apr, 2023 at 04:20 UTC.

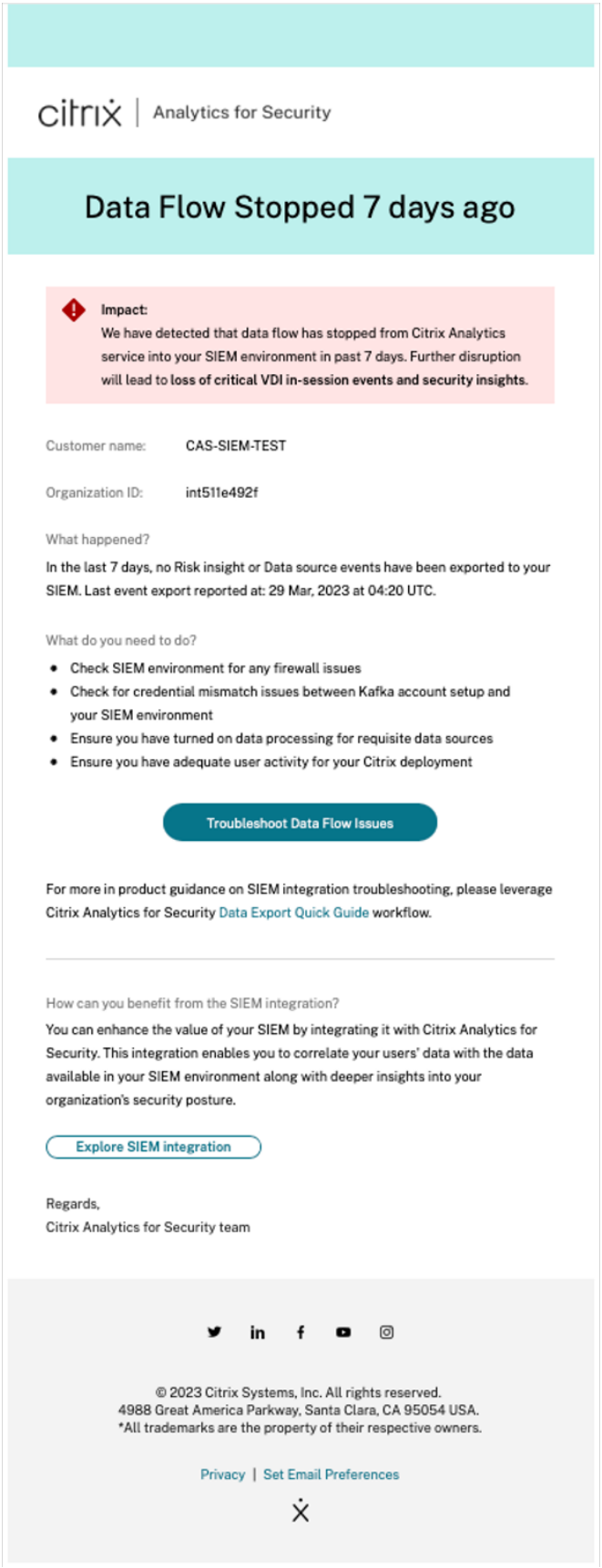
What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

Regards,
Citrix Analytics for Security team



citrix | Analytics for Security

Data Flow Stopped 7 days ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in past 7 days. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 7 days, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 29 Mar, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

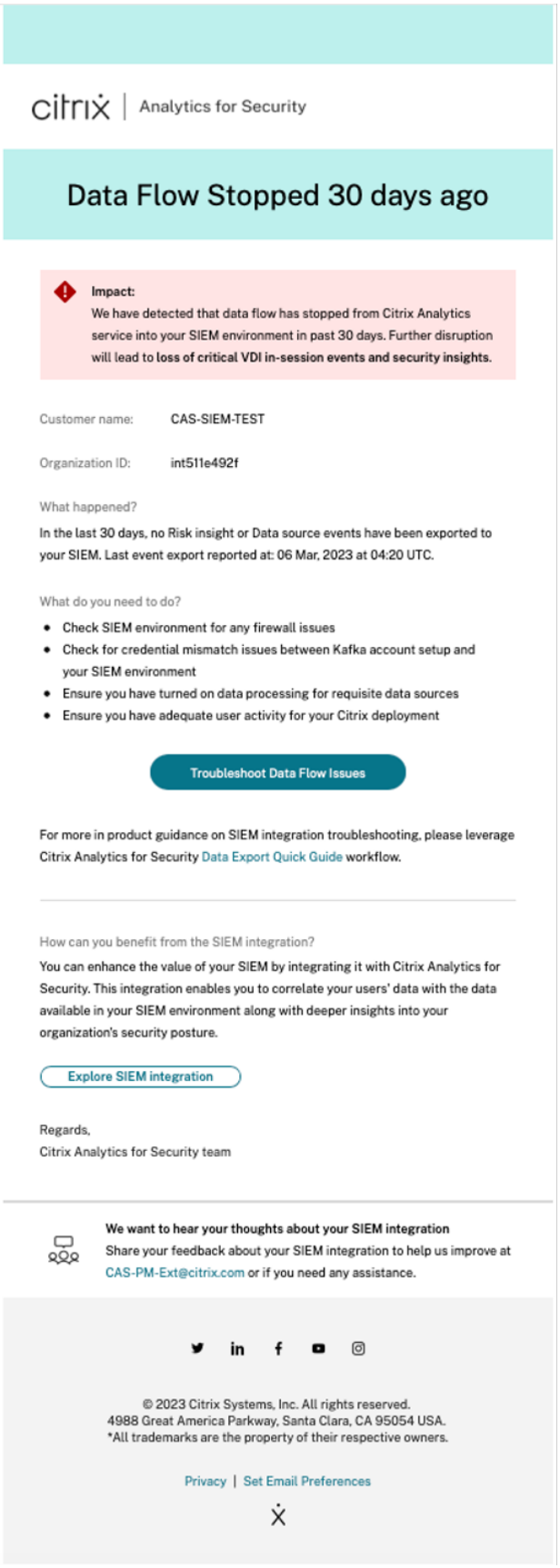
For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

How can you benefit from the SIEM integration?

You can enhance the value of your SIEM by integrating it with Citrix Analytics for Security. This integration enables you to correlate your users' data with the data available in your SIEM environment along with deeper insights into your organization's security posture.

Explore SIEM integration

Regards,
Citrix Analytics for Security team



citrix | Analytics for Security

Data Flow Stopped 30 days ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in past 30 days. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 30 days, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 06 Mar, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

How can you benefit from the SIEM integration?

You can enhance the value of your SIEM by integrating it with Citrix Analytics for Security. This integration enables you to correlate your users' data with the data available in your SIEM environment along with deeper insights into your organization's security posture.

Explore SIEM integration

Regards,
Citrix Analytics for Security team

We want to hear your thoughts about your SIEM integration
Share your feedback about your SIEM integration to help us improve at CAS-PM-Ext@citrix.com or if you need any assistance.

Security Insight 用のシグマ署名の例

December 7, 2023

このページには、管理者が Citrix Security Analytics を使用して有意義な結果を達成するのに役立つクエリの例が含まれています。

これらの例は、以下のカテゴリのリスクを対象としています:

- 侵害されたエンドポイント
- インサイダーの脅威
- データ流出

これらの例の使用方法

データソースを表示し、データ処理をオンにする

データソースを表示するには、Citrix Analytics GUI で［設定］**>**［データソース］**>**［セキュリティ］をクリックします。[アプリとデスクトップ**-Workspace** アプリ] サイトカードが [データソース] ページに表示されます。Citrix Analytics がこのデータソースのデータの処理を開始できるようにするには、［データ処理を有効にする］をクリックします。

Citrix Analytics for Security は、次の 2 種類のリスクインサイトデータを SIEM サービスに送信します:

- リスクインサイトイベント (デフォルトエクスポート)
- データソースイベント (オプションのエクスポート)

SIEM 環境の一部として、リスクインサイトイベントデータソースが利用可能で、デフォルトでは常に有効になっています。詳しくは、「Citrix Analytics for Security から SIEM サービスにエクスポートされるデータイベント」を参照してください。

CAS 署名または Sigma 署名を使用して、データソース内の特定のユーザーイベントを検証できます。CAS クエリには、Citrix Analytics GUI のセルフサービス検索ページからアクセスできます。シグマ署名はシンプルまたはユーザーフレンドリーな形式で記述されているため、さまざまな SIEM 環境と互換性があります。

CAS クエリーの使用

セルフサービス検索ページの CAS クエリを使用して、さまざまなデータソースから受信したユーザーイベントを検索してフィルタリングできます。Citrix Analytics GUI から［検索］をクリックし、検索ボックスにクエリを入力します。詳細については、「セルフサービス検索の使用方法」を参照してください。

既存のテンプレートを使用してカスタムリスク指標を作成することもできます。カスタムリスク指標を作成するには、[セキュリティ] **>** [カスタムリスク指標] **>** [指標の作成] に移動します。詳細については、「カスタムリスク指標の作成」を参照してください。

シグマ署名の使用

Sigma は、アナリストがログイベントの説明に使用できるテキストベースのクエリを作成するためのユーザーフレンドリーなオープンシグネチャ形式で、検出を簡単に記述できます。Sigma 署名を SIEM ツールのクエリ言語に変換する方法はいくつかあります。

- シグマが提供する CLI ツールと Python SDK を使用できます。シグマ署名の詳細については、「ルールの使用法」を参照してください。
- 無料利用枠を提供する uncoder.io のシグマ翻訳エンジンなどの公開ツールを使用できます。

さまざまなリスクインサイトについては、以下のさまざまなカスタム指標のユースケースを参照してください:

- 認可されていないブラウザ
- 認可されていないオペレーティングシステム
- 未承認のワークスペースアプリバージョン
- 許可リスト外の不正なオペレーティングシステム
- 不正な IP アドレスまたはサブネット
- 無許可の仮想アプリ
- 珍しいデスクトップ名
- 特定のアプリケーションを監視する
- SaaS アプリからの印刷
- SaaS アプリでのクリップボードの使用

侵害されたエンドポイント

November 26, 2023

認可されていないブラウザ

これは、ユーザーが組織の IT ポリシーまたはセキュリティの脆弱性により許可されていないブラウザの種類またはバージョンからコンテンツにアクセスしようとした場合に発生します。

詳細

データソース: アプリとデスクトップ (Workspace アプリ)

CAS クエリー

```
Event-Type = "Session.Logon" AND Browser-Name !~ "<Browser-Name>"
<!--NeedCopy-->
```

Session.Logon イベントは、ユーザーが資格情報を入力してアプリまたはデスクトップセッションにログオンしたときにトリガーされます。

Sigma シグネチャー

```
author: Citrix
date: 2023/01/31
description: This occurs when a user accesses content from an
    authorized browser which might cause an undesirable event or action
    through the internet.
detection:
  condition: index_selection and selection and not filter
  filter:
  - browser_name|contains: '<Browser-Name>'
  index_selection:
    source: cas_siem_consumer://<env>_<tenant_identifier>
  selection:
  - occurrence_event_type: Session.logon
logsource:
  product: citrixanalytics
  service: security
title: Access from unauthorized browser
<!--NeedCopy-->
```

認可されていないオペレーティングシステム

これは、組織の IT ポリシーまたはセキュリティの脆弱性により許可されていないオペレーティングシステムのタイプまたはバージョンのデバイスにユーザーがアクセスしようとした場合に発生します。

詳細

データソース: アプリとデスクトップ (Workspace アプリ)

CAS クエリー

```
Event-Type = "Session.Logon" AND OS-Name ~ "<OS-Name>" AND OS-Version =
    "<OS-Version>" AND OS-Extra-Info = "<OS-Extra-Info>"
<!--NeedCopy-->
```


Sigma シグネチャー

```
author: Citrix
date: 2023/01/31
description: This occurs when a user attempts to access apps from
    servers with blocked listed operating systems.
detection:
  condition: index_selection and selection
  filter_null: []
  index_selection:
    source: cas_siem_consumer://<env>_<tenant_identifier>
  selection:
    occurrence_event_type: Session.logon
    os_name|contains: '<OS-Name>'
    os_version: '<OS-Version>'
    os_extra_info: '<OS-Extra-Info>'
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized operating systems in block list
<!--NeedCopy-->
```

不正な **IP** アドレスまたはサブネット

これは、組織の IT ポリシーで許可されていないとマークされている IP アドレスまたは範囲からユーザーがアクセスを試みた場合に発生します。

詳細

データソース: アプリとデスクトップ (Workspace アプリ)

CAS クエリー

```
Event-Type = "Session.Logon" AND Client-IP = "<XX.YY.ZZ.*>"
<!--NeedCopy-->
```

Sigma シグネチャー

```
author: Citrix
date: 2023/01/31
description: This occurs when a user accessing content from an
    unauthorized IPs which might cause an undesirable event or action
    through the internet.
detection:
  condition: selection and not filter_null and filter
```



```
  filter:
  - client_ip: '<IP>'
  filter_null:
  - client_ip: null
  selection:
  - occurrence_event_type: Session.Logon
logsource:
  product: citrixanalytics
  service: security
title: Access from unauthorized IP
<!--NeedCopy-->
```

許可リスト外の不正なオペレーティングシステム

これは、ユーザーが許可リストに含まれていないオペレーティングシステムをホストするサーバーからアプリケーションにアクセスしようとしたときに発生します。

詳細

データソース: アプリとデスクトップ (Workspace アプリ)

CAS クエリー

```
Event-Type = "Session.Logon" AND OS-Name !~ "<OS-Name>" AND OS-Version
    != "<OS-Version>" AND OS-Extra-Info != "<OS-Extra-Info>"
<!--NeedCopy-->
```

Sigma シグネチャー

```
author: Citrix
date: 2023/01/31
description: Unauthorized operating systems outside allow list
detection:
  condition: selection and not filter_null and not filter_os and not
     filter_os_version and not filter_os_extra
  filter_os:
  - os_name|contains: '<OS INFO>'
  filter_os_version:
  - os_version: '<OS Version>'
  filter_os_extra:
  - os_extra_info: '<OS Extra Info>'
  filter_null:
  - os_name: null
  - os_version: null
  - os_extra_info: null
```



```
    selection:
    - occurrence_event_type: Session.Logon
  logsource:
    product: citrixanalytics
    service: security
  title: Unauthorized operating systems outside allow list
  <!--NeedCopy-->
```

未承認の **Workspace** アプリバージョン

これは、サポートされていないクライアントバージョンの Workspace アプリにユーザーがアクセスしようとしたときに発生します。このような場合、ユーザーはクライアントをサポートされているバージョンにアップグレードする必要があります。詳細については、「サポートクライアントバージョン」を参照してください。

詳細

データソース: アプリとデスクトップ (Workspace アプリ)

CAS クエリー

```
Event-Type = "Session.Logon" AND Client-Type IN ("Windows", "Macintosh"
    , "Unix/Linux") AND Workspace-App-Version != "20*" AND Workspace-App
    -Version != "21*"
<!--NeedCopy-->
```

Sigma シグネチャー

```
author: Citrix
date: 2023/01/31
description: Unsupported Workspace app versions
detection:
  condition: selection and not filter_null and filter_product and not
     filter_product_version
  filter_product:
  - product: ['Windows', 'Mac', '<Other type>']
  filter_product_version:
  - product_version|contains: ['<Product Version1>', '<Product Version2
     >']
  filter_null:
  - product: null
  - product_version: null
  selection:
  - occurrence_event_type: Session.Logon
logsource:
  product: citrixanalytics
```



```
  service: security
title: Unsupported Workspace app versions
<!--NeedCopy-->
```

インサイダーの脅威

November 26, 2023

珍しいデスクトップ名

これは、ユーザーが通常とは見なされないデスクトップを起動しようとしたときに発生します。

詳細

データソース: アプリとデスクトップ (Workspace アプリ)

CAS クエリー

```
Event-Type = "Session.Logon" AND Session-Launch-Type = "desktop" AND
    App-Name ~ "<Desktop Name>"
<!--NeedCopy-->
```

Sigma シグネチャー

```
author: Citrix
date: 2023/01/31
description: Unusual desktop names
detection:
  condition: selection1 and selection2 and not filter_null and
     filter_app_name
  filter_app_name:
  - app_name|contains: '<App Name>'
  filter_null:
  - app_name: null
  selection1:
  - occurrence_event_type: Citrix.EventMonitor.AppStart
  selection2:
  - launch_type: 'desktop'
logsource:
  product: citrixanalytics
  service: security
```



```
title: Unusual desktop names
<!--NeedCopy-->
```

特定のプロセスを監視する

これは、ウォッチリストにある公開アプリケーションをユーザーが起動したときに発生します。その目的は、特定の公開アプリケーションの使用状況を監視することかもしれません。

詳細

データソース: アプリとデスクトップ (Session Recording)

CAS クエリー

```
Event-Type = "Citrix.EventMonitor.AppStart" AND App-Name IN ("<App-Name-1>", "<App-Name-2>")
<!--NeedCopy-->
```

Sigma シグネチャー

```
author: Citrix
date: 2023/01/31
description: Monitor specific process
detection:
  condition: selection and not filter_null and filter_app_name
  filter_app_name:
  - app_name: ['<App-Name1>', '<App-Name2>']
  filter_null:
  - app_name: null
  selection:
  - occurrence_event_type: Citrix.EventMonitor.AppStart
logsource:
  product: citrixanalytics
  service: security
title: Monitor specific process
<!--NeedCopy-->
```

無許可の仮想アプリ

これは、ユーザーが不正な仮想アプリにアクセスしたときに発生します。

詳細

データソース: アプリとデスクトップ (Workspace アプリ)

CAS クエリー

```
Event-Type = "App.Start" AND App-Name IN ("<App-Name1>", "<App-Name2>")
<!--NeedCopy-->
```

Sigma シグネチャー

```
date: 2023/01/31
description: Unauthorized virtual apps
detection:
  condition: selection and not filter_null and filter_app_name
  filter_app_name:
  - app_name: ['<App-Name1>', '<App-Name2>']
  filter_null:
  - app_name: null
  selection:
  - occurrence_event_type: App.Start
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized virtual apps
<!--NeedCopy-->
```

データ流出

November 26, 2023

SaaS アプリからの印刷

これは、印刷が許可されていない SaaS アプリケーションからファイルを印刷した場合に発生します。SaaS アプリケーションでの印刷操作による潜在的なデータ漏えいを検出します。

詳細

データソース: アプリとデスクトップ (Citrix Enterprise Browser)

CAS クエリー

```
Event-Type = "App.SaaS.File.Print" AND SaaS-App-Name = "<App-Name>"
<!--NeedCopy-->
```

Sigma シグネチャー

```
author: Citrix
date: 2023/01/31
description: Printing from SaaS apps
detection:
  condition: selection and not filter_null and filter_saas_app_name
  filter_saas_app_name:
  - saas_app_name: '<App-Name>'
  filter_null:
  - saas_app_name: null
  selection:
  - occurrence_event_type: App.SaaS.File.Print
logsource:
  product: citrixanalytics
  service: security
title: Printing from SaaS apps
<!--NeedCopy-->
```

SaaS アプリでのクリップボードの使用

これは、任意の SaaS アプリケーションから切り取り、コピー、貼り付けが行われたときに発生します。クリップボードの操作を監視することで、組織内の SaaS アプリケーションからの潜在的なデータ漏洩を検出します。

詳細

データソース: アプリとデスクトップ (Citrix Enterprise Browser)

CAS クエリー

```
Event-Type = "App.SaaS.Clipboard" AND Clipboard-Result = "success" AND
    Clipboard-Operation IN ( "copy" , "cut" )
<!--NeedCopy-->
```

Sigma シグネチャー


```
author: Citrix
date: 2023/01/31
description: Clipboard usage on SaaS apps
detection:
  condition: selection and not filter_null and
     filter_clipboard_details_result and filter_clipboard_operation
  filter_clipboard_details_result:
  - clipboard_details_result: 'success'
  filter_clipboard_operation:
  - clipboard_operation: ['cut', 'copy', '<Other Operation>']
  filter_null:
  - clipboard_operation: null
  - clipboard_details_result: null
  selection:
  - occurrence_event_type: App.SaaS.Clipboard
logsource:
  product: citrixanalytics
  service: security
title: Clipboard usage on SaaS apps
<!--NeedCopy-->
```

ユーザーダッシュボード

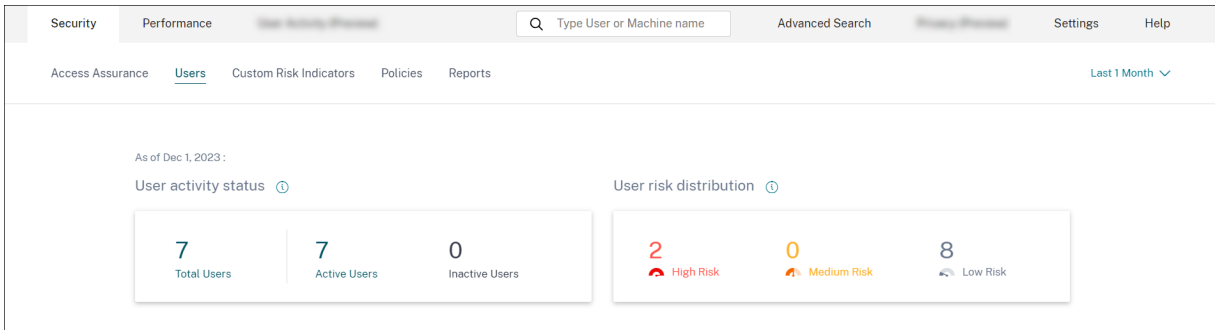
February 14, 2024

概要

ユーザーダッシュボードは、ユーザーの行動分析と脅威防止の出発点です。

このダッシュボードは、組織全体のユーザー行動パターンを可視化します。このデータを使用すると、フィッシングやランサムウェア攻撃など、通常とは異なる行動をプロアクティブに監視、検出、フラグを立てることができます。

ユーザーダッシュボードを表示するには、[セキュリティ **] > [**ユーザー] に移動します。[ユーザー] ダッシュボードには、次のセクションがあります。



- ユーザーアクティブステータス**:** 全ユーザー、アクティブユーザー、非アクティブユーザーの分布。

- ユーザーリスク分布: アクティブユーザー、非アクティブユーザー、合計ユーザー数の分布、および選択した期間に計算された最高リスクスコアに基づく、高、中、低のプロファイルにおけるリスクユーザーの分布。
- トップユーザー: トップユーザーはリスクスコアでソートされ、全ユーザー、特権ユーザー、ウォッチリストユーザーごとに分類されます。
- リスクカテゴリ:Citrix Analytics がサポートするリスクカテゴリを表示します。同様の行動パターンを持つリスク指標はカテゴリに分類されます。
- リスク指標とアクション: 選択した期間にわたってプロットされたリスク指標とアクションを組織内のすべてのユーザーに分散させます。
- アクセス概要: ユーザーが組織内のリソースにアクセスしようとした合計回数を要約します。
- ポリシーとアクション: ユーザープロファイルに適用されたポリシーとアクションの上位 5 つが表示されます。
- リスク指標: 組織の上位 5 つのリスク指標を表示します。

ユーザーアクティビティステータス

Analytics を有効にしたデータソースを使用している組織内のユーザーの総数。アカウントに関連付けられたリスクスコアがある場合とない場合があります。このタイルには、アクティブなユーザーの数が表示されます。アクティブユーザーとは、選択した期間内にイベントが検出されたユーザーです。ユーザーアクティビティステータスドロップダウンメニューをクリックすると、アクティブユーザーと非アクティブユーザーの合計ユーザー数の分布を確認できます。

- 合計ユーザー数: 選択した期間内のユーザーの総数。
- アクティブユーザー: 選択した期間にイベントが検出されたユーザー。
- 非アクティブなユーザー: 選択した期間にイベントが検出されなかったユーザー。

すべてのユーザーがリスクを伴うとは想定されていないため、ユーザーダッシュボードのユーザーの総数はリスクのあるユーザーの数よりも多い場合があります。

> 注
>
> : ユーザーページには、選択した期間に関係なく、過去 30 日間のユーザーの総数が表示されます。

ファセット

次のカテゴリに基づいてユーザーイベントをフィルタリングします。

- リスクスコア: 高リスク、中リスク、低リスク、およびゼロリスクのスコアに基づくユーザーイベント。
- ユーザー: 管理者権限、エグゼクティブ権限、およびウォッチリストユーザーに基づくユーザーイベント。
- 検出されたデータソース: オンボーディングしたデータソースに基づくユーザーイベント。

検索ボックス

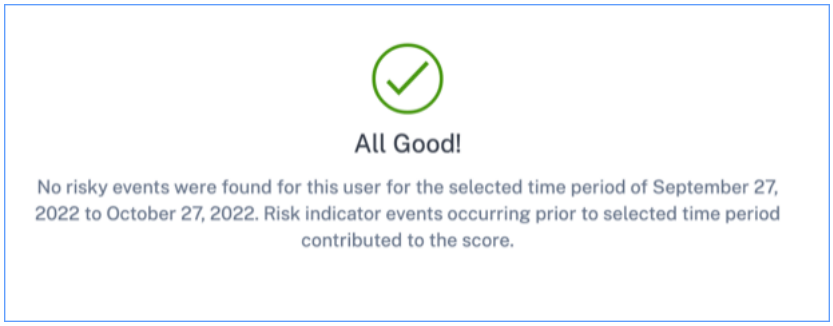
検索ボックスを使用して、ユーザーのイベントを検索します。クエリで演算子を使用して、検索の焦点を絞り込むことができます。クエリで使用できる有効な演算子については、「セルフサービス検索」を参照してください。

最新スコア

リスクスコアは、特定の期間にユーザーが組織に提起するリスクのレベルを決定します。リスクスコアの値は動的で、ユーザー行動分析に基づいて変化します。最新のリスクスコアに基づいて、ユーザーは高リスクユーザー、中リスクユーザー、低リスクユーザー、およびリスクスコアがゼロのユーザーのいずれかに分類されます。

ユーザー

Analytics によって検出されたすべてのユーザーのリスト。ユーザー名を選択して、ユーザーのユーザー情報とリスクタイムラインを表示します。ユーザーがリスク指標をトリガーしたかどうか、またはトリガーしていない可能性があります。このユーザーに関連する危険なイベントがない場合は、次のメッセージが表示されます。



ユーザーに関連するリスクのあるイベントがある場合は、リスクタイムラインにリスク指標が表示されます。リスクタイムラインを表示するユーザーを選択します。

ユーザーをウォッチリストに`privileged`としてマークして追加できます。

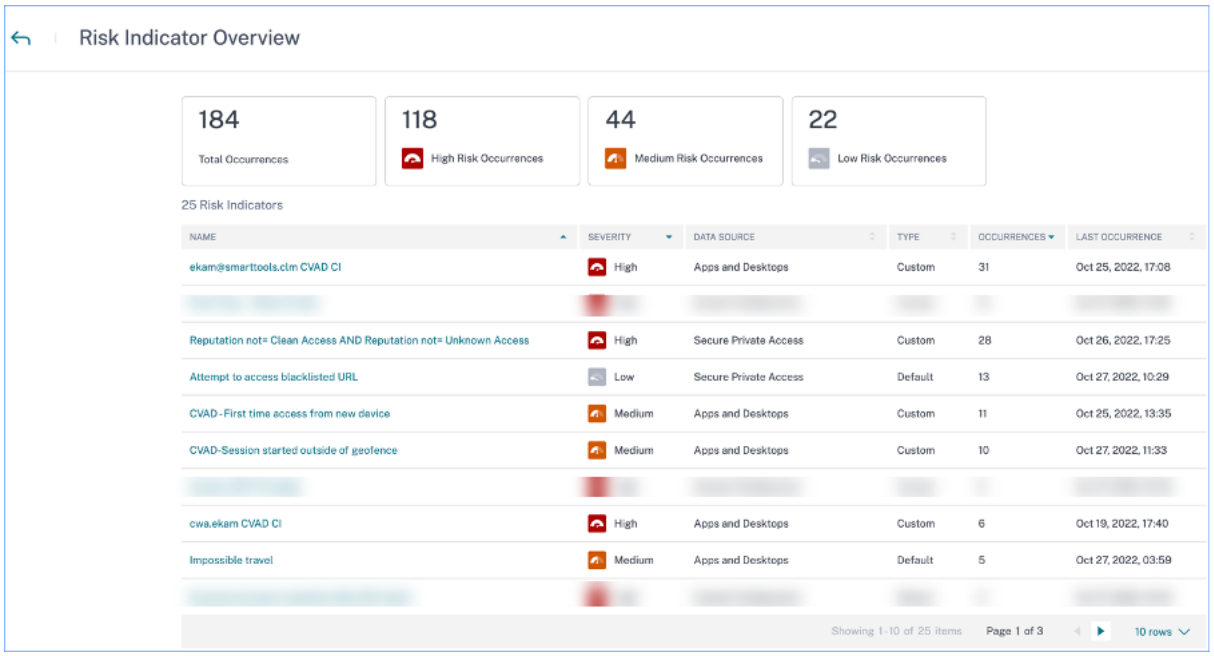
検出されたデータソース

ユーザーに関連付けられているデータソース。ユーザーがデータソースをアクティブに使用している場合、Analytics はそのデータソースからユーザーイベントを受信します。ユーザーイベントを受信するには、データソースサイトカードのデータ処理を有効にする必要があります。このカードは、[データソース] ページで使用できます。

トリガーされたインジケーター

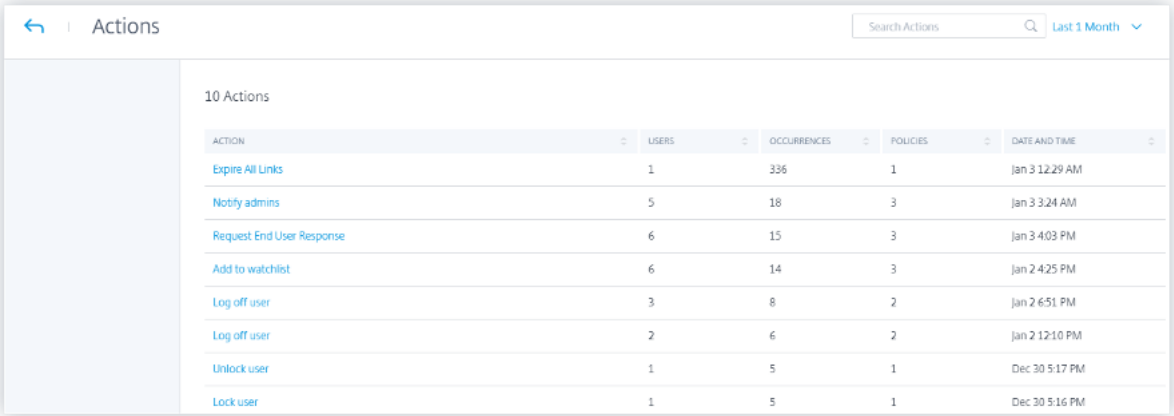
選択した期間にユーザー全体でトリガーされたリスク指標の数を示します。指標トリガータイルをクリックすると、リスク指標の詳細が表示されます。リスク指標表には次の詳細が表示されます:

- 名前: リスク指標の名前。
- 重要度: イベントに関連するリスクの重大度。リスクは、高、中、低のいずれかです。
- データソース: リスク指標テンプレートが適用されるデータソース。
- タイプ: リスク指標のタイプ。リスク指標は、デフォルトまたはカスタムにすることができます。
- 発生回数: ユーザーのリスク指標がトリガーされた回数。期間を選択すると、リスク指標の発生は、選択した時間に基づいて変化します。
- 最終出現日: 最後に出現した日付と時刻が表示されます。



適用されたアクション

選択した期間にユーザー全体に適用されたアクションの数を示します。これには、管理者が手動で適用したアクションとポリシー主導のアクションが含まれます。アクション適用タイルをクリックすると、アクションの詳細が表示されます。このセクションには、ユーザープロファイルに手動で適用したアクションは表示されません。

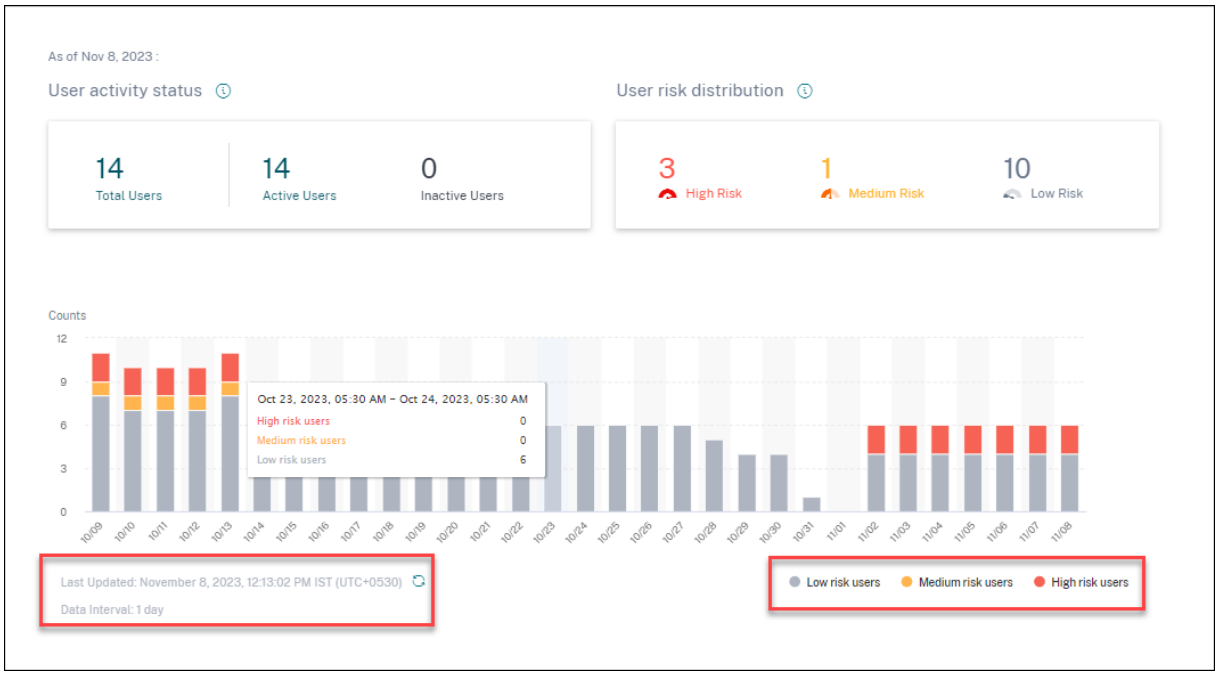


アクションテーブルには次の情報が表示されます。

- アクション: ポリシーに従って適用されたアクションの名前。
- ユーザー: アクションが適用されたユーザーの数。
- 出現回数: アクションの発生回数。
- 日付と時刻: 適用されたアクションの日付と時刻。

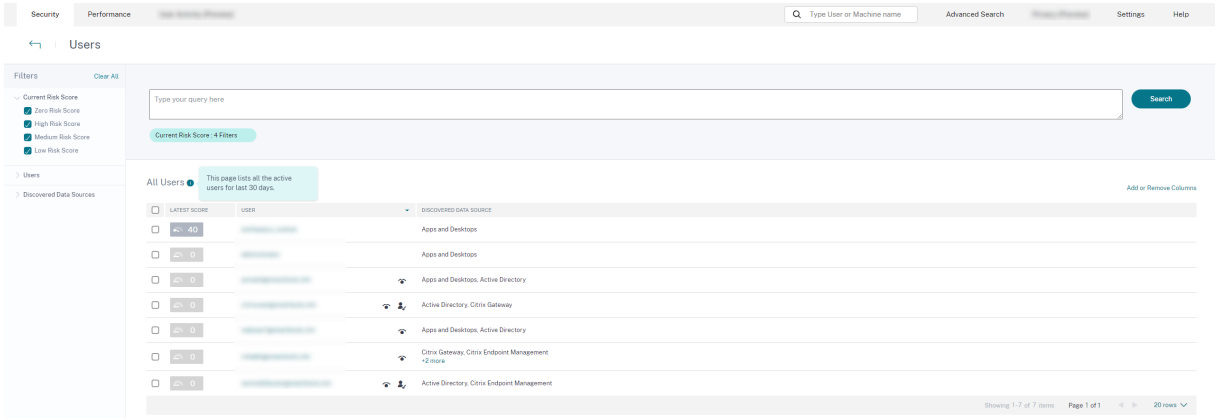
処理されたイベント

接続されたデータソースから受信し、Analytics によって処理されたユーザーイベントの総数。



ユーザーリスク分布

選択した期間に計算された最高リスクスコアに基づいて、高プロファイル、中プロファイル、低プロファイルのユーザー数を表示できます。全体数の下には、低リスク、中リスク、高リスクユーザーの分布の経時変化が棒グラフに表示されます。



リスクレベルは 3 つのカラーコードに分類されます。

- 赤-リスクの高いユーザーを表します。
- オレンジ—中リスクのユーザーを表します。
- グレー—リスクの低いユーザーを表します。

特定の期間に基づいてカラーバーにカーソルを合わせると、危険なユーザーの数（高、中、低）を表示できます。データ間隔情報とともに、最終更新情報 (日付と時刻) を表示できます。任意のカラーバーをクリックすると、その期間のリスクユーザーが表示されます。更新オプションをクリックして、更新されたデータを取得します。

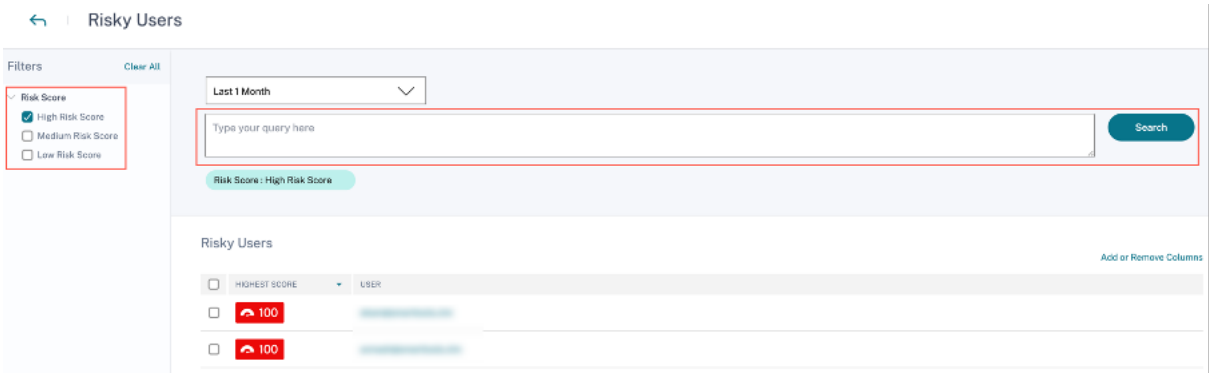
リスクの高いユーザー

リスクの高いユーザーとは、リスクのあるイベントが関連付けられ、少なくとも 1 つのリスク指標をトリガーしたユーザーです。特定の期間にユーザがネットワークに提起するリスクのレベルは、ユーザに関連付けられたリスクスコアによって決定されます。リスクスコアの値は動的で、ユーザー行動分析に基づいています。

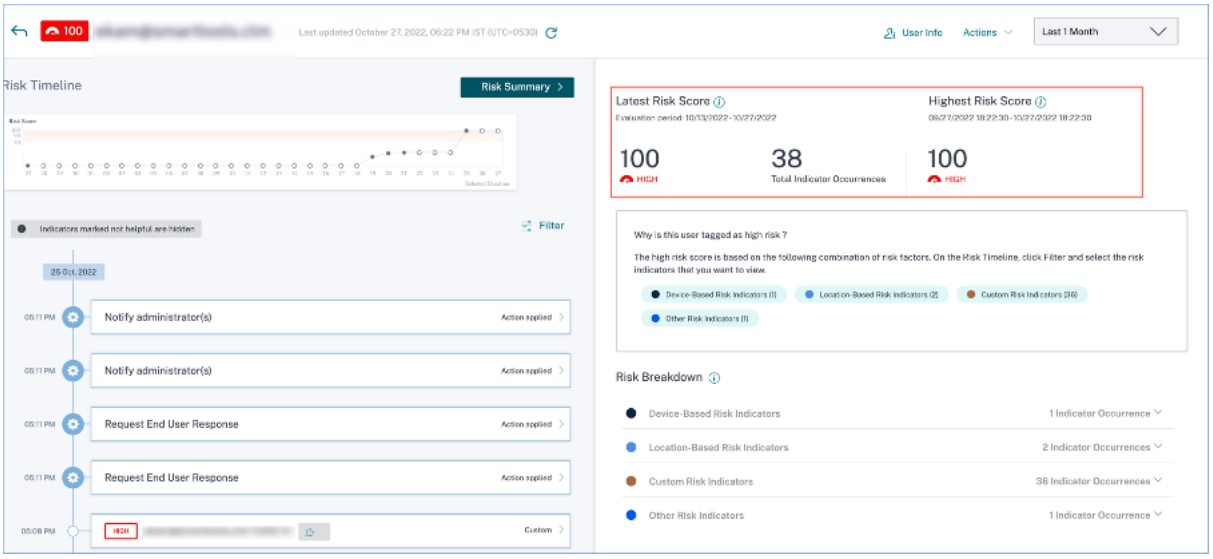
各ユーザーのリスクは、ユーザーのアクティビティに基づいて定期的に更新されます。そのため、ある時点ではリスクが中程度または高でも、後で低いリスクレベルに低下するユーザーもいます。リスクスコアに基づいて、リスクの高いユーザーは次のカテゴリのいずれかに分類されます。

- ハイリスク
- 中程度のリスク
- 低リスク

「危険なユーザー」ページでは、選択した期間に関連するリスクレベルに基づいてファセットをフィルタリングしたり、検索バーを使用して特定のユーザーを検索したりできます。



ユーザーの電子メール ID をクリックすると、選択した特定のユーザーのリスクタイムラインページが表示されます。このページには、選択した期間に基づいて、リスク指標と「最新」および「最高」のリスクスコアの詳細が表示されます。



ハイリスク

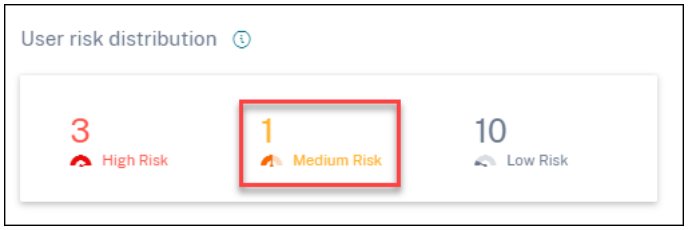
リスクスコアが 90～100 のユーザー。これらのユーザーは、中程度から重度のリスク要因と一致する複数の行動を示しており、組織にとって差し迫った脅威となる可能性があります。

ユーザーダッシュボードでは、選択した期間に計算された最高リスクスコアに基づいて、リスクの高いユーザーの数を表示できます。

「高リスク」オプションをクリックすると、「危険なユーザー」ページが表示されます。このページには、リスクの高いユーザーに関する詳細が表示されます。

中程度のリスク

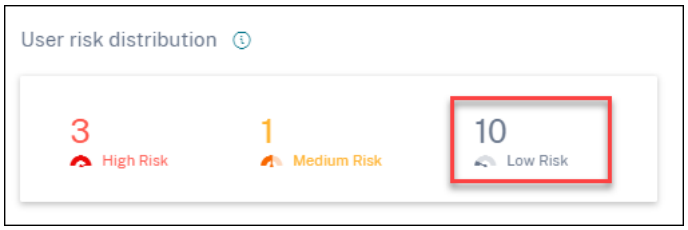
リスクスコアが 70～89 のユーザー。これらのユーザーは通常、疑わしい、または異常と思われるアクティビティを 1 つ以上行っているため、注意深く監視する価値があります。



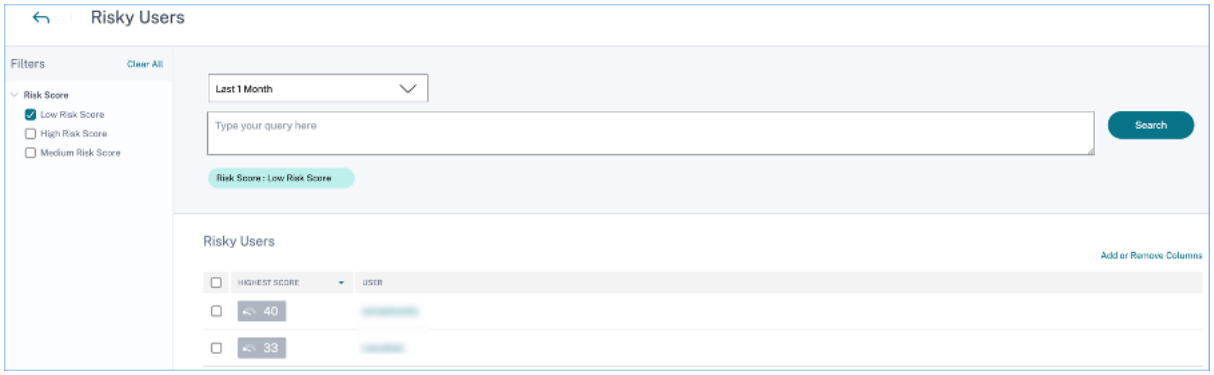
「リスクが中程度」オプションをクリックすると、「リスクの高いユーザー」ページが表示されます。このページには、中リスクのユーザーに関する詳細が表示されます。

低リスク

リスクスコアが 1 ～69 のユーザー。これらのユーザーには、異常または予期しない行動を反映するリスク指標が少なくとも 1 つありますが、より深刻なリスク分類を行うには十分ではありません。

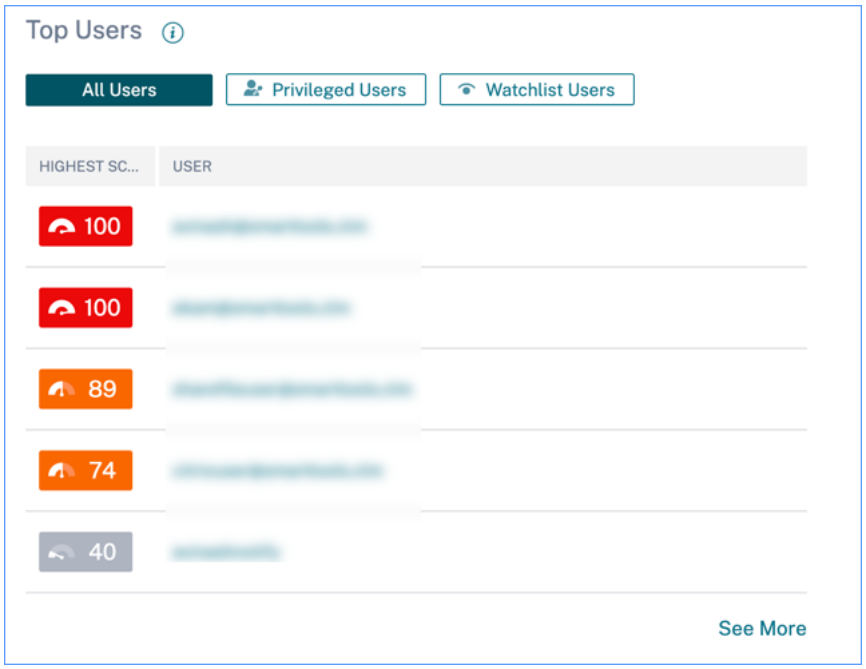


「低リスク」オプションをクリックすると、「リスクの高いユーザー ** 」ページが表示されます。このページには、リスクの低いユーザーに関する詳細が表示されます。



上位ユーザー

選択した期間のさまざまなユーザーカテゴリの上位ユーザーを、最も高いリスクスコアでソートして表示できます。次のトップユーザー表には、最新のリスクスコアではなく、選択した期間に計算されたリスクスコアに基づいて、リスクの高い上位 5 人のユーザー（全ユーザー、特権ユーザー、ウォッチリストユーザー）が示されています。

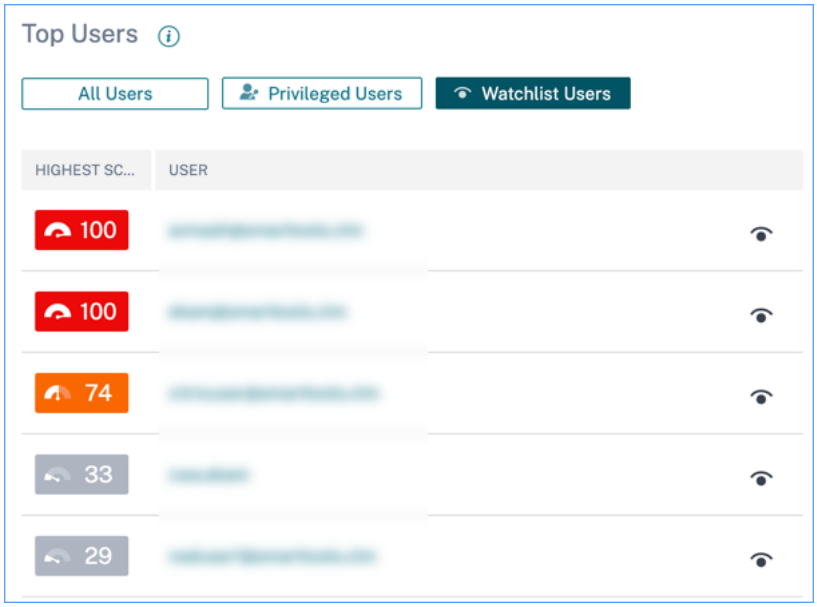


> 注:
>
> 以前のバージョンでは、選択した期間に関係なく、Top Users テーブルには常に最新のリスクスコアが表示されていました。

ウォッチリストユーザー

潜在的な脅威について綿密に監視されているユーザーのリスト。たとえば、組織内の正社員ではないユーザーをウォッチリストに追加することで、それらのユーザーを監視できます。また、特定のリスク指標を頻繁にトリガーするユーザーを監視することもできます。ウォッチリストにユーザーを手動で追加するか、ウォッチリストにユーザーを追加するためのポリシーを定義します 。

ウォッチリストにユーザーを追加した場合、最高スコアに基づいてウォッチリストの上位 5 人のユーザーを表示できます。



「すべてのユーザー」ペインの 「もっと見る」リンクをクリックすると、「ユーザー」ページが表示されます。このページには、ウォッチリスト内のすべてのユーザーのリストが表示されます。

> 注:
>
> [ユーザー] ダッシュボードと [ユーザー] ページには、選択した期間に関係なく、過去 13 か月間のウォッチリスト内のユーザー数が表示されます。期間を選択すると、選択した時間に基づいてリスク指標の発生が変化します。

詳細: ウォッチリスト

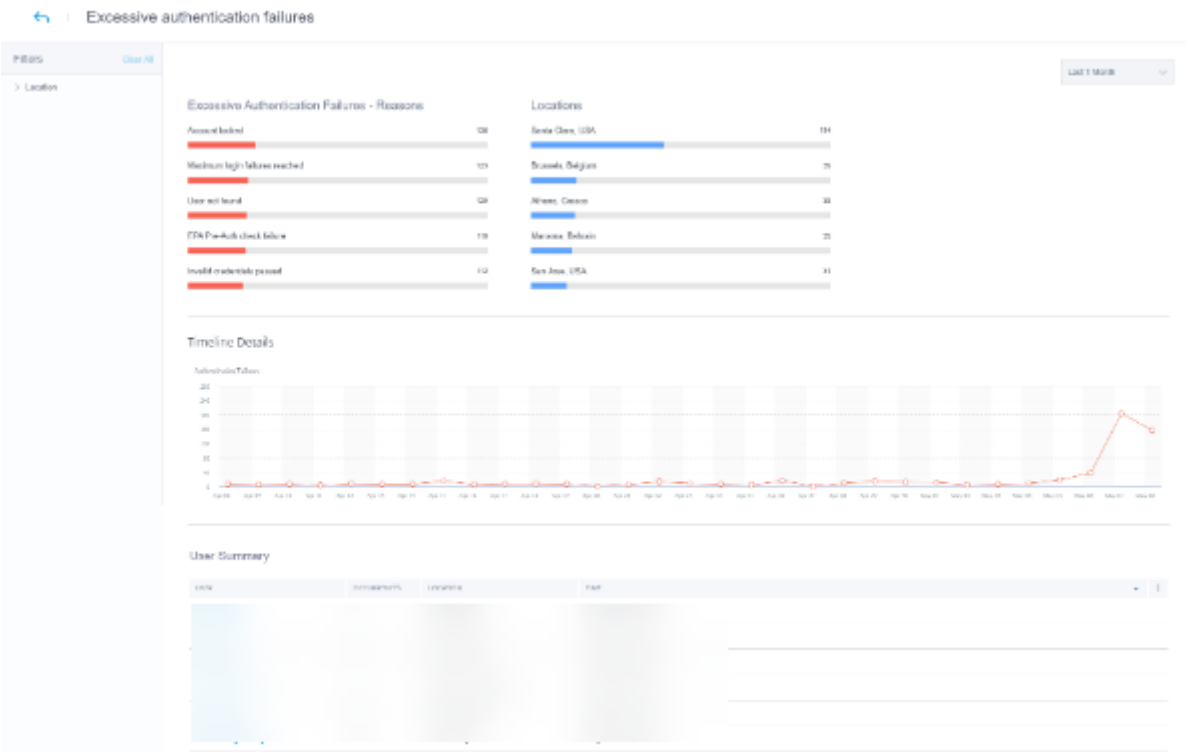
リスクカテゴリー

リスクカテゴリのドーナツチャートには、選択した期間における指標の出現回数がリスクカテゴリ別にまとめられています。各チャートセグメントにカーソルを合わせると、ユニークユーザー数が表示され、対応するリスク指標カテゴリの概要ページにリンクされます。リスク分類はデフォルトとカスタムリスク指標でサポートされています。

リスクカテゴリダッシュボードの目的は、Citrix Virtual Apps and Desktops および Citrix DaaS 管理者がユーザーリスクを管理し、専門家レベルのセキュリティ知識がなくてもセキュリティ担当者と簡単に話し合えるようにすることです。これにより、セキュリティ強制を組織レベルで有効にすることができ、セキュリティ管理者だけに限定されません。

使用例

Citrix Virtual Apps and Desktops の管理者であり、組織内の従業員のアプリケーションアクセス権を管理しているとします。[リスクカテゴリ] > [侵害されたユーザー] > [過度の認証失敗**-NetScaler Gateway** リスク指標] セクションに移動すると、アクセスを許可した従業員が侵害されたかどうかを評価できます。さらに移動すると、失敗の理由、サインイン場所、タイムラインの詳細、ユーザーの概要など、このリスク指標のより正確な洞察を得ることができます。アクセスを許可されたユーザーと侵害されたユーザーとの間に不一致があることに気付いた場合は、セキュリティ管理者にその旨を通知できます。セキュリティ管理者へのこのタイムリーな通知は、組織レベルでのセキュリティの実施に貢献します。

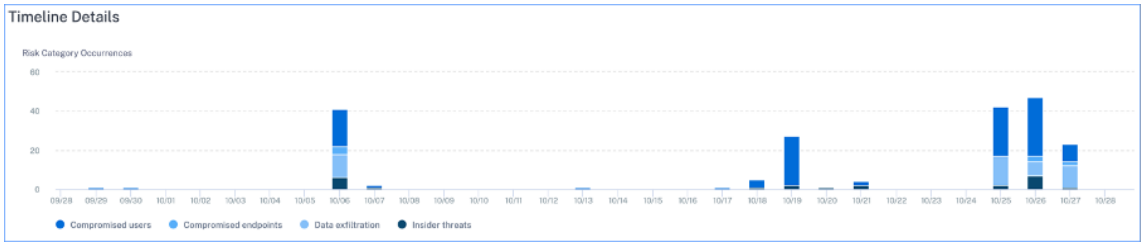


リスクカテゴリダッシュボードを分析するには

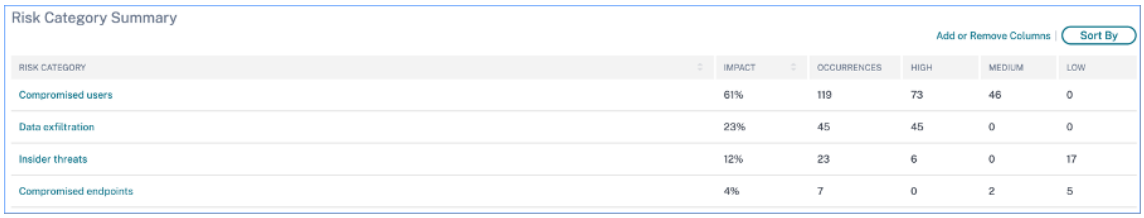
[リスクカテゴリ] ダッシュボードで [詳細を表示] を選択すると、リスクカテゴリの詳細をまとめたページにリダイレクトされます。このページには、次の詳細が含まれています。

- リスクカテゴリレポート：選択した期間における各カテゴリのリスク指標の発生総数を表します。

- タイムラインの詳細: 選択した期間におけるすべてのリスクカテゴリの合計リスク指標の発生回数をグラフィカルに表示します。このセクションの下部に移動すると、リスクカテゴリに基づいて並べ替えて、リスク指標に関するより正確な洞察を得ることができます。

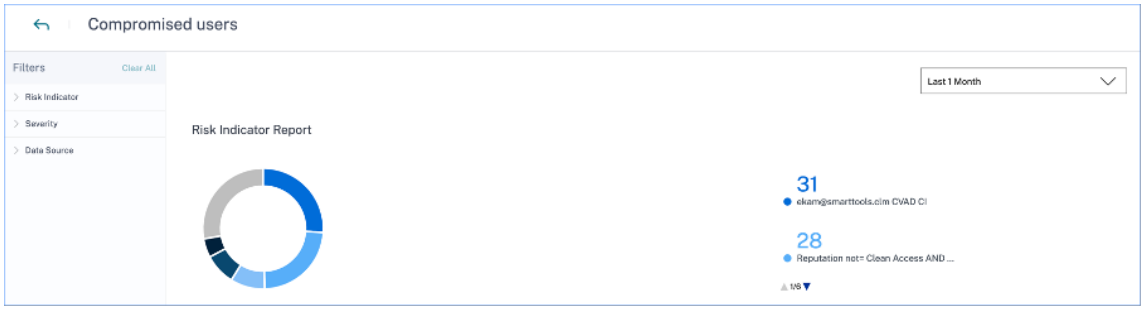


- リスクカテゴリの概要: このセクションには、各カテゴリに関連付けられたリスク指標の影響、発生および重大度などの詳細が表示されます。任意のリスクカテゴリを選択して、そのカテゴリに関連付けられたリスク指標の詳細を表示します。たとえば、[侵害されたユーザー] カテゴリを選択すると、[侵害されたユーザー] ページにリダイレクトされます。

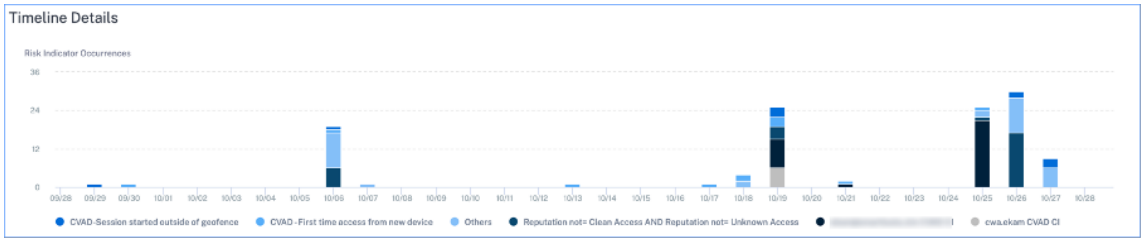


[侵害されたユーザー] ページには、次の詳細が表示されます。

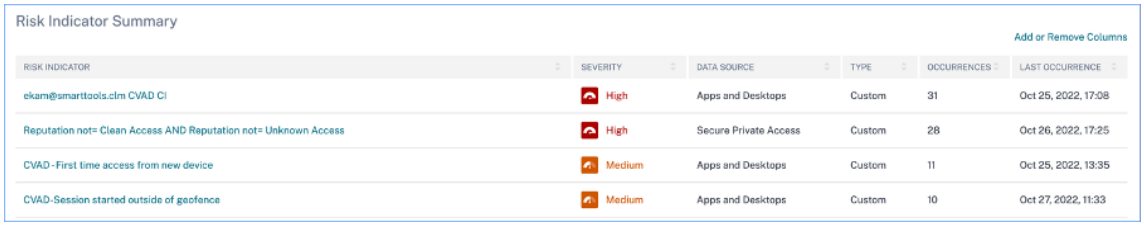
- リスク指標レポート: 選択した期間の [侵害されたユーザー] カテゴリに属するリスク指標を表示します。また、選択した期間中にトリガーされたリスク指標の合計発生回数も表示されます。



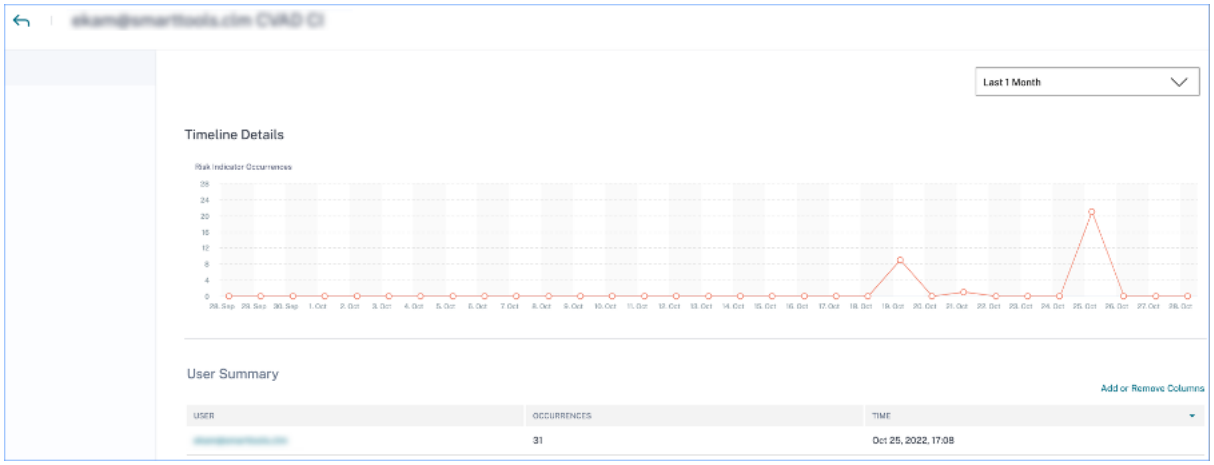
- タイムラインの詳細: 選択した期間におけるリスク指標の発生をグラフィカルに表示します。



- リスク指標の概要: 侵害されたユーザーのカテゴリで生成されたリスク指標の概要を表示します。このセクションには、重大度、データソース、リスクインジケータの種類、発生回数、および最後の発生も表示されます。



リスク指標を選択すると、その指標の詳細をまとめたページにリダイレクトされます。たとえば、[新しいデバイスからの初回アクセス] リスク指標を選択すると、この指標の詳細をまとめたページにリダイレクトされます。概要には、このイベントの発生に関するタイムラインの詳細と、このリスク指標をトリガーしたユーザー、リスク指標の発生、およびイベントの時刻を一覧表示するユーザー概要が含まれます。ユーザーを選択すると、ユーザーのリスクタイムラインにリダイレクトされます。



> 注
>
> Citrix Analytics は、適切なリスクカテゴリの下にデフォルトのリスク指標をグループ化します。カスタムリスク指標の場合は、[指標の作成] ページでリスクカテゴリを選択する必要があります。詳細については、「カスタムリスク指標」を参照してください。

リスクカテゴリのタイプ

データ流出　このカテゴリでは、マルウェア、または組織内のデバイスとの間で不正なデータ転送やデータ盗難を行う従業員によってトリガーされるリスク指標をグループ化します。指定した期間に発生したすべてのデータ漏洩アクティビティに関するインサイトを取得し、ユーザープロファイルにアクションをプロアクティブに適用することで、このカテゴリに関連するリスクを軽減できます。

データ漏えいリスクカテゴリには、次のリスク指標が分類されています:

データソース	ユーザーリスク指標
Citrix Virtual Apps and Desktops および Citrix DaaS	データ流出の可能性

インサイダーの脅威　このカテゴリは、組織内の従業員によってトリガーされるリスク指標をグループ化します。従業員は企業固有のアプリケーションへのアクセスレベルが高いため、組織はセキュリティリスクにさらされる可能性が高くなります。危険な活動は、悪意のある内部関係者によって意図的に引き起こされたり、ヒューマンエラーの結果である可能性があります。いずれのシナリオでも、組織に対するセキュリティ上の影響は甚大です。このカテゴリは、指定した期間中に発生したすべての内部脅威活動に関する洞察を提供します。これらのインサイトを利用して、ユーザープロファイルにアクションを積極的に適用することで、このカテゴリに関連するリスクを軽減できます。

インサイダー脅威リスクカテゴリは、次のリスク指標をまとめてグループ化します。

データソース	ユーザーリスク指標
Citrix Secure Private Access	禁止リストに登録された URL にアクセスしようとしています
Citrix Secure Private Access	過剰なデータのダウンロード
Citrix Secure Private Access	危険なウェブサイトへのアクセス
Citrix Secure Private Access	異常なアップロードボリューム

侵害されたユーザー　このカテゴリでは、ユーザーが不審なサインインやサインイン失敗などの異常な行動パターンを示すリスク指標をグループ化します。または、異常なパターンは、ユーザーアカウントが侵害された結果である可能性があります。特定の期間に発生したすべての侵害されたユーザーイベントに関するインサイトを取得し、ユーザープロファイルにアクションを積極的に適用することで、このカテゴリに関連するリスクを軽減できます。

侵害を受けたユーザーのリスクカテゴリでは、次のリスク指標がまとめられています。

データソース	ユーザーリスク指標
Citrix Gateway	エンドポイント分析スキャンの失敗
Citrix Gateway	過剰な認証失敗
Citrix Gateway	あり得ない移動
Citrix Gateway	疑わしい IP からのログオン
Citrix Gateway	異常な認証の失敗
Citrix Virtual Apps and Desktops および Citrix DaaS	疑わしいログオン
Citrix Virtual Apps and Desktops および Citrix DaaS	あり得ない移動
Microsoft Graph Security	Azure AD アイデンティティ保護リスクインジケーター
Microsoft Graph Security	エンドポイント向け Microsoft Defender リスクインジケータ

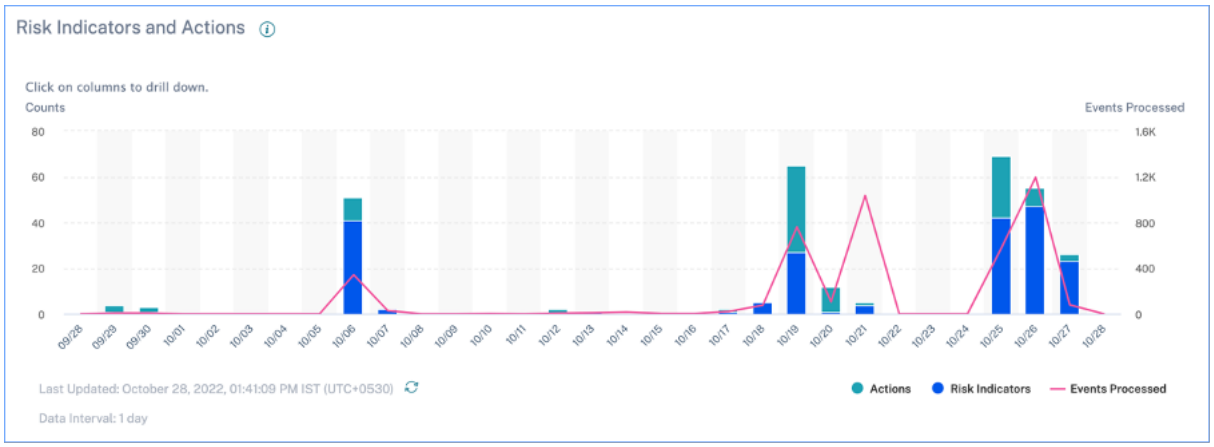
侵害されたエンドポイント　このカテゴリは、デバイスがセキュリティ保護されていない動作を示す場合にトリガーされるリスク指標をグループ化します。

侵害されたエンドポイントのリスクカテゴリは、次のリスク指標をまとめてグループ化します。

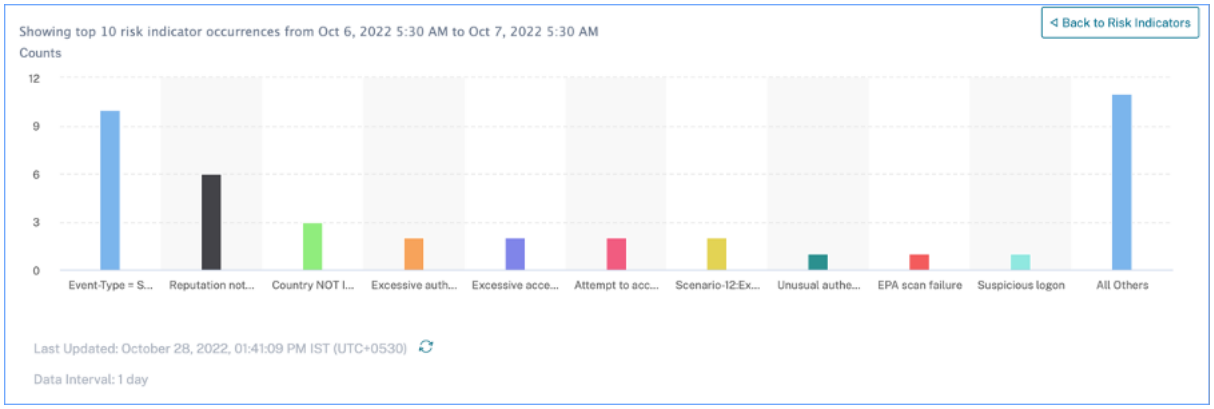
データソース	ユーザーリスク指標
Citrix Endpoint Management	管理対象外のデバイスが検出されました
Citrix Endpoint Management	ジェイルブレイクまたは Root 化されたデバイスが検出されました
Citrix Endpoint Management	禁止リストに登録されたアプリが検出されたデバイス

リスク指標とアクション

選択した期間にトリガーされたリスク指標とユーザーに適用されたアクションを表示できます。新しいリスク指標とアクションの棒グラフには、選択した期間から導き出された全体的な時間範囲とバー間隔とともに、時間の経過に伴う指標、アクション、およびイベントの数の詳細が表示されます。



インジケーターまたはアクションのいずれかのバーセグメントをクリックすると、インジケーターまたはアクションごとのカウントがそれぞれドリルダウンで視覚化されます。



指標のドリルダウンで、個々の指標バーをクリックすると、選択した期間の対応するリスク指標ページに移動します。

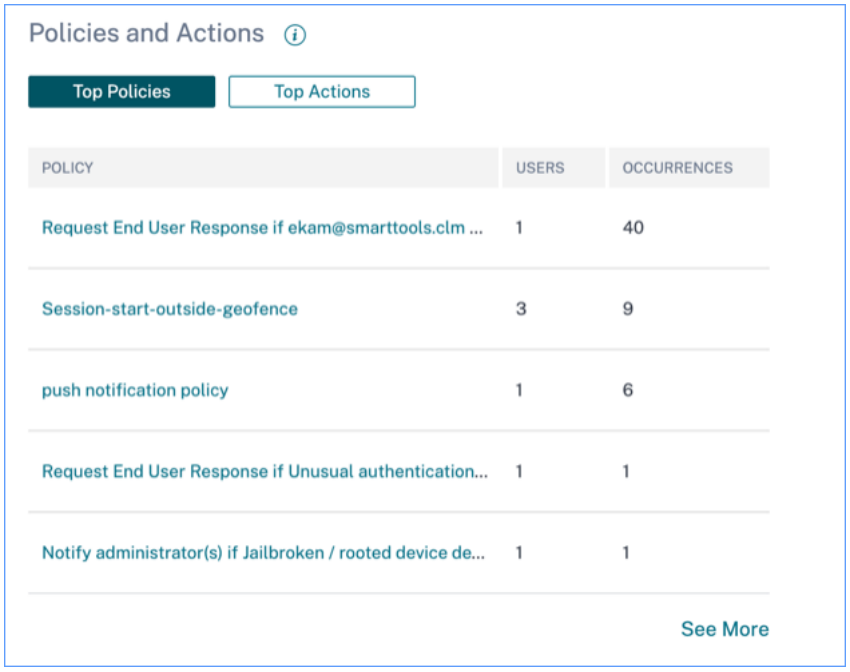
アクセスサマリー

このダッシュボードには、選択した期間のすべての Gateway アクセスイベントの概要が表示されます。NetScaler Gateway を介したアクセスの総数、成功したアクセス、および失敗したアクセスの数が表示されます。

グラフ上のポインタをクリックして、ゲートウェイのセルフサービス検索ページを表示します 。サインインシナリオが成功すると、ゲートウェイアクセスイベントはページのステータスコードでソートされます。

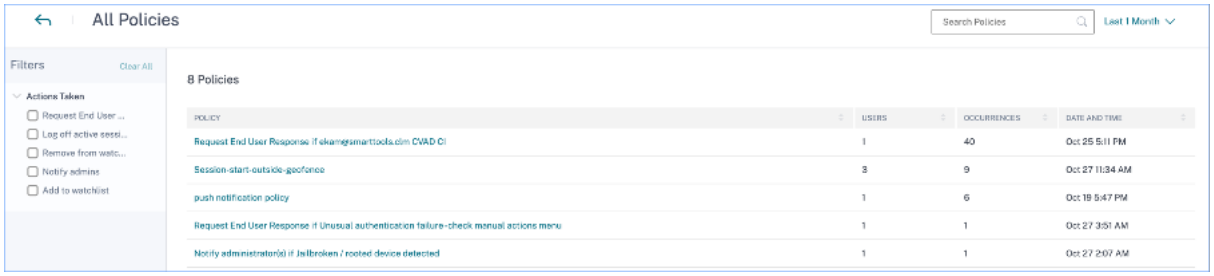
ポリシーとアクション

選択した期間にユーザプロファイルに適用されたポリシーとアクションの上位 5 つが表示されます。ポリシーとアクションに関する詳細情報を表示するには、[ポリシーと操作] ペインの [詳細を表示] リンクをクリックします。



トップポリシー

設定されている上位 5 つのポリシーは、発生数に基づいて決定されます。ダッシュボードの [上位ポリシー] セクションで [詳細を表示] を選択すると、[すべてのポリシー] ページにリダイレクトされます。



すべてのポリシー　このページには、設定されているすべてのポリシーに関する詳細情報が表示されます。いずれかのポリシーを選択すると、[ポリシーのセルフサービス検索] ページにリダイレクトされます。左側のペインで、適用されたアクションに基づいてフィルタリングできます。

ユーザー名を選択すると、リスクタイムラインにリダイレクトされます。ポリシーベースのアクションがユーザーのリスクタイムラインに追加されます。アクションを選択すると、その詳細がリスクタイムラインの右ペインに表示されます。

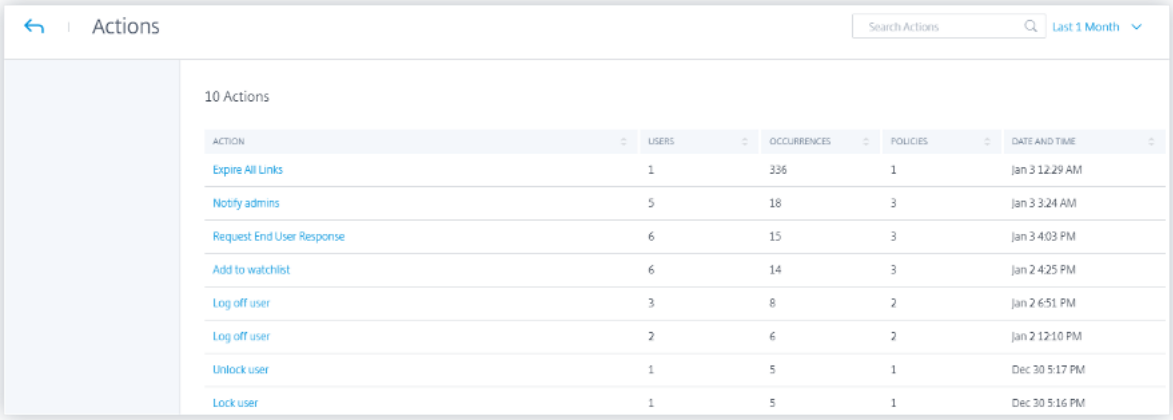
上位のアクション

ユーザープロファイルに適用されたポリシーに関連する上位 5 つのアクション。このセクションには、ユーザープロファイルに手動で適用したアクションは表示されません。上位のアクションは、出現回数によって決まります。

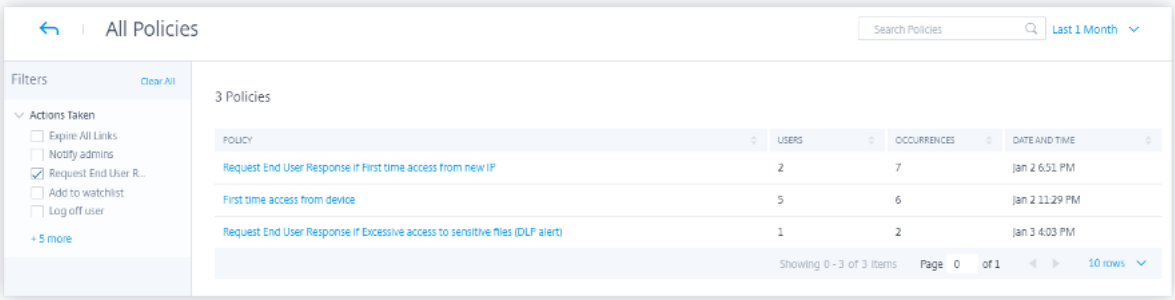
[詳細を表示] をクリックして、[アクション] ページでポリシーベースのアクションをすべて表示します。

操作　このページには、選択した期間にユーザーに適用されたすべてのポリシーベースのアクションのリストが表示されます。次の情報が表示されます。

- ポリシーに従って適用されるアクションの名前
- アクションが適用されたユーザー数
- アクションの出現回数
- アクションに関連付けられているポリシーの数
- 適用されたアクションの日時



アクションをクリックすると、関連付けられているすべてのポリシーが表示されます。これらのポリシーは、出現回数に基づいてソートされます。たとえば、[アクション] ページで [エンドユーザー応答を要求] をクリックします。[すべてのポリシー] ページには、[エンドユーザーレスポンスの要求] アクションに関連付けられているすべてのポリシーが表示されます。



[すべてのポリシー（All Policies）] ページで、ポリシーをクリックして、アクションが適用されたユーザーイベントを表示します。

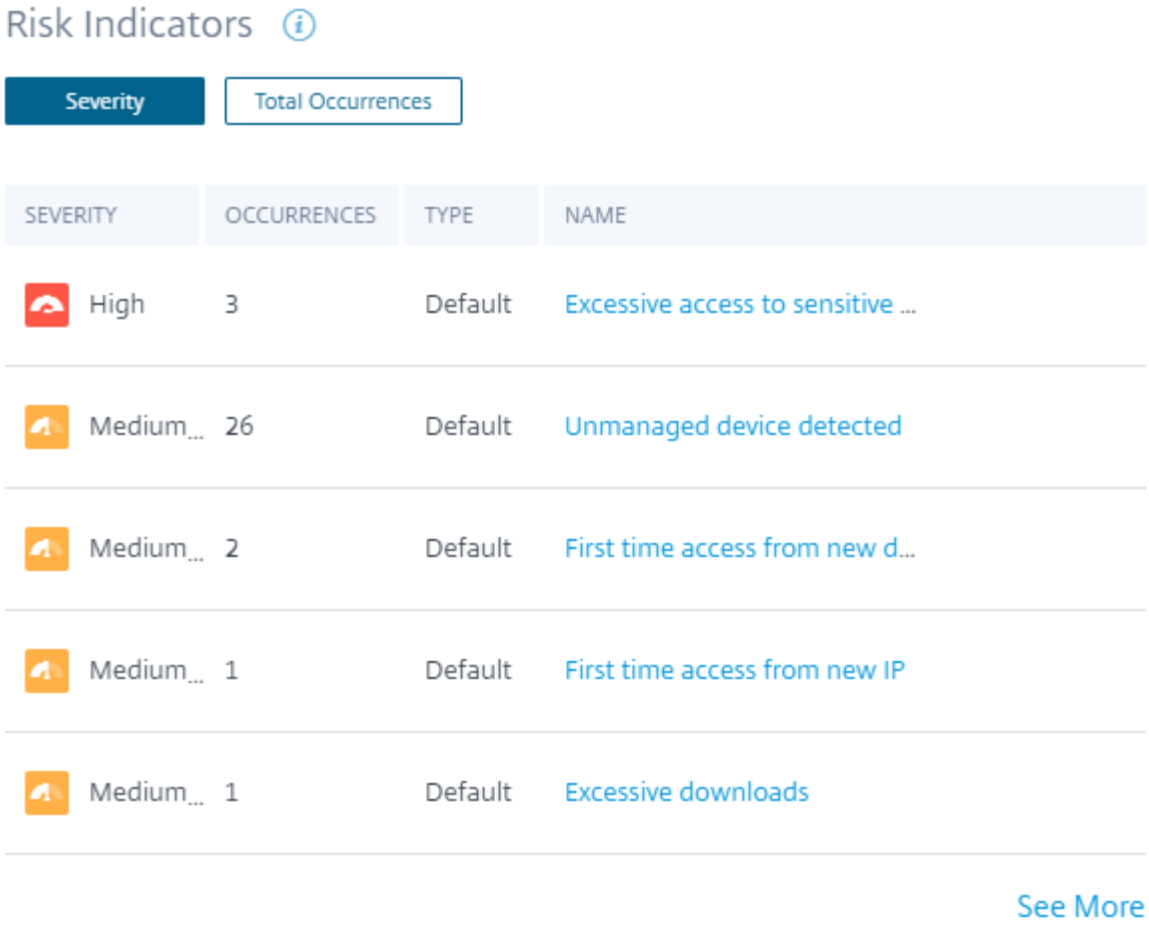
リスクインジケータ

選択した期間の上位 5 つのリスク指標を要約します。リスク指標は、デフォルトまたはカスタムにすることができます。デフォルトのリスク指標の場合、Citrix Analytics は検出されたデータソースからデータを収集し、データ処理が有効になっています。

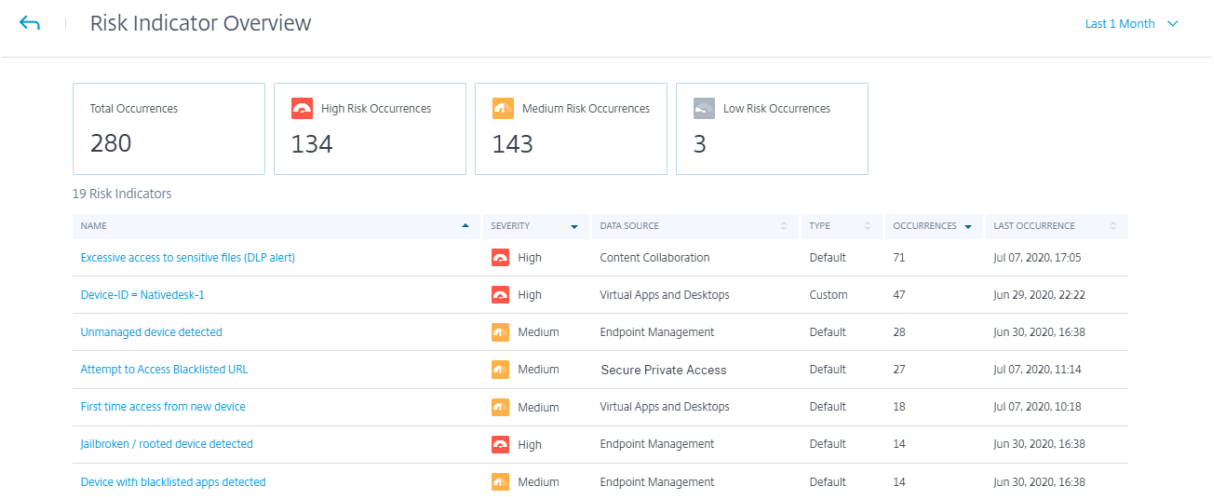
カスタムリスク指標の場合、Citrix Analytics は、生成された危険なイベントに基づいて、次のデータソースからデータを収集します。

- Citrix Gateway
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS（旧称：Citrix Virtual Apps and Desktops サービス）

[リスク指標] ペインでは、上位 5 つのリスク指標を表示し、発生総数または重大度に基づいて並べ替えることができます。



[リスク指標] ペインの **[**** 詳細を表示] をクリックして、[リスク指標の概要 **] ページを表示します。



アクセス保証ダッシュボード

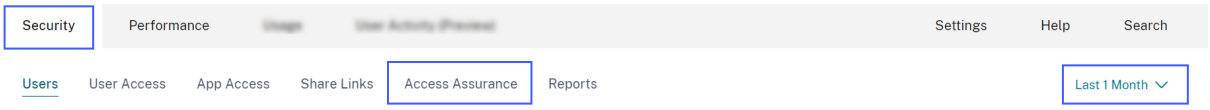
December 6, 2022

リモートワークの増加に伴い、シトリックスの IT 管理者は、ユーザーが通常の安全な場所から Citrix Virtual Apps and Desktops または Citrix DaaS（旧 Citrix Virtual Apps and Desktops サービス）にアクセスしていることを保証したいと思うかもしれません。不明な場所や新しい場所からログオンしているユーザーがいる場合は、ログオンの詳細を検証し、Citrix IT 環境に対する脅威を軽減するために必要なアクションを実行できます。

Access Assurance ダッシュボードには、ユーザーが仮想アプリケーションまたは仮想デスクトップにアクセスしている場所とネットワークの概要が表示されます。Citrix Analytics for Security は、ユーザーのデバイスにインストールされている Citrix Workspace アプリからこれらのユーザーログオンイベントを受信します。サポートされているバージョンの詳細については、Citrix Workspace アプリのバージョンマトリックスを参照してください。

ダッシュボードを表示する

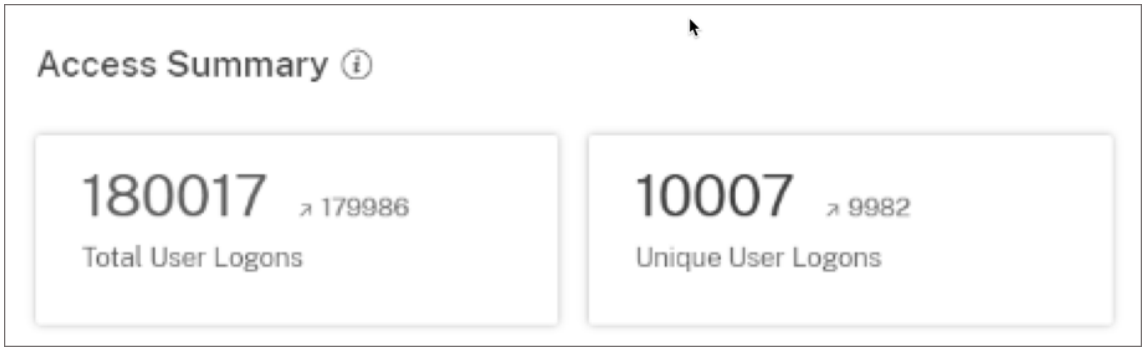
ダッシュボードを表示するには、[セキュリティ] **>** [アクセス保証] の順にクリックします。ログオンの詳細を表示する期間を選択します。



アクセス概要

ダッシュボードの概要セクションには、選択した期間に関する次の情報が表示されます。

1. ロケーション全体でのユーザーログオンの総数（全世界）。
2. ロケーション全体でのユニークユーザーログオンの総数（全世界）。



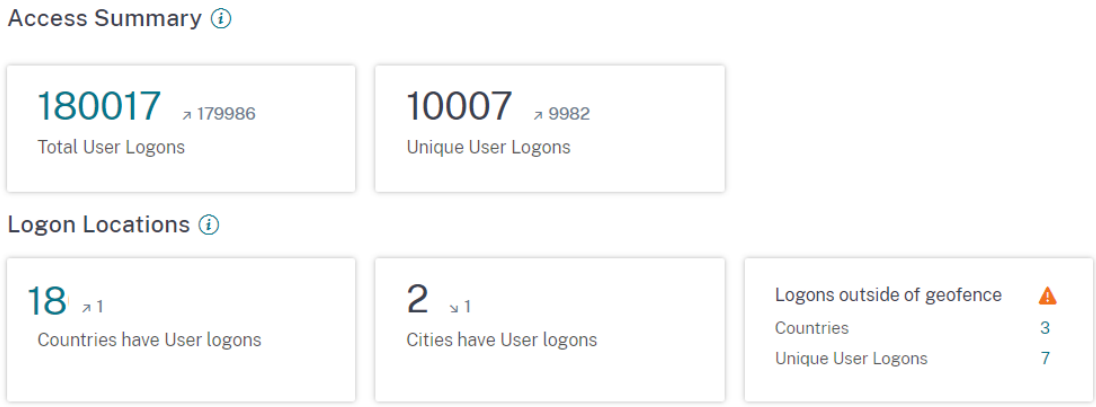
ログオン場所

「ログオン場所」セクションには、選択した期間に関する次の情報が表示されます。

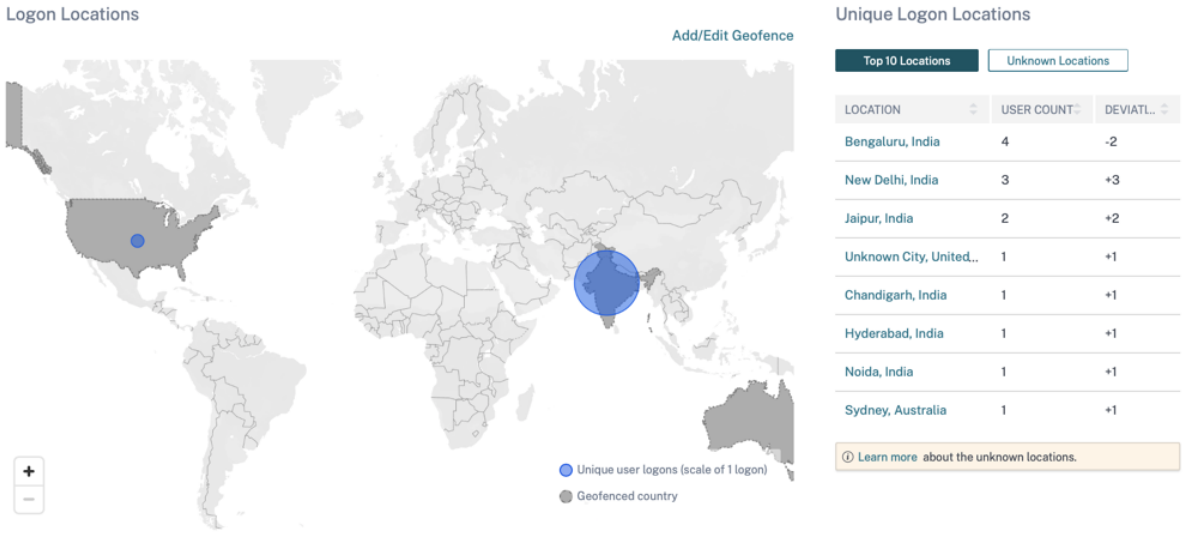
- ユーザーがログオンした国の総数。
- ユーザーがログオンした都市の総数。
- ジオフェンシングエリア内の国と一意のユーザーログオンの総数。ジオフェンシングエリアのログオン詳細を表示するには、ジオフェンシングを有効にします。
- 一意のユーザーログオンがある上位 10 の場所。場合によっては、上位のユニークユーザーログオンが不明な都市や国のものでもあり、これらは [不明な場所] タブに表示されます。不明な場所のリストも、上位 10 の場所のサブセットです。一部のロケーションが識別できない理由については、「利用できないと識別されたロケーション」を参照してください。

また、全世界のユーザーログオン数の増加傾向または減少傾向と、全世界のユニークユーザーログオン数の増加傾向または減少傾向も確認できます。上位 10 つの場所について、[偏差] 列には、各場所のユーザーログオンの変化 (正 (+) または負 (-)) が表示されます。この比較は、選択した期間と、同じ長さの前の期間に基づきます。たとえば、[過去 **1** か月] の期間を選択した場合、ユーザーログオンの傾向と偏差が、過去 1 か月と前から 1 か月間の間で比較されます。

> 注:
>
> 位置情報は都市レベルおよび国レベルで提供され、正確な位置情報を表すものではありません。アクセス保証、ジオロケーションの詳細については、よくある質問を参照してください。

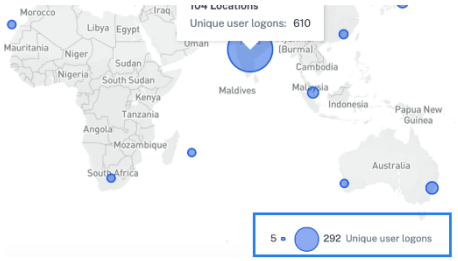


[一意のログオン場所の上位 **10** 個] テーブルで、ユーザー、ユーザーのアクセスプロファイル 、およびログオンの詳細を表示する場所を選択します。



マップには、選択した期間のさまざまな場所からのユニークユーザー数が表示されます。青いバブルにカーソルを合わせるか、場所を拡大して、その場所からの一意のユーザーログオンの総数を表示します。青い吹き出しをクリックすると、ロケーションのアクセス詳細が表示されます 。

マップの右下隅には、一意のユーザーログオンの範囲を表示できます。選択した期間について、小さなバブルは、ロケーション全体の一意のユーザーログオンの最小数を示します。大きなバブルは、ロケーション全体の一意のユーザーログオンの最大数を示します。

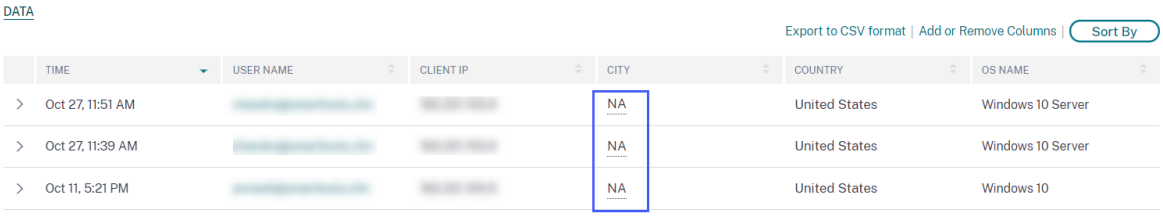


利用できないと識別された場所

[一意のログオン場所の上位 **10** 個] テーブルに、不明な場所または使用できない場所がある場合があります。不明な場所をクリックすると、[User **Logons]** ページに対応するユーザーログオンの詳細が表示されます。

国や都市の情報がない場合は、[ユーザーログオン] ページの [**DATA]** テーブルに **NA** ラベルが表示されます。

NA ラベルにカーソルを合わせると、位置情報が使用できない理由が表示されます。



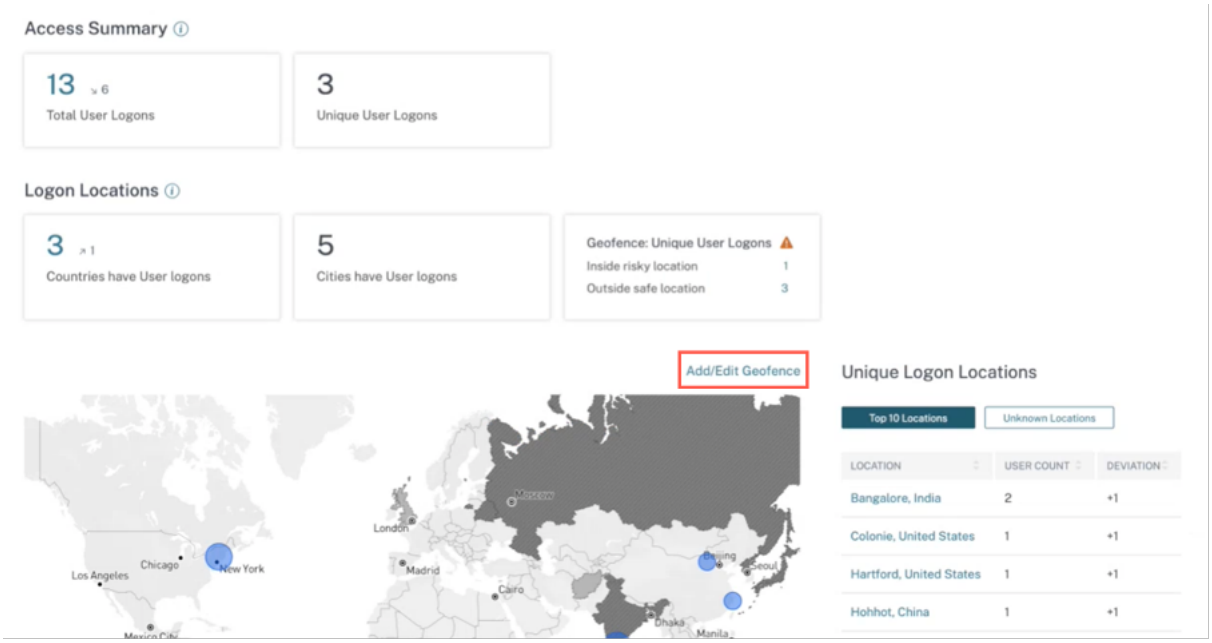
ロケーションを使用できない場合に、次のいずれかのシナリオが表示される場合があります。

シナリオ	理由
都市名と国名は利用できません。	以下のいずれかのサーバーオペレーティングシステム 1. ユーザーがサポートされていないバージョンの Citrix Workspace アプリを使用しています。ロケーション情報を表示するには、クライアントをサポートされているバージョンに更新します。
プライベート IP を持つロケーション	ユーザーのデバイスがプライベートネットワーク内にある。この場合、Citrix Analytics では位置情報を使用できません。
国名は利用可能ですが、都市名は利用できません。	ユーザーのデバイスが企業 IP を使用している可能性があります。企業 IP 範囲は、外部ジオロケーションサービスで難読化されます。したがって、Citrix Analytics では位置情報を使用できません。

ジオフェンシングを有効にする

ジオフェンシングは、安全なジオフェンスの外側や危険なジオフェンスエリア内から仮想アプリや仮想デスクトップにアクセスするユーザーを特定するのに役立ちます。アクセス概要ページを表示するには、「セキュリティ」**>**「アクセス保証」に移動します。

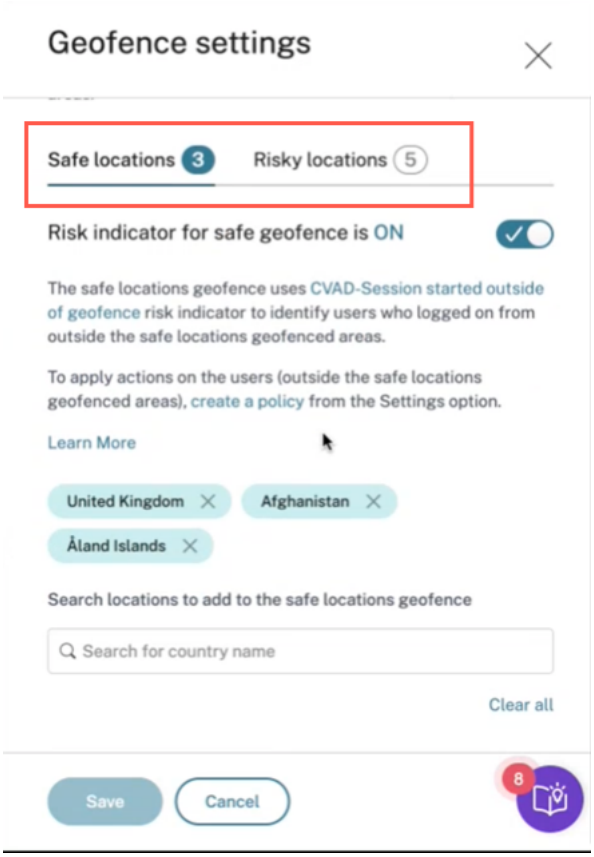
デフォルトでは、ジオフェンス設定は常にオンになっています。ジオフェンスを構成するには、[ジオフェンスの追加/編集] をクリックします。



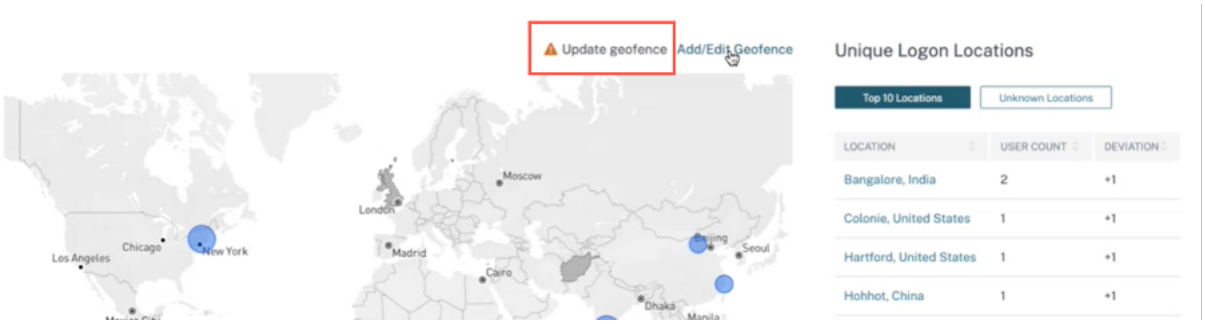
[ジオフェンス設定] ウィンドウに 2 つのタブが表示されます。

- 安全な場所: 安全な場所に該当する国を設定または削除できます。
- 危険な場所: 危険な場所に該当する国を設定または削除できます。

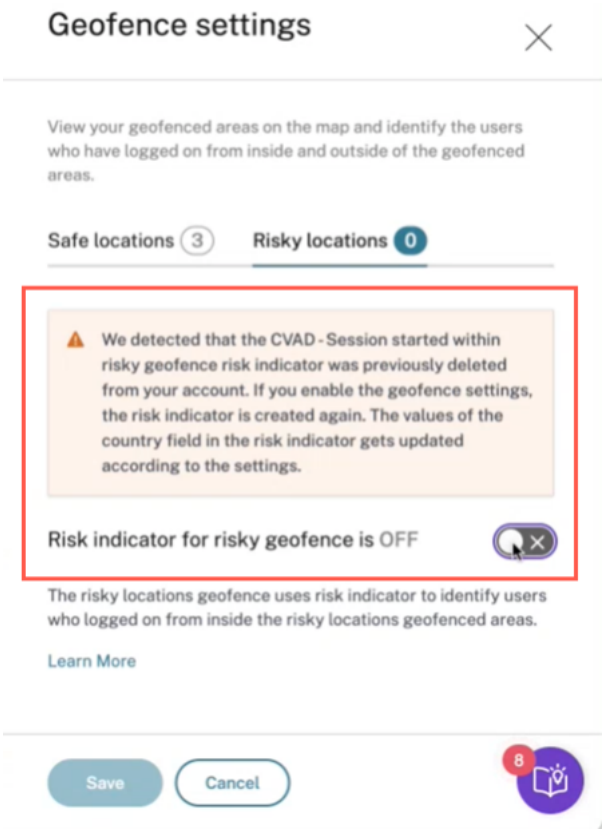
  また、各タブに設定されている安全な場所と危険な場所の総数を表示することもできます。セーフロケーションジオフェンスまたはリスクロケーションジオフェンスから国を削除または削除するには、国の横にある閉じる (X) 記号をクリックします。[保存] をクリックして Geofence 設定を保存します。



危険な場所のジオフェンスに該当する国を設定できます。Risky Locations ジオフェンスにリスク指標が追加されていないか、リスク指標が削除されている場合は、**[** ジオフェンスの追加**/**編集**]** の横に **[**ジオフェンスの更新**]** 警告メッセージが表示されます。



インジケーターを再作成するには、[危険な場所] タブに移動し、[危険なジオフェンスのリスクインジケーター] トグルをオンにします。



指標は危険な場所のデフォルトリストで作成されます。

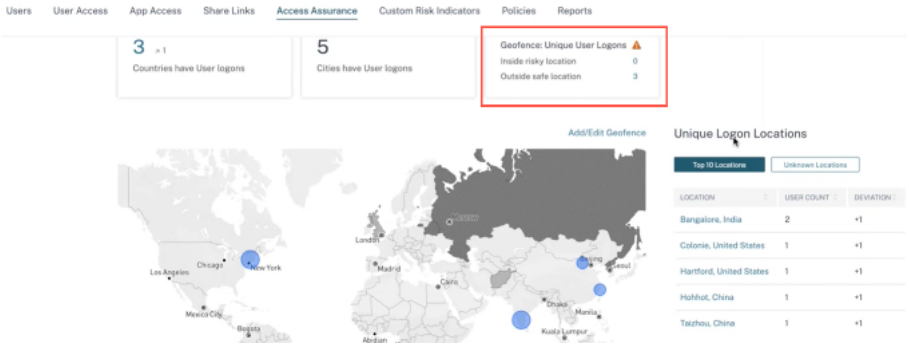
アクセス概要ページには、ジオフェンスされた安全で危険な国も表示されます。

- ジオフェンスセーフ国は薄い灰色の円でマークされています。
- ジオフェンスされた危険な国は、濃い灰色の円でマークされています。

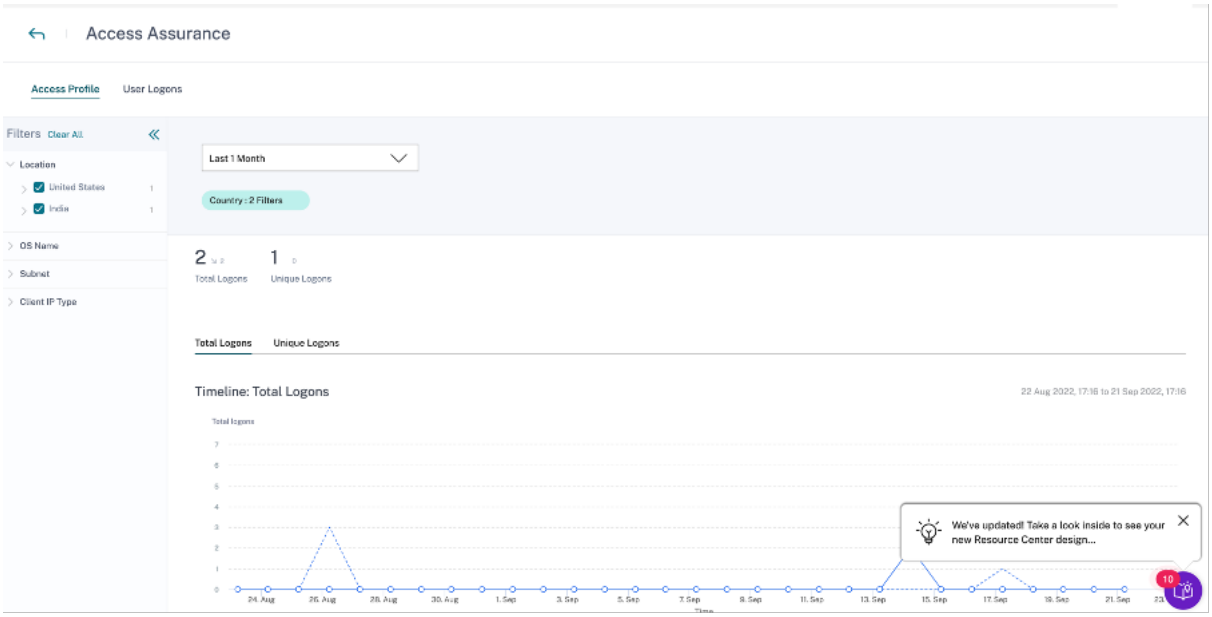
ジオフェンス**:** ユニークユーザーログオン

アクセス概要ページに移動すると、「ジオフェンス: ユニークユーザーログオン」が表示されます。カードには、内部の危険な場所と外部の安全な場所の数が表示されます。

- 危険なロケーション内: 危険なロケーションのジオフェンスエリア内からログインしたユーザーを特定します。
- 安全な場所外の安全な場所ジオフェンスされた安全な場所の外からログオンしたユーザーを特定します。



ログイン総数とユニークユーザーログオン数の詳細を確認するには、[危険な場所の内部] または [安全な場所以外] の横にある数字をクリックします。



この機能は、次の事前設定されたカスタムリスク指標を使用します。

- **CVAD-Session** がジオフェンスの外部で開始されました: 安全なジオフェンスの外でのユーザーログオンを監視するため。
- 危険なジオフェンス内で開始された **CVAD-Session**: 危険なジオフェンス内のユーザーログオンを監視するため。

ジオフェンスの外部でユーザーのログオンが検出されると、リスク指標がトリガーされ、[ジオフェンス外でセッションが開始されました] ポリシーがそれらのユーザーに適用されます。このポリシーは、エンドユーザー応答のリクエ

ストアクションをトリガーし、ユーザーの応答に基づいて、疑わしいログオンによる脅威を防ぐための適切なアクションを実行できます。詳細については、事前構成されたカスタムリスク指標を参照してください。

> メモ
>
> - ジオフェンスの設定で、国を変更すると、ジオフェンスのリスク指標の外で開始された *CVAD* セッションも更新されます。
> - たとえば、オーストラリアとインドを新しいジオフェンス対象国として選択して保存すると、リスク指標の事前構成された条件は、米国（デフォルトのジオフェンス）に加えて、新しい国で更新されます。デフォルトのジオフェンスされた国 [米国] を削除することもできます。
>
>   リスク指標の事前設定された条件:
>
>   ```
>   Event-Type = \"Session.logon\" AND Country != \"\" AND Country
>    ~ \"\" AND Country != \"United States\"
>   ```
>
>   ジオフェンス設定を更新した後、リスク指標の状態は次のようになります。
>
>   ```
>   Event-Type = \"Session.logon\" AND Country != \"\" AND Country
>    ~ \"\" AND Country NOT IN (\"Australia\", \"United States\",
>   \"India\"
>   ```
>
> - ジオフェンスのリスク指標の外で開始された *CVAD* セッションが以前にアカウントから削除されている場合、**Geofence Settings** を有効にすると、リスク指標が再度作成されます。リスク指標のジオフェンスされた国は、ジオフェンスの設定から制御されます。

[ジオフェンス設定] を有効にすると、ジオフェンスされたエリアと、これらのエリアからの一意のユーザーログオンがマップに表示されます。

ログオンネットワーク

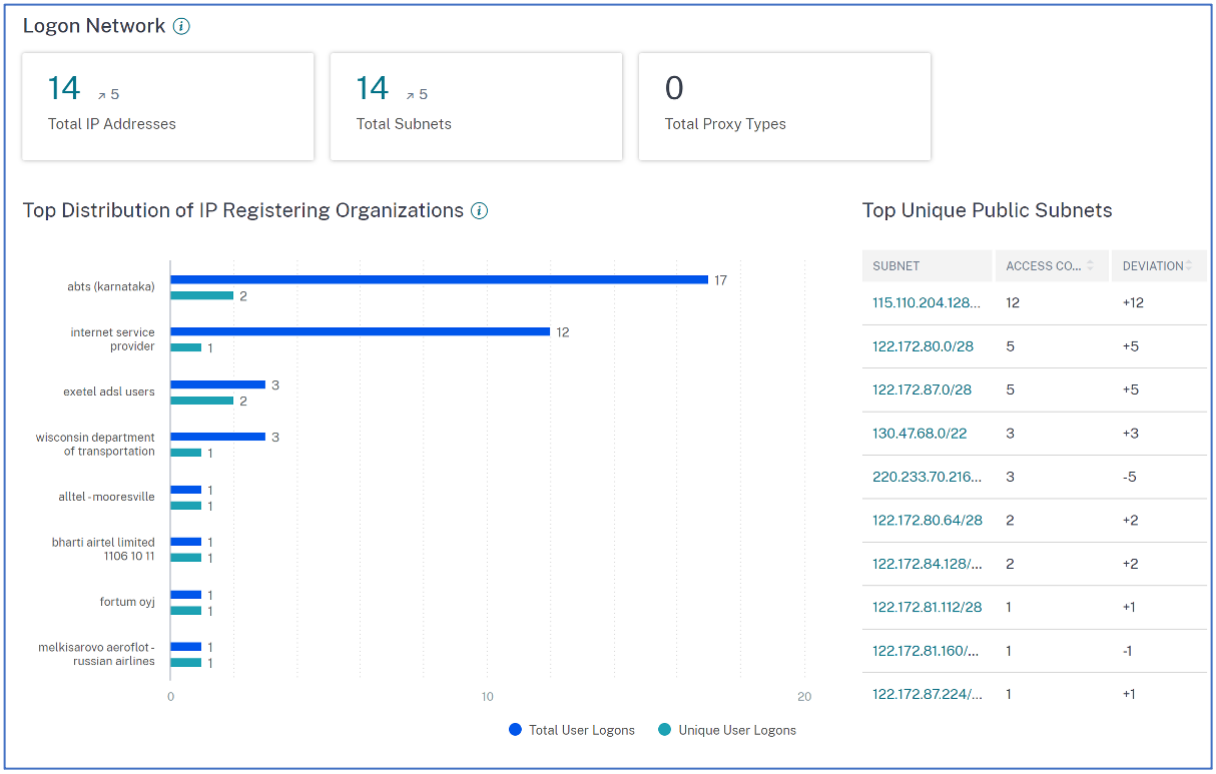
Access Assurance ダッシュボードでは、以下の追加ユーザー詳細を表示できるようになりました。

- ユーザーがログオンした IP アドレスに関連する組織。これらの組織には、企業、政府、教育機関、インターネットサービスプロバイダーなどの団体が含まれます。
- ユーザーがログオンしたユニークパブリックサブネットとプライベートサブネットの合計。
- ユーザーがプロキシとプライベート VPN サービスを使用してログオンした詳細。

これらの追加情報を使用して、管理者はユーザーログオンの詳細を検証し、ユーザーログオンが組織のセキュリティ要件の範囲内であるかどうかを確認できます。

ユーザーネットワークの詳細を表示する

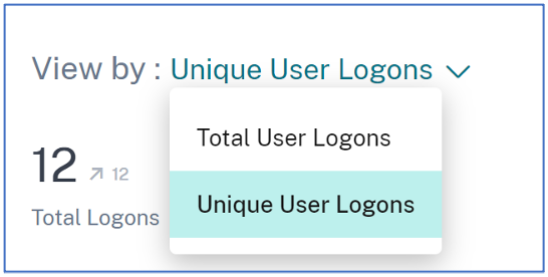
[セキュリティ] **>** [アクセス保証] に移動し、下にスクロールして [ログオンネットワーク] の下に詳細を表示します。



- **IP** アドレスの合計: 仮想セッションへのログオンに使用されるユニーク IP アドレスの総数を示します。
- サブネットの合計: 仮想セッションへのログオンに使用されたサブネットの総数を示します。
- プロキシタイプの合計: サーバーがユーザー接続をプロキシするために使用するネットワークまたはプロトコルの合計タイプを示します。
- **IP** 登録組織のトップディストリビューションでは、ユーザーログオン総数と各組織 (ISP) からの固有のログオン詳細の概要を視覚化できます。グラフをクリックすると、ユーザーの詳細、選択した組織に関連するユーザーのアクセスプロファイル、ログオンの詳細が表示されます。
- ユニークパブリックサブネットの合計では、サブネットの概要、各サブネットからのユーザーログオン総数、および各サブネットの偏差傾向を視覚化できます。各サブネットをクリックすると、ユーザーの詳細、選択したサブネットに関連するユーザーのアクセスプロファイルとログオンの詳細が表示されます。

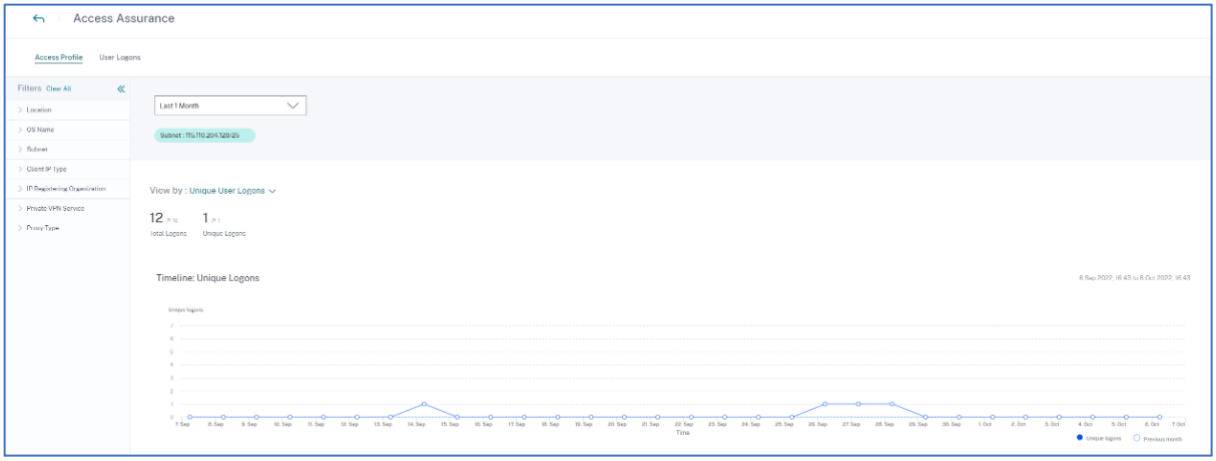
ユーザーのアクセスプロファイルを表示する

指標（場所、組織、またはサブネット）をドリルダウンすると、アクセスプロファイルページには、選択した場所からの仮想アプリケーションまたは仮想デスクトップへのユーザーのアクセスの概要が表示されます。[個別ログオン] または [総ログオン] オプションを選択して、選択した期間の傾向分析を表示できます。



選択した指標 (場所、組織、またはサブネット) の上位アクセスイベントを表示できます。この情報は、脅威の調査と分析のために、アクセスパターンと詳細を確認するのに役立ちます。

ユーザーログオン数の合計と一意のユーザーログオン数の増加傾向または下降傾向は、選択した期間と前回の同じ期間に基づいて比較されます。たとえば、期間を [過去 **1** か月] として選択すると、過去 1 か月と過去 1 か月間の傾向が比較されます。



ファセット

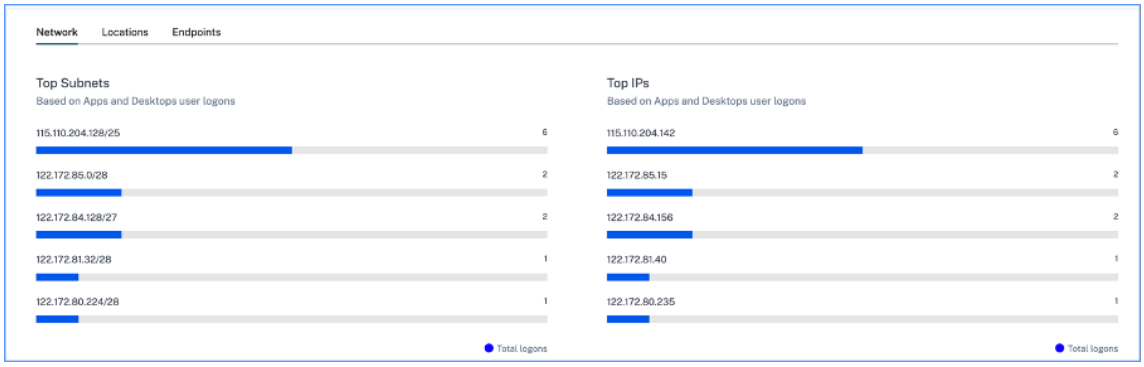
アクセスイベントには以下のファセットを使用できます。

- 場所-アクセスイベントを国と都市で絞り込みます。
- **OS**-オペレーティングシステムとそのバージョンによってアクセスイベントをフィルタリングします。
- サブネット-アクセスイベントをサブネットでフィルタリングします。
- クライアント **IP** タイプ-アクセスイベントをパブリックまたはプライベートでフィルタリングします。
- **IP** 登録組織-パブリック IP アドレスに関連付けられている組織をフィルタリングします。
- プライベート **VPN** サービス-プライベート VPN ネットワーク名でアクセスイベントをフィルタリングします。
- プロキシタイプ-HTTP、Web、Tor、SOCKS などのプロキシタイプ分類でアクセスイベントをフィルタリングします。

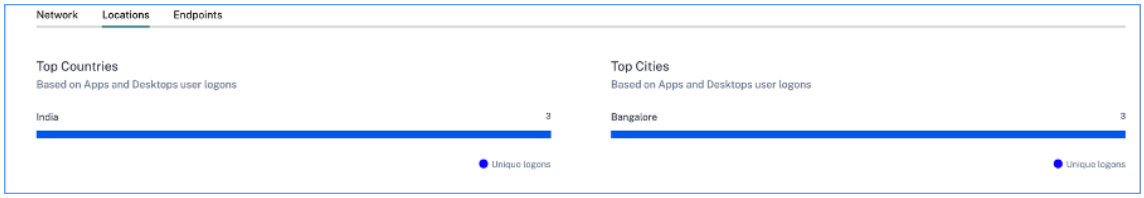
> 注
>
> また、データが利用できないか識別されていない場合も、[利用不可] ラベルが表示されることがあります。

適用されたフィルターに基づいて、合計ユーザーログオン数と個別ユーザーログオン数に関する次の情報を表示します。

- ネットワーク-ユーザーが仮想アプリまたは仮想デスクトップにログオンした上位サブネットと IP アドレス。



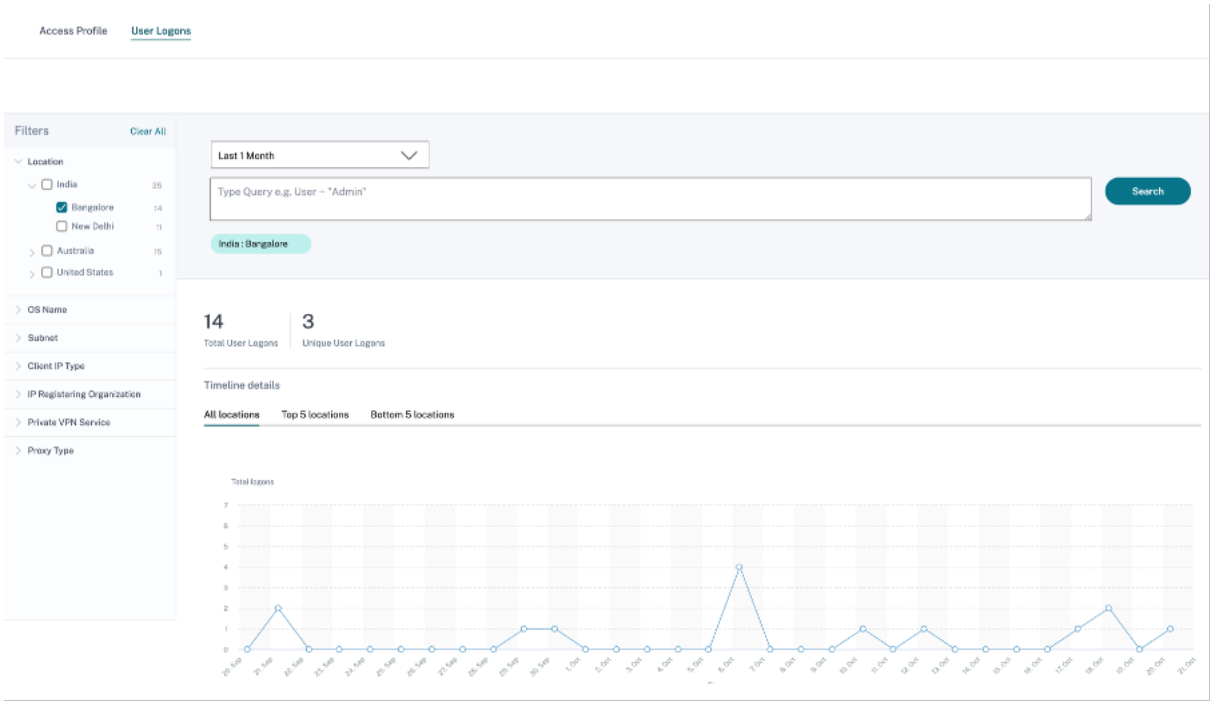
- 場所-ユーザーが仮想アプリまたは仮想デスクトップにログオンした上位の国と都市。



- エンドポイント-アプリとデスクトップのユーザーログオンに基づく上位のデバイス名と OS 名。

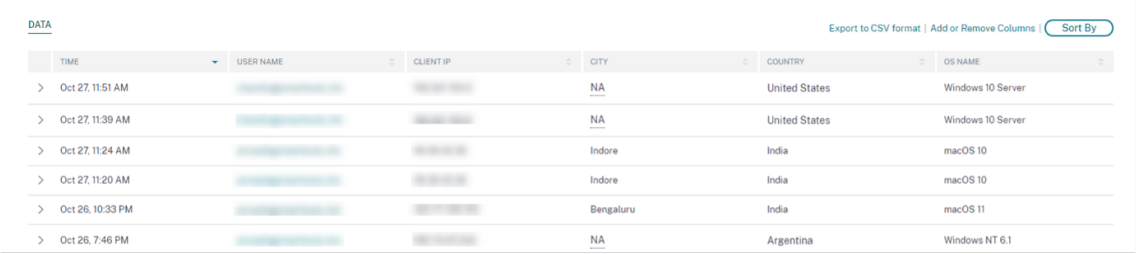
ユーザーのログオン詳細の表示

[ユーザーログオン] ページには、選択した場所から仮想アプリケーションまたは仮想デスクトップへのユーザーログオンの詳細が表示されます。この情報は、脅威の調査と分析を行う際に役立ちます。



DATA テーブルには、選択した場所と期間について、次のログオン詳細が表示されます。

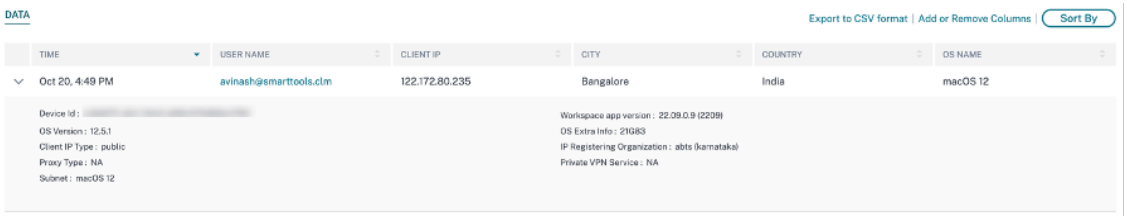
- 時間。ユーザーがログオンした日時。
- ユーザー名。ユーザーの ID。
- クライアント **IP**。ユーザーデバイスの IP アドレス。
- クライアント **IP** タイプ。パブリックまたはプライベートなど、ユーザの IP アドレスのタイプ。
- 都市と国。ユーザーが仮想アプリケーションまたは仮想デスクトップにログオンした場所。
- デバイス **ID**。ユーザーデバイスの ID コード。
- **OS** 名。ユーザーデバイス上のオペレーティングシステム。詳しくは、「アプリとデスクトップのセルフサービス検索」を参照してください。



各イベントを展開すると、次の詳細が表示されます。

- **OS** バージョン。ユーザーデバイス上のオペレーティングシステムのバージョン。詳しくは、「アプリとデスクトップのセルフサービス検索」を参照してください。

- **OS** 追加情報-ビルド番号、サービスパック、パッチなど、オペレーティングシステムの追加情報。詳しくは、「アプリとデスクトップのセルフサービス検索」を参照してください。
- **Workspace** アプリのバージョン。Citrix Workspace アプリまたは Citrix Receiver のビルドバージョンです。



DATA テーブルでは、次の操作を実行できます。

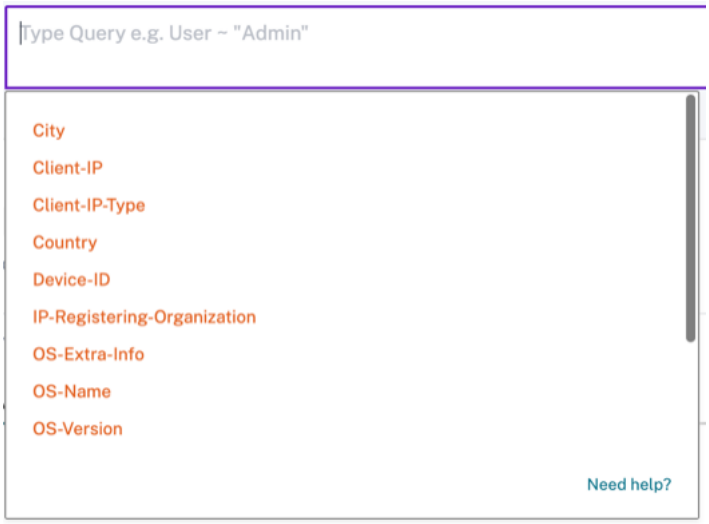
- [列の追加] または [削除] をクリックして、データの表示方法に基づいてテーブルの列を更新します。
- 「ソート基準」をクリックし、複数列のソートを実行するデータ要素を選択します。詳細については、「複数列の並べ替え」を参照してください。
- [**CSV** 形式にエクスポート] をクリックして、DATA テーブルに表示されているデータを CSV ファイルにダウンロードし、分析に使用します。

検索バー

また、検索バーを使用して、ログオンイベントに関連付けられたディメンションを使用してクエリを定義することもできます。

例:

```
User = “test user” AND Client-IP = “10.xx.xx.xx AND Client-IP-Type = public”

User = “demo_user@citrix.com” AND OS-Major-Version = “macOS 10.13” AND OS-Minor-Version = 6
```

ファセット

ログオンイベントには、次のファセットを使用できます。

- **Locations**-ログオンイベントを国と都市で絞り込みます。
- **OS**-オペレーティングシステムとそのバージョンでログオンイベントをフィルタリングします。
- サブネット-アクセスイベントをサブネットでフィルタリングします。
- **Client IP type**-パブリック IP タイプとプライベート IP タイプでアクセスイベントをフィルタリングします。
- **IP** 登録組織-アクセスイベントをユーザーが利用できる ISP 別にフィルタリングします。
- プライベート **VPN** サービス-プライベート VPN ネットワーク名でアクセスイベントをフィルタリングします。
- プロキシタイプ-HTTP、Web、Tor、SOCKS などのプロキシタイプ分類でアクセスイベントをフィルタリングします。

> 注
>
> また、データが利用できないか識別されていない場合も、[利用不可] ラベルが表示されることがあります。

ユーザーリスクのタイムラインとプロファイル

December 7, 2023

> ** 注注意 **
>
> ：シトリックスの Content Collaboration と ShareFile はサポート終了となり、ユーザーは使用できなくな

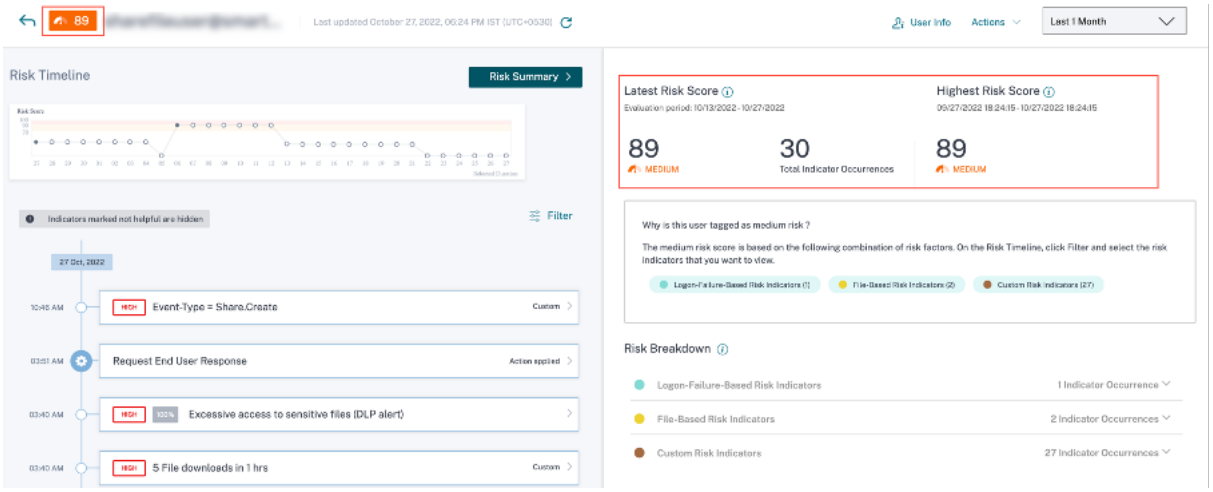
> ります。

ユーザーのプロファイルのユーザーリスクタイムラインを使用すると、Citrix Analytics 管理者は、ユーザーのリスクの高い行動に関するより深い洞察を得ることができます。デフォルトでは、過去 1 か月間のユーザーリスクタイムラインが表示されます。また、選択した期間にアカウントで実行された対応するアクションを確認することもできます。ユーザーリスクタイムラインから、ユーザーのプロファイルを深く掘り下げて、次のことを理解できます。

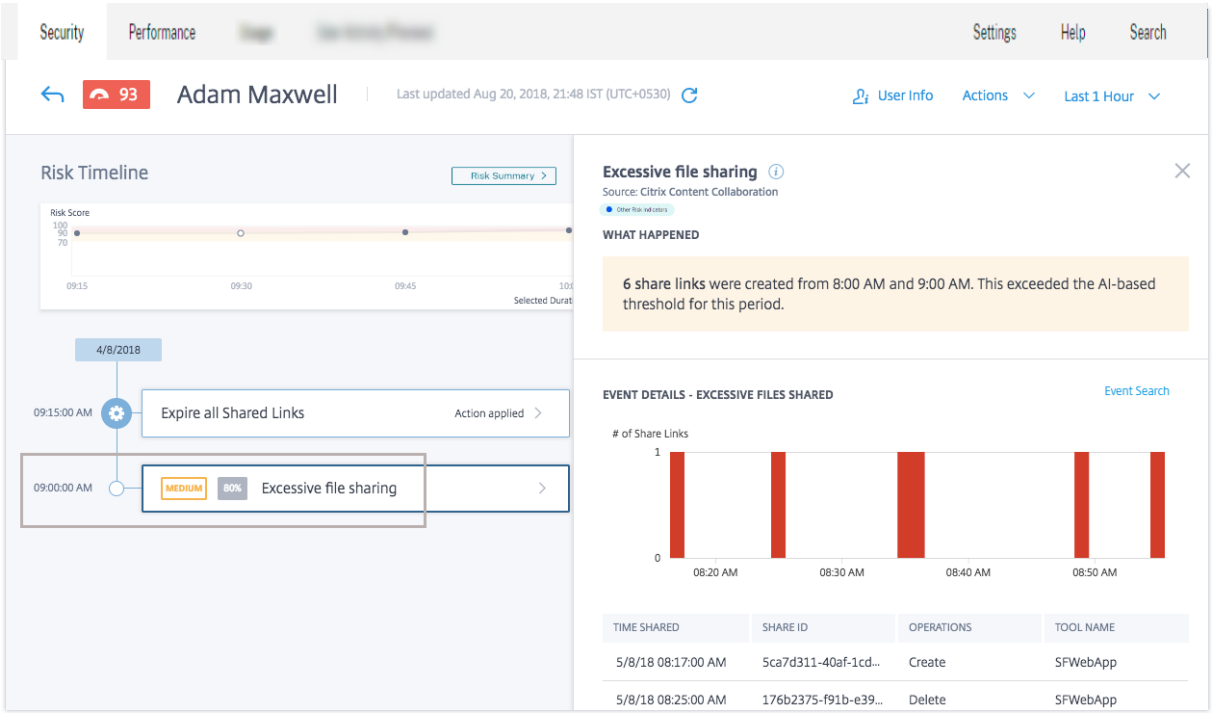
- アプリケーションの使用状況
- データ使用量
- デバイス使用量
- ロケーションの使い方

また、ユーザーのリスクスコアとリスク指標の傾向を表示し、ユーザーがリスクの高いユーザーであるかどうかを判断できます。

ユーザーリスクタイムラインページの左上隅に、ユーザーの最新のリスクスコアが表示されます。リスク概要ビューレポートには、最新の最大スコアと過去の最大スコアの両方が表示されます。



ユーザーのリスクタイムラインに移動すると、リスク指標またはアカウントに適用されているアクションのいずれかを選択できます。上記のいずれかを選択すると、右側のペインにリスク指標セクションまたはアクションセクションが表示されます。

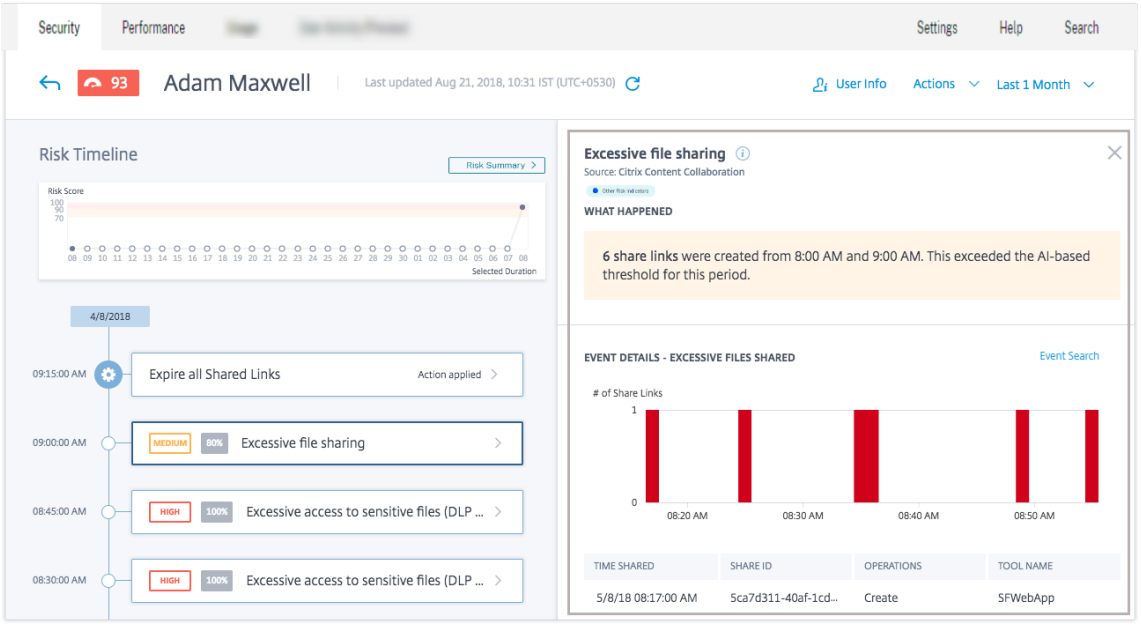


リスクタイムライン

リスクタイムラインには、次の情報が表示されます。

- リスク指標。リスク指標は、疑わしい、または組織にセキュリティ上の脅威をもたらす可能性のあるユーザーアクティビティです。インジケーターは、ユーザーの行動が通常の動作から逸脱したときにトリガーされます。リスク指標は、次のデータソースの場合があります。
  - Citrix Content Collaboration
  - Citrix Gateway
  - Citrix Endpoint Management
  - Citrix Virtual Apps and Desktops または Citrix DaaS（旧 Citrix Virtual Apps and Desktops サービス）
  - Citrix Secure Private Access

  ユーザーのタイムラインからリスク指標を選択すると、右側のペインにリスク指標情報セクションが表示されます。リスク指標の理由をイベントの詳細とともに表示できます。これらは、次のセクションに大きく分類されます。



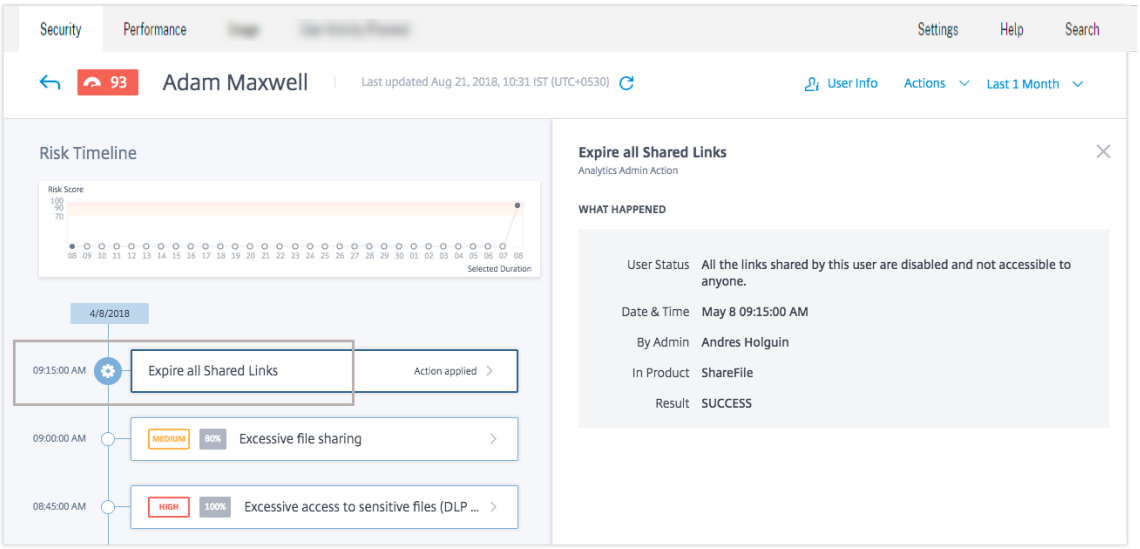
- 何が起こったのですか。リスク指標の概要は、こちらで確認できます。たとえば、[過剰なファイル共有] リスク指標を選択した場合などです。[何が起こったか] セクションでは、受信者に送信された共有リンクの数と、共有イベントがいつ発生したかを確認できます。
- イベントの詳細。個々のイベントエントリは、イベントの詳細とともにグラフ形式および表形式で表示できます。[イベント検索] をクリックして、セルフサービス検索ページにアクセスし、ユーザーのリスク指標に対応するイベントを表示します。詳細については、「セルフサービス検索」を参照してください。
- 追加のコンテキスト情報。このセクションでは、イベントの発生中に共有されたデータがある場合は、そのデータを表示できます。

リスク指標を「役に立った」または「役に立たない」と手動でマークできます。詳細については、「ユーザーリスク指標へのフィードバックの提供」を参照してください。

詳細: リスク指標

- アクション。アクションは、疑わしいイベントに対応し、将来の異常イベントの発生を防ぐのに役立ちます。ユーザーのプロファイルに適用されたアクションは、リスクタイムラインに表示されます。これらのアクションは、構成されたポリシーを通じてユーザーのアカウントに自動的に適用されるか、または手動で特定のアクションを適用できます。

  詳細: ポリシーとアクション。



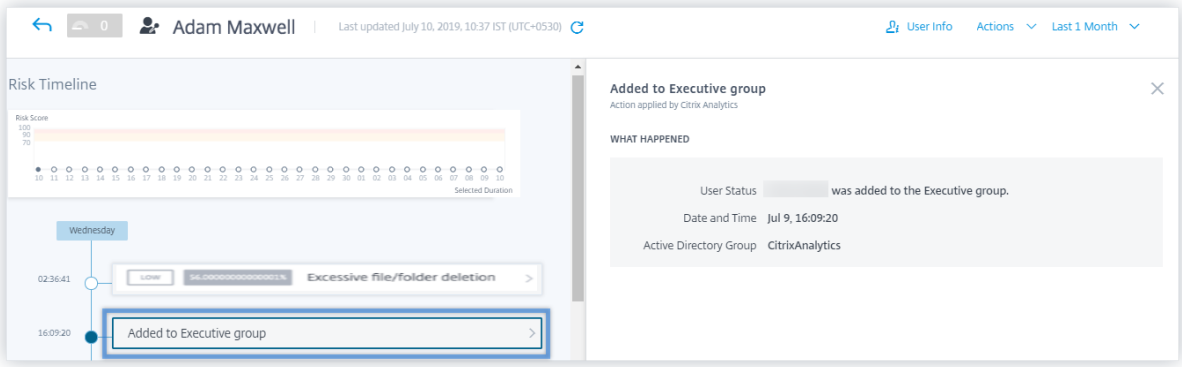
- 特権ユーザーイベント。特権ユーザイベントは、ユーザの Admin または Executive 権限ステータスが変更されるたびにトリガされます。ユーザーに対してリスク指標がトリガーされると、その指標を指定された特権ステータス変更イベントに関連付けることができます。必要に応じて、ユーザープロファイルに適切なアクションを適用できます。ユーザーリスクタイムラインに表示される管理者またはエグゼクティブ権限イベントは次のとおりです。

  - エグゼクティブグループに追加されました
  - エグゼクティブグループから削除されました
  - 特権が管理者に昇格されました
  - 管理者権限が削除されました

  エグゼクティブ特権グループ **CitrixAnalytics** に追加されたユーザー Adam Maxwell を考えてみましょう。**Executive** グループに追加イベントがユーザーのリスクタイムラインに追加されます。さて、Adam はファイルやフォルダを過剰に削除し始め、異常な動作を検出する機械学習アルゴリズムをトリガーします。ファイルやフォルダの過剰な削除リスクインジケータがユーザーのリスクタイムラインに追加されます。リスクタイムラインでイベントとリスク指標を比較できます。比較後、リスク指標がイベントの結果としてトリガーされたかどうかを判断できます。その場合は、Adam のプロファイルに適切なアクションを適用できます。特権ユーザーの詳細については、「特権ユーザー」を参照してください。

ユーザのタイムラインからイベントを選択すると、右側のペインにイベント情報セクションが表示されます。

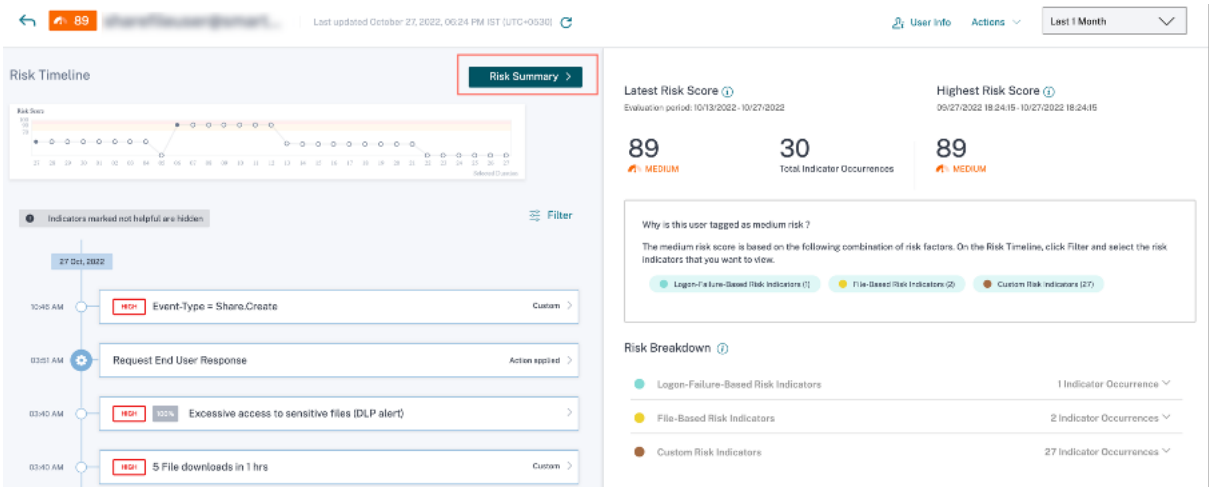
エグゼクティブの場合、右側のペインには、ユーザーステータス、日付と時刻、**Active Directory** グループなどの情報が表示されます。



管理者権限イベントの場合、右側のペインには、ユーザーステータス、日付と時刻、および製品内の情報が表示されます **。

リスクサマリー

リスクスコアに貢献したユーザーに関連付けられているリスク要因を表示します。選択した期間に最大値として取得されたリスクスコアの詳細が、最新のスコアと対応するリスク指標の数とともに表示されます。メインのランディングページまたは危険なユーザーページからユーザータイムラインに移動すると、ソースページの時間選択が保持されます。リスク要因について詳しくは、「Citrix ユーザーリスク指標」を参照してください。

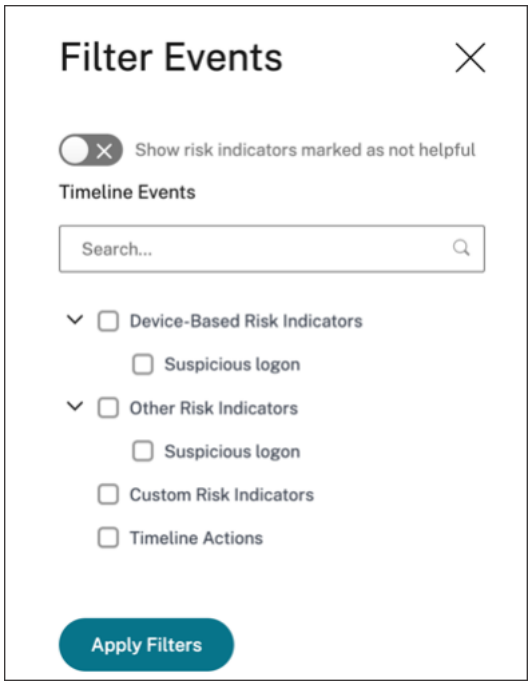


[リスクの概要] をクリックして、次の情報を表示します。

- 最新のリスクスコア: 最新のリスクスコアは、最近の行動に基づくユーザーの現在のリスクを示します。リスクスコアは、ユーザーが過去 2 週間に組織にもたらすリスクのレベルを決定します。リスクスコアの値は動的で、ユーザー行動分析に基づいて変化します。スコアに基づいて、ユーザーは「高リスクユーザー」、「中リスクユーザー」、「低リスクユーザー」、「リスクスコアがゼロのユーザー」のいずれかに分類されます。ユーザーカテゴリの詳細については、「ユーザーダッシュボード」を参照してください。
  - 指標発生回数の合計: 過去 2 週間にユーザーによってトリガーされたリスク指標の総数を示します。これらのトリガーされたリスク指標は、ユーザーのリスクスコアを決定します。

- 最も高いリスクスコア: 最も高いリスクスコアは、選択した期間内にこのユーザーについて計算されたリスクスコアの最大値を示します。これはユーザーの総合リスクを表すものであり、常に最新のリスクスコアと等しいとは限りません。
- リスク要因: リスクスコアに寄与したユーザーアクティビティに関連するリスク要因の 1 つ以上の組み合わせを示します。
- リスク内訳: 各リスク要因についてユーザーがトリガーしたリスク指標の数を示します。行を展開して詳細を表示します。

ユーザータイムラインで、[フィルタ] をクリックし、リスク要因、適用されたアクション、またはユーザーに関連付けられている特権ユーザーのステータスを選択し、対応するイベントを表示します。



ユーザープロフィール

ユーザープロファイルページには、ユーザーのアクティブディレクトリから取得された次のユーザー情報が表示されます。

- ジョブタイトル
- アドレス
- メール
- 電話
- 位置情報
- 組織

Citrix ユーザーリスク指標

April 12, 2024

> 注
>
> :Citrix Content Collaboration と ShareFile は廃止され、ユーザーは利用できなくなりました。

ユーザーリスク指標は、疑わしいと思われるユーザーアクティビティや、組織にセキュリティ上の脅威をもたらす可能性のあるユーザーアクティビティです。これらのリスク指標は、展開で使用されるすべての Citrix 製品にまたがります。リスク指標は、ユーザーの行動が正常から逸脱したときにトリガーされます。各リスク指標には、1 つ以上のリスク要因を関連付けることができます。これらのリスク要因は、ユーザーイベントの異常の種類を判断するのに役立ちます。リスク指標とそれに関連するリスク要因は、ユーザーのリスクスコアを決定します。

リスク指標に関連するリスク要因は次のとおりです。

- デバイスベースのリスク指標：ユーザーのデバイス履歴に基づいて異常と見なされるデバイスからユーザーがサインインしたときにトリガーされます。
- ロケーションベースのリスク指標：ユーザーのロケーション履歴に基づいて異常と見なされるロケーションに関連付けられた IP アドレスからユーザーがサインインするとトリガーされます。
- **IP** ベースのリスク指標：ユーザーが疑わしいと識別された IP アドレスからリソースにアクセスしようとしたときにトリガーされます。IP アドレスがユーザーにとって異常かどうかは関係ありません。
- ログオン失敗ベースのリスク指標：ユーザーが過度または異常なログオン失敗のパターンを持つ場合にトリガーされます。
- データベースのリスク指標：ユーザーが Workspace セッションからデータを取り出そうとしたときにトリガーされます。観察中のユーザーの行動には、コピーまたは貼り付けイベント、ダウンロードパターンなどが含まれます。
- ファイルベースのリスク指標:Content Collaboration でのファイルアクセスに関するユーザーの行動が、過去のアクセスパターンに基づいて異常であると見なされたときにトリガーされます。監視対象のユーザーの行動には、ダウンロードパターン、機密コンテンツへのアクセス、ランサムウェアを示すアクティビティなどが含まれます。
- カスタムリスク指標：事前設定された条件またはユーザー定義の条件が満たされたときにトリガーされます。詳しくは、次の記事を参照してください：

  - カスタムリスク指標
  - 事前設定されたカスタムリスクインジケーターとポリシー

- その他のリスク指標-デバイスベース、ロケーションベース、ログオン失敗ベースなど、事前定義されたリスク要因のいずれにも属さないリスク指標。

また、リスク指標は、類似するリスクに基づいてリスクカテゴリに分類されます。詳細については、「リスクカテゴリ」を参照してください。

次の表は、リスク指標、リスク因子、およびリスクカテゴリの相関関係を示しています。

製品	ユーザーリスクインジケータ	リスクファクター	リスクカテゴリ
Citrix Endpoint Management	禁止リストに登録されたアプリが検出されたデバイス	その他のリスク指標	侵害されたエンドポイント
	ジェイルブレイクまたは Root 化されたデバイスが検出されました	その他のリスク指標	侵害されたエンドポイント
	管理対象外のデバイスが検出されました	その他のリスク指標	侵害されたエンドポイント
Citrix Gateway	エンドポイント分析 (EPA) スキャンの失敗	その他のリスク指標	侵害されたユーザー
	過剰な認証失敗	ログオン失敗ベースのリスク指標	侵害されたユーザー
	あり得ない移動	ロケーションベースのリスク指標	侵害されたユーザー
	疑わしい IP からのログオン	IP ベースのリスク指標	侵害されたユーザー
	疑わしいログオン	デバイスベースのリスク指標、IP ベースのリスク指標、ロケーションベースのリスク指標、およびその他のリスク指標	侵害されたユーザー
	異常な認証の失敗	ログオン失敗ベースのリスク指標	侵害されたユーザー
Citrix Secure Private Access	ブラックリストに載っている URL にアクセスしようとしました	その他のリスク指標	インサイダーの脅威

製品	ユーザーリスクインジケータ	リスクファクター	リスクカテゴリ
	過剰なデータのダウンロード	その他のリスク指標	インサイダーの脅威
	危険なウェブサイトへのアクセス	その他のリスク指標	インサイダーの脅威
	異常なアップロードボリューム	その他のリスク指標	インサイダーの脅威
Citrix DaaS（旧 Citrix Virtual Apps and Desktops サービス）およびオンプレミスの Citrix Virtual Apps and Desktops	あり得ない移動	ロケーションベースのリスク指標	侵害されたユーザー
	データ流出の可能性	データベースのリスク指標	データ流出
	疑わしいログオン	デバイスベースのリスク指標、IP ベースのリスク指標、ロケーションベースのリスク指標、およびその他のリスク指標	侵害されたユーザー

リスク指標を「役に立った」または「役に立たない」と手動でマークできます。詳細については、「ユーザーリスク指標へのフィードバックの提供」を参照してください。

Citrix Endpoint Management リスク指標

May 10, 2022

ブラックリストに登録されたアプリが検出されたデバイス

Citrix Analytics は、ブラックリストに登録されたアプリを含むデバイスのアクティビティに基づいてアクセスの脅威を検出し、対応するリスク指標をトリガーします。

ブラックリストに登録されたアプリが検出されたデバイスは、Endpoint Management サービスがソフトウェアインベントリ中にブラックリストに登録されたアプリを検出したときにトリガーされます。このアラートにより、組織のネットワーク上にあるデバイスでは、承認されたアプリのみが実行されることが保証されます。

ブラックリストに登録されたアプリが検出されたデバイスに関連するリスク要因は、その他のリスク指標です。リスク要因について詳しくは、「Citrix ユーザーリスク指標」を参照してください。

ブラックリストに載っているアプリが検知されたデバイスはいつトリガーされますか?

ブラックリストに登録されたアプリが検出されたデバイスのリスクインジケータは、ユーザーのデバイスでブラックリストに登録されたアプリが検出されたときに報告されます。Endpoint Management サービスが、ソフトウェアインベントリ中にデバイス上のブラックリストに登録されたアプリケーションを検出すると、Citrix Analytics にイベントが送信されます。

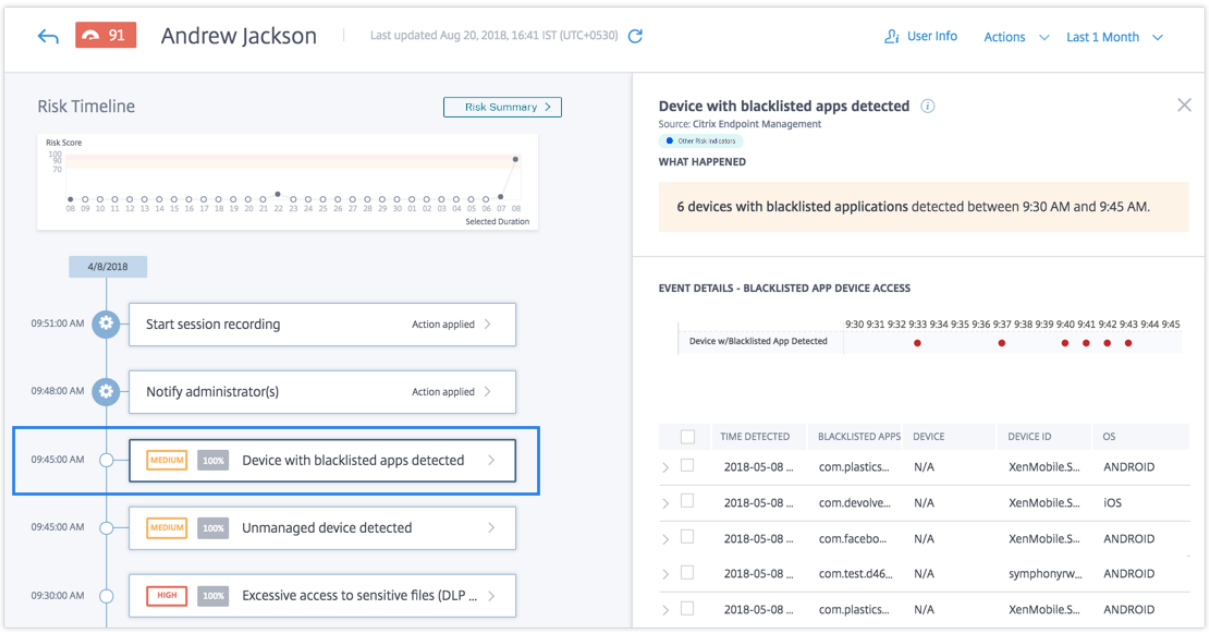
Citrix Analytics はこれらのイベントを監視し、ユーザーのリスクスコアを更新します。また、ブラックリストに登録されたアプリが検出されたリスク指標エントリを含むデバイスをユーザーのリスクタイムラインに追加します。

ブラックリストに登録されたアプリでデバイスを分析する方法は?

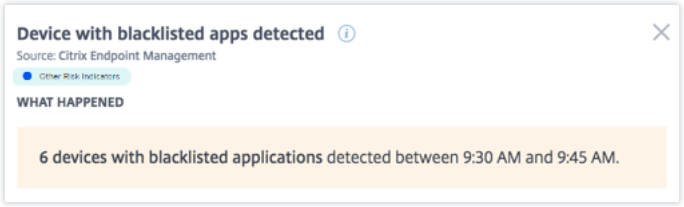
ブラックリストに登録されたアプリが最近インストールされたデバイスを使用した Andrew Jackson ユーザーについて考えてみましょう。Endpoint Management は、この状態を Citrix Analytics に報告し、Andrew Jackson に更新されたリスクスコアを割り当てます。

Andrew Jackson のリスクタイムラインから、報告されたブラックリストに登録されたアプリでリスクインジケータが検出されたデバイスを選択できます。イベントの理由は、ブラックリストに登録されたアプリのリスト、Endpoint Management がブラックリストに登録されたアプリを検出した時間などの詳細とともに表示されます。

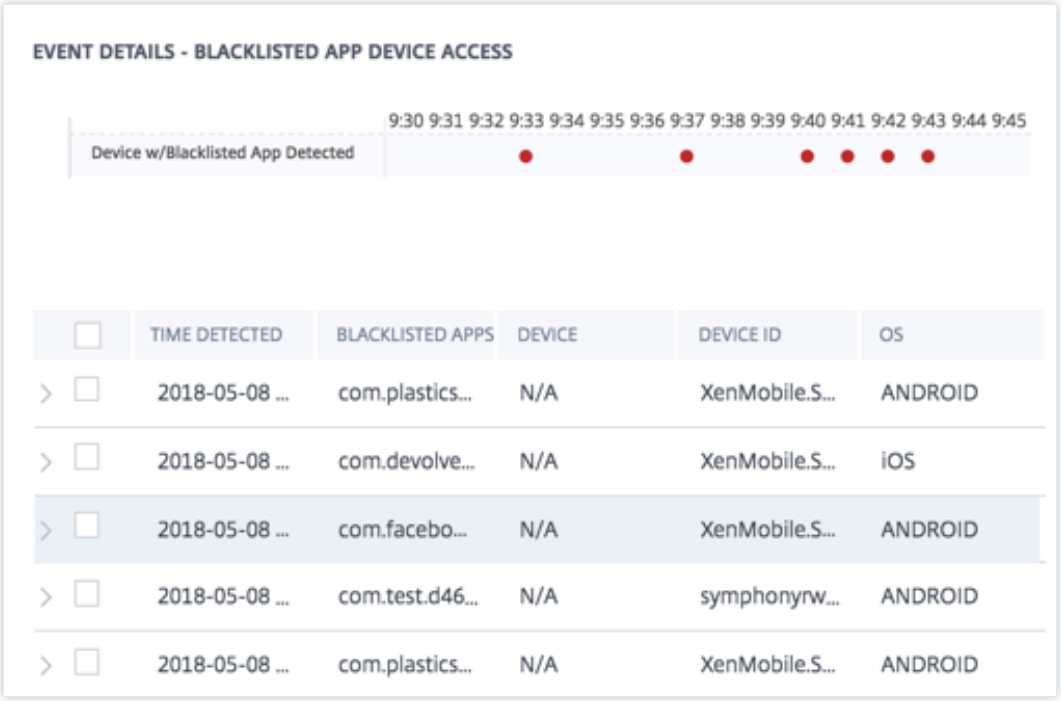
ブラックリストに登録されたアプリがユーザーのリスク指標を検出したデバイスを表示するには、[セキュリティ] > [ユーザー] に移動し、ユーザーを選択します。



- WHAT **HAPPENED** セクションでは、イベントの概要を表示できます。Endpoint Management サービスによって検出されたブラックリストに登録されたアプリケーションがインストールされたデバイスの数と、イベントが発生した時刻を表示できます。



- [イベントの詳細—ブラックリストに登録されたアプリデバイスのアクセス] セクションでは、イベントがグラフ形式および表形式で表示されます。イベントはグラフに個別のエントリとして表示され、テーブルには次の重要な情報が表示されます。
  - 検出された時間-Endpoint Management によってブラックリストに登録されたアプリの存在が報告された日時。
  - ブラックリストに登録されたアプリ-デバイス上のブラックリストに登録されているアプリ。
  - デバイス-使用されているモバイルデバイス。
  - **Device ID**：セッションへのログオンに使用されるデバイスの ID に関する情報。
  - **OS**-モバイルデバイスのオペレーティングシステム。



> 注:
>
> 詳細を表形式で表示するだけでなく、アラートのインスタンスに対する矢印をクリックして詳細を表示できま

> す。

ユーザーに適用できるアクション

ユーザーのアカウントでは、次の操作を実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントで異常なアクティビティや疑わしいアクティビティが発生すると、すべての管理者または選択した管理者に電子メール通知が送信されます。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

ジェイルブレイクまたは **Root** 化されたデバイスが検出されました

Citrix Analytics は、ジェイルブレイクまたは Root 化されたデバイスのアクティビティに基づいてアクセスの脅威を検出し、対応するリスク指標をトリガーします。

ジェイルブレイクまたは **Root** 化されたデバイスのリスクインジケータは、ユーザーがジェイルブレイクまたは Root 化されたデバイスを使用してネットワークに接続するとトリガーされます。Secure Hub はデバイスを検出し、Endpoint Management サービスにインシデントを報告します。このアラートは、許可されたユーザーとデバイスのみが組織のネットワーク上にあることを保証します。

ジェイルブレイクまたは Root 化されたデバイスのリスク指標に関連するリスク要因は、その他のリスク指標です。リスク要因について詳しくは、「Citrix ユーザーリスク指標」を参照してください。

ジェイルブレイクまたは **Root** 化されたデバイスが検出されたリスク指標はいつトリガーされますか**?**

セキュリティ担当者は、ユーザーがネットワーク準拠のデバイスを使用して接続できるようにすることが重要です。ジェイルブレイクまたは **Root** 化されたデバイスが検出されたリスクインジケータは、ジェイルブレイクされた iOS デバイスまたは Root 化されている Android デバイスを持つユーザーに警告します。

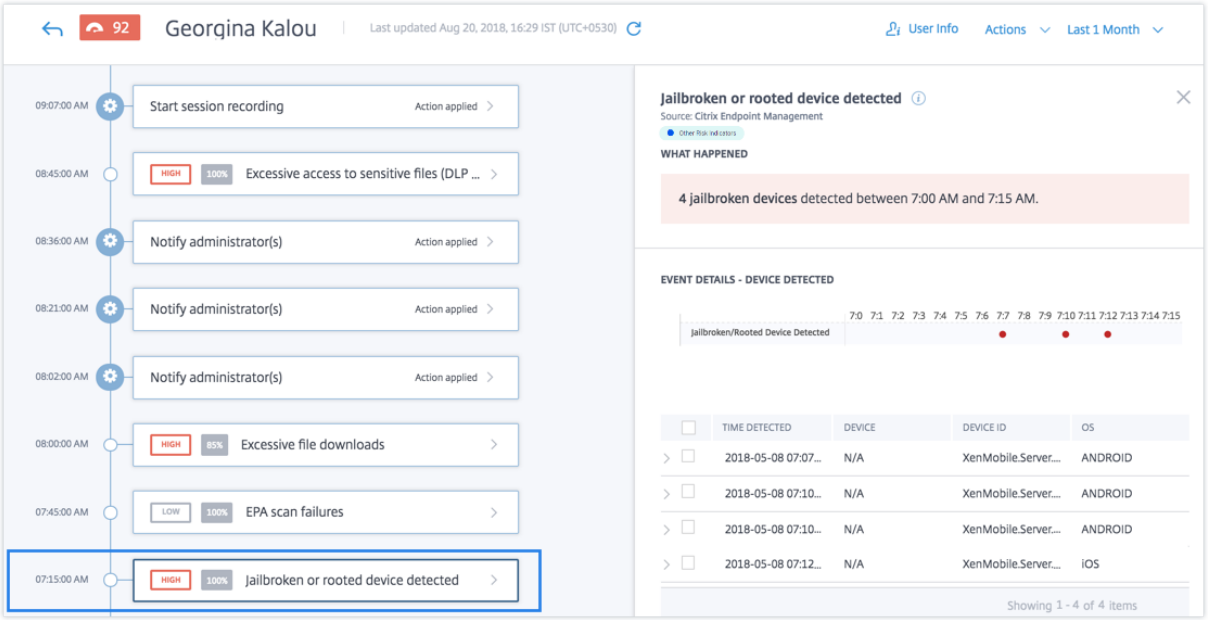
ジェイルブレイクまたは **Root** 化されたデバイスのリスクインジケータは、登録されたデバイスがジェイルブレイクまたは Root 化されたときにトリガーされます。Secure Hub はデバイス上のイベントを検出し、Endpoint Management サービスに報告します。

ジェイルブレイクまたは **Root** 化されたデバイスが検出されたリスク指標を分析するにはどうすればよいですか**?**

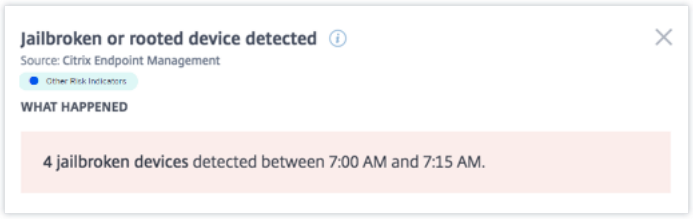
登録された iOS デバイスが最近ジェイルブレイクされたユーザー、Georgina Kalou を考えてみましょう。この不審な動作は、Citrix Analytics によって検出され、リスクスコアは Georgina Kalou に割り当てられます。

Georgina Kalou のリスクタイムラインから、報告されたジェイルブレイクまたはルートデバイスが検出されたリスク指標を選択できます。イベントの理由は、リスク指標がトリガーされた時間、イベントの説明などの詳細とともに表示されます。

ユーザーのジェイルブレイクまたは **Root** 化されたデバイスで検出されたリスクインジケータを表示するには、[セキュリティ **] > [**ユーザー] に移動し、ユーザーを選択します。

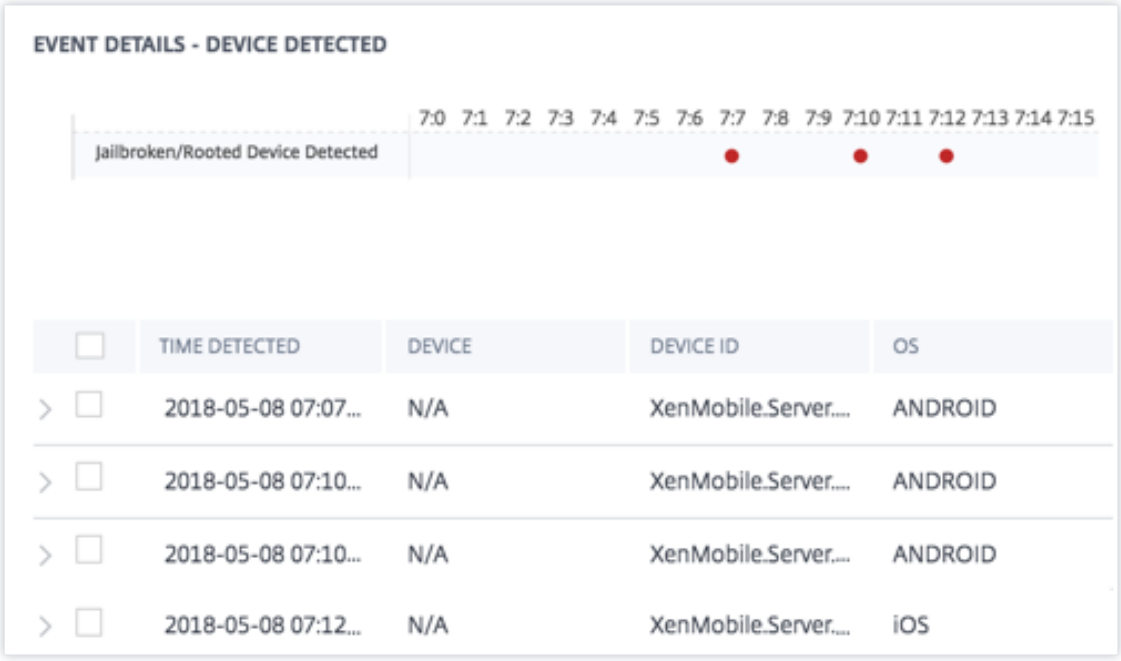


- **WHAT HAPPENED** セクションでは、イベントの概要を表示できます。検出されたジェイルブレイクまたは Root 化されたデバイスの数と、イベントが発生した時刻を表示できます。



- [**EVENT DETAILS —DEVICE DETECTED**] セクションでは、イベントがグラフおよび表形式で表示されます。イベントはグラフに個別のエントリとして表示され、テーブルには次の重要な情報が表示されます。
  - 時間が検出されました。ジェイルブレイクまたは Root 化されたデバイスが検出された時刻。
  - **[**デバイス**]**。使用したモバイルデバイス。
  - デバイス **ID**。セッションへのログオンに使用されるデバイスの ID に関する情報。

– **OS** からインストールできます。モバイルデバイスのオペレーティングシステム。



> 注:
>
> 詳細を表形式で表示するだけでなく、アラートのインスタンスに対する矢印をクリックして詳細を表示します。

ユーザーに適用できるアクション

ユーザーのアカウントでは、次の操作を実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントで異常なアクティビティや疑わしいアクティビティが発生すると、すべての管理者または選択した管理者に電子メール通知が送信されます。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

管理対象外のデバイスが検出されました

Citrix Analytics は、管理対象外のデバイスのアクティビティに基づいてアクセスの脅威を検出し、対応するリスク指標をトリガーします。

管理対象外デバイスが検出されたリスクインジケータは、デバイスが次の場合にトリガーされます。

- 自動化されたアクションにより、リモートでワイプされます。
- 管理者によって手動でワイプされます。
- ユーザーによって登録解除されました。

管理対象外デバイスが検出されたリスク指標に関連するリスク要因は、その他のリスク指標です。リスク要因について詳しくは、「Citrix ユーザーリスク指標」を参照してください。

管理対象外デバイスで検出されたリスク指標はいつトリガーされますか?

管理対象外のデバイスが検出されたリスクインジケータは、ユーザーのデバイスが管理対象外になったときに報告されます。デバイスが管理対象外状態に変化する原因は次のとおりです。

- ユーザーによって実行されるアクション。
- Endpoint Management 管理者またはサーバーによって実行されるアクション。

組織では、Endpoint Management サービスを使用して、ネットワークにアクセスするデバイスとアプリを管理できます。詳細については、「管理モード」を参照してください。

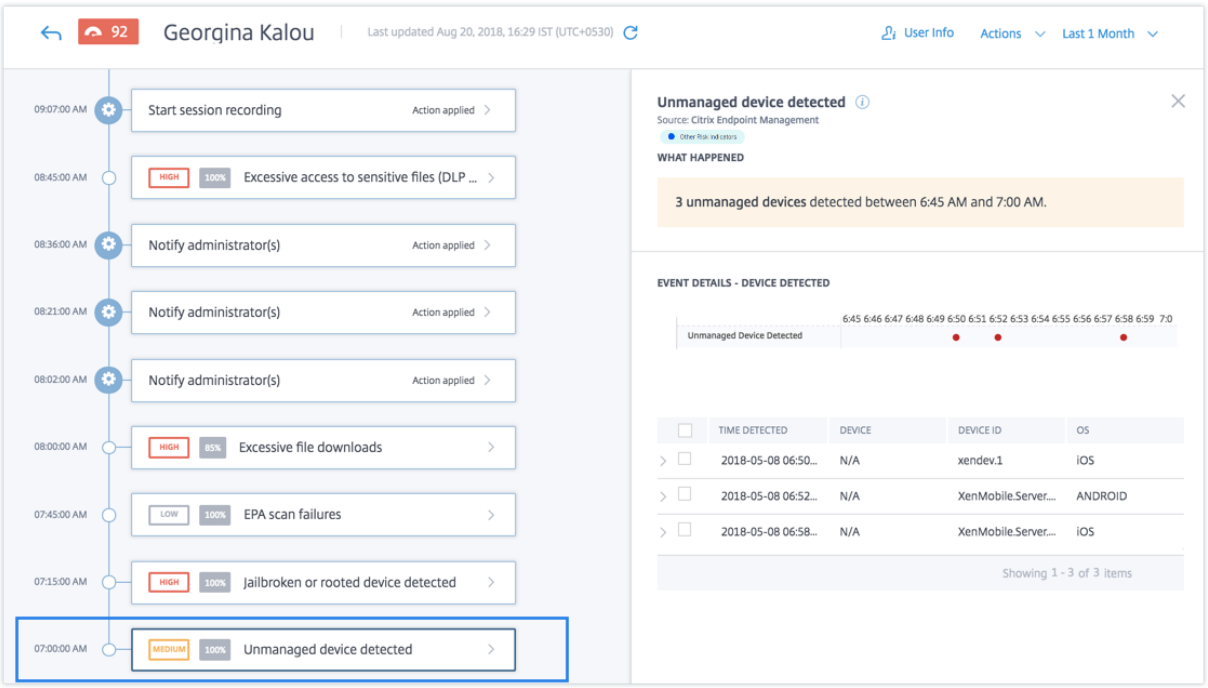
ユーザーのデバイスが管理対象外の状態に変更されると、Endpoint Management サービスはこのイベントを検出して Citrix Analytics にレポートします。ユーザーのリスクスコアが更新されます。管理対象外のデバイスで検出されたリスク指標がユーザーのリスクタイムラインに追加されます。

管理対象外のデバイスが検出されたリスク指標を分析するには?

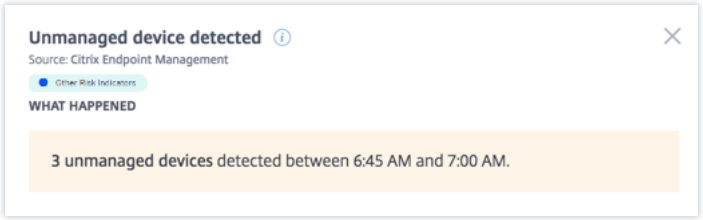
Georgina Kalou のユーザーを考えてみましょう。そのデバイスは、サーバー上の自動化されたアクションによってリモートでワイプされます。Endpoint Management では、このイベントが Citrix Analytics に報告され、更新されたリスクスコアが Georgina Kalou に割り当てられます。

Georgina Kalou のリスクタイムラインから、報告された管理外デバイスで検出されたリスク指標を選択できます。イベントの理由は、リスク指標がトリガーされた時間、イベントの説明などの詳細とともに表示されます。

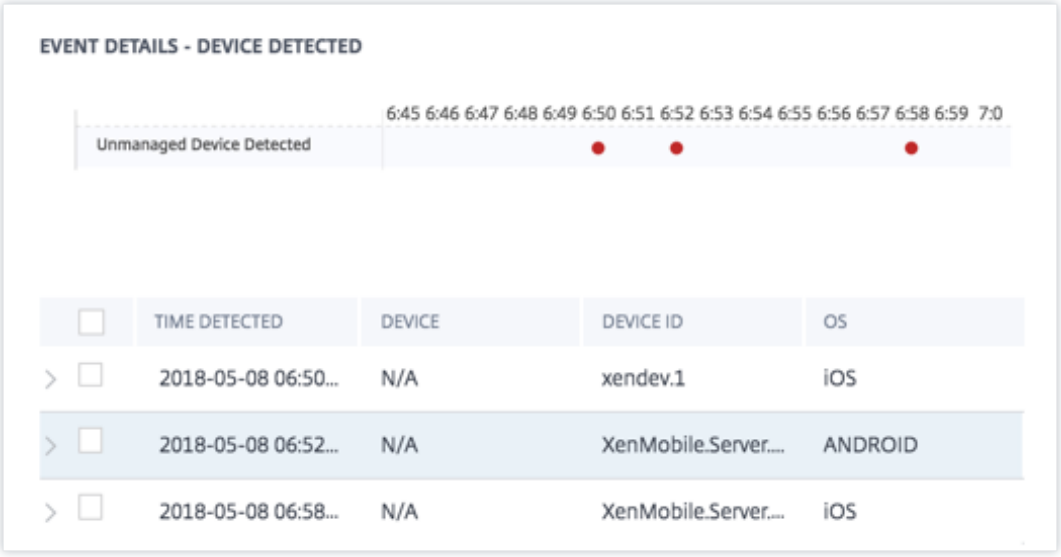
ユーザーの管理対象外デバイスが検出したリスクインジケータを表示するには、[セキュリティ] **>** [ユーザー] に移動し、ユーザーを選択します。



- **WHAT HAPPENED** セクションでは、イベントの概要を表示できます。検出された管理対象外デバイスの数と、イベントが発生した時刻を表示できます。



- [**EVENT DETAILS** —**DEVICE DETECTED**] セクションでは、イベントがグラフおよび表形式で表示されます。イベントはグラフに個別のエントリとして表示され、テーブルには次の重要な情報が表示されます。
  - 時間が検出されました。イベントが検出された時刻。
  - **[**デバイス**]**。使用したモバイルデバイス。
  - デバイス **ID**。モバイルデバイスのデバイス ID。
  - **OS** からインストールできます。モバイルデバイスのオペレーティングシステム。



ユーザーに適用できるアクション

ユーザーのアカウントでは、次の操作を実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントで異常なアクティビティや疑わしいアクティビティが発生すると、すべての管理者または選択した管理者に電子メール通知が送信されます。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

Citrix Gateway リスク指標

July 15, 2022

エンドポイント分析 **(EPA)** スキャンの失敗

Citrix Analytics は、EPA スキャン失敗アクティビティに基づいてユーザーアクセスベースの脅威を検出し、対応するリスク指標をトリガーします。

エンドポイント分析スキャン失敗リスク指標に関連付けられたリスク要因は、その他のリスク指標です。リスク要因について詳しくは、「Citrix ユーザーリスク指標」を参照してください。

EPA スキャン失敗リスク指標はいつトリガーされますか**?**

EPA スキャン失敗リスクインジケータは、Citrix Gateway のエンドポイント分析（EPA）スキャンポリシーで事前認証または認証後のスキャンポリシーに失敗したデバイスを使用してユーザーがネットワークにアクセスしようとしたときに報告されます。

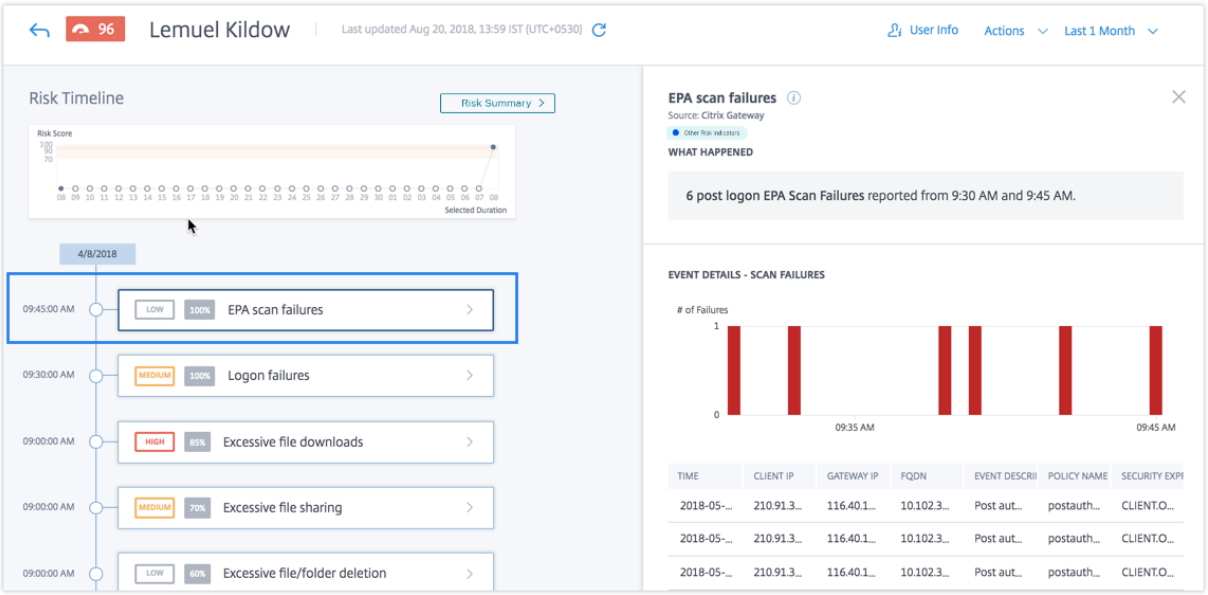
Citrix Gateway はこれらのイベントを検出し、Citrix Analytics に報告します。Citrix Analytics はこれらのイベントをすべて監視して、ユーザーが EPA スキャンに失敗したかどうかを検出します。Citrix Analytics がユーザーの過度の EPA スキャン失敗を判断すると、ユーザーのリスクスコアが更新され、ユーザーのリスクタイムラインに EPA スキャン失敗リスクインジケータエントリが追加されます。

EPA スキャン失敗リスク指標を分析するには**?**

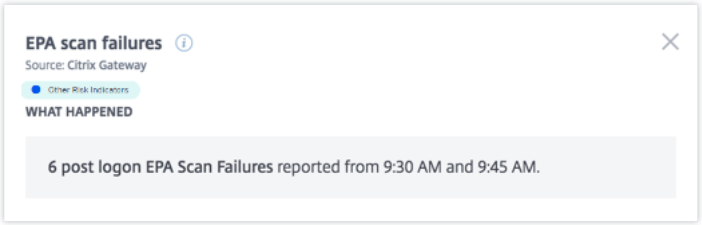
最近、Citrix Gateway の EPA スキャンに失敗したデバイスを使用してネットワークに複数回アクセスしようとしたユーザー Lemuel を考えてみましょう。Citrix Gateway は、この失敗を Citrix Analytics に報告し、Citrix Analytics は更新されたリスクスコアを Lemuel に割り当てます。EPA スキャン失敗リスク指標は Lemuel Kildow のリスクタイムラインに追加されます。

ユーザーの **EPA** スキャン失敗エントリを表示するには、[セキュリティ**] > [**ユーザー] に移動し、ユーザーを選択します。

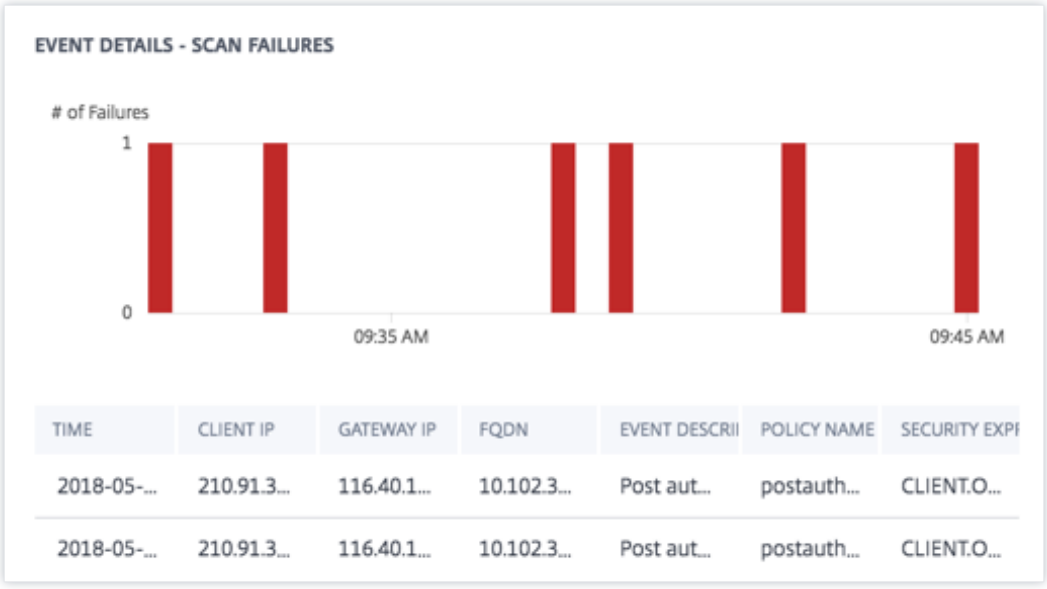
Lemuel Kildow のリスクタイムラインから、ユーザーに対して報告された最新の **EPA** スキャン失敗リスク指標を選択できます。タイムラインから EPA スキャン失敗リスク指標のエントリを選択すると、対応する詳細情報パネルが右側のペインに表示されます。



- **WHAT HAPPENED** セクションには、EPA スキャン失敗リスク指標の簡単な概要が記載されています。また、選択した期間中に報告されたログオン後 EPA スキャン失敗の数も含まれます。



- [イベントの詳細—スキャン失敗] セクションには、選択した期間中に発生した個々の EPA スキャン失敗イベントのタイムラインが表示されます。また、各イベントに関する次の重要な情報を提供するテーブルも含まれています。
  - 時間。EPA スキャンが失敗した時刻。
  - クライアント **IP**。EPA スキャン失敗の原因となるクライアントの IP アドレス。
  - ゲートウェイ **IP**。EPA スキャンの失敗を報告した Citrix Gateway の IP アドレス。
  - **FQDN**。Citrix Gateway の完全修飾ドメイン名。
  - イベントの説明。EPA スキャンが失敗した理由の簡単な説明。
  - ポリシー名。Citrix Gateway で構成された EPA スキャンポリシー名。
  - セキュリティ表現。Citrix Gateway で構成されたセキュリティ式。



ユーザーに適用できるアクション

ユーザーのアカウントでは、次の操作を実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントで異常なアクティビティや疑わしいアクティビティが発生すると、すべての管理者または選択した管理者に電子メール通知が送信されます。
- ユーザーをログオフします。ユーザーが自分のアカウントからログオフすると、Citrix Gateway 管理者がユーザーのログオフアクションをクリアするまで、Citrix Gateway 経由でリソースにアクセスできません。
- ユーザーのロック：異常な動作によってユーザーのアカウントがロックされると、Gateway 管理者がアカウントのロックを解除するまで、Citrix Gateway を介してリソースにアクセスできません。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

過剰な認証失敗

Citrix Analytics は、過剰な認証失敗に基づいてユーザーアクセスベースの脅威を検出し、対応するリスク指標をトリガーします。

過剰な認証失敗のリスク指標に関連するリスク要因は、ログオン失敗ベースのリスク指標です。リスク要因について詳しくは、「Citrix ユーザーリスク指標」を参照してください。

過剰な認証失敗のリスク指標はいつトリガーされますか?

ログオン失敗リスクインジケータは、ユーザーが一定期間内に複数の Citrix Gateway 認証失敗に遭遇したときに報告されます。Citrix Gateway の認証失敗は、ユーザーに多要素認証が構成されているかどうかに応じて、プライマリ、セカンダリ、またはターシャリの認証失敗になります。

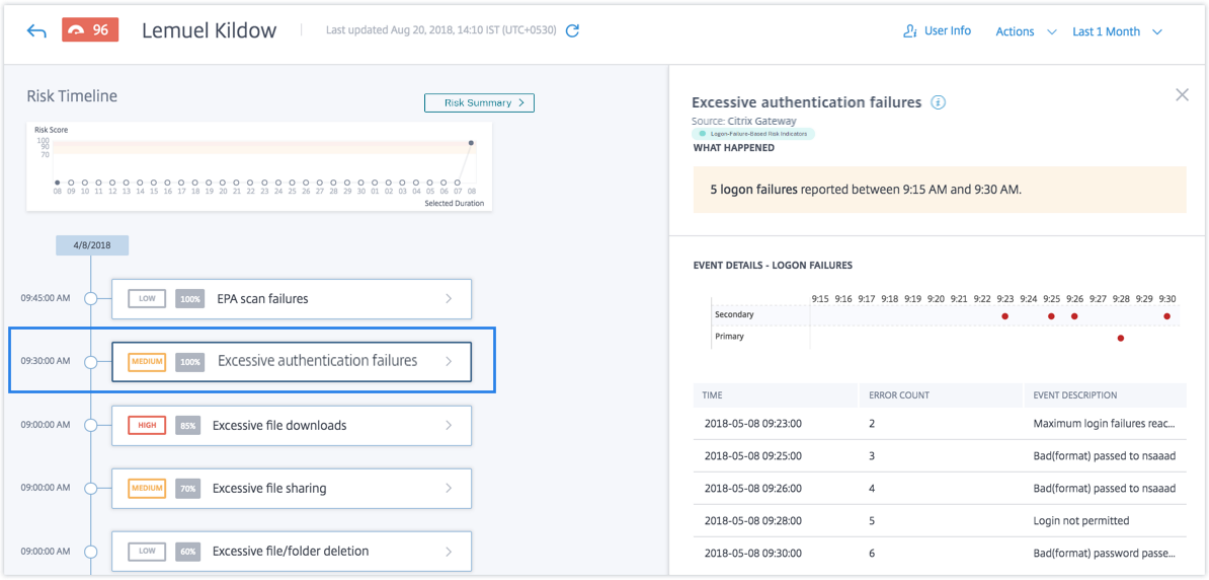
Citrix Gateway は、すべてのユーザー認証エラーを検出し、これらのイベントを Citrix Analytics に報告します。Citrix Analytics は、これらすべてのイベントを監視して、ユーザーの認証エラーが多すぎるかどうかを検出します。Citrix Analytics が過剰な認証失敗を判断すると、ユーザーのリスクスコアが更新されます。過剰な認証失敗のリスクインジケータがユーザーのリスクタイムラインに追加されます。

過剰な認証失敗のリスク指標を分析するには

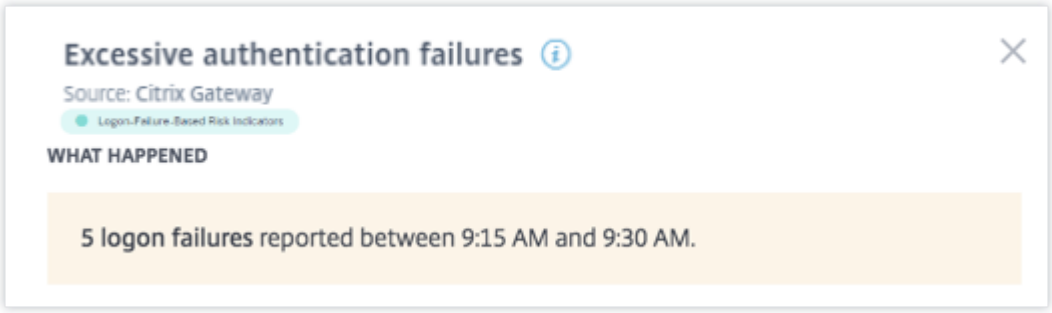
最近、ネットワーク認証の試行を複数回失敗したユーザー Lemuel を考えてみましょう。Citrix Gateway はこれらの障害を Citrix Analytics に報告し、更新されたリスクスコアが Lemuel に割り当てられます。過剰な認証失敗のリスク指標が Lemuel Kildow のリスクタイムラインに追加されます。

ユーザーの過剰な認証失敗のリスク指標エントリを表示するには、**[セキュリティ] > [ユーザー]** に移動して、ユーザーを選択します。

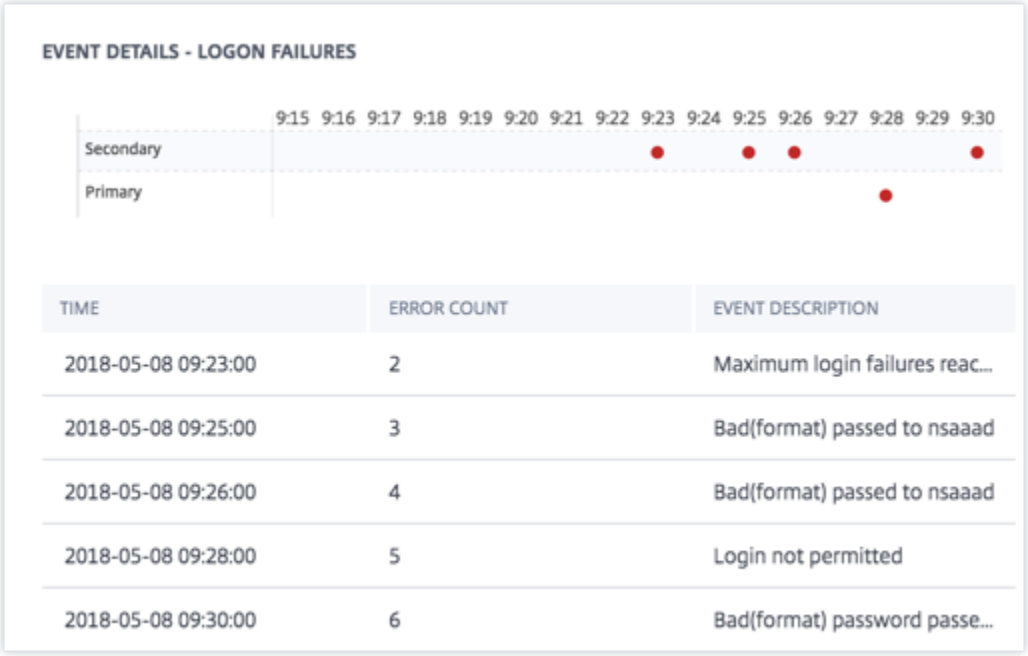
Lemuel Kildow のリスクタイムラインから、ユーザーに対して報告された最新の過剰な認証失敗リスク指標を選択できます。リスクタイムラインから [過剰な認証失敗リスクインジケータ] エントリを選択すると、対応する詳細情報パネルが右側のペインに表示されます。



- **WHAT** HAPPENED セクションには、選択した期間中に発生した認証失敗の数など、リスク指標の簡単な概要が表示されます。



- [**EVENT DETAILS**] セクションには、選択した期間中に発生した個々の過剰認証失敗イベントのタイムラインが表示されます。また、各イベントに関する次の重要な情報も表示できます。
  - 時間。ログオン失敗が発生した時刻。
  - エラー数。イベント発生時および過去 48 時間の間にユーザに対して検出された認証失敗の数。
  - イベントの説明。ログオン失敗の理由の簡単な説明。



ユーザーに適用できるアクション

ユーザーのアカウントでは、次の操作を実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントで異常なアクティビティや疑わしいアクティビティが発生すると、すべての管理者または選択した管理者に電子メール通知が送信されます。
- ユーザーをログオフします。ユーザーが自分のアカウントからログオフすると、Citrix Gateway 管理者がユーザーのログオフアクションをクリアするまで、Citrix Gateway 経由でリソースにアクセスできません。
- ユーザーのロック：異常な動作によってユーザーのアカウントがロックされると、Gateway 管理者がアカウントのロックを解除するまで、Citrix Gateway を介してリソースにアクセスできません。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

あり得ない移動

Citrix Analytics は、2 つの異なる国からの連続したログオンが、国間の予想される移動時間よりも短い期間内に行われた場合、ユーザーのログオンが危険であると検出します。

あり得ない移動時間のシナリオは、次のリスクを示しています。

- 侵害された認証情報: リモートの攻撃者が正当なユーザーの資格情報を盗みます。
- 共有認証情報: 異なるユーザーが同じユーザー資格情報を使用しています。

あり得ない移動リスク指標はいつトリガーされますか

あり得ない移動リスク指標は、連続するユーザーログオンの各ペア間の時間と推定距離を評価し、その距離が個々の人がその時間内に移動できるよりも長い場合にトリガーされます。

> 注:
>
> このリスク指標には、ユーザーの実際の場所を反映していない次のシナリオの誤検知アラートを減らすためのロジックも含まれています。
>
> - ユーザーがプロキシ接続から Citrix Gateway 経由でログオンするとき。
> - ユーザーがホストされているクライアントから Citrix Gateway 経由でログオンするとき。

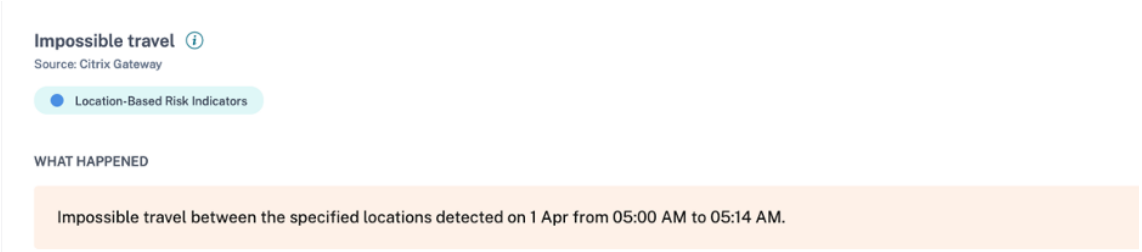
インポッシブルリスク指標の分析方法

ユーザー Adam Maxwell が、インドのバンガロールとノルウェーのオスロの 2 つの場所から 1 分以内にログオンするとします。Citrix Analytics は、このログオンイベントをあり得ない移動シナリオとして検出し、あり得ない移動リスク指標をトリガーします。リスク指標が Adam Maxwell のリスクタイムラインに追加され、リスクスコアが Adam Maxwell に割り当てられます。

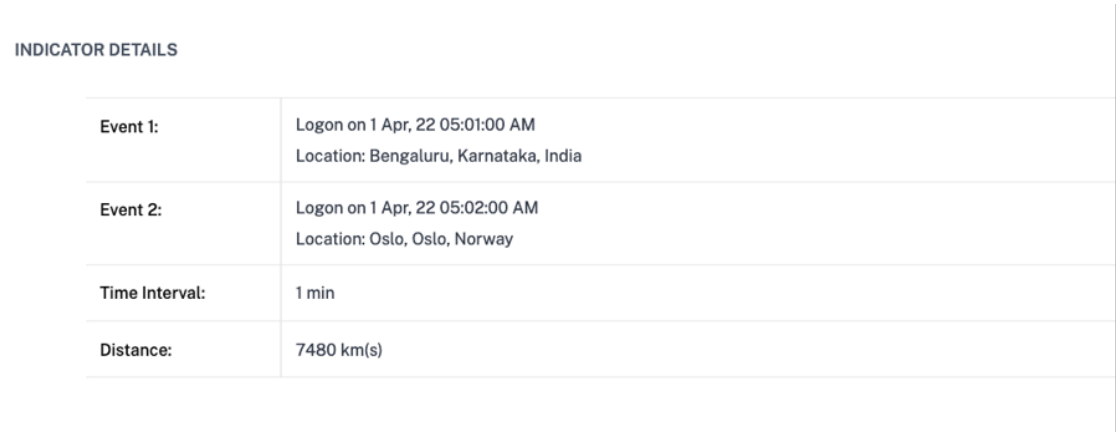
Adam Maxwell のリスクタイムラインを表示するには、[セキュリティ**] > [**ユーザー] を選択します。[危険なユーザー] ペインから、ユーザー Adam Maxwell を選択します。

Adam Maxwell のリスクタイムラインから、あり得ない移動リスク指標を選択します。次の情報を表示できます。

- **WHAT HAPPENED** セクションには、あり得ない移動イベントの概要が記載されています。

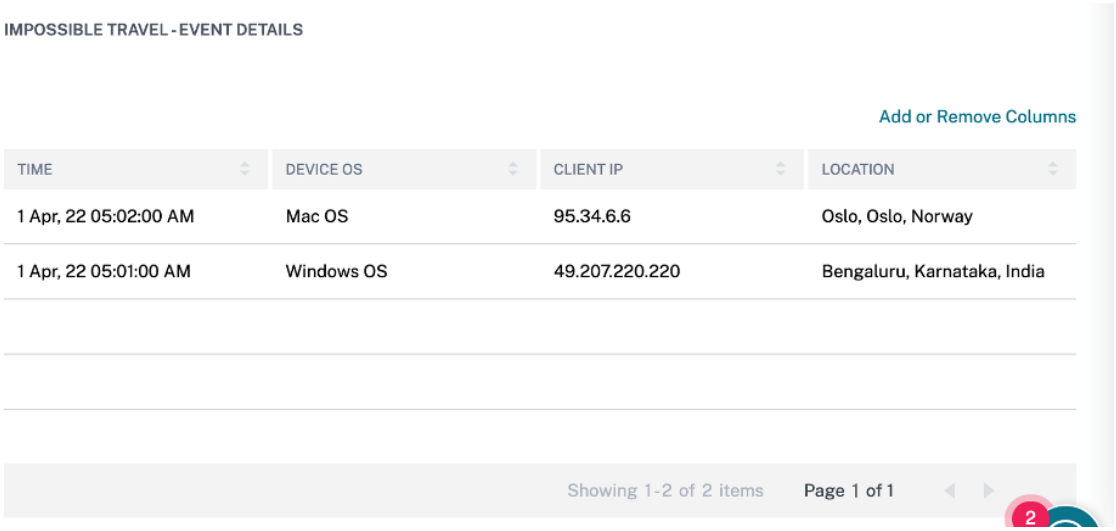


- [INDICATOR **DETAILS**] セクションには、ユーザーがログオンした場所、連続してログオンするまでの時間、および 2 つの場所の間の距離が表示されます。



- [**LOGON LOCATION-LAST 30 DAYS**] セクションには、あり得ない移動場所とユーザーの既知の場所の地理的マップビューが表示されます。過去 30 日間の位置データが表示されます。マップ上のポインターにカーソルを合わせると、各場所からの合計ログオン数が表示されます。

- 「あり得ない移動-イベントの詳細」セクションには、あり得ない移動イベントに関する次の情報が表示されます。
  - 時刻: ログオンの日付と時刻を示します。
  - **Device OS**: ユーザーデバイスのオペレーティングシステムを示します。
  - クライアント **IP**: ユーザーデバイスの IP アドレスを示します。
  - 場所: ユーザーがログオンした場所を示します。



ユーザーに適用できるアクション

ユーザーのアカウントに対して次のアクションを実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントに異常または疑わしいアクティビティがある場合、すべての管理者または選択した管理者に電子メール通知が送信されます。
- ユーザーをログオフします。ユーザーが自分のアカウントからログオフすると、Citrix Gateway 管理者がユーザーのログオフアクションをクリアするまで、Citrix Gateway 経由でリソースにアクセスできません。
- ユーザーのロック：異常な動作のためにユーザーのアカウントがロックされると、Gateway 管理者がアカウントのロックを解除するまで、Citrix Gateway を介してリソースにアクセスできません。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

疑わしい IP からのログオン

Citrix Analytics は、疑わしい IP からのサインインアクティビティに基づいてユーザーアクセスの脅威を検出し、このリスクインジケータをトリガーします。

疑わしい IP からのログオンリスク指標に関連するリスク要因は、IP ベースのリスク指標です。リスク要因について詳しくは、「Citrix ユーザーリスク指標」を参照してください。

［疑わしい **IP** からのログオン］リスク指標はいつトリガーされますか**?**

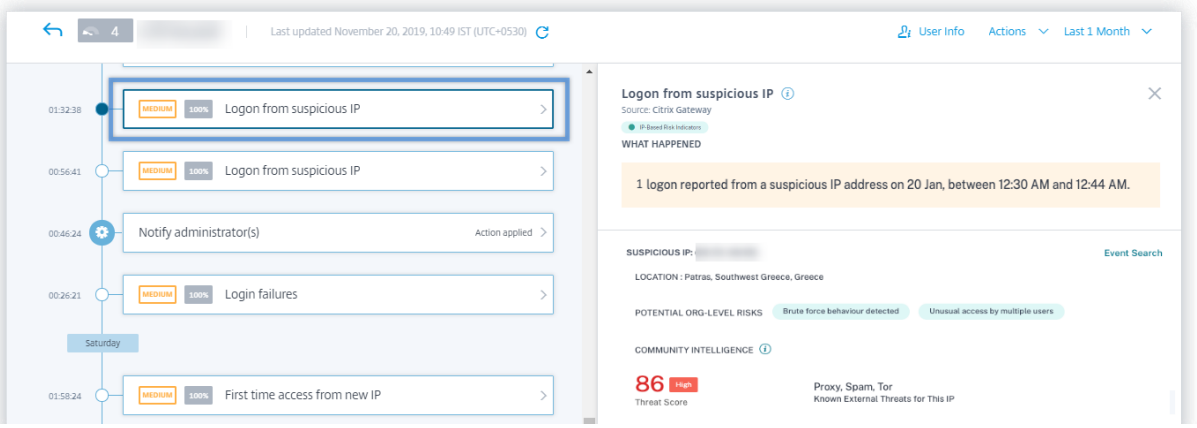
疑わしい **IP** からのログオンのリスクインジケータは、Citrix Analytics が疑わしいと識別する IP アドレスからユーザーがネットワークにアクセスしようとしたときにトリガーされます。IP アドレスは、次のいずれかの条件に基づいて疑わしいと見なされます。

- 外部 IP 脅威インテリジェンスフィードにリストされている
- 異常な場所から複数のユーザーサインインレコードがある
- 過剰なログイン試行が失敗し、ブルートフォース攻撃を示す可能性があります。

Citrix Analytics は、Citrix Gateway から受信したサインインイベントを監視し、ユーザーが疑わしい IP からサインインしているかどうかを検出します。Citrix Analytics が疑わしい IP からのサインイン試行を検出すると、ユーザーのリスクスコアが更新され、ユーザーのリスクタイムラインに「疑わしい **IP** からのログオン」リスク指標エントリが追加されます。

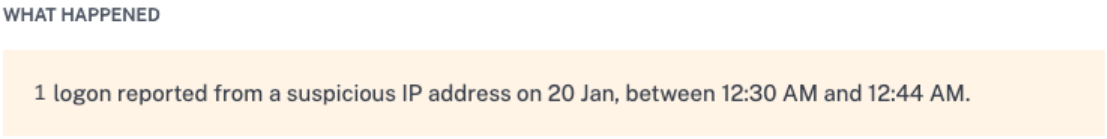
不審な **IP** リスク指標からのログオンを分析するには**?**

Citrix Analytics が疑わしいと識別する IP アドレスからネットワークにアクセスしようとしたユーザー Lemuel を考えてみましょう。Citrix Gateway はサインインイベントを Citrix Analytics に報告し、更新されたリスクスコアを Lemuel に割り当てます。疑わしい **IP** からのログオンのリスク指標が Lemuel Kildow のリスクタイムラインに追加されます。

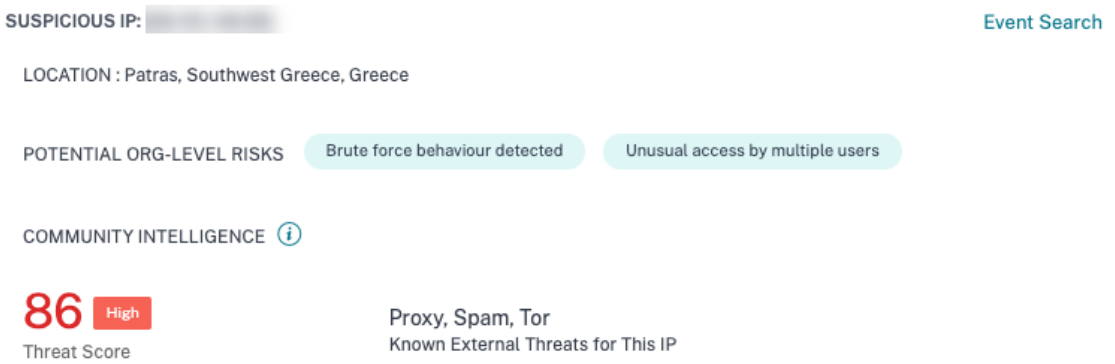


ユーザーについて報告された疑わしい IP からのログオンリスク指標を表示するには、［セキュリティ］ > ［ユーザー］に移動して、ユーザーを選択します。Lemuel Kildow のリスクタイムラインから、ユーザーに報告された疑わしい **IP** リスク指標から最新のログオンを選択できます。タイムライン から疑わしい **IP** リスク指標エントリからログオンを選択すると、対応する詳細情報パネルが右側のペインに表示されます。

- **WHAT HAPPENED** セクションには、疑わしい IP からのログオンリスクインジケータの簡単な概要が表示されます。また、選択した期間中に報告された疑わしい IP アドレスからのサインイン数も含まれます。

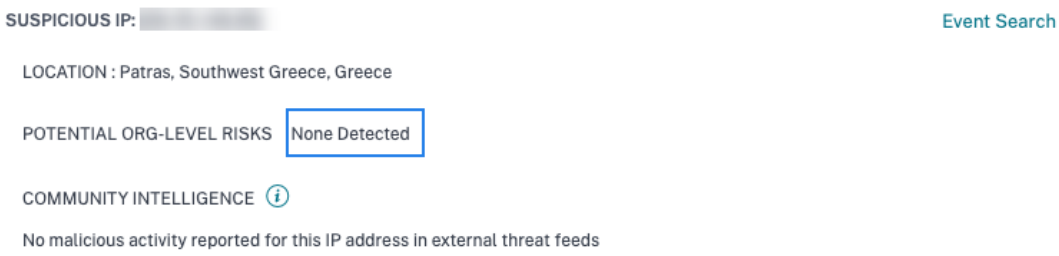


- [疑わしい **IP**] セクションには、次の情報が表示されます。



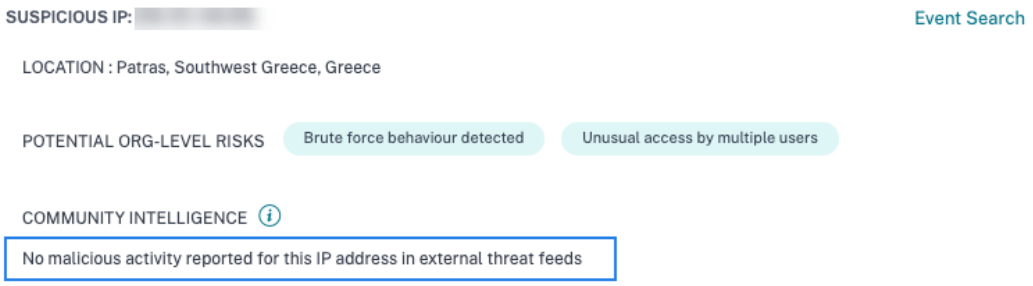
  - 疑わしい **IP** だな疑わしいサインインアクティビティに関連付けられた IP アドレス。
  - 場所。ユーザーの市、地域、国。これらの場所は、データの可用性に基づいて表示されます。
  - 組織レベルのリスクの可能性がある。Citrix Analytics が組織で最近検出した疑わしい IP アクティビティのパターンを示します。危険なパターンには、潜在的な総当たり試行と一貫した過剰なログイン失敗や、複数のユーザーによる異常なアクセスなどがあります。

    組織内の IP アドレスに対して危険なパターンが検出されない場合は、次のメッセージが表示されます。

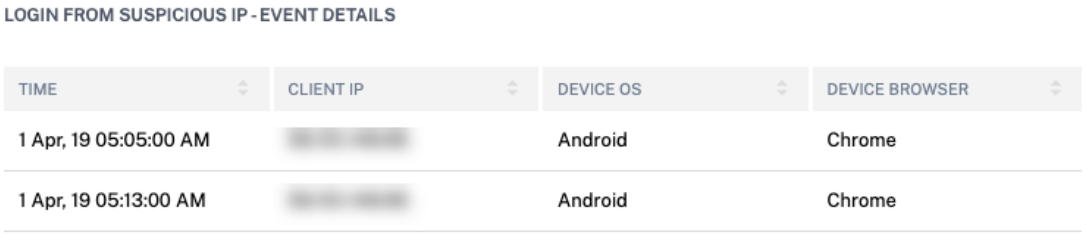


  - コミュニティインテリジェンス。外部 IP 脅威インテリジェンスフィードでハイリスクとして識別される IP アドレスの脅威スコアと脅威カテゴリを提供します。Citrix Analytics では、リスクスコアが高リスクの IP アドレスに割り当てられます。リスクスコアは 80 から始まります。

    外部 IP 脅威インテリジェンスフィードで利用可能な脅威インテリジェンスが IP アドレスにない場合は、次のメッセージが表示されます。



- [**EVENT DETAILS**] セクションには、疑わしいサインインアクティビティに関する次の情報が表示されます。



  - 時間。疑わしいサインインアクティビティの時刻。
  - クライアント **IP**。疑わしいサインインアクティビティに使用されたユーザーのデバイスの IP アドレス。
  - デバイス **OS**。ブラウザのオペレーティングシステム。
  - デバイスブラウザ。疑わしいサインインアクティビティに使用する Web ブラウザ。

ユーザーに適用できるアクション

ユーザーのアカウントでは、次の操作を実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントで異常なアクティビティや疑わしいアクティビティが発生すると、すべての管理者または選択した管理者に電子メール通知が送信されます。
- ユーザーをログオフします。ユーザーが自分のアカウントからログオフすると、Citrix Gateway 管理者がユーザーのログオフアクションをクリアするまで、Citrix Gateway 経由でリソースにアクセスできません。
- ユーザーのロック：異常な動作によってユーザーのアカウントがロックされると、Gateway 管理者がアカウントのロックを解除するまで、Citrix Gateway を介してリソースにアクセスできません。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

疑わしいログオン

> メモ
>
> - このリスク指標は、[異常な場所からのアクセス] リスク指標に代わるものです。
> - 通常とは異なる場所からのアクセス」リスク指標に基づくポリシーは、疑わしいログオンリスク指標に自動的にリンクされます。

Citrix Analytics は、ユーザーが使用するデバイス、場所、ネットワークによって共同で定義される複数のコンテキスト要因に基づいて、異常または危険に見えるユーザーのログオンを検出します。

疑わしいログオンリスクインジケータはいつトリガーされますか?

リスク指標は、次の要因の組み合わせによってトリガーされます。各要因は、1 つまたは複数の条件に基づいて潜在的に疑わしいと見なされます。

要素	条件
異常なデバイス	ユーザーは、過去 30 日間に使用されたデバイスとは異なる署名を持つデバイスからログオンします。デバイスのシグネチャは、デバイスのオペレーティングシステムと使用するブラウザに基づきます。
通常以外の場所	過去 30 日間にユーザーがログオンしていない都市または国からログオンします。 都市または国が、最近の (過去 30 日間) のログオン場所から地理的に離れている。 過去 30 日間に都市または国からログオンしたユーザー数が 0 人または最小です。
異常なネットワーク	ユーザーが過去 30 日間に使用していない IP アドレスからログオンします。 ユーザーが過去 30 日間に使用していない IP サブネットからログオンします。 過去 30 日間にゼロ人または最小のユーザーが IP サブネットからログオンしました。
IP 脅威	IP アドレスは、コミュニティ脅威インテリジェンスフィード（Webroot）によって高リスクとして識別されます。

要素	条件
	Citrix Analytics は最近、他のユーザーの IP アドレスから非常に疑わしいログオンアクティビティを検出しました。

疑わしいログオンリスク指標を分析する方法

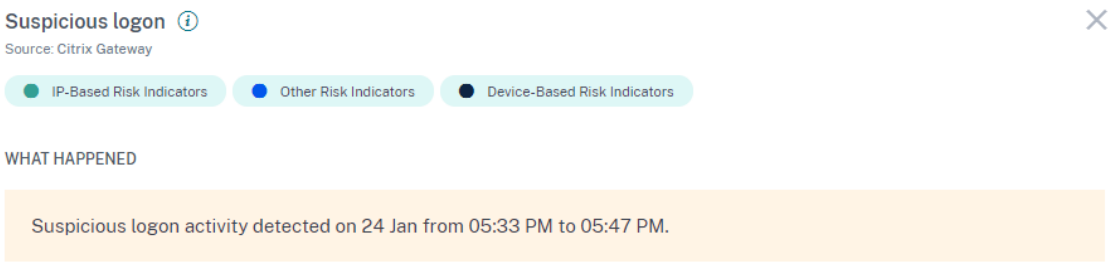
インドのアーンドラ・プラデーシュ州から初めてサインインしたユーザー Adam Maxwell について考えてみましょう。既知の署名を持つデバイスを使用して、組織のリソースにアクセスします。しかし、彼は過去 30 日間使用していないネットワークから接続します。

Citrix Analytics では、場所やネットワークなどの要因が通常の動作から逸脱しているため、このログオンイベントを疑わしいものとして検出し、疑わしいログオンリスク指標をトリガーします。リスク指標は Adam Maxwell のリスクタイムラインに追加され、リスクスコアが彼に割り当てられます。

Adam Maxwell のリスク時間を表示するには、[セキュリティ**] > [**ユーザー] を選択します。[危険なユーザー] ペインから、ユーザー Adam Maxwell を選択します。

Adam Maxwell のリスクタイムラインから、疑わしいログオンリスク指標を選択します。次の情報が表示されます。

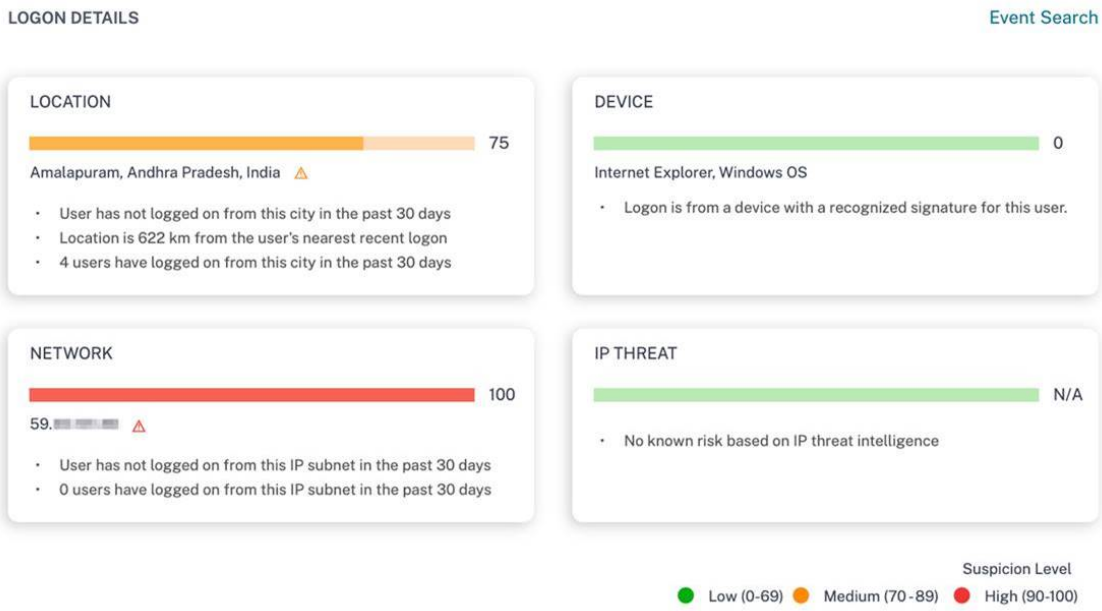
- 「**WHAT** HAPPENED」セクションには、リスク要因やイベントの発生時間など、疑わしいアクティビティの概要が表示されます。



- **[LOGON DETAILS**] セクションには、各リスク要因に対応する疑わしいアクティビティの詳細な概要が表示されます。各リスクファクターには、疑わしいレベルを示すスコアが割り当てられます。単一のリスク要因は、ユーザーからのリスクが高いことを示すものではありません。全体的なリスクは、複数のリスク因子の相関に基づいています。

疑惑レベル	指示
0–69	この要因は正常に見え、疑わしいとは見なされません。
70–89	この要因はわずかに通常とは違うように見え、他の要因では適度に疑わしいと考えられます。

疑惑レベル	指示
90–100	この要因はまったく新しいものまたは通常とは違うものであり、他の要因と非常に疑わしいと考えられています。

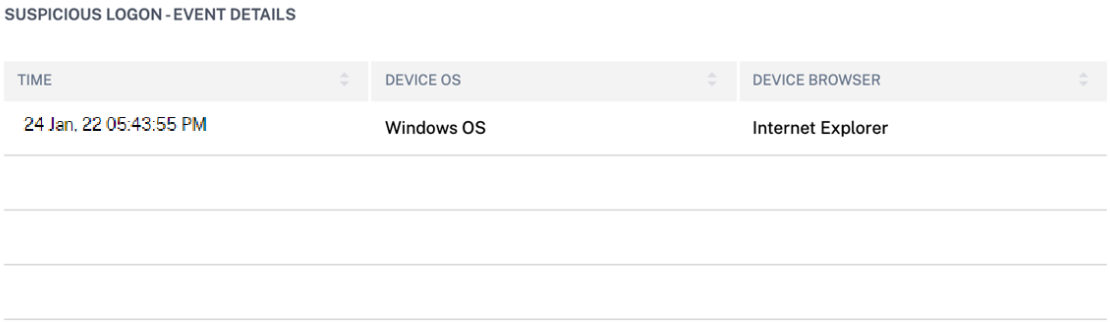


- [ログオン場所-過去 **30** 日間] には、最後に認識された場所とユーザーの現在の場所の地理的なマップビューが表示されます。過去 30 日間の位置データが表示されます。マップ上のポインターにカーソルを合わせると、各場所からの合計ログオン数が表示されます。

- [疑わしいログオン-イベントの詳細] セクションには、疑わしいログオンイベントに関する次の情報が表示さ

れます。

- 時刻: 疑わしいログオンの日付と時刻を示します。
- **Device OS**: ユーザーデバイスのオペレーティングシステムを示します。
- デバイスブラウザ: Citrix Gateway へのサインインに使用する Web ブラウザを示します。



ユーザーに適用できるアクション

ユーザーのアカウントでは、次の操作を実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントで異常なアクティビティや疑わしいアクティビティが発生すると、すべての管理者または選択した管理者に電子メール通知が送信されます。
- ユーザーをログオフします。ユーザーが自分のアカウントからログオフすると、Citrix Gateway 管理者がユーザーのログオフアクションをクリアするまで、Citrix Gateway 経由でリソースにアクセスできません。
- ユーザーのロック: 異常な動作によってユーザーのアカウントがロックされると、Gateway 管理者がアカウントのロックを解除するまで、Citrix Gateway を介してリソースにアクセスできません。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

異常な認証の失敗

Citrix Analytics は、ユーザーが異常な IP アドレスからのログオンに失敗したときにアクセスベースの脅威を検出し、対応するリスク指標をトリガーします。

異常な認証リスク指標に関連するリスク要因は、ログオン失敗ベースのリスク指標です。リスク要因について詳しくは、「Citrix ユーザーリスク指標」を参照してください。

異常な認証失敗インジケータはいつトリガーされますか

組織内のユーザーが通常の動作に反する異常な IP アドレスからのログオンに失敗した場合、通知を受け取ることができます。

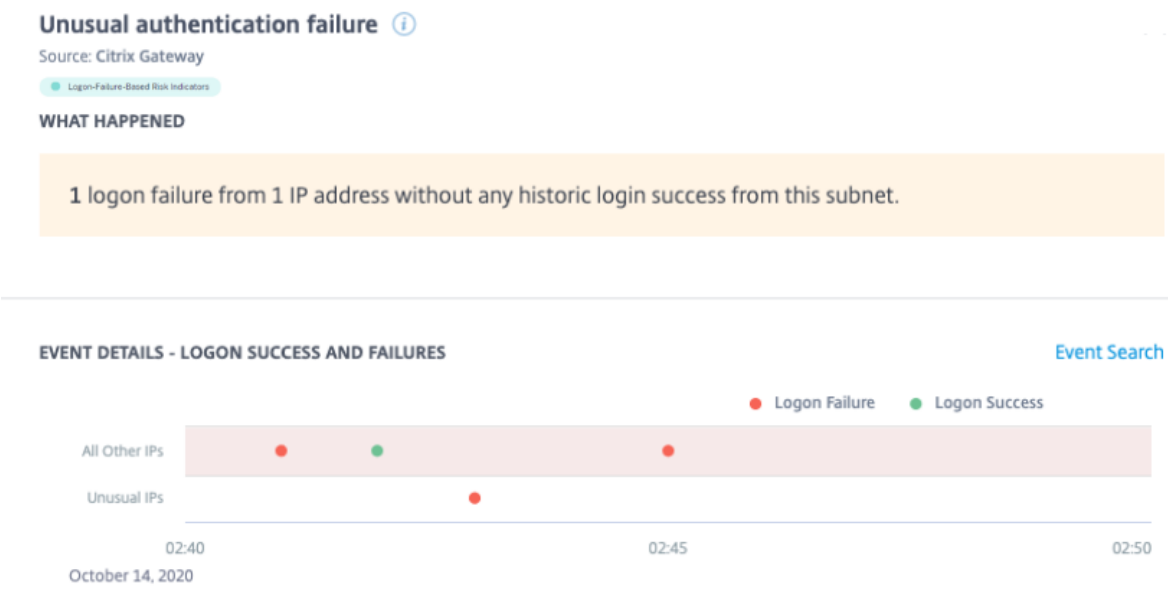
Citrix Gateway はこれらのイベントを検出し、Citrix Analytics に報告します。Citrix Analytics はイベントを受信し、ユーザーのリスクスコアを上げます。異常な認証失敗リスクインジケータがユーザーのリスクタイムラインに追加されます。

異常な認証失敗インジケーターを分析する方法は

通常のホームネットワークやオフィスネットワークから Citrix Gateway に定期的にサインインしているユーザー Georgina Kalou を考えてみましょう。リモートの攻撃者が異なるパスワードを推測して Georgina のアカウントを認証しようとすると、不慣れなネットワークからの認証に失敗します。

このシナリオでは、Citrix Gateway はこれらのイベントを Citrix Analytics に報告し、Citrix Analytics は更新されたリスクスコアを Georgina Kalou に割り当てます。異常な認証失敗リスク指標は Georgina Kalou のリスクタイムラインに追加されます。

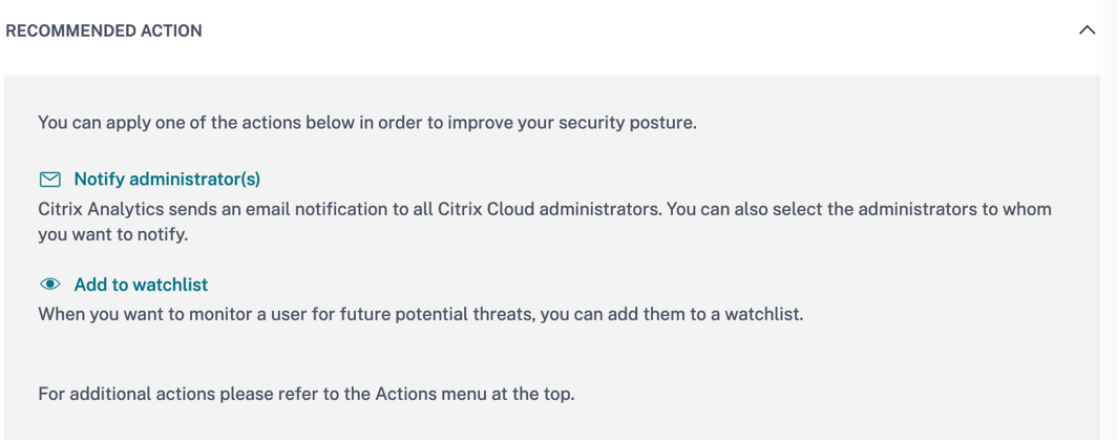
Georgina Kalou のリスクタイムラインから、報告された異常な認証失敗リスク指標を選択できます。イベントの理由が、イベントの時間や場所などの詳細とともに表示されます。



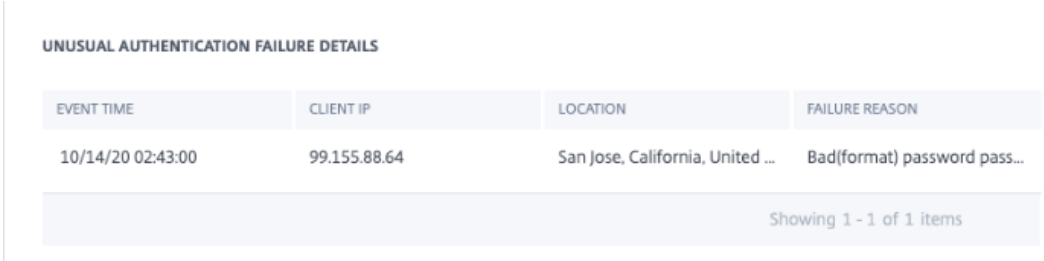
- [**WHAT** HAPPENED] セクションでは、認証失敗の総数とイベントの時刻を含む簡単なサマリーを表示できます。

- [推奨アクション] セクションには、リスク指標に適用できる推奨アクションが表示されます。Citrix Analytics for Security では、ユーザーがもたらすリスクの重大度に応じてアクションを推奨します。推奨されるアクションは、次のアクションの 1 つまたは組み合わせです。
  - 管理者に通知
  - ウォッチリストに追加
  - ポリシーを作成する

  レコメンデーションに基づいてアクションを選択できます。または、「アクション」(Actions) メニューの選択内容に応じて、適用するアクションを選択することもできます。詳細については、「アクションを手動で適用する」を参照してください。

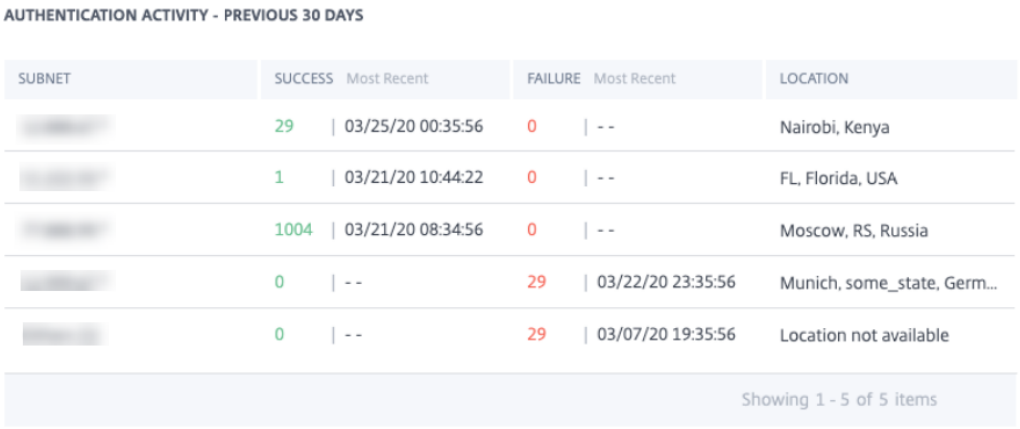


- [**EVENT DETAILS** —**LOGON SUCCESS and** Failures] セクションでは、異常な認証失敗と、同じ期間中に検出されたその他のログオンアクティビティを示すグラフを表示できます。
- [異常な認証の詳細] セクションのテーブルには、異常な認証失敗に関する次の情報が表示されます。
  - ログオン時刻—イベントの日時
  - クライアント **IP** —ユーザーデバイスの IP アドレス
  - ロケーション—イベントが発生したロケーションです。
  - 失敗理由—認証失敗の理由



- [ユーザー認証アクティビティ-前の **30** 日間] セクションでは、この表には、ユーザーの過去 30 日間の認証アクティビティに関する次の情報が表示されます。

- サブネット—ユーザーネットワークの IP アドレス。
- [Success]：ユーザの成功した認証イベントの合計数と、最後に成功したイベントの時刻。
- [Failure]：失敗した認証イベントの総数と、ユーザの直近の失敗イベントの時刻。
- Location —認証イベントが発生した場所。



ユーザーに適用できるアクション

ユーザーのアカウントでは、次の操作を実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントで異常なアクティビティや疑わしいアクティビティが発生すると、すべての管理者または選択した管理者に電子メール通知が送信されます。
- ユーザーをログオフします。ユーザーが自分のアカウントからログオフすると、Citrix Gateway 管理者がユーザーのログオフアクションをクリアするまで、Citrix Gateway 経由でリソースにアクセスできません。
- ユーザーのロック：異常な動作によってユーザーのアカウントがロックされると、Gateway 管理者がアカウントのロックを解除するまで、Citrix Gateway を介してリソースにアクセスできません。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

Citrix Secure Private Access リスク指標

April 12, 2024

危険なウェブサイトへのアクセス

> 注:
> セキュア・プライベート・アクセスによるカテゴリベースの Web フィルタリングの廃止により、Citrix Analytics for Security の以下の機能が影響を受けます。
>
> 1. カテゴリグループ、カテゴリ、URL のレピュテーションなどのデータフィールドは、Citrix Analytics for Security ダッシュボードでは使用できなくなりました。
> 2. 同じデータに依存する危険な Web サイトアクセスインジケーターも廃止され、お客様には表示されなくなりました。
> 3. データフィールド（カテゴリグループ、カテゴリ、URL の評価）とそれに関連するポリシーを使用する既存のカスタムリスク指標は、もうトリガーされません。

セキュア・プライベート・アクセスからの廃止の詳細については、「機能の非推奨」を参照してください。

ブラックリストに載っている **URL** にアクセスしようとしました

Citrix Analytics は、ユーザーがアクセスしたブラックリストに登録された URL に基づいてデータアクセスの脅威を検出し、対応するリスク指標をトリガーします。

［ブラックリスト **URL** へのアクセスの試み］リスク指標は、［セキュアプライベートアクセス］で構成されたブラックリストに登録された URL にユーザーがアクセスしようとすると、Citrix Analytics で報告されます。

ブラックリスト **URL** にアクセスしようとするリスク指標に関連するリスク要因は、その他のリスク指標です。リスク要因について詳しくは、「Citrix ユーザーリスク指標」を参照してください。

ブラックリストに登録された **URL** リスク指標へのアクセスの試みがトリガーされるのはいつですか**?**

Secure Private Access には、ブラックリストに登録された URL へのアクセスを制限するポリシーベースの制御を提供する URL 分類機能が含まれています。ユーザーがブラックリストに登録された URL にアクセスしようとすると、セキュアプライベートアクセスはこのイベントを Citrix Analytics に報告します。Citrix Analytics では、ユーザーのリスクスコアが更新され、ユーザーのリスクタイムラインにブラックリストに登録された **URL** リスク指標へのアクセス試行エントリが追加されます。

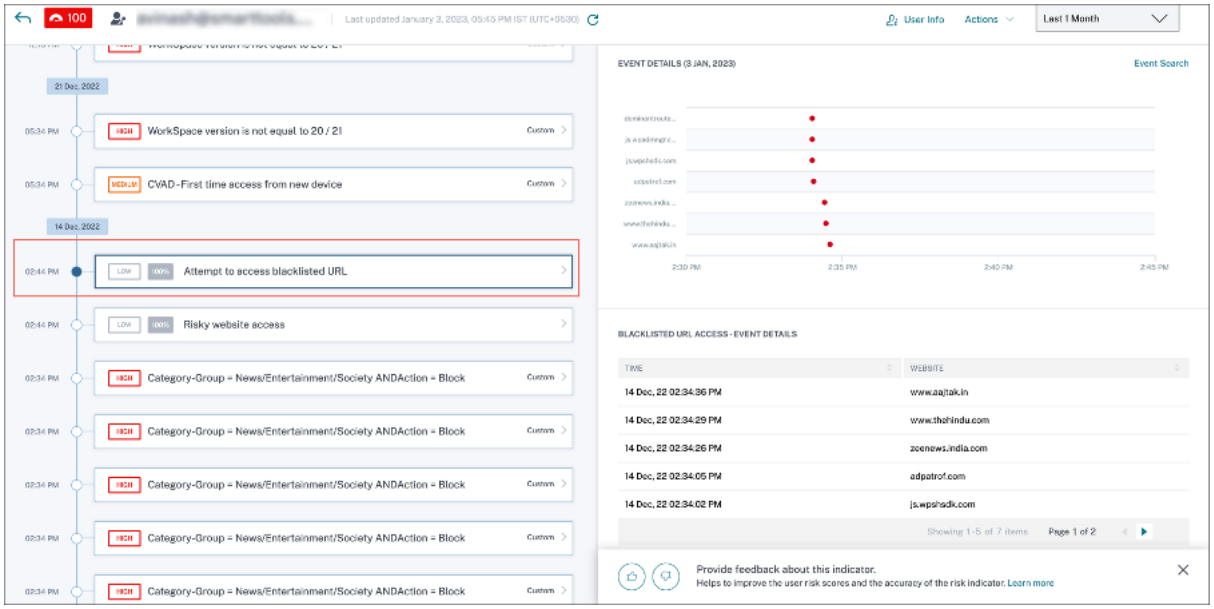
ブラックリストに登録された **URL** リスク指標へのアクセスの試みを分析する方法は

ユーザー Georgina Kalou が、セキュア・プライベート・アクセスで構成されたブラックリストに登録された URL にアクセスしたとします。セキュアプライベートアクセスはこのイベントを Citrix Analytics に報告し、更新されたリスクスコアを Georgina Kalou に割り当てます。ブラックリストに登録された **URL** にアクセスしようとするリスク指標が Georgina Kalou のリスクタイムラインに追加されます。

Georgina Kalou のリスクタイムラインから、報告された「ブラックリスト **URL** へのアクセス試み」リスク指標を選択できます。イベントの理由は、イベントの時間、Web サイトの詳細など、イベントの詳細とともに表示されます。

ユーザの **[**ブラックリストへのアクセスの試行] エントリを表示するには、[セキュリティ **] > [**ユーザ] に移動し、ユーザを選択します。

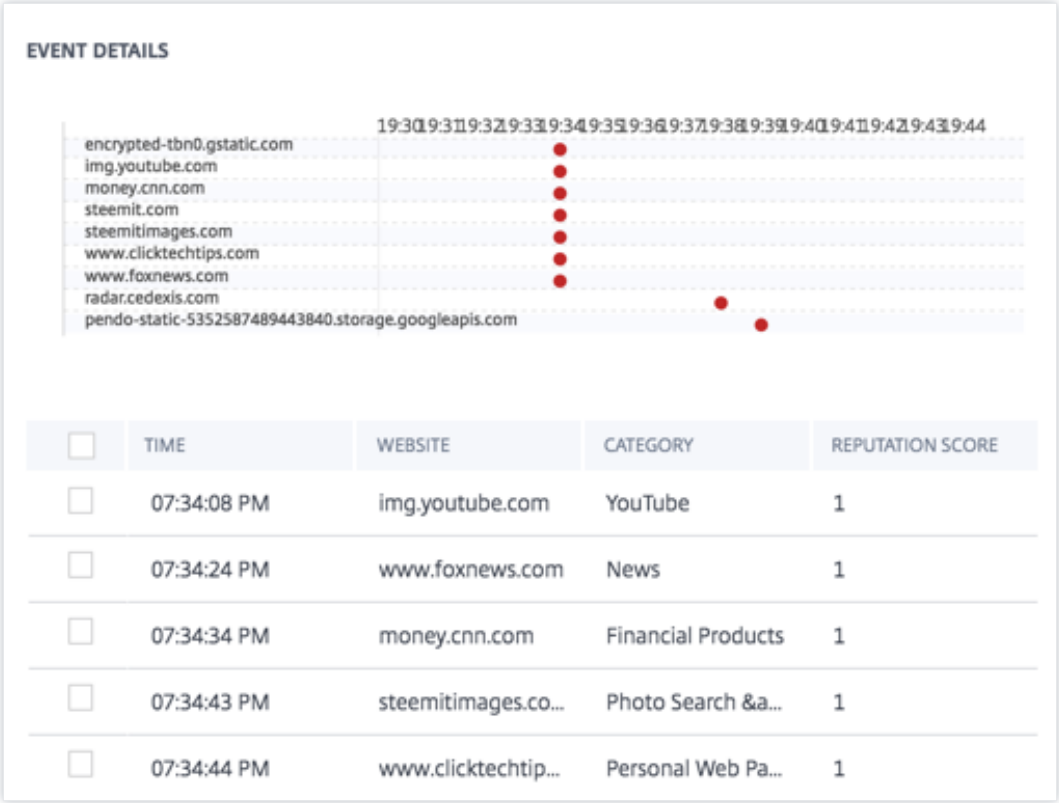
タイムラインから [ブラックリストに載った **URL** リスク指標へのアクセスを試みる] エントリを選択すると、対応する詳細情報パネルが右側のペインに表示されます。



- **WHAT HAPPENED** セクションには、リスク指標の簡単な概要が表示されます。これには、選択した期間中にユーザーがアクセスしたブラックリストに登録された URL の詳細が含まれます。

- [**EVENT DETAILS**] セクションには、選択した期間中に発生した個々のイベントのタイムラインビジュアライゼーションが含まれます。また、各イベントに関する次の重要な情報も表示できます。

- 時間。イベントが発生した時刻。
- ウェブサイト。ユーザーがアクセスする危険な Web サイト。
- カテゴリ。ブラックリストに登録された URL の [セキュアプライベートアクセス] で指定されたカテゴリ。
- 評判評価。ブラックリストに登録された URL について、セキュアプライベートアクセスによって返されるレピュテーション評価。詳細については、URL レピュテーションスコアを参照してください。



ユーザーに適用できるアクション

ユーザーのアカウントでは、次の操作を実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントで異常なアクティビティや疑わしいアクティビティが発生すると、すべての管理者または選択した管理者に電子メール通知が送信されます。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

異常なアップロードボリューム

Citrix Analytics は、異常なアップロードボリュームアクティビティに基づいてデータアクセスの脅威を検出し、対応するリスク指標をトリガーします。

異常なアップロードボリュームリスク指標は、ユーザーがアプリケーションまたは Web サイトに過剰量のデータをアップロードしたときに報告されます。

異常なアップロードボリュームのリスク指標に関連するリスク要因は、その他のリスク指標です。リスク要因について詳しくは、「Citrix ユーザーリスク指標」を参照してください。

異常なアップロードボリュームリスク指標はいつトリガーされますか?

Secure Private Access を構成して、アクセスした悪意のある、危険な、または不明な Web サイト、消費された帯域幅、危険なダウンロードやアップロードなどのユーザーアクティビティを監視できます。組織内のユーザーがアプリケーションまたは Web サイトにデータをアップロードすると、Secure Private Access はこれらのイベントを Citrix Analytics に報告します。

Citrix Analytics これらすべてのイベントを監視し、このユーザーアクティビティがユーザーの通常の行動に反していると判断した場合、ユーザーのリスクスコアを更新します。異常なアップロードボリュームリスク指標がユーザーのリスクタイムラインに追加されます。

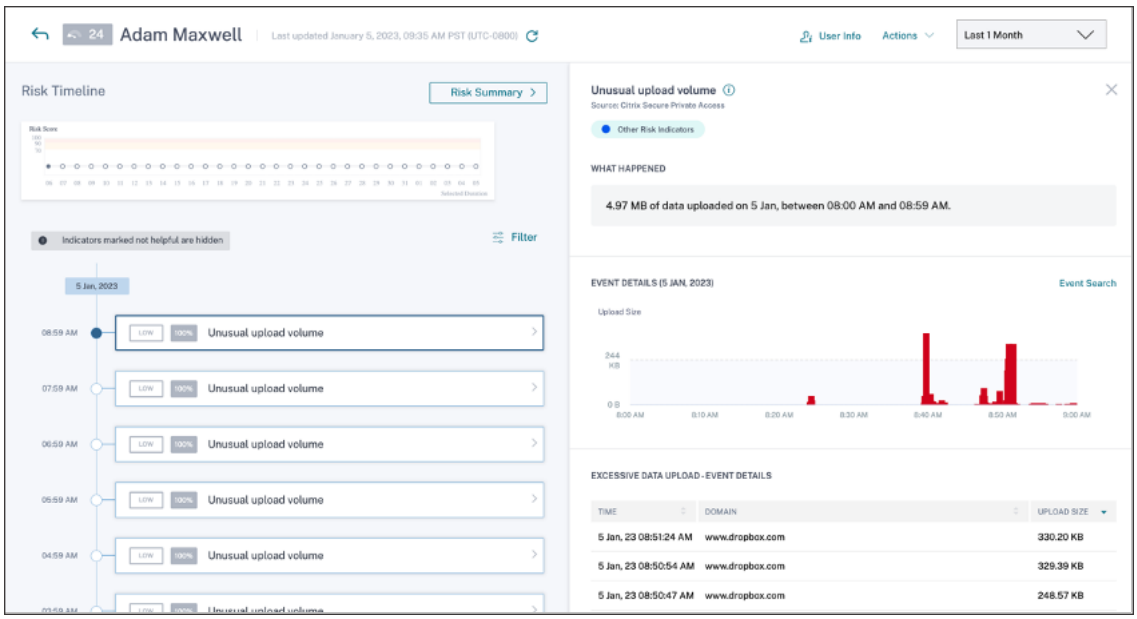
異常なアップロードボリュームのリスク指標を分析するには?

アプリケーションやウェブサイトに過剰な量のデータをアップロードしたユーザー Adam Maxwell を考えてみましょう。セキュアプライベートアクセスはこれらのイベントを Citrix Analytics に報告し、更新されたリスクスコアを Adam Maxwell に割り当てます。異常なアップロードボリュームリスク指標が Adam Maxwell のリスクタイムラインに追加されます。

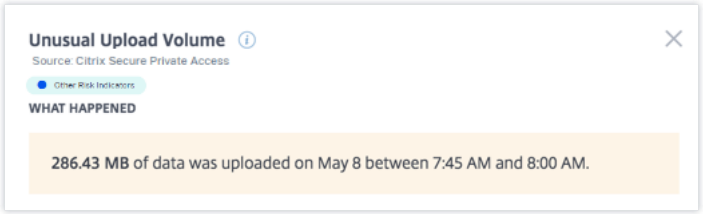
Adam Maxwell のリスクタイムラインから、報告された異常なアップロードボリュームリスク指標を選択できます。イベントの理由は、イベントの時間やドメインなど、イベントの詳細とともに表示されます。

異常なアップロードボリュームリスク指標を表示するには、[セキュリティ] **>** [ユーザー] に移動し、ユーザーを選択します。

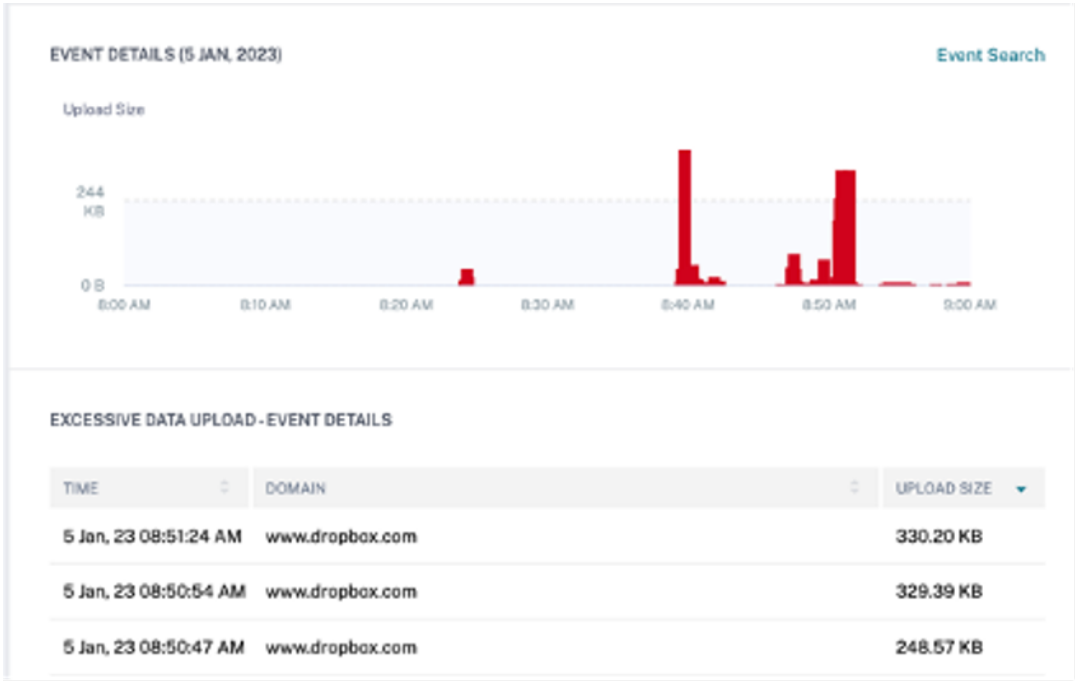
タイムラインから [異常なアップロードボリュームのリスクインジケータ] エントリを選択すると、対応する詳細情報パネルが右側のペインに表示されます。



- **WHAT HAPPENED** セクションには、選択した期間中にアップロードされたデータの量など、リスク指標の簡単な概要が表示されます。



- [**EVENT DETAILS**] セクションには、選択した期間中に発生した個々のデータアップロードイベントのタイムラインビジュアライゼーションが含まれます。また、各イベントに関する次の重要な情報も表示できます。
  - 時間。過剰なデータがアプリケーションまたは Web サイトにアップロードされた時刻。
  - ドメイン。ユーザーがデータをアップロードしたドメイン。
  - アップロードサイズ。ドメインにアップロードされたデータの量。



ユーザーに適用できるアクション

ユーザーのアカウントでは、次の操作を実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントで異常なアクティビティや疑わしいアクティビティが発生すると、すべての管理者または選択した管理者に電子メール通知が送信されます。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

過剰なデータのダウンロード

Citrix Analytics は、ネットワーク内のユーザーがダウンロードした過剰なデータに基づいてデータアクセスの脅威を検出し、対応するリスク指標をトリガーします。

リスク指標は、組織内のユーザーがアプリケーションまたは Web サイトから過剰な量のデータをダウンロードしたときに報告されます。

過剰なデータダウンロードリスク指標はいつトリガーされますか?

Secure Private Access を構成して、アクセスした悪意のある、危険な、または不明な Web サイト、消費された帯域幅、危険なダウンロードやアップロードなどのユーザーアクティビティを監視できます。組織内のユーザーがアプリケーションまたは Web サイトからデータをダウンロードすると、Secure Private Access はこれらのイベントを Citrix Analytics に報告します。

Citrix Analytics は、これらすべてのイベントを監視し、ユーザーアクティビティがユーザーの通常の行動に反していると判断した場合、ユーザーのリスクスコアを更新します。過剰データのダウンロードリスク指標がユーザーのリスクタイムラインに追加されます。

過剰なデータダウンロードのリスク指標に関連するリスク要因は、その他のリスク指標です。リスク要因について詳しくは、「Citrix ユーザーリスク指標」を参照してください。

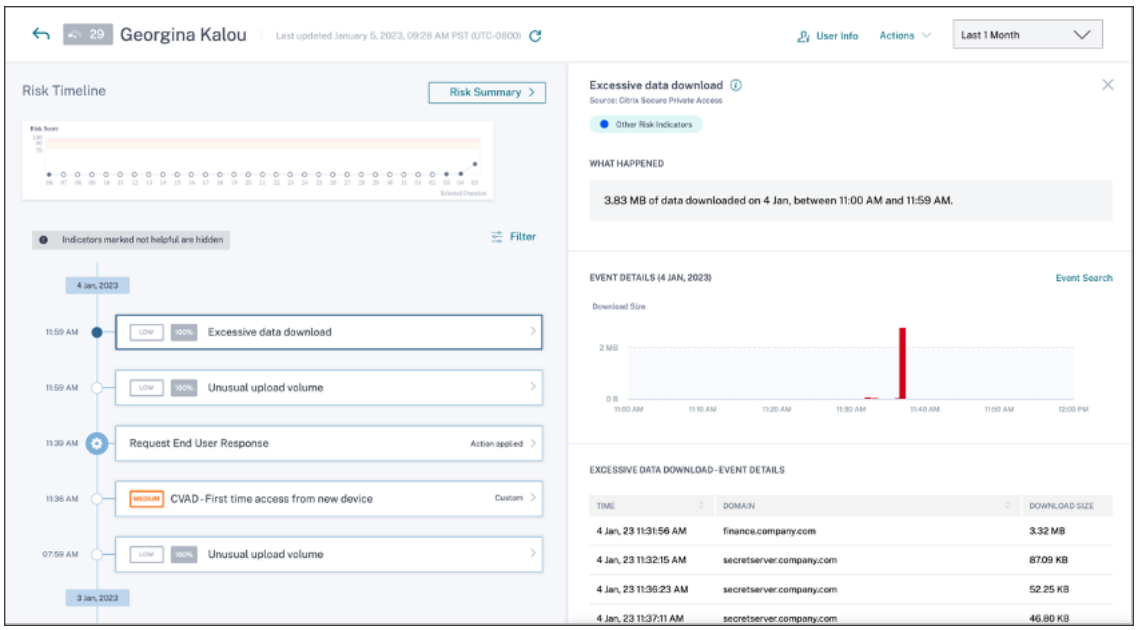
過剰なデータダウンロードのリスク指標を分析する方法は

ユーザー「Georgina Kalou」を考えてみましょう。Gergina はアプリケーションや Web サイトから過剰な量のデータをダウンロードしました。Secure Private Access はこれらのイベントを Citrix Analytics に報告し、更新されたリスクスコアを Georgina Kalou に割り当て、ユーザーのリスクタイムラインに過剰なデータダウンロードリスク指標エントリを追加します。

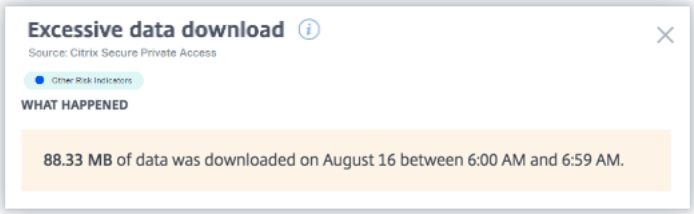
Georgina Kalou のリスクタイムラインから、報告された過剰データのダウンロードリスク指標を選択できます。イベントの理由は、時間やドメインの詳細など、イベントの詳細とともに表示されます。

[過剰なデータダウンロード**]** リスク指標を表示するには、**[**セキュリティ**] > [**ユーザー**]** に移動して、ユーザーを選択します。

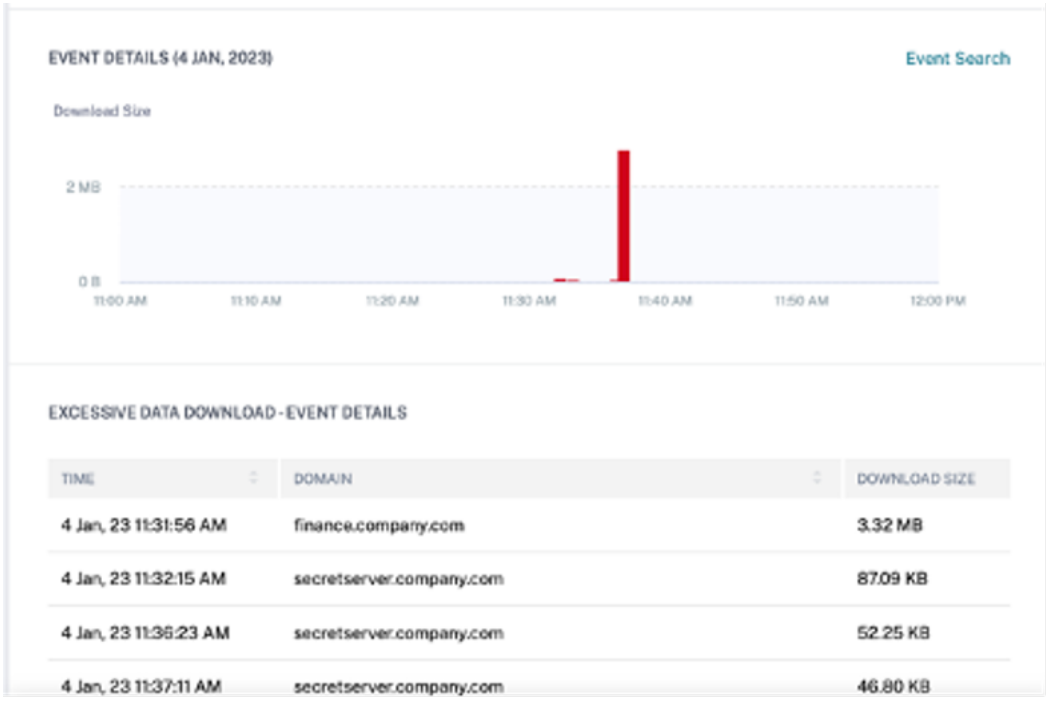
タイムラインから [過剰なデータのダウンロードリスクインジケータ] エントリを選択すると、対応する詳細情報パネルが右側のペインに表示されます。



- **WHAT HAPPENED** セクションには、選択した期間中にダウンロードされたアップロードされたデータの量など、リスク指標の簡単な概要が表示されます。



- [**EVENT DETAILS**] セクションには、選択した期間中に発生した個々のデータダウンロードイベントのタイムラインビジュアライゼーションが含まれます。また、各イベントに関する次の重要な情報も表示できます。
  - 時間。過剰なデータがアプリケーションまたは Web サイトにダウンロードされた時刻。
  - ドメイン。ユーザーがデータをダウンロードしたドメイン。
  - ダウンロードサイズ。ドメインにダウンロードされたデータの量。



ユーザーに適用できるアクション

ユーザーのアカウントでは、次の操作を実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントで異常なアクティビティや疑わしいアクティビティが発生すると、すべての管理者または選択した管理者に電子メール通知が送信されます。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

Citrix Virtual Apps and Desktops および Citrix DaaS リスク指標

July 15, 2022

あり得ない移動

Citrix Analytics は、2 つの異なる国からの連続したログオンが、国間の予想される移動時間よりも短い期間内に行われた場合、ユーザーのログオンが危険であると検出します。

あり得ない移動時間のシナリオは、次のリスクを示しています。

- 侵害された認証情報: リモートの攻撃者が正当なユーザーの資格情報を盗みます。
- 共有認証情報: 異なるユーザーが同じユーザー資格情報を使用しています。

あり得ない移動リスク指標はいつトリガーされますか

あり得ない移動リスク指標は、連続するユーザーログオンの各ペア間の時間と推定距離を評価し、その距離が個々の人がその時間内に移動できるよりも長い場合にトリガーされます。

> 注:
>
> このリスク指標には、ユーザーの実際の場所を反映していない次のシナリオの誤検知アラートを減らすためのロジックも含まれています。
>
> - ユーザーがプロキシ接続から仮想アプリケーションとデスクトップにログオンしたとき。
> - ユーザーがホストされているクライアントから仮想アプリケーションとデスクトップにログオンしたとき。

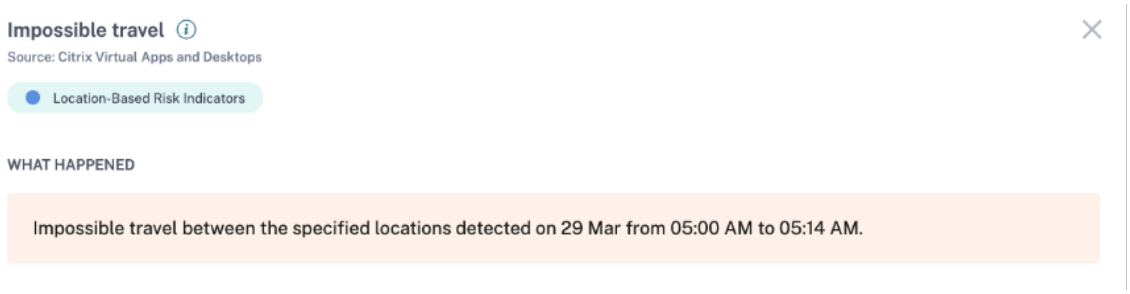
インポッシブルリスク指標の分析方法

ユーザー Adam Maxwell について考えてみましょう。Adam Maxwell は、ロシアのモスクワと中国のフフホトの 2 つの場所から 1 分以内にログオンします。Citrix Analytics は、このログオンイベントをあり得ない移動シナリオとして検出し、あり得ない移動リスク指標をトリガーします。リスク指標が Adam Maxwell のリスクタイムラインに追加され、リスクスコアが Adam Maxwell に割り当てられます。

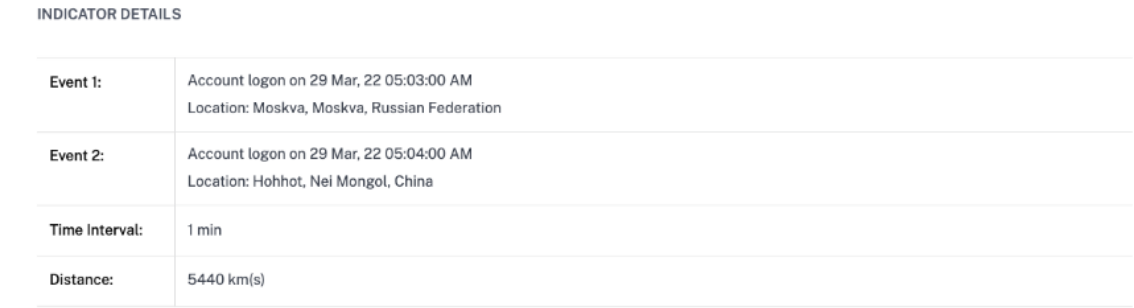
Adam Maxwell のリスクタイムラインを表示するには、[セキュリティ**] > [**ユーザー] を選択します。[危険なユーザー] ペインから、ユーザー Adam Maxwell を選択します。

Adam Maxwell のリスクタイムラインから、あり得ない移動リスク指標を選択します。次の情報を表示できます。

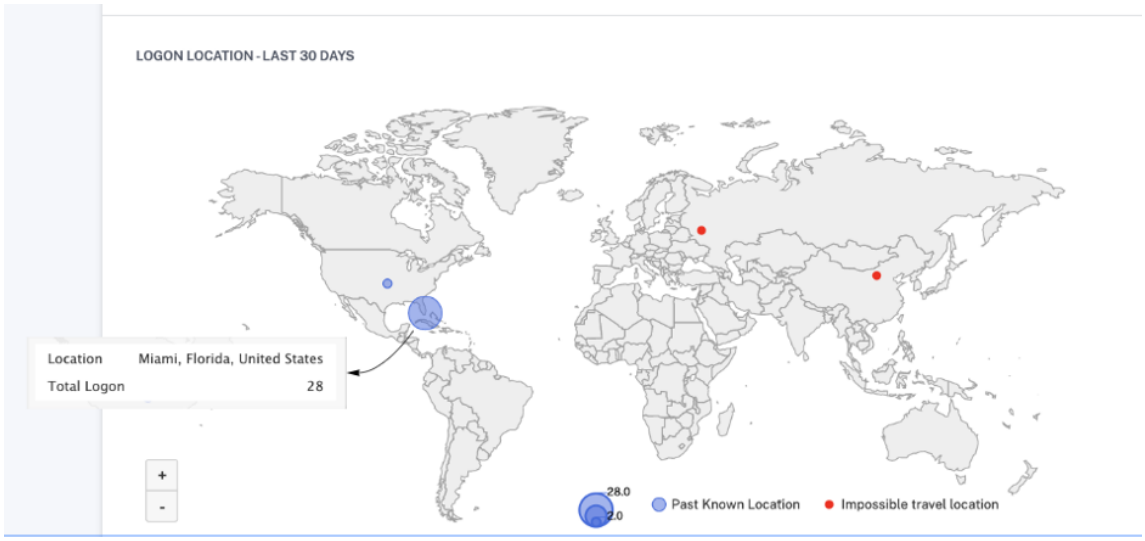
- **WHAT HAPPENED** セクションには、あり得ない移動イベントの概要が記載されています。



- [INDICATOR **DETAILS**] セクションには、ユーザーがログオンした場所、連続してログオンするまでの時間、および 2 つの場所の間の距離が表示されます。



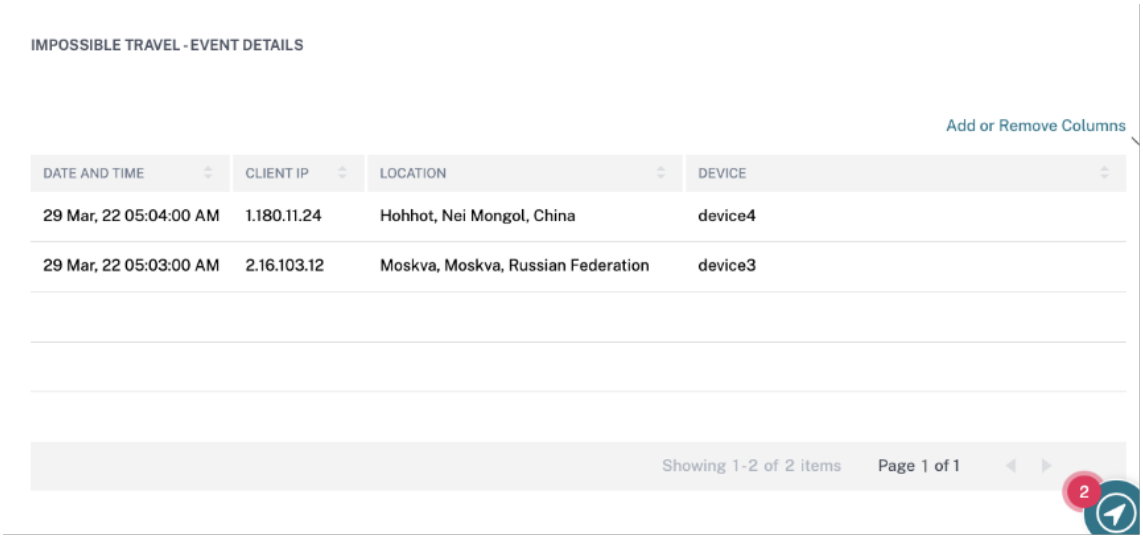
- [**LOGON LOCATION-LAST 30 DAYS**] セクションには、あり得ない移動場所とユーザーの既知の場所の地理的マップビューが表示されます。過去 30 日間の位置データが表示されます。マップ上のポインターにカーソルを合わせると、各場所からの合計ログオン数が表示されます。



- 「あり得ない移動-イベントの詳細」セクションには、あり得ない移動イベントに関する次の情報が表示されます。

  - 日時: ログオンの日付と時刻を示します。
  - クライアント **IP**: ユーザーデバイスの IP アドレスを示します。
  - 場所: ユーザーがログオンした場所を示します。
  - デバイス: ユーザーのデバイス名を示します。
  - ログオンの種類: ユーザーアクティビティがセッションログオンかアカウントログオンかを示します。アカウントログオンイベントは、ユーザーのアカウントへの認証が成功するとトリガーされます。一方、セッションログオンイベントは、ユーザーが資格情報を入力してアプリまたはデスクトップセッションにログオンしたときにトリガーされます。
  - **OS**: ユーザーデバイスのオペレーティングシステムを示します。

– ブラウザ: アプリケーションへのアクセスに使用される Web ブラウザを示します。



ユーザーに適用できるアクションは何ですか

ユーザーのアカウントに対して次のアクションを実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントに異常または疑わしいアクティビティがある場合、すべての管理者または選択した管理者に電子メール通知が送信されます。
- ユーザーをログオフします。ユーザーが自分のアカウントからログオフすると、Virtual Desktops を介してリソースにアクセスできなくなります。
- セッションの記録を開始します。ユーザーの Virtual Desktops アカウントに異常なイベントが発生した場合、管理者は今後のログオンセッションにおけるユーザーのアクティビティの記録を開始できます。ただし、ユーザーが Citrix Virtual Apps and Desktops 7.18 以降を使用している場合、管理者はユーザーの現在のログオンセッションの記録を動的に開始および停止できます。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

データ流出の可能性

Citrix Analytics は、データ漏洩の過度の試みに基づいてデータの脅威を検出し、対応するリスク指標をトリガーします。

潜在的なデータ漏洩リスク指標に関連するリスク要因は、データベースのリスク指標です。リスク要因について詳しくは、「Citrix ユーザーリスク指標」を参照してください。

潜在的なデータ漏洩リスク指標は、Citrix Receiver ユーザーがドライブまたはプリンターにファイルをダウンロードまたは転送しようとしたときにトリガーされます。このデータは、ローカルドライブ、マップされたドライブ、または外部ストレージデバイスへのファイルのダウンロードなど、ファイルのダウンロードイベントである可能性があります。データは、クリップボードを使用するか、コピーと貼り付けの操作によっても引き出すことができます。

> 注
>
> クリップボード操作は、SaaS アプリケーションでのみサポートされています。

潜在的なデータ漏洩リスク指標はいつトリガーされますか?

ユーザーが一定期間内にドライブまたはプリンタに過剰な数のファイルを転送した場合に通知を受け取ることができます。このリスク指標は、ユーザーがローカルコンピューターでコピー/貼り付け操作を使用したときにもトリガーされます。

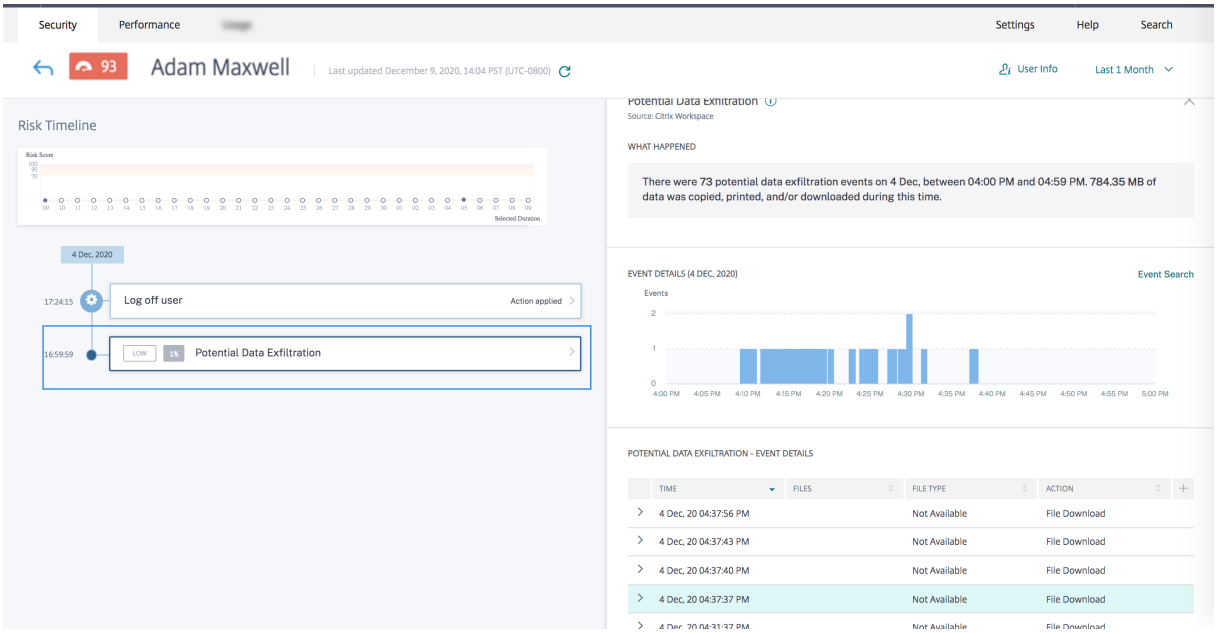
Citrix Receiver がこの動作を検出すると、Citrix Analytics はこのイベントを受け取り、各ユーザーにリスクスコアを割り当てます。潜在データ漏出リスク指標がユーザーのリスクタイムラインに追加されます。

潜在的なデータ流出リスク指標を分析する方法は

セッションにログオンし、事前定義された制限を超えるファイルを印刷しようとするユーザー Adam Maxwell を考えてみましょう。このアクションにより、Adam Maxwell は、機械学習アルゴリズムに基づく通常のファイル転送動作を超えていました。

Adam Maxwell のタイムラインから、潜在的なデータの流出リスク指標を選択できます。イベントの理由は、転送されたファイルやファイルの転送に使用されたデバイスなどの詳細とともに表示されます。

ユーザーについて報告された潜在的なデータ漏洩リスク指標を表示するには、[セキュリティ] **>** [ユーザー] に移動し、ユーザーを選択します。

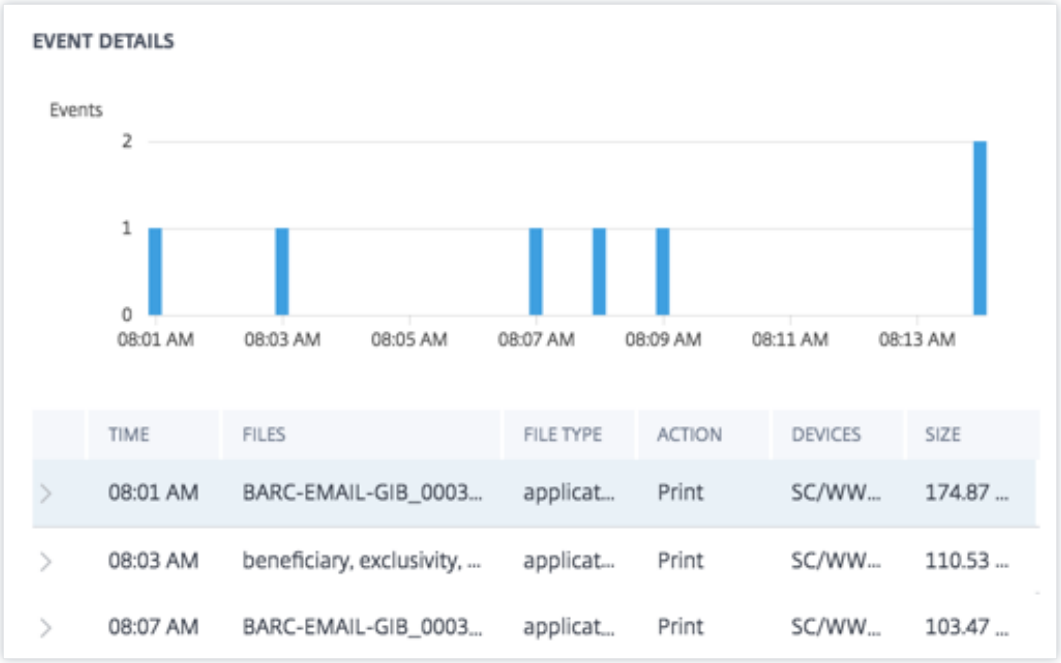


- **WHAT HAPPENESED** セクションでは、潜在的なデータ漏洩イベントの概要を表示できます。特定の期間におけるデータ漏洩イベントの数を表示できます。

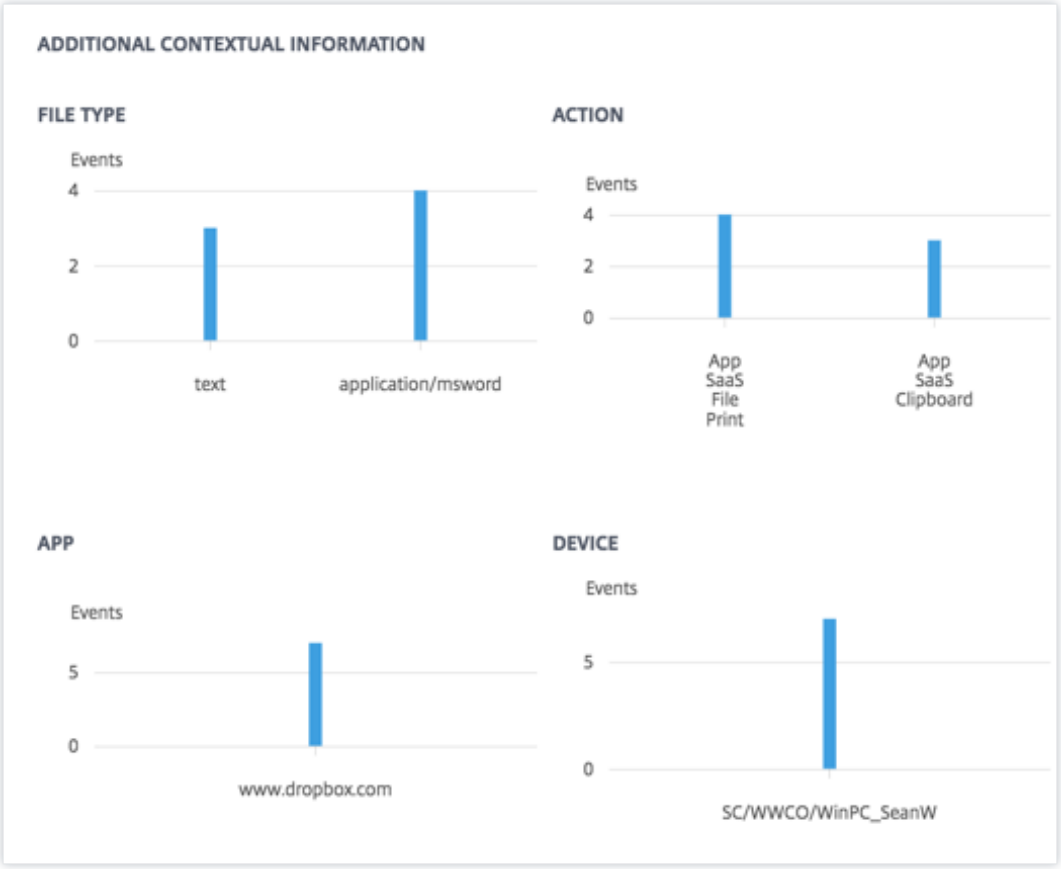
- [**EVENT DETAILS**] セクションでは、データ漏出の試行がグラフおよび表形式で表示されます。イベントはグラフに個別のエントリとして表示され、表には次の重要な情報が表示されます。
  - 時間。データ流出イベントが発生した時刻。
  - **[**ファイル**]**。ダウンロード、印刷、またはコピーされたファイル。
  - ファイルタイプ。ダウンロード、印刷、またはコピーされたファイルの種類。

    > 注
    >
    > 印刷されたファイル名は、SaaS アプリの印刷イベントからのみ使用できます。

  - 操作。実行されたデータ漏洩イベントの種類（印刷、ダウンロード、コピー）。
  - デバイス。使用したデバイス。
  - **[**サイズ**]**。流出されるファイルのサイズ。
  - 場所。ユーザーがデータを取り出そうとしている都市。



- 「追加のコンテキスト情報」セクションでは、イベントの発生中に、次の項目を表示できます。
  - 流出されたファイルの数。
  - 実行されたアクション。
  - 使用したアプリケーション。
  - ユーザーが使用するデバイス。



ユーザーに適用できるアクション

ユーザーのアカウントでは、次の操作を実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントで異常なアクティビティや疑わしいアクティビティが発生すると、すべての管理者または選択した管理者に電子メール通知が送信されます。
- ユーザーをログオフします。ユーザーが自分のアカウントからログオフすると、Virtual Desktops を介してリソースにアクセスできなくなります。
- セッションの記録を開始します。ユーザーの仮想デスクトップアカウントに異常なイベントがある場合、管理者は将来のログオンセッションでのユーザーのアクティビティの記録を開始できます。ただし、ユーザーが Citrix Virtual Apps and Desktops 7.18 以降を使用している場合、管理者はユーザーの現在のログオンセッションの記録を動的に開始および停止できます。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

疑わしいログオン

Citrix Analytics は、ユーザーが使用するデバイス、場所、ネットワークによって共同で定義される複数のコンテキスト要因に基づいて、異常または危険に見えるユーザーのログオンを検出します。

疑わしいログオンリスクインジケータはいつトリガーされますか?

リスク指標は、次の要因の組み合わせによってトリガーされます。各要因は、1 つまたは複数の条件に基づいて潜在的に疑わしいと見なされます。

要素	条件
異常なデバイス	ユーザーは、過去 30 日間に使用されていないデバイスからログオンします。 ユーザーは、デバイスの署名がユーザーの履歴と矛盾している HTML5 クライアントまたは Chrome クライアントからログオンします。
通常以外の場所	過去 30 日間にユーザーがログオンしていない都市または国からログオンします。 都市または国が、最近の (過去 30 日間) のログオン場所から地理的に離れている。 過去 30 日間に都市または国からログオンしたユーザー数が 0 人または最小です。
異常なネットワーク	ユーザーが過去 30 日間に使用していない IP アドレスからログオンします。 ユーザーが過去 30 日間に使用していない IP サブネットからログオンします。 過去 30 日間にゼロ人または最小のユーザーが IP サブネットからログオンしました。
IP 脅威	IP アドレスは、コミュニティ脅威インテリジェンスフィード (Webroot) によって高リスクとして識別されます。 Citrix Analytics は最近、他のユーザーの IP アドレスから非常に疑わしいログオンアクティビティを検出しました。

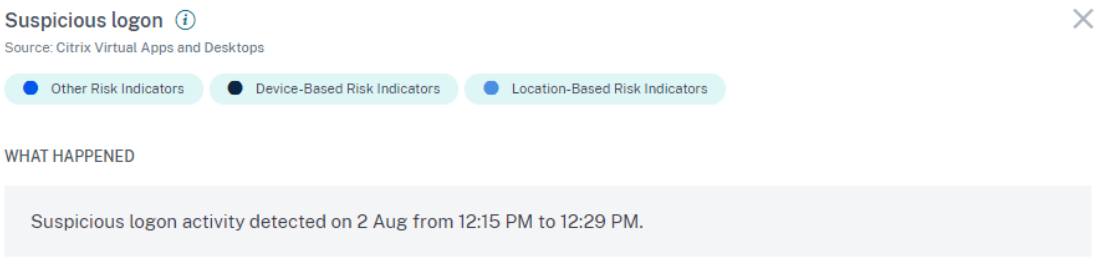
疑わしいログオンリスク指標を分析する方法

インドのムンバイから初めてログオンしたユーザー Adam Maxwell を考えてみましょう。新しいデバイス、または過去 30 日間使用されなかったデバイスを使用して、Citrix Virtual Apps and Desktops 新しいネットワークにログオンして接続しました。Citrix Analytics は、場所、デバイス、ネットワークなどの要因が通常の動作から逸脱し、疑わしいログオンリスク指標をトリガーするため、このログオンイベントを疑わしいとして検出します。リスク指標は Adam Maxwell のリスクタイムラインに追加され、リスクスコアが彼に割り当てられます。

Adam Maxwell のリスク時間を表示するには、[セキュリティ] **>** [ユーザー] を選択します。[危険なユーザー] ペインから、ユーザー Adam Maxwell を選択します。

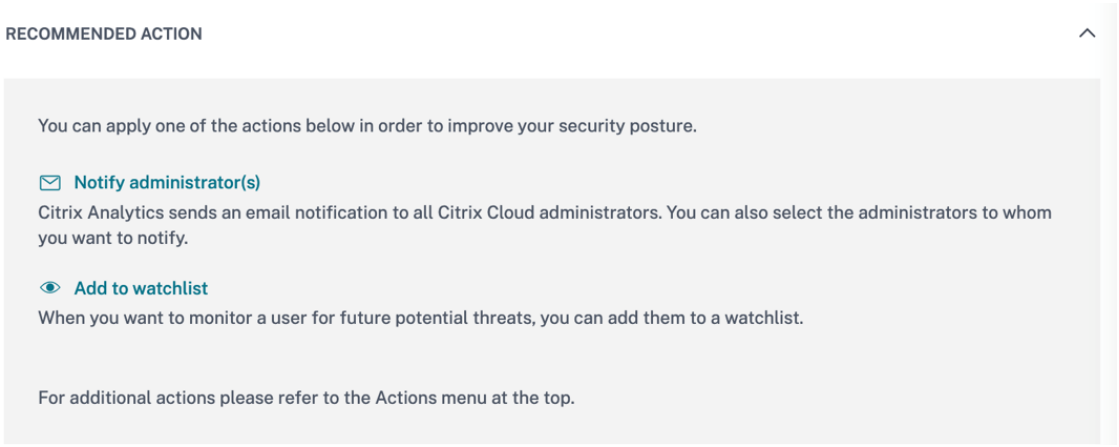
Adam Maxwell のリスクタイムラインから、疑わしいログオンリスク指標を選択します。次の情報を表示できます。

- 「**WHAT** HAPPENED」セクションには、リスク要因やイベントの発生時間など、疑わしいアクティビティの概要が表示されます。



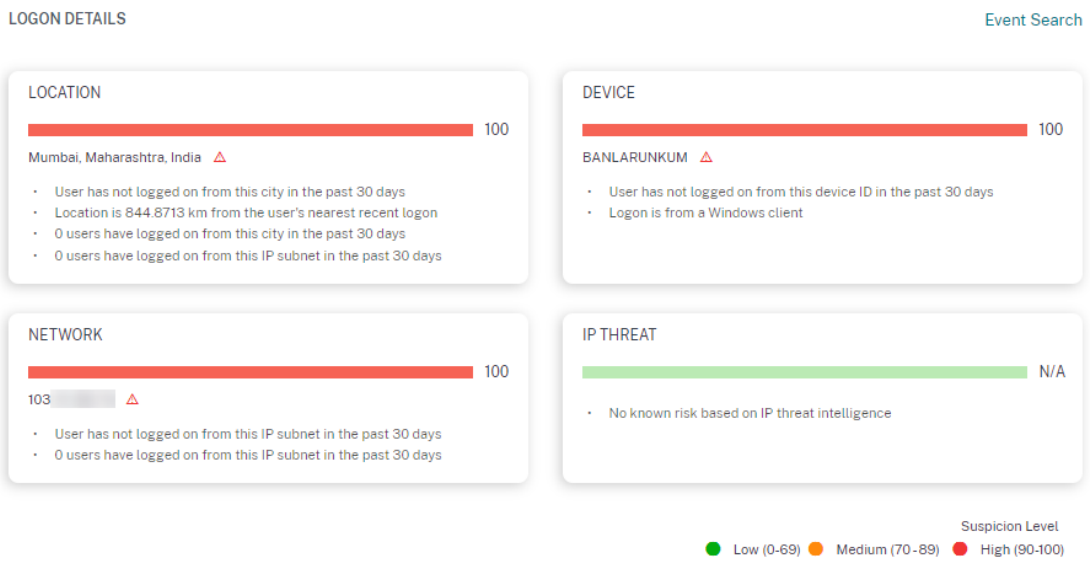
- [推奨アクション] セクションには、リスク指標に適用できる推奨アクションが表示されます。Citrix Analytics for Security では、ユーザーがもたらすリスクの重大度に応じてアクションを推奨します。推奨されるアクションは、次のアクションの 1 つまたは組み合わせです。
  - 管理者に通知
  - ウォッチリストに追加
  - ポリシーを作成する

  レコメンデーションに基づいてアクションを選択できます。または、「アクション」(Actions) メニューの選択内容に応じて、適用するアクションを選択することもできます。詳細については、「アクションを手動で適用する」を参照してください。



- **[LOGON DETAILS**] セクションには、各リスク要因に対応する疑わしいアクティビティの詳細な概要が表示されます。各リスクファクターには、疑わしいレベルを示すスコアが割り当てられます。単一のリスク要因は、ユーザーからのリスクが高いことを示すものではありません。全体的なリスクは、複数のリスク因子の相関に基づいています。

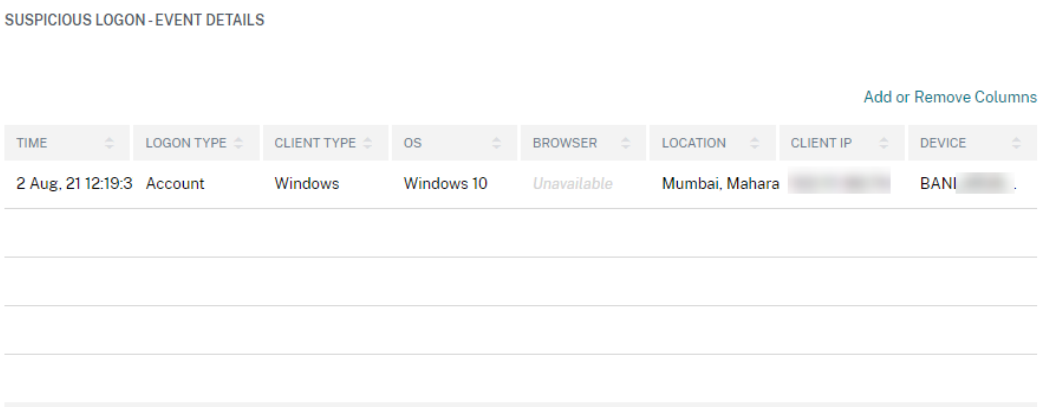
疑惑レベル	指示
0–69	この要因は正常に見え、疑わしいとは見なされません。
70–89	この要因はわずかに通常とは違うように見え、他の要因では適度に疑わしいと考えられます。
90–100	この要因はまったく新しいものまたは通常とは違うものであり、他の要因と非常に疑わしいと考えられています。



- [**LOGON LOCATION-**過去 **30** 日間] セクションには、最後に認識された場所とユーザーの現在の場所の地

理的マップビューが表示されます。過去 30 日間の位置データが表示されます。マップ上のポインターにカーソルを合わせると、各場所からの合計ログオン数が表示されます。

- [疑わしいログオン-イベントの詳細] セクションには、疑わしいログオンイベントに関する次の情報が表示されます。
  - 時刻: 疑わしいログオンの日付と時刻を示します。
  - ログオンの種類: ユーザーアクティビティがセッションログオンかアカウントログオンかを示します。アカウントログオンイベントは、ユーザーのアカウントへの認証が成功するとトリガーされます。一方、セッションログオンイベントは、ユーザーが資格情報を入力してアプリまたはデスクトップセッションにログオンしたときにトリガーされます。
  - クライアントの種類: ユーザーデバイスにインストールされている Citrix Workspace アプリの種類を示します。ユーザーデバイスのオペレーティングシステムに応じて、クライアントの種類は Android、iOS、Windows、Linux、Mac などです。
  - **OS**: ユーザーデバイスのオペレーティングシステムを示します。
  - ブラウザ: アプリケーションへのアクセスに使用される Web ブラウザを示します。
  - 場所: ユーザーがログオンした場所を示します。
  - クライアント **IP**: ユーザーデバイスの IP アドレスを示します。
  - デバイス: ユーザーのデバイス名を示します。



ユーザーに適用できるアクションは何ですか

ユーザーのアカウントでは、次の操作を実行できます。

- ウォッチリストに追加する。将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。
- 管理者に通知します。ユーザーのアカウントで異常なアクティビティや疑わしいアクティビティが発生すると、すべての管理者または選択した管理者に電子メール通知が送信されます。
- ユーザーをログオフします。ユーザーが自分のアカウントからログオフすると、Virtual Desktops を介してリソースにアクセスできなくなります。
- セッションの記録を開始します。ユーザーの仮想デスクトップアカウントに異常なイベントがある場合、管理者は将来のログオンセッションでのユーザーのアクティビティの記録を開始できます。ただし、ユーザーが Citrix Virtual Apps and Desktops 7.18 以降を使用している場合、管理者はユーザーの現在のログオンセッションの記録を動的に開始および停止できます。

アクションの詳細とアクションを手動で設定する方法については、「ポリシーとアクション」を参照してください。

アクションをユーザーに手動で適用するには、ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューからアクションを選択し、[適用] をクリックします。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

ユーザーリスク指標へのフィードバックを提供する

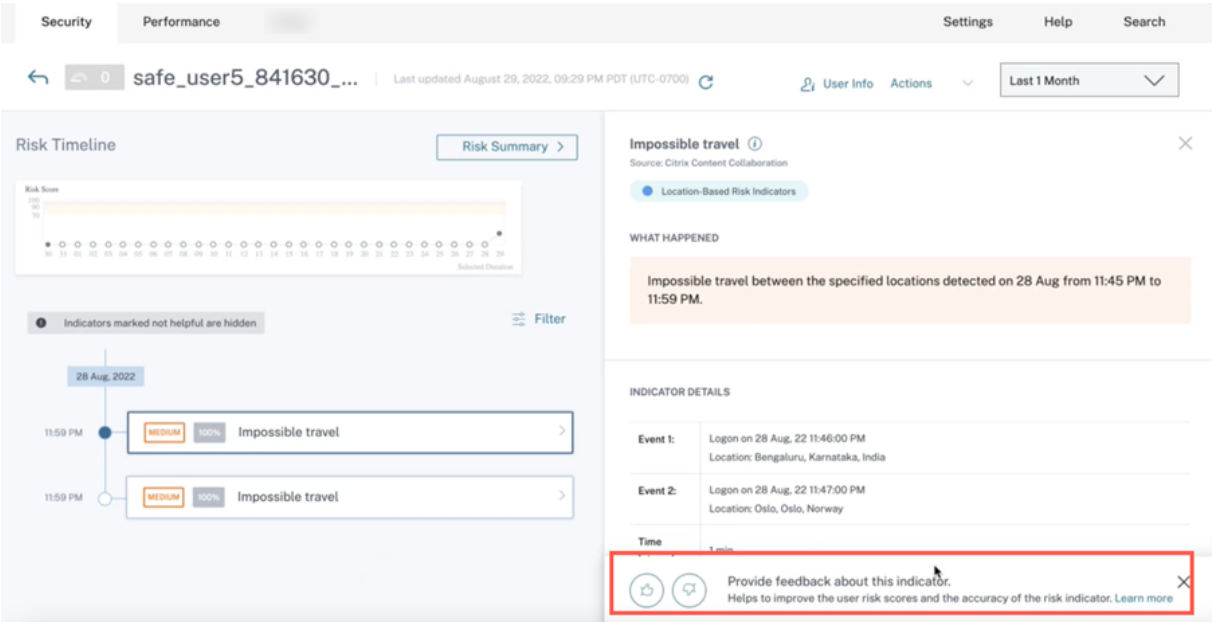
October 20, 2022

リスク指標は、ユーザーのリスクスコアを自動的に増加させながら、疑わしいまたは異常なユーザーアクティビティを検出して報告するように設計されています。実際には、リスク指標の出現は正当な根底にあるセキュリティ上の脅威に対応するものもあれば、無害であることが判明するものもあります。

指標フィードバック機能により、リスク指標の発生を明示的にフラグ付けできます。

- 根底にある真のユーザーリスクがあると思われる場合に役立ちます
- セキュリティ上の脅威がないと判断した場合は役に立ちません。この場合、指標の発生はデフォルトでユーザーのタイムラインから非表示になり、ユーザーのリスクスコアは、その後の計算でこの指標の発生を除外するように自動的に調整されます。

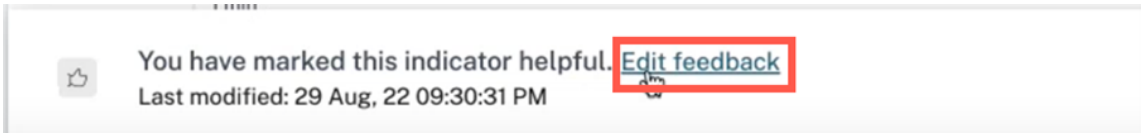
さらに、収集されたフィードバックは、リスク指標アルゴリズムの将来の改善を促進するために使用されます。



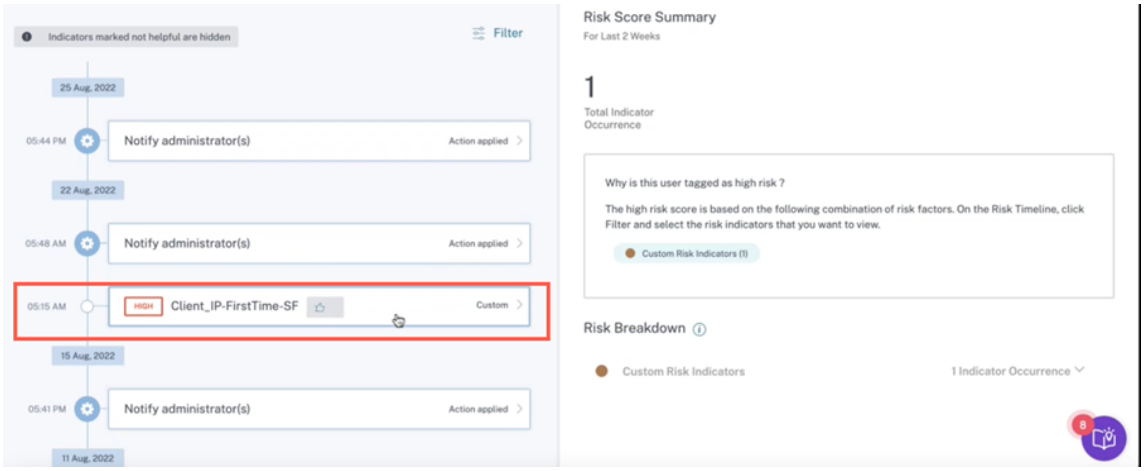
ユーザータイムラインのデフォルトリスク指標エントリごとに、フィードバックバナー（親指を立てるアイコンと下向きのアイコン付き）が表示されます。

- 親指を立てるアイコン - インジケーターは役に立ち、危険なアクティビティを正しく識別します。親指を立てるアイコンをクリックして、指標がどのように役立つのか、またその利点について追加のコメントを入力できます。

  フィードバックを保存して、インジケーターに役立ったマークを付けることができます。また、[フィードバックを編集] をクリックしてコメントを編集することもできます。フィードバックバナーには、最後に送信されたフィードバックのタイムラインが表示されます。

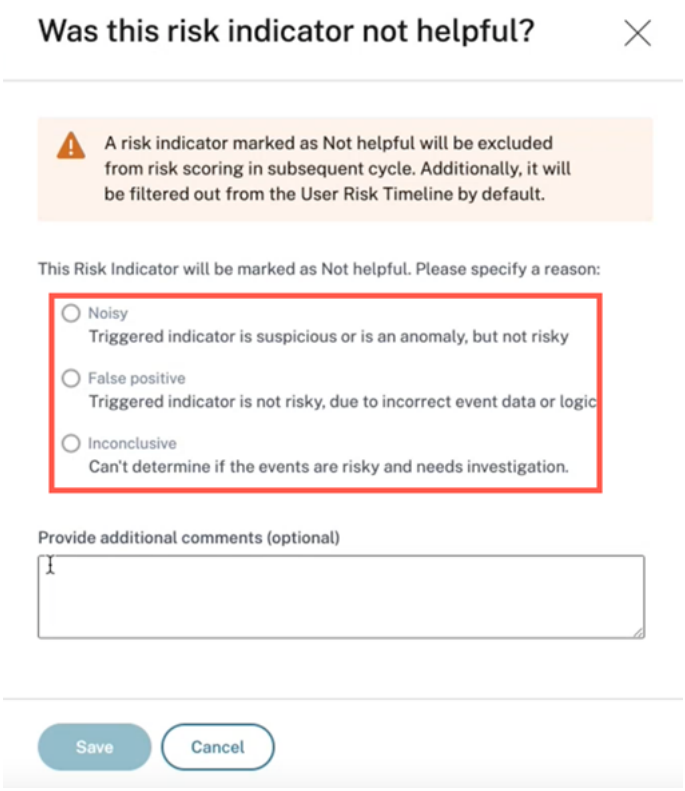
  

  リスク指標が役に立つとマークされると、このフィードバックは対応するユーザータイムラインのエントリに表示され、Citrix Analytics に報告されます。ユーザーのリスクスコアは影響を受けません。



- 親指を下げるアイコン -インジケーターが役に立たないか、誤ってトリガーされます。インジケーターを「役に立たない」とマークして、「ノイズ」、「誤検知」、または「不確定」に分類できます。このリスク指標の発生は、ユーザーのリスクスコアに対するその後のすべての更新から除外されます。必要に応じて、追加のコメントを入力することもできます。
  - 騒々しい—トリガーされたインジケーターが疑わしい、または異常ですが、危険ではありません。
  - 誤検知—イベントデータまたはロジックが正しくないため、トリガーされたインジケーターは危険ではありません。
  - 不確定—イベントが危険であるかどうかを判断できず、調査が必要です。

    > 注
    >
    > リスクスコアの再調整には最大 15 分かかります。

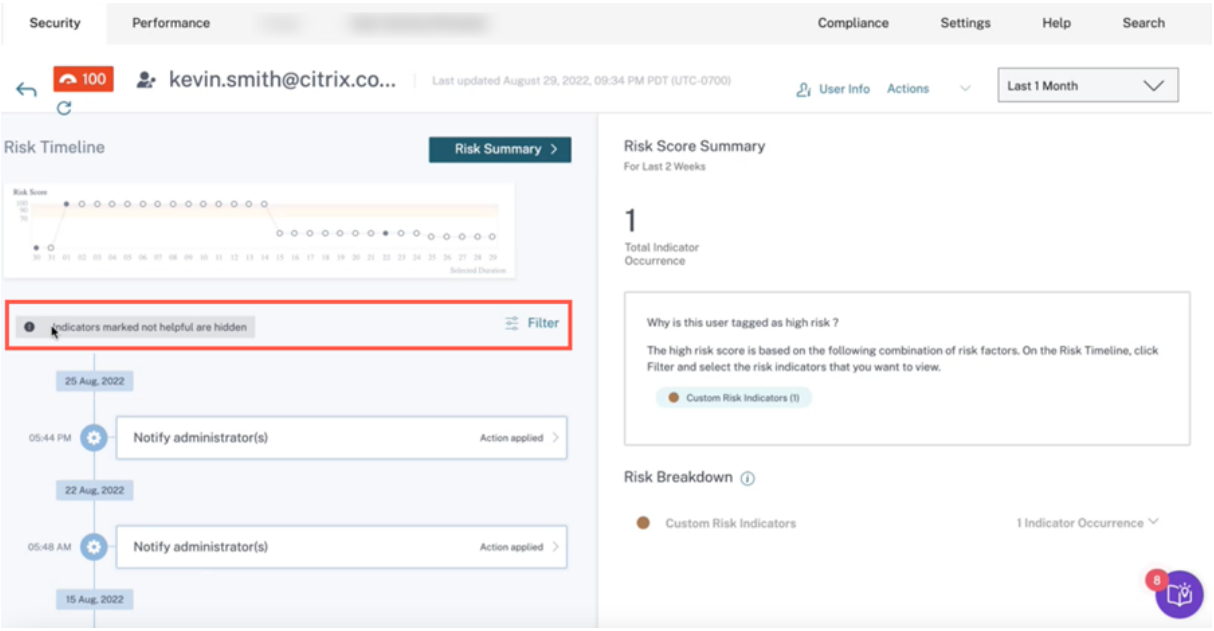


指標が「役に立たない」とマークされている場合、次の結果が表示されます。

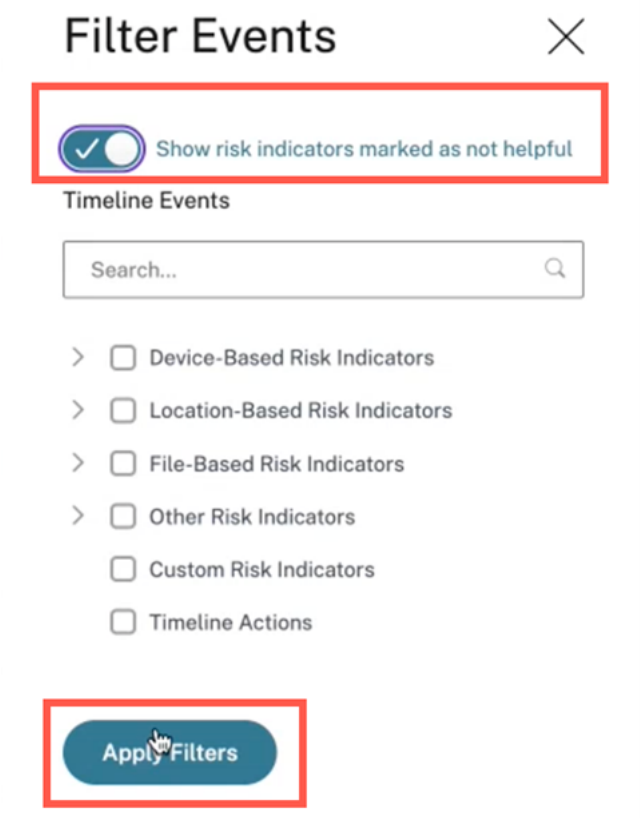
- その特定の指標はタイムラインから隠されています。
- リスクスコアは、以降の更新でこの指標の発生をリスクスコアの計算から除外した結果として再調整されます。
- テキストによるフィードバックとして提供された追加情報は、後で参照できるように保持されます。

フィルターを表示

役に立たないとマークされた指標は、デフォルトで非表示になっています。

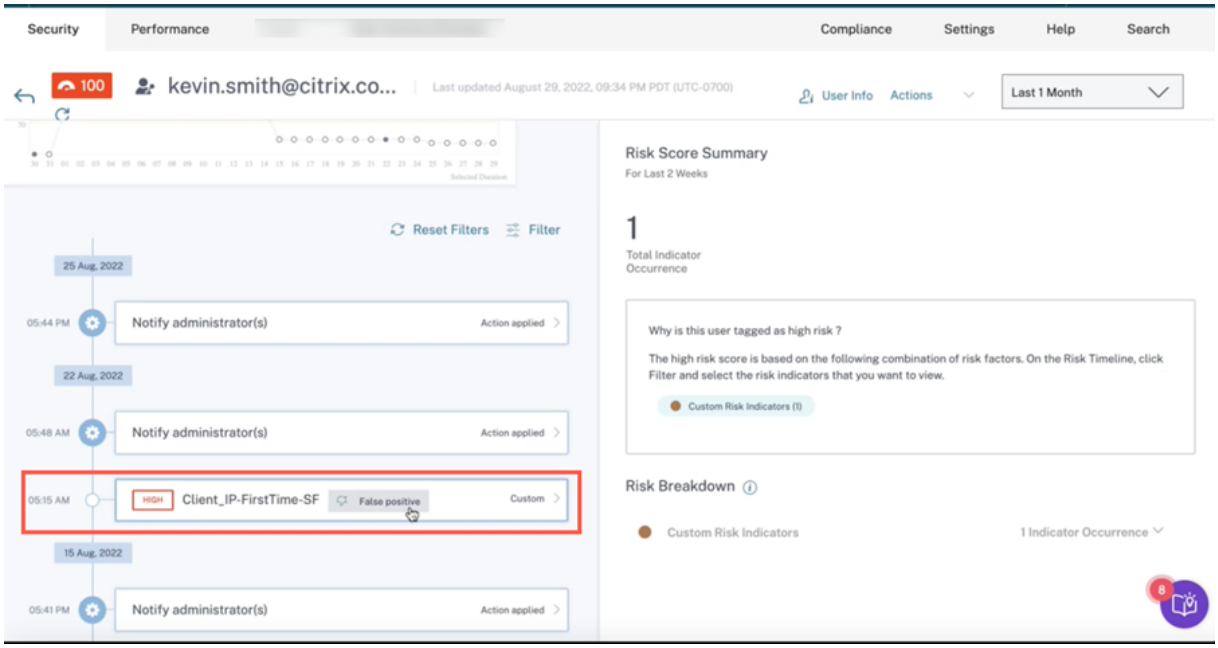


非表示のインジケーターを表示するには、[フィルター] をクリックします。表示される [イベントのフィルター] ウィンドウで、[役に立たないとマークされたリスク指標を表示] をオンにします。



カテゴリに基づいて指標を検索できます。たとえば、ロケーションベースの非表示リスク指標を表示するには、カテ

ゴリを選択して [フィルターを適用] をクリックします。フィードバックの詳細では役に立たない位置ベースの指標をすべて表示できます。



管理者は、必要に応じて次のアクションを実行することもできます。

- フィードバックを変更
- 以前のフィードバックと関連するメタデータを確認する
- 他の管理者から提供されたフィードバックと関連するメタデータを確認してください

> 注
>
> - テナントレベルではなく、ユーザーレベルごとにフィードバックを提供できます。あるリスク指標のフィードバックが、その特定のリスク指標のすべてのインスタンスに適用されるわけではありません。
> - あるユーザーへのフィードバックは、他のユーザーには適用されません。

Microsoft Graph セキュリティリスク指標

April 12, 2024

Microsoft Graph セキュリティは、エンドポイントセキュリティプロバイダー向けの Azure AD アイデンティティ保護または Microsoft**Defender** からデータを受信し、その情報を Citrix Analytics 送信します。

Azure AD ID 保護は、次のリスク指標をトリガーし、Microsoft Graph セキュリティに情報を送信します。

- 匿名 IP アドレス
- 非定型的な場所への移動は不可能
- 漏洩した認証情報を持つユーザー
- 感染したデバイスからのサインイン
- 疑わしいアクティビティを持つ IP アドレスからのサインイン
- 不慣れな場所からのサインイン

エンドポイント用 Defender の詳細については、「エンドポイント向け Microsoft Defender」を参照してください。

リスク指標に関連する危険因子は、IP ベースのリスク指標です。リスク要因について詳しくは、「Citrix ユーザーリスク指標」を参照してください。

Microsoft Graph セキュリティリスク指標を分析する方法

前述の危険な行動の 1 つを示すユーザー Maria Brown を考えてみましょう。Microsoft はインシデントを検出し、アラートを生成します。Citrix Analytics はこのアラートを取得し、更新されたリスクスコアを Maria Brown に割り当てます。また、適切なリスク指標が Maria Brown のリスクタイムラインに追加されます。

ユーザーの Microsoft Graph セキュリティリスク指標エントリを表示するには、[セキュリティ] > [ユーザー] に移動し、ユーザーを選択します。

Maria のタイムラインから、リスクタイムラインから最新のリスク指標エントリを選択できます。対応する詳細情報パネルが右側のペインに表示されます。**WHAT HAPPENED** セクションには、リスク指標の簡単な概要が表示されます。

リスク指標に関する詳細情報の入手方法

詳細については、「Azure Active Directory のリスクイベント」を参照してください。

ユーザーに適用できるアクションは何ですか

現在、Microsoft Graph セキュリティデータソースを介してユーザーのアカウントに対して適切なアクションを実行する機能は利用できません。

Microsoft Graph セキュリティのオンボーディングの詳細については、「Microsoft Graph セキュリティ」を参照してください。

カスタムリスク指標

December 7, 2023

セキュリティ向け Citrix Analytics には、次の 2 種類のリスク指標が表示されます。

- デフォルトのリスク指標: これらのリスク指標は、機械学習アルゴリズムに基づいています。詳しくは、「Citrix ユーザーリスク指標」を参照してください。
- カスタムリスク指標: これらのリスク指標は管理者が手動で作成します。

カスタムリスク指標を作成すると、ユースケースに基づいてトリガー条件とパラメーターを定義できます。ユーザーイベントが定義した条件に一致すると、Citrix Analytics はカスタムリスク指標をトリガーし、ユーザーのリスクタイムラインに表示します。

次のデータソースに対してカスタムリスク指標を作成します。

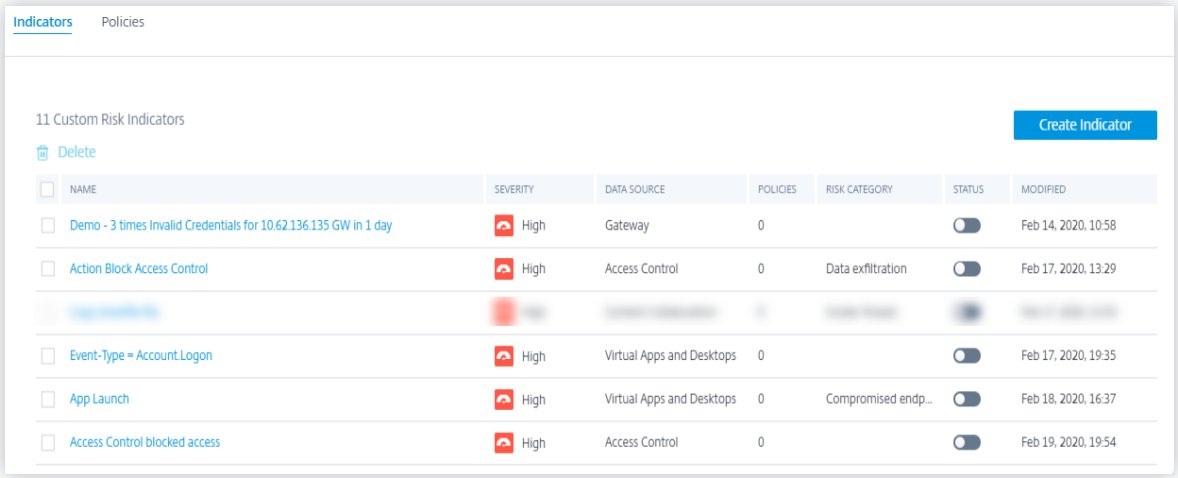
- Citrix Gateway
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops オンプレミス
- Citrix DaaS（旧称：Citrix Virtual Apps and Desktops サービス）
- Citrix Secure Browser

事前設定されたカスタムリスク指標

また、Citrix インフラストラクチャのセキュリティを監視するために、条件が事前に構成されたカスタムリスク指標もいくつか用意されています。事前設定された条件は、ユースケースに基づいて変更できます。詳細については、「事前構成されたカスタムリスク指標」を参照してください。

カスタムリスク指標ページ

[カスタムリスク指標] ページには、ユーザー、重大度、データソース、ポリシーの数、リスクカテゴリ、ステータス、および指標の最終更新日時に生成されたすべてのカスタムリスク指標に関する洞察が表示されます。カスタムリスク指標を作成するには、「カスタムリスク指標の作成」を参照してください。



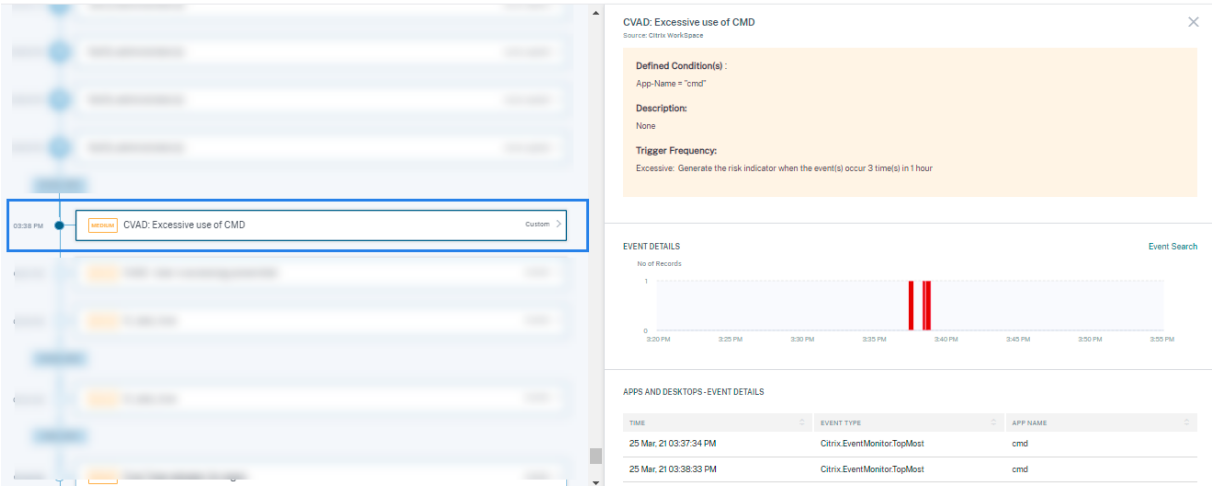
リスク指標を選択すると、[リスク指標の変更] ページにリダイレクトされます。詳細については、「カスタムリスク指標の変更」を参照してください。

カスタムリスク指標の分析

定義したカスタムリスク指標をトリガーしたアクションを持つユーザーを考えてみましょう。Citrix Analytics では、ユーザーのリスクタイムラインにカスタムリスク指標が表示されます。

ユーザーのリスクタイムラインでカスタムリスク指標を選択すると、右側のペインに次の情報が表示されます。

- 定義された条件**:** カスタムリスク指標の作成時に定義した条件の概要を表示します。
- 説明: カスタムリスク指標の作成時に提供する説明の概要を提供します。カスタムリスク指標の作成中に説明が指定されていない場合、このセクションには [なし] が反映されます。
- トリガー頻度: カスタムリスク指標の作成時に **[**詳細オプション**]** セクションで選択したオプションが表示されます。
- イベントの詳細: カスタムリスク指標をトリガーしたユーザーイベントのタイムラインと詳細を表示します。[イベント検索] をクリックすると、セルフサービス検索ページでユーザーイベントを表示できます。セルフサービス検索ページには、ユーザーに関連付けられたイベントとカスタムリスクインジケータが表示されます。検索クエリには、カスタムリスク指標に定義された条件が表示されます。



> 注
>
> カスタムリスク指標は、ユーザーリスクタイムライン上のラベルで表されます。

ユーザーに適用できるアクション

ユーザーに対してカスタムリスク指標がトリガーされると、アクションを手動で適用することも、アクションを自動的に適用するポリシーを作成することもできます。詳細については、「ポリシーとアクション」を参照してください。

カスタムリスク指標テンプレート

事前定義されたテンプレートのいずれかを使用してカスタムリスク指標を作成することも、テンプレートを使用せずに続行することもできます。

テンプレートは、カスタムリスク指標を作成するための開始点として機能します。ユースケースに基づいて選択できる定義済みのクエリとパラメーターを提供することで、カスタムリスク指標の作成をガイドします。

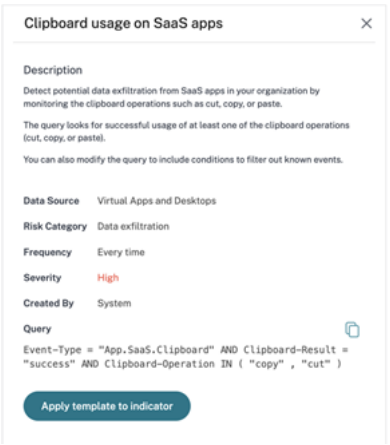
テンプレートはそのまま使用することも、要件に合わせて変更することもできます。管理者はテンプレートを使用して、追加のトレーニングをしなくても、関心のあるリスク指標を作成できます。

テンプレートは次の情報で構成されます。

- 説明: テンプレートに定義されているクエリの目的を示します。
- データソース: テンプレートが適用されるデータソースを示します。
- リスクカテゴリ: クエリで検索されたイベントに関連付けられているリスクカテゴリを示します。危険なイベントには、データ漏洩、内部脅威、侵害されたユーザー、および侵害エンドポイントの 4 つのカテゴリがあります。詳細については、「リスクカテゴリ」を参照してください。
- 頻度: クエリがトリガーされる頻度を示します。

- 重大度: イベントに関連するリスクの重大度を示します。リスクは、高、中、低のいずれかです。
- 作成者: テンプレートの作成者を示します。テンプレートは常にシステム定義です。
- クエリー: テンプレートに定義されている条件を示します。クエリは、条件を満たすユーザーイベントを取得します。

次の図は、SaaS アプリでのユースケースクリップボード使用のテンプレートを示しています。

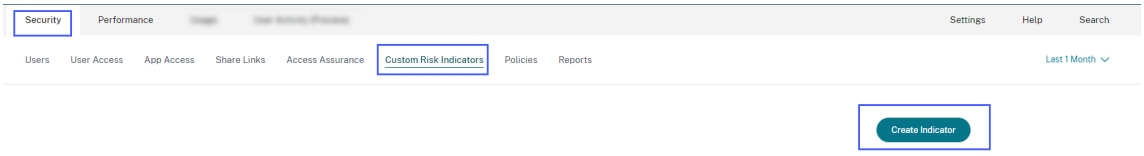


ユースケースに適したテンプレートが見つからない場合、または独自のクエリを定義する場合は、テンプレートなしで続行できます。

カスタムリスク指標の作成

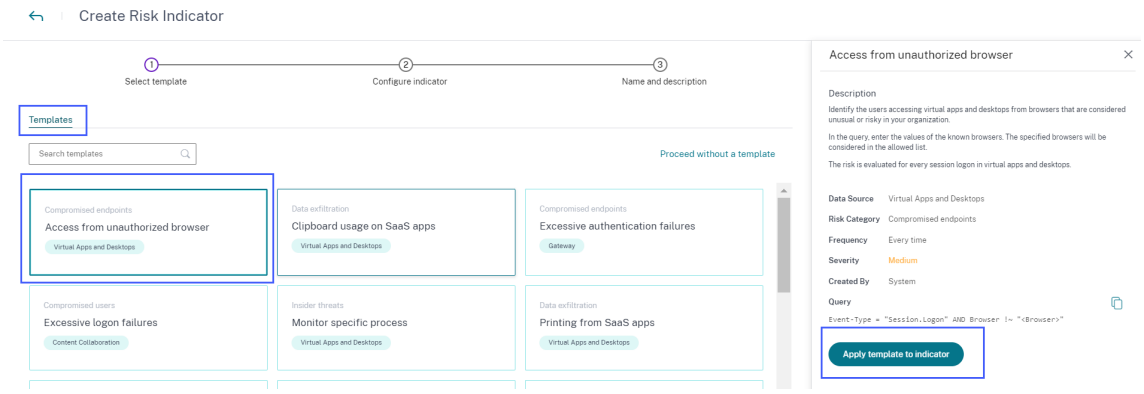
カスタムリスク指標を作成するには:

1. [セキュリティ] **>** [カスタムリスク指標] **>** [指標の作成] に移動します。

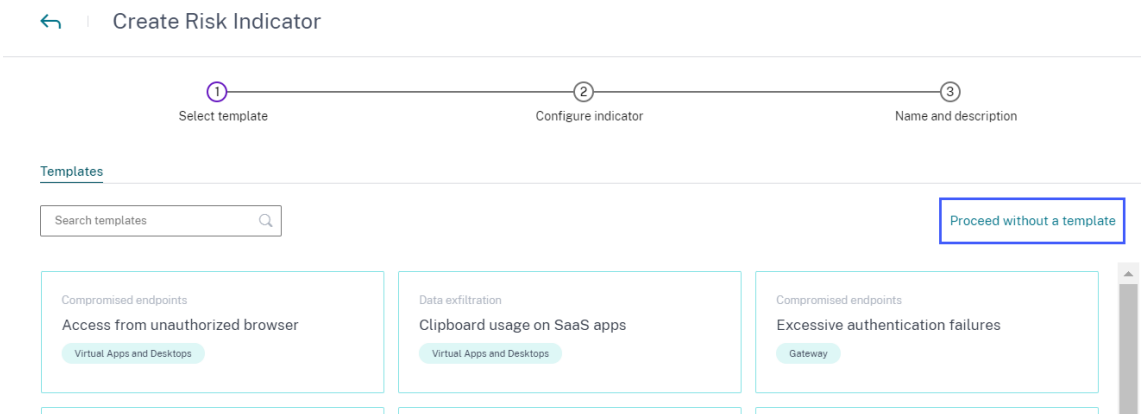


2. テンプレートを選択してユースケースを表示します。要件を満たしている場合は、[指標にテンプレートを適用] を選択します。

> 注
>
> また、テンプレートの定義済み条件とパラメータを変更することもできます。



3. 目的のテンプレートが見つからない場合、または独自の条件を作成する場合は、[テンプレートなしで続行] を選択します。



4. 画面の指示に従ってインジケーターを作成します。

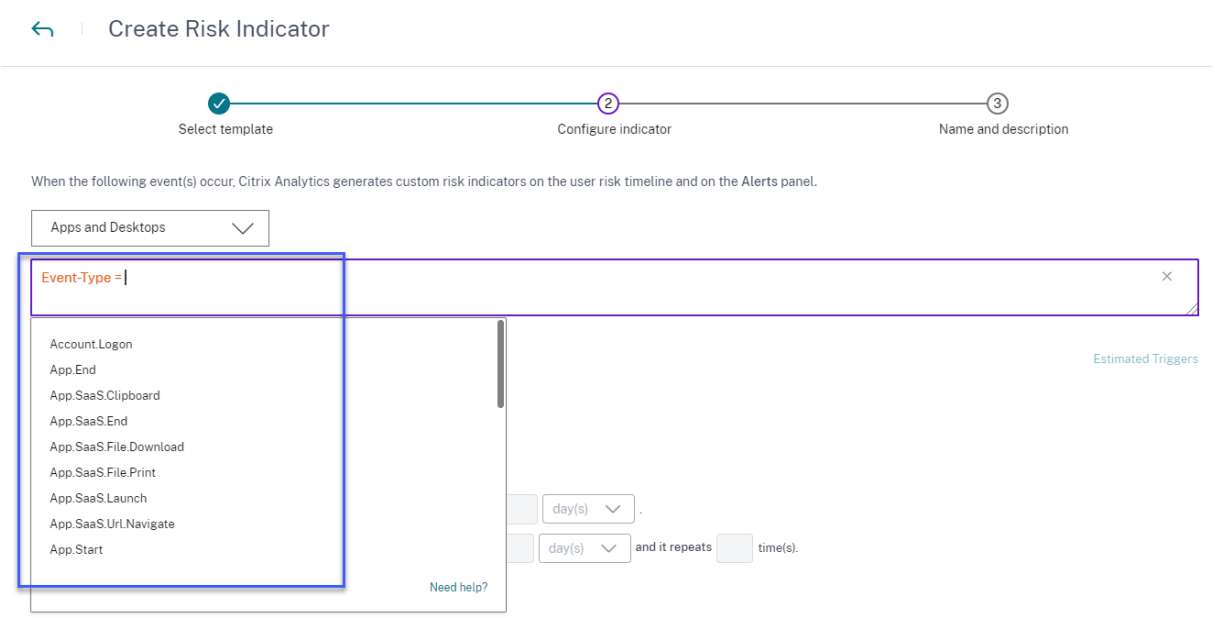
> メモ
>
> - カスタムリスク指標は、最大 50 個まで作成できます。この上限に達した場合は、既存のカスタムリスク指標を削除または編集して、カスタムリスク指標を作成する必要があります。
> - カスタムリスク指標がトリガーされると、すぐにユーザータイムラインに表示されます 。ただし、ユーザーのリスクサマリーとリスクスコアは数分（約 15 ～20 分）後に更新されます。

カスタムリスク指標の条件の定義

クエリボックスを使用して、カスタムリスク指標の条件を定義します。選択したデータソースに応じて、対応するディメンションと 、条件を定義するための有効な演算子が取得されます 。

特定のディメンション（`Event-Type`や`Clipboard-Operation`など）を有効な演算子と一緒に選択すると、ディメンションの値が自動的に表示されます。推奨オプションから値を選択するか、要件に応じて新しい値を入力できます。

次の図は、ディメンションの推奨値を示しています `Event-Type`。



テンプレートを使用する場合、条件は事前に定義されています。ただし、ユースケースに基づいて、定義済みの条件を追加または変更できます。

クエリボックスの下に、[推定トリガー] リンクが表示されます。リンクをクリックして、定義された条件に対してトリガーされるカスタムリスク指標のおおよそのインスタンスを予測します。これらのインスタンスは、Citrix Analytics が保持し、定義された条件を満たす履歴データに基づいて計算されます。

[**Estimated Triggers**] をクリックして、最後に定義された条件に対するカスタムリスク指標の発生数を予測します。

詳細オプションを使う

[詳細オプション] セクションで、カスタムリスク指標をトリガーするイベントの頻度を選択します。オプションを選択しない場合、Citrix Analytics では「毎回: イベントが発生するたびにリスク指標を生成する」がデフォルトのオプションとして考慮され、カスタムリスク指標が生成されます。次のいずれかのオプションを選択できます。

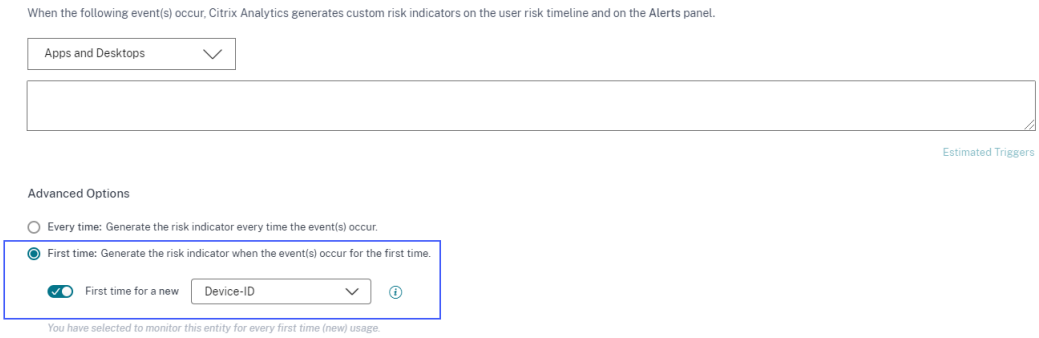
- 毎回: リスク指標は、イベントが定義された条件を満たすたびにトリガーされます。
- 初回: リスク指標は、イベントが定義された条件を初めて満たしたときにトリガーされます。
  - **First time for a new:** 新しいエンティティから初めて受信したイベントを検出するには、このオプションを有効にします。エンティティの例としては、クライアント IP、国、都市、デバイス ID などがあります。データソースに基づいて選択できるエンティティは 1 つだけです。このオプションを使用すると、エンティティの明示的な値を指定せずにリスク指標を作成できます。たとえば、エンティティを「City」として選択した場合、都市名を指定する必要はありません。リスク指標は、新しい都市から初めてイベントを受信したときにトリガーされます。

    次の表に、各データソースに対応するエンティティとそのトリガー条件を示します。

データソース	エンティティ	トリガー条件
Secure Private Access	市区町村	ユーザーが新しい都市から初めてログオンしたとき。
	クライアント IP	ユーザーが新しい IP アドレスから初めてログオンしたとき。
	国	ユーザーが新しい国から初めてログオンしたとき。
アプリケーションとデスクトップ	アプリ名	ユーザーが新しい仮想アプリケーションまたは SaaS アプリケーションを初めて開いたとき。
	アプリ URL	ユーザーが仮想デスクトップのブラウザで新しいアプリ URL を初めて入力したとき。
	市区町村	ユーザーが新しい都市からアプリまたはデスクトップを初めて起動したとき。
	クライアント IP	ユーザーが新しい IP アドレスから初めてログオンしたとき。
	国	ユーザーが新しい国のアプリまたはデスクトップを初めて起動したとき。
	デバイス ID	ユーザーがモバイル、ラップトップ、デスクトップマシンなどの新しいデバイスから仮想アプリまたは仮想デスクトップを初めて起動したとき。
	ダウンロードデバイスタイプ	ユーザーが USB ドライブなどの新しいストレージメディアを初めて使用したとき。
	印刷ファイル形式	印刷ファイルの形式。
	印刷ファイルサイズ	印刷ファイルのサイズ (バイト単位)。
	印刷ファイル名	印刷されるファイルの名前。
	プリンタ名	使用するプリンタの名前。
	総部数-印刷済み	ユーザーが印刷した部数の合計。
	合計ページ数-印刷済み	ユーザーが印刷した文書ページの総数。
Gateway	クライアント IP	ユーザーが新しい IP アドレスから初めてログオンしたとき。
Secure Browser	User-Name	イベントを開始したユーザーの名前。

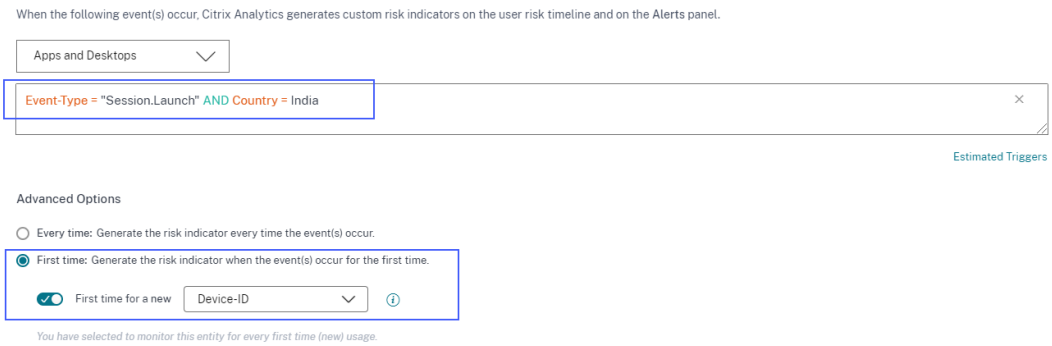
データソース	エンティティ	トリガー条件
	アクセス許可	ユーザーがホストサービスへのアクセスを許可されているか拒否されているか。
	クライアント IP	ユーザーデバイスの IP アドレス。
	ホスト名アクセス	ユーザーがネットワーク経由でアクセスするホストサービス。
	セッション ID	ユーザーセッションに割り当てられた固有の番号。

次の例は、Apps and Desktops データソース用に作成されたカスタムリスク指標を示しています。リスク指標は、ユーザーが新しいデバイスから仮想デスクトップまたは仮想アプリケーションを初めて起動したときにトリガーされます。



また、新しいオプションの **[初回]** とともに条件を追加することもできます。この場合、リスク指標は、新しいエンティティからのイベントを初めて検出し、イベントが定義された条件を満たすときにトリガーされます。

次の例は、カスタムリスク指標に対して定義された条件と、新しいデバイス **ID** オプションの **[初回]** オプションを有効にした状態を示しています。リスクインジケータは、インドにいるユーザーが新しいデバイスから仮想デスクトップセッションを初めて起動したときにトリガーされます。



- 過剰: リスク指標は、次の条件が満たされた後にトリガーされます。

  - イベントは定義された条件を満たしています。
  - イベントは、指定された期間中に指定された回数だけ発生します。

- 頻繁: リスク指標は、次の条件が満たされた後にトリガーされます。
  - イベントは、定義された条件を満たしています。
  - イベントは、指定された期間中、指定された回数だけ発生します。
  - イベントパターンは、指定された回数だけ繰り返されます。

リスクカテゴリの選択

カスタムリスク指標のリスクカテゴリを選択します。

リスク指標は、カスタムリスク指標のリスクエクスポージャーのタイプに基づいてグループ化されます。リスクカテゴリの選択については、リスクカテゴリを参照してください。

重大度の選択

重大度は、リスク指標によって検出される危険なイベントの重大度を示します。カスタムリスク指標を作成するときは、重大度-高、中、低のいずれかを選択します。

テンプレートを適用すると、重大度オプションがあらかじめ選択されています。この事前選択は、ユースケースに応じて変更できます。

条件の定義でサポートされる演算子

条件を定義する際には、次の演算子を使用できます。

演算子	説明	例	出力
:	検索クエリに値を割り当てます。	User-Name : John	ユーザー John のイベントを表示します。
=	検索クエリに値を割り当てます。	User-Name = John	ユーザー John のイベントを表示します。
~	類似の値を検索します。	User-Name ~ test	類似のユーザー名を持つイベントを表示します。
“”	値をスペースで区切って囲みます。	User-Name = “John Smith”	ユーザー John Smith のイベントを表示します。

演算子	説明	例	出力
<, >	リレーショナル値を検索します。	Data Volume > 100	データボリュームが 100 GB を超えるイベントを表示します。
および	両方の条件が真である値を検索します。	User-Name : John AND Data Volume > 100	データボリュームが 100 GB を超えるユーザー John のイベントを表示します。
*	文字に一致する値を 0 回以上検索します。	User-Name = John*	John で始まるすべてのユーザー名のイベントを表示します。
		User-Name = *John*	John を含むすべてのユーザー名のイベントを表示します。
		User-Name = *Smith	Smith で終わるすべてのユーザー名のイベントを表示します。
!~	ユーザーイベントで、指定したマッチングパターンがあるかどうかをチェックします。この NOT LIKE 演算子は、イベント文字列のどこにも一致するパターンを含まないイベントを返します。	ユーザー名！ ~ ジョン	John、John Smith、または一致する名前「John」を含むユーザー以外のユーザーのイベントを表示します。
!=	ユーザーイベントで、指定した文字列が正確にチェックされます。この NOT EQUAL 演算子は、イベント文字列のどこにも正確な文字列を含まないイベントを返します。	国!= 米国	米国以外の国のイベントを表示します。
IN	ディメンションに複数の値を割り当てて、1 つ以上の値に関連するイベントを取得します。	ユーザーネーム IN (ジョン、ケビン)	ジョンまたはケビンに関連するすべてのイベントを見つける。

演算子	説明	例	出力
NOT IN	ディメンションに複数の値を割り当てて、指定した値を含まないイベントを検索します。	User-Name NOT IN (John, Kevin)	John と Kevin 以外のすべてのユーザーのイベントを検索します。
IS EMPTY	ディメンションの NULL 値または空の値をチェックします。この演算子は、App-Name、Browser、Countryなどの文字列タイプのディメンションでのみ機能します。Upload-File-Size、Download-File-Size、Client-IP などの非文字列 (数値) タイプのディメンションには使用できません。	Country IS EMPTY	国名が利用できない、または空である (指定されていない) イベントを検索します。
IS NOT EMPTY	ディメンションの NULL 値でない値または特定の値がないかどうかをチェックします。この演算子は、App-Name、Browser、Countryなどの文字列タイプのディメンションでのみ機能します。Upload-File-Size、Download-File-Size、Client-IP などの非文字列 (数値) タイプのディメンションには使用できません。	Country IS NOT EMPTY	国名が利用可能または指定されているイベントを検索します。

演算子	説明	例	出力
または	どちらかまたは両方の条件に該当する値を検索します。	(ユーザー名 = John* またはユーザー名 = *Smith) およびイベントタイプ = 「Session.Logon」	John で始まる、または Smith Session.Logon で終わるすべてのユーザー名のイベントを表示します。

> 注
>
> **NOT EQUAL** 演算子では、条件のディメンションの値を入力するときに、データソースのセルフ・サービス検索ページで使用可能な正確な値を使用します 。寸法値では、大文字と小文字が区別されます。

カスタムリスク指標の変更

1. [セキュリティ] > [カスタムリスク指標] に移動します。
2. 変更するカスタムリスク指標を選択します。
3. [インジケータの変更] ページで、必要に応じて情報を変更します。
4. [変更の保存] をクリックします。

> 注
>
> 既存のカスタムリスク指標の条件、リスクカテゴリ、重大度、名前などの属性をユーザータイムラインで変更しても、そのユーザーに対してトリガーされたカスタムリスク指標（古い属性を含む）の以前の発生を表示できます。
>
> たとえば、*Country!* という条件でカスタムリスク指標を作成したとします。= インド。したがって、このカスタムリスク指標は、ユーザーがインド国外からログオンしたときにトリガーされます。ここで、カスタムリスク指標の条件を *Country* に変更します。= 「米国」。この場合でも、[国] という条件で、カスタムリスク指標の以前の発生を表示できます。= リスク指標をトリガーしたユーザータイムラインのインド。

カスタムリスク指標を削除する

1. [セキュリティ] > [カスタムリスク指標] に移動します。
2. 削除するカスタムリスク指標を選択します。
3. [削除] をクリックします。
4. ダイアログで、カスタムリスク指標を削除するリクエストを確認します。

> 注
>
> カスタムリスク指標を削除しても、ユーザータイムラインで、そのユーザーに対してトリガーされたカスタムリスク指標の以前の発生を表示できます。
>
> たとえば、条件 *Country!* の既存のカスタムリスク指標を削除するとします。= インド。この場合でも、[国*]* という条件で、カスタムリスク指標の以前の発生を表示できます。= リスク指標をトリガーしたユーザータイムラインのインド。

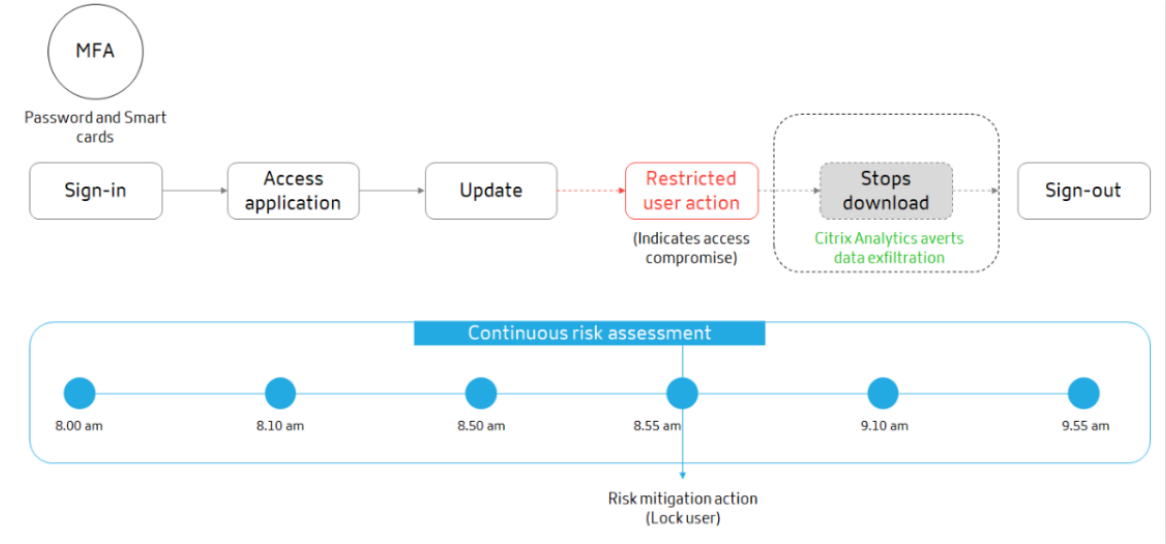
継続的なリスク評価

December 7, 2023

ポータブルコンピューティングデバイスとインターネットの使用が増加すると、Citrix Workspace ユーザーは、ほぼすべての場所とデバイスから作業できます。この柔軟性の課題は、リモートアクセスは、データの漏洩、盗難、破壊行為、サービスの中断などのサイバー犯罪行為を通じて、機密データをセキュリティリスクにさらすことです。組織内の従業員もこの被害の一因になりそうです。

このようなリスクに対処する従来の方法には、多要素認証、ショートサインインセッションなどを実装する方法があります。これらのリスク評価方法では、より高いレベルのセキュリティが保証されますが、ユーザーの初期検証後の完全なセキュリティは提供されません。悪意のあるユーザーがネットワークへのアクセスに成功すると、組織に有害な機密データを悪用します。

セキュリティの側面を強化し、ユーザーエクスペリエンスを向上させるために、Citrix Analytics は継続的なリスク評価のソリューションを導入しています。このソリューションは、Citrix Virtual Apps and Desktops または Citrix DaaS（旧 Citrix Virtual Apps and Desktops s サービス）を使用するユーザーのリスクにさらされるリスクを、ユーザーが毎回証明する必要なく、初期段階で検証されたときと同じ状態に保つことで、外部のサイバー犯罪者と悪意のある内部関係者の両方からデータを保護します。このソリューションは、セッション中に危険なイベントを継続的に評価し、組織のリソースがさらに悪用されるのを防ぐためのアクションを自動的に適用することで実現されます。



使用例

Adam Maxwell というユーザーについて考えてみましょう。Adam Maxwell は、通常の動作に反する異常な場所からのサインイン試行が複数回失敗した後、初めてネットワークにアクセスできました。また、この場所はサイバー攻撃の実績があります。このシナリオでは、Adam のアカウントがさらに悪用されないように、直ちに行動を取る必要があります。アダムのアカウントをロックして、実行されたアクションについて彼に通知することができます。このアクションは、ユーザーのアカウントに一時的にサービスの中断を引き起こす可能性があります。ユーザーは、管理者に連絡してアカウントを復元できます。

Adam が新しいデバイスと新しい IP から初めてネットワークにアクセスした別のシナリオを考えてみましょう。アダムに連絡して、このアクティビティを特定しているかどうかを確認することができます。もしそうなら、アダムが自分の作業デバイスを変更し、ホームネットワークから作業している可能性があります。このアクティビティは、組織のセキュリティに害を及ぼすものではなく、無視してもかまいません。ただし、ユーザーがこのアクティビティを実行しなかった場合は、アカウントが侵害されている可能性があります。このシナリオでは、ユーザーのアカウントをロックして、それ以上の損害を防ぐことができます。

主な機能

継続的なリスク評価は、ポリシーと可視性ダッシュボードに関連する機能の一部を自動化します。

複数の条件をサポートする

ポリシーを作成または変更する場合、最大 4 つの条件を追加できます。条件には、デフォルトのリスク指標とカスタムリスク指標、ユーザーリスクスコア、またはその両方の組み合わせを含めることができます。

詳細については、「ポリシーとは」を参照してください。

アクションを適用する前にユーザーに通知する

ユーザーのアカウントに適切なアクションを適用する前に、ユーザーに通知し、検出された異常なアクティビティの性質を評価できます。

詳細については、「エンドユーザーへの応答をリクエストする」を参照してください。

アクションの適用後にユーザーに通知する

一部のアクティビティでは、アクションを適用する前にユーザーの応答を待っていると、ユーザーのアカウントと Organization のセキュリティが危険にさらされる可能性があります。このようなシナリオでは、異常なアクティビティを検出したときに中断アクションを適用し、ユーザーに同じことを通知できます。

詳細については、「中断アクションを適用した後にユーザーに通知する」を参照してください。

強制モードと監視モード

要件に基づいて、ポリシーを強制モードまたは監視モードに設定できます。強制モードのポリシーは、ユーザーのアカウントに直接影響します。ただし、ポリシーを実装する前にポリシーの影響または結果を評価する場合は、ポリシーをモニタモードに設定できます。

詳細については、「サポートされるモード」を参照してください。

アクセスダッシュボードとポリシーダッシュボードの可視化

Access Summary ダッシュボードを使用すると、ユーザーによるアクセスの試行回数に関する洞察を得ることができます。詳細については、「アクセスの概要」を参照してください。

[ポリシーとアクション] ダッシュボードを使用すると、ユーザーアカウントに適用されているポリシーとアクションに関する洞察を得ることができます。詳細については、「ポリシーとアクション」を参照してください。

既定のポリシー

Citrix Analytics には、デフォルトでポリシーダッシュボードで有効になっている定義済みのポリシーが導入されています。これらのポリシーは、事前定義された条件としてリスク指標とユーザーリスクスコアを使用して作成されます。グローバルアクションは、すべてのデフォルトポリシーに割り当てられます。

> 注:
>
> 環境内に表示されるポリシーは、Citrix Analytics を初めて使用し始めた時期や、ローカルで変更を行ったかどうかによって異なる場合があります。

詳細については、「ポリシーとは」を参照してください。

次のデフォルトポリシーを使用することも、要件に基づいて変更することもできます。

ポリシー名	条件	データソース	アクション
認証情報の不正利用の成功	[過剰な認証失敗] と [疑わしいログオンリスク] インジケータがトリガーされたとき	Citrix Gateway	ユーザーのロック
データ流出の可能性	潜在的なデータ漏洩リスク指標がトリガーされたとき	Citrix Virtual Apps and Desktops および Citrix DaaS	ユーザーのログオフ
疑わしい IP からの異常なアクセス	「疑わしいログオン」および「疑わしい IP からのログオン」リスク指標がトリガーされたとき	Citrix Gateway	ユーザーのロック
デバイスからの初回アクセス	CVAD-新しいデバイスリスク指標からの初回アクセスがトリガーされたとき	Citrix Virtual Apps and Desktops および Citrix DaaS	エンドユーザーへの応答をリクエストする
アクセス中の移動は不可能	インポッシブル・トラベル・リスク・インジケーターがトリガーされたとき	Citrix Virtual Apps and Desktops および Citrix DaaS	エンドユーザーへの応答をリクエストする
認証では旅行不可能	インポッシブル・トラベル・リスク・インジケーターがトリガーされたとき	Citrix Gateway	エンドユーザーへの応答をリクエストする

ポリシーとアクション

December 7, 2023

> ** 注注意 **
>
> : シトリックスの Content Collaboration と ShareFile はサポート終了となり、ユーザーは使用できなくなります。

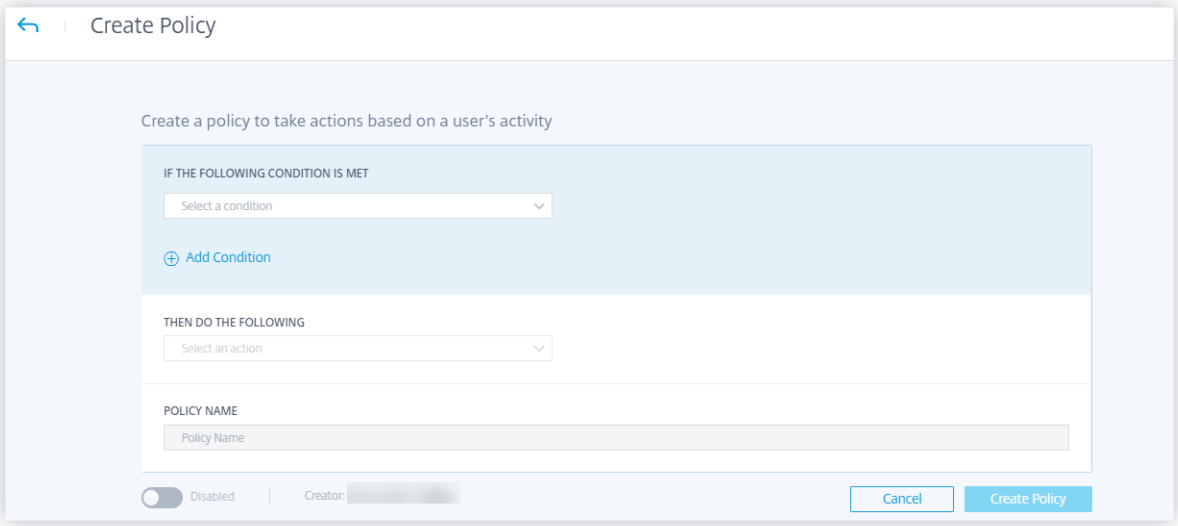
Citrix Analytics でポリシーを作成して、異常なアクティビティや疑わしいアクティビティが発生した場合にユーザーアカウントでアクションを実行するのに役立ちます。ポリシーを使用すると、ユーザーの無効化やウォッチリスト

へのユーザーの追加などのアクションを適用するプロセスを自動化できます。ポリシーを有効にすると、異常イベントが発生してポリシー条件が満たされた直後に、対応するアクションが適用されます。また、異常なアクティビティがあるユーザーアカウントにアクションを手動で適用することもできます。

どのようなポリシーがありますか

ポリシーは、アクションを適用するために満たす必要がある一連の条件です。ポリシーには、1 つ以上の条件と 1 つのアクションが含まれます。複数の条件と、ユーザーのアカウントに適用できる 1 つのアクションを含むポリシーを作成できます。

リスクスコア はグローバル条件です。グローバル条件は、特定のデータソースの特定のユーザーに適用できます。異常なアクティビティを示すユーザーアカウントを監視し続けることができます。その他の条件は、データソースとそのリスク指標に固有のものです。条件には、リスクスコア、デフォルトのリスク指標、およびカスタムリスク指標の組み合わせが含まれます。ポリシーを作成するときは、最大 4 つの条件を追加できます。



たとえば、組織で機密データを使用している場合、ユーザーが内部で共有またはアクセスするデータの量を制限できます。しかし、大規模な組織がある場合、1 人の管理者が多くのユーザーを管理および監視することは実現できません。機密データを過度に共有しているすべてのユーザーをウォッチリストに追加したり、アカウントをすぐに無効にしたりするポリシーを作成できます。

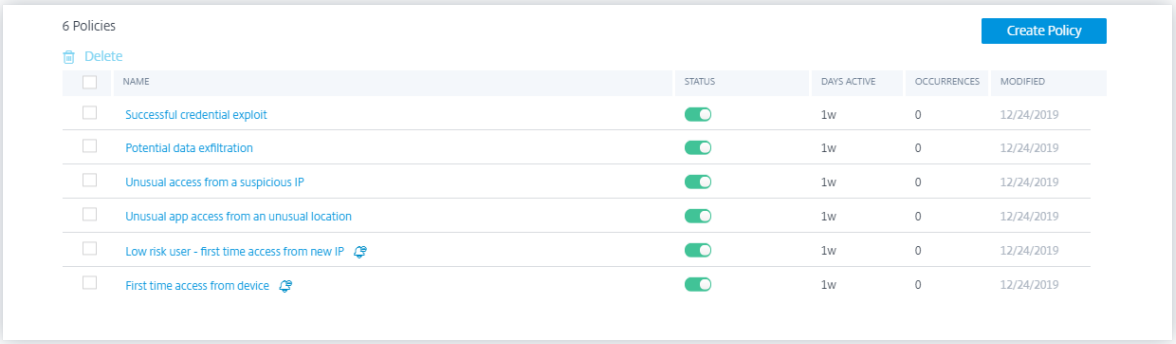
既定のポリシー

デフォルトのポリシーは、[ポリシー] ダッシュボードで事前に定義され、有効になっています。定義済みの条件に基づいて作成され、対応するアクションがすべてのデフォルトポリシーに割り当てられます。デフォルトポリシーを使用することも、要件に基づいて変更することもできます。

Citrix Analytics では、次のデフォルトポリシーがサポートされています。

- 認証情報の悪用が成功しました
- データ流出の可能性
- 疑わしい IP からの異常なアクセス
- デバイスからの初回アクセス
- Virtual Apps and Desktops、Citrix DaaS-アクセスできなければ移動不可能
- ゲートウェイ-認証では移動不可能

前述のデフォルトポリシーに関する事前設定された条件とアクションの詳細については、「継続的なリスク評価」を参照してください。



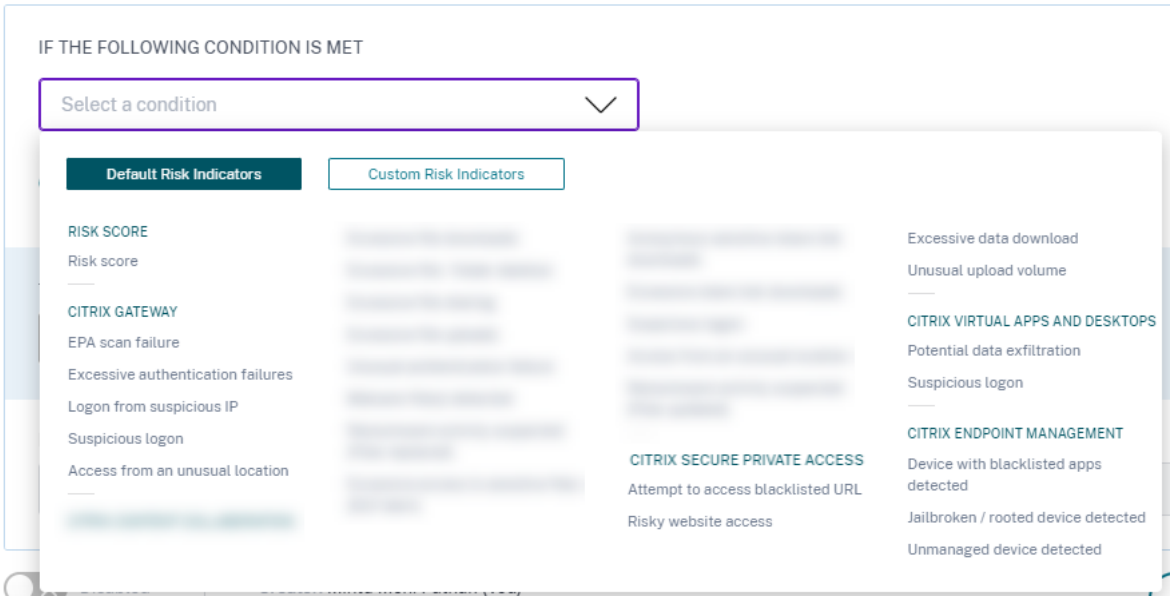
ジオフェンシングのユースケースの定義済みポリシーの詳細については、「構成済みポリシー」を参照してください。

条件を追加または削除するには

さらに条件を追加するには、［ポリシーの作成］ページの［次の条件が満たされる場合］セクションで［条件の追加］を選択します。条件を削除するには、条件の横に表示される [-] アイコンを選択します。

デフォルトリスク指標とカスタムリスク指標

条件メニューは、[ポリシーの作成] ページの [既定のリスク指標] タブと [カスタムリスク指標] タブに基づいて分離されています。これらのタブを使用すると、ポリシー設定の条件を選択するときに選択するリスク指標のタイプを簡単に識別できます。



アクションは何ですか

アクションは、将来の異常イベントの発生を妨げる疑わしいイベントへの応答です。異常な動作や疑わしい動作を表示するユーザーアカウントに対してアクションを適用できます。ユーザーのアカウントにアクションを自動的に適用するようにポリシーを構成するか、ユーザーのリスクタイムラインから特定のアクションを手動で適用できます。

Citrix データソースごとにグローバルアクションまたはアクションを表示できます。また、ユーザーに対して以前に適用したアクションをいつでも無効にできます。

> 注:
>
> リスク指標をトリガーするデータソースに関係なく、他のデータソースに関連するアクションを適用できます。

次の表に、実行できるアクションを示します。

アクション名	説明	適用可能なデータソース
グローバルアクション		
ウォッチリストに追加	将来の潜在的な脅威についてユーザーを監視する場合は、ウォッチリストに追加できます。	すべてのデータソース

アクション名	説明	適用可能なデータソース
	[ウォッチリストのユーザー] ペインには、アカウントでの 異常なアクティビティに基づいて潜在的な脅威を監視するすべてのユーザーが表示されます。組織のポリシーに基づいて、[ウォッチリストに追加] アクションを使用して、ユーザーをウォッチリストに追加できます。 ユーザーをウォッチリストに追加するには、ユーザーのプロフィールに移動し、[アクション] メニューから [ウォッチリストに追加] を選択します。[適用] をクリックして、アクションを適用します。	

アクション名	説明	適用可能なデータソース
管理者に通知	ユーザーに対してリスク指標がトリガーされると、管理者に手動で通知したり、自動通知のポリシーを作成したりできます。Citrix Cloud ドメインおよび組織内の他の Citrix Cloud 以外のドメインから管理者を選択できます。フルアクセス権を持つ Citrix Cloud 管理者の場合、デフォルトでは、Citrix Cloud アカウントの電子メール通知は無効になっています。電子メール通知を受信するには、Citrix Cloud アカウントで有効にします。詳細については、「メール通知を受信する」を参照してください。Security Analytics を管理するためのカスタムアクセス許可（読み取り専用およびフルアクセス）を持つ Citrix Cloud 管理者である場合、Citrix Cloud アカウントで電子メール通知が有効になります。Citrix Analytics からの電子メール通知の受信を停止するには、Citrix Cloud のフルアクセス管理者に、通知管理者の配布リストから自分の名前を削除するよう依頼します。の詳細については、「電子メール配布リスト」を参照してください。	
エンドユーザーへの応答をリクエストする	ユーザーのアカウントに異常なアクティビティや不審なアクティビティがある場合は、ユーザーがアクティビティを識別するかどうかを確認するようにユーザーに通知できます。アクティビティに基づいて、ユーザーのアカウントで実行する次のアクションを決定できます。詳細については、「エンドユーザーへの応答をリクエストする」を参照してください。	

アクション名	説明	適用可能なデータソース
エンドユーザーに通知	ユーザーのアカウントで異常または疑わしいアクティビティが発生した場合、電子メール通知でエンドユーザーに通知できます。詳細については、「エンドユーザーへの通知」を参照してください。	
NetScaler Gateway のアクション		
アクティブセッションをログオフする	アクションが適用されると、現在アクティブなユーザーセッションがログオフされます。将来のユーザーセッションはブロックされません。	NetScaler Gateway のオンプレミスおよび NetScaler Application Delivery Management
ユーザーアカウントをロック	異常な動作によりユーザーのアカウントがロックされると、Gateway 管理者がアカウントのロックを解除するまで、NetScaler Gateway ateway 経由でリソースにアクセスできなくなります。	NetScaler Gateway オンプレミス
ユーザーアカウントのロック解除	異常な動作が検出されなかったにもかかわらず、ユーザーのアカウントが誤ってロックされた場合、このアクションを適用してロックを解除し、アカウントへのアクセスを復元できます。	Citrix Gateway オンプレミス
Citrix Virtual Apps and Desktops と **Citrix DaaS** アクション		
アクティブセッションをログオフする	アクションが適用されると、現在アクティブなユーザーセッションがログオフされます。将来のユーザーセッションはブロックされません。	Citrix DaaS（旧称：Citrix Virtual Apps and Desktops サービス）

アクション名	説明	適用可能なデータソース
セッションの録画を開始	ユーザーの Virtual Desktops アカウントに異常なイベントが発生した場合、管理者はユーザーの現在のアクティブセッションの記録を開始できます。ユーザーが Citrix Virtual Apps and Desktops 7.18 以降のバージョンを使用していて、仮想セッションにログインしている場合、管理者は Citrix Analytics for Security からセッション記録開始アクションを動的にトリガーして、ユーザーの現在のアクティブなセッションの記録を開始できます。	Citrix DaaS（旧称：Citrix Virtual Apps and Desktops サービス）

> メモ
>
> - データソースに関係なく、リスク指標には任意のアクションを適用できます。
> - 管理者は、Citrix DaaS サイトで動的セッション記録アクションを実行したり、ユーザーの仮想セッションを動的に記録したりできるようになりました。
> - 匿名ユーザーは Active Directory に電子メールアドレスを持っていないため、「エンドユーザーへの応答を要求」および「エンドユーザーへの通知」アクションは適用できません。そのため、**Active Directory** と **Citrix**Cloud の間に確立された接続により、ユーザーのメールアドレスが Active Directoryで使用可能であることを確認してください。

表示専用共有

ユーザーのアカウントで「リンクを表示専用共有に変更」アクションを適用する前に、次の条件が満たされていることを確認します。

前提条件

- 管理者は、Content Collaboration で [リンクを変更して表示のみの共有] アクションを使用するには、Enterprise アカウントが必要です。
- 表示のみの共有は、Citrix Content Collaboration のエンタープライズアカウントでリクエストに応じて利用できる機能です。Citrix Analytics で［表示専用共有へのリンクの変更］アクションを適用する前に、ユーザーと管理者の Content Collaboration エンタープライズアカウントで［表示のみの共有］機能が既に有効になっていることを確認してください。詳しくは、Citrix サポート記事「CTX208601」を参照してください。

サポートされているファイルタイプ　表示のみの共有アクションは、次のファイルタイプにのみ適用されます。

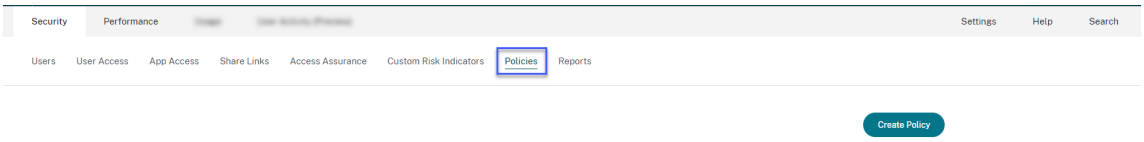
- Microsoft Office ファイル
- PDF
- イメージファイル (SZC v3.4.1 以降が必要):
  - BMP
  - GIF
  - JPG
  - JPEG
  - PNG
  - TIF
  - TIFF
- Citrix が管理するストレージゾーンに保存されているオーディオおよびビデオファイル。

ポリシーとアクションの構成

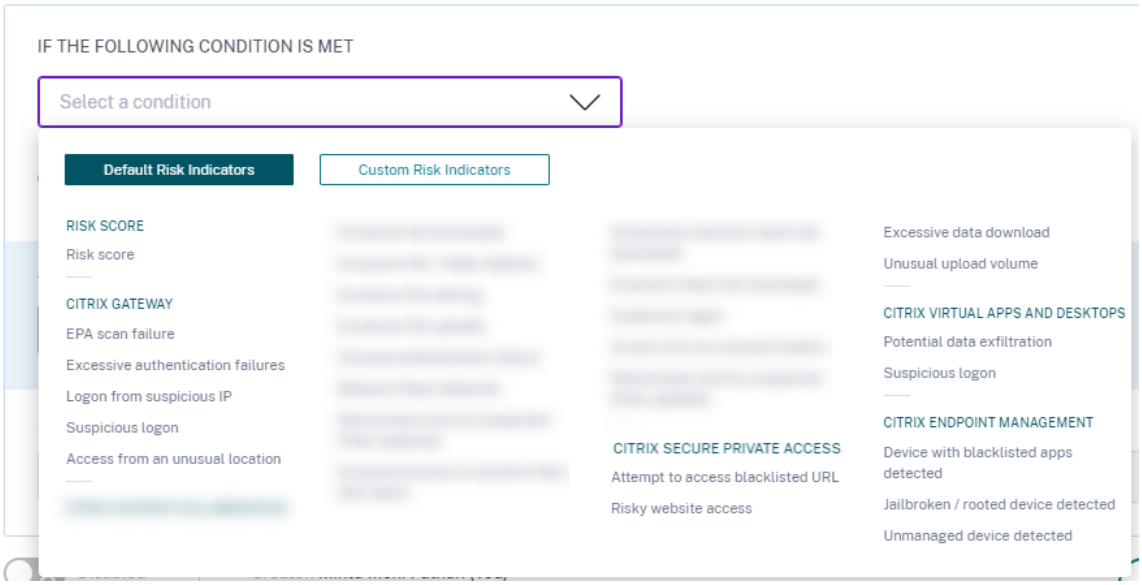
たとえば、以下の手順に従って、過剰なファイル共有ポリシーを作成できます。このポリシーを使用すると、組織内のユーザーが異常に大量のデータを共有すると、共有リンクは自動的に期限切れになります。ユーザーがそのユーザーの通常の動作を超えるデータを共有すると、通知されます。過剰なファイル共有ポリシーを適用し、即座に対処することで、ユーザーのアカウントからのデータの漏洩を防ぐことができます。

ポリシーを作成するには、次の手順を実行します。

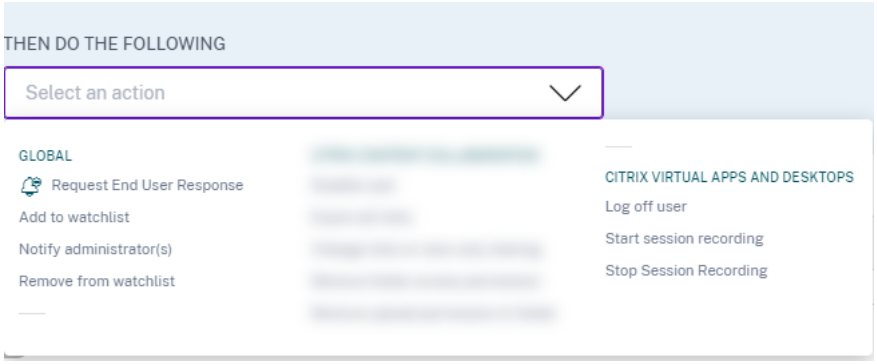
1. Citrix Analytics にサインインしたら、[セキュリティ] **>** [ポリシー] **>** [ポリシーの作成] の順に選択します。



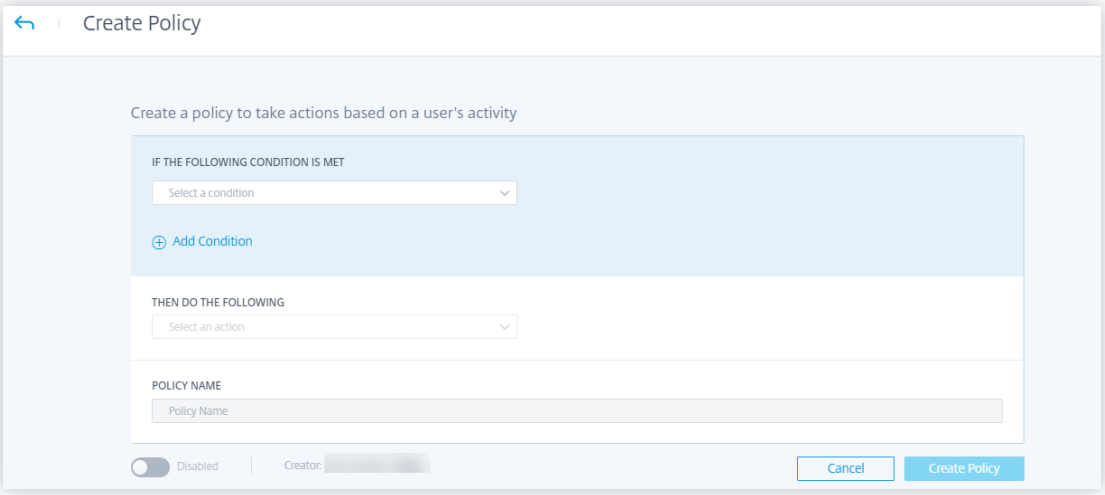
2. [次の条件が満たされている場合] リストボックスから、アクションを適用する既定のリスク指標条件またはカスタムリスク指標条件を選択します。



3. 「次に実行する」リストから、アクションを選択します。



4. [**Policy Name**] テキストボックスに名前を入力し、表示されるトグルボタンを使用してポリシーを有効にします。



5. [ポリシーの作成] をクリックします。

ポリシーを作成すると、ポリシーが [ポリシー（**Policies**）] ダッシュボードに表示されます。

［ポリシー］ダッシュボードには、正常に検出され、Citrix Analytics に接続されたデータソースに関連付けられたポリシーが表示されます。ダッシュボードには、未検出のデータソースに対して条件が定義されているポリシーは表示されません。

ただし、すでに接続されているデータソースのデータ処理をオフにしても、**[**ポリシー**]** ダッシュボードの既存のポリシーには影響しません。

エンドユーザーへの応答をリクエストする

エンドユーザー応答のリクエストは、Citrix アカウントで異常なアクティビティを検出した直後にユーザーに警告できるグローバルアクションです。アクションを適用すると、ユーザーに電子メール通知が送信されます。ユーザーは、自分の活動の正当性について電子メールで返信する必要があります。

ユーザーに適用するアクションを決定します。

ユーザーの応答に基づいて、次のアクションコースを決定できます。「ウォッチリストに追加」、「管理者に通知」などのグローバルアクションを適用できます。または、Citrix Gateway-ユーザーのロックなど、データソース固有のアクションを適用することもできます。

ユーザーが報告されたアクティビティを実行したという応答を受け取った場合、そのアクティビティは疑わしくなく、ユーザーのアカウントに対してアクションを実行する必要はありません。ユーザーにセキュリティアラートを送信できる 1 日あたりの上限は、3 通です。

Citrix Content Collaboration ユーザーで、80 分間のリスクスコアが 80 を超えたとします。この異常な動作についてユーザーに警告するには、「エンドユーザーレスポンスを要求」アクションを適用します。セキュリティアラートは、電子メール ID `security-analytics@cloud.com`からユーザーに送信されます。

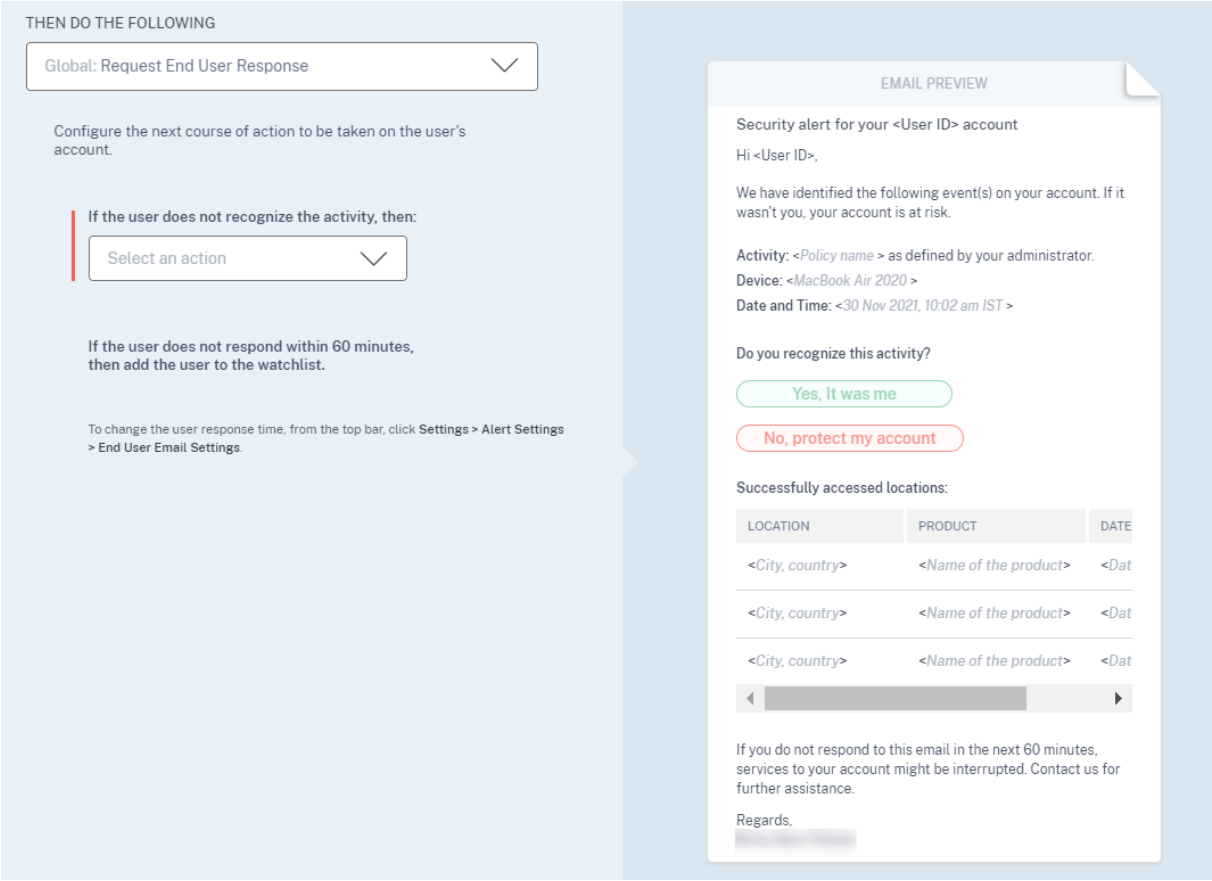
電子メールには次の情報が含まれています。

- リスク指標をトリガーしたユーザーのアクティビティ
- ユーザーのデバイス
- ユーザーアクティビティの日時
- 製品またはサービスに正常にアクセスできる場所（都市および国）。都市または国が使用できない場合、対応する値は「不明」と表示されます。

エンドユーザー応答 の要求アクションがユーザーのリスクタイムラインに追加されます。

Citrix アカウントで検出されたアクティビティをユーザーが認識しない場合、Citrix Analytics は定義したアクションを適用します。

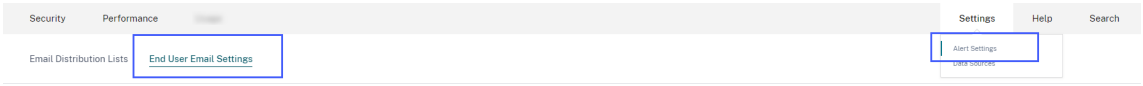
電子メールを受信してから 1 時間以内にユーザーが応答を送信しなかった場合、Citrix Analytics はそのユーザーをウォッチリストに追加します。ユーザーとそのアカウントに不審なアクティビティがないか監視し、それに応じてアクションを実行できます。



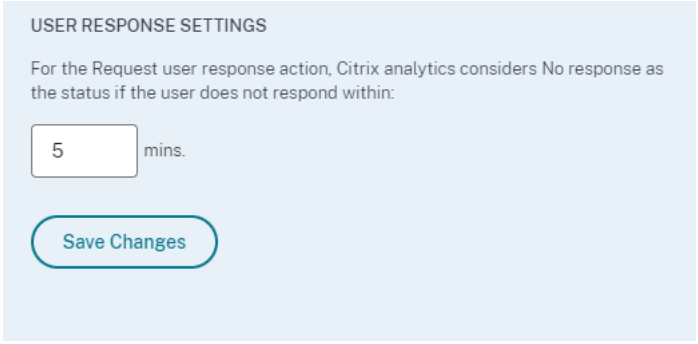
ユーザーの応答時間を設定する方法は　セキュリティ警告メールに対するユーザーの応答時間を設定できます。指定された期間内に報告されたアクティビティにユーザーが応答しない場合、そのユーザーは監視対象のウォッチリストに追加されます。

ユーザーの応答時間を設定する手順は、次のとおりです。

1. 設定 **>** アラート設定 **>** エンドユーザーメール設定をクリックします。



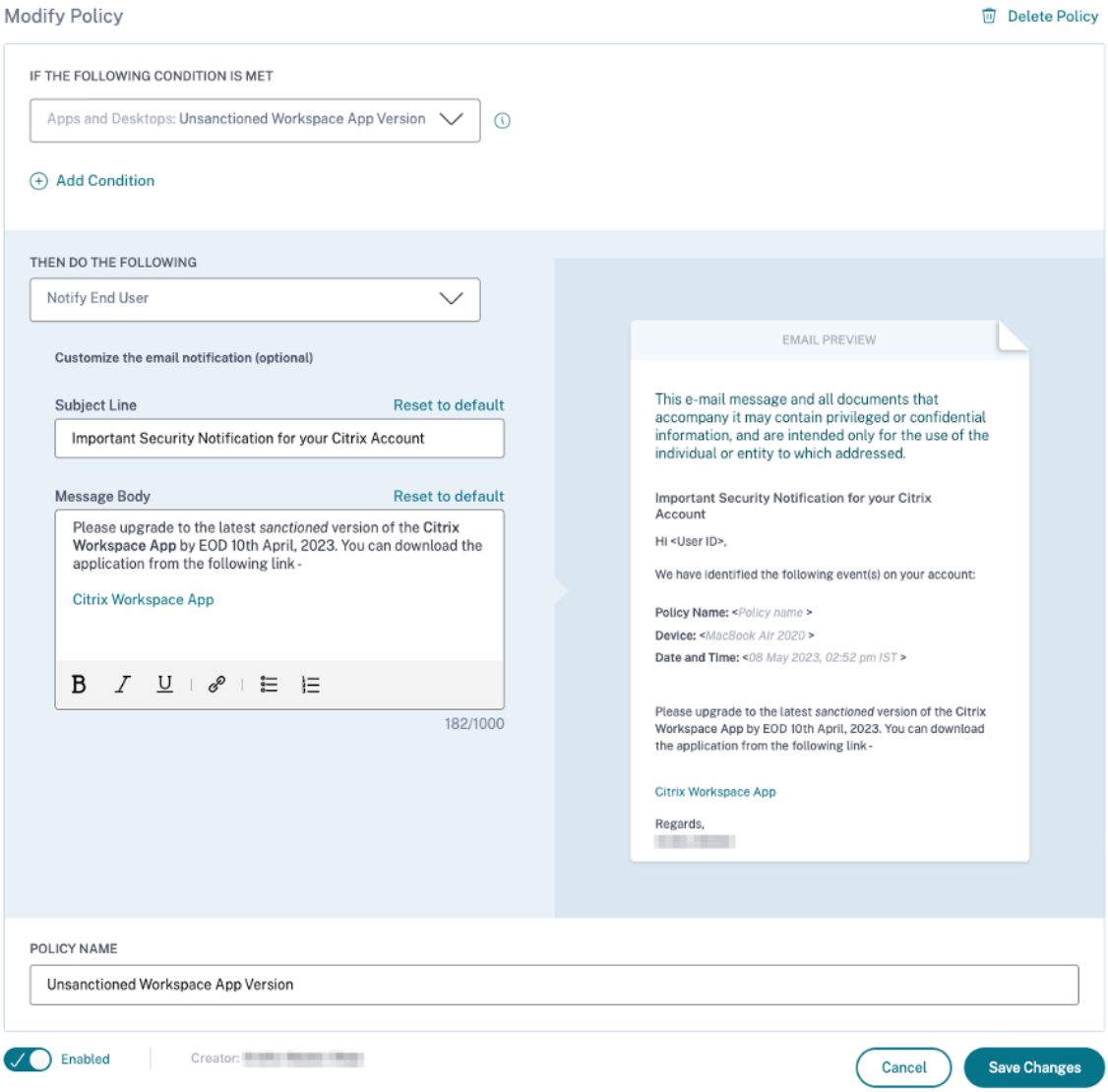
2. [エンドユーザの電子メール設定] ページで、テキストボックスに分数を入力します。



3. ［変更の保存］をクリックします。

また、セキュリティ警告メールにバナー、ヘッダーテキスト、フッターテキストを追加して、正当に見えるようにしたり、ユーザーの注意を引いたり、応答時間を長くしたりすることもできます。詳細については、「エンドユーザーのメール設定」を参照してください。

エンドユーザーに通知　エンドユーザーへの通知は、エンドユーザーの Citrix アカウントで異常または疑わしい動作が検出されたときに、エンドユーザーに電子メール通知を送信できるグローバルアクションです。メールの件名とメッセージ本文はカスタマイズ可能です。ポリシーがトリガーされた後にアクションが適用されると、ユーザーに電子メール通知が送信されます。エンドユーザーからの応答は要求されず、ユーザーのアカウントに対して破壊的なアクションは実行されません。



このアクションは、組み込みまたはカスタムのリスク指標トリガーに基づいて、さまざまなコンプライアンスユース

ケースに対応するのに役立ちます。メールの件名と本文はカスタマイズ可能なため、エンドユーザーへの通知の一般的なユースケースの多くにも柔軟に対応できます。これらのユースケースでは、ユーザーのアカウントで応答や混乱を招くようなアクションを実行する必要がありません。

電子メールには次の情報が含まれています。

- アクションに関連するポリシー名。
- ユーザーのデバイス (利用可能な場合)
- ユーザーアクティビティの日時

エンドユーザーへのメール通知は、電子メール ID `security-analytics@cloud.com`から送信されます。

> 注:
>
> 各ポリシーでの 1 日の上限は、1 ユーザーあたり **3** 通のメールです。このしきい値を超えると、アクションは適用されず、エンドユーザーには電子メール通知は送信されません。アクションはユーザーのタイムラインビューに表示され、「ユーザーの **1** 日あたりのメールの上限に達しました」というメッセージが表示されます。

アクションはユーザーのリスクタイムラインに追加されます。ただし、これは手動操作ではないため、タイムラインビューからユーザーに適用することはできません。

エンドユーザーのメールコンテンツのカスタマイズ　以前は、Citrix Analytics の管理者がエンドユーザーに手動で連絡して、疑わしいアクティビティの検出に関する修正手順を提供していましたが、インシデントをクローズするには時間のかかるプロセスでした。

エンドユーザーへの応答要求、エンドユーザーへの通知、および情報メールに、エンドユーザーの電子メールコンテンツのカスタマイズ機能が導入されました。エンドユーザーへの返信メールは、ユーザーの検証/応答を求めていますが、情報メールには、疑わしいアクティビティの種類と、すでに実行された修復アクションの種類が表示されます。エンドユーザーへの通知メールは、エンドユーザーに返信を求めることなく、Citrix アカウントでのコンプライアンス違反や疑わしいアクティビティについてエンドユーザーに通知します。

エンドユーザーのメールコンテンツのカスタマイズ機能を使用すると、**Citrix Analytics** 管理者は、エンドユーザーへの応答要求/エンドユーザーへの通知/情報メール本文テンプレートにカスタムメッセージを追加できます。リッチテキストボックスエディタを使用すると、管理者は太字、斜体、ハイパーリンクなどのさまざまな編集ツールを使用して、ポリシーごとにコンテンツを変更できます。

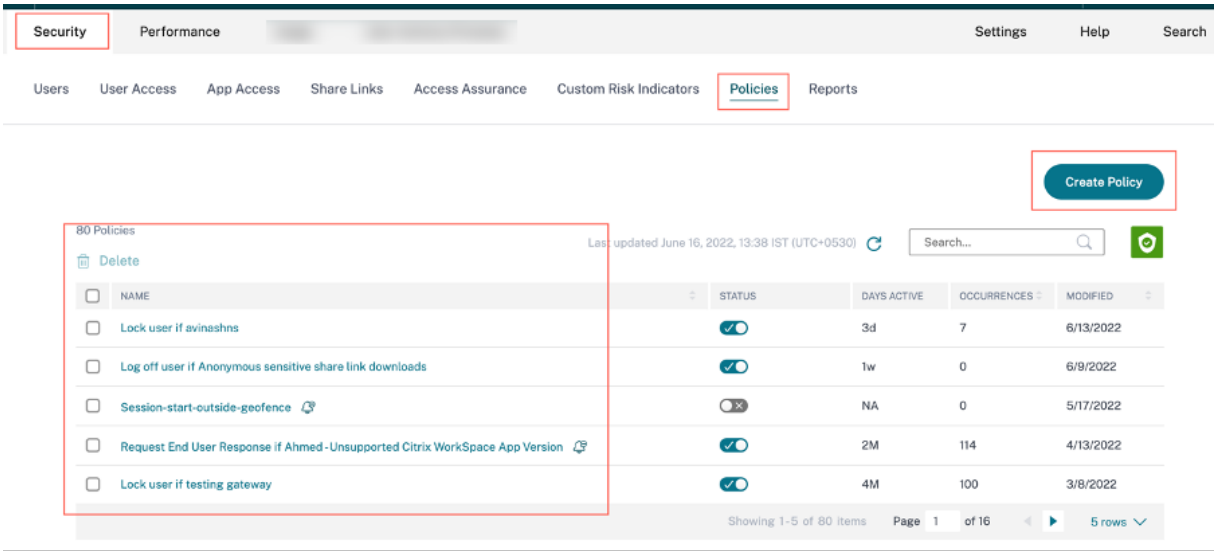
> 注:
>
> エンドユーザーの電子メールコンテンツのカスタマイズ機能は、ポリシーベースのアクションでのみ使用でき、手動アクションには使用できません 。

次の 3 種類のメールの内容をカスタマイズできます。

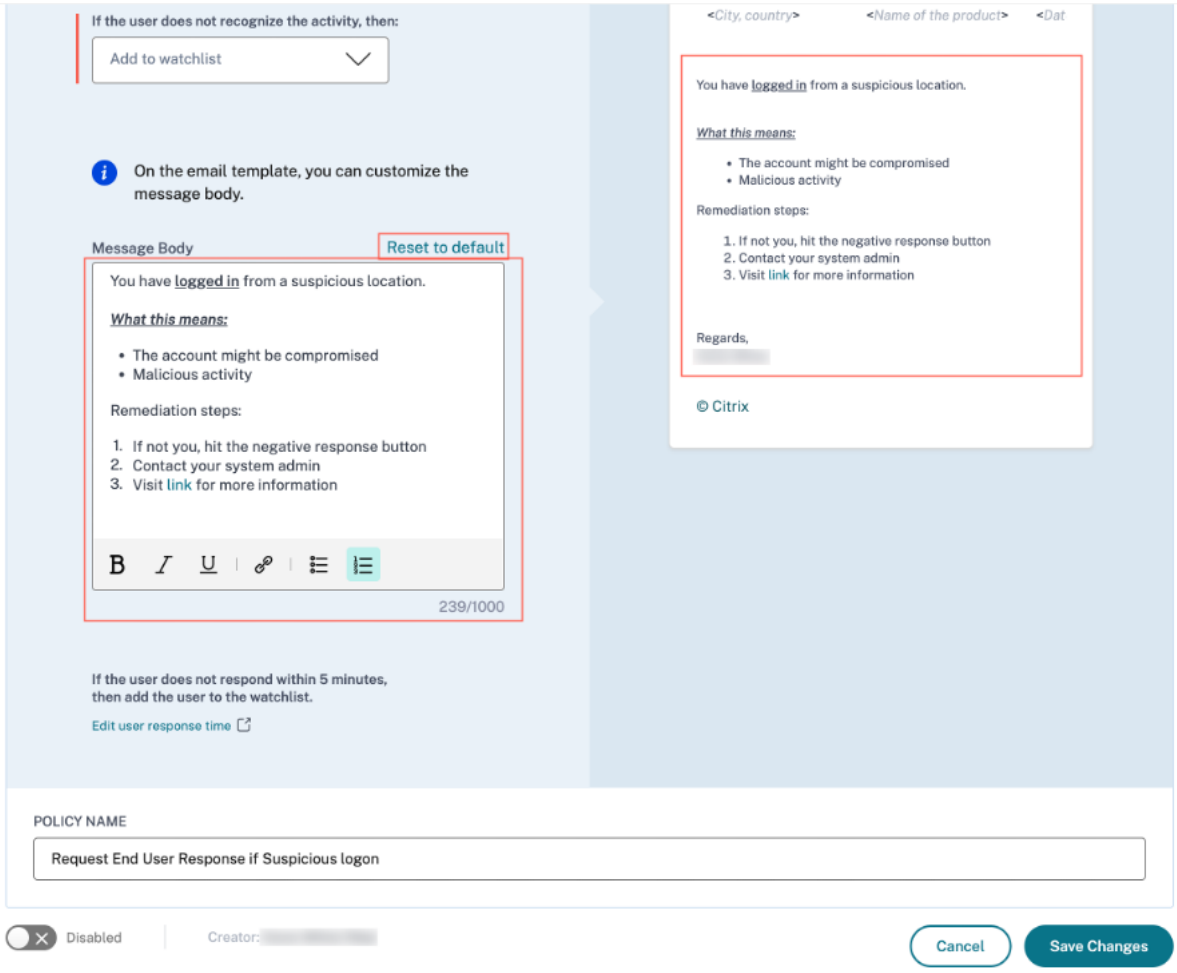
- エンドユーザーからの返信メールをリクエストします。

- エンドユーザーへのメール通知
- 以下のエンドユーザーアクションのいずれかが実行された場合に送信される電子メール。
  - ［**Citrix** アプリとデスクトップ］の下のログオフアクション
  - ログオフして **NetScaler Gateway** でユーザーをロックする

ポリシーのリストは、[セキュリティ **] > [** ポリシー] タブで表示できます。



既存のポリシーをクリックするか、新しいポリシーを作成する際に、カスタマイズされたメール本文を表示できます。右側のペインには、更新された電子メールコンテンツのプレビューが表示されます。



> 注
>
> - 管理者は、「デフォルトにリセット」リンクをクリックして、コンテンツをデフォルトテンプレートに設定できます。カスタムボディの文字数制限は 1000 です。
> - 「エンドユーザーに通知」アクションでは、「件名」フィールドも管理者がカスタマイズできます。「デフォルトにリセット」リンクをクリックすると、デフォルトにリセットできます。カスタムメールの件名の文字制限は 500 文字です。

[**Save Changes**] をクリックして、ポリシーを作成/更新します。ポリシーがトリガーされると、次の電子メール通知がエンドユーザーに送信されます。

- エンドユーザー応答メールのリクエスト: ユーザー応答を要求するメールを送信するポリシーアクションです。
- エンドユーザーへの通知メール: エンドユーザーに、Citrix アカウントでのコンプライアンス上の問題や疑わしいアクティビティなどを知らせるメール通知です。
- 情報メール: エンドユーザーのアクション後に送信される情報メール。

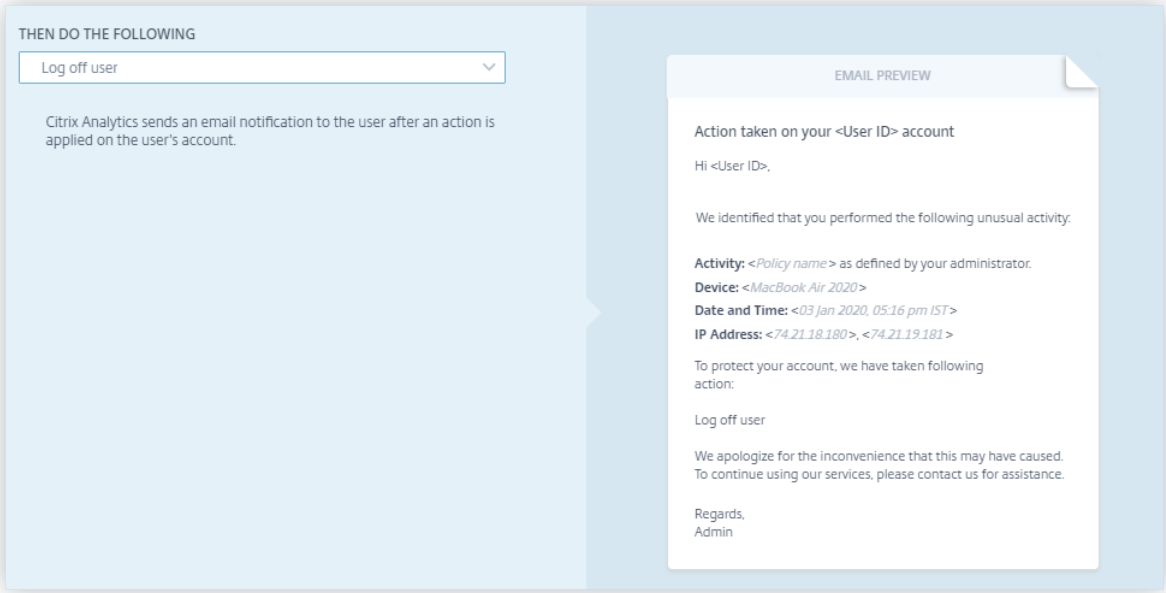
エンドユーザーは電子メールを読み、管理者の要求に応じて修復アクションを完了できます。

> 注:
>
> 読み取り専用アクセス権を持つ管理者は、メール本文を編集/追加できません。

中断を伴うアクションを適用した後にユーザーに通知する

このアクションタイプでは、異常なアクティビティが検出されたときに、ユーザーのログオフやユーザーのロックなどの中断を伴うアクションをユーザーのアカウントに適用できます。ユーザーのアカウントにアクションが適用されると、そのアカウントへのサービスが中断される場合があります。そのような場合、ユーザーは以前のように自分のアカウントにアクセスできるように管理者に連絡する必要があります。

Citrix Content Collaboration ユーザーで、80 分間のリスクスコアが 80 を超えたとします。ユーザーをログオフできます。このタスクを実行すると、ユーザーは自分のアカウントにアクセスできなくなり、電子メール ID `security-analytics@cloud.com`から電子メール通知がユーザーに送信されます。電子メールには、アクティビティ、デバイス、日付と時刻、IP アドレスなどのイベントの詳細が含まれています。ユーザーは、以前のように管理者に連絡してアカウントにアクセスする必要があります。

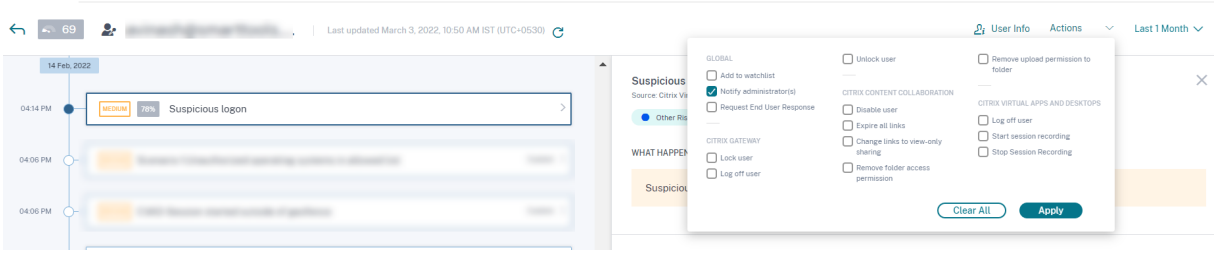


アクションを手動で適用する

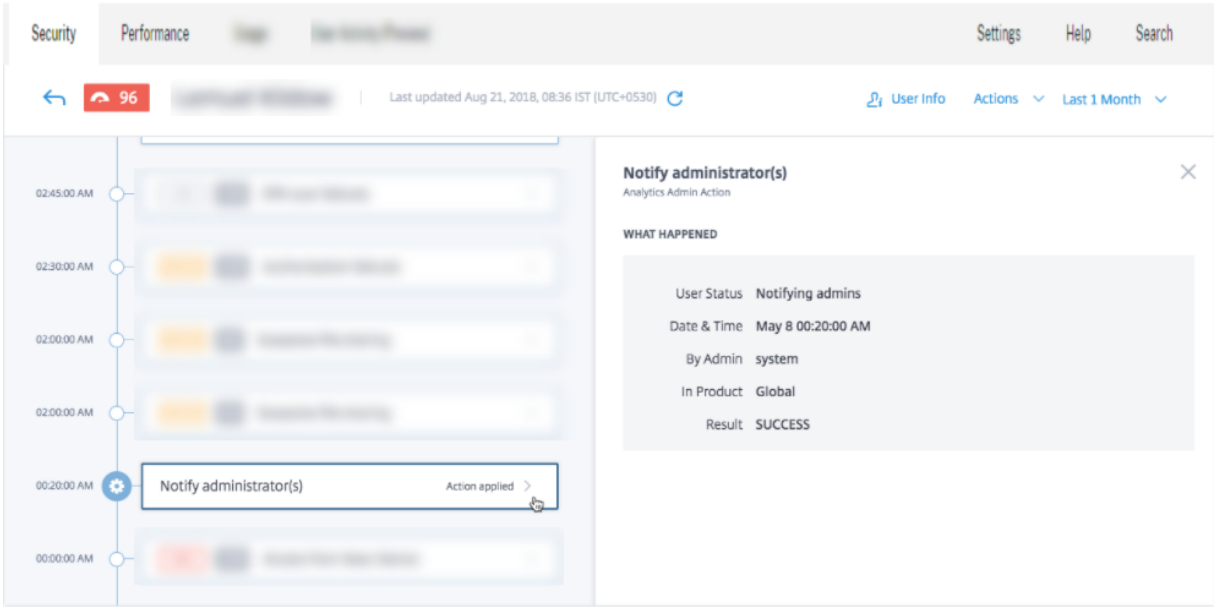
新しいデバイスを使用して初めてネットワークにサインインするユーザー Lemuel を考えてみましょう。彼女の行動が異常であるために彼女のアカウントを監視するには、[管理者に通知] アクションを使用できます。

アクションをユーザーに手動で適用するには、次の操作を行う必要があります。

ユーザーのプロファイルに移動し、適切なリスク指標を選択します。[アクション] メニューから、[管理者に通知] アクションを選択し、[適用] をクリックします。



アカウントを監視するために、すべての管理者または選択した管理者に電子メール通知が送信されます。適用されたアクションがリスクタイムラインに追加され、アクションの詳細がリスクタイムラインページの右ペインに表示されます。



メモ

- フルアクセス権を持つ Citrix Cloud 管理者の場合、デフォルトでは、Citrix Cloud アカウントの電子メール通知は無効になっています。電子メール通知を受信するには、Citrix Cloud アカウントで有効にします。詳細については、「メール通知を受信する」を参照してください。
- Security Analytics を管理するためのカスタムアクセス許可（読み取り専用およびフルアクセス）を持つ Citrix Cloud 管理者である場合、Citrix Cloud アカウントで電子メール通知が有効になります。Citrix Analytics からの電子メール通知の受信を停止するには、Citrix Cloud のフルアクセス管理者に、通知管理者の配布リストから自分の名前を削除するよう依頼します。の詳細については、「電子メール配布リスト」を参照してください。

ポリシーの管理

ポリシーダッシュボードを表示して、Citrix Analytics で作成されたすべてのポリシーを管理して、ネットワーク上の不整合を監視および識別できます。[ポリシー] ダッシュボードでは、次の操作を実行できます。

1. ポリシーのリストを表示する
2. ポリシーの詳細
    - ポリシーの名前
    - ステータス—有効または無効。
    - ポリシーの期間：ポリシーがアクティブまたは非アクティブであった日数。
    - 発生回数—ポリシーがトリガーされた回数。
    - Modified —ポリシーが変更された場合のみタイムスタンプ。
3. ポリシーを削除する
    - ポリシーを削除するには、削除するポリシーを選択し、[**Delete**] をクリックします。
    - または、ポリシーの名前をクリックして、[ポリシーの変更] ページにリダイレクトできます。[ポリシーの削除] をクリックします。ダイアログで、ポリシーを削除するリクエストを確認します。
4. ポリシーを作成する
5. ポリシーの名前をクリックすると、詳細が表示されます。ポリシーの名前をクリックしたときに、ポリシーを変更することもできます。他に実行できる変更は次のとおりです。
    - ポリシーの名前を変更します。
    - ポリシーの条件。
    - 適用されるアクション。
    - ポリシーを有効または無効にします。
    - ポリシーを削除します。

> 注
>
> - ポリシーを削除したくない場合は、ポリシーを無効にすることができます。
> - [ポリシー] ダッシュボードでポリシーを再度有効にするには、次の手順を実行します。
>   - On the Policies dashboard, click the **Status** slider button and refresh the page. The **Status** slider button turns green.
>   - On the Modify Policy page, click the **Enabled** slider button on the bottom of the page.

サポートされるモード

Citrix Analytics は、次のポリシーモードをサポートしています。

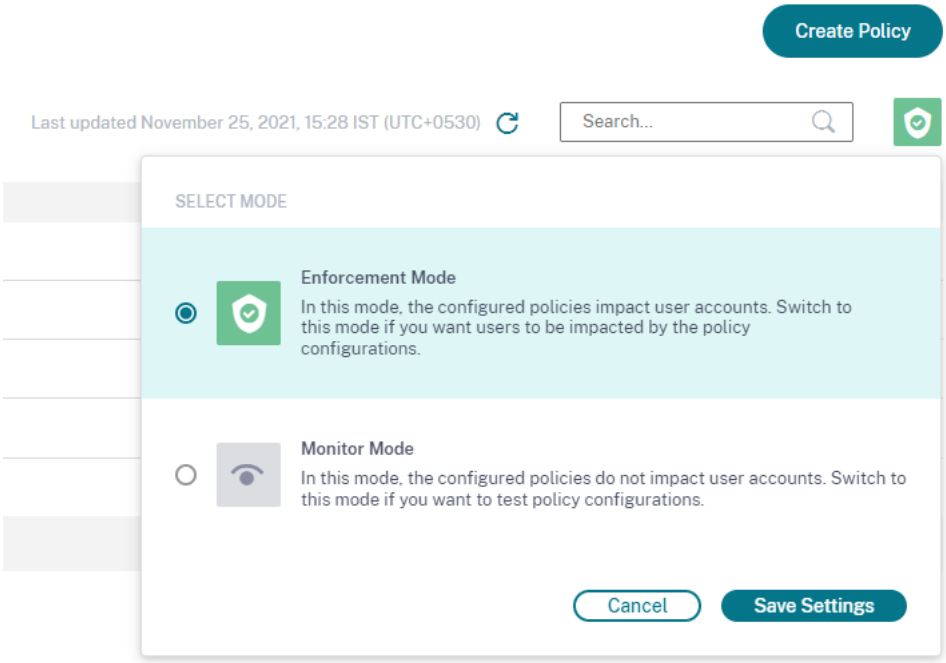
- 強制モード -このモードでは、構成されたポリシーがユーザーアカウントに影響します。

- モニタモード -このモードでは、設定されたポリシーはユーザアカウントに影響を与えません。ポリシー設定をテストする場合は、ポリシーをこのモードに設定できます。

次の手順に従って、ポリシーのモードを設定します。

1. [セキュリティ] > [ポリシー] に移動します。
2. ポリシーページで、検索バーの横に表示されている右上隅のアイコンを選択します。**[**モードを選択**]** ウィンドウが表示されます。
3. 目的のモードを選択し、[設定の保存] をクリックします。

> 注
>
> Analytics によって作成されたデフォルトのポリシーは、監視モードに設定されます。その結果、既存のポリシーもこのモードを継承します。すべてのポリシーの影響をまとめて評価し、強制モードに変更できます。



ポリシーのセルフサービス検索

[セルフサービス検索 （Self-Service Search）] ページでは、ポリシーで定義されている条件を満たしたユーザーイベントを表示できます。このページには、これらのユーザーイベントに適用されたアクションも表示されます。適用されたアクションに基づいてユーザーイベントをフィルタリングします。

事前設定されたカスタムリスクインジケーターとポリシー

December 7, 2023

Citrix Analytics for Security には、事前構成されたカスタムリスク指標のリストと 、Citrix インフラストラクチャのセキュリティを監視するのに役立つポリシーが用意されています 。これらの事前設定されたカスタムリスク指標とポリシーの条件は、侵害されたユーザー、内部者の脅威、データ漏洩などの特定のセキュリティリスクシナリオに従って既に定義されています。また、これらの事前構成済みの条件を変更したり、セキュリティ要件に応じて独自の条件を追加し、カスタムリスク指標を使用してリスクを軽減することもできます。

現在、事前設定されたカスタムリスク指標は、次のシナリオで使用できます。

- ジオフェンシング
- 初回アクセス

ジオフェンシングシナリオの事前設定されたカスタムリスク指標

以下の事前設定されたカスタムリスク指標を使用して、ジオフェンスエリア外からのユーザーイベントを検出します。

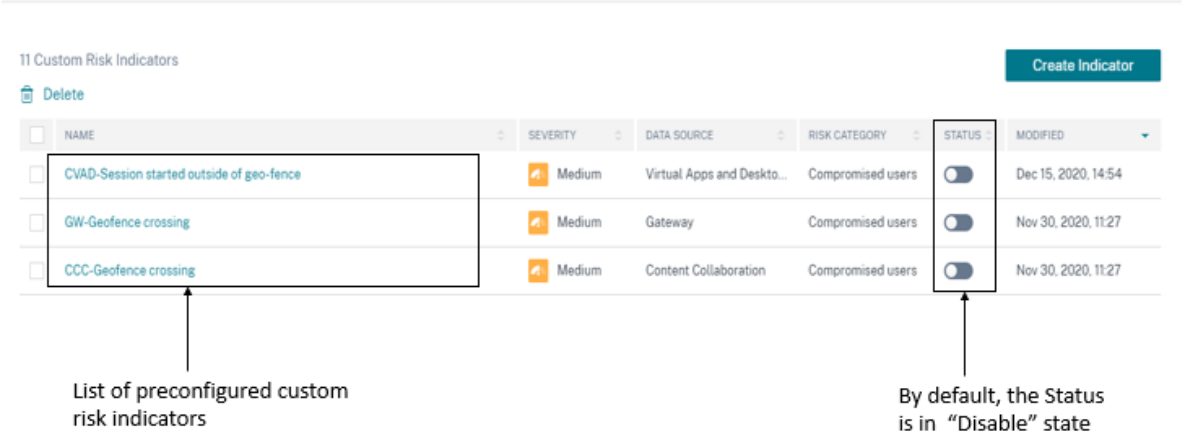
- CVAD-セッションがジオフェンスの外で開始されました
- GW-ジオフェンスクロッシング

事前構成されたカスタムリスク指標は、ユーザーが通常の運用国またはジオフェンスの外部から Citrix 製品にアクセスするたびにトリガーされます。デフォルトでは、ジオフェンスは「米国」に設定されています。必要な国をジオフェンスとして設定できます。

> （注
>
> ）ジオフェンスのリスクインジケータの外で開始された *CVAD* セッションは、アクセス保証ロケーション機能のジオフェンス設定にリンクされています。したがって、リスク指標の状態でジオフェンスされた国を直接変更することはできません。リスク指標でジオフェンスされた国を更新するには、[アクセス保証ロケーション] ダッシュボードの [ジオフェンスの設定] で国を選択します。詳細については、アクセス保証ロケーションダッシュボードを参照してください。

事前設定されたカスタムリスク指標を表示するには、[セキュリティ] **>** [カスタムリスク指標] を選択します。

デフォルトでは、事前設定されたカスタムリスク指標は無効になっています。**STATUS** ボタンを使用して有効にします。



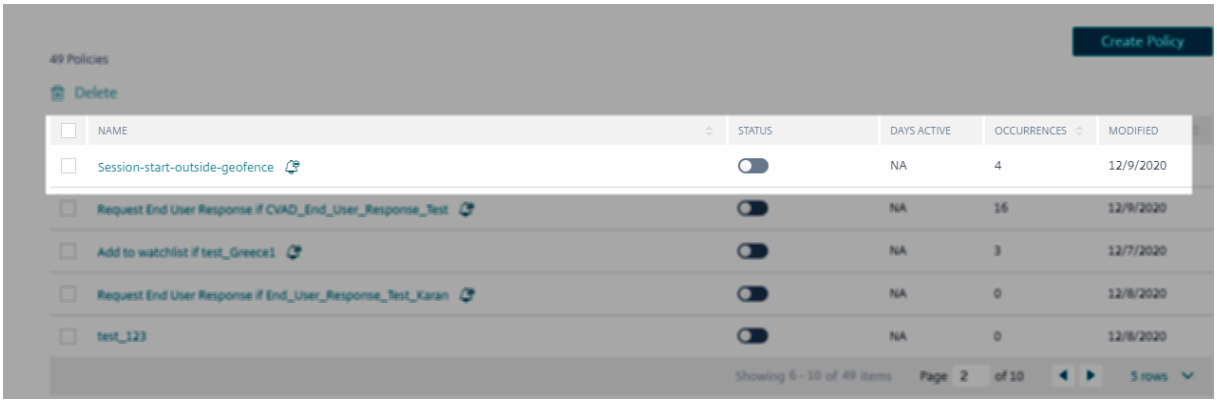
次の表に、ジオフェンスの事前構成済みのさまざまなカスタムリスク指標を示します。

カスタムリスク指標名	シナリオ	カスタムインジケーター条件	データソース	リスクカテゴリ
CVAD-セッションがジオフェンスの外で開始されました	ユーザーが操作する国以外で仮想セッションを開始しました	Event-Type = session.Logon Country! =「アメリカ合衆国」	Citrix Workspace アプリ	侵害されたユーザー
GW-ジオフェンスクロッシング	ユーザーは、自国のオペレーション国外からの認証に成功しました	Event-Type =「VPN_AI」と国! =「アメリカ合衆国」	NetScaler Gateway (オンプレミス)	侵害されたユーザー

ジオフェンシングシナリオの事前設定されたポリシー

シトリックスには、ユーザーが運用国以外から仮想セッションを開始するたびに、ユーザーアカウントに「エンドユーザー応答の要求」アクションを適用する構成済みのポリシーが用意されています。ユーザーは電子メールを受信し、ユーザーの応答に基づいて、ユーザーをウォッチリストに追加したり、追加のアクションを管理者に通知するなど、適切なアクションが実行されます。詳細については、「エンドユーザーへの応答をリクエストする」を参照してください。

構成済みのポリシーを表示するには、[セキュリティ] **>** [ポリシー] を選択します。



次の表に、ジオフェンシングの事前設定されたポリシーについて説明します。

ポリシー名	シナリオ	ポリシー条件	適用されたアクション
ジオフェンス外でのセッション開始	ユーザーが操作国外で仮想セッションを開始したときに、管理者が「エンドユーザー応答のリクエスト」アクションを通じてユーザーの正当性を検証する機能	事前設定されたカスタムリスクインジケータ-「ジオフェンスの外部で開始された CVAD-セッション」とともに使用します	エンドユーザー応答のリクエスト 次のユーザーの応答に基づいて、対応するアクションが適用されます。 ユーザーがアクティビティを認識しない場合: ウォッチリストに追加する ユーザーがアクティビティを認識した場合: アクションは不要 ユーザーがメールを受信してから 60 分以内に応答しない場合: ユーザーをウォッチリストに追加します。

> 注
>
> エンドユーザー応答のリクエストアクションは、米国リージョンでのみサポートされています。そのため、組織が Citrix Cloud の欧州連合リージョンにオンボーディングされている場合、事前構成されたポリシーはアカウントに適用されません。事前設定されたポリシーを使用するには、ポリシーを変更して、選択した別のアクションを選択します。

ジオフェンシングのカスタムリスク指標を事前に構成して独自のポリシーを作成する

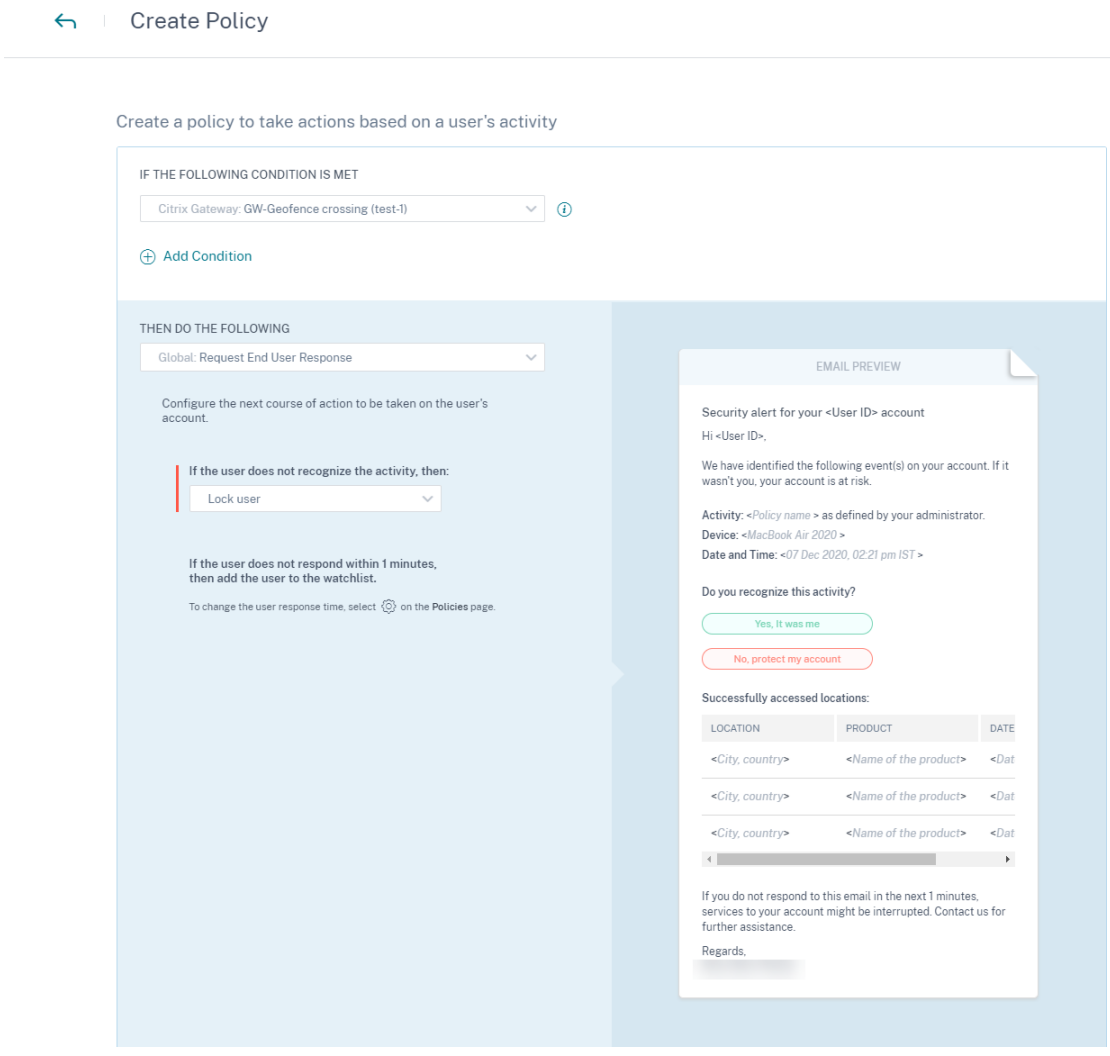
また、これらの事前設定されたカスタムリスク指標を使用して独自のポリシーを作成し、指標がトリガーされるたびにユーザーのロックやユーザーのログオフなどのアクションを適用することもできます。ポリシーの作成方法については、「ポリシーとアクションの構成」を参照してください。

次の例は、米国外から Citrix サービスにアクセスしようとするユーザーをロックするポリシーを示しています。ユーザーがアクセスアクティビティを認識しない場合、ユーザーアクセスはロックされます。

条件:GW-Geofence 交差点

アクション: エンドユーザーの応答をリクエストする

次のアクション: ユーザーがアクティビティを認識しない場合、ユーザーをロックする



> 注
>
> エンドユーザー応答のリクエストアクションは、米国リージョンでのみサポートされています。したがって、組

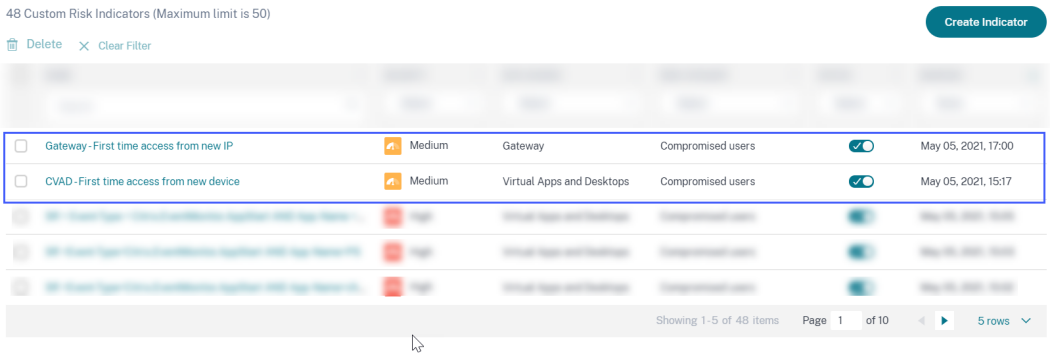
> 織が欧州連合地域にオンボーディングされている場合は、エンドユーザー応答の要求 アクションではなく、選択した別のアクションを選択してください。

初回アクセスシナリオ用に事前設定されたカスタムリスク指標

次のカスタムリスク指標を使用して、初回アクセスシナリオのユーザーイベントを検出します。

- CVAD-新しいデバイスからの初回アクセス
- 新しい IP からのゲートウェイファーストタイムアクセス

デフォルトでは、これらの事前設定されたカスタムリスク指標は有効状態です。**STATUS** ボタンを無効にするには、[STATUS] ボタンを使用します。



次の表は、初回アクセス用に事前設定されたカスタムリスク指標を示しています。

カスタムインジケータ名	シナリオ	事前構成された条件	データソース	リスクカテゴリ
CVAD-新しいデバイスからの初回アクセス	Citrix Workspace アプリユーザーが次のいずれかからサインインすると:	デフォルトでは、次の条件が有効になっています。	Citrix Virtual Apps and Desktops オンプレミスと Citrix DaaS（旧 Citrix Virtual Apps and Desktops サービス）	侵害されたユーザー
	新しいデバイス	新しいデバイス ID を初めて使用する。		

カスタムインジケータ名	シナリオ	事前構成された条件	データソース	リスクカテゴリ
	過去 90 日間使用されていない既存のデバイス。	`Event-Type = "Session.Logon"AND Client-Type IN ("XA.Receiver.Windows", "XA.Receiver.Mac", "XA.Receiver.Chrome", "XA.Receiver.Android", "XA.Receiver.Linux", "XA.Receiver.iOS")`		
新しい IP からのゲートウェイファーストタイムアクセス	NetScaler Gateway ユーザーが次のいずれかから正常に署名した場合: 新しいパブリック IP アドレス 過去 90 日間使用されていない既存のパブリック IP アドレス。	デフォルトでは、次の条件が有効になっています。 新しいクライアント IP を初めて使用する `Event-Type = "Authentication"AND Status-Code = "Successful login"AND Client-IP-Type != "private"AND Access-Insight-Flags = 1`	Citrix Gateway	侵害されたユーザー

条件バーでは、要件に従って脅威を特定するために、事前設定された条件に加えて、独自の条件を追加することもできます。

たとえば、特定の国のユーザーイベントを特定する場合は、事前設定された条件とともに国ディメンションを追加できます。

- `Event-Type = "Session.Logon"AND Client-Type IN ("XA.Receiver.Windows", "XA.Receiver.Mac", "XA.Receiver.Chrome", "XA.Receiver.Android", "XA.Receiver.Linux", "XA.Receiver.iOS")AND Country = “United States”`
- `Event-Type = "Authentication"AND Status-Code = "Successful login" AND Client-IP-Type != "private"AND Access-Insight-Flags = 1 AND Country = “United States”`

エンドユーザーのメール設定

December 7, 2023

エンドユーザーの電子メール設定は、グローバルアクション「エンドユーザー応答を要求」に関連付けられている電子メールテンプレートを制御します。このアクションを適用すると、ユーザーのアカウントで異常なアクティビティが検出された場合に、ユーザーからの応答が得られます。ユーザーは、Citrix Analytics for Security から受信した電子メールを介して応答します。

メール設定を使用して、次の操作を行うことができます。

- 適切なバナー、ヘッダーテキスト、およびフッターテキストを追加して、ユーザーの注意を引き、ユーザーの反応を得ます。また、メールの正当性が高くなります。
- ユーザーがメールに返信しなければならない時間 (分単位) を追加します。ユーザーが応答時間内に応答しない場合、Citrix Analytics は指定されたアクションをユーザーに適用します。

メール設定の変更

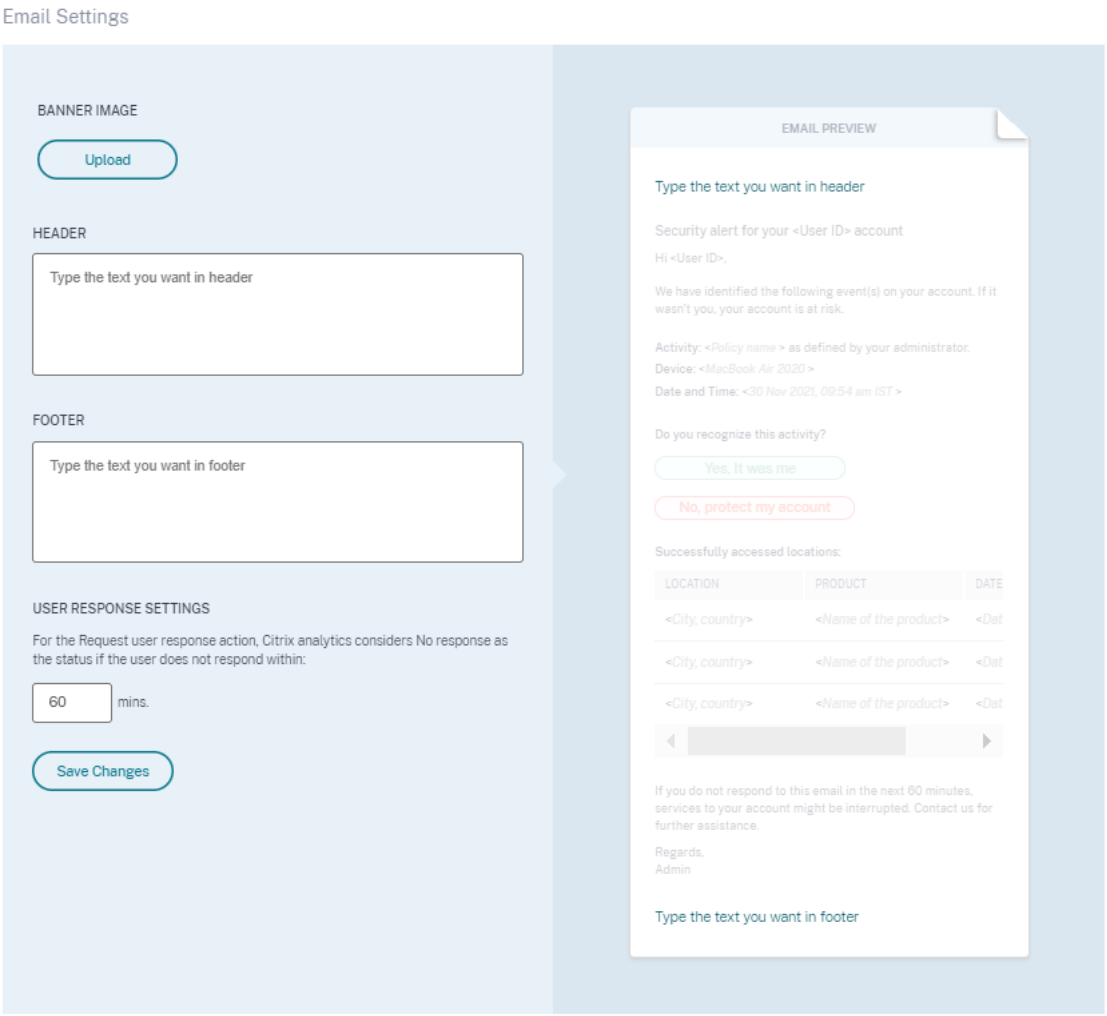
メール設定を変更するには、次の手順に従います。

1. トップバーで、[設定] **>** [アラート設定] **>** [エンドユーザーの電子メール設定] をクリックします。

2. [編集] をクリックして、バナー画像をアップロードまたは参照します。イメージファイルをアップロードするときは、イメージが次の要件を満たしていることを確認してください。

- サポートされる形式:JPEG または PNG
- 最大寸法:400* 100 ピクセル
- 最大ファイルサイズ:5 MB

3. [ヘッダー] と [フッター] フィールドにテキストを入力します。これらのフィールドはオプションです。
4. ユーザ応答設定に時間を入力します。
5. メールをプレビューし、[変更を保存] をクリックします。



管理者メール設定

December 7, 2023

管理者メール設定ページでは、システムアラートのカスタム配布リスト受信者を設定できます。これにより、管理者は自分にとって有益なシステムアラートを確実に受け取ることができます。

管理者メール設定機能には、次の機能があります。

システムアラート、アラートを受信したメール配信リスト、アラート設定を最後に変更したユーザー、およびアラートが最後に変更された日付を表示します。
アラート設定を変更します。さまざまなシステムアラートのターゲット配布リストを変更します。

アラート設定を変更

アラート設定を変更するには:

1. トップバーで、[設定] **>** [アラート設定] **>** [管理者メール設定] をクリックします。

2. メール配布リストを変更したいアラートをクリックします。
3. [メール配布リストを選択] ドロップダウンリストから、アラートを受信する必要がある配布リストを選択します。
   [メール配布リストを作成] をクリックして、独自の配布リストを作成することもできます。詳細については、「メール配布リストの作成」を参照してください。
4. [変更の保存] をクリックします。

ウォッチリスト

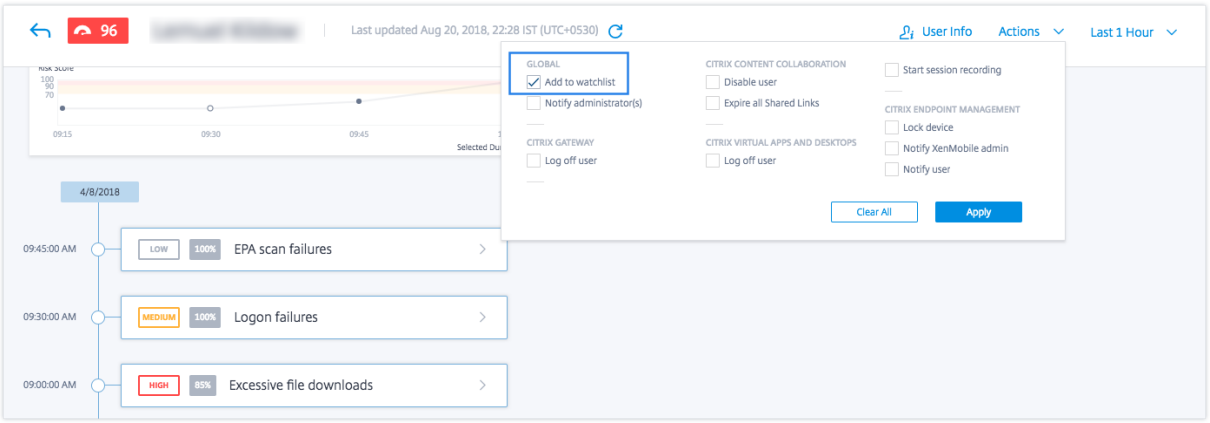
February 14, 2023

ウォッチリストを使用して、特定のユーザーのアクティビティを監視し、潜在的な脅威がないか監視します。たとえば、組織の正社員ではないユーザーや、特定のリスク指標を頻繁にトリガーするユーザーを監視できます。

ウォッチリストにユーザーを追加する方法

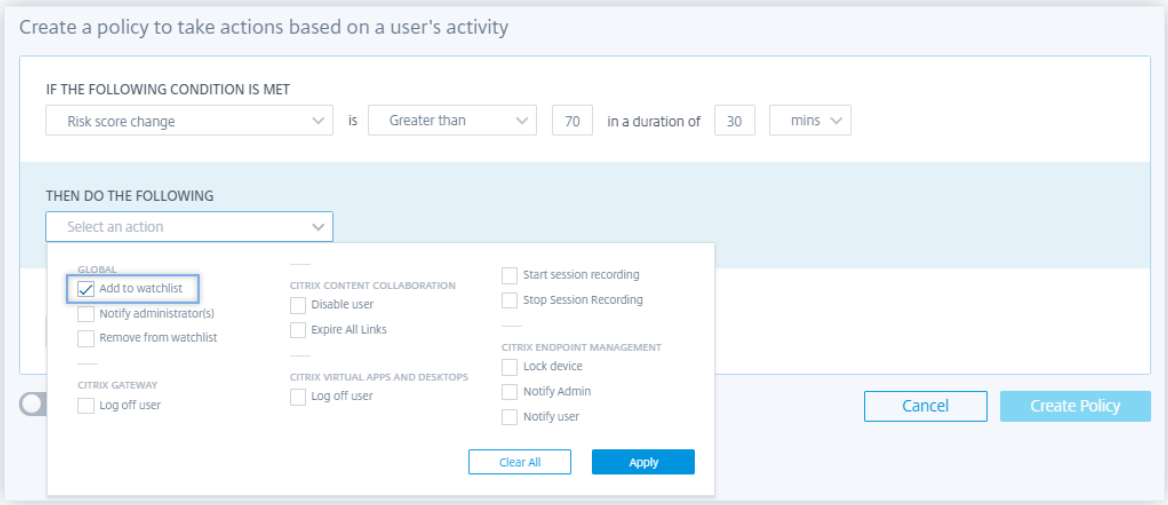
ウォッチリストに手動でユーザーを追加することも、トリガーされたときにウォッチリストにユーザーを追加するポリシーを定義することもできます。

ウォッチリストにユーザーを手動で追加するには、リスクタイムライン上のユーザーのプロフィールに移動します。次に、「アクション」メニューから「ウォッチリストに追加」を選択します。[適用] をクリックし、プロンプトに従ってアクションを実行します。



ポリシーを使用してウォッチリストにユーザーを追加するには、満たす必要がある一連の条件を含むポリシーを作成します。「ウォッチリストに追加」アクションを選択します。条件が満たされると、ユーザーはウォッチリストに追加されます。たとえば、ユーザーのリスクスコアの変化が 30 分間で 70 を超える場合は、ユーザーをウォッチリストに追加したい場合があります。

ポリシーの作成について詳しくは、「ポリシーとアクションの設定」を参照してください。

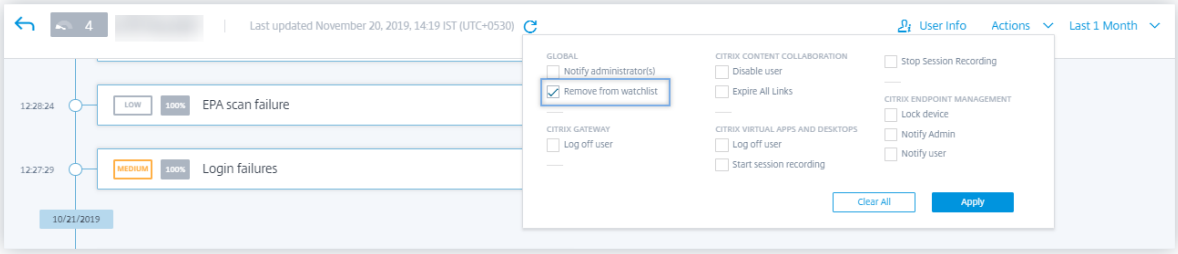


ウォッチリストからユーザーを削除する方法

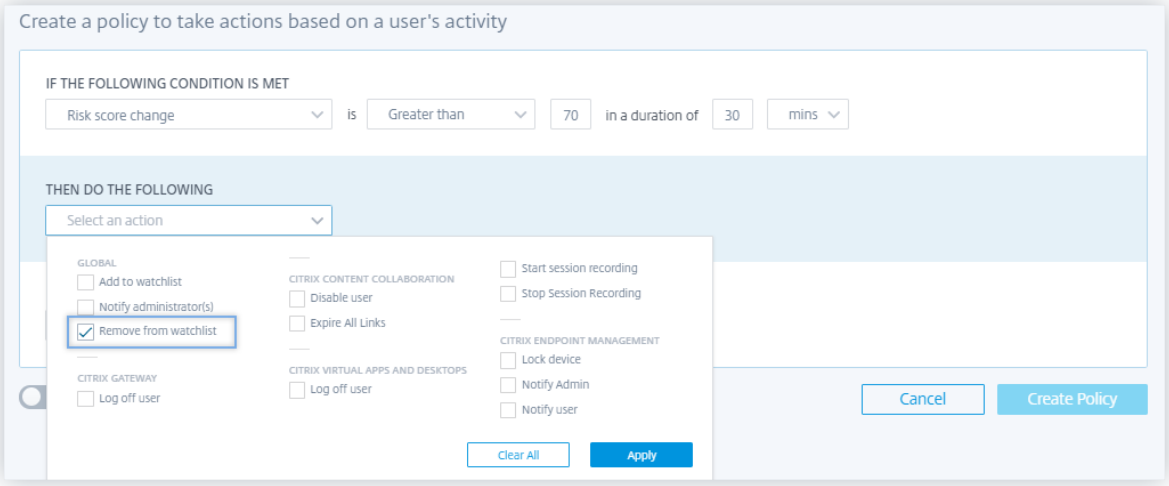
ウォッチリストからユーザーを手動で削除することも、トリガーされたときにウォッチリストからユーザーを削除するポリシーを定義することもできます。

ウォッチリストからユーザーを手動で削除するには、リスクタイムライン上のユーザーのプロフィールに移動します。次に、「アクション」メニューから「ウォッチリストから削除」を選択します。[適用] をクリックし、プロンプトに従ってアクションを実行します。

> 注
>
> ユーザーがウォッチリストに載っていて、そのユーザーを削除したい場合、アクションメニューに「ウォッチリストから削除」オプションが表示されます。



ポリシーを使用してユーザーを監視リストから削除するには、満たす必要がある一連の条件を含むポリシーを作成します。「ウォッチリストから削除」アクションを選択します。条件が満たされると、ユーザーはウォッチリストから削除されます。たとえば、ユーザーのリスクスコアの変化が 60 分で 70 未満になった場合、ウォッチリストからユーザーを削除したい場合があります。ポリシーの作成について詳しくは、「ポリシーとアクションの設定」を参照してください。



ウォッチリスト内のユーザーを監視する方法

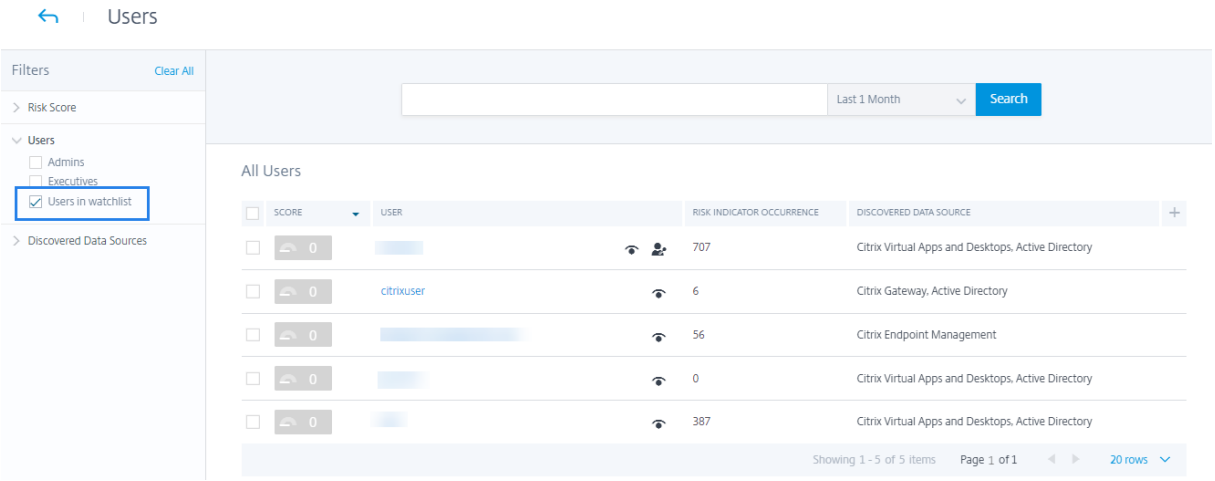
[セキュリティ] **>** [ユーザー] ダッシュボードで、以下を表示します。

- 過去 13 か月間のウォッチリスト内のユーザー数の概要。このボックスをクリックすると、「ウォッチリストのユーザー」ペインにウォッチリスト内のすべてのユーザーのリストが表示されます。
- リスクスコアに基づいてウォッチリストの上位 5 人のユーザーが一覧表示されます。「ウォッチリストのユーザー」ペインで、リスクスコアとリスク指標の出現回数をユーザーの名前とともに表示します。「もっと見る」をクリックすると、「ユーザー」ページのウォッチリストにあるすべてのユーザーのリストが表示されます。

- ウォッチリストに登録されている最も危険なユーザー。リスクの高いユーザーペインでは、ユーザーの横にある「目」アイコンは、そのユーザーがウォッチリストに含まれていることを示します。

ユーザーページで、ウォッチリスト内のすべてのユーザーのリストを表示します。ユーザーのリスクスコア、トリガーされたリスク指標の数 、関連するデータソースなどの詳細を表示します。

検索ボックスを使用して、ユーザーとそのイベントの詳細を検索します。期間を選択すると、特定の期間におけるリスク指標の発生状況が表示されます。



毎週のメール通知

December 7, 2023

Citrix Analytics は、組織の IT インフラストラクチャにおけるセキュリティリスクの概要を記載した電子メール通知を毎週送信します。毎週の通知により、前週に発生したリスクの高いイベントとその発生を常に把握し、通知することができます。Citrix Analytics にサインインしなくても、注意やアクションが必要なイベントがあるかどうかを確認できます。この情報により、IT セキュリティドメインで何が起きているかを常に把握できます。

メール通知を有効にする

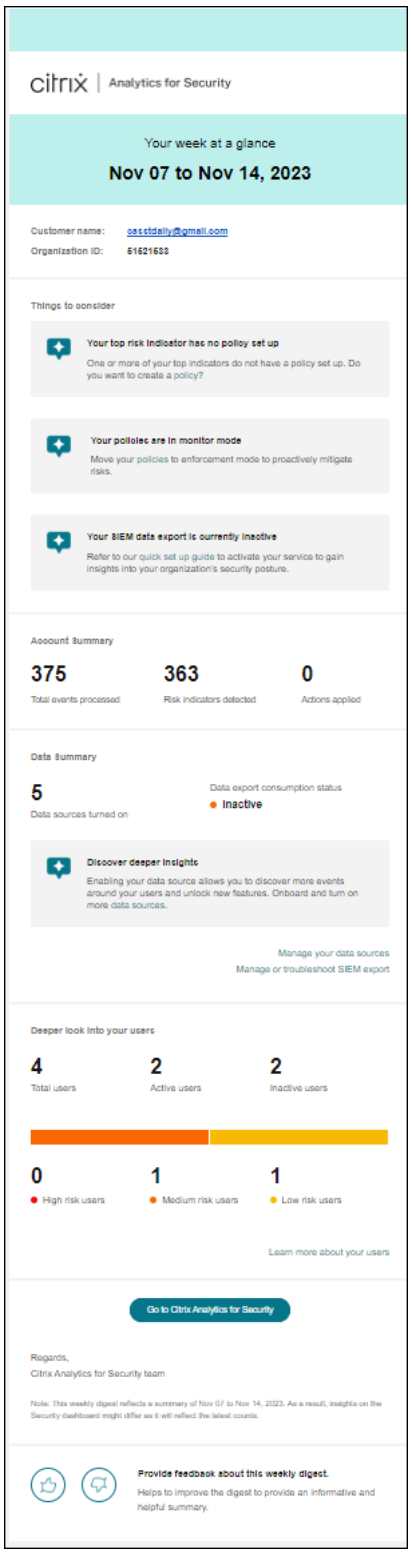
- フルアクセス権限またはカスタムアクセス権を持つ Citrix Cloud 管理者の場合、メール通知は Citrix Cloud アカウントでデフォルトで無効になっています。Citrix Analytics などの Citrix Cloud サービスから電子メール通知を受信するには、Citrix Cloud で通知オプションを有効にします。詳細については、「メール通知を受信する」を参照してください。Active Directory/Azure AD グループを通じて追加された管理者は、通知設定を使用できません。
- デフォルトでは、メール通知は Citrix セキュリティ管理者（デフォルトリスト）に送信されます。これを変更するには、毎週のアラートのカスタム配布リスト受信者を設定します。詳細については、「管理者メール設定」を参照してください。

Citrix Analytics からメールが届くのはいつですか

毎週火曜日に、Citrix Cloud から電子メール通知が送信されます < donotreplynotifications@citrix.com >。

電子メール通知では、次の情報が提供されます。

- 処理されたイベントの総数、検出されたリスク指標、および適用されたアクションの概要
- アクティブなデータソースの総数とデータエクスポートの消費状況の概要
- 上位 3 つのリスク指標
- リスク指標に対して取られた措置の上位 3 つ
- アクティブユーザーの総数とリスクの高いユーザーの総数
- 注意が必要なイベントや行動



citrix | Analytics for Security

Your week at a glance

Nov 07 to Nov 14, 2023

Customer name: oesstdaily@gmail.com
Organization ID: 61621683

Things to consider

Your top risk indicator has no policy set up
One or more of your top indicators do not have a policy set up. Do you want to create a policy?

Your policies are in monitor mode
Move your policies to enforcement mode to proactively mitigate risks.

Your SIEM data export is currently inactive
Refer to our quick set up guide to activate your service to gain insights into your organization's security posture.

Account Summary

375	363	0
Total events processed	Risk indicators detected	Actions applied

Data Summary

5
Data sources turned on

Data export consumption status
Inactive

Discover deeper insights
Enabling your data source allows you to discover more events around your users and unlock new features. Onboard and turn on more data sources.

Manage your data sources
Manage or troubleshoot SIEM export

Deeper look into your users

4	2	2
Total users	Active users	Inactive users

0	1	1
High risk users	Medium risk users	Low risk users

Learn more about your users

Go to Citrix Analytics for Security

Regards,
Citrix Analytics for Security team

Note: This weekly digest reflects a summary of Nov 07 to Nov 14, 2023. As a result, insights on the Security dashboard might differ as it will reflect the latest counts.

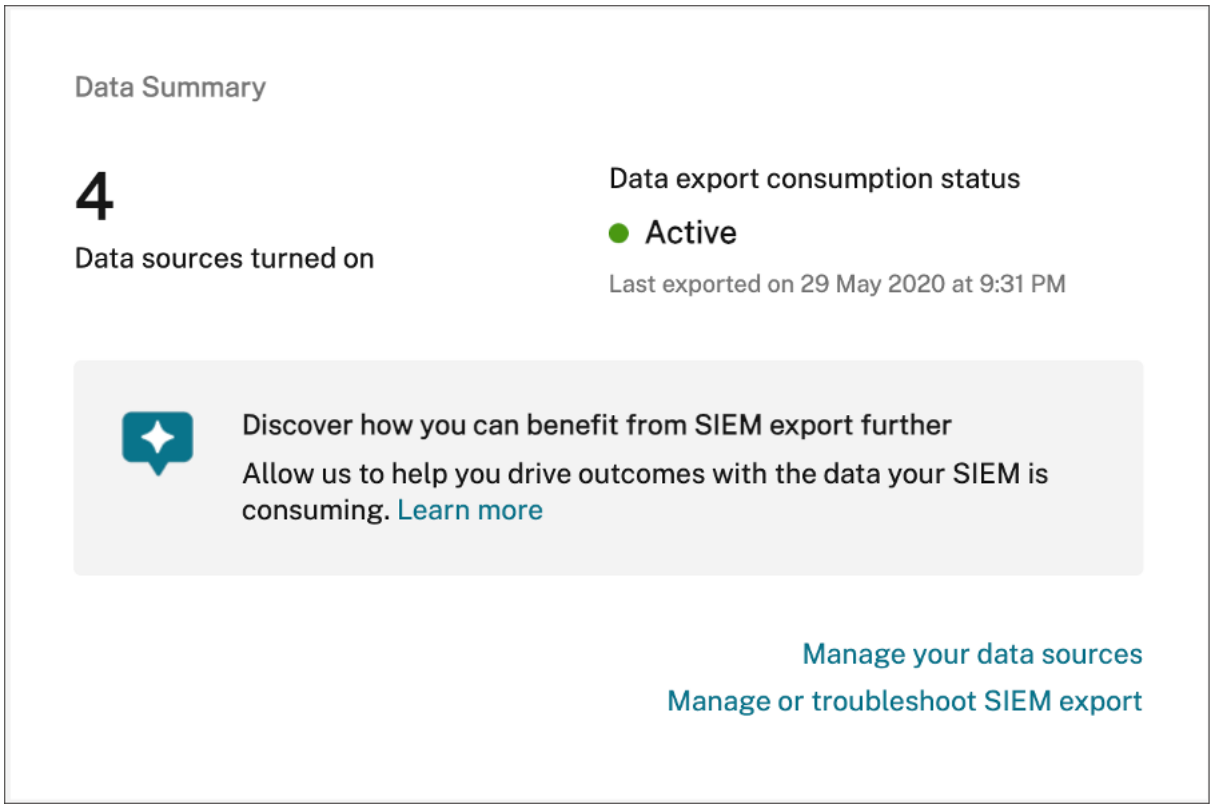
Provide feedback about this weekly digest.
Helps to improve the digest to provide an informative and helpful summary.

アカウントサマリー

毎週のメールには、処理されたイベントの総数、検出されたリスク指標、および適用されたアクションの概要が記載されています。

データサマリー

毎週のメールには、データエクスポートの消費状況とともに、有効になっているデータソースに関するインサイトも記載されています。



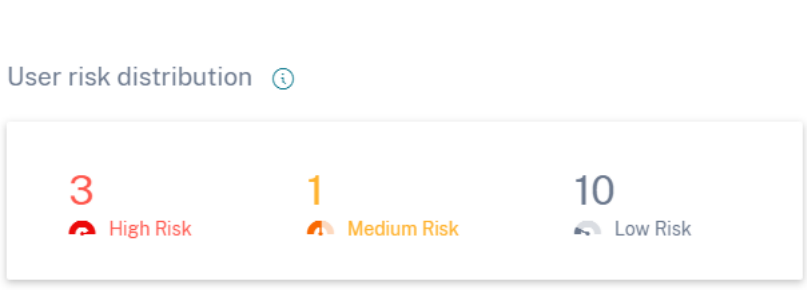
メールの「データソースの管理」をクリックすると、Citrix Analytics の「データソース」ページが表示されます。データソースをオンボードしてデータ処理を有効にすると、Citrix Analytics でデータを処理できるようになります。分析の有効化の詳細については、「データソースで分析を有効にする 」を参照してください。

[**SIEM** エクスポートの管理またはトラブルシューティング] をクリックすると、Citrix Analytics の [データエクスポート] ページが表示され、環境のトラブルシューティングやデータエクスポート設定の管理を行うことができます。

ユーザー情報

毎週のメールには、ユーザーの総数と危険な行動をとったユーザーの総数に関する洞察が記載されています。

- 高リスクユーザーの数—赤色で表示されます。それらは組織にとって差し迫った脅威となります。
- 中リスクの数—オレンジ色で表示されます。選択した週に、アカウントに複数の重大な違反があったため、注意深く監視する必要があります。
- 低リスクユーザーの数—黄色で示されます。アカウントには重大な違反がいくつかありますが、脅威とは見なされない可能性があります。

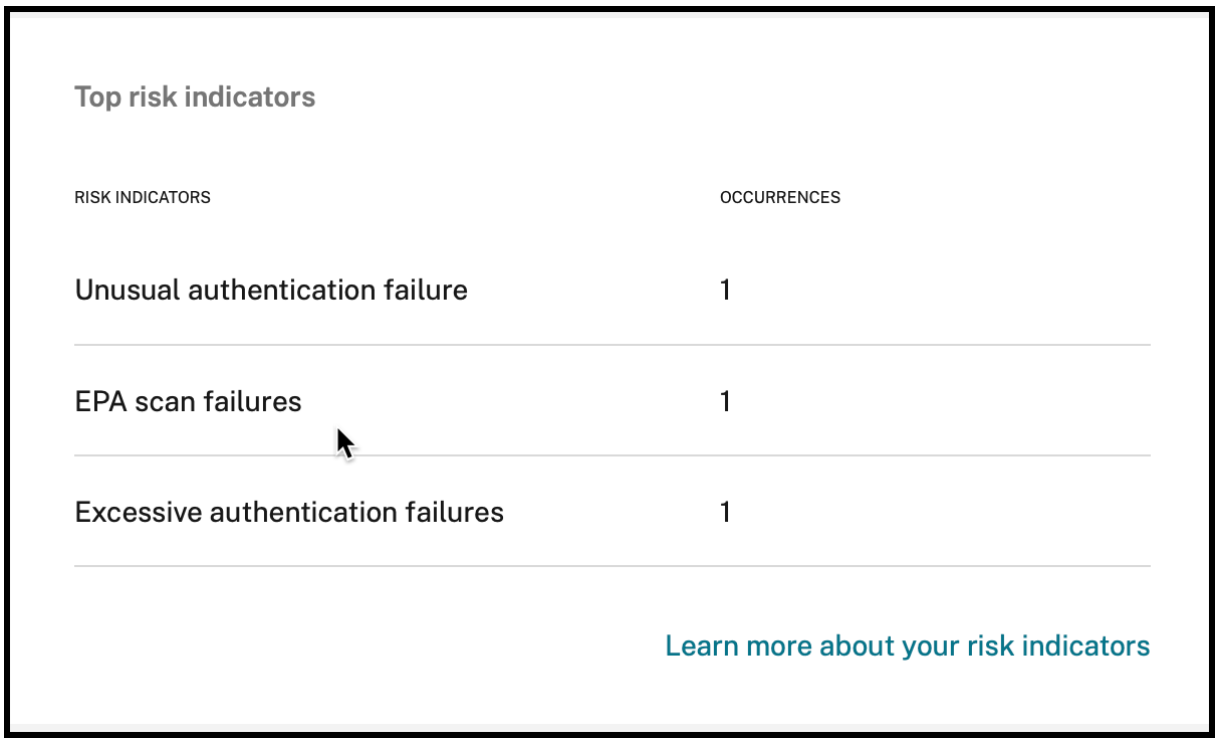


詳細については、「危険なユーザー」を参照してください。

Citrix Analytics の「** リスクの高いユーザー」ページを表示するには、「ユーザーについて詳しく知る ** 」をクリックします。アクティブユーザーとリスク分類についてより深い洞察を得ることができます。

トップリスク指標

毎週のメールには、選択した週の上位 3 つのリスク指標と発生回数に関する洞察が記載されています。発生回数に応じて、選択した週のデフォルトリスク指標とカスタムリスク指標の両方が表示されます。

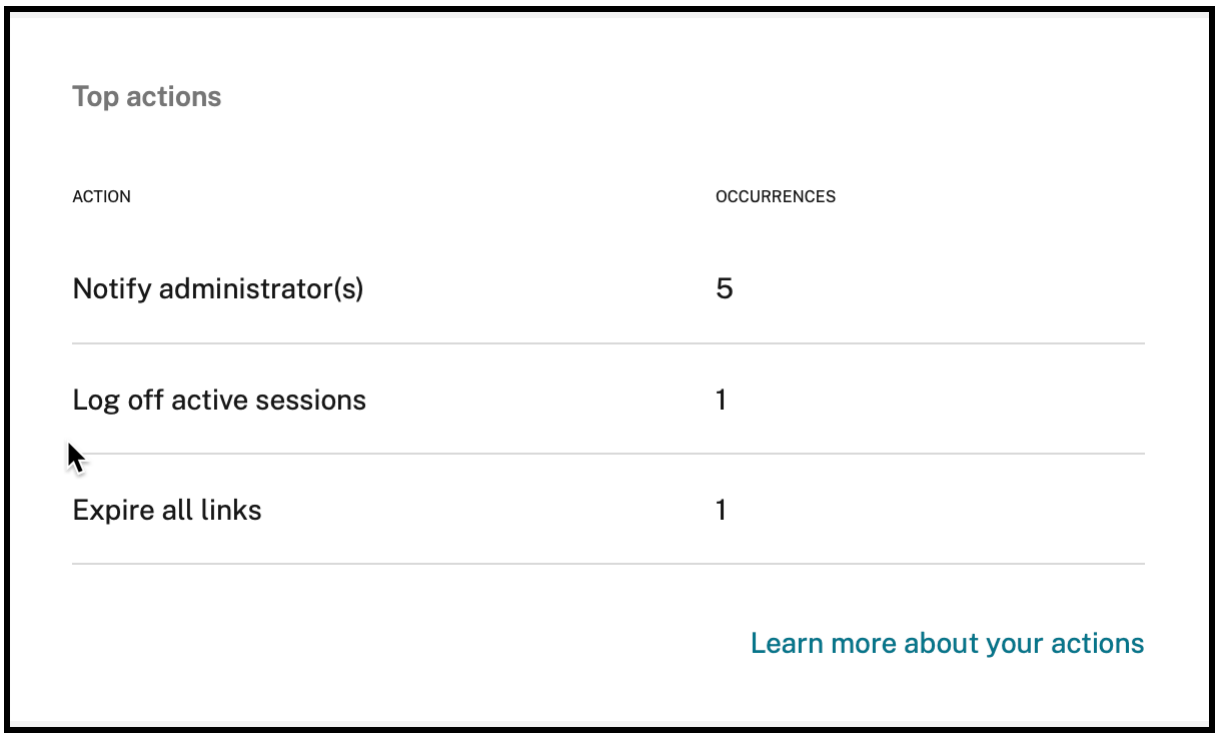


詳細については、「リスク指標」を参照してください。

メールに記載されている「リスク指標の詳細」をクリックすると、Citrix Analytics の「リスク指標の概要」ページが表示されます。

上位のアクション

毎週のメールには、先週発生した疑わしい脅威や異常な脅威への対応として取られた上位 3 つのアクションに関する洞察が記載されています。発生回数に応じて、選択した週のグローバルアクションと NetScaler Gateway アクションの両方が表示されます。



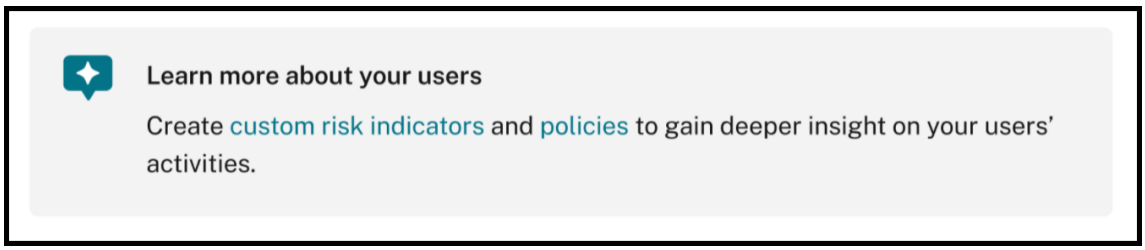
アクションの詳細とアクションの設定については、「ポリシーとアクション」を参照してください。

メールに記載されたアクションの詳細を確認をクリックすると、Citrix Analytics の「トップアクション」ページが表示されます。

メールを受信した後、どのようなアクションを取る必要がありますか

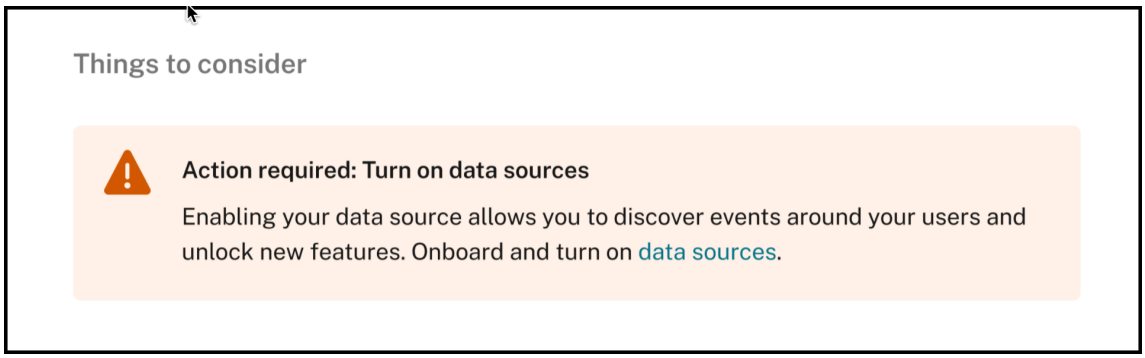
毎週メールを送信すると、注意が必要なイベントやアクションがあるかどうかを確認できます。

- その週のリスク指標が検出されない場合、カスタムリスク指標をさらに作成するように求める次のメッセージが表示されます。

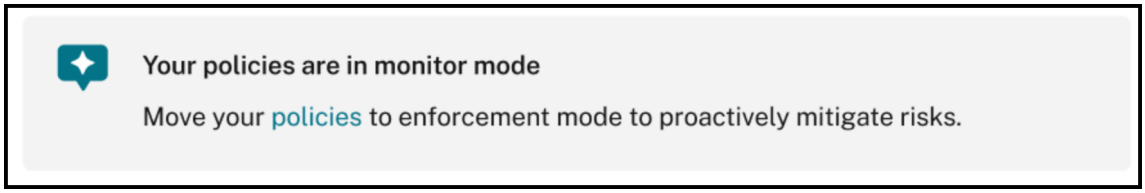


Citrix Analytics にログインして、より多くのカスタムリスク指標を作成できます。

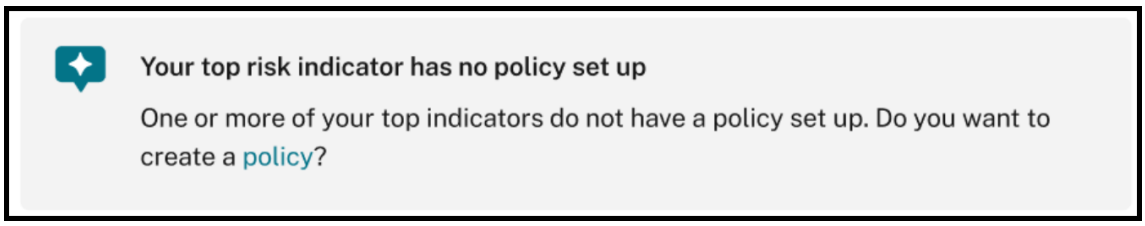
- Security Analytics でどのデータソースもオンになっていない場合は、データソースのデータ処理を有効にするように求める次のメッセージが表示されます。



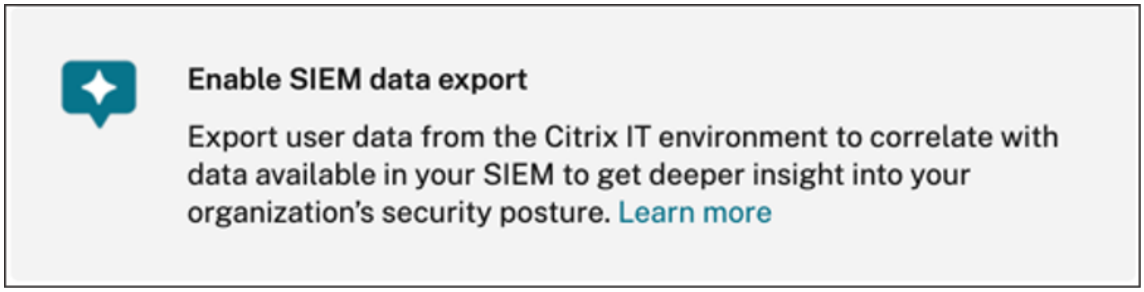
- どのポリシーも監視モードになっていない場合は、ポリシーを強制モードに移行するように求める次のメッセージが表示されます。



- その週の上位 3 つのリスク指標のいずれにもポリシーが設定されていない場合は、ポリシーを作成するように求める次のメッセージが表示されます。

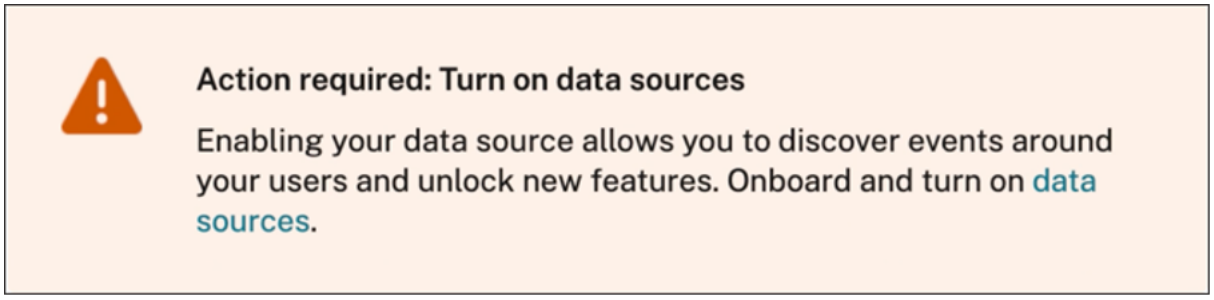


- Citrix Analytics テナントでデータエクスポートを有効にしていない場合、以下の推奨事項に従うと、Citrix データを **SIEM** 環境にエクスポートできるデータエクスポートオプションの詳細がわかります。



- データエクスポートの消費ステータスが非アクティブの場合、サービスをアクティブ化するように求める次のメッセージが表示されます。

> 注:
>
> データ送信は、少なくとも 1 つのデータソースでデータ処理がオンになっている場合にのみ有効になります。すべてのデータソースでデータ処理がオフになっている場合は、データソースを有効にするよう求める次の警告メッセージが表示されます。



監査ログ

June 24, 2021

監査ログには、Citrix Analytics で生成されたイベントの監査情報が記録されます。エラーなどのシステムイベントや、Citrix Analytics 管理者が実行する構成操作の監査証跡などです。

構成を追加、削除、または更新するたびに、イベント情報が監査ログに書き込まれます。この情報は、変更内容、変更日時、変更者に関する情報です。

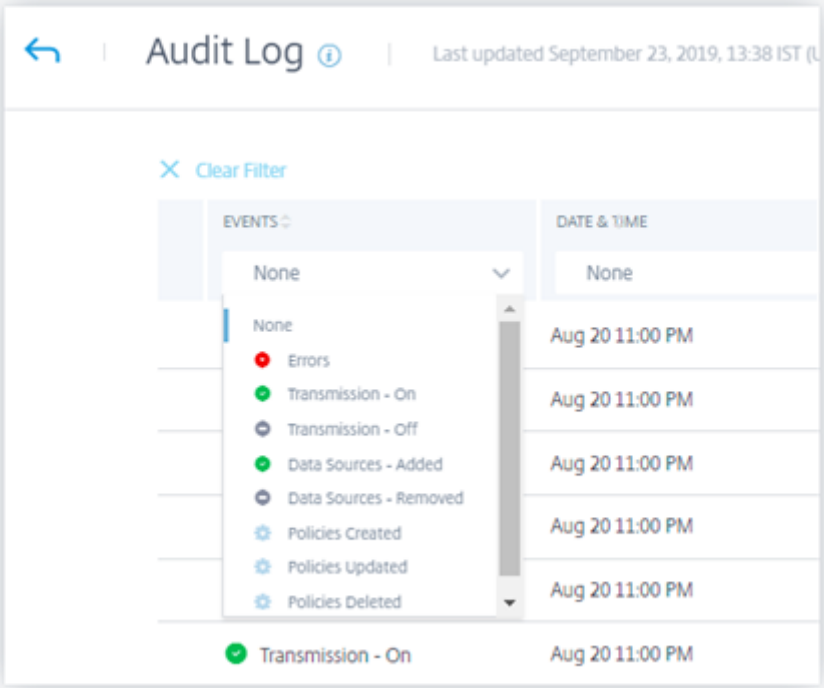
過去 3 か月間の監査ログ情報を表示できます。

監査イベントを生成するアクティビティ

Citrix Analytics では、以下のイベントが登録されます。

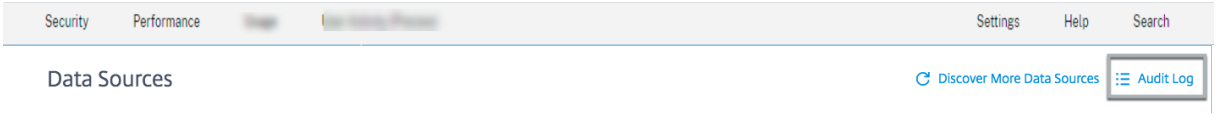
- エラーが生成されました
- 送信がオンになっている
- 送信がオフになっています。

- 追加されたデータソース
- データソースが削除されました
- 作成されたポリシー
- 更新されたポリシー
- 削除されたポリシー



監査ログを表示する方法

監査ログを表示するには、Citrix Analytics にログオンします。**[** 設定**] > [**データソース**]** に移動します。**[**データソース**]** ページで、右上隅にある **[**監査ログ**]** をクリックします。

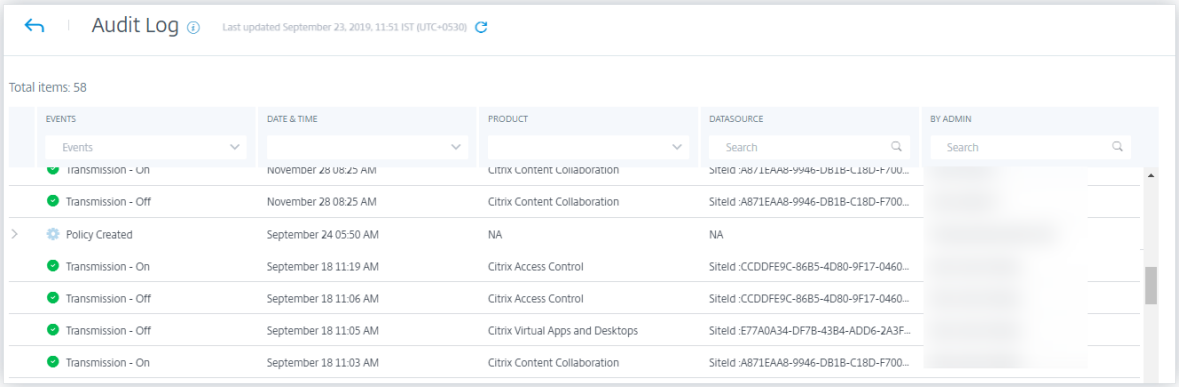


監査ログの使用方法

監査ログを使用して、Citrix Analytics 上のイベントを確認して認識できます。「監査ログ」ページを更新して、最新の監査データをフェッチします。このページには、監査データが最後に更新された日時が表示されます。

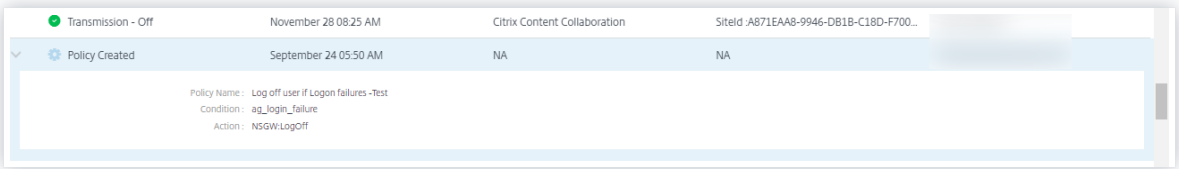
「監査 ログ」ページでは、次の監査 情報を表示できます。また、これらのフィールドに基づいて監査データをフィルタリングすることもできます。

- イベント。イベントには、システム生成または Citrix Analytics で管理者が適用する構成があります。イベントは、アクションやデータソースの適用に失敗したなどのエラーを表すこともできます。デフォルトでは、すべてのイベントのログが表示されます。表示するイベントの種類に基づいてフィルタリングできます。
- 日付と時刻。イベントが発生したデータと時刻。ログを表示する期間に基づいてフィルタリングできます。当日、過去 7 日間、過去 15 日間、先月、過去 3 か月間のイベントを表示できます。
- 製品。イベントが生成された製品。イベントは製品上で生成され、Citrix Analytics で集約されて表示されます。ログは、1 つ以上の製品に基づいてフィルタリングできます。
- データソース。監査エントリに関連付けられた製品インスタンスの名前。特定のデータソースを検索して、その監査データを表示できます。
- 管理者別。管理者アクティビティを実行した Citrix Analytics 管理者。特定の管理者が実行したアクティビティを検索できます。



登録したイベントがポリシーに基づいている場合は、矢印アイコンをクリックすると、次のような詳細を表示できます。

- ポリシー名
- 指定された条件
- 結果のアクション



カスタムレポート

June 18, 2024

Citrix Analytics for Security で利用できるイベントとインサイトを使用して、カスタムレポートを作成およびスケジュールできます。カスタムレポートを使用すると、特定の関心のある情報を抽出し、データをグラフィカルに整理できます。選択したデータソースのセキュリティを長期にわたって分析するのに役立ちます。

カスタムレポートは次のデータソースをサポートします:

- アプリケーションとデスクトップ
- Gateway
- Secure Private Access
- Secure Browser
- ポリシー
- リスクインジケータ
- リスクスコア

カスタムレポートでサポートされるフィールド

一部のデータソースはセルフサービス検索でも利用できます。これらのイベントタイプとサポートされているフィールドを表示するには、次のデータソースをクリックしてください。

- アプリケーションとデスクトップ
- Gateway
- Secure Private Access
- Secure Browser
- ポリシー

次のデータソースはカスタムレポートでのみ使用できます。次の表は、以下のデータソースのカスタムレポートでサポートされているフィールドの一覧です:

- リスクインジケータ
- リスクスコア

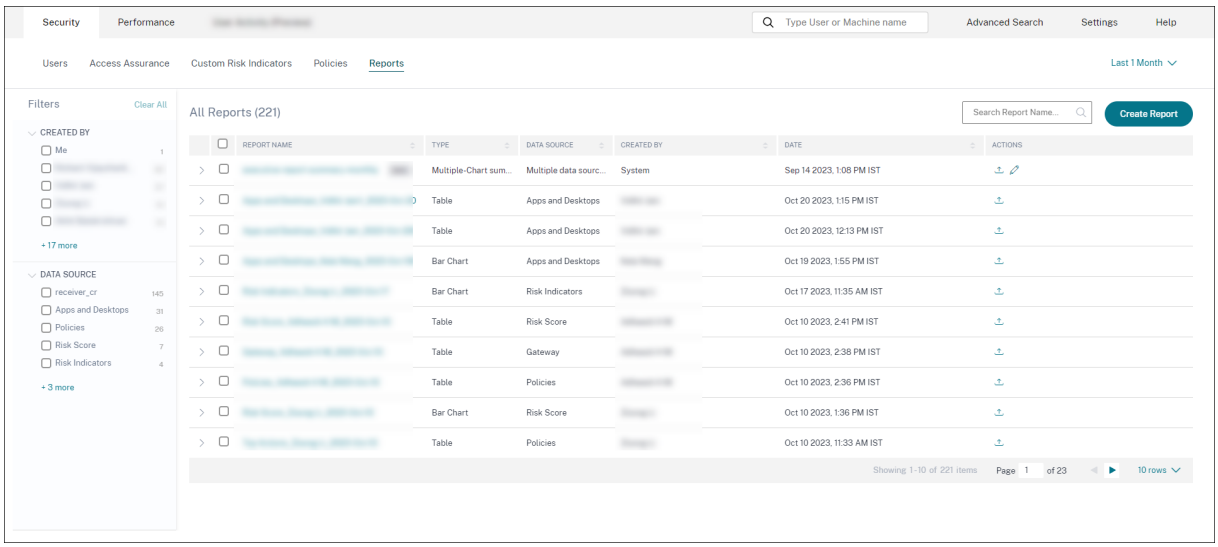
データソース	ディメンション	説明
リスクインジケータ	カテゴリ	リスク指標のカテゴリを示します。リスク指標は、エンドポイントの侵害、ユーザーの侵害、データ流出、内部脅威の 4 つのカテゴリのいずれかに分類されます。
	リスク指標名	リスク指標の名前。カスタムリスク指標の場合、名前は指標の作成時に管理者が定義します。

データソース	ディメンション	説明
	重要度	リスクの重大度を示します。低、中、高のいずれかになります。
	User-Name	ログインに使用するユーザー名またはドメイン\ ユーザー名。
リスクスコア	リスクスコア	ユーザーに割り当てられたリスクスコア。リスクスコアは、ユーザーのアクティビティに関連する脅威の重大度に応じて 0 から 100 まで変化します。
	User-Name	ログインに使用するユーザー名またはドメイン\ ユーザー名。
	リスクスコアカテゴリ	リスクスコアに基づいて、リスクの高いユーザーは、高リスク、中リスク、低リスクのいずれかのカテゴリに分類されます。

レポート

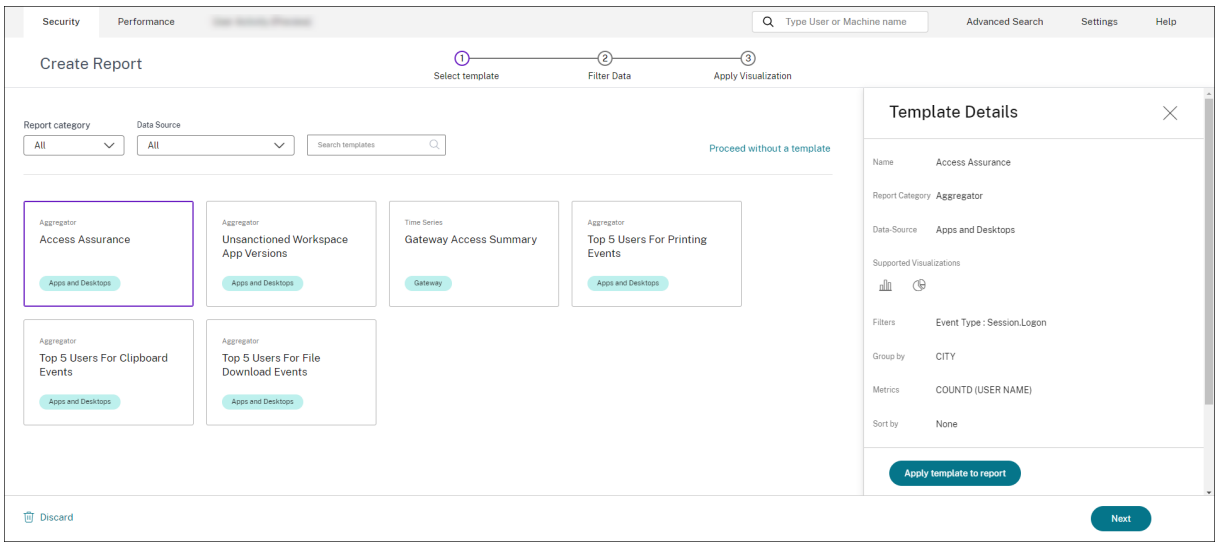
このビューを使用して、レポートに対して次のアクションを実行できます。

- 「レポートを作成」をクリックして、カスタムレポートを作成します。
- 行を展開すると、既存のカスタムレポートのプレビューが表示されます。
- レポート名をクリックすると、詳細なレポートビジュアライゼーションが表示されます。
- エクスポートアイコンをクリックして、既存のカスタムレポートを PDF 形式でエクスポートします。
- 編集アイコンをクリックして、作成したレポートを編集します。
- 削除アイコンをクリックして、作成したレポートを削除します。



カスタムレポートの作成

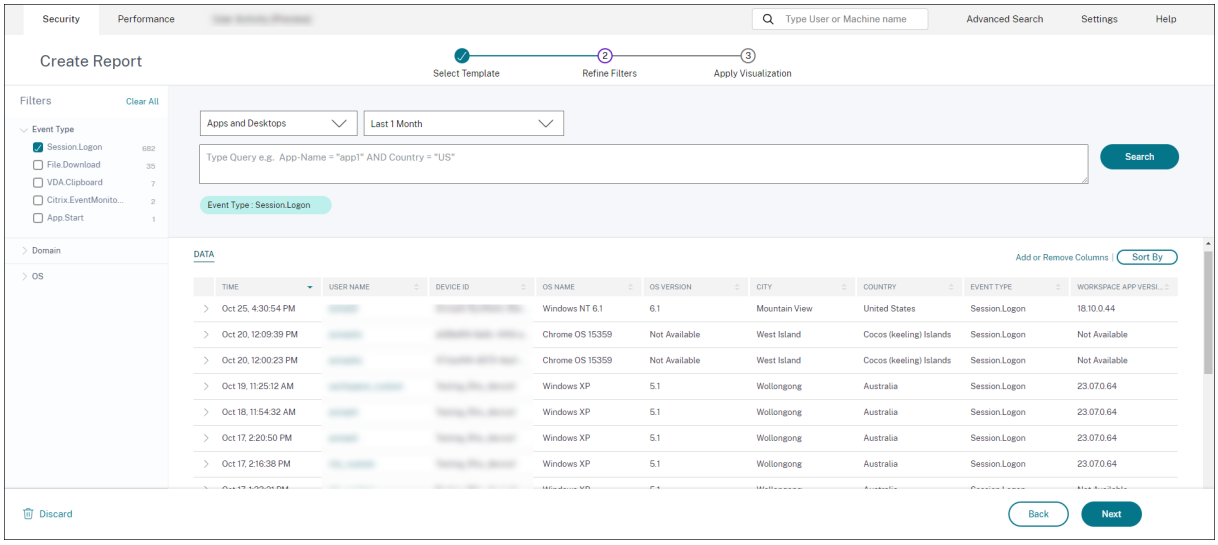
カスタムレポートを作成するには、「レポートを作成」をクリックします。レポートの作成ページでは、テンプレートを使用するカスタムレポートを作成するか、テンプレートなしで作成するかを選択できます。



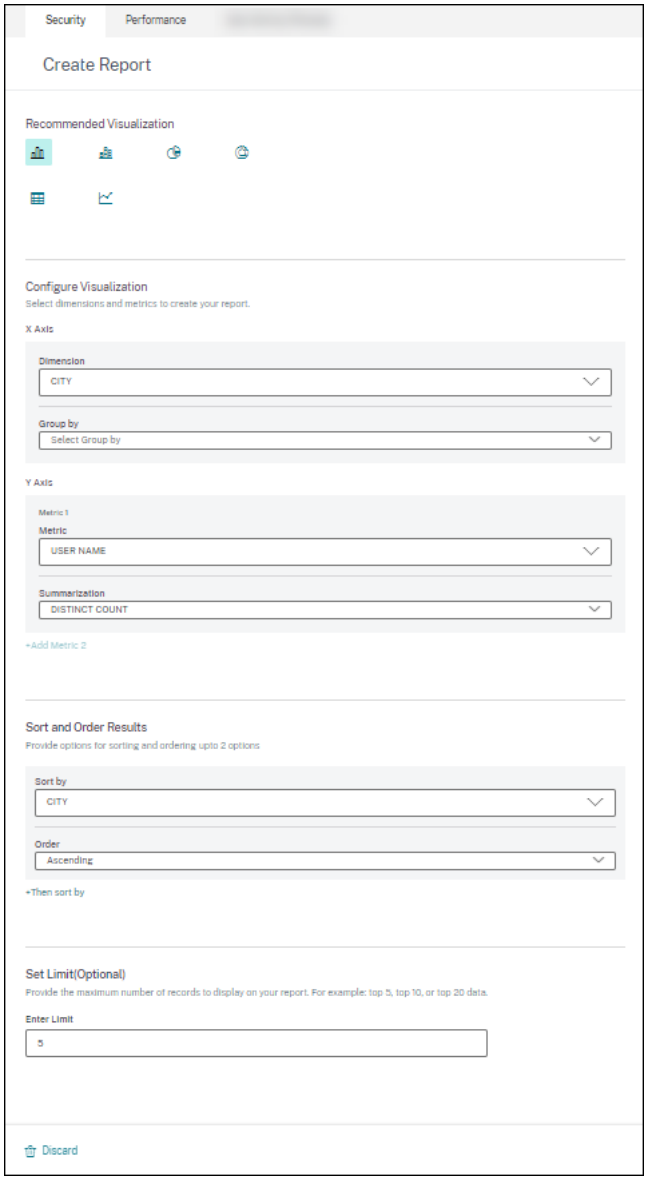
テンプレートを使ったカスタムレポートの作成

テンプレートを使用してカスタムレポートを作成するには:

1. テンプレートを選択**:** テンプレートをクリックすると、テンプレートの詳細が右側に一覧表示されます。「テンプレートをレポートに適用」をクリックして、選択したテンプレートをレポートで使用できるようにします。
2. フィルターを絞り込む**:** フィルターの絞り込みページには ****** 、選択したテンプレートにあらかじめ定義されているフィルターが表示されます。必要な変更を加え、**[**** 次へ] をクリックします。



1. ビジュアライゼーションを適用: レポートを表示するために利用可能なビジュアライゼーションを 1 つ選択します。



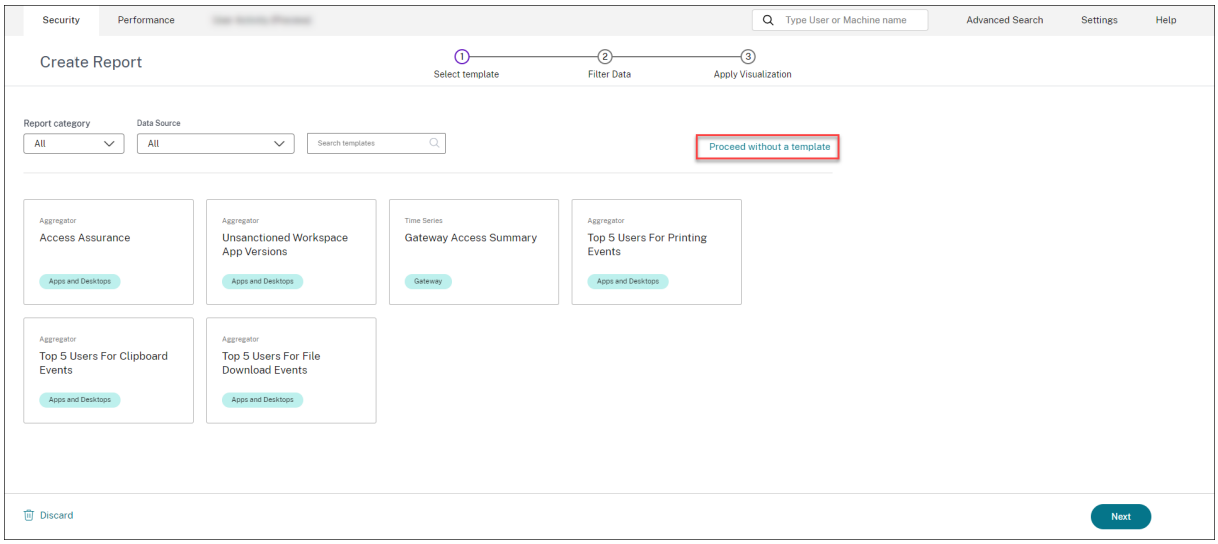
- 棒グラフ: 高さが値に比例する縦の長方形の棒でデータを表示します。イベントの比較に使用されます。
- 積み上げ縦棒グラフ: データを棒状に重ねて表示します。複数のサブカテゴリにわたるデータの合計を視覚化するために使用されます。
- 円グラフ: データを円の形式で表示します。データの相対サイズまたはパーセンテージを視覚化するために使用されます。
- ドーナツグラフ: データをドーナツ形式で表示します。データの相対サイズまたはパーセンテージを視覚化するために使用されます。- テーブル: データをテーブル形式で表示します。必要なだけ多くのディメンションを視覚化するために使用されます。
- 折れ線グラフ: データを点と点を直線セグメントで結んで表示します。一定期間のデータ傾向を視覚化するために使用されます。

1. 次に、次のパラメータを使用してビジュアライゼーションを設定します。

- X 軸の寸法
- Y 軸にプロットされる指標
- 指標に適用される集計または集計（平均やカウントなど）
- 並べ替えと順序のオプション
- レポートに表示する最大レコード数のオプション制限です。

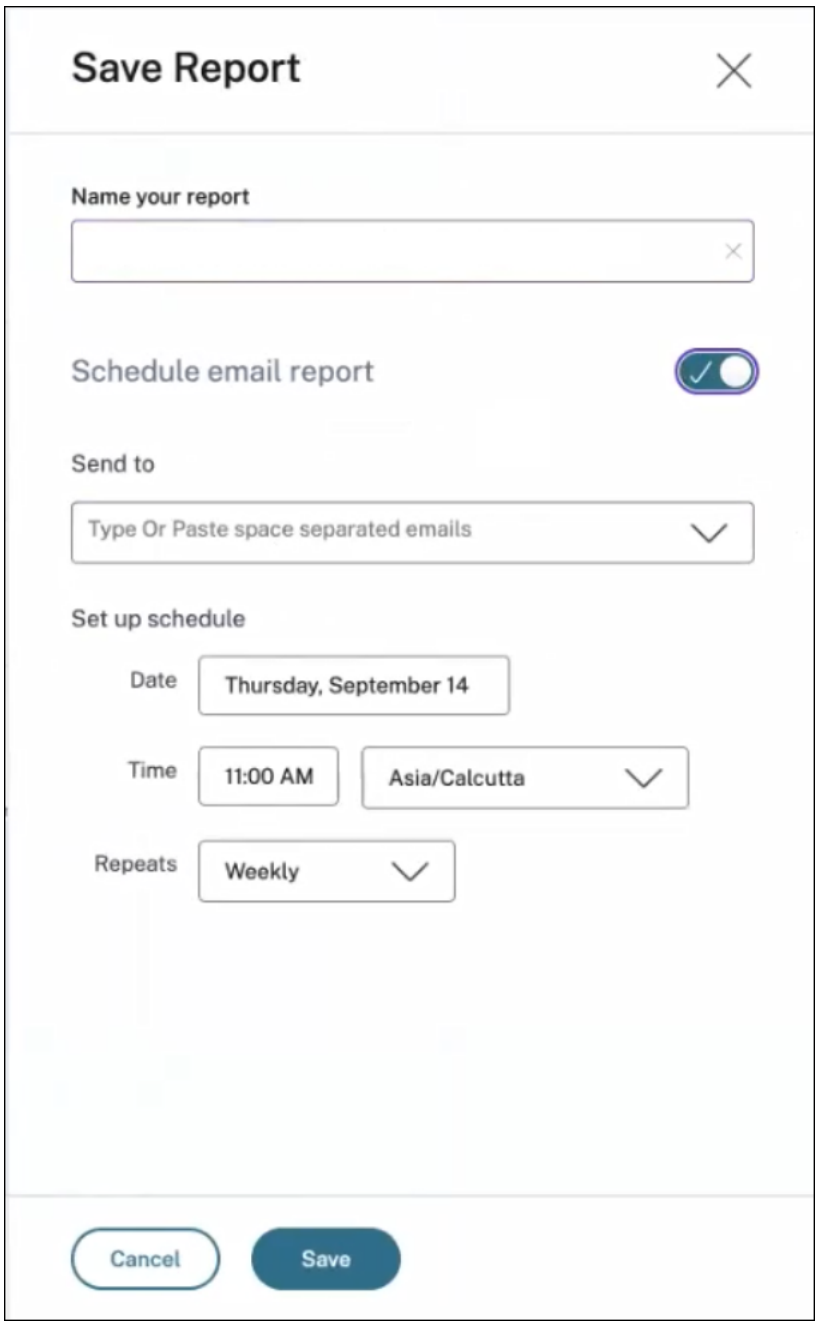
テンプレートを使用しないカスタムレポートの作成

定義済みのテンプレートなしでカスタムレポートを作成することもできます。[テンプレートなしでカスタムレポートを作成] をクリックします。ドロップダウンリストからデータソースを選択します。手順に従って、フィルターを定義し、視覚化を適用し、レポートを保存し、スケジュールを設定します。



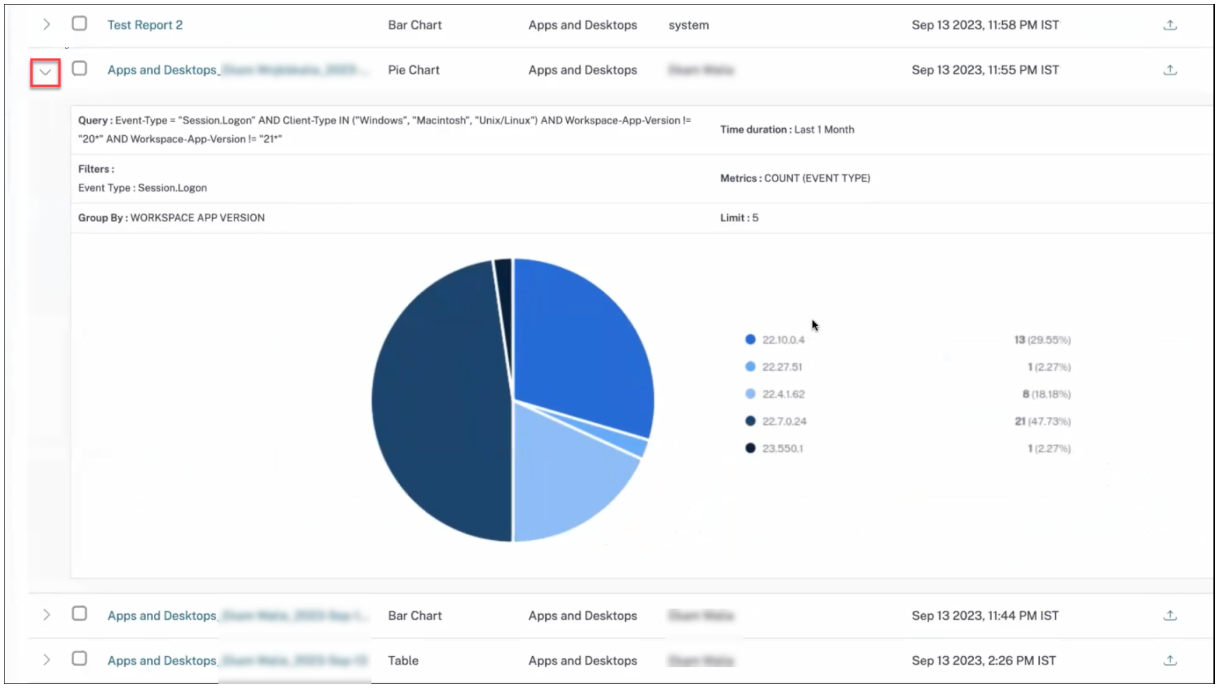
レポートを保存する

1. レポートを保存するには、[保存] をクリックします。レポートのタイトルを指定します。
2. 特定の日時、または定期的なスケジュールで、指定された電子メール ID と配布リストにレポートを電子メールで送信するようにスケジュールできます。



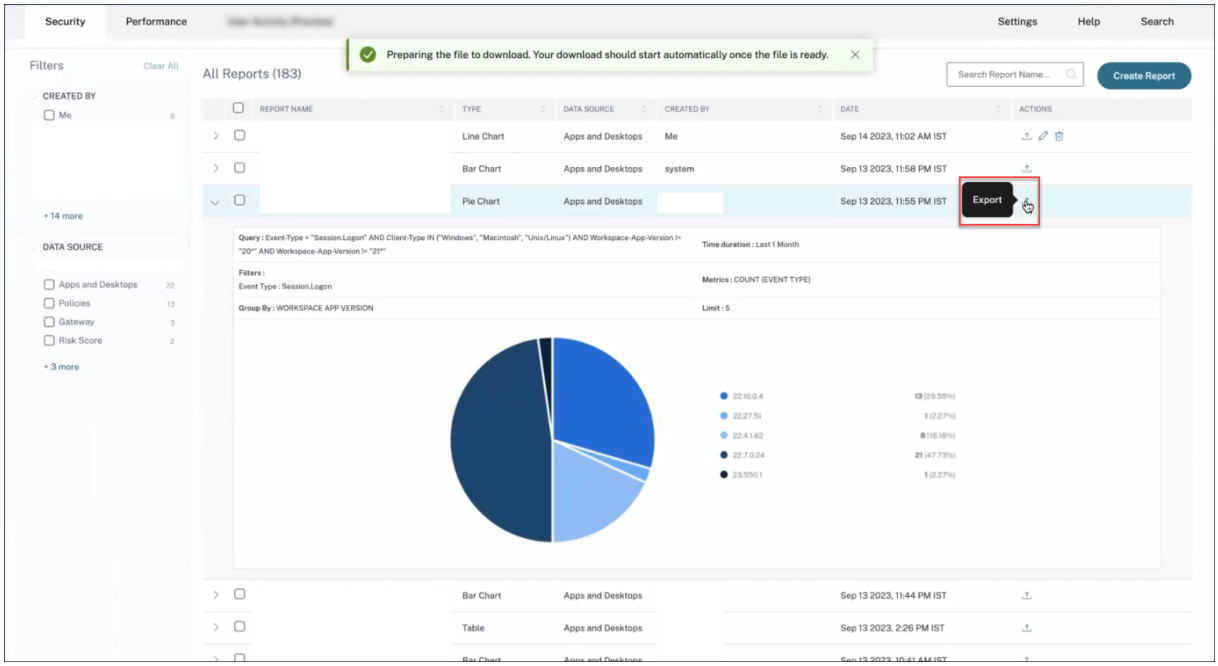
レポートを表示する

1. レポートを作成して保存したら、レポートページでレポートを表示できます。保存したレポートを変更または削除することもできます。
2. ドロップダウンボタンをクリックしてレポートをプレビューします。



レポートのエクスポート

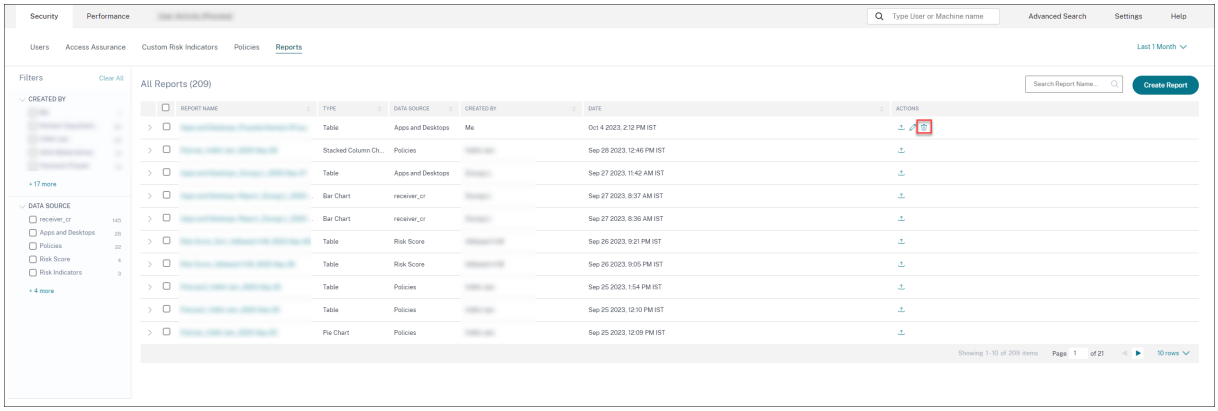
エクスポートアイコンをクリックしてレポートをエクスポートします。



レポートを削除する

レポートを削除するには、削除アイコンをクリックします。

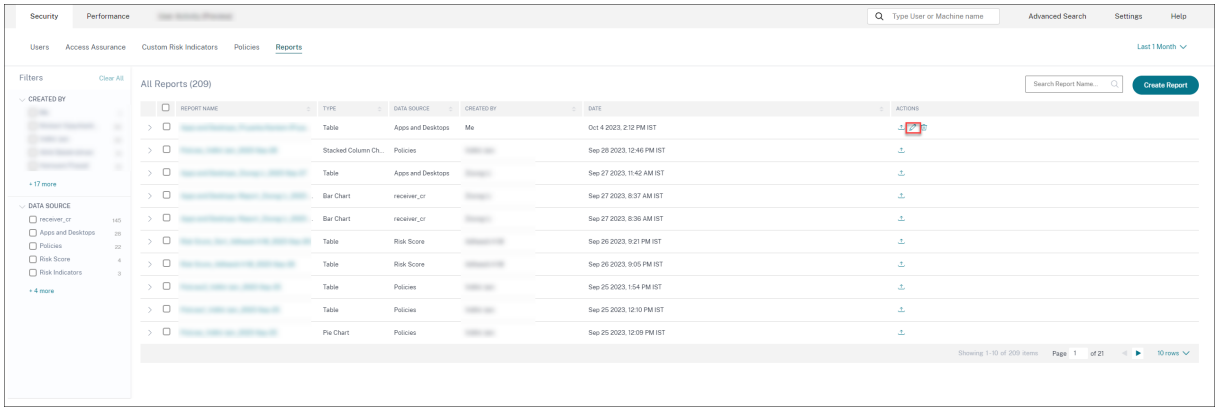
> 注記:
>
> レポートを作成したユーザーのみがレポートを削除できます。



レポートを編集する

編集アイコンをクリックしてレポートを編集します。

> 注記:
>
> レポートを作成したユーザーのみが編集できます。



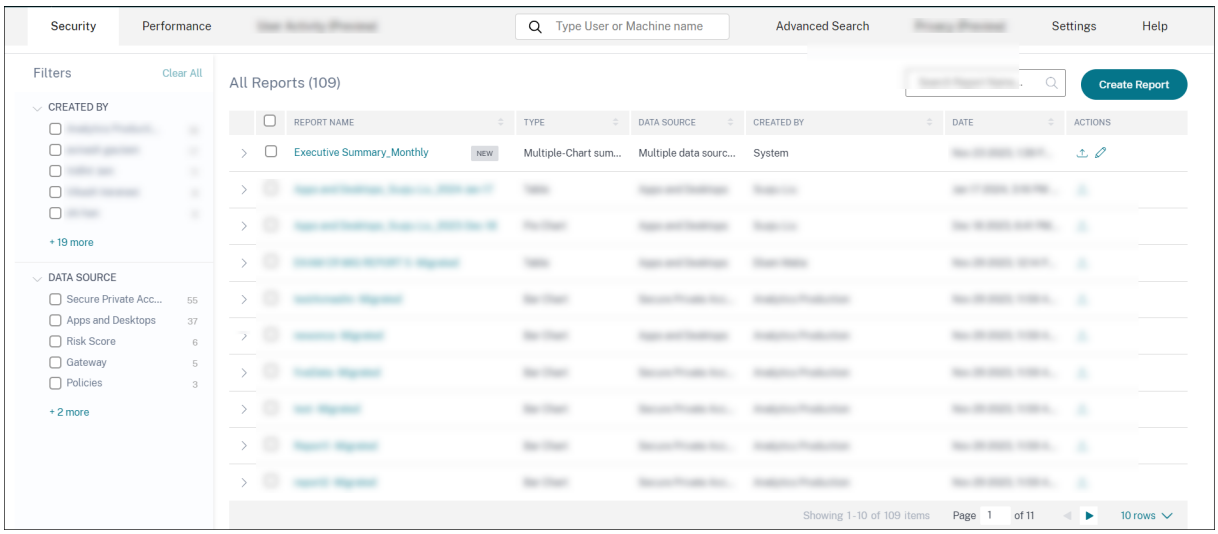
エグゼクティブ・サマリー・レポート

事前に作成されたエグゼクティブサマリーレポートの PDF を含む自動エクスポートを電子メールでスケジュールできます。エグゼクティブサマリーレポートは、選択した期間における企業のセキュリティ体制を一目で把握できるレポートを集めたもので、選択した対象者に向けて提供されます。

次の期間のデータのレポートを作成できます:

- 過去 1 時間

- 過去 12 時間
- 過去 1 日
- 過去 1 週間
- 過去 1 か月



どのようなレポートが含まれていますか**?**

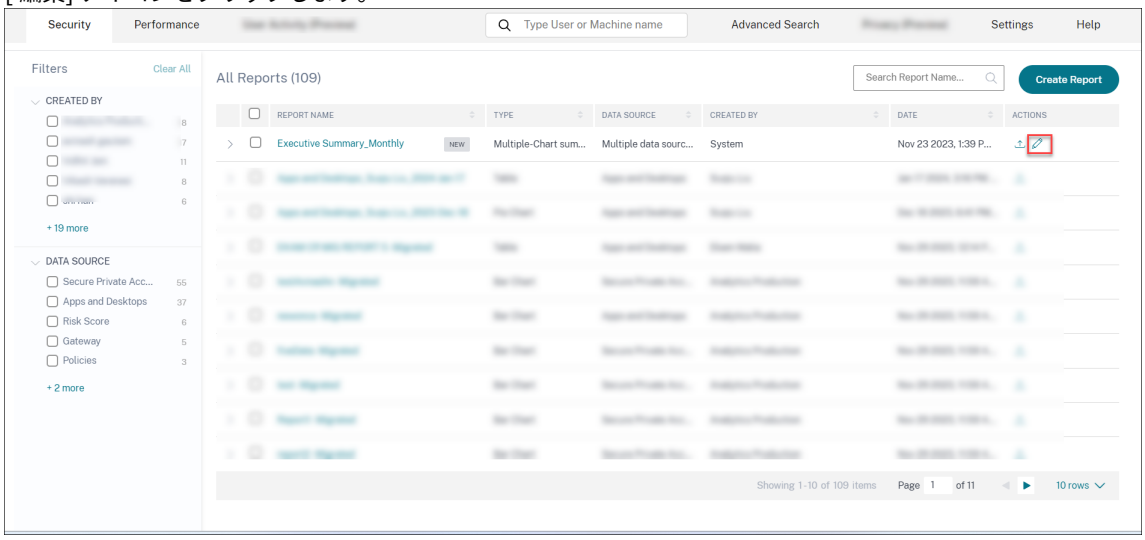
エグゼクティブサマリーレポートには次のレポートが含まれます:

- ユーザーリスク分布: 選択した期間に計算された最高リスクスコアに基づいて、高リスク、中リスク、低リスクプロファイルの分布を示します。
- 最もリスクの高いユーザー: 選択した期間のリスクスコアが最も高い順にソートされた、全ユーザーの中でリスクが高いユーザーです。
- カテゴリー別のリスク発生状況**:** 早急な対応が必要なリスクカテゴリー別のリスクエクスポージャーとクリティカルリスクの種類を包括的に把握したもの。リスク指標は次のカテゴリに分類されます:
  - 侵害されたユーザー
  - 侵害されたエンドポイント
  - データ流出
  - インサイダーの脅威
- リスク指標: 選択した期間にユーザーにトリガーされたリスク指標。
- アクション: 選択した期間にユーザーに対してトリガーされたリスク指標に適用されたアクション。
- トップポリシー: 選択した期間に最も多くトリガーされたポリシーの上位 5 つ。
- トップアクション: 選択した期間に最も多くトリガーされたアクションの上位 5 つ。
- 重要度別のリスク指標**:** 重要度に基づいてソートされたユーザーによってトリガーされるデフォルトおよびカスタムのリスク指標。
- 総発生回数別のリスク指標**:** 発生回数に基づいてソートされたユーザーによってトリガーされるデフォルトリスク指標とカスタムリスク指標。

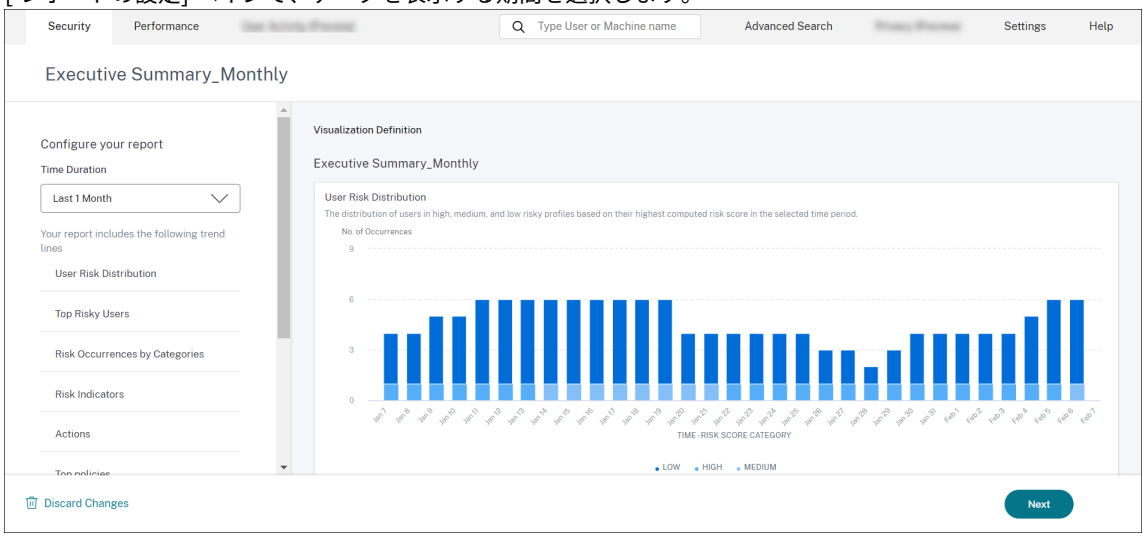
エグゼクティブレポートを編集する

エグゼクティブレポートを編集するには、次の手順を実行します:

1. [編集] アイコンをクリックします。



2. [レポートの設定] ペインで、データを表示する期間を選択します。



3. [次へ] をクリックします。[レポートの保存] ウィンドウが表示されます。

> 注記:
>
> 変更を破棄するには、「変更を破棄」をクリックします。

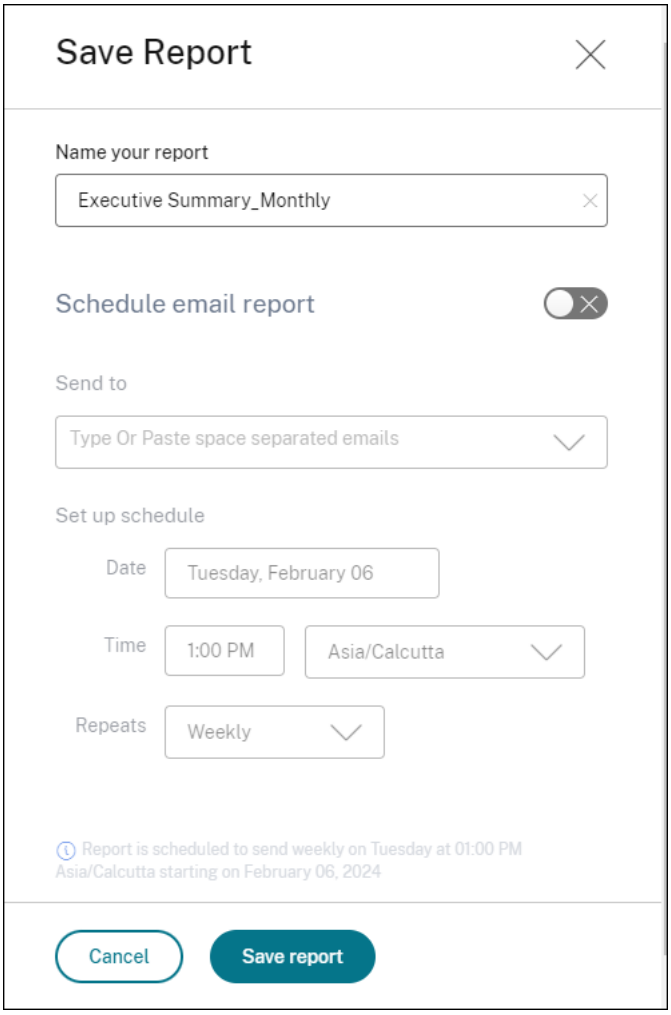
4. [レポートの保存] ペインで、次の詳細を入力します:

   a) レポートに名前を付ける: エグゼクティブレポートの名前。

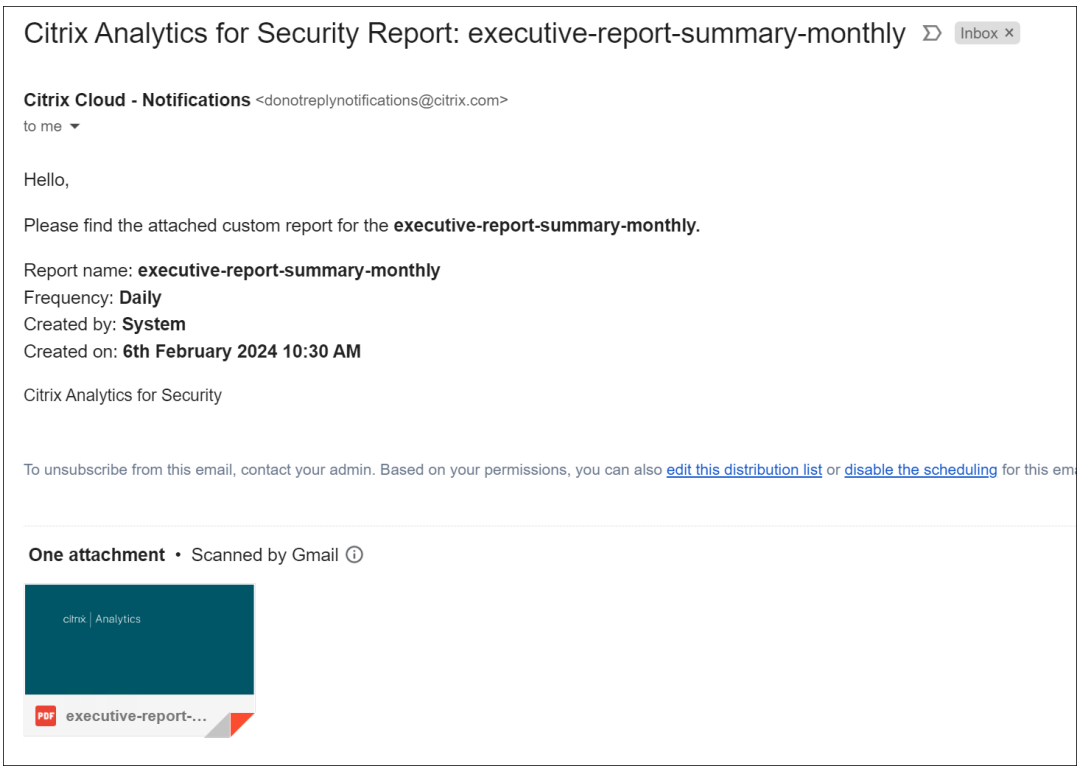
   b) メールレポートをスケジュールする: オンに切り替えてレポートをスケジュールします。トグルはデフォルトではオフになっています。

c) 送信先: ドロップダウンから配布リストを選択します。配布リストと個々の電子メールアドレスを組み合わせて追加することもできます。カスタマイズされた配布リストを作成するには、「管理者メール設定」を参照してください。

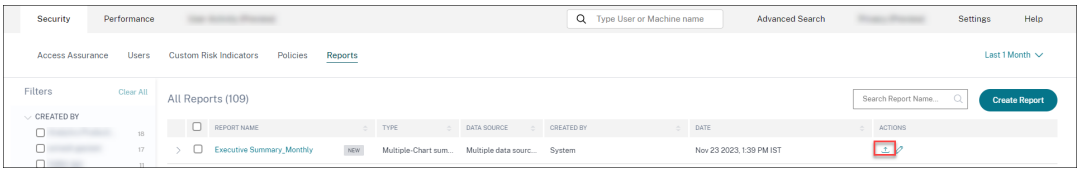
d) スケジュールの設定: 選択した対象者にレポートを最初に送信する時間と、レポートを繰り返す時間を選択します。



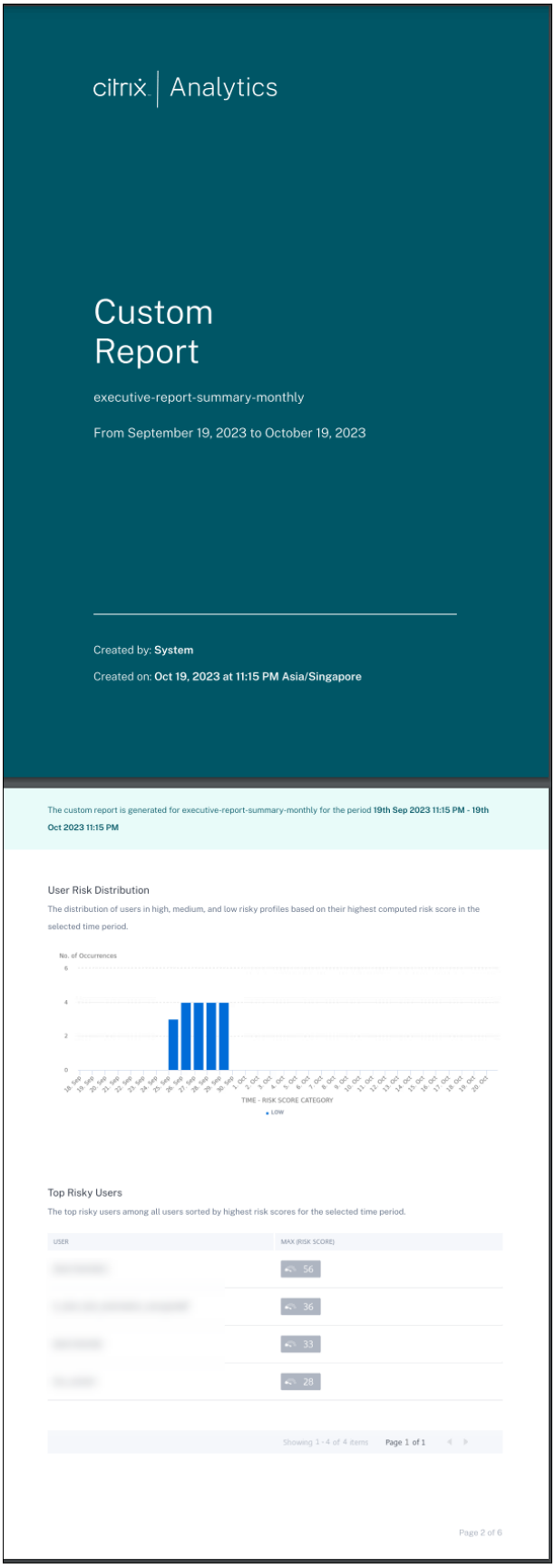
e) [レポートを保存] をクリックします。その後、レポートはリストされた受信者に電子メールとして送信されます。



または、エクスポート記号を使用してエグゼクティブレポートを PDF としてエクスポートすることもできます。



次のスクリーンショットは、PDF 出力のサンプルを示しています:



セルフサービス検索

December 7, 2023

セルフサービス検索とは何ですか

セルフサービス検索機能を使用すると、データソースから受信したユーザーイベントを検索してフィルタリングできます。基礎となるユーザーイベントとその属性を調べることができます。これらのイベントは、データの問題を特定し、トラブルシューティングするのに役立ちます。検索ページには、データソースのさまざまなファセット (ディメンション) と指標が表示されます。検索クエリを定義し、フィルタを適用して、定義した基準に一致するイベントを表示できます。デフォルトでは、セルフサービス検索ページには、過去 1 日のユーザーイベントが表示されます。

現在、セルフサービス検索機能は、次のデータソースで使用できます。

- Authentication
- Gateway
- Secure Browser
- Secure Private Access
- アプリケーションとデスクトップ
- パフォーマンスユーザー、マシン、セッション

また、定義したポリシーに一致するイベントに対してセルフサービス検索を実行することもできます。詳細については、ポリシーのセルフサービス検索を参照してください。

セルフサービス検索にアクセスする方法

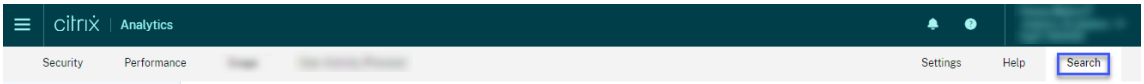
次のオプションを使用して、セルフサービス検索にアクセスできます。

- トップバー: トップバーの [検索] をクリックすると、選択したデータソースのすべてのユーザーイベントが表示されます。
- ユーザープロファイルページのリスクタイムライン:[イベント検索] をクリックして、各ユーザーのイベントを表示します。

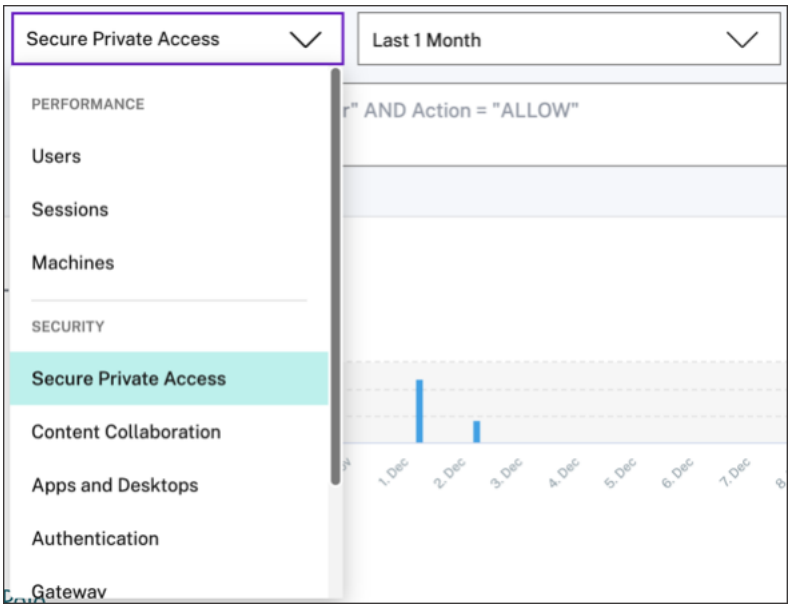
トップバーからのセルフサービス検索

ユーザーインターフェイスの任意の場所からセルフサービス検索ページに移動するには、このオプションを使用します。

1. [検索（Search）] をクリックして、セルフサービスページを表示します。



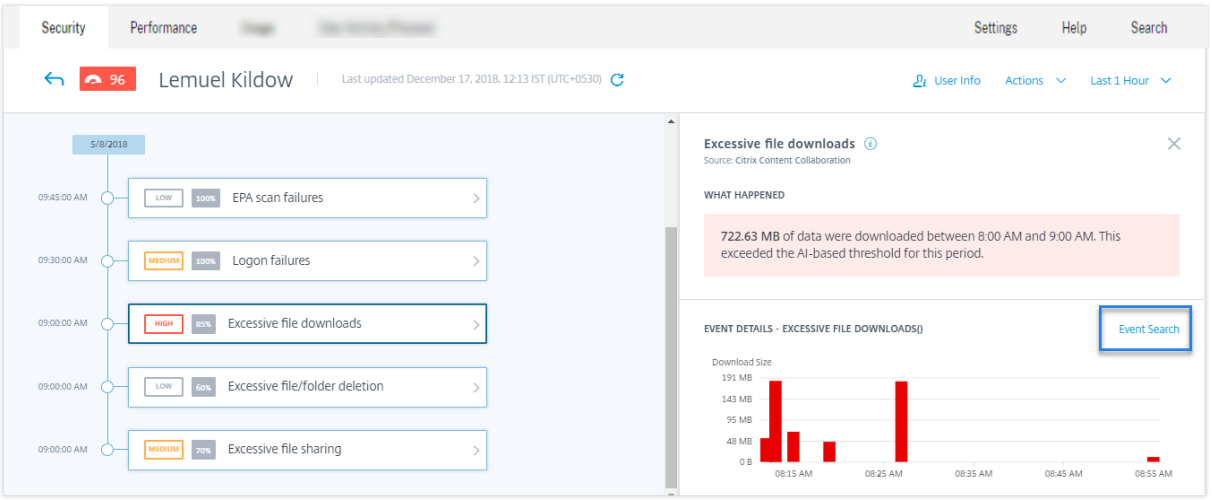
2. データソースと期間を選択して、対応するイベントを表示します。



ユーザーのリスクタイムラインからのセルフサービス検索

リスク指標に関連付けられたユーザーイベントを表示する場合は、このオプションを使用します。

ユーザーのタイムラインからリスク指標を選択すると、右側のペインにリスク指標情報セクションが表示されます。[イベント検索] をクリックして、セルフサービス検索ページで、ユーザーおよびデータソース (リスク指標がトリガーされる) に関連付けられたイベントを調べます。



ユーザーリスクタイムラインの詳細については、「リスクタイムライン」を参照してください。

セルフサービス検索の使用方法

セルフサービス検索ページの次の機能を使用します。

- イベントをフィルタリングするファセット 。
- 検索ボックスにクエリを入力し 、イベントをフィルタリングします。
- 期間を選択するための時間セレクタ 。
- タイムラインの詳細 。イベントグラフを表示します。
- イベントデータを使用して 、イベントを表示します。
- CSV 形式にエクスポートして 、検索イベントを CSV ファイルとしてダウンロードします。
- ビジュアルサマリーをエクスポートして 、検索クエリのビジュアルサマリーレポートをダウンロードします。
- イベントを複数の列で並べ替えるには 、複数列でソートします。

ファセットを使用してイベントをフィルタリングする

ファセットは、イベントを構成するデータポイントの要約です。ファセットはデータソースによって異なります。たとえば、Secure Private Access データソースのファセットは、評判、アクション、場所、およびカテゴリグループです。一方、アプリとデスクトップのファセットは、イベントタイプ、ドメイン、プラットフォームです。

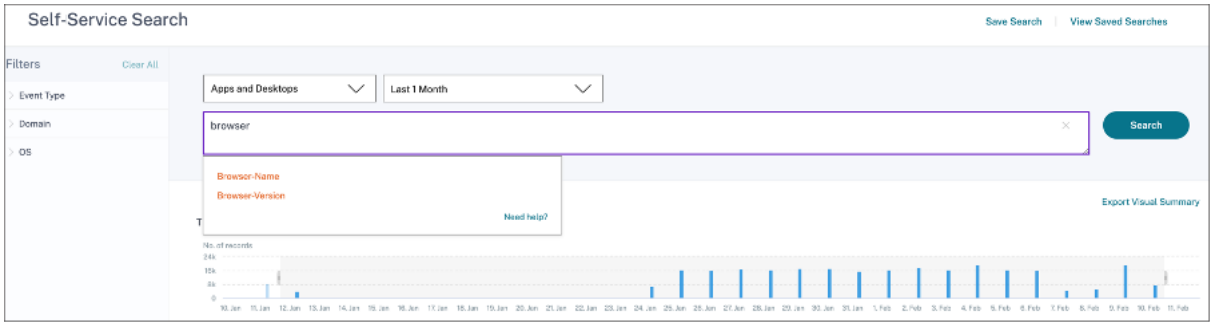
ファセットを選択して、検索結果をフィルタリングします。選択したファセットがチップとして表示されます。

各データソースに対応するファセットについて詳しくは、この記事で前述したデータソースのセルフサービス検索の記事を参照してください。

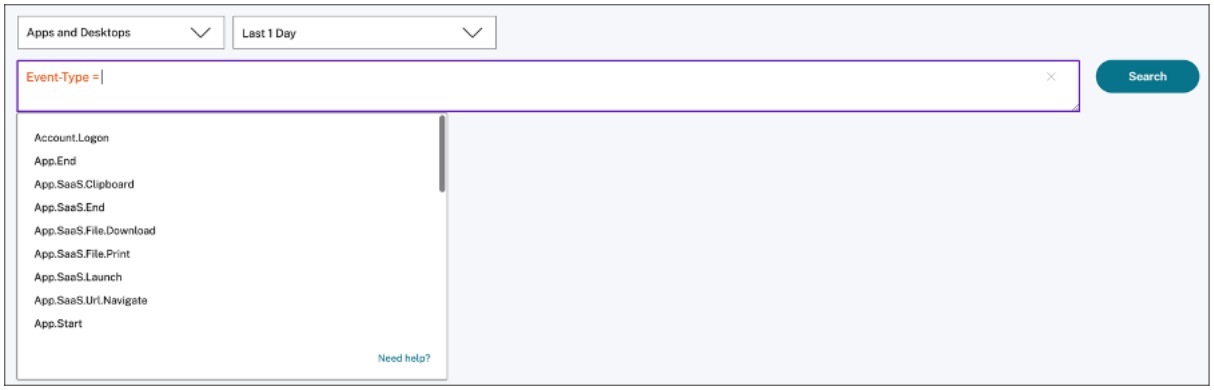
検索ボックスで検索クエリを使用してイベントをフィルタリングする

検索ボックスにカーソルを置くと、ユーザーイベントに基づいたディメンションのリストが検索ボックスに表示されます。これらのディメンションは、データソースによって異なります。ディメンションと有効な演算子を使用して 、検索条件を定義し、必要なイベントを検索します。

たとえば、アプリとデスクトップのセルフサービス検索では、`Browser`ディメンションに対して次の値が取得されます。ディメンションを使用してクエリを入力し、期間を選択して、[検索] をクリックします。



特定のディメンション（Event-TypeやClipboard-Operationなど）を有効な演算子と一緒に選択すると、ディメンションの値が自動的に表示されます。推奨オプションから値を選択するか、要件に応じて新しい値を入力できます。



検索クエリでサポートされる演算子　検索クエリで次の演算子を使用して、検索結果を絞り込みます。

演算子	説明	例	出力
	検索ディメンションに値を割り当てます。	User-Name : John	ユーザー John のイベントを表示します。
=	検索ディメンションに値を割り当てます。	User-Name = John	ユーザー John のイベントを表示します。
~	類似した値を持つイベントを検索します。	User-Name ~ test	類似のユーザー名を持つイベントを表示します。
" "	値をスペースで区切って囲みます。	User-Name = “John Smith”	ユーザー John Smith のイベントを表示します。
< >	リレーショナル値を検索します。	Data Volume > 100	データボリュームが 100 GB を超えるイベントを表示します。
AND	指定した条件が真であるイベントを検索します。	User-Name : John AND Data Volume > 100	データボリュームが 100 GB を超えるユーザー John のイベントを表示します。
!~	指定した一致するパターンについてイベントをチェックします。この NOT LIKE 演算子は、イベント文字列のどこにも一致するパターンを含まないイベントを返します。	ユーザー名！~ ジョン	John、John Smith、または一致する名前「John」を含むユーザー以外のユーザーのイベントを表示します。

演算子	説明	例	出力
! =	イベントで、指定した文字列が正確にチェックされます。この NOT EQUAL 演算子は、イベント文字列のどこにも正確な文字列を含まないイベントを返します。	国!= 米国	米国以外の国のイベントを表示します。
*	指定した文字列に一致するイベントを検索します。現在、*演算子は次の演算子、:、=および!=でのみサポートされています。検索結果では大文字と小文字が区別されます。	User-Name = John*	John で始まるすべてのユーザー名のイベントを表示します。
		User-Name = *John*	John を含むすべてのユーザー名のイベントを表示します。
		User-Name = *Smith	Smith で終わるすべてのユーザー名のイベントを表示します。
		ユーザー名:John*	John で始まるすべてのユーザー名のイベントを表示します。
		ユーザー名:*John*	John を含むすべてのユーザー名のイベントを表示します。
		ユーザー名:*Smith	Smith で終わるすべてのユーザー名のイベントを表示します。
		ユーザー名! = ジョン *	John で始まるすべてのユーザー名のイベントを表示します。
		ユーザー名! = * スミス	Smith で終わらないすべてのユーザー名のイベントを表示します。

演算子	説明	例	出力
IN	検索ディメンションに複数の値を割り当てて、1 つ以上の値に関連するイベントを取得します。注：現在、この演算子は、アプリとデスクトップ -Device ID、Domain、Event-TypeおよびUser-Nameのディメンションで使用できます。この演算子は、文字列値にのみ適用されます。	ユーザーネーム IN (ジョン、ケビン)	ジョンまたはケビンに関連するすべてのイベントを見つける。
NOT IN	検索ディメンションに複数の値を割り当てて、指定した値を含まないイベントを検索します。注：現在、この演算子は、アプリとデスクトップ -Device ID、Domain、Event-TypeおよびUser-Nameのディメンションで使用できます。この演算子は、文字列値にのみ適用されます。	User-Name NOT IN (John, Kevin)	John と Kevin 以外のすべてのユーザーのイベントを検索します。

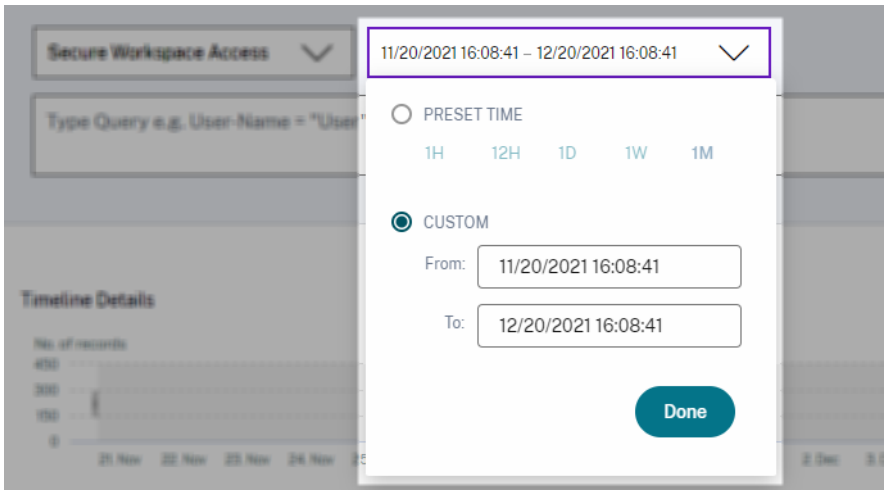
演算子	説明	例	出力
IS EMPTY	ディメンションの NULL 値または空の値をチェックします。この演算子は、App-Name、Browser、Countryなどの文字列タイプのディメンションでのみ機能します。Upload-File-Size、Download-File-Size、Client-IP などの非文字列 (数値) タイプのディメンションには使用できません。	Country IS EMPTY	国名が利用できない、または空である (指定されていない) イベントを検索します。
IS NOT EMPTY	ディメンションの NULL 値でない値または特定の値がないかどうかをチェックします。この演算子は、App-Name、Browser、Countryなどの文字列タイプのディメンションでのみ機能します。Upload-File-Size、Download-File-Size、Client-IP などの非文字列 (数値) タイプのディメンションには使用できません。	Country IS NOT EMPTY	国名が利用可能または指定されているイベントを検索します。
OR	どちらかまたは両方の条件に該当する値を検索します。	(ユーザー名 = John* またはユーザー名 = *Smith) およびイベントタイプ = 「Session.Logon」	John で始まる、または Smith Session.Logon で終わるすべてのユーザー名のイベントを表示します。

> 注
>
> **NOT EQUAL** 演算子では、クエリーのディメンションの値を入力するときに、データ・ソースのセルフ・サービス検索ページで使用可能な正確な値を使用します。寸法値では、大文字と小文字が区別されます。

データソースの検索クエリを指定する方法の詳細については、この記事で前述したデータソースのセルフサービス検索の記事を参照してください。

イベントを表示する時間を選択

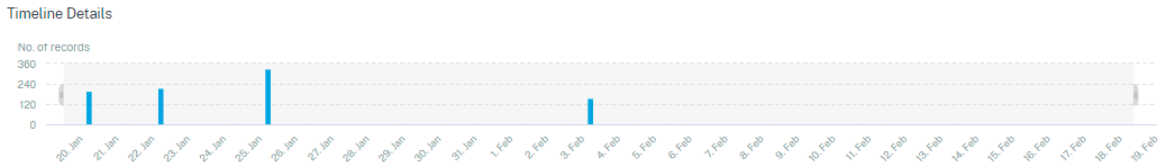
プリセット時間を選択するか、カスタムの時間範囲を入力して [検索（Search）] をクリックしてイベントを表示します。



タイムラインの詳細を表示する

タイムラインには、選択した期間のユーザーイベントがグラフィカルに表示されます。セレクタバーを移動して時間範囲を選択し、選択した時間範囲に対応するイベントを表示します。

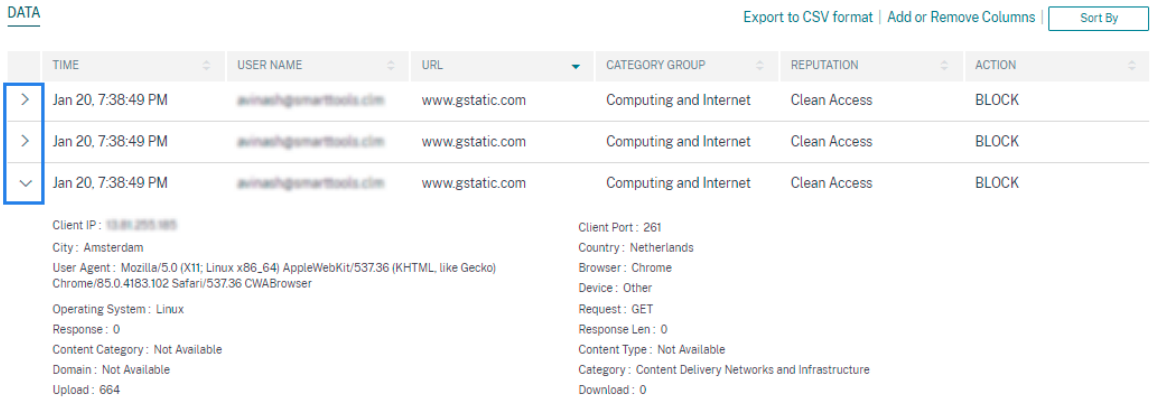
この図は、アクセスデータのタイムラインの詳細を示しています。



イベントを見る

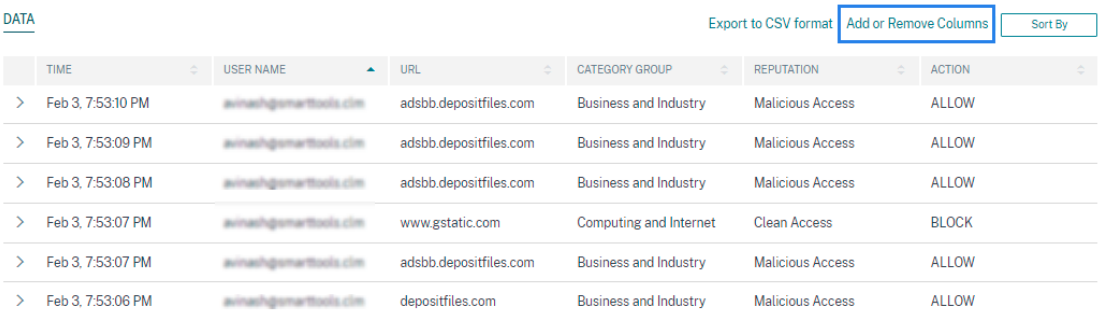
ユーザーイベントに関する詳細情報を表示できます。**DATA** テーブルで、各列の矢印をクリックして、ユーザーイベントの詳細を表示します。

この図は、ユーザーのアクセスデータに関する詳細を示しています。

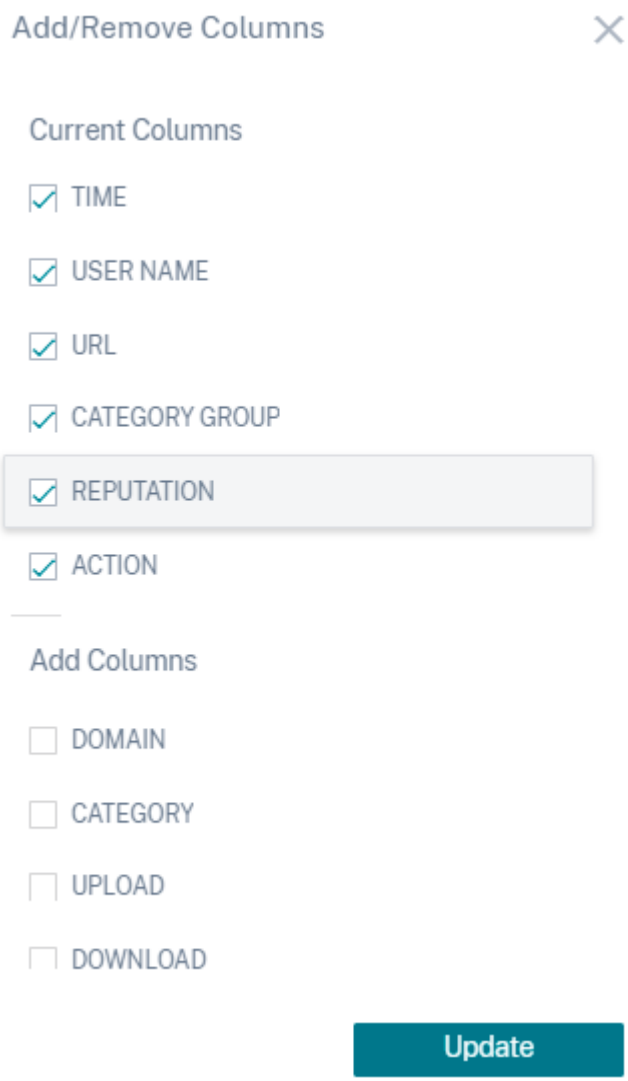


列を追加または削除する　イベントテーブルの列を追加または削除して、対応するデータポイントを表示または非表示にすることができます。以下を実行します:

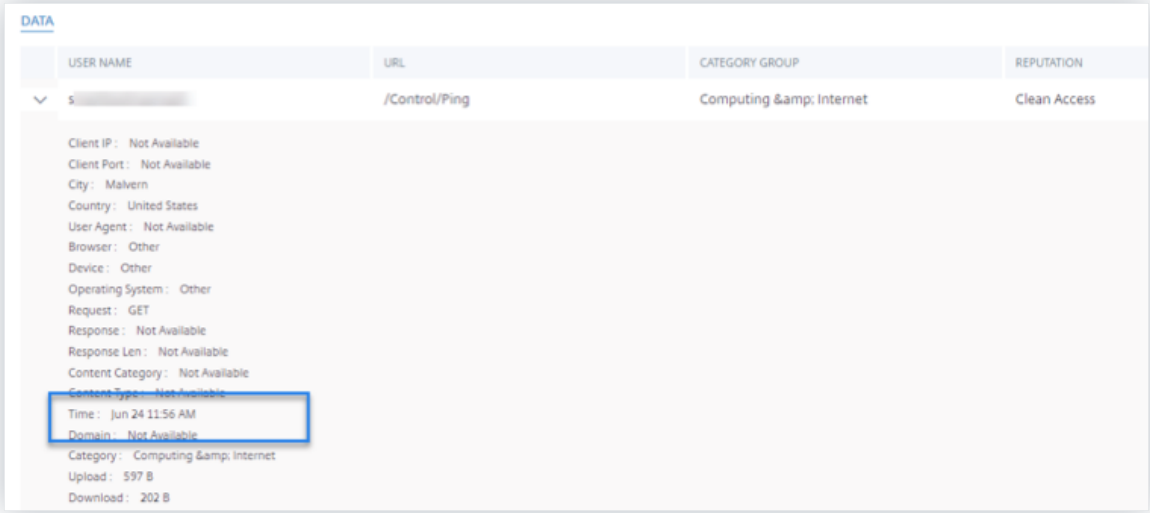
1. [列の追加または削除] をクリックします。



2. リストからデータ要素を選択または選択解除し、「更新」をクリックします。

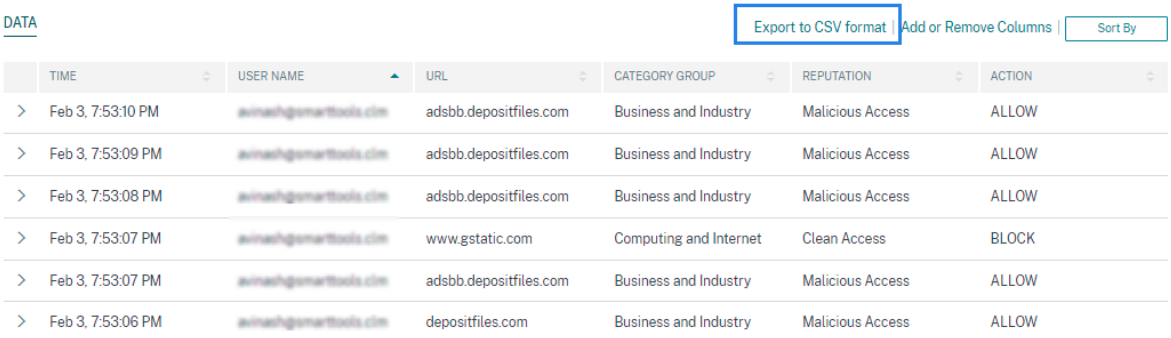


リストからデータポイントを選択解除すると、対応する列がイベントテーブルから削除されます。ただし、ユーザーのイベント行を展開すると、そのデータポイントを表示できます。たとえば、リストから **TIME** データポイントを選択解除すると、**TIME** 列がイベントテーブルから削除されます。時間レコードを表示するには、ユーザのイベント行を展開します。



イベントを **CSV** ファイルにエクスポートする

検索結果を CSV ファイルにエクスポートし、参照用に保存します。[**CSV** 形式にエクスポート（**Export to CSV format**）] をクリックしてイベントをエクスポートし、生成された CSV ファイルをダウンロードします。**CSV** 形式へのエクスポート機能を使用して、**10** 万行をエクスポートできます。



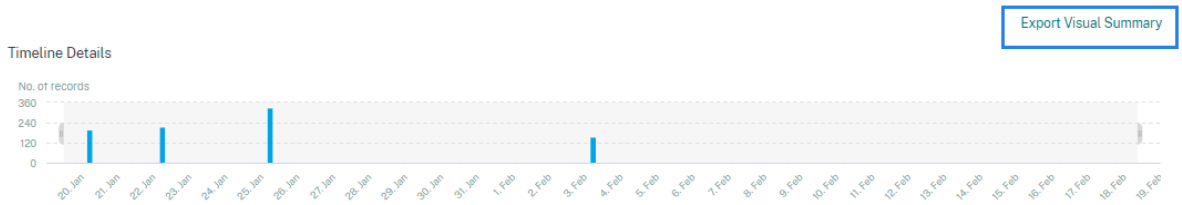
ビジュアルサマリーを書き出す

検索クエリのビジュアルサマリーレポートをダウンロードし、他のユーザー、管理者、またはエグゼクティブチームとコピーを共有できます。

ビジュアルサマリーをエクスポートをクリックして、ビジュアルサマリーレポートを PDF としてダウンロードします。レポートには、次の情報が含まれています。

- 選択した期間のイベントに対して指定した検索クエリ。
- 選択した期間のイベントに適用したファセット（フィルタ）。
- 選択した期間の検索イベントのタイムラインチャート、棒グラフ、グラフなどの視覚的なサマリー。

データソースの場合、データが棒グラフ、タイムラインの詳細などのビジュアル形式で表示される場合にのみ、ビジュアルサマリーレポートをダウンロードできます。それ以外の場合、このオプションは使用できません。たとえば、アプリとデスクトップ、セッションなどのデータソースのビジュアルサマリーレポートをダウンロードして、データをタイムラインの詳細と棒グラフとして表示できます。Users や Machines などのデータソースの場合、データは表形式でのみ表示されます。したがって、ビジュアルサマリーレポートをダウンロードすることはできません。

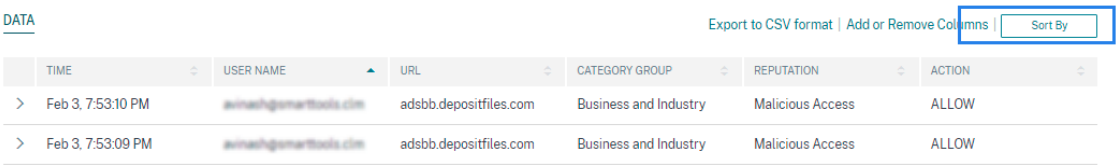


複数列の並べ替え

並べ替えは、データの整理に役立ち、可視性を高めます。セルフサービス検索ページで、ユーザーイベントを 1 つ以上の列で並べ替えることができます。列は、ユーザー名、日付と時刻、URL などのさまざまなデータ要素の値を表します。これらのデータ要素は、選択したデータソースによって異なります。

複数列の並べ替えを実行するには、次の操作を行います。

1. [並べ替え] をクリックします。

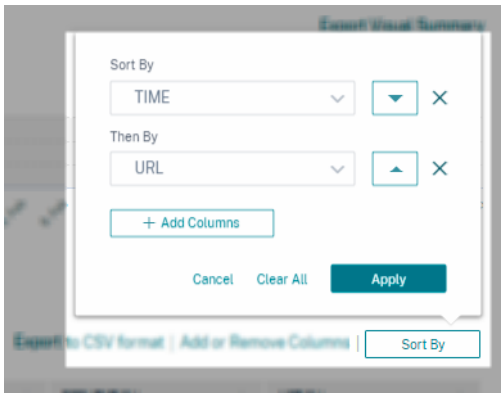


2. [並べ替え基準] リストから列を選択します。
3. 列内のイベントを並べ替えるには、昇順 (上矢印) または降順 (下矢印) の並べ替え順序を選択します。
4. [**+** 列の追加] をクリックします。
5. [次の項目] リストから別の列を選択します。
6. 列内のイベントをソートするには、ソート順として、昇順（上矢印）または降順（下方向エラー）を選択します。

   > 注
   >
   > 最大 6 つの列を追加して、並べ替えを実行できます。

7. [適用] をクリックします。
8. 上記の設定を適用しない場合は、[キャンセル] をクリックします。選択した列の値を削除するには、「すべてクリア」**(Clear All)** をクリックします。

次の例は、Secure Private Access イベントに対する複数列のソートを示しています。イベントは、時刻 (新しい順)、URL (アルファベット順) の順にソートされます。



または、**Shift** キーを使用して複数列の並べ替えを実行することもできます。**Shift** キーを押しながら列見出しをクリックして、ユーザーイベントを並べ替えます。

セルフサービス検索を保存する方法

管理者は、セルフサービスクエリを保存できます。この機能により、分析やトラブルシューティングで頻繁に使用するクエリを書き換える時間と労力を節約できます。次のオプションは、クエリーとともに保存されます。

- 適用された検索フィルタ
- 選択したデータソースと期間

セルフサービスクエリを保存するには、次の手順を実行します。

1. 必要なデータソースと期間を選択します。
2. 検索バーにクエリを入力します。
3. 必要なフィルターを適用します。
4. [検索を保存] をクリックします。
5. カスタムクエリを保存する名前を指定します。

   > (注
   >
   >) クエリ名が一意であることを確認します。それ以外の場合、クエリは保存されません。

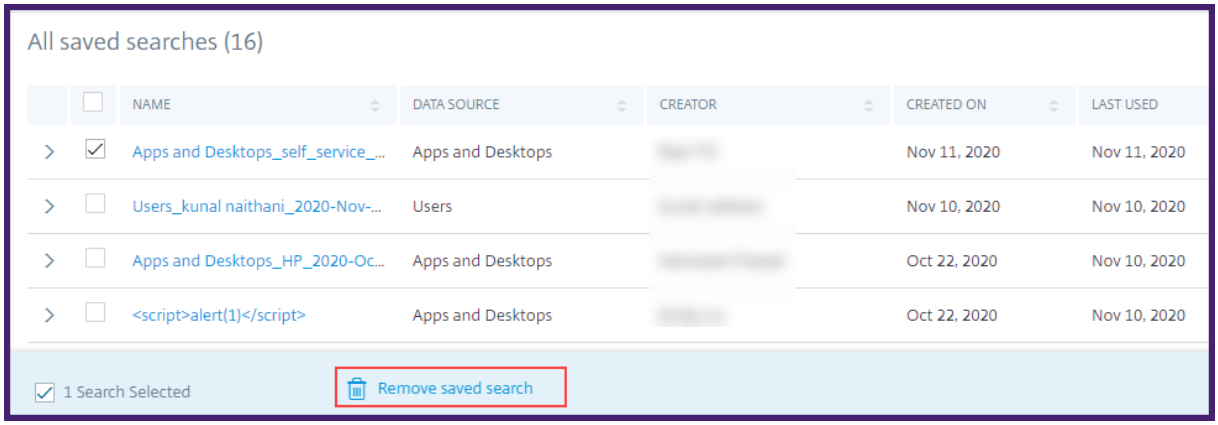
6. 検索クエリレポートのコピーを自分や他のユーザーに定期的に送信する場合は、**[**電子メールレポートのスケジュール] ボタンを有効にします。詳細については、「検索クエリのメールをスケジュールする」を参照してください。
7. [保存] をクリックします。

保存した検索を表示するには、次の手順に従います。

1. [保存された検索の表示] をクリックします。
2. 検索クエリの名前をクリックします。

保存した検索を削除するには:

1. [保存された検索の表示] をクリックします。
2. 保存した検索クエリを選択します。
3. [保存された検索条件を削除] をクリックします。



保存済み検索を変更するには、次の操作を行います。

1. [保存された検索の表示] をクリックします。
2. 保存した検索クエリの名前をクリックします。
3. 要件に基づいて、検索クエリまたはファセットの選択を変更します。
4. [検索の更新] **>** [保存] をクリックして、変更した検索を同じ検索クエリ名で更新して保存します。
5. 変更した検索を新しい名前で保存する場合は、下矢印をクリックし、[新しい検索として保存] **>** [名前を付けて保存] をクリックします。

検索を新しい名前に置き換えると、検索は新しいエントリとして保存されます。置換時に既存の検索名を保持すると、変更された検索データが既存の検索データを上書きします。

> 注
>
> - クエリの所有者のみが、保存された検索を変更または削除できます。
> - 保存した検索リンクアドレスをコピーして、他のユーザーと共有することができます。

検索クエリのメールをスケジュールする

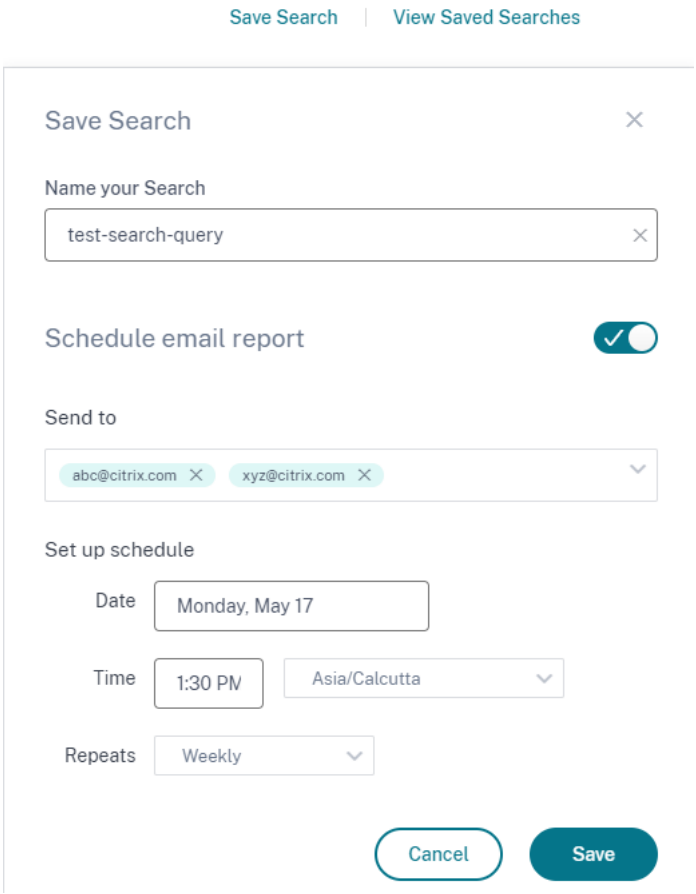
メール配信スケジュールを設定することで、検索クエリレポートのコピーを自分や他のユーザーに定期的に送信できます。

このオプションは、検索クエリレポートに棒グラフ、タイムラインの詳細などのビジュアル形式のデータが含まれている場合にのみ使用できます。そうしないと、メール配信をスケジュールできません。たとえば、[アプリとデスクトップ]、[セッション] などのデータソースの電子メールをスケジュールして、タイムラインの詳細と棒グラフとしてデータを表示できます。Users や Machines などのデータソースの場合、データは表形式でのみ表示されます。したがって、メールをスケジュールすることはできません。

検索クエリの保存中にメールをスケジュールする

検索クエリの保存中に、電子メール配信スケジュールを次のように設定します。

1. [検索の保存] ダイアログボックスで、[電子メールレポートのスケジュール] ボタンを有効にします。



2. 受信者の電子メールアドレスを入力または貼り付けます。

   > 注
   >
   > メールグループはサポートされていません。

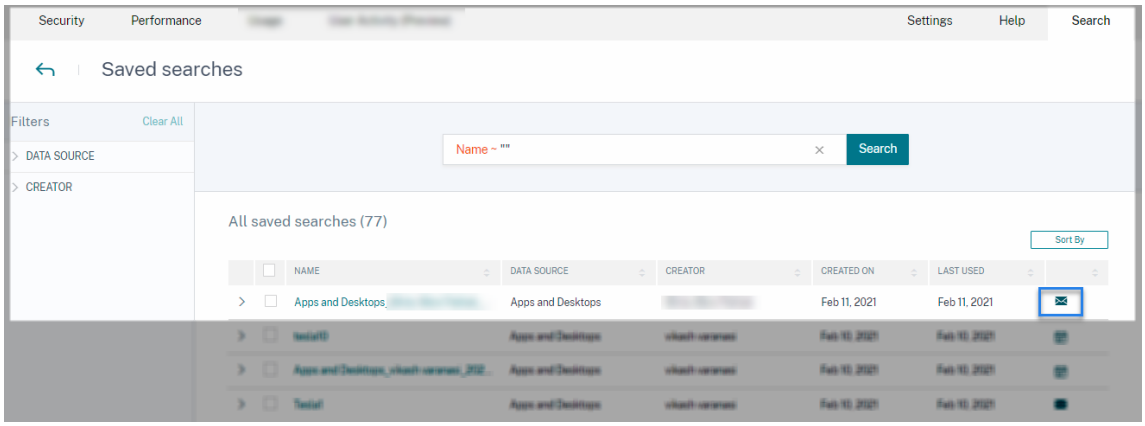
3. メール配信の日付と時刻を設定します。
4. 配信頻度（毎日、毎週、または毎月）を選択します。
5. ［保存］をクリックします。

すでに保存されている検索クエリのメールをスケジュールする

以前に保存した検索クエリの電子メール配信スケジュールを設定する場合は、次の操作を行います。

1. [保存された検索の表示] をクリックします。
2. 作成した検索クエリに移動します。[このクエリを電子メールで送信] アイコンをクリックします。

> 注
>
> 保存した検索クエリの電子メール配信をスケジュールできるのは、クエリの所有者だけです。



3. [電子メールレポートをスケジュールする] ボタンを有効にします。
4. 受信者の電子メールアドレスを入力または貼り付けます。

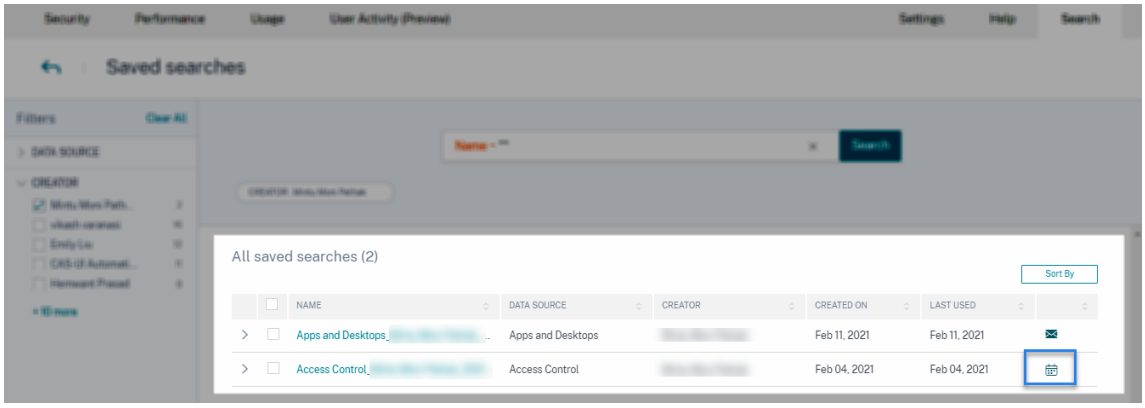
> 注
>
> メールグループはサポートされていません。

5. メール配信の日付と時刻を設定します。
6. 配信頻度（毎日、毎週、または毎月）を選択します。
7. [保存] をクリックします。

検索クエリのメール配信スケジュールを停止する

1. [保存された検索の表示] をクリックします。
2. 作成した検索クエリに移動します。[メール配信スケジュールの表示] アイコンをクリックします。

> 注
>
> 保存した検索クエリの電子メールスケジュールを停止できるのは、クエリの所有者だけです。



3. [電子メールレポートのスケジュール] ボタンを無効にします。
4. ［保存］をクリックします。

メールコンテンツ

受信者は、「Citrix Cloud-通知 < donotreplynotifications@citrix.com >」から検索クエリレポートに関する電子メールを受信します。レポートは PDF ドキュメントとして添付されます。メールは、[電子メールレポートのスケジュール] 設定で定義した一定の間隔で送信されます。

検索クエリレポートには、次の情報が含まれています。

- 選択した期間のイベントに対して指定した検索クエリ。
- イベントに適用したファセット (フィルタ)。
- タイムラインチャート、棒グラフ、検索イベントのグラフなどの視覚的なサマリー。

フルアクセス管理者および読み取り専用アクセス管理者の権限

- フルアクセス権を持つ Citrix Cloud 管理者は、［検索］ページで使用できるすべての機能を使用できます。
- 読み取り専用アクセス権を持つ Citrix Cloud 管理者の場合、［検索］ページでは次のアクティビティのみを実行できます。
  - データソースと期間を選択して、検索結果を表示します。
  - 検索クエリを入力し、検索結果を表示します。
  - 他の管理者の保存済み検索結果を表示します。
  - ビジュアルサマリーをエクスポートし、検索結果を CSV ファイルとしてダウンロードします。

管理者の役割について詳しくは、「Citrix Analytics の管理者の役割の管理」を参照してください。

認証のセルフサービス検索

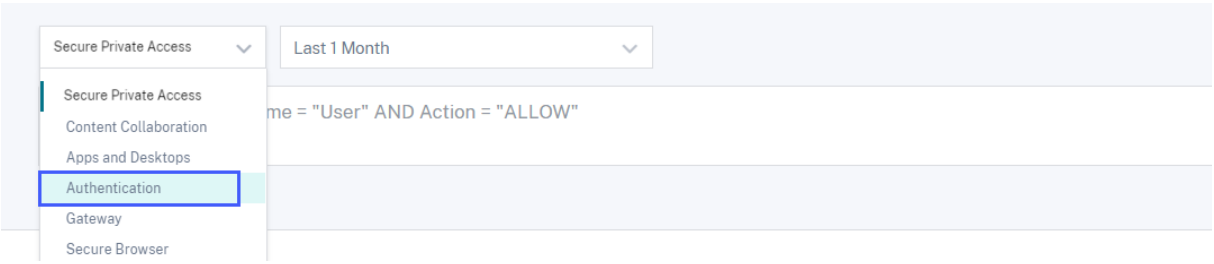
October 11, 2021

セルフサービス検索を使用して、企業内の Citrix Cloud ユーザーのユーザー認証の詳細に関するインサイトを取得します。Citrix Analytics for Security は、Citrix Cloud のアイデンティティおよびアクセス管理サービスからユーザー認証イベントを受信します。ユーザーログイン、ユーザーのログオフ、クライアントの更新などの認証イベントは、セルフサービス検索ページに表示されます。

検索機能の詳細については、「セルフサービス検索」を参照してください。

認証データソースを選択します

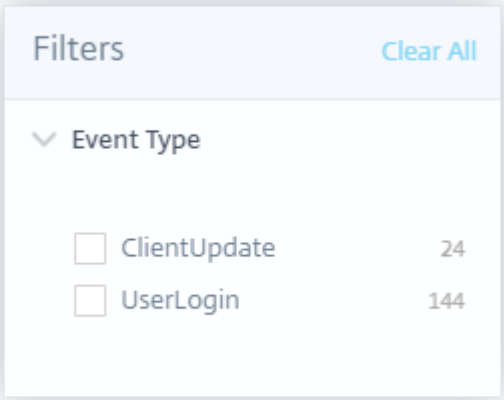
認証イベントを表示するには、リストから [認証] を選択します。デフォルトでは、セルフサービスページには過去 1 日のイベントが表示されます。また、イベントを表示する期間を選択することもできます。



イベントをフィルタリングするファセットを選択します

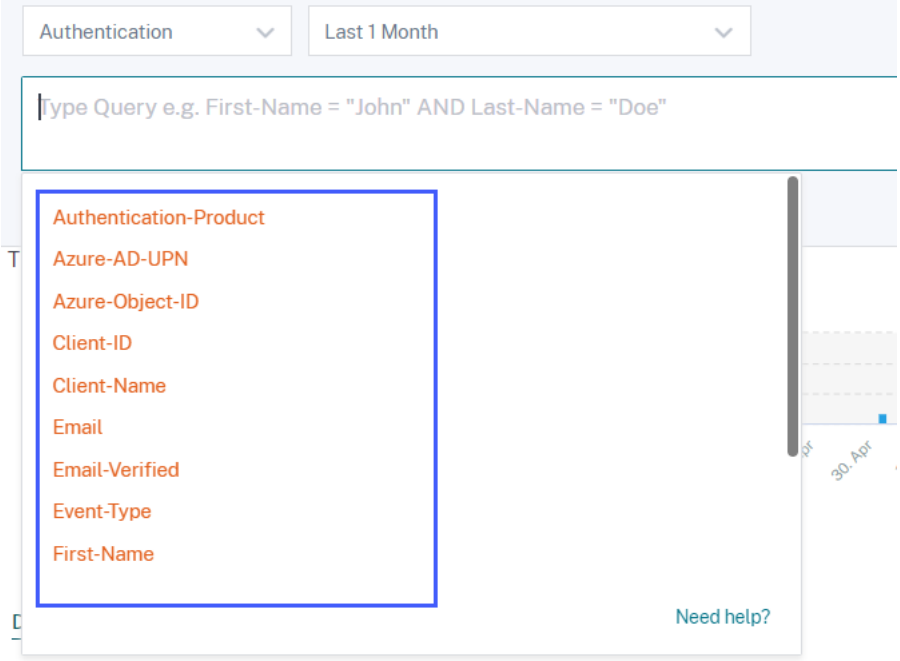
認証イベントには次のフィルタを使用します。

- **Event Type**: ユーザログイン、ユーザログオフ、クライアントアップデートなどのユーザイベントタイプに基づいてイベントを検索します。



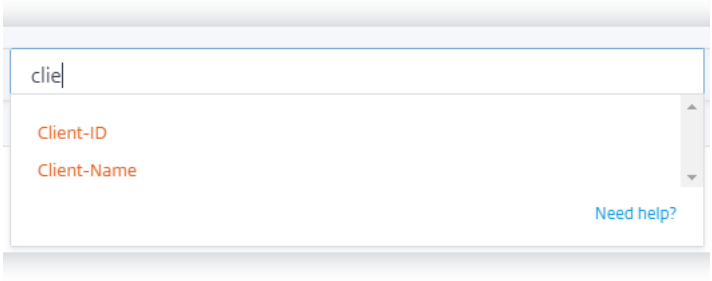
イベントをフィルタリングする検索クエリを指定する

検索ボックスにカーソルを置いて、認証イベントのディメンションのリストを表示します。ディメンションと演算子を使用してクエリを指定し 、必要なイベントを検索します。

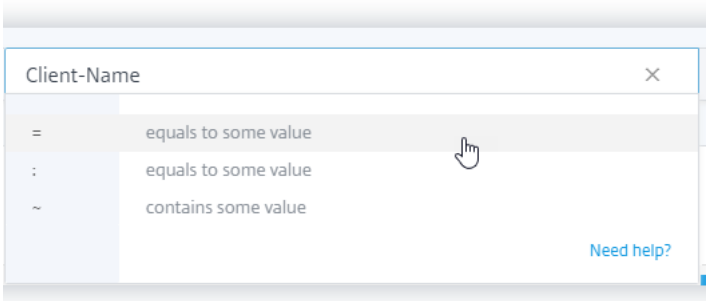


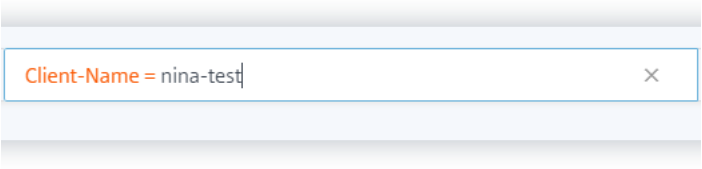
たとえば、電子メールステータスが検証されたクライアント「nina-test」の認証イベントを表示するとします。

1. 検索ボックスに「client」と入力して、関連するディメンションを取得します。

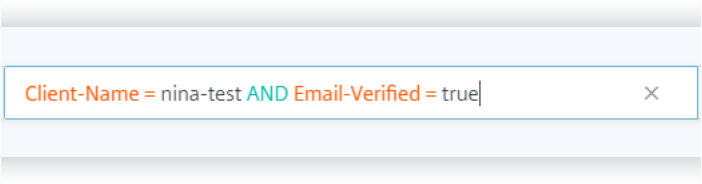


2. [クライアント名] を選択し、等号演算子を使用して値「nina-test」を指定します。





3. AND 演算子を選択し、[電子メールで検証済み] ディメンションを選択します。等号演算子を使用して、[電子メール検証済み] に値「true」を割り当てます。「true」の値は、ユーザーのメールが検証されていることを示します。



4. 期間を選択し、［検索］をクリックして、**DATA** テーブルのイベントを表示します。

Gateway セルフサービス検索

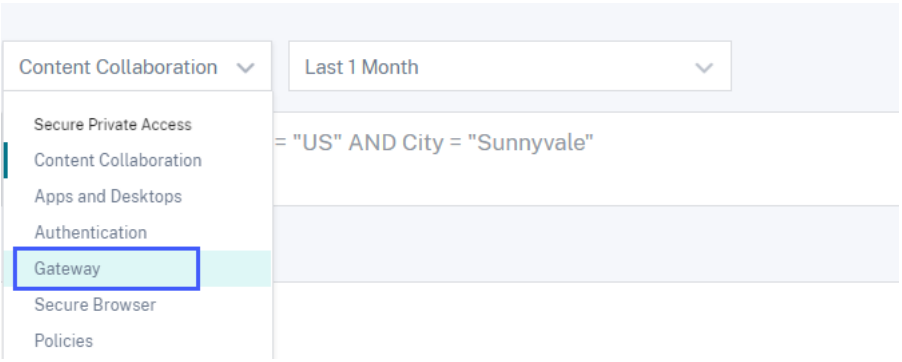
October 11, 2021

セルフサービス検索機能を使用して、Citrix Gateway データソースから受信したユーザーイベントに関する洞察を取得します。ユーザーが Citrix Gateway を介してファイルサーバー、アプリケーション、Web サイトなどのネットワークリソースにアクセスすると、ユーザー接続ごとにイベントが生成されます。ユーザイベントの例としては、認証ステージ、認可タイプ、VPN セッションコードなどがあります。Citrix Analytics for Security はこれらのイベントを受信し、セルフサービス検索ページに表示します。ユーザーとそのアクセスの詳細を表示できます。

検索機能の詳細については、「セルフサービス検索」を参照してください。

[Gateway] データソースを選択します

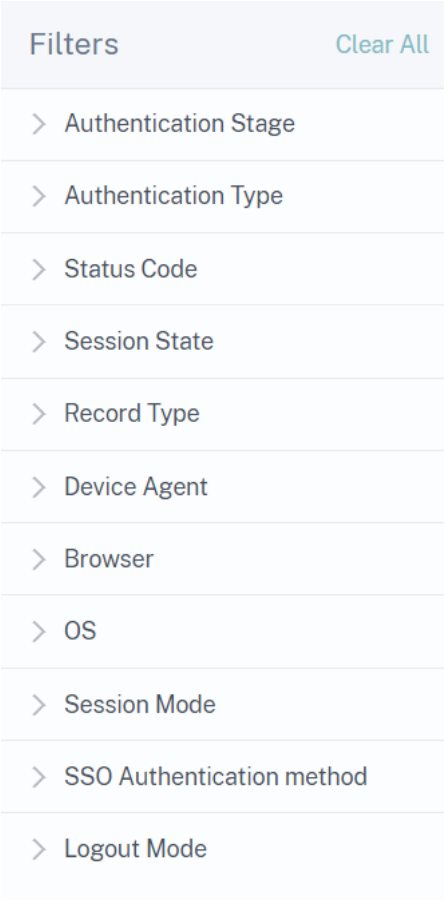
ゲートウェイイベントを表示するには、リストから [ゲートウェイ] を選択します。デフォルトでは、セルフサービスページには過去 1 日のイベントが表示されます。また、イベントを表示する期間を選択することもできます。



> 注
>
> または、[セキュリティ] > [ユーザー] > [アクセスの概要] ダッシュボードから、[ゲートウェイのセルフサービス検索] ページにアクセスできます。正常なログインシナリオでは、ステータスコードでデータにアクセスできます。詳細については、「アクセスサマリー 」ダッシュボードを参照してください。

ファセットを使用してイベントをフィルタリングする

ファセットは、データソースから受信したイベントに基づいて分類されます。イベントをフィルタリングするには、次のファセットを使用します。



- **Authentication Stage**-プライマリ、セカンダリ、ターシャリなどのクライアント認証のさまざまなステージに基づいてイベントを検索します。
- 認証タイプ-ローカル、RADIUS、LDAP、TACACS、クライアント証明書認証（スマートカード認証を含む）などのクライアント認証タイプに基づいてイベントを検索します。
- デバイスエージェント-iPhone、iPad、Windows Mobile などのクライアントデバイスに基づいてイベントを検索します。

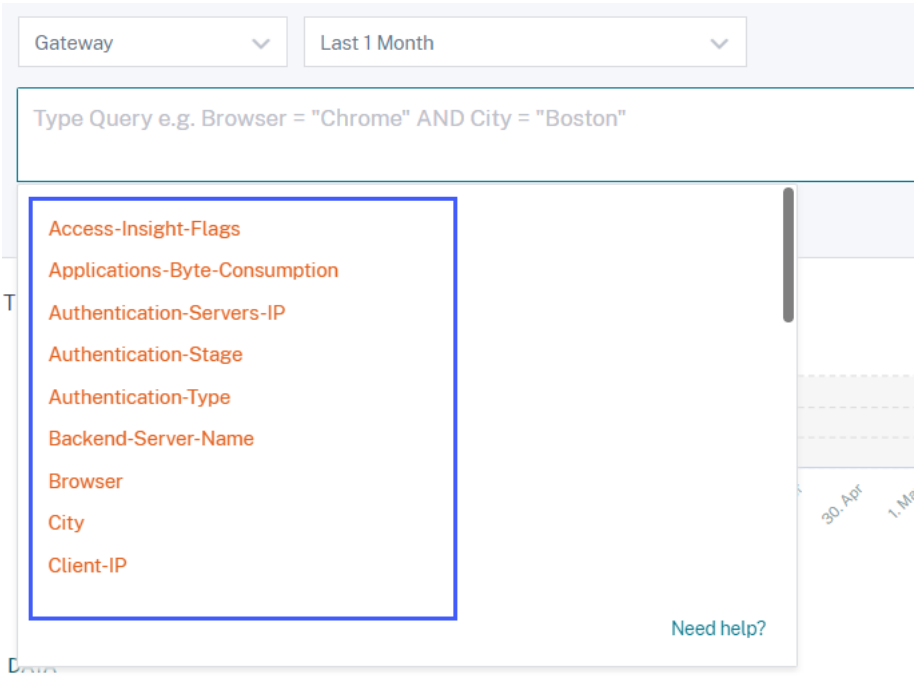
- レコードタイプ-VPN レコードのタイプに基づいてイベントを検索します。次の VPN レコードタイプを使用できます。

レコードタイプ	説明
VPN_AI	認証に関連するユーザーイベントをフィルタリングします。
VPN_IF	ICA ファイルに関連するユーザーイベントをフィルタリングします。
VPN_ST	セッションログアウトに関連するユーザーイベントをフィルタリングします。

- ブラウザ-Internet Explorer, Chrome, Firefox, Safari などのブラウザに基づいてイベントを検索します。
- **OS**-Windows、Mac、Linux、Android、iOS などのクライアントオペレーティングシステムに基づいてイベントを検索します。
- **[Status Code]**：SSL リダイレクト応答の失敗、認証失敗、シングルサインオンの失敗など、VPN ステータスコードに基づいてイベントを検索します。
- [**Session State]**：クライアントの状態、許可状態、SSO 状態、アプリケーション帯域幅の更新などの VPN セッション状態に基づいてイベントを検索します。
- セッションモード-フルトンネル、ICA プロキシ、クライアントレスなどの VPN セッションモードに基づいてイベントを検索します。
- **SSO** 認証方法-基本、ダイジェスト、NTLM、Kerberos、AG 基本、フォームベースの SSO など、さまざまなシングルサインオン認証方式に基づいてイベントを検索します。
- **Logout Mode**-内部エラーログアウト、セッションタイムアウトログアウト、ユーザ開始ログアウト、管理者がセッションを終了したなど、VPN ログアウトモードに基づいてイベントを検索します。

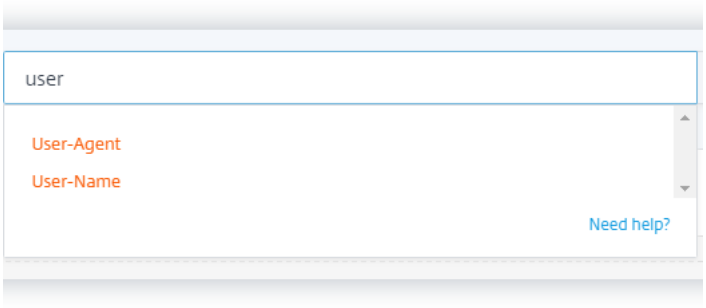
イベントをフィルタリングする検索クエリを指定する

検索ボックスにカーソルを置いて、Gateway イベントのディメンションのリストを表示します。ディメンションと演算子を使用してクエリを指定し 、必要なイベントを検索します。

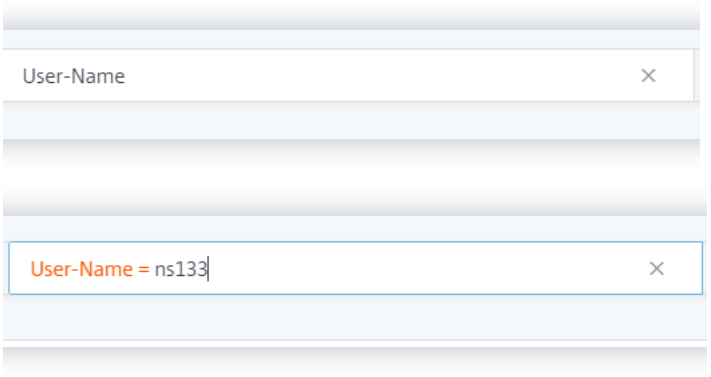


たとえば、VPN ステータスコードが「成功ログイン」であるユーザ「ns133」のイベントを表示するとします。

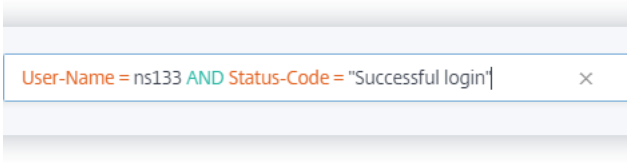
1. 検索ボックスに「user」と入力して、関連するディメンションを選択します。



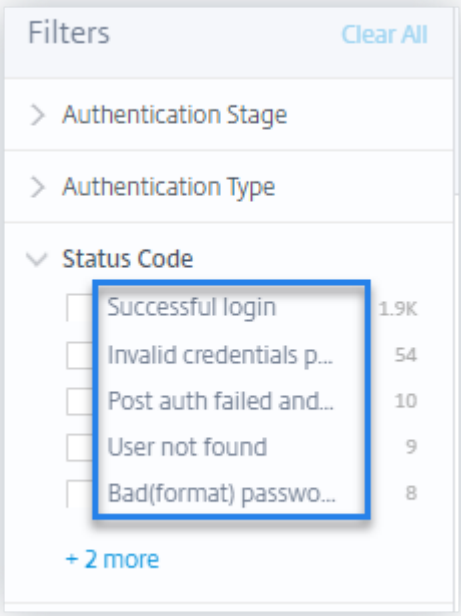
2. [ユーザー名] を選択し、等号演算子を使用して値「ns133」を入力します。



3. AND 演算子を選択し、次に [ステータスコード] ディメンションを選択します。等号演算子を使用して、ステータスコードに「正常なログイン」という文字列を入力します。



ステータスコードの可能な文字列値を識別するには、[ステータスコード] フィルタリストを展開し、検索クエリの文字列としてフィルタ名を使用します。



4. 期間を選択し、［検索］をクリックして、**DATA** テーブルのイベントを表示します。

検索クエリでサポートされる値

ディメンションに次の値を入力して、検索クエリを定義します。

アクセスインサイトフラグ

VPN セッションの状態を示します。次のいずれかのフラグ値を入力します。

VPN セッションステート	フラグ値
事前認証	2
nFactor (多要素) 認証の最終状態または最終状態	1
認証後	4

> 注
>
> このフラグは、認証イベントの前の VPN セッションステートにのみ適用されます。他のすべてのイベントでは、フラグの値はゼロです。

アプリケーション-バイト消費

Applications-Byte-Consumptionディメンションに、次の値を入力します。

値	種類	説明
例: 40, 100	数	使用しているアプリケーションによって消費されるデータ (バイト単位)。

認証サーバー**-IP**

Authentication-Servers-IPディメンションに、次の値を入力します。

値	種類	説明
例: 10.xxx.xx.xx	文字列	認証サーバの IP アドレス。

認証ステージ

Authentication-Stageディメンションに、次の値を入力します。

値	種類	説明
Primary、Secondary、または Tertiary	文字列	クライアント認証のさまざまな段階。

認証タイプ

Authentication-Typeディメンションに、次の値を入力します。

値	種類	説明
LDAP、SAML、Local、Radius、TACACS、SAMLIDP、またはOTP。	文字列	使用可能な方法のいずれかを使用してユーザーを認証します。

バックエンドサーバー名

Backend-Server-Nameディメンションに、次の値を入力します。

値	種類	説明
例: 10.xxx.xxx.xx	文字列	バックエンドサーバーの IP アドレス。

ブラウザー

Browserディメンションに、次の値を入力します。

値	種類	説明
PN Agent、Edge、Firefox、Chrome、または Safari。	文字列	使用するブラウザ。

市区町村

Cityディメンションに、次の値を入力します。

値	種類	説明
例: Boston, Beijing	文字列	ユーザーがログオンした市区町村。

クライアント **IP**

Client-IPディメンションに、次の値を入力します。

値	種類	説明
例: 10.xxx.xxx.xx	文字列	ユーザーデバイスの IP アドレス。

クライアント **IP** タイプ

Client-IP-Typeディメンションに、次の値を入力します。

値	種類	説明
公立、プライベート	文字列	ユーザー IP アドレスがパブリックかプライベートかを示します。

> 注
>
> 値では大文字と小文字が区別されます。値を小文字で入力します。

クライアントポート

Client-Portディメンションに、次の値を入力します。

値	種類	説明
例: 45334	数	ユーザーデバイスのポート番号。

国

Countryディメンションに、次の値を入力します。

値	種類	説明
例: United States, India	文字列	ユーザーがログオンした国。

> 注
>
> 値にスペースが含まれている場合は、値を「」で囲みます。例: 国 =「Unites States」。

イベントタイプ

Event-Typeディメンションに、次の値を入力します。

値	種類	説明
認証、ICA ファイル、セッションログアウト	文字列	ユーザーイベントのタイプ。

ゲートウェイ **FQDN**

Gateway-FQDNディメンションに、次の値を入力します。

値	種類	説明
例：Gateway-test	文字列	Citrix Gateway のドメイン名。

ゲートウェイ **IP**

Gateway-IPディメンションに、次の値を入力します。

値	種類	説明
例：10.xxx.xxx.xx	文字列	Citrix Gateway の IP アドレス。

ゲートウェイポート

Gateway-Portディメンションに、次の値を入力します。

値	種類	説明
例：443	文字列	Citrix Gateway のポート番号。

ログアウトモード

Logout-Modeディメンションに、次の値を入力します。

値	種類	説明
"Internal error"、"Inactive time out"、"User initiated logout"、または"Administrator killed session"。	文字列	VPN セッションのタイムアウトまたは終了の理由。

> 注
>
> 値にスペースが含まれている場合は、値を「」で囲みます。例: ログアウトモード = "Internal error"。

NetScaler-IP

NetScaler-IPディメンションに、次の値を入力します。

値	種類	説明
例: 10.xxx.xx.xx	文字列	Citrix ADC アプライアンスの IP アドレス。

OS

OSディメンションに、次の値を入力します。

値	種類	説明
例: MAC_OS, WINDOWS	文字列	ユーザーデバイスのオペレーティングシステム。

レコードタイプ

Record Typeディメンションに、次の値を入力します。

値	種類	説明
VPN_AI	文字列	認証に関連するユーザーイベントを示します。

値	種類	説明
VPN_IF	文字列	ICA ファイルに関連するユーザーイベントを示します。
VPN_ST	文字列	セッションログアウトに関連するユーザーイベントを示します。

SSO 認証方式

SSO-Authentication-Methodディメンションに、次の値を入力します。

値	種類	説明
NSAUTH_BEARER、NSAUTH_FORM、NSAUTH_CITRIXAGBASIC、NSAUTH_NEGOTIATE、NSAUTH_NTLM、またはNSAUTH_BASIC。	文字列	シングルサインオン認証のさまざまな方法。

サーバー **IP**

Server-IPディメンションに、次の値を入力します。

値	種類	説明
例: 10.xx.xxx.xx	文字列	バックエンドサーバーの IP アドレス。

サーバーポート

Server-Portディメンションに、次の値を入力します。

値	種類	説明
例: 47054	数	バックエンドサーバーのポート番号。

セッションステート

Session-Stateディメンションに、次の値を入力します。

値	種類	説明
"Set Client State"、"Authorization State"、"SSO State"、"Application Bandwidth Update"	文字列	VPN セッションステート。

> 注
>
> 値にスペースが含まれている場合は、値を「」で囲みます。例: セッションステート = "Set Client State"。

ステータスコード

Status-Codeディメンションに、次の値を入力します。

値	種類	説明
"Successful login"、"Invalid credentials passed"、"Post auth failed and connection quarantined"、"Login not permitted"、"Maximum login failures reached"	文字列	VPN ステータスコード。

> 注
>
> 値にスペースが含まれている場合は、値を「」で囲みます。例: セッションコード = "Successful login"。

ユーザーエージェント

User-Agentディメンションに、次の値を入力します。

値	種類	説明
IPHONE、IPAD、または WINPHONE	文字列	VPN へのアクセスに使用されたエージェントまたはデバイス。

VPN-セッション **ID**

VPN-Session-IDディメンションに、次の値を入力します。

値	種類	説明
c2c290c61dfe4e07247bde1e3f42a12	文字列	サーバーによってユーザーの VPN セッションに割り当てられるセッション ID。

VPN セッションモード

VPN-Session-Modeディメンションに、次の値を入力します。

値	種類	説明
"Full Tunnel"、"ICA Proxy"、または Clientless	文字列	ユーザーの VPN セッションのさまざまなモード。

> 注
>
> 値にスペースが含まれている場合は、値を「」で囲みます。例: セッションコード = "Full Tunnel"。

ポリシーのセルフサービス検索

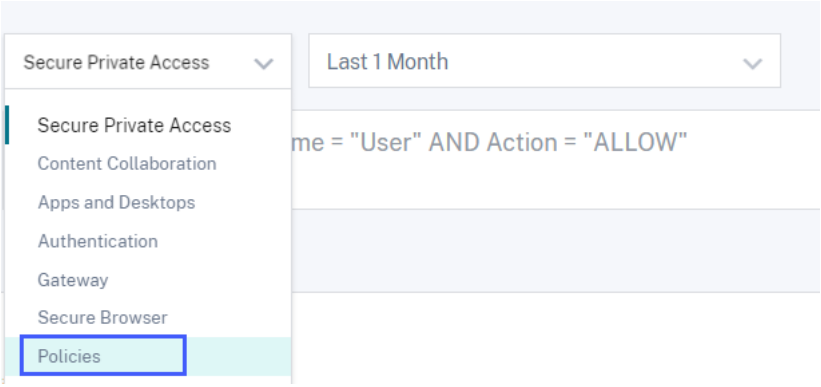
May 10, 2022

Citrix Analytics for Security を使用すると、ポリシーを作成し 、ユーザーアカウントの異常なイベントまたは疑わしいイベントにアクションを適用できます 。ユーザーイベントが定義済みのポリシーを満たすと、ユーザーアカウントにアクションが自動的に適用され、脅威を隔離し、今後異常なイベントが発生するのを防ぎます。セルフサービス検索を使用すると、定義したポリシーを満たすユーザーイベントを表示し、これらの異常イベントに適用されたアクションを表示できます。

検索機能の詳細については、「セルフサービス検索」を参照してください。

ポリシーデータセットを選択します

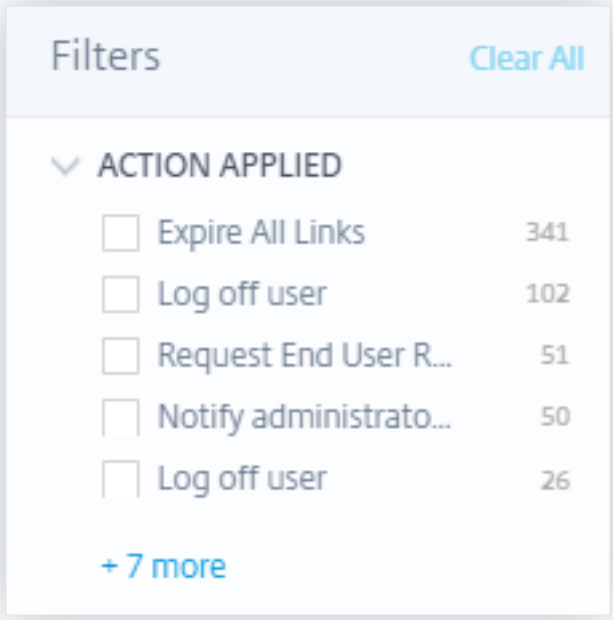
定義済みのポリシーに関連するイベントを表示するには、リストから [ポリシー（**Policies**）] を選択します。デフォルトでは、セルフサービスページには過去 1 日のイベントが表示されます。また、イベントを表示する期間を選択することもできます。



> 注
>
> [セキュリティ] > [ユーザー] > [ポリシーとアクション] ダッシュボードから、[ポリシーのセルフサービス検索] ページにアクセスすることもできます。ダッシュボードでポリシーを選択して、ポリシーに関連するユーザーイベントを表示します。詳細については、「ポリシーとアクション」ダッシュボードを参照してください。

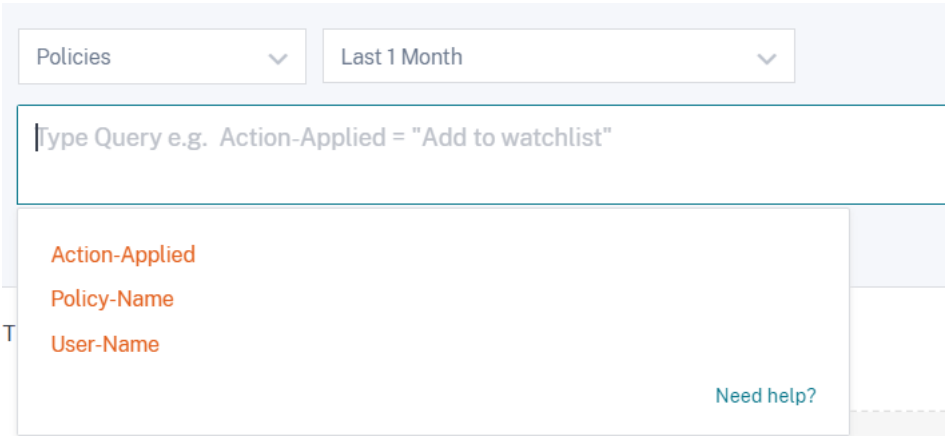
イベントをフィルタリングするファセットを選択します

ファセットリストには、ユーザーイベントに適用されたアクションが表示されます。ファセットリストから適用されたアクションを選択し、適用されたアクションに基づいてイベントを表示します。ポリシーの構成時に適用できるアクションの詳細については、「アクションとは」を参照してください。



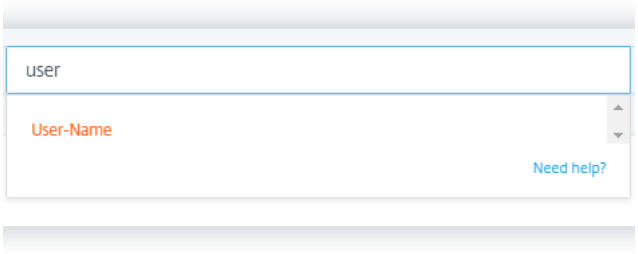
イベントをフィルタリングする検索クエリを指定する

検索ボックスにカーソルを置くと、ポリシーに関連するイベントのディメンションのリストが表示されます。ディメンションと演算子を使用してクエリを指定し、必要なイベントを検索します。

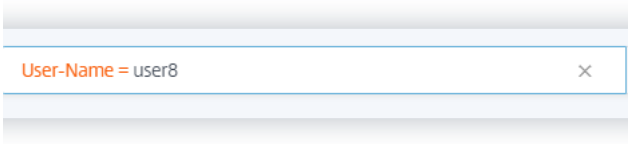


たとえば、ユーザー「user8」の異常なイベントを表示し、それらのイベントに適用されたアクションが「Disable user」であるとします。

1. 検索ボックスに「user」と入力して、関連するディメンションを取得します。

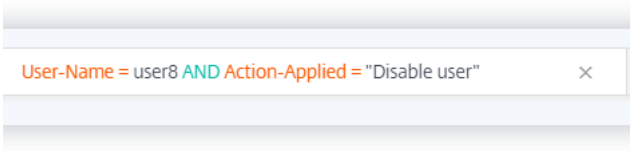


2. [ユーザー名] を選択し、等号演算子を使用して値「user8」を入力します。

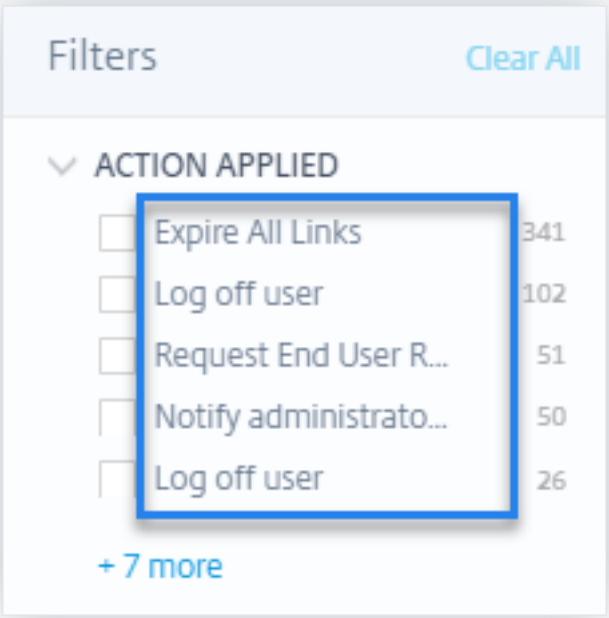


3. AND 演算子を選択し、アクション適用ディメンションを選択します。等号演算子を使用して、[アクション-適用] の文字列「Disable user」を入力します。

> 注:
>
> 文字列値に 2 つ以上の単語が含まれている場合は、演算子 “” <!--NeedCopy-->で囲む必要があります。たとえば、 “Disable user” <!--NeedCopy-->、「セッション録画の停止」などです。



Action-Applied の可能な文字列値を識別するには、ファセットリストを展開し、検索クエリの文字列としてフィルタ名を使用します。



4. 期間を選択し、［検索］をクリックして、**DATA** テーブルのイベントを表示します。

リモートブラウザ隔離のためのセルフサービス検索 **(Secure Browser)**

December 7, 2023

セルフサービス検索を使用すると、シトリックスの Remote Browser Isolation サービスを使用している Citrix Workspace ユーザーのブラウジングセッションを把握できます。Citrix Remote Browser Isolation は、企業ネットワークのセキュリティを損なうことなく、安全なインターネットブラウジング体験を提供するクラウドサービスです。ユーザーが Remote Browser Isolation を使用して Web アプリケーションにアクセスすると、セッション接続、セッション起動、公開アプリケーション、削除されたアプリケーションなどのイベントがユーザー接続ごとに生成されます。Citrix Analytics for Security はこれらのイベントを受信し、セルフサービスページに表示します。ユーザーとその閲覧セッションを追跡できます。

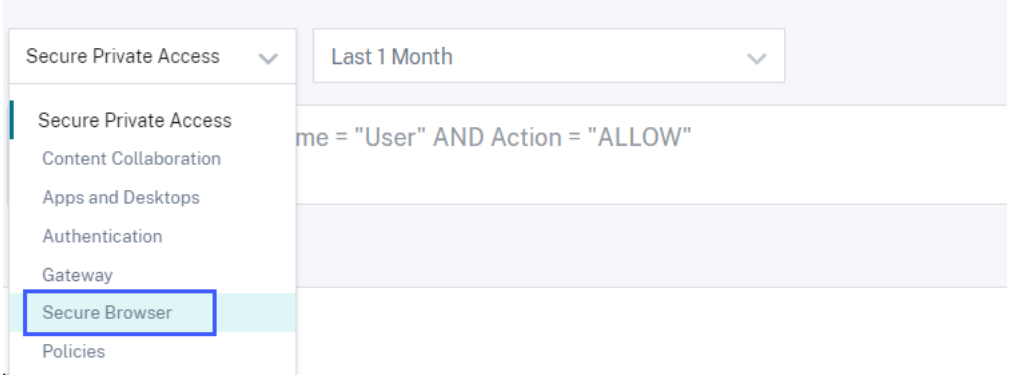
検索機能の詳細については、「セルフサービス検索」を参照してください。

前提条件

Remote Browser Isolation からイベントを受信するには、**Remote Browser Isolation** でホスト名追跡を有効にして、ユーザーセッションのホスト名をログに記録します。この情報は Citrix Analytics for Security に送信されます。詳細については、「公開されている Remote Browser Isolation の管理」を参照してください。

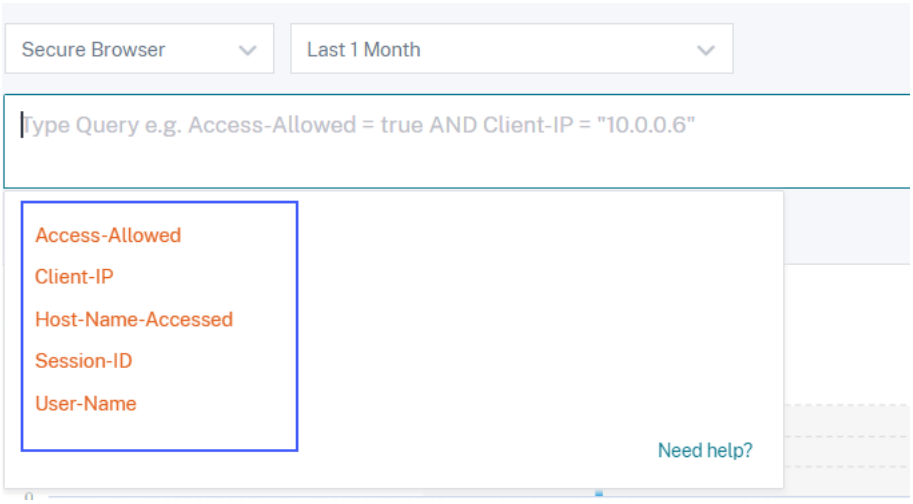
Remote Browser Isolation データソースを選択してください

Remote Browser Isolation イベントを表示するには、リストから「**Remote Browser Isolation** 」を選択します。デフォルトでは、セルフサービスページには過去 1 日のイベントが表示されます。また、イベントを表示する期間を選択することもできます。



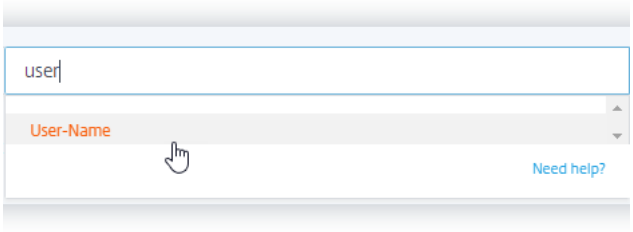
イベントをフィルタリングする検索クエリを指定する

検索ボックスにカーソルを置くと、Remote Browser Isolation イベントのディメンションのリストが表示されます。ディメンションと演算子を使用してクエリを指定し 、必要なイベントを検索します。

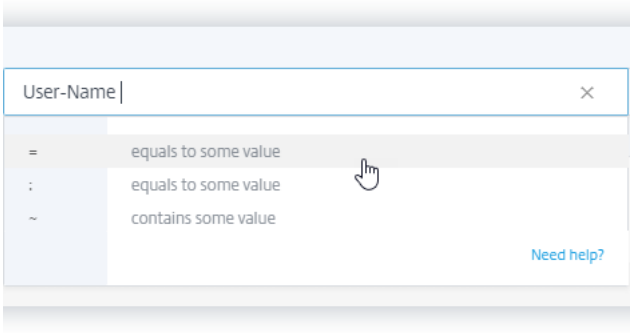


たとえば、google.com、amazon.com などのさまざまなホストサービスにアクセスする権限を持つユーザー「aa」の閲覧イベントの詳細を表示するとします。

1. 検索ボックスに「user」と入力して、関連するディメンションを表示します。



2. [ユーザー名] をクリックし、等号演算子を使用して値「aa」を入力します。



3. AND 演算子と **Allow-Access** ディメンションを選択します。等号演算子を使用して、**Allow-Access** に値「true」を割り当てます。「true」の値は、ユーザーがホストサービスにアクセスできることを示します。

4. 期間を選択し、［検索］をクリックして、**DATA** テーブルのイベントを表示します。

ユーザーイベントの詳細の表示

Remote Browser Isolation サービスから受信した次のデータを表示できます。

- **Time**：ユーザーイベントが発生した日時。
- ユーザー名-イベントを開始したユーザー。
- セッション **ID**-ユーザーセッションに割り当てられた一意の番号。
- クライアント **IP**：ユーザデバイスの IP アドレス。
- ホスト名-ユーザーがネットワーク経由でアクセスするホストサービス。
- アクセスを許可する-ユーザーは、ホストサービスへのアクセスを許可または拒否されます。

セキュアなプライベートアクセスのためのセルフサービス検索

April 12, 2024

セルフサービス検索を使用して、組織内の Citrix Cloud ユーザーのアクセスイベントに関するインサイトを取得します。アクセスイベントの例としては、URL カテゴリ、コンテンツカテゴリ、ブラウザ、デバイスなどがあります。Citrix Analytics for Security は、これらのイベントをセキュアプライベートアクセスサービスから受信し、セルフサービス検索に表示します。ユーザーとそのアクセスの詳細を追跡できます。

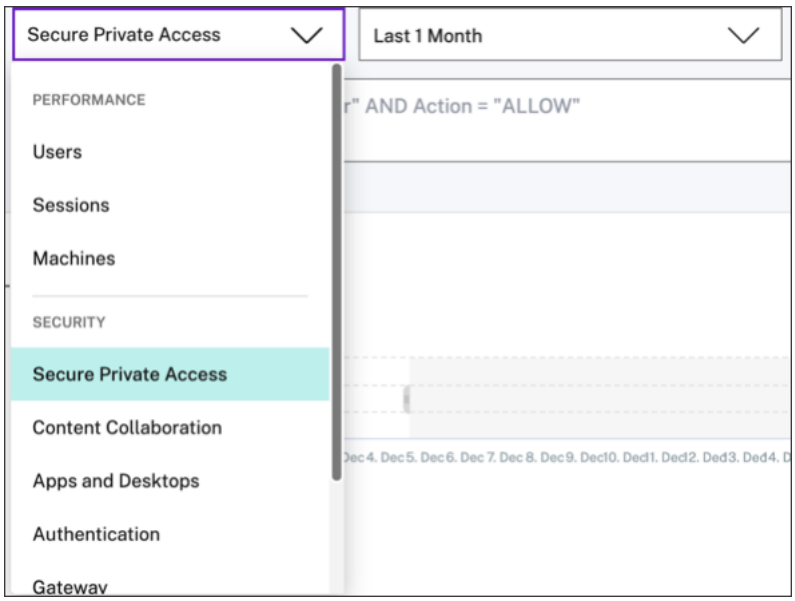
検索機能の詳細については、「セルフサービス検索」を参照してください。

> 注:
>
> セキュア・プライベート・アクセスによるカテゴリベースの Web フィルタリングの廃止により、Citrix Analytics for Security の以下の機能が影響を受けます。
>
> 1. カテゴリグループ、カテゴリ、URL のレピュテーションなどのデータフィールドは、Citrix Analytics for Security ダッシュボードでは使用できなくなりました。
> 2. 同じデータに依存する危険な Web サイトアクセスインジケーターも廃止され、お客様には表示されなくなりました。
> 3. データフィールド（カテゴリグループ、カテゴリ、URL の評価）とそれに関連するポリシーを使用する既存のカスタムリスク指標は、もうトリガーされません。

セキュア・プライベート・アクセスからの廃止の詳細については、「機能の非推奨」を参照してください。

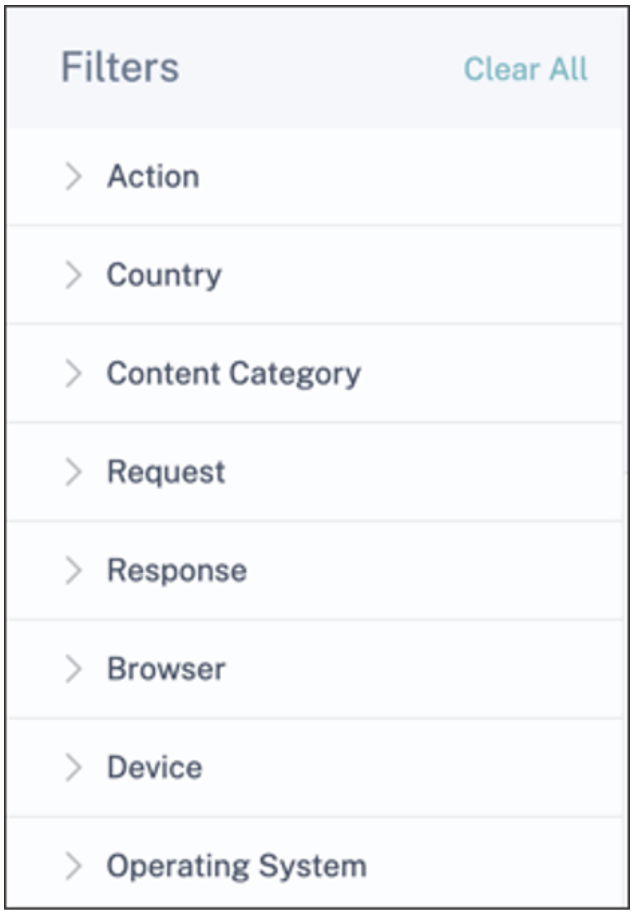
セキュア・プライベート・アクセス・データ・ソースを選択します

セキュア・プライベート・アクセスのイベントを表示するには、リストから「セキュア・プライベート・アクセス」を選択します。デフォルトでは、セルフサービスページには過去 1 日のイベントが表示されます。また、イベントを表示する期間を選択することもできます。



イベントをフィルタリングするファセットを選択します

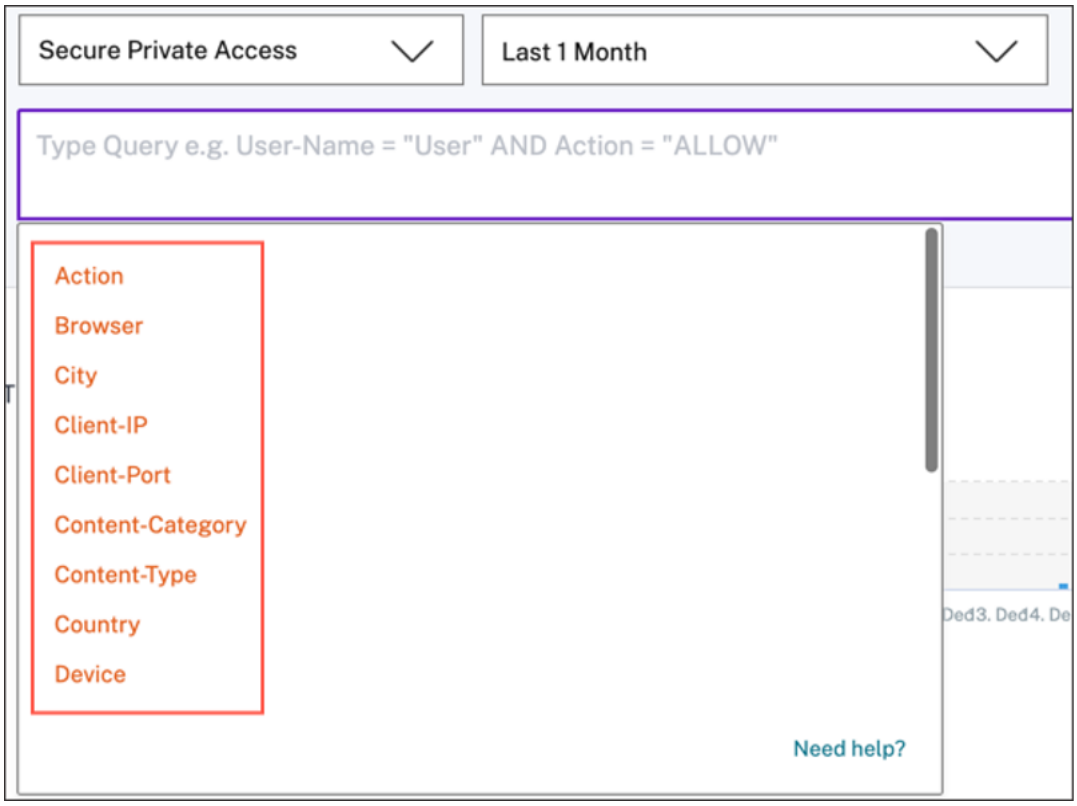
Secure Private Access イベントに関連付けられている次のファセットを使用します。



- アクション-許可、ブロック、リダイレクトなど、ユーザーのアプリケーションで実行されたアクションに基づいてイベントを検索します。
- 国-ユーザーのアクセス場所に基づいてイベントを検索します。
- コンテンツカテゴリ-アプリケーション、画像、テキストなど、アクセスされたコンテンツのカテゴリに基づいてイベントを検索します。
- 要求-GET、POST、PUT、DELETE などの HTTP メソッドに基づいてイベントを検索します。
- レスポンス-HTTP レスポンスに基づいてイベントを検索します。
- **Browser**-ユーザーが使用するブラウザに基づいてイベントを検索します。
- デバイス-Android フォン、iPhone、MacBook など、使用されているデバイスに基づいてイベントを検索します。
- オペレーティングシステム-デバイスにインストールされているオペレーティングシステムに基づいてイベントを検索します。

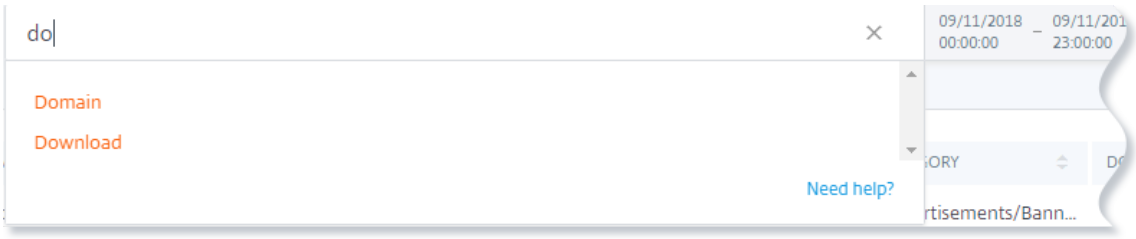
イベントをフィルタリングする検索クエリを指定する

検索ボックスにカーソルを置くと、Secure Private Access イベントのディメンションのリストが表示されます。ディメンションと演算子を使用してクエリを指定し 、必要なイベントを検索します。

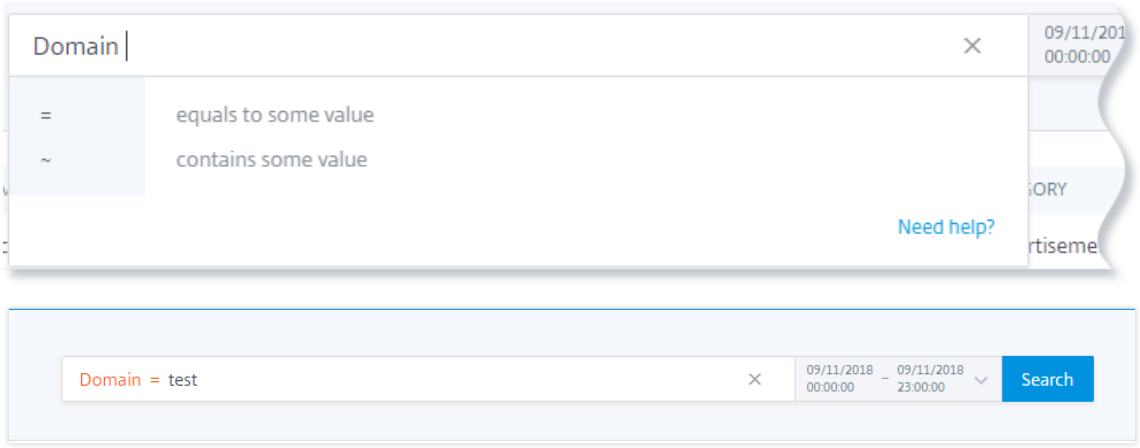


たとえば、データダウンロード量が 2,000 バイトを超えるテストドメインを表示するとします。検索クエリを次のように指定します。

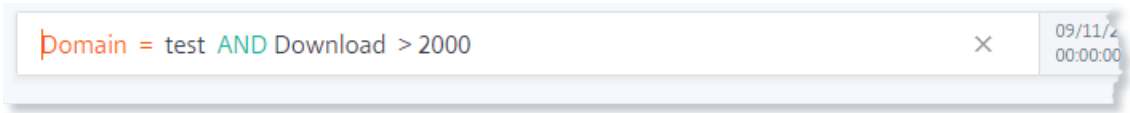
1. 検索ボックスに「do」と入力すると、関連する候補が表示されます。



2. [ドメイン] をクリックし、等号演算子を使用して「test」の値を指定します。



3. **AND** 演算子を使用して、**[**** ダウンロード] ディメンションを選択します。** ** 演算子を選択し、ダウンロードボリュームをバイト単位で入力します。



4. 期間を選択し、［検索］をクリックして、**DATA** テーブルのイベントを表示します。

アプリとデスクトップのセルフサービス検索

February 14, 2024

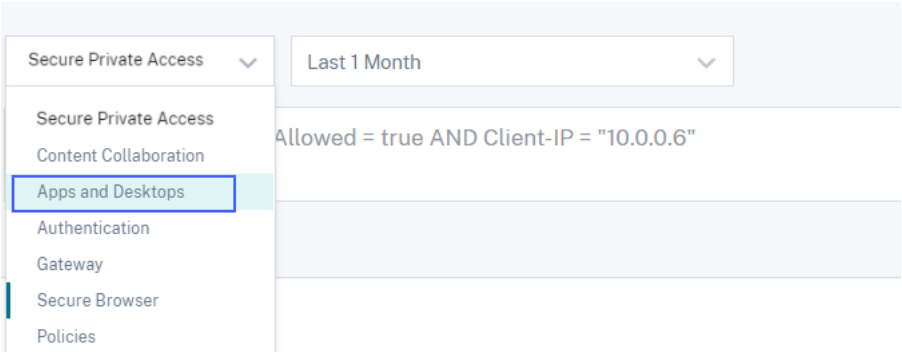
セルフサービス検索を使用すると、Citrix Virtual Apps and Desktops データソースと Citrix DaaS（旧 Citrix Virtual Apps and Desktops サービス）データソースから受信したユーザーイベントに関する洞察を得ることができます。ユーザーが仮想アプリケーションまたは仮想デスクトップを使用すると、ユーザーのアクティビティとアクションに対応するイベントが生成されます。ユーザーイベントの例としては、ファイルのダウンロード、アカウント

ログオン、アプリの起動などがあります。Citrix Analytics for Security は、これらのユーザーイベントを受信し、セルフサービスページに表示します。ユーザーとそのアクティビティを追跡できます。

検索機能の詳細については、「セルフサービス検索」を参照してください。

[アプリとデスクトップ] データソースを選択します

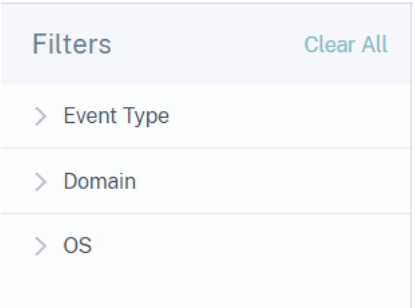
Citrix Virtual Apps and Desktops または Citrix DaaS からのイベントを表示するには、リストから［アプリとデスクトップ］を選択します。デフォルトでは、セルフサービスページには過去 1 日のイベントが表示されます。また、イベントを表示する期間を選択することもできます。



デフォルトでは、セルフサービスページには過去 1 か月のイベントが表示されます。このページには、いくつかのファセットと、必要なイベントをフィルタリングしてフォーカスするための検索ボックスも用意されています。

イベントをフィルタリングするファセットを選択します

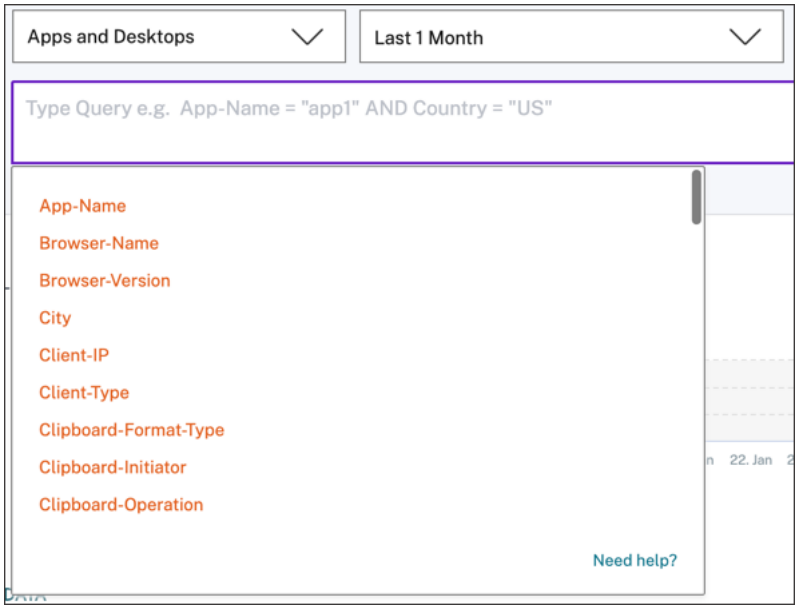
アプリとデスクトップのイベントに関連付けられている次のファセットを使用します。



- イベントタイプ-アカウントログオン、アプリ終了、セッション終了などのイベントタイプに基づいてイベントを検索します。
- ドメイン-citrate.net などのドメインに基づいてイベントを検索します。
- **OS**-ユーザーのデバイスで使用されている Chrome、iOS、Windows などのオペレーティングシステムに基づいてイベントを検索します。イベントをフィルタリングするオペレーティングシステムの名前とバージョンを選択します。オペレーティングシステムのバージョンの詳細については、「検索クエリでサポートされる値」を参照してください。

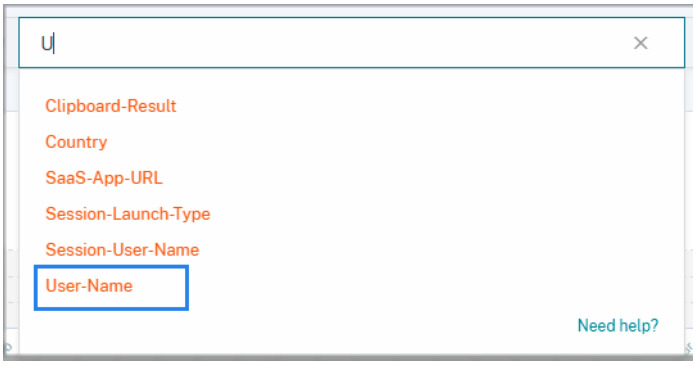
イベントをフィルタリングする検索クエリを指定する

検索ボックスにカーソルを置くと、アプリとデスクトップのイベントのディメンションの一覧が表示されます。ディメンションと演算子を使用してクエリを指定し 、必要なイベントを検索します。



たとえば、Windows オペレーティングシステムを使用しているユーザー「John Doe」のイベントを検索するとします。

1. 検索ボックスに「U」と入力すると、関連する候補が表示されます。



2. [ユーザー名] をクリックし、等号演算子を使用して値「John」を入力します。

3. AND 演算子と **OS** 名ディメンションを選択します。等号演算子を使用して、値「Windows 7」を割り当てます。

```
User-Name = "John" AND OS-Name = "Windows 7"
```

4. 期間を選択し、［検索］をクリックして、**DATA** テーブルに基づいてイベントを表示します。

イベントタイプとサポートされているフィールド

次のフィールドは、VDA.Print を除くすべてのイベントタイプで使用できます。

- 市区町村
- クライアント IP
- 国
- デバイス ID
- OS 名
- OS のバージョン
- OS 追加情報
- 時間
- ユーザー名
- Workspace App バージョン
- Workspace アプリのステータス

次の表は、Apps and Desktops データソースで使用できるイベントタイプと、各イベントタイプに固有のフィールドを示しています。

Value	説明	フィールド
`Account.Logon`	Citrix Workspace アプリからストアにログオンしたときにトリガーされます。注: アカウントログオンは HTML5 クライアントでは使用できません。	上記で説明したように、共通フィールドを確認してください。
`Session.Logon`	仮想セッションにログオンしたときにトリガーされます。	アプリ保護ポリシー、ドメイン、セッション起動タイプ、セッションサーバー名、セッションユーザー名

Value	説明	フィールド
Session.End	仮想セッションを終了するとトリガーされます。	ドメイン、セッション起動タイプ、セッションサーバー名、セッションユーザー名
App.Start	仮想アプリセッションを開始するとトリガーされます。注: このイベントタイプは、デスクトップセッション内でアプリケーションを起動した場合には適用されません。	アプリ名、ドメイン、セッション起動タイプ、セッションサーバー名、セッションユーザー名
App.End	仮想アプリセッションを終了するとトリガーされます。注: このイベントタイプは、デスクトップセッション内でアプリケーションを起動した場合には適用されません。	アプリ名、ドメイン、セッション起動タイプ、セッションサーバー名、セッションユーザー名
File.Download	ユーザーがリモート仮想セッションからクライアントデバイスにファイルをコピーするとトリガーされます。仮想セッション内で行われるファイル転送ではトリガーされません。注: このイベントタイプは、サーバーがファイルリダイレクションを許可し (詳細はファイルリダイレクト設定を参照)、クライアントワークスペースのファイルアクセス設定が [読み取りと書き込み] に設定されている場合にのみ送信されます。	ドメイン、ダウンロードデバイスタイプ、ダウンロードファイル名、ダウンロードファイルパス、ダウンロードファイルサイズ、セッションサーバー名、セッションユーザー名

Value	説明	フィールド
Printing	Citrix Workspace アプリを起動したセッションでクライアントプリンター経由でファイルを印刷するとトリガーされます。注: Citrix Workspace アプリには、印刷イベントに影響する 2 つの技術的な制限があります。まず、すべてのプラットフォームに共通する既知の問題のため、Printment Document Name のテレメトリは印刷イベントに含まれていません。2 つ目の理由は、もう 1 つの既知の技術的制限のため、印刷ファイルサイズのテレメトリが Windows の印刷イベントに含まれていないことです。これらのデータセット (ファイル名/ファイルサイズ) を収集するには、VDA.Print イベントを使用します。詳しくは、「Citrix DaaS 印刷テレメトリーの有効化」を参照してください。	ブラウザ名、ブラウザバージョン、ドメイン、プリンタ名、印刷ファイル形式、印刷ファイルサイズ、セッションサーバ名、セッションユーザー名
AppProtection.ScreenCapture	保護されたセッションでユーザーがスクリーンショットをキャプチャしようとしたときにトリガーされます。注: 詳細については、「アプリ保護」を参照してください。	保護対象アプリタイトル、画面キャプチャツール名、画面キャプチャツールパス
App.SaaS.Launch	Citrix Workspace アプリが Citrix Enterprise Browser で SaaS アプリケーションを起動したときにトリガーされます。	ブラウザ名、ブラウザバージョン、SaaS アプリケーション名、SaaS アプリケーション URL
App.SaaS.End	Citrix Workspace アプリが Citrix Enterprise Browser ーの SaaS アプリを閉じるとトリガーされます。	ブラウザ名、ブラウザバージョン、SaaS アプリケーション URL

Value	説明	フィールド
App.SaaS.Clipboard	Citrix Enterprise Browser でクリップボード操作が実行されるとトリガーされます。	ブラウザ名、ブラウザバージョン、クリップボード詳細フォーマットサイズ、クリップボード詳細フォーマットタイプ、クリップボード詳細イニシエータ、クリップボード詳細結果、クリップボード操作、SaaS アプリ URL
App.SaaS.File.Download	Citrix Enterprise Browser でファイルがダウンロードされるとトリガーされます。	ブラウザ名、ブラウザバージョン、ダウンロードデバイスタイプ、ダウンロードファイルパス、ダウンロードファイルサイズ
App.SaaS.File.Print	Citrix Enterprise Browser で印刷が開始されたときにトリガーされます。	ブラウザ名、ブラウザバージョン、印刷ファイル名、SaaS アプリケーション名、SaaS アプリケーション URL
App.SaaS.Url.Navigate	Citrix Enterprise Browser が URL をナビゲートしたときにトリガーされます。	ブラウザ名、ブラウザバージョン、SaaS アプリケーション名、SaaS アプリケーション URL
Citrix.EventMonitor.AppStart	Session Recording サーバーのアプリ監視リストに追加されたアプリケーションが仮想デスクトップセッション内で起動したときにトリガーされます 。	アプリ名
Citrix.EventMonitor.AppEnd	Session Recording サーバーのアプリ監視リストに追加されたアプリケーションが仮想デスクトップセッション内で停止したときにトリガーされます。	アプリ名
Citrix.EventMonitor.Clipboard	セッション記録内でクリップボードアクションが実行されたときにトリガーされます。	クリップボードデータ形式タイプ、プロセス名、ウィンドウタイトル
Citrix.EventMonitor.FileTransfer	ユーザーが仮想デスクトップセッションとユーザーのマシン間でファイルを転送するとトリガーされます。	ファイルサイズ、操作方向 (ホストからクライアント、クライアントからホスト)、ソースパス、デスティネーションパス

Value	説明	フィールド
Citrix.EventMonitor.RegistryChange	レジストリ操作が実行されるとトリガーされます。可能なレジストリ操作は、作成、削除、名前の変更、値の設定、および値の削除です。	レジストリ操作、レジストリ名、レジストリパス、プロセス ID、プロセスファイルパス
Citrix.EventMonitor.SessionEnd	セッションの記録が終了するとトリガーされます。	説明
Citrix.EventMonitor.SessionLaunch	セッションの記録が開始されたときにトリガーされます。	セッション記録タイプ
Citrix.EventMonitor.TopMost	一番上のウィンドウが変更されたときにトリガーされます。	アプリ名
Citrix.EventMonitor.IdleStart	セッションがアイドル状態になるとトリガーされます。	上記で説明したように、共通フィールドを確認してください。
Citrix.EventMonitor.IdleEnd	アイドルセッションが終了するとトリガーされます。	上記で説明したように、共通フィールドを確認してください。
Citrix.EventMonitor.WebBrowsing	ユーザーが仮想デスクトップセッション内でブラウザ上の Web ページを操作したときにトリガーされます。	アプリ名、URL
Citrix.EventMonitor.FileCreate	監視対象のファイルシステムパス内の仮想デスクトップセッションでファイルまたはフォルダーが作成されるとトリガーされます。	ファイル名、ファイルパス、ファイルサイズ
Citrix.EventMonitor.FileRename	監視対象のファイルシステムパス内の仮想デスクトップセッションでファイルまたはフォルダーの名前が変更されたときにトリガーされます。	上記で説明したように、共通フィールドを確認してください。
Citrix.EventMonitor.FileMove	監視対象のファイルシステムパスにあるファイルまたはフォルダーが仮想デスクトップセッションで、またはセッションホスト（VDA）とクライアントデバイス間で移動されたときにトリガーされます。	上記で説明したように、共通フィールドを確認してください。
Citrix.EventMonitor.FileDelete	監視対象のファイルシステムパス内のファイルまたはフォルダーが仮想デスクトップセッションで削除されたときにトリガーされます。	ファイル名、ファイルパス、ファイルサイズ

Value	説明	フィールド
Citrix.EventMonitor.CDMUSBDriveAttach	仮想アプリとデスクトップセッションが接続されているクライアントに、クライアントドライブマッピング (CDM) でマッピングされた USB 大容量記憶装置が挿入されたときにトリガーされます。	上記で説明したように、共通フィールドを確認してください。
Citrix.EventMonitor.GenericUSBDriveAttach	仮想アプリとデスクトップセッションが接続されているクライアントに、汎用リダイレクトされた USB 大容量記憶装置が挿入されたときにトリガーされます。	上記で説明したように、共通フィールドを確認してください。
Citrix.EventMonitor.RDPConnection	ユーザーが VDA マシン内でリモートデスクトップ接続を作成するとトリガーされます。	送信先 IP、プロセス ID
Citrix.EventMonitor.UserAccountModification	アカウントの作成、有効化、無効化、削除、名前の変更、パスワードの変更など、あらゆる種類のユーザーアカウント操作のトリガーです。	説明、ターゲットユーザー名
VDA.Print	アプリとデスクトップで印刷ジョブが開始されるとトリガーされます。注: このイベントは Citrix DaaS データソースにのみ適用されます。詳しくは、「Citrix DaaS 印刷テレメトリーの有効化」を参照してください。	ドキュメントユーザー名、マシン名、印刷ファイル名、印刷ファイルサイズ、プリンタ名、時間、印刷総部数、印刷ページ総数
VDA.Clipboard	アプリとデスクトップでクリップボード操作が実行されるとトリガーされます。注: このイベントは Citrix DaaS データソースにのみ適用されます。詳しくは、「Citrix DaaS のクリップボードテレメトリの有効化」を参照してください。	クリップボードフォーマットタイプ、クリップボード操作、クリップボード操作方向、クリップボード操作許可、クリップボードサイズ、マシン名

> 注
>
> すべてのセッション記録イベントでは、そのイベントを記録するポリシーを Session Recording サーバーで有効にする必要があります。詳しくは、「カスタムイベント検出ポリシーの作成」を参照してください。

検索クエリでサポートされる値

ディメンションに次の値を入力して、検索クエリを定義します。

ディメンション	Value	種類	説明
App-Name	アプリケーションセッションまたはデスクトップセッション。 アプリケーションセッションの例: ファーム名のないセッション: #Cloud - Excel 2016 およびファーム名のセッション: XA65PROD#Concur デスクトップセッションの例: ファーム名のないセッション: #SINXIAP0616 $S1-1 およびファーム名のセッション: XA65PROD# SINXIAP0616 $S1 -1	文字列	起動されたアプリケーションまたはデスクトップの名前。
App-Protection-Policies	例: AntiScreenCaptureEnabled	文字列	セッションのアクティブなアプリケーション保護ポリシー。
Browser-Name	例: Google Chrome、Citrix Enterprise Browser、Microsoft Edge、FIREFOX、SAFARI	文字列	ブラウザー名
Browser-Version	例:80.0.3987.122、101.0.9999.0	文字列	ブラウザーのバージョン
City	例: サンタクララ、ヒューストン、シカゴ	文字列	ユーザーの都市名。
Client-IP	IP アドレス。例:10.10.10	文字列	ユーザーエンドポイントの IP アドレス。

ディメンション	Value	種類	説明
Client-Type	Android、Windows、Macintosh、Chrome、HTML5、Unix/Linux、iOS、SessionRecording、Monitor	文字列	オペレーティングシステムまたは元のデータソースに基づいて、さまざまなタイプの Citrix Workspace アプリを示します。
Clipboard-Format-Type	例: テキスト、HTML、CF_UNICODETEXT	文字列	クリップボードにコピーされたデータ形式。
Clipboard-Initiator	例: キーボード、コンテキストメニュー、javascript	文字列	クリップボードの操作が開始された方法を示します。注:SaaS アプリケーションでのみサポートされます。
Clipboard-Operation	コピー、切り取り、貼り付け、配置	文字列	どのクリップボード操作が実行されるかを示します。注: 配置操作は、データがクリップボードに配置されていることを示します。これは、クリップボード内のデータがクライアントによって貼り付けられたか使用されたかを保証するものではありません。この操作は VDA.Clipboard イベントでのみサポートされています。
Clipboard-Operation-Direction	クライアントからホスト、ホストからクライアント	文字列	クリップボード操作の方向を示します。注: アプリとデスクトップ（Citrix DaaS）のクリップボード操作でのみサポートされます。

ディメンション	Value	種類	説明
Clipboard-Operation-Permitted	許可または拒否	文字列	アプリとデスクトップセッションでクリップボード操作が許可されているかどうかを示します。注: アプリとデスクトップ（Citrix DaaS）のクリップボード操作でのみサポートされます。
Clipboard-Result	成功またはブロック	文字列	クリップボード操作の結果を示します。注:SaaS アプリケーションでのみサポートされます。
Clipboard-Size	例:10、20	数	クリップボードに現在保存されているデータのサイズ(バイト単位)。
Country	例: アメリカ、インド	文字列	ユーザーの国名。
Description	**Citrix.EventMonitor.UserAccountModification** イベントの場合: ユーザーアカウントが作成され、ユーザーアカウントが有効になり、アカウントのパスワードのリセットが試みられました。	文字列	アカウントの作成、削除、名前の変更、パスワードのリセットが試みられたなど、ユーザーアカウントの変更ステータスについて説明します。
	Citrix.EventMonitor.SessionEnd イベントの場合: 不明、ログオフ、ロールオーバー、トリガー、未完了		セッションの記録が終了した理由を説明します。
Destination-IP	例:10.60.110.xxx	文字列	リモートデスクトップの IP アドレス。
Destination-Path	例:\ H$\ デスクトップ\ フォルダ\ example.txt	文字列	転送が完了した後のファイルの最終パス。

ディメンション	Value	種類	説明
Device-ID	例: cb781185-18ad-4f45-B75f	文字列	ライセンスに使用されるデバイス ID、クライアント名、またはオペレーティングシステムのハードウェア ID。
Domain	例:example.com	構造	リクエストを送信したサーバーのドメイン名。
Download-Device-Type	例:USB、ハードディスクドライブ、リモートドライブ、CDROM、またはブラウザのダウンロード。	文字列	ファイルがダウンロードまたは転送されるデバイスタイプ。
Download-File-Format	例: テキスト、PDF、XLSX、docx	文字列	ダウンロードされたファイルの形式。
Download-File-Name	例:example-file.txt	文字列	ダウンロードしたファイルの名前。
Download-File-Path	例:C:\Users\admin\Desktop	文字列	ダウンロードしたファイルのパス。
Download-File-Size	例:8.05	数	ダウンロードしたファイルのサイズ (キロバイト単位)。

ディメンション	Value	種類	説明
Event-Type	Account.Logon, Session.Logon, Session.End, App.Start, App.End, File.Download, Printing, AppProtection.ScreenCapture, App.SaaS.Launch, App.SaaS.End, App.SaaS.Clipboard, App.SaaS.File.Download, App.SaaS.File.Print, App.SaaS.Url.Navigate, Citrix.EventMonitor.AppStart, Citrix.EventMonitor.AppEnd, Citrix.EventMonitor.TopMost, Citrix.EventMonitor.WebBrowsing, Citrix.EventMonitor.FileCreate, Citrix.EventMonitor.FileRename, Citrix.EventMonitor.FileMove, Citrix.EventMonitor.FileDelete, Citrix.EventMonitor.CDMUSBDriveAttach, Citrix.EventMonitor.GenericUSBDriveAttach, Citrix.EventMonitor.RDPConnection, Citrix.EventMonitor.UserAccountModification, VDA.Print, VDA.Clipboard, Citrix.EventMonitor.RegistryChange, Citrix.EventMonitor.SessionLaunch, Citrix.EventMonitor.SessionEnd,	文字列	詳細については、「イベントタイプとサポートされるフィールド」を参照してください。

ディメンション	Value	種類	説明
Jail-Broken	はいまたはいいえ	文字列	デバイスが Root 化されているかどうかを示します。注: このディメンションがない場合、デバイスはルート化されません。このキーは、iOS および Android デバイス用の Citrix Workspace アプリに適用されます。
Operation-Direction	ホストからクライアント/クライアントからホスト	文字列	ファイル転送の方向を示します。
OS-Extra-Info	例:20G80、サービスパック 1、19043	文字列	ビルド番号、サービスパック、パッチなど、オペレーティングシステムの追加情報を示します。
OS-Name	例: macOS 11、Windows 7、Android 8.1、Windows 10 Enterprise	文字列	オペレーティングシステムの名前を示します。
OS-Version	例:11.5.1、14.7.1、2009	文字列	オペレーティングシステムのバージョンを示します
Print-File-Format	例: PDF、PS、DOCX	文字列	印刷ファイルの形式。
Print-File-Name	例:example-file.pdf	文字列	印刷されるファイルの名前。
Print-File-Size	例:10、20	文字列	印刷ファイルのサイズ (バイト単位)。
Printer-Name	例: テストプリンタ-1	文字列	使用するプリンタの名前。

ディメンション	Value	種類	説明
Process-ID	例:11248	文字列	** 新しいプロセスの作成とリモートデスクトップ接続の確立という 2 つのアクションを実行する特定のプロセスを識別するために使用されるプロセス **ID を指します。プロセス ID は現在、Citrix.EventMonitor.RDPConnection イベントにのみ関連付けられています。
Protected-App-Titles	例: 管理デスクトップ-Citrix Workspace	文字列	保護されたセッションで実行されているアプリケーションの名前。
Registry-Name	変更されたレジストリの名前	文字列	変更されたレジストリの名前。
Registry-Operation	名前の変更、作成、削除、値の設定、値の削除	文字列	どのレジストリ操作が実行されたかを示します。
Registry-Path	変更されたレジストリのパス	文字列	変更されたレジストリのパス。
SaaS-App-Name	例: Workday	文字列	SaaS アプリケーションの名前。
SaaS-App-URL	例: https://xyz.com|String	文字列	SaaS アプリケーションの URL またはゲートウェイ/プロキシ URL。注: ゲートウェイ/プロキシ URL は、SaaS アプリケーションが最初に起動されたときに App.SaaS.Launch イベントに表示されます。
Screen-Capture-Tool-Name	例:ScreenShotTool.exe	文字列	画面キャプチャツールの名前。
Screen-Capture-Tool-Path	例:c:\Program ファイル (x86)\ スクリーンコンテンツクライアント	文字列	画面キャプチャツールのパス。

ディメンション	Value	種類	説明
Session-Launch-Type	アプリケーションまたはデスクトップ	文字列	起動したセッションがアプリケーションタイプかデスクトップタイプかを示します。
Session-Recording-Type	従来の録音/イベントのみの録画	文字列	起動されたセッションレコーディングのタイプを示します。
Session-Server-Name	例: ホスト型デスクトップ、クラウド VDA-1	文字列	サーバーから受信した接続先のアプリケーションまたはデスクトップの名前。
Session-User-Name	例: デモユーザー、テストユーザー	文字列	サーバーから受信したユーザー名。
Source-Path	例:C:\Users\admin\Desktop\example.txt	文字列	転送前のファイルの初期パス。
Target-User-Name	例: ユーザー 01	文字列	現在、ターゲットユーザー名は Citrix.EventMonitor.UserAccountModif イベントにのみ使用されます。このイベントでは、変更されたのはユーザーアカウントです。
Total-Copies-Printed	例:1、2	数	ユーザーが印刷した部数の合計。
Total-Pages-Printed	例:1,2	数	ユーザーが印刷した文書ページの総数。
User-Name	ユーザー名またはドメイン\ ユーザー名	文字列	ユーザー名またはドメイン\ ユーザー名。StoreFront のログインに使用されます。StoreFront ログオンが HTML5 または Chrome 用の Citrix Workspace アプリを経由しない場合、この値はサーバーから受信した値と同じです。
VDA-Name	例: TSVDA-19-01.xd.local	文字列	VDA マシンの名前を示します。

ディメンション	Value	種類	説明
Window-Title	例: 管理者-01 コマンドプロンプト	文字列	クリップボード操作が実行されたウィンドウのタイトルを示します。
Workspace-App-Version	例：20.8.0.3（2008 年）	文字列	Citrix Workspace アプリまたは Citrix Receiver バージョンがユーザーのデバイスにインストールされ、リモート仮想アプリおよびデスクトップセッションの起動に使用されます。
Workspace-App-Status	サポート対象またはサポート対象外	文字列	ユーザーのデバイスにインストールされている Citrix Workspace アプリまたは Citrix Receiver のバージョンが、Citrix Analytics for Security でサポートされているかどうかを示します。Workspace アプリがサポートされていない場合は、[サポートされていません] にカーソルを合わせます。ポップアップウィンドウが開き、サポートされているバージョンのリストを表示するリンクが表示されます。Workspace アプリのバージョンがサポート対象外の状態に近づくと、セルフサービス検索ページにバナーが表示され、アップグレードを開始できるサポート対象バージョンが表示されます。

オペレーティングシステムの名前付け形式

Citrix Analytics は、ユーザーデバイスのオペレーティングシステム（OS）の詳細を受信し、それらを OS 名、OS バージョン、および OS 追加情報に変換します。

- **[OS** 名] は、オペレーティングシステムの名前を示します。
- **OS Version** は、オペレーティングシステムのリリース ID またはリリースバージョンを示します。
- **OS Extra Info** は、ビルド番号、サービスパック、パッチなど、オペレーティングシステムの追加情報を示します。

次の表に、オペレーティングシステムのバージョン番号付けフォーマットの例をいくつか示します。

OS 名	OS のバージョン	OS 追加情報
macOS 11	11.5.1	20G80
iOS 14	14.7.1	利用できない
Windows 10 Enterprise	2009	19043
Windows 7	6.1	Service Pack 1
Android 8.1	8.1.0	利用できない

> メモ
>
> - Mac バージョン 11.x 以降の OS の詳細を取得するには、Mac 2108 以降の Citrix Workspace アプリをお勧めします。
> - Windows 10 の OS の詳細は現在利用できません。

セキュリティとパフォーマンスに関する **Citrix Analytics** トラブルシューティング

December 7, 2023

このセクションでは、Citrix Analytics for Security を使用するときに発生する可能性のある次の問題を解決する方法について説明します。

- 匿名ユーザーを正当なユーザーとして検証します。
- データソースからのイベント転送の問題をトラブルシューティングします。
- Virtual Apps and Desktops イベント、SaaS イベントをトリガーし、Citrix Analytics for Security へのイベント送信を検証します。

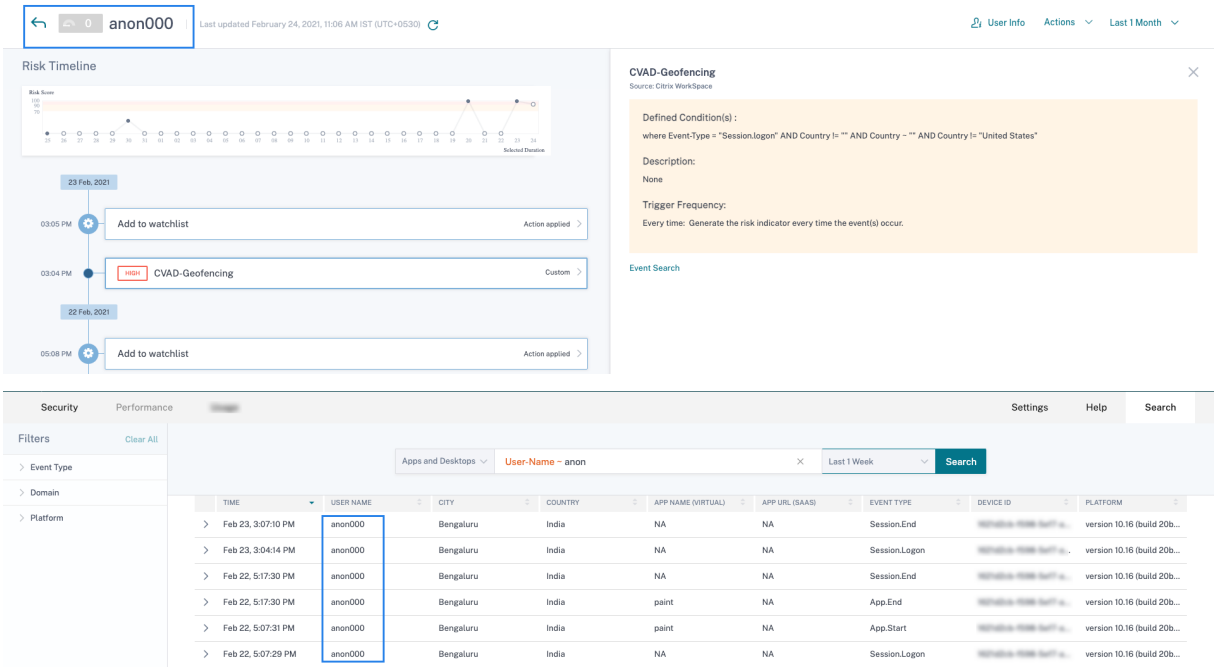
- Session Recording サーバーが接続に失敗する。
- Splunk 用 Citrix Analytics アドオンの設定に関する問題

匿名ユーザーを正当なユーザーとして検証する

August 22, 2022

管理者として、Citrix Analytics for Citrix Virtual Apps and Desktops Security で一部のユーザーおよび Citrix DaaS （以前の Citrix Virtual Apps and Desktops サービス）ユーザーが匿名として表示されることがあります。これらのユーザーは、検出されたユーザーとして識別されます。ただし、ユーザー名 anonXYZ （「XYZ」は 3 桁の数字を表します）は、次のページに表示されます。

- ユーザー
- ユーザーのタイムライン
- リスクの高いユーザー
- アプリとデスクトップデータソースのセルフサービス検索



そのようなユーザーが表示されたら、次のことを知りたいかもしれません。

- これらのユーザーは誰ですか?
- これらのユーザーは本質的に合法的で悪意のあるのですか?
- それらを検証するには?

- これらのユーザーに対して適用する必要があるアクションは何ですか?

Citrix IT 環境では、次のシナリオで匿名ユーザーが表示されます。

- 公開済みのセキュアブラウザアプリをユーザーが使用している場合
- ユーザーが認証されていないストアを使用している場合

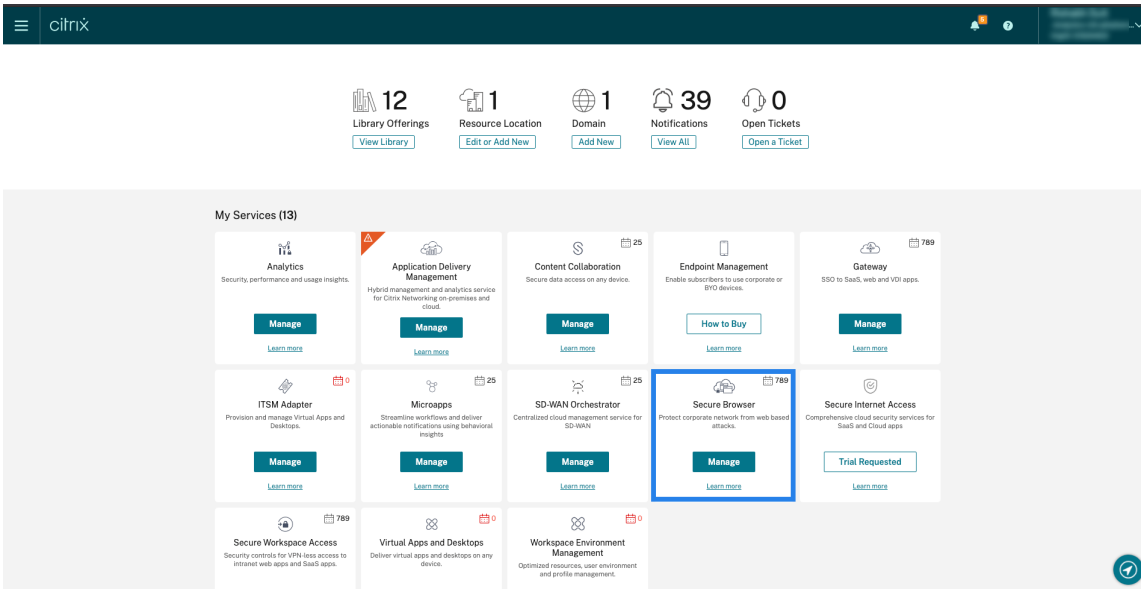
公開済みのセキュアブラウザアプリを使用しているユーザー

セキュアブラウザアプリは、Citrix Secure Browser サービスを使用して公開される Web アプリです。これらのアプリは、Web ブラウジングイベントを隔離し、ブラウザベースの攻撃から企業ネットワークを保護します。詳細については、「セキュリティで保護されたブラウザサービス」を参照してください。

セキュアブラウザアプリは、の匿名セッション機能を使用します Citrix DaaS。

Citrix Cloud アカウントでセキュアブラウザが構成されているかどうかを確認するには:

1. Citrix Cloud にサインインします。
2. [セキュアブラウザ] カードで、[管理] をクリックします。



3. [管理] ページで、公開されているセキュアなブラウザアプリを確認します。

ユーザーが Web ブラウザを使用して Citrix Receiver for Web サイトを介して StoreFront ストアにアクセスし、公開されているセキュリティで保護されたブラウザアプリを使用している場合、ユーザーの ID は非表示になります。したがって、Citrix Analytics はユーザーを匿名として表示します。

ユーザーがデバイスにインストールされている Citrix Receiver アプリまたは Citrix Workspace アプリを介して StoreFront ストアにアクセスし、公開されているセキュリティで保護されたブラウザアプリを使用する場合、Citrix Analytics StoreFront で指定されたユーザー名としてユーザーを表示します。

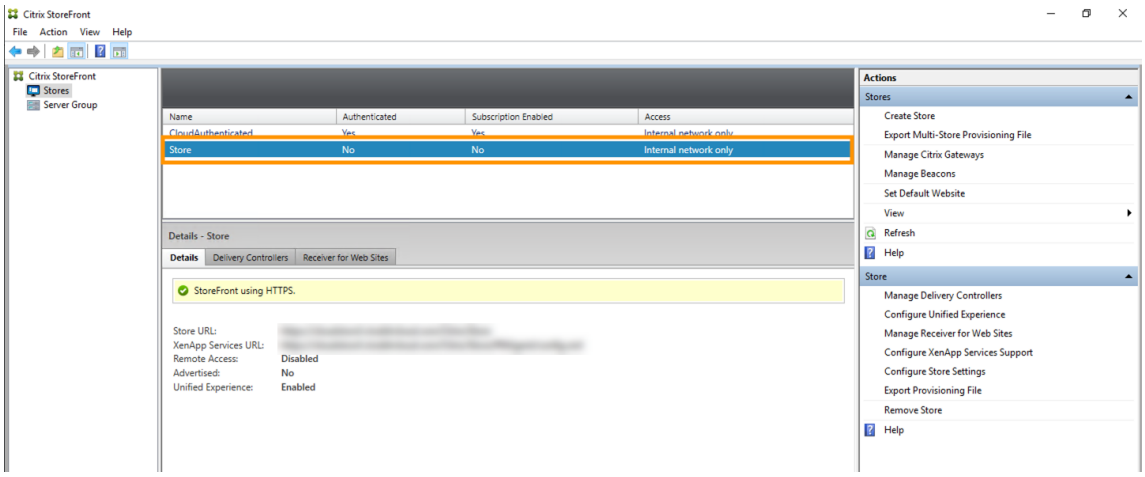
したがって、そのユーザーを組織の正当なユーザーと見なすことができます。危険な動作がユーザーに関連付けられていない場合は、アクションを適用する必要はありません。

認証されていないストアを使用しているユーザー

認証されていないストアは Citrix StoreFront の機能で、お客様が管理するストアに適用されます。この機能は、認証されていない (匿名) ユーザーのアクセスをサポートします。

組織に認証されていないストアがあるかどうかを確認するには、次の手順を実行します。

1. Citrix Studio を起動します。
2. [ストア] をクリックします。
3. ストアの場合は、[認証済み] 列で認証ステータスを確認します。



ストアが認証されておらず、ユーザーがその非認証ストアにアクセスしている場合、ユーザー ID は匿名のままになります。したがって、Citrix Analytics はユーザーを匿名として表示します。このユーザーを組織の正当なユーザーと見なすことができます。危険な動作がユーザーに関連付けられていない場合は、アクションを適用する必要はありません。

データソースからのイベント転送に関する問題のトラブルシューティング

April 12, 2024

このセクションでは、Citrix Analytics for Security でのデータ転送に関する問題のトラブルシューティングに役立ちます。データソースがユーザーイベントを正確に送信できない場合、ユーザーやリスク指標の検出不能などの問題が発生する可能性があります。

チェックリスト

シーケンス	チェック
1	Security Analytics を使用するための正しい資格を持っていますか?
2	そのデータソースはホームリージョンでサポートされていますか?
3	ご使用の環境は、すべてのシステム要件を満たしていますか。
4	Analytics ですべてのデータソースが検出され、データ処理が有効になっていますか?
5	データソースでのユーザーアクティビティは、Analytics にイベントを正確に送信していますか?
6	仮想アプリケーションとデスクトップのイベントは Analytics に送信されますか。
7	ユーザーイベントは Analytics のセルフサービス検索ページに表示されていますか?
8	ユーザーは Analytics によって検出されていますか?

チェック **1-**セキュリティアナリティクスを使用するための正しいエンタイトルメントがありますか**?**

Citrix Analytics for Security は、サブスクリプションベースのサービスです。詳しくは、「はじめに」を参照してください。

チェック **2-**データソースはご使用のホームリージョンでサポートされていますか

Citrix Analytics for Security は、次のホームリージョンでサポートされています。

- 米国（米国）

- 欧州連合 (EU)
- アジア太平洋南部 (APS)

組織の場所に応じて、いずれかのホームリージョンの Citrix Cloud にオンボーディングできます。

ただし、一部のホームリージョンではサポートされていないデータソースもあります。[データソース]((/en-us/security-analytics/data-sources.html)）は、Citrix Analytics for Security がユーザーイベントを受信する製品のことです。

データソースがサポートされていないホームリージョンで組織が Citrix Cloud にオンボーディングされている場合、データソースからユーザーイベントは取得されません。

次の表を使用して、データソースと、そのデータソースがサポートされているリージョンを表示します。

データソース	米国リージョンでのサポート	EU リージョンでのサポート	APS リージョンでサポートされています
Citrix Endpoint Management	はい	はい	はい
NetScaler Gateway (オンプレミス)	はい	はい	はい
Citrix ID プロバイダー	はい	はい	はい
Citrix Secure Browser	はい	はい	はい
Citrix Secure Private Access	はい	番号	番号
Citrix DaaS（旧称: Citrix Virtual Apps and Desktops サービス）	はい	はい	はい
Citrix Virtual Apps and Desktops オンプレミス	はい	はい	はい
Microsoft Active Directory	はい	はい	はい
Microsoft Graph Security	はい	はい	はい

チェック **3-**ご使用の環境がすべてのシステム要件を満たしていますか

Citrix Analytics は、データソースからユーザーイベントを受信するまでに数分かかる場合があります。データソースサイトカードにユーザーイベントが表示されない場合は、環境が前提条件とシステム要件を満たしていることを確認してください。

前提条件

1. Citrix Cloud サブスクリプションはすべてアクティブである必要があります。[Citrix Cloud] ページで、すべての Citrix Cloud サービスがアクティブであることを確認します。
2. オンプレミスで使用している場合は Citrix Virtual Apps and Desktops、Citrix Workspace にサイトを追加し、サイトアグリゲーションを構成する必要があります。Citrix Analytics は、Citrix Workspace に追加されたサイトを自動的に検出します。詳細については、「ワークスペースでのオンプレミスの仮想アプリケーションおよびデスクトップの集約」を参照してください。
3. サイトで StoreFront 展開環境を使用している場合は、Citrix Workspace アプリがユーザーイベントを Citrix Analytics に送信できるように StoreFront サーバーを構成します。StoreFront のバージョンが 1906 以降であることを確認します。StoreFront サーバーを構成しない場合、Citrix Analytics Citrix Virtual Apps and Desktops はオンプレミスからのユーザーイベントの受信に失敗します。StoreFront の展開環境を構成するには、StoreFront のドキュメントの「Citrix Analytics サービス 」
4. Citrix Virtual Apps and DesktopsCitrix DaaS ユーザーとユーザーは、指定したバージョンの Citrix Workspace アプリまたは Citrix Receiver をエンドポイントで使用する必要があります。そうしないと、Analytics はユーザーエンドポイントからユーザーイベントを受信しません。Citrix Workspace アプリまたは Citrix Receiver のサポートされるバージョンのリストは、Citrix Virtual Apps and Desktops および Citrix DaaS データソースで確認できます。
5. 公開されたセキュアブラウザセッションからユーザーのイベントを受信するには、セキュアブラウザでホスト名トラッキング設定を有効にします。デフォルトでは、この設定は無効になっています。詳細については、「公開されたセキュリティで保護されたブラウザーを管理する」を参照してください。
6. 次の記事で説明されているように、データソースをオンボーディングします。
    - Citrix Endpoint Management データソース
    - NetScaler Gateway データソース
    - Citrix Secure Private Access データソース
    - Citrix Virtual Apps and Desktops および Citrix DaaS データソース
    - Microsoft Active Directory 統合
    - Microsoft Graph セキュリティ統合

チェック **4-Analytics** ですべてのデータソースが検出され、データ処理が有効になっていますか

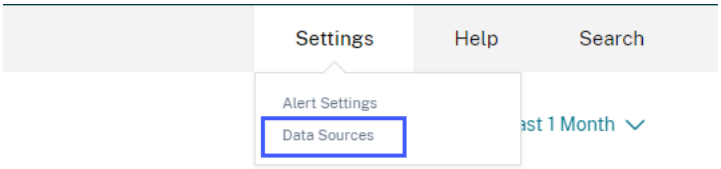
すべてのデータソースが検出され、そのデータソースのデータ処理が有効になっていることを確認します。データソースのデータ処理を有効にしないと、そのデータソースを使用しているユーザーは検出されません。このような状況では、潜在的なセキュリティリスクが生じる可能性があります。

データ処理を有効にすると、Citrix Analytics でユーザーイベントが確実に処理されます。Citrix Analytics にイベントが送信されるのは、ユーザーがデータソースをアクティブに使用している場合のみです。

> 注
>
> Citrix Analytics は、お客様の環境から積極的にデータを取得しません。

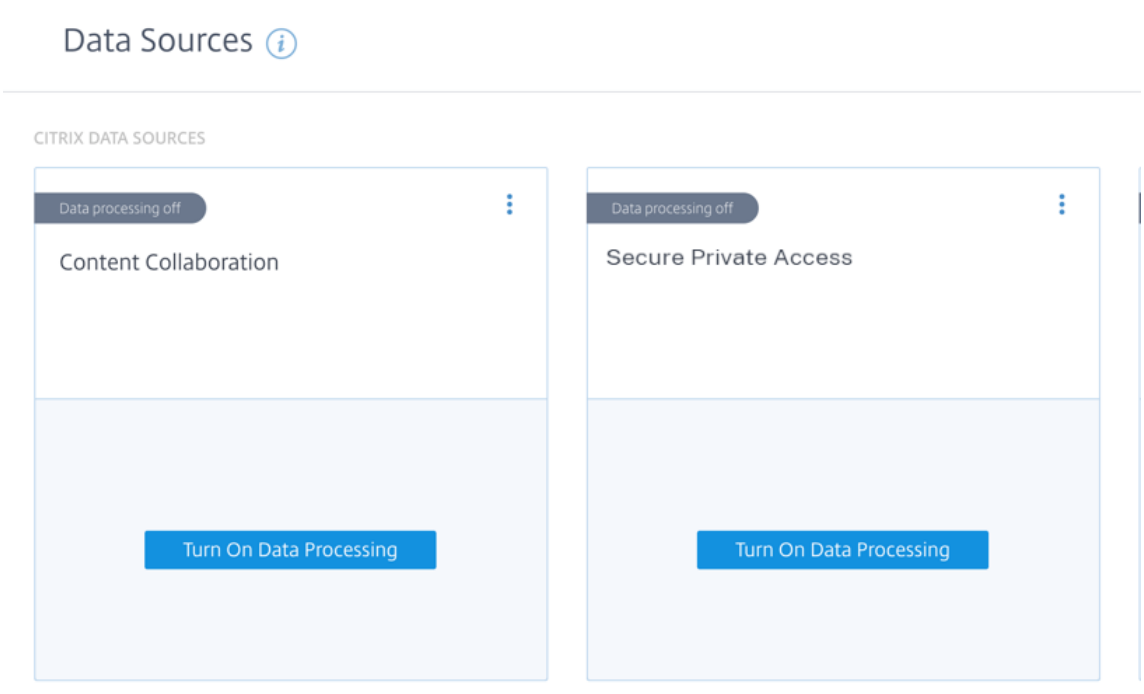
データソースを検出して分析を有効にするには、次の操作を行います。

1. [設定] > [データソース] > [セキュリティ] をクリックして、検出されたデータソースを表示します。Citrix Analytics は、ユーザーが Citrix Cloud アカウントにサブスクライブしているデータソースを自動的に検出します。

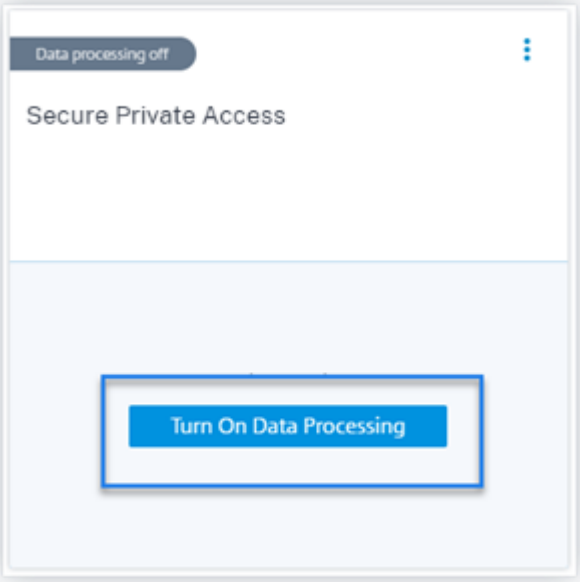


2. [データソース] ページに、検出されたデータソースがサイトカードとして表示されます。デフォルトでは、データ処理はオフになっています。

> 重要
>
> Citrix Analytics は、お客様の同意を得た後、お客様のデータを処理します。



3. Citrix Analytics でイベントを処理するサイトカードの［データ処理をオンにする］をクリックします。たとえば、Citrix Secure Private Access サイトカードの [データ処理を有効にする] をクリックします。



4. データ処理を有効にすると、Citrix Analytics はデータソースのイベントを処理します。サイトカードのステータスが [データ処理] に変わります。選択した期間に基づいて、ユーザー数と受信したイベントを表示できます。

5. 検出されたすべてのデータソースについて、「はじめに 」に記載されている手順に従って分析を有効にします。

チェック **5-**データソースでのユーザーアクティビティは、**Analytics** にイベントを正確に送信していますか

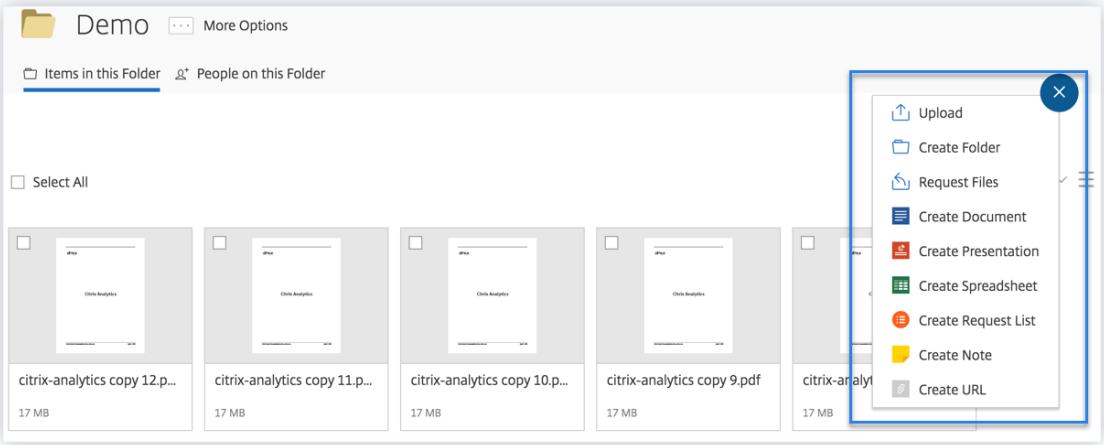
Citrix Analytics は、ユーザーがデータソースをアクティブに使用しているときに、データソースからユーザーイベントを受信します。ユーザーは、イベントを生成するために、データソースに対して何らかのアクティビティを実行する必要があります。たとえば、Apps and Desktops データソースからイベントを受信するには、Apps and Desktops ユーザーは一部のファイルを共有、アップロード、またはダウンロードする必要があります。

> 注
>
> Citrix Analytics は、お客様の環境から積極的にデータを取得しません。

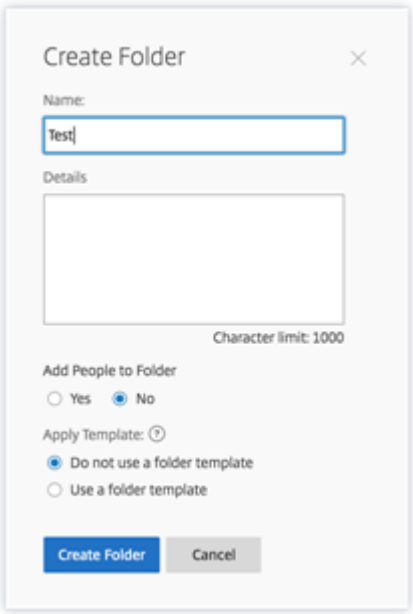
Citrix Analytics でデータソースのユーザーイベントが表示されない場合、その時点でユーザーがアクティブではない可能性が高くなります。

Citrix Analytics がユーザーイベントを正確に受信したことを確認するには、次のアクティビティを実行します。このアクティビティでは、Citrix アプリとデスクトップのデータソースを使用します。サブスクリプションに基づいて、他の Citrix 製品（データソース）を使用して同様のアクティビティを実行できます。

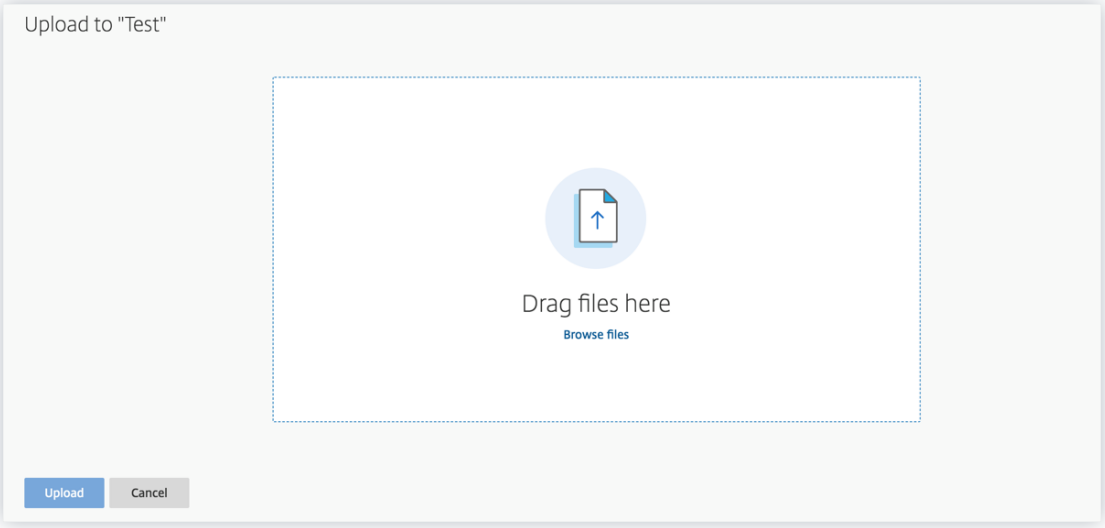
1. Citrix アプリとデスクトップサービスにログオンします。
2. フォルダーの作成、ファイルのダウンロード、ファイルのアップロード、ファイルの削除など、通常のユーザーアクティビティを実行します。



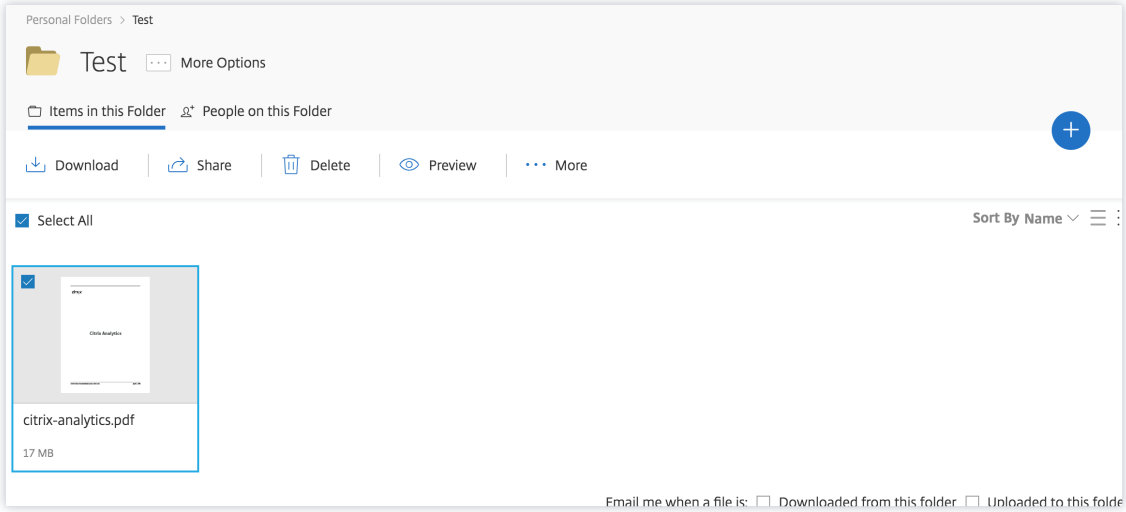
3. たとえば、Test フォルダーを作成します。



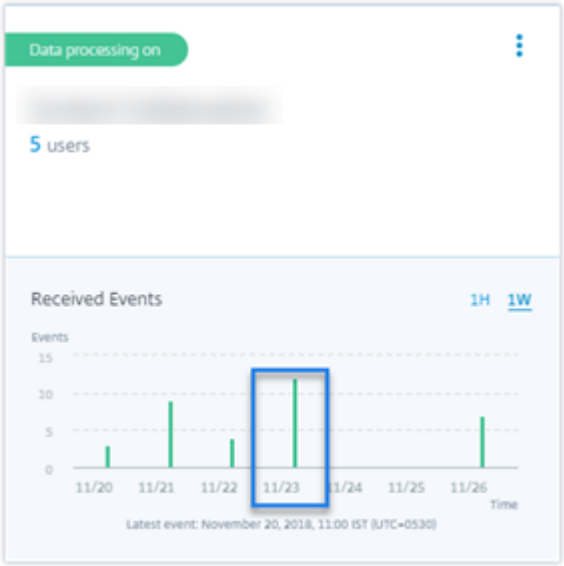
4. ローカルファイルをいくつかアップロードします。



5. フォルダ内のファイルをいくつか削除します。



6. Citrix Analytics に戻り、［データソース］ページの［アプリとデスクトップ］サイドカードを確認します。Citrix Analytics は、アプリとデスクトップのデータソースからユーザーイベントを受信し、サイトカードに表示します。



チェック **6:** 仮想アプリケーションとデスクトップのイベントは **Analytics** に送信されますか**?**

一部のバージョンの Citrix Workspace アプリまたは Citrix Receiver クライアントは、ユーザーイベントを Citrix Analytics に送信できません。ユーザーがこれらのクライアントを介して仮想アプリケーションやデスクトップを起動すると、サポートされているイベントが実行されるまで、Citrix Analytics はユーザーを検出できません。

たとえば、Linux 2006 以降の Citrix Workspace アプリは、**SaaS アプリケーションの起動イベントと SaaS アプリケーション終了イベントを Citrix** Analytics に送信しません。Linux 向け Citrix Workspace アプリを使用して SaaS アプリを起動したユーザーは、Citrix Analytics では検出されません。

サポートされるイベント

各クライアントバージョンでサポートされるユーザーイベントを確認するには、次の表を参照してください。

- はい-イベントはクライアントから Citrix Analytics に送信されます。
- いいえ-イベントはクライアントから Citrix Analytics に送信されません。
- **NA**-イベントはクライアントには適用されません。

イベント	Windows 1907 以降用のワークスペースアプリ	Mac 向け Work-space アプリ 1910.2 以降	Linux 2006 以降用のワークスペースアプリ	Android 用ワークスペースアプリ-Google Play で利用可能な最新バージョン	iOS 用ワークスペースアプリ-Apple App Store で入手可能な最新バージョン	Chrome 用ワークスペースアプリ-Chrome Web Store で入手可能な最新バージョン	HTML5 2007 以降用のワークスペースアプリ
アカウントログオン	はい	はい	はい	はい	はい	番号	番号
セッションログオン	はい	はい	はい	はい	はい	はい	はい
セッションの起動	はい	はい	はい	はい	はい	はい	はい
セッション終了	はい	はい	はい	はい	はい	はい	はい
アプリ開始	はい	はい	はい	番号	はい	はい	はい
アプリ終了	はい	はい	はい	番号	はい	はい	はい
ファイルのダウンロード	はい	はい	はい	番号	番号	はい	はい
印刷	番号	はい	はい	番号	番号	はい	はい
SaaS アプリケーションの起動	はい	はい	番号	番号	番号	番号	番号
SaaS アプリ終了	はい	はい	番号	番号	番号	番号	番号

イベント	Windows 1907 以降用のワークスペースアプリ	Mac 向け Work-space アプリ 1910.2 以降	Linux 2006 以降用のワークスペースアプリ	Android 用ワークスペースアプリ-Google Play で利用可能な最新バージョン	iOS 用ワークスペースアプリ-Apple App Store で入手可能な最新バージョン	Chrome 用ワークスペースアプリ-Chrome Web Store で入手可能な最新バージョン	HTML5 2007 以降用のワークスペースアプリ
SaaS アプリ URL ナビゲーション	はい	はい	番号	番号	番号	番号	番号
SaaS アプリのクリップボードへのアクセス	はい	はい	番号	番号	番号	番号	番号
SaaS アプリファイルのダウンロード	はい	はい	番号	番号	番号	番号	番号
SaaS アプリファイル印刷	はい	はい	番号	番号	番号	番号	番号

イベントの送信状態に基づいて、次の問題が発生する可能性があります。

- ユーザーがクライアントを使用して Citrix Virtual Apps and Desktops または Citrix DaaS に接続すると、サポートされているイベント（アクティビティ）が実行されるまで、Citrix Analytics でユーザーが検出されないことがあります。たとえば、アプリケーションの開始と SaaS アプリケーションの起動という 2 つのユーザーイベントについて考えてみます。iOS 向け Citrix Workspace アプリを使用しているユーザーの場合、Citrix Analytics はアプリケーション開始イベントを受信しますが、SaaS アプリ起動イベントは受信しません。したがって、ユーザーが仮想アプリケーションを起動すると、アプリケーション開始イベントが Citrix Analytics に送信され、ユーザーが検出されます。ただし、ユーザーが SaaS アプリケーションを起動した場合、Citrix Analytics は SaaS アプリケーションの起動イベントを受信せず、ユーザーは検出されません。検出されたユーザの詳細については、検出されたユーザを参照してください。
- テーブルで「いいえ」とマークされたイベントは、セルフサービス検索ページに表示されません。セルフサービスページの使用方法については、「セルフサービス検索について」を参照してください。

推奨

Analytics のメリットを最大限に活用するには、次をお勧めします。

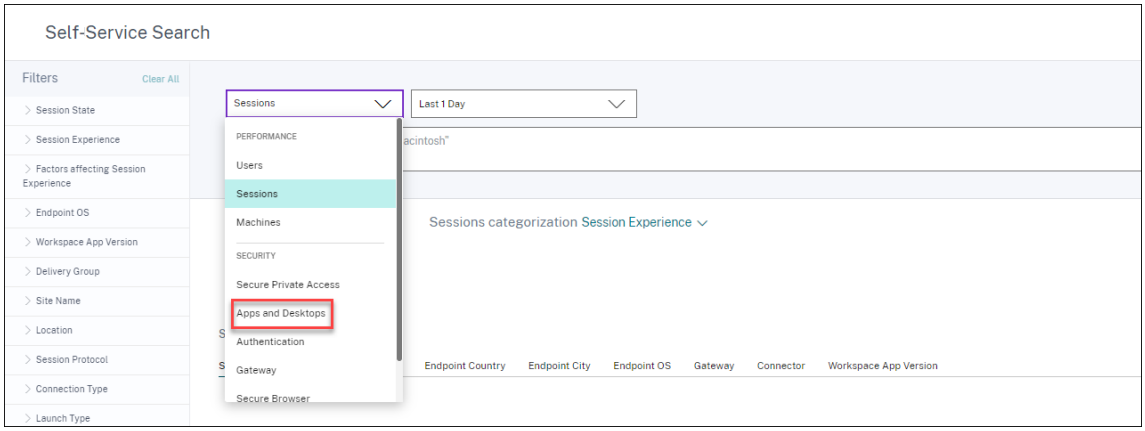
- **Windows** ユーザー: Windows 1907 以降の Citrix Workspace Citrix Virtual Apps and Desktops および Citrix DaaS アプリを使用してに接続します。
- **Mac** ユーザー: **Mac**1910.2 以降の Mac 向け Citrix Citrix Virtual Apps and Desktops および Citrix DaaS Workspace アプリを使用して接続します。

チェック **7-Analytics** のセルフサービス検索ページにユーザーイベントが表示されていますか

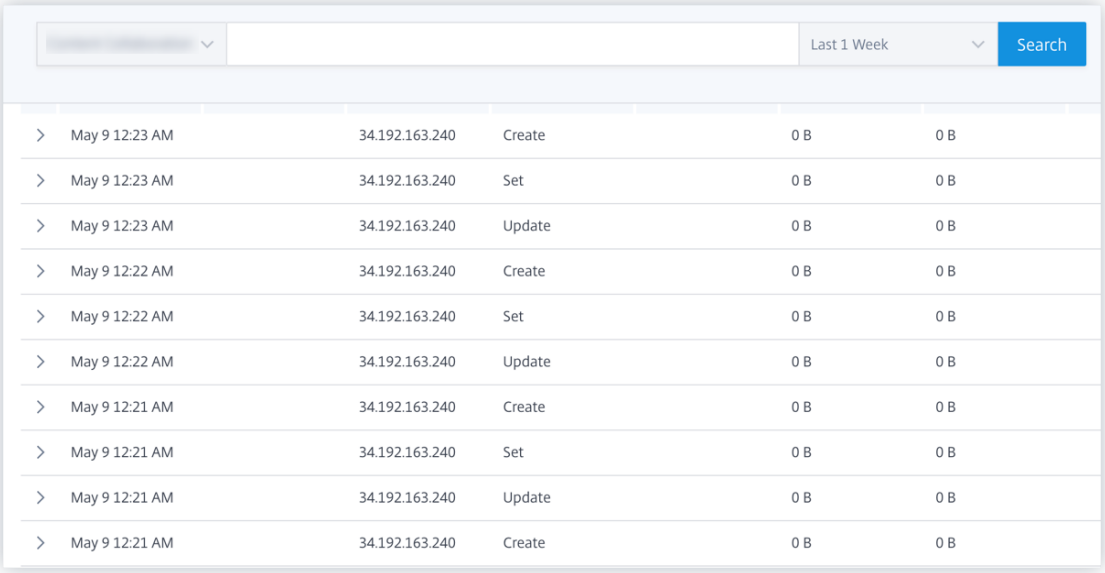
この最終チェックを実行して、イベントが Citrix Analytics に正確に送信されていることを確認します。

1. トップバーの [詳細検索] をクリックして、セルフサービス検索ページに移動します。

2. データソースを選択して、対応する検索ページとイベントを表示します。



3. アプリとデスクトップのイベントに関連するデータを表示するには、リストから **[**** アプリとデスクトップ] を選択し、期間を選択して、[検索] をクリックします。**

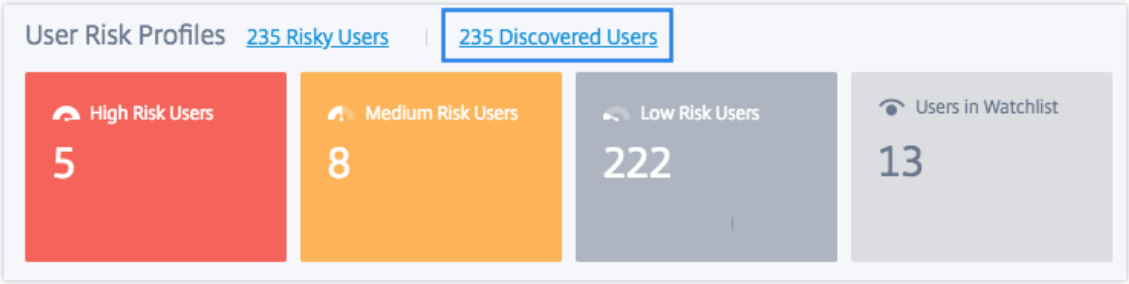


詳細については、「セルフサービス検索」を参照してください。

チェック **8-**ユーザーは **Analytics** によって検出されていますか

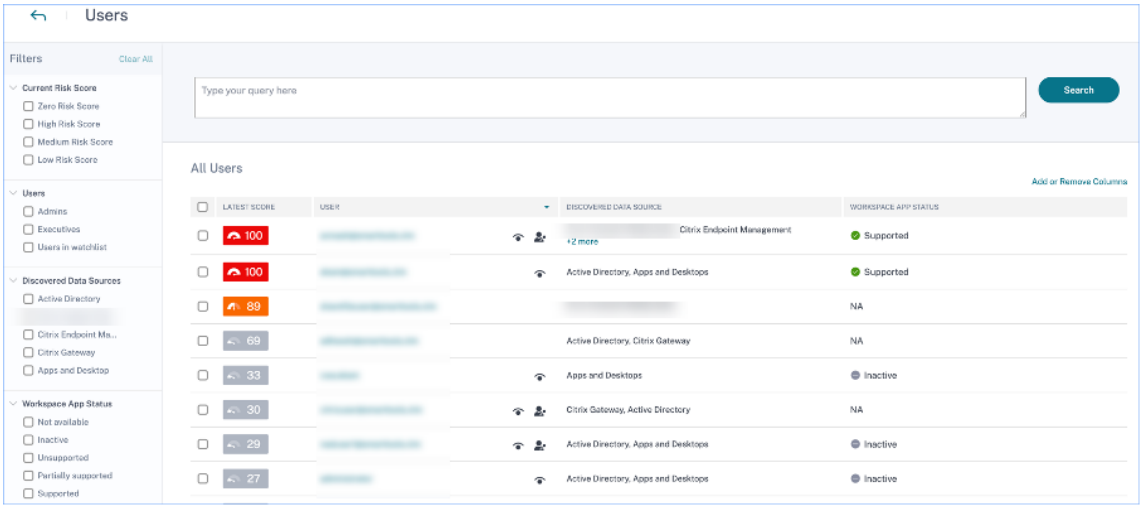
イベントが Citrix Analytics に流れ始めると、イベントを生成したユーザーが検出され、［ユーザー］ダッシュボードに表示されます。このプロセスは、通常、ダッシュボードに表示できるようになるまでに約数分かかります。

1. ［ユーザー］ダッシュボードの［検出されたユーザー **］リンクをクリックすると、Citrix Analytics によって検出されたユーザーの完全なリストが表示されます。



2. ユーザーページには、過去 31 日間に検出されたすべてのユーザーのリストが表示されます。リスク指標の発生を表示する期間を選択します。

> 注:
>
> 31 日を超える値を設定しようとすると、「日付範囲が無効です」というエラーメッセージが表示されます。開始日から終了日までの最大許容範囲は **31** 日です。



イベントが正常に送信されると、Citrix Analytics 環境は期待どおりに動作しています。リスク指標は、異常が検出されたときに生成されます。

Virtual Apps and Desktops イベント、**SaaS** イベントのトリガー、およびイベント送信の検証

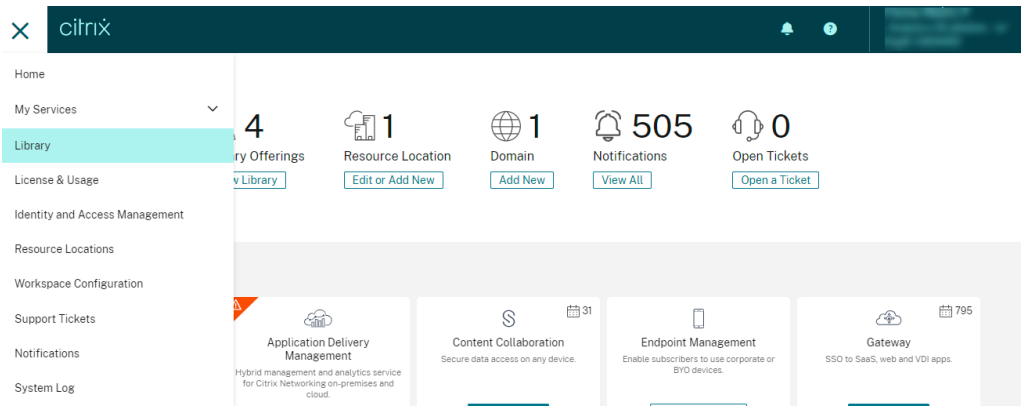
April 12, 2024

このセクションでは、アプリとデスクトップのイベント、SaaS イベントをトリガーし、Citrix Analytics for Security がこれらのユーザーイベントをアクティブに受信していることを確認する手順について説明します。

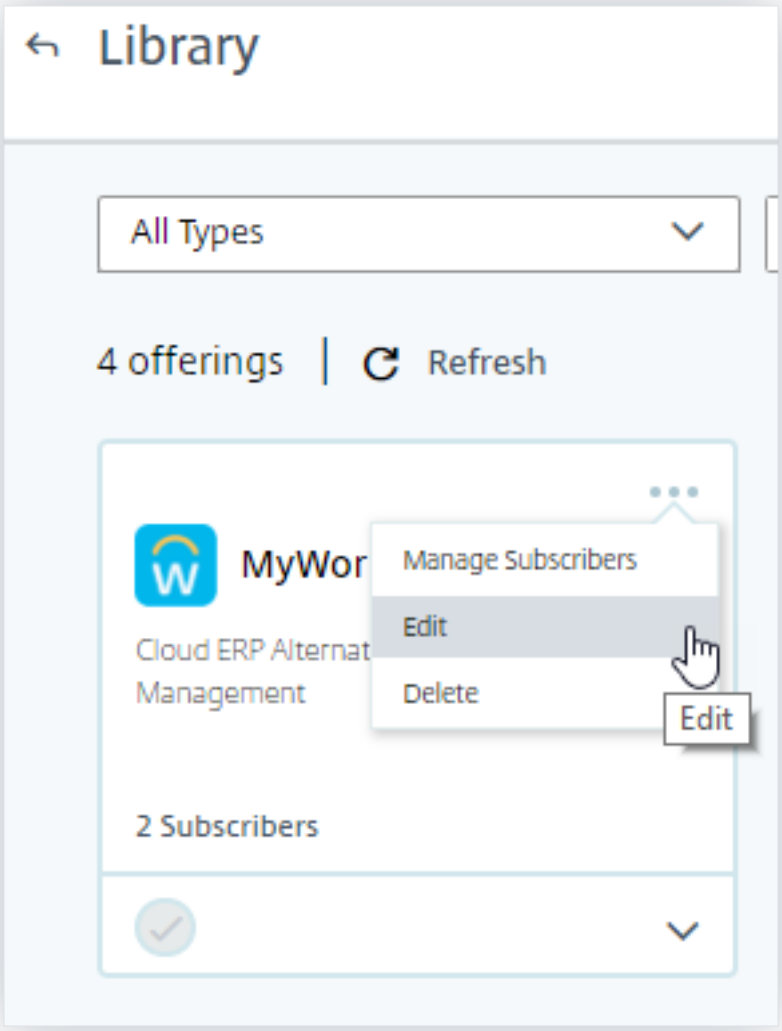
前提条件

- オンプレミスを使用している場合は Citrix Virtual Apps and Desktops、オンプレミスサイトを Citrix Analytics にオンボーディングし、サイトカードからデータ処理を有効にします。Citrix DaaS（以前の Citrix Virtual Apps and Desktops サービス）を使用している場合は、サイトカードから直接データ処理を有効にします。詳しくは、「Citrix Virtual Apps and Desktops」および「Citrix DaaS データソース」を参照してください。
- イベントが Citrix Analytics に正確に送信されるように、ユーザーのエンドポイントデバイスで正しいバージョンの Citrix Workspace アプリまたは Citrix Receiver を使用します。詳しくは、「Citrix Virtual Apps and Desktops」および「Citrix DaaS データソース」を参照してください。
- 仮想デスクトップから印刷イベントをトリガーする前に、アプリとデスクトップ環境でプリンターが構成およびプロビジョニングされていることを確認します。プリンタの管理について詳しくは、「印刷」を参照してください。

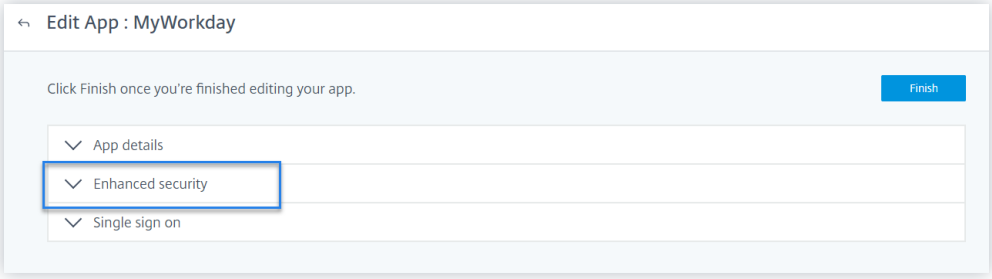
- SaaS アプリケーションの起動、SaaS アプリケーション URL ナビゲーション、SaaS アプリケーションファイルのダウンロードなどの SaaS イベントをトリガーするには、Workspace から構成された SaaS アプリを使用する必要があります。一般的に使用される SaaS アプリケーションには、Salesforce、Workday、Concur、GoTo ミーティングなどがあります。
  - 構成済みの SaaS アプリがない場合は、SaaS アプリを構成して公開する必要があります。詳細については、「サービスとしてのソフトウェアアプリのサポート」を参照してください。SaaS アプリケーションを構成するときは、次のセキュリティオプションが無効になっていることを確認します。
    * クリップボードへのアクセスを制限する
    * 印刷を制限
    * ナビゲーションを制限する
    * ダウンロードを制限する
  - Workspace から設定済みの SaaS アプリを使用してイベントをトリガーする場合は、SaaS アプリに対して指定した拡張セキュリティオプションが無効になっていることを確認します。
    1. Citrix Cloud アカウントに移動し、［ライブラリ］を選択します。



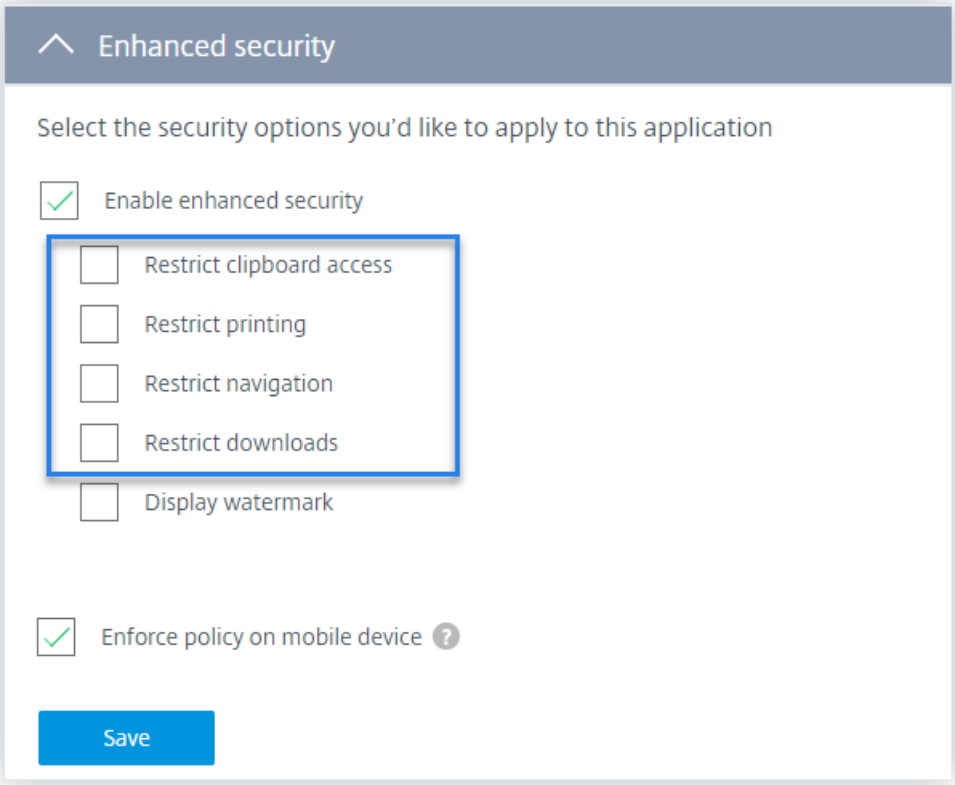
    2. [ライブラリ] ページで、イベントの検証に使用する SaaS アプリを特定します。たとえば、Workday と入力します。
    3. 楕円をクリックし、[編集] を選択します。



4. **[**アプリケーションの編集] ページで、[強化されたセキュリティ] の下矢印をクリックします。



5. 次のセキュリティオプションが選択されていないことを確認します。



既知の問題

一部のバージョンの Citrix Workspace アプリと Citrix Receiver では、一部のイベントを Citrix Analytics に送信できませんしたがって、Citrix Analytics は、これらのイベントに関する洞察を提供したり、リスク指標を生成したりすることはできません。この問題とその回避策の詳細については、既知の問題である CAS-16151を参照してください。

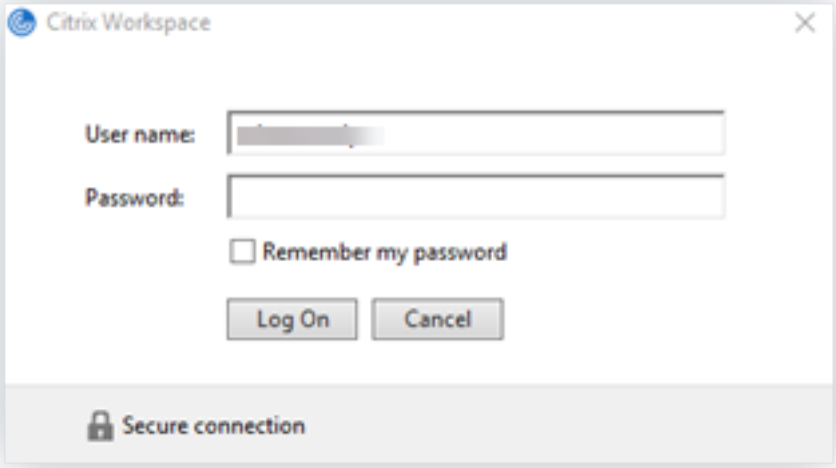
手順

次の手順を順番に実行して、アプリとデスクトップ環境でイベントをトリガーし、Citrix Analytics for Security がこれらのイベントをアクティブに受信していることを確認します。

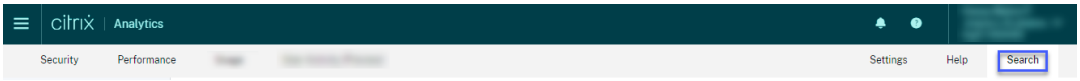
> 注
>
> - イベントが Citrix Analytics に到達するまでに時間がかかる場合があります。トリガーされたイベントが表示されない場合は、[Citrix Analytics] ページを更新します。
> - この手順では、SaaS イベントをトリガーするために、Workday アプリを例として使用します。Workspace から設定済みの任意の SaaS アプリを使用して SaaS イベントをトリガーできます。

- アカウントログオン

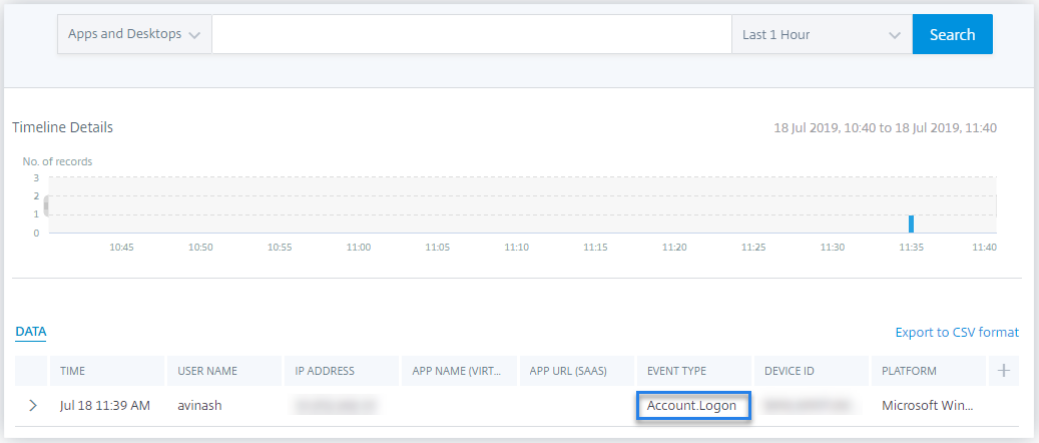
1. Citrix Workspace アプリまたは Citrix Receiver を起動して、ワークスペースまたは StoreFront にアクセスします。
2. 資格情報を入力して、Citrix Workspace アプリまたは Citrix Receiver にログオンします。



3. Citrix Analytics に移動します。
4. [検索] をクリックし、リストから [アプリとデスクトップ] を選択します。



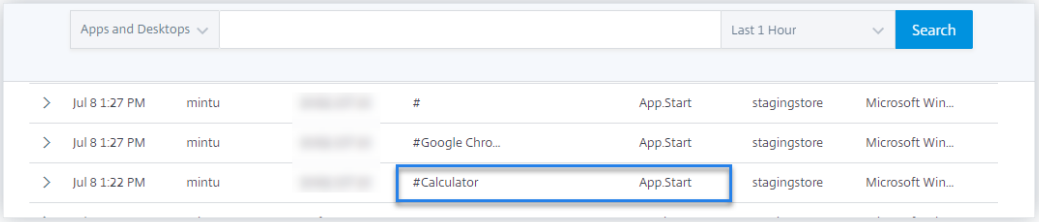
5. 検索ページで、**Account.Logon** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。



- アプリ開始

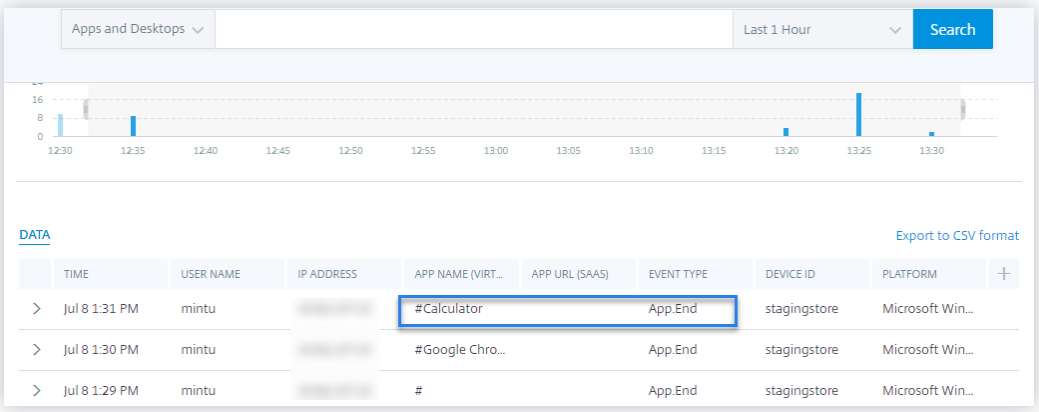
1. Citrix Workspace アプリまたは Citrix Receiver を起動して、ワークスペースまたは StoreFront にアクセスします。

2. 電卓などのアプリケーションを起動します。
3. Citrix Analytics に移動します。
4. [検索] をクリックし、[アプリとデスクトップ] を選択します。
5. 検索ページで、**App.Start** イベントデータのデータを表示します。行を展開して、イベントの詳細を表示します。



- アプリ終了

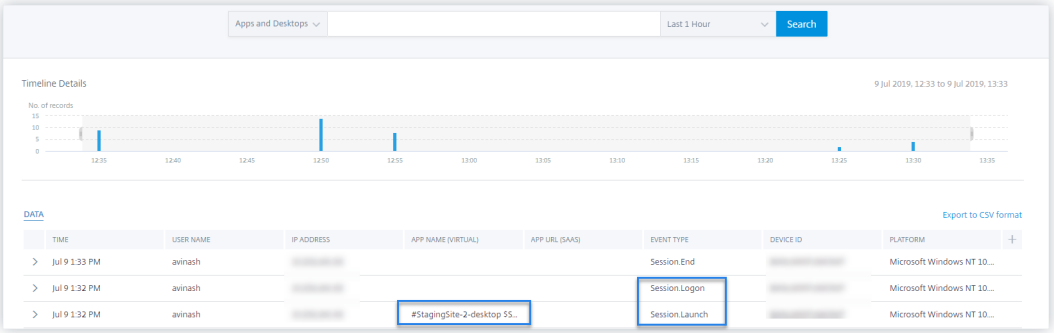
1. ワークスペースまたは StoreFront ですでに起動している計算ツールを閉じます。
2. Citrix Analytics に移動します。
3. [検索] をクリックし、[アプリとデスクトップ] を選択します。
4. 検索ページで、**App.End** イベントデータのデータを表示します。行を展開して、イベントの詳細を表示します。



- セッションログオンとセッション起動

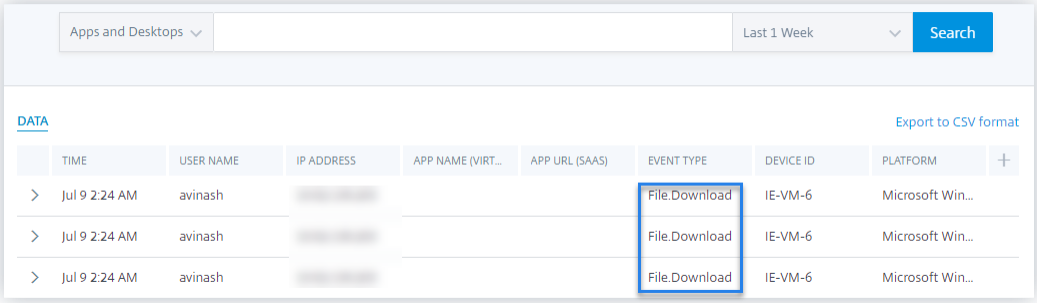
1. Citrix Workspace アプリまたは Citrix Receiver を起動して、ワークスペースまたは StoreFront にアクセスします。
2. 仮想デスクトップを起動します。
3. Citrix Analytics に移動します。
4. [検索] をクリックし、[アプリとデスクトップ] を選択します。

5. 検索ページで、**Session.Logon** および Session.Launch** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。



- ファイルのダウンロード

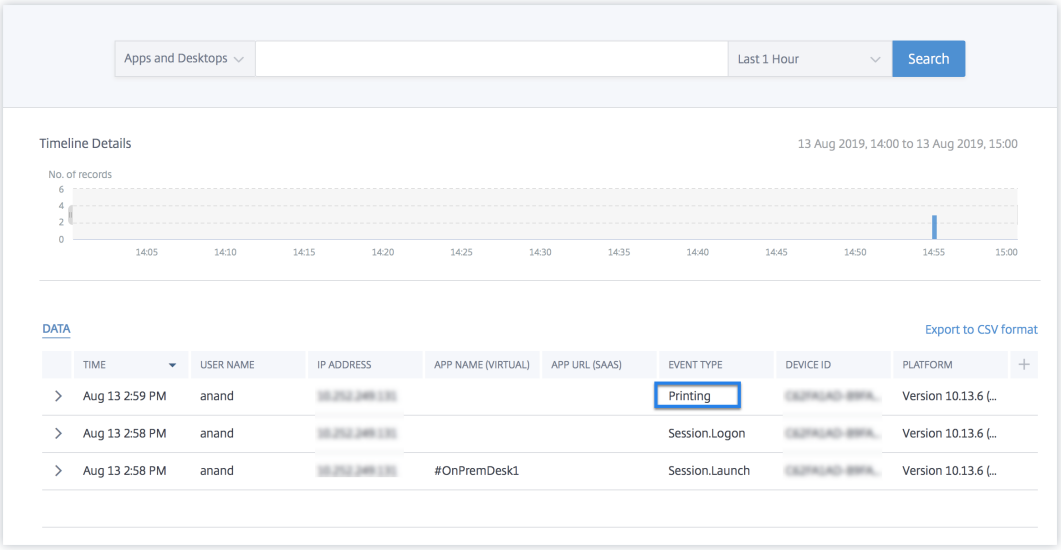
1. Citrix Workspace アプリまたは Citrix Receiver を起動して、ワークスペースまたは StoreFront にアクセスします。
2. 仮想デスクトップを起動します。
3. 仮想デスクトップからローカルコンピュータにファイルをコピーします。
4. Citrix Analytics に移動します。
5. [検索] をクリックし、[アプリとデスクトップ] を選択します。
6. 検索ページで、**File.Download** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。



- 印刷

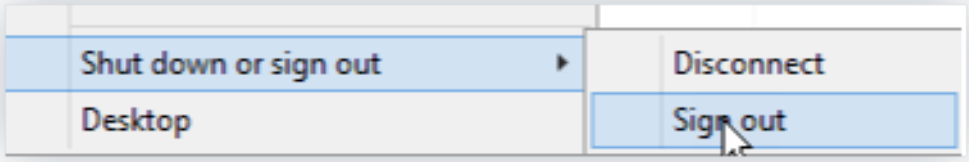
1. Citrix Workspace アプリまたは Citrix Receiver を起動してワークスペースにアクセスします。
2. 仮想デスクトップを起動します。
3. 仮想デスクトップで構成されたプリンタを使用して、ドキュメントを印刷します。
4. Citrix Analytics に移動します。
5. [検索] をクリックし、[アプリとデスクトップ] を選択します。

6. [検索] ページで、**Printing** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。

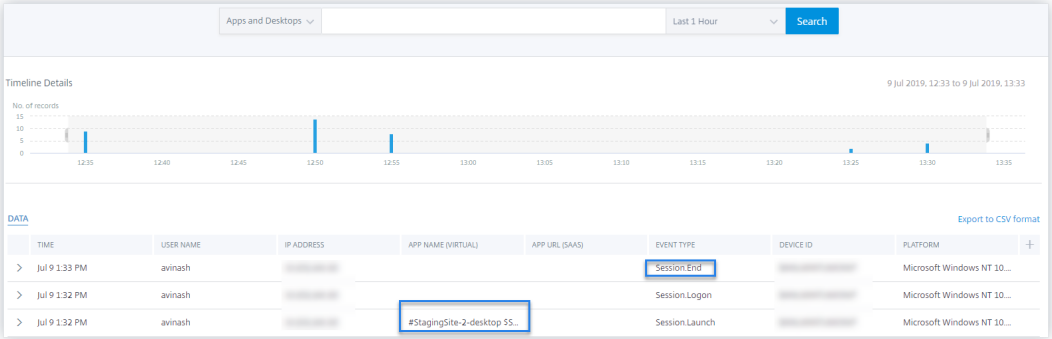


- セッション終了

1. 仮想デスクトップからサインアウトします。たとえば、Windows 仮想デスクトップを使用している場合は、[サインアウト] オプションを選択します。



2. Citrix Analytics に移動します。
3. [検索] をクリックし、[アプリとデスクトップ] を選択します。
4. 検索ページで、**Session.End** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。

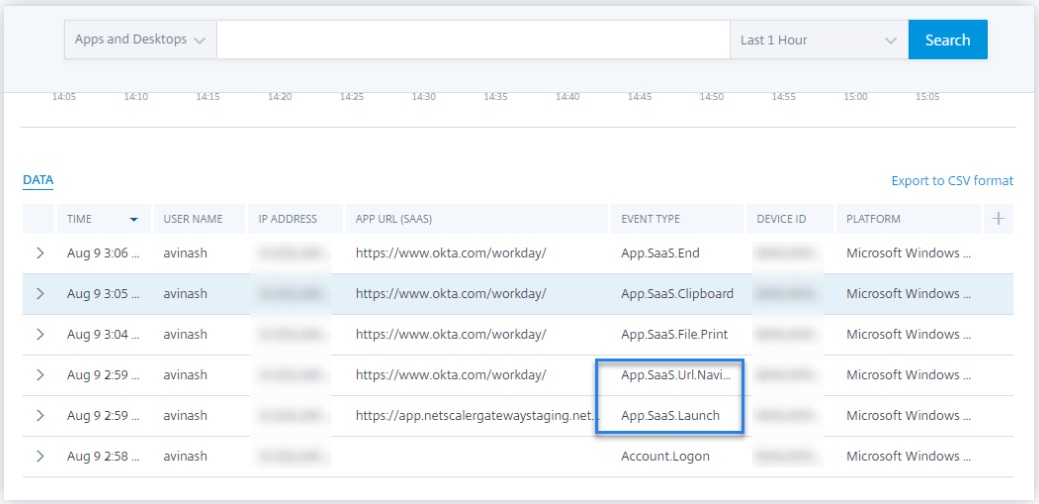


- **SaaS** アプリケーションの起動と **SaaS** アプリケーション **URL** ナビゲーション

  1. Citrix Workspace アプリまたは Citrix Receiver を起動して、ワークスペースまたは StoreFront にアクセスします。
  2. Workday などの SaaS アプリケーションを起動し、[Workday] ページが読み込まれるまで待ちます。Workday の Web ページ内を移動します。

     > 注
     >
     > [セキュリティの強化] セクションの [ナビゲーションの制限] オプションが無効になっていることを確認します。詳細については、「前提条件」を参照してください。

  3. Citrix Analytics に移動します。
  4. [検索] をクリックし、[アプリとデスクトップ] を選択します。
  5. 検索ページで、**app.saas.Launch** イベントと app.saas.url.Navigation** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。



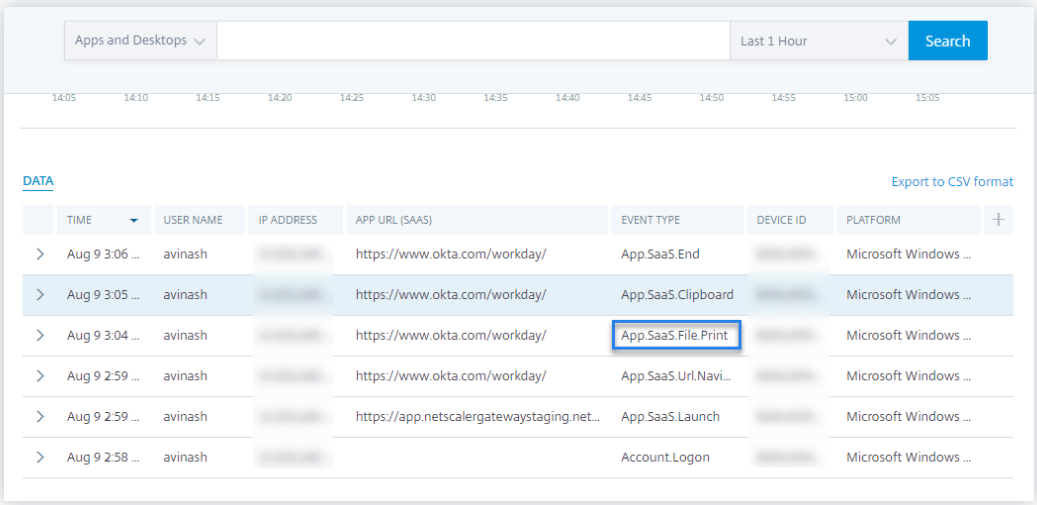
- **SaaS** アプリファイル印刷

  1. 現在表示している [Workday] ページを印刷します。

     > 注
     >
     > [セキュリティの強化] セクションの [印刷を制限する] オプションが無効になっていることを確認します。詳細については、「前提条件」を参照してください。

  2. Citrix Analytics に移動します。
  3. [検索] をクリックし、[アプリとデスクトップ] を選択します。

4. 検索ページで、**app.Saas.File.Print** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。

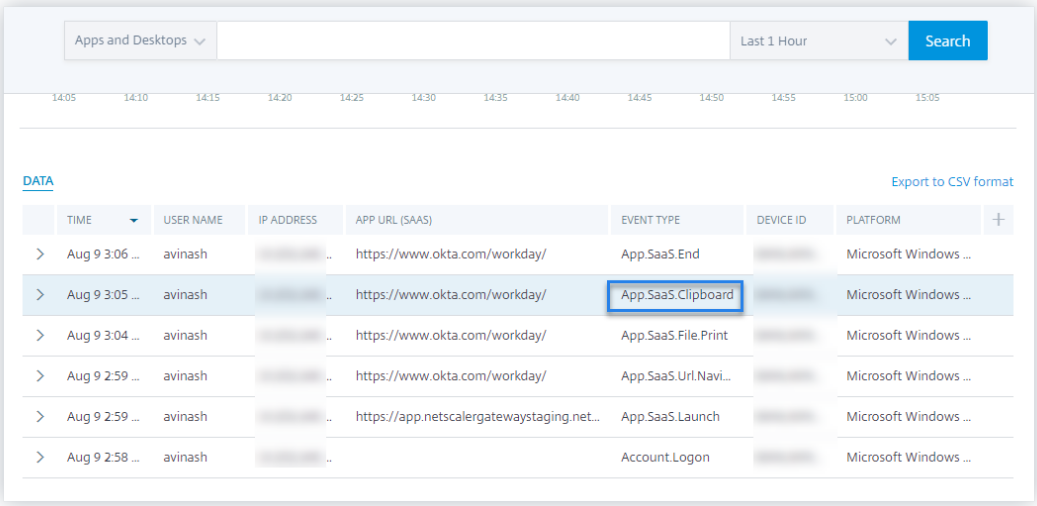


- **SaaS** アプリのクリップボードへのアクセス

1. [Workday] ページから、テキストをシステムのクリップボードにコピーします。

> 注
>
> [セキュリティの強化] セクションの [クリップボードへのアクセスを制限する] オプションが無効になっていることを確認します。詳細については、「前提条件」を参照してください。

2. Citrix Analytics に移動します。
3. [検索] をクリックし、[アプリとデスクトップ] を選択します。
4. 検索ページで、**app.SaaS.Clipboard** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。

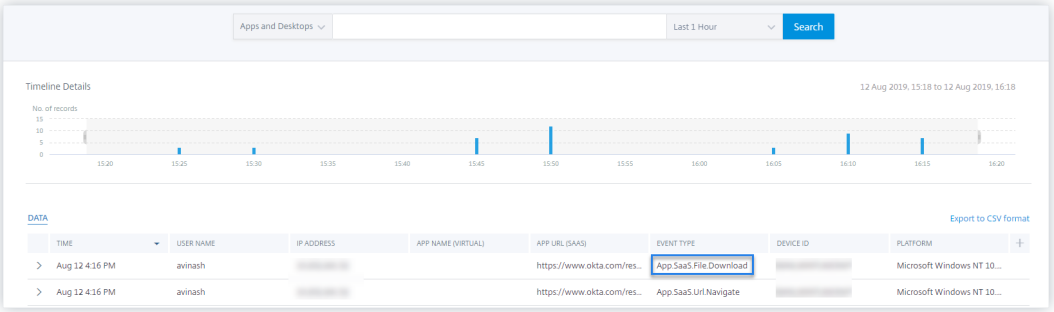


- **SaaS** アプリファイルのダウンロード

  1. [Workday] ページで、ホワイトペーパーなどの公開ドキュメントを検索し、そのドキュメントをダウンロードします。

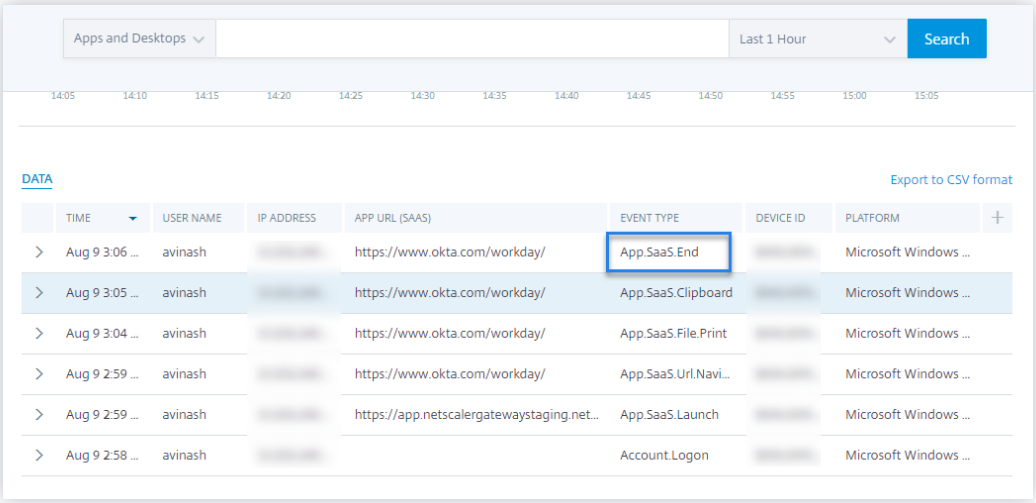
     > 注
     >
     > [セキュリティの強化] セクションの [ダウンロードを制限する] オプションが無効になっていることを確認します。詳細については、「前提条件」を参照してください。

  2. Citrix Analytics に移動します。
  3. [検索] をクリックし、[アプリとデスクトップ] を選択します。
  4. [検索] ページで、**app.saas.file.Download** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。



- **SaaS** アプリ終了

  1. [Workday] ページを閉じます。
  2. Citrix Analytics に移動します。
  3. [検索] をクリックし、[アプリとデスクトップ] を選択します。
  4. 検索ページで、**App.Saas.End** イベントのデータを表示します。行を展開して、イベントの詳細を表示します。



- **VDA.Print**

  前提条件

  印刷イベントをトリガーする前に、「Citrix DaaS の印刷テレメトリの有効化」を参照してください。

  印刷イベントをトリガーするには、次のアクションを実行します。

  1. テキストドキュメントをメモ帳または印刷が許可されているその他のアプリで開きます。
  2. [ファイル] **>** [印刷] をクリックするか、**Ctrl+P** を押します。
  3. [プリンタの選択] でプリンタを選択し、[適用] をクリックして印刷します。

- **VDA** クリップボード

  前提条件

  印刷イベントをトリガーする前に、「Citrix DaaS のクリップボードテレメトリの有効化」を参照してください。

  クリップボードイベントをトリガーするには、次のアクションを実行します。

  1. メモ帳または任意のテキストエディタでテキストドキュメントを開きます。
  2. コピーするコンテンツを選択します。
  3. [コピー] を右クリックするか、Ctrl+C を押します。

サポートされている **Citrix Workspace** アプリのバージョンからユーザーイベントを受信していません

July 15, 2022

Citrix Analytics でサポートされている Citrix Workspace アプリのバージョンを使用しているユーザーからのイベントが表示されない場合は、次のいずれかに問題がある可能性があります。

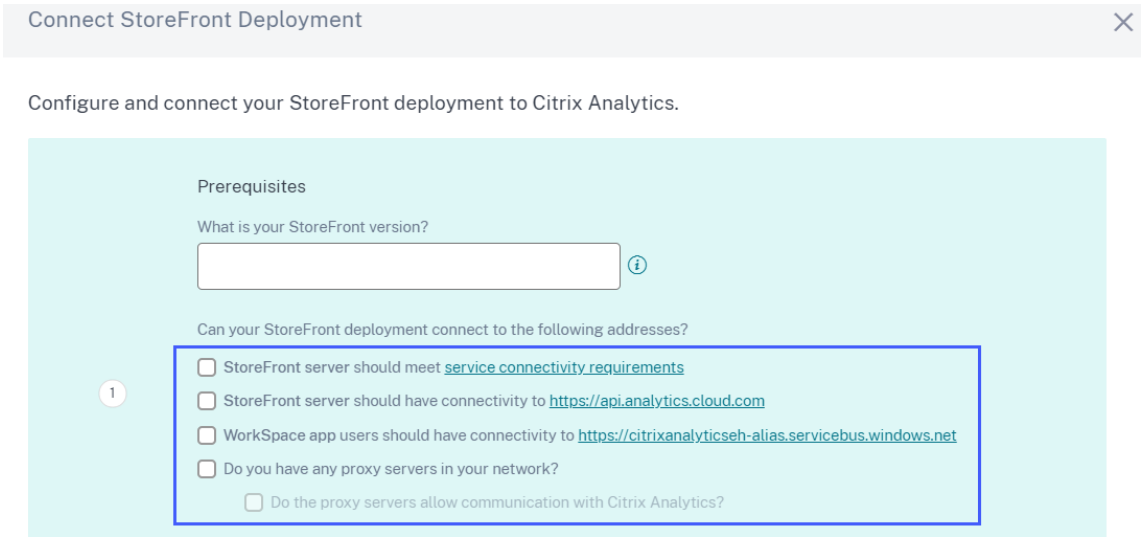
- StoreFront の構成
- Web 起動要件

StoreFront の構成

StoreFront 展開環境が Citrix Analytics に接続されている場合は、［最終更新日］のタイムスタンプを確認します。ユーザーが SStoreFront にアクティブにアクセスしている場合は、少なくとも週に 1 回は時刻を更新する必要があります。頻繁な更新は、StoreFront 展開環境と Citrix Analytics の間の正常な接続を示します。そうしないと、接続の問題がいくつかあります。

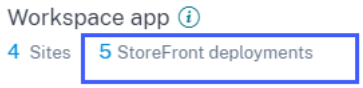
次の接続要件を確認します。

- StoreFront サーバーは、システム要件と接続要件を満たしている必要があります。
- StoreFront サーバーは`https://api.analytics.cloud.com`に接続できる必要があります
- Workspace アプリのユーザーは、`https://citrixanalyticseh-alias.servicebus.windows.net`に接続できる必要があります
- プロキシサーバーで Citrix Analytics イベントハブへの接続を許可する必要があります。
  - 米国リージョン: `https://citrixanalyticseh-alias.servicebus.windows.net/`
  - 欧州連合地域: `https://citrixanalyticseheu-alias.servicebus.windows.net/`
  - アジア太平洋南部リージョン: `https://citrixanalyticsehaps-alias.servicebus.windows.net/`

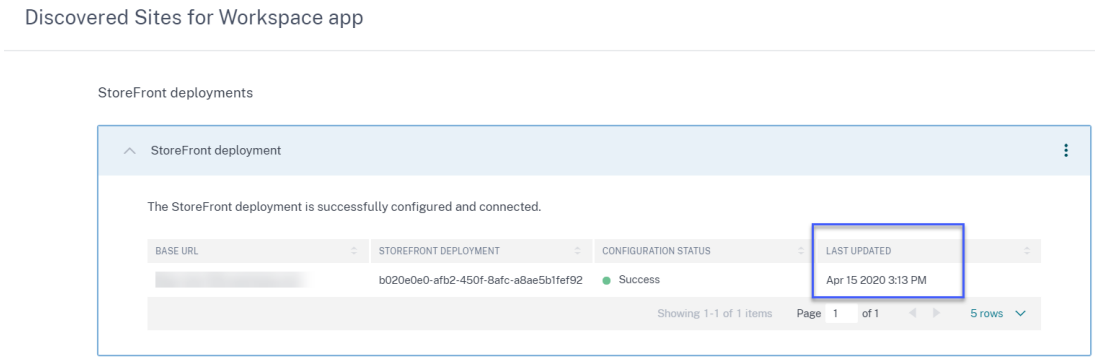


最終更新時刻を確認するには:

1. [設定] **>** [データソース] をクリックします。
2. Workspace アプリサイトカードで、接続されている StoreFront サーバーの数をクリックします。



3. SStoreFront 展開環境で、最終更新時刻を確認します。



接続要件を満たしても最終更新タイムスタンプが頻繁に更新されない場合は、StoreStoreFront 構成します。詳しくは、「StoreFront を使用した Virtual Apps and Desktops サイトのオンボード」を参照してください。

Web 起動要件

ユーザーは、次のいずれかの方法で仮想アプリケーションおよびデスクトップを起動できます。

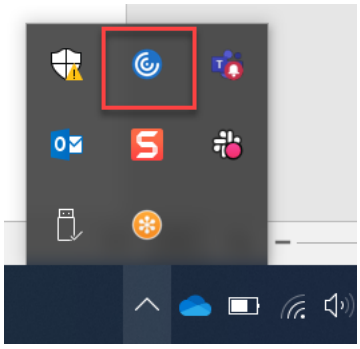
- Citrix Workspace アプリからシトリックスストアまたは Citrix Workspace にアクセスします。このアプローチをネイティブ起動と呼びます。
- Web ブラウザーで Citrix ストア URL または Citrix Workspace の URL を開きます。アプリケーションまたは仮想デスクトップをクリックして、対応する ICA ファイルをダウンロードします。次に、Web ブラウザーを使用して ICA ファイルを開き、アプリケーションまたは仮想デスクトップを起動します。このアプローチは Web 起動と呼ばれます。

Web 起動の場合は、デバイスのオペレーティングシステムに基づいて、ユーザーデバイスに次のいずれかのクライアントが必要であることを確認します。

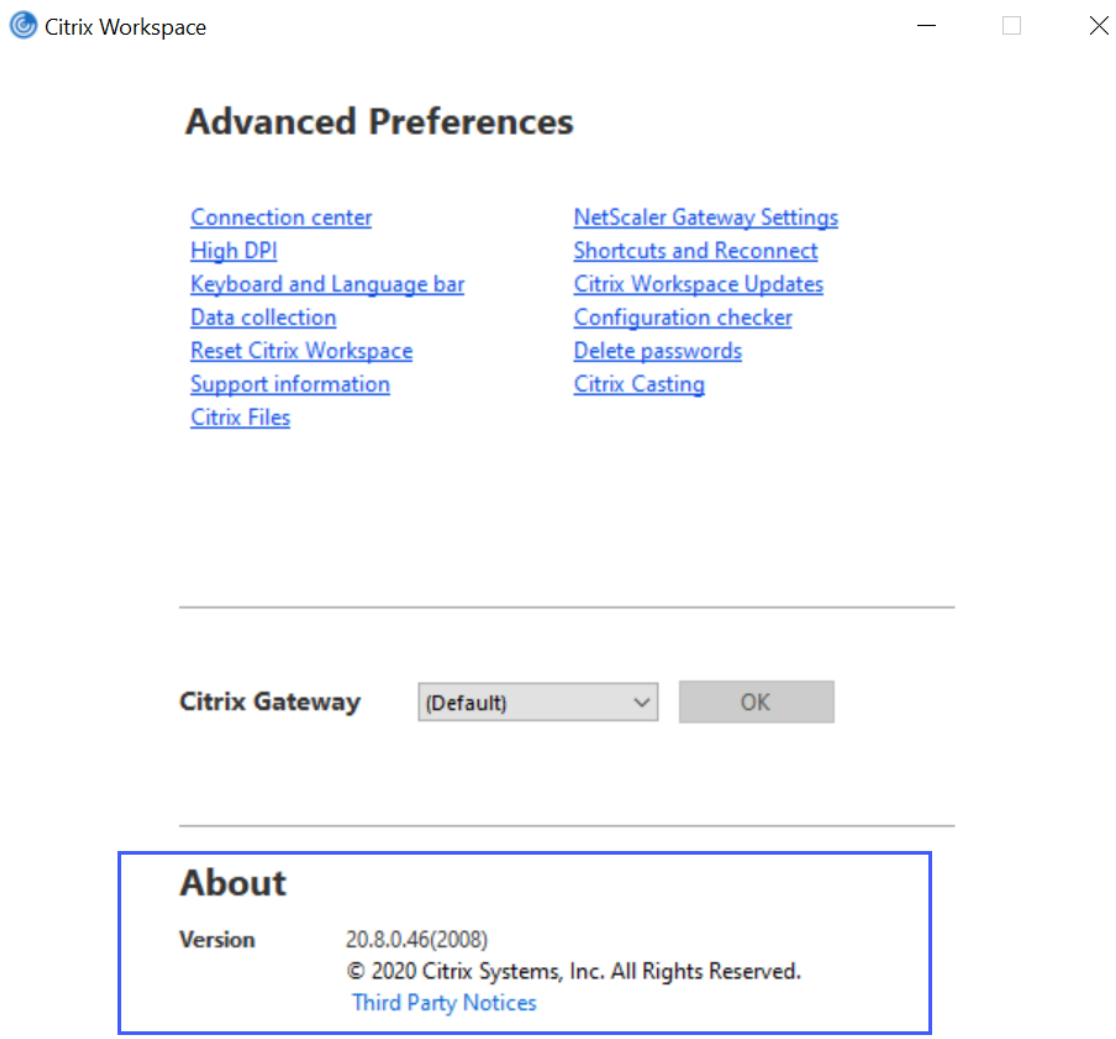
クライアント	バージョン	構築
Windows 向け Citrix Workspace アプリ	2006.1 以降	20.6.0.38 またはそれ以降
Mac 向け Citrix Workspace アプリ	2006 以降	20.06.0.7 以降

Citrix Workspace アプリのバージョンを確認するには:

1. ユーザーのローカルマシンで、Citrix Workspace アプリのアイコンを右クリックします。



2. [詳細設定] をクリックし、[バージョン情報] セクションをチェックしてバージョンを表示します。



構成された **Session Recording** サーバーが接続に失敗する

July 15, 2022

構成後、Session Recording サーバーが Citrix Analytics に接続できない。したがって、**Session Recording** サイトカードに構成済みのサーバーが表示されません。

この問題のトラブルシューティングを行うには、次の操作を行います。

1. 設定した Session Recording サーバーで、次の PowerShell コマンドを実行して、クライアントマシン識別 (CMID) を確認します。

```
Get-WmiObject -class SoftwareLicensingService | select
    Clientmachineid
```


2. CMID が空の場合、指定したパスに次のレジストリファイルを追加します。

レジストリ名	レジストリのパス	キー型	値
AuditorUniqueID	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\	文字列	UUID を入力します。
EnableCASUseAuditorUniqueID	Computer/HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/SmartAuditor/Server/	REG_DWORD	1

3. 次のサービスを再起動します:

   - Citrix Session Recording Analytics サービス
   - Citrix Session Recording ストレージマネージャー

StoreFront サーバーを Citrix Analytics と接続

January 5, 2023

Citrix Analytics から StoreFront サーバーに構成設定をインポートすると、StoreFront サーバーは Citrix Analytics への接続に失敗します。

StoreFront サーバーに構成設定をインポートする方法については、「StoreFront を使用した Virtual Apps and Desktops サイトのオンボード」を参照してください。

CAS Onboarding Assistant は、この記事で説明されている問題の確認とトラブルシューティングに役立ちます。詳しくは、「Citrix Analytics サービス（CAS）オンボーディングアシスタント」を参照してください。

この問題のトラブルシューティングを行うには、次の操作を行います。

1. StoreFront サーバーで、Citrix Analytics 地域固有のエンドポイントに ping を実行して 、StoreFront サーバーと Citrix Analytics サーバー間の接続をテストします。また、前提条件が満たされていることを確認します 。

> 注
>
> StoreFront サーバーでは、地域固有のエンドポイントに直接 ping を実行するか、Web ブラウザーを開いて地域固有のエンドポイントにアクセスすることで、接続をテストできます。

2. StoreFront サーバーで詳細ログを有効にして、ログをトレースします。詳細ロギングについて詳しくは、CTX139592 の記事を参照してください。
3. インターネットインフォメーションサービス (IIS) マネージャを開き、次の点を確認します。
   - StoreFront サイトが IIS のデフォルトサイトの下にある場合、IIS は StoreFront サイトを再起動します。
   - StoreFront サイトが他のドライバーにあるか、デフォルトサイトにない場合は、コマンドウィンドウを開いて次のように入力します `iisreset`。
4. 次のコマンドを実行して、Citrix Analytics の設定をインポートします。

```
Import-STFCasConfiguration -Path "configuration file path"
```

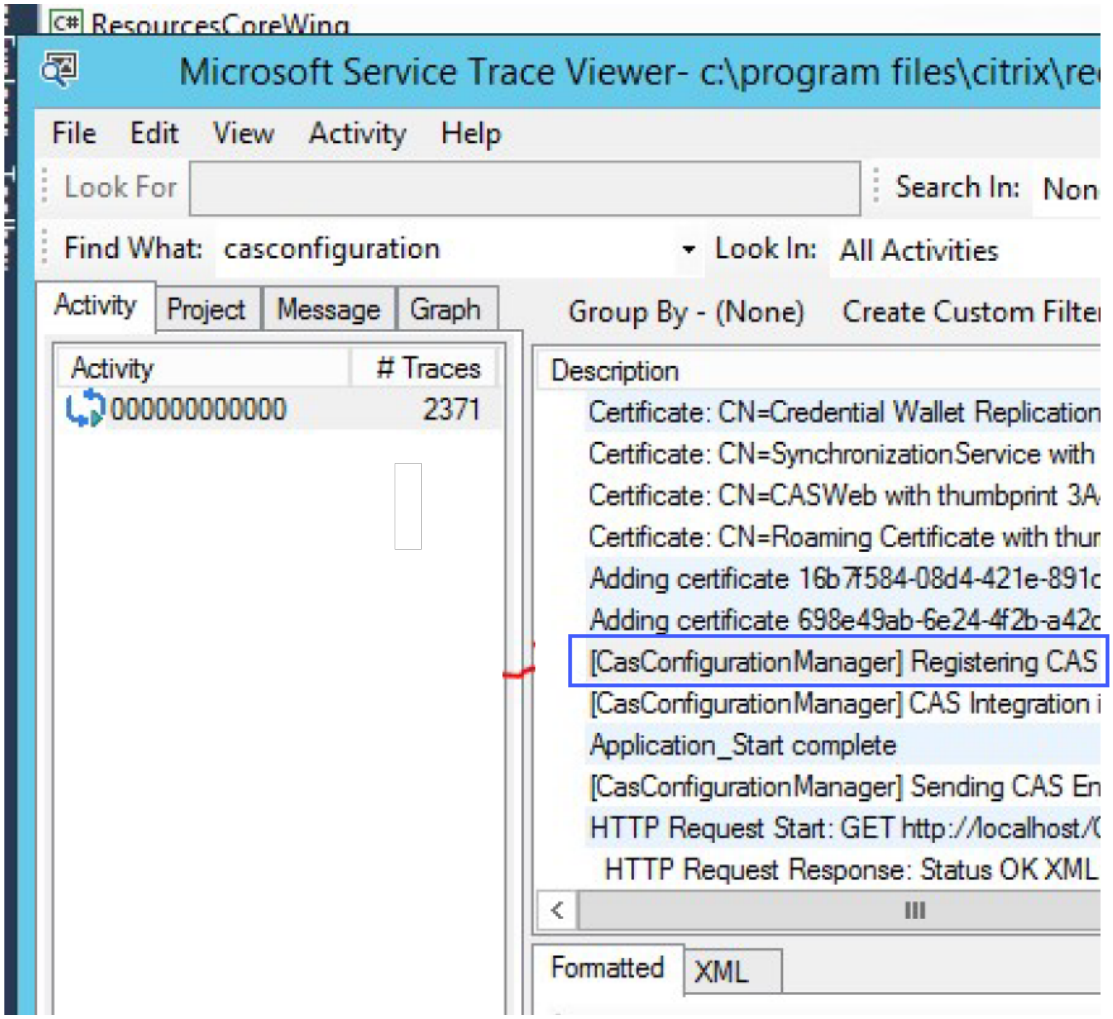
5. 次のコマンドを実行して、インポートした設定を確認します。

```
Get-STFCasConfiguration
```

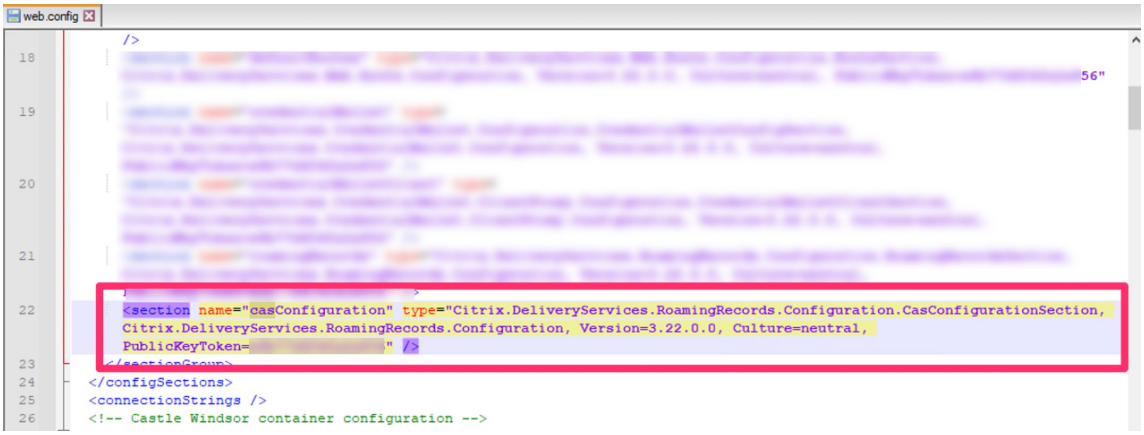
6. StoreFront サイトが他のドライバー内にあるか、デフォルトサイトの下にない場合は、コマンドウィンドウを開きます。StoreFront サイトに Citrix Analytics の設定を読み取らせるには `iisreset` を入力します
7. StoreFront の詳細ログファイルを次の場所から取得します。

```
C:\Program Files\Citrix\Receiver StoreFront\Admin\trace
```

   上記の場所には、イベントビューアで開くことができる複数の svclog ファイルがあります。
8. Microsoft サービストレースビューアを使用して、次のログを開きます。
   - StoreFront ログ
   - ローミングサイトの詳細ログ
9. ログで、**CASConfigurationManager** セクションと Citrix Analytics サーバー情報が利用可能であることを確認します。



10. CASConfigurationManager セクションが使用できない場合は、にあるローミングサイトの web.config `roaming site\folder`ファイルを開きます。
11. `web.config` ファイルで［**CASConfiguration**］セクションを探し、Citrix Analytics サーバーの情報が利用可能であることを確認します。



12. StoreFront サーバーがインストールされている Windows サーバーマシンで、以下を確認します。

- TLS 1.2 クライアントは有効になっています。
- 次の暗号スイートのうち少なくとも 1 つが有効になっている。
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

TLS 暗号スイートの順序を設定する方法については、Microsoft のドキュメントを参照してください。

13. Windows Server 2012 マシンを使用している場合は、Diffie-Hellman Exchange (ECDHE/DHE) が有効になっていることを確認します。
14. StoreFront サーバーがインストールされている Windows Server マシンに、Microsoft のドキュメントに記載されているレジストリ設定が含まれている必要があることを確認します。

> 重要
>
> : グループポリシーを使用して TLS/SSL 暗号スイートを更新します。TLS/SSL 暗号スイートを手動で変更しないでください。グループポリシーの使用方法の詳細については、Microsoft のドキュメントを参照してください。

たとえば、Windows Server マシンで次のレジストリ設定を使用できる必要があります。

TLS 1.2 クライアント**:**

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"Enabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000

<!--NeedCopy-->
```

Diffie-Hellman KEAs:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman
    ]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

AES-128/AES-256 暗号**:**


```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Ciphers\AES 128/128]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Ciphers\AES 256/256]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

SHA256/SHA384 ハッシュ**:**

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Hashes\SHA256]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Hashes\SHA384]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

よくある質問

November 26, 2023

データソース

データソースって何ですか**?**

データソースは、Citrix Analytics にデータを送信する Citrix のサービスおよび製品です。

詳細: データソース

データソースを追加するにはどうすればいいですか

Citrix Analytics にログオンした後、［ようこそ］画面で［はじめに］を選択して、データソースを Citrix Analytics に追加します。または、[設定**] > [**データソース**]** に移動して、データソースを追加することもできます。

NetScaler ADM エージェント

オンプレミスのハイパーバイザーにエージェントをインストールするための最小リソース要件は何ですか**?**

8 GB RAM、4 仮想 CPU、120 GB ストレージ、1 仮想ネットワークインターフェイス、1 Gbps スループット

プロビジョニング中に **NetScaler ADM** エージェントに追加のディスクを割り当てる必要がありますか

いいえ、ディスクを追加する必要はありません。エージェントは、Citrix Analytics とエンタープライズデータセンターのインスタンスとの間の仲介としてのみ使用されます。追加のディスクを必要とするインベントリや分析データは保存されません。

エージェントにログオンするためのデフォルトの認証情報は何ですか

エージェントにログオンするためのデフォルトの認証情報は`nsrecover`/`nsroot`です。これにより、エージェントのシェルプロンプトにログオンします。

間違った値を入力した場合、エージェントのネットワーク設定を変更するにはどうすればいいですか

ハイパーバイザーのエージェントコンソールにログオンし、資格情報 `nsrecover`/`nsroot`を使用してシェルプロンプトにアクセスし、コマンド`networkconfig`を実行します。

サービス **URL** とアクティベーションコードが必要なのはなぜですか

エージェントは、サービス URL を使用してサービスを検索し、アクティベーションコードを使用してエージェントをサービスに登録します。

エージェントコンソールでサービス **URL** を間違って入力した場合、どうすれば再入力できますか

資格情報`nsrecover`/`nsroot`を使用してエージェントのシェルプロンプトにログオンし、次のように入力します。`deployment_type.py` このスクリプトを使用すると、サービス URL とアクティベーションコードを再入力できます。

新しいアクティベーションコードはどうやって入手できますか

NetScaler ADM サービスから新しいアクティベーションコードを取得できます。NetScaler ADM サービスにログオンし、[ネットワーク] **>** [エージェント] に移動します。[エージェント] ページの **[**アクションの選択**]** リストから、[アクティベーションコードの生成] を選択します。

アクティベーションコードを複数のエージェントで再利用できますか**?**

いいえ、あなたはできません。

NetScaler ADM エージェントはいくつインストールする必要がありますか

エージェントの数は、データセンターのマネージドインスタンスの数と合計スループットによって異なります。Citrix では、各データセンターに少なくとも 1 つのエージェントをインストールすることをお勧めします。

複数の **NetScaler ADM** エージェントをインストールするにはどうすればいいですか

[データソース] ページで、NetScaler Gateway の横にあるプラス（+）記号をクリックし、指示に従って別のエージェントをインストールします。

または、NetScaler ADM GUI にアクセスして [ネットワーク] > [エージェント] に移動し、[エージェントの設定] をクリックして、複数のエージェントをインストールすることもできます。

高可用性セットアップで **2** つのエージェントをインストールできますか**?**

いいえ、あなたはできません。

エージェントの登録に失敗した場合の対処方法

- エージェントがインターネットにアクセスできることを確認します (DNS の設定)。
- アクティベーションコードを正しくコピーしたことを確認してください。
- サービス URL が正しく入力されていることを確認してください。
- 必要なポートが開いていることを確認してください。

登録は成功しましたが、エージェントが正常に動作しているかどうかはどうすればわかりますか

エージェントが正常に動作しているかどうかを確認するには、次の操作を行います。

- エージェントが正常に登録されたら、NetScaler ADM にアクセスし、[ネットワーク**] > [**エージェント] に移動します。このページで検出されたエージェントを表示できます。エージェントが正常に動作している場合、ステータスは緑色のアイコンで示されます。実行中でない場合、状態は赤いアイコンで示されます。
- エージェントのシェルプロンプトにログオンし、`ps -ax | grep mas`と`ps -ax | grep ulfd` コマンドを実行します。次のプロセスが実行中であることを確認します。

- 実行されていないプロセスがある場合は、コマンド **masd restart** を実行します。すべてのデーモンを起動するには時間がかかる場合があります (1 分程度)。
- エージェントの登録が成功したら、/mpsconfigでagent.confが作成されていることを確認してください。

NetScaler Gateway インスタンスのオンボード

NetScaler Gateway インスタンスは **Citrix Analytics** に追加されますが、エージェントで **Analytics** が有効になっているかどうかはどうすればわかりますか

エージェントのシェルプロンプトを使用して、エージェントで分析が有効になっているかどうかを確認できます。エージェントでアナリティクスが正常に有効になっている場合、turnOnEventパラメータは/mpsconfig/telemetry_cloud.confファイル内でYに設定されます。

エージェントのシェルプロンプトにログオンし、cat /mpsconfig/telemetry_cloud.confコマンドを実行し、turnOnEventパラメータの値を確認します。

誤って **NetScaler Gateway** オンボーディングウィザードを閉じてしまいました。設定は最初から始める必要がありますか

いいえ。Citrix Analytics は進行状況を保存し、［データソース］**>**［設定］ページにタイルとして不完全な構成を表示します。[セットアップを続行] をクリックして設定を完了します。

Virtual Apps and Desktops サイトのオンボーディング

データ処理をオフにするにはどうすればいいですか

サイトから Citrix Analytics へのデータ処理を一時的に無効にする場合は、［サイト］カードをクリックし、［データ処理を無効にする］をクリックします。

自分のサイトを **Workspace** に追加して「**Test STA**」をクリックすると、テストが失敗します。どのように対処すればよいですか**?**

NetScaler Gateway とクラウドコネクタの間に接続の問題がある可能性があります。トラブルシューティングを行うには、Citrixサポート Knowledge Center CTX232517 を参照してください 。

Citrix Analytics のヘルプはどこで入手できますか

https://discussions.citrix.com/forum/1710-citrix-analytics/ にある Citrix Analytics ディスカッションフォーラムで、質問をしたり、Citrix Analytics 専門家と連絡を取ったりすることができます。

フォーラムに参加するには、Citrix ID でサインインする必要があります。

アクセス保証—ジオロケーション

位置情報の詳細は **Analytics** によってどのように導き出されますか

Citrix Analytics は、ワークスペースクライアントが起動されたデバイスの IP アドレスを使用します。Citrix Analytics は、サードパーティの IP 位置情報データプロバイダーを利用して、IP アドレスからユーザーの位置情報を導き出します。セッションログオンを実行すると、ユーザーの場所 (IPv4 アドレス) が国または都市に解決され、マッピングが定期的に更新されます。組織は、国によって定義されたこれらの場所を使用して、ビジネスを行わない場所からのアクセスパターンを監視できます。

ユーザーの位置情報を導き出す精度はどれくらいですか

Citrix Analytics は、サードパーティの IP 位置情報データプロバイダーを利用して、IP アドレスからユーザーの位置情報を導き出します。GeoIP サービスは、ほとんどの場合、適切な都市または場所に解決できますが、GeoIP ルッ

クアップが完全に正確になることはありません。ユーザーに表示されている場所が、アクセスした正確な場所と異なる場合があります。

IP GeoPoint のドキュメントによると、カバレッジレベルは世界中で割り当てられている IP アドレス (IPv4 ルーティング可能な IP アドレス) の約 99.99% です。位置の精度に関しては、必須のロケーションフィールド (国、州、都市、郵便番号) のそれぞれに [信頼係数] が付いています。

位置の決定が不正確になるのはどのような場合ですか

位置情報データの精度は、デバイスがインターネットに接続する方法によって異なります。デバイスは次の方法でインターネットに接続できます。

- モバイルゲートウェイ
- VPN またはホスティング施設
- 地域または国際的なプロキシ/アノニマイザーサーバー

このような場合、IP ジオロケーションプロバイダソフトウェアを使用しても、ジオロケーションデータは正確ではありません。

サポートされている **Citrix Workspace** アプリのバージョンは何ですか

オペレーティングシステムがセキュリティのために Citrix Analytics に **IP** アドレス属性を送信するために必要な **Citrix** Workspace アプリの最小バージョンがあります。詳細については、[マトリックス表または利用できないと特定された場所を参照してください](/ja-jp/security-analytics/access-assurance-location.html#locations-identified-as-not-available) 。

地質学的詳細を受け取らないのはどのような場合ですか

ジオロケーションの詳細を表示するには、「利用できないと識別されたロケーション 」セクションで詳細を参照してください。

Citrix Analytics がユーザーの位置を報告するために使用する地理位置情報サービスは何ですか? **IP** の間違った場所を報告するにはどうすればいいですか

Citrix Analytics は、Neustar ファイルベースの位置情報サービスを使用して 、着信アクセス用の位置情報データを提供します。公開されている IP 訂正ページがあり、訂正要求を自己提出するために使用できます。修正リクエストが送信されると、そのリクエストは Neustar によって正確性が確認され、処理されます。

GeoIP プロバイダは、できるだけ正確な情報を表示するのに役立ちます。残念ながら、GeoIP の本質的な性質により、GeoIP データが不正確になる場合があります。

用語集

April 12, 2024

- アクション: 不審なイベントに対するクローズドループ応答。アクションは、今後異常なイベントが発生するのを防ぐために適用されます。詳細情報。
- **Cloud Access Security Broker (CASB)**: クラウドサービスコンシューマーとクラウドサービスプロバイダーの間に配置される、オンプレミスまたはクラウドベースのセキュリティポリシー適用ポイント。CASB は、クラウドベースのリソースにアクセスする際に、エンタープライズセキュリティポリシーを組み合わせて介入します。また、組織がオンプレミスインフラストラクチャのセキュリティ制御をクラウドに拡張するのにも役立ちます。
- **NetScaler ADC**（アプリケーション **Delivery Controller**）: ファイアウォールと 1 つ以上のアプリケーションサーバーの間に戦略的に配置された、データセンター内に存在するネットワークデバイス。サーバー間の負荷分散を処理し、エンタープライズアプリケーションのエンドユーザーのパフォーマンスとセキュリティを最適化します。詳細情報。
- **NetScaler ADM**（アプリケーションデリバリ管理）: 一元化されたネットワーク管理、分析、オーケストレーションソリューション。管理者は、1 つのプラットフォームから、スケールアウトアプリケーションアーキテクチャのネットワークサービスを表示、自動化、管理できます。詳細情報。
- **NetScaler ADM** エージェント: NetScaler ADM とデータセンター内の管理対象インスタンス間の通信を可能にするプロキシ。詳細情報。
- **Citrix Analytics**: サービスや製品（オンプレミスとクラウド）にまたがるデータを収集し、実用的な洞察を生成するクラウドサービスです。これにより、管理者はユーザーやアプリケーションのセキュリティ脅威にプロアクティブに対処し、アプリのパフォーマンスを向上させ、継続的な運用をサポートできます。詳細情報。
- **Citrix Cloud**: 任意のクラウドまたはインフラストラクチャ（オンプレミス、パブリッククラウド、プライベートクラウド、ハイブリッドクラウド）上の Citrix Cloud Connector を介してリソースに接続するプラットフォーム。詳細情報。
- **NetScaler Gateway**: リモートアクセスインフラストラクチャを統合して、データセンター、クラウド、または SaaS として提供されるすべてのアプリケーションにわたってシングルサインオンを提供する統合リモートアクセスソリューションです。もっと詳しく知る。
- **Citrix Hypervisor**: アプリケーション、デスクトップ、およびサーバーの仮想化インフラストラクチャ向けに最適化された仮想化管理プラットフォームです。詳細情報。
- **Citrix Workspace** アプリ（旧称 Citrix Receiver）: スマートフォン、タブレット、PC、Mac など、あらゆるデバイスからアプリケーション、デスクトップ、およびデータへのシームレスで安全なアクセスを提供するクライアントソフトウェアです。詳細情報。
- **DLP (Data Loss Prevention)**: ファイル、電子メール、パケット、アプリケーション、データストアなどのオブジェクトに含まれる情報を分類するための一連のテクノロジーと検査手法を記述したソリューションで

す。また、オブジェクトはストレージ内、使用中、またはネットワーク上に存在することもできます。DLP ツールは、ログ、レポート、分類、再配置、タグ付け、暗号化などのポリシーを動的に適用できます。DLP ツールは、エンタープライズデータ権利管理保護を適用することもできます。詳細情報。

- **DNS (**ドメインネームシステム**)**: インターネットドメイン名を検索し、インターネットプロトコル (IP) アドレスに変換するために使用されるネットワークサービス。DNS は、エンティティの物理的な場所に関係なく、ユーザーが指定した Web サイト名を、マシンが提供する IP アドレスに対応付けて、Web サイトを特定します。
- データ処理: データソースから Citrix Analytics にデータを処理する方法です。詳細情報。
- データソース: Citrix Analytics にデータを送信する製品またはサービス。データソースは内部でも外部でもかまいません。[もっと詳しく] /en-us/citrix-analytics/data-sources.html)。
- データのエクスポート: Citrix Analytics からデータを受け取り、洞察を提供する製品またはサービス。詳細情報。
- 検出されたユーザー: 組織内でデータソースを使用しているユーザーの総数。詳細情報。
- **FQDN**（完全修飾ドメイン名）: 内部（StoreFront）および外部（NetScaler ADC）アクセス用の完全なドメイン名。
- 機械学習: 明示的にプログラムされずに知識を抽出するデータ分析テクノロジーの一種。アプリケーション、センサー、ネットワーク、デバイス、アプライアンスなど、さまざまなソースからのデータが、機械学習システムに入力されます。システムはデータを使用し、アルゴリズムを適用して独自のロジックを構築し、問題の解決、洞察の導出、または予測を行います。
- **Microsoft Graph** セキュリティ: 顧客のセキュリティと組織のデータをつなぐゲートウェイ。アクションを実行する必要がある場合に、確認しやすいアラートと修復オプションを提供します。詳細情報。
- パフォーマンス分析: 組織全体のユーザーセッションの詳細を可視化するサービスです。詳細情報。
- ポリシー: ユーザーのリスクプロファイルにアクションを適用するために満たす一連の条件。詳細情報。
- リスク指標: 組織が特定の時点で抱えているビジネスリスクへのエクスポージャーのレベルに関する情報を提供するメトリック。詳細情報。
- リスクスコア: あらかじめ決められた監視期間中に、ユーザーまたはエンティティが IT インフラストラクチャにもたらすリスクの総レベルを示す動的な値です。詳細情報。
- リスクタイムライン: ユーザーまたはエンティティのリスクの高い行動を記録することで、管理者はリスクプロファイルを精査し、データ使用量、デバイス使用量、アプリケーション使用状況、場所の使用状況を把握できます。詳細情報。
- 危険なユーザー: 危険な行動をとった、または危険な行動を示したユーザー。詳細情報。
- セキュリティ分析: セキュリティ監視や脅威ハンティングなど、説得力のあるセキュリティ成果を達成するために使用されるデータの高度な分析。詳細情報。
- **Secure Private Access**: シングルサインオン、リモートアクセス、コンテンツ検査を、エンドツーエンドのアクセス制御のための単一のソリューションに統合するサービスです。詳細情報。

- **Splunk**: Citrix Analytics からインテリジェントなデータを受け取り、潜在的なビジネスリスクに関する洞察を提供する SIEM（セキュリティ情報およびイベント管理）ソフトウェア。詳細情報。
- **UBA**（**User Behavior Analytics**）: ユーザーのアクティビティと行動をピアグループ分析と組み合わせてベースライン化し、潜在的な侵入や悪意のあるアクティビティを検出するプロセス。
- **Watchlist**: 管理者が疑わしいアクティビティを監視したいユーザーまたはエンティティのリスト。詳細情報。