新機能

Citrix の目標は、利用可能になった時点で Citrix Analytics のお客様に新機能と製品アップデートを提供することです。新しいリリースはより多くの価値を提供するため、アップデートを遅らせる理由はありません。

お客様にとって、このプロセスは透過的です。最初のアップデートは Citrix の内部サイトにのみ適用され、その後、段階的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提供することで、製品の品質を確保し、可用性を最大化するのに役立ちます。

April 15, 2024

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、必要な期間でスケジュール設定できるようになりました。この新機能により、対象ユーザーには必要なグラフィカル情報のみが提供されます。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。

January 29, 2024

Workspace Appステータスフィールドの更新

- **セルフサービス検索**: 新しく導入された **Workspace App status** フィールドを **Citrix Apps and Desktops** データソースに利用することで、Workspace Appバージョンのサポートステータスを検索するクエリを実行できるようになりました。
- **ユーザー**: **Workspace App Status** 列は削除されました。

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

January 25, 2024

CAS UI の不整合が解消されました

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不同に表示されていたイベントが、正しく表示されるようになりました。
- デフォルトの列が更新されました。

January 24, 2024

SIEM環境における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、以下が含まれるようになりました。

- IPアドレスのインサイト
- Citrix Virtual Apps and Desktops™ および Citrix DaaS (旧称 Citrix Virtual Apps and Desktops service) のロケーションインサイト

これらの新しい機能強化により、組織のデータへのアクセスに使用されたクライアントの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るようになります。

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。

December 01, 2023

週次メールおよび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**機能を使用すると、システムアラートのカスタム配布リスト受信者を構成できます。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 - 新しいアクティブユーザー数時間フィルターと概要セクションの更新

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 を有効にしているデータソースを考慮して、特定の期間における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、組織内のユーザー総数と、現在ログオンしているアクティブユーザーおよび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」(/ja-jp/security-analytics/users-dashboard.html)を参照してください。

強化されたカスタムレポート

- Citrix Analytics for Securityで利用可能な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。カスタムレポートは、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するのに役立ちます。
- セルフサービス検索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メトリックのカバー、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」(/ja-jp/security-analytics/create-custom-report.html)を参照してください。

November 30, 2023

Citrix AnalyticsにおけるすべてのShareFile機能の削除

以下のShareFile検出機能は削除されました。

- 共有リンク
- 関連するリスクインジケーター
- 発生を伴うポリシー
- コンテンツコラボレーションデータエクスポート構成
- コンテンツコラボレーションレポート
- 検索上のコンテンツコラボレーションデータソース
- コンテンツコラボレーション保存済み検索
- コンテンツコラボレーションデータソース。

これらの機能が削除されると、リスクスコアとユーザータイムラインに一時的な不整合が生じる可能性があります。その他のCitrix Analyticsの機能はすべて変更ありません。

ShareFile.com から、ShareFile がセキュリティコントロールへのアクセスを直接簡素化する方法を学びましょう。

September 22, 2023

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

Citrix Secure Browserデータソースのリスクインジケーターを作成して、Secure Browser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、(/ja-jp/security-analytics/custom-risk-indicators.html)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機能強化

SIEMデータエクスポートを有効にすることで、週次メールが強化され、組織のセキュリティ体制に関するより深い洞察が得られ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、ユーザーに関する幅広いイベントを発見できるようになりました。週次メールには、以下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環境におけるデータ消費のステータスが表示されます。
- データエクスポートの消費状況に基づいたデータエクスポートの推奨事項。

詳細については、(/ja-jp/security-analytics/weekly-email.html)を参照してください。

メールにおけるカスタム管理者の通知設定の利用

Citrix Analytics for Securityは、Citrix Cloudでカスタム管理者が設定した通知設定を尊重するようになりました。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るようになります。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活用されます。

詳細については、(/ja-jp/security-analytics/manage-security-admins.html)を参照してください。

July 04, 2023

セルフサービス検索とカスタムインジケーターにおけるOR演算子のサポート

OR演算子が、**セルフサービス検索**および**カスタムリスクインジケーター**機能で利用可能になりました。**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ー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ている演算子」を参照してください。

June 15, 2023

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重要な情報を提供します。VDAクリップボードイベント属性は、セルフサービス検索およびカスタムリスクインジケーターワークフローでも利用できます。

- **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詳細の確認ができます。
- **カスタムリスクインジケーター**: 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利用できます。これらのイベントのキー/値ペアを使用して、カスタムインジケーターのトリガーを設定し、アクションを含む自動ポリシーをセットアップできます。

セキュリティ監視のためのクリップボード場所メタデータ収集ポリシーを使用して、クリップボードテレメトリとクリップボードログのCitrix Analytics for Securityへの送信を有効にできます。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て無効にし、VDAからのデータ収集を停止します。

詳細については、「Citrix DaaSのクリップボードテレメトリを有効にする」を参照してください。

June 14, 2023

Citrix Analytics for Securityにおけるセッションレコーディングのアプリライフサイクルおよびレジストリイベントの利用可能性

セッションレコーディングからの以下の**アプリライフサイクル**および**レジストリ**イベントが、Citrix Analytics for Securityで利用可能になりました。

- Citrix.EventMonitor.RegistryChange
- Citrix.EventMonitor.SessionLaunch
- Citrix.EventMonitor.SessionEnd
- Citrix.EventMonitor.Clipboard
- Citrix.EventMonitor.FileTransfer

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

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

June 08, 2023

修正された問題

- Citrix Analytics for Securityに送信されるセッションログオンイベントの一部には、ユーザー名がありません。このため、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。また、**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場合、アクセス保証IP登録組織チャートで合計ログオン数がゼロ以外であっても、一意のユーザー数がゼロになることがあります。この問題は修正されました。
- Apps and Desktopsのセルフサービス検索において、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ディメンションには、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、Delivery Groupの名前が入力され、管理者を誤解させる可能性があります。App-Nameディメンションは、App.Start/App.Endイベントのクエリに役立ちます。これは、起動されているアプリケーションを指すためです。詳細については、「Apps and Desktopsのセルフサービス検索」を参照してください。この問題は修正されました。
- 組織が**アジア太平洋南部**のホームリージョンで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。この問題は修正されました。
- Citrix WorkspaceアプリとCitrix Receiverクライアントの一部のバージョンは、特定のイベントをCitrix Analyticsに送信しません。そのため、Citrix Analyticsはこれらのイベントに関するインサイトを提供したり、リスクインジケーターを生成したりできません。この問題は修正されました。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に送信されますか？」を参照してください。

May 29, 2023

Splunk用Citrix AnalyticsアドオンがSplunk Cloud Platformで利用可能に

Citrix AnalyticsのSplunk統合は、Splunk用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、このアドオンはSplunk Enterpriseレイヤーへのインストールのみがsplunkによって検証されており、顧客はオンプレミスのSplunk環境内でアドオンを構成する責任がありました。最新バージョン2.1.2では、このアドオンはSplunk CloudとのSplunkプラットフォーム互換性が追加されました。IDMを使用する**Classic**インスタンスまたは**Victoria**インスタンスを使用している顧客は、このプラットフォーム互換性の強化を利用できます。現在、顧客はSplunk統合を容易にするためにアドオンの展開を検討する際に、Splunk EnterpriseまたはSplunk Cloudのいずれかを選択する柔軟性があります。

詳細については、「Splunk Integration」を参照してください。

SIEMでのセッション記録イベント

セッション記録イベントを、Apps and Desktopsの**Risk Insight**イベントおよび**Data Source**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**ページのデータエクスポートステージで見つけることができます。

詳細については、「Policies and Actions」を参照してください。

May 24, 2023

エンドユーザーへの通知グローバルアクション

Citrix Analyticsの**ポリシーとアクション**機能は、組み込みまたはカスタムのリスクインジケータートリガーと組み合わせることができる**エンドユーザーへの通知**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、エンドユーザーのみにメール通知を生成する**エンドユーザーへの通知**アクションを含むポリシーを作成できます。このアクションは、承認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アカウントでの疑わしい動作について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のユースケースに使用できます。管理者は、特定のシナリオに応じてメールの本文と件名をカスタマイズできます。

詳細については、「Notify End User」を参照してください。

May 04, 2023

テストイベントの生成

テストイベント生成機能は、顧客が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ました。以前は、管理者がこの統合をテストする必要がある場合、Citrix Analyticsによってイベントが生成され、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、ダミーイベントをSIEM環境に送信し、提供されたクエリを使用してCitrix Analytics SIEM統合が期待どおりに設定されているかを確認できます。これは、障害点を特定するのに役立つため、中断されたデータフローのデバッグを試みている管理者にも役立ちます。

詳細については、「Test Event Generation」を参照してください。

SIEMメールアラートの生成

SIEM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、または中断を示す可能性のあるアクティビティに対してシステムアラートを送信します。このメールは、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でのみ実行された場合、データフローの中断につながる可能性があります。このアラートには、パスワードリセットが実行された時刻が含まれているため、データフローを正常に戻すのがはるかに簡単になります。
2. **SIEMデータエクスポートアラート - データフロー停止**

このメールは、顧客がデータフローの中断に直面するたび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**付きの**データエクスポートサマリー**タブを利用して、データフローを迅速に正常に戻すための重要な時間です。
- **7日以上** - 各顧客のトピックに対するKafkaの保持ポリシーは7日間であり、一部のセキュリティ関連データ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復元するために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** - これは、顧客がセキュリティ関連データに問題があり、Citrix AnalyticsからSIEM環境へのデータフローの復元に直ちに注意を払う必要があることを意味します。

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。

April 13, 2023

修正された問題

Windows Citrix Workspace™ Appは、Citrix Workspace Appバージョン2203以降のバージョンから、空のファイル名、パス、および形式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、およびダウンロードファイル形式の列にNA値が表示されます。この問題は現在修正されています。

March 31, 2023

Citrix Analytics for Securityにおけるセッション記録イベント

Citrix Apps and Desktopsに、セッション記録ベースのイベントを特定および評価するのに役立つ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、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**カスタムリスクインジケーター**ページと**セルフサービス検索**ページでも確認できます。

- **セルフサービス検索**: これらのイベントを属性の詳細とともに表示できます。
- **カスタムリスクインジケーター**: これらのイベントタイプを使用して、カスタムインジケーターを構成できます。 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App Protectionイベント

Citrix Apps and Desktopsデータソースの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**ページでも利用できます。

- **セルフサービス検索**: **AppProtection.ScreenCapture**の結果をすべての属性の詳細とともに表示できます。
- **データエクスポート**: データエクスポートセクションで**AppProtection.ScreenCapture**イベントタイプを表示できます。**設定 > データエクスポート > 構成 > エクスポートするデータイベ**

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**Apps and Desktops**を選択します。

Session.Logonイベントの新しい属性である**App Protection Policies**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るフィールド」を参照してください。

March 30, 2023

カスタムロールのサポート

管理者は、Active DirectoryまたはAzure Active Directoryのグループを使用してカスタムロールに追加したり、Citrix Analytics for SecurityのOkta統合を設定したりできます。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管理するための合理化されたアプローチが可能になります。

管理者をActive DirectoryまたはAzure Active Directoryに正常に追加した後、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、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UIは、以下の変更で強化されました。

- **概要タブ**: 概要タブには、SIEMイベントメトリック、データソースのオンボーディングステータス、および以下のシナリオにおけるデータ消費ステータスが記述されています。
  - **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を提供します。
  - **SIEM消費に利用可能なイベント**: SIEM環境に送信されているインサイトの数を提供します。
  - **SIEMによるデータ消費**: データ消費ステータスを提供します。
- **構成タブ**: **構成**タブには、アカウント設定、SIEM環境設定、およびデータイベント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、SIEM統合の設定と維持を簡素化する**クイックガイド**を利用できるようになりました。**データエクスポートクイックガイド**リンクは、**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。

March 24, 2023

ユーザープロファイル表示の変更

アプリケーション、場所、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**ページでは利用できません。Active Directoryから取得される以下のユーザー情報は引き続き利用可能です。

- 役職
- 住所
- メールアドレス
- 電話番号
- ロケーション
- 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オートサジェストの削除

テナントの履歴データに基づいたディメンションのオートサジェスト機能は、以下のページで非推奨になりました。

- セルフサービス検索
- カスタムリスクインジケーター

ただし、**Event-Type** や **Clipboard-Operations** などのディメンションの静的サジェストは、検索ボックスで引き続き利用できます。

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。

March 21, 2023

オンプレミスStoreFront™データソースのオンボーディングを支援する推奨パネル

データソースページに新しい**推奨**パネルが導入されました。**データソース**ページの**推奨**パネルは、オンプレミスStoreFrontデータソースのオンボーディングの重要性についてユーザーに情報を提供します。これにより、ユーザーはオンプレミスStoreFrontデータソースを簡単にオンボーディングでき、利用可能なすべてのデータソースのオンボーディングを確認および保証するためのオプションも提供されます。

詳細については、StoreFront展開への接続を参照してください。

February 23, 2023

修正された問題

Citrix Apps and Desktop のバージョンが 1912 より大きいオンプレミス Citrix Apps and Desktop 展開で、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のアクションの両方で確認されています。この問題は修正されました。

仮想アプリが一度しか起動されていない場合でも、「アプリとデスクトップのセルフサービス検索」ページに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 クライアントバージョンの Citrix Workspace アプリで発生します。この問題は修正されました。

2022 年 4 月 4 日以降から 2022 年 5 月末までの Secure Private Access サービスからのユーザーイベントが、Citrix Analytics テナントで利用できない場合があります。この問題は修正されました。

February 22, 2023

週次メール通知の機能強化

Citrix Analytics は、組織のセキュリティリスクエクスポージャーを要約するのに役立つ週次メール通知を送信します。週次メール通知は、以下の更新により改善されました。

- ユーザーのリスク分布の表示 - 1 週間の検出されたユーザーの総数、リスクのあるユーザー数、リスクのないユーザー数
- 1 週間に処理されたイベントの総数

- 1 週間にトリガーされたインジケーターの総数
- 1 週間に実行されたアクションの総数
- データ処理のために有効になっているデータソースの総数

詳細については、「週次メール通知」を参照してください。

App.SaaS.File.Download イベントタイプに Download File Format フィールドを追加

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 **Download File Format** 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インジケーターを設定したり、CSV 形式へのエクスポートの一部としてこのフィールドをエクスポートしたりできるようになりました。

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。

ブラウザ派生フィールドの変更

以前は、セルフサービス検索ページには、ブラウザ名とバージョンを表す **Browser**、**Browser Major Version**、および **Browser Minor Version** フィールドがありました。しかし、明確さと正確性を確保するため、これら3つのフィールドは非推奨となり、セルフサービス検索、カスタムインジケーターテンプレート、および Apps and Desktops データソースの CSV ダウンロードで **Browser Name** と **Browser Version** に置き換えられました。

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

February 16, 2023

修正された問題

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、一部のEUおよびAPSのお客様の週次メールが影響を受けていました。その結果、例外により管理者は10通の同一の週次メールを受信していました。例外が発生すると、後続のテナントは週次メールを受信しませんでした。この問題は現在修正されています。

February 03, 2023

欧州連合およびアジア太平洋南部地域で利用可能な Citrix Secure Private Access™ サービスに対するアナリティクスサポート

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されている場合、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。

January 11, 2023

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 フィルタリングの非推奨化により、Citrix Analytics for Security の以下の機能が影響を受けます。

1. Category-Group、Category、URL の Reputation 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利用できなくなりました。
2. 同じデータに依存する Risky website access インジケーターも非推奨となり、お客様に対してはトリガーされません。
3. 既存のカスタムリスクインジケーターで、データフィールド（カテゴリグループ、カテゴリ、URLの評価）を使用しているもの、およびそれに関連するポリシーは、今後トリガーされません。
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、urlcategory、urlcategorygroup、urlcategoryreputationの属性が、以下のダミー値とともにしばらくの間引き続き含まれます。
    - カテゴリおよびカテゴリグループには99999
    - 評価には0

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。

December 27, 2022

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

セルフサービス検索ページで、データソースリストがデフォルトで**アプリとデスクトップ**ではなく**セッション**を反映するように変更されました。また、パフォーマンスデータソースが表示されていなかったため、パフォーマンスセクションがセキュリティセクションの前に移動されました。

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。

December 13, 2022

ユーザーダッシュボードの機能強化

ユーザーダッシュボードは、管理者が組織のセキュリティ体制を監視するのに役立つサマリーとグラフで刷新されました。このビューでは、検出されたユーザー、トリガーされたリスクインジケーター、適用されたアクションの詳細を提供するだけでなく、リスクをより適切に評価するための重要なメトリックの時系列トレンドラインも提供します。管理者は、関心のあるデータをドリルダウンし、適切なコンテキストで関連するダッシュボードに移動して、リスク分析を迅速化できます。

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。

December 05, 2022

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、以下のユーザー詳細が提供されます。

- ユーザーがログオンしたIPアドレスに関連付けられている組織。
- ユーザーがログオンした合計一意のパブリックサブネットとプライベートサブネット。
- ユーザーがプロキシおよびプライベートVPNサービスを使用してログオンした詳細。

これらの追加の詳細を使用することで、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を満たしてい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。

November 18, 2022

修正された問題

- ソースイベントがないにもかかわらず誤ってトリガーされていたジオフェンスインジケーターが修正されました。

November 08, 2022

アクション名の変更

Citrix Analytics for Securityで使用されている一部のアクションは、より明確にするために名前が変更されました。それらのアクションは次のとおりです。

- **管理者への通知** - 管理者への通知
- **ユーザーのロック** - ユーザーアカウントのロック
- **ユーザーのログオフ** - 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を解除する
- **ユーザーの無効化** - 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。

修正された問題

- タイムラインアクションのドロップダウンからオプションを選択すると、 ボタンと ボタンが表示されないため、手動アクションをトリガーできません。この現象は、最新のFirefoxバージョンで発生します。この問題は修正されました。
- Apps and Desktopsデータソースのセルフサービス検索におけるDownload-Device-Typeフィールドで、**HardDrive**、**harddrive**、**HDD**のカテゴリが**Hard Disk Drive**という単一のカテゴリに統合されました。
- Microsoft Graphから同じアラートIDを持つ重複した通知が受信され、重複したリスクイベントが作成されることがありました。この問題を防止するため、アプリケーション内に重複排除メカニズムが実装されました。

October 19, 2022

データ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および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、セキュリティ管理者およびセキュリティ運用 (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) に集約された他のデータソースイベントと関連付ける
- ストレージコスト最適化のために、どのデータイベントをSIEMに流すかを制御する

データイベントは、既存のSIEM統合およびデータコネクタに配信されます。これは、セルフサービスイベント検索ビューで利用可能なものと同等です。

詳細については、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を参照してください。

October 18, 2022

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、ユーザーの仮想セッションを動的に記録できるようになりました。Citrix Analytics for Securityによって特定のユーザーによる危険なアクティビティが検出された場合、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でアクションを設定できます。

詳細については、アクションとはを参照してください。

October 14, 2022

ユーザーリスクインジケーターのフィードバックを提供する

Citrix Analytics for Security管理者は、インジケーターの詳細パネルでフィードバックを提供することにより、ユーザーリスクインジケーターが役立つか役立たないかを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、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、他の管理者と追加のコンテキストを共有できます。追加の結果として、役に立たないリ

スクインジケーターはユーザーのタイムラインから非表示になり、ユーザーリスクスコアが再調整されます。

詳細については、ユーザーリスクインジケーターのフィードバックを提供するを参照してください。

September 26, 2022

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

ジオフェンス設定に**安全な場所**と**危険な場所**のタブが追加されました。

- 安全な場所のジオフェンシングは、定義されたジオフェンスエリア外からのアクセスを特定し、制限するのに役立ちます。
- 危険な場所の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、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の両方が、独自の事前設定されたカスタムリスクインジケーターによってサポートされています。

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。

修正された問題

- Citrix Cloud APIは、メール本文に**顧客名**を表示します。現在、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**を表示します。
- Citrix Gatewayデータソースカードは、**Citrix Analytics for Security**と**Citrix Analytics for Performance™**で共通です。データ処理は常にCitrix Analytics for Securityエンドポイントを呼び出しており、**Citrix Analytics for Performance**のエンタイトルメントのみを持つお客様にとっては機能していませんでした。
- Citrix Cloudから複数のエンタイトルメントメッセージが同時に受信されると、Redisキャッシュ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、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を更新するように修正されました。

September 13, 2022

Sharelinkダッシュボードの機能強化

Sharelinkダッシュボードは、概要ビューと詳細ビューで刷新されました。概要ビューには、最もアクティブな共有と最もリスクの高い共有が含まれます。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、コンテンツなどの属性が導入され、管理者により多くの情報が提供されます。管理者は必要に応じてさらにドリルダウンしてフィルタリングし、関心のあるデータを確認するために期間を変更/指定できます。

詳細については、Share Linksダッシュボードを参照してください。

September 09, 2022

Impossible Travel RIの機能強化

Impossible Travelリスクインジケーターは、クライアントIPアドレスの登録組織とルーティングタイプを報告するように強化されました。これらの新しいフィールドは、ユーザータイムラインインジケーターの詳細ビューと、SIEMに送信されるインジケーター詳細の両方で利用できます。

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

August 19, 2022

VDA印刷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印刷イベントは、**セルフサービス検索**および**カスタムリスクインジケーター**ページでも利用できます。

- **セルフサービス検索**: VDA.Printの結果を、そのすべての属性の詳細とともに表示できます。
- **カスタムリスクインジケーター**: EventHubを介してVDA印刷テレメトリ用の新しいイベントが提供され、カスタムインジケーター内でも利用できます。これらのイベントのキー/値ペアを使用して、カスタムインジケーターのトリガーを設定できます。

印刷テレメトリを有効にし、印刷ログをCitrix Analytics for Securityに送信するには、レジストリキーを作成し、VDAを構成する必要があります。これらの印刷ログは、プリンター名、印刷ファ

イル名、合計印刷部数など、印刷アクティビティに関する重要な情報を提供します。セキュリティ管理者として、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。

詳細については、「Citrix DaaSの印刷テレメトリを有効にする」を参照してください。

August 18, 2022

修正された問題

- Apps and Desktopsのセルフサービス検索および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、ダウンロードされたCSVファイルにWorkspaceアプリのバージョン値が**NA**（利用不可）として入力されていましたが、ページビューでは利用可能でした。この問題は修正されました。

August 17, 2022

ポリシーごとのエンドユーザーメールのカスタマイズ

ポリシーごとにエンドユーザーに送信されるメールの内容を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要求アクションまたはユーザーアカウントに対する中断アクション（ユーザーのログオフやユーザーのロックなど）を含むポリシーを作成した場合、ポリシー適用時にエンドユーザーに送信されるメールの内容をカスタマイズできます。

ポリシーごとのエンドユーザーメールのカスタマイズの詳細については、「ポリシーとアクション」を参照してください。

August 11, 2022

「**Access assurance – Geolocation**」に関する新しい質問が**FAQ**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

- **View All Notifications**ボタンをクリックすると、管理者はタイプミスのある週次メールリンク `https://citrix.cloud.com/notifications` にリダイレクトされていました。

June 17, 2022

新しい有償エンタイトルメントではデータ処理がデフォルトで有効になります

以前は、Citrix Analytics for Security の新しい有償エンタイトルメントを持つお客様は、特定のデータソースのデータ処理を開始するために、そのデータソースのサイトカードでデータ処理を有効にする必要がありました。

このリリースでは、Citrix Analytics for Security の新しい有償エンタイトルメントがプロビジョニングされると、以下のCitrix Cloudサービスでデータ処理がデフォルトで有効になります。

- シトリックス セキュア プライベート アクセス
- シトリックス コンテンツ コラボレーション™
- シトリックス DaaS

詳細については、はじめにを参照してください。

June 09, 2022

修正された問題

- Azure AD Identity Protection および Microsoft Defender for Endpoint によって生成された Microsoft Graph のリスクインジケーターが、Security Analytics で複数回表示される場合がありました。この問題は修正されました。

June 02, 2022

修正された問題

- 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。
- 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誤って表示されていました。この問題は、実際の値がKB単位であったにもかかわらず、UIがその値をバイトとして処理したため、ユーザーに誤った値が表示されたために発生しました。

May 24, 2022

Content Collaboration、Citrix DaaS、Citrix Virtual Apps and Desktops、およびGatewayデータソース向けの不可能トラベルリスクインジケーターの導入

ユーザーが、経過時間内に移動するには遠すぎる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トラベルシナリオとして検出し、**不可能トラベル**リスクインジケーターをトリガーします。不可能トラベルリスクインジケーターの詳細については、次の記事を参照してください。

- Citrix Content Collaborationリスクインジケーター
- Citrix Gateway リスクインジケーター
- Citrix Virtual Apps and DesktopsおよびCitrix DaaSのリスクインジケーター

May 17, 2022

Virtual Apps and DesktopsはApps and Desktopsに名称変更されました

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において、すべてのVirtual Apps and Desktopsのラベルが、ブランド変更された製品名に合わせてApps and Desktopsに更新されました。

たとえば、ページでは、Virtual Apps and DesktopsのラベルがApps and Desktopsに名称変更されています。

Apps and Desktopsラベルは、組織内のCitrix on-premises Citrix Virtual Apps and DesktopsとCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）の両方を表します。

修正された問題

Citrix Analytics は、Citrix Cloud アカウントに関連付けられている Citrix DaaS Cloud Monitor または Director サイトを自動的に検出することはありません。

April 05, 2022

新機能

Secure Workspace Access が Secure Private Access に名称変更されました

Analytics のダッシュボードとレポートでは、ブランド変更された製品名に合わせて、すべての **Secure Workspace Access** ラベルが **Secure Private Access** に更新されました。

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** ラベルが **Secure Private Access** に名称変更されています。

March 21, 2022

修正された問題

- **リスクインジケーターの作成**ページで、検索クエリの以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提案が機能しません。

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



March 10, 2022

新機能

管理者へのメール通知の機能強化

- **管理者への通知**アクションのメール通知で、トリガーされたポリシーに関連付けられている複数のリスクインジケーター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インジケーターの名前、重大度レベル、およびトリガー日を表示できます。
- をクリックすると、Citrix Analytics の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インジケーターが表示されます。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インジケーターも表示できます。

管理者へのメール通知機能の強化(/en-us/citrix-analytics/media/notify-email-enhancements.png)

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。

修正された問題

Citrix Analytics は、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ユーザーイベントが表示されません。また、Secure Workspace Access データソースのカスタムリスクインジケーターを作成することもできません。

March 03, 2022

新機能

エンドユーザー応答要求を手動で適用する

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 アクションを適用できました。 このリリースでは、ユーザータイムラインの リストからアクションを選択し、リスクインジケーターにこのアクションを手動で適用できます。

アクションとアクションを手動で適用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。

エンドユーザー応答要求を手動で適用する(/en-us/citrix-analytics/media/request-user-manual-action.png)

ポリシーのエンドユーザー応答要求の機能強化

アクションを含むポリシーを作成すると、次の機能強化が表示されます。

- 次のアクションとして を選択すると、デフォルトのメール配布リストと作成済みのメール配布リストを表示して、そこから選択できるようになりました。

  管理者配布リストに通知(/en-us/citrix-analytics/media/req-end-user-notify-admin.png)

- Citrix Content Collaboration または Citrix Virtual Apps and Desktops および Citrix DaaS のアクションのいずれかを次のアクションとして選択できるようになりました。以前は、グローバルアクションまたはCitrix Gatewayアクションのいずれかしか選択できませんでした。

  フォローアップアクション(/en-us/citrix-analytics/media/req-end-user-follow-up-actions.png)

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。

February 23, 2022

新機能

リスクインジケーターの推奨アクション

Citrix Analytics は、ユーザーに対して次のリスクインジケーターがトリガーされたときに、**管理者への通知**、**ウォッチリストへの追加**、**ポリシーの作成**などのアクションを適用することを提案します。

- 異常な認証失敗 (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 および 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インジケーターを選択すると、**推奨アクション**セクションにすべての提案されたアクションが表示されます。

たとえば、異常な認証失敗のリスクインジケーターでは、次の推奨アクションを表示できます。

推奨アクション(/en-us/citrix-analytics/media/recommended-action-rn.png)

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、推奨リスト外の適切なアクションを、リスク分析に基づいて実行することもできます。

修正された問題

- 組織が**アジア太平洋南部**ホームリージョンでCitrix Cloudにオンボーディングされている場合、Citrix Analyticsは認証データソースからユーザーイベントを受信しない可能性があります。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場合があります。この問題は修正されました。

February 17, 2022

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改善

このリリースでは、以下の変更点があります。

- Citrix WorkspaceアプリクライアントおよびCitrix Monitorサービスからのイベントのデータ収集、関連付け、レポート機能の改善。
- 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、セルフサービス検索、カスタムリスクインジケーター、および全体的なリスク検出に利用できるようになりました。

Content Collaborationにおけるセッションイベントおよびアプリイベント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、ファイル、フォルダー、セッション、共有、およびユーザーイベントに関連する関連フィールドの詳細のみを表示できるようになりました。イベントに適用されないフィールドは削除されます。

たとえば、`File.Copy`イベントの以下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
- 宛先ファイルパス
- ストリームID
- ゾーンID

これらの詳細は、危険な行動に関連付けられたユーザーアカウントのリスク調査と分析に役立ちます。危険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、「コンテンツコラボレーションのセルフサービス検索」を参照してください。

February 10, 2022

新機能

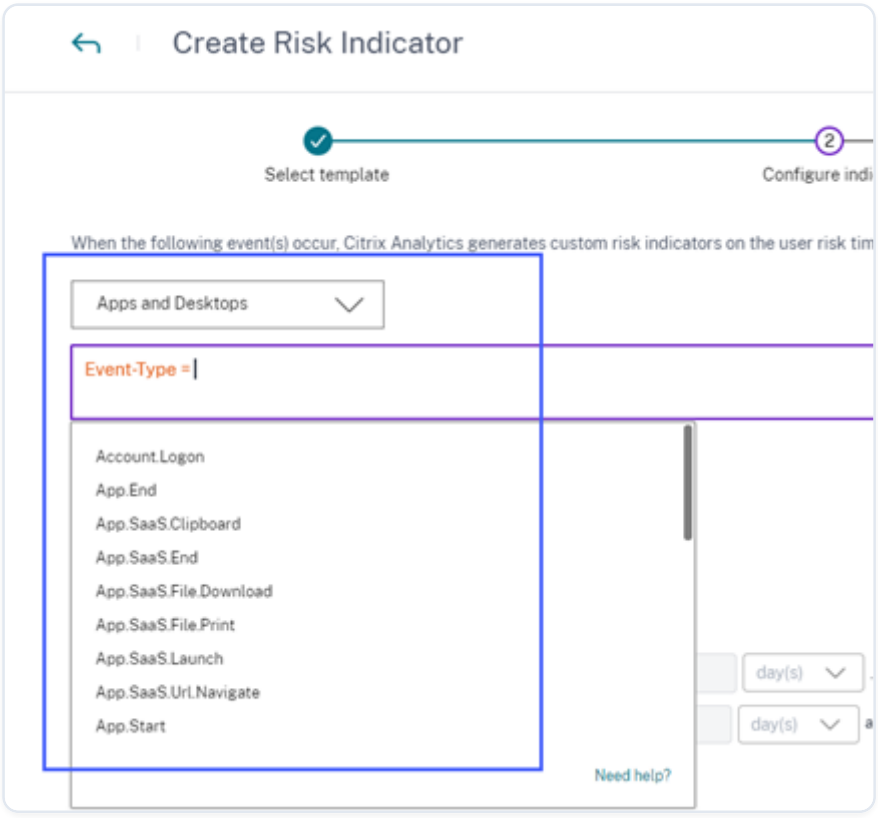
カスタムリスクインジケーターのディメンションに対する自動提案値

カスタムリスクインジケーターページで、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、そのディメンションの値が自動的に表示されます。自動提案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、レコードで利用可能な一致する値が自動提案されます。

ディメンションに対して提案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。

例えば、ディメンション `Event-Type` と代入演算子を選択すると、既知の値が自動提案されます。要件に応じて値を選択できます。

詳細については、「カスタムリスクインジケーター」を参照してください。



February 09, 2022

新機能

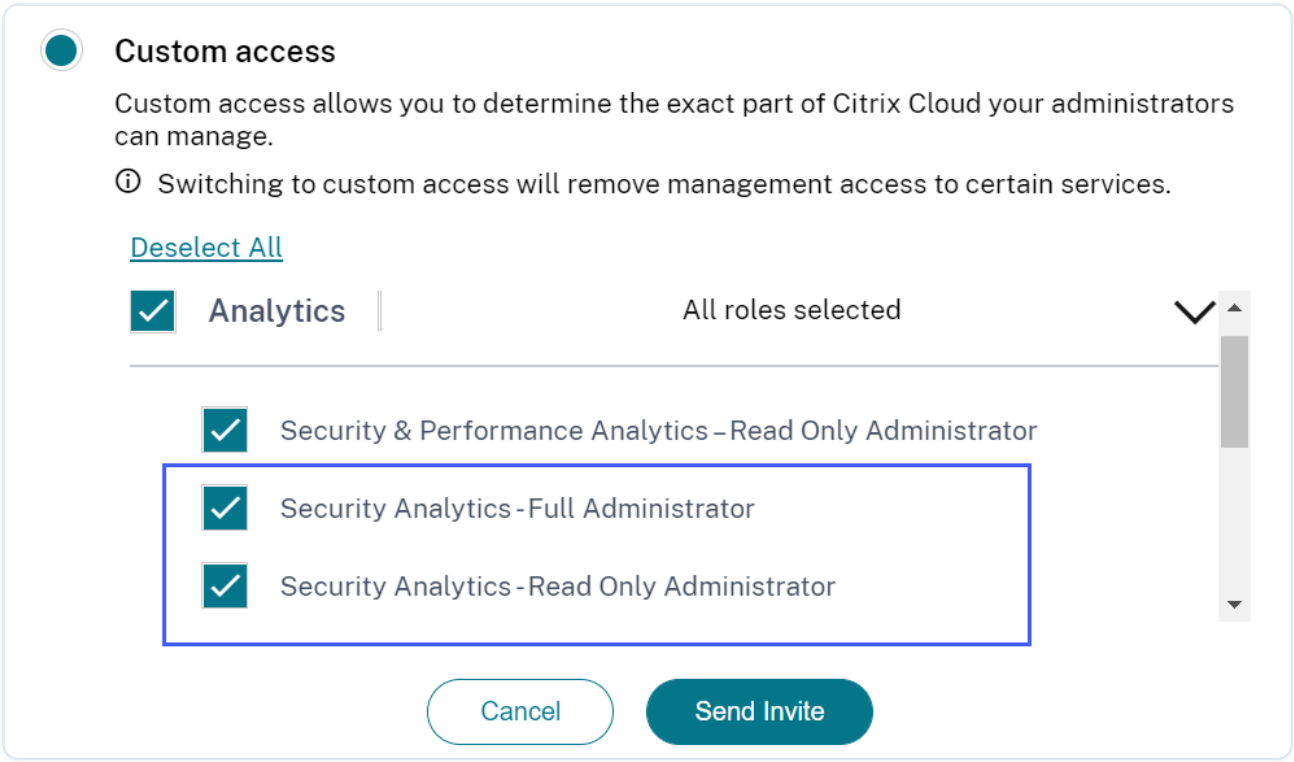
管理者向けの新しいカスタムロール

Citrix Cloudのフルアクセス権限を持つ管理者として、組織内のSecurity Analyticsを管理するために他の管理者を招待できます。招待された管理者には、以下のカスタムロールを割り当てることができます。

- Security Analytics - フル管理者
- Security Analytics - 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のいずれかの権限を付与し、Security Analyticsのさまざまな機能を管理させることができます。

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の管理者ロールを管理する」を参照してください。



カスタムアクセス管理者向けのメール通知のサポート

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Citrix Cloud管理者である場合、以下の通知を受け取ることができます。

- 組織で検出されたセキュリティリスクに関する週次通知。詳細については、「週次メール通知」を参照してください。
- **管理者への通知**アクションが手動で適用された場合、またはポリシーによってトリガーされた場合のリスクインジケーターに関する通知。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。

January 28, 2022

新機能

Content CollaborationおよびGatewayデータソース向けの不審なログオンリスクインジケーターの導入

Citrix Analytics for Securityは、以下のような複数の状況要因に基づいて、不審なユーザーログオンを検出するようになりました。

- ユーザーおよび組織の履歴に関して、場所が異常であると見なされる場合
- デバイスは、ユーザーおよび組織の履歴に関して異常と見なされます。
- ネットワークは、ユーザーおよび組織の履歴に関して異常と見なされます。
- 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、ユーザーが疑わしいコンテキストからログオンすると、リスクインジケーターがトリガーされます。

このリスクインジケーターは、Citrix Content CollaborationおよびCitrix Gatewayデータソースに関連付けられている「異常な場所からのアクセス」リスクインジケーターを置き換えます。「異常な場所からのアクセス」リスクインジケーターに基づいている既存のポリシーはすべて、新しいリスクインジケーター「疑わしいログオン」に自動的にリンクされます。

リスクインジケーターの詳細については、「疑わしいログオン - Content Collaboration」および「疑わしいログオン - Gateway」を参照してください。

リスクインジケーターのスキーマの詳細については、「SIEM 用 Citrix Analytics データ形式」を参照してください。

January 20, 2022

新機能

マイクロソフト アジュール アクティブ ディレクトリ の統合

Azure Active Directory を Citrix Analytics for Security に接続して、次のことを実行できるようになりました。

- 組織のドメインからユーザーの詳細とユーザーグループを Citrix Analytics for Security にインポートします。
- 役職、組織、オフィス所在地、メール、連絡先などの追加情報でユーザープロファイルを充実させ、リスク調査と分析に役立てます。

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

January 18, 2022

新機能

すべてのコンテンツコラボレーションリスクインジケーターにおける共有リンクアクションのサポート

以前は、コンテンツコラボレーションサービスに関連する以下の共有リンクベースのリスクインジケーターに対して、共有リンクアクションである**すべてのリンクを期限切れにする**と**リンクを閲覧専用共有に変更する**を適用できました。

- 匿名による機密共有リンクのダウンロード
- 過剰な共有リンクのダウンロード
- 過剰なファイル共有

このリリースにより、コンテンツコラボレーションサービスに関連する以下のユーザーベースのリスクインジケーターに対して、共有リンクアクションを適用できるようになりました。

- 通常とは異なる場所からのアクセス
- 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
- 過剰なファイルまたはフォルダーの削除
- マルウェアファイルの検出
- ランサムウェア活動の疑い
- 不審な認証失敗

Content Collaborationサービスに関連付けられたカスタムリスクインジケーターに、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インジケーターの詳細については、以下の記事を参照してください。

- ポリシーとアクション
- Content Collaborationのリスクインジケーター
- カスタムリスクインジケーター

SIEMとの統合が一般提供開始

Citrix Analytics for SecurityをSecurity Information and Event Management (SIEM) サービスと統合し、Citrix IT環境からユーザーデータを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関連付け、組織のセキュリティを全体的に把握することができます。

現在、Citrix Analytics for Securityは以下のサービスと統合できます。

- スプランク
- マイクロソフト センチネル
- エラスティックサーチ
- KafkaまたはLogstashベースのデータコネクタを使用したその他のSIEMサービス

詳細については、「Security Information and Event Management (SIEM) の統合」を参照してください。

December 23, 2021

新機能

共有リンクのリスクインジケーターの機能強化

以下の機能強化が行われました。

- **匿名による機密共有リンクのダウンロード**リスクインジケーターを使用してポリシーを作成できるようになりました。
- **匿名による機密共有のダウンロード**リスクインジケーターは、共有リンクのリスクインジケーターとして区別するために、**匿名による機密共有リンクのダウンロード**に名称変更されました。
- **過剰なダウンロード**リスクインジケーターは、共有リンクのリスクインジケーターとして区別し、ユーザーベースの**過剰なファイルダウンロード**リスクインジケーターと区別するために、**過剰な共有リンクのダウンロード**に名称変更されました。

詳しくは、「Citrix 共有リンクのリスクインジケーター」を参照してください。

December 21, 2021

新機能

リスクインジケーターに関する通知をCitrix Cloud管理者以外の管理者に送信する

管理者への通知アクションを使用して、組織内のCitrix Cloud管理者以外の管理者に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、メール配布リストを作成します。メール配布リスト内の管理者は、Citrix Cloudに接続されている外部ドメインから選択するか、メールアドレスを直接使用して選択します。**管理者への通知**アクションを適用する際は、Citrix Cloud管理者以外の管理者を含むメール配布リストを選択します。

詳しくは、「メール配布リスト」を参照してください。

December 20, 2021

新機能

ユーザー応答通知をContent Collaborationユーザーに送信する

Active Directoryユーザーに加えて、Content Collaborationユーザーにも**Request End User Response**アクションを適用できるようになりました。

このアクションは、Citrix AnalyticsがCitrixアカウントで異常なアクティビティを検出した場合に、ユーザーに電子メール通知を送信します。**Request End User Response**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。

Access ControlがSecure Workspace Accessに名称変更されました

Security Analyticsのダッシュボードとレポートでは、ブランド変更された製品名に合わせて、すべての**Access Control**ラベルが**Secure Workspace Access**に更新されました。

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、Access Controlラベルが Secure Workspace Accessに名称変更されています。

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、値が利用可能であるにもかかわらず、利用不可（N/A）と表示されます。たとえば、`Download File Name`、`Session Launch Type`、

および`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、ダウンロードしたCSVファイルではこれらの値が利用不可（N/A）と表示されます。この問題は修正されました。

December 09, 2021

新機能

テンプレートを使用してカスタムリスクインジケーターを簡単に作成

ユースケースに基づいてテンプレートを選択し、カスタムリスクインジケーターを作成できるようになりました。テンプレートは、事前定義されたクエリとパラメータを提供することで、作成をガイドします。これにより、カスタムリスクインジケーターの作成作業が軽減されます。

詳細については、「カスタムリスクインジケーター」を参照してください。

December 07, 2021

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を受信しません。この問題は、2021年9月リリース以降のCitrix Secure Browserで**ホスト名追跡**ポリシーが表示されず、Citrix Analytics for Securityと統合するために有効にできないために発生します。この問題は修正されました。

December 02, 2021

新機能

マルウェアファイル検出リスクインジケーター

Content Collaboration でユーザーが感染ファイルをアップロードしたときに、アラートを受け取れるようになりました。

このリスクインジケーターは、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たファイルを検出します。ファイル所有者、ウイルス名、ファイル場所など、悪意のあるファイルの詳細を可視化します。

マルウェアファイル検出リスクインジケーターに関連付けられているリスクファクターは、ファイルベースのリスクインジケーターです。

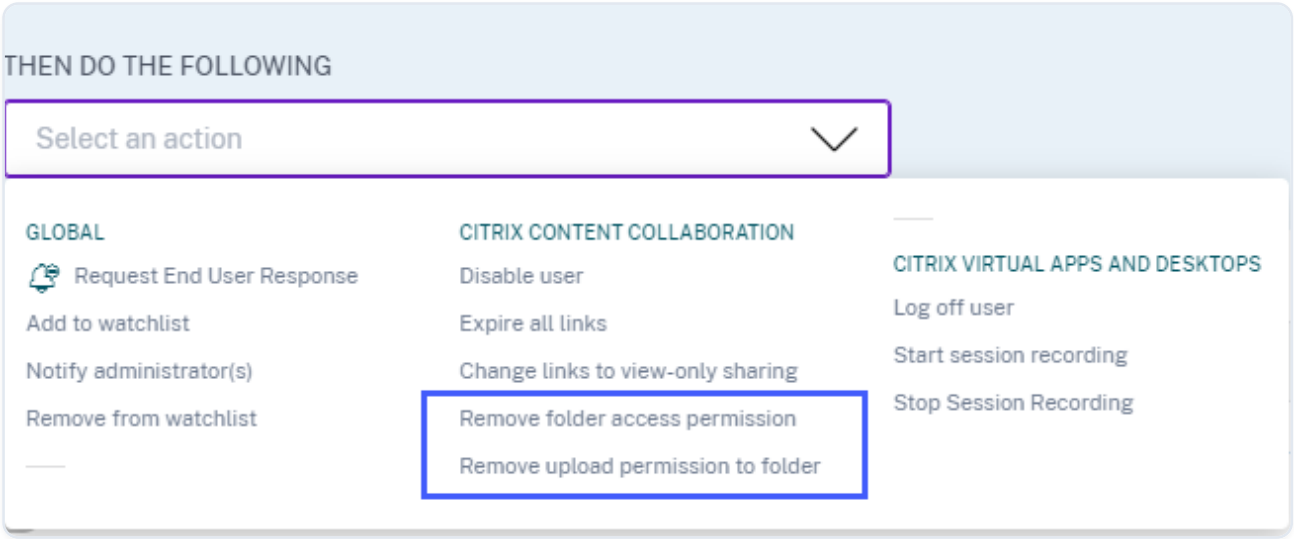
リスクインジケーターと適用できるアクションの詳細については、「マルウェアファイル検出リスクインジケーター」を参照してください。

Content Collaboration データソースの新しいアクション

ユーザーに対して**マルウェアファイル検出**リスクインジケーターがトリガーされた場合、次のアクションを適用できます。

- **フォルダーアクセス権を削除する**。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なくなります。
- **フォルダー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なくなります。

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。



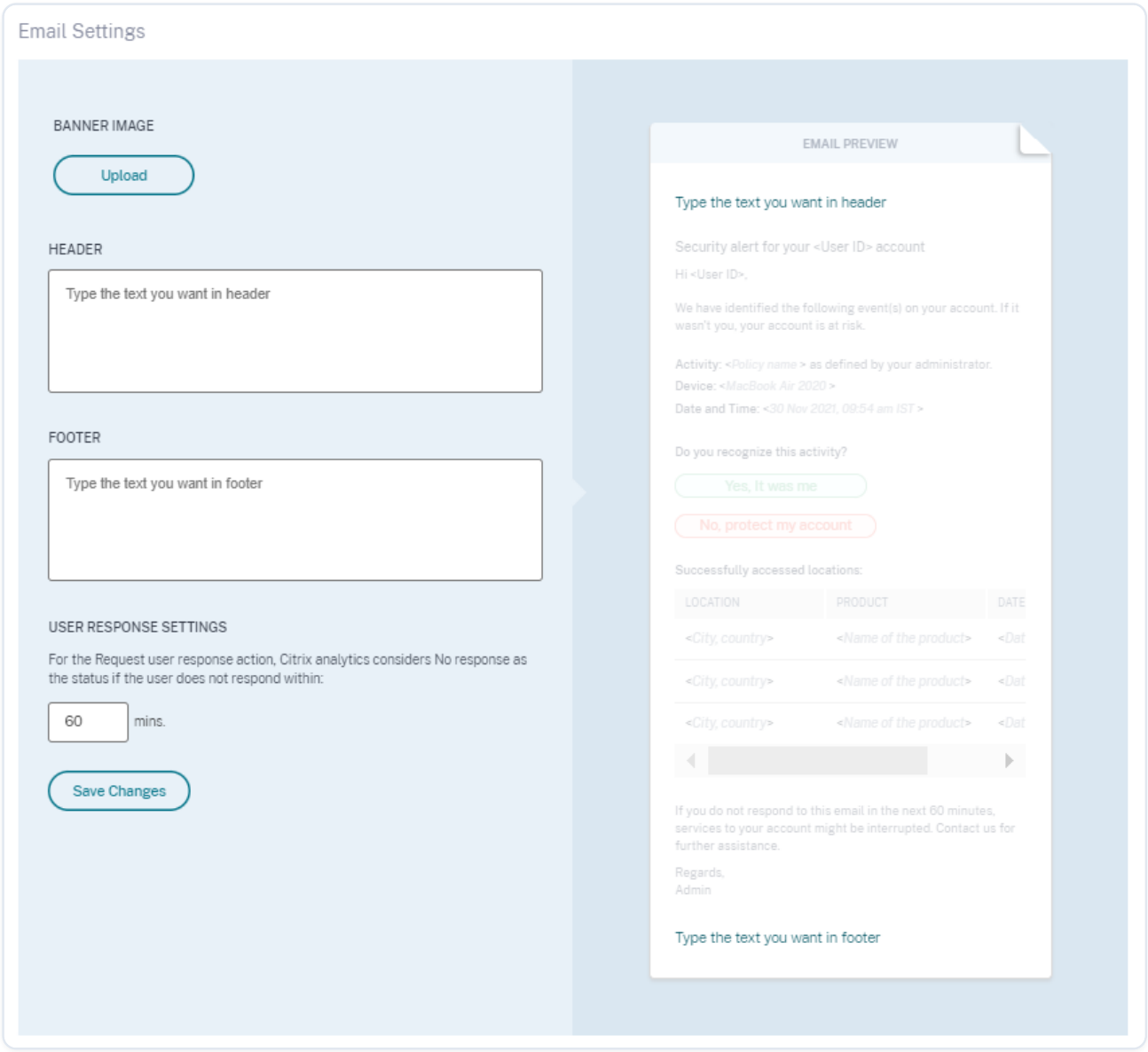
November 29, 2021

新機能

ユーザー通知のメール設定の機能強化

管理者として、ユーザー応答メールテンプレートにバナー画像、ヘッダー、フッター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、ユーザーのメールへの注意と応答を増加させます。

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。



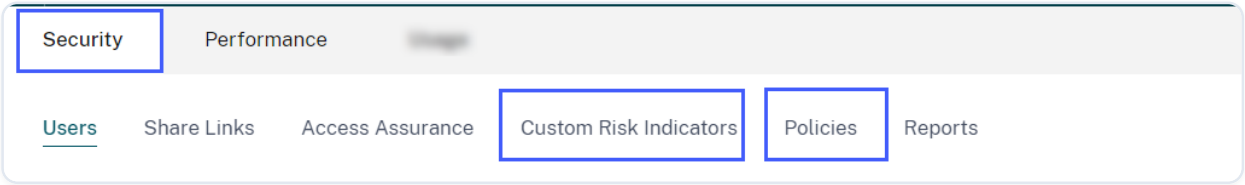
November 26, 2021

新機能

カスタムリスクインジケーターとポリシーメニューの変更

以下の機能のナビゲーションリンクが更新されました。

- カスタムリスクインジケーター: この機能を使用するには、 > をクリックします。
- ポリシー: この機能を使用するには、 > をクリックします。



November 25, 2021

新機能

セキュリティ情報およびイベント管理 (SIEM) 統合の機能強化

> **注**
>
> この統合はプレビュー版です。

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

- マイクロソフト センチネル
- Kibana などの視覚化サービス、および 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 サービス内の異なるログからデータを関連付け、分析し、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復するのに役立ちます。

詳しくは、「セキュリティ情報およびイベント管理 (SIEM) の統合」を参照してください。

November 09, 2021

修正された問題

- 一部のテナントで、ユーザーポリシーが機能していません。この問題は、仮想アプリのアラートのドメインに空の文字列値がある場合に発生しました。この問題は修正されました。

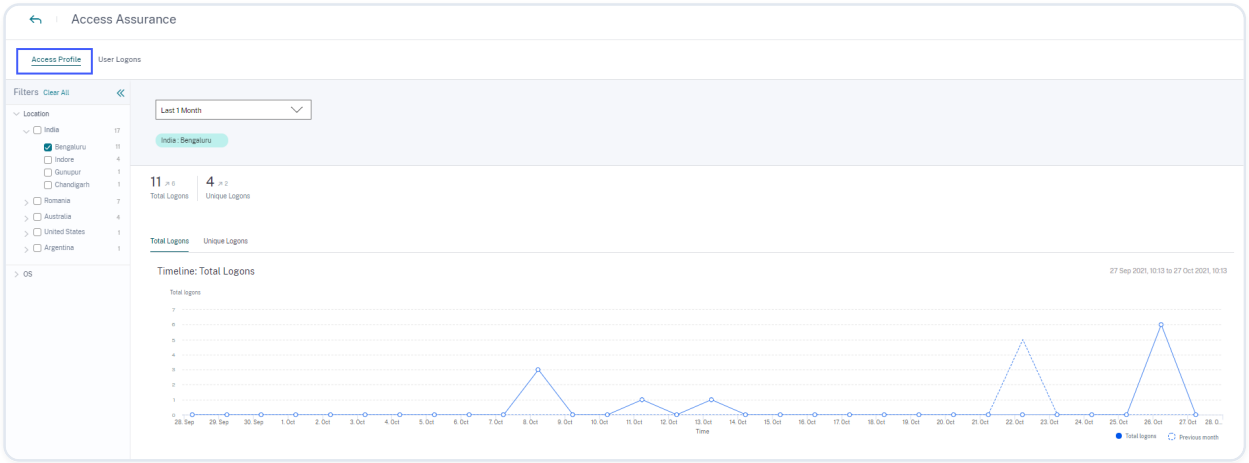
November 02, 2021

新機能

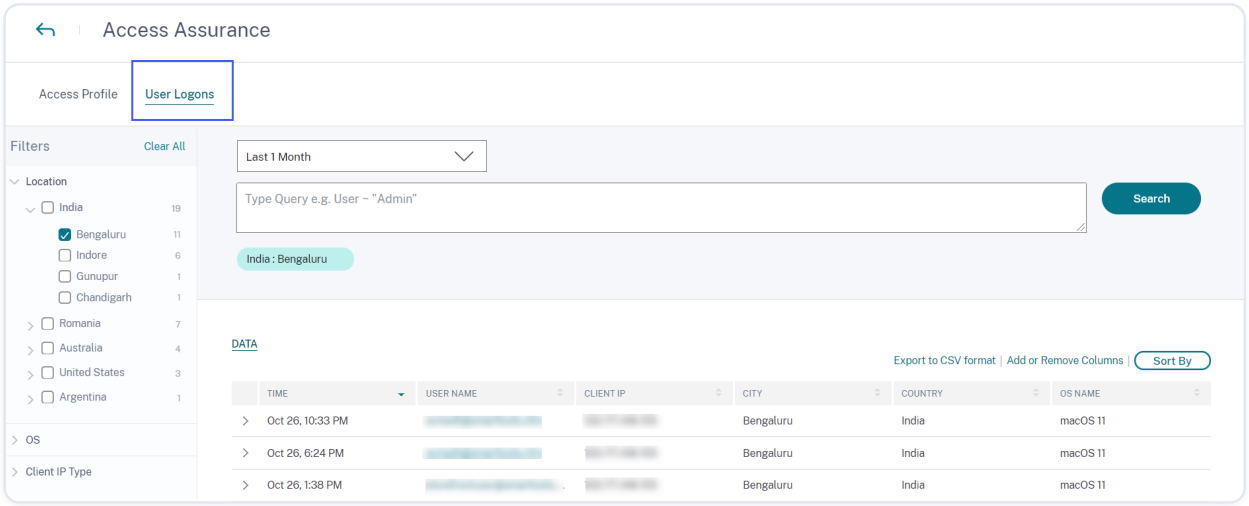
Citrix Virtual Apps and Desktops および Citrix DaaS ユーザーのアクセスプロファイルとログオンの詳細を表示する

Access Assurance Location ダッシュボードで、仮想アプリと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の詳細を表示できます。この情報は、脅威の調査と分析に役立ちます。

- **アクセスプロファイル**ページには、選択した場所からのユーザーアクセス概要が表示されます。合計ユーザーとユニークユーザーのログオン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、選択した場所からの仮想アプリ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。

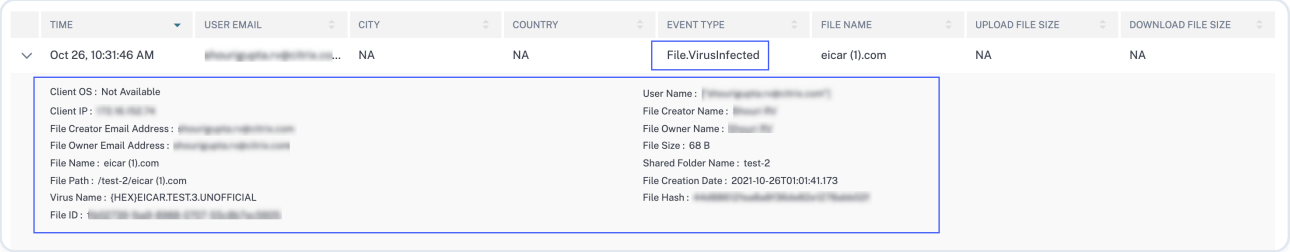


詳細については、「」を参照してください。(/ja-jp/security-analytics/access-assurance-dashboard.html).

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 でイベントを処理する際に、一部の Content Collaboration ユーザーが誤って非従業員として設定されていました。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でした。この問題は修正されました。

October 20, 2021

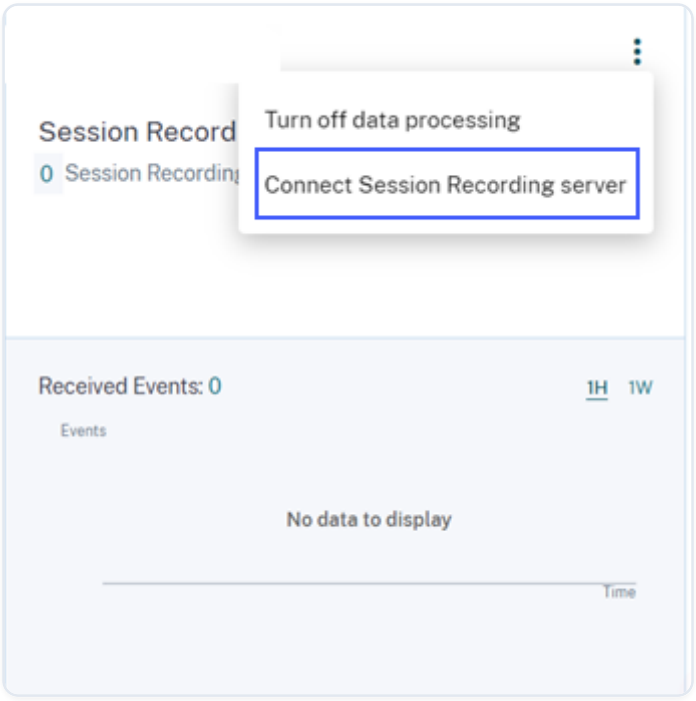
新機能

Session Recording サーバーの統合

Citrix Virtual Apps and Desktops および Citrix DaaS の展開では、Session Recording サーバーを設定して、ユーザーイベントを Citrix Analytics for Security に送信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洞察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 Server の接続**」を選択します。

詳細については、Connect to Session Recording deploymentを参照してください。



October 19, 2021

新機能

管理者への通知メールテンプレートの機能強化

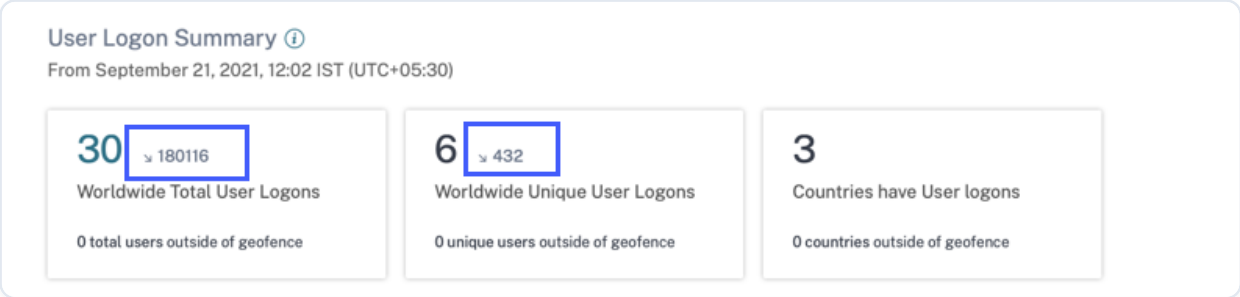
Notify administrator(s)アクションを適用した後に管理者が受け取るメール通知が強化され、ユーザーの危険なイベントに関するより良い洞察が得られるようになりました。

- 通知には、トリガーされたリスクインジケーターまたは適用されたポリシーに関する詳細情報が提供されるようになりました。たとえば、デフォルトおよびカスタムのリスクインジケーターの重大度とトリガーされた時間を確認できます。コンテンツ構造は、読みやすさを向上させるために改善されました。
- 管理者は、メール通知から直接ユーザータイムラインにアクセスし、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、管理者からの回答を収集し、その回答に基づいて通知のコンテンツを継続的に改善するのに役立ちます。

Notify administrator(s)アクションの詳細については、Policies and actionsを参照してください。

ユーザーログオン概要の機能強化

- 世界全体の総ユーザーログオン数と世界全体のユニークユーザーログオン数の、ユーザーログオンの増加または減少傾向を表示できるようになりました。



- **Unique Logon Locations**テーブルの**DEVIATION**列は、特定の場所におけるユニークユーザーログオンの増加または減少の変化を示します。



これらのメトリックは、以前の期間からユーザーログオンがどのように変化したか（肯定的または否定的）を理解するのに役立ちます。Citrix Virtual Apps and DesktopsおよびCitrix DaaS展開におけるユーザーインタラクションの可視性を提供します。

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。

修正された問題

- **アクセス保証ロケーション**ダッシュボードで、ジオフェンスエリア外からユーザーがログオンしない場合、**ユーザーログオンサマリー**カードにユーザーログオンメトリック（全世界の総ユーザーログオン数、全世界のユニークユーザーログオン数、ユーザーログオンのある国）が表示されない問題。この問題は修正されました。

October 01, 2021

新機能

Content Collaborationのセルフサービス検索で監査ログを表示

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すると、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として、リスク調査と分析に役立ちます。

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が、以前の期限切れセッションIDが新しいセッションIDとともに送信された場合に、Citrix Analyticsサービスにアクセスできない問題。この問題は修正されました。

September 29, 2021

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提供開始

このダッシュボードは、Citrix Virtual Apps and DesktopsおよびCitrix DaaSユーザーのロケーションに関する可視性を提供します。ジオフェンシングを有効にすることで、異常なロケーションのユーザーを特定し、脅威を防ぐために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**をクリックします。場所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。

September 15, 2021

新機能

カスタムリスクインジケーターの機能強化

- カスタムリスクインジケーター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後（約15〜20分）に更新されます。
- 既存のカスタムリスクインジケーターの条件、リスクカテゴリ、重大度、名前などの属性を変更した場合でも、ユーザータイムラインでは、ユーザーに対してトリガーされたカスタムリスクインジケーターの以前の発生（古い属性を持つもの）を表示できます。
- カスタムリスクインジケーターを削除した場合でも、ユーザータイムラインでは、ユーザーに対してトリガーされたカスタムリスクインジケーターの以前の発生を表示できます。

詳細については、「カスタムリスクインジケーター」を参照してください。

September 14, 2021

新機能

不審なログオンリスクインジケーターの導入

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、不審な性質のユーザーログオンを検出するようになりました。

- ユーザーおよび組織の履歴に関して、場所が異常であると見なされる
- ユーザーおよび組織の履歴に関して、デバイスが異常であると見なされる
- ネットワークは、ユーザーと組織の履歴に関して異常と見なされます。
- 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、Citrix Virtual Apps and DesktopsおよびCitrix DaaSユーザーが疑わしいコンテキストからログオンすると、リスクインジケーターがトリガーされます。

このリスクインジケーターは、Citrix Virtual Apps and Desktopsデータソースに関連付けられている**異常な場所からのアクセス**リスクインジケーターを置き換えます。**異常な場所からのアクセス**リスクインジケーターに基づいている既存のポリシーはすべて、新しいリスクインジケーターである**疑わしいログオン**に自動的にリンクされます。

リスクインジケーターの詳細については、「Citrix Virtual Apps and DesktopsおよびCitrix DaaSのリスクインジケーター」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**リスクインジケーターのスキーマ詳細をSIEMサービスに送信するようになりました。インジケーターの概要と**疑わしいログオン**リスクインジケーターのイベント詳細のスキーマを表示できます。詳細については、「SIEM用Citrix Analytics データ形式」を参照してください。

修正された問題

- Apps and Desktopsのセルフサービス検索では、ダウンロードされた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。

August 19, 2021

新機能

Splunk用Citrix Analyticsアプリの紹介

> **注**
>
> このアプリはプレビュー版です。

> Splunk用Citrix Analyticsアプリを使用すると、Citrix Analytics for Securityから収集されたデータを、Splunk上の洞察に満ちたダッシュボードの形式で表示できます。ダッシュボードは、ユーザーの危険なイベントに関する洞察を提供します。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。アプリをSplunk検索ヘッドにインストールします。

詳細については、Citrix Analytics App for Splunkを参照してください。

SIEM用のカスタムリスクインジケータスキーマ

SIEMサービスで、Citrix Virtual Apps and DesktopsおよびCitrix DaaS用に作成されたカスタムリスクインジケータ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の状況を把握するのに役立ちます。

カスタムリスクインジケータスキーマの詳細については、Citrix Analytics data format for SIEM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設定し、Security Analytics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に接続され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特定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、接続されているすべてのサイトを表示できます。

Directorでサイトを設定する方法の詳細については、Citrix Virtual Apps and Desktops and Citrix DaaS data source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、ジオフェンス領域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領域（国）と、ジオフェンスの内外からのユーザーログオンが表示されます。この機能は、**CVAD-Session started outside of geofence**リスクインジケータを使用してユーザーログオンを監視します。

詳細については、Access assurance location dashboardを参照してください。

ユーザーページでの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。ページには次のステータスが表示されます。

- サポート済み
- 部分的にサポートされています
- サポートされていません
- 利用できません
- 非アクティブ

このステータスは、ユーザーが使用してい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、ユーザーに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よう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データソースをオンボーディングする必要があります。そうしないと、すべてのCitrix Virtual Apps and DesktopsおよびCitrix DaaSユーザーのステータスが**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

カスタムリスクインジケーターを作成する際に、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などの文字列型ディメンションでのみ機能します。

詳細については、カスタムリスクインジケーターを参照してください。

リスクスコアリングの改善

ユーザーのタイムラインで、ユーザーのリスク概要を表示できるようになりました。リスク概要には、ユーザーイベントに関連するリスク要因に関する情報が提供されます。リスク要因は、ユーザーイベントにおける異常の種類を特定し、リスクスコアを決定するのに役立ちます。リスク要因は次のとおりです。

- デバイスベースのリスクインジケーター
- ロケーションベースのリスクインジケーター
- IPベースのリスクインジケーター
- ログオン失敗ベースのリスクインジケーター
- データベースのリスクインジケーター

- ファイルベースのリスクインジケーター
- カスタムリスクインジケーター
- その他のリスクインジケーター

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

詳細については、以下のトピックを参照してください。

- Citrixユーザーリスクインジケーター
- ユーザーリスクのタイムラインとプロファイル

July 29, 2021

非推奨の機能

Citrix Endpoint Management™ に関連する非推奨のアクション

以下の操作はCitrix Endpoint Managementデータソースから削除されました。これらの操作をリスクインジケーターに適用したり、これらの操作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。

- デバイスをロック
- Endpoint Management管理者に通知
- ユーザーに通知
- デバイスを取り消す
- デバイスをワイプ

既存のポリシーでこれらの操作がすでに使用されている場合、それらは自動的に**ウォッチリストに追加**操作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できます。

July 14, 2021

新機能

IS NOT EMPTY演算子のサポート

カスタムリスクインジケーターを作成する際、ディメンションが空でない（空白でない）ことを確認するために、条件で**IS NOT EMPTY**演算子を使用できるようになりました。

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

> 例えば、以下の条件は、国値がnullではない（つまり、国名が指定されている）任意の国からのユーザーログオンイベントを検出します。

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

詳細については、カスタムリスクインジケーターを参照してください。

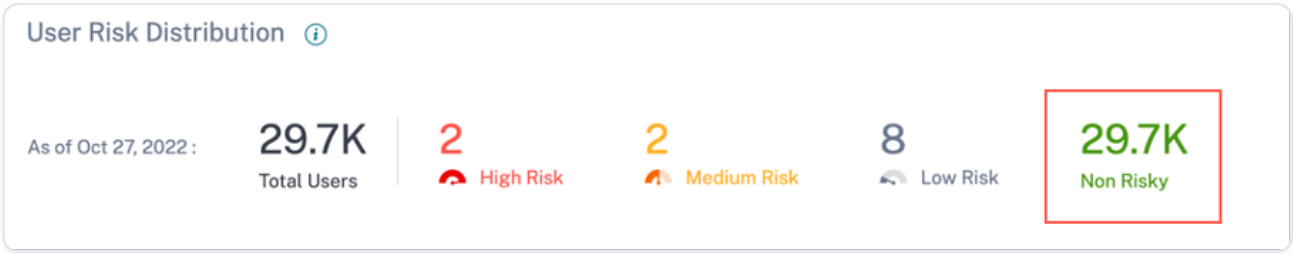
July 06, 2021

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。これらの検出されたユーザーは、選択した期間のゼロリスクスコアに基づいてリスクがないと識別されます。**リスクのないユーザー**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を表示できます。

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。



July 01, 2021

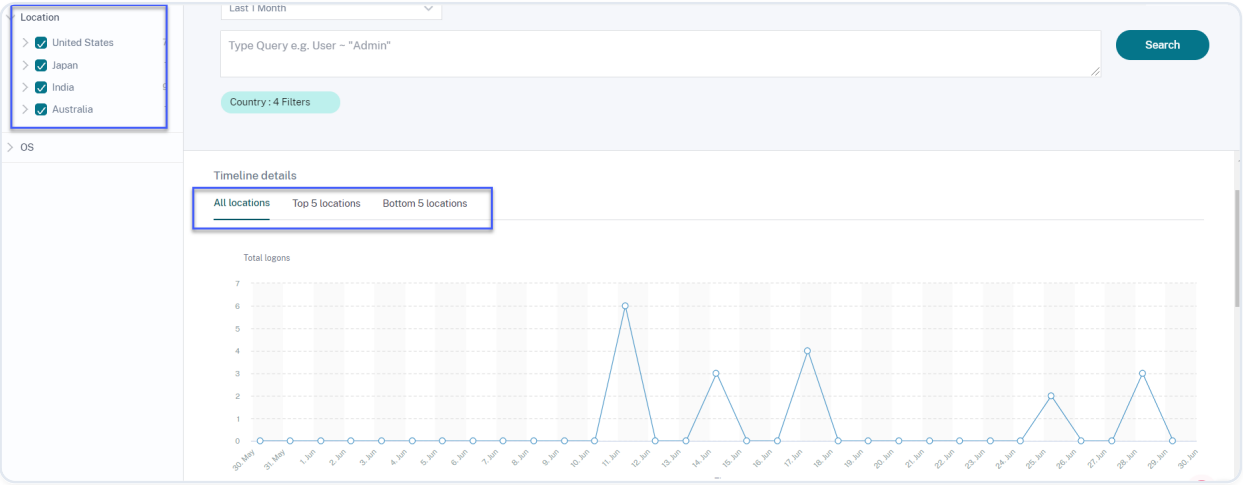
新機能

アクセス保証ロケーションダッシュボードの機能強化

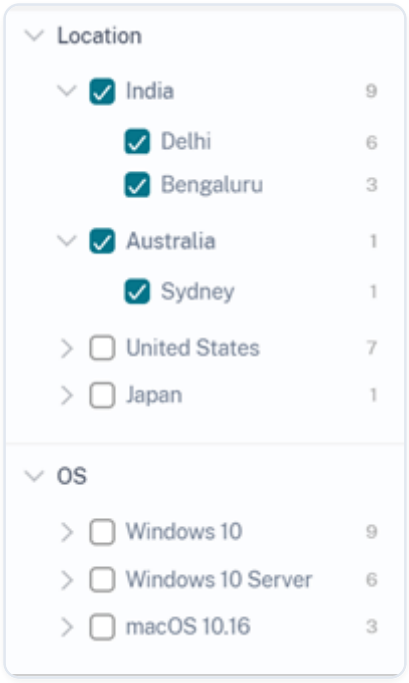
- **上位10件の固有のログオン場所**テーブルで、不明な場所からの固有のユーザーログオン数を表示できます。このリストは、上位10件の固有のログオン場所のサブセットです。場所が不明である理由と、ユーザーの場所を取得する可能性のある方法も確認できます。



- **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。



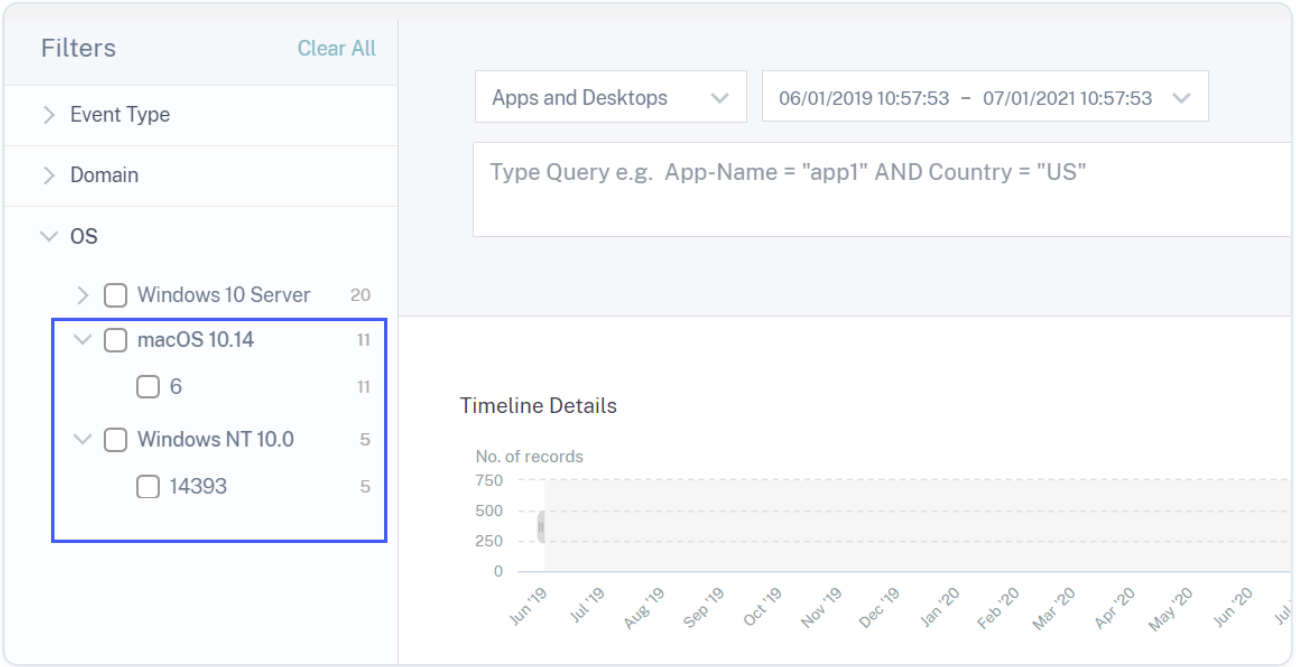
- **アクセス場所**ページでは、国とその都市、オペレーティングシステム（メジャーバージョンとマイナーバージョン）などのネストされたファセットを使用できます。これらのファセットを使用すると、イベントをきめ細かくフィルタリングできます。



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で OS ファセットを更新

ネストされた OS ファセットを使用して、Apps and 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、イベントを詳細にフィルタリングします。詳細については、「Apps and Desktops のセルフサービス検索」を参照してください。



June 30, 2021

新機能

Apps and Desktops のカスタムリスクインジケーター条件に Workspace アプリバージョンを追加

Apps and Desktops データソースの場合、カスタムリスクインジケーターを作成する際に、**Workspace-App-Version** ディメンションを使用して条件を定義できるようになりました。このディメンションの詳細については、「Apps and Desktops のセルフサービス検索」を参照してください。



June 23, 2021

新機能

SIEM メッセージの機能強化

リスクインジケーターのスキーマに次のフィールドが追加されました。

- `indicator_vector_name` - リスクインジケーター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インジケーター、場所ベースのリスクインジケーター、ログオン失敗ベースのリスクインジケーター、IPベースのリスクインジケーター、データベースのリスクインジケーター、ファイルベースのリスクインジケーター、およびその他のリスクインジケーターです。
- `indicator_vector_id` - リスクベクターに関連付けられたID。ID 1 = デバイスベースのリスクインジケーター、ID 2 = ロケーションベースのリスクインジケーター、ID 3 = ログオン失敗

ベースのリスクインジケーター、ID 4 = IPベースのリスクインジケーター、ID 5 = IPベースのリスクインジケーター、ID 6 = データベースのリスクインジケーター、ID 7 = その他のリスクインジケーター、ID 999 = 利用不可。

詳細については、「Citrix Analytics data format for SIEM」を参照してください。

June 07, 2021

新機能

管理者への通知アクションの機能強化

リスクインジケーターに**管理者への通知**アクションを適用するか、そのアクションを含むポリシーを作成する場合、ユーザーの危険な行動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。こ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。

読み取り専用共有アクションのサポートを追加

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**リスクインジケーターをトリガーします。ユーザーのリスクタイムラインから、**過剰なファイル共有**リスクインジケーターに**リンクを読み取り専用共有に変更**アクションを適用できるようになりました。共有リンクのリスクタイムライン上の特定の共有リンクにもこのアクションを適用できます。このアクションにより、他のユーザーは共有リンクに関連付けられたファイルをダウンロード、コピー、または印刷できなくなります。こ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。

May 18, 2021

新機能

デフォルトのリスクインジケーターをカスタムリスクインジケーターに移行する

次のデフォルトのリスクインジケーターは、事前構成済みのカスタムリスクインジケーターに移行されます。

デフォルトのリスクインジケーター	データソース	事前構成済みのカスタムリスクインジケーター
新しいデバイスからの初回アクセス	シトリックス バーチャルアプリ アンド デスクトップ および シトリックス DaaS	CVAD - 新しいデバイスからの初回アクセス

デフォルトのリスクインジケーター	データソース	事前構成済みのカスタムリスクインジケーター
新しいIPからの初回アクセス	シトリックス ゲートウェイ	Gateway - 新しいIPからの初回アクセス

カスタムリスクインジケーターへのこの移行に伴い、デフォルトのリスクインジケーターおよび関連する機械学習アルゴリズムは非推奨となります。

対応するカスタムリスクインジケーターは、以下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場合、または90日以上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アドレスから初めてサインインした場合、または90日以上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場合。

事前設定された条件に加えて、Citrix環境の脅威を特定するために、これらのカスタムリスクインジケーターに独自の条件を追加できるようになりました。このオプションにより、セキュリティ要件に基づいてカスタムリスクインジケーターを柔軟に構成できます。また、これらのカスタムリスクインジケーターによって検出された危険なイベントに対して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インジケーターとそのイベントを引き続き表示できます。

これらのデフォルトのリスクインジケーターに関連付けられたポリシーは、対応する事前設定されたカスタムリスクインジケーターに自動的にリンクされます。

詳細については、「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」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**」フィルターは「**レコードタイプ**」に名称変更されました。イベントをフィルタリングするには、次のレコードタイプのいずれかを選択してください - 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。

次の表は、レコードタイプとイベントタイプの相関関係を示しています。

レコードタイプ	イベントタイプ
VPN_AI	認証
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

- カスタムリスクインジケーターは、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が含まれるユーザーイベントでは、次の動作が見られます。
  - `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ーがトリガーされます。

    `Event-Type = Session.Logon AND Device-ID NOTIN (“1621d2cb-f598-5ef7-a5bf-81747496ed2e”)`
  - 同じデバイスに対して `Device-ID` ディメンションの値を大文字で入力した場合、カスタムインジケーター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、カスタムリスクインジケーターは条件値の大文字と小文字の区別に関係なくトリガーされるようになりました。

April 29, 2021

新機能

カスタムリスクインジケーターのイベント詳細

ユーザーのリスクタイムラインページで、カスタムリスクインジケーター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、カスタムリスクインジケーターの定義された条件、説明、トリガー頻度のみを表示できました。ユーザーとリスクインジケーターに関連付けられたイ

ベントの詳細を表示するには、**イベント検索**をクリックします。 詳細については、カスタムリスクインジケーターを参照してください。

修正された問題

- 管理者のアクセス権限が読み取り専用管理者からフル管理者に変更された後でも、カスタムリスクインジケーターを作成できません。

April 16, 2021

新機能

SIEMメッセージの機能強化

リスクインジケーターのスキーマ形式で、以下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インジケーター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アドレスは一部のバッチリスクインジケーターでのみ利用可能でした。
    - EPAスキャン失敗
    - 過剰な認証失敗
    - 不審なIPからのログオン
    - 異常な場所からのアクセス
    - 異常な認証失敗
    - 匿名による機密共有ダウンロード
    - 潜在的なデータ流出
- 整数データ型フィールドの値が利用できない場合、割り当てられる値は **-999** です。例: `"latitide" = -999`。
- 文字列データ型フィールドの値が利用できない場合、割り当てられる値は **NA** です。例: `"city"= "NA"`。

詳細については、「Citrix Analytics data format for SIEM」を参照してください。

March 26, 2021

新機能

SIEMメッセージの制限

Citrix Analyticsは、各リスクインジケーターの発生につき最大1000件のイベント詳細をSIEMサービスに送信します。これらのイベントは発生の時系列順に送信されます。詳細については、「Citrix Analytics data format for SIEM」を参照してください。

SIEMメッセージにデータソースIDとインジケーターカテゴリIDフィールドを追加

インジケーターサマリースキーマとインジケーターイベント詳細スキーマに以下のフィールドが追加されました。

フィールド	説明
`data_source_id`	データソースに関連付けられているID。ID 0 = シトリックス コンテンツ コラボレーション、ID 1 = シトリックス ゲートウェイ、ID 2 = シトリックス エンドポイント マネジメント、ID 3 = シトリックス バーチャル アプリケーションズ アンド デスクトップス、ID 4 = シトリックス アクセス コントロール™
`indicator_category_id`	リスクインジケーターカテゴリに関連付けられたID。ID 1 = データ流出、ID 2 = 内部脅威、ID 3 = 侵害されたユーザー

詳細については、SIEM用Citrix Analyticsデータ形式を参照してください。

March 18, 2021

新機能

アクセス保証ロケーションダッシュボード

> **注**
>
> この機能はプレビュー版です。

> **アクセス保証ロケーション**ダッシュボードは、選択した期間にCitrix Virtual Apps and DesktopsおよびCitrix DaaSユーザーがログオンした場所の概要を提供します。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、**Security > Access Assurance** をクリックします。

選択した期間について、以下の情報を表示できます。

- 特定の場所から、およびすべての場所からのユーザーログオンの合計数。
- すべての場所からのユニークユーザーログオンの合計数。
- ユーザーがログオンした国の合計数。
- ユニークユーザーログオンが多い上位10か所。

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インジケーター条件で、NOT LIKE (!~) 演算子を使用できるようになりました。この演算子は、指定した一致パターンについてユーザーイベントをチェックします。イベント文字列内のどこにも指定されたパターンが含まれていないイベントを返します。

たとえば、クエリ `User-Name !~ “John”` は、John、John Smith、または「John」という一致する名前を含むその他のユーザーを除く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。

翻訳されたオペレーティングシステムバージョン

Citrix Virtual Apps and Desktops および Citrix DaaS データソースの場合、**Platform** ディメンションは、**OS-Major-Version**、**OS-Minor-Version**、および **OS-Extra-Details** ディメンションとして翻訳されるようになりました。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、Citrix Analytics はこれらのディメンションをセルフサービス検索ページに表示します。

これらのディメンションを使用して、カスタムリスクインジケーターの条件を定義できます。

以前に作成されたカスタムリスクインジケーターで、条件として**Platform**ディメンションを使用していた場合、Citrix Analyticsは**Platform**ディメンションを**OS-Major-Version**、**OS-Minor-Version**、および**OS-Extra-Details**に自動的に置き換えます。この更新は、定義され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。

Apps and Desktopsのデータフィールドを更新しました

Apps and Desktops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。

詳細については、「Apps and Desktops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およびVPN_SUイベントを削除しました

Citrix Gatewayデータソースのセルフサービス検索ページから、以下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いたカスタムリスクインジケーター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。

March 11, 2021

新機能

ユーザーリスクスコアスキーマの現在のタイムスタンプ

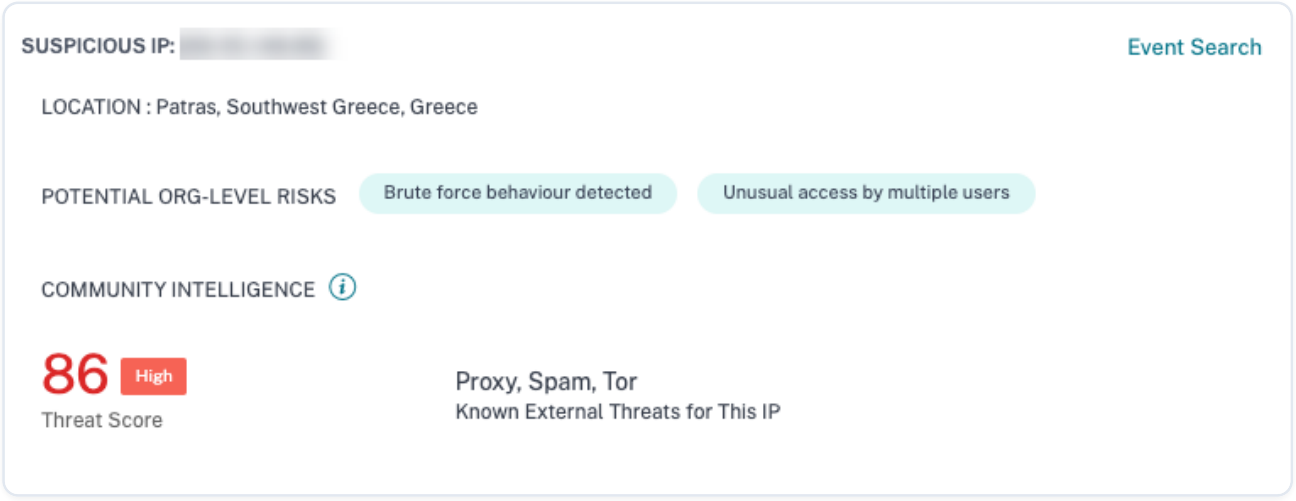
新しいフィールド `last_update_timestamp` がユーザーリスクスコアスキーマ形式に追加されました。このフィールドは、リスクスコアが最後に更新された時間を示します。スキーマ形式の詳細については、ユーザーリスクスコアスキーマを参照してください。

March 03, 2021

新機能

不審なIPからのログオンリスクインジケーターの機能強化

ユーザーのリスクタイムラインページに、**不審なIPからのログオン**リスクインジケーターの新しいセクション**不審なIP**が表示されます。このセクションには、次の情報が表示されます。



- 不審なサインインアクティビティが検出されたIPアドレス。
- ユーザーの場所。
- Citrix Analytics が最近組織内で検出した不審な IP アクティビティのパターン。
- IPアドレスに関するコミュニティレベルのインテリジェンスフィード。

詳細については、不審なIPからのログオンリスクインジケーターを参照してください。

「異常な場所からのアクセス」リスクインジケーターの機能強化

- 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ーで、イベントテーブルに **TOOL NAME** 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。詳細については、「Citrix Content Collaboration のリスクインジケーター」を参照してください。

- Citrix Virtual Apps and Desktops および Citrix DaaS の「異常な場所からのアクセス」リスクインジケーターで、イベントテーブルに **DEVICE ID** 列と **RECEIVER TYPE** 列を追加しました。詳細については、Citrix Virtual Apps and Desktops のリスクインジケーターを参照してください。

SIEM 用 Citrix Analytics データ形式

この記事では、SIEM サービス用に Citrix Analytics が生成する処理済み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` の値が null の場合、そ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。

February 18, 2021

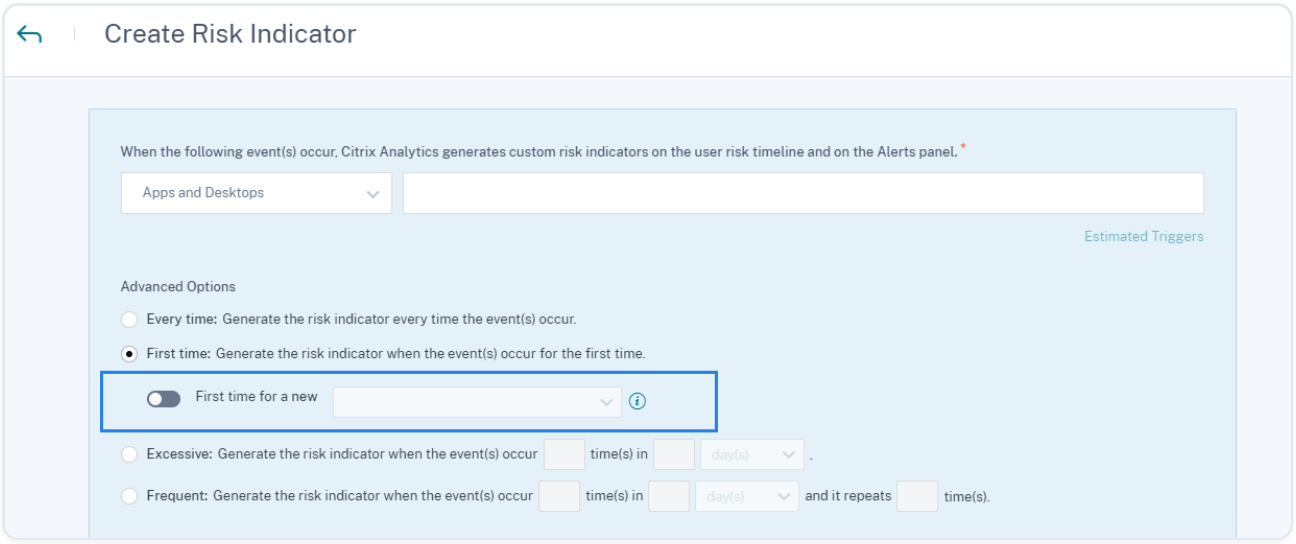
新機能

カスタムリスクインジケーターにおける新しいエンティティからの初回アクセスをサポート

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インジケーター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。

「**インジケーターの作成**」ページで、「**初回**」オプションをクリックします。「**新規の初回**」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**」を選択した場合、Citrix Analytics は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リスクインジケーターをトリガーします。

詳細については、カスタムリスクインジケーターの作成を参照してください。



カスタムリスクインジケーター作成の最大制限

カスタムリスクインジケーターを最大50個まで作成できるようになりました。この最大制限に達した場合は、カスタムリスクインジケーターを作成するために、既存のカスタムリスクインジケーターを削除または編集する必要があります。

詳細については、「カスタムリスクインジケーター」を参照してください。

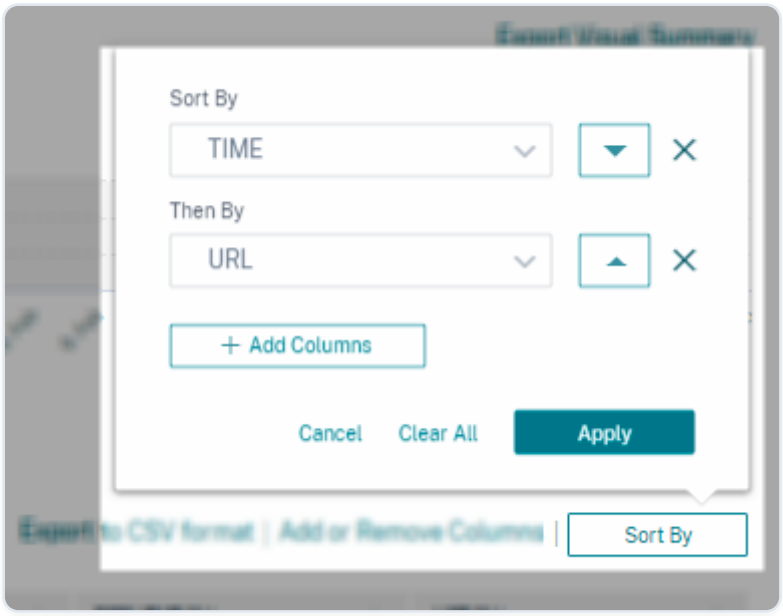
Citrix Virtual Apps and DesktopsおよびCitrix DaaSからのユーザー位置情報データ

ユーザー情報ページで、Citrix AnalyticsはCitrix Virtual Apps and DesktopsおよびCitrix DaaSデータソースからのユーザーの位置情報を表示するようになりました。

ユーザーの位置情報の詳細については、「ユーザープロファイル」を参照してください。

複数列ソート

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ソートできるようになりました。**ソート基準**をクリックし、列とソート順を追加します。**適用**をクリックしてユーザーイベントをソートします。複数列ソートを実行するために、最大6つの列を追加できます。



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。

非推奨の機能

過剰な認証失敗リスクインジケーターは非推奨になりました

Citrix Gatewayのリスクインジケーターである**過剰な認証失敗**は非推奨になりました。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。

この非推奨化の一環として、以下の変更が適用されます。

- Citrix Analyticsはこれらのリスクインジケーターを生成しなくなりました。
- Citrix Analyticsは、これらのリスクインジケーターを条件とするポリシーを生成しなくなりました。
- これらのリスクインジケーターを条件とするデフォルトポリシーは、もはや有効ではありません。

詳細については、Citrix Gatewayリスクインジケーターを参照してください。

January 27, 2021

新機能

異常な場所からのアクセスリスクインジケーターの機能強化

Citrix Content Collaboration、Citrix Gateway、およびCitrix Virtual Apps and Desktopsの場合、**異常な場所からのアクセス**リスクインジケーターは、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場所から異常に離れた新しい都市からサインインしたときにトリ

ガーされるようになりました。その他の要因には、ユーザーの全体的な移動レベル、および組織内のすべてのユーザーにおけるその都市からのサインインの相対的な頻度が含まれます。すべての場合において、ユーザーの位置履歴は過去30日間のサインインアクティビティに基づいています。

リスクインジケーターの詳細については、以下のトピックを参照してください。

- Citrix Content Collaborationリスクインジケーター
- Citrix Gatewayリスクインジケーター
- Citrix Virtual Apps and DesktopsおよびCitrix DaaSリスクインジケーター

January 20, 2021

修正された問題

- オンプレミスのStoreFrontを使用するApps and Desktopsデータソースの場合、StoreFront展開が正常に接続されていても、データ処理が失敗します。

January 19, 2021

修正された問題

- カスタムリスクインジケーターページで、検索フィールドの無効な条件を修正した後、**トリガーの推定**リンクが応答しません。

  たとえば、無効な条件 *Client-IP = 10.10.10.10* を入力します。この条件を修正して *Client-IP = "10.10.10.10"* と入力しても、**トリガーの推定**リンクは応答しません。

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

January 13, 2021

新機能

Citrix Analytics Add-on for Splunk の新しいバージョンが利用可能です

Citrix Analytics Add-on for Splunk バージョン 2.1.0 が利用可能になりました。ファイルをダウンロードするには、ダウンロードページにアクセスしてください。

Splunk Cloud Inputs Data Manager (IDM) および Splunk 8.1 64ビットのサポートを追加

Citrix Analytics for Security を Splunk Cloud 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 の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

Citrix Analytics for Security を Splunk 7.1 64ビットと統合することは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 の統合を参照してください。

January 11, 2021

修正済みの問題

- Virtual Apps and Desktopsサイトカードで、**サポートされているクライアントユーザー**というラベルが**ユーザーから受信したイベント**に名前が変更されました。**サポートされていないクライアントユーザー**というラベルは**ユーザーからイベントを受信できません**に名前が変更されました。

December 17, 2020

新機能

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、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、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のリストを提供します。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発信される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、事前設定されたカスタムリスクインジケーターとポリシーです。

- CVAD-ジオフェンス外で開始されたセッション
- GW-ジオフェンス交差
- CCC-ジオフェンス交差

- ジオフェンス外でのセッション開始

詳細については、「事前設定されたカスタムリスクインジケーターとポリシー」を参照してください。

ユーザー応答メールでアクセスされた場所を表示する

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、ユーザーが過去15分間に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>`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、ユーザー応答の要求を参照してください。

コンテンツコラボレーションリスクインジケーターの名称変更 - 新しい場所からの初回アクセス

Citrix Content Collaborationリスクインジケーター「**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**」に名称変更されました。

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

リスクインジケーターのフィードバック

リスクインジケーターのフィードバックメカニズムは削除されました。Content Collaborationリスクインジケーター「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、誤検知として報告したり、フィードバックを提供したりすることはできなくなりました。

December 07, 2020

新機能

潜在的なデータ流出リスクインジケーターの改善

リスクインジケーターに以下の機能強化が加えられました。

- 「**何が起こったか**」セクションの情報が更新されました。一貫性を保つために、時刻形式が更新されました。
- デバイスの位置情報がイベントリストに表示されます。

リスクインジケーターの詳細については、潜在的なデータ流出を参照してください。

コンテンツコラボレーションリスクインジケーターの改善 - 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**を選択すると、以下の情報が表示されます。

- **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異常な場所の地理的な地図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上位6つの通常の場所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します。
- **異常な場所のイベント詳細**: 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。

リスクインジケーターの詳細については、「新しい場所からの初回アクセス」を参照してください。

November 30, 2020

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、以下の改善が行われました。

- 検索ボックスにクエリの例が表示され、独自のクエリの入力方法が示されます。

  検索ボックスのクエリ(/en-us/citrix-analytics/media/search-bar-query.png)
- macOSでは、ディメンション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。

  Macのスクロールバー(/en-us/citrix-analytics/media/macos-scroll-bar.png)
- 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。

  フィルターチップ(/en-us/citrix-analytics/media/filter-chips.png)
- 「**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。

  アイコンの更新(/en-us/citrix-analytics/media/label-update-add-remove.png)

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、Citrix Analyticsで正常に検出され接続されたデータソースに関連付けられているポリシーが表示されるようになりました。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**ページ上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。

November 04, 2020

新機能

不審な認証失敗 - Citrix Gatewayリスクインジケーター

Citrix Analyticsは、ユーザーが通常とは異なるIPアドレスからのログオンに失敗した場合に、アクセスベースの脅威を検出し、「**不審な認証失敗**」リスクインジケーターをトリガーします。

このリスクインジケーターは、組織内のユーザーが通常の行動とは異なる不審なIPアドレスからのログオンに失敗した場合にトリガーされます。

詳細については、「Citrix Gatewayリスクインジケーター」を参照してください。

認証失敗(/en-us/citrix-analytics/media/gateway-authentication-failure.png)

October 20, 2020

修正された問題

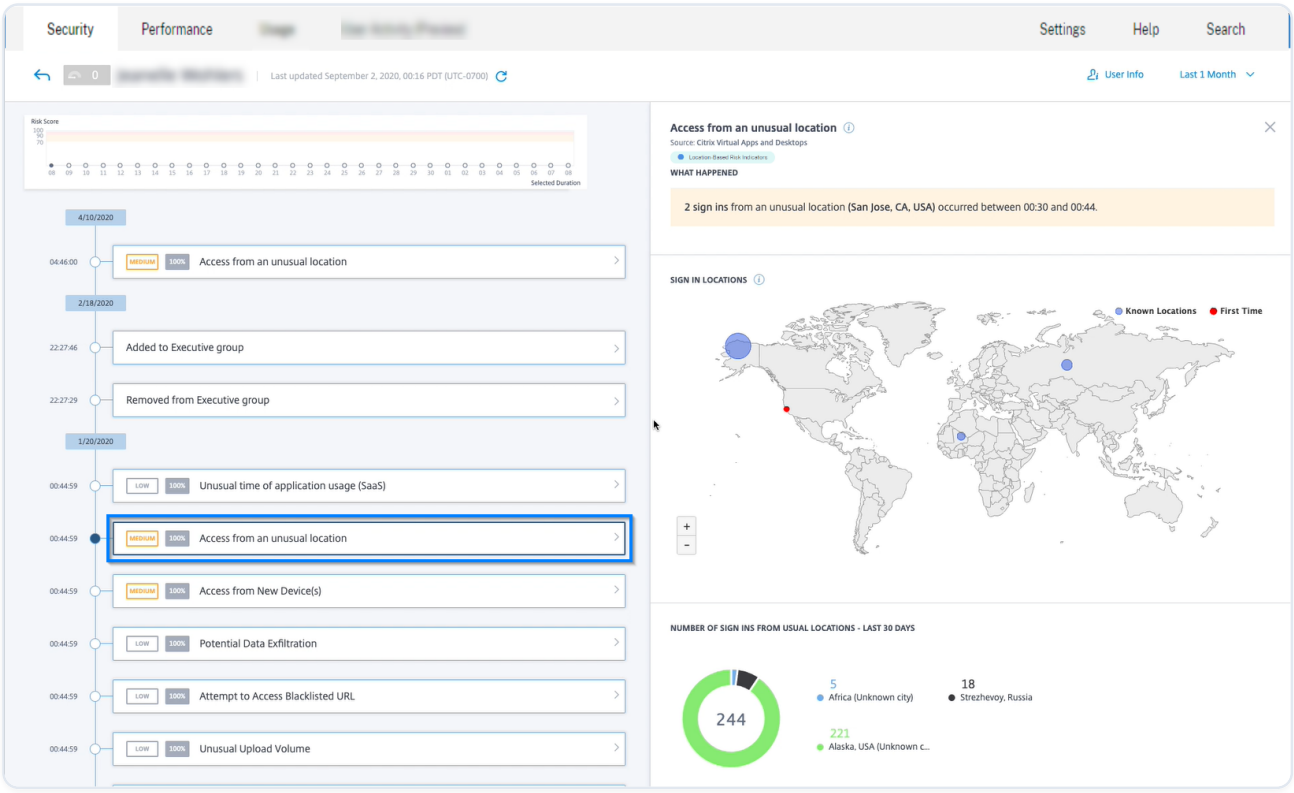
- 「**新しいデバイスからの初回アクセス**」というリスクインジケーターに「**ユーザーをログオフ**」アクションが適用されている場合、期待どおりに動作しません。

October 15, 2020

新機能

不審な場所からのアクセス – Citrix Virtual Apps and DesktopsおよびCitrix DaaSのリスクインジケーター

Citrix Analyticsは、Citrix Workspaceからの不審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、対応するリスクインジケーターをトリガーします。



詳細については、「Citrix Virtual Apps and DesktopsおよびCitrix DaaSのリスクインジケーター」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

- SHARE URL列はSHARE 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。
- ダッシュボードの時間選択機能は削除されました。このダッシュボードでは、選択された期間ではなく、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るようになりました。
- すべての共有リンクは、まず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。デフォルトでは、リスクインジケーターのカウント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、危険な動作を示すアクティブなリンクが表示されます。期限切れのリンクは表示されません。デフォルトでは、リスクインジケーターのカウント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は削除されました。

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。

共有リンクのリスクタイムラインの機能強化

リスクタイムラインに、共有URLではなく共有IDが表示されるようになりました。詳細については、「共有リンクのリスクタイムライン」を参照してください。

非推奨の機能

サポートされていないオペレーティングシステム (OS) を搭載したデバイスからのアクセスリスクインジケーターは非推奨になりました

Citrix Virtual Apps and Desktops のリスクインジケーター - **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** は非推奨になりました。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。

この非推奨化の一環として、以下の変更が適用されます。

- Analytics はこれらのリスクインジケーターを生成しなくなりました。
- Analytics は、これらのリスクインジケーターを条件とするポリシーを生成しなくなりました。
- これらのリスクインジケーターを条件とするデフォルトポリシーは、もはや有効になりません。

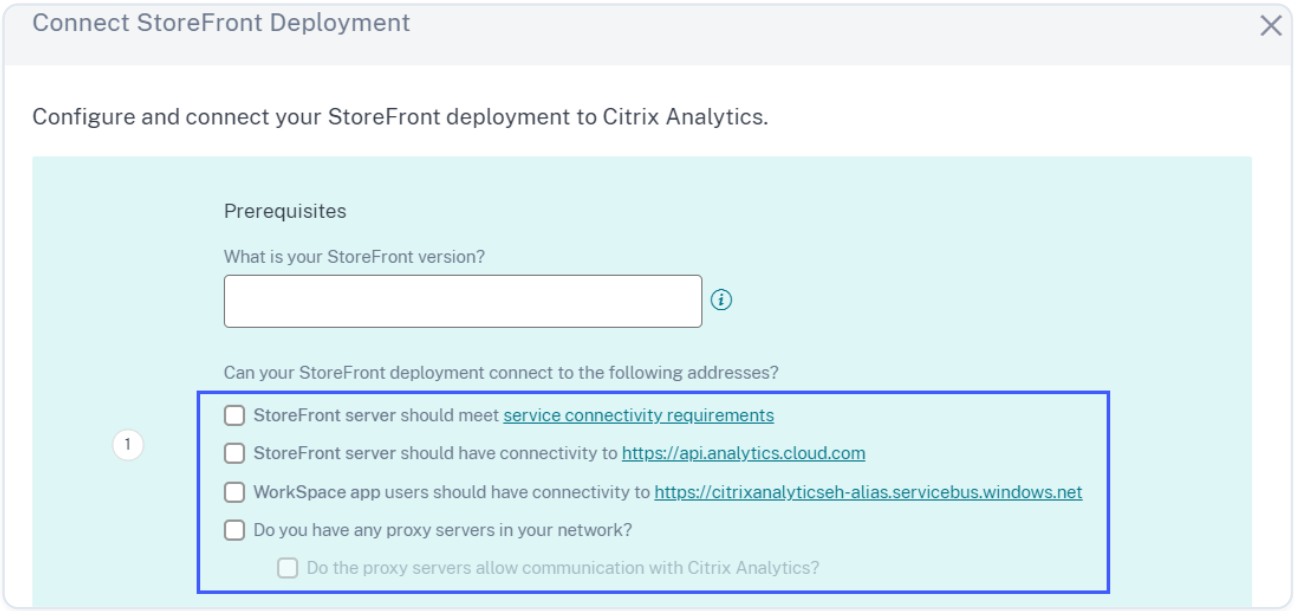
詳細については、「Citrix Virtual Apps and Desktops および Citrix DaaS のリスクインジケーター」(/ja-jp//security-analytics/risk-indicators/citrix-virtual-apps-and-desktops-risk-indicators.html) を参照してください。

September 10, 2020

新機能

StoreFront のチェックリスト

Citrix Analytics に、StoreFront 構成ファイルをダウンロードする前に満たす必要がある前提条件のリスト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てください。最小要件が選択されていない場合、構成ファイルをダウンロードできません。詳細については、「Citrix Virtual Apps and Desktops データソース」(/ja-jp/citrix-analytics/data-sources/virtual-apps-desktops-onboarding.html#onboard-virtual-apps-and-desktops-sites-using-storefront)を参照してください。



セルフサービス検索 - NOT EQUAL (!=) 演算子に対応

以下の機能のクエリで、NOT EQUAL (!=) 演算子を使用できるようになりました。

- カスタムリスクインジケーター
- セルフサービス検索

この演算子は、以下の条件で使用できます。

データソース	ディメンション
コンテンツコラボレーション	国、都市、クライアントOS
アクセスコントロール	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
ゲートウェイ	認証ステージ、クライアントIP

演算子を使用して、「Country != XYZ」のような単一値のカスタムインジケーター式を作成し、ユーザーのリストを表示します。次に、ウォッチリストへの追加、管理者への通知、ユーザーの無効化などのアクションを適用するポリシーを作成します。 指定されたデータソースのセルフサービス検索で演算子を使用して、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てください。ディメンション値は大文字と小文字を区別します。

September 08, 2020

新機能

ユーザー相関

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ます。このメカニズムにより、検出されたユーザー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には、データソースとリスクインジケーターとともに、一意のユーザーのリストが表示され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JosephSm、<joe.smith@citrix.com>、およびjoe.smithなどの複数のユーザー識別子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。他のすべてのユーザー識別子は関連付けられ、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

アクションリストからアクションオプションを選択し、**適用**をクリックすると、エラーメッセージが表示されます。

August 11, 2020

修正された問題

- Microsoft Graph SecurityをCitrix Analyticsと統合できません。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。

July 31, 2020

修正された問題

- カスタムリスクインジケーターの**推定トリガー**オプションは、過去1日間のカスタムリスクインジケーターインスタンスを予測しません。

July 09, 2020

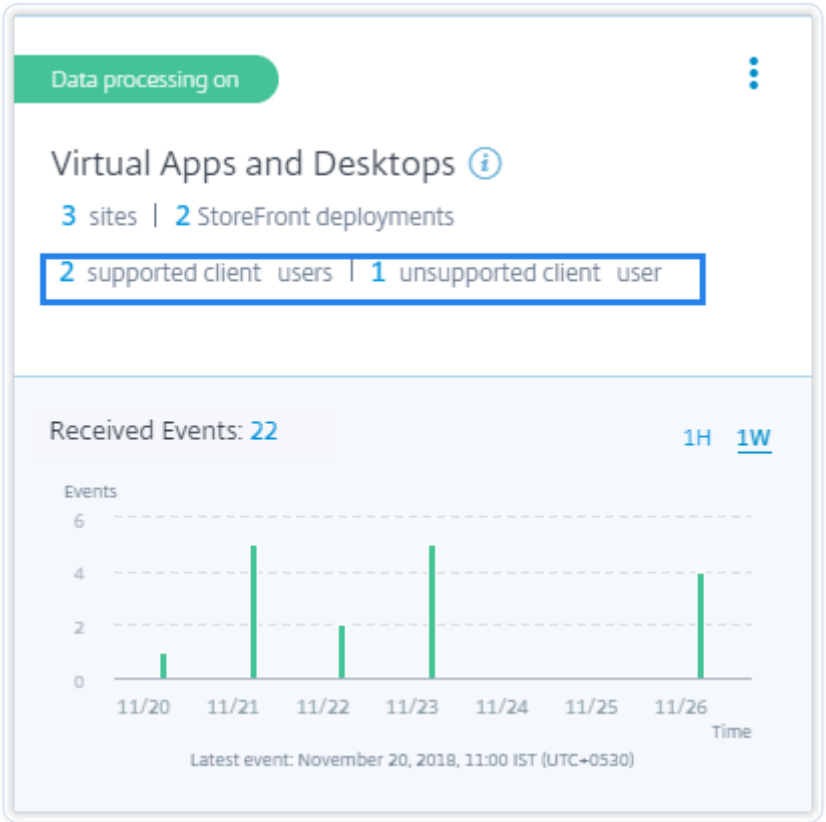
新機能

Virtual Apps and Desktopsサイトカードに、サポート対象およびサポート対象外のクライアントを使用しているユーザーが表示されます

サイトカードで、エンドポイントでサポート対象およびサポート対象外バージョンのCitrix WorkspaceアプリまたはCitrix Receiver™クライアント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。

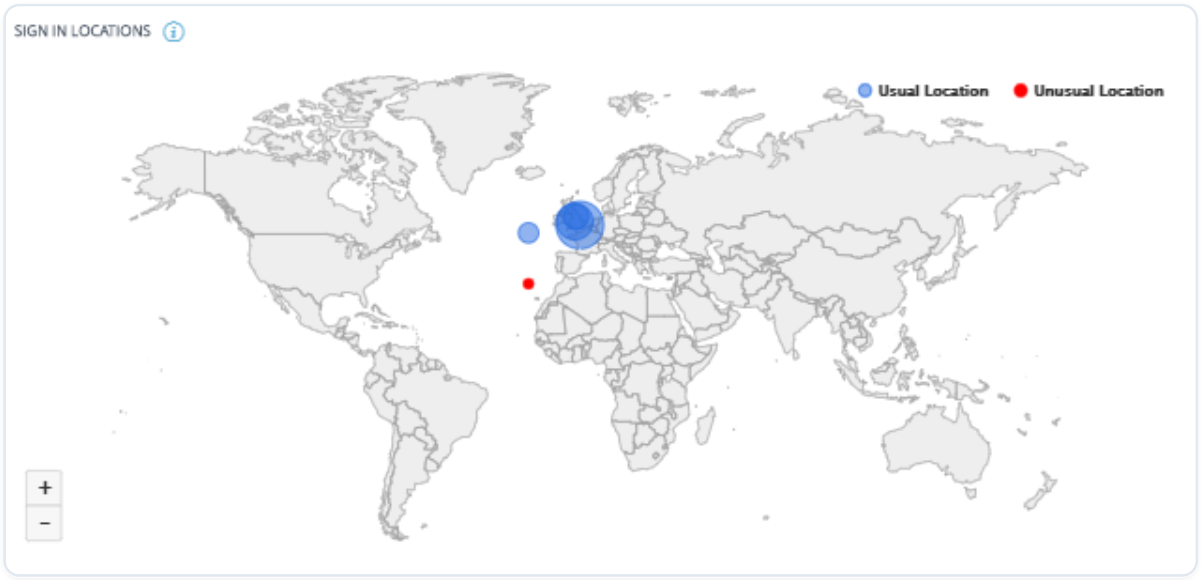
- サポート対象クライアントのユーザー数をクリックすると、検出されたすべてのユーザーが表示される**ユーザー**ページが表示されます。
- サポート対象外クライアントのユーザー数をクリックすると、CSVファイルがダウンロードされます。このファイルには、ユーザーとそのサポート対象外のクライアントバージョンが一覧表示されます。Analyticsはサポート対象外のクライアントからユーザーイベントを受信しないため、ユーザーを検出されたユーザーとして追加しません。CSVファイルを使用して、Analyticsがユーザーの行動に関するセキュリティインサイトを提供できるように、クライアントをサポート対象バージョンにアップグレードする必要があるユーザーを特定します。

サポート対象クライアントのリストを表示するには、「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。



異常な場所からのアクセスリスクインジケーター

- Citrix Gatewayリスクインジケーターの**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**に名称変更されました。
- ユーザーリスクタイムラインのイベント詳細セクションに、地理マップと円グラフが導入されました。
  - **サインイン場所**: このセクションには、ユーザーの通常の場所と異常な場所の地理マップビューが表示されます。通常の場所と異常な場所は、地理マップの右上セクションに色分けで示されます。地理マップをズームして、場所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上位6つの通常の場所を示す円グラフが表示されます。各場所は異なる色分けでマークされています。選択した場所の詳細なビューを表示するには、場所でセクションを並べ替えることができます。

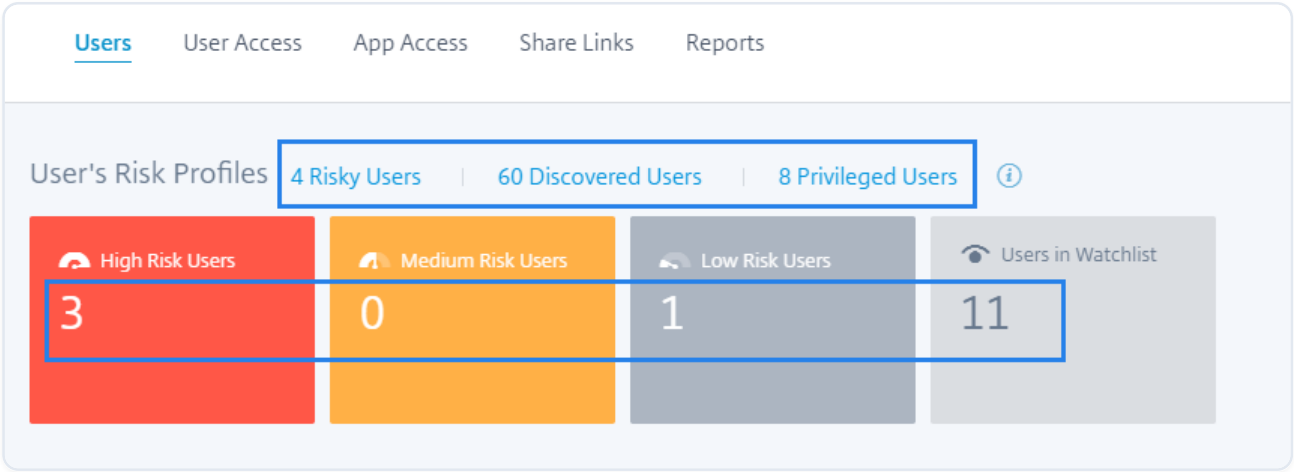


詳細については、「異常な場所からのアクセス」を参照してください。

ユーザーダッシュボードデータ

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は、**ユーザー**ダッシュボードと**ユーザー**ページで選択された期間に関係なく、過去13か月間表示されます。期間を選択すると、リスクインジケーターの発生回数が変化します。

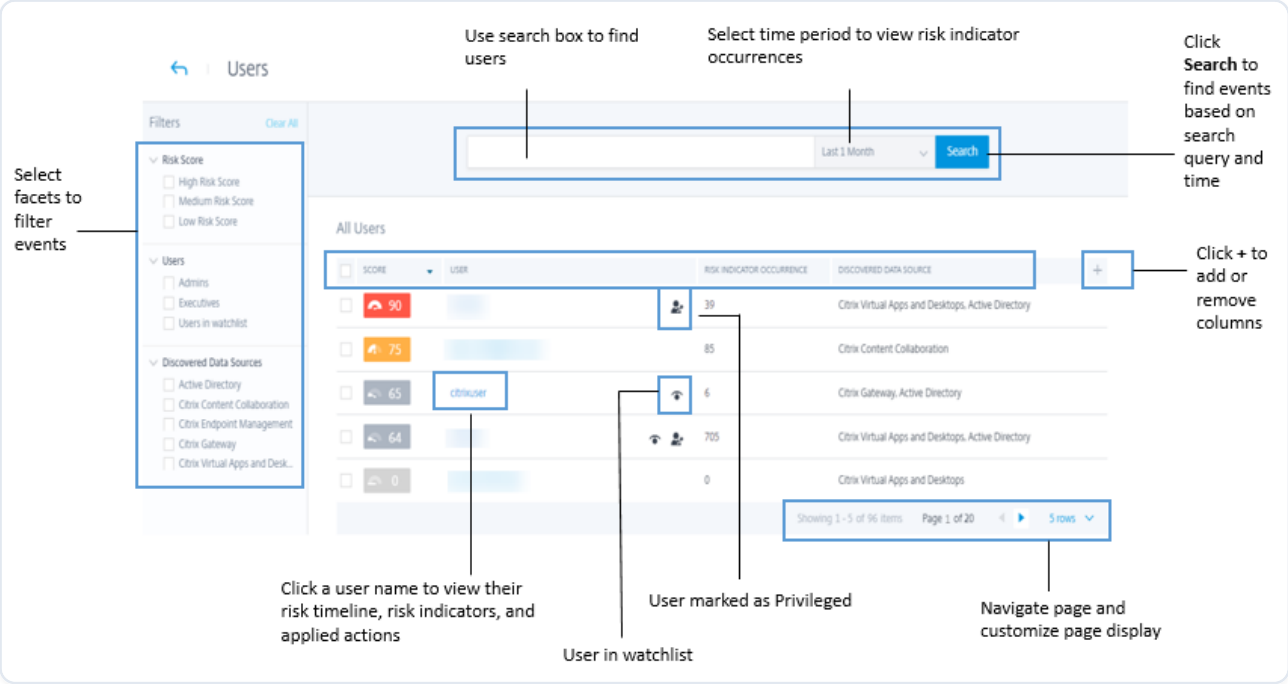
詳細については、「ユーザーダッシュボード」を参照してください。



再設計されたユーザーページ

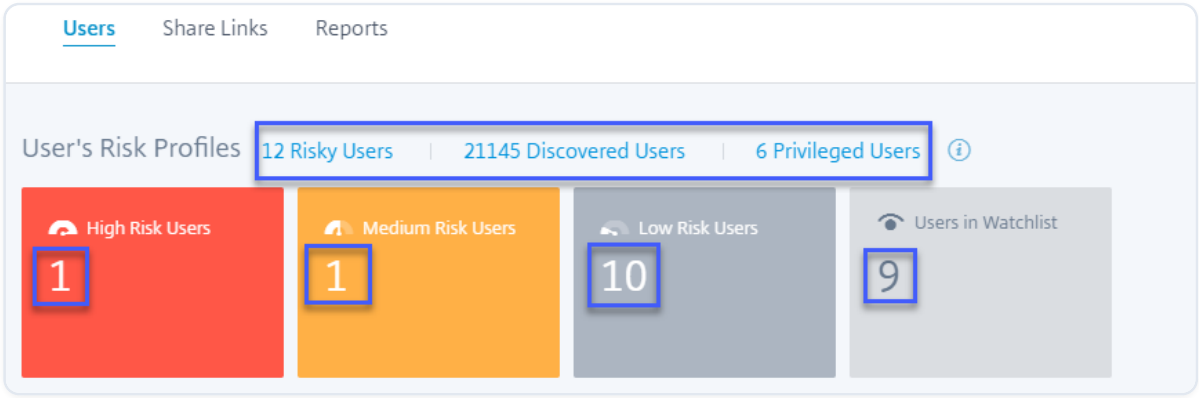
ユーザーページは、より良いユーザーエクスペリエンスのために強化されました。ユーザーのリスクスコア、データソース、およびユーザータイプに基づいて、ユーザーイベントの統合された概要を提供します。

より焦点を絞った検索をサポートするために、**ユーザー**ページには左ペインに**フィルター**セクションと上部に検索バーが含まれています。プリセット時間またはカスタマイズされた時間範囲でユーザー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:

- **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。
  - 次のいずれかのリンクまたはカードをクリックします。



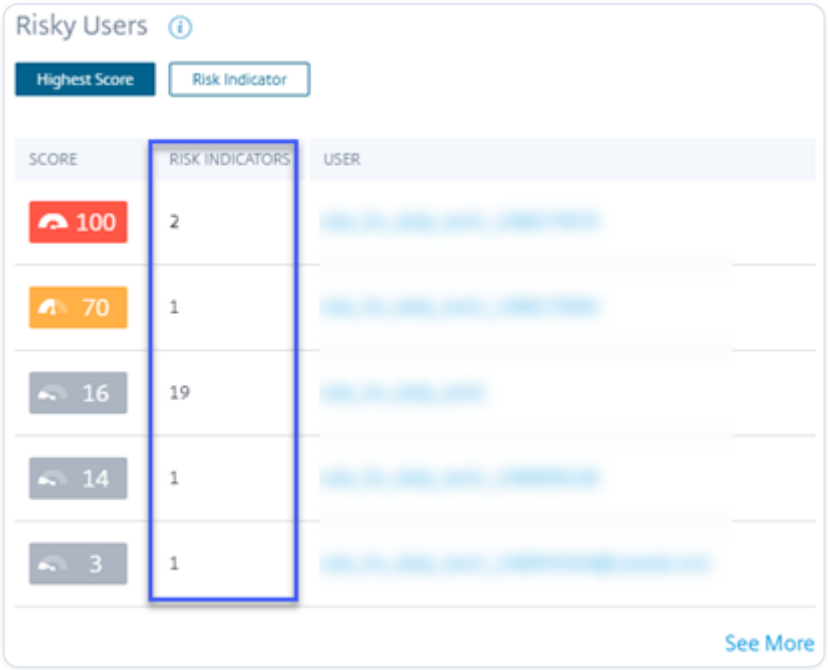
  - **リスクのあるユーザー**ペインで、**さらに表示**をクリックします。
  - **ウォッチリスト内のユーザー**ペインで、**さらに表示**をクリックします。
  - **特権ユーザー**ペインで、**さらに表示**をクリックします。
- **設定 > データソース > セキュリティ**に移動します。任意のデータソースサイトカードでユーザー数をクリックします。

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。

リスクのあるユーザーペインの機能強化

変更列は**リスクインジケーター**列に置き換えられました。**リスクインジケーター**列には、特定の期間におけるユーザーのリスクインジケーターの合計発生数が表示されます。

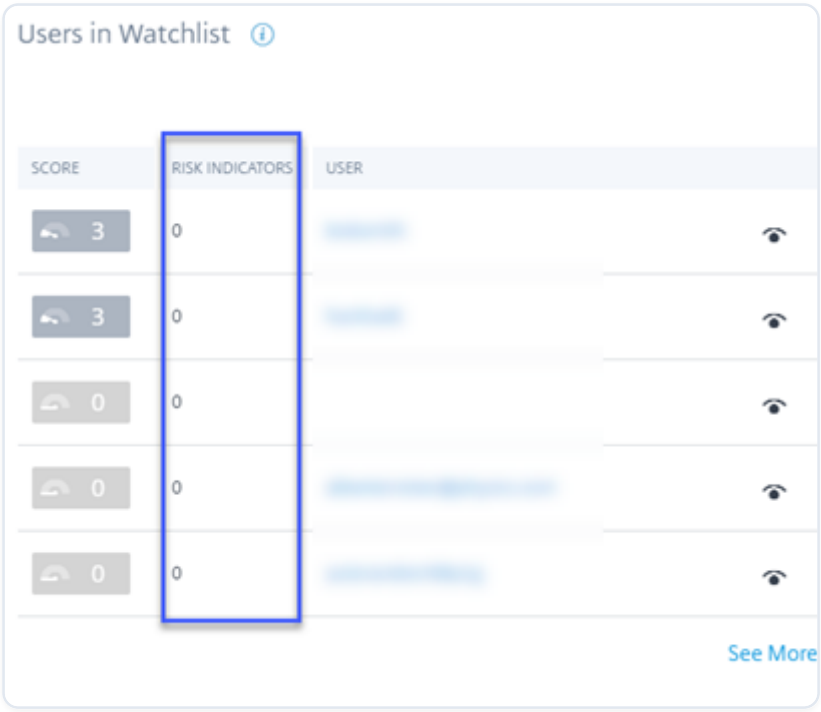
詳細については、リスクのあるユーザーを参照してください。



ウォッチリスト内のユーザーペインの機能強化

変更列は**リスクインジケーター**列に置き換えられました。**リスクインジケーター**列には、特定の期間におけるユーザーのリスクインジケーターの合計発生数が表示されます。

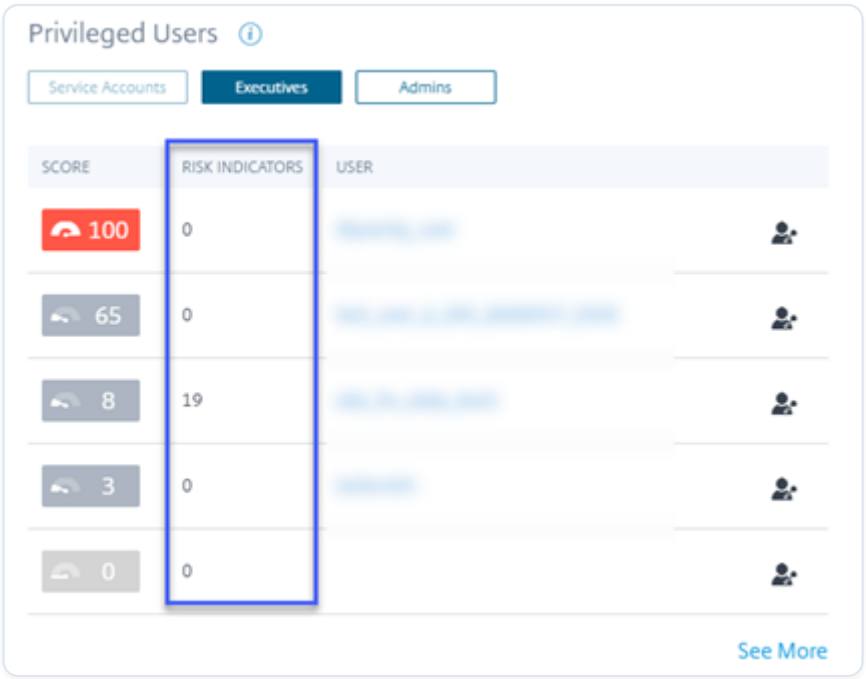
詳細については、ウォッチリスト内のユーザーを参照してください。



特権ユーザーペインの機能強化

- 「**Change**」列は「**Risk Indicators**」列に置き換えられました。「**Risk Indicators**」列には、特定の期間におけるユーザーの合計リスク指標発生数が表示されます。
- 「**See More**」をクリックすると、「**Users**」ページが表示されます。「**Users**」ページには、管理者およびエグゼクティブの特権ユーザーのリストが表示されます。このページで、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。

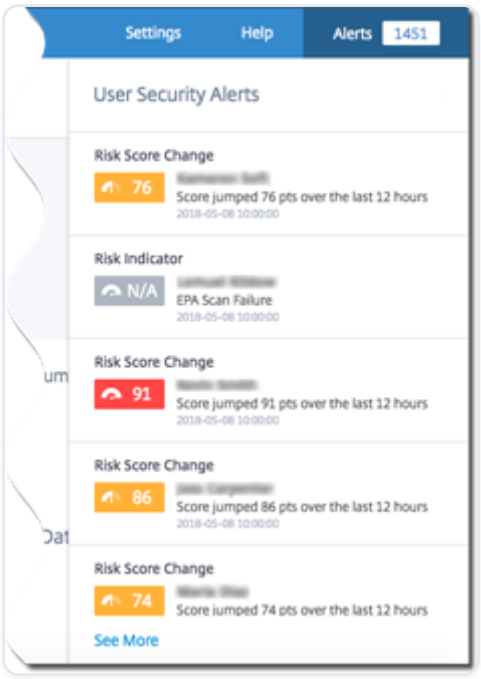
詳細については、「特権ユーザー」を参照してください。



非推奨の機能

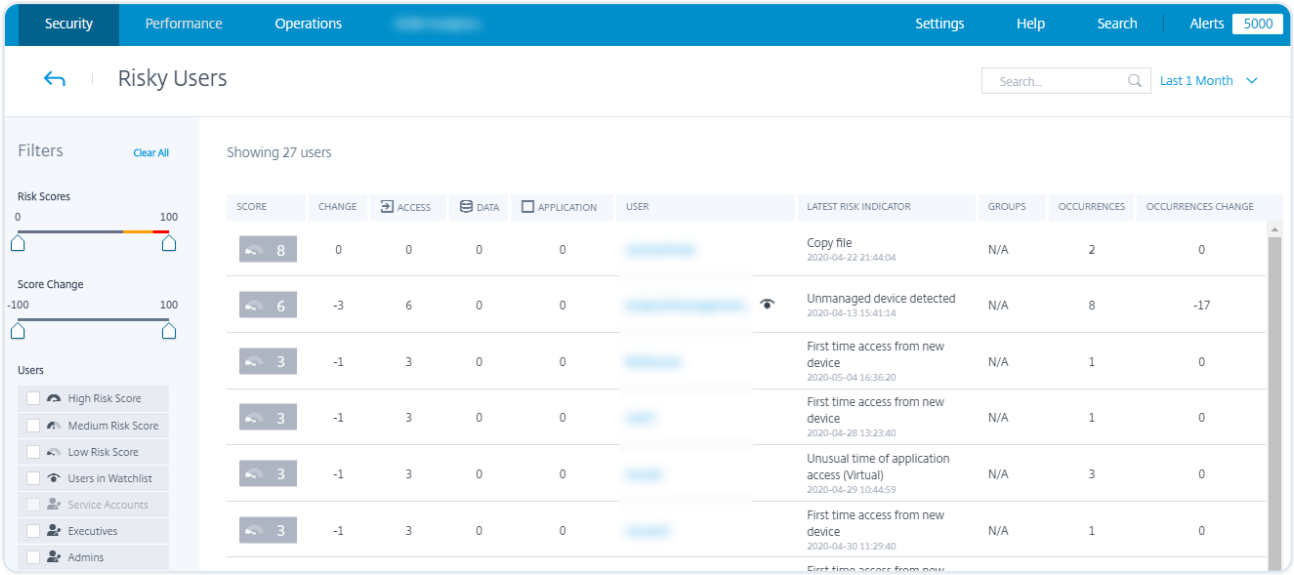
アラート

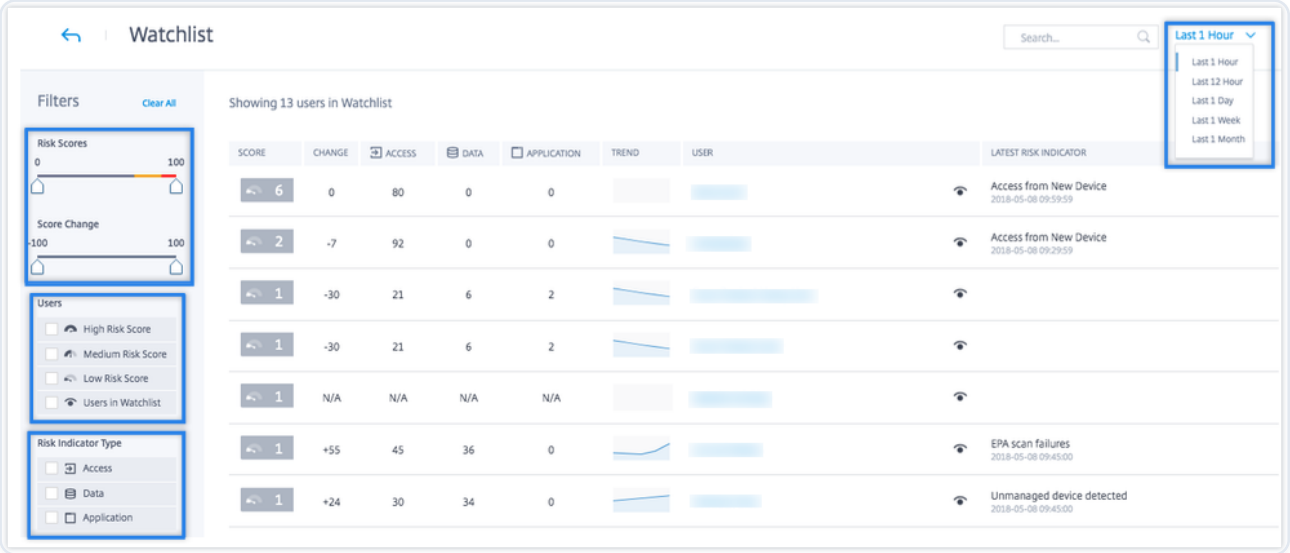
「**Alerts**」機能は非推奨となり、Analyticsユーザーインターフェースでは利用できなくなりました。



リスキーユーザーとウォッチリストのページ

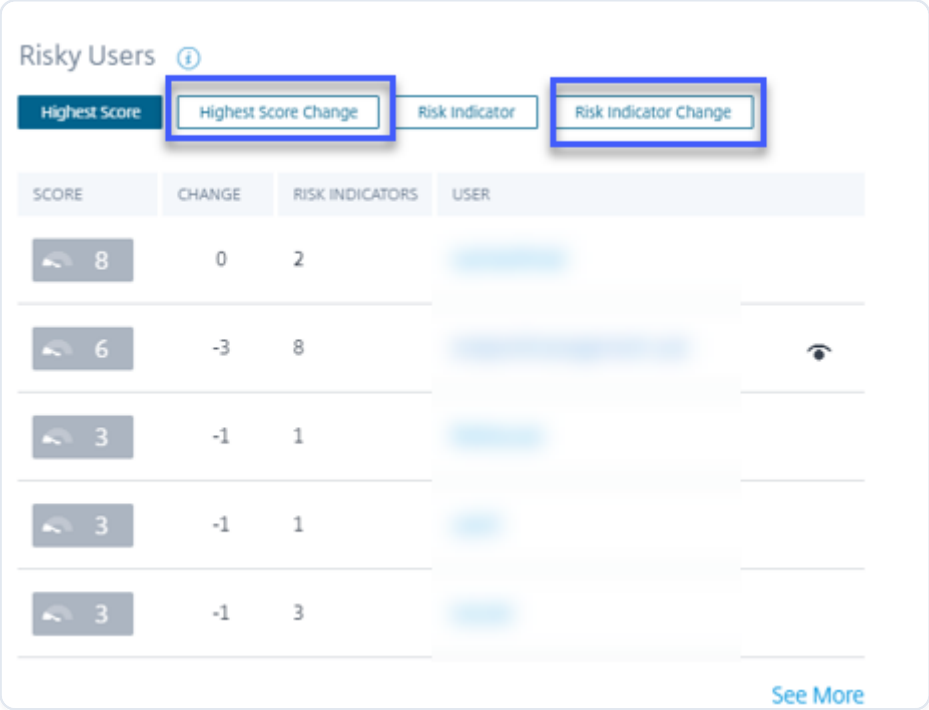
「**Risky Users**」ページと「**Watchlist**」ページは非推奨になりました。これらは、すべてのリスクのあるユーザーイベントとウォッチリスト内のユーザーをまとめた「**Users**」ページに置き換えられました。





リスキーユーザーペイン

「**Highest Score Change**」タブと「**Risk Indicator Change**」タブは、「**Risky Users**」ペインから削除されました。



リスクインジケーターペイン

- **発生変更**タブと**変更**列が削除されました。

  リスクインジケーターペイン(/en-us/citrix-analytics/media/risk-indicators-pane-deprecated-sections.png)

- **リスクインジケーターの詳細**ページは非推奨になりました。以前は、**リスクインジケーター**ペインまたは**リスクインジケーターの概要**ページでリスクインジケーターが選択されたときに、このページが表示されていました。

  リスクインジケーター詳細ページ(/en-us/citrix-analytics/media/risk-indicator-details-page-deprecated.png)

トレンドビュー

ユーザーダッシュボードで、**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**ウォッチリスト内のユーザー**カードから、ユーザー数のトレンドビューが削除されました。

トレンドビュー(/en-us/citrix-analytics/media/trend-deprecated.png)

ユーザーグループページ

設定オプションの下にある**ユーザーグループ**ページは非推奨になりました。特権グループとしてユーザーグループを追加または削除することは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することはできます。詳細については、「特権ユーザー」を参照してください。

ユーザーグループページ(/en-us/citrix-analytics/media/user-groups-page-deprecated.png)

June 26, 2020

非推奨の機能

アプリケーションアクセス時間の異常 (仮想/SaaS) リスクインジケーターが非推奨になりました

Citrix Virtual Apps and Desktops のリスクインジケーターである**アプリケーションアクセス時間の異常 (仮想)** および**アプリケーションアクセス時間の異常 (SaaS)** は非推奨になりました。これら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。

この非推奨化の一環として、以下の変更が適用されます。

- Analytics はこれらのリスクインジケーターを生成しなくなりました。
- Analytics は、これらのリスクインジケーターを条件とするポリシーを生成しなくなりました。
- これらのリスクインジケーターを条件とするデフォルトポリシーは、もはや有効になりません。

詳細については、「Citrix Virtual Apps and Desktops および Citrix DaaS のリスクインジケーター」(/ja-jp//security-analytics/risk-indicators/citrix-virtual-apps-and-desktops-risk-indicators.html)を参照してください。

June 02, 2020

修正された問題

- 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（ポリシーベースまたは手動適用）のステータスが「失敗」と表示されますが、実際にはアクションはユーザーアカウントに正常に適用されています。たとえば、**セッション記録の開始**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。

  アクション失敗ステータス(/en-us/citrix-analytics/media/cvad-action-failure.png)

May 11, 2020

修正された問題

- 一部のユーザーでは、ポリシーベースのアクションがトリガーされず、ポリシー適用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。

  ,

- 一部のユーザーに対してカスタムリスクインジケーターを作成できません。この問題は、顧客IDが小文字でない場合に発生します。

April 29, 2020

修正された問題

- Citrix Virtual Apps and Desktopsのリスクインジケーターに適用されたアクションは、Analyticsがアクションが正常に適用されたというメッセージを表示しても、有効になりません。この問題は、Citrix Virtual Apps and Desktops 7 1912バージョンで確認されています。

April 02, 2020

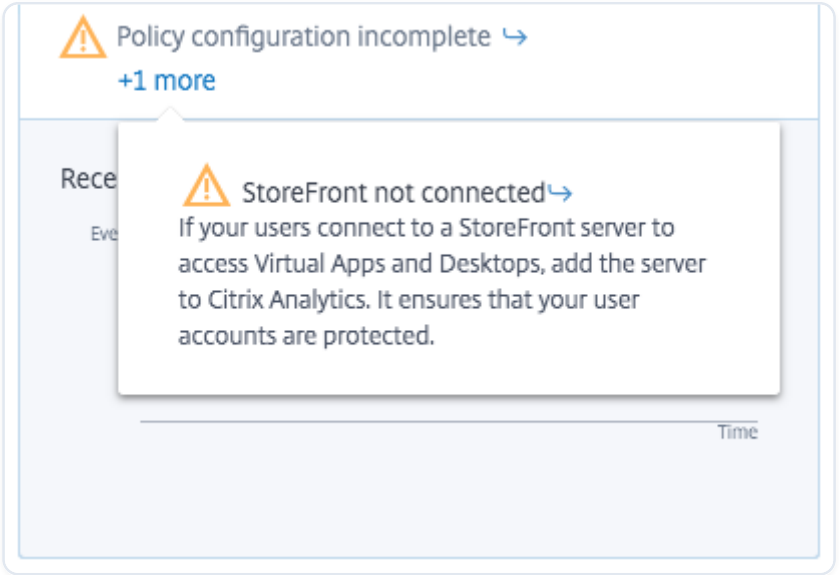
新機能

StoreFrontが追加されていない場合のデータ処理の無効化

「**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、StoreFrontをオンボーディングしていない場合、「**データ処理を有効にする**」ボタンは有効になりません。サイトカードに「**StoreFrontが接続されていません**」という警告メッセージが表示されます。Analyticsでデータを受信したい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ている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保護されます。

「**Virtual Apps and Desktops**」サイトカードで、縦の省略記号 (⋮) を選択し、「**StoreFront展開を接続**」をクリックします。表示される画面で、指示に従ってStoreFrontの設定を完了します。

詳細については、「StoreFrontを使用してCitrix Virtual Apps and Desktopsオンプレミスサイトをオンボーディングする」を参照してください。



修正された問題

- 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は有効になりません。
  - カスタムリスクインジケーターの条件が定義されている場合
  - ユーザーのリスクインジケーターが生成されるまで

March 04, 2020

修正された問題

- Gatewayユーザーが初めてAnalyticsにオンボーディングすると、**Citrix ADCが応答しないか、資格情報が正しくありません**というエラーが表示されます。再試行すると、**このIPアドレスを持つデバイスはすでに存在します**というエラーが表示されます。

February 20, 2020

新機能

シトリックス アナリティクス フォー セキュリティ の提供

Citrix Analytics for Security は、個別のサブスクリプションで利用可能になりました。 Citrix Analytics for Security を購読して、この提供に特化したインサイトを得ることができます。詳細については、Get started を参照してください。

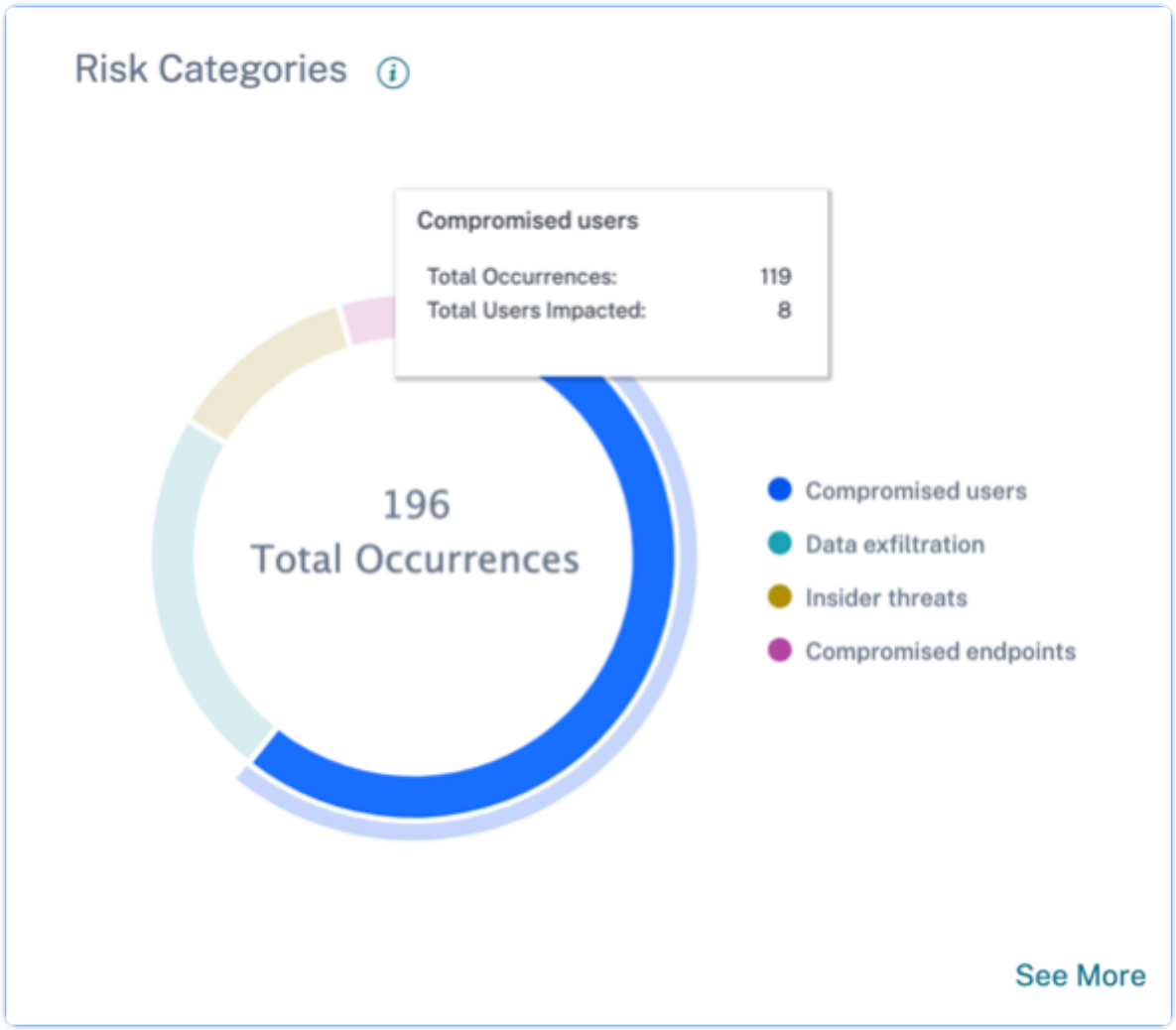
リスクカテゴリダッシュボード

Citrix Analyticsは、組織のセキュリティ面に同様の影響を与えるリスクに基づいて、リスクインジケータの分類を導入しています。このダッシュボードは、リスクエクスポージャーと即座の注意が必要な重大なリスクの包括的なビューを提供します。デフォルトのリスクインジケータの場合、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。カスタムリスクインジケータの場合、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は以下のリスクカテゴリをサポートしています。

- データ漏洩
- 内部脅威
- 侵害されたユーザー
- 侵害されたエンドポイント

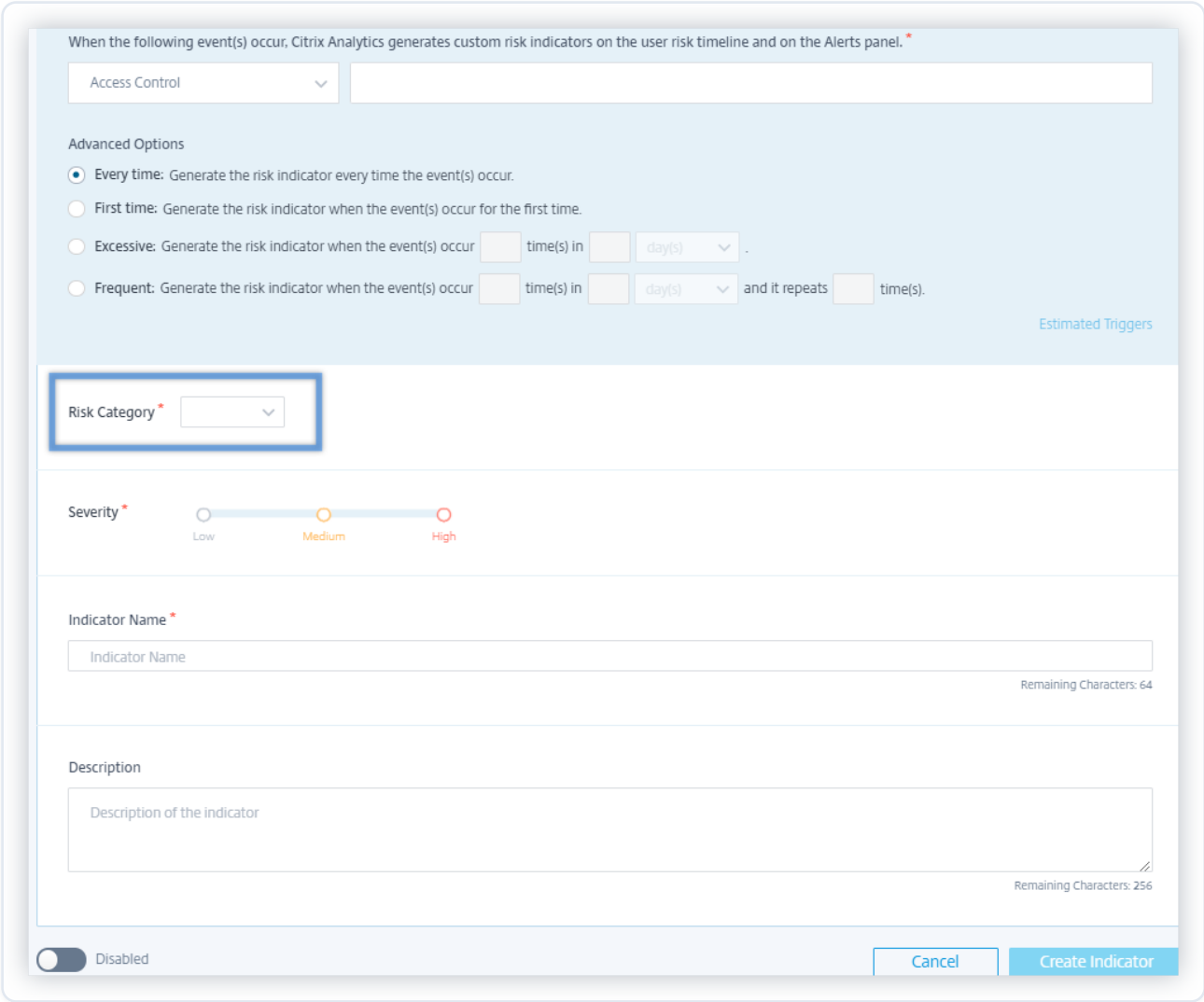
詳細については、「リスクカテゴリ」を参照してください。



カスタムインジケータページの「リスクカテゴリ」列

カスタムリスクインジケータページに**リスクカテゴリ**列が導入されました。リスクエクスポージャーの種類に基づいて、カスタムリスクインジケータのリスクカテゴリを選択できます。以前に作成されたカスタムリスクインジケータは、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、「カスタムリスクインジケータ」を参照してください。



リスクインジケータ名の変更

以下のリスクインジケータ名が変更されました。

データソース	旧名	新名
シトリックス バーチャル アプリケーションズ アンド デスクトップス および シトリックス DaaS	不審なアプリケーション使用状況（仮想）	不審なアプリケーションアクセス時間（仮想）
シトリックス バーチャルアプリおよびデスクトップとシトリックス DaaS	異常なアプリケーション使用状況 (SaaS)	異常なアプリケーションアクセス時間 (SaaS)
シトリックス コンテンツコラボレーション	過剰なログオン失敗	過剰な認証失敗

データソース	旧名	新名
シトリックス コンテンツコラボレーション	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
シトリックス アクセスコントロール	異常なダウンロード量	過剰なデータダウンロード
シトリックス ゲートウェイ	ログオン失敗	過剰な認証失敗
シトリックス ゲートウェイ	認証失敗	過剰な認証失敗
シトリックス ゲートウェイ	不審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、「リスクインジケーター」を参照してください(/ja-jp/security-analytics/risk-indicators.html)。

修正された問題

- 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が有効になっているにもかかわらず、Citrix AnalyticsはVirtual Apps and Desktopsからデータを受信できません。
- 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。そのため、以下のリスクインジケーターはトリガーされません。
    - 匿名による機密共有ファイルのダウンロード
    - 過剰な共有リンクのダウンロード
    - 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
- 新しくオンボードされたユーザーの場合、Citrix Gateway のリスクインジケーター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効果がありません。
- 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。

January 09, 2020

新機能

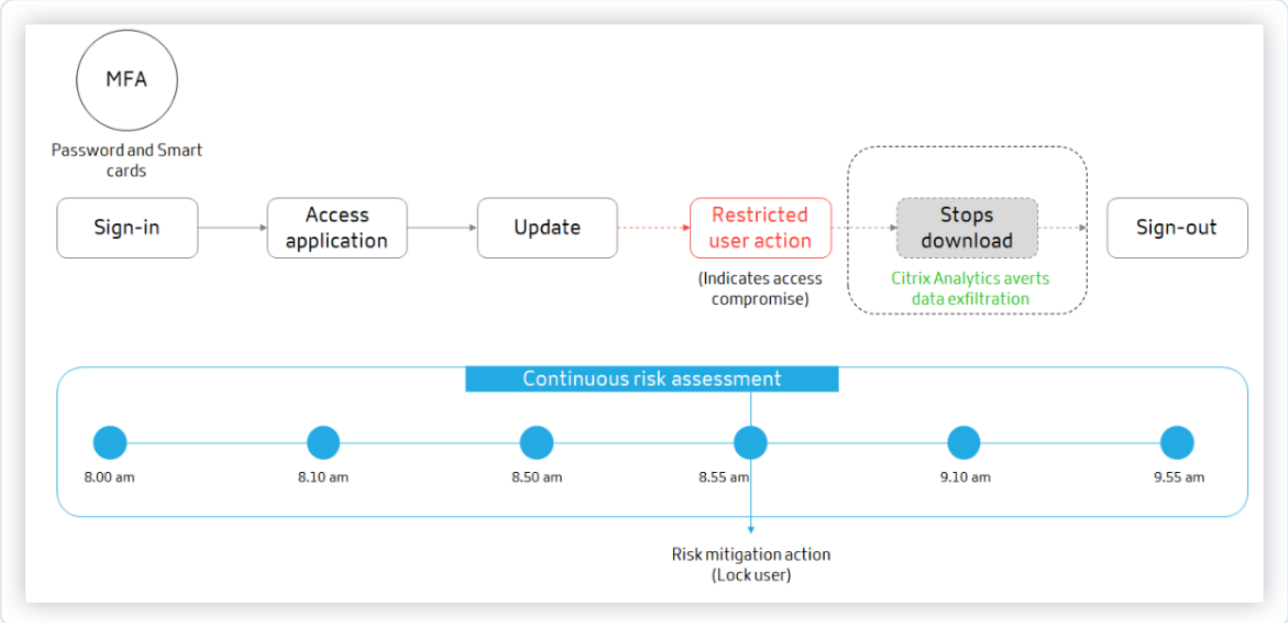
継続的なリスク評価

Citrix Workspace ユーザーが直面する課題のいくつかとして、リモートアクセスは、データ流出、盗難、破壊行為、サービス中断などのサイバー犯罪活動を通じて、機密データをセキュリティリスクにさらすという点があります。組織内の従業員も、この損害に寄与する可能性があります。

これらのリスクに対処する方法としては、多要素認証の実装、短いサインインタイムアウトの強制などが挙げられます。これらのリスク評価方法はより高いレベルのセキュリティを保証しますが、初期検証後の完全なセキュリティを提供するものではありません。

セキュリティ面を強化し、より良いユーザーエクスペリエンスを確保するために、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。



ポリシー構成

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。以下の機能を利用して、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、以下のデフォルトポリシーをサポートしています。

- 認証情報の悪用成功
- 潜在的なデータ流出
- 不審なIPからの異常なアクセス
- 異常な場所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

要件に基づいてデフォルトポリシーを変更できます。

デフォルトポリシー(/en-us/citrix-analytics/media/default-policies.png)

- **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インジケーターの組み合わせ、またはその両方で設定できます。

  条件の追加と削除(/en-us/citrix-analytics/media/policy-add-remove-condition.png)

- **デフォルトおよびカスタムのリスクインジケーター**: **ポリシーの作成**ページにある条件メニューは、デフォルトとカスタムのリスクインジケーター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際、デフォルトとカスタムのリスクインジケータータブを切り替えて、リスクインジケーターの条件を設定できます。

  条件の追加と削除(/en-us/citrix-analytics/media/policy-default-custorm-ri-tabs.png)

- **エンドユーザー応答の要求**: Citrix Analyticsは、**エンドユーザー応答の要求**アクションを導入しました。このアクションを使用すると、検出された危険なアクティビティについてユーザーに電子メール通知を送信できます。ユーザーがアクティビティについて応答すると、そのアカウントに対して次に取るべきアクションを決定できます。ユーザーの応答時間も設定できます。応答がない場合、Citrix Analyticsはステータスを**応答なし**と見なします。

  エンドユーザー応答の要求(/en-us/citrix-analytics/media/request-end-user-response-email.png)

- **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**などの中断アクションが適用された場合、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。このアクションは、さらなる悪用を防ぐために、ユーザーアカウントへのサービスを一時的に中断します。アカウントへのアクセスを継続するには、ユーザーは管理者に連絡してサポートを求める必要があります。

  中断アクションの適用(/en-us/citrix-analytics/media/disruptive-action-email-preview.png)

- **適用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。

  「ポリシーモード」(/en-us/citrix-analytics/media/policy-modes.png)

ポリシーの機能強化について詳しくは、「ポリシーとアクション」(/ja-jp/security-analytics/policies-and-actions.html)を参照してください。

ユーザーのロックとユーザーのロック解除アクション

Citrix Analyticsには、次のGateway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、手動で適用することも、ポリシーを設定するときに適用することもできます。

詳しくは、「アクションとは」(/ja-jp/security-analytics/policies-and-actions.html#what-are-the-actions)を参照してください。

「次に、以下を実行します」(/en-us/citrix-analytics/media/policies-actions-menu.png)

アクセス概要ダッシュボード

Citrix Analyticsには、**ユーザー**ダッシュボードに**アクセス概要**パネルが導入されています。このパネルには、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がまとめられています。

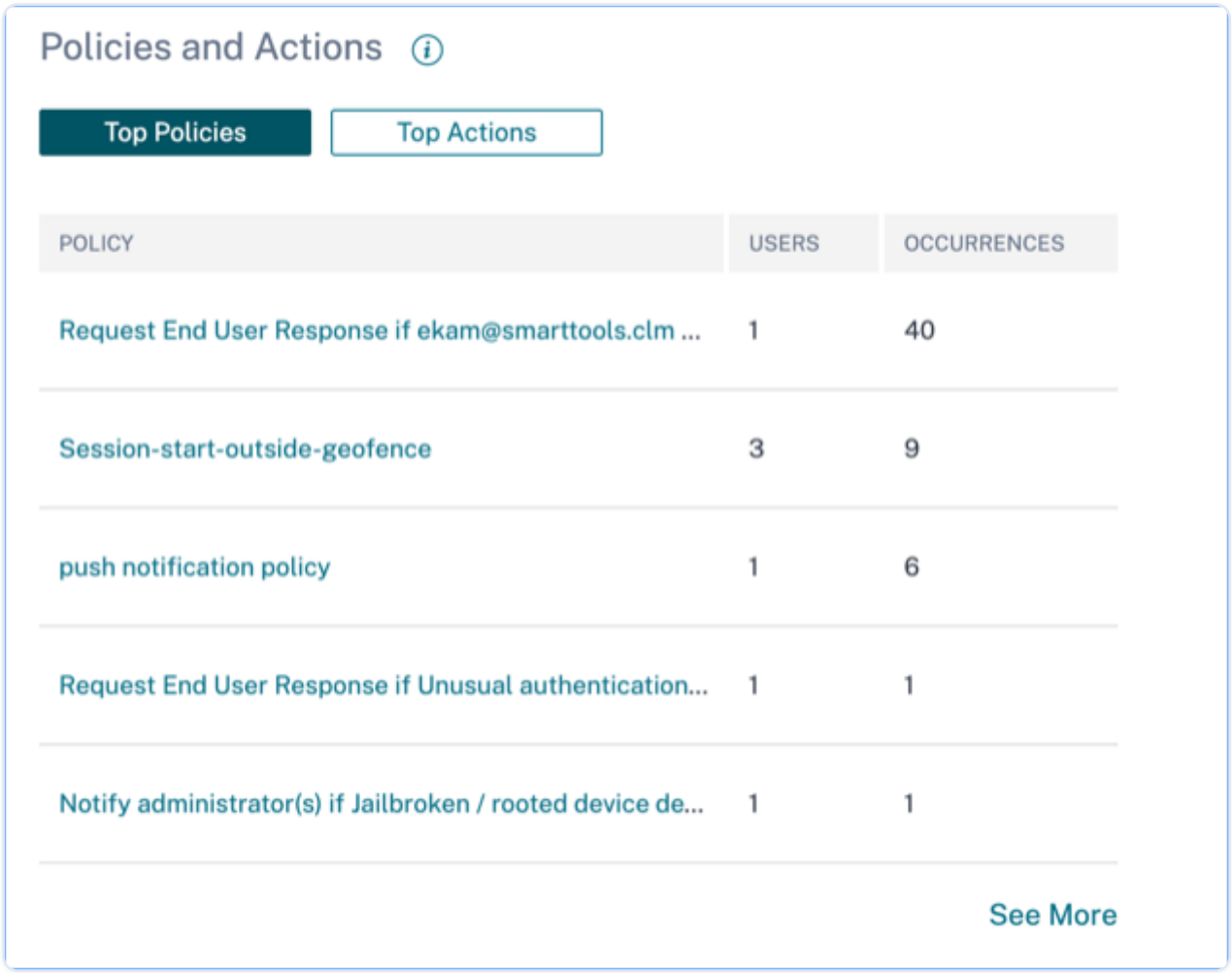
詳しくは、「アクセス概要」(/ja-jp/security-analytics/users-dashboard.html#access-summary)を参照してください。

「アクセス概要ダッシュボード」(/en-us/citrix-analytics/media/access-summary-dashboard.png)

ポリシーとアクションのダッシュボード

Citrix Analyticsには、**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。このパネルには、ユーザープロファイルに適用された上位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並べ替えることができます。

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。



ポリシーのセルフサービス検索

定義したポリシーに合致したユーザーイベントを表示するには、セルフサービス検索を使用します。また、Analytics がこれらの異常なイベントに適用したアクションも表示できます。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、期間を選択してから、**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。

非推奨の機能

リスクスコア変更ポリシーベース条件の削除

ポリシーを設定する際、**リスクスコア変更**ポリシーベース条件は使用できなくなりました。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アクションの削除

ポリシーを設定する際、複数のアクションを適用することはできなくなりました。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ています。

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。

修正された問題

- 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**アプリアクセス**ダッシュボードにアクセスする際にエラーが発生します。

December 12, 2019

新機能

Splunkのバージョンサポート

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メリット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。

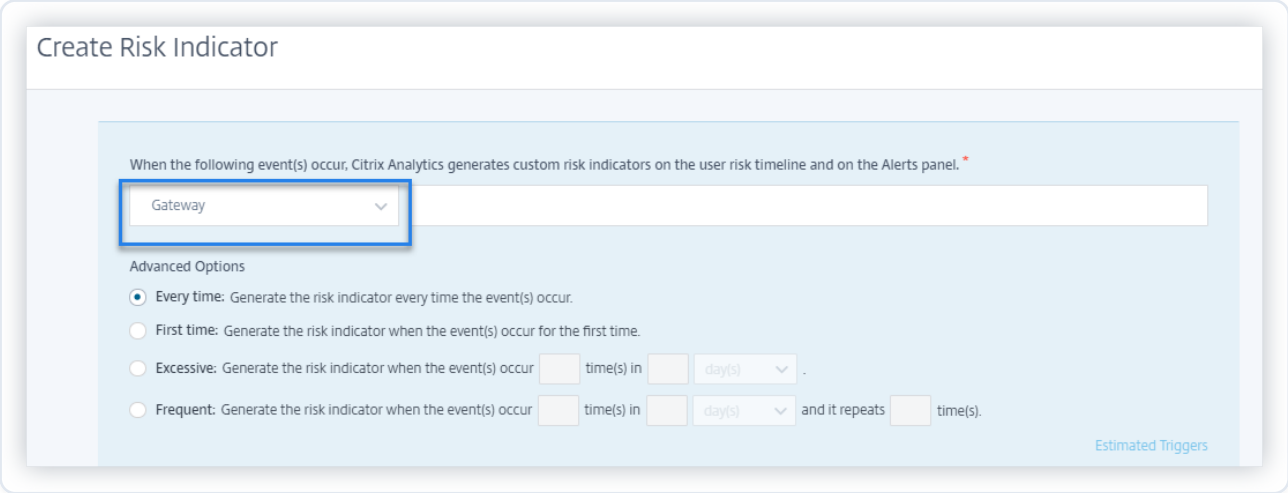
サポートされているSplunkのバージョンについて詳しくは、サポートされているバージョンを参照してください。

December 04, 2019

新機能

Citrix Gatewayのカスタムリスクインジケーター

カスタムリスクインジケーターを使用すると、Citrix Gatewayイベントのリスクインジケーターをトリガーする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はリスクインジケーターをトリガーします。カスタムリスクインジケーターの作成方法について詳しくは、カスタムリスクインジケーターを参照してください。



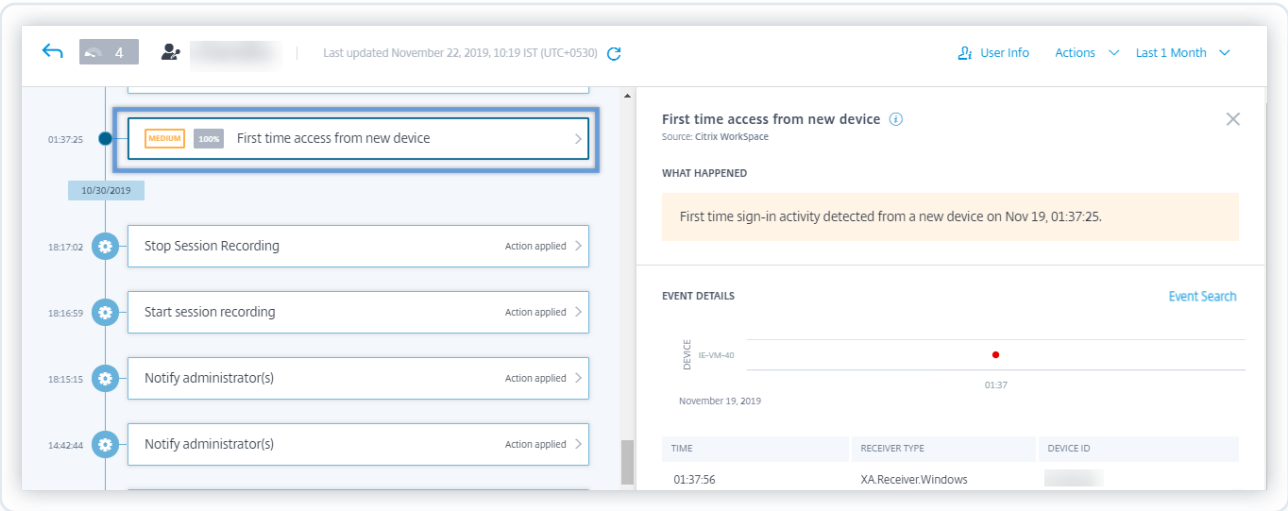
November 22, 2019

新機能

新しいデバイスからの初回アクセス – Citrix Virtual Apps and Desktops リスクインジケーター

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脅威を検出し、対応するリスクインジケーターをトリガーします。

新しいデバイスからの初回アクセスリスクインジケーターは、ユーザーが90日ぶり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 が過去90日間、この新しいまたはなじみのないデバイスからのサインイン記録を持っていないためにトリガーされます。詳細については、「Citrix Virtual Apps and Desktops および Citrix DaaS のリスクインジケーター」を参照してください。

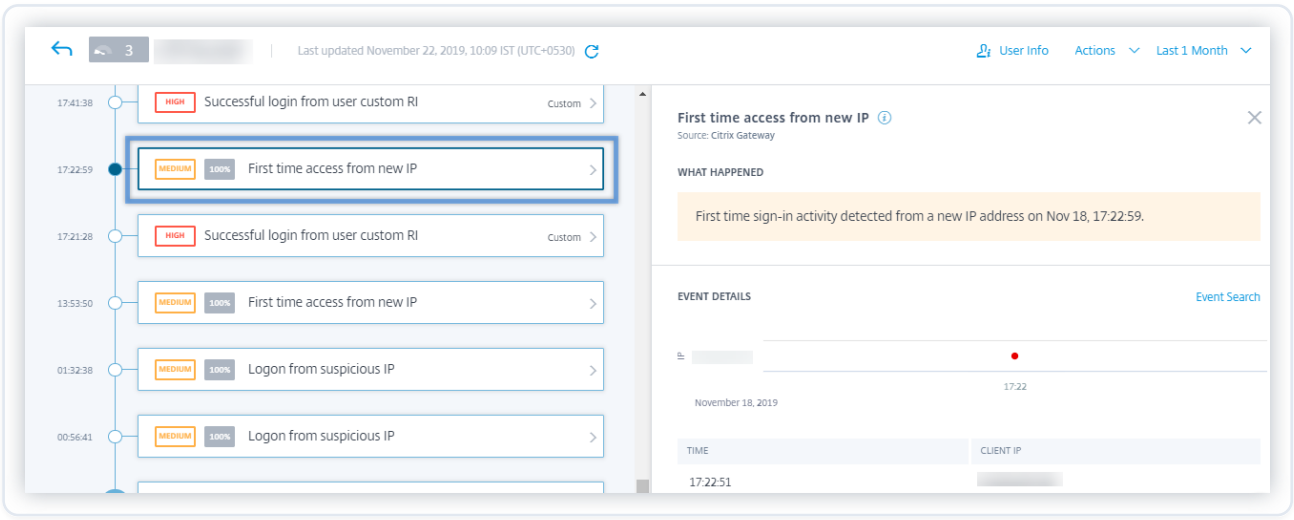


新しいIPからの初回アクセス – Citrix Gateway リスクインジケーター

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脅威を検出し、対応するリスクインジケーターをトリガーします。

新しいIPからの初回アクセスリスクインジケーターは、ユーザーが90日ぶりに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 が過去90日間、この新しいまたはなじみのないIPアドレスからのサインイン記録を持っていないためにトリガーされます。

詳細については、「Citrix Gateway のリスクインジケーター」を参照してください。



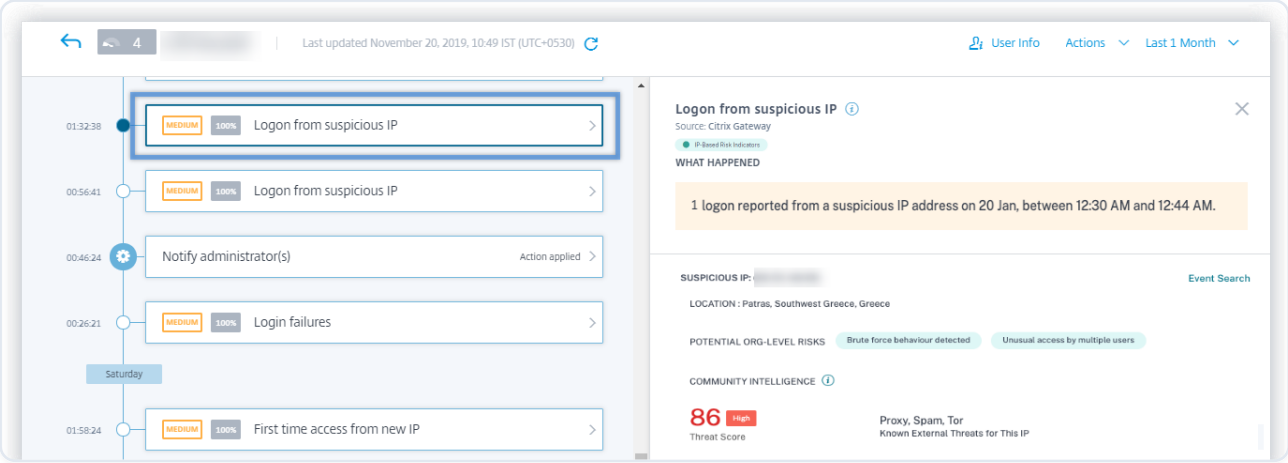
不審なIPからのログオン – Citrix Gateway リスクインジケーター

Citrix Analytics は、不審な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脅威を検出し、**不審なIPからのログオン**リスクインジケーターをトリガーします。

このリスクインジケーターは、ユーザーが不審な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 は、以下のいずれかの条件に基づいてIPアドレスを不審と見なします。

- 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
- 異常な場所からの複数のユーザーサインイン記録がある
- ブルートフォース攻撃を示す可能性のある過剰なサインイン失敗試行がある

詳細については、Citrix Gateway のリスクインジケーターを参照してください。



Citrix 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、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インサイトを取得します。Citrix Analytics は、Citrix 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、基になるデータを探索します。

イベントを表示するには、検索ボックスでリストから **Gateway** を選択し、期間を選択してから、**Search** 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して、Citrix Remote Browser Isolation Service から受信したブラウジング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、基になるデータを探索します。

イベントを表示するには、検索ボックスでリストから **Remote Browser Isolation** を選択し、期間を選択してから、**Search** 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。

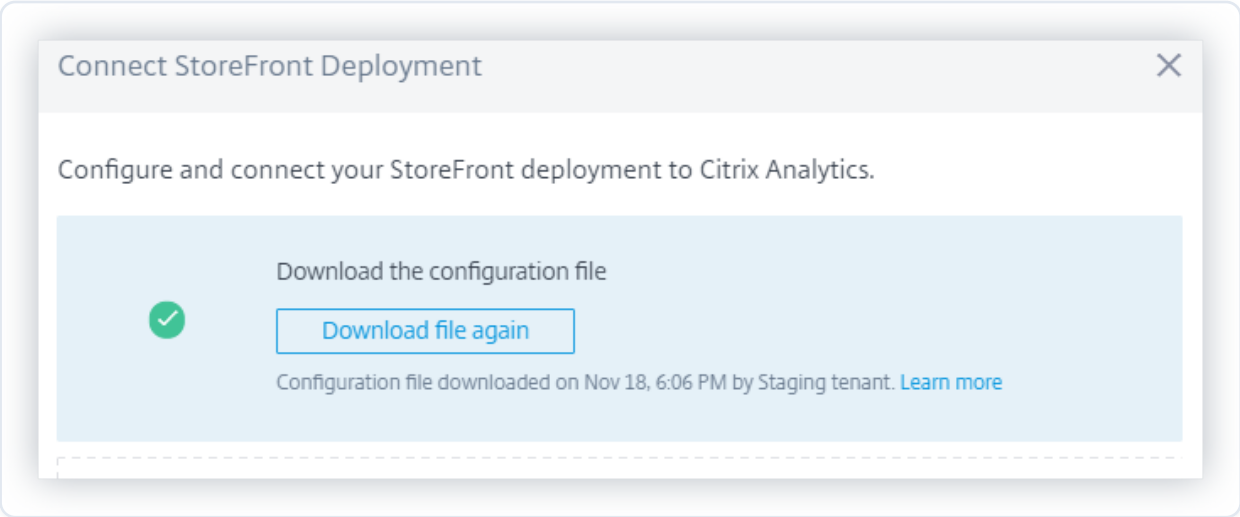
ウォッチリストから削除アクション

ウォッチリストからユーザーを削除するには、手動の方法を適用するか、ポリシーベースの方法を適用します。詳細については、「ウォッチリスト」を参照してください。

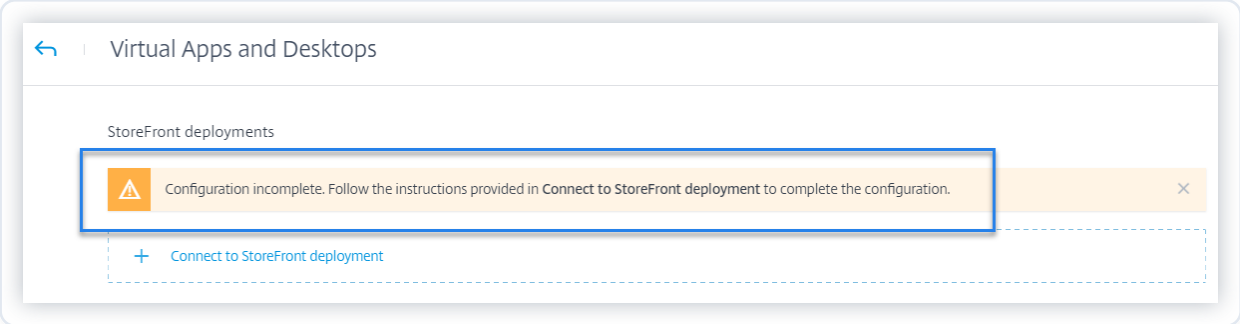
StoreFront 展開の構成時のオンボーディングメッセージの改善

Citrix Analytics は、StoreFront 展開の構成に役立つ次のメッセージを提供するようになりました。

- 構成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、**Download file** ボタンが **Download file again** に変わります。



- StoreFrontの設定が不完全な場合、設定手順に従ってStoreFront展開をAnalyticsに接続するよう指示する警告メッセージが表示されます。



StoreFront展開の構成方法の詳細については、「StoreFrontを使用してCitrix Virtual Apps and Desktopsオンプレミスサイトをオンボードする」を参照してください。

非推奨の機能

リスクインジケーター - 新しいデバイスからのアクセス削除

Citrix Analyticsは、**新しいデバイスからのアクセス**リスクインジケーター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、このリスクインジケーター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されたポリシーについては、ポリシーを変更するか、新しいリスクインジケーターである**新しいデバイスからの初回アクセス**を使用してポリシーを作成する必要があります。

修正された問題

- 認証のセルフサービス検索でイベントが表示されません。

November 08, 2019

修正された問題

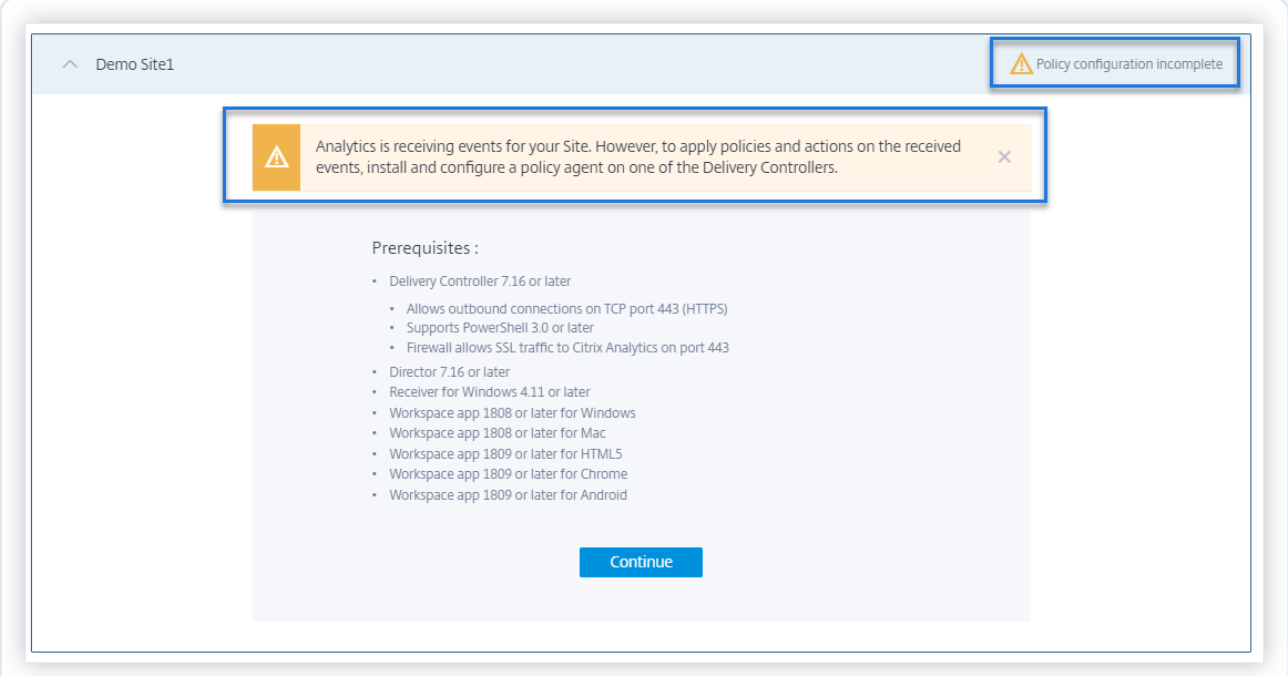
- Citrix Content Collaborationのリスクインジケーターの場合、ユーザーはリスクタイムラインでアクションを適用できません。
- バージョン1911より前のChrome用Citrix Workspaceアプリは、イベントの詳細をCitrix Analyticsに送信できません。

October 21, 2019

新機能

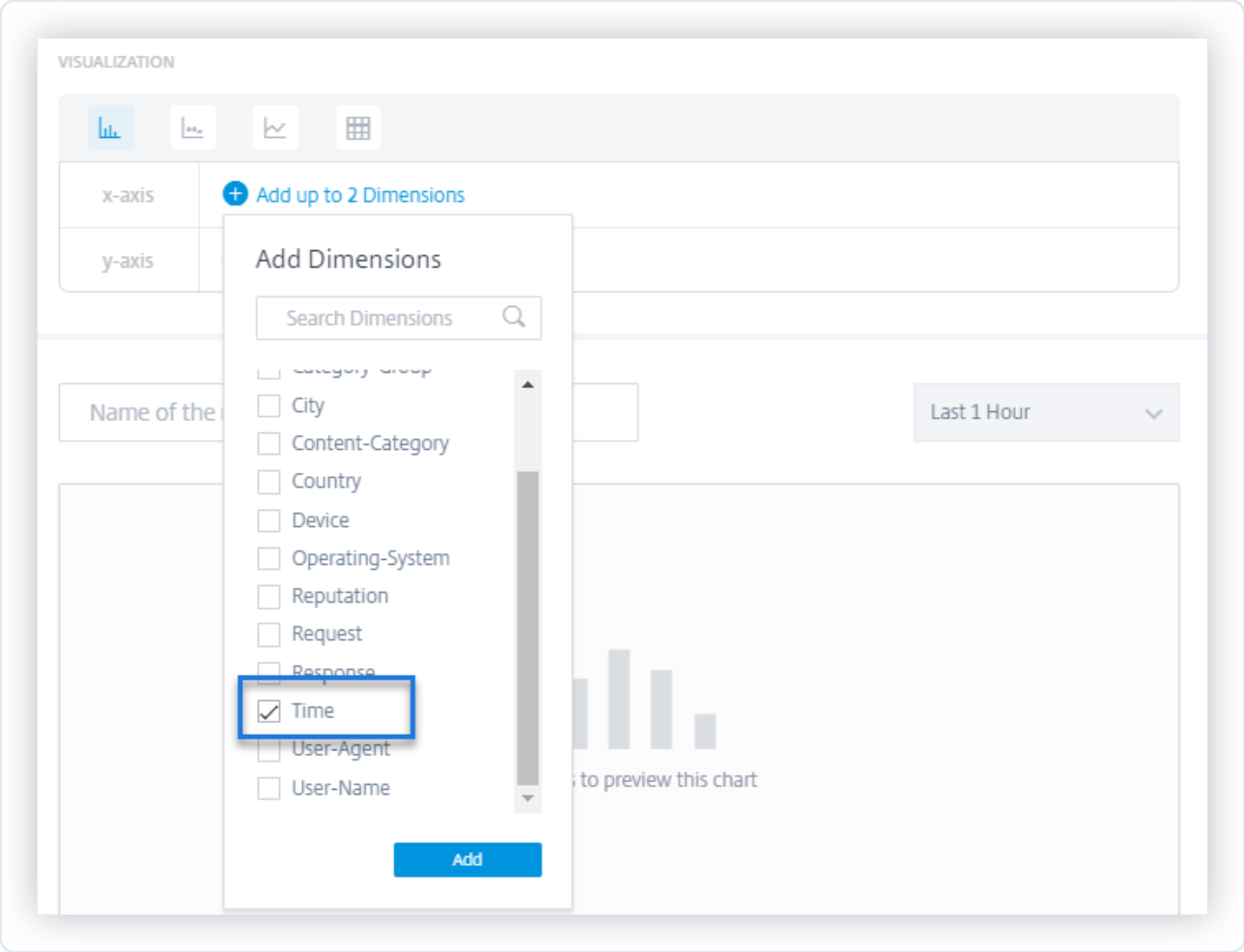
アナリティクスエージェントの名称変更

エージェント名は、その役割を示すためにユーザーインターフェイスで**Analytics policy agent**と表記されるようになりました。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際、Citrix Analyticsは、ポリシーエージェントがサイトのポリシーとアクションを設定するためにのみ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、データソースからのデータ送信には関与しません。詳細については、「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軸に**時間**ディメンションを選択することで、イベントを時間に基づいて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され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。

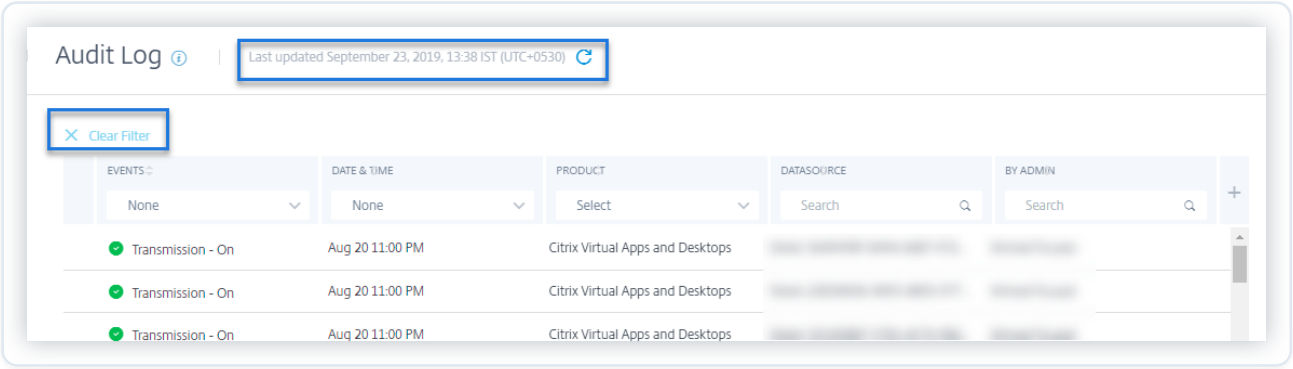


監査ログの機能強化

監査ログページのユーザーエクスペリエンスが向上しました。

- **監査ログ**ページが最後に更新された日時を表示し、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ーをクリアできます。

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。



修正された問題

- Microsoft Graph Securityが正常にオンボーディングされていても、Citrix Analyticsは**匿名IPアドレス**のリスクインジケーターを生成できません。
- Citrix Workspace app for HTML5 バージョン 1910 より前のバージョンでは、イベントの詳細を Citrix Analytics に送信できません。

September 23, 2019

修正された問題

- データソースサイトカードで、**最新イベント**フィールドに誤った日時情報が表示されます。

August 30, 2019

新機能

ダッシュボード全体のデフォルト期間の変更

以下のダッシュボードのデフォルト期間が、**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
- 共有リンク
- アラート履歴

現在、ダッシュボードはデフォルトで過去1か月間のイベントを表示します。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、**アプリアクセス**

ダッシュボードを開くと、ダッシュボードはデフォルトで過去1か月間のアプリアクセスイベントを表示します。

デフォルトの時間範囲の選択(/en-us/citrix-analytics/media/default-time-change.png)

修正された問題

- コンテンツコラボレーションのリスクインジケーターの場合、**ユーザーを無効にする**ポリシーベースのアクションを正常に適用できません。
- Citrix AnalyticsはCitrix Gateway 13.0からのイベントを処理できません。この問題は、Citrix 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。

August 20, 2019

新機能

セルフサービス検索の強化

- 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。これで、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間をシームレスに切り替えることができます。
- イベントを時間で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に最初に表示されます。**時間**列の並べ替えアイコンをクリックして、最新の時間または最も古い時間のいずれかに基づいてイベントを並べ替えます。

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。(/ja-jp/security-analytics/self-service-search.html).

カスタムレポートの強化

- アクセス制御、コンテンツコラボレーション、およびアプリとデスクトップの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。データソースには次のディメンションが追加されています。
    - **アクセス制御**: ユーザーエージェント、ユーザー名
    - **コンテンツコラボレーション**: ユーザーメール、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、ジェイルブレイク済み、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、印刷プリンター名、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

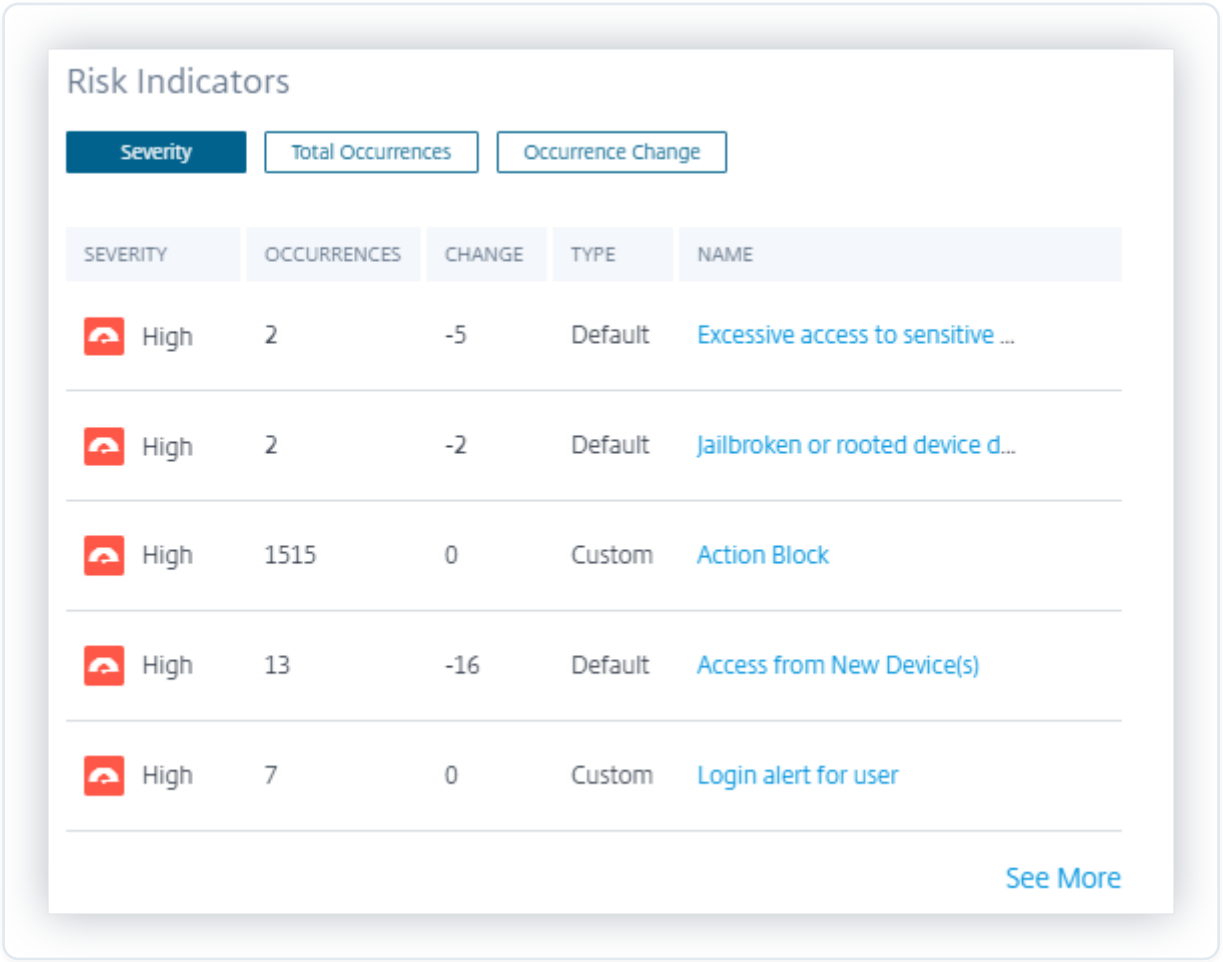
- カスタムレポートのユーザーインターフェイスは、ページネーションのサポートと、フィルターの**すべてクリア**オプションにより強化されました。

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。

リスクインジケーターダッシュボード

ユーザーページに**リスクインジケーター**ダッシュボードが導入されました。これには、ユーザーの上位5つのデフォルトおよびカスタムリスクインジケーターが要約されています。「さらに表示」リンクをクリックすると、**リスクインジケーターの概要**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インジケーター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。

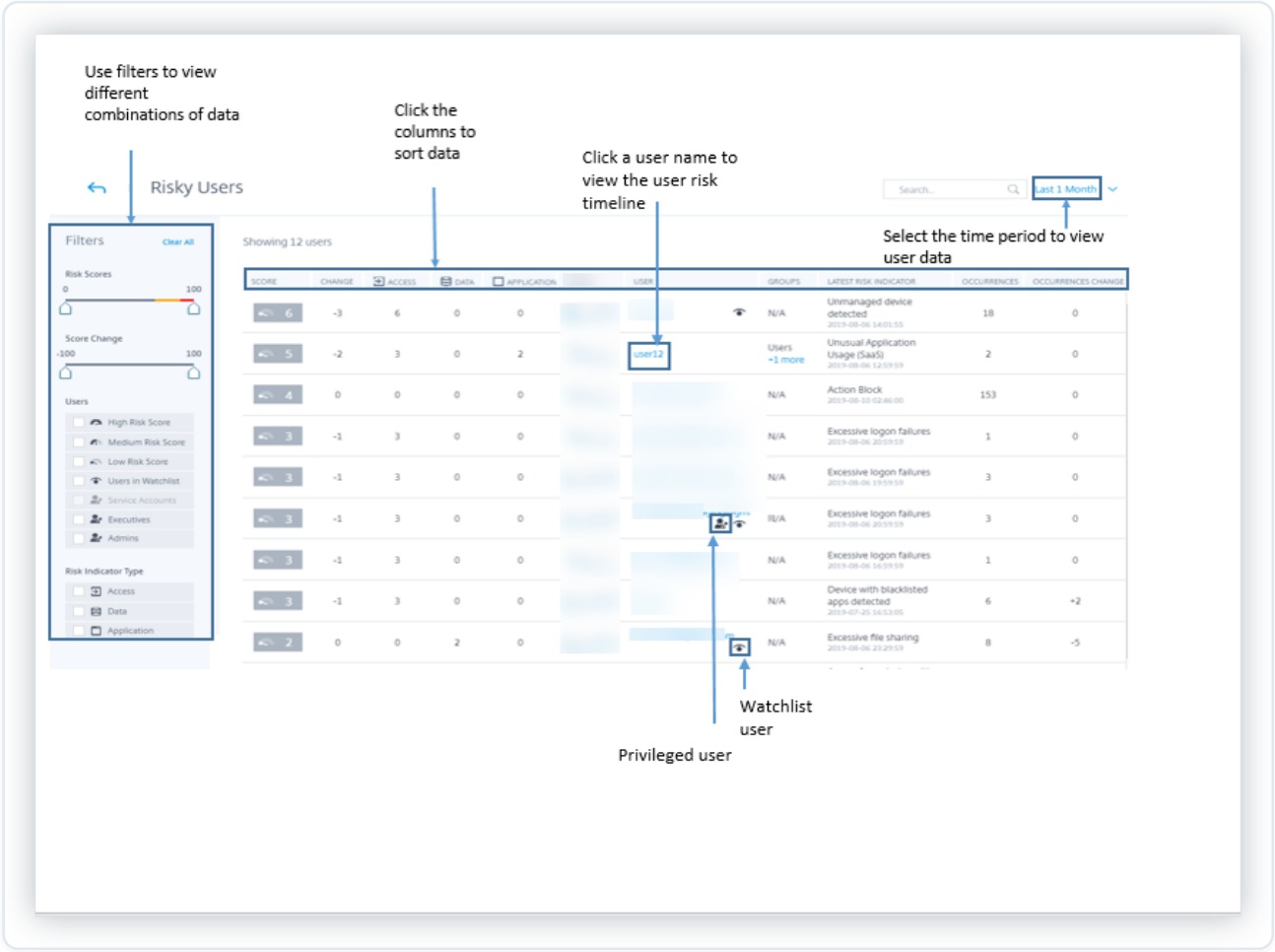


リスキーユーザーダッシュボードの機能強化

Citrix Analyticsでは、**リスキーユーザー**ダッシュボードに**リスクインジケーター**タブと**リスクインジケーターの変更**タブが導入されました。これらのタブに基づいて、上位5つのリスキーユーザーを表示できます。ダッシュボードには、**リスクインジケーター**列も導入されています。これには、ユーザーのリスクインジケーターの数が表示されます。

リスキーユーザーページには、**発生回数**列と**発生回数の変更**列が導入されています。これらの列には、カスタムおよびデフォルトのリスクインジケーターの合計発生回数と発生回数の変更が要約されています。

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。



共有リンクのリスクインジケーター - 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脅威を検出し、**過剰なダウンロード**リスクインジケーターをトリガーします。以前の動作に基づいて過剰なダウンロードを伴う共有リンクを特定することで、潜在的な攻撃に対して共有リンクを監視できます。このリスクインジケーターは、過剰なファイルダウンロードアクティビティを特定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、Citrix Cloud の Identity and Access Management サービスから、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受信します。この検索機能は、認証イベントに関する詳細なレポートを提供し、認証の問題を特定してトラブルシューティングするのに役立ちます。定義した条件に一致するイベントを取得するための検索クエリを定義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 を選択し、期間を選択してから、 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。

July 11, 2019

新機能

カスタムリスクインジケーター

Citrix Analytics が生成するデフォルトのリスクインジケーターは、機械学習アルゴリズムに基づいています。Citrix Analytics では、カスタムリスクインジケーター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、カスタムリスクインジケーターを作成できます。

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インジケーターと同様にカスタムリスクインジケーターを生成し、ユーザーのリスクタイムラインに表示します。カスタムリスクインジケーターは、ユーザーのリスクタイムライン上でラベルで示されます。

詳細については、「カスタムリスクインジケーター」を参照してください。

リスクタイムライン上の特権ステータス

ユーザーの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の特権ステータスに変更があった場合に、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
- 管理者特権が削除されました

ユーザーのリスクインジケーターがトリガーされた場合、指定された特権ステータス変更イベントと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、「ユーザーリスクタイムライン」を参照してください。

共有リンクの有効期限切れアクション

Citrix Analyticsでは、共有リンクのリスクインジケーター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、**共有リンクの有効期限切れ**です。

詳細については、「Citrix共有リンクのリスクインジケーター」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、任意の文字に0回以上一致させます。たとえば、検索クエリ「User-Name = "John*"」は、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。
- **ファセットに「すべてクリア」オプションを追加**: **すべてクリア**をクリックすると、選択したすべてのファセットを一度に削除できます。
- **イベントリストで非表示の列データを表示**: イベントテーブルから列を削除した後、ユーザーイベントリストで対応するデータを表示します。ユーザーのイベント行を展開して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状態

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かった場合、サイトカードには赤色で**データが受信されていません**というラベルが表示されます。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を確認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利用可能です。

詳細については、「CitrixデータソースでAnalyticsを有効にする」を参照してください。

修正された問題

- Access Controlデータソースの場合、サイトカード上のイベント数がセルフサービス検索結果と一致しません。

June 19, 2019

修正された問題

- **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、データ送信のオン/オフステータスが表示されます。
- **ユーザー**ダッシュボードの時間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。
- Splunkからテナントに接続する際に、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時々失敗します。

June 17, 2019

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、StoreFrontをCitrix Analyticsに接続するように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、ユーザーの行動に関する実用的なインサイトを生成します。これらのインサイトは、異常なユーザー行動を検出し、組織内のセキュリティ脅威にプロアクティブに対処するのに役立ちます。詳細については、「StoreFrontを使用してCitrix Virtual Apps and Desktopsオンプレミスサイトをオンボードする」を参照してください。

May 30, 2019

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脅威を検出し、「過剰なログオン失敗」リスクインジケーターをトリガーします。このリスクインジケーターは、ユーザー

がContent Collaborationへのアクセスに複数回失敗した場合にトリガーされます。以前の行動に基づいて過剰なログオン失敗のあるユーザーを特定することで、管理者はブルートフォース攻撃に対してユーザーアカウントを監視できます。

> **注**
>
> **過剰なログオン失敗**は、**過剰な認証失敗**に名称変更されました。

修正された問題

- Citrix Workspaceアプリによって送信された一部のユーザーイベントについて、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。
- **ユーザー**ダッシュボードは、**過去1か月**の期間で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エラーが発生することもあります。
- 一部のユーザーがCitrix Cloudでサービスを購読しているにもかかわらず、Citrix Content Collaborationがデータソースとして検出されません。

May 09, 2019

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は、選択したデータソースに応じて、ディメンションとメトリックのリストを提供します。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、テーブルなどの視覚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ことで、データをグラフィカルに整理および分析できます。

カスタムレポートを作成するには、**セキュリティ**タブから、**レポート** > **レポートの作成**をクリックします。以前に作成したレポートを表示するには、**セキュリティ**タブから、**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行動異常を綿密に監視できます。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るため、彼らの日常的な活動と悪意のある活動を区別することは困難です。そのため、特権ユーザーの悪意のある活動は長期間検出されないままになります。この機能を使用すると、そのような活動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 は、次の種類の特権ユーザーの監視をサポートしています。

- **管理者** - 各 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。
- **役員** - Citrix Analytics では、AD グループを役員グループとしてマークできます。AD グループを役員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行動異常をさらにサポートする必要がなくなった場合は、そのグループを役員グループから削除できます。

詳細については、「特権ユーザー」を参照してください。

週次メールサマリー

Citrix Analytics は、組織の IT 環境におけるセキュリティリスクの露出をまとめた週次メールを管理者に送信します。この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を強調表示します。このメールにより、管理者は Citrix Analytics にサインインすることなく、セキュリティリスクの露出について通知されます。詳細については、「週次メールサマリー」を参照してください。

April 26, 2019

新機能

委任された管理者

Citrix Analytics は、委任された管理者ロールをサポートするようになりました。この機能により、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 管理者である場合、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、委任された管理者と呼ばれます。現在、委任された管理者に

は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。

修正された問題

データストリーミングを使用するデータソースの一部のリスクインジケーターは、アラートを生成しません。次のいずれかのリスクインジケーターがトリガーされても、アラート通知は受信されず、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 のリスクインジケーター** - 管理対象外のデバイス、ジェイルブレイクまたはルート化されたデバイス、ブラックリストに登録されたアプリを含むデバイス。
- **Citrix Virtual Apps and Desktops のリスクインジケーター** - 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 リスクインジケーター** - 機密ファイルへの過剰なアクセス。

February 19, 2019

新機能

Splunk連携

Citrix AnalyticsはSplunkと連携し、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向上させます。この連携により、既存のデータソースが、リスクインジケーター、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で強化されます。Citrix Analyticsはリスク分析情報をチャネルにエクスポートし、Splunkはそのチャネルから情報を取り込みます。

Splunk連携には、Citrix Analyticsでの構成、**Citrix Analytics Add-on for Splunk**アプリのインストール、およびアプリの構成が含まれます。少なくとも1つのデータソースでデータ処理をオンにしてください。これにより、Citrix AnalyticsはSplunk連携プロセスを開始できます。

詳細については、「Splunk連携」を参照してください。

動的セッション記録

Citrix Analytics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を提供します。これにより、リスク分析に必要な証拠をキャプチャし、セッションの切断やユーザーのブロックなどの適切なインシデント対応アクションを実行できます。

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。

共有リンクダッシュボードとリスクインジケーター

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。これにより、共有リンクがトリガーするリスクインジケーターを通じて、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。

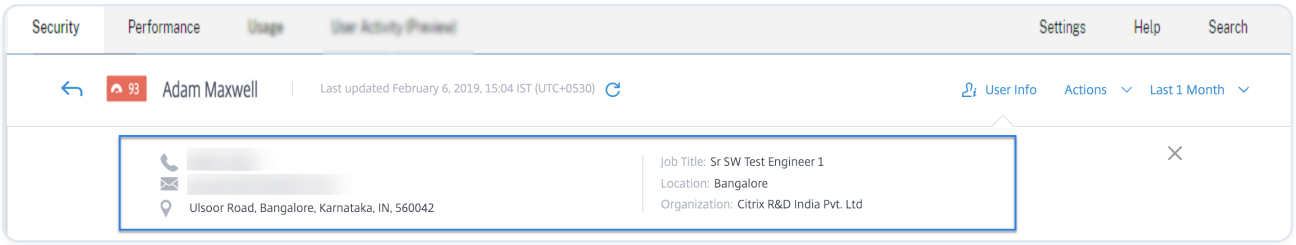
現在、共有リンクに対して「匿名機密共有ダウンロード」リスクインジケーターがトリガーされます。Content Collaborationがこの危険な動作を検出すると、Citrix Analyticsはイベントを受信します。**アラート**パネルで通知され、「匿名機密共有ダウンロード」リスクインジケーターが共有リンクのリスクタイムラインに追加されます。

詳細については、Share Link のリスクタイムラインと Citrix Share Link のリスクインジケーターを参照してください。

マイクロソフト アクティブディレクトリ統合

Microsoft Active Directory を Citrix Analytics と統合できるようになりました。この統合により、役職、組織、オフィス所在地、メール、連絡先などの追加情報で、リスクのある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向上させることができます。

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



January 04, 2019

新機能

既存のリスクインジケーターへの SOURCE 列の追加

以下のリスクインジケーターの**イベント詳細**セクションに、**SOURCE**列が導入されました。

- 過剰なファイルアップロード
- 過剰なファイルダウンロード
- 過剰なファイル共有

- 過剰なファイルまたはフォルダーの削除

詳細については、Citrix Content Collaboration のリスクインジケーターを参照してください。

高度なユーザープロファイル

ユーザープロファイルの**ユーザー情報**ビューが強化されました。**アプリケーション**、**デバイス**、および**データ使用量**セクションの右上隅に**トレンドビュー**リンクが導入されました。**場所**セクションの右上隅に**マップビュー**リンクが導入されました。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示を提供します。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**
>
> **認証**および**ドメイン**データは現在、ユーザー情報プロファイルでは利用できません。

> 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。



Microsoft Graph Security のリスクインジケーター

オンボードされたMicrosoft Graph Securityは、以下のいずれかのセキュリティプロバイダーからリスクインジケーターの詳細を受信し、Citrix Analyticsに転送できます。

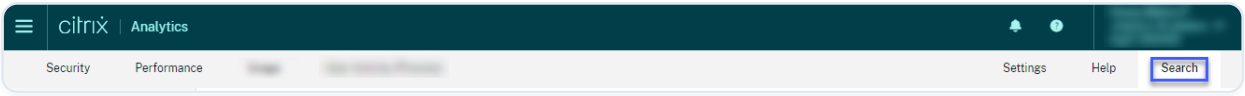
- Azure AD アイデンティティ保護
- マイクロソフト ディフェンダー for エンドポイント

詳細については、「Microsoft Graph Security のリスクインジケーター」を参照してください。

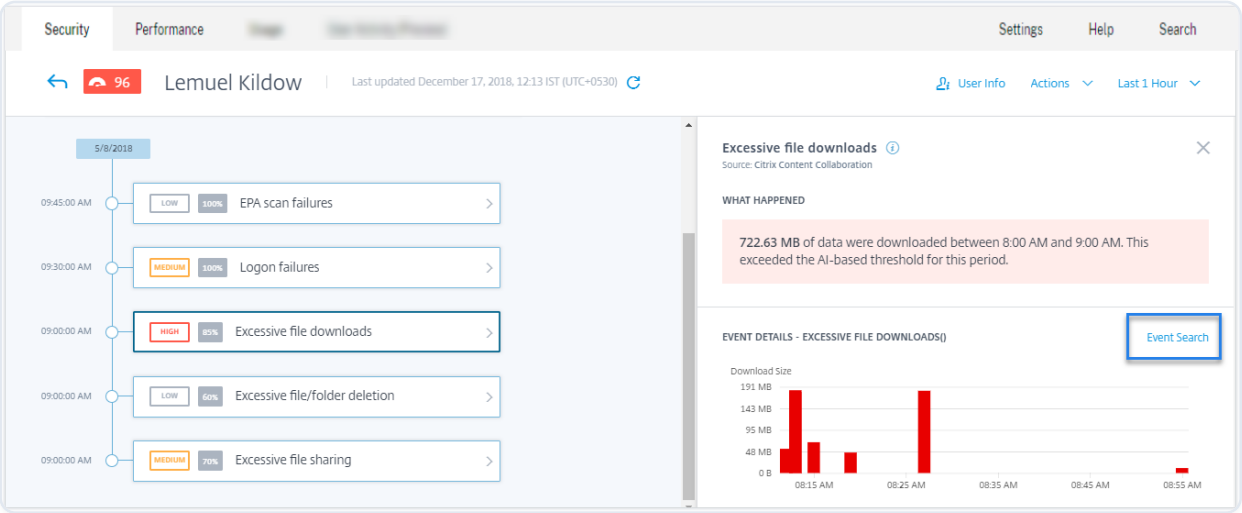
セルフサービス検索ページへのアクセス方法

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インジケーター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向けセルフサービス検索

Content Collaborationデータソースに関連付けられたイベントに関する洞察を得るには、セルフサービス検索を使用します。イベントを表示するには、リストから**Content Collaboration**を選択し、期間を選択してから、**Search**をクリックします。 詳細については、「Content Collaboration向けセルフサービス検索」を参照してください。

Apps and Desktops向けセルフサービス検索

Apps and Desktopsデータソースに関連付けられたイベントに関する洞察を得るには、セルフサービス検索を使用します。イベントを表示するには、リストから**Apps and Desktops**を選択し、期間を選択してから、**Search**をクリックします。詳細については、「Apps and Desktops向け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

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、将来の使用の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向けオンボーディングの改善

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、より良いユーザーエクスペリエンスが提供されるようになりました。サイトカードとオンボーディング手順が変更されました。詳細については、「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。

November 29, 2018

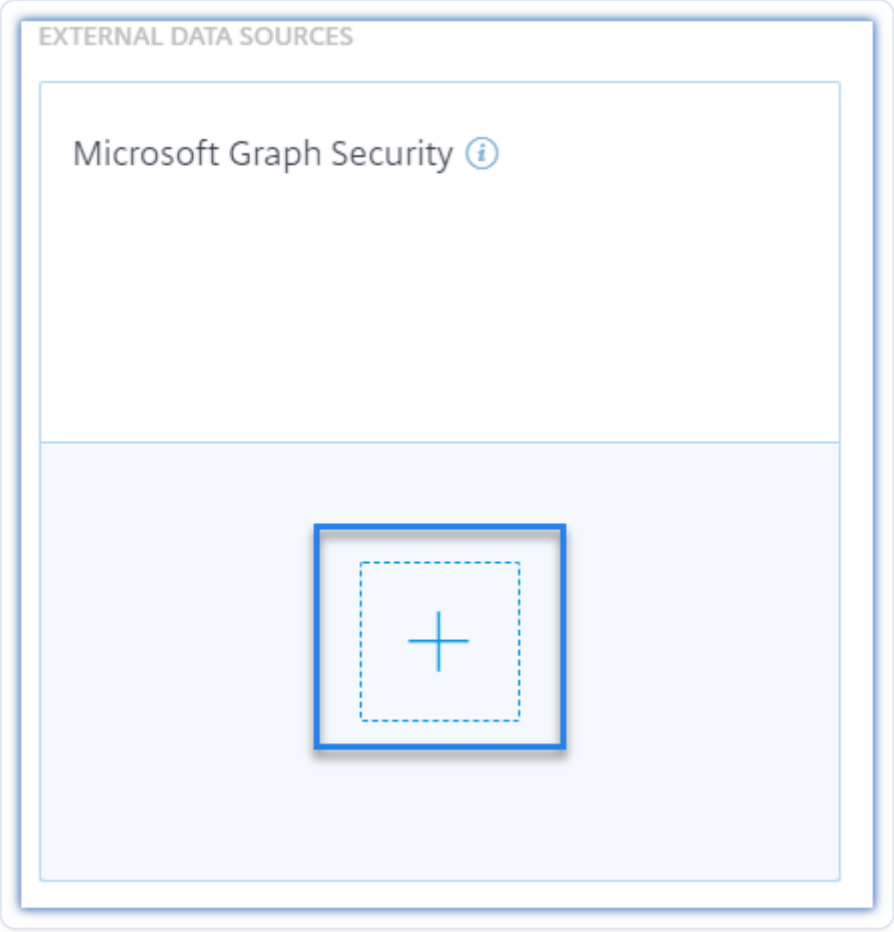
新機能

Microsoft Security Graphデータソース

Microsoft Graph Securityは、複数のセキュリティプロバイダーからのデータを集約する外部データソースです。また、ユーザーインベントリデータへのアクセスも提供します。

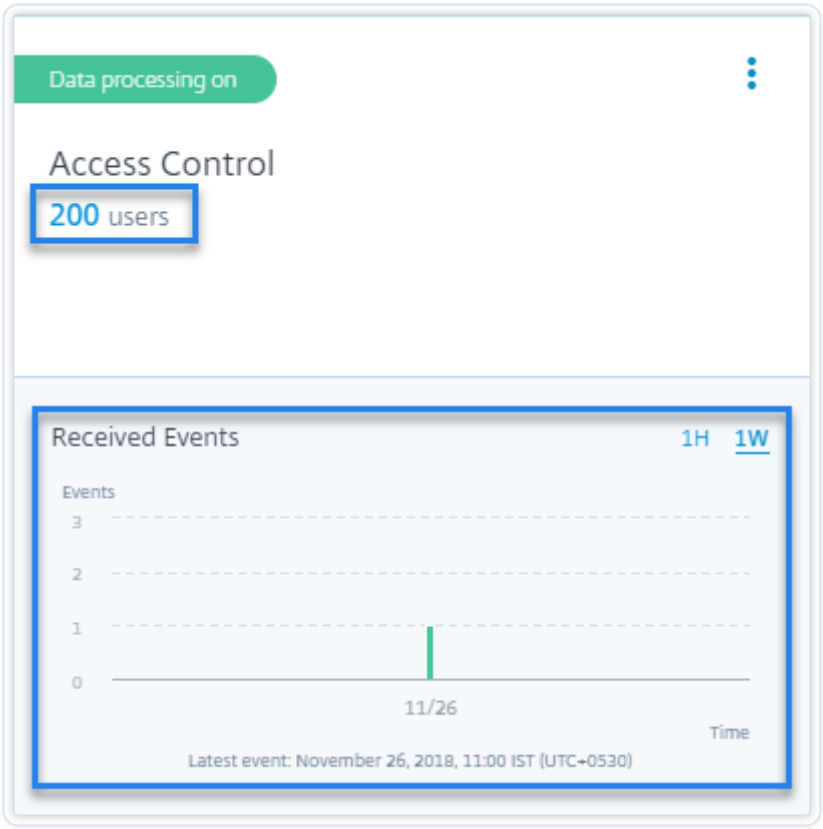
Citrix Analyticsは現在、このデータソースに関連付けられている**Azure AD identity protection**および**Microsoft Defender for Endpoint**セキュリティプロバイダーをサポートしています。

このデータソースをオンボーディングするには、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 Security」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を表示

データソースのサイトカードに、イベントの詳細とユーザー数が表示されるようになりました。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Analyticsを有効にする」を参照してください。



November 16, 2018

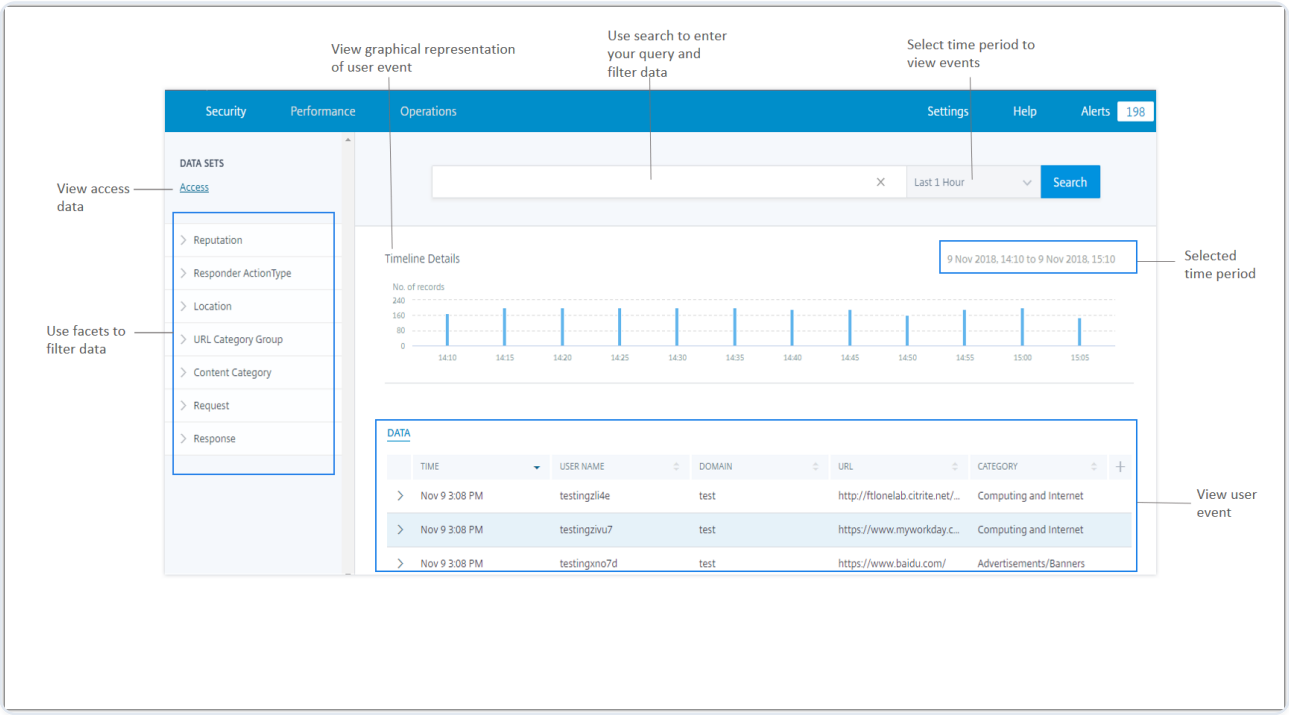
新機能

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して、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 Access Control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］タブから［イベント検索］**をクリックします。

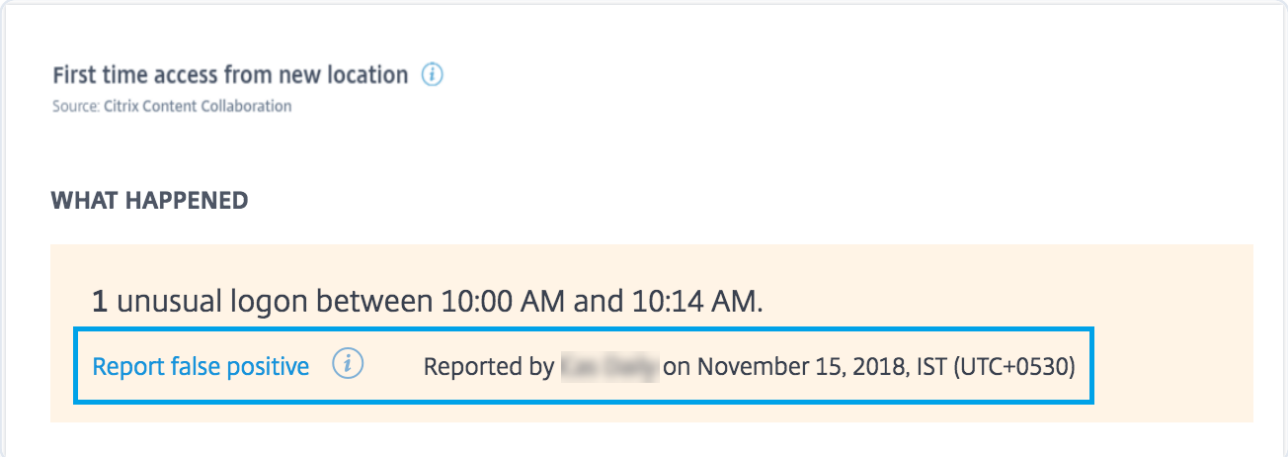
詳細については、「アクセスのセルフサービス検索」を参照してください。



リスクインジケーターのフィードバック

Citrix Analyticsのリスクインジケーターフィードバック機能を使用すると、リスクインジケーター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］**リスクインジケーターでサポートされています。このリスクインジケーターのトリガーが正しくない場合は、誤検知として報告し、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、お客様のフィードバックを収集し、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。



修正された問題

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

既知の問題

Citrix Analytics for Security™ には、以下の既知の問題があります。

- Web ブラウザ経由でアプリとデスクトップを開き、ネイティブクライアント上の ICA® から起動した場合、Citrix Workspace™ アプリ for Linux は Citrix Analytics に印刷イベントを送信できません。

> **注**
>
> すべてのプラットフォームにおける Citrix Workspace アプリおよび Citrix Receiver のライフサイクル日付とライフサイクルフェーズ（一般提供、メンテナンス終了、サポート終了）の詳細については、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。

Analyticsの提供機能

データソース

データソースとは、Citrix Analyticsにデータを送信するクラウドサービスおよびオンプレミス製品のことです。

Citrixデータソース

次の表に、Citrix Analytics for Securityでサポートされているさまざまなデータソースを示します。詳細については、「はじめに」を参照してください。

データソース	展開タイプ	必要なエージェント	製品コンポーネントとバージョン
シトリックス エンドポイント マネジメント	サービス	該当なし	シトリックス エンドポイント マネジメント
ゲートウェイ	オンプレミス	アプリケーションデリバリー管理エージェント	シトリックス ゲートウェイ 12.0.56.16 以降
シトリックス アイデンティティ プロバイダー	サービス	N/A	シトリックス アイデンティティ アンド アクセス マネジメント
シトリックス セキュア プライベート アクセス	サービス	(該当なし) N/A	シトリックス セキュア プライベート アクセス
シトリックス リモート ブラウザ アイソレーション	サービス	N/A	シトリックス リモート ブラウザ アイソレーション
シトリックス DaaS (旧称 Virtual Apps and Desktops service)	サービス	N/A	Windows向けCitrix Workspaceアプリ 1907以降、Mac向けCitrix Workspaceアプリ1910.2以降、

データソース	展開タイプ	必要なエージェント	製品コンポーネントとバージョン
			HTML5向けCitrix Workspaceアプリ2007以降、Chrome向けCitrix Workspaceアプリ - Chromeウェブストアで入手可能な最新バージョン、Android向けCitrix Workspaceアプリ - Google Playで入手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
シトリックス バーチャル アプリケーションズ アンド デスクトップ	オンプレミス	Virtual Apps and Desktopsエージェント	シトリックス バーチャル アプリケーションズ アンド デスクトップ 7 1808、シトリックス ゼナップ アンド ゼンダスクトップ 7.16 以降
		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、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ウェブストアで入手可能な最新

データソース	展開タイプ	必要なエージェント	製品コンポーネントとバージョン
			バージョン、Android向けCitrix Workspaceアプリ - Google Playで入手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
			シトリックス ディレクター 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。
			StoreFrontユーザーの場合: StoreFront展開バージョンはStoreFront 1906以降である必要があります。StoreFrontには、次のいずれかのクライアントを使用してアクセスする必要があります: HTML5互換ブラウザのCitrix Receiver™ for Webサイト、Windows向けCitrix Workspace™アプリ1907以降、Linux向

データソース	展開タイプ	必要なエージェント	製品コンポーネントとバージョン
			けCitrix Workspaceアプリ2006以降、Mac向けCitrix Workspaceアプリ2006以降。
			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 servicesを参照してください。

外部データソース

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) を次の表に示します。

データソース	展開タイプ	必要なエージェント
マイクロソフト グラフ セキュリティ	サービス	該当なし
マイクロソフト アクティブ ディレクトリ	オンプレミス	シトリックス クラウド コネクタ™

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 (US)

- 欧州連合 (EU)
- アジア太平洋南部 (APS)

組織の所在地に応じて、いずれかのホームリージョンでCitrix Cloud™にオンボーディングできます。

組織が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Citrix Cloudにオンボーディングされている場合、そのデータソースからの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確認してください。

データソース	米国リージョンでサポート	EUリージョンでサポート	APSリージョンでサポート
シトリックス エンドポイント マネジメント™	はい	はい	はい
Citrix Gateway (オンプレミス)	はい	はい	はい
Citrix アイデンティティプロバイダー	はい	はい	はい
Citrix セキュアプライベートアクセス™	はい	はい	はい
Citrix リモートブラウザ分離™	はい	はい	はい
シトリックス DaaS (旧称 シトリックス バーチャル アプリケーションズ アンド デスクトップス 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
マイクロソフト アクティブ ディレクトリ	はい	はい	はい

データソース	米国リージョンでサポート	EUリージョンでサポート	APSリージョンでサポート
マイクロソフト グラフ セキュリティ	はい	はい	はい

Citrix Workspaceアプリのバージョンマトリックス

このセクションでは、すべてのテレメトリを送信し、必要なすべての重要なバグ修正を含むCitrix Workspaceアプリのサポートされているバージョンを表示します。

以下の表に、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ます。

プラットフォーム	サポートされているバージョン
Windows	CU3以降のすべてのLTSR 2203リリース
	23.0.3.0以降
HTML5	21.5.0.0以降
Macintosh	21.0.4.0以降
Linux	21.4.0.0以降
Chrome	21.5.0.0以降
iOS	21.4.0.0 以降
アンドロイド	21.5.0.0 以降

次の表に、Citrix Analytics for Securityで次のユーザーイベント属性を受信するためにオペレーティングシステムで必要となるCitrix Workspaceアプリの最小バージョンを示します。

イベント属性	関連機能	ウィンドウズ	MAC	リナックス	HTML 5	クローム	IOS	アンドロイド
市区町村、国	アクセス保証ロケーショ	2008以降	2006以降	2104以降	2007以降	Chromeウェブストアで利	Apple App Storeで利用	Google Playで利用可能な

イベント属性	関連機能	ウィンドウズ	MAC	リナックス	HTML 5	クローム	IOS	アンドロイド
	ン、セルフサービス検索 - アプリとデスクトップ					用可能な最新バージョン	可能な最新バージョン	最新バージョン
クライアントIP	セルフサービス検索 - アプリとデスクトップ	2008以降	2006以降	2104以降	2007以降	Chromeウェブストアで利用可能な最新バージョン	Apple App Storeで入手可能な最新バージョン	Google Playで入手可能な最新バージョン
OS名、OSバージョン、OS追加情報	セルフサービス検索 - アプリとデスクトップ	2109以降	2108以降	2104以降	2007以降	Chrome Web Storeで入手可能な最新バージョン	Apple App Storeで入手可能な最新バージョン	Google Playで入手可能な最新バージョン
プリンター名	セルフサービス検索 - アプリとデスクトップ	2106以降	1809以降	2006以降	1911以降	Chromeウェブストアで入手可能な最新バージョン	Apple App Storeで入手可能な最新バージョン	Google Playで入手可能な最新バージョン
Web起動に関するすべてのユー	セルフサービス検索 - アプリとデ	2008以降	2006以降	2006以降	該当なし	サポートされていません	Apple App Storeで入手可能な	Google Playで入手可能な最新

イベント属性	関連機能	ウィンドウズ	MAC	リナックス	HTML 5	クローム	IOS	アンドロイド
ザーイベント	スクトップ						最新バージョン	バージョン

データガバナンス

システム要件

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

Citrix Analytics for Security のサブスクリプション

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。

データソースの要件

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 が正確に機能するには、Analytics のデータソースとして機能する以下の製品のいずれかを使用するための有効なサブスクリプションが必要です。

- Citrix ADC (オンプレミス) と Citrix Application Delivery Management のサブスクリプション
- シトリックス エンドポイント マネジメント サービス
- Citrix Gateway (オンプレミス)
- Citrix Identity プロバイダー
- シトリックス リモート ブラウザ アイソレーション
- シトリックス セキュア プライベート アクセス サービス
- シトリックス Virtual Apps and Desktops または シトリックス DaaS (旧 シトリックス Virtual Apps and Desktops サービス)
- マイクロソフト アクティブ ディレクトリ
- マイクロソフト グラフ セキュリティ

サポートされているブラウザ

Analytics にアクセスするには、ワークステーションに以下のサポートされている Web ブラウザが必要です。

- Google Chrome の最新バージョン

- Mozilla Firefox の最新バージョン
- Microsoft Edge の最新バージョン
- Apple Safari の最新バージョン

Security Analytics の管理者ロールを管理する

> **注:**
>
> 2023 年 7 月以降、Microsoft は Azure Active Directory (Azure AD) を Microsoft Entra ID に名称変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD へのすべての参照は、Microsoft Entra ID を指します。

フルアクセス権限を持つ Citrix Cloud™ 管理者として、他の管理者を招待して Security Analytics オファリングを管理させ、以下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。

- **Security Analytics - フル管理者**
- **Security Analytics - 読み取り専用管理者**

新しい管理者は、個々のユーザーとして、または Azure Active Directory グループを使用して、2 つの方法で追加できます。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** ユーザーがユーザーとして直接、および Azure Active Directory グループを介してアクセス権を付与された場合、ユーザーに個別に付与されたアクセス権が有効になります。

カスタムロールの権限

Security Analytics - フル管理者ロールを持つ管理者は、Security Analytics オファリングのすべての機能にアクセスできます。組織の要件に応じて機能を使用および変更できます。たとえば、フル管理者はカスタムリスクインジケーターを作成したり、ジオフェンスを有効にしたり、ポリシーを作成したりできます。

Security Analytics - 読み取り専用管理者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。これらのダッシュボードでユーザーの行動を監視し、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インジケーターに手動でアクションを適用する
- カスタムリスクインジケーターを作成、変更、または削除する
- カスタムレポートを作成する
- 他の管理者ユーザーを追加、変更、または削除する
- アクセス保証ロケーションのジオフェンスを追加または変更する

管理者向けのセキュリティアラート通知

フルアクセス権限を持つCitrix Cloud管理者と同様に、カスタムロール（フルアクセスおよび読み取り専用アクセス）を持つ管理者もSecurity Analyticsからメール通知を受け取ります。

管理者は2種類のメール通知を受け取ります。

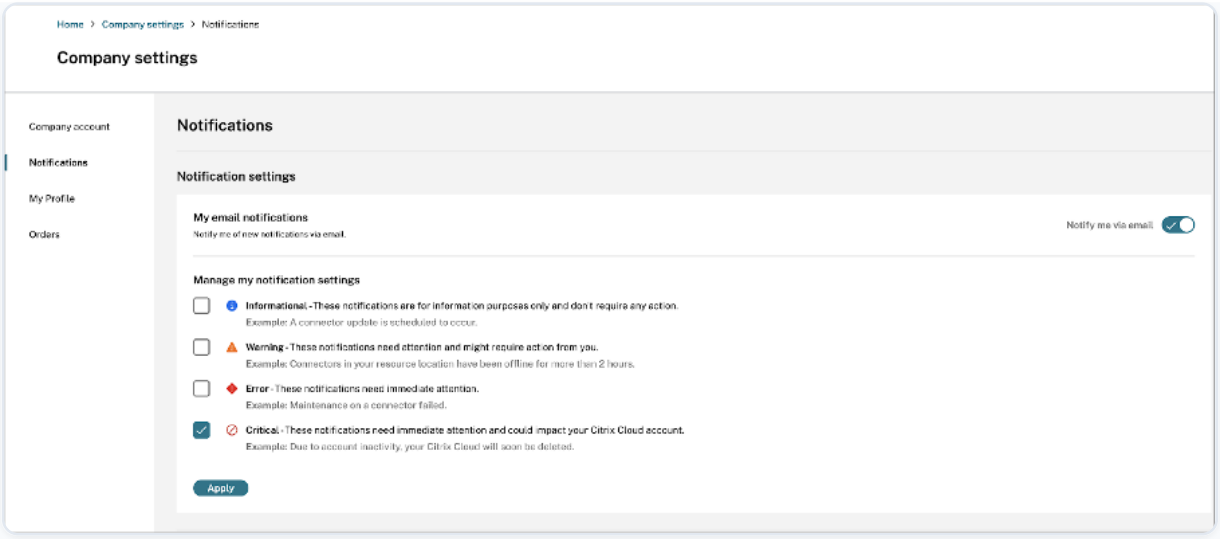
- 組織内のセキュリティインサイトに関する週次通知。詳細については、「週次メール通知」を参照してください。
- 管理者に通知アクションに基づく通知。詳細については、「ポリシーとアクション」を参照してください。

フルアクセスまたはカスタムアクセス権限を持つCitrix Cloud管理者である場合、Citrix Cloudアカウントではメール通知がデフォルトで無効になっています。Citrix AnalyticsなどのCitrix Cloudサービスからメール通知を受け取るには、Citrix Cloudで通知オプションを有効にしてください。詳細については、「受信したメール通知」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には、通知設定は利用できません。

通知設定は、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を送信する際に利用されます。メール通知について、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限を持つ管理者が配布リストからあなたを削除する必要があります。配布リストの詳細については、「メール配布リスト」を参照してください。

> **注**

Citrix Cloud管理者（フルアクセスまたはカスタムアクセス権限を持つ）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け取りません。



詳細については、「Citrix Analyticsの管理者を管理する」を参照してください。

利用開始

このドキュメントでは、Citrix Analytics for Security™ を初めて利用開始する方法について説明します。

利用開始(/en-us/citrix-analytics/media/getting-started-steps-security.png)

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てください。

Citrix Cloud アカウントをお持ちでない場合は、まず 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。詳細な手順については、(/ja-jp/citrix-cloud/overview/get-started/signing-up-for-citrix-cloud.html) を参照してください。

ステップ 2: Security Analytics へのアクセスを取得する

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

- **Citrix Analytics for Security のトライアルをリクエストする**。Citrix Cloud にサインインした後、次の操作を行います。

  a. **Available Services** セクションで、**Analytics** タイルの **Manage** 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。

  b. **Security** タイルで、**Request Trial** をクリックするか、Citrix アカウントまたは Citrix パートナーに直接お問い合わせください。

- **Citrix Analytics for Security を購読する**。Citrix Analytics for Security の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、Citrix Analytics の専門家にお問い合わせください。

> **注**

- March 8, 2023 より、Citrix Analytics for Security は、ShareFile/Citrix Content Collaboration とのスタンドアロン製品としては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) を発表します。Citrix Analytics for Security のお客様の既存の権利は、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 統合のトライアル、更新、新規購入はサポートされません。他の Citrix 製品向けの Citrix Analytics Service 統合は、既存の Citrix DaaS プラン、Citrix Virtual Apps and Desktops 展開、および Citrix Workspace 展開とのスタンドアロンまたはバンドル製品として引き続き提供されます。
- February 03, 2020 より、Citrix Analytics for Security は Workspace Premium および Workspace Premium Plus サブスクリプションに含まれなくなりました。February 03, 2020 より前に Workspace Premium または Workspace Premium Plus サブスクリプションを購入されたお客様は、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 は現在、Citrix Workspace パッケージ (Workspace Standard、Workspace Premium、Workspace Premium Plus) のアドオンサービスとして提供されています。詳細については、Citrix Cloud services 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お持ちの場合、またはトライアルへのアクセスが承認されている場合、Analytics の概要ページで、セキュリティ製品の ボタンが に変わります。 をクリックして、ユーザーダッシュボードを表示します。

ようこそページ(/en-us/citrix-analytics/media/citrix-analytics-overview-page.png)

Analytics は、Citrix データソース と 外部データソース の両方をサポートしています。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信するには、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、 **> >** をクリックします。

次のステップ

- Citrix Analytics for Security の資格が承認されると、以下のクラウドサービスでデータ処理が有効になります。
    - Citrix データソース

    - シトリックス セキュア プライベート アクセス
    - シトリックス バーチャル アプリケーションズ アンド デスクトップ および シトリックス DaaS

- データ処理のステータスを確認したり、手動で有効にする方法を知るには、以下の記事を参照してください。
    - Citrix データソース:
        - シトリックス エンドポイント マネジメント
        - シトリックス ゲートウェイ
    - 外部データソース:
        - マイクロソフト グラフ セキュリティ
        - マイクロソフト アクティブ ディレクトリ(/ja-jp/security-analytics/getting-started-security/active-directory-integration.html)
- Analyticsから処理済みデータを以下の製品にエクスポートします。
    - スプランク(/ja-jp/security-analytics/siem-integration/splunk-integration.html)
    - マイクロソフト アジュール センチネル(/ja-jp/security-analytics/siem-integration/azure-sentinel-integration.html)
    - エラスティックサーチ(/ja-jp/security-analytics/siem-integration/elasticsearch-integration.html)
    - 「KafkaまたはLogstashベースのデータコネクタを使用するその他のSIEM」(/ja-jp/security-analytics/siem-integration/kafka-or-logstash-siem-integration.html)
- 発見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するには、ユーザーダッシュボードを使用します。**ユーザー**ダッシュボードは、ユーザー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。

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

シトリックス エンドポイント マネジメント™ データソース

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で提供されているCitrix Endpoint Managementを購読します。Endpoint Managementサービスの設定方法については、「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。
- **Cloud SiteとEnterprise Directory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マシンが2台あることを確認してください。
- **Cloud Connectorがインストールされていること**。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、お使いの環境が要件を満たしていることを確認してください。

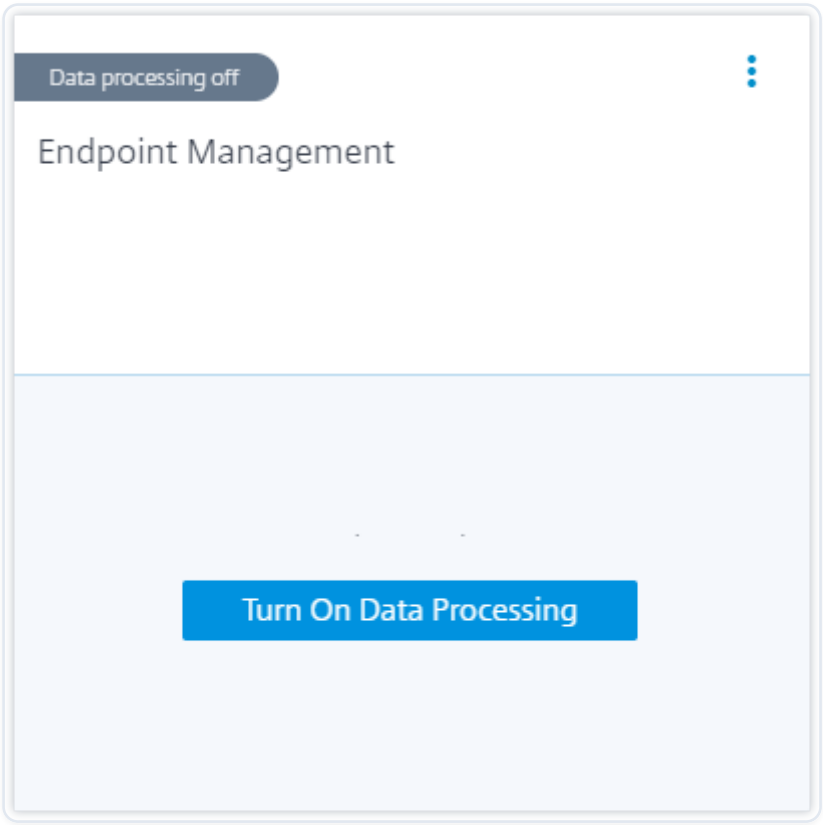
データソースの表示とデータ処理の有効化

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:

上部のバーから、**設定** > **データソース** > **セキュリティ** をクリックします。

データソースページにEndpoint Managementデータソースのサイトカードが表示されます。**データ処理を有効にする**をクリックして、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します。



ユーザーと受信イベントの表示

サイトカードには、Endpoint Managementユーザー、デバイス、および受信イベントの数が、デフォルトの時間選択である過去1時間分表示されます。1週間 (**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、**ユーザー** ページでユーザーの詳細が表示されます。

エンドポイントデータソース(/en-us/citrix-analytics/media/endpoint-event.png)

データ処理を有効にすると、サイトカードに「**データが受信されていません**」というステータスが表示されることがあります。このステータスが表示される理由は2つあります。

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** ページを更新してください。
2. 過去1時間以内に、Analyticsがデータソースからイベントを受信していません。

   データなしエンドポイント(/en-us/citrix-analytics/media/no-data-end-point.png)

データ処理のオン/オフを切り替える

データ処理を停止するには、サイトカードの縦三点リーダー (⋮) をクリックし、次に「**データ処理をオフにする**」をクリックします。Citrix Analyticsは、このデータソースのデータ処理を停止します。

エンドポイントデータソース(/en-us/citrix-analytics/media/endpoint-turn-off.png)

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。

エンドポイントデータソース(/en-us/citrix-analytics/media/endpoint-turn-on-again.png)

Citrix Gateway (オンプレミス) データソース

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

ユーザーがGatewayを介してサービスや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の詳細については、Citrix Analyticsプラットフォームのドキュメントにある Citrix Gatewayデータソースの記事を参照してください。

シトリックス リモートブラウザアイソレーション™ データソース

Citrix Remote Browser Isolation Service は、Webブラウジングを分離して、企業ネットワークをブラウザベースの攻撃から保護します。ユーザーデバイスの設定は不要で、インターネットでホストされているWebアプリケーションへの一貫した安全なリモートアクセスを提供します。

Citrix Analytics for Securityでは、公開された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。

公開された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はユーザーセッション中に使用されたホスト名をCitrix Analytics for Securityに送信できるようになります。 詳細については、「公開されたRemote Browser Isolationの管理」を参照してください。

シトリックス セキュア プライベート アクセス™ データソース

「**Secure Private Access**」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 Secure Private Access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で提供されているCitrix Secure Private Accessサービスを購読します。開始方法については、「Secure Private Accessサービス」を参照してください。
- システム要件を確認し、環境が要件を満たしていることを確認します。

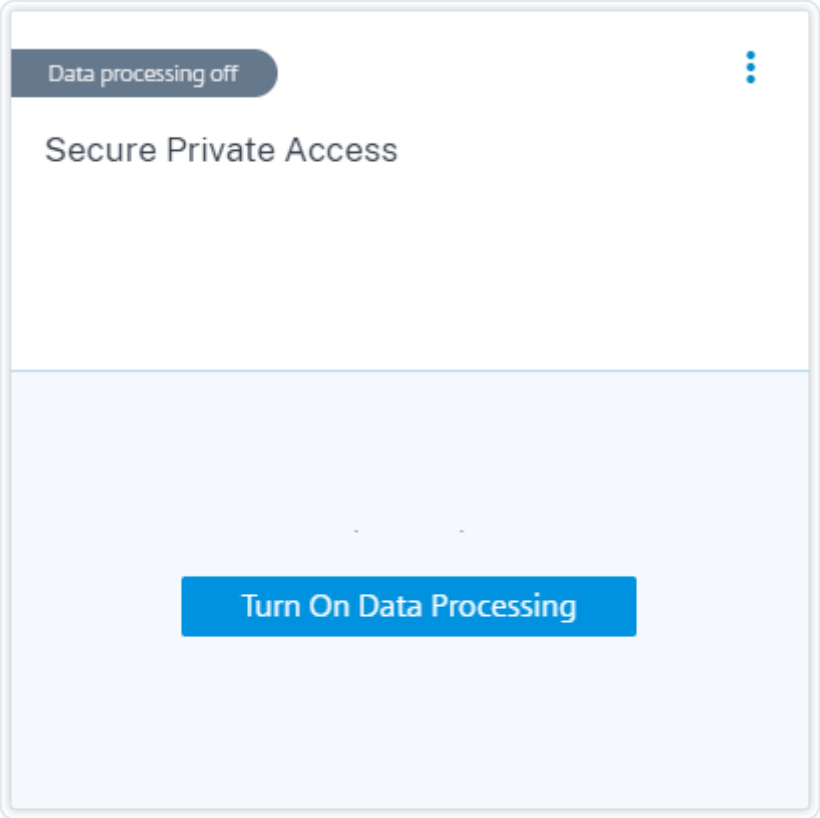
データソースの表示とデータ処理の有効化

Citrix Analyticsは、Citrix Cloud™アカウントに関連付けられているSecure Private Access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：

上部のバーで、［設定］ > ［データソース］ > ［セキュリティ］ の順にクリックします。

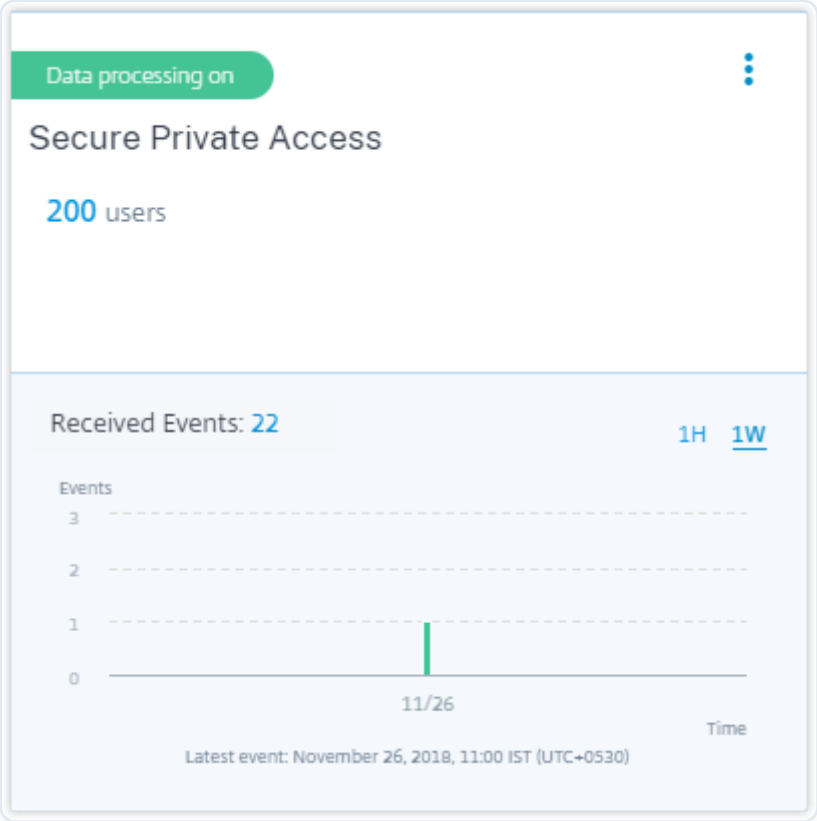
［データソース］ ページに、**Secure Private Access** データソースのサイトカードが表示されます。［データ処理を有効にする］ をクリックして、Citrix Analyticsがこのデータソースのデータ処理を開始できるようにします。



ユーザーと受信イベントの表示

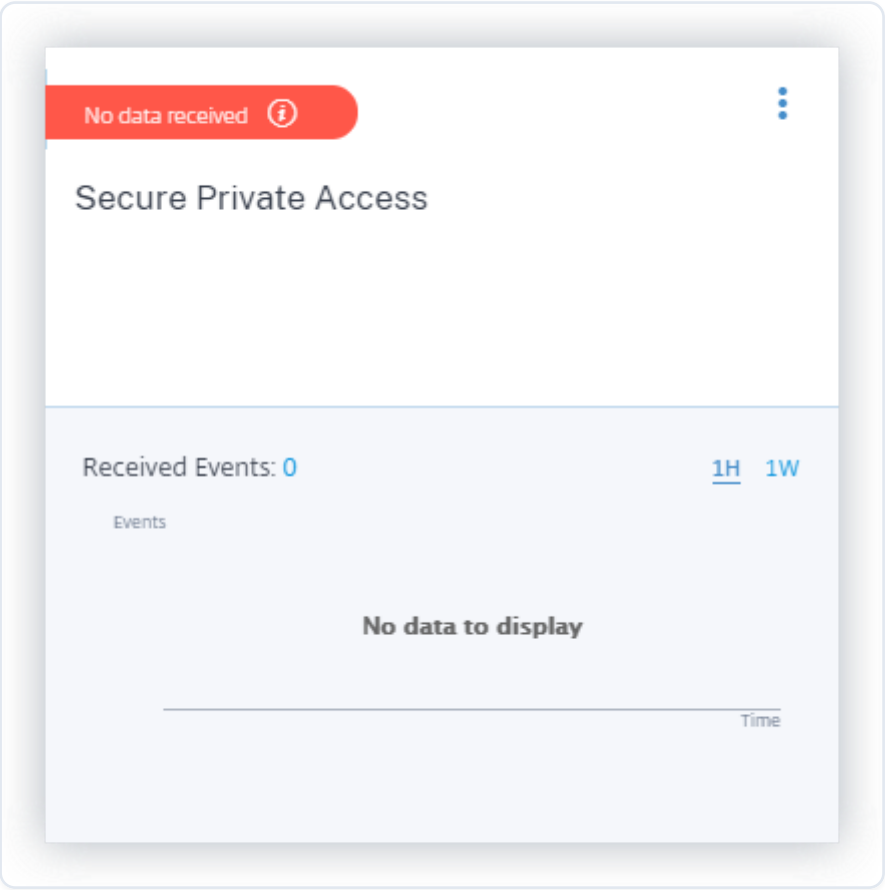
サイトカードには、アクティブなユーザー数と、データソースから過去1時間に受信したイベントが表示されます。これはデフォルトの時間選択です。1週間 (1 W) を選択してデータを表示することもできます。

ユーザー数をクリックすると、［**ユーザー**］ ページでユーザーの詳細が表示されます。受信イベント数をクリックすると、セルフサービス検索ページでイベントの詳細が表示されます。



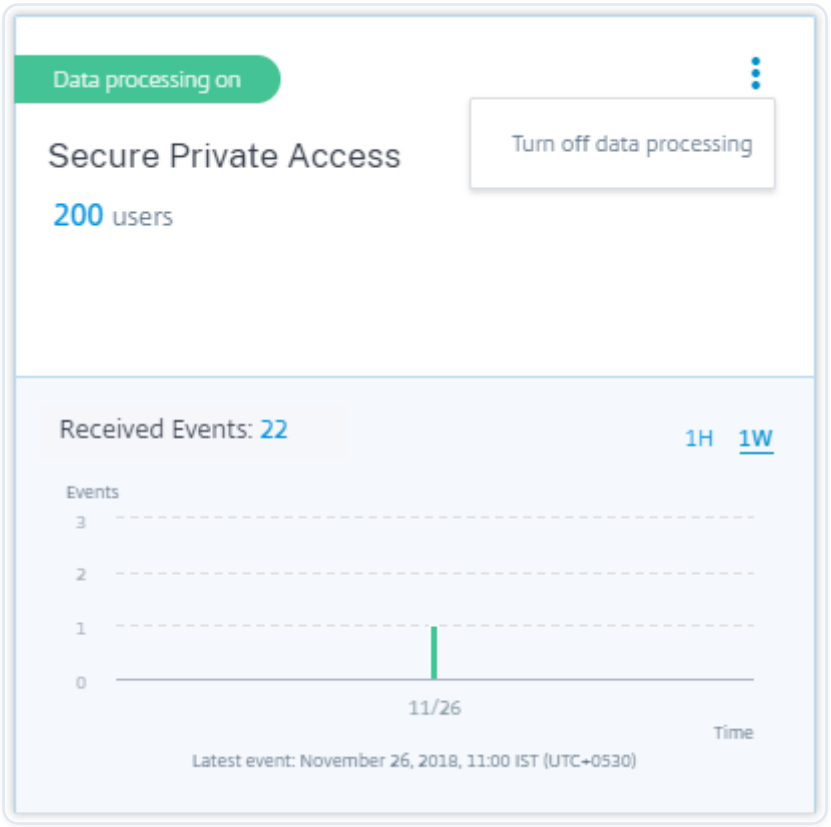
データ処理を有効にすると、サイトカードに**データが受信されていません**というステータスが表示されることがあります。このステータスが表示される理由は2つあります。

1. データ処理を初めて有効にした場合、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、ステータスは**データ処理中**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**ページを更新してください。
2. Analyticsは、過去1時間以内にデータソースからイベントを受信していません。

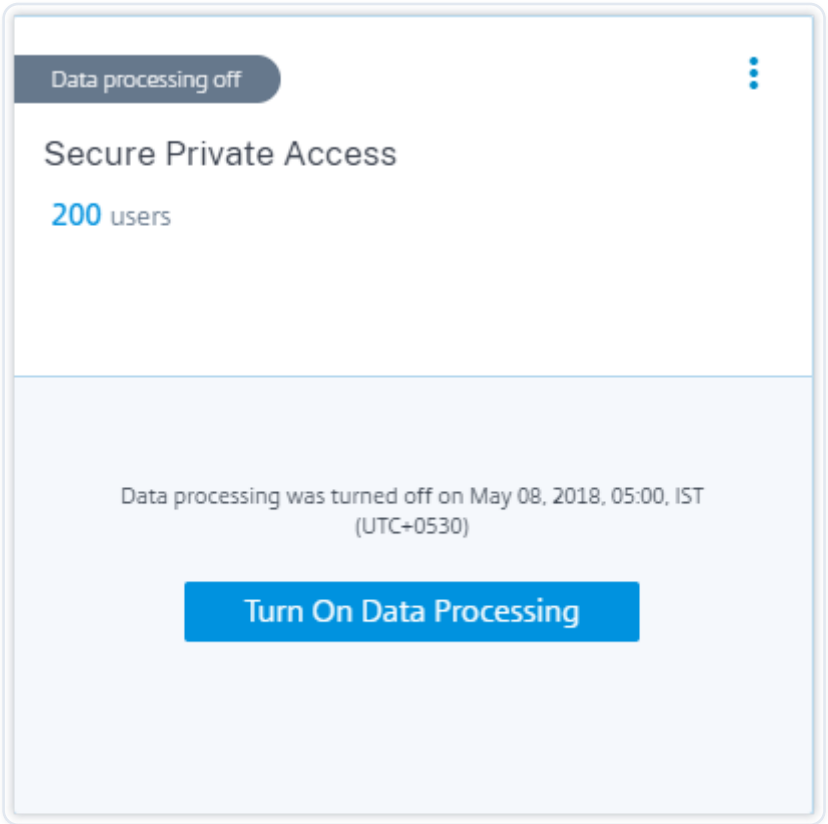


データ処理の有効化または無効化

データ処理を停止するには、サイトカードの縦三点リーダー (⋮) 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、このデータソースのデータ処理を停止します。



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

Apps and Desktops データソースは、組織内のオンプレミス Citrix Virtual Apps and Desktops および Citrix DaaS (旧称 Citrix Virtual Apps and Desktops サービス) を表します。

Citrix Analytics for Security™ は両方のサービスをサポートし、データソースからユーザーイベントを受信します。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 および Citrix DaaS™ データソースの以下のコンポーネント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ている Citrix Workspace™ アプリ
- オンプレミス展開用の Citrix Director
- Citrix Monitor サービス
- セッション記録サーバー

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、ユーザーイベントは Citrix Analytics for Security でリアルタイムに受信されます。

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ユーザーは、クライアントを以下のいずれかのバージョンにアップグレードする必要があります。

- Windows 用 Citrix Workspace アプリ 1907 以降
- Mac 用 Citrix Workspace アプリ 1910.2 以降
- HTML5 用 Citrix Workspace アプリ 2007 以降
- Chrome 用 Citrix Workspace アプリ - Chrome Web Store で入手可能な最新バージョン
- Citrix Workspace app for Android - Google Playで入手可能な最新バージョン
- Citrix Workspace app for iOS - Apple App Storeで入手可能な最新バージョン
- Linux 版 Citrix Workspace アプリ 2006 以降

Citrix DaaSでAnalyticsを有効にする

前提条件

- Citrix Cloudで提供されるCitrix DaaSを購読します。Citrix DaaSの開始方法については、「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てください。

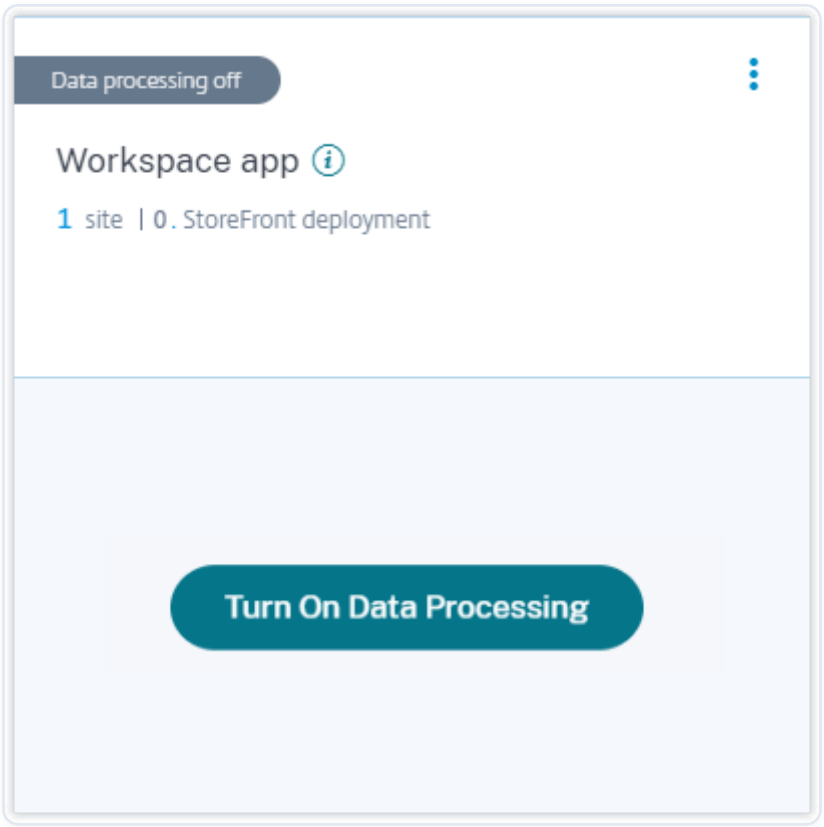
データソースを表示し、データ処理を有効にする

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:

上部のバーから、**設定** > **データソース** > **セキュリティ** をクリックします。

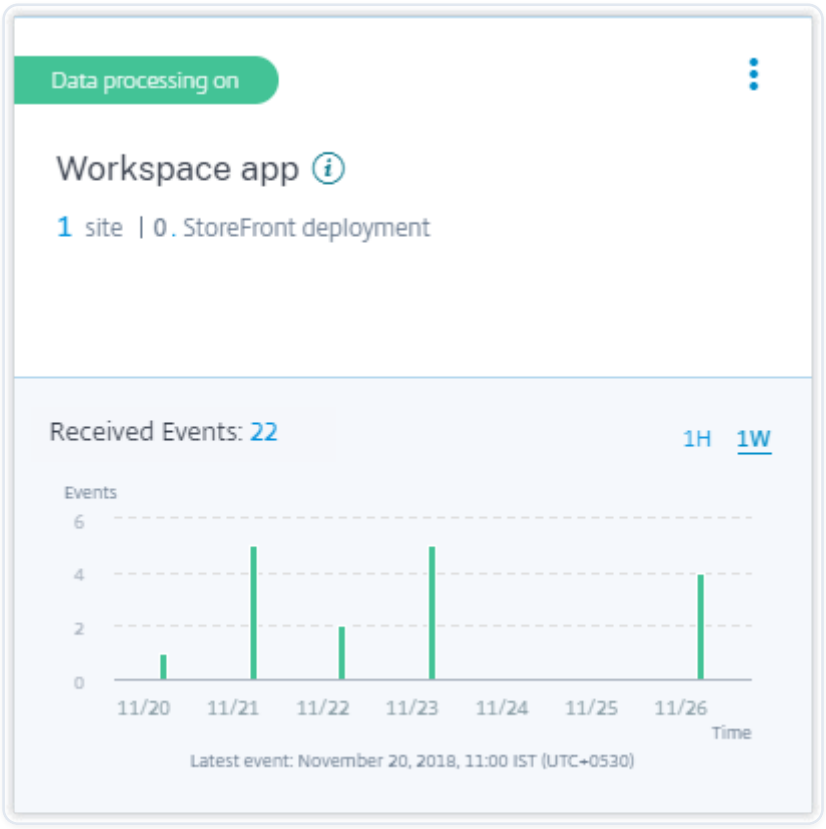
データソースページに**アプリとデスクトップ - Workspaceアプリ**サイトカードが表示されます。**データ処理を有効にする**をクリックして、Citrix Analyticsがこのデータソースのデータ処理を開始できるようにします。



クラウドサイト、ユーザー、および受信イベントを表示する

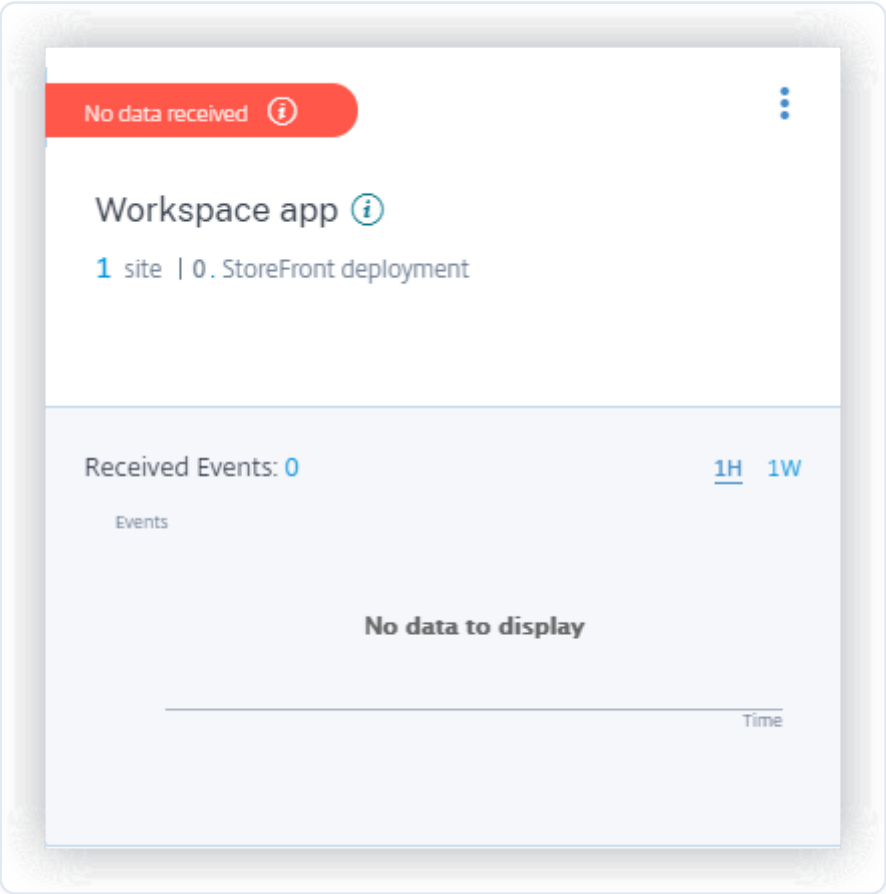
サイトカードには、アプリとデスクトップのユーザー数、検出されたクラウドサイト、および過去1時間（デフォルトの時間選択）に受信されたイベントが表示されます。1週間（1 W）を選択してデータを表示することもできます。

受信したイベントの数をクリックして、(/ja-jp/security-analytics/self-service-search/self-service-search-virtual-apps-desktops.html)ページで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**データが受信されていません**というステータスが表示されることがあります。このステータスが表示される理由は2つあります。

1. データ処理を初めて有効にした場合、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、ステータスは**データ処理中**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**ページを更新してください。
2. Analyticsが過去1時間以内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™展開を介して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。

組織が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、以下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を使用してオンプレミスサイトをオンボーディングする
- 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オンプレミスの開始方法については、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てください。
- Directorのバージョンは1912 CU2以降である必要があります。詳細については、機能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**。サイトをCitrix Workspaceに追加する場合は、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の専門家にお問い合わせください。

- **Workspace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へのオンボーディングを進める前に、サイトをCitrix Workspaceに追加してください。このプロセスは**サイト集約**と呼ばれます。

  サイト集約では、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のためにNetScaler Gateway STAサーバーを構成し、その後サイトをWorkspaceに追加する必要があります。サイト集約の詳細な手順については、(/ja-jp/citrix-cloud/workspaces/add-on-premises-site.html)を参照してください。

- **StoreFrontのバージョン**。サイトにStoreFront展開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てください。

StoreFrontを使用してCitrix Virtual Apps and Desktopsオンプレミスサイトをオンボーディングする

前提条件とオンボーディング手順については、Citrix Analyticsプラットフォームドキュメントの(/ja-jp/citrix-analytics/data-sources/virtual-apps-desktops-onboarding.html)記事を参照してください。

Workspaceを使用してCitrix Virtual Apps and Desktopsオンプレミスサイトをオンボーディングする

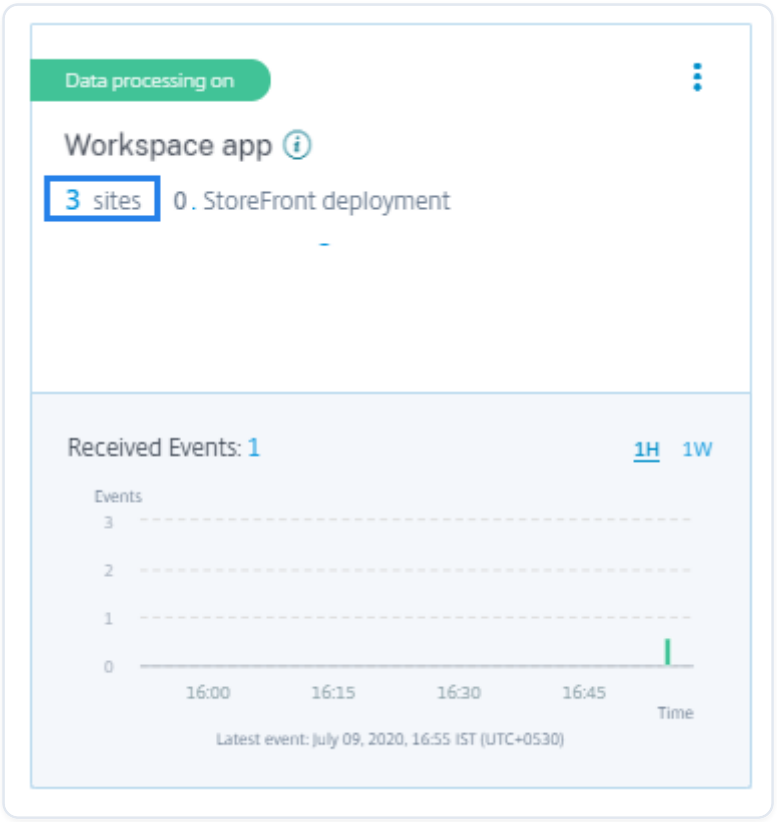
Citrix Workspaceにすでに追加されているサイト

Citrix Analyticsは、Citrix Workspaceにすで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：

上部のバーから、**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され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。ユーザー数をクリックすると、**ユーザー**ページで検出されたユーザーが表示されます。

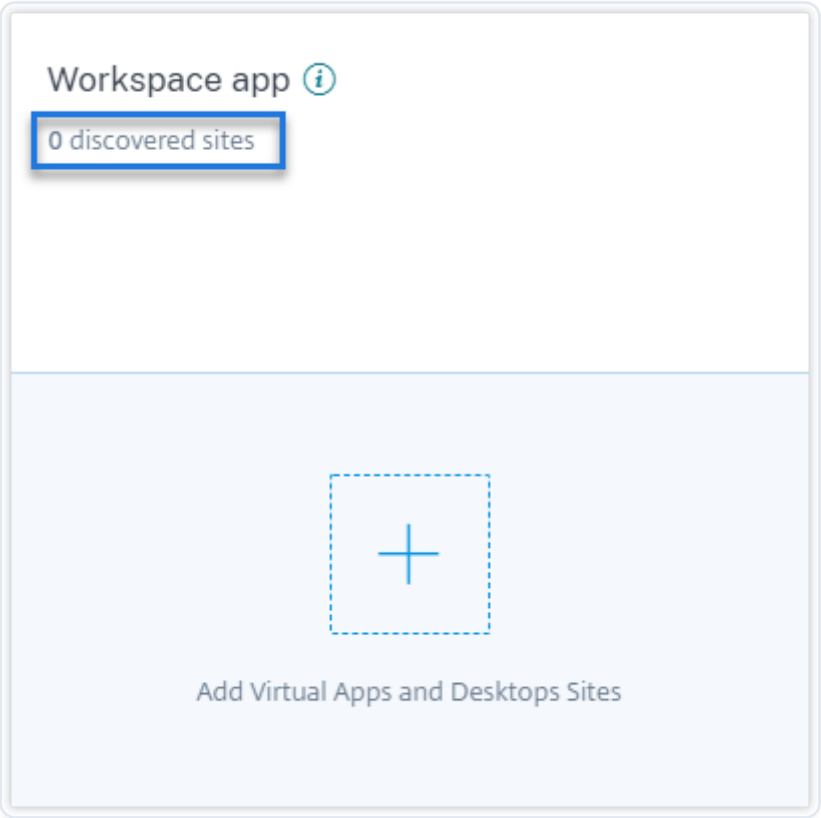


Citrix Workspaceに追加されていないサイト

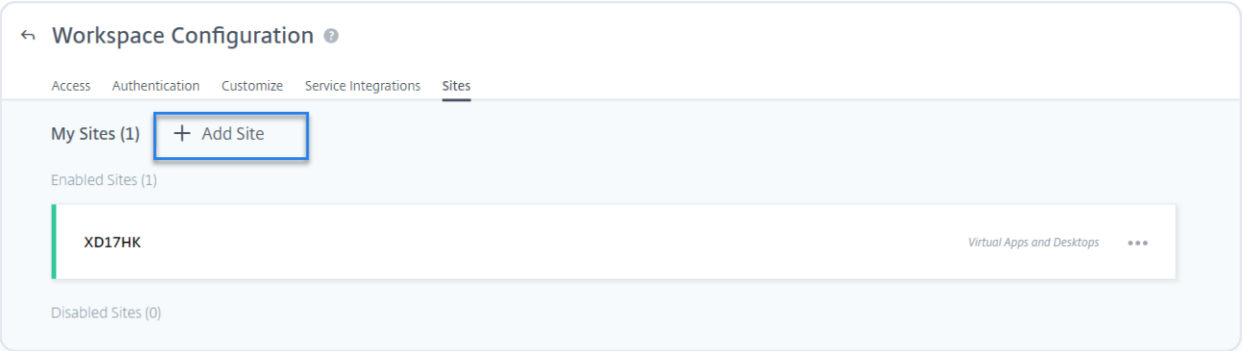
オンプレミスサイトをWorkspaceにまだ追加していない場合、Analyticsはサイトを検出できません。サイトカードには**0個の検出されたサイト**と表示されます。

サイトをWorkspaceに追加するには：

1. サイトカードの+をクリックします。



2. **Workspace Configuration**ページで、**+Add Site**をクリックします。

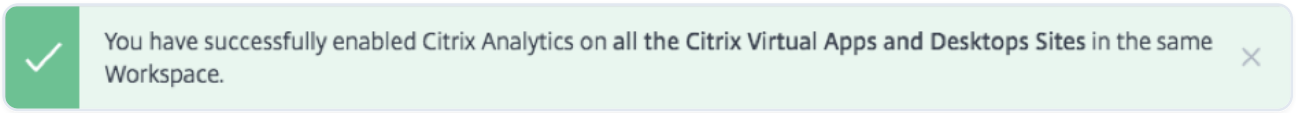


3. 画面の指示に従ってサイトを追加します。詳細については、ワークスペースでのオンプレミス仮想アプリとデスクトップの集約を参照してください。
4. サイトを追加した後、Citrix Analyticsに再度ログインし、**データソース**ページを更新して、最近追加されたサイトをサイトカードで表示します。

データ処理をオンにして、受信したイベントを表示する

Analyticsが検出されたサイトのデータ処理を開始できるようにするには、サイトカードの**データ処理をオンにする**をクリックし、画面の指示に従います。

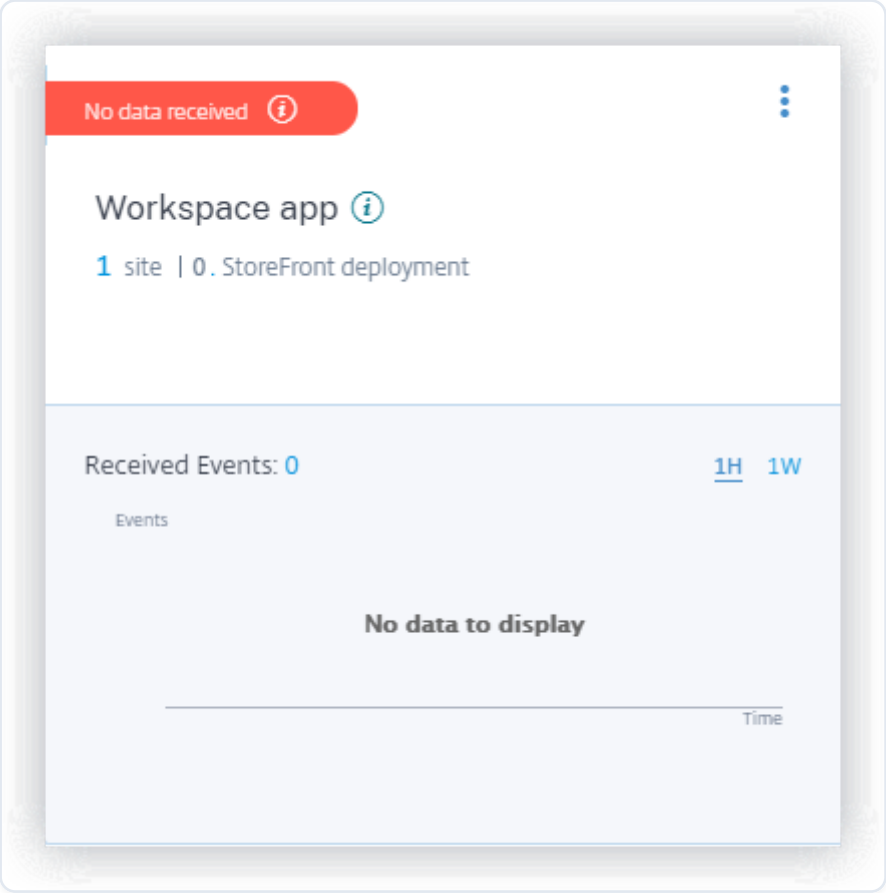
同じWorkspaceに複数のサイトを追加している場合、AnalyticsはWorkspace内のすべてのサイトのデータを処理および保存します。すべてのサイトでAnalyticsが正常に有効になると、成功メッセージが表示されます。



サイトカードには、デフォルトの時間選択である過去1時間の受信イベントが表示されます。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を表示できます。

データ処理を有効にした後、サイトカードに**データが受信されていません**というステータスが表示される場合があります。このステータスが表示される理由は2つあります。

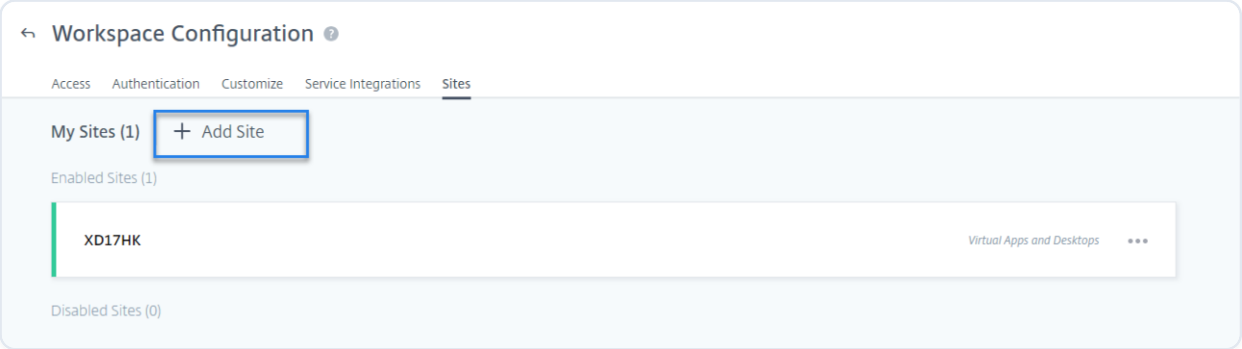
1. 初めてデータ処理をオンにした場合、イベントがCitrix Analyticsのイベントハブに到達するまでに時間がかかります。Citrix Analyticsがイベントを受信すると、ステータスは**データ処理中**に変わります。しばらくしてもステータスが変わらない場合は、**データソース**ページを更新してください。
2. Analytics は過去 1 時間、データソースからイベントを受信していません。



サイトを追加

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. Workspace構成ページで、**+サイトの追加**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、「ワークスペースでオンプレミスの仮想アプリとデスクトップを集約する」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、最近追加されたサイトをサイトカードで表示します。

オンプレミスサイトのCitrix Directorへの接続

Citrix Directorは、Citrix Virtual Apps and Desktops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、Citrix Analytics for Security (Security Analytics) 用のオンプレミスサイトを構成できます。サイトが構成されると、Directorは監視イベントをSecurity Analytics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 Security Analyticsにイベントを送信します。

クラウドとオンプレミスの両方の展開があるハイブリッド環境では、Security AnalyticsはCitrix MonitorサービスとCitrix Directorにオンボードされたサイトからイベントを受信します。

前提条件と構成手順

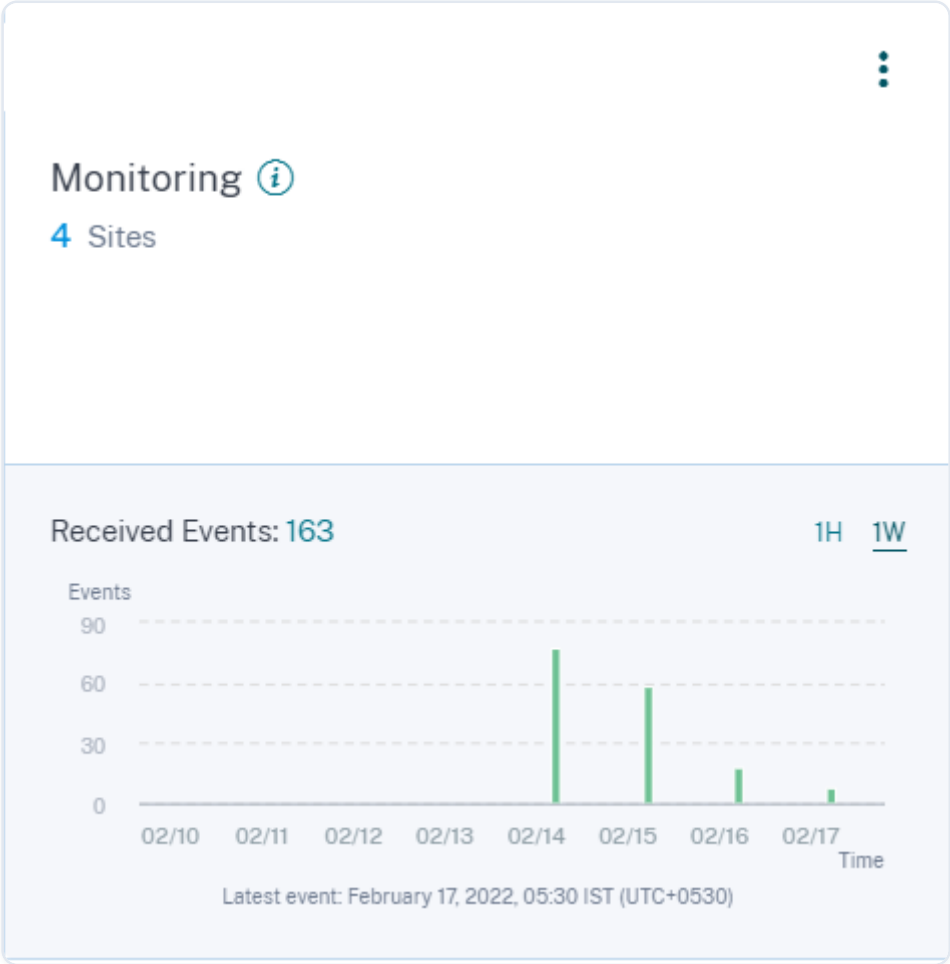
注

- 現在、Directorのユーザーインターフェイスには、Citrix Analytics for Performance™ (Performance Analytics) 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、Citrix Analytics for Security (Security Analytics) にも適用されます。Security AnalyticsのCitrix Cloudエンタイトルメントがアクティブな場合は、これらの手順に従ってCitrix Directorに接続できます。
- Citrix CloudアカウントにSecurity AnalyticsとPerformance Analyticsの両方のアクティブな資格があり、Performance Analytics用にサイトをすでに構成している場合、Security Analytics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は、Citrix Analytics for Performanceドキュメントを参照してください。

接続されている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. **Apps and Desktops- Monitoring**サイトカードで、オンプレミスサイトまたはクラウドサイト（該当する場合）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されます。

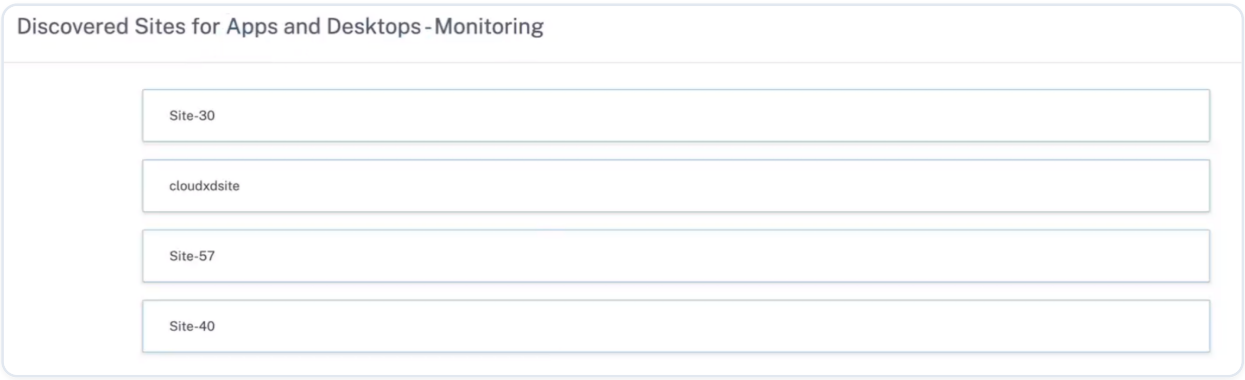


注

- 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が処理されるまでに時間がかかる（約1時間）ことがあり、**Apps and Desktops- Monitoring**サイトカードに接続されたサイトが表示されるまでに遅延が生じる可能性があります。

- 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デフォルトで有効になっています。要件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から最大限のメリットを得るためには、データ処理をオンにしておくことをお勧めします。

4. サイトをクリックして詳細を表示します。



Session Recording展開に接続する

Session Recordingを使用すると、Citrix Virtual Apps and DesktopsおよびCitrix DaaSの任意のユーザーセッションの画面アクティビティを記録できます。Session Recordingサーバーを構成して、ユーザーイベントをCitrix Analytics for Securityに送信できます。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洞察を提供するために処理されます。

前提条件

始める前に、以下を確認してください。

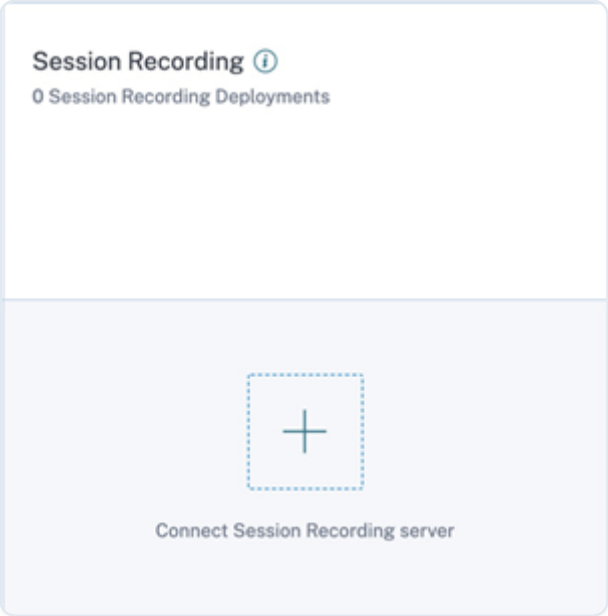
- Session RecordingサーバーとVDAエージェントは2103以降である必要があります。
- Session Recordingサーバーは、必要なアドレスに接続できる必要があります。URLの詳細については、ネットワーク要件を参照してください。
- Session Recording展開では、アウトバウンドインターネット接続用にポート443が開いている必要があります。ネットワーク上のプロキシサーバーは、Citrix Analytics for Securityとのこの通信を許可する必要があります。
- Citrix Virtual Apps and Desktops 7 1912 LTSR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

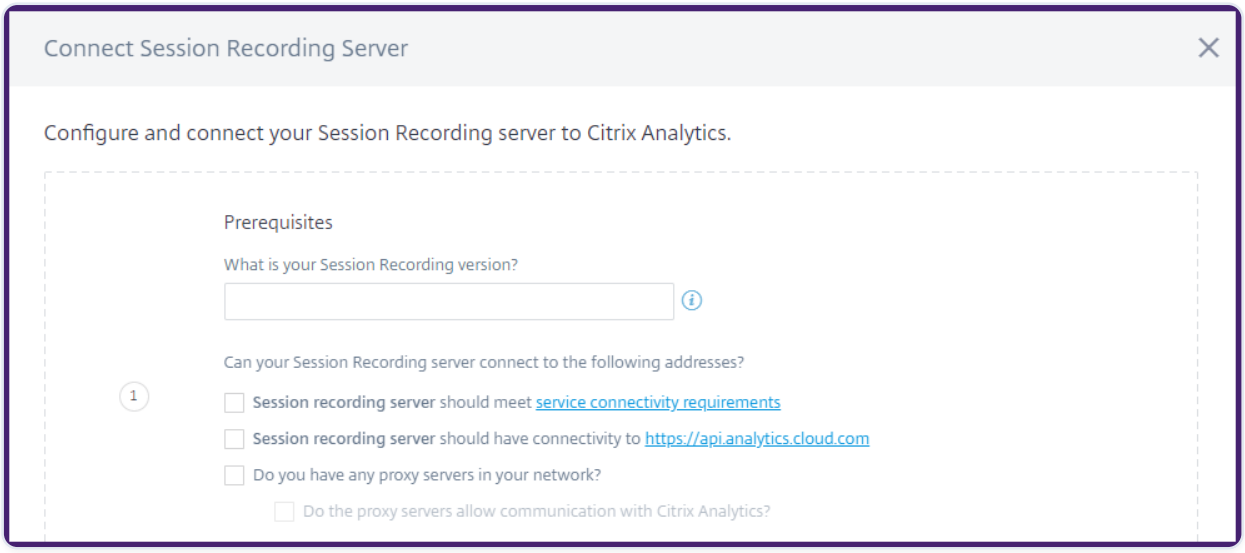
> **Session Recording**サービスを使用する際は、追加の接続要件を確認してください。

Session Recordingサーバーを構成する

1. **Apps and Desktops- Session Recording**サイトカードで、**Connect Session Recording server**をクリックします。



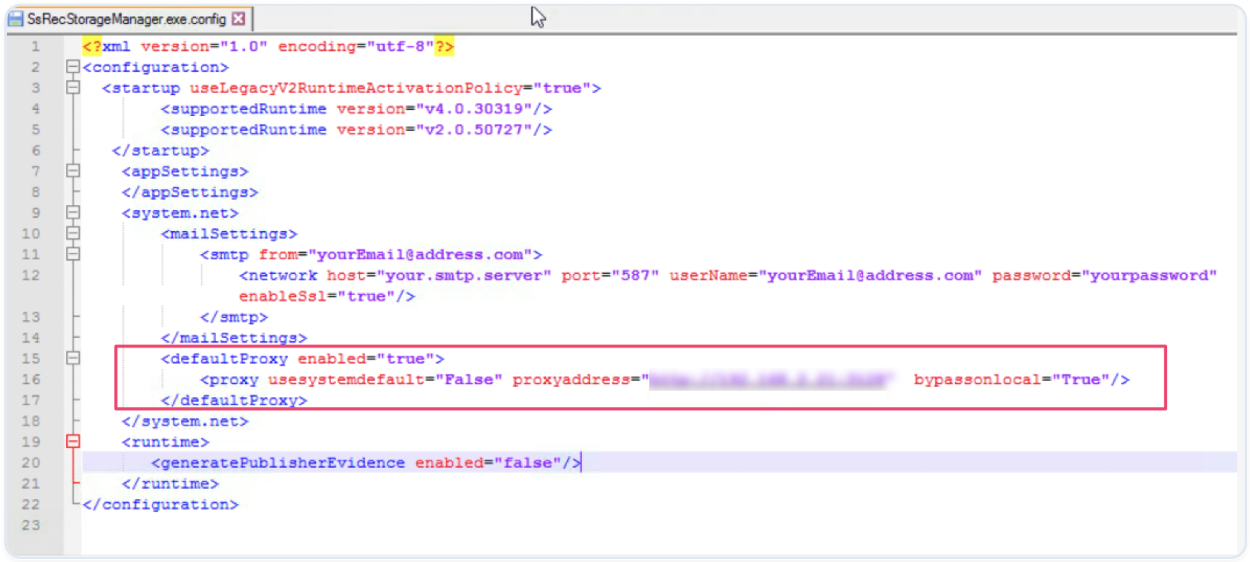
2. **Connect Session Recording Server**ページで、チェックリストを確認し、すべての必須要件を選択します。必須要件を選択しない場合、オプションは無効になります。



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*SsRecStorageManager.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`<Session Recording Server installation path>\bin\SsRecStorageManager.exe.config`にあります。

例: `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。ファイルは安全な場所に保管してください。

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. 展開環境に複数の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、各サーバーを構成する手順に従う必要があります。
7. Session Recordingサーバーで、設定をインポートするために次のコマンドを実行します。

```
&lt;Session Recording Server installation path>\bin\SsRecUtils.exe
-Import_SRCasConfigurations &lt;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 分析サービス
- Citrix Session Recording ストレージマネージャー

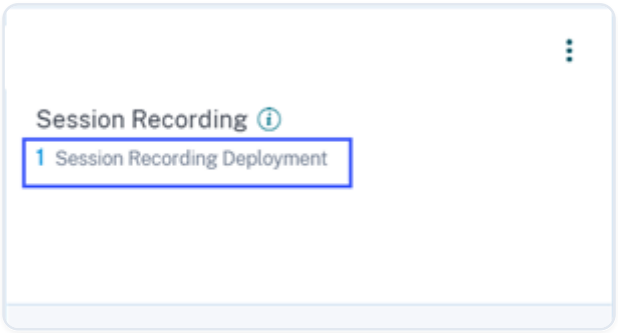
9. 構成が成功したら、Citrix Analytics for Securityに移動して、接続されているSession Recordingサーバーを表示します。Citrix Analytics for Securityがデータを処理できるように、「**データ処理を有効にする**」をクリックします。

> 「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、Citrix Analytics for Securityで接続されているSession Recordingサーバーを表示するには、まずApps and Desktopsセッションを起動する必要があります。そうしないと、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。

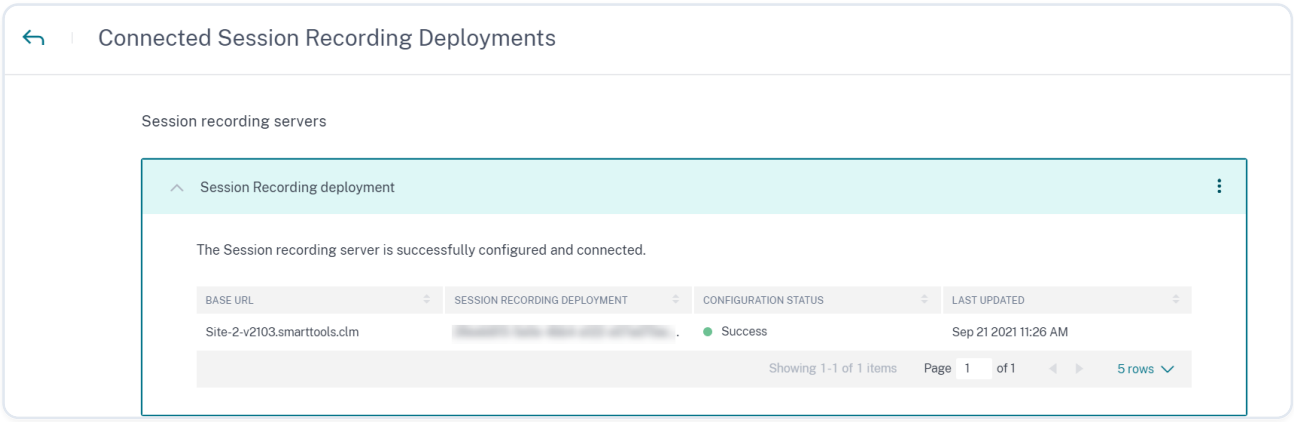
接続されている展開を表示

サーバーの展開は、構成が成功した場合にのみセッション記録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 との接続が確立されている構成済みサーバーの数が表示されます。

構成が成功した後もセッション記録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すると、Citrix Analytics for Security に接続されているサーバーグループが表示されます。たとえば、**1 Session Recording Deployment** をクリックすると、接続されているサーバーまたはサーバーグループが表示されます。各セッション記録サーバーは、ベースURLとServerGroupIDで表されます。



受信したイベントを表示

サイトカードには、接続されているセッション記録の展開と、これらの展開から過去1時間（デフォルトの時間選択）に受信したイベントが表示されます。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でイベントが表示されます。

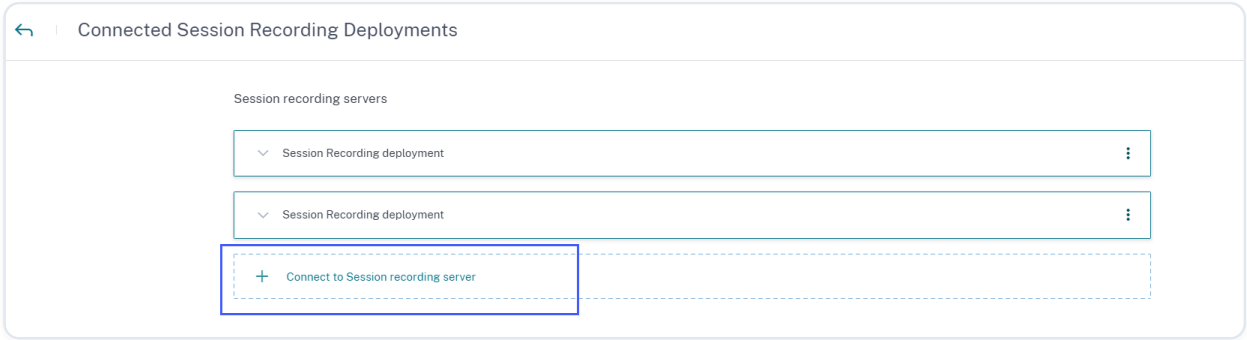
データ処理を有効にした後、サイトカードに「**データが受信されていません**」というステータスが表示されることがあります。このステータスが表示される理由は2つあります。

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、ステータスは「**データ処理中**」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てください。
2. Citrix Analyticsが過去1時間、データソースからイベントを受信していません。

セッション記録サーバーを追加

セッション記録サーバーを追加するには、次のいずれかを実行します。

- 「**接続されているセッション記録の展開**」ページで、「**セッション記録サーバーに接続**」をクリックします。



- 「**Apps and Desktops- Session Recording**」サイトカードで、縦の省略記号（⋮）をクリックし、「**Connect Session Recording server**」を選択します。

セッションレコーディング接続(/en-us/citrix-analytics/media/sr-connect.png)

構成ファイルをダウンロードし、Session Recordingサーバーを構成する手順に従ってください。

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、削除したい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。

   セッションレコーディングサーバーを削除(/en-us/citrix-analytics/media/sr-remove.png)
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。

   ```
   &lt;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（旧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、プリンター名、印刷ファイル名、合計印刷部数などの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のみで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**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、これらのログを使用して、ユーザーのリスク分析と調査を行うことができます。

デフォルトでは、これらの印刷ログの収集と送信を行う印刷テレメトリ機能は、Virtual Delivery Agent (VDA) で無効になっています。

印刷テレメトリと印刷ログのCitrix Analytics for Securityへの送信を有効にするには、レジストリキーを作成し、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。詳細については、「Citrix Virtual Apps and Desktops 7 2203 baseline components」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、次のシナリオを持つ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バージョンがCitrix Virtual Apps and Desktops 7 2203 LTSRより低い既存のマスターイメージで印刷テレメトリを有効にする

1. マスターVDAマシンにログオンし、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-PrintService/Operational
   - ShowJobTitleInEventLogs

   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。詳細については、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. マシンの電源をオフにし、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、 をクリックして、画面の指示に従います。詳細については、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。構成は24時間以内に自動的にプッシュされます。構成がすで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**** 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以降と同じ既存のマスターイメージで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-PrintService/Operational
   - ShowJobTitleInEventLogs

   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、 をクリックして、画面の指示に従います。
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**** 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します

> **注**
>
> オプション2の方法は、静的マシンでのみ機能します。ランダムマシンについては、オプション1の方法 (上記のとおり) 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-PrintService/Operational
- ShowJobTitleInEventLogs

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**
>
> いずれかのドメインコントローラーで、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**** 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VM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、以下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-PrintService/Operational
   - ShowJobTitleInEventLogs

   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、**Master Image**オプションを選択します。詳細については、「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。詳細については、「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。詳細については、「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。詳細については、「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。構成は、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

電源管理されていないマシンには、以下のシナリオを持つ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

Citrix Virtual Apps and Desktops 7 2203 LTSRより前のVDAバージョンを使用している既存の物理VDAで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-PrintService/Operational
   - ShowJobTitleInEventLogs

   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。詳細については、「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。構成は24時間以内に自動的にプッシュされます。構成がすで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で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. VM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-PrintService/Operational
   - ShowJobTitleInEventLogs

   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、Remote PC Access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。詳細については、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。詳細については、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。構成は、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。

レジストリキーの作成

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を使用し、展開内の物理VDAの数が少ない場合に適用します。
- 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。この方法は、展開内の物理VDAマシンの数が多い場合や、すべてのVDAで印刷テレメトリを有効にする必要がある場合に適用します。

レジストリキーの詳細

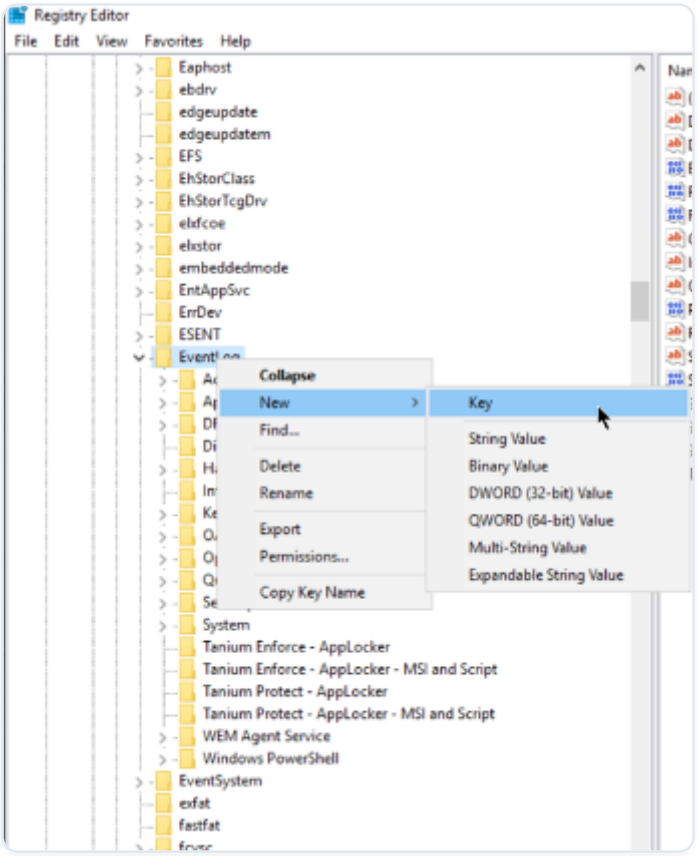
NO.	レジストリキー名	キーの目的	レジストリの詳細
1	Microsoft-Windows-PrintService/Operational	イベントビューアーで印刷サービスログを有効にします。	**レジストリパス**: HKLM:\SYSTEM\CurrentControlSet\Services\EventLog

NO.	レジストリキー名	キーの目的	レジストリの詳細
2	ShowJobTitleInEventLogs	印刷ジョブ名が印刷イベントログに含まれるかどうかを制御します。含まれない場合は、汎用ジョブ名「Print Document」と見なされます。	**レジストリハイブ**: HKEY_LOCAL_MACHINE
			レジストリパス: Software\Policies\Microsoft\Windows NT\Printers
			値の名前: ShowJobTitleInEventLogs
			値の型: REG_DWORD
			値: 1

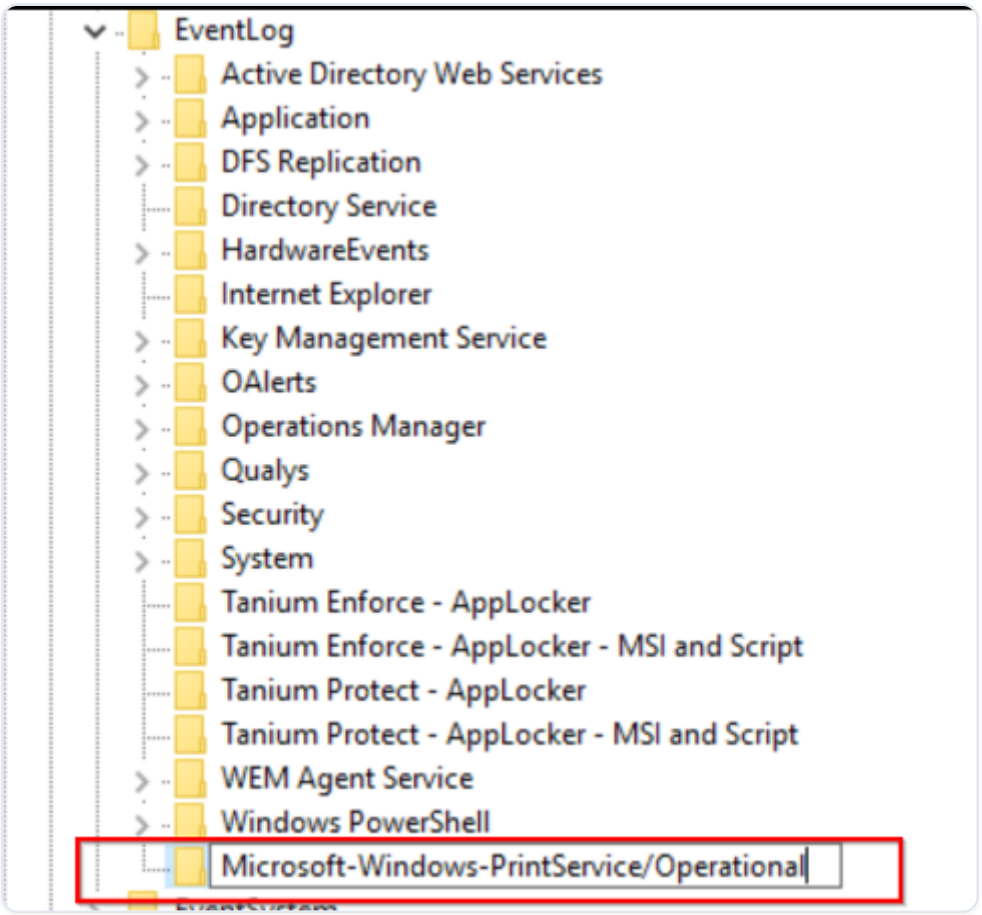
VDAマシンでレジストリキーを手動で作成する

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、そのマスターイメージを使用して作成されるすべての種類の VDA でキーを永続的に保持できます。

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. 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。

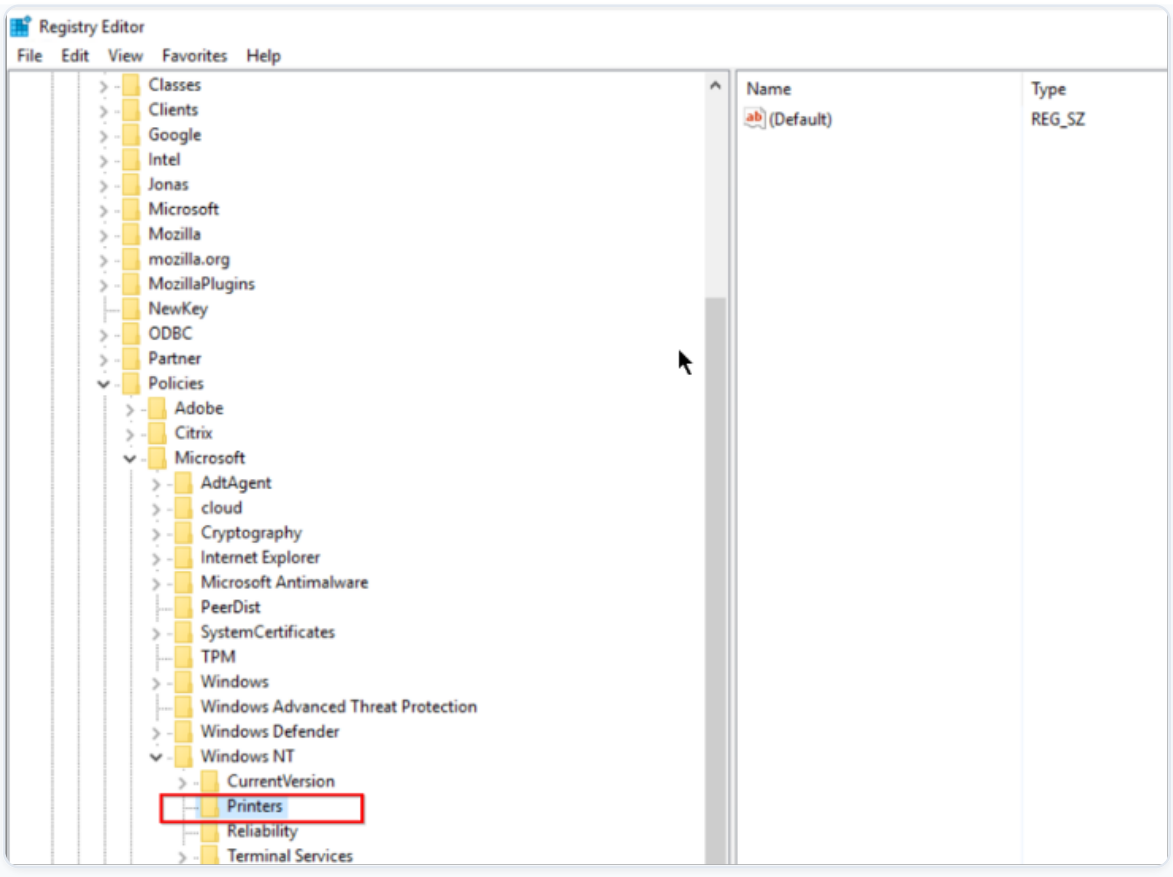


5. **Microsoft-Windows-PrintService/Operational** という名前のキーを作成します。このキーにより、印刷サービスのログが有効になります。

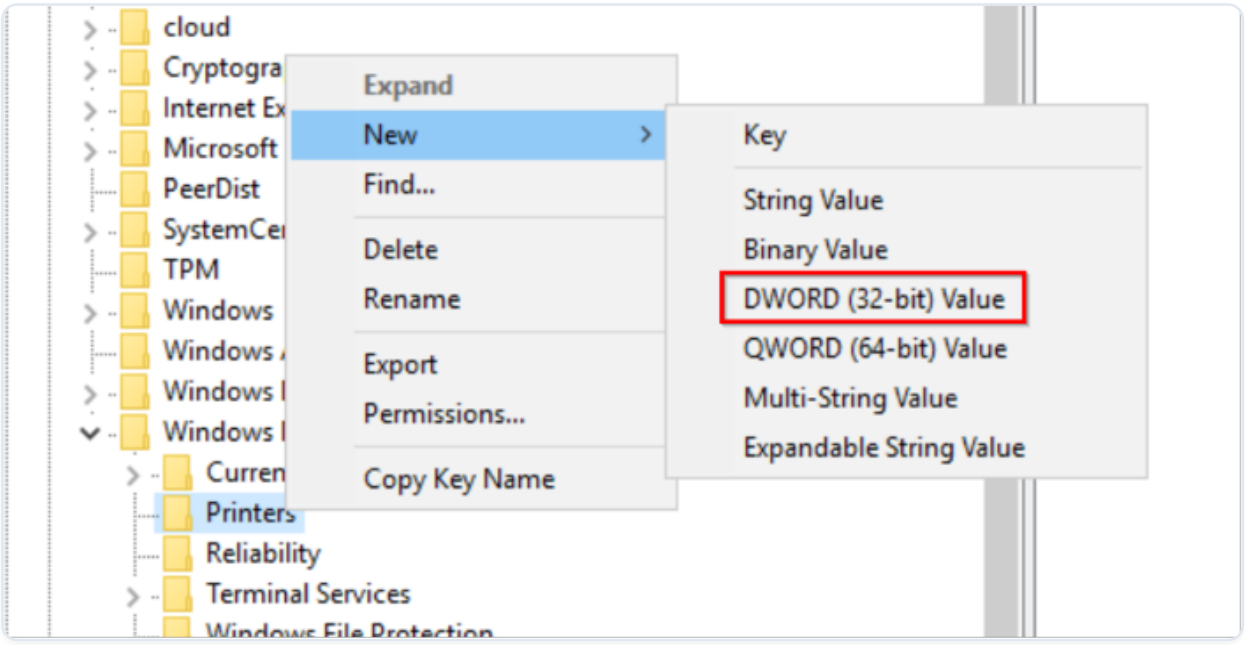


6. **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers** に移動します。

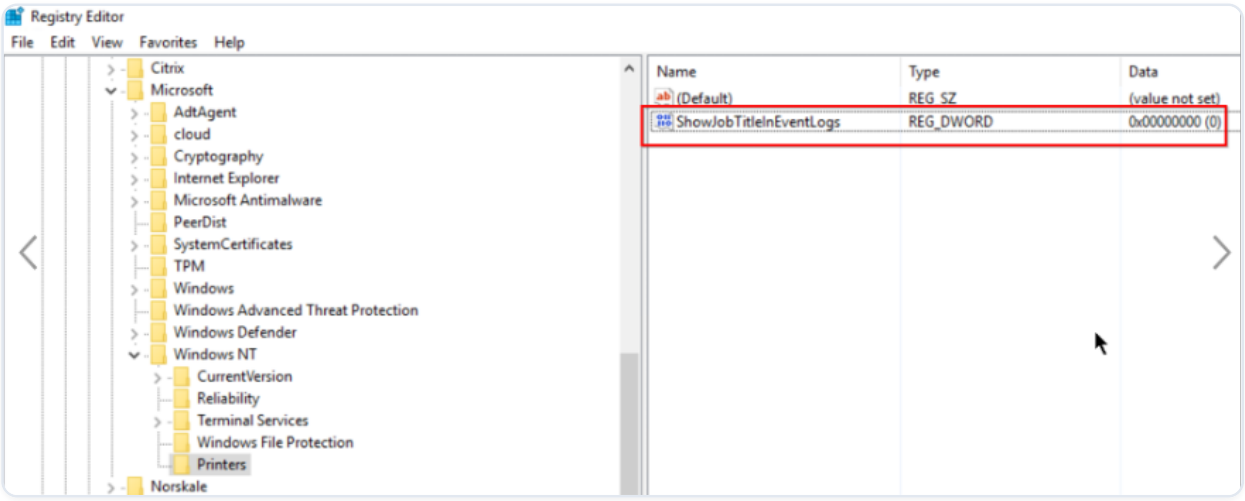
> **注**
>
> Printers フォルダーがない場合は、Windows NT フォルダーに Printers という名前のキーを作成します。



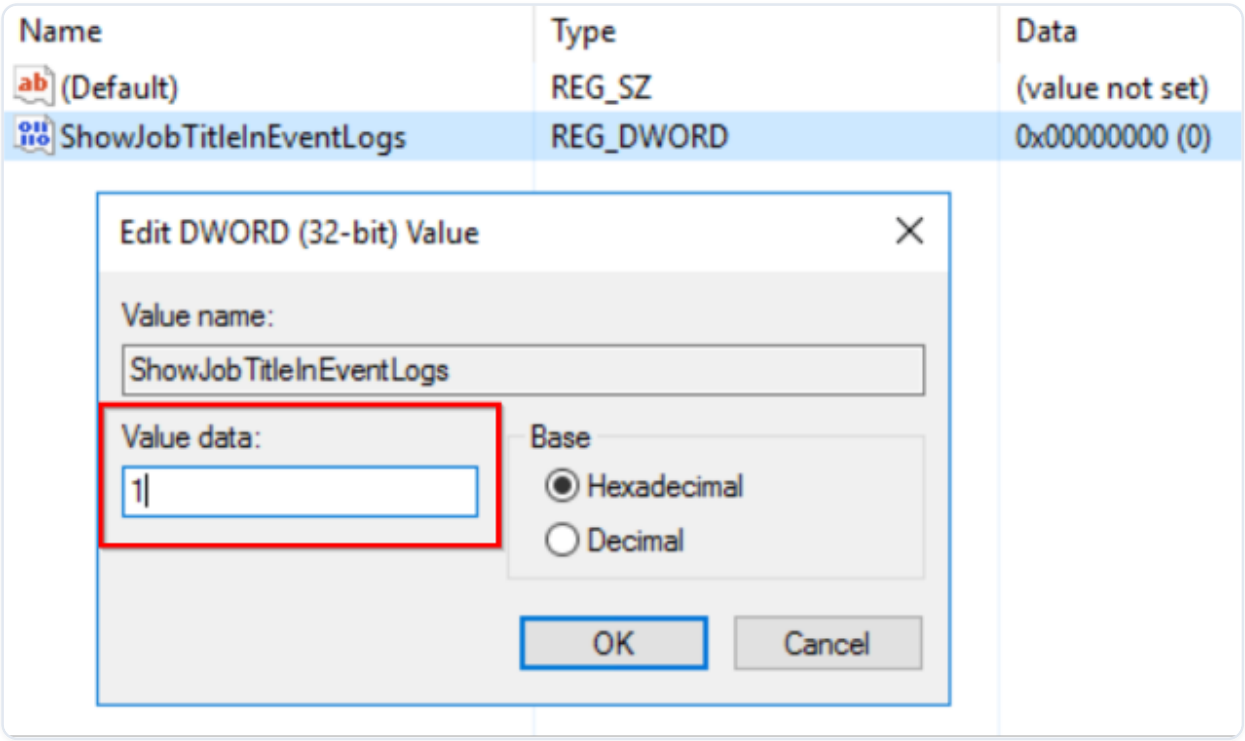
7. **Printers** フォルダーを右クリックし、**新規 > DWORD (32 ビット) 値** を選択します。



8. **ShowJobTitleInEventLogs** という名前の値を作成します。



9. **ShowJobTitleInEventLogs** を右クリックし、**変更** を選択します。**値のデータ** に 1 と入力し、**OK** をクリックします。

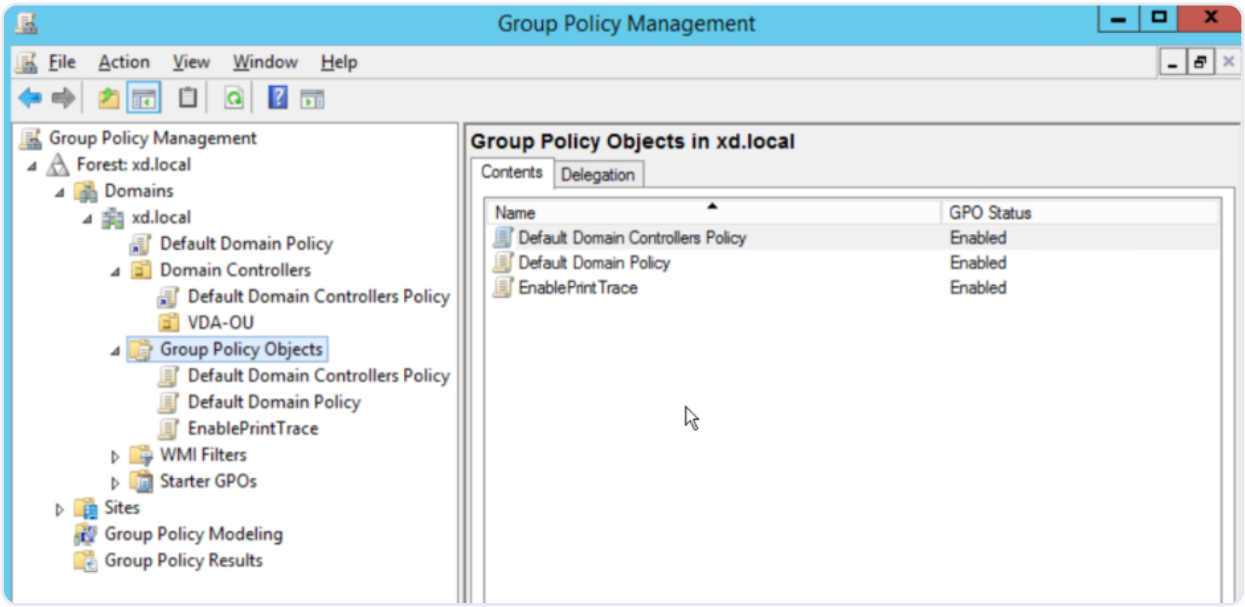


GPO を使用して複数の VDA にレジストリキーを作成する

このアプローチは永続 VDA にのみ機能し、レジストリキーの作成後に VDA の再起動が必要です。永続 VDA とは、再起動後も状態を維持するマシンです。再起動後もユーザーデータは失われません。

レジストリキーを含むレジストリ GPO を作成する

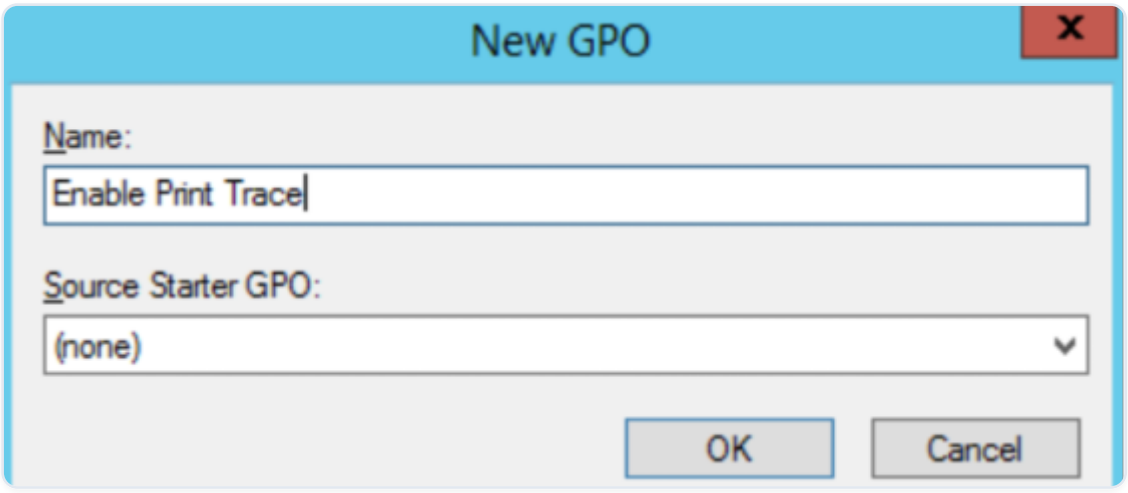
1. グループポリシー管理を開き、**グループポリシーオブジェクト** を右クリックします。



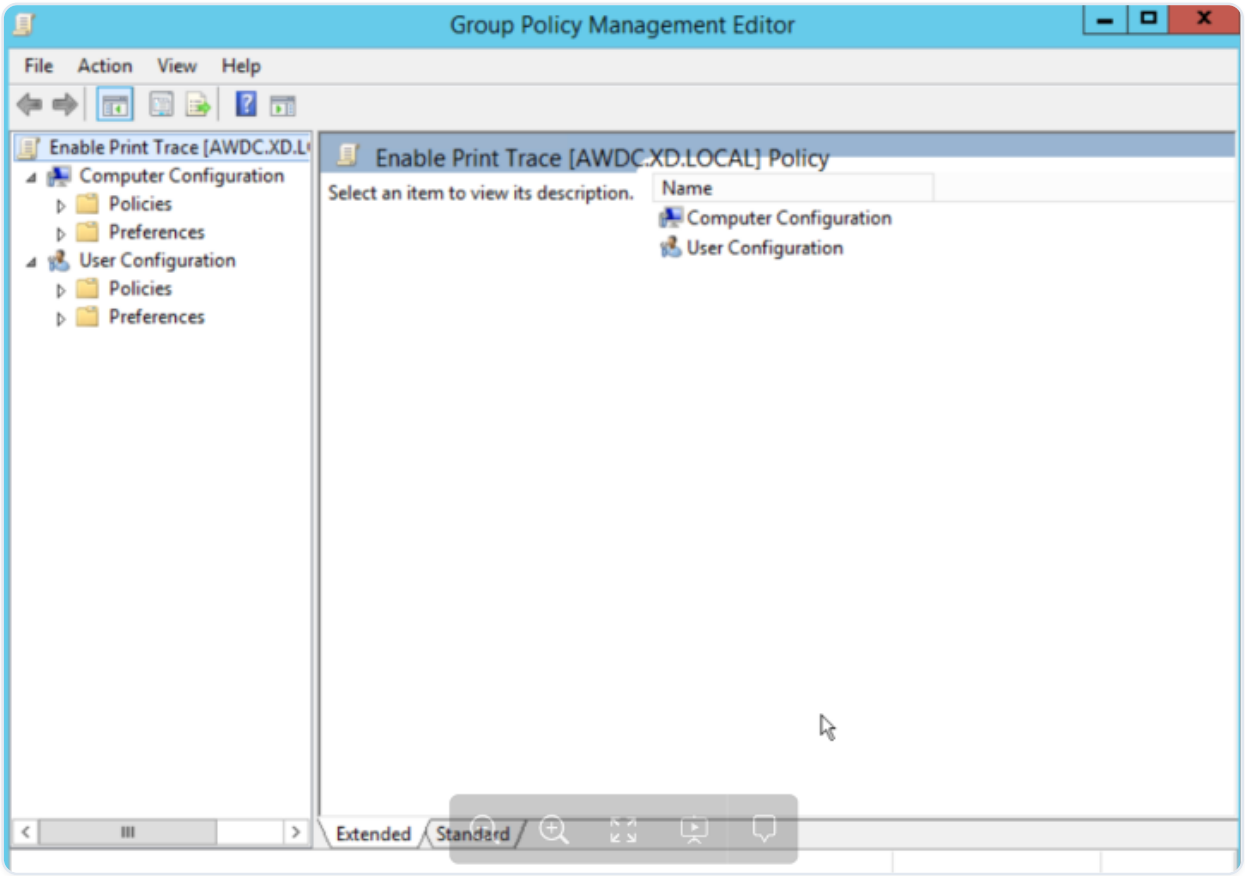
2. **新しい GPO** ウィンドウで、次のフィールドに値を入力します。

   - 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 **印刷トレースを有効にする** オブジェクトを右クリックし、**編集** を選択します。



5. 「**コンピューターの構成**」リストで、「**基本設定 > Windows の設定**」を選択します。

   Windows の設定(/en-us/citrix-analytics/media/windows-settings.png)

6. 「**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。

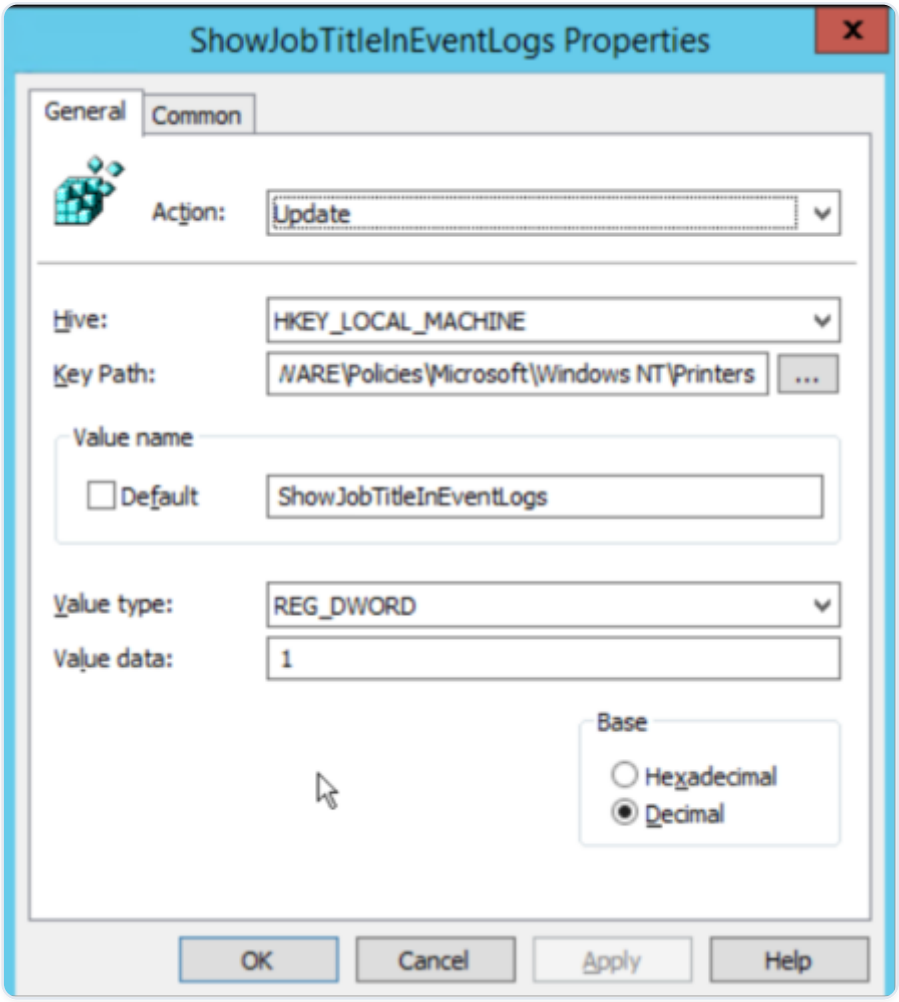
   - アクション: 更新

- ハイブ: HKEY_LOCAL_MACHINE
- キーパス: SYSTEM\CurrentControlSet\Services\EventLog\Microsoft-Windows-PrintService/Operational

新しいレジストリ項目(/en-us/citrix-analytics/media/new-registry-item.png)

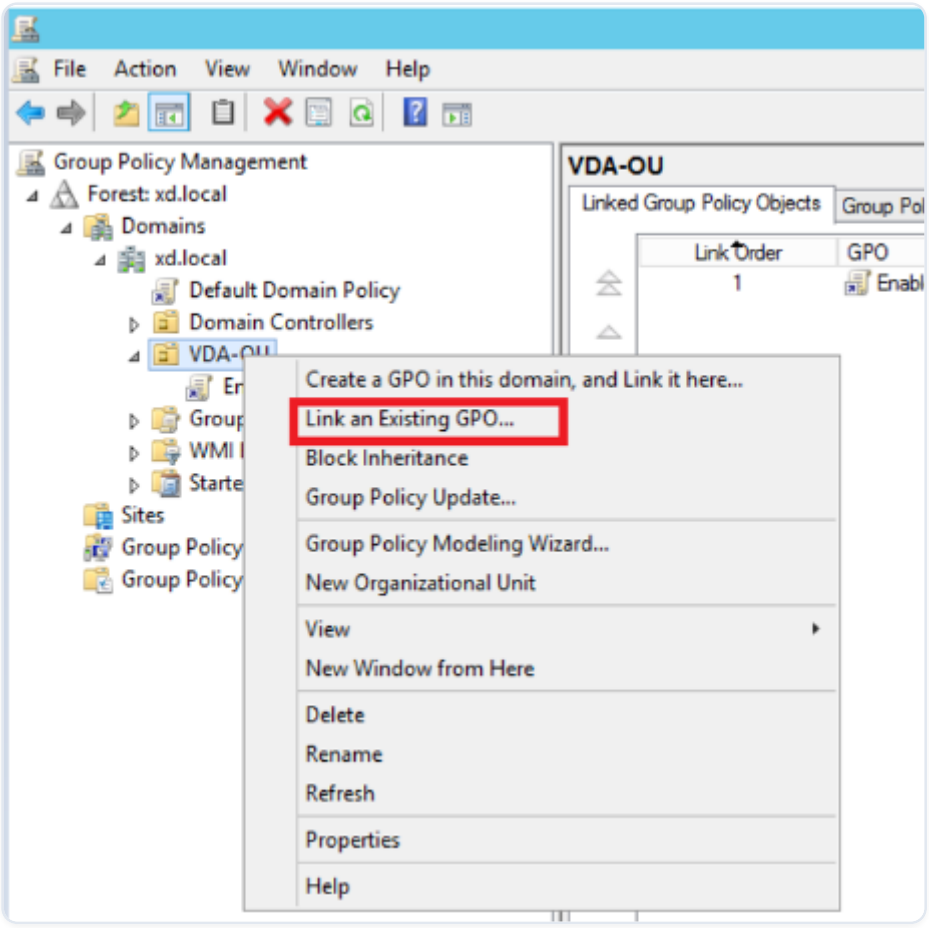
7. 「**適用**」を選択し、次に「**OK**」を選択します。
8. 再度、「**レジストリ**」を右クリックし、「**新規 > レジストリ項目**」を選択します。印刷ジョブ名を有効にするには、次のプロパティを入力します。

- アクション: 更新
- ハイブ: HKEY_LOCAL_MACHINE
- キーパス: SOFTWARE\Policies\Microsoft\Windows NT\Printers
- 値の名前: ShowJobTitleInEventLogs
- 値の型: REG_DWORD
- 値のデータ: 1
- 基数: 10進数

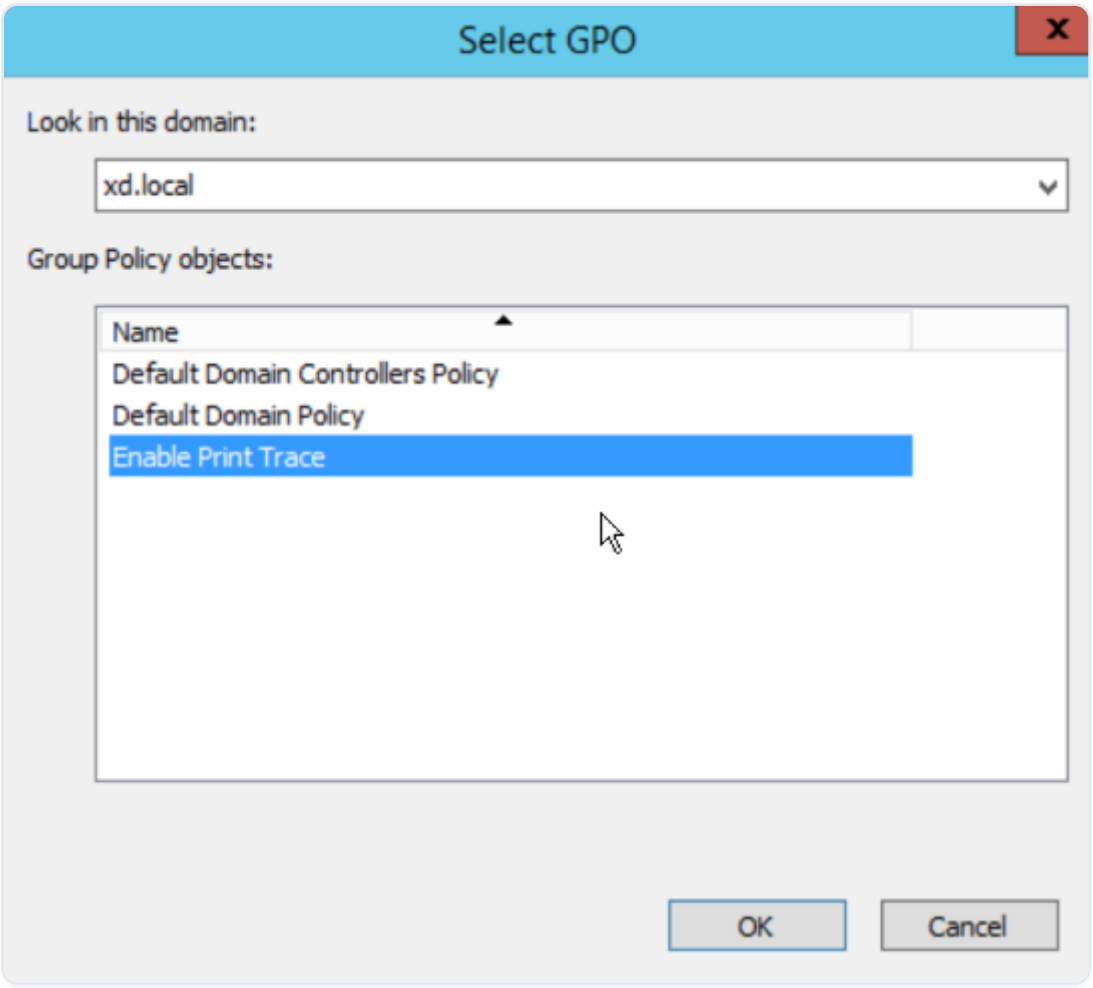


組織単位の印刷トレースを有効にする

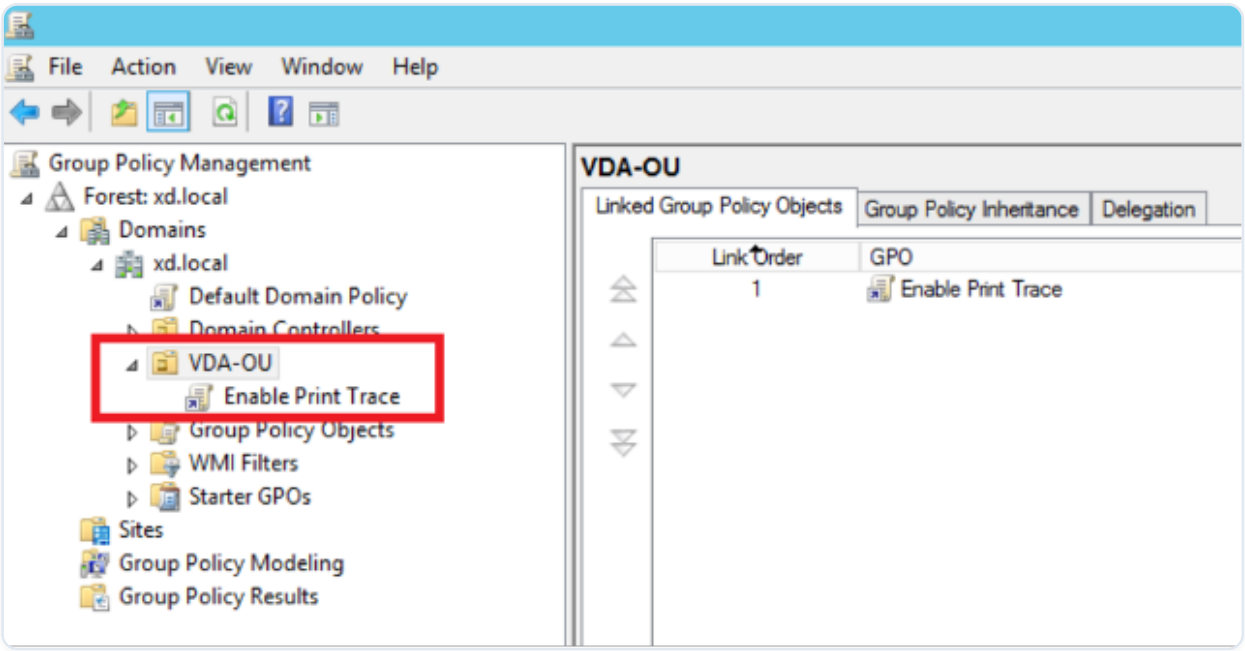
1. **グループポリシー管理**を開き、ドメイン (例: xd.local) またはVDAがその一部である場合はOU (例: VDA-OU) を選択します。
2. ドメイン (xd.local) またはOU (VDA-OU) を右クリックし、**既存のGPOをリンク**を選択します。



3. **GPOの選択**ダイアログボックスで、 を選択し、**OK**を選択します。



4. **印刷トレースを有効にする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失われ、Citrix Analyticsでは利用できなくなります。
- この再起動は、単一セッションVDAへの影響は小さいです。これは、一度にアクティブにできるセッションが1つだけであり、それに伴いイベントの数が少ないためです。
- この再起動は、マルチセッションVDAへの影響は大きいです。これは、再起動中にすべてのアクティブな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です。

Citrix DaaSのクリップボードテレメトリを有効にする

Citrix DaaS（旧称Citrix Virtual Apps and Desktopsサービス）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、貴重な情報を提供します。

セキュリティ管理者として、Citrix Analytics for Securityの**検索**ページで**Apps and Desktops**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利用できます。

注

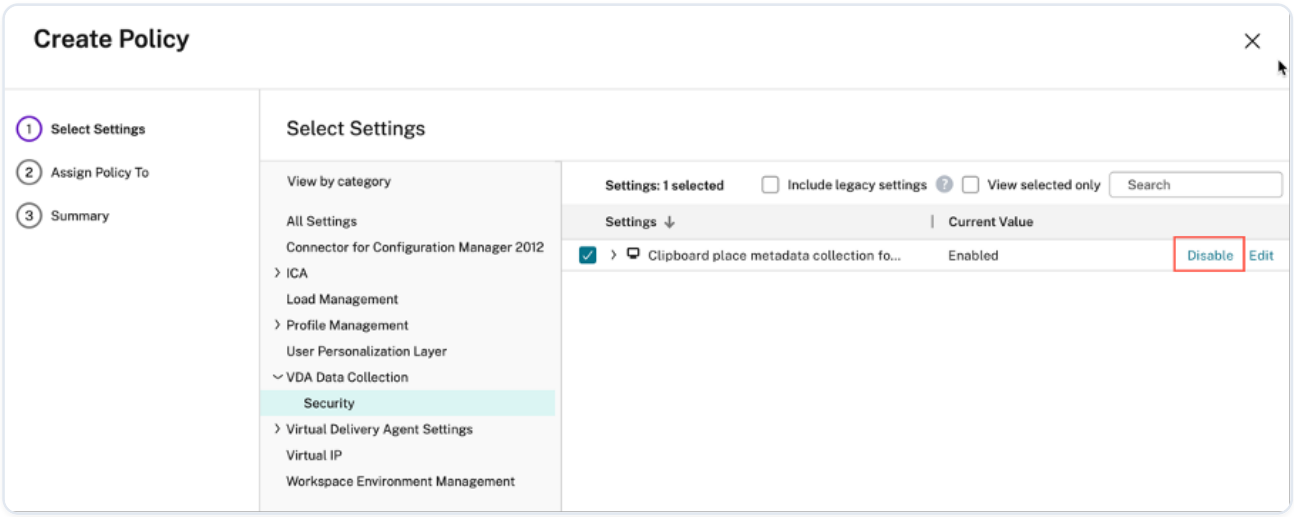
- デフォルトでは、これらのクリップボードログの収集と送信はVirtual Delivery Agent (VDA) で有効になっています。
- この構成はWindows VDAにのみ適用されます。

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。詳細については、「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**設定が禁止状態に構成されていないことを確認してください。詳細については、「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。

セキュリティ監視のためのクリップボードメタデータ収集ポリシーを使用して、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データ収集**の下にある**セキュリティ**を選択し、ポリシーをチェックして、**無効にする**をクリックします。



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メタデータ収集」を参照してください。

データソースでのデータ処理のオン/オフを切り替える

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処理を停止します。Apps and Desktops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に適用されます。

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。

マイクロソフト アクティブ ディレクトリとアジュール アクティブ ディレクトリの統合

> **注:**
>
> 2023年7月以降、Microsoft は Azure Active Directory (Azure AD) を Microsoft Entra ID に名称変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD へのすべての参照は、Microsoft Entra ID を指します。

Active Directory または Azure Active Directory を接続し、組織のドメインからユーザーの詳細とユーザーグループを Citrix Analytics for Security にインポートします。

この統合により、役職、組織、オフィス所在地、メール、連絡先などのユーザーIDの詳細がCitrix Analytics for Securityのユーザープロファイルを強化します。ユーザープロファイルページで、これらのユーザー詳細を表示でき、リスク調査と分析に役立ちます。

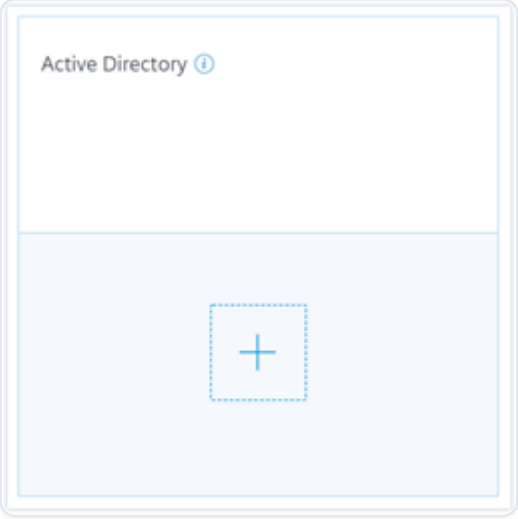
前提条件

- Active Directory を Citrix Analytics for Security に接続する場合は、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。詳細については、「Active Directory を Citrix Cloud に接続する」を参照してください。
- Azure Active Directory を Citrix Analytics for Security に接続する場合は、まず Azure 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。詳細については、「Azure Active Directory を Citrix Cloud に接続する」を参照してください。

Microsoft Active Directory を接続する

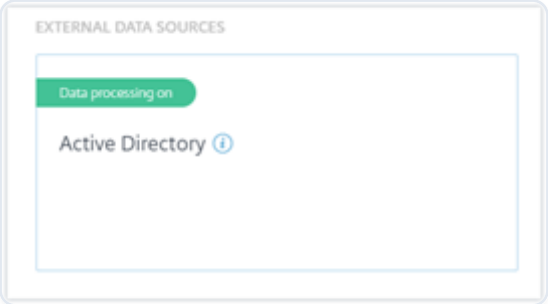
Active Directory を Citrix Analytics for Security に接続するには、次の手順を実行します。

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. **Active Directory** サイトカードで、プラス記号の **+** をクリックします。



3. Citrix Analytics は、Active Directory を Citrix Cloud™ アカウントに接続するよう促します。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、Citrix Analytics 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** ページで、Active Directory サイトカードに **データ処理オン** と表示されます。



「**データ処理オン**」のステータスは、Active Directoryが検出され、ユーザー情報がActive Directoryから取得されていることを示します。

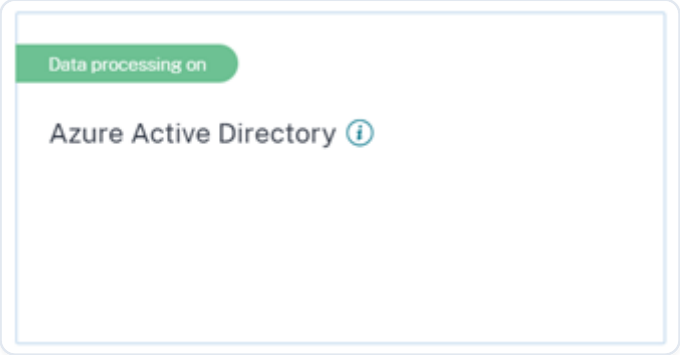
マイクロソフト アジュール アクティブディレクトリを接続する

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。

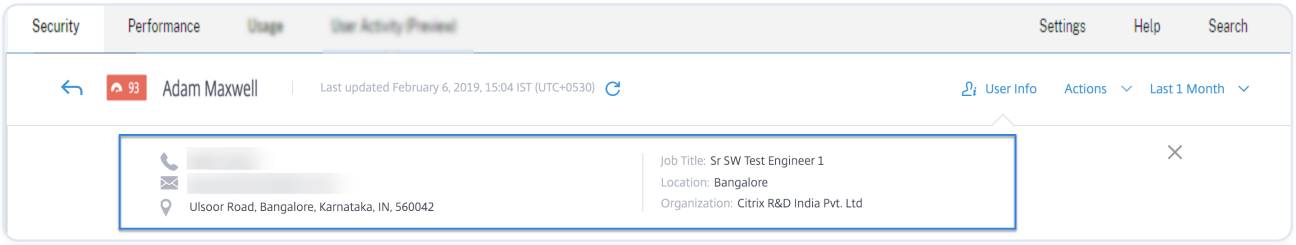
   アジュール アクティブディレクトリを追加(/en-us/citrix-analytics/media/azure-ad-add.png)
3. Citrix Analyticsは、Azure Active DirectoryをCitrix Cloudアカウントに接続するよう促します。詳細については、「Azure Active DirectoryをCitrix Cloudに接続する」を参照してください。

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**ページで、**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から取得されていることを示します。



ユーザー情報の表示

セキュリティタブから、リスクのある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に存在する場合、ユーザープロファイルページで役職、組織、メール、連絡先番号を表示できます。



マイクロソフト グラフ セキュリティ 連携

Microsoft Graph Securityは、複数のセキュリティプロバイダーからデータを集約する外部データソースです。また、ユーザー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の次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 ID 保護
- マイクロソフト ディフェンダー フォー エンドポイント

セキュリティプロバイダーの詳細については、次のリンクを参照してください。

- **Azure AD Identity Protection**については、`<https://docs.microsoft.com/ja-jp/azure/active-directory/reports-monitoring/concept-risk-events>`
- **Microsoft Defender for Endpoint**については、`<https://docs.microsoft.com/ja-jp/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、Microsoft IDプラットフォームから、テナントに代わって必要な権限を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、以下を確認してください。

- 管理者が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ること。
- エンドユーザーが職場または学校アカウントでMicrosoft Storeにサインインしていること。

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** に移動し、次に**外部データソース**セクションに移動します。

2. Microsoft Graph Securityサイトカードでプラス記号（+）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。

   MSGオンボーディング(/en-us/citrix-analytics/media/msg-plus.png)

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。

   MSGオンボーディング(/en-us/citrix-analytics/media/msg-authenticate.png)

5. **同意**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。Microsoft Graph SecurityデータソースがCitrix Cloud™アカウントにリンクされました。

   MSGオンボーディング(/en-us/citrix-analytics/media/msg-permissions.png)

データ処理のオン/オフを切り替える

データ処理を無効にするには、サイトカードの縦三点リーダー（⋮）をクリックし、**データ処理をオフにする**を選択します。これにより、Citrix Analyticsがこのデータソースのデータを処理するのを停止します。

サイトカードで**データ処理をオンにする**を選択することで、データ処理を再度オンにできます。

MSGオンボーディング(/en-us/citrix-analytics/media/msg-data-processing.png)

Microsoft Graph Securityリスクインジケーターの詳細については、Microsoft Graph Securityリスクインジケーター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) 統合

> **注**
>
> SIEM 統合、SIEM へのデータのエクスポート、およびフィードバックの提供に関する支援をリクエストするには、mailto:CAS-PM-Ext@cloud.com にお問い合わせください。

> Citrix Analytics for Security™ を SIEM サービスと統合し、Citrix IT 環境からユーザーデータを SIEM にエクスポートします。エクスポートされたデータを SIEM で利用可能なデータと関連付けて、組織のセキュリティ体制に関するより深い洞察を得ます。

この統合により、Citrix Analytics for Security と SIEM の両方の価値が向上します。

利点

- セキュリティ運用チームが、異なるログからのデータを関連付け、分析し、検索できるようにします。
- 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、迅速に修復するのに役立ちます。
- セキュリティアラートを一元的に可視化します。
- リスクインジケーター、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に、潜在的なセキュリティ脅威を検出するための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 内で接続されている外部データソースと結合および関連付ける機能。

SIEM 統合アーキテクチャ

SIEM 統合は、Citrix Analytics for Security クラウドにデプロイされた北向きの Kafka と接続します。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 設定ファイルで提供されているパラメータと、JKS ファイルまたは PEM ファイルの証明書詳

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 に接続してデータをプルできます。

- **Logstash エンジン**: 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 からのリスクインサイトデータを、Logstash でサポートされている 出力プラグイン のいずれかに送信できます。

以下のSIEMソリューションアーキテクチャ図を参照して、Citrix Analytics for SecurityからSIEMサービスへのデータの流れを理解してください。

SIEMソリューションアーキテクチャ(/en-us/citrix-analytics/media/siem-solution-architecture.png)

データ転送のオン/オフを切り替える

Citrix Analytics for Securityからのデータ転送を停止するには：

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。

> データ転送がオンになっています(/en-us/citrix-analytics/media/data-transmission-turnedon.png)

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

SIEMにデータを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
- 事前入力された構成をダウンロードし、SIEM環境をセットアップする
- エクスポートするデータイベント

SIEMエクスポートアカウントのセットアップ

1. アカウントを設定するには、 **> >** の順に移動します。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。

アカウント設定(/en-us/citrix-analytics/media/account-set-up.png)

2. をクリックして構成ファイルを生成します。構成ファイルには、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 および SSL 属性も事前設定されます。

SIEM の構成と環境設定

必要に応じて SIEM 環境を選択します。Citrix Analytics for Security は、次のサービスと統合できます。詳細情報と SIEM 固有の構成については、次のリンクを参照してください。

- スプランク
- マイクロソフト センチネル
- エラスティックサーチ
- Kafka または Logstash ベースのデータコネクタを使用するその他の SIEM

SIEM 環境(/en-us/citrix-analytics/media/siem-environment.png)

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

SIEM エクスポートの一部として、2 種類のデータセットがあります。

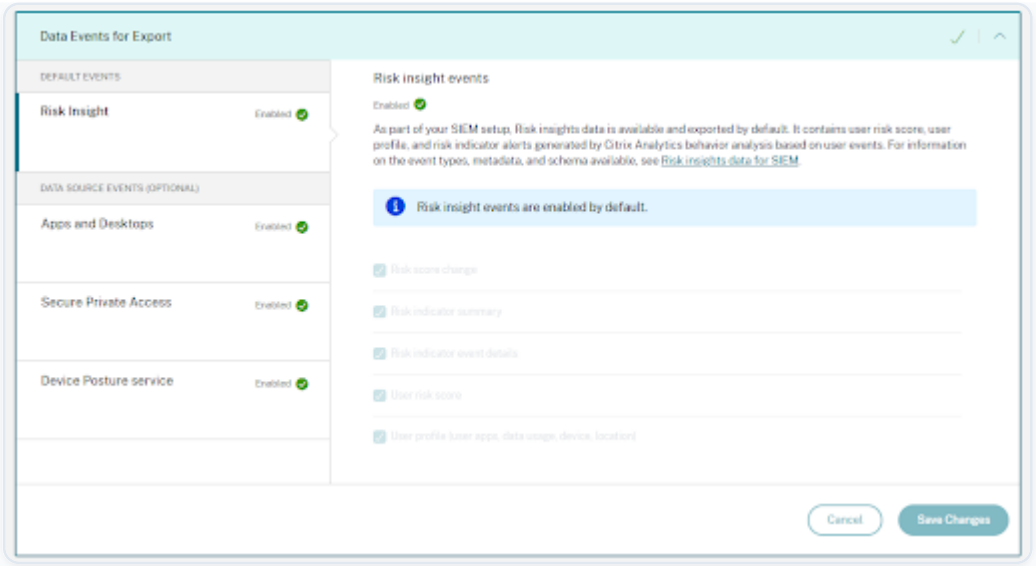
1. **リスクインサイトイベント（デフォルトのエクスポート）** – アカウント構成と SIEM セットアップが完了すると、デフォルトデータ（リスクインサイトイベント）が SIEM 展開に流れ始めます。リスクインサイトデータには、ユーザーリスクスコア、ユーザープロファイル、およびリスクインジケーターアラートが含まれます。これらは、Citrix Analytics の機械学習アルゴリズム、ユーザー行動分析、およびユーザーイベントに基づいて生成されます。利用可能なイベントタイプ、メタデータ、およびスキーマについては、「SIEM のリスクインサイトデータ」を参照してください。
2. **データソースイベント（オプションのエクスポート）** - さらに、データエクスポート機能を構成して、Citrix Analytics for Security が有効な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できます。Citrix 環境で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可能な未処理のリアルタイムユーザーおよび製品使用状況データです。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、およびセキュリティおよび IT インフラ全体での他の非 Citrix データソースイベントとの関連付けに使用できます。

現在、Citrix Analytics for Security は、Citrix Virtual Apps and Desktops™、Secure Private Access、および Device Posture サービスというデータソースのユーザーイベントを SIEM に送信します。

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。

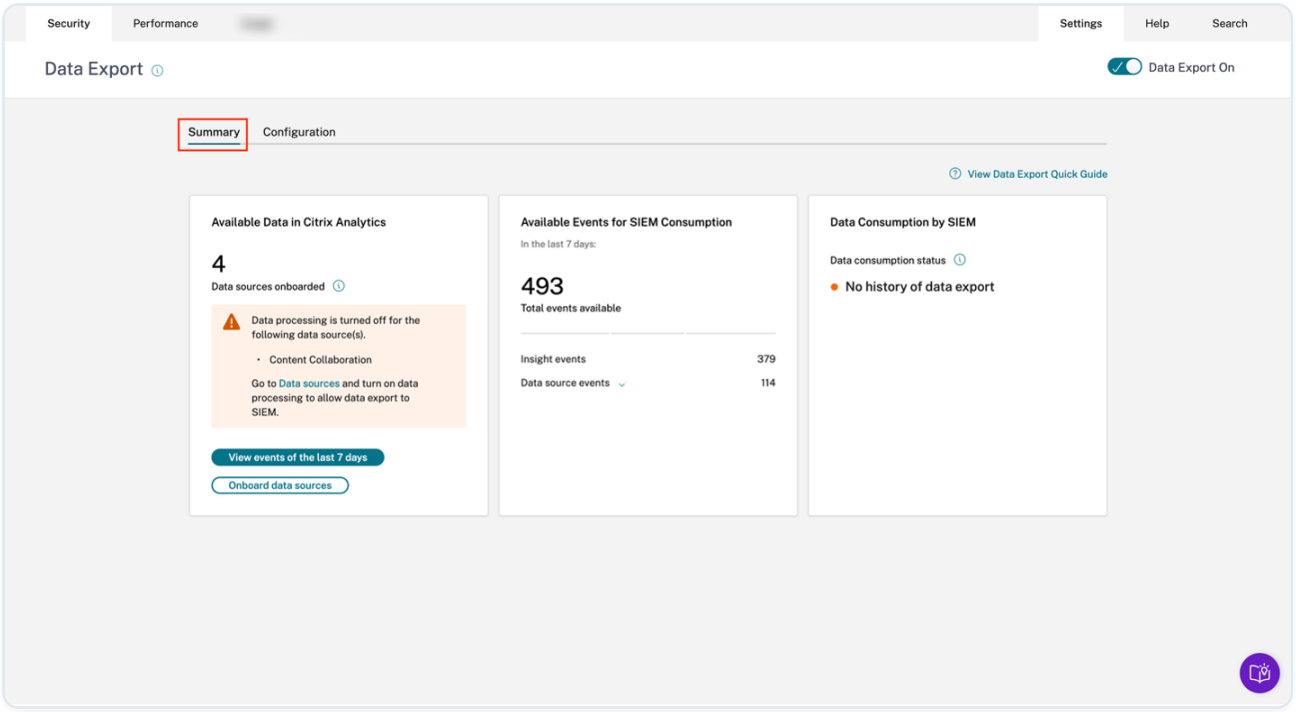
注

Logstashデータブローカーを使用しているお客様は、Citrix Analytics for Securityポータルから最新の構成ファイルをダウンロードし、Logstashサービス展開で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インデックスで利用可能になります。



SIEM統合のトラブルシューティング

セキュリティのデータエクスポートビューには、管理者がCitrix AnalyticsとのSIEM統合をトラブルシューティングするのに役立つ**概要**タブが含まれています。**概要**ダッシュボードは、トラブルシューティングプロセスを支援するチェックポイントを通じて、データの健全性とフローを可視化します。



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連携

Citrix Analytics for SecurityをSplunkと連携させ、Citrix IT環境からのユーザーデータをSplunkにエクスポートして(/ja-jp/security-analytics/siem-integration/entity-data-model.html)、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。

連携の利点と、SIEMに送信される処理済みデータの種類について詳しくは、(/ja-jp/security-analytics/siem-integration.html)を参照してください。

Splunk展開方法論を包括的に理解し、効果的な計画のための戦略を採用するには、SplunkとCitrix® AnalyticsアプリケーションがSplunkでホストされているアーキテクチャドキュメントを参照してください。

Citrix Analytics for Security™をSplunkと連携させる

Citrix Analytics for SecurityをSplunkと連携させるには、記載されているガイドラインに従ってください。

- (#data-export)。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はこのリスクインテリジェンスをチャネルから取得します。
- Citrix Analyticsで構成を取得します。認証のために、事前定義されたアカウントのパスワードを作成します。Citrix Analytics for Securityは、Splunk用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。

- (#download-and-install-citrix-analytics-add-on-for-splunk)。SplunkbaseまたはSplunk Cloudのいずれかを使用して**Citrix Analytics Add-on for Splunk**をダウンロードし、インストールプロセスを完了します。
- (#configure-citrix-analytics-add-on-for-splunk)。Citrix Analytics for Securityによって提供される構成の詳細を使用してデータ入力を設定し、Splunk用Citrix Analyticsアドオンを構成します。

Citrix Analytics構成ファイルの準備が完了したら、以下を参照してください。

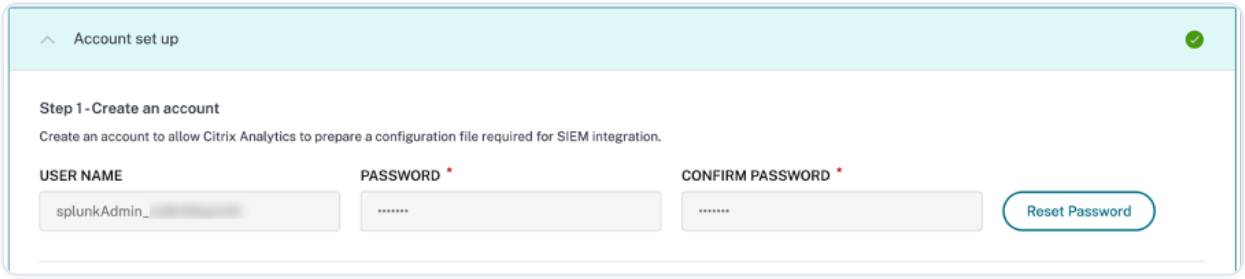
- (#reset-password-capability)
- (#turn-on-or-off-data-transmission)

Splunk用Citrix Analyticsアドオンが構成されたら、以下を参照してください。

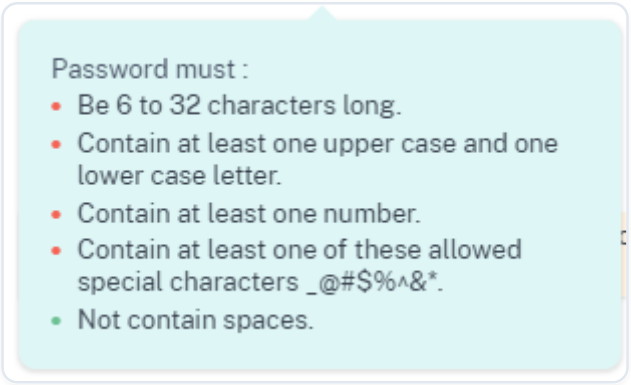
- (#how-to-consume-events-in-your-splunk-environment)
- Splunk 用 Citrix Analytics アプリの構成方法

データのエクスポート

1. 「**設定**」>「**データのエクスポート**」の順に移動します。
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、統合に必要な構成ファイルの準備に使用されます。

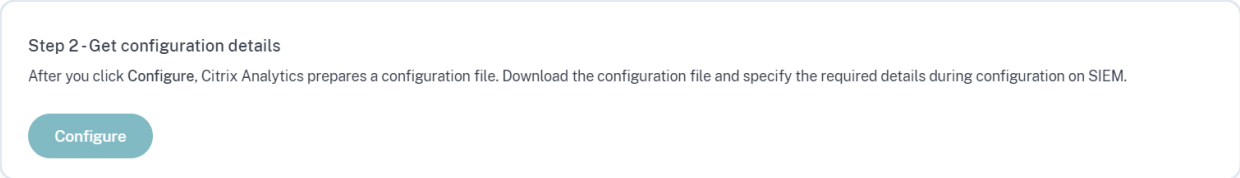


3. パスワードが次の条件を満たしていることを確認してください。



4. 「**構成**」を選択します。

   Citrix Analytics for Security は、Splunk 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、グループ名を含む構成の詳細をコピーします。

   これらの詳細は、以降の手順で Splunk 用 Citrix Analytics アドオンを構成するために必要です。

> **重要**
>
> これらの詳細は機密情報であるため、安全な場所に保管する必要があります。

構成の詳細(/en-us/citrix-analytics/media/splunk-config-details.png)

Splunk連携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ます。これにより、Citrix Analytics for SecurityはSplunk連携プロセスを開始できます。

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、次の手順を実行します。

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。

   SIEMパスワードのリセット(/en-us/citrix-analytics/media/siem-reset-password.png)
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**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ってください。

   SIEMパスワード要件(/en-us/citrix-analytics/media/siem-account-password.png)
3. **リセット**をクリックします。構成ファイルの準備が開始されます。

   SIEMパスワードのリセット(/en-us/citrix-analytics/media/siem-reset-password-confirm.png)

> **注**

> 構成パスワードをリセットした後、Splunk環境の**データの追加**ページでデータ入力を設定する際に、新しいパスワードを更新してください。これにより、Citrix Analytics for SecurityはSplunkへのデータ送信を継続できます。

データ送信のオン/オフ

Citrix AnalyticsからのSplunkデータエクスポートのデータ送信は、デフォルトでオンになっています。

Citrix Analytics for Securityからのデータ送信を停止するには：

1. 「**Settings > Data Exports**」に移動します。
2. **データ送信**を無効にするには、トグルボタンをオフにします。

   SIEM送信をオフにする(/en-us/citrix-analytics/media/siem-turn-off-splunk.png)

データ送信を再度有効にするには、トグルボタンをオンにします。

Splunk用Citrix Analyticsアドオン

アドオンアプリケーションは、以下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。

- スプランク エンタープライズ (ヘビーフォワーダー)
- スプランク クラウド

Splunk用Citrix Analyticsアドオン (オンプレミス/エンタープライズ)

サポートされているバージョン

Citrix Analytics for Securityは、以下のオペレーティングシステムでの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
- レッドハット エンタープライズ リナックス サーバー 7.0以降
- Ubuntu 18.04 LTS以降

> **注**

- Citrix 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 各ベンダーからまだサポートされているバージョンを使用することを推奨します。
- Linux カーネル (64 ビット) オペレーティングシステムの場合、Splunk でサポートされ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 ドキュメントを参照してください。

当社の Splunk 統合は、Splunk 8.1 (64 ビット) 以降の Splunk バージョンで構成できます。

前提条件

- **Citrix Analytics add-on for Splunk** は、Citrix Analytics for Security 上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てください。

エンドポイント	米国リージョン	欧州連合リージョン	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`
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`	`casnb-aps-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`
	`casnb-3.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 アドオンのダウンロードとインストール

アドオンは、**ファイルからアプリをインストール**するか、または Splunk環境内からインストールできます。

ファイルからアプリをインストール

1. Splunkbase にアクセスします。
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 のホームページで、**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見つけて、**アップロード**をクリックします。

> **注**
>
> - アドオンの古いバージョンがある場合は、**アプリをアップグレード**を選択して上書きします。
> - バージョン2.0.0より前のバージョンから**Citrix Analytics Add-on for Splunk**を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の*/bin*フォルダ内にある以下のファイルとフォルダを削除し、Splunk ForwarderまたはSplunk Standalone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のホームページから、**+その他のアプリを検索**をクリックします。
2. その他のアプリを参照ページで、**Citrix Analytics Add-on for 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。

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 Citrix Analytics アドオンを構成する

Citrix Analytics for Security から提供された構成の詳細を使用して、Splunk 用 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**に移動します。

   Splunk の構成(/en-us/citrix-analytics/media/splunk-data-inputs.png)

2. **ローカル入力**セクションで、**Citrix Analytics Add-on**をクリックします。

   Splunk の構成(/en-us/citrix-analytics/media/splunk-local-inputs.png)

3. **新規**をクリックします。

   Splunk の構成(/en-us/citrix-analytics/media/splunk-local-inputs-new.png)

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。

   Splunk の構成(/en-us/citrix-analytics/media/splunk-add-data.png)

5. デフォルト設定をカスタマイズするには、**その他の設定**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。

   Splunk の構成(/en-us/citrix-analytics/media/splunk-add-data-more-settings.png)

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 Citrix Analytics アドオンが正常に構成されます。

Splunk 用 Citrix Analytics アドオン (クラウド)

当社のSplunk統合は、以下のSplunkバージョンで構成できます: Splunk 8.1および それ以降。

前提条件

Splunk用Citrix Analyticsアドオンは、Citrix Analytics for Securityに接続するために、以下のIPアドレスとアウトバウンドポートに接続します。以下のIPアドレスとアウトバウンドポート（Citrix Cloud™リージョン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アドレスとアウトバウンドポートを構成するには、「**Admin Configuration Service (ACS) を使用してCitrix AnalyticsのIPアドレス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**」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	欧州連合リージョン	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
キャスエヌビー-0シトリックス・コム	20.242.21.84	9094	キャスエヌビー-EU-0シトリックス・コム	20.229.150.41	9094	casnb-aps-0citrix.com	20.211.0.214	9094
casnb-1.citrix.com	20.98.232.61	9094	casnb-eu-1.citrix.com	20.107.97.59	9094	casnb-aps-1citrix.com	20.211.38.102	9094
キャスエヌビー-2.シトリックス.コム	20.242.21.108	9094	キャスエヌビー-イーユー-2.シトリックス.コム	51.124.223.162	9094	キャスエヌビー-エーピーエス-2シトリックス.コム	20.211.36.180	9094
キャスエヌビー-3.シトリックス.コム	20.242.57.140	9094						

注記

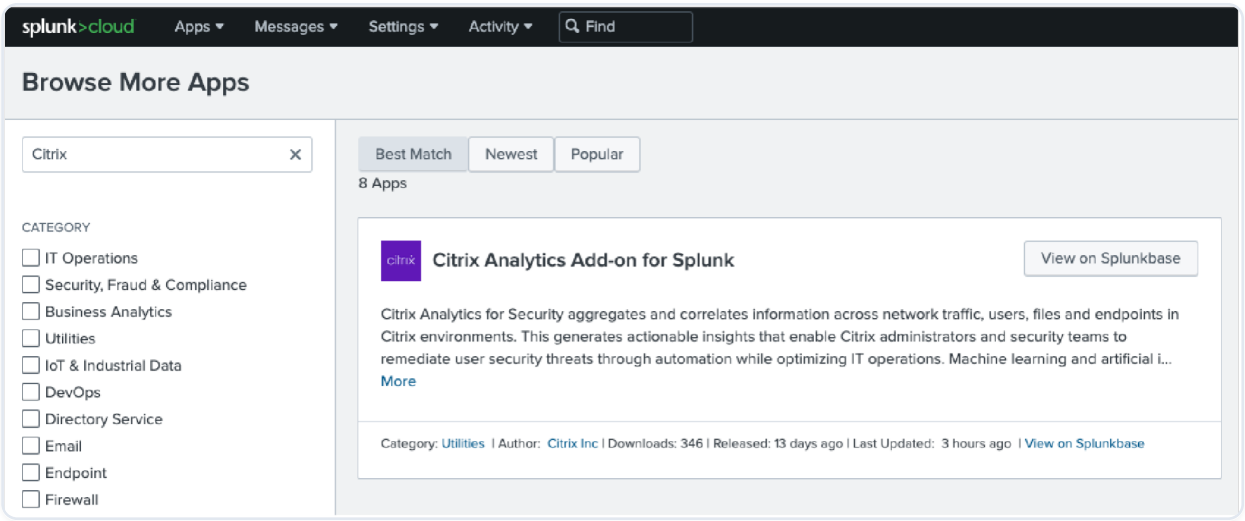
> これらのIPはローテーションの対象となります。 上記に示されている最新のIPでIP許可リストを更新し続けてください。

Admin Configuration Service (ACS) を使用して、Citrix Analyticsの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のリージョンに応じて、許可リストに追加する必要があるIPを特定します。
2. Splunk Cloud PlatformでAdmin Configuration Service (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、許可リスト用のトークンを作成します。
4. cURL GET および POST コマンドを実行する を使用して、それぞれのポートでサブネットを許可リストに追加し、それらが正常に追加されたことを検証します。
5. cURL 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、それらが正常に追加されたことを検証します。

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

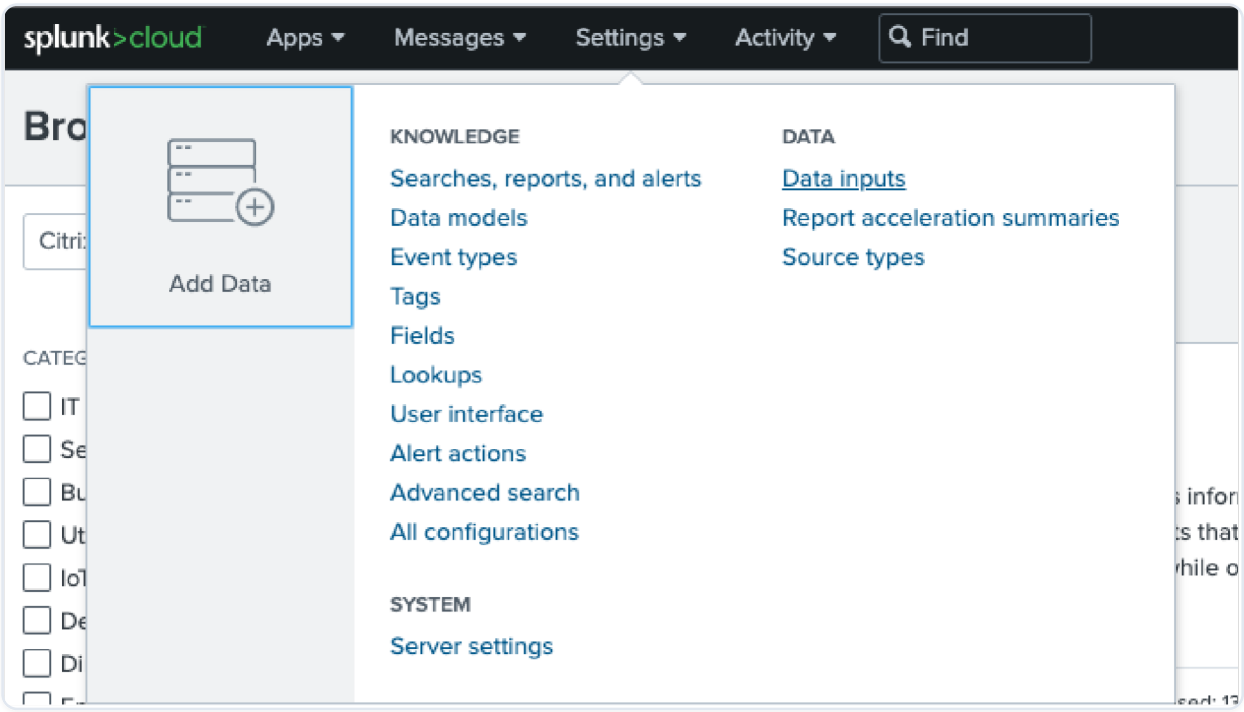
1. **アプリ > その他のアプリを検索 > Citrix Analytics Add-on for Splunk を検索** に移動します。



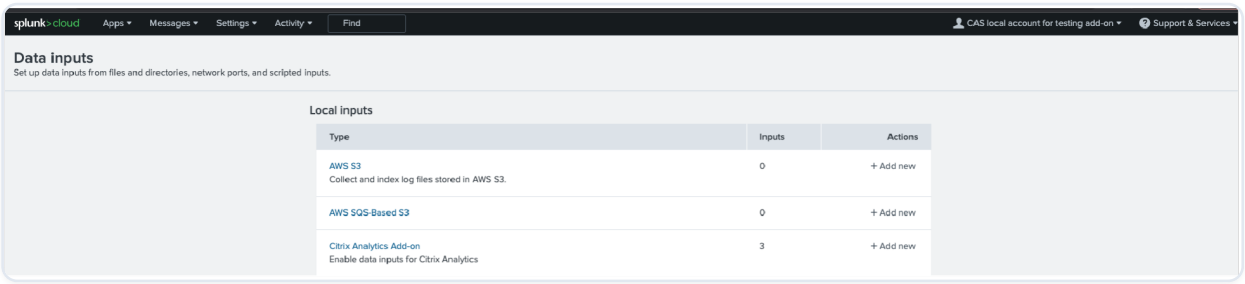
2. アプリをインストールします。
3. アプリがアプリリストに表示されていることを確認します。

Splunk 用 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。



2. 入力を追加します: Splunk integration | Citrix Analytics for Security。**Add New** をクリックします。



3. **Citrix Analytics Data Exports**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。

   Splunkデータ入力の詳細(/en-us/citrix-analytics/media/splunk-data-input-details.png)

4. データ入力が正常に追加されたことを確認します。

   Splunkデータ入力が正常に追加されました(/en-us/citrix-analytics/media/splunk-data-input-added.png)

Splunk環境でイベントを消費する方法

アドオンを構成すると、SplunkはCitrix Analytics for Securityからリスクインテリジェンスの取得を開始します。構成されたデータ入力に基づいて、Splunk検索ヘッドで組織のイベントの検索を開始できます。

検索結果は次の形式で表示されます。

イベント消費形式(/en-us/citrix-analytics/media/consume-events-format.png)

出力例:

イベント消費の出力例(/en-us/citrix-analytics/media/consume-events-sample-output.png)

アドオンに関する問題を検索およびデバッグするには、次の検索クエリを使用します。

イベント検索クエリを消費する(/en-us/citrix-analytics/media/consume-events-search-query.png)

結果は次の形式で表示されます。

イベント検索結果を消費する(/en-us/citrix-analytics/media/consume-events-search-result.png)

データ形式の詳細については、Citrix Analytics data format for SIEM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 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てください。詳細については、「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**
>
> Splunk 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依頼するには、mailto:CAS-PM-Ext@cloud.com にお問い合わせください。

Splunk 用 Citrix Analytics アプリ

> **注**
>
> このアプリはプレビュー版です。

Splunk 用 Citrix Analytics アプリを使用すると、Splunk Enterprise 管理者は、Citrix Analytics for Security から収集されたユーザーデータを、Splunk 上で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危険な行動を詳細に把握し、インサイダー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、Citrix Analytics for Security 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。この関連付けにより、

> 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措置を講じることができます。

サポートされている Splunk のバージョン

Splunk 用 Citrix Analytics アプリは、以下の Splunk バージョンで動作します。

- 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 アプリの前提条件

- Splunk 用 Citrix Analytics アドオンをインストールします。
- Citrix Analytics add-on for Splunk に記載されている 前提条件 が満たされていることを確認します。
- Citrix Analytics for Security から Splunk にデータが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?

Splunk 検索ヘッド

アプリのインストールと構成方法?

Citrix Analytics App for Splunk は、Splunkbase からダウンロードするか、Splunk 内からインストールできます。

ファイルからアプリをインストール

1. Splunkbase にアクセスします。
2. Citrix Analytics App for Splunk ファイルをダウンロードします。
3. Splunk Web のホームページで、**Apps** の横にある歯車アイコンをクリックします。
4. **Install app from file** をクリックします。
5. ダウンロードしたファイルを見つけて、**Upload** をクリックします。

> **注**
>
> アプリの古いバージョンがある場合は、**Upgrade app** を選択して上書きします。

6. 「**Apps**」リストにアプリが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のホームページから、「**+Find More Apps**」をクリックします。
2. 「Browse More Apps」ページで、「**Citrix Analytics App for Splunk**」を検索します。
3. アプリの横にある「**Install**」をクリックします。

データを関連付けるようにインデックスとソースタイプを構成する

1. アプリをインストールしたら、「**Set up now**」をクリックします。

   アプリをセットアップ(/en-us/citrix-analytics/media/set-up-app-splunk.png)
2. 次のクエリを入力します。

   - Citrix Analytics for Securityからのデータが保存されてい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用Citrix Analyticsアドオンで指定されているものと同じである必要があります。詳細については、「Splunk用Citrix Analyticsアドオンを構成する」を参照してください。

   - Citrix Analytics for Securityとデータを関連付けたいインデックス。

     ソースとインデックス(/en-us/citrix-analytics/media/splunk-app-index.png)
3. 構成を完了するには、「**Finish App Setup**」をクリックします。

Citrix Analytics App for Splunk を構成およびセットアップした後、Citrix Analytics dashboards を使用して Splunk でユーザーイベントを表示します。

Splunk 連携の詳細については、以下のリンクを参照してください。

- Citrix Analytics と Splunk の連携
- Splunkbase で利用可能になった Splunk 用 Citrix Analytics アプリ

Citrix Analytics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

Splunkは、以下の3つの層を含む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

Splunkは、データをSplunkに簡単に取り込み、インデックス化して検索可能にするための幅広いデータ収集メカニズムをサポートしています。この層は、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層ではなく、ヘビーフォワーダー層にインストールする必要があります。なぜなら、構造化されたデータ（json、csv、tsvなど）のいくつかの例外を除いて、ユニバーサルフォワーダーはログソースをイベントに解析しないため、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からです。

また、Pythonの簡易版が付属しているため、完全なSplunkスタック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が完全な解析パイプラインを含み、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を作成したりすることなく、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、個々のイベントを理解し、それに基づいて動作することができます。アドオンアプリケーションは完全なSplunk Enterpriseインストールであるため、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したり、Splunk HTTP Event Collector (HEC) のエンドポイントとして機能したりできます。

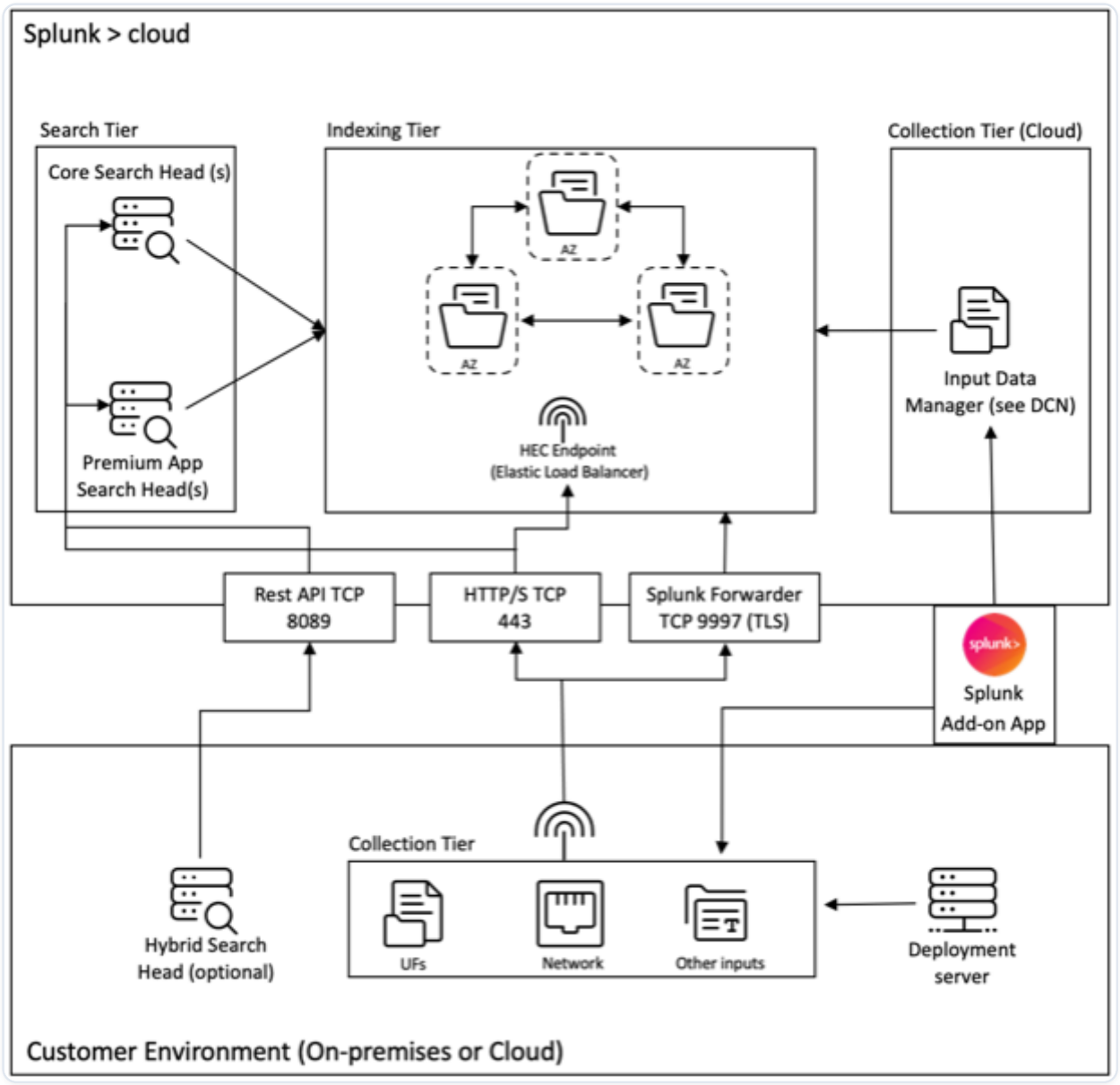
データが収集されると、インデックス化または処理され、検索可能になるように保存されます。

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の作成に利用できます。検索はデータから情報を抽出するものです。

一般的に、Splunkアドオンアプリケーションはコレクション層（Splunk Enterpriseレベル）にデプロイされ、当社のダッシュボードアプリケーションは検索層（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つの層すべてを単一の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して知られています）。

コレクション層は、Splunk用アドオンアプリケーションを使用するのに非常に優れた方法です。アドオンアプリケーションをインストールする方法は2つあります。顧客環境下のコレクション層にインストールするか、**Splunk Cloudインスタンス**下の入力データマネージャーにインストールするかのいずれかです。

当社のアドオンアプリケーションを使用したSplunkデプロイメントアーキテクチャを理解するには、以下の図を参照してください。



前述の図に示されているインプットデータマネージャー (IDM) は、スクリプト化された入力とモジュラー入力のみをサポートするデータ収集ノード (DCN) のSplunk Cloud管理による実装です。それ以上のデータ収集のニーズには、Splunkのヘビーフォワーダーを使用して環境にDCNをデプロイして管理できます。

Splunkは、さまざまなソースからデータを収集、インデックス作成、検索することを可能にします。データを収集する1つの方法はAPIを介することであり、これによりSplunkは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ます。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、および/またはJDBCを含めることができます。Splunkおよびサードパーティの開発者は、Splunkモジュラー入力フレームワークを介した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

は通常、適切に機能するために完全なSplunk Enterpriseソフトウェアのインストールを必要とします。

APIを介したデータ収集を容易にするために、DCNとしてヘビーフォワーダーを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含み、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を介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作成する前に処理することができます。

Splunk Cloudデプロイメントのハイレベルアーキテクチャの詳細については、Splunk Validated Architecturesを参照してください。

Splunk 用 Citrix Analytics ダッシュボード

> **注**
>
> **注意**: Citrix Content Collaboration™ および ShareFile は、サポート終了 (EOL) に達し、ユーザーは利用できなくなりました。

> この機能はプレビュー版です。

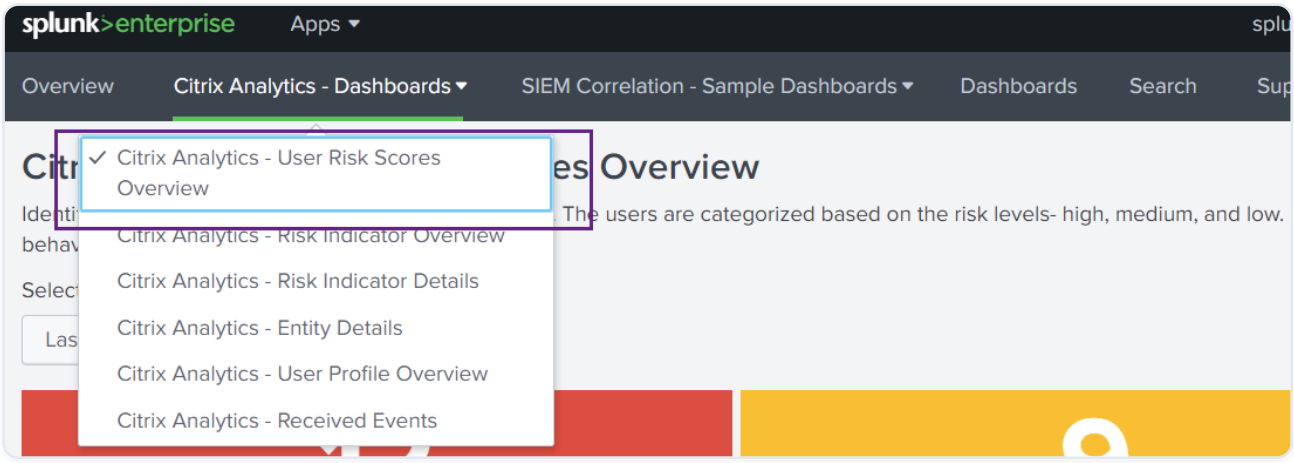
前提条件

以下の Citrix Analytics ダッシュボードを使用するには、Citrix Analytics App for Splunk をすでに構成およびセットアップしていることを確認してください。

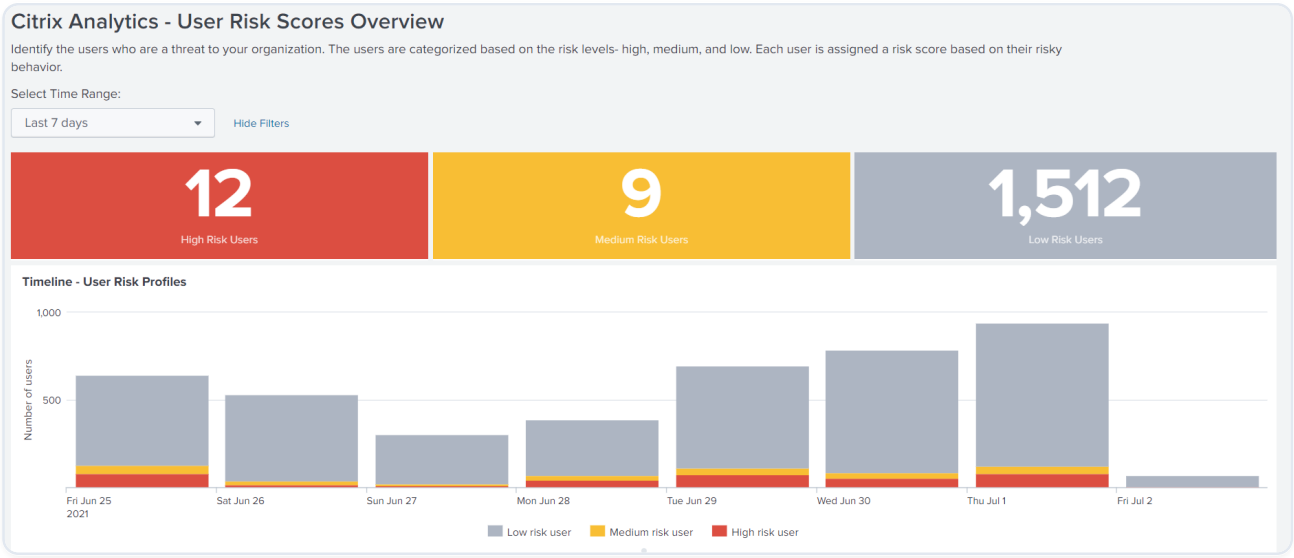
ユーザーリスクスコアの概要

このダッシュボードは、組織内の危険なユーザーの統合ビューを提供します。ユーザーは、高、中、低のリスクレベルで分類されます。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、それに応じてリスクスコアが割り当てられます。危険なユーザーの種類に関する詳細については、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- Dashboards > Citrix Analytics- User Risk Scores Overview** をクリックします。



危険なユーザーのタイムラインとその詳細を表示するには、プリセットの時間範囲またはカスタムの時間範囲を選択します。



危険なユーザーの表には、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 - Entity Details ダッシュボードでユーザーの危険な行動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検出されました**: 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インジケーターの数を示します。
- **侵害されたユーザーのリスクが検出されました**: 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インジケーターの数を示します。
- **データ漏洩のリスクが検出されました**: データ漏洩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インジケーターの数を示します。
- **内部脅威のリスクが検出されました**: 内部脅威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インジケーターの数を示します。
- **リスクスコア**: ユーザーのリスクスコアを示します。

ユーザー名でユーザーを検索し、必要な詳細情報を取得することもできます。

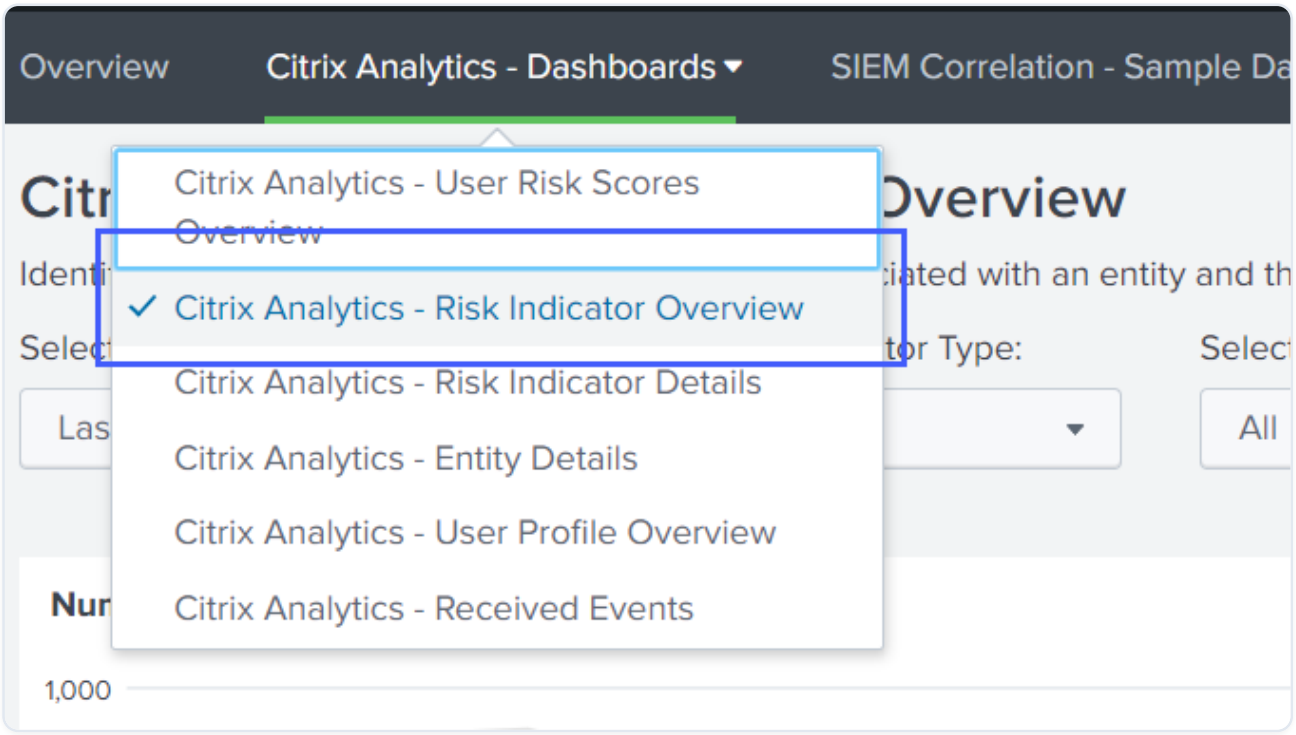
詳細については、リスクカテゴリを参照してください。



リスクインジケーターの概要

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インジケーター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 - リスクインジケーターの概要**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、リスクインジケーターを検索します。

- **期間**: 事前設定された期間またはカスタム期間を選択して、その期間にトリガーされたリスクインジケーターを表示します。

- **リスクインジケーターの種類**: リスクインジケーターの種類（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**：関連するリスクインジケーターを表示するユーザーを選択します。
- **グループ**：データソース、インジケーターカテゴリ、インジケーター名、インジケータータイプ、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する基準を選択し、関連するリスクインジケーターを表示します。

  リスクインジケーターの概要カテゴリ(/en-us/citrix-analytics/media/risk-indicator-overview-category-splunk.png)

レポートの表示

1つ以上のカテゴリを選択して、リスクインジケーターの詳細を表示するには、次のレポートを使用します。

- **トリガーされたリスクインジケーターの数**：選択した期間にトリガーされたリスクインジケーターの数を表示します。このレポートを使用して、危険なアクティビティのパターンと領域を特定します。また、組織内の上位の危険なアクティビティを特定します。
- **リスクインジケーターイベントの合計および個別エンティティ数**：リスクインジケーターに対応する合計イベント数とユニークイベント数を表示します。このレポートを使用して、各リスクインジケーターの発生状況と組織内の上位のリスクインジケーターを特定します。また、特定のリスクインジケーターをトリガーしたユニークユーザーの数を確認し、そのリスクインジケーターがより大規模なユーザーグループまたはより小規模なユーザーグループによってトリガーされたかどうかを確認することもできます。
- **場所別のリスクインジケーター**：場所をまたいでユーザーによってトリガーされたリスクインジケーターの数を表示します。このレポートを使用して、より危険なアクティビティを示す場所を特定し、その場所が組織の運用範囲外であるかどうかを確認します。
- **リスクインジケーターの詳細**：関連するデータソース、インジケーターカテゴリ、インジケータータイプ、発生回数など、リスクインジケーターに関する詳細を表示します。

リスクインジケーターの概要レポート1(/en-us/citrix-analytics/media/risk-indicator-overview-report-1.png)

リスクインジケーターの概要レポート2(/en-us/citrix-analytics/media/risk-indicator-overview-report-2.png)

リスクインジケーターの詳細

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のリスクインジケーターに関する詳細情報が表示されます。詳細については、「Citrixユーザーリスクインジケーター」および「カスタムリスクインジケーター」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- Dashboards > Citrix Analytics- Risk Indicator Details** をクリックします。

リスクインジケーターの詳細選択(/en-us/citrix-analytics/media/risk-indicator-details-selection-splunk.png)

レポートを表示するカテゴリを選択します

1つ以上のカテゴリを選択して、リスクインジケーター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、その期間にトリガーされたリスクインジケーターの詳細を表示します。
- **エンティティタイプ**: ユーザーを選択して、関連するリスクインジケーターの詳細を表示します。
- **リスクインジケータータイプ** - 組み込みまたはカスタムのリスクインジケーターのタイプを選択して、その詳細を表示します。
- **データソース** - データソースを選択して、関連するリスクインジケーターの詳細を表示します。
- **リスクインジケーターカテゴリ** - リスクカテゴリを選択して、関連するリスクインジケーターの詳細を表示します。
- **リスクインジケーター** - リスクインジケーターを選択して、その詳細を表示します。

レポートを表示する

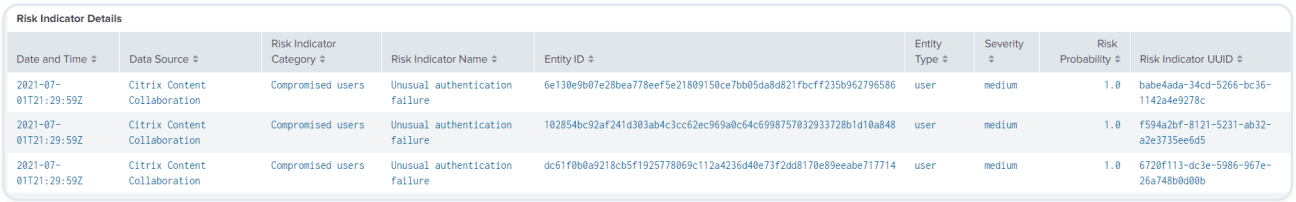
たとえば、「リスクインジケーターの選択」リストから「**異常な認証失敗 (Citrix Content Collaboration)**」を選択し、「**送信**」をクリックして、次の情報を表示します。

- リスクインジケーターに関連付けられた上位10ユーザー
- リスクインジケーターに関する詳細（例：）
    - トリガーの日時
    - 関連するデータソース
    - 関連するリスクカテゴリ
    - 関連付けられたエンティティIDとユーザーエンティティタイプ

- リスクの重大度 - 高、中、または低
- ユーザーイベントのリスク確率
- リスクインジケーターの一意のID (UUID)



「**リスクインジケーター別上位10エンティティ**」でエンティティをクリックすると、「**Citrix Analytics - エンティティ詳細**」ダッシュボードでその詳細が表示されます。



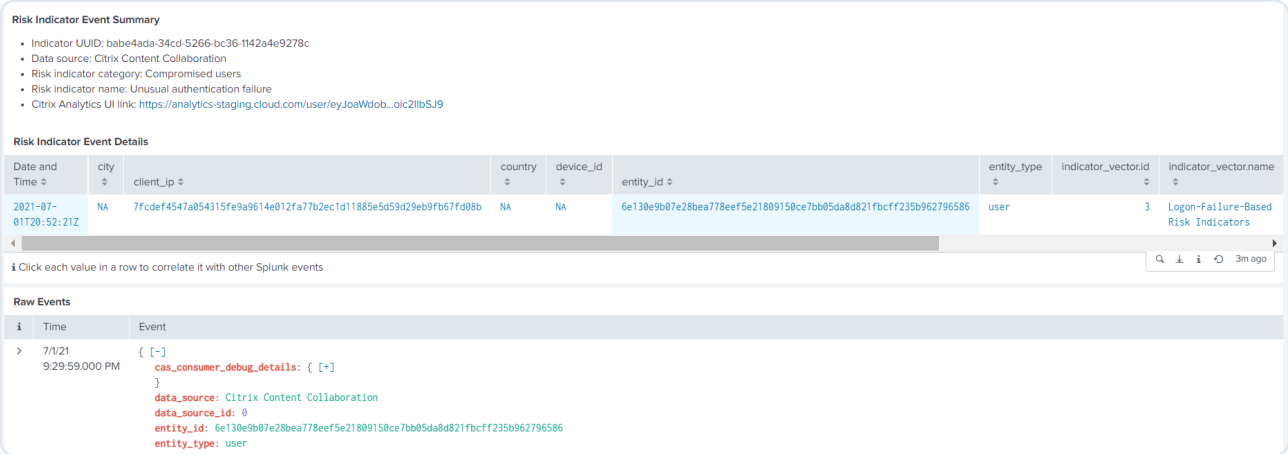
Risk Indicator Details

Date and Time	Data Source	Risk Indicator Category	Risk Indicator Name	Entity ID	Entity Type	Severity	Risk Probability	Risk Indicator UUID
2021-07-01T21:29:59Z	Citrix Content Collaboration	Compromised users	Unusual authentication failure	6e130e9b07e28bea778eef5e21809150ce7bb05da8d821fbcff235b962796586	user	medium	1.0	babe4ada-34cd-5266-bc36-1142a4e9278c
2021-07-01T21:29:59Z	Citrix Content Collaboration	Compromised users	Unusual authentication failure	102854bc92af241d303ab4c3cc62ec969a0c64c6998757032933728b1d10a848	user	medium	1.0	f594a2bf-8121-5231-ab32-a2e3735ee6d5
2021-07-01T21:29:59Z	Citrix Content Collaboration	Compromised users	Unusual authentication failure	dc61f0b0a9218cb5f1925778069c112a4236d40e73f2dd8170e89eeabe717714	user	medium	1.0	6720f113-dc3e-5986-967e-26a748b0d00b

「**リスクインジケーターの詳細**」テーブルの各行をクリックすると、選択したリスクインジケーターのイベント概要、イベント詳細、および生イベントが表示されます。

「**リスクインジケーターイベント概要**」セクションで、「**Citrix Analytics UIリンク**」をクリックすると、SplunkからCitrix Analytics for Security™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、リスクインジケーター、関連イベント、およびユーザーに適用されたアクションを表示します。

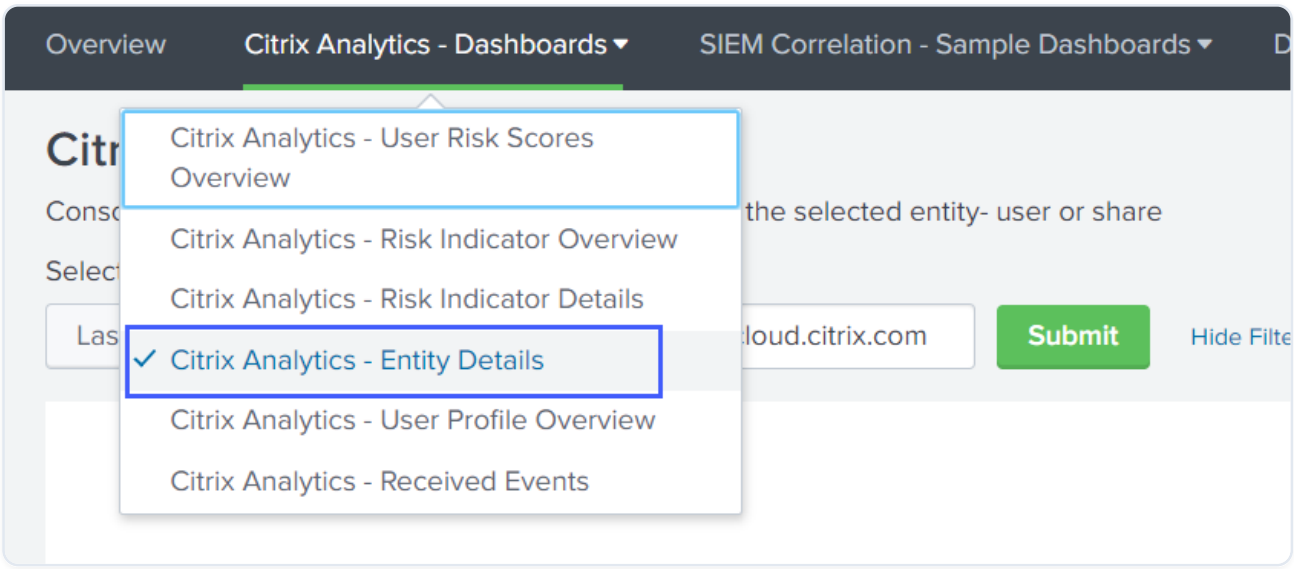
イベント概要とイベント詳細の詳細については、「SIEM用Citrix Analyticsデータ形式」を参照してください。



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 - エンティティ詳細**」をクリックします。



レポートを表示

期間とエンティティ（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、以下のダッシュボードからエンティティの詳細情報を表示することもできます。

- **Citrix Analytics- Risk Indicator Details** で、**Top 10 Entities by Risk Indicators** に移動し、エンティティをクリックします。

  エンティティビュー(/en-us/citrix-analytics/media/entity-splunk.png)

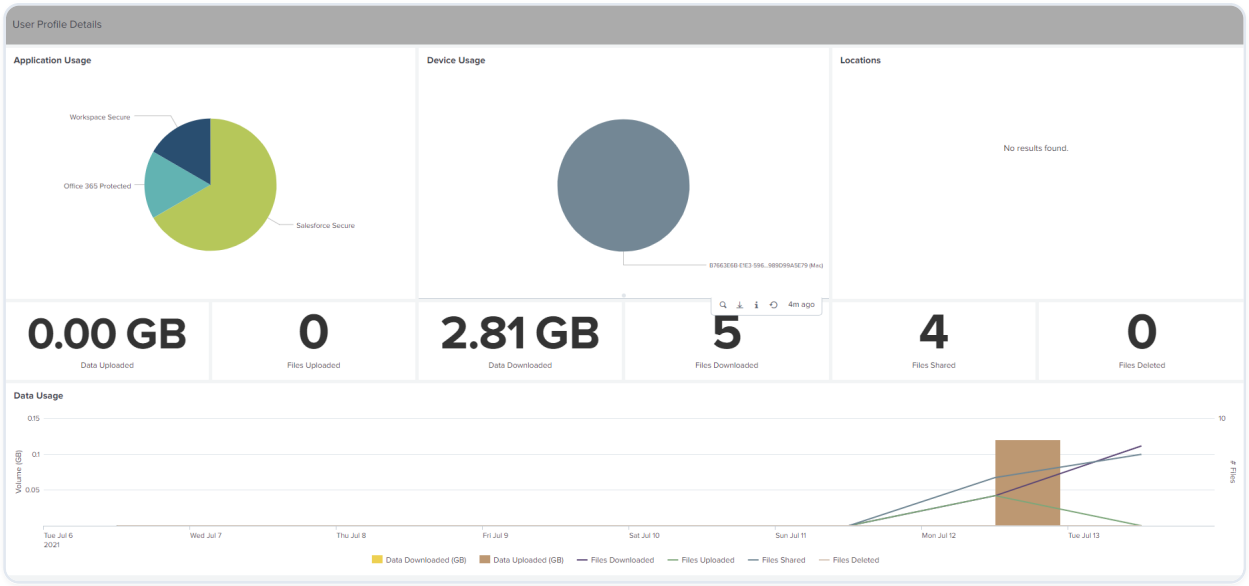
- **Citrix Analytics- Risk Score Overview** で、**Risky Users** に移動し、ユーザー名をクリックします。

  ユーザー名選択(/en-us/citrix-analytics/media/risky-user-splunk.png)

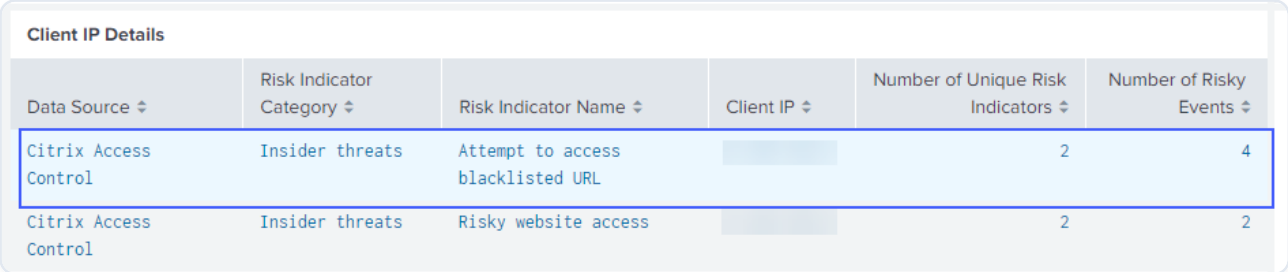
以下の詳細情報が表示されます。

- 選択した期間の現在のリスクスコアとリスクスコアのタイムライン。
- リスクインジケーターの割合分布。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。
- リスクインジケーターの地理的分布。異常な場所や高リスクの場所を特定するのに役立ちます。
- 危険な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す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インジケーターの詳細。

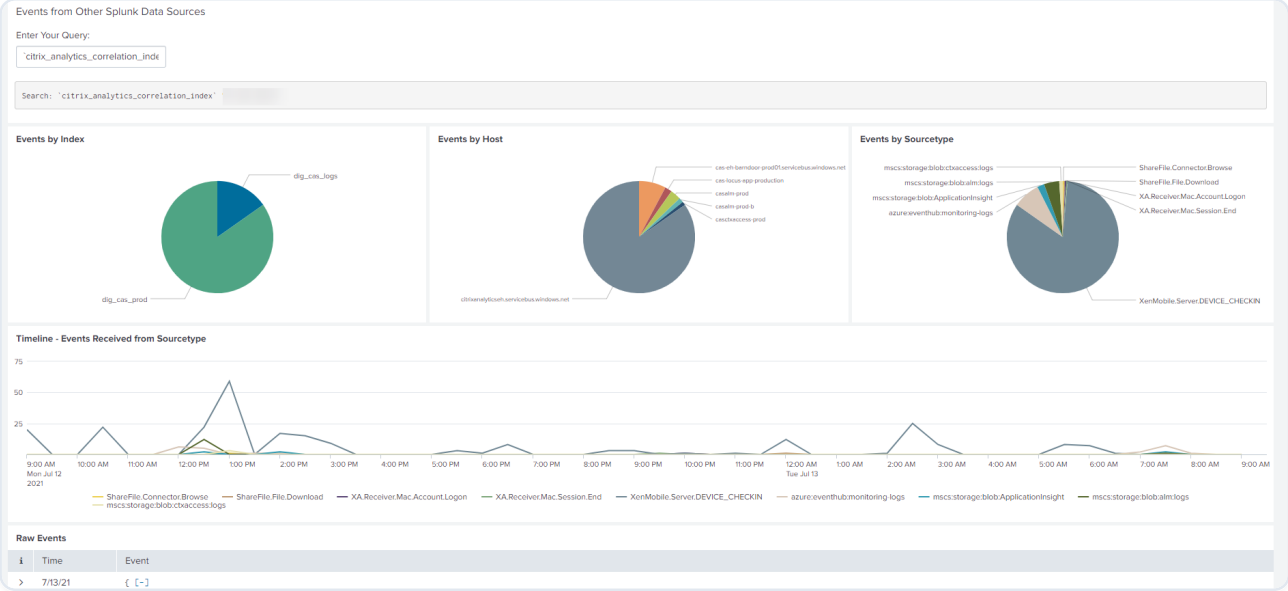
  エンティティ詳細ビュー 1(/en-us/citrix-analytics/media/entity-details-splunk-1.png)



危険なアクティビティに関連付けられたクライアント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。



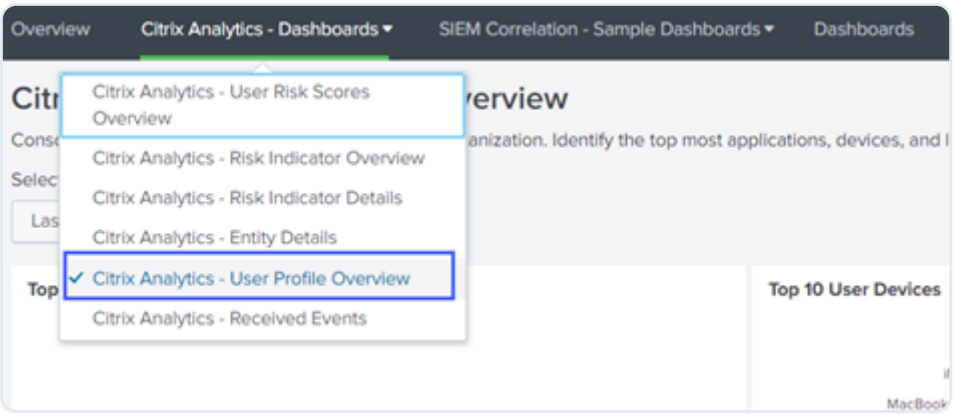
Citrix Analyticsイベント相関ダッシュボードでは、選択したクライアントIPに関連付けられたイベントを、他のセキュリティデータソース（インデックスとソースタイプに基づく）から相関させて表示できます。これらのイベントは、クライアントIPに関連する悪意のあるアクティビティに関するより深い洞察を提供します。



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た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- Dashboards > Citrix Analytics- User Profile Overview**をクリックします。



イベントの表示

時間範囲を選択し、次のメトリックを表示します。

- ユーザーが使用した上位10のアプリケーション
- ユーザーが使用した上位10のデバイス
- ユーザーが使用した上位10の場所
- 使用されたWebおよびSaaSアプリケーションの数
- 使用されたデバイスの数
- 複数の場所からアクセスしたユーザーの数
- アップロード、ダウンロード、共有されたファイルなどのデータ使用状況メトリック

これらのメトリックは、組織内のユーザーアクティビティに関する洞察を提供します。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。

ユーザープロファイルの概要(/en-us/citrix-analytics/media/user-profile-report-splunk.png)

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。イベントはユーザー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- Dashboards > Citrix Analytics- Received Events** をクリックします。

受信イベントの選択(/en-us/citrix-analytics/media/received-events-selection-splunk.png)

レポートの表示

受信したさまざまな種類のイベントを表示および比較するために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合計: Citrix Analytics for Security から受信したすべてのイベントの集計であり、以下が含まれます。
    - リスクインジケーターイベントの合計: ユーザーによってトリガーされたリスクインジケーターに関連するイベントを示します。
    - リスクインジケーター詳細イベントの合計: トリガーされたリスクインジケーターの詳細に関連するイベントを示します。

- リスクスコア変更イベントの合計: 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合計リスクスコアイベント: ユーザーのリスクスコア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合計アプリケーションイベント: ユーザーが使用するアプリケーション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合計デバイスイベント: ユーザーが使用するデバイス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合計データ使用量イベント: 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の合計ロケーションイベント: ユーザーがアクセスしたロケーションに関連するイベントを示します。

  受信イベントダッシュボード(/en-us/citrix-analytics/media/received-events-report-splunk.png)

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と、Splunk 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を関連付けます。複数のデータソースから収集されたユーザーの危険なアクティビティに関するより深い洞察を得て、イベント間の関係を見つけ、脅威を特定できます。

ダッシュボードを表示するには、**SIEM Correlation- Sample Dashboards > Citrix Analytics Event Correlation** をクリックします。

イベント相関の選択(/en-us/citrix-analytics/media/event-correlation-selection-splunk.png)

前提条件

相関を実行するには、以下を確認してください。

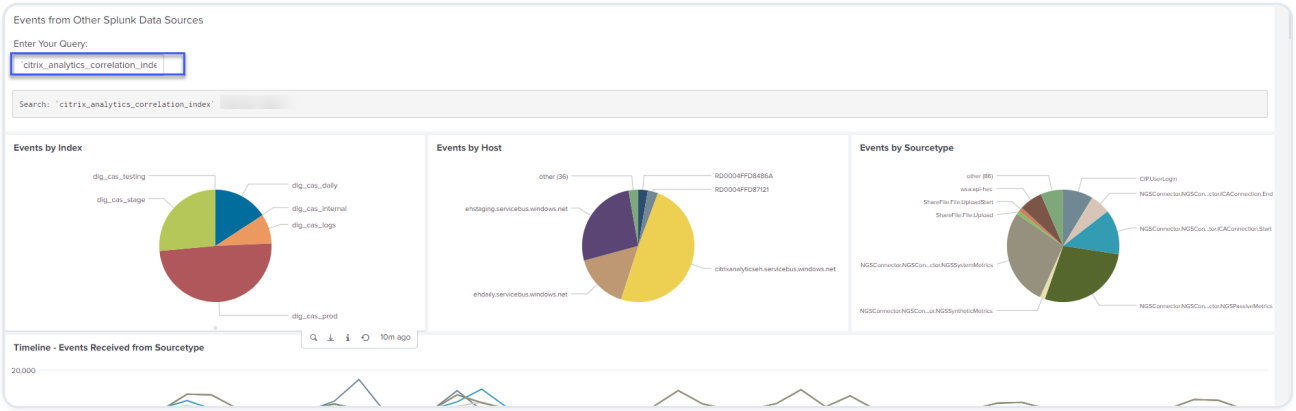
- 相関させるには、他のセキュリティデータソースからのイベントが必要です。たとえば、Splunk で構成された他のデータソースから受信した、ユーザー、デバイス、クライアント IP アドレスに関連するイベントなどです。
- 構成時に相関インデックスがすでに定義されている必要があります。

イベントを関連付ける

Citrix Analytics for Securityによって検出された、最もリスクの高いエンティティと最もリスクの高い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）と関連付けるには、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。要件に基づいて、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。

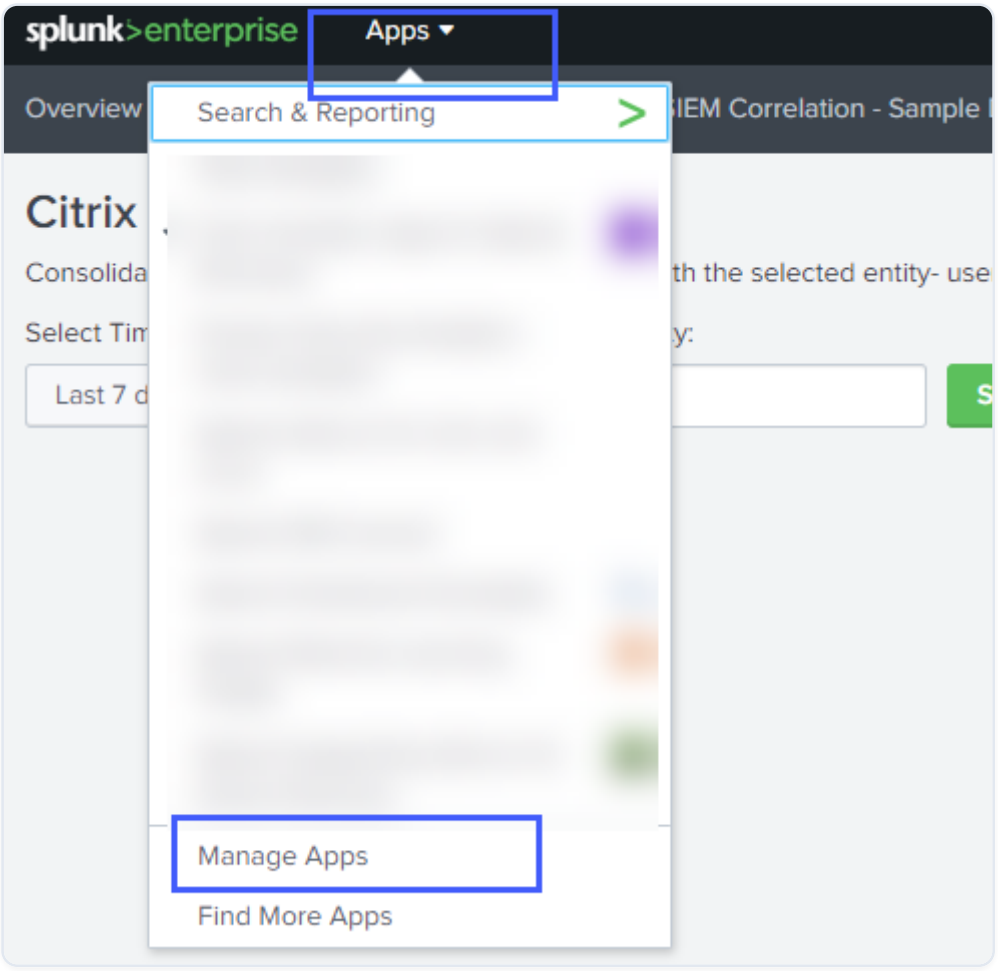


イベントがない場合のトラブルシューティング

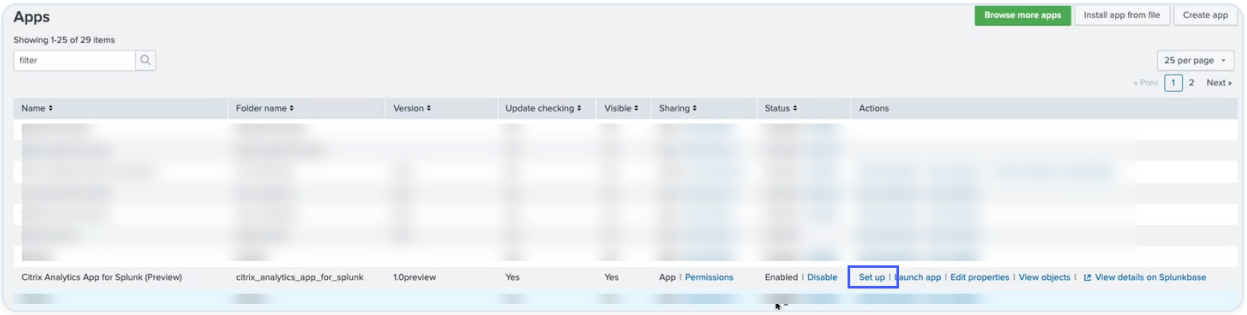
すべてのダッシュボードでイベントが見つからない場合は、Citrix Analytics App for SplunkおよびCitrix Analytics add-on for Splunkの設定に問題がある可能性があります。このような場合は、インデックス値とソースタイプ値を確認してください。インデックスとソースタイプの値が、アプリとアドオンの両方で同じであることを確認してください。

Citrix Analytics App for Splunkの設定を表示するには：

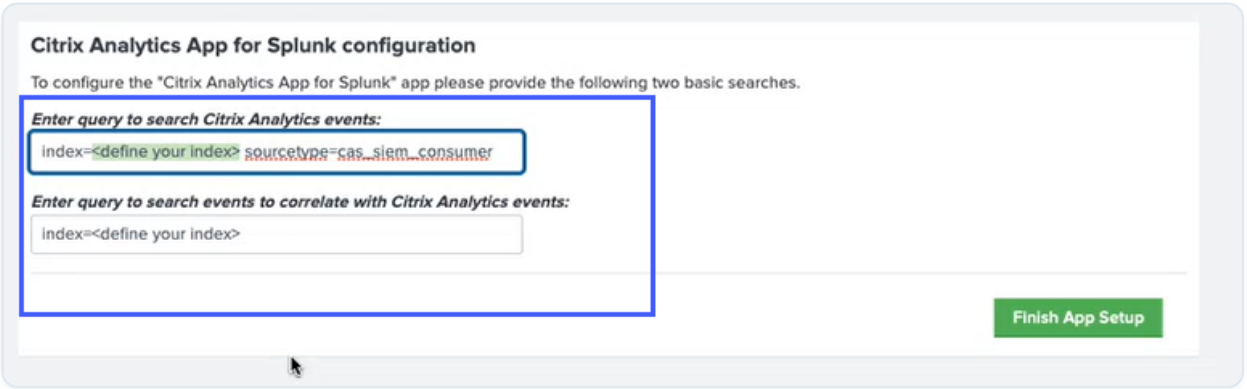
1. **>** をクリックします。



2. リストからCitrix Analytics App for Splunkを見つけます。 をクリックします。

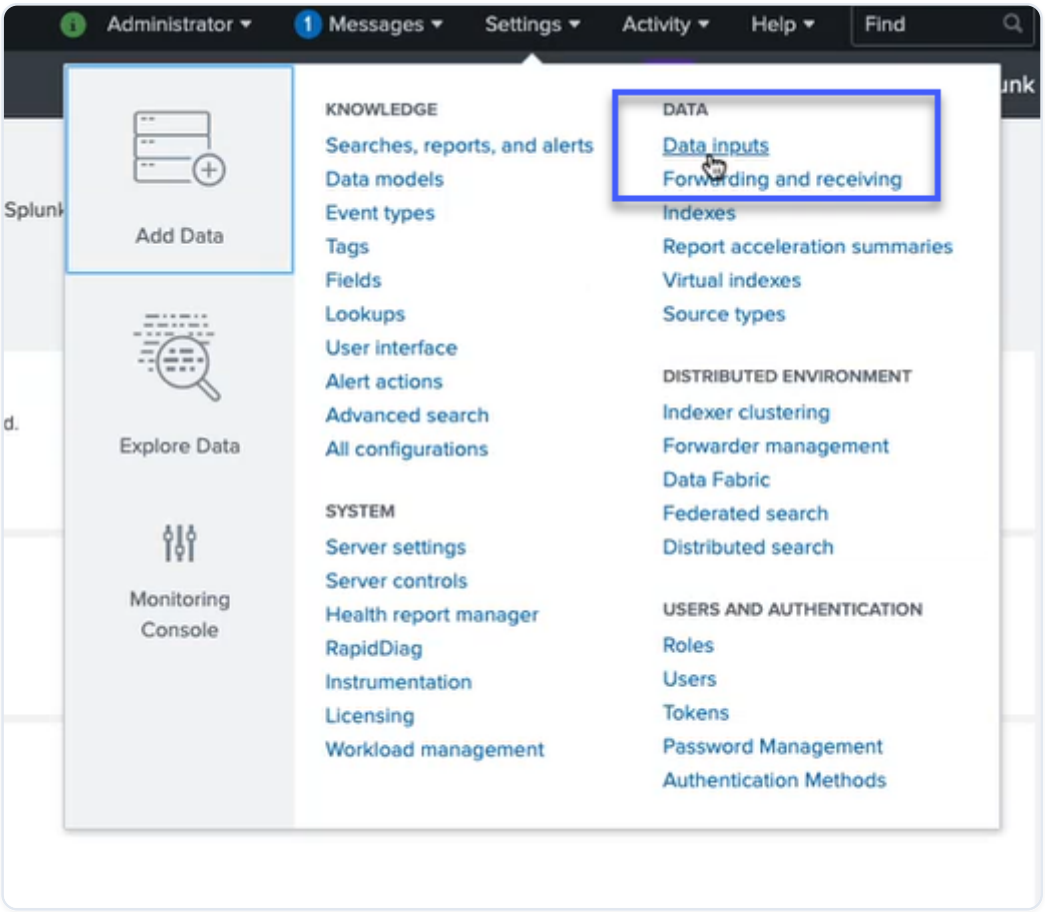


3. ソースタイプとインデックスを確認します。

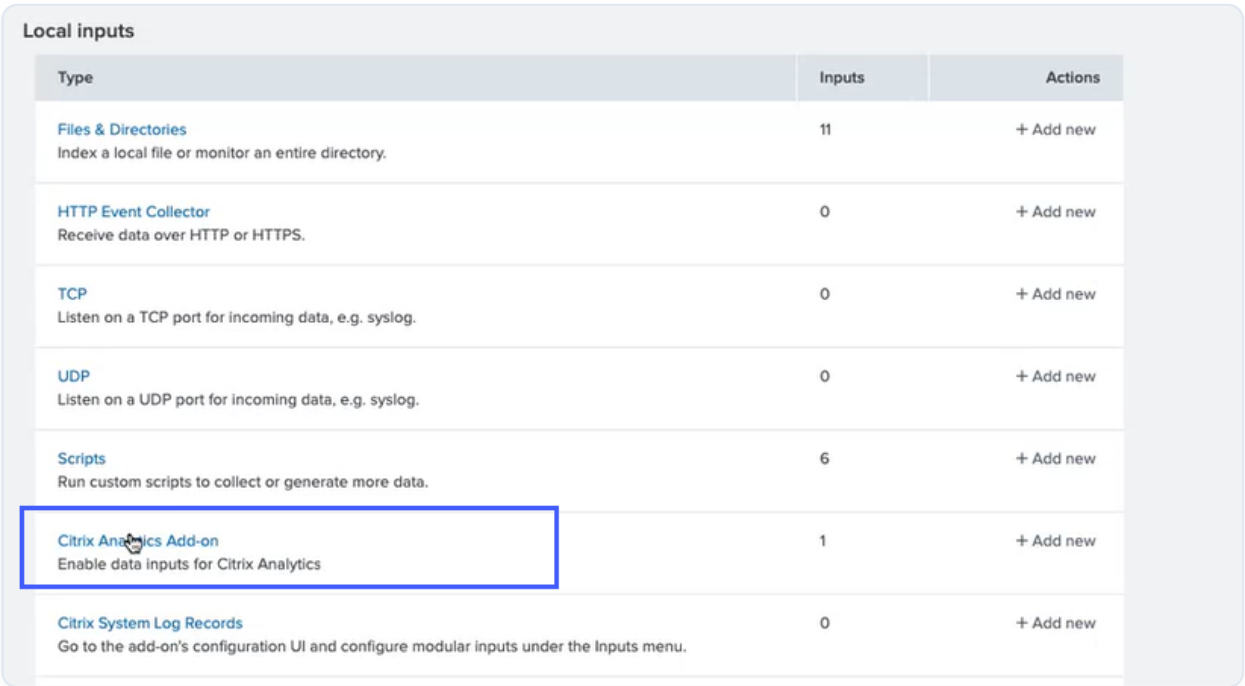


Citrix Analytics add-on for Splunkの設定を表示するには：

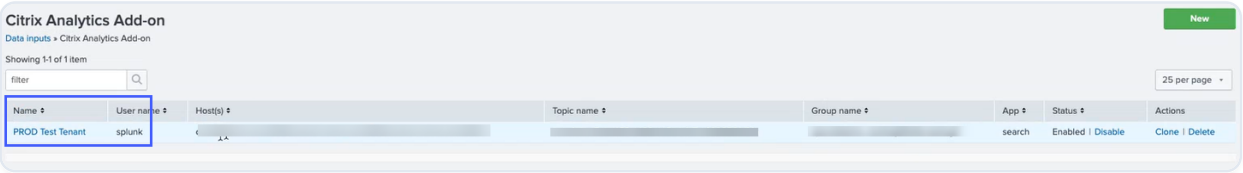
1. **>** をクリックします。



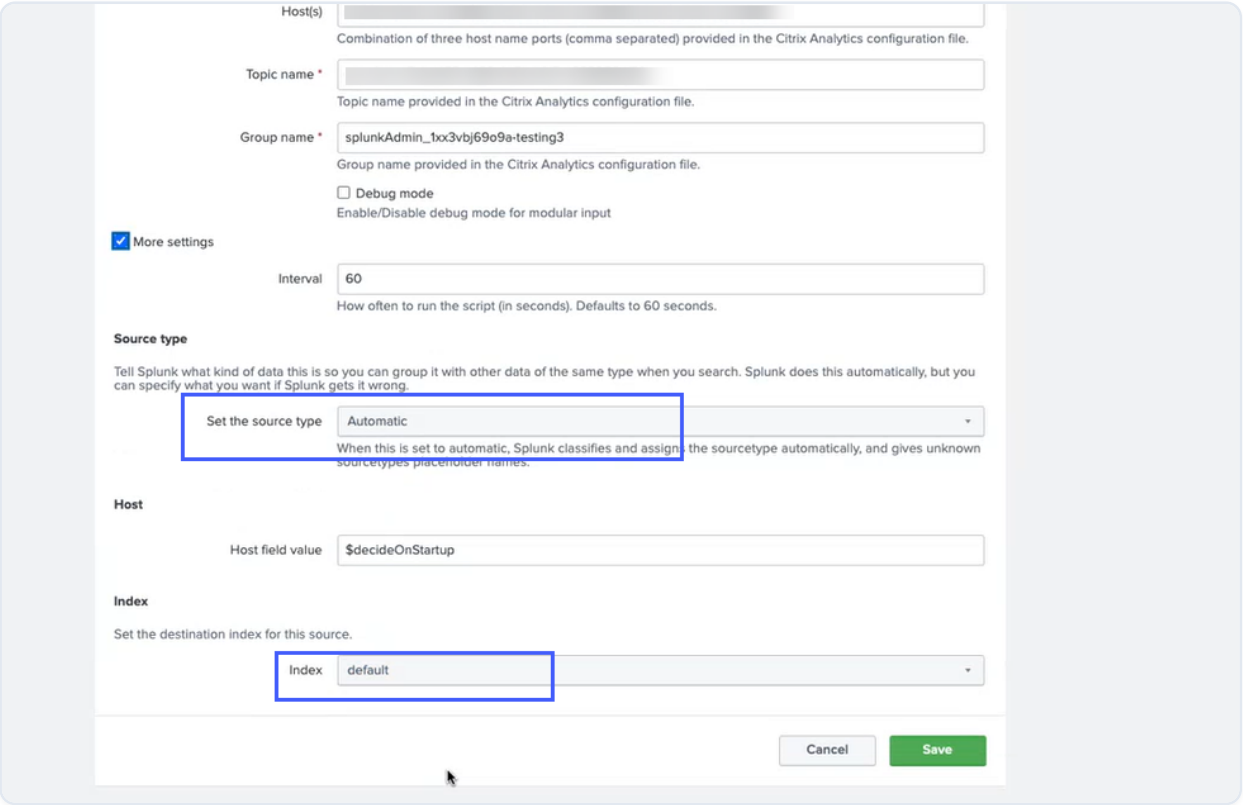
2. **Citrix Analytics Add-on** をクリックします。



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。



構成の詳細については、「Splunk 用 Citrix Analytics アドオンの構成」を参照してください。

Splunk 用 Citrix Analytics アドオンの構成に関する問題

Microsoft Sentinel との統合

> **注**
>
> - Microsoft Sentinel との統合、Microsoft Sentinel 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依頼するには、mailto:CAS-PM-Ext@cloud.com にお問い合わせください。
> - Logstash エンジンを使用した Microsoft Sentinel へのデータのエクスポートはプレビュー段階です。この機能はサービスレベル契約なしで提供されており、本番ワーク

> ロードでの使用は推奨されません。詳細については、Microsoft Sentinel 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。Splunk 環境で Citrix Analytics for Security 独自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について詳しくは、「セキュリティ情報およびイベント管理の統合」を参照してください。

前提条件

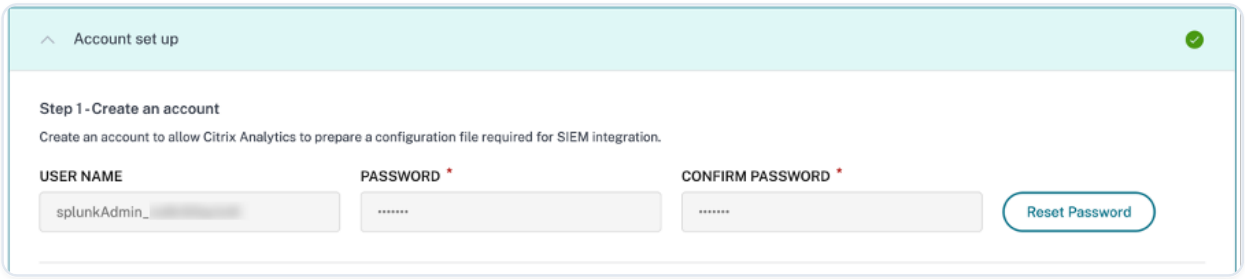
- 少なくとも 1 つのデータソースでデータ処理をオンにします。これにより、Citrix Analytics for Security が Microsoft Sentinel 統合プロセスを開始するのに役立ちます。
- 次のエンドポイントがネットワークの許可リストに含まれていることを確認してください。

エンドポイント	米国リージョン	欧州連合リージョン	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`
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`	`casnb-aps-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`		

- LogstashのMicrosoft Sentinel出力プラグインを使用する場合、Logstashのバージョン7.17.7以降（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）を使用していることを確認してください。

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、統合に必要な構成ファイルを準備するために使用されます。



3. パスワードが以下の条件を満たしていることを確認してください。

   SIEMパスワード要件(/en-us/citrix-analytics/media/siem-account-password.png)

4. Logstash構成ファイルを生成するには、**構成**をクリックします。

   構成(/en-us/citrix-analytics/media/siem-configure.png)

5. 構成ファイルをダウンロードするには、Azure Sentinel (プレビュー) タブを選択します。

   - **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、出力セクション）が含まれています。

     Logstash構成ファイルの構造については、Logstash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ています。

   > **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。

   > Microsoft Sentinelの選択(/en-us/citrix-analytics/media/azure-sentinel-select.png)

6. Azure Sentinel統合を準備します。

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か、既存のワークスペースを使用してMicrosoft Sentinelを実行できます。
b. メインメニューから、**データコネクタ**を選択してデータコネクタギャラリーを開きます。
c. **Citrix Analytics (Security)** を検索します。
d. 「**Citrix Analytics (Security)**」を選択し、「**コネクタページを開く**」を選択します。

   Sentinelデータコネクタページ(/en-us/citrix-analytics/media/azure-sentinel-connector-page.png)
e. 「**Citrix Analytics (Security)**」ページから、「**ワークスペースID**」と「**プライマリキー**」をコピーします。この情報は、後続の手順でLogstash設定ファイルに入力する必要があります。

   データコネクタ設定ページ(/en-us/citrix-analytics/media/azure-sentinel-config-page.png)
f. ホストマシンでLogstashを構成します。

   i. LinuxまたはWindowsホストマシンに、LogstashとLogstash用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、以下のファイルを指定されたディレクトリに配置します。

ホストマシンの種類	ファイル名	ディレクトリパス
Linux (リナックス)	CAS_AzureSentinel_LogStash_Config.config	Debianおよび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および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`

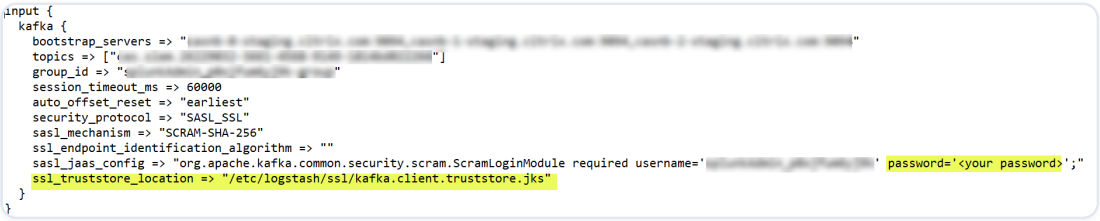
ホストマシンの種類	ファイル名	ディレクトリパス
Windows (ウィンドウズ)	CAS_AzureSentinel_LogStash_Config.config	`C:\logstash-7.xx.x\config`
	kafka.client.truststore.jks	

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。

i. ファイルの入力セクションに、次を入力します。

- **パスワード**: 設定ファイルを準備するためにCitrix Analytics for Securityで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、ホストマシン上のkafka.client.truststore.jksファイルの場所です。



ii. 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. 処理されたデータをCitrix Analytics for SecurityからMicrosoft Sentinelに送信するには、Logstashホストマシンを再起動します。

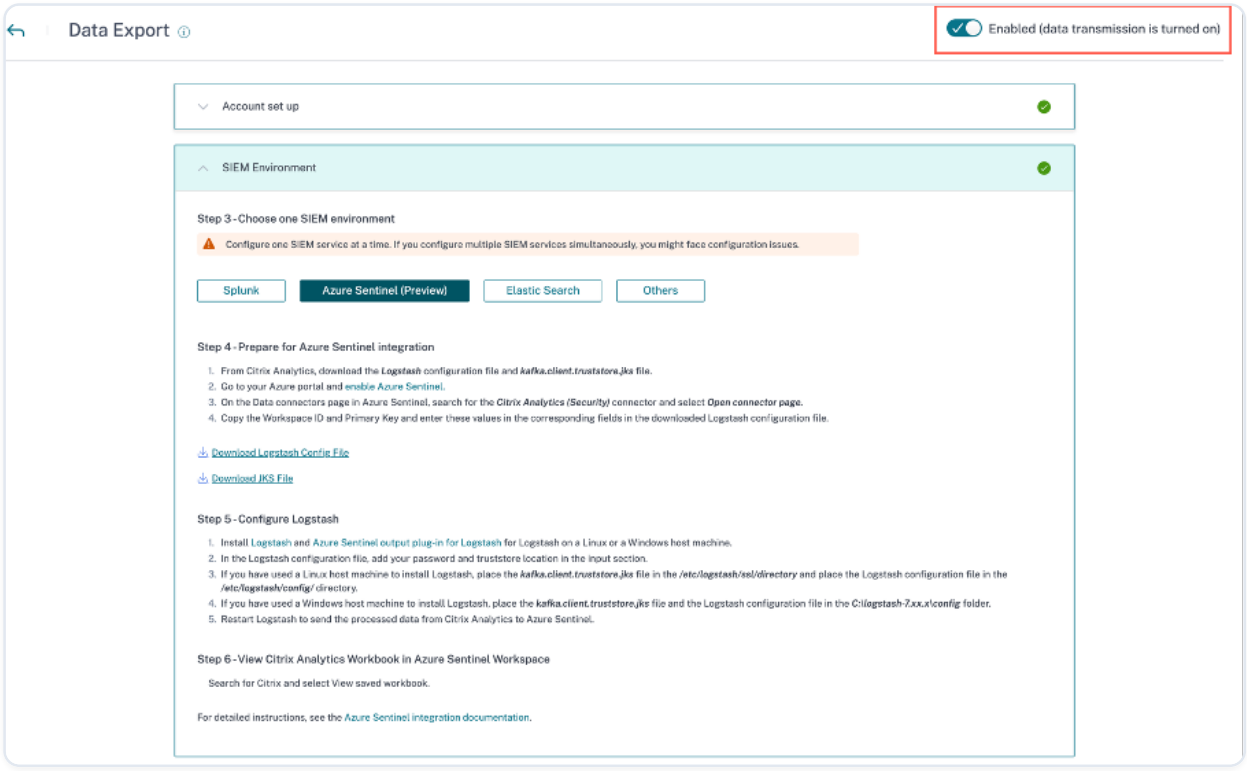
g. Microsoft Sentinel Workspaceに移動し、Citrix Analytics workbookでデータを表示します。

データ転送をオンまたはオフにする

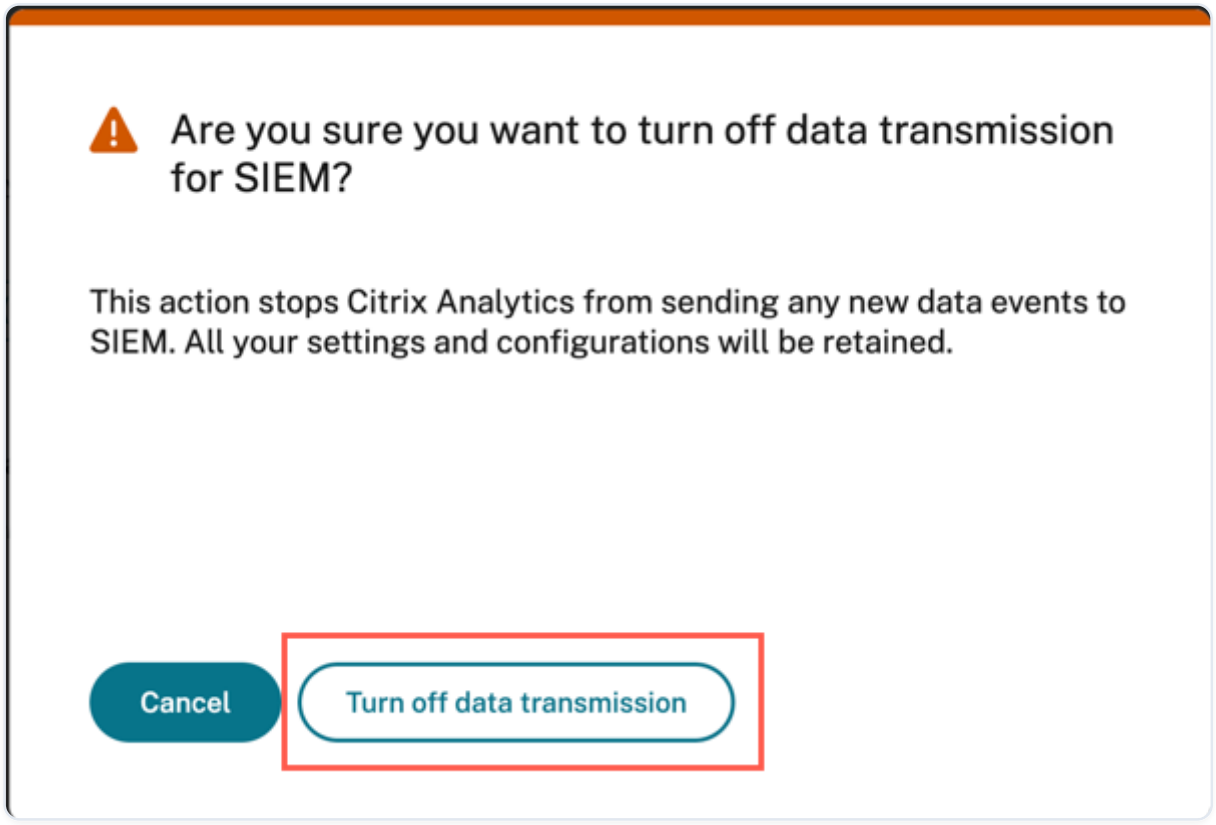
Citrix Analytics for Securityが構成ファイルを準備すると、Microsoft Sentinelのデータ転送がオンになります。

Citrix Analytics for Securityからのデータ転送を停止するには：

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。



確認のための警告ウィンドウが表示されます。**データ転送をオフにする**ボタンをクリックして、転送アクティビティを停止します。



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、以下のリンクを参照してください。

- シトリックス アナリティクス と マイクロソフト センチネル の統合
- Citrix Analytics for SecurityとMicrosoft Sentinelで脅威ハンティングを強化する

Microsoft Sentinel 用 Citrix Analytics ワークブック

> **注**
>
> この機能はプレビュー版です。

この記事では、Microsoft Sentinel ワークスペースで利用できる Citrix Analytics ワークブックについて説明します。

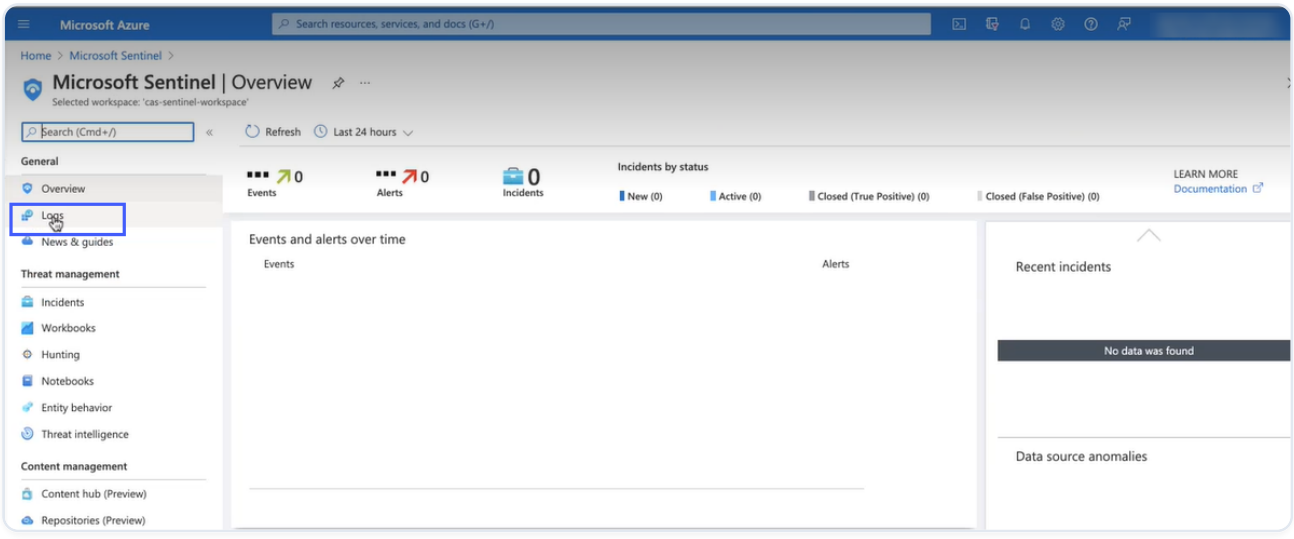
前提条件

Citrix Analytics ワークブックを使用するには、Microsoft Sentinel と Citrix Analytics for Security を統合済みであ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 イベントの表示

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 ワークスペースにイベントのプッシュを開始します。**Azure portal** で、統合に使用した Microsoft Sentinel ワークスペースを開きます。

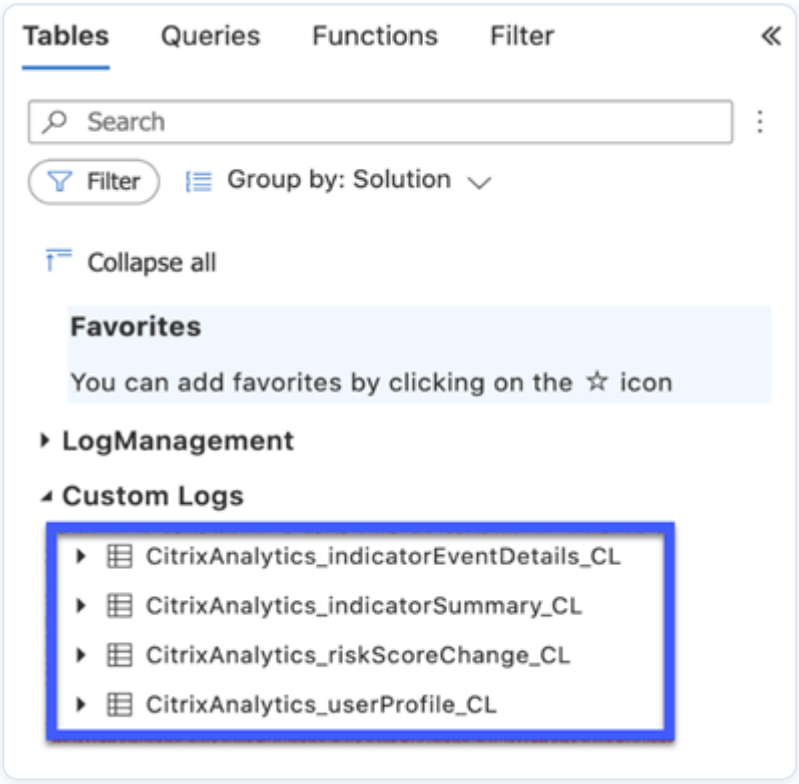
Microsoft Sentinel が Citrix Analytics for Security からイベントを受信していることを確認するには、**ログ > カスタムログ** を選択します。



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た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

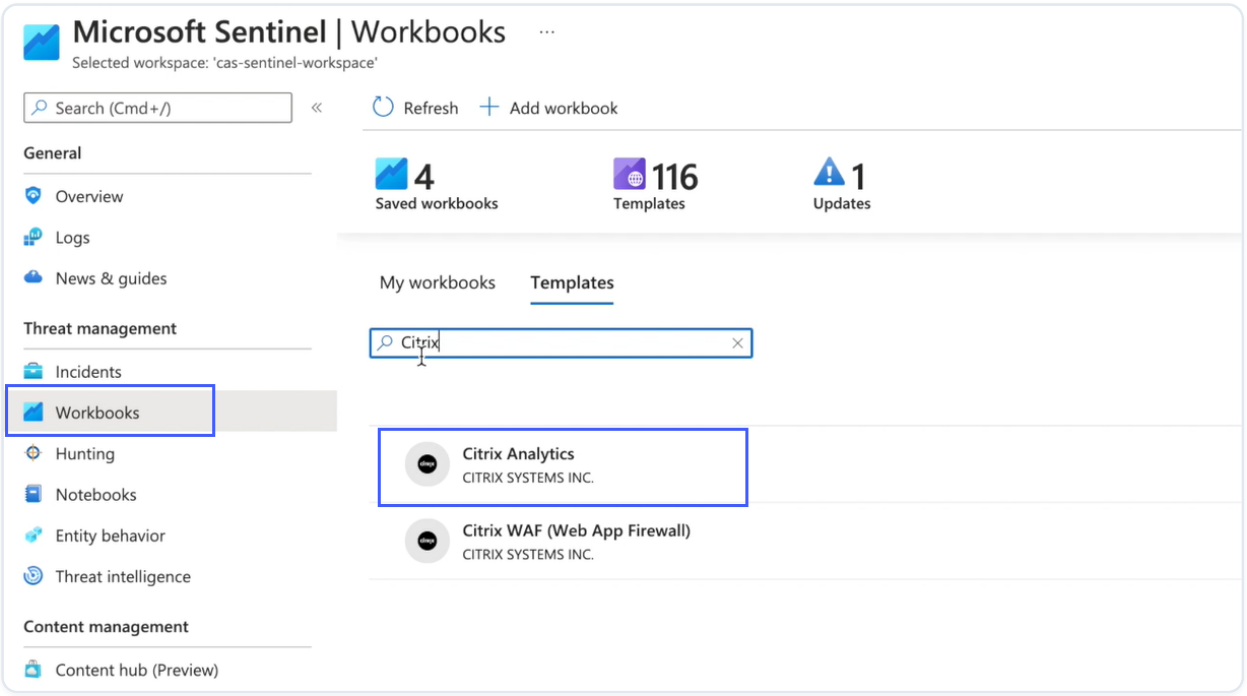
Citrix Analytics for Security から送信されたイベントが Microsoft Sentinel ワークスペースに表示されるまでに数時間かかる場合があります。そのため、イベントのログテーブルの作成に遅延が生じる可能性があります。



Citrix Analytics ワークブックの表示

ログテーブルが正常に作成されたら、次の操作を行います。

1. **Workbooks** を選択し、**Citrix Analytics** を検索します。**Citrix Analytics** を選択します。



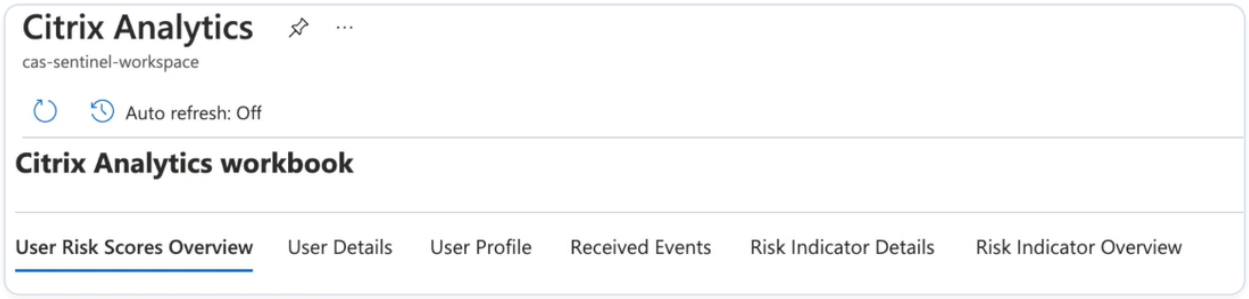
2. Citrix Analytics ワークブックを開くには、**View Template** を選択します。



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**: 組織内のリスクのあるユーザーの統合ビューを提供します。
- **ユーザーの詳細**: ユーザーとそのリスクのある行動の詳細を提供します。
- **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ックを提供します。
- **受信イベント**: Citrix Analytics for Security から受信したイベントを提供します。
- **リスクインジケーターの詳細**: 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のリスクインジケーターに関する詳細を提供します。

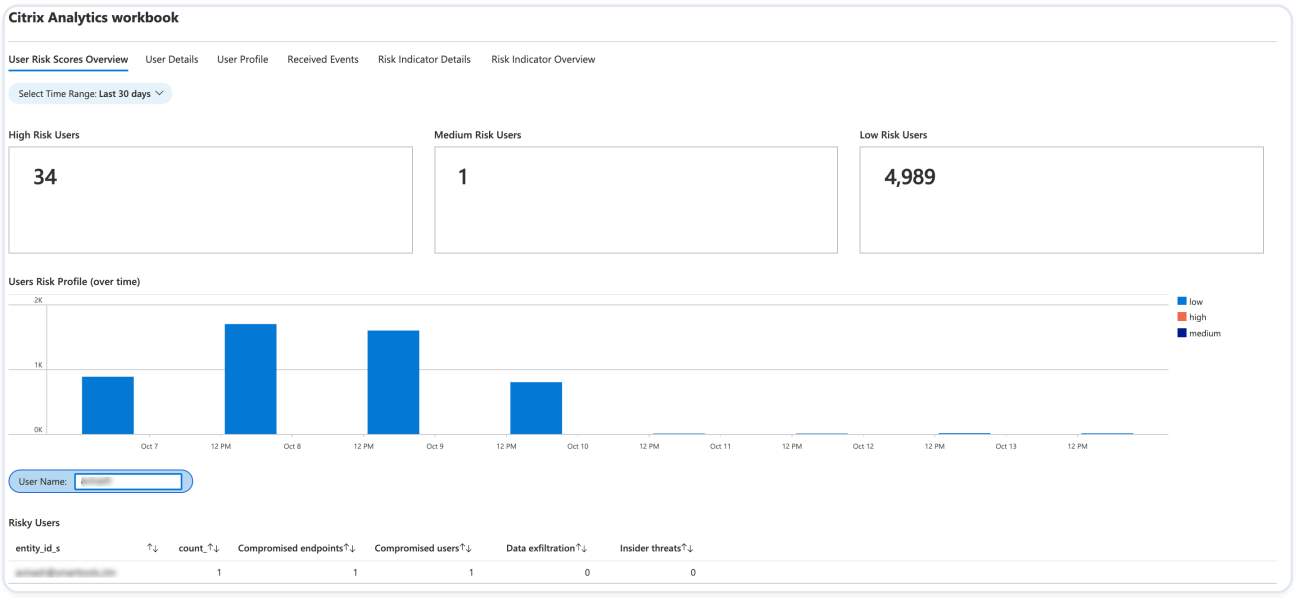
- **リスクインジケーターの概要**: ユーザーによってトリガーされたリスクインジケーターの統合ビューを提供します。



ユーザーリスクスコアの概要

このダッシュボードは、組織内のリスクのあるユーザーの統合ビューを提供します。ユーザーは、高、中、低のリスクレベルで分類されます。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、それに応じてリスクスコアが割り当てられます。リスクのあるユーザーの種類に関する詳細については、ユーザーダッシュボード を参照してください。

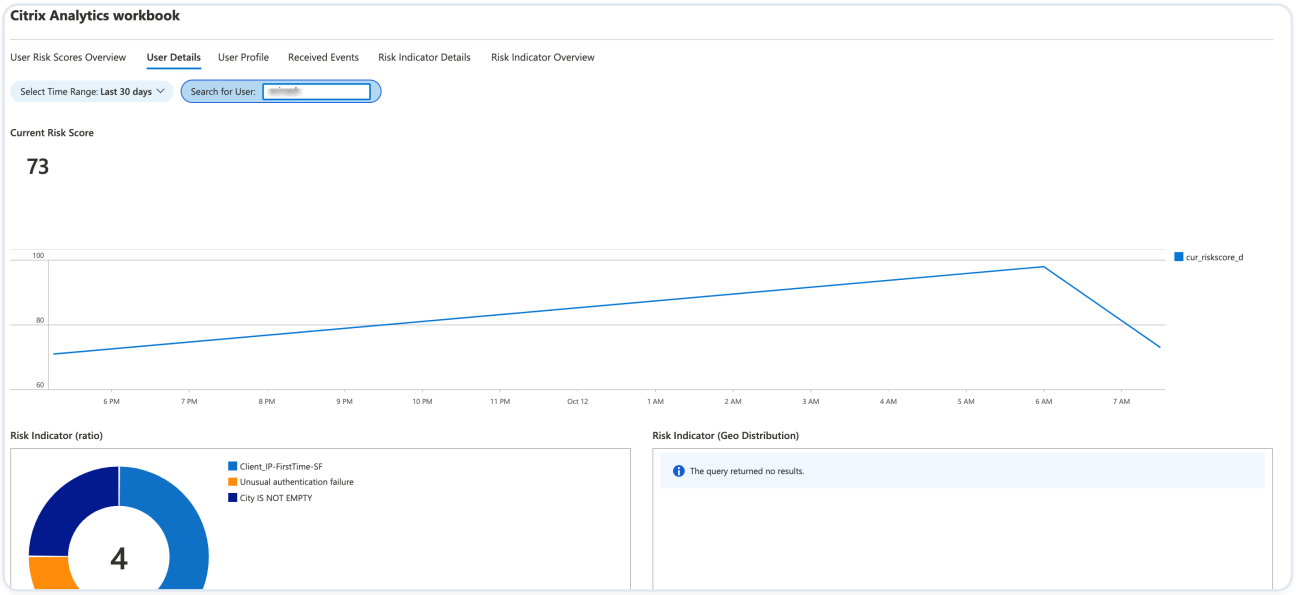
組織内のリスクのあるユーザーを表示するために、期間を選択します。



ユーザーの詳細

このダッシュボードは、ユーザーに関連付けられたリスクスコアとリスクインジケーターを提供します。

ユーザーを検索し、組織に脅威をもたらす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措置を講じることができます。



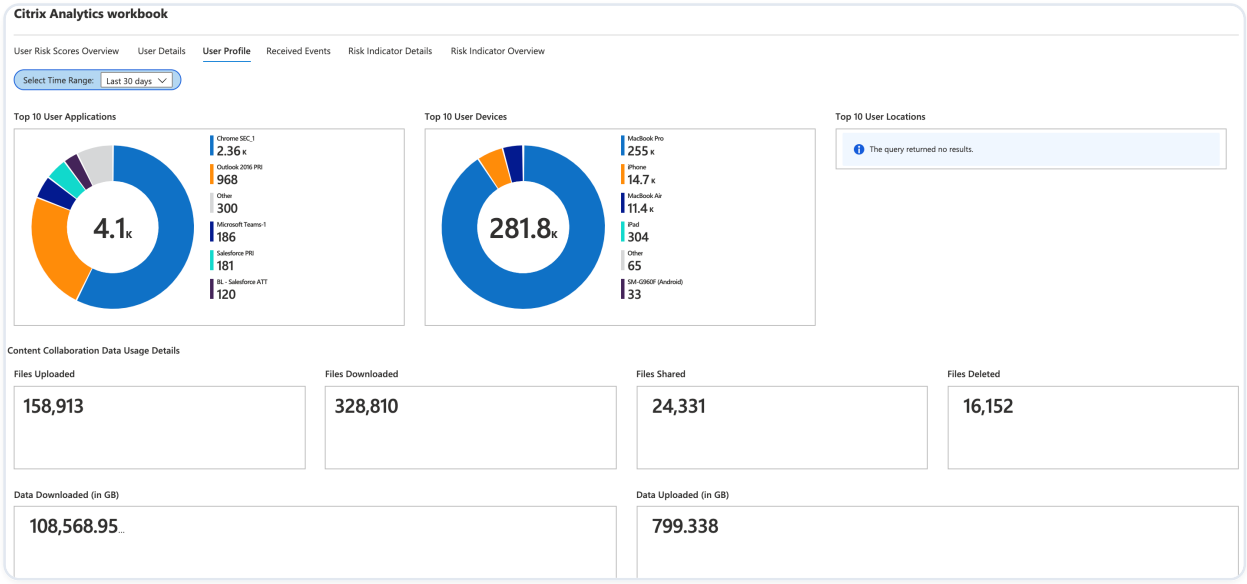
ユーザープロファイル

このダッシュボードは、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クスの詳細を提供します。これらのメトリクスは、次のようなユーザーアクティビティに関する洞察を提供します。

- ユーザーが使用した上位10のアプリケーション
- ユーザーが使用した上位10のデバイス
- ユーザーがログオンした上位10の場所

レポートを使用して、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発見する
- ユーザーからの潜在的な危険なアクセスがないか確認する

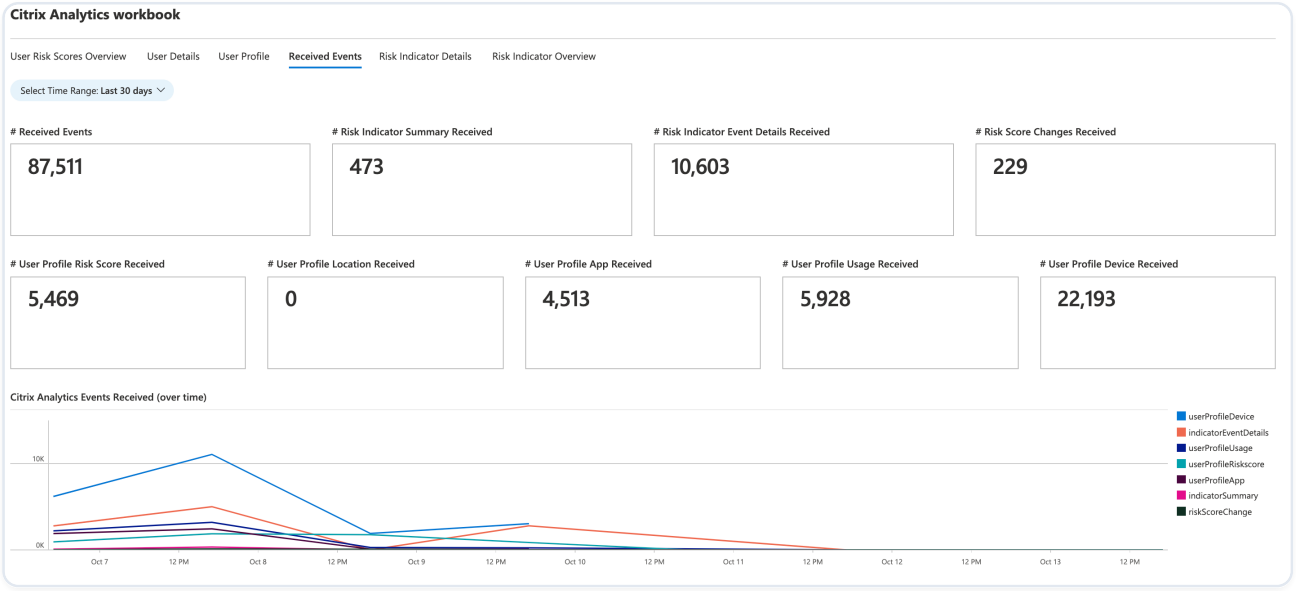


受信したイベント

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合計には、次のものが含まれます。

- リスクインジケーターの概要: ユーザーのリスクインジケーターの概要に関連付けられたイベントを示します。さまざまなリスクインジケーターの概要イベントについては、「リスクインジケータースキーマ」を参照してください。
- リスクインジケーターイベントの詳細: ユーザーのリスクインジケーターの詳細に関連付けられたイベントを示します。さまざまなリスクインジケーターの詳細イベントについては、「リスクインジケータースキーマ」を参照してください。
- ユーザープロファイルのリスクスコア: 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。
- 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た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た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状況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デバイス: ユーザーが使用するデバイスに関連付けられた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、イベントが Microsoft Sentinel ワークスペースに適切に流れていることを確認できます。受信したイベントの合計に不一致がある場合、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。

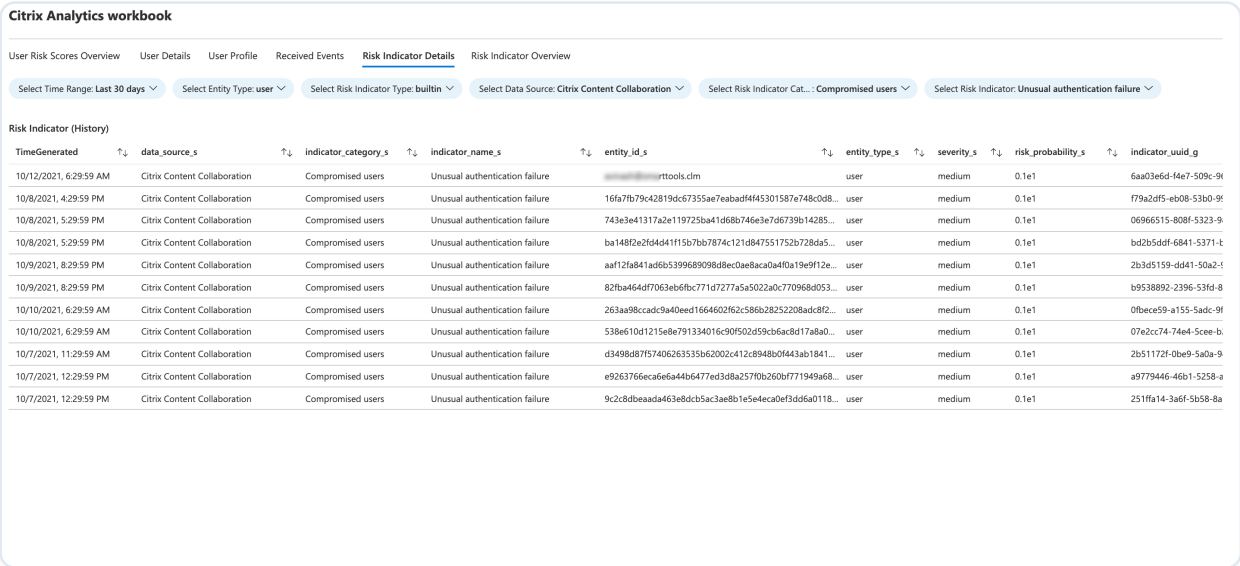


リスクインジケーターの詳細

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インジケーターの詳細が表示されます。

1つ以上のカテゴリを選択して、リスクインジケーターの詳細を表示できます。

- 時間範囲: 期間中にトリガーされたリスクインジケーターの詳細を表示するには、時間範囲を選択します。
- エンティティタイプ: 関連するリスクインジケーターの詳細を表示するには、ユーザーを選択します。
- リスクインジケータータイプ: 組み込みまたはカスタムのリスクインジケーターのいずれかを選択して、その詳細を表示します。
- データソース: 関連するリスクインジケーターを表示するには、データソースを選択します。
- リスクインジケーターカテゴリ: 関連するリスクインジケーターを表示するには、リスクカテゴリを選択します。
- リスクインジケーター: 名前でリスクインジケーターを選択し、その詳細を表示します。

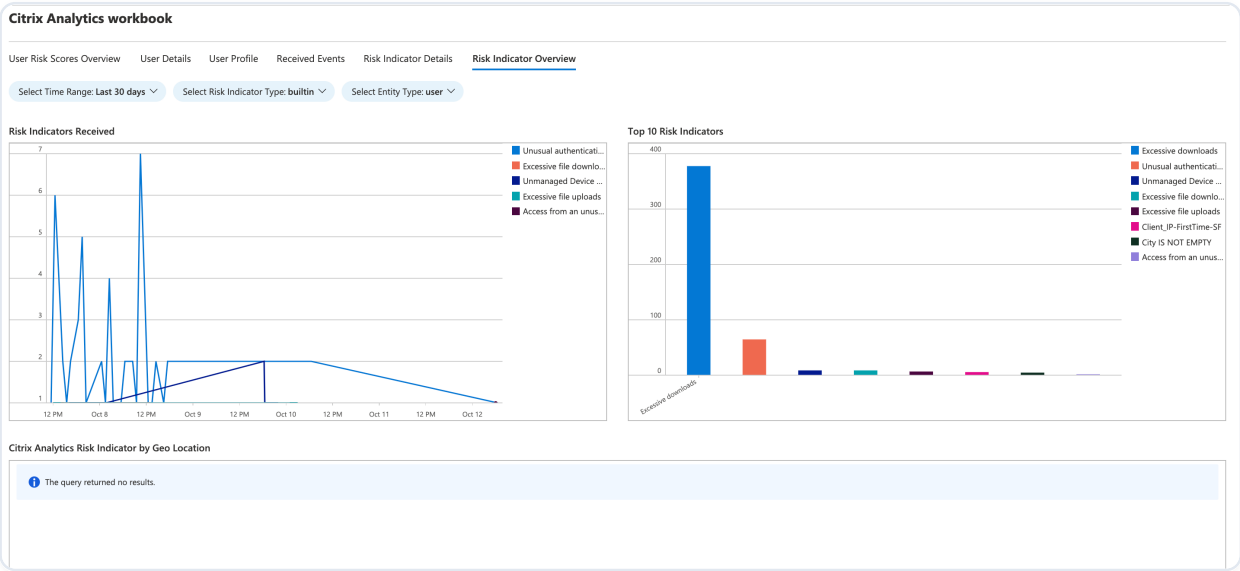


リスクインジケーターの概要

このダッシュボードは、ユーザーによってトリガーされたすべてのリスクインジケーターの統合ビューを提供します。

1つ以上のカテゴリを選択して、リスクインジケーターを表示できます。

- 時間範囲: その期間中にトリガーされたリスクインジケーターを表示するには、期間を選択します。
- リスクインジケータータイプ: 関連するリスクインジケーターを表示するには、組み込みまたはカスタムのいずれかを選択します。
- エンティティタイプ: 関連するリスクインジケーターを表示するには、ユーザーを選択します。



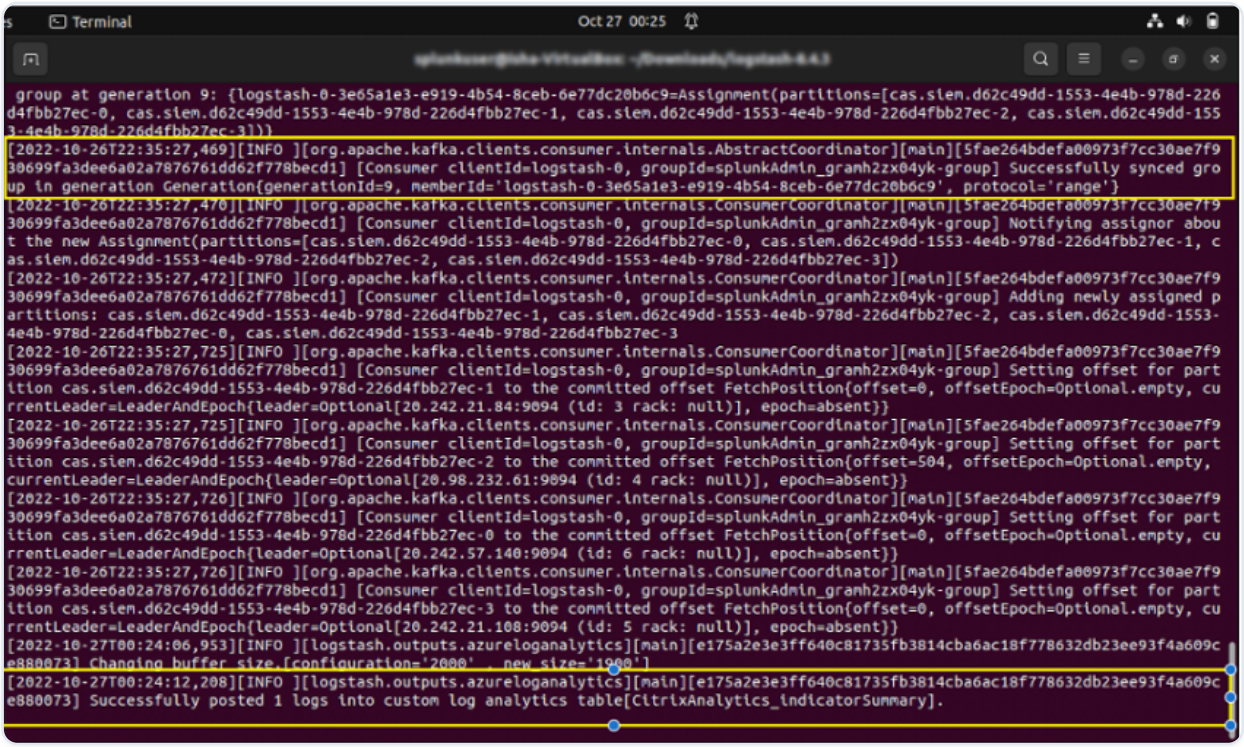
Logstash を介した Sentinel 統合のトラブルシューティングガイダンス

この記事では、Logstash を使用して Microsoft Sentinel と Citrix Analytics を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一覧表示します。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 サーバーログの確認

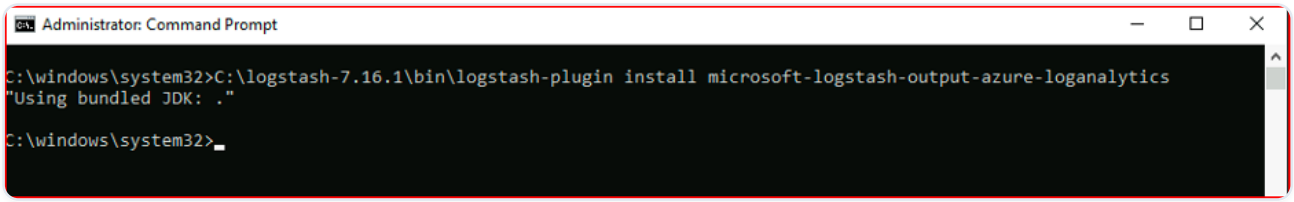
ターミナルウィンドウに表示される Logstash サーバーログを確認して、データが Sentinel ワークスペースのカスタムログテーブルに正しく取り込まれているかどうかを検証できます。

1. ログの詳細を表示するには、**設定 > データエクスポート > 構成**タブ **> SIEM 環境**を展開し、Logstash 構成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)** の下で、**Logstash 構成ファイルのダウンロード**をクリックします。
2. 構成ファイルを使用して Logstash サーバーを起動すると、Microsoft Azure がホストする Log Analytics ワークスペースへの接続が成功したことを示す次のログが同じターミナルウィンドウに表示されます。

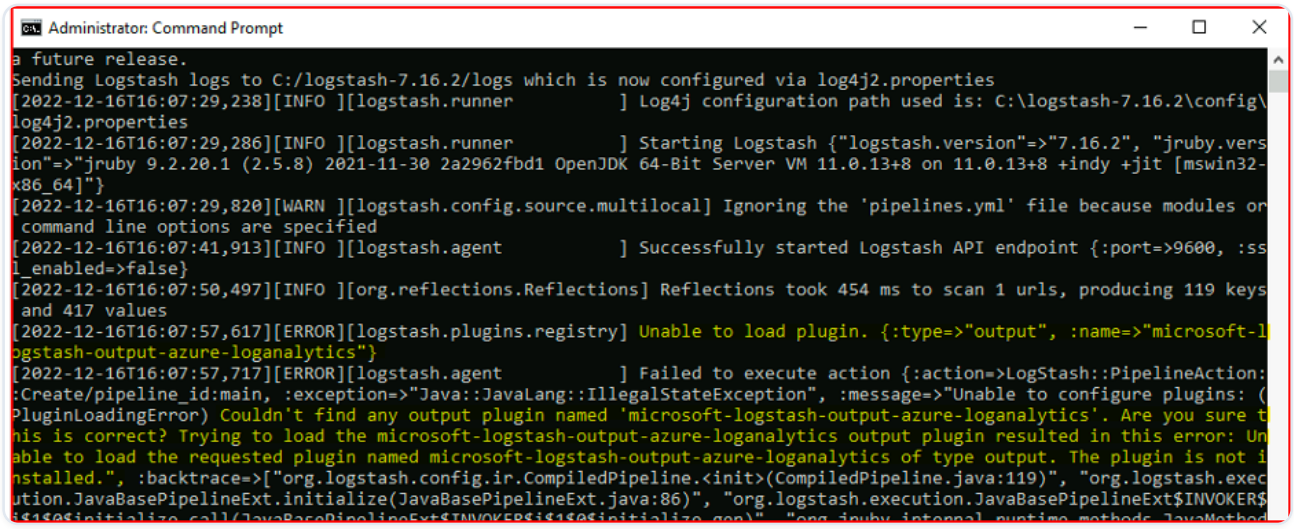


一般的なエラー: バンドルされた JDK の使用

Microsoft Log Analytics プラグインをインストールしようとすると、以下に示す一般的なエラーが報告されます。



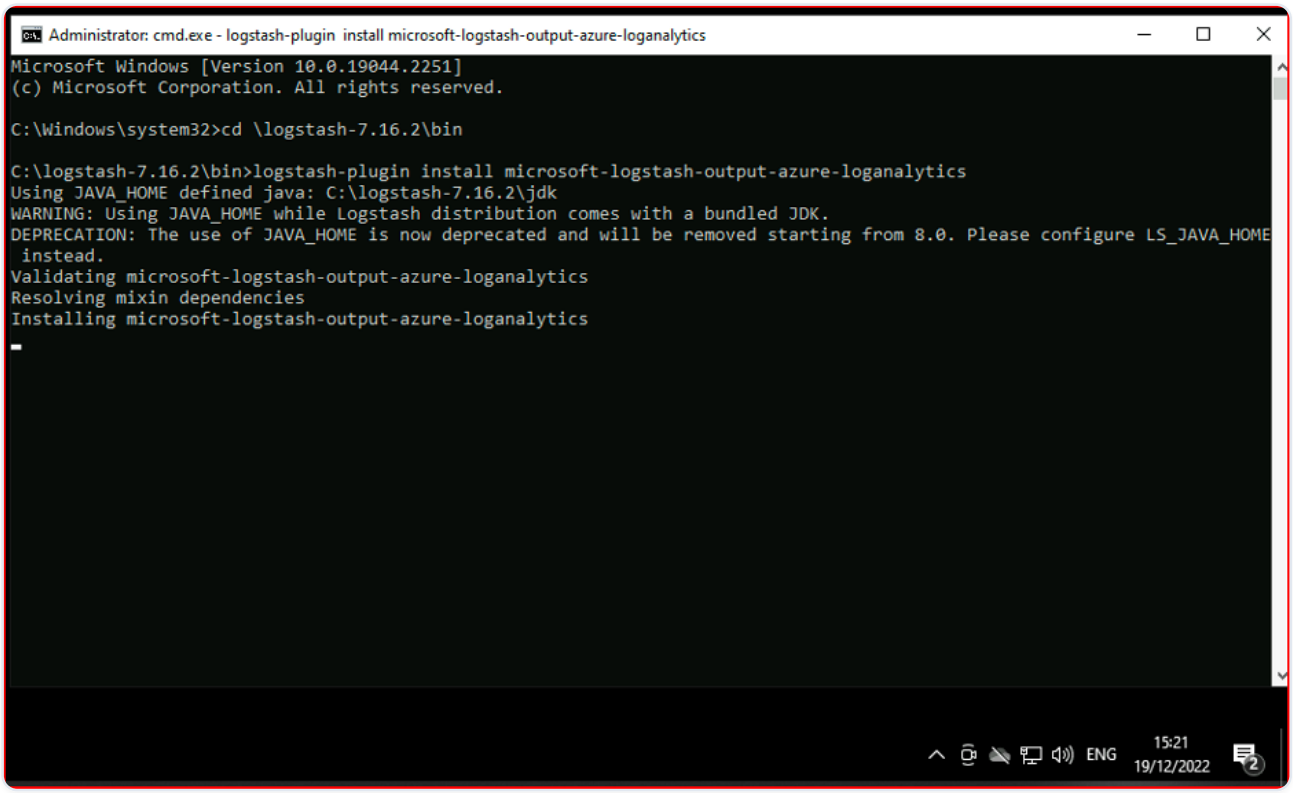
この後、Logstash サーバーを実行しようとすると、次のエラーが表示される場合があります。



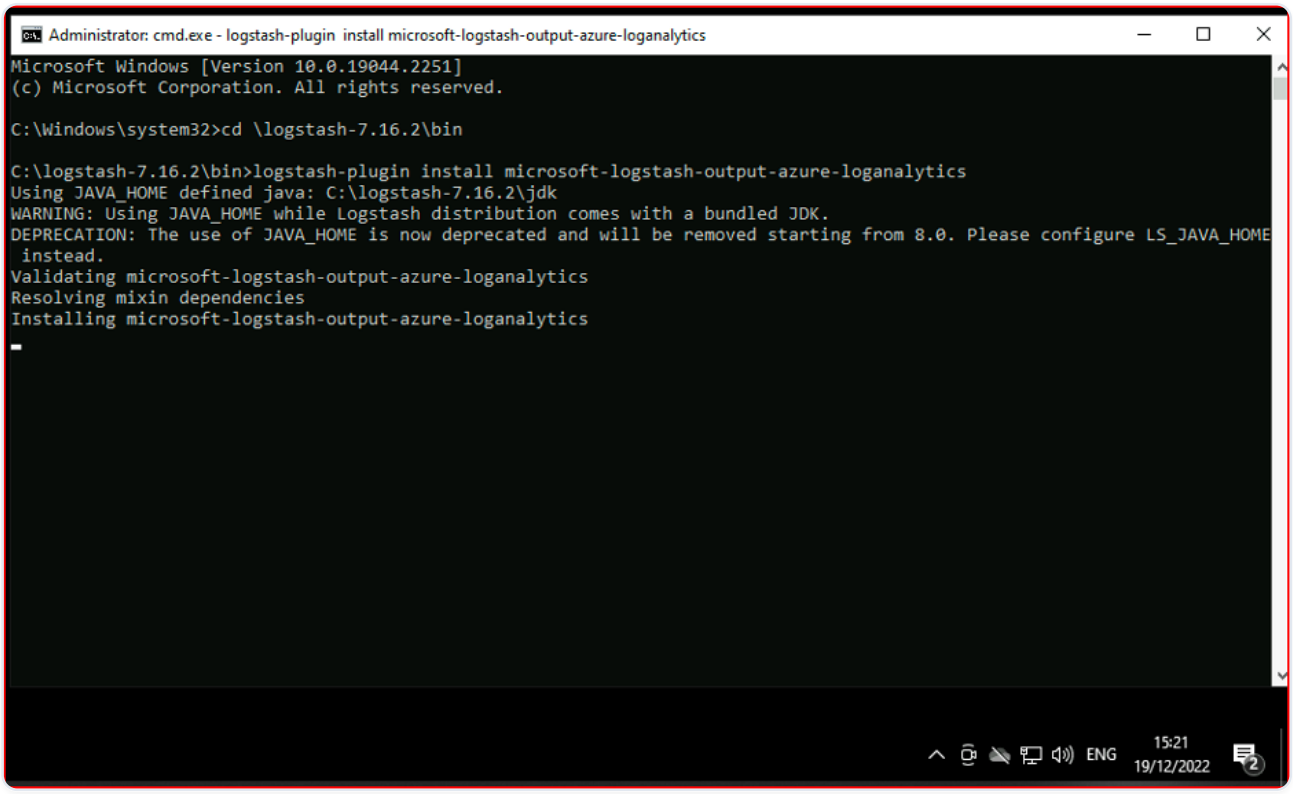
これを解決するには、JAVA_HOME をバンドルされた JDK に設定します。

1. Windows 環境変数に移動します
2. “JAVA_HOME” という名前で新しいシステム変数を作成します
3. バンドルされたLogstash JDKへのパスを追加します (< path_to_logstash >/logstash-X.X.X/jdk)

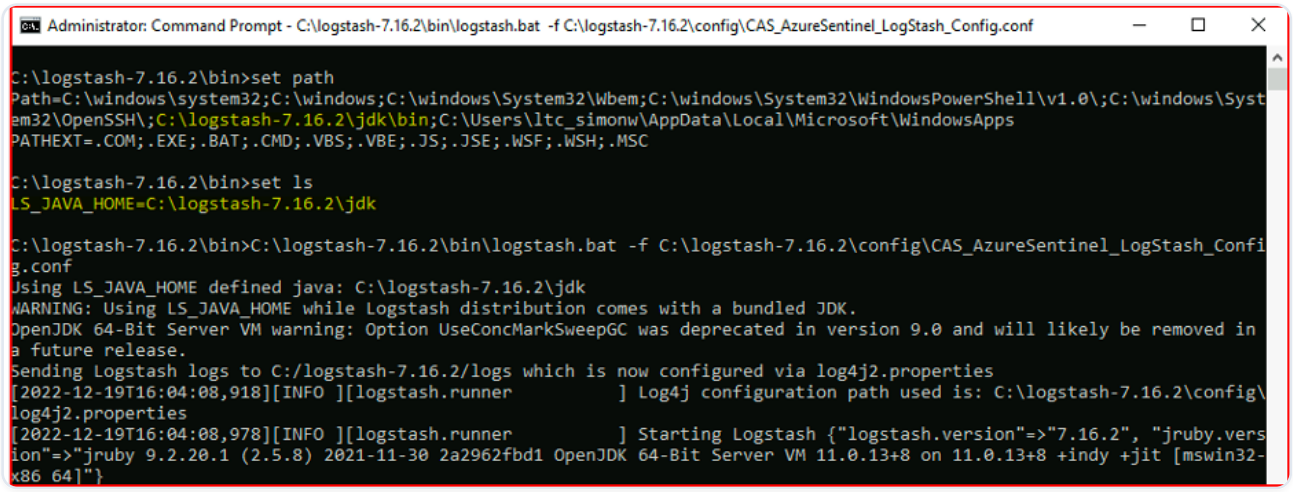
上記の手順を実行した後、プラグインを再度インストールしようとすると、次の画面が表示されます。



LS_JAVA_HOMEを使用する場合（JAVA_HOMEは非推奨のため）、システムPATH変数にバンドルされたJDKの場所も指定する必要があり、このパスは**jdk\bin**フォルダーを指している必要があります（LS_JAVA_HOME変数とは異なります）。



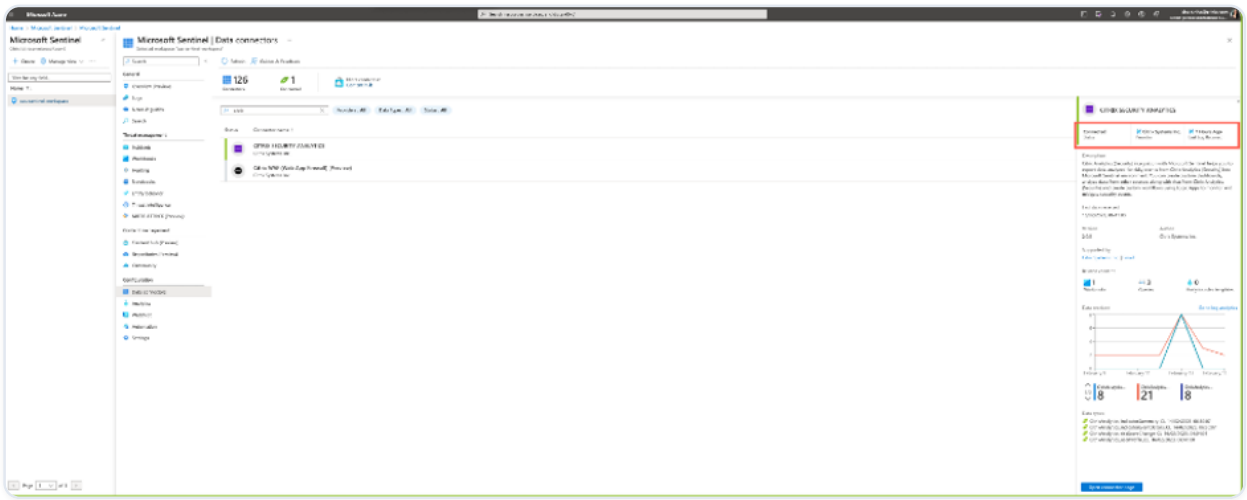
LS_JAVA_HOMEを使用する場合（JAVA_HOMEは非推奨のため）、システムPATH変数にバンドルされたJDKの場所も指定する必要があり、このパスは**jdk\bin**フォルダーを指している必要があります（LS_JAVA_HOME変数とは異なります）。



Microsoft Sentinel ワークブックを確認する

Citrix Analyticsから送信されたデータが、Log Analyticsワークスペース内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の統合の詳細については、Microsoft Sentinel integrationを参照してください）：

1. **Azure portal > 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 Security Analytics**を選択してクリックします。
2. 上部のバーで接続ステータスを確認します。



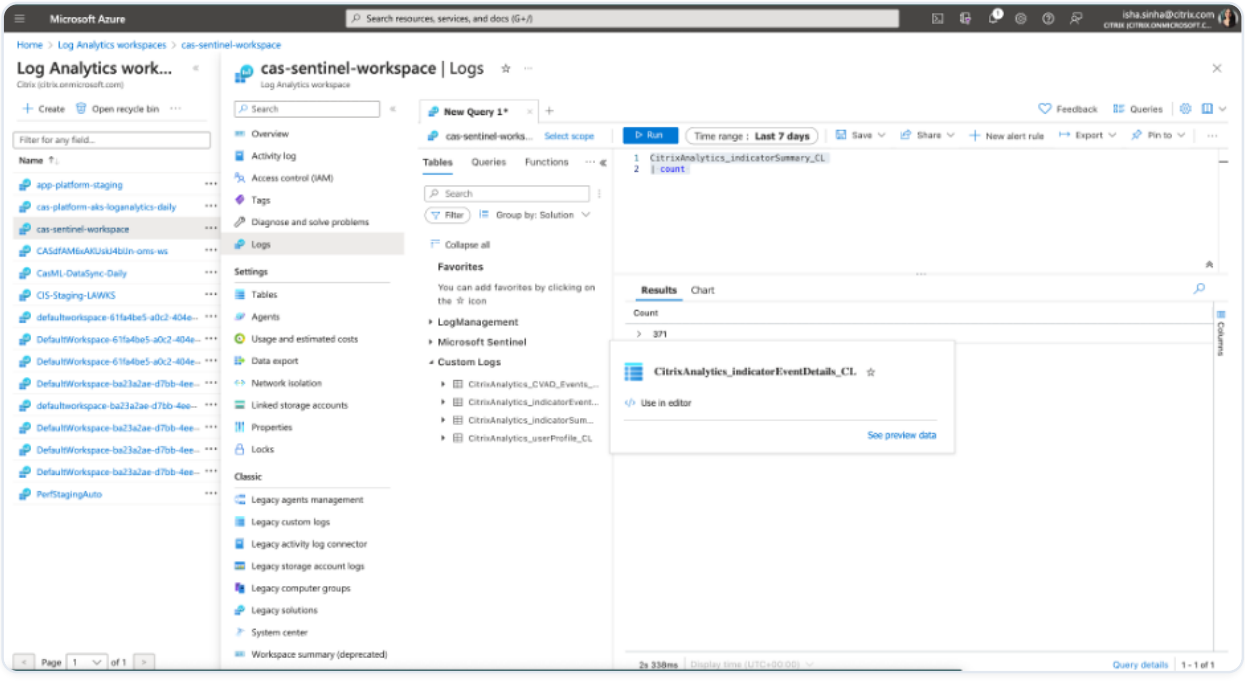
3. ワークブックの下では、直感的なフィルターを使用してデータをさらにドリルダウンし、リスクインジケーター情報を取得できます。情報を取得するには、**Azure portal > Microsoft Sentinel > データコネクタ > CITRIX SECURITY ANALYTICS > ワークブック**に移動します。



KQLを使用してLog Analyticsワークスペースのログを確認する

該当するカスタムログテーブルに対してKQLクエリを実行することで、正しいデータがLog Analyticsワークスペースに到達したかどうかを確認することもできます。

1. **Azure portal > Log Analyticsワークスペース** に移動し、正しい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** タブの下にある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。(Log Analyticsワークスペースでの KQLクエリに関するガイダンスについては、Log Analytics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。



エラスティックサーチ連携

> **注**
>
> Elasticsearch連携、Elasticsearchへのデータエクスポート、またはフィードバックについては、mailto:CAS-PM-Ext@cloud.comまで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と連携させます。この連携により、Citrix IT環境からユーザーデータを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関するより深い洞察を得ることができます。また、Elasticsearchを視覚化サービスや、KibanaやLogRhythmのようなSIEMと組み合わせて使用することもできます。

連携の利点と、SIEMに送信される処理済みデータの種類について詳しくは、セキュリティ情報およびイベント管理の連携を参照してください。

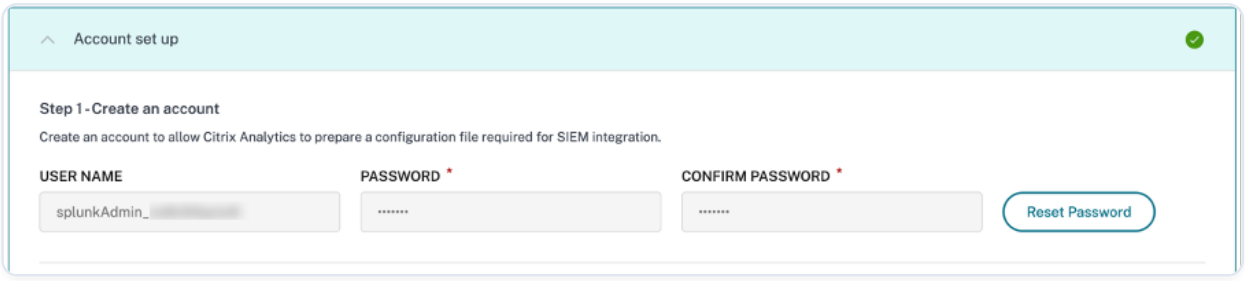
前提条件

- 少なくとも1つのデータソースでデータ処理をオンにします。これにより、Citrix Analytics for Security™がElasticsearch連携プロセスを開始するのに役立ちます。
- 以下の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てください。

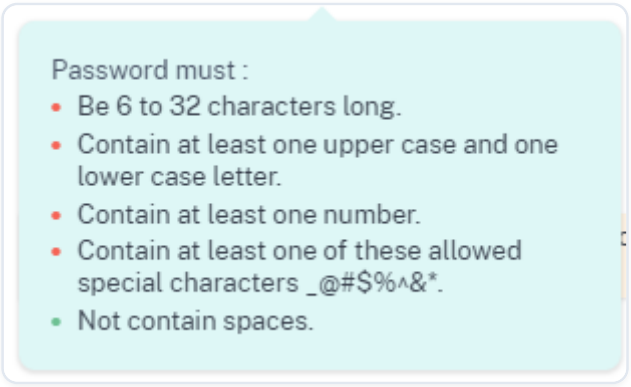
エンドポイント	米国リージョン	欧州連合リージョン	アジア太平洋南部リージョン
Kafkaブローカー	`casnb-0.citrix.com:9094`	`casnb-eu-0.citrix.com:9094`	`casnb-aps-0.citrix.com:9094`
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`	`casnb-aps-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`		

Elasticsearch と統合する

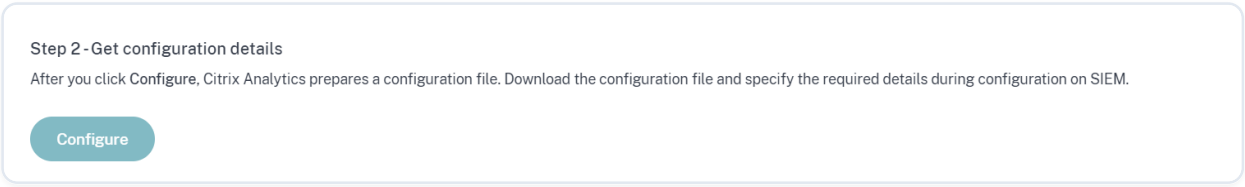
1. **設定 > データエクスポート** に移動します。
2. **アカウント設定** セクションで、ユーザー名とパスワードを指定してアカウントを作成します。このアカウントは、統合に必要な設定ファイルの準備に使用されます。



3. パスワードが以下の条件を満たしていることを確認してください。



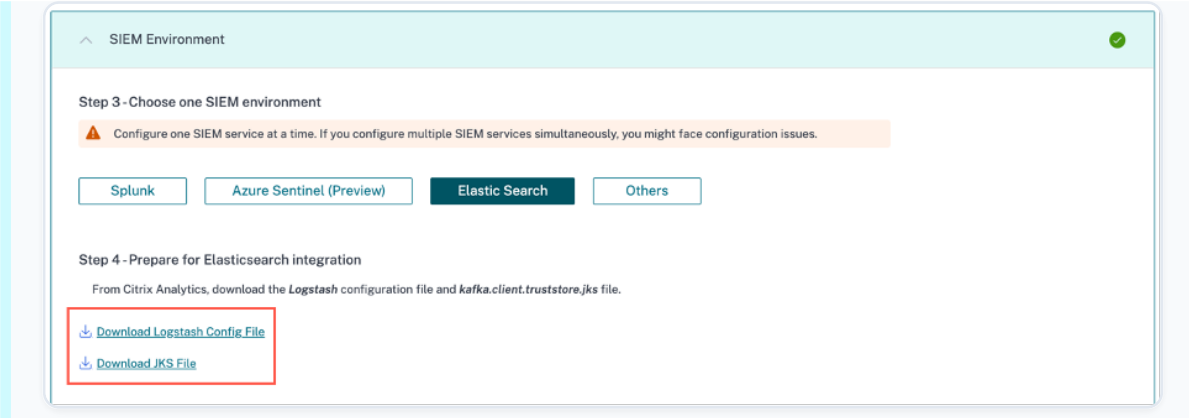
4. **設定** をクリックして、Logstash 設定ファイルを生成します。



5. SIEM環境セクションから**Elastic Search**タブを選択し、構成ファイルをダウンロードします。

- **Logstash設定ファイル**: 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設定データ（入力、フィルター、出力セクション）が含まれています。Logstash設定ファイルの構造については、Logstash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ています。

> **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を構成します。

   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、指定されたディレクトリに以下のファイルを配置します。

ホストマシンの種類	ファイル名	ディレクトリパス
リナックス	CAS_Elasticsearch_LogStash_Config.config	Debian および 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 および 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`
ウィンドウズ	CAS_Elasticsearch_LogStash_Config.config	`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 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. ファイルの入力セクションに、次の情報を入力します。

- **パスワード**: 設定ファイルを準備するために Citrix Analytics for Security で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、ホストマシン上の 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で、ホストマシンまたはElasticsearchが実行されている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. Citrix Analytics for Securityから処理済みデータをElasticsearchに送信するには、ホストマシンを再起動します。

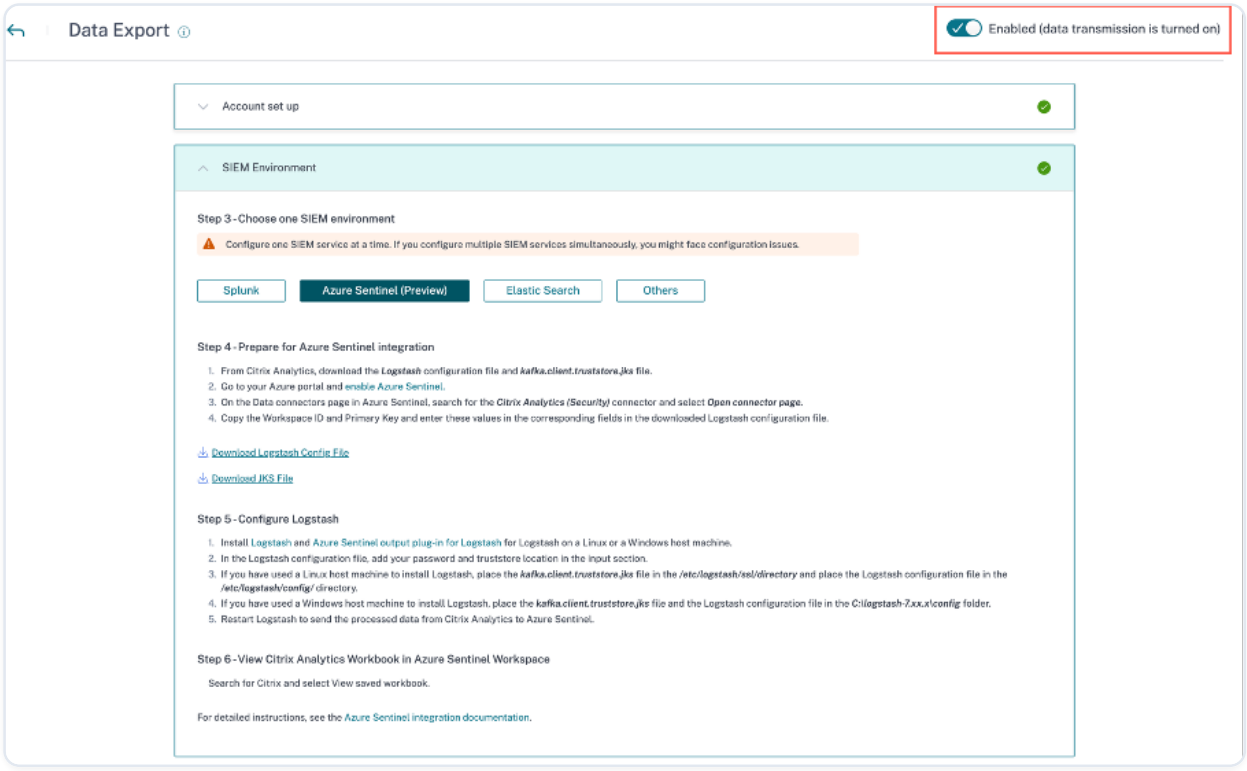
設定が完了したら、Citrix AnalyticsのデータがElasticsearchで表示できることを確認します。

データ転送のオン/オフを切り替える

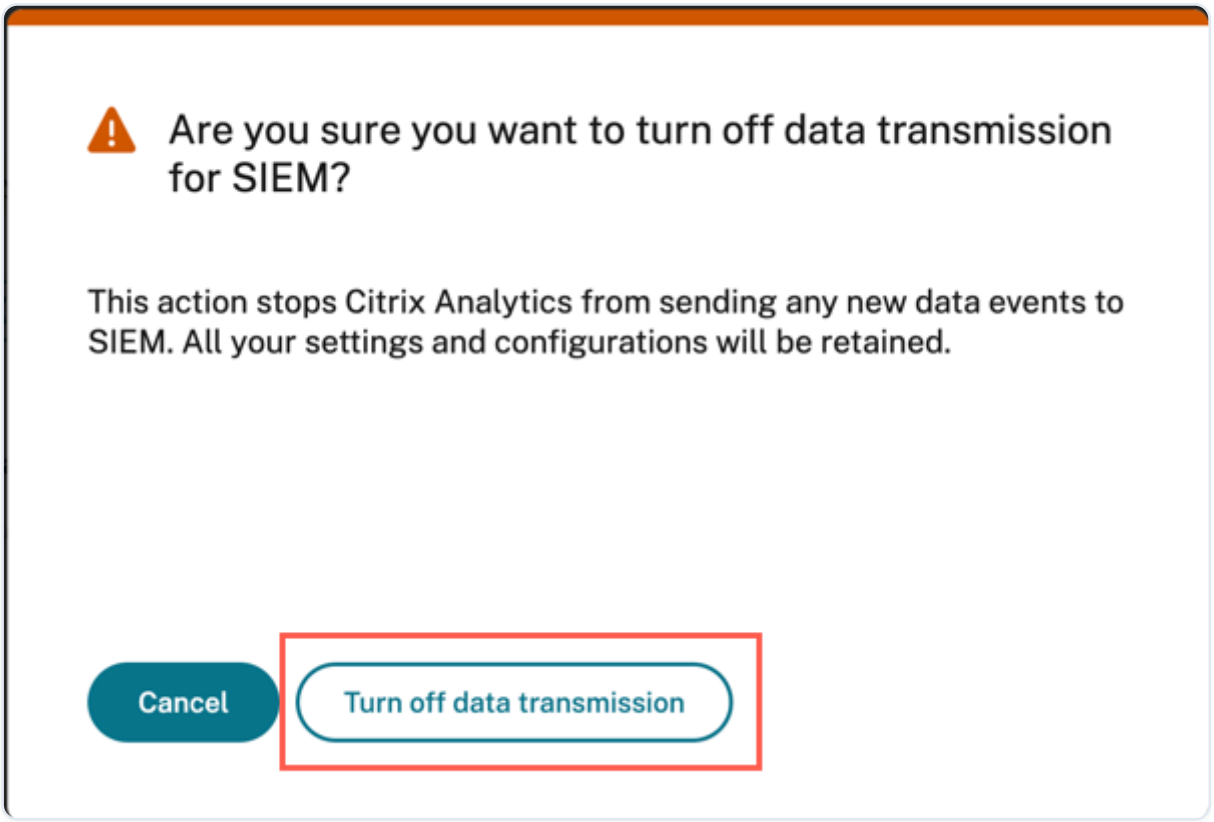
Citrix Analytics for Securityが設定ファイルを準備すると、Elasticsearchへのデータ転送が有効になります。

Citrix Analytics for Securityからのデータ転送を停止するには：

1. **設定 > データエクスポート**に移動します。
2. データ転送を無効にするには、トグルボタンをオフにします。デフォルトでは、**データ転送**は常に有効になっています。



確認のための警告ウィンドウが表示されます。転送アクティビティを停止するには、**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

Citrix Analytics for Security™ SIEM統合により、Citrix AnalyticsからSIEM環境にユーザーデータを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関する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タイプ（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、セキュリティ情報およびイベント管理の統合を参照してください。

Citrix Analytics for Securityは、次の2つのメカニズム（SIEMおよびIT展開でサポートされている）を介してSIEMソリューションと統合できます。

1. Kafkaエンドポイント経由で接続
2. Kafkaベースの取り込みによるLogstashデータブローカー経由で接続

前提条件

- 少なくとも1つのデータソースでデータ処理をオンにします。これにより、Citrix Analytics for SecurityはSIEMツールとの統合を開始できます。
- 次の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てください。

エンドポイント	米国リージョン	欧州連合リージョン	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`
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`	`casnb-aps-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`
	`casnb-3.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あり、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、より迅速なインサイトを得ることができます。主に、十分なデータを扱う大規模な組織がKafkaを使用しています。

ノースバウンドKafkaは、Citrix AnalyticsがKafkaエンドポイントを介してSIEM顧客とリアルタイムデータフィードを共有できるようにする内部ミドルレイヤーです。SIEMがKafkaエンドポイントをサポートしている場合は、Logstash設定ファイルで提供されているパラメータと、JKSファイルまたはPEMファイル内の証明書詳細を使用して、SIEMをCitrix Analytics for Securityと統合します。

Kafkaを使用して統合するには、以下のパラメータが必要です。

属性名	説明	設定データ例
ユーザー名	Kafkaによって提供されるユーザー名。	`'sasl.username': cas_siem_user_name,`
ホスト	接続したい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	コンシューマーによって共有されたメッセージを読み取る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	セキュアな認証を実装するために、通常暗号化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。クライアントトラストストアのパスワードはオプションであり、空のままにすることが想定されています。	`'ssl.ca.location': ca_location`

属性名	説明	設定データ例
セッションタイムアウト	Kafkaの使用中にクライアントの障害を検出するため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際の動作を定義します。latest、earliest、noneなどの値を設定できます。	`'auto.offset.reset': 'earliest',`

以下は、設定出力のサンプルです。

```
{'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',

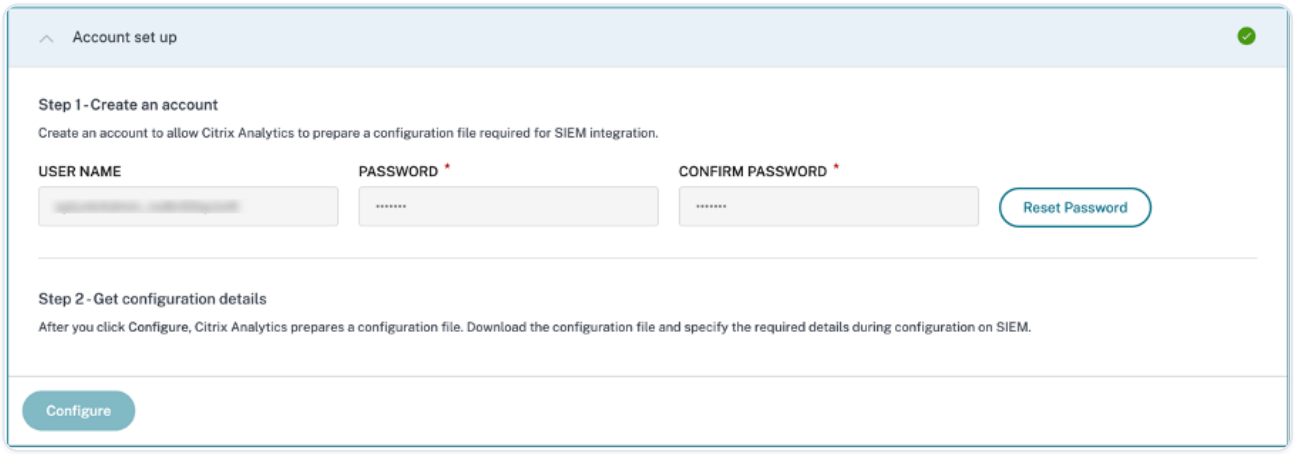
                    'sasl.mechanisms': 'SCRAM-SHA-256',

                    'sasl.username': cas_siem_user_name,

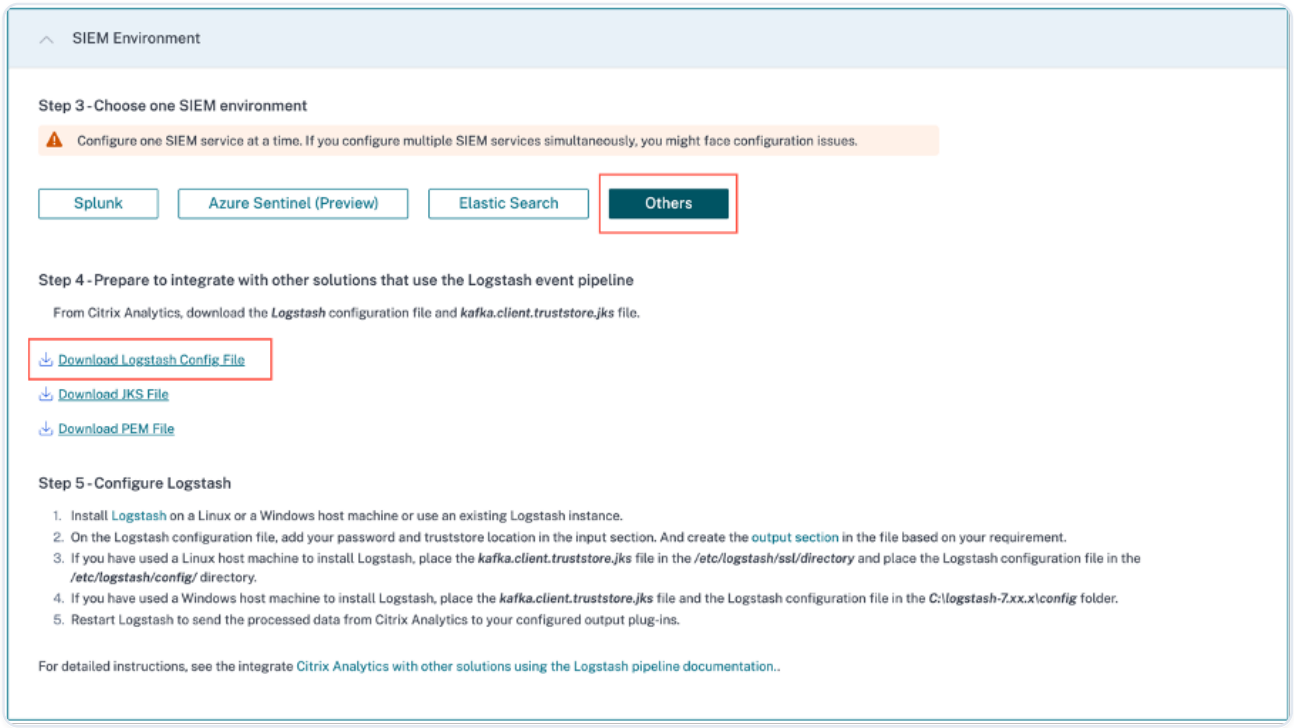
                    'sasl.password': self.CLEAR_PASSWORD,

                    'ssl.ca.location': ca_location

            }
```



前述のパラメーターは、Logstash設定ファイルで利用できます。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**タブを選択して、**Logstash設定ファイルのダウンロード**をクリックします。



設定値の詳細については、構成を参照してください。

データフロー

認証データの通信は、Kafkaサーバー側のブローカー (Citrix Analytics for Securityクラウド) 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、有効なSASL_SSLセキュリティプロトコルを使用し、公開アクセスには9094ポートをターゲットとします。

Apache Kafkaには、SSL暗号化を使用して転送中のデータを暗号化するためのセキュリティコンポーネントがあります。 暗号化が有効になり、SSL証明書が設定されている場合、ネットワーク

経由のデータ送信は暗号化され、保護されます。最初と最後のマシンのみが、SSL経由で送信されるパケットを復号化する能力を持っています。

認証

以下の2つのレベルの認証が利用可能です。

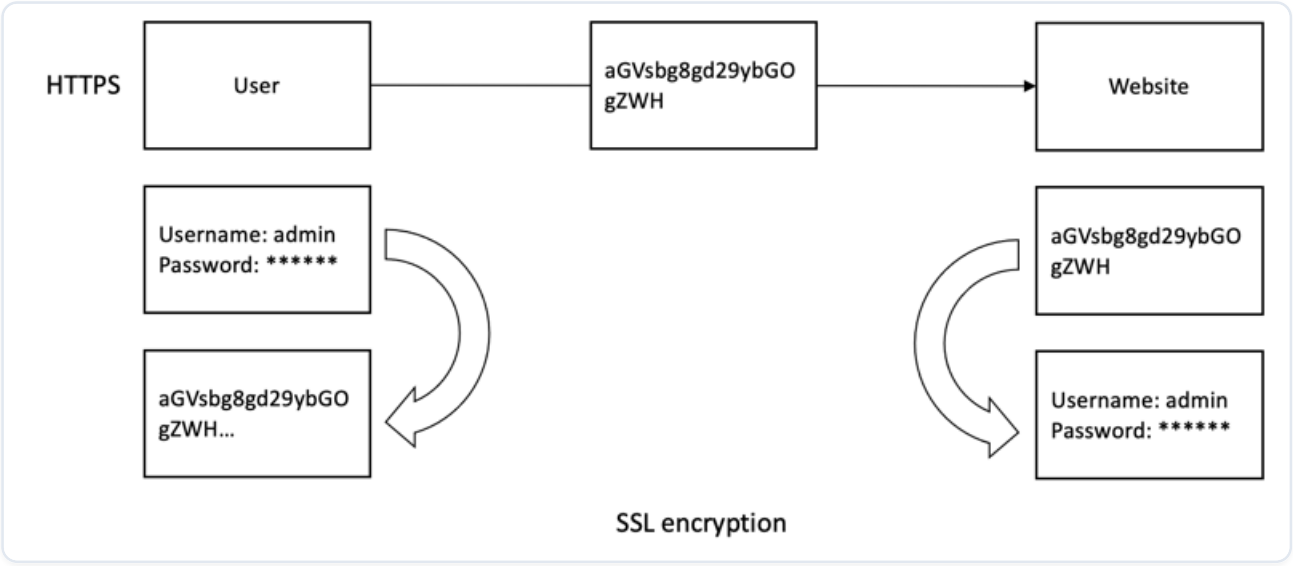
1. TLS/クライアントとサーバー間。
    - クライアントとサーバー間で交換されるTLS認証用のサーバー証明書（公開鍵）。
    - クライアントベース認証または双方向認証はサポートされていません（クライアント秘密鍵証明書が必要な場合）。
2. TOPICS/エンドポイントへのアクセス制御のためのユーザー名/パスワード
    - 特定のクライアントが特定の顧客トピックからのみ読み取れるようにする
    - SASL/SCRAMは、安全な認証を実装するために、TLS暗号化とともにユーザー名/パスワード認証メカニズムとして使用されます。

SSLによる暗号化とSASL/SSLおよびSASL/PLAINTEXTによる認証

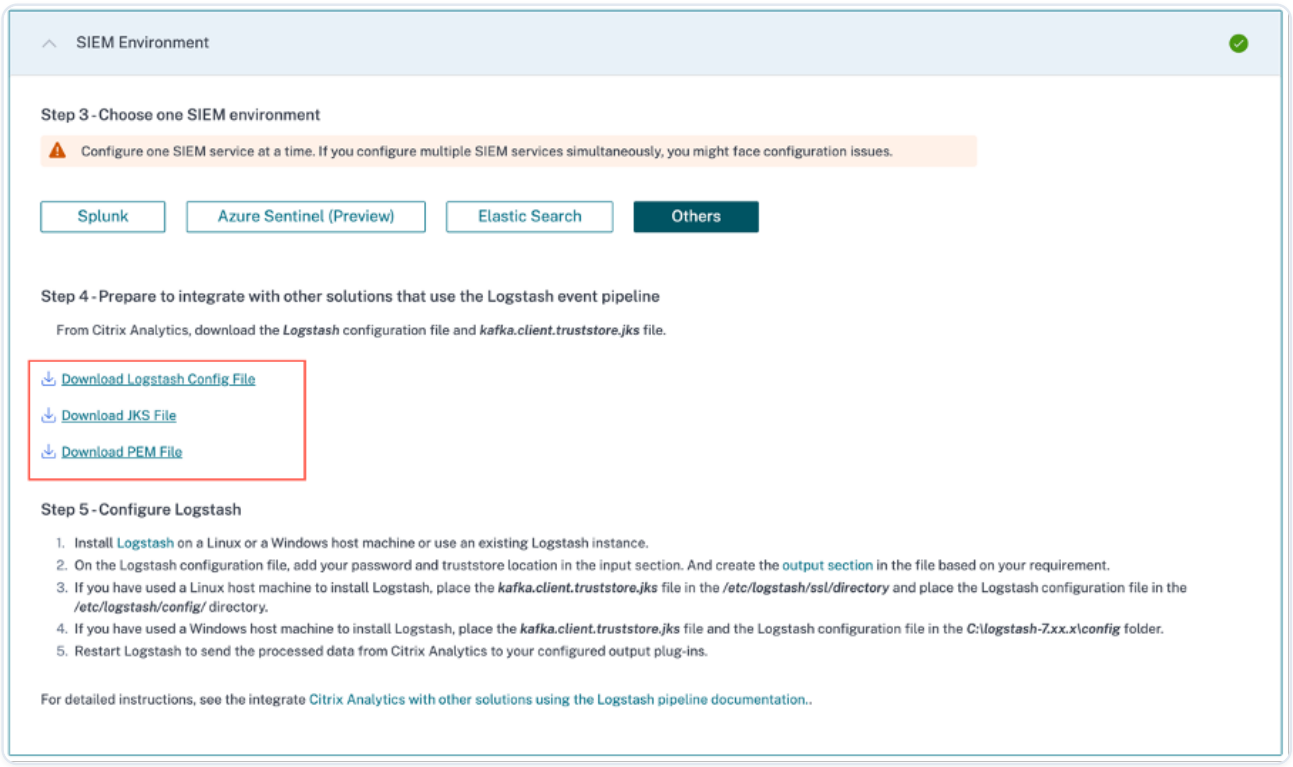
デフォルトでは、Apache KafkaはPLAINTEXTで通信し、すべてのデータは平文で送信され、ルーターのいずれかがデータコンテンツを読み取ることができます。Apache Kafkaには、SSL暗号化を使用して転送中のデータを暗号化するセキュリティコンポーネントがあります。暗号化を有効にし、SSL証明書を慎重に設定することで、データは暗号化され、ネットワーク経由で安全に送信されます。SSL暗号化を使用すると、最初と最後のマシンだけが送信されるパケットを復号化する能力を持ちます。

双方向SSL暗号化が使用されているため、ユーザー名/パスワードログインは外部通信に対して安全です。

暗号化は転送中のみであり、データはブローカーのディスク上では暗号化されていないままです。



クライアント構成では、クライアントトラストストアJKSファイルとPEMファイル（トラストストアJKSファイルから変換されたもの）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。



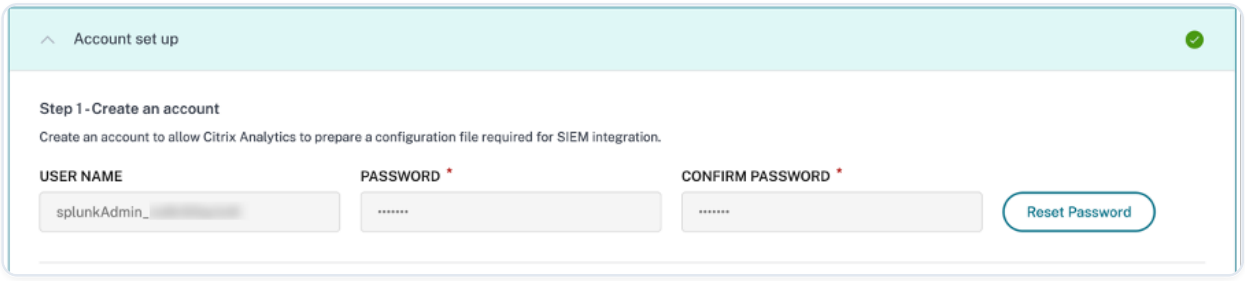
Logstashを使用したSIEM統合

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Logstashでサポートされている出力プラグインのいずれかにデータイベントを送信できます。

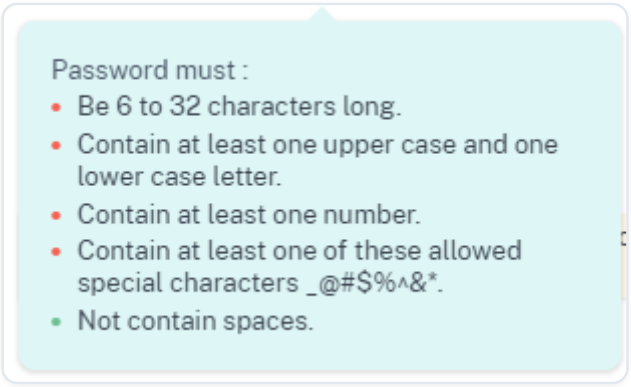
以下のセクションでは、Logstashを使用してSIEMをCitrix Analytics for Securityと統合するために従う必要がある手順について説明します。

Logstashを使用してSIEMサービスと統合する

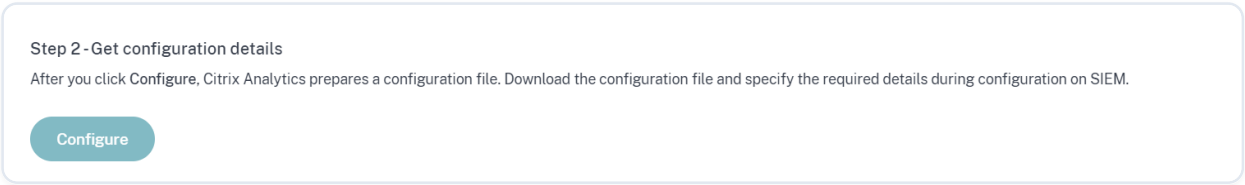
1. **設定 > データエクスポート**に移動します。
2. **アカウント設定**ページで、ユーザー名とパスワードを指定してアカウントを作成します。このアカウントは、統合に必要となる構成ファイルを準備するために使用されます。



3. パスワードが以下の条件を満たしていることを確認してください。



4. **Configure**を選択して、Logstash設定ファイルを生成します。

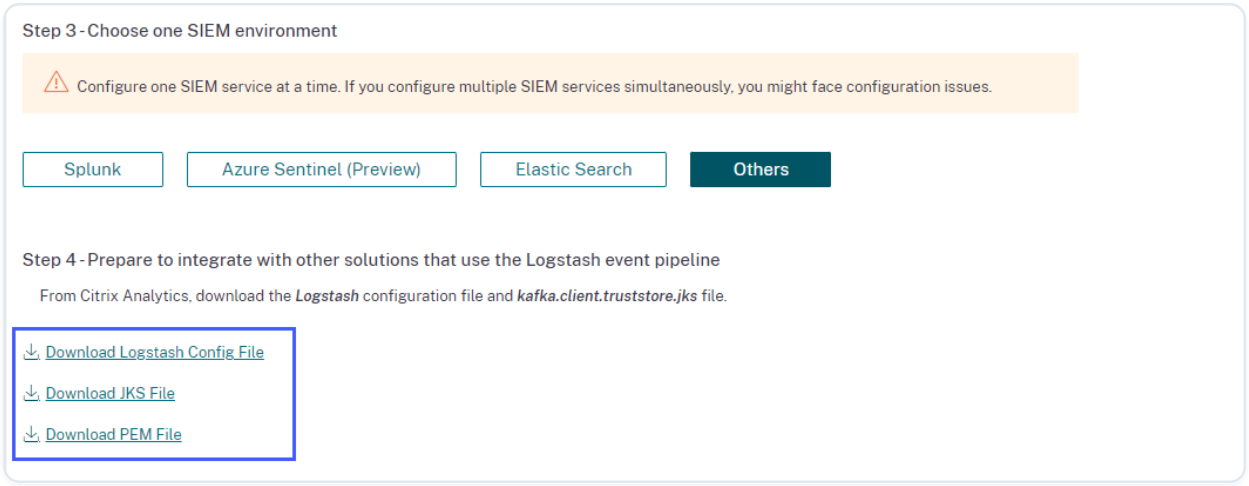


5. **Others**タブを選択して、設定ファイルをダウンロードします。

   - **Logstash設定ファイル**: 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、出力セクション）が含まれています。Logstash設定ファイルの構造については、Logstash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。Logstashを使用してSIEMを統合する場合、このファイルが必要です。
   - **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。Kafkaを使用してSIEMを統合する場合、このファイルが必要です。

   > **注**

> これらのファイルには機密情報が含まれています。安全でセキュアな場所に保管してください。



6. Logstashを構成する:

   a. LinuxまたはWindows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、指定されたディレクトリに以下のファイルを配置します。

ホストマシンの種類	ファイル名	ディレクトリパス
リナックス	CAS_Others_LogStash_Config.config	Debianおよび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および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`

ホストマシンの種類	ファイル名	ディレクトリパス
ウィンドウズ	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の認証情報、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を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。統合を保護するために、Logstashキーストアを使用して、それぞれの値を持つキーを追加し、設定ファイル内でキー名を使用して参照できます。Logstashキーストアと、それが設定のセキュリティをどのように強化するかについての追加情報については、安全な設定のためのシークレットキーストアを参照してください。

d. Logstash設定ファイルを開き、以下を実行します。

ファイルの入力セクションに、以下の情報を入力します。

- **パスワード**: 設定ファイルを準備するためにCitrix Analytics for Securityで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、ホストマシン上のkafka.client.truststore.jksファイルの場所です。

```
input {
  kafka {
    bootstrap_servers => [redacted]
    topics => [redacted]
    group_id => [redacted]
    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='[redacted]' password='<your password>';"
    ssl_truststore_location => "/etc/logstash/ssl/kafka.client.truststore.jks"
  }
```

ファイルの出力セクションで、データを送信する宛先パスまたは詳細を入力します。出力プラグインの詳細については、Logstash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. Citrix Analytics for SecurityからSIEMサービスに処理済みデータを送信するには、ホストマシンを再起動します。

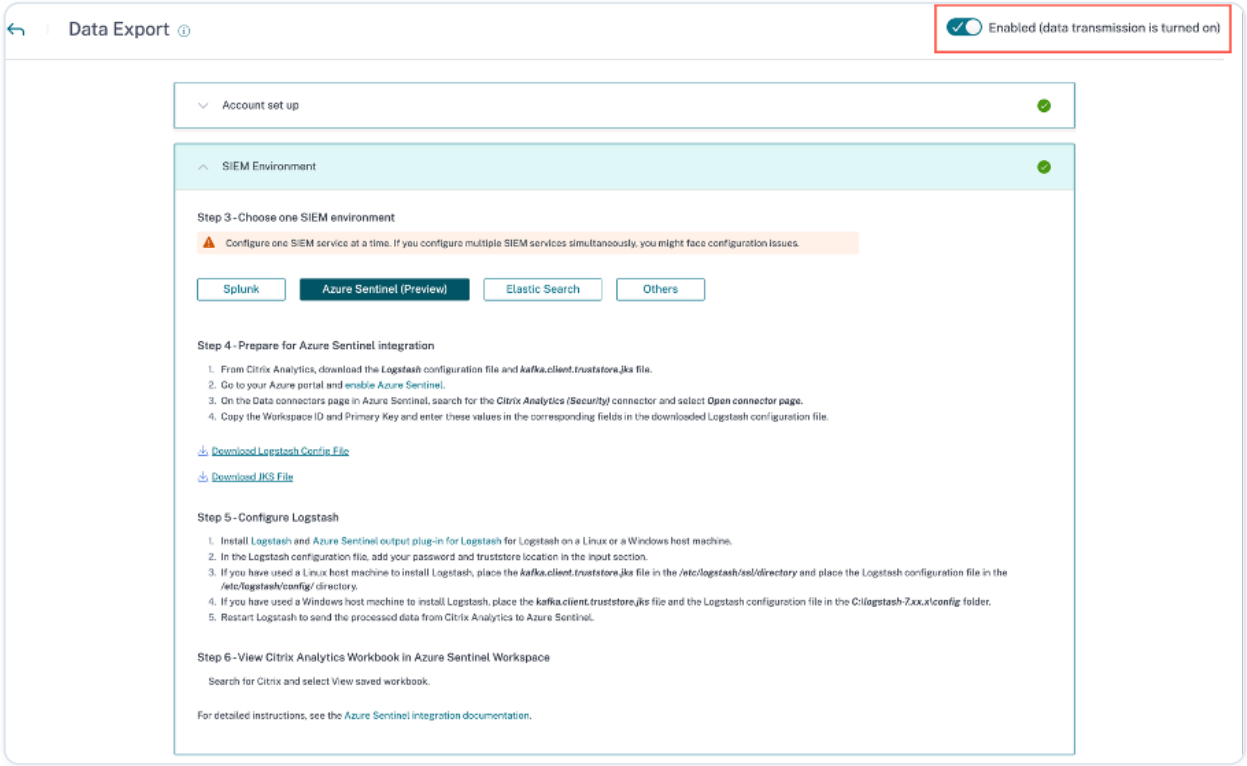
設定が完了したら、SIEMサービスにログインし、SIEMでCitrix Analyticsデータを確認します。

データ転送のオン/オフ

Citrix Analytics for Securityが設定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。

Citrix Analytics for Securityからのデータ転送を停止するには：

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。



確認のための警告ウィンドウが表示されます。**データ転送をオフにする**ボタンをクリックして、転送アクティビティを停止します。

「SIEM送信オフ警告」(/en-us/citrix-analytics/media/siem-turn-off-warning.png)

データ送信を再度有効にするには、トグルボタンをオンにします。

> **注**
>
> SIEM統合に関する支援、SIEMへのデータエクスポート、またはフィードバックの提供を要請するには、mailto:CAS-PM-Ext@cloud.comに連絡してください。

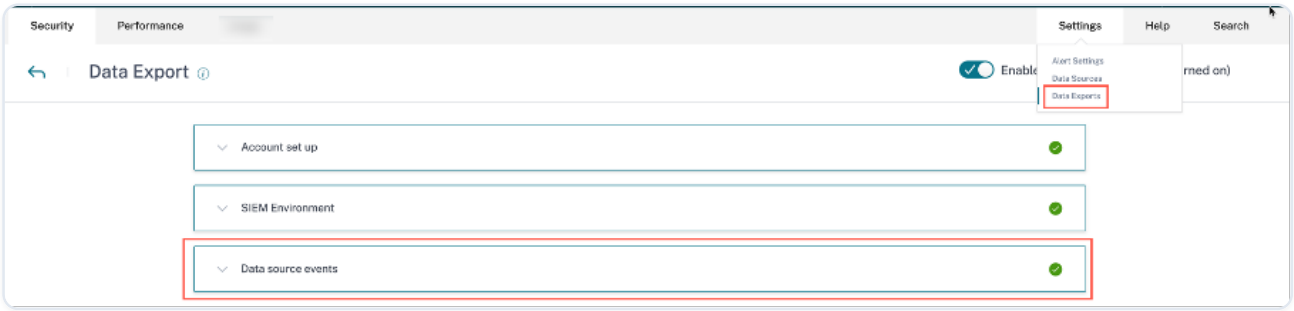
Citrix AnalyticsのSIEM向けデータエクスポート形式

Citrix Analytics for Security™ は、セキュリティ情報およびイベント管理 (SIEM) サービスとの統合を可能にします。この統合により、Citrix Analytics for Security は SIEM サービスにデータを送信し、組織のセキュリティリスク状況を把握するのに役立ちます。

現在、Citrix Analytics for Security を以下の SIEM サービスと統合できます。

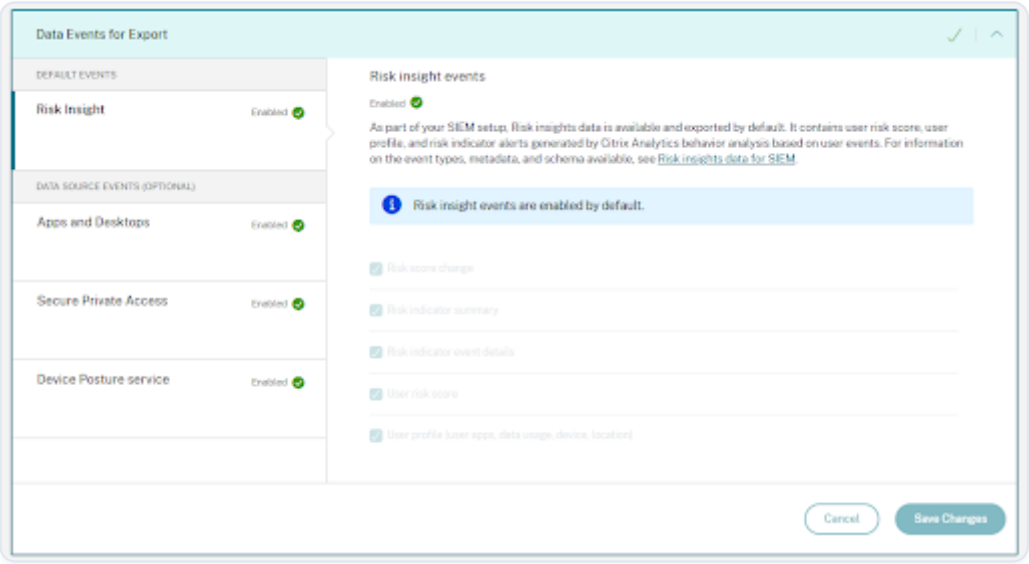
- スプランク
- マイクロソフト アジュール センチネル
- エラスティックサーチ
- KafkaまたはLogstashベースのデータコネクタを使用するその他のSIEM

データエクスポートオプションは、**設定**の下でグローバルに利用可能になりました。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 が SIEM サービスに送信するリスクインサイトデータは、次の2種類です。

- 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 (オプションエクスポート)



SIEM向けリスクインサイトデータ

アカウント設定とSIEMセットアップが完了すると、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展開に流れ込み始めます。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、およびリスクインジケーター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。

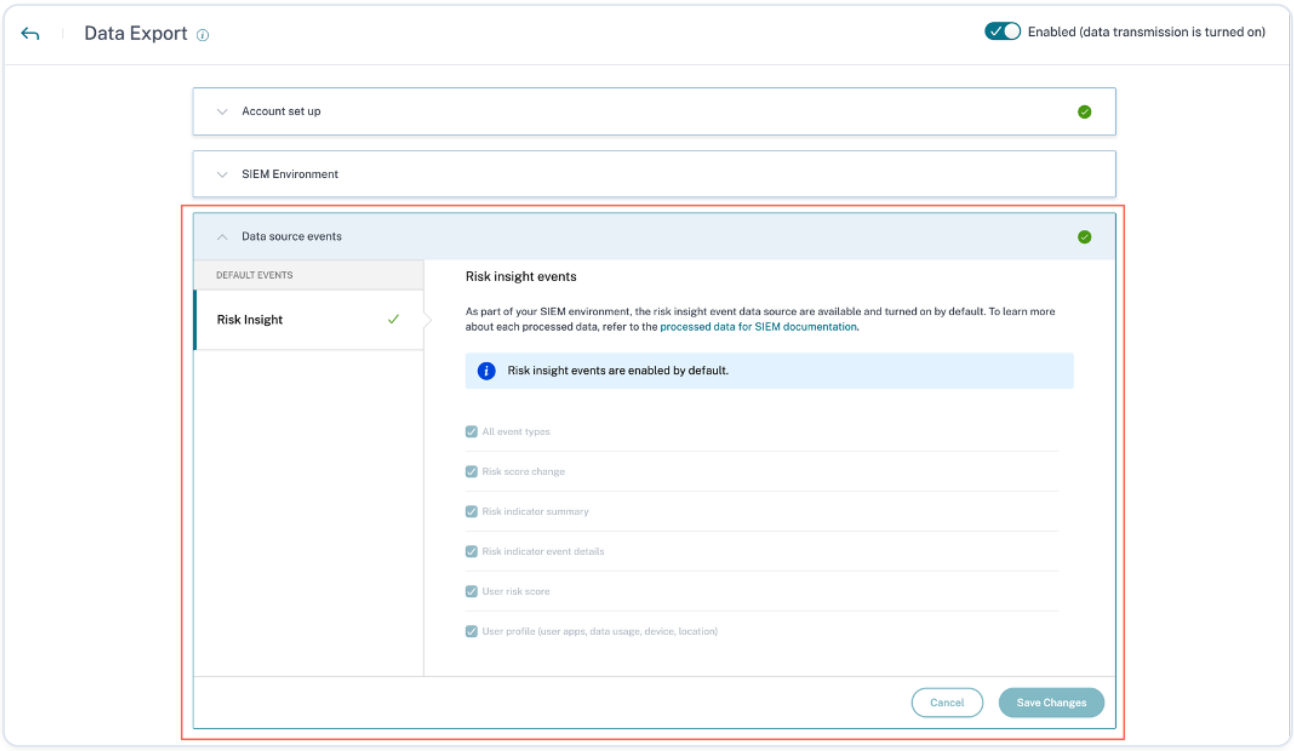
ユーザーのリスクインサイトデータセットには、以下が含まれます。

- **リスクスコアの変更**: ユーザーのリスクスコアの変更を示します。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%を超えて減少した場合、データはSIEMサービスに送信されます。
- **リスクインジケーターの概要**: ユーザーに対してトリガーされたリスクインジケーターの詳細。
- **リスクインジケーターイベントの詳細**: リスクインジケーターに関連付けられたユーザーイベント。Citrix Analyticsは、各リスクインジケーターの発生につき最大1000件のイベント詳細を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、以下に分類できます。
    - **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たデバイス。Citrix Analytics for Securityは、このデータをCitrix Virtual AppsおよびCitrix Endpoint Management™から取得し、12時間ごとにSIEMサービスに送信します。
- **ユーザーの場所**: 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™（旧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。

データソースイベントの基本設定を表示できるが構成できない場合は、必要な管理者権限がありません。 詳細については、「セキュリティ分析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済みデータのスキーマについて説明します。

注記

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、あくまでも例示目的です。実際のフィールド値は、ユーザープロファイル、ユーザーイベント、およびリスクインジケーターに基づいて異なります。

以下の表は、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のスキーマ全体で共通のフィールド名について説明しています。

フィールド名	説明
`entity_id`	エンティティに関連付けられたID。この場合、エンティティはユーザーです。
`entity_type`	リスクのあるエンティティ。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種類。例：ユーザーの場所、ユーザーのデータ使用量、またはユーザーのデバイスアクセス情報。
`tenant_id`	顧客の一意のID。
`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バージョン。現在のスキーマバージョンは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
```

```
}
```

ユーザーロケーションのフィールド説明

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種類。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都市。
`cnt`	過去12時間でそのロケーションにアクセスされた回数。

ユーザーのクライアント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
}
```

クライアントIPのフィールドの説明

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時間以内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たID。この場合、エンティティはユーザーです。
`entity_type`	リスクのあるエンティティ。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種類。例: ユーザーの場所、ユーザーのデータ使用量、またはユーザーのデバイスアクセス情報。
`tenant_id`	顧客の一意のID。
`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バージョン。現在のスキーマバージョンは2です。

ユーザーデータ使用量スキーマ


```
{

  "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

  }
```

ユーザーデータ使用量のフィールド説明

フィールド名	説明
`data_usage_bytes`	ユーザーが使用したデータ量（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合計です。
`deleted_file_cnt`	ユーザーによって削除されたファイルの数。
`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種類。この場合、イベントタイプはユーザーの使用状況プロファイルです。
`shared_file_count`	ユーザーが共有したファイルの数。
`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

  }
```


ユーザーデバイスのフィールド説明。

フィールド名	説明
`cnt`	過去12時間で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種類。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。

ユーザーアプリのスキーマ


```
{

  "tenant_id": "demo_tenant", "entity_id": "demo", "entity_type": "user",
"timestamp": "2021-02-10T21:00:00Z", "event_type": "userProfileApp",
"version": 2, "session_domain":
"99e38d488136f62f828d4823edd120b4f32d724396a7410e6dd1b0",
"user_samaccountname": "testnameeikragz779", "app": "Chromeeikragz779",
"cnt": 189

  }
```


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種類。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、LAN Managerなどの以前のバージョンのWindowsのクライアントおよびサーバーのログオン名。この名前は、Citrix StoreFrontへの

フィールド名	説明
	ログオン、およびリモートWindowsマシンへのログオンに使用されます。
`app`	ユーザーがアクセスしたアプリケーションの名前。
`cnt`	過去12時間でアプリケーションにアクセスされた回数。

ユーザーリスクスコアのスキーマ

```
{

  "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

  }
```

ユーザーリスクスコアのフィールド説明。

フィールド名	説明
`cur_riskscore`	ユーザーに割り当てられた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大度に応じて0から100まで変化します。
`event_type`	SIEMサービスに送信されるデータの種類。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。

フィールド名	説明
`timestamp`	ユーザーの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

  }
```

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

  }
```

リスクスコア変更のフィールド説明。

フィールド名	説明
`alert_message`	リスクスコア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によるものか、リスクスコアの割合の大幅な低下によるものかを示します。ユーザーのリスクスコアの変化が3以上であり、この変化がどのような割合であっても増加するか、または10%を超えて低下した場合、データはSIEMサービスに送信されます。
`alert_value`	リスクスコア変更に割り当てられた数値。リスクスコア変更は、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た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大度に応じて0から100まで変化します。
`event_type`	SIEMサービスに送信されるデータの種類です。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更です。
`timestamp`	ユーザーのリスクスコアの最新の変更が検出された日時。

リスクインジケータスキーマ

リスクインジケータスキーマは、インジケータサマリースキーマとインジケータ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。リスクインジケータに基づいて、スキーマ内のフィールドとその値がそれに応じて変化します。

次の表は、すべてのインジ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ています。

フィールド名	説明
`data source`	Citrix Analytics for Security にデータを送信する製品。例えば: Citrix Secure Private

フィールド名	説明
	Access™、Citrix Gateway、および Citrix Apps and Desktops。
`data_source_id`	データソースに関連付けられたID。ID 1 = シトリックス ゲートウェイ、ID 2 = シトリックス エンドポイント マネジメント、ID 3 = シトリックス アプリケーションズ アンド デスクトップス、ID 4 = シトリックス セキュア プライベート アクセス
`entity_type`	リスクのあるエンティティ。ユーザーである可能性があります。
`entity_id`	リスクのあるエンティティに関連付けられたID。
`event_type`	SIEMサービスに送信されるデータの種類。この場合、イベントタイプはリスクインジケーターの概要です。
`indicator_category`	リスクインジケーターのカテゴリを示します。リスクインジケーターは、侵害されたエンドポイント、侵害されたユーザー、データ漏洩、内部脅威のいずれかのリスクカテゴリにグループ化されます。
`indicator_id`	リスクインジケーターに関連付けられた一意のID。
`indicator_category_id`	リスクインジケーターカテゴリに関連付けられたID。ID 1 = データ漏洩、ID 2 = 内部脅威、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`	リスクインジケーターの名前。カスタムリスクインジケーターの場合、この名前はインジケーターの作成時に定義されます。
`indicator_type`	リスクインジケーターがデフォルト（組み込み）かカスタムかを示します。

フィールド名	説明
`indicator_uuid`	リスクインジケーターインスタンスに関連付けられた一意のID。
`indicator_vector_name`	リスクインジケーター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インジケーター、場所ベースのリスクインジケーター、ログオン失敗ベースのリスクインジケーター、IPベースのリスクインジケーター、データベースのリスクインジケーター、ファイルベースのリスクインジケーター、およびその他のリスクインジケーターです。
`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インジケーター、ID 2 = 場所ベースのリスクインジケーター、ID 3 = ログオン失敗ベースのリスクインジケーター、ID 4 = IPベースのリスクインジケーター、ID 5 = データベースのリスクインジケーター、ID 6 = ファイルベースのリスクインジケーター、ID 7 = その他のリスクインジケーター、ID 999 = 利用不可。
`occurrence_details`	リスクインジケーター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。カスタムリスクインジケーターの場合、ポリシーベースのインジケーターであるため、risk_probabilityは常に1.0です。
`severity`	リスクの重大度を示します。低、中、高のいずれかです。
`tenant_id`	顧客の一意のID。
`timestamp`	リスクインジケーターがトリガーされた日付と時刻。

フィールド名	説明
`ui_link`	Citrix Analyticsユーザーインターフェイス上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する時刻からタイムスタンプまでの時間。この期間中に異常な動作が検出された場合、リスクインジケーターがトリガーされます。

次の表は、すべてのインジケーターイベント詳細スキーマに共通するフィールド名について説明しています。

フィールド名	説明
`data_source_id`	データソースに割り当てられているIDです。ID 1 は Citrix Gateway、ID 2 は Citrix Endpoint Management、ID 3 は Citrix Apps and Desktops、ID 4 は Citrix Secure Private Access です。
`indicator_category_id`	リスクインジケーターカテゴリに関連付けられたID。ID 1 = データ持ち出し、ID 2 = 内部脅威、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たID。
`entity_type`	リスクのあるエンティティ。ユーザーである可能性があります。
`event_type`	SIEMサービスに送信されるデータの種類。この場合、イベントタイプはリスクインジケーターイベントの詳細です。
`indicator_id`	リスクインジケーターに関連付けられた一意のID。
`indicator_uuid`	リスクインジケーターインスタンスに関連付けられた一意のID。

フィールド名	説明
`indicator_vector_name`	リスクインジケーター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インジケーター、場所ベースのリスクインジケーター、ログオン失敗ベースのリスクインジケーター、IPベースのリスクインジケーター、データベースのリスクインジケーター、ファイルベースのリスクインジケーター、およびその他のリスクインジケーターです。
`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インジケーター、ID 2 = 場所ベースのリスクインジケーター、ID 3 = ログオン失敗ベースのリスクインジケーター、ID 4 = IPベースのリスクインジケーター、ID 5 = データベースのリスクインジケーター、ID 6 = ファイルベースのリスクインジケーター、ID 7 = その他のリスクインジケーター、および ID 999 = 利用不可
`tenant_id`	顧客の一意のID。
`timestamp`	リスクインジケーターがトリガーされた日付と時刻。
`version`	処理されたデータのスキーマバージョン。現在のスキーマバージョンは2です。
`client_ip`	ユーザーデバイスのIPアドレス。

注

- 整数データ型のフィールド値が利用できない場合、割り当てられる値は-999です。例えば、`"latitude": -999`、`"longitude": -999`。
- 文字列データ型のフィールド値が利用できない場合、割り当てられる値はNAです。例えば、`"city": "NA"`、`"region": "NA"`。

Citrix Secure Private Accessリスクインジケータースキーマ

ブラックリストに登録されたURLへのアクセス試行リスクインジケータースキーマ

インジケーターサマリースキーマ


```
{
  "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": {
    "observation_start_time": "2018-03-15T10:44:59Z",
    "relevant_event_type": "Blacklisted External Resource Access"
  }
}
```

インジケーターイベント詳細スキーマ

```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 401,
  "indicator_uuid": "c421f3f8-33d8-59b9-ad47-715b9d4f65f4",
  "indicator_category_id": 2,
  "indicator_vector": {
    "name": "Other Risk Indicators",
    "id": 7 },
  "data_source_id": 4,
  "timestamp": "2018-03-15T10:57:21Z",
  "event_type": "indicatorEventDetails",
```

```
  "entity_type": "user",

  "entity_id": "demo_user",

  "version": 2,

  "domain_name": "googleads.g.doubleclick.net",

  "executed_action": "blocked",

  "reason_for_action": "URL Category match",

  "client_ip": "157.xx.xxx.xxx"

}
```

次の表は、ブラックリストに登録されたURLへのアクセス試行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について説明しています。

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た時刻からタイムスタンプまでの時間。この期間中に異常な動作が検出された場合、リスクインジケーターがトリガーされます。
`executed_action`	ブラックリストに登録されたURLに適用されたアクション。アクションには「許可」と「ブロック」が含まれます。
`reason_for_action`	URLにアクションを適用する理由。

過剰なデータダウンロードのリスクインジケーターのスキーマ

インジケーターの概要スキーマ

```
{
```

```
"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"

  }

}
```

インジケーターイベントの詳細スキーマ

```
{

  "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

}
```


次の表は、過剰なデータダウンロード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ています。

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た時刻からタイムスタンプまでの時間。この期間中に異常な動作が検出された場合、リスクインジケーターがトリガーされます。
`data_volume_in_bytes`	ダウンロードされたデータのバイト単位の量。
`relevant_event_type`	ユーザーイベントのタイプを示します。
`domain_name`	データがダウンロードされたドメインの名前。
`downloaded_bytes`	ダウンロードされたデータの量（バイト単位）。

不審なアップロード量リスクインジケーターのスキーマ

インジケーターサマリーのスキーマ


```
{

  "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"

}
```

```
}
```

インジケーターイベント詳細のスキーマ

```
{
  "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
}
```

次の表は、不審なアップロード量に関する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について説明しています。

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た時刻からタイムスタンプまでの時間。この期間中に異常な動作が検出された場合、リスクインジケーターがトリガーされます。
`data_volume_in_bytes`	アップロードされたデータの量（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バイト単位の量。

Citrix Endpoint Management リスクインジケータースキーマ

ジェイルブレイクまたはルート化されたデバイス検出インジケータースキーマ

インジケーターサマリースキーマ

```
{
  "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
}
```


インジケーター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
}
```


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

インジケーターサマリースキーマ


```
{
  "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
}
```


インジケーター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
}
```


管理対象外デバイスが検出されました

インジケーターサマリースキーマ


```
{
  "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
}
```


インジケーター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
}
```


Citrix Gatewayリスクインジケーターのスキーマ

EPAスキャン失敗リスクインジケーターのスキーマ

インジケーターサマリーのスキーマ


```
{
  "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"
  }
}
```

インジケーター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",
  "country": "United States",
```

```
  "city": "San Jose",
  "region": "California",
  "cs_vserver_name": "demo_vserver",
  "device_os": "Windows OS",
  "security_expression": "CLIENT.OS(Win12) EXISTS",
  "vpn_vserver_name": "demo_vpn_vserver",
  "vserver_fqdn": "10.xxx.xx.xx"
}
```


この表は、EPAスキャン失敗リスクインジケーター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説明しています。

フィールド名	説明
`event_description`	認証後の失敗や隔離グループなしなど、EPAスキャン失敗の理由を説明します。
`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`	Citrix Gatewayのドメイン名。
`gateway_ip`	Citrix Gateway の IP アドレス。
`policy_name`	Citrix Gateway で構成されている 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都市。
`region`	ユーザーアクティビティが検出された地域。
`cs_vserver_name`	コンテンツスイッチ仮想サーバーの名前。

フィールド名	説明
`device_os`	ユーザーデバイスのオペレーティングシステム。
`security_expression`	Citrix Gateway で構成されているセキュリティ式。
`vpn_vserver_name`	Citrix Gateway仮想サーバーの名前。
`vserver_fqdn`	Citrix 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

```
{

  "tenant_id": "demo_tenant",

  "indicator_id": 101,

  "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"
  }
}
```

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
}
```

次の表は、過剰な認証失敗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について説明しています。

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種類を示します。
`event_description`	パスワードの誤りなど、過剰な認証失敗イベントの理由を説明します。
`authentication_stage`	認証ステージがプライマリ、セカンダリ、またはターシャリのいずれであるかを示します。
`authentication_type`	LDAP、ローカル、OAuthなどの認証タイプを示します。
`auth_server_ip`	認証サーバーのIPアドレス。
`gateway_domain_name`	Citrix Gatewayのドメイン名。
`gateway_ip`	Citrix GatewayのIPアドレス。
`cs_vserver_name`	コンテンツスイッチ仮想サーバーの名前。
`vpn_vserver_name`	Citrix Gateway仮想サーバーの名前。
`vserver_fqdn`	Citrix 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都市。
`region`	ユーザーアクティビティが検出された地域。

不可能な移動リスクインジケーター

インジケーターサマリースキーマ

```
{
  "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

  }

}
```


インジケーター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": {
    "name": "Location-Based Risk Indicators",
    "id": 2
  },
  "data_source_id": 1,
  "timestamp": "2020-06-06T05:05:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "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_os": "Linux OS",
  "device_browser": "Chrome 62.0.3202.94"
}
```

次の表は、不可能な移動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について説明しています。

フィールド名	説明
`distance`	不可能な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がアクセスされた回数。
`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種類を示します。
`observation_start_time`	Citrix Analyticsがユーザーアクティビティの監視を開始した時刻からタイムスタンプまでの時間。この期間中に異常な動作が検出された場合、リスクインジケーター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都市。
`region`	ユーザーがログオンした地域を示します。
`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`	ユーザーが使用したWebブラウザ。
`device_os`	ユーザー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アドレスの登録組織
`ip_routing_type`	クライアントIPルーティングタイプ

不審なIPからのログオンリスクインジケータースキーマ

インジケーターサマリースキーマ

```
{
  "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"
  }
}
```


インジケーター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"
}
```


以下の表は、サマリースキーマと、疑わしいIPからのログイン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た理由。
`webroot_reputation`	脅威インテリジェンスプロバイダーであるWebrootが提供するIPレピュテーションインデックス。

フィールド名	説明
`webroot_threat_categories`	脅威インテリジェンスプロバイダーであるWebrootによって、疑わしいIPに対して識別された脅威カテゴリ。
`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`	使用された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都市。
`region`	ユーザーアクティビティが検出された地域。

不審な認証失敗リスクインジケーターのスキーマ

インジケーターサマリーのスキーマ


```
{
  "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"
  }
}
```


インジケーターイベント詳細のスキーマ


```
{
  "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"
}
```

次の表は、不審な認証失敗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について説明しています。

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種類を示します。
`event_description`	ログオンが成功したか失敗したかを示します
`authentication_stage`	認証段階がプライマリ、セカンダリ、またはターシャリのいずれであるかを示します。
`authentication_type`	LDAP、ローカル、OAuthなどの認証の種類を示します。
`is_risky`	ログオンが成功した場合、is_risky の値は false です。ログオンが失敗した場合、is_risky の値は true です。
`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都市。
`region`	ユーザーアクティビティが検出された地域。

不審なログオンのリスクインジケーター

インジケーターの概要スキーマ

```
{

  "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
  }
}
```

インジケーターイベントの詳細スキーマ

```
{
  "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",
  "device_os": "Windows OS",
  "device_id": "NA",
  "client_ip": "99.xxx.xx.xx"
}
```

次の表は、不審なログオン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ています。

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がアクセスされた回数。
`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種類を示します。
`observation_start_time`	Citrix Analyticsがユーザーアクティビティの監視を開始した時刻からタイムスタンプまでの時間。この期間中に異常な動作が検出された場合、リスクインジケーターがトリガーされます。
`occurrence_event_type`	ユーザーイベントのタイプ（アカウントログオンなど）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都市。
`region`	ユーザーがログオンした地域を示します。
`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`	ユーザーが使用した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`	ユーザーが使用したデバイスの名前。

フィールド名	説明
`user_location_risk`	ユーザーがログオンした場所の疑わしさのレベルを示します。低い疑わしさのレベル: 0〜69、中程度の疑わしさのレベル: 70〜89、高い疑わしさのレベル: 90〜100
`user_device_risk`	ユーザーがログオンしたデバイスの疑わしさのレベルを示します。低い疑わしさのレベル: 0〜69、中程度の疑わしさのレベル: 70〜89、高い疑わしさのレベル: 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わしさのレベルを示します。低い疑わしさのレベル: 0〜69、中程度の疑わしさのレベル: 70〜89、高い疑わしさのレベル: 90〜100
`suspicious_network_risk`	Webroot IP脅威インテリジェンスフィードに基づいたIP脅威レベルを示します。低い脅威レベル: 0〜69、中程度の脅威レベル: 70〜89、高い脅威レベル: 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たIPアドレスから検出された脅威の種類を示します。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、スキャナー、サービス拒否、レピュテーション、フィッシング、プロキシ、未指定、モバイル脅威、Torプロキシがあります。

Citrix DaaSおよびCitrix Virtual Apps and Desktopsのリスクインジケータースキーマ

不可能な移動のリスクインジケーター

インジケーター概要スキーマ

```
{

  "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

  }

}
```


インジケーター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"
}
```


次の表は、サマリースキーマと、不可能移動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ています。

フィールド名	説明
`distance`	不可能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がアクセスされた回数。
`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種類を示します。
`observation_start_time`	Citrix Analyticsがユーザーアクティビティの監視を開始した時刻からタイムスタンプまでの時間。この期間中に異常な動作が検出された場合、リスクインジケーター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都市。
`region`	ユーザーがログオンした地域を示します。
`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`	ユーザーが使用した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`	ユーザーが使用したデバイスの名前。
`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™の種類。
`ip_organization`	クライアントIPアドレスの登録組織

フィールド名	説明
`ip_routing_type`	クライアントIPルーティングタイプ

潜在的なデータ持ち出しリスクインジケーター

インジケーターサマリースキーマ

```
{
  "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
  }
}
```


インジケーター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"
}
```


次の表は、潜在的なデータ持ち出し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について説明しています。

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た時刻からタイムスタンプまでの時間。この期間中に異常な動作が検出された場合、リスクインジケーター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。

フィールド名	説明
`exfil_data_volume_in_bytes`	データ漏洩の量。
`occurrence_event_type`	SaaSアプリでのクリップボード操作など、データ漏洩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`	ファイルの種類。
`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。
`app_url`	ユーザーがアクセスしたアプリケーションのURL。
`entity_time_zone`	ユーザーのタイムゾーン。

不審なログオンリスクインジケーターのスキーマ

インジケーターの概要スキーマ

```
{

  "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
  }
}
```

インジケーターイベントの詳細スキーマ

```
{
  "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"

}
```

次の表は、不審なログオン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ています。

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がアクセスされた回数。
`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種類を示します。
`observation_start_time`	Citrix Analyticsがユーザーアクティビティの監視を開始した時刻からタイムスタンプまでの時間。この期間中に異常な動作が検出された場合、リスクインジケーター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の種類を示します。
`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都市。
`region`	ユーザーがログオンした地域を示します。
`latitude`	ユーザーがログオンした場所の緯度を示します。

フィールド名	説明
`longitude`	ユーザーがログオンした場所の経度を示します。
`browser`	ユーザーが使用したWebブラウザ。
`os`	ユーザーデバイスのオペレーティングシステム。
`device_id`	ユーザーが使用しているデバイスの名前。
`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のタイプ。
`user_location_risk`	ユーザーがログオンした場所の疑わしさのレベルを示します。疑わしさのレベル（低）：0～69、疑わしさのレベル（中）：70～89、疑わしさのレベル（高）：90～100
`user_device_risk`	ユーザーがログオンしたデバイスの疑わしさのレベルを示します。疑わしさのレベル（低）：0～69、疑わしさのレベル（中）：70～89、疑わしさのレベル（高）：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わしさのレベルを示します。疑わしさのレベル（低）：0～69、疑わしさのレベル（中）：70～89、疑わしさのレベル（高）：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。脅威レベル（低）：0～69、脅威レベル（中）：70～89、脅威レベル（高）：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種類を示します。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、スキャナー、サービス拒否、レピュテーション、フィッシング、プロキシ、

フィールド名	説明
	未指定、モバイル脅威、Torプロキシがあります。

Microsoft Active Directoryインジケーター

インジケーターサマリーのスキーマ


```
{
  "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
}
```


インジケーターイベント詳細のスキーマ


```
{
  "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
}
```


カスタムリスクインジケーターのスキーマ

以下のセクションでは、カスタムリスクインジケーター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のカスタムリスクインジケーターに関連するデータをSIEMサービスに送信しています。

次の表は、カスタムリスクインジケーターサマリーのスキーマのフィールド名を示しています。

フィールド名	説明
`data source`	Citrix Analytics for Security にデータを送信する製品です。例として、Citrix Secure Private Access、Citrix Gateway、および Citrix Apps and Desktops などがあります。
`data_source_id`	データソースに関連付けられているID。ID 1 = シトリックス ゲートウェイ、ID 2 = シトリックス エンドポイント マネジメント、ID 3 = シトリックス アプリケーションズ アンド デスクトップス、ID 4 = シトリックス セキュア プライベート アクセス
`entity_id`	リスクのあるエンティティに関連付けられたID。
`entity_type`	リスクのあるエンティティ。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種類。この場合、イベントタイプはリスクインジケーターの概要です。
`indicator_category`	リスクインジケーターのカテゴリを示します。リスクインジケーターは、侵害されたエンドポイント、侵害されたユーザー、データ漏洩、または内部脅威のいずれかのリスクカテゴリに分類されます。
`indicator_id`	リスクインジケーターに関連付けられた一意のID。

フィールド名	説明
`indicator_category_id`	リスクインジケーターカテゴリに関連付けられたID。ID 1 = データ漏洩、ID 2 = 内部脅威、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`	リスクインジケーターの名前。カスタムリスクインジケーターの場合、この名前はインジケーターの作成時に定義されます。
`indicator_type`	リスクインジケーターがデフォルト（組み込み）かカスタムかを示します。
`indicator_uuid`	リスクインジケーターインスタンスに関連付けられた一意のID。
`occurrence_details`	リスクインジケーターのトリガー条件に関する詳細。
`pre_configured`	カスタムリスクインジケーターが事前設定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。カスタムリスクインジケーターの場合、ポリシーベースのインジケーターであるため、risk_probabilityは常に1.0です。
`severity`	リスクの重大度を示します。低、中、高のいずれかです。
`tenant_id`	顧客の一意のID。
`timestamp`	リスクインジケーターがトリガーされた日時。
`ui_link`	Citrix Analyticsユーザーインターフェース上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バージョン。現在のスキーマバージョンは2です。

次の表は、カスタムリスクインジケーターイベント詳細スキーマ全体で共通のフィールド名について説明しています。

フィールド名	説明
`data_source_id`	データソースに関連付けられているID。ID 1 = シトリックス ゲートウェイ、ID 2 = シトリックス エンドポイント マネジメント、ID 3 = シトリックス アプリケーションズ アンド デスクトップス、ID 4 = シトリックス セキュア プライベート アクセス
`indicator_category_id`	リスクインジケーターカテゴリに関連付けられたID。ID 1 = データ持ち出し、ID 2 = 内部脅威、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種類。この場合、イベントタイプはリスクインジケーターイベントの詳細です。
`tenant_id`	顧客の一意のID。
`entity_id`	リスクのあるエンティティに関連付けられたID。
`entity_type`	リスクのあるエンティティ。この場合はユーザーです。
`indicator_id`	リスクインジケーターに関連付けられた一意のID。
`indicator_uuid`	リスクインジケーターインスタンスに関連付けられた一意のID。
`timestamp`	リスクインジケーターがトリガーされた日付と時刻。
`version`	処理されたデータのスキーマバージョン。現在のスキーマバージョンは2です。
`event_id`	ユーザーイベントに関連付けられたID。

フィールド名	説明
`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のユーザーイベントのタイプを示します。
`product`	Windows用Citrix Workspaceアプリなど、Citrix Workspaceアプリのタイプを示します。
`client_ip`	ユーザーデバイスのIPアドレス。
`session_user_name`	Citrix Apps and Desktopsセッションに関連付けられているユーザー名。
`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`	ユーザーが使用したデバイスの名前。
`os_name`	ユーザー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。詳細については、「Apps and Desktopsのセルフサービス検索」を参照してください。
`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。
`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付けられている追加の詳細です。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。

Citrix DaaSおよびCitrix Virtual Apps and Desktopsのカスタムリスクインジケーター

インジケーターサマリースキーマ


```
{
  "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

}
```

セッションログオンイベントのインジケーター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",
}
```


次の表は、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について説明しています。

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`	サーバー名。
`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ー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",

}
```

次の表は、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について説明しています。

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ー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",

}
```


次の表は、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ています。

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ー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",

}
```

次の表は、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について説明しています。

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`	アクティブセッションのGUID。

アプリ起動イベントのインジケーター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.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"
}
```

次の表は、アプリ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について説明しています。

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ー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"
}
```


次の表は、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について説明しています。

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。

ファイルダウンロードイベントのインジケーター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": "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"
}
```


次の表は、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について説明しています。

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`	サーバー名。
`session_guid`	アクティブセッションのGUID。
`device_type`	ファイルがダウンロードされたデバイスの種類を示します。

印刷イベントのインジケーター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"
}
```


次の表は、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について説明しています。

フィールド名	説明
`printer_name`	印刷ジョブに使用されたプリンターの名前。
`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ーなどの印刷ジョブのサイズ。
`job_details_filename`	印刷されたファイルの名前。
`job_details_format`	印刷ジョブの形式。

アプリSAAS起動イベントのインジケーター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",

}
```


次の表は、アプリ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について説明しています。

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SAAS終了イベントのインジケーター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",
}
```

次の表は、アプリ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ています。

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が有効な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利用可能な未処理のリアルタイムユーザーおよび製品使用状況データです。これらのイベントに含まれるメタデータは、より深い脅威分析、新しいダッシュボードの作成、およびセキュリティとITインフラ全体での他のCitrix以外のデータソースイベントとの関連付けにさらに使用できます。

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に送信します。

データソースイベントのスキーマ詳細

シトリックス バーチャルアプリおよびデスクトップ イベント

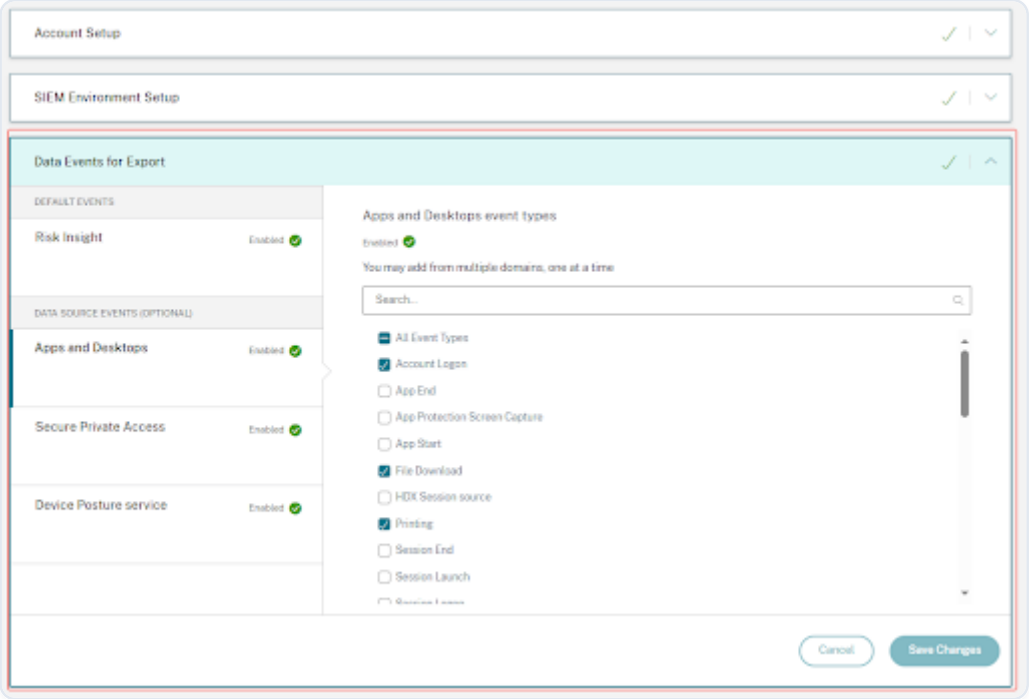
ユーザーが仮想アプリまたは仮想デスクトップを使用すると、ユーザーイベントはCitrix Analytics for Securityでリアルタイムに受信されます。詳細については、「Citrix Virtual Apps and Desktops およびCitrix DaaSデータソース」を参照してください。SIEMでCitrix Virtual Apps and Desktopsに関連付けられている次のユーザーイベントを表示できます。

- 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)
- 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)
- 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になっていてSIEMに流れているかを確認できます。テナントに適用可能なイベントタイプを設定または削除し、 ボタンをクリックして設定を保存できます。

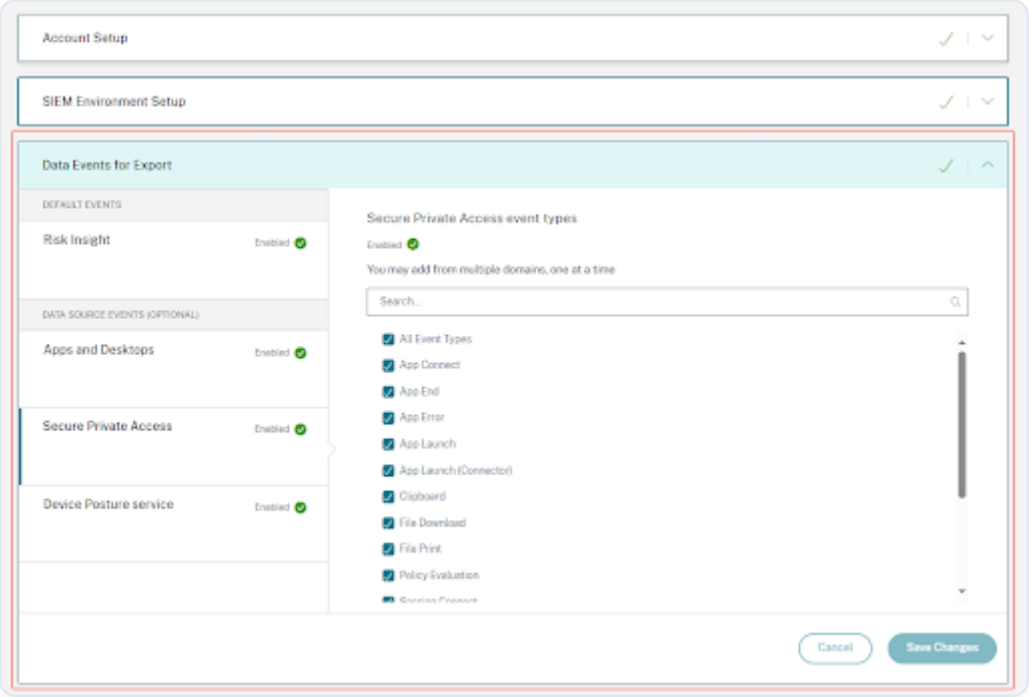


Secure Private Accessイベント

ユーザーイベントは、ユーザーがCitrix Workspace App、Citrix Secure Accessクライアント、またはCitrix Enterprise BrowserなどのCitrix Secure Private Accessを介してアプリケーションにアクセスすると、Citrix Analytics for Securityでリアルタイムに受信されます。SIEMでSecure Private Accessに関連する以下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 (接続、起動、終了、エラー)
- ファイル (印刷、ダウンロード)
- ポリシー評価
- クリップボード

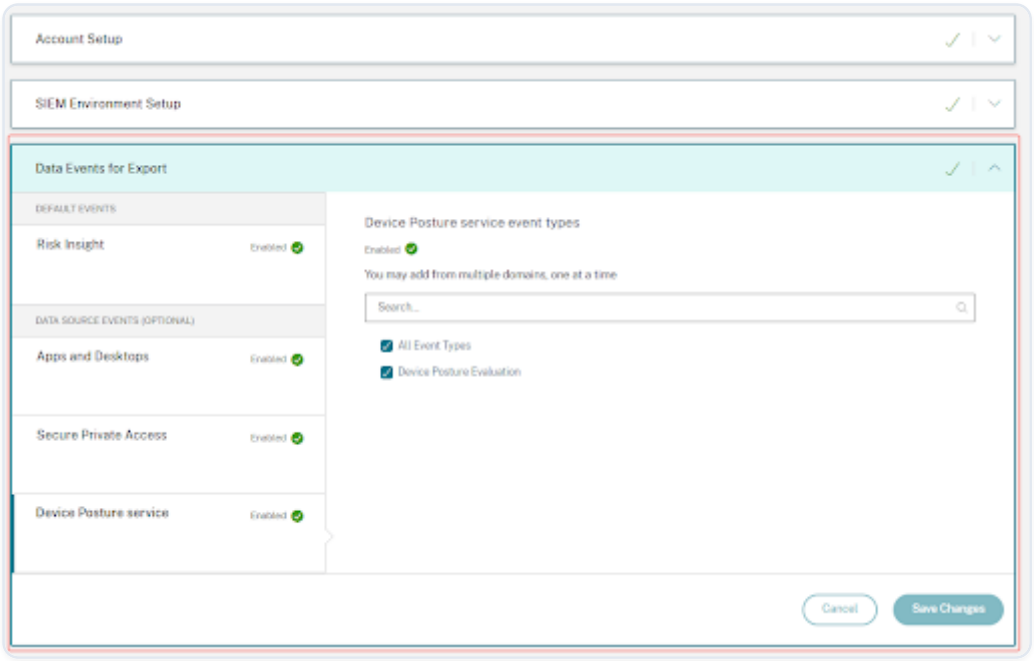
- セッション (接続、起動)
- URL
- ユーザーログイン
- SPAサービスログ



デバイスポスチャサービスイベント

ユーザーイベントは、Citrix Endpoint Analysis (EPA) クライアントがCitrix Virtual Apps and DesktopsまたはCitrix Secure Private Accessリソースへのアクセスを試みるデバイスに対してポスチャチェックを実行したときに生成されます。SIEMでデバイスポスチャサービスに関連する以下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
- デバイスポスチャ評価



テナントで有効になっているイベントタイプを確認し、それらがSIEMに流れていることを確認できます。該当す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適用できます。

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

この記事では、顧客の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関係について説明します。これを明確にするために、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シナリオの例を見てみましょう。以下の方法で、これらの属性をユーザーと関連付ける方法について説明します。

- カスタムリスクインジケーターのインサイトを使用する
- データソースイベントを使用する

以下の例では、SplunkがSIEM環境として紹介されています。同様のデータ相関は、Citrix AnalyticsによるワークブックテンプレートをSentinelでも実行できます。詳細については、Citrix Analytics workbook for Microsoft Sentinelを参照してください。

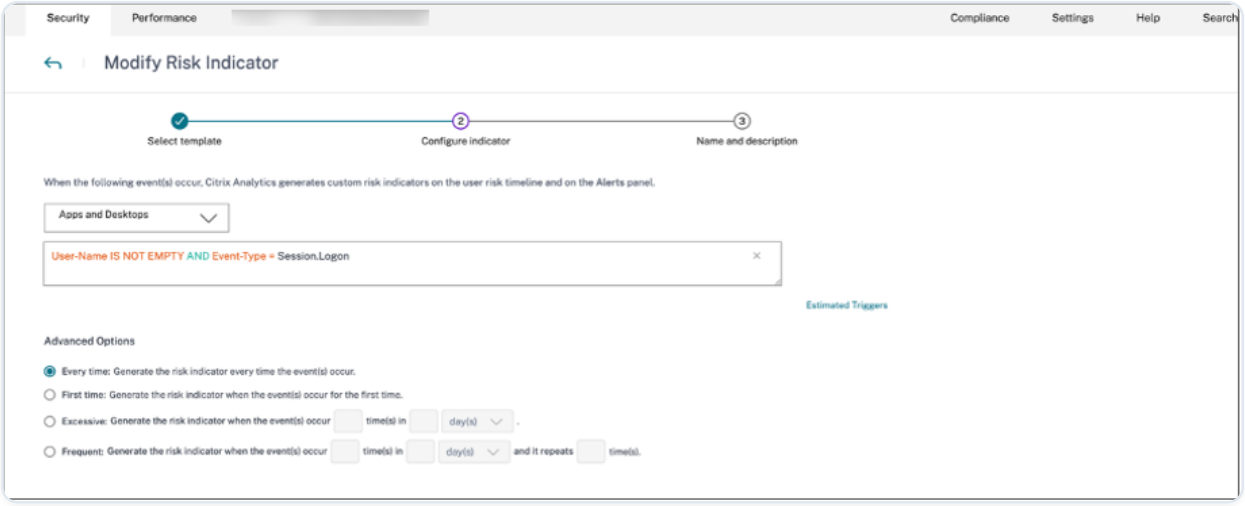
カスタムリスクインジケーターのインサイト

Citrix Analytics data exports format for SIEMで述べられているように、インジケーターの概要とイベント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の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の有無にかか

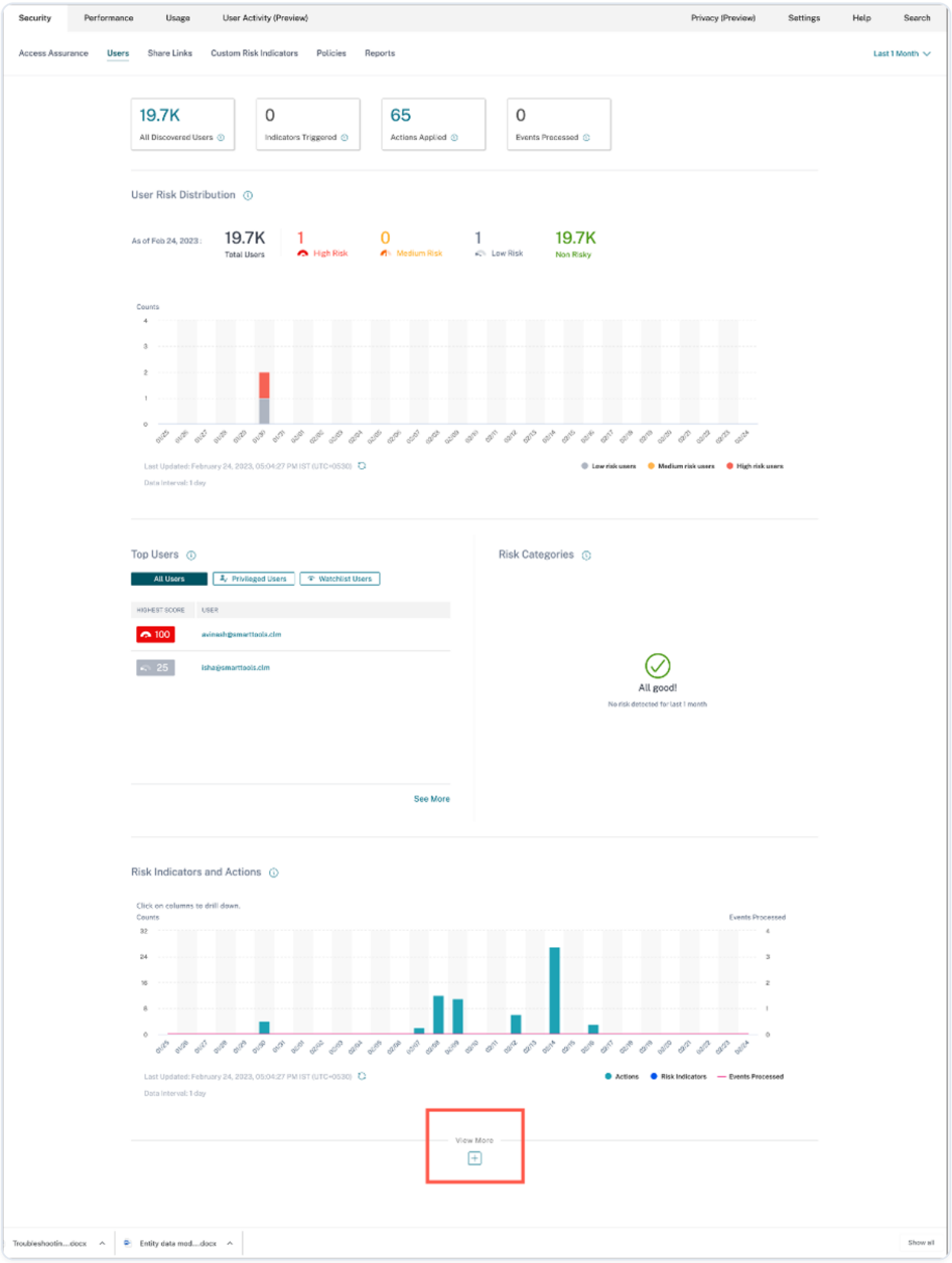
わらずカスタムインジケーターを設定した場合、これらのデータポイントはSplunk環境に流れ込みます。

Citrix Analyticsでのカスタムリスクインジケーターの設定

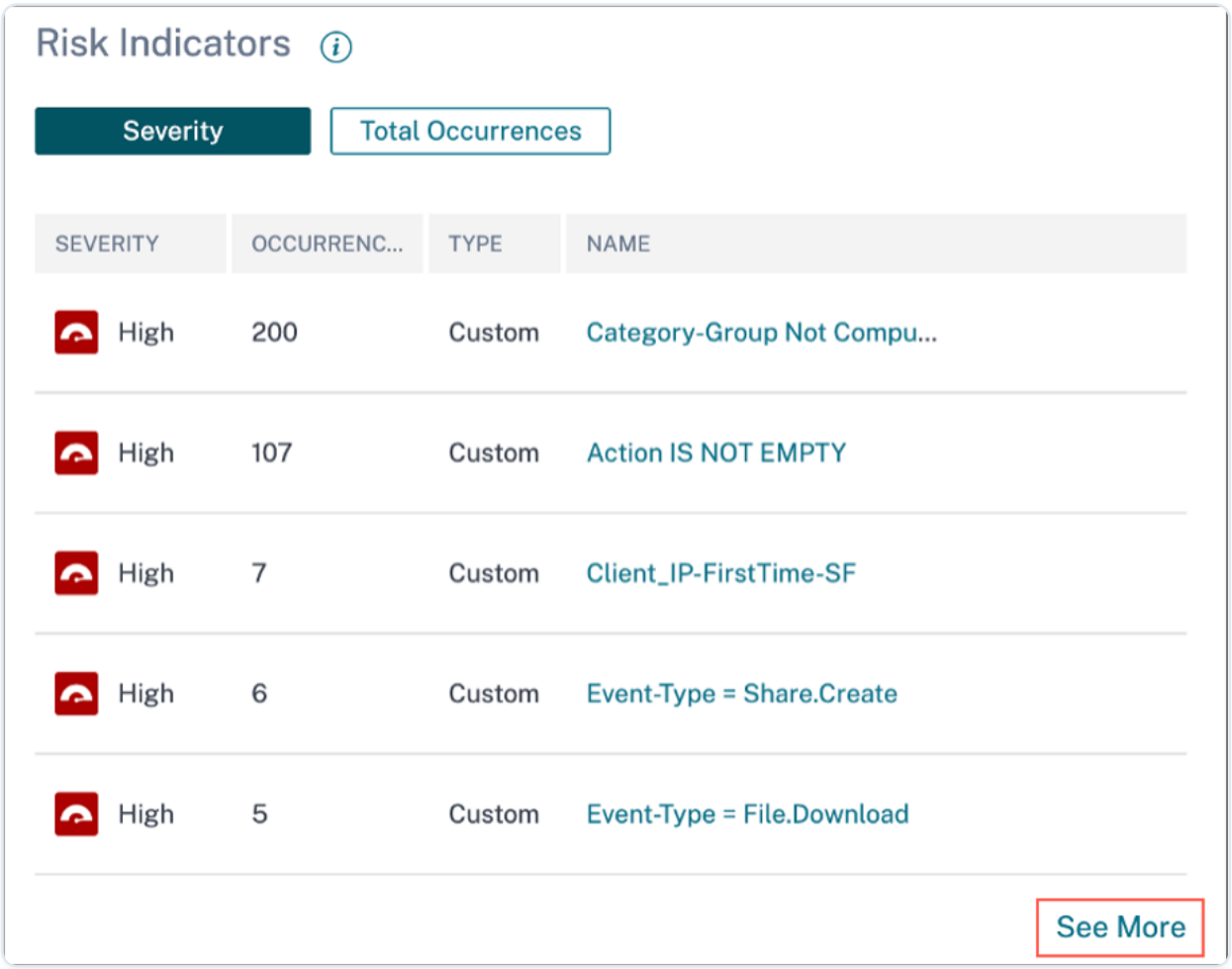
1. **Citrix Analytics for Security™ダッシュボード > カスタムリスクインジケーター > インジケーターの作成**に移動します。ユーザーの行動を監視するのに役立つ任意の条件でカスタムリスクインジケーターを作成できます。カスタムインジケーターを設定すると、関連する条件をトリガーしたすべてのユーザーがSplunk環境に表示されます。



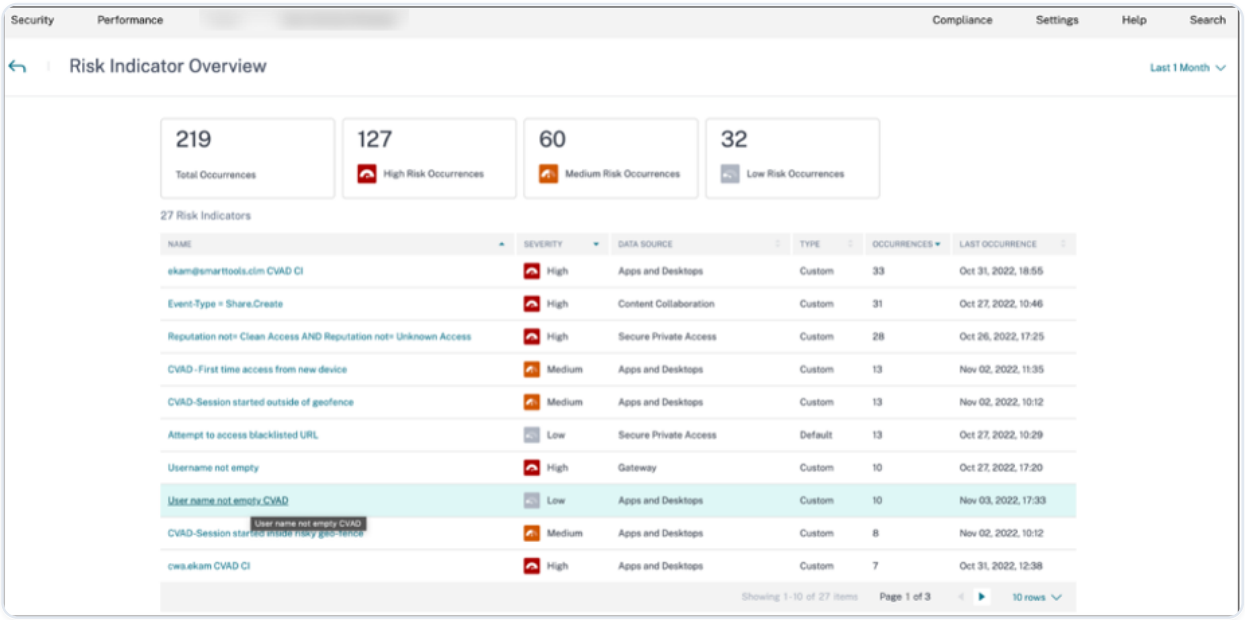
2. Citrix Analytics for Securityで作成されたリスクインジケーターの発生状況を表示するには、**セキュリティ > ユーザー**に移動します。ページの下部に移動し、プラス (+) アイコンをクリックします。



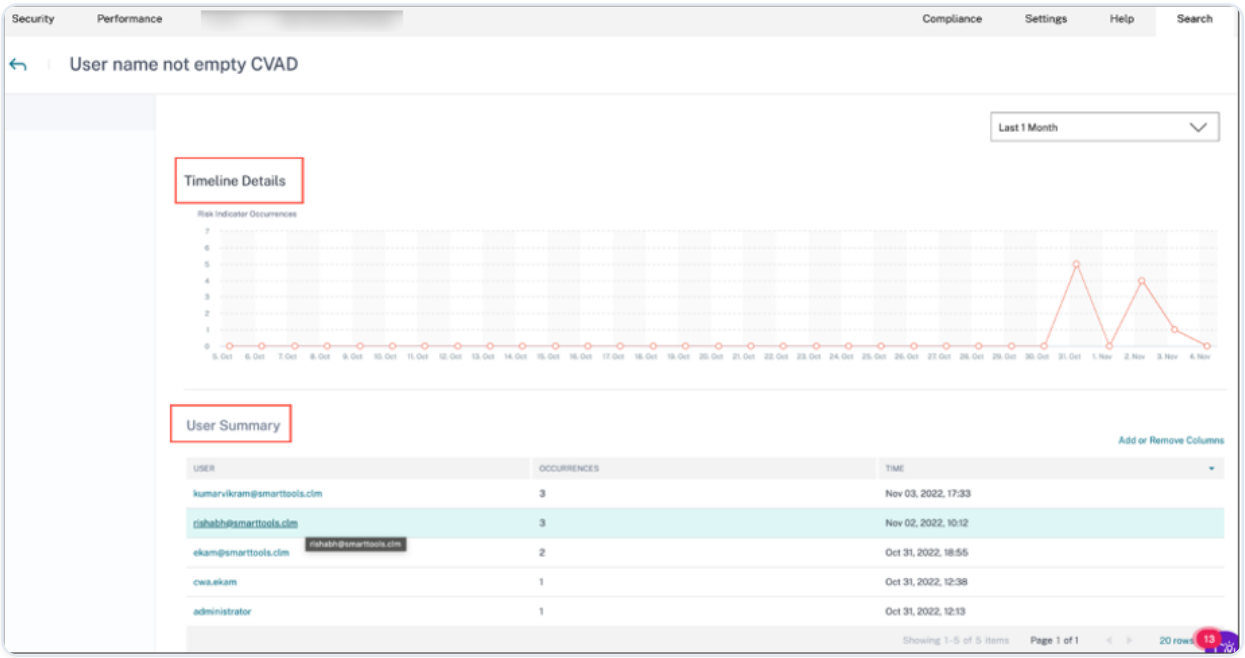
リスクインジケーターカードが表示されます。リスクインジケーター、重大度、および発生状況の詳細を表示できます。



3. **詳細を見る**をクリックします。リスクインジケーターの**概要**ページが表示されます。



「リスクインジケーターの概要」ページでは、インジケーター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サマリーで確認できます。タイムラインの詳細については、「ユーザーリスクのタイムラインとプロファイル」を参照してください。

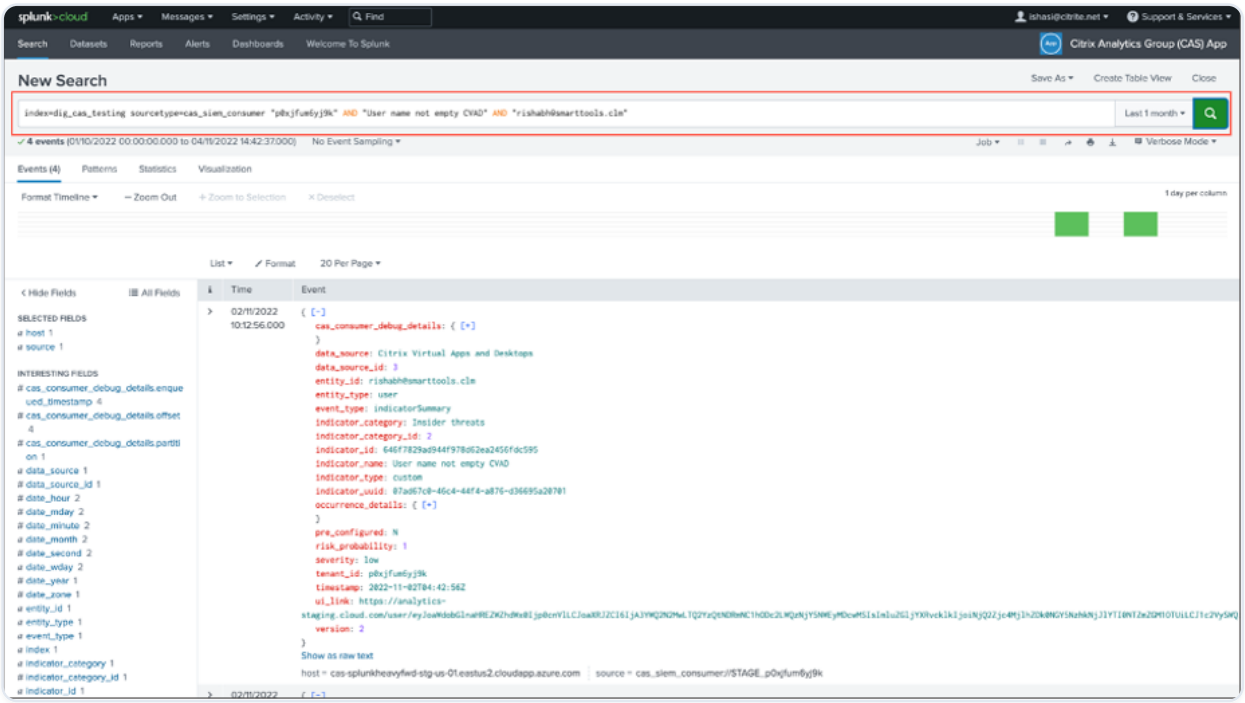


Splunkでのリスクインジケーターの発生 - 生クエリ

Splunk EnterpriseでCitrix Analytics for Securityアドオンのデータ入力を設定する際に、Splunkインフラストラクチャ管理者が使用したインデックスとソースタイプを使用することで、クライアントIPとOS情報を取得することもできます。

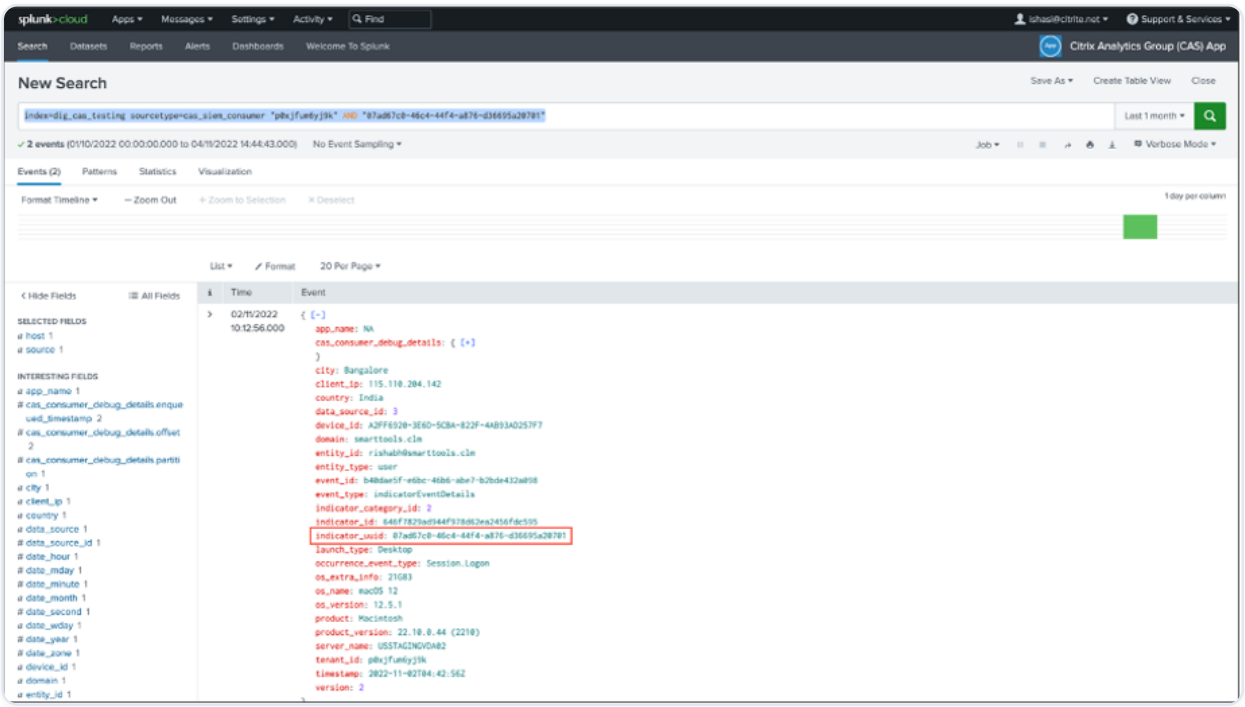
1. **Splunk > 新しい検索**に移動します。検索クエリに、次のクエリを入力して実行します。

```
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>"
```



2. indicator_uuid を取得し、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>"
```



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。イベント詳細には、**クライアントIP**と**OS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、「SIEM向けCitrix Analyticsデータエクスポート形式」を参照してください。

Splunkでのリスクインジケーターの発生 - ダッシュボードアプリ

Splunk用Citrix Analyticsアプリのインストール方法については、以下の記事を参照してください。

- Splunk用Citrix Analyticsアプリ
- Splunk用Citrix Analyticsダッシュボード

1. 「**Citrix Analytics – Dashboard**」タブをクリックし、ドロップダウンリストから「**Risk Indicator Details**」オプションを選択します。

   リスクインジケーターの詳細オプション(/en-us/citrix-analytics/media/risk-indicator-details-option.png)
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、「**Submit**」をクリックします。

   リスクインジケーターの詳細オプションフィルター(/en-us/citrix-analytics/media/risk-indicator-details-option-filter.png)
3. 詳細を取得するには、ユーザーインスタンスをクリックします。

   リスクインジケーターのユーザーインスタンス(/en-us/citrix-analytics/media/risk-indicator-user-instance.png)
4. このページの下部で、「**Client IP**」と「**OS information**」（名前、バージョン、追加情報）を表示できます。

   クライアントIPとOS情報(/en-us/citrix-analytics/media/client-ip-and-os-information.png)

データソースイベント

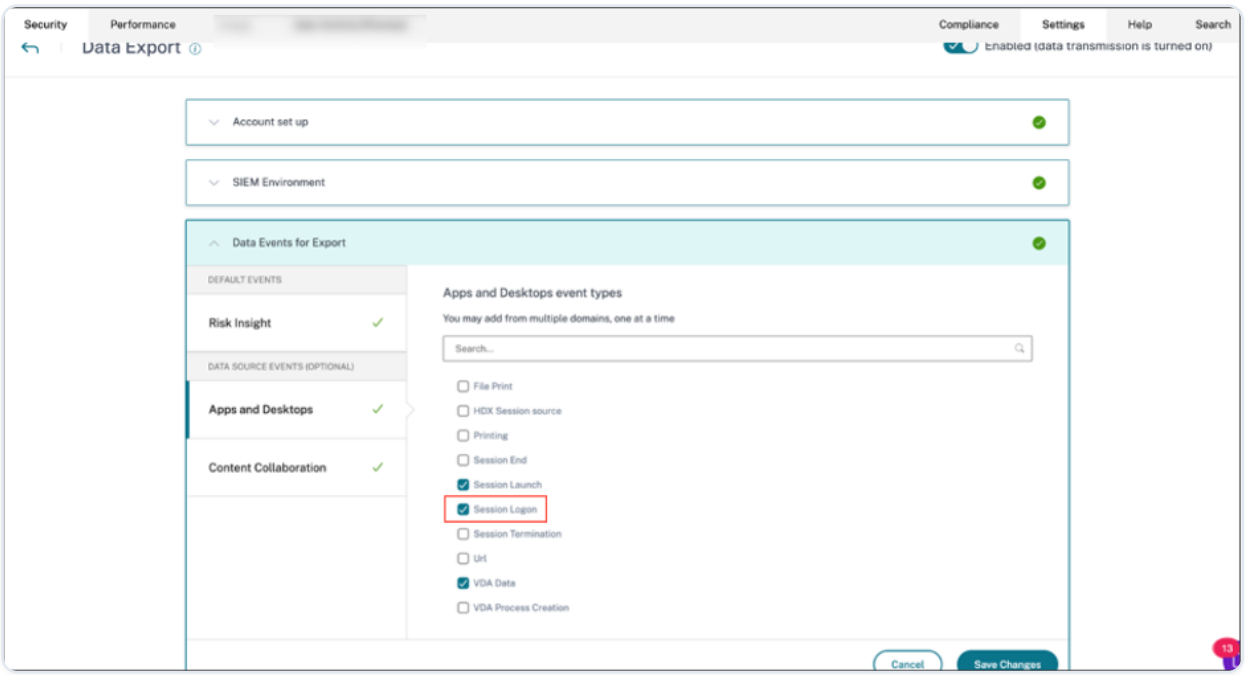
Splunk環境でクライアントIPとOSの詳細を取得するもう1つの方法は、エクスポート用のデータソースイベントを構成することです。この機能により、セルフサービス検索ビューに表示されるイベントがSplunk環境に直接流れるようになります。Virtual Apps and Desktopsのイベントタイプを SIEMにエクスポートするように構成する方法の詳細については、次の記事を参照してください。

- 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 Security dashboard > Search**」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それに関連する情報が利用可能です。次のスクリーンショットでは、「**Session.Logon**」イベントタイプが例として表示されています。

   セッションログオン(/en-us/citrix-analytics/media/session-logon.png)

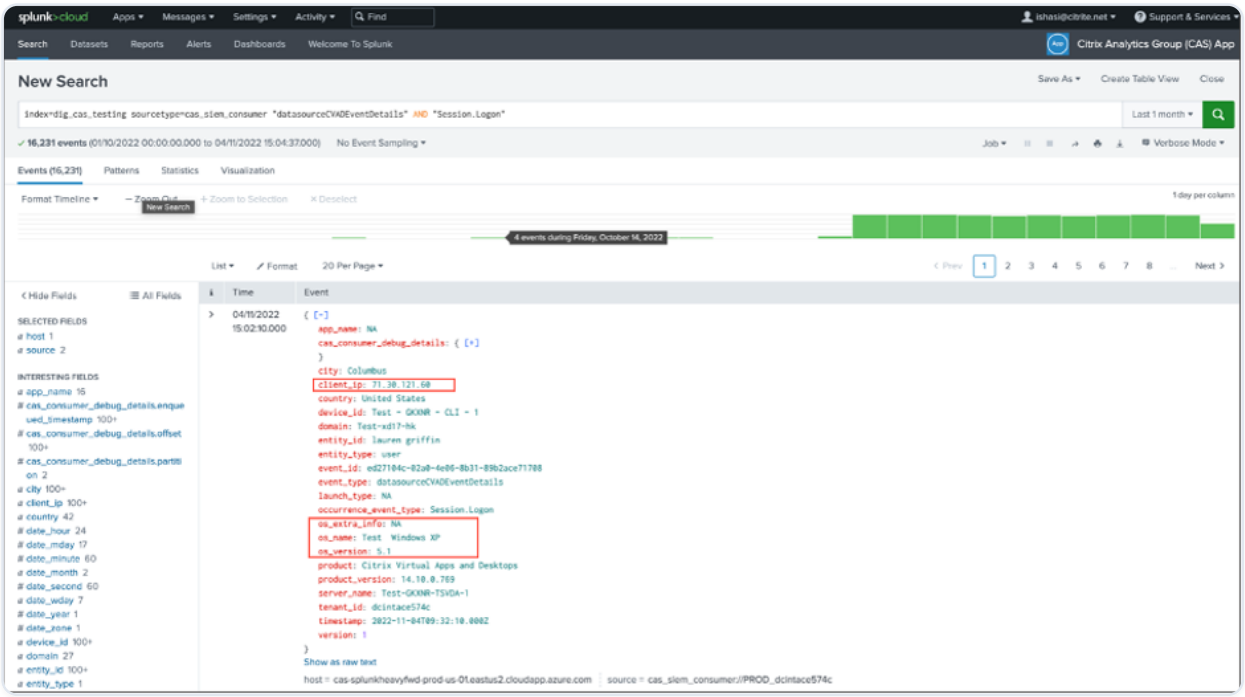
2. エクスポート用のデータソースイベントで「**Session.Logon**」を構成し、「**Save**」をクリックしてSplunk環境に流れるようにします。



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>"
```

   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

セキュリティのデータエクスポートビューには、管理者がCitrix AnalyticsとのSIEM統合をトラブルシューティングするのに役立つ**概要**タブが含まれています。**概要**ダッシュボードは、トラブルシューティングプロセスを支援するチェックポイントを通じて、データの健全性とフローを可視化します。

データエクスポートのトラブルシューティング(/en-us/citrix-analytics/media/troubleshooting-data-exports.png)

概要タブ

概要タブは、データエクスポートビューにおけるセルフサービスによるトラブルシューティングワークフローの基盤を形成します。このタブでは、次の3つのカードを使用してSIEMの設定を説明します。

- **Citrix Analyticsで利用可能なデータ**: このカードは、データソース構成の状態を示します。
- **SIEM消費に利用可能なイベント**: このカードは、SIEM環境で消費される準備ができているイベントの数を表示します。
- **SIEMによるデータ消費**: このカードは、SIEM環境におけるデータフローの状態を表示します。

Citrix Analyticsで利用可能なデータ

Citrix Analyticsで利用可能なデータ(/en-us/citrix-analytics/media/available-data-in-citrix-analytics.png)

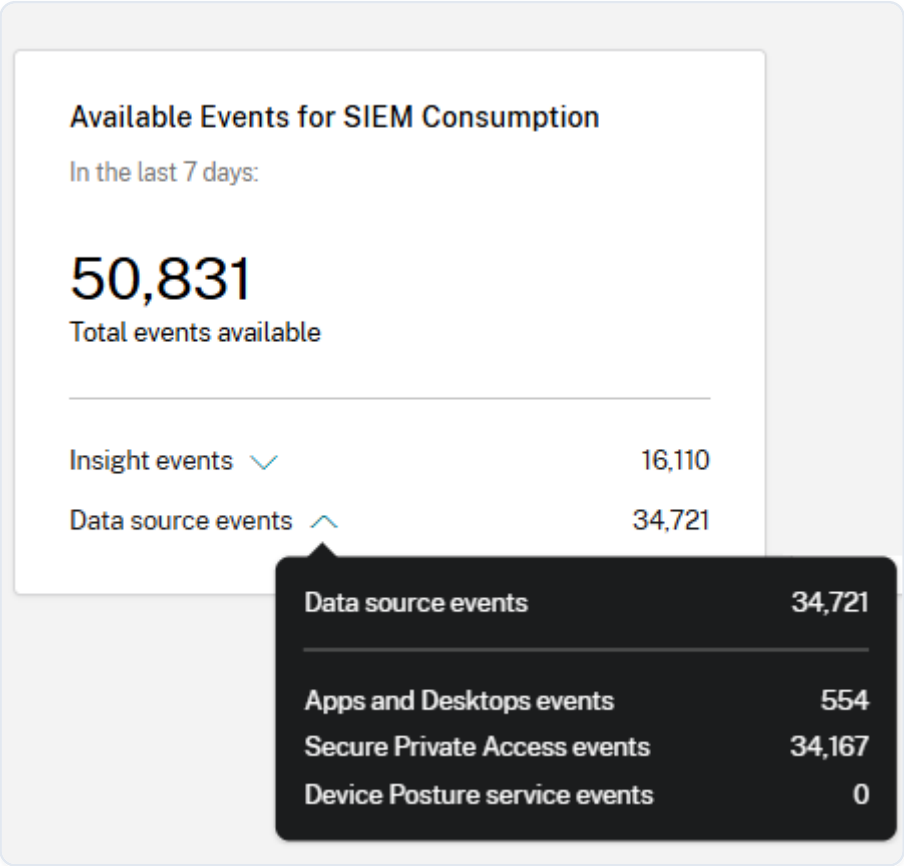
Citrix Analyticsで利用可能なデータカードには、Citrix Analytics for Securityにオンボーディングされ、最終的にSIEMインサイトに貢献できるデータソースの数が表示されます。現在、データエクスポートでサポートされているデータソースは、Apps and Desktops、Gateway、Secure Private Accessの3つです。これらのデータソースがオンボーディングされていても、データ処理がオフになっているデータソースではデータエクスポートは機能しません。そのようなデータソースが検出されると、上記の画像に示されているような適切な警告メッセージが表示されます。

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、イベントがCitrix Analytics for Securityに流入したことを確認できます。**データソースをオンボーディング**ボタンをクリックすると、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確認できます。

オンボーディングされたデータソースがない場合、次のスクリーンショットに示すように、適切な警告メッセージが表示されます。

データソースがない場合の警告メッセージ(/en-us/citrix-analytics/media/warning-message-for-no-data-sources.png)

SIEM消費に利用可能なイベント



「**SIEM消費に利用可能なイベント**」カードには、Insightおよびデータソースイベントの数と、SIEM環境に流れることが期待されるそれらの内訳が表示されます。展開すると、エクスポートされる各データイベントタイプのさらに詳細な内訳も利用できます。

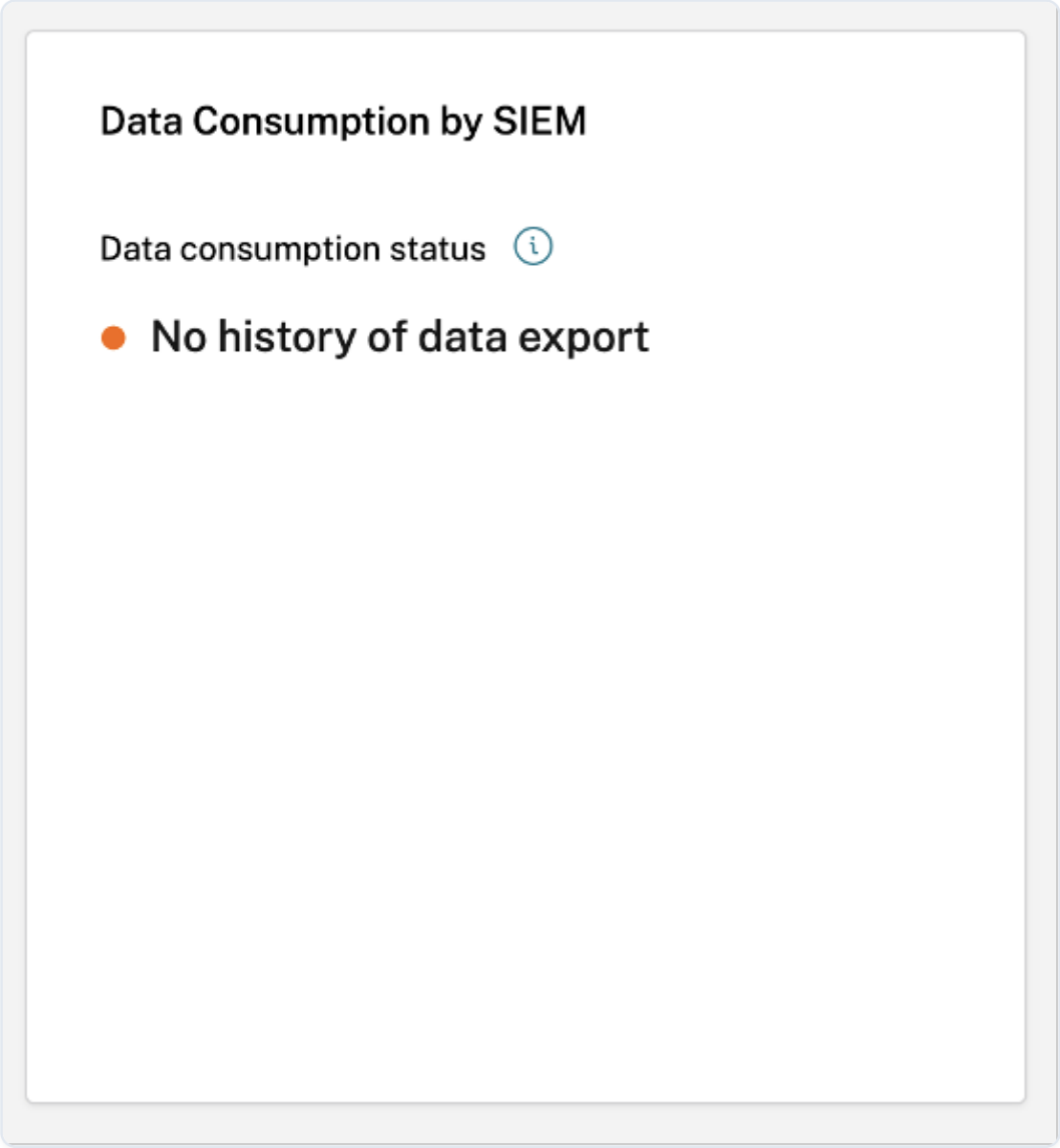
SIEMによるデータ消費

「**SIEMによるデータ消費**」カードは、Citrix Analyticsによって準備されたデータがSIEM環境に流れることの健全性を示します。データ消費ステータスは、**Kafka**トピック内のオフセットの動きに基づいています。利用可能な場合、このカードには、データ消費が最後に正常に検出され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は両方とも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、こちらをクリックしてください。

データ消費ステータスは、次の状態をとることができます。

1. **非アクティブな消費**

    - **データエクスポートの履歴なし**: この状態は、Citrix Analyticsによって準備されたデータがSIEM環境に正常に流れたことがないことを示すオレンジ色の点で表されます。



これは次の原因が考えられます -

- データソースの設定が不正確/不完全です。「**Citrix Analyticsで利用可能なデータ**」カードを使用して、十分なデータソースがあるか、およびエクスポートを許可するためにデータ処理がオンになっているかを確認できます。
- ユーザーアクティビティの不足。「**Citrix Analyticsで利用可能なデータ**」カードの「**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消費に利用可能なイベント**」カードを使用して、Citrix AnalyticsによってSIEMに流れるように準備されたInsightまたはデータソースイベントがあるかを確認できます。
- SIEM設定が不正確/不完全です。「**構成**」タブの「アカウント設定」段階が正常に完了していることを確認してください。設定が完了している場合、「アカウント設定」段階に緑色のチェックマークが表示されます。

アカウント設定が正常に完了した後で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ってください。

- 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アカウント設定またはSIEM環境での認証情報の問題 – 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ませんでした**: この状態は、少なくとも過去10分間、データがSIEM環境に正常に流れ込んでいないことを示します。カードには、データの最後の正常な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**の場合と同様に、**Citrix Analyticsで利用可能なデータ**カードと**SIEM消費で利用可能なイベント**カードを使用して、これをトラブルシューティングできます。利用可能なイベント数が増加するとともに十分なユーザーアクティビティがある場合は、最後の成功したタイムスタンプに注目し、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発生したかどうかを確認することをお勧めします。



- **7日以上前にエクスポートされました**: 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ます。上記の2つの状態と同様に、この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**カードと**SIEM消費で**

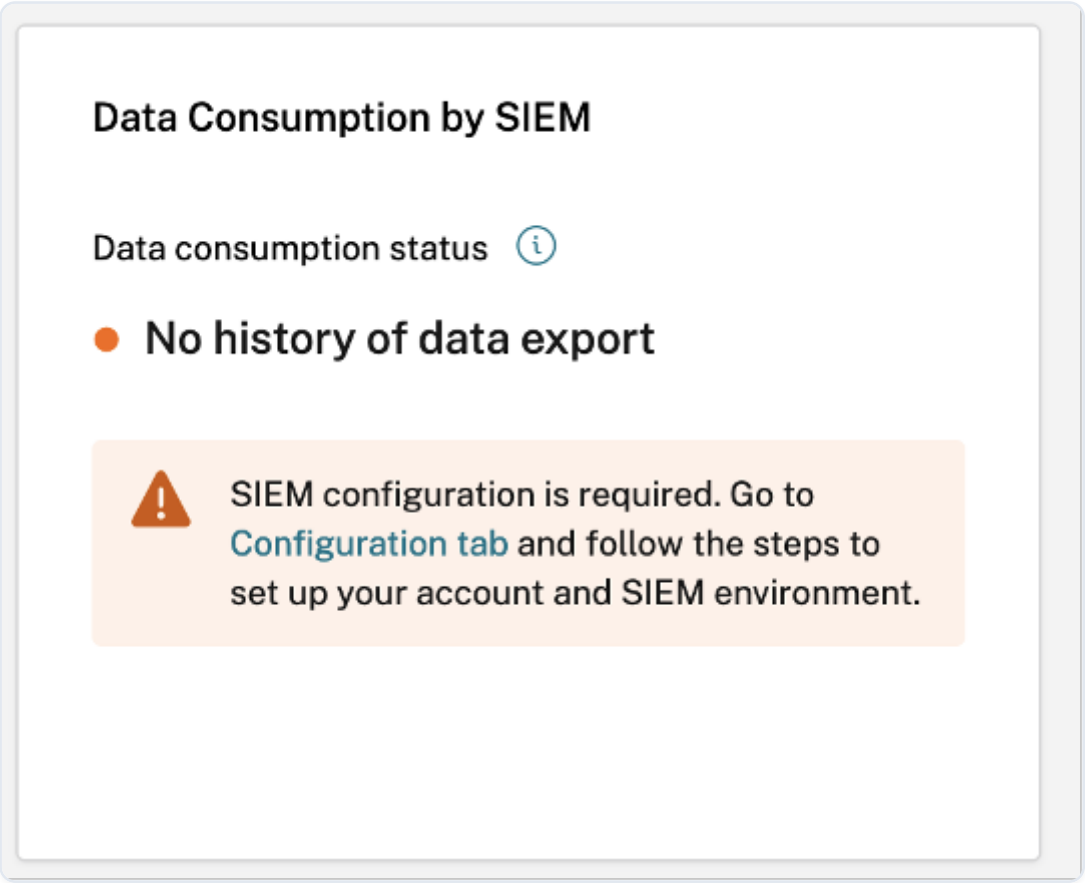
利用可能なイベントカードを使用してSIEMのセットアップをトラブルシューティングしてください。



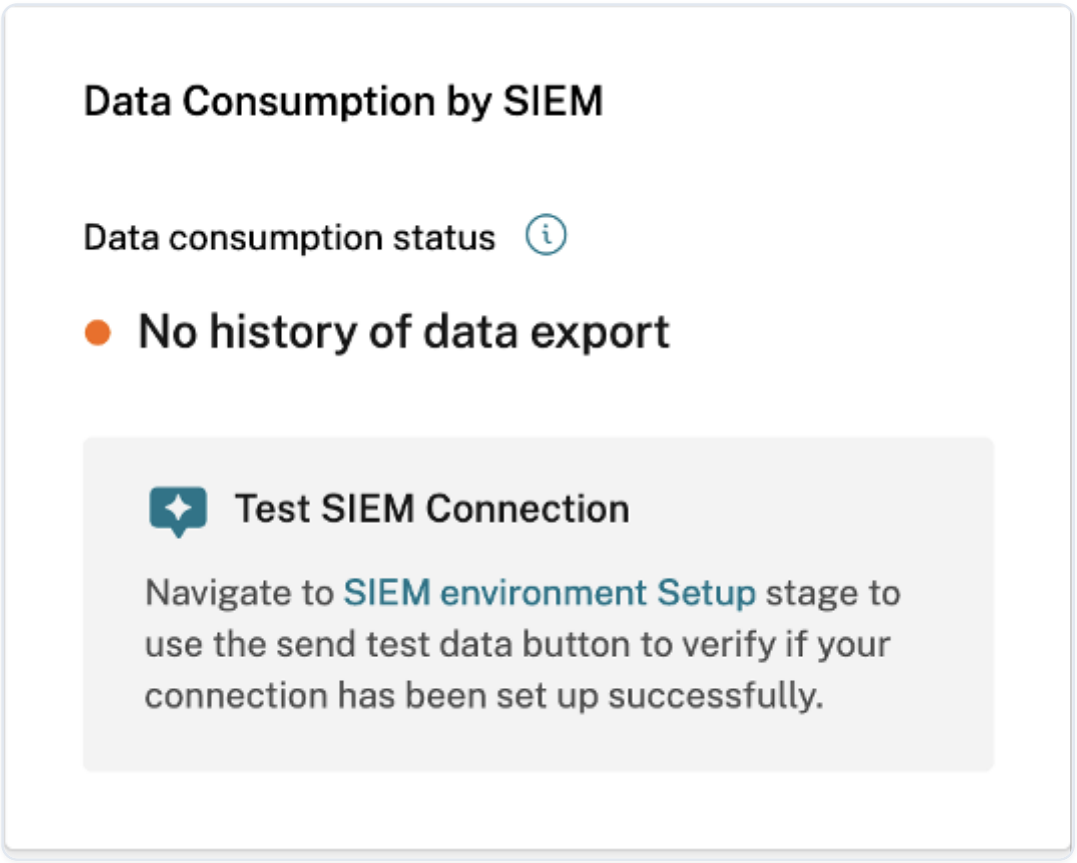
> **注**
>
> **Kafka保持ポリシー**: Citrix AnalyticsのKafkaトピックは、イベントを最大7日間のみ保持します。潜在的なデータ損失を回避または防止するために、データポーリング間隔を7日を超えないように設定することをお勧めします。

非アクティブな消費では、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を表示できます。

データエクスポートの履歴なしのケースで強調されているように、SIEMのセットアップが完了していない場合、データはSIEM環境に一切流れ込みません。したがって、次のスクリーンショットに示すように、アカウントのセットアップを完了するために、ユーザーは**構成**タブにリダイレクトされます。

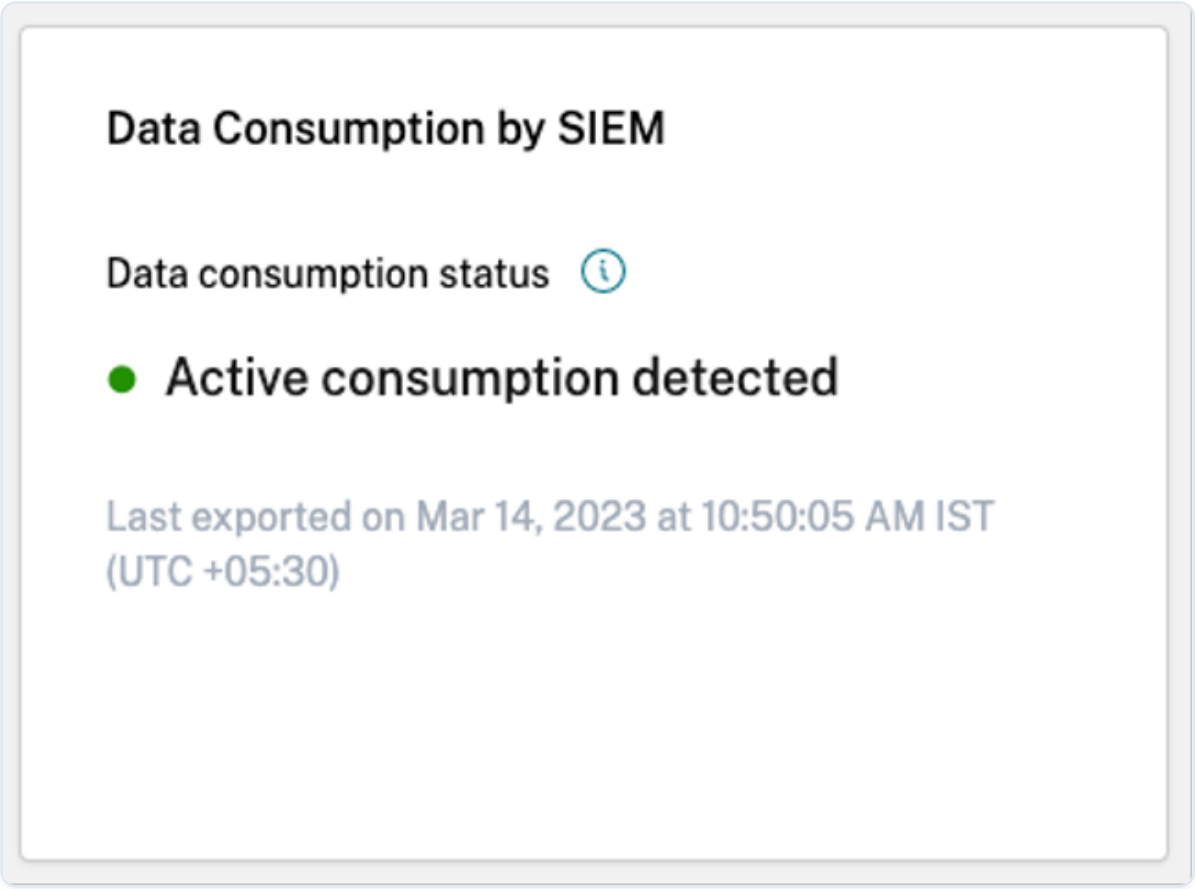


SIEMのセットアップが完了していても、**アクティブな消費が検出されませんでした**または**7日以上前にエクスポートされました**の状態に示されているように、データがアクティブに流れていない場合があります。したがって、次の警告メッセージで強調されているように、ユーザーはSIEM接続をテストするために**テストイベント生成**セクションに移動するよう促されます。



2. **アクティブな消費**

   - **アクティブな消費が検出されました**: この状態は、SIEMでアクティブな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

「**概要**」タブには、「**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、SIEMセットアップの展開、管理、トラブルシューティングが容易になります。セキュリティビューのデータエクスポートに関する包括的なガイドを提供するだけでなく、クイックガイドには、関連ドキュメントへのリンクを提供することで、SIEM環境をセットアップおよび管理する方法に関する役立つヒントも含まれています。

「データエクスポートクイックガイド1」(/en-us/citrix-analytics/media/data-export-quick-guide1.png)

「データエクスポートクイックガイド2」(/en-us/citrix-analytics/media/data-export-quick-guide2.png)

「データエクスポートクイックガイド3」(/en-us/citrix-analytics/media/data-export-quick-guide3.png)

クイックガイドブレードには「**SIEM接続のテスト**」セクションもあり、ユーザーはSIEM環境セットアップステージ内のSIEM接続テストステージにリダイレクトされます。これにより、ユーザーはSIEM統合自体が破損しているかどうかを調査し、Citrix Analytics for Securityがイベントを処理

する際の問題の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。

「SIEM接続のテスト1」(/en-us/citrix-analytics/media/test-siem-connection1.png)

「**構成**」タブは、展開設定をガイドするだけでなく、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、および一般的な落とし穴も提供します。適切な警告は、次の場合に表示されます。

- Citrix Analyticsは、データソースがオンボーディング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たテレメトリを収集するために、Apps and Desktopsをオンボーディングすることをお勧めします。オンボーディングされたデータソースがない場合、SIEMのセットアップが正常に完了していても、データフローは観測されません。

  「オンボーディングされたデータソースなし」(/en-us/citrix-analytics/media/no-data-sources-onboarded.png)
- 次の図に示すように、アカウント設定が正常に完了するまで、SIEM環境設定とエクスポート用データイベントのステージは無効になります。

  「SIEM環境設定とデータイベントを無効にする」(/en-us/citrix-analytics/media/disable-siem-environment-setup-and-data-events.png)
- データエクスポートが無効になっています。エクスポート用データイベントステージの警告は、変更を有効にするためにデータエクスポートを有効にするよう促すものです。

  「データエクスポートが無効になっています」(/en-us/citrix-analytics/media/data-exports-turned-off.png)
- エクスポート用データイベントステージで、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、SIEMにはデータソースイベントが流れません。これを有効にするには、目的のデータソースイベントのタイプを設定して選択する必要があります。さらに、データがCitrix Analyticsに到達するように、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。

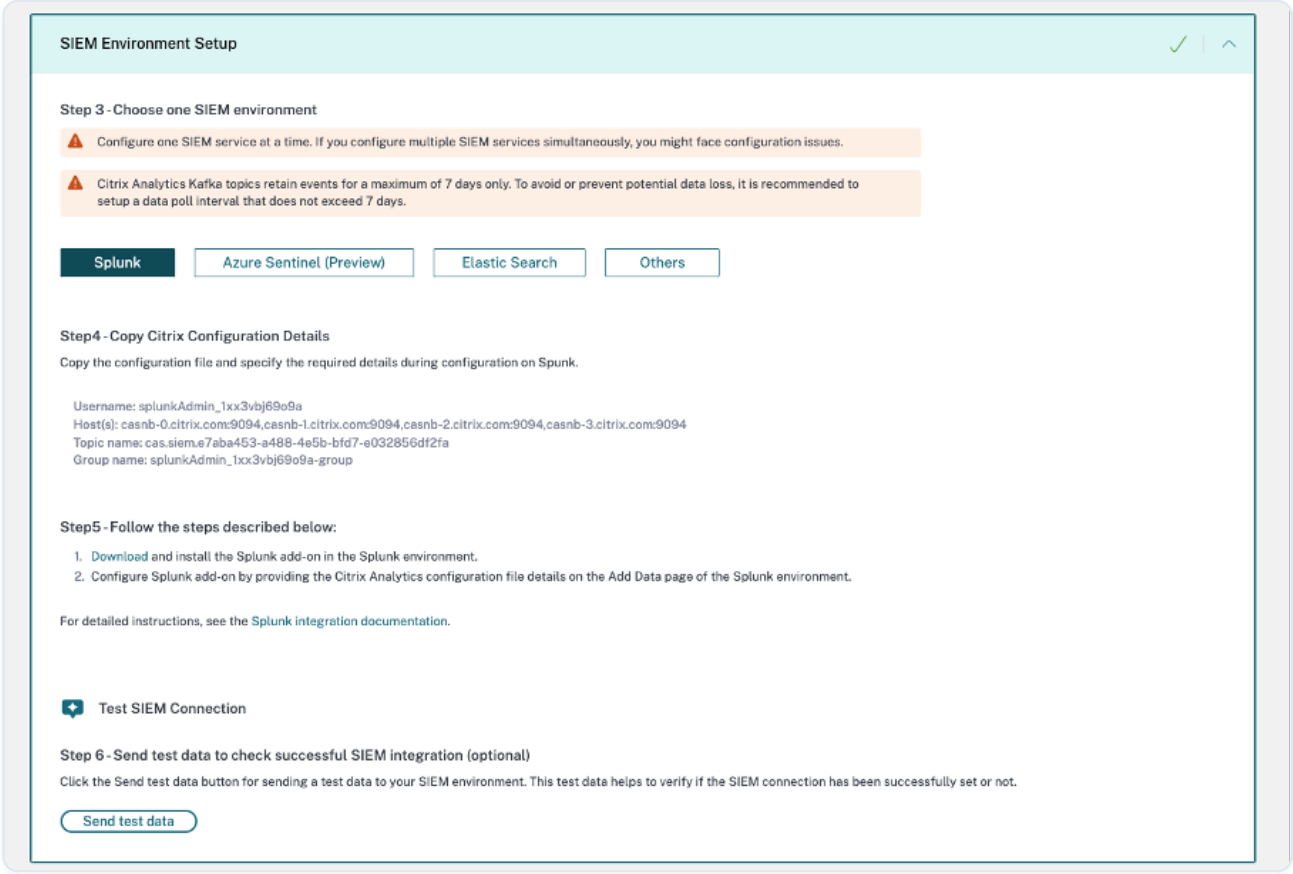
  「エクスポート用データイベントステージで」(/en-us/citrix-analytics/media/on-data-events-for-export-stage.png)

テストイベント生成

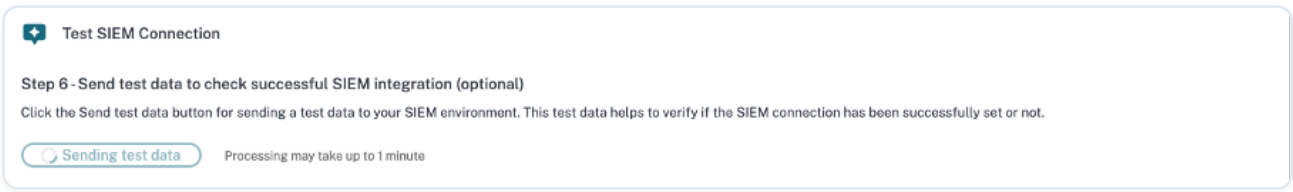
テストイベント生成は、トラブルシューティングエクスペリエンスを向上させるために、**SIEM環境設定**段階の一部として提供されます。ユーザーがSIEM設定を完了すると、テストイベント生成

により、顧客のSIEMデータエクスポートKafkaトピックにテストイベントを直接送信することで、SIEM接続を迅速にテストする方法が提供されます。

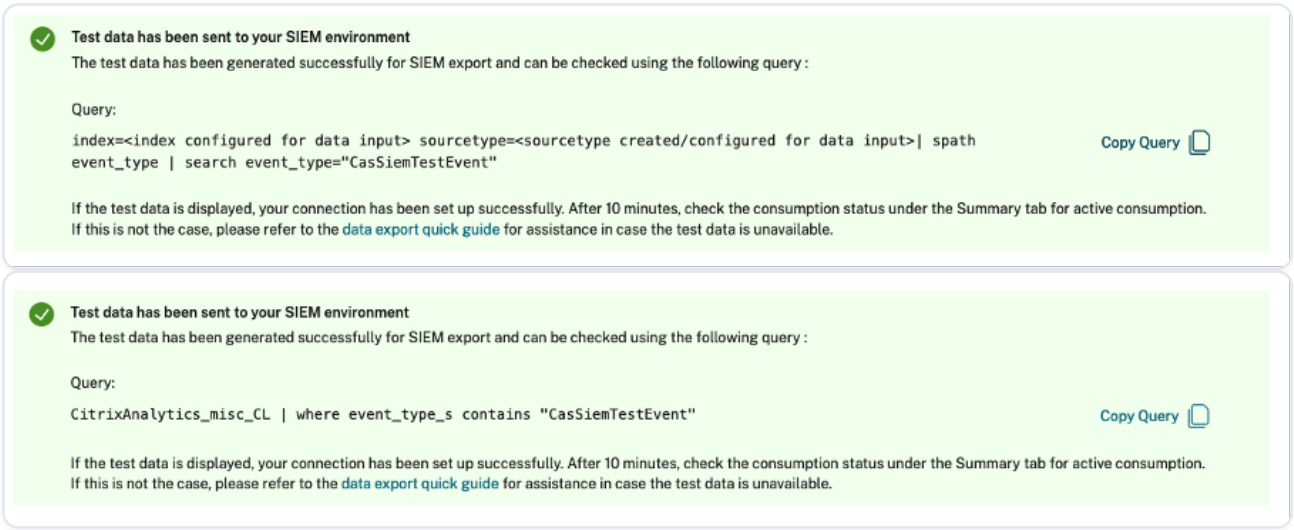
また、新規ユーザーが新しいデータソースを明示的にオンボーディングし、その後ユーザーアクティビティを生成することなく、Citrix AnalyticsとのSIEM統合を迅速にテストできるようにします。



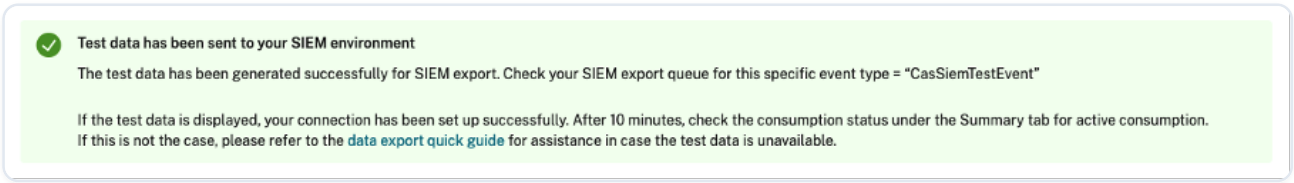
この機能をテストするには、ユーザーは**テストデータを送信**ボタンをクリックする必要があります。これによりダミーのテストイベントが生成され、顧客のSIEMデータエクスポートKafkaトピックに送信されます。このテストイベント生成プロセスには、次のスクリーンショットに示すように、最大1分かかる場合があります。



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た場合、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およびSentinel）に応じて、管理者はクエリをコピーし、SIEM環境でテストイベントを確認できます。

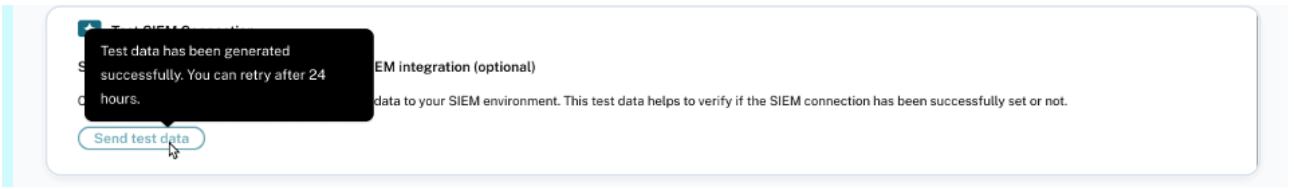


Elasticsearchおよびその他の環境の場合、次の成功メッセージが表示されます。



注

テストイベントが生成されると、**テストデータを送信**ボタンは次の24時間無効になり、ユーザーが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時間後、ボタンが有効になり、ユーザーは再度機能をテストできます。



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い場合、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。ユーザーは接続をテストするためにデータを再度送信できます。



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について管理者に通知するために、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態勢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過程をナビゲートするのにも役立ちます。

受信トレイでこれらのメールアラートを見つけるのに役立つ、このメールアラートセットのいくつかの重要なプロパティは次のとおりです。

- このメールは、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布されます。
- 送信者はCitrix Cloud **mailto:donotreplynotifications@citrix.com**です。
- 件名は次のとおりです。
    - パスワードリセットメールアラートの場合: **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.**
    - データフロー中断メールアラートの場合: **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.**

メール通知を有効にする方法?

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、セキュリティおよびパフォーマンス読み取り専用）を持つCitrix Cloud管理者で、Security Analyticsを管理している場合、メール通知はCitrix Cloudアカウントで常に有効になっています。デフォルトでは、週次メール通知はCitrix Security Administrators - default listに送信されます。このアラートを受信す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。

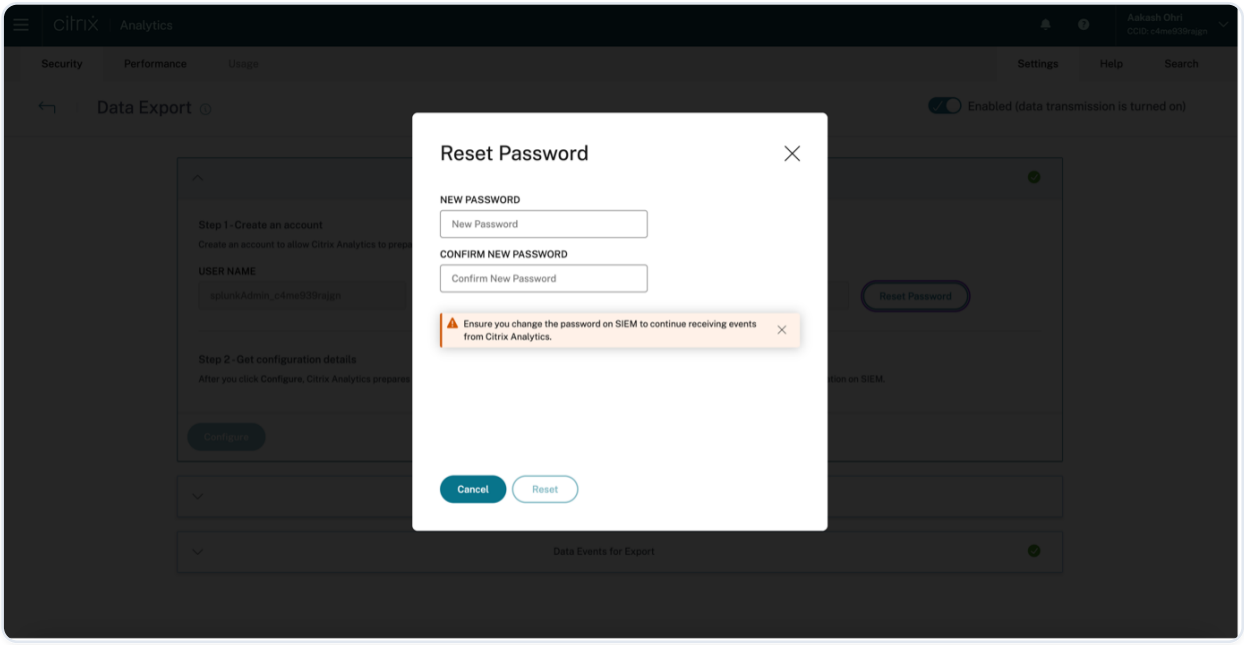
カスタムアクセス権限（セキュリティフル管理者、セキュリティ読み取り専用管理者、セキュリティおよびパフォーマンス読み取り専用）を持つCitrix Cloud管理者で、Security Analyticsを管理している場合、メール通知はCitrix Cloudアカウントで常に有効になっています。

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、Data Exportsページから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でSIEMパスワードをリセットするだけでは、SIEMで設定されているパスワードとの不一致が生じる可能性があります。これにより、データフローが中断されます。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、**Summary**タブに移動し、「last exported at」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することで、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環境へのデータフローがすぐに正常に戻るのに役立ちます。



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場合に送信されます。このメールには、最後のイベントがエクスポートされた時刻と、データフローを復旧するために実行できる役立つトラブルシューティングのヒントが含まれています。これは、セキュリティ保護されたデータを失わないように、データフローを迅速に再開するための適切なタイミングです。

3. **7日間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トピックの保持期間は7日間であるため、このメールはセキュリティ保護された情報の永続的な損失の状況を警告しているため、それ以上のデータを失わないように、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**ページで利用可能なクイックガイドの助けを借りることが重要です。

4. **30日間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日以上中断された場合に送信されます。この時点までに、お客様はセキュリティ保護されたデータを失っており、できるだけ早くフローを再開するためにトラブルシューティング機能を使用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

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,

セキュリティインサイトのためのSigmaシグネチャの例

このページには、管理者がCitrix Security Analyticsを使用して有意義な成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
- 内部脅威
- データ持ち出し

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 **> >** をクリックします。 ページに サイト カードが表示されます。 をクリックして、Citrix Analyticsがこのデータソースのデータ処理を開始できるようにします。

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（デフォルトのエクスポート）
- 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は利用可能であり、常にデフォルトでオンになっています。詳細については、「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。

データソース内の特定のユーザーイベントを検証するには、CASまたはSigmaシグネチャのいずれかを使用できます。CASクエリは、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。Sigmaシグネチャは、シンプルでユーザーフレンドリーな形式で記述されており、さまざまなSIEM環境と互換性があります。

CASクエリの使用

「**セルフサービス検索**」ページで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および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、カスタムリスクインジケーターを作成することもできます。カスタムリスクインジケーターを作成するには、**セキュリティ > カスタムリスクインジケーター > インジケーターの作成**に移動します。詳細については、「カスタムリスクインジケーターの作成」を参照してください。

Sigmaシグネチャの使用

Sigmaは、アナリストがログイベントを記述するため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あり、検出の記述を容易にします。SigmaシグネチャをSIEMツールのクエリ言語に変換するには、いくつかの異なる方法があります。

- Sigmaが提供するCLIツールとPython SDKを使用できます。Sigmaシグネチャの詳細については、「ルールの使用方法」を参照してください。
- uncoder.ioのSigma Translation Engineなど、無料枠を提供する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、以下の異なるカスタムインジケーターのユースケースを参照してください。

- 未承認のブラウザ
- 未承認のオペレーティングシステム
- 未承認のWorkspaceアプリバージョン
- 許可リスト外の未承認のオペレーティングシステム
- 未承認のIPアドレスまたはサブネット
- 未承認の仮想アプリ
- 異常なデスクトップ名
- 特定のアプリケーションの監視
- SaaSアプリからの印刷(/ja-jp/security-analytics/example-sigma-signatures-for-security-insights/data-exfiltration.html#printing-from-saas-apps)
- SaaSアプリでのクリップボードの使用(/ja-jp/security-analytics/example-sigma-signatures-for-security-insights/data-exfiltration.html#clipboard-usage-on-saas-apps)

侵害されたエンドポイント

未承認のブラウザ

これは、ユーザーが組織のITポリシーで許可されていない、またはセキュリティ脆弱性があるブラウザの種類やバージョンからコンテンツ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 App)

CASクエリ

```
Event-Type = "Session.Logon" AND Browser-Name !~ "<Browser-Name>"
```

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

```
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
```

未承認のオペレーティングシステム

これは、ユーザーが組織のITポリシーで許可されていない、またはセキュリティ脆弱性があるオペレーティングシステムの種類やバージョンを持つデバイス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 App)

CASクエリ

```
Event-Type = "Session.Logon" AND OS-Name ~ "<OS-Name>" AND OS-Version =
"<OS-Version>" AND OS-Extra-Info = "<OS-Extra-Info>"
```

Sigmaシグネチャ

```
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
```

不正なIPアドレスまたはサブネット

これは、ユーザーが組織のITポリシーによって不正とマークされたIPアドレスまたは範囲から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 App)

CASクエリ

```
Event-Type = "Session.Logon" AND Client-IP = "<XX.YY.ZZ.*>"
```

Sigmaシグネチャ

```
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
```

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外の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 App)

CASクエリ

```
Event-Type = "Session.Logon" AND OS-Name !~ "<OS-Name>" AND OS-Version !=
"<OS-Version>" AND OS-Extra-Info != "<OS-Extra-Info>"
```

Sigmaシグネチャ

```
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
```

未承認のWorkspaceアプリバージョン

これは、ユーザーがサポートされていないクライアントバージョンのWorkspaceアプリにアクセスしようとした場合に発生します。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、「サポートされている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 App)

CAS クエリ

```
Event-Type = "Session.Logon" AND Client-Type IN ("Windows", "Macintosh",
"Unix/Linux") AND Workspace-App-Version != "20*" AND Workspace-App-
Version != "21*"
```

Sigma シグネチャ

```
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
```

内部脅威

不審なデスクトップ名

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 App)

CASクエリ

```
Event-Type = "Session.Logon" AND Session-Launch-Type = "desktop" AND App-
Name ~ "<Desktop Name>"
```

Sigmaシグネチャ

```
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
```

特定のプロセスを監視

これは、ユーザーが監視リストにある公開アプリケーションを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である可能性があります。

詳細

データソース: アプリとデスクトップ (セッションレコーディング)

CASクエリ

```
Event-Type = "Citrix.EventMonitor.AppStart" AND App-Name IN ("<App-Name-1>", "<App-Name-2>")
```

Sigmaシグネチャ

```
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
```

不正な仮想アプリ

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 App)

CASクエリ

```
Event-Type = "App.Start" AND App-Name IN ("<App-Name1>", "<App-Name2>")
```

Sigmaシグネチャ

```
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
```

データ持ち出し

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が印刷され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持ち出しを検出します。

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

```
Event-Type = "App.SaaS.File.Print" AND SaaS-App-Name = "<App-Name>"
```

Sigmaシグネチャ

```
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
```

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、または貼り付けのアクティビティが行われた場合に発生します。クリップボード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持ち出しを検出します。

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

```
Event-Type = "App.SaaS.Clipboard" AND Clipboard-Result = "success" AND
Clipboard-Operation IN ( "copy" , "cut" )
```

Sigmaシグネチャ

```
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
```

ユーザーダッシュボード

概要

ユーザーダッシュボードは、ユーザー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、異常な行動をプロアクティブに監視、検出、フラグ付けできます。

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、次のセクションが含まれています。

ユーザーダッシュボード(/en-us/citrix-analytics/media/users-dashboard.png)

- **ユーザーアクティブステータス**: 合計ユーザー、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、合計ユーザーの分布、および選択した期間における最高計算リスクスコアに基づいて、高、中、低プロファイルの危険ユーザーの分布。
- **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、すべてのユーザー、特権ユーザー、ウォッチリストユーザーに分類されます。
- **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。類似の行動パターンを持つリスクインジケーターはカテゴリにグループ化されます。
- **リスクインジケーターとアクション**: 組織内のすべてのユーザーについて、選択した期間にわたってプロットされたリスクインジケーターとアクションの分布。
- **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上位5つのポリシーとアクションを表示します。
- **リスクインジケーター**: 組織内の上位5つのリスクインジケーターを表示します。

ユーザーアクティビティステータス

アナリティクス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です。これらのユーザーには、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のドロップダウンメニューをクリックすると、総ユーザー数をアクティブユーザーと非アクティブユーザーに分類した分布を表示できます。

- 総ユーザー数: 選択した期間内のユーザーの総数。
- アクティブユーザー: 選択した期間内にイベントが検出されたユーザー。
- 非アクティブユーザー: 選択した期間内にイベントが検出されなかったユーザー。

ユーザーダッシュボードに表示されるユーザーの総数は、すべてのユーザーが危険であるとは限らないため、危険なユーザーの数よりも多くなる可能性があります。

> **注**
>
> **ユーザー**ページでは、選択した期間に関係なく、過去30日間のユーザー総数が表示されます。

ファセット

以下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、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、役員権限、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。

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あり、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、ユーザーは次のいずれかのカテゴリに分類されます：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。

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。ユーザー名を選択すると、そのユーザーのユーザー情報とリスクタイムラインが表示されます。ユーザーはリスクインジケーターをトリガーしている場合とトリガーしていない場合があります。このユーザーに関連付けられた危険なイベントがない場合、次のメッセージが表示されます。

危険なイベントはありません(/en-us/citrix-analytics/media/no-risky-event.png)

ユーザーに関連付けられた危険なイベントがある場合、そのリスクタイムラインにリスクインジケーターが表示されます。ユーザーを選択して、そのリスクタイムラインを表示します。

ユーザーは`privileged`としてマークされ、ウォッチリストに追加できます。

検出されたデータソース

ユーザーに関連付けられたデータソース。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**ページで利用可能なデータソースサイトカードでデータ処理をオンにする必要があります。

トリガーされたインジケーター

選択した期間にわたってユーザー全体でトリガーされたリスクインジケーターの数を示します。**トリガーされたインジケーター**タイルをクリックして、リスクインジケーターの詳細を表示します。リスクインジケーターテーブルには、次の詳細が表示されます。

- **名前**: リスクインジケーター名。
- **重大度**: イベントに関連付けられたリスクの重大度。リスクは高、中、低のいずれかです。
- **データソース**: リスクインジケーターテンプレートが適用されるデータソース。
- **タイプ**: リスクインジケーターのタイプ。リスクインジケーターはデフォルトまたはカスタムのいずれかです。
- **発生回数**: ユーザーに対してリスクインジケーターがトリガーされた回数。期間を選択すると、リスクインジケーターの発生回数は時間の選択に基づいて変化します。

- **最終発生**: 最終発生日時を表示します。

危険なユーザーリンク(/en-us/citrix-analytics/media/indicator-triggered.png)

適用されたアクション

選択した期間にわたってユーザーに適用されたアクションの数を示します。これには、管理者によって手動で適用されたアクションと、ポリシー駆動型のアクションが含まれます。**適用されたアクション**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。

適用されたアクション(/en-us/citrix-analytics/media/actions-page.png)

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。
- **発生回数**: アクションの発生回数。
- **日時**: 適用されたアクションの日時。

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。

処理されたイベント(/en-us/citrix-analytics/media/events-processed.png)

ユーザーリスク分布

選択した期間における、計算された最高リスクスコアに基づいて、高、中、低プロファイルのユーザー数を表示できます。全体のカウントの下には、低、中、高リスクユーザーの分布の時間的変化を示す棒グラフが表示されます。

ユーザーリスク分布(/en-us/citrix-analytics/media/user-risk-distribution.png)

リスクレベルは3つのカラーコードに分類されます。

- **赤** - 高リスクユーザーを表します。
- **オレンジ** – 中リスクユーザーを表します。
- **グレー** – 低リスクユーザーを表します。

特定期間に基づいてカラーバーにマウスを合わせると、リスクのあるユーザー（高、中、低）の数を確認できます。データ間隔情報とともに、最終更新の詳細（日付と時刻）を確認できます。い

ずれか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。更新されたデータを取得するには、更新オプションをクリックします。

リスクのあるユーザー

リスクのあるユーザーとは、リスクのあるイベントが関連付けられており、少なくとも1つのリスクインジケーターをトリガーしたユーザーです。特定の期間にユーザーがネットワークにもたらすリスクのレベルは、ユーザーに関連付けられたリスクスコアによって決定されます。リスクスコア値は動的であり、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、ユーザーアクティビティに基づいて時間の経過とともに定期的に更新されます。そのため、ある時点では中リスクまたは高リスクのユーザーが、後でより低いリスクレベルに低下する可能性があります。リスクスコアに基づいて、リスクのあるユーザーは次のいずれかのカテゴリに分類されます。

- 高リスク
- 中リスク
- 低リスク

リスクのあるユーザーページでは、ファセットを使用して選択した期間に関連付けられたリスクレベルに基づいて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クエリしたりできます。

リスクのあるユーザーのファセット(/en-us/citrix-analytics/media/risky-users-facet.png)

ユーザーのメールIDをクリックすると、その特定の選択されたユーザーの**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、選択された期間に基づいて、リスクインジケーターと**最新**および**最高リスクスコア**の詳細が表示されます。

最新かつ最高の危険度スコア(/en-us/citrix-analytics/media/latest-and-highest-risk-score.png)

高リスク

リスクスコアが90から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、組織に対する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、選択した期間で計算された最高の危険度スコアに基づいて、高リスクユーザーの数を確認できます。

高リスクユーザー(/en-us/citrix-analytics/media/high-risk-users.png)

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、高リスクユーザーに関する詳細が表示されます。

中リスク

リスクスコアが70から89のユーザー。これらのユーザーは通常、潜在的に疑わしい、または異常に見える1つ以上の活動を行っており、綿密な監視が必要となる可能性があります。

中リスクユーザー(/en-us/citrix-analytics/media/medium-risk-users.png)

中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、中リスク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から69のユーザー。これらのユーザーは、通常とは異なる、または予期せぬ行動を示す少なくとも1つのリスク指標を持っていますが、より深刻なリスク分類を必要とするほどではありません。

低リスクユーザー(/en-us/citrix-analytics/media/low-risk-users.png)

低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、低リスクユーザーに関する詳細が表示されます。

低リスクスコア(/en-us/citrix-analytics/media/low-risk-score.png)

上位ユーザー

選択した期間で最もリスクスコアが高い上位ユーザーを、さまざまなユーザーカテゴリで表示できます。以下の**上位ユーザー**テーブルには、最新のリスクスコアではなく、選択した期間で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（すべて、特権、ウォッチリストユーザー）が表示されます。

上位ユーザー(/en-us/citrix-analytics/media/top-users.png)

> **注**
>
> 以前のバージョンでは、上位ユーザーテーブルは、選択された期間に関係なく、常に最新のリスクスコアを表示していました。

ウォッチリストユーザー

潜在的な脅威がないか厳密に監視されているユーザーのリストです。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監視できます。また、特定の危険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。ユーザーをウォッチリストに手動で追加するか、ポリシーを定義してウォッチリストにユーザーを追加します。

ユーザーをウォッチリストに追加している場合、最もスコアが高いウォッチリスト内の上位5人のユーザーを表示できます。

ウォッチリストにユーザーがいません(/en-us/citrix-analytics/media/zero-users-in-watchlists.png)

すべてのユーザーペインの**詳細を見る**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**ページでは、ウォッチリスト内のユーザー数は、選択された期間に関係なく、過去13か月間表示されます。期間を選択すると、リスク指標の発生は期間の選択に基づいて変化します。

> 詳細はこちら: ウォッチリスト

リスクカテゴリ

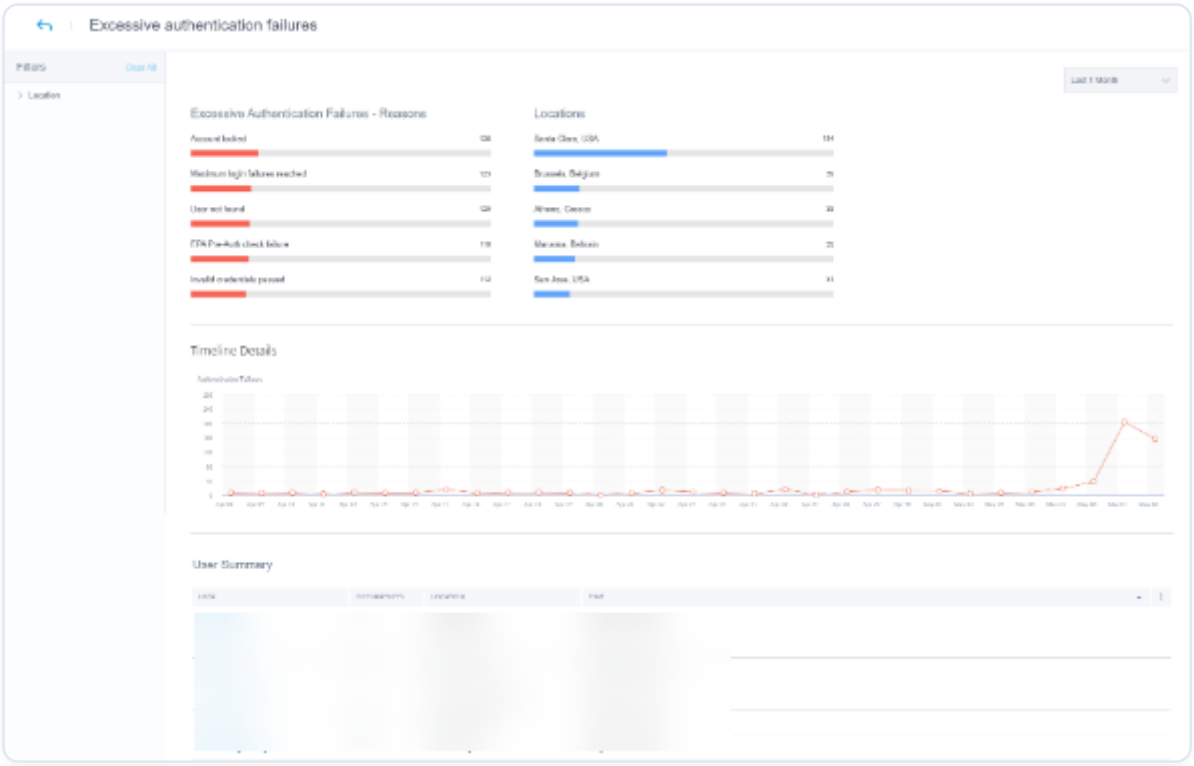
リスクカテゴリドーナツチャートは、選択した期間におけるリスクカテゴリ別の指標発生数を要約します。各チャートセグメントにカーソルを合わせると、一意のユーザー数が表示され、対応する**リスク指標カテゴリ**概要ページにリンクします。リスク分類は、デフォルトおよびカスタムのリスク指標によってサポートされています。



「**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 の管理者がユーザーリスクを管理し、専門的なセキュリティ知識を必要とせずにセキュリティ担当者と簡潔な議論を行えるようにすることです。これにより、セキュリティの強制が組織レベルで有効になり、セキュリティ管理者のみに限定されません。

ユースケース

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**」>「**認証失敗の過剰 - Citrix Gateway**」リスクインジケータ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。さらに詳しく調べると、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、このリスクインジケータに関する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矛盾があることに気づいた場合は、セキュリティ管理者に通知できます。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強制に貢献します。



リスクカテゴリダッシュボードを分析する方法?

「**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、リスクカテゴリに関する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。

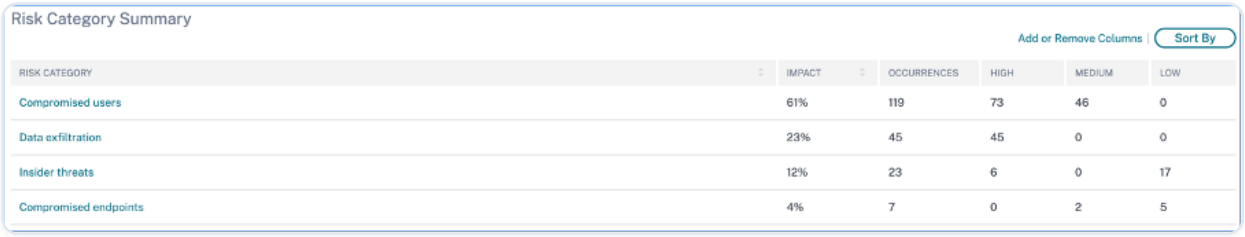
- **リスクカテゴリレポート**: 選択した期間における各カテゴリの合計リスクインジケータ発生数を表します。



- **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インジケータ発生数をグラフで表示します。このセクションの下部に移動すると、リスクインジケータに関するより正確な洞察を得るために、リスクカテゴリに基づいて並べ替えることができます。



- **リスクカテゴリの概要**: このセクションでは、各カテゴリに関連付けられたリスクインジケータの影響、発生数、重大度などの詳細が提供されます。いずれかのリスクカテゴリを選択すると、そのカテゴリに関連付けられたリスクインジケータの詳細が表示されます。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。

- **リスクインジケータレポート**: 選択した期間における侵害されたユーザーカテゴリに属するリスクインジケータを表示します。また、選択した期間中にトリガーされたリスクインジケータの合計発生数も表示されます。

  侵害されたユーザーページ(/en-us/citrix-analytics/media/compromised-users-risk-category-ri-report.png)

- **タイムラインの詳細**: 選択した期間におけるリスクインジケーターの発生状況をグラフィカルに表示します。

  侵害されたユーザーページ(/en-us/citrix-analytics/media/compromised-users-risk-category-timeline-details.png)

- **リスクインジケーターの概要**: 侵害されたユーザーカテゴリで生成されたリスクインジケーター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ーの種類、発生回数、および最終発生日時も表示されます。

  侵害されたユーザーページ(/en-us/citrix-analytics/media/compromised-users-risk-indicator-summary.png)

リスクインジケーターを選択すると、そのインジケーター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**リスクインジケーターを選択すると、このインジケーター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、このリスクインジケーターをトリガーしたユーザー、リスクインジケーターの発生回数、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、その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。

侵害されたユーザーページ(/en-us/citrix-analytics/media/risk-categories-first-time-access-from-new-device-ri-details-page.png)

注

Citrix Analytics は、デフォルトのリスクインジケーターを適切なリスクカテゴリにグループ化します。カスタムリスクインジケーターの場合は、**インジケーターの作成**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、「カスタムリスクインジケーター」を参照してください。

リスクカテゴリの種類

データ持ち出し

このカテゴリは、マルウェアによって、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実行する従業員によってトリガーされるリスクインジケーターをグループ化します。指定された期間中に発生したすべてのデータ持ち出し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プロアクティブにアクションを適用することで、このカテゴリに関連するリスクを軽減できます。

データ持ち出しリスクカテゴリには、次のリスクインジケーターがグループ化されています。

データソース	ユーザーリスクインジケーター
シトリックス バーチャル アプリケーションズ アンド デスクトップス および Citrix DaaS	潜在的なデータ持ち出し

内部脅威

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より高いレベルのアクセス権を持っているため、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ることもあれば、人為的なミスの結果であることもあります。どちらのシナリオでも、組織へのセキュリティ上の影響は甚大です。このカテゴリは、指定され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。これらの洞察を活用することで、ユーザープロファイルにプロアクティブにアクションを適用することにより、このカテゴリに関連するリスクを軽減できます。

内部脅威リスクカテゴリは、次のリスク指標をグループ化します。

データソース	ユーザーリスク指標
シトリックス セキュア プライベート アクセス™	ブラックリストに登録されたURLへのアクセス試行
シトリックス セキュア プライベート アクセス	過剰なデータダウンロード
シトリックス セキュア プライベート アクセス	危険なウェブサイトへのアクセス
シトリックス セキュア プライベート アクセス	異常なアップロード量

侵害されたユーザー

このカテゴリは、疑わしいサインインやサインインの失敗など、ユーザーが異常な行動パターンを示すリスクインジケーターをグループ化します。あるいは、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もあります。指定された期間中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洞察を得て、ユーザープロファイルに積極的にアクションを適用することで、このカテゴリに関連するリスクを軽減できます。

侵害されたユーザーのリスクカテゴリは、以下のリスクインジケーターをグループ化します。

データソース	ユーザーリスクインジケーター
シトリックス ゲートウェイ	エンドポイント分析スキャン失敗
シトリックス ゲートウェイ	過剰な認証失敗
シトリックス ゲートウェイ	不可能な移動
シトリックス ゲートウェイ	疑わしいIPからのログオン
シトリックス ゲートウェイ	異常な認証失敗
シトリックス バーチャル アプリ アンド デスクトップ および シトリックス DaaS	不審なログオン
シトリックス バーチャル アプリ アンド デスクトップ および シトリックス DaaS	ありえない移動
マイクロソフト グラフ セキュリティ	Azure AD Identity Protection のリスクインジケーター

データソース	ユーザーリスクインジケーター
マイクロソフト グラフ セキュリティ	Microsoft Defender for Endpoint のリスクインジケーター

侵害されたエンドポイント

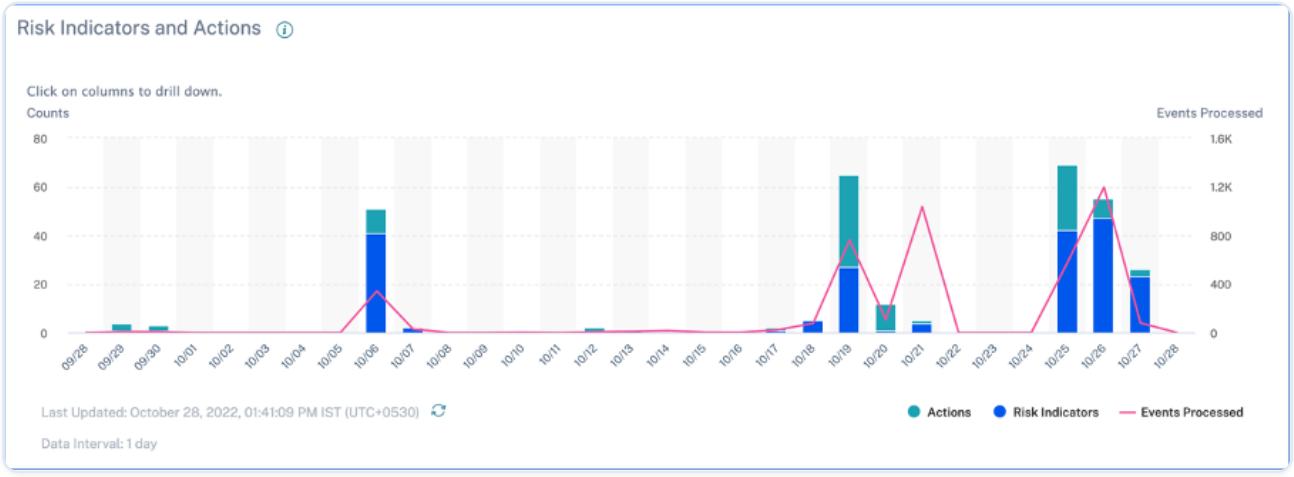
このカテゴリは、デバイスが侵害を示す可能性のある安全でない動作を示した場合にトリガーされるリスクインジケーターをグループ化します。

侵害されたエンドポイントのリスクカテゴリは、次のリスクインジケーターをグループ化します。

データソース	ユーザーリスクインジケーター
シトリックス エンドポイント マネジメント™	管理対象外のデバイスが検出されました
シトリックス エンドポイント マネジメント	ジェイルブレイクまたはルート化されたデバイスが検出されました
シトリックス エンドポイント マネジメント	ブラックリストに登録されたアプリがインストールされたデバイスが検出されました

リスクインジケーターとアクション

選択した期間について、ユーザーに対してトリガーされたリスクインジケーターと適用されたアクションを表示できます。新しい**リスクインジケーターとアクション**棒グラフは、選択した期間から導き出された全体的な時間範囲と棒の間隔で、時間経過に伴うインジケーター、アクション、およびイベントの詳細のカウントを提供します。



インジケーターまたはアクションの棒セグメントをクリックすると、それぞれのインジケーターまたはアクションごとのカウントのドリルダウン視覚化が表示されます。



インジケーターのドリルダウンで、個々のインジケーターの棒をクリックすると、選択した期間に対応するリスクインジケーターページに移動します。

アクセス概要

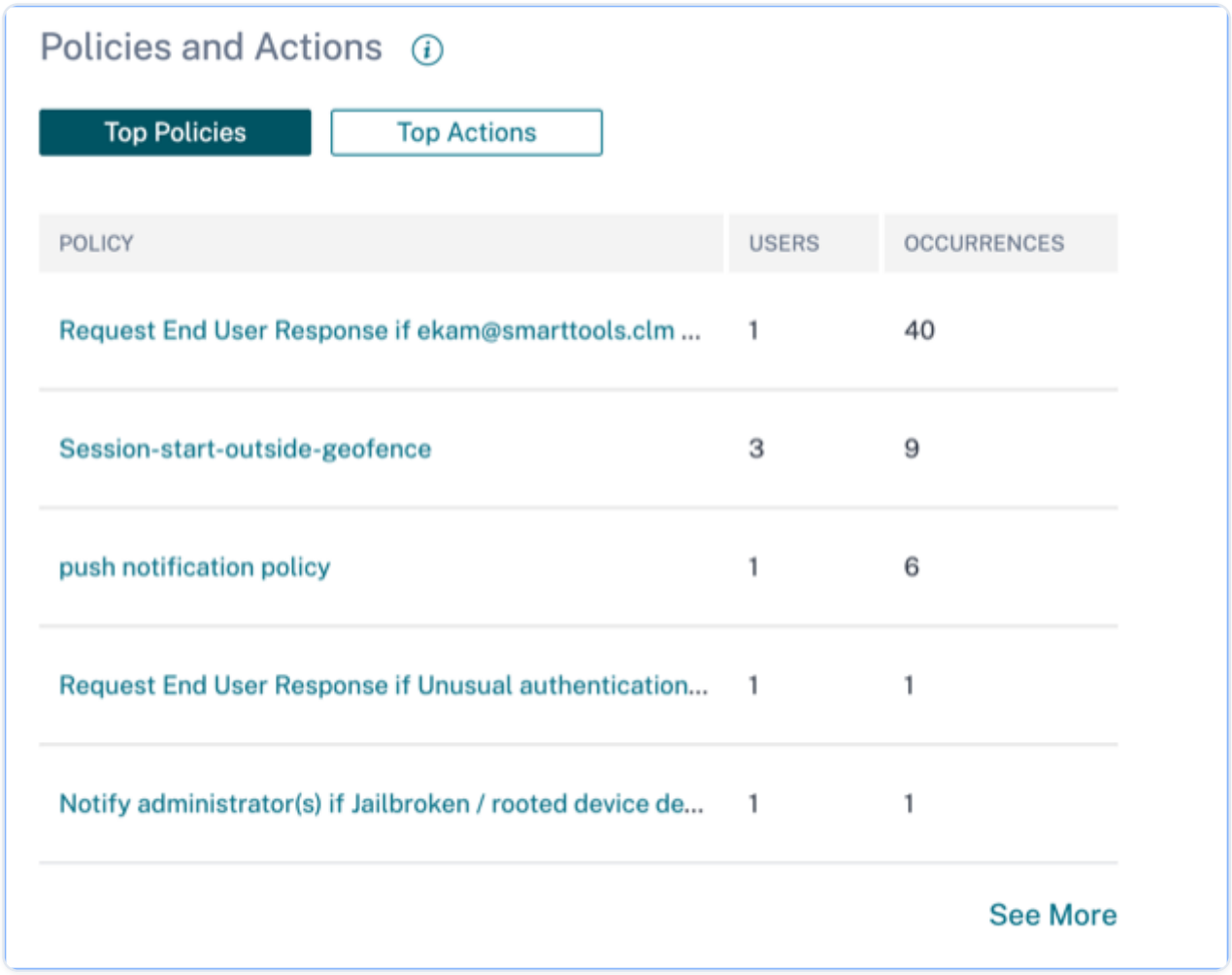
このダッシュボードは、選択した期間のすべてのGatewayアクセスイベントを要約します。Citrix Gatewayを介した合計アクセス数、成功したアクセス数、および失敗したアクセス数を表示します。

グラフ上のポインターをクリックすると、Gatewayのセルフサービス検索ページが表示されます。サインインが成功したシナリオの場合、Gatewayアクセスイベントはページ上のステータスコードによってソートされます。



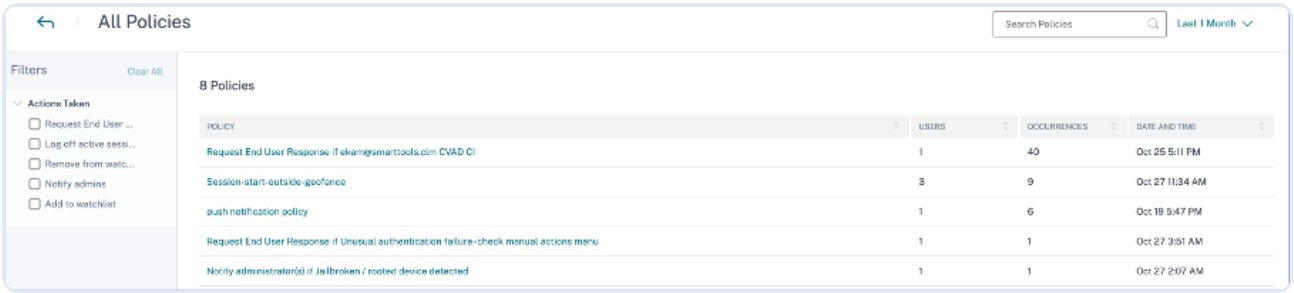
ポリシーとアクション

選択した期間にユーザープロファイルに適用された上位5つのポリシーとアクションを表示します。ポリシーとアクションの詳細については、 ペインの リンクをクリックしてください。



上位のポリシー

設定された上位5つのポリシーは、発生回数に基づいて決定されます。ダッシュボードの セクションで を選択すると、 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。左側のペインでは、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は、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側のペインに表示されます。

上位のアクション

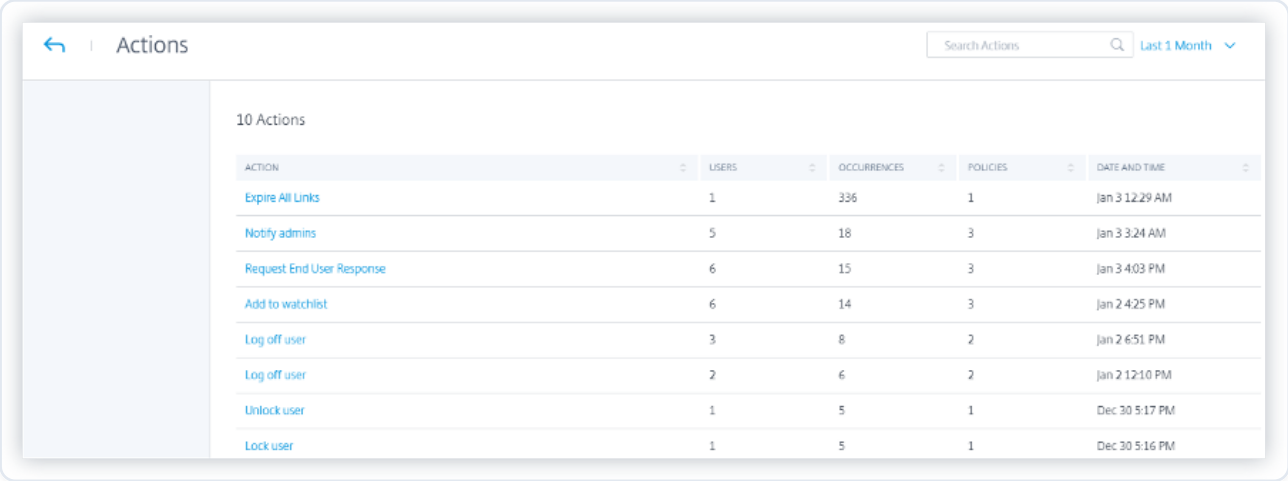
ユーザープロファイルに適用されたポリシーに関連付けられている上位5つのアクションです。このセクションには、ユーザープロファイルに手動で適用したアクションは表示されません。上位のアクションは、発生回数によって決定されます。

をクリックすると、 ページですべてのポリシーベースのアクションを表示できます。

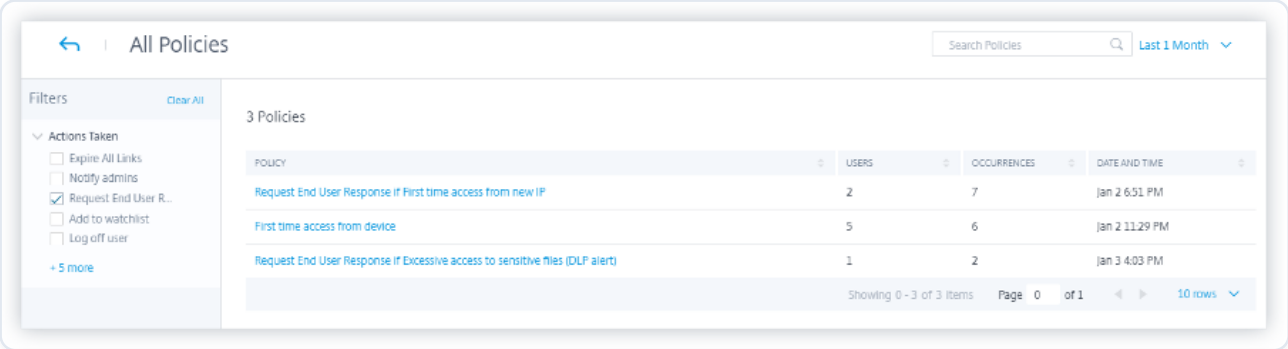
アクション

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。以下の情報が表示されます。

- ポリシーに従って適用されたアクションの名前
- アクションが適用されたユーザーの数
- アクションの発生回数
- 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



関連付けられているすべてのポリシーを表示するには、アクションをクリックします。これらのポリシーは、発生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、**エンドユーザー応答を要求**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。



すべてのポリシーページで、ポリシーをクリックすると、アクションが適用されたユーザーイベントが表示されます。

リスクインジケーター

選択した期間のトップ5のリスクインジケーターを要約します。リスクインジケーターは、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インジケーターの場合、Citrix Analyticsは、検出されたデータソースから、データ処理が有効になっているデータを収集します。

カスタムリスクインジケーターの場合、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。

- シトリックス ゲートウェイ
- シトリックス セキュア プライベート アクセス
- シトリックス バーチャル アプリケーションズ アンド デスクトップ™
- シトリックス DaaS (旧称 シトリックス バーチャル アプリケーションズ アンド デスクトップ サービス)

「**リスクインジケーター**」ペインでは、上位5つのリスクインジケーターを表示し、合計発生回数または重大度に基づいて並べ替えることができます。

リスクインジケーターペイン(/en-us/citrix-analytics/media/risk-indicators-pane.png)

「**リスクインジケーター**」ペインで「**さらに表示**」をクリックすると、「**リスクインジケーターの概要**」ページが表示されます。

リスクインジケーターの概要(/en-us/citrix-analytics/media/risk-indicator-overview.png)

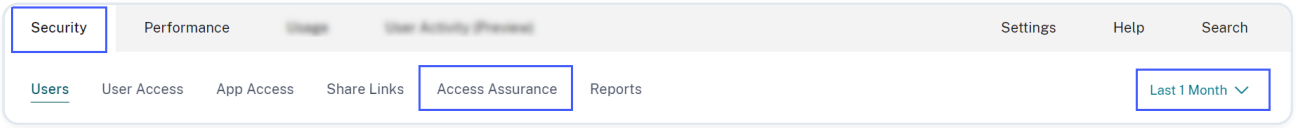
アクセス保証ダッシュボード

リモートワークの増加に伴い、Citrix IT管理者として、ユーザーがCitrix Virtual Apps and DesktopsまたはCitrix DaaS（旧Citrix Virtual Apps and Desktops service）に通常かつ安全な場所からアクセスしていることを確認したいと考えるかもしれません。もし、不明な場所や新しい場所からログオンしたユーザーがいる場合、そのログオン詳細を検証し、Citrix IT環境への脅威を軽減するために必要な措置を講じることができます。

アクセス保証ダッシュボードは、ユーザーが仮想アプリ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を提供します。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 app version matrixを参照してください。

ダッシュボードを表示する

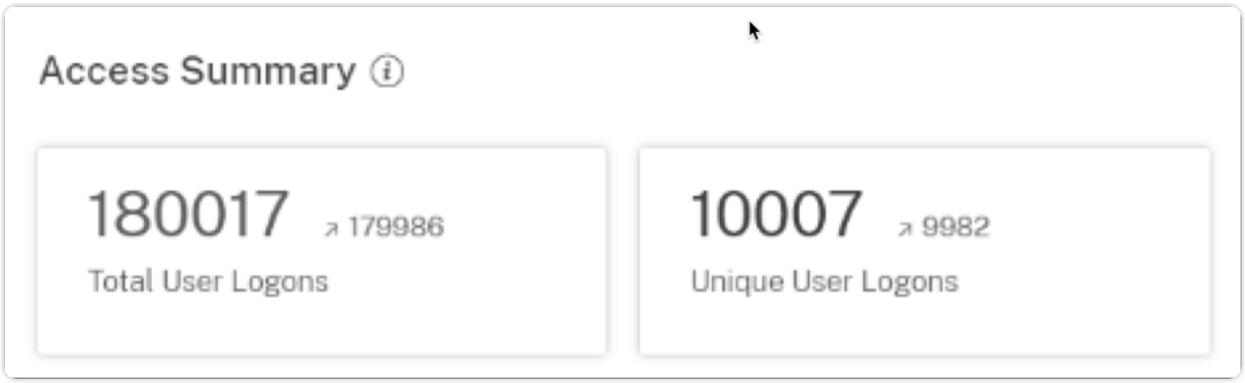
ダッシュボードを表示するには、**セキュリティ > アクセス保証**をクリックします。ログオン詳細を表示したい期間を選択します。



アクセスの概要

ダッシュボードの概要セクションには、選択した期間について以下の情報が表示されます。

1. (全世界の)すべての場所からのユーザーログオンの総数。
2. (全世界の)すべての場所からのユニークユーザーログオンの総数。



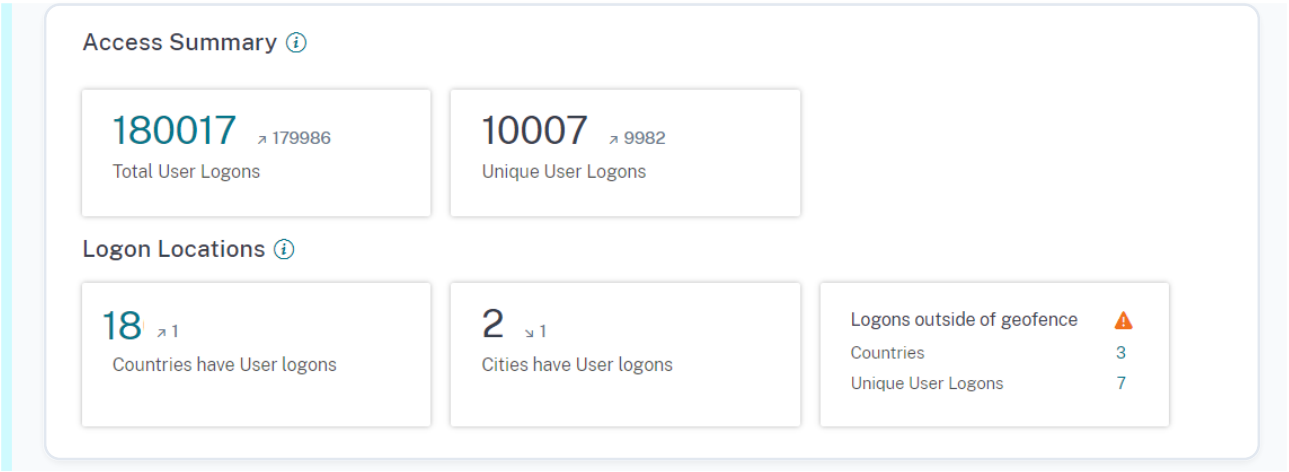
ログオン場所

ログオン場所セクションには、選択した期間について以下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。
- geofencingエリア内の国とユニークユーザーログオンの総数。geofencingエリアからのログオン詳細を表示するには、geofencingを有効にする。
- ユニークユーザーログオンが多い上位10か所。上位のユニークユーザーログオンは、不明な都市や国からのものである場合もあり、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か所のサブセットです。一部の場所が特定されない理由については、利用不可として識別された場所を参照してください。

全世界の総ユーザーログオン数と全世界の総ユニークユーザーログオン数の上昇または下降トレンドも表示できます。上位10か所については、**DEVIATION**列に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、選択された期間と、同じ長さの前の期間に基づいています。たとえば、期間として**過去1か月**を選択した場合、ユーザーログオンのトレンドと偏差は、過去1か月と前々月で比較されます。

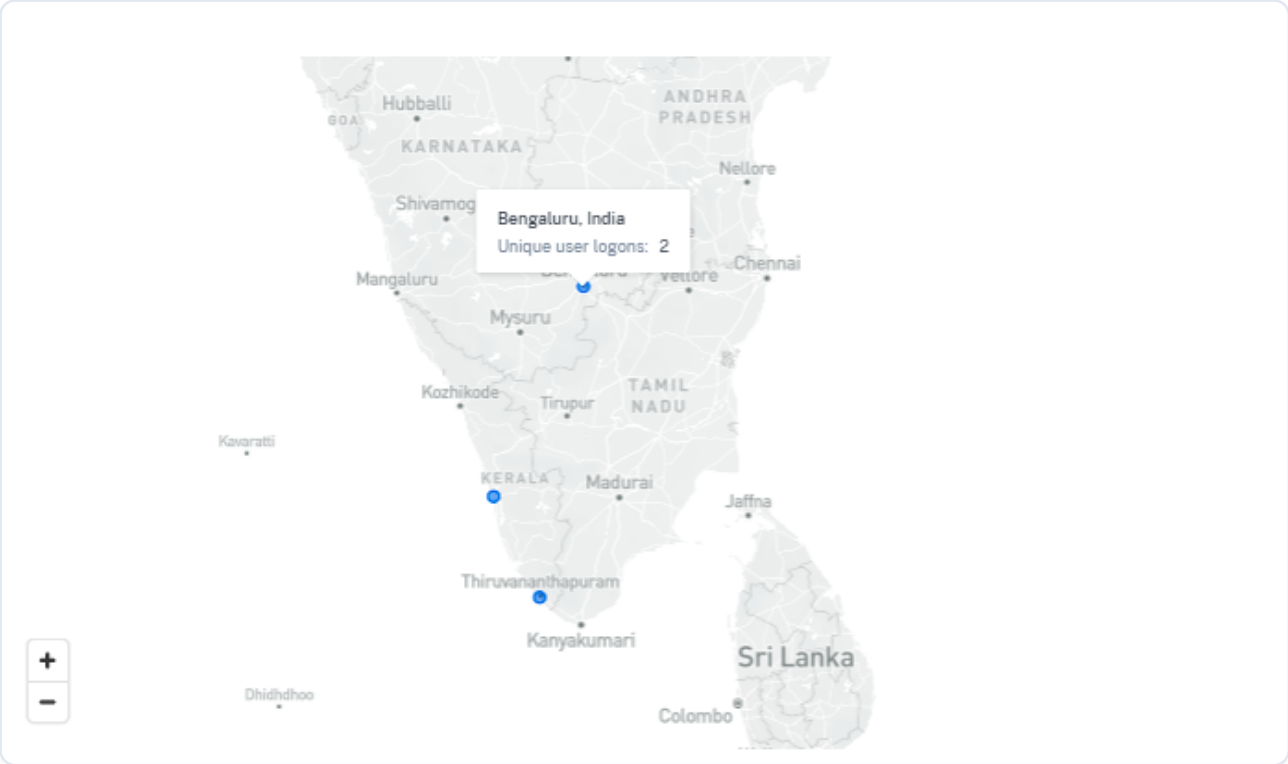
> **注**
>
> 場所の情報は都市および国レベルで提供され、正確な地理的位置を表すものではありません。Access assurance、Geolocation の詳細については、FAQを参照してください。



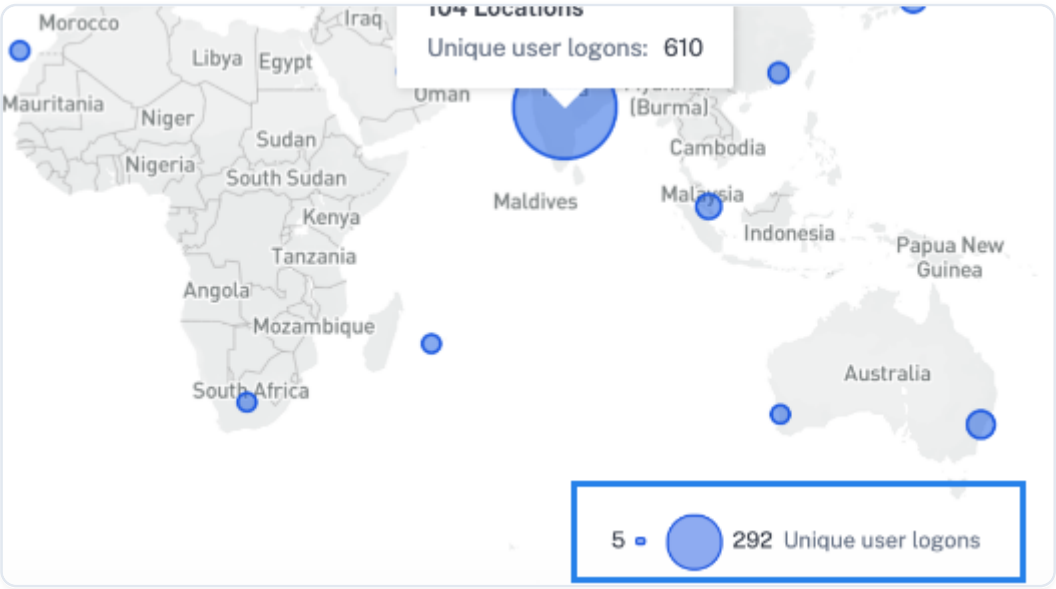
上位10のユニークログオン場所テーブルで、場所を選択すると、ユーザーとそのアクセスプロファイルおよびログオン詳細を表示できます。



マップには、選択した期間における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、場所を拡大すると、その場所からのユニークユーザーログオンの総数を表示できます。青いバブルをクリックすると、場所のアクセス詳細を表示できます。



マップの右下隅には、ユニークユーザーログオンの範囲が表示されます。選択した期間について、小さいバブルは場所全体のユニークユーザーログオンの最小数を示します。大きいバブルは場所全体のユニークユーザーログオンの最大数を示します。



利用不可として識別された場所

上位10のユニークログオン場所テーブルで、一部の場所が不明または利用不可として表示される場合があります。不明な場所をクリックすると、**ユーザーログオン**ページで対応するユーザーログオンの詳細を表示できます。

ユーザーログオンページでは、国または都市の情報が利用できない場合、**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、場所情報が利用できない理由が表示されます。

場所が利用できません(/en-us/citrix-analytics/media/access-location-null-locations.png)

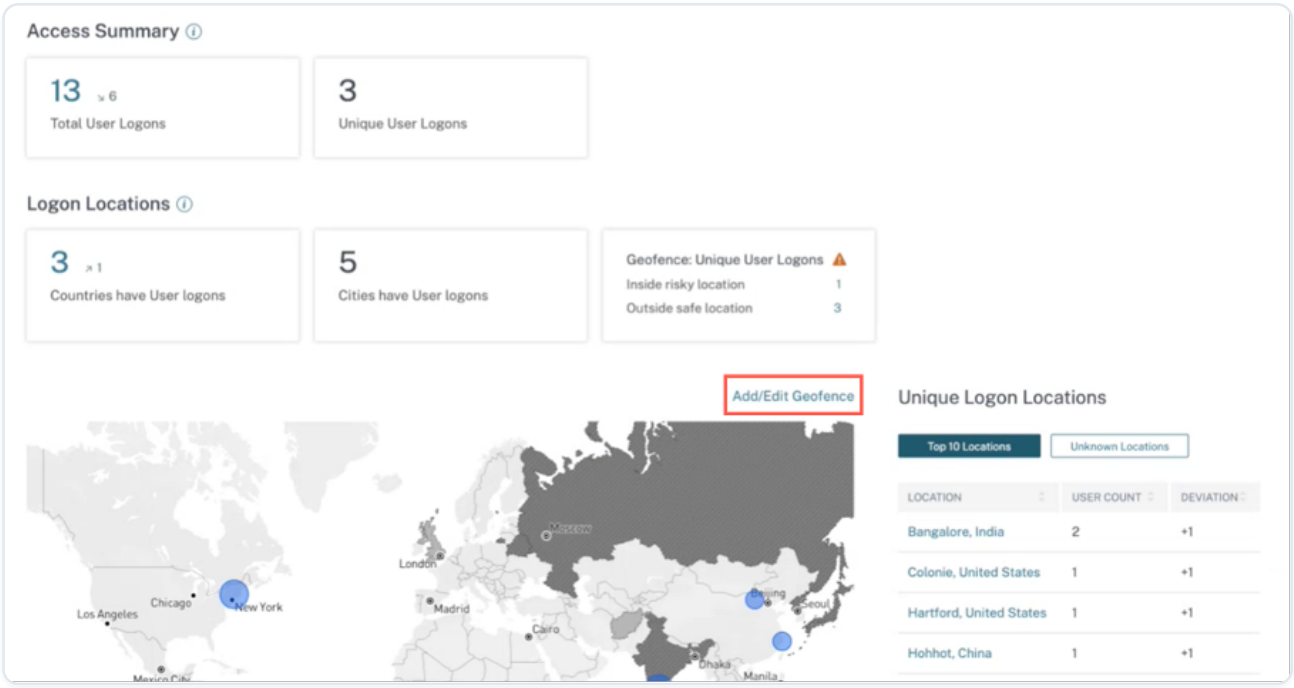
場所が利用できない場合、次のいずれかのシナリオが表示されることがあります。

シナリオ	理由
市名と国名が利用できません。	次のいずれか：
	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。場所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てください。
	1. ユーザーのネットワークのパブリックIPアドレスが利用できないため、Citrix Analyticsは場所を特定できません。
	1. 外部の地理位置情報サービスがCitrix Analyticsに場所情報を送信できません。
プライベートIPを持つ場所	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ります。この場合、Citrix Analyticsは場所情報を利用できません。
国名は利用可能ですが、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範囲は外部の地理位置情報サービスで難読化されています。そのため、Citrix Analyticsは場所情報を利用できません。

ジオフェンシングを有効にする

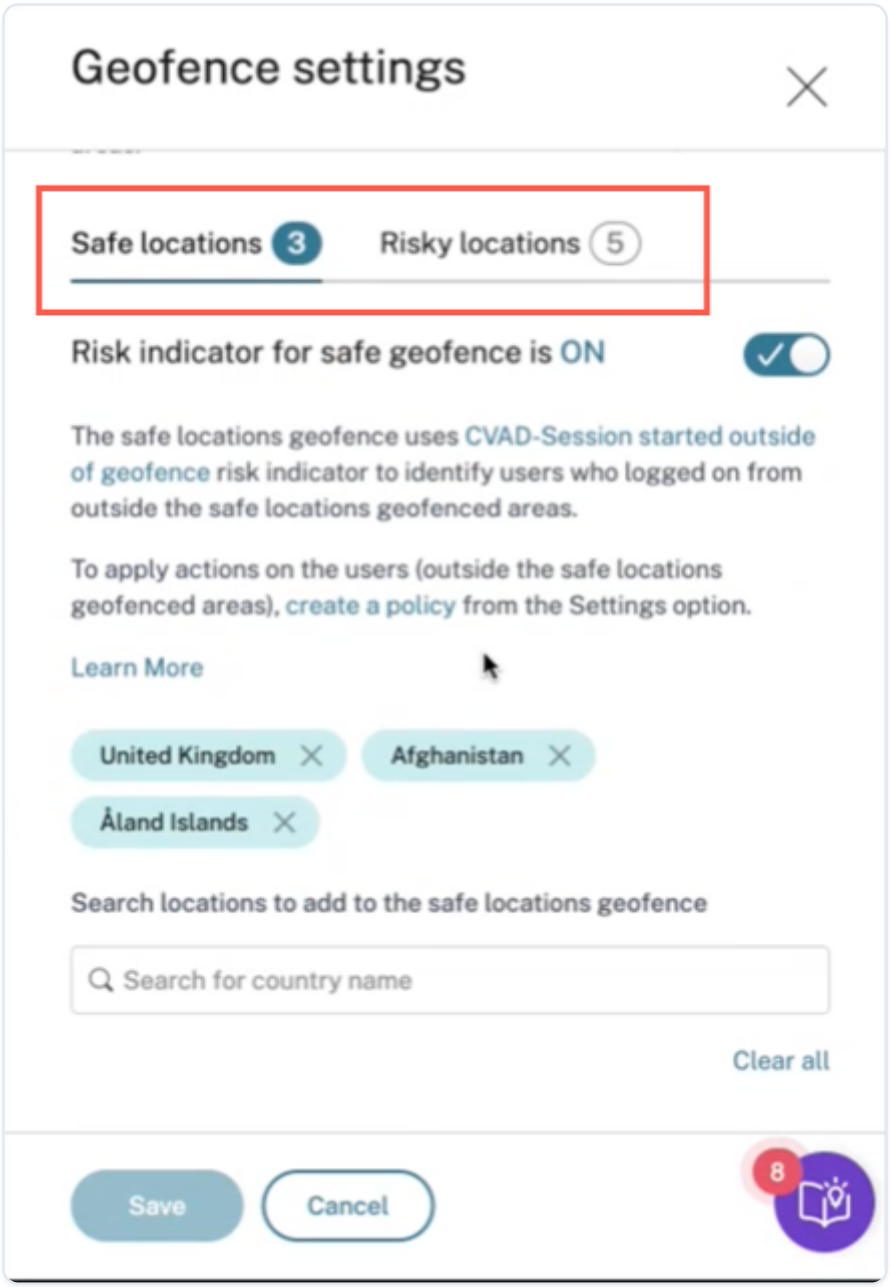
ジオフェンシングは、安全なジオフェンス外および危険なジオフェンス内から仮想アプリまたは仮想デスクトップにアクセスするユーザーを特定するのに役立ちます。**アクセス概要**ページを表示するには、**セキュリティ > アクセス保証**に移動します。

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。ジオフェンスを設定するには、**ジオフェンスの追加/編集**をクリックします。

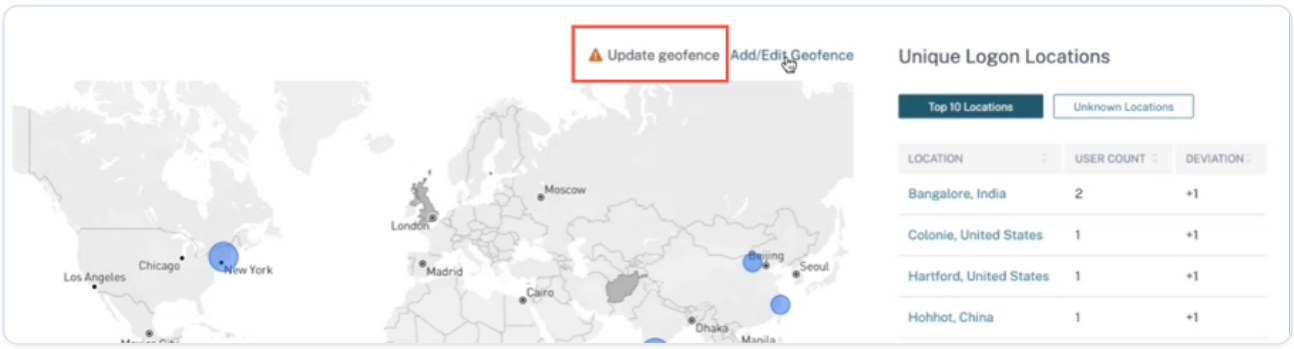


ジオフェンス設定ウィンドウに2つのタブが表示されます。

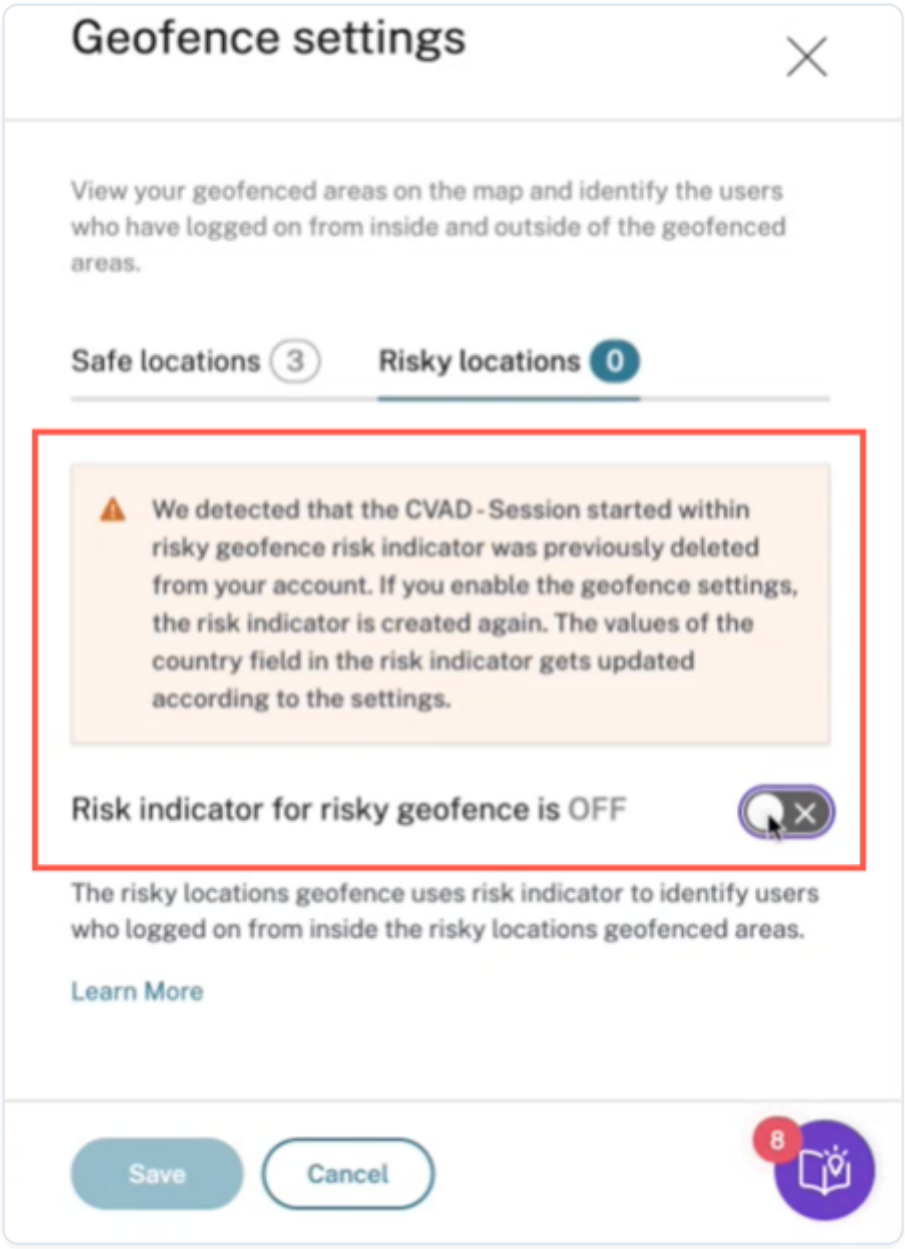
- **安全な場所**: 安全な場所に該当する国を設定または削除できます。
- **危険な場所**: 危険な場所に該当する国を設定または削除できます。 各タブで設定されている安全な場所と危険な場所の合計数も表示できます。安全な場所のジオフェンスまたは危険な場所のジオフェンスから国を削除するには、国の横にある閉じる (X) 記号をクリックします。**保存**をクリックしてジオフェンス設定を保存します。



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。危険な場所のジオフェンスにリスクインジケーターが追加されていない場合、またはリスクインジケーター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**という警告メッセージが表示されます。



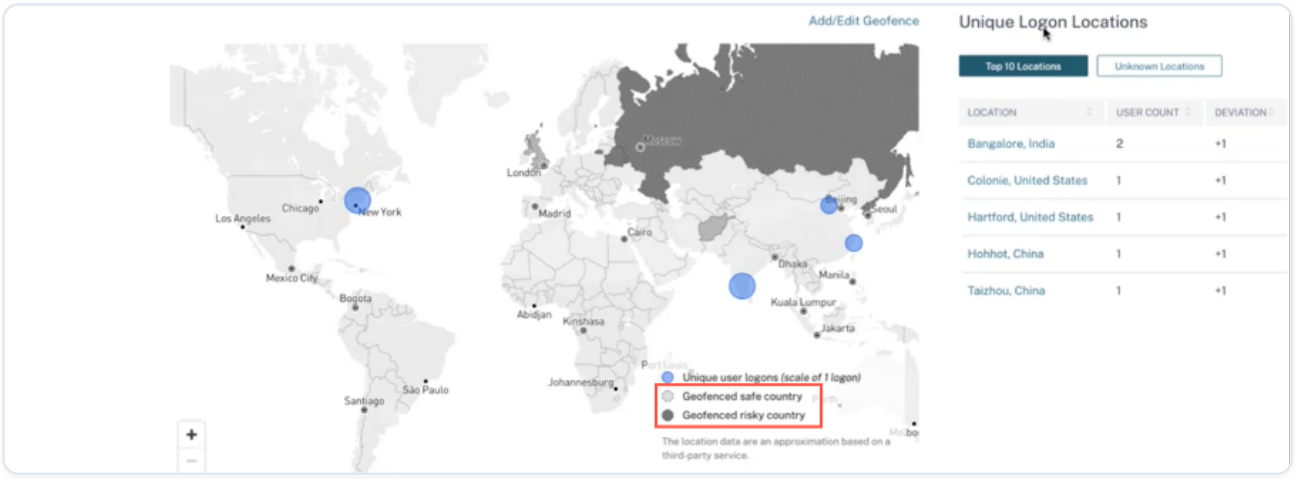
インジケーターを再作成するには、**危険な場所**タブに移動し、**危険なジオフェンスのリスクインジケーター**トグルをオンにします。



インジケーターは、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、ジオフェンスで保護された安全な国と危険な国も表示されます。

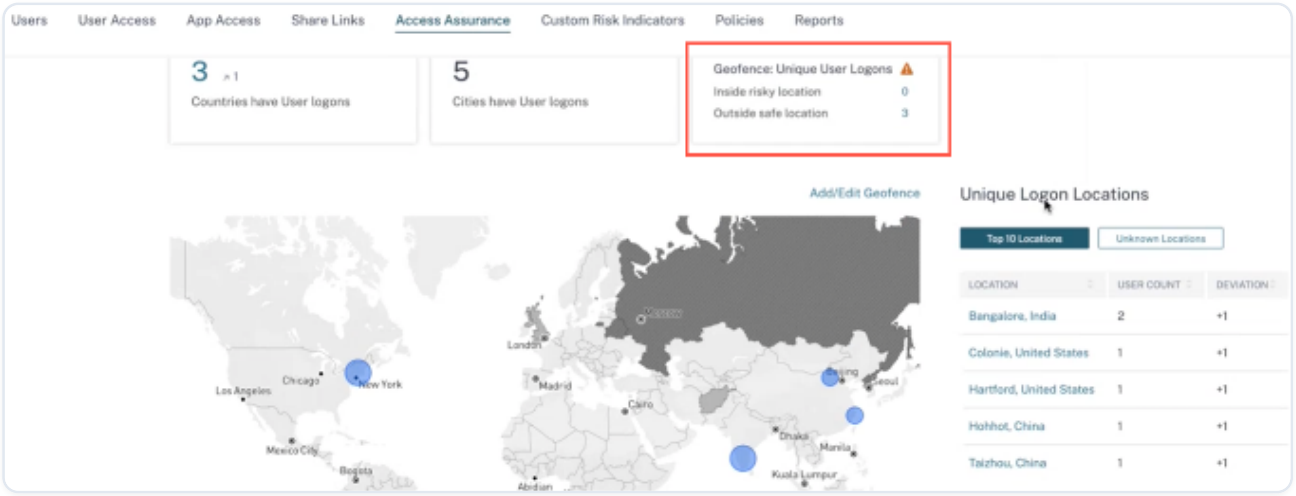
- ジオフェンスで保護された安全な国は、薄い灰色の円でマークされています。
- ジオフェンスで保護された危険な国は、濃い灰色の円でマークされています。



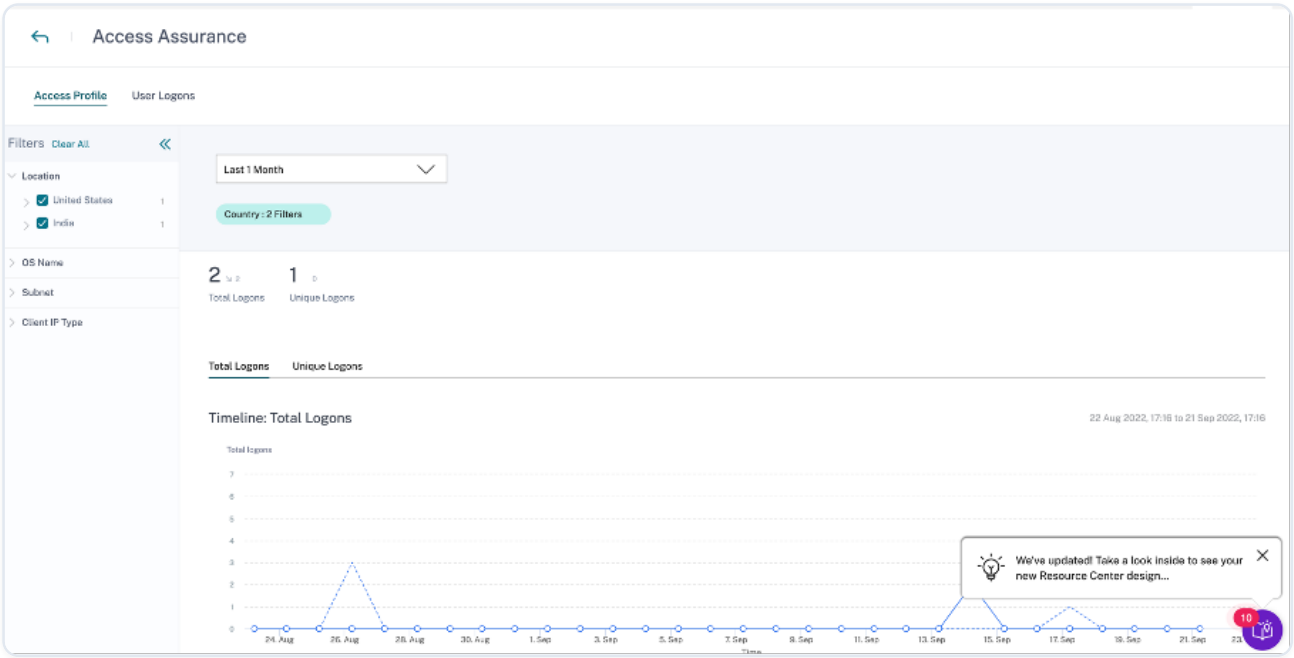
ジオフェンス: ユニークユーザーログオン

アクセス概要ページに移動して、「ジオフェンス: ユニークユーザーログオン」を表示します。このカードには、危険な場所の内側と安全な場所の外側の数が表示されます。

- **危険な場所の内側**: 危険な場所のジオフェンスエリア内からログオンしたユーザーを特定します。
- **安全な場所の外側**: 安全な場所のジオフェンスエリア外からログオンしたユーザーを特定します。



合計およびユニークユーザーログオンの詳細な概要については、「危険な場所の内側」または「安全な場所の外側」の横にある数字をクリックしてください。



この機能では、次の事前設定されたカスタムリスクインジケーターを使用します。

- **CVAD-セッションがジオフェンス外で開始されました**: 安全なジオフェンス外からのユーザーログオンを監視するため。
- **CVAD-セッションが危険なジオフェンス内で開始されました**: 危険なジオフェンス内からのユーザーログオンを監視するため。

ジオフェンス外でユーザーログオンが検出された場合、リスクインジケーターがトリガーされ、ジオフェンス外で開始されたセッション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要求*」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に適切な措置を講じることができます。詳細については、事前設定されたカスタムリスクインジケーターを参照してください。

注

- **ジオフェンス設定**で国を変更すると、「*CVAD-セッションがジオフェンス外で開始されました*」リスクインジケーターも更新されます。
- 例えば、オーストラリアとインドを新しいジオフェンス国として選択して保存すると、リスクインジケーターの事前設定された条件が、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国である米国を削除することもできます。

  リスクインジケーター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、リスクインジケーターの条件:

```
Event-Type = \"Session.logon\" AND Country != \"\" AND Country ~ \"\"
AND Country NOT IN (\"Australia\", \"United States\", \"India\"
```

- *CVAD-Session started outside of geofence* リスクインジケーターが以前にアカウントから削除されている場合、**ジオフェンス設定**を有効にすると、リスクインジケーターが再度作成されます。リスクインジケーターのジオフェンス国は、**ジオフェンス設定**から制御されます。

ジオフェンス設定を有効にすると、マップにはジオフェンスされたエリアと、これらのエリアからのユニークなユーザーログオンが表示されます。

ログオンネットワーク

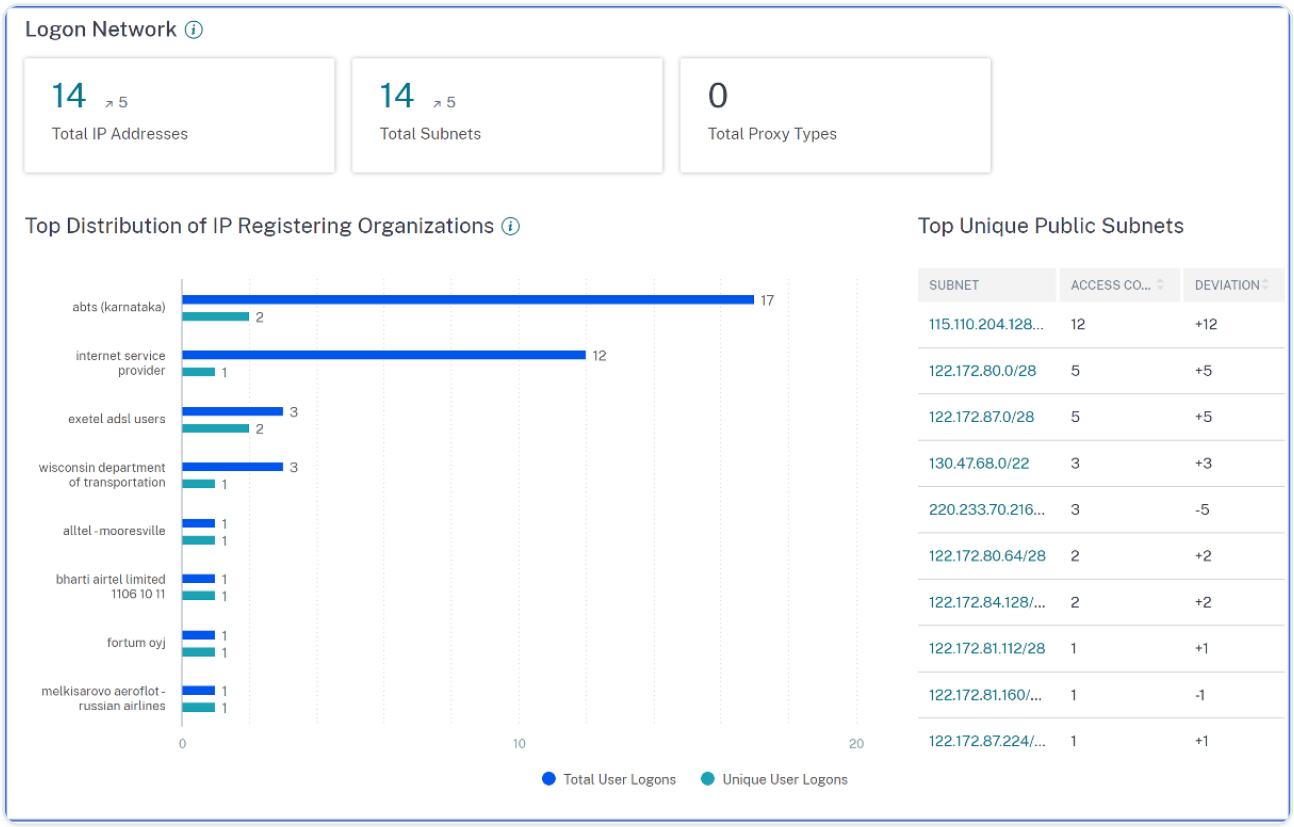
Access Assuranceダッシュボードで、以下の追加のユーザー詳細を表示できるようになりました。

- ユーザーがログオンしたIPアドレスに関連付けられている組織。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エンティティが含まれます。
- ユーザーがログオンした合計ユニークなパブリックサブネットとプライベートサブネット。
- ユーザーがプロキシおよびプライベートVPNサービスを使用してログオンした詳細。

これらの追加の詳細を使用することで、管理者として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内にあることを確認できます。

ユーザーネットワークの詳細を表示

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**の下の詳細を表示します。



- **合計IPアドレス**: 仮想セッションにログオンするために使用されたユニークなIPアドレスの総数を示します。
- **合計サブネット**：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。
- **合計プロキシタイプ**：サーバーがユーザー接続をプロキシするために利用したネットワークまたはプロトコルの総タイプ数を示します。
- **IP登録組織のトップ分布**の下で、各組織（ISP）からの合計ユーザーログオンと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、選択した組織に関連付けられたユーザーの詳細、アクセスプロファイル、およびログオン詳細をドリルダウンして表示できます。
- **合計固有パブリックサブネット**の下で、サブネットの概要、各サブネットからの合計ユーザーログオン、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、選択したサブネットに関連付けられたユーザーの詳細、アクセスプロファイル、およびログオン詳細をドリルダウンして表示できます。

ユーザーのアクセスプロファイルを表示する

いずれかのメトリック（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または仮想デスクトップへのユーザーのアクセス概要が表示されます。固有のログオンまたは合計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。

固有および合計ユーザーログオン(/en-us/citrix-analytics/media/unique-and-total-user-logon.png)

選択したメトリック（場所、組織、またはサブネット）のトップアクセスイベントを表示できます。この情報は、アクセスパターンと脅威調査および分析の詳細を確認するのに役立ちます。

合計ユーザーログオンと固有ユーザーログオンの増加または減少傾向は、選択された期間と、それと同じ長さの前の期間に基づいて比較されます。たとえば、期間として「**過去1か月**」を選択した場合、傾向は過去1か月と過去2か月の間で比較されます。

アクセスプロファイルページビュー(/en-us/citrix-analytics/media/access-profile-page.png)

ファセット

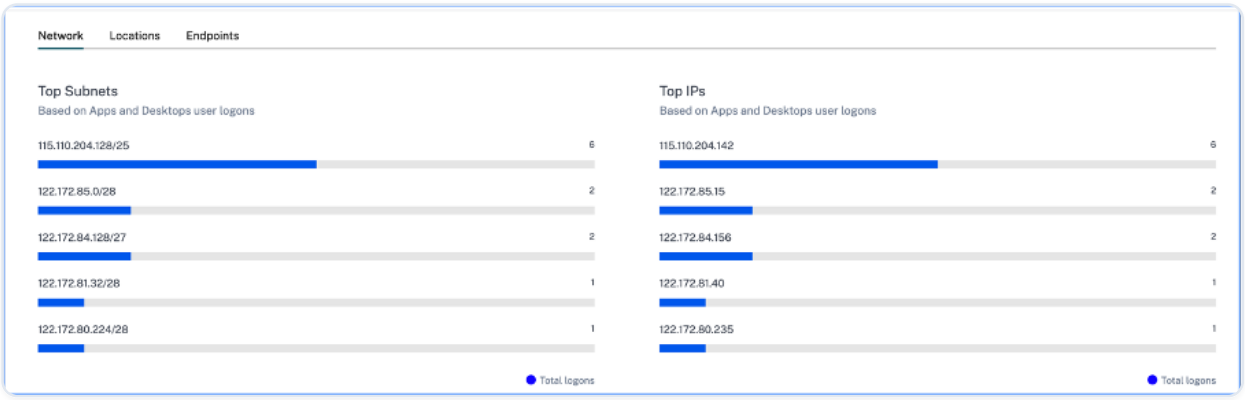
アクセスイベントには、以下のファセットを使用できます。

- **場所**- アクセスイベントを国と都市でフィルタリングします。
- **OS**- アクセスイベントをオペレーティングシステムとそのバージョンで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た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。

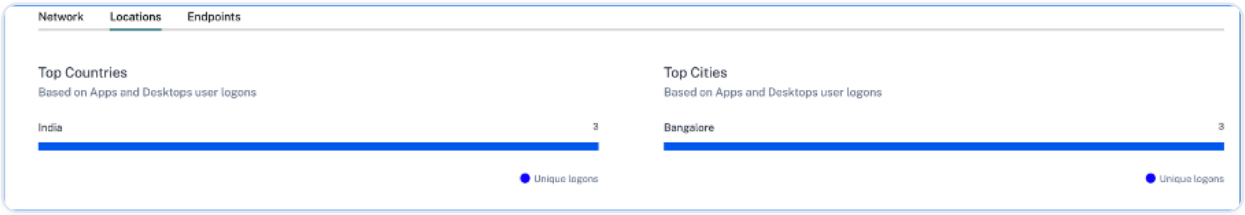
> **注**
>
> データが利用できないか、識別されていない場合、「利用不可」ラベルが表示される場合があります。

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ユニークユーザーログオン数について次の情報を表示します。

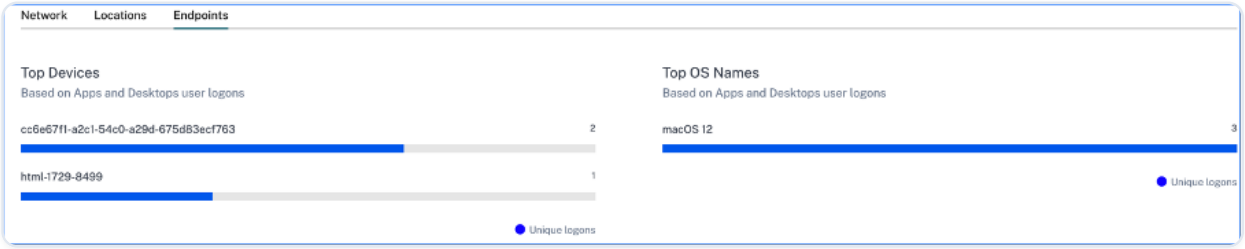
- **ネットワーク** - ユーザーが仮想アプリまたは仮想デスクトップにログオンした上位のサブネットとIPアドレス。



- **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いた上位のデバイス名とOS名。



ユーザーのログオン詳細を表示する

ユーザーログオンページには、選択した場所からの仮想アプリ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、脅威の調査と分析に役立ちます。

ユーザーログオンページ(/en-us/citrix-analytics/media/access-assurance-logon-page.png)

DATAテーブルには、選択した場所と期間について、以下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、ユーザーのIPアドレスの種類。
- **都市と国**。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場所。
- **デバイスID**。ユーザーデバイスの識別コード。

- **OS名**。ユーザーデバイス上のオペレーティングシステム。詳細については、「Self-service search for Apps and Desktops」を参照してください。

  ユーザーログオンデータテーブル(/en-us/citrix-analytics/media/user-logon-data-table.png)

各イベントを展開すると、以下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。詳細については、「Self-service search for Apps and Desktops」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。詳細については、「Self-service search for Apps and Desktops」を参照してください。
- **Workspaceアプリバージョン**。Citrix Workspace™アプリまたは Citrix Receiverのビルドバージョン。

  アクセスログオンデータテーブル(/en-us/citrix-analytics/media/access-logon-data-table.png)

DATAテーブルで、以下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。
- **並べ替え**をクリックし、データ要素を選択して複数列の並べ替えを実行します。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形式でエクスポート**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、分析に利用できます。

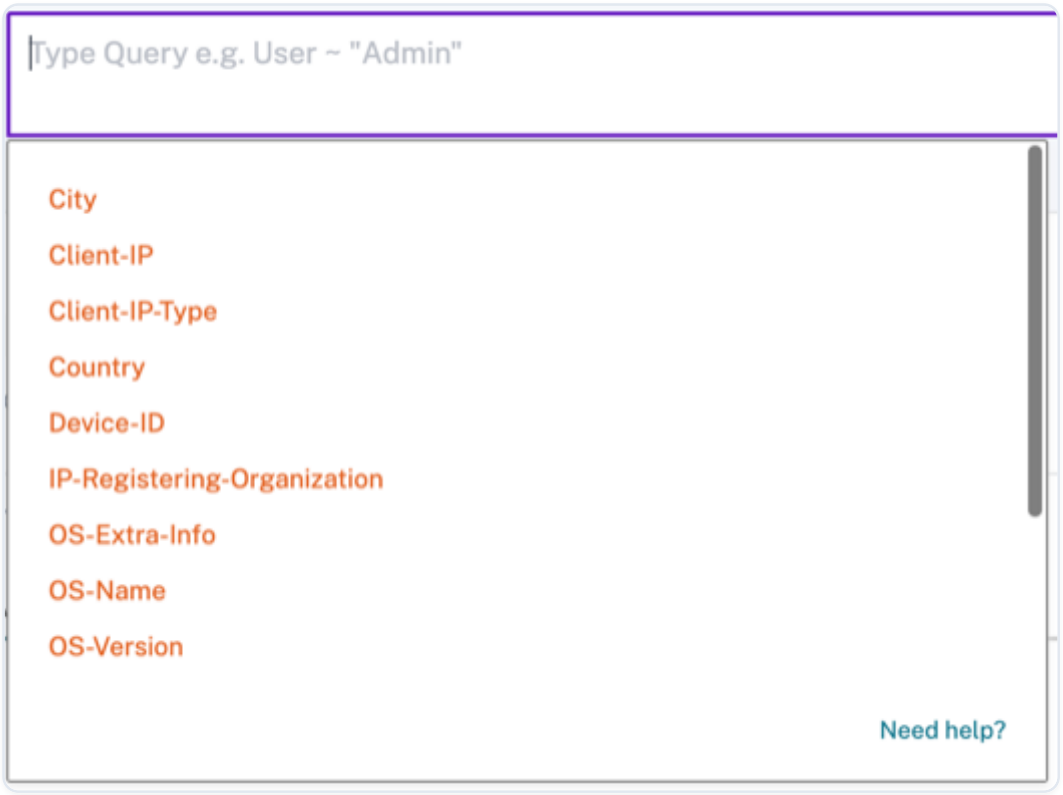
検索バー

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、検索バーで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対して、以下のファセットを使用できます。

- **場所** - ログオンイベントを国と都市でフィルタリングします。
- **OS** - ログオンイベントをオペレーティングシステムとそのバージョンで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** - 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** - ユーザーが利用したISPでアクセスイベント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**
>
> データが利用できないか、または識別できない場合、「利用不可」というラベルが表示されることがあります。

ユーザーリスクタイムラインとプロファイル

> **注**

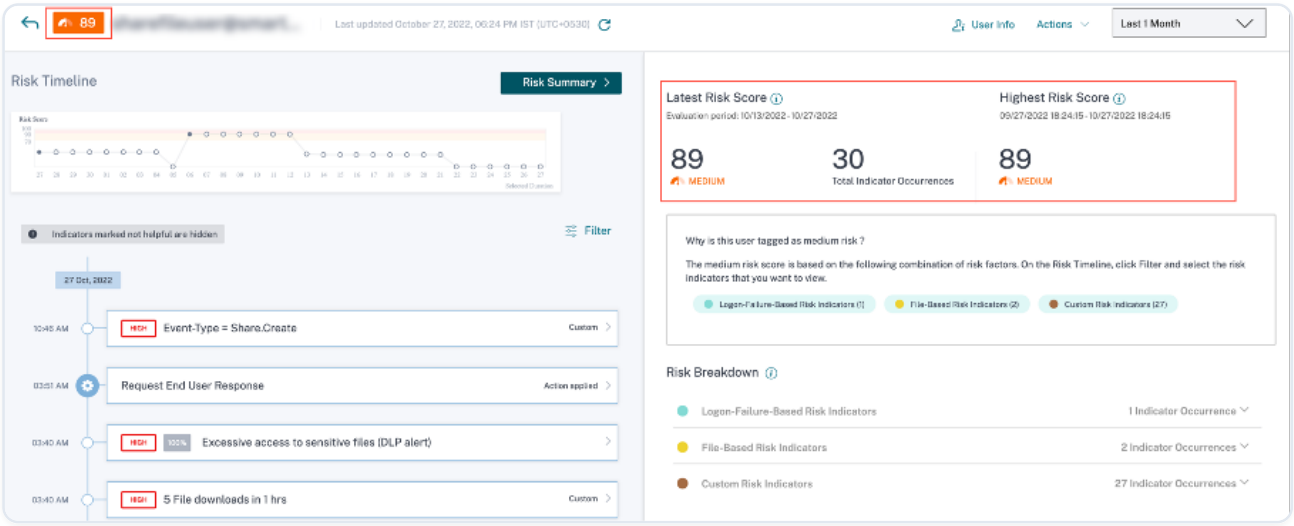
> **注意**: Citrix Content Collaboration™ および ShareFile はサポート終了となり、ユーザーは利用できなくなりました。

> ユーザープロファイル上のユーザーリスクタイムラインにより、Citrix Analytics 管理者はユーザーの危険な行動についてより深い洞察を得ることができます。デフォルトでは、ユーザーリスクタイムラインは過去1か月間表示されます。選択した期間にアカウントに対して実行された対応するアクションも確認できます。ユーザーリスクタイムラインから、ユーザープロファイルをさらに深く掘り下げて、次のことを理解できます。

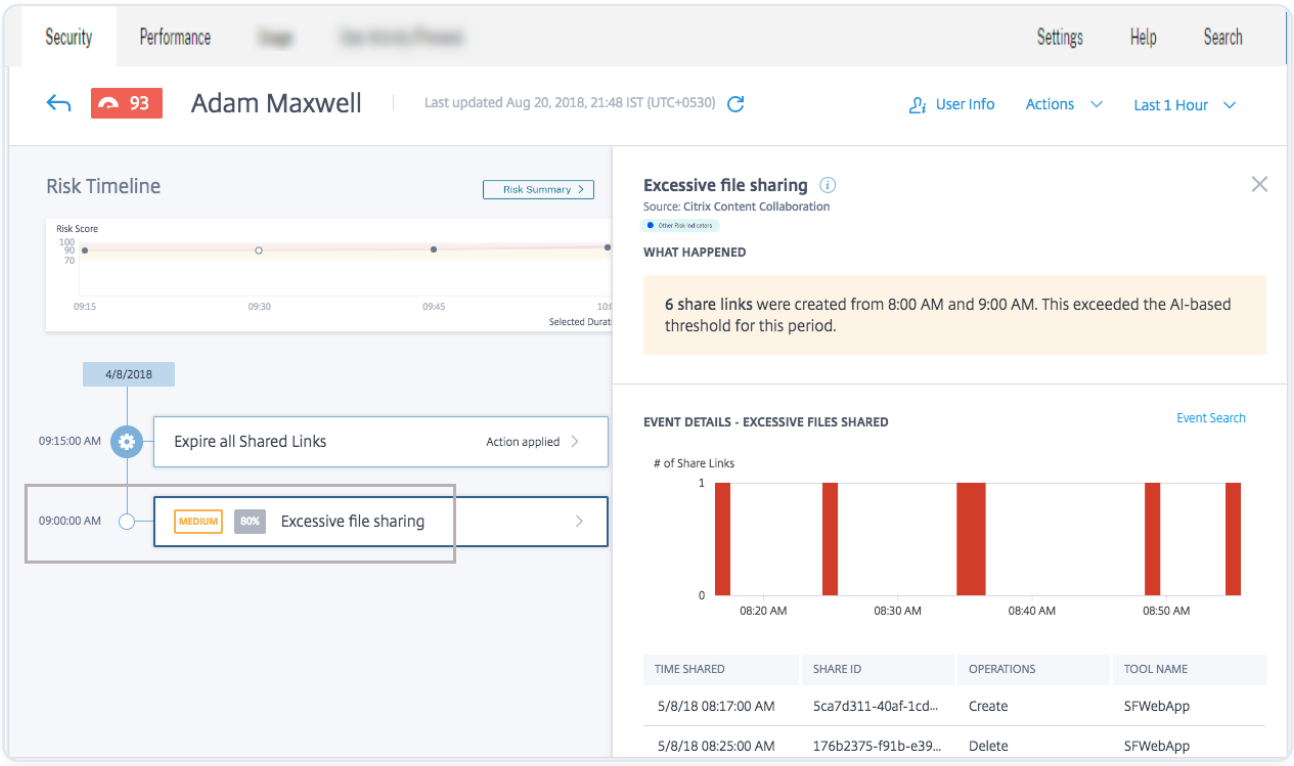
- アプリケーションの使用状況
- データ使用状況
- デバイス使用状況
- 場所の使用状況

また、ユーザーのリスクスコアとリスクインジケータの傾向を表示し、そのユーザーが高リスク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で、ユーザーの最新のリスクスコアを表示できます。**リスク概要**ビューレポートには、最新の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、リスクインジケータまたはアカウントに適用された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インジケータ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。



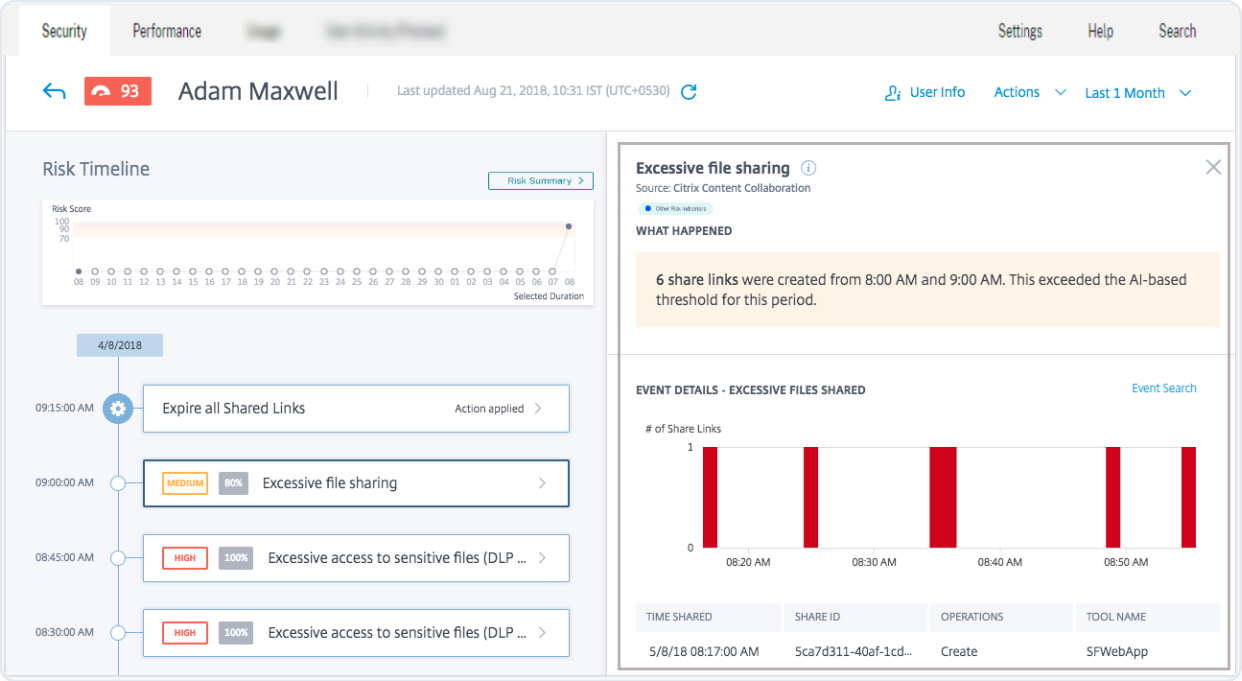
リスクタイムライン

リスクタイムラインには、次の情報が表示されます。

- **リスクインジケーター**。リスクインジケーターとは、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行動から逸脱した場合にトリガーされます。リスクインジケーターは、以下のデータソースに対応しています。

- シトリックス コンテンツ コラボレーション
- シトリックス ゲートウェイ
- シトリックス エンドポイント マネジメント™
- シトリックス バーチャルアプリ&デスクトップ または シトリックス DaaS (旧称 シトリックス バーチャルアプリ&デスクトップ サービス)
- シトリックス セキュア プライベート アクセス

ユーザーのタイムラインからリスクインジケーターを選択すると、右ペインにリスクインジケーター情報セクションが表示されます。リスクインジケーターの理由とイベントの詳細を表示できます。これらは、以下のセクションに大別されます。



- **何が起こったか**。ここでは、リスクインジケーターの概要を表示できます。たとえば、**過剰なファイル共有**リスクインジケーターを選択した場合、「何が起こったか」セクションで、受信者に送信された共有リンクの数と共有イベントが発生した日時を表示できます。
- **イベントの詳細**。個々のイベントエントリを、イベントの詳細とともにグラフィカル形式および表形式で表示できます。**イベント検索**をクリックすると、セルフサービス検索ページにアクセスし、ユーザーのリスクインジケーターに対応するイベントを表示できます。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。
- **追加のコンテキスト情報**。このセクションでは、イベント発生時に共有されたデータ（もしあれば）を表示できます。

リスクインジケーターを手動で「役立つ」または「役立たない」とマークできます。詳細については、ユーザーリスクインジケーターのフィードバックを提供するを参照してください。

詳細情報: リスクインジケーター

- **アクション**。アクションは、疑わしいイベントに対応し、将来の異常な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アカウントに自動的に適用されるか、特定のアクションを手動で適用できます。

  詳細情報: ポリシーとアクション。

  リスクタイムラインのアクション(/en-us/citrix-analytics/media/risk-timeline-actions.png)

- **特権ユーザーイベント**。ユーザーの管理者またはエグゼクティブの特権ステータスに変更があるたびに、特権ユーザーイベントがトリガーされます。ユーザーに対してリスクインジケーターがトリガーされた場合、指定された特権ステータス変更イベントと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。ユーザーの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の特権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
  - 管理者権限に昇格しました
  - 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。**エグゼクティブグループに追加されました**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。その後、Adamはファイルやフォルダーを過度に削除し始め、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。**過剰なファイルまたはフォルダーの削除**リスクインジケーター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インジケーターを比較できます。比較後、リスクインジケーター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、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。

ユーザーのタイムラインからイベントを選択すると、イベント情報セクションが右ペインに表示されます。

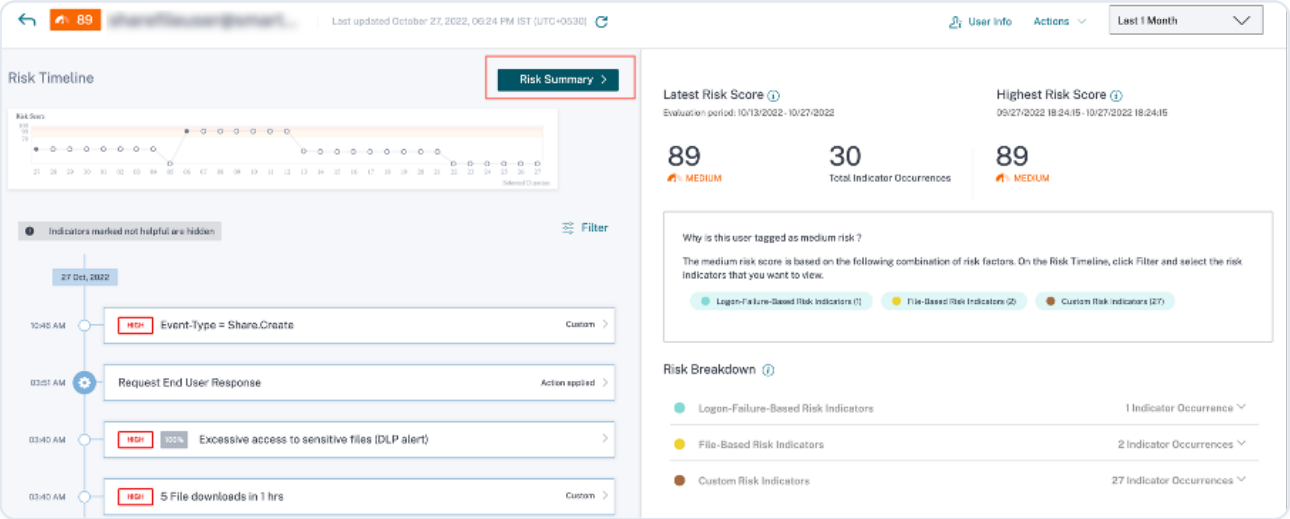
エグゼクティブの場合、右ペインには**ユーザーの状態**、**日付と時刻**、**Active Directoryグループ**などの情報が表示されます。

特権ユーザー(/en-us/citrix-analytics/media/privileged-user-risk-timeline.png)

管理者特権イベントの場合、右ペインには**ユーザーの状態**、**日付と時刻**、**製品内**などの情報が表示されます。

リスクの概要

View the risk factors associated with the user that contributed to their risk score. You can see the risk score details taken as the maximum over the selected time period, along with the latest score and corresponding risk indicator count. Upon navigation to the User Timeline from either the main landing page or the Risky Users page, the time selection is preserved from the source page. For more information about the risk factors, see Citrix user risk indicators.

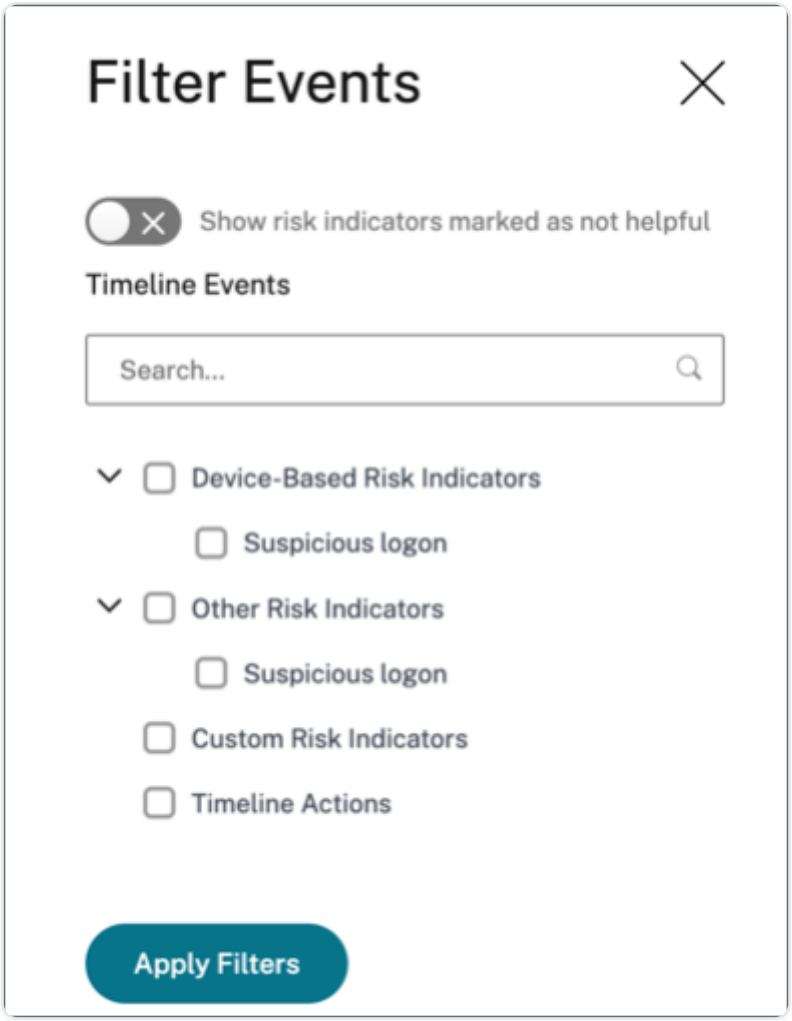


「**リスク概要**」をクリックして、次の情報を表示します。

- **最新のリスクスコア**：最新のリスクスコアは、最近の行動に基づいてユーザーの現在のリスクを示します。リスクスコアは、過去2週間にわたってユーザーが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あり、ユーザー行動分析に基づいて変化します。このスコアに基づいて、ユーザーは次のいずれかのカテゴリに分類されます：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。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。
    - **インジケーターの合計発生数**：過去2週間にユーザーによってトリガーされたリスクインジケーターの合計数を示します。これらのトリガーされたリスクインジケーターがユーザーのリスクスコアを決定します。
- **最高リスクスコア**：最高リスクスコアは、選択された期間内にこのユーザーに対して計算されたリスクスコアの最大値を示します。これはユーザーの集計リスクを表すものであり、必ずしも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。

- **リスクの内訳**：各リスク要因についてユーザーによってトリガーされたリスクインジケーターの数を示します。詳細を表示するには、行を展開してください。

ユーザータイムラインで、**フィルター**をクリックし、ユーザーに関連付けられたリスク要因、適用されたアクション、または特権ユーザーのステータスを選択して、対応するイベントを表示します。



ユーザープロファイル

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以下のユーザー情報が表示されます。

- 役職
- 住所
- メール
- 電話
- 場所

- 組織


Last updated March 10, 2023, 05:44 PM IST (UTC+0530)
User Info
Actions
Last 1 Month
9980058254
agautam@ibco.com
Ulsoor Road, Bangalore, Karnataka, IN, 560075
Job Title: Sr SW Test Engineer 2
Location: Bangalore
Organization: Citrix R&D India Pvt. Ltd

Citrix® ユーザーリスクインジケーター

> **注**

> **注意**: Citrix Content Collaboration™ および ShareFile は、サポート終了 (EOL) に達し、ユーザーは利用できなくなりました。

> ユーザーリスクインジケーターは、疑わしいと思われる、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。これらのリスクインジケーターは、展開で使用されているすべてのCitrix製品にわたって適用されます。リスクインジケーターは、ユーザーの行動が通常から逸脱した場合にトリガーされます。各リスクインジケーターには、1つ以上のリスク要因が関連付けられています。これらのリスク要因は、ユーザーイベントにおける異常の種類を特定するのに役立ちます。リスクインジケーターとそれに関連するリスク要因によって、ユーザーのリスクスコアが決定されます。

以下は、リスクインジケーターに関連するリスク要因です。

- **デバイスベースのリスクインジケーター**: 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。
- **場所ベースのリスクインジケーター**: ユーザーの場所履歴に基づいて異常と見なされる場所に関連付けられたIPアドレスからユーザーがサインインしたときにトリガーされます。
- **IPベースのリスクインジケーター**: ユーザーにとってIPアドレスが異常であるかどうかにかかわらず、疑わしいと特定されたIPアドレスからユーザーが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。
- **ログオン失敗ベースのリスクインジケーター**: ユーザーが過剰または異常なログオン失敗のパターンを示したときにトリガーされます。
- **データベースのリスクインジケーター**: ユーザーがWorkspaceセッションからデータを持ち出そうとしたときにトリガーされます。監視対象のユーザー行動には、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インジケーター**: ユーザーのContent Collaborationでのファイルアクセスに関する行動が、過去のアクセスパターンに基づいて異常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。

- **カスタムリスクインジケーター**: 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。詳細については、以下の記事を参照してください。
  - カスタムリスクインジケーター
  - 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
- その他のリスクインジケーター - デバイスベース、場所ベース、ログオン失敗ベースなどの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インジケーター。

リスクインジケーターは、類似のリスクに基づいてリスクカテゴリにもグループ化されます。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、リスクインジケーター、リスク要因、およびリスクカテゴリ間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ー	リスク要因	リスクカテゴリ
シトリックス エンドポイント マネジメント	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	その他のリスクインジケーター	侵害されたエンドポイント
	ジェイルブレイクまたはルート化されたデバイスが検出されました	その他のリスクインジケーター	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	その他のリスクインジケーター	侵害されたエンドポイント
シトリックス ゲートウェイ	エンドポイント分析 (EPA) スキャン失敗 (/ja-jp/security-analytics/risk-indicators/citrix-gateway-risk-indicators.html#end-point-analysis-epa-scan-failures)	その他のリスクインジケーター	侵害されたユーザー

製品	ユーザーリスクインジケーター	リスク要因	リスクカテゴリ
	過剰な認証失敗(/ja-jp/security-analytics/risk-indicators/citrix-gateway-risk-indicators.html#excessive-authentication-failures)	ログオン失敗に基づくリスクインジケーター	侵害されたユーザー
	不可能な移動(/ja-jp/security-analytics/risk-indicators/citrix-gateway-risk-indicators.html#impossible-travel)	場所に基づくリスクインジケーター	侵害されたユーザー
	不審なIPからのログオン(/ja-jp/security-analytics/risk-indicators/citrix-gateway-risk-indicators.html#logon-from-suspicious-ip)	IPに基づくリスクインジケーター	侵害されたユーザー
	不審なログオン(/ja-jp/security-analytics/risk-indicators/citrix-gateway-risk-indicators.html#suspicious-logon)	デバイスベースのリスクインジケーター、IPベースのリスクインジケーター、ロケーションベースのリスクインジケーター、およびその他のリスクインジケーター	侵害されたユーザー
	不審な認証失敗	ログオン失敗ベースのリスクインジケーター	侵害されたユーザー
シトリックス セキュア プライベート アクセス	ブラックリストに登録されたURLへのアクセス試行	その他のリスクインジケーター	内部脅威

製品	ユーザーリスクインジケーター	リスク要因	リスクカテゴリ
	過剰なデータダウンロード	その他のリスクインジケーター	内部脅威
	危険なWebサイトへのアクセス	その他のリスクインジケーター	内部脅威
	異常なアップロード量	その他のリスクインジケーター	内部脅威
シトリックス DaaS (旧称 シトリックス Virtual Apps and Desktops service) およびオンプレミスのシトリックス Virtual Apps and Desktops	ありえない移動	場所ベースのリスクインジケーター	侵害されたユーザー
	潜在的なデータ流出	データベースのリスクインジケーター	データ流出
	不審なログオン	デバイスベースのリスクインジケーター、IPベースのリスクインジケーター、場所ベースのリスクインジケーター、およびその他のリスクインジケーター	侵害されたユーザー

リスクインジケーターを、手動で役立つか否かとしてマークできます。詳細については、ユーザーリスクインジケーターのフィードバックを提供するを参照してください。

Citrix Endpoint Management™ リスクインジケーター

ブラックリスト登録済みアプリが検出されたデバイス

Citrix Analytics は、ブラックリスト登録済みアプリがインストールされているデバイスでのアクティビティに基づいてアクセス脅威を検出し、対応するリスクインジケーターをトリガーします。

ブラックリスト登録済みアプリが検出されたデバイスのリスクインジケーターは、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登録済み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のデバイスでは、承認されたアプリのみが実行されるようになります。

ブラックリスト登録済みアプリが検出されたデバイスのリスクインジケーターに関連付けられているリスク要因は、その他のリスクインジケーターです。リスク要因の詳細については、「Citrix ユーザーリスクインジケーター」を参照してください。

ブラックリスト登録済みアプリが検出されたデバイスのリスクインジケーターはいつトリガーされます?

ブラックリスト登録済みアプリが検出されたデバイスのリスクインジケーターは、ユーザーのデバイスでブラックリスト登録済み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で1つ以上のブラックリスト登録済みアプリを検出すると、イベントが Citrix Analytics に送信されます。

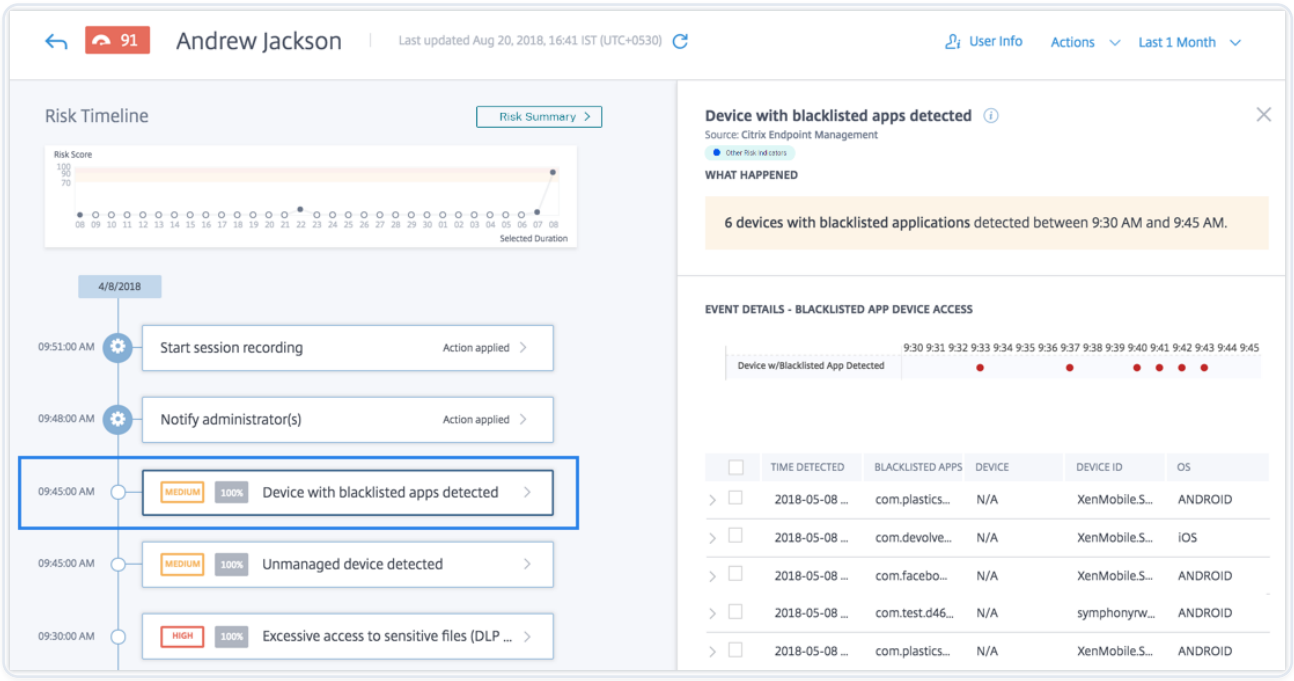
Citrix Analytics はこれらのイベントを監視し、ユーザーのリスクスコアを更新します。また、ユーザーのリスクタイムラインに**ブラックリスト登録済みアプリが検出されたデバイス**のリスクインジケーターエントリを追加します。

ブラックリスト登録済みアプリが検出されたデバイスのリスクインジケーターを分析する方法?

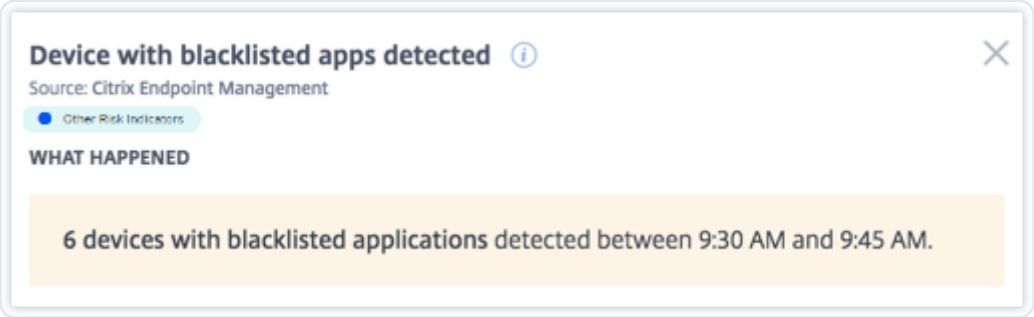
最近ブラックリスト登録済みアプリがインストールされたデバイスを使用したユーザー、Andrew Jackson を考えてみましょう。Endpoint Management はこの状態を Citrix Analytics に報告し、Citrix Analytics は Andrew Jackson に更新されたリスクスコアを割り当てます。

Andrew Jackson のリスクタイムラインから、報告された**ブラックリスト登録済みアプリが検出されたデバイス**のリスクインジケーターを選択できます。イベントの理由が、ブラックリスト登録済みアプリのリスト、Endpoint Management がブラックリスト登録済みアプリを検出した時刻などの詳細とともに表示されます。

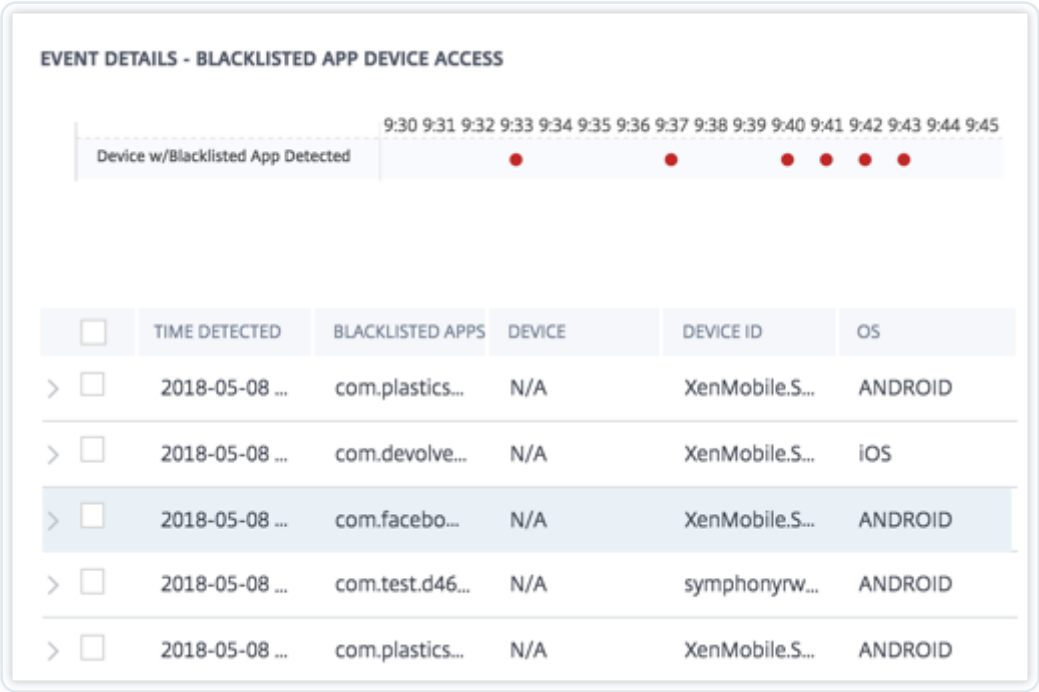
ユーザーの**ブラックリスト登録済みアプリが検出されたデバイス**のリスクインジケーターを表示するには、**セキュリティ > ユーザー**に移動し、ユーザーを選択します。



- **発生した事象**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登録済みアプリケーションがインストールされているデバイスの数と、イベントが発生した時刻を表示できます。



- 「**イベント詳細 – ブラックリスト登録済みアプリデバイスアクセス**」セクションでは、イベントがグラフィック形式と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も表示され、表には以下の主要情報が記載されています。
  - **検出時刻** - Endpoint Managementによって報告されたブラックリスト登録済みアプリの存在が検出された時刻。
  - **ブラックリスト登録済みアプリ** - デバイス上のブラックリスト登録済みアプリ。
  - **デバイス** - 使用され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** - モバイルデバイスのオペレーティングシステム。



注

表形式で詳細を表示するだけでなく、アラートのインスタンスの横にある矢印をクリックすると、さらに詳細を確認できます。

ユーザーに適用できるアクション?

ユーザー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**。将来的な潜在的脅威についてユーザーを監視したい場合は、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーアカウントに異常または不審なアクティビティがあった場合、すべてまたは選択された管理者に電子メール通知が送信されます。

アクションと手動での設定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。

ユーザーにアクションを手動で適用するには、ユーザープロファイルに移動し、適切なリスクインジケーターを選択します。「**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

> リスクインジケーター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ルート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ルート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脅威を検出し、対応するリスクインジケーターをトリガーします。

ジェイルブレイクまたはルート化されたデバイスのリスクインジケーターは、ユーザーがジェイルブレイクまたはルート化されたデバイスを使用してネットワークに接続したときにトリガーされます。Secure Hubはデバイスを検出し、インシデントをEndpoint Managementサービスに報告します。このアラートにより、承認されたユーザーとデバイスのみが組織のネットワークに接続されていることが保証されます。

ジェイルブレイクまたはルート化されたデバイスのリスクインジケーターに関連するリスク要因は、その他のリスクインジケーターです。リスク要因の詳細については、「Citrixユーザーリスクインジケーター」を参照してください。

ジェイルブレイクまたはルート化されたデバイスが検出されたリスクインジケーターはいつトリガーされます?

セキュリティ担当者にとって、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していることを確認できることは重要です。**ジェイルブレイクまたはルート化されたデバイスが検出されました**のリスクインジケーターは、ジェイルブレイクされたiOSデバイスまたはルート化されたAndroidデバイスを使用しているユーザーに警告します。

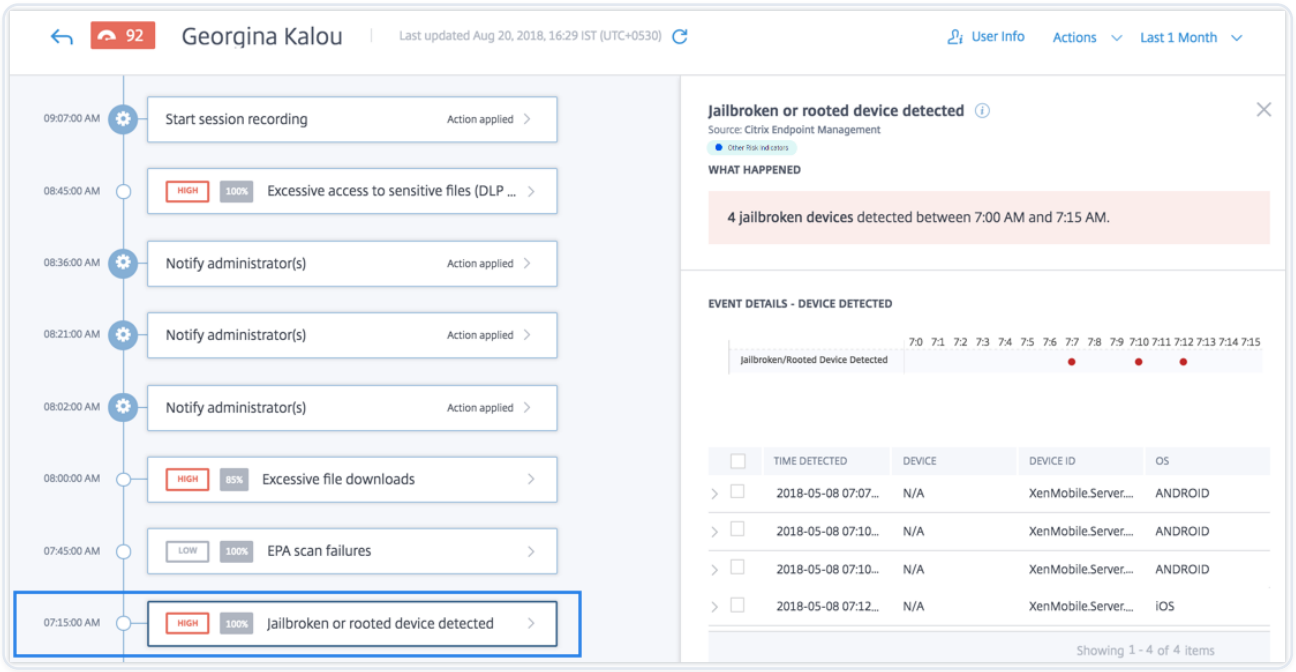
ジェイルブレイクまたはルート化されたデバイスのリスクインジケーターは、登録済みのデバイスがジェイルブレイクまたはルート化されたときにトリガーされます。Secure Hubはデバイス上のイベントを検出し、Endpoint Managementサービスに報告します。

ジェイルブレイクまたはルート化されたデバイスが検出されたリスクインジケーターを分析する方法?

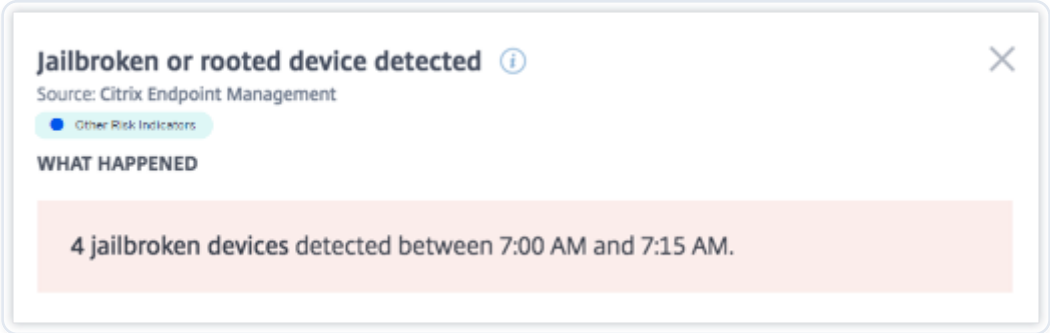
登録済みのiOSデバイスが最近ジェイルブレイクされたユーザーGeorgina Kalouを考えてみましょう。この疑わしい動作はCitrix Analyticsによって検出され、Georgina Kalouにリスクスコアが割り当てられます。

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化されたデバイスが検出されました**のリスクインジケーターを選択できます。イベントの理由が、リスクインジケーターがトリガーされた時刻、イベントの説明などの詳細とともに表示されます。

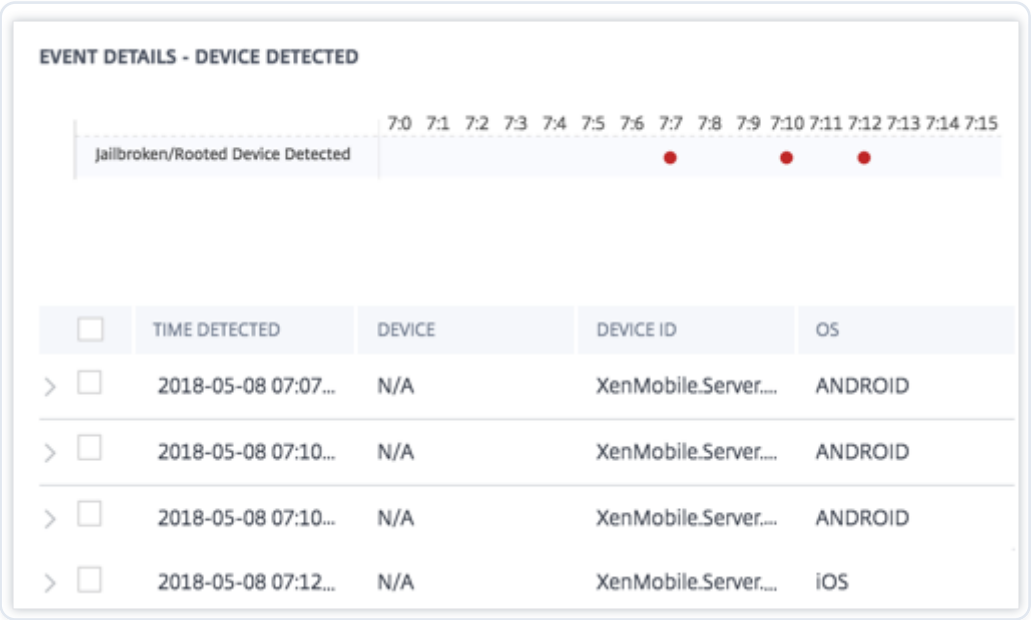
ユーザーの**ジェイルブレイクまたはルート化されたデバイスが検出されました**のリスクインジケーターを表示するには、**セキュリティ > ユーザー**に移動し、ユーザーを選択します。



- **何が起こったか**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ルート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。



- **イベント詳細 – デバイス検出**セクションでは、イベントがグラフィカル形式と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も表示され、表には次の主要情報が示されます。
  - **検出時刻**。ジェイルブレイクまたはルート化されたデバイスが検出された時刻。
  - **デバイス**。使用され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**。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の横にある矢印をクリックすると、さらに詳細が表示されます。

ユーザーに適用できるアクション?

ユーザー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**。将来の潜在的な脅威についてユーザーを監視したい場合は、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーアカウントで異常または不審なアクティビティがあった場合、すべてまたは選択された管理者に電子メール通知が送信されます。

アクションとそれらを手動で構成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。

ユーザーにアクションを手動で適用するには、ユーザーのプロファイルに移動し、適切なリスクインジケーターを選択します。**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。

注記

> リスクインジケーターをトリガーするデータソースに関わらず、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。

管理対象外デバイスが検出されました

Citrix Analyticsは、管理対象外デバイスのアクティビティに基づいてアクセス脅威を検出し、対応するリスクインジケーターをトリガーします。

管理対象外デバイスが検出されましたリスクインジケーターは、デバイスが次の状態のときにトリガーされます。

- 自動アクションによりリモートでワイプされた。
- 管理者によって手動でワイプされた。
- ユーザーによって登録解除された。

管理対象外デバイスが検出されましたリスクインジケーターに関連付けられているリスク要因は、その他のリスクインジケーターです。リスク要因の詳細については、Citrixユーザーリスクインジケーターを参照してください。

管理対象外デバイス検出リスクインジケーターがトリガーされるタイミング?

管理対象外デバイスが検出されましたリスクインジケーターは、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の状態になるのは、次の理由によります。

- ユーザーによって実行されたアクション。
- Endpoint Management管理者またはサーバーによって実行されたアクション。

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わると、Endpoint Managementサービスはこのイベントを検出し、Citrix Analyticsに報告します。ユーザーのリスクスコアが更新されます。**管理対象外デバイスが検出されました**リスクインジケーターがユーザーのリスクタイムラインに追加されます。

「管理対象外デバイス検出」リスクインジケーターを分析する方法?

ユーザーのGeorgina Kalouを例に考えてみましょう。彼女のデバイスは、サーバー上の自動アクションによってリモートワイプされました。Endpoint Managementは、このイベントをCitrix Analyticsに報告し、Citrix AnalyticsはGeorgina Kalouに更新されたリスクスコアを割り当てます。

Georgina Kalouのリスクタイムラインから、報告された「管理対象外デバイス検出」リスクインジケーターを選択できます。イベントの理由は、リスクインジケーターがトリガーされた時刻、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検出**リスクインジケーターを表示するには、**セキュリティ > ユーザー**に移動し、そのユーザーを選択します。

管理対象外デバイス検出(/en-us/citrix-analytics/media/endpoint-management-unmanaged-device-detected.png)

- **何が起こったか**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発生時刻を表示できます。

管理対象外デバイス検出で何が起こったか(/en-us/citrix-analytics/media/endpoint-management-unmanaged-device-detected-what-happened.png)

- **イベントの詳細 – デバイス検出**セクションでは、イベントがグラフ形式と表形式で表示されます。イベントはグラフ内で個別のエントリとしても表示され、表には次の主要情報が示されます。
    - **検出時刻**。イベントが検出された時刻。
    - **デバイス**。使用され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**。モバイルデバイスのオペレーティングシステム。

      管理対象外デバイス検出イベントの詳細(/en-us/citrix-analytics/media/endpoint-management-unmanaged-device-detected-event-details.png)

ユーザーに適用できるアクション?

ユーザー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**。将来的な潜在的脅威についてユーザーを監視したい場合は、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーアカウントで異常または不審なアクティビティがあった場合、すべてまたは選択された管理者にメール通知が送信されます。

アクションとそれらを手動で構成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。

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、適切なリスクインジケーターを選択します。**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**
>
> リスクインジケーター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 リスクインジケーター

エンドポイント分析 (EPA) スキャン失敗

Citrix Analytics は、EPA スキャン失敗の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、対応するリスクインジケーターをトリガーします。

エンドポイント分析スキャン失敗リスクインジケーターに関連付けられているリスク要因は、その他のリスクインジケーターです。リスク要因の詳細については、「Citrix ユーザーリスクインジケーター」を参照してください。

EPA スキャン失敗リスクインジケーター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ーは、ユーザーが Citrix Gateway の認証前または認証後のエンドポイント分析 (EPA) スキャンポリシーに失敗したデバイスを使用して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。

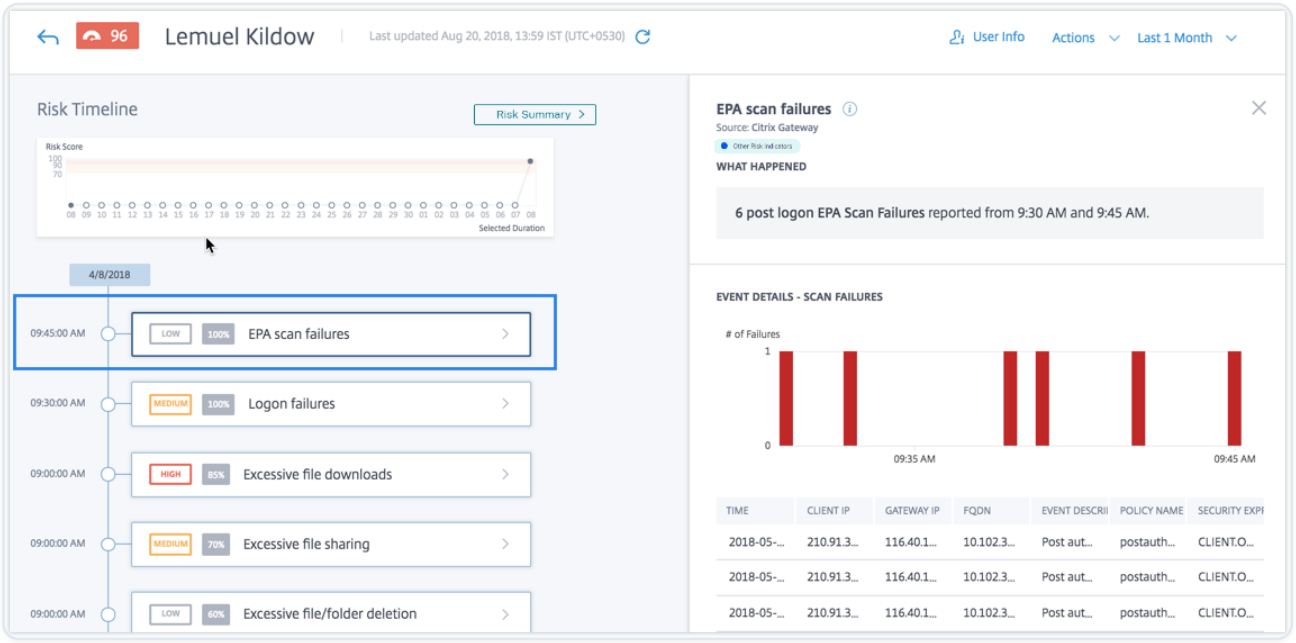
Citrix Gateway はこれらのイベントを検出し、Citrix Analytics に報告します。Citrix Analytics は、ユーザーが過剰な EPA スキャン失敗を経験したかどうかを検出するために、これらすべてのイベントを監視します。Citrix Analytics がユーザーの過剰な EPA スキャン失敗を判断すると、ユーザーのリスクスコアを更新し、ユーザーのリスクタイムラインに EPA スキャン失敗リスクインジケーターのエントリを追加します。

EPA スキャン失敗リスクインジケーターを分析する方法?

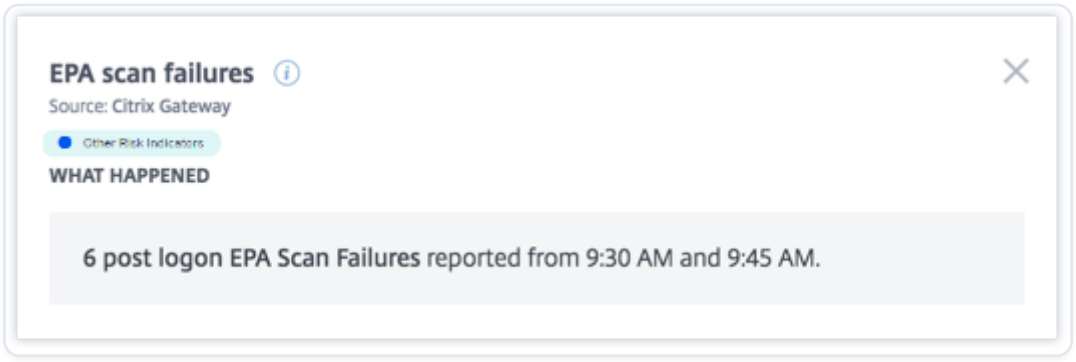
最近、Citrix Gateway の EPA スキャンに失敗したデバイスを使用してネットワークに複数回アクセスしようとしたユーザー Lemuel を考えてみましょう。Citrix Gateway はこの失敗を Citrix Analytics に報告し、Citrix Analytics は Lemuel に更新されたリスクスコアを割り当てます。EPA スキャン失敗リスクインジケーターは Lemuel Kildow のリスクタイムラインに追加されます。

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、ユーザーについて報告された最新の **EPA スキャン失敗** リスクインジケーターを選択できます。タイムラインから EPA スキャン失敗リスクインジケーターのエントリを選択すると、対応する詳細情報パネルが右ペインに表示されます。



- **何が起こったか** セクションには、EPA スキャン失敗リスクインジケーターの簡単な概要が示されます。また、選択した期間中に報告されたログオン後の EPA スキャン失敗の数も含まれます。



- **イベント詳細 – 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視覚化が含まれます。また、各イベントに関する以下の主要情報を提供するテーブルも含まれます。

  - **時間**。EPAスキャン失敗が発生した時刻。
  - **クライアントIP**。EPAスキャン失敗を引き起こしたクライアントのIPアドレス。
  - **ゲートウェイIP**。EPAスキャン失敗を報告したCitrix GatewayのIPアドレス。

- **FQDN**。シトリックス ゲートウェイ の FQDN。
- **イベントの説明**。EPAスキャン失敗の理由の簡単な説明。
- **ポリシー名**。Citrix Gatewayに設定されているEPAスキャンポリシー名。
- **セキュリティ式**。Citrix Gatewayに設定されているセキュリティ式。

EPAスキャン失敗イベントの詳細(/en-us/citrix-analytics/media/gateway-epa-scan-failures-event-details.png)

ユーザーに適用できるアクション?

ユーザー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**。将来の潜在的な脅威についてユーザーを監視したい場合は、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーアカウントに異常または不審なアクティビティがあった場合、すべてまたは選択された管理者に電子メール通知が送信されます。
- **ユーザーのログオフ**。ユーザーがアカウントからログオフされると、Citrix Gateway管理者がログオフユーザーアクションをクリアするまで、Citrix Gatewayを介してリソースにアクセスできなくなります。
- **ユーザーのロック**: 異常な動作によりユーザーのアカウントがロックされた場合、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なくなります。

アクションと手動での設定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。

ユーザーに手動でアクションを適用するには、ユーザーのプロファイルに移動し、適切なリスクインジケーターを選択します。**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**
>
> リスクインジケーター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、対応するリスクインジケーターをトリガーします。

過剰な認証失敗リスクインジケーターに関連するリスク要因は、ログオン失敗ベースのリスクインジケーターです。リスク要因の詳細については、Citrixユーザーリスクインジケーターを参照してください。

過剰な認証失敗リスクインジケーター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ーは、ユーザーが特定の期間内に複数のCitrix Gateway認証失敗に遭遇した場合に報告されます。Citrix Gateway認証失敗は、ユーザーに対して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、またはターシャリ認証失敗である可能性があります。

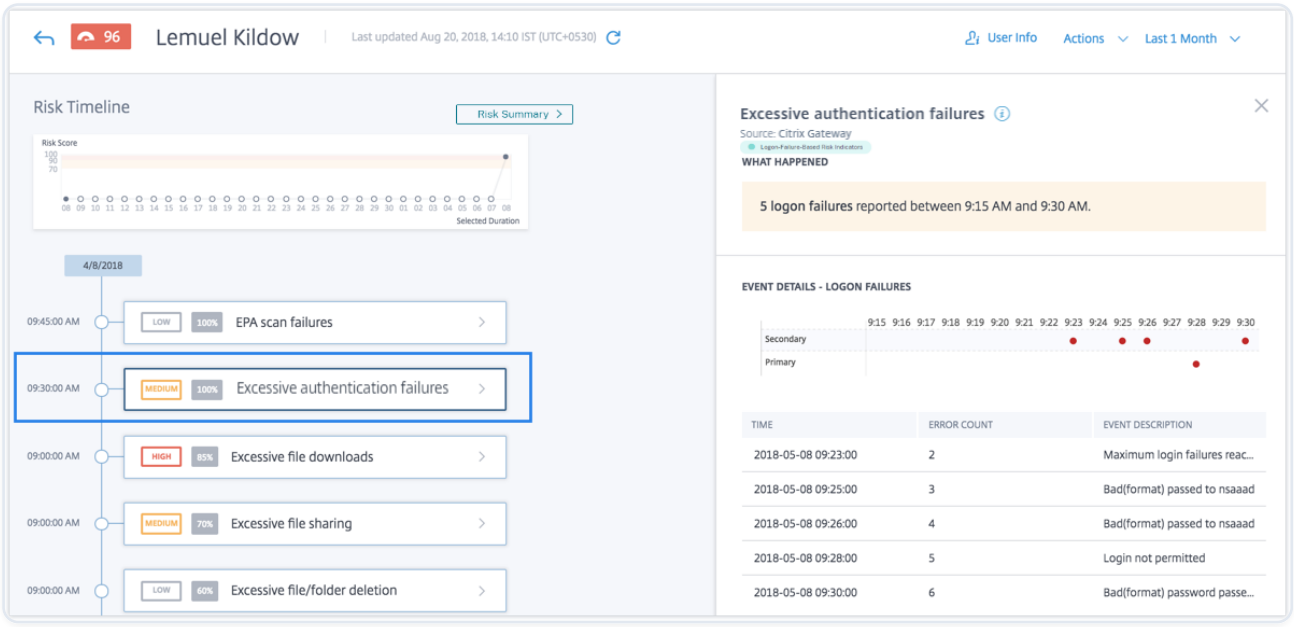
Citrix Gatewayは、すべてのユーザー認証失敗を検出し、これらのイベントをCitrix Analyticsに報告します。Citrix Analyticsは、これらのすべてのイベントを監視して、ユーザーが過剰な認証失敗を経験したかどうかを検出します。Citrix Analyticsが過剰な認証失敗を判断すると、ユーザーのリスクスコアを更新します。過剰な認証失敗リスクインジケーターは、ユーザーのリスクタイムラインに追加されます。

過剰な認証失敗リスクインジケーターを分析する方法?

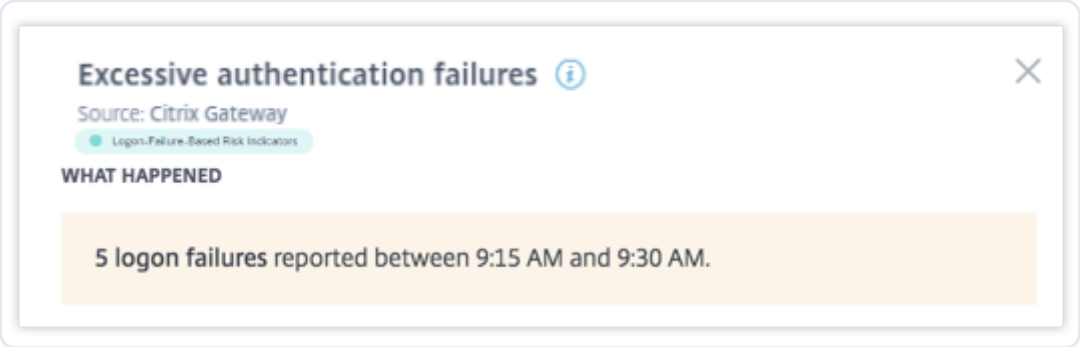
最近、ネットワーク認証に複数回失敗したユーザーLemuelを考えてみましょう。Citrix Gatewayはこれらの失敗をCitrix Analyticsに報告し、更新されたリスクスコアがLemuelに割り当てられます。**過剰な認証失敗**リスクインジケーターは、Lemuel Kildowのリスクタイムラインに追加されます。

ユーザーの**過剰な認証失敗**リスクインジケーター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、ユーザーについて報告された最新の**過剰な認証失敗**リスクインジケーターを選択できます。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ーエントリを選択すると、対応する詳細情報パネルが右ペインに表示されます。

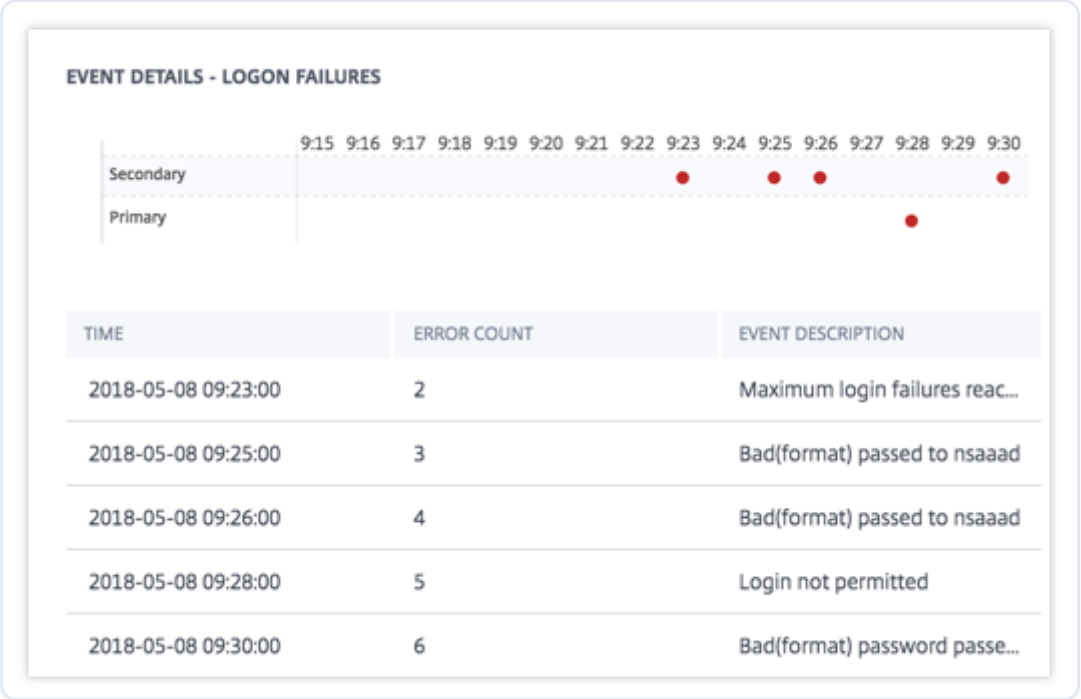


- **何が起こったか**セクションには、選択した期間中に発生した認証失敗の数を含む、リスクインジケーターの簡単な概要が記載されています。



- 「**イベント詳細**」セクションには、選択した期間中に発生した個々の認証失敗回数の過剰イベントのタイムライン視覚化が含まれています。また、各イベントに関する以下の主要情報を表示できます。

  - **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時間にユーザーに対して検出された認証失敗の回数。
  - **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**。将来の潜在的な脅威のためにユーザーを監視したい場合は、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーのアカウントで異常または不審なアクティビティがあった場合、すべてまたは選択された管理者にメール通知が送信されます。
- **ユーザーのログオフ**。ユーザーがアカウントからログオフされると、Citrix Gateway管理者が「ユーザーのログオフ」アクションを解除するまで、Citrix Gatewayを介してリソースにアクセスできなくなります。
- **ユーザーのロック**。異常な動作によりユーザーのアカウントがロックされた場合、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なくなります。

アクションとそれらを手動で構成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。

ユーザーにアクションを手動で適用するには、ユーザーのプロファイルに移動し、適切なリスクインジケーターを選択します。「**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**

リスクインジケーター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。

不可能な移動

Citrix Analyticsは、連続するログオンが、国間の予想移動時間よりも短い期間内に2つの異なる国から行われた場合、ユーザーのログオンを危険と検出します。

不可能な移動時間のシナリオは、以下のリスクを示します。

- **侵害された資格情報**: リモート攻撃者が正当なユーザーの資格情報を盗みます。
- **共有された資格情報**: 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。

不可能な移動リスクインジケーターはいつトリガーされますか?

不可能な移動リスクインジケーターは、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、その時間内に個人が移動できる距離よりも距離が大きい場合にトリガーされます。

注

このリスクインジケーターには、ユーザーの実際の場所を反映しない以下のシナリオに対する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場合。
- ユーザーがホスト型クライアントからCitrix Gateway経由でログオンする場合。

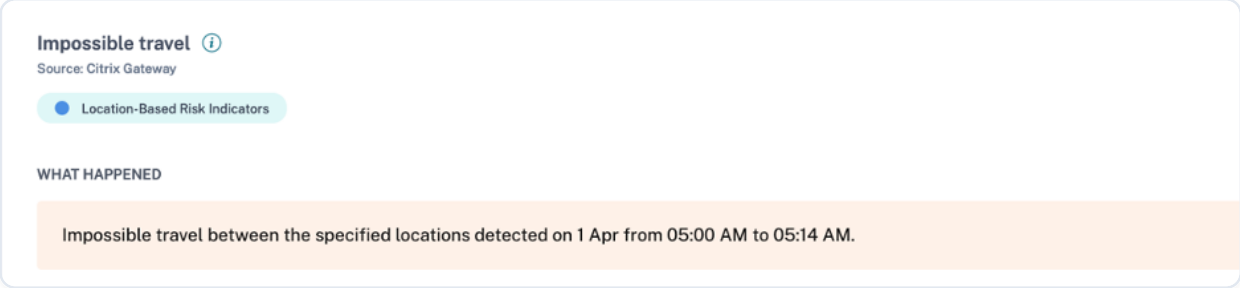
不可能なリスクインジケーターを分析する方法

Adam Maxwellというユーザーが、1分以内にインドのバンガロールとノルウェーのオスロという2つの場所からログオンしたとします。Citrix Analyticsは、このログオンイベントを不可能な移動シナリオとして検出し、**不可能な移動**リスクインジケーターをトリガーします。このリスクインジケーターはAdam Maxwellのリスクタイムラインに追加され、彼にリスクスコアが割り当てられます。

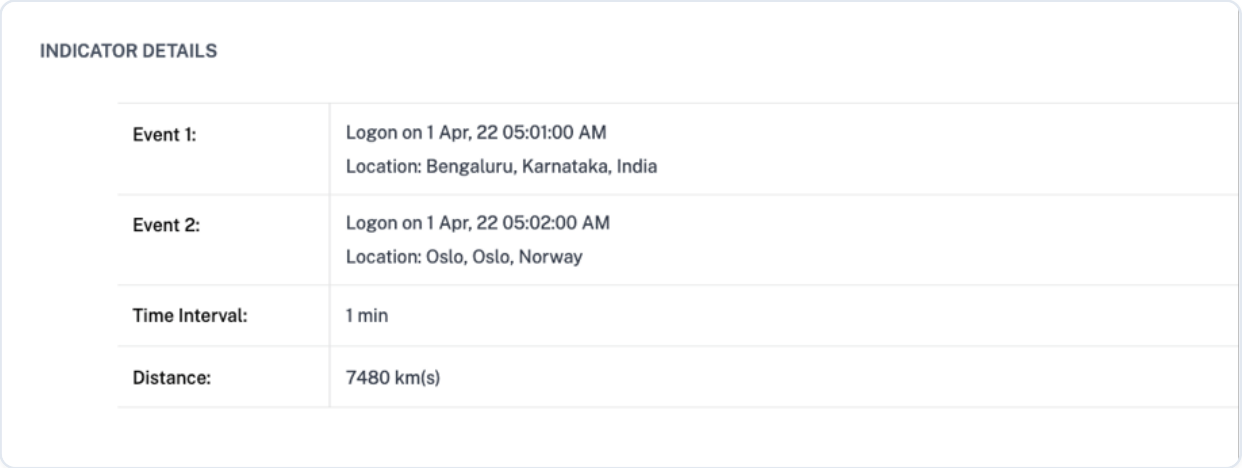
Adam Maxwellのリスクタイムラインを表示するには、**セキュリティ > ユーザー**を選択します。**危険なユーザー**ペインから、ユーザーAdam Maxwellを選択します。

Adam Maxwellのリスクタイムラインから、**不可能移動**リスクインジケーターを選択します。以下の情報を表示できます。

- **何が起こったか**セクションには、不可能移動イベントの簡単な概要が記載されています。



- **インジケーターの詳細**セクションには、ユーザーがログオンした場所、連続するログオン間の時間、および2つの場所間の距離が記載されています。

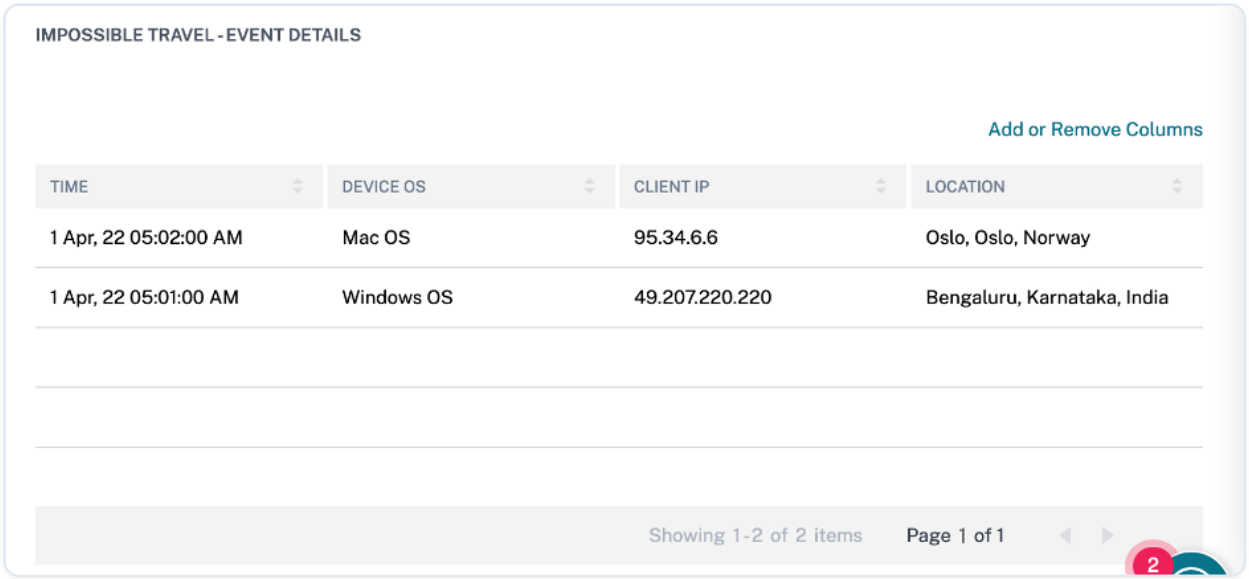


- **ログオン場所 - 過去30日間**セクションには、不可能移動の場所とユーザーの既知の場所の地理的な地図ビューが表示されます。場所のデータは過去30日間について表示されます。地図上のポインターにカーソルを合わせると、各場所からの合計ログオン数を表示できます。



- **不可能移動 - イベント詳細**セクションには、不可能移動イベントに関する以下の情報が記載されています。

- **時間**: ログオンの日付と時間を示します。
- **デバイス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は何ですか?

ユーザーのアカウントに対して、以下の操作を実行できます。

- **ウォッチリストに追加**。ユーザーを将来的な潜在的脅威から監視したい場合、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーアカウントに異常または不審なアクティビティがあった場合、すべてまたは選択された管理者にメール通知が送信されます。
- **ユーザーのログオフ**。ユーザーがアカウントからログオフされると、Citrix Gateway管理者が「ユーザーのログオフ」アクションを解除するまで、Citrix Gatewayを介してどのリソースにもアクセスできなくなります。
- **ユーザーのロック**: ユーザーアカウントが異常な動作によりロックされた場合、Gateway管理者がアカウントのロックを解除するまで、Citrix Gatewayを介してどのリソースにもアクセスできなくなります。

アクションとその手動設定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。

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、適切なリスクインジケーターを選択します。**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**
>
> リスクインジケーター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。

不審なIPからのログオン

Citrix Analyticsは、不審な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脅威を検出し、このリスクインジケーターをトリガーします。

「不審なIPからのログオン」リスクインジケーターに関連するリスクファクターは、IPベースのリスクインジケーターです。リスクファクターの詳細については、「Citrixユーザーリスクインジケーター」を参照してください。

不審なIPからのログオンリスクインジケーターはいつトリガーされますか?

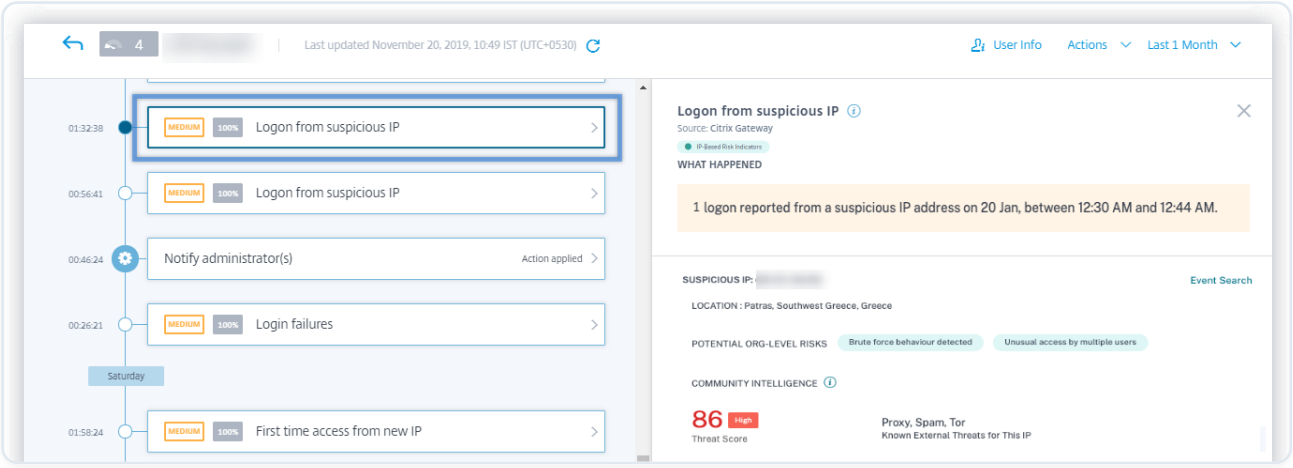
不審なIPからのログオンリスクインジケーターは、ユーザーがCitrix Analyticsが不審と識別するIPアドレスからネットワークにアクセスしようとしたときにトリガーされます。IPアドレスは、以下のいずれかの条件に基づいて不審と見なされます。

- 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
- 異常な場所からの複数のユーザーサインイン記録がある
- ブルートフォース攻撃を示している可能性のある、過剰なサインイン失敗試行がある

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 からサインインした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を更新し、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**」リスクインジケーターエントリを追加します。

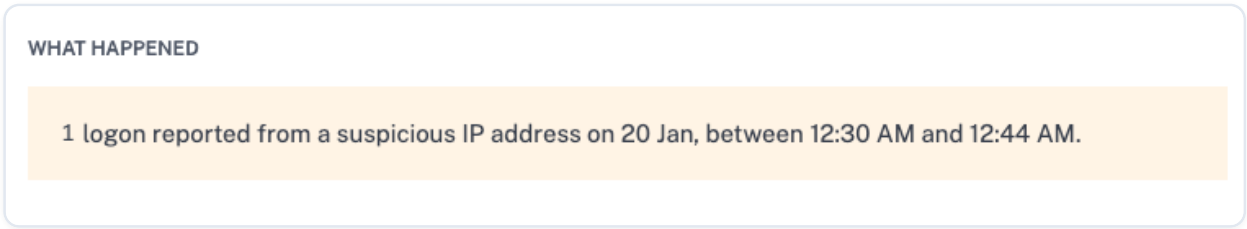
疑わしいIPからのログオンリスクインジケーターを分析する方法?

Citrix Analytics が疑わしいと識別した 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、Citrix Analytics は Lemuel に更新されたリスクスコアを割り当てます。「**疑わしいIPからのログオン**」リスクインジケーターが Lemuel Kildow のリスクタイムラインに追加されます。

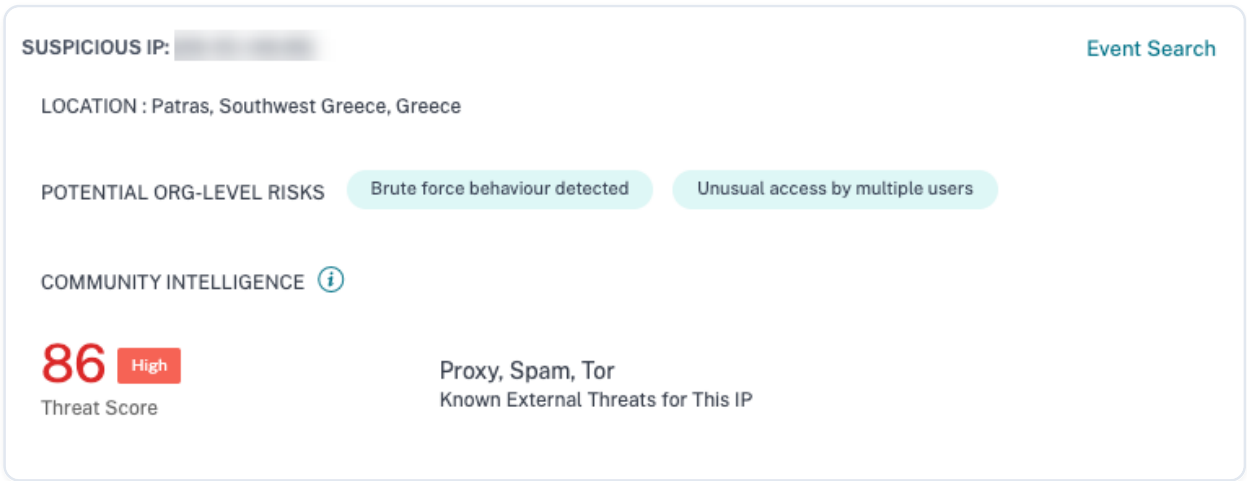


ユーザーについて報告された「疑わしいIPからのログオン」リスクインジケーターを表示するには、**セキュリティ** > **ユーザー** に移動し、ユーザーを選択します。Lemuel Kildow のリスクタイムラインから、ユーザーについて報告された最新の「**疑わしいIPからのログオン**」リスクインジケーターを選択できます。タイムラインから「**疑わしいIPからのログオン**」リスクインジケーターエントリを選択すると、対応する詳細情報パネルが右ペインに表示されます。

- 「**何が起こったか**」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ー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。



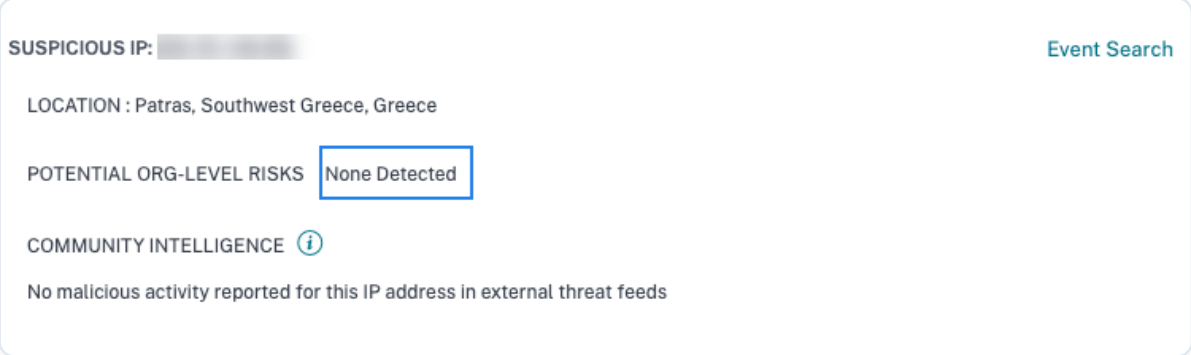
- 「**疑わしいIP**」セクションには、次の情報が表示されます。



  - **疑わしいIP**。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**。ユーザーの都市、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。

- **組織レベルの潜在的なリスク**。Citrix Analytics が最近組織で検出した疑わしいIPアクティビティのパターンを示します。リスクの高いパターンには、潜在的なブルートフォース攻撃と一致する過剰なログイン失敗、および複数のユーザーによる異常なアクセスが含まれます。

  組織内のIPアドレスに対してリスクの高いパターンが検出されない場合、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高リスクと識別された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は、高リスクIPアドレスにリスクスコアを割り当てます。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IPアドレスに脅威インテリジェンスが利用できない場合、次のメッセージが表示されます。

  インテリジェンスフィードなし(/en-us/citrix-analytics/media/gateway-logon-from-suspicious-ip-no-feed.png)

- **イベントの詳細**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。

  疑わしいIPからのログオン(/en-us/citrix-analytics/media/gateway-logon-from-suspicious-ip-event-details.png)

  - **時間**。疑わしいサインインアクティビティの時間。
  - **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されたWebブラウザ。

ユーザーに適用できるアクションは何ですか?

ユーザー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**。将来の潜在的な脅威のためにユーザーを監視したい場合は、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーアカウントで異常または疑わしいアクティビティがあった場合、すべてまたは選択された管理者に電子メール通知が送信されます。
- **ユーザーのログオフ**。ユーザーがアカウントからログオフされると、Citrix Gateway管理者がユーザーログオフアクションをクリアするまで、Citrix Gatewayを介してリソースにアクセスできません。
- **ユーザーのロック**: 異常な動作によりユーザーアカウントがロックされた場合、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。

アクションとそれらを手動で構成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。

アクションを手動でユーザーに適用するには、ユーザーのプロファイルに移動し、適切なリスクインジケーターを選択します。**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**
>
> リスクインジケーター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。

不審なログオン

> **注**
>
> - このリスクインジケーターは、「通常とは異なる場所からのアクセス」リスクインジケーターに代わるものです。
> - 「通常とは異なる場所からのアクセス」リスクインジケーターに基づくポリシーは、すべて「不審なログオン」リスクインジケーター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、異常または危険と見なされるユーザーのログオンを検出します。

不審なログオンのリスクインジケーターはいつトリガーされますか?

リスクインジケーターは、以下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つ以上の条件に基づいて潜在的に不審であると見なされます。

要因	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。デバイスの署名は、デバイスのオペレーティングシステムと使用されているブラウザに基づいています。
異常な場所	ユーザーが過去30日間にログオンしたことのない都市または国からのログオン。
	その都市または国は、最近（過去30日間）のログオン場所から地理的に遠い。
	過去30日間にその都市または国からログオンしたユーザーがゼロまたは最小限である。
異常なネットワーク	ユーザーが過去30日間に使用したことのないIPアドレスからのログオン。
	ユーザーが過去30日間に使用したことのないIPサブネットからのログオン。
	過去30日間にそのIPサブネットからログオンしたユーザーがゼロまたは最小限である。
IP脅威	その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であるWebrootによって高リスクと識別されている。
	Citrix Analyticsは最近、他のユーザーからのそのIPアドレスからの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。

不審なログオンリスクインジケーターを分析する方法

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するユーザー、アダム・マックスウェルを考えてみましょう。彼は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が、過去30日間使用していないネットワークから接続しています。

Citrix Analyticsは、場所とネットワークという要素が彼の通常の行動から逸脱しているため、このログオンイベントを不審なものとして検出し、「不審なログオン」リスクインジケーターをトリガーします。このリスクインジケーターはアダム・マックスウェルのリスクタイムラインに追加され、彼にリスクスコアが割り当てられます。

アダム・マックスウェルのリスクタイムを表示するには、**セキュリティ > ユーザー**を選択します。**リスクのあるユーザー**ペインから、ユーザーのアダム・マックスウェルを選択します。

Adam Maxwellの危険度タイムラインから、**不審なログオン**の危険度インジケーターを選択します。以下の情報が表示されます。

- **何が起こったか**セクションには、危険因子とイベントの時刻を含む不審なアクティビティの簡単な概要が示されます。

  不審なログオンで何が起こったか(/en-us/citrix-analytics/media/suspicious-logon-gw-what-happened.png)

- **ログオンの詳細**セクションには、各危険因子に対応する不審なアクティビティの詳細な概要が示されます。各危険因子には、疑わしさのレベルを示すスコアが割り当てられます。単一の危険因子だけでは、ユーザーからの高いリスクを示すものではありません。全体的なリスクは、複数の危険因子の相関関係に基づいて判断されます。

疑わしさのレベル	表示
0–69	この要因は正常に見え、不審とは見なされません。
70–89	この要因はわずかに異常に見え、他の要因と合わせて中程度の不審と見なされます。
90–100	この要因はまったく新しいか異常であり、他の要因と合わせて非常に不審と見なされます。

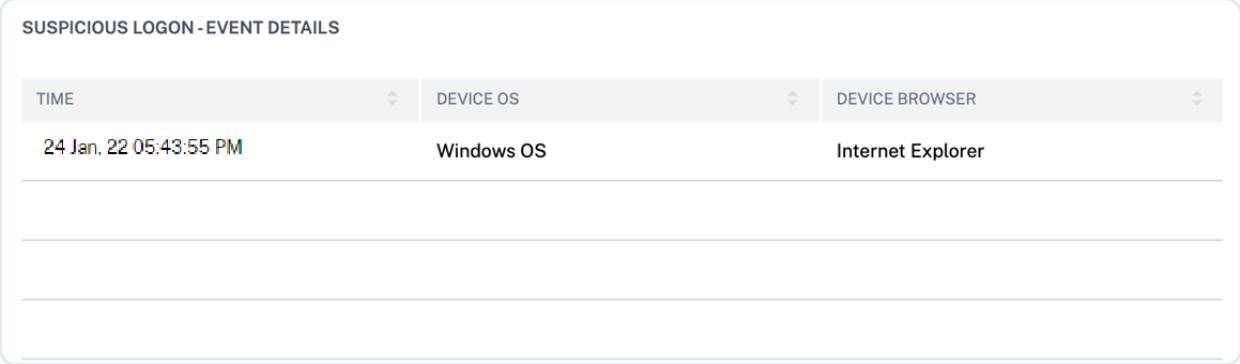
  不審なログオンの詳細(/en-us/citrix-analytics/media/suspicious-logon-gw-details.png)

- **ログオン場所 - 過去30日間**には、ユーザーの最後に確認された場所と現在の場所の地理的な地図ビューが表示されます。場所のデータは過去30日間のものが表示されます。地図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を表示できます。

  不審なログオン場所の詳細(/en-us/citrix-analytics/media/susp-logon-gw-locations-map.png)

- **SUSPICIOUS LOGON- EVENT DETAILS**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。

  - **時間**: 疑わしいログオンの日時を示します。
  - **デバイス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された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**。将来の潜在的な脅威についてユーザーを監視したい場合は、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーアカウントで異常または不審なアクティビティがあった場合、すべてまたは選択された管理者にメール通知が送信されます。
- **ユーザーのログオフ**。ユーザーがアカウントからログオフされると、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を介してリソースにアクセスできません。
- **ユーザーのロック**: 異常な動作によりユーザーアカウントがロックされた場合、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。

アクションとそれらを手動で構成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。

ユーザーにアクションを手動で適用するには、ユーザーのプロファイルに移動し、適切なリスクインジケーターを選択します。**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**
>
> リスクインジケーター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。

不審な認証失敗

Citrix Analyticsは、ユーザーが通常とは異なるIPアドレスからログオンに失敗した場合にアクセスベースの脅威を検出し、対応するリスクインジケーターをトリガーします。

不審な認証リスクインジケーターに関連付けられているリスク要因は、ログオン失敗ベースのリスクインジケーターです。リスク要因の詳細については、「Citrixユーザーリスクインジケーター」を参照してください。

不審な認証失敗インジケーターはいつトリガーされますか?

組織内のユーザーが、通常の行動とは異なる不審なIPアドレスからログオンに失敗した場合に通知を受け取ることができます。

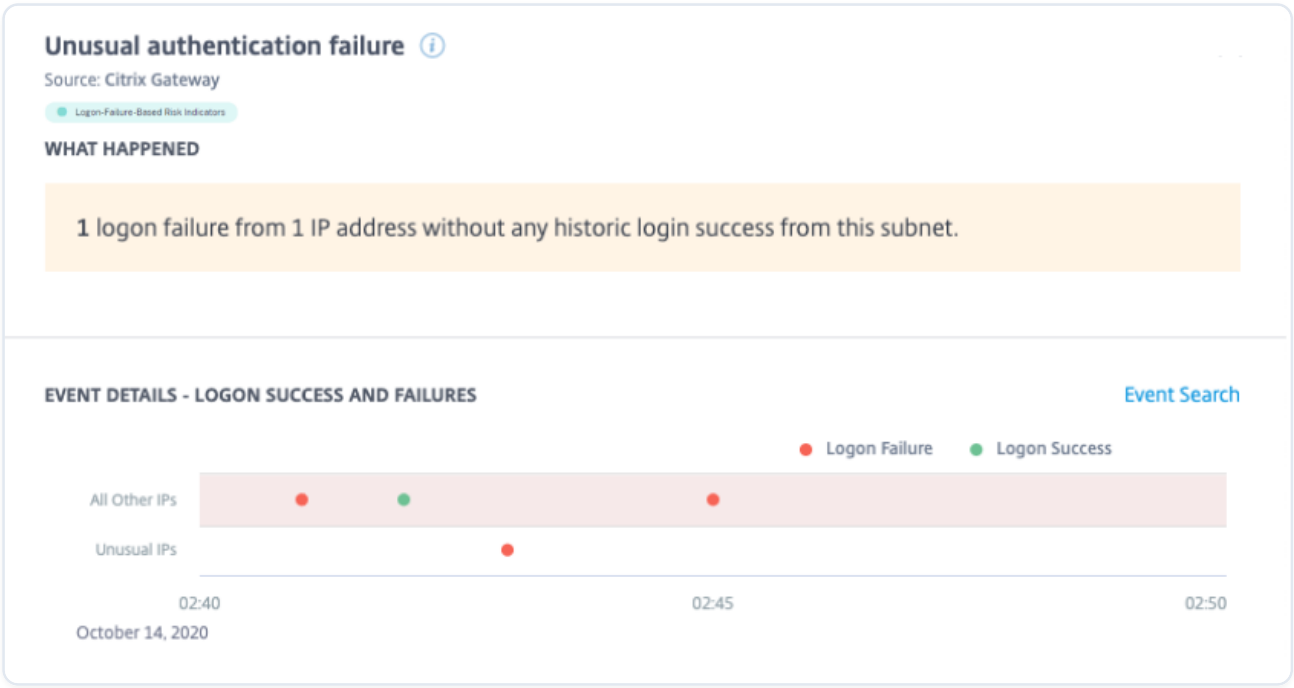
Citrix Gatewayはこれらのイベントを検出し、Citrix Analyticsに報告します。Citrix Analyticsはイベントを受信し、ユーザーのリスクスコアを増加させます。**不審な認証失敗**リスクインジケーターがユーザーのリスクタイムラインに追加されます。

不審な認証失敗インジケーターを分析する方法?

通常、自宅やオフィスのネットワークからCitrix Gatewayにサインインするユーザー Georgina Kalouを考えてみましょう。リモート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し、その結果、見慣れないネットワークからの認証失敗が発生します。

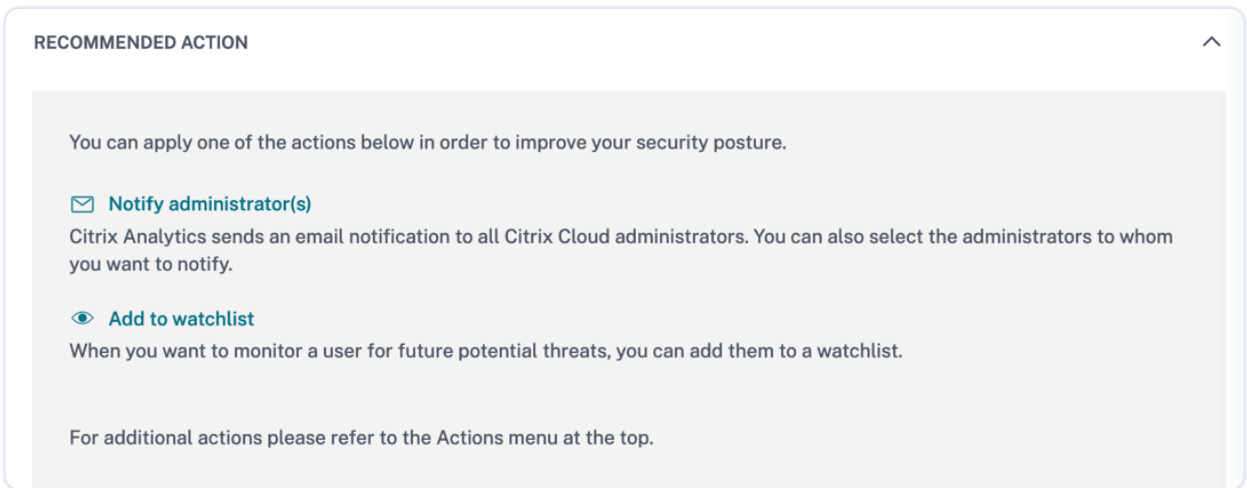
このシナリオでは、Citrix GatewayがこれらのイベントをCitrix Analyticsに報告し、Citrix AnalyticsはGeorgina Kalouに更新されたリスクスコアを割り当てます。不審な認証失敗リスクインジケーターがGeorgina Kalouのリスクタイムラインに追加されます。

Georgina Kalouのリスクタイムラインから、報告された不審な認証失敗リスクインジケーターを選択できます。イベントの理由が、イベントの時刻や場所などの詳細とともに表示されます。

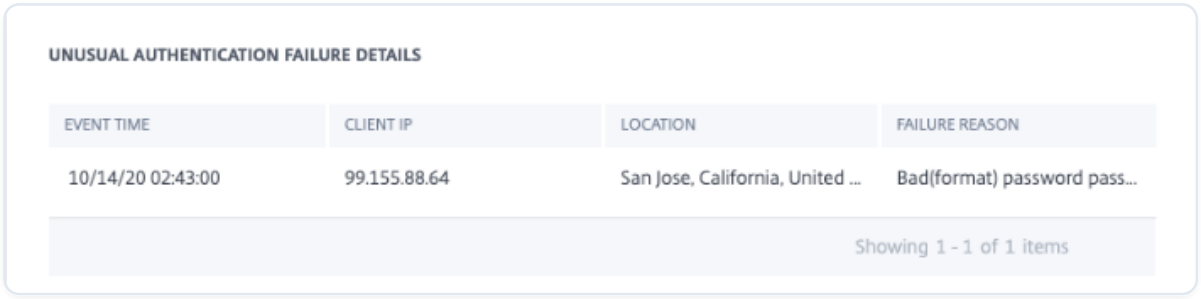


- **何が起こったか**セクションでは、認証失敗の合計数とイベントの時刻を含む簡単な概要を表示できます。
- **推奨されるアクション**セクションでは、リスクインジケーターに適用できる推奨アクションを見つけることができます。Citrix Analytics for Security™は、ユーザーがもたらすリスクの重大度に応じてアクションを推奨します。推奨事項は、次のアクションのいずれか、またはそれらの組み合わせです。
  - 管理者に通知する
  - ウォッチリストに追加する
  - ポリシーを作成する

  推奨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**メニューから、選択に応じて適用したいアクションを選択できます。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。



- **イベントの詳細 – ログオンの成功と失敗**セクションでは、不審な認証失敗を示すグラフと、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表示できます。
- **不審な認証の詳細**セクションのテーブルには、不審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** – イベントの日付と時刻
    - **クライアントIP** – ユーザーデバイスのIPアドレス
    - **場所** – イベントが発生した場所
    - **失敗理由** – 認証失敗の理由



- **ユーザー認証アクティビティ – 過去30日間**セクションのテーブルには、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からのIPアドレス。
    - 成功 – 成功した認証イベントの総数と、ユーザーの最新の成功イベントの時刻。
    - 失敗 – 失敗した認証イベントの総数と、ユーザーの最新の失敗イベントの時刻。
    - 場所 – 認証イベントが発生した場所。

      認証アクティビティ(/en-us/citrix-analytics/media/gw-auth-failure2.png)

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**。将来的な潜在的脅威のためにユーザーを監視したい場合、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーのアカウントで異常または不審なアクティビティがあった場合、すべてまたは選択された管理者にメール通知が送信されます。
- **ユーザーをログオフ**。ユーザーがアカウントからログオフされると、Citrix Gateway管理者が「ユーザーをログオフ」アクションを解除するまで、Citrix Gatewayを介してどのリソースにもアクセスできなくなります。

- **ユーザーをロック**: 異常な動作によりユーザーのアカウントがロックされた場合、Gateway管理者がアカウントのロックを解除するまで、Citrix Gatewayを介してどのリソースにもアクセスできなくなります。

アクションとそれらの手動設定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。

ユーザーにアクションを手動で適用するには、ユーザーのプロファイルに移動し、適切なリスクインジケーターを選択します。**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**
>
> リスクインジケーター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™ のリスクインジケーター

危険なWebサイトへのアクセス

> **注** 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の評価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利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、お客様に対してはトリガーされません。
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）を使用する既存のカスタムリスクインジケーターおよびそれに関連するポリシーは、今後トリガーされません。

> Secure Private Access からの廃止の詳細については、「機能の廃止」を参照してください。

ブラックリストに登録されたURLへのアクセス試行

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脅威を検出し、対応するリスクインジケーターをトリガーします。

ブラックリストに登録されたURLへのアクセス試行リスクインジケーターは、ユーザーがSecure Private Access で構成されたブラックリストに登録されたURLへのアクセスを試行したときに、Citrix Analytics で報告されます。

ブラックリストに登録されたURLへのアクセス試行リスクインジケーターに関連付けられているリスク要因は、その他のリスクインジケーターです。リスク要因の詳細については、「Citrixユーザーリスクインジケーター」を参照してください。

ブラックリストに登録されたURLへのアクセス試行リスクインジケーターがトリガーされるタイミング?

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ための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へのアクセスを試行すると、Secure Private Access はこのイベントをCitrix Analytics に報告します。Citrix Analytics はユーザーのリスクスコアを更新し、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へのアクセス試行**リスクインジケーターのエントリを追加します。

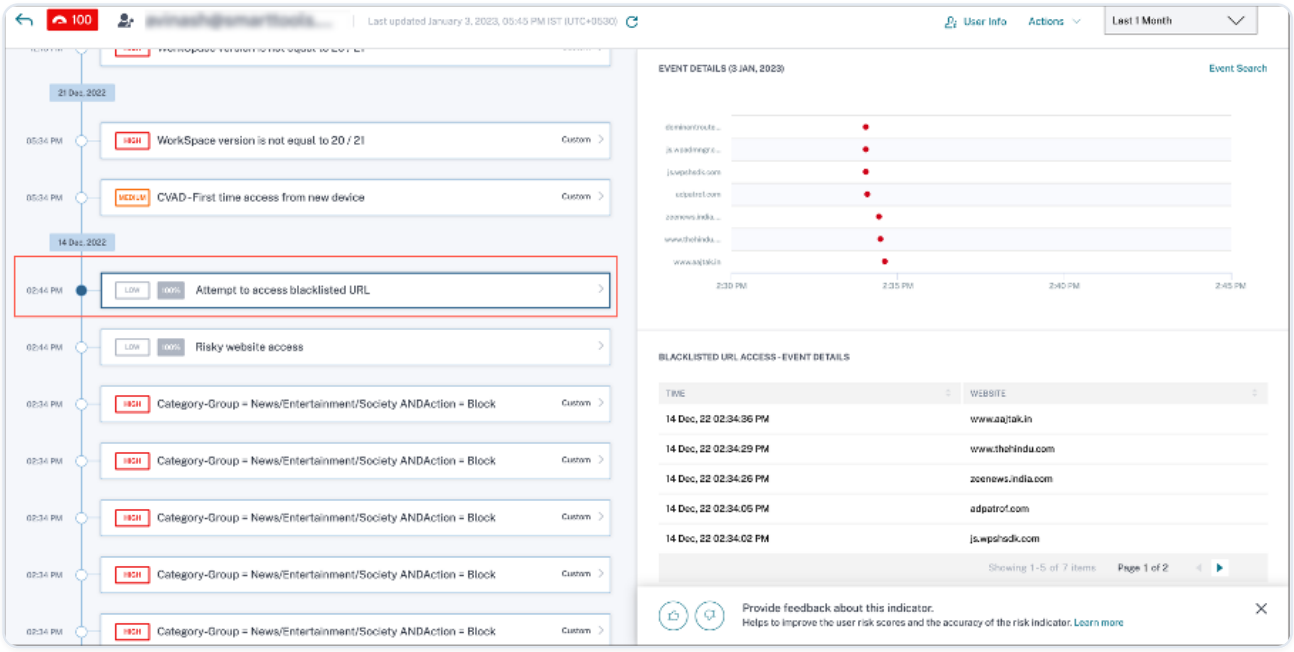
ブラックリストに登録されたURLへのアクセス試行リスクインジケーターを分析する方法?

Secure Private Access で構成されたブラックリストに登録されたURLにアクセスしたユーザーGeorgina Kalouを考えてみましょう。Secure Private Access はこのイベントをCitrix Analytics に報告し、Citrix Analytics はGeorgina Kalouに更新されたリスクスコアを割り当てます。**ブラックリストに登録されたURLへのアクセス試行**リスクインジケーターは、Georgina Kalouのリスクタイムラインに追加されます。

Georgina Kalouの危険度タイムラインから、報告された**ブラックリストに登録されたURLへのアクセス試行**危険度インジケーターを選択できます。イベントの理由が、イベントの時刻、ウェブサイトの詳細などのイベントに関する詳細とともに表示されます。

ユーザーの**ブラックリストに登録されたURLへのアクセス試行**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。

タイムラインから**ブラックリストに登録されたURLへのアクセス試行**危険度インジケーターエントリを選択すると、対応する詳細情報パネルが右ペインに表示されます。

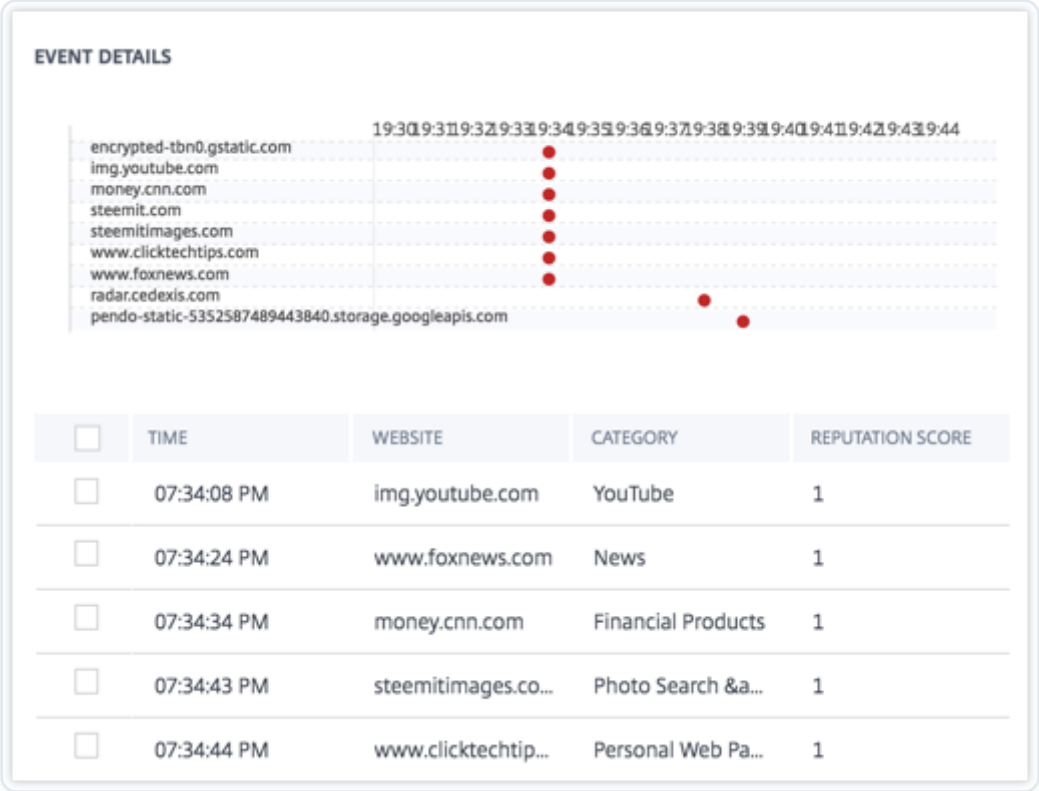


- **何が起こったか**セクションには、危険度インジケーターの簡単な概要が示されます。これには、選択した期間中にユーザーがアクセスしたブラックリストに登録されたURLの詳細が含まれます。



- **イベントの詳細**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視覚化が含まれます。また、各イベントに関する以下の主要情報を表示できます。

  - **時刻**。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した危険なウェブサイト。
  - **カテゴリ**。Secure Private Accessによってブラックリストに登録されたURLに指定されたカテゴリ。
  - **評価スコア**。Secure Private Accessによってブラックリストに登録されたURLに対して返された評価スコア。詳細については、URL評価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**。将来の潜在的な脅威についてユーザーを監視したい場合は、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーアカウントで異常または不審なアクティビティがあった場合、すべてまたは選択された管理者にメール通知が送信されます。

アクションと手動での設定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。

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、適切なリスクインジケーターを選択します。**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**
>
> リスクインジケーター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。

不審なアップロード量

Citrix Analyticsは、不審なアップロード量のアクティビティに基づいてデータアクセス脅威を検出し、対応するリスクインジケーターをトリガーします。

不審なアップロード量リスクインジケーターは、ユーザーがアプリケーションまたはWebサイトに過剰な量のデータをアップロードしたときに報告されます。

不審なアップロード量リスクインジケーターに関連するリスク要因は、その他のリスクインジケーターです。リスク要因の詳細については、「Citrixユーザーリスクインジケーター」を参照してください。

不審なアップロード量リスクインジケーターはいつトリガーされますか?

Secure Private Accessは、悪意のある、危険な、または不明なWebサイトへのアクセス、消費された帯域幅、危険なダウンロードとアップロードなど、ユーザーのアクティビティを監視するように構成できます。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は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行動に反すると判断した場合、ユーザーのリスクスコアを更新します。**不審なアップロード量**リスクインジケーターがユーザーのリスクタイムラインに追加されます。

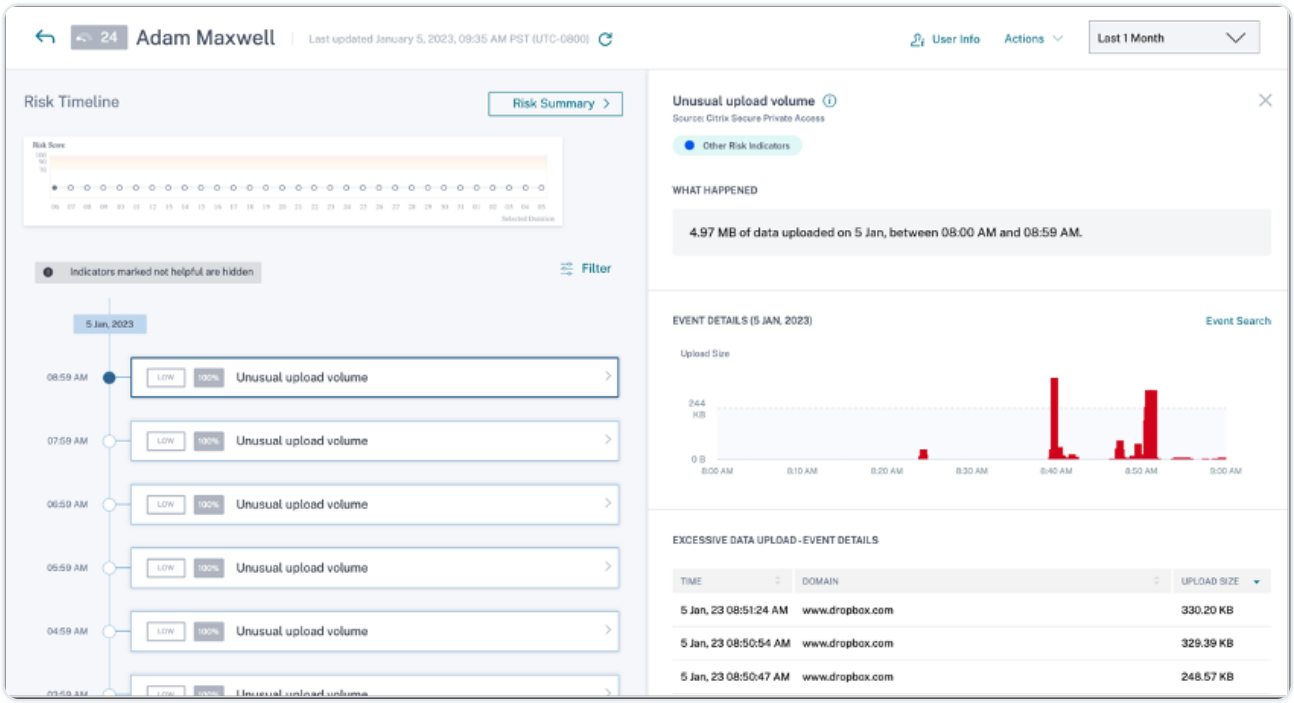
不審なアップロード量リスクインジケーターを分析する方法?

アダム・マックスウェルというユーザーが、アプリケーションまたはWebサイトに過剰な量のデータをアップロードしたとします。Secure Private AccessはこれらのイベントをCitrix Analyticsに報告し、Citrix Analyticsはアダム・マックスウェルに更新されたリスクスコアを割り当てます。**不審なアップロード量**リスクインジケーターは、アダム・マックスウェルのリスクタイムラインに追加されます。

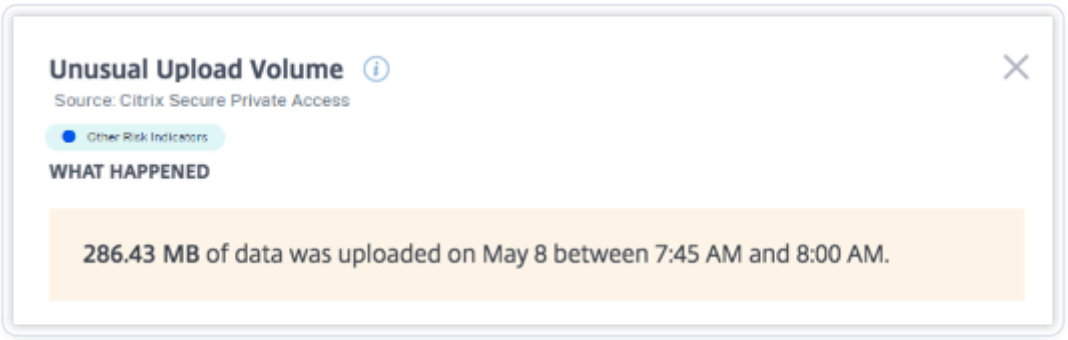
アダム・マックスウェルのリスクタイムラインから、報告された**不審なアップロード量**リスクインジケーターを選択できます。イベントの理由が、イベントの時刻やドメインなどの詳細とともに表示されます。

「**異常なアップロード量**」のリスクインジケーターを表示するには、**セキュリティ > ユーザー**に移動し、ユーザーを選択します。

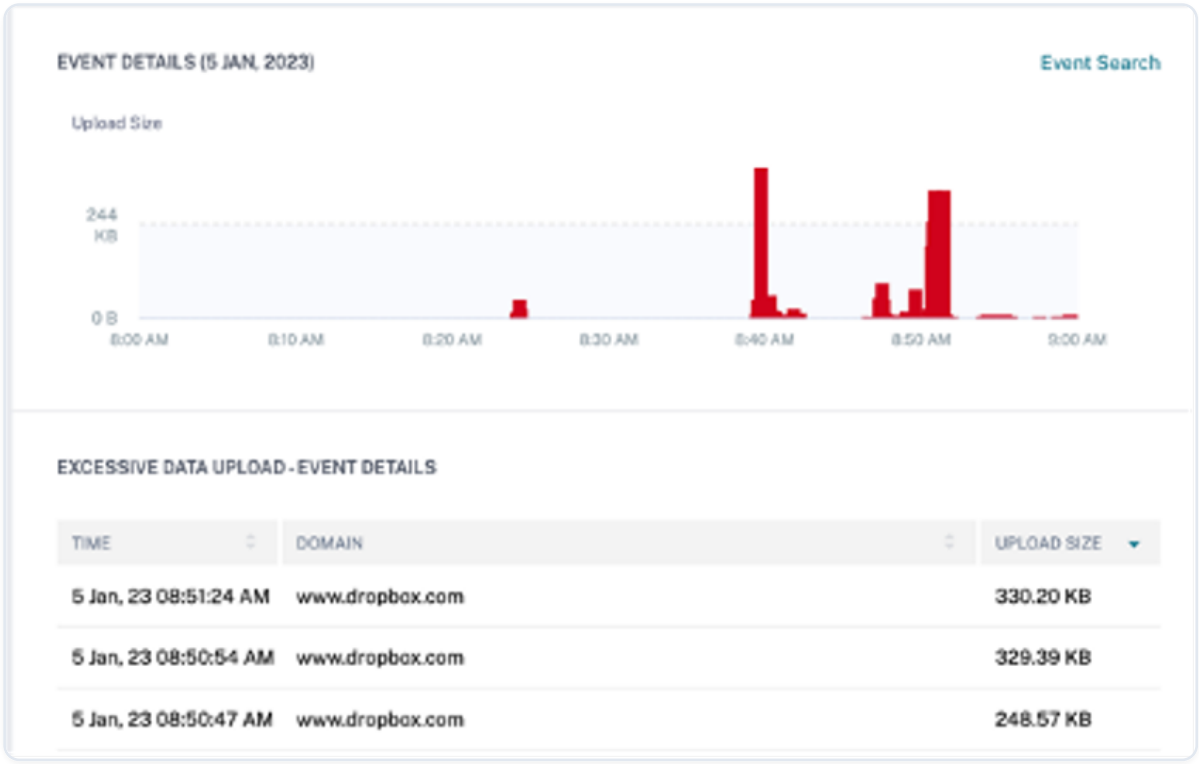
タイムラインから「**異常なアップロード量**」のリスクインジケーターエントリを選択すると、対応する詳細情報パネルが右ペインに表示されます。



- 「**何が起こったか**」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量を含む、リスクインジケーターの簡単な概要が示されます。



- 「**イベント詳細**」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視覚化が含まれます。また、各イベントに関する次の主要情報を表示できます。
  - **時間**。過剰なデータがアプリケーションまたはウェブサイトにアップロードされた時間。
  - **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**。将来の潜在的な脅威についてユーザーを監視したい場合は、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーのアカウントで異常または不審なアクティビティがあった場合、すべてまたは選択された管理者にメール通知が送信されます。

アクションとそれらを手動で構成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。

ユーザーに手動でアクションを適用するには、ユーザーのプロファイルに移動し、適切なリスクインジケーターを選択します。**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**
>
> リスクインジケーター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脅威を検出し、対応するリスクインジケーターをトリガーします。

このリスクインジケーターは、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のリスクインジケーターはいつトリガーされますか?

Secure Private Accessを構成して、悪意のある、危険な、または不明なWebサイトへのアクセス、消費された帯域幅、危険なダウンロードとアップロードなど、ユーザーの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、ユーザーのアクティビティが通常の行動と異なることを判断した場合、ユーザーのリスクスコアを更新します。過剰なデータダウンロードのリスクインジケーター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インジケーターに関連するリスク要因は、その他のリスクインジケーターです。リスク要因の詳細については、Citrixユーザーリスクインジケーター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インジケーターを分析する方法?

ユーザーのGeorgina Kalou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します。Secure Private AccessはこれらのイベントをCitrix Analyticsに報告し、Citrix AnalyticsはGeorgina Kalouに更新されたリスクスコアを割り当て、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**のリスクインジケーター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**過剰なデータダウンロード**のリスクインジケーターを選択できます。イベントの理由が、時間やドメインの詳細などのイベントに関する詳細とともに表示されます。

過剰なデータダウンロードのリスクインジケーターを表示するには、**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**過剰なデータダウンロード**のリスクインジケーターエントリを選択すると、対応する詳細情報パネルが右ペインに表示されます。

Secure Private Access 過剰なデータダウンロード(/en-us/citrix-analytics/media/access-control-unusual-download-volume.png)

- 「**何が起こったか**」セクションでは、選択した期間中にアップロードまたはダウンロードされたデータ量を含む、リスクインジケーターの簡単な概要が提供されます。

  Secure Private Access 過剰なデータダウンロード 何が起こったか(/en-us/citrix-analytics/media/access-control-unusual-download-volume-what-happened.png)

- 「**イベント詳細**」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視覚化が含まれています。また、各イベントに関する以下の主要な情報を表示できます。

  - **時間**。過剰なデータがアプリケーションまたはウェブサイトにダウンロードされた時間。
  - **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量。

    Secure Private Access 過剰なデータダウンロード イベント詳細(/en-us/citrix-analytics/media/access-control-unusual-download-volume-event-details.png)

ユーザーにどのようなアクションを適用できますか?

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**。将来の潜在的な脅威のためにユーザーを監視したい場合は、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーのアカウントで異常または不審なアクティビティがあった場合、すべてまたは選択された管理者にメール通知が送信されます。

アクションとそれらを手動で構成する方法の詳細については、「」(/ja-jp/security-analytics/policies-and-actions.html#configure-policies-and-actions)を参照してください。

ユーザーにアクションを手動で適用するには、ユーザーのプロファイルに移動し、適切なリスクインジケーターを選択します。「**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**
>
> リスクインジケーターをトリガーするデータソースに関わらず、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 のリスクインジケーター

ありえない移動

Citrix Analytics は、連続するログオンが、2つの異なる国から、それらの国間の予想移動時間よりも短い時間内に行われた場合、ユーザーのログオンを危険と判断します。

ありえない移動時間のシナリオは、以下のリスクを示します。

- **侵害された資格情報**: 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。
- **共有された資格情報**: 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。

ありえない移動リスクインジケーターはいつトリガーされますか?

ありえない移動リスクインジケーターは、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、その距離が個人がその時間内に移動できる距離よりも大きい場合にトリガーされます。

> **注**
>
> このリスクインジケーターには、ユーザーの実際の場所を反映しない以下のシナリオにおける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およびデスクトップにログオンする場合。
> - ユーザーがホスト型クライアントから仮想アプリおよびデスクトップにログオンする場合。

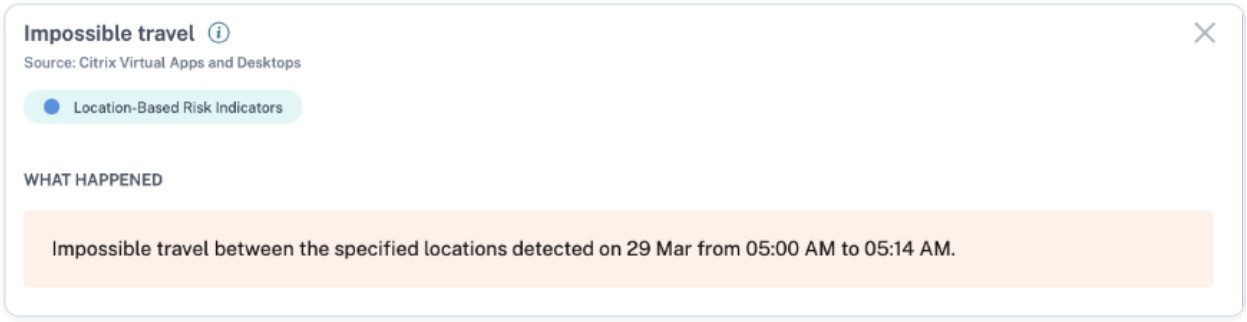
ありえない移動リスクインジケーターを分析する方法

Adam Maxwell というユーザーが、ロシアのモスクワと中国のフフホトという2つの場所から1分以内にログオンしたとします。Citrix Analytics はこのログオンイベントをありえない移動シナリオとして検出し、**ありえない移動**リスクインジケーターをトリガーします。このリスクインジケーターは Adam Maxwell のリスクタイムラインに追加され、彼にリスクスコアが割り当てられます。

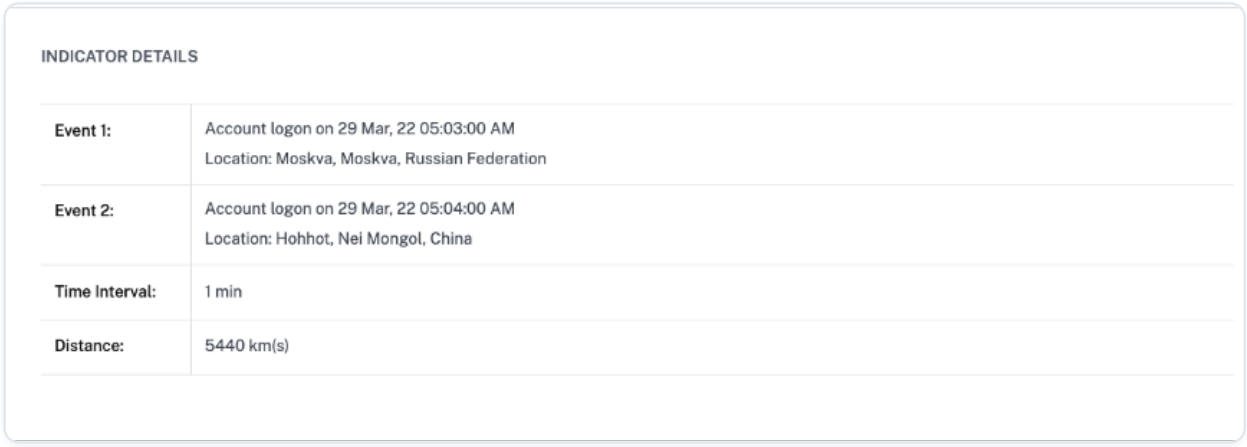
Adam Maxwell のリスクタイムラインを表示するには、**セキュリティ > ユーザー**を選択します。**危険なユーザー**ペインから、ユーザー Adam Maxwell を選択します。

アダム・マックスウェルのリスクタイムラインから、**不可能移動**リスクインジケーターを選択します。次の情報が表示されます。

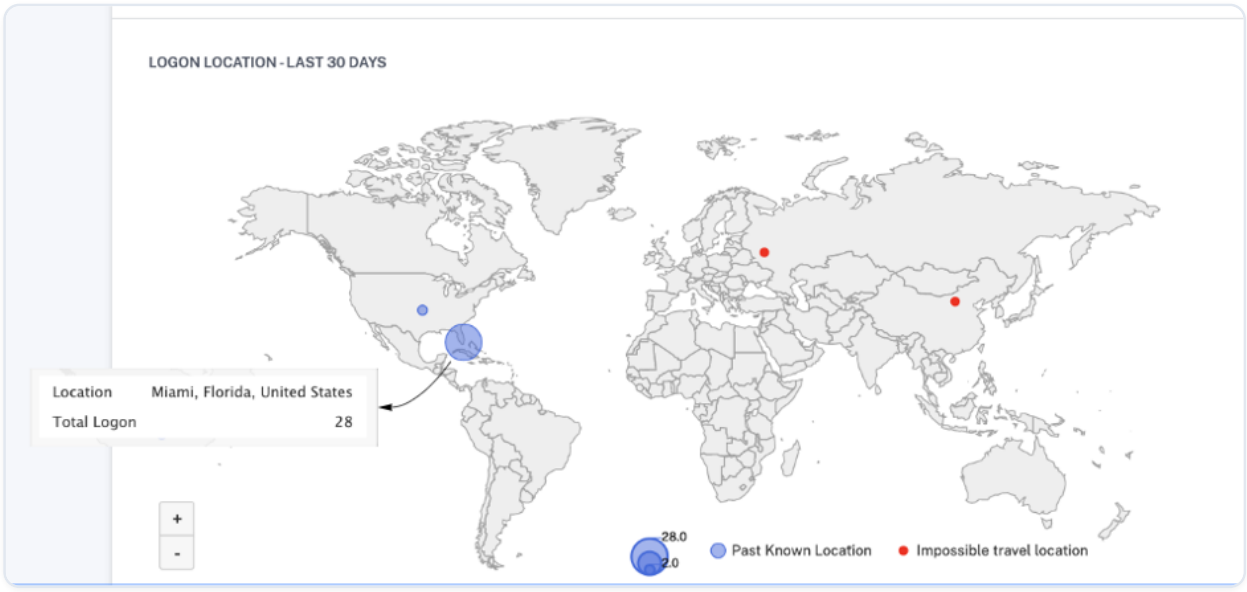
- **何が起こったか**セクションには、不可能移動イベントの簡単な概要が記載されています。



- **インジケーターの詳細**セクションには、ユーザーがログオンした場所、連続するログオン間の時間、および2つの場所間の距離が記載されています。



- **ログオン場所 - 過去30日間**セクションには、不可能移動の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。場所データは過去30日間のものが表示されます。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を表示できます。



- **不可能移動 - イベントの詳細**セクションには、不可能移動イベントに関する次の情報が記載されています。
    - **日付と時刻**: 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。
    - **ログオンタイプ**: 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したときにトリガーされます。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、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。

    過去30日間のログオン場所(/en-us/citrix-analytics/media/impossible-travel-event-details.png)

ユーザーに適用できるアクション?

ユーザー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**。将来的な潜在的脅威についてユーザーを監視したい場合は、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーアカウントで異常または不審なアクティビティがあった場合、すべてまたは選択された管理者にメール通知が送信されます。
- **ユーザーのログオフ**。ユーザーがアカウントからログオフされると、Virtual Desktops を介してリソースにアクセスできなくなります。
- **セッション記録の開始**。ユーザーの Virtual Desktops アカウントで異常なイベントが発生した場合、管理者は将来のログオンセッションのユーザー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。

アクションとそれらを手動で構成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。

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、適切なリスクインジケーターを選択します。**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**
>
> リスクインジケーター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。

潜在的なデータ流出

Citrix Analytics は、データ流出の過剰な試行に基づいてデータ脅威を検出し、対応するリスクインジケーターをトリガーします。

潜在的なデータ流出リスクインジケーターに関連するリスク要因は、データベースのリスクインジケーターです。リスク要因の詳細については、「Citrix ユーザーリスクインジケーター」を参照してください。

潜在的なデータ流出リスクインジケーターは、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のファイル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、クリップボードまたはコピー＆ペーストアクションを使用して流出させることもできます。

> **注**
>
> クリップボード操作は、SaaSアプリケーションのみでサポートされています。

潜在的なデータ漏洩リスクインジケーターはいつトリガーされますか?

ユーザーが特定の期間内に過剰な数のファイルをドライブまたはプリンターに転送した場合に通知を受け取ることができます。このリスクインジケーターは、ユーザーがローカルコンピューターでコピー＆ペースト操作を使用した場合にもトリガーされます。

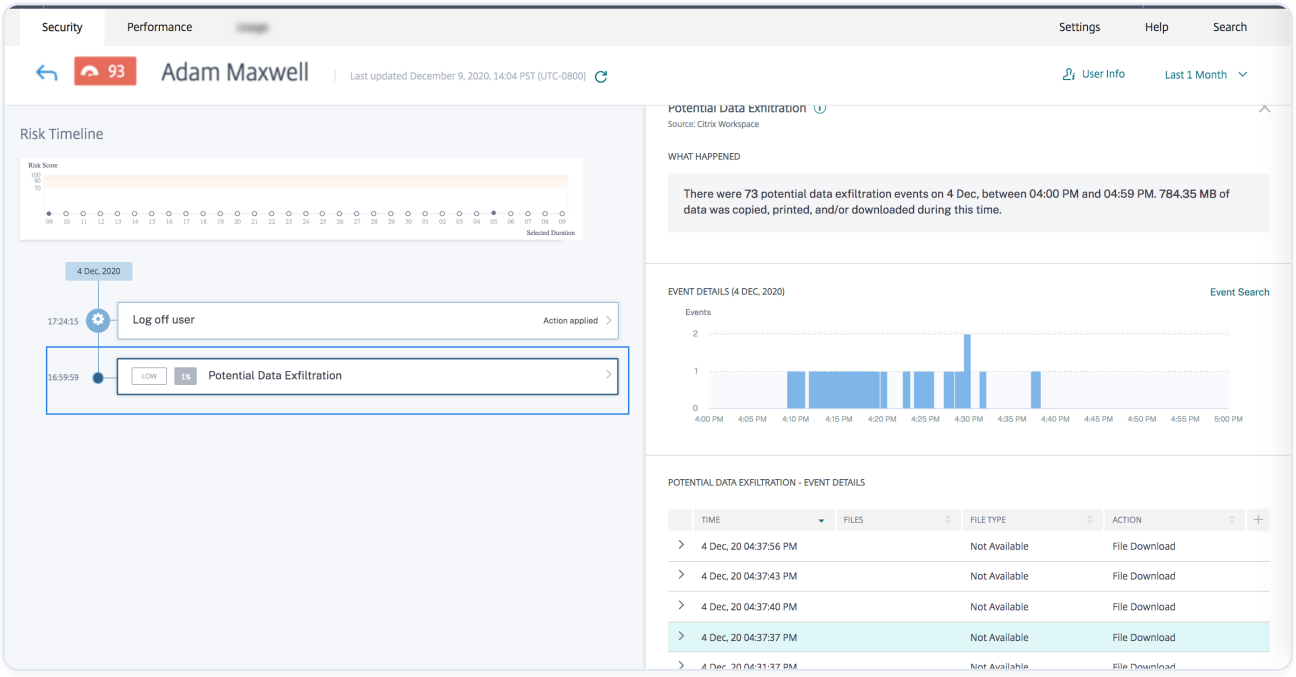
Citrix Receiverがこの動作を検出すると、Citrix Analyticsはこのイベントを受信し、該当するユーザーにリスクスコアを割り当てます。**潜在的なデータ漏洩**リスクインジケーターがユーザーのリスクタイムラインに追加されます。

潜在的なデータ漏洩リスクインジケーターの分析方法?

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いて、通常のファイル転送動作を超過しました。

Adam Maxwellのタイムラインから、**潜在的なデータ漏洩**リスクインジケーターを選択できます。イベントの理由が、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**リスクインジケーターを表示するには、**セキュリティ > ユーザー**に移動し、ユーザーを選択します。



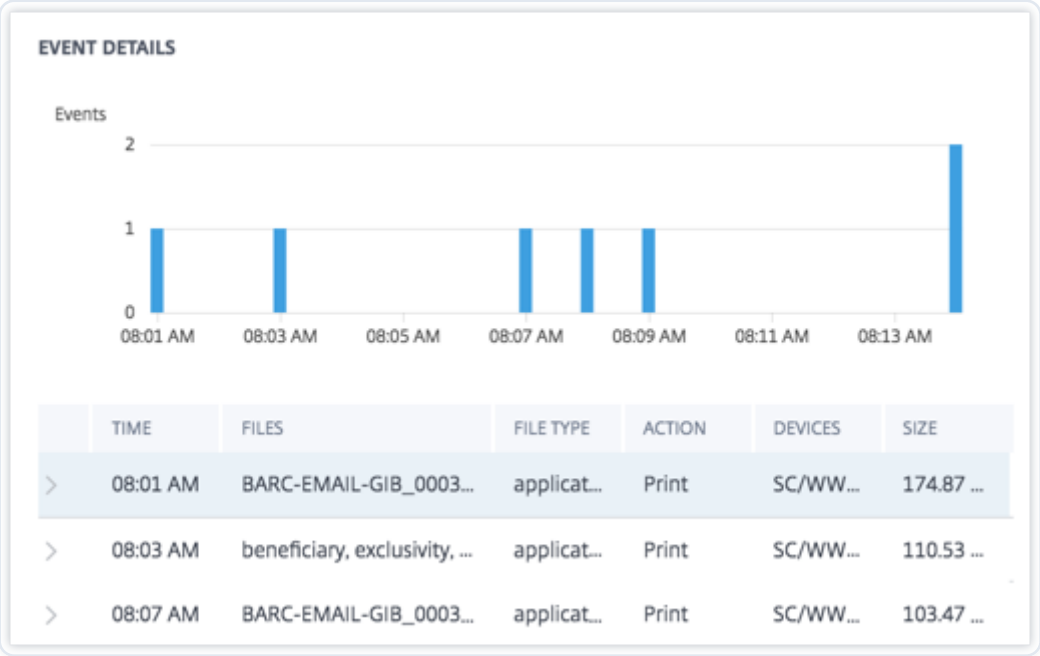
- **何が起こったか**セクションでは、潜在的なデータ漏洩イベントの概要を表示できます。特定の期間におけるデータ漏洩イベントの数を表示できます。



- **イベントの詳細**セクションでは、データ漏洩の試行がグラフ形式と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、表には次の主要情報が示されます。
  - **時間**。データ漏洩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。
  - **ファイルの種類**。ダウンロード、印刷、またはコピーされたファイルの種類。

> **注記**
>
> 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利用可能です。

- **アクション**。実行されたデータ持ち出しイベントの種類（印刷、ダウンロード、またはコピー）。
- **デバイス**。使用されたデバイス。
- **サイズ**。持ち出されたファイルのサイズ。
- **場所**。ユーザーがデータを持ち出そうとしている都市。



- イベント発生時、**追加のコンテキスト情報**セクションで以下を表示できます。
  - 持ち出されたファイルの数。
  - 実行されたアクション。
  - 使用されたアプリケーション。
  - ユーザーが使用したデバイス。



ユーザーにどのようなアクションを適用できますか?

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**。将来的な潜在的脅威のためにユーザーを監視したい場合、ウォッチリストに追加できます。
- **管理者への通知**。ユーザーのアカウントで異常または不審なアクティビティがあった場合、すべてまたは選択された管理者にメール通知が送信されます。
- **ユーザーのログオフ**。ユーザーがアカウントからログオフされると、Virtual Desktops を介してリソースにアクセスできなくなります。
- **セッション記録の開始**。ユーザーの Virtual Desktops アカウントで異常なイベントが発生した場合、管理者は将来のログオンセッションのユーザー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手動での設定方法については、「ポリシーとアクション」を参照してください。

ユーザーにアクションを手動で適用するには、ユーザーのプロファイルに移動し、適切なリスクインジケーターを選択します。**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

リスクインジケーター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。

不審なログオン

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、異常または危険と見なされるユーザーのログオンを検出します。

不審なログオンのリスクインジケーターはいつトリガーされますか?

リスクインジケーターは、以下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つ以上の条件に基づいて潜在的に不審であると見なされます。

要因	条件
異常なデバイス	ユーザーが、過去30日間に使用されていないデバイスからログオンする。
	ユーザーが、仮想アプリおよびデスクトップサーバーによって管理されていないデバイスからログオンする。
	ユーザーが、デバイス署名がユーザーの履歴と一致しないHTML5クライアントまたはChromeクライアントからログオンする。
異常な場所	ユーザーが過去30日間にログオンしていない都市または国からログオンする。
	その都市または国は、最近（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日間にその都市または国からログオンしたユーザーがゼロまたは最小限である。
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する。

要因	条件
	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する。
	過去30日間にそのIPサブネットからログオンしたユーザーがゼロまたは最小限である。
IP脅威	その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であるWebrootによって高リスクとして識別される。
	Citrix Analyticsは、最近、他のユーザーからのそのIPアドレスからの非常に疑わしいログオンアクティビティを検出した。

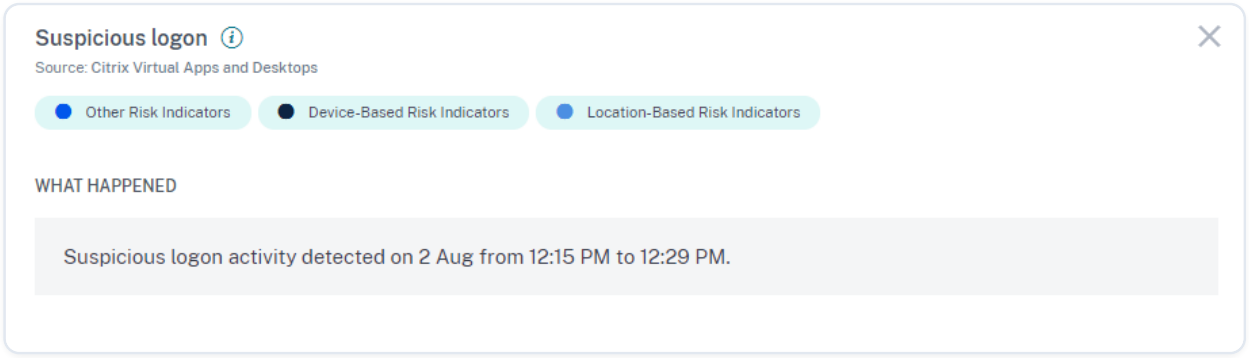
「不審なログオン」リスクインジケーターを分析する方法

インドのムンバイから初めてログオンするユーザー、Adam Maxwellを考えてみましょう。彼は新しいデバイス、または過去30日間使用されていなかったデバイスを使用してCitrix Virtual Apps and Desktopsにログオンし、新しいネットワークに接続しました。Citrix Analyticsは、場所、デバイス、ネットワークという要素が彼の通常の行動から逸脱しているため、このログオンイベントを不審なものとして検出し、「**不審なログオン**」リスクインジケーターをトリガーします。このリスクインジケーターはAdam Maxwellのリスクタイムラインに追加され、彼にはリスクスコアが割り当てられます。

Adam Maxwellのリスクタイムを表示するには、「**セキュリティ > ユーザー**」を選択します。「**リスクのあるユーザー**」ペインから、ユーザーAdam Maxwellを選択します。

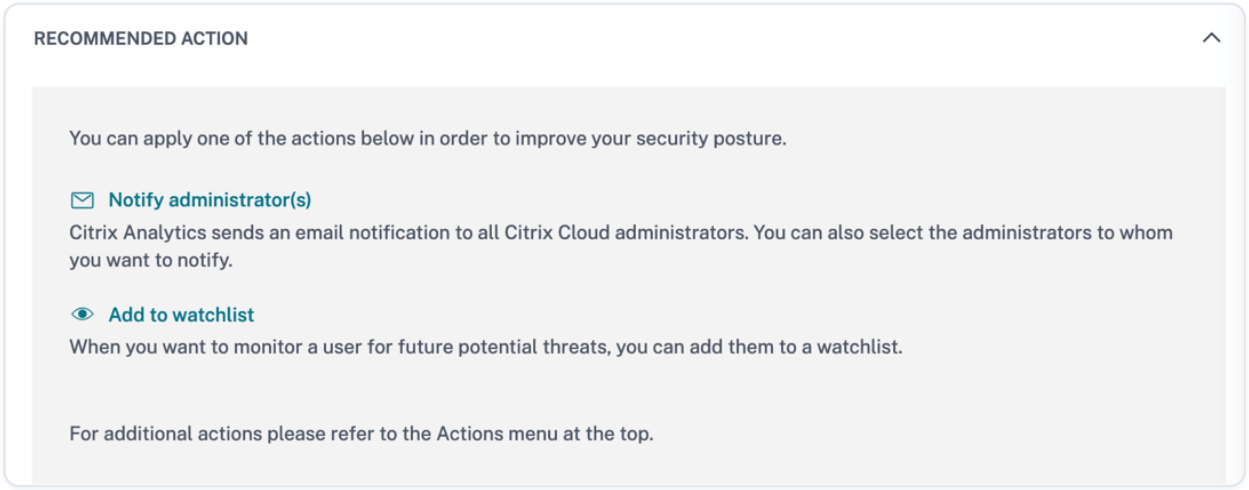
Adam Maxwellのリスクタイムラインから、「不審なログオン」リスクインジケーターを選択します。次の情報を表示できます。

- 「**何が起こったか**」セクションには、リスク要因とイベントの時刻を含む不審なアクティビティの簡単な概要が示されます。



- 「**推奨されるアクション**」セクションには、リスクインジケーターに適用できる推奨アクションが表示されます。Citrix Analytics for Security™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。推奨事項は、次のアクションの1つまたは組み合わせです。
  - 管理者に通知する
  - ウォッチリストに追加する
  - ポリシーを作成する

  推奨事項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**」メニューから、選択に応じて適用したい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。



- 「**ログオンの詳細**」セクションには、各リスク要因に対応する不審なアクティビティの詳細な概要が示されます。各リスク要因には、疑わしさのレベルを示すスコアが割り当てられます。単一のリスク要因だけでは、ユーザーからの高いリスクを示すものではありません。全体的なリスクは、複数のリスク要因の相関関係に基づいています。

疑わしさのレベル	表示
0〜69	その要因は正常に見え、不審とは見なされません。
70〜89	その要因はやや異常に見え、他の要因と合わせて中程度に不審と見なされます。
90〜100	その要因はまったく新しいか異常であり、他の要因と合わせて非常に不審と見なされます。

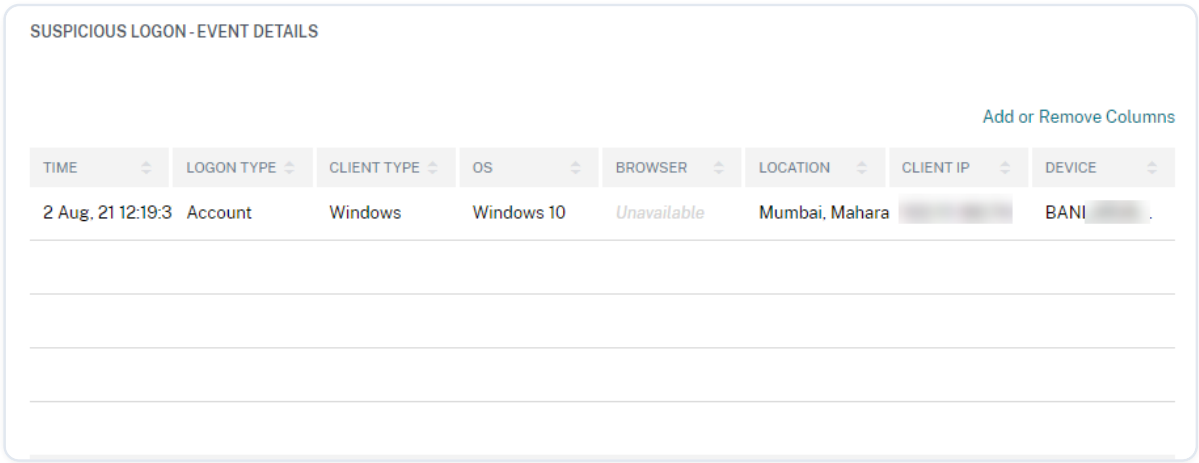
不審なログオンの詳細(/en-us/citrix-analytics/media/susp-logon-cvad-details.png)

- **ログオン場所 - 過去30日間**セクションには、ユーザーの最後に確認された場所と現在の場所の地理的な地図ビューが表示されます。場所データは過去30日間のものが表示されます。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を表示できます。

  不審なログオン場所(/en-us/citrix-analytics/media/susp-logon-cvad-locations-details.png)

- **不審なログオン - イベントの詳細**セクションには、不審な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**: 不審なログオンの日時を示します。
  - **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したときにトリガーされます。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などになります。
  - **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。
  - **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?

ユーザー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**。将来的な潜在的脅威についてユーザーを監視したい場合は、ウォッチリストに追加できます。

- **管理者への通知**。ユーザーアカウントで異常または不審なアクティビティがあった場合、すべてまたは選択された管理者にメール通知が送信されます。
- **ユーザーのログオフ**。ユーザーがアカウントからログオフされると、Virtual Desktops を介してリソースにアクセスできなくなります。
- **セッション記録の開始**。ユーザーの Virtual Desktops アカウントで異常なイベントが発生した場合、管理者は将来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。

アクションとそれらを手動で構成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。

ユーザーにアクションを手動で適用するには、ユーザープロファイルに移動し、適切なリスクインジケーターを選択します。**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**
>
> リスクインジケーター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。

ユーザーリスクインジケーターのフィードバックを提供する

リスクインジケーターは、潜在的に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報告するとともに、ユーザーのリスクスコアを自動的に増加させるように設計されています。実際には、リスクインジケーターの発生の中には、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りますが、無害であることが判明するものもあります。

インジケーターフィードバック機能を使用すると、リスクインジケーターの発生を明示的にフラグ付けできます。

- 真の根底にあるユーザーリスクがあると判断した場合に「役立つ」として
- セキュリティ上の脅威がないと判断した場合に「役立たない」として。この場合、インジケーターの発生はデフォルトでユーザータイムラインから非表示になり、その後の計算でこのインジケーターの発生を除外するようにユーザーのリスクスコアが自動的に調整されます。

さらに、皆様からのフィードバックは、リスクインジケーターアルゴリズムの将来の改善を推進するために使用されます。

フィードバックを提供する(/en-us/citrix-analytics/media/risk-indicator-feedback.png)

フィードバックバナー（親指を立てるアイコンと下げるアイコン付き）は、ユーザータイムラインの各デフォルトリスクインジケーターエントリに表示されます。

- **親指を立てる**アイコン - インジケーターが役立ち、危険なアクティビティを正しく特定したことを示します。親指を立てるアイコンをクリックして、インジケーターがどのように役立つか、その利点について追加のコメントを提供できます。

  フィードバックを保存し、インジケーターを役立つものとしてマークできます。「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。

  フィードバックを編集(/en-us/citrix-analytics/media/risk-indicator-edit-feedback.png)

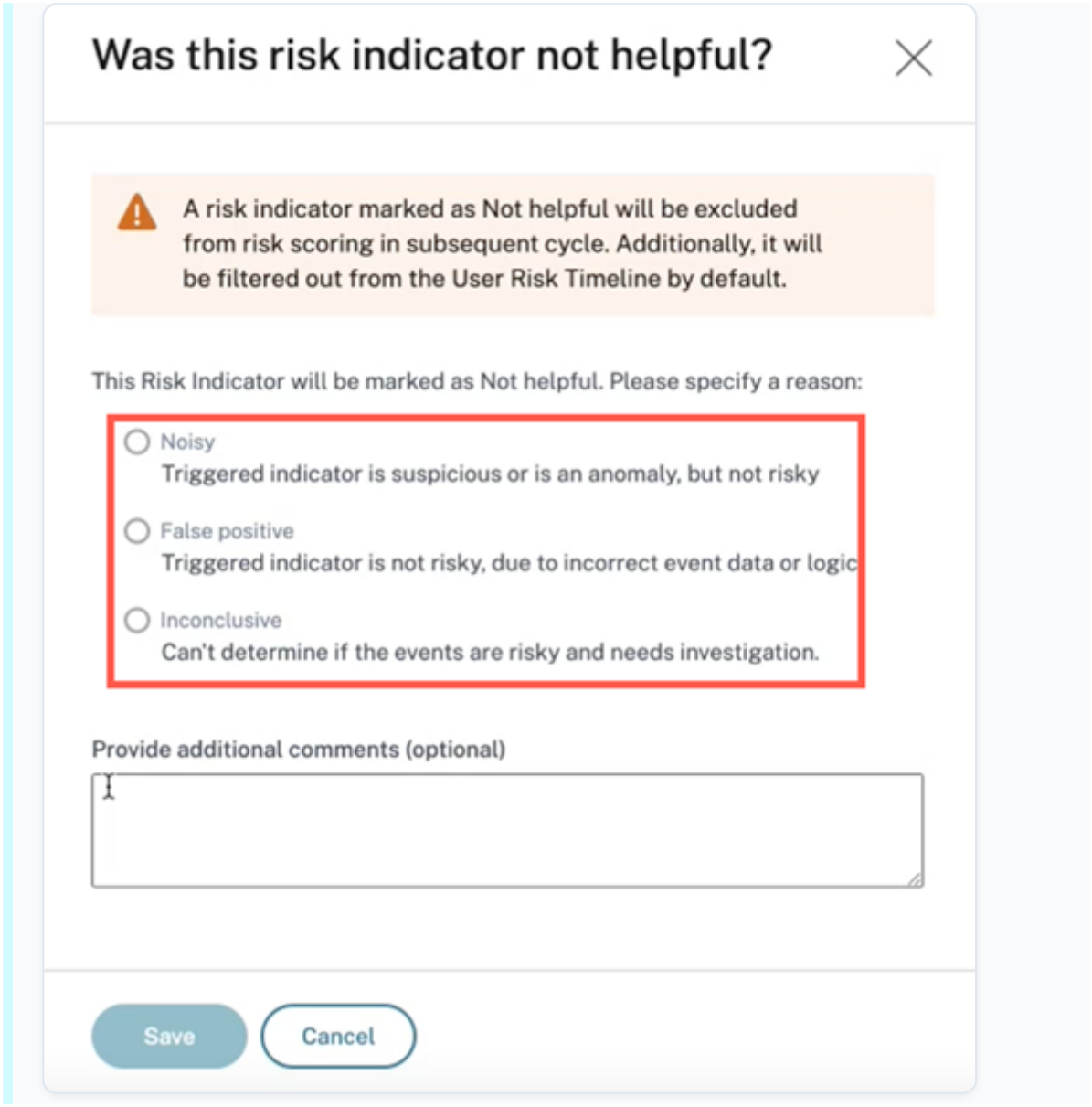
  リスクインジケーターが役立つとマークされると、このフィードバックは対応するユーザータイムラインエントリに表示され、Citrix Analyticsに報告されます。ユーザーリスクスコアには影響しません。

  マークされたフィードバック(/en-us/citrix-analytics/media/risk-indicator-marked-feedback.png)

- **親指を下げる**アイコン - インジケーターが役立たないか、誤ってトリガーされたことを示します。インジケーターを役立たないものとしてマークし、**ノイズ**、**誤検知**、または**結論が出ない**に分類できます。このリスクインジケーターの発生は、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、追加のコメントを提供することもできます。

  - **ノイズ** – トリガーされたインジケーターは疑わしいか異常ですが、危険ではありません。
  - **誤検知** – トリガーされたインジケーターは、イベントデータまたはロジックの誤りのため、リスクがない。
  - **判断不能** – イベントにリスクがあるかどうかを判断できず、調査が必要である。

    > **注**
    >
    > リスクスコアの再調整には最大15分かかります。

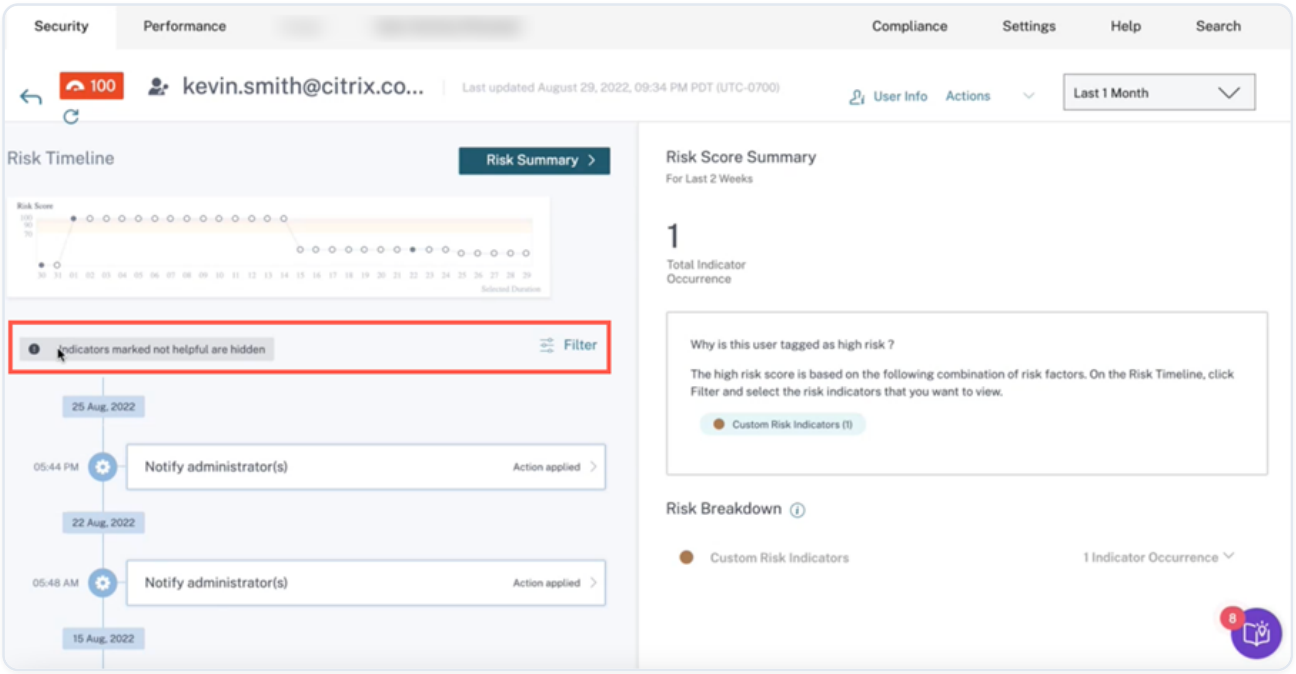


インジケーターが役に立たないとマークされた場合、次の結果が表示されます。

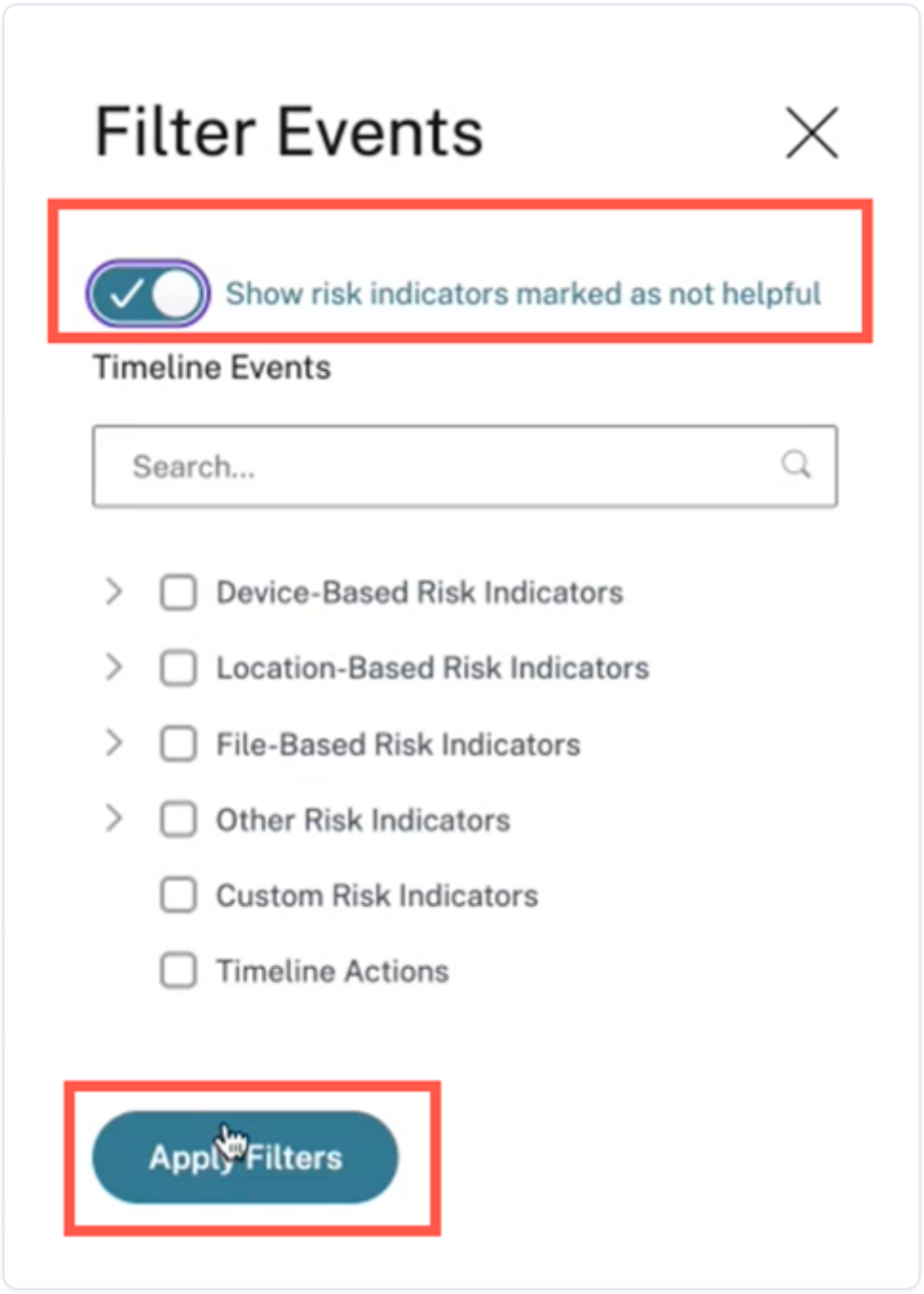
- その特定のインジケーターはタイムラインから非表示になります。
- このインジケーターの発生がその後の更新でリスクスコア計算から除外される結果として、リスクスコアが再調整されます。
- テキストフィードバックとして提供された追加情報は、後で参照できるように保持されます。

フィルターの表示

役に立たないとマークされたインジケーターは、デフォルトで非表示になります。



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インジケーターを表示**をオンにします。



カテゴリに基づいてインジケーターを検索できます。たとえば、場所ベースの非表示のリスクインジケーターを表示するには、カテゴリを選択し、**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とともに、役に立たない場所ベースのすべてのインジケーターを表示できます。

フィルターを適用(/en-us/citrix-analytics/media/risk-indicator-apply-filters.png)

管理者として、必要に応じて、以下の操作も実行できます。

- フィードバックを変更する
- 以前のフィードバックおよび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および関連するメタデータを確認する

注

- フィードバックはテナントレベルではなく、ユーザーレベルで提供できます。1つのリスクインジケーターに対するフィードバックは、その特定のリスクインジケーター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。
- 1人のユーザーに対するフィードバックは、他のユーザーには適用されません。

Microsoft Graph Security のリスクインジケーター

注:

2023年7月以降、Microsoft は Azure Active Directory (Azure AD) を Microsoft Entra ID に名称変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD へのすべての参照は、Microsoft Entra ID を指します。

Microsoft Graph Security は、**Azure AD Identity Protection** または **Microsoft Defender for Endpoint** セキュリティプロバイダーからデータを受信し、その情報を Citrix Analytics に送信します。

Azure AD Identity Protection は、以下のリスクインジケーターをトリガーし、その情報を Microsoft Graph Security に送信します。

- 匿名 IP アドレス
- 異常な場所へのありえない移動
- 資格情報が漏洩したユーザー
- 感染したデバイスからのサインイン
- 不審なアクティビティのある 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

Defender for Endpoint の詳細については、Microsoft Defender for Endpoint を参照してください。

リスクインジケーターに関連付けられているリスク要因は、IP ベースのリスクインジケーターです。リスク要因の詳細については、Citrix ユーザーリスクインジケーター を参照してください。

Microsoft Graph Security のリスクインジケーターを分析する方法

前述の危険な行動のいずれかを示すユーザー Maria Brown を考えてみましょう。Microsoft はこの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、Maria Brown に更新されたリスクスコアを割り当てます。また、適切なリスクインジケーターが 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 Security リスクインジケーター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の最新のリスクインジケーターエントリを選択できます。対応する詳細情報パネルが右ペインに表示されます。**何が起こったか** セクションには、リスクインジケーターの簡単な概要が記載されています。

リスクインジケーターに関する詳細情報を取得する方法

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

現在、Microsoft Graph Security データソースを介し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する機能は利用できません。

Microsoft Graph Security のオンボーディングについては、Microsoft Graph Security を参照してください。

カスタムリスクインジケーター

Citrix Analytics for Security™には、次の2種類のリスクインジケーターがあります。

- **デフォルトのリスクインジケーター**: これらのリスクインジケーターは、機械学習アルゴリズムに基づいています。詳細については、「Citrixユーザーリスクインジケーター」を参照してください。
- **カスタムリスクインジケーター**: これらのリスクインジケーターは、管理者が手動で作成します。

カスタムリスクインジケーターを作成する際は、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と一致すると、Citrix Analyticsはカスタムリスクインジケーターをトリガーし、ユーザーのリスクタイムラインに表示します。

次のデータソースのカスタムリスクインジケーターを作成します。

- Citrix Gateway (シトリックス ゲートウェイ)
- Citrix Secure Private Access™ (シトリックス セキュア プライベート アクセス™)
- Citrix Virtual Apps and Desktops™オンプレミス
- Citrix DaaS (シトリックス DaaS) (旧称 Citrix Virtual Apps and Desktops サービス)
- Citrix Secure Browser (シトリックス セキュア ブラウザ)

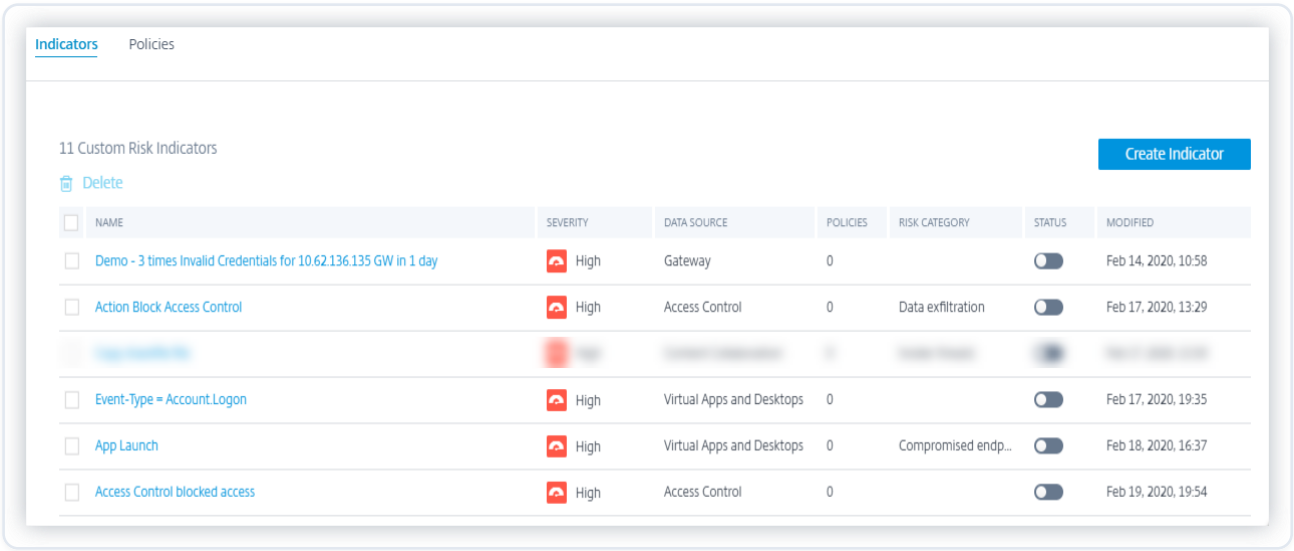
事前構成されたカスタムリスクインジケーター

Citrixは、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、事前構成された条件を持ついくつかのカスタムリスクインジケーターも提供しています。ユースケースに基づいて、事前構成された条件を変更できます。詳細については、「事前構成されたカスタムリスクインジケーター」を参照してください。

カスタムリスクインジケーターページ

カスタムリスクインジケーターページには、ユーザーに対して生成されたすべてのカスタムリスクインジケーター、重大度、データソース、ポリシー数、リスクカテゴリ、ステータス、およびイ

ンジケーターの最終変更日時に関する情報が表示されます。カスタムリスクインジケーターを作成するには、「カスタムリスクインジケーターの作成」を参照してください。



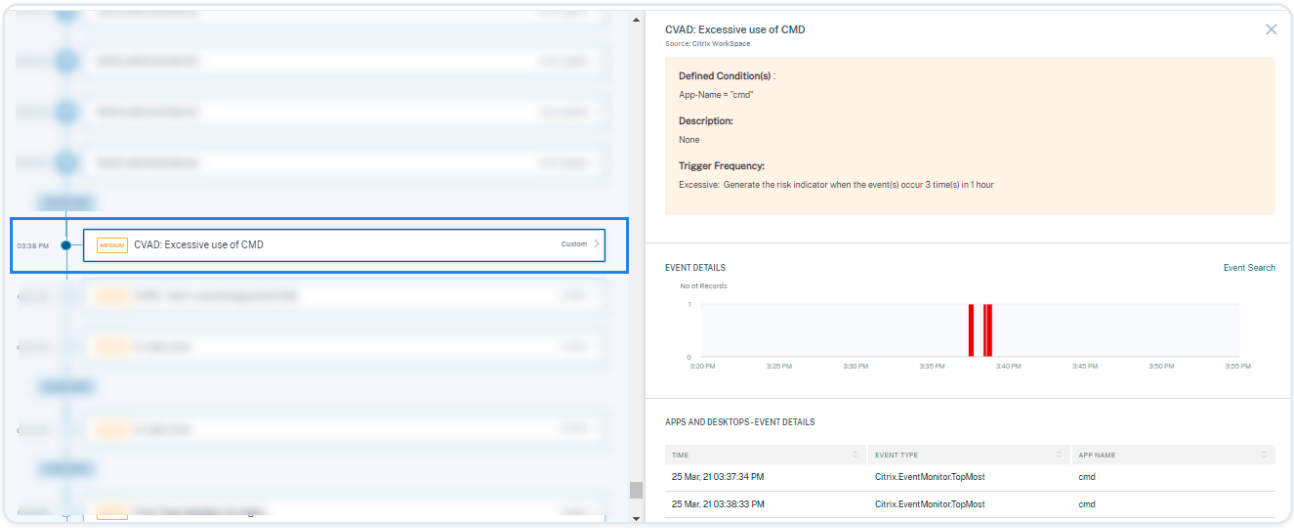
リスクインジケーターを選択すると、**リスクインジケーターの変更**ページにリダイレクトされます。詳細については、「カスタムリスクインジケーターの変更」(#modifying-a-custom-risk-indicator)を参照してください。

カスタムリスクインジケーターの分析

定義したカスタムリスクインジケーターをトリガーしたユーザーを考えてみましょう。Citrix Analyticsは、ユーザーのリスクタイムラインにカスタムリスクインジケーターを表示します。

ユーザーのリスクタイムラインでカスタムリスクインジケーターを選択すると、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**: カスタムリスクインジケーターの作成時に定義する条件の概要が表示されます。
- **説明**: カスタムリスクインジケーターの作成時に指定する説明の概要が表示されます。カスタムリスクインジケーターの作成時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**と表示されます。
- **トリガー頻度**: カスタムリスクインジケーターの作成時に**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**: カスタムリスクインジケーター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が表示されます。**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、ユーザーとカスタムリスクインジケーターに関連付けられたイベントが表示されます。検索クエリには、カスタムリスクインジケーターに定義された条件が表示されます。



注

カスタムリスクインジケーターは、ユーザーのリスクタイムライン上にラベルで表示されます。

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インジケーターがトリガーされた場合、手動でアクションを適用するか、アクションを自動的に適用するポリシーを作成できます。詳細については、「ポリシーとアクション」(/ja-jp/security-analytics/policies-and-actions.html#configure-policies-and-actions)を参照してください。

カスタムリスクインジケーターテンプレート

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インジケーターを作成するか、テンプレートを使用せずに続行できます。

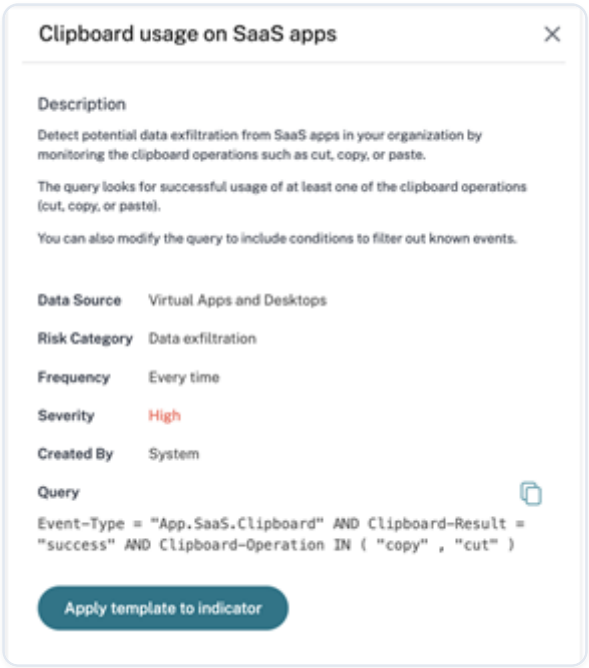
テンプレートは、カスタムリスクインジケーターを作成するための出発点となります。ユースケースに基づいて選択できる事前定義されたクエリとパラメーターを提供することで、カスタムリスクインジケーターの作成をガイドします。

テンプレートを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。テンプレートを使用することで、管理者は追加のトレーニングなしに関心のあるリスクインジケーターを作成できます。

テンプレートは以下の情報で構成されます。

- **説明**: テンプレートで定義された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**: クエリによって検索されるイベントに関連付けられたリスクカテゴリを示します。リスクの高いイベントには、データ漏洩、内部脅威、侵害されたユーザー、侵害されたエンドポイントの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**: イベントに関連付けられた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**: テンプレートで定義された条件を示します。クエリは、条件を満たすユーザーイベントを取得します。

次の画像は、SaaSアプリでのクリップボード使用のユースケースのテンプレートを示しています。

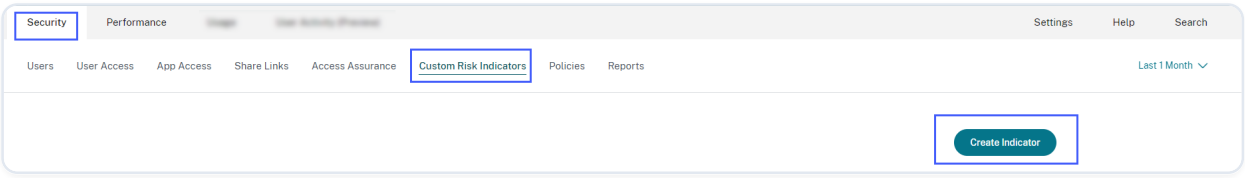


ユースケースに適したテンプレートが見つからない場合、または独自のクエリを定義したい場合は、テンプレートを使用せずに続行できます。

カスタムリスクインジケーターの作成

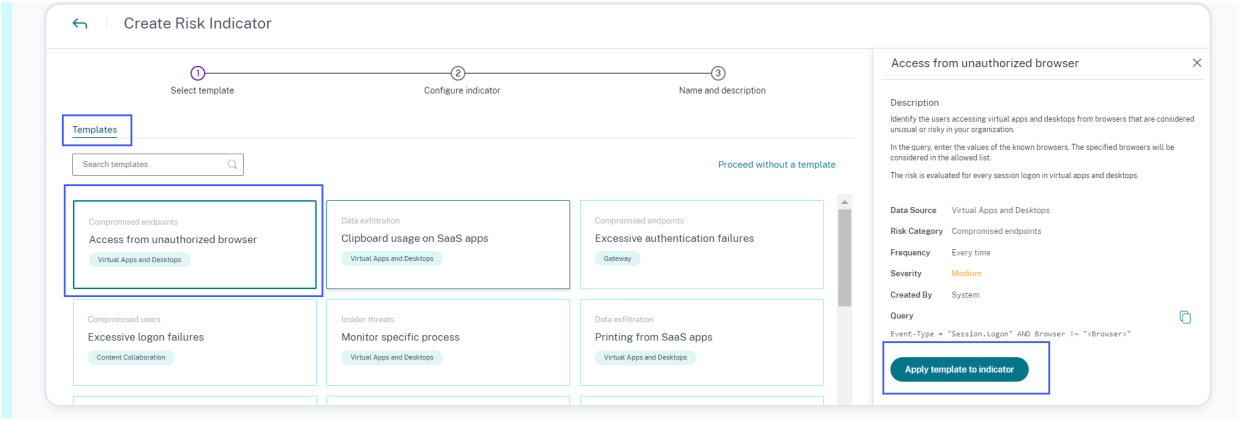
カスタムリスクインジケーターを作成するには：

1. 「**セキュリティ > カスタムリスクインジケーター > インジケーターの作成**」に移動します。

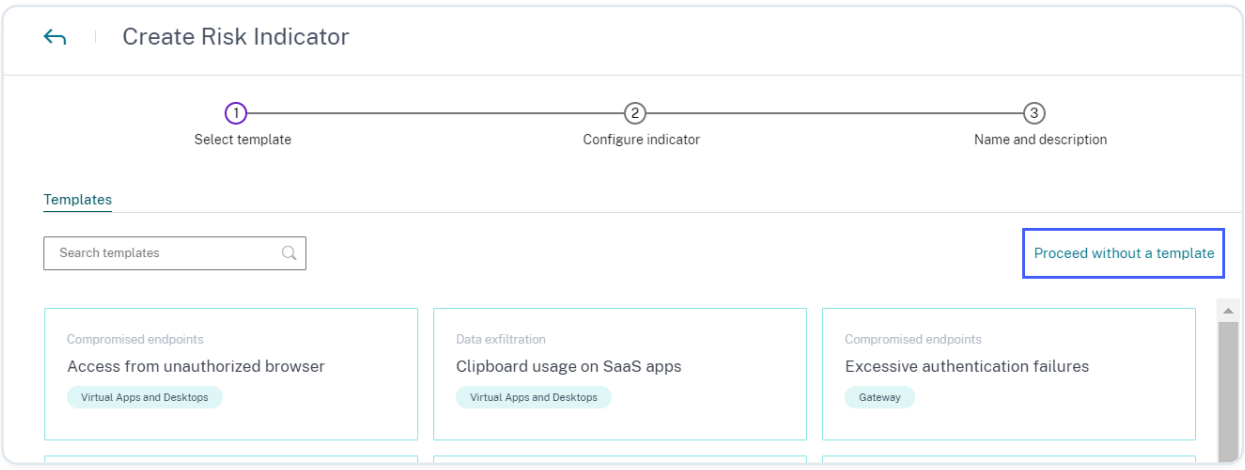


2. ユースケースを表示するにはテンプレートを選択します。要件を満たしている場合は、**テンプレートをインジケーターに適用**を選択します。

> **注**
>
> テンプレートの事前定義された条件とパラメーターも変更できます。



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したい場合は、**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。

> **注**

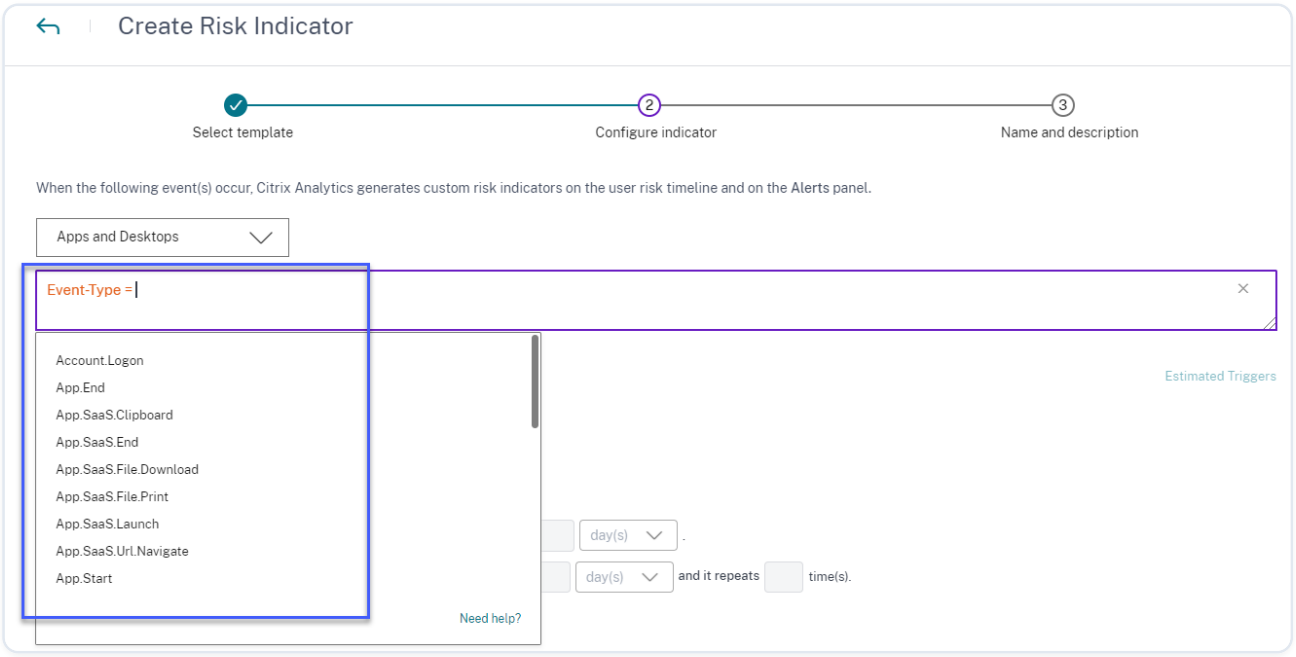
- カスタムリスクインジケーターは最大50個まで作成できます。この最大制限に達した場合は、カスタムリスクインジケーターを作成するために、既存のカスタムリスクインジケーターを削除または編集する必要があります。
- カスタムリスクインジケーターがトリガーされると、すぐにユーザータイムラインに表示されます。ただし、ユーザーのリスク概要とリスクスコアは数分後（約15〜20分後）に更新されます。

カスタムリスクインジケーターの条件を定義する

クエリボックスを使用して、カスタムリスクインジケーターの条件を定義します。選択したデータソースに応じて、条件を定義するための対応するディメンションと有効な演算子が表示されます。

特定のディメンション（`Event-Type` や `Clipboard-Operation` など）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。提案された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。

次の画像は、ディメンション `Event-Type` の推奨値を示しています。



テンプレートを使用する場合、条件は事前定義されています。ただし、ユースケースに基づいて、事前定義された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。このリンクをクリックすると、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インジケーターのおおよそのインスタンスを予測できます。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。

最後に定義された条件に対するカスタムリスクインジケーターの発生数を予測するには、必ず**推定トリガー**をクリックしてください。

高度なオプションの使用

高度なオプションセクションで、カスタムリスクインジケーター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は**毎回: イベントが発生するたびにリスクインジケーターを生成する**をデフォルトオプションとみなし、カスタムリスクインジケーターを生成します。次のいずれかのオプションを選択できます。

- **毎回**: イベントが定義された条件を満たすたびに、リスクインジケーターがトリガーされます。
- **初回**: イベントが定義された条件を初めて満たしたときに、リスクインジケーターがトリガーされます。
    - **新規の初回**: このオプションを有効にすると、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できます。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、1つのエンティティのみを選択できます。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インジケーターを作成できます。たとえば、エンティティとして「都市」を選択した場合、都市名を指定する必要はありません。新しい都市から初めてイベントが受信されたときに、リスクインジケーターがトリガーされます。

      次の表は、各データソースに対応するエンティティを一覧表示し、トリガー条件について説明しています。

データソース	エンティティ	トリガー条件
セキュアプライベートアクセス	都市	ユーザーが初めて新しい都市からログオンした場合。
	クライアントIP	ユーザーが初めて新しいIPアドレスからログオンした場合。
	国	ユーザーが初めて新しい国からログオンした場合。
アプリとデスクトップ	アプリ名	ユーザーが初めて新しい仮想アプリケーションまたは

データソース	エンティティ	トリガー条件
		SaaSアプリケーションを開いた場合。
	アプリURL	ユーザーが初めて仮想デスクトップのブラウザで新しいアプリURLを入力した場合。
	都市	ユーザーが初めて新しい都市からアプリまたはデスクトップを起動した場合。
	クライアントIP	ユーザーが初めて新しいIPアドレスからログオンしたとき。
	国	ユーザーが初めて新しい国からアプリまたはデスクトップを起動したとき。
	デバイスID	ユーザーが初めて、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起動したとき。
	ダウンロードデバイスタイプ	ユーザーが初めてUSBドライブなどの新しいストレージメディアを使用したとき。
	印刷ファイル形式	印刷されたファイルの形式。
	印刷ファイルサイズ	印刷されたファイルのサイズ（バイト単位）。
	印刷ファイル名	印刷されたファイルの名前。

データソース	エンティティ	トリガー条件
	プリンター名	使用されたプリンターの名前。
	印刷部数合計	ユーザーが印刷したコピーの総数。
	印刷ページ数合計	ユーザーが印刷したドキュメントページの総数。
ゲートウェイ	クライアントIP	ユーザーが初めて新しいIPアドレスからログインした場合。
セキュアブラウザ	ユーザー名	イベントを開始したユーザーの名前。
	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。
	アクセスされたホスト名	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。
	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。

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インジケーターを示しています。このリスクインジケーターは、ユーザーが新しいデバイスから初めて仮想デスクトップまたは仮想アプリを起動したときにトリガーされます。

初めてのデバイスID(/en-us/citrix-analytics/media/first-time-device-id.png)

また、**新規の初回**オプションと合わせて条件を追加することもできます。この場合、リスクインジケーターは、新しいエンティティからのイベントを初めて検出し、かつそのイベントが定義された条件を満たしたときにトリガーされます。

次の例は、カスタムリスクインジケーターに定義された条件と、**新規のDevice-IDの初回**オプションが有効になっている状態を示しています。このリスクインジケーターは、インドにいるユーザーが新しいデバイスから初めて仮想デスクトップセッションを起動したときにトリガーされます。

条件付きの初回(/en-us/citrix-analytics/media/first-time-for-new-with-condition.png)

- **過剰**: リスクインジケーターは、次の条件が満たされた後にトリガーされます。
  - イベントが定義された条件を満たしている。
  - イベントが指定された期間内に指定された回数発生する。
- **頻繁**: リスクインジケーターは、次の条件が満たされた後にトリガーされます。
  - イベントが定義された条件を満たしている。
  - イベントが指定された期間内に指定された回数発生する。
  - イベントパターンが指定された回数繰り返される。

リスクカテゴリの選択

カスタムリスクインジケーターのリスクカテゴリを選択します。

リスクインジケーターは、カスタムリスクインジケーターのリスクエクスポージャーの種類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、リスクインジケーターによって検出される危険なイベントの深刻度を示します。カスタムリスクインジケーターを作成する際は、重大度（高、中、低）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事前に選択されます。この事前選択は、ユースケースに応じて変更できます。

条件定義でサポートされている演算子

条件を定義する際に、以下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。	ユーザー名 : 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。	ユーザー名 = 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。	ユーザー名 ~ test	類似のユーザー名を持つイベントを表示します。
""	スペースで区切られた値を囲みます。	ユーザー名 = "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。	データ量 > 100	データ量が100 GBを超えるイベントを表示します。
AND	両方の条件が真である値を検索します。	ユーザー名 : John AND データ量 > 100	データ量が100 GBを超えるユーザーJohnのイベントを表示します。
*	その文字に0回以上一致する値を検索します。	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。
!~	指定した一致パターンについてユーザーイベントをチェックします。このNOT LIKE演算子は、イベ	ユーザー名 !~ John	John、John Smith、または「John」という一致名を含むその他のユーザーを除く

演算子	説明	例	出力
	ント文字列内のどこにも一致パターンが含まれていないイベントを返します。		イベントを表示します。
!=	指定した正確な文字列についてユーザーイベントをチェックします。このNOT EQUAL演算子は、イベント文字列内のどこにも正確な文字列が含まれていないイベントを返します。	国 != USA	USAを除く国のイベントを表示します。
IN	1つ以上の値に関連するイベントを取得するために、ディメンションに複数の値を割り当てます。	ユーザー名 IN (John, Kevin)	JohnまたはKevinに関連するすべてのイベントを検索します。
NOT IN	ディメンションに複数の値を割り当て、指定された値を含まないイベントを検索します。	ユーザー名 NOT IN (John, Kevin)	JohnとKevinを除くすべてのユーザーのイベントを検索します。
空である	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`のような文字列型のディメンションにのみ機能します。`Upload-File-Size`、`Download-File-Size`、`Client-IP`のような非文字列	国が空である	国名が利用できない、または空（指定されていない）であるイベントを検索します。

演算子	説明	例	出力
	（数値）型のディメンションには機能しません。		
空ではない	ディメンションのnullではない値または特定の値をチェックします。この演算子は、`App-Name`、`Browser`、`Country`のような文字列型のディメンションにのみ機能します。`Upload-File-Size`、`Download-File-Size`、`Client-IP`のような非文字列（数値）型のディメンションには機能しません。	国が空ではない	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	いずれかまたは両方の条件が真である値を検索します。	(User-Name = `John*` または User-Name = `*Smith`) かつ Event-Type = “Session.Logon”	Johnで始まる、またはSmithで終わるすべてのユーザー名の`Session.Logon`イベントを表示します。

注

NOT EQUAL演算子の場合、条件内のディメンションの値を入力する際は、データソースのセルフサービス検索ページで利用可能な正確な値を使用してください。ディメンション値は大文字と小文字を区別します。

カスタムリスクインジケーターの変更

1. 「**Security > Custom Risk Indicators**」に移動します。

2. 変更したいカスタムリスクインジケーターを選択します。
3. 「**Modify Indicator**」ページで、必要に応じて情報を変更します。
4. 「**Save Changes**」をクリックします。

注

既存のカスタムリスクインジケーターの条件、リスクカテゴリ、重大度、名前などの属性を変更した場合でも、ユーザータイムラインでは、そのユーザーに対してトリガーされたカスタムリスクインジケーターの以前の発生（古い属性を持つもの）を引き続き表示できます。

例えば、条件が *Country != India* のカスタムリスクインジケーターを作成したとします。このカスタムリスクインジケーターは、ユーザーがインド国外からログインしたときにトリガーされます。ここで、カスタムリスクインジケーターの条件を *Country != "United States"* に変更します。この場合でも、リスクインジケーターをトリガーしたユーザーのタイムラインで、条件が *Country != India* のカスタムリスクインジケーターの以前の発生を引き続き表示できます。

カスタムリスクインジケーターの削除

1. 「**Security > Custom Risk Indicators**」に移動します。
2. 削除したいカスタムリスクインジケーターを選択します。
3. 「**Delete**」をクリックします。
4. ダイアログで、カスタムリスクインジケーターの削除リクエストを確認します。

注

カスタムリスクインジケーターを削除した場合でも、ユーザータイムラインでは、そのユーザーに対してトリガーされたカスタムリスクインジケーターの以前の発生を引き続き表示できます。

例えば、条件が *Country != India* の既存のカスタムリスクインジケーターを削除したとします。この場合でも、リスクインジケーターをトリガーしたユーザーのタイムラインで、条件が *Country != India* のカスタムリスクインジケーターの以前の発生を引き続き表示できます。

継続的なリスク評価

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したことで、Citrix Workspace™ユーザーはほぼあらゆる場所、あらゆるデバイスから作業できるようになりました。この柔軟性に伴う課題は、リモートアクセスがデータ持ち出し、盗難、破壊行為、サービス中断などのサイバー犯罪活動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、この損害の一因となる可能性があります。

このようなリスクに対処する従来のいくつかの方法は、多要素認証、短いサインインセッションなどを実装することです。これらのリスク評価方法はより高いレベルのセキュリティを保証しますが、ユーザーの初期検証後も完全なセキュリティを提供するわけではありません。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した場合、組織に有害な機密データを悪用します。

セキュリティ面を強化し、より良いユーザーエクスペリエンスを確保するために、Citrix Analyticsは継続的なリスク評価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 service) を使用しているユーザーのリスク露出が、初期段階で検証されたときと同じままであり、ユーザーが毎回それを証明する必要がないようにすることで、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にアクションを自動的に適用することによって実現されます。

継続的なリスク評価(/en-us/citrix-analytics/media/continuous-risk-assessment.png)

ユースケース

通常の行動とは異なる、異常な場所からの複数回のサインイン試行失敗の後、初めてネットワークにアクセスできたユーザー、Adam Maxwellを考えてみましょう。また、その場所はサイバー攻撃の履歴があります。このシナリオでは、Adamのアカウントがさらに悪用されるのを防ぐために、直ちに対策を講じる必要があります。Adamのアカウントをロックし、講じられた対策について彼に通知することができます。この対策により、ユーザーのアカウントに一時的なサービス中断が発生する可能性があります。ユーザーはアカウントを復元するために管理者に連絡して支援を求めることができます。

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。Adamに連絡し、このアクティビティを認識しているか確認を求めることができま

す。もしそうであれば、Adamが作業デバイスを変更し、自宅の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、無視できます。しかし、ユーザーがこのアクティビティを実行しなかった場合、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、さらなる損害を防ぐためにユーザーのアカウントをロックすることができます。

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一部の機能を自動化します。

複数の条件をサポート

ポリシーを作成または変更する際に、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インジケーターとカスタムリスクインジケーター、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することができます。

詳細については、「エンドユーザーの応答を要求する」を参照してください。

アクション適用後にユーザーに通知する

一部の活動では、アクションを適用する前にユーザーの応答を待つと、ユーザーのアカウントと組織のセキュリティが危険にさらされる可能性があります。そ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破壊的なアクションを適用し、その旨をユーザーに通知できます。

詳細については、「破壊的なアクションの適用後にユーザーに通知する」を参照してください。

適用モードと監視モード

要件に基づいて、ポリシーを適用モードまたは監視モードに設定できます。適用モードのポリシーは、ユーザーのアカウントに直接影響を与えます。ただし、ポリシーを実装する前にその影響や結果を評価したい場合は、ポリシーを監視モードに設定できます。

詳細については、「サポートされているモード」を参照してください。

アクセスおよびポリシーダッシュボードの可視性

アクセス概要ダッシュボードを使用すると、ユーザーによるアクセス試行回数に関するインサイトを得ることができます。詳細については、「アクセス概要」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たポリシーとアクションに関するインサイト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。

デフォルトポリシー

Citrix Analyticsでは、**ポリシー**ダッシュボードでデフォルトで有効になっている事前定義されたポリシーが導入されています。これらのポリシーは、リスクインジケーターとユーザーリスクスコアを事前定義された条件として使用して作成されます。すべてのデフォルトポリシーにはグローバルアクションが割り当てられています。

> **注**
>
> 環境に表示されるポリシーは、Citrix Analyticsを初めて使用した時期や、ローカルで変更を加え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。

以下のデフォルトポリシーを使用するか、要件に基づいて変更できます。

ポリシー名	条件	データソース	アクション
認証情報の悪用成功	過剰な認証失敗 と 不審なログオン のリスクインジケーターがトリガーされた場合	シトリックス ゲートウェイ	ユーザーをロック
潜在的なデータ流出	潜在的なデータ流出 のリスクインジケーターがトリガーされた場合	シトリックス バーチャルアプリおよびデスクトップおよびシトリックス DaaS	ユーザーをログオフ
不審なIPからの異常なアクセス	不審なログオン と 不審なIPからのログオン のリスクインジ	シトリックス ゲートウェイ	ユーザーをロックする

ポリシー名	条件	データソース	アクション
	ケーターがトリガーされた場合		
デバイスからの初回アクセス	CVAD- First time access from new deviceリスクインジケーターがトリガーされた場合	シトリックス バーチャル アプリケーションズ アンド デスクトップ および シトリックス DaaS	エンドユーザーの応答を要求する
アクセス時の不可能な移動	Impossible Travelリスクインジケーターがトリガーされた場合。	シトリックス バーチャル アプリケーションズ アンド デスクトップ および シトリックス DaaS	エンドユーザーの応答を要求する
認証時の不可能な移動	Impossible Travelリスクインジケーターがトリガーされた場合。	シトリックス ゲートウェイ	エンドユーザーの応答を要求する

ポリシーとアクション

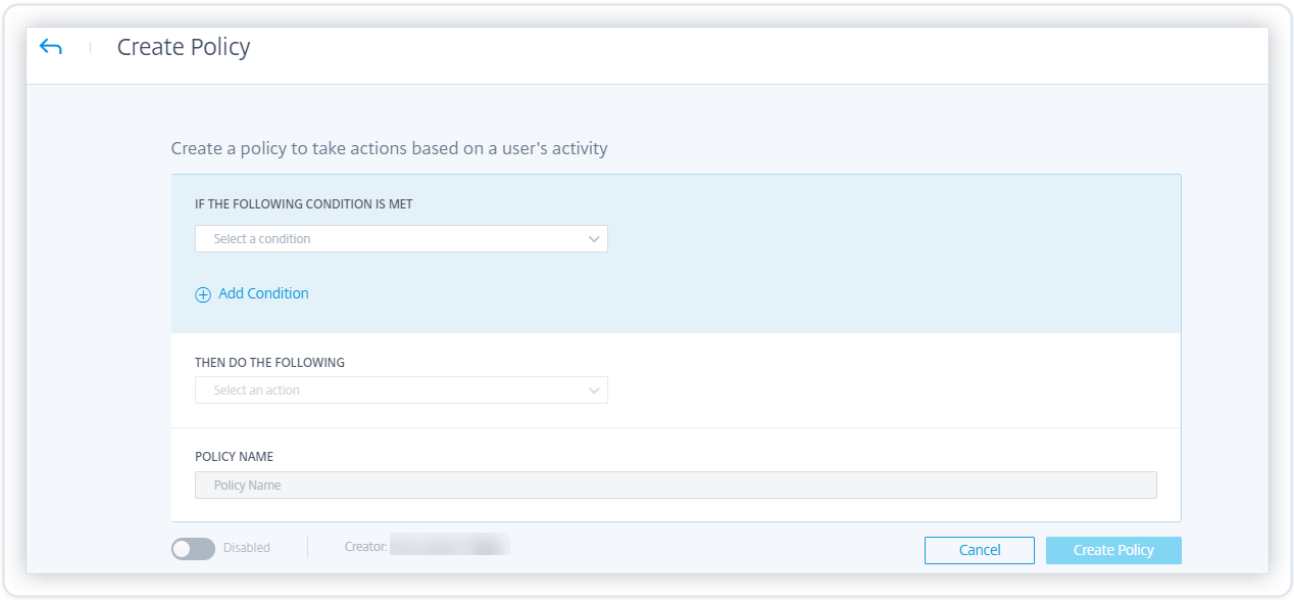
> **注**
>
> **注意**: Citrix Content Collaboration™ および ShareFile は、サポート終了 (EOL) に達し、ユーザーは利用できなくなりました。

Citrix Analytics でポリシーを作成すると、異常なアクティビティや不審なアクティビティが発生した場合に、ユーザーアカウントに対してアクションを実行できます。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、異常なイベントが発生し、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。異常なアクティビティがあるユーザーアカウントに対して、手動でアクションを適用することもできます。

ポリシーとは何ですか?

ポリシーとは、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、ユーザーアカウントに適用できる1つのアクションを持つ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できます。その他の条件は、データソースとそのリスクインジケーターに固有のものです。条件には、リスクスコア、デフォルトのリスクインジケーター、カスタムリスクインジケーターの組み合わせが含まれます。ポリシーを作成する際に、最大4つの条件を追加できます。



たとえば、組織が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したいと考えるかもしれません。しかし、大規模な組織の場合、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現実的ではありません。機密データを過度に共有するユーザーをウォッチリストに追加したり、アカウントを即座に無効にしたりするポリシーを作成できます。

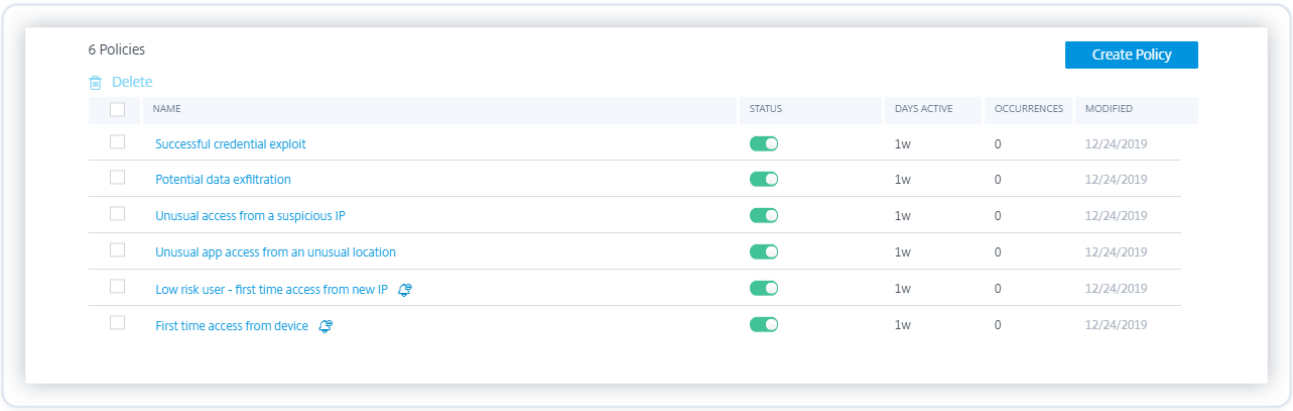
デフォルトポリシー

デフォルトポリシーは、**ポリシー**ダッシュボードで事前定義され、有効になっています。これらは事前定義された条件に基づいて作成され、すべてのデフォルトポリシーに対応するアクションが割り当てられます。デフォルトポリシーを使用するか、要件に基づいて変更することができます。

Citrix Analytics は、以下のデフォルトポリシーをサポートしています。

- 資格情報の悪用成功
- データ流出の可能性
- 不審な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 および Citrix DaaS - アクセス時のありえない移動
- Gateway - 認証時のありえない移動

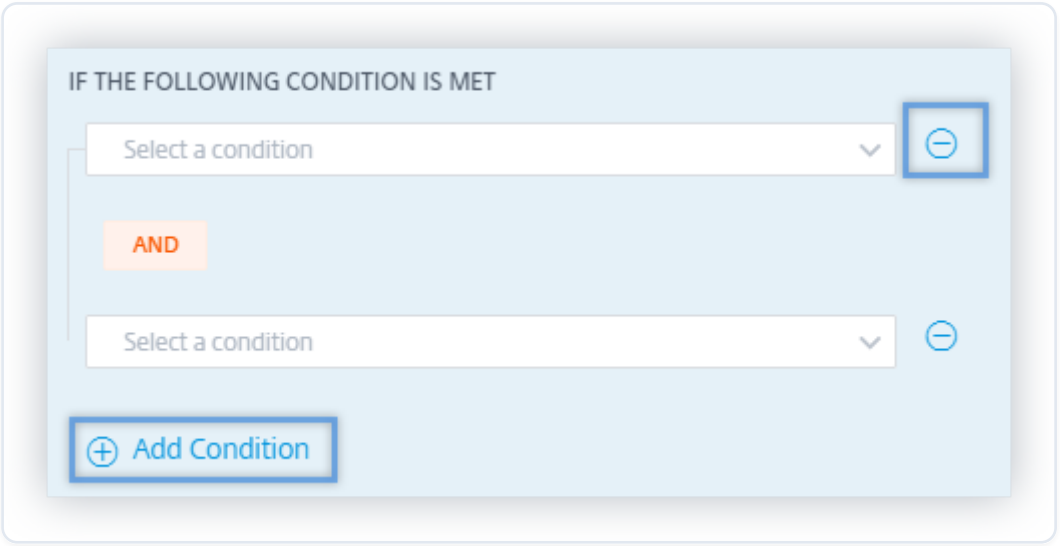
前述のデフォルトポリシーに関する事前設定された条件とアクションについては、「継続的なリスク評価」を参照してください。



ジオフェンシングのユースケースに対する事前定義されたポリシーについては、「事前設定されたポリシー」を参照してください。

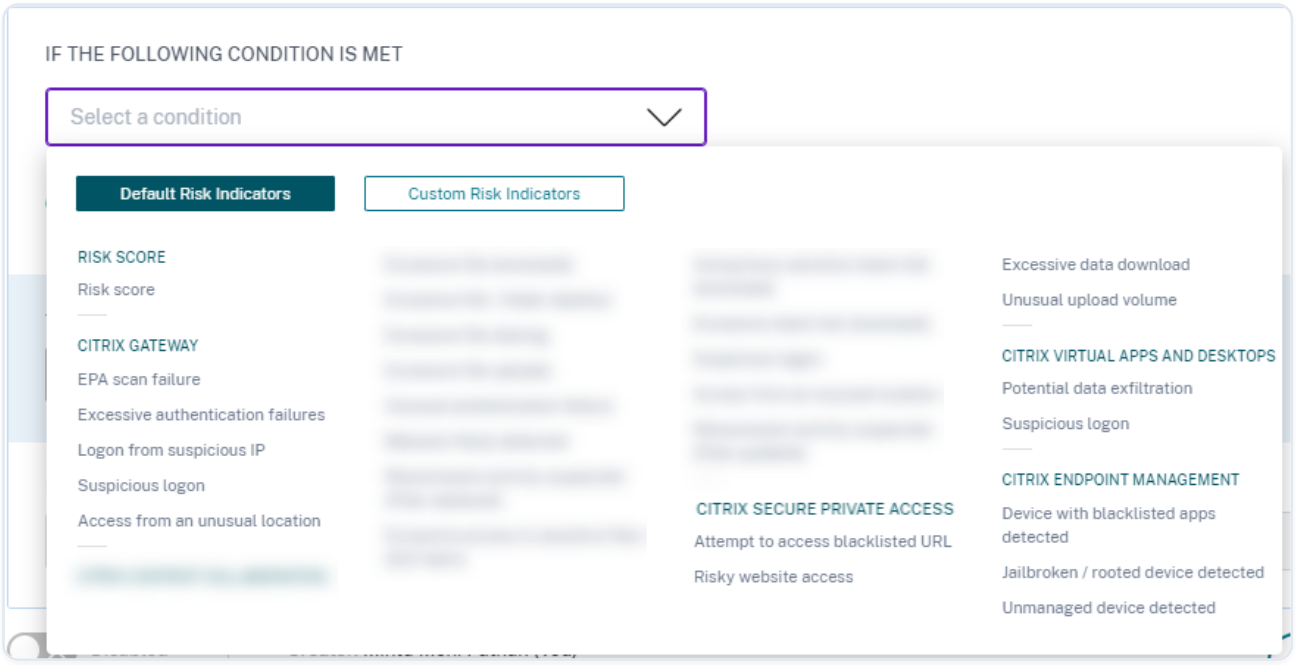
条件を追加または削除する方法?

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た場合**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。



デフォルトおよびカスタムのリスクインジケーター

条件メニューは、**ポリシーの作成**ページの**デフォルトのリスクインジケーター**タブと**カスタムのリスクインジケーター**タブに基づいて分類されています。これらのタブを使用すると、ポリシー構成の条件を選択する際に、選択したいリスクインジケーターの種類を簡単に特定できます。



アクションとは何ですか?

アクションとは、将来の異常なイベントの発生を防ぐための不審なイベントへの対応です。異常または不審な動作を示すユーザーアカウントにアクションを適用できます。ポリシーを設定してユーザーアカウントにアクションを自動的に適用するか、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することができます。

グローバルアクションまたはCitrixデータソースごとの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されたアクションをいつでも無効にすることができます。

注

リスクインジケーター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。

次の表は、実行できるアクションについて説明しています。

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対してユーザーを監視したい場合	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
	は、ウォッチリストに追加できます。	
	ウォッチリストのユーザーペインには、アカウント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したい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、ユーザーのプロファイルに移動し、**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。	
管理者への通知	ユーザーに対してリスクインジケーターがトリガーされた場合、管理者に手動で通知するか、自動通知のポリシーを作成できます。組織内のCitrix Cloudドメインおよびその他のCitrix Cloud以外のドメインから管理者を選択できます。フルアクセス権限を持つCitrix Cloud管理者である場合、デフォルトでは、Citrix Cloudアカウントのメール通知は無効になっています。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、「メール通知の受信」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	

アクション名	説明	適用可能なデータソース
	権限（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アカウントのメール通知は有効になっています。Citrix Analyticsからの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、通知管理者配布リストから名前を削除するよう依頼してください。詳細については、「メール配布リスト」を参照してください。	
エンドユーザーの応答を要求	ユーザーアカウントで異常または不審なアクティビティがあった場合、ユーザーがそのアクティビティを認識しているかどうかを確認するためにユーザーに通知できます。そのアクティビティに基づいて、ユーザーアカウントに対して次に取るべき行動を決定できます。詳細については、「エンドユーザーの応答を要求する」を参照してください。	
エンドユーザーに通知	ユーザーアカウントで異常または不審なアクティビティが発生した場合、電子メール通知を介してエンドユーザーに通知できます。詳細については、「エンドユーザーに通知」を参照してください。	
Citrix Gatewayアクション		
アクティブなセッションをログオフ	この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	Citrix Gatewayオンプレミスおよび Citrix Application Delivery Management

アクション名	説明	適用可能なデータソース
	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。	
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アカウントがロックされた場合、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することはできません。	Citrix Gatewayオンプレミス
ユーザーアカウントのロックを解除	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™およびCitrix DaaSアクション		
アクティブなセッションをログオフ	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 (以前の Citrix Virtual Apps and Desktops のサービス)
セッション記録の開始	ユーザーのVirtual Desktopsアカウントで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アクティブな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おり、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から動的にセッション記録開始	Citrix DaaS (以前の Citrix Virtual Apps and Desktops のサービス)

アクション名	説明	適用可能なデータソース
	アクションをトリガーして、ユーザーの現在アクティブなセッションの記録を開始できます。	

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

Citrix Analytics for Security は、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、事前設定された(/ja-jp/security-analytics/custom-risk-indicators.html)と(/ja-jp/security-analytics/policies-and-actions.html)のリストを提供します。これらの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の条件は、侵害されたユーザー、内部脅威、データ流出などの特定のセキュリティリスクシナリオに従ってすでに定義されています。これらの事前設定された条件を変更したり、セキュリティ要件に応じて独自の条件を追加したりして、カスタムリスクインジケーター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インジケーターは、以下のシナリオで利用できます。

- 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インジケーター

ジオフェンスされたエリア外からのユーザーイベントを検出するには、以下の事前設定されたカスタムリスクインジケーターを使用します。

- CVAD-ジオフェンス外でセッションが開始されました
- GW-ジオフェンス交差

事前設定されたカスタムリスクインジケーターは、ユーザーが通常の運用国またはジオフェンス外から 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

CVAD-ジオフェンス外でセッションが開始されました リスクインジケーターは、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。そのため、リスクインジケーターの条件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。リスクインジ

> ケーターの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 **ジオフェンス設定** で国を選択します。詳細については、(/ja-jp/security-analytics/access-assurance-dashboard.html#enable-geofencing)を参照してください。

> 事前設定されたカスタムリスクインジケーターを表示するには、**セキュリティ > カスタムリスクインジケーター** 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インジケーターは無効になっています。**ステータス** ボタンを使用して有効にします。

(/en-us/citrix-analytics/media/preconfig-ci.png)

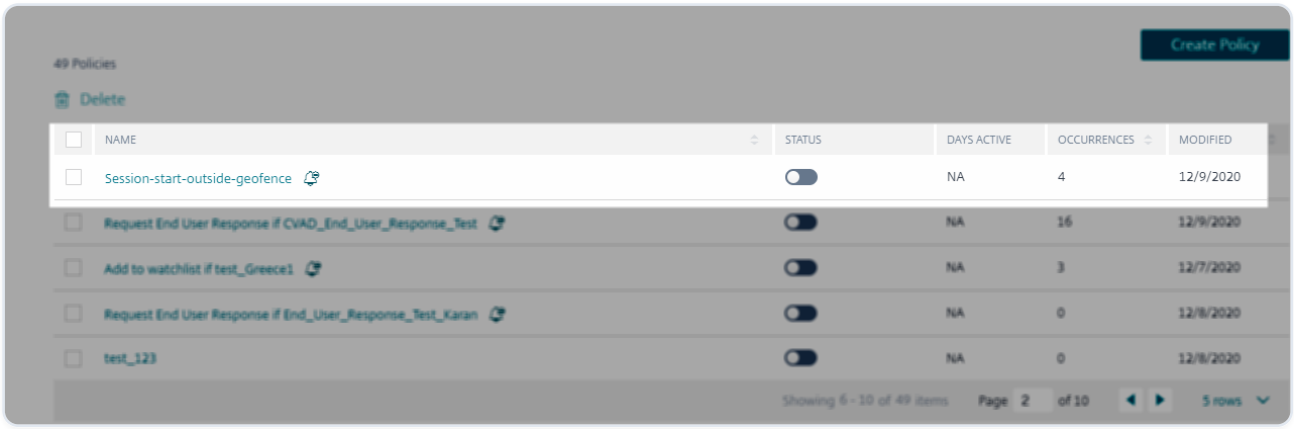
以下の表は、ジオフェンシング用のさまざまな事前設定済みカスタムリスクインジケーターについて説明しています。

カスタムリスクインジケーター名	シナリオ	カスタムインジケーターの条件	データソース	リスクカテゴリ
CVAD - ジオフェンス外で開始されたセッション	ユーザーが自国の運用範囲外で仮想セッションを開始しました	イベントタイプ = Session.logon 国 != "米国"	Citrix Workspaceアプリ	侵害されたユーザー
GW - ジオフェンス交差	ユーザーが自国の運用範囲外から認証に成功しました	イベントタイプ = "VPN_AI" AND 国 != "米国"	Citrix 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構成済みポリシー

Citrix は、ユーザーが自国の運用地域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事前構成済みポリシーを提供します。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、管理者にさらなるアクションを通知したりするなど、適切なアクションが実行されます。詳細については、「エンドユーザー応答の要求」を参照してください。

事前構成済みポリシーを表示するには、［**セキュリティ**］>［**ポリシー**］ の順に選択します。



次の表は、ジオフェンシングの事前構成済みポリシーについて説明しています。

ポリシー名	シナリオ	ポリシー条件	適用されるアクション
ジオフェンス外からのセッション開始	ユーザーが自国の運用地域外から仮想セッションを開始したときに、「エンドユーザー応答の要求」アクションを通じて管理者がユーザーの正当性を検証する機能	事前構成済みカスタムリスクインジケーター「CVAD-Session started outside of geofence」と併用	エンドユーザー応答の要求
			以下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**
			ユーザーがアクティビティを認識する場合: **アクションは不要**
			ユーザーがメール受信後60分以内に応答しない場合: **ユー**

ポリシー名	シナリオ	ポリシー条件	適用されるアクション
			ザーをウォッチリストに追加

> **注**
>
> 「**エンドユーザー応答の要求**」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、事前構成済みのポリシーはアカウントに適用されません。事前構成済みのポリシーを使用するには、ポリシーを変更し、別の任意のアクションを選択してください。

ジオフェンシング用の事前構成済みカスタムリスクインジケーターを使用して独自のポリシーを作成する

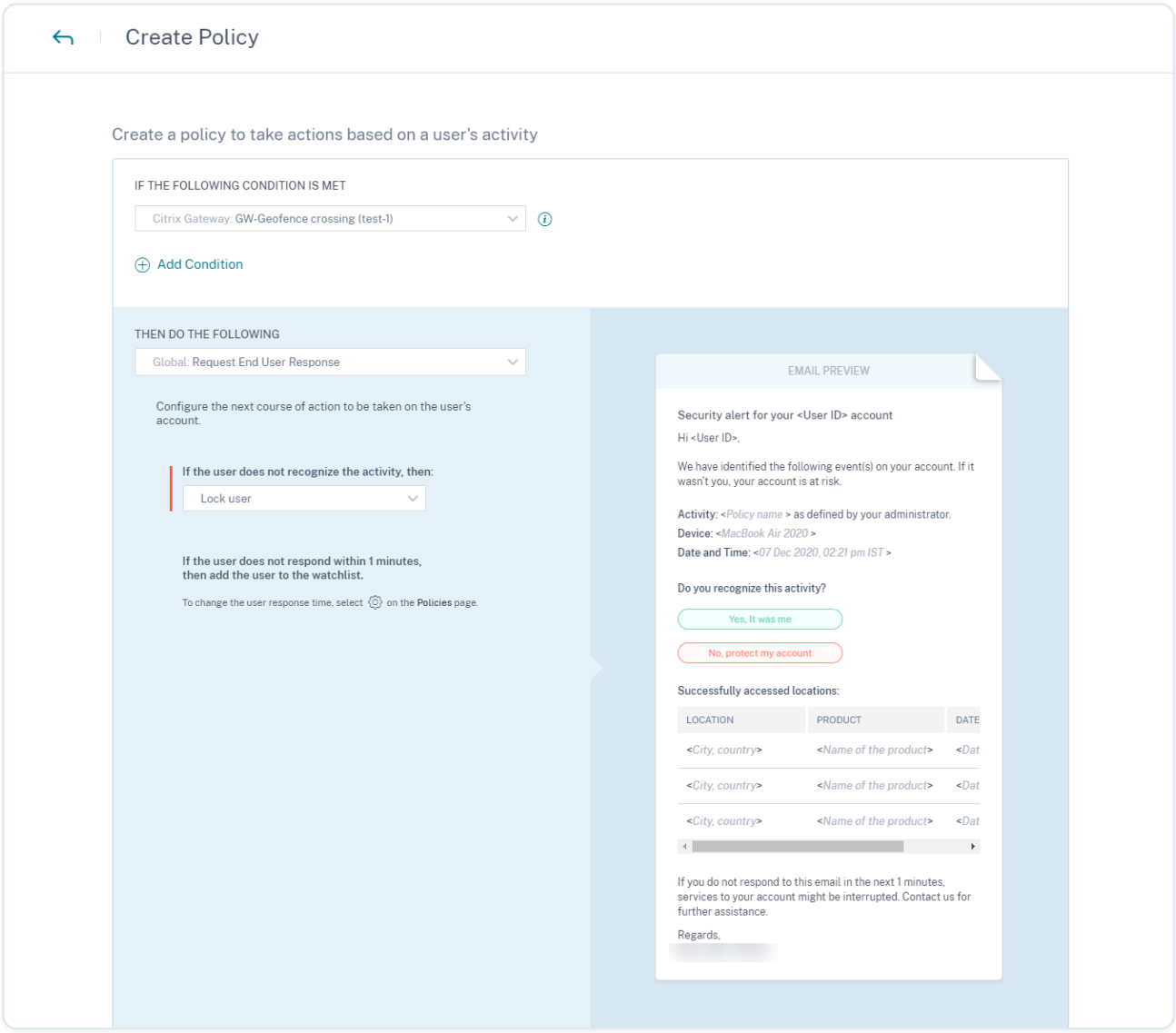
これらの事前構成済みカスタムリスクインジケーターを使用して独自のポリシーを作成し、インジケーターがトリガーされたときにユーザーをロックしたり、ユーザーをログオフしたりするなどのアクションを適用することもできます。ポリシーの作成方法については、「ポリシーとアクションの構成」を参照してください。

次の例は、米国以外から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-ジオフェンス横断

アクション: エンドユーザー応答の要求

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要求**」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は、「**エンドユーザー応答の要求**」アクションの代わりに、別の任意のアクションを選択してください。

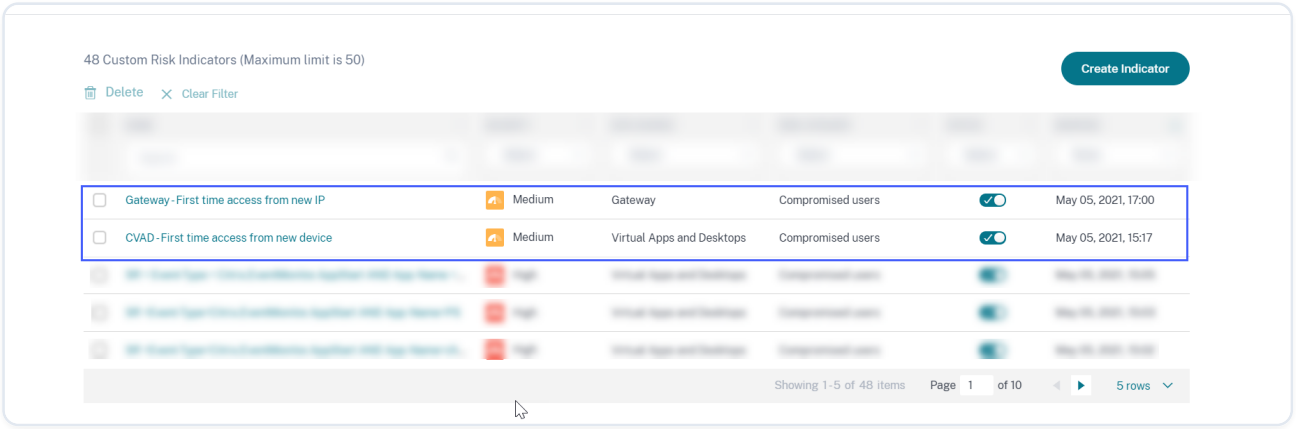
初回アクセスシナリオ用の事前構成済みカスタムリスクインジケーター

以下のカスタムリスクインジケーターを使用して、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

- Gateway - 新しいIPからの初回アクセス

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インジケーターは有効な状態です。無効にする場合は、**STATUS** ボタンを使用します。



次の表は、初回アクセス用の事前設定されたカスタムリスクインジケーターについて説明しています。

カスタムインジケーター名	シナリオ	事前設定された条件	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アプリのユーザーが以下のいずれかからサインインした場合：	以下の条件はデフォルトで有効になっています：	Citrix Virtual Apps and Desktopsオンプレミスおよび 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での初回。		
	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.`		

カスタムインジケーター名	シナリオ	事前設定された条件	データソース	リスクカテゴリ
		`Chrome", "XA.Receiver.Android", "XA.Receiver.Linux", "XA.Receiver.iOS")`		
Gateway - 新しいIPからの初回アクセス	Citrix Gateway ユーザーが以下のいずれかから正常にサインインした場合：	以下の条件はデフォルトで有効になっています：	シトリックス ゲートウェイ	侵害されたユーザー
	新しいパブリックIPアドレス	新しいクライアントIPでの初回。		
	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。	`Event-Type = "Authentication" AND Status-Code = "Successful login" AND Client-IP-Type != "private" AND Access-Insight-Flags = 1`		

条件バーでは、事前設定された条件に加えて、要件に応じて脅威を特定するための独自の条件を追加することもできます。

例えば、特定の国からのユーザーイベントを識別したい場合、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

エンドユーザーのメール設定は、グローバルアクション Request End User Response に関連付けられた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検出された異常なアクティビティについて、ユーザーから応答を得ることができます。ユーザーは、Citrix Analytics for Security から受信するメールを通じて応答します。

メール設定を使用して、次のことができます。

- ユーザーの注意を引き、応答を得るために、適切なバナー、ヘッダーテキスト、フッターテキストを追加します。これにより、メールの信頼性も高まります。
- ユーザーがメールに応答する必要がある時間（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：

1. 上部のバーで、**Settings > Alert Settings > End User Email Settings** をクリックします。



2. バナー画像をアップロードまたは参照するには、 をクリックします。画像ファイルをアップロードする際は、以下の要件を満たしていることを確認してください。
   - サポートされている形式：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. **HEADER** フィールドと **FOOTER** 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. ユーザー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。

メール設定(/en-us/citrix-analytics/media/email-settings.png)

ウォッチリスト

ウォッチリストを使用して、特定のユーザーの活動を潜在的な脅威がないか監視します。たとえば、組織内の正社員ではないユーザーや、特定の危険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

ユーザーをウォッチリストに手動で追加することも、トリガーされたときにユーザーをウォッチリストに追加するポリシーを定義することもできます。

ユーザーをウォッチリストに手動で追加するには、リスクタイムラインでユーザーのプロファイルに移動します。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適用します。

ウォッチリストに追加するアクション(/en-us/citrix-analytics/media/add-watchlist-manually.png)

ポリシーを使用してユーザーをウォッチリストに追加するには、満たす必要のある一連の条件を持つ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分で70を超えた場合に、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。

ポリシーの作成の詳細については、ポリシーとアクションの設定を参照してください。

ウォッチリストに追加するポリシー(/en-us/citrix-analytics/media/add-watchlist-action-rule.png)

ウォッチリストからユーザーを削除する方法

ユーザーをウォッチリストから手動で削除することも、トリガーされたときにユーザーをウォッチリストから削除するポリシーを定義することもできます。

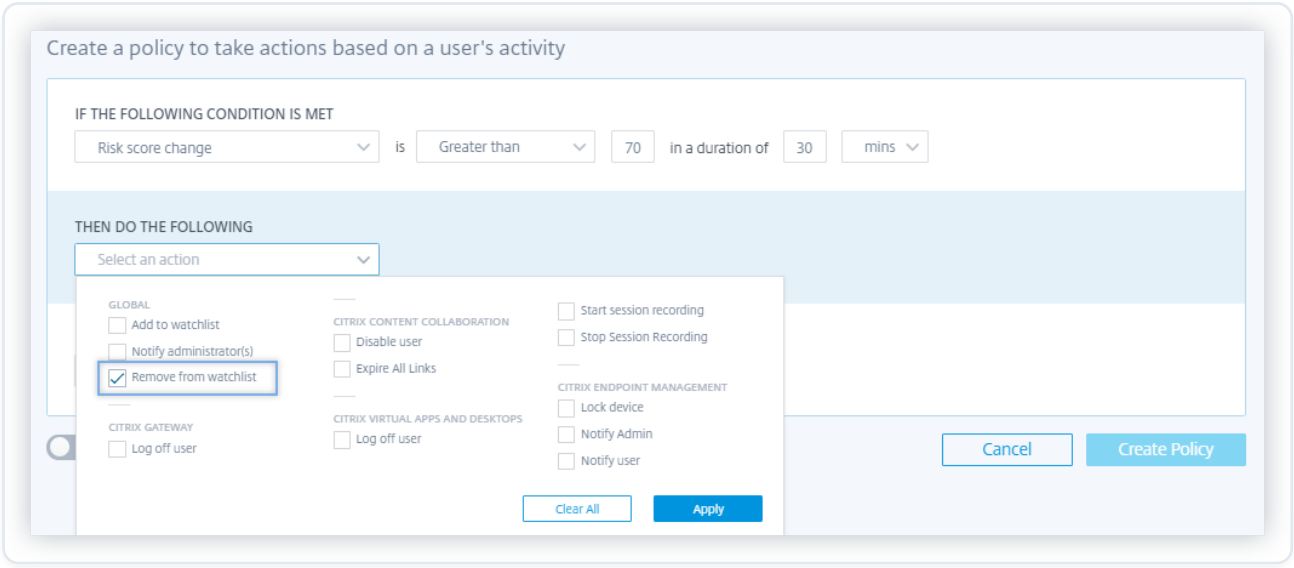
ユーザーをウォッチリストから手動で削除するには、リスクタイムラインでユーザーのプロファイルに移動します。次に、**アクション**メニューから**ウォッチリストから削除**を選択します。**適用**をクリックし、プロンプトに従ってアクションを適用します。

> **注**

> ユーザーがウォッチリストに登録されており、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。

> ウォッチリストから削除するアクション(/en-us/citrix-analytics/media/remove-watchlist-manually.png)

ポリシーを使用してウォッチリストからユーザーを削除するには、満たす必要のある一連の条件を持つ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未満の場合、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。



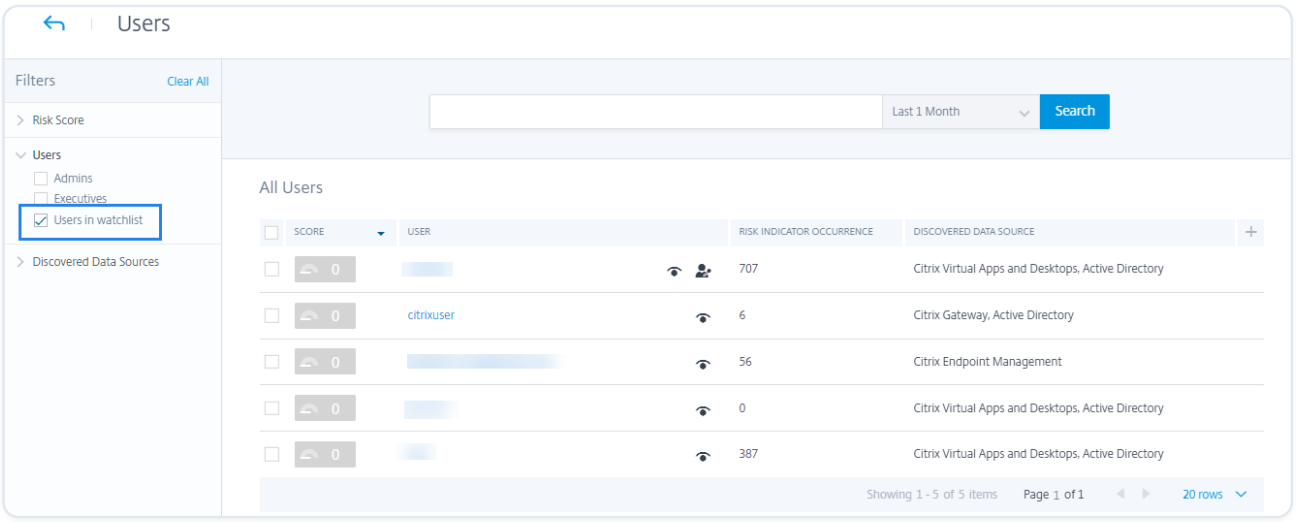
ウォッチリスト内のユーザーを監視する方法

Security > Users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。ボックスをクリックすると、**Users in Watchlist**ペインで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リストされたウォッチリスト内の上位5人のユーザー。**Users in Watchlist**ペインで、リスクスコア、リスクインジケーターの発生回数、およびユーザーの名前を表示します。**See More**をクリックすると、**Users**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が表示されます。
- ウォッチリストに登録されているリスクの高い上位ユーザー。**Risky Users**ペインでは、ユーザーの横にある「目」のアイコンは、そのユーザーがウォッチリストに登録されていることを示します。

Users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インジケーターの数、および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。特定の期間のリスクインジケーターの発生回数を表示するには、期間を選択します。



週次メール通知

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露出を要約した週次メール通知を送信します。週次通知により、前週の危険なイベントとその発生について常に把握し、情報を受け取ることができます。Citrix Analyticsにサインインしなくても、注意や対応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こっているかを常に把握できます。

メール通知を有効にする

- フルアクセスまたはカスタムアクセス権限を持つCitrix Cloud管理者である場合、Citrix Cloudアカウントでは、メール通知は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てください。詳細については、「メール通知の受信」を参照してください。Active Directory/Azure ADグループを介して追加された管理者には、通知設定は利用できません。
- デフォルトでは、メール通知はCitrix Security Administrators - デフォルトリストに送信されます。週次アラートのカスタム配布リスト受信者を構成することで、これを変更できます。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からメール通知が送信されます mailto:donotreplynotifications@citrix.com。

メール通知には、次の情報が記載されています。

- 処理されたイベントの総数、検出されたリスクインジケーター、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つのリスクインジケーター
- リスクインジケーターに対して実行された上位3つのアクション
- アクティブユーザーの総数と危険なユーザーの総数
- 注意が必要なイベントまたはアクション

citrix | Analytics for Security

Your week at a glance

Nov 07 to Nov 14, 2023

Customer name: oasstdaily@gmail.com
Organization ID: 51521533

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

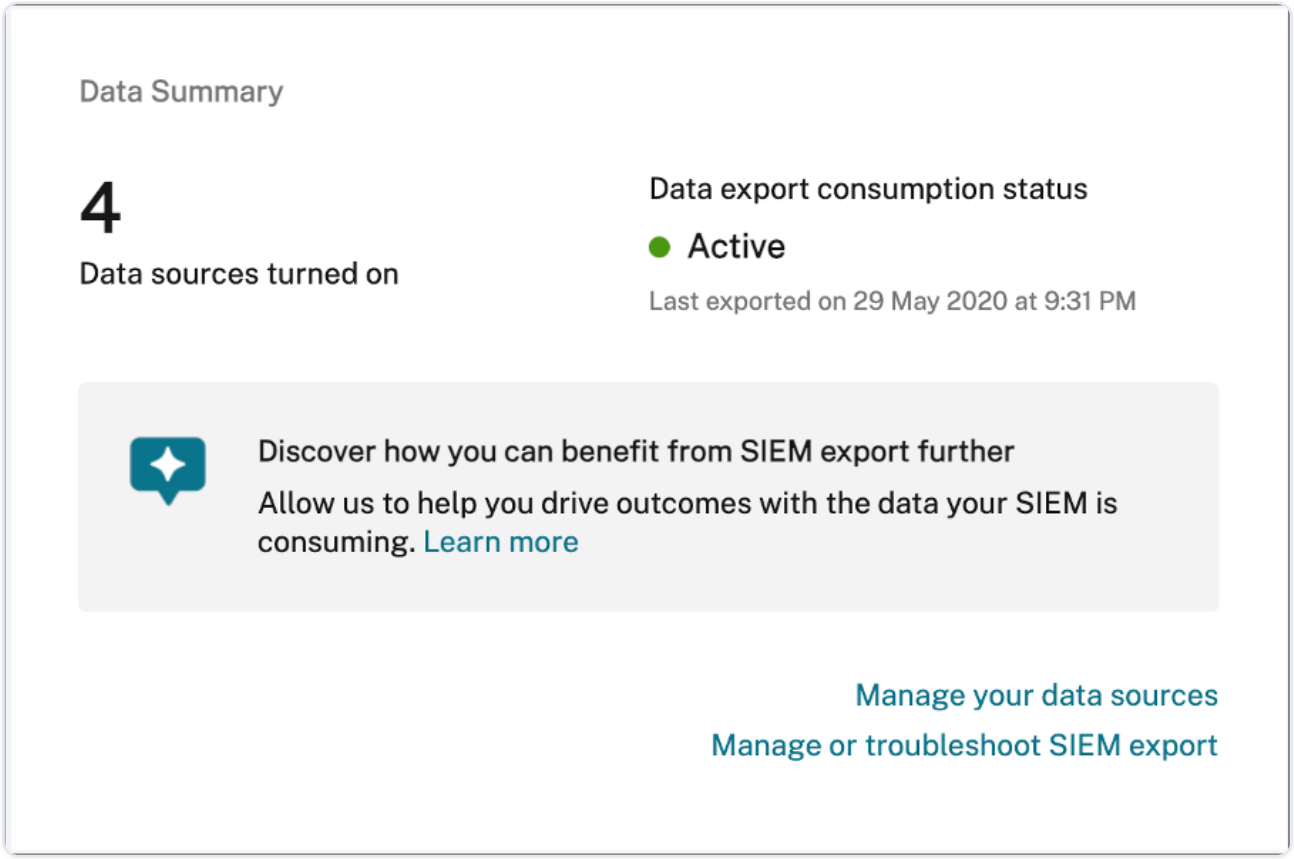
アカウントの概要

週次メールには、処理されたイベントの総数、検出されたリスクインジケーター、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。



データの概要

週次メールでは、有効になっているデータソースとデータエクスポートの使用状況に関する情報も提供されます。



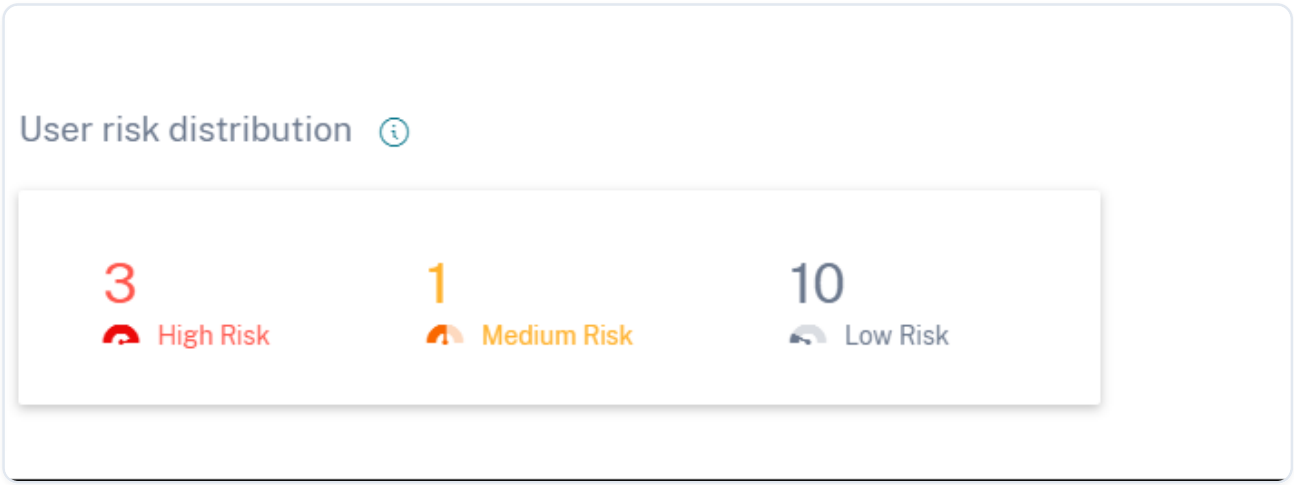
メールの**データソースの管理**をクリックすると、Citrix Analyticsの**データソース**ページが表示されます。データソースをオンボードし、データ処理を有効にすることで、Citrix Analyticsがデータの処理を許可するように設定できます。分析の有効化の詳細については、データソースの分析の有効化を参照してください。

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

週次メールでは、ユーザーの総数と危険な行動をとったユーザーに関する情報が提供されます。

- **高リスクユーザーの数** – 赤色で識別されます。組織にとって差し迫った脅威となります。
- **中リスクの数** – オレンジ色で識別されます。選択した週にアカウントで複数の重大な違反があり、厳密に監視する必要があります。
- **低リスクユーザーの数** – 黄色で識別されます。アカウントにいくつかの重大な違反がありますが、潜在的に脅威とは見なされません。

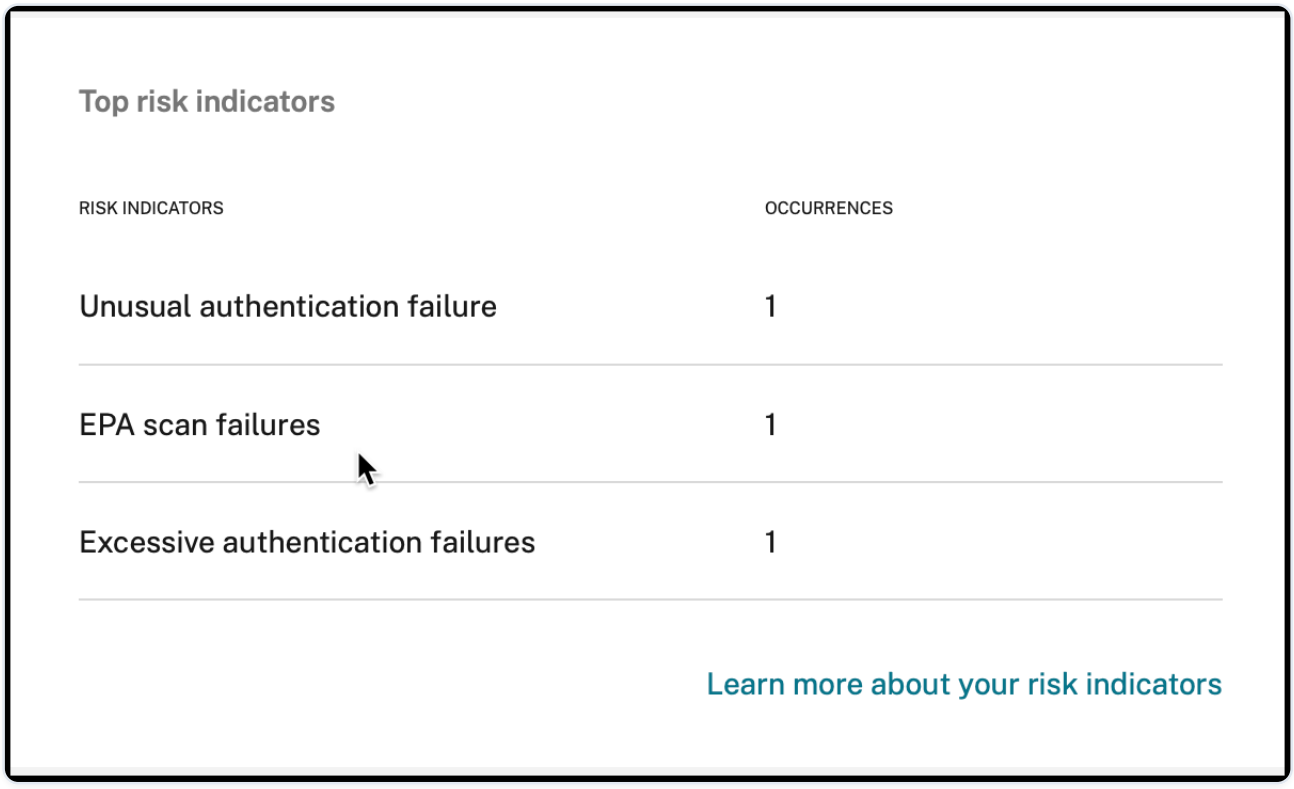


詳細については、危険なユーザーを参照してください。

「**ユーザーの詳細を確認**」をクリックして、Citrix Analyticsの「**リスクのあるユーザー**」ページを表示します。アクティブなユーザーとリスクの分類について、より深い洞察を得ることができます。

上位のリスクインジケーター

週次メールでは、選択した週の上位3つのリスクインジケーターと発生回数に関する洞察が提供されます。発生回数に応じて、選択した週のデフォルトおよびカスタムのリスクインジケーターの両方が表示されます。

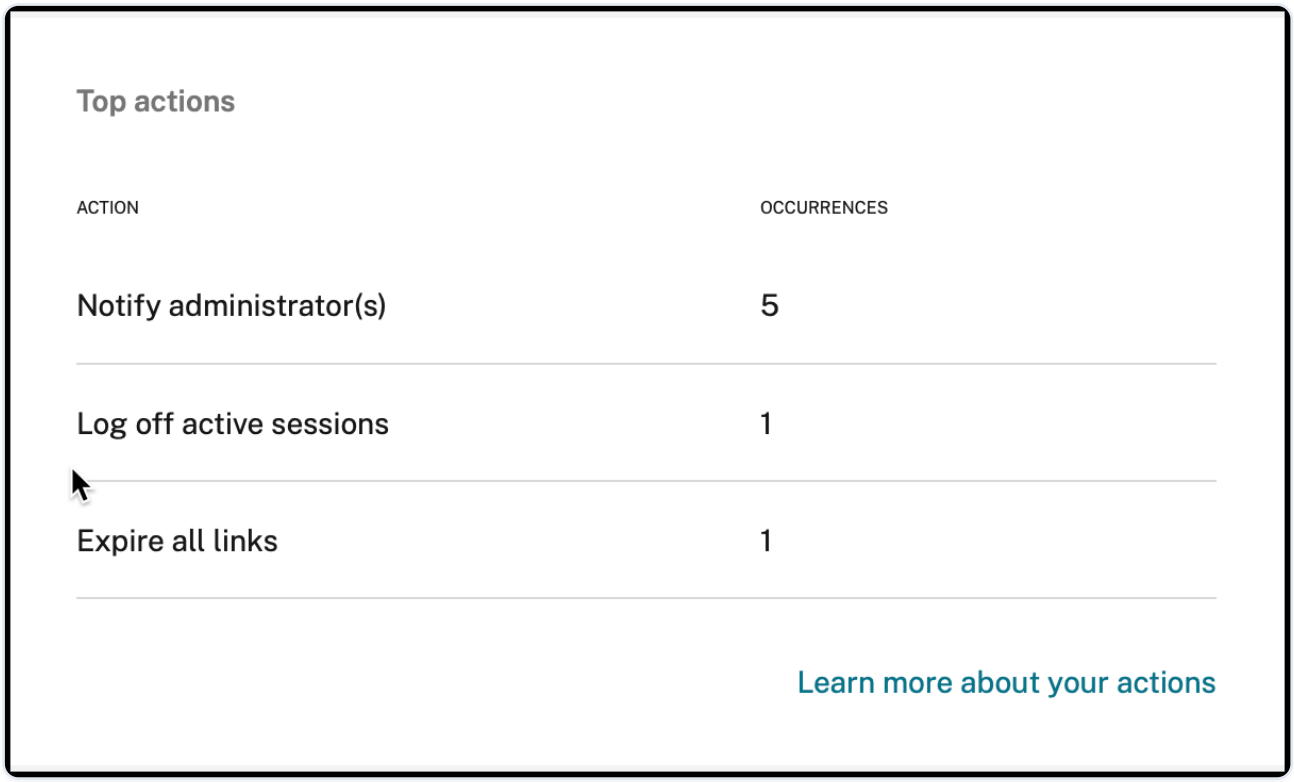


詳細については、リスクインジケーターを参照してください。

メール内の「**リスクインジケーターの詳細を確認**」をクリックして、Citrix Analyticsの「**リスクインジケーターの概要**」ページを表示します。

上位のアクション

週次メールでは、先週発生した不審な脅威や異常な脅威に対応して実行された上位3つのアクションに関する洞察が提供されます。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Citrix Gatewayアクションの両方が表示されます。



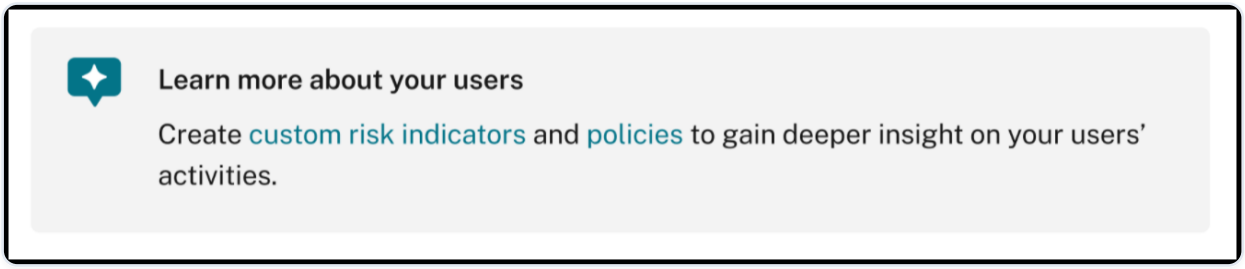
アクションとアクションの設定の詳細については、ポリシーとアクションを参照してください。

メール内の「**アクションの詳細を確認**」をクリックして、Citrix Analyticsの「**上位のアクション**」ページを表示します。

メールを受信した後、どのようなアクションを実行する必要がありますか?

週次メールを使用すると、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。

- その週にリスクインジケーターが検出されなかった場合、カスタムリスクインジケーターをさらに作成するように促す次のメッセージが表示されます。



Citrix Analyticsにログインして、カスタムリスクインジケーターをさらに作成できます。

- Security Analyticsでデータソースが1つも有効になっていない場合、データソースのデータ処理を有効にするよう促す次のメッセージが表示されます。

データソースが有効になっていません(/en-us/citrix-analytics/media/turnon-data-sources-security-analytics.png)

- ポリシーが監視モードになっていない場合、ポリシーを適用モードに移行するよう促す次のメッセージが表示されます。

  監視モードのポリシー(/en-us/citrix-analytics/media/policies-monitoring-mode.png)

- 今週のトップ3リスクインジケーターのいずれにもポリシーが設定されていない場合、ポリシーを作成するよう促す次のメッセージが表示されます。

  ポリシーが設定されていません(/en-us/citrix-analytics/media/top-risk-indicator-no-policy.png)

- 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、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**オプションの詳細について、次の推奨事項が示されます。

  データエクスポートを有効にする(/en-us/citrix-analytics/media/enable-siem-dataexport.png)

- 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促す次のメッセージが表示されます。

  データエクスポートの消費ステータス(/en-us/citrix-analytics/media/dataexport-consumption-status.png)

> **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有効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、データソースを有効にするよう促す次の警告メッセージが表示されます。

データ送信が有効になっています(/en-us/citrix-analytics/media/action-req.png)

監査ログ

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述されます。これらは、エラーなどのシステムイベント、または Citrix Analytics 管理者によって実行された構成アクションの監査証跡である場合があります。

構成が追加、削除、または更新されるたびに、イベント情報が監査ログに書き込まれます。この情報には、何が変更されたか、いつ変更されたか、誰が変更したかが含まれます。

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 には次のイベントが登録されます。

- 生成されたエラー
- 送信が有効になりました
- 送信が無効になりました
- データソースが追加されました
- データソースが削除されました
- ポリシーが作成されました
- ポリシーが更新されました
- ポリシーが削除されました

監査ログイベント(/en-us/citrix-analytics/media/audit-logs-events.png)

監査ログの表示方法

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。

監査ログに移動(/en-us/citrix-analytics/media/navigate-to-audit-log.png)

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、把握できます。最新の監査データを取得するには、**監査ログ**ページを更新します。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。

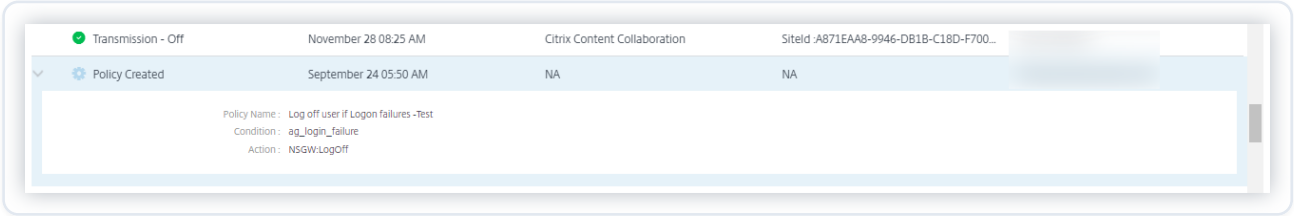
監査ログページで、以下の監査情報を表示できます。これらのフィールドに基づいて監査データをフィルタリングすることもできます。

- **イベント**。イベントは、システムによって生成されるか、管理者が Citrix Analytics に適用した構成である場合があります。イベントは、アクションまたはデータソースの適用失敗などのエラーを表すこともあります。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。表示したい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日時。ログを表示したい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ヶ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。1つ以上の製品に基づいてログを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ている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。

監査ログページ(/en-us/citrix-analytics/media/audit-log-page.png)

登録されたイベントがポリシーに基づいていた場合、矢印アイコンをクリックして、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

Citrix Analytics for Securityで利用可能な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し、スケジュールすることができます。カスタムレポートは、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するのに役立ちます。これにより、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できます。

カスタムレポートは、以下のデータソースをサポートしています。

- 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
- セキュアブラウザ
- ポリシー
- リスクインジケーター
- 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るフィールドを表示するには、以下のデータソースをクリックしてください。

- 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
- セキュアブラウザ
- ポリシー

以下のデータソースはカスタムレポートでのみ利用可能です。以下の表に、これらのデータソースにおけるカスタムレポートでサポートされているフィールドを示します。

- リスクインジケーター
- 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ー	カテゴリ	リスクインジケーターのカテゴリを示します。リスクインジケーターは、侵害されたエンドポイント、侵害されたユーザー、データ持ち出し、内部脅威の4つのカテゴリのいずれかに分類されます。
	リスクインジケーター名	リスクインジケーターの名前です。カスタムリスクインジケーターの場合、名前はインジケーターの作成時に管理者が定義します。
	重大度	リスクの重大度を示します。低、中、高のいずれかです。
	ユーザー名	ログインに使用され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。
	ユーザー名	ログインに使用され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、危険なユーザーは、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。

- **レポートの作成**をクリックして、カスタムレポートを作成します。
- 行を展開して、既存のカスタムレポートのプレビューを表示します。
- レポート名をクリックして、詳細なレポートの視覚化を表示します。
- 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。
- 作成したレポートを編集するには、編集アイコンをクリックします。
- 作成した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。

カスタムレポートページ(/en-us/citrix-analytics/media/custom-report-page.png)

カスタムレポートを作成する

カスタムレポートを作成するには、**レポートの作成**をクリックします。**レポートの作成**ページで、テンプレートを使用するかどうかを選択してカスタムレポートを作成できます。

テンプレートを使用したレポートの作成(/en-us/citrix-analytics/media/create-report-template.png)

テンプレートを使用し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. **テンプレートの選択**: 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表示されます。選択したテンプレートをレポートで使用できるようにするには、**レポートにテンプレートを適用**をクリックします。
2. **フィルターの絞り込み**: **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用に事前定義されたフィルターが表示されます。必要な変更を行い、**次へ**をクリックします。

絞り込まれたフィルター(/en-us/citrix-analytics/media/refined-filters.png)

1. **視覚化の適用**: レポートを表示するために利用可能な視覚化のいずれかを選択します。

視覚化の適用(/en-us/citrix-analytics/media/apply-visualization.png)

- **棒グラフ**: 値に比例する高さの垂直な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**: 互いに積み重ねられた棒の形式でデータを表示します。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。データの相対的なサイズや割合を視覚化するために使用されます。
- **ドーナツグラフ**：データをドーナツの形式で表示します。データの相対的なサイズや割合を視覚化するために使用されます。 - **表**: データを表の形式で表示します。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**：直線の線分で結ばれた点でデータを表示します。一定期間のデータトレンドを視覚化するために使用されます。

1. 次に、以下のパラメータで視覚化を設定します。

    - X軸のディメンション
    - Y軸にプロットするメトリクス
    - メトリクスに適用する、平均やカウントなどの要約または集計
    - 並べ替えと順序付けのオプション
    - レポートに表示されるレコードの最大数に対するオプションの制限。

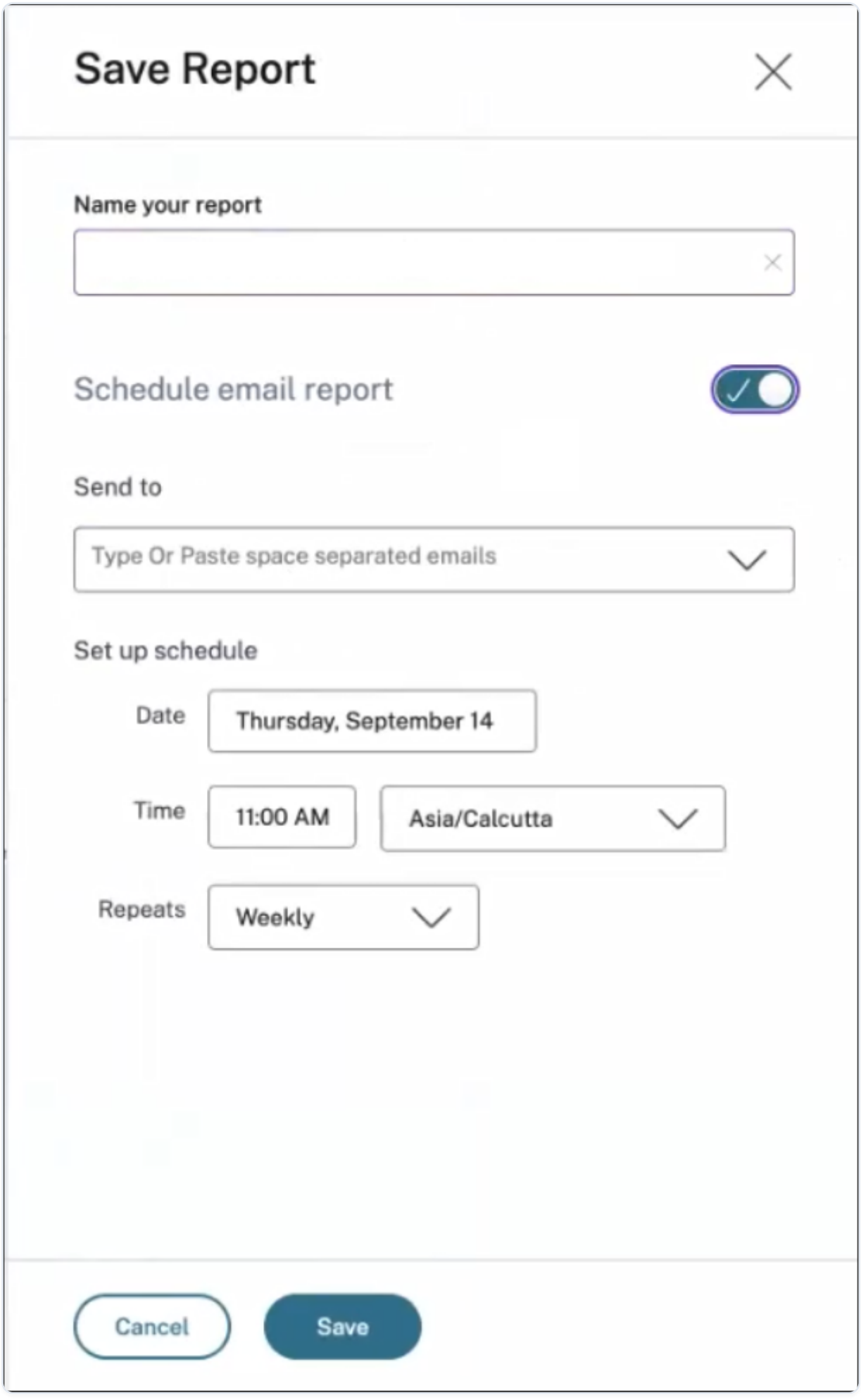
テンプレートなしでカスタムレポートを作成する

事前定義された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。フィルタの定義、視覚化の適用、レポートの保存、およびスケジュール設定の手順に従います。

テンプレートなしのカスタムレポート(/en-us/citrix-analytics/media/custom-report-without-template.png)

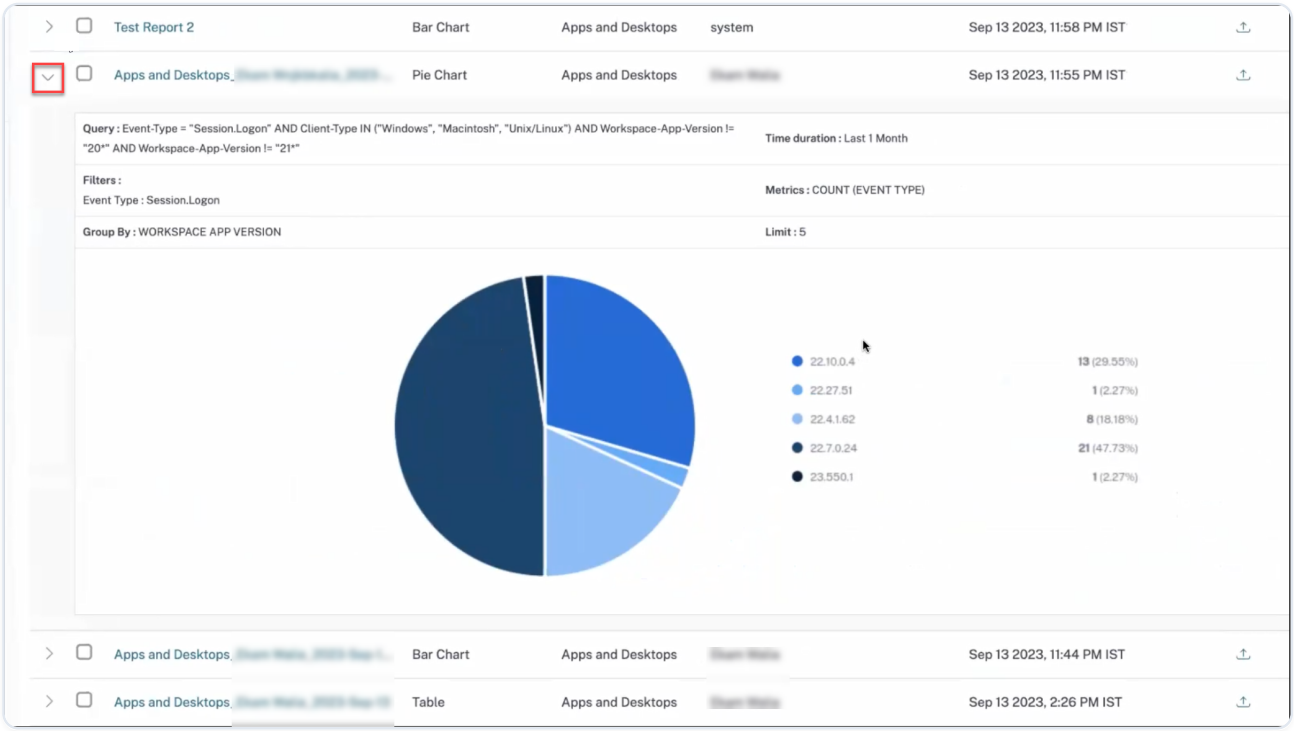
レポートを保存する

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. 指定されたメールIDと配布リストに、特定の日時または定期的なスケジュールでレポートをメール送信するようにスケジュールできます。


Save Report
Name your report
Schedule email report
Send to
Type Or Paste space separated emails
Set up schedule
Date
Thursday, September 14
Time
11:00 AM
Asia/Calcutta
Repeats
Weekly
Cancel
Save

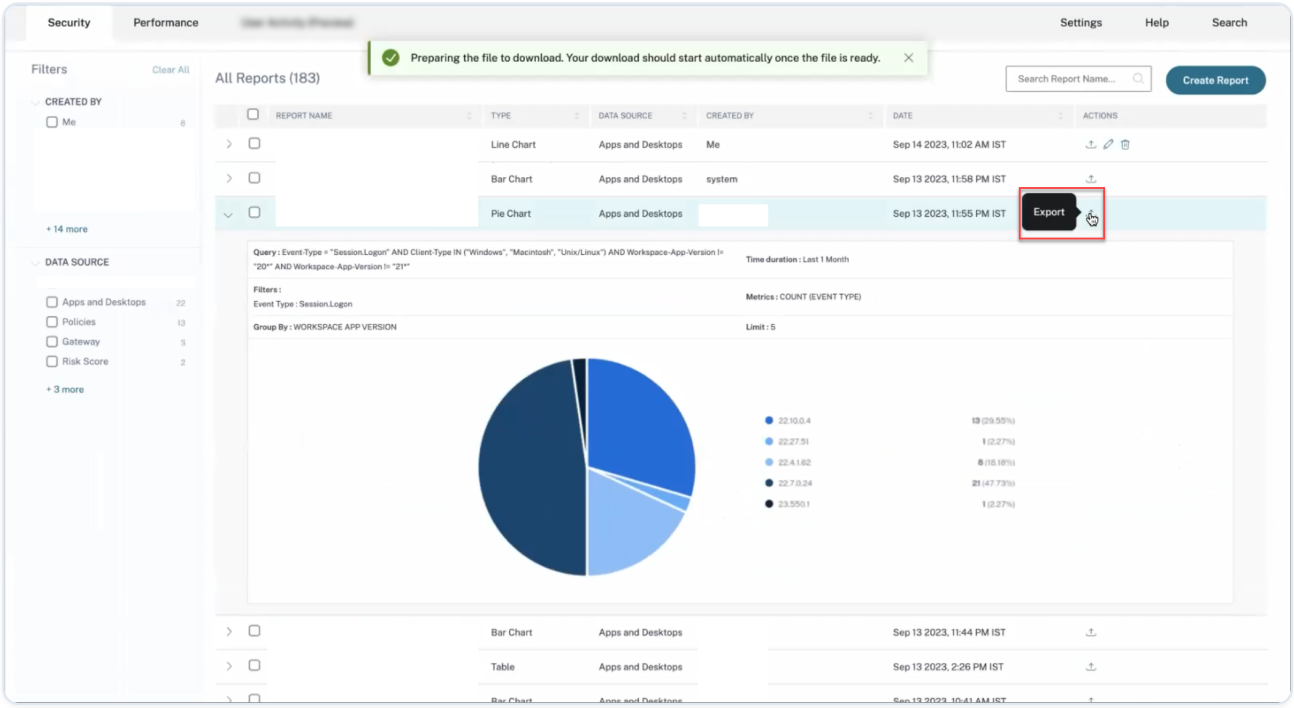
レポートを表示

1. レポートを作成して保存した後、**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修正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。



レポートをエクスポート

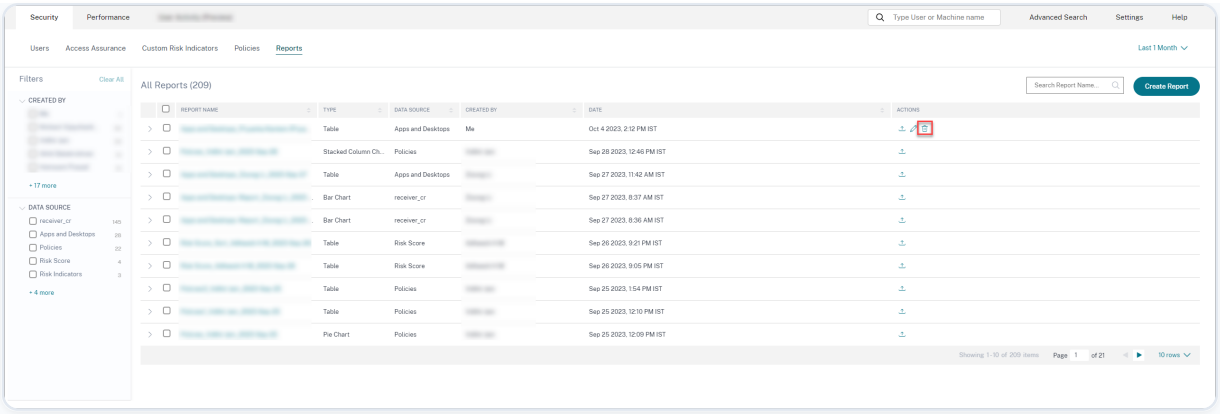
エクスポートアイコンをクリックして、レポートをエクスポートします。



レポートを削除

削除アイコンをクリックして、レポートを削除します。

> 注:
>
> レポートを作成したユーザーのみが削除できます。



レポートを編集

編集アイコンをクリックして、レポートを編集します。

> 注:
>
> レポートを作成したユーザーのみが編集できます。

> レポートの編集(/en-us/citrix-analytics/media/custom-report-edit-report.png)

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、メールによる自動エクスポートを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、選択した対象者向けに一目で示すレポートの集まりです。

以下の期間のデータについて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

エグゼクティブレポート(/en-us/citrix-analytics/media/executive-report.png)

どのようなレポートが含まれていますか?

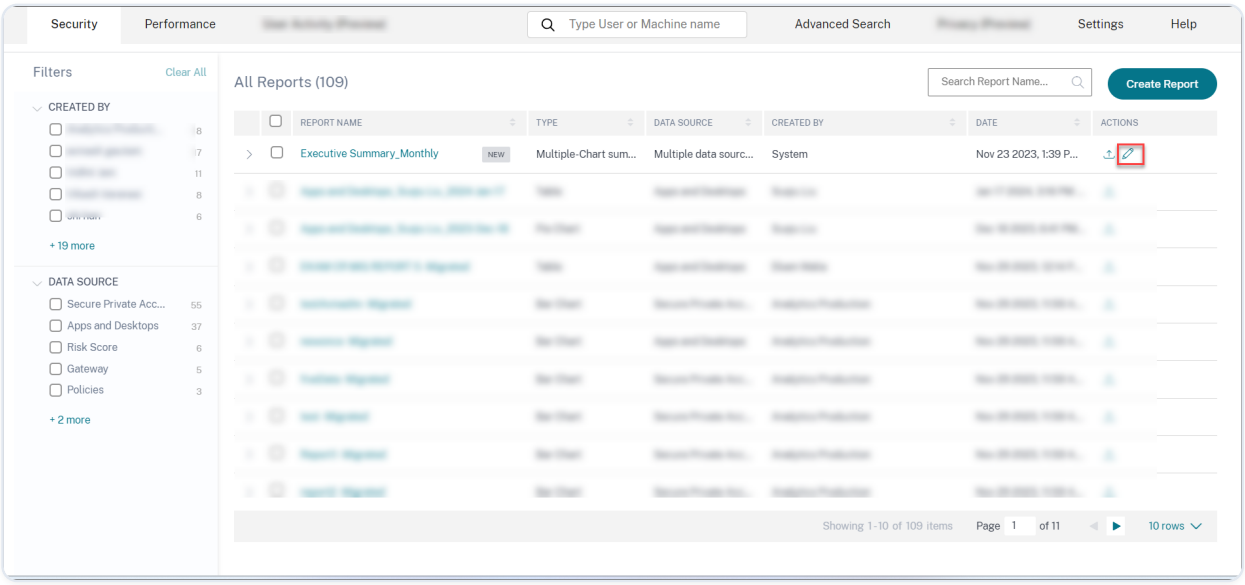
エグゼクティブサマリーレポートには、以下のレポートが含まれています。

- **ユーザーリスク分布**: 選択した期間における、最も高い計算済みリスクスコアに基づいた、高、中、低リスクプロファイルの分布。
- 最もリスクの高いユーザー：選択した期間において、最も高いリスクスコアでソートされた全ユーザーの中で、最もリスクの高いユーザー。
- **カテゴリ別のリスク発生状況**：即座の対応が必要なリスクカテゴリによって提供される、リスクエクスポージャーの種類と重大なリスクの包括的なビュー。リスク指標は以下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
  - データ持ち出し
  - 内部脅威
- **リスク指標**：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。
- **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。
- **上位ポリシー**：選択した期間に最も多くトリガーされた上位5つのポリシー。
- **上位アクション**：選択した期間に最も多くトリガーされた上位5つのアクション。
- **重大度別のリスク指標**：ユーザーによってトリガーされた、重大度に基づいてソートされた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**：ユーザーによってトリガーされた、発生回数に基づいてソートされたデフォルトおよびカスタムのリスク指標。

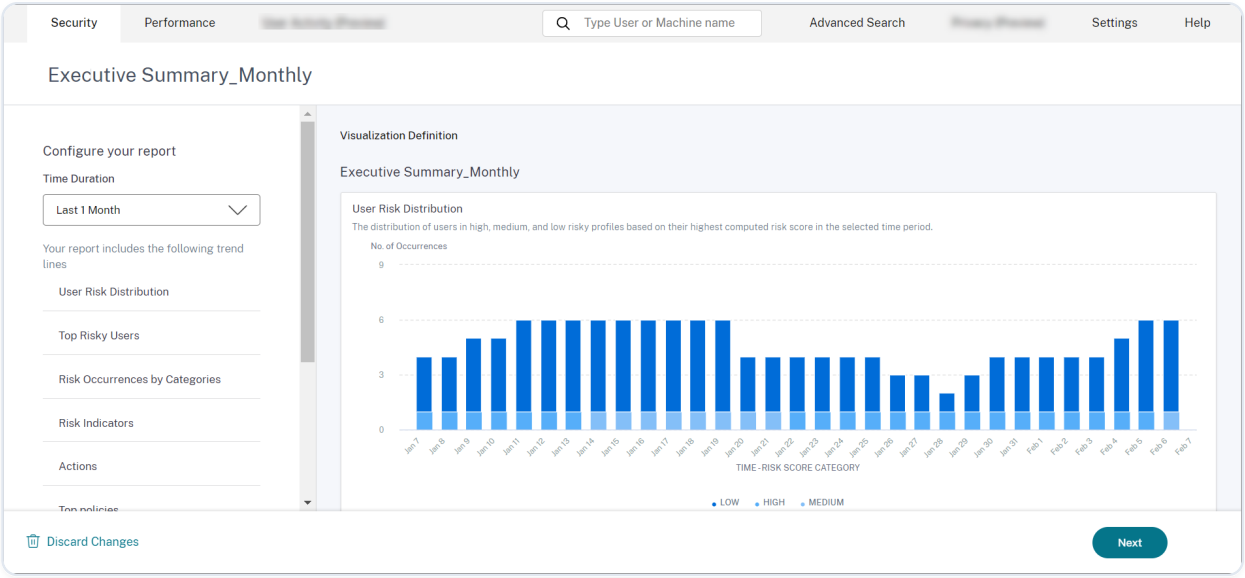
エグゼクティブレポートを編集する

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**記号をクリックします。



2. 「**レポートの設定**」ペインで、データを表示したい期間を選択します。



3. 「**次へ**」をクリックします。「**レポートの保存**」ペインが表示されます。

> 「**注:**」:
>
> 変更を破棄するには、「**変更を破棄**」をクリックします。

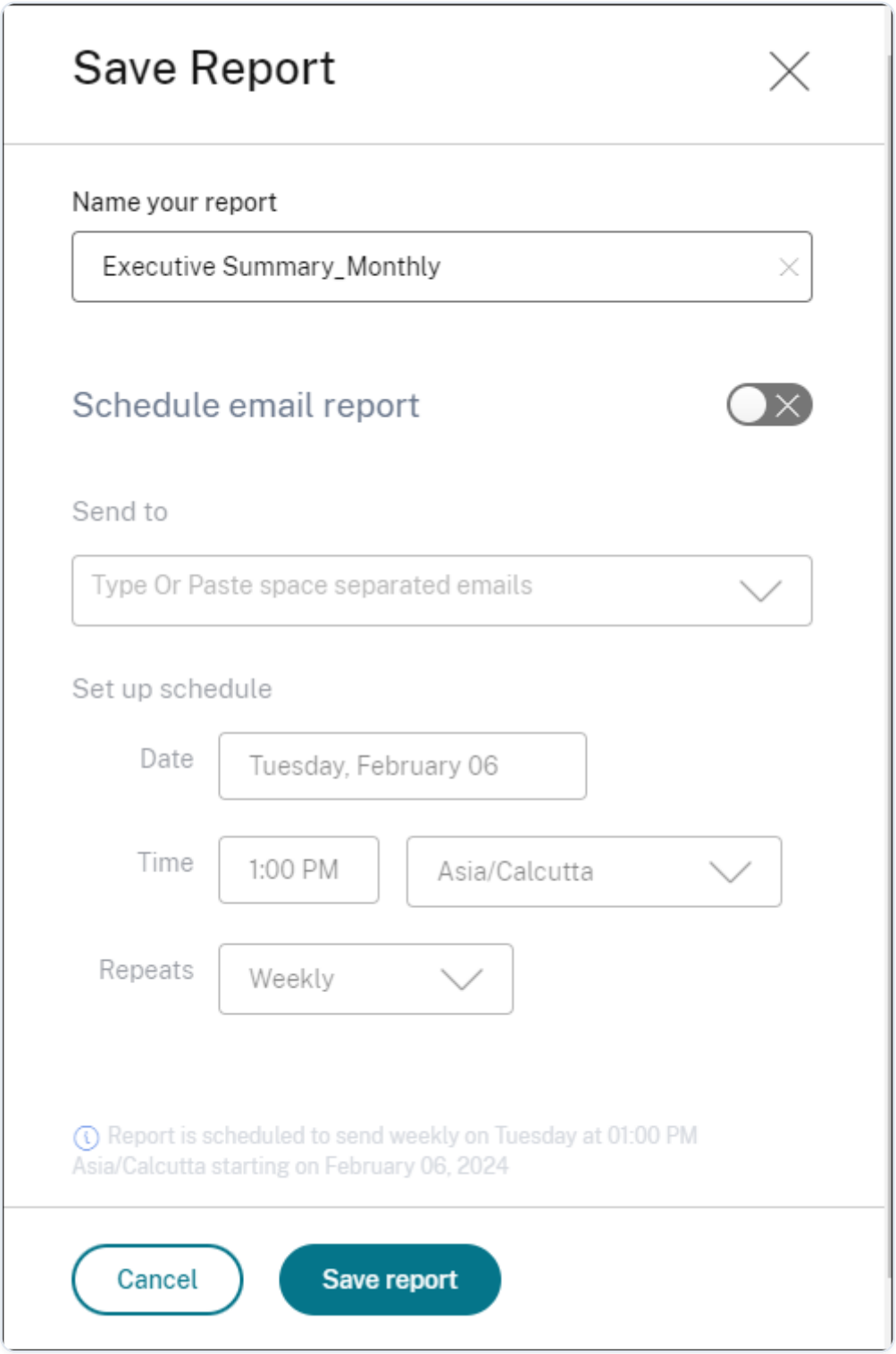
4. 「**レポートの保存**」ペインで、次の詳細を入力します。

   a. 「**レポート名**」: エグゼクティブレポートの名前。

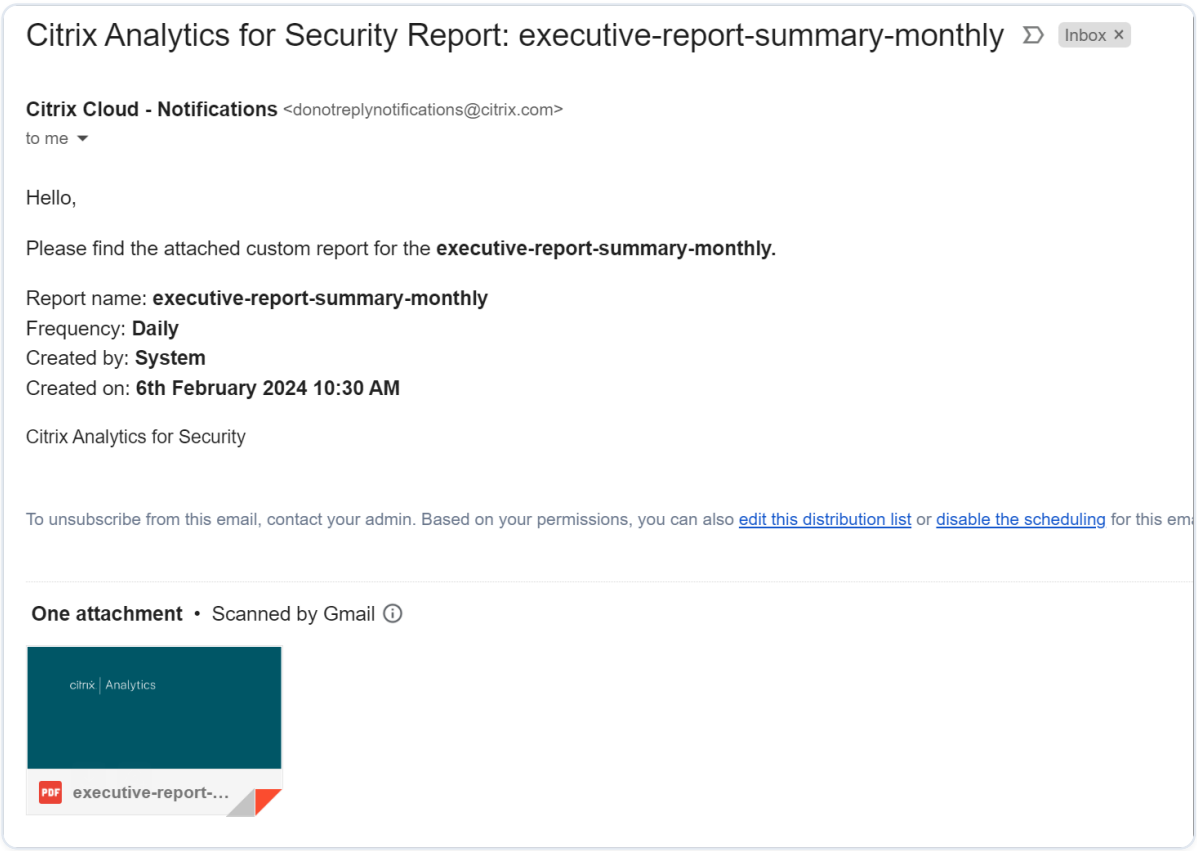
   b. 「**メールレポートのスケジュール設定**」: レポートをスケジュールするには、オンに切り替えます。このトグルはデフォルトでオフになっています。

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メールアドレスの組み合わせを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。

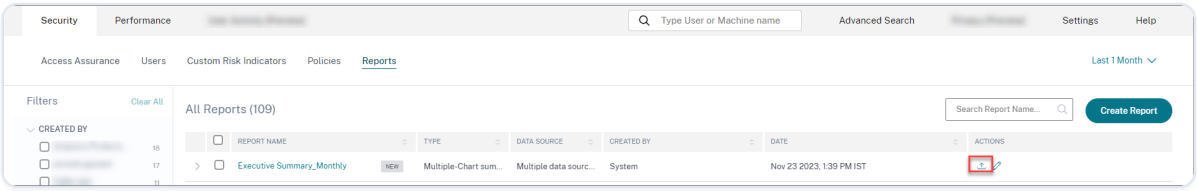
d. 「**スケジュール設定**」：レポートが選択した対象者に最初に送信される希望時刻と、繰り返される時刻を選択します。



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メールで送信されます。



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。

citrix | Analytics

Custom Report

executive-report-summary-monthly

From September 19, 2023 to October 19, 2023

Created by: **System**

Created on: **Oct 19, 2023 at 11:15 PM Asia/Singapore**

The custom report is generated for executive-report-summary-monthly for the period **19th Sep 2023 11:15 PM - 19th Oct 2023 11:15 PM**

User Risk Distribution

The distribution of users in high, medium, and low risky profiles based on their highest computed risk score in the selected time period.



セルフサービス検索

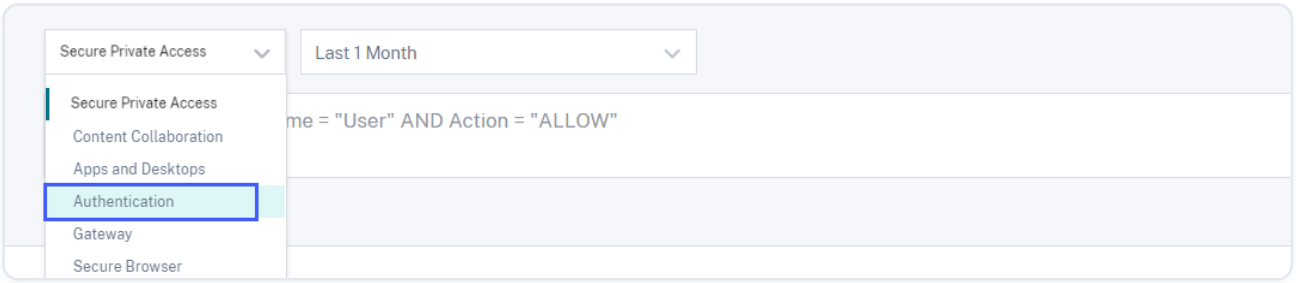
認証のセルフサービス検索

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洞察を得ます。Citrix Analytics for Security™は、Citrix CloudのIdentity and Access Management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、ユーザーログオフ、クライアント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する

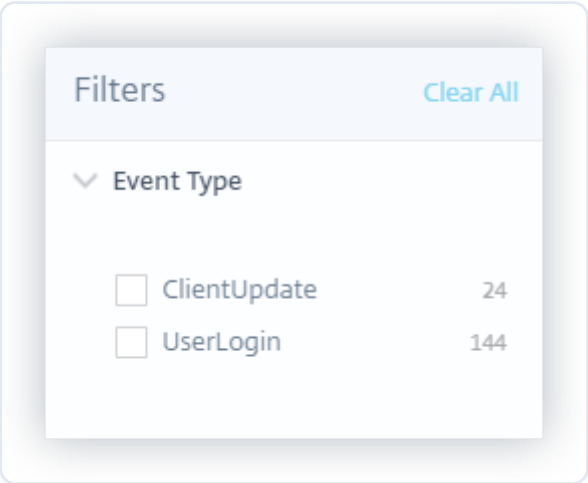
認証イベントを表示するには、リストから**認証**を選択します。デフォルトでは、セルフサービスページには過去1日間のイベントが表示されます。イベントを表示したい期間を選択することもできます。



イベントをフィルタリングするファセットを選択する

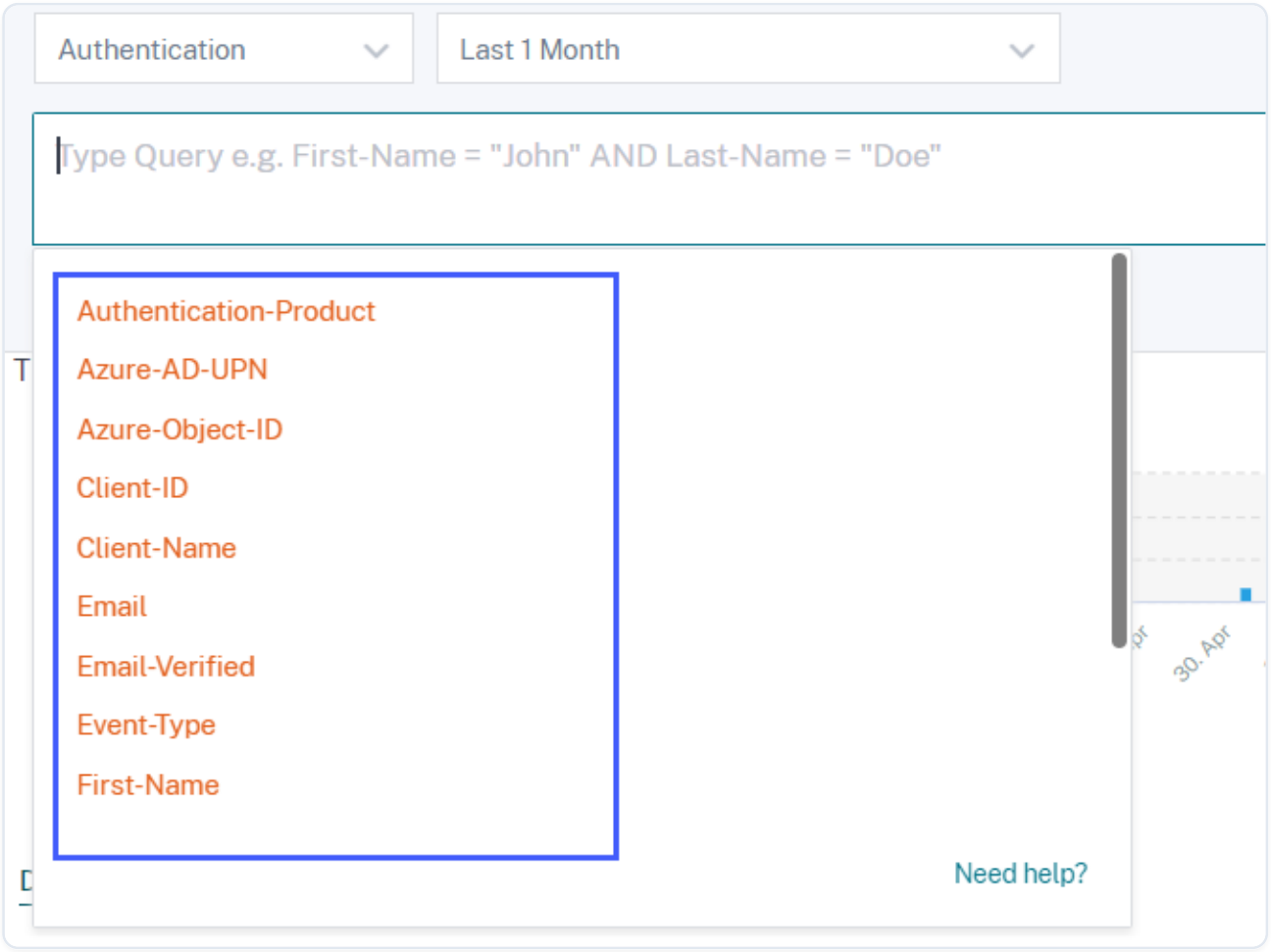
認証イベントには次のフィルターを使用します。

- **イベントタイプ** - 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ユーザーイベントタイプに基づいてイベントを検索します。



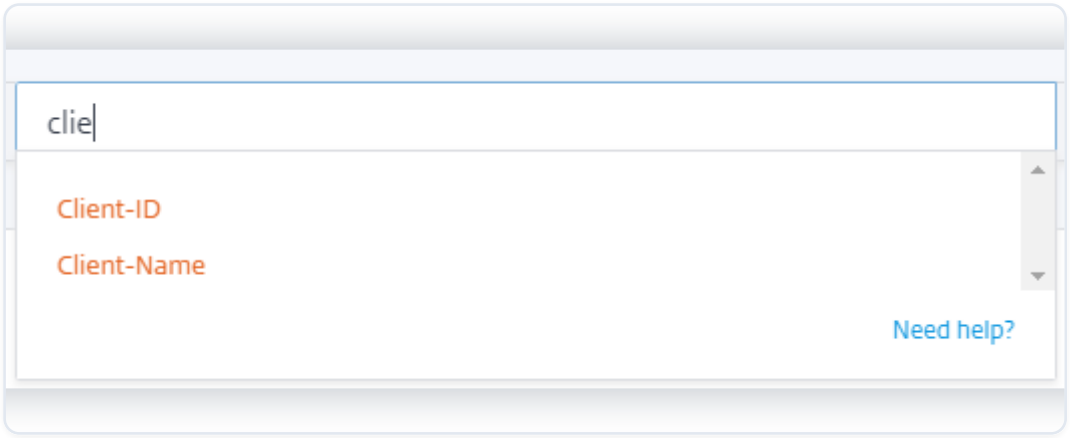
イベントをフィルタリングする検索クエリを指定する

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。

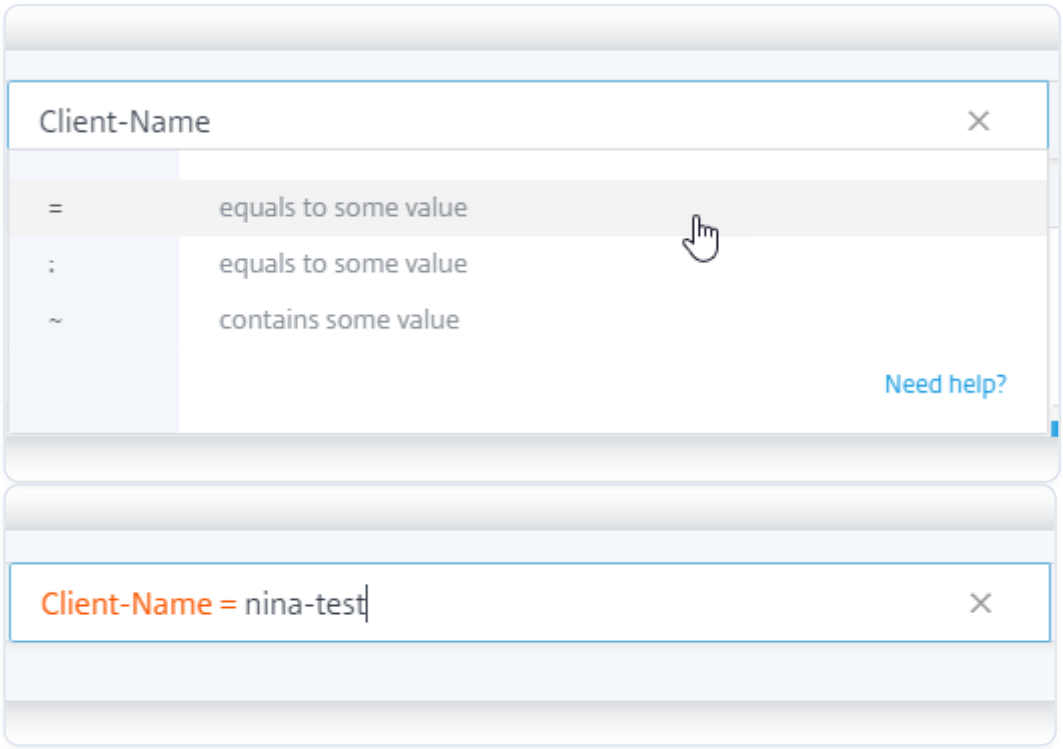


例えば、メールステータスが検証済みのクライアント「nina-test」の認証イベントを表示したいとします。

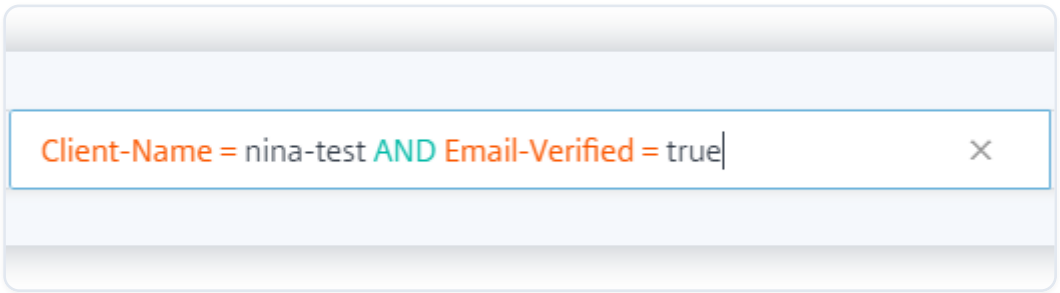
1. 検索ボックスに「client」と入力して、関連するディメンションを取得します。



2. **Client-Name**を選択し、等号演算子を使用して「nina-test」という値を指定します。



3. **AND**演算子を選択し、**Email-Verified**ディメンションを選択します。等号演算子を使用して、**Email-Verified**に「true」という値を割り当てます。「true」という値は、ユーザーのメールが検証済みであることを示します。



4. 期間を選択し、**検索**をクリックして**DATA**テーブルでイベントを表示します。

ゲートウェイ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、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インサイトを取得します。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、各ユーザー接続に対して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、認証ステージ、承認タイプ、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**」(/ja-jp/citrix-analytics/self-service-search.html)を参照してください。

ゲートウェイデータソースを選択する

ゲートウェイイベントを表示するには、リストから **Gateway** 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日間のイベントが表示されます。イベントを表示する期間を選択することもできます。

ゲートウェイデータソースを選択(/en-us/citrix-analytics/media/search-gateway-datasource.png)

> **注**
>
> または、**セキュリティ** > **ユーザー** > **アクセス概要** 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。ログインが成功したシナリオでは、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、「アクセス概要」(/ja-jp/security-analytics/users-dashboard.html#access-summary)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。

ゲートウェイファセット(/en-us/citrix-analytics/media/self-search-gateway-facets-1.png)

- **認証ステージ** - プライマリ、セカンダリ、ターシャリなど、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、スマートカード認証を含むクライアント証明書認証など、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。

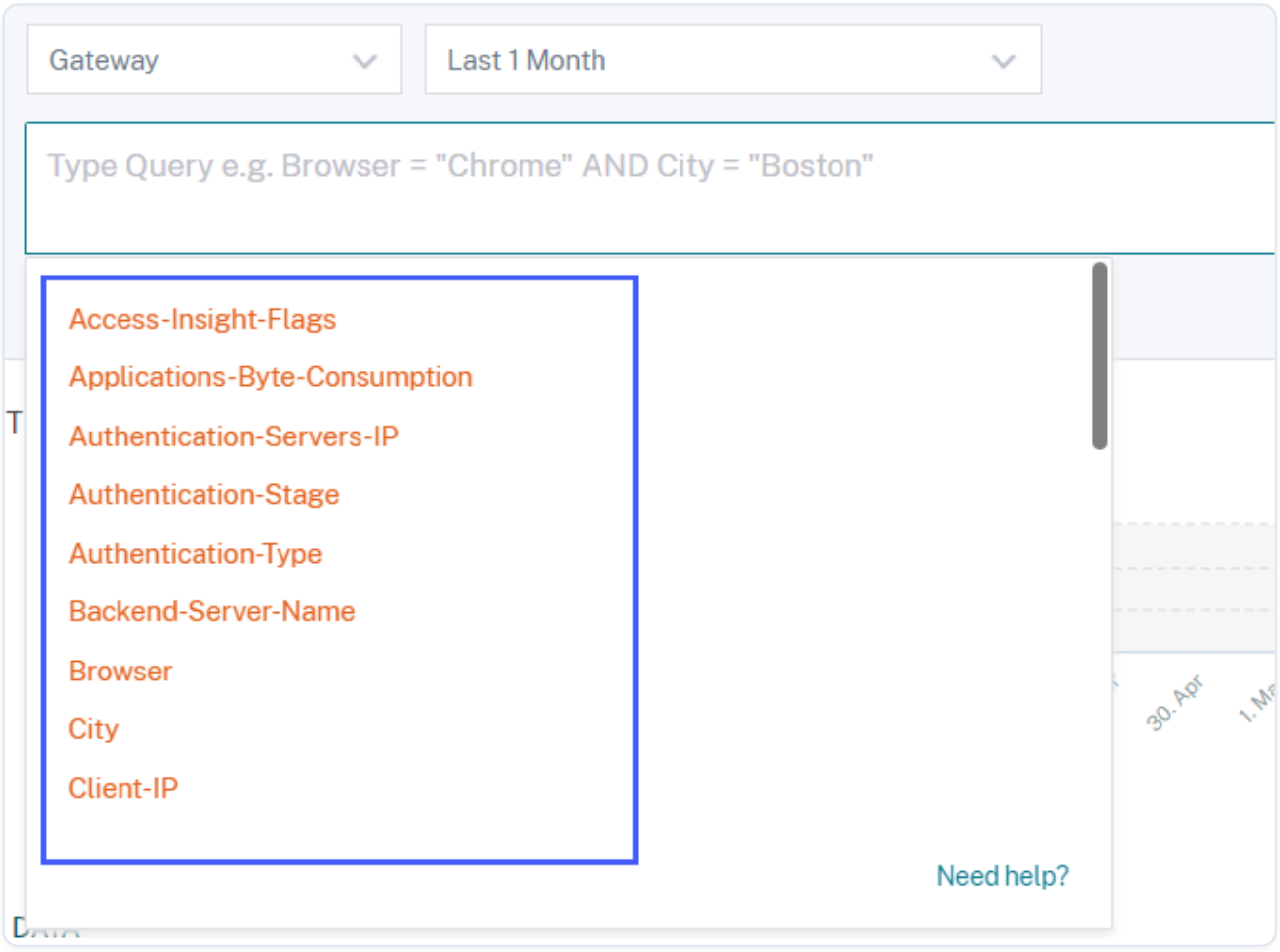
- **デバイスエージェント** - iPhone、iPad、Windows Mobileなどのクライアントデバイスに基づいてイベントを検索します。
- **レコードタイプ** - VPNレコードのタイプに基づいてイベントを検索します。次のVPNレコードタイプが利用可能です。

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。
- **ステータスコード** - SSLリダイレクト応答の失敗、認証の失敗、シングルサインオンの失敗などのVPNステータスコードに基づいてイベントを検索します。
- **セッション状態** - クライアント状態、認証状態、SSO状態、アプリケーション帯域幅更新などの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SSOなどのシングルサインオン認証のさまざまな方法に基づいてイベントを検索します。
- **ログアウトモード** - 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、ユーザー開始ログアウト、管理者によるセッション終了などのVPNログアウトモードに基づいてイベントを検索します。

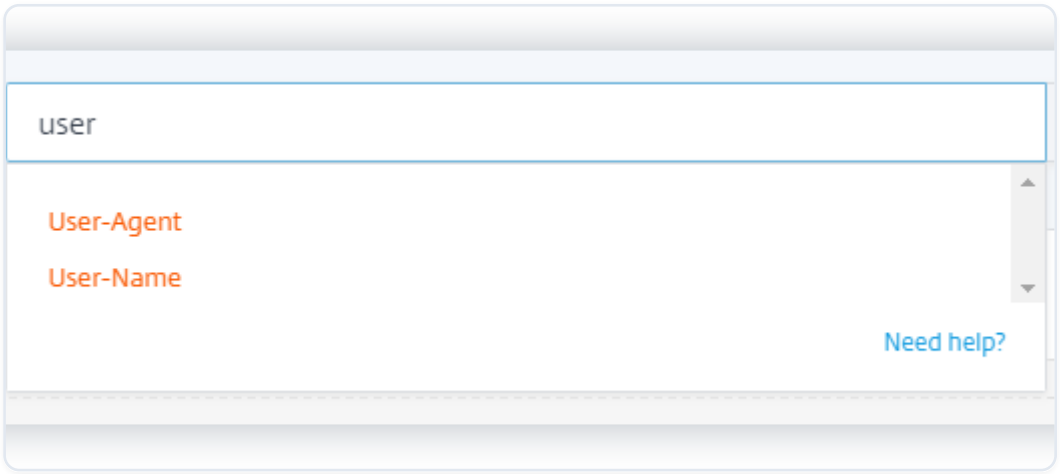
イベントをフィルタリングするための検索クエリを指定する

検索ボックスにカーソルを置くと、Gatewayイベントのディメンション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。

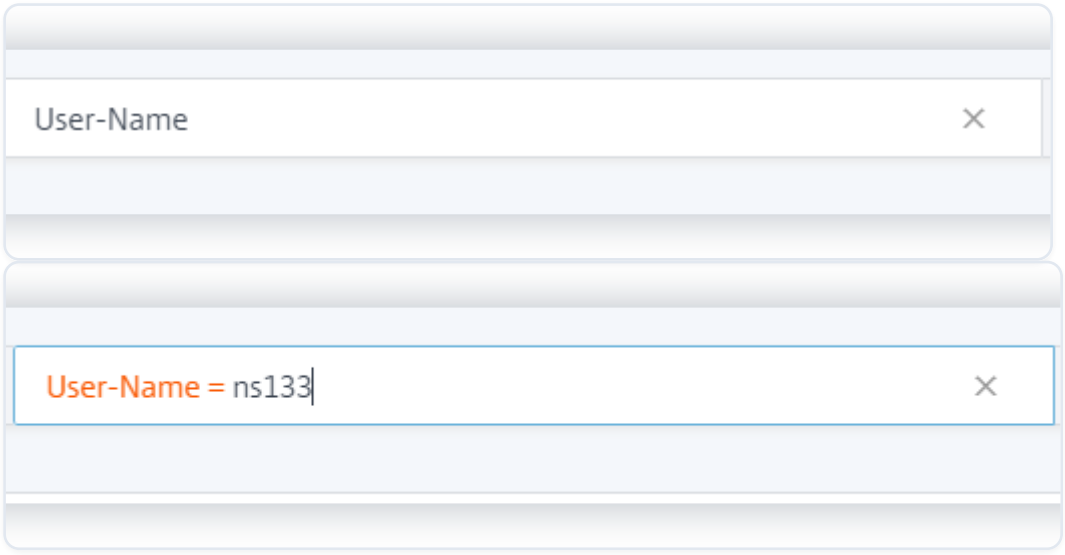


例えば、VPNステータスコードが「successful login」であるユーザー「ns133」のイベントを表示したいとします。

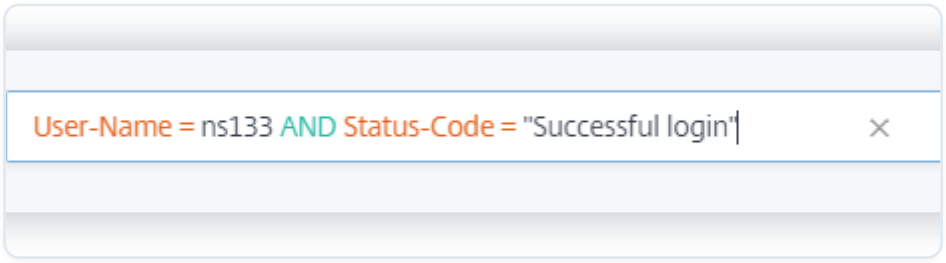
1. 検索ボックスに「user」と入力し、関連するディメンションを選択します。



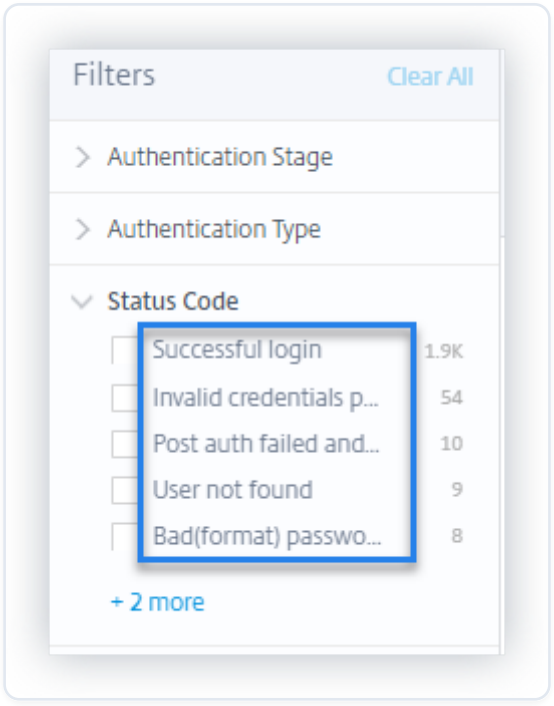
2. **User-Name**を選択し、等号演算子を使用して値「ns133」を入力します。



3. **AND**演算子を選択し、次に**Status Code**ディメンションを選択します。等号演算子を使用して、**Status Code**に文字列「Successful login」を入力します。



Status Codeの可能な文字列値を特定するには、**Status Code**フィルターリストを展開し、フィルター名を検索クエリの文字列として使用します。



4. 期間を選択し、**Search**をクリックして、**DATA**テーブルでイベントを表示します。

検索クエリでサポートされる値

検索クエリを定義するために、ディメンションに以下の値を入力します。

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。以下のフラグ値のいずれかを入力してください。

VPNセッションの状態	フラグ値
事前認証	2
nFactor（多要素）認証の最終状態	1
認証後	4

注

このフラグは、認証イベントの先行するVPNセッション状態にのみ適用されます。その他のすべてのイベントでは、フラグ値はゼロです。

アプリケーション-バイト-消費

`Applications-Byte-Consumption` ディメンションには、以下の値を入力します。

値	タイプ	説明
例: `40`、`100`	数値	使用しているアプリケーションによって消費されたデータ(バイト単位)。

認証サーバーIP

`Authentication-Servers-IP` ディメンションには、次の値を入力します。

値	タイプ	説明
例: `10.xxx.xx.xx`	文字列	認証サーバーのIPアドレス。

認証ステージ

`Authentication-Stage` ディメンションの場合、次の値を入力します。

値	タイプ	説明
`Primary`、`Secondary`、または`Tertiary`	文字列	クライアント認証の異なる段階。

認証タイプ

`Authentication-Type`ディメンションの場合、次の値を入力します。

値	タイプ	説明
`LDAP`、`SAML`、`Local`、`Radius`、`TACACS`、`SAMLIDP`、または`OTP`。	文字列	利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` ディメンションについては、次の値を入力します。

値	タイプ	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

`Browser` ディメンションについては、次の値を入力します。

値	タイプ	説明
`PN Agent`、`Edge`、`Firefox`、`Chrome`、または`Safari`。	文字列	使用されたブラウザ。

都市

`City`ディメンションには、次の値を入力します。

値	タイプ	説明
例: `Boston`, `Beijing`	文字列	ユーザーがログインした都市。

クライアントIP

`Client-IP`ディメンションには、次の値を入力します。

値	タイプ	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`ディメンションには、次の値を入力します。

値	タイプ	説明
パブリック, プライベート	文字列	ユーザーのIPアドレスがpublicかprivateかを示します。

> **注**
>
> 値は大文字と小文字を区別します。値を小文字で入力してください。

クライアントポート

`Client-Port`ディメンションには、次の値を入力します。

値	タイプ	説明
例: `45334`	数値	ユーザーデバイスのポート番号。

国

`Country`ディメンションの場合、次の値を入力します。

値	タイプ	説明
例: `United States`、`India`	文字列	ユーザーがログインした国。

> **注記**
>
> 値にスペースが含まれる場合は、値を「」で囲みます。**例**: Country = "Unites States"。

イベントタイプ

`Event-Type`ディメンションには、次の値を入力します。

値	タイプ	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`ディメンションには、次の値を入力します。

値	タイプ	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` ディメンションには、次の値を入力します。

値	タイプ	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` ディメンションには、次の値を入力します。

値	タイプ	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`ディメンションの場合、次の値を入力します。

値	タイプ	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**: Logout-Mode = `"Internal error"`。

NetScaler-IP

`NetScaler-IP`ディメンションの場合、次の値を入力します。

値	タイプ	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`ディメンションには、次の値を入力します。

値	タイプ	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`ディメンションには、次の値を入力します。

値	タイプ	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。
`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-認証方法

`SSO-Authentication-Method`ディメンションには、次の値を入力します。

値	タイプ	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`ディメンションには、次の値を入力します。

値	タイプ	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`ディメンションには、次の値を入力します。

値	タイプ	説明
例: `47054`	数値	バックエンドサーバーのポート番号。

セッション状態

`Session-State`ディメンションには、次の値を入力します。

値	タイプ	説明
`"Set Client State"`、`"Authorization State"`、`"SSO State"`、および`"Application Bandwidth Update"`	文字列	VPNセッションの状態。

注

値にスペースが含まれる場合は、値を「」で囲みます。**例**: Session-State = `"Set Client State"`。

ステータスコード

`Status-Code`ディメンションには、次の値を入力します。

値	タイプ	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る場合は、値を「」で囲みます。**例**: Session-Code = `"Successful login"`。

ユーザーエージェント

`User-Agent`ディメンションには、次の値を入力します。

値	タイプ	説明
`IPHONE`、`IPAD`、または `WINPHONE`	文字列	VPNへのアクセスに使用されるエージェントまたはデバイス。

VPNセッションID

`VPN-Session-ID`ディメンションの場合、次の値を入力します。

値	タイプ	説明
`c2c290c61dfe4e07247bde1e22142a12`	文字列	ユーザーのVPNセッションに対してサーバーによって割り当てられたセッションID。

VPNセッションモード

`VPN-Session-Mode`ディメンションの場合、次の値を入力します。

値	タイプ	説明
`"Full Tunnel"`、`"ICA Proxy"`、または `Clientless`	文字列	ユーザーのVPNセッションの異なるモード。

> **注**
>
> 値にスペースが含まれる場合は、その値を「」で囲みます。**例**: Session-Code = `"Full Tunnel"`。

ポリシーのセルフサービス検索

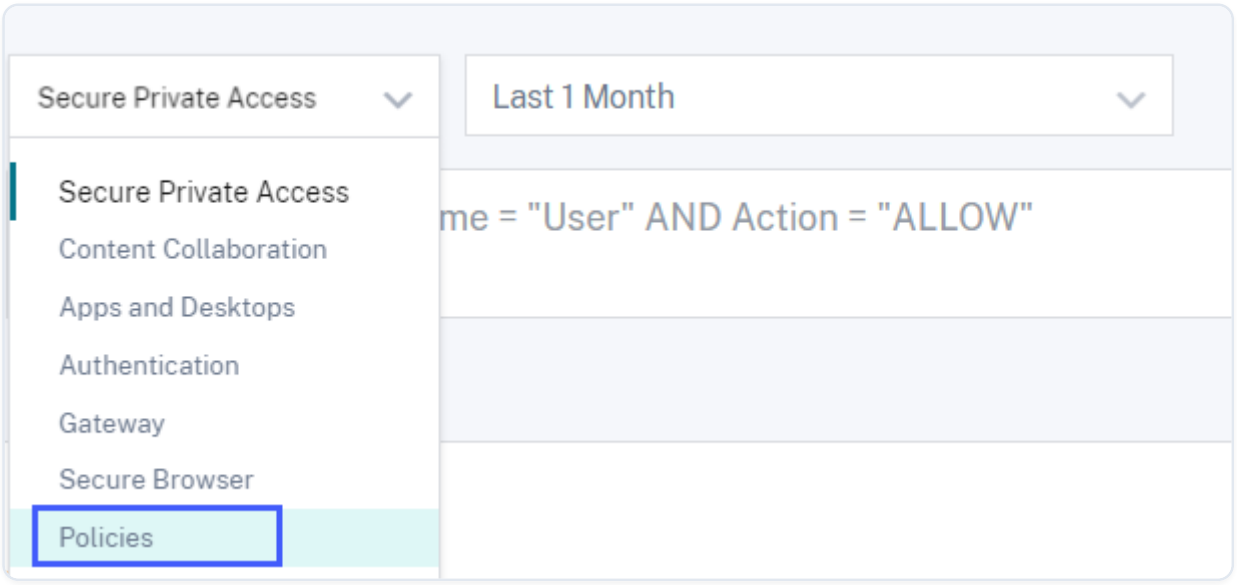
Citrix Analytics for Security を使用すると、ユーザーアカウント上の異常または不審なイベントに対してポリシーを作成し、アクションを適用できます。ユーザーイベントが定義されたポリシーに合致すると、脅威を隔離し、将来の異常なイベントの発生を防ぐために、アクションがユーザーア

カウントに自動的に適用されます。セルフサービス検索を使用すると、定義されたポリシーに合致したユーザーイベントを表示し、これらの異常な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する

定義された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 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日間のイベントが表示されます。イベントを表示したい期間を選択することもできます。

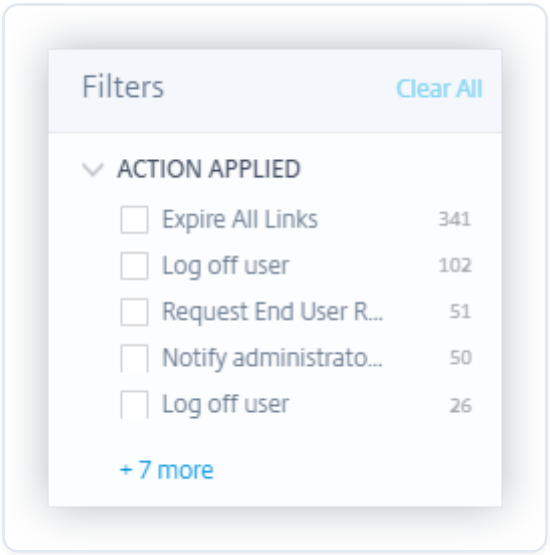


注

> > 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すると、そのポリシーに関連するユーザーイベントが表示されます。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。

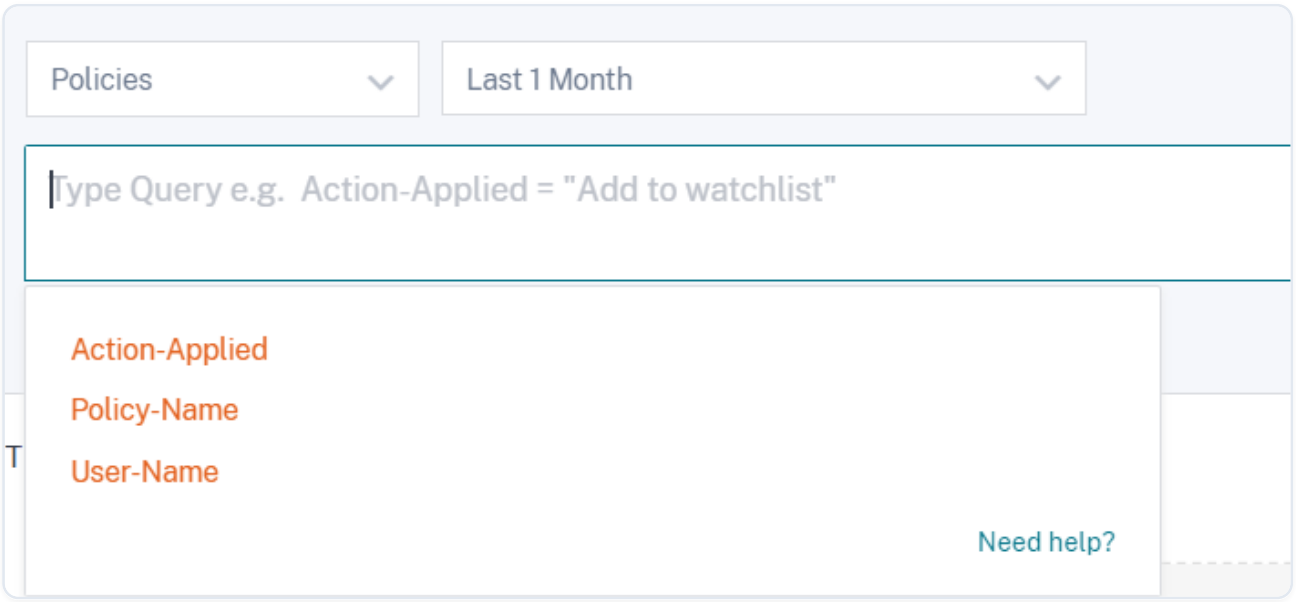
イベントをフィルタリングするファセットを選択する

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。ポリシーの設定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。



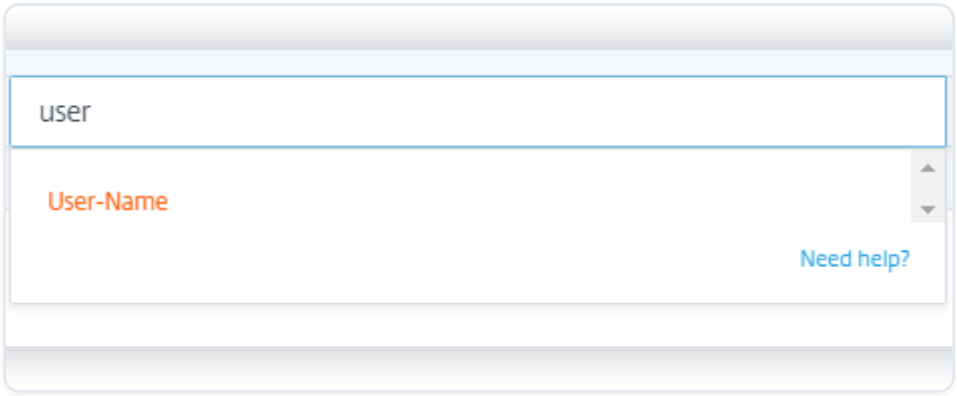
イベントをフィルタリングする検索クエリを指定する

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。

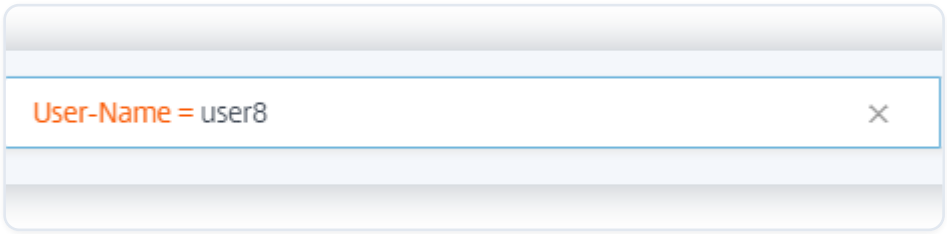


たとえば、ユーザー「user8」の異常なイベントで、それらのイベントに適用されたアクションが「ユーザーを無効にする」であるものを表示したいとします。

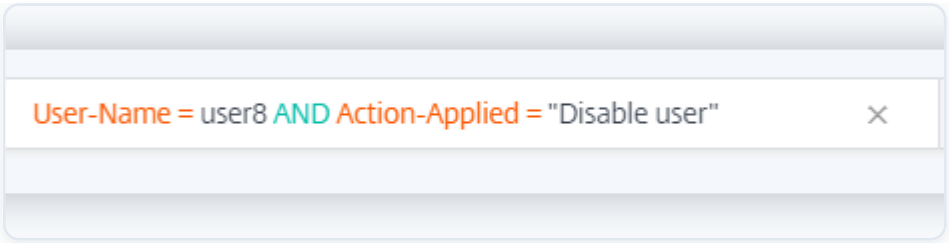
1. 検索ボックスに「user」と入力して、関連するディメンションを取得します。



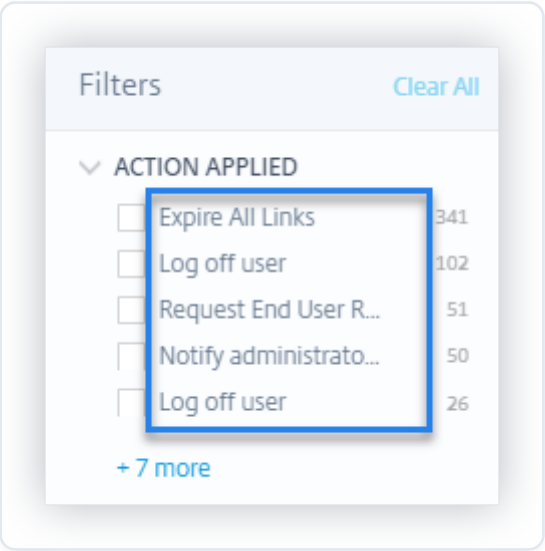
2. **User-Name** を選択し、等号演算子を使用して「user8」という値を入力します。



3. **AND** 演算子を選択し、次に **Action-Applied** ディメンションを選択します。等号演算子を使用して、**Action-Applied** に文字列「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る場合、演算子 `“”` で囲む必要があります。例えば、`“Disable user”`、「Stop Session Recording」のようにです。
>
> 
>

Action-Applied の可能な文字列値を特定するには、ファセットリストを展開し、検索クエリでフィルター名を文字列として使用します。



4. 期間を選択し、**検索**をクリックして**DATA**テーブルでイベントを表示します。

Remote Browser Isolation (Secure Browser) のセルフサービス検索

Citrix Remote Browser Isolation™ Service 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に関するインサイトを得るには、セルフサービス検索を使用します。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エクスペリエンス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。ユーザーとそのブラウジングセッションを追跡できます。

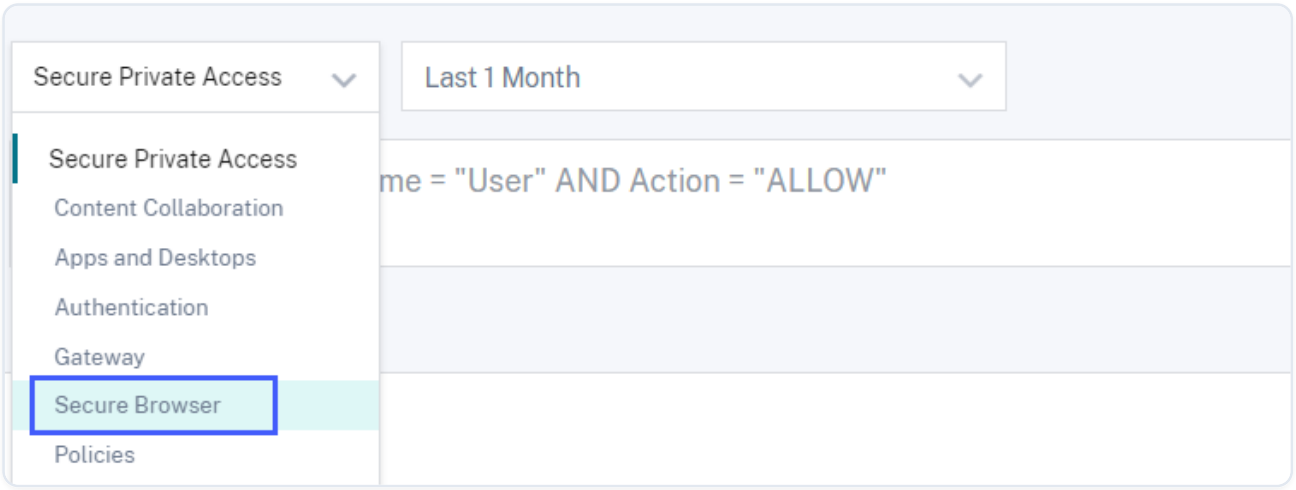
検索機能の詳細については、「**セルフサービス検索**」を参照してください。

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、「公開された Remote Browser Isolation の管理」を参照してください。

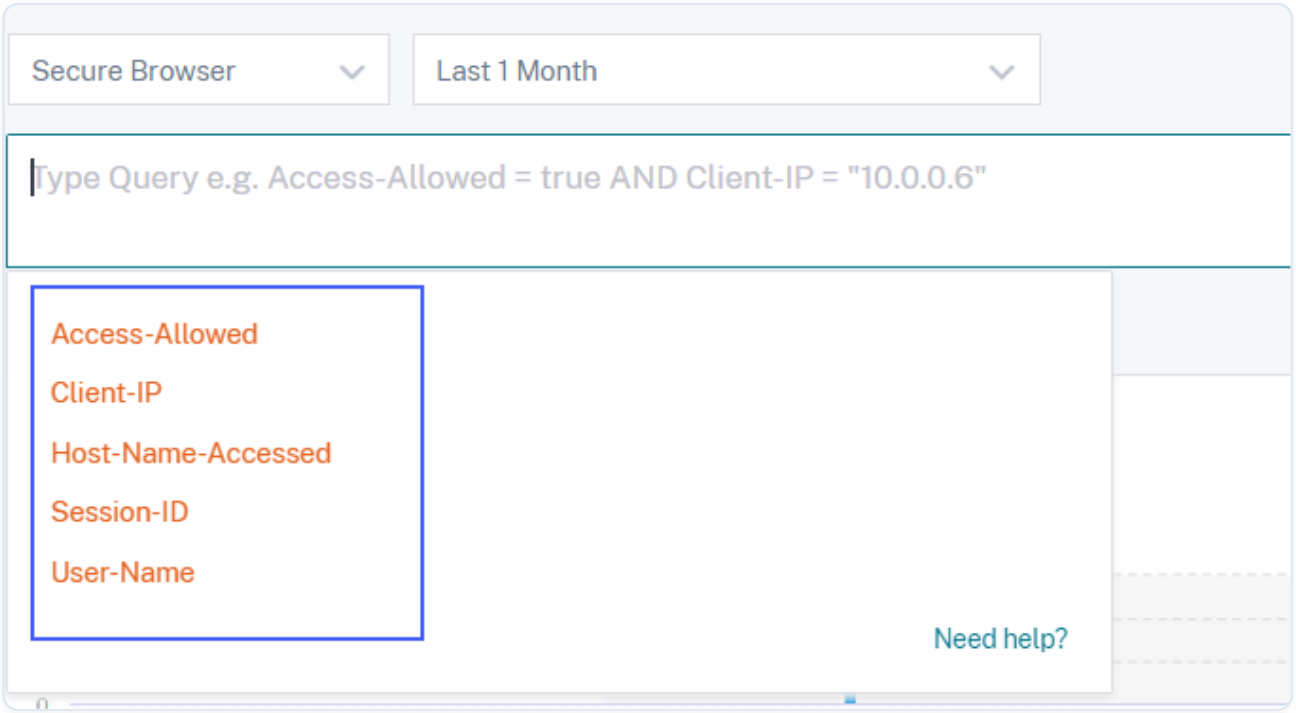
Remote Browser Isolation データソースを選択する

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日間のイベントが表示されます。イベントを表示したい期間を選択することもできます。



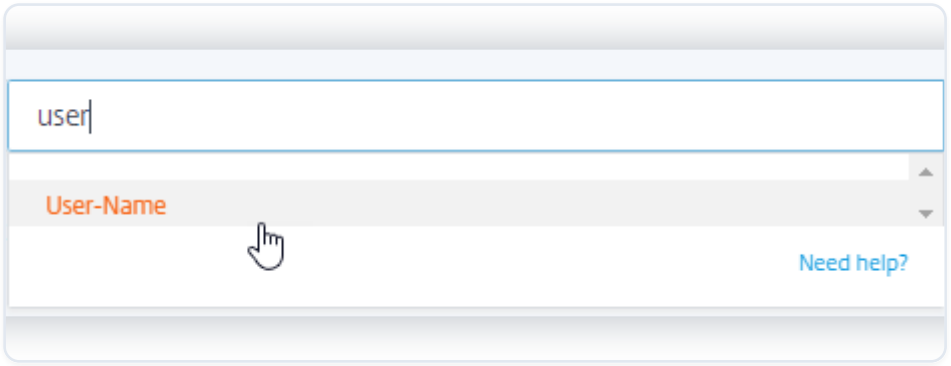
イベントをフィルタリングする検索クエリを指定する

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。

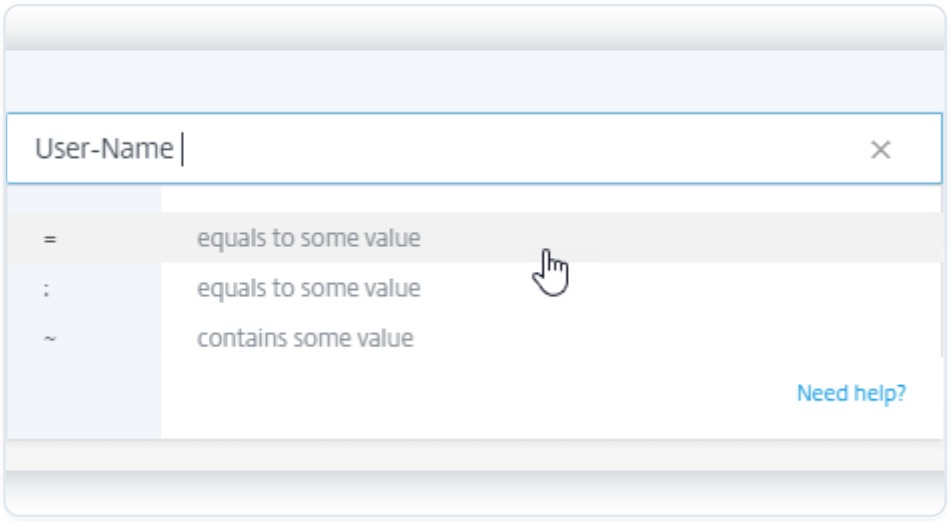


たとえば、google.com、amazon.com など、さまざまなホストサービスへのアクセス権を持つユーザー「aa」のブラウジングイベントの詳細を表示したいとします。

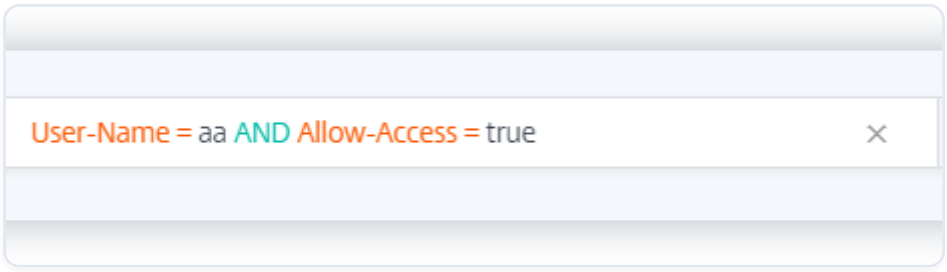
1. 検索ボックスに「user」と入力して、関連するディメンションを表示します。



2. **User-Name** 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「true」の値を割り当てます。「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**テーブルでイベントを表示します。

ユーザーイベントの詳細を表示

リモートブラウザ分離サービスから受信した以下のデータを確認できます。

- **時間** - 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** - ユーザーデバイスの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したホストサービス。
- **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。

Secure Private Access のセルフサービス検索

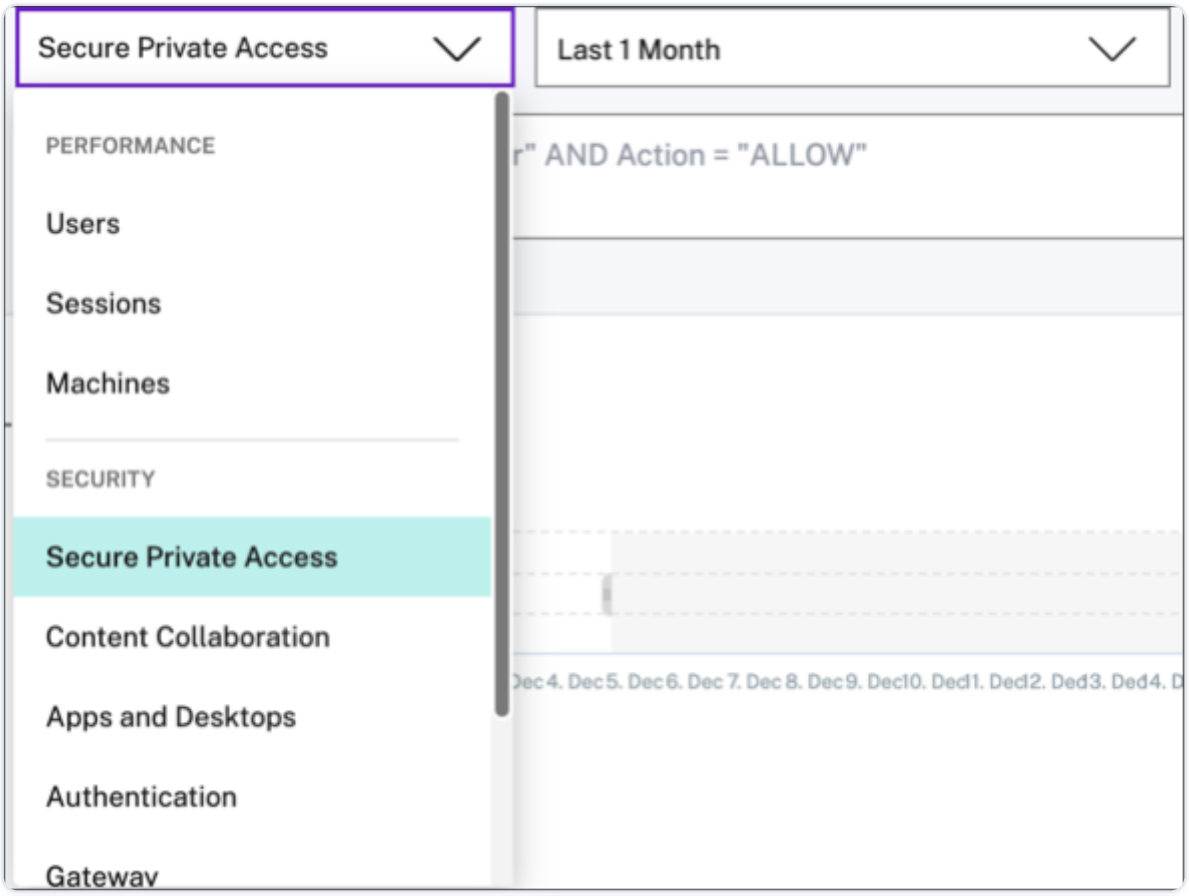
セルフサービス検索を使用して、組織内の Citrix Cloud ユーザーのアクセスイベントに関するインサイトを取得します。アクセスイベントの例としては、URL カテゴリ、コンテンツカテゴリ、ブラウザ、デバイスなどがあります。Citrix Analytics for Security™ は、Secure Private Access サービスからこれらのイベントを受信し、セルフサービス検索に表示します。ユーザーとそのアクセス詳細を追跡できます。

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**
>
> 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 の評価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利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も廃止され、顧客に対してはトリガーされません。
> 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) を使用する既存のカスタムリスクインジケータおよびそれに関連するポリシーは、今後トリガーされません。
>
> Secure Private Access からの廃止の詳細については、「機能の廃止」を参照してください。

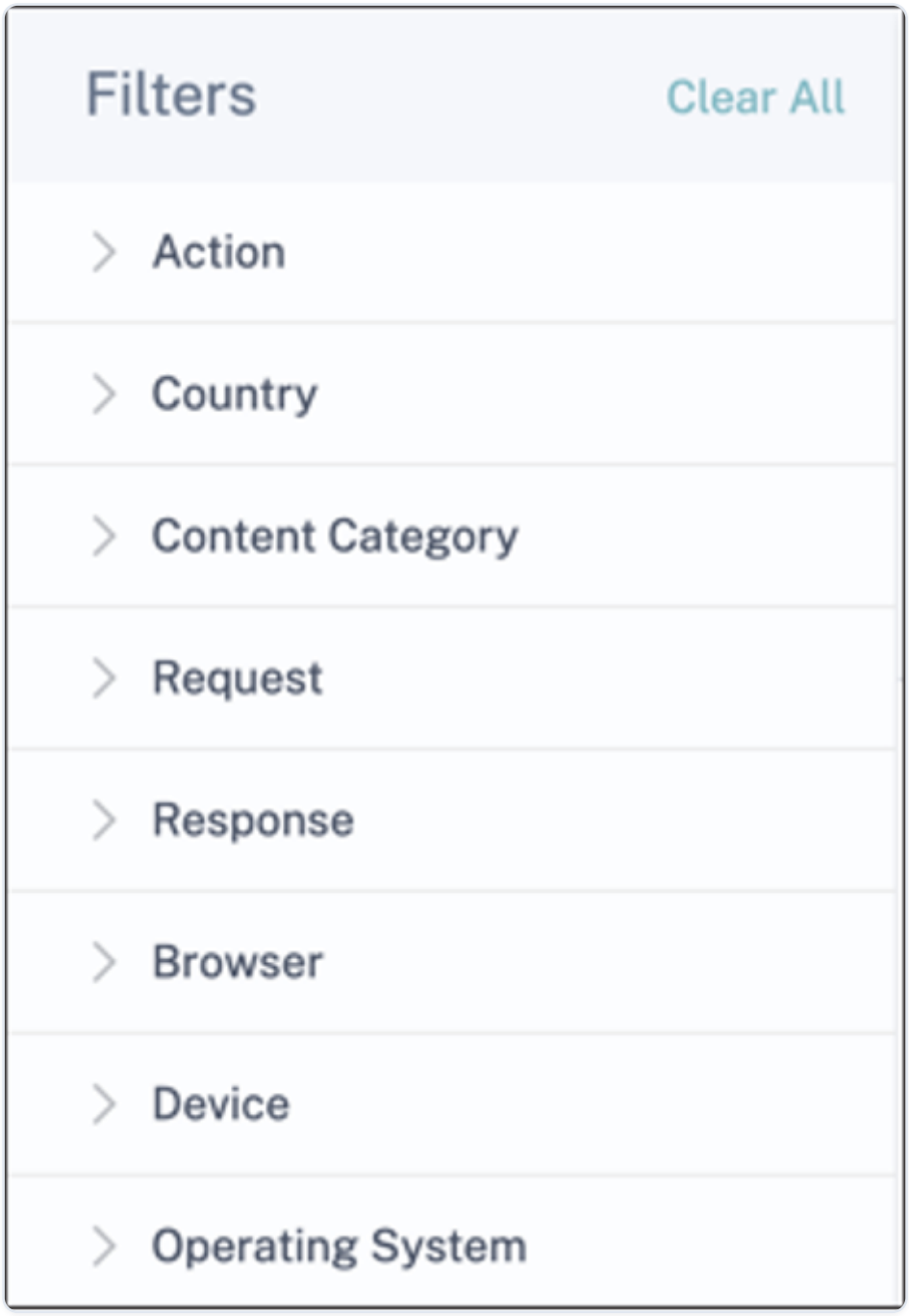
Secure Private Access データソースを選択する

Secure Private Access イベントを表示するには、リストから **Secure Private Access** 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 日間のイベントが表示されます。イベントを表示したい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する

Secure Private Access イベントに関連付けられている以下のファセットを使用します。

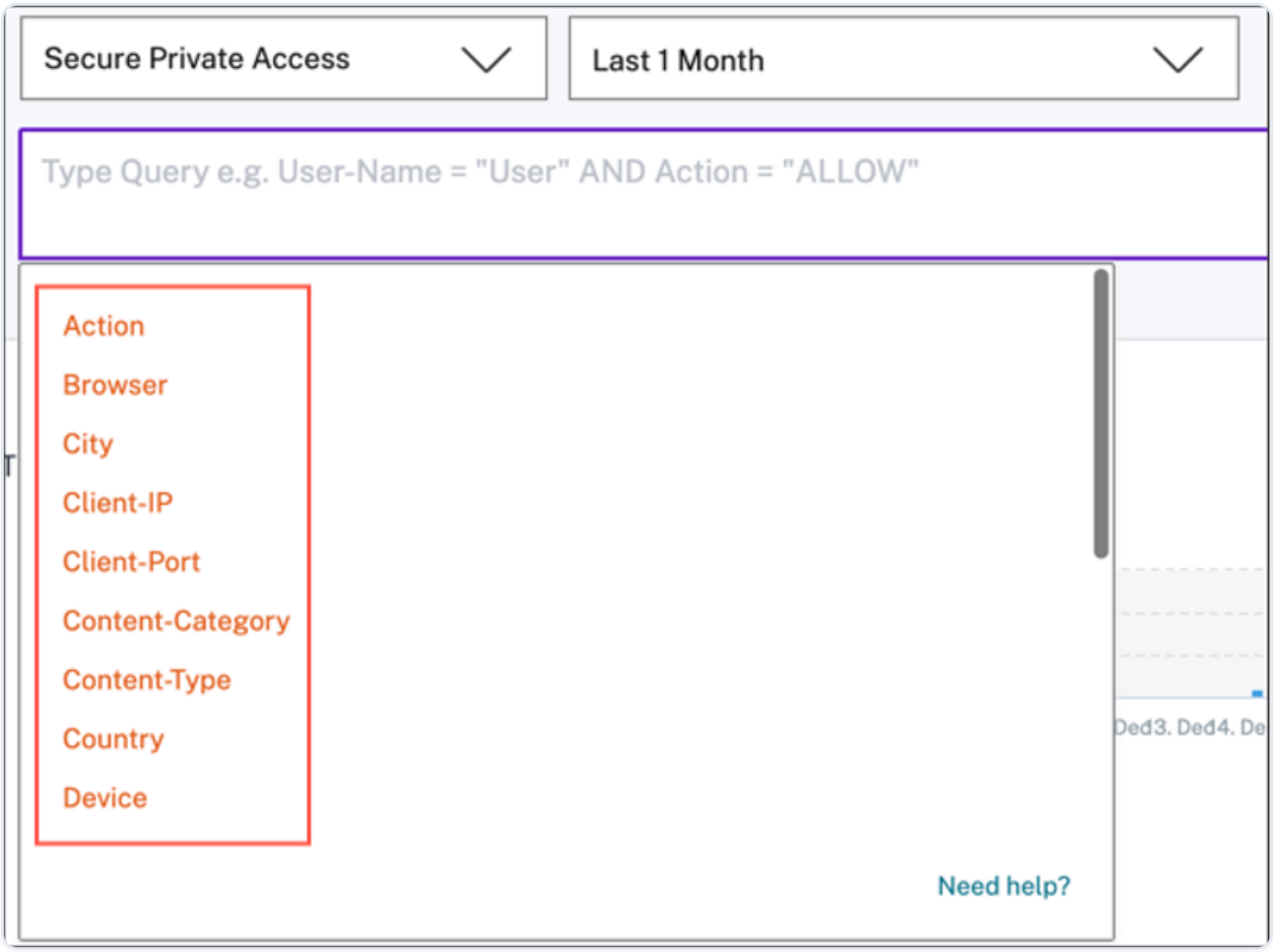


- **アクション** - ユーザーのアプリケーションに対して実行されたアクション（許可、ブロック、リダイレクトなど）に基づいてイベントを検索します。
- **国** - ユーザーのアクセス場所に基づいてイベントを検索します。
- **コンテンツカテゴリ** - アクセスされたコンテンツのカテゴリ（アプリケーション、画像、テキストなど）に基づいてイベントを検索します。
- **リクエスト** - GET、POST、PUT、DELETEなどのHTTPメソッドに基づいてイベントを検索します。
- **レスポンス** - HTTPレスポンスに基づいてイベントを検索します。
- **ブラウザ** - ユーザーが使用した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などの使用された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。

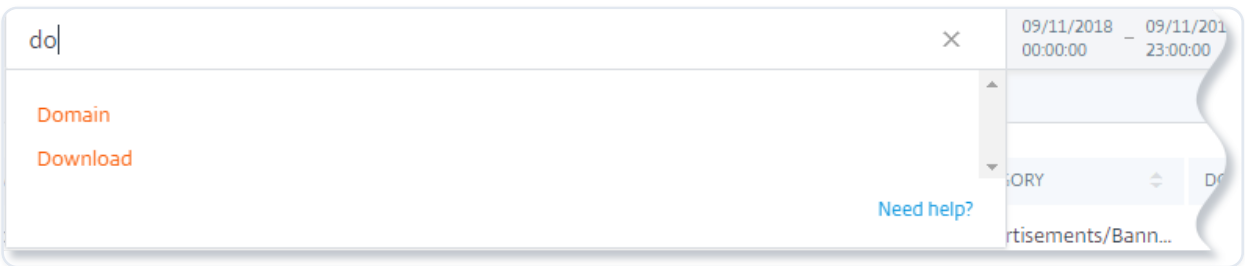
イベントをフィルタリングするための検索クエリを指定する

検索ボックスにカーソルを置いて、Secure Private Access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、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したいとします。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」と入力して、関連する候補を取得します。



2. **ドメイン**をクリックし、等号演算子を使用して「test」という値を指定します。

   「アクセス検索クエリ 3」(/en-us/citrix-analytics/media/self-service-search-query-3.png)

   「アクセス検索クエリ 4」(/en-us/citrix-analytics/media/self-service-search-query-4.png)

3. **AND**演算子を使用し、**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、ダウンロード量をバイト単位で入力します。

   「アクセス検索クエリ 5」(/en-us/citrix-analytics/media/self-service-search-query-5.png)

4. 期間を選択し、**検索**をクリックして、**データ**テーブルでイベントを表示します。

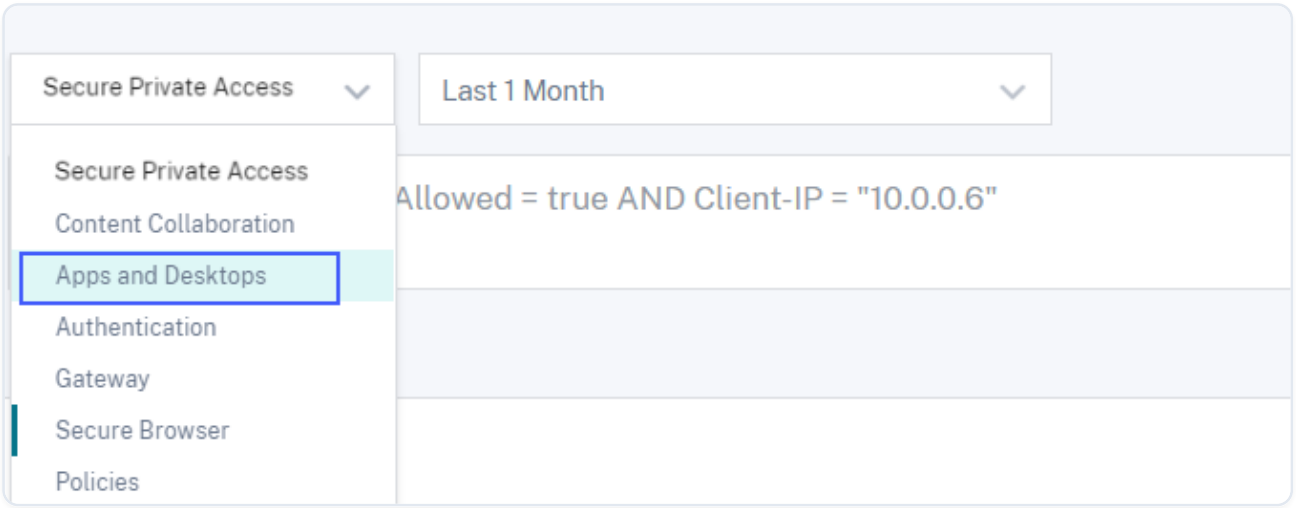
アプリとデスクトップのセルフサービス検索

セルフサービス検索を使用して、Citrix Virtual Apps and Desktopsデータソースおよび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ます。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、そ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、ファイルダウンロード、アカウントログオン、アプリ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する

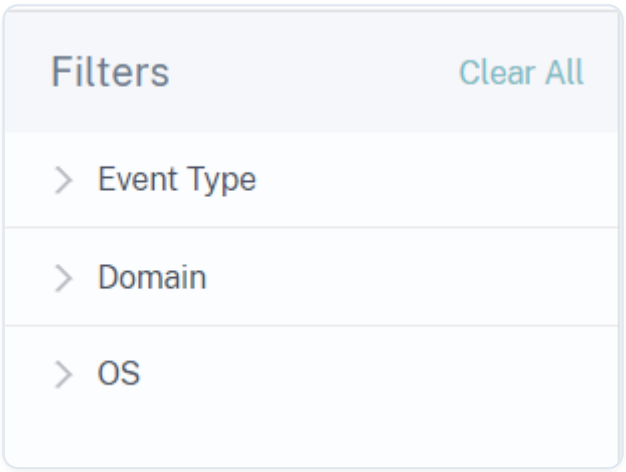
Citrix Virtual Apps and DesktopsまたはCitrix DaaSからのイベントを表示するには、リストから**Apps and Desktops**を選択します。デフォルトでは、セルフサービスページには過去1日間のイベントが表示されます。イベントを表示したい期間を選択することもできます。



デフォルトでは、セルフサービスページには過去1か月間のイベントが表示されます。このページでは、必要なイベントをフィルタリングして絞り込むためのいくつかのファセットと検索ボックスも提供されています。

イベントをフィルタリングするファセットを選択する

アプリとデスクトップ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には、オペレーティングシステム名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てい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。

仮想アプリおよびデスクトップのディメンション(/en-us/citrix-analytics/media/search-cvad-dimensions.png)

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」のイベントを検索したいとします。

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。

仮想アプリおよびデスクトップの検索クエリ 1(/en-us/citrix-analytics/media/virtual-apps-desktops-search-query1.png)

2. **User-Name** をクリックし、等号演算子を使用して「John」という値を入力します。

   仮想アプリおよびデスクトップの検索クエリ 2(/en-us/citrix-analytics/media/virtual-apps-desktops-search-query2.png)

3. **AND** 演算子と **OS-Name** ディメンションを選択します。等号演算子を使用して「Windows 7」という値を割り当てます。

   仮想アプリおよびデスクトップの検索クエリ 3(/en-us/citrix-analytics/media/virtual-apps-desktops-search-query3.png)

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。

イベントの種類とサポートされるフィールド

VDA.Print を除くすべてのイベントタイプで、以下のフィールドが利用可能です。

- 市区町村
- クライアント IP
- 国
- デバイス ID
- OS名
- OSバージョン
- OS追加情報
- 時間
- ユーザー名
- Workspaceアプリバージョン
- Workspaceアプリステータス

次の表は、Apps and Desktopsデータソースで利用可能なイベントタイプと、各イベントタイプに固有のフィールドについて説明しています。

値	説明	フィールド
`Account.Logon`	Citrix Workspaceアプリを介してStoreにログオンしたときにトリガーされます。**注**:	上記で説明した共通フィールドを確認してください。

値	説明	フィールド
	Account.LogonはHTML5クライアントでは利用できません。	
`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
`Session.End`	仮想セッションを終了したときにトリガーされます。	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したときにトリガーされます。**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が起動され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したときにトリガーされます。**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が起動され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したときにトリガーされます。仮想セッション内で発生す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トを許可している場合（詳細についてはファイルリダイレクト設定を参照）と、クライアントワークスペースの**ファイルアクセス**	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

値	説明	フィールド
	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。	
`Printing`	クライアントプリンターを介してCitrix Workspaceアプリが起動したセッション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バリアントで既知の問題があるため、印刷ドキュメント名テレメトリは印刷イベントに含まれません。次に、別の既知の技術的な制限があるため、Windowsの印刷イベントには印刷ファイルサイズテレメトリは含まれません。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。詳細については、「Citrix DaaSの印刷テレメトリを有効にする」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、プリンター名、印刷ファイル形式、印刷ファイルサイズ、セッションサーバー名、セッションユーザー名
`AppProtection.ScreenCapture`	保護されたセッション中にユーザーがスクリーンショットをキャプチャしようとするとトリガーされます。**注**: 詳細については、「App Protection」を参照してください。	保護されたアプリのタイトル、スクリーンキャプチャツール名、スクリーンキャプチャツールパス
`App.SaaS.Launch`	Citrix WorkspaceアプリがCitrix Enterprise BrowserでSaaSアプリを起動す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アプリ名、SaaSアプリURL

値	説明	フィールド
`App.SaaS.End`	Citrix Workspaceアプリが Citrix Enterprise Browserで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URL
`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形式サイズ、クリップボード詳細形式タイプ、クリップボード詳細イニシエーター、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、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アプリ名、SaaSアプリURL
`App.SaaS.Url.Navigate`	Citrix Enterprise BrowserがURLに移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アプリ名、SaaSアプリURL
`Citrix.EventMonitor.AppStart`	セッション記録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開始されたときにトリガーされます。	アプリ名
`Citrix.EventMonitor.AppEnd`	セッション記録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	アプリ名

値	説明	フィールド
	止されたときにトリガーされます。	
`Citrix.EventMonitor.Clipboard`	セッション記録内でクリップボード操作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したときにトリガーされます。	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、宛先パス
`Citrix.EventMonitor.RegistryChange`	レジストリ操作が実行されたときにトリガーされます。可能なレジストリ操作は、作成、削除、名前変更、値の設定、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`	セッション記録が終了したときにトリガーされます。	説明
`Citrix.EventMonitor.SessionLaunch`	セッション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`	最上位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ったときにトリガーされます。	上記で説明した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したときにトリガーされます。	上記で説明した共通フィールドを確認してください。
`Citrix.EventMonitor.WebBrowsing`	仮想デスクトップセッション内のブラウザでユーザーがウェブ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	ファイル名、ファイルパス、ファイルサイズ

値	説明	フィールド
	フォルダが作成されたときにトリガーされます。	
`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。	上記の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内、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。	上記の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
`Citrix.EventMonitor.CDMUSBDriveAttach`	仮想アプリおよび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) でマップされたUSBマスストレージデバイスが挿入されたときにトリガーされます。	上記の共通フィールドを確認してください。
`Citrix.EventMonitor.GenericUSBDriveAttach`	仮想アプリおよび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マスストレージデバイスが挿入されたときにトリガーされます。	上記の共通フィールドを確認してください。

値	説明	フィールド
`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したときにトリガーされます。	宛先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、すべての種類のユーザーアカウント操作に対してトリガーされます。	説明、ターゲットユーザー名
`VDA.Print`	Apps and Desktopsで印刷ジョブが開始されたときにトリガーされます。**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。詳細については、「Citrix DaaSの印刷テレメトリを有効にする」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、プリンター名、時刻、印刷部数合計、印刷ページ数合計
`VDA.Clipboard`	Apps and Desktopsでクリップボード操作が実行されたときにトリガーされます。**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。詳細については、「Citrix DaaSのクリップボードテレメトリを有効にする」を参照してください。	クリップボード形式タイプ、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、イベントをログに記録するためのポリシーがセッション記録サーバーで有効になっている必要があります。詳細については、「カスタムイベント検出ポリシーを作成する」を参照してください。

検索クエリでサポートされている値

検索クエリを定義するには、ディメンションに次の値を入力します。

ディメンション	値	タイプ	説明
`App-Name`	アプリケーションまたはデスクトップセッション。	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。
	アプリケーションセッションの例: ファーム名なしのセッション: `#Cloud - Excel 2016` ファーム名ありのセッション: `XA65PROD#Concur`		
	デスクトップセッションの例: ファーム名なしのセッション: `#SINXIAP0616 $S1-1` ファーム名ありのセッション: `XA65PROD#SINXIAP 0616 $S1-1`		
`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: グーグル クローム, シトリックス エンタープライズ ブラウザ™, マイクロソフト エッジ, ファイアフォックス, サファリ	文字列	ブラウザ名
`Browser-Version`	例: 80.0.3987.122, 101.0.9999.0	文字列	ブラウザバージョン

ディメンション	値	タイプ	説明
`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: 10.10.10.10	文字列	ユーザーエンドポイントのIPアドレス。
`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、Citrix Workspaceアプリの異なる種類を示します。
`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	クリップボード操作がどのように開始されたかを示します。**注**: SaaSアプリケーションのみでサポートされています。
`Clipboard-Operation`	コピー、切り取り、貼り付け、または配置	文字列	どのクリップボード操作が実行されたかを示します。**注**: **place** 操作は、データがクリップボードに配置されたことを示します。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 Event

ディメンション	値	タイプ	説明
			のみで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のみでサポートされています。
`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のみでサポートされています。
`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 アプリケーションのみでサポートされています。
`Clipboard-Size`	例: 10, 20	数値	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: USA、India	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た、ユーザーアカ	文字列	アカウントが作成、削除、名前変更された、またはパスワードのリセットが試行されたなど、ユーザーアカウントの変

ディメンション	値	タイプ	説明
	ウントが有効化された、アカウントのパスワードをリセットしようとした。		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、不完全		セッション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$ \Desktop\Folder\example.txt	文字列	転送完了後のファイルの最終パス。
`Device-ID`	例: cb781185-18ad-4f45-b75f	文字列	ライセンス、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に使用されるデバイス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、RemoteDrive、CD-ROM、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の種類。
`Download-File-Format`	例として: txt, 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`	例として: example-file.txt	文字列	ダウンロードされたファイルの名前。

ディメンション	値	タイプ	説明
`Download-File-Path`	例: C:\Users\admin\Desktop	文字列	ダウンロードされたファイルのパス。
`Download-File-Size`	例: 8.05	数値	ダウンロードされたファイルのサイズ（キロバイト単位）。
`Event-Type`	Account.ログオン, Session.ログオン, Session.終了, App.開始, App.終了, ファイル.ダウンロード, 印刷, AppProtection.画面キャプチャ, App.SaaS.起動, App.SaaS.終了, App.SaaS.クリップボード, App.SaaS.ファイル.ダウンロード, App.SaaS.ファイル.印刷, App.SaaS.URL.ナビゲート, Citrix.EventMonitor.アプリ開始, Citrix.EventMonitor.アプリ終了, Citrix.EventMonitor.最前面, Citrix.EventMonitor.Webブラウジング, Citrix.EventMonitor.ファイル作成, Citrix.EventMonitor.ファイル名変更, Citrix.EventMonitor.ファイル移動, Citrix.EventMonitor.ファイル削除,	文字列	詳細については、「イベントの種類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	値	タイプ	説明
	Citrix.EventMonitor.CDMUSBDriveアタッチ, Citrix.EventMonitor.汎用USBDriveアタッチ, Citrix.EventMonitor.RDP接続, Citrix.EventMonitor.ユーザーアカウント変更, VDA.印刷, VDA.クリップボード, Citrix.EventMonitor.レジストリ変更, Citrix.EventMonitor.セッション起動, Citrix.EventMonitor.セッション終了, Citrix.EventMonitor.クリップボード, Citrix.EventMonitor.ファイル転送		
`Jail-Broken`	はい、またはいいえ	文字列	デバイスがルート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存在しない場合、デバイスはルート化されていません。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へ/クライアントからホストへ	文字列	ファイル転送の方向を示します。

ディメンション	値	タイプ	説明
`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 エンタープライズ	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	印刷されたファイルの形式。
`Print-File-Name`	例: example-file.pdf	文字列	印刷されたファイルの名前。
`Print-File-Size`	例: 10, 20	文字列	印刷されたファイルのサイズ（バイト単位）。
`Printer-Name`	例として: testprinter-1	文字列	使用されたプリンターの名前。
`Process-ID`	例: 11248	文字列	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。このプロセスは、**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します。プロセスIDは現在、Citrix.EventMonitor.RDPConnectionイベン

ディメンション	値	タイプ	説明
			トのみに関連付けられています。
`Protected-App-Titles`	例: アドミン デスクトップ - シトリックス ワークスペース	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 アプリケーション	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/プロキシのURL。**注**: ゲートウェイ/プロキシの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 files (x86)\ScreenContent Client のようなファイルパス	文字列	画面キャプチャツールのパス。

ディメンション	値	タイプ	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	起動され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`	従来のレコーディング/イベントのみのレコーディング	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: ホステッド デスクトップ, Cloud-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`	例として、demo-user や test-user などがあります。	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	ファイルが転送される前の初期パス。
`Target-User-Name`	例: user01	文字列	現在、Target-User-Name は Citrix.EventMonitor.UserAccountModification イベントでのみ使用され、そのイベントでは変更されたユーザーアカウントを指します。
`Total-Copies-Printed`	例: 1, 2	数値	ユーザーが印刷したコピーの総数。
`Total-Pages-Printed`	例: 1,2	数値	ユーザーが印刷したドキュメントページの総数。

ディメンション	値	タイプ	説明
`User-Name`	ユーザー名または Domain\username	文字列	ユーザー名または domain\username。StoreFrontログインに使用されます。StoreFrontへのログオンがCitrix Workspace app for HTML5またはChromeを介していない場合、この値はサーバーから受信したものと同じになります。
`VDA-Name`	例: TSVDA-19-01.xd.local	文字列	VDAマシンの名前を示します。
`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)	文字列	ユーザーのデバイスにインストールされ、リモートの仮想アプリおよびデスクトップセッションを起動するために使用されるCitrix WorkspaceアプリまたはCitrix Receiverのバージョン。
`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

ディメンション	値	タイプ	説明
			Securityによってサポートされているか、サポートされていないかを示します。Workspaceアプリがサポートされていない場合は、**サポート対象外**にカーソルを合わせます。サポートされているバージョンの一覧を表示するためのリンクを含むポップアップウィンドウが表示されます。 Workspaceアプリのバージョンがサポート対象外になる時期が近づくと、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利用可能なサポート対象バージョンが一覧表示されます。

オペレーティングシステムの命名形式

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）の詳細を受け取り、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バージョン**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、パッチなどのオペレーティングシステムの追加情報を示します。

次の表は、オペレーティングシステムのバージョン番号形式のいくつかの例を示しています。

OS名	OSバージョン	OS追加情報
macOS 11	11.5.1	20G80
iOS 14	14.7.1	利用不可
ウィンドウズ 10 エンタープライズ	2009	19043
ウィンドウズ 7	6.1	サービスパック 1
Android 8.1 バージョン	8.1.0	利用不可

注

- Macバージョン11.x以降のOS詳細を取得するには、Citrix Workspaceアプリ for Mac 2108以降のクライアントバージョンが推奨されます。
- Windows 10のOS詳細は現在利用できません。

Citrix Analytics for Security and Performanceのトラブルシューティング

匿名ユーザーを正規ユーザーとして検証

データソースからのイベント送信に関する問題のトラブルシューティング

Virtual Apps and Desktopsイベント、SaaSイベントのトリガーとイベント送信の検証

サポートされているCitrix Workspace™アプリバージョンからユーザーイベントが受信されない

構成済みSession Recordingサーバーの接続失敗

StoreFront™サーバーをCitrix Analyticsに接続できない

FAQ

用語集