Citrix Analytics for Security

Machine translated content

Disclaimer

Contents

新增功能

June 18, 2024

Citrix 的目标是在 Citrix Analytics 客户可用时向其提供新增功能和产品更新。新版本会带来更多的价值，应立即将更新告知客户。

对您（即客户）来说，此过程是透明的。初始更新仅应用于 Citrix 内部站点，然后逐步应用于客户环境。以分阶段的递增方式提供更新有助于确保产品质量并最大程度地保证可用性。

2024 年 **4** 月 **15** 日

新的执行摘要报告

现在，您可以选择将多个报告合并为一份执行报告，该报告可以安排在所需的时间段内。使用这项新功能，您仅向受众提供必要的图形信息。有关详细信息，请参阅执行摘要报告。

2024 年 **1** 月 **29** 日

Workspace 应用程序状态字段更新

- 自助搜索：现在，您可以使用新推出的 **Citrix Apps and Desktops** 数据源的 **Workspace** 应用程序状态字段执行查询，以了解 Workspace 应用程序版本的支持状态。
- 用户：**Workspace** 应用程序状态列已删除。

有关详细信息，请参阅应用程序和桌面的自助式搜索。

2024 年 **1** 月 **25** 日

简化了 **CAS UI** 中的不一致之处

应用程序和桌面数据源的自助搜索功能中解决了以下问题：

- 以前在会话中无序显示的事件现在可以正确显示。
- 默认列已更新。

2024 年 **1** 月 **24** 日

增强了 **SIEM** 环境中的用户个人资料事件

导出到您的 SIEM 环境的用户配置文件事件现在包括：

- IP 地址见解
- Citrix Virtual Apps and Desktops 和 Citrix DaaS（前身为 Citrix Virtual Apps and Desktops 服务）位置见解

这些新的增强功能使您能够识别用于访问组织数据的客户端 IP 地址，并从 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 收集用户位置信息。

有关详细信息，请参阅 SIEM 的风险洞察数据。

2023 年 12 月 1 日

每周电子邮件和 **SIEM** 警报的管理员电子邮件设置页面

新的管理员电子邮件设置功能允许您为系统警报配置自定义分发列表收件人。此增强功能可确保管理员仅收到与其相关的系统警报。

有关详细信息，请参阅管理员电子邮件设置。

用户控制面板-新的活跃用户计数时间筛选器并更新了概述部分

考虑到启用了 Citrix Analytics 的数据源，用户控制面板中的新时间筛选器允许您查看和修改组织在特定时间段内的活跃用户总数。

用户控制面板中增强的概述部分显示了您组织中的用户总数，以及当前登录的活跃和非活跃用户的数量。

有关详细信息，请参阅 用户控制板。

增强的自定义报告

- 现在，您可以使用 Citrix Analytics for Security 中提供的事件和见解来创建和计划定制报告。自定义报告可帮助您提取特定感兴趣的信息并以图形方式组织数据。
- 现在，您可以使用增强的自定义报告平台功能，包括基于自助搜索查询的报告、模板、更好的可视化效果、涵盖所有数据源和指标、计划报告以及导出 PDF。

有关详细信息，请参阅 自定义报告。

2023 年 11 月 30 日

移除 **Citrix Analytics** 中的所有 **ShareFile** 功能

删除了以下 ShareFile 检测功能：

- 分享链接

- 相关风险指标
- 策略及其发生次数
- Content Collaboration 数据导出配置
- Content Collaboration 报告
- Content Collaboration 搜索数据源
- Content Collaboration 保存的搜索
- Content Collaboration 数据源。

删除这些功能可能会导致风险评分和用户时间表暂时不一致。所有其他 Citrix Analytics 功能保持不变。

了解 ShareFile 如何简化直接从 ShareFile.com 访问安全控制的过程。

2023 年 **9** 月 **22** 日

自定义指标中的 **Citrix Secure Browser** 数据源

现在，您可以为 Citrix Secure Browser 数据源创建风险指标，以跟踪用户在安全浏览器中的活动。有关详细信息，请参阅自定义指标。

通过 **SIEM** 数据导出增强每周电子邮件

每周电子邮件已得到增强，通过启用 SIEM 数据导出，可以更深入地了解贵组织的安全状况。现在，您可以加入并激活更多数据源，以发现用户周围的各种事件。每周电子邮件包含以下新增内容：

- 数据摘要部分显示了 SIEM 环境中的数据消耗状态。
- 基于数据导出消耗状态的数据导出建议。

有关详细信息，请参阅每周电子邮件通知。

在电子邮件中使用自定义管理员的通知首选项

Citrix Analytics for Security 现在支持自定义管理员在 Citrix Cloud 中设置的通知偏好。此增强功能使自定义管理员可以更灵活地管理其通知首选项。在发送通知电子邮件（例如每周电子邮件、通知管理员操作电子邮件和数据导出警报）时，也会利用此首选项。

有关详细信息，请参阅管理安全分析的管理员角色。

2023 年 7 月 4 日

在自助搜索和自定义指示器中为操作员提供支持

OR 运算符现在可以在自助搜索和自定义风险指示器功能中使用。您可以在搜索视图中使用 **OR** 运算符，例如自助搜索和自定义指标查询。

有关详细信息，请参阅搜索查询中支持的运算符。

2023 年 6 月 15 日

启用 **VDA** 剪贴板遥测

当您在 Citrix Apps and Desktops. 中启动任何剪贴板操作时，都会触发名为 VDA.Clipboard 的事件。这些剪贴板日志提供重要信息，例如 VDA 名称、剪贴板大小、剪贴板格式类型、客户端 IP、剪贴板操作、剪贴板操作方向以及是否允许剪贴板操作。VDA 剪贴板事件属性也可在自助搜索和自定义风险指示器工作流程中找到。

- 自助搜索：您可以生成报告、保存查询并查看 vda.clipboard 事件及其所有属性详细信息。
- 自定义风险指示器：VDA 剪贴板事件的属性可在自定义指标工作流程中使用。您可以使用这些事件键/值对来配置自定义指标触发器并使用操作设置自动策略。

您可以使用 剪贴板放置安全元数据集合监视 策略来启用剪贴板遥测并将剪贴板日志传输到 Citrix Analytics for Security。默认情况下，此策略处于启用状态。要禁用，请导航到策略页面并将其禁用，以停止从 VDA 收集数据。

有关详细信息，请参阅为 Citrix DaaS 启用剪贴板遥测。

2023 年 6 月 14 日

Citrix Analytics for Security 中会话录制应用程序生命周期和注册表事件的可用性

来自 **Session Recordin** 的以下应用程序生命周期和注册表事件现已在 Citrix Analytics for Security 中可用：

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

您可以查看这些事件，创建自定义指标，并将这些事件导出到您的 SIEM 环境。

有关详细信息，请参阅事件类型和支持的字段。

2023 年 6 月 8 日

已修复的问题

- 发送到 Citrix Analytics for Security 的某些会话登录事件没有用户名。这会导致自助服务搜索和访问保障用户登录页面上的某些事件的用户名列显示为 **NA** 。有时，尽管在访问保障 IP 注册组织图表中查看小时间范围（例如过去 **1** 小时或最近 **1** 天）的数据时，总登录次数不为零，但这也会导致唯一用户数为零。此问题现已修复。[CAS-70954]
- 在“应用程序和桌面的自助式搜索”中，对于 Session.Logon 和 Session.end 用户事件，搜索查询中的应用程序名称维度将填充交付组名称，而不是启动的应用程序或桌面的名称，这可能会误导管理员。应用程序名称维度对于查询 App.Start/App.End 事件更有用，因为它指向正在启动的应用程序。有关更多详细信息，请参阅应用程序和桌面的自助式搜索。此问题现已修复。[CAS-67968]
- 如果您的组织已加入 亚太南部 主区域的 Citrix Cloud，则 Content Collaboration 事件在您的 Citrix Analytics 租户中不可见。此问题现已修复。[CAS-62317]
- 很少版本的 Citrix Workspace 应用程序和 Citrix Receiver 客户端不会向 Citrix Analytics 发送特定事件。因此，Citrix Analytics 无法为这些事件提供见解并生成风险指示器。此问题现已修复。有关详细信息，请参阅检查 6：虚拟应用程序和桌面事件是否已传输到 Analytics? 。[CAS-16151]

2023 年 5 月 29 日

适用于 **Splunk** 的 **Citrix Analytics** 加载项现已在 **Splunk** 云平台上线

适用于 Citrix Analytics 的 Splunk Integration 利用适用于 Splunk 的 Citrix Analytics 插件连接到分析环境并将关键业务数据引入您的 Splunk 环境。

早些时候，Splunk 对插件进行了审查，仅用于安装在 Splunk Enterprise 层上，客户负责在本地 Splunk 环境中配置该附加组件。在最新版本的 2.1.2 中，该插件增加了 Splunk 平台与 Splunk Cloud 的兼容性。使用带有 IDM 或 **Victoria** 实例的经典实例的客户可以利用此平台兼容性增强功能。现在，客户可以灵活地在 Splunk Enterprise 或 Splunk Cloud 之间进行选择，同时考虑部署我们的插件以促进 Splunk 集成。

有关详细信息，请参阅 Splunk 集成。

SIEM 中的 **Session Recordin** 事件

Session Recordin 事件现在可以以应用程序和桌面的风险洞察事件和数据源事件的形式导出到 SIEM。新添加的事件类型可以在“数据导出”页面下的“导出数据事件”阶段中找到。

有关详细信息，请参阅 策略和操作。

2023 年 5 月 24 日

通知最终用户全球操作

Citrix Analytics 中的“策略和操作”功能现在支持“通知最终用户”全局操作，该操作可以与内置或自定义的风险指标触发器配对。管理员可以使用“通知最终用户”操作创建策略，该策略仅为最终用户生成电子邮件通知。此操作可用于各种合规用例，例如通知用户未经批准的应用程序使用情况，或者在不采取任何破坏性操作的情况下提醒用户注意其 Citrix 帐户的可疑行为。管理员可以根据特定场景自定义电子邮件正文和主题行。

有关详细信息，请参阅通知最终用户。

2023 年 5 月 4 日

测试事件生成

创建测试事件生成功能的目的是帮助客户快速测试其 Citrix Analytics-SIEM 管道。以前，如果管理员必须测试此集成，则她/他必须等待数据源引导和用户活动，才能检查事件是否由 Citrix Analytics 生成并由其 SIEM 环境接收。这已不再是必需的。只需单击“发送测试数据”按钮即可将虚拟事件发送到 SIEM 环境，然后使用提供的查询来检查 Citrix Analytics SIEM 集成是否按预期设置。这也适用于试图调试中断的数据流的管理员，因为它可以帮助确定故障点。

有关详细信息，请参阅 测试事件生成。

生成 **SIEM** 电子邮件警报

SIEM 电子邮件警报生成功能将数据导出的故障排除之旅提升到了一个新的轻松水平。Citrix Analytics 会针对可能导致或表明 SIEM 数据流中断的活动发送系统警报。该电子邮件将分发给 Citrix Cloud 管理员、安全完全管理员、安全只读管理员以及安全和性能只读管理员。以下是发送的不同类型的警报：

1. **SIEM** 数据导出警报**-**密码已重置

   每当从“数据导出”页面重置帐户密码时，就会触发此电子邮件。如果仅在 Citrix Analytics for Security GUI 上完成，则可能导致数据流中断。此警报包含执行密码重置的时间，因此可以更轻松地恢复成功的数据流。

2. **SIEM** 数据导出警报**-**数据流已停止

每当客户面临数据流中断表单时，就会触发此电子邮件

- 超过 **24** 小时 -使用警报中的有用故障排除提示或使用快速 指南中的“数据导出摘要”选项卡快速恢复成功的数据流的关键时机。
- 超过 **7** 天 -每位客户主题的 Kakfa 保留策略为七天，这意味着某些安全发布的数据可能已过期。必须使用故障排除工具恢复向 SIEM 的数据流。
- 超过 **30** 天 -这意味着客户受到了安全性数据的影响，需要立即注意恢复从 Citrix Analytics 到 SIEM 环境的数据流。

有关详细信息，请参阅 SIEM 电子邮件警报生成。

2023 年 4 月 13 日

已修复的问题

Windows Citrix Workspace 应用程序从 Citrix Workspace 应用程序版本 2203 及更高版本发送一个空文件名、路径和格式属性。因此，Citrix Analytics for Security GUI 显示了“下载文件名”、“下载文件路径”和“下载文件格式”列的 NA 值。此问题现已修复。[CAS-73498]

2023 年 3 月 31 日

Citrix Analytics for Security 中的会话记录事件

在 Citrix 应用程序和桌面中，添加了两种新的事件类型，以帮助识别和评估基于会话记录的事件。

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

管理员现在可以轻松识别和评估潜在的安全风险。他们可以使用这些事件来收集有关重要数据的信息，例如进程 ID、目标 IP 地址和用户帐户操作描述。此外，这些事件还可以在 自定义风险指示器 页面和 自助搜索 页面上找到。

- 自助搜索：您可以查看这些事件及其属性详细信息。
- 自定义风险指示器：您可以使用这些事件类型配置任何自定义指标。
  有关详细信息，请参阅事件类型和支持的字段。

自助搜索中的 **App Protection** 事件

当您在 Citrix Apps and Desktops 数据源下的受保护会话中尝试捕获屏幕截图时，会触发一个名为 **AppProtection.ScreenCapture** 的新事件。**AppProtection.ScreenCapture** 事件也可以在自助搜索和数据导出页面上找到。

- 自助搜索：您可以查看 **AppProtection.ScreenCapture** 结果及其所有属性详细信息。
- 数据导出：您可以在“数据导出”部分下查看 **AppProtection.ScreenCapture** 事件类型。导航到“设置” **>** “数据导出” **>** “配置” **>** “要导出的数据事件”从“数据源事件（可选）”类别中选择“应用程序和桌面”。

您还可以查看 **Session.Logon** 事件的名为“**App Protection** 策略”的新属性。

有关详细信息，请参阅事件类型和支持的字段。

2023 年 3 月 30 日

自定义角色支持

可以使用 Active Directory 或 Azure Active Directory 中的组为自定义角色添加管理员，也可以为 Citrix Analytics for Security 设置 Okta 集成。这种集成使管理所有组管理员的服务访问权限的简化方法成为可能。

成功将管理员添加到 Active Directory 或 Azure Active Directory 后，管理员可以创建组并将自定义角色分配给特定组。如果管理员是两个权限的成员，则个人权限优先于组权限。

有关详细信息，请参阅 自定义角色支持。

SIEM 用户界面的故障排除面板

通过以下更改增强了数据导出用户界面：

- 摘要选项卡：摘要选项卡描述了以下场景中的 SIEM 事件指标、数据源载入状态和数据消耗状态：
  - **Citrix Analytics** 中的可用数据：提供不同数据源的载入状态。
  - 适用于 **SIEM** 消费的可用事件：提供发送到您的 SIEM 环境的见解数量。
  - **SIEM** 的数据消耗：提供数据消耗状态。
- 配置选项卡：“配置”选项卡包含有关您的帐户设置、SIEM 环境设置和数据事件选择的信息。
- 数据导出快速指南：管理员现在可以使用 快速指南，这样可以更轻松地设置和维护 SIEM 集成。可从“摘要”和“配置”选项卡访问“数据导出快速指南”链接。

有关详细信息，请参阅 数据导出故障排除。

2023 年 3 月 24 日

更改用户个人资料视图

与应用程序、位置、设备和 ShareFile 数据使用情况相关的用户个人资料数据在用户时间轴的用户信息页面上不可用。以下来自 Active Directory 的用户信息仍然可用-

- 职称
- 地址
- 电子邮件
- 電話
- 位置
- 组织

导出到 SIEM 的用户配置文件数据没有变化。有关详细信息，请参阅 用户个人资料。

从所有搜索视图中移除动态自动建议

以下页面现已弃用基于租户历史数据的维度自动建议功能：

- 自助搜索
- 自定义风险指示器

但是，搜索框中仍然提供事件类型和剪贴板操作等维度的静态建议。

有关详细信息，请参阅如何使用自助搜索。

2023 年 3 月 21 日

建议面板可帮助载入本地 **StoreFront** 数据源

数据源页面上引入了新的推荐面板。数据源页面上的“建议”面板向用户介绍载入本地 StoreFront 数据源的重要性。它可以帮助用户轻松加载本地 StoreFront 数据源，还为用户提供了查看和确保载入所有可用数据源的选项。

有关更多详细信息，请参阅连接到 StoreFront 部署。

2023 年 2 月 23 日

已修复的问题

对于 Citrix Apps and Desktop 版本高于 1912 的本地 Citrix Apps and Desktop 部署，操作将失败。在手动操作和基于策略的操作中都发现了此问题。此问题现已修复。[CAS-69098]

当虚拟应用程序仅启动一次时，“应用程序和桌面的自助式搜索”页面会显示多个应用程序启动和应用程序结束事件。适用于 Linux 客户端的 Citrix Workspace 应用程序版本会出现此问题。此问题现已修复。[CAS-36236]

在 2022 年 4 月 4 日之后，最晚到 2022 年 5 月底之前，您的 Citrix Analytics 租户可能无法使用来自 Secure Private Access 服务的用户事件。此问题现已修复。[CAS-66897]

2023 年 2 月 22 日

增强了每周电子邮件通知

Citrix Analytics 每周发送电子邮件通知，帮助汇总贵组织的安全风险敞口。通过以下更新改进了每周电子邮件通知：

- 提供用户风险分布视图-一周内发现的用户总数、风险用户和非风险用户数
- 一周内处理的事件总数
- 一周内触发的指示器总数
- 一周内执行的操作总数

- 已开启数据处理的数据源总数

有关更多详细信息，请参阅每周电子邮件通知。

为 **App.SaaS.File.Download** 事件类型添加了“下载文件格式”字段

在应用程序和桌面数据源的自助搜索页面中，为 App.SaaS.File.Download 事件类型添加了一个新的下载文件格式字段。通过此更改，您现在可以为“下载文件格式”字段配置自定义风险指示器，也可以将该字段作为“导出至 CSV 格式”的一部分导出。

有关详细信息，请参阅应用程序和桌面的自助式搜索。

浏览器衍生字段的变化

以前，自助搜索页面包含浏览器、浏览器主要版本和浏览器次要版本字段来表示浏览器名称和版本。但是，为了确保清晰度和准确性，现在不推荐使用这三个字段，取而代之的是自助搜索中的浏览器名称和浏览器版本、自定义指示器模板以及应用程序和桌面数据源的 CSV 下载。

有关详细信息，请参阅应用程序和桌面的自助式搜索。

2023 年 **2** 月 **16** 日

已修复的问题

在获取租户的用户名屏蔽状态时，某些欧盟和 APS 客户的每周电子邮件会受到影响。结果，由于例外情况，管理员每周会收到 10 封相同的电子邮件。异常发生后，后续租户没有收到每周的电子邮件。此问题现已修复。[CAS-76138]

2023 年 **2** 月 **3** 日

对欧盟和亚太南部地区提供的 **Citrix Secure Private Access** 服务的分析支持

Citrix Analytics for Security 现在可以处理来自欧盟地区和亚太南部地区提供的 Citrix Secure Private Access 的用户事件。如果您的组织是从欧盟地区或亚太南部地区加入 Citrix Cloud 的，则可以查看使用 Secure Private Access 服务的用户的风险见解。

有关详细信息，请参阅 数据源。

2023 年 1 月 11 日

从“**Secure Private Access**”中移除 **Web** 过滤功能

Web 过滤功能已从“Secure Private Access”类别中删除。由于 Secure Private Access 已弃用基于类别的 Web 筛选，Citrix Analytics for Security 的以下功能受到影响：

1. Citrix Analytics for Security 控制板上不再提供诸如类别组、类别和 URL 信誉之类的数据字段。
2. 依赖于相同数据的风险 Web 站点访问指示器也已弃用，不会为客户触发。
3. 任何使用数据字段（类别组、类别和 URL 信誉）及其关联策略的现有自定义风险指示器都不会再触发。
4. “用户访问权限”和“应用程序访问权限”选项卡。
5. 一段时间以来，SIEM 导出继续具有 urlcategory、urlcategorygroup 和 urlcategoryreputation 属性，虚拟值如下：
    - 99999 表示类别和类别组
    - 0 表示信誉

有关详细信息，请参阅 Secure Private Access 的自助搜索。

2022 年 12 月 27 日

更改自助搜索的数据源下拉列表

默认情况下，数据源列表已更改为反映会话，而不是自助搜索页面中的应用程序和桌面。此外，由于性能数据源不可见，性能部分移至顶部，然后移至安全部分。

有关详细信息，请参阅 自助搜索。

2022 年 12 月 13 日

用户控制板增强

用户控制板经过改进，增加了摘要和图表，以帮助管理员监视组织的安全状况。该视图不仅提供发现的用户、触发的风险指示器和应用的操作的详细信息，还提供了基于时间的关键指示器趋势线，以便更好地评估风险。管理员可以深入研究感兴趣的数据，并在正确的上下文中导航到相关的控制板，以更快地进行风险分析。

有关详细信息，请参阅 用户控制板。

2022 年 12 月 5 日

访问保障控制面板-登录网络

新添加了“登录网络”部分，它提供了以下用户详细信息：

- 与用户登录的 IP 地址相关的组织。
- 用户登录的唯一公有子网和私有子网的总数。
- 用户使用代理和私有 VPN 服务登录的详细信息。

使用这些其他详细信息，管理员可以验证用户登录详细信息，并确保用户登录符合组织的安全期望。

有关更多详细信息，请参阅 访问保障控制面板。

2022 年 11 月 18 日

已修复的问题

- 在没有任何源事件的情况下错误触发的地理围栏指示器已修复。[CAS-73222]

2022 年 11 月 8 日

重命名操作

为了提高清晰度，Citrix Analytics for Security 中使用的某些操作已重命名。这些操作如下：

- 通知管理员 -通知管理员
- 锁定用户 -锁定用户帐户
- 注销用户 -注销活动会话
- 解锁用户 -解锁用户帐户
- 禁用用户 -禁用用户帐户

有关详细信息，请参阅 操作有哪些?

已修复的问题

- 如果从时间轴操作下拉列表中选择一个选项，则无法触发任何手动操作，因为“清除”和“应用”按钮不可见。这种情况发生在最新的 Firefox 版本中。此问题现已修复。[CAS-72051]
- **HardDrive**、**harddrive** 和 **HDD** 类别合并为一个类别，作为“应用程序和桌面”数据源自助搜索中“下载-设备类型”字段的“硬盘驱动器”。[CAS-67188]
- 有时，会从 Microsoft Graph 收到具有相同警报 ID 的重复通知，这会导致创建重复的风险事件。在应用程序中实施了重复数据删除机制，以防止出现此问题。[CAS-66731]

2022 年 10 月 19 日

日期源事件选择和导出

除了计算机学习生成的风险洞察事件和相关数据外，您现在还可以利用新的数据事件导出工作流程来导出数据源事件。

这使安全和安全运营 (SOC) 管理员能够：

- 将来自 Citrix Analytics 的数据与聚合在安全信息和事件管理 (SIEM) 上的其他数据源事件关联起来
- 控制哪些数据事件流向 SIEM 以优化存储成本

数据事件将传送到您现有的 SIEM 集成和数据连接器，与我们的自助服务事件搜索视图中提供的数据相同。

有关详细信息，请参阅 从 Citrix Analytics for Security 导出到您的 SIEM 服务的数据事件。

2022 年 10 月 18 日

允许管理员在 **Citrix DaaS** 站点上运操作态会话录制操作

管理员现在可以在 Citrix DaaS 站点上运操作态会话录制操作以及动态录制用户的虚拟会话。他们可以将操作配置为在 Citrix Analytics for Security 检测到给定用户的危险活动时自动开始记录用户会话的策略。

有关详细信息，请参阅 操作有哪些?

2022 年 10 月 14 日

为用户风险指示器提供反馈

Citrix Analytics for Security 管理员现在可以通过在指示器详细信息面板上提供反馈，将用户风险指示器报告为有用或无用。此功能使管理员能够报告误报，减少频繁触发的指示器的干扰，并与其他管理员共享更多上下文。另一个结果是，无用的风险指示器被隐藏在用户的时间表中，并且对用户风险评分进行了重新校准。

有关详细信息，请参阅为用户风险指示器提供反馈。

2022 年 9 月 26 日

访问保证以支持地理围栏封禁列表

在地理围栏设置下添加了安全和危险位置选项卡。

- 安全位置地理围栏有助于识别和限制在已定义的地理围栏区域之外的进入。
- 危险位置地理围栏有助于根据组织的已知行为检测和缩小有风险的用户访问范围。

安全和风险地理围栏均由其自己预先配置的自定义风险指示器支持。

有关详细信息，请参阅启用地理围栏。

已修复的问题

- Citrix Cloud API 用于在电子邮件正文中显示客户名称。现在，该电子邮件使用昵称在发送给管理员的电子邮件正文中显示客户名称。[CAS-65350]
- Citrix Gateway 数据源卡在 **Citrix Analytics for Security** 和 **Citrix Analytics for Performance** 中很常见。数据处理经常调用 Citrix Analytics for Security 端点，对于只有 **Citrix Analytics for Performance** 授权的客户已损坏。[CAS-70817]
- 当同时从 Citrix Cloud 收到多条授权消息时，在更新 Redis 缓存时会出现争用情况。在这种情况下，一条授权消息被更新到缓存中，剩下的则丢失。此问题现已修复，更新缓存中的所有授权消息。[CAS-70823]

2022 年 **9** 月 **13** 日

Sharelink 控制面板增强功能

Sharelink 控制面板经过了改进，增加了摘要和详细视图。摘要视图包括最活跃的股票和风险最高的股票。详细视图向管理员提供了更多信息，包括创建者的属性、活动计数、身份验证类型、权限、共享类型和内容。管理员可以根据需要向下钻取和进一步筛选，并更改/提供时间范围以查看感兴趣的数据。

有关详细信息，请参阅 共享链接控制板。

2022 年 **9** 月 **9** 日

不可能的旅行 **RI** 增强版

不可能的旅行风险指示器已得到增强，可以报告客户端 IP 地址的注册组织和路由类型。这些新字段在用户时间轴指示器详细视图和发送给 SIEM 的指示器详细信息中都可用。

有关默认策略的更多信息，请参阅以下文章：

- 持续的风险评估。
- 策略和操作

2022 年 **8** 月 **19** 日

启用 **VDA** 打印遥测

在 Citrix Apps and Desktops 中启动打印作业时，将触发名为 VDA.Print 的事件。VDA 打印事件也可在自助搜索和自定义风险指示器页面上找到。

- 自助搜索：您可以查看 VDA.Print 结果及其所有属性详细信息。
- 自定义风险指示器：通过 EventHub 为 VDA 打印遥测提供了新事件，也可以在自定义指示器中使用。您可以使用这些事件键/值对来配置自定义指示器触发器。

要启用打印遥测和将打印日志传输到 Citrix Analytics for Security，您需要创建注册表项并配置 VDA。这些打印日志提供有关打印活动的重要信息，例如打印机名称、打印文件名和打印副本总数。作为安全管理员，您可以使用这些日志来分析风险并调查您的用户。

有关详细信息，请参阅为 Citrix DaaS 启用打印遥测。

2022 年 8 月 18 日

已修复的问题

- 在“应用程序和桌面的自助式搜索”和“访问保障位置”控制面板下的“用户登录”页面中，Workspace 应用程序版本值在下载的 CSV 文件中填充为 **NA**（不适用），而该值在页面视图中可用。此问题现已修复。[CAS-70361]

2022 年 8 月 17 日

根据策略自定义最终用户电子邮件

现在，您可以根据策略自定义发送给最终用户的电子邮件的内容。具体而言，当您使用“请求最终用户响应”操作或对用户帐户（例如“注销用户”和“锁定用户”）执行中断性操作来创建策略时，应用该策略时发送给最终用户的电子邮件内容是可自定义的。

有关按策略自定义最终用户邮件的详细信息，请参阅 策略和操作。

2022 年 8 月 11 日

在常见问题解答文章下已添加有关访问保障 - 地理位置的新问题。有关更多详细信息，请参阅常见问题解答。

已修复的问题

- 查看所有通知按钮会将管理员重定向到有错字的每周电子邮件链接 `https://citrix.cloud.com/notifications`。[CAS-69236]

2022 年 6 月 17 日

默认情况下，为新的付费权利启用数据处理

以前，拥有 Citrix Analytics for Security 的新付费授权的客户必须在特定数据源的站点卡中开启数据处理，才能开始处理这些数据源的数据。

在此版本中，当配置 Citrix Analytics for Security 的新付费权限时，以下 Citrix Cloud 服务的数据处理功能默认处于开启状态：

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

有关详细信息，请参阅 入门。

2022 年 6 月 9 日

已修复的问题

- 由 Azure AD 身份保护和 Microsoft Defender for Endpoint 生成的 Microsoft Graph 风险指示器可能会在 Security Analytics 中多次显示。此问题现已修复。[CAS-66593,CAS-66731]

2022 年 6 月 2 日

已修复的问题

- 在策略的自助搜索中，在搜索查询中选择 策略名称 维度以筛选事件时，会建议无效策略列表以及用于 Security Analytics 的有效策略。[CAS-66838]
- 来自 Windows Citrix Receiver 的 **File.Download** 事件的下载文件大小在自助搜索中显示不正确。此问题浮出水面，因为实际值以 KB 为单位，并且 UI 将该值视为字节，导致向用户显示错误的值。[CAS-67105]

2022 年 5 月 24 日

为 **Content Collaboration**、**Citrix DaaS** 和 **Citrix Virtual Apps and Desktops** 以及网关数据源推出不可能的差旅风险指示器

如果用户从相距太远而无法在经过的时间内旅行的两个位置登录，Citrix Analytics 会将此活动检测为不可能的出行情景，并触发不可能旅行风险指示器。有关不可能旅行风险指示器的更多信息，请参阅以下文章：

- Citrix Content Collaboration 风险指示器

- Citrix Gateway 风险指示器
- Citrix Virtual Apps and Desktops 和 Citrix DaaS 风险指示器

2022 年 5 月 17 日

Virtual Apps and Desktops 重命名为 Apps and Desktops

在 Security Analytics 控制面板和报表以及由 Security Analytics 发送到 SIEM 服务的数据中，所有 Virtual Apps and Desktops 标签现在都更新为应用程序和桌面，以与更名的产品名称保持一致。

例如，在数据源页面上，Virtual Apps and Desktops 标签被重命名为 Apps and Desktops。

应用程序和桌面标签表示组织中的 Citrix 本地 Citrix Virtual Apps and Desktops 以及 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）。

已修复的问题

Citrix Analytics 不会自动发现与您的 Citrix Cloud 帐户关联的 Citrix DaaS Cloud Monitor 或 Director 站点。[CAS-66801]

2022 年 4 月 5 日

新增功能

Secure Workspace Access 已重命名为 Secure Private Access

在 Analytics 控制板和报告中，所有 **Secure Workspace Access** 标签现在都更新为 **Secure Private Access**，以便与重新命名的产品名称保持一致。

例如，在数据源页面和自助搜索页面上，**Secure Workspace Access** 标签被重命名为 **Secure Private Access**。

2022 年 3 月 21 日

已修复的问题

- 在“创建风险指示器”页面中，如果搜索查询的先前条件包含用空格分隔的维度值，则维度和运算符的自动建议将不起作用。

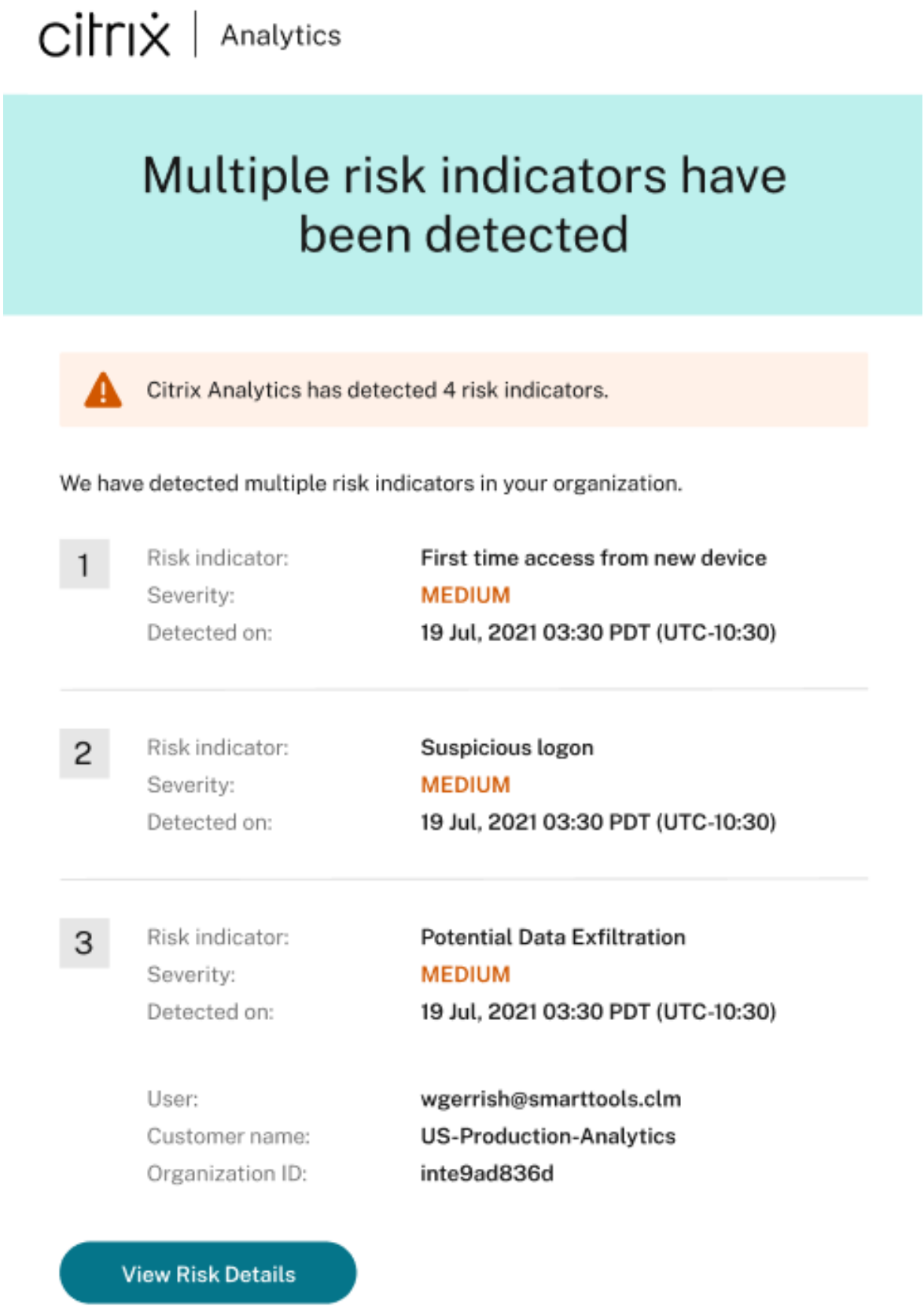
  例如，在以下查询中，将城市选择为 San Jose 后，自动建议将停止运行。此问题现已修复。[CAS-64126]

2022 年 **3** 月 **10** 日

新增功能

通知管理员电子邮件增强功能

- 通知 管理员操作的电子邮件通知 现在提供与触发的策略关联的多个风险指示器的详细信息。
- 您可以查看与策略关联的每个风险指示器的名称、严重性级别和触发日期。
- 单击 查看风险详细信息 可在 Citrix Analytics 中打开用户时间轴页面并查看触发策略的最新风险指示器。在用户时间轴页面上，您还可以查看为用户触发的所有风险指示器。



有关 通知管理员操作的详细信息，请参阅 策略和操作。

已修复的问题

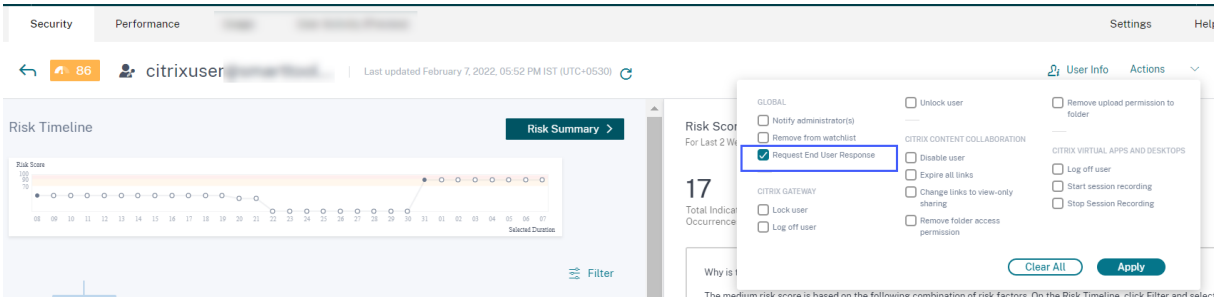
Citrix Analytics 无法从 Secure Workspace Access 数据源接收用户事件。因此，您不会在相应的自助搜索页面中看到用户事件。此外，您无法为 Secure Workspace Access 数据源创建自定义风险指示器。[CAS-64619]

2022 年 **3** 月 **3** 日

新增功能

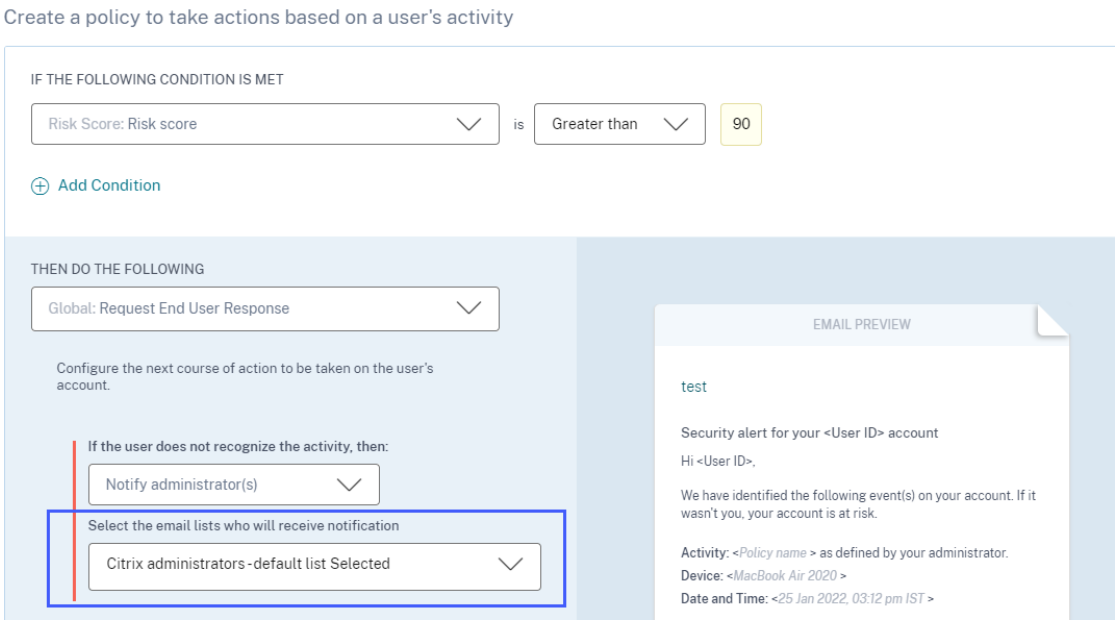
手动应用请求最终用户响应　以前，您只能通过创建策略对用户帐户应用“请求最终用户响应”操作。
在此版本中，您可以从用户时间轴上的“操作”(Actions) 列表中选择操作，然后手动将此操作应用于风险指示器。

有关操作以及如何手动应用操作的更多信息，请参阅 策略和操作。

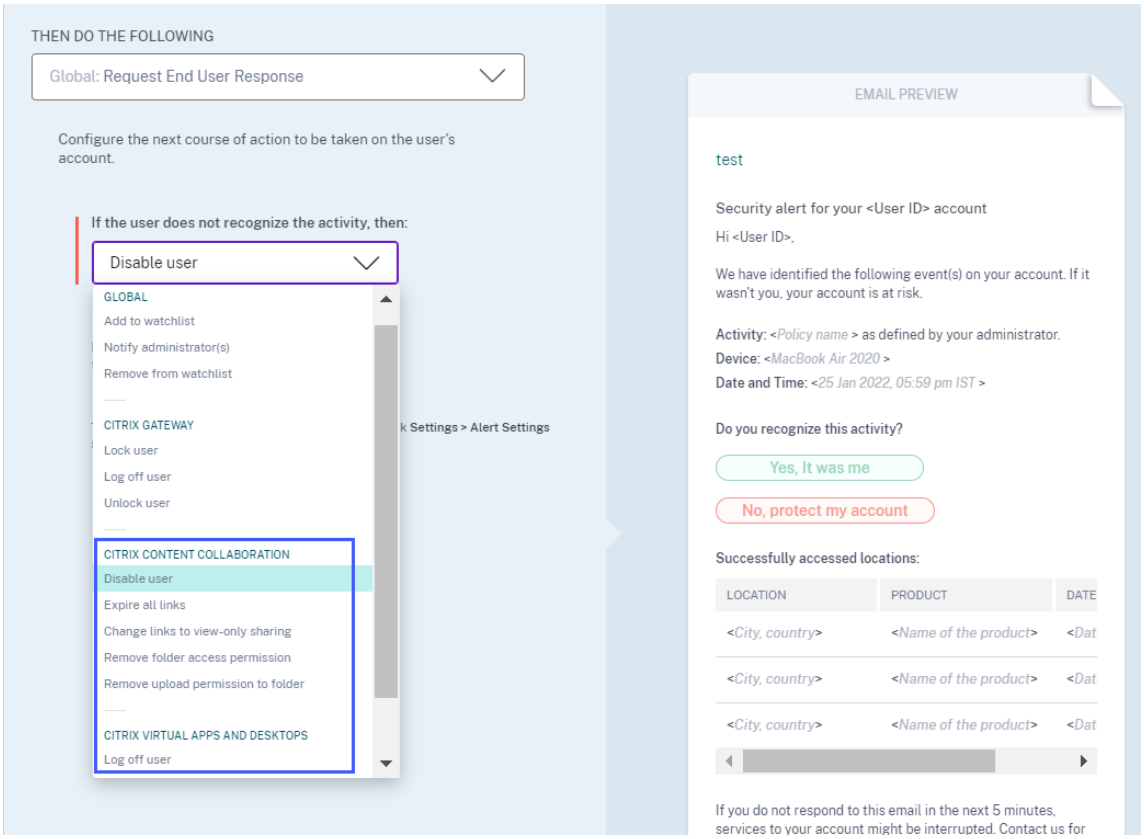


请求针对策略的最终用户响应增强功能　使用“请求最终用户响应”操作创建策略时，您会看到以下增强功能：

- 选择“通知管理员”作为下一个操作后，您现在可以查看默认的电子邮件通讯组列表和已创建的电子邮件通讯组列表，供您选择。



- 现在，您可以从 Citrix Content Collaboration 或 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 中选择一个操作作为下一个操作。以前，您只能选择全局操作或 Citrix Gateway 操作之一。



有关操作的详细信息，请参阅 策略和操作。

2022 年 2 月 23 日

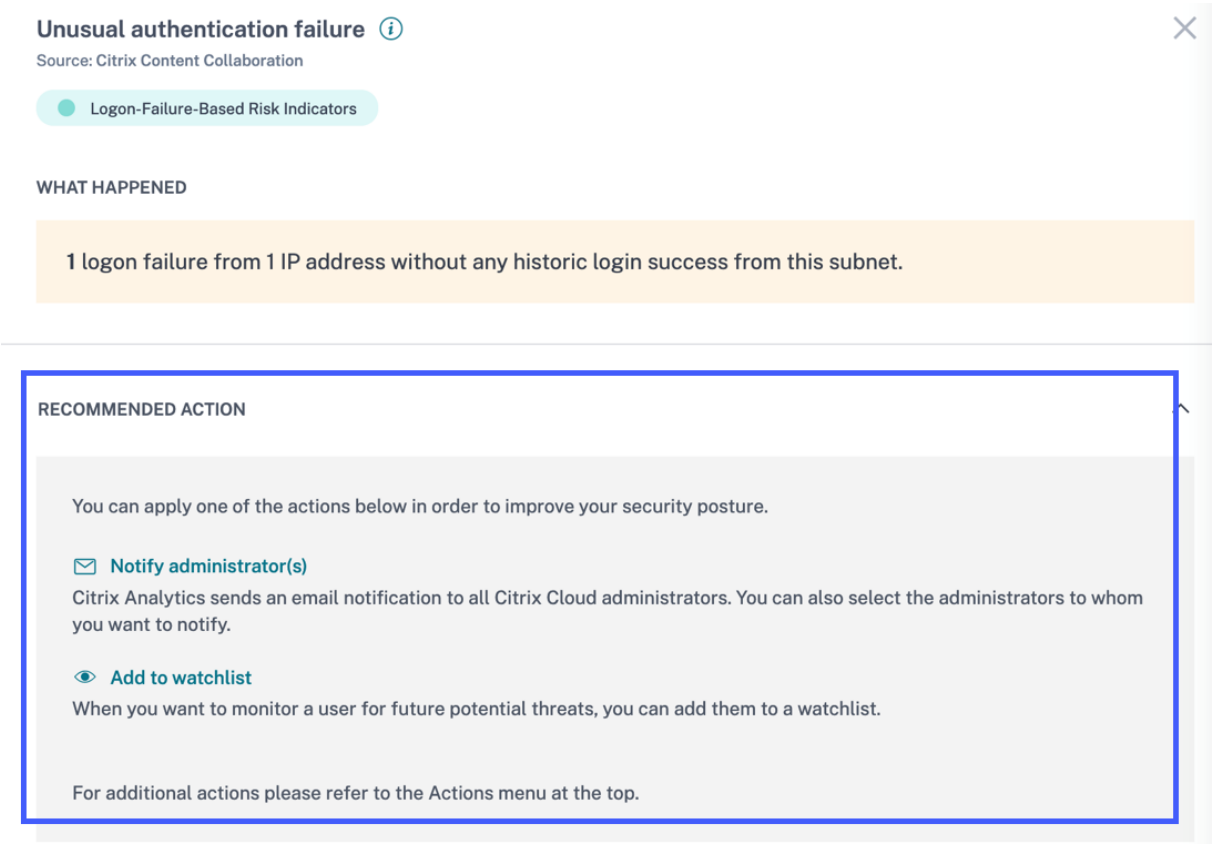
新增功能

针对风险指示器的建议操作　Citrix Analytics 建议您在为用户触发以下风险指示器时应用通知管理员、添加到监视名单和创建策略等操作：

- 异常身份验证失败（Content Collaboration 数据源）
- 异常身份验证失败 （网关数据源）
- 可疑登录 （Citrix Virtual Apps and Desktops 以及 Citrix DaaS 数据源）

当您转到用户时间线并选择风险指示器时，您可以在“建议的操作”部分中查看所有 建议的操作。

例如，在异常身份验证失败风险指示器中，您可以查看以下建议的操作：



此功能提供指导，指导您根据用户构成的风险的严重程度选择可以采取的措施。但是，您也可以采取建议列表之外的适当措施，具体取决于您的风险分析。

已修复的问题

- 如果您的组织已加入位于 亚太地区南部 主区域的 Citrix Cloud，则 Citrix Analytics 可能不会从身份验证数据源接收用户事件。因此，您可能不会在相应的自助搜索页面中看到用户事件。此问题已修复。[CAS-62300]

2022 年 2 月 17 日

新增功能

改进了 **Citrix Virtual Apps and Desktops** 和 **Citrix DaaS** 数据源的数据收集和报告　在此版本中，您将看到以下更改：

- 改进了来自 Citrix Workspace 应用程序客户端和 Citrix Monitor 服务的数据收集、关联和事件报告。
- 改进了从用户和客户端版本接收的事件的质量，可用于自助搜索、自定义风险指示器和整体风险检测。

支持 **Content Collaboration** 中的会话事件和应用程序事件的上下文模板　现在，在自助搜索页面上，您只能查看与文件、文件夹、会话、共享和用户事件关联的相关字段的详细信息。事件的不适用字段将被删除。

例如，您可以查看 `File.Copy` 事件的以下详细信息：

- 文件 ID
- 文件副本 ID
- 文件路径
- 目标文件路径
- 流 ID
- 区域 ID

这些详细信息可在风险调查和分析与风险行为相关的用户帐户时为您提供帮助。您可以深入查看看似有风险的事件的特定属性。

有关这些字段的详细信息，请参阅 Content Collaboration 的自助搜索。

2022 年 2 月 10 日

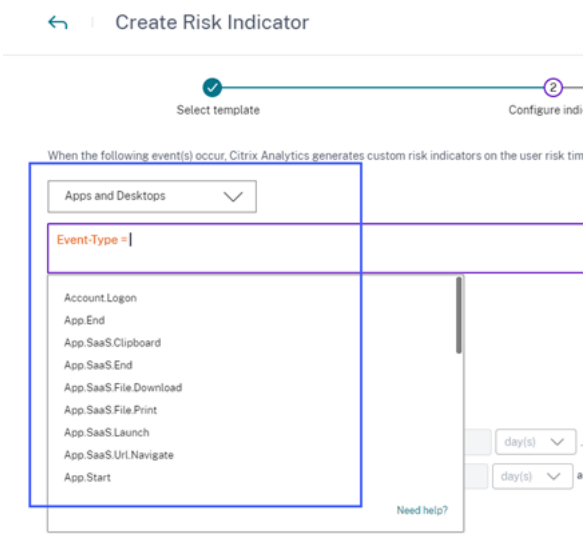
新增功能

自定义风险指示器中维度的自动建议值　在自定义风险指示器页面中，当您在条件栏中选择维度和有效运算符时，将自动显示该维度的值。从自动建议列表中选择一个值，或者根据您的用例手动输入值。键入值时，系统会自动建议记录中可用的匹配值。

为维度建议的值列表要么是数据库中预定义的（已知值），要么基于历史事件。

例如，当您选择维度 `Event-Type` 和赋值运算符时，系统会自动建议已知值。您可以根据需要选择一个值。

有关详细信息，请参阅自定义风险指标。



2022 年 **2** 月 **9** 日

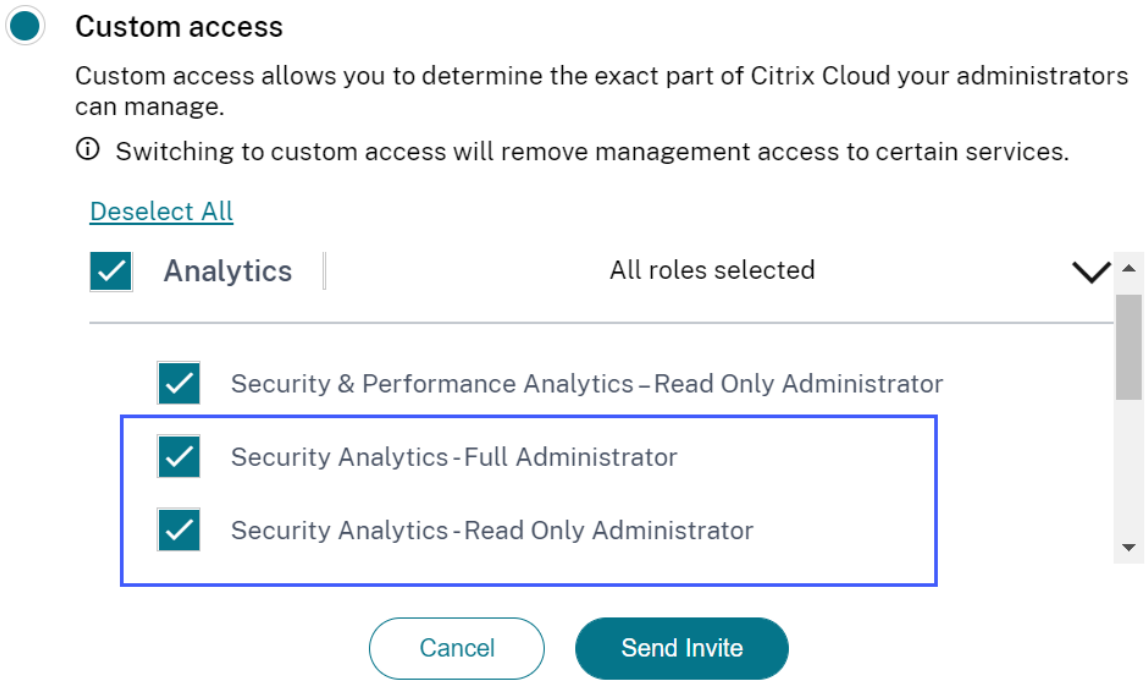
新增功能

管理员的新自定义角色　作为具有完全访问权限的 Citrix Cloud 管理员，您可以邀请其他管理员来管理组织中的 Security Analytics。现在，您可以将以下自定义角色分配给受邀的管理员：

- Security Analytics - 完全权限管理员
- Security Analytics - 只读管理员

使用自定义角色，您可以向管理员提供只读或完全访问权限，并允许他们管理 Security Analytics 的各种功能。

有关这些自定义角色的访问权限的更多信息，请参阅 管理 Security Analytics 的管理员角色。



支持自定义访问管理员的电子邮件通知　如果您是具有管理 Security Analytics 的自定义访问权限（只读或完全访问权限）权限的 Citrix Cloud 管理员，您现在会收到以下通知：

- 关于组织中检测到的安全风险的每周通知。有关详细信息，请参阅每周电子邮件通知。
- 手动应用“通知管理员”操作或由策略触发时有关风险指示器的通知。有关详细信息，请参阅 策略和操作。

2022 年 1 月 28 日

新增功能

为 **Content Collaboration** 和网关数据源引入可疑登录风险指示器　Citrix Analytics for Security 现在可基于多种上下文因素检测本质上可疑的用户登录，例如：

- 就用户和组织历史记录而言，该位置被视为不寻常
- 就用户和组织历史记录而言，该设备被视为异常
- 就用户和组织历史而言，该网络被认为是不寻常的
- 根据 IP 威胁情报馈送，IP 地址被视为可疑

当用户基于这些因素的组合从可疑环境中登录时，将触发风险指示器。

此风险指示器取代了与 Citrix Content Collaboration 和 Citrix Gateway 数据源关联的异常位置访问风险指示器。任何基于 异常位置访问风险指示器的 现有策略都会自动链接到新的风险指示器- 可疑登录。

有关风险指标的更多信息，请参阅可疑登录-Content Collaboration 和可疑登录 - Gateway。

有关风险指示器架构的详细信息，请参阅适用于 SIEM 的 Citrix Analytics 数据格式。

2022 年 1 月 20 日

新增功能

Microsoft Azure Active Directory 集成　您现在可以将 Azure Active Directory 与 Citrix Analytics for Security 连接起来，以便：

- 将用户详细信息和用户组从组织的域导入到 Citrix Analytics for Security。
- 使用职位、组织、办公地点、电子邮件和联系方式等其他详细信息来丰富用户档案，这有助于您进行风险调查和分析。

有关详细信息，请参阅 Azure Active Directory 集成。

2022 年 1 月 18 日

新增功能

支持对所有 **Content Collaboration** 风险指示器执行共享链接操作　以前，您可以在以下与 Content Collaboration 服务关联的基于共享链接的风险指示器上应用共享链接操作 - 终止所有链接和将链接更改为仅查看共享：

- 匿名敏感分享链接下载
- 分享链接下载量过多
- 过多的文件共享

在此版本中，您现在可以对以下与 Content Collaboration 服务关联的基于用户的风险指示器应用共享链接操作：

- 从不寻常的位置访问
- 过度访问敏感文件
- 文件上载过多
- 文件下载过多
- 删除过多的文件或文件夹
- 检测到恶意软件文件
- 怀疑勒索软件活动
- 异常的验证失败

您还可以对与 Content Collaboration 服务关联的自定义风险指示器应用共享链接操作。

有关操作和风险指示器的更多信息，请参阅以下文章：

- 策略和操作
- Content Collaboration 风险指示器
- 自定义风险指示器

与 **SIEM** 的集成现已正式推出　您可以将 Citrix Analytics for Security 与 Security Information and Event Management (SIEM) 服务集成，并将用户数据从 Citrix IT 环境导出到 SIEM。该集成可帮助您关联从各种来源收集的数据，并全面了解组织的安全性。

目前，您可以将 Citrix Analytics for Security 与以下服务集成：

- Splunk
- Microsoft Sentinel
- Elasticsearch
- 使用基于 Kafka 或 Logstash 的数据连接器提供的其他 SIEM 服务

有关详细信息，请参阅 安全信息和事件管理 (SIEM) 集成。

2021 年 **12** 月 **23** 日

新增功能

共享链接风险指示器增强功能　进行了以下增强：

- 现在，您可以使用 匿名敏感共享链接下载 风险指示器创建策略。
- 匿名敏感共享下载 风险指示器被重命 名为匿名敏感共享链接下载，以将其区分为共享链接风险指示器。
- 过度下载 风险指示器被重命名为 共享链接下载过多，以区分它作为共享链接风险指示器，并将其与基于用户的文件下载过多 风险指示器区分开来。

有关详细信息，请参阅 Citrix 共享链接风险指示器。

2021 年 **12** 月 **21** 日

新增功能

向非 **Citrix Cloud** 管理员发送有关风险指示器的通知　现在，您可以通过“通知管理员”操作 通知组织中的非 **Citrix Cloud** 管理员。

要通知这些管理员，请创建电子邮件通讯组列表。从连接到 Citrix Cloud 的外部域或直接使用其电子邮件地址在电子邮件通讯组列表中选择管理员。应用“通知管理员”操作时，选择包含非 Citrix Cloud 管理员的电子邮件通讯组列表。

有关详细信息，请参阅 电子邮件通讯组列表。

2021 年 12 月 20 日

新增功能

向 **Content Collaboration** 用户发送用户回复通知　除了 Active Directory 用户之外，您现在还可以将“请求最终用户响应”操作应用于 Content Collaboration 用户。

当 Citrix Analytics 检测到用户的 Citrix 帐户中存在任何异常活动时，此操作会向用户发送电子邮件通知。有关“请求最终用户响应”操作的更多信息，请参阅 策略和操作。

访问控制已重命名为 **Secure Workspace Access**　现在，在 **Security Analytics** 控制板和报表中，所有访问控制标签都将更新为 **Secure Workspace Access**，以与重新命名的产品名称保持一致。

例如，在“数据源”页面、“自助搜索”页面和“策略”页面上，“访问控制”标签被重命名为 Secure Workspace Access。

已修复的问题

- 对于应用程序和桌面数据源，当您将搜索报告下载为 CSV 文件时，CSV 文件中的某些字段值会显示为不可用 (N/A)，尽管它们的值可用。例如，自助服务搜索 页面上会显示 `Download File Name`、`Session Launch Type` 和 `Workspace App Version` 等字段的值，但在下载的 CSV 文件中，您会看到这些值不可用 (N/A)。此问题现已修复。[CAS-62299]

2021 年 12 月 9 日

新增功能

使用模板轻松创建自定义风险指示器　现在，您可以根据自己的用例选择模板并创建自定义风险指示器。这些模板通过提供预定义的查询和参数来指导您。在创建自定义风险指示器时，它可以简化您的工作。

有关详细信息，请参阅自定义风险指标。

2021 年 12 月 7 日

已修复的问题

- 在 Citrix Analytics for Security 上，您不会收到使用 2021 年 9 月发布的 Citrix Secure Browser 用户的事件。存在此问题的原因是，主机名跟踪策略在 2021 年 9 月发布的 Citrix Secure Browser 中不可见，因此无法启用与 Citrix Analytics for Security 集成。此问题现已修复。[CAS-62254]

2021 年 12 月 2 日

新增功能

检测到恶意软件文件风险指示器　现在，当用户在 Content Collaboration 中上载受感染文件时，您可以收到警报。

风险指示器检测到受恶意软件（如特洛伊木马、病毒或任何其他恶意威胁）感染的文件。它提供了对恶意文件的详细信息的可见性，例如文件所有者、病毒名称和文件位置。

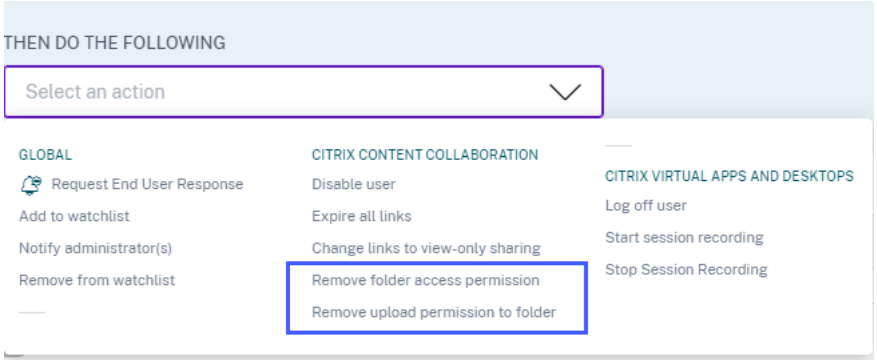
与检测到的恶意软件文件风险指示器相关的风险因素是基于文件的风险指示器。

有关风险指示器和可以应用的操作的详细信息，请参阅 检测到恶意软件文件风险指示器。

针对 **Content Collaboration** 数据源的新操作　当用户触发“检测到恶意软件文件”风险指示器时，您可以应用以下操作：

- 删除文件夹访问权限。您可以阻止上载受感染文件的用户的访问权限。用户无法访问上载受感染文件的文件夹。
- 移除文件夹的上载权限。您可以阻止上载受感染文件的用户的上载权限。用户无法将文件上载到已上载受感染文件的文件夹。

有关 Content Collaboration 操作的详细信息，请参阅 策略和操作。

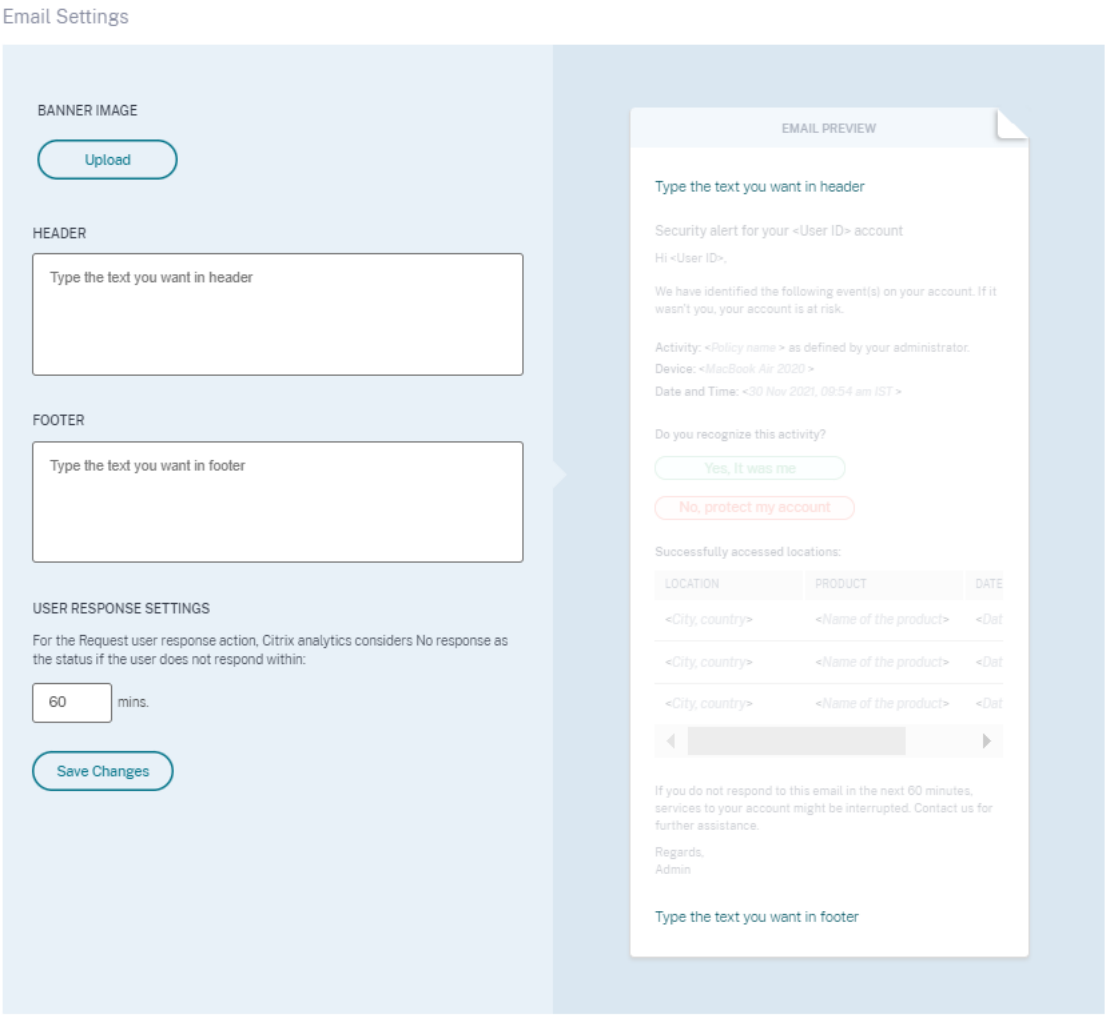


2021 年 11 月 29 日

新增功能

用户通知的电子邮件设置增强　作为管理员，您现在可以在用户回复电子邮件模板中添加横幅图像、页眉和页脚文本。这些字段增强了电子邮件的合法性，从而增加了用户对电子邮件的关注和回复。

有关详细信息，请参阅最终用户电子邮件设置。



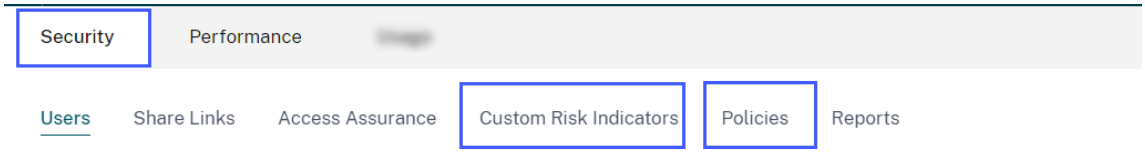
2021 年 11 月 26 日

新增功能

自定义风险指示器和策略菜单更改　以下功能的导航链接已更新：

- 自定义风险指示器：通过单击 安全 > 自定义风险指示器使用此功能。

- 策略：通过单击 安全 > 策略使用此功能。



2021 年 11 月 25 日

新增功能

安全信息和事件管理 (SIEM) 集成增强功能

> 注意
>
> 此集成处于预览版。

现在，您可以将 Citrix Analytics for Security 与以下 SIEM 服务集成：

- Microsoft Sentinel
- 使用可视化服务（例如 Kibana）和像 LogRythm 这样的 SIEM 服务进行 Elasticsearch
- 使用 Logstash 数据收集引擎的任何其他 SIEM 服务

根据您的业务需求，将用户的数据从 Citrix Analytics for Security 导入到 SIEM 服务。这种集成使您的安全运营团队能够关联、分析和搜索组织中 SIEM 服务中不同日志中的数据，从而帮助他们识别并快速修复安全风险。

有关详细信息，请参阅 安全信息和事件管理 (SIEM) 集成。

2021 年 11 月 9 日

已修复的问题

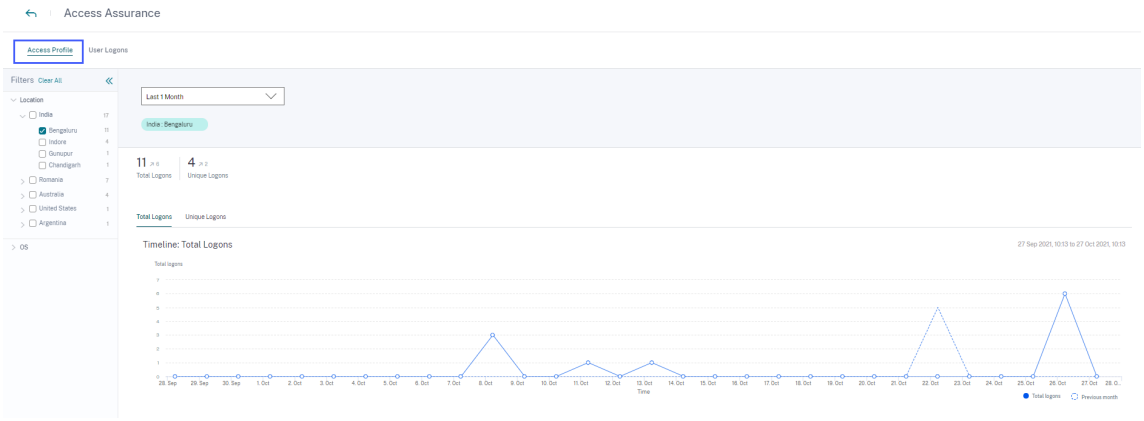
- 在少数租户上，用户策略不起作用。当虚拟应用程序的警报具有域的空字符串值时，就会出现此问题。此问题现已修复。[CAS-60920]

2021 年 11 月 2 日

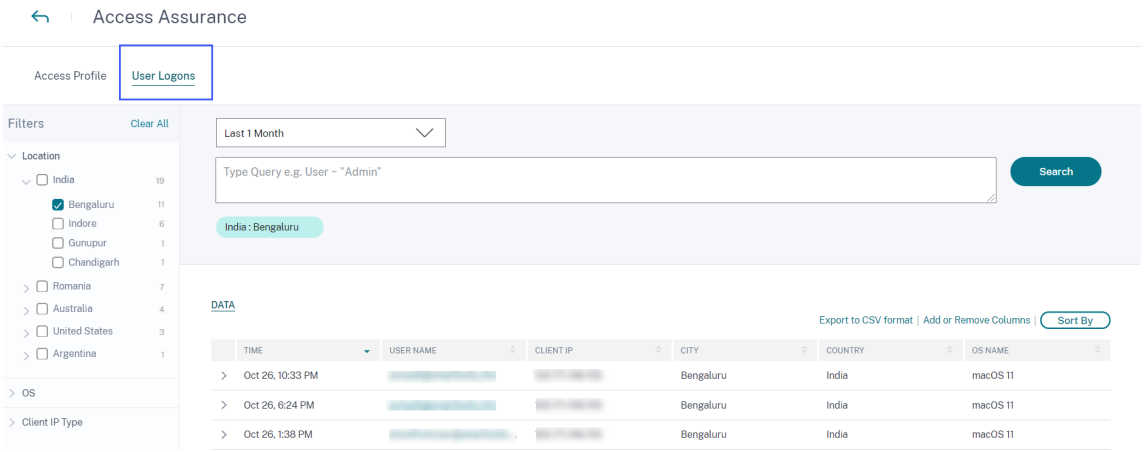
新增功能

查看 Citrix Virtual Apps and Desktops 和 Citrix DaaS 用户的访问配置文件和登录详细信息　在访问保证位置控制板上，您可以查看访问配置文件以及已登录虚拟应用程序和虚拟桌面的用户的登录详细信息。这些信息在威胁调查和分析过程中有所帮助。

- “访问配置文 件”页面提供了用户从所选位置进行的访问的摘要。您可以查看总用户和唯一用户登录的趋势分析和最高访问权限事件。



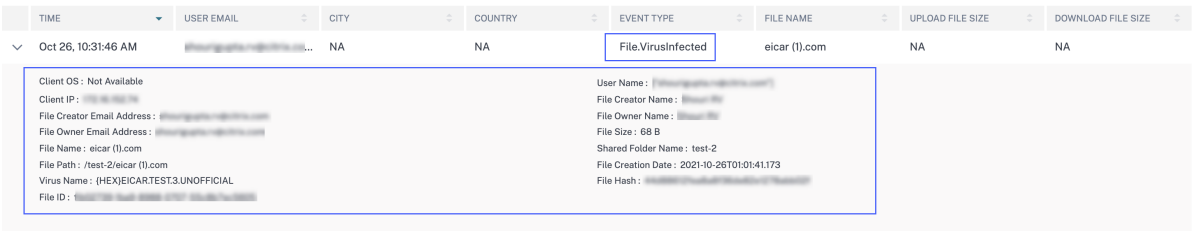
- “用户登录”页面提供了用户从所选位置登录到虚拟应用程序和虚拟桌面的详细信息。



有关详细信息，请参阅 访问保证位置控制板。

在 **Content Collaboration** 的自助搜索页面上查看恶意软件日志　在 Content Collaboration 的自助服务页面上，您现在可以查看恶意软件事件 `File.VirusInfected` 及其相关日志。当 Content Collaboration 用户上载感染了恶意软件的文件时触发此事件。

有关详细信息，请参阅 Content Collaboration 的自助搜索



已修复的问题

- 在 Citrix Analytics 中处理事件时，一些 Content Collaboration 用户被错误地设置为非员工。因此，这些用户不会被标识为已发现的用户。此问题现已修复。[CAS-59608]

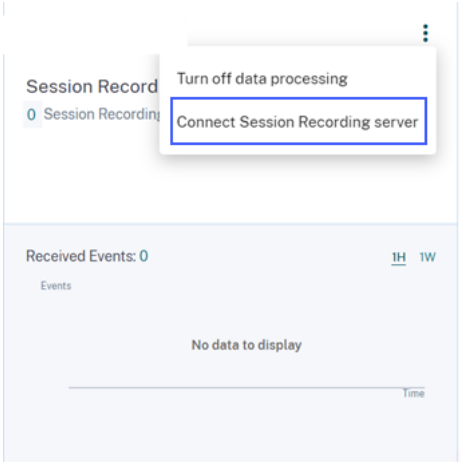
2021 年 10 月 20 日

新增功能

Session Recording Server 集成　对于 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 部署，您现在可以将 Session Recording Server 配置为将用户事件发送到 Citrix Analytics for Security。对这些用户事件进行处理，以便为用户的行为提供切实可行的见解。

在“数据源”**>**“安全性”页面上，转到 **Virtual Apps and Desktops** 站点卡片。在 **Session Recording** 站点卡上，单击垂直省略号 (⋮)，然后选择 连接 **Session Recording Server**。

有关详细信息，请参阅连接到 Session Recording 部署。



2021 年 10 月 19 日

新增功能

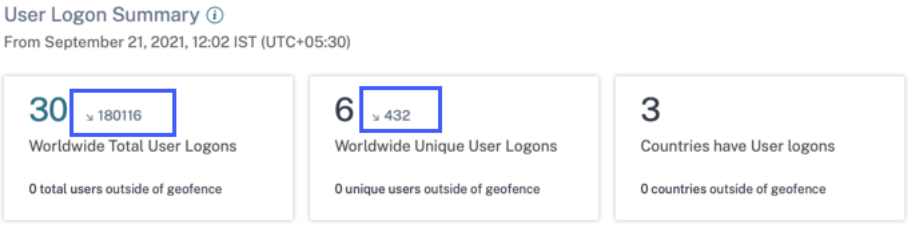
通知管理员邮件模板增强　管理员在应用“通知管理员”操作后收到的电子邮件通知得到了增强，可以更好地洞察用户的风险事件。

- 通知现在提供有关触发的风险指示器或所应用策略的详细信息。例如，您可以查看默认和自定义风险指示器的严重性和触发时间。改进了内容结构以提高可读性。
- 管理员现在可以直接从电子邮件通知访问用户时间线，并查看有关风险事件的详细信息。
- 通知中添加了反馈选项。此选项有助于收集管理员的回复，并根据响应不断改进通知的内容。

有关 通知管理员操作的详细信息，请参阅 策略和操作。

用户登录摘要增强功能

- 现在，您可以查看全球用户登录总数和全球唯一用户登录次数的用户登录数的上升或下降趋势。



- 唯一登录位置 表中的 **DEVIATION** 列显示了特定位置的唯一用户登录次数向上或向下变化。

这些指示器可帮助您了解用户登录次数与上一时期相比有何变化（正面或负面）。它提供了用户与您的 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 部署之间的交互的可见性。

有关详细信息，请参阅 访问保证位置控制板。

已修复的问题

- 在 访问保障位置 控制板上，当没有 用户从地理围栏区域之外登录时，用户登录摘要 卡无法显示用户登录量度（全球用户登录总数、全球唯一用户登录次数和国家/地区有用户登录）。此问题现已修复。[CAS-59595]

2021 年 **10** 月 **1** 日

新增功能

查看自助搜索 **Content Collaboration** 的审核日志　在 Content Collaboration 的自助搜索中，您现在可以查看审核日志。这些日志提供了有关 Content Collaboration 管理员对用户帐户应用的权限和操作的见解。使用这些数据，

您可以验证 Content Collaboration 管理员是否对其用户帐户采取了有效的操作。作为安全管理员，它可以在风险调查和分析期间为您提供帮助。

有关审核日志的详细信息，请参阅 Content Collaboration 的自助搜索。

已修复的问题

使用 Azure AD 登录 Citrix Cloud 的管理员将无法访问 Citrix Analytics Service，如果上一个过期的会话 ID 与新的会话 ID 一起出现。此问题现已修复。[CAS-59385]

2021 年 9 月 29 日

新增功能

访问保障位置控制板现已正式推出　该控制板可让您查看您的 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 用户的位置。您可以通过启用地理围栏来识别位置异常的用户，并应用适当的操作来防止任何威胁。

要查看控制板，请单击“安全”**>**“访问保障”。选择要查看位置详细信息的时间段。

有关详细信息，请参阅 访问保证位置控制板。

2021 年 9 月 15 日

新增功能

自定义风险指示器增强

- 触发自定义风险指示器时，它会立即显示在 用户时间轴 上。但是，用户的风险摘要和风险评分会在几分钟后（大约 15 至 20 分钟）更新。
- 如果在用户时间轴上修改现有自定义风险指示器的状况、风险类别、严重性和名称等属性，您仍然可以查看先前为用户触发的自定义风险指示器（使用旧属性）的出现次数。
- 如果删除自定义风险指示器，则仍然可以在用户时间轴上查看先前为用户触发的自定义风险指示器的出现次数。

有关详细信息，请参阅自定义风险指标。

2021 年 9 月 14 日

新增功能

引入可疑登录风险指示器　Citrix Analytics for Security 现在可基于多种上下文因素检测本质上可疑的用户登录，例如：

- 就用户和组织历史记录而言，该位置被视为不寻常
- 就用户和组织历史记录而言，该设备被视为异常
- 就用户和组织历史而言，该网络被认为是不寻常的
- 根据 IP 威胁情报馈送，IP 地址被视为可疑

当 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 用户基于这些因素的组合从可疑环境中登录时，会触发风险指示器。

此风险指示器替换了与 Citrix Virtual Apps and Desktops 数据源关联的从异常位置访问风险指示器。任何基于 异常位置访问风险指示器的 现有策略都会自动链接到新的风险指示器- 可疑登录。

有关风险指示器的详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 风险指示器。

SIEM 消息增强　Citrix Analytics for Security 现在会将可疑登录风险指示器的架构详细信息发送到 SIEM 服务。您可以查看指示器摘要的架构和可 疑登录 风险指示器的事件详细信息。有关详细信息，请参阅适 用于 SIEM 的 Citrix Analytics 数据格式。

已修复的问题

- 对于应用程序和桌面自助搜索，下载的 CSV 文件中缺少客户端 IP 值。此问题现已修复。[CAS-58426]

2021 年 **8** 月 **19** 日

新增功能

推出适用于 **Splunk** 的 **Citrix Analytics** 应用

> 注意
>
> 该应用程序处于预览中。

适用于 Splunk 的 Citrix Analytics 应用程序使您能够在 Splunk 上以富有洞察力的控制板的形式查看从 Citrix Analytics for Security 收集的数据。控制板可让您深入了解用户的风险事件。您还可以将 Citrix Analytics 数据与从其他各种数据源收集的日志相关联。关联可帮助您查找事件之间的关系，并及时采取措施来保护您的 IT 环境。

要下载该应用程序，请转到 Splunkbase。在 Splunk 搜索头上安装应用程序。

有关详细信息，请参阅适用于 Splunk 的 Citrix Analytics 应用。

SIEM 的自定义风险指示器架构　在 SIEM 服务中，您现在可以查看为 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 创建的自定义风险指示器的架构。这些数据可帮助您深入了解组织的安全风险状况。

有关自定义风险指示器架构的更多信息，请参阅 适用于 SIEM 的 Citrix Analytics 数据格式。

支持将 **Citrix Director** 作为数据源　现在，您可以在 Citrix Director 上配置本地站点，以将事件发送到 Security Analytics。这些事件用于发现连接到 Security Analytics 的用户，并确定用户设备上安装的 Workspace 应用程序版本。

默认情况下，在发现站点之后启用数据处理。在 监视 卡上，您可以查看所有已连接的站点。

有关如何在 Director 上配置站点的详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源。

在访问保证位置控制板中支持地理围栏　现在，您可以使用控制板中的 地理围栏设置 来选择和启用地理围栏区域。启用地理围栏后，地图将显示地理围栏区域（国家/地区）以及用户从地理围栏外部和内部登录的情况。此功能使用在 地理围栏风险指示器之外启动的 **CVAD** 会话 来监视用户登录。

有关详细信息，请参阅 访问保证位置控制板。

用户页面上的 **Workspace** 应用程序状态　在 用户 页面上，您现在可以查看 Citrix Analytics 支持的 Citrix Workspace 应用程序客户端的状态。该页面显示以下状态：

- 支持
- 部分支持
- 不受支持
- 不可用
- 不活跃

该状态可帮助您识别用户使用的任何不受支持的客户端版本，并建议用户将其客户端升级到受支持的版本。受支持的客户端版本会将用户事件发送到 Citrix Analytics。

> 注意
>
> 要查看 Citrix Workspace 应用程序状态，必须加载 Citrix Director 数据源。否则，每个 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 用户的状态都显示为 非活动。

有关详细信息，请参阅用 户控制板。

支持 **IS EMPTY** 运算符　在创建自定义风险指示器时，您现在可以在条件中使用 **IS EMPTY** 运算符来检查空维度或空维度。

> 注意
>
> 该运算符仅适用于字符串类型的维度，例如应用程序名称、浏览器和国家/地区。

有关详细信息，请参阅自定义风险指标。

改进了风险评分　在用户的时间轴上，您现在可以查看用户的风险摘要。风险摘要提供有关与用户事件相关的风险因素的信息。风险因素可帮助您识别用户事件中的异常类型，并确定风险评分。以下是风险因素：

- 基于设备的风险指示器
- 基于位置的风险指示器
- 基于 IP 的风险指示器
- 基于登录失败的风险指示器
- 基于数据的风险指示器
- 基于文件的风险指示器
- 自定义风险指示器
- 其他风险指示器

在用户的时间轴上，您现在可以根据风险因素应用过滤器来查看用户事件。

有关详细信息，请参阅以下主题：

- Citrix 用户风险指示器
- 用户风险时间表和概况

2021 年 **7** 月 **29** 日

已弃用的功能

与 **Citrix Endpoint Management** 关联的已弃用操作　将从 Citrix Endpoint Management 数据源中删除以下操作。您不能再对风险指示器应用这些操作或使用这些操作创建策略。

- 锁定设备
- 通知 Endpoint Management 管理员
- 通知用户
- 吊销设备
- 擦除设备

在现有策略中，如果这些操作已在使用中，则它们将自动替换为“添加到监视名单”操作。您可以从监视名单中监视此类用户。

2021 年 7 月 14 日

新增功能

支持 IS NOT EMPTY 运算符　在创建自定义风险指示器时，您现在可以在条件中使用 **IS NOT EMPTY** 运算符来检查维度是否为空（不是空白）。

> 注意
>
> 该运算符仅适用于字符串类型的维度，例如应用程序名称、浏览器和国家/地区。

例如，以下条件会检测来自国家/地区值不为空的任何国家/地区的用户登录事件。换句话说，指定了国家/地区名称。

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

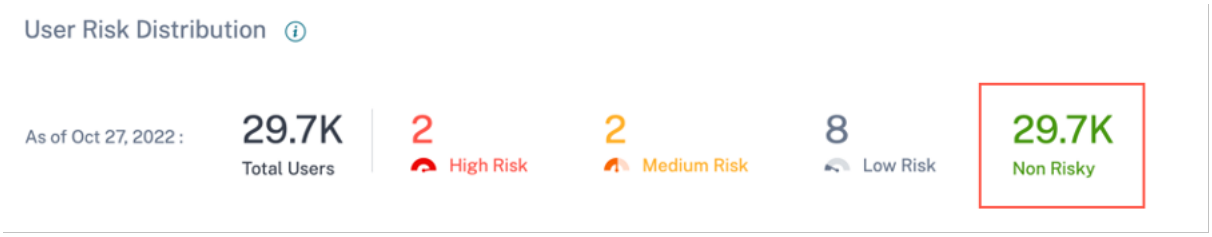
有关详细信息，请参阅自定义风险指标。

2021 年 7 月 6 日

新增功能

在“用户”控制板上查看非风险用户　在“用 户”控制面板上，您现在可以查看所选时间段内非风险用户的数量。根据所选期间的零风险评分，将这些发现的用户标识为非风险用户。单击“非风险用户”卡可查看所有具有零风险评分的用户。

有关详细信息，请参阅 用户控制板。

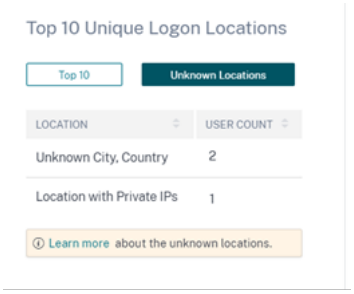


2021 年 7 月 1 日

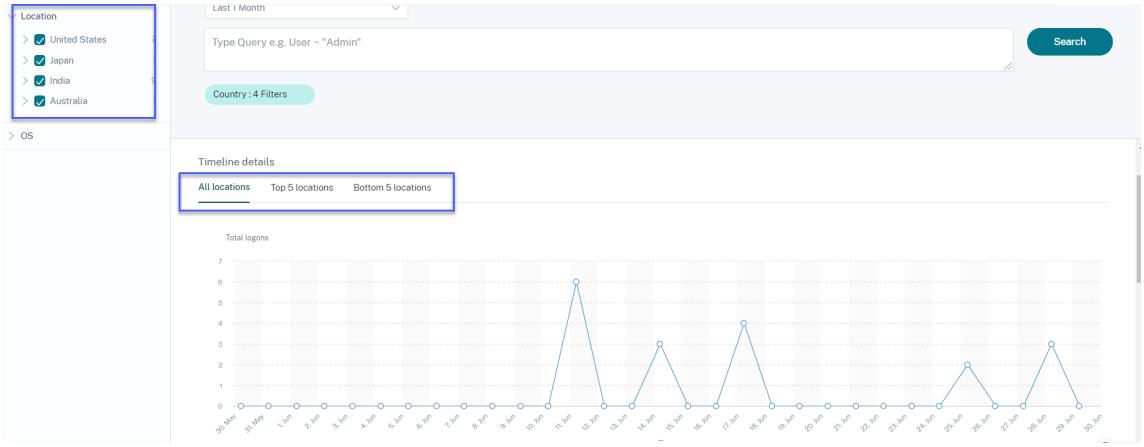
新增功能

访问保证位置控制板增强

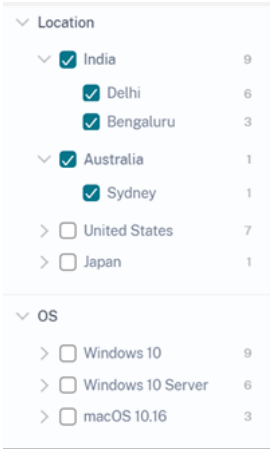
- 在“前 **10** 个唯一登录位置”表中，您可以查看来自未知位置的唯一用户登录次数。此列表是前 10 个唯一登录位置的子集。您还可以找到位置未知的原因以及获取用户位置的可能方法。



- 在“访问位置”页面上，如果选择多个位置，则可以查看和比较来自所有位置、前五个位置和最后五个位置的用户登录的时间轴详细信息。

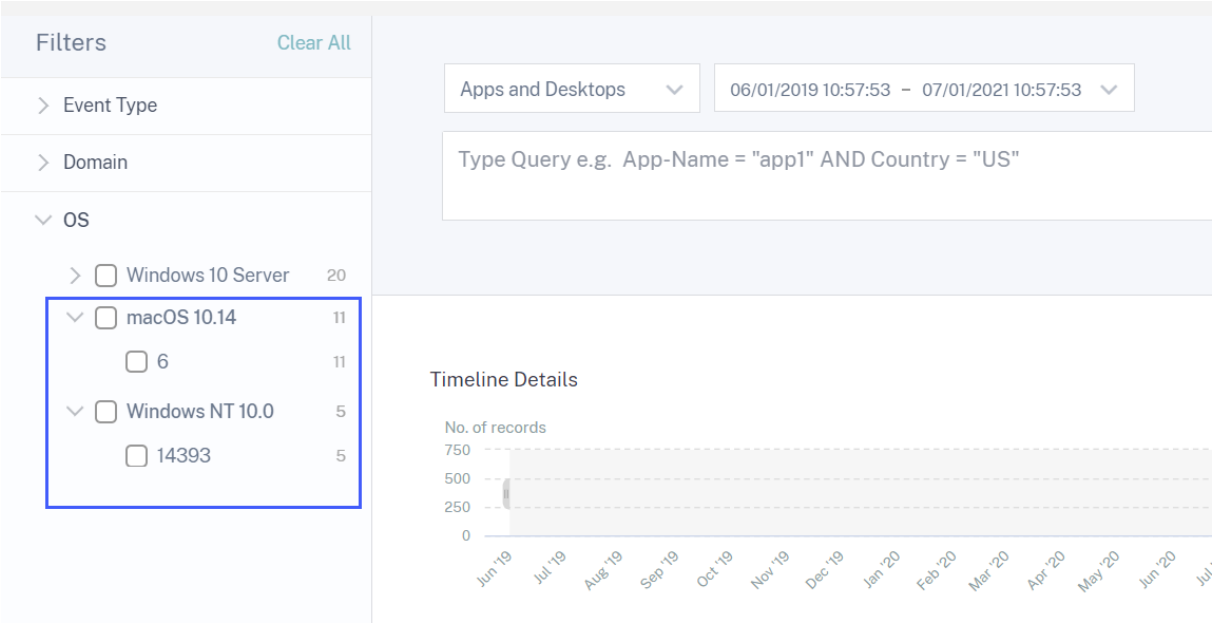


- 在“访问位置”页面上，您可以使用嵌套的方面，例如国家/地区及其城市、操作系统-主要版本和次要版本。这些方面使您能够以细粒度的方式过滤事件。



有关详细信息，请参阅 访问保证位置。

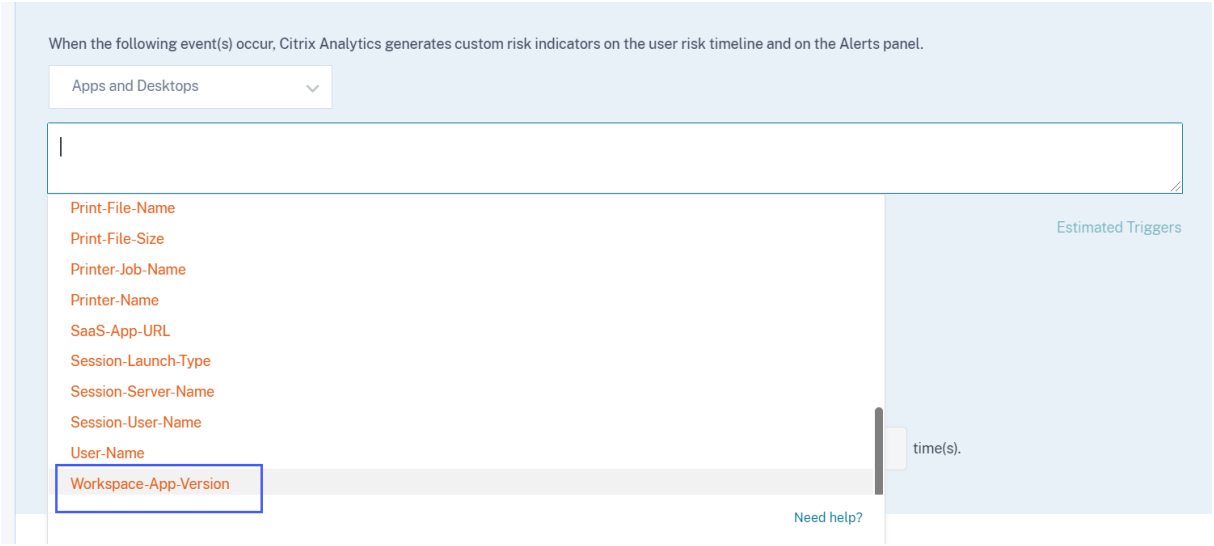
更新了 **Virtual Apps and Desktops** 的自助搜索中的操作系统方面　现在，您可以使用嵌套的操作系统方面过滤应用程序和桌面事件。选择与操作系统关联的主要版本和次要版本，然后以细粒度方式过滤事件。有关详细信息，请参阅应用程序和桌面的自助式搜索。



2021 年 6 月 30 日

新增功能

为应用程序和桌面添加了处于自定义风险指示器条件的 **Workspace** 应用程序版本　对于 应用程序和桌面 数据源，您现在可以在创建自定义风险指示器时使用 **Workspace App-Version** 维度来定义您的状况。有关维度的详细信息，请参阅应用程序和桌面的自助式搜索。



2021 年 6 月 23 日

新增功能

SIEM 消息增强　现在，以下字段已添加到风险指示器的架构中：

- `indicator_vector_name`-表示与风险指示器关联的风险载体。风险载体包括基于设备的风险指示器、基于位置的风险指示器、基于登录故障的风险指示器、基于 IP 的风险指示器、基于数据的风险指示器、基于文件的风险指示器和其他风险指示器。
- `indicator_vector_id`-与风险向量关联的 ID。ID 1 = 基于设备的风险指示器，ID 2 = 基于位置的风险指示器，ID 3 = 基于登录失败的风险指示器，ID 4 = 基于 IP 的风险指示器，ID 5 = 基于 IP 的风险指示器，ID 6 = 基于数据的风险指示器，ID 7 = 其他风险指示器，ID 999 = 不可用。

有关详细信息，请参阅适 用于 SIEM 的 Citrix Analytics 数据格式。

2021 年 6 月 7 日

新增功能

通知管理员操作的增强功能　当您将“通知管理 员”操作应用于风险指示器或使用该操作创建策略时，您现在可以选择接收有关用户风险行为的通知的管理员。有关操作的详细信息，请参阅 策略和操作。

添加了对仅查看共享操作的支持　如果用户过度共享文件，Citrix Analytics 会触发文 件共享过多 风险指示器。从用户的风险时间表中，您现在可以将“更改链接至仅查看共享”操作应用于“过多的文件共享 风险”指示器。您还可以在股份链接风险时间表上对特定的共享链接应用操作。此操作可防止其他用户下载、复制或打印与共享链接关联的文件。有关操作的详细信息，请参阅 策略和操作。

2021 年 5 月 18 日

新增功能

将默认风险指示器迁移到自定义风险指示器　以下默认风险指示器已迁移到预配置的自定义风险指示器。

默认风险指示器	数据源	预配置的自定义风险指示器
首次从新设备访问	Citrix Virtual Apps and Desktops 和 Citrix DaaS	CVAD-首次从新设备访问
首次从新 IP 访问	Citrix Gateway	网关-从新 IP 首次访问

随着这种迁移到自定义风险指示器，默认风险指示器和相关的计算机学习算法将被弃用。

根据以下预先配置的条件触发相应的自定义风险指示器：

- 当用户首次从新设备访问或至少 90 天未使用的现有设备时。
- 用户首次从新 IP 地址或至少 90 天未使用的现有 IP 地址登录时。

除了预配置的条件外，您现在可以为这些自定义风险指示器添加自己的条件，以识别 Citrix 环境中的威胁。通过此选项，您可以根据安全需求灵活配置自定义风险指示器。您还可以创建策略，对这些自定义风险指示器检测到的风险事件应用操作。

但是，在用户的时间表上，您仍然可以查看之前触发的默认风险指示器及其事件。

与这些默认风险指示器关联的策略将自动链接到相应的预先配置的自定义风险指示器。

有关详细信息，请参阅 预配置的自定义风险指示器和策略。

网关自助搜索的增强功能

- 事 件类型 过滤器现在重命名为 “记录类型”。选择以下记录类型之一以筛选事件-VPN_AI、VPN_IF 和 VPN_ST。
- 在 **DATA** 表中，展开用户事件的行以查看相应的事件类型。事件类型可以是以下类型之一-身份验证、ICA 文件或会话注销。

下表描述了记录类型与事件类型之间的关联。

记录类型	事件类型
VPN_AI	身份验证
VPN_IF	ICA 文件
VPN_ST	会话注销

有关详细信息，请参阅 网关的自助搜索。

已修复的问题

- 自定义风险指示器根据条件值的区分大小写而触发。例如，在允许列表中包含设备 ID 的用户事件中，您会看到以下行为：
  - 如果以小写字母输入 `Device-ID` 维度的值，则会触发自定义指示器。

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

  - 如果以大写字母为同一设备输入 `Device-ID` 维度的值，则不会触发自定义指示器。

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


此问题现已修复，无论条件值是否区分大小写，都会触发自定义风险指示器。

[CAS-50153]

2021 年 4 月 29 日

新增功能

自定义风险指示器的事件详情　在用户的风险时间表页面上，您现在可以查看触发自定义风险指示器的事件。以前，您只能查看自定义风险指示器的定义条件、描述和触发频率。单击 事件搜索 以查看与用户关联的事件的详细信息和风险指示器。
有关详细信息，请参阅自定义风险指标。

已修复的问题

- 即使管理员的访问权限从只读管理员更改为完全管理员，管理员也无法创建自定义风险指示器。[CAS-49628]

2021 年 4 月 16 日

新增功能

SIEM 消息增强　您可以查看风险指示器架构格式的以下增强功能：

- 客户端 IP 地址现在可用于所有批量风险指示器的模式中。以前，客户端 IP 地址仅适用于几个批量风险指示器：
  - EPA 扫描失败
  - 验证失败过多
  - 从可疑 IP 登录
  - 从不寻常的位置访问
  - 异常的身份验证
  - 匿名敏感分享下载
  - 潜在的数据泄露
- 如果整数数据类型字段值不可用，则分配的值为 **-999**。例如，`"latitide"= -999`。
- 如果字符串数据类型字段值不可用，则分配的值为 **NA**。例如，`"city"= "NA"`。

有关详细信息，请参阅适 用于 SIEM 的 Citrix Analytics 数据格式。

2021 年 3 月 26 日

新增功能

对 **SIEM** 消息的限制　Citrix Analytics 向 SIEM 服务发送每个风险指示器发生的最多 1000 个事件详细信息。这些事件按发生时间顺序发送。有关详细信息，请参阅适 用于 SIEM 的 Citrix Analytics 数据格式。

在 **SIEM** 消息中添加了数据源 **ID** 和指示器类别 **ID** 字段　在指示器摘要架构和指示器事件详细信息架构中添加了以下字段。

字段	说明
`data_source_id`	与数据源关联的 ID。ID 0 = Citrix Content Collaboration, ID1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Virtual Apps and Desktops, ID 4 = Citrix Access Control
`indicator_category_id`	与风险指示器类别关联的 ID。ID 1 = 数据泄露，ID 2= 内幕威胁，ID 3 = 受到攻击的用户

有关详细信息，请参阅适 用于 SIEM 的 Citrix Analytics 数据格式。

2021 年 3 月 18 日

新增功能

访问保障位置控制板

> 注意
>
> 该功能处于预览中。

访问保障位置控制板概述了 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 用户在选定时间段内登录的位置。Citrix Analytics 从用户设备上安装的 Citrix Workspace 应用程序接收这些用户登录事件。

要查看控制板，请单击“安全”**>**“访问保障”。

您可以查看所选期间的以下信息：

- 来自特定位置和跨位置的用户登录总数。
- 跨地点的唯一用户登录总数。
- 用户登录的国家/地区总数。
- 具有唯一用户登录名的前 10 个位置。

有关详细信息，请参阅 访问保证位置。

支持 **NOT LIKE (!~)** 运算符　对于自助搜索查询和自定义风险指示器条件，您现在可以使用 NOT LIKE (!~) 运算符。运算符会检查用户事件是否符合您指定的匹配模式。它返回事件字符串中任意位置不包含指定模式的事件。

例如，查询 `User-Name !~ “John”` 显示除了 John、John Smith 或包含匹配名称“约翰”的任何此类用户以外的用户的事件。

有关详细信息，请参阅 自助搜索。

翻译的操作系统版本　对于 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 数据源，平台维度现在转换为操作系统主要版本、操作系统次要版本和操作系统额外细节维度。根据用户的操作系统详细信息，Citrix Analytics 会在自助服务搜索页面上显示这些维度。

您可以使用这些维度来定义自定义风险指示器的条件。

对于之前创建的自定义风险指示器，如果您已将 平台 维度用作条件，Citrix Analytics 会自动将 平台 维度替换为 操作系统主要版本、操作系统次要版本和 操作系统额外详细信息。此更新不会影响您定义的条件的完整性。

有关新维度的详细信息，请参阅 Virtual Apps and Desktops 的自助搜索。

更新了应用程序和桌面的数据字段　在“应用程序和桌面的自助式搜索”中，根据上下文模板查看更新的数据字段。

有关详细信息，请参阅应用程序和桌面的自助式搜索。

已弃用的功能

从自助搜索页面中删除了 **VPN_AF** 和 **VPN_SU** 事件　现在，在 Citrix Gateway 数据源的自助搜索页面上，以下记录类型现在已删除。

记录类型	记录名
VPN_SU	会话更新记录
VPN_AF	应用启动失败记录

因此，您无法根据这些记录类型筛选和查看事件。任何基于这些记录类型的自定义风险指示器都停止运行。

有关详细信息，请参阅 网关的自助搜索。

2021 年 3 月 11 日

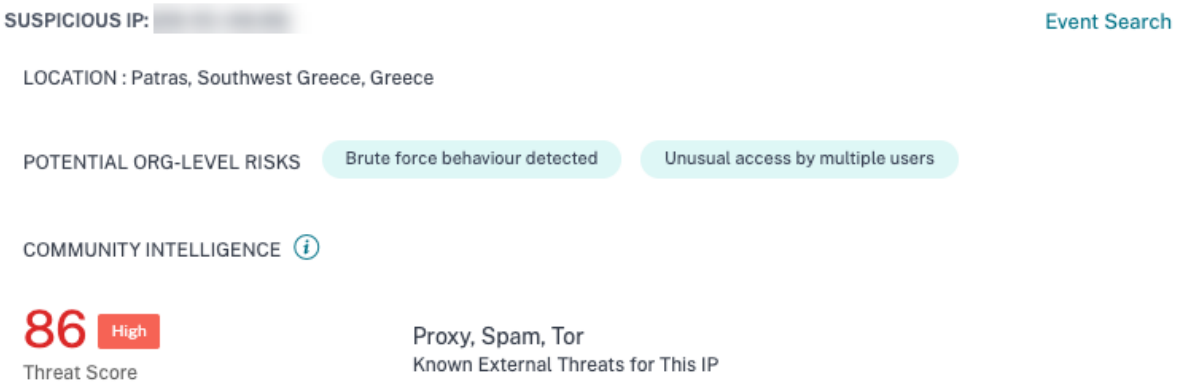
新增功能

用户风险评分模式的当前时间戳　将以用户风险评分模式格式添加一个新 `last_update_timestamp` 字段。此字段表示风险评分上次更新的时间。有关架构格式的详细信息，请参阅 用户风险评分架构。

2021 年 3 月 3 日

新增功能

对可疑 **IP** 风险指示器登录的增强　在用户的风险时间表页面上，将为从可疑 **IP** 登录风险指示器显示一个新的可疑 **IP** 部分。本部分提供以下信息：



- 检测到可疑登录事件的 IP 地址。
- 用户的位置。
- Citrix Analytics 最近在组织中检测到的任何可疑 IP 事件模式。
- 有关 IP 地址的社区级情报源。

有关详细信息，请参阅 从可疑 IP 登录 风险指示器。

通过不寻常的位置风险指示器增强访问权限

- 在 Citrix Content Collaboration 的从异常位置访问风险指示器中，在事件表中添加了 **TOOL NAME** 列。从事件表中删除了 设备浏览器 列。有关详细信息，请参阅 Citrix Content Collaboration 风险指示器。
- 在 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 的“从异常位置访问”风险指示器中，在事件表中添加了设备 **ID** 和 **RECEIVER** 类型列。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 风险指示器。

适用于 **SIEM** 的 **Citrix Analytics** 数据格式　本 文 介绍了 Citrix Analytics 为您的 SIEM 服务生成的已处理数据的架构。

已修复的问题

- 对于 Content Collaboration 用户，如果 `Is Employee<!--NeedCopy-->` 值为空，则该用户不会显示在已发现的用户列表中。[CAS-47815]

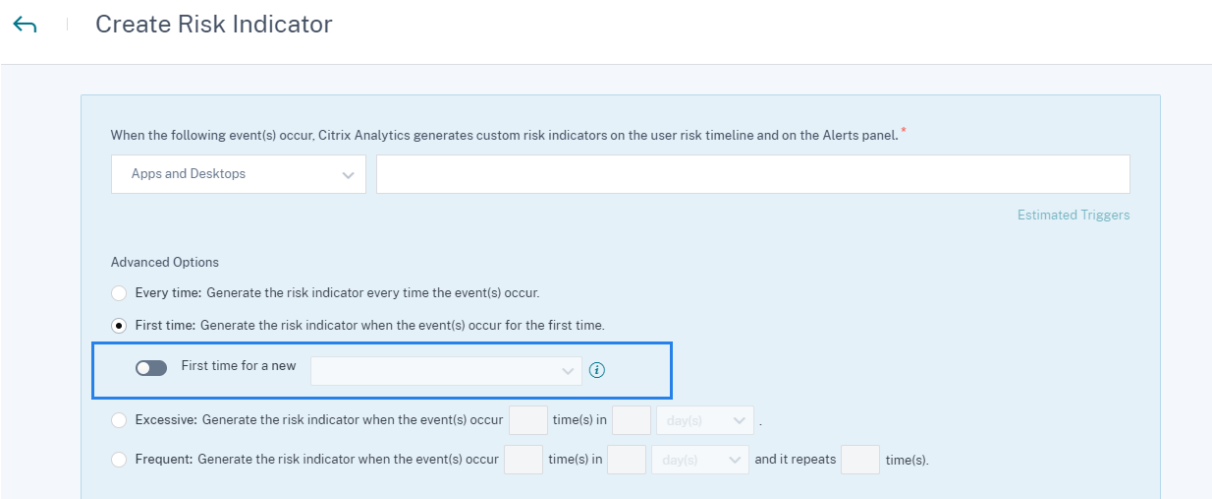
2021 年 **2** 月 **18** 日

新增功能

支持从自定义风险指示器中的新实体首次访问　现在，您可以创建风险指示器，当 Citrix Analytics 首次收到来自新实体的事件时触发该风险指示器。实体的一些示例包括客户端 IP、城市和国家/地区。

在 创建指示器 页面上，单击 首次 选项。启用“首次创建新”按钮，然后根据数据源从列表中选择一个有效的实体。您无需为实体分配任何特定值。例如，如果从列表中选择 城市，则每当用户首次从新城市登录时，Citrix Analytics 都会触发一个风险指示器。

有关详细信息，请参阅 创建自定义风险指示器。



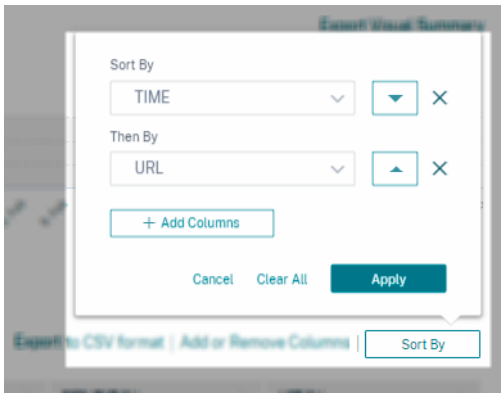
创建自定义风险指示器的最大限制　现在，您可以创建最多 50 个自定义风险指示器。如果达到此最大限制，则必须删除或编辑任何现有的自定义风险指示器以创建自定义风险指示器。

有关详细信息，请参阅自定义风险指标。

来自 **Citrix Virtual Apps and Desktops** 和 **Citrix DaaS** 的用户位置数据　在用户信息页面上，Citrix Analytics 现在显示来自 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 数据源的用户位置。

有关用户位置的详细信息，请参阅 用户配置文件。

多列排序　在自助搜索页面上，您现在可以按多列对用户事件进行排序。单击 排序方式，添加列和排序顺序。单击 应用对用户事件进行排序。您最多可以添加六列来执行多列排序。



有关详细信息，请参阅 自助搜索。

已弃用的功能

已弃用过多的授权失败风险指示器　Citrix Gateway 风险指示器 - 授权失败过多已被弃用。您只能查看与此指示器相关的历史数据。

以下更改适用于此弃用的一部分：

- Citrix Analytics 不再生成这些风险指示器。
- Citrix Analytics 不再以这些风险指示器为条件生成策略。
- 将这些风险指示器作为条件的默认策略不再生效。

有关详细信息，请参阅 Citrix Gateway 风险指示器。

2021 年 1 月 27 日

新增功能

增强了从异常位置访问风险指示器　对于 Citrix Content Collaboration、Citrix Gateway 和 Citrix Virtual Apps and Desktops，当用户从与新国家/地区关联的 IP 地址或远离任何以前登录的新城市登录时，将触发从异常位置访问风险指示器位置。其他因素包括用户的整体移动性水平以及组织中所有用户从城市登录的相对频率。在所有情况下，用户位置历史记录都基于过去 30 天的登录事件。

有关风险指示器的更多信息，请参阅以下主题：

- Citrix Content Collaboration 风险指示器
- Citrix Gateway 风险指示器
- Citrix Virtual Apps and Desktops 和 Citrix DaaS 风险指示器

2021 年 1 月 20 日

已修复的问题

- 对于具有本地 StoreFront 的应用程序和桌面数据源，尽管已成功连接 StoreFront 部署，但数据处理仍会失败。

  [CAS-46656]

2021 年 1 月 19 日

已修复的问题

- 在自定义风险指示器页面中，在更正搜索字段中的无效条件后，估计触发器 链接不会响应。

  例如，您键入无效条件 *Client-IP = 10.10.10.10*。更正此条件并键入 *Client-IP =* “*10.10.10.10*”后，估计触发器链接不响应。

  解决办法：刷新自定义指示器页面，然后创建具有有效条件的自定义指示器。

  [CAS-46316]

2021 年 1 月 13 日

新增功能

适用于 **Splunk** 的 **Citrix Analytics** 加载项的新版本已推出　适用于 Splunk 的 Citrix Analytics 附加版本 2.1.0 现已推出。转到下 载 页面下载文件。

增加了对 **Splunk** 云输入数据管理器 **(IDM)** 和 **Splunk 8.1 64** 位的支持　现在，您可以将 Citrix Analytics for Security 与 Splunk Cloud IDM 和 Splunk 8.1 64 位集成。有关详细信息，请参阅 Splunk 集成。

已弃用的支持

已删除对 **Splunk 7.1 64** 位的支持　您无法再将 Citrix Analytics for Security 与 Splunk 7.1 64 位集成。有关受支持的 Splunk 版本的信息，请参阅 Splunk 集成。

2021 年 **1** 月 **11** 日

已修复的问题

- 在“Virtual Apps and Desktops”站点卡上，支持的客户端用户标签将重命名为已收到用户的事件。标签 不受支持的客户端用户 被重命名为 无法接收来自用户的事件。

  [CAS-44773]

2020 年 **12** 月 **17** 日

新增功能

使用预配置的自定义风险指示器和策略来阻止来自异常位置的访问（地理围栏）　Citrix 提供了预配置的自定义风险指示器列表以及可帮助您监视 Citrix 基础架构安全性的策略。借助这些指示器和策略，您可以阻止来自其通常运营国家/地区以外的国家/地区的用户访问权限。默认情况下，国家/地区设置为“美国”。您可以为地理围栏设置所需的国家/地区。

以下是预配置的自定义风险指示器和策略：

- CVAD-会话在地理围栏之外开始
- GW-Geofence 穿越
- CCC-地理围栏穿越
- 会话在地理围栏之外开始

有关详细信息，请参阅 预配置的自定义风险指示器和策略。

查看用户响应电子邮件中访问的位置　用户回复电子邮件现在显示用户在过去 15 分钟内访问过的所有位置，而不是用户设备的 IP 地址。该位置以 `<City>,<Country><!--NeedCopy-->` 格式显示。如果城市或国家/地区不可用，相应的值将显示为“未知”。

有关详细信息，请参阅请求用户响应。

已重命名 **Content Collaboration** 风险指示器-首次从新位置访问　Citrix Content Collaboration 风险指示器首次从新位置进 行 访问将重命名为从异常位置访问。

有关详细信息，请参阅 从异常位置访问。

已弃用的功能

风险指示器反馈　删除了风险指示器反馈机制。如果 Content Collaboration 风险指示器-从异常位置访问被错误地触发，则无法再将其报告为误报并提供反馈。

2020 年 12 月 7 日

新增功能

潜在数据泄露风险指示器的改进　对风险指示器进行了以下增强：

- “发生了什么”部分中的信息已更新。时间格式已更新以保持一致性。
- 设备位置信息显示在事件列表中。

有关风险指示器的更多信息，请参阅 潜在的数据泄露。

Content Collaboration 风险指示器的改进-首次从新位置访问　在用户风险时间表上，选择 首次从新位置访问 以查看以下信息：

- 登录位置：显示用户登录的通常和不寻常位置的地理地图视图。
- 从常规位置登录的次数-过去 **30** 天：显示用户在过去 30 天内登录的前 6 个常用位置的饼图视图。它还显示来自这些位置的登录事件的数量。
- 异常位置的事件详细信息：为用户提供来自异常位置的登录事件的列表。

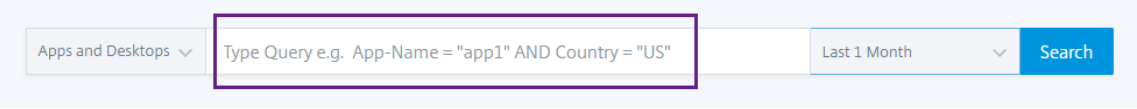
有关风险指示器的更多信息，请参阅 首次从新位置访问。

2020 年 11 月 30 日

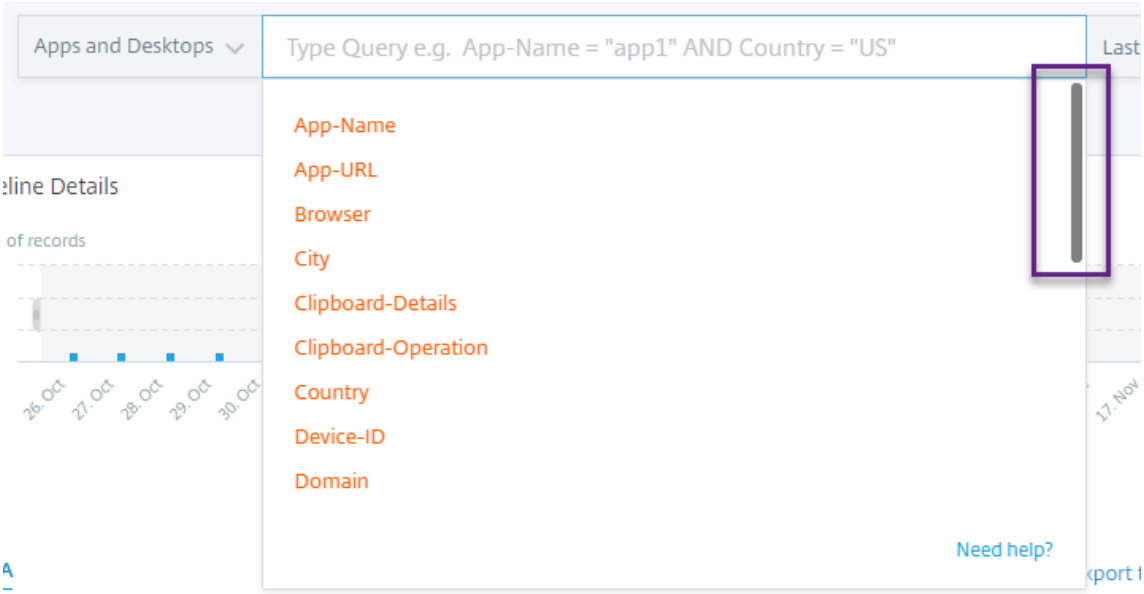
新增功能

自助搜索页面改进　为增强自助搜索页面的可用性，进行了以下改进：

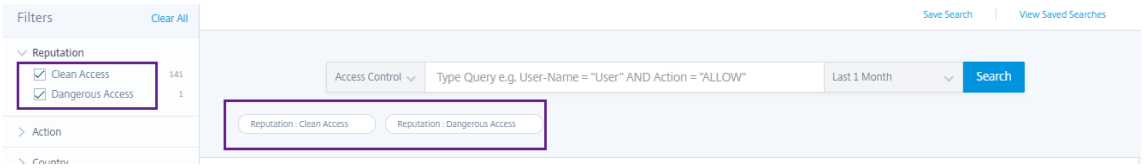
- 搜索框显示一个查询示例，指示如何键入自己的查询。



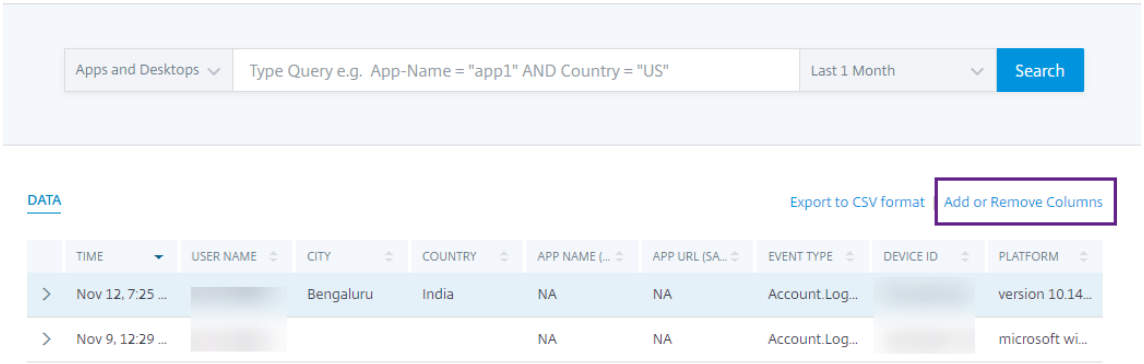
- 在 macOS 中，默认情况下会显示维度列表上的滚动条。



- 应用的滤镜现在显示为筹码。



- 添加或删除列 标签将替换 **+** 图标。



有关详细信息，请参阅 自助搜索。

策略改进　现在，“策略”页面显示与成功发现并连接到 Citrix Analytics 的数据源关联的策略。此页面不显示为未发现的数据源定义了条件的策略。关闭已连接的数据源的数据处理不会影响“策略”页面上的现有 策略。

有关详细信息，请参阅 配置策略和操作。

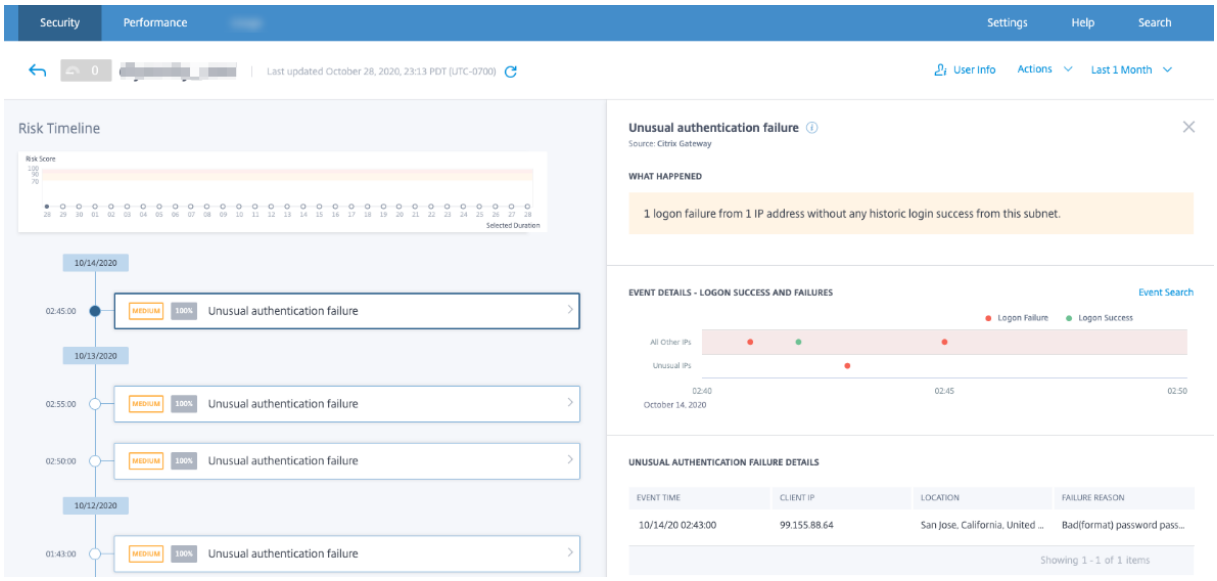
2020 年 11 月 4 日

新增功能

异常身份验证失败 **- Citrix Gateway** 风险指　当用户从异常 IP 地址登录失败时，Citrix Analytics 会检测基于访问的威胁，并触发 异常身份验证失败 风险指示器。

当组织中的用户从不正常的 IP 地址登录失败时，会触发此风险指示器。

有关详细信息，请参阅 Citrix Gateway 风险指示器。



2020 年 10 月 20 日

已修复的问题

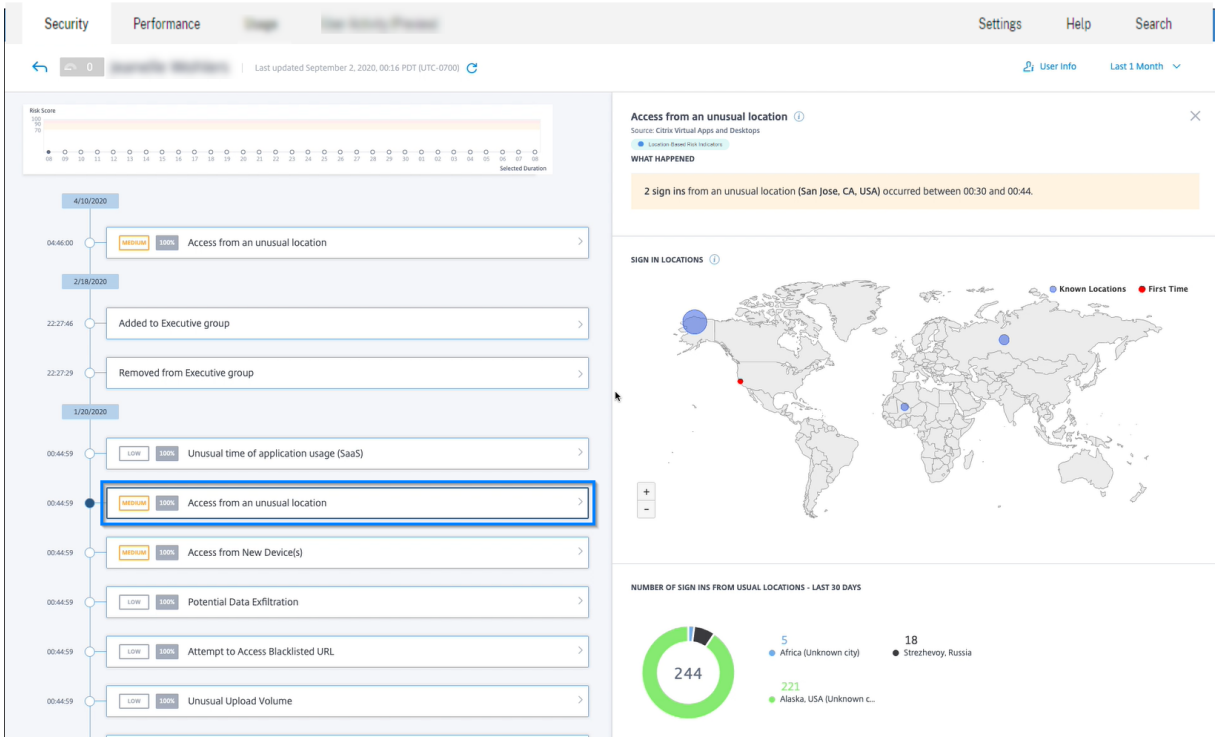
- 风险指示器应用了 注销用户 操作的 新设备首次访问 未按预期工作。

  [CAS-40743]

2020 年 10 月 15 日

新增功能

从异常位置访问—**Citrix Virtual Apps and Desktops** 和 **Citrix DaaS** 风险指示器　Citrix Analytics 会根据来自 Citrix Workspace 的异常登录来检测基于访问的威胁，并触发相应的风险指示器。



有关详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 风险指示器。

共享链接控制板增强

- 共享 URL 列现在由共享 ID 列替换。现在，每个共享 URL 都使用共享 ID 进行标识。
- 控制板上的时间选择已删除。现在，此控制板显示从事件状态到过期状态的所有共享链接，而不是选定的时间段。
- 所有共享链接先按事件链接的顺序排序，然后按过期链接的顺序进行排序。默认情况下，具有最高风险指示器计数的共享链接显示在列表顶部。
- 风险链接现在显示存在风险行为的事件链接。它不会显示过期的链接。默认情况下，具有最高风险指示器计数的风险链接显示在列表顶部。
- 已删除“风险共享链接”卡和“所有共享链接”卡中的趋势视图。

有关详细信息，请参阅 共享链接控制板。

分享链接风险时间表增强　风险时间表现在显示的是共享 ID，而不是共享 URL。有关详细信息，请参阅 共享链接风险时间表。

已弃用的功能

不建议从操作系统 **(OS)** 风险指示器不受支持的设备进行访问　Citrix Virtual Apps and Desktops 风险指示器 - 从操作系统 **(OS)** 不受支持的设备进行访问已被弃用。您只能查看与此指示器相关的历史数据。

以下更改适用于此弃用的一部分：

- 分析不再生成这些风险指示器。
- Analytics 不再以这些风险指示器为条件生成策略。
- 将这些风险指示器作为条件的默认策略不再生效。

有关详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 风险指示器。

2020 年 9 月 10 日

新增功能

StoreFront 清单　Citrix Analytics 现在会显示下载 StoreFront 配置文件之前必须满足的先决条件列表。查看清单并确保选择了所有最低要求。如果未选择最低要求，则无法下载配置文件。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 数据源。

自助搜索-支持 **NOT EQUAL (!=)** 运算符　在以下功能中，您现在可以在查询中使用 NOT EQUAL (!=) 运算符：

- 自定义风险指示器
- 自助搜索

您可以在以下情况下使用此运算符：

数据源	维度
Content Collaboration	国家、城市、客户端操作系统
访问控制	国家、城市、操作、URL、URL 类别、信誉、浏览器、操作系统、设备
Citrix Cloud Labs 应用程序和桌面	国家、城市、应用名称、剪贴板操作、浏览器、操作系统
网关	身份验证阶段，客户端 IP

使用运算符，创建具有单个值的自定义指示器表达式，例如“国家/地区!= XYZ”并查看用户列表。然后创建策略以应用诸如“添加到监视名单”、“通知管理员”或“禁用用户”等操作。
您还可以在指定数据源的自助搜索中使用运算符来筛选用户事件。

在为查询中的维度输入值时，请使用数据源的自助搜索页面上显示的精确值。尺寸值区分大小写。

2020 年 9 月 8 日

新增功能

用户关联　Analytics 现在将从各种数据源中发现的用户关联起来。此机制将大多数重复用户从发现的用户列表中删除。Analytics 中发现的用户现在会显示唯一用户的列表以及他们的数据源和风险指示器。

例如，用户“Joe Smith”可以有多个用户标识符 - JosephSm、joe.smith@citrix.com 和 joe.smith，具体取决于数据源。Analytics 现在使用唯一的标识符名称来识别此用户。所有其他用户标识符都是相关的，从各种数据源为 Joe Smith 接收的事件都链接到此唯一名称。
有关详细信息，请参阅 发现的用户

已修复的问题

在“操 作”列表中，选择操作选项并单击“应用”后，将显示一条错误消息。

[CAS-39914]

2020 年 8 月 11 日

已修复的问题

- 您无法将 Microsoft Graph 安全性与 Citrix Analytics 集成。出现此问题的原因是 Microsoft 门户无法重定向到 Citrix Analytics。

[CAS-38021]

2020 7 月 31 日

已修复的问题

- 自定义风险指示器中的“估计触发器”选项不能预测最近一天的自定义风险指示器实例。

[CAS-38129]

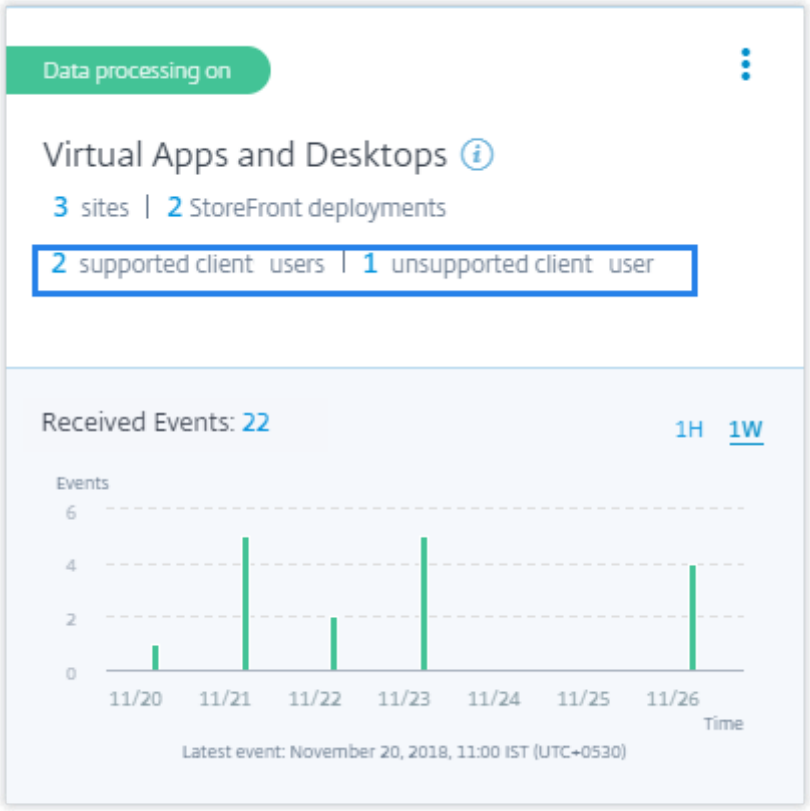
2020 年 7 月 9 日

新增功能

Virtual Apps and Desktops 站点卡片显示具有受支持和不支持客户端　现在，在站点卡片上，您可以查看在其终端上使用受支持和不受支持的 Citrix Workspace 应用程序或 Citrix Receiver 客户端版本的用户数量。

- 单击受支持客户端的用户计数可查看显示所有发现的 用户 的“用户”页。
- 单击不受支持的客户端的用户数以下载 CSV 文件。该文件列出了用户及其不受支持的客户端版本。Analytics 不会从不受支持的客户端接收用户事件，因此不会将用户添加为已发现的用户。使用 CSV 文件，您可以识别必须将其客户端升级到受支持版本的用户，以便 Analytics 能够对其行为提供安全洞察。

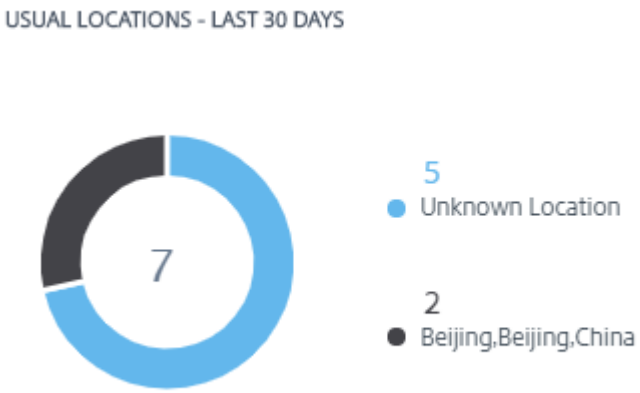
要查看支持的客户端列表，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源。



从异常位置风险指示器访问

- Citrix Gateway 风险指示器首次从新位置进行访问将重命名为从异常位置访问。
- 在用户风险时间表上，事件详细信息部分中介绍了地理地图和饼图。
  - 登录位置：此部分显示用户通常和不寻常位置的地理地图视图。地理地图右上角的颜色代码表示通常和不寻常的位置。您可以缩放地理地图以更仔细地查看该位置。

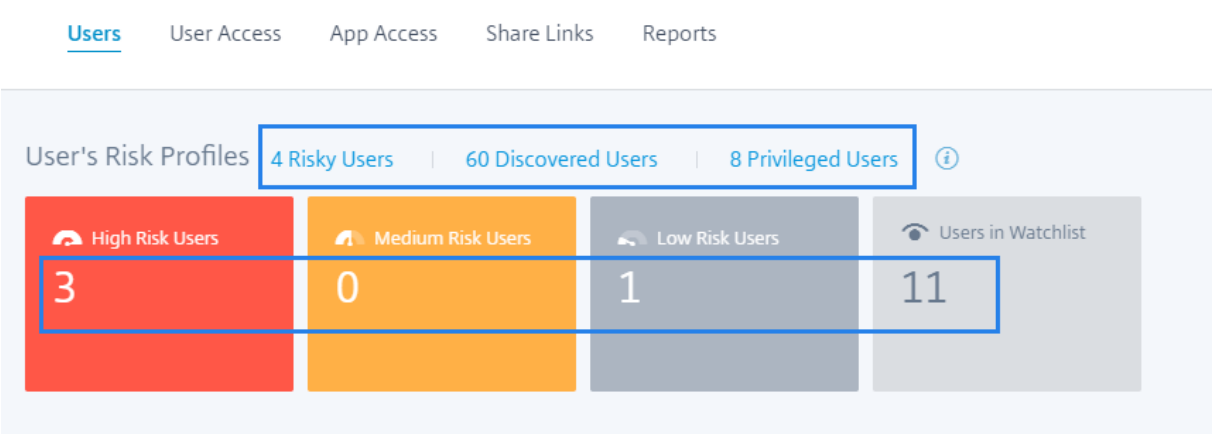
– 通常的位置-过去 **30** 天：此部分显示一个饼图，其中显示了用户登录的前 6 个常用位置。每个位置都使用不同的颜色代码进行标记。您可以按位置对部分进行排序，以获取所选位置的详细视图。



有关详细信息，请参阅 从异常位置访问。

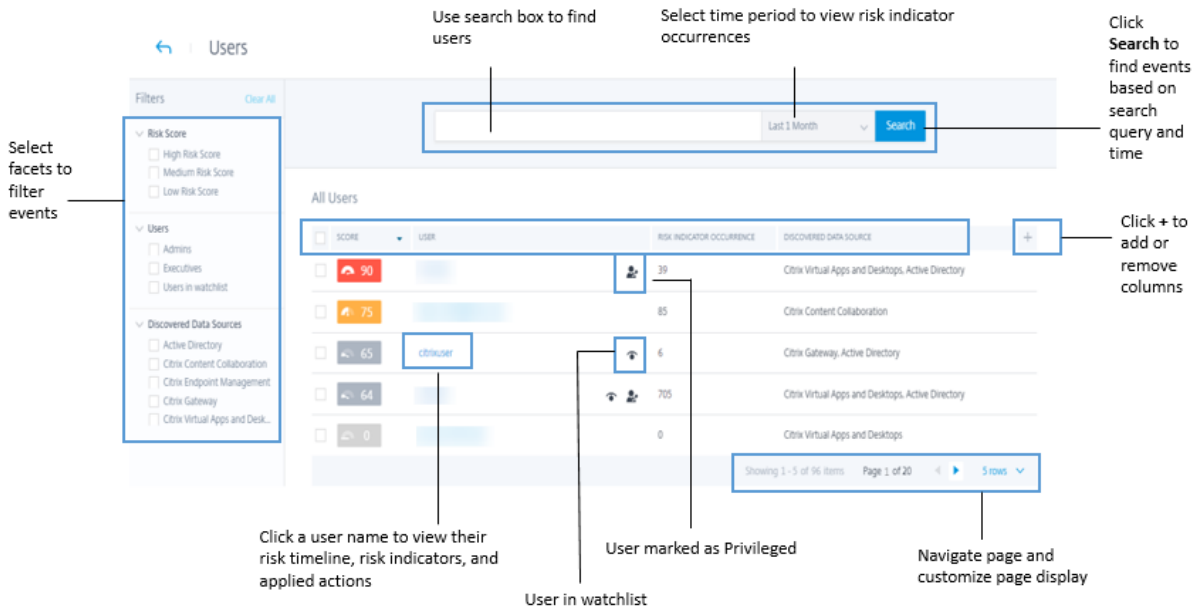
用户控制板数据　无论在“用户”控制板和“用户”页面上选择的时间段如何，都会显示过去 13 个月内监视名单中存在风险的用户、发现的 用户、特权用 户和 用户 的数量。当您选择时间段时，风险指示器的出现次数会发生变化。

有关详细信息，请参阅 用户控制板。



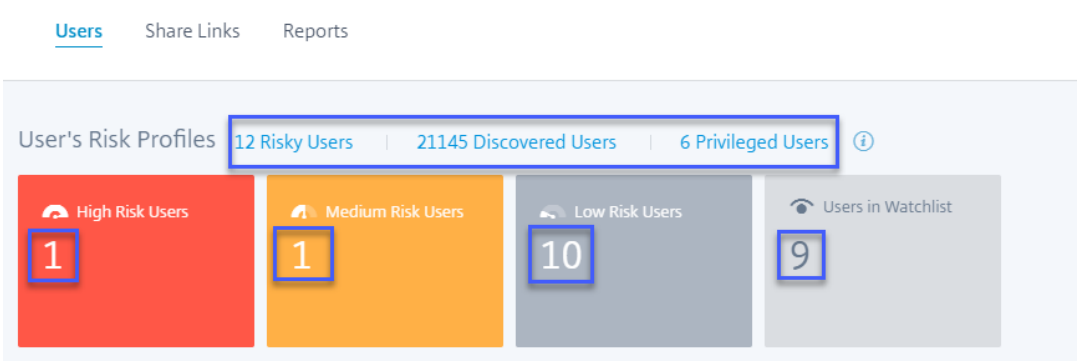
重新设计的用户页面　用 户 页面已得到增强，以获得更好的用户体验。它根据用户风险评分、数据源和用户类型提供了用户事件的综合摘要。

为了支持更有针对性的搜索，“用户”页面在左侧窗格中包含“筛选器”部分，顶部包含搜索栏。您可以搜索预设时间或自定义时间范围内的用户事件。



要查看“用 户”页面：

- 转到“安全”**>**“用户”以查看“用 户”控制板并执行以下操作：
  - 单击以下链接之一或卡片。



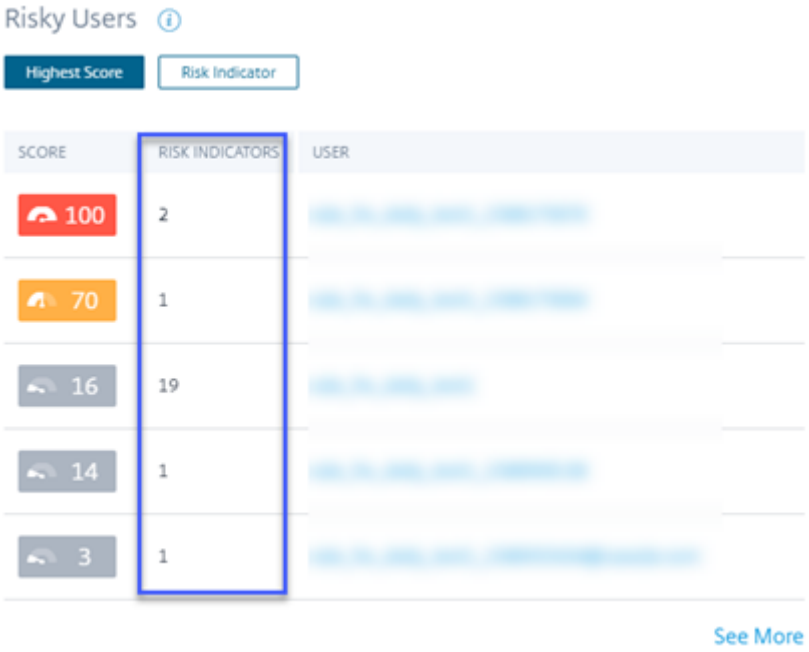
  - 在“风险用户”窗格上，单击“查看更多”。
  - 在监视名单中的用户 窗格中，单击 查看更多。
  - 在“特权用户”窗格上，单击“查看更多”。

- 转到 设置 **>** 数据源 **>** 安全性。单击任何数据源站点卡片上的用户数。

有关详细信息，请参阅 用户控制板。

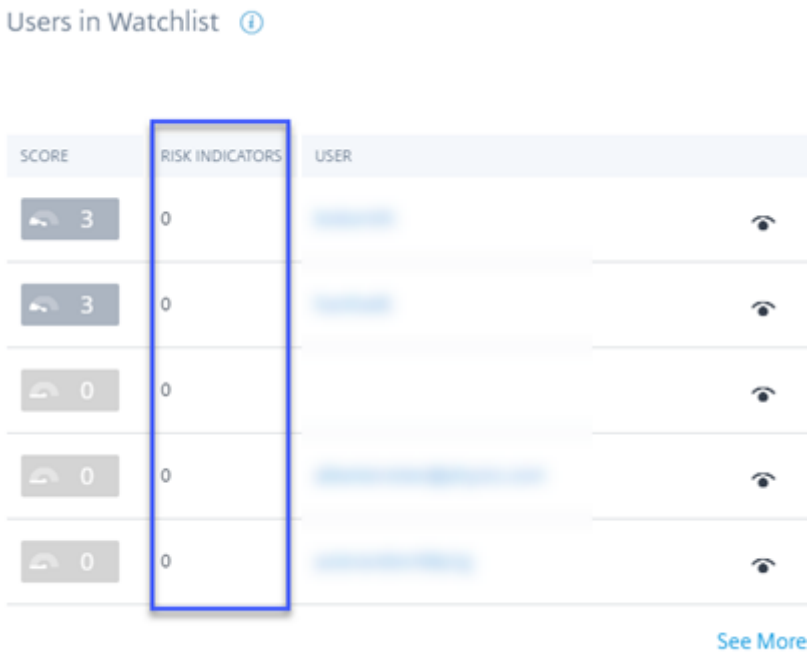
风险用户窗格的增强　变化 列将替换为 风险指示器 列。“风险指 示器”列显示用户在特定时间段内的总风险指示器出现次数。

有关详细信息，请参阅 风险用户。



监视名单窗格中的用户增强　变化 列将替换为 风险指示器 列。“风险指 示器”列显示用户在特定时间段内的总风险指示器出现次数。

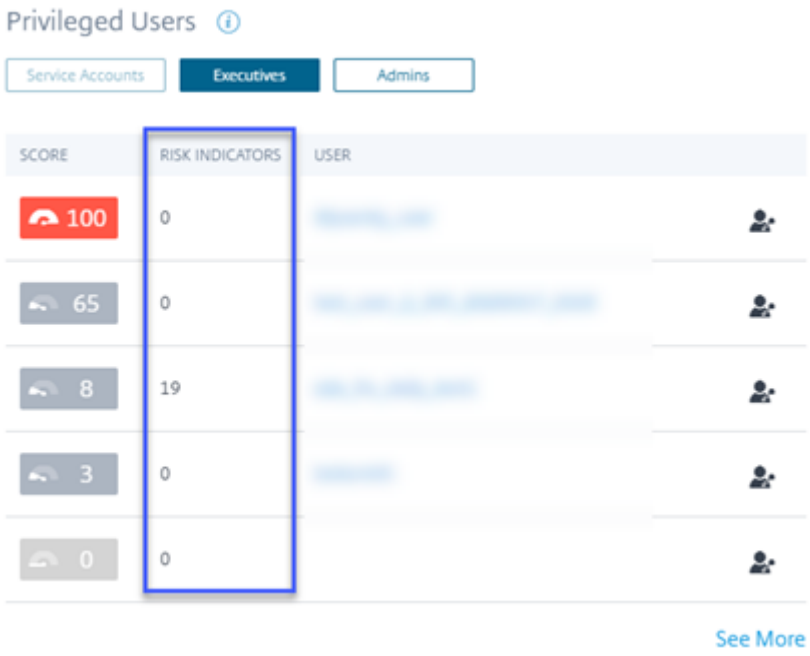
有关详细信息，请参阅 监视名单中的用户。



特权用户窗格的增强

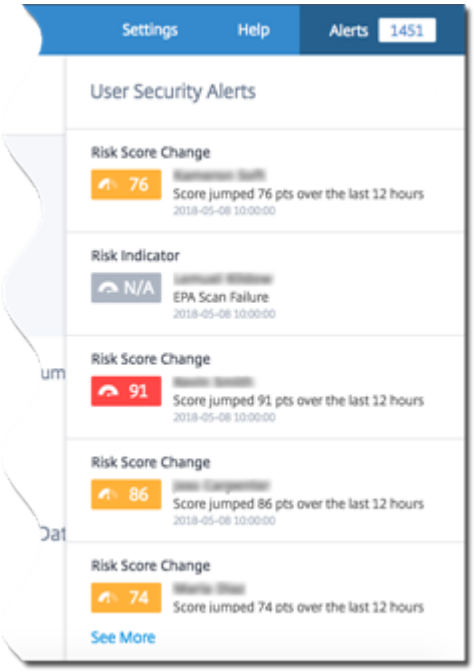
- 变化 列将替换为 风险指示器 列。“风险指 示器”列显示用户在特定时间段内的总风险指示器出现次数。
- 单击查 看更多 以查看用 户 页面。显示管理员和执行特权用户列表的 **Users** 页面。在此页面上，您可以添加或删除作为特权用户的用户。

有关详细信息，请参阅 特权用户。

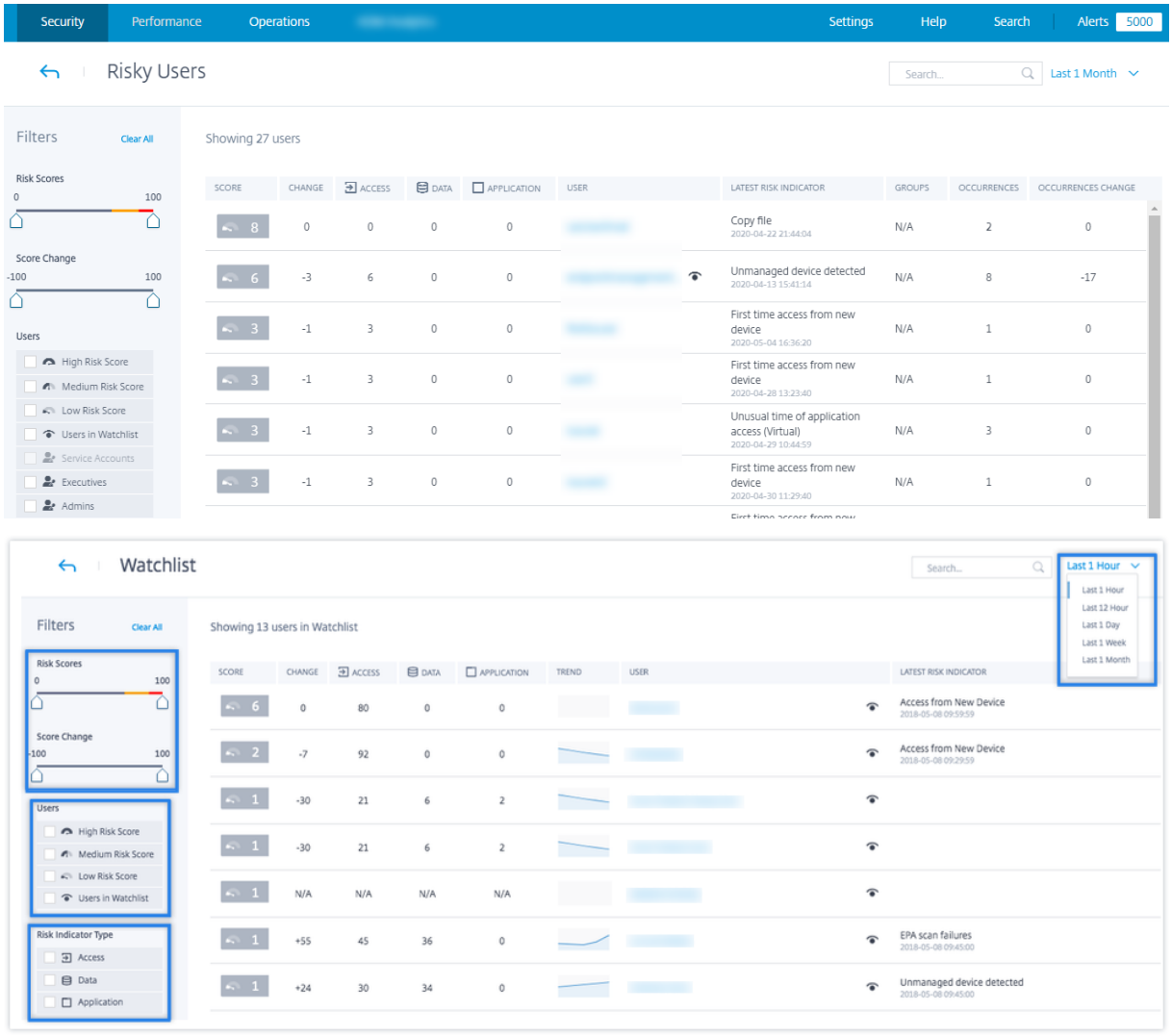


已弃用的功能

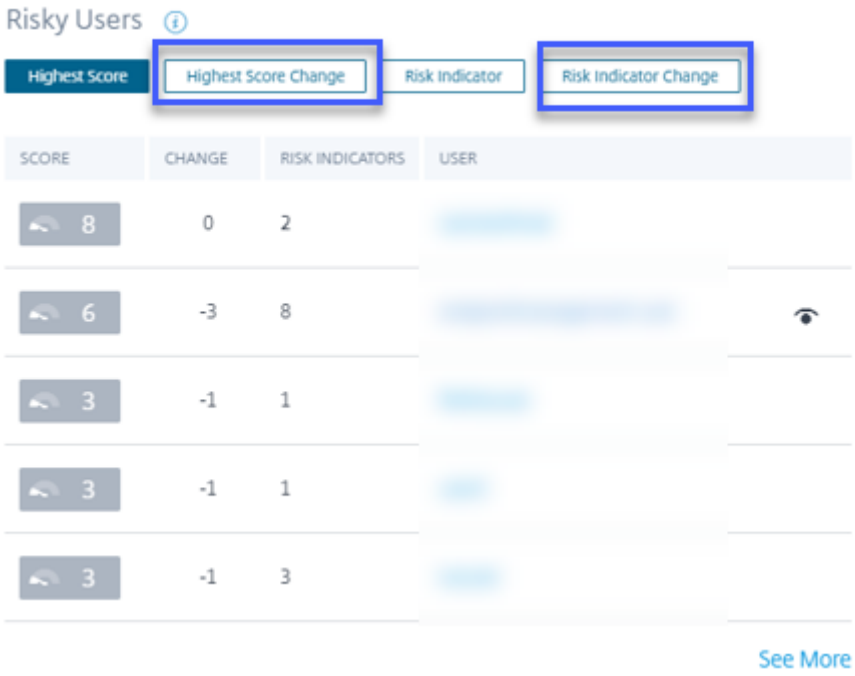
警报　警 报功能现已弃用，在 Analytics 用户界面上不再可用。



“风险用户和监视名单”页面　不建议使用“风险用户”和“监视名单”页面。它们将替换为 用户 页面，该页面汇总了所有有风险的用户事件和监视名单中的用户。

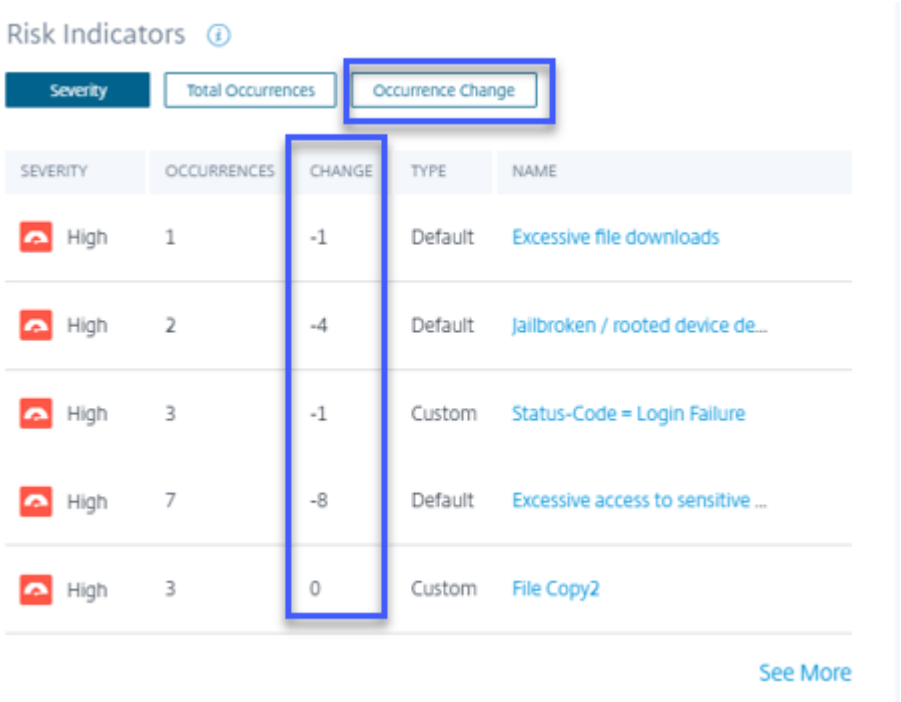


风险用户窗格　最 高分变化 和 风险指示器更改 选项卡将从风 险用户窗格中移除。

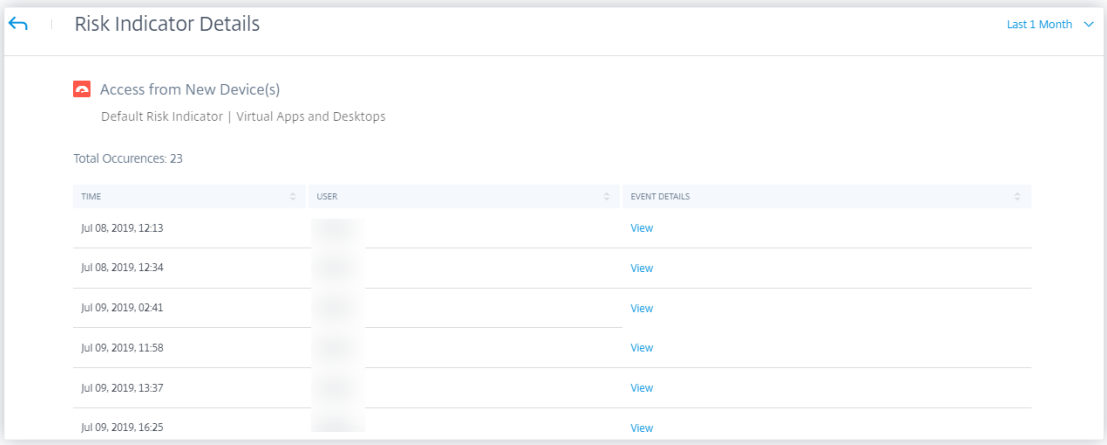


风险指示器窗格

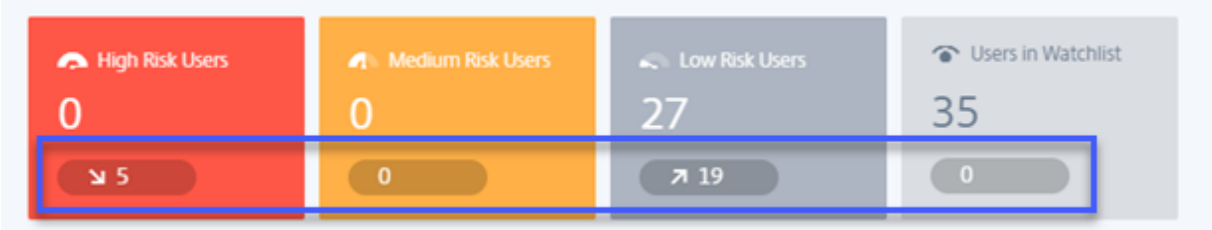
- 将删除 具体值更改选项卡和更改列。



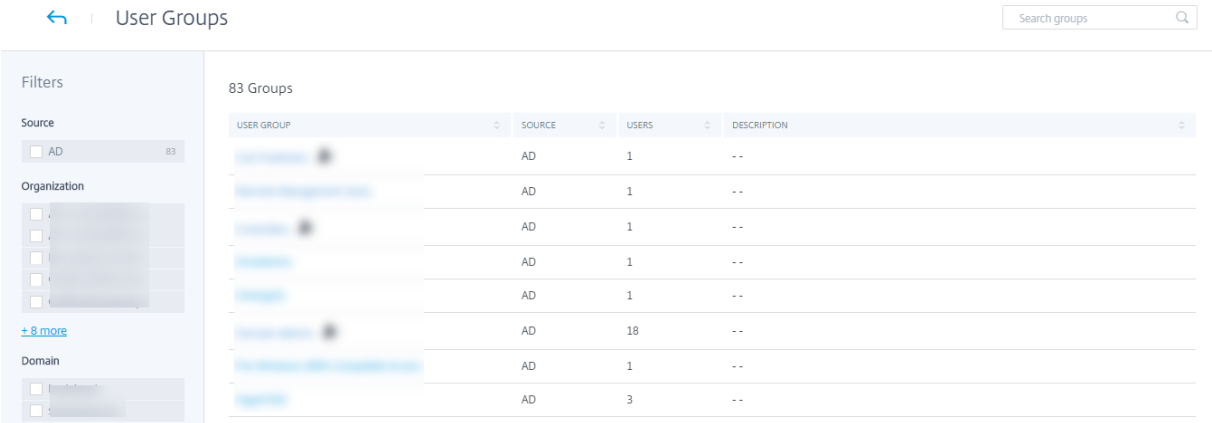
- 风险指示器详细信息 页面已弃用。以前，当在风险指示器窗格或风险指示器 概述页面上选择 风险指 示器时，会显示此页面。



趋势视图　在“用户”控制板上，用户计数的趋势视图将从“高风险用户”、“中风险用户 **”、“低风险用户”和“监视名单中的用户 **”卡中删除。



“用户组”页面　不建议使 用“设置”选项下的“用户组”页面。您不能再添加或删除作为特权组的用户组。但是，您可以添加或删除单个用户作为特权用户。有关详细信息，请参阅 特权用户。



2020 年 6 月 26 日

已弃用的功能

不建议使用异常应用程序访问时间（虚拟 **/SaaS**）风险指示器　Citrix Virtual Apps and Desktops 风险指示器 - 异常应用程序访问时间（虚拟）和应用程序访问异常时间 **(SaaS)** 已被弃用。您只能查看与这些指示器相关的历史数据。

以下更改适用于此弃用的一部分：

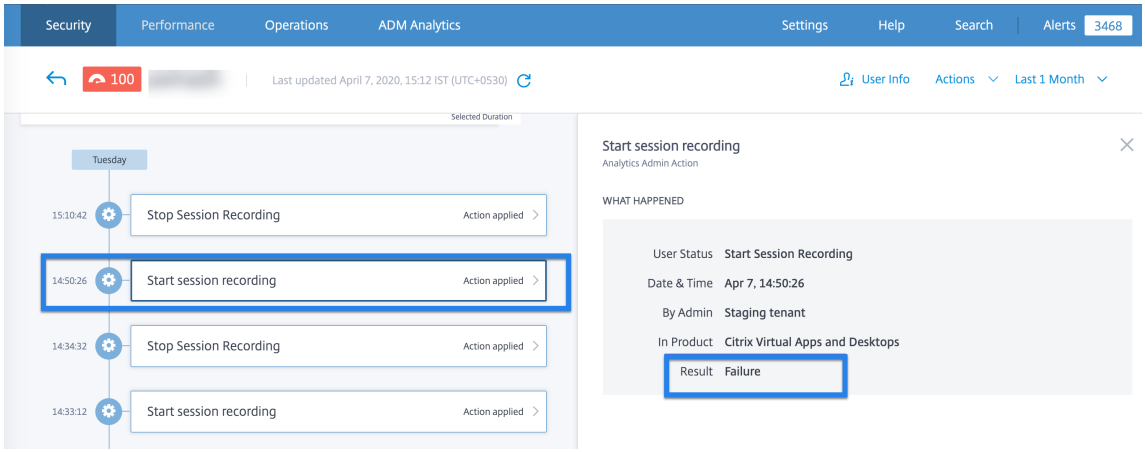
- 分析不再生成这些风险指示器。
- Analytics 不再以这些风险指示器为条件生成策略。
- 将这些风险指示器作为条件的默认策略不再生效。

有关详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 风险指示器。

2020 年 6 月 2 日

已修复的问题

- 在用户风险时间轴上，Virtual Apps and Desktops 操作（基于策略或手动应用）的状态显示为“失败”，即使这些操作已成功应用于用户帐户。例如，启动会话录制操作已成功应用于用户帐户，但结果显示为“失败”。[CAS-32773]



2020 年 5 月 11 日

已修复的问题

- 对于某些用户，不会触发基于策略的操作，也无法应用策略实施模式。当客户 ID 不是小写时，会出现此问题。[CAS-34209]、[CAS-34141]

- 无法为某些用户创建自定义风险指示器。当客户 ID 不是小写时，会出现此问题。

  [CAS-34139]

2020 年 4 月 29 日

已修复的问题

- 尽管 Analytics 会显示已成功应用操作的消息，但在 Citrix Virtual Apps and Desktops 上应用的操作风险指示器无法生效。Citrix Virtual Apps and Desktops 7 1912 版本中会发现此问题。

  [CAS-31544]

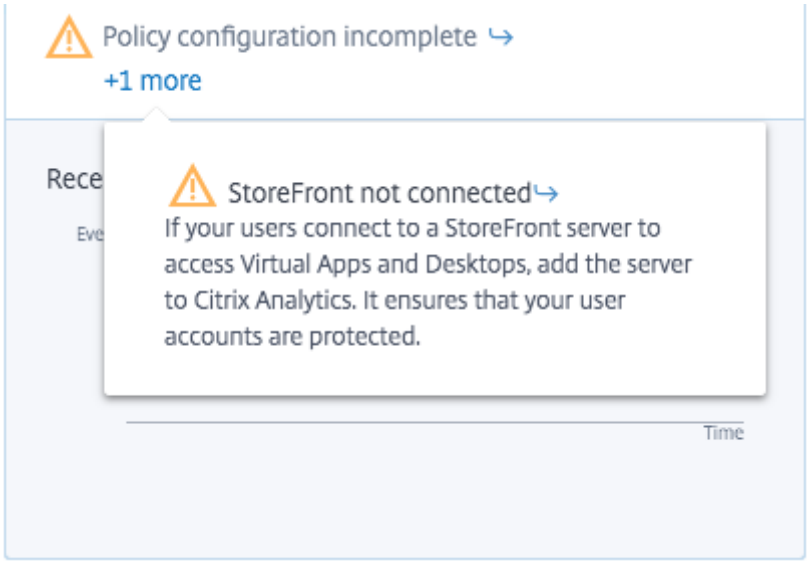
2020 年 4 月 2 日

新增功能

未添加 **StoreFront** 时禁用数据处理　在“设置”>“数据源”>“安全”>“**Virtual Apps and Desktops**”数据源站点卡片 上，如果您尚未加入 **StoreFront**，则不会启用“打开数据处理”按钮。您会在站点卡片上看到 **StoreFront** 未连接 警告消息。如果您有希望 Analytics 从中接收数据的活动本地站点，则必须验证是否已将 StoreFront 加载到 Citrix Analytics。它可以确保您的用户帐户受到保护。

在 **Virtual Apps and Desktops** 站点卡片上，选择垂直省略号 (⋮)，然后单击连接 **StoreFront** 部署。在显示的屏幕上，按照说明操作并完成 StoreFront 配置。

有关详细信息，请参阅使用 StoreFront 登录 Citrix Virtual Apps and Desktops 本地站点。



已修复的问题

- 对于 Citrix Content Collaboration 用户，基于策略的操作在以下情况下无法生效：
  - 定义自定义风险指示器条件时
  - 直到为用户生成风险指示器

  [CAS-29226]

2020 年 **3** 月 **4** 日

已修复的问题

- 当网关用户首次加入 Analytics 时，他们会看到错误 **Citrix ADC** 无响应或凭据不正确。重试后，他们会看到错误的 具有此 **IP** 地址的设备已存在。

[CAS-31180]

2020 年 **2** 月 **20** 日

新增功能

Citrix Analytics for Security 产品　Citrix Analytics for Security 现在可用于个人订阅。
您可以订阅 Citrix Analytics for Security，并获取特定于此产品的见解。有关详细信息，请参阅入门。

风险类别控制板　Citrix Analytics 引入了基于对组织安全方面具有类似影响的风险的风险指示器的分类。此控制板提供了需要立即关注的风险敞口和关键风险的全面视图。对于默认风险指示器，Analytics 会根据风险敞口自动分配风险类别。对于自定义风险指示器，您必须根据风险敞口选择适当的风险类别。

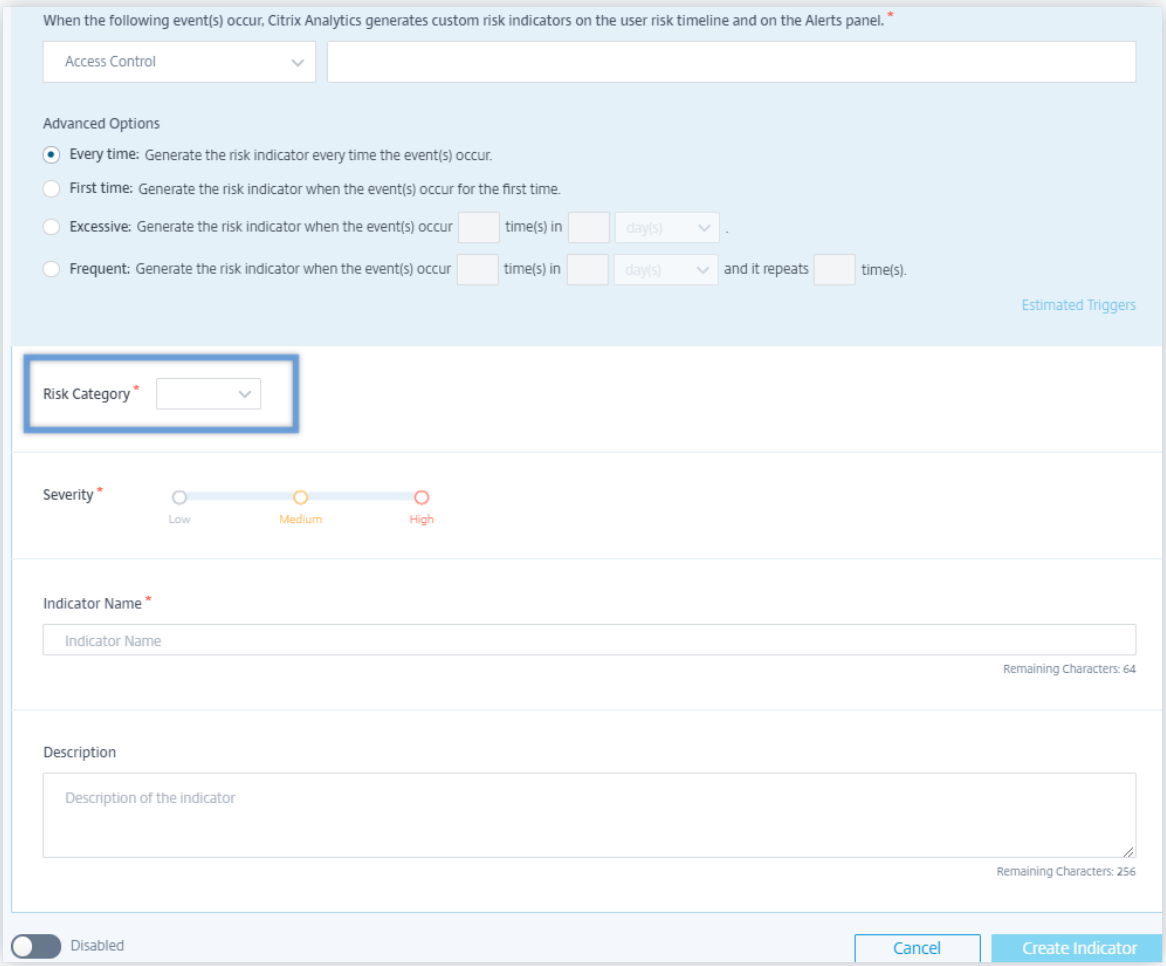
分析支持以下风险类别：

- 数据泄露
- 内幕威胁
- 受影响的用户
- 受损的端点

有关详细信息，请参阅 风险类别。

自定义指示器页面上的“风险类别”列　风险类别 列在自定义风险指示器页面上引入。根据风险敞口的类型，您可以为自定义风险指示器选择风险类别。如果您通过选择风险类别进行修改，以前创建的自定义风险指示器将显示在“风险类别”控制面板上。

有关详细信息，请参阅自定义风险指标。



风险指示器名称的更改　以下风险指示器名称已更改：

数据源	旧的名字	新名字
Citrix Virtual Apps and Desktops 和 Citrix DaaS	异常应用程序使用情况（虚拟	不寻常的应用程序访问时间（虚拟）
Citrix Virtual Apps and Desktops 和 Citrix DaaS	异常应用程序使用情况 (SaaS)	不寻常的应用程序访问时间 (SaaS)
Citrix Content Collaboration	登录失败过多	验证失败过多
Citrix Content Collaboration	不寻常的登录访问	首次从新位置访问
Citrix 访问控制	不寻常的下载量	数据下载过多
Citrix Gateway	登录失败	验证失败过多
Citrix Gateway	授权失败	授权失败过多

数据源	旧的名字	新名字
Citrix Gateway	不寻常的登录访问	首次从新位置访问

有关详细信息，请参阅 风险指示器。

已修复的问题

- 对于某些用户，即使数据源已成功载入并启用了 StoreFront，Citrix Analytics 也无法从 Virtual Apps and Desktops 接收任何数据。[CAS-24134]
- Citrix Analytics 无法接收来自 Citrix Content Collaboration 的下载事件。因此，不会触发以下风险指示器：
  - 匿名敏感分享下载
  - 分享链接下载量过多
  - 过度访问敏感文件
  - 文件下载过多

  [CAS-29207]
- 对于新加入的用户，在 Citrix Gateway 风险指示器上应用的手动操作和基于策略的操作不会生效。[CAS-29029]
- 某些用户无法在“数据源”页面上查看站点卡片。通过重新填充缓存可以解决此问题。[CAS-28781]

2020 年 **1** 月 **9** 日

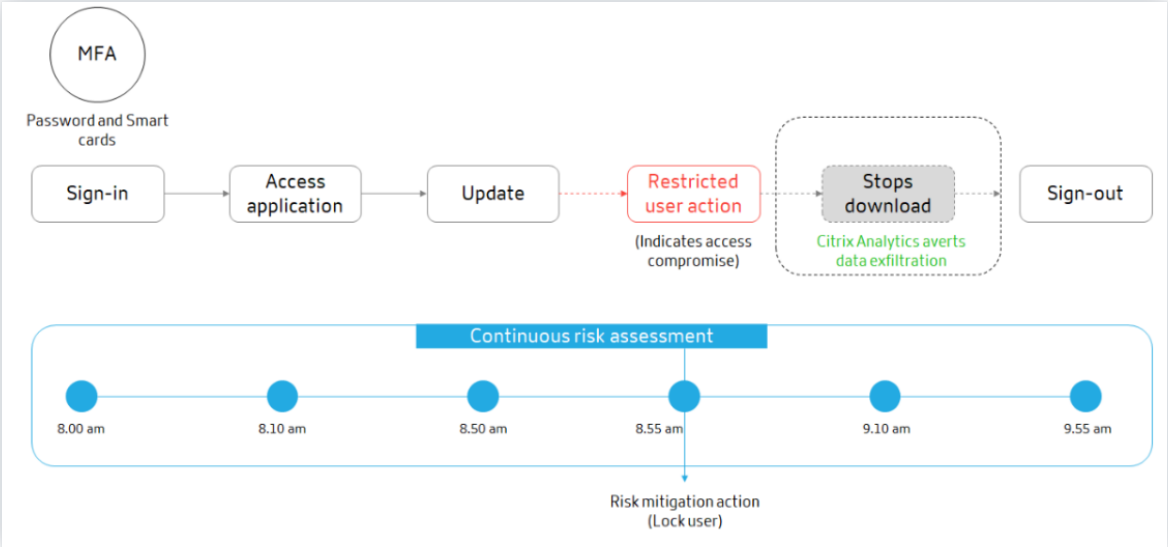
新增功能

持续的风险评估　Citrix Workspace 用户面临的一些挑战是，远程访问会通过数据泄露、盗窃、故意破坏和服务中断等网络犯罪事件使敏感数据面临安全风险。组织内的员工也可能为这种损害做出贡献。

解决这些风险的一些方法是实施多重身份验证、强制短登录超时等。尽管这些风险评估方法可确保更高级别的安全性，但在初始验证后它们并不能提供完全的安全性。

为了增强安全性并确保更好的用户体验，Citrix Analytics 推出了持续风险评估解决方案。此解决方案可帮助您持续监视用户配置文件，并在检测到风险事件时采取各种措施。

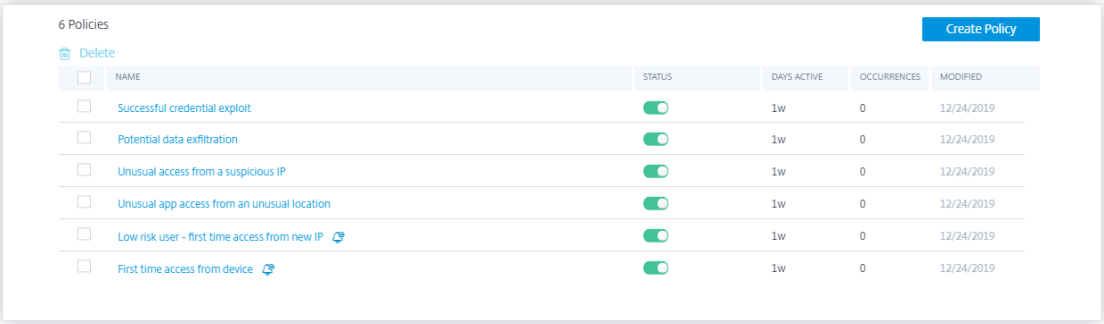
有关详细信息，请参阅 持续风险评估。



策略配置　Citrix Analytics 可帮助您更有效地管理策略配置。借助以下功能，您可以保护用户帐户免受恶意攻击：

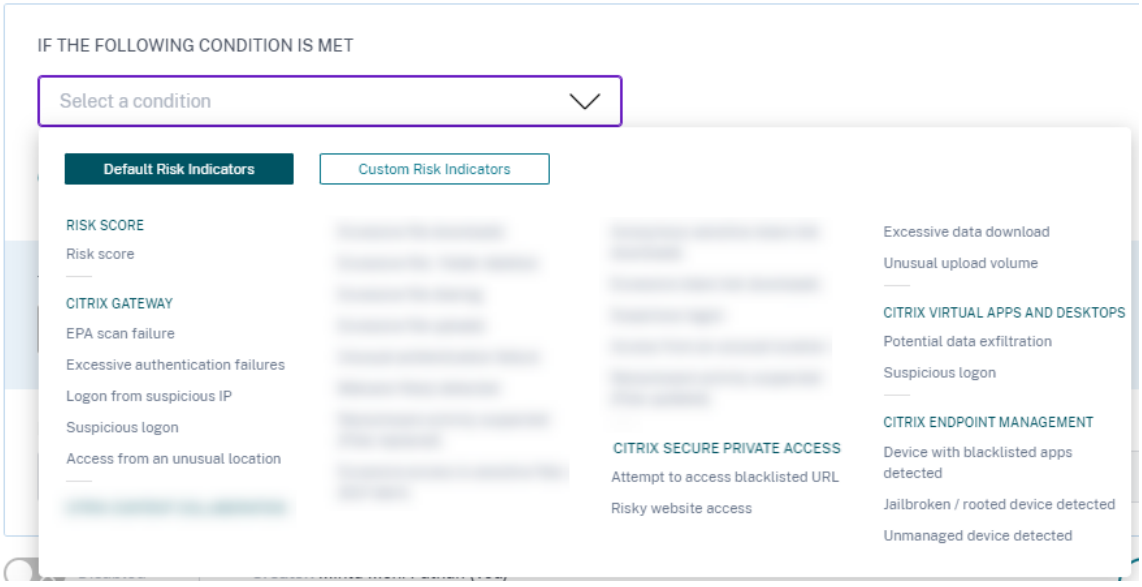
- 默认策略：Citrix Analytics 支持以下默认策略：
  - 成功利用凭据
  - 潜在的数据泄露
  - 来自可疑 IP 的异常访问
  - 来自异常位置的异常应用程序
  - 低风险用户-首次从新 IP 访问
  - 首次从设备访问

  您可以根据自己的要求修改默认策略。

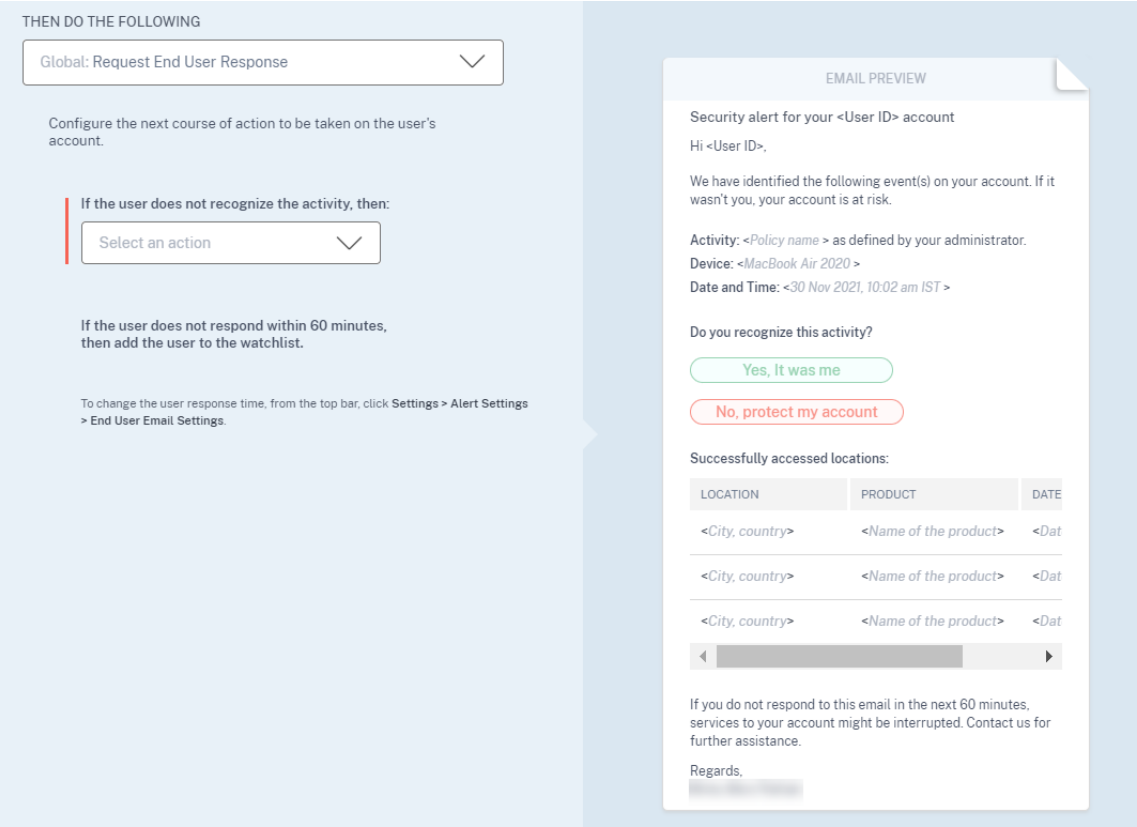


- 多个条件：一个策略最多可以包含四个条件。可以使用风险评分和/或风险指示器的组合来设置条件。

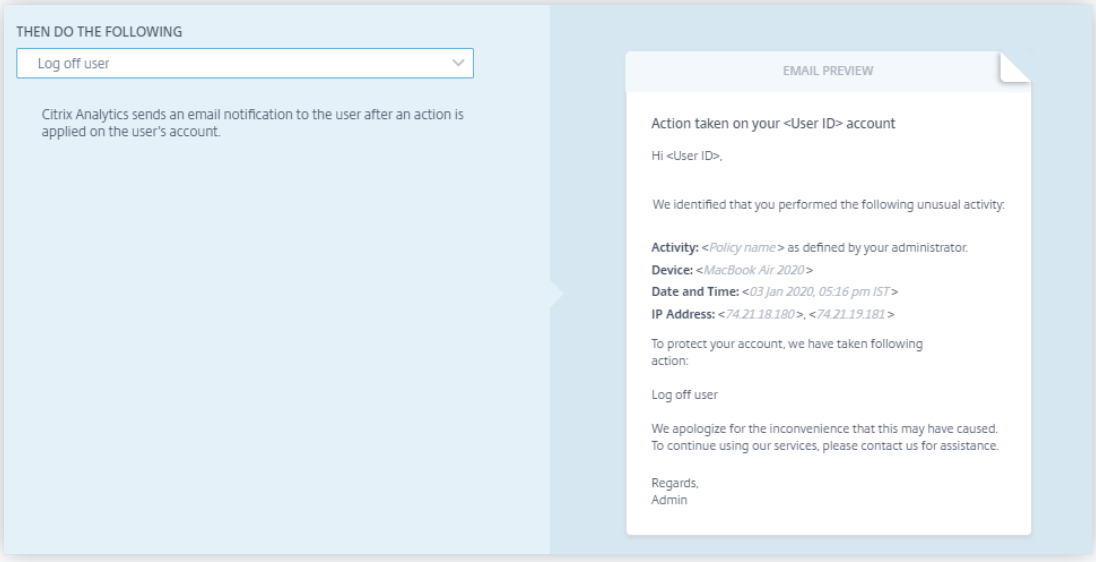
- 默认和自定义风险指示器：创建策略 页面上的条件菜单现在基于默认和自定义风险指示器进行隔离。创建策略时，您可以在默认和自定义风险指示器选项卡之间切换，并设置风险指示器条件。



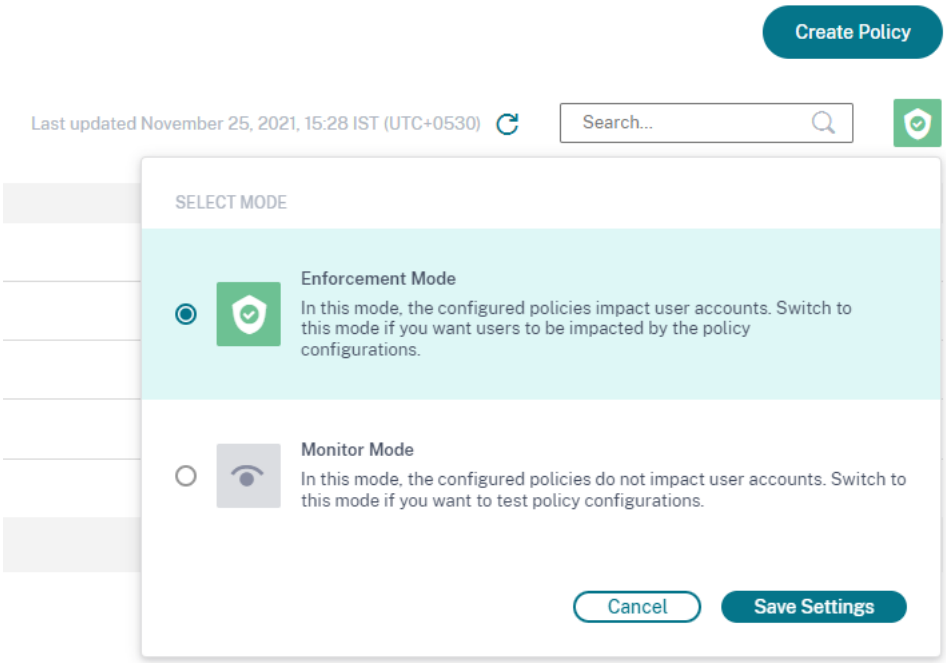
- 请求最终用户响应：Citrix Analytics 引入了 请求最终用户响应 操作。使用此操作，您可以向用户发送有关检测到的风险事件的电子邮件通知。一旦用户对事件做出回应，您就可以确定对其帐户采取的下一步操作。您还可以设置用户响应时间。如果未收到任何响应，Citrix Analytics 会将“无响应”视为状态。



- 应用中断性操作：当应用中断性操作（如 注销用户或锁定用户）时，您可以通知用户。系统会向用户发送通知，其中包含事件和应用操作的详细信息。此操作会暂时中断用户帐户的服务，以防止进一步滥用。要继续访问该帐户，用户必须联系管理员寻求帮助。



- 强制和监视模式：您可以为策略设置实施模式或监视模式。



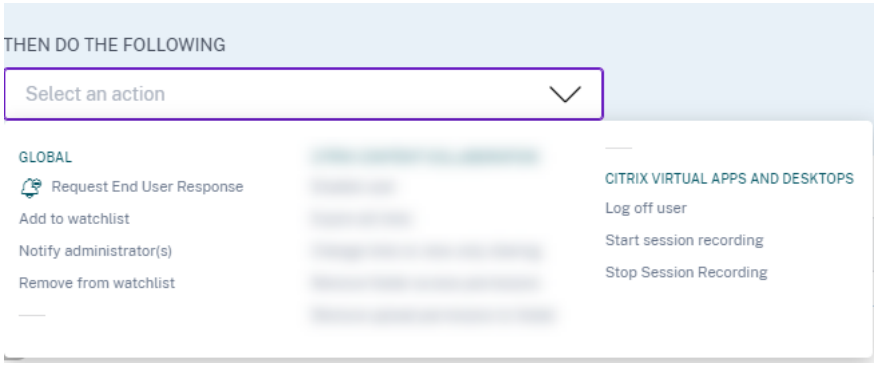
有关策略增强功能的更多信息，请参阅 策略和操作。

锁定用户和解锁用户操作　Citrix Analytics 引入了以下网关操作：

- 锁定用户
- 解锁用户

您可以手动或在配置策略时应用这些操作。

有关详细信息，请参阅 什么是操作。

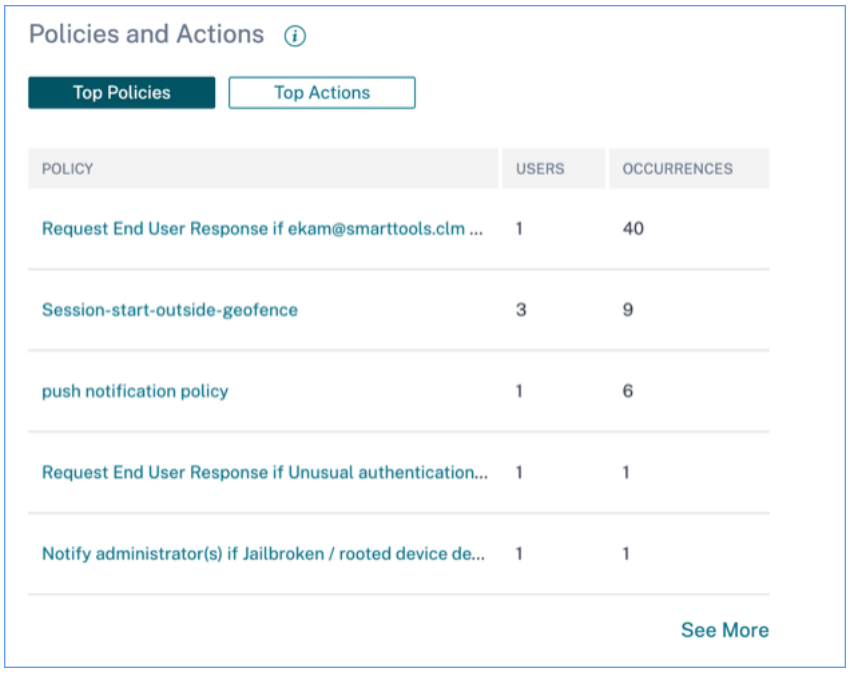


访问摘要控制板　Citrix Analytics 在 用户 控制板上引入了 访问摘要 面板。它汇总了用户尝试访问组织内资源的总次数。

有关详细信息，请参阅 访问摘要。

策略和操作控制板　Citrix Analytics 在 用户 控制板上引入了“策略和操作”面板。它显示应用于用户配置文件的前五个策略和操作。您可以根据所选时间段内的顶级策略和顶级操作对数据进行排序。

有关详细信息，请参阅 策略和操作。



面向策略的自助搜索　使用自助搜索可查看符合定义策略的用户事件。您还可以查看 Analytics 针对这些异常事件应用的操作。使用 facets 和搜索框搜索所需的事件。

要查看事件，请在搜索框中，从列表中选择 策略，选择时间段，然后单击 搜索。

有关详细信息，请参阅面向策略的自助搜索。

已弃用的功能

删除了基于策略的风险评分变更条　配置策略时，您不能再使用基于策略的 风险评分更改 条件。Citrix Analytics 不支持这种情况。

有关详细信息，请参阅 策略和操作。

删除了多个基于策略的操　配置策略时，不能再应用多个操作。Citrix Analytics 仅支持对每个策略执行一项操作。

有关详细信息，请参阅 策略和操作。

已修复的问题

- 委派的只读管理员在访问“用户访问”和“应用程序访问”控制板时遇到错误。[CAS-16297]

2019 年 12 月 12 日

新增功能

Splunk 版本支持　Citrix Analytics 支持以下版本的 Splunk：

- **Splunk 8.0 64** 位
- **Splunk 7.3 64** 位

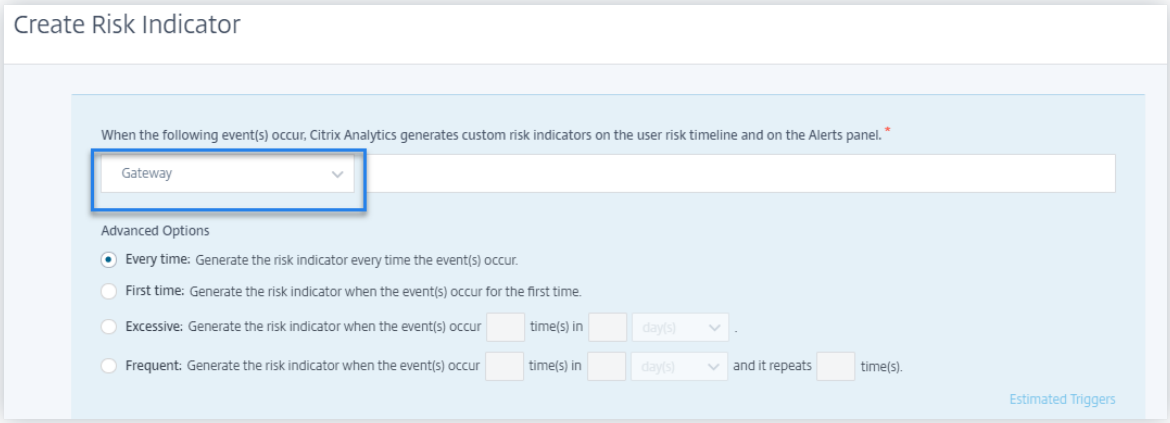
要获得 Splunk 集成的最大安全优势，请从 下载 页面升级到最新版本的 Splunk 附加应用程序。

有关受支持的 Splunk 版本的更多信息，请参阅 支持的版本。

2019 年 12 月 4 日

新增功能

Citrix Gateway 的自定义风险指示器　使用自定义风险指示器，您现在可以定义触发 Citrix Gateway 事件的风险指示器的条件和频率。当用户事件满足条件时，Analytics 会触发风险指示器。有关如何创建自定义风险指示器的更多信息，请参阅 自定义风险指示器。

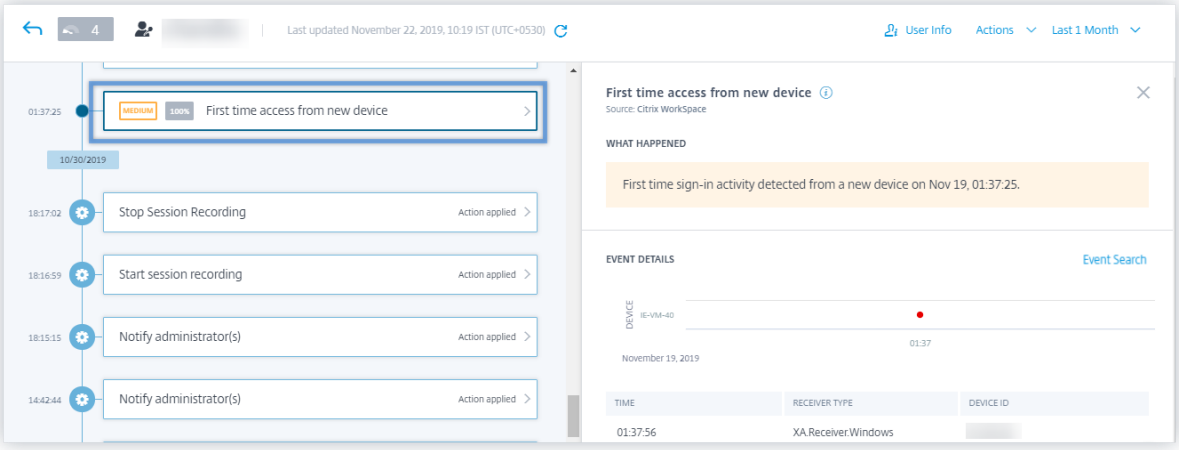


2019 年 **11** 月 **22** 日

新增功能

首次从新设备访问 **- Citrix Virtual Apps and Desktops** 风险指示器　Citrix Analytics 会根据来自新设备的访问权限检测访问威胁，并触发相应的风险指示器。

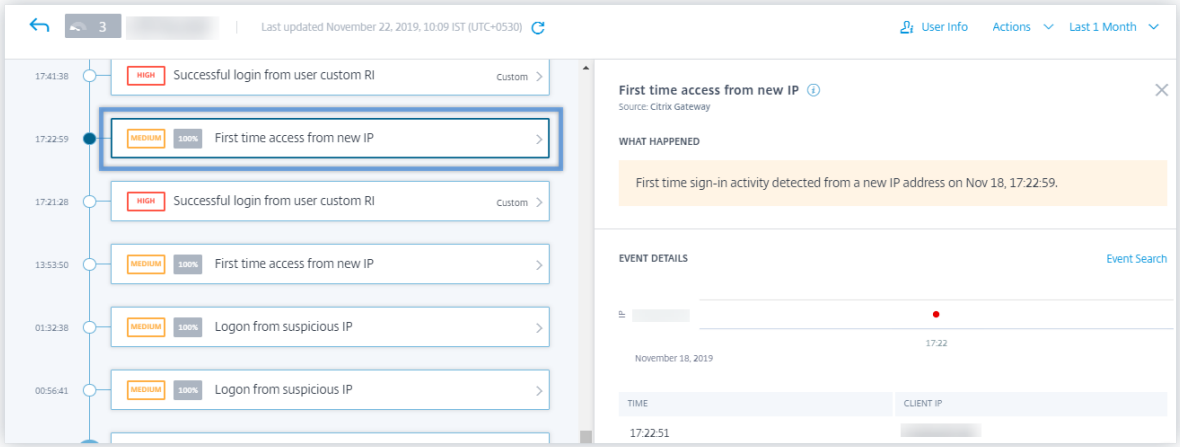
当用户在 90 天后 从设备登录时，将触发首次从新设备访 问风险指示器。触发此事件的原因是 Citrix Receiver 在过去 90 天内没有来自此新设备或陌生设备的登录记录。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 风险指示器。



首次从新 **IP** 访问 **- Citrix Gateway** 风险指示器　Citrix Analytics 会根据来自新 IP 地址的访问来检测访问威胁，并触发相应的风险指示器。

当用户在 90 天后 从 **IP** 地址登录时，将触发首次从新 **IP** 风险指示器访 问。触发此事件的原因是 Citrix Receiver 在过去 90 天内没有来自新 IP 地址或陌生 IP 地址的登录记录。

有关详细信息，请参阅 Citrix Gateway 风险指示器。

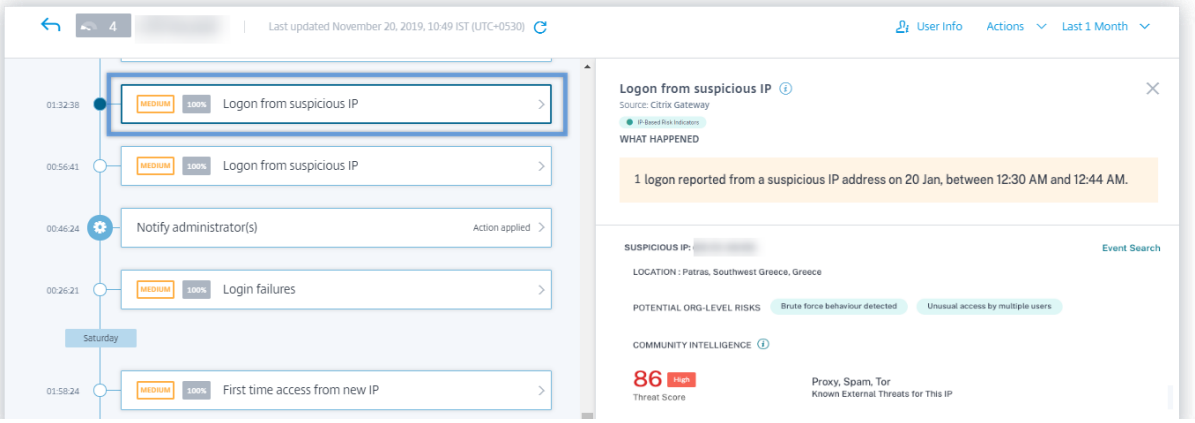


从可疑 **IP** 登录 **- Citrix Gateway** 风险指示器　Citrix Analytics 会根据可疑 IP 登录事件检测用户访问威胁，并触发 从可疑 **IP** 登录 风险指示器。

当用户尝试从可疑 IP 地址访问网络时，会触发此风险指示器。Analytics 根据以下任何一种情况将 IP 地址视为可疑地址：

- 在外部 IP 威胁智能源上列出
- 有来自异常位置的多个用户登录记录
- 登录尝试失败过多，可能表明存在暴力攻击

有关详细信息，请参阅 Citrix Gateway 风险指示器。



自助搜索 **Citrix Gateway** 事件　使用自助搜索功能深入了解从 Citrix Gateway 数据源接收的用户事件。Citrix Analytics 接收 Citrix Gateway 用户的身份验证阶段、授权类型、VPN 会话代码、VPN 会话状态等事件。使用 facets 和搜索框搜索所需的事件并浏览基础数据。

要查看事件，请在搜索框中，从列表中选择 网关，选择时间段，然后单击 搜索。

有关详细信息，请参阅 网关的自助搜索。

自助搜索 **Citrix Remote Browser Isolation** 事件　使用自助搜索功能深入了解从 Citrix Remote Browser Isolation 服务收到的浏览事件。Citrix Analytics 为每个用户连接接收会话连接、会话启动、已发布的应用程序、已删除的应用程序等事件。使用搜索框搜索所需的事件并浏览基础数据。

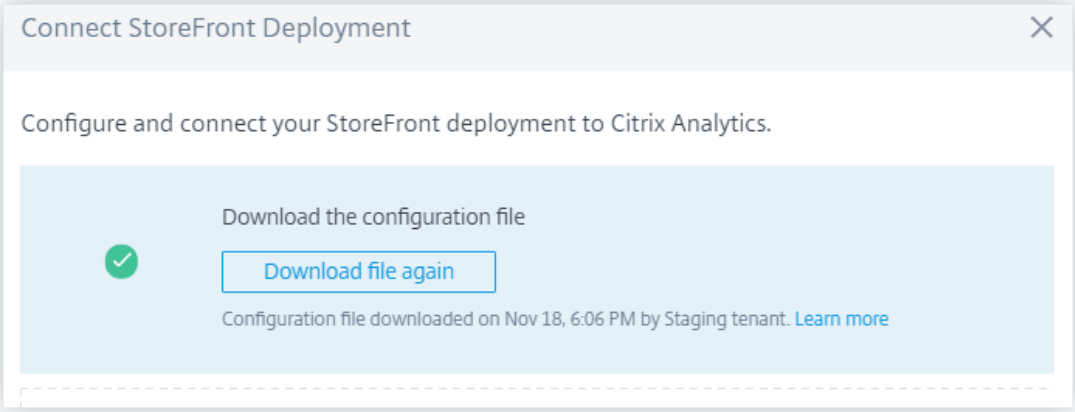
要查看事件，请在搜索框中从列表中选择“**Remote Browser Isolation**”，选择时间段，然后单击“搜索”。

有关详细信息，请参阅自助搜索 Remote Browser Isolation。

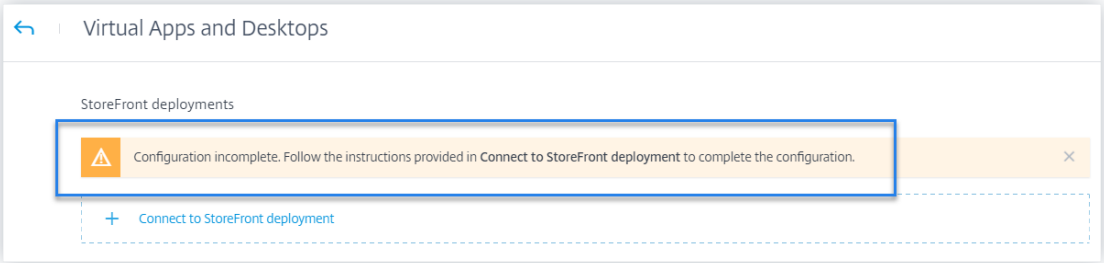
从监视名单中删除操作　您可以通过应用手动方法或应用基于策略的方法将用户从监视名单中删除。有关详细信息，请参阅 监视名单。

改进了配置 **StoreFront** 部署时的载入信息　Citrix Analytics 现在提供以下消息来帮助您配置 StoreFront 部署：

- 下载配置文件后，您会看到一条消息，指示下载的日期和时间以及用户名。刷新此页面时，“下载文件”按钮将再次变为“下载文件”。



- 如果您的 StoreFront 配置不完整，您会看到一条警告消息，指示您按照配置步骤操作并将 StoreFront 部署与 Analytics 连接起来。



有关如何配置 StoreFront 部署的详细信息，请参阅使用 StoreFront 在本地部署 Citrix Virtual Apps and Desktops 站点。

已弃用的功能

风险指示器-从新设备访问删除　Citrix Analytics 不再触发“从新设备访问”风险指示器。但是，在用户控制板、用户时间轴和策略控制板上，您可以查看与此风险指示器相关的历史数据。

对于之前基于 从新设备访问创建的策略，您必须修改策略或使用新的风险指示器创建策略 首次从新设备进行访问。

已修复的问题

- 用于身份验证的自助搜索无法显示事件。[CAS-24959]

2019 年 11 月 8 日

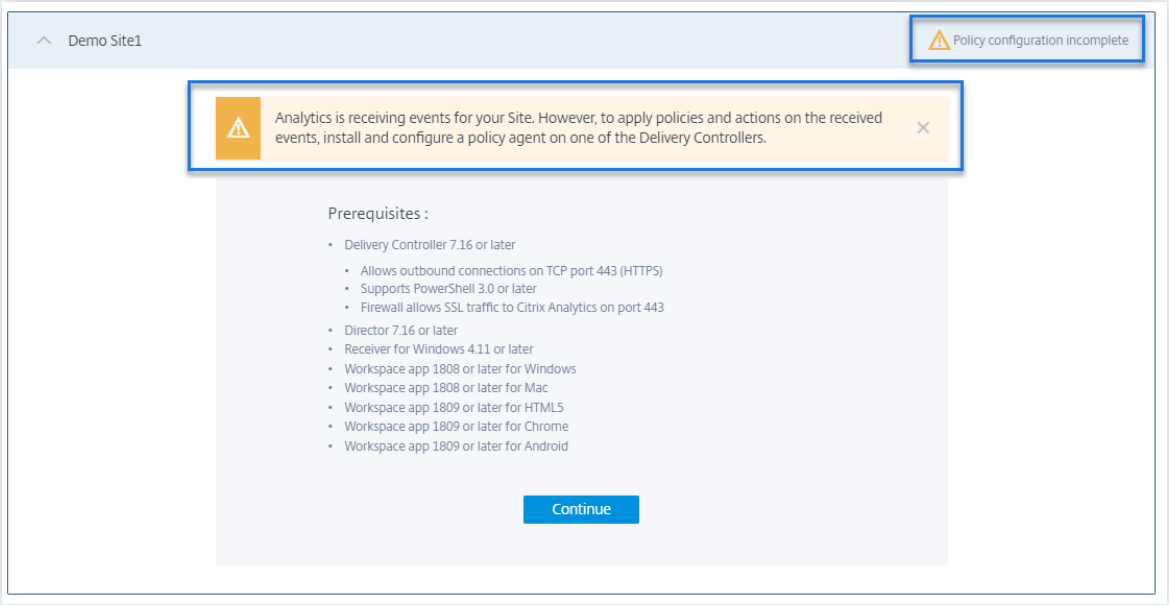
已修复的问题

- 对于 Citrix Content Collaboration 风险指示器，用户无法在风险时间表上应用操作。[CAS-24844]
- 适用于 Chrome 的 Citrix Workspace 应用程序 1911 版之前无法将事件详细信息发送到 Citrix Analytics。[CAS-24938]

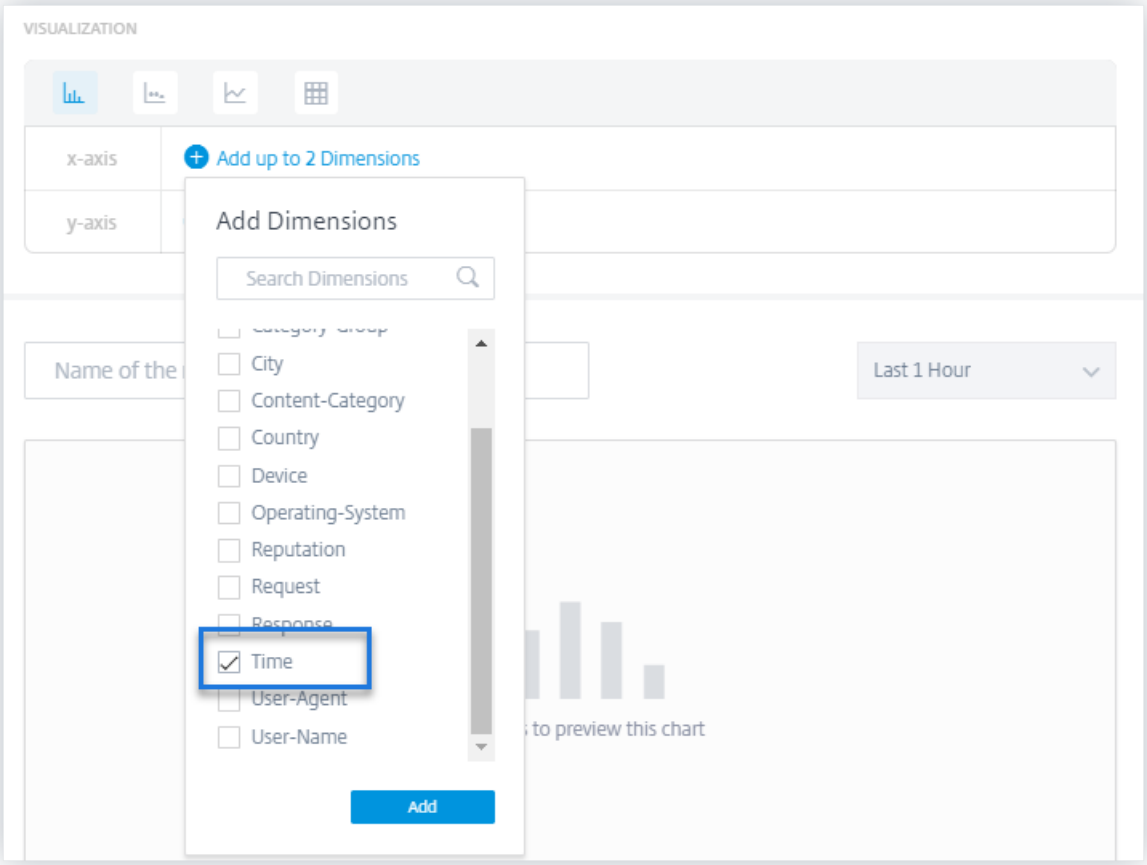
2019 年 10 月 21 日

新增功能

已修改分析代理的名称　现在，代理名称在用户界面上被称为 **Analytics** 策略代理，以表示其角色。载入本地 Citrix Virtual Apps and Desktops 数据源时，Citrix Analytics 会明确通知，只需要策略代理来配置站点的策略和操作。此代理在从数据源传输数据方面没有任何角色。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源。



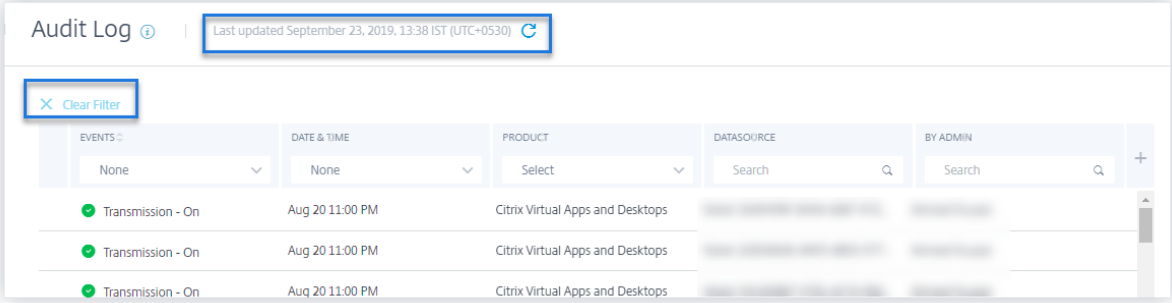
支持自定义报告的时间维度　现在，您可以通过选择 x 轴的时间维度，根据 时间 对事件进行分组。该报告根据所选时段的时间间隔显示接收的事件总数。有关如何创建报告的更多信息，请参阅 自定义报告。



审核日志的增强　审核日志 页面的用户体验得到了增强。

- 您可以查看上次更新 审核日志 页面的日期和时间详细信息，并刷新页面以查看最新的审核日志。
- 您可以清除审核日志中应用的所有筛选器。

有关审核数据的更多信息，请参阅 审核日志。



已修复的问题

- 即使 Microsoft Graph 安全性已成功加入，Citrix Analytics 仍无法生成匿名 **IP** 地址风险指示器。[CAS-21329]
- 版本 1910 之前的适用于 HTML5 的 Citrix Workspace 应用程序无法将事件详细信息发送到 Citrix Analytics。[CAS-24938]

2019 年 **9** 月 **23** 日

已修复的问题

- 在数据源站点卡片上，“最新事件”字段显示的日期和时间信息不正确。[CAS-24087]

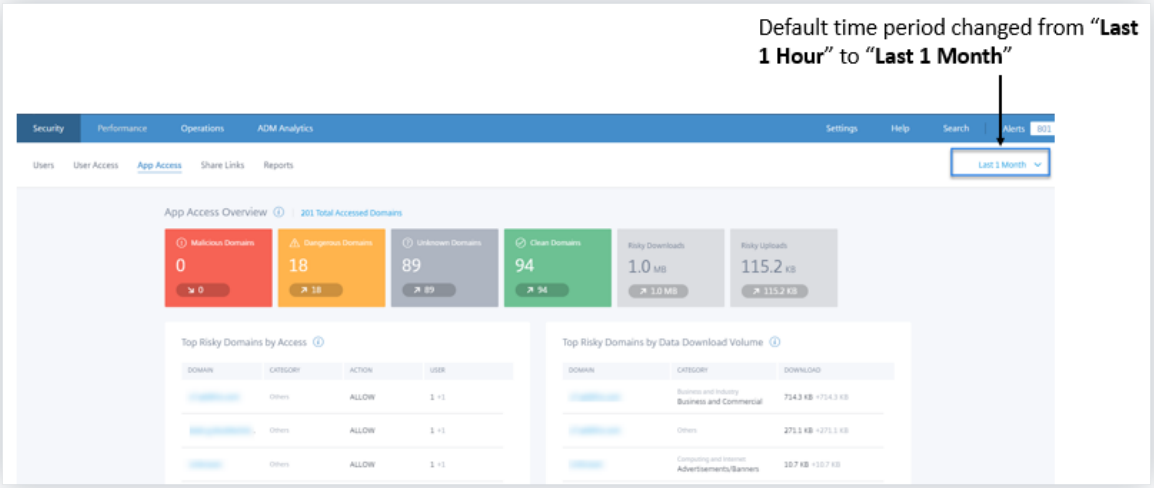
2019 年 **8** 月 **30** 日

新增功能

控制板之间默认时间段的更改　以下控制板上的默认时间段从“过去 **1** 小 时”更改为“最近 **1** 个月”：

- 用户
- 风险时间表
- 用户访问权限
- 应用程序访问
- 分享链接
- 警报历史

现在，控制板默认显示过去一个月的事件。使用这些控制板时，您将获得更具吸引力的体验。例如，当您打开“应用程序访问”控制板时，控制板会默认显示最近一个月的应用程序访问事件。



已修复的问题

- 对于 Content Collaboration 风险指示器，无法成功应 用禁用基于用户 策略的操作。[CAS-17304]
- Citrix Analytics 无法处理来自 Citrix Gateway 13.0 的事件。出现此问题的原因是 Citrix Gateway 13.0 无法在发送到 Citrix Analytics 的登录事件中提供用户名。[CAS-21339]

2019 年 8 月 20 日

新增功能

自助式搜索增强

- 自助服务页面的用户体验得到了增强。现在，您可以在用户风险时间表和自助搜索页面之间来回无缝切换。
- 现在，您可以按时间对事件进行排序。默认情况下，最新的事件首先出现在事件表中。单击“时间”列上的排序图标可以根据最新时间或最早时间对事件进行排序。

有关如何使用自助搜索的详细信息，请参阅 自助搜索。

自定义报告增强

- 为访问控制、Content Collaboration 以及 Apps and Desktops 数据源添加了新维度。您可以选择这些维度来创建报告。为数据源添加了以下维度：
  - 访问控制：用户代理、用户名
  - **Content Collaboration**：用户电子邮件、用户名、创建者、帐户 ID、OAuth 客户端 ID、事件 ID、文件夹 ID、文件夹名称、资源 ID、表单 ID、客户端 IP

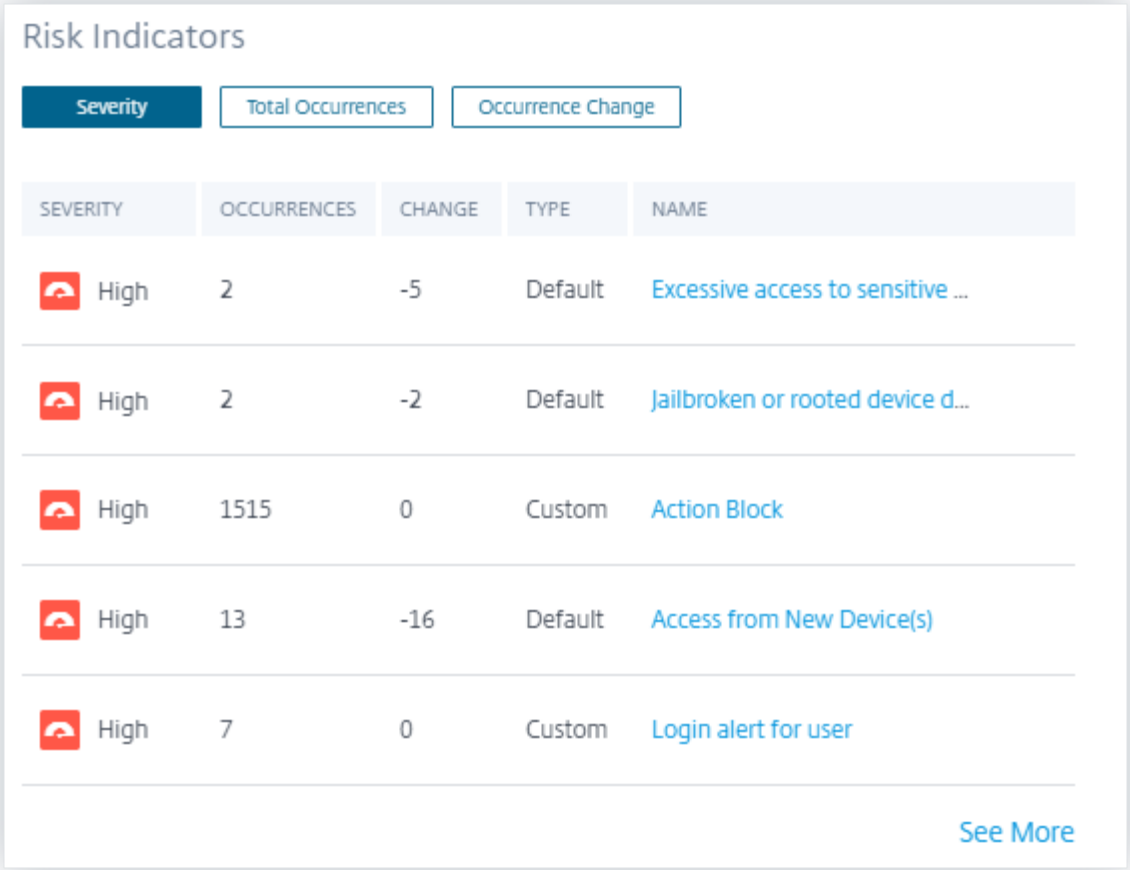
  - 应用程序和桌面：用户名、IP 地址、设备 ID、越狱、会话启动类型、会话服务器名称、会话用户名、下载文件名、下载文件路径、打印打印机名称、打印作业详细信息文件名、SaaS 应用程序启动 URL、剪贴板操作、剪贴板详细信息结果

- 自定义报告用户界面增强了对分页的支持和筛选器的 全部清除 选项。

有关如何使用这些维度创建自定义报表的更多信息，请参阅 自定义报表。

风险指示器控制板　风险指示器 控制板在 用户 页面上介绍。它总结了用户的前五个默认和自定义风险指示器。查看更多链接将您重定向到 风险指示器概述 页面。此页面提供有关在选定时间段内生成的风险指示器的详细信息。

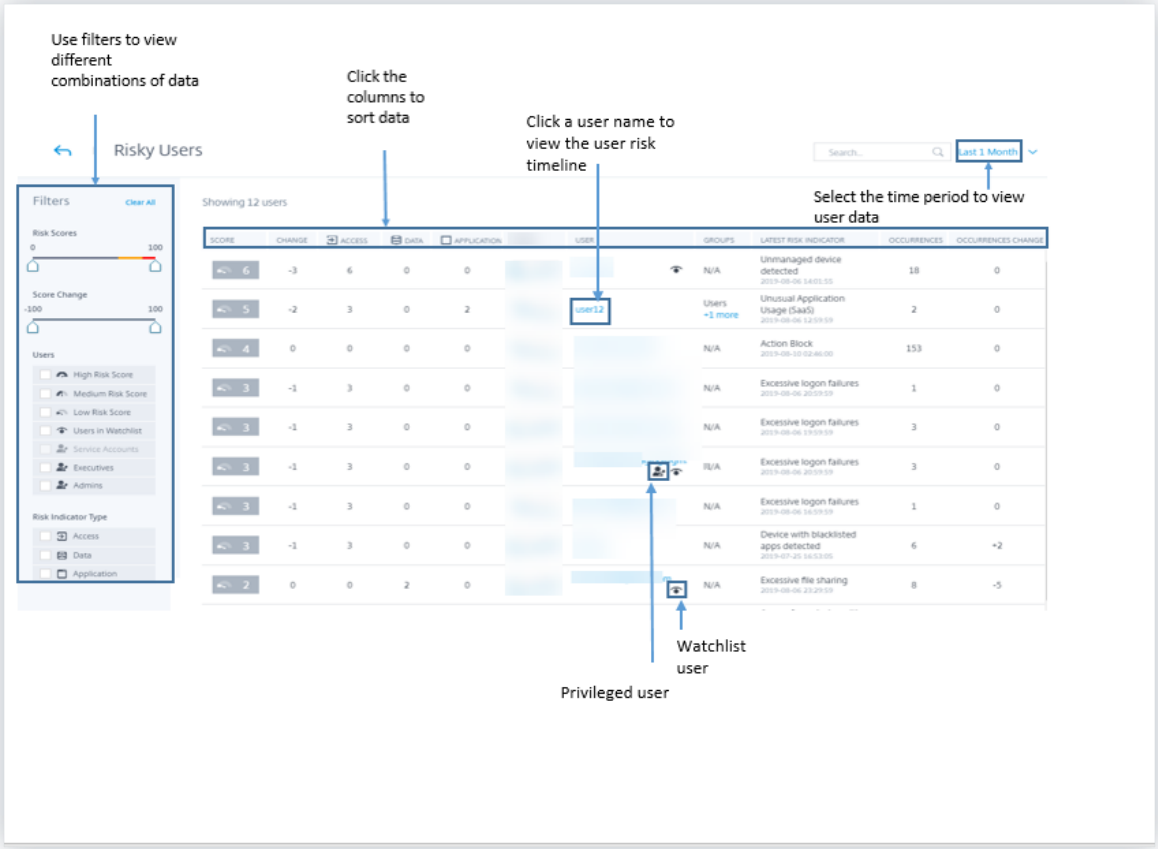
有关详细信息，请参阅 用户控制板。



风险用户控制板增强　Citrix Analytics 在 风险 用 户控制板上引入了风险指示器和风险指示器更改选项卡。您可以根据这些选项卡查看风险最高的五个用户。控制板还引入了“风险指示器”列。它显示了用户的风险指示器的数量。

风险用户页面介绍了“发生次数”和“发生次数更改”。这些列汇总了自定义和默认风险指示器的总发生次数和发生次数的变化。

有关详细信息，请参阅用户控制板。



共享链接风险指示器-下载量过多　Citrix Analytics 会根据共享链接上的过多下载来检测访问威胁，并触发下 载过多风险指示器。通过根据以前的行为识别下载量过多的共享链接，您可以监视共享链接是否存在潜在的攻击。此风险指示器可帮助您识别过多的文件下载事件。

有关详细信息，请参阅 下载量过多。

自助搜索身份验证数据　使用自助搜索功能深入了解身份验证事件。Citrix Analytics 从 Citrix Cloud 的身份和访问管理服务接收身份验证事件，例如用户登录、用户注销和客户端更新。搜索提供有关身份验证事件的详细报告，帮助您识别任何身份验证问题并进行故障排除。您还可以定义搜索查询以检索符合定义条件的事件。

要查看事件，请从列表中选择 身份验证，选择时间段，然后单击 搜索。

有关详细信息，请参阅 自助搜索身份验证。

2019 年 7 月 11 日

新增功能

自定义风险指示器　Citrix Analytics 生成的默认风险指示器基于计算机学习算法。Citrix Analytics 现在允许您创建自定义风险指示器。根据用户事件，您可以定义条件并创建自定义风险指示器。

满足定义的条件后，Citrix Analytics 会生成类似于默认风险指示器的自定义风险指示器，并将其显示在用户的风险时间表中。自定义风险指示器在用户的风险时间线上标注。

有关详细信息，请参阅自定义风险指标。

风险时间表上的特权状态

每当用户的 Admin 或 Executive 权限状态发生更改时，用户风险时间表都会显示以下事件：

- 已添加到执行组
- 已从执行组中删除
- 权限提升为管理员
- 管理员权限已移

当为用户触发风险指示器时，您可以将其与指定的权限状态更改事件关联起来。如有必要，您可以对用户配置文件应用适当的操作。

有关详细信息，请参阅 用户风险时间表。

过期共享链接操作

Citrix Analytics 使您能够对共享链接风险指示器应用操作。目前，支持的操作是 **Expire** 共享链接。

有关详细信息，请参阅 Citrix 共享链接风险指示器。

自助式搜索增强

- * 在搜索查询中支持通配符 **：使用搜索查询中的星号 (*) 字符匹配任何字符零次或多次。例如，搜索查询用户名 = “John*” 显示以 John 开头的所有用户名的事件。
- 为面添加了“全部清除”选项：单击“全部清除”以一次移除所有选定面。
- 查看事件列表中的隐藏列数据：从事件表中移除列后，可以在用户事件列表中查看对应的数据。展开用户的事件行并查看数据。

有关详细信息，请参阅 自助搜索。

站点卡上的数据错误状态

当 Citrix Analytics 在过去一小时内 未从数据源接收 事件时，站点卡片将以红色显示“未收到数据”标签。它还显示收到的事件数量，并链接到相应的自助搜索页面。此功能可帮助您在自助搜索页面上查看相应的事件，并检查是否存在任何数据传输问题。

> 注意
>
> 目前，自助搜索仅适用于 Access、Content Collaboration 以及 Apps and Desktops 数据源。

有关详细信息，请参阅 在 Citrix 数据源上启用分析。

已修复的问题

- 对于访问控制数据源，站点卡片上的事件数与自助搜索结果不匹配。[CAS-18286]

2019 年 6 月 19 日

已修复的问题

- 每次发现 Active Directory 数据源时，“审核日志”页面都会显示数据传输的打开或关闭状态。[CAS-17575]
- 用户 控制板上的时间段菜单无法准确加载。它显示一条超时错误消息。[CAS-19467]
- 从 Splunk 连接到租户时，用户会在 Citrix Analytics 上收到错误消息。有时，新数据源的载入会失败。[CAS-19429]

2019 年 6 月 17 日

新增功能

StoreFront 配置

如果您的组织使用本地 StoreFront，则现在可以将 StoreFront 配置为连接到 Citrix Analytics。使用从 Citrix Analytics 导入的配置文件执行配置。配置成功后，Citrix Workspace 应用程序会将用户事件发送到 Citrix Analytics，以生成有关用户行为的可操作见解。这些见解可帮助您检测任何异常的用户行为，并主动处理组织中的安全威胁。有关详细信息，请参阅使用 StoreFront 登录 Citrix Virtual Apps and Desktops 本地站点。

2019 年 5 月 30 日

新增功能

登录失败过多

Citrix Analytics 会根据过多的登录事件检测访问威胁，并触发登录失败过多风险指示器。当用户遇到多次访问 Content Collaboration 失败的登录尝试时触发此风险指示器。通过根据以前的行为识别登录失败过多的用户，管理员可以监视用户帐户的暴力攻击。

> 注意
>
> 过多的登录失败现在被重命名为身份验证失败过多。

已修复的问题

- 对于 Citrix Workspace 应用程序传输的某些用户事件，数据源被错误地标识为 Endpoint Management，而不是 Citrix Virtual Apps and Desktops。

  [CAS-17323]

- 在 过去 **1** 个月 的时间段内，用户 控制板需要很长时间才能加载。当用户数量很多时，会出现此问题。在某些情况下，您甚至可能会遇到 601 个错误。

  [CAS-16300]

- 尽管有些用户在 Citrix Cloud 上订阅了 Citrix Content Collaboration 服务，但不会将 Citrix 内容协作作为数据源进行发现。

  [CAS-16299]

2019 年 5 月 9 日

新增功能

创建自定义报告

现在，您可以根据自己的操作要求创建自定义报告。Citrix Analytics 根据所选数据源提供维度和指示器列表。选择所需的参数和可视化类型，例如条形图、事件图、折线图或表格来创建报表。创建报告可帮助您以图形方式组织和分析数据。

要创建自定义报告，请从“安全”选项卡中单击“报 告”>“创建报告”。要查看以前创建的报告，请在“安 全”选项卡中单击“报告”。有关详细信息，请参阅 自定义报告。

特权用户监视

Citrix Analytics 使您能够密切监视组织中特权用户的行为异常情况。由于特权用户非常容易受到安全威胁的攻击，因此区分他们的日常事件和恶意事件变得具有挑战性。因此，长期以来，特权用户的恶意事件一直未被发现。此功能使您能够主动监视此类事件，并对相应的用户帐户采取适当的操作。特权用户在“用户”控制板上 用 一个图标表示。

Citrix Analytics 支持对以下类型的特权用户进行监视：

- 管理员-由相应 **Citrix** 服务分 配管理员权限的用户。目前，Citrix Analytics 支持对 Content Collaboration 服务中具有管理员权限的用户进行特权用户监视。
- 管理人员 -在 Citrix Analytics 上，您可以将 AD 组标记为管理人员组。将 AD 组标记为执行组会使该组中的所有用户成为特权用户。如果不需要进一步支持 AD 组中用户的行为异常，则可以将该组作为执行组删除。

有关详细信息，请参阅 特权用户。

每周电子邮件摘

Citrix Analytics 每周向管理员发送一封电子邮件，总结其组织 IT 环境中的安全风险暴露。电子邮件通知每周二发送给管理员，并突出显示上周发生的安全事件。此电子邮件可确保管理员在不登录 Citrix Analytics 的情况下获悉安全风险暴露。有关详细信息，请参阅每周电子邮件摘要。

2019 年 **4** 月 **26** 日

新增功能

委派管理员

Citrix Analytics 现在支持委派管理员角色。通过此功能，您可以邀请其他管理员加入您的 Citrix Cloud 帐户，以便为您的组织管理 Citrix Analytics。如果您是具有完全访问权限的 Citrix Analytics 管理员，则可以将其他管理员添加到 Citrix Cloud 帐户。这些额外的管理员称为委派管理员。您当前可以向委派管理员分配只读访问权限。有关详细信息，请参阅 委派管理员。

已修复的问题

很少有使用数据流的数据源的风险指示器不会生成警报。如果触发了以下任一风险指示器，则不会收到任何警报通知，也不会自动应用基于策略的操作：

- **Citrix Endpoint Management** 风险指示器 - 非托管的设备、已越狱或获得 root 权限的设备以及具有黑名单应用程序的设备。
- **Citrix Virtual Apps and Desktops** 风险指示器 - 从操作系统 (OS) 不受支持的设备进行访问。

- **Citrix Content Collaboration** 风险指示器 -对敏感文件的过度访问。

[CAS-14590]

2019 年 **2** 月 **19** 日

新增功能

Splunk 集成

Citrix Analytics 与 Splunk 集成，以增强您的安全事件监视和故障排除体验。此集成利用 Citrix Analytics for Security 的风险分析功能和智能（如风险指示器、风险评分和用户配置文件），增强了现有的数据源。Citrix Analytics 将风险分析信息导出到频道。Splunk 从这个频道中提取了同样的内容。

Splunk 集成包括在 Citrix Analytics 上进行配置、安装适用于 **Splunk** 的 **Citrix Analytics** 加载项应用程序以及应用程序的配置。请确保为至少一个数据源启用数据处理。它可以帮助 Citrix Analytics 开始 Splunk 集成过程。

有关详细信息，请参阅 Splunk 集成。

动态会话录制　Citrix Analytics 引入了在用户当前 Virtual Apps and Desktops 会话上动态触发会话录制的功能。它有助于捕获风险分析所需的证据，并采取适当的事件响应措施，例如断开会话连接和阻止用户。

有关详细信息，请参阅 策略和操作。

共享链接控制板和风险指示器　Citrix Analytics 基于从 Citrix Content Collaboration 收集的数据引入了共享链接的风险可见性。它可以通过共享链接触发的风险指示器帮助您了解共享链接的风险敞口。

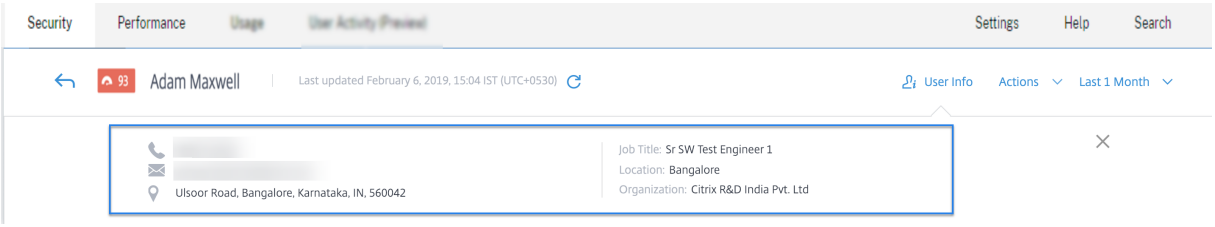
有关详细信息，请参阅 共享链接控制板。

目前，针对共享链接触发匿名敏感共享下载风险指示器。当 Content Collaboration 检测到此危险行为时，Citrix Analytics 会收到事件。您将在“警报”面板中收到通知，并且匿名敏感共享下载风险指示器将添加到共享链接的风险时间表中。

有关详细信息，请参阅 共享链接风险时间表 和 Citrix Share Link 风险指示器。

Microsoft Active Directory 集成　现在，您可以将 Microsoft Active Directory 与 Citrix Analytics 集成。这种集成通过职称、组织、办公地点、电子邮件和联系方式等其他信息增强了风险用户的环境。您可以在 Citrix Analytics 的用户配置文件页面上更好地了解用户。

有关详细信息，请参阅 将分析与 Microsoft Active Directory集成。



2019 年 1 月 4 日

新增功能

为现有风险指示器添加 **SOURCE** 列　在事件详细信息部分中引入了以下风险指示器的来源列：

- 文件上载过多
- 文件下载过多
- 过多的文件共享
- 删除过多的文件或文件夹

有关详细信息，请参阅 Citrix Content Collaboration 风险指示器。

高级用户资料　用 户配置文件上的“用户信息”视图已得到增强。趋势视图 链接已在应用 程序、设备和 数据使用情况部分的右上角引入。“地 图视图”链接已在“位置”部分的右上角引入。这些链接提供了有关用户在特定时间段内历史行为的图形表示。您可以从用户的风险时间表或从“数据源”页面导航到“用户信息”。

> 注意
>
> 身份验证和域数据当前在用户信息配置文件中不可用。

有关详细信息，请参阅用户风险时间表和配置文件。

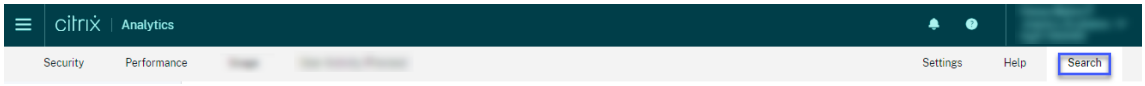
Microsoft Graph 安全性风险指示器　已加入的 Microsoft Graph 安全性可以从以下安全提供商之一接收风险指示器详细信息，然后将其转发给 Citrix Analytics：

- Azure AD 身份保护
- Microsoft Defender for Endpoint

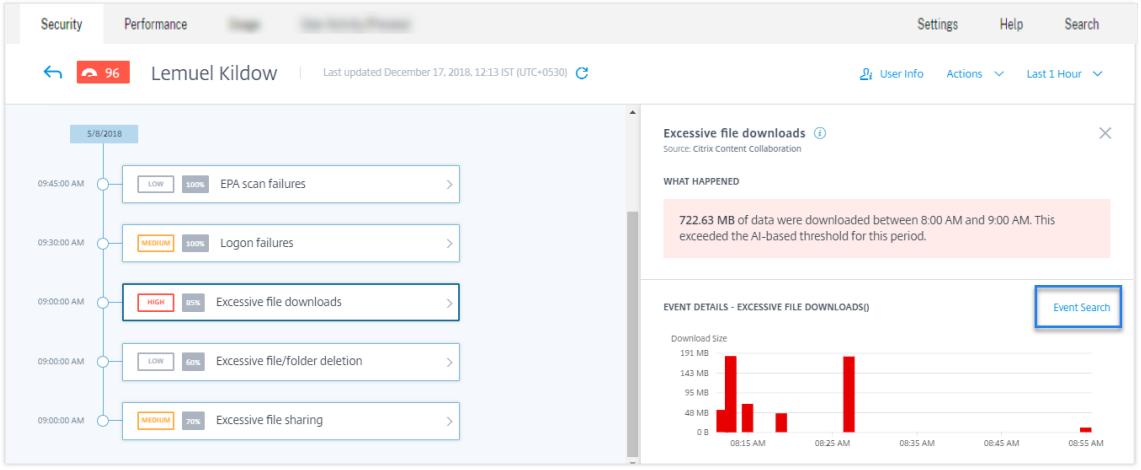
有关详细信息，请参阅 Microsoft Graph 安全性风险指示器。

进入自助搜索页面的方法　现在，您可以使用以下选项访问自助搜索页面：

- 顶栏：单击顶部栏上的 搜索 可直接访问搜索页面。



- 用户资料页面上的风险时间表：单击 事件搜 索可访问搜索页面并查看与特定用户的风险指示器和数据源对应的事件。有关详细信息，请参阅 自助搜索。



自助搜索 **Content Collaboration**　使用自助搜索来深入了解与 Content Collaboration 数据源关联的事件。要查看事件，请从列表中选择 **Content Collaboration**，选择时间段，然后单击搜索。
有关详细信息，请参阅 Content Collaboration 的自助搜索。

应用程序和桌面的自助式搜索　使用自助式搜索深入了解与应用程序和桌面数据源关联的事件。要查看事件，请从列表中选择 应用程序和桌面，选择时间段，然后单击 搜索。有关详细信息，请参阅应用程序和桌面的自助式搜索。

将自助搜索事件导出到 **CSV** 文件　现在，您可以将自助搜索事件导出为 CSV 文件，然后下载该文件以备将来使用。有关详细信息，请参阅 自助搜索。

改进了 **Citrix Virtual Apps and Desktops** 的载入能力　Citrix Virtual Apps and Desktops 数据源的载入流程现已得到改进，以提供更好的用户体验。现场卡和登机步骤已被修改。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源。

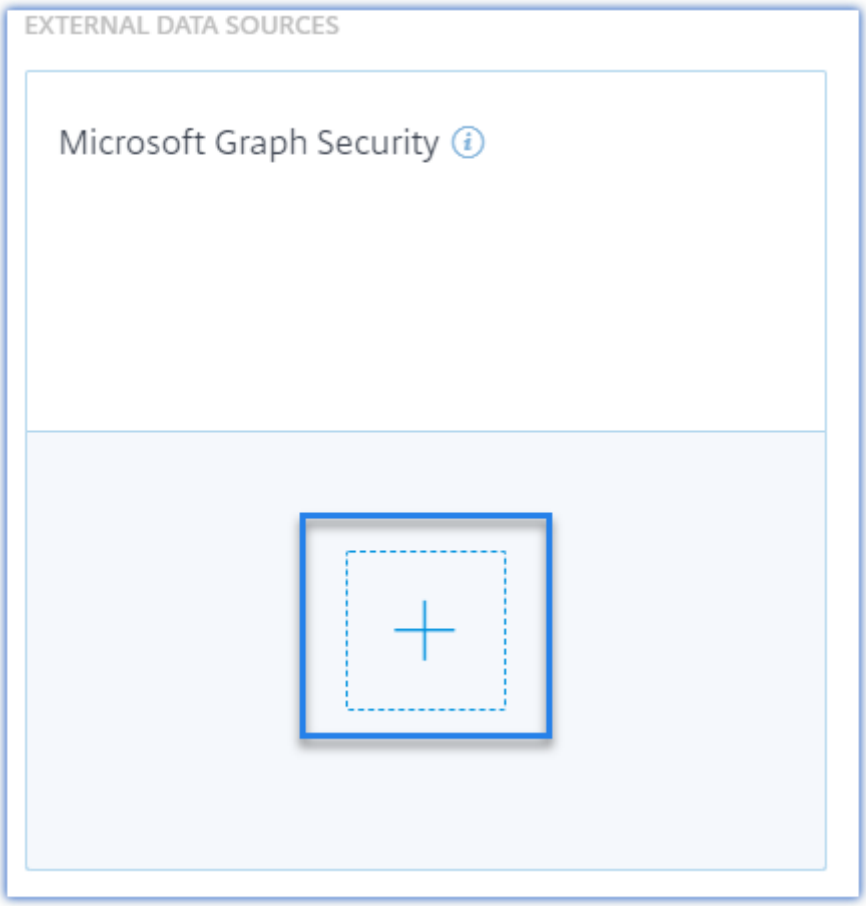
2018 年 **11** 月 **29** 日

新增功能

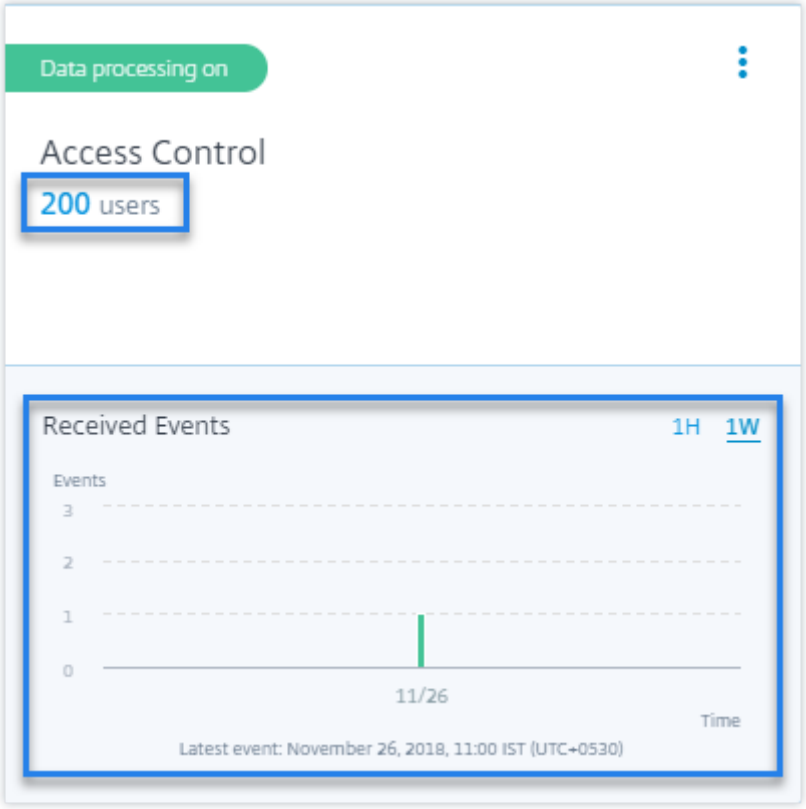
Microsoft Security Graph 数据源　Microsoft Graph 安全性是一个外部数据源，可聚合来自多个安全提供商的数据。它还提供对用户清单数据的访问。

Citrix Analytics 目前支持与此数据源关联的 **Azure AD** 身份保护和 **Microsoft Defender for Endpoint**。

要加载此数据源，您必须从 Microsoft 身份平台获取权限。有关详细信息，请参阅 Microsoft Graph 安全性。



在数据源的站点卡片上查看事件详细信息和发现的用户　数据源的站点卡片现在显示事件详细信息和用户数量。例如，您可以在站点卡片上查看事件详细信息和访问控制的用户。有关详细信息，请参阅对 数据源启用分析。



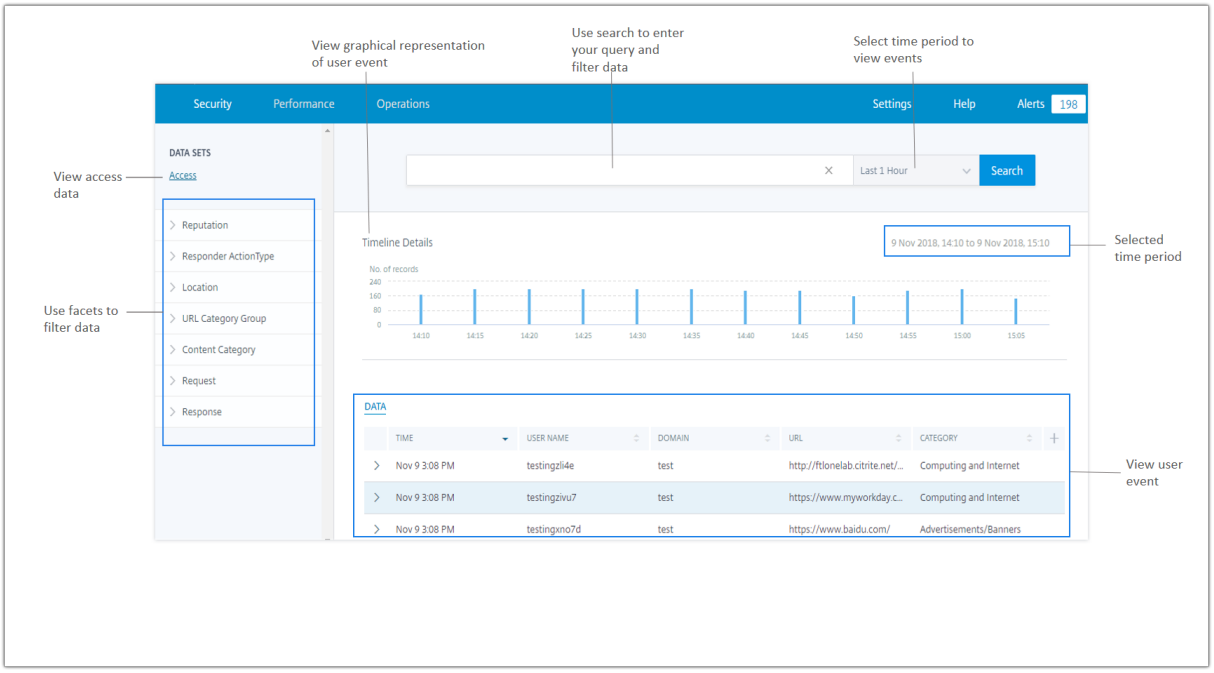
2018 年 **11** 月 **16** 日

新增功能

自助搜索访问数据　您可以使用自助搜索来深入了解企业中用户的访问详细信息。Citrix Analytics 从 Citrix 访问控制服务中收集用户的访问详细信息。使用 Facets 和搜索查询缩小搜索结果的范围。

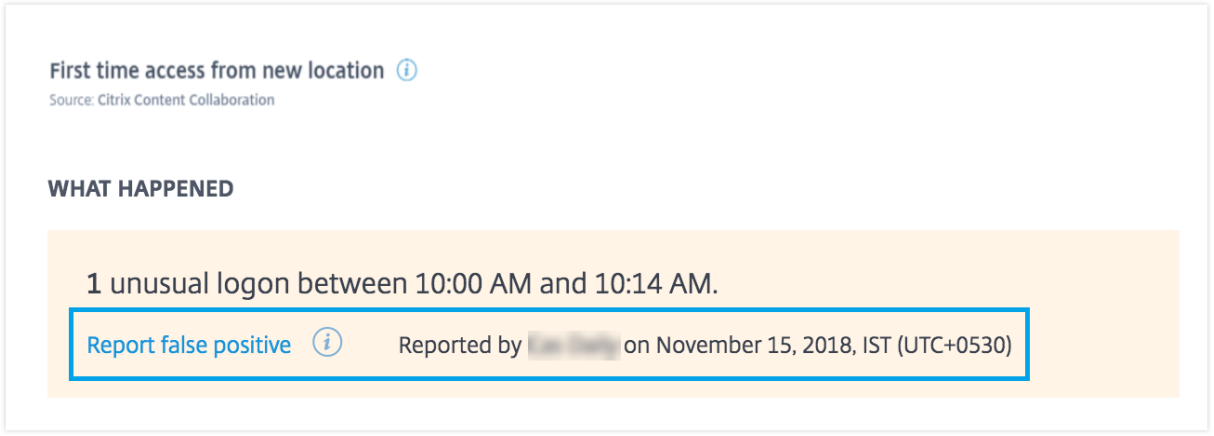
要使用自助搜索页面，请在“安全性”选项卡中单击“事件搜索”。

有关详细信息，请参阅 自助搜索访问权限。



风险指示器反馈　使用 Citrix Analytics 上的风险指示器反馈功能，您可以提供有关风险指示器的反馈。您的反馈有助于确认所报告的安全事件是否准确。

目前，Content Collaboration 数据源触发的 异常登录访问 风险指示器支持此功能。如果触发的此风险指示器不正确，您可以将其报告为误报并提供反馈。您还可以编辑之前提交的反馈。Citrix Analytics 可捕获您的反馈并验证预测信息，以优化异常行为检测。



已修复的问题

- 如果使用 Internet Explorer 11.0 访问 Citrix Analytics，则无法编辑和保存策略。

已知问题

December 7, 2023

Citrix Analytics for Security 存在以下已知问题：

- 通过 Web 浏览器打开应用程序和桌面并从本机客户端上的 ICA 启动时，适用于 Linux 的 Citrix Workspace 应用程序无法向 Citrix Analytics 发送打印事件。[CAS-36238]

  > 注意
  >
  > 有关 Citrix Workspace 应用程序和 Citrix Receiver 在所有平台上的生命周期日期和生命周期阶段（正式发布、维护结束和生命周期终止）的详细信息，请参阅 Citrix Workspace 应用程序和 Citrix Receiver 的生命周期里程碑。

Citrix Analytics 产品

December 7, 2023

Citrix Analytics for Security

整理并提供从客户互联数据源（例如安全私有访问、Citrix 虚拟应用程序和桌面、Citrix DaaS 站点或 NetScaler Gateway）收集的用户和应用程序行为的可见性。您可以跟踪行为的各个方面，通过利用先进的机器学习算法，可以区分正常行为和恶意攻击者。因此，使您能够主动识别和管理内部和外部威胁。

了解更多信息：Citrix Analytics for Security

Citrix Analytics for Performance

为 Citrix 虚拟应用程序和桌面 Virtual Apps 和 Citrix DaaS 站点的混合部署提供全面的端到端可见性。性能由用户体验分数表示，该分数量化了历史因素和指标，这些因素和指标定义了用户在使用 Citrix 提供的已发布应用程序、已发布的桌面或远程 PC 时所获得的体验。

了解更多信息：Citrix Analytics for Performance

Citrix Analytics - 使用情况（生命周期已结束）

> 注意
>
> 注意
>
> ：Citrix Usage Analytics 已达到生命周期已结束状态，不再向用户提供。

数据源

April 12, 2024

数据源是将数据发送到 Citrix Analytics 的云服务和本地产品。

Citrix 数据源

下表列出了 Citrix Analytics for Security 支持的各种 Citrix 数据源。有关更多信息，请参阅 入门。

数据源	部署类型	所需的代理	产品组件和版本
Citrix Endpoint Management	服务	不适用	Citrix Endpoint Management
网关	本地	Application Delivery Management 代理	Citrix Gateway 12.0.56.16 或更高版本
Citrix 身份提供程序	服务	不适用	Citrix 身份和访问管理
Citrix Secure Private Access	服务	（不适用）N/A	Citrix Secure Private Access
Citrix Remote Browser Isolation	服务	不适用	Citrix Remote Browser Isolation

数据源	部署类型	所需的代理	产品组件和版本
Citrix DaaS（以前称为 Virtual Apps and Desktops 服务）	服务	不适用	适用于 Windows 的 Citrix Workspace 应用程序 1907 或更高版本、适用于 Mac 的 Citrix Workspace 应用程序 1910.2 或更高版本、适用于 HTML5 的 Citrix Workspace 应用程序 2007 或更高版本、适用于 Chrome 网上应用店中提供的最新 Chrome 版本的 Citrix Workspace 应用程序、适用于 Google Play 中提供的最新 Android 版本的 Citrix Workspace 应用程序、适用于 Apple App Store 中提供的最新 iOS 版本的 Citrix Workspace 应用程序、适用于 Linux 的 Citrix Workspace 应用程序 2006 或更高版本
Citrix Virtual Apps and Desktops	本地	Virtual Apps and Desktops 代理	Citrix Virtual Apps and Desktops 7 1808、Citrix XenApp 和 XenDesktop 7.16 及更高版本

数据源	部署类型	所需的代理	产品组件和版本
		Actions 等高级功能需要代理。	适用于 Windows 的 Citrix Workspace 应用程序 1907 或更高版本、适用于 Mac 的 Citrix Workspace 应用程序 1910.2 或更高版本、适用于 HTML5 的 Citrix Workspace 应用程序 2007 或更高版本、适用于 Chrome 网上应用店中提供的最新 Chrome 版本的 Citrix Workspace 应用程序、适用于 Google Play 中提供的最新 Android 版本的 Citrix Workspace 应用程序、适用于 Apple App Store 中提供的最新 iOS 版本的 Citrix Workspace 应用程序、适用于 Linux 的 Citrix Workspace 应用程序 2006 或更高版本 Citrix Director 7.16 或更高版本 对于 **Workspace** 用户：必须使用站点聚合将 Virtual Apps and Desktops 本地站点添加到 Workspace。

数据源	部署类型	所需的代理	产品组件和版本
			对于 **StoreFront** 用户：StoreFront 部署版本必须为 StoreFront 1906 或更高版本。必须使用以下客户端之一访问 StoreFront：兼容 HTML5 的浏览器中的 Citrix Receiver for Web 站点、适用于 Windows 的 Citrix Workspace 应用程序 1907 或更高版本、适用于 Linux 的 Citrix Workspace 应用程序 2006 或更高版本、适用于 Mac 的 Citrix Workspace 应用程序 2006 或更高版本。 **LTSR** 支持：对于 Citrix Virtual Apps and Desktops 7 1912 LTSR，受支持的 StoreFront 版本是 1912。

> 注意
>
> 有关 Citrix 产品及其订阅的信息，请参阅 Citrix Cloud 服务。

外部数据源

下表列出了 Citrix Analytics for Security 支持的外部数据源（第三方产品）。

数据源	部署类型	所需的代理
Microsoft Graph 安全性	服务	不适用
Microsoft Active Directory	本地	Citrix Cloud Connector

支持的主区域

以下主区域支持 Citrix Analytics for Security：

- 美国 (US)
- 欧洲联盟（EU）
- 亚太南部 (APS)

根据组织所在的位置，您可以在其中一个主区域加入 Citrix Cloud。

如果您的组织在不支持数据源的主区域中加入了 Citrix Cloud，则不会从数据源获取用户事件。

使用下表查看数据源及其受支持的区域。

数据源	在美国地区受支持	在欧盟地区受支持	APS 区域支持
Citrix Endpoint Management	是	是	是
Citrix Gateway（本地）	是	是	是
Citrix 身份提供程序	是	是	是
Citrix Secure Private Access	是	是	是
Citrix Remote Browser Isolation	是	是	是
Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）	是	是	是
Citrix Virtual Apps and Desktops 本地	是	是	是
Microsoft Active Directory	是	是	是
Microsoft Graph 安全性	是	是	是

Citrix Workspace 应用程序版本列表

本部分显示了 Citrix Workspace 应用程序的支持版本，该版本可发送所有遥测数据，并包含所需的所有关键错误修复。

下表列出了 Citrix Workspace 应用程序支持和不支持的版本。

平台	支持的版本
Windows	CU3 之后发布的所有 LTSR 2203 版本 23.0.3.0 或更高版本
HTML5	21.5.0.0 或更高版本
Macintosh	21.0.4.0 或更高版本
Linux	21.4.0.0 或更高版本
Chrome	21.5.0.0 或更高版本
iOS	21.4.0.0 或更高版本
Android	21.5.0.0 或更高版本

下表列出了操作系统在 Citrix Analytics for Security 中接收以下用户事件属性所需的最低版本的 Citrix Workspace 应用程序。

事件属性	关联的功能	Windows	Mac	Linux	HTML5	Chrome	iOS	Android
城市、国家/地区	访问保障位置、自助搜索 - 应用程序和桌面	2008 或更高版本	2006 或更高版本	2104 或更高版本	2007 或更高版本	Chrome 网上应用店中提供的最新版本	Apple App Store 中提供的最新版本	Google Play 中可用的最新版本
客户端 IP	自助搜索 - 应用程序和桌面	2008 或更高版本	2006 或更高版本	2104 或更高版本	2007 或更高版本	Chrome 网上应用店中提供的最新版本	Apple App Store 中提供的最新版本	Google Play 中可用的最新版本
操作系统名称、操作系统版本、操作系统的额外信息	自助搜索 - 应用程序和桌面	2109 或更高版本	2108 或更高版本	2104 或更高版本	2007 或更高版本	Chrome 网上应用店中提供的最新版本	Apple App Store 中提供的最新版本	Google Play 中可用的最新版本
打印机名称	自助搜索 - 应用程序和桌面	2106 或更高版本	1809 或更高版本	2006 或更高版本	1911 或更高版本	Chrome 网上应用店中提供的最新版本	Apple App Store 中提供的最新版本	Google Play 中可用的最新版本

事件属性	关联的功能	Windows	Mac	Linux	HTML5	Chrome	iOS	Android
网络启动的所有用户事件	自助搜索 - 应用程序和桌面	2008 或更高版本	2006 或更高版本	2006 或更高版本	不适用	不支持	Apple App Store 中提供的最新版本	Google Play 中可用的最新版本

数据治理

April 12, 2024

本节提供有关 Citrix Analytics 服务收集、存储和保留日志的信息。未在“定 义”部分中定义 的任何大写术语均具有 Citrix 最终用户服务协议中指定的含义。

Citrix Analytics 旨在让客户深入了解其 Citrix 计算环境中的事件。Citrix Analytics 使安全管理员能够选择他们想要监视的日志，并根据记录的事件采取定向措施。这些见解可帮助安全管理员管理对其计算环境的访问，并在客户的计算环境中保护客户内容。

数据驻留

Citrix Analytics 日志与数据源分开维护，并聚合到位于美国、欧盟和亚太南部地区的多个 Microsoft Azure 云环境中。日志的存储取决于 Citrix Cloud 管理员在将组织加入 Citrix Cloud 时选择的主区域。例如，如果您在将组织加入 Citrix Cloud 时选择了欧洲区域，则 Citrix Analytics 日志将存储在欧盟的 Microsoft Azure 环境中。

有关更多信息，请参阅 Citrix Cloud Services 客户内容和日志处理 以及 地理注意事项。

数据收集

Citrix Cloud 服务经过精心设计，可将日志传输到 Citrix Analytics。日志是从以下数据源收集的：

- Citrix ADC（本地）以及 Citrix Application Delivery Management 的订阅
- Citrix Endpoint Management
- Citrix Gateway（本地）
- Citrix 身份提供程序
- Citrix Secure Browser

- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）
- Microsoft Active Directory
- Microsoft Graph 安全性

数据传输

Citrix Cloud 日志安全传输到 Citrix Analytics。当客户环境的管理员明确启用 Citrix Analytics 时，这些日志将被分析并存储在客户数据库中。这同样适用于配置了 Citrix Workspace 的 Citrix Virtual Apps and Desktops 数据源。

对于 Citrix ADC 数据源，只有当管理员为特定数据源明确启用 Citrix Analytics 时，才会启动日志传输。

数据控制

管理员可以随时打开或关闭发送到 Citrix Analytics 的日志。

当 Citrix ADC 本地数据源关闭时，特定 ADC 数据源与 Citrix Analytics 之间的通信将停止。

如果对其他数据源全部关闭，则不再分析特定数据源的日志并将其存储在 Citrix Analytics 中。

数据保留

Citrix Analytics 日志以可识别的形式保留最长 13 个月或 396 天。所有日志和相关的分析数据（如用户风险概况、用户风险评分详细信息、用户风险事件详细信息、用户观察列表、用户操作和用户配置文件）将在此期间保留。

例如，如果您已于 2021 年 1 月 1 日在数据源上启用了分析，则默认情况下，2021 年 1 月 1 日收集的数据将保留在 Citrix Analytics 中，直到 2022 年 1 月 31 日。同样，2021 年 1 月 15 日收集的数据将保留到 2022 年 2 月 15 日，依此类推。

即使在关闭数据源的数据处理或从 Citrix Analytics 中删除数据源之后，此数据仍会在默认数据保留期内存储。

Citrix Analytics 将在订阅期或试用期到期后 90 天内删除所有客户内容。

数据导出

本节介绍从 Citrix Analytics for Security 和 Citrix Analytics for Performance 中导出的数据。

Citrix Analytics for Performance 从数据源收集和分析性能指标。

您可以将自助搜索页面中的数据下载为 CSV 文件。

Citrix Analytics for Security 从各种产品（数据源）收集用户事件。对这些事件进行处理，以提供对用户风险和异常行为的可见性。您可以将这些与用户风险洞察和用户事件相关的已处理数据导出到系统信息和事件管理 (SIEM) 服务。

目前，可以通过两种方式从 Citrix Analytics for Security 中导出数据：

- 将 Citrix Analytics for Security 与您的 SIEM 服务集成
- 将自助搜索页面中的数据作为 CSV 文件下载。

将 Citrix Analytics for Security 与 SIEM 服务集成时，数据将通过使用北向的 Kafka 主题或基于 Logstash 的数据连接器发送到您的 SIEM 服务。

目前，您可以与以下 SIEM 服务集成：

- Splunk（通过 Citrix Analytics 附加组件进行连接）
- 任何支持 Kafka 主题或基于 Logstash 的数据连接器的 SIEM 服务，例如 Elasticsearch 和 Microsoft Azure Sentinel

您还可以使用 CSV 文件将数据导出到 SIEM 服务。在自助搜索页面中，您可以查看数据源的数据（用户事件）并将这些数据下载为 CSV 文件。有关 CSV 文件的详细信息，请参阅 自助搜索。

> 重要提示
>
> 将数据导出到 SIEM 服务后，Citrix 不负责安全性、存储、管理和导出数据在 SIEM 环境中的使用。

您可以打开或关闭从 Citrix Analytics for Security 到 SIEM 服务的数据传输。

有关处理过的数据和 SIEM 集成的信息，请参阅安全信息和事件管理 (SIEM) 集成和适用于 SIEM 的 Citrix Analytics 数据格式。

Citrix Services Security Exhibit

有关应用于 Citrix Analytics 的安全控制的详细信息，包括访问和身份验证、安全计划管理、业务连续性和事件管理，都包含在 Citrix Services 安全展览中。

定义

客户内容 是指上载到客户帐户以供存储的任何数据，或客户环境中允许 Citrix 执行服务的数据。

日志是指与服务相关的事件记录，包括衡量性能、稳定性、使用率、安全性和支持的记录。

服务 是指上述为 Citrix Analytics 目的概述的 Citrix Cloud 服务。

数据收集协议

将数据上传到 Citrix Analytics 并使用 Citrix Analytics 的功能，即表示您同意并同意 Citrix 可以收集、存储、传输、维护、处理和使用有关 Citrix 产品和服务的技术、用户或相关信息。

Citrix 始终根据 Citrix 隐私政策处理收到的信息。

附录：收集的日志

- Citrix Analytics for Security 日志
- Citrix Analytics for Performance 日志

Citrix Analytics for Security 日志

常规日志

通常，Citrix Analytics 日志包含以下标头标识数据点：

- 标题键
- 设备识别
- 标识
- IP 地址
- 组织
- 产品
- 产品版本
- 系统时间
- 租户身份
- 类型
- 用户：电子邮件、ID、SAM 帐户名、域、UPN
- 版本

Citrix Endpoint Management 服务日志

Citrix Endpoint Management 服务日志包含以下数据点：

- 合规性

- 企业拥有
- 设备 ID
- 设备型号
- 设备类型
- 地理纬度
- 地理经度
- 主机名
- IMEI
- IP 地址
- 越狱
- 上次事件
- 管理模式
- 操作系统
- 操作系统版本
- 平台信息
- 原因
- 序列号
- 受监督

Citrix Secure Private Access 日志

- AAA 用户名
- 身份验证策略操作名称
- 身份验证会话 ID
- 请求 URL
- URL 类别策略名称
- VPN 会话 ID
- 虚拟服务器 IP
- AAA 用户电子邮件 ID
- 实际模板代码

- 应用程序 FQDN
- 应用程序名称
- 应用名称虚拟服务器 LS
- 应用标志
- 身份验证类型
- 认证阶段
- 身份验证状态码
- 后端服务器 Dst IPv4 地址
- 后端服务器 IPv4 地址
- 后端服务器 IPv6 地址
- 类别域名
- 类别域名来源
- 客户端 IP
- 客户端 MSS
- 客户端快速 Rex 计数
- 客户端 TCP 抖动
- 重新传输的客户端 TCP 数据包
- 客户端 TCP RTO 计数
- 客户端 TCP 零窗口计数
- 客户端流标志 Rx
- 客户端流标志 Tx
- 客户端 TCP 标志 Rx
- 客户端 TCP 标志 Tx
- 连接链跳数
- 连接链 ID
- 出口接口
- 导出进程 ID
- 流量标志 Rx
- 流量标志 Tx

- HTTP 内容类型
- HTTP 域名
- HTTP 请求授权
- HTTP Req Cookie
- HTTP Req Forw FB
- HTTP Req Forw LB
- HTTP 请求主机
- HTTP 请求方法
- HTTP Rq Rcv FB
- HTTP Req Rcv LB
- HTTP Req 引用
- HTTP 请求 URL
- HTTP Req XForwarded For
- HTTP Res Forw FB
- HTTP Res Forw LB
- HTTP 资产位置
- HTTP Res Rcv FB
- HTTP Res Rcv LB
- HTTP Res Set Cookie
- HTTP Rsp Len
- HTTP Rsp 状态
- HTTP 事务结束时间
- HTTP 事务 ID
- IC Cont Gp 名称
- IC 标志
- IC 没有商店标志
- IC 策略名称
- 入口接口客户端
- NetScaler Gateway Service 应用程序 ID

- NetScaler Gateway Service 应用程序名称
- NetScaler Gateway Service 应用程序类型
- NetScaler 分区 ID
- 观察域 ID
- 观察点 ID
- 起源资源状态
- 原产地 Rsp Len
- 协议标识符
- 速率限制标识符名称
- 记录类型
- 响应程序操作类型
- 响应媒体类型
- Srv Flow 标志 Rx
- Srv Flow 标志 Tx
- srvr 快速 Rex 计数
- 服务器 TCP 抖动
- 服务器 TCP 数据包已重新传输
- 服务器 TCP 恢复计数
- 服务器 TCP 零窗口计数
- SSL 密码值 BE
- SSL 密码值 FE
- SSL 客户端证书大小 BE
- SSL 客户端证书大小 FE
- SSL 客户端证书签名哈希 BE
- SSL Cnt 证书签名哈希 FE
- SSL Err 应用程序名称
- SSL 错误标志
- SSL 标志 BE
- SSL 标志 FE

- SSL 握手错误消息
- SSL 服务器证书大小 BE
- SSL 服务器证书大小 FE
- SSL 会话 ID BE
- SSL 会话 ID FE
- SSL Sig 哈希算法 BE
- SSL Sig 哈希算法 FE
- SSL 服务器证书签名哈希 BE
- SSL 服务器证书签名哈希 FE
- SSL iDomain 类别
- SSL iDomain 类别组
- SSL iDomain 名称
- SSL iDomain 声誉
- SSL iExecuted 操作
- SSL iPolicy 操作
- SSL iReason 采取行动
- SSL iURL 集已匹配
- SSL iURL 设置为私有
- 订户标识符
- Svr Tcp 标志 Rx
- Svr Tcp 标志 Tx
- 租户姓名
- 跟踪请求父跨度 ID
- 跟踪请求跨度 ID
- 跟踪跟踪 ID
- Trans Ct Dst IPv4 地址
- 事务客户端目标 IPv6 地址
- 事务客户端目标端口
- Trans Ct Flow 最终使用 Rx

- Trans Clt Flow End Usec Tx
- Trans Ct Flow 开始使用 Rx
- Trans Clt Flow Start Usec Tx
- Trans Clr IPv4 地址
- Trans Clr IPv6 地址
- Trans Ct 数据包 Tt Cnt Rx
- Trans Clt Packet Tot Cnt Tx
- 事务客户端 RTT
- Trans Clr Ssc 端口
- Trans Ct Tt Rx Oct Cnt
- Trans Ct Tt Tx Oct Cnt
- Trans Info
- Trans Srv Dst 端口
- Trans srv 数据包 Tt Cnt Rx
- Trans Srv 数据包 Tt Cnt Tx
- Trans Srv Src 端口
- Trans Svr Flow End Usec Rx
- Trans Svr Flow End Usec Tx
- Trans Svr Flow Start Usec Rx
- Trans Svr Flow Start Usec Tx
- 事务服务器 RTT
- Trans Svr Tot Rx Oct Cnt
- Trans Svr Tot Tx Oct Cnt
- 事务 ID
- URL 类别
- URL 类别组
- URL 类别声誉
- URL 类别操作原因
- URL 集已匹配

- URL 设置为私人
- URL 对象 ID
- VLAN 编号

Citrix Virtual Apps and Desktops 和 **Citrix DaaS** 日志

Citrix Virtual Apps and Desktops 和 Citrix DaaS 日志包含以下数据点：

- 应用程序名称
- 浏览器
- 客户 ID
- 详细信息：格式大小、格式类型、启动器、结果
- 设备 ID
- 设备类型
- 反馈
- 反馈 ID
- 文件名
- 文件路径
- 文件大小
- 就像
- 越狱
- 作业详细信息：文件名、格式、大小
- 位置：估计、纬度、经度

  > 注意
  >
  > 位置信息是在城市和国家/地区级别提供的，并不代表精确的地理位置。

- 长 CMD 线
- 模块文件路径
- 操作
- 操作系统
- 平台额外信息
- 打印机名称

- 问题
- 问题 ID
- SaaS 应用程序名称
- 会话域
- 会话服务器名称
- 会话用户名
- 会话 GUID
- 时间戳
- 时区：Bias、DST、名称
- 打印的总份数
- 打印的总页数
- 类型
- URL
- 用户代理

Citrix ADC 日志

Citrix ADC 日志包含以下数据点：

- 集装箱
- 文件
- 格式
- 类型

Citrix DaaS Standard for Azure 日志

适用于 Azure 的 Citrix DaaS 标准日志包含以下数据点：

- 应用程序名称
- 浏览器
- 详细信息：格式大小、格式类型、启动器、结果
- 设备 ID
- 设备类型

- 文件名
- 文件路径
- 文件大小
- 越狱
- 作业详细信息：文件名、格式、大小
- 位置：估计、纬度、经度

  > 注意
  >
  > 位置信息是在城市和国家/地区级别提供的，并不代表精确的地理位置。

- 长 CMD 线
- 模块文件路径
- 操作
- 操作系统
- 平台额外信息
- 打印机名称
- SaaS 应用程序名称
- 会话域
- 会话服务器名称
- 会话用户名
- 会话 GUID
- 时间戳
- 时区：Bias、DST、名称
- 类型
- URL
- 用户代理

Citrix 身份提供程序日志

- 用户登录：
  - Authentication Domains: Name, Product, IdP Type, IdP Display Name

        * IdP Properties: App, Auth Type, Customer Id, Client Id, Directory, Issuer, Logo, Resources, TID
        * 扩展程序:
            - Workspace: Background Color, Header Logo, Logon Logo, Link Color, Text Color, StoreFront Domains
            - ShareFile: Customer Id, Customer Geo
            - Long Lived Token: Enabled, Expiry Type, Absolute Expiry Seconds, Sliding Expiry Seconds
    - Authentication Result: User Name, Error Message
    - Sign-in Message: Client Id, Client Name
    - User Claim: AMR, Access Token Hash, Aud, Auth Time, CIP Cred, Auth Alias, Auth Domains, Groups, Product, System Aliases, Email, Email Verified, Exp, Family Name, Given Name, IAT, IdP, ISS, Locale, Name, NBF, SID, Sub
        * Auth Alias Claims: Name, Value
        * Directory Context: Domain, Forrest, Identity Provider, Tenant Id
        * User: Customers, Email, OID, SID, UPN
        * IdP Extra Fields: Azure AD OID, Azure AD TID
- User Logoff: Client Id, Client Name, Nonce, Sub
- Client Update: Action, Client Id, Client Name

Citrix Gateway 日志

- 交易事件:
    - ICA App: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx, ICA Flags, Connection Id, Padding Octets Two, ICA Device Serial Number, IP Version 4, Protocol Identifier, Source IPv4 Address Rx, Destination IPv4 Address Rx, Source Transport Port Rx, Destination Transport Port Rx, ICA Application Start up Duration, ICA Launch Mechanism, ICA Application Start up Time, ICA Process ID Launch, ICA Application Name, ICA App Module Path, ICA Application Termination Type, ICA Application Termination Time, Application Name App Id, ICA App Process ID Terminate, ICA App
    - ICA Event: Record Type, Actual Template Code, Source IPv4 Address Rx, Destination IPv4 Address Rx, ICA Session Guid, MSI Client Cookie, Connection Chain ID, ICA Client

Version, ICA Client Host Name, ICA User Name, ICA Domain Name, Logon Ticket Setup, Server Name, Server Version, Flow Id Rx, ICA Flags, Observation Point Id, Exporting Process Id, Observation Domain Id, Connection Id, ICA Device Serial Number, ICA Session Setup Time, ICA Client IP, NS ICA Session Status Setup, Source Transport Port Rx, Destination Transport Port Rx, ICA Client Launcher, ICA Client Type, ICA Connection Priority Setup, NS ICA Session Server Port, NS ICA Session Server IP Address, IPv4, Protocol Identifier,Connection Chain Hop Count, Access Type

- ICA Update: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx,ICA Flags, Connection Id, ICA Device Serial Number, IPv4, Protocol Identifier, Padding Octets Two, ICA RTT, Client Side RX Bytes, Client Side Packets Retransmit, Server Side Packets Retransmit, Client Side RTT, Client Side Jitter, Server Side Jitter, ICA Network Update Start Time, ICA Network Update End Time, Client Side SRTT, Server Side SRTT,Client Side Delay, Server Side Delay, Host Delay, Client Side Zero Window Count, Server Side Zero Window Count, Client Side RTO Count, Server Side RTO Count, L7 Client Latency, L7 Server Latency, App Name App Id, Tenant Name, ICA Session Update Begin Sec, ICA Session Update End Sec, ICA Channel Id 1, ICA Channel Id 2, ICA Channel Id 2 Bytes, ICA Channel Id 3, ICA Channel Id 3 Bytes, ICA Channel Id 4, ICA Channel Id 4 Bytes, ICA Channel Id 5, ICA Channel Id 5 Bytes
- AppFlow Config: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, System Rule Flag 1, System Safety Index, AppFlow Profile Relaxed Flags, AppFlow Profile Block Flags, AppFlow Profile Log Flags, AppFlow Profile Learn Flags, AppFlow Profile Stats Flags, AppFlow Profile None Flags, AppFlow App Name Id, AppFlow Profile Sign Disabled, AppFlow Profile Sign Block Count, AppFlow Profile Sign Log Count, AppFlow Profile Sign Stat Count, AppFlow Incarnation Number,AppFlow Sequence Number, AppFlow Profile Sign Auto Update, AppFlow Safety Index, AppFlow App Safety Index, AppFlow Profile Sec Checks Safety Index, AppFlow Profile Type, Iprep App Safety Index, AppFlow Profile Name, AppFlow Sig Name, AppFlow App Name Ls, AppFlow Sig Rule ID1, AppFlow Sig Rule ID2, AppFlow Sig Rule ID3, AppFlow Sig Rule ID4, AppFlow Sig Rule ID5, AppFlow Sig Rule Enabled Flags, AppFlow Sig Rule Block Flags, AppFlow Sig Rule Log Flags, AppFlow Sig Rule File Name, AppFlow Sig Rule Category1, AppFlow Sig Rule Logstring1, AppFlow Sig Rule Category2, AppFlow Sig Rule Logstring2, AppFlow Sig Rule Category3, AppFlow Sig Rule Category4, AppFlow Sig Rule Logstring4, AppFlow Sig Rule Category5, AppFlow Sig Rule LogString5
- AppFlow: Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, Transaction Id, Appfw Violation Occurred Time, App Name App Id, Appfw Violation Severity, Appfw Violation Type, Appfw Violation Location, Appfw Violation Threat Index, Appfw NS Longitude, Appfw NS Latitude, Source IPv4 Address Rx, Appfw Http Method, Appfw App Threat Index, Appfw Block Flags, Appfw Transform Flags, Appfw

Violation Profile Name, Appfw Session Id, Appfw Req Url, Appfw Geo Location, Appfw Violation Type Name 1, Appfw Violation Name Value 1, Appfw Sig Category 1, Appfw Violation Type Name 2, Appfw Violation Name Value 2, Appfw Sig Category 2, Appfw Violation Type Name 3, Appfw Violation Name Value 3, Appfw Sig Category3, Appfw Req X Forwarded For, Appfw App Name Ls,App Name Ls, Iprep Category, Iprep Attack Time, Iprep Reputation Score, Iprep NS Longitude, Iprep NS Latitude, Iprep Severity, Iprep HTTP Method, Iprep App Threat Index, Iprep Geo Location, Tcp Syn Attack Cntr, Tcp Slow Ris Cntr, Tcp Zero Window Cntr, Appfw Log Expr Name, Appfw Log Expr Value, Appfw Log Expr Comment

- VPN: Actual Template Code, Observation Domain Id, Access Insight Flags, Observation Point Id, Exporting Process Id, Access Insight Status Code, Access Insight Timestamp, Authentication Duration, Device Type, Device ID, Device Location, App Name App Id, App Name App Id1, Source Transport Port Rx, Destination Transport Port Rx, Authentication Stage, Authentication Type, VPN Session ID, EPA Id, AAA User Name, Policy Name, Auth Agent Name, Group Name, Virtual Server FQDN, cSec Expression, Source IPv4 Address Rx, Destination IPv4 Address Rx, Cur Factor Policy Label, Next Factor Policy Label, App Name Ls, App Name 1 Ls,AAA User Email Id, Gateway IP, Gateway Port, Application Byte Count, VPN Session State, VPN Session Mode, SSO Auth Method, IIP Address, VPN Request URL, SSO Request URL, Backend Server Name, VPN Session Logout Mode, Logon Ticket File Info, STA Ticket, Session Sharing Key, Resource Name, SNIP Address, Temp VPN Session ID
- HTTP: Actual Template Code, Http Req Method, Http Req Url, Http Req User Agent, Http Content Type, Http Req Host, Http Req Authorization, Http Req Cookie, Http Req Referer, Http Res Set Cookie, Ic Cont Grp Name, Ic Flags, Ic Nostore Flags, Ic Policy Name, Response Media Type, Ingress Interface Client, Origin Res Status, Origin Rsp Len, Srv Flow Flags Rx, Srv Flow Flags Tx, Flow Flags Rx, Flow Flags Tx, App Name, Observation Point Id, Exporting Process Id, Observation Domain Id, Http Trans End Time, Transaction Id, Http Rsp Status, Trans Clt Ipv4 Address, Trans Clt Dst Ipv4 Address, Backend Svr Dst Ipv4 Address, Backend Svr Ipv4 Address, Http Rsp Len, Trans Svr RTT, Trans Clt RTT, Http Req Rcv FB, Http Req Rcv LB, Http Res Rcv FB, Http Res Rcv LB, Http Req Forw FB, Http Req Forw LB, Http Res Forw FB, Http Res Forw LB, Http Req X Forwarded For, Http Domain Name, Http Res Location, Protocol Identifier, Egress Interface, Backend Svr Ipv6 Address, SSL Flags BE, SSL Flags FE, SSL Session IDFE, SSL Session IDBE, SSL Cipher Value FE, SSL Cipher Value BE, SSL Sig Hash Alg BE, SSL Sig Hash Alg FE, SSL Srvr Cert Sig Hash BE, SSL Srvr Cert Sig Hash FE, SSL Clnt Cert Sig Hash FE, SSL Clnt Cert Sig Hash BE, SSL Server Cert Size FE, SSL Server Cert Size BE, SSL Client Cert Size FE, SSL Client Cert Size BE, SSL Err App Name, SSL Err Flag, SSL Handshake Error Msg, Client IP, Virtual Server IP, Connection Chain Id, Connection Chain Hop Count, Trans Clt Tot Rx Oct Cnt, Trans Clt TotTx Oct Cnt, Trans Clt Src Port, Trans Clt Dst Port, Trans Srv Src Port, Trans Srv Dst Port, VLAN Number, Client Mss, Trans Info, Trans Clt Flow End Usec Rx, Trans Clt Flow End Usec Tx, Trans Clt Flow Start Usec Rx, Trans Clt

Flow Start Usec Tx, Trans Svr Flow End Usec Rx, Trans Svr Flow End Usec Tx, Trans Svr Flow Start Usec Rx, Trans Svr Flow Start Usec Tx, Trans Svr Tot Rx Oct Cnt, Trans Svr Tot Tx Oct Cnt, Clt Flow Flags Tx, Clt Flow Flags Rx, Trans Clt Ipv6 Address, Trans Clt Dst Ipv6 Address, Subscriber Identifier, SSLi Domain Name, SSLi Domain Category, SSLi Domain Category Group, SSLi Domain Reputation, SSLi Policy Action, SSLi Executed Action, SSLi Reason For Action, SSLi URL Set Matched, SSLi URL Set Private, URL Category, URL Category Group, URL Category Reputation, Responder Action Type, URL Set Matched, URL Set Private, Category Domain Name, Category Domain Source, AAA User Name, VPN Session ID, Tenant Name

- 指标事件：
  - VServer LB: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU, GSLB Server, GSLB VServer, Interface, Memory Pool, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer LB: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Clt Ttlb Pkt Rcvd, RATE Si Tot Clt Ttlb Pkt Sent, RATE Vsvr Tot Hits, Si Cur Clients, Si Cur Conn Established, Si Cur Servers, Si Cur State, Si Tot Request Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rcvd, Si Tot Pkt Sent, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions, Vsvr Active Svcs, Vsvr Tot Hits, Vsvr tot Req Resp Invalid, Vsvr Tot Req Resp Invalid Dropped
  - CPU: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, Cc CPU Use GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User
  - Server Service Group: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, Cc CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Service Group: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot_Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions,Si Tot Svr Tlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions
  - Server SVC CFG: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer

User, Server Svc Cfg: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Svr Busy Err, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Cur Transport, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rcvd, Si Tot Pkt Sent, Si Tot Svr Busy Err, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions, Si Tot Svr Ttlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions

- NetScaler: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, GSLB Server, GSLB VServer, Interface, Memory Pool, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, NetScaler: RATE All Nic Tot Rx Mbits, RATE All Nic Tot Rx Mbits, RATE Dns Tot Queries, RATE Dns Tot Neg Nxdmn Entries,RATE Http Tot Gets, RATE Http Tot Others, RATE Http Tot Posts, RATE Http Tot Requests, RATE Http Tot Requests 1.0, RATE Http Tot Requests 1.1, RATE Http Tot Responses, RATE Http Tot Rx Request Bytes, RATE Http Tot Rx Response Bytes, RATE Ip Tot Rx Mbits, RATE Ip Tot Rx Bytes, RATE Ip Tot Rx Pkts, RATE Ip Tot Tx Mbits, RATE Ip Tot Tx Bytes, RATE Ip Tot Tx Pkts, RATE SSL Tot Dec Bytes, RATE SSL Tot Enc Bytes,RATE SSL Tot SSL Info Session Hits, RATE SSL Tot SSL Info Total Tx Count, RATE Tcp Err Rst, RATE Tcp Tot Client Open, RATE Tcp Tot Server Open, RATE Tcp Tot Rx Bytes, RATE Tcp Tot Rx Pkts, RATE Tcp Tot Syn, RATE Tcp Tot Tx Bytes, RATE Tcp Tot Tx Pkts, RATE Udp Tot Rx Bytes, RATE Udp Tot Rx Pkts, RATE Udp Tot Tx Bytes, RATE Udp Tot Tx Pkts, All Nic Tot Rx Mbits, All Nic Tot Tx Mbits, Cpu Use, Dns Tot Queries, Dns Tot Neg Nxdmn Entries, Http Tot Gets, Http Tot Others, Http Tot Posts, Http Tot Requests, Http Tot Requests1.0, Http Tot Requests1.1, Http Tot Responses, Http Tot Rx Request Bytes, Http Tot Rx Response Bytes, Ip Tot Rx Mbits, Ip Tot Rx Bytes, Ip Tot Rx Pkts, Ip Tot Tx Mbits, Ip Tot Tx Bytes, Ip Tot Tx Pkts, Mem Cur Free size, Mem Cur Free size Actual, Mem Cur Used size, Mem Tot Available, Mgmt Additional Cpu Use, Mgmt Cpu 0 Use, Mgmt Cpu Use, SSL Tot Dec Bytes, SSL Tot Enc Bytes, SSL Tot SSL Info Session Hits, SSL Tot SSL Info Total Tx Count, Sys Cpus, Tcp Cur Client Conn, Tcp Cur Client Conn Closing, Tcp Cur Client Conn Est, Tcp Cur Server Conn, Tcp Cur Server Conn Closing, Tcp Cur Server Conn Est, Tcp Err Rst, Tcp Tot Client Open, Tcp Tot Server Open, Tcp Tot Rx Bytes, Tcp Tot Rx Pkts, Tcp Tot Syn, Tcp Tot Tx Bytes, Tcp Tot Tx Pkts, Udp Tot Rx Bytes, Udp Tot Rx Pkts, Udp Tot Tx Bytes, Udp Tot Tx Pkts
- Memory Pool: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Interface, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Memory Pool: Mem Cur Alloc Size, Mem Err Alloc Failed, Mem Tot Available
- Monitoring Service Binding: Bind Entity Name, Entity Name, NetScalerId, SchemaType,

Time, CPU, Gslb Server, Gslb VServer, Interface, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, Mon Service Binding: RATE Mon Tot Probes, Mon Tot Probes

- Interface: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, Interface: RATE NIC Tot Rx Bytes, RATE NIC Tot Rx Packets, RATE NIC Tot Tx Bytes, RATE NIC Tot Tx Packets, NIC Tot Rx Bytes, NIC Tot Rx Packets, NIC Tot Tx Bytes, NIC Tot Tx Packets
- VServer CS: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, VServer Cs: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb,RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, RATE Vsvr Tot Hits, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rvd, Si Tot Pkt Sent, Si Tot Ttlb Frustrating Transactions, Si Tot Tlb Tolerating Transactions, Vsvr Tot Hits, Vsvr Tot Req Resp Invalid, Vsvr Tot Req Resp Invalid Dropped

安全浏览器日志

- 申请帖子：
  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL
- 应用程序删除：
  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource

Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect

- Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL

- 应用程序更新：
  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL
- 权利创建：
  - Logs before the entitlement creation: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
  - Logs after the entitlement creation: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
- 权利更新：
  - Logs before the entitlement update: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
  - Logs after the entitlement update: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
- Session Access Host: Accept Host, Client IP, Date Time, Host, Session, User Name
- 会话连接：

  - Logs before the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Logs after the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- 会话启动:
  - Logs before the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Logs after the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- 会话勾号:
  - Logs before the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Logs after the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name

Microsoft Graph 安全性日志

- 租户 ID
- 用户 ID
- 指标 ID
- 指标 UUID
- 事件时间
- 创建时间
- 警报类别
- 登录位置
- 登录 IP
- 登录类型
- 用户帐户类型
- 供应商信息
- 厂商提供商信息
- 漏洞状态
- 漏洞严重性

Microsoft Active Directory 日志

- 租户 ID
- 收集时间
- 类型
- 目录上下文
- 组
- 身份
- 用户类型
- 帐户名称
- 密码计数错误
- 城市
- 普通名
- 公司
- 国家/地区
- 密码到期前的天数
- 部门
- 说明
- 显示名称
- 唯一判别名
- 电子邮件
- 传真号码
- 名字
- 组类别
- 组范围
- 家庭电话
- 首字母缩写
- IP 电话
- 帐户是否已启用
- 帐户被锁定了

- 是安全组
- 姓氏
- 经理
- 的成员
- 移动电话
- 寻呼机
- 密码永不过期
- 实物配送办公室名称
- 邮局信箱
- 邮政编码
- 主要组 ID
- 状态
- 街道地址
- 标题
- 用户帐户控制
- 用户组列表
- 用户主体名称
- 工作电话

Citrix Analytics for Performance 日志

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

- applicationtype
- applicationversion
- associateduserfullnames
- associatedusername
- associatedusernames
- associateduserupns
- authenticationduration
- autoreconnectcount
- autoreconnecttype
- AvgEndpointThroughputBytesReceived
- AvgEndpointThroughputBytesSent
- blobcontainer
- blobendpoint
- blobpath
- brokerapplicationchanged
- brokerapplicationcreated
- brokerapplicationdeleted
- brokeringdate
- brokeringduration
- brokerloadindex
- brokerregistrationstarted
- browsername
- catalogchangeevent
- catalogcreatedevent
- catalogdeletedevent
- catalogid
- catalogname
- catalogsync
- clientaddress

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

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

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

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

- modifieddate
- NGSConnector.ICAConnection.Start
- NGSConnector.NGSSyntheticMetrics
- NGSConnector.NGSPassiveMetrics
- NGSConnector.NGSSystemMetrics
- network
- networkindex
- networklatency
- networkinfoperiodic
- NetworkInterfaceType
- ostype
- outputbandwidthavailable
- outputbandwidthused
- path
- percentcpu
- persistentuserchanges
- powerstate
- processname
- profileloadenddate
- profileloadstartdate
- protocol
- provisioningschemeid
- provisioningtype
- publishedname
- registrationstate
- serversessionvalidatedate
- sessioncount
- sessionend
- sessionfailure

- sessionid
- sessionidlesince
- sessionindex
- sessionkey
- sessionstart
- sessionstate
- sessionsupport
- sessiontermination
- sessiontype
- sid
- SignalStrength
- siteid
- sitename
- startdate
- totalmemory
- triggerinterval
- triggerlevel
- triggerperiod
- triggervalue
- usedmemory
- userid
- userinputdelay
- username
- usersid
- vdalogonduration
- vdaprocessdata
- vdaresourcedata
- version
- vmstartenddate

- vmstartstartdate
- windowsconnectionsetting
- xd.SessionStart

系统要求

April 12, 2024

在开始使用 Citrix Analytics for Security 之前，请查看以下要求。

Citrix Analytics for Security 订阅

此分析产品是基于订阅的产品。您必须拥有有效的订阅才能使用安全分析。有关更多信息，请参阅 产品概述 页面。

数据源要求

Citrix Analytics for Security 接收来自各种数据源的事件。要使 Analytics 准确运行，您必须拥有有效的订阅才能使用以下产品中的至少一种，这些产品充当 Analytics 的数据源：

- Citrix ADC（本地） 以及 Citrix Application Delivery Management 的订阅
- Citrix Endpoint Management 服务
- Citrix Gateway（本地）
- Citrix 身份提供程序
- Citrix Remote Browser Isolation
- Citrix Secure Private Access 服务
- Citrix Virtual Apps and Desktops 或 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）
- Microsoft Active Directory
- Microsoft Graph 安全性

支持的浏览器

要访问 Analytics，您的工作站必须具有以下受支持的网络浏览器：

- Google Chrome 的最新版本

- Mozilla Firefox 的最新版本
- Microsoft Edge 的最新版本
- Apple Safari 的最新版本

管理 **Security Analytics** 的管理员角色

December 7, 2023

作为具有完全访问权限的 Citrix Cloud 管理员，您可以邀请其他管理员管理 Security Analytics 产品，并为他们分配以下自定义角色之一：

- **Security Analytics -** 完全权限管理员
- **Security Analytics -** 只读管理员

您可以通过两种方式添加新管理员：单独添加用户或使用 Azure Active Directory 组。有关添加新管理员的更多信息，请参阅 管理管理员角色。

> 注意
> 如果用户直接以用户身份通过 Azure Active Directory 组获得访问权限，则单独授予该用户的访问权限将生效。

自定义角色的权限

具有 Secur **ity Analytics-**完全权限管理员 角色的管理员可以访问安全分析产品的所有特性和功能。他们可以根据自己的组织要求使用和修改功能。例如，完全权限管理员可以创建自定义风险指示器、启用地理围栏和创建策略。

具有“安全分析**-**只读管理员”角色的管理员 只能访问和查看安全控制面板（用户、用户访问权限、应用程序访问权限、访问保障和报告）。他们可以监控用户行为并在这些仪表板上查看用户事件。但是，不允许他们执行任何关键任务，例如：

- 打开或关闭数据源的数据处理
- 创建或删除策略和操作
- 对用户风险时间表上显示的风险指示器手动应用操作
- 创建、修改或删除自定义风险指标
- 创建自定义报告
- 添加、修改或删除其他管理员用户
- 添加或修改访问保障位置的地理围栏

管理员的安全警报通知

与具有完全访问权限的 Citrix Cloud 管理员一样，具有自定义角色（完全访问权限和只读访问权限）的管理员会收到来自 Security Analytics 的电子邮件通知。

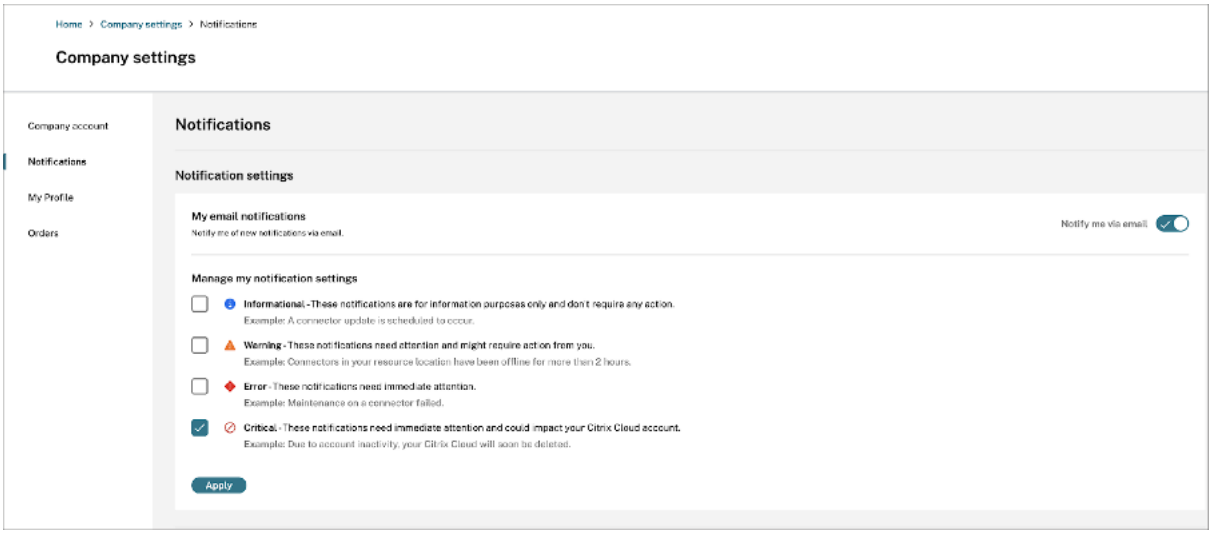
管理员会收到两种类型的电子邮件通知：

- 每周通知其组织中的安全洞察。有关详细信息，请参阅每周电子邮件通知。
- 基于“通知管理员”操作的通知。有关更多信息，请参阅 策略和操作。

如果您是具有完全或自定义访问权限的 Citrix Cloud 管理员，则默认情况下，您的 Citrix Cloud 帐户中的电子邮件通知处于禁用状态。要接收来自任何 Citrix Cloud 服务（例如 Citrix Analytics）的电子邮件通知，请在 Citrix Cloud 中启用通知选项。有关详细信息，请参阅 收到的电子邮件通知。通知首选项不适用于通过 Active Directory/Azure AD 组添加的管理员。

在发送每周电子邮件、通知管理员操作电子邮件和数据导出提醒等通知时，会利用通知首选项。对于电子邮件通知，如果您希望停止接收电子邮件，则具有安全分析完全访问权限的管理员必须将您从通讯组列表中删除。有关通讯组列表的详细信息，请参阅 电子邮件通讯组列表。

> 注意
>
> Citrix Cloud 管理员（具有完全或自定义访问权限）不会收到来自其他利用“通知首选项”的 Citrix Cloud 服务的通知。



有关更多信息，请参阅 管理 Citrix Analytics 的管理员。

快速入门

April 12, 2024

本文档介绍了如何首次开始使用 Citrix Analytics for Security。

步骤 **1**：登录到 **Citrix Cloud**

要使用 Citrix Analytics for Security，您必须拥有 Citrix Cloud 帐户。转到 https://citrix.cloud.com 并使用您现有的 Citrix Cloud 帐户登录。

如果您没有 Citrix Cloud 帐户，则必须首先创建 Citrix Cloud 帐户或加入组织中其他人创建的现有帐户。有关如何继续的详细过程和说明，请参阅 注册 Citrix Cloud。

第 **2** 步：获取 **Security Analytics** 的访问权限

您可以通过以下方式之一访问 Citrix Analytics for Security：

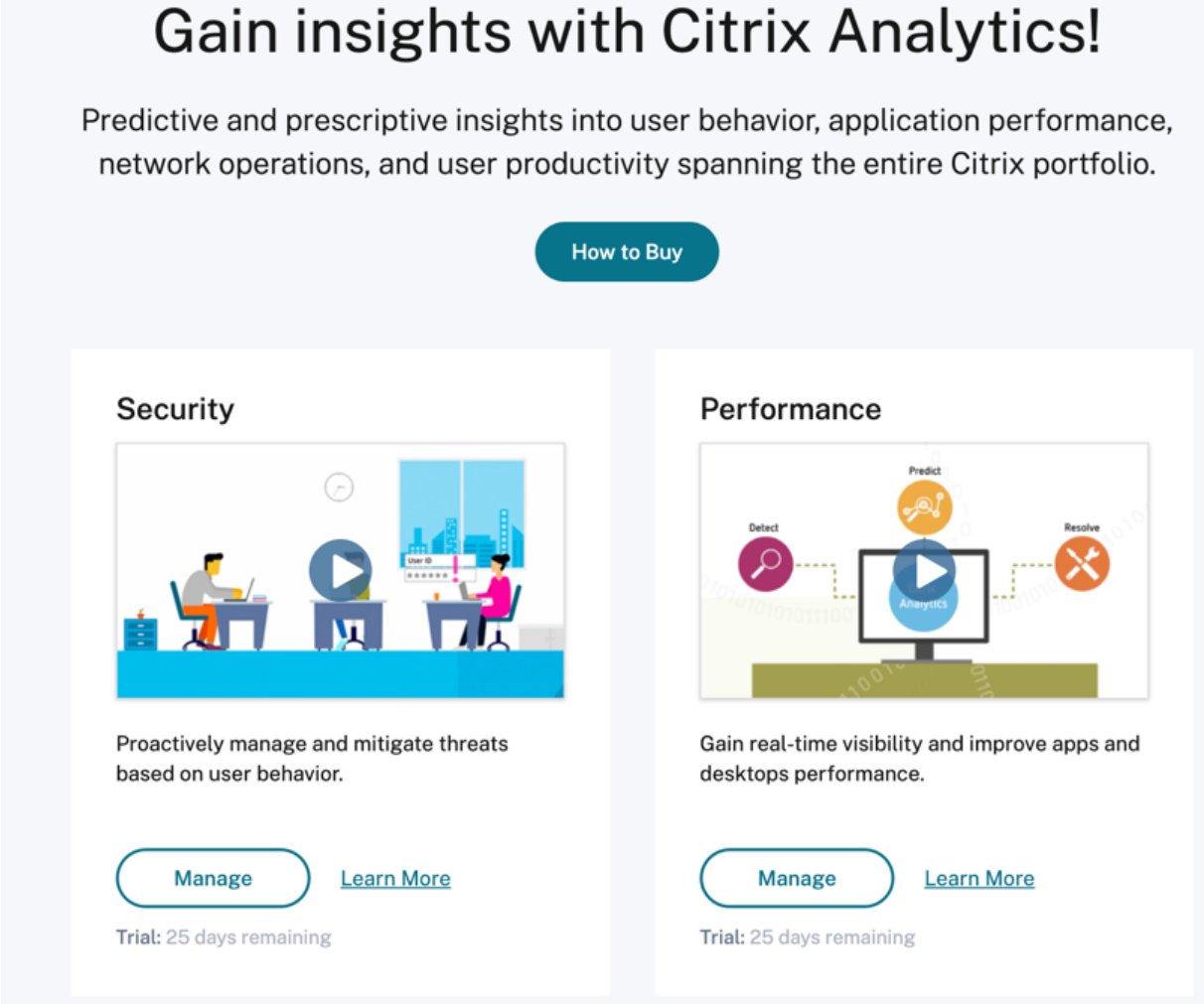
- 申请 **Citrix Analytics for Security** 试用版。登录 Citrix Cloud 后，请执行以下操作：
  1. 在可用服务部分中，单击分析磁贴上的管理。您将被重定向到分析概述页面。
  2. 在“安全”图块上，单击“申请试用”或直接联系您的 Citrix 帐户或 Citrix Partner。
- 订阅 **Citrix Analytics for Security**。要购买 Citrix Analytics for Security 订阅，请访问 https://www.citrix.com/en-in/products/citrix-analytics/form/inquiry/ 并联系可以为您提供帮助的 Citrix Analytics 专家。

> 注意
>
> - 自 2023 年 3 月 8 日起，Citrix Analytics for Security 将不再作为独立产品与 ShareFile/Citrix Content Collaboration 一起购买。我们宣布适用于 ShareFile/Citrix Content Collaboration 的 Citrix Analytics Service 独立插件的销售终止 (EOS) 和续订终止 (EOR)。客户在 Citrix Analytics for Security 的现有权利在订阅到期之前仍然有效。但是，Sharefile/Citrix Content Collaboration 集成将不支持试用、续订和新购买。其他 Citrix 产品的 Citrix Analytics Service 集成将继续作为独立产品或捆绑产品与现有 Citrix DaaS 计划、Citrix 虚拟应用程序和桌面部署以及 Citrix Workspace 部署一起提供。
> - 自 2020 年 2 月 3 日起，Citrix Analytics for Security 不再包含在 Workspace Premium 和 Work-

> space Premium Plus 订阅中。在 2020 年 2 月 3 日之前购买了 Workspace Premium 或 Workspace Premium Plus 订阅的客户，在订阅到期之前，可以作为 Workspace 订阅的一部分访问 Citrix Analytics for Security。Citrix Analytics for Security 现在作为附加服务与 Citrix Workspace 软件包 Workspace Standard、Workspace Premium 和 Workspace Premium Plus 一起提供。有关详细信息，请参阅 Citrix Cloud 服务。

步骤 3：管理 Security Analytics

获得必要的订阅或获得访问试用版的授权后，在 Analytics 概述页面上，安全产品的“请求试用”按钮将更改为 管理。单击“管理”以查看用户控制板。



Analytics 同时支持 Citrix 数据源 和 外部数据源。它会自动发现与您的 Citrix Cloud 帐户关联的 Citrix 数据源。要接收来自外部数据源的数据，您需要将外部数据源与 Analytics 集成。要查看发现的数据源，请单击“设置” > “数据源” > “安全性”。

接下来做什么

- 当 Citrix Analytics for Security 授权获得批准后，以下云服务的数据处理功能将启用：
  - Citrix 数据源
    - Citrix Secure Private Access
    - Citrix Virtual Apps and Desktops 和 Citrix DaaS
- 要验证数据处理状态或知道如何手动打开它，请参阅以下文章：
  - Citrix 数据源：
    - Citrix Endpoint Management
    - Citrix Gateway
  - 外部数据源：
    - Microsoft Graph 安全性
    - Microsoft Active Directory
- 将处理后的数据从 Analytics 导出到以下产品：
  - Splunk
  - Microsoft Azure Sentinel
  - Elasticsearch
  - 其他使用基于 Kafka 或 Logstash 的数据连接器的 SIEM
- 使用“用 户”控制面板 查看发现的用户及其安全风险配置文件。用户 仪表板是用户行为分析和威胁防御的起点。

  > 注意
  >
  > 如果您是首次使用 Analytics，则用户风险配置文件需要一些时间才能显示在控制板上。Analytics 使用机器学习来确定用户事件中的风险模式或异常情况，并根据风险的严重程度将用户配置文件识别为高风险、中风险和低风险。

- 使用 自助搜索 功能可以查看和筛选从数据源接收的用户事件（原始数据）。

Citrix Endpoint Management 数据源

December 6, 2021

Endpoint Management 数据源表示与您的 Citrix Cloud 帐户关联的 Citrix Endpoint Management 服务。当用户使用此服务时，Citrix Analytics 会实时接收与用户端点及其事件相关的用户 事 件。处理用户事件以检测任何安全威胁。

必备条件

- 订阅 Citrix Cloud 上提供的 Citrix Endpoint Management。要了解如何设置 Endpoint Management 服务，请参阅 入门和资源设置。
- 已设置云站点和企业目录。确保你有两台运行 Windows 2012 R2 或 Windows 2016 服务器的计算机来安装 Cloud Connector。
- 已安装 **Cloud Connector**。在属于 Active Directory 的虚拟机上下载并安装 Cloud Connector。
- 查看系 统要求 并确保您的环境符合要求。

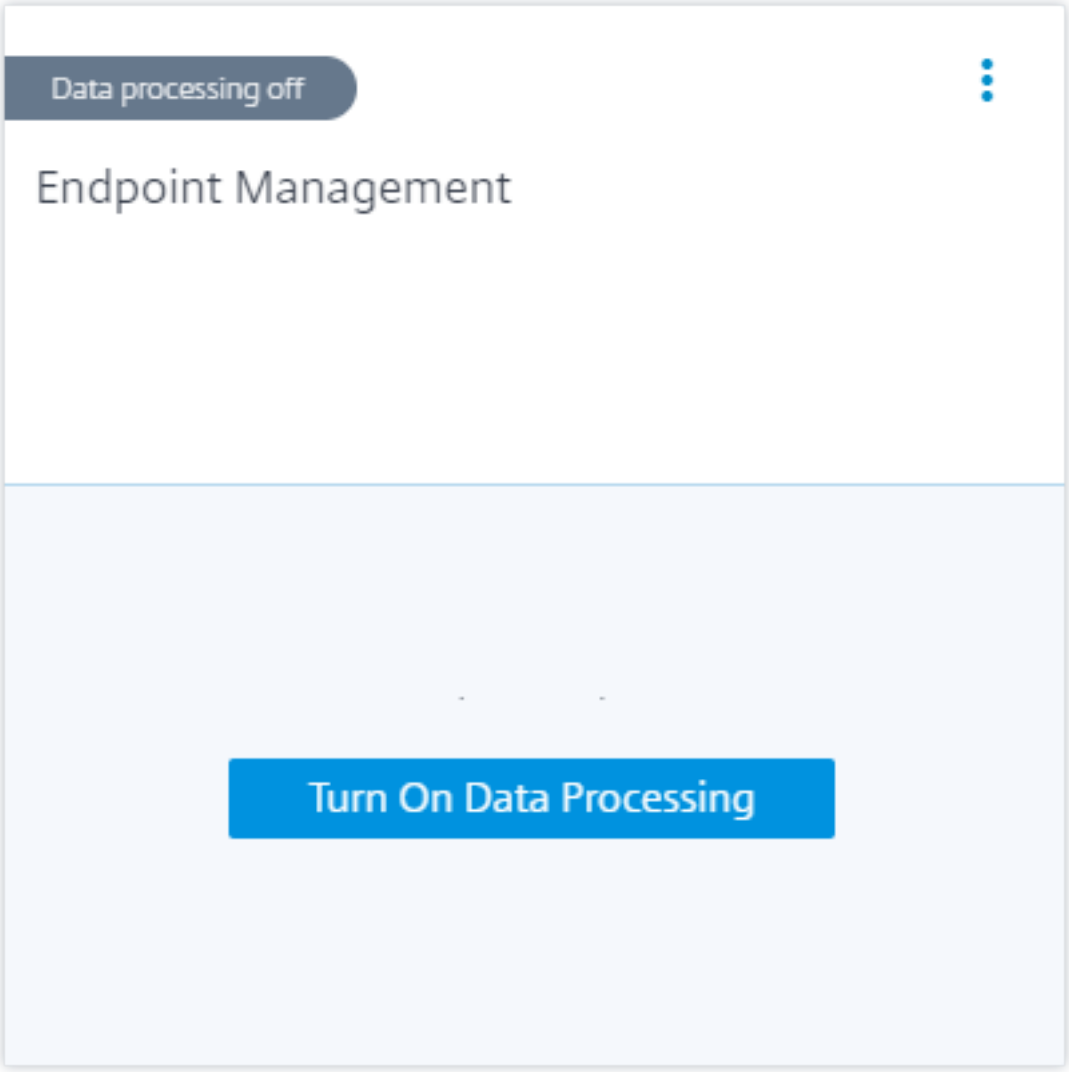
查看数据源并打开数据处理

Citrix Analytics 会自动发现与您的 Citrix Cloud 帐户关联的所有 Endpoint Management 数据源。

要查看数据源：

在顶栏中，单击 设置 > 数据源 > 安全性。

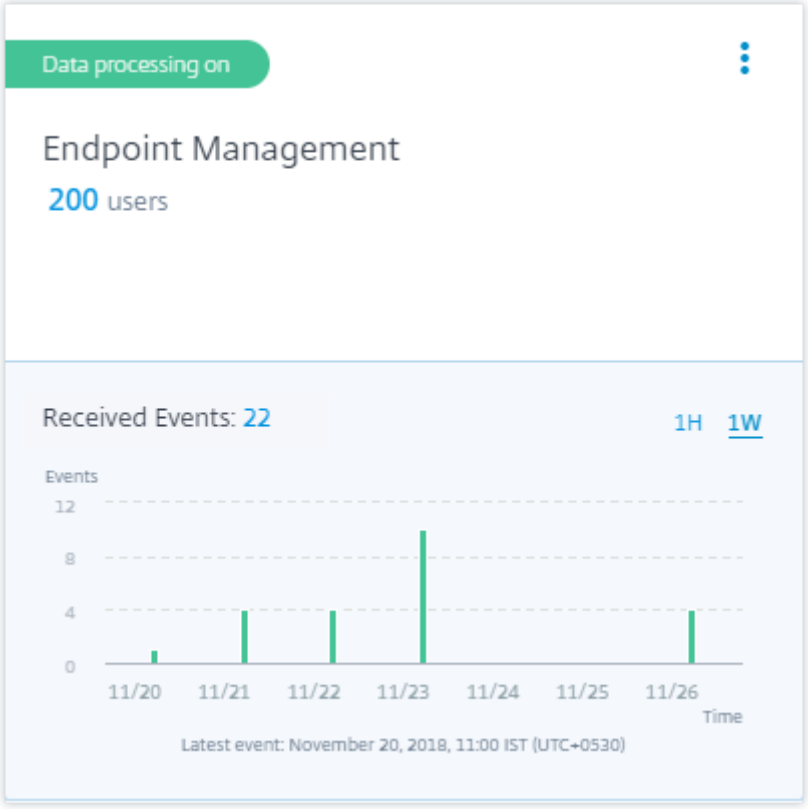
Endpoint Management 数据源的站点卡将显示在“数据源”页面上。单 击打开数据处理 以允许 Citrix Analytics 开始处理此数据源的数据。



查看用户和接收的事件

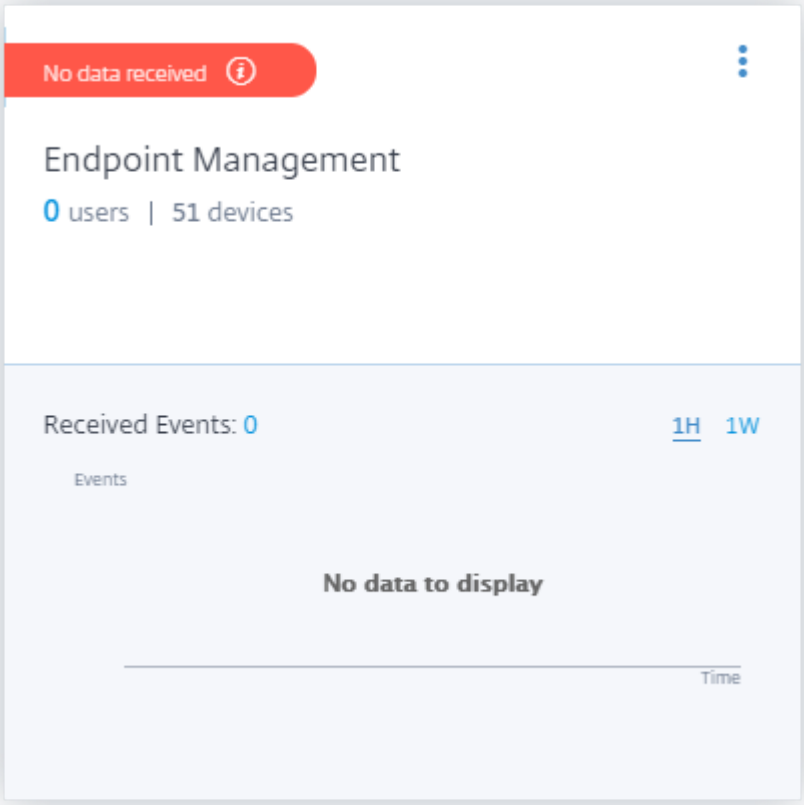
站点卡片显示最近一小时内 Endpoint Management 用户、设备和接收的事件的数量，这是默认的时间选择。您还可以选择 1 周（**1W**）并查看数据。

单击用户数可在“用户”页面上查看用户详细信息。



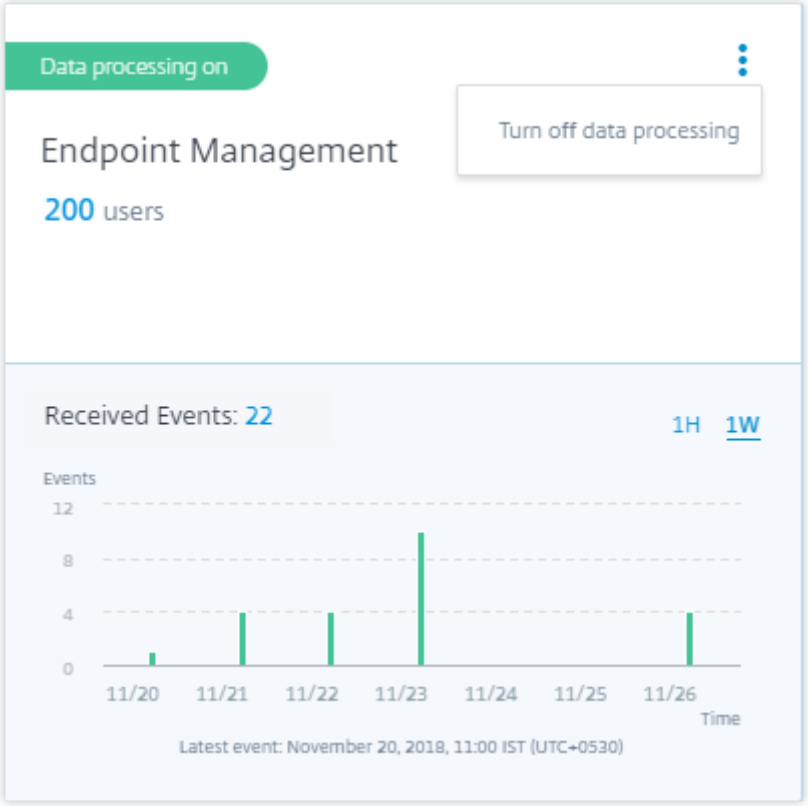
启用数据处理后，站点卡片可能会显示“未收到数据”状态。出现此状态的原因有两个：

1. 如果您是首次启用数据处理，则事件需要一些时间才能到达 Citrix Analytics 中的事件中心。当 Citrix Analytics 收到事件时，状态将更改为“数据处理开启”。如果状态在一段时间后仍未更改，请刷新 数据源 页面。
2. Analytics 在过去一小时内未收到来自数据源的任何事件。

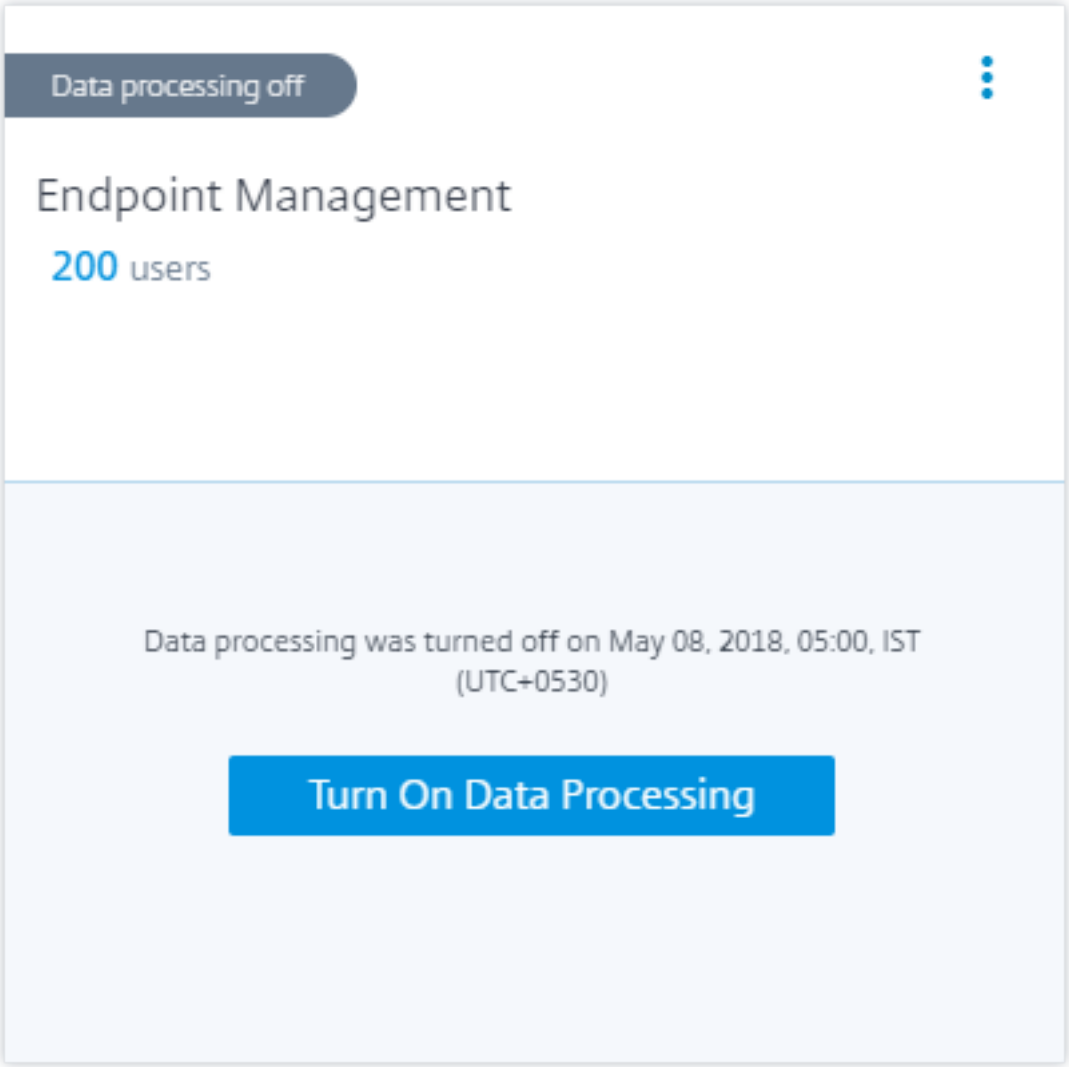


打开或关闭数据处理

要停止数据处理，请单击站点卡片上的垂直省略号 ()，然后单击 关闭数据处理。Citrix Analytics 停止处理此数据源的数据。



要再次启用数据处理，请单击“打开数据处理”。



Citrix Gateway（本地）数据源

April 12, 2024

网关 数据源表示环境中的本地 Citrix Gateway 实例。Citrix Analytics 会自动发现 Citrix Application Delivery Management (ADM) 代理和添加到 Citrix ADM 服务的网关实例。

当用户通过网关访问任何服务或应用程序时，Citrix Analytics 会实时接收用户访问 事件 。处理用户事件以检测任何安全威胁。

有关必备条件和入门步骤的信息，请参阅 Citrix Analytics 平台文档中的 Citrix Gateway 数据源文章。

Citrix Remote Browser Isolation 数据源

March 24, 2023

Remote Browser Isolation 服务隔离 Web 浏览以保护企业网络免受基于浏览器的攻击。它提供对 Internet 托管的 Web 应用程序的一致、安全的远程访问，而无需用户设备配置。

在 Citrix Analytics for Security 中，您可以查看已发布的 Remote Browser Isolation 会话的用户事件。有关用户事件的更多信息，请参阅自助搜索 Remote Browser Isolation。

要接收来自已发布的 Remote Browser Isolation 会话的用户事件，请在远程浏览器隔离中启用主机名跟踪策略。默认情况下，该策略处于禁用状态。

启用主机名跟踪策略允许 Remote Browser Isolation 将用户会话期间使用的主机名发送到 Citrix Analytics for Security。
有关更多信息，请参阅管理已发布的 Remote Browser Isolation。

Citrix Secure Private Access 数据源

April 12, 2024

Secure Private Access 数据源表示与您的 Citrix Cloud 帐户关联的 Citrix Secure Private Access 服务。当用户使用此服务时，Citrix Analytics 会实时接收用户访问 事件 （日志）。处理用户事件以检测任何安全威胁。

必备条件

- 订阅 Citrix Cloud 上提供的 Citrix Secure Private Access 服务。要了解如何开始使用，请参阅 Secure Private Access 服务。
- 查看系 统要求 并确保您的环境符合要求。

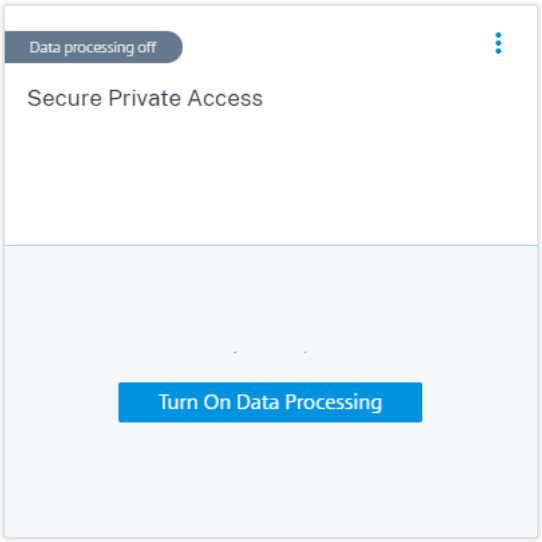
查看数据源并打开数据处理

Citrix Analytics 会自动发现与您的 Citrix Cloud 帐户关联的 Secure Private Access 数据源。

要查看数据源，请执行以下操作：

在顶栏中，单击 设置 > 数据源 > 安全性。

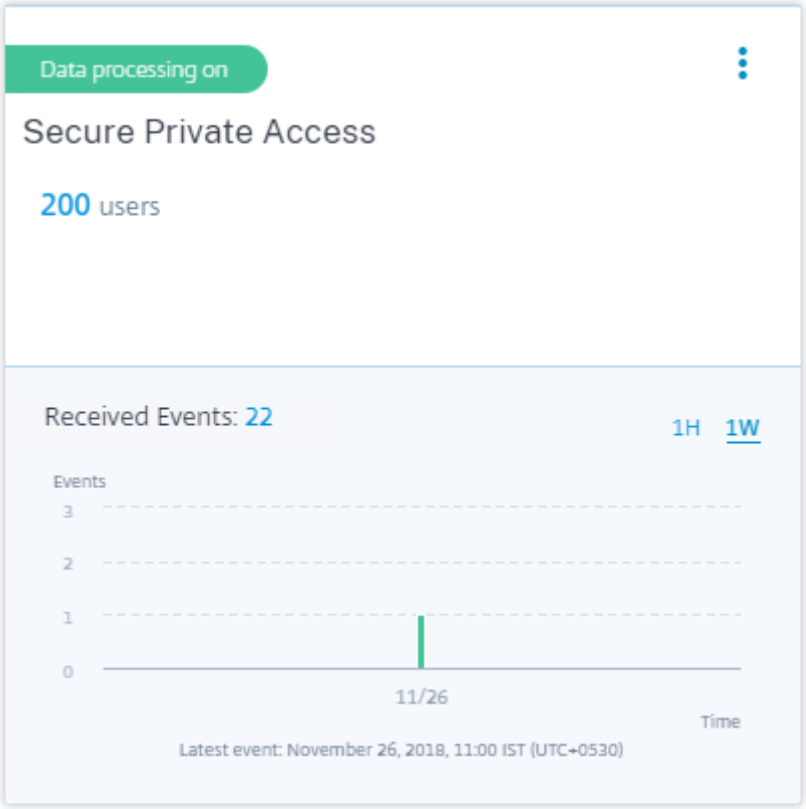
Secure Private Access 数据源的站点卡将显示在“数据源”页面上。单 击打开数据处理 以允许 Citrix Analytics 开始处理此数据源的数据。



查看用户和接收的事件

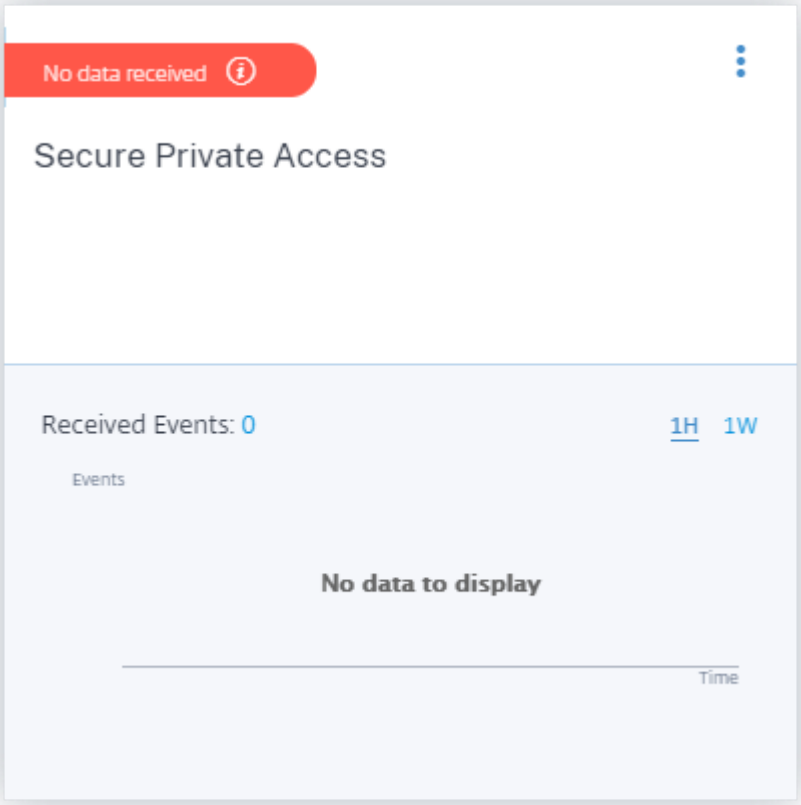
站点卡片显示事件用户数以及过去一小时内从数据源接收的事件，这是默认的时间选择。您还可以选择 1 周 (1 W) 并查看数据。

单击用户数可在“用户”页面上查看用户详细信息。单击已接收事件的数量可在 自助搜索 页面上查看事件详细信息。



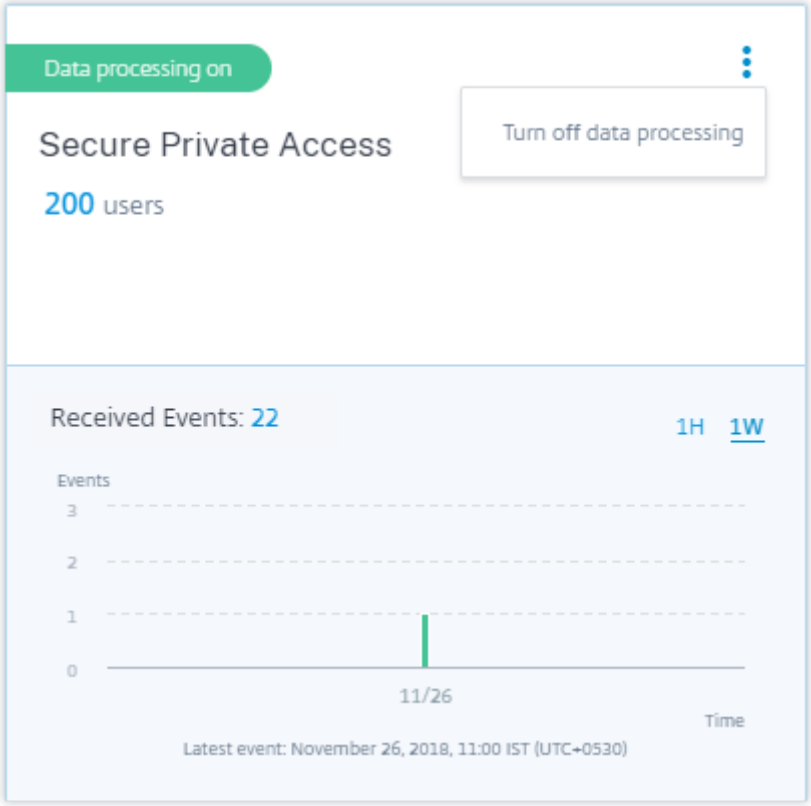
启用数据处理后，站点卡片可能会显示“未收到数据”状态。出现此状态有两种原因：

1. 如果您是首次打开数据处理，事件将需要一些时间才能到达 Citrix Analytics 中的事件中心。当 Citrix Analytics 收到事件时，状态将更改为 **Data processing on**（数据处理已启用）。如果状态在一段时间后仍未更改，请刷新数据源页面。
2. Analytics 在过去一小时内未收到来自数据源的任何事件。

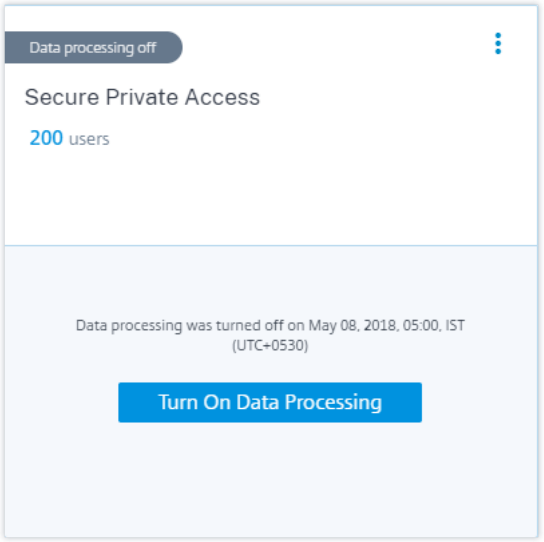


打开或关闭数据处理

要停止数据处理，请单击站点卡片上的垂直省略号 (⋮)，然后单击关闭数据处理。Citrix Analytics 停止处理此数据源的数据。



要再次启用数据处理，请单击“打开数据处理”。



Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源

April 12, 2024

应用程序和桌面数据源代表组织中的本地 Citrix Virtual Apps and Desktops 以及 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）。

Citrix Analytics for Security 支持这两种产品，并从数据源接收用户事件。本文将向您介绍在这两种产品上启用 Analytics 的必备条件和步骤。

Citrix Analytics for Security 从 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 数据源的以下组件接收用户事件：

- 用户设备上安装的 Citrix Workspace 应用程序
- 适用于本地部署的 Citrix Director
- Citrix 监视器服务
- Session Recording Server

当用户使用虚拟应用程序或虚拟桌面时，将在 Citrix Analytics for Security 中实时接收用户事件。

支持的客户版本

当在用户终端节点上使用受支持的客户端版本时，Citrix Analytics 会收到用户事件。如果用户使用的是任何不受支持的客户端版本，则必须将其客户端升级到以下版本之一：

- 适用于 Windows 的 Citrix Workspace 应用程序 1907 或更高版本
- 适用于 Mac 的 Citrix Workspace 应用程序 1910.2 或更高版本
- 适用于 HTML5 的 Citrix Workspace 2007 或更高版本
- 适用于 Chrome 的 Citrix Workspace 应用程序 -Chrome 网上应用店中提供的最新版本
- 适用于 Android 的 Citrix Workspace 应用程序 Google Play 中提供了最新版本
- 适用于 iOS 的 Citrix Workspace 应用程序 - Apple App Store 中提供的最新版本
- 适用于 Linux 的 Citrix Workspace 2006 或更高版本

在 **Citrix DaaS** 上启用分析

必备条件

- 订阅 Citrix Cloud 上提供的 Citrix DaaS。要了解如何开始使用 Citrix DaaS，请参阅安装和配置。
- 查看 系统要求 部分并确保满足要求。

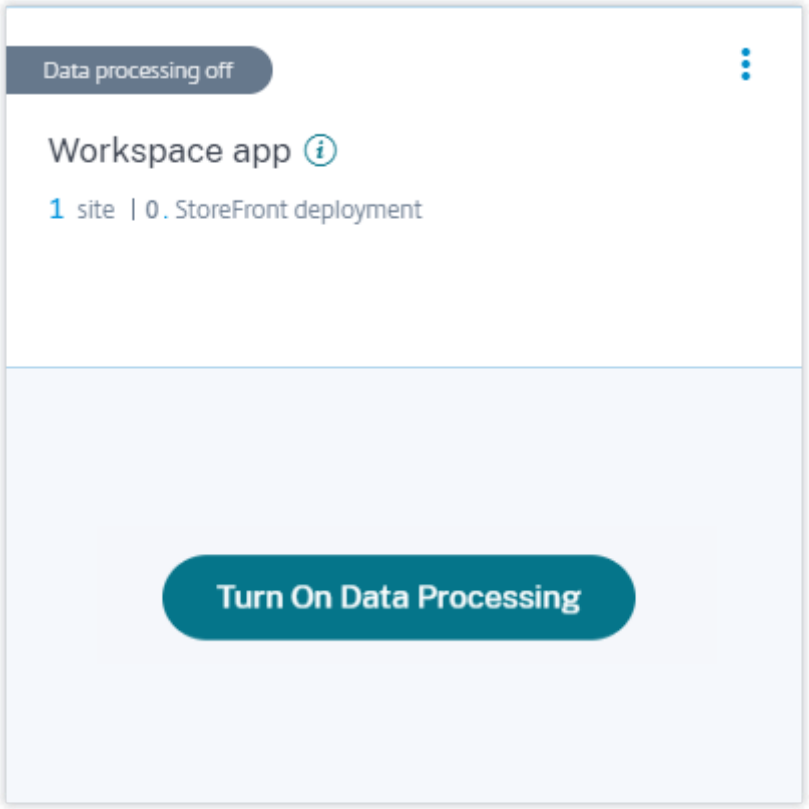
查看数据源并打开数据处理

Citrix Analytics 会自动发现与您的 Citrix Cloud 帐户关联的 Citrix DaaS。

要查看数据源，请执行以下操作：

在顶栏中，单击 设置 > 数据源 > 安全性。

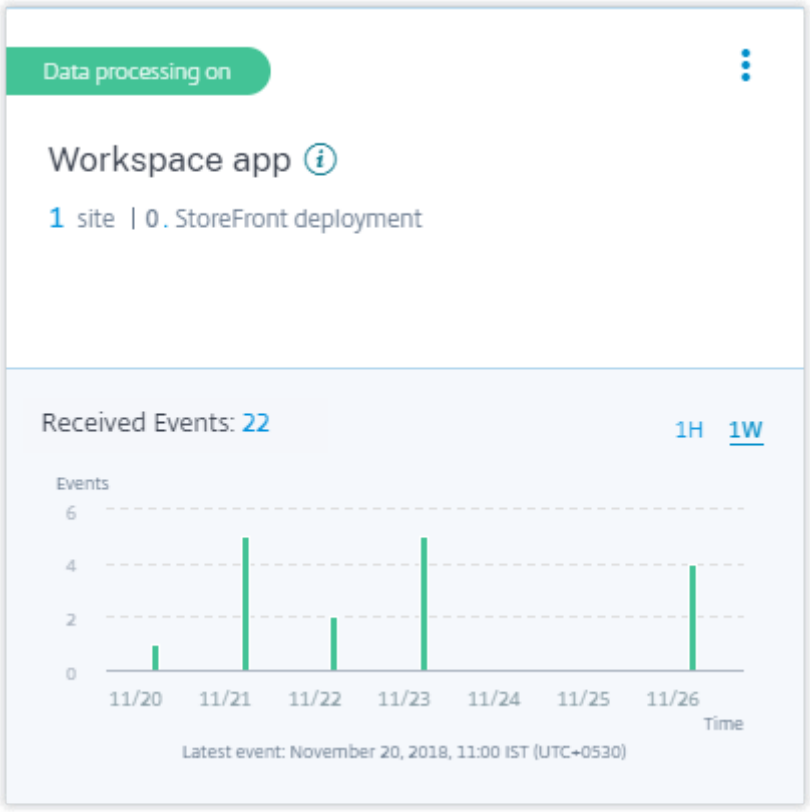
应用程序和桌面 **- Workspace** 应用程序站点卡显示在“数据源”页面上。单 击打开数据处理 以允许 Citrix Analytics 开始处理此数据源的数据。



查看云站点、用户和接收的事件

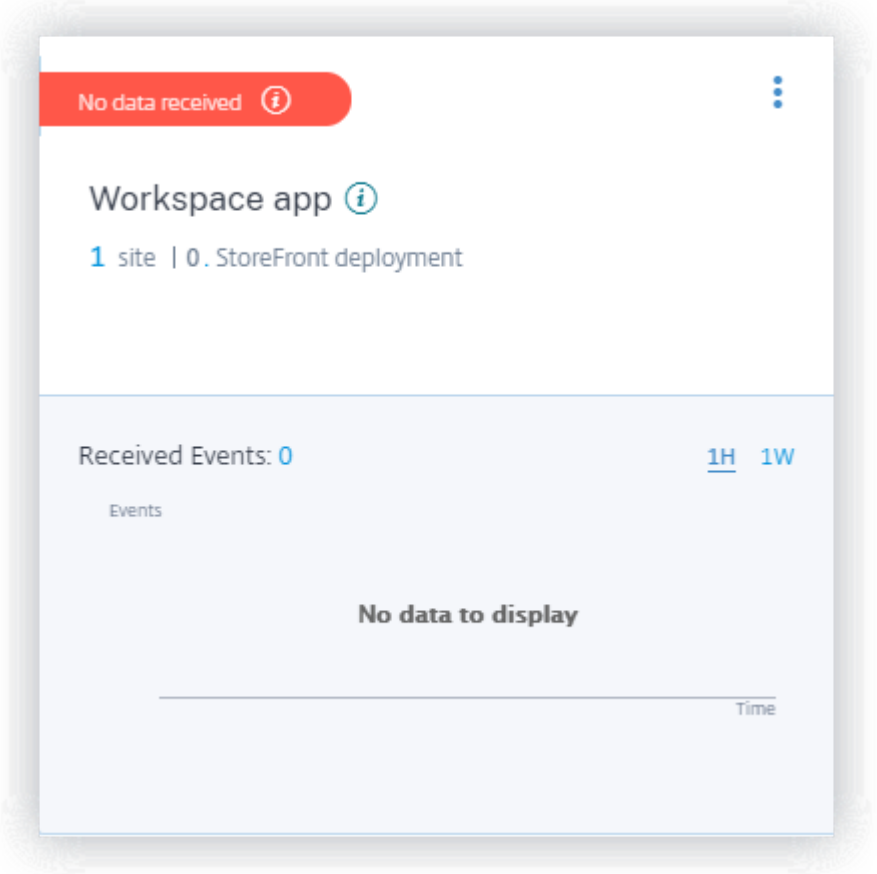
站点卡显示应用程序和桌面用户的数量、发现的云站点以及过去一小时（默认时间选择）内收到的事件。还可以选择 1 周 (1 W) 并查看数据。

单击接收的事件数可在 自助搜索 页面上查看事件。



启用数据处理后，站点卡片可能会显示“未收到数据”状态。出现此状态有两种原因：

1. 如果您是首次打开数据处理，事件将需要一些时间才能到达 Citrix Analytics 中的事件中心。当 Citrix Analytics 收到事件时，状态将更改为 **Data processing on**（数据处理已启用）。如果状态在一段时间后仍未更改，请刷新数据源页面。
2. Analytics 在过去一小时内未收到来自数据源的任何事件。



在本地的 **Citrix Virtual Apps and Desktops** 上启用分析

Citrix Analytics 从添加到 Workspace 的本地站点和通过 StoreFront 部署访问的站点接收用户事件。

如果您的组织正在使用本地站点，则必须使用以下方法之一来加载站点，以便 Analytics 发现站点：

- 使用 StoreFront 加载本地站点
- 使用 Workspace 加载本地站点

必备条件

- 您必须拥有许可证才能使用 Citrix Virtual Apps and Desktops 本地解决方案。要了解如何在本地开始使用 Citrix Virtual Apps and Desktops，请参阅安装和配置。
- 查看 系统要求 部分并确保满足要求。
- 您的 Director 使用的是 1912 CU2 或更高版本。有关详细信息，请参阅功能兼容性列表。
- 订阅 **Citrix Workspace**。如果要将站点添加到 Citrix Workspace，则必须需要 Workspace 订阅。

要购买 Citrix Workspace 订阅，请访问 https://www.citrix.com/products/citrix-workspace/get-started.html 并联系可以为您提供帮助的 Citrix Workspace 专家。

- 已添加到 **Workspace** 的站点。Citrix Analytics 会自动发现添加到 Citrix Workspace 站点。在继续在 Citrix Analytics 上进行登录之前，将站点添加到 Citrix Workspace 此过程称为 站点聚合。

  站点聚合要求您安装 Cloud Connector，配置 NetScaler Gateway STA 服务器以实现与 Workspace 资源的内部和外部连接，然后将站点添加到 Workspace 中。有关站点聚合的详细说明，请参阅聚合工作区中的本地虚拟应用程序和桌面。

- **StoreFront** 版本。如果您正在为站点使用 StoreFront 部署，请确保 StoreFront 版本为 1906 或更高版本。

使用 **StoreFront** 载入 **Citrix Virtual Apps and Desktops** 本地站点

有关必备条件和入门步骤的信息，请参阅 Citrix Analytics 平台文档中的 Citrix Virtual Apps and Desktops 数据源文章。

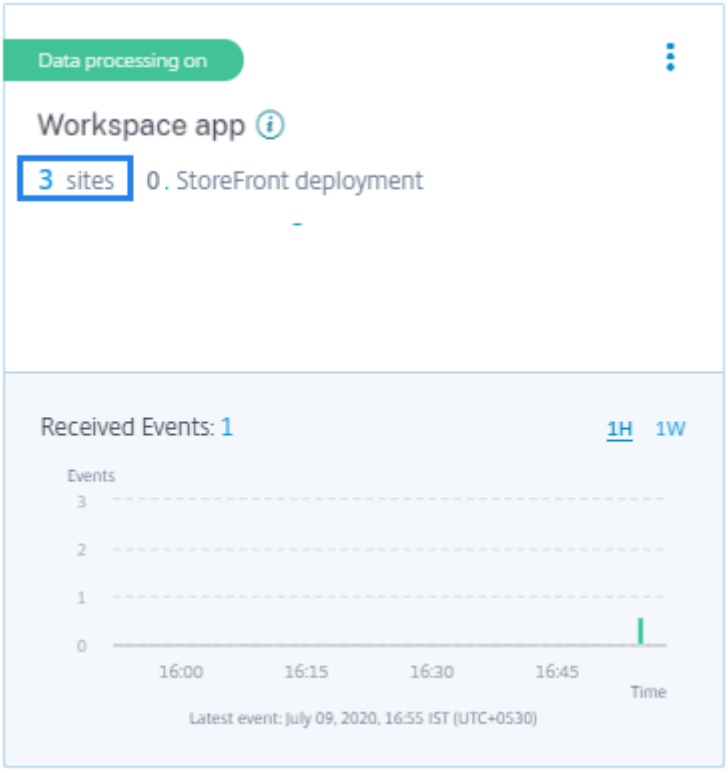
使用 **Workspace** 上载 **Citrix Virtual Apps and Desktops** 本地站点

已添加到 **Citrix Workspace** 的站点　Citrix Analytics 会自动发现已添加到 Citrix Workspace 的本地站点，并将其显示在数据源站点卡片上。

要查看数据源，请执行以下操作：

在顶栏中，单击 设置 > 数据源 > 安全性。

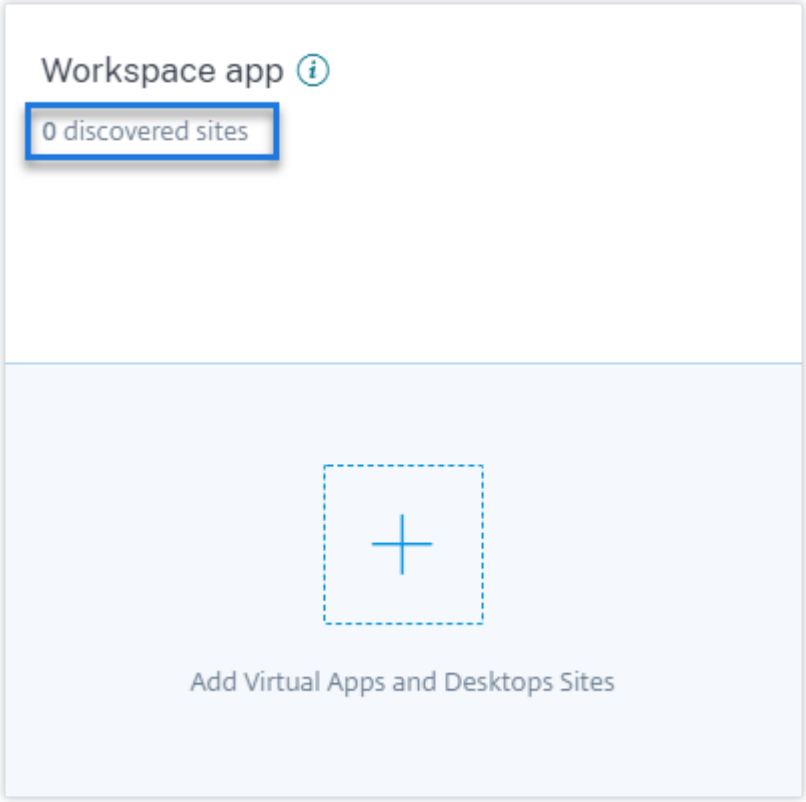
“应用程序和桌面”站点卡显示添加到 Workspace 的站点数量以及连接到这些站点的用户。单击站点计数以查看发现的站点。单击用户计数可在“用户”页面上查看发现的 用户。



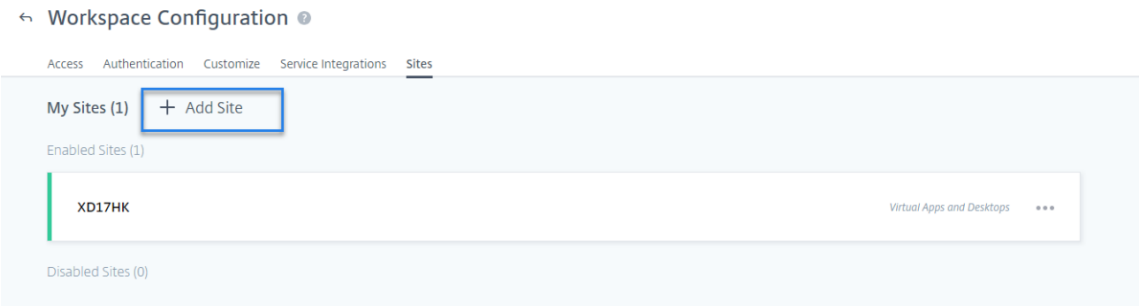
未添加到 **Citrix Workspace** 的站点　如果您尚未将本地站点添加到 Workspace，Analytics 将无法发现您的站点。站点卡片显示 **0** 个已发现的站点。

要将站点添加到 **Workspace**，请执行以下操作：

1. 单击站点卡片上的 +。



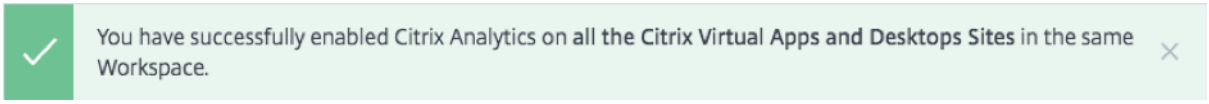
2. 在“**Workspace** 配置”页面上，单击 **+** 添加站点。



3. 按照屏幕上的说明添加站点。有关更多信息，请参阅 聚合工作区中的本地虚拟应用程序和桌面。
4. 添加站点后，重新登录到 Citrix Analytics 并刷新“数据源”页面以在站点卡片上查看最近添加的站点。

打开数据处理并查看接收的事件　要允许 Analytics 开始处理已发现站点的数据，请单击站点卡片上的“打开数据处理”，然后按照屏幕上的提示进行操作。

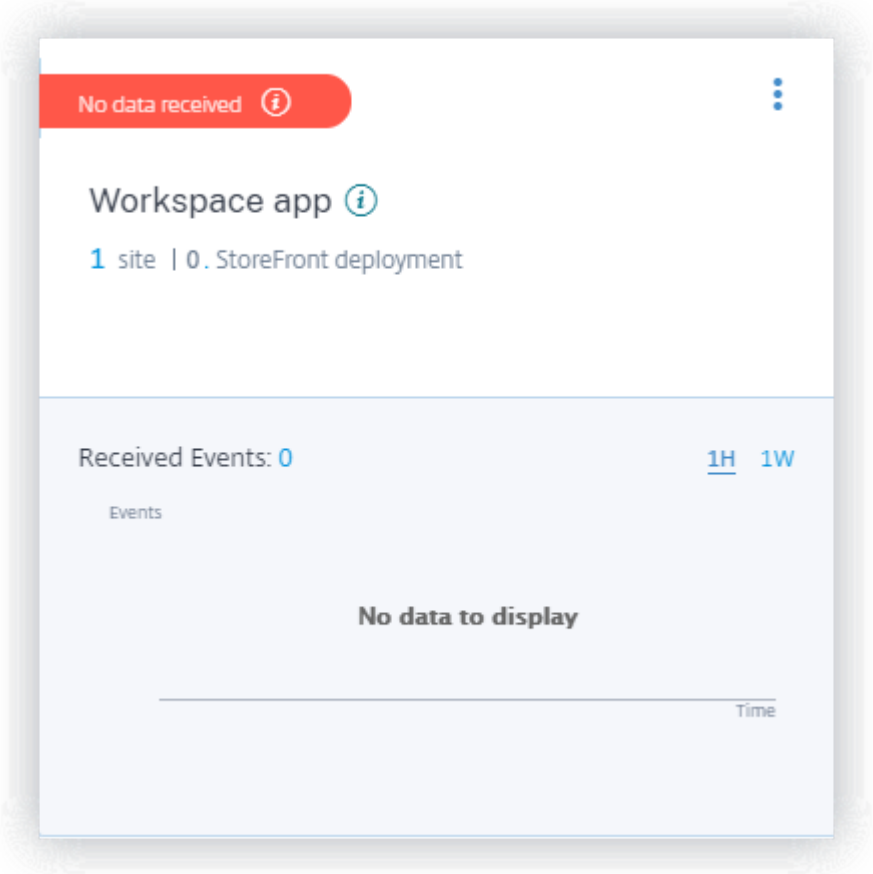
如果您有多个站点添加到同一个 Workspace，Analytics 将处理并存储工作区中所有站点的数据。在所有网站上成功启用 Analytics 后，您会收到一条成功消息。



站点卡片显示最近一小时内收到的事件，这是默认的时间选择。还可以选择 1 周 (1 W) 并查看数据。单击接收的事件数可在相应的 自助搜索 页面上查看事件。

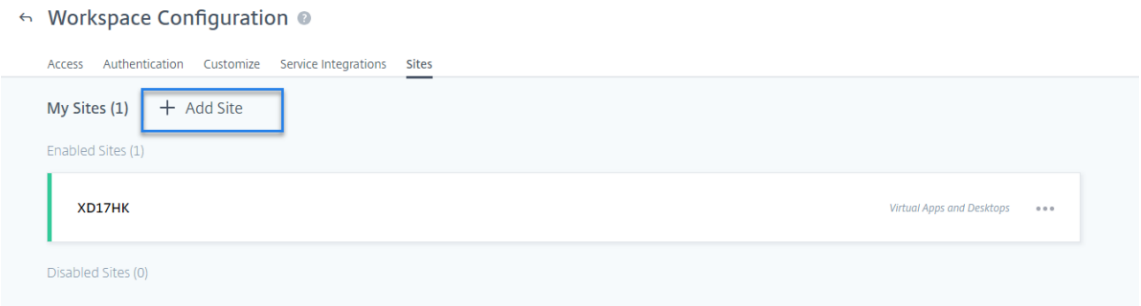
启用数据处理后，站点卡片可能会显示“未收到数据”状态。出现此状态有两种原因：

1. 如果您是首次打开数据处理，事件将需要一些时间才能到达 Citrix Analytics 中的事件中心。当 Citrix Analytics 收到事件时，状态将更改为 **Data processing on**（数据处理已启用）。如果状态在一段时间后仍未更改，请刷新数据源页面。
2. Analytics 在过去一小时内未收到来自数据源的任何事件。



添加站点　如果要向 Workspace 添加另一个本地站点，可以通过 Analytics 进行添加：

1. 在“Workspace 配置”页面上，单击 **+** 添加站点。



2. 按照屏幕上的说明添加站点。有关更多信息，请参阅 聚合工作区中的本地虚拟应用程序和桌面。
3. 添加站点后，请转到 Citrix Analytics 并刷新“数据源”页面以查看站点卡上最近添加的站点。

连接到适用于本地站点的 **Citrix Director**

Citrix Director 是适用于 Citrix Virtual Apps and Desktops 的监视和故障排除控制台。您可以使用 Director 为 Citrix Analytics for Security (Security Analytics). 配置本地站点。配置站点后，Director 会将监视事件发送到 Security Analytics。

如果您使用的是 Citrix DaaS，Citrix Monitor 服务会将事件从您的云站点发送到 Security Analytics。

在同时进行云和本地部署的混合环境中，Security Analytics 会接收来自 Citrix Monitor 服务和 Citrix Director 上载站点的事件。

先决条件和配置步骤

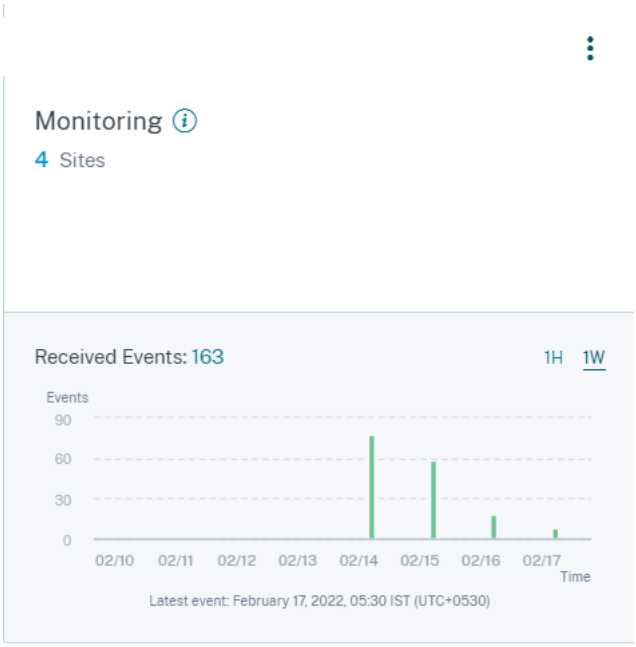
> 备注
>
> - 目前，Director 用户界面显示与 Citrix Analytics for Performance (Performance Analytics) 相关的配置步骤。这些配置步骤也适用于 Citrix Analytics for Security (Security Analytics)。如果您拥有 Security Analytics 的有效 Citrix Cloud 授权，则可以按照以下步骤连接到 Citrix Director。
> - 如果您的 Citrix Cloud 帐户具有 Security Analytics 和 Performance Analytics 的有效授权，并且您已经为站点配置了 Performance Analytics，则无需再次为 Security Analytics 配置 Director。

有关必备条件和配置步骤的信息，请参阅 Citrix Analytics for Performance 文档。

查看已连接的站点和接收的事件

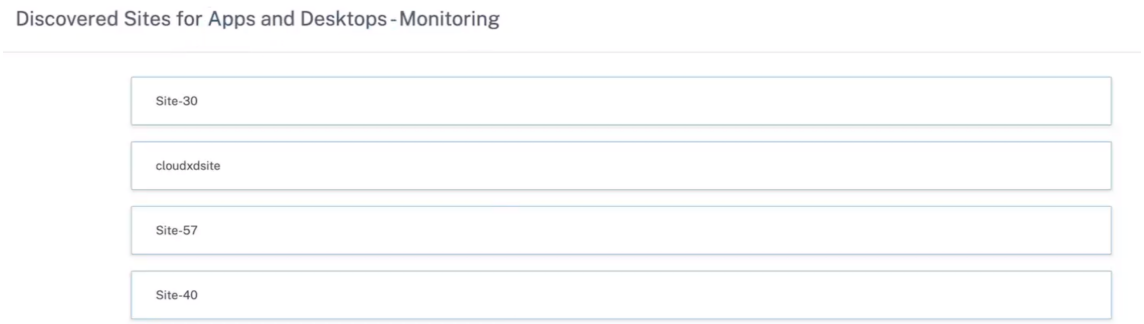
1. 在 Citrix Analytics 中，转到“数 据源”页面。
2. 单击安全选项卡。

3. 在“应用程序和桌面-监视”站点卡上，您可以查看本地站点或云站点（以适用者为准）。您还可以查看从站点接收的事件。



> 备注
>
> - 首次在 Director 上配置本地站点时，来自该站点的事件可能需要一些时间（大约一个小时）才能得到处理，从而导致连接的站点在 应用程序和桌面监视 站点卡上的显示延迟。
> - 在监视站点卡片上，默认情况下启用监视器服务或 Director 数据源的数据处理。您还可以根据需要关闭数据处理。但是，建议继续进行数据处理，以便从 Security Analytics 中获得最大收益。

4. 点击该网站查看详细信息。



连接到 **Session Recording** 部署

Session Recording 允许您在 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 中录制任何用户会话的屏幕活动。您可以将 Session Recording Server 配置为将用户事件发送给 Citrix Analytics for Security。处理用户事件以提供有关用户危险行为的切实可行的见解。

必备条件

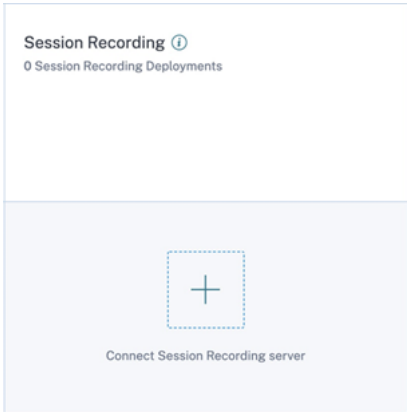
在开始之前，请确保执行以下操作：

- 您的 Session Recording Server 和 VDA 代理必须为 2103 或更高版本。
- Session Recording Server 必须能够连接到所需的地址。有关 URL 的详细信息，请参阅网络要求。
- Session Recording 部署必须为出站 Internet 连接打开端口 443。网络上的任何代理服务器都必须允许与 Citrix Analytics for Security 进行此通信。
- 如果您使用的是 Citrix Virtual Apps and Desktops 7 1912 LTSR，支持的 Session Recording 版本为 2103 或更高版本。

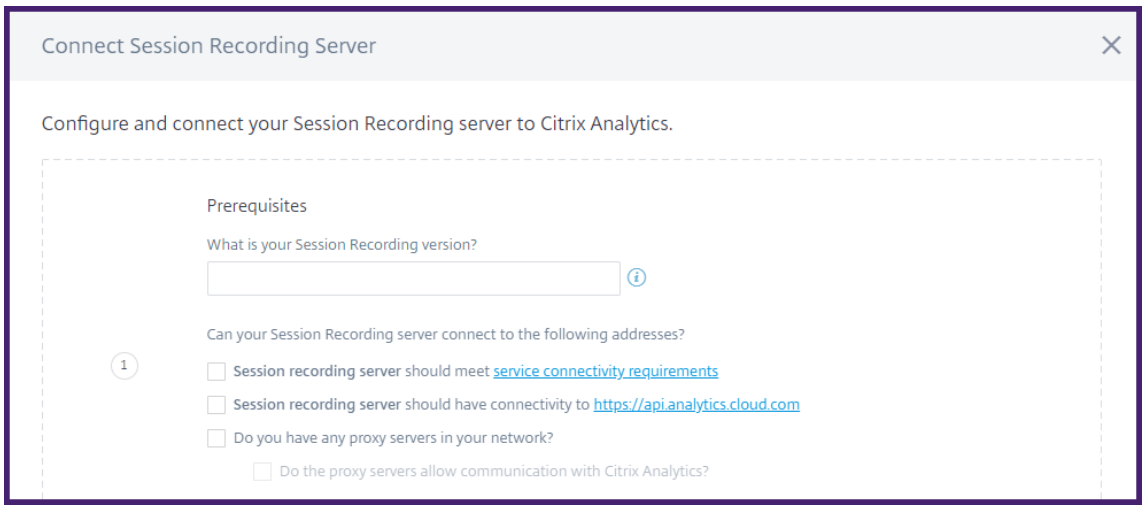
> 注意：
>
> 使用 **Session Recording** 服务时，请务必验证其他连接要求。

配置 **Session Recording Server**

1. 在应用程序和桌面 **- Session Recording** 站点卡上，单击连接 **Session Recording Server**。



2. 在 **Connect Session Recording Server**（连接 Session Recording Server）页面上，查看核对清单，然后选择所有必须满足的要求。如果未选择必须满足的要求，则会禁用 Download File（下载文件）选项。



3. 如果您的网络中有代理服务器，请在 Session Recording Server 的 *SsRecStorageManager.exe.config* 文件中输入代理地址。

   配置文件位于 `<Session Recording Server installation path>\bin\SsRecStorageManager.exe.config`

   例如：`C:\Program Files\Citrix\SessionRecording\Server\Bin\SsRecStorageManager.exe.config`

4. 单击下载文件以下载 *SessionRecordingConfigurationFile.json* 文件。

   > 注意
   >
   > 该文件包含敏感信息。请将该文件保存在安全的位置。

5. 请将该文件复制到要连接到 Citrix Analytics for Security 的 Session Recording Server 。
6. 如果您的部署中有多个 Session Recording Server ，则必须在要连接的每台服务器中复制该文件，然后按照步骤配置每台服务器。

7. 在 Session Recording Server 上，运行以下命令以导入设置：

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

例如：

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

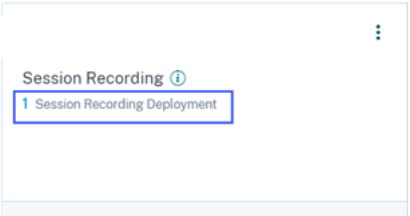
8. 重新启动以下服务：
   - Citrix Session Recording Analytics Service
   - Citrix Session Recording Storage Manager
9. 配置成功后，转到 Citrix Analytics for Security 查看连接的 Session Recording Server 。单击打开数据处理以允许 Citrix Analytics for Security 处理数据。

> 注意
>
> 如果使用的是 Session Recording Server 版本 2103 或 2104，则必须首先启动应用程序和桌面会话，才能在 Citrix Analytics for Security 上查看连接的 Session Recording Server。否则，连接的 Session Recording Server 将无法显示。此要求不适用于 Session Recording Server 版本 2106 及更高版本。

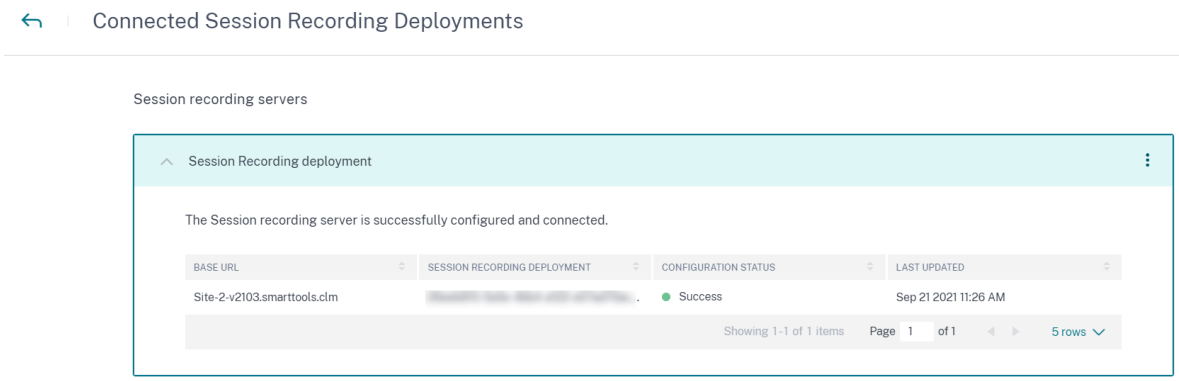
查看已连接的部署

仅当配置成功时，服务器部署才会显示在 Session Recording 站点卡片上。站点卡片显示已与 Citrix Analytics for Security 建立连接的已配置服务器的数量。

如果即使在配置成功之后仍看不到 Session Recording Server，请参阅故障排除一文。



在站点卡片上，单击部署数量以查看与 Citrix Analytics for Security 连接的服务器组。例如，单击 **1 Session Recording Deployment**（1 Session Recording 部署）可查看连接的一个或多个服务器组。每个 Session Recording Server 都由一个基本 URL 和一个 ServerGroupID 表示。



查看收到的事件

站点卡片显示连接的 Session Recording 部署以及过去一小时（默认时间选择）从这些部署接收的事件。还可以选择 1 周并查看数据。单击接收的事件数量可在自助搜索页面上查看事件。

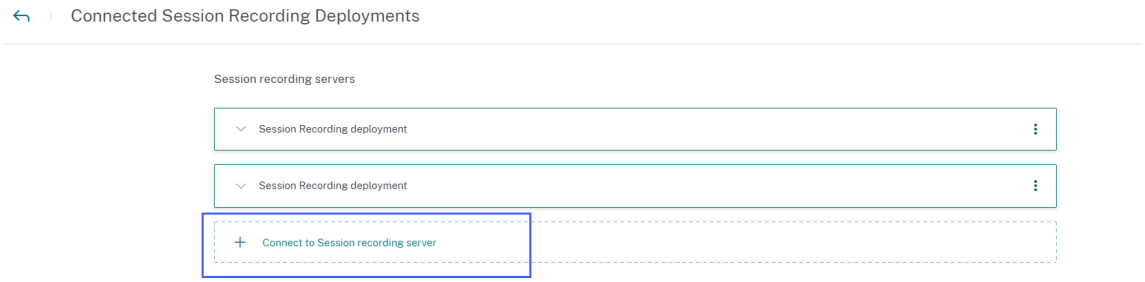
启用数据处理后，站点卡片可能会显示 **No data received**（未收到数据）状态。出现此状态有两种原因：

1. 如果您是首次打开数据处理，事件将需要一些时间才能到达 Citrix Analytics 中的事件中心。当 Citrix Analytics 收到事件时，状态将更改为 **Data processing on**（数据处理已启用）。如果状态在一段时间后仍未发生变化，请刷新“Data Sources”（数据源）页面。
2. Citrix Analytics 在过去一小时内未收到来自数据源的任何事件。

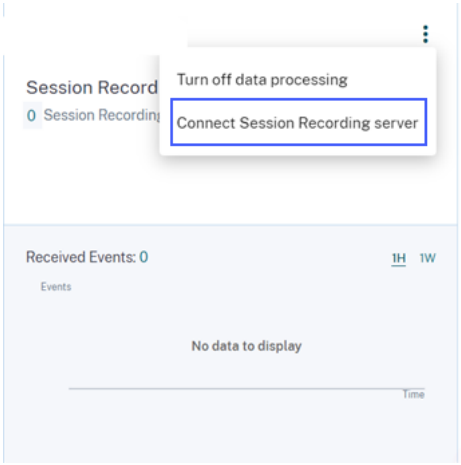
添加 **Session Recording Server**

要添加 Session Recording Server ，请执行以下操作之一：

- 在 **Connected Session Recording Deployments**（已连接的 Session Recording 部署）页面上，单击 **Connect to Session recording server**（连接到 Session Recording Server）。



- 在应用程序和桌面 **- Session Recording** 站点卡上，单击垂直省略号 (⋮)，然后选择连接 **Session Recording Server**。

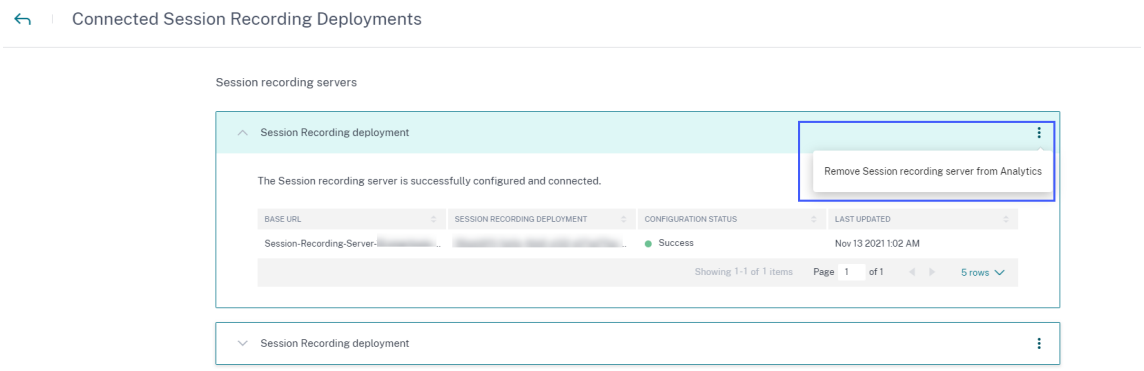


按照步骤下载配置文件并配置 Session Recording Server 。

删除 **Session Recording Server**

要删除 Session Recording Server ，请执行以下操作：

1. 在 Citrix Analytics for Security 上，转到 **Connected Session Recording Deployments**（已连接的 Session Recording 部署）页面，然后选择要删除的服务器部署。
2. 单击垂直省略号 (⋮)，然后选择 **Remove Session Recording server from Analytics**（从 Analytics 中选择删除 Session Recording Server)。



3. 在已从 Citrix Analytics 中删除的 Session Recording Server 上，运行以下命令：

```
<Session Recording Server installation path>\bin\SsRecUtils.exe -
    Remove_SRCasConfigurations
```

例如：

```
C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.
exe -Remove_SRCasConfigurations
```


为 **Citrix DaaS** 启用打印遥测

当用户在 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）中执行打印作业时，您可以在 Citrix Analytics for Security 中查看与这些打印作业相关的日志。这些打印日志提供有关打印活动的重要信息，例如打印机名称、打印文件名和打印份数总数。

> 注意
>
> 只有 Citrix DaaS 支持此功能。

在 Citrix Analytics for Security 中，在“搜索”页面上，您可以选择 应用程序和桌面 数据源来查看打印日志。作为安全管理员，您可以使用这些日志对用户进行风险分析和调查。

默认情况下，打印遥测功能（即收集和传输这些打印日志）在 Virtual Delivery Agent (VDA) 上处于禁用状态。

要启用打印遥测和将打印日志传输到 Citrix Analytics for Security，您需要创建注册表项并配置 VDA。

> 重要
>
> 信息此配置仅适用于 Windows VDA。

必备条件

- 您的 VDA 版本必须与 Citrix Virtual Apps and Desktops 7 2203 LTSR 或更高版本的基准版本相同。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 7 2203 基准组件。
- 您必须具有完全访问权限才能执行注册表项更新。

在电源管理的计算机中启用打印遥测

电源管理的计算机包括虚拟机或刀片 PC，其情景如下：

- 现有主映像
- 新的主映像

为 **VDA** 版本低于 **Citrix Virtual Apps and Desktops 7 2203 LTSR** 的现有主映像启用打印遥测

1. 登录主 VDA 计算机并创建当前状态的快照。
2. 通过添加以下注册表项启用打印服务日志：
   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   有关注册表项的更多信息，请参阅 创建注册表项。

3. 将 VDA 升级到 Citrix Virtual Apps and Desktops 7 2203 LTSR 或更高版本的基准版本。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 7 2203 基准组件。
4. 关闭计算机电源并拍摄最新状态的快照。
5. 登录 Citrix Cloud。选择计算机目录，单击 更新计算机，然后按照屏幕上的说明进行操作。有关详细信息，请参阅创建计算机目录。
6. 等待 24 小时。配置会在 24 小时内自动推送。如果配置已经完成，则无需等待。
7. 使用 Citrix Workspace 应用程序启动桌面会话。使用客户端打印机触发的所有打印事件都在 Citrix Analytics for Security 的搜索页面上可见。

对现有主映像启用打印遥测功能，其中 **VDA** 版本与 **Citrix Virtual Apps and Desktops 7 2203 LTSR** 或更高版本相同　选项 **1**：在主 VDA 中添加打印注册表项并更新虚拟桌面。

1. 登录主 VDA 计算机并创建当前状态的快照。
2. 通过添加以下注册表项启用打印服务日志：

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   有关注册表项的更多信息，请参阅 创建注册表项。
3. 关闭 VDA 计算机的电源并拍摄最新状态的快照。
4. 登录 Citrix Cloud，选择计算机目录，单击“更新计算机”，然后按照屏幕上的说明进行操作。
5. 使用 Citrix Workspace 应用程序启动桌面会话。使用客户端打印机触发的所有打印事件都在 Citrix Analytics for Security 的搜索页面上可见。

选项 **2**：将虚拟桌面移动到组织单位 (OU) 并使用 GPO 创建注册表项

> 注意
>
> 选项 2 方法仅适用于静态计算机。对于随机计算机，必须遵循选项 1 的方法（如上所述）。

1. 登录到域控制器计算机。
2. 通过添加以下注册表项启用打印服务日志：

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   有关注册表项的更多信息，请参阅 创建注册表项。

> 注意
>
> 在任何域控制器中，创建注册表项都是一次性任务。

1. 从 Citrix Cloud 重新启动 VDA 计算机。
2. 使用 Citrix Workspace 应用程序启动桌面会话。使用客户端打印机触发的所有打印事件都在 Citrix Analytics for Security 的搜索页面上可见。

在新主映像中启用打印遥测

1. 使用虚拟机管理程序的管理工具创建虚拟机 (VM)。此 VM 被视为主 VDA。
2. 确保已将主 VDA 添加到所需的域中。
3. 登录主 VDA 并通过添加以下注册表项启用打印服务日志：

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   有关更多信息，请参阅 创建注册表项。
4. 安装适用于 Citrix Virtual Apps and Desktops 7 2203 LTSR 或更高版本的 VDA 版本。安装 VDA 时，选择主映像选项。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 7 2203 基准组件。
5. 确保已将托管连接添加到 Citrix Cloud。有关详细信息，请参阅创建计算机目录。
6. 使用主映像创建计算机目录。有关详细信息，请参阅创建计算机目录。
7. 创建交付组并添加计算机目录。有关详细信息，请参阅创建交付组。
8. 等待 24 小时。组策略引擎会在 24 小时内自动推送配置。
9. 使用 Citrix Workspace 应用程序启动桌面会话。使用客户端打印机触发的所有打印事件都在 Citrix Analytics for Security 的搜索页面上可见。

在未进行电源管理的计算机中启用打印遥测

非电源管理的计算机包括具有以下情形的物理计算机：

- 现有物理 VDA
- 新的物理 VDA

为 **VDA** 版本低于 **Citrix Virtual Apps and Desktops 7 2203 LTSR** 的现有物理 **VDA** 启用打印遥测

1. 通过添加以下注册表项启用打印服务日志：

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   有关更多信息，请参阅 创建注册表项。

2. 将 VDA 升级到 Citrix Virtual Apps and Desktops 7 2203 LTSR 或更高版本的基准版本。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 7 2203 基准组件。
3. 等待 24 小时。配置会在 24 小时内自动推送。如果配置已经完成，则无需等待。
4. 使用 Citrix Workspace 应用程序启动桌面会话。使用客户端打印机触发的所有打印事件都在 Citrix Analytics for Security 的搜索页面上可见。

为新的物理 **VDA** 启用打印遥测

1. 创建物理 VM 并将域更改为所需的域名。
2. 登录到 VM 并通过添加以下注册表项启用打印服务日志：

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   有关更多信息，请参阅 创建注册表项。
3. 安装适用于 Citrix Virtual Apps and Desktops 7 2203 LTSR 版本或更高版本的 VDA 版本。安装 VDA 时，选择“Remote PC Access”选项。
4. 创建计算机目录。有关详细信息，请参阅创建计算机目录。

   > 注意
   >
   > 必须将计算机管理选为 非电源管理的计算机（例如，物理机）。

5. 创建交付组并添加计算机目录。有关详细信息，请参阅创建交付组。
6. 等待 24 小时。组策略引擎会在 24 小时内自动推送配置。
7. 使用 Citrix Workspace 应用程序启动桌面会话。所有使用客户端打印机触发的打印事件都在 Citrix Analytics for Security 的“搜索”页面中可见。

创建注册表项

在 VDA 中，执行以下选项之一：

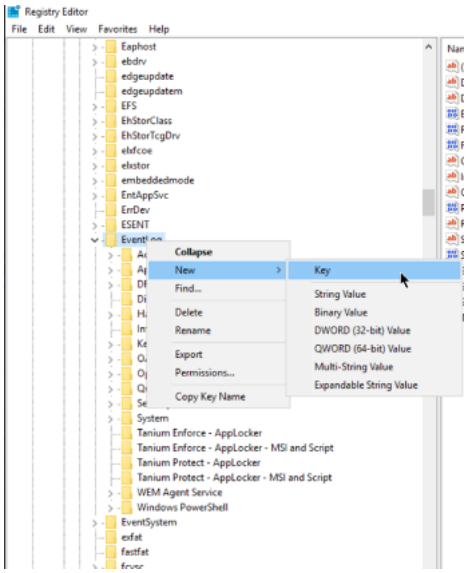
- 手动创建注册表项。此方法适用于主 VDA，且部署中的物理 VDA 数量较少。
- 使用组策略对象 (GPO) 创建注册表项。当您的部署具有更多物理 VDA 计算机并且必须在所有计算机中启用打印遥测功能时，请使用此方法。

注册表项详情

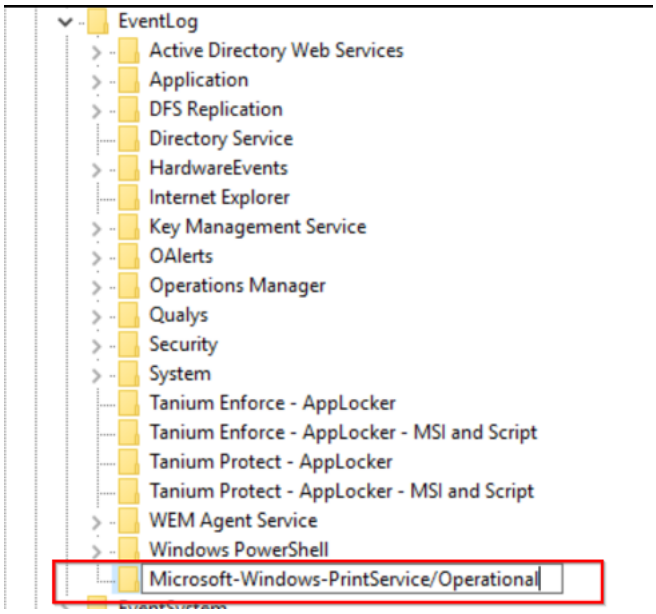
SL	注册表项名称	密钥的用途	注册表详情
1	Microsoft-Windows-PrintService/Operational	在事件查看器中启用打印服务日志。	注册表路径：HKLM:\SYSTEM\CurrentControlSet\
2	ShowJobTitleInEventLogs	控制打印事件日志中是否包含打印作业名称，如果不包含，则考虑使用通用作业名称“打印文档”。	注册表配置单元：HKEY_LOCAL_MACHINE 注册表路径：Software\Policies\Microsoft\Windows NT\Printers 值名称：ShowJobTitleInEventLogs 值类型：REG_DWORD 值：1

在 **VDA** 计算机中手动创建注册表项　使用此方法在 VDA 主映像中创建注册表项。将密钥添加到主映像有助于保持使用主映像创建的所有类型的 VDA 的密钥持久性。

1. 登录 VDA 主计算机。
2. 打开运行并键入注册表编辑器以打开 Windows 注册表。
3. 前往位置 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog
4. 右键单击 **EventLog**，然后选择 新建 **>** 密钥。

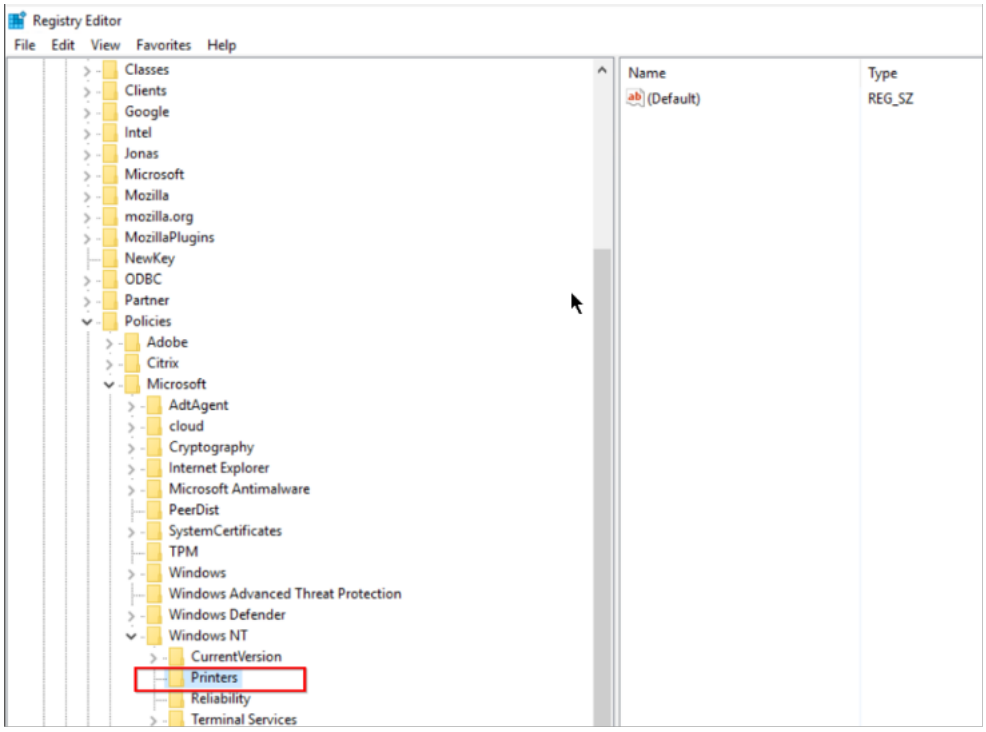


5. 创建名为 **Microsoft-Windows-PrintService/Operational** 的键此键启用打印服务日志。

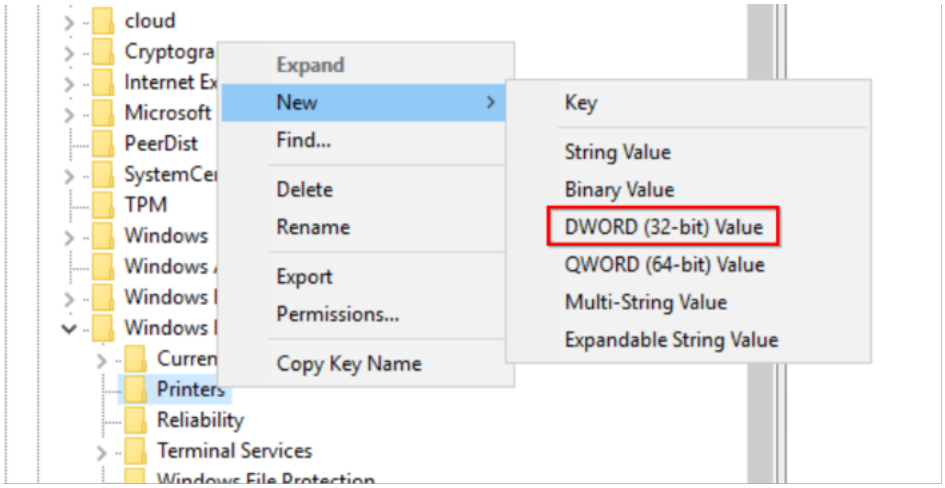


6. 前往位置 **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers**。

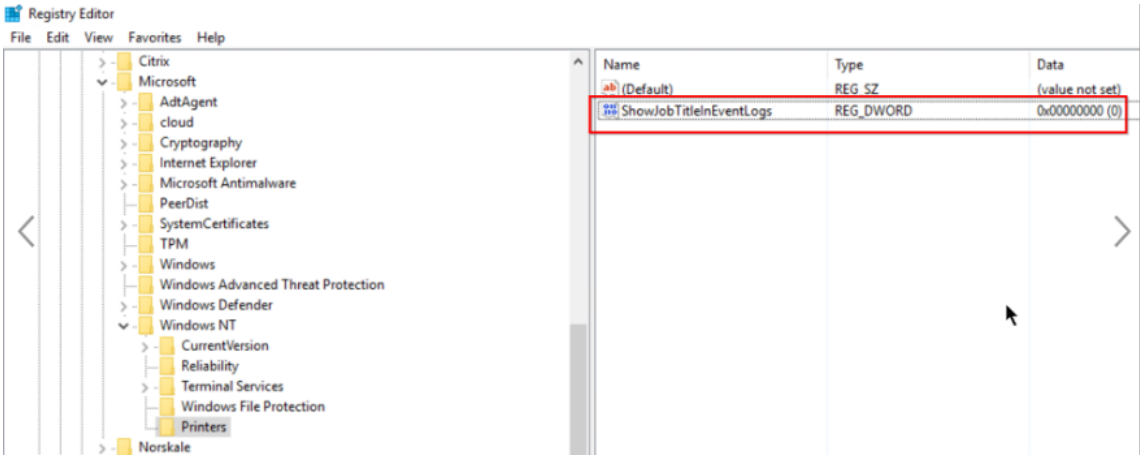
> 注意
>
> 如果“打印机”文件夹不可用，请在 Windows NT 文件夹中创建名为“打印机”的密钥。



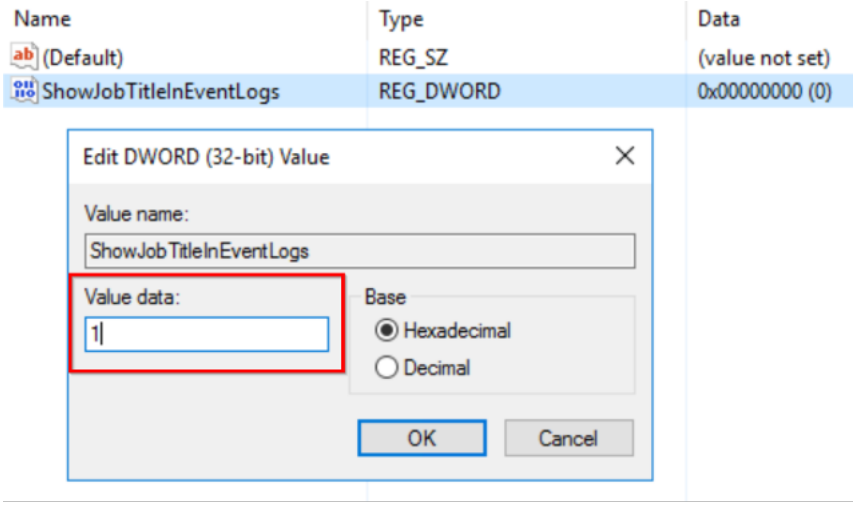
7. 右键单击打印机文件夹，然后选择新建 **> DWORD (32 位)** 值。



8. 创建一个名为 **ShowJobTitleInEventLogs** 的值。



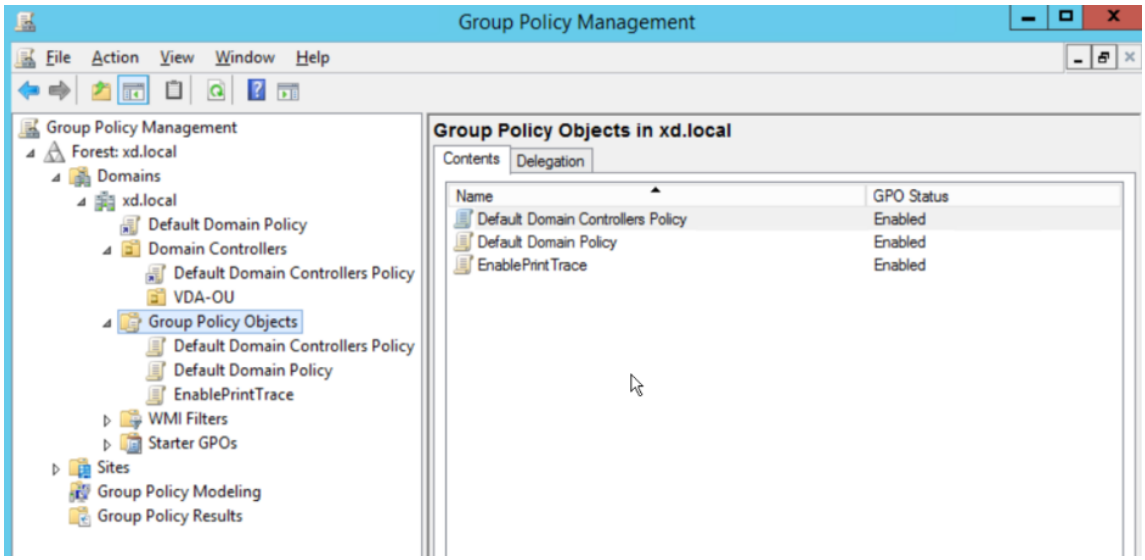
9. 右键单击 **ShowJobTitleInEventLogs**，然后选择修改。将值数据输入为 1，然后单击“确定”。



使用 **GPO** 在多个 **VDA** 中创建注册表项　此方法仅适用于持久性 VDA，并且需要在创建注册表项后重新启动 VDA。持久 VDA 是指在重新启动后保持其状态的计算机。用户的数据在重启后不会丢失。

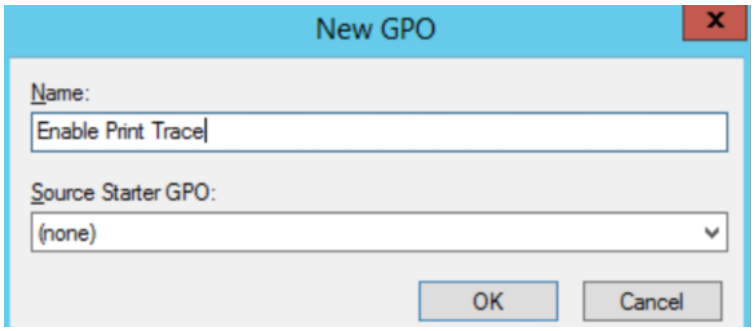
使用注册表项创建注册表 **GPO**

1. 打开“组策略管理”，然后右键单击组策略对象。

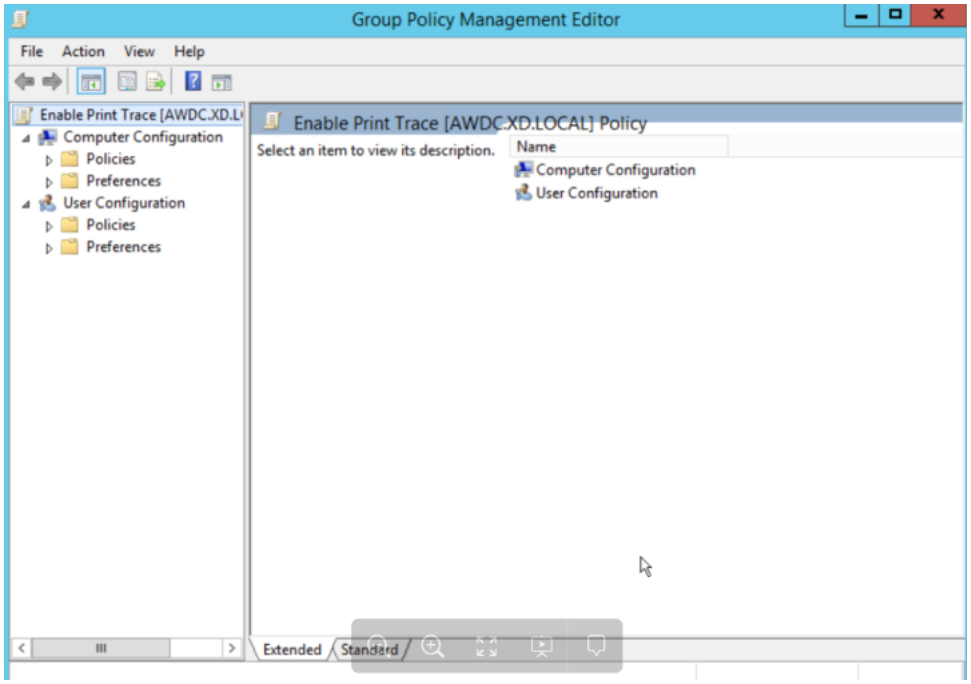


2. 在“新建 **GPO**”窗口中，在以下字段中输入值：

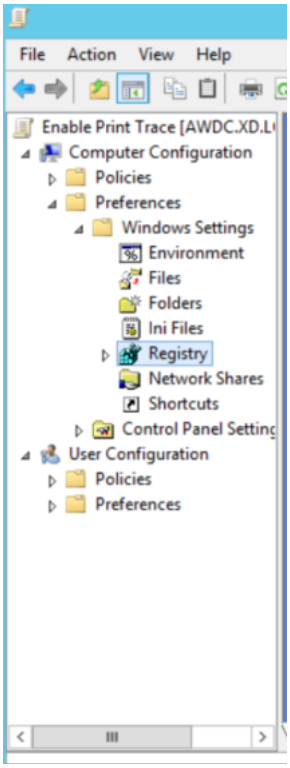
   - 名称：启用打印跟踪
   - 源启动器 GPO：（无）



3. 选择确定。
4. 右键单击已创建的启用打印跟踪对象，然后选择编辑。

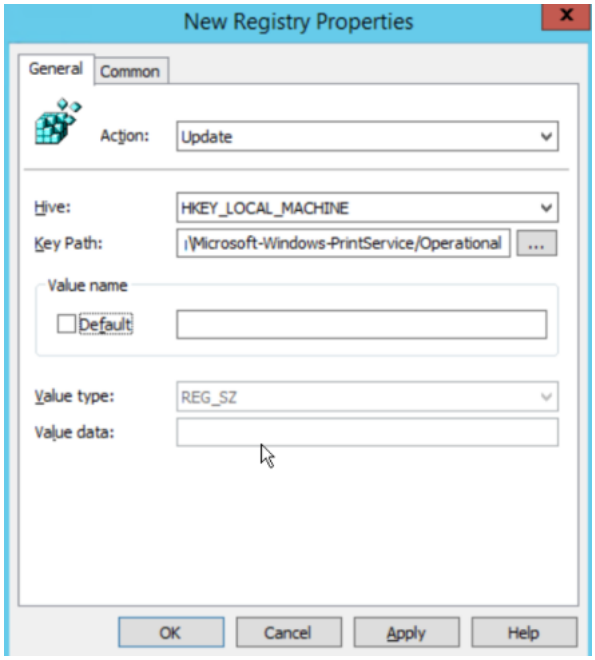


5. 在计算机配置列表中，选择首选项 **> Windows** 设置。



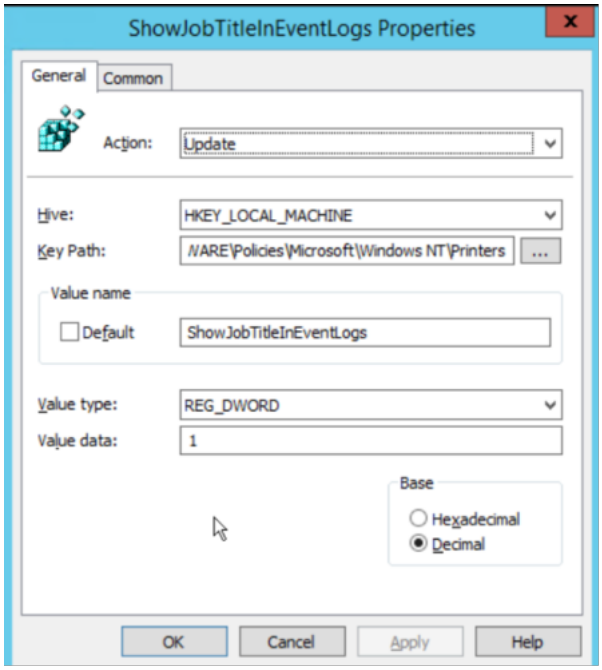
6. 右键单击 注册表，选择 新建 **>** 注册表项。输入以下属性以启用打印日志：

   - 操作：更新
   - 注册表配置单元：HKEY_LOCAL_MACHINE
   - 关键路径:SYSTEM\CurrentControlSet\Services\EventLog\Microsoft-Windows-PrintService/Operational



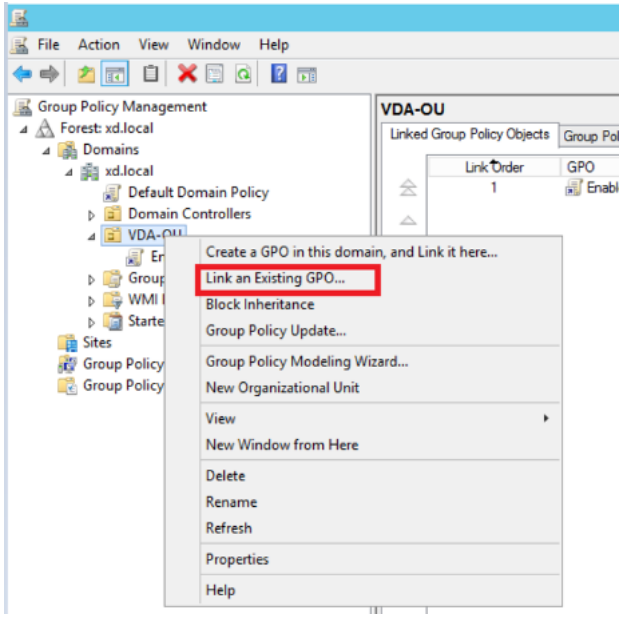
7. 选择应用，然后选择确定。
8. 再次右键单击注册表，选择新建 **>** 注册表项。输入以下属性以启用打印作业名称：

   - 操作：更新
   - 注册表配置单元：HKEY_LOCAL_MACHINE
   - 密钥路径：SOFTWARE\Policies\Microsoft\Windows NT\Printers
   - 值名称：ShowJobTitleInEventLogs
   - 值类型：REG_DWORD
   - 值数据：1
   - 基数：十进制

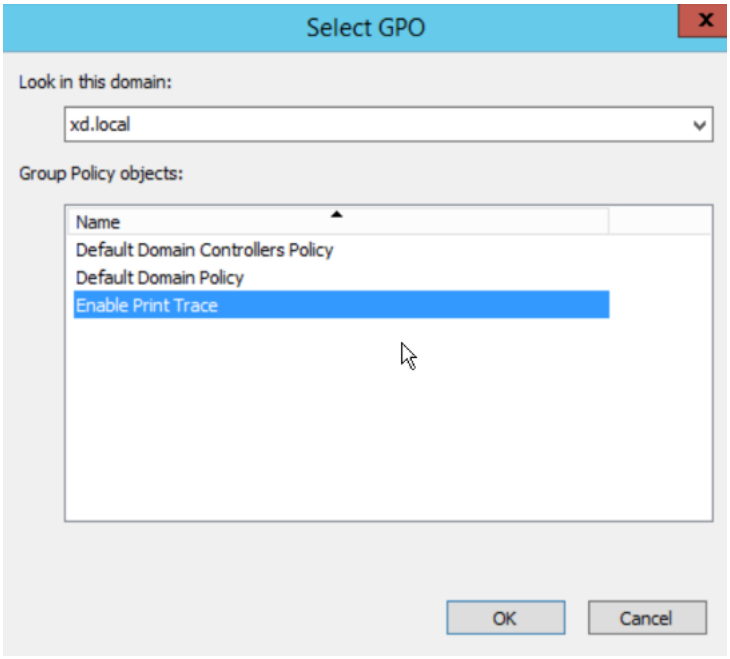


为组织单位启用打印跟踪

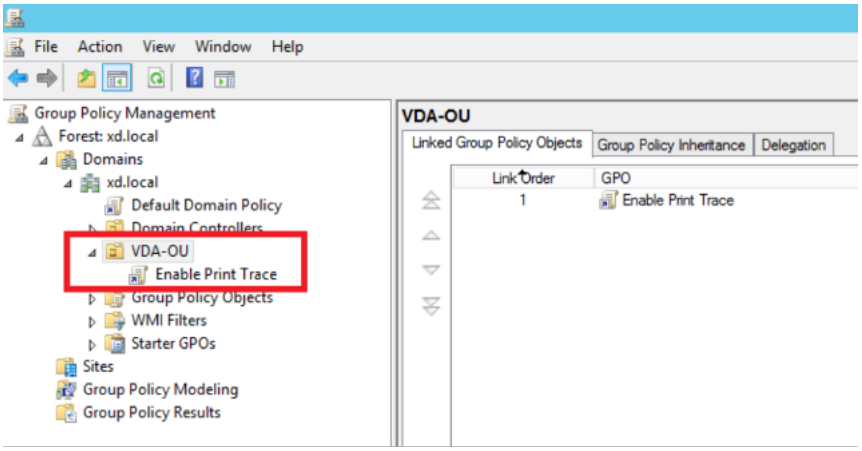
1. 打开 组策略管理 并选择域（例如- xd.local）或组织单元（如果是 VDA 的一部分）（例如 VDA-OU）。
2. 右键单击域 (xd.local) 或 OU (VDA-OU)，然后选择 链接现有 **GPO**。



3. 在选择 **GPO** 对话框中，选择“启用打印跟踪”并选择确定。



4. 验证启用打印跟踪 **GPO** 是否已链接到 OU。



> 注意
>
> - 重新启动 VDA 时，队列中的所有事件都将丢失，并且在 Citrix Analytics 中将不可用。
> - 此重新启动对单个会话 VDA 的影响较小，因为在给定时间只能有一个会话处于活动状态，因此事件数量会减少。
> - 此重新启动对多会话 VDA 的影响很大，因为所有活动会话将在重新启动期间终止，队列中的事件将丢失。

为 **Citrix DaaS** 启用剪贴板遥测

Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）允许用户执行剪贴板操作，相关日志可以在 Citrix Analytics for Security 中查看。这些剪贴板日志提供有价值的信息，例如 VDA 名称、剪贴板大小、剪贴板格式类型、客户端 IP、剪贴板操作、剪贴板操作方向以及是否允许剪贴板操作。

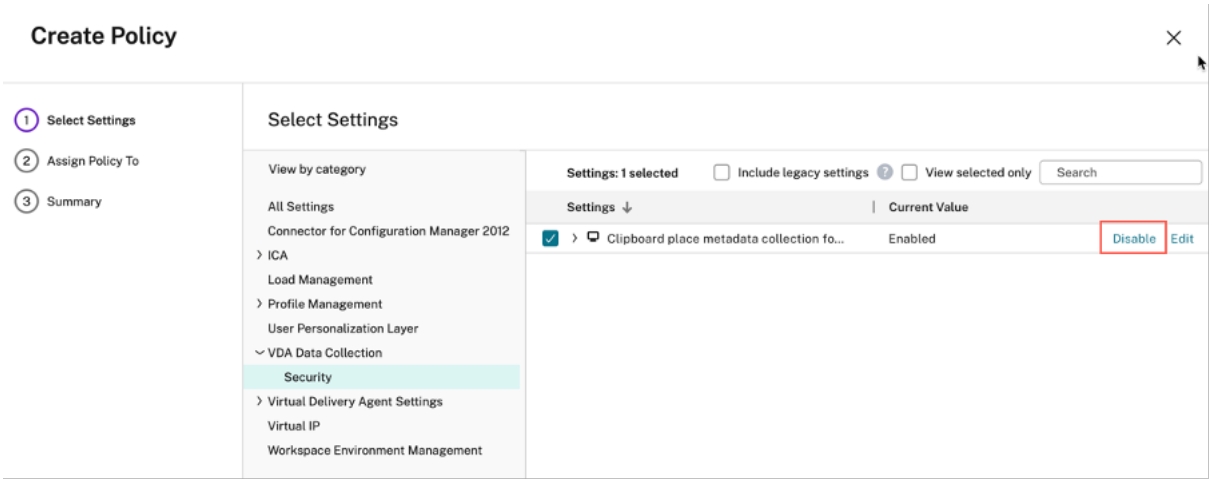
作为安全管理员，您可以通过在 Citrix Analytics for Security 的“搜索”页面上选择应用程序和桌面数据源，使用这些日志进行风险分析和调查。

> 注意
>
> - 默认情况下，在 Virtual Delivery Agent (VDA) 上启用这些剪贴板日志的收集和传输。
> - 此配置仅适用于 Windows VDA。

必备条件

- 您的 VDA 版本必须与 Citrix Virtual Apps and Desktops 7 2305 或更高版本的基准版本相同。有关更多信息，请参阅 Citrix Virtual Apps and Desktops 7 2305。
- 确保 **Web Studio** 策略页面上的客户端剪贴板重定向设置未配置为禁止状态。有关更多信息，请参阅 客户端剪贴板重定向。

您可以使用 安全监视策略的剪贴板放置元数据集合 来启用或禁用剪贴板遥测。默认情况下，此策略处于启用状态。要禁用，必须转到“策略”页面 > 在“**VDA** 数据收集”下选择“安全”> 查看策略 > 单击“禁用”。



有关更多信息，请参见 剪贴板放置元数据集合以进行安全监视。

打开或关闭数据源上的数据处理

您可以随时停止特定数据源（Director 和 Workspace 应用程序）的数据处理。在数据源站点卡片上，单击垂直省略号 **(⋮) >** 关闭数据处理。Citrix Analytics 将停止处理该数据源的数据。也可以从“应用程序和桌面”站点卡停止数据处理。此选项适用于数据源 Director 和 Workspace 应用程序。

要再次启用数据处理，请单击“打开数据处理”。

Microsoft Active Directory 和 Azure Active Directory 集成

October 13, 2022

连接 Active Directory 或 Azure Active Directory，然后将用户详细信息和用户组从组织的域导入到 Citrix Analytics for Security。

此集成通过职位、组织、办公地点、电子邮件和联系方式等用户身份详细信息增强了 Citrix Analytics for Security 中的用户配置文件。在 用户个人资料 页面上，您可以查看这些用户详细信息，这些详细信息在风险调查和分析过程中对

必备条件

- 如果要将 Active Directory 与 Citrix Analytics for Security 连接起来，请确保首先将 Active Directory 连接到您的 Citrix Cloud 帐户有关更多信息，请参阅 将 Active Directory 连接到 Citrix Cloud。
- 如果要将 Azure Active Directory 与 Citrix Analytics for Security 连接起来，请确保首先将 Azure Active Directory 连接到 Citrix Cloud 帐户。有关详细信息，请参阅将 Azure Active Directory 连接到 Citrix Cloud。

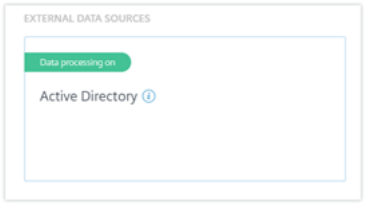
连接 Microsoft Active Directory

要将 Active Directory 连接到 Citrix Analytics for Security，请执行以下操作：

1. 转到“设置”>“数据源”>“安全性”，然后导航到“外部数据源”部分。
2. 在 **Active Directory** 站点卡上，单击加号 **+** 。

3. Citrix Analytics 会提示您将 Active Directory 连接到您的 Citrix Cloud 帐户。有关更多信息，请参阅 先决条件。

将 Active Directory 关联到 Citrix Cloud 帐户后，Citrix Analytics 会自动发现此新数据源。在“数 据源”页面上，Active Directory 站点卡显示 数据处理已启用。

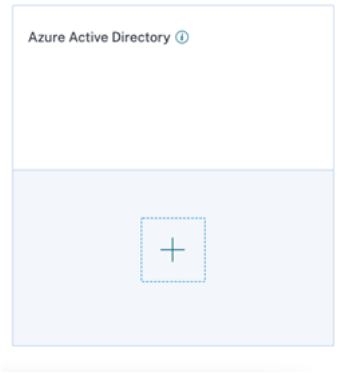


数据处理开 启状态表示已发现 Active Directory，并且正在从 Active Directory 获取用户信息。

连接 **Microsoft Azure Active Directory**

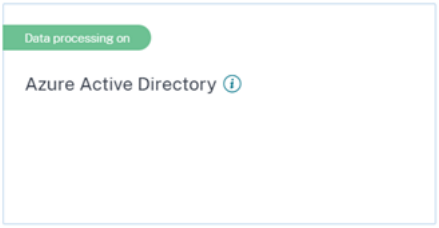
要将 Azure Active Directory 连接到 Citrix Analytics，请执行以下操作：

1. 转到“设置” > “数据源” > “安全性”，然后导航到“外部数据源”部分。
2. 在 **Azure Active Directory** 站点卡片上，单击加号 +。



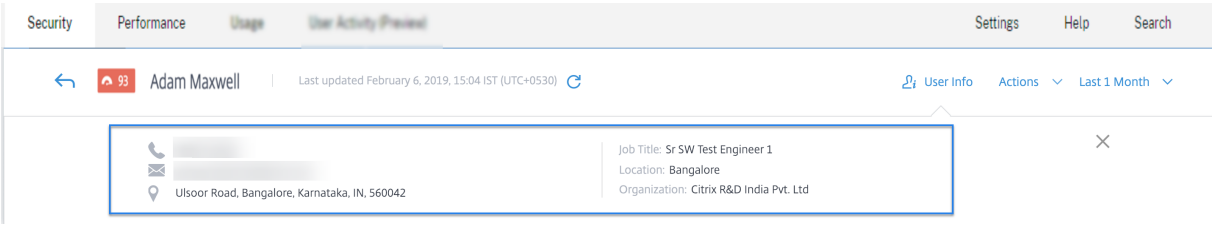
3. Citrix Analytics 会提示你将 Azure Active Directory 连接到您的 Citrix Cloud 帐户。有关详细信息，请参阅将 Azure Active Directory 连接到 Citrix Cloud。

将 Azure Active Directory 连接到 Citrix Cloud 帐户后，Citrix Analytics 会自动发现此新数据源。在“数据源”页面上，**Azure Active Directory** 站点卡片显示 数据处理已打开。此状态表示已发现 Azure Active Directory，并且正在从 Azure Active Directory 获取用户信息。



查看用户信息

在“安全”选项卡中，单击有风险的用户以查看用户配置文件页面。如果用户在 Active Directory 或 Azure Active Directory 中可用，则可以在用户配置文件页面上查看其职务、组织、电子邮件和联系电话。



Microsoft Graph 安全性集成

June 23, 2021

Microsoft Graph 安全 是聚合来自多个安全提供商的数据的外部数据源。它还提供对用户清单数据的访问。

Citrix Analytics 目前支持来自 Microsoft Graph 安全的以下安全提供商：

- Azure AD 身份保护
- Microsoft Defender for Endpoint

有关安全提供商的更多信息，请参阅以下链接：

- 对于 **Azure AD** 身份保护：https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events
- 对于 端点的微软后卫：https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection

要加入 Microsoft Graph Security 数据源，你需要代表租户从 Microsoft 身份平台获取所需的权限。

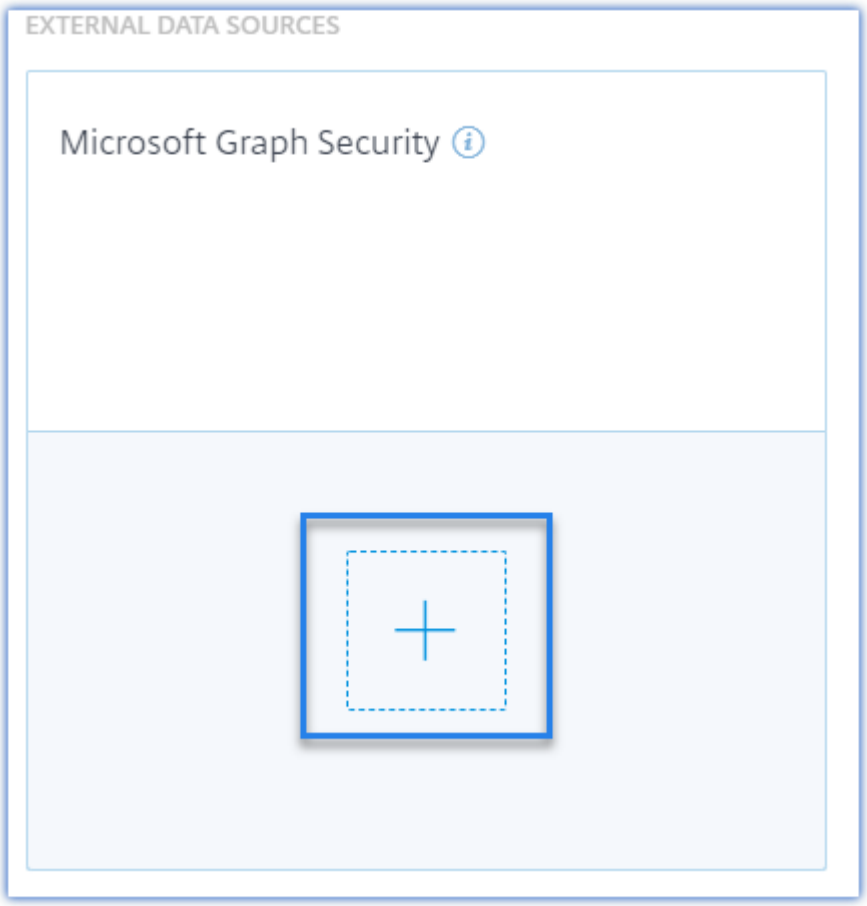
必备条件

在开始加入 Microsoft Graph 安全数据源之前，请确保：

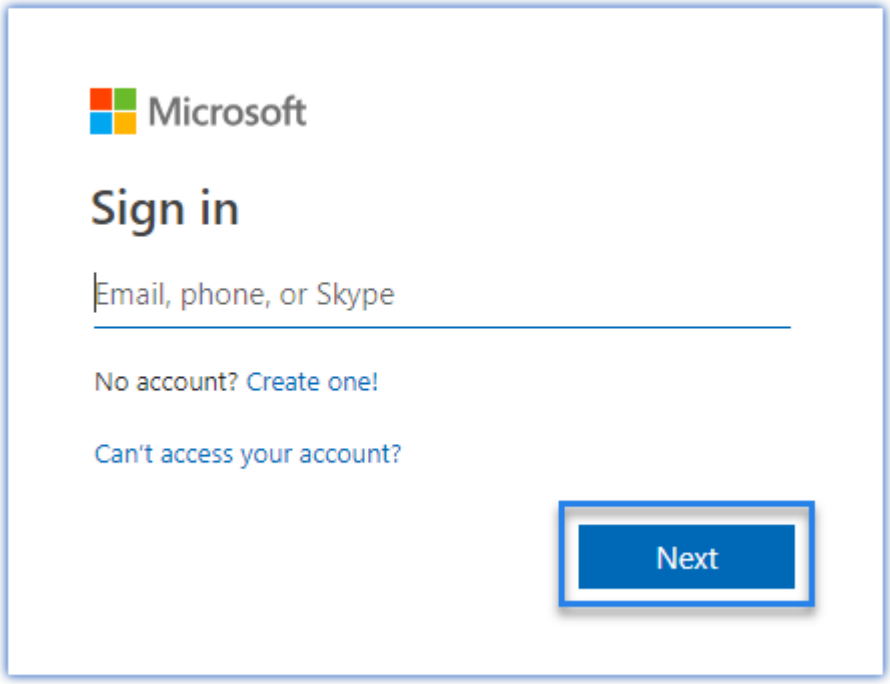
- 管理员正在使用 Azure AD 身份保护（Azure AD 高级 P2 的一部分）安全提供程序。
- 最终用户使用工作或学校帐户登录到 Microsoft Store。

加入 **Microsoft Graph** 形安全实例

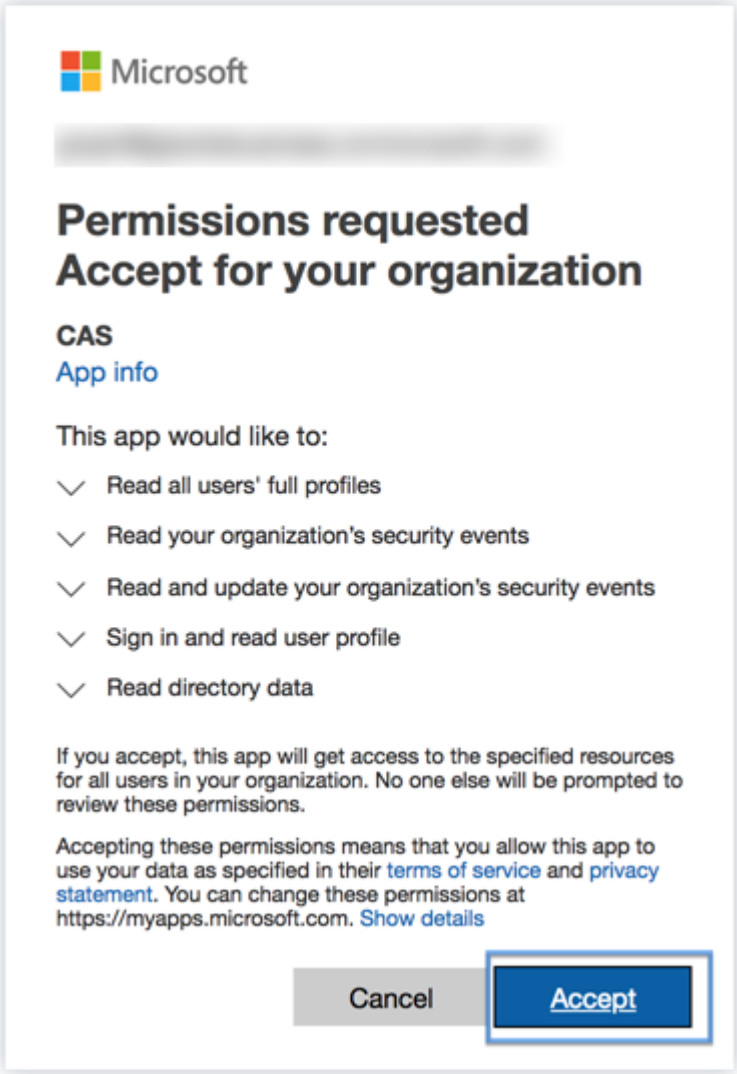
1. 转到“设置”>“数据源”>“安全性”，然后导航到“外部数据源”部分。
2. 单击 Microsoft Graph 安全网站卡片上的加号 (**+**)。您将被重定向到授权端点。



3. 在 微软 窗口中，使用 Azure 登录凭据登录以注册帐户。或者，选择现有帐户。
4. 单击下一步。



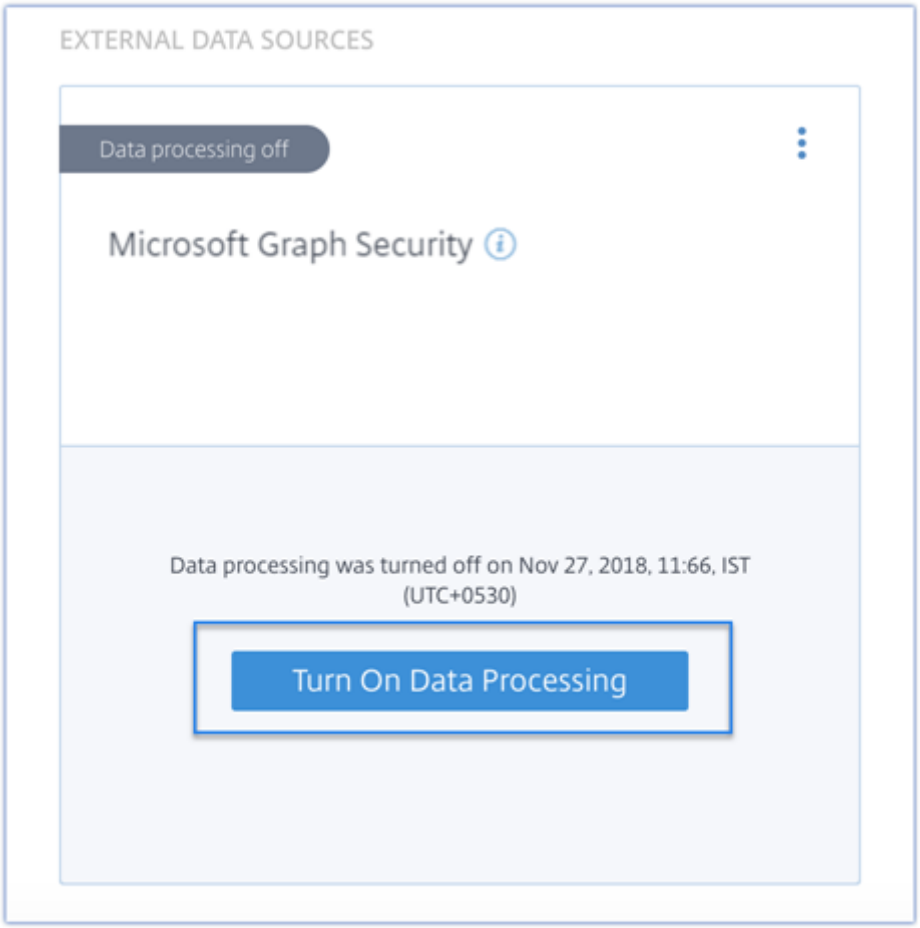
5. 单击 **Accept**（接受）。您将被重定向到“数据源”页面。Microsoft Graph 安全性数据源现已链接到您的 Citrix Cloud 帐户。



打开或关闭数据处理

要禁用数据处理，请单击站点卡上的垂直省略号 ()，然后选择 关闭数据处理。它阻止 Citrix Analytics 处理此数据源的数据。

您可以通过选择站点卡上的“打开数据处理”再次启用数据处理。



有关 Microsoft Graph 安全性风险指示器的信息，请参阅Microsoft Graph 安全性风险指示器。

安全信息和事件管理 **(SIEM)** 集成

December 7, 2023

> 注意
>
> 联系 CAS-PM-Ext@cloud.com 以请求有关 SIEM 集成、将数据导出到 SIEM 的帮助并提供反馈。

将 Citrix Analytics for Security 与 SIEM 服务集成，并将用户的数据从 Citrix IT 环境导出到 SIEM。将导出的数据与 SIEM 中的可用数据相关联，以更深入地了解组织的安全状况。

这种集成增强了 Citrix Analytics for Security 和 SIEM 的价值。

优势

- 使您的安全运营团队能够关联、分析和搜索来自不同日志的数据。

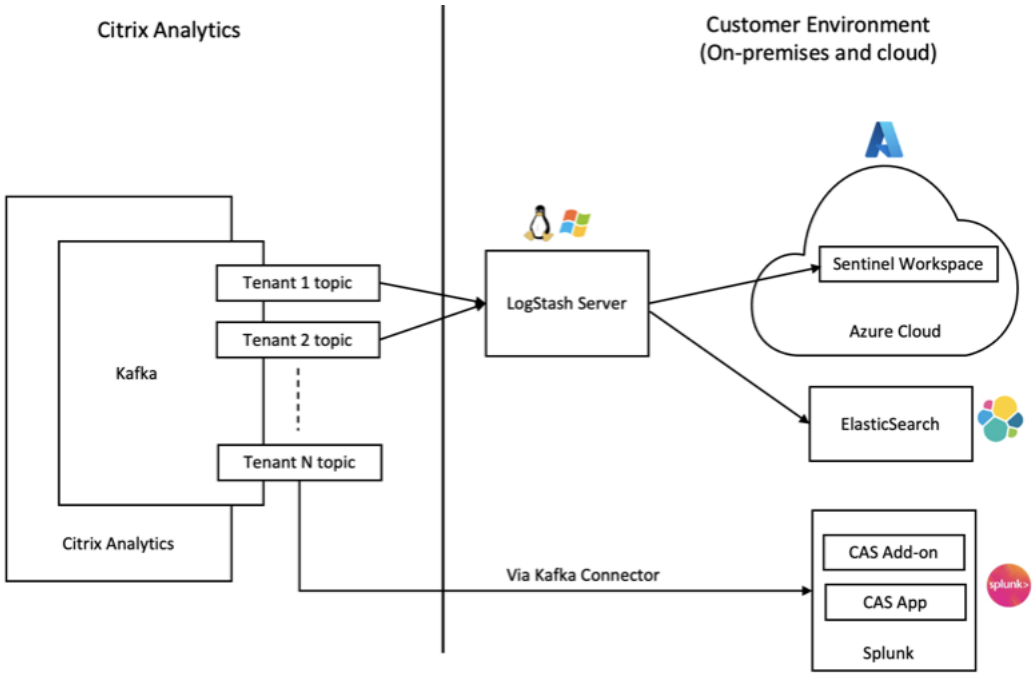
- 帮助您的安全运营团队识别并快速补救安全风险。
- 在集中的位置查看安全警报。
- 为组织风险分析功能（例如风险指示器、用户配置文件和风险评分）检测潜在安全威胁的集中式方法。
- 能够将用户帐户的 Citrix Analytics 风险情报信息与 SIEM 中连接的外部数据源进行组合和关联。

SIEM 集成架构

您的 SIEM 集成与部署在 Citrix Analytics for Security 云上的北向 Kafka 相连。这可以通过以下两种方式实现：

- **Kafka** 端点：如果您的 SIEM 支持 Kafka 端点，请使用 Logstash 配置文件中提供的参数以及 JKS 文件或 PEM 文件中的证书详细信息将您的 SIEM 与 Citrix Analytics for Security 集成。使用 Kafka 端点，您可以将数据连接并拉取到所选的 SIEM。
- **Logstash** 引擎：如果您的 SIEM 不支持 Kafka 端点，则可以使用 Logstash 数据收集引擎。您可以将来自 Citrix Analytics for Security 的风险洞察数据发送到 Logstash 支持的 输出插件 之一。

请参阅以下 SIEM 解决方案架构图，了解数据如何从 Citrix Analytics for Security 流向您的 SIEM 服务：

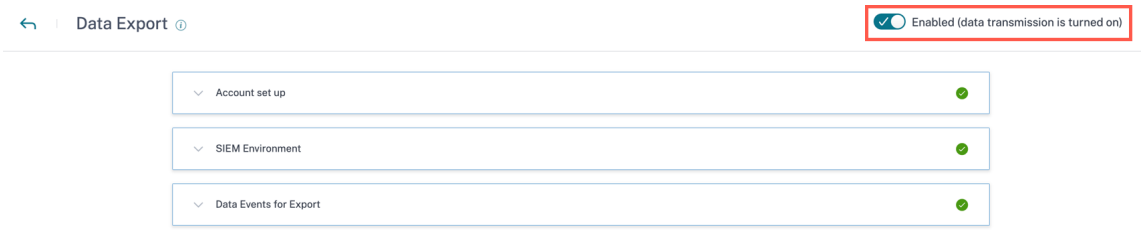


打开或关闭数据传输

要停止从 Citrix Analytics for Security 传输数据，请执行以下操作：

1. 前往“设置”**>**“数据导出”。
2. 关闭切换按钮以禁用数据传输。

> 注意
>
> 默认情况下，SIEM 的数据传输始终处于开启/启用状态。



要再次启用数据传输，请打开切换按钮。

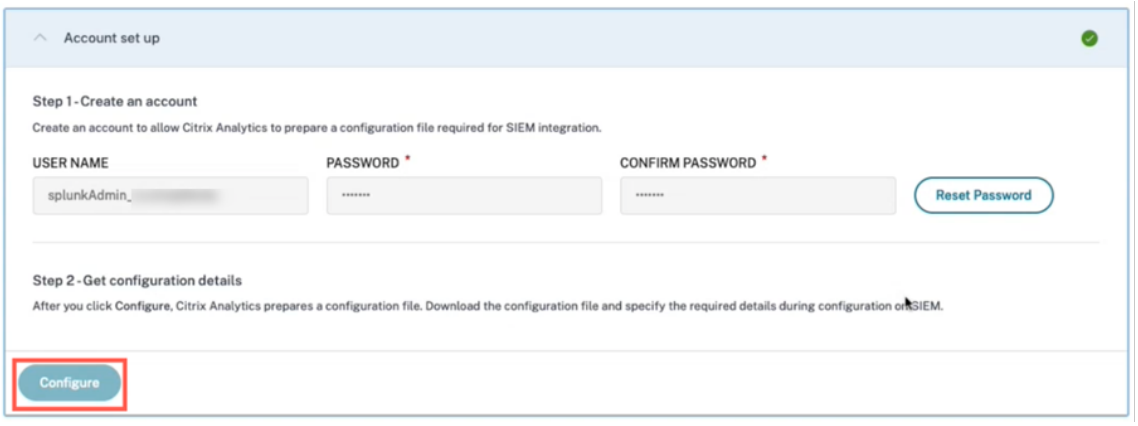
设置 **SIEM** 环境

要将数据导出到 SIEM，必须执行以下操作：

- 设置您的 Kafka 帐户和身份验证凭据
- 下载预先填充的配置并设置 SIEM 环境
- 要导出的数据事件

SIEM 导出帐户设置

1. 要设置您的帐户，请导航到 设置 **>** 数据导出 **>** 展开帐户设置。通过指定用户名和密码来创建帐户。一旦您设置了帐户，您的 Kafka 详细信息就会生成。这些详细信息会在生成配置文件时自动嵌入。

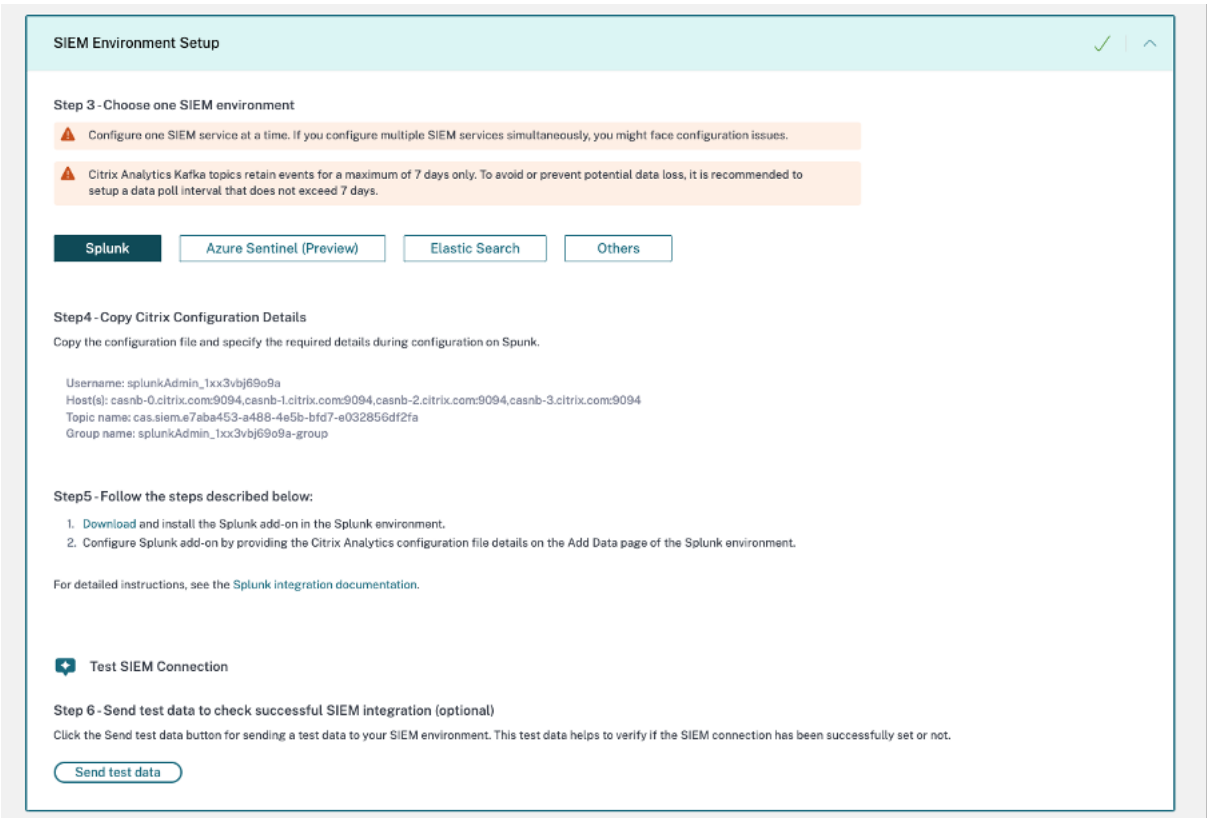


2. 单击“配置”生成配置文件。配置文件包含详细信息，例如 Kafka 终端节点、您的特定订阅主题和群组 ID。此外，它还预先配置了完成身份验证和数据流所需的 Kafka 和 SSL 属性。

SIEM 配置和环境设置

根据需要选择 SIEM 环境。您可以将 Citrix Analytics for Security 与以下服务集成。请参阅以下链接以获取详细信息和 SIEM 特定配置：

- Splunk
- Microsoft Sentinel
- Elasticsearch
- 其他使用基于 Kafka 或 Logstash 的数据连接器的 SIEM



数据事件从 Citrix Analytics for Security 导出到您的 SIEM 服务

作为 SIEM 导出的一部分，有两种类型的数据集：

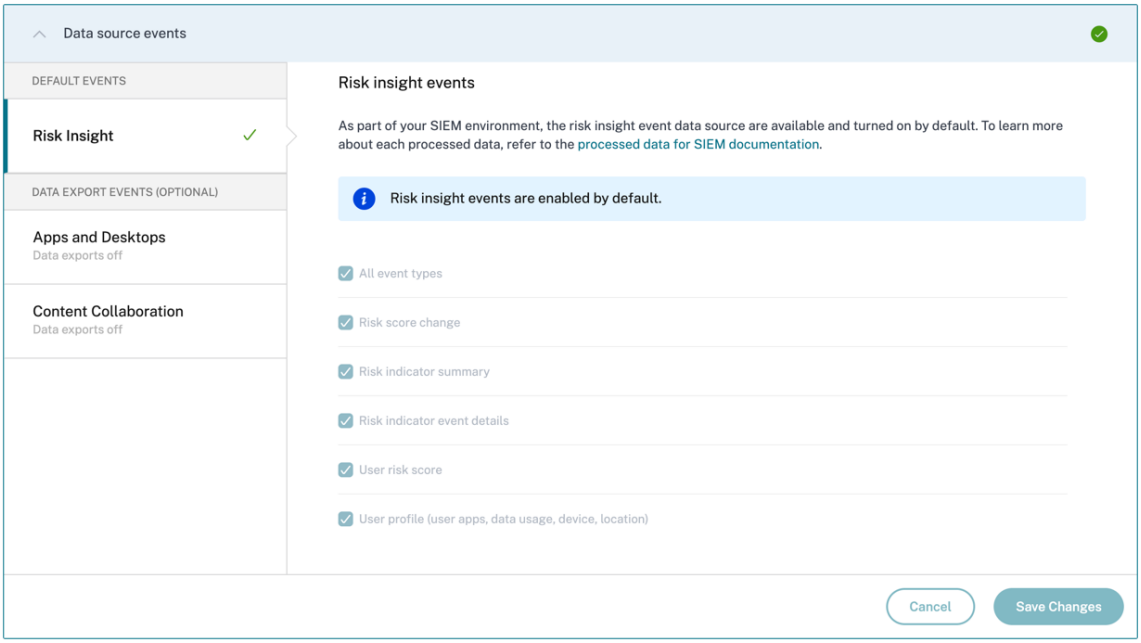
1. 风险洞察事件（默认导出）—完成帐户配置和 SIEM 设置后，默认数据（风险洞察事件）开始流向您的 SIEM 部署。风险洞察数据包含用户风险评分、用户资料和风险指标警报。它们由 Citrix Analytics 计算机学习算法、用户行为分析生成，并基于用户事件。有关可用事件类型、元数据和架构的信息，请参阅 SIEM 的风险洞察数据。
2. 数据源事件（可选导出） -此外，您可以配置数据导出功能以从启用了 Citrix Analytics for Security 的产品数据源中导出用户事件。在 Citrix 环境中执行任何活动时，都会生成数据源事件。导出的事件是自助服务视图中提

供的未经处理的实时用户和产品使用数据。这些事件中包含的元数据可以进一步用于更深入的威胁分析、创建新的控制板，以及与安全和 IT 基础架构中的其他非 Citrix 数据源事件相关联。

目前，Citrix Analytics for Security 会向您的 SIEM 发送有关 Citrix 虚拟应用程序和桌面数据源的用户事件。

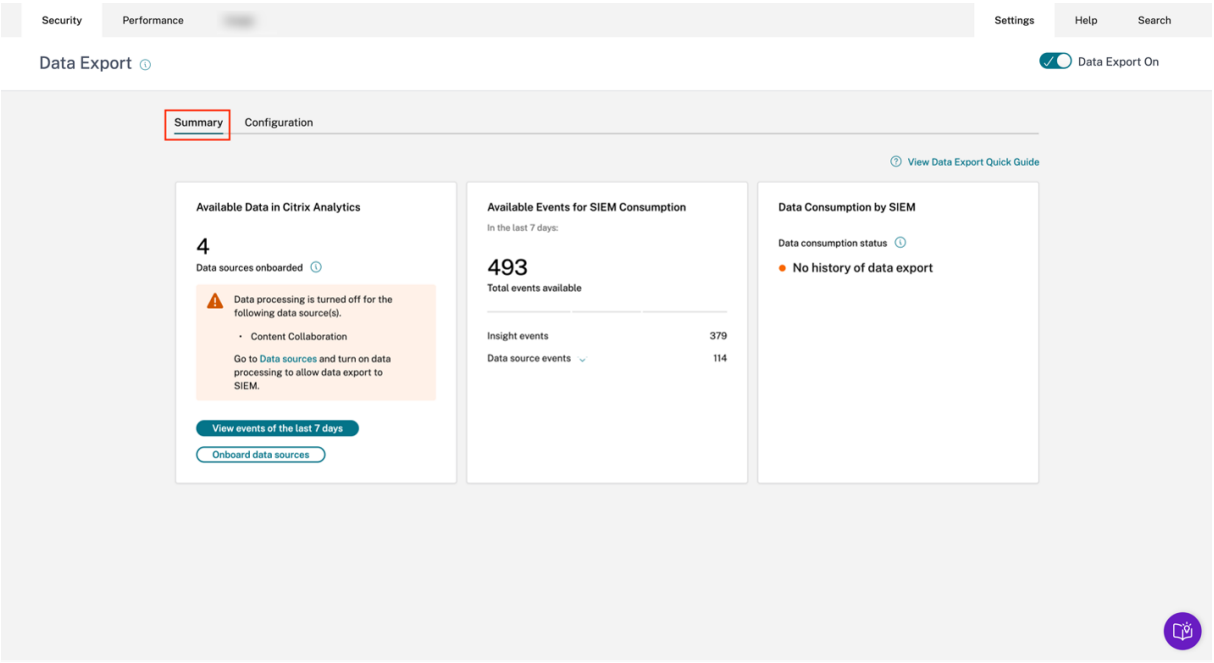
有关可用事件类型、元数据和架构的信息，请参阅 数据源事件。

> 注意
>
> 使用 Logstash 数据代理的客户，建议从 Citrix Analytics for Securit y 门户下载最新的配置文件，并在 Logstash 服务部署时进行更新。这样可以确保创建正确的数据源事件表，并且这些事件现在在 SIEM 索引中可用。



排除 **SIEM** 集成

安全数据导出视图包含摘要选项卡，可帮助管理员解决其 SIEM 与 Citrix Analytics 的集成问题。摘要控制板通过有助于故障排除过程的检查点，让您可以查看数据的运行状况和流向。



要了解有关此功能的更多信息，请参阅 数据导出疑难解答。

Splunk 集成

November 26, 2023

将 Citrix Analytics for Security 与 Splunk 集成，将用户数据从您的 Citrix IT 环境导出并关联到 Splunk，从而更深入地了解组织的安全状况。

有关集成的好处以及发送到 SIEM 的已处理数据类型的更多信息，请参阅 安全信息和事件管理集成。

要全面了解 Splunk 部署方法并采用有效规划的策略，请参阅 Splunk 中托管的 Splunk 体系结构和 Citrix Analytics 应用程序文档。

将 **Citrix Analytics for Security** 与 **Splunk** 集成

遵循上述准则，将 Citrix Analytics for Security 与 Splunk 集成：

- 数据导出。Citrix Analytics for Security 创建 Kafka 频道并导出风险洞察和数据源事件。Splunk 从渠道检索此风险智能。
- 在 Citrix Analytics 上获取配置。为您的预定义帐户创建密码以进行身份验证。Citrix Analytics for Security 准备您配置适用于 Splunk 的 Citrix Analytics 加载项所需的配置文件。
- 下载并安装适用于 Splunk 的 Citrix Analytics 加载项。使用 Splunkbase 或 Splunk Cloud 下载适用于 **Splunk** 的 **Citrix Analytics** 加载项以完成安装过程。

- 配置适用于 Splunk 的 Citrix Analytics 加载项。使用 Citrix Analytics for Security 提供的配置详细信息来设置数据输入，并配置适用于 Splunk 的 Citrix Analytics 加载项。

准备好 Citrix Analytics 配置文件后，请参阅：

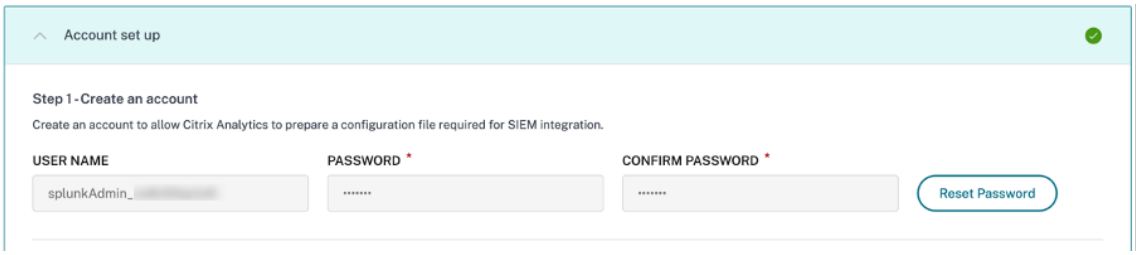
- 重置密码功能
- 打开或关闭数据传输

配置适用于 Splunk 的 Citrix Analytics 加载项后，请参阅：

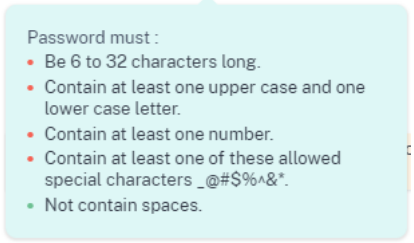
- 如何在 Splunk 环境中使用事件
- 如何为 Splunk 配置 Citrix Analytics 应用程序

数据导出

1. 前往“设置”**>**“数据导出”。
2. 在“帐户设置”部分，通过指定用户名和密码来创建帐户。此帐户用于准备集成所需的配置文件。

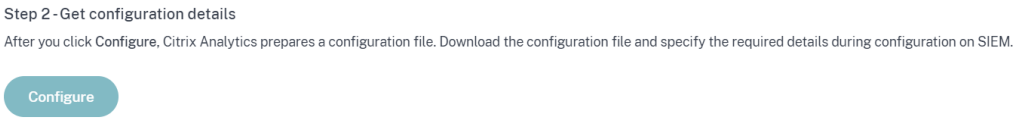


3. 确保密码满足以下条件：



4. 选择 配置。

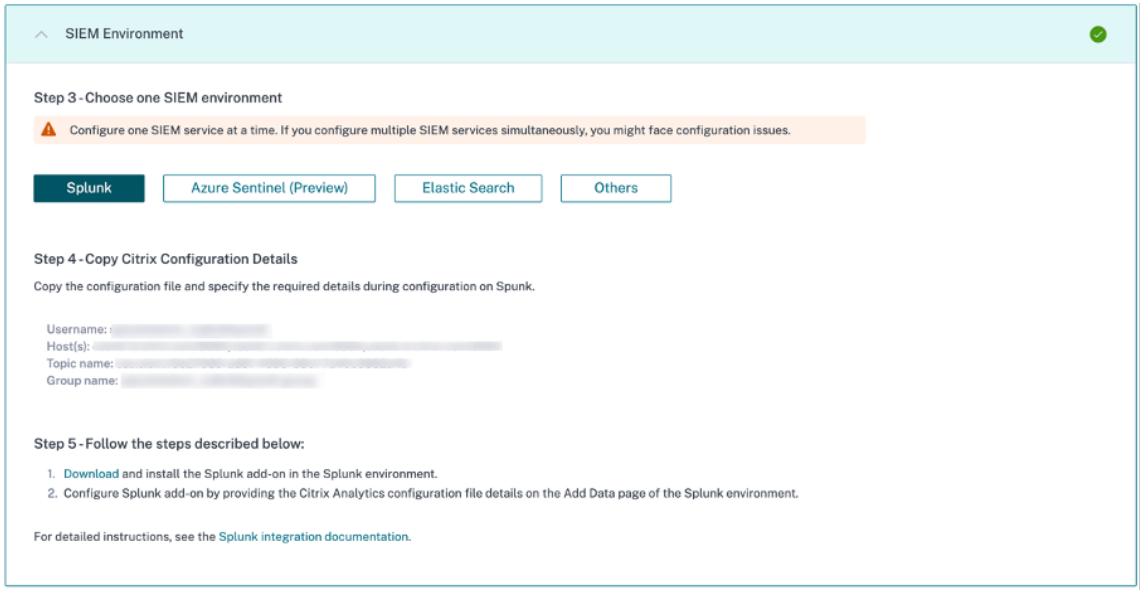
   Citrix Analytics for Security 准备了 Splunk 集成所需的配置详细信息。



5. 选择 **Splunk**。
6. 复制配置详细信息，包括用户名、主机、Kafka 主题名称和组名。

   在后续步骤中，您需要这些详细信息才能配置适用于 Splunk 的 Citrix Analytics 加载项。

> 重要
>
> 这些详细信息是敏感的，您必须将它们存储在安全的位置。

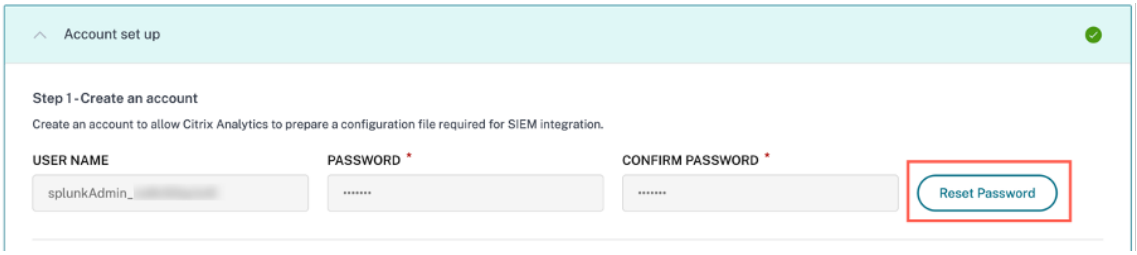


要为 Splunk Integration 生成候选数据，请为至少一个数据源开启数据处理或使用 测试事件生成功能。它有助于 Citrix Analytics for Security 启动 Splunk 集成流程。

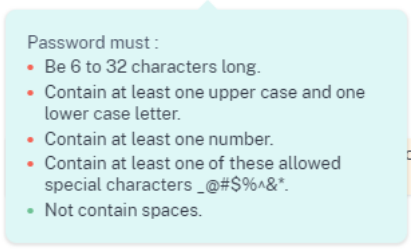
重置密码功能

如果要在 Citrix Analytics for Security 上重置配置密码，请执行以下步骤：

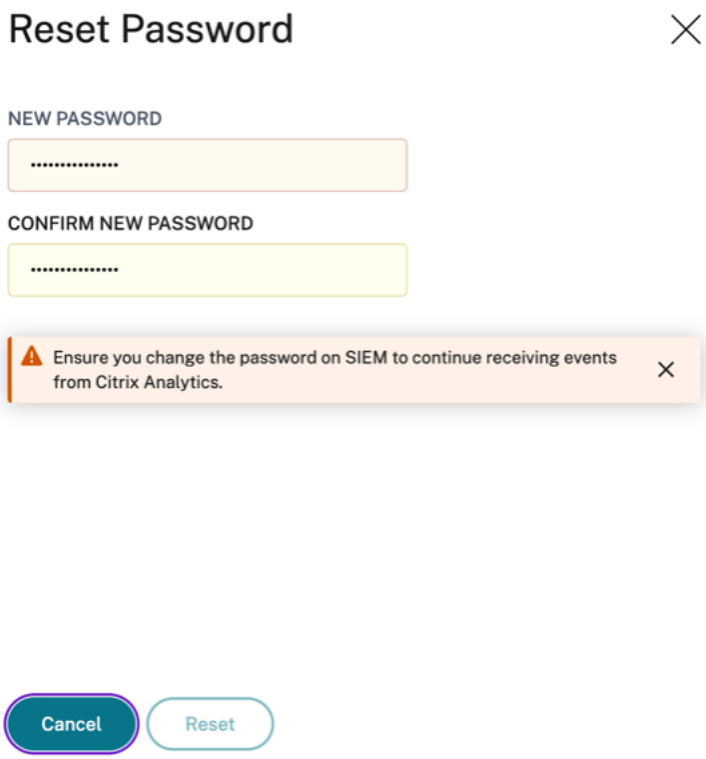
1. 在“帐户设置”页面上，单击“重置密码”。



2. 在重置密码窗口中，在新密码和确认新密码字段中指定更新后的密码。遵循显示的密码规则。



3. 单击重置。配置文件准备工作已启动。



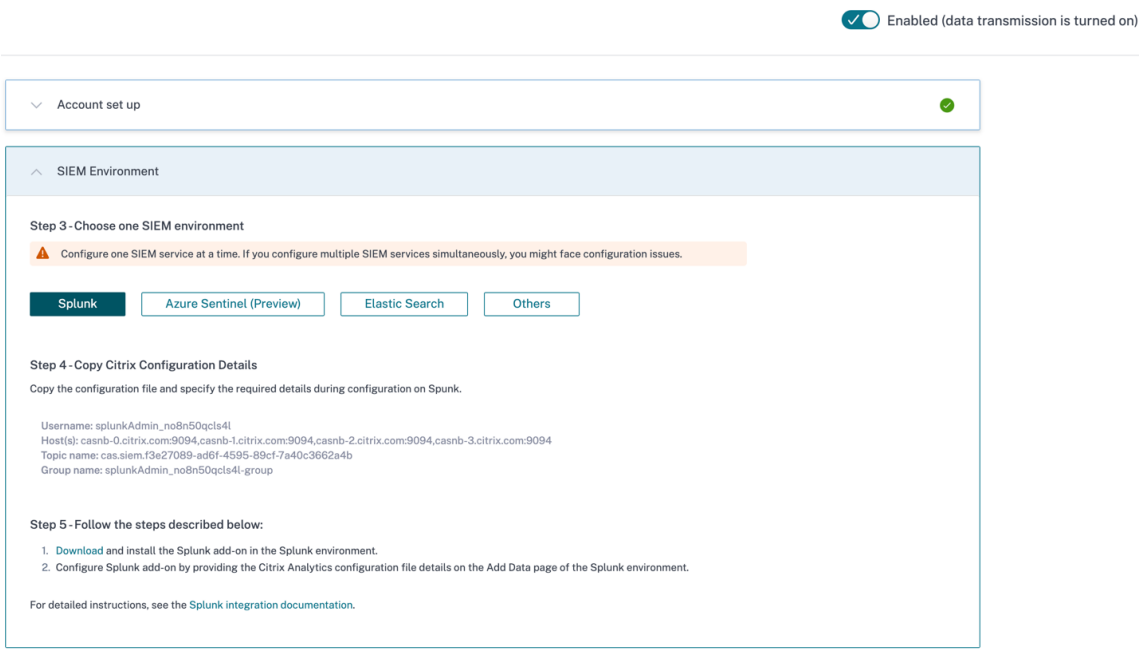
> 注意
>
> 重置配置密码后，请确保在 Splunk 环境的添加数据页面上设置数据输入时更新新密码。它有助于 Citrix Analytics for Security 继续向 Splunk 传输数据。

打开或关闭数据传输

默认情况下，从 Citrix Analytics 导出的 Splunk 数据传输处于启用状态。

要停止从 Citrix Analytics for Security 传输数据，请执行以下操作：

1. 前往“设置”**>**“数据导出”。
2. 关闭切换按钮以禁用数据传输。



要再次启用数据传输，请打开切换按钮。

适用于 **Splunk** 的 **Citrix Analytics** 加载项

您可以选择在以下任一平台上安装附加应用程序：

- Splunk Enterprise (Heavy Forwarder)
- Splunk Cloud

适用于 **Splunk** 的 **Citrix Analytics** 插件（本地/企业版）

支持的版本

Citrix Analytics for Security 支持在以下操作系统上集成 Splunk：

- CentOS Linux 7 及更高版本
- Debian GNU/Linux 10.0 及更高版本
- 红帽企业 Linux 服务器 7.0 及更高版本
- Ubuntu 18.04 LTS 及更高版本

> 注意
>
> - Citrix 建议使用先前操作系统的最新版本或仍在相应供应商支持的版本。
> - 对于 Linux 内核（64 位）操作系统，请使用 Splunk

> 支持的内核版本。有关更多信息，请参阅 Splunk 文档。

您可以在以下 Splunk 版本上配置我们的 Splunk 集成：Splunk 8.1 (64 位）及更高版本。

必备条件

- 适用于 **Splunk** 的 **Citrix Analytics** 加载项连接到 Citrix Analytics for Security 上的以下端点。确保终端节点位于网络中的允许列表中。

端点	美国地区	欧盟区域	亚太南部地区
Kafka 代理	casnb-0.citrix.com:9094 casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-0.citrix.com:9094 casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-0.citrix.com:9094 casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

> 注意：
>
> 尝试使用端点名称而不是 IP 地址。终端节点的公有 IP 地址可能会更改。

下载并安装适用于 **Splunk** 的 **Citrix Analytics** 加载项

您可以选择使用 从文件安装应用程序或从 Splunk 环境中安装插件。

从文件安装应用

1. 转到 Splunkbase。
2. 下载适用于 Splunk 的 Citrix Analytics 加载项文件。
3. 在 Splunk Web 主页上，单击 应用程序旁边的齿轮图标。
4. 单击 从文件安装应用程序。
5. 找到下载的文件，然后单击 上传。

> 备注
>
> - 如果您有旧版本的加载项，请选择 升级应用程序 以覆盖它。
> - 如果要从 2.0.0 之前的版本升级适用于 **Splunk** 的 **Citrix Analytics** 加载项，则必须删除附加组件安装文件夹的 */bin* 文件夹中的以下文件和文件夹，然后重新启动 Splunk 转发器或 Splunk 独立版环境：
>
> ```
> - 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. 验证应用程序是否显示在应用程序列表中。

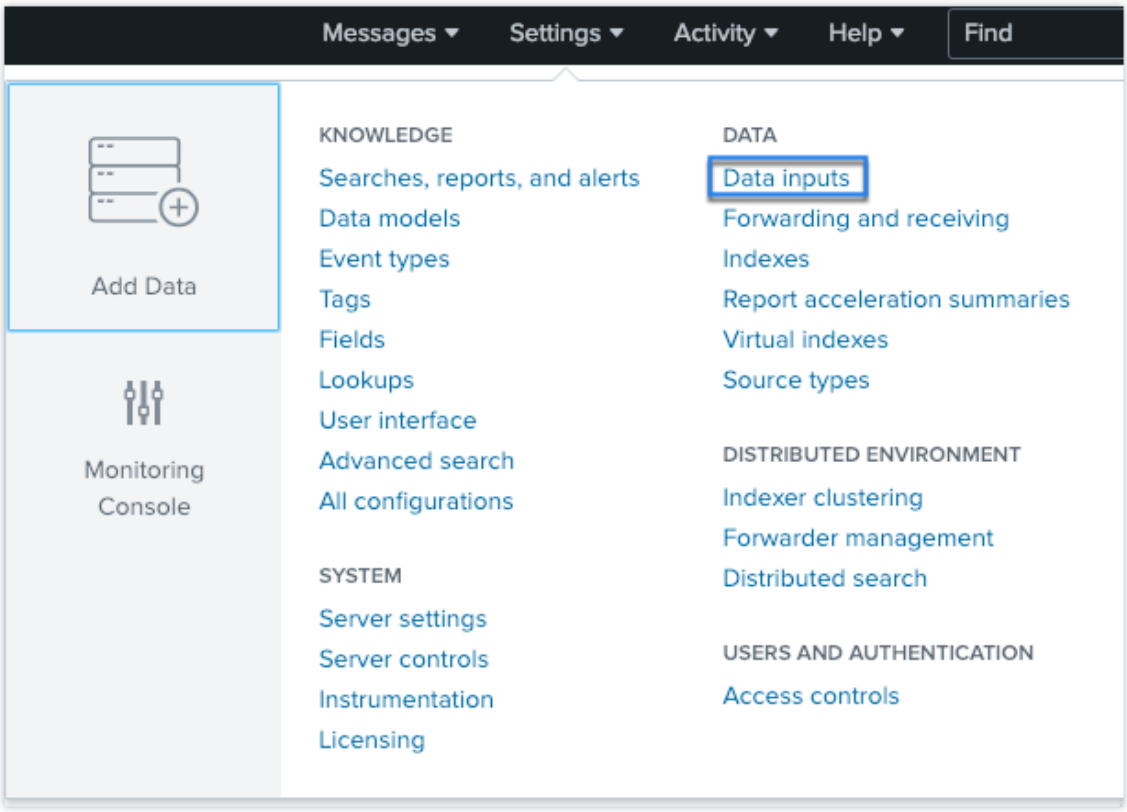
从 **Splunk** 内部安装应用

1. 在 Splunk Web 主页上，单击 **+** 查找更多应用程序。
2. 在浏览更多应用程序页面上，搜索 **Citrix Analytics Add-on for Splunk**（适用于 Splunk 的 Citrix Analytics 加载项）。
3. 单击应用程序旁边的 安装。
4. 验证应用程序是否显示在应用程序列表中。

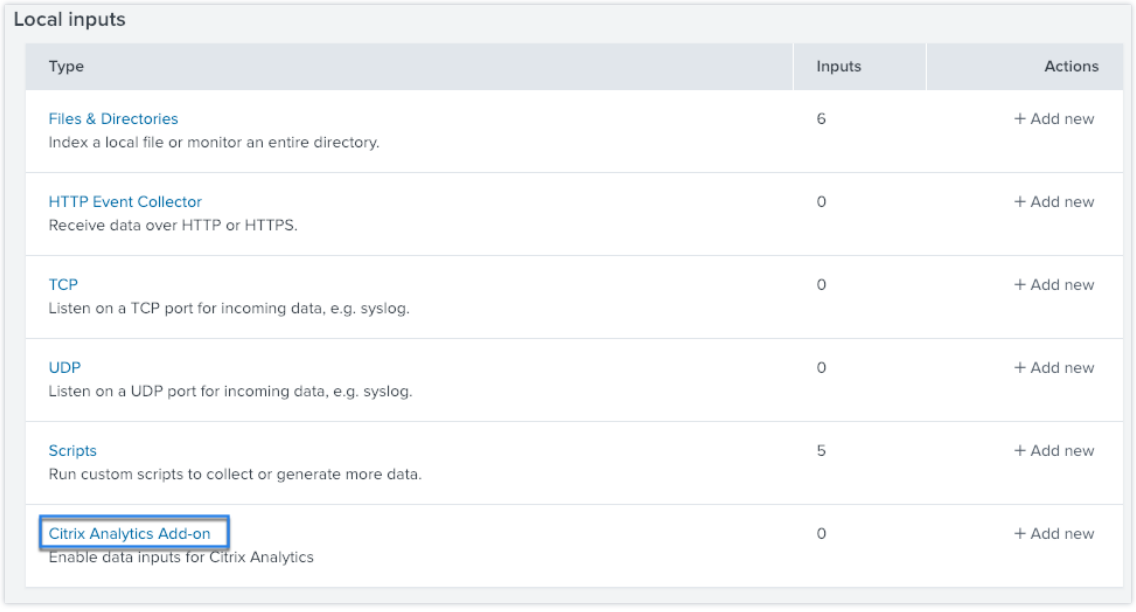
配置适用于 **Splunk** 的 **Citrix Analytics** 加载项

使用 Citrix Analytics for Security 提供的配置详细信息配置适用于 Splunk 的 Citrix Analytics 加载项。成功配置加载项后，Splunk 开始使用 Citrix Analytics for Security 中的事件。

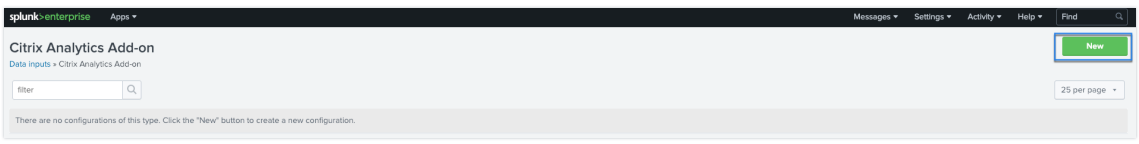
1. 在 Splunk 主页上，转到设置 > 数据输入。



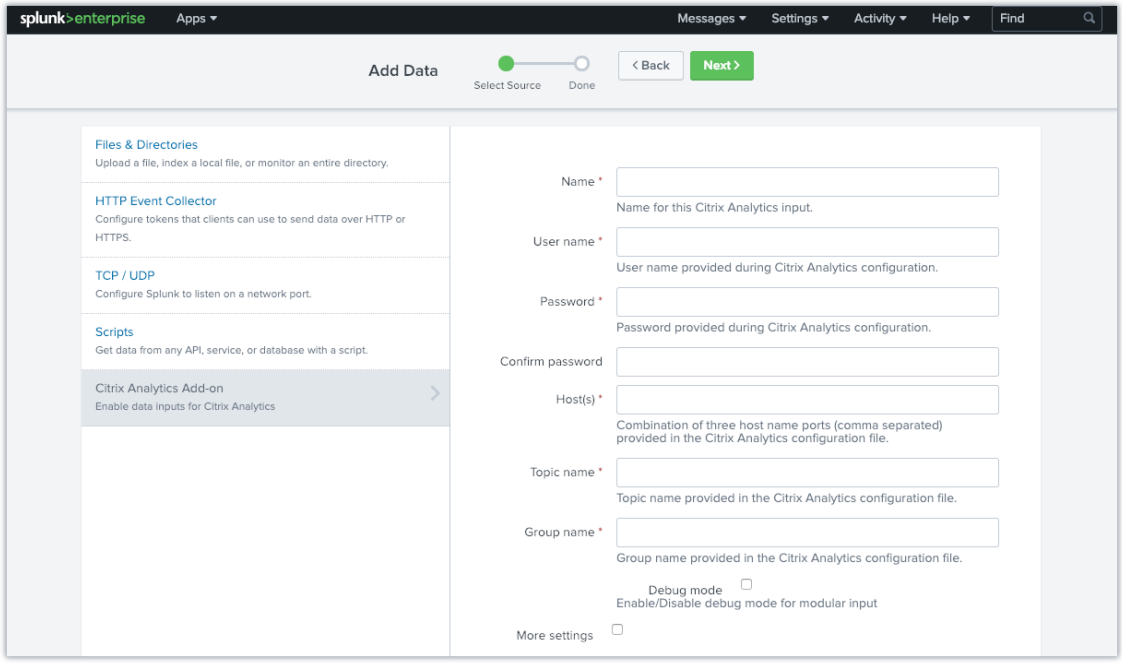
2. 在 本地输入 部分中，单击 **Citrix Analytics** 加载项。



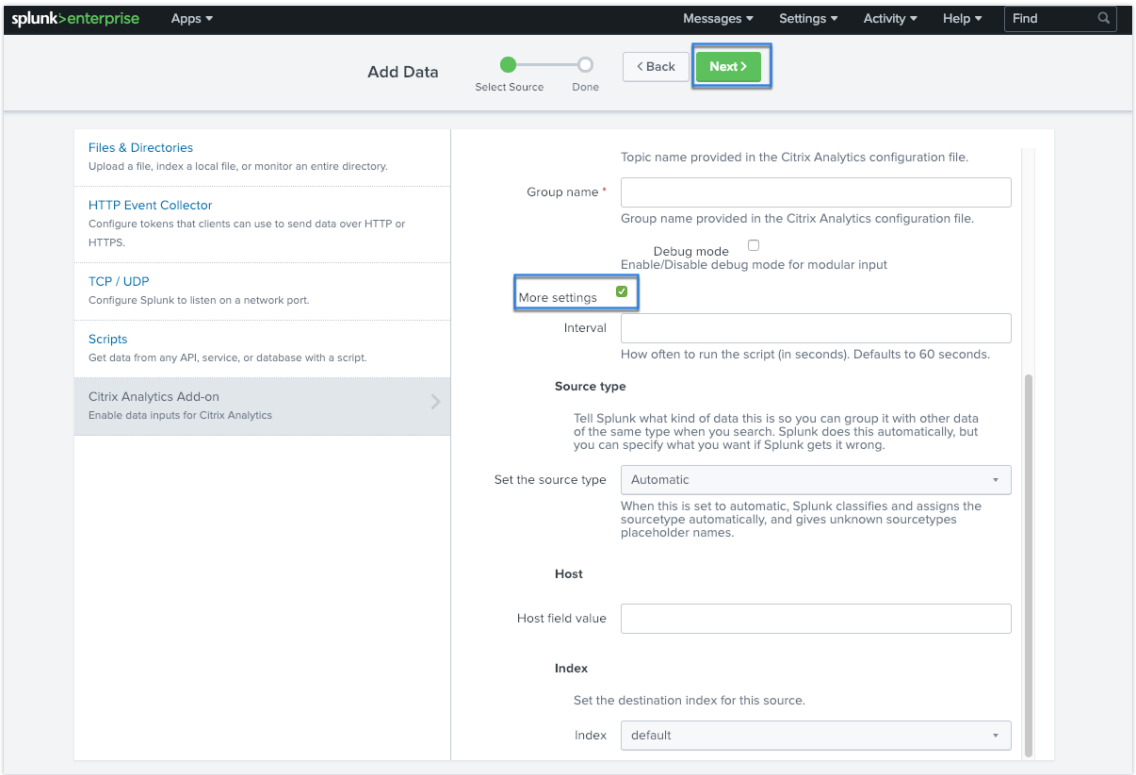
3. 单击新建。



4. 在 添加数据 页面上，输入 Citrix Analytics 配置文件中提供的详细信息。



5. 要自定义默认设置，请单击 更多设置并设置 数据输入。您可以定义自己的 Splunk 索引、主机名和源类型。



6. 单击下一步。您的 Citrix Analytics 数据输入已创建，并且已成功配置适用于 Splunk 的 Citrix Analytics 加载项。

适用于 **Splunk**（云端）的 **Citrix Analytics** 插件

您可以在以下 Splunk 版本上配置我们的 Splunk 集成：Splunk 8.1 及更高版本。

必备条件

适用于 Splunk 的 Citrix Analytics 插件连接到以下 IP 和出站端口，以连接到 Citrix Analytics for Security。确保以下 IP 和出站端口（取决于您的 Citrix Cloud 区域）位于您的网络的允许列表中。要配置这些 IP 和出站端口，请参阅使用 **Admin Configuration Service (ACS)** 将 **Citrix Analytics IP** 和出站端口添加到 **Splunk Cloud** 允许列表部分。

美国地区	IP	出站端口	欧盟区域	IP	出站端口	亚太南部地区	IP	出站端口
casnb-0 cit-rix.com	20.242.21.89	9094	casnb-eu-0 cit-rix.com	20.229.150.91	9094	casnb-aps-0 cit-rix.com	20.211.0.219	9094
casnb-1.citrix.com	20.98.232.69	9094	casnb-eu-1.citrix.com	20.107.97.59	9094	casnb-aps-1 cit-rix.com	20.211.38.102	9094
casnb-2.citrix.com	20.242.21.108	9094	casnb-eu-2.citrix.com	51.124.223.169	9094	casnb-aps-2 cit-rix.com	20.211.36.180	9094
casnb-3.citrix.com	20.242.57.14	9094						

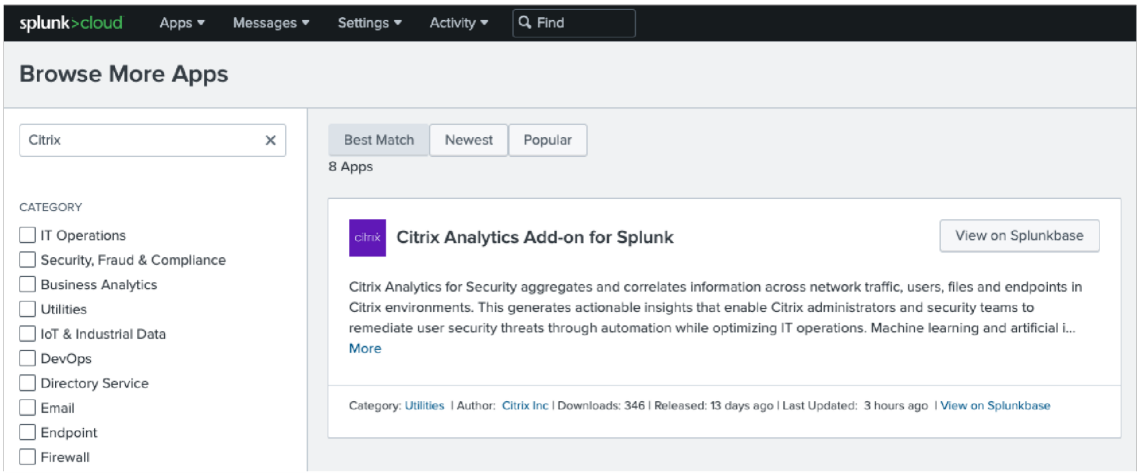
> 注意
>
> 这些 IP 可能会轮换。如上所示，
> 确保使用最新的 IP 更新您的 IP 允许列表。

Admin Configuration Service (ACS) 将 **Citrix Analytics IP** 和出站端口添加到 **Splunk Cloud** 允许列表

1. 根据您的 Citrix Cloud 区域，必须将零个 IP 添加到允许列表中。
2. 在 Splunk 云平台上启用 Admin Configuration Service (ACS)。
3. 使用具有管理员权限的本地帐户为允许列表创建令牌。
4. 运行 cURL GET 和 POST 命令将子网添加到相应端口的允许列表中，并验证它们是否已成功添加。
5. 运行 cURL GET 和 POST 命令 将出站端口添加到允许列表中，并验证它们是否已成功添加。

下载并安装适用于 **Splunk** 的 **Citrix Analytics** 加载项

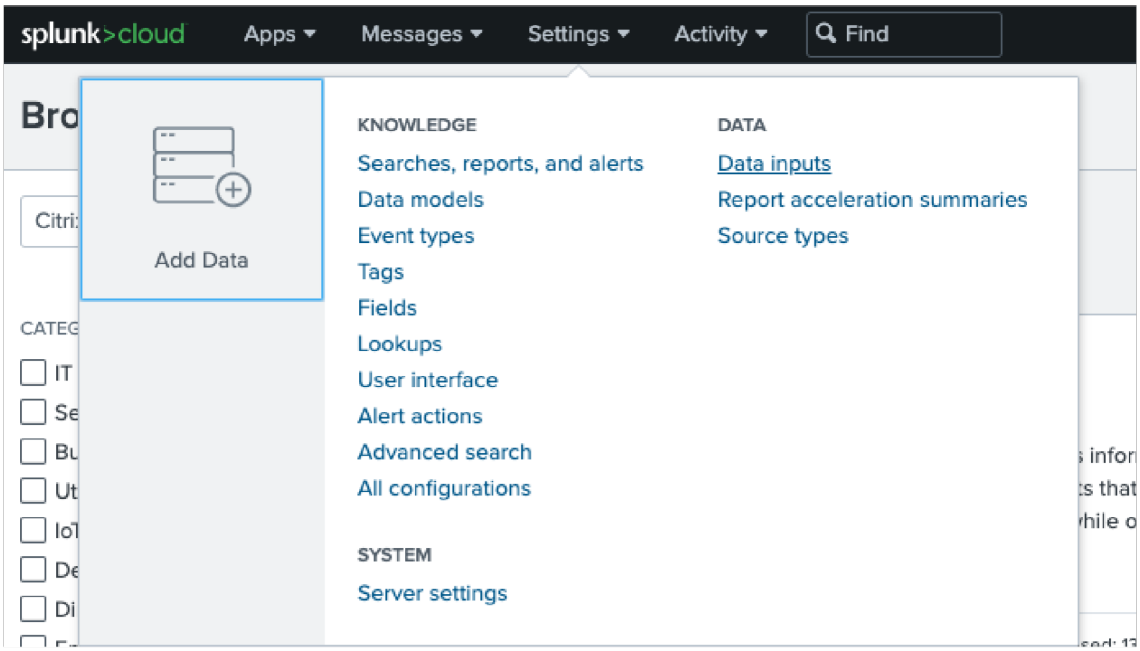
1. 转到应用程序 **>** 查找更多应用程序 **>** 搜索适用于 **Splunk** 的 **Citrix Analytics** 加载项。



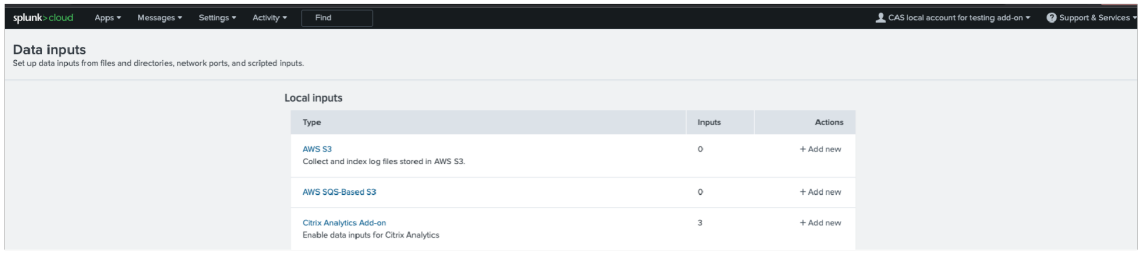
2. 安装应用程序。
3. 验证应用程序是否显示在应用程序列表中。

配置适用于 **Splunk** 的 **Citrix Analytics** 加载项

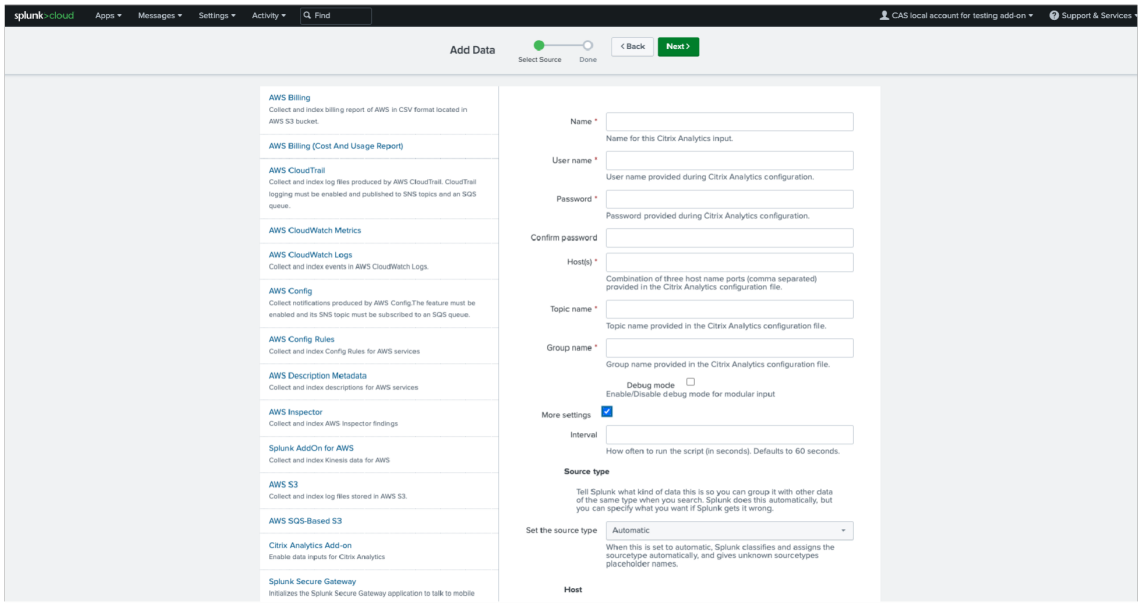
1. 前往“设置”**>**“数据输入”**> Citrix Analytics** 加载项。



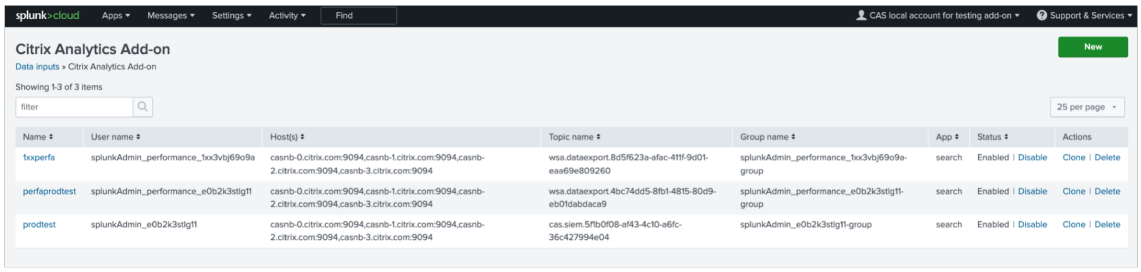
添加输入：Splunk 集成	Citrix Analytics for Security。单击添加新项。

2. 

3. 通过输入 **Citrix Analytics** 数据导出页面上配置的详细信息来配置数据输入。



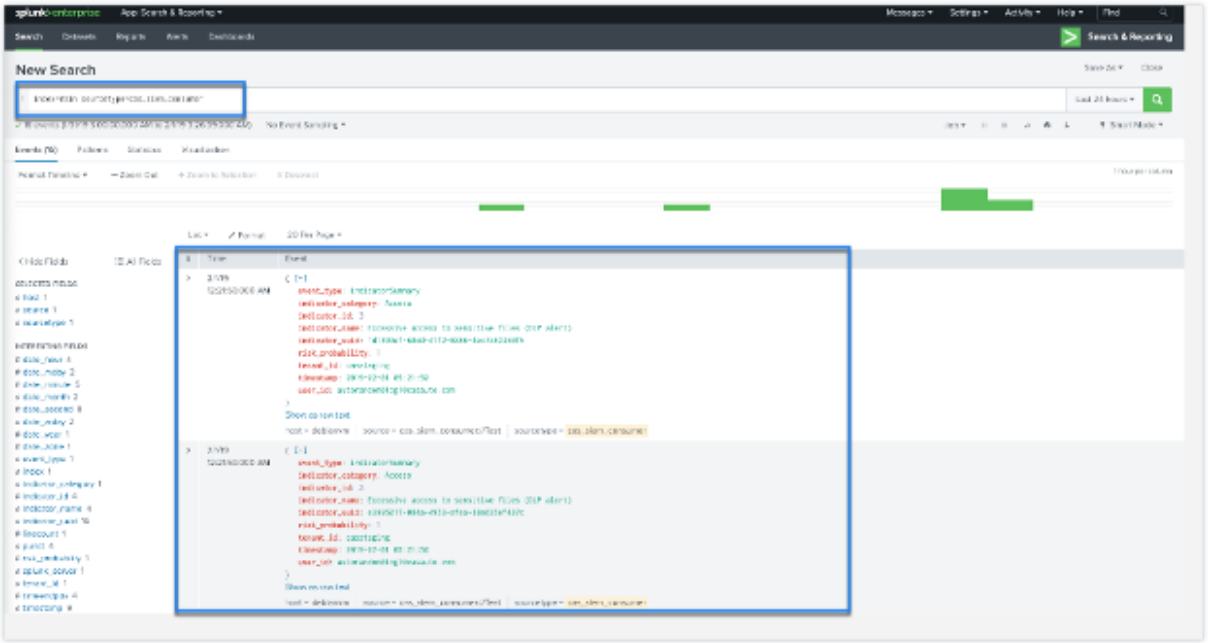
4. 验证您的数据输入是否已成功添加。



如何在 **Splunk** 环境中使用事件

配置附加组件后，Splunk 开始从 Citrix Analytics for Security 检索风险情报。您可以根据配置的数据输入在 Splunk 搜索头上开始搜索组织的事件。

搜索结果按以下格式显示：



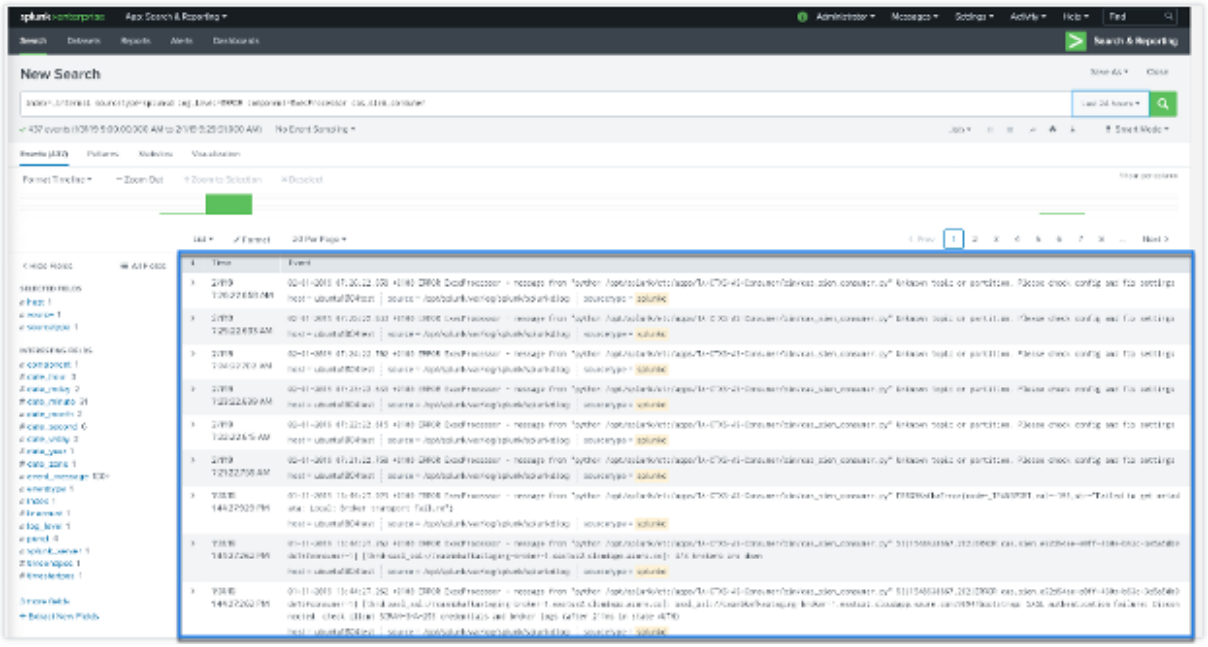
输出示例：

```
{"event_type": "indicatorSummary", "indicator_category": "Access",
"indicator_id": 200, "indicator_name": "Jailbroken / Rooted Device
Detected", "indicator_uuid": "1b97c3be-0000-000-0000-0000000000",
"risk_probability": 1.0, "tenant_id": "notcloud", "timestamp": "2017-11-16
23:59:59", "user_id": "testuser00001"}
```

要搜索和调试插件的问题，请使用以下搜索查询：

```
index=_internal sourcetype=splunkd log_level=ERROR component=ExecProcessor
cas_siem_consumer
```

结果按以下格式显示：



有关数据格式的更多信息，请参阅 适用于 SIEM 的 Citrix Analytics 数据格式。

对适用于 **Splunk** 的 **Citrix Analytics** 加载项进行故障排除

如果您在 Splunk 控制板中看不到任何数据，或者在配置适用于 Splunk 的 Citrix Analytics 加载项时遇到问题，请执行调试步骤来修复问题。有关更多信息，请参阅适用于 Splunk 的 Citrix Analytics 加载项的配置问题。

> 注意
>
> 联系 CAS-PM-Ext@cloud.com 以请求有关 Splunk 集成、将数据导出到 Splunk 的帮助或提供反馈。

适用于 **Splunk** 的 **Citrix Analytics** 应用

> 注意
>
> 此应用程序处于预览中。

适用于 Splunk 的 Citrix Analytics 应用程序使 Splunk Enterprise 管理员能够在 Splunk 上以富有洞察力且可操作的控制板形式查看从 Citrix Analytics for Security 收集的用户数据。使用这些控制板，您可以详细了解组织中用户的风险行为，并及时采取措施来缓解任何内部威胁。您还可以将从 Citrix Analytics for Security 收集的数据与 Splunk 上配置的其他数据源关联起来。这种关联使您可以从多个来源了解用户的风险活动，并采取措施保护您的 IT 环境。

支持的 **Splunk** 版本

适用于 Splunk 的 Citrix Analytics 应用程序在以下 Splunk 版本上运行：

- Splunk 9.0 64 位
- Splunk 8.2 64 位
- Splunk 8.1 64 位

适用于 **Splunk** 的 **Citrix Analytics** 应用的先决条

- 安装适用于 Splunk 的 Citrix Analytics 加载项。
- 确保已满足适用于 Splunk 的 Citrix Analytics 加载项提及的必备条件。
- 确保数据从 Citrix Analytics for Security 传输到 Splunk。

安装和配置

在哪里安装应用程序　Splunk 搜索头

如何安装和配置应用程序　您可以通过从 Spl unkbase 下载适用于 Splunk 的 Citrix Analytics 应用程序或从 Splunk 中安装来安装该应用程序。

从文件安装应用

1. 转到 Splunkbase。
2. 下载适用于 Splunk 的 Citrix Analytics 应用程序文件。
3. 在 Splunk Web 主页上，单击 应用程序旁边的齿轮图标。
4. 单击 从文件安装应用程序。
5. 找到下载的文件，然后单击 上传。

   > 注意
   >
   > 如果您使用的是旧版本的应用程序，请选择 升级应用程序 以覆盖它。

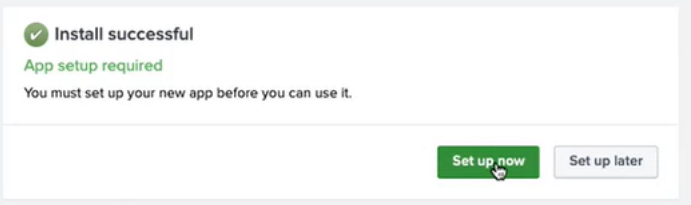
6. 验证应用程序是否显示在应用程序列表中。

从 **Splunk** 内部安装应用

1. 在 Splunk Web 主页上，单击 **+** 查找更多应用程序。
2. 在浏览更多应用程序页面上，搜索适用于 **Splunk** 的 **Citrix Analytics** 应用程序。
3. 单击应用程序旁边的 安装。

配置索引和源类型以关联数据

1. 安装应用程序后，单击 立即设置。

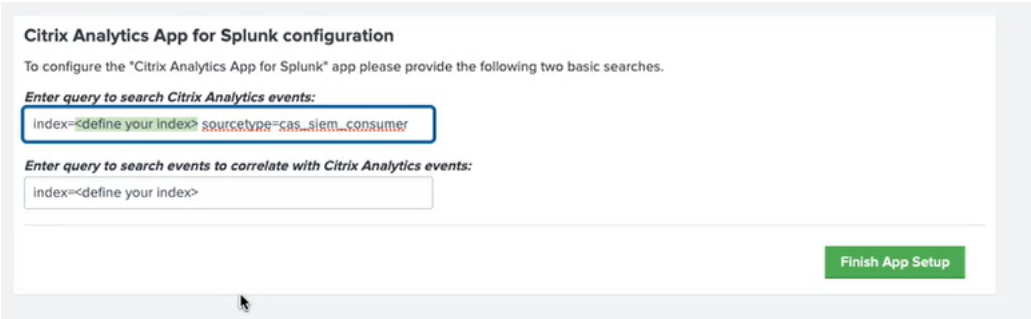


2. 输入以下查询：

   - 存储来自 Citrix Analytics for Security 的数据的索引和源类型。

     > 注意
     >
     > 这些查询值必须与适用于 Splunk 的 Citrix Analytics 加载项中指定的相同。有关更多信息，请参阅配置适用于 Splunk 的 Citrix Analytics 加载项。

   - 要从中将数据与 Citrix Analytics for Security 关联起来的索引。



3. 单击 完成应用程序安装程序 以完成配置。

配置并设置适用于 Splunk 的 Citrix 分析应用程序后，使用 Citrix Analytics 控制板 查看 Splunk 上的用户事件。

有关 Splunk 集成的更多信息，请参阅以下链接：

- Citrix Analytics 与 Splunk 集成
- 适用于 Splunk 的 Citrix Analytics 应用程序现已在 Splunkbase 中

采用 **Citrix Analytics** 附加应用程序的 **Splunk** 架构

February 14, 2023

Splunk 遵循的架构包含以下三个层级：

- 集合

- 索引
- 正在搜索

Splunk 支持多种数据收集机制，可帮助将数据轻松提取到 Splunk 中，这样就可以对其进行索引并可供搜索。这个层不过是您的重型转发器或通用转发器。

您必须在重型转发器层而不是通用转发器层上安装附加应用程序。因为，除了结构良好的数据（例如 json、csv、tsv）很少有例外，通用转发器不会将日志源解析为事件，因此它无法执行任何需要了解日志格式的操作。

它还附带了精简版的 Python，这使得它与任何需要完整的 Splunk 堆栈才能运行的模块化输入应用程序不兼容。重型转发器不过是您的集合层。

通用转发器和重型转发器之间的关键区别在于，重型转发器包含完整的解析管道，无需在磁盘上实际写入和索引事件即可执行与索引器相同的功能。这使重型转发器能够理解单个事件并对其采取操作，例如屏蔽数据、筛选和基于事件数据的路由。由于附加应用程序安装了完整的 Splunk Enterprise，因此它可以托管需要完整的 Python 堆栈才能正确收集数据的模块化输入，也可以充当 Splunk HTTP 事件收集器 (HEC) 的端点。

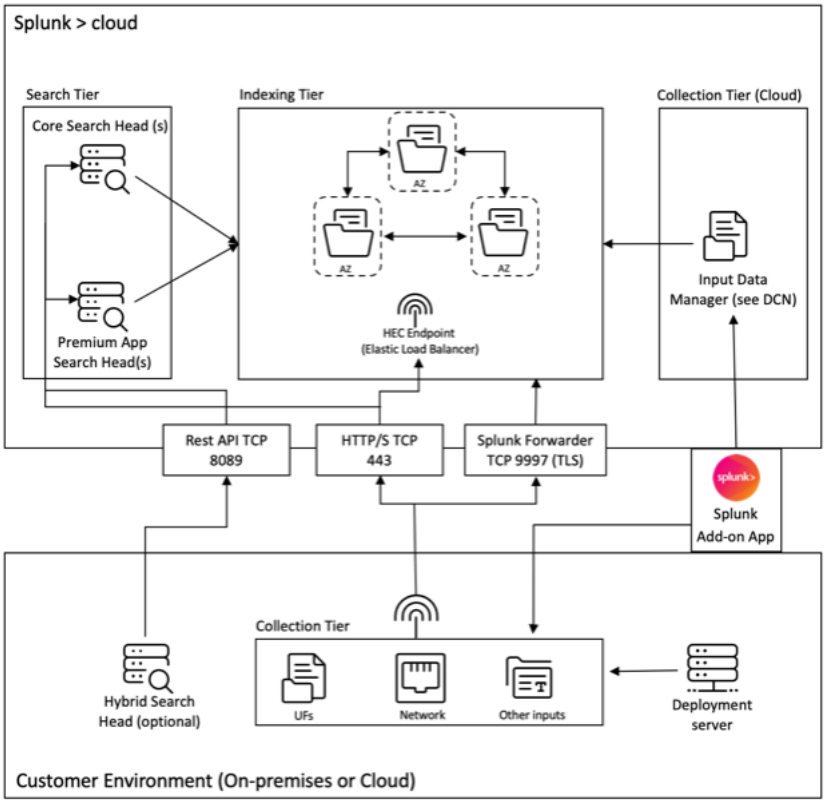
收集数据后，将对其进行索引或处理，并以使其可搜索的方式存储。

客户浏览数据的主要方式是搜索。搜索可以另存为报告，并用于为控制板面板提供动力。搜索是从您的数据中提取的信息。

通常，Splunk 附加应用程序部署在集合层（Splunk 企业级），而我们的控制板应用程序部署在搜索层（Splunk Cloud 级别）。在简单的本地设置中，您可以将所有这三个层都放在单个 Splunk 主机上（称为单服务器部署）。

集合层是使用 Splunk 附加应用程序的更好方式。安装附加应用程序有两种方法。您可以将其安装在客户环境下的集合层，也可以将其安装在 **Splunk Cloud** 实例下的输入数据管理器中。

请参阅下图，了解我们的附加应用程序的 Splunk 部署架构：



上述图表中显示的输入数据管理器 (IDM) 是 Splunk 云托管的数据收集节点 (DCN) 的实现，仅支持脚本和模块化输入。对于除此之外的数据收集需求，您可以使用 Splunk 重型转发器在您的环境中部署和管理 DCN。

Splunk 允许收集、索引和搜索来自各种来源的数据。收集数据的一种方法是通过 API，这允许 Splunk 访问存储在其他系统或应用程序中的数据。这些 API 可以包括 REST、Web 服务、JMS 和/或 JDBC 作为查询机制。Splunk 和任何第三方开发人员提供了一系列通过 Splunk 模块化输入框架实现 API 交互的应用程序。这些应用程序通常需要安装完整的 Splunk 企业软件才能正常运行。

为了便于通过 API 收集数据，通常将重型转发器部署为 DCN。重型转发器比通用转发器更强大，因为它们包含完整的解析管道，可以理解单个事件并对单个事件采取操作。这使他们能够通过 API 收集数据并对其进行处理，然后再将其转发到 Splunk 实例进行索引。

要了解有关 Splunk 云部署高级架构的更多信息，请参阅 Splunk 验证架构。

Splunk 的 Citrix Analytics 控制板

December 7, 2023

> ** 注意事项 **
>
> ：Citrix Content Collaboration 和 ShareFile 的使用寿命已接近尾声，不再向用户开放。

> 此功能在预览版中提供。

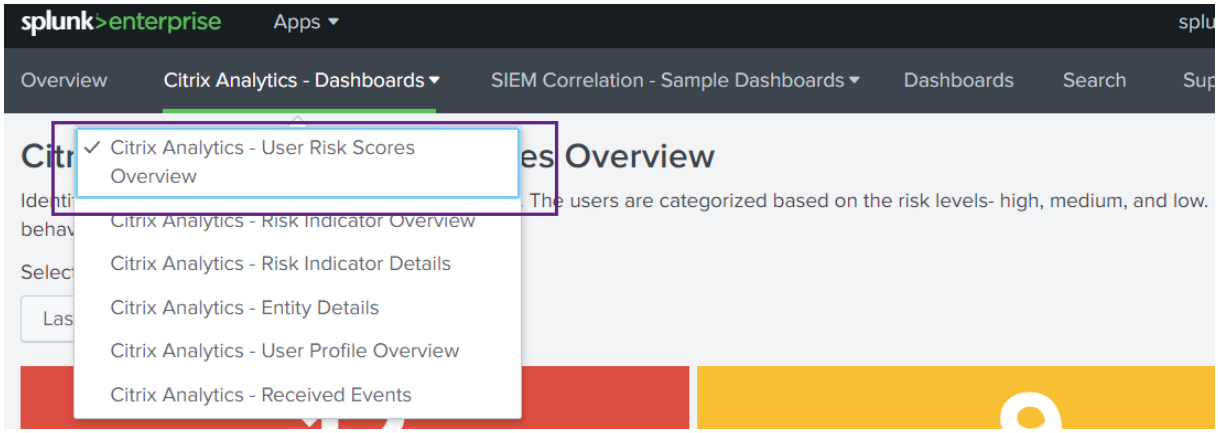
必备条件

要使用以下 Citrix Analytics 控制板，请确保您已经配置并设置了适用于 Splunk 的 Citrix Analytics 应用程序。

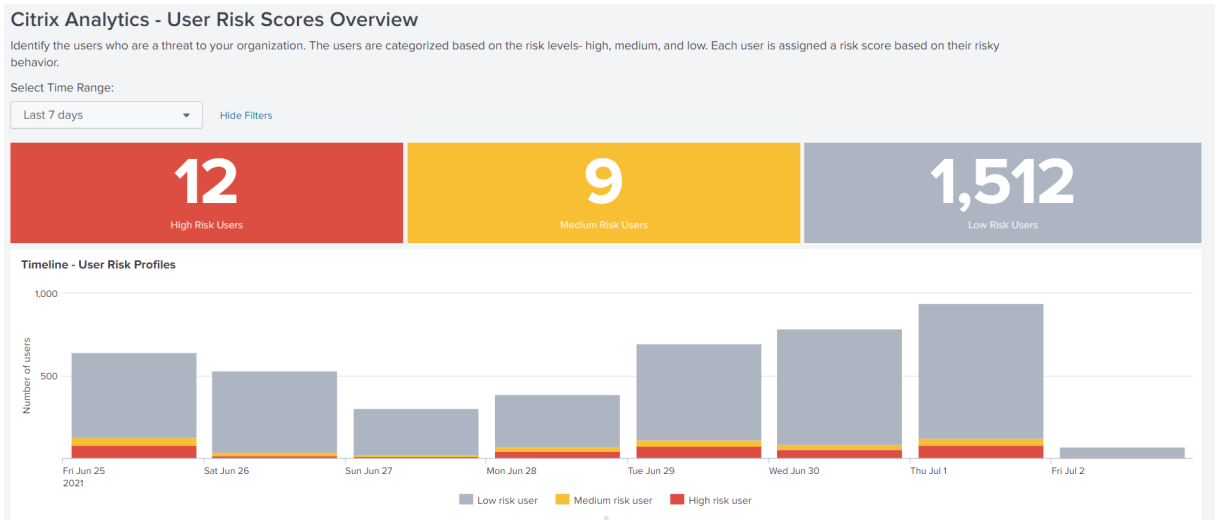
用户风险评分概述

此控制板提供了组织中存在风险的用户的综合视图。用户按风险级别进行分类-高、中和低。风险级别基于用户事件中的异常情况，因此会分配风险评分。有关风险用户类型的更多信息，请参阅用 户控制板。

要查看此控制板，请单击 **Citrix Analytics-**控制板 **> Citrix Analytics-**用户风险评分概述。



选择预设的时间范围或自定义时间范围以查看有风险的用户的时间轴及其详细信息。



“风险用户”表提供以下信息：

- 用户：表示用户名。单击用户名可在 Citrix Analytics-实体详细信息控制板上查看有关用户风险行为的详细信息。

- 发现的受损端点风险：表示属于受感染终端风险类别的用户触发的风险指示器的数量。
- 发现的受感染用户风险：表示属于受感染用户风险类别的用户触发的风险指示器的数量。
- 发现的数据泄露风险：表示属于数据泄露风险类别的用户触发的风险指示器的数量。
- 发现的内部威胁风险：表示属于内部威胁风险类别的用户触发的风险指示器的数量。
- 风险评分：表示用户的风险评分。

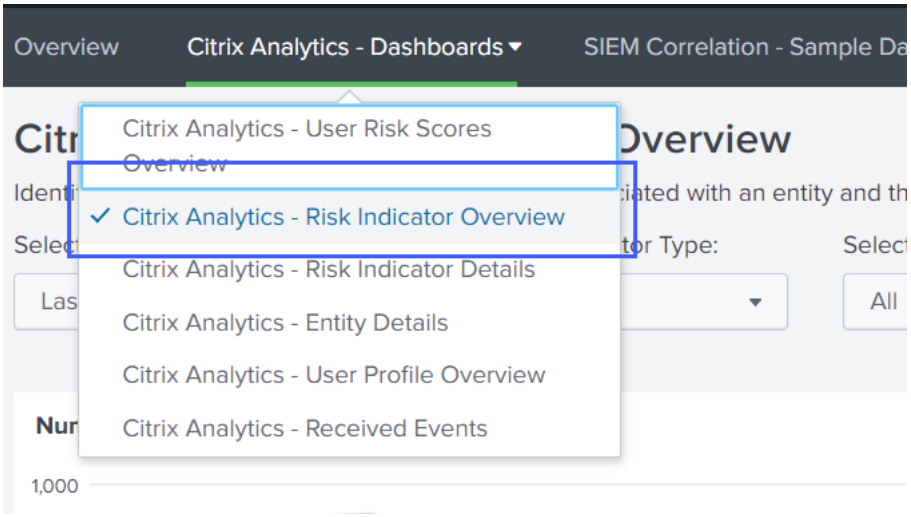
您还可以按用户名搜索用户并获取所需的详细信息。

有关更多信息，请参阅 风险类别。

风险指标概述

控制面板提供了组织中用户触发的风险指示器的综合视图。

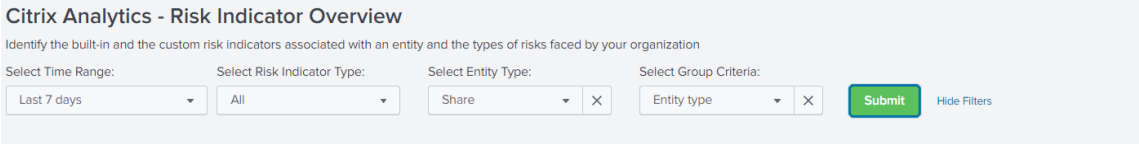
要查看控制板，请单击 **Citrix Analytics-**控制板 **> Citrix Analytics-**风险指示器概述。



选择类别以查看报告

通过选择一个或多个类别来搜索风险指标：

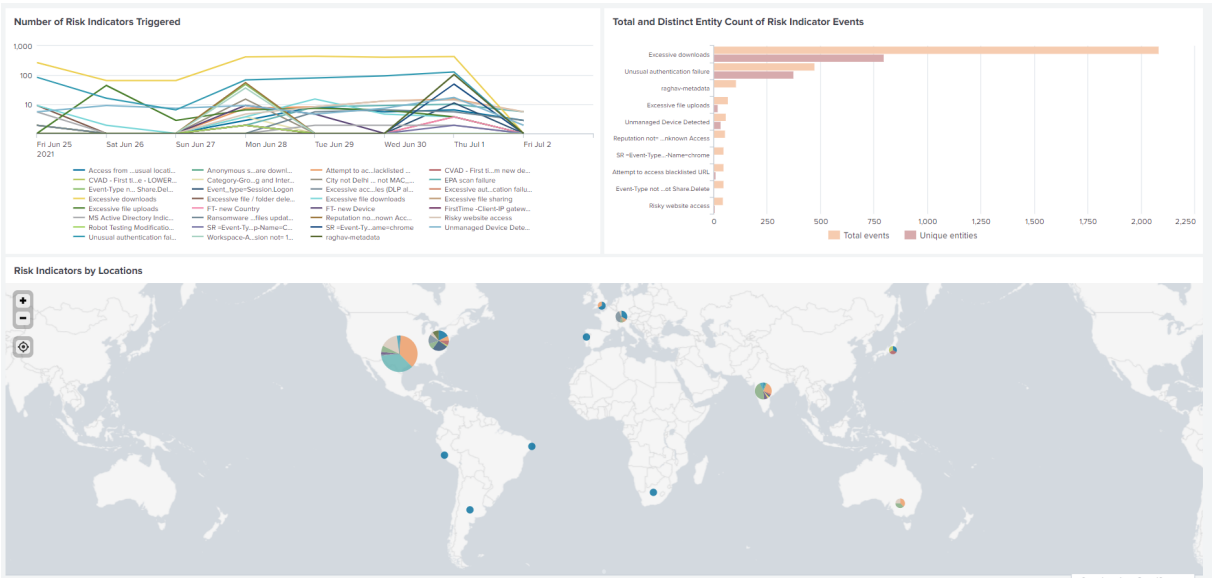
- 时间范围：选择预设时间范围或自定义时间范围以查看该时间段内触发的风险指示器。
- 风险指示器类型：选择风险指示器的类型：内置或自定义。
- 实体类型：选择一个用户来查看相关的风险指标。
- 组：选择一个条件以按数据源、指标类别、指标名称、指标类型或实体类型对用户事件进行分组，然后查看关联的风险指标。



查看报告

通过选择一个或多个类别，使用以下报表查看有关风险指示器的详细信息：

- 触发的风险指示器数量：显示在选定期间内触发的风险指示器的数量。使用此报告可以确定风险事件的模式和区域。另外，确定组织中风险最大的事件。
- 风险指示器事件的总数和不同实体计数：显示与风险指示器对应的事件总数和唯一事件。使用此报告来确定组织中每个风险指标和主要风险指标的出现情况。您还可以确定有多少独立用户触发了特定的风险指标，并检查该风险指标是由更大还是更小的用户组触发的。
- 按位置划分的风险指示器：显示用户在不同位置触发的风险指示器的数量。使用此报告可以确定显示风险较高的事件的位置，并检查这些地点是否在组织的运营区域之外。
- 风险指示器详细信息：显示有关风险指示器的详细信息，例如关联的数据源、指标类别、指标类型和出现次数。



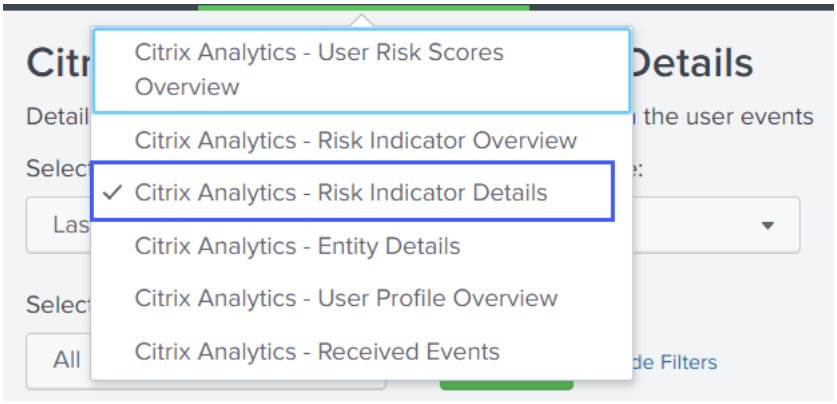
Risk Indicator Details

Data source	Indicator category	Indicator type	Indicator name	Number of Risk Indicator Events
Citrix Content Collaboration	Data exfiltration	builtin	Excessive downloads	2084
Citrix Content Collaboration	Compromised users	builtin	Unusual authentication failure	473
Citrix Virtual Apps and Desktops	Data exfiltration	custom	raghav-metadata	104
Citrix Content Collaboration	Insider threats	builtin	Excessive file uploads	68
Citrix Endpoint Management	Compromised endpoints	builtin	Unmanaged Device Detected	59
Citrix Access Control	Compromised users	custom	Reputation not= Clean Access AND Reputation not= Unknown Access	55
Citrix Virtual Apps and Desktops	Compromised users	custom	SR =Event-Type=Citrix.EventMonitor.AppStart AND App-Name=chrome	49
Citrix Access Control	Insider threats	builtin	Attempt to access blacklisted URL	48
Citrix Content Collaboration	Compromised users	custom	Event-Type not Share.Create AND Event-Type not Share.Delete	48
Citrix Access Control	Insider threats	builtin	Risky website access	44

风险指标详情

控制板提供有关用户触发的内置和自定义风险指标的详细信息。有关详细信息，请参阅 Citrix 用户风险指示 器和 自定义风险指示器。

要查看控制板，请单击 **Citrix Analytics-**控制板 **> Citrix Analytics-**风险指示器详细信息。



选择类别以查看报告

通过选择一个或多个类别来查看风险指标的详细信息：

- 时间范围：选择预设的时间范围或自定义时间范围以查看该时间段内触发的风险指示器的详细信息。
- 实体类型：选择一个用户来查看相关风险指标的详细信息。
- 风险指示器类型-选择内置或自定义的风险指标类型以查看其详细信息。
- 数据源-选择数据源以查看相关风险指示器的详细信息。
- 风险指示器类别-选择风险类别以查看相关风险指标的详细信息。
- 风险指示器-选择风险指示器以查看其详细信息。

查看报告

例如，从选择风险指示器列表中，选择 异常身份验证失败 **(Citrix Content Collaboration)**，单击 提交，然后查看以下信息：

- 与风险指标相关的前 10 位用户
- 有关风险指标的详细信息，例如
  - 触发的日期和时间
  - 关联的数据源
  - 关联的风险类别
  - 关联的实体 ID 和用户实体类型
  - 风险严重程度-高、中或低
  - 用户事件的风险概率
  - 风险指示器的唯一标识 (UUID)

在 按风险指示器排名前 **10** 位的实体中，单击实体以在 **Citrix Analytics**-实体详细信息控制板上查看其详细信息。

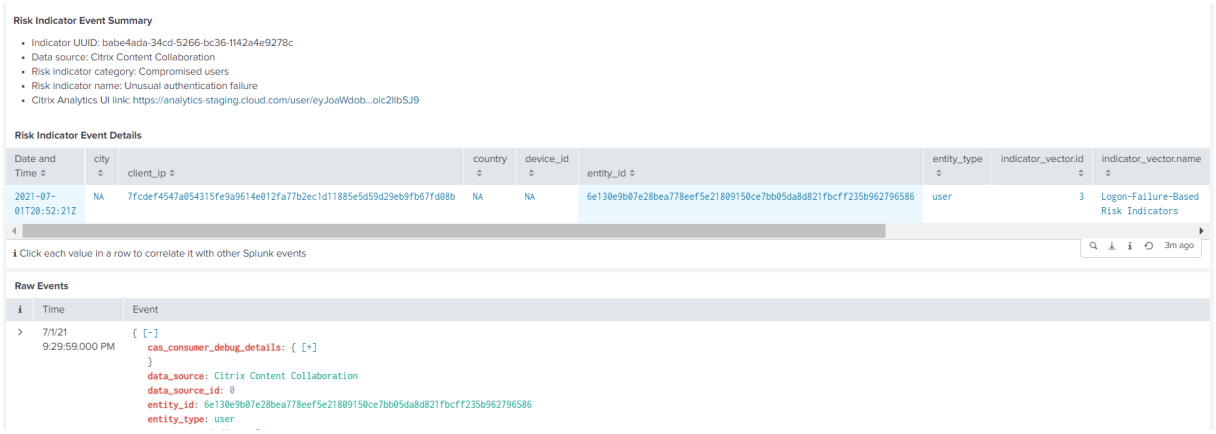
Risk Indicator Details

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	102854bc92af241d303ab4c3cc62ec969a0c64c69985703293372 8b1d10a848	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

单击“风险指标详细信息”表的每一行，查看所选风险指标的事件摘要、事件详细信息和原始事件。

在风险指示器事件摘要部分中，单击 **Citrix Analytics UI** 链接，直接从 Splunk 转到 Citrix Analytics for Security 上的用户时间轴。在用户时间轴上，查看风险指示器、相关事件以及针对用户应用的任何操作。

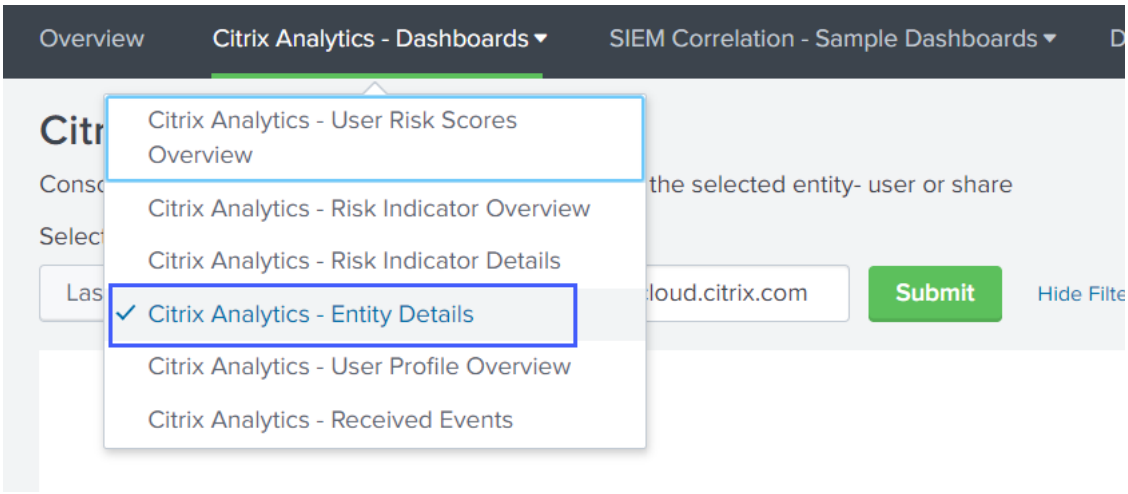
有关事件摘要和事件详细信息的更多信息，请参阅 SIEM 的 Citrix Analytics 数据格式。



实体详情

使用仪表板查看有关用户实体用户及其风险行为的详细信息。

要查看控制板，请单击 **Citrix Analytics-**控制板 **> Citrix Analytics-**实体详细信息。

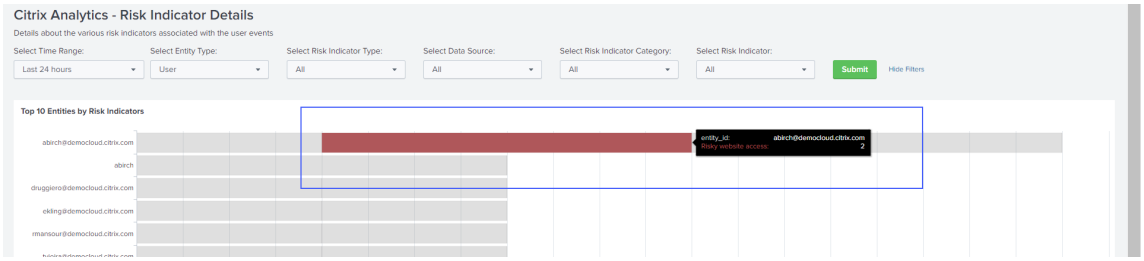


查看报告

输入时间范围和实体（用户名），然后单击“提交”以查看详细信息。

或者，您也可以从以下控制板中查看有关实体的详细信息：

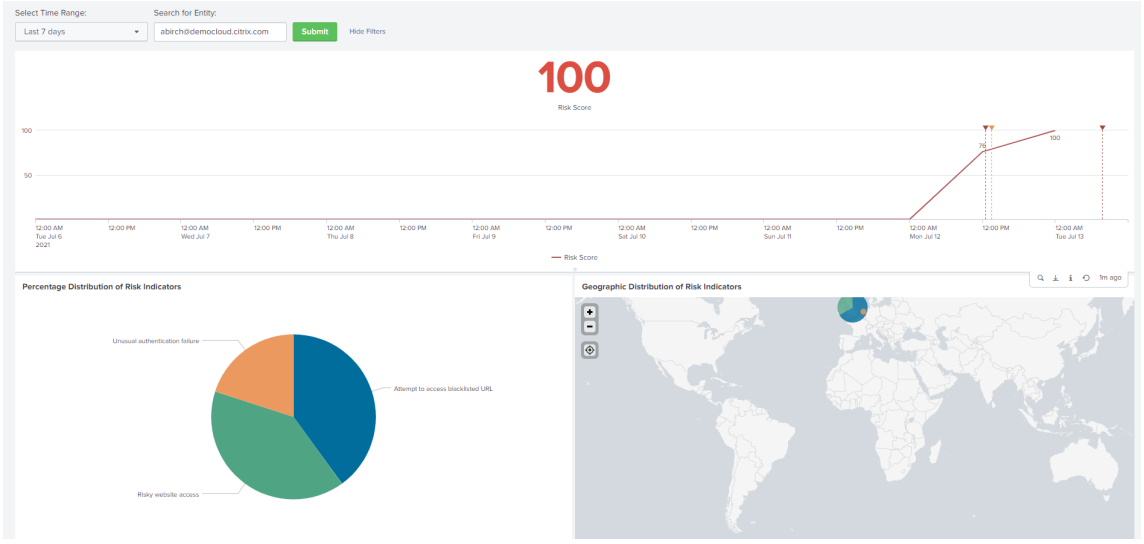
- 在 **Citrix Analytics-**风险指示器详细信息上，转到 按风险指示器排名前 **10** 位的实体，然后单击一个实体。

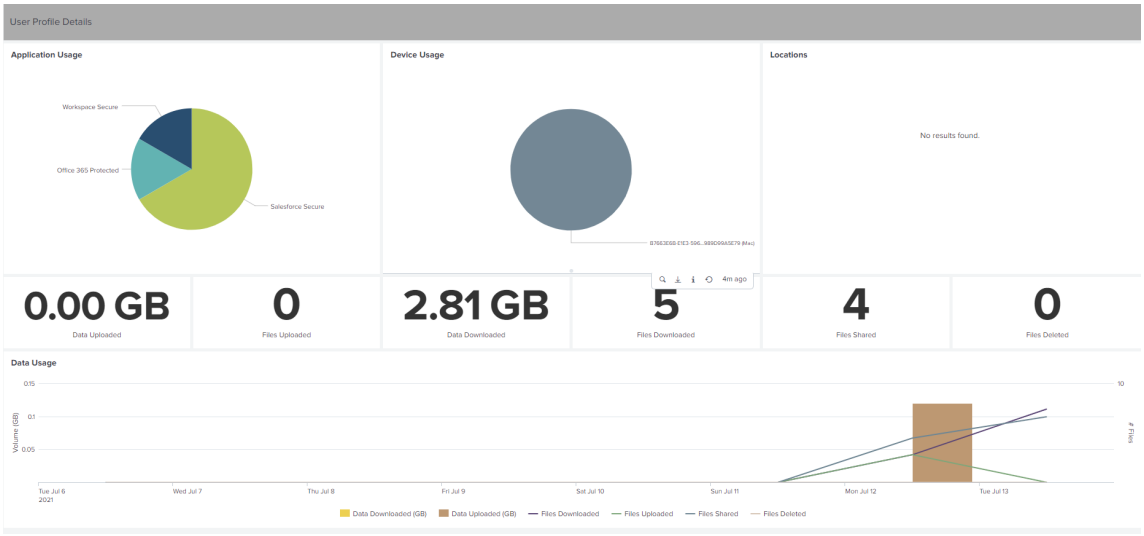


- 在 **Citrix Analytics-**风险评分概述上，转到风 险用户，然后单击用户名。

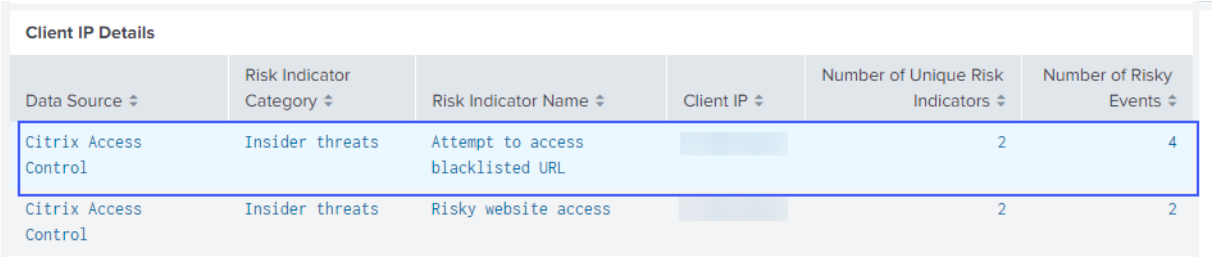
将显示以下详细信息：

- 所选时间范围内的当前风险评分和风险评分时间表。
- 风险指标的百分比分布。帮助您分析实体的危险事件模式。
- 风险指标的地理分布。帮助您识别不寻常和高风险的地点。
- 与风险事件相关的客户端 IP 详细信息。
- 与风险事件相关的用户设备详细信息。
- 风险指示器详细信息，例如关联的数据源、风险类别、风险严重程度等。





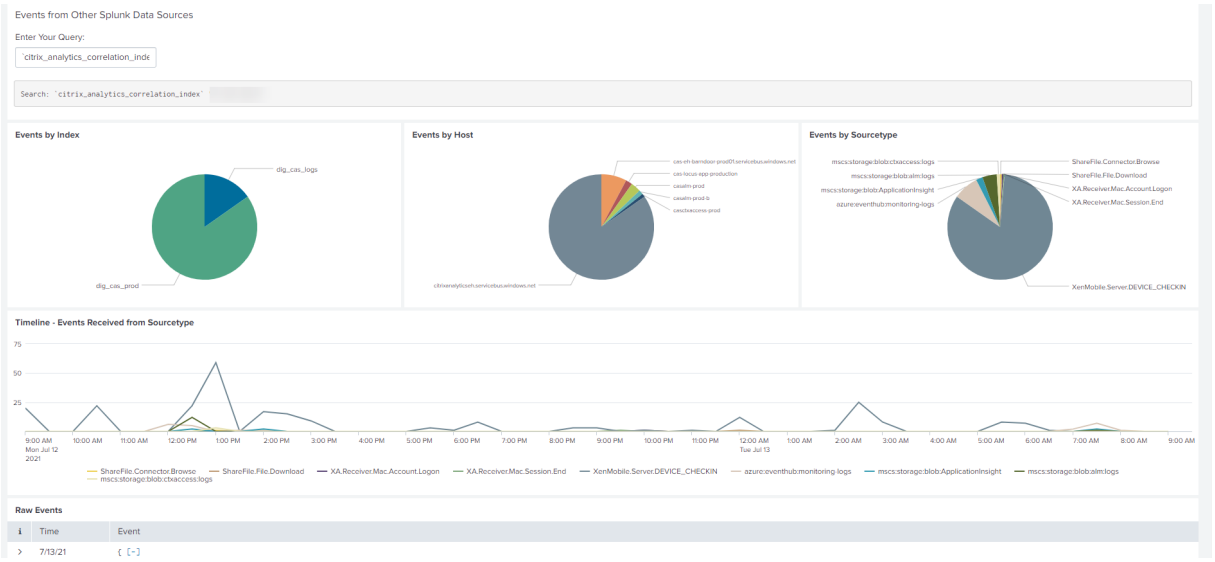
将与危险活动相关的客户端 IP 和用户设备与从与 Splunk 关联的其他安全来源收集的事件关联起来。例如，单击“客户端 **IP** 详细信息”表中的一行。



Client IP Details

Data Source	Risk Indicator Category	Risk Indicator Name	Client IP	Number of Unique Risk Indicators	Number of Risky Events
Citrix Access Control	Insider threats	Attempt to access blacklisted URL		2	4
Citrix Access Control	Insider threats	Risky website access		2	2

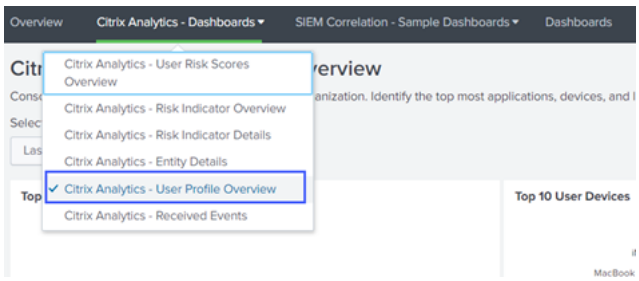
在 **Citrix Analytics** 事件关 联控制板上，您可以查看与所选客户端 IP 关联的事件，这些事件与其他安全数据源（基于索引和源类型）相关联。这些事件可以更深入地了解与客户端 IP 相关的恶意事件。



用户资料概述

使用控制面板查看与组织中的用户关联的事件量度。

要查看控制板，请单击 **Citrix Analytics-**控制板 **> Citrix Analytics-**用户配置文件概述。

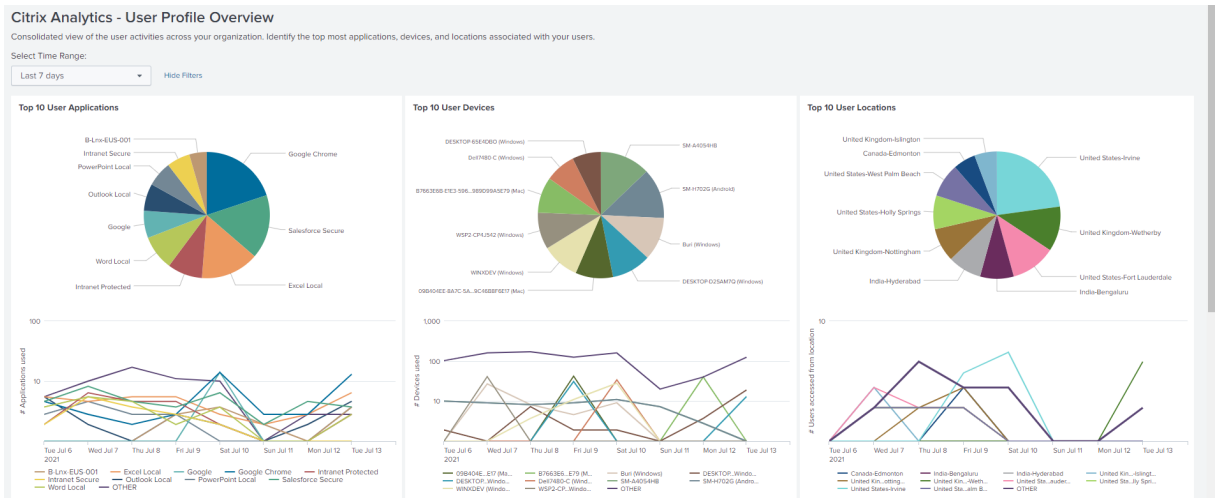


查看事件

选择时间范围并查看以下指标：

- 用户使用的前 10 个应用程序
- 用户使用的十大设备
- 用户使用的前 10 个位置
- 使用的 Web 和 SaaS 应用程序的数量
- 使用的设备数量
- 跨位置访问过的用户数量
- 数据使用情况指标，例如上传、下载、共享的文件

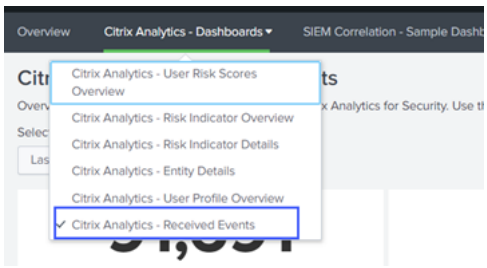
这些指标可让您深入了解组织中的用户事件。您可以识别最重要的应用程序和设备、使用模式、不合规的设备和应用程序、异常位置、存在风险的访问以及异常的文件事件。



收到的事件

使用控制板查看从 Citrix Analytics for Security 接收的事件。事件表示用户事件的类型。

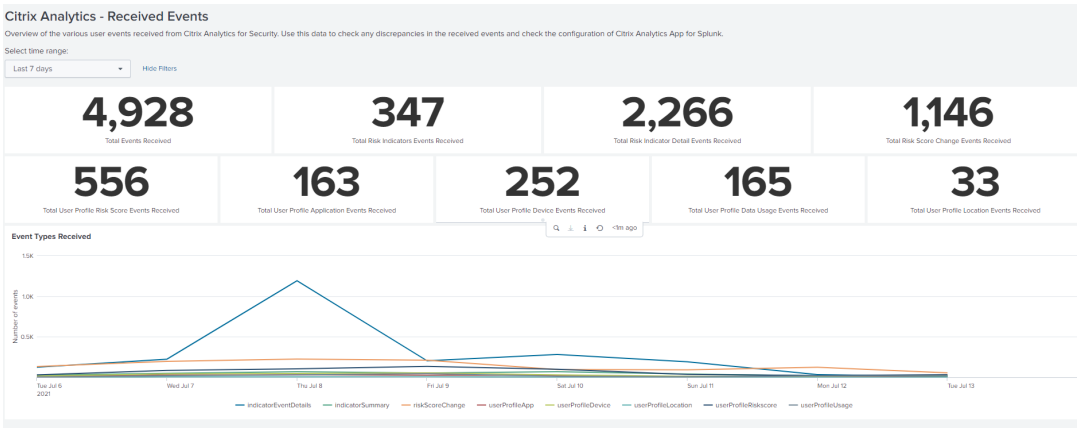
要查看控制板，请单击 **Citrix Analytics-**控制板 **> Citrix Analytics-**已收到的事件。



查看报告

选择时间范围来查看和比较收到的各种类型的事件。控制面板提供以下信息：

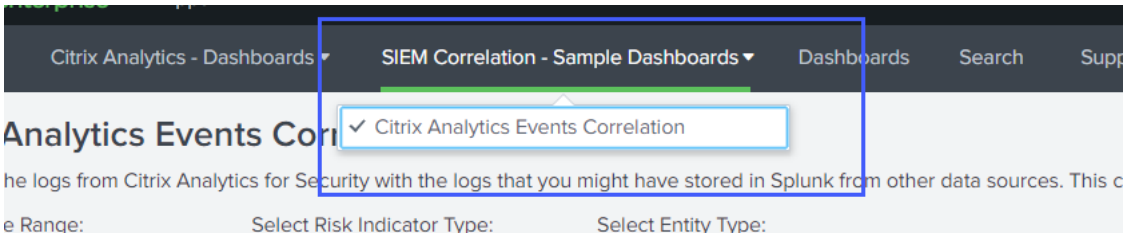
- 收到的事件总数：它是从 Citrix Analytics for Security 收到的所有事件的汇总，包括以下内容：
  - 风险指示器事件总数：表示用户与触发的风险指示器关联的事件。
  - 总风险指示器详细信息事件：表示与触发的风险指示器的详细信息相关联的事件。
  - 风险评分变化事件总数：表示与用户风险评分变化相关的事件。
  - 用户配置文件风险评分事件总数：表示与用户的风险评分关联的事件。
  - 用户配置文件应用程序事件总数：表示与用户使用的应用程序相关联的事件。
  - 用户配置文件设备事件总数：表示与用户使用的设备相关联的事件。
  - 用户配置文件数据使用事件总数：表示与用户的数据使用情况相关联的事件。
  - 用户配置文件位置事件总数：表示与用户访问的位置相关联的事件。



示例事件关联

使用控制板将从 Citrix Analytics for Security 接收的事件与从在 Splunk 中配置的其他安全数据源收集的事件关联起来。您可以更深入地了解从多个数据源收集的用户的风险活动，找出事件之间的关系，并识别任何威胁。

要查看控制板，请单击 **SIEM** 关联-示例控制板 **> Citrix Analytics** 事件关联。



必备条件

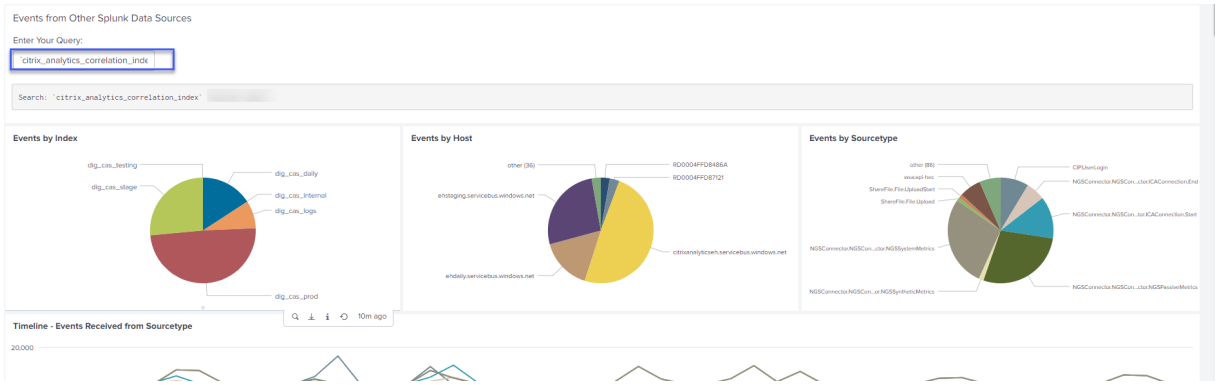
要执行关联，请确保执行以下操作：

- 您必须具有来自其他安全数据源的事件才能关联。例如，与从 Splunk 中配置的其他数据源接收的用户、设备和客户端 IP 地址相关联的事件。
- 在配置过程中，您必须已经定义了相关索引。

关联事件

可以查看 Citrix Analytics for Security 检测到的风险最高的实体和风险最高的 IP 地址。要将这些事件与其他数据源（在索引和源类型中定义）关联起来，请单击表中的实体或 IP 地址。

查询字段中显示的索引值是在应用程序配置期间定义的。您可以根据要求将索引值更改为不同的安全数据源。

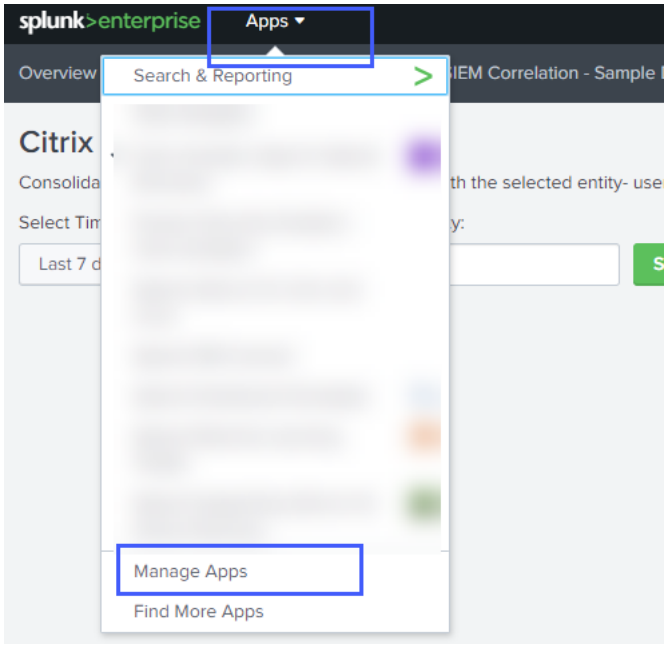


没有事件的故障排除

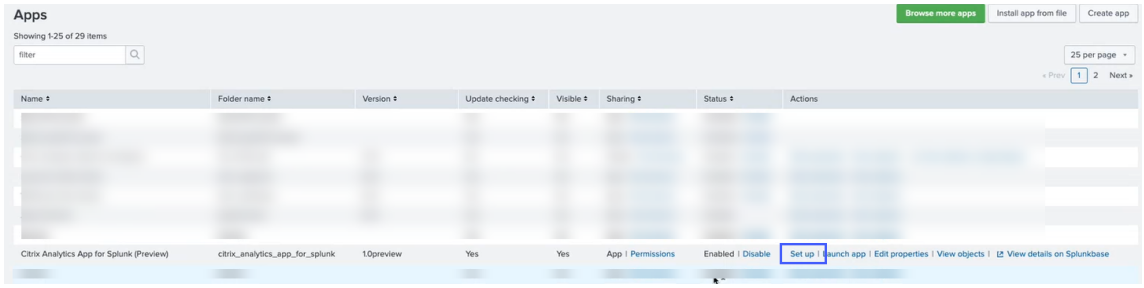
如果未在所有控制板上找到任何事件，则可能是因为适用于 Splunk 的 Citrix Analytics 应用程序和适用于 Splunk 的 Citrix Analytics 附加组件中存在配置问题。在这种情况下，验证索引值和源类型值。确保应用程序和插件中索引和源类型的值相同。

要查看适用于 Splunk 的 Citrix Analytics 应用程序的配置设置：

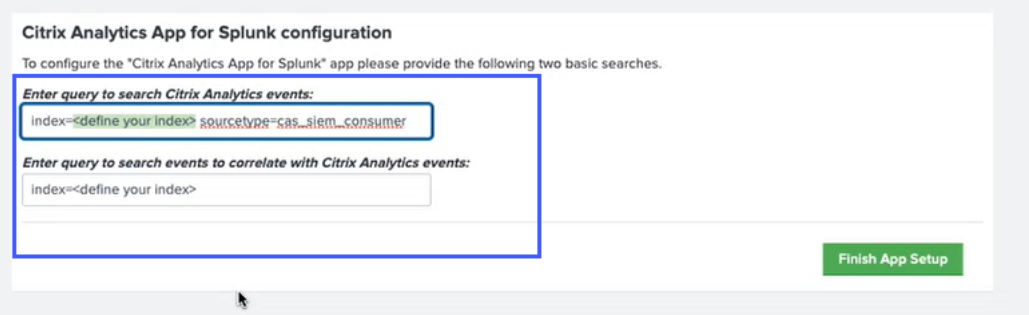
1. 单击 应用 **>** 管理应用程序。



2. 从列表中找到适用于 Splunk 的 Citrix Analytics 应用程序。单击 设置。

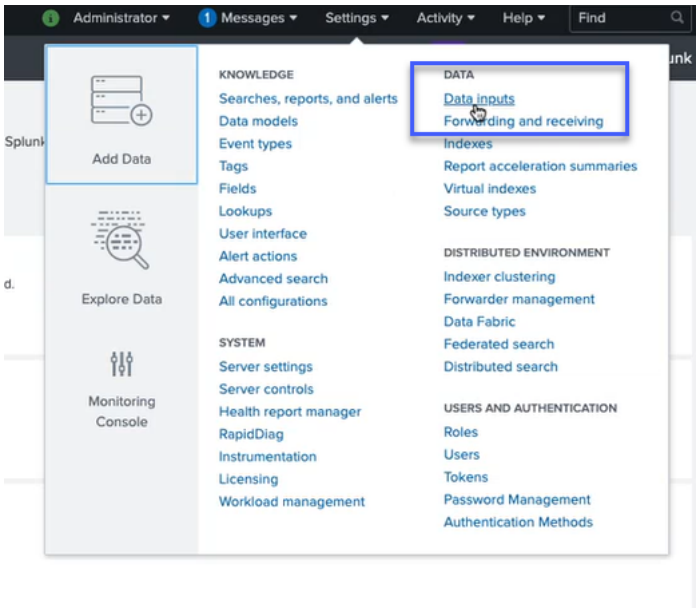


3. 检查源类型和索引。

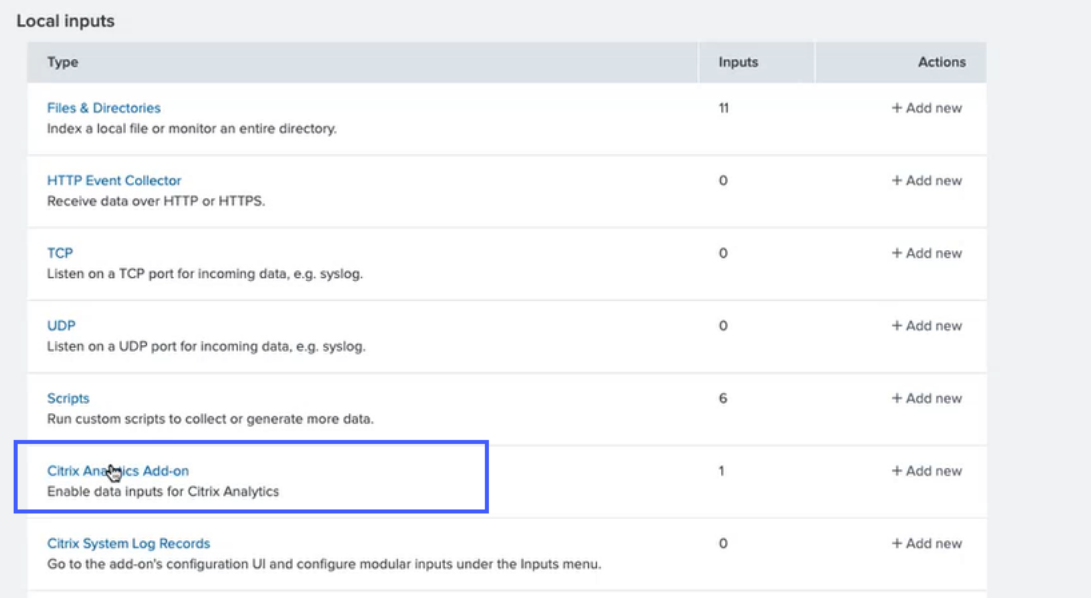


要查看适用于 Splunk 的 Citrix Analytics 附加组件的配置设置：

1. 单击 设置 **>** 数据输入。

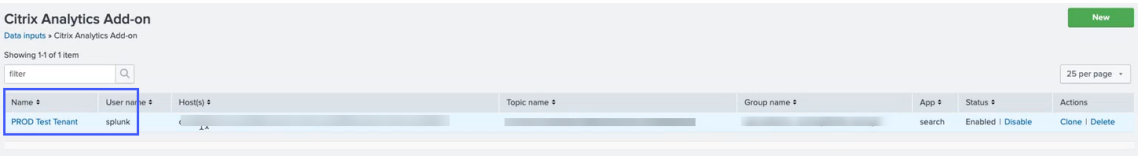


2. 单击 **Citrix Analytics** 加载项。

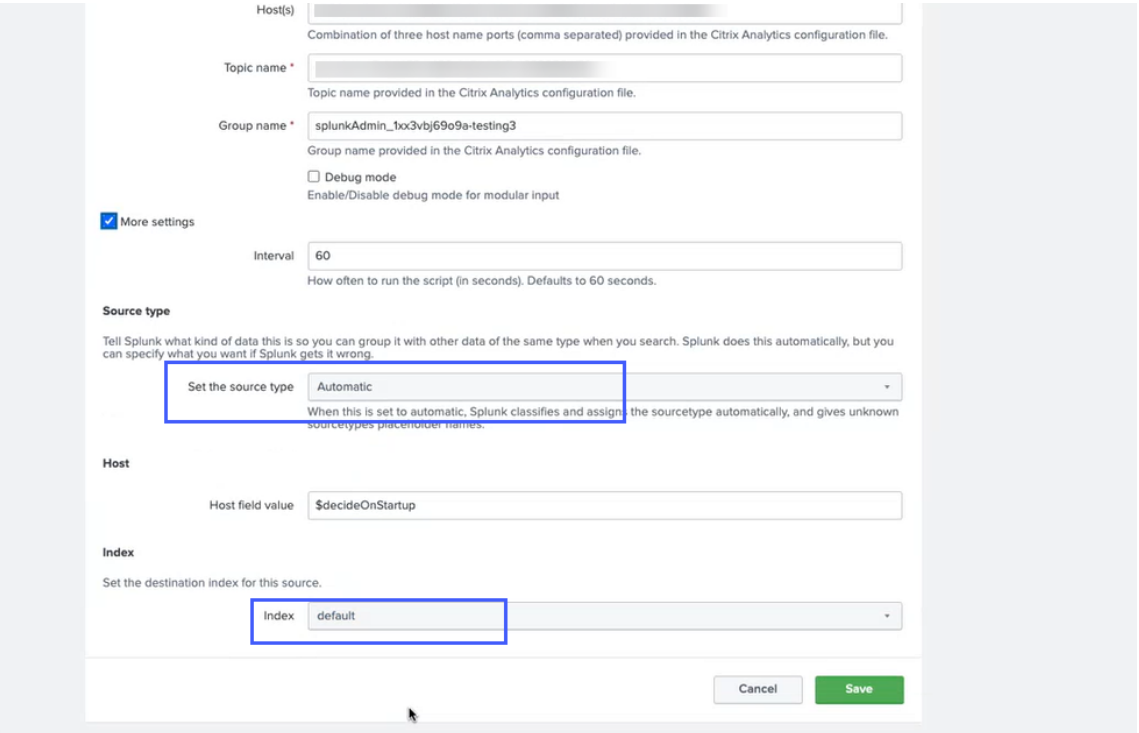


3. 单击从中获取事件的租户。

4. 选择 更多设置。



5. 检查源类型和索引。



有关配置的更多信息，请参阅 为 Splunk 配置 Citrix Analytics 加载项。

适用于 **Splunk** 的 **Citrix Analytics** 加载项存在配置问题

July 12, 2022

Citrix Analytics 加载项设置不可用

在您的 Splunk Forwarder 或 Splunk 独立环境中安装适用于 Splunk 的 Citrix Analytics 加载项后，您不会在“设置” **>** “数据输入”下看到 Citrix Analytics 加载项设置。

原因

在不受支持的 Splunk 环境中安装适用于 Splunk 的 Citrix Analytics 加载项时，会出现此问题。

修复

在受支持的 Splunk 环境中安装适用于 Splunk 的 Citrix Analytics 加载项。有关受支持版本的信息，请参阅 Splunk 集成。

Splunk 控制板上没有可用的数据

在 Splunk Forwarder 或 Splunk Standalone 环境中安装和配置适用于 Splunk 的 Citrix Analytics 加载项后，您在 Splunk 控制板中看不到来自 Citrix Analytics 的任何数据。

检查

要解决此问题，请在您的 Splunk 转发器或 Splunk 独立环境中验证以下各项：

1. 确保满足 Splunk 集成的 必备条件 。
2. 转到 设置 **>** 数据输入 **> Citrix Analytics** 加载项。确保 Citrix Analytics 配置详细信息 可用。
3. 如果配置详细信息可用，请运行以下查询以检查日志中是否存在与适用于 Splunk 的 Citrix Analytics 加载项相关的任何错误：

```
index=_internal sourcetype=splunkd log_level=ERROR component=
    ExecProcessor cas_siem_consumer
```


4. 如果您没有发现任何错误，适用于 Splunk 的 Citrix Analytics 加载项将按预期工作。如果在日志中发现任何错误，可能是由于以下原因之一：

   - 无法在您的 Splunk 环境与 Citrix Analytics Kafka 端点之间建立连接。此问题可能是由于防火墙设置造成的。

     修复：请咨询网络管理员以解决此问题。

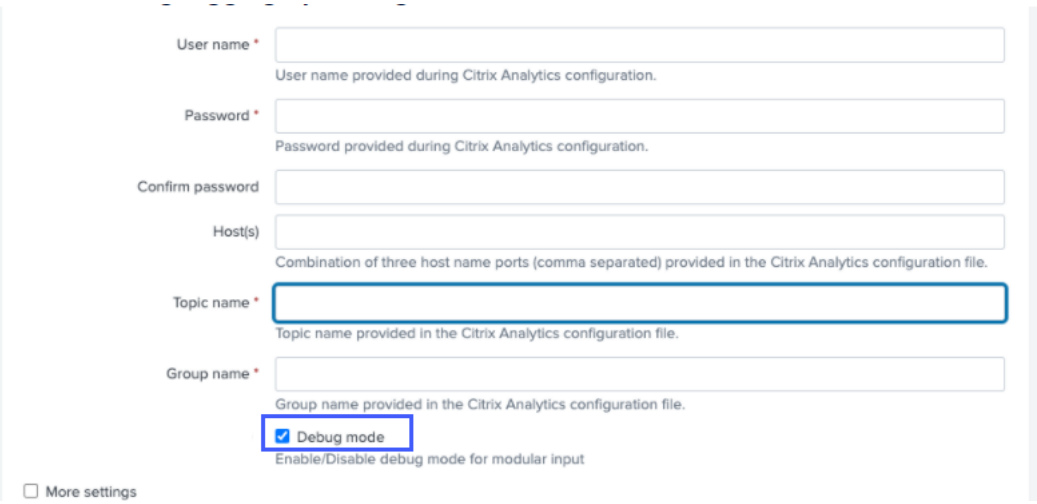
   - 设置 **>** 数据输入 **> Citrix Analytics** 加载项中的配置详细信息不正确。

     修复：确保按照 Citrix Analytics 配置文件正确输入了 Citrix Analytics 配置详细信息，例如用户名、密码、主机端点、主题和使用者组。有关更多信息，请参阅 为 Splunk 配置 Citrix Analytics 加载项。

5. 如果您无法从上述日志中找到问题的原因并希望进一步调查：

   a) 在 设置 **>** 数据输入 **> Citrix Analytics** 加载项 中启用 调试模式。

   > 注意
   >
   > 默认情况下，调试模式处于 禁用状态。启用此模式会生成太多日志。因此，请仅在需要时使用此选项，并在完成调试任务后将其禁用。

   b) 在以下位置找到生成的调试日志，并检查是否有任何错误：

   ```
   $SPLUNK_HOME$/var/log/splunk.Filename
       splunk_citrix_analytics_add_on_debug_connection.log
   ```

   c)（可选）使用适用于 Splunk 的 Citrix Analytics 加载项提供的调试脚本 `splunk cmd python cas_siem_consumer_debug.py`。此脚本生成一个日志文件，其中包含您的 Splunk 环境和连接检查的详细信息。您可以使用详细信息来调试问题。使用以下命令运行脚本：

   ```
   cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin/; /opt/splunk/bin/
       splunk cmd python cas_siem_consumer_debug.py
   ```


错误消息

在与适用于 Splunk 的 Citrix Analytics 加载项相关的日志中，您可能会看到以下错误：

```
ERRORKafkaError{ code=_TRANSPORT,val=-195,str="Failed to get metadata
: Local: Broker transport failure"}
```

此错误是由于网络连接问题或身份验证问题造成的。

要调试问题，请执行以下操作：

1. 在您的 Splunk 转发器或 Splunk 独立环境中，启用调试模式以获取调试日志。请参考前面的步骤 5.a。
2. 运行以下查询以查找调试日志中的任何身份验证问题：

```
index=_internal source="*
    splunk_citrix_analytics_add_on_debug_connection.log*" "
    Authentication failure"
```

3. 如果在调试日志中未发现任何身份验证问题，则该错误是由于网络连接问题造成的。
4. 使用 telnet 或前面的步骤 5.c 中提到的调试脚本查找并解决问题。

从低于 **2.0.0** 的版本升级加载项失败

在您的 Splunk 转发器或 Splunk 独立环境中，当您将适用于 Splunk 的 Citrix Analytics 加载项从 2.0.0 之前的版本升级到 最新 版本时，升级将失败。

修复

1. 删除适用于 Splunk 的 Citrix Analytics 加载项安装文件夹的 /bin 文件夹的以下文件和文件夹：
   - cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin
   - rm -rf splunklib
   - rm -rf mac
   - rm -rf linux_x64
   - rm CARoot.pem
   - rm certificate.pem
2. 重启您的 Splunk 转发器或 Splunk 独立版环境。

Microsoft Sentinel 集成

November 26, 2023

> 备注
>
> - 联系 CAS-PM-Ext@cloud.com 以请求 Microsoft Sentinel 集成、将数据导出到 Microsoft Sentinel 或提供反馈方面的帮助。
> - 使用 Logstash 引擎将数据导出到 Microsoft Sentinel 正在预览中。此功能在没有服务级别协议的情况下提供，不建议用于生产工作负载。有关更多信息，请参阅 Microsoft Sentinel 文档。

使用 Logstash 引擎将 Citrix Analytics for Security 与 Microsoft Sentinel 集成。

此集成使您能够将用户数据从 Citrix IT 环境导出并关联到 Microsoft Sentinel，从而更深入地了解组织的安全状况。在 Splunk 环境中查看 Citrix Analytics for Security 独有的富有洞察力的控制板。您还可以根据自己的安全要求创建自定义视图。

有关集成的好处以及发送到 SIEM 的已处理数据类型的更多信息，请参阅 安全信息和事件管理集成。

必备条件

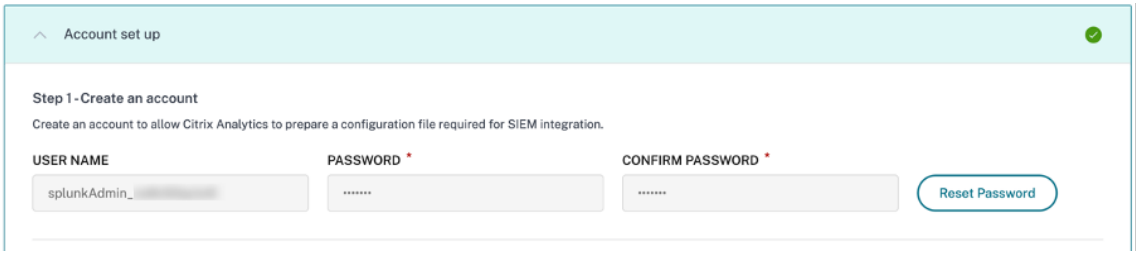
- 为至少一个数据源启用数据处理。它有助于 Citrix Analytics for Security 开始 Microsoft Sentinel 集成过程。
- 确保以下终端节点位于网络的允许列表中。

端点	美国地区	欧盟区域	亚太南部地区
Kafka 代理	casnb-0.citrix.com:9094 casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-0.citrix.com:9094 casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-0.citrix.com:9094 casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

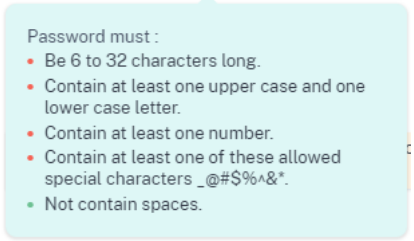
- 确保将 logstash 版本 7.17.7 或更高版本（与 Citrix Analytics for Security 的兼容性测试版本：v7.17.7 和 v8.5.3）与适用于 Logstash 的 Microsoft Sentinel 输出插件一起使用。

与 **Microsoft Sentinel** 集成

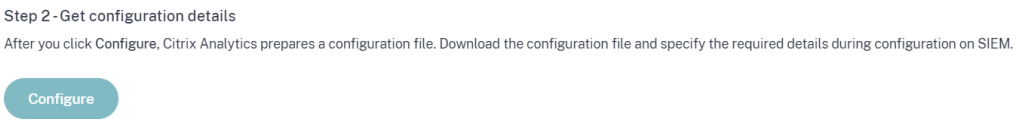
1. 前往“设置”**>**“数据导出”。
2. 在“帐户设置”部分，通过指定用户名和密码来创建帐户。此帐户用于准备集成所需的配置文件。



3. 确保密码满足以下条件：



4. 单击 配置 以生成 Logstash 配置文件。



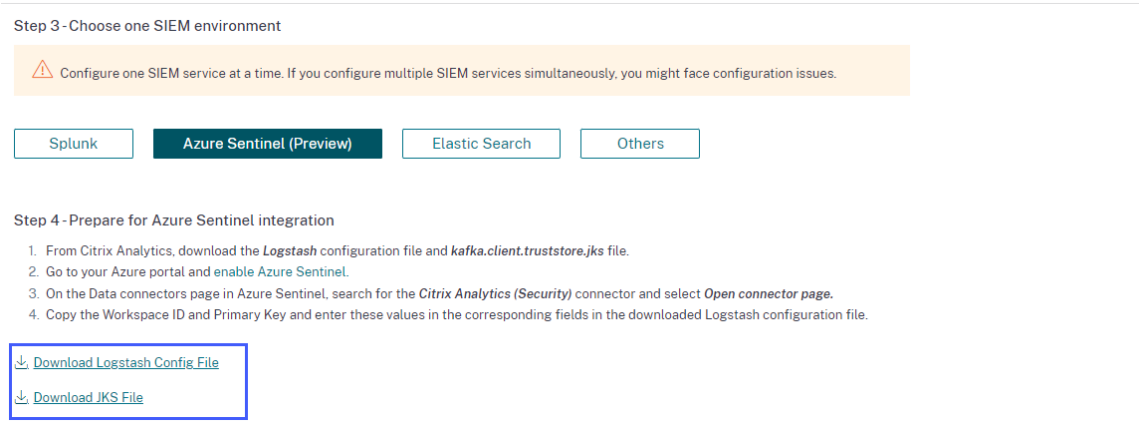
5. 选择 Azure Sentinel（预览）选项卡以下载配置文件：

   - **Logstash** 配置文件：包含用于使用 Logstash 数据收集引擎将事件从 Citrix Analytics for Security 发送到 Microsoft Sentinel 的配置数据（输入、筛选和输出部分）。

     有关 Logstash 配置文件结构的信息，请参阅 Logstash 文档。

   - **JKS** 文件：包含 SSL 连接所需的证书。

   > 注意
   >
   > 这些文件包含敏感信息。将它们存放在安全可靠的地方。



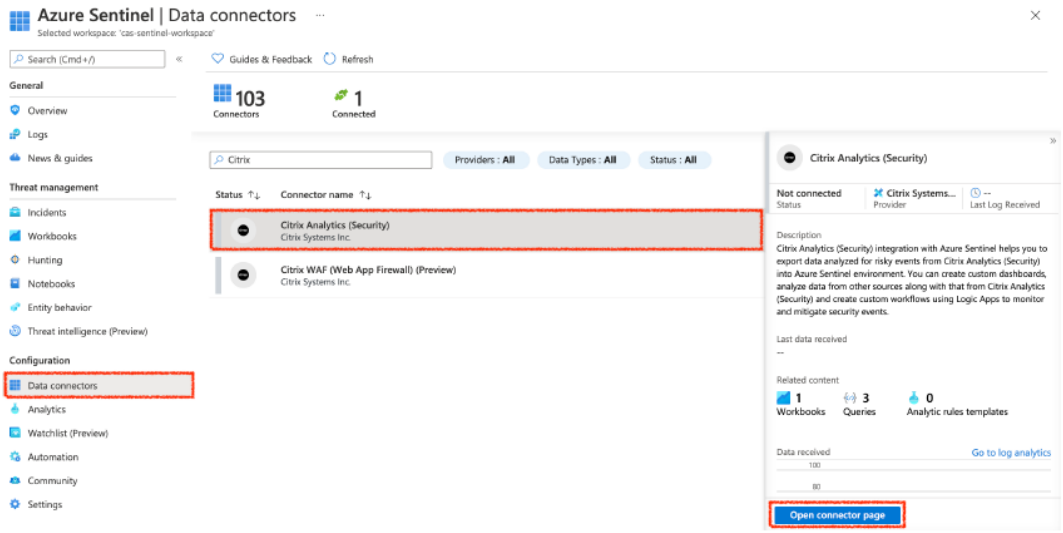
6. 准备 Azure Sentinel 集成：

   a) 在 Azure 门户上，启用 Microsoft Sentinel。您可以创建一个工作区或使用现有的工作区来运行 Microsoft Sentinel。

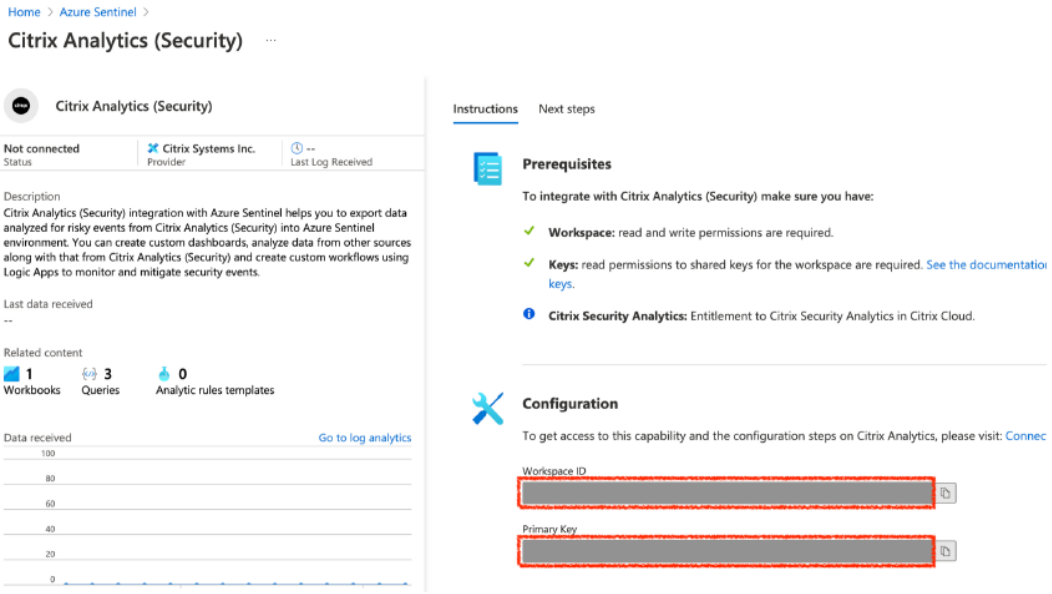
   b) 从主菜单中，选择 数据连接器 以打开数据连接器库。

   c) 搜索 **Citrix Analytics**（安全性）。

   d) 选择 **Citrix Analytics**（安全），然后选择 打开连接器页面。



   e) 在 **Citrix Analytics**（安全性）页面中，复制 **Workspace ID** 和 主键。在后续步骤中，必须在 Logstash 配置文件中输入此信息。



f) 在您的主机上配置 Logstash：

i. 在您的 Linux 或 Windows 主机上，安装 Logstash 和适用于的 Logstash 和 Microsoft Sentinel 输出插件。

ii. 在安装了 Logstash 的主机上，将以下文件放在指定的目录中：

主机类型	文件名	目录路径
Linux	CAS_AzureSentinel_LogStash_Config.config	对于 Debian 和 RPM 软件包：`/etc/logstash/conf.d/` 对于.zip 和.tar.gz 存档：`{ extract.path } /config`
	kafka.client.truststore.jks	对于 Debian 和 RPM 软件包：`/etc/logstash/ssl/` 对于.zip 和.tar.gz 存档：`{ extract.path } /ssl`
Windows	CAS_AzureSentinel_LogStash_Config.config	`C:\logstash-7.xx.x\config`
	kafka.client.truststore.jks	

有关 Logstash 安装包的默认目录结构的信息，请参阅 Logstash 文档。

iii. 打开 Logstash 配置文件并执行以下操作：

A. 在文件的输入部分，输入以下内容：

- 密码：您在 Citrix Analytics for Security 中创建的用于准备配置文件的帐户的密码。
- **SSL** 信任存储位置：SSL 客户端证书的位置。这是主机中 kafka.client.truststore.jks 文件的位置。

```
input {
  kafka {
    bootstrap_servers => "
    topics => ["
    group_id => "
    session_timeout_ms => 60000
    auto_offset_reset => "earliest"
    security_protocol => "SASL_SSL"
    sasl_mechanism => "SCRAM-SHA-256"
    ssl_endpoint_identification_algorithm => ""
    sasl_jaas_config => "org.apache.kafka.common.security.scram.ScramLoginModule required username='
    ssl_truststore_location => "/etc/logstash/ssl/kafka.client.truststore.jks"
  }
}
```

B. 在文件的输出部分，在文件的输出部分输入 Works **pace ID** 和 主键（您从 Microsoft Sentinel 复制的）。

```
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. 重新启动 Logstash 主机，将处理过的数据从 Citrix Analytics for Security 发送到 Microsoft Sentinel。

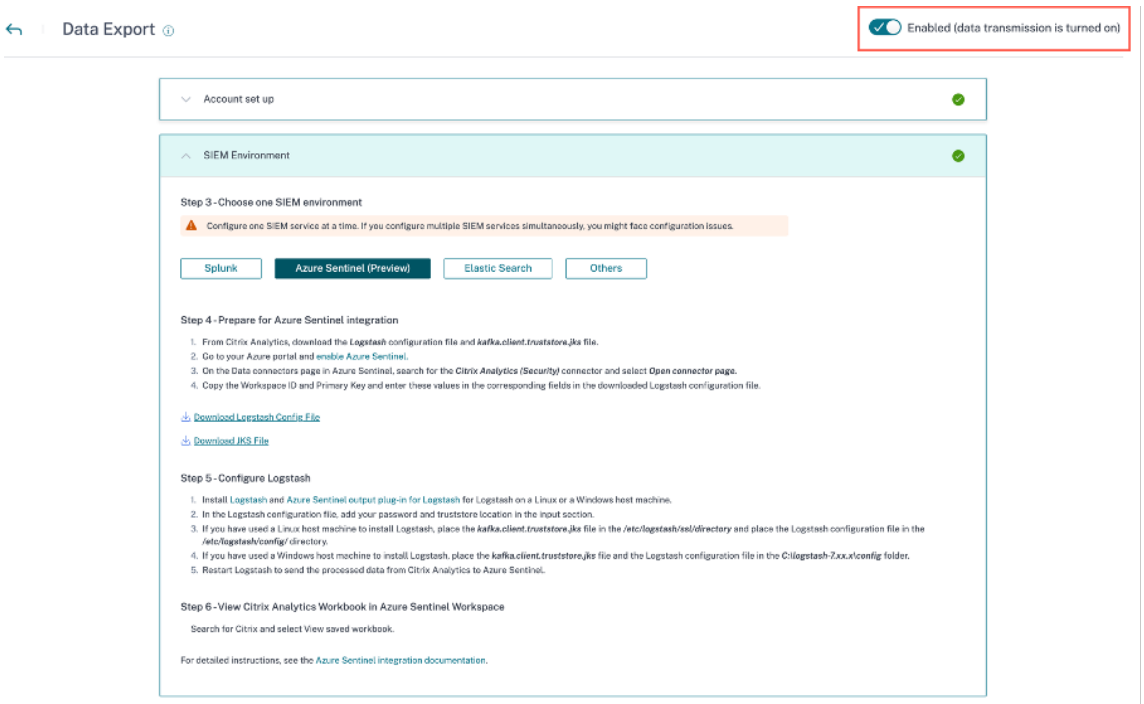
g) 转到您的 Microsoft Sentinel Workspace 并查看 Citrix Analytics 工作簿中的数据。

打开或关闭数据传输

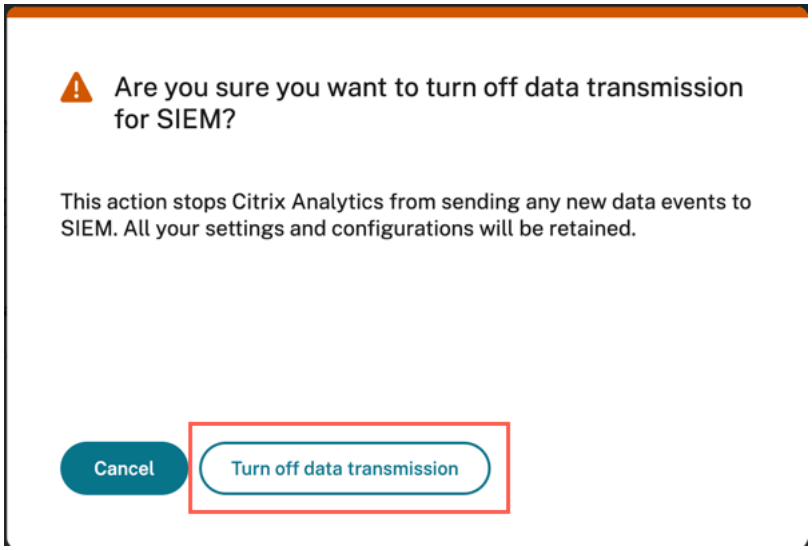
Citrix Analytics for Security 准备配置文件后，Microsoft Sentinel 的数据传输将打开。

要停止从 Citrix Analytics for Security 传输数据，请执行以下操作：

1. 前往“设置”>“数据导出”。
2. 关闭切换按钮以禁用数据传输。默认情况下，数据传输始终处于启用状态。



此时会出现一个警告窗口供您确认。单击“关闭数据传输”按钮以停止传输活动。



要再次启用数据传输，请打开切换按钮。

要了解有关 Microsoft Sentinel 集成的更多信息，请参阅以下链接：

- Citrix Analytics 与 Microsoft Sentinel 集成
- 使用 Citrix Analytics for Security 和 Microsoft Sentinel 提升您的威胁狩猎游戏

Microsoft Sentinel 的 Citrix Analytics 工作簿

December 7, 2023

> 注意
>
> 此功能在预览版中提供。

本文介绍了 Microsoft Sentinel 工作区中提供的 Citrix Analytics 工作簿。

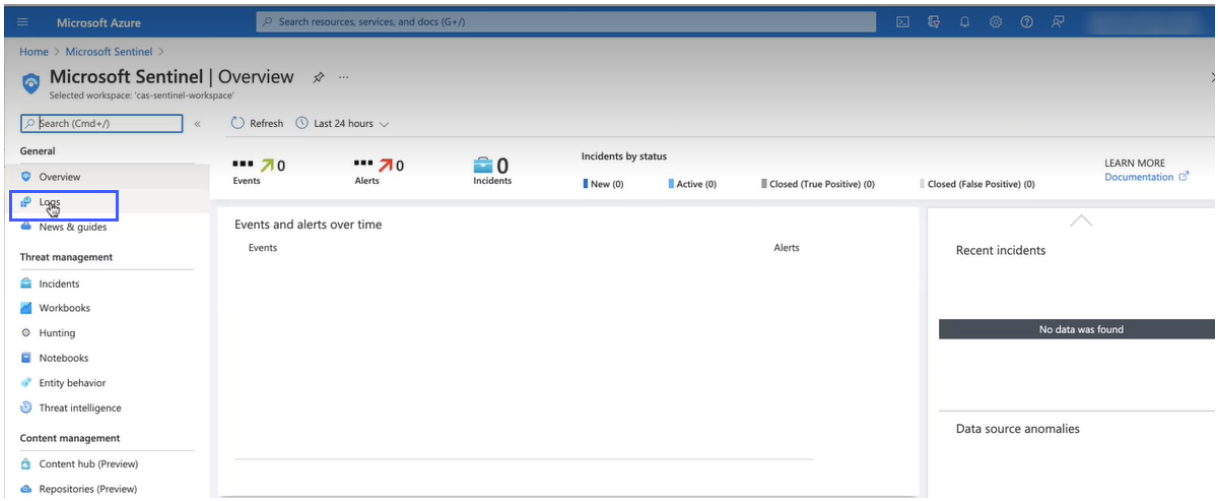
必备条件

要使用 Citrix Analytics 工作簿，请确保已将 Microsoft Sentinel 与 Citrix Analytics for Security 集成在一起。有关详细信息，请参阅 Microsoft Sentinel 集成。

查看 Citrix Analytics 活动

将 Citrix Analytics for Security 与 Microsoft Sentinel 集成后，Logstash 连接器开始将事件从 Citrix Analytics for Security 推送到 Microsoft Sentinel 工作区。在您的 **Azure** 门户上，打开你用于集成的 Microsoft Sentinel 工作区。

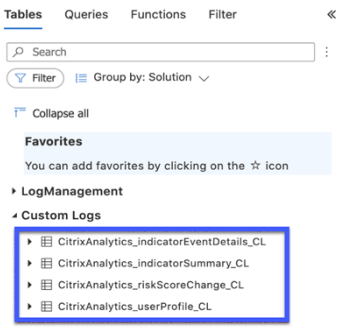
要验证 Microsoft Sentinel 是否正在接收来自 Citrix Analytics for Security 的事件，请选择日志 **>** 自定义日志。



在 自定义日志 部分中，您可以查看为存储从 Citrix Analytics for Security 接收的事件而自动创建的日志表。这些日志表充当 Citrix Analytics 工作簿上控制板的源。

> 注意

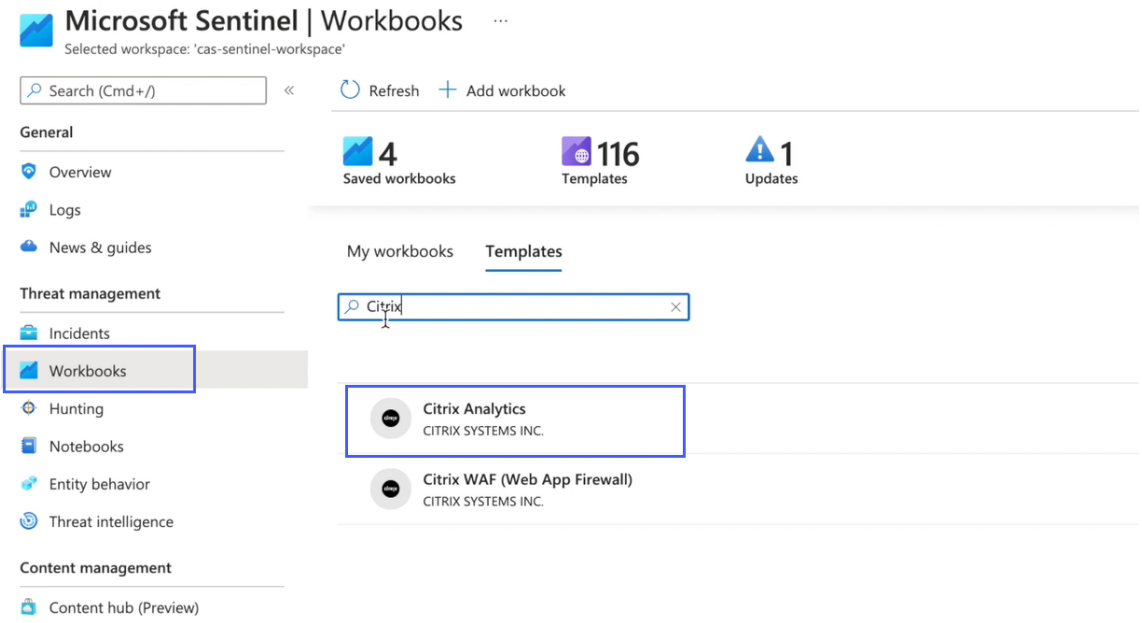
> 从 Citrix Analytics for Security 发送的事件可能需要几个小时才能显示在 Microsoft Sentinel 工作区中。因此，您可能会看到在为事件创建日志表时出现延迟。



查看 **Citrix Analytics** 工作簿

成功创建日志表后，请执行以下操作：

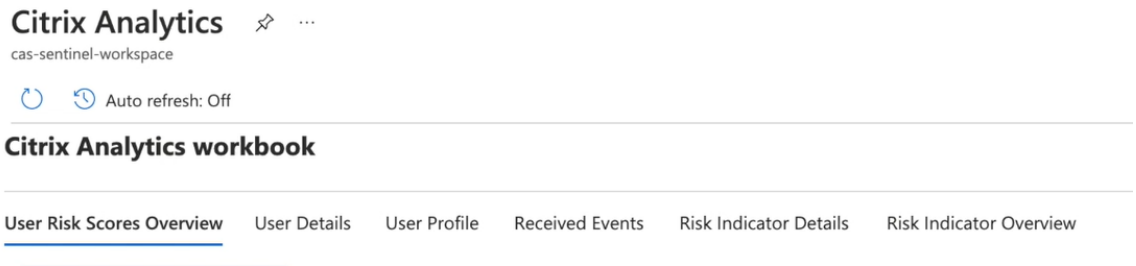
1. 选择 工作簿 并搜索 **Citrix Analytics**。选择 **Citrix Analytics**。



2. 选择 查看模板 以打开 Citrix Analytics 工作簿。

在 Citrix Analytics 工作簿中，您可以在以下控制板中查看用户事件：

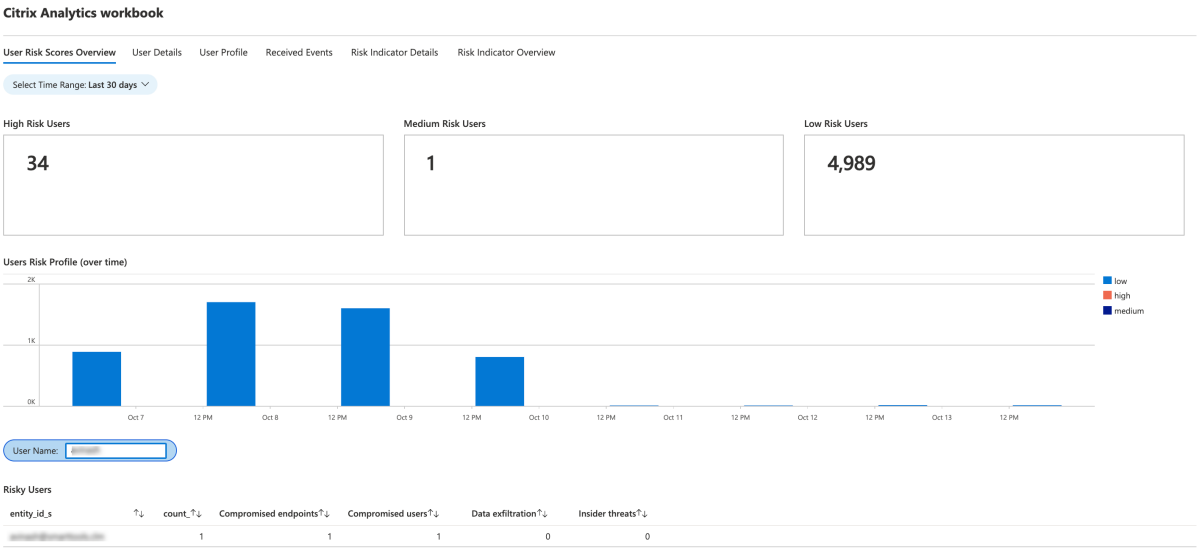
- 用户风险评分概述：提供组织中风险用户的综合视图。
- 用户详细信息：提供用户及其危险行为的详细信息。
- 用户配置文件：提供与用户关联的事件量度。
- 收到的事件：提供从 Citrix Analytics for Security 收到的事件。
- 风险指示器详细信息：提供有关用户触发的内置和自定义风险指示器的详细信息。
- 风险指标概述：提供用户触发的风险指标的综合视图。



用户风险评分概述

此控制板提供了组织中存在风险的用户的综合视图。用户按风险级别进行分类-高、中和低。风险级别基于用户事件中的异常情况，因此会分配风险评分。有关风险用户类型的更多信息，请参阅用 户控制板。

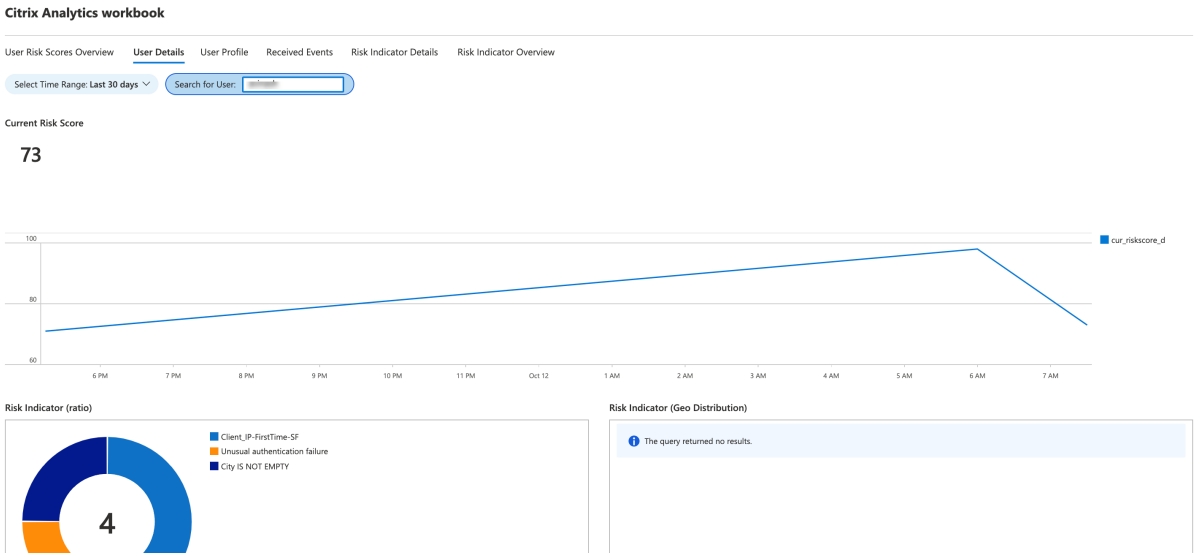
选择时间段来查看组织中的风险用户。



用户详情

此控制板提供与用户关联的风险评分和风险指示器。

搜索用户并查看他们可能对您的组织构成威胁的危险活动。要缓解威胁，您可以根据用户帐户的风险严重程度对其采取适当的措施。



用户资料

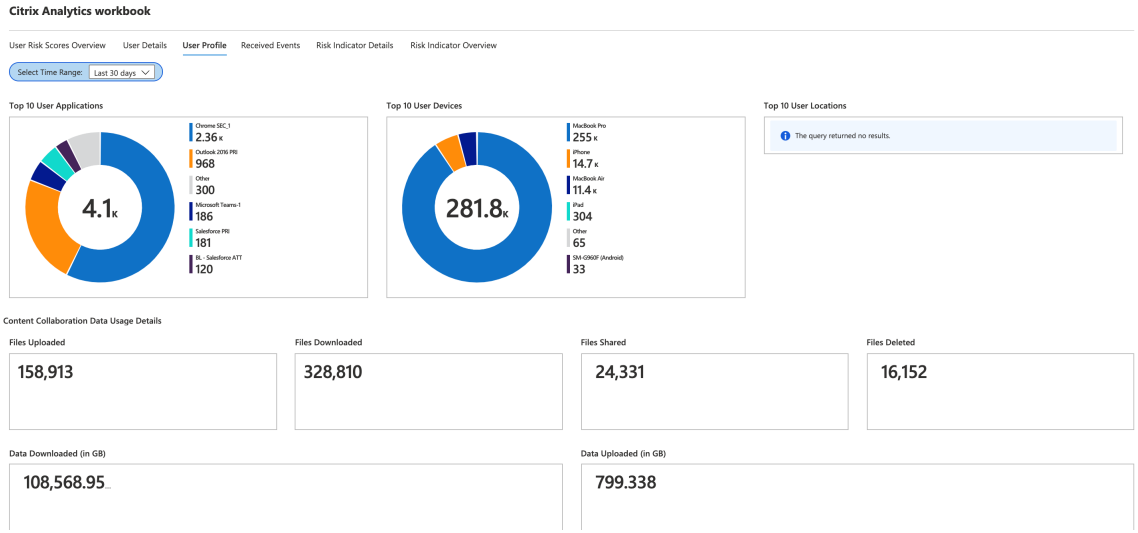
此控制面板提供在选定时间段内与用户关联的事件指标的详细信息。这些指标提供了对用户活动的见解，例如：

- 用户使用的前 10 个应用程序
- 用户使用的十大设备

- 用户登录的前 10 个位置

使用这些报告，您可以：

- 确定用户的使用趋势
- 发现用于访问资源的不合规设备
- 检查您的用户是否有任何潜在的危险访问

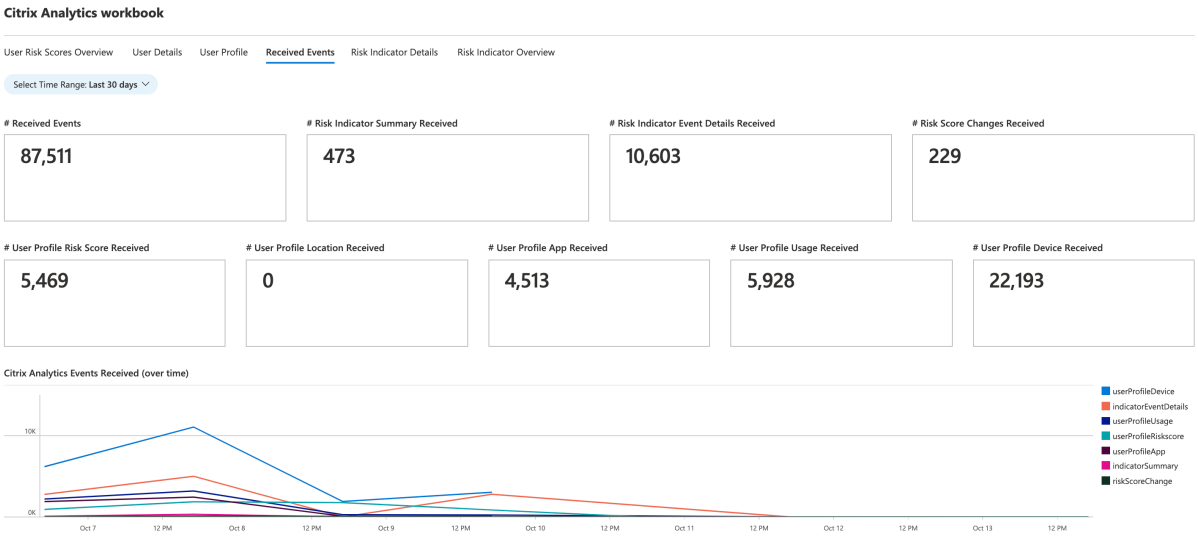


收到的事件

在选定的时间段内，您可以查看从 Citrix Analytics for Security 接收的事件总数。收到的事件总数包括以下各项：

- 风险指示器摘要：指示与用户风险指标摘要关联的事件。有关各种风险指示器摘要事件的信息，请参阅 风险指示器架构。
- 风险指示器事件详细信息：指示与用户风险指示器详细信息相关的事件。有关各种风险指示器详细信息事件的信息，请参阅 风险指示器架构。
- 用户配置文件风险评分：指示与用户风险评分相关的事件。有关信息，请参阅“用户”控制板。
- 风险评分变化：指示与用户风险评分变化相关的事件。有关信息，请参阅“用户”控制板。
- 用户配置文件位置：指示与用户登录的位置相关联的事件。
- 用户配置文件应用程序：指示与用户使用的应用程序关联的事件。
- 用户配置文件使用情况：指示与用户的数据使用相关的事件。
- 用户配置文件 device：指示与用户使用的设备关联的事件。

通过定期查看控制板，您可以确保事件是否正确地流向您的 Microsoft Sentinel 工作区。收到的事件总数中的任何差异都可能表示与 Citrix Analytics for Security 的集成存在问题。您可以执行必要的步骤来调试问题。

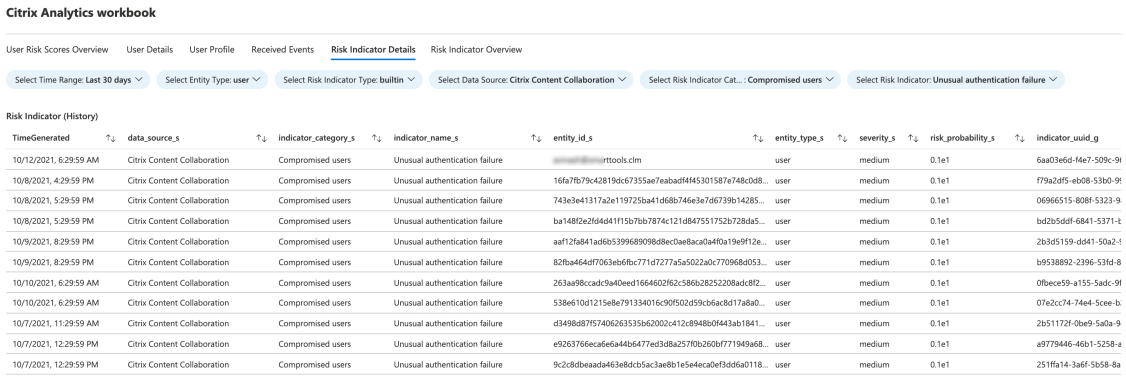


风险指标详情

此控制板提供用户触发的风险指示器的详细信息。

您可以通过选择一个或多个类别来查看风险指示器详细信息：

- 时间范围：选择时间范围以查看该期间触发的风险指标的详细信息。
- 实体类型：选择一个用户来查看相关风险指标的详细信息。
- 风险指示器类型：选择 内置 或 自定义 风险指示器以查看其详细信息。
- 数据源：选择 数据源 以查看关联的风险指示器。
- 风险指示器类别：选择 风险类别 以查看关联的风险指示器。
- 风险指示器：按名称选择风险指示器并查看其详细信息。

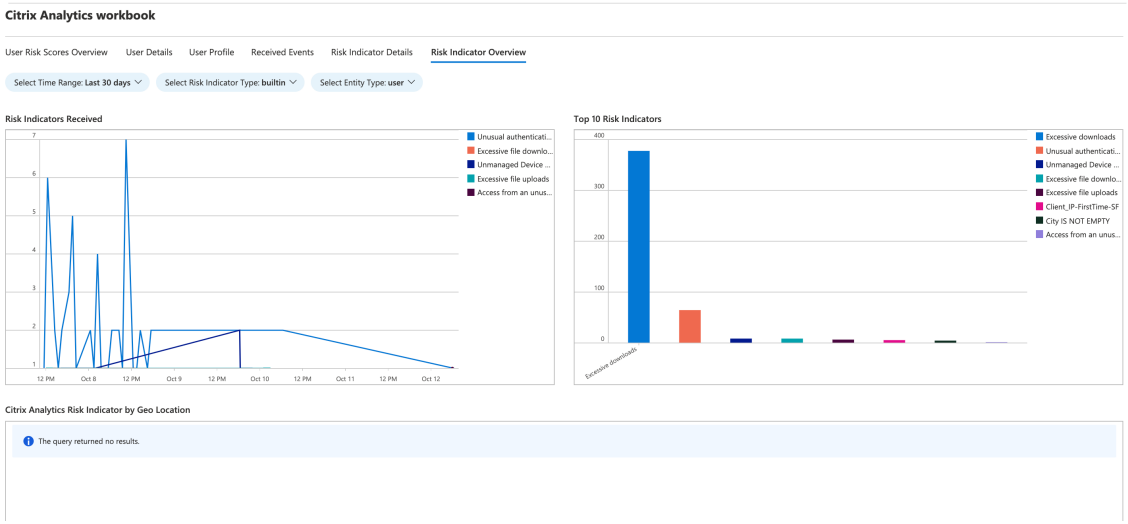


风险指标概述

此控制板提供用户触发的所有风险指示器的综合视图。

您可以通过选择一个或多个类别来查看风险指示器：

- 时间范围：选择一个时间段以查看在该时段内触发的风险指示器。
- 风险指示器类型：选择 内置 或 自定义 以查看关联的风险指示器。
- 实体类型：选择任一用户以查看相关的风险指标。



通过 **Logstash** 集成 **Sentinel** 的故障排除指南

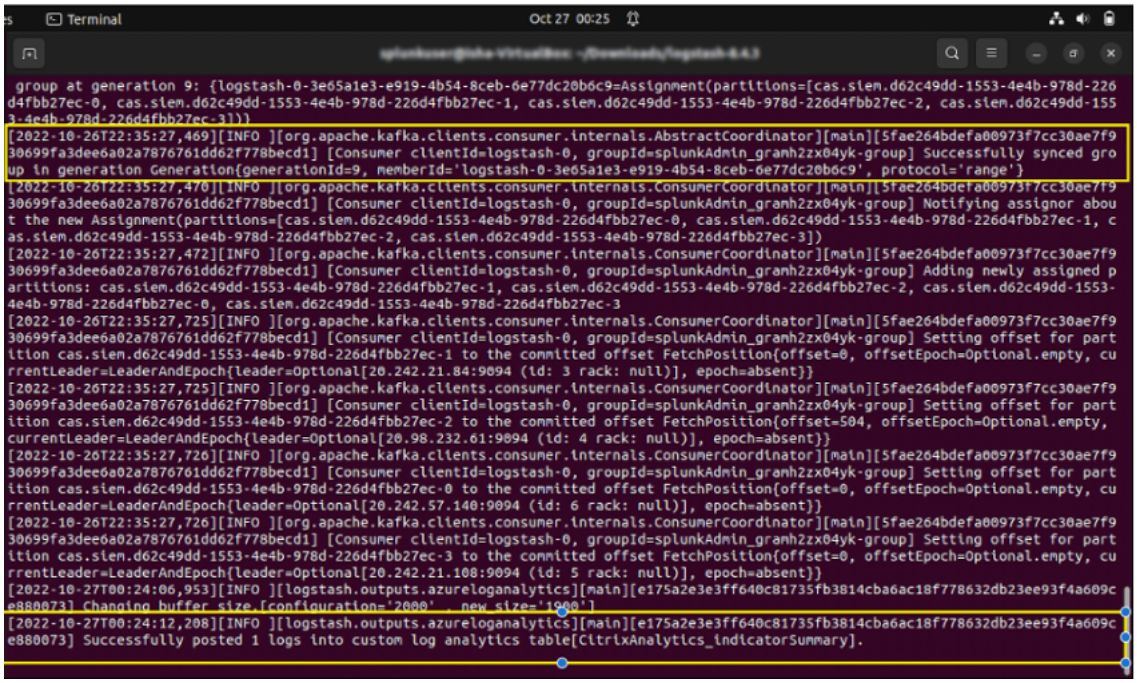
May 8, 2023

本文列出了一些注意事项，以解决您在使用 Logstash 将 Microsoft Sentinel 与 Citrix Analytics 集成时可能遇到的问题。要了解更多相关信息，请参阅 使用基于 Kafka 或基于 Logstash 的数据连接器进行 SIEM 集成。

查看 **Logstash** 服务器日志

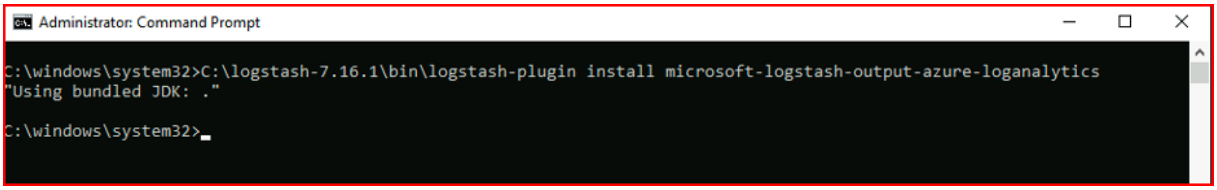
您可以检查终端窗口上显示的 Logstash 服务器日志，以验证数据是否已正确导入到 Sentinel 工作区的自定义日志表中。

1. 要查看日志详细信息，必须从“设置” **>** “数据导出” **>** “配置”选项卡 ** 展开 **SIEM** 环境中下载 Logstash 配置文件。在 Azure Sentinel（预览版）下，单击“下载 Logst**ash 配置文件”。
2. 使用配置文件启动 Logstash 服务器后，您可以在同一个终端窗口中查看以下日志，这些日志表明已成功连接到 Microsoft Azure 托管的日志分析工作区。

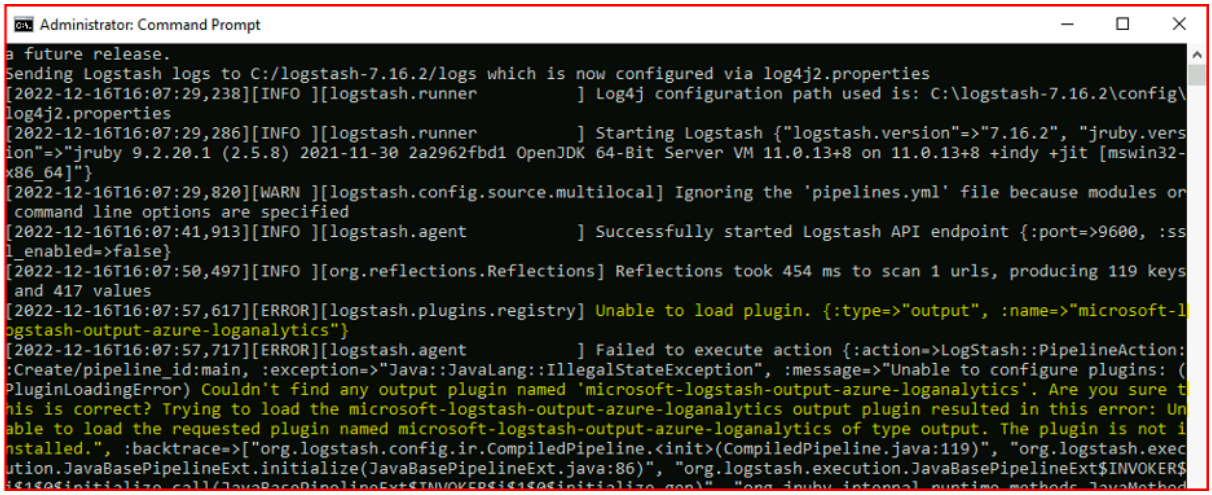


常见错误：使用捆绑的 **JDK**

尝试安装 Microsoft 日志分析插件时，报告的常见错误如下所示：



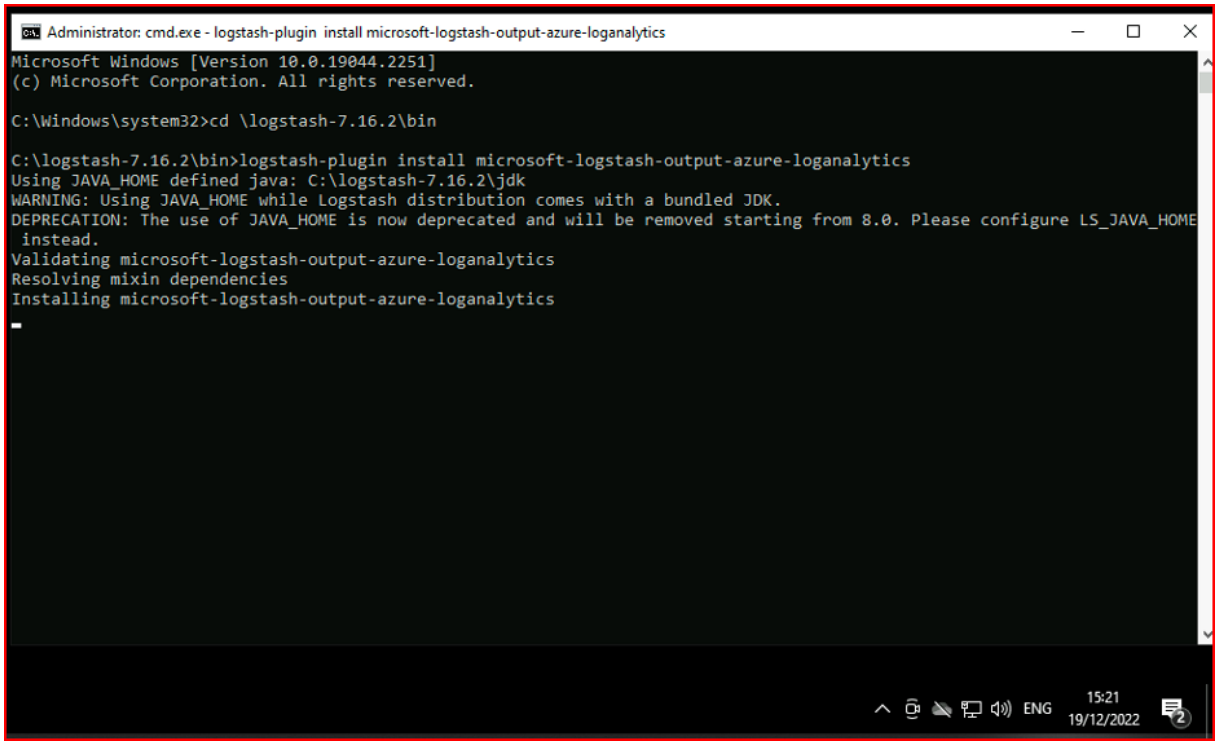
之后，在尝试运行 Logstash 服务器时，您可能会看到以下错误：



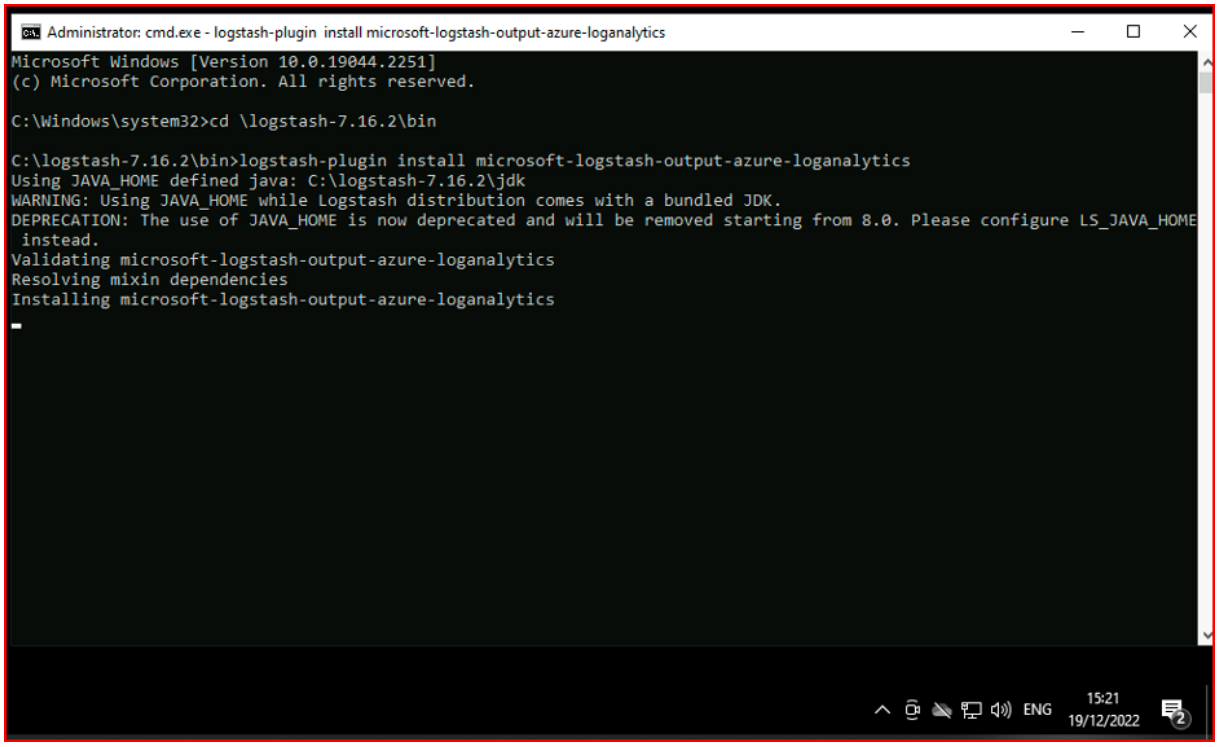
要解决此问题，请将 JAVA_HOME 设置为捆绑的 JDK：

1. 转到 Windows 环境变量
2. 创建一个名为“JAVA_HOME”的新系统变量
3. < path_to_logstash > 添加捆绑的 Logstash JDK 的路径 /logstash-x.x.x/JDK)

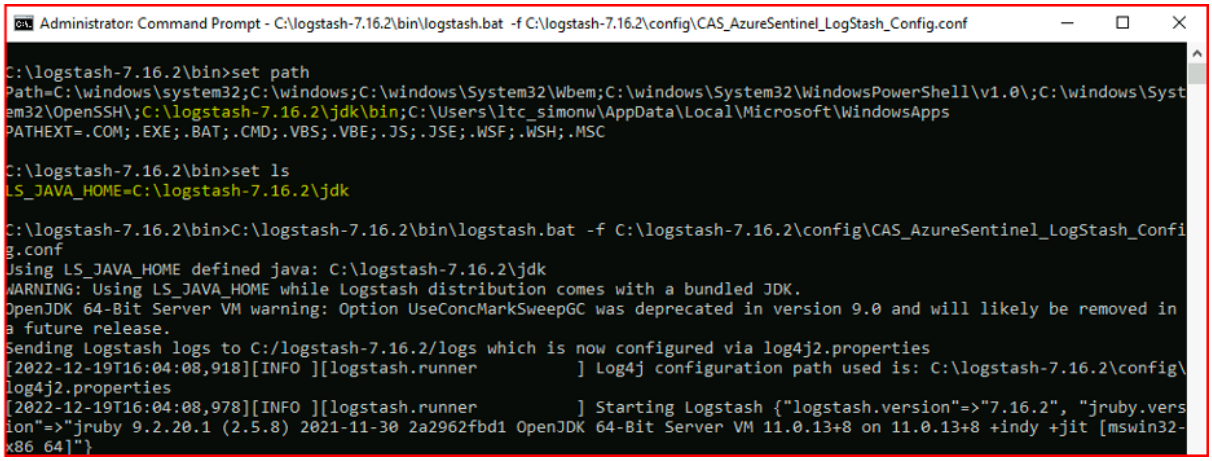
完成上述步骤后，尝试再次安装插件时，会出现以下屏幕：



如果您使用 LS_JAVA_HOME（不推荐使用 JAVA_HOME），则还必须在系统 PATH 变量中指定捆绑的 JDK 的位置，并且此路径必须指向 jdk\ bin 文件夹（与 LS_ **J** AVA_HOME 变量不同）：



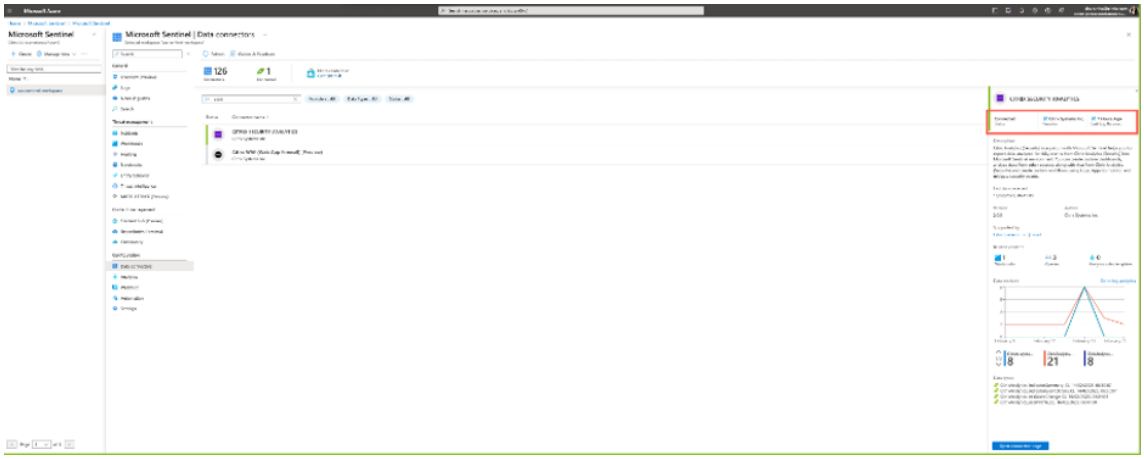
如果您使用 LS_JAVA_HOME（不推荐使用 JAVA_HOME），则还必须在系统 PATH 变量中指定捆绑的 JDK 的位置，并且此路径必须指向 jdk\ bin 文件夹（与 LS_ **J** AVA_HOME 变量不同）：



查看微软 **Sentinel** 工作簿

要确认 Citrix Analytics 发送的数据是否已成功输入到日志分析工作区的相应自定义日志表中（要了解有关 Microsoft Sentinel 与 Citrix Analytics 集成的更多信息，请参阅微软 Sentinel 集成）：

1. 导航到 Azure 门户 > 微软 Sentinel > 选择 approte_workspace > 数据连接器 ** 选择并单击 Citrix 安全分析。**
2. 检查顶栏以验证连接状态。

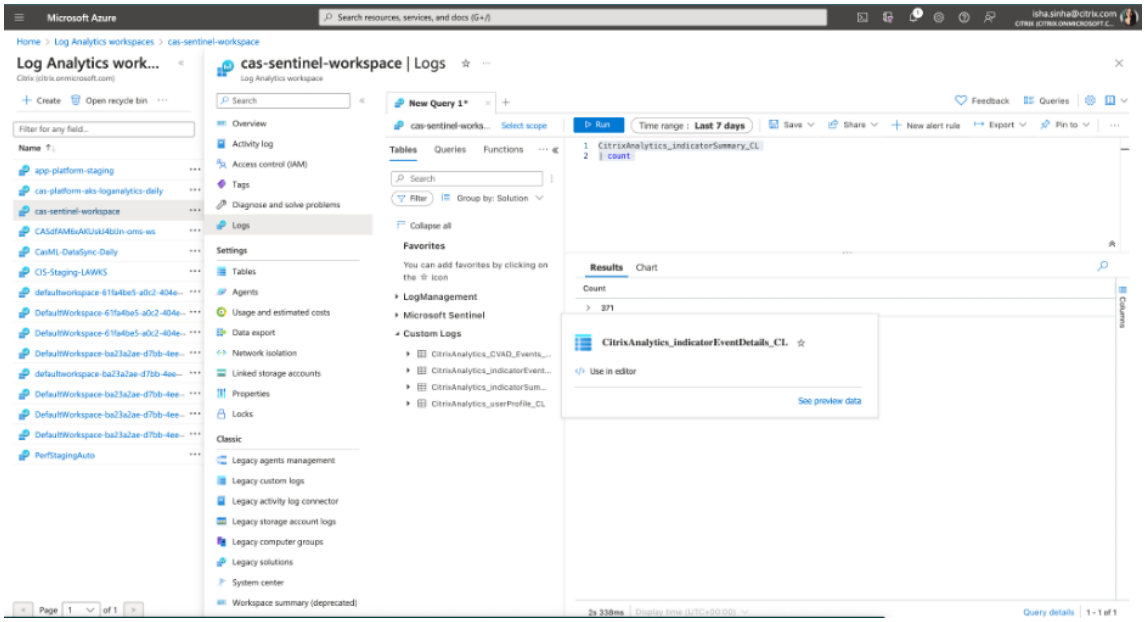


3. 在工作簿下，您可以使用直观的筛选器进一步深入分析数据以获取风险指标信息。要获取信息，请导航到 **Azure** 门户 **>** 微软 **Sentinel >** 数据连接器 **> CITRIX** 安全分析工作簿。

使用 **KQL** 查看日志分析工作区日志

您还可以通过对相应的自定义日志表运行 KQL 查询，检查是否有正确的数据进入了 LogAnalytics 工作空间。

1. 导航到 **Azure** 门户 **>** 日志分析工作 区，然后搜索正确的工作空间。
2. 在左侧面板下，选择 日志，然后在表格选项卡下搜索自定义日志分析 表。
3. 选择自定义日志分析表，然后单击“在编辑器中使用”。（有关日志分析工作区上的 KQL 查询的指导，请参阅 日志分析教程）。
4. 单击运行。



Elasticsearch 集成

November 26, 2023

> 注意
>
> 如需帮助 Elasticsearch 集成、将数据导出到 Elasticsearch 或提供反馈，请联系 CAS-PM-Ext@cloud.com。

通过使用 Logstash 引擎将 Citrix Analytics for Security 与 Elasticsearch 集成在一起。通过此集成，您可以将 Citrix IT 环境中的用户数据导出并将其关联到 Elasticsearch，从而更深入地了解组织的安全状况。您还可以将 Elasticsearch 与可视化服务和 SIEM（例如 Kibana 和 LogRhythm）分别结合使用。

有关集成的好处以及发送到 SIEM 的已处理数据类型的更多信息，请参阅 安全信息和事件管理集成。

必备条件

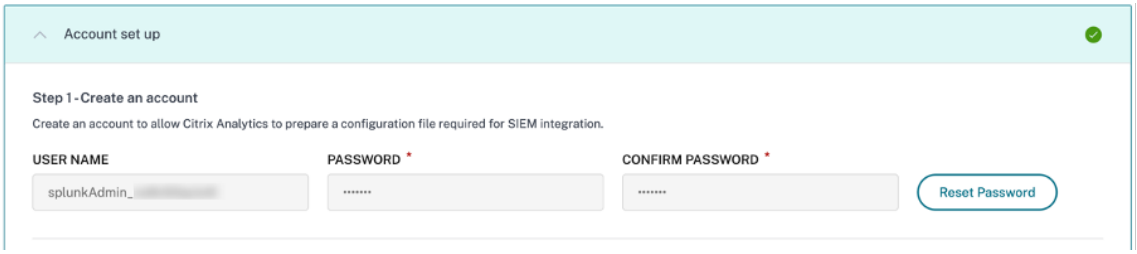
- 为至少一个数据源启用数据处理。它可以帮助 Citrix Analytics for Security 开始 Elasticsearch 集成过程。
- 确保以下终端节点位于网络的允许列表中。

端点	美国地区	欧盟区域	亚太南部地区
Kafka 代理	`casnb-0.citrix.com:9094`	`casnb-eu-0.citrix.com:9094`	`casnb-aps-0.citrix.com:9094`

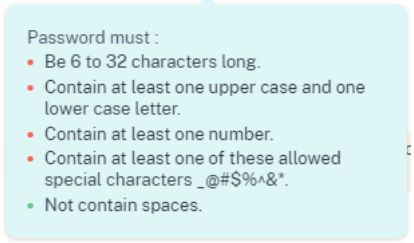
端点	美国地区	欧盟区域	亚太南部地区
	casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

与 **Elasticsearch** 集成

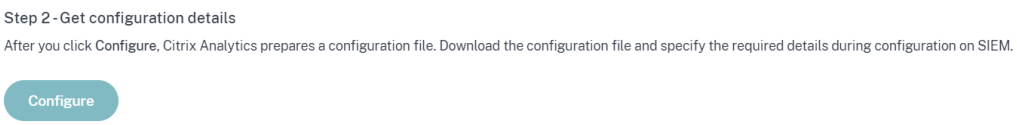
1. 前往“设置”**>**“数据导出”。
2. 在“帐户设置”部分，通过指定用户名和密码来创建帐户。此帐户用于准备集成所需的配置文件。



3. 确保密码满足以下条件：



4. 单击 配置 以生成 Logstash 配置文件。

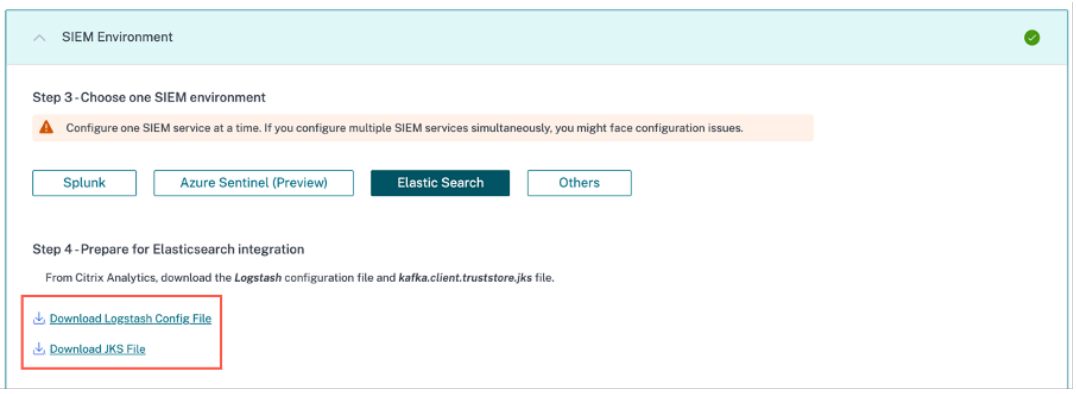


5. 从“SIEM 环境”部分选择弹性搜索选项卡以下载配置文件：

   - **Logstash** 配置文件：包含用于使用 Logstash 数据收集引擎将事件从 Citrix Analytics 安全版发送到 Elasticsearch 的配置数据（输入、筛选和输出部分）。有关 Logstash 配置文件结构的信息，请参阅 Logstash 文档。

- **JKS** 文件：包含 SSL 连接所需的证书。

> 注意
>
> 这些文件包含敏感信息。将它们存放在安全可靠的地方。



6. 配置 Logstash：

   a) 在您的 Linux 或 Windows 主机上，安装 Logstash。您也可以使用现有的 Logstash 实例。

   b) 在安装了 Logstash 的主机上，将以下文件放在指定的目录中：

主机类型	文件名	目录路径
Linux	CAS_Elasticsearch_LogStash_Config.conf	对于 Debian 和 RPM 软件包：`/etc/logstash/conf.d/` 对于.zip 和.tar.gz 存档：`{ extract.path } /config`
	kafka.client.truststore.jks	对于 Debian 和 RPM 软件包：`/etc/logstash/ssl/` 对于.zip 和.tar.gz 存档：`{ extract.path } /ssl`
Windows	CAS_Elasticsearch_LogStash_Config.conf	`C:\Logstash-7.xx.x\config`
	kafka.client.truststore.jks	

   有关 Logstash 安装包的默认目录结构的信息，请参阅 Logstash 文档。

   c) 打开 Logstash 配置文件并执行以下操作：

      i. 在文件的输入部分，输入以下信息：

- 密码：您在 Citrix Analytics for Security 中创建的用于准备配置文件的帐户的密码。
- **SSL** 信任存储位置：SSL 客户端证书的位置。这是主机中 kafka.client.truststore.jks 文件的位置。

```
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"
  }
}
```

ii. 在文件的输出部分，输入运行 Elasticsearch 的主机或群集的地址。

```
}
output {
  elasticsearch {
    hosts => ["<your logstash host : port>"]
    index => "citrixanalytics-%{+YYYY.MM.dd}"
  }
}
```

d) 重新启动主机，将 Citrix Analytics for Security 中的已处理数据发送到 Elasticsearch。

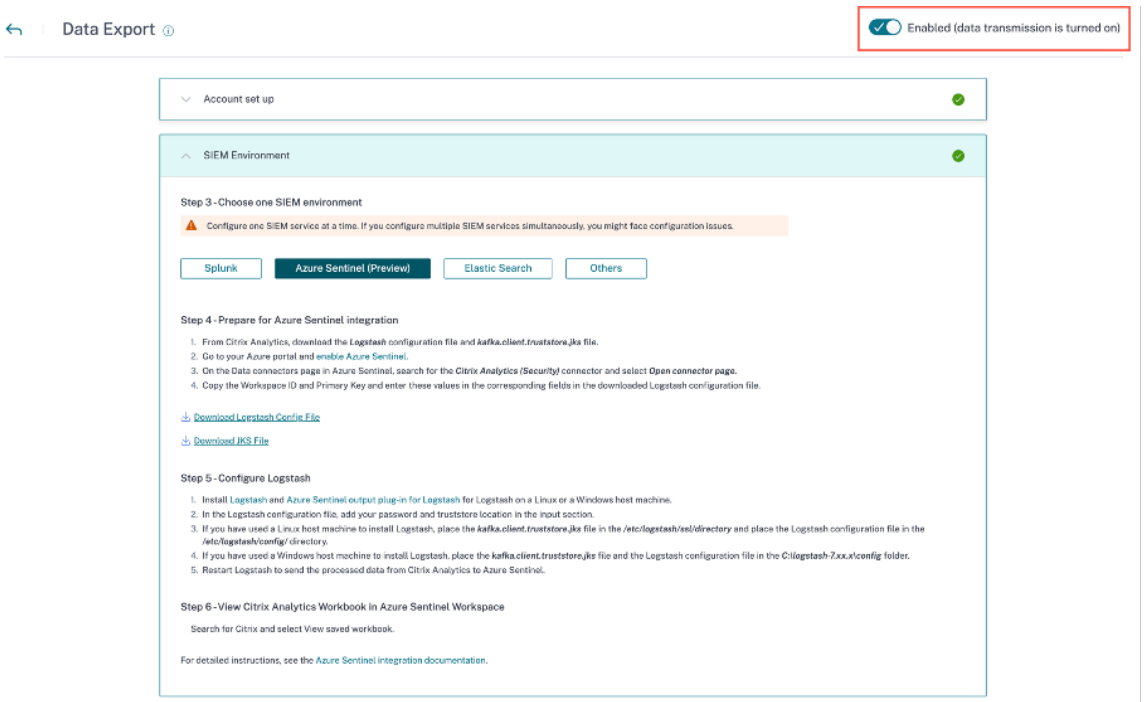
配置完成后，确认您可以在 Elasticsearch 中查看 Citrix Analytics 数据。

打开或关闭数据传输

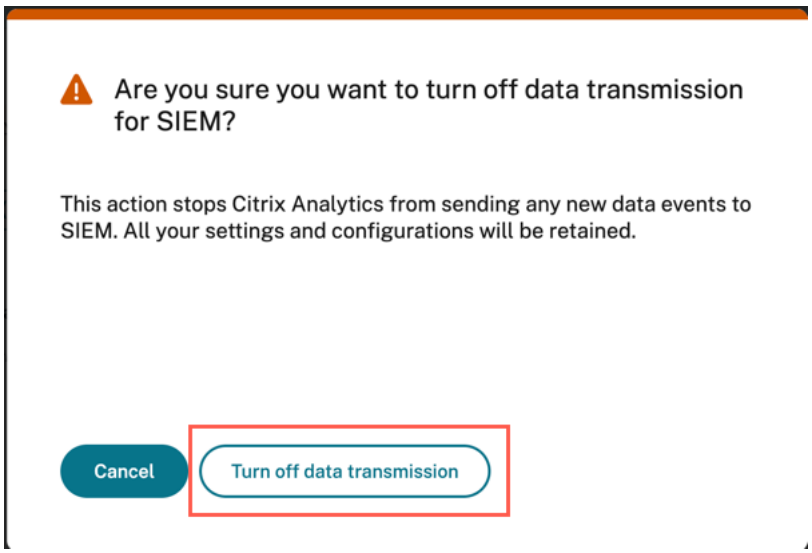
Citrix Analytics for Security 准备配置文件后，将为 Elasticsearch 开启数据传输。

要停止从 Citrix Analytics for Security 传输数据，请执行以下操作：

1. 前往“设置”**>**“数据导出”。
2. 关闭切换按钮以禁用数据传输。默认情况下，数据传输始终处于启用状态。



此时会出现一个警告窗口供您确认。单击“关闭数据传输”按钮以停止传输活动。



要再次启用数据传输，请打开切换按钮。

使用基于 **Kafka** 或 **Logstash** 的数据连接器进行 **SIEM** 集成

November 26, 2023

Citrix Analytics for Security SIEM 集成使您能够将用户的数据从 Citrix Analytics 导出并关联到 SIEM 环境，从而

更深入地了解组织的安全状况。

有关集成的好处以及发送到您的 SIEM 的数据事件类型（风险洞察和数据源事件）的更多信息，请参阅安全信息和事件管理集成。

您可以通过以下两种机制（由您的 SIEM 和 IT 部署支持）将 Citrix Analytics for Security 与 SIEM 解决方案集成：

1. 通过 Kafka 端点进行连接
2. 通过 Logstash 数据代理使用基于 Kafka 的采集功能进行连接

必备条件

- 为至少一个数据源启用数据处理。它可以帮助 Citrix Analytics for Security 开始与 SIEM 工具的集成。
- 确保以下终端节点位于网络的允许列表中。

端点	美国地区	欧盟区域	亚太南部地区
Kafka 代理	casnb-0.citrix.com:9094 casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-0.citrix.com:9094 casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-0.citrix.com:9094 casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

使用 **Kafka** 与 **SIEM** 服务集成

Kafka 是一款开源软件，用于实时传输数据。使用 Kafka，您可以分析实时数据以更快地获得见解。大多数情况下，处理足够数据的大型组织使用 Kafka。

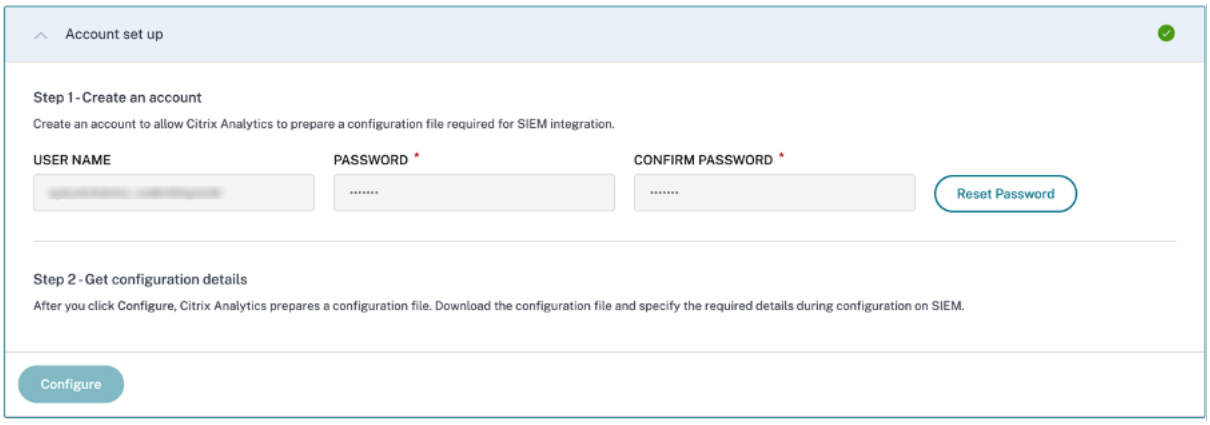
Northbound Kafka 是一个内部中间层，使 Citrix Analytics 能够通过 Kafka 端点与 SIEM 客户共享实时数据源。如果您的 SIEM 支持 Kafka 端点，请使用 Logstash 配置文件中提供的参数以及 JKS 文件或 PEM 文件中的证书详细信息将 SIEM 与 Citrix Analytics for Security 集成。

使用 Kafka 进行集成需要以下参数：

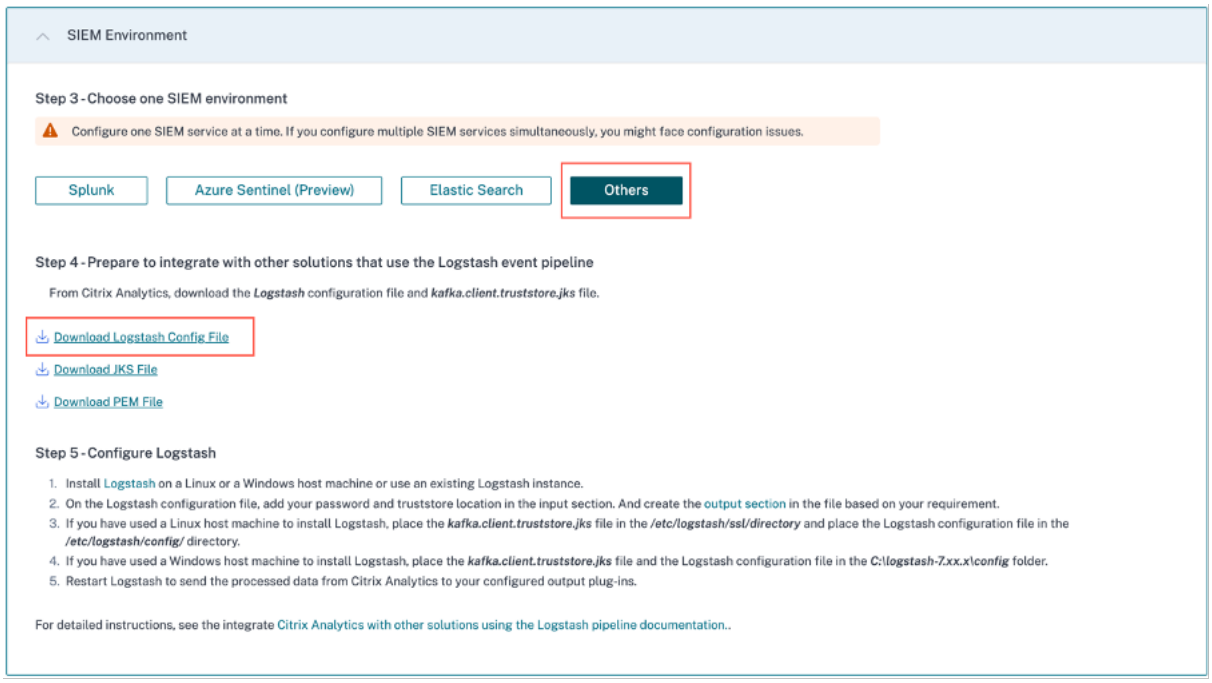
属性名称	说明	配置数据示例
用户名	Kafka 提供的用户名。	`'sasl.username': cas_siem_user_name,`
主机	要连接的 Kafka 服务器的主机名。	`'bootstrap.servers': cas_siem_host,`
主题名称/客户端 ID	分配给每个租户的客户端 ID。	`'client.id': cas_siem_topic,`
组名称/ID	读取消费者共享的消息所需的组名称。	`'group.id': cas_siem_group_id,`
安全协议	安全协议的名称。	`'security.protocol': 'SASL_SSL',`
SASL 机制	通常用于加密以实现安全身份验证的身份验证机制。	`'sasl.mechanisms': 'SCRAM-SHA-256',`
SSL 信任存储位置	可以存储证书文件的位置。客户端信任存储密码是可选的，应留空。	`'ssl.ca.location': ca_location`
会话超时	会话超时用于在使用 Kafka 时检测客户端故障。	`'session.timeout.ms': 60000,`
自动偏移复位	定义在没有初始偏移量时使用来自主题分区的数据时的行为。您可以设置值，例如最新、最早或无。	`'auto.offset.reset': 'earliest',`

以下是示例配置输出：

```
{
 'bootstrap.servers': cas_siem_host,
                      'client.id': cas_siem_topic,
                      'group.id': cas_siem_group_id,
                      'session.timeout.ms': 60000,
                      'auto.offset.reset': 'earliest',
                      'security.protocol': 'SASL_SSL',
                      'sasl.mechanisms': 'SCRAM-SHA-256',
                      'sasl.username': cas_siem_user_name,
                      'sasl.password': self.CLEAR_PASSWORD,
                      'ssl.ca.location': ca_location
              }


<!--NeedCopy-->
```

上述参数在 Logstash 配置文件中可用。要下载配置文件，请导航到“设置”**>**“数据导出”**>**“**SIEM** 环境”选择“其他”选项卡 > 单击“下载 **Logstash** 配置文件”。



要了解/了解有关配置值的更多信息，请参阅配置。

数据流

身份验证数据通信发生在 Kafka 服务器端代理（Citrix Analytics for Security 云）和 Kafka 客户端之间。所有代理/外部客户端的通信都使用启用的 SASL_SSL 安全协议和目标 9094 端口进行公共访问。

Apache Kafka 有一个安全组件，可以使用 SSL 加密对飞行中的数据进行加密。
启用加密并设置 SSL 证书后，网络上的数据传输将得到加密和保护。只有第一台和最后一台计算机具有解密通过 SSL 发送的数据包的能力。

身份验证

有两个级别的身份验证可用，如下所示：

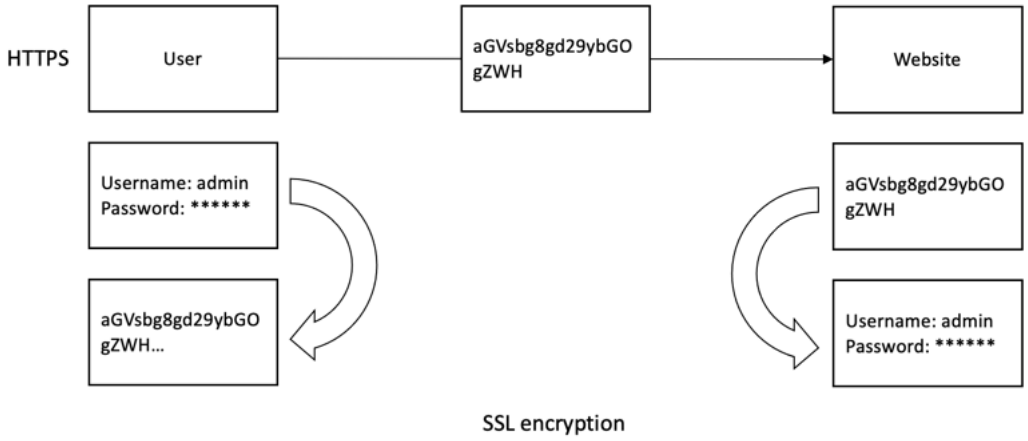
1. TLS/在客户端和服务器之间。
    - 用于在客户端和服务器之间交换 TLS 身份验证的服务器证书（公钥）。
    - 不支持基于客户端的身份验证或双向身份验证（需要客户端私钥证书）。
2. 用于控制主题/端点访问的用户名/密码
    - 确保特定客户只能从特定客户主题中读取
    - SASL/SCRAM 用于用户名/密码身份验证机制以及 TLS 加密，以实现安全身份验证。

使用 **SSL** 加密和使用 **SASL/SSL&SASL/PLAINTEXT** 进行身份验证

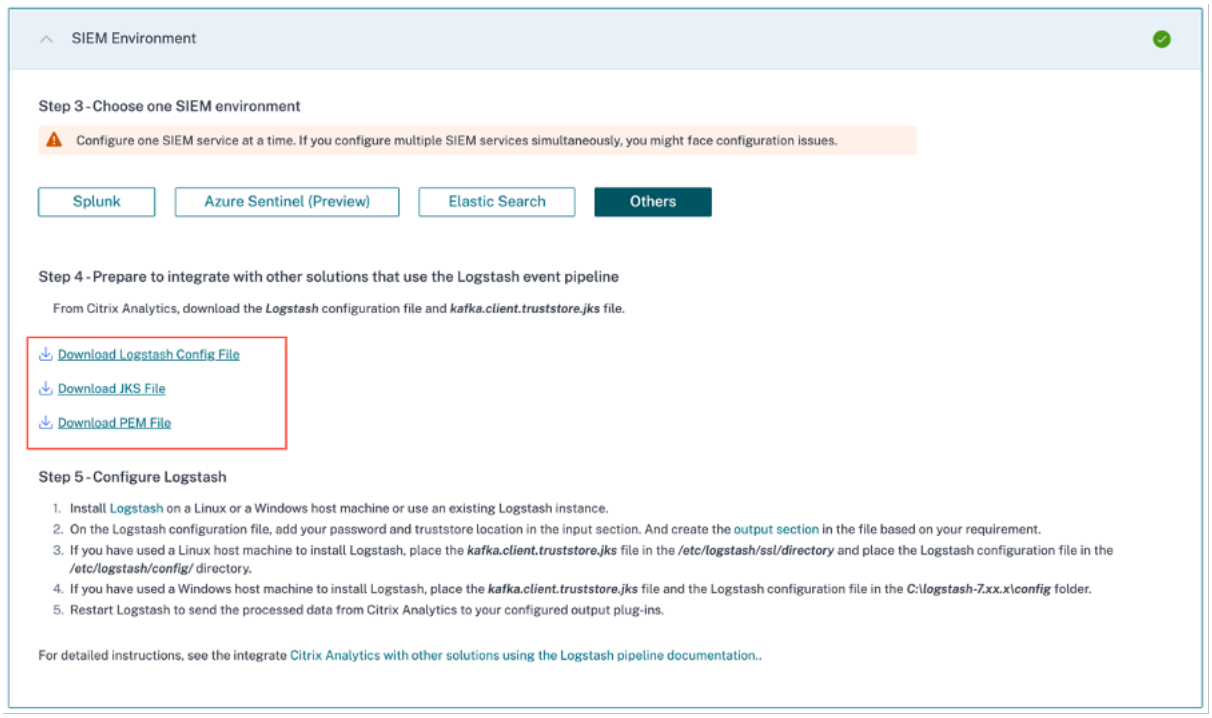
默认情况下，Apache Kafka 以纯文本方式进行通信，其中所有数据均以明文发送，任何路由器都可以读取数据内容。Apache Kafka 有一个安全组件，可以使用 SSL 加密对飞行中的数据进行加密。启用加密并仔细设置 SSL 证书后，数据现在已加密并通过网络安全传输。使用 SSL 加密，只有第一台和最后一台计算机具有解密发送的数据包的能力。

由于使用双向 SSL 加密，因此用户名/密码登录对于外部通信是安全的。

加密仅在进行中，数据仍未加密在代理的磁盘上。



在客户端配置中，需要客户端信任存储 JKS 文件和 PEM 文件（从信任存储 jks 文件转换）。您可以从 Citrix Analytics for Security GUI 下载这些文件，如以下屏幕截图所示：



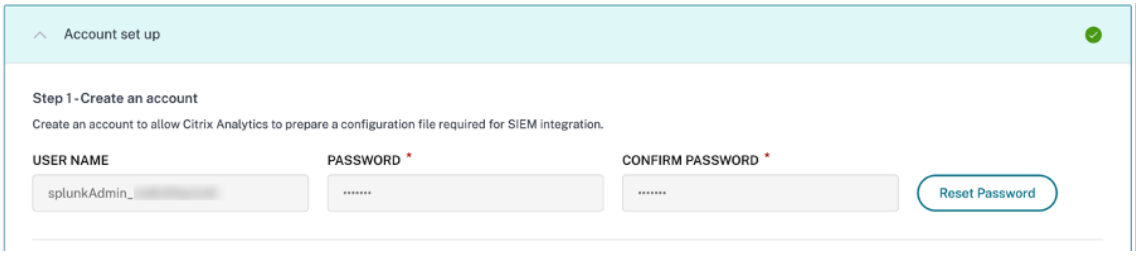
使用 **Logstash** 集成 **SIEM**

如果您的 SIEM 不支持 Kafka 端点，可以使用 **Logstash** 数据收集引擎。您可以将数据事件从 Citrix Analytics for Security 发送到 Logstash 支持的输出插件之一。

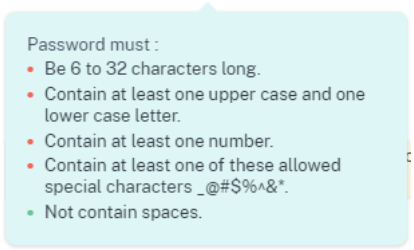
以下部分介绍了使用 Logstash 将 SIEM 与 Citrix Analytics for Security 集成时必须遵循的步骤。

使用 **Logstash** 与 **SIEM** 服务集成

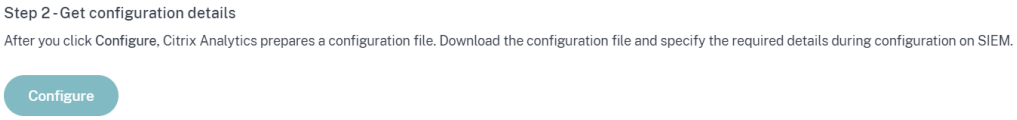
1. 前往“设置”**>**“数据导出”。
2. 在“帐户设置”页面上，通过指定用户名和密码来创建帐户。此帐户用于准备集成所需的配置文件。



3. 确保密码满足以下条件：



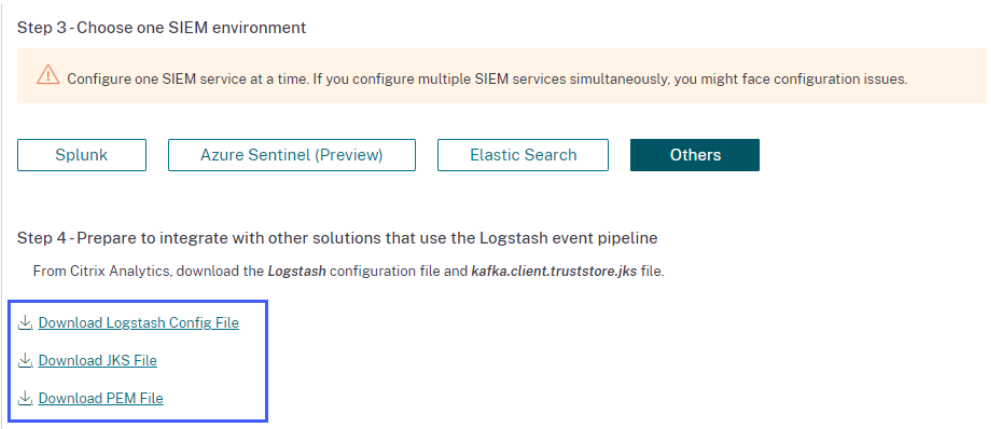
4. 选择 配置 以生成 Logstash 配置文件。



5. 选择“其他”选项卡以下载配置文件。

   - **Logstash** 配置文件：此文件包含用于使用 Logstash 数据收集引擎从 Citrix Analytics for Security 发送事件的配置数据（输入、筛选器和输出部分）。有关 Logstash 配置文件结构的信息，请参阅 Logstash 文档。
   - **JKS** 文件：此文件包含 SSL 连接所需的证书。使用 Logstash 集成您的 SIEM 时，这个文件是必需的。
   - **PEM** 文件：此文件包含 SSL 连接所需的证书。使用 Kafka 集成 SIEM 时需要此文件。

     > 注意
     >
     > 这些文件包含敏感信息。将它们存放在安全可靠的地方。



6. 配置 Logstash：

   a) 在您的 Linux 或 Windows 主机上，安装 Logstash （与 Citrix Analytics for Security 兼容性的测试版本：v7.17.7 和 v8.5.3）。您也可以使用现有的 Logstash 实例。

   b) 在安装了 Logstash 的主机上，将以下文件放在指定的目录中：

主机类型	文件名	目录路径
Linux	CAS_Others_LogStash_Config.config	对于 Debian 和 RPM 软件包： /etc/logstash/conf.d/ 对于.zip 和.tar.gz 存档： { extract.path } /config
	kafka.client.truststore.jks	对于 Debian 和 RPM 软件包： /etc/logstash/ssl/ 对于.zip 和.tar.gz 存档： { extract.path } /ssl
Windows	CAS_Others_LogStash_Config.config	C:\logstash-7.xx.x\config
	kafka.client.truststore.jks	C:\logstash-7.xx.x\config

c) Logstash 配置文件包含敏感信息，例如 Kafka 凭据、LogAnalytics Workspace ID、主密钥。建议不要将这些敏感凭据存储为纯文本。为了确保集成，可以使用 Logstash 密钥库来添加带有相应值的密钥，这些密钥又可以在配置文件中使用密钥名称进行引用。有关 Logstash 密钥库及其如何增强设置安全性的更多信息，请参阅安全设置的 Secr ets 密钥库。

d) 打开 Logstash 配置文件并执行以下操作：

在文件的输入部分，输入以下信息：

- 密码：您在 Citrix Analytics for Security 中创建的用于准备配置文件的帐户的密码。
- **SSL** 信任存储位置：SSL 客户端证书的位置。这是主机中 kafka.client.truststore.jks 文件的位置。

```
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"
  }
}
```

在文件的输出部分，输入要将数据发送到的目标路径或详细信息。有关输出插件的信息，请参阅 Logstash 文档。

以下代码段显示输出已写入本地日志文件。


```
output {
        file {
        path => "./citrixanalytics-%{+YYYY.MM.dd}.log"
    }
}
```

e) 重新启动主机，将 Citrix Analytics for Security 处理后的数据发送到 SIEM 服务。

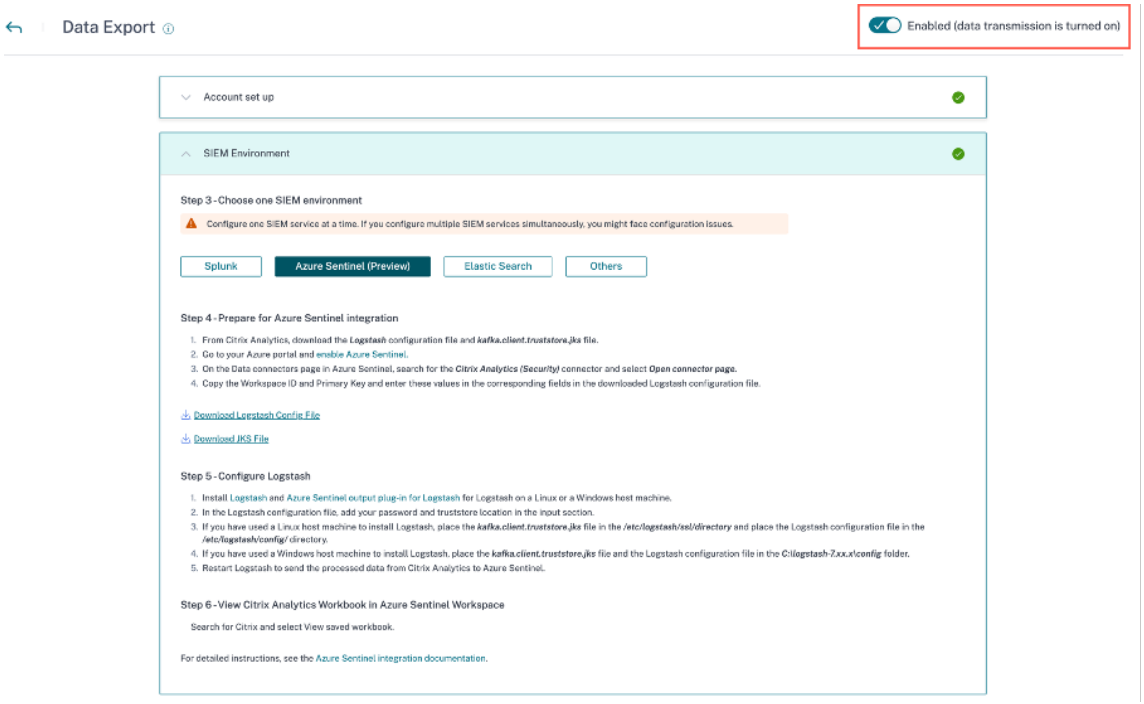
配置完成后，登录 SIEM 服务并验证 SIEM 中的 Citrix Analytics 数据。

打开或关闭数据传输

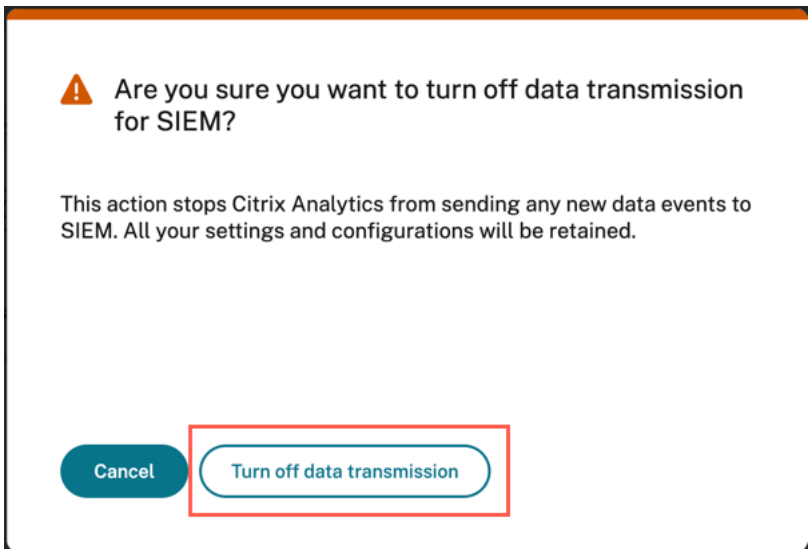
Citrix Analytics for Security 准备配置文件后，将为您的 SIEM 启用数据传输。

要停止从 Citrix Analytics for Security 传输数据，请执行以下操作：

1. 前往“设置” > “数据导出”。
2. 关闭切换按钮以禁用数据传输。默认情况下，数据传输始终处于启用状态。



此时会出现一个警告窗口供您确认。单击“关闭数据传输”按钮以停止传输活动。



要再次启用数据传输，请打开切换按钮。

> 注意
>
> 请联系 CAS-PM-Ext@cloud.com 以请求有关您的 SIEM 集成、将数据导出到 SIEM 的帮助或提供反馈。

SIEM 的 Citrix Analytics 数据导出格式

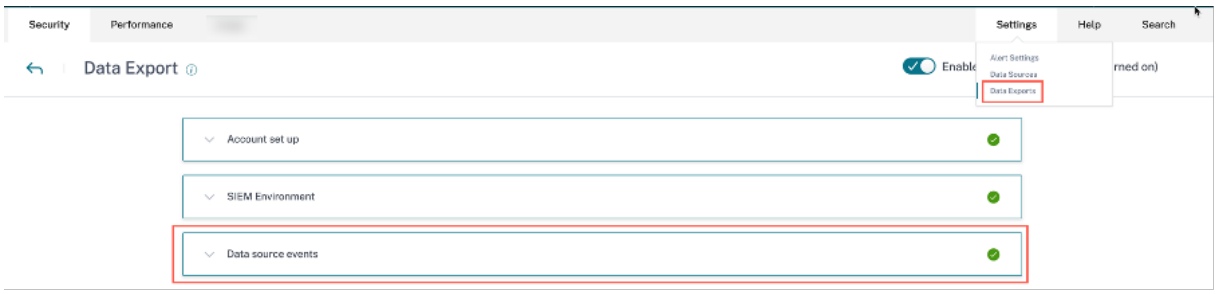
February 14, 2024

Citrix Analytics for Security 允许您与 Security Information and Event Management (SIEM) 服务集成。这种集成使得 Citrix Analytics for Security 能够向您的 SIEM 服务发送数据，并帮助您深入了解组织的安全风险状况。

目前，您可以将 Citrix Analytics for Security 与以下 SIEM 服务集成：

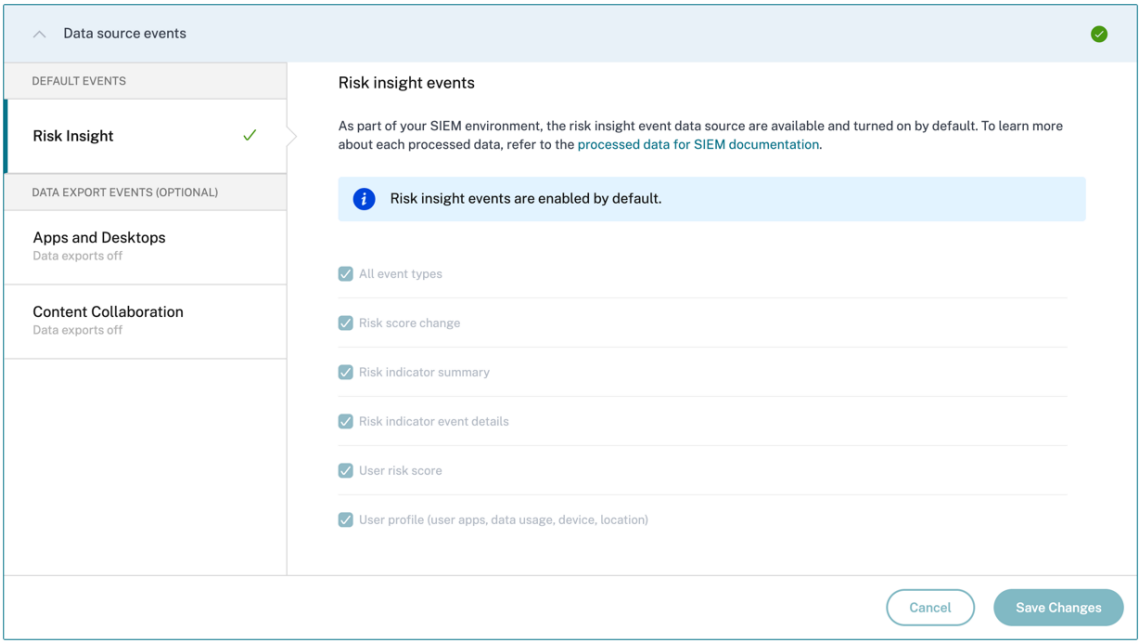
- Splunk
- Microsoft Azure Sentinel
- Elasticsearch
- 其他使用基于 Kafka 或 Logstash 的数据连接器的 SIEM

现在，“设置”下的“数据导出”选项在全球范围内可用。要查看数据源事件，请导航到 设置 **>** 数据导出 **>** 数据源事件。



Citrix Analytics for Security 向您的 SIEM 服务发送的风险洞察数据有两种类型：

- 风险洞察事件（默认导出）
- 数据源事件（可选导出）



SIEM 的风险洞察数据

完成帐户配置和 SIEM 设置后，默认数据集（风险洞察事件）开始流入您的 SIEM 部署。风险洞察数据集包括用户风险评分事件、用户资料事件和风险指标警报。它们由 Citrix Analytics 机器学习算法和用户行为分析通过利用用户事件生成。

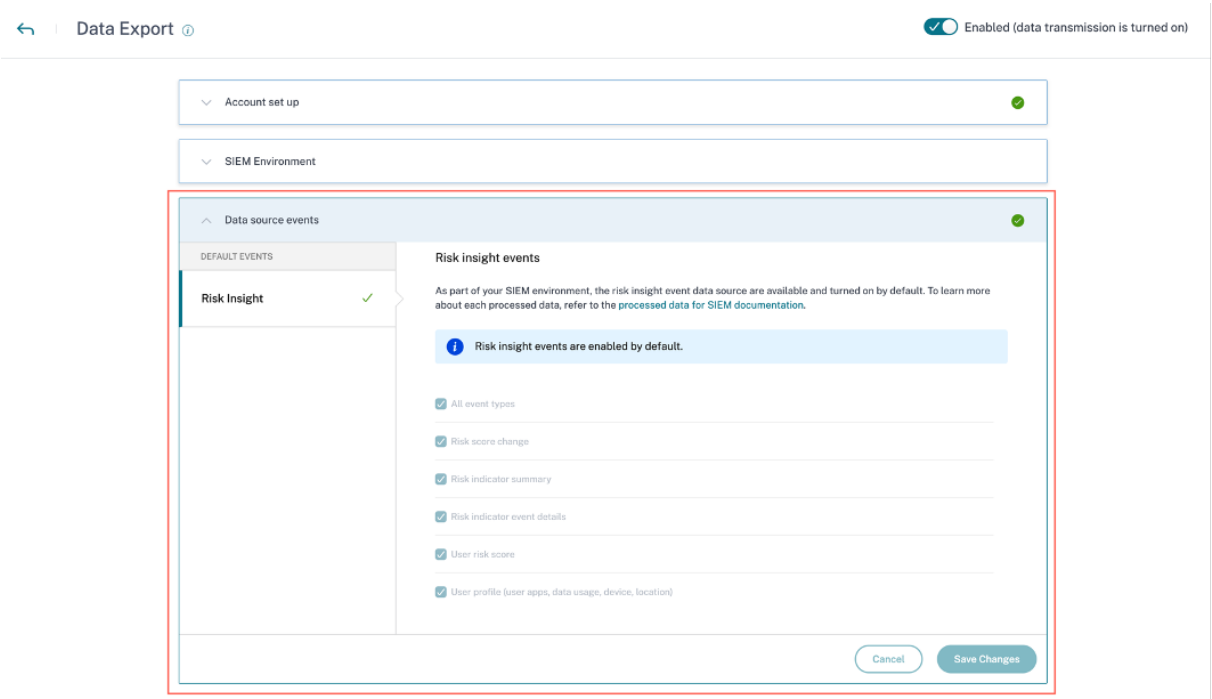
用户的风险洞察数据集包括以下内容：

- 风险评分变化：表示用户风险评分的变化。当用户的风险评分变化等于或大于 3，并且这种变化以任何速度增加或下降超过 10% 时，数据将发送到 SIEM 服务。
- 风险指标摘要：为用户触发的风险指标的详细信息。
- 风险指标事件详细信息：与风险指标相关的用户事件。Citrix Analytics 向 SIEM 服务发送每个风险指标发生情况的最多 1000 个事件详细信息。这些事件按发生的时间顺序发送。

- 用户风险评分事件：用户当前的风险分数。Citrix Analytics for Security 每 12 小时向 SIEM 服务发送一次此数据。
- 用户配置文件：用户配置文件数据可以分为：
  - 用户应用程序：用户启动和使用的应用程序。Citrix Analytics for Security 从 Citrix Virtual Apps 检索这些数据，并每 12 小时将其发送到 SIEM 服务。
  - 用户设备：与用户关联的设备。Citrix Analytics for Security 会从 Citrix Virtual Apps 和 Citrix Endpoint Management 中检索此数据，并每 12 小时将其发送到 SIEM 服务。
  - 用户位置：上次检测到用户所在的城市。Citrix Analytics for Security 从 Citrix Virtual Apps and Desktops 和 Citrix DaaS（前身为 Citrix Virtual Apps and Desktops 服务）检索这些数据。Citrix Analytics for Security 每 12 小时将此信息发送到您的 SIEM 服务。
  - 用户客户端 **IP**：用户设备的客户端 IP 地址。Citrix Analytics for Security 从 Citrix Virtual Apps and Desktops 和 Citrix DaaS（前身为 Citrix Virtual Apps and Desktops 服务）检索这些数据，并每 12 小时将这些信息发送到您的 SIEM 服务。

如果您只能查看但无法配置数据源事件首选项，则您没有必要的管理员权限。
要了解更多信息，请参阅管理 Security Analytics 的管理员角色。

在以下示例中，“保存更改”按钮被禁用。默认情况下，风险洞察事件处于启用状态。



风险洞察事件的架构详情

以下部分介绍 Citrix Analytics for Security 生成的已处理数据的架构。

> 注意
>
> 以下架构示例中显示的字段值仅用于表示目的。实际字段值因用户配置文件、用户事件和风险指标而异。

下表描述了整个架构中所有用户配置文件数据、用户风险评分和风险评分更改的常见字段名称。

字段名称	说明
entity_id	与实体关联的身份。在这种情况下，实体是用户。
entity_type	面临风险的实体。在这种情况下，实体是用户。
event_type	发送到 SIEM 服务的数据类型。例如：用户的位置、用户的数据使用情况或用户的设备访问信息。
tenant_id	客户的独特身份。
timestamp	最近用户事件的日期和时间。
version	已处理数据的模式版本。当前模式版本为 2。

用户配置文件数据架

用户位置模式

```
{

  "tenant_id": "demo_tenant", "entity_id": "demo_user", "entity_type":
     "user", "timestamp": "2021-02-10T15:00:00Z", "event_type": "
     userProfileLocation", "country": "India", "city": "Bengaluru", "
     cnt": 4, "version": 2
   }


<!--NeedCopy-->
```

用户位置的字段描述

字段名称	说明
event_type	发送到 SIEM 服务的数据类型。在这种情况下，事件类型是用户的位置。
country	用户登录的国家/地区。
city	用户登录的城市。
cnt	过去 12 小时内访问该位置的次数。

用户客户端 **IP** 架构

```
{
```



```
 2
 3   "client_ip": "149.147.136.10",
 4   "cnt": 3,
 5   "entity_id": "r2_up_user_1",
 6   "entity_type": "user",
 7   "event_type": "userProfileClientIps",
 8   "tenant_id": "xaxddaily1",
 9   "timestamp": "2023-09-18T10:45:00Z",
10   "version": 2
11  }
12
13
14
15 <!--NeedCopy-->
```

客户端 IP 的字段描述

字段名称	说明
client_ip	用户设备的 IP 地址。
cnt	用户在过去 12 小时内访问设备的次数。
entity_id	与实体关联的身份。在这种情况下，实体是用户。
entity_type	面临风险的实体。在这种情况下，事件类型是用户的客户端 IP。
event_type	发送到 SIEM 服务的数据类型。例如：用户的位置、用户的数据使用情况或用户的设备访问信息。
tenant_id	客户的独特身份。
timestamp	最近用户活动的日期和时间。
version	已处理数据的模式版本。当前模式版本为 2。

用户数据使用模式

```
1 {
2
3   "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
4    }
5
6
7 <!--NeedCopy-->
```

用户数据使用情况的字段描述

字段名称	说明
data_usage_bytes	用户使用的数据量（以字节为单位）。它是用户下载和上载卷的汇总。
deleted_file_cnt	用户删除的文件数。
downloaded_bytes	用户下载的数据量。
downloaded_file_count	用户下载的文件数。
event_type	发送到 SIEM 服务的数据类型。在这种情况下，事件类型是用户的使用情况配置文件。
shared_file_count	用户共享的文件数。
uploaded_bytes	用户上载的数据量。
uploaded_file_cnt	用户上载的文件数。

用户设备模式

```
{

  "cnt": 2, "device": "user1612978536 (Windows)", "entity_id": "demo",
     "entity_type": "user", "event_type": "userProfileDevice", "
     tenant_id": "demo_tenant", "timestamp": "2021-02-10T21:00:00Z", "
     version": 2
   }


<!--NeedCopy-->
```

用户设备的字段描述。

字段名称	说明
cnt	过去 12 小时内设备的访问次数。
device	设备的名称。
event_type	发送到 SIEM 服务的数据类型。在这种情况下，事件类型是用户的设备访问信息。

用户应用模式

```
{

  "tenant_id": "demo_tenant", "entity_id": "demo", "entity_type": "user
     ", "timestamp": "2021-02-10T21:00:00Z", "event_type": "
     userProfileApp", "version": 2, "session_domain": "99
     e38d488136f62f828d4823edd120b4f32d724396a7410e6dd1b0", "
     user_samaccountname": "testnameeikragz779", "app": "
     Chromeeikragz779", "cnt": 189
```



```
    }


<!--NeedCopy-->
```

用户应用的字段描述。

字段名称	说明
event_type	发送到 SIEM 服务的数据类型。在这种情况下，事件类型是用户的设备访问信息。
session_domain	用户已登录的会话的 ID。
user_samaccountname	以前版本的 Windows（例如 Windows NT 4.0、Windows 95、Windows 98 和局域网管理器）的客户端和服务器的登录名称。此名称用于登录 Citrix StoreFront 并登录远程 Windows 计算机。
app	用户访问的应用程序的名称。
cnt	过去 12 小时内应用程序被访问的次数。

用户风险评分模式

```
{

  "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
   }


<!--NeedCopy-->
```

用户风险评分的字段描述。

字段名称	说明
cur_riskscore	分配给用户的当前风险评分。风险评分从 0 到 100 不等，具体取决于与用户事件相关的威胁严重程度。
event_type	发送到 SIEM 服务的数据类型。在这种情况下，事件类型是用户的风险评分。
last_update_timestamp	上次为用户更新风险评分的时间。
timestamp	收集用户风险评分事件并发送到 SIEM 服务的时间。此事件将在每 12 小时后发送至您的 SIEM 服务。

风险评分变更模式

示例 **1**:

```
{

  "alert_message": "Large risk score drop percent since last check", "
     alert_type": "riskscore_large_drop_pct", "alert_value": -21.73913,
      "cur_riskscore": 18, "entity_id": "demo_user", "entity_type": "
     user", "event_type": "riskScoreChange", "tenant_id": "demo_tenant"
     , "timestamp": "2021-02-11T05:45:00Z", "version": 2
   }


<!--NeedCopy-->
```

示例 **2**:

```
{

  "alert_message": "Risk score increase since last check", "alert_type"
     : "riskscore_increase", "alert_value": 39.0, "cur_riskscore": 76,
     "entity_id": "demo_user", "entity_type": "user", "event_type": "
     riskScoreChange", "tenant_id": "demo_tenant", "timestamp": "
     2021-02-11T03:45:00Z", "version": 2
   }


<!--NeedCopy-->
```

风险评分变化的字段描述。

字段名称	说明
alert_message	显示的风险评分变化的消息。
alert_type	指示警报是针对风险评分的提高还是风险评分百分比显著下降。如果用户的风险评分变化等于或超过 3，且此变化以任何速度增加或下降超过 10%，则数据将发送到 SIEM 服务。
alert_value	为风险评分变化分配的数值。风险评分变化是指用户当前风险评分与之前的风险评分之间的差异。警报值从 -100 到 100 不等。
cur_riskscore	分配给用户的当前风险评分。风险评分从 0 到 100 不等，具体取决于与用户事件相关的威胁严重程度。
event_type	发送到 SIEM 服务的数据类型。在这种情况下，事件类型是用户风险评分的变化。
timestamp	为用户检测到风险评分的最新更改的日期和时间。

风险指标架构

风险指标架构由两部分组成：指标摘要架构和指标事件详细信息架构。根据风险指标，模式中的字段及其值会相应地发生变化。

下表描述了所有指标摘要架构中通用的字段名称。

字段名称	说明
data source	向 Citrix Analytics for Security 发送数据的产品。例如：Citrix Secure Private Access、Citrix Gateway 以及 Citrix Apps and Desktops。
data_source_id	与数据源关联的 ID。ID 1 = Citrix Gateway、ID 2 = Citrix Endpoint Management、ID 3 = Citrix Apps and Desktops、ID 4 = Citrix Secure Private Access
entity_type	面临风险的实体。它可以是用户。
entity_id	与面临风险的实体关联的 ID。
event_type	发送到 SIEM 服务的数据类型。在这种情况下，事件类型是风险指标的摘要。
indicator_category	表示风险指标的类别。风险指标分为风险类别之一，即受到破坏的终端、受损的用户、数据泄露或内部威胁。
indicator_id	与风险指标关联的唯一 ID。
indicator_category_id	与风险指示器类别关联的 ID。ID 1 = 数据泄露，ID 2 = 内幕威胁，ID 3 = 受到攻击的用户，ID 4 = 受威胁的终端
indicator_name	风险指标的名称。对于自定义风险指标，此名称是在创建指标时定义的。
indicator_type	指示风险指标是默认的（内置）还是自定义指示器。
indicator_uuid	与风险指标实例关联的唯一 ID。
indicator_vector_name	表示与风险指标关联的风险向量。风险载体包括基于设备的风险指示器、基于位置的风险指示器、基于登录故障的风险指示器、基于 IP 的风险指示器、基于数据的风险指示器、基于文件的风险指示器和其他风险指示器。
indicator_vector_id	与风险载体关联的 ID。ID 1 = 基于设备的风险指标，ID 2 = 基于位置的风险指标，ID 3 = 基于登录失败的风险指标，ID 4 = 基于 IP 的风险指标，ID 5 = 基于数据的风险指标，ID 6 = 基于文件的风险指标，ID 7 = 其他风险指标，ID 999 = 不可用
occurrence_details	有关风险指标触发条件的详细信息。

字段名称	说明
risk_probability	表示与用户事件相关的风险的可能性。该值从 0 到 1.0 不等。对于自定义风险指标，risk _ 概率始终为 1.0，因为它是基于策略的指标。
severity	表示风险的严重程度。它可以是低、中或高。
tenant_id	客户的独特身份。
timestamp	触发风险指标的日期和时间。
ui_link	在 Citrix Analytics 用户界面上指向用户时间轴视图的链接。
observation_start_time	Citrix Analytics 开始监视用户事件直到时间戳的时间。如果在此时间段内检测到任何异常行为，则会触发风险指标。

下表描述了所有指标事件详细信息架构中通用的字段名称。

字段名称	说明
data_source_id	与数据源关联的 ID。ID 1 = Citrix Gateway、ID 2 = Citrix Endpoint Management、ID 3 = Citrix Apps and Desktops、ID 4 = Citrix Secure Private Access
indicator_category_id	与风险指示器类别关联的 ID。ID 1 = 数据泄露，ID 2 = 内幕威胁，ID 3 = 受到攻击的用户，ID 4 = 受威胁的终端
entity_id	与面临风险的实体关联的 ID。
entity_type	面临风险的实体。它可以是用户。
event_type	发送到 SIEM 服务的数据类型。在这种情况下，事件类型是风险指标事件的详细信息。
indicator_id	与风险指标关联的唯一 ID。
indicator_uuid	与风险指标实例关联的唯一 ID。
indicator_vector_name	表示与风险指标关联的风险向量。风险载体包括基于设备的风险指示器、基于位置的风险指示器、基于登录故障的风险指示器、基于 IP 的风险指示器、基于数据的风险指示器、基于文件的风险指示器和其他风险指示器。
indicator_vector_id	与风险载体关联的 ID。ID 1 = 基于设备的风险指标，ID 2 = 基于位置的风险指标，ID 3 = 基于登录失败的风险指标，ID 4 = 基于 IP 的风险指标，ID 5 = 基于数据的风险指标，ID 6 = 基于文件的风险指标，ID 7 = 其他风险指标，ID 999 = 不可用

字段名称	说明
tenant_id	客户的独特身份。
timestamp	触发风险指标的日期和时间。
version	已处理数据的模式版本。当前模式版本为 2。
client_ip	用户设备的 IP 地址。

> 注意
>
> - 如果整数数据类型字段值不可用，则分配的值为 -999。例如，"latitude": -999、"longitude": -999。
> - 如果字符串数据类型字段值不可用，则分配的值为 NA。例如，"city": "NA"、"region": "NA"。

Citrix Secure Private Access 风险指标架构

尝试访问列入黑名单的 **URL** 风险指标架构

指标摘要架构

```
{

  "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"
   }

 }


<!--NeedCopy-->
```

指标事件详情模式

```
{

  "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"
 }


<!--NeedCopy-->
```

下表描述了特定于摘要架构的字段名称以及尝试访问列入黑名单的 URL 的事件详细信息架构。

字段名称	说明
observation_start_time	Citrix Analytics 开始监视用户事件直到时间戳的时间。如果在此时间段内检测到任何异常行为，则会触发风险指标。
executed_action	在列入黑名单的 URL 上应用的操作。该操作包括“允许”和“阻止”。
reason_for_action	为 URL 应用操作的原因。

数据下载过多的风险指标架构

指标摘要架构

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 403,
  "indicator_uuid": "67d21b81-a89a-531e-af0b-c5688c2e9d40",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Excessive data download",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2018-03-16T10:00:00Z",
    "data_volume_in_bytes": 24000,
    "relevant_event_type": "External Resource Access"
   }

 }


<!--NeedCopy-->
```

指标事件详情模式

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 403,
  "indicator_uuid": "67d21b81-a89a-531e-af0b-c5688c2e9d40",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:30:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
```



```
  "entity_id": "demo_user",
  "version": 2,
  "domain_name": "www.facebook.com",
  "client_ip": "157.xx.xxx.xxx",
  "downloaded_bytes": 24000
 }


<!--NeedCopy-->
```

下表介绍了特定于摘要架构的字段名称以及用于下载过多数据的事件详细信息架构。

字段名称	说明
observation_start_time	Citrix Analytics 开始监视用户事件直到时间戳的时间。如果在此时间段内检测到任何异常行为，则会触发风险指标。
data_volume_in_bytes	下载的数据量（以字节为单位）。
relevant_event_type	指示用户事件的类型。
domain_name	从中下载数据的域的名称。
downloaded_bytes	下载的数据量（以字节为单位）。

异常的上载量风险指标架构

指标摘要架构

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 402,
  "indicator_uuid": "4f2a249c-9d05-5409-9c5f-f4c764f50e67",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Unusual upload volume",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
```



```
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2018-03-16T10:00:00Z",
    "data_volume_in_bytes": 24000,
    "relevant_event_type": "External Resource Access"
   }

 }


<!--NeedCopy-->
```

指标事件详情模式

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 402,
  "indicator_uuid": "c6abf40c-9b62-5db4-84bc-5b2cd2c0ca5f",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:30:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "domain_name": "www.facebook.com",
  "client_ip": "157.xx.xxx.xxx",
  "uploaded_bytes": 24000
 }


<!--NeedCopy-->
```

下表介绍了特定于摘要架构的字段名称以及异常上载卷的事件详细信息架构。

字段名	说明
observation_start_time	Citrix Analytics 开始监视用户事件直到时间戳的时间。如果在此时间段内检测到任何异常行为，则会触发风险指标。
data_volume_in_bytes	上载的数据量（以字节为单位）。
relevant_event_type	指示用户事件的类型。

字段名	说明
domain_name	上载数据的域名。
uploaded_bytes	上载的数据量（以字节为单位）。

Citrix Endpoint Management 风险指标架构

越狱或根设备检测到的指标模式

指标摘要架构

```
{

  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 200,
  "indicator_name": "Jailbroken / Rooted Device Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "aa872f86-a991-4219-ad01-2a070b6e633d",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-13T17:49:05Z",
  "ui_link": "https://analytics.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```

指标事件详情模式

```
{

  "indicator_id": 200,
  "client_ip": "122.xx.xx.xxx",
  "data_source_id": 2,
```



```
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_uuid": "9aaaa9e1-39ad-4daf-ae8b-2fa2caa60732",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T17:50:35Z",
  "version": 2
 }


<!--NeedCopy-->
```

检测到已列入黑名单的应用

指标摘要架构

```
{

  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 201,
  "indicator_name": "Device with Blacklisted Apps Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "3ff7bd54-4319-46b6-8b98-58a9a50ae9a7",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-13T17:49:23Z",
  "ui_link": "https://analytics.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```


指标事件详情模式

```
{

  "indicator_id": 201,
  "client_ip": "122.xx.xx.xxx",
  "data_source_id": 2,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_uuid": "743cd13a-2596-4323-8da9-1ac279232894",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T17:50:39Z",
  "version": 2
 }


<!--NeedCopy-->
```

检测到非托管设备

指标摘要架构

```
{

  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 203,
  "indicator_name": "Unmanaged Device Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "e28b8186-496b-44ff-9ddc-ae50e87bd757",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
```



```
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-13T12:56:30Z",
  "ui_link": "https://analytics.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```

指标事件详情模式

```
{

  "indicator_id": 203,
  "client_ip": "127.xx.xx.xxx",
  "data_source_id": 2,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_uuid": "dd280122-04f2-42b4-b9fc-92a715c907a0",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T18:41:30Z",
  "version": 2
 }


<!--NeedCopy-->
```

Citrix Gateway 风险指标架构

EPA 扫描失败风险指标架构

指标摘要架构

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 100,
  "indicator_uuid": "3c17454c-86f5-588a-a4ac-0342693d8a70",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
```



```
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "EPA scan failure",
  "severity": "low",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "event_description": "Post auth failed, no quarantine",
    "observation_start_time": "2017-12-21T07:00:00Z",
    "relevant_event_type": "EPA Scan Failure at Logon"
   }

 }


<!--NeedCopy-->
```

指标事件详情模式

```
{

  "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",
```



```
28    "security_expression": "CLIENT.OS(Win12) EXISTS",
29    "vpn_vserver_name": "demo_vpn_vserver",
30    "vserver_fqdn": "10.xxx.xx.xx"
31   }
32
33  <!--NeedCopy-->
```

该表描述了摘要架构特定的字段名称以及 EPA 扫描失败风险指标的事件详细信息架构。

字段名	说明
event_description	描述 EPA 扫描失败的原因，例如身份验证后失败和没有隔离组。
relevant_event_type	指示 EPA 扫描失败事件的类型。
gateway_domain_name	Citrix Gateway 的域名。
gateway_ip	Citrix Gateway 的 IP 地址。
policy_name	Citrix Gateway 上配置的 EPA 扫描策略名称。
country	检测到用户事件的国家/地区。
city	检测到用户事件的城市。
region	检测到用户事件的区域。
cs_vserver_name	内容交换机虚拟服务器的名称。
device_os	用户设备的操作系统。
security_expression	Citrix Gateway 上配置的安全表达式。
vpn_vserver_name	Citrix Gateway 虚拟服务器的名称。
vserver_fqdn	Citrix Gateway 虚拟服务器的 FQDN。

过度验证失败风险指标架构

指标摘要架构

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": 101,
5    "indicator_uuid": "4bc0f759-93e0-5eea-9967-ed69de9dd09a",
6    "indicator_category_id": 3,
7    "indicator_vector": {
8
9      "name": "Logon-Failure-Based Risk Indicators",
10     "id": 3  }
11   ,
12   "data_source_id": 1,
```



```
  "timestamp": "2017-12-21T07:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Excessive authentication failures",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/” ,
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2017-12-21T07:00:00Z",
    "relevant_event_type": "Logon Failure"
   }

 }

<!--NeedCopy-->
```

指标事件详情模式

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 101,
  "indicator_uuid": "a391cd1a-d298-57c3-a17b-01f159b26b99",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:10:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo-user",
  "version": 2,
  "event_description": "Bad (format) password passed to nsaaad",
  "authentication_stage": "Secondary",
  "authentication_type": "LDAP",
  "auth_server_ip": "10.xxx.x.xx",
  "client_ip": "24.xxx.xxx.xx",
  "gateway_ip": "24.xxx.xxx.xx",
  "vserver_fqdn": "demo-fqdn.citrix.com",
  "vpn_vserver_name": "demo_vpn_vserver",
  "cs_vserver_name": "demo_cs_vserver",
  "gateway_domain_name": "xyz",
  "country": "United States",
  "region": "California",
  "city": "San Jose",
```



```
  "nth_failure": 5
 }


<!--NeedCopy-->
```

下表介绍了特定于摘要架构的字段名称以及过度身份验证失败的事件详细信息架构。

字段名	说明
relevant_event_type	指示事件的类型，例如登录失败。
event_description	描述身份验证失败事件过多的原因，例如密码不正确。
authentication_stage	指示身份验证阶段是主要、次要还是第三阶段。
authentication_type	指示身份验证的类型，例如 LDAP、本地或 OAuth。
auth_server_ip	身份验证服务器的 IP 地址。
gateway_domain_name	Citrix Gateway 的域名。
gateway_ip	Citrix Gateway 的 IP 地址。
cs_vserver_name	内容交换机虚拟服务器的名称。
vpn_vserver_name	Citrix Gateway 虚拟服务器的名称。
vserver_fqdn	Citrix Gateway 虚拟服务器的 FQDN。
nth_failure	用户身份验证失败的次数。
country	检测到用户事件的国家/地区。
city	检测到用户事件的城市。
region	检测到用户事件的区域。

不可能旅行风险指标

指标摘要架构

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "111",
  "indicator_uuid": "83d68a6d-6588-5b77-9118-8a9e6a5b462b",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Location-Based Risk Indicators",
    "id": 2
   }
 ,
```



```
  "data_source_id": 1,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Impossible travel",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Impossible travel",
    "distance": 7480.44718,
    "observation_start_time": "2020-06-06T12:00:00Z",
    "historical_logon_locations": "[{
 "country":"United States","region":"Florida","city":"Miami","latitude"
    :25.7617,"longitude":-80.191,"count":28 }
 ,{
 "country":"United States","latitude":37.0902,"longitude":-95.7129,"
    count":2 }
 ]",
    "historical_observation_period_in_days": 30
   }

 }


<!--NeedCopy-->
```

指标事件详情模式

```
{

  "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"
 }


<!--NeedCopy-->
```

下表描述了特定于摘要架构的字段名称和不可能旅行的事件详细信息架构。

字段名称	说明
distance	与不可能行驶相关的事件之间的距离 (km)。
historical_logon_locations	在观察期间，用户访问的位置以及每个位置的访问次数。
historical_observation_period_in_days	每个地点都被监视 30 天。
relevant_event_type	指示事件的类型，例如登录。
observation_start_time	Citrix Analytics 开始监视用户事件直到时间戳的时间。如果在此时间段内检测到任何异常行为，则会触发风险指标。
country	用户登录的国家/地区。
city	用户登录的城市。
region	表示用户登录的区域。
latitude	指示用户登录的位置的纬度。
longitude	表示用户登录的位置的经度。
device_browser	用户使用的 Web 浏览器。
device_os	用户设备的操作系统。
ip_organization	注册客户端 IP 地址的组织
ip_routing_type	客户端 IP 路由类型

从可疑的 **IP** 风险指标架构登录

指标摘要架构

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 102,
  "indicator_uuid": "0100e910-561a-5ff3-b2a8-fc556d199ba5",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "data_source_id": 1,
  "timestamp": "2019-10-10T10:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 0.91,
  "indicator_category": "Compromised users",
  "indicator_name": "Logon from suspicious IP",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Logon",
    "client_ip": "1.0.xxx.xx",
    "observation_start_time": "2019-10-10T10:00:00Z",
    "suspicion_reasons": "brute_force|external_threat"
   }

 }

<!--NeedCopy-->
```

指标事件详情模式

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 102,
  "indicator_uuid": "4ba77b6c-bac0-5ad0-9b4a-c459a3e2ec33",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "data_source_id": 1,
  "timestamp": "2019-10-10T10:11:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
```



```
  "entity_id": "demo_user",
  "version": 2,
  "suspicion_reasons": "external_threat",
  "gateway_ip": "gIP1",
  "client_ip": "128.0.xxx.xxx",
  "country": "Sweden",
  "city": "Stockholm",
  "region": "Stockholm",
  "webroot_reputation": 14,
  "webroot_threat_categories": "Windows Exploits|Botnets|Proxy",
  "device_os": "Windows OS",
  "device_browser": "Chrome"
 }


<!--NeedCopy-->
```

下表描述了特定于摘要架构的字段名称以及从可疑 IP 登录的事件详细信息架构。

字段名称	说明
suspicious_reasons	识别 IP 地址为可疑的原因。
webroot_reputation	威胁情报提供商 Webroot 提供的 IP 信誉指数。
webroot_threat_categories	威胁情报提供商 Webroot 为可疑 IP 确定的威胁类别。
device_os	用户设备的操作系统。
device_browser	使用的 Web 浏览器。
country	检测到用户事件的国家/地区。
city	检测到用户事件的城市。
region	检测到用户事件的区域。

异常身份验证失败风险指标

指标摘要架构

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 109,
  "indicator_uuid": "dc0174c9-247a-5e48-a2ab-d5f92cd83d0f",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
```



```
  "timestamp": "2020-04-01T06:44:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Unusual authentication failure",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Logon Failure",
    "observation_start_time": "2020-04-01T05:45:00Z"
   }

 }


<!--NeedCopy-->
```

指标事件详情模式

```
{

  "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"
 }

```



```
30
31 <!--NeedCopy-->
```

下表介绍了特定于摘要架构的字段名称以及异常身份验证失败的事件详细信息架构。

字段名	说明
relevant_event_type	指示事件的类型，例如登录失败。
event_description	指示登录是成功还是失败
authentication_stage	指示身份验证阶段是主要、次要还是第三阶段。
authentication_type	指示身份验证的类型，例如 LDAP、本地或 OAuth。
is_risky	对于成功登录，is_ 冒险值为假。对于登录失败，is_ 冒险值为真。
device_os	用户设备的操作系统。
device_browser	用户使用的 Web 浏览器。
country	检测到用户事件的国家/地区。
city	检测到用户事件的城市。
region	检测到用户事件的区域。

可疑登录风险指标

指标摘要架构

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": "110",
5    "indicator_uuid": "67fd935-a6a3-5397-b596-636aa1588c",
6    "indicator_category_id": 3,
7    "indicator_vector": [
8      {
9
10       "name": "Location-Based Risk Indicators",
11       "id": 2
12      }
13   ,
14     {
15
16       "name": "IP-Based Risk Indicators",
17       "id": 4
18      }
19   ,
20     {
21
```



```
      "name": "Other Risk Indicators",
      "id": 7
     }

  ],
  "data_source_id": 1,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 0.71,
  "indicator_category": "Compromised users",
  "indicator_name": "Suspicious logon",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2020-06-06T12:00:00Z",
    "relevant_event_type": "Logon",
    "event_count": 1,
    "historical_observation_period_in_days": 30,
    "country": "United States",
    "region": "Florida",
    "city": "Miami",
    "historical_logon_locations": "[{
"country":"United States","region":"New York","city":"New York City","
    latitude":40.7128,"longitude":-74.0060,"count":9 }
]",
    "user_location_risk": 75,
    "device_id": "",
    "device_os": "Windows OS",
    "device_browser": "Chrome",
    "user_device_risk": 0,
    "client_ip": "99.xxx.xx.xx",
    "user_network_risk": 75,
    "webroot_threat_categories": "Phishing",
    "suspicious_network_risk": 89
   }

 }



<!--NeedCopy-->
```

指标事件详情模式

```
{

  "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"
}


<!--NeedCopy-->
```

下表描述了特定于摘要架构的字段名称和可疑登录的事件详细信息架构。

字段名称	说明
historical_logon_locations	在观察期间，用户访问的位置以及每个位置的访问次数。
historical_observation_period_in_days	每个地点都被监视 30 天。
relevant_event_type	指示事件的类型，例如登录。

字段名称	说明
observation_start_time	Citrix Analytics 开始监视用户事件直到时间戳的时间。如果在此时间段内检测到任何异常行为，则会触发风险指标。
occurrence_event_type	指示用户事件类型，例如帐户登录。
country	用户登录的国家/地区。
city	用户登录的城市。
region	表示用户登录的区域。
latitude	指示用户登录的位置的纬度。
longitude	表示用户登录的位置的经度。
device_browser	用户使用的 Web 浏览器。
device_os	用户设备的操作系统。
device_id	用户使用的设备的名称。
user_location_risk	表示用户登录的位置的可疑级别。低怀疑等级：0—69，中等怀疑等级：70—89，高怀疑等级：90—100
user_device_risk	表示用户从中登录的设备的可疑级别。低怀疑等级：0—69，中等怀疑等级：70—89，高怀疑等级：90—100
user_network_risk	表示用户登录的网络或子网的可疑级别。低怀疑等级：0—69，中等怀疑等级：70—89，高怀疑等级：90—100
suspicious_network_risk	表示基于 Webroot IP 威胁情报源的 IP 威胁级别。低威胁级别：0—69，中等威胁级别：70—89，高威胁级别：90—100
webroot_threat_categories	指示从基于 Webroot IP 威胁情报源的 IP 地址检测到的威胁类型。威胁类别可以是垃圾邮件源、Windows 漏洞利用、Web 攻击、僵尸网络、扫描程序、拒绝服务、信誉、网络钓鱼、代理、未指定、移动威胁和 Tor 代理

Citrix DaaS 和 **Citrix Virtual Apps and Desktops** 风险指标架构

不可能旅行风险指标

指标摘要架构

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "313",
  "indicator_uuid": "c78d1dd4-5e70-5642-ba6f-1cdf31bc6ab2",
```



```
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Location-Based Risk Indicators",
    "id": 2
   }
 ,
  "data_source_id": 3,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Impossible travel",
  "severity": "medium",
  "data_source": "Apps and Desktops",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Impossible travel",
    "distance": 7480.44718,
    "observation_start_time": "2020-06-06T12:00:00Z",
    "historical_logon_locations": "[{
"country":"United States","region":"Florida","city":"Miami","latitude"
   :25.7617,"longitude":-80.191,"count":28 }
 ,{
 "country":"United States","latitude":37.0902,"longitude":-95.7129,"
    count":2 }
 ]",
    "historical_observation_period_in_days": 30
   }

 }


<!--NeedCopy-->
```

指标事件详情模式

```
{

  "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
   }
```



```
13   ,
14    "data_source_id": 3,
15    "timestamp": "2020-06-06T05:05:00Z",
16    "event_type": "indicatorEventDetails",
17    "entity_type": "user",
18    "entity_id": "demo_user",
19    "version": 2,
20    "occurrence_event_type": "Account.Logon",
21    "client_ip": "95.xxx.xx.xx",
22     “ip_organization” :  “global telecom ltd” ,
23     “ip_routing_type” :  “mobile gateway” ,
24    "country": "Norway",
25    "region": "Oslo",
26    "city": "Oslo",
27    "latitude": 59.9139,
28    "longitude": 10.7522,
29    "device_id": "device1",
30    "receiver_type": "XA.Receiver.Linux",
31    "os": "Linux OS",
32    "browser": "Chrome 62.0.3202.94"
33   }
34
35
36  <!--NeedCopy-->
```

下表描述了特定于摘要架构的字段名称和不可能旅行的事件详细信息架构。

字段名称	说明
distance	与不可能行驶相关的事件之间的距离 (km)。
historical_logon_locations	在观察期间，用户访问的位置以及每个位置的访问次数。
historical_observation_period_in_days	每个地点都被监视 30 天。
relevant_event_type	指示事件的类型，例如登录。
observation_start_time	Citrix Analytics 开始监视用户事件直到时间戳的时间。如果在此时间段内检测到任何异常行为，则会触发风险指标。
country	用户登录的国家/地区。
city	用户登录的城市。
region	表示用户登录的区域。
latitude	指示用户登录的位置的纬度。
longitude	表示用户登录的位置的经度。
browser	用户使用的 Web 浏览器。

字段名称	说明
os	用户设备的操作系统。
device_id	用户使用的设备的名称。
receiver_type	用户设备上安装的 Citrix Workspace 应用程序或 Citrix Receiver 的类型。
ip_organization	注册客户端 IP 地址的组织
ip_routing_type	客户端 IP 路由类型

潜在的数据泄露风险指标

指标摘要架构

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 303,
  "indicator_uuid": "fb649ff7-5b09-5f48-8a04-12836b9eed85",
  "indicator_category_id": 1,
  "indicator_vector": {

    "name": "Data-Based Risk Indicators",
    "id": 5  }
 ,
  "data_source_id": 3,
  "timestamp": "2018-04-02T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Data exfiltration",
  "indicator_name": "Potential data exfiltration",
  "severity": "low",
  "data_source": "Citrix Apps and Desktops",
  "ui_link": "https://analytics.cloud.com/user/ ",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Download/Print/Copy",
    "observation_start_time": "2018-04-02T10:00:00Z",
    "exfil_data_volume_in_bytes": 1172000
   }

 }


<!--NeedCopy-->
```


指标事件详情模式

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 303,
  "indicator_uuid": "fb649ff7-5b09-5f48-8a04-12836b9eed85",
  "indicator_category_id": 1,
  "indicator_vector": {

    "name": "Data-Based Risk Indicators",
    "id": 5  }
 ,
  "data_source_id": 3,
  "timestamp": "2018-04-02T10:57:36Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "occurrence_event_type": "App.SaaS.Clipboard",
  "file_size_in_bytes": 98000,
  "file_type": "text",
  "device_id": "dvc5",
  "receiver_type": "XA.Receiver.Windows",
  "app_url": "https://www.citrix.com",
  "client_ip": "10.xxx.xx.xxx",
  "entity_time_zone": "Pacific Standard Time"
 }


<!--NeedCopy-->
```

下表介绍了特定于摘要架构的字段和潜在数据泄露的事件详细信息架构。

字段名称	说明
observation_start_time	Citrix Analytics 开始监视用户事件直到时间戳的时间。如果在此时间段内检测到任何异常行为，则会触发风险指标。
relevant_event_type	表示用户事件，例如下载、打印或复制数据。
exfil_data_volume_in_bytes	数据泄露的量。
occurrence_event_type	指示数据泄露的发生方式，例如 SaaS 应用程序中的剪贴板操作。
file_size_in_bytes	文件的大小。
file_type	文件的类型。
device_id	用户设备的 ID。
receiver_type	安装在用户设备上的 Citrix Workspace 应用程序或 Citrix Receiver。

字段名称	说明
app_url	用户访问的应用程序的 URL。
entity_time_zone	用户的时区。

可疑登录风险指标架构

指标摘要架构

```
{

  "tenant_id": "tenant_1",
  "indicator_id": "312",
  "indicator_uuid": "1b97c3be-abcd-efgh-ijkl-1234567890",
  "indicator_category_id": 3,
  "indicator_vector":
  [
    {

      "name": "Other Risk Indicators",
      "id": 7
     }
 ,
    {

      "name":"Location-Based Risk Indicators",
      "id":2
     }
 ,
    {

      "name":"IP-Based Risk Indicators",
      "id":4
     }
 ,
    {

      "name": "Device-Based Risk Indicators",
      "id": 1
     }
 ,
  ],
  "data_source_id": 3,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "user2",
  "version": 2,
  "risk_probability": 0.78,
  "indicator_category": "Compromised users",
```



```
  "indicator_name": "Suspicious logon",
  "severity": "medium",
  "data_source": "Citrix Apps and Desktops",
  "ui_link": "https://analytics.cloud.com/user/ ",
  "indicator_type": "builtin",
  "occurrence_details":
  {

    "user_location_risk": 0,
    "city": "Some_city",
    "observation_start_time": "2020-06-06T12:00:00Z",
    "event_count": 1,
    "user_device_risk": 75,
    "country": "United States",
    "device_id": "device2",
    "region": "Some_Region",
    "client_ip": "99.xx.xx.xx",
    "webroot_threat_categories": "'Spam Sources', 'Windows Exploits', '
       Web Attacks', 'Botnets', 'Scanners', 'Denial of Service'",
    "historical_logon_locations": "[{
 "country":"United States","latitude":45.0,"longitude":45.0,"count":12
     }
 ,{
 "country":"United States","region":"Some_Region_A","city":"Some_City_A
    ","latitude":0.0,"longitude":0.0,"count":8 }
 ]",
    "relevant_event_type": "Logon",
    "user_network_risk": 100,
    "historical_observation_period_in_days": 30,
    "suspicious_network_risk": 0
   }

 }


<!--NeedCopy-->
```

指标事件详情模式

```
{

  "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
     }
 ,
    {
```



```
16
17        "name":"Location-Based Risk Indicators",
18        "id":2
19       }
20   ,
21      {
22
23        "name":"IP-Based Risk Indicators",
24        "id":4
25       }
26   ,
27      {
28
29        "name": "Device-Based Risk Indicators",
30        "id": 1
31       }
32   ,
33    ],
34    "data_source_id": 3,
35    "timestamp": "2020-06-06 12:02:30",
36    "event_type": "indicatorEventDetails",
37    "entity_type": "user",
38    "entity_id": "user2",
39    "version": 2,
40    "occurrence_event_type": "Account.Logon",
41    "city": "Some_city",
42    "country": "United States",
43    "region": "Some_Region",
44    "latitude": 37.751,
45    "longitude": -97.822,
46    "browser": "Firefox 1.3",
47    "os": "Windows OS",
48    "device_id": "device2",
49    "receiver_type": "XA.Receiver.Chrome",
50    "client_ip": "99.xxx.xx.xx"
51   }
52
53
54  <!--NeedCopy-->
```

下表描述了特定于摘要架构的字段名称和可疑登录的事件详细信息架构。

字段名称	说明
historical_logon_locations	在观察期间，用户访问的位置以及每个位置的访问次数。
historical_observation_period_in_days	每个地点都被监视 30 天。
relevant_event_type	指示事件的类型，例如登录。

字段名称	说明
observation_start_time	Citrix Analytics 开始监视用户事件直到时间戳的时间。如果在此时间段内检测到任何异常行为，则会触发风险指标。
occurrence_event_type	指示用户事件类型，例如帐户登录。
country	用户登录的国家/地区。
city	用户登录的城市。
region	表示用户登录的区域。
latitude	指示用户登录的位置的纬度。
longitude	表示用户登录的位置的经度。
browser	用户使用的 Web 浏览器。
os	用户设备的操作系统。
device_id	用户使用的设备的名称。
receiver_type	用户设备上安装的 Citrix Workspace 应用程序或 Citrix Receiver 的类型。
user_location_risk	表示用户登录的位置的可疑级别。低怀疑等级：0—69，中等怀疑等级：70—89，高怀疑等级：90—100
user_device_risk	表示用户从中登录的设备的可疑级别。低怀疑等级：0—69，中等怀疑等级：70—89，高怀疑等级：90—100
user_network_risk	表示用户登录的网络或子网的可疑级别。低怀疑等级：0—69，中等怀疑等级：70—89，高怀疑等级：90—100
suspicious_network_risk	表示基于 Webroot IP 威胁情报源的 IP 威胁级别。低威胁级别：0—69，中等威胁级别：70—89，高威胁级别：90—100
webroot_threat_categories	指示从基于 Webroot IP 威胁情报源的 IP 地址检测到的威胁类型。威胁类别可以是垃圾邮件源、Windows 漏洞利用、Web 攻击、僵尸网络、扫描程序、拒绝服务、信誉、网络钓鱼、代理、未指定、移动威胁和 Tor 代理

Microsoft Active Directory 指示器

指标摘要架构

```
{

  "data_source": "Microsoft Graph Security",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
```



```
  "indicator_category": "Compromised users",
  "indicator_id": 1000,
  "indicator_name": "MS Active Directory Indicator",
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "9880f479-9fbe-4ab0-8348-a613f9de5eba",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-01-27T16:03:46Z",
  "ui_link": "https://analytics-daily.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```

指标事件详情模式

```
{

  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_id": 1000,
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "indicator_uuid": "9880f479-9fbe-4ab0-8348-a613f9de5eba",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-01-27T16:03:46Z",
  "version": 2
 }


<!--NeedCopy-->
```

自定义风险指标架构

下一节描述了自定义风险指标的架构。

> 注意
>
> 目前，Citrix Analytics 会将与 Citrix DaaS 和 Citrix Virtual Apps and Desktops 的自定义风险指标相关的数据发送到您的 SIEM 服务。

下表描述了自定义风险指标摘要架构的字段名称。

字段名称	说明
data source	向 Citrix Analytics for Security 发送数据的产品。例如：Citrix Secure Private Access、Citrix Gateway 以及 Citrix Apps and Desktops。
data_source_id	与数据源关联的 ID。ID 1 = Citrix Gateway、ID 2 = Citrix Endpoint Management、ID 3 = Citrix Apps and Desktops、ID 4 = Citrix Secure Private Access
entity_id	与面临风险的实体关联的 ID。
entity_type	面临风险的实体。在这种情况下，实体是用户。
event_type	发送到 SIEM 服务的数据类型。在这种情况下，事件类型是风险指标的摘要。
indicator_category	表示风险指标的类别。风险指标分为风险类别之一，即受到破坏的终端、受损的用户、数据泄露或内部威胁。
indicator_id	与风险指标关联的唯一 ID。
indicator_category_id	与风险指标类别关联的 ID。ID 1 = 数据泄露，ID 2 = 内部威胁，ID 3 = 受感染的用户，ID 4 = 受感染的终端
indicator_name	风险指标的名称。对于自定义风险指标，此名称是在创建指标时定义的。
indicator_type	指示风险指标是默认的（内置）还是自定义指示器。
indicator_uuid	与风险指标实例关联的唯一 ID。
occurrence_details	有关风险指标触发条件的详细信息。
pre_configured	指示自定义风险指标是否已预配置。
risk_probability	表示与用户事件相关的风险的可能性。该值从 0 到 1.0 不等。对于自定义风险指标，risk _ 概率始终为 1.0，因为它是基于策略的指标。
severity	表示风险的严重程度。它可以是低、中或高。
tenant_id	客户的独特身份。
timestamp	触发风险指标的日期和时间。
ui_link	在 Citrix Analytics 用户界面上指向用户时间轴视图的链接。

字段名称	说明
version	已处理数据的模式版本。当前模式版本为 2。

下表描述了自定义风险指标事件详细信息架构中通用的字段名称。

字段名称	说明
data_source_id	与数据源关联的 ID。ID 1 = Citrix Gateway、ID 2 = Citrix Endpoint Management、ID 3 = Citrix Apps and Desktops、ID 4 = Citrix Secure Private Access
indicator_category_id	与风险指标类别关联的 ID。ID 1 = 数据泄露，ID 2 = 内部威胁，ID 3 = 受感染的用户，ID 4 = 受感染的终端
event_type	发送到 SIEM 服务的数据类型。在这种情况下，事件类型是风险指标事件的详细信息。
tenant_id	客户的独特身份。
entity_id	与面临风险的实体关联的 ID。
entity_type	面临风险的实体。在这种情况下，它是用户。
indicator_id	与风险指标关联的唯一 ID。
indicator_uuid	与风险指标实例关联的唯一 ID。
timestamp	触发风险指标的日期和时间。
version	已处理数据的模式版本。当前模式版本为 2。
event_id	与用户事件关联的 ID。
occurrence_event_type	指示用户事件的类型，例如会话登录、会话启动和帐户登录。
product	指示 Citrix Workspace 应用程序的类型，例如适用于 Windows 的 Citrix Workspace 应用程序
client_ip	用户设备的 IP 地址。
session_user_name	与 Citrix Apps and Desktops 会话关联的用户名。
city	从中检测到用户事件的城市的名称。
country	从中检测到用户事件的国家/地区的名称。
device_id	用户使用的设备的名称。
os_name	用户设备上安装的操作系统。有关详细信息，请参阅应用程序和桌面的自助式搜索。

字段名称	说明
os_version	用户设备上安装的操作系统的版本。有关详细信息，请参阅应用程序和桌面的自助式搜索。
os_extra_info	与用户设备上安装的操作系统相关的额外详细信息。有关详细信息，请参阅应用程序和桌面的自助式搜索。

Citrix DaaS 和 Citrix Virtual Apps and Desktops 的自定义风险指标

指标摘要架构

```
{

  "data_source": " Citrix Apps and Desktops",
  "data_source_id": 3,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised users",
  "indicator_category_id": 3,
  "indicator_id": "ca97a656ab0442b78f3514052d595936",
  "indicator_name": "Demo_user_usage",
  "indicator_type": "custom",
  "indicator_uuid": "8e680e29-d742-4e09-9a40-78d1d9730ea5",
  "occurrence_details": {

    "condition": "User-Name ~ demo_user", "happen": 0, "new_entities":
       "", "repeat": 0, "time_quantity": 0, "time_unit": "", "type": "
       everyTime" }
 ,
  "pre_configured": "N",
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-02-10T14:47:25Z",
  "ui_link": "https://analytics.cloud.com/user/ ",
  "version": 2
 }


<!--NeedCopy-->
```

会话登录事件的指示器事件详细信息架构

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
```



```
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.Logon",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "SYD04-MS1-S102",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
 }


<!--NeedCopy-->
```

下表描述了特定于会话登录事件的事件详细信息架构的字段名称。

字段名称	说明
app_name	启动的应用程序或桌面的名称。
launch_type	表示应用程序或桌面。
domain	发送请求的服务器的域名。
server_name	服务器的名称。
session_guid	事件会话的 GUID。

会话启动事件的指标事件详细信息架构

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
```



```
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.Launch",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
 }


<!--NeedCopy-->
```

下表描述了特定于会话启动事件的事件详细信息架构的字段名称。

字段名称	说明
app_name	启动的应用程序或桌面的名称。
launch_type	表示应用程序或桌面。

帐户登录事件的指标事件详细信息架构

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Account.Logon",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
```



```
 }


<!--NeedCopy-->
```

下表描述了特定于帐户登录事件的事件详细信息架构的字段名称。

字段名称	说明
app_name	启动的应用程序或桌面的名称。

会话结束事件的指标事件详细信息架构

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
 }


<!--NeedCopy-->
```

下表描述了特定于会话结束事件的事件详细信息架构的字段名称。

字段名称	说明
app_name	启动的应用程序或桌面的名称。
launch_type	表示应用程序或桌面。
domain	发送请求的服务器的域名。
server_name	服务器的名称。
session_guid	事件会话的 GUID。

应用启动事件的指标事件详细信息架构

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.Start",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "module_file_path": "/root/folder1/folder2/folder3"
 }


<!--NeedCopy-->
```

下表介绍了特定于应用程序启动事件的事件详细信息架构的字段名称。

字段名称	说明
app_name	启动的应用程序或桌面的名称。
launch_type	表示应用程序或桌面。
domain	发送请求的服务器的域名。
server_name	服务器的名称。
session_guid	事件会话的 GUID。
module_file_path	正在使用的应用程序的路径。

应用结束事件的指标事件详细信息架构

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "module_file_path": "/root/folder1/folder2/folder3"
 }


<!--NeedCopy-->
```

下表介绍了特定于应用程序结束事件的事件详细信息架构的字段名称。

字段名称	说明
app_name	启动的应用程序或桌面的名称。
launch_type	表示应用程序或桌面。
domain	发送请求的服务器的域名。
server_name	服务器的名称。
session_guid	事件会话的 GUID。
module_file_path	正在使用的应用程序的路径。

文件下载事件的指标事件详细信息架构

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "File.Download",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "file_download_file_name": "File5.txt",
  "file_download_file_path": "/root/folder1/folder2/folder3",
  "file_size_in_bytes": 278,
  "launch_type": "Desktop",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "device_type": "USB"
 }


<!--NeedCopy-->
```

下表描述了特定于文件下载事件的事件详细信息架构的字段名称。

字段名称	说明
file_download_file_name	下载文件的名称。
file_download_file_path	下载文件的目标路径。
launch_type	表示应用程序或桌面。
domain	发送请求的服务器的域名。
server_name	服务器的名称。
session_guid	事件会话的 GUID。
device_type	指示下载文件的设备的类型。

打印事件的指标事件详细信息架构

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Printing",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "printer_name": "Test-printer",
  "launch_type": "Desktop",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "job_details_size_in_bytes": 454,
  "job_details_filename": "file1.pdf",
  "job_details_format": "PDF"
 }


<!--NeedCopy-->
```


下表描述了特定于打印事件的事件详细信息架构的字段名称。

字段名称	说明
printer_name	用于打印作业的打印机的名称。
launch_type	表示应用程序或桌面。
domain	发送请求的服务器的域名。
server_name	服务器的名称。
session_guid	事件会话的 GUID。
job_details_size_in_bytes	打印作业（例如文件或文件夹）的大小。
job_details_filename	打印文件的名称。
job_details_format	打印作业的格式。

应用程序 **SaaS** 启动事件的指标事件详细信息架构

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.SaaS.Launch",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "launch_type": "Desktop",
 }


<!--NeedCopy-->
```

下表介绍了特定于应用程序 SaaS 启动事件的事件详细信息架构的字段名称。

字段名称	说明
launch_type	表示应用程序或桌面。

应用程序 **SaaS** 结束事件的指标事件详细信息架构

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.SaaS.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "launch_type": "Desktop",
 }


<!--NeedCopy-->
```

下表介绍了特定于应用程序 SaaS 结束事件的事件详细信息架构的字段名称。

字段名称	说明
launch_type	表示应用程序或桌面。

数据源事件

此外，您可以配置数据导出功能，从启用 Citrix Analytics for Security 的产品数据源中导出用户事件。在 Citrix 环境中执行任何活动时，都会生成数据源事件。导出的事件是未经处理的实时用户和产品使用数据，可在自助服务视图中找到。这些事件中包含的元数据可以进一步用于更深入的威胁分析、创建新的控制板，并与安全和 IT 基础设施中的其他非 Citrix 数据源事件相关联。

目前，Citrix Analytics for Security 会向您的 SIEM 发送针对 Citrix Virtual Apps and Desktops 数据源的用户事件。

数据源事件的架构详细信息

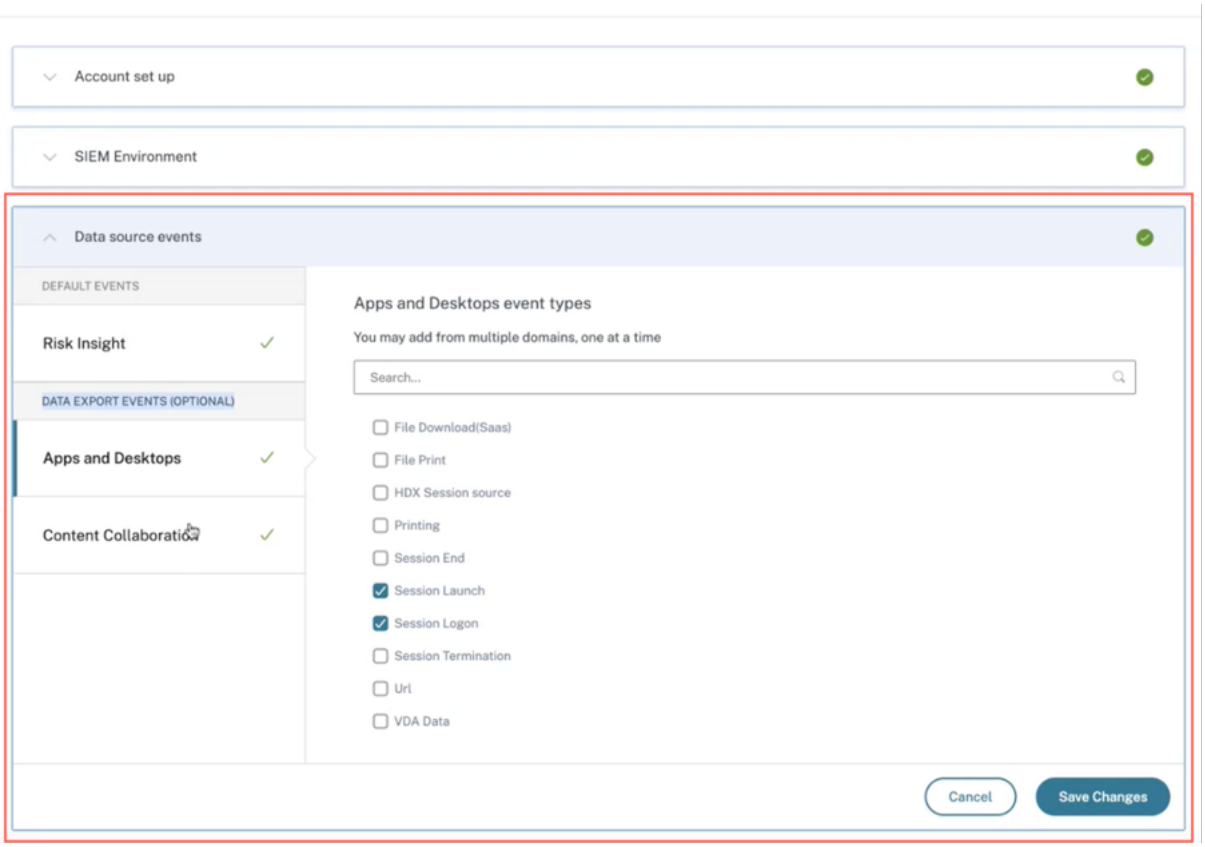
Citrix Virtual Apps and Desktops 事件

当用户使用虚拟应用程序或虚拟桌面时，Citrix Analytics for Security 会实时接收用户事件。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源。您可以在 SIEM 中查看以下与 Citrix Virtual Apps and Desktops 相关的用户事件：

- 所有事件类型
- 帐户登录
- 应用程序（开始、启动、结束）
- 剪贴板
- 文件（打印、下载）
- 文件下载 (SaaS)
- HDX 会话源
- 打印
- 会话（登录、启动、结束、终止）
- Url
- VDA 数据
- 创建 VDA 进程

有关事件及其属性的更多信息，请参阅 Virtual Apps and Desktops 自助搜索。

您可以查看哪些事件类型已启用并流向 SIEM。您可以配置或删除适用于租户的事件类型，然后单击“保存更改”按钮以保存您的设置。



利用 **Citrix Analytics SIEM** 数据模型进行威胁分析和数据关联

June 26, 2023

本文解释了发送到客户的 SIEM 环境的事件所表现出的实体数据关系。为了阐明这一点，让我们举一个威胁猎捕场景的例子，其中，客户端 IP 和操作系统是重点。将讨论将上述属性与用户关联的以下方法：

- 使用自定义风险指标见解
- 使用数据源事件

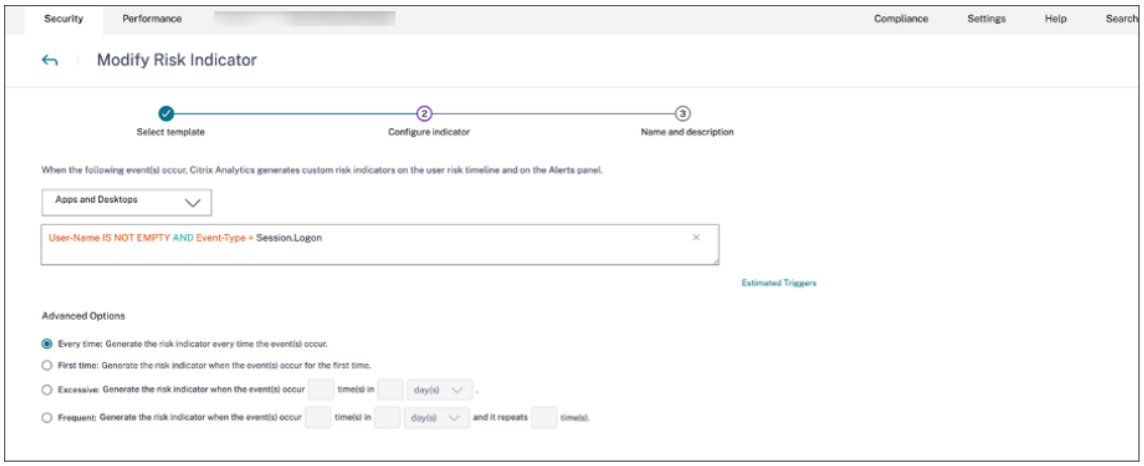
Splunk 是选择在以下示例中展示的 SIEM 环境。也可以使用 Citrix Analytics 的工作簿模板在 Sentinel 上执行类似的数据关联。要进一步探讨这个问题，请参阅 Microsoft Sentinel 的 Citrix Analytics 工作簿。

自定义风险指标见解

正如 SIEM 的 Citrix Analytics 数据导出格式中提到的那样，指标摘要和事件详细信息见解是默认风险洞察数据集的一部分。对于 Citrix Virtual Apps and Desktops 指标数据集，默认情况下会导出客户端 IP 和操作系统。因此，如果管理员设置了带有或不包含这些字段的条件的自定义指标，则所述数据点将流入您的 Splunk 环境。

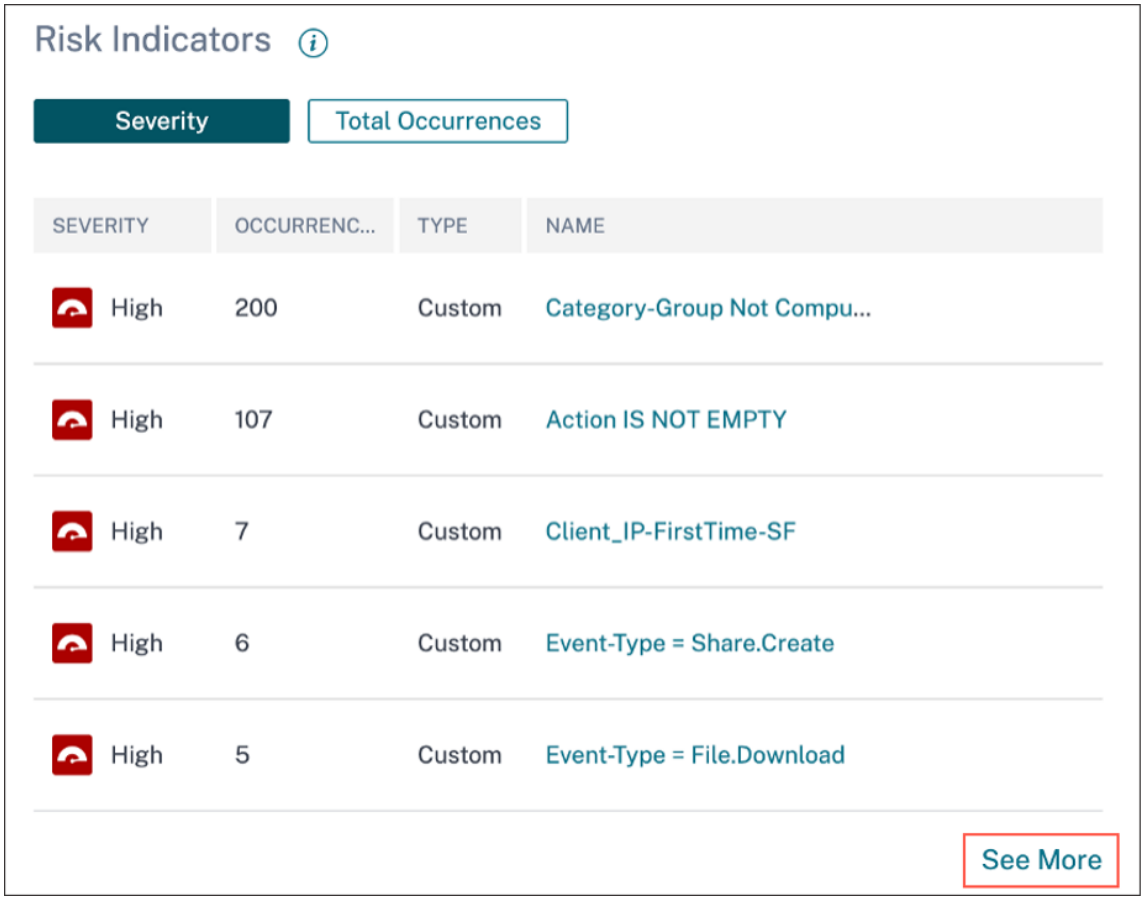
在 **Citrix Analytics** 中设置自定义风险指标

1. 导航到 **Citrix Analytics for Security** 控制板 **>** 自定义风险指标 **>** 创建指标。您可以创建包含任何条件的自定义风险指标，以帮助您监视用户的行为。设置自定义指标后，触发相关条件的所有用户都将在 Splunk 环境中可见。

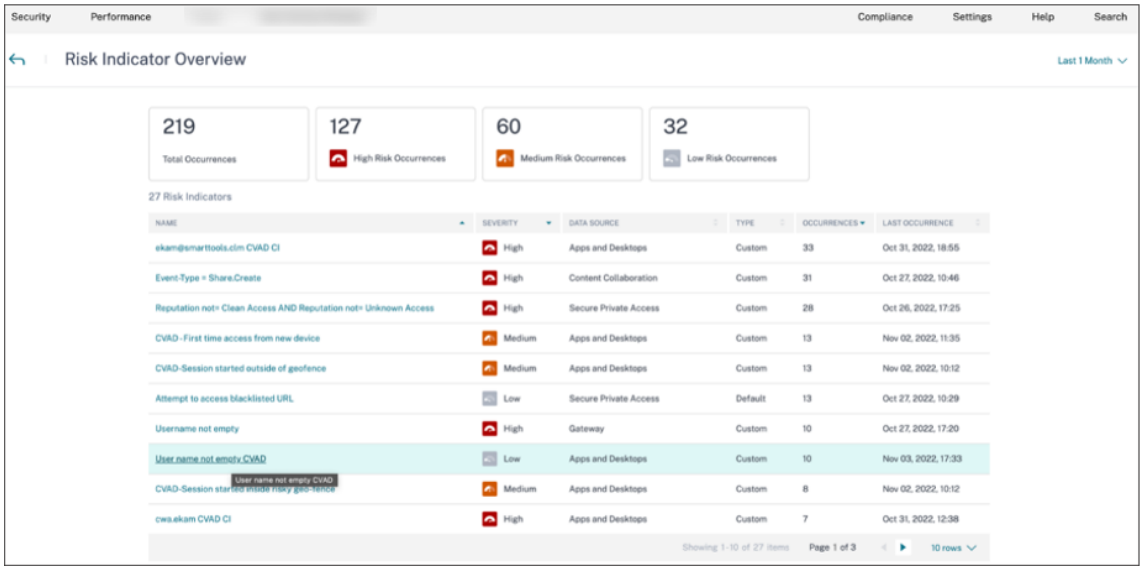


2. 要在 Citrix Analytics for Security 上查看创建的风险指标出现情况，请导航到 安全 **>** 用户。导航到页面底部，然后单击加号 **(+)** 图标。

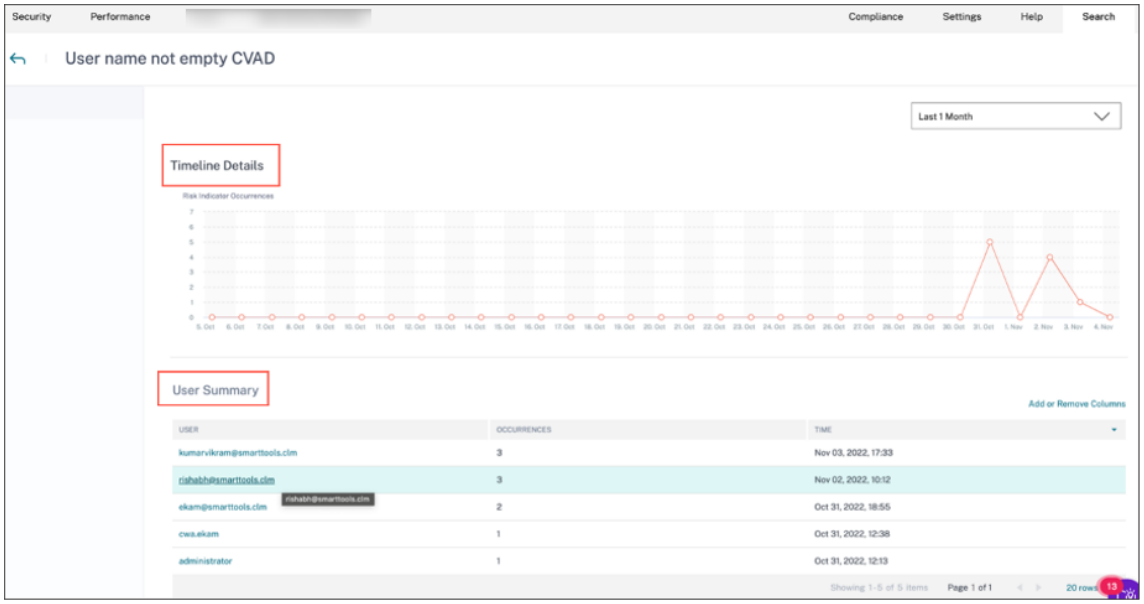
出现“风险指标”卡。您可以查看风险指标、严重程度和发生率的详细信息。



3. 单击“查看更多”。将出现“风险指标 概述”页面。



在风险指标概述页面中，您可以通过详细的时间表视图和用户摘要查看触发该指标的用户的详细信息。要了解有关时间表的更多信息，请参阅 用户风险时间表和概况。

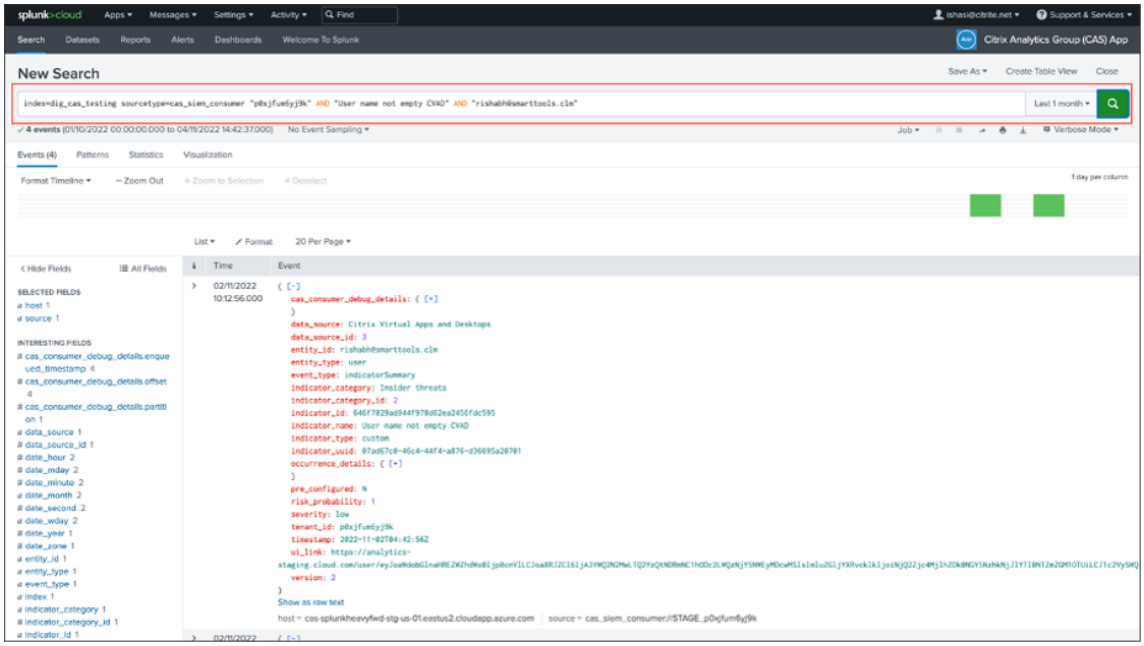


Splunk 上出现的风险指标-原始查询

您还可以使用 Splunk 基础架构管理员在 Splunk Enterprise for Citrix Analytics for Security 加载项上设置数据输入时使用的索引和源类型来获取客户端 IP 和操作系统信息。

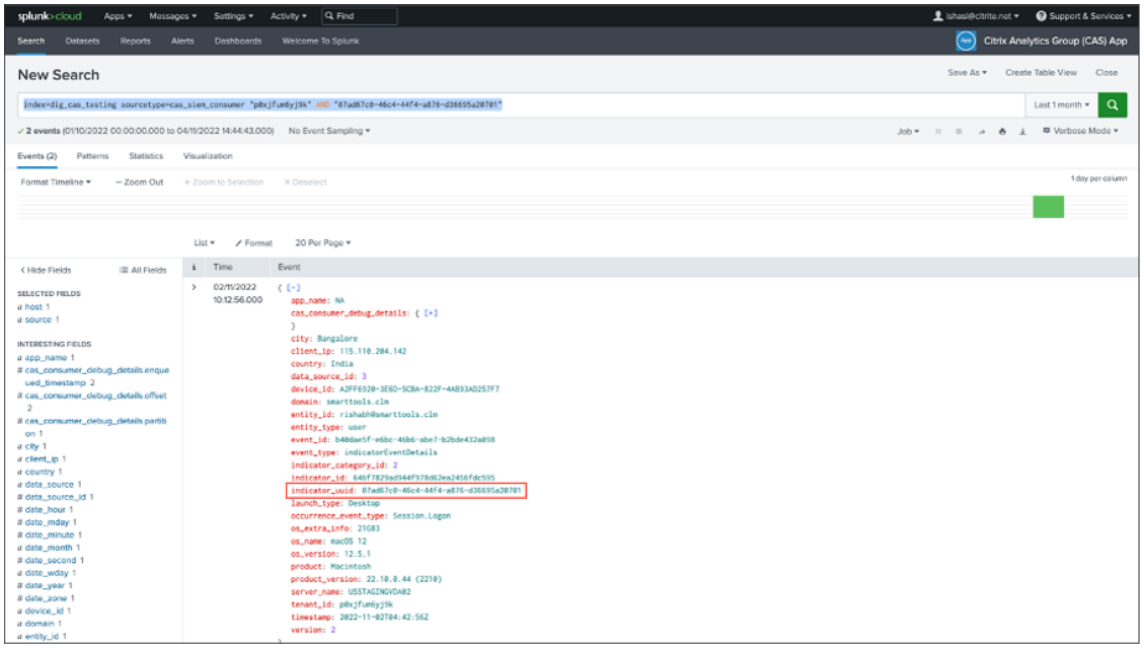
1. 导航到 **Splunk >** 新建搜索。在搜索查询中，输入并运行以下查询：

```
index=<index configured by you> sourcetype=<sourcetype configured
    by you> AND "<tenant_id>" AND "<indicator name configured by
    you on CAS>" AND "<user you are interested in>"

<!--NeedCopy-->
```

2. 选取 indicator_uuid 并运行以下查询：

```
index=<index configured by you> sourcetype=<sourcetype configured
    by you> "<tenant_id>" AND "<indicator_uuid>"

<!--NeedCopy-->
```



事件结果包含指标事件摘要和指标事件详情（由您的指标触发的活动）。事件详细信息包含客户端 **IP** 和操作系统信息（名称、版本、额外信息）。

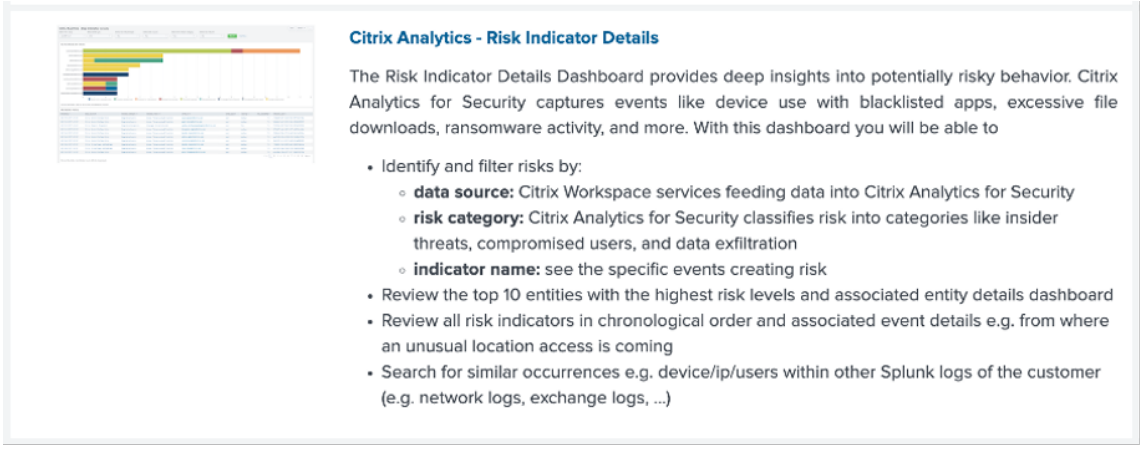
要了解有关数据格式的更多信息，请参阅 SIEM 的 Citrix Analytics 数据导出格式。

Splunk 上出现的风险指标-控制板应用程序

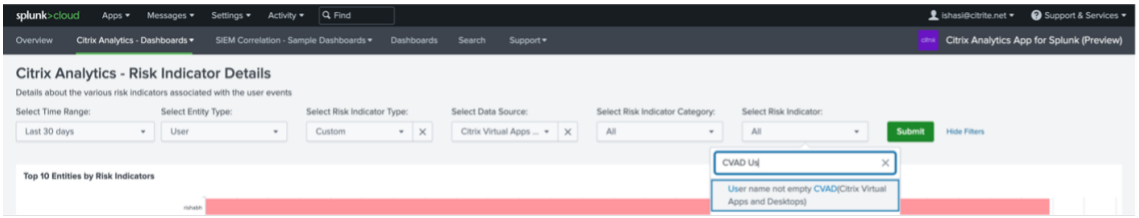
有关如何安装适用于 Splunk 的 Citrix Analytics 应用程序的指导，请参阅以下文章：

- 适用于 Splunk 的 Citrix Analytics 应用
- Splunk 的 Citrix Analytics 控制板

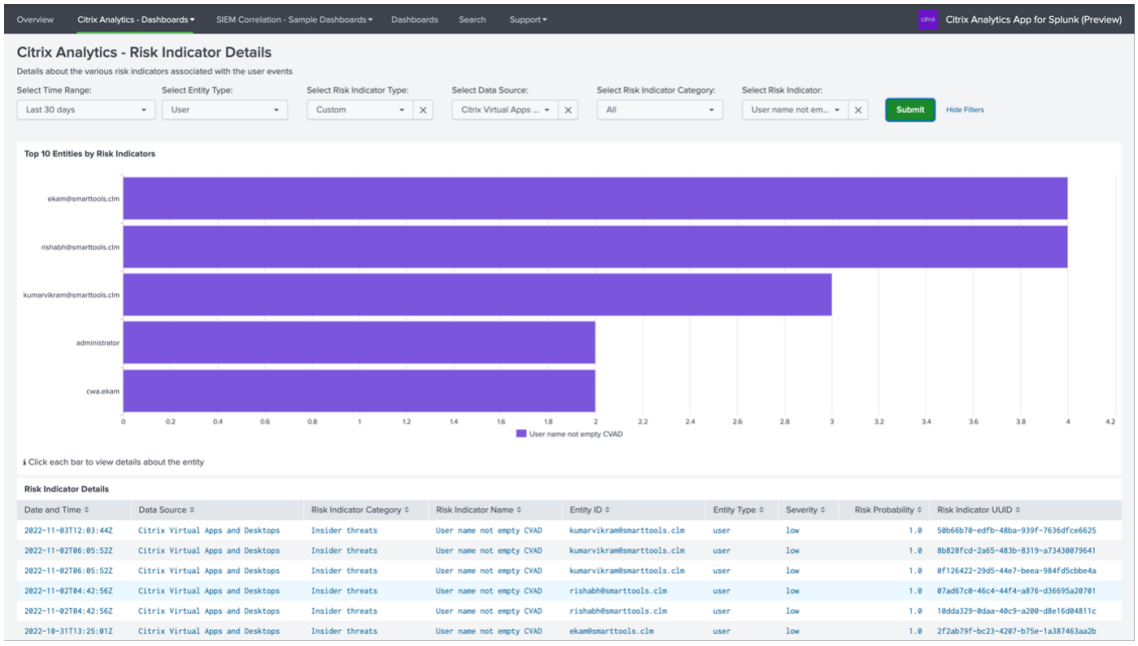
1. 单击 **Citrix Analytics** —控制面板 选项卡，然后从下拉列表中选择“风险指标详细信息”选项。



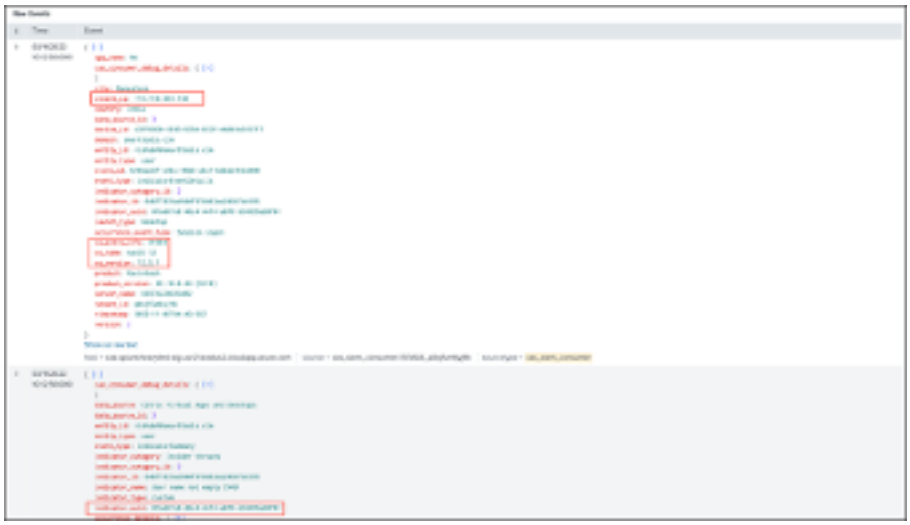
2. 从下拉列表中适当筛选内容，然后单击“提交”。



3. 单击用户实例以获取详细信息。



4. 您可以在此页面底部查看客户端 **IP** 和操作系统信息（名称、版本、其他信息）：

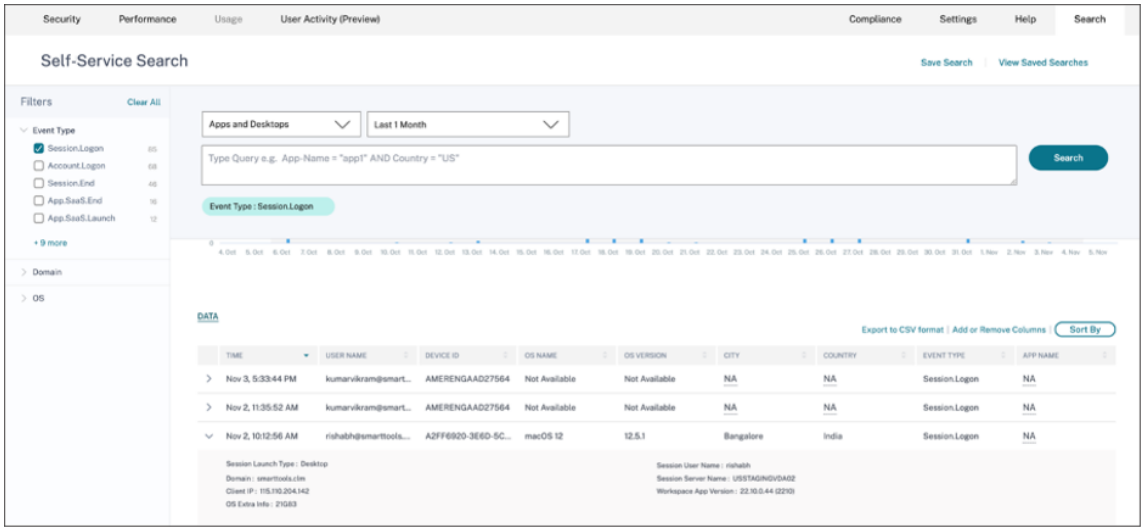


数据源事件

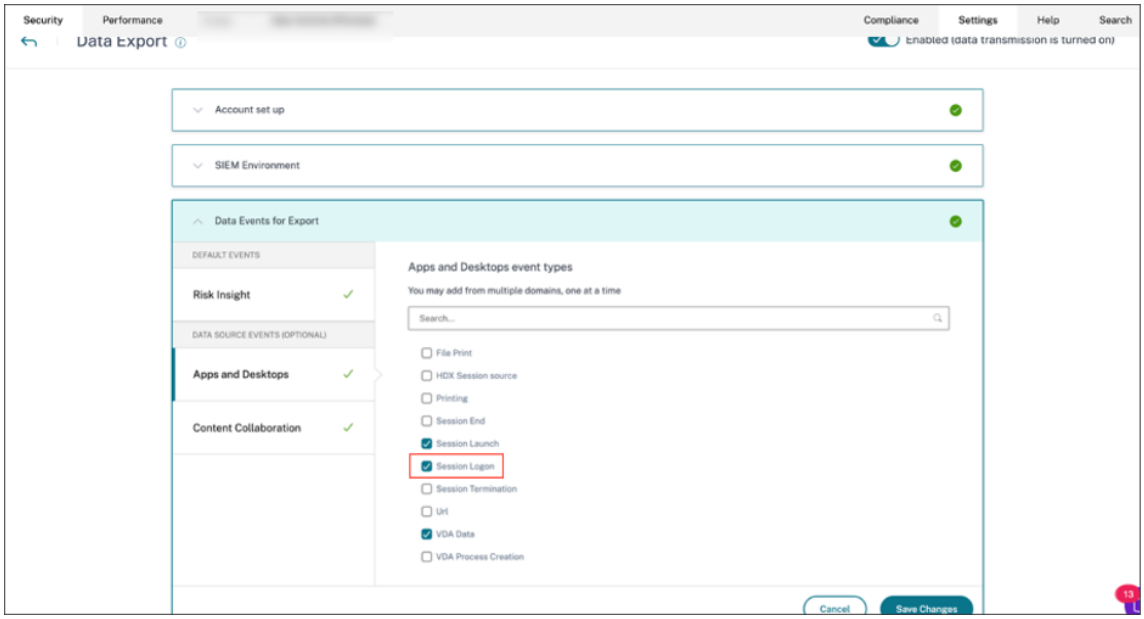
在 Splunk 环境中获取客户端 IP 和操作系统详细信息的另一种方法是配置要导出的数据源事件。此功能允许在自助搜索视图中出现的事件直接流入您的 Splunk 环境。有关如何为要导出到 SIEM 的 Virtual Apps and Desktops 配置事件类型的更多信息，请参阅以下文章：

- 数据事件从 Citrix Analytics for Security 导出到您的 SIEM 服务。
- 数据源事件

1. 导航到 **Citrix Analytics for Security** 控制板 **>** 搜索。在此自助搜索页面中，所有事件类型及其相关信息都可用。在以下屏幕截图中，您可以将 **Session.Logon** 事件类型作为示例：



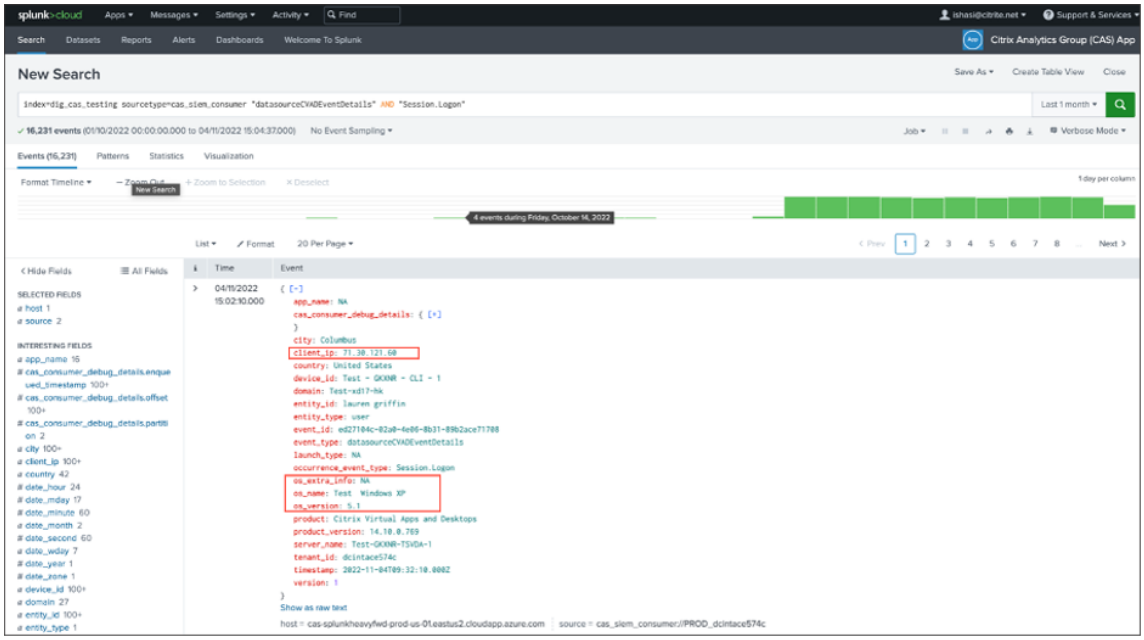
2. 将 **Session.Logonin** 数据源事件配置为导出，然后单击“保存”以使其流入您的 Splunk 环境。



3. 转到 Splunk 然后输入并运行以下查询：

```
index="<index you configured>" sourcetype="<sourcetype you
    configured>" "<tenant_id>" AND "datasourceCVADEventDetails" AND
     "Session.Logon"  AND "<user you' re interested in>"

<!--NeedCopy-->
```

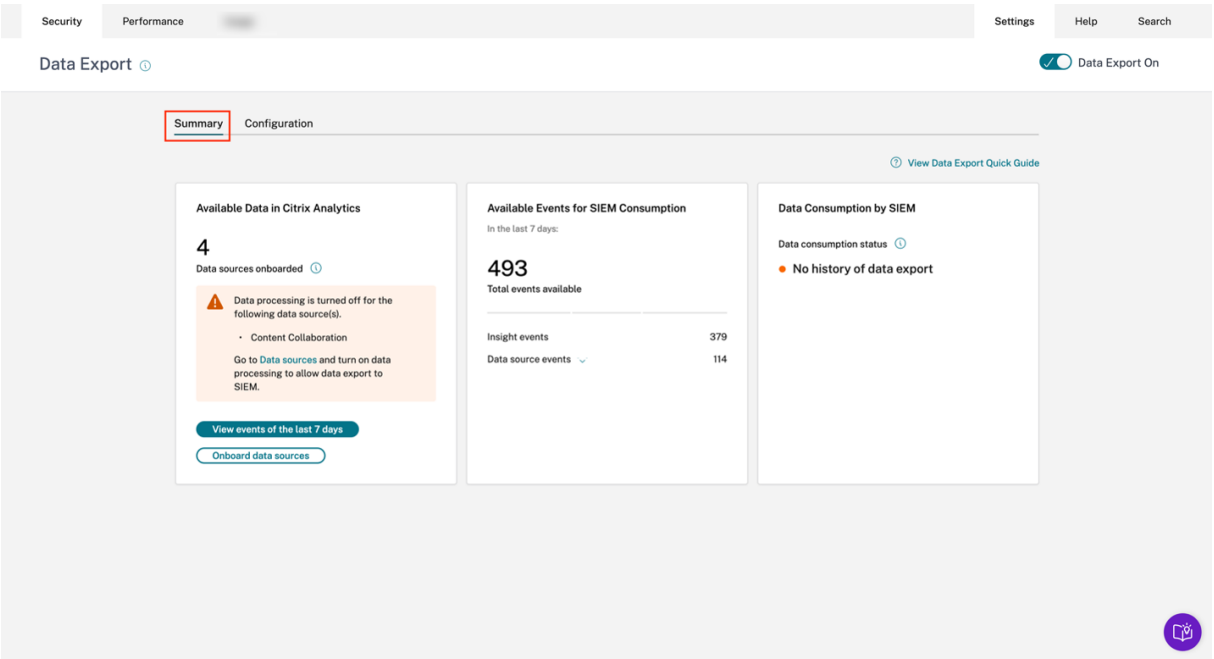
与客户端 IP 和操作系统相关的字段会突出显示。



数据导出故障排除

December 7, 2023

安全数据导出视图包含摘要选项卡，可帮助管理员解决其 SIEM 与 Citrix Analytics 的集成问题。摘要控制板通过有助于故障排除过程的检查点，让您可以查看数据的运行状况和流向。

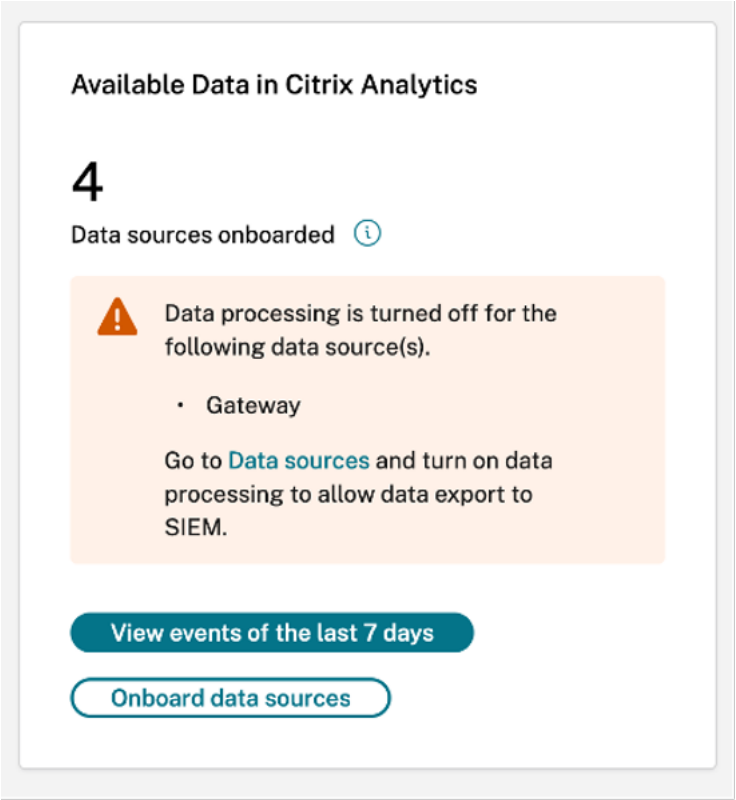


摘要选项卡

摘要 选项卡构成了“数据导出”视图中自助故障排除工作流程的基础。它使用以下三张卡来描述您的 SIEM 设置：

- **Citrix Analytics** 中的可用数据：此卡显示您的数据源配置的状态。
- 可用于 **SIEM** 消费的事件：此卡显示您的 SIEM 环境已准备好使用的事件数量。
- **SIEM** 的数据消耗：此卡显示您的 SIEM 环境中数据流的状态。

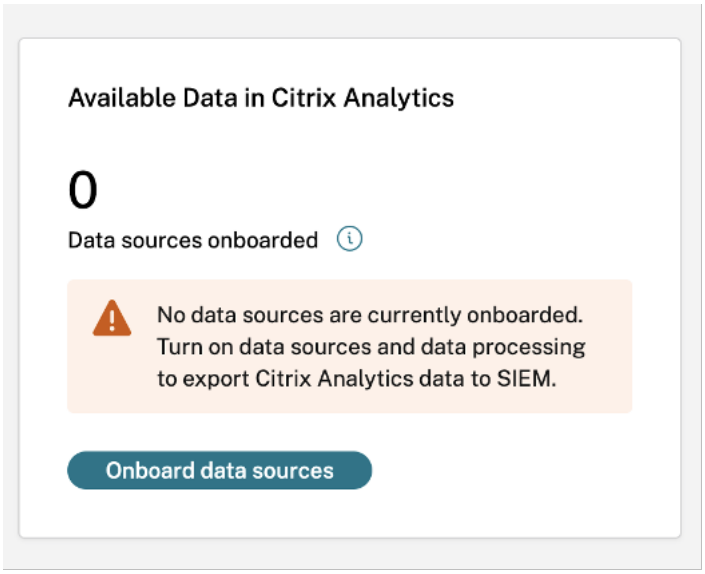
Citrix Analytics 中的可用数据



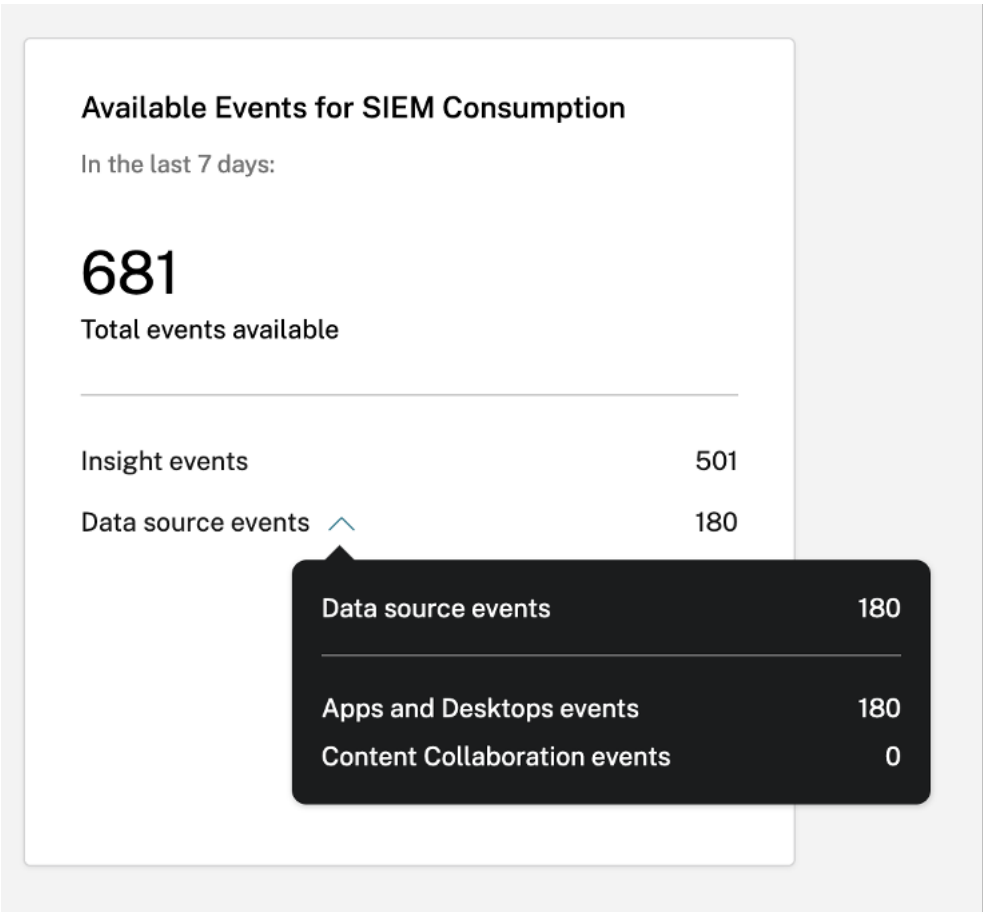
Citrix Analytics 中的可用数据 卡显示了最终可为 Citrix Analytics for Security 提供的 SIEM 见解的数据源的数量。目前支持三个数据源进行数据导出：应用程序和桌面、网关和安全私有访问。即使这些数据源已加载，对于已关闭数据处理的数据源，数据导出也不会起作用。检测到此类数据源时，会显示相应的警告消息，例如上图所示的警告。

查看最近 **7** 天的事件 按钮可将管理员重定向到自助搜索视图，管理员可以通过该视图验证事件是否已流入 Citrix Analytics for Security。“载入数据源”按钮重定向到“数据源”视图，您可以在其中深入了解入职流程。

如果没有载入的数据源，则会显示相应的警告消息，如以下屏幕截图所示：



适用于 **SIEM** 消费的可用活动



SIEM 消费的可用事件 卡显示预计将流入您的 SIEM 环境的洞察和数据源事件的数量及其细分。扩展后，还可以进一步细分每种类型的导出数据事件。

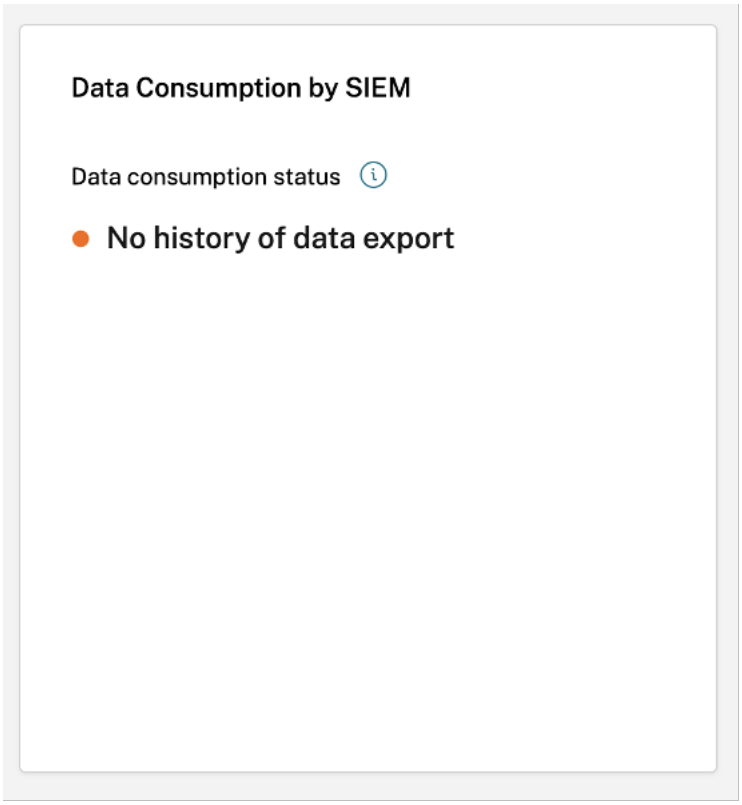
SIEM 的数据消耗

SIEM 的数据消耗量 卡描述了 Citrix Analytics 准备的数据流到您的 SIEM 环境的运行状况。数据消耗状态基于您的 **Kafka** 主题内的偏移量。如果可用，该卡还会显示上次检测到成功数据消耗的时间戳。数据消耗状态和时间戳每隔 10 分钟刷新一次。单击 此处 了解有关 Kafka 消费者群体/抵消量管理的更多信息。

数据消耗状态可以呈现以下状态：

1. 非活跃消费

   - 没有数据导出历史记录：此状态由橙色圆点表示，表示 Citrix Analytics 准备的任何数据从未成功传送到您的 SIEM 环境。



   这可能是由于-

   – 数据源配置不正确/不完整。**Citrix Analytics** 卡中的可用数据 可用于验证是否有足够的数据源，以及它们是否已开启数据处理以允许导出。

   – 缺乏用户活动。**Citrix Analytics** 卡中的可用数据中的“查看最近 **7** 天的事件”按钮可用于验证是否存在用户活动。此外，**SIEM** 消费的可用事件 卡可用于验证 Citrix Analytics 是否准备好流入您的 SIEM 的任何洞察或数据源事件。

   – SIEM 设置不正确/不完整。验证“配置”选项卡中的“帐户设置”阶段是否已成功完成。如果设置完成，则在帐户设置阶段会出现绿色勾号。

     如果即使在成功设置帐户后状态仍未改变，请通过检查以下内容进一步排除故障：

  * 防火墙问题或 SIEM 设置配置错误-请参阅 设置 SIEM 环境。
  * Kafka 帐户设置或您的 SIEM 环境存在凭据问题—请参阅使用 Kafka 进行 SIEM 集成。

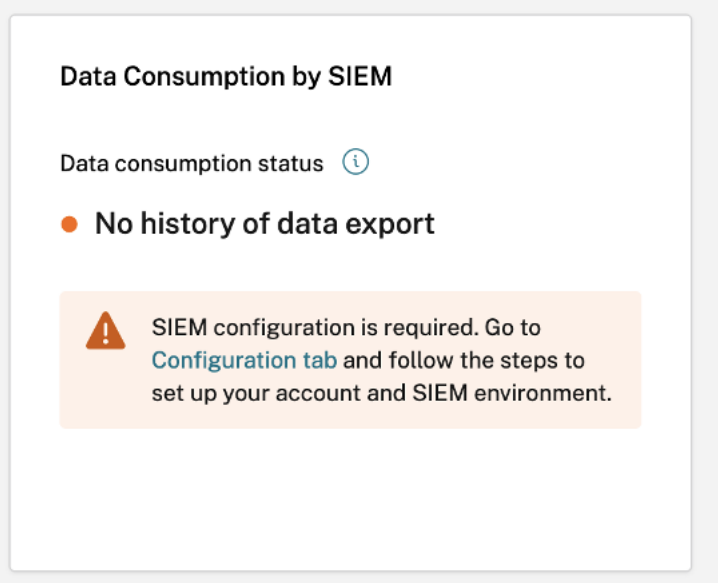
- 未检测到活跃消耗：此状态表示至少在过去 10 分钟内，数据未成功流入您的 SIEM 环境。该卡片还将显示上次成功移动数据的时间戳。与“无数据导出历史记录”一样，您可以使用 **Citrix Analytics** 中的可用数据 和 SIEM 消费卡的 可用事件对此进行 故障排除。如果有足够的用户活动且可用事件数量增加，则最好将重点放在最后一次成功的时间戳上，以检查在所述时间戳之后是否发生了任何防火墙更改或密码轮换。

- **7** 天前导出：此状态表示上次检测到您的 SIEM 上的活跃消费是在一周多以前。与上述两种状态类似，如果这是检测到的数据消耗状态，请使用 **Citrix Analytics** 中的可用数据和 **SIEM** 消费卡的可用事件对 SIEM 设置进行故障排除。

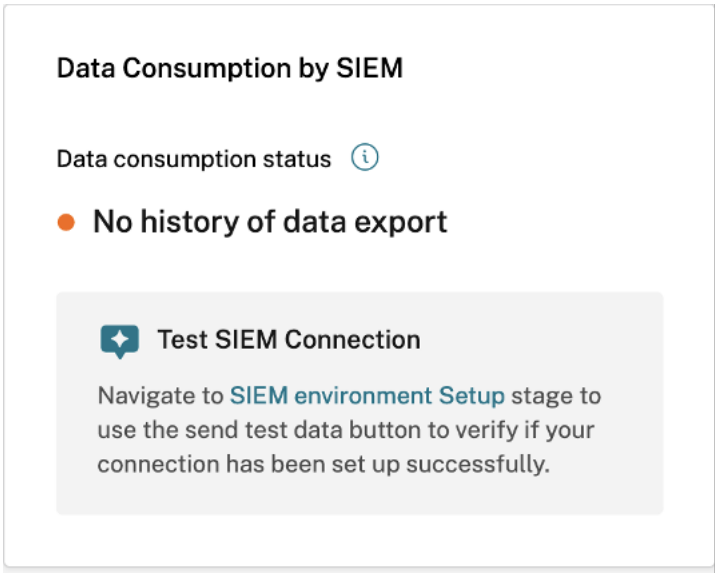
> 注意
>
> **Kafka** 保留策略：Citrix Analytics Kafka 主题最多只能保留活动 7 天。为避免或防止潜在的数据丢失，建议将数据轮询间隔设置为不超过 7 天。

在非活跃消费中，您可以查看以下警告消息，以帮助您完成故障排除过程。

正如“无数据导出历史记录”案例中所强调的那样，如果 SIEM 设置未完成，则不会有数据流入 SIEM 环境。因此，用户被重定向到“配置”选项卡以完成帐户设置，如以下屏幕截图所示：

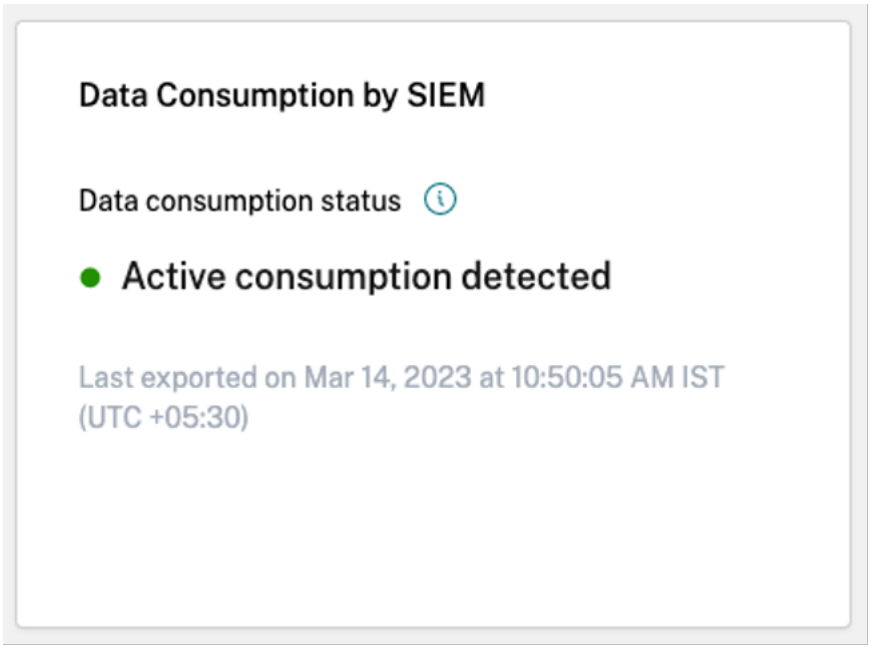


如果 SIEM 设置已完成，则仍可能出现数据不 活跃的情况，如 7 天前未检测到或导出活动消耗量 状态所示。因此，我们敦促用户转到“测试事件生成”部分，测试 SIEM 连接，如以下警告消息所示。



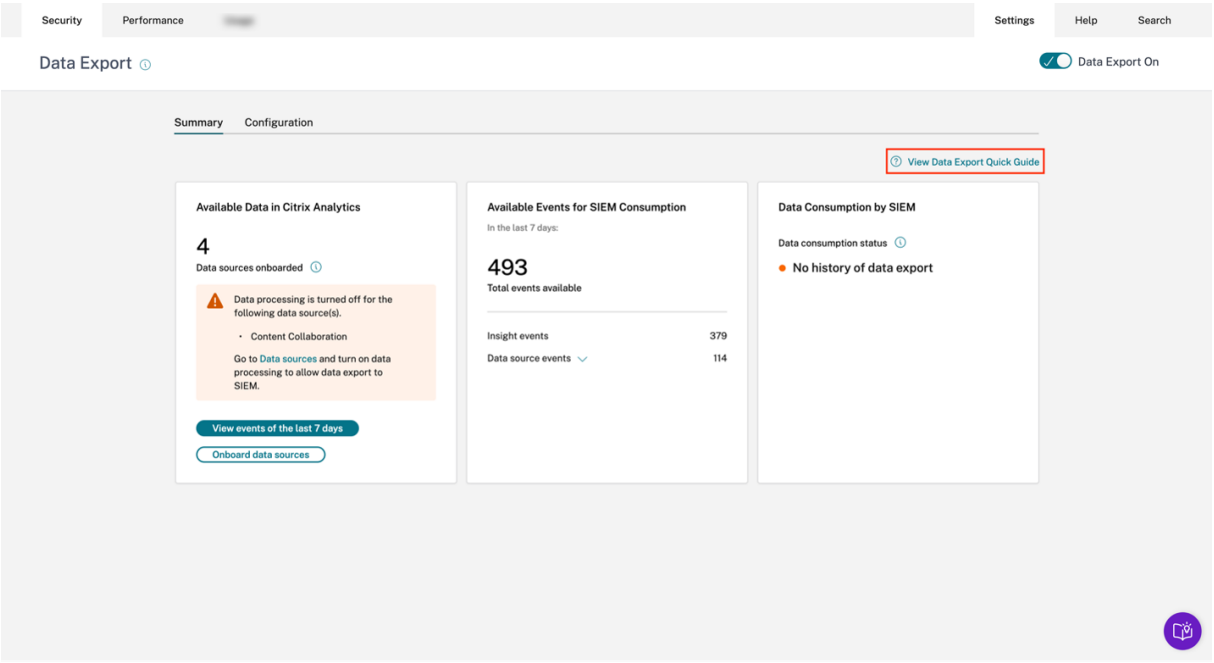
2. 主动消费

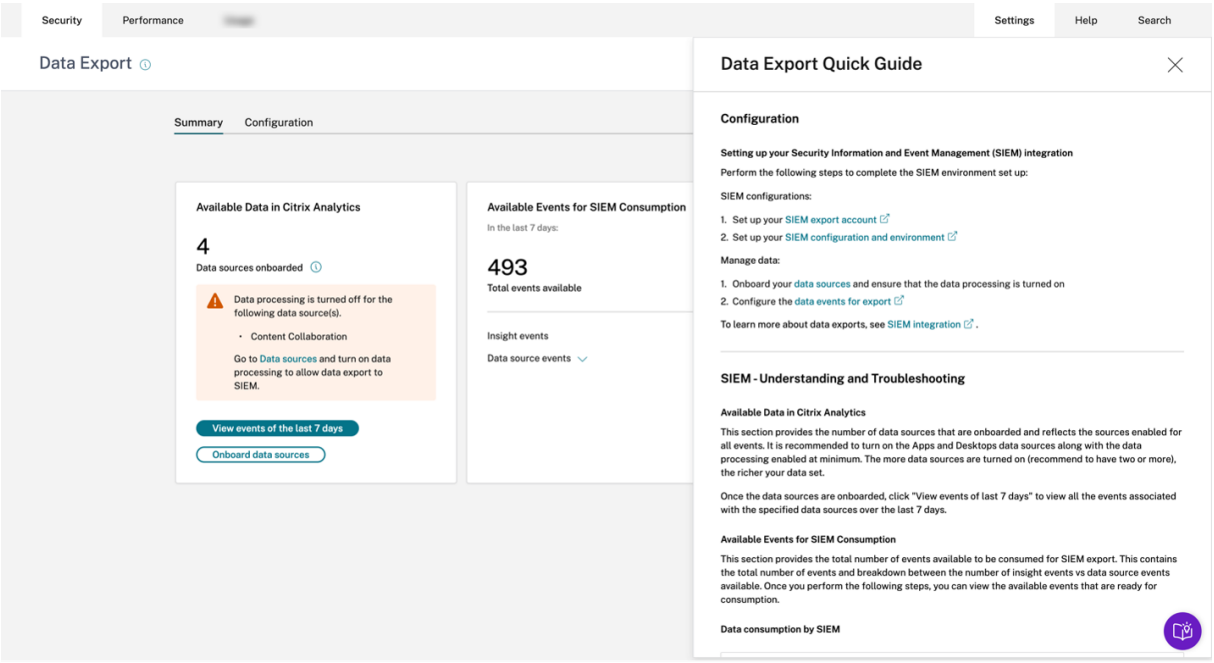
   - 检测到有效消费：此状态表示已在您的 SIEM 上检测到主动消费。

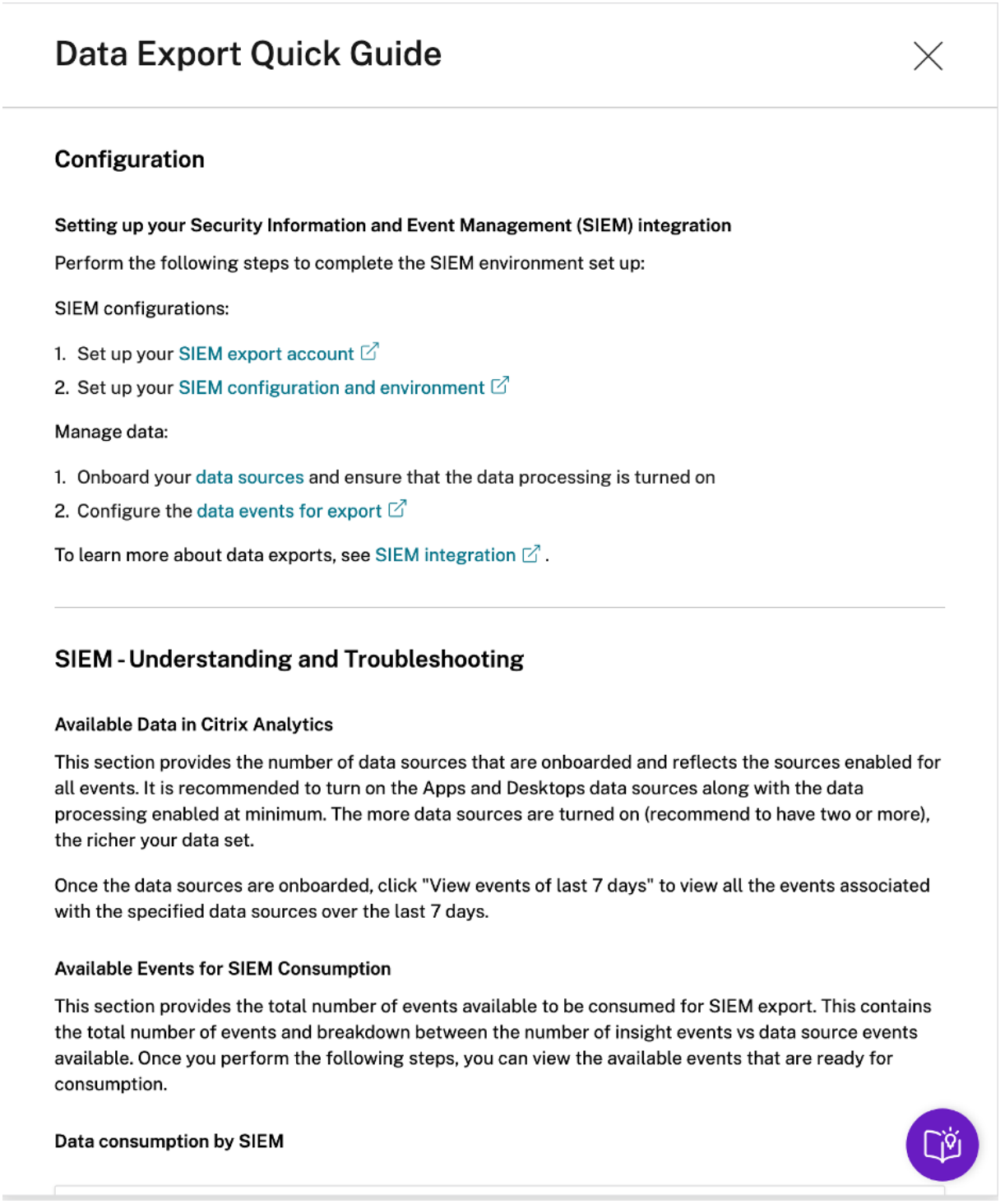


数据导出快速指南

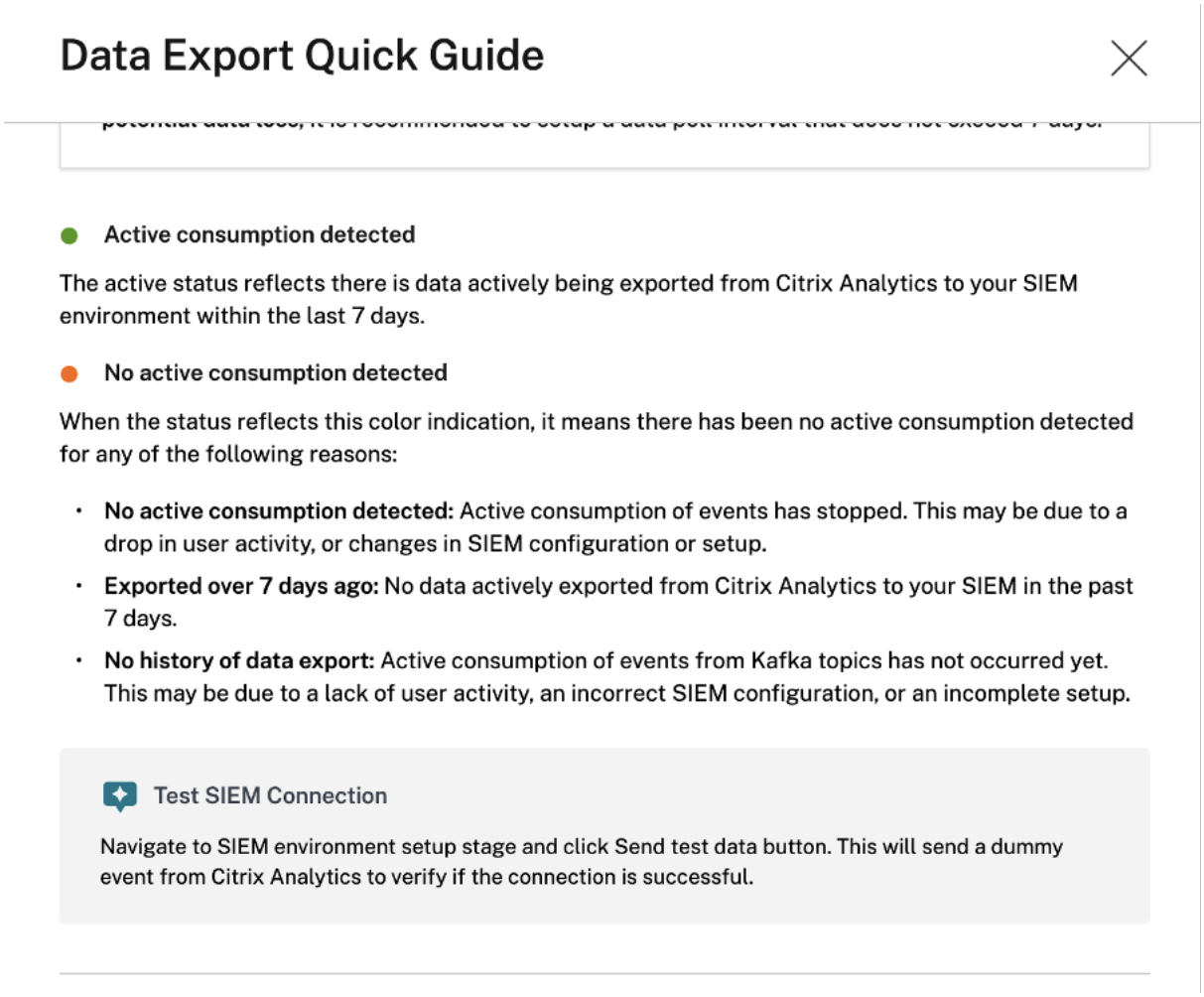
摘要 选项卡辅以 数据导出快速指南 刀片，可简化 SIEM 设置的部署、管理和故障排除。除了提供有关“数据导出安全性”视图的全面指南外，快速指南还通过提供相关文档的链接，包括有关如何设置和管理 SIEM 环境的有用提示。





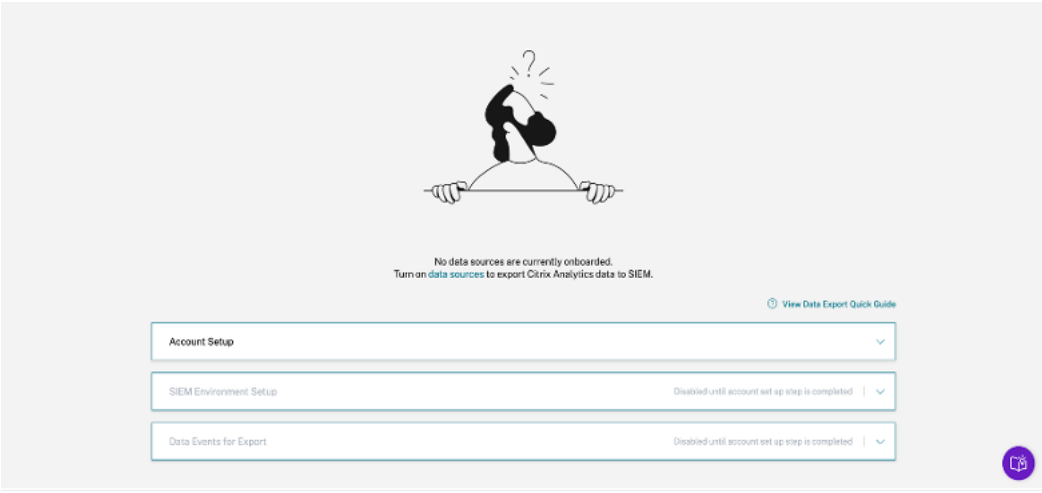


快速指南中还有一个“测试 **SIEM** 连接”部分，可将用户重定向到 SIEM 环境设置阶段中的“测试 SIEM 连接”阶段。这使用户能够调查 SIEM 集成本身是否已中断，从而排除 Citrix Analytics for Security 在处理事件时出现问题的可能性。然后，用户可以修复 SIEM 连接以启用数据流。

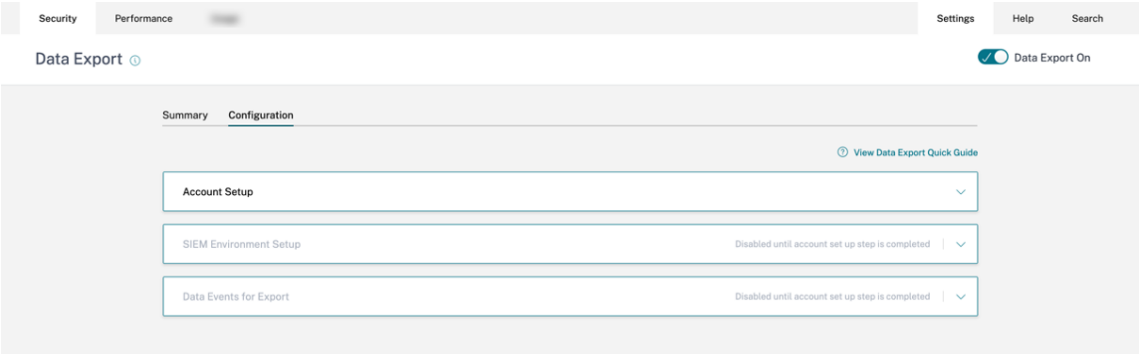


配置 选项卡在指导部署设置的同时，还可以帮助管理员在设置 SIEM 时提供有用的提示、警告消息和常见陷阱。在以下情况下会显示相应的警告：

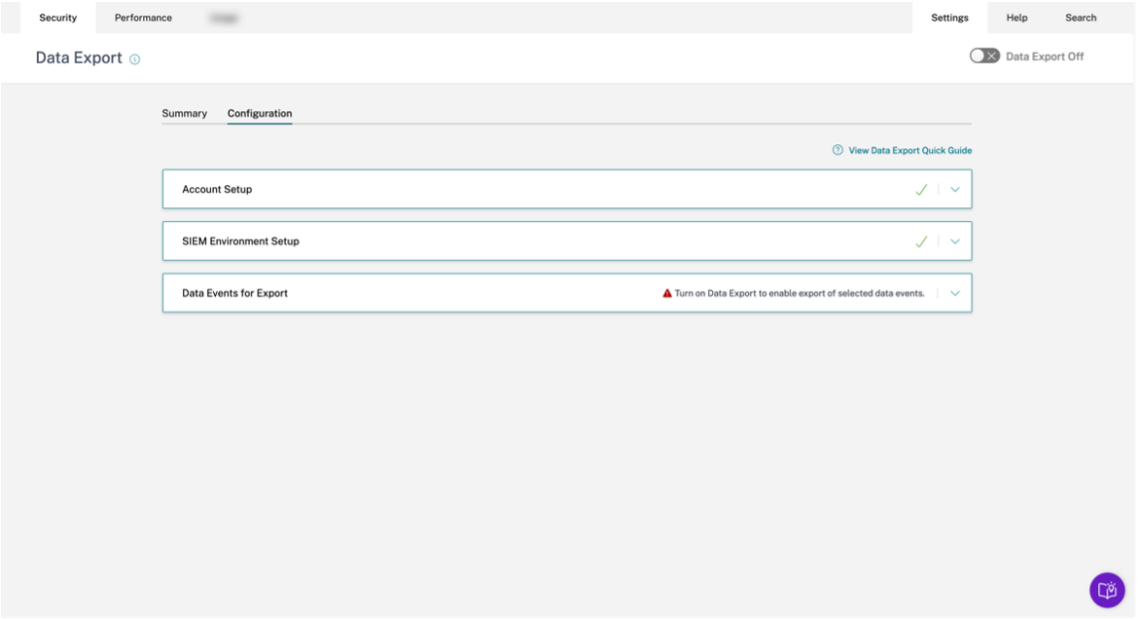
- Citrix Analytics 检测到尚未载入任何数据源。建议安装应用程序和桌面，以便根据用户活动收集遥测数据。在没有载入数据源的情况下，即使您的 SIEM 设置可能已成功完成，也不会观察到任何数据流。



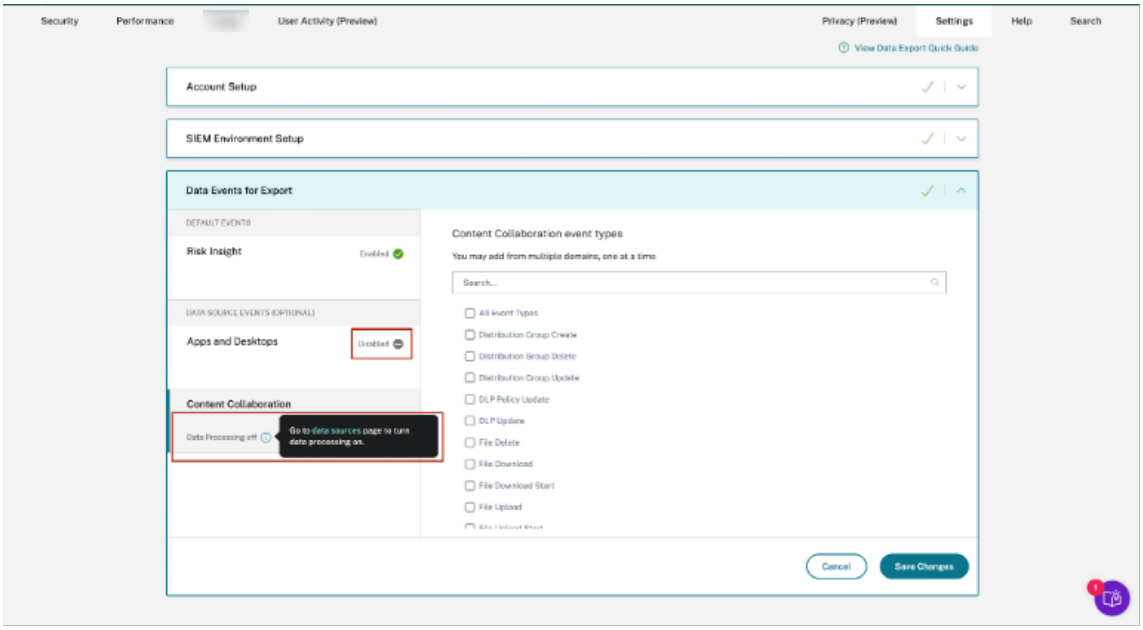
- 如下图所示，在成功完成账户设置之前，SIEM 环境设置和导出数据事件阶段将被禁用。



- 数据导出已关闭。导出数据事件阶段的警告旨在提醒用户启用“数据导出”以使所有更改生效。



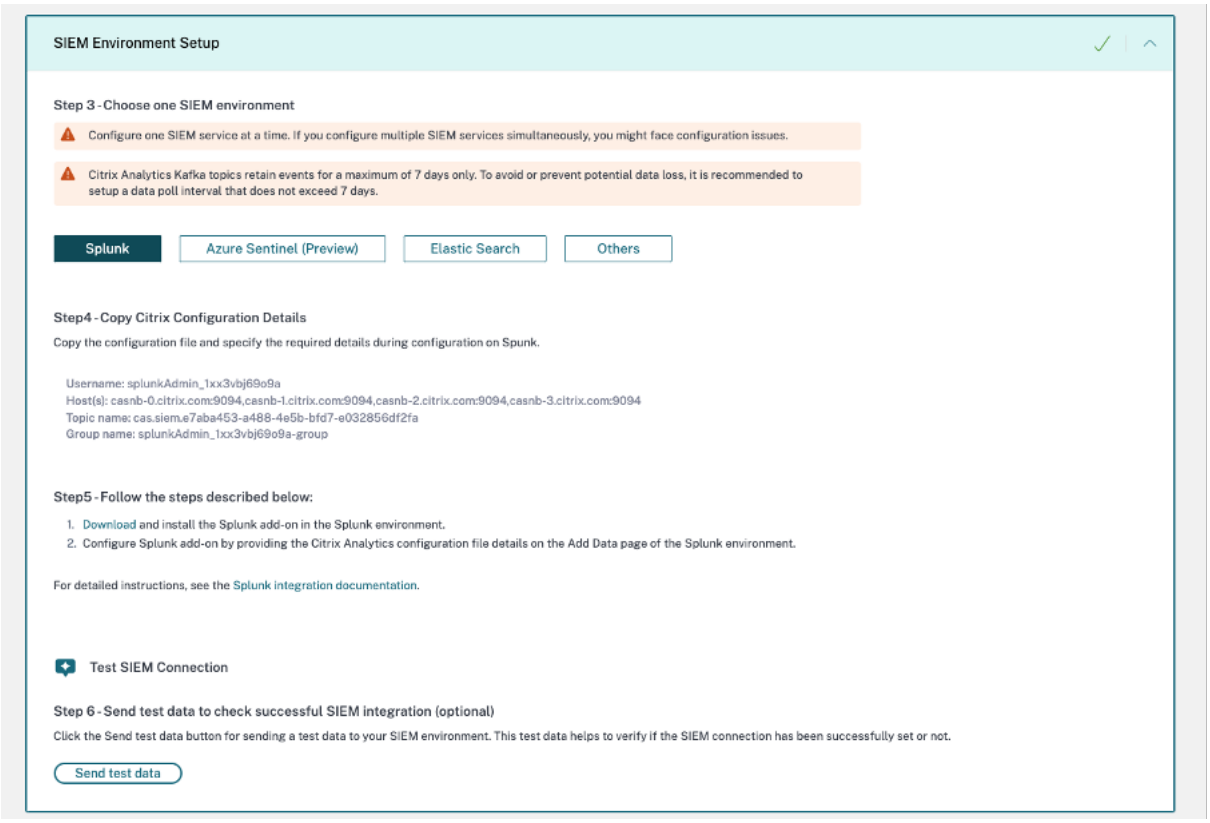
- 在“要导出的数据事件”阶段，如果禁用了特定数据源的数据导出，则不会有数据源事件流向 SIEM。必须通过配置和选择所需的数据源事件类型来启用此功能。此外，请确保启用相应数据源的数据处理，以确保数据到达 Citrix Analytics。



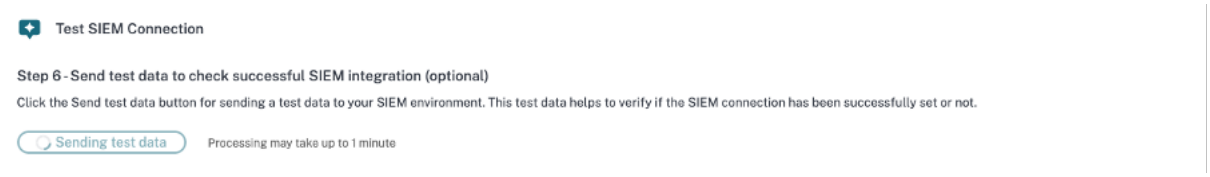
测试事件生成

测试事件生成是作为 **SIEM** 环境设置 阶段的一部分提供的，旨在增强故障排除体验。用户完成 SIEM 设置后，生成测试事件提供了一种通过将测试事件直接发送到客户的 SIEM 数据导出 Kafka 主题来快速测试 SIEM 连接的方法。

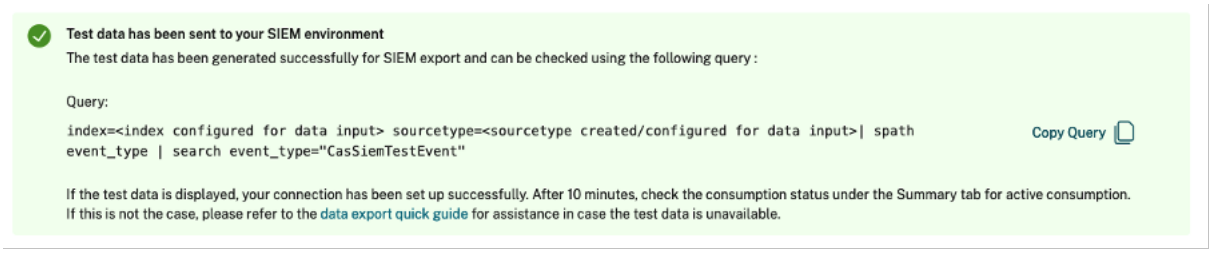
它还使新用户能够快速测试他们的 SIEM 与 Citrix Analytics 的集成，无需明确加入新的数据源并随后生成用户活动。

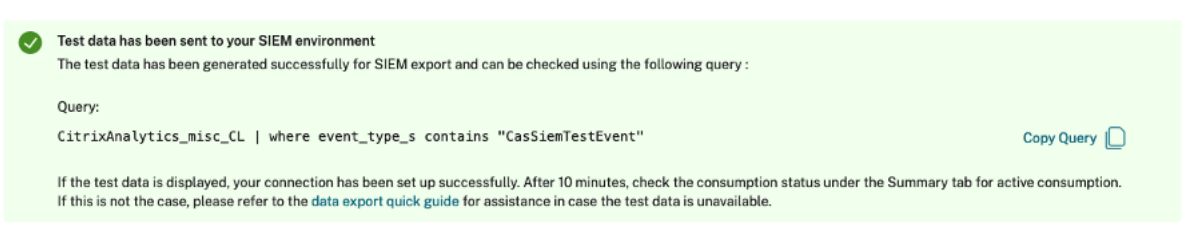


要测试此功能，用户需要单击“发送测试数据”按钮。这会生成一个虚拟测试事件并将其发送到客户的 SIEM 数据导出 Kafka 主题。此测试事件生成过程最多可能需要 1 分钟，如以下屏幕截图所示：

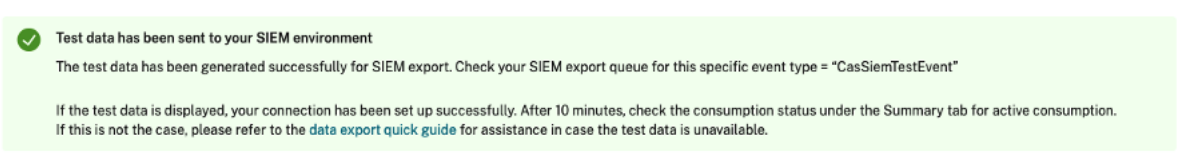


如果在客户 Kafka 主题中成功写入测试事件数据，则会显示一条成功消息，表明 SIEM 连接成功。根据您选择的环境（Splunk 和 Sentinel），管理员可以复制查询并检查其 SIEM 环境中是否有测试事件。

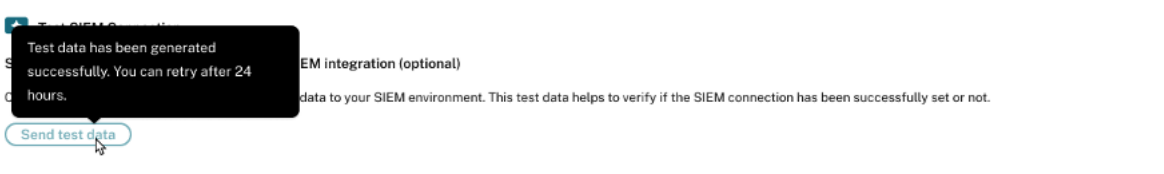




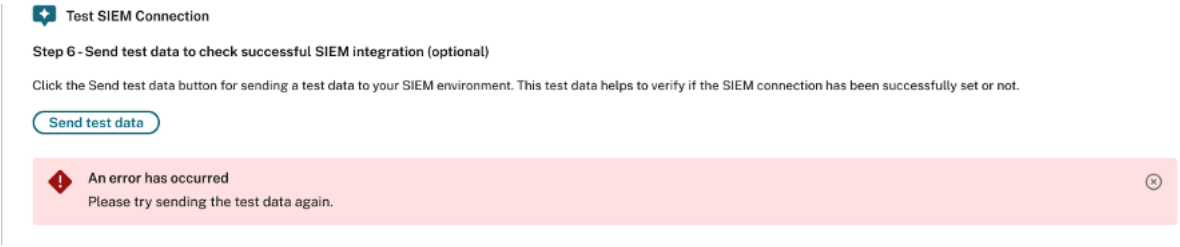
对于 Elasticsearch 和其他环境，将显示以下成功消息。



> 注意
>
> 生成测试事件后，“发送测试数据”按钮将在接下来的 24 小时内禁用，用户将鼠标悬停在该按钮上时会看到以下弹出窗口。距离最近的成功时间戳 24 小时后，该按钮将启用，供用户再次测试功能。



如果测试事件数据未成功写入客户 Kafka 主题，则会显示一条失败消息，如以下屏幕截图所示。用户可以再次发送数据来测试连接。



SIEM 电子邮件提醒

Citrix Analytics 会发送电子邮件警报，通知管理员有关可能导致其 SIEM 环境数据流中断的情况。它包含有关可能导致临时/永久安全姿势数据丢失的活动的情境信息。它还有助于顺利完成 SIEM 数据导出的自助故障排除之旅。

这组电子邮件警报的一些重要属性可帮助您在收件箱中找到相同的内容：

- 该邮件分发给 Citrix Cloud 管理员、安全完全管理员、安全只读管理员以及安全和性能只读管理员。
- 发件人是 Citrix Cloud **donotreplynotifications@citrix.com**。
- 主题行是：

- **SIEM** 数据导出警报 **-** 密码已重置，密码已重置电子邮件警报。
- **SIEM** 数据导出警报 **-** 数据流已停止，数据流已中断电子邮件警报。

如何启用电子邮件通知

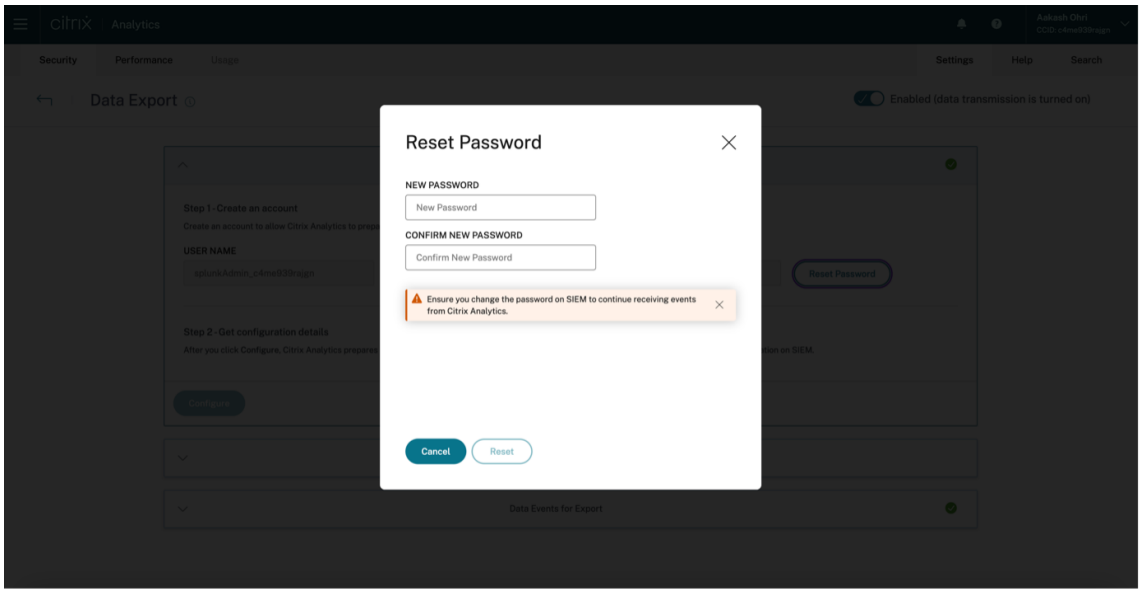
如果您是具有管理安全分析的自定义访问权限（安全完全管理、安全只读管理、安全和性能只读）的 Citrix Cloud 管理员，则始终会为您的 Citrix Cloud 帐户启用电子邮件通知。默认情况下，每周电子邮件通知会发送到 Citrix 安全管理员-默认列表。您也可以修改接收此警报的分发列表。有关更多信息，请参阅。

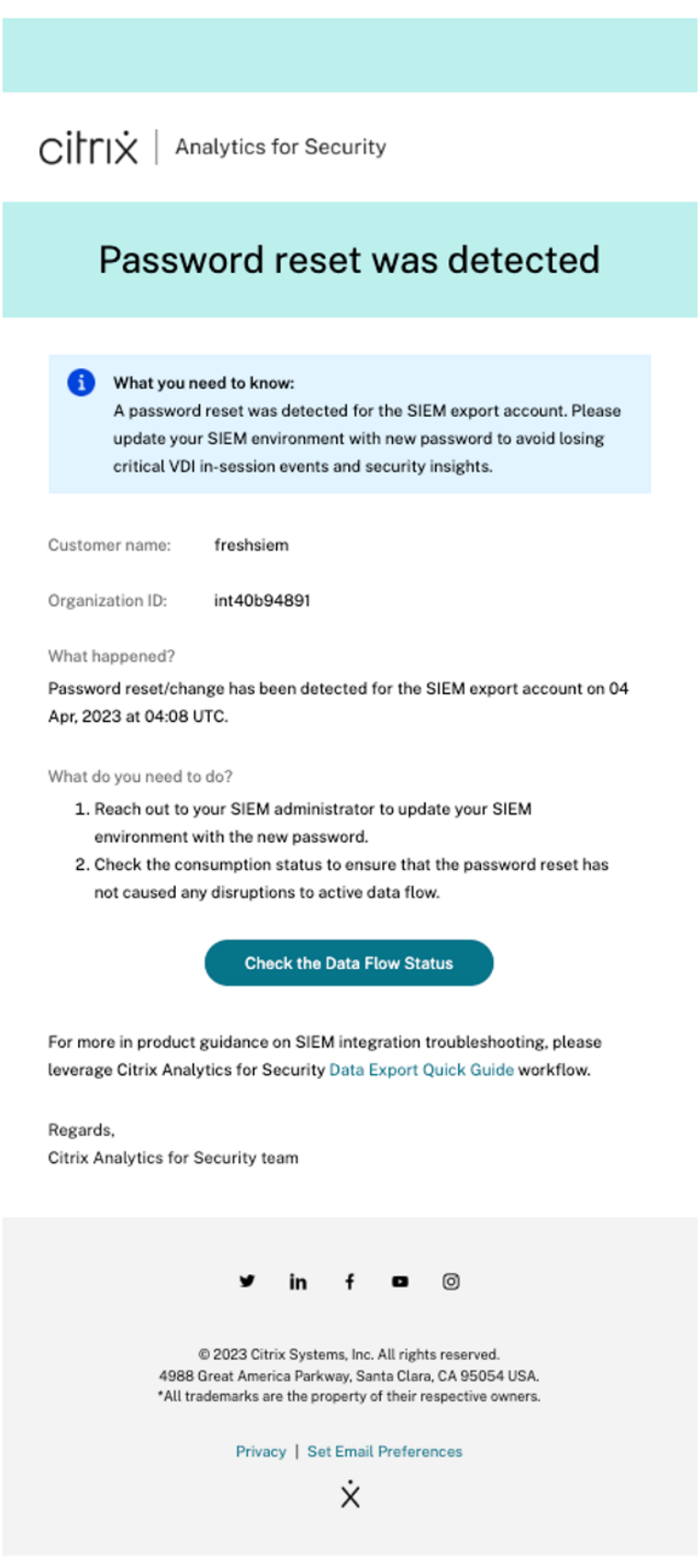
如果您是 Citrix Cloud 管理员，拥有管理 Security Analytics 的自定义访问权限（安全完全权限管理员、安全只读管理员、安全和性能只读），则始终为您的 Citrix Cloud 帐户启用电子邮件通知。

SIEM 电子邮件警报的类型

1. **SIEM** 密码重置电子邮件提醒

   通过“数据导出”页面重置帐户密码时，会收到 SIEM 密码重置提醒电子邮件。仅在 Citrix Analytics 用户界面上重置 SIEM 密码就可能导致密码与在 SIEM 上配置的密码不匹配。这会导致数据流中断。此电子邮件警报包含密码重置的时间。如果数据流停止，则可以转到“摘要”选项卡，检查“上次导出时间”的时间戳是否接近密码重置时间戳，然后转发必要的密码更改。这缩短了调试过程，帮助您立即成功恢复数据流入 SIEM 环境的状态。





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. 数据流中断 **24** 小时电子邮件提醒

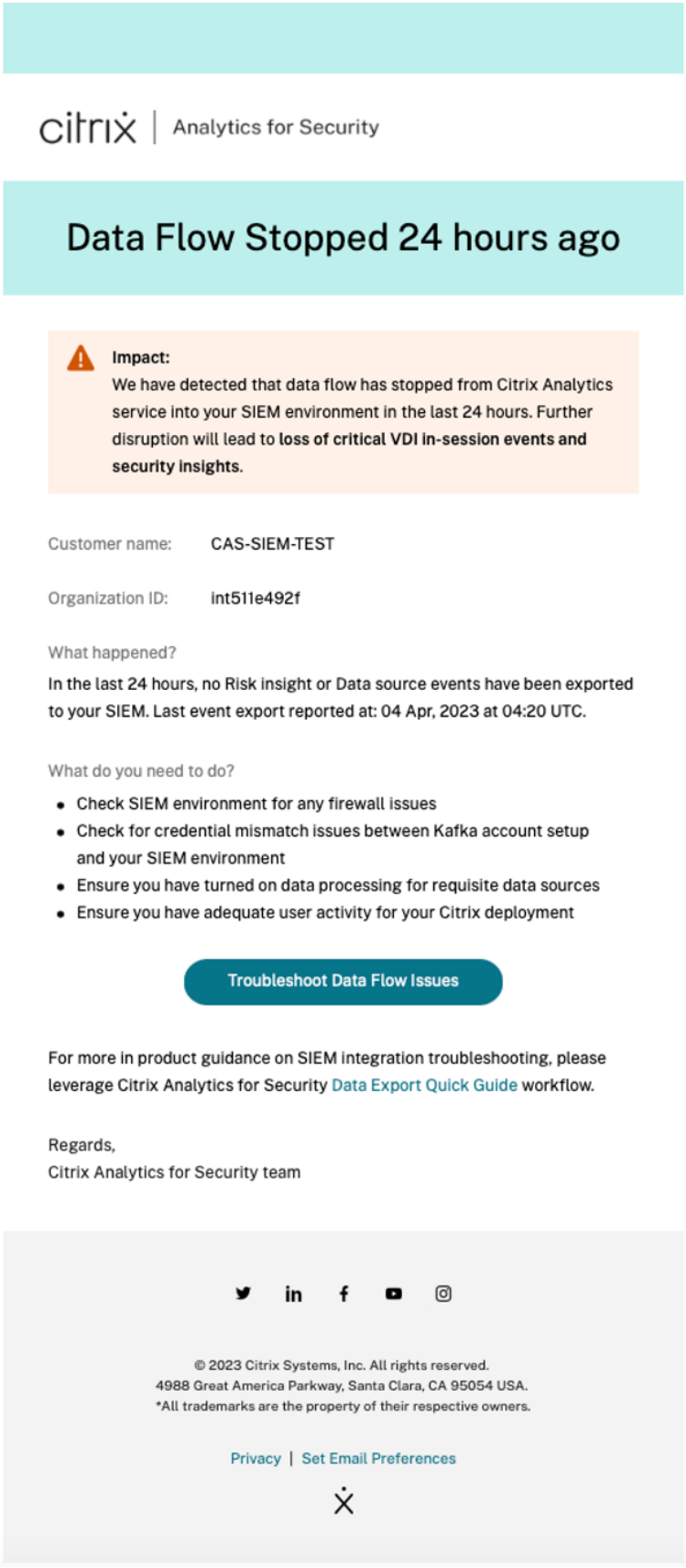
   当从 Citrix Analytics 服务流入您的 SIEM 环境的数据流中断超过 24 小时时，就会发送此电子邮件提醒。该电子邮件包括上次事件的导出时间以及有用的故障排除快速提示，这些提示可以用来恢复数据流。这是快速恢复数据流的正确时机，这样就不会丢失任何经过安全处理的数据。

3. 数据流中断 **7** 天电子邮件提醒

   当从 Citrix Analytics 服务流入您的 SIEM 环境的数据流中断超过 7 天时，就会发送此电子邮件提醒。由于客户的 Kafka 主题的保留期为 7 天，因此务必要遵循故障排除提示并借助“数据导出”页面上提供的快速指南，以免丢失任何其他数据，因为此电子邮件警告安全状态信息将永久丢失。

4. 数据流中断 **30** 天电子邮件提醒

   当从 Citrix Analytics 服务流入您的 SIEM 环境的数据流中断超过 30 天时，就会发送此电子邮件提醒。到目前为止，客户已经丢失了安全姿势数据，必须使用故障排除功能尽快恢复流程。



citrix | Analytics for Security

Data Flow Stopped 24 hours ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in the last 24 hours. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 24 hours, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 04 Apr, 2023 at 04:20 UTC.

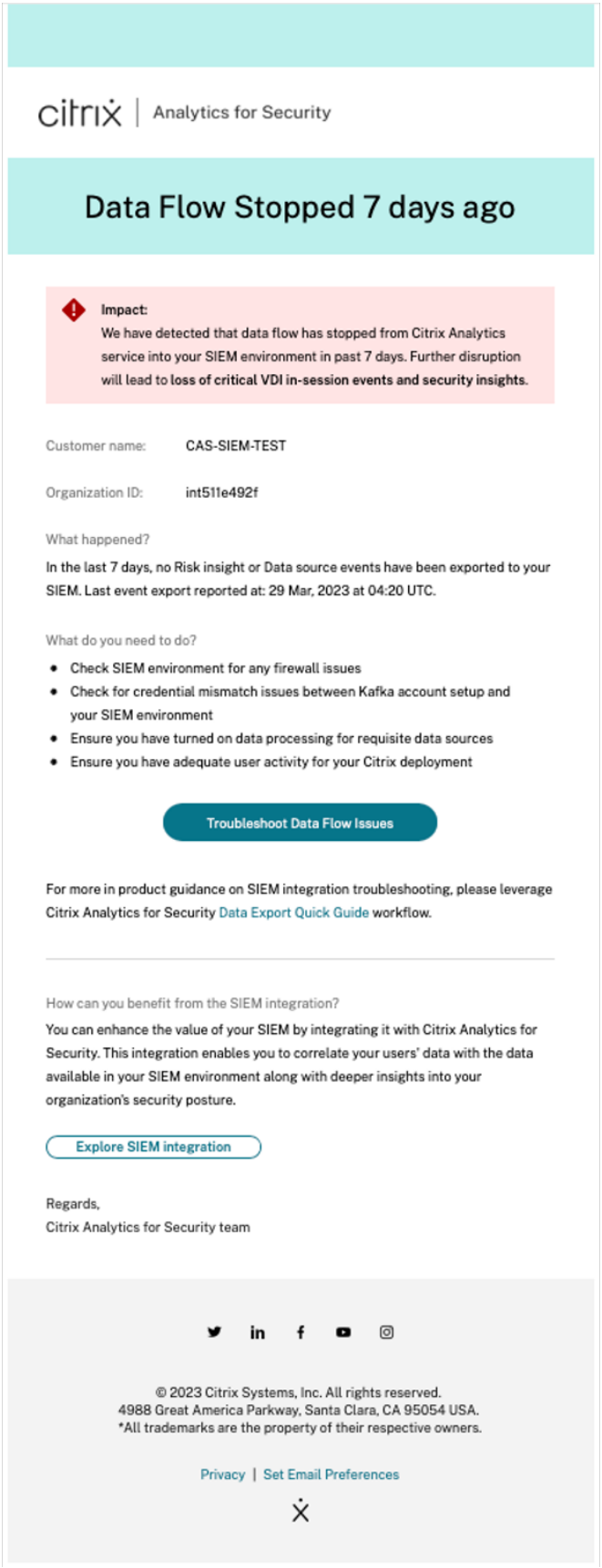
What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

Regards,
Citrix Analytics for Security team



citrix | Analytics for Security

Data Flow Stopped 7 days ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in past 7 days. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 7 days, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 29 Mar, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

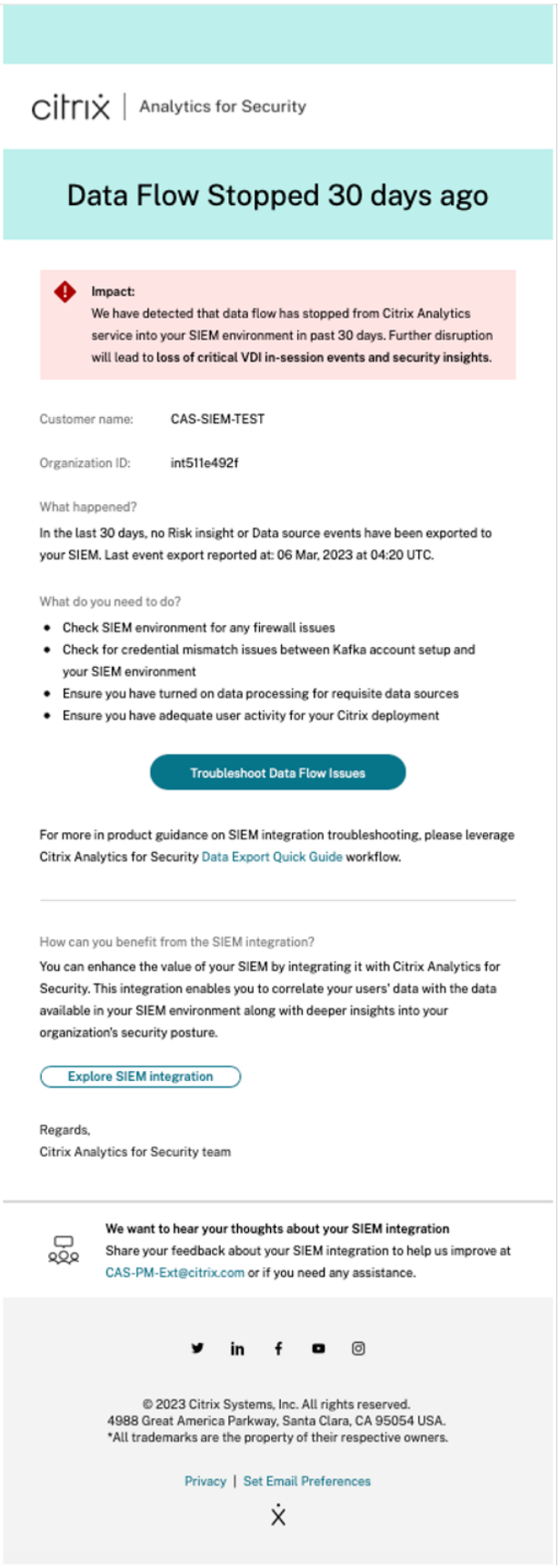
For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

How can you benefit from the SIEM integration?

You can enhance the value of your SIEM by integrating it with Citrix Analytics for Security. This integration enables you to correlate your users' data with the data available in your SIEM environment along with deeper insights into your organization's security posture.

Explore SIEM integration

Regards,
Citrix Analytics for Security team



citrix | Analytics for Security

Data Flow Stopped 30 days ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in past 30 days. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 30 days, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 06 Mar, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

How can you benefit from the SIEM integration?

You can enhance the value of your SIEM by integrating it with Citrix Analytics for Security. This integration enables you to correlate your users' data with the data available in your SIEM environment along with deeper insights into your organization's security posture.

Explore SIEM integration

Regards,
Citrix Analytics for Security team

We want to hear your thoughts about your SIEM integration
Share your feedback about your SIEM integration to help us improve at CAS-PM-Ext@citrix.com or if you need any assistance.

安全洞察的 **Sigma** 签名示例

December 7, 2023

本页包含示例查询，可帮助管理员使用 Citrix Security Analytics 取得有意义的结果。

这些示例涵盖以下类别的风险：

- 受损的端点
- 内幕威胁
- 数据泄露

如何使用这些示例

查看数据源并开启数据处理

要查看数据源，请在 Citrix Analytics GUI 中单击“设置” **>** “数据源” **>** “安全”。应用程序和桌面 **- Workspace** 应用程序站点卡显示在“数据源”页面上。单 击打开数据处理 以允许 Citrix Analytics 开始处理此数据源的数据。

Citrix Analytics for Security 将以下两种类型的风险洞察数据发送到您的 SIEM 服务：

- 风险洞察事件（默认导出）
- 数据源事件（可选导出）

作为 SIEM 环境的一部分，风险洞察事件数据源可用且默认情况下始终处于打开状态。有关更多信息，请参阅 从 Citrix Analytics for Security 导出到您的 SIEM 服务的数据事件。

您可以使用 CAS 或 Sigma 签名来验证数据源中的任何特定用户事件。CAS 查询可通过 Citrix Analytics GUI 上的“自助搜索”页面进行访问。Sigma 签名以简单或用户友好的格式编写，使其与各种 SIEM 环境兼容。

使用 **CAS** 查询

您可以使用“自助搜索”页面下的 CAS 查询来查找和筛选从各种数据源收到的用户事件。在 Citrix Analytics GUI 中单击“搜索”，然后在搜索框中输入查询。有关更多详细信息，请参阅如何使用自助搜索。

您还可以使用现有模板创建自定义风险指标。要创建自定义风险指标，请导航到安全 **>** 自定义风险指标 **>** 创建指标。有关更多详细信息，请参阅创建自定义风险指标。

使用 **Sigma** 签名

Sigma 是一种用户友好的开放签名格式，用于创建基于文本的查询，分析人员可以使用这些查询来描述日志事件，从而使检测结果更易于编写。有几种不同的方法可以将 Sigma 签名转换为 SIEM 工具的查询语言。

- 您可以使用 Sigma 提供的 CLI 工具和 Python SDK。有关 Sigma 签名的更多信息，请参阅规则用法。
- 您可以使用公共工具，例如 uncoder.io 的 Sigma 翻译引擎，它提供免费套餐。

有关不同的风险见解，请参阅以下不同的自定义指标用例：

- 未经批准的浏览器
- 未经批准的操作系统
- 未经批准的 Workspace 应用程序版本
- 允许列表之外的未授权操作系统
- 未经授权的 IP 地址或子网
- 未经授权的虚拟应用程序
- 不寻常的桌面名称
- 监视特定的应用程序
- 从 SaaS 应用程序打印
- 在 SaaS 应用程序上使用剪贴板

受损的端点

November 26, 2023

未经批准的浏览器

当用户尝试访问组织 IT 政策不允许的浏览器类型或版本的内容或由于安全漏洞而出现时，就会发生这种情况。

详细信息

数据源：应用程序和桌面（Workspace 应用程序）

CAS 查询

```
Event-Type = "Session.Logon" AND Browser-Name !~ "<Browser-Name>"
<!--NeedCopy-->
```

当用户输入其凭据并登录其应用程序或桌面会话时，Session.Logon 事件就会触发。

Sigma 签名

```
author: Citrix
date: 2023/01/31
description: This occurs when a user accesses content from an
    authorized browser which might cause an undesirable event or action
    through the internet.
detection:
  condition: index_selection and selection and not filter
  filter:
  - browser_name|contains: '<Browser-Name>'
  index_selection:
    source: cas_siem_consumer://<env>_<tenant_identifier>
  selection:
  - occurrence_event_type: Session.logon
logsource:
  product: citrixanalytics
  service: security
title: Access from unauthorized browser
<!--NeedCopy-->
```

未经批准的操作系统

当用户尝试访问您的组织 IT 政策不允许或存在安全漏洞的操作系统类型或版本的设备时，就会发生这种情况。

详细信息

数据源：应用程序和桌面（Workspace 应用程序）

CAS 查询

```
Event-Type = "Session.Logon" AND OS-Name ~ "<OS-Name>" AND OS-Version =
    "<OS-Version>" AND OS-Extra-Info = "<OS-Extra-Info>"
<!--NeedCopy-->
```

Sigma 签名

```
author: Citrix
date: 2023/01/31
description: This occurs when a user attempts to access apps from
    servers with blocked listed operating systems.
detection:
  condition: index_selection and selection
  filter_null: []
  index_selection:
```



```
    source: cas_siem_consumer://<env>_<tenant_identifier>
  selection:
    occurrence_event_type: Session.logon
    os_name|contains: '<OS-Name>'
    os_version: '<OS-Version>'
    os_extra_info: '<OS-Extra-Info>'
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized operating systems in block list
<!--NeedCopy-->
```

未经授权的 IP 地址或子网

当用户尝试从贵组织的 IT 策略标记为未授权的 IP 地址或范围进行访问时，就会发生这种情况。

详细信息

数据源：应用程序和桌面（Workspace 应用程序）

CAS 查询

```
Event-Type = "Session.Logon" AND Client-IP = "<XX.YY.ZZ.*>"
<!--NeedCopy-->
```

Sigma 签名

```
author: Citrix
date: 2023/01/31
description: This occurs when a user accessing content from an
    unauthorized IPs which might cause an undesirable event or action
    through the internet.
detection:
  condition: selection and not filter_null and filter
  filter:
  - client_ip: '<IP>'
  filter_null:
  - client_ip: null
  selection:
  - occurrence_event_type: Session.Logon
logsource:
  product: citrixanalytics
  service: security
title: Access from unauthorized IP
<!--NeedCopy-->
```


允许列表之外的未授权操作系统

当用户尝试从托管允许列表之外的操作系统的服务器访问应用程序时，就会发生这种情况。

详细信息

数据源：应用程序和桌面（Workspace 应用程序）

CAS 查询

```
Event-Type = "Session.Logon" AND OS-Name !~ "<OS-Name>" AND OS-Version
    != "<OS-Version>" AND OS-Extra-Info != "<OS-Extra-Info>"
<!--NeedCopy-->
```

Sigma 签名

```
author: Citrix
date: 2023/01/31
description: Unauthorized operating systems outside allow list
detection:
  condition: selection and not filter_null and not filter_os and not
     filter_os_version and not filter_os_extra
  filter_os:
  - os_name|contains: '<OS INFO>'
  filter_os_version:
  - os_version: '<OS Version>'
  filter_os_extra:
  - os_extra_info: '<OS Extra Info>'
  filter_null:
  - os_name: null
  - os_version: null
  - os_extra_info: null
  selection:
  - occurrence_event_type: Session.Logon
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized operating systems outside allow list
<!--NeedCopy-->
```

未经批准的 **Workspace** 应用程序版本

当用户尝试访问不支持的客户端版本的 Workspace 应用程序版本时，就会发生这种情况。在这种情况下，用户必须将其客户端升级到支持的版本。有关更多信息，请参阅 支持客户端版本。

详细信息

数据源：应用程序和桌面（Workspace 应用程序）

CAS 查询

```
Event-Type = "Session.Logon" AND Client-Type IN ("Windows", "Macintosh", "Unix/Linux") AND Workspace-App-Version != "20*" AND Workspace-App-Version != "21*"
<!--NeedCopy-->
```

Sigma 签名

```
author: Citrix
date: 2023/01/31
description: Unsupported Workspace app versions
detection:
  condition: selection and not filter_null and filter_product and not filter_product_version
  filter_product:
  - product: ['Windows', 'Mac', '<Other type>']
  filter_product_version:
  - product_version|contains: ['<Product Version1>', '<Product Version2>']
  filter_null:
  - product: null
  - product_version: null
  selection:
  - occurrence_event_type: Session.Logon
logsource:
  product: citrixanalytics
  service: security
title: Unsupported Workspace app versions
<!--NeedCopy-->
```

内幕威胁

November 26, 2023

不寻常的桌面名称

当用户尝试启动不正常的桌面时，就会发生这种情况。

详细信息

数据源：应用程序和桌面（Workspace 应用程序）

CAS 查询

```
Event-Type = "Session.Logon" AND Session-Launch-Type = "desktop" AND
    App-Name ~ "<Desktop Name>"
<!--NeedCopy-->
```

Sigma 签名

```
author: Citrix
date: 2023/01/31
description: Unusual desktop names
detection:
  condition: selection1 and selection2 and not filter_null and
     filter_app_name
  filter_app_name:
  - app_name|contains: '<App Name>'
  filter_null:
  - app_name: null
  selection1:
  - occurrence_event_type: Citrix.EventMonitor.AppStart
  selection2:
  - launch_type: 'desktop'
logsource:
  product: citrixanalytics
  service: security
title: Unusual desktop names
<!--NeedCopy-->
```

监视特定进程

当用户启动监视列表中的已发布应用程序时，就会发生这种情况。其目的可能是监视特定已发布应用程序的使用情况。

详细信息

数据源：应用程序和桌面 (Session Recording)

CAS 查询


```
Event-Type = "Citrix.EventMonitor.AppStart" AND App-Name IN ("<App-Name-1>", "<App-Name-2>")
<!--NeedCopy-->
```

Sigma 签名

```
author: Citrix
date: 2023/01/31
description: Monitor specific process
detection:
  condition: selection and not filter_null and filter_app_name
  filter_app_name:
  - app_name: ['<App-Name1>', '<App-Name2>']
  filter_null:
  - app_name: null
  selection:
  - occurrence_event_type: Citrix.EventMonitor.AppStart
logsource:
  product: citrixanalytics
  service: security
title: Monitor specific process
<!--NeedCopy-->
```

未经授权的虚拟应用程序

当用户访问未经授权的虚拟应用程序时，就会发生这种情况。

详细信息

数据源：应用程序和桌面（Workspace 应用程序）

CAS 查询

```
Event-Type = "App.Start" AND App-Name IN ("<App-Name1>", "<App-Name2>")
<!--NeedCopy-->
```

Sigma 签名

```
date: 2023/01/31
description: Unauthorized virtual apps
detection:
  condition: selection and not filter_null and filter_app_name
  filter_app_name:
```



```
  - app_name: ['<App-Name1>', '<App-Name2>']
  filter_null:
  - app_name: null
  selection:
  - occurrence_event_type: App.Start
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized virtual apps
<!--NeedCopy-->
```

数据泄露

November 26, 2023

从 **SaaS** 应用程序打印

当从不允许打印的 SaaS 应用程序打印文件时，就会发生这种情况。它通过在 SaaS 应用程序中进行打印操作来检测潜在的数据泄露。

详细信息

数据源：应用程序和桌面 (Citrix Enterprise Browser)

CAS 查询

```
Event-Type = "App.SaaS.File.Print" AND SaaS-App-Name = "<App-Name>"
<!--NeedCopy-->
```

Sigma 签名

```
author: Citrix
date: 2023/01/31
description: Printing from SaaS apps
detection:
  condition: selection and not filter_null and filter_saas_app_name
  filter_saas_app_name:
  - saas_app_name: '<App-Name>'
  filter_null:
  - saas_app_name: null
  selection:
```



```
    - occurrence_event_type: App.SaaS.File.Print
  logsource:
    product: citrixanalytics
    service: security
  title: Printing from SaaS apps
  <!--NeedCopy-->
```

在 **SaaS** 应用程序上使用剪贴板

当使用任何 SaaS 应用程序完成剪切、复制或粘贴活动时，就会发生这种情况。它通过监视剪贴板操作来检测组织中 SaaS 应用程序的潜在数据泄露情况。

详细信息

数据源：应用程序和桌面 (Citrix Enterprise Browser)

CAS 查询

```
Event-Type = "App.SaaS.Clipboard" AND Clipboard-Result = "success" AND
   Clipboard-Operation IN ( "copy" , "cut" )
<!--NeedCopy-->
```

Sigma 签名

```
author: Citrix
date: 2023/01/31
description: Clipboard usage on SaaS apps
detection:
  condition: selection and not filter_null and
     filter_clipboard_details_result and filter_clipboard_operation
  filter_clipboard_details_result:
  - clipboard_details_result: 'success'
  filter_clipboard_operation:
  - clipboard_operation: ['cut', 'copy', '<Other Operation>']
  filter_null:
  - clipboard_operation: null
  - clipboard_details_result: null
  selection:
  - occurrence_event_type: App.SaaS.Clipboard
logsource:
  product: citrixanalytics
  service: security
title: Clipboard usage on SaaS apps
<!--NeedCopy-->
```


用户控制板

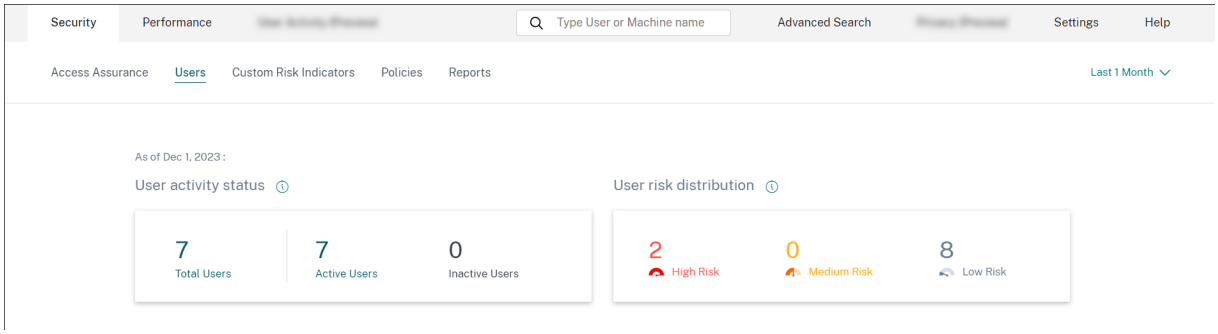
February 14, 2024

概述

用户控制板是用户行为分析和威胁防御的起点。

此控制板可让您了解整个组织的用户行为模式。使用这些数据，您可以主动监视、检测和举报超出常态的行为，例如网络钓鱼或勒索软件攻击。

要查看用户控制面板，请转到安全 **>** 用户。“用户”控制板包含以下部分：



- 用户活跃状态：总数、活跃和非活动用户的分布。
- 用户风险分布：根据选定时间段内计算得出的最高风险分数，活跃、不活跃、总用户的分布以及高、中、低风险用户的分布。
- 热门用户：顶级用户按其风险评分排序，并按所有用户、特权用户和关注列表用户细分。
- 风险类别：显示 Citrix Analytics 支持的风险类别。具有相似行为模式的风险指标分为几类。
- 风险指标和行动：在选定时间内绘制的风险指标和操作在组织中的所有用户的分布情况。
- 访问摘要：汇总用户尝试访问组织内资源的总次数。
- 策略和操作：显示应用于用户配置文件的前五个策略和操作。
- 风险指示器：显示组织中排名前五的风险指示器。

用户活动状态

组织中使用已启用 Analytics 的数据源的用户总数。他们的帐户可能有也可能没有关联的风险评分。此图块显示活跃用户的数量。活跃用户是指在所选时间段内检测到事件的用户。您可以单击“用户活动状态”下拉菜单来查看总用户分为活跃用户和非活动用户的分布情况。

- 用户总数：选定时间范围内的用户总数。

- 活跃用户：在所选时间范围内检测到事件的用户。
- 非活跃用户：在所选时间范围内未检测到任何事件的用户。

由于预计所有用户都不会面临风险，因此用户控制面板上的用户总数可能超过风险用户的数量。

> 注意
>
> 在“用户”页面上，无论选定的时间段如何，都会显示最近 30 天的用户总数。

Facets

根据以下类别筛选用户事件：

- 风险评分：基于高风险、中等风险、低风险和零风险分数的用户事件。
- 用户：基于管理员权限、执行权限和监视列表用户的用户事件。
- 发现的数据源：基于您已载入的数据源的用户事件。

搜索框

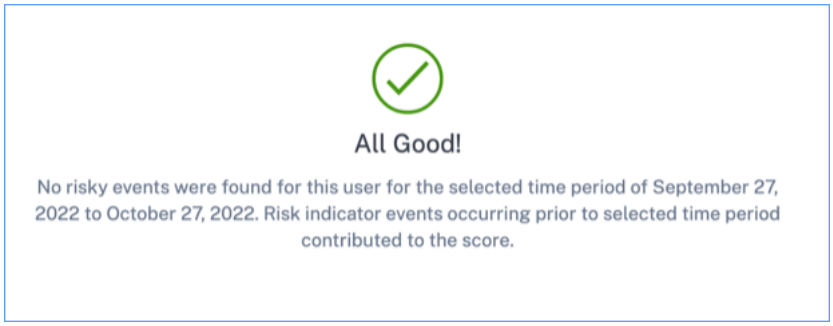
使用搜索框搜索用户的事件。您可以在查询中使用运算符来缩小搜索范围。有关可在查询中使用的有效运算符的信息，请参阅 自助搜索。

最新分数

风险评分决定了用户在特定时间段内对组织构成的风险级别。风险评分值是动态的，根据用户行为分析的不同而有所不同。根据最新的风险评分，用户可能属于以下类别之一：高风险用户、中等风险用户、低风险用户和风险评分为零的用户。

用户

Analytics 发现的所有用户的列表。选择用户名以查看用户的用户信息和风险时间表。用户可能触发或可能未触发任何风险指示器。如果没有与此用户关联的危险事件，您将看到以下消息。



如果存在与用户相关的风险事件，您将在风险时间表上看到风险指示器。选择用户以查看其 风险时间表。

可以将用户标记为 `privileged` 并添加到监视名单中。

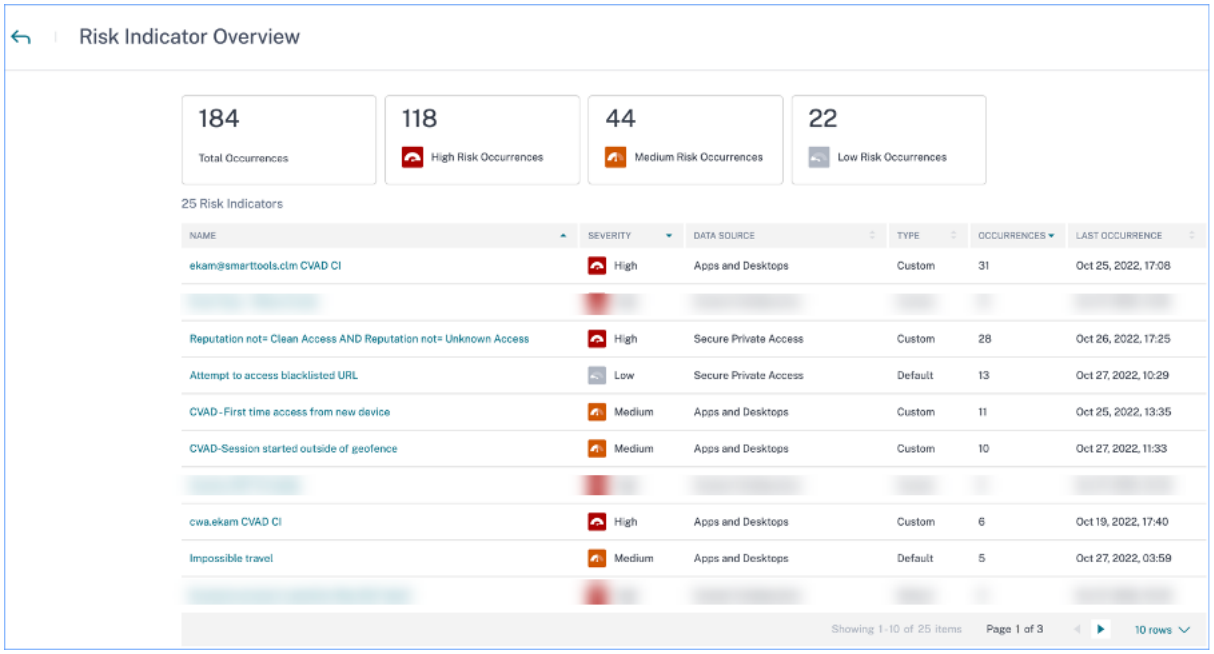
已发现的数据源

与用户关联的数据源。当用户主动使用数据源时，Analytics 会从该数据源接收用户事件。要接收用户事件，必须在“数据源”页面上提供的数据源站点卡片上打开 数据 处理。

触发的指标

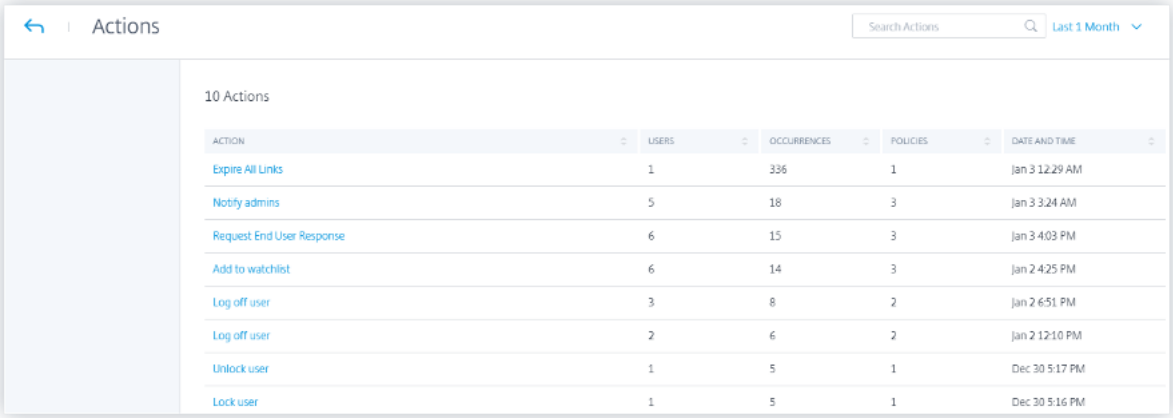
表示在选定持续时间内用户触发的风险指示器数量。单击“触发的指标”图块以查看风险指标的详细信息。风险指标表提供以下详细信息：

- 名称：风险指示器名称。
- 严重性：与事件相关的风险的严重程度。风险可以是高、中或低。
- 数据源：风险指示器模板所适用的数据源。
- 类型：风险指示器的类型。风险指示器可以是 默认 的或 自定义的。
- 发生次数：为用户触发风险指示器的次数。当您选择时间段时，风险指示器的出现次数会根据所选时间而变化。
- 上次出现：显示上次出现的日期和时间。



已应用的操作

表示在选定持续时间内对用户应用的操作数量。这包括管理员手动应用的操作和策略驱动的操作。单击“已应用的操作”图块以查看操作的详细信息。此部分不显示您在用户配置文件上手动应用的操作。

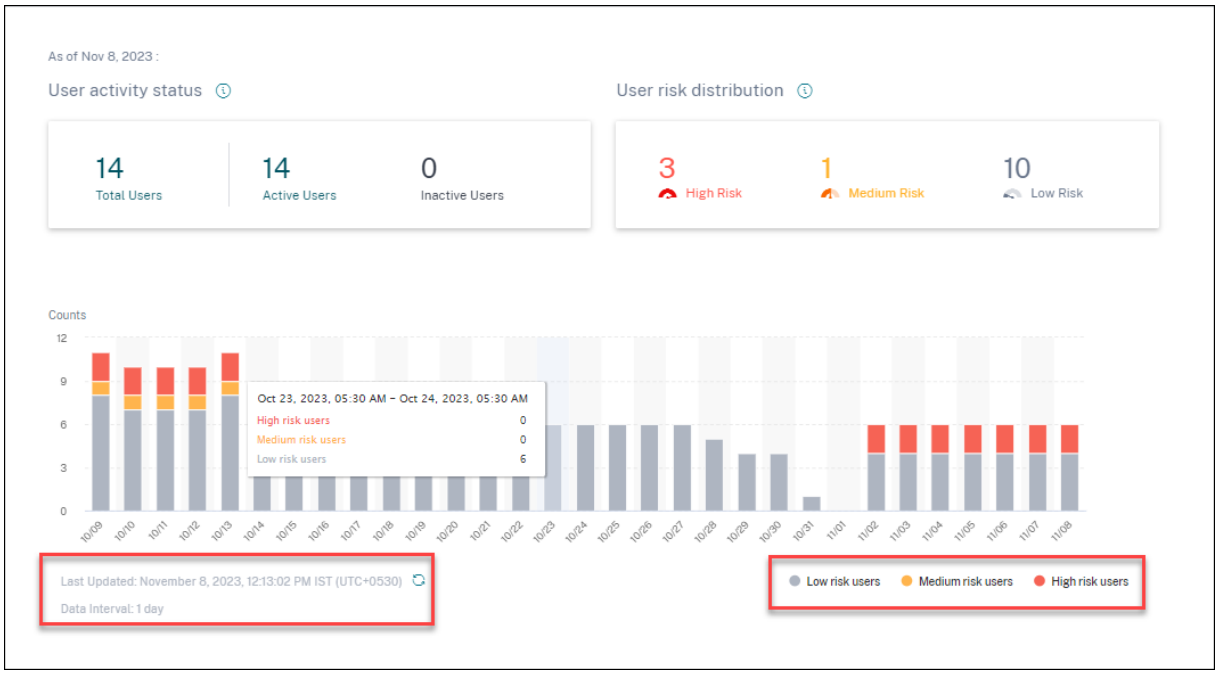


操作 表提供以下信息：

- 操作：根据策略应用的操作的名称。
- 用户：已应用操作的用户数量。
- 发生次数：操作的发生次数。
- 日期和时间：应用操作的日期和时间。

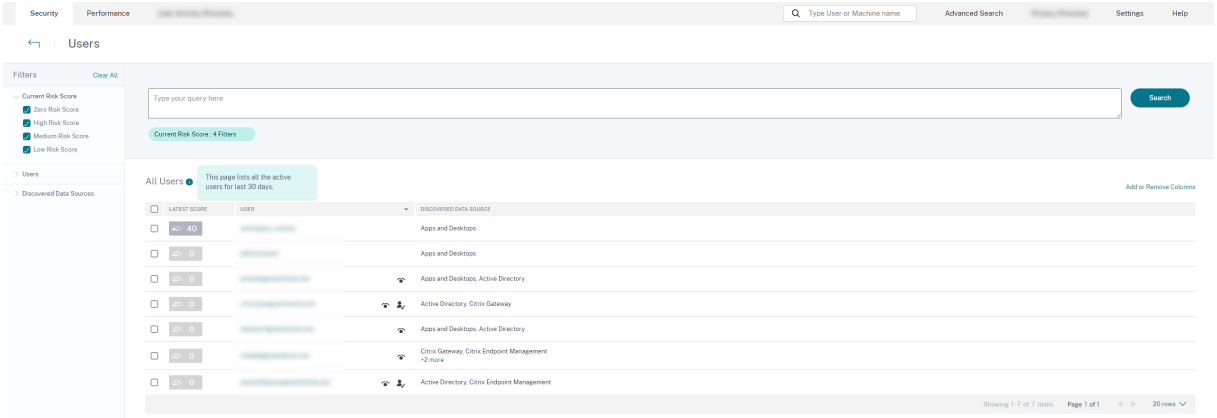
已处理的事件

从您的连接数据源收到并由 Analytics 处理的用户事件总数。



用户风险分布

您可以根据所选时间段内计算得出的最高风险分数来查看处于高、中和低配置的用户数量。在总数下方，条形图显示了低、中和高风险用户分布随时间推移而发生的变化。



风险级别分为三种颜色代码。

- 红色 - 代表高风险用户。
- 橙色 - 代表中等风险用户。
- 灰色 - 代表低风险用户。

您可以根据特定时间段将鼠标悬停在颜色栏上时查看风险用户的数量（高、中和低）。您可以使用数据间隔信息查看上次更新的详细信息（日期和时间）。单击任意颜色栏可查看该时间段内的风险用户。单击“刷新”选项以获取更新的数据。

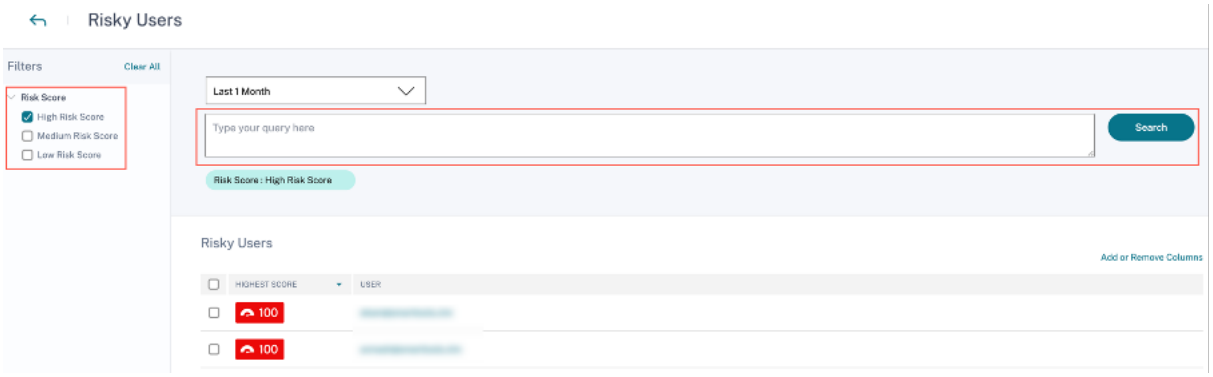
有风险的用户

风险用户是指与风险事件关联且触发了至少一个风险指标的用户。用户在特定时间段内对网络构成的风险级别取决于与用户相关的风险评分。风险评分值是动态的，基于用户行为分析。

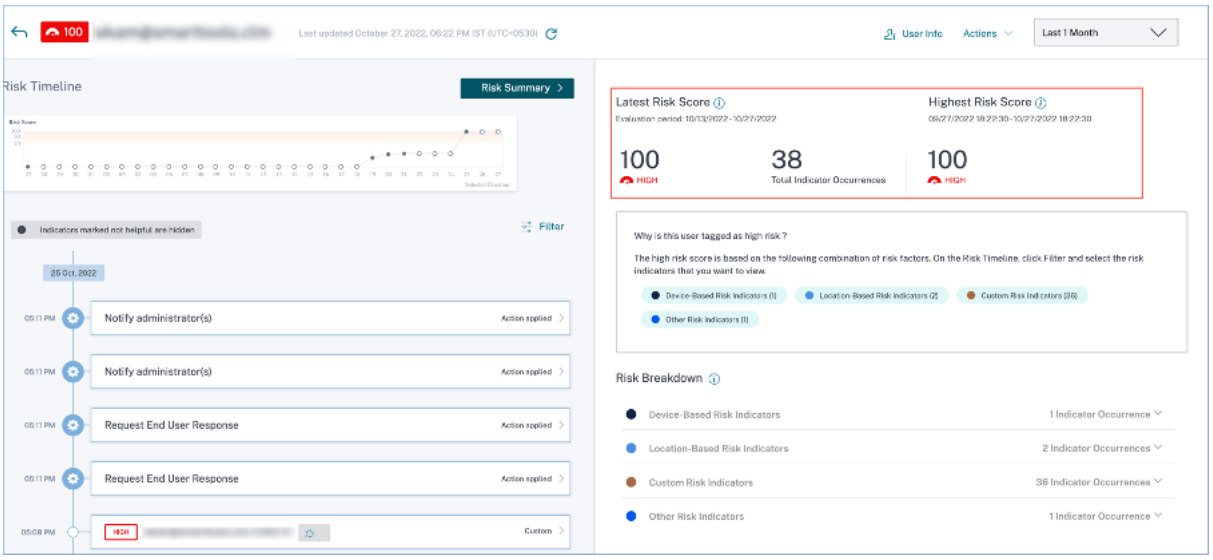
随着时间的推移，每个用户的风险都会根据用户活动定期更新。因此，用户在某一时间点可能处于中等或高风险，但随后会降至较低的风险级别。根据风险评分，有风险的用户可能属于以下类别之一：

- 高风险
- 中等风险
- 低风险

在风险用户页面上，您可以使用分面根据与所选时间段相关的风险级别进行筛选，也可以使用搜索栏来查询一个或多个特定用户。



单击用户的电子邮件 ID 以查看该特定选定用户的风险时间表页面。此页面根据所选时间段显示风险指示器以及最新和最高风险评分的详细信息。



高风险

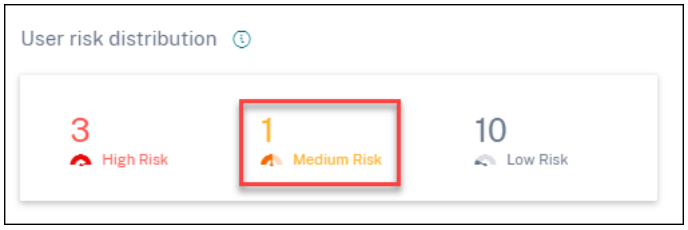
风险评分介于 90 到 100 之间的用户。这些用户表现出与中度至重度风险因素一致的多种行为，可能对组织构成直接威胁。

在用户控制面板上，您可以根据所选时间段内计算得出的最高风险分数查看高风险用户的数量。

单击“高风险”选项以查看“风险用户”页面。该页面显示有关高风险用户的详细信息。

中等风险

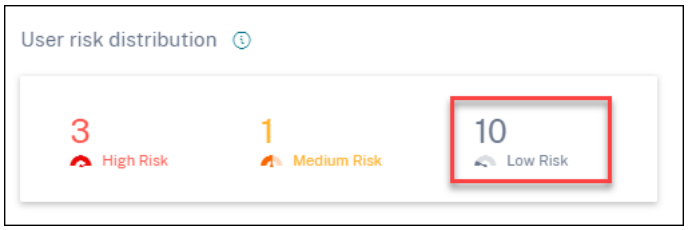
风险评分介于 70 到 89 之间的用户。这些用户通常具有一项或多项看似可疑和/或异常的活动，可能值得密切监视。



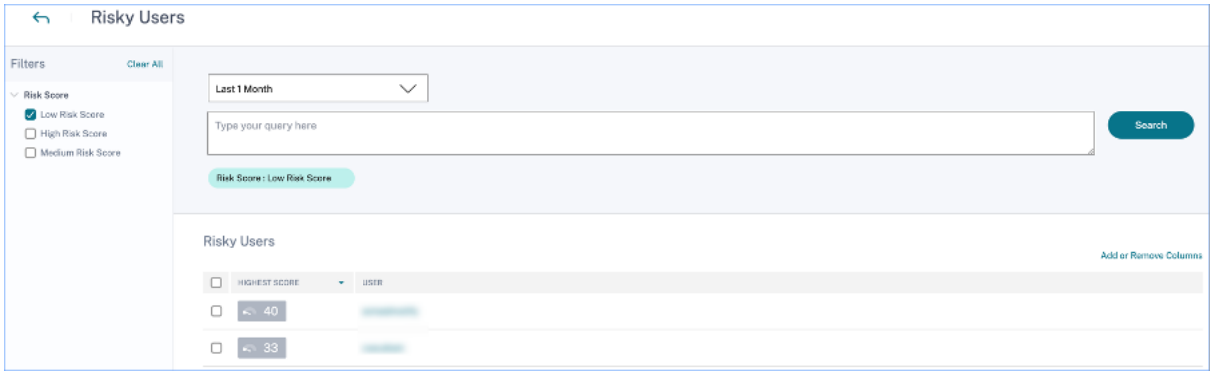
单击“中等风险”选项以查看“风险用户”页面。该页面显示有关中等风险用户的详细信息。

低风险

风险评分介于 1 到 69 之间的用户。这些用户至少有一个风险指示器反映了一些异常或意想不到的行为，但不足以进行更严重的风险分类。

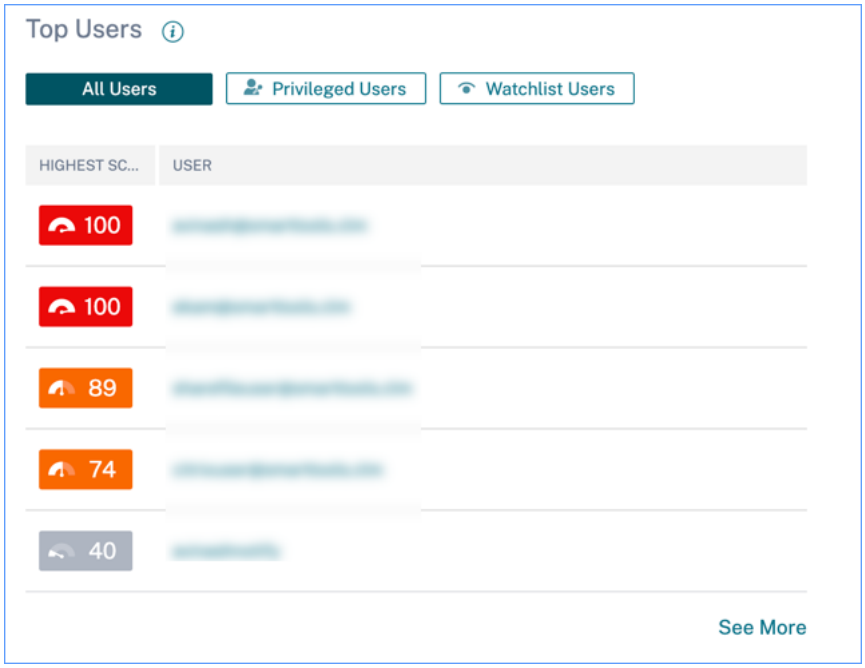


单击“低风险”选项以查看“风险用户”页面。该页面显示有关低风险用户的详细信息。



热门用户

您可以查看所选时间段内按最高风险评分排序的各种用户类别中的热门用户。下面的“热门用户”表根据在选定时间段内计算的风险分数而不是最新的风险分数，显示了风险最高的五名用户（所有用户、特权用户和监视列表用户）。

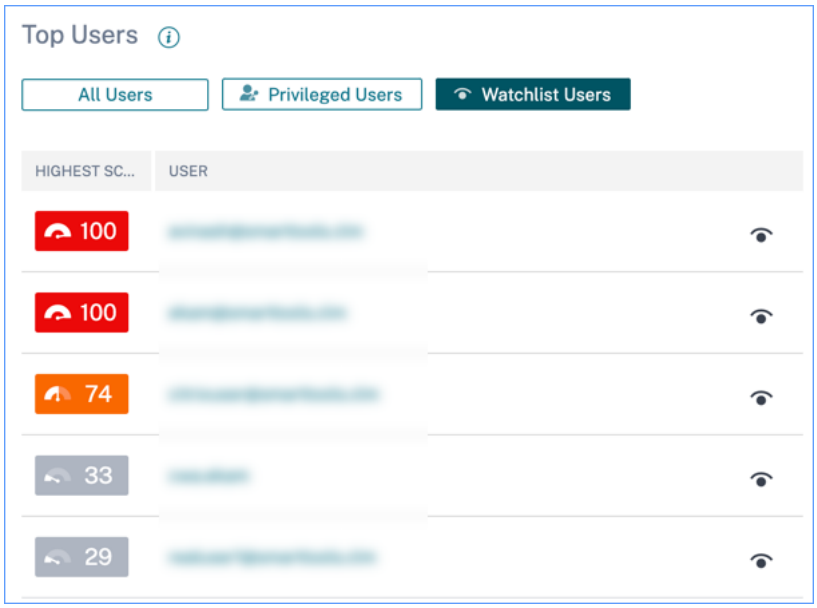


> 注意
>
> 在早期版本中，无论选择的时间段如何，“热门用户”表始终显示最新的风险评分。

监视列表用户

密切监视潜在威胁的用户列表。例如，您可以通过将这些用户添加到监视列表来监视组织内不是全职员工的用户。您还可以监视频繁触发特定风险指示器的用户。您可以手动将用户添加到监视列表，也可以定义将用户添加到监视列表的 策略 。

如果您已将用户添加到监视列表，则可以根据最高分查看监视列表中排名前五的用户。



单击“所有用户”窗格上的“查看更多”链接以查看“用户”页面。该页面显示监视列表中所有用户的列表。

> 注意
>
> 在“用户”控制面板和“用户”页面上，无论选定的时间段如何，监视列表中的用户数都会显示最近 13 个月的用户数。选择时间段时，风险指示器的出现情况会根据所选时间而变化。

了解更多：关 注列表

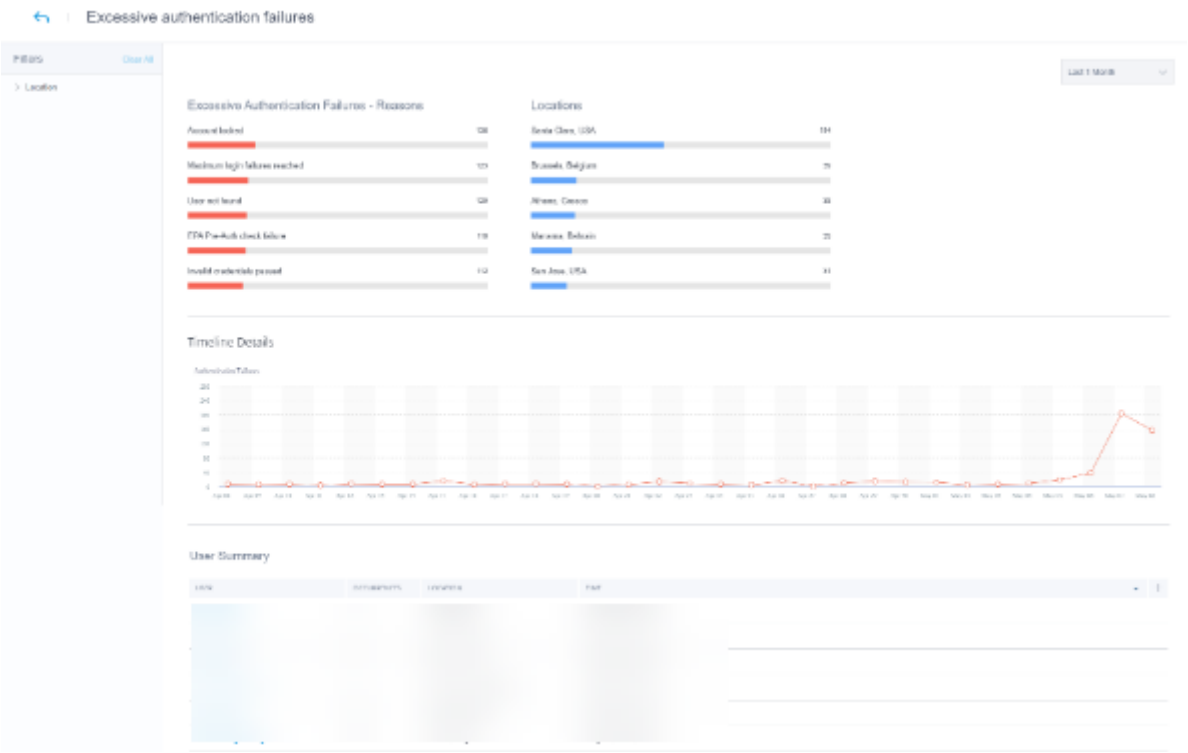
风险类别

风险类别 圆环图汇总了所选时间段内按风险类别划分的指标出现次数。将鼠标悬停在每个图表分段上方时会显示唯一的用户数量，这反过来又链接到相应的风险指标类别概述页面。默认支持风险分类和自定义风险指标。

风险类别控制面板的目的是使 Citrix Virtual Apps and Desktops 和 Citrix DaaS 管理员能够管理用户风险，简化与安全同行的讨论，而无需具备专家级别的安全知识。它允许安全实施在组织级别生效，而不仅限于安全管理员。

用例

假设您是 Citrix Virtual Apps and Desktops 管理员，并且管理组织中员工的应用程序访问权限。如果转到“风险类别”>“受感染的用户”>“身份验证失败过多**-Citrix Gateway** 风险指示器”部分，则可以评估您授予访问权限的员工是否受到威胁。如果您进一步浏览，则可以更准确地了解此风险指示器，例如失败原因、登录位置、时间轴详细信息和用户摘要。如果您发现被授予访问权限的用户与被入侵的用户之间存在任何差异，则可以将此通知安全管理员。这种及时向安全管理员发出的通知有助于在组织层面强制实施安全性。

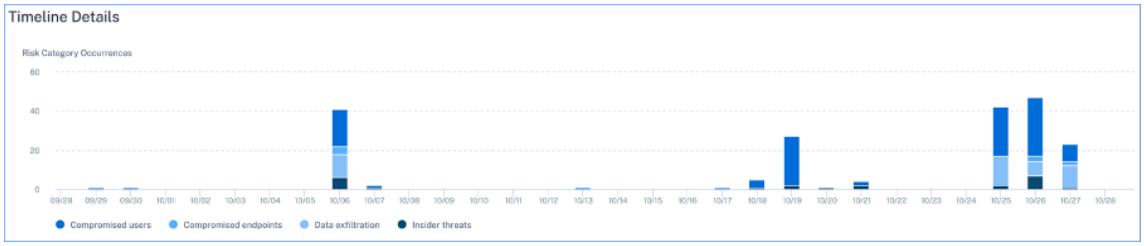


如何分析“风险类别”控制面板

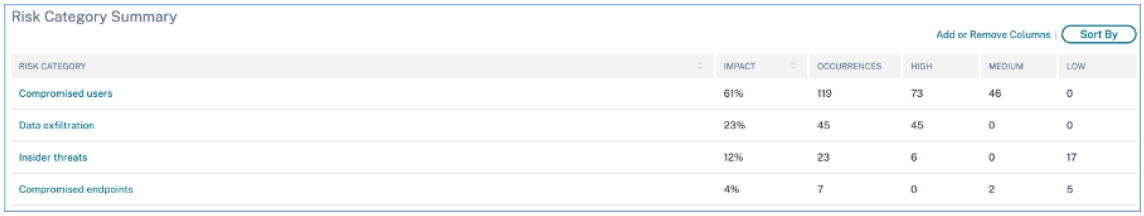
当您在“风险类别”控制面板上选择“查看更多”时，您将被重定向到汇总风险类别详细信息的页面。此页面包含以下详细信息：

- 风险类别报告：表示在选定时间段内每个类别的总风险指示器出现次数。

- 时间轴详细信息：提供选定时间段内每个风险类别的总风险指示器出现次数的图形表示。如果您导航到本部分的底部，则可以根据风险类别进行排序，以获得有关风险指示器的更准确的见解。

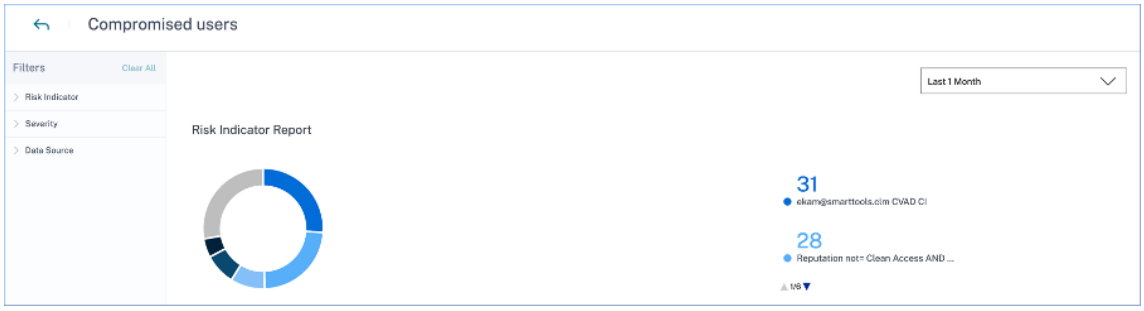


- 风险类别摘要：本部分提供与每个类别相关的风险指示器的影响、发生次数和严重程度等详细信息。选择任何风险类别以查看与该类别关联的风险指示器的详细信息。例如，当您选择“受感染的用户”类别时，您将被重定向到“受感染的用户”页面。

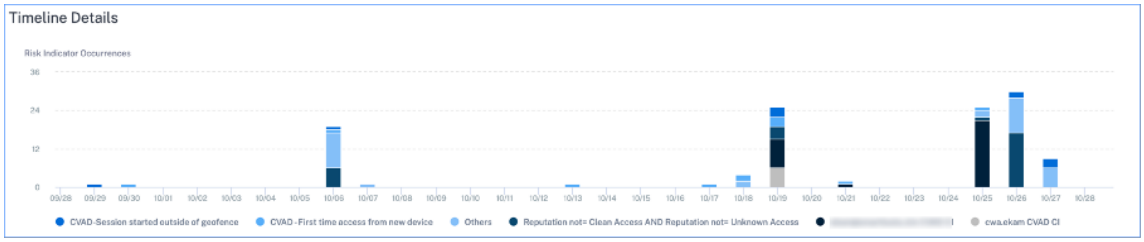


受 感染的用户 页面显示以下详细信息：

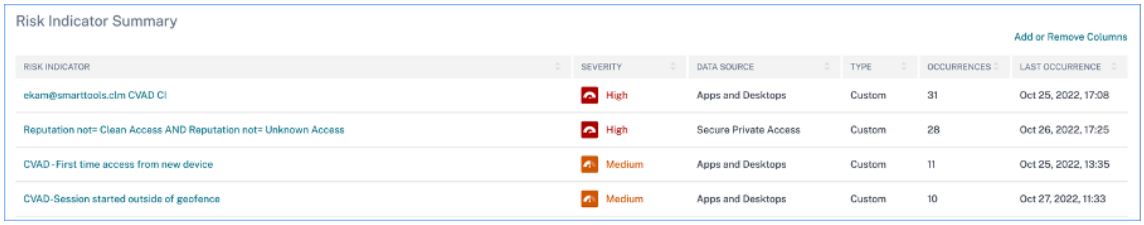
- 风险指示器报告：显示在选定时间段内属于“受感染用户”类别的风险指示器。它还显示在选定时间段内触发的风险指示器的总出现次数。



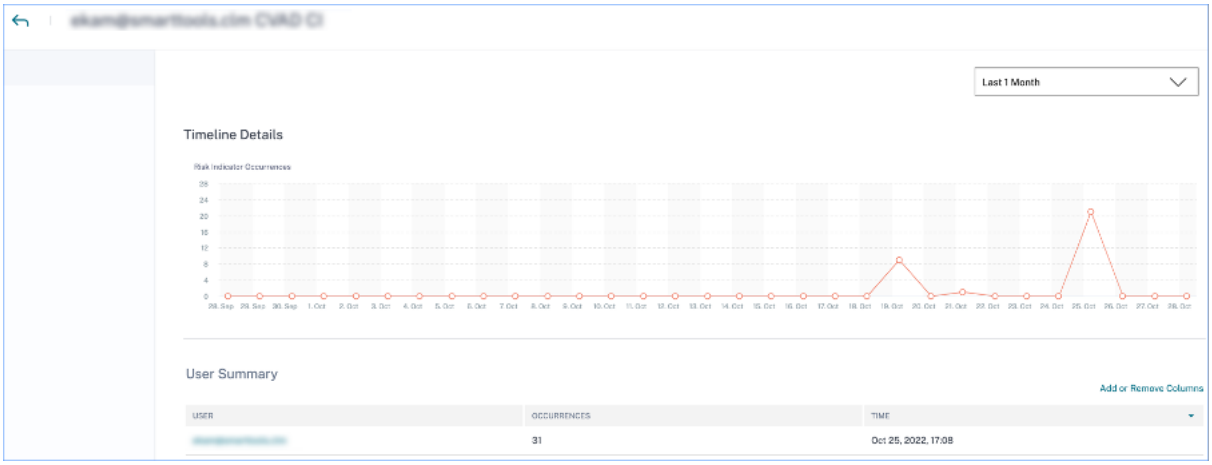
- 时间轴详细信息：提供在选定时间段内出现的风险指示器的图形表示。



- 风险指示器摘要：显示在“受感染用户”类别下生成的风险指示器的摘要。此部分还显示严重性、数据源、风险指示器类型、发生次数和最后一次出现的情况。



当您选择风险指标时，您将被重定向到汇总该指标详细信息的页面。例如，如果选择 首次从新设备访问 风险指示器，则会重定向到汇总此指示器详细信息的页面。摘要包括有关此事件发生的时间表详细信息以及列出触发此风险指标的用户、风险指标出现次数和事件发生时间的用户摘要。选择用户时，系统会将您重定向到该用户的风险时间表。



> 注意
>
> Citrix Analytics 将默认风险指示器分组在适当的风险类别下。对于自定义风险指示器，您必须在创建指示器页面上选择风险类别。有关详细信息，请参阅自定义风险指标。

风险类别的类型

数据泄露　此类别对恶意软件触发的风险指标或员工在组织中的设备进行未经授权的数据传输或数据盗窃行为触发的风险指标进行分组。您可以深入了解在指定时间段内发生的所有数据泄露活动，并通过主动对用户配置文件应用操作来降低与此类别相关的风险。

数据泄露风险类别对以下风险指标进行了分组：

数据源	用户风险指示器
Citrix Virtual Apps and Desktops 和 Citrix DaaS	潜在的数据泄露

内幕威胁　此类别对组织内员工触发的风险指示器进行分组。由于员工对公司特定应用程序的访问权限更高，因此组织面临安全风险的可能性更高。危险活动可能是由恶意内部人员故意造成的，也可能是人为错误造成的。在这两种情况下，对组织的安全影响都是破坏性的。此类别提供了在指定时间段内发生的所有内部威胁活动的见解。借助这些见解，您可以通过主动对用户个人资料应用操作来降低与此类别相关的风险。

内幕威胁风险类别将以下风险指示器组合在一起：

数据源	用户风险指示器
Citrix Secure Private Access	尝试访问列入黑名单的 URL
Citrix Secure Private Access	数据下载过多
Citrix Secure Private Access	网站访问风险

数据源	用户风险指示器
Citrix Secure Private Access	不寻常的上载量

受影响的用户　此类别对风险指标进行分组，在这些指标中，用户表现出异常的行为模式，例如可疑登录和登录失败。或者，异常模式可能是由于用户帐户遭到入侵造成的。您可以深入了解在指定时间段内发生的所有受感染用户事件，并通过主动对用户个人资料应用操作来降低与此类别相关的风险。

受感染用户的风险类别将以下风险指标组合在一起：

数据源	用户风险指示器
Citrix Gateway	端点分析扫描失败
Citrix Gateway	验证失败过多
Citrix Gateway	不可能旅行
Citrix Gateway	从可疑 IP 登录
Citrix Gateway	异常的身份验证
Citrix Virtual Apps and Desktops 和 Citrix DaaS	可疑登录
Citrix Virtual Apps and Desktops 和 Citrix DaaS	不可能旅行
Microsoft Graph 安全性	Azure AD 身份保护风险指示器
Microsoft Graph 安全性	Microsoft Defender 的端点风险指示器

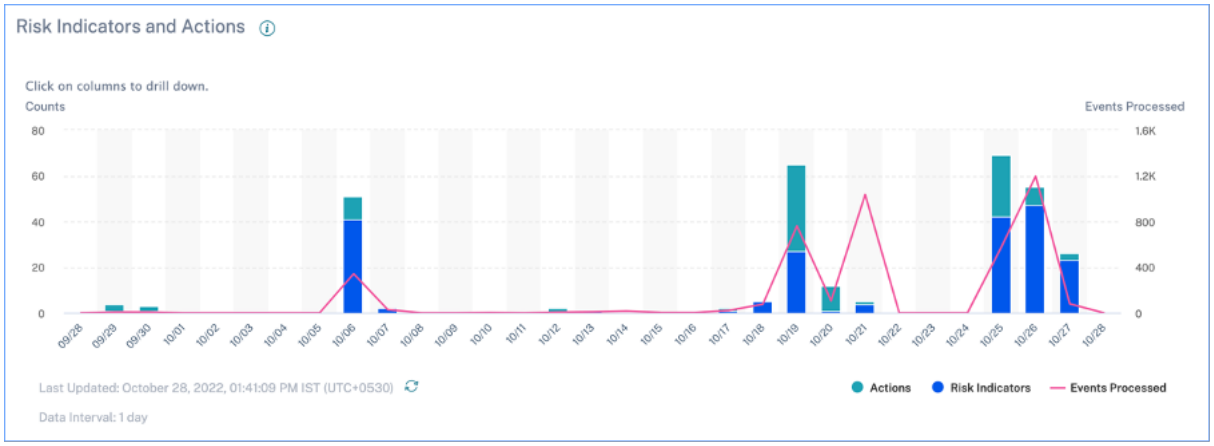
受损的端点　此类别将当设备表现出可能表明存在危险的不安全行为时触发的风险指示器进行分组。

受损端点风险类别将以下风险指示器组合在一起：

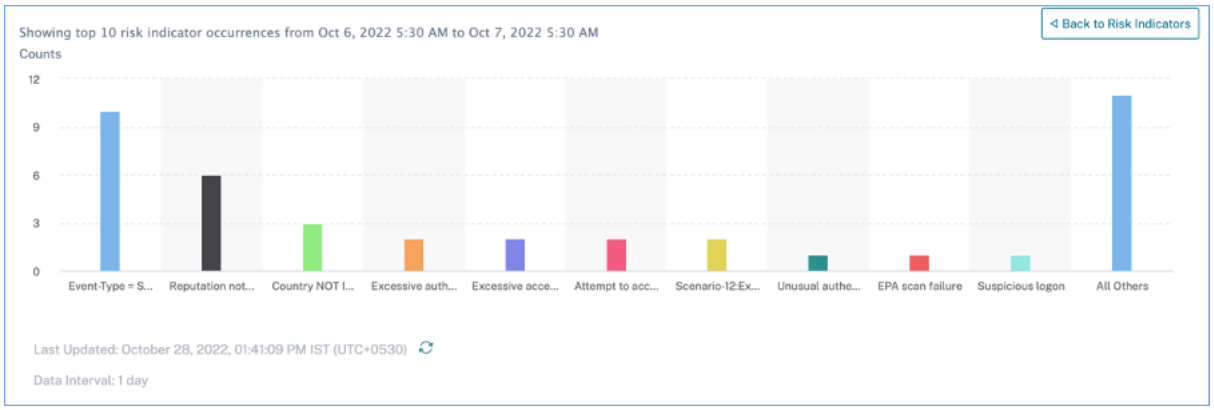
数据源	用户风险指示器
Citrix Endpoint Management	检测到非托管设备
Citrix Endpoint Management	检测到越狱或获得 Root 权限的设备
Citrix Endpoint Management	检测到已列入黑名单的应用

风险指示器和行动

您可以查看所选时间段内触发的风险指示器和适用于您的用户的操作。新的风险指标和操作条形图提供了一段时间内的指标、操作和事件的详细计数，以及从所选时间段得出的总体时间范围和柱间隔。



单击指标或操作的条形段可分别向下深入查看每个指标或操作的计数。



在指标向下钻取中，单击单个指标栏将进入选定时间段内的相应风险指示器页面。

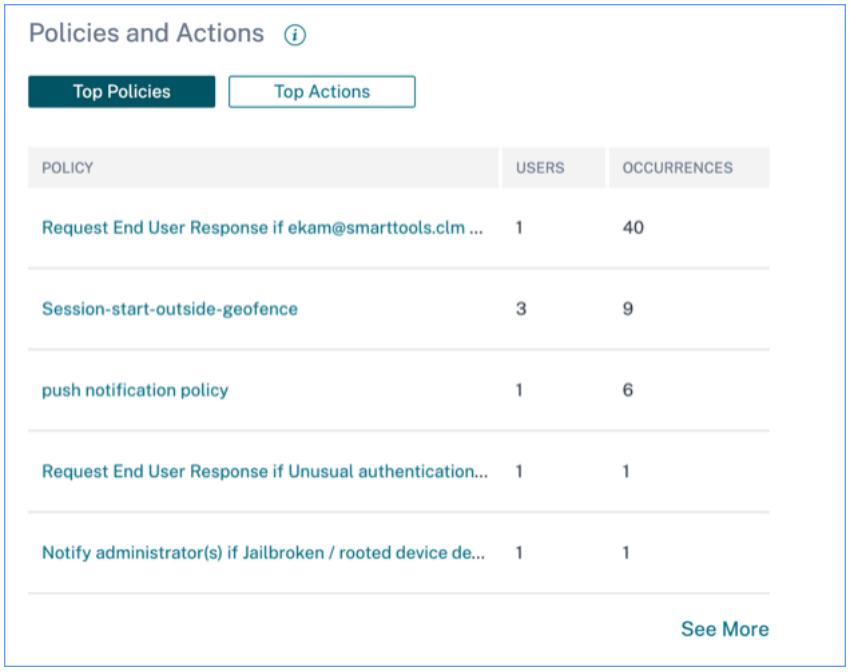
访问摘要

此控制面板汇总了选定时间段内的所有网关访问事件。它显示了通过 Citrix Gateway 的总访问次数、成功访问次数和失败访问次数。

单击图表上的指针可查看“网关的自助搜索”页。对于成功的登录方案，网关访问事件按页面上的状态代码进行排序。

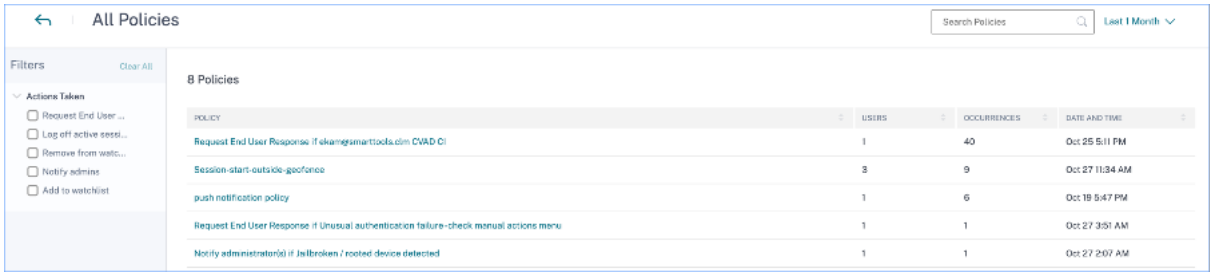
策略和操作

显示在选定时间段内应用于用户配置文件的前五个策略和操作。单击 策略和操作 窗格上的 查看更多 链接以获取有关策略和操作的详细信息。



热门政策

前五个已配置的策略是根据出现次数确定的。当您在控制面板的“顶级政策”部分并选择“查看更多”时，您将被重定向到“所有策略”页面。



所有政策　本页提供有关所有已配置策略的详细信息。当您选择任何策略时，您将被重定向到 自助搜索策 略页面。在左窗格中，您可以根据应用的操作进行筛选。

选择用户名后，系统会将您重定向到风险时间表。基于策略的操作将添加到用户的风险时间表中。选择操作时，其详细信息将显示在风险时间轴的右窗格中。

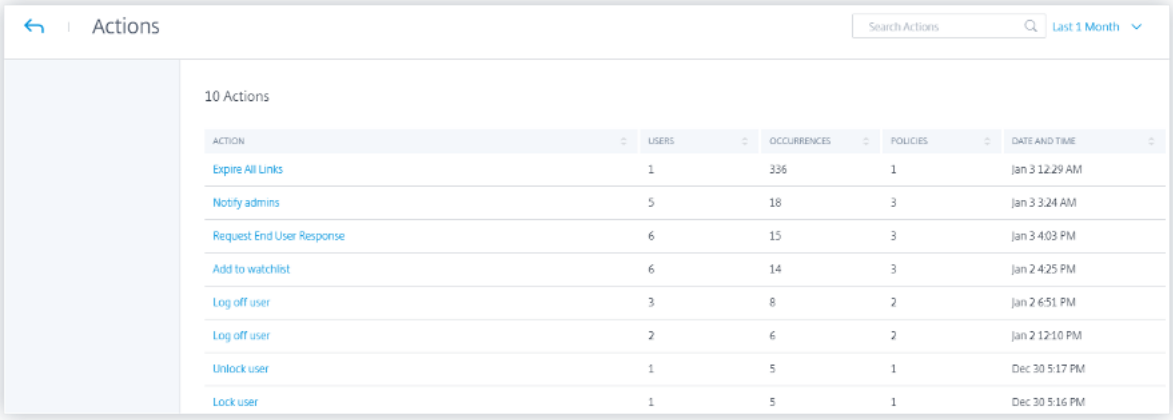
热门动作

与应用于用户配置文件的策略相关的前五项操作。此部分不显示您在用户配置文件上手动应用的操作。顶级操作取决于发生次数。

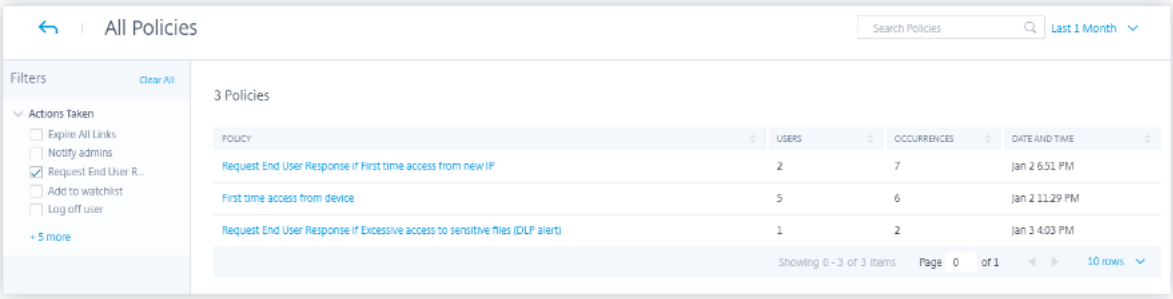
单击查 看更多 以查看“操作”页面上的所有基于策略的 操作。

操作　该页面提供了在所选时间段内应用于您的用户的所有基于策略的操作的列表。您可以查看以下信息：

- 根据策略应用的操作的名称
- 已应用操作的用户数
- 操作发生的次数
- 与操作关联的策略数
- 应用操作的日期和时间



单击某个操作以查看所有关联的策略。这些策略根据发生次数进行排序。例如，在“操作”页面上单击“请求最终用户响应”。“所有策略”页面显示与“请求最终用户响应”操作关联的所有策略。



在 所有策 略页面上，单击策略以查看已应用该操作的用户事件。

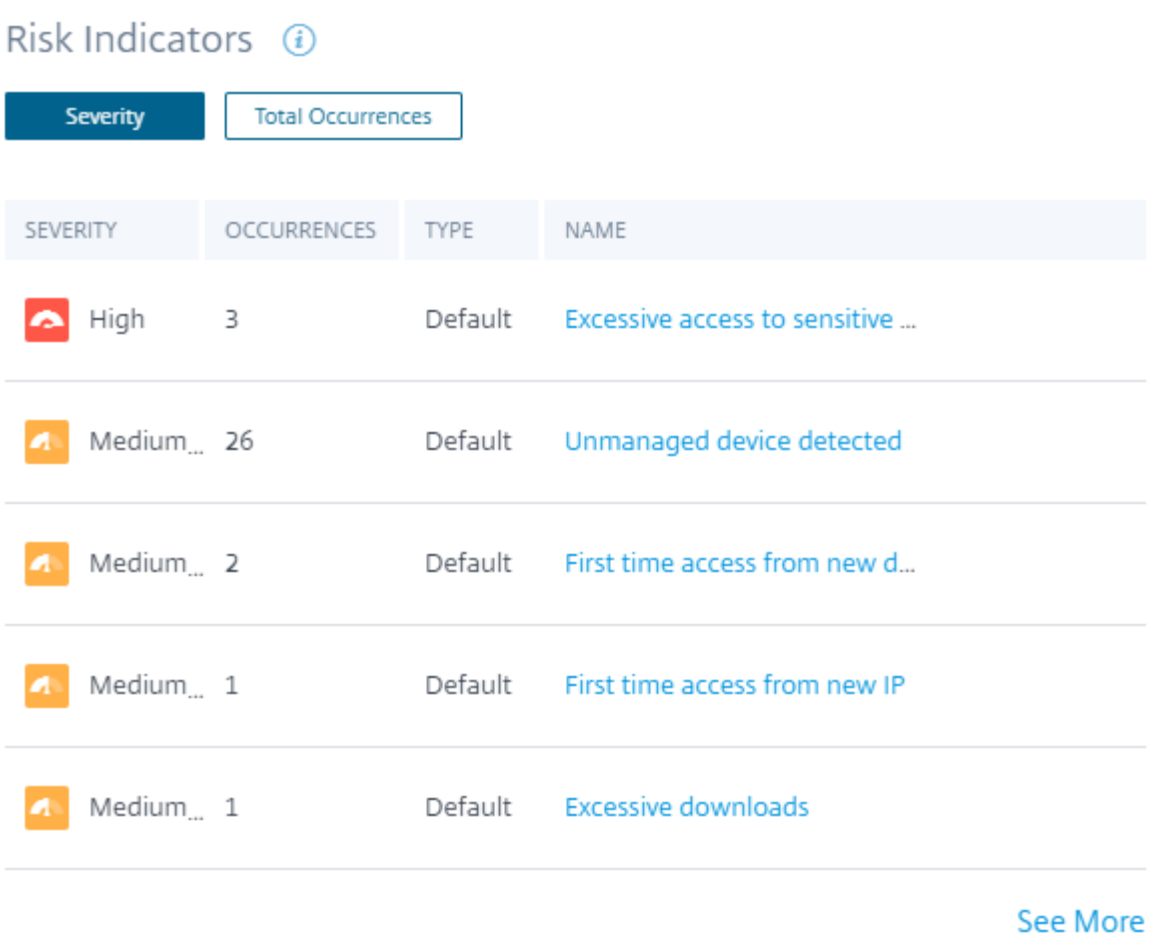
风险指示器

总结了选定时间段内的前五个风险指示器。风险指示器可以是 默认 的或 自定义的。对于默认风险指示器，Citrix Analytics 会从已发现的数据源中收集数据，并启用了数据处理功能。

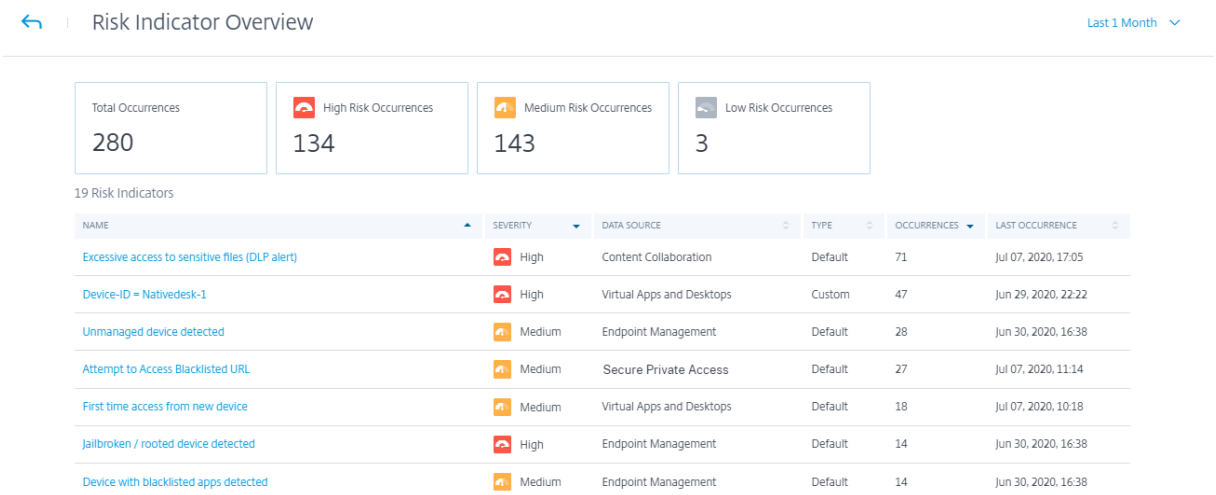
对于自定义风险指示器，Citrix Analytics 会根据生成的风险事件从以下数据源收集数据：

- Citrix Gateway
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）

在“风险指示器”窗格中，您可以查看前五个风险指示器，并根据总发生次数或严重程度对它们进行排序。



单击 风险指 示器窗格上的查 看更多 以查看 风险指示器概述 页面。



访问保障仪表板

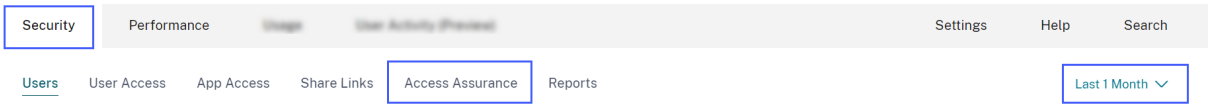
December 5, 2022

随着远程办公的增加，作为 Citrix IT 管理员，您可能希望确保您的用户可以从他们平常的安全位置访问 Citrix Virtual Apps and Desktops 或 Citrix DaaS（以前是 Citrix Virtual Apps and Desktops 服务）。如果有用户从未知位置或新位置登录，则可以验证他们的登录详细信息并采取必要措施来缓解 Citrix IT 环境的任何威胁。

Access Assurance 控制面板概述了用户访问虚拟应用程序或虚拟桌面的位置和网络。Citrix Analytics for Security 从用户设备上安装的 Citrix Workspace 应用程序接收这些用户登录事件。有关支持版本的更多详细信息，请参阅 Citrix Workspace 应用程序版本矩阵。

查看控制板

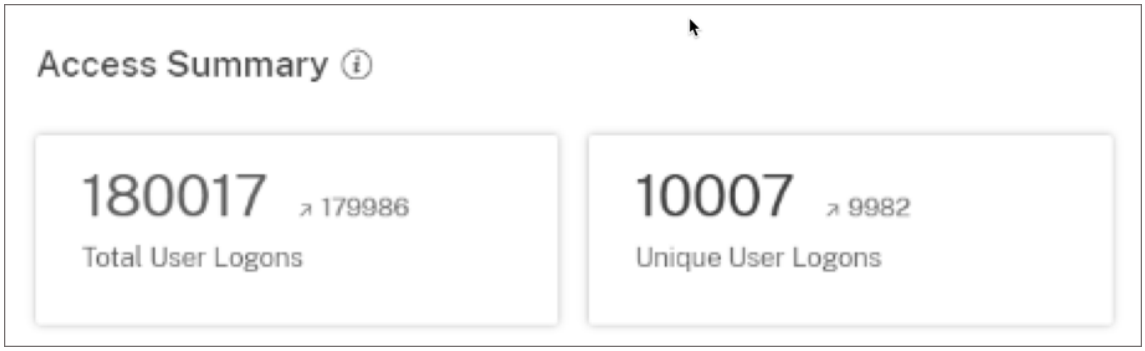
要查看控制板，请单击“安全”**>**“访问保障”。选择要查看登录详细信息的时间段。



访问摘要

控制面板的摘要部分提供选定时段的以下信息：

1. 各个位置（全球）的用户登录总数。
2. 各个位置（全球）的唯一用户登录总数。



登录位置

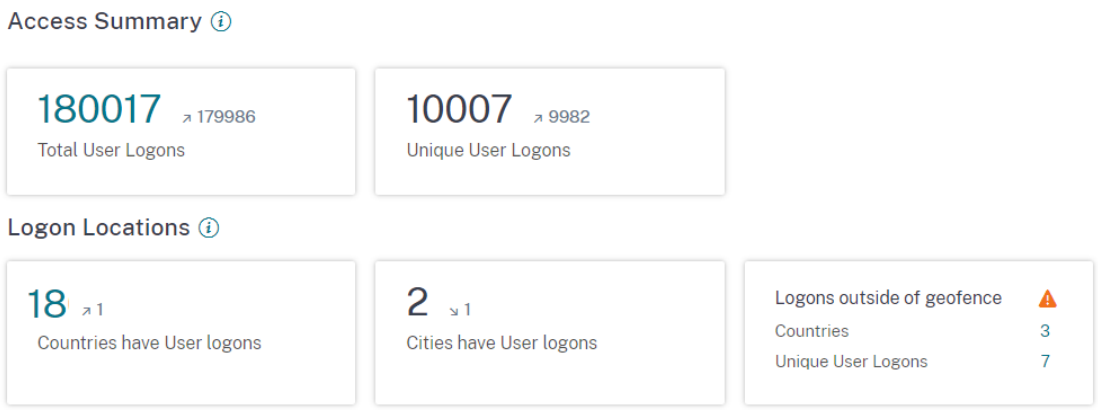
“登录位置”部分提供所选时段内的以下信息：

- 用户登录的国家/地区总数。

- 用户登录的城市总数。
- 地理围栏区域中的国家/地区总数和唯一用户登录次数。要查看地理围栏区域的登录详细信息，请启用地理围栏。
- 具有唯一用户登录名的前 10 个位置。有时，排名靠前的唯一用户登录也来自未知的城市和国家，这些登录列在“未知位置”选项卡下。未知位置列表也是前 10 个位置的子集。要查找某些位置未被识别的原因，请参阅 标识为不可用的位置。

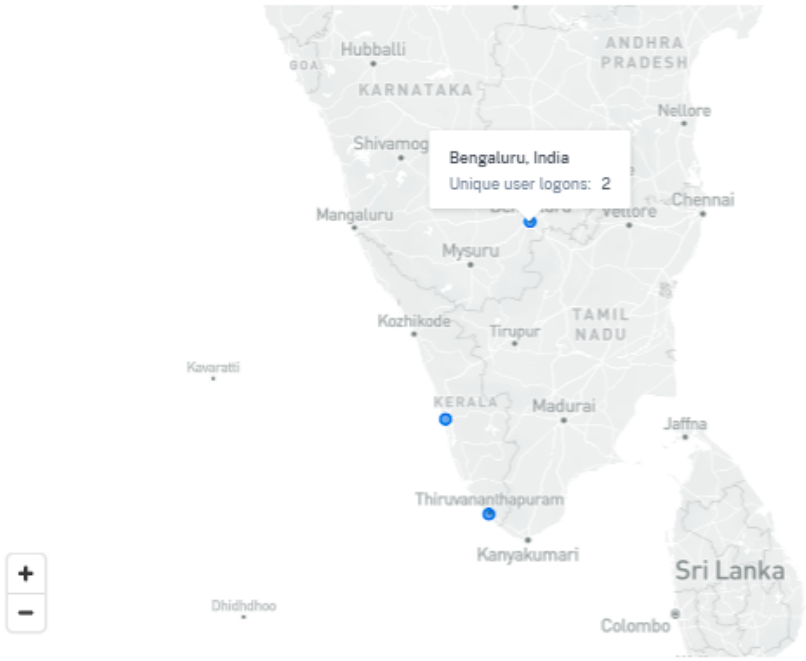
您还可以查看全球用户登录总数和全球唯一用户登录总数的上升或下降趋势。对于前 10 个位置，“偏差”列显示每个位置的用户登录信息的变化（正 (+) 或负数 (-)）。此比较基于选定的时间段和上一个相等长度的时间段。例如，如果选择过去 **1** 个月时间段，则会比较过去 1 个月与之前到过去 1 个月之间的用户登录趋势和偏差。

> 注意
>
> 位置信息是在城市和国家层面提供的，并不代表精确的地理位置。有关访问保障、地理定位的更多详细信息，请参阅 常见问题解答。

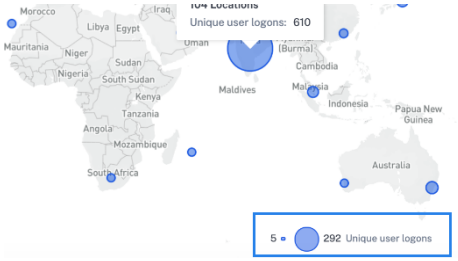


在“前 **10** 个唯一登录位置”表格中，选择一个位置以查看用户及其 访问配置文件 和 登录详细信息。

地图显示选定时间段内来自不同位置的唯一用户数量。将鼠标悬停在蓝色气泡上或放大到某个位置以查看该位置的唯一用户登录的总数。单击蓝色气泡可查看某个位置的 访问详细信息 。



在地图的右下角，您可以查看唯一用户登录的范围。在选定的时间段内，小气泡表示跨位置唯一用户登录的最小数量。大泡表示各个位置中唯一用户登录的最大数量。

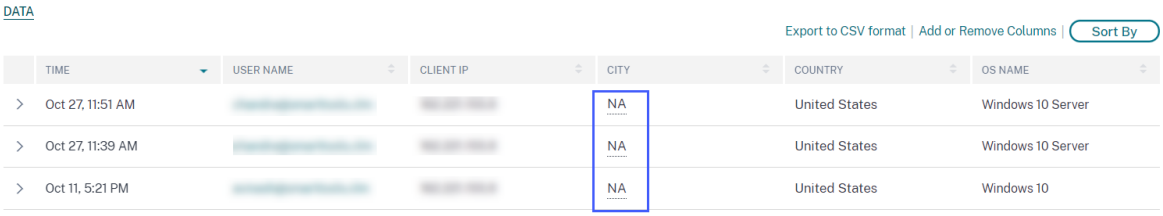


被确定为不可用的地点

在 前 **10** 个唯一登录位置 表中，您可能会看到某些位置未知或不可用。单击未知位置可在“用户登录”页面上查看相应的 用户登 录详细信息。

在 用户登录页面 上，如果有任何国家或城市信息不可用，**DATA** 表将显示 **NA** 标签。

将鼠标悬停在 **NA** 标签上可查看位置信息不可用的原因。



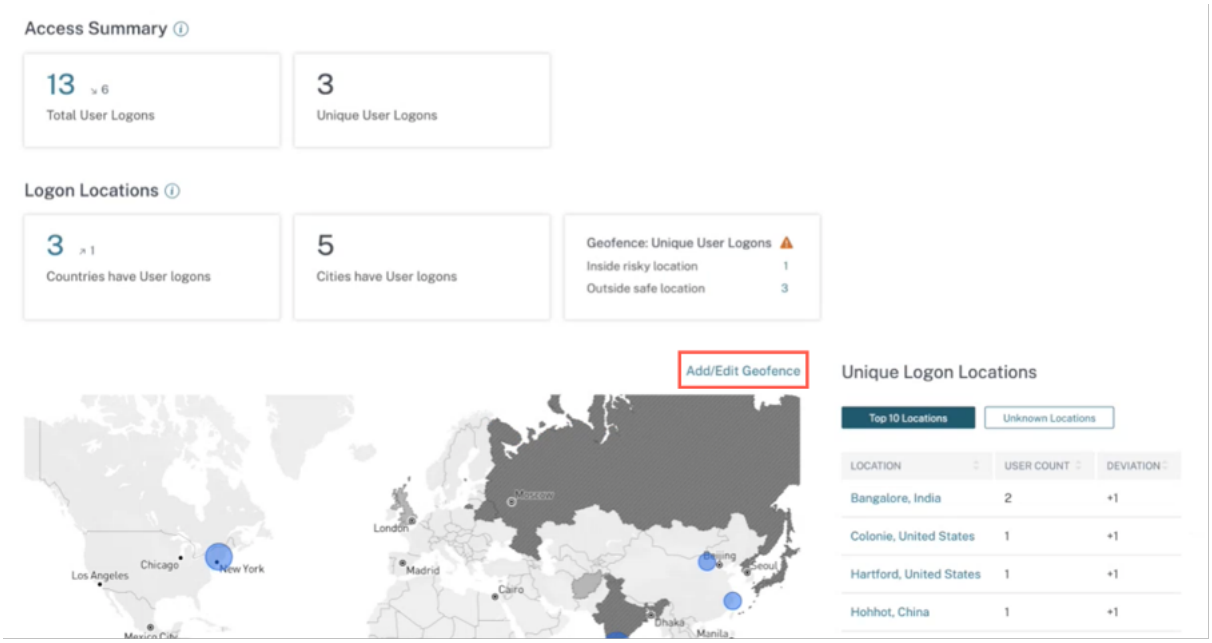
您可能会看到位置不可用的以下情况之一：

场景	原因
城市名称和国家/地区名称不可用。	以下其中一种： 1. 用户正在使用不受支持的 Citrix Workspace 应用程序版本。要查看位置信息，请将客户端更新到 受支持的版本。
拥有私有 IP 的地点	用户的设备位于专用网络中。在这种情况下，Citrix Analytics 不可用位置信息。
国家/地区名称可用，但城市名称不可用。	用户的设备可能正在使用公司 IP。公司 IP 范围在外部地理位置服务中被模糊处理。因此，Citrix Analytics 不可用位置信息。

启用地理围栏

地理围栏可帮助您识别从安全地理围栏外部和危险的地理围栏区域内访问虚拟应用程序或虚拟桌面的用户。要查看“访问摘要”页面，请导航到“安全”**>**“访问保障”。

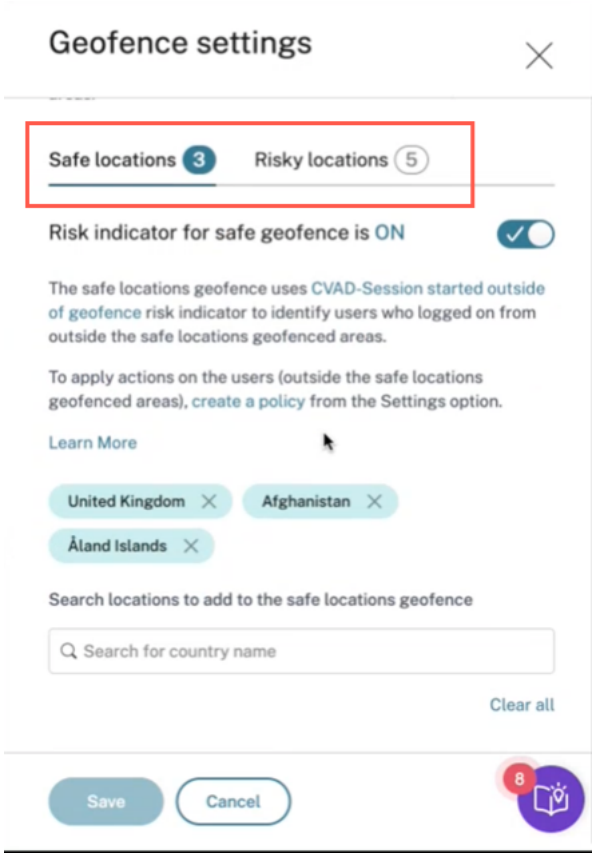
默认情况下，地理围栏设置始终处于打开状态。要配置地理围栏，请单击 添加/编辑地理围栏。



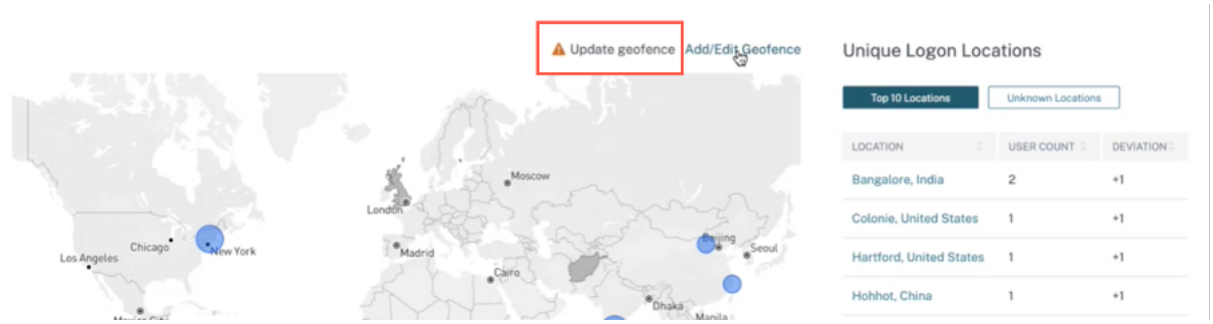
地理围栏设置窗口出现时有两个选项卡：

- 安全位置：您可以配置或删除属于安全位置的国家/地区。
- 危险位置：您可以配置或删除属于危险位置的国家/地区。

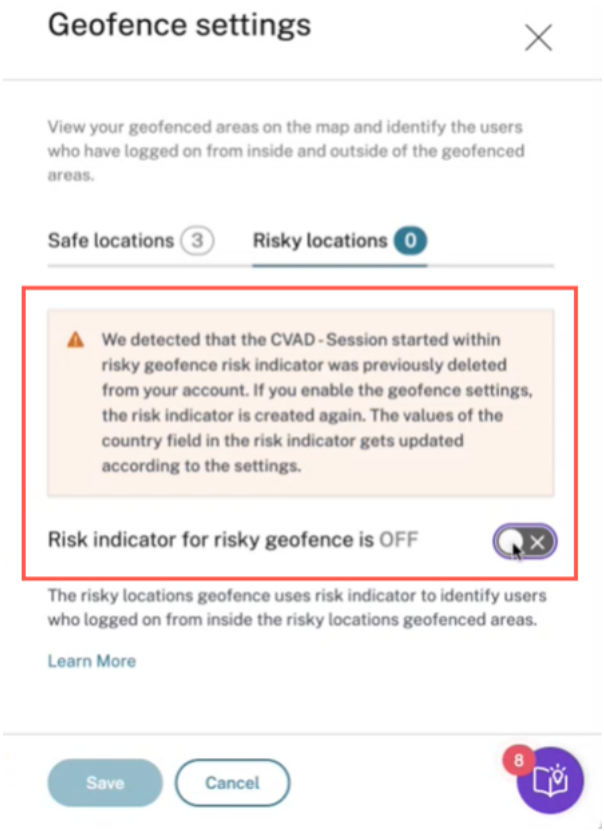
  还可以查看在每个选项卡上配置的安全和危险位置的总数。要从安全位置地理围栏或风险位置地理围栏中删除或移除某个国家，请单击该国家旁边的关闭 (X) 标志。单击“保存”以保存地理围栏设置。



您可以配置属于危险地点地理围栏的国家/地区。如果没有为风险位置地理围栏添加风险指示器或风险指示器被删除，则可以在 添加/编辑地理围栏旁边看到更新地理围栏警告消息。



要重新创建指示器，请导航到“风险位置”选项卡，然后打开“风险地理围栏的风险指示器”开关。



该指标是使用默认的风险位置列表创建的。

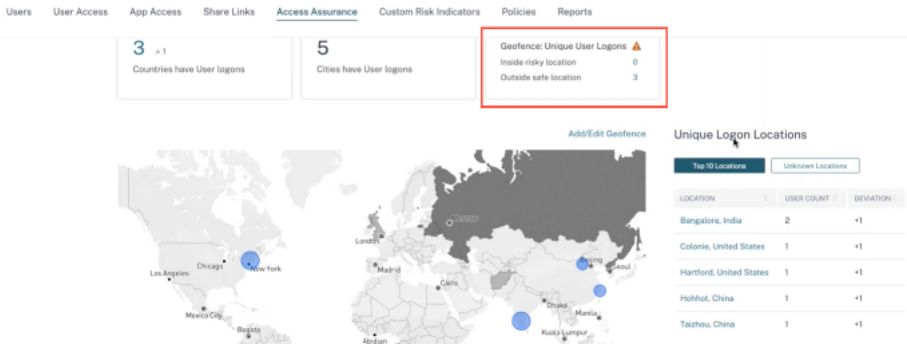
访问摘要页面还显示了带地理围栏的安全和风险国家/地区。

- 带地理围栏的安全国家/地区标有浅灰色圆圈。
- 带地理蔚蓝的风险国家/地区标有深灰色圆圈。

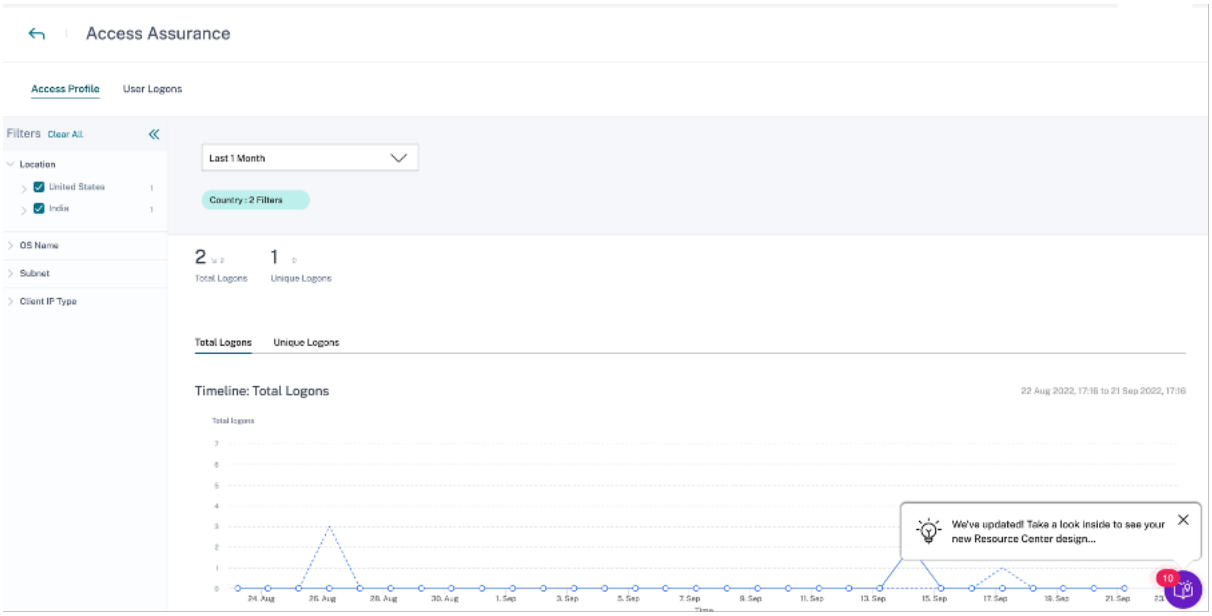
地理围栏：唯一用户登录

导航到“访问摘要”页面查看地理围栏：唯一用户登录。该卡显示内部危险位置和外部安全位置的数量。

- 在危险位置内：识别从危险位置地理围栏区域内登录的用户。
- 外部安全位置 识别从安全位置地理围栏区域之外登录的用户。



要查看用户登录总数和唯一登录次数的详细摘要，请单击“内部危险位置”或“外部安全位置”旁边的数字。



此功能使用以下预配置的自定义风险指示器：

- **CVAD** 会话在地理围栏之外启动：监视安全地理围栏之外的用户登录情况。
- **CVAD** 会话在有风险的地理围栏中启动：监视有风险的地理围栏内的用户登录。

如果在地理围栏之外检测到任何用户登录，则会触发风险指示器，并对这些用户应用在地理围栏之外启动的会话策略。该策略会触发“请求最终用户响应”操作，根据用户的响应，您可以采取适当的措施来防止来自任何可疑登录的威胁。有关更多信息，请参阅 预配置的自定义风险指标。

> 备注
>
> - 在 地理围栏设置中，当您修改国家/地区时，在 地理围栏风险指示器之外启动的 *CVAD* 会话 也会更新。
> - 例如，如果您选择国家/地区澳大利亚和印度并将其保存为新的地理围栏国家/地区，则除了美国（默认的地理围栏）之外，风险指示器的预配置条件将更新为新的国家/地区。您还可以删除默认的地理围栏国家/地区

> 美国。
>
> 风险指示器的预配置状况：
>
> ```
> Event-Type = \"Session.logon\" AND Country != \"\" AND Country
>  ~ \"\" AND Country != \"United States\"
> ```
>
> 更新 地理围栏设置后，风险指示器的状况：
>
> ```
> Event-Type = \"Session.logon\" AND Country != \"\" AND Country
>  ~ \"\" AND Country NOT IN (\"Australia\", \"United States\",
> \"India\"
> ```
>
> - 如果之前从您的帐户中删除了在 地理围栏风险指示器之外启动的 *CVAD* 会话，则启用 **Geofence** 设置 会再次创建风险指示器。风险指示器的地理围栏国家/地区由 地理围栏设置进行控制。

启用 地理围栏设置后，地图将显示地理围栏区域以及这些区域的唯一用户登录信息。

登录网络

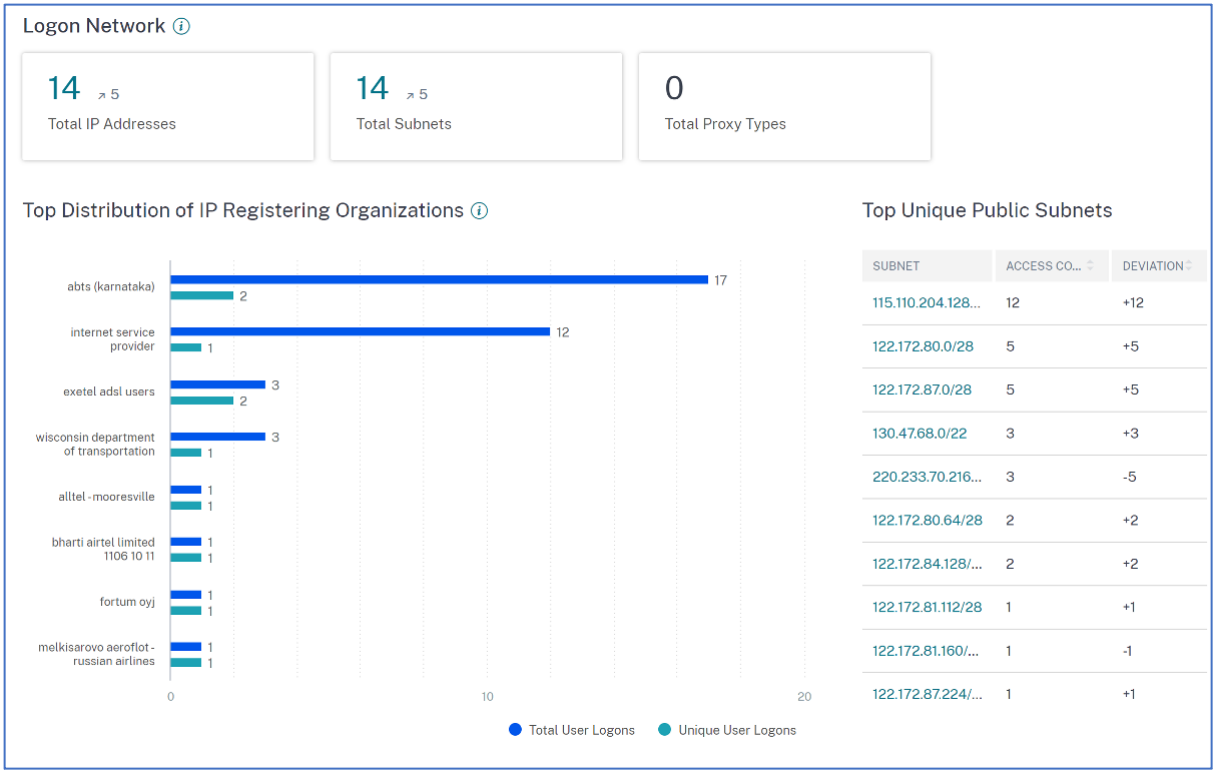
在 Access Assurance 控制面板中，您现在可以查看以下其他用户详细信息：

- 与用户登录的 IP 地址相关的组织。这些组织包括企业、政府、教育实体和互联网服务提供商等实体。
- 用户登录的唯一公有子网和私有子网的总数。
- 用户使用代理和私有 VPN 服务登录的详细信息。

作为管理员，使用这些其他详细信息，您可以验证用户登录详细信息，并确保用户登录是否符合组织的安全期望。

查看用户网络详情

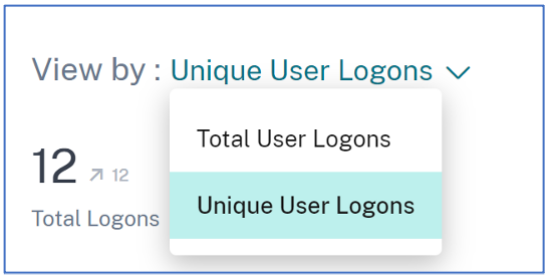
导航到“安全”**>**“访问保障”，然后向下滚动以查看 “登录网络”下的详细信息。



- **IP** 地址总数：表示用于登录虚拟会话的唯一 IP 地址总数。
- 子网总数：表示用于登录虚拟会话的子网总数。
- 代理类型总数：表示服务器用来代理用户连接的网络或协议的总类型。
- 在 **IP** 注册组织的顶级分布下，您可以直观显示每个组织 (ISP) 的用户登录总数和唯一登录详细信息的概览。您可以单击图表深入查看用户的详细信息，以及他们的访问配置文件和与所选组织相关的登录详细信息。
- 在“唯一公有子网总数”下，您可以可视化子网概览、每个子网的用户登录总数以及每个子网的偏差趋势。您可以单击每个子网进行深入查看，以查看用户的详细信息及其访问配置文件和与所选子网相关的登录详细信息。

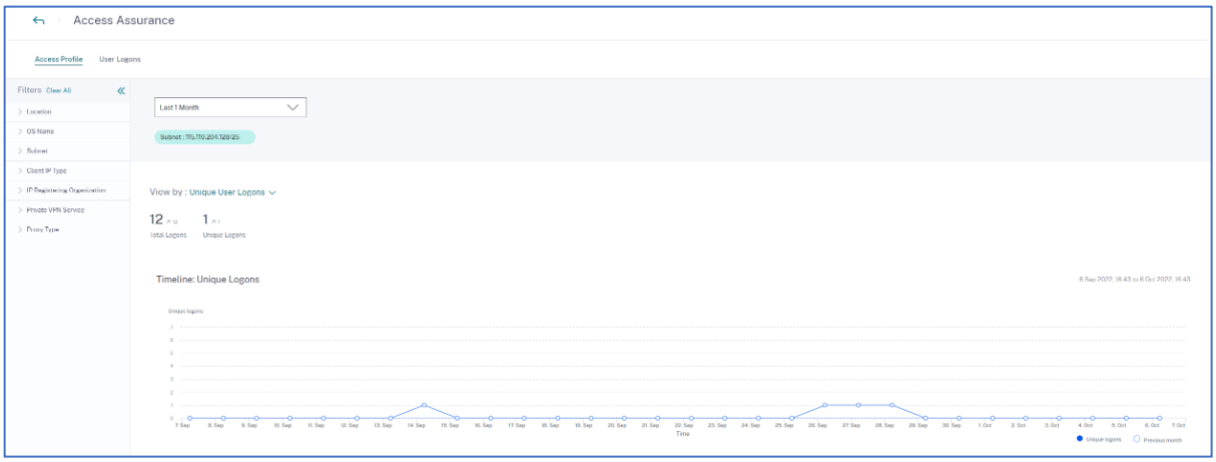
查看用户的访问配置文件

当您深入查看任何指标（位置、组织或子网）时，访问配置文件 页面会提供用户从所选位置访问虚拟应用程序或虚拟桌面的摘要。您可以选择唯一登录或总登录选项来查看所选时段的趋势分析。



您可以查看所选指标（位置、组织或子网）的热门访问事件。此信息可帮助您查看访问模式和威胁调查和分析的详细信息。

根据选定的时间段和上一个相等长度的时间段，比较用户登录总数和唯一用户登录次数的上升或下降趋势。例如，如果您将时间段选择为“最近 **1** 个月”，则会比较过去 1 个月和上一个月与过去 1 个月之间的趋势。



Facets

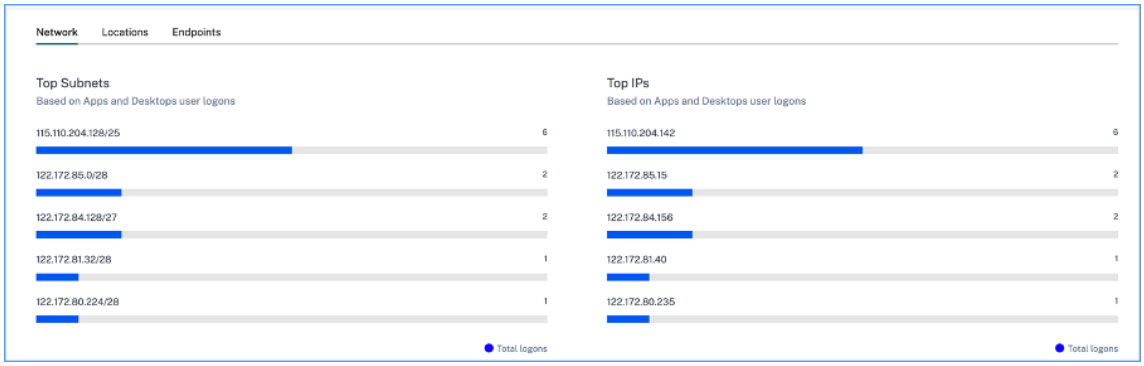
您可以对访问事件使用以下方面：

- 位置-按国家和城市筛选访问事件。
- 操作系统-按操作系统及其版本过滤访问事件。
- 子网-按子网筛选访问事件。
- 客户端 **IP** 类型-按公共或私有过滤访问事件。
- **IP** 注册组织-筛选与公共 IP 地址关联的组织。
- 专用 **VPN** 服务-按专用 VPN 网络名称筛选访问事件。
- 代理类型-按代理类型分类（例如 HTTP、Web、Tor 和 SOCKS）筛选访问事件。

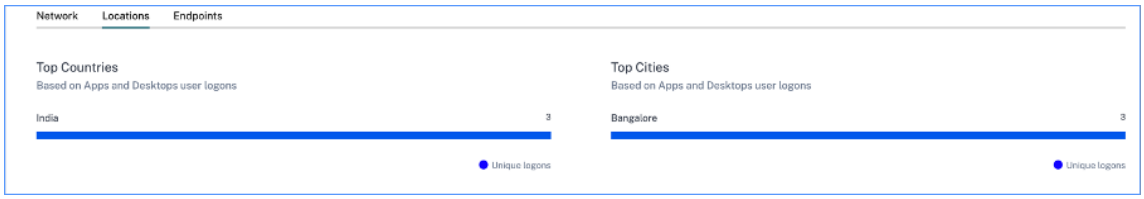
> 注意
>
> 如果数据不可用或未识别，您可能还会看到不可用的标签。

根据应用的筛选器，查看以下信息，了解用户登录总数和唯一用户登录次数：

- 网络-用户登录虚拟应用程序或虚拟桌面的顶级子网和 IP 地址。



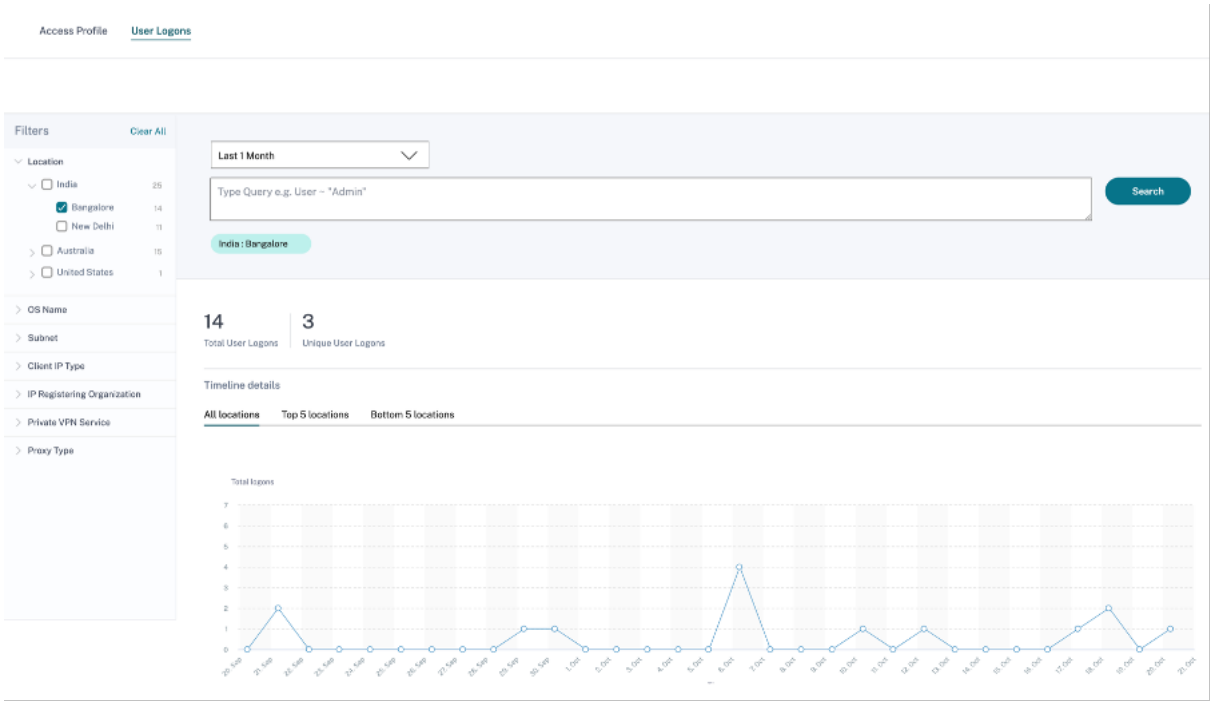
- 地点-用户登录虚拟应用程序或虚拟桌面的排名靠前的国家和城市。



- 端点-基于应用程序和桌面用户登录的顶级设备和操作系统名称。

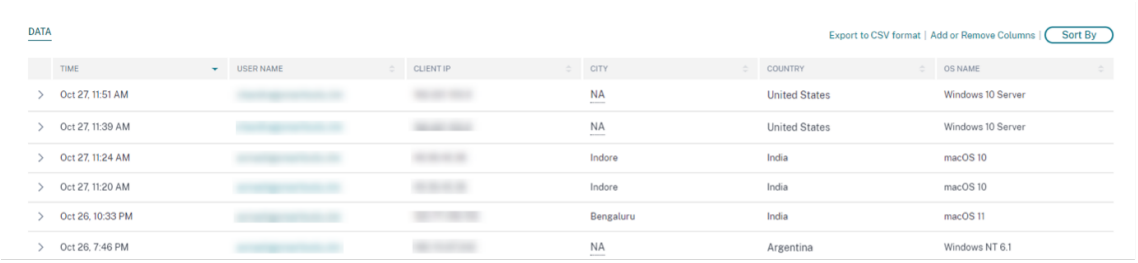
查看用户的登录详细信息

“用户登录”页面提供了用户从所选位置登录到虚拟应用程序或虚拟桌面的详细信息。这些信息在威胁调查和分析过程中有所帮助。



DATA 表显示所选位置和时间段的以下登录详细信息：

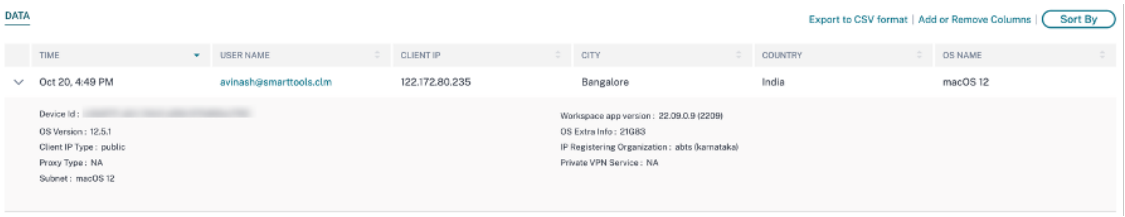
- 时间。用户登录的日期和时间。
- 用户名。用户的身份。
- 客户端 **IP**。用户设备的 IP 地址。
- 客户端 **IP** 类型。用户的 IP 地址类型，例如公共或私有。
- 城市和国家。用户登录到虚拟应用程序或虚拟桌面的位置。
- 设备 **ID**。用户设备的身份代码。
- 操作系统名称。用户设备上的操作系统。有关详细信息，请参阅应用程序和桌面的自助式搜索。



如果您扩展每个事件，则可以看到以下详细信息：

- 操作系统版本。用户设备上的操作系统版本。有关详细信息，请参阅应用程序和桌面的自助式搜索。
- 操作系统附加信息-操作系统的任何其他信息，例如内部版本号、Service Pack 和补丁程序。有关详细信息，请参阅应用程序和桌面的自助式搜索。

- 工作区应用版本。Citrix Workspace 应用程序或 Citrix Receiver 的构建版本。



在 **DATA** 表上，您可以执行以下操作：

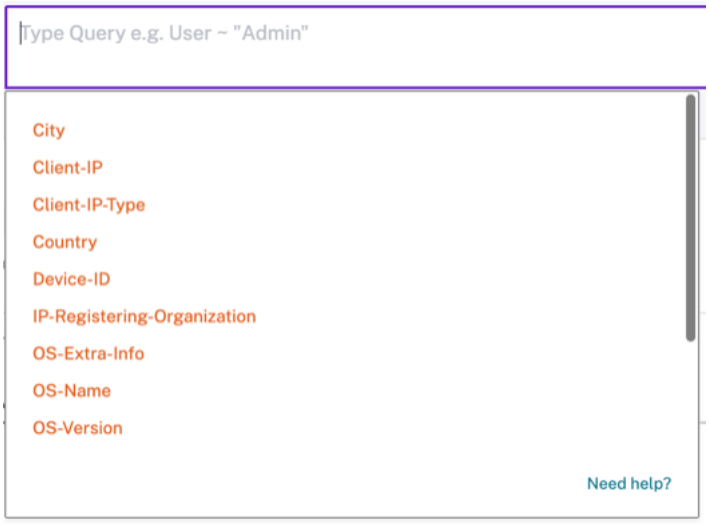
- 单击 添加或删除列 以根据要查看数据的方式更新表列。
- 单击 排序依 据，然后选择要执行多列排序的数据元素。有关详细信息，请参阅 多列排序。
- 单击 导出为 **CSV** 格式，将 DATA 表中显示的数据下载到 CSV 文件，然后将其用于分析。

搜索栏

您还可以使用搜索栏使用与登录事件关联的维度来定义查询。

例如：

```
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
```



Facets

您可以对登录事件使用以下方面：

- 位置-按国家/地区及其城市筛选登录事件。
- 操作系统-按操作系统及其版本过滤登录事件。
- 子网-按子网筛选访问事件。
- 客户端 **IP** 类型-按公共和私有 IP 类型过滤访问事件。
- **IP** 注册组织-按用户可用的 ISP 筛选访问事件。
- 专用 **VPN** 服务-按专用 VPN 网络名称筛选访问事件。
- 代理类型-按代理类型分类（例如 HTTP、Web、Tor 和 SOCKS）筛选访问事件。

> 注意
>
> 如果数据不可用或未识别，您可能还会看到不可用的标签。

用户风险时间表和概况

December 7, 2023

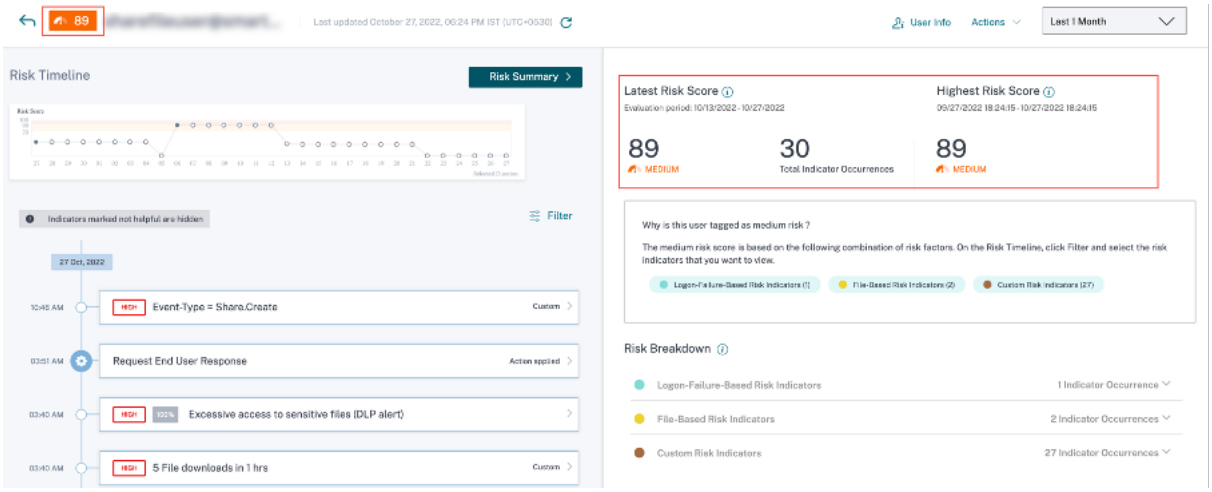
> ** 注意事项 **
>
> ：Citrix Content Collaboration 和 ShareFile 的使用寿命已接近尾声，不再向用户开放。

作为 Citrix Analytics 管理员，您可以通过用户个人资料上的用户风险时间表更深入地了解用户的风险行为。默认情况下，将显示最近一个月的用户风险时间表。您还可以查看在选定时间段内对他们的帐户执行的相应操作。从用户风险时间表中，您可以深入研究用户的个人资料，以了解以下内容：

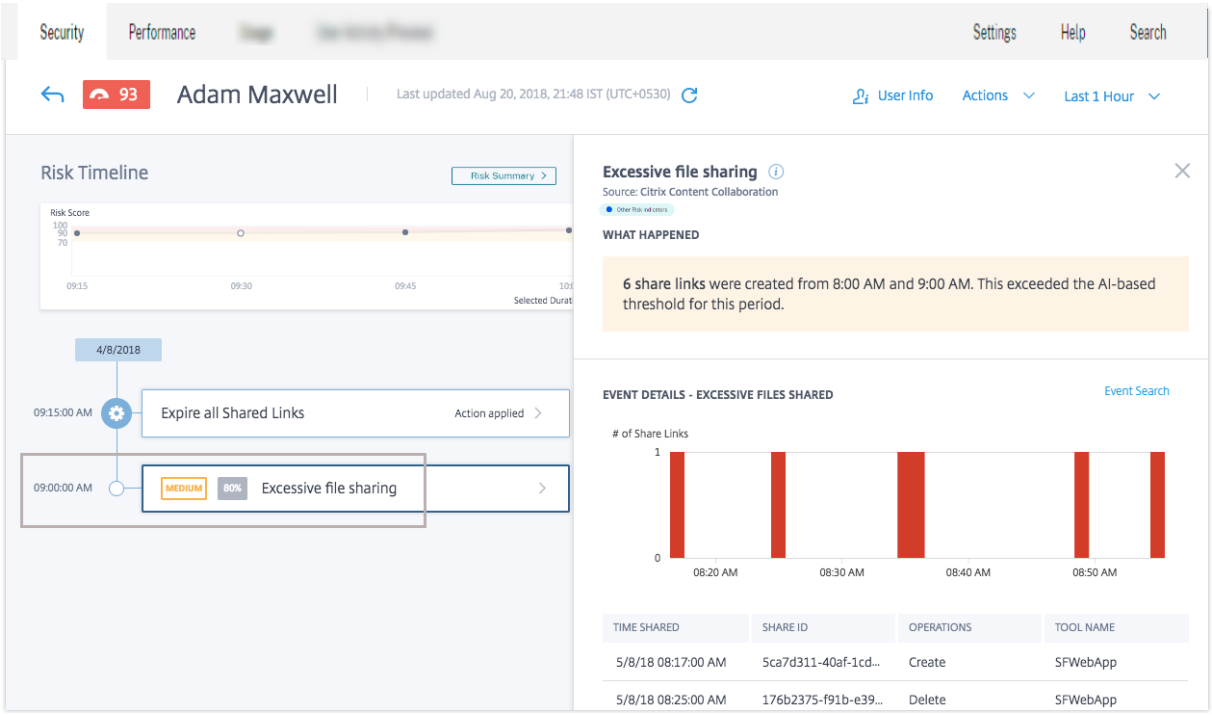
- 应用程序使用情况
- 数据使用量
- 设备使用情况
- 地点使用情况

此外，您还可以查看用户的风险评分和风险指示器趋势，并确定用户是否为高风险用户。

您可以在用户风险时间表页面的左上角查看用户的最新风险评分。风险摘要 视图报告显示最新和历史最高分数。



当您转到用户的风险时间表时，您可以选择风险指示器或已应用于其帐户的操作。如果选择上述选项之一，右窗格将显示风险指示器部分或操作部分。



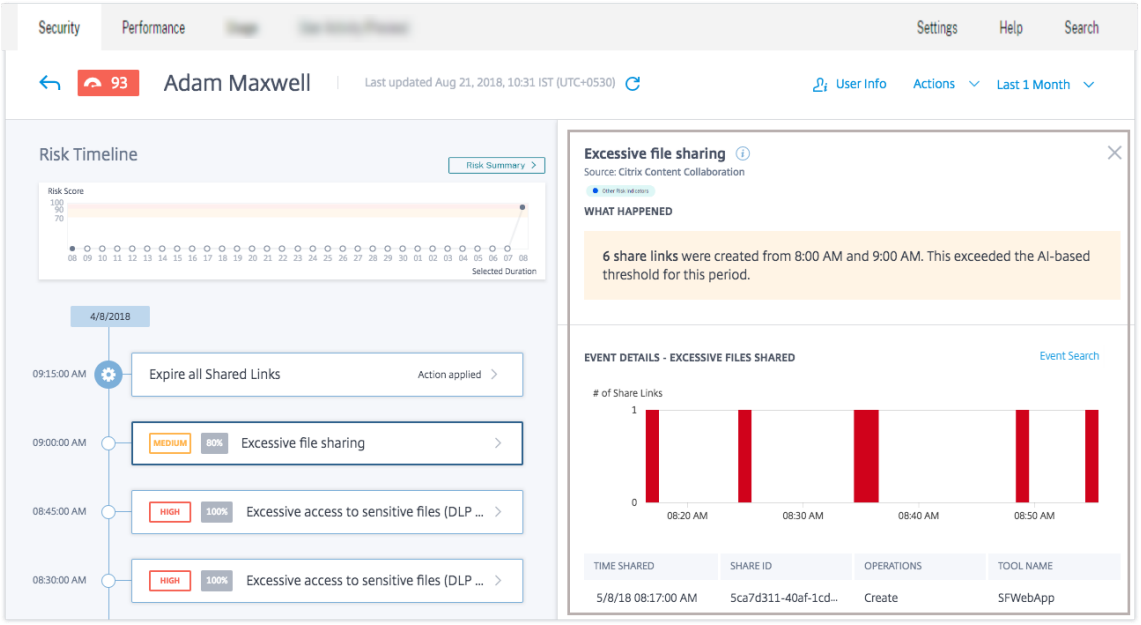
风险时间表

风险时间表显示以下信息：

- 风险指示器。风险指示器是可疑或可能对组织构成安全威胁的用户活动。当用户的行为偏离其正常行为时，就会触发这些指标。风险指示器可以用于以下数据源：
  - Citrix Content Collaboration

- Citrix Gateway
- Citrix Endpoint Management
- Citrix Virtual Apps and Desktops 或 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）
- Citrix Secure Private Access

当您从用户的时间轴中选择风险指示器时，风险指示器信息部分将显示在右窗格中。您可以查看风险指示器的原因以及事件的详细信息。它们大致分为以下几个部分：



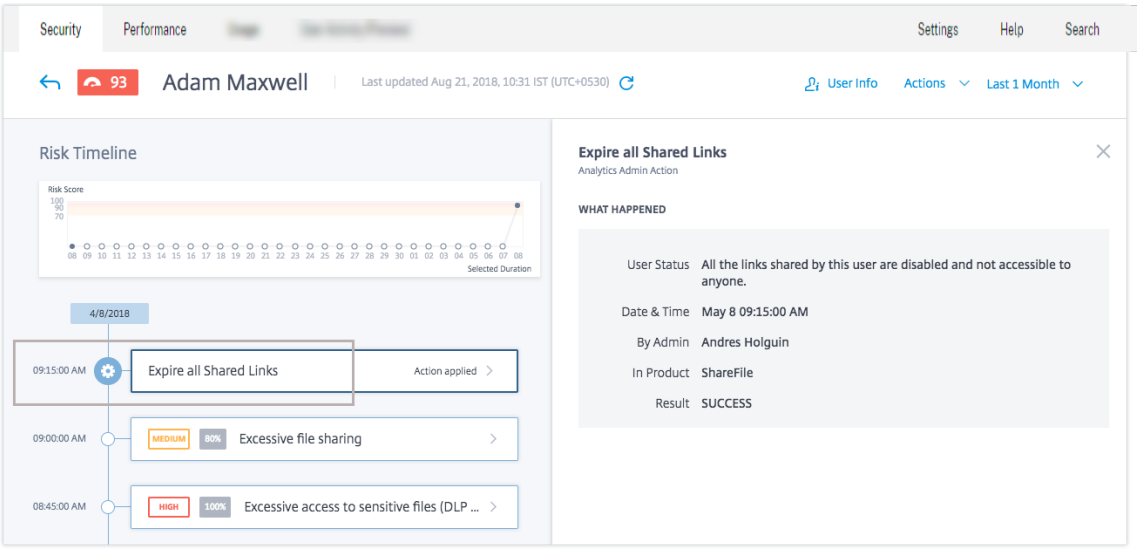
- 发生了什么事。您可以在此处查看风险指示器的摘要。例如，如果您选择了 过多的文件共享 风险指示器。在发生了什么部分，您可以查看发送给收件人的共享链接的数量以及发生共享事件的时间。
- 活动详情。您可以以图形和表格格式查看各个事件条目以及事件的详细信息。单击 事件搜索 以访问自助搜索页面并查看与用户风险指示器对应的事件。有关详细信息，请参阅 自助搜索。
- 其他上下文信息。在此部分中，您可以查看事件发生期间共享的数据（如果有）。

您可以手动将风险指示器标记为有用或无用。有关详细信息，请参阅为用户风险指示器提供反馈。

了解更多：风险指示器

- 操作。操作可帮助您应对可疑事件并防止将来发生异常事件。已应用于用户个人资料的操作显示在风险时间表上。这些操作可以通过配置的策略自动应用到用户的帐户，也可以手动应用特定操作。

  了解更多信息：政策和行动。



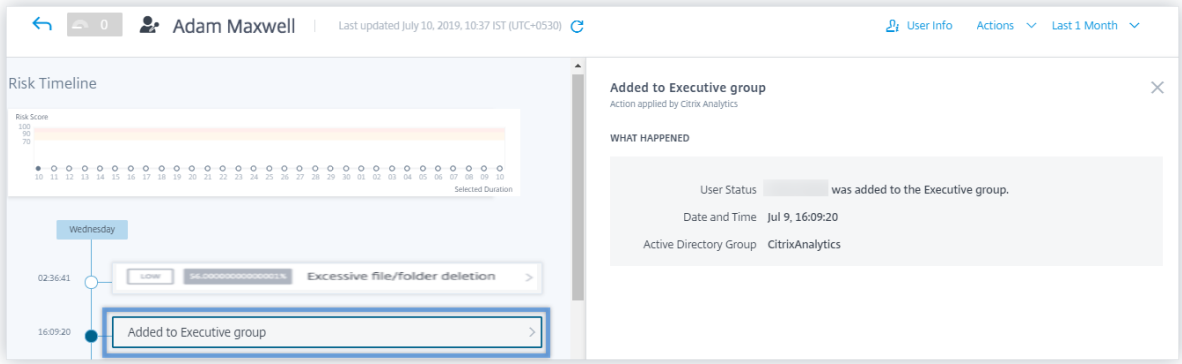
- 特权用户事件。每当用户的 Admin 或 Executive 权限状态发生变化时，都会触发特权用户事件。当为用户触发风险指示器时，您可以将其与指定的权限状态更改事件关联起来。如有必要，您可以对用户配置文件应用适当的操作。用户风险时间表上显示的管理员或执行人员权限事件如下：

  - 已添加到执行组
  - 已从执行组中删除
  - 权限提升为管理员
  - 管理员权限已移

  以添加到高管特权组 **CitrixAnalytics** 中的用户 Adam Maxwell 为例。添加到管理人员组 事件将添加到用户的风险时间表中。现在，Adam 开始过度删除文件和文件夹，并触发检测异常行为的机器学习算法。文件或文件夹删除过多 风险指示器将添加到用户的风险时间表中。您可以在风险时间表上比较事件和风险指示器。比较之后，您可以确定风险指示器是否是由于事件而触发的。如果是，你可以对亚当的个人资料采取适当的行动。有关特权用户的详细信息，请参阅 特权用户。

从用户的时间轴中选择事件时，事件信息部分将显示在右窗格中。

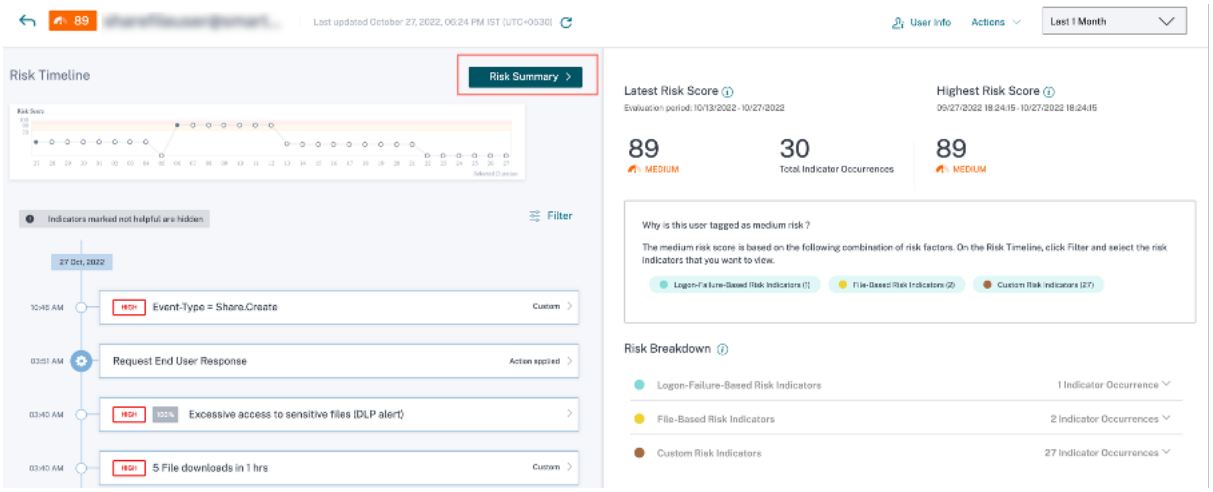
对于管理人员，右窗格显示诸如 用户状态、日期和时间以及 **Active Directory** 组之类的信息。



对于管理员权限事件，右窗格会显示 用户状态、日期和时间以及在产品中等信息。

风险摘要

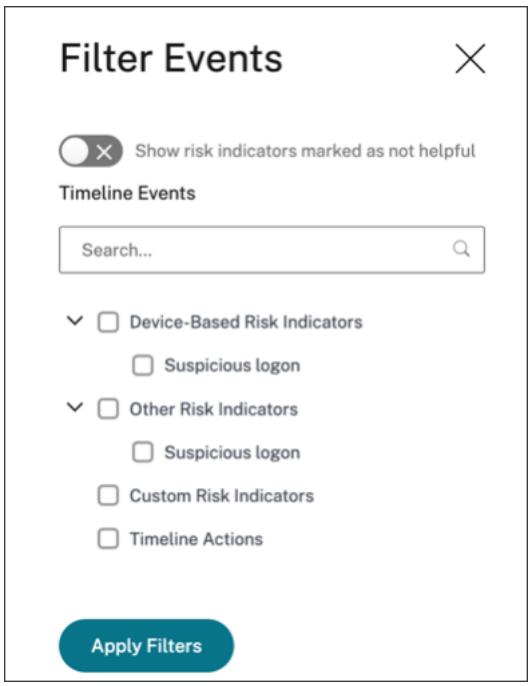
查看与影响其风险评分的用户相关的风险因素。您可以查看所选时间段内作为最大值的风险评分详情，以及最新的分数和相应的风险指标数量。从主登录页面或风险用户页面导航到用户时间轴后，源页面上的时间选择将保留。有关风险因素的更多信息，请参阅 Citrix 用户风险指示器。



单击 风险摘要 查看以下信息：

- 最新风险评分：最新的风险评分根据最近的行为表明了用户的当前风险。风险评分决定了用户在过去 2 周内对组织构成的风险级别。风险评分值是动态的，根据用户行为分析的不同而有所不同。根据分数，用户可以属于以下类别之一：高风险用户、中等风险用户、低风险用户和零风险分数的用户。有关用户类别的更多信息，请参阅 用户控制板。
  - 指标出现次数总数：表示过去两周内用户触发的风险指示器总数。这些触发的风险指示器决定了用户的风险评分。
- 最高风险分数：最高风险分数表示在所选时段内为该用户计算的风险评分的最大值。它代表了用户的总体风险，可能并不总是等于最新的风险分数。
- 风险因素：表示与构成风险评分的用户活动相关的风险因素的一种或多种组合。
- 风险细分：表示用户针对每个风险因素触发的风险指标数量。展开该行以查看详细信息。

在用户时间轴上，单击 筛 选，然后选择与用户关联的风险因素、应用的操作或特权用户状态，然后查看相应的事件。



用户资料

用户配置文件 页面显示来自用户活动目录的以下用户信息：

- 职称
- 地址
- 电子邮件
- 電話
- 位置
- 组织

Citrix 用户风险指示器

April 12, 2024

> 注意
>
> 注意
>
> ：Citrix Content Collaboration 和 ShareFile 已到期，用户无法再使用。

用户风险指示器是看起来可疑或可能对组织构成安全威胁的用户活动。这些风险指示器涵盖部署中使用的所有 Citrix 产品。当用户的行为偏离正常情况时，会触发风险指示器。每个风险指标都可以有一个或多个与之相关的风险因素。这些风险因素可帮助您确定用户事件中的异常类型。风险指示器及其相关的风险因素决定用户的风险评分。

以下是与风险指标相关的风险因素：

- 基于设备的风险指示器：当用户从根据用户的设备历史记录被视为异常的设备登录时触发。
- 基于位置的风险指示器：当用户使用与根据用户的位置历史记录被视为不寻常的位置关联的 IP 地址登录时触发。
- 基于 **IP** 的风险指示器：当用户尝试从已确定为可疑的 IP 地址访问资源时触发，无论该 IP 地址对用户来说是否异常。
- 基于登录失败的风险指示器：当用户出现过多或异常登录失败的模式时触发。
- 基于数据的风险指示器：当用户尝试从 Workspace 会话中泄露数据时触发。正在观察的用户行为包括复制或粘贴事件、下载模式等。
- 基于文件的风险指示器：根据用户的历史访问模式，当用户在 Content Collaboration 上有关文件访问的行为被视为异常时触发。正在观察的用户行为包括下载模式，对敏感内容的访问，表示勒索软件的活动等。
- 自定义风险指示器：当满足预配置的条件或用户定义的条件时触发。有关详细信息，请参阅以下文章：
  - 自定义风险指示器
  - 预配置的自定义风险指标和策略
- 其他风险指示器-不属于任何一个预定义风险因素的风险指示器，例如基于设备、基于位置和基于登录失败的风险指示器。

风险指标还根据相似的风险分为风险类别。有关更多信息，请参阅 风险类别。

下表显示了风险指标、风险因素和风险类别之间的相关性。

产品	用户风险指示器	风险因素	风险类别
Citrix Endpoint Management	检测到已列入黑名单的应用	其他风险指示器	受损的端点
	检测到越狱或获得 Root 权限的设备	其他风险指示器	受损的端点
	检测到非托管设备	其他风险指示器	受损的端点
Citrix Gateway	端点分析 (EPA) 扫描失败	其他风险指示器	受影响的用户

产品	用户风险指示器	风险因素	风险类别
	验证失败过多	基于登录失败的风险指示器	受影响的用户
	不可能旅行	基于位置的风险指示器	受影响的用户
	从可疑 IP 登录	基于 IP 的风险指示器	受影响的用户
	可疑登录	基于设备的风险指标、基于 IP 的风险指示器、基于位置的风险指示器和其他风险指标	受影响的用户
	异常的身份验证	基于登录失败的风险指示器	受影响的用户
Citrix Secure Private Access	尝试访问列入黑名单的 URL	其他风险指示器	内幕威胁
	数据下载过多	其他风险指示器	内幕威胁
	网站访问风险	其他风险指示器	内幕威胁
	不寻常的上载量	其他风险指示器	内幕威胁
Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）和本地 Citrix Virtual Apps and Desktops	不可能旅行	基于位置的风险指示器	受影响的用户
	潜在的数据泄露	基于数据的风险指示器	数据泄露
	可疑登录	基于设备的风险指标、基于 IP 的风险指示器、基于位置的风险指示器和其他风险指标	受影响的用户

您可以手动将风险指示器标记为有用或无用。有关详细信息，请参阅为用户风险指示器提供反馈。

Citrix Endpoint Management 风险指示器

May 7, 2022

检测到已列入黑名单的应用

Citrix Analytics 会根据包含黑名单应用程序的设备中的活动检测访问威胁，并触发相应的风险指示器。

当 Endpoint Management 服务在软件清单期间检测 到列入黑名单的应用程序时，触发检测到黑名单的应用程序的设 备风险指示器。该警报可确保只有授权的应用程序才能在组织网络上的设备上运行。

与检测到已列入黑名单的应用程序的设备风险指示器相关的风险因素是其他风险指示器。有关风险因素的更多信息，请参阅 Citrix 用户风险指示器。

什么时候检测到带有黑名单应用程序的设备的风险指示器触发?

在用户的 设备上检测到黑名单应 用程序时，将报告检测到黑名单应用程序的设备风险指示器。当 Endpoint Management 服务在软件清点期间检测到设备上的一个或多个列入黑名单的应用程序时，会向 Citrix Analytics 发送事件。

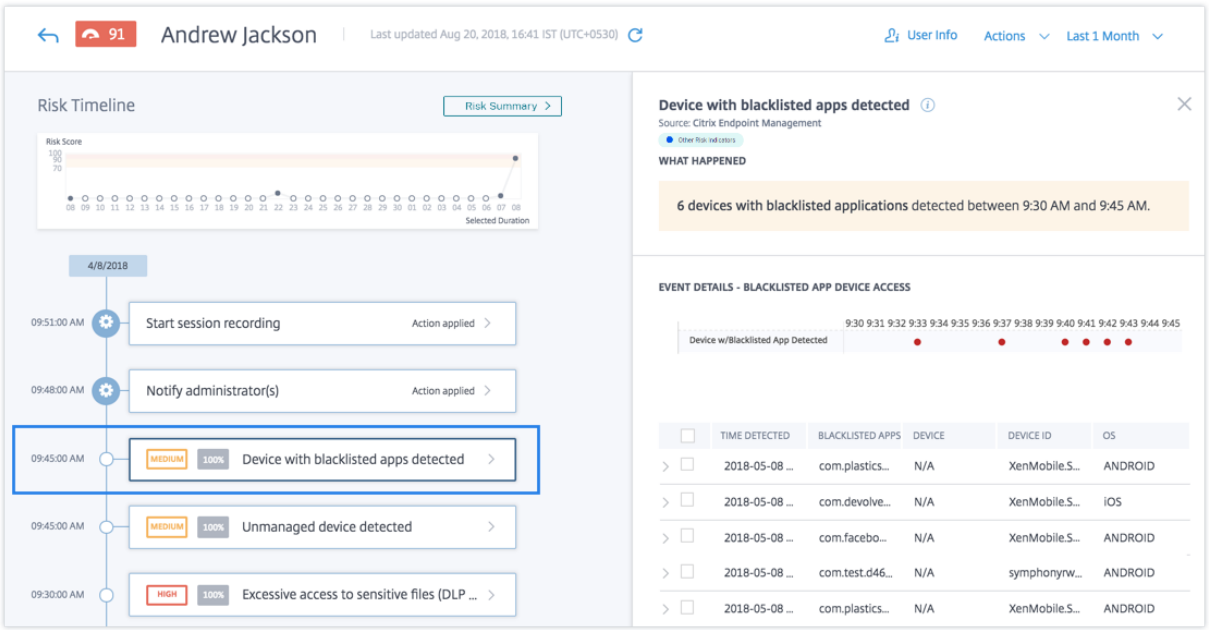
Citrix Analytics 会监控这些事件并更新用户的风险评分。此外，它还将一个 设备添加到用户的风险时间表中，其中检测到了黑名单应 用程序的风险指示

如何分析设备与被列入黑名单的应用程序检测到的风险指示器?

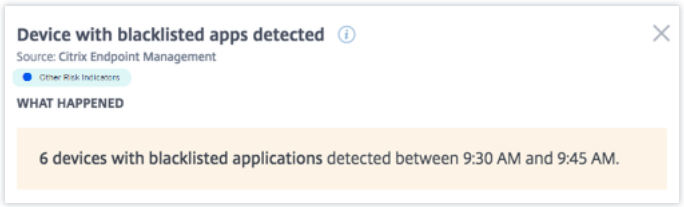
以用户安德鲁·杰克逊为例，他使用的设备最近安装了黑名单的应用程序。Endpoint Management 将此情况报告给 Citrix Analytics，Citrix Analytics 将更新的风险评分分配给 Andrew Jackson。

从安德鲁·杰克逊的风险时间表中，您可以选择已报告的 设备，其中检测到了黑名单应用程序此时将显示事件的原因以及详细信息，例如列入黑名单的应用程序的列表、Endpoint Management 检测到列入黑名单的应用程序的时间等。

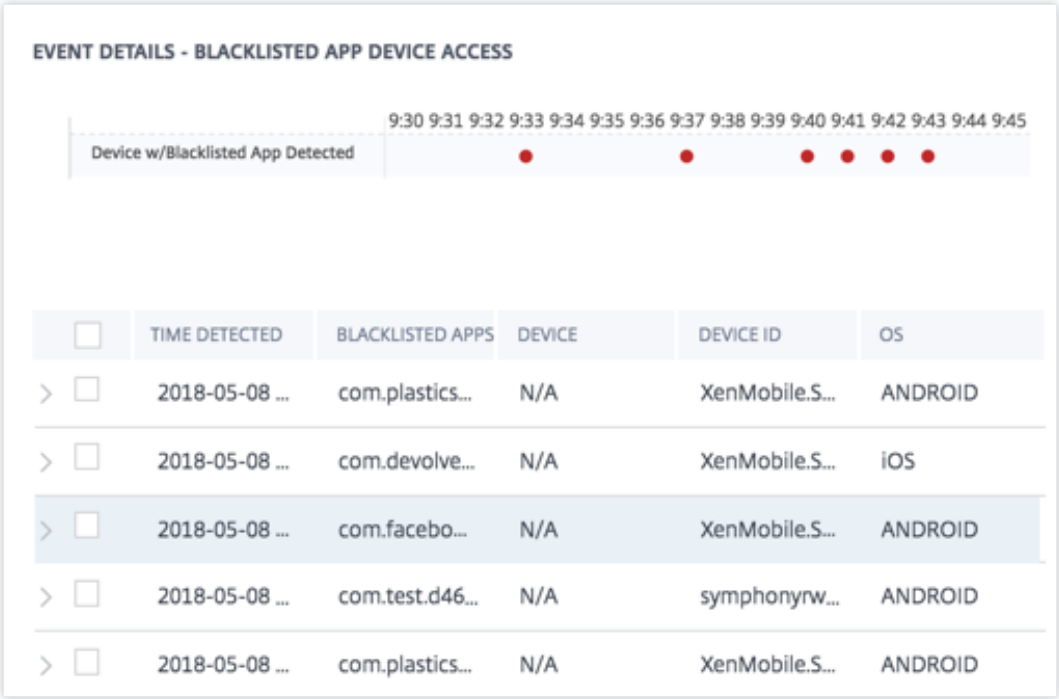
要查看 检测到用户的黑名单应用程序的设备 风险指示器，请导航到“安全”>“用户”，然后选择该用户。



- 在发 生了什么 部分，您可以查看事件的摘要。您可以查看 Endpoint Management 服务检测到的具有列入黑名单的应用程序的设备数量以及事件发生的时间。



- 事 件详细信息—列入黑名单的应用程序设备访问 部分，事件以图形和表格格式显示。这些事件还在图表中显示为单个条目，并且该表提供了以下关键信息：
  - 检测到的时间-Endpoint Management 报告的黑名单应用程序存在时。
  - 列入黑名单的应用程序-设备上列入黑名单的应用。
  - 设备-使用的移动设备。
  - 设备 **ID**-有关用于登录会话的设备 ID 的信息。
  - 操作系统**-**移动设备的操作系统。



> 注意：
>
> 除了以表格格式查看详细信息之外，您还可以单击警报实例对应的箭头以查看更多详细信息。

您可以对用户应用哪些操作**?**

您可以对用户的帐户执行以下操作：

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。

- 通知管理员。当用户帐户中存在任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的个人资料并选择相应的风险指示器。从操作菜单中，选择一个操作，然后单击应用。

> 注意
>
> 无论触发风险指示器的数据源如何，都可以应用与其他数据源相关的操作。

检测到越狱或获得 **Root** 权限的设备

Citrix Analytics 会根据越狱或获得 Root 权限的设备活动检测访问威胁，并触发相应的风险指示器。

当用户使用 已越狱或获得 **Root** 权限的设备 连接到网络时，将触发越狱或获得 Root 权限的设备风险指示器。Secure Hub 检测设备并将事件报告给 Endpoint Management 服务。该警报可确保您组织的网络上只有授权用户和设备。

与越狱或已获得 Root 权限的设备风险指示器相关的风险因素是其他风险指示器。有关风险因素的更多信息，请参阅 Citrix 用户风险指示器。

检测到越狱或获得 **Root** 权限的设备的风险指示器何时触发**?**

对于安全管理人员来说，确保用户使用符合网络标准的设备进行连接非常重要。检测到越狱或获得 **Root** 权限的设备 的风险指示器会向您发出警报，提醒您使用已越狱的 iOS 设备或已获得 root 权限的 Android 设备的用户。

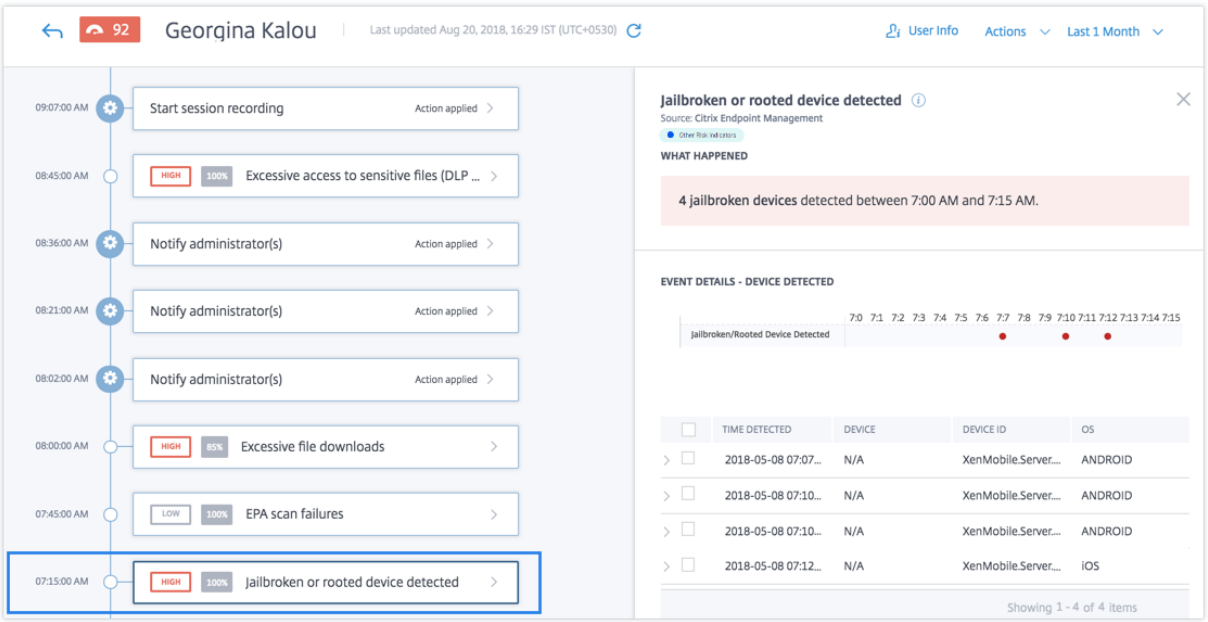
当注册的 设备越狱或获得 **Root** 权 限时，会触发越狱或获得 Root 权限的设备风险指示器。Secure Hub 在设备上检测到事件并将其报告给 Endpoint Management 服务。

如何分析检测到的越狱或已获得 **Root** 权限的设备的风险指示器

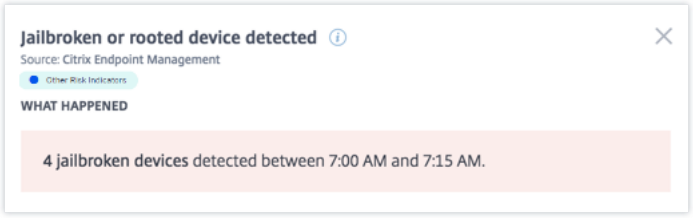
以用户 Georgina Kalou 为例，他的注册 iOS 设备最近越狱了。Citrix Analytics 检测到这种可疑行为，并将风险评分分配给 Georgina Kalou。

从 Georgina Kalou 的风险时间表中，您可以选择报告的 已越狱或已获得 **Root** 设备检测到 的风险指示器。事件的原因与详细信息一起显示，例如触发风险指示器的时间、事件的描述等。

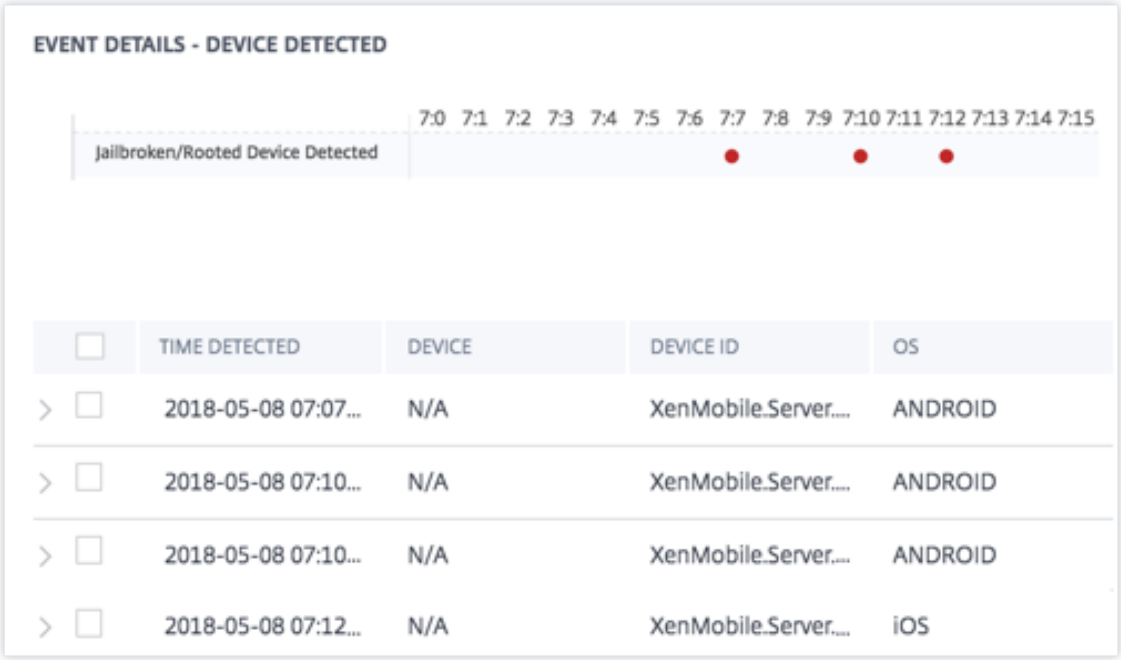
要查看用户的 已越狱或已获得 **Root** 权限的设备检测到 的风险指示器，请导航到 “安全” **>** “用户”，然后选择该用户。



- 在 发生了什么 部分，你可以查看事件的摘要。您可以查看检测到的越狱或获得 Root 权限的设备的数量以及事件发生的时间。



- 事 件详细信息—检测到设备 部分，事件以图形和表格格式显示。这些事件还在图表中显示为单个条目，并且该表提供了以下关键信息：
  - 检测到时间。检测到越狱或获得 Root 权限的设备的时间。
  - 设备。使用的移动设备。
  - 设备 **ID**。有关用于登录会话的设备的 ID 的信息。
  - 操作系统。移动设备的操作系统。



> 注意
>
> 除了以表格格式查看详细信息之外，还可以单击警报实例对应的箭头以查看更多详细信息。

您可以对用户应用哪些操作?

您可以对用户的帐户执行以下操作：

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户中存在任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的个人资料并选择相应的风险指示器。从操作菜单中，选择一个操作，然后单击应用。

> 注意
>
> 无论触发风险指示器的数据源如何，都可以应用与其他数据源相关的操作。

检测到非托管设备

Citrix Analytics 会根据非托管设备活动检测访问威胁并触发相应的风险指示器。

当 设备出现以下情况时，会触发检测到的非 托管设备风险指示器：

- 由于自动操作而远程擦除。

- 由管理员手动擦除。
- 用户已取消注册。

与检测到的非托管设备风险指示器相关的风险因素是其他风险指示器。有关风险因素的更多信息，请参阅 Citrix 用户风险指示器。

检测到非托管设备的风险指示器何时触发?

当用户的设备处于非托管状态时，将报告检测到的未托管设备风险指示器。由于以下原因，设备更改为非托管状态：

- 用户执行的操作。
- Endpoint Management 员或服务器执行的操作。

在组织中，使用 Endpoint Management 服务，您可以管理访问网络的设备和应用程序。有关详细信息，请参阅 管理模式。

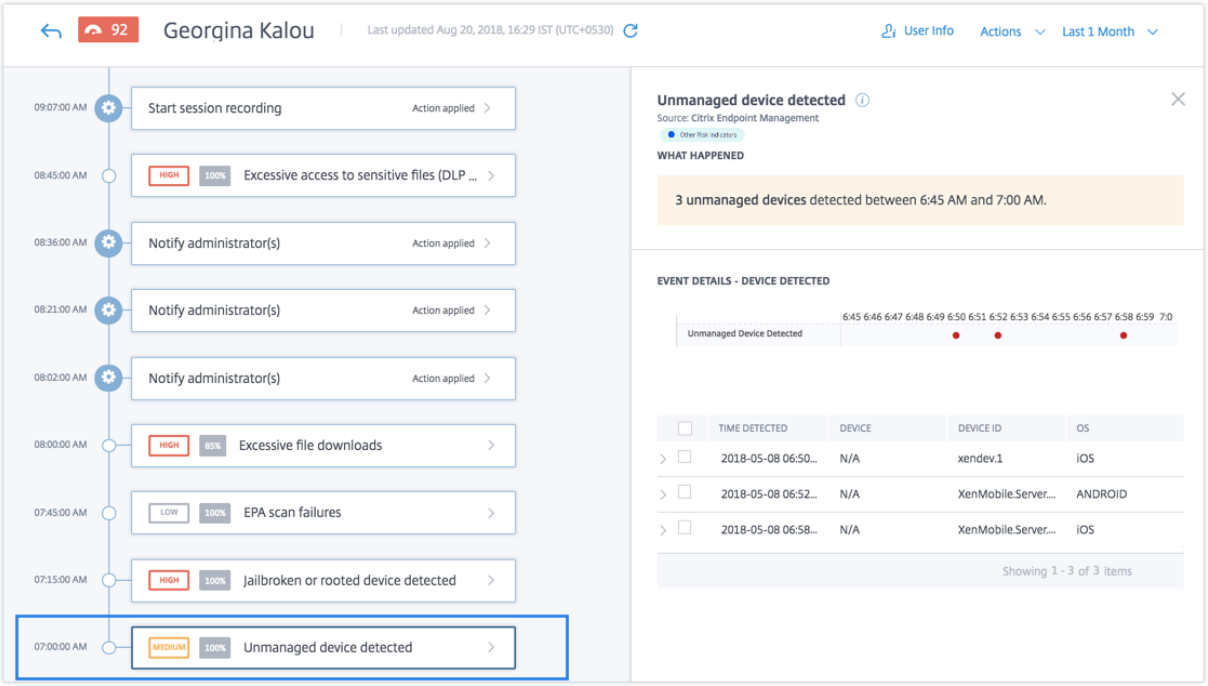
当用户的设备更改为非托管状态时，Endpoint Management 服务会检测到此事件并将其报告给 Citrix Analytics。用户的风险评分已更新。检测到的未托管设备风险指示器将添加到用户的风险时间表中。

如何分析非托管设备检测到的风险指示器?

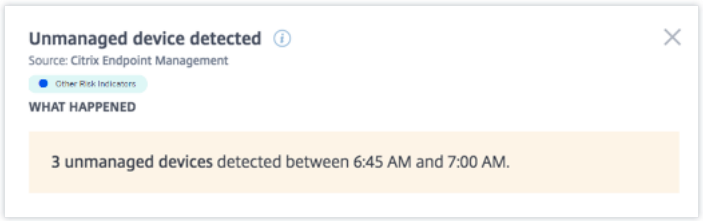
考虑用户 Georgina Kalou，他的设备被服务器上的自动操作远程擦除。Endpoint Management 将此事件报告给 Citrix Analytics，后者将更新的风险评分分配给 Georgina Kalou。

从 Georgina Kalou 的风险时间表中，您可以选择报告的检测到的非托管设备风险指示器。事件的原因与详细信息一起显示，如触发风险指示器的时间、事件描述等。

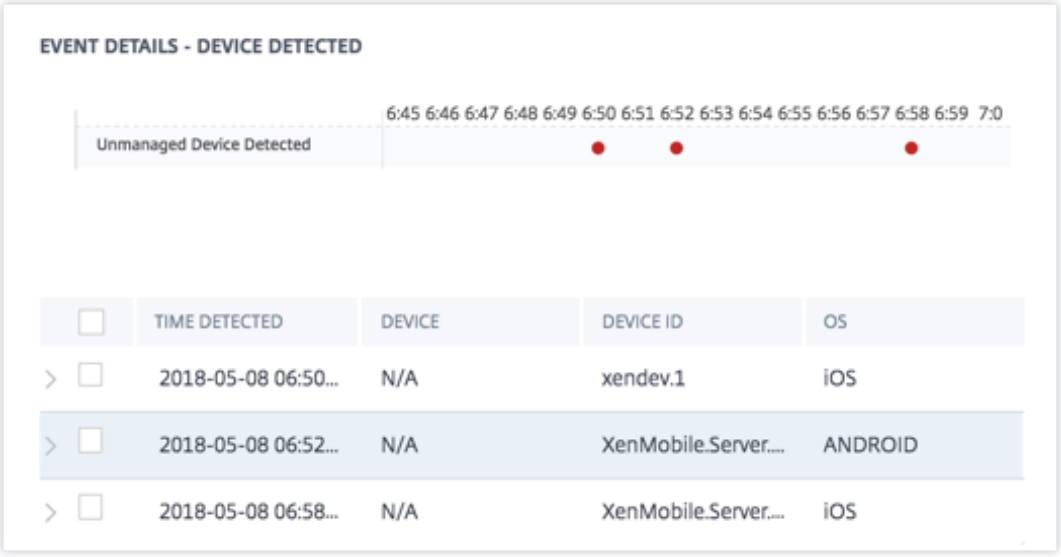
要查看用户的检测到的未托管设备风险指示器，请导航到安全 > 用户，然后选择该用户。



- 在 发生了什么 部分，你可以查看事件的摘要。您可以查看检测到的非托管设备的数量以及事件发生的时间。



- 事 件详细信息—检测到设备 部分，事件以图形和表格格式显示。这些事件还在图表中显示为单个条目，并且该表提供了以下关键信息：
  - 检测到时间。检测到事件的时间。
  - 设备。使用的移动设备。
  - 设备 **ID**。移动设备的设备 ID。
  - 操作系统。移动设备的操作系统。



您可以对用户应用哪些操作**?**

您可以对用户的帐户执行以下操作：

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户中存在任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的个人资料并选择相应的风险指示器。从操作菜单中，选择一个操作，然后单击应用。

> 注意
>
> 无论触发风险指示器的数据源如何，都可以应用与其他数据源相关的操作。

Citrix Gateway 风险指示器

July 12, 2022

端点分析 **(EPA)** 扫描失败

Citrix Analytics 会根据 EPA 扫描失败活动检测基于用户访问的威胁，并触发相应的风险指示器。

与端点分析扫描失败风险指示器相关的风险因素是其他风险指示器。有关风险因素的更多信息，请参阅 Citrix 用户风险指示器。

EPA 扫描故障风险指示器何时触发**?**

当用户尝试使用未通过 Citrix Gateway 的端点分析 (EPA) 扫描策略进行预身份验证或身份验证后的设备访问网络时，将报告 EPA 扫描失败风险指示器。

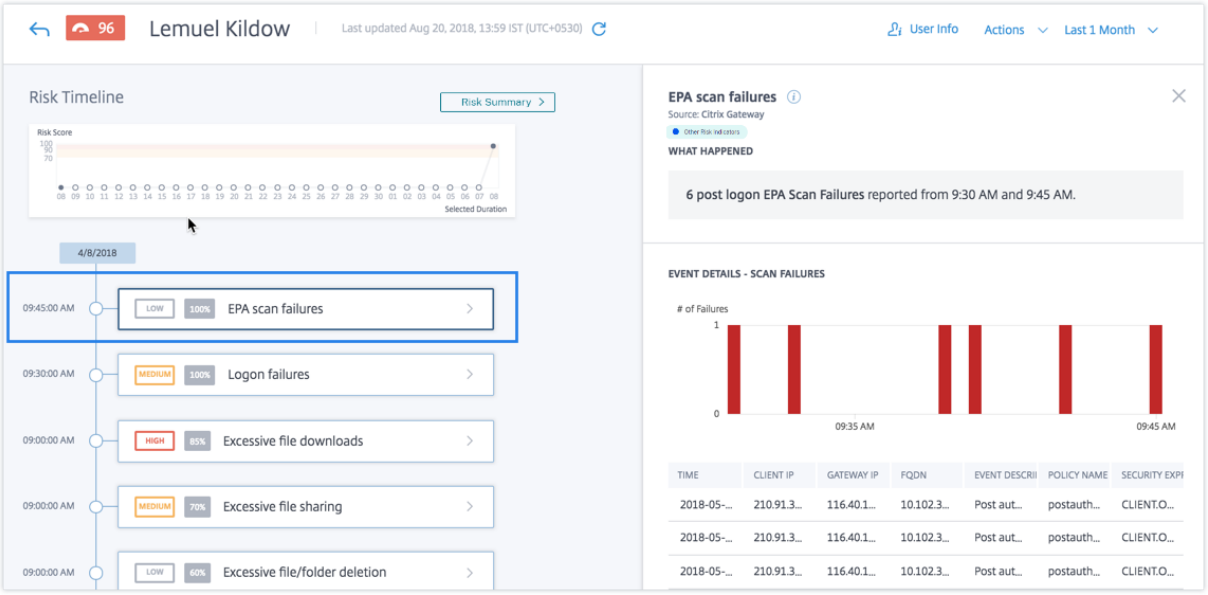
Citrix Gateway 检测到这些事件并将其报告给 Citrix Analytics。Citrix Analytics 会监视所有这些事件，以检测用户是否有太多 EPA 扫描故障。当 Citrix Analytics 确定用户的 EPA 扫描失败过多时，它会更新用户的风险评分，并将 EPA 扫描失败风险指示器条目添加到用户的风险时间表中。

如何分析 **EPA** 扫描故障风险指示器**?**

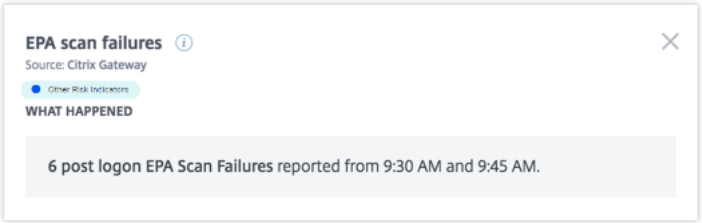
以用户 Lemuel 为例，他最近多次尝试使用 Citrix Gateway 的 EPA 扫描失败的设备访问网络。Citrix Gateway 将此失败报告给 Citrix Analytics，该分析会向 Lemuel 分配更新的风险评分。EPA 扫描失败风险指示器已添加到 Lemuel Kildow 的风险时间表中。

要查看用户的 **EPA** 扫描失败 条目，请导航到“安全”**>**“用户”，然后选择该用户。

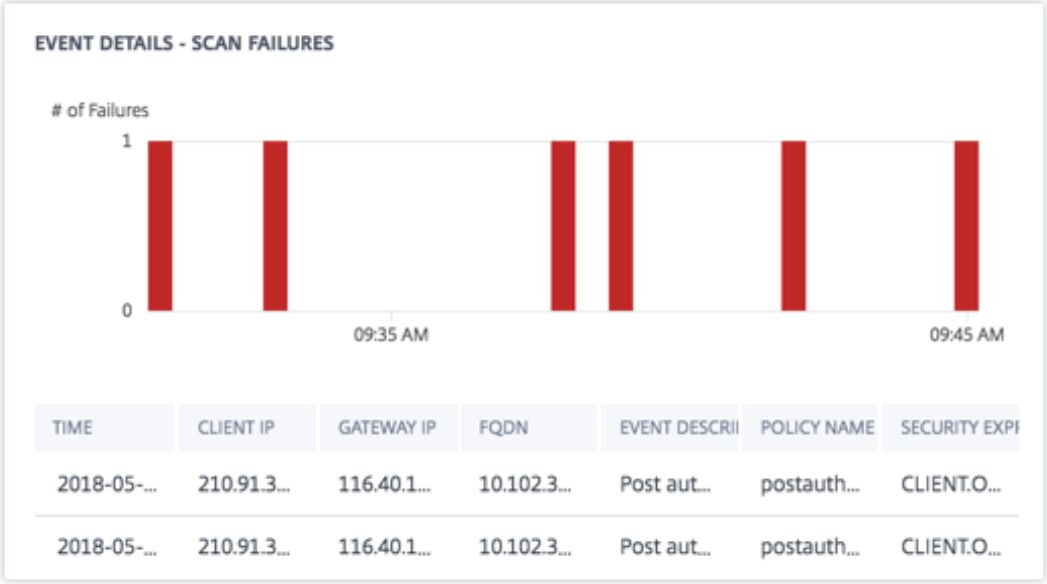
从 Lemuel Kildow 的风险时间表中，您可以选择为用户报告的最新 **EPA** 扫描失败 风险指示器。当您从时间轴中选择 EPA 扫描故障风险指示器条目时，右侧窗格中会显示相应的详细信息面板。



- 发生了什么 部分提供了 EPA 扫描失败风险指示器的简要摘要。并且，包括在选定时间段内报告的登录后 EPA 扫描失败的数量。



- “事 件详细信息—扫描失败”部分包括在选定时间段内发生的单个 EPA 扫描失败事件的时间轴可视化。此外，它还包括一个表，其中提供了有关每个事件的以下关键信息：
  - 时间。EPA 扫描失败发生的时间。
  - 客户端 **IP**。导致 EPA 扫描失败的客户端的 IP 地址。
  - 网关 **IP**。报告 EPA 扫描失败的 Citrix Gateway 的 IP 地址。
  - **FQDN**。Citrix Gateway 的 FQDN。
  - 事件描述。EPA 扫描失败原因的简要说明。
  - 策略名称。Citrix Gateway 上配置的 EPA 扫描策略名称。
  - 安全表达式。Citrix Gateway 上配置的安全表达式。



您可以对用户应用哪些操作**?**

您可以对用户的帐户执行以下操作：

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户中存在任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。
- 注销用户。当用户从其帐户注销时，在 Citrix Gateway 管理员清除“注销用户”操作之前，他们无法通过 Citrix Gateway 访问任何资源。
- 锁定用户：当用户的帐户由于异常行为而被锁定时，在网关管理员解锁帐户之前，他们无法通过 Citrix Gateway 访问任何资源。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的个人资料并选择相应的风险指示器。从操作菜单中，选择一个操作，然后单击应用。

> 注意
>
> 无论触发风险指示器的数据源如何，都可以应用与其他数据源相关的操作。

验证失败过多

Citrix Analytics 会根据过多的身份验证失败检测基于用户访问的威胁并触发相应的风险指示

与过多的身份验证失败风险指示器相关的风险因素是基于登录失败的风险指示器。有关风险因素的更多信息，请参阅 Citrix 用户风险指示器。

何时触发身份验证失败过多风险指示器

当用户在给定时间段内遇到多个 Citrix Gateway 身份验证失败时，会报告登录失败风险指示器。Citrix Gateway 身份验证失败可以是主要、次要或三级身份验证失败，具体取决于是否为用户配置了多重身份验证。

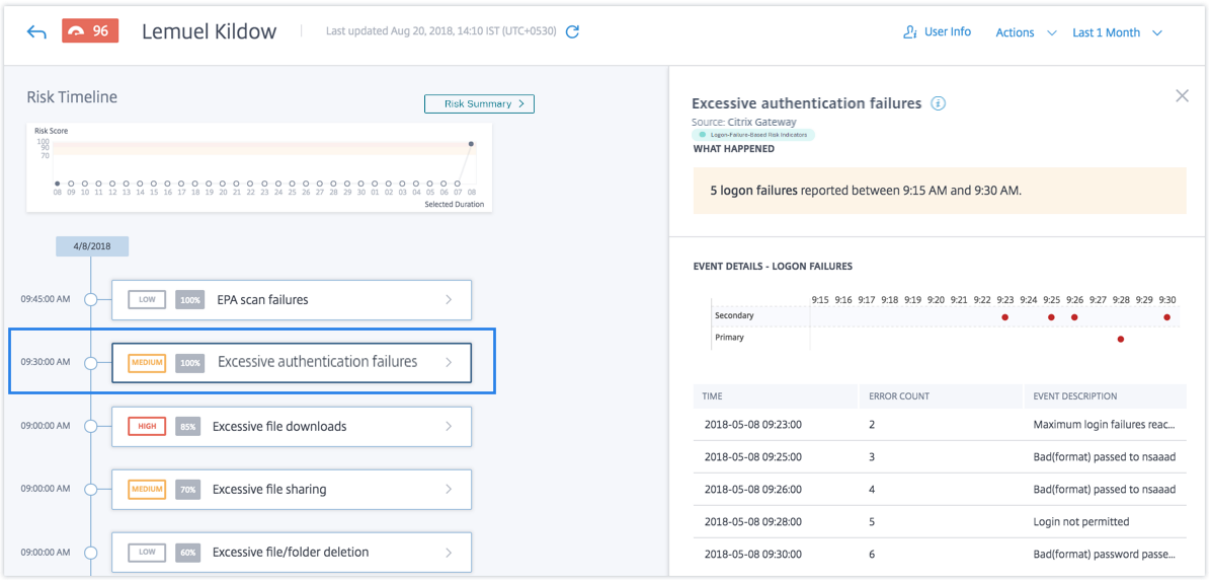
Citrix Gateway 会检测所有用户身份验证失败并将这些事件报告给 Citrix Analytics。Citrix Analytics 会监视所有这些事件，以检测用户是否遇到过多的身份验证失败。当 Citrix Analytics 确定过多的身份验证失败时，它会更新用户的风险评分。过度身份验证失败风险指示器已添加到用户的风险时间表中。

如何分析过多的身份验证失败风险指示器?

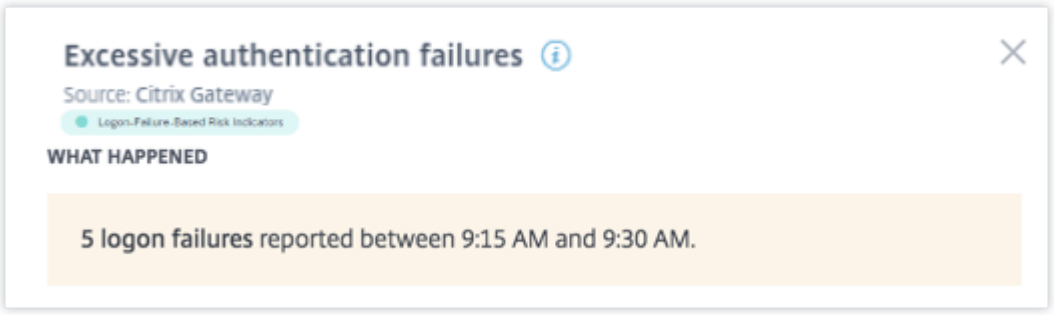
以用户 Lemuel 为例，他最近多次尝试对网络进行身份验证失败。Citrix Gateway 将这些失败报告给 Citrix Analytics，并将更新的风险评分分配给 Lemuel。过度验证失败 风险指示器添加到 Lemuel Kildow 的风险时间表中。

要查看用户的身份验证失败过多风险指示器条目，请导航到“安全”**>**“用户”，然后选择该用户。

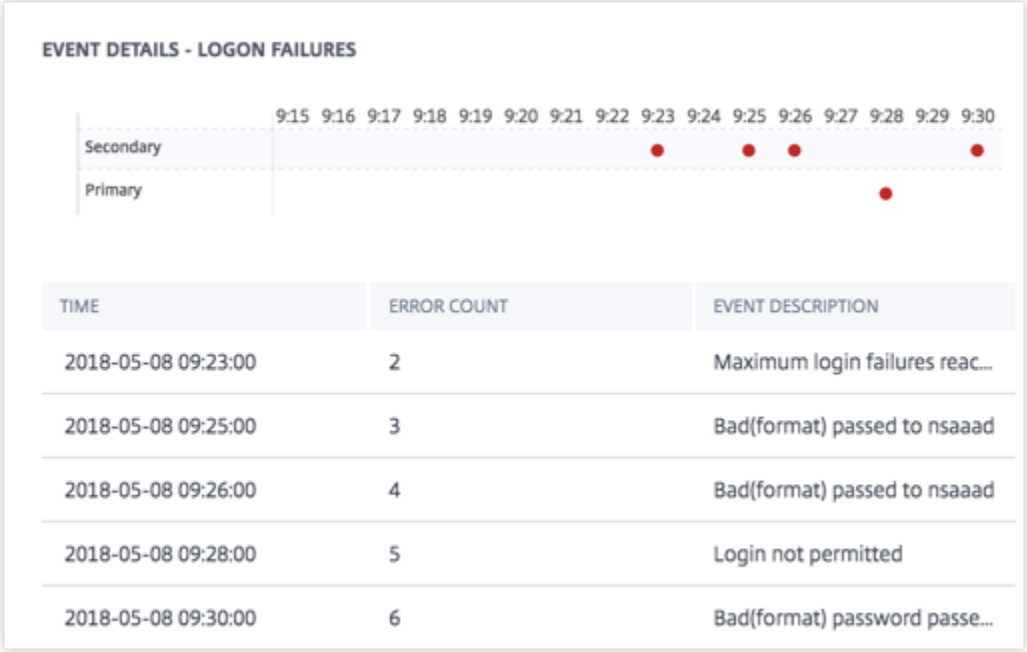
从 Lemuel Kildow 的风险时间表中，您可以选择为用户报告的最新 过多身份验证失败 风险指示器。从风险时间表中选择“过多身份验证失败 风险指示器”条目时，右窗格中将显示相应的详细信息面板。



- 发 生了什么事情 部分提供了风险指示器的简要摘要，包括在选定时间段内发生的身份验证失败的次数。



- “事 件详细信息”部分包括在选定时间段内发生的各个过多身份验证失败事件的时间轴可视化。此外，您还可以查看有关每个事件的以下关键信息：
  - 时间。登录失败发生的时间。
  - 错误计数。事件发生时和过去 48 小时内为用户检测到的身份验证失败次数。
  - 事件描述。登录失败原因的简要说明。



您可以对用户应用哪些操作?

您可以对用户的帐户执行以下操作:

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户中存在任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。
- 注销用户。当用户从其帐户注销时，在 Citrix Gateway 管理员清除“注销用户”操作之前，他们无法通过 Citrix Gateway 访问任何资源。
- 锁定用户：当用户的帐户由于异常行为而被锁定时，在网关管理员解锁帐户之前，他们无法通过 Citrix Gateway 访问任何资源。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的个人资料并选择相应的风险指示器。从操作菜单中，选择一个操作，然后单击应用。

> 注意
>
> 无论触发风险指示器的数据源如何，都可以应用与其他数据源相关的操作。

不可能旅行

Citrix Analytics 检测到用户的登录存在风险，如果连续登录来自两个不同的国家/地区，且时间段少于这两个国家/地区之间的预期旅行时间。

不可能的旅行时间情景表明存在以下风险：

- 凭据泄露：远程攻击者窃取合法用户的凭据。
- 共享凭据：不同的用户使用相同的用户凭据。

不可能的旅行风险指示器何时触发

不可能旅行风险指示器评估每对连续用户登录之间的时间和估计距离，并在距离大于个人在这段时间内可能行驶的距离时触发。

> 注意
>
> 此风险指示器还包含用于减少以下情况的误报警报的逻辑，这些情况不反映用户的实际位置：
>
> - 当用户通过代理连接通过 Citrix Gateway 登录时。
> - 当用户通过 Citrix Gateway 从托管客户端登录时。

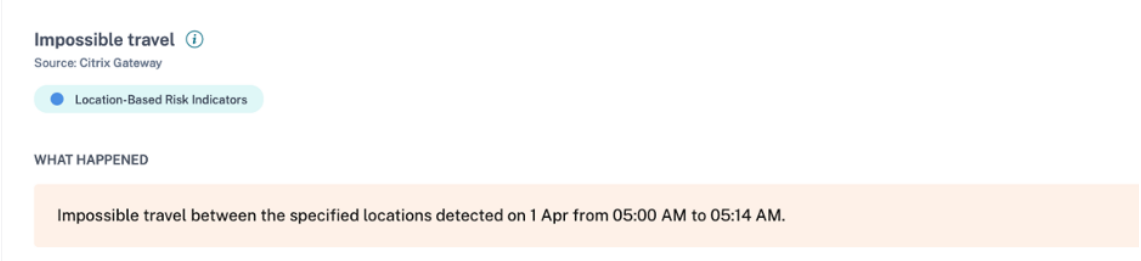
如何分析不可能的风险指标

以用户 Adam Maxwell 为例，他在一分钟的时间内从印度班加罗尔和挪威奥斯陆这两个地点登录。Citrix Analytics 将此登录事件检测为不可能的旅行场景，并触发不可能旅行风险指示器。风险指标被添加到 Adam Maxwell 的风险时间表中，并为他分配了风险评分。

要查看 Adam Maxwell 的风险时间表，请选择安全 **>** 用户。从“风险用户”窗格中，选择用户 Adam Maxwell。

从 Adam Maxwell 的风险时间表中，选择不可能的旅行风险指示器。您可以查看以下信息：

- 发生了什么 事部分简要概述了不可能旅行事件。



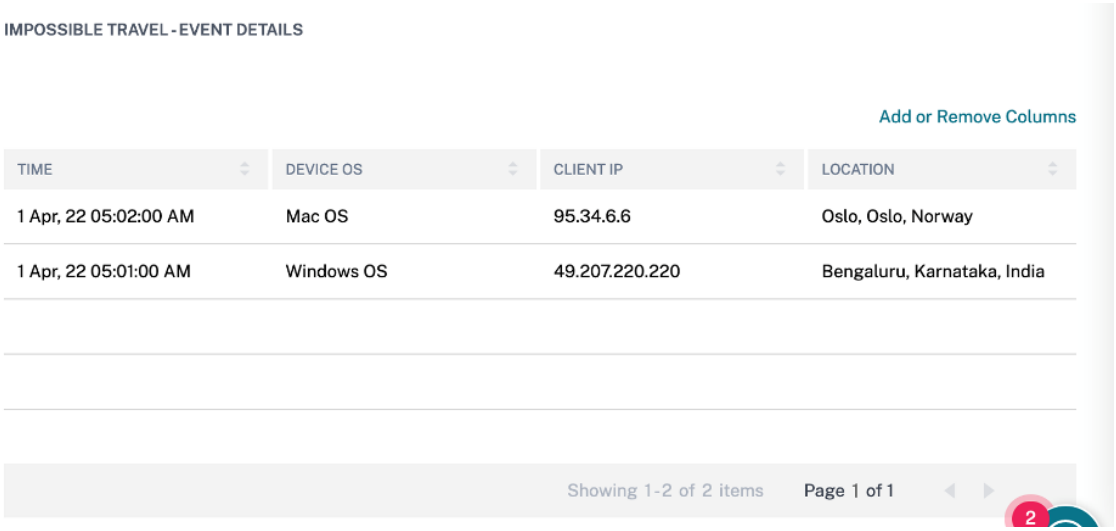
- 指标详情部分提供用户登录的位置、连续登录之间的持续时间以及两个位置之间的距离。

INDICATOR DETAILS

Event 1:	Logon on 1 Apr, 22 05:01:00 AM Location: Bengaluru, Karnataka, India
Event 2:	Logon on 1 Apr, 22 05:02:00 AM Location: Oslo, Oslo, Norway
Time Interval:	1 min
Distance:	7480 km(s)

- 登录位置 **-** 最近 **30** 天部分显示了用户不可能的出行地点和已知位置的地理地图视图。显示的是过去 30 天的位置数据。您可以将鼠标悬停在地图上的指针上，以查看每个位置的总登录次数。

- 不可能旅行 **-** 事件详情部分提供了有关不可能旅行事件的以下信息：
  - 时间：表示登录的日期和时间。
  - 设备操作系统：指示用户设备的操作系统。
  - 客户端 **IP**：表示用户设备的 IP 地址。
  - 位置：表示用户登录的位置。



您可以对用户应用哪些操作**?**

您可以对用户的帐户执行以下操作：

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户有任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。
- 注销用户。当用户从其帐户注销时，在 Citrix Gateway 管理员清除“注销用户”操作之前，他们无法通过 Citrix Gateway 访问任何资源。
- 锁定用户：如果用户的帐户因异常行为而被锁定，则在网关管理员解锁帐户之前，他们无法通过 Citrix Gateway 访问任何资源。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的配置文件并选择相应的风险指示器。从操作菜单中，选择一个操作，然后单击应用。

> 注意
>
> 无论触发风险指示器的数据源如何，都可以应用与其他数据源相关的操作。

从可疑 **IP** 登录

Citrix Analytics 根据来自可疑 IP 的登录活动检测用户访问威胁，并触发此风险指示器。

与可疑 IP 登录风险指示器相关的风险因素是基于 IP 的风险指示器。有关风险因素的更多信息，请参阅 Citrix 用户风险指示器。

何时触发来自可疑 **IP** 的登录风险指示器**?**

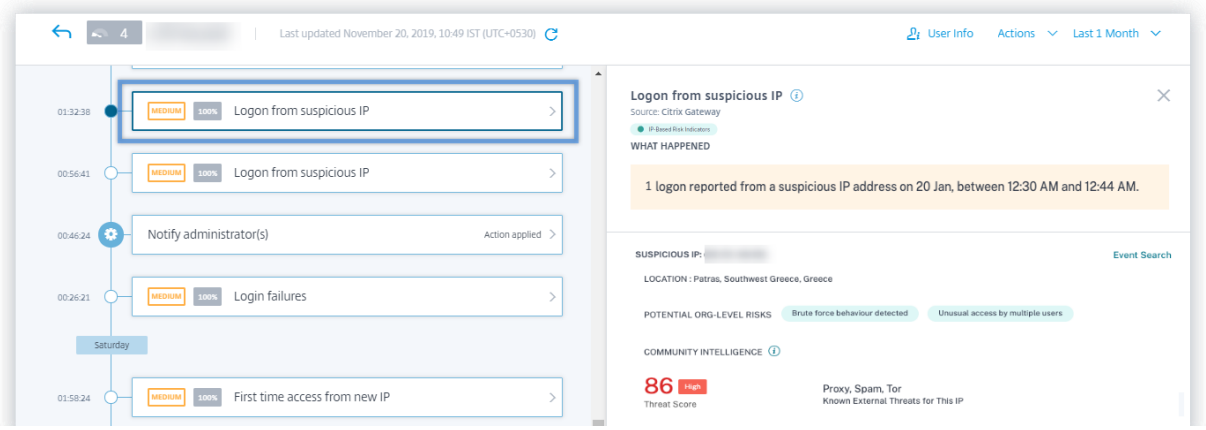
当用户尝试 从 **Citrix Analytics** 识别为可疑的 **IP** 地址访问网络时，将触发从可疑 **IP** 登 录风险指示器。根据以下情况之一，IP 地址被视为可疑：

- 在外部 IP 威胁智能源上列出
- 有来自异常位置的多个用户登录记录
- 登录尝试失败过多，可能表明存在暴力攻击

Citrix Analytics 监视从 Citrix Gateway 收到的登录事件，并检测用户是否已从任何可疑 IP 登录。当 Citrix Analytics 检测到来自可疑 IP 的登录尝试时，它会更新用户的风险评分，并将 可疑 **IP** 风险指示器条目中的登录 添加到用户的风险时间表中。

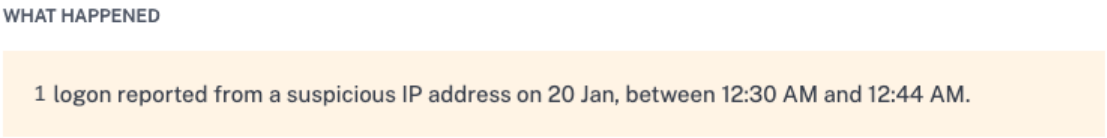
如何从可疑的 **IP** 风险指示器分析登录**?**

考虑试图从 Citrix Analytics 识别为可疑的 IP 地址访问网络的用户勒缪尔。Citrix Gateway 向 Citrix Analytics 报告登录事件，该分析将更新的风险分数分配给 Lemuel。从可疑 **IP** 登录 风险指示器已添加到 Lemuel Kildow 的风险时间表中。

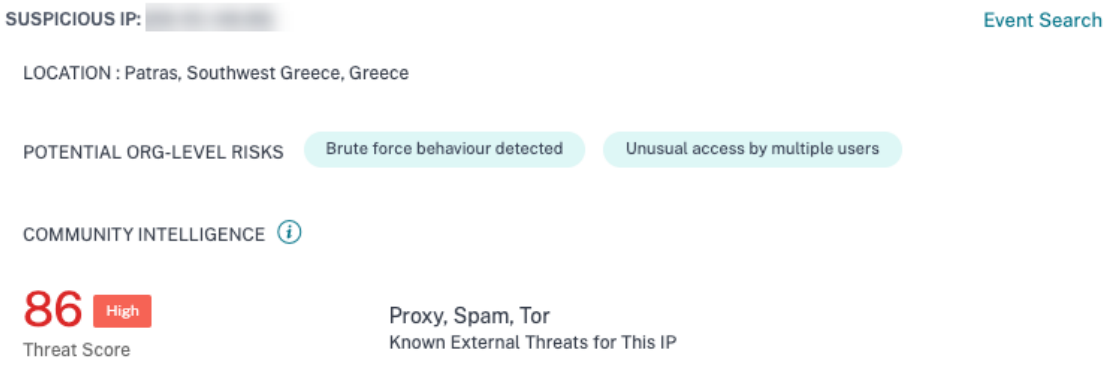


若要查看为用户报告的可疑 IP 风险登录指示器，请导航到“安全”>“用 户”，然后选择用户。从 Lemuel Kildow 的风险时间表中，您可以 从为用户报告的可疑 **IP** 风险指示器中选择最新的登录。从时间轴中选择 从可疑 **IP** 风险指示器条目中选择登录 时，右侧窗格中将显示相应的详细信息面板。

- “发生了什么”部分提供了来自可疑 IP 风险指示器的登录的简要摘要。并且，包括在选定时间段内报告的来自可疑 IP 地址的登录次数。

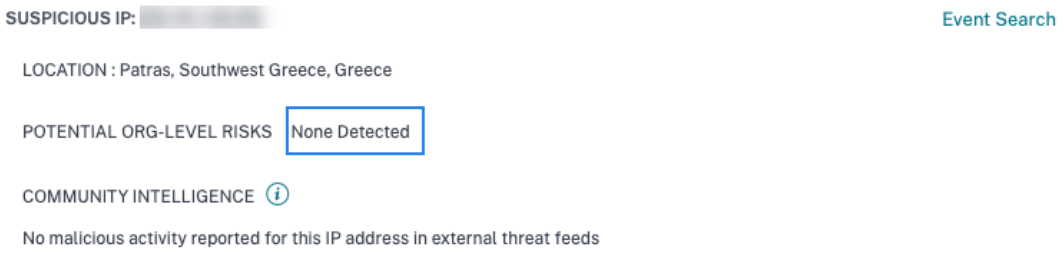


- 可疑 **IP** 部分提供以下信息：



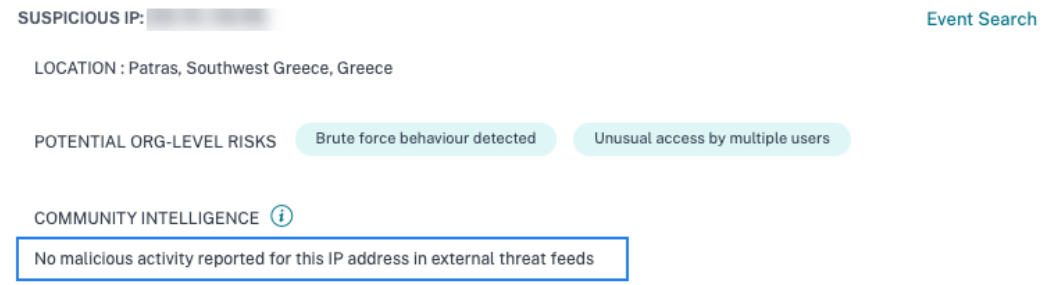
  - 可疑的 **IP**。与可疑登录活动关联的 IP 地址。
  - 位置。用户的城市、地区和国家/地区。根据数据的可用性显示这些位置。
  - 潜在的组织级风险。表示 Citrix Analytics 最近在您的组织中检测到的任何可疑 IP 活动模式。风险模式包括与潜在的暴力尝试一致的过度登录失败以及多个用户的异常访问。

    如果没有检测到组织中的 IP 地址的风险模式，则会看到以下消息。

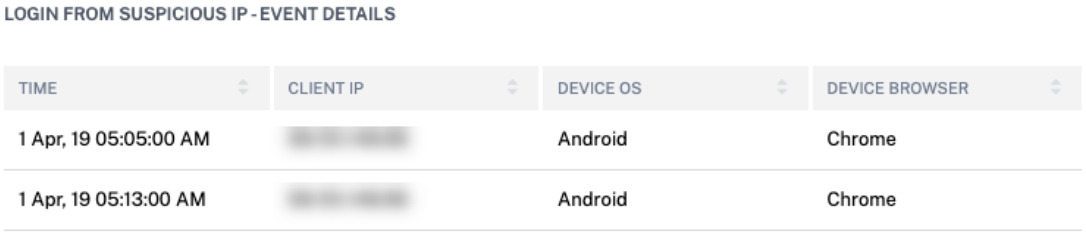


  - 社区情报。提供在外部 IP 威胁情报源中被确定为高风险的 IP 地址的威胁评分和威胁类别。Citrix Analytics 为高风险 IP 地址分配风险评分。风险评分从 80 开始。

    如果 IP 地址在外部 IP 威胁情报源中没有任何可用的威胁情报，则会看到以下消息。



- 事 件详细 信息部分提供了有关可疑登录活动的以下信息：


LOGIN FROM SUSPICIOUS IP - EVENT DETAILS

TIME	CLIENT IP	DEVICE OS	DEVICE BROWSER
1 Apr, 19 05:05:00 AM	[redacted]	Android	Chrome
1 Apr, 19 05:13:00 AM	[redacted]	Android	Chrome

- 时间。可疑登录活动的时间。
- 客户端 **IP**。用于可疑登录活动的用户设备的 IP 地址。
- 设备操作系统。浏览器的操作系统。
- 设备浏览器。用于可疑登录活动的 Web 浏览器。

您可以对用户应用哪些操作**?**

您可以对用户的帐户执行以下操作：

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户中存在任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。
- 注销用户。当用户从其帐户注销时，在 Citrix Gateway 管理员清除“注销用户”操作之前，他们无法通过 Citrix Gateway 访问任何资源。
- 锁定用户：当用户的帐户由于异常行为而被锁定时，在网关管理员解锁帐户之前，他们无法通过 Citrix Gateway 访问任何资源。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的个人资料并选择相应的风险指示器。从操作菜单中，选择一个操作，然后单击应用。

> 注意
>
> 无论触发风险指示器的数据源如何，都可以应用与其他数据源相关的操作。

可疑登录

> 备注
>
> - 此风险指示器取代了来自异常位置的访问风险指示器。
> - 任何基于“从异常位置访问”风险指示器的策略都会自动链接到可疑登录风险指示器。

Citrix Analytics 会根据多个上下文因素（由用户使用的设备、位置和网络共同定义）来检测看起来异常或有风险的用户登录。

何时触发可疑登录风险指示器

风险指示器是由以下因素的组合触发的，根据一种或多种条件，每个因素都被视为潜在的可疑因素。

因数	条件
异常的设备	用户使用与过去 30 天内使用的设备不同的签名从设备登录。设备签名基于设备的操作系统和所使用的浏览器。
位置不寻常	从用户在过去 30 天内未登录的城市或国家/地区登录。
	城市或国家/地区在地理上与最近（过去 30 天）的登录位置相距甚远。
	在过去 30 天内，从城市或国家/地区登录的用户数为零或最少。
异常的网络	使用用户在过去 30 天内未使用的 IP 地址登录。
	从用户在过去 30 天内未使用的 IP 子网登录。
	在过去 30 天内，从 IP 子网登录的用户数为零或最少。
IP 威胁	社区威胁情报源 Webroot 将该 IP 地址标识为高风险。
	Citrix Analytics 最近从其他用户的 IP 地址检测到高度可疑的登录活动。

如何分析可疑登录风险指示器

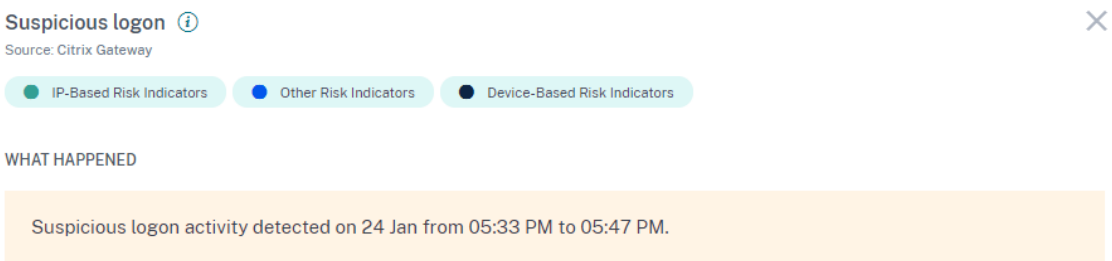
以用户 Adam Maxwell 为例，他首次从印度安得拉邦登录。他使用具有已知签名的设备访问组织的资源。但是他从过去 30 天没有使用过的网络进行连接。

Citrix Analytics 将此登录事件检测为可疑事件，因为因素-位置和网络偏离了他的通常行为，并触发可疑登录风险指示器。风险指示器被添加到 Adam Maxwell 的风险时间表中，并为他分配了风险评分。

要查看 Adam Maxwell 的风险时间，请选择“安全” **>** “用户”。从“风险用户”窗格中，选择用户 Adam Maxwell。

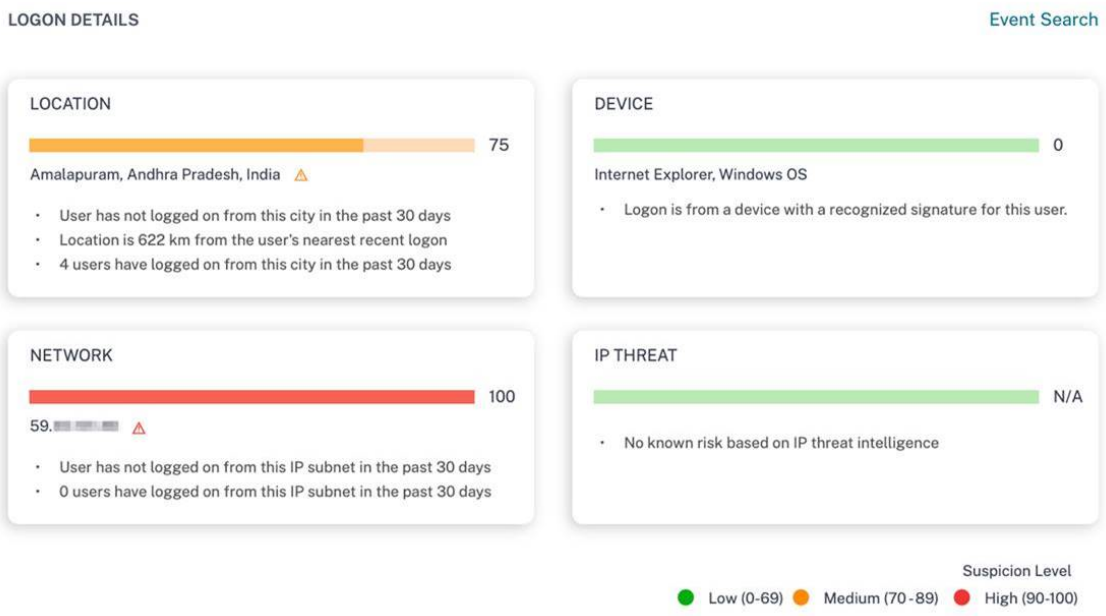
从 Adam Maxwell 的风险时间表中，选择可疑登录风险指示器。您可以查看以下信息：

- 发生了什么部分简要概述了可疑活动，包括风险因素和事件发生时间。



- 登录详细信息部分提供了与每个风险因素相对应的可疑活动的详细摘要。为每个风险因素分配一个表示怀疑水平的分数。任何单一风险因素都不表示来自用户的高风险。总体风险基于多个风险因素的相关性。

怀疑等级	指示
0–69	该因素看起来正常，不被视为可疑因素。
70–89	该因素看起来有点不寻常，被认为与其他因素有中等可疑性。
90–100	该因素是全新的或不寻常的，被认为与其他因素高度可疑。



- 登录位置 **-** 过去 **30** 天显示最近已知位置和用户当前位置的地理地图视图。显示的是过去 30 天的位置数据。您可以将鼠标悬停在地图上的指针上，以查看每个位置的总登录次数。

- 可疑登录 - 事件详细信息部分提供了有关可疑登录事件的以下信息：
  - 时间：表示可疑登录的日期和时间。
  - 设备操作系统：指示用户设备的操作系统。
  - 设备浏览器：表示用于登录 Citrix Gateway 的 Web 浏览器。

SUSPICIOUS LOGON - EVENT DETAILS

TIME	DEVICE OS	DEVICE BROWSER
24 Jan, 22 05:43:55 PM	Windows OS	Internet Explorer

您可以对用户应用哪些操作?

您可以对用户的帐户执行以下操作：

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户中存在任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。
- 注销用户。当用户从其帐户注销时，在 Citrix Gateway 管理员清除“注销用户”操作之前，他们无法通过 Citrix Gateway 访问任何资源。
- 锁定用户：当用户的帐户由于异常行为而被锁定时，在网关管理员解锁帐户之前，他们无法通过 Citrix Gateway 访问任何资源。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的个人资料并选择相应的风险指示器。从操作菜单中，选择一个操作，然后单击应用。

> 注意
>
> 无论触发风险指示器的数据源如何，都可以应用与其他数据源相关的操作。

异常的身份验证

当用户从异常 IP 地址登录失败时，Citrix Analytics 会检测基于访问的威胁，并触发相应的风险指示器。

与异常身份验证风险指示器相关的风险因素是基于登录失败的风险指示器。有关风险因素的更多信息，请参阅 Citrix 用户风险指示器。

什么时候触发异常身份验证失败指示器

当组织中的用户从不正常的 IP 地址登录失败时，您可能会收到通知，这与他们的常规行为相反。

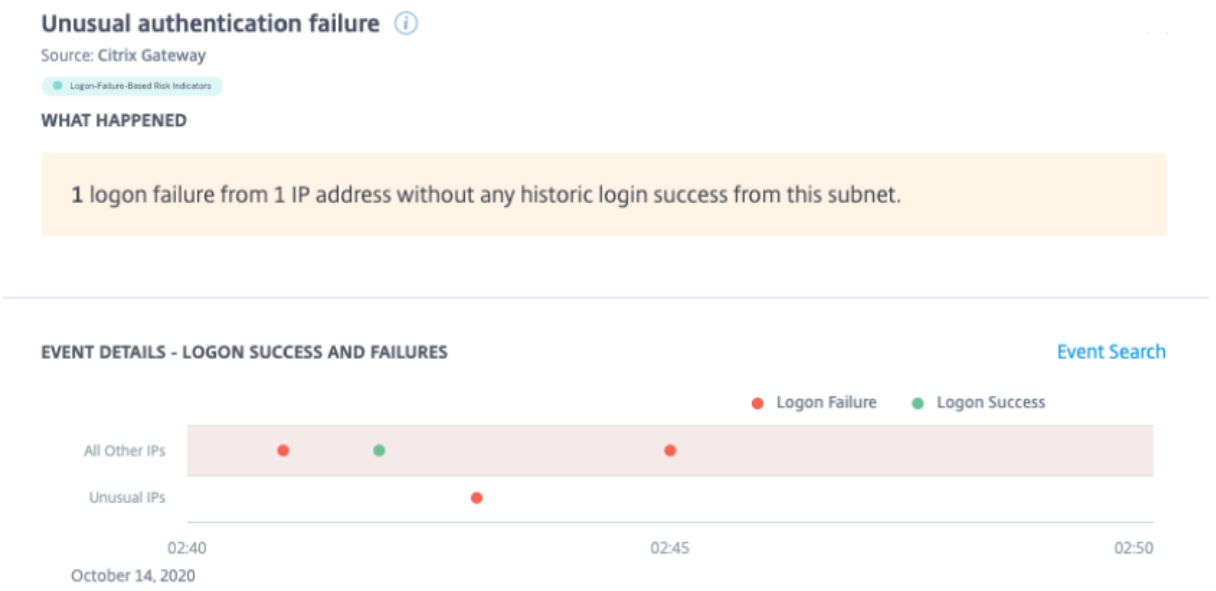
Citrix Gateway 检测到这些事件并将其报告给 Citrix Analytics。Citrix Analytics 会接收事件并提高用户的风险评分。异常身份验证失败 风险指示器添加到用户的风险时间表中。

如何分析不寻常的身份验证失败指示器

以用户 Georgina Kalou 为例，她经常从她通常的家庭和办公室网络登录 Citrix Gateway。远程攻击者试图通过猜测不同的密码来验证 Georgina 的帐户，从而导致陌生网络的身份验证失败。

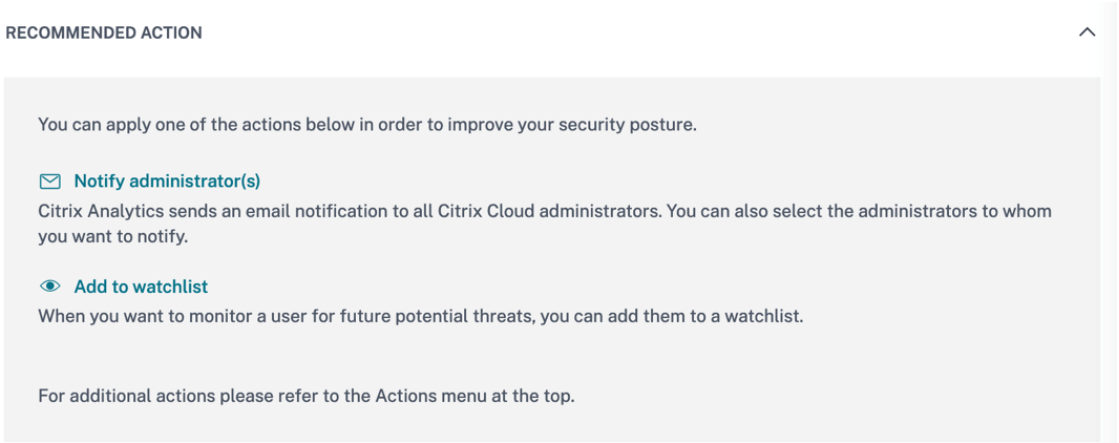
在这种情况下，Citrix Gateway 将这些事件报告给 Citrix Analytics，后者将更新的风险评分分配给 Georgina Kalou。异常身份验证失败风险指示器添加到 Georgina Kalou 的风险时间表中。

从 Georgina Kalou 的风险时间表中，您可以选择报告的异常身份验证失败风险指示器。活动的原因与活动时间和地点等详细信息一起显示。



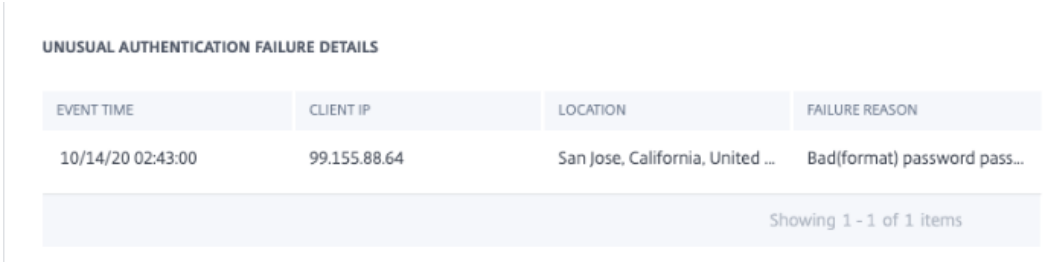
- 在“发生了什么”部分中，您可以查看简短的摘要，其中包括身份验证失败总数和事件发生时间。
- 在建议的操作部分，您可以找到可以应用于风险指示器的建议操作。Citrix Analytics for Security 会根据用户构成的风险的严重程度推荐操作。建议可以是以下操作之一，也可以是以下操作的组合：
  - 通知管理员
  - 添加到播放列表
  - 创建策略

  您可以根据建议选择操作。或者，您可以根据从操作菜单中选择要应用的操作。有关详细信息，请参阅手动应用操作。

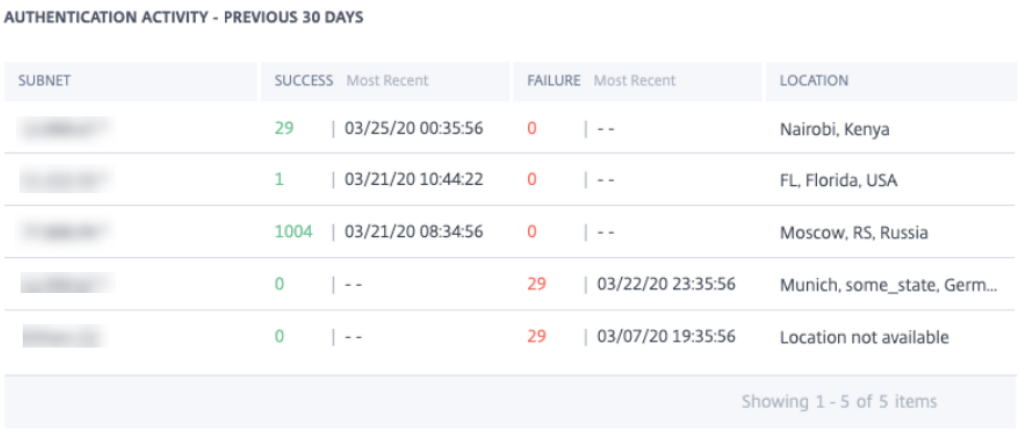


- 在“事 件详细信息—登录成功和失败”部分中，您可以查看指示异常身份验证失败以及在同一持续时间内检测到的任何其他登录活动的图表。
- 在 异常身份验证详细 信息部分中，该表提供了有关异常身份验证失败的以下信息：

- 登录时间—事件的日期和时间
- 客户端 **IP** —用户设备的 IP 地址
- 位置—事件发生的位置
- 失败原因—身份验证失败的原因



- 在“用 户身份验证活动—前 **30** 天”部分中，该表提供了有关用户过去 30 天的身份验证活动的以下信息：
  - 子网—来自用户网络的 IP 地址。
  - 成功—用户成功的身份验证事件总数和最近一次成功事件的时间。
  - 失败—用户的失败身份验证事件总数和最近失败事件的时间。
  - 位置—发生身份验证事件的位置。



您可以对用户应用哪些操作**?**

您可以对用户的帐户执行以下操作：

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户中存在任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。
- 注销用户。当用户从其帐户注销时，在 Citrix Gateway 管理员清除“注销用户”操作之前，他们无法通过 Citrix Gateway 访问任何资源。

- 锁定用户：当用户的帐户由于异常行为而被锁定时，在网关管理员解锁帐户之前，他们无法通过 Citrix Gateway 访问任何资源。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的个人资料并选择相应的风险指示器。从操作菜单中，选择一个操作，然后单击应用。

> 注意
>
> 无论触发风险指示器的数据源如何，都可以应用与其他数据源相关的操作。

Citrix Secure Private Access 风险指示器

April 12, 2024

网站访问风险

> 注意
> 由于弃用了通过 Secure Private Access 进行的基于类别的 Web 筛选，Citrix Analytics for Security 的以下功能受到影响：
>
> 1. Citrix Analytics for Security 控制板上不再提供 URL 的类别组、类别和信誉等数据字段。
> 2. 依赖于相同数据的风险 Web 站点访问指标也已弃用，不会为客户触发。
> 3. 任何使用数据字段（URL 的类别组、类别和信誉）及其关联策略的现有自定义风险指标都不再触发。

有关 Secure Private Access 中的弃用的详细信息，请参阅功能弃用。

尝试访问列入黑名单的 **URL**

Citrix Analytics 会根据用户访问的列入黑名单的 URL 检测数据访问威胁，并触发相应的风险指示器。

当用户尝试访问在 Secure Private Access 中配置的列入黑名单的 URL 时，Citrix Analytics 会报告尝试访问列入黑名单的 **URL** 风险指示器。

与 尝试访问列入黑名单的 **URL** 风险指示器相关的风险因素是其他风险指示器。有关风险因素的更多信息，请参阅 Citrix 用户风险指示器。

何时触发尝试访问列入黑名单的 **URL** 风险指示器

Secure Private Access 包括 URL 分类功能，该功能提供基于策略的控制，以限制对列入黑名单的 URL 的访问。当用户尝试访问列入黑名单的 URL 时，Secure Private Access 会向 Citrix Analytics 报告此事件。Citrix Analytics 会更新用户的风险评分，并将 尝试访问列入黑名单的 **URL** 风险指示器条目添加到用户的风险时间表中。

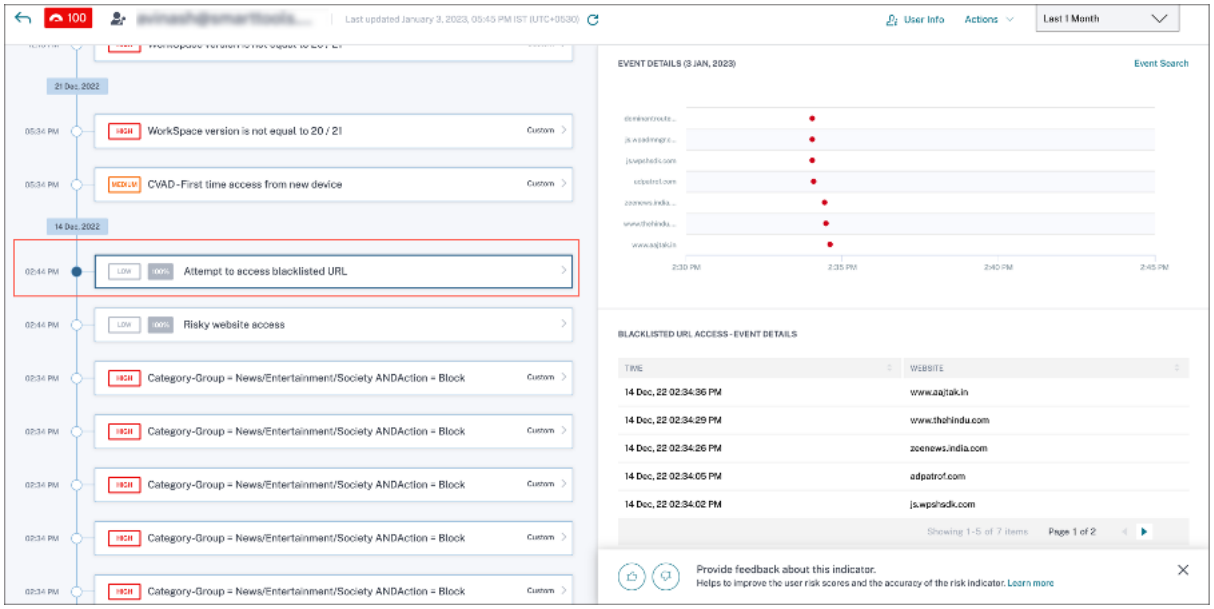
如何分析尝试访问列入黑名单的 **URL** 风险指示器

假设用户 Georgina Kalou 访问了在 Secure Private Access 中配置的列入黑名单的 URL。Secure Private Access 将此事件报告给 Citrix Analytics，后者会为 Georgina Kalou 分配更新的风险评分。尝试访问列入黑名单的 **URL** 风险指示器已添加到 Georgina Kalou 的风险时间表中。

从 Georgina Kalou 的风险时间表中，您可以选择报告的 尝试访问黑名单 **URL** 风险指示器。活动的原因与活动的详细信息一起显示，例如活动的时间、网站详细信息。

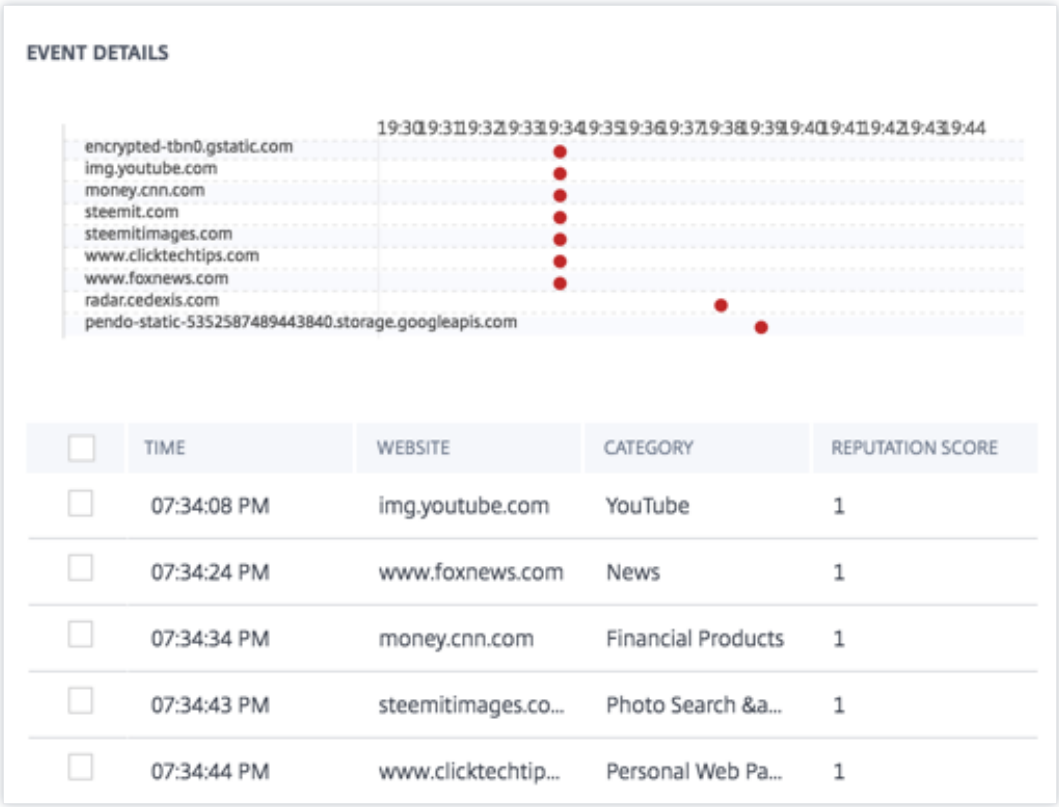
要查看 尝试访问用户的列入黑名单的 **URL** 条目，请导航到“安全” **>** “用户”，然后选择该用户。

当您从时间轴中选择 尝试访问列入黑名单的 **URL** 风险指示器条目时，右侧窗格中将显示相应的详细信息面板。



- 发生了什么 部分提供了风险指标的简要摘要。它包括用户在选定时间段内访问的列入黑名单的 URL 的详细信息。

- “事 件详细信息”部分包括在选定时间段内发生的各个事件的时间轴可视化。此外，您还可以查看有关每个事件的以下关键信息：
  - 时间。事件发生的时间。
  - **Web** 站点站。用户访问的有风险的网站。
  - **Category**（类别）。Secure Private Access 为列入黑名单的 URL 指定的类别。
  - 声誉评级。Secure Private Access 为列入黑名单的 URL 返回的信誉等级。有关详细信息，请参阅 URL 信誉得分。



您可以对用户应用哪些操作**?**

您可以对用户的帐户执行以下操作：

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户中存在任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的个人资料并选择相应的风险指示器。从操作菜单中，选择一个操作，然后单击应用。

> 注意
>
> 无论触发风险指标的数据源如何，都可以应用与其他数据源相关的操作。

不寻常的上传量

Citrix Analytics 会根据异常上传量活动检测数据访问威胁，并触发相应的风险指示器。

当用户向应用程序或网站 上传过量的数据时，会报告异常 上传量风险指示器。

与异常上传量风险指示器相关的风险因素是其他风险指示器。有关风险因素的更多信息，请参阅 Citrix 用户风险指示器。

什么时候触发异常上传量风险指示器

您可以配置 Secure Private Access 来监视用户活动，例如访问的恶意、危险或未知网站、消耗的带宽以及有风险的下载和上载。当组织中的用户将数据上传到应用程序或网站时，Secure Private Access 会向 Citrix Analytics 报告这些事件。

Citrix Analytics 会监视所有这些事件，如果它确定此用户活动与用户的通常行为相反，它将更新用户的风险评分。不寻常的上传量 风险指示器已添加到用户的风险时间表中。

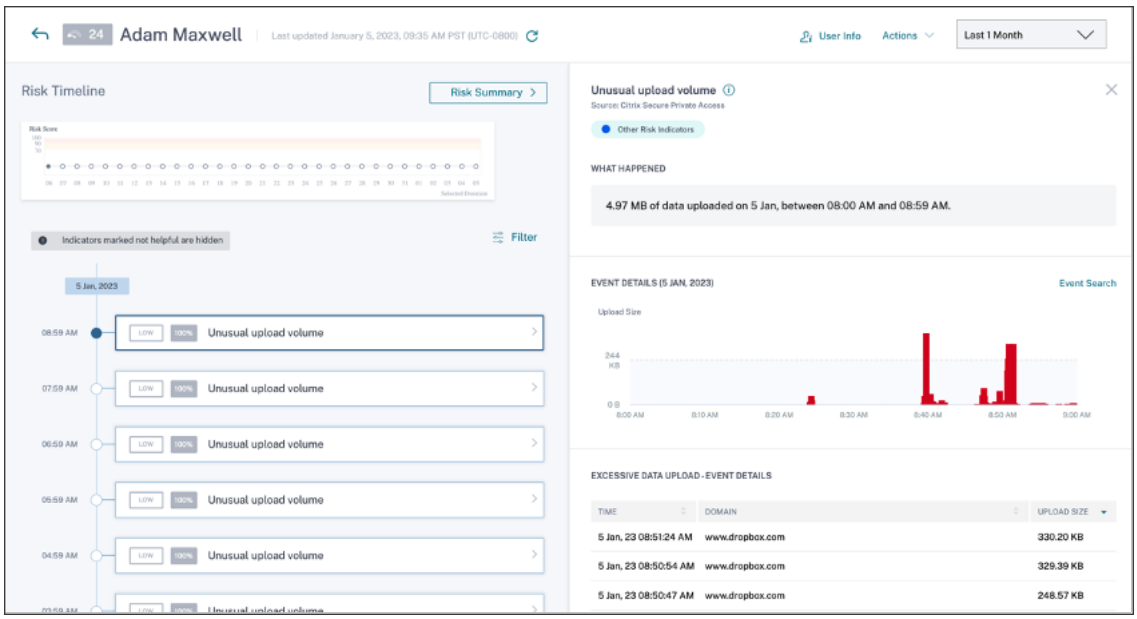
如何分析异常上载量风险指示器?

考虑一个用户 Adam Maxwell，他将过多的数据上传到应用程序或网站。Secure Private Access 将这些事件报告给 Citrix Analytics，后者会为 Adam Maxwell 分配更新的风险评分。异常上传量 风险指示器添加到 Adam Maxwell 的风险时间表中。

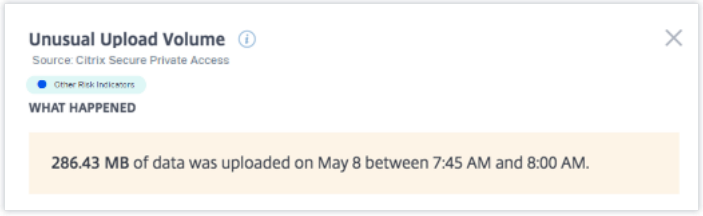
从 Adam Maxwell 的风险时间表中，您可以选择报告的异常上载量风险指标。事件的原因与事件的详细信息一起显示，例如事件的时间和域名。

要查看 异常上传量 风险指示器，请导航到“安全”>“用户”，然后选择用户。

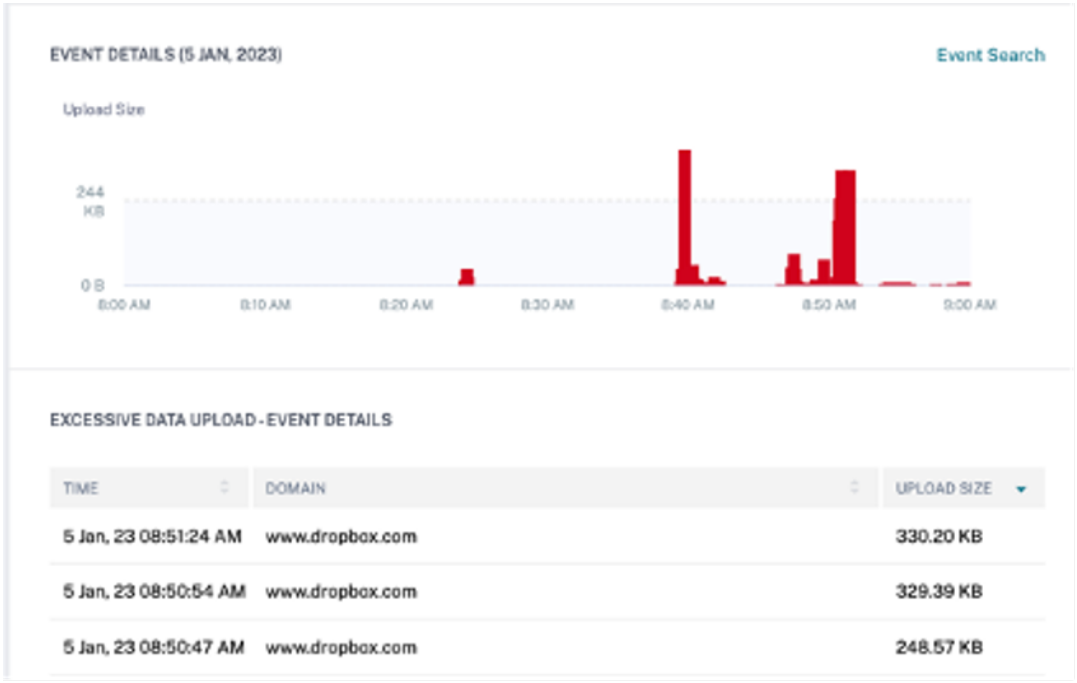
当您从时间轴中选择 异常上传量 风险指示器条目时，右侧窗格中会出现相应的详细信息面板。



- “发生了什么”部分提供了风险指示器的简要摘要，包括所选期间上传的数据量。



- “事 件详细信息”部分包括在选定时间段内发生的各个数据上传事件的时间轴可视化。此外，您还可以查看有关每个事件的以下关键信息：
  - 时间。将过多数据上传到应用程序或网站的时间。
  - 域。用户将数据上传到的域。
  - 上传大小。上传到域的数据量。



您可以对用户应用哪些操作?

您可以对用户的帐户执行以下操作:

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户中存在任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的个人资料并选择相应的风险指示器。从操作菜单中，选择一个操作，然后单击应用。

> 注意
>
> 无论触发风险指标的数据源如何，都可以应用与其他数据源相关的操作。

数据下载过多

Citrix Analytics 会根据网络中用户下载的过多数据检测数据访问威胁，并触发相应的风险指示器。

当组织中的用户从应用程序或网站下载过多数据时，会报告风险指示器。

何时触发过多数据下载风险指示器

您可以配置 Secure Private Access 来监视用户活动，例如访问的恶意、危险或未知网站、消耗的带宽以及有风险的下载和上载。当组织中的用户从应用程序或网站下载数据时，Secure Private Access 会向 Citrix Analytics 报告这

些事件。

Citrix Analytics 会监视所有这些事件，如果它确定用户活动与用户的通常行为相反，它将更新用户的风险评分。数据下载过多风险指示器已添加到用户的风险时间表中。

与过多的数据下载风险指示器相关的风险因素是其他风险指示器。有关风险因素的更多信息，请参阅 Citrix 用户风险指示器。

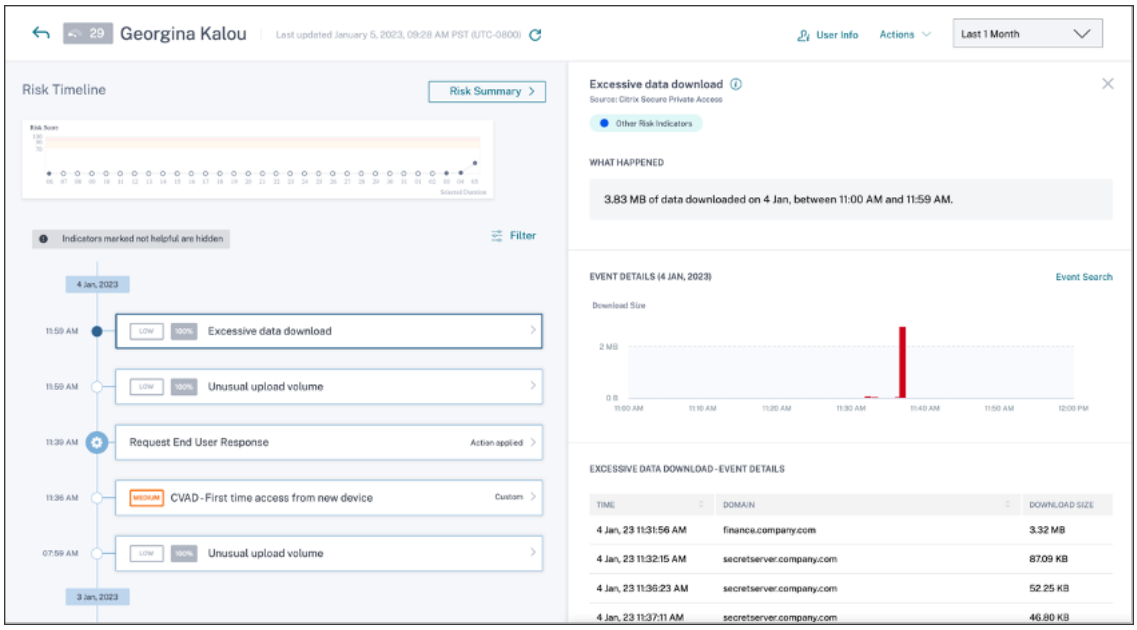
如何分析数据下载过多风险指标

假设用户 Georgina Kalou 从应用程序或网站下载过剩数据量。Secure Private Access 将这些事件报告给 Citrix Analytics，Citrix Analytics 会为 Georgina Kalou 分配更新的风险评分，并将过多的数据下载风险指示器条目添加到用户的风险时间表中。

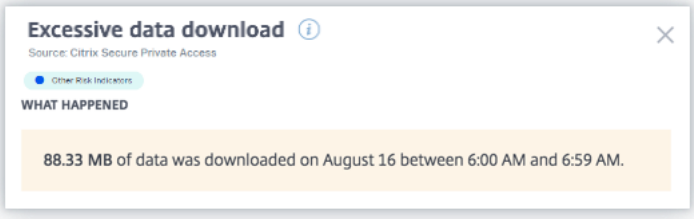
从 Georgina Kalou 的风险时间表中，您可以选择报告的 过多数据下载 风险指标。事件的原因与事件的详细信息一起显示，例如时间和域名详细信息。

要查看数据下载过多风险指示器，请导航到“安全性”**>**“用户”，然后选择用户。

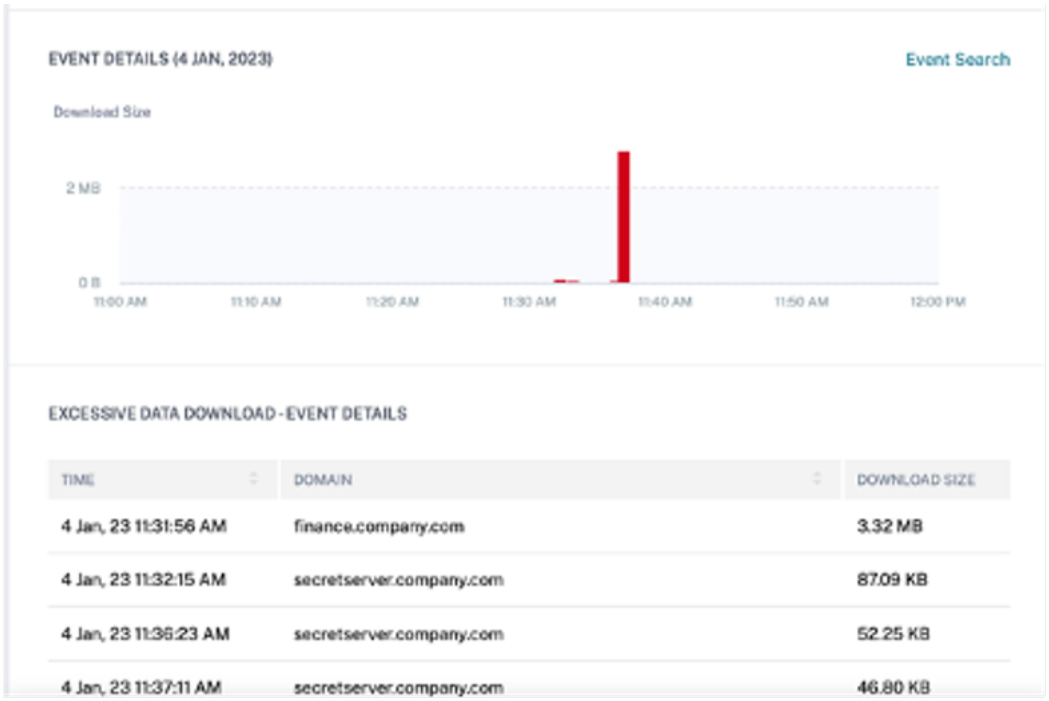
当您从时间轴中选择 过多的数据下载 风险指示器条目时，右侧窗格中将显示相应的详细信息面板。



- 发生了什么事 部分提供了风险指示器的简要摘要，包括在选定时间段内下载的数据量。



- “事 件详细信息”部分包括在选定时间段内发生的各个数据下载事件的时间轴可视化。此外，您还可以查看有关每个事件的以下关键信息：
  - 时间。将过多数据下载到应用程序或网站的时间。
  - 域。用户下载数据的域。
  - 下载大小。下载到域的数据量。



您可以对用户应用哪些操作**?**

您可以对用户的帐户执行以下操作：

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户中存在任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的个人资料并选择相应的风险指示器。从操作菜单中，选择一个操作，然后单击应用。

> 注意
>
> 无论触发风险指标的数据源如何，都可以应用与其他数据源相关的操作。

Citrix Virtual Apps and Desktops 和 Citrix DaaS 风险指示器

July 12, 2022

不可能旅行

Citrix Analytics 检测到用户的登录存在风险，如果连续登录来自两个不同的国家/地区，且时间段少于这两个国家/地区之间的预期旅行时间。

不可能的旅行时间情景表明存在以下风险：

- 凭据泄露：远程攻击者窃取合法用户的凭据。
- 共享凭据：不同的用户使用相同的用户凭据。

不可能的旅行风险指示器何时触发

不可能旅行风险指示器评估每对连续用户登录之间的时间和估计距离，并在距离大于个人在这段时间内可能行驶的距离时触发。

> 注意
>
> 此风险指示器还包含用于减少以下情况的误报警报的逻辑，这些情况不反映用户的实际位置：
>
> - 当用户通过代理连接登录到虚拟应用程序和桌面时。
> - 当用户从托管客户端登录到虚拟应用程序和桌面时。

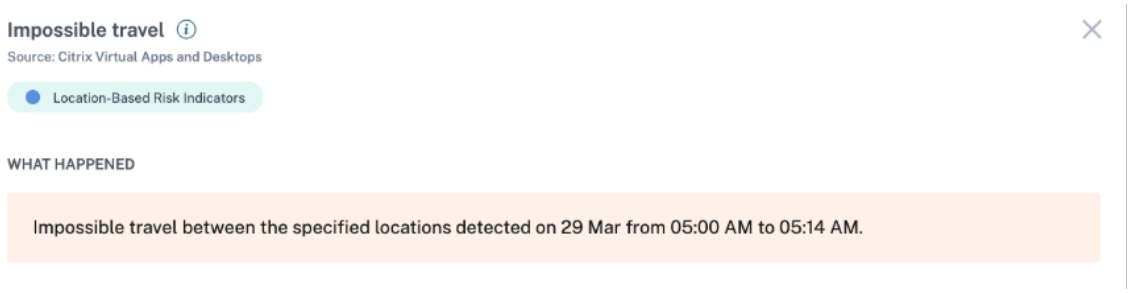
如何分析不可能的风险指标

以用户 Adam Maxwell 为例，他在一分钟的时间内从俄罗斯莫斯科和中国呼和浩特这两个地点登录。Citrix Analytics 将此登录事件检测为不可能的旅行场景，并触发不可能旅行风险指示器。风险指标被添加到 Adam Maxwell 的风险时间表中，并为他分配了风险评分。

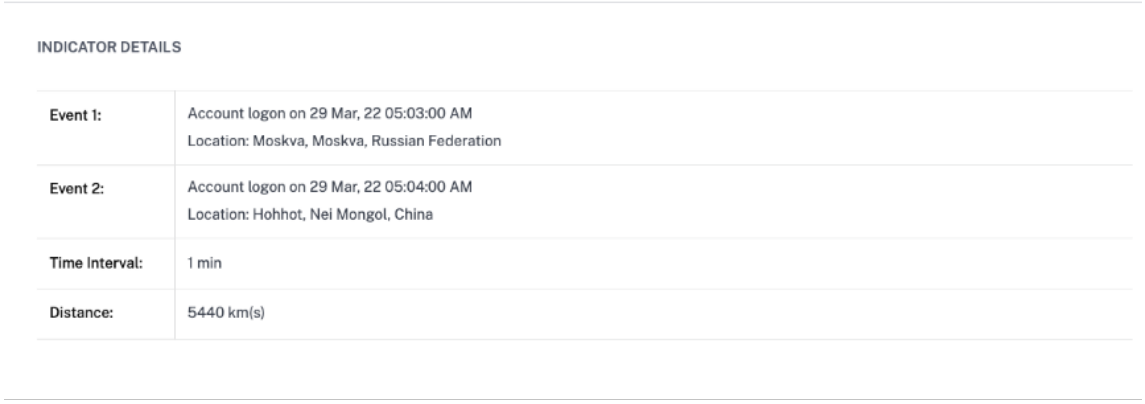
要查看 Adam Maxwell 的风险时间表，请选择安全 **>** 用户。从“风险用户”窗格中，选择用户 Adam Maxwell。

从 Adam Maxwell 的风险时间表中，选择不可能的旅行风险指示器。您可以查看以下信息：

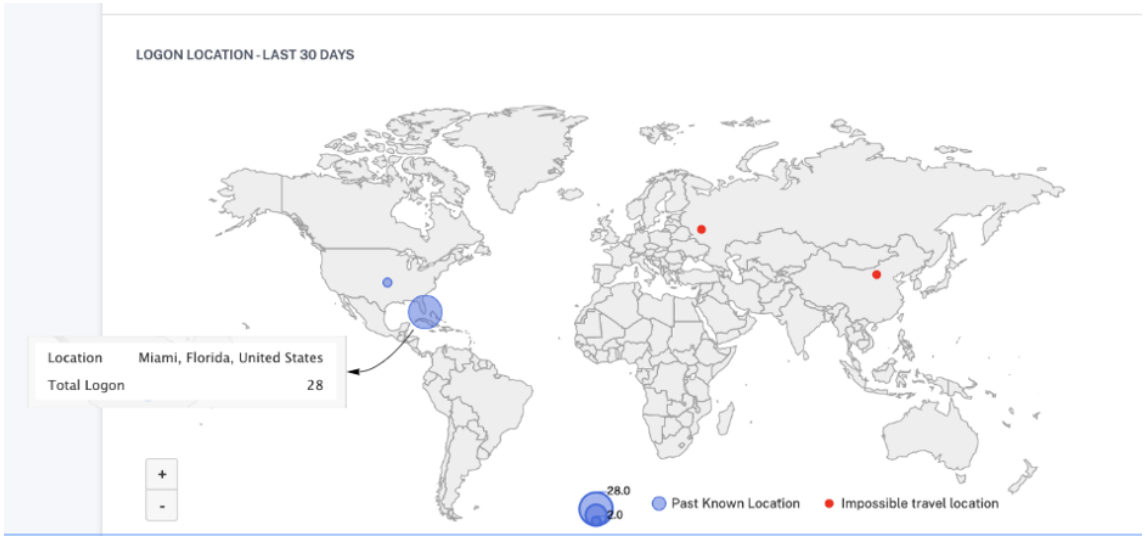
- 发生了什么 事部分简要概述了不可能旅行事件。



- 指标详情部分提供用户登录的位置、连续登录之间的持续时间以及两个位置之间的距离。

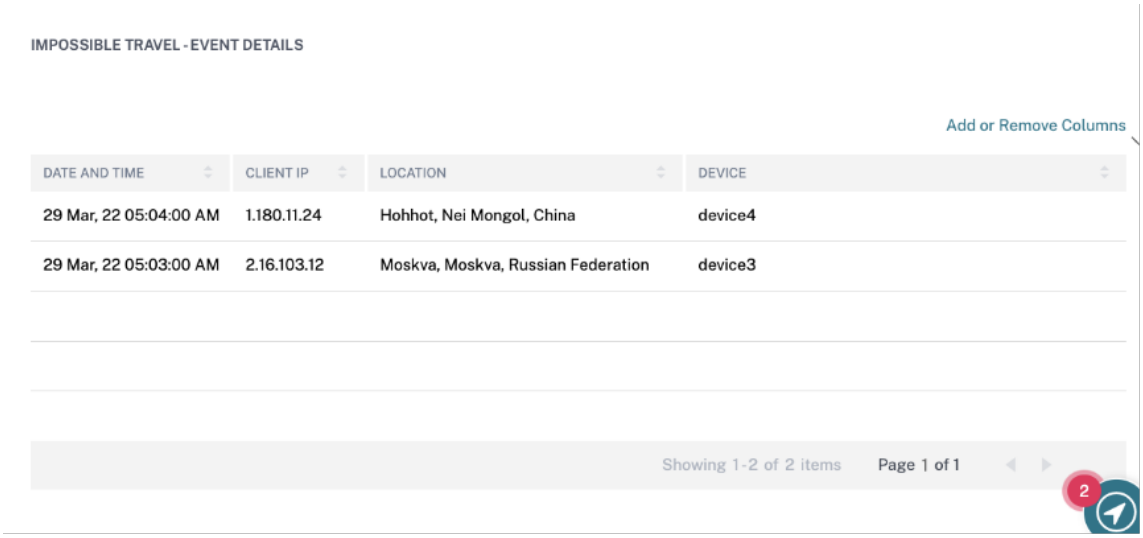


- 登录位置 **-** 最近 **30** 天部分显示了用户不可能的出行地点和已知位置的地理地图视图。显示的是过去 30 天的位置数据。您可以将鼠标悬停在地图上的指针上，以查看每个位置的总登录次数。



- 不可能旅行 **-** 事件详情部分提供了有关不可能旅行事件的以下信息：
  - 日期和时间：表示登录的日期和时间。
  - 客户端 **IP**：表示用户设备的 IP 地址。
  - 位置：表示用户登录的位置。
  - 设备：表示用户的设备名称。

- 登录类型：指示用户活动是会话登录还是帐户登录。当用户成功验证其帐户时，会触发帐户登录事件。而当用户输入凭据并登录其应用程序或桌面会话时，会触发会话登录事件。
- **OS**：表示用户设备的操作系统。
- 浏览器：表示用于访问应用程序的 Web 浏览器。



你可以对用户应用什么操作

您可以对用户的帐户执行以下操作：

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户有任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。
- 注销用户。当用户从其帐户注销时，他们将无法通过虚拟桌面访问资源。
- 开始会话录制。如果用户的 Virtual Desktops 帐户发生异常事件，管理员可以开始记录用户在将来登录会话中的活动。但是，如果用户使用的是 Citrix Virtual Apps and Desktops 7.18 或更高版本，则管理员可以动态启动和停止记录用户的当前登录会话。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的配置文件并选择相应的风险指示器。从“操 作”菜单中选择一个操作，然后单击“应用”。

> 注意
>
> 无论触发风险指示器的数据源如何，都可以应用与其他数据源相关的操作。

潜在的数据泄露

Citrix Analytics 会根据过度尝试泄露数据来检测数据威胁，并触发相应的风险指示器。

与潜在数据泄露风险指示器相关的风险因素是基于数据的风险指示器。有关风险因素的更多信息，请参阅 Citrix 用户风险指示器。

当 Citrix Receiver 用户尝试将文件下载或传输到驱动器或打印机时，将触发 潜在的数据泄 露风险指示器。此数据可能是文件下载事件，例如将文件下载到本地驱动器、映射驱动器或外部存储设备。也可以使用剪贴板或通过复制粘贴操作泄露数据。

> 注意
>
> 剪贴板操作仅受 SaaS 应用程序支持。

什么时候触发潜在数据泄露风险指示器

当用户在特定时间段内将过多文件传输到驱动器或打印机时，您会收到通知。当用户在本地计算机上使用复制粘贴操作时，也会触发此风险指示器。

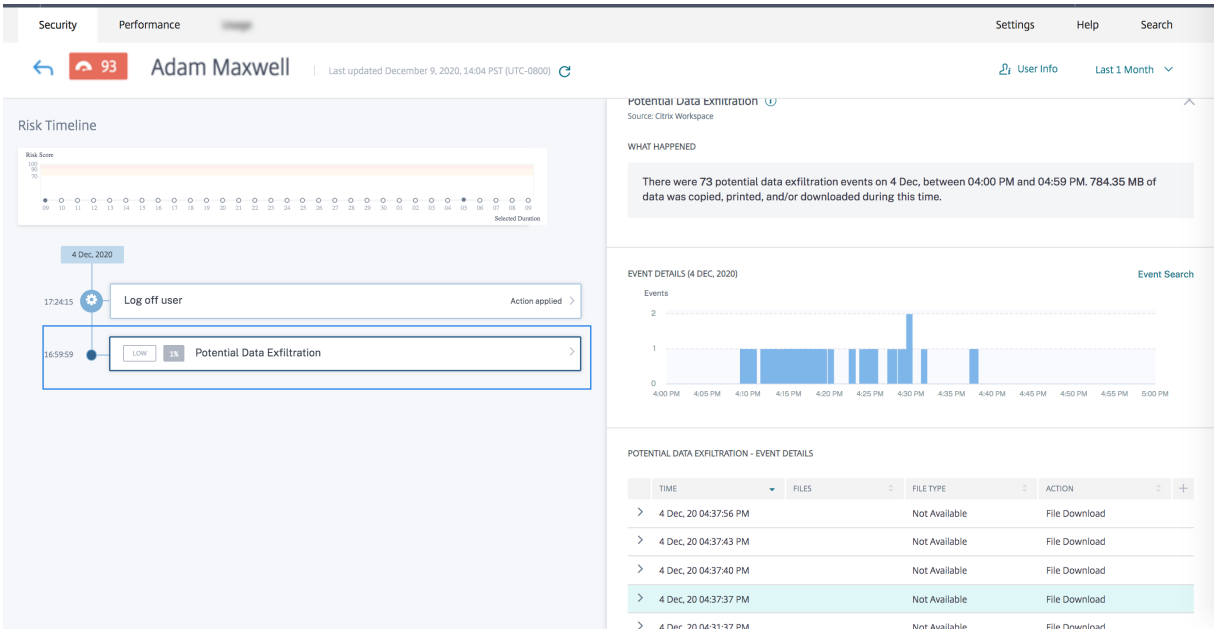
当 Citrix Receiver 检测到此行为时，Citrix Analytics 会收到此事件并向相应的用户分配风险评分。潜在的数据泄露风险指示器已添加到用户的风险时间表中。

如何分析潜在数据泄露风险指标

考虑用户 Adam Maxwell，他登录到会话并尝试打印超出预定义限制的文件。通过此操作，Adam Maxwell 已经超出了他基于机器学习算法的正常文件传输行为。

从 Adam Maxwell 的时间表中，您可以选择潜在的数据泄露风险指标。此时将显示事件的原因以及传输文件所使用的设备等详细信息。

要查看为用户报告的 潜在数据泄露 风险指示器，请导航到“安全” > “用户”，然后选择该用户。

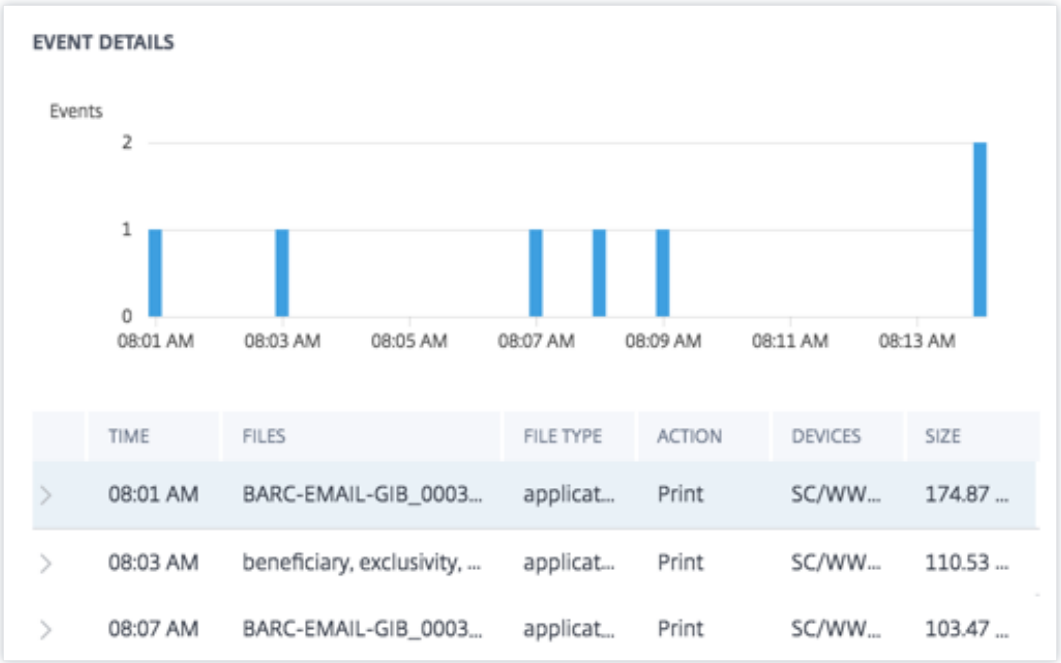


- 在 发生了什么 部分，您可以查看潜在的数据泄露事件的摘要。您可以查看特定时间段内的数据泄露事件数。

- 在“事件详细信息”部分，数据泄露尝试以图形和表格格式显示。这些事件在图表中显示为单个条目，并且该表提供了以下关键信息：
  - 时间。数据泄露事件发生的时间。
  - 文件。已下载、打印或复制的文件。
  - 文件类型。已下载、打印或复制的文件类型。

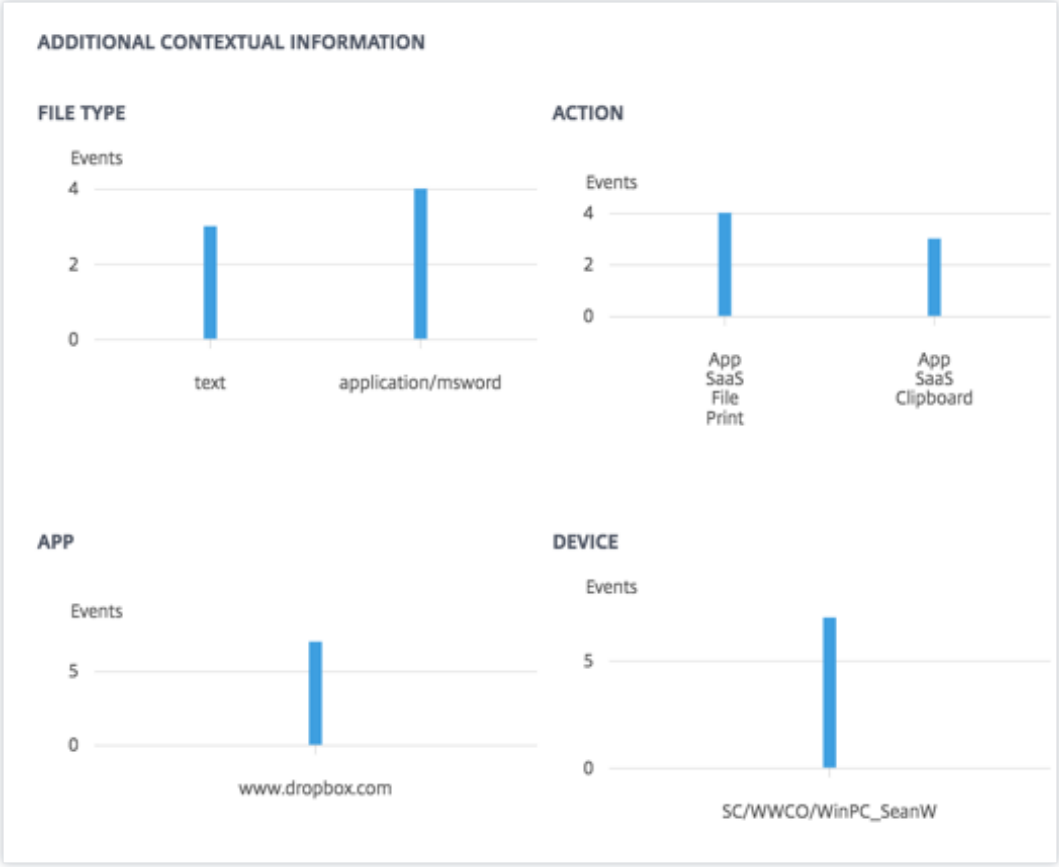
    > 注意
    >
    > 打印的文件名仅在 SaaS 应用程序打印事件中可用。

  - 操作。执行的数据泄露事件的种类—打印、下载或复制。
  - 设备。使用的设备。
  - 大小。泄露的文件的大小。
  - 位置。用户试图从中泄露数据的城市。



- “其他上下文信息”部分，在活动发生期间，您可以查看以下内容：
  - 已泄露的文件数。

- 执行的操作。
- 使用的应用程序。
- 用户使用的设备。



您可以对用户应用哪些操作**?**

您可以对用户的帐户执行以下操作：

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户中存在任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。
- 注销用户。当用户从其帐户注销时，他们将无法通过虚拟桌面访问资源。
- 开始会话录制。如果用户的虚拟桌面帐户发生异常事件，管理员可以开始记录用户在未来登录会话中的事件。但是，如果用户使用的是 Citrix Virtual Apps and Desktops 7.18 或更高版本，管理员可以动态启动和停止记录用户的当前登录会话。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的个人资料并选择相应的风险指示器。从“操 作”菜单中选择一个操作，然后单击“应用”。

> 注意
>
> 无论触发风险指示器的数据源如何，都可以应用与其他数据源相关的操作。

可疑登录

Citrix Analytics 会根据多个上下文因素（由用户使用的设备、位置和网络共同定义）来检测看起来异常或有风险的用户登录。

何时触发可疑登录风险指示器

风险指示器是由以下因素的组合触发的，根据一种或多种条件，每个因素都被视为潜在的可疑因素。

因数	条件
异常的设备	用户从过去 30 天内未使用过的设备登录。
位置不寻常	用户从设备签名与用户历史记录不一致的 HTML5 客户端或 Chrome 客户端登录。 从用户在过去 30 天内未登录的城市或国家/地区登录。 城市或国家/地区在地理上与最近（过去 30 天）的登录位置相距甚远。 在过去 30 天内，从城市或国家/地区登录的用户数为零或最少。
异常的网络	使用用户在过去 30 天内未使用的 IP 地址登录。 从用户在过去 30 天内未使用的 IP 子网登录。 在过去 30 天内，从 IP 子网登录的用户数为零或最少。
IP 威胁	社区威胁情报源 Webroot 将该 IP 地址标识为高风险。 Citrix Analytics 最近从其他用户的 IP 地址检测到高度可疑的登录活动。

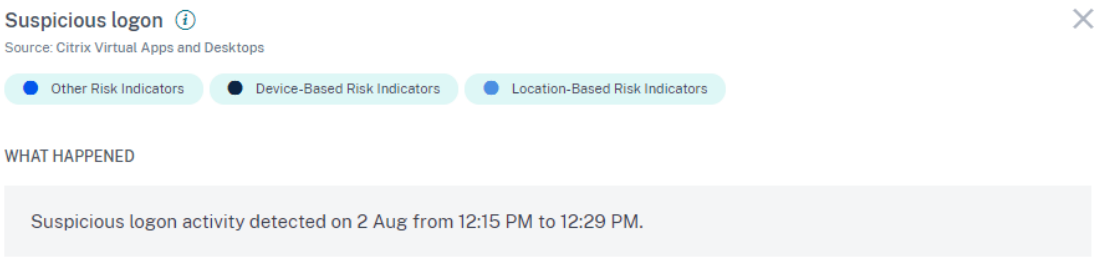
如何分析可疑登录风险指示器

考虑首次从印度孟买登录的用户 Adam Maxwell。他使用新设备或过去 30 天未使用的设备登录 Citrix Virtual Apps and Desktops 并连接到新网络。Citrix Analytics 将此登录事件检测为可疑，因为位置、设备和网络因素与其通常的行为不同，并触发 可疑登录 风险指示器。风险指示器被添加到 Adam Maxwell 的风险时间表中，并为他分配了风险评分。

要查看 Adam Maxwell 的风险时间，请选择“安全”**>**“用户”。从“风险用户”窗格中，选择用户 Adam Maxwell。

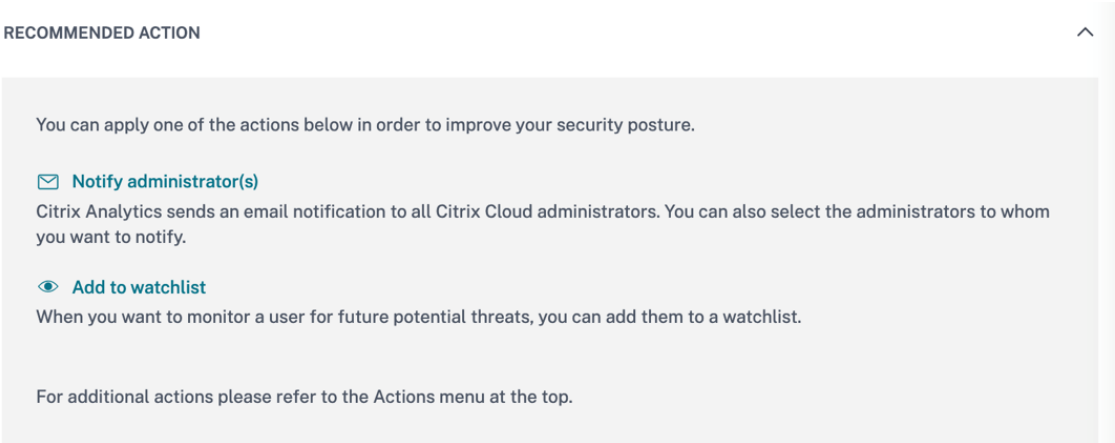
从 Adam Maxwell 的风险时间表中，选择可疑登录风险指示器。您可以查看以下信息：

- 发生了什么部分简要概述了可疑活动，包括风险因素和事件发生时间。



- 在建议的操作部分，您可以找到可以应用于风险指示器的建议操作。Citrix Analytics for Security 会根据用户构成的风险的严重程度推荐操作。建议可以是以下操作之一，也可以是以下操作的组合：
  - 通知管理员
  - 添加到播放列表
  - 创建策略

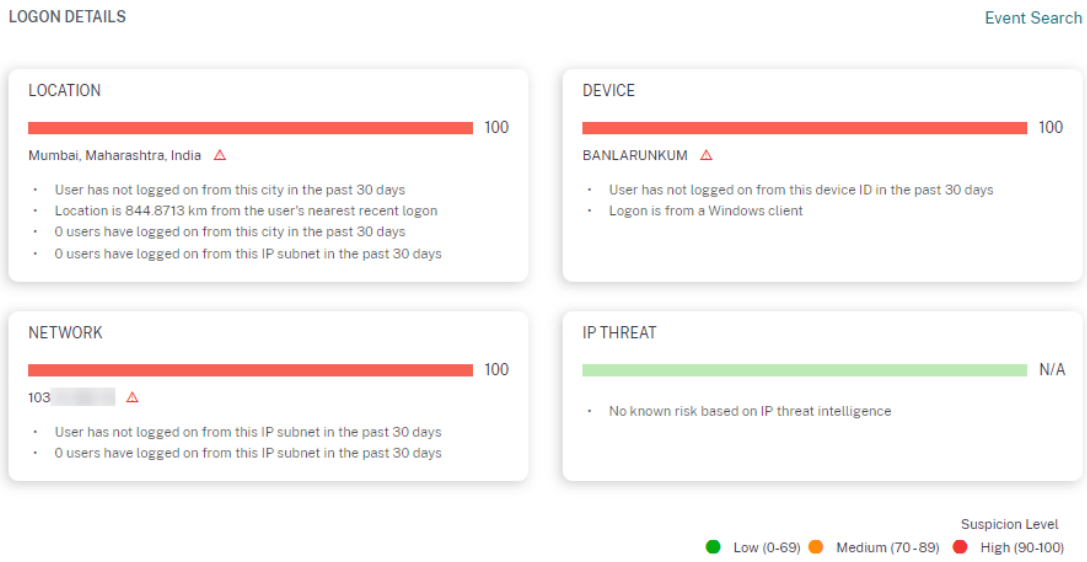
  您可以根据建议选择操作。或者，您可以根据从操作菜单中选择要应用的操作。有关详细信息，请参阅手动应用操作。



- 登录详细信息部分提供了与每个风险因素相对应的可疑活动的详细摘要。为每个风险因素分配一个表示怀疑水平的分数。任何单一风险因素都不表示来自用户的高风险。总体风险基于多个风险因素的相关性。

怀疑等级	指示
0–69	该因素看起来正常，不被视为可疑因素。
70–89	该因素看起来有点不寻常，被认为与其他因素有中等可疑性。

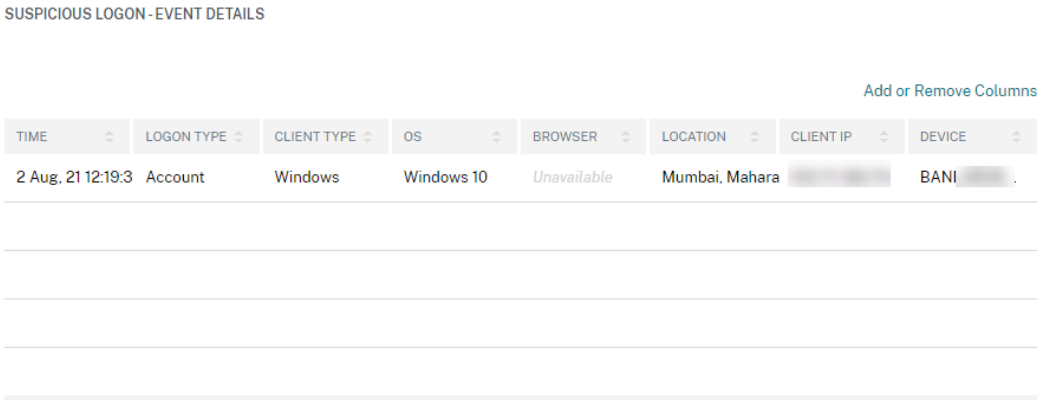
怀疑等级	指示
90–100	该因素是全新的或不寻常的，被认为与其他因素高度可疑。



- “登录位置-过去 **30** 天”部分显示了最近已知位置和用户当前位置的地理地图视图。显示的是过去 30 天的位置数据。您可以将鼠标悬停在地图上的指针上，以查看每个位置的总登录次数。

- 可疑登录 **-** 事件详细信息部分提供了有关可疑登录事件的以下信息：
  - 时间：表示可疑登录的日期和时间。

- 登录类型：指示用户活动是会话登录还是帐户登录。当用户对其帐户进行身份验证成功时，将触发帐户登录事件。而当用户输入凭据并登录其应用程序或桌面会话时，会触发会话登录事件。
- 客户端类型：表示用户设备上安装的 Citrix Workspace 应用程序的类型。根据用户设备的操作系统，客户端类型可以是 Android、iOS、Windows、Linux、Mac 等。
- **OS**：表示用户设备的操作系统。
- 浏览器：表示用于访问应用程序的 Web 浏览器。
- 位置：表示用户登录的位置。
- 客户端 **IP**：表示用户设备的 IP 地址。
- 设备：表示用户的设备名称。



你可以对用户应用什么操作

您可以对用户的帐户执行以下操作：

- 添加到播放列表。当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。
- 通知管理员。当用户帐户中存在任何异常或可疑活动时，系统会向所有管理员或选定的管理员发送电子邮件通知。
- 注销用户。当用户从其帐户注销时，他们将无法通过虚拟桌面访问资源。
- 开始会话录制。如果用户的虚拟桌面帐户发生异常事件，管理员可以开始记录用户在未来登录会话中的事件。但是，如果用户使用的是 Citrix Virtual Apps and Desktops 7.18 或更高版本，管理员可以动态启动和停止记录用户的当前登录会话。

要了解有关操作以及如何手动配置操作的更多信息，请参阅 策略和操作。

要手动将操作应用于用户，请导航到用户的个人资料并选择相应的风险指示器。从“操 作”菜单中选择一个操作，然后单击“应用”。

> 注意
>
> 无论触发风险指示器的数据源如何，都可以应用与其他数据源相关的操作。

为用户风险指标提供反馈

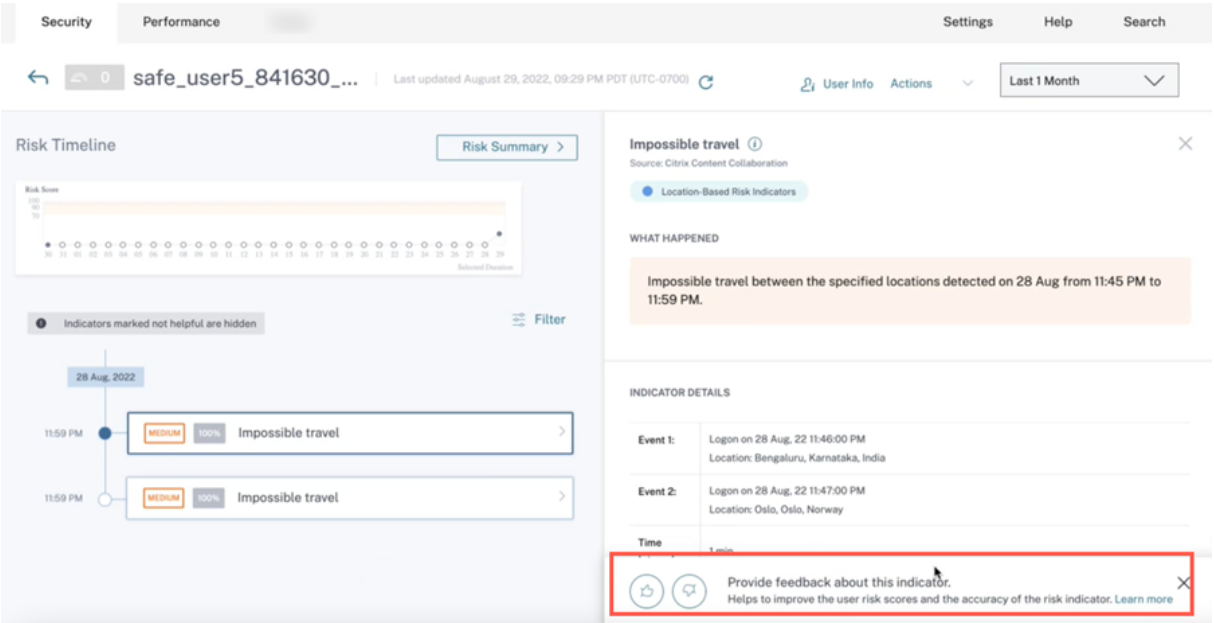
October 19, 2022

风险指示器旨在检测和报告潜在的可疑或异常用户活动，同时自动提高用户的风险评分。实际上，尽管某些风险指标的出现与合法的潜在安全威胁相对应，但其他风险指标的出现却是良性的。

指标反馈功能允许您明确标记风险指标的出现情况：

- 当您认为存在真正的潜在用户风险时同样有用
- 如果您确定不存在安全威胁，则无济于事。在这种情况下，默认情况下，指标出现次数在用户时间表中处于隐藏状态，并且会自动调整用户的风险分数，以便在后续计算中排除该指标的出现。

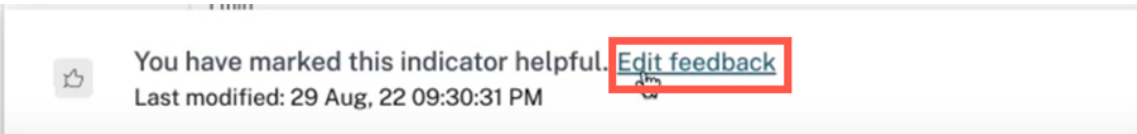
此外，您的集体反馈用于推动风险指标算法的未来改进。



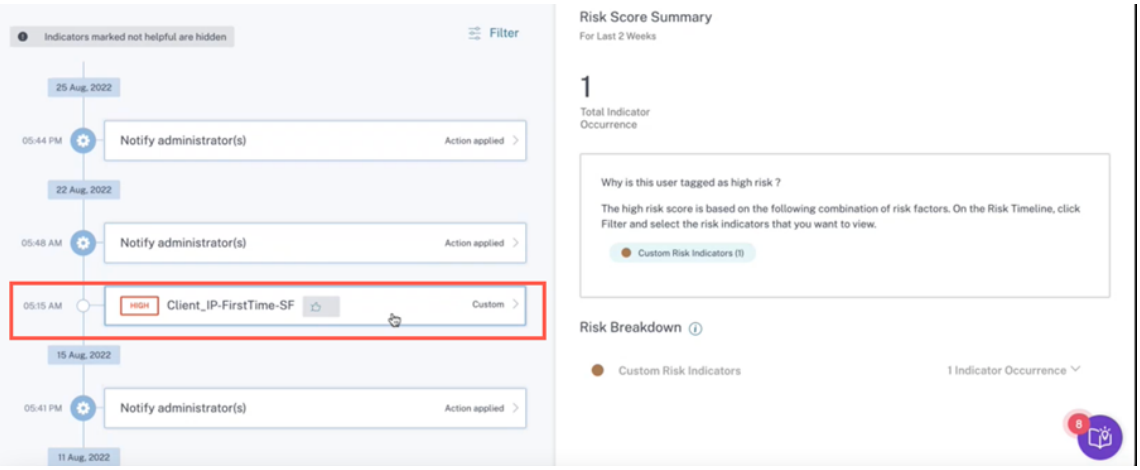
用户时间轴中的每个默认风险指示器条目都会显示反馈横幅（带有竖起大拇指和向下竖起的图标）。

- 竖起大拇指 图标- 指示器很有用，可以正确识别危险活动。您可以点击竖起大拇指图标并就该指标的用处及其优势提供更多评论。

  您可以保存反馈并将该指标标记为有用。您也可以通过单击“编辑反馈”来编辑您的评论。反馈横幅提供上次提交反馈的时间表。

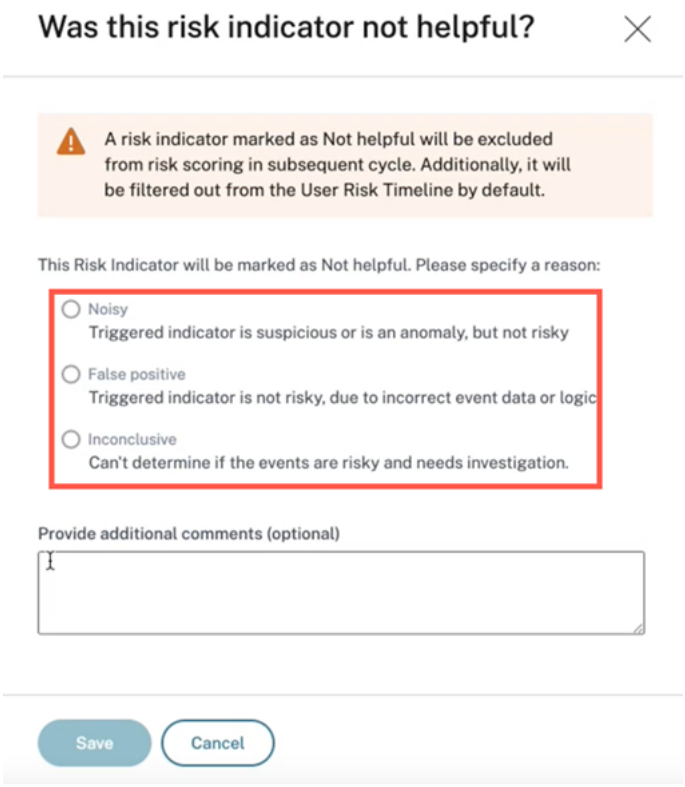


当风险指示器被标记为有用时，该反馈将显示在相应的用户时间表条目中，并报告给 Citrix Analytics。用户风险评分不受影响。



- 竖起大拇指 图标 -指示器无用或触发不正确。您可以将该指标标记为无用，并将其归类为“噪声”、“误报”或“无定论”。此风险指标的出现将排除在用户风险评分的所有后续更新中。如有必要，您还可以提供其他评论。
  - 噪音—触发的指示器可疑或异常，但没有风险。
  - 误报—由于事件数据或逻辑不正确，触发的指标没有风险。
  - 无定论—无法确定事件是否存在风险并需要调查。

    > 注意
    >
    > 重新校准风险评分最多需要 15 分钟。

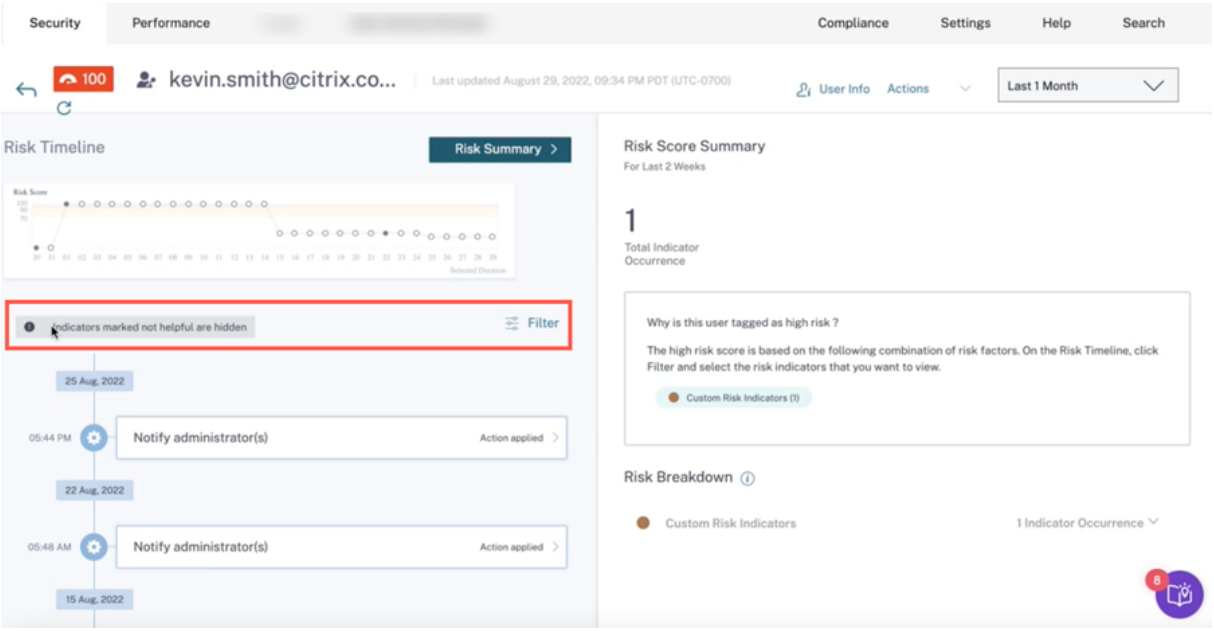


如果指标被标记为无用，则可以查看以下结果：

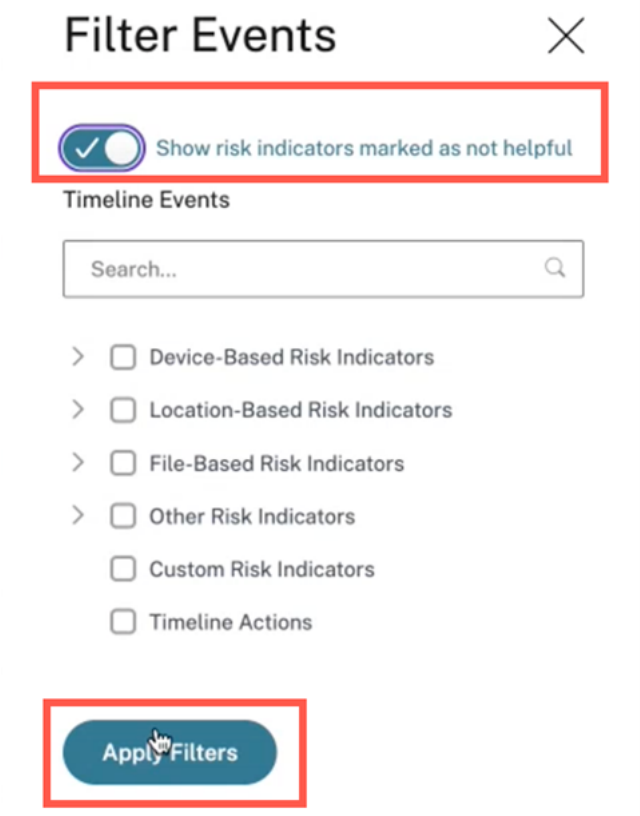
- 该特定指标在时间轴上处于隐藏状态。
- 由于在后续更新中将该指标的出现排除在风险评分计算之外，因此重新校准了风险分数。
- 以文字反馈形式提供的任何其他信息都将保留，以备日后参考。

查看筛选条件

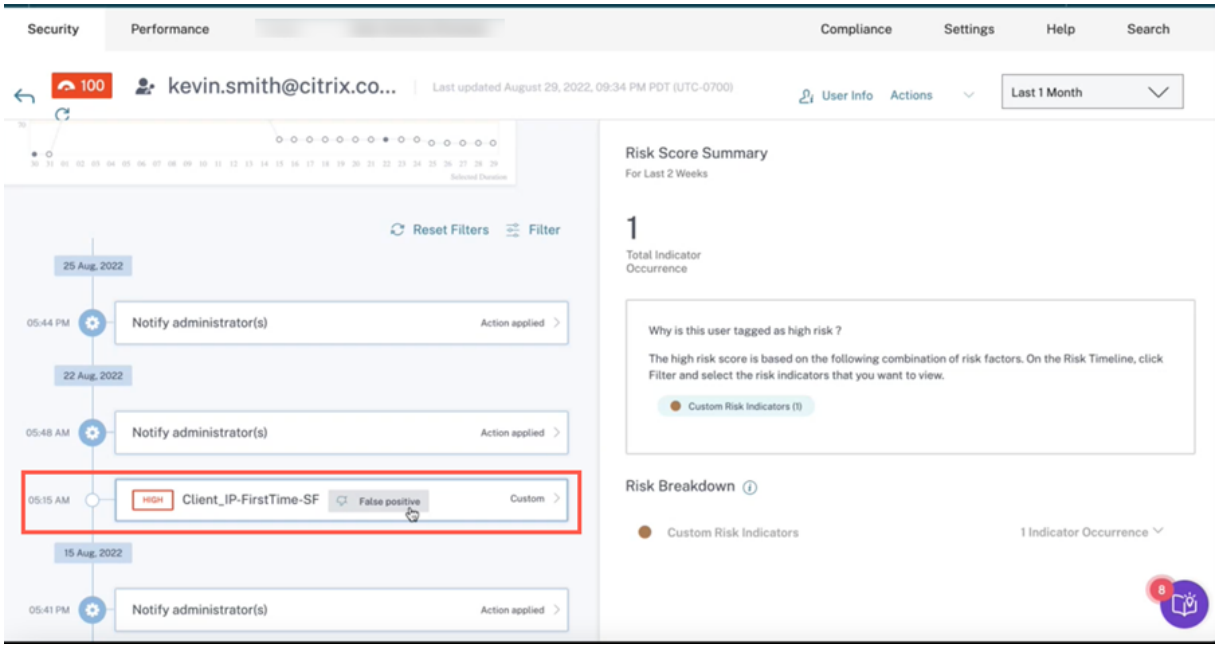
默认情况下，标记为“无用”的指标处于隐藏状态。



要查看隐藏的指标，请单击“筛选”。在出现的“筛选事件”窗口中，打开“显示标记为无用的风险指标”。



您可以根据类别搜索指标。例如，要查看基于位置的隐藏风险指示器，请选择类别并单击“应用筛选器”。您可以查看所有对反馈详细信息没有帮助的基于位置的指标。



作为管理员，您还可以根据需要执行以下操作：

- 更改反馈
- 查看之前的反馈和相关的元数据
- 查看其他管理员提供的反馈和相关的元数据

> 注意
>
> - 您可以按用户级别而不是租户级别提供反馈。一个风险指标的反馈并不适用于该特定风险指标的所有实例。
> - 一个用户的反馈不适用于其他用户。

Microsoft Graph 安全风险指标

April 12, 2024

Microsoft Graph 安全从 **Azure AD** 身份保护 或 微软 **Defender** 接收针对端点 安全提供商的数据，然后将这些信息发送给 Citrix Analytics。

Azure AD 身份保护会触发以下风险指示器并将信息发送到 Microsoft Graph 安全：

- 匿名 IP 地址
- 不可能前往非典型地点
- 凭据泄露的用户

- 从受感染的设备登录
- 从具有可疑活动的 IP 地址登录
- 从不熟悉的位置登录

有关终端版 Defender 的信息，请参阅适用于 端点的 Microsoft Defender。

与风险指标相关的风险因素是基于知识产权的风险指标。有关风险因素的更多信息，请参阅 Citrix 用户风险指示器。

如何分析 **Microsoft Graph** 安全风险指标

考虑一个表现出前面提到的危险行为之一的用户玛丽亚·布朗。微软检测到事件并生成警报。Citrix Analytics 会检索此警报，并将更新的风险评分分配给玛丽亚·布朗。此外，适当的风险指标也会添加到玛丽亚·布朗的风险时间表中。

要查看用户的 Microsoft Graph Security 风险指示器条目，请导航到“安全”> “用户”，然后选择该用户。

从 Maria 的时间表中，您可以从风险时间表中选择最新的风险指标条目。其相应的详细信息面板显示在右窗格中。发生了什么 部分提供了风险指标的简要摘要。

如何获取有关风险指标的更多信息

有关详细信息，请参阅 Azure Active Directory 风险事件。

你可以对用户应用什么操作

目前，无法通过 Microsoft Graph Security 数据源对用户帐户执行适当操作。

有关 Microsoft Graph 安全入门的信息，请参阅 Microsoft Graph 安全性。

自定义风险指示器

December 7, 2023

您在 Citrix Analytics for Security 中看到两种类型的风险指示器：

- 默认风险指示器：这些风险指示器基于计算机学习算法。有关更多信息，请参阅 Citrix 用户风险指示器。
- 自定义风险指示器：这些风险指示器由管理员手动创建。

创建自定义风险指示器时，您可以根据用例定义触发条件和参数。如果用户事件符合您定义的条件，Citrix Analytics 会触发自定义风险指示器并将其显示在用户的风险时间表上。

为以下数据源创建自定义风险指示器：

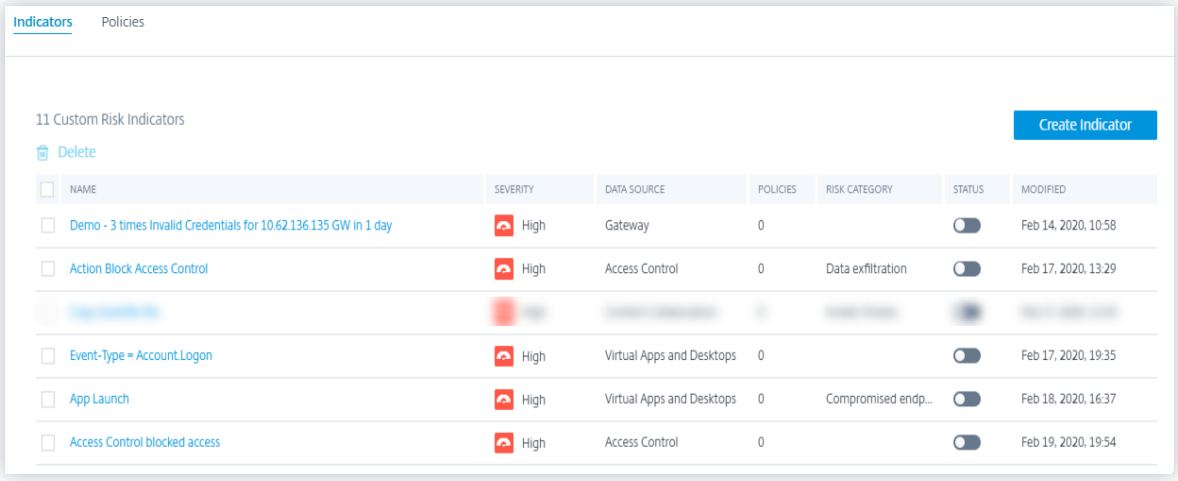
- Citrix Gateway
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops 本地
- Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）
- Citrix Secure Browser

预配置的自定义风险指示器

Citrix 还提供了一些带有预配置条件的自定义风险指示器，以帮助您监视 Citrix 基础架构的安全性。您可以根据自己的使用案例修改预配置的条件。有关更多信息，请参阅 预配置的自定义风险指示器。

自定义风险指示器页

自定义风险指示器 页面提供了对为用户生成的所有自定义风险指示器、严重性、数据源、策略数量、风险类别、状态以及指标的最后修改日期和时间的见解。要创建自定义风险指示器，请参阅 创建自定义风险指示器。



当您选择风险指示器时，您将被重定向到 修改风险指示器 页面。有关更多信息，请参阅 修改自定义风险指示器。

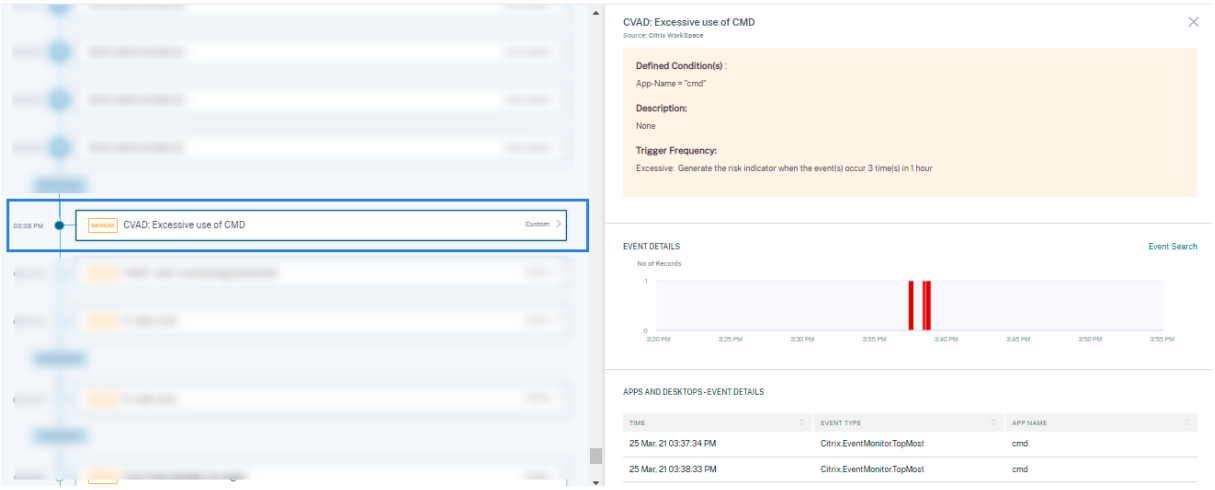
分析自定义风险指示器

考虑一个用户，其操作触发了您定义的自定义风险指示器。Citrix Analytics 会在用户的风险时间表上显示自定义风险指示器。

当您在用户的风险时间轴上选择自定义风险指示器时，右窗格将显示以下信息：

- 定义的条件：显示您在创建自定义风险指示器时定义的条件的摘要。
- 描述：提供您在创建自定义风险指示器时提供的描述的摘要。如果在创建自定义风险指示器时未提供描述，则此部分将反映“无”。

- 触发频率：显示您在创建自定义风险指示器时在高级选项部分中选择的选项。
- 事件详细信息：显示时间表和触发自定义风险指示器的用户事件的详细信息。您可以单击 事件搜索 以在自助搜索页面上查看用户事件。自助搜索页面显示与用户关联的事件和自定义风险指示器。搜索查询显示为自定义风险指示器定义的条件。



> 注意
>
> 自定义风险指示器用用户风险时间表上的标签表示。

可以应用于用户的操作

为用户触发自定义风险指示器时，您可以手动应用操作或创建策略以自动应用操作。有关更多信息，请参阅 策略和操作。

自定义风险指示器模板

您可以使用预定义的模板之一创建自定义风险指示器，也可以在不使用模板的情况下继续操作。

模板充当创建自定义风险指示器的起点。它通过提供可根据用例选择的预定义查询和参数来指导您创建自定义风险指示器。

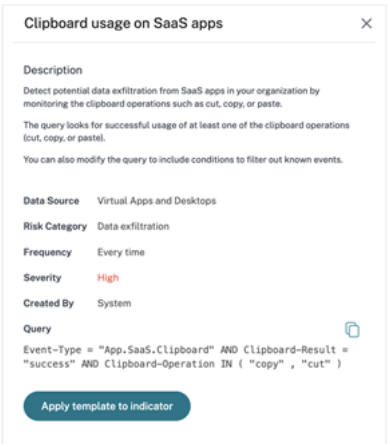
您可以按原样使用模板，也可以对其进行修改以满足您的要求。使用这些模板，管理员无需额外培训即可创建感兴趣的风险指标。

模板包含以下信息：

- 说明：指示模板中定义的查询的用途。
- 数据源：指示应用模板的数据源。
- 风险类别：指示与查询搜索的事件关联的风险类别。风险事件分为四类：数据泄露、内部威胁、用户入侵和危害端点。有关信息，请参阅 风险类别。

- 频率：指示触发查询的频率。
- 严重性：表示与事件关联的风险的严重性。风险可以是高、中或低。
- 创建者：表示模板的创建者。模板始终是系统定义的。
- 查询：表示模板中定义的条件。该查询将检索满足条件的用户事件。

下图显示了 SaaS 应用程序上用例剪贴板的模板。

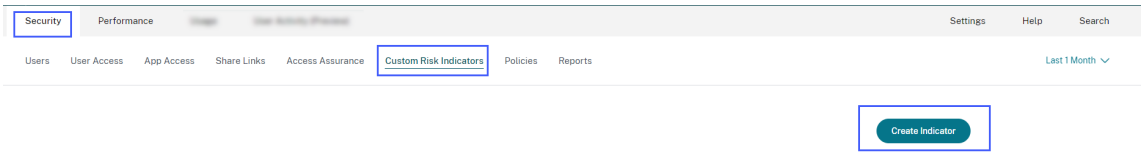


如果找不到适合自己用例的模板，或者想要定义自己的查询，则可以在没有模板的情况下继续。

创建自定义风险指示器

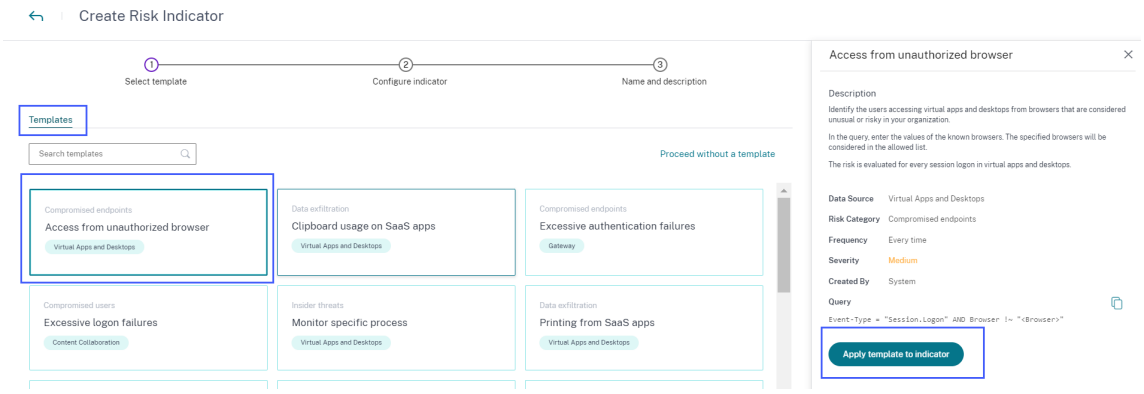
要创建自定义风险指示器，请执行以下操作：

1. 导航到 安全 **>** 自定义风险指示器 **>** 创建指标。

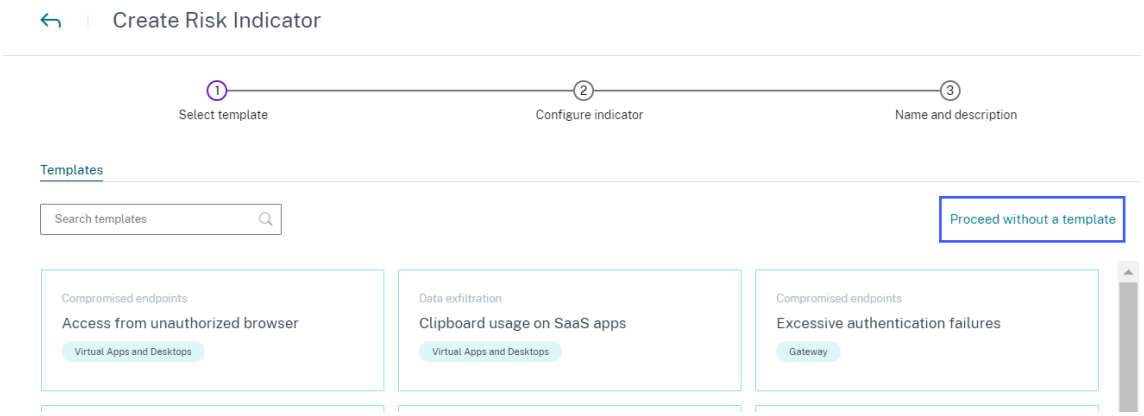


2. 选择一个模板以查看使用案例。如果符合您的要求，请选择 将模板应用于指标。

> 注意
>
> 您还可以修改模板的预定义条件和参数。



3. 如果找不到所需的模板或想要创建自己的状况，请选择在没有 模板的情况下继续。



4. 按照屏幕上的说明创建指标。

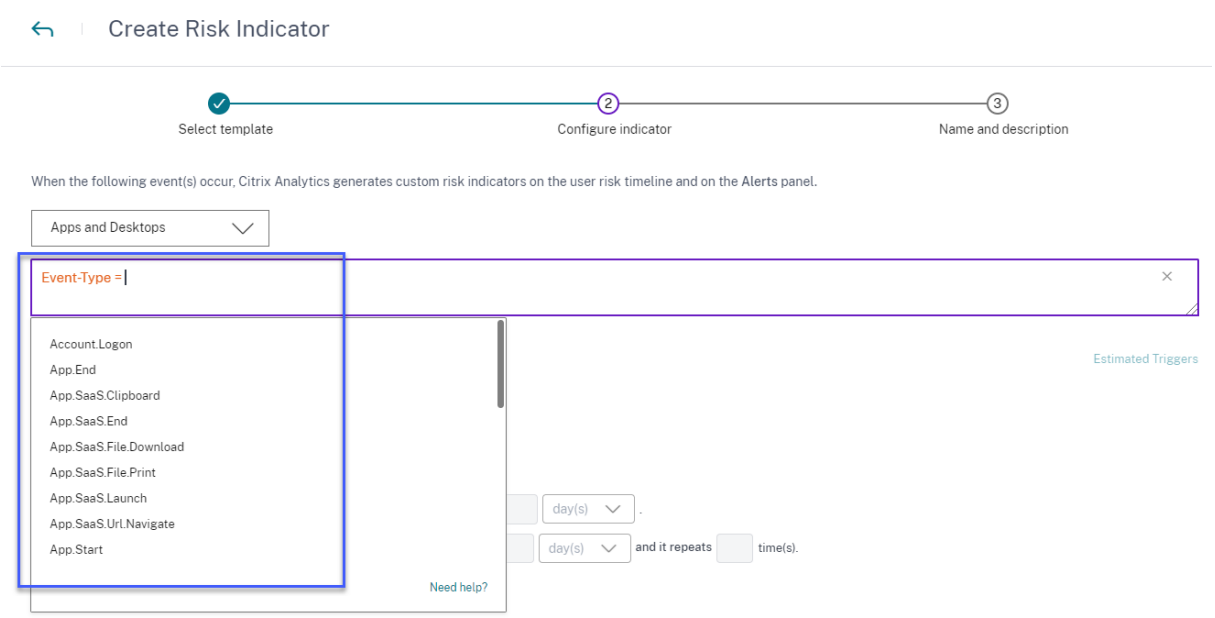
> 备注
>
> - 您可以创建最多 50 个自定义风险指示器。如果达到此最大限制，则必须删除或编辑任何现有的自定义风险指示器以创建自定义风险指示器。
> - 触发自定义风险指示器时，它会立即显示在 用户时间轴 上。但是，用户的风险摘要和风险评分会在几分钟后（大约 15 至 20 分钟）更新。

定义自定义风险指示器的条件

使用查询框定义自定义风险指示器的条件。根据所选数据源，您将获得相应的 维度和 用于定义条件的 有效运算符 。

当选择某些维度（例如 `Event-Type` 和 `Clipboard-Operation` 以及有效的运算符）时，维度的值会自动显示。您可以从建议的选项中选择一个值，也可以根据需要输入一个新值。

下图显示了建议的维度值 `Event-Type`。



如果使用模板，则条件是预定义的。但是，您可以根据自己的用例追加或修改预定义的条件。

在查询框下方，您会看到“估计触发器”链接。单击链接可预测在定义的条件下将触发的自定义风险指示器的大致实例。这些实例是根据 Citrix Analytics 维护并满足定义条件的历史数据计算得出的。

确保单击“估计触发器”以预测上次定义条件的自定义风险指示器出现次数。

使用高级选项

在 高级选项 部分，选择触发自定义风险指示器的事件频率。如果未选择任何选项，Citrix Analytics 会考虑 每次：每次发生事件时生成风险指示器 作为默认选项，然后生成自定义风险指示器。您可以选择以下选项之一：

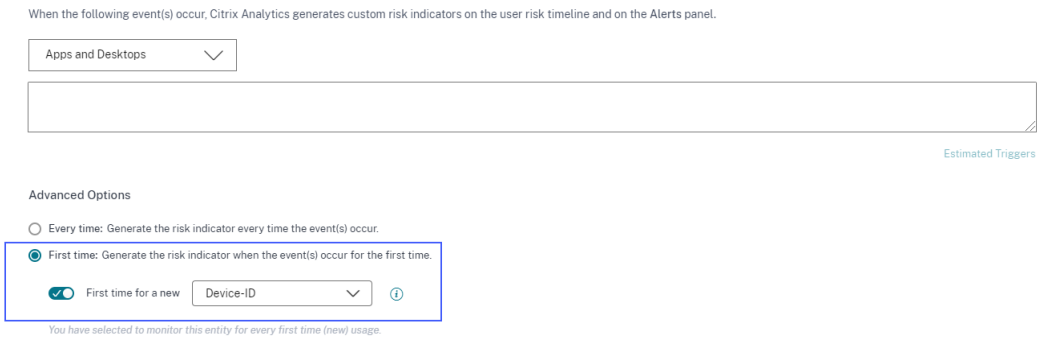
- 每次：只要事件满足定义的条件，就会触发风险指示器。
- 第一次：当事件首次满足定义的条件时，将触发风险指示器。
  - 第一次使用新实体：启用此选项可首次检测从新实体接收的事件。实体的一些示例包括客户端 IP、国家/地区、城市和设备 ID。您只能根据数据源选择一个实体。此选项允许您创建风险指示器，而无需为实体指定明确的值。例如，当您选择实体作为“城市”时，无需指定城市名称。当首次收到来自新城市的事件时，将触发风险指示器。

    下表列出了与每个数据源对应的实体，并描述了触发条件。

数据源	实体	触发条件
Secure Private Access	城市	当用户首次从新城市登录时。
	Client-IP	当用户首次从新 IP 地址登录时。
	国家/地区	当用户首次从新国家/地区登录时。

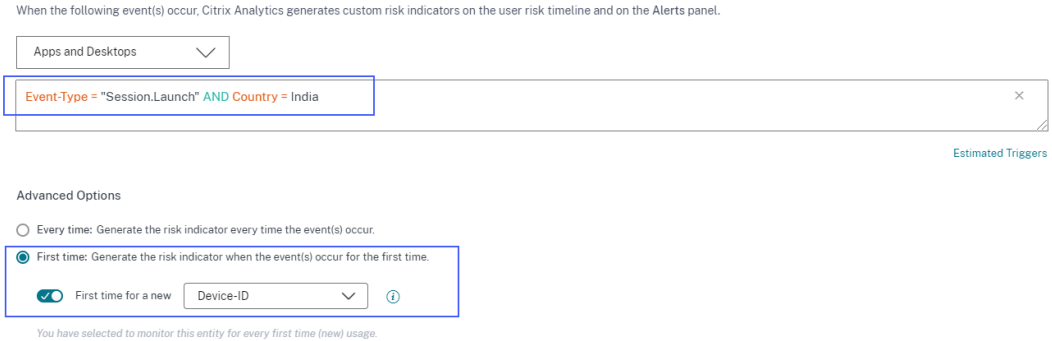
数据源	实体	触发条件
应用程序和桌面	应用程序名称	当用户首次打开新的虚拟应用程序或 SaaS 应用程序时。
	应用程序 URL	当用户首次在其虚拟桌面的浏览器上输入新的应用程序 URL 时。
	城市	用户首次从新城市启动应用程序或桌面时。
	Client-IP	当用户首次从新 IP 地址登录时。
	国家/地区	用户首次从新国家/地区启动应用程序或桌面时。
	设备 ID	当用户首次从移动设备、便携式计算机或台式机等新设备启动虚拟应用程序或虚拟桌面时。
	下载设备类型	当用户首次使用新的存储介质（例如 USB 驱动器）时。
	打印文件格式	打印文件的格式。
	打印文件大小	打印文件的大小（以字节为单位）。
	打印文件名	打印文件的名称。
	打印机名称	使用的打印机的名称。
	Total-Copies-Printed	用户打印的总份数。
	Total-Pages-Printed	用户打印的文档总页数。
网关	Client-IP	当用户首次从新 IP 地址登录时。
Secure Browser	用户名称	发起事件的用户的姓名。
	允许访问	是允许还是拒绝用户访问主机服务。
	Client-IP	用户设备的 IP 地址。
	主机名已访问	用户通过网络访问的主机服务。
	会话 ID	分配给用户会话的唯一号码。

以下示例显示了为应用程序和桌面数据源创建的自定义风险指示器。当用户首次从新设备启动虚拟桌面或虚拟应用程序时，将触发风险指示器。



您还可以在 首次为新选项添加条件的同时 添加条件。在这种情况下，当风险指示器首次检测到来自新实体的事件并且事件满足定义的条件时，就会触发风险指示器。

以下示例显示了为自定义风险指示器定义的条件以及 首次启用新设备 **ID** 选项的条件。当位于印度的用户首次从新设备启动虚拟桌面会话时，将触发风险指示器。



- 过度：在满足以下条件后触发风险指示器：
  - 事件符合规定的条件。
  - 在指定时间段内，事件发生的次数是指定的。
- 频繁：在满足以下条件后触发风险指示器：
  - 这些事件符合定义的条件。
  - 这些事件在指定时间段内发生指定的次数。
  - 事件模式重复指定的次数。

选择风险类别

为自定义风险指示器选择风险类别。

风险指标根据自定义风险指标的风险敞口类型进行分组。有关选择风险类别的帮助，请参阅 风险类别。

选择严重性

严重性表示风险事件的严重程度，由风险指示器检测到。创建自定义风险指示器时，请选择严重性高、中或低。

如果应用模板，则会预先选择严重性选项。您可以根据自己的用例修改此预选。

支持用于定义条件的运算符

定义条件时可以使用以下运算符。

操作员	说明	示例	输出
	为搜索查询分配一个值。	用户名：John	显示用户 John 的事件。
=	为搜索查询分配一个值。	用户名 = John	显示用户 John 的事件。
~	搜索类似的值。	用户名 ~ test	显示具有相似用户名的事件。
""	用空格分隔的值括起来。	User-Name = "John Smith"	显示用户约翰·史密斯的事件。
<, >	搜索关系价值。	数据量 > 100	显示数据量大于 100 GB 的事件。
AND	搜索两个条件均为 true 的值。	User-Name : John AND Data Volume > 100	显示用户 John 的事件，其中数据量大于 100 GB。
*	搜索与字符零次或更多次匹配的值。	User-Name = John*	显示以 John 开头的所有用户名的事件。
		User-Name = *John*	显示包含 John 的所有用户名的事件。
		User-Name = *Smith	显示以 Smith 结尾的所有用户名的事件。
!~	检查用户事件中指定的匹配模式。此 NOT LIKE 运算符返回事件字符串中任意位置不包含匹配模式的事件。	User-Name !~ John	显示除 John、John Smith 或包含匹配名称 "John" 的任何此类用户以外的用户的事件。
!=	检查用户事件是否确切指定的字符串。此 NOT EQUAL 运算符返回事件字符串中任意位置不包含确切字符串的事件。	Country != USA	显示除美国以外国家/地区的事件。
IN	为一个维度分配多个值以获取与一个或多个值相关的事件。	User-Name IN (John, Kevin)	查找与约翰或凯文相关的所有事件。

操作员	说明	示例	输出
NOT IN	为一个维度分配多个值，然后查找不包含指定值的事件。	User-Name NOT IN (John, Kevin)	查找除 John 和 Kevin 之外的所有用户的事件。
IS EMPTY	检查维度的空值或空值。此运算符仅适用于字符串类型的维度，例如 App-Name、Browser 和 Country。它不适用于非字符串（数字）类型的维度，例如 Upload-File-Size、Download-File-Size 和 Client-IP。	国家/地区 IS EMPTY	查找国家名称不可用或为空（未指定）的事件。
IS NOT EMPTY	检查维度的非空值或特定值。此运算符仅适用于字符串类型的维度，例如 App-Name、Browser 和 Country。它不适用于非字符串（数字）类型的维度，例如 Upload-File-Size、Download-File-Size 和 Client-IP。	国家/地区 IS NOT EMPTY	查找可用或指定了国家/地区名称的事件。
或者	搜索其中一个或两个条件均为 true 时的值。	(User-Name = John* OR User-Name = *Smith) AND Event-Type = “Session.Logon”	显示所有以 John 开头或以 Smith 结尾的用户名的 Session.Logon 事件。

> 注意
>
> 对于 **NOT EQUAL** 运算符，在为条件中的维度输入值时，请使用自助搜索页面上提供的数据源的精确值。尺寸值区分大小写。

修改自定义风险指示器

1. 导航到 安全 **>** 自定义风险指示器。
2. 选择要修改的自定义风险指示器。
3. 在 修改指标 页面上，根据需要修改信息。
4. 单击保存更改。

> 注意
>
> 如果在用户时间轴上修改现有自定义风险指示器的状况、风险类别、严重性和名称等属性，您仍然可以查看先前为用户触发的自定义风险指示器（使用旧属性）的出现次数。
>
> 例如，您已经创建了一个自定义风险指示器，条件为“国家/地区”！= 印度。因此，当用户从印度以外的国家/地区登录时，将触发此自定义风险指示器。现在，您将自定义风险指示器的条件修改为 国家/地区！=“美国”。在这种情况下，您仍然可以查看先前出现的自定义风险指示器的条件为 C *ountry!=* 触发风险指示器的用户时间轴上的印度。

删除自定义风险指示器

1. 导航到 安全 **>** 自定义风险指示器。
2. 选择要删除的自定义风险指示器。
3. 单击删除。
4. 在对话框中，确认删除自定义风险指示器的请求。

> 注意
>
> 如果删除自定义风险指示器，则仍然可以在用户时间轴上查看先前为用户触发的自定义风险指示器的出现次数。
>
> 例如，您删除条件为“国家/地区”的现有自定义风险指示器！= 印度。在这种情况下，您仍然可以查看先前出现的自定义风险指示器的条件为 C *ountry!=* 触发风险指示器的用户时间轴上的印度。

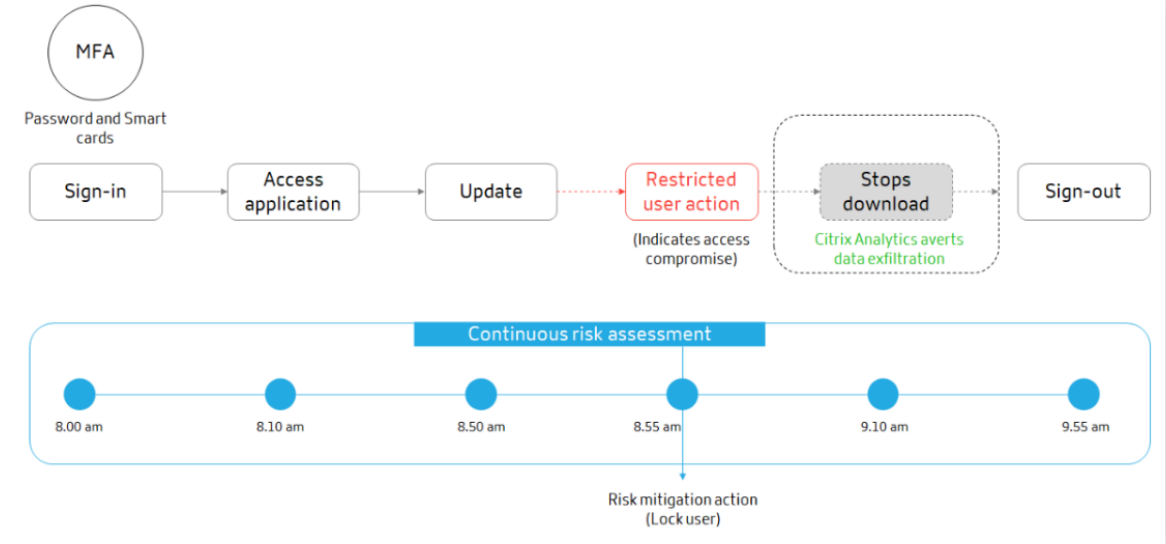
持续的风险评估

December 7, 2023

随着便携式计算设备和互联网的使用增加，Citrix Workspace 用户几乎可以在任何位置和任何设备上工作。这种灵活性带来的挑战在于，远程访问会通过数据泄露、盗窃、故意破坏和服务中断等网络犯罪活动使敏感数据面临安全风险。组织内的员工也可能为这种损害做出贡献。

解决此类风险的一些传统方法是实施多因素身份验证、短登录会话等。尽管这些风险评估方法可确保更高级别的安全性，但在对用户进行初步验证后，它们并不能提供完全的安全性如果恶意用户成功获得网络访问权限，他们就会滥用对组织有害的敏感数据。

为了增强安全性并确保更好的用户体验，Citrix Analytics 推出了持续风险评估解决方案。该解决方案可确保使用 Citrix Virtual Apps and Desktops 或 Citrix DaaS（前身为 Citrix Virtual Apps and Desktops 服务）的用户的风险暴露与初始阶段验证时相同，无需用户每次都进行证明，从而保护您的数据免受外部网络罪犯和恶意内部人员的侵害。此解决方案是通过在会话期间持续评估风险事件以及自动应用措施以防止组织的资源进一步滥用来实现的。



用例

假设一个用户 Adam Maxwell，在从一个不寻常的位置进行多次登录尝试失败后，他首次能够访问网络，这与他们的常规行为相反。此外，该地点还有网络攻击的记录。在这种情况下，你需要立即采取行动，避免 Adam 的帐户被进一步滥用。你可以锁定 Adam 的帐户并通知他所采取的行动。此操作可能会暂时对用户的帐户造成服务中断。用户可以联系管理员以获取恢复帐户的帮助。

考虑另一种情况，即 Adam 首次从新设备和新 IP 访问网络。您可以联系 Adam，询问他是否识别出此活动。如果是这样，可能是因为 Adam 更换了工作设备并且正在使用家庭网络工作。此活动不会对组织的安全造成任何损害，可以忽略。但是，如果用户没有执行此活动，则该帐户可能已被盗用。在这种情况下，您可以锁定用户的帐户以防止任何进一步的损害。

主要功能

持续风险评估可自动执行与策略和可见性控制板相关的一些功能：

支持多种条件

创建或修改策略时，最多可以添加四个条件。这些条件可以包含默认风险指标和/或自定义风险指标、用户风险评分的组合。

有关更多信息，请参阅 什么是策略。

在应用操作之前通知用户

在对用户的帐户应用适当的操作之前，您可以通知用户并评估已检测到的异常活动的性质。

有关详细信息，请参阅请求最终用户响应。

应用操作后通知用户

对于某些活动，在应用操作之前等待用户响应可能会使用户的帐户和组织的安全受到威胁。在这种情况下，您可以在检测到异常活动时应用破坏性操作，然后通知用户相同的情况。

有关详细信息，请参阅应用中断性操作后通知用户。

强制和监控模式

您可以根据自己的要求将策略设置为强制或监控模式。处于强制模式的策略对用户的帐户有直接影响。但是，如果要在实施策略之前评估策略的影响或结果，则可以将策略设置为监控模式。

有关详细信息，请参阅 支持的模式。

访问权限和策略控制板的可见性

使用“访问摘要”控制板，您可以深入了解用户尝试访问的次数。有关更多信息，请参阅 访问摘要。

使用“政 策和操作”控制板，您可以深入了解应用于用户帐户的策略和操作。有关更多信息，请参阅 策略和操作。

默认策略

Citrix Analytics 引入了默认情况下在“策略”控制板上启用的预定义 策略。这些策略是通过使用风险指标和用户风险评分作为预定义的条件来创建的。每个默认策略都会分配一个全局操作。

> 注意
>
> 您的环境中列出的策略可能会有所不同，具体取决于您首次开始使用 Citrix Analytics 的时间以及是否进行了任何本地更改。

有关更多信息，请参阅 什么是策略。

您可以使用以下默认策略或根据需要修改它们：

策略名称	条件	数据源	操作
成功利用凭据	触发 身份验证失败过多 和 可疑登录 风险指标时	Citrix Gateway	锁定用户
潜在的数据泄露	触发 潜在数据泄露 风险指标时	Citrix Virtual Apps and Desktops 和 Citrix DaaS	注销用户
来自可疑 IP 的异常访问	触发“可疑登录”和“从可疑 IP 登录”风险指标时	Citrix Gateway	锁定用户
首次从设备访问	当 CVAD-首次从新设备访问时 风险指标被触发	Citrix Virtual Apps and Desktops 和 Citrix DaaS	请求最终用户响应
进入时不可能旅行	当触发不可能的旅行风险指标时。	Citrix Virtual Apps and Desktops 和 Citrix DaaS	请求最终用户响应
无法通过身份验证旅行	当触发不可能的旅行风险指标时。	Citrix Gateway	请求最终用户响应

策略和操作

December 7, 2023

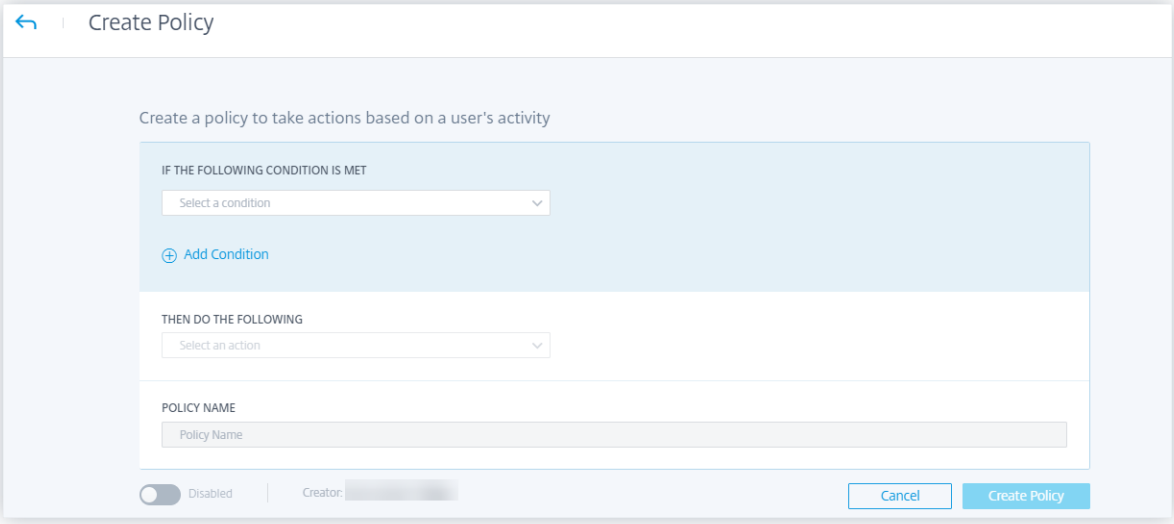
> ** 注意事项 **
>
> ：Citrix Content Collaboration 和 ShareFile 的使用寿命已接近尾声，不再向用户开放。

您可以在 Citrix Analytics 上创建策略，以帮助您在发生异常或可疑事件时对用户帐户执行操作。策略允许您自动执行诸如禁用用户和将用户添加到监视列表之类的操作的过程。启用策略后，会在发生异常事件并满足策略条件后立即应用相应的操作。您还可以手动对具有异常事件的用户帐户应用操作。

策略是什么

策略是应用操作必须满足的一组条件。策略包含一个或多个条件和单个操作。您可以创建具有多个条件的策略和一个可应用于用户帐户的操作。

风险评分是一个全局条件。全局条件可应用于特定数据源的特定用户。您可以密切关注显示任何异常事件的用户帐户。其他条件特定于数据源及其风险指示器。这些条件包含风险评分、默认风险指示器和自定义风险指示器的组合。创建策略时，您最多可以添加 4 个条件。



例如，如果您的组织使用敏感数据，则可能需要限制用户内部共享或访问的数据量。但是，如果您有一个庞大的组织，单个管理员管理和监视许多用户是不可行的。您可以创建一个策略，其中任何过度共享敏感数据的人都可以添加到监视列表或立即禁用其帐户。

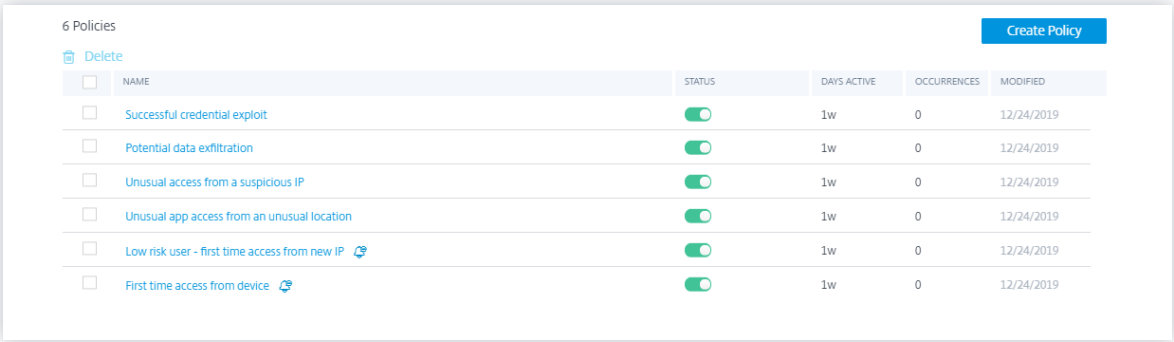
默认策略

默认策略是预先定义的，并在策略控制板上启用。它们是根据预定义的条件创建的，并为每个默认策略分配相应的操作。您可以使用默认策略，也可以根据需要对其进行修改。

Citrix Analytics 支持以下默认策略：

- 成功利用凭据
- 潜在的数据泄露
- 来自可疑 IP 的异常访问
- 首次从设备访问
- Virtual Apps and Desktops 以及 Citrix DaaS - 访问时不可能旅行
- Gateway-无法通过身份验证传输

有关上述默认策略的预设条件和操作的信息，请参阅 持续风险评估。



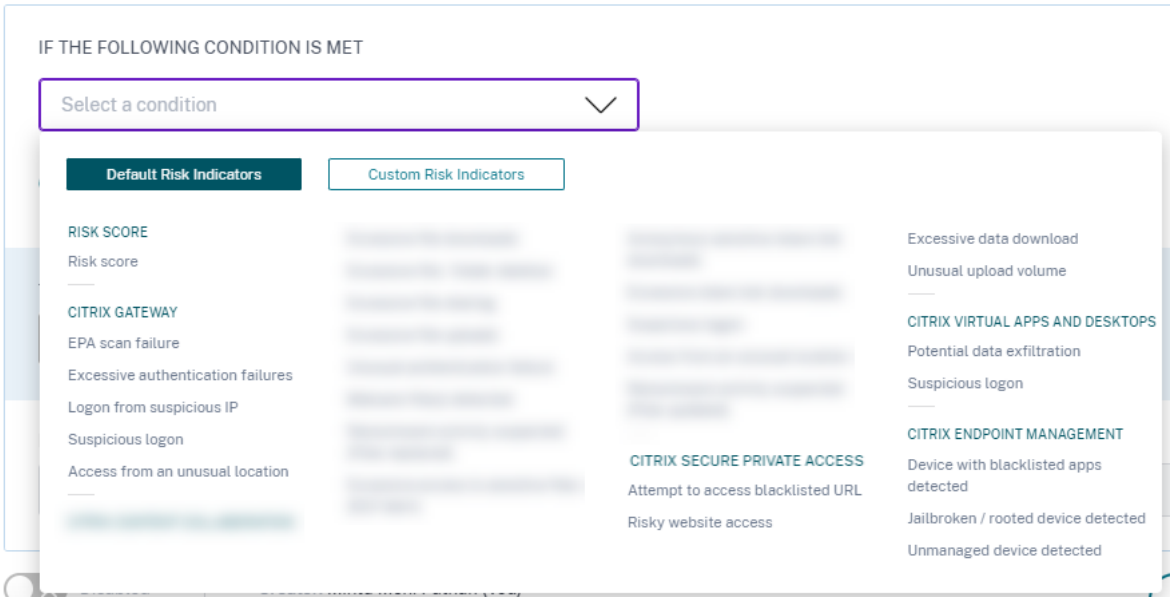
有关地理围栏用例的预定义策略的信息，请参阅 预配置的策略。

如何添加或删除条件

要添加更多条件，请在创建策略页面的如果满足以下条件部分中选择添加条件。要删除条件，请选择条件旁边显示的 - 图标。

默认和自定义风险指示器

条件菜单根据 创建策略 页面上的 默认风险指示器 和 自定义风险指示器 选项卡进行隔离。使用这些选项卡，您可以轻松确定在选择策略配置条件时要选择的风险指示器类型。



有什么行动

操作是对可疑事件的响应，可防止将来发生异常事件。您可以对显示异常或可疑行为的用户帐户应用操作。您可以配置策略以自动对用户的帐户应用操作，也可以从用户的风险时间表手动应用特定操作。

您可以查看每个 Citrix 数据源的全局操作或操作。您还可以随时为用户禁用以前应用的操作。

> 注意
>
> 无论触发风险指示器的数据源如何，都可以应用与其他数据源相关的操作。

下表介绍了您可以执行的操作。

动作名称	说明	适用的数据源
全球行动		
添加到播放列表	当您想要监视用户未来的潜在威胁时，可以将它们添加到监视列表中。 “**Watchlist** 中的用户”窗格显示您希望根据其帐户上的异常事件监视潜在 威胁的所有用户。根据组织的策略，您可以使用“添加至监视列表”操作将用户添加到监视列表中。 要将用户添加到监视列表，请导航到该用户的个人资料，从“操作”菜单中选择“添加到监视列表”。单击“应用”以强制执行操作。	所有数据源

动作名称	说明	适用的数据源
通知管理员	当触发用户的风险指示器时，您可以手动通知管理员或创建自动通知策略。您可以从组织中的 Citrix Cloud 域和其他非 Citrix Cloud 域中选择管理员。如果您是具有完全访问权限的 Citrix Cloud 管理员，则默认情况下，将为您的 Citrix Cloud 帐户禁用电子邮件通知。要接收电子邮件通知，请在您的 Citrix Cloud 帐户上启用它。有关详细信息，请参阅 接收电子邮件通知。如果您是具有管理 Security Analytics 的自定义访问权限（只读和完全访问权限）的 Citrix Cloud 管理员，则会为您的 Citrix Cloud 帐户启用电子邮件通知。要停止接收来自 Citrix Analytics 的电子邮件通知，请请求您的 Citrix Cloud 完全访问权限管理员从通知管理员通讯组列表中删除您的姓名。有关信息，请参阅电子邮件通讯组列表。	
请求最终用户响应	当用户帐户中存在任何异常或可疑事件时，您可以通知用户确认用户是否识别了该事件。根据事件，您可以确定对用户帐户采取的下一个操作方案。有关详细信息，请参阅请求最终用户响应。	
通知最终用户	当用户的帐户发生任何异常或可疑活动时，您可以通过电子邮件通知通知最终用户。有关更多信息，请参阅通知最终用户。	
Citrix Gateway 操作		
注销活动会话	应用操作后，它会注销当前处于事件状态的用户会话。它不会阻止将来的任何用户会话。	Citrix Gateway 本地和 Citrix Application Delivery Management

动作名称	说明	适用的数据源
锁定用户帐户	当用户的帐户由于异常行为而被锁定时，他们无法通过 Citrix Gateway 访问任何资源，直到网关管理员解锁该帐户。	Citrix Gateway 本地
解锁用户帐户	如果用户的帐户在没有检测到异常行为的情况下被意外锁定，则可以应用此操作来解锁该帐户并恢复对该帐户的访问权限。	Citrix Gateway 本地
Citrix Virtual Apps and Desktops 以及 **Citrix DaaS** 操作		
注销活动会话	应用操作后，它会注销当前处于事件状态的用户会话。它不会阻止将来的任何用户会话。	Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）
开始会话录制	如果用户的 Virtual Desktops 帐户出现异常事件，管理员可以开始记录用户当前的活动会话。如果用户使用的是 Citrix Virtual Apps and Desktops 7.18 或更高版本并登录到虚拟会话，则管理员可以动态触发 Citrix Analytics for Security 的启动会话录制操作，该操作开始录制用户的当前活动会话。	Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）

> 备注
>
> - 无论数据源如何，您都可以对风险指示器应用任何操作。
> - 管理员现在可以在 Citrix DaaS 站点上运操作态会话录制操作以及动态录制用户的虚拟会话。
> - “请求最终用户回复”和“通知最终用户”操作无法应用于匿名用户，因为他们在 A **ctive Directory** 中没有电子邮件地址。因此，通过在 A **ctiv** e Directory 和 Citrix Cloud 之间建立连接，确保用户的任一电子邮件地址在 ActiveDirectory 中可用。

仅查看共享

在对用户帐户应用“将链接更改为仅供查看”共享 操作之前，请确保满足以下条件：

必备条件

- 管理员必须在 Content Collaboration 中拥有一个企业帐户才能使用“更改链接以进行仅查看共享”操作。
- “仅查看共享”是 Citrix Content Collaboration 的企业帐户中应请求提供的一项功能。在 Citrix Analytics 中将 链接应用于仅查看共享 操作之前，请确保用户和管理员的 Content Collaboration 企业帐户中已启用“仅查看共享”功能。有关更多信息，请参阅 Citrix 支持文章- CTX208601。

受支持的文件类型　仅查看共享操作仅适用于以下文件类型：

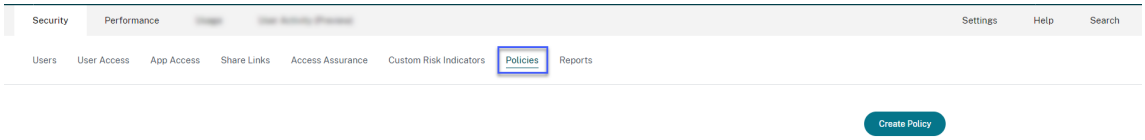
- Microsoft Office 文件
- PDF
- 映像文件（需要 SZC v3.4.1 或更高版本）：
  - BMP
  - GIF
  - JPG
  - JPEG
  - PNG
  - TIF
  - TIFF
- 存储在 Citrix 管理的存储区域中的音频和视频文件。

配置策略和操作

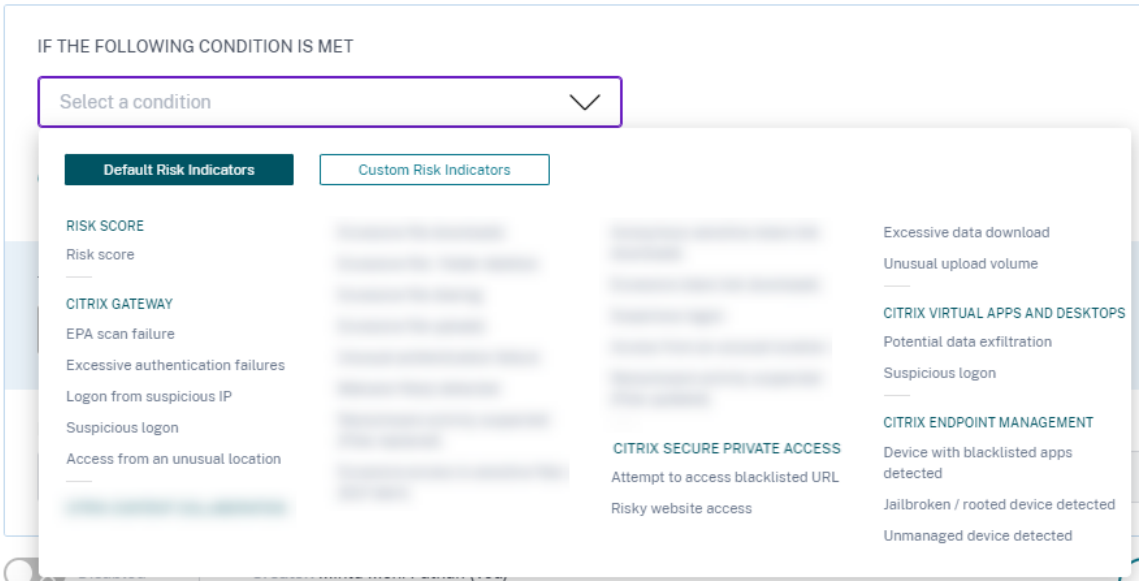
例如，按照以下步骤，您可以创建过度文件共享策略。使用此策略，当组织中的用户共享异常大量的数据时，共享链接将自动过期。当用户共享的数据超过该用户正常行为时，会收到通知。通过应用“过多的文件共享”策略并立即采取行动，您可以防止数据从任何用户的帐户中泄露。

要创建策略，请执行以下操作：

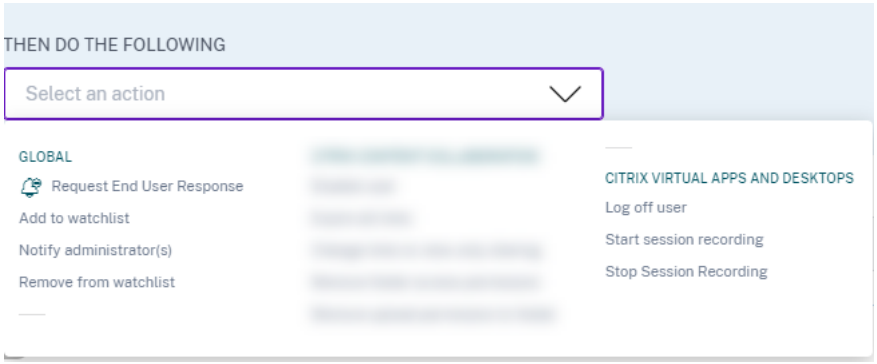
1. 登录 Citrix Analytics 后，转到安全 **>** 策略 **>** 创建策略。



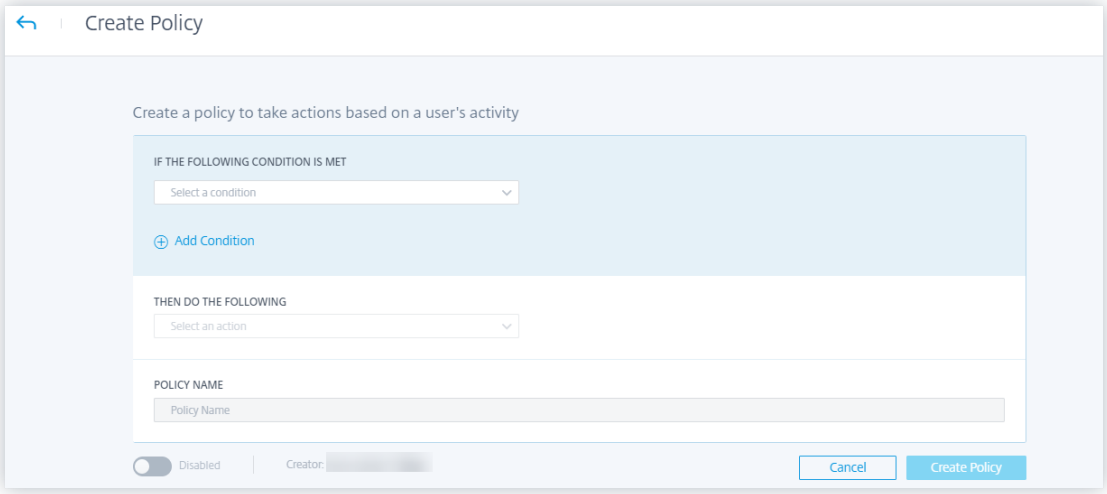
2. 从如果满足以下条件列表框中，选择要应用操作的默认或自定义风险指示器条件。



3. 从则执行以下操作列表中，选择一个操作。



4. 在 策略名称 文本框中，提供名称并使用提供的切换按钮启用策略。



5. 单击创建策略。

创建策略后，该策略将显示在“策略”控制板上。

策略 控制板显示与成功发现并连接到 Citrix Analytics 的数据源关联的策略。控制面板不显示为未发现的数据源定义了条件的策略。

但是，关闭已连接的数据源的数据处理不会影响“策略”控制板上的现有 策略。

请求最终用户响应

请求最终用户响应 是一项全局操作，您可以在检测到用户的 Citrix 帐户中存在异常活动后立即向用户发出警报。应用操作时，系统会向用户发送电子邮件通知。用户需要通过电子邮件回复其活动的合法性。

确定要为用户应用的操作：

根据用户的回应，您可以确定要采取的下一个操作方案。您可以应用全局操作，例如“添加到监视列表”、“通知管理员”。或者你可以应用特定于数据源的操作，例如 Citrix Gateway-Lock 用户。

如果您收到用户执行了报告的事件的响应，则表示该事件不可疑，您无需对用户的帐户采取措施。向用户发送安全警报的每日限制为三封电子邮件。

假设某个 Citrix Content Collaboration 用户的风险分数在 80 分钟内超过 80。您可以通过应用“请求最终用户响应”操作向用户 发出有关此异常行为的警报。安全警报将通过电子邮件 ID `security-analytics@cloud.com` 发送给用户。

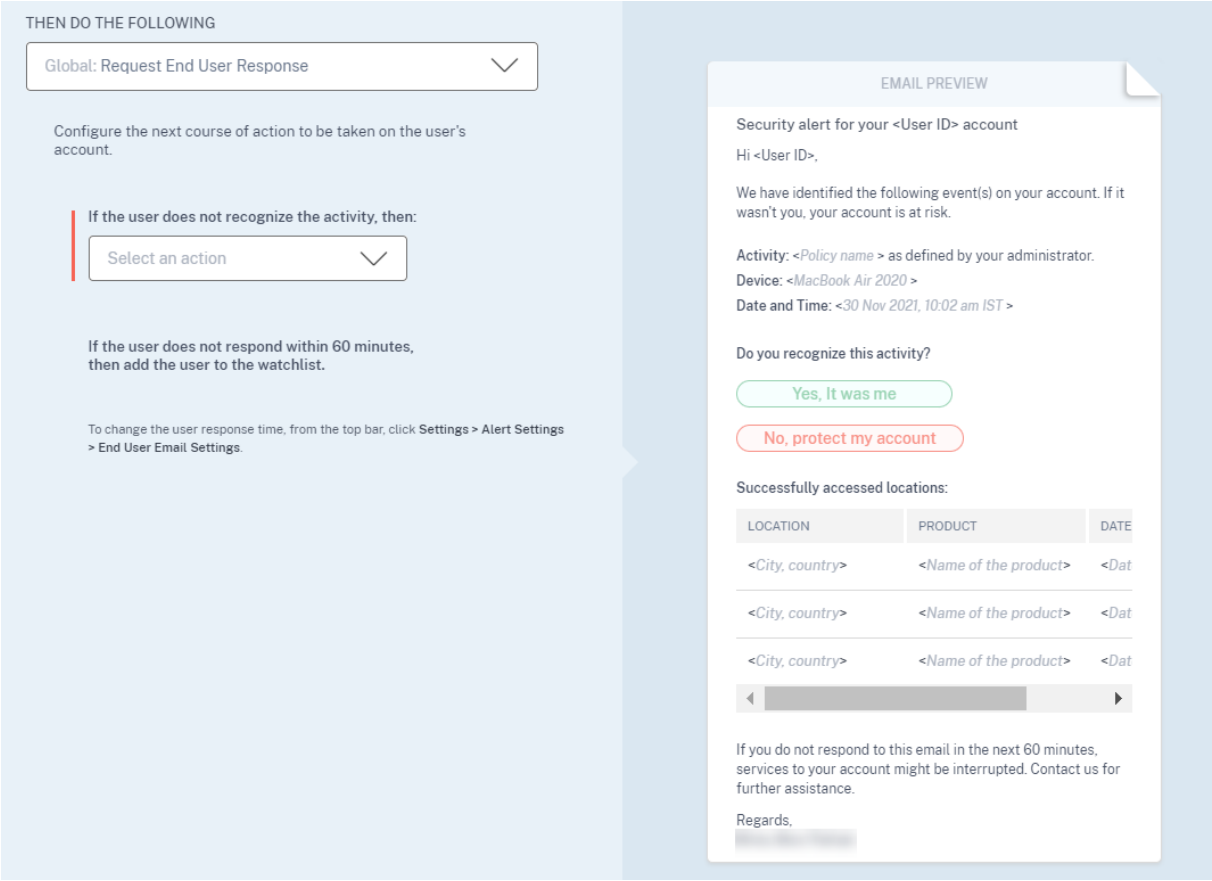
该电子邮件包含以下信息：

- 触发风险指示器的用户事件
- 用户的设备
- 用户事件的日期和时间
- 成功访问产品或服务的位置（城市和国家/地区）。如果城市或国家/地区不可用，相应的值将显示为“未知”

请求最终用户响应 操作将添加到用户的风险时间表中。

如果用户无法识别其 Citrix 帐户中检测到的活动，Citrix Analytics 将应用您定义的操作。

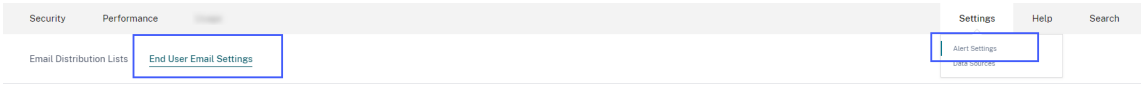
如果用户在收到电子邮件后的一小时内未能发送响应，Citrix Analytics 会将该用户添加到监视列表中。您可以监控用户及其帐户中是否存在任何可疑活动，并采取相应的措施。



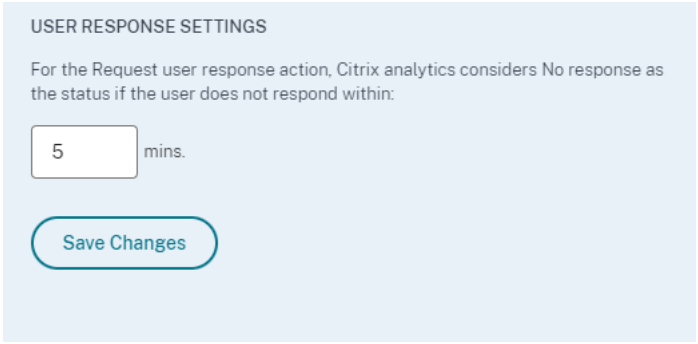
如何设置用户响应时间　您可以配置用户对安全警报电子邮件的响应时间。如果用户在指定的时间段内没有对报告的活动做出回应，则该用户将被添加到监视列表中进行监控。

按照以下步骤配置用户的响应时间：

1. 单击 设置 **>** 警报设置 **>** 最终用户电子邮件设置。



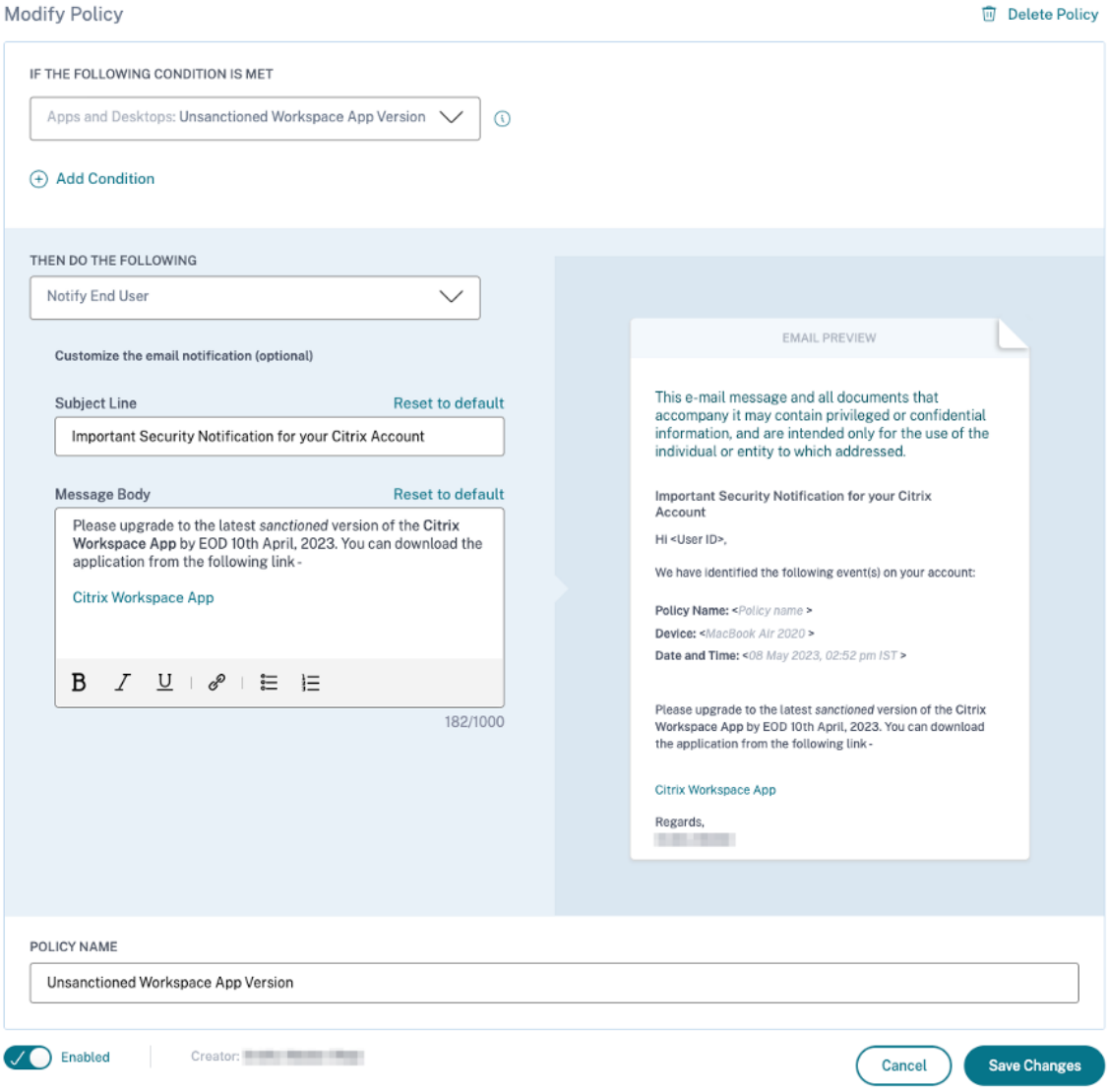
2. 在“最 终用户电子邮件设置”页面上，在文本框中输入分钟数。



3. 单击保存更改。

您还可以在安全警报电子邮件中添加横幅、标题文本和页脚文本，使其看起来合法、吸引用户的注意力并延长响应时间。有关详细信息，请参阅 最终用户电子邮件设置

通知最终用户　通知最终用户是一项全局操作，当检测到终端用户的 Citrix 帐户出现异常或可疑行为时，您可以使用该操作向最终用户发送电子邮件通知。电子邮件主题行和邮件正文是可自定义的。触发策略后应用操作时，会向用户发送电子邮件通知。不要求最终用户做出任何回应，也不会对用户的帐户执行任何破坏性操作。



此操作可以帮助基于内置或自定义风险指标触发器为各种合规用例提供服务。凭借可自定义的电子邮件主题行和邮件正文，它还足够灵活，可以为许多通用的最终用户通知用例提供服务，这些用例不需要对用户的帐户进行响应或执行破坏性操作。

该电子邮件包含以下信息：

- 与操作相关的策略名称。
- 用户的设备（如果有）
- 用户事件的日期和时间

最终用户的电子邮件通知是从电子邮件 ID `security-analytics@cloud.com` 发送的。

> 注意
>
> 各项策略的每日限制为每位用户三封电子邮件。一旦超过此阈值，便不会应用该操作，也不会向最终用户发送任何电子邮件通知。该操作在用户的时间轴视图中可见，消息显示用户已达到每日电子邮件限制。

该操作将添加到用户的风险时间表中。但是，它不是手动操作，不能从时间轴视图应用于用户。

自定义最终用户电子邮件内容　以前，Citrix Analytics 管理员手动联系最终用户，提供有关检测可疑活动的补救说明，而结案是一个耗时的过程。

引入 了最终用户电子邮件内容的自定义 功能，用于请求最终用户响应、通知最终用户和信息性电子邮件。最终用户回复电子邮件寻求用户验证/回复，但是，信息性电子邮件会显示可疑活动的类型以及已经采取的补救措施。通知最终用户电子邮件会通知最终用户有关其 Citrix 帐户中的合规违规行为/可疑活动，而不要求他们回复。

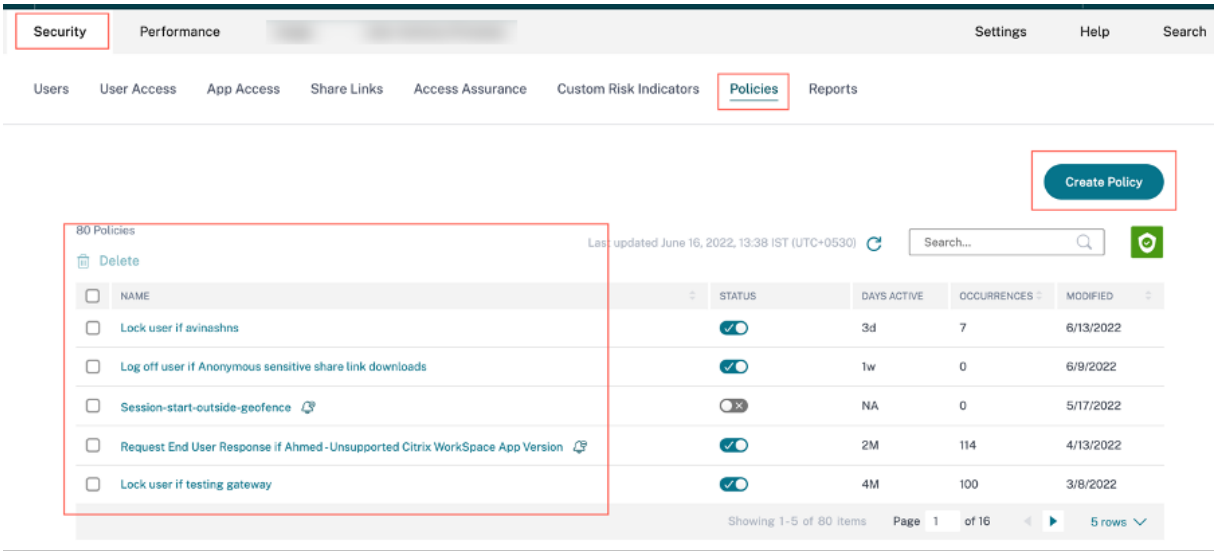
借助 自定义最终用户电子邮件内容 功能，Citrix Analytics 管理员可以在请求最终用户回复/通知最终用户/信息邮件正文模板中添加自定义消息。使用富文本框编辑器，管理员可以使用各种编辑工具（如粗体、斜体、超链接等）来更改每个策略的内容。

> 注意
>
> 自定义最终用户电子邮件内容功能仅适用于 基于策略的操作 ，不适用于手动操作。

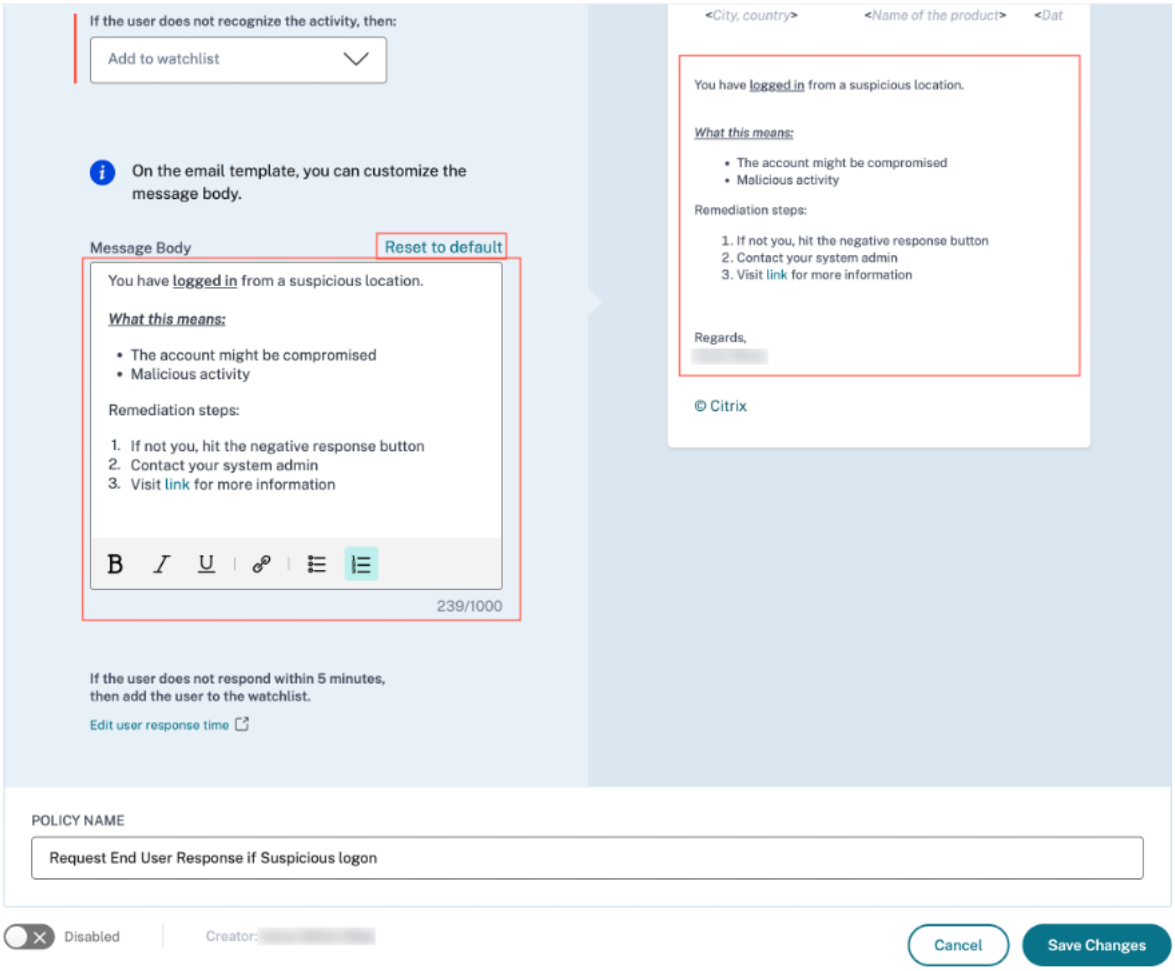
您可以自定义三种类型的电子邮件的内容：

- 请求最终用户回复电子邮件。
- 通知最终用户电子邮件
- 执行以下任一最终用户操作时发送的电子邮件：
  - **Citrix Apps and Desktops** 下的注销操作
  - 在 **Citrix Gateway** 下注销并锁定用户

您可以在安全 **>** 策略选项卡中查看策略列表。



您可以通过单击现有策略或在创建新策略时查看自定义的电子邮件正文。在右侧窗格中，您可以预览更新的电子邮件内容。



> 注意
>
> - 管理员可以通过单击“重置为默认值”链接将内容设置为默认模板。自定义正文的字符数限制为 1000。
> - 对于“通知最终用户”操作，“主题行”字段也可以由管理员自定义。单击“重置为默认值”链接可以将其重置为默认值。自定义电子邮件主题的字符限制为 500。

单击保存更改以创建/更新策略。触发策略时，将向最终用户发送以下电子邮件通知：

- 请求最终用户回复电子邮件：发送电子邮件请求用户回复的策略操作。
- 通知最终用户电子邮件：发送给最终用户的电子邮件通知，告知他们其 Citrix 帐户中有关合规性问题、可疑活动等使。
- 信息性电子邮件：在最终用户执行操作后发送的信息性电子邮件。

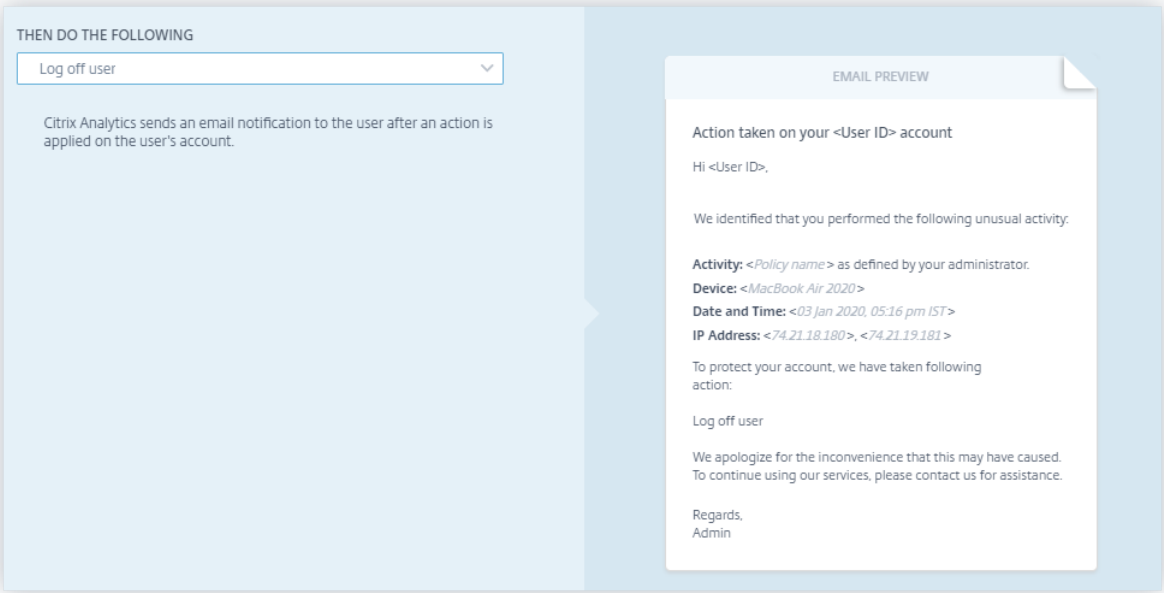
最终用户可以阅读电子邮件并根据管理员的请求完成补救操作。

> 注意
>
> 具有只读权限的管理员无法编辑/添加电子邮件正文。

应用中断性操作后通知用户

在此操作类型中，您可以应用中断性措施，例如在检测到异常事件时 注销用户 和 锁定 用户帐户上的用户。当对用户的帐户应用操作时，其帐户的服务可能会中断。在这种情况下，用户必须联系管理员才能像之前一样访问其帐户。

假设某个 Citrix Content Collaboration 用户的风险分数在 80 分钟内超过 80。您可以将用户注销。执行此任务后，用户将无法访问其帐户，并且会通过电子邮件 ID `security-analytics@cloud.com` 向用户发送电子邮件通知。该电子邮件包含事件的详细信息，例如事件、设备、日期和时间以及 IP 地址。用户必须像以前一样联系管理员才能访问其帐户。

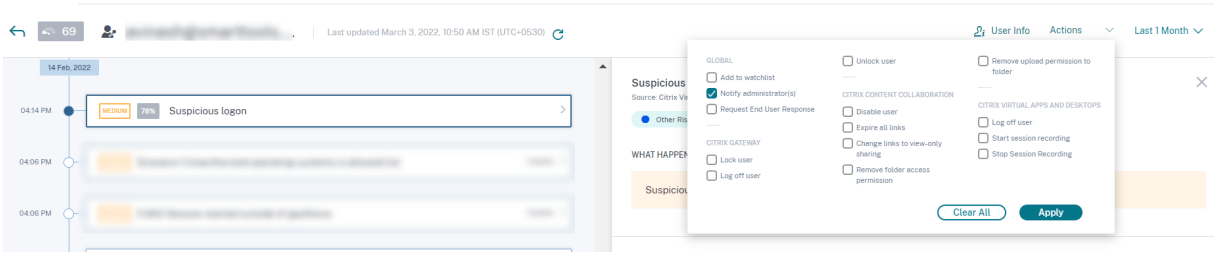


手动应用操作

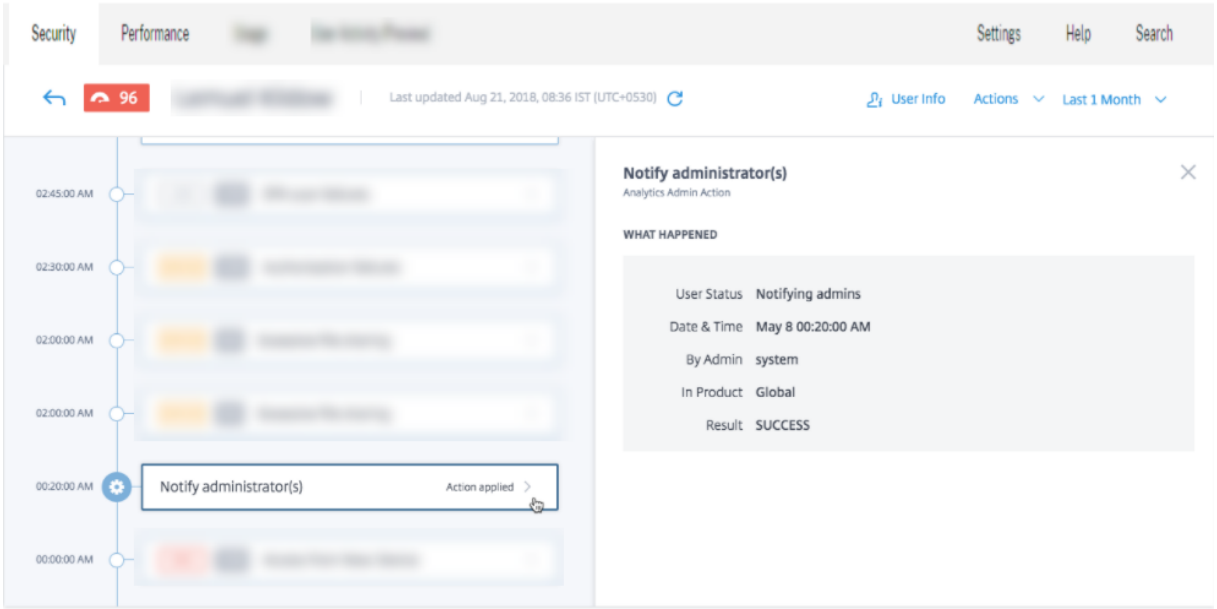
考虑一个用户，即 Lemuel，他首次使用新设备登录网络。由于她的行为异常，要监视她的帐户，您可以使用“通知管理员”操作。

要手动将操作应用于用户，您必须：

导航到用户的个人资料，然后选择相应的风险指示器。从“操 作”菜单中，选择“通知管理员”操作，然后单击“应用”。



系统会向所有管理员或选定的管理员发送电子邮件通知，以监视其帐户。应用的操作将添加到她的风险时间表中，操作详细信息显示在风险时间表页面的右侧窗格中。



备注

- 如果您是具有完全访问权限的 Citrix Cloud 管理员，则默认情况下，将为您的 Citrix Cloud 帐户禁用电子邮件通知。要接收电子邮件通知，请在您的 Citrix Cloud 帐户上启用它。有关详细信息，请参阅 接收电子邮件通知。
- 如果您是具有管理 Security Analytics 的自定义访问权限（只读和完全访问权限）的 Citrix Cloud 管理员，则会为您的 Citrix Cloud 帐户启用电子邮件通知。要停止接收来自 Citrix Analytics 的电子邮件通知，请请求您的 Citrix Cloud 完全访问权限管理员从通知管理员通讯组列表中删除您的姓名。有关信息，请参

> 阅电子邮件通讯组列表。

管理策略

您可以查看“策略”控制板来管理在 Citrix Analytics 上创建的所有策略，从而监视和识别网络中的不一致情况。在策略控制面板上，您可以：

1. 查看策略列表
2. 该策略的详细信息
    - 策略的名称
    - 状态—已启用或禁用。
    - 策略的持续时间—策略处于事件状态或非事件状态的天数。
    - 发生次数—触发策略的次数。
    - 已修改—时间戳，仅当策略已修改时。
3. 删除策略
    - 要删除策略，您可以选择要删除的策略，然后单击 删除。
    - 或者，您可以单击策略的名称以定向到修改策略页面。单击 删除策略。在对话框中，确认删除策略的请求。
4. 创建策略
5. 单击策略的名称可查看更多详细信息。您也可以在单击策略名称时对其进行修改。可以进行的其他修改如下：
    - 更改策略的名称。
    - 保单的条件。
    - 要应用的操作。
    - 启用或禁用策略。
    - 删除策略。

> 注意
>
> - 如果您不想删除策略，则可以选择禁用该策略。
> - 要在“策略”控制板上重新启用策略，请执行以下操作：
>   - On the Policies dashboard, click the **Status** slider button and refresh the page. The **Status** slider button turns green.
>   - On the Modify Policy page, click the **Enabled** slider button on the bottom of the page.

支持的模式

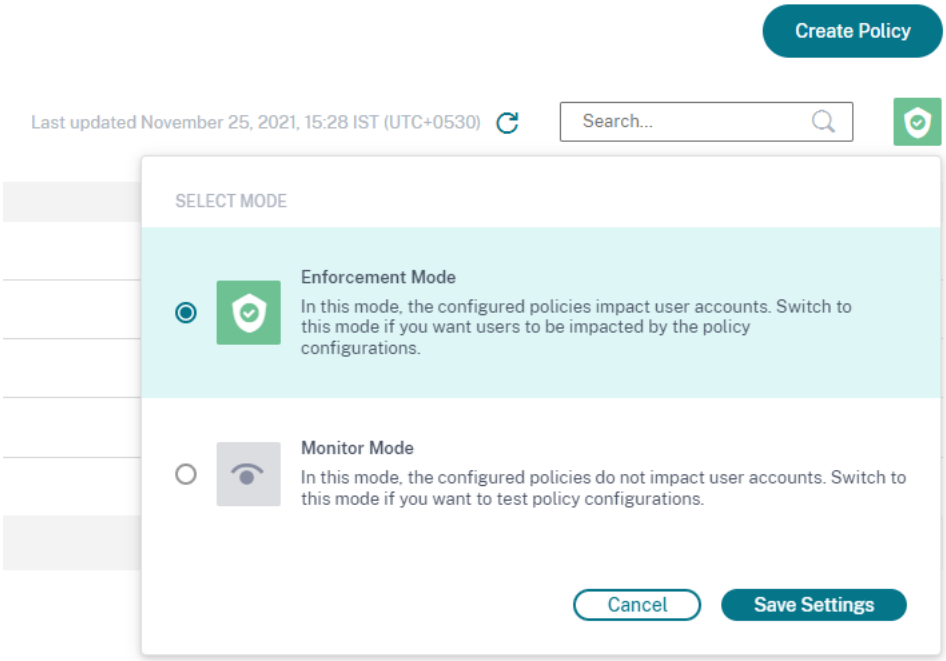
Citrix Analytics 支持以下策略模式：

- 强制模式 -在此模式下，配置的策略会影响用户帐户。
- 监视模式 -在此模式下，配置的策略不会影响用户帐户。如果要测试任何策略配置，可以将策略设置为此模式。

使用以下说明在策略上配置模式：

1. 导航到 安全 > 策略。
2. 在“策略”页面上，选择右上角显示在搜索栏旁边的图标。此时将显示“选择模式”窗口。
3. 选择您选择的模式，然后单击 保存设置。

> 注意
>
> Analytics 创建的默认策略设置为监视模式。因此，现有策略也会继承此模式。您可以一起评估所有策略的影响，然后将它们更改为强制模式。



面向策略的自助搜索

在 自助搜索 页面上，您可以查看满足策略中定义的条件的用户事件。该页面还显示应用于这些用户事件的操作。根据应用的操作过滤用户事件。

预配置的自定义风险指标和策略

December 7, 2023

Citrix Analytics for Security 供了预配置的自定义风险指示器列表和策略，以帮助您监视 Citrix 基础架构的安全性。这些预配置的自定义风险指标和策略的条件已根据特定的安全风险场景（例如受到攻击的用户、内部威胁和数据泄露）来定义。您还可以修改这些预配置的条件，或根据自己的安全要求添加自己的条件，并使用自定义风险指示器来降低风险。

目前，预配置的自定义风险指标可用于以下情况：

- 地理围栏
- 首次访问

为地理围栏场景预先配置了自定义风险指标

使用以下预先配置的自定义风险指标来检测来自地理围栏区域之外的用户事件。

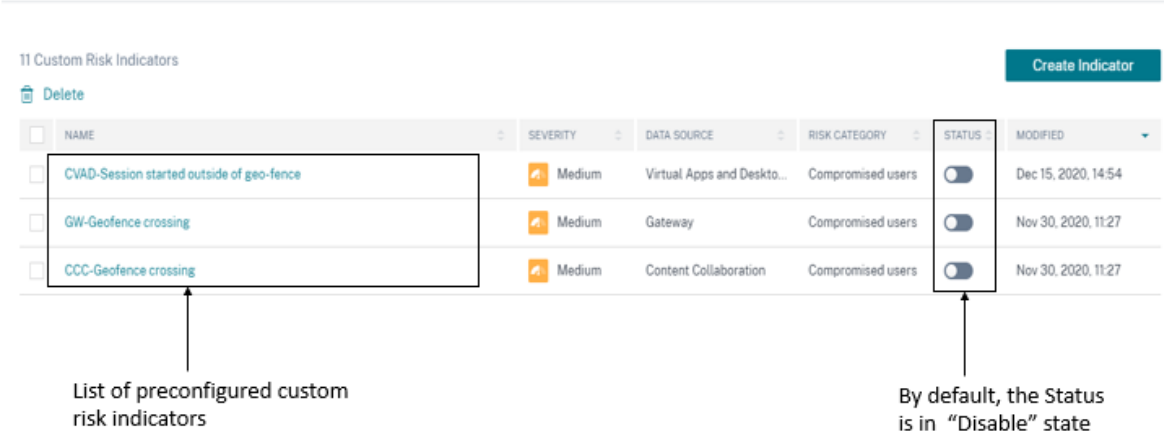
- CVAD-会话在地理围栏之外开始
- GW-Geofence 穿越

每当用户从其常规运营国家或地理围栏以外的地方访问 Citrix 产品时，都会触发预配置的自定义风险指示器。默认情况下，地理围栏设置为“美国”。您可以将所需的国家/地区设置为地理围栏。

> 注意
>
> 在 地理围栏风险指示器之外启动的 *CVAD* 会话 链接到访问保证位 置功能的地理围栏 设置。因此，您不能在风险指示器的条件下直接修改地理围栏的国家/地区。要更新风险指示器中的地理围栏国家/地区，请在访问保证位置控制板 的地理围栏设置 中选择国家/地区。有关详细信息，请参阅 访问保证位置控制板。

要查看预配置的自定义风险指示器，请选择 安全 **>** 自定义风险指示器。

默认情况下，预先配置的自定义风险指标处于禁用状态。使用 状态 按钮启用它们。



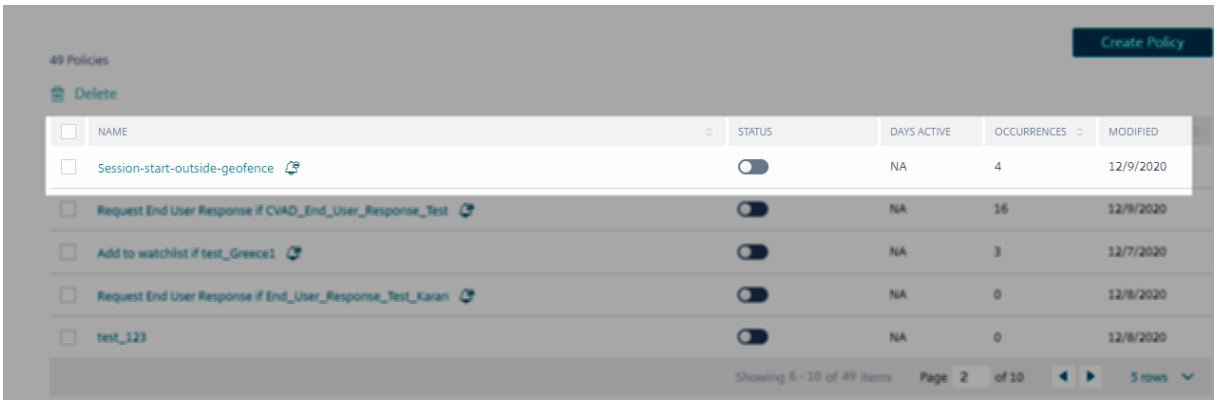
下表介绍了用于地理围栏的各种预配置的自定义风险指标。

自定义风险指标名称	场景	自定义指标条件	数据源	风险类别
CVAD-会话在地理围栏之外开始	用户在运作国家/地区外开始虚拟会话	Event-Type = Session.logon Country != “United States”	Citrix Workspace 应用程序	受影响的用户
GW-Geofence 穿越	用户在运作国家/地区外成功身份验证	Event-Type = “VPN_AI” AND Country != “United States”	Citrix Gateway（本地）	受影响的用户

针对地理围栏场景的预配置策略

Citrix 提供了预配置的策略，每当 用户从其运营国家/地区之外启动虚拟会话时，该策略都会将“请求最终 用户响应”操作应用于用户帐户。用户会收到一封电子邮件，并根据用户的回复采取适当的操作，例如将用户添加到监视列表或通知管理员采取进一步措施。有关详细信息，请参阅请求最终用户响应。

要查看预配置的策略，请选择 安全 > 策略。



下表介绍了用于地理围栏的预配置策略。

策略名称	场景	保单条件	应用的操作
会话在地理围栏之外开始	当用户在其运营国家/地区之外启动虚拟会话时，管理员能够通过“请求最终用户响应”操作来验证用户的合法性	与预配置的自定义风险指示器一起使用-“CVAD 会话在地理围栏之外启动”	请求最终用户响 根据以下用户的响应，将应用相应的操作： 如果用户无法识别事件：添加到关注列表 如果用户识别出事件：无需执行任何操作 如果用户在收到电子邮件后 60 分钟内没有回复：将用户添加到监视列表

> 注意
>
> “请求最终用户响应”操作仅在美国区域受支持。因此，如果您的组织已加入 Citrix Cloud 中的欧盟区域，则预配置的策略不会应用于您的帐户。要使用预配置的策略，请修改策略并选择您选择的其他操作。

使用预配置的自定义风险指标来创建自己的策略，用于地理围

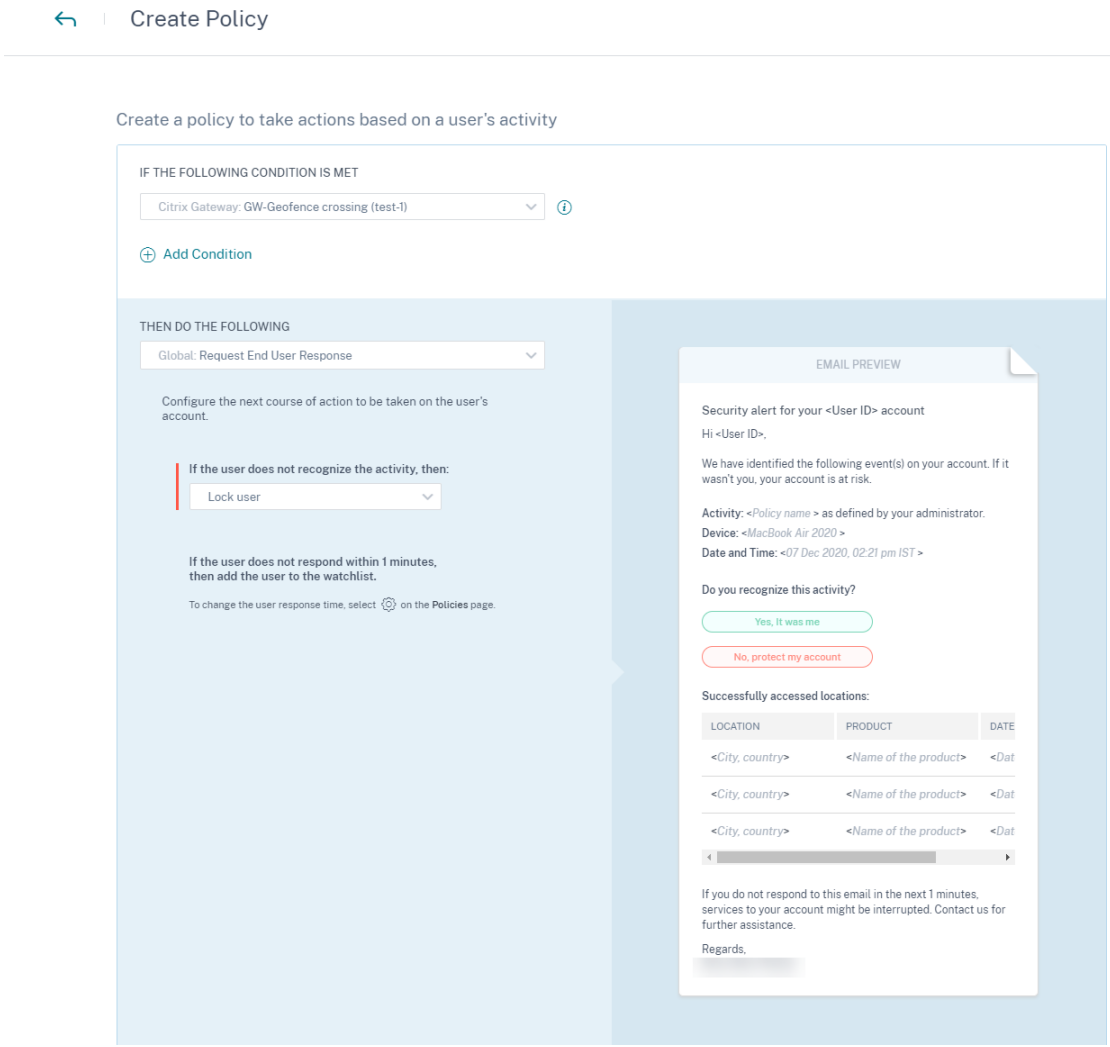
您还可以使用这些预先配置的自定义风险指标创建自己的策略，并在触发指标时应用诸如锁定用户或注销用户之类的操作。有关如何创建策略的信息，请参阅 配置策略和操作。

以下示例显示了锁定尝试从美国境外访问 Citrix 服务的用户的策略。如果用户无法识别其访问事件，则用户访问权限将被锁定。

条件：GW-Geofence 穿越

操作：请求最终用户回复

下一步操作：如果用户无法识别事件，则锁定用户



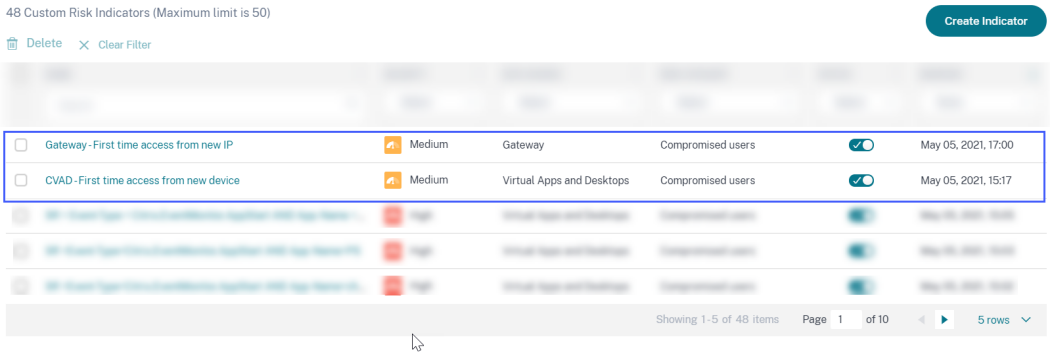
> 注意
>
> “请求最终用户响应”操作仅在美国区域受支持。因此，如果您的组织已加入欧盟地区，请选择您选择的其他操作，而不是“请求最终用户响应”操作。

首次访问场景预先配置的自定义风险指示器

使用以下自定义风险指标来检测首次访问场景的用户事件：

- CVAD-首次从新设备访问
- 网关-从新 IP 首次访问

默认情况下，这些预配置的自定义风险指示器处于启用状态。如果要禁用它们，请使用 **STATUS** 按钮。



下表描述了首次访问时预先配置的自定义风险指标。

自定义指标名称	场景	预配置的条件	数据源	风险类别
CVAD-首次从新设备访问	当 Citrix Workspace 应用程序用户从以下选项之一登录时： 一款新设备 过去 90 天未使用的现有设备。	默认情况下，启用以下条件： 第一次使用新的设备 ID。 `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")`	本地 Citrix Virtual Apps and Desktops 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）	受影响的用户

自定义指标名称	场景	预配置的条件	数据源	风险类别
网关-从新 IP 首次访问	NetScaler Gateway 用户成功从以下其中一项签名时： 新的公有 IP 地址 过去 90 天未使用的现有公有 IP 地址。	默认情况下，启用以下条件： 第一次使用新的 Client-IP `Event-Type = " Authentication "AND Status-Code = " Successful login"AND Client-IP-Type != " private"AND Access-Insight-Flags = 1`	Citrix Gateway	受影响的用户

在条件栏上，除了预配置的条件之外，您还可以添加自己的条件，以便根据自己的要求识别威胁。

例如，如果要识别来自特定国家/地区的用户事件，可以添加国家/地区维度以及预配置的条件：

- `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”`

最终用户电子邮件设

December 7, 2023

最终用户电子邮件设置控制与全局操作 请求最终用户响应关联的电子邮件模板。您可以应用此操作来获得用户对在其帐户中检测到的任何异常活动的响应。用户通过从 Citrix Analytics for Security 收到的电子邮件进行回复。

您可以使用电子邮件设置来：

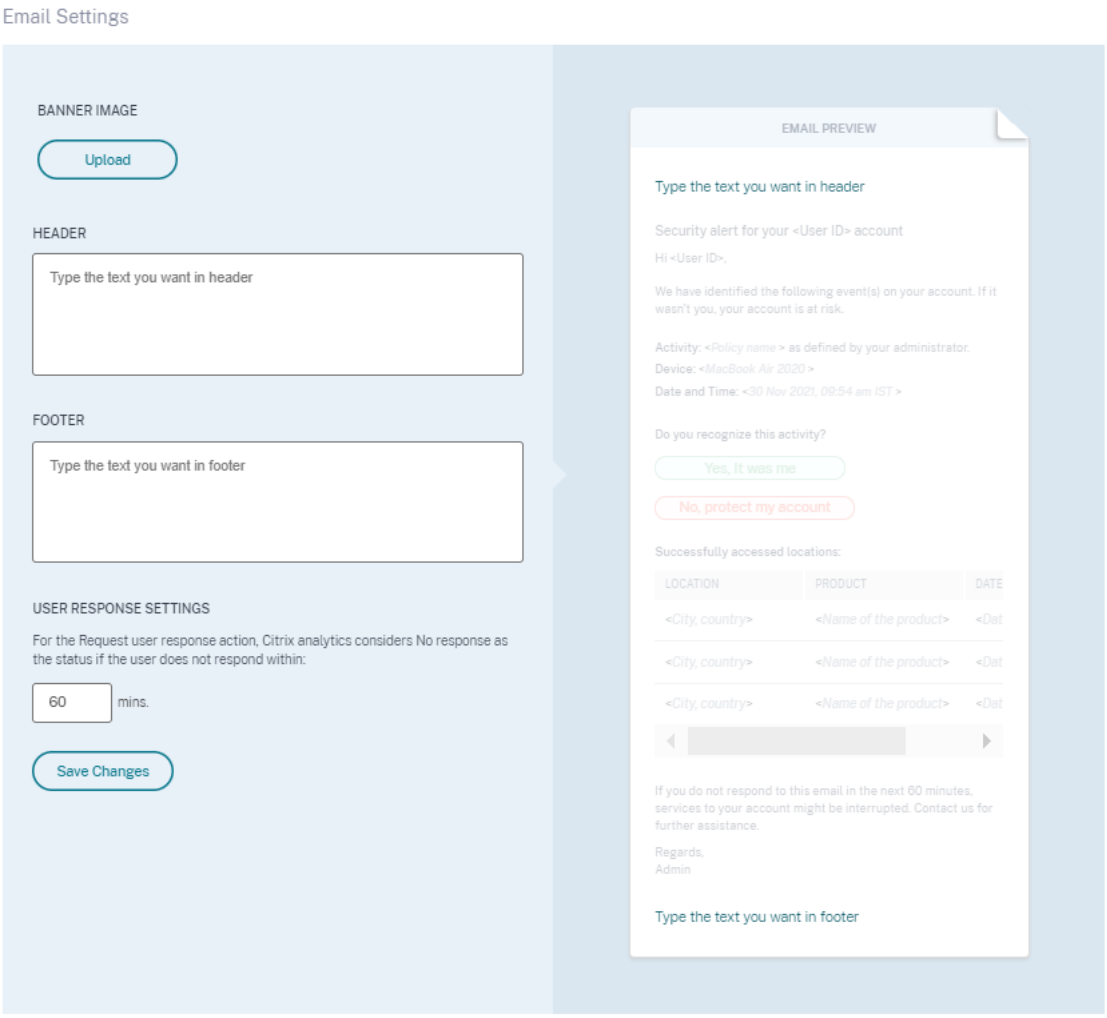
- 添加适当的横幅、标题文本和页脚文本以吸引用户的注意力并获得他们的回复。这也使您的电子邮件看起来更合法。
- 添加用户必须回复电子邮件的持续时间（以分钟为单位）。如果用户未在响应时间内做出响应，Citrix Analytics 将对用户应用指定的操作。

修改邮件设置

要修改电子邮件设置：

1. 在顶部栏上，单击 设置 **>** 警报设置 **>** 最终用户电子邮件设置。

2. 点击编辑上传或浏览横幅图片。上传图片文件时，请确保图片符合以下要求：
    - 支持的格式：JPEG 或 PNG
    - 最大尺寸：400* 100 像素
    - 最大文件大小：5 MB
3. 在页 眉 和 页脚 字段中输入您的文本。这些字段是可选的。
4. 在用户响应设置中输入时间。
5. 预览电子邮件，然后单击 保存更改。



管理员电子邮件设置

December 7, 2023

管理员电子邮件设置 页面允许您为系统警报配置自定义分发列表收件人。这可确保管理员收到对他们有用的系统警报。

管理员电子邮件设置 功能提供以下功能：

查看系统警报、接收警报的电子邮件分发列表、上次修改警报设置的用户以及上次修改警报的日期。
修改警报设置。更改各种系统警报的目标分发列表。

修改警报设置

要修改警报设置，请执行以下操作：

1. 在顶部栏上，单击“设置” > “警报设置” > “管理员电子邮件设置”。

2. 单击您要修改其电子邮件分发列表的警报。
3. 从“选择 电子邮件分发列表”下拉列表中选择必须接收警报的通讯 组列表。
   您也可以通过单击“创建 电子邮件通讯组列表”来创建自己的通讯组列表。有关更多信息，请参阅 创建电子邮件分发名单。
4. 单击保存更改。

监视名单

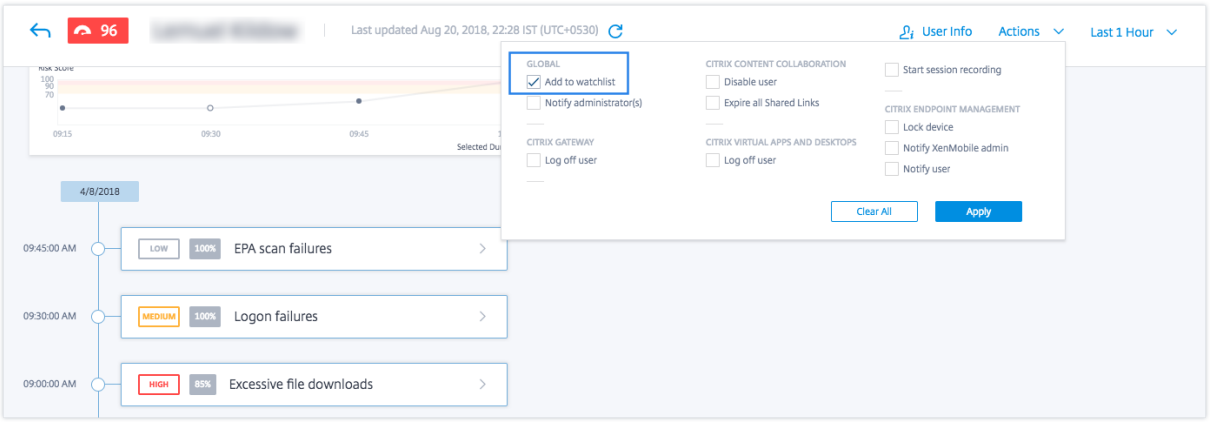
February 14, 2023

使用监视名单监视特定用户的活动，以防潜在威胁。例如，您可以监控组织中非全职员工的用户或经常触发特定风险指标的用户。

如何将用户添加到监视名单

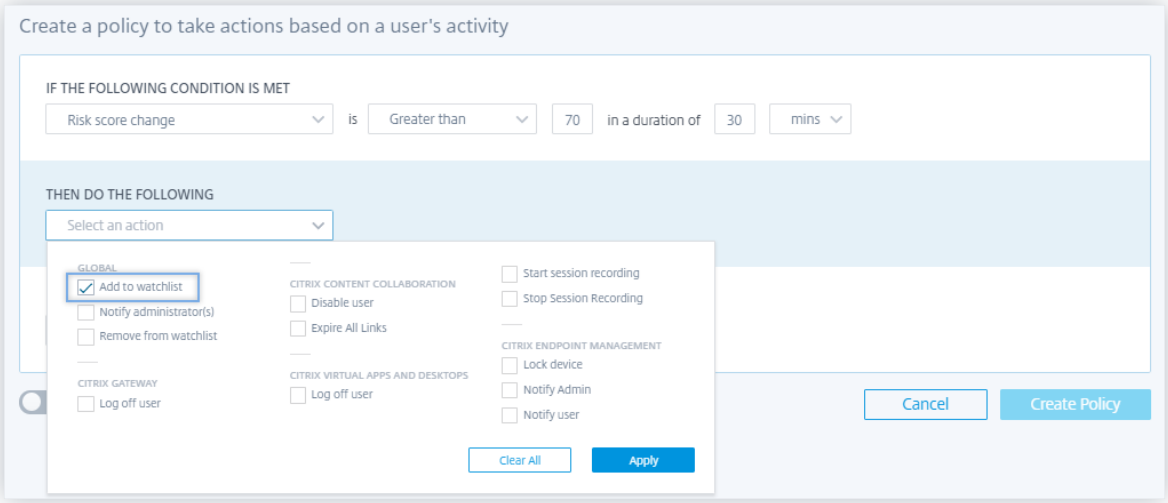
您可以手动将用户添加到监视名单，也可以定义在触发时将用户添加到监视名单的策略。

要手动将用户添加到监视名单，请在风险时间表上导航到该用户的个人资料。然后，从“操作”菜单中选择“添加到监视名单”。单击“应用”，然后按照提示强制执行该操作。



要使用策略将用户添加到监视名单，请创建一个包含一组必须满足的条件的策略。选择“添加到监视名单”操作。满足条件后，用户将被添加到监视名单中。例如，如果用户在 30 分钟内风险评分变化大于 70，则可能需要将该用户添加到监视名单中。

有关创建策略的更多信息，请参阅 配置策略和操作。

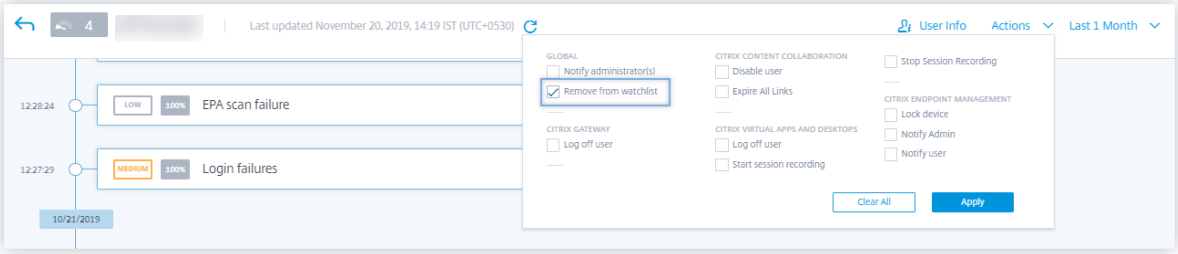


如何从监视名单中删除用户

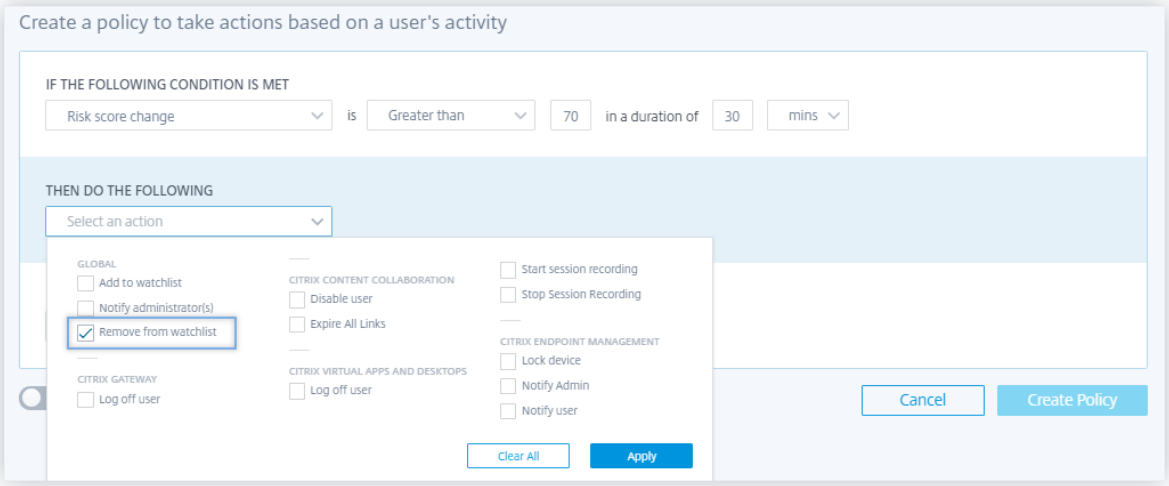
您可以手动将用户从监视名单中删除，也可以定义在触发时将用户从监视名单中移除的策略。

要手动从监视名单中删除用户，请在风险时间表上导航到该用户的个人资料。然后，从“操作”菜单中选择“从监视名单中删除”。单击“应用”，然后按照提示强制执行该操作。

> 注意
>
> 当用户在监视名单中并且您想要将其移除时，您会在“操作”菜单中看到“从监视名单中删除”选项。



要使用策略将用户移至监视名单，请创建一个包含一组必须满足的条件的策略。选择“从监视名单中删除”操作。满足条件后，用户将从监视名单中删除。例如，如果用户在 60 分钟内的风险评分变化小于 70，则您可能需要将该用户从监视名单中删除。要了解有关创建策略的更多信息，请参阅配置策略和操作。



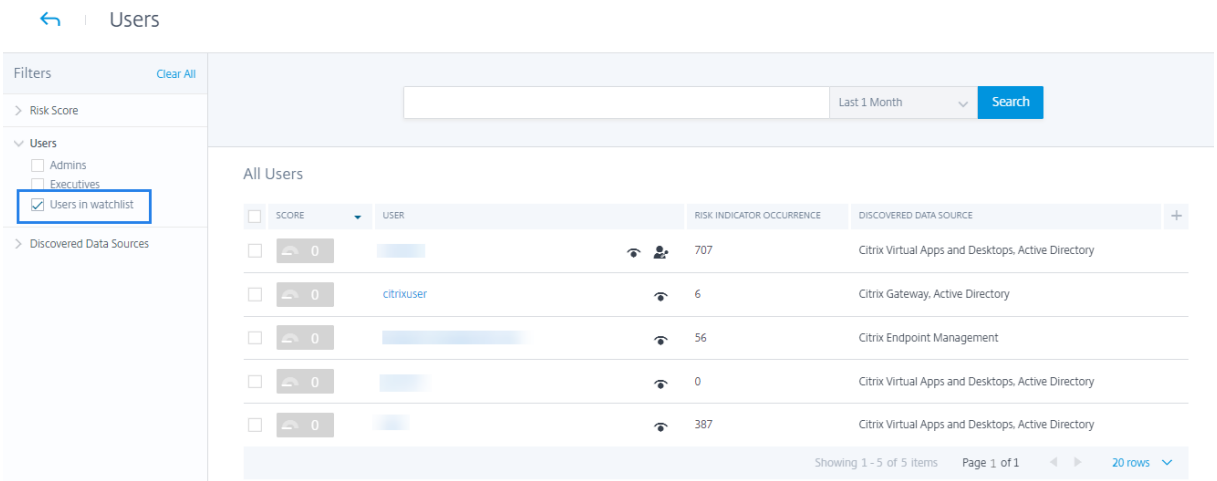
如何监控监视名单中的用户

在“安全”>“用户”控制板上，查看以下内容：

- 过去 13 个月监视名单中的用户数量摘要。单击该框可在“监视名单中的用户”窗格中查看监 视列表中所有用户的列表。
- 根据风险评分列出的监视名单中排名前五的用户。在“监视名单中的用户”窗格中，查看风险评分和风险指示器出现次数以及用户名称。单击“查看更多”可查看“用户”页面上监视名单中所有 用户的 列表。
- 监视名单中风险最高的用户。在风险用户窗格中，用户旁边的“眼睛”图标表示该用户在监视名单中。

在 用户 页面上，查看监视名单中所有用户的列表。查看用户的风险分数、触发的风险指标数量和关联数据源等详细信息。

使用搜索框查找用户及其活动详细信息。选择时间段以查看特定时段的风险指示器出现次数。



每周电子邮件通知

December 7, 2023

Citrix Analytics 每周发送电子邮件通知，总结贵组织的 IT 基础架构中存在的安全风险暴露情况。每周通知可让您了解和了解风险事件及其在前一周发生的情况。您可以在不登录 Citrix Analytics 的情况下了解是否有任何事件需要您关注或采取操作。这些信息可让您随时了解您的 IT 安全领域中正在发生的事情。

启用电子邮件通知

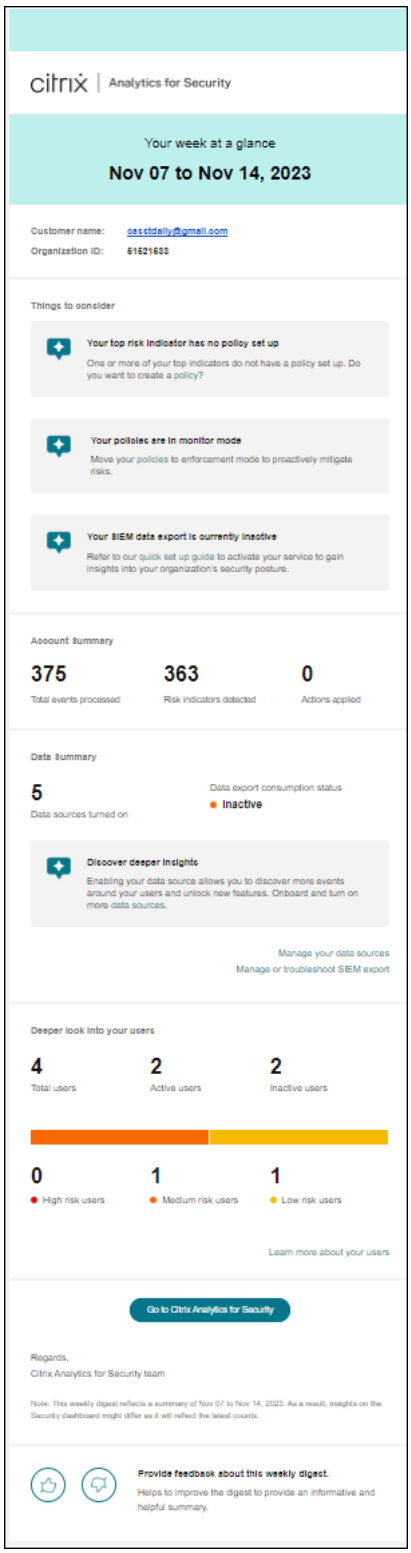
- 如果您是具有完全或自定义访问权限的 Citrix Cloud 管理员，则默认情况下，您的 Citrix Cloud 帐户中的电子邮件通知处于禁用状态。要接收来自任何 Citrix Cloud 服务（例如 Citrix Analytics）的电子邮件通知，请在 Citrix Cloud 中启用通知选项。有关详细信息，请参阅 接收电子邮件通知。通知首选项不适用于通过 Active Directory/Azure AD 组添加的管理员。
- 默认情况下，电子邮件通知会发送到 Citrix 安全管理员-默认列表。您可以通过为每周警报配置自定义通讯组列表收件人来更改此设置。有关更多信息，请参阅 管理员电子邮件设置。

您什么时候会收到来自 **Citrix Analytics** 的电子邮件

每周二，Citrix Cloud 都会向您发送一封电子邮件通知 donotreplynotifications@citrix.com。

电子邮件通知提供以下信息：

- 已处理的事件总数、检测到的风险指示器和应用的操作的摘要
- 活跃数据源总数和数据导出消耗状态摘要
- 前三大风险指示器
- 对风险指示器采取的主要三项行动
- 活跃用户总数和风险用户总数
- 任何需要您注意的事件或行为

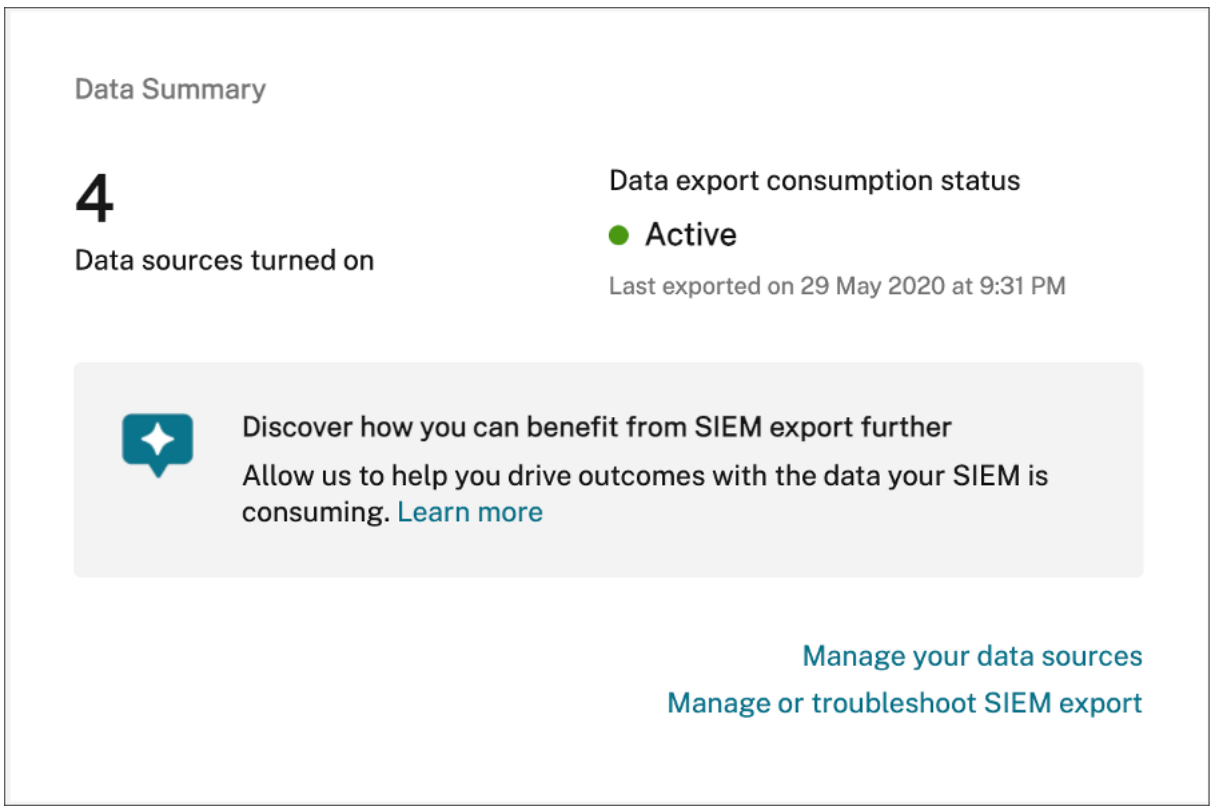


帐户摘要

每周电子邮件概述了已处理的事件总数、检测到的风险指示器和应用的操作。

数据摘要

每周电子邮件还提供有关已开启的数据源以及数据导出消耗状态的见解。



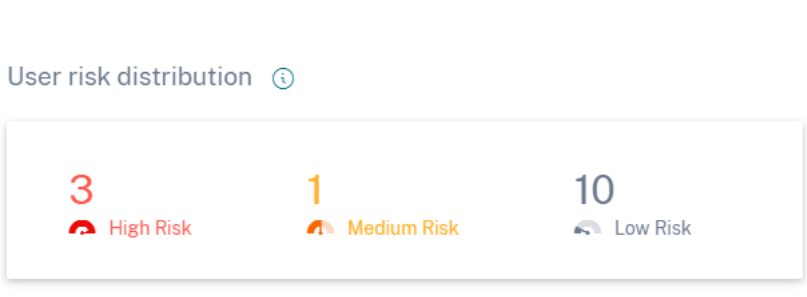
在电子邮件中单击“管理您的数据源”以查看 Citrix Analytics 中的“数据源”页面。您可以载入数据源并开启数据处理，以使 Citrix Analytics 能够处理数据。有关启用分析的更多信息，请参阅对数据源启用分析。

单击“管理 **SIEM** 导出”或“排除 **SIEM** 导出故障”，查看 Citrix Analytics 中的“数据导出”页面，对环境进行故障排除并管理数据导出设置。

用户信息

每周一封电子邮件提供对以冒险方式行事的用户和用户总数的见解。

- 高风险用户数量 -以红色标识。它们对该组织构成直接威胁。
- 中等风险数量—以橙色标识。在选定的一周内，他们的帐户有多起严重违规行为，必须对其进行密切监视。
- 低风险用户数量 -以黄色标识。他们的账户上有一些严重的违规行为，但可能不被视为威胁。

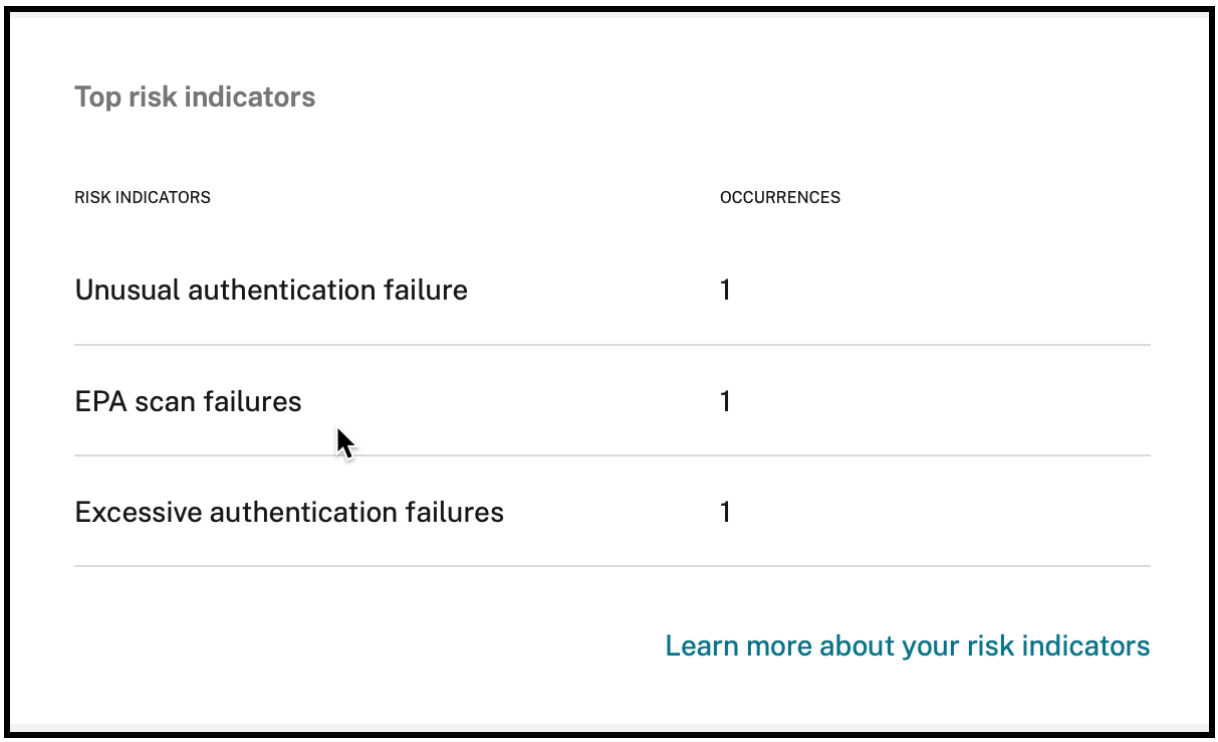


有关更多信息，请参阅风险用户。

单击“了解有关您的用户的更多信息”，查看 Citrix Analytics 中的“风险用户”页面。您可以更深入地了解活跃用户和风险分类。

主要风险指示器

每周电子邮件提供有关前三个风险指示器和所选周发生次数的见解。根据发生次数，将显示所选周的默认和自定义风险指示器。

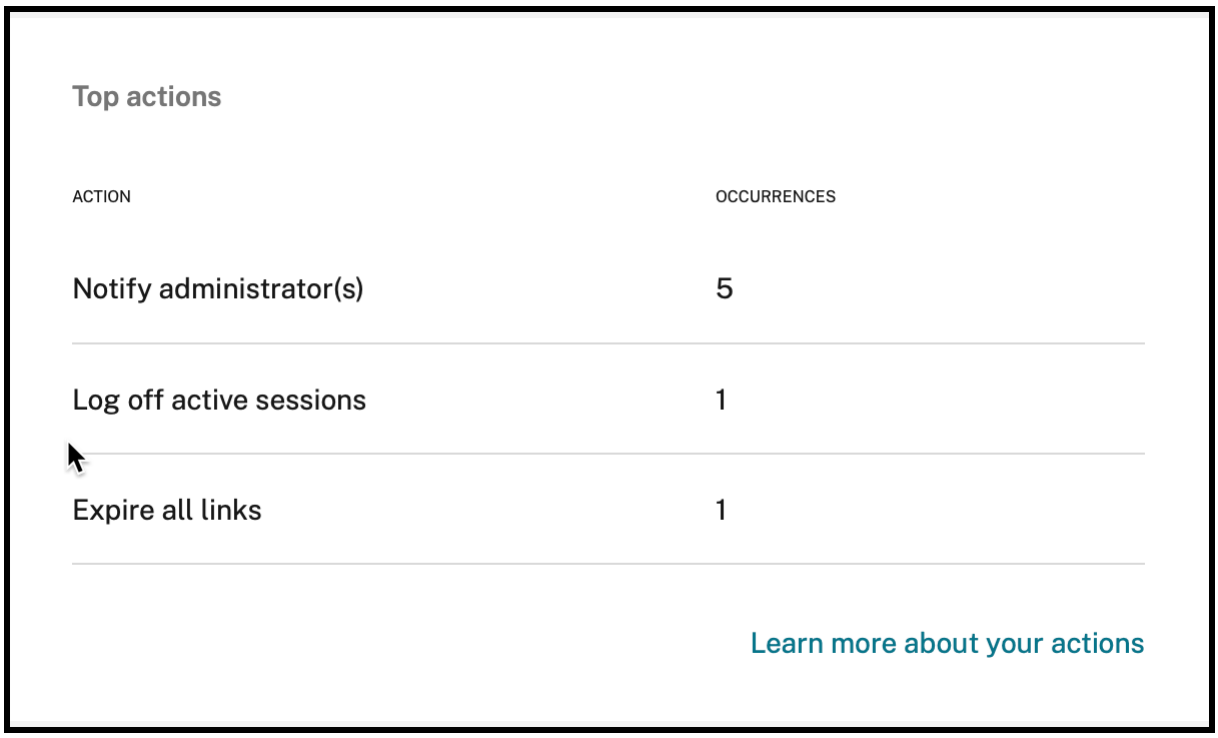


有关更多信息，请参阅风险指示器。

在电子邮件中单击“了解有关您的风险指示器的更多信息”以查看 Citrix Analytics 中的“风险指示器概述”页面。

热门动作

每周电子邮件提供了有关为应对上周发生的可疑和异常威胁而采取的前三项行动的见解。根据出现次数，将显示所选周的全局操作和 NetScaler Gateway 操作。



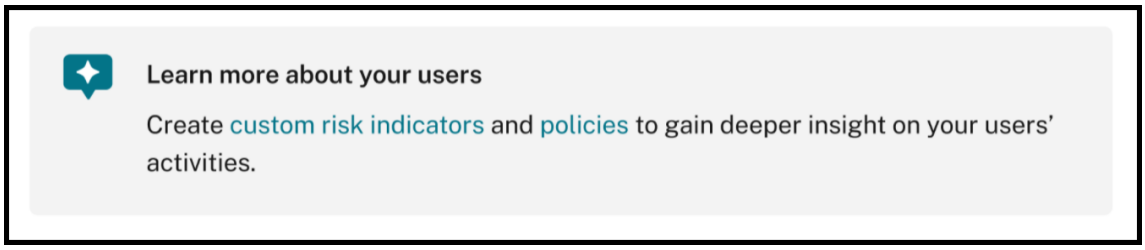
有关操作和配置操作的更多信息，请参阅策略和操作。

单击“了解有关您在电子邮件上的操作的更多信息”以查看 Citrix Analytics 中的“热门操作”页面。

收到电子邮件后您需要采取什么行动

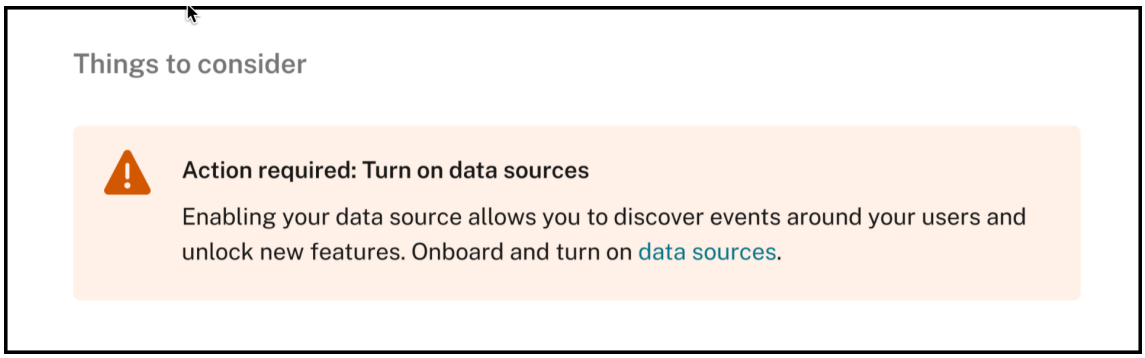
每周发送电子邮件使您能够了解是否有任何事件或行为需要您关注。

- 如果本周未检测到风险指示器，您将收到以下消息，提示您创建更多自定义风险指示器。

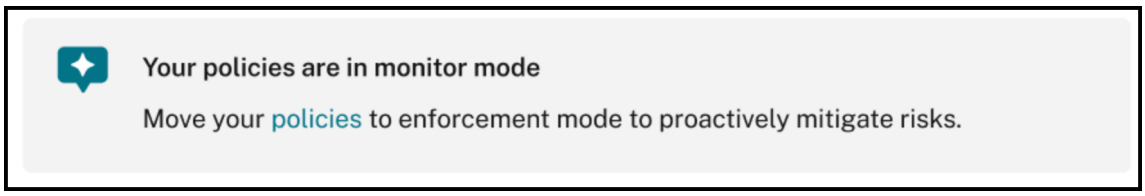


你可以登录 Citrix Analytics 来创建更多自定义风险指标。

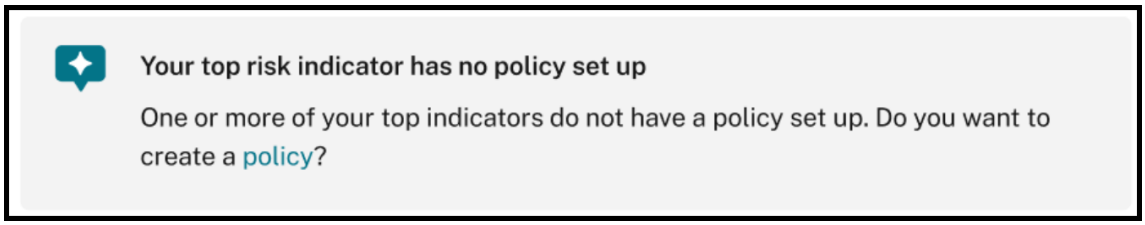
- 如果 Security Analytics 中没有开启任何数据源，您将收到以下消息，提示您开启数据源的数据处理。



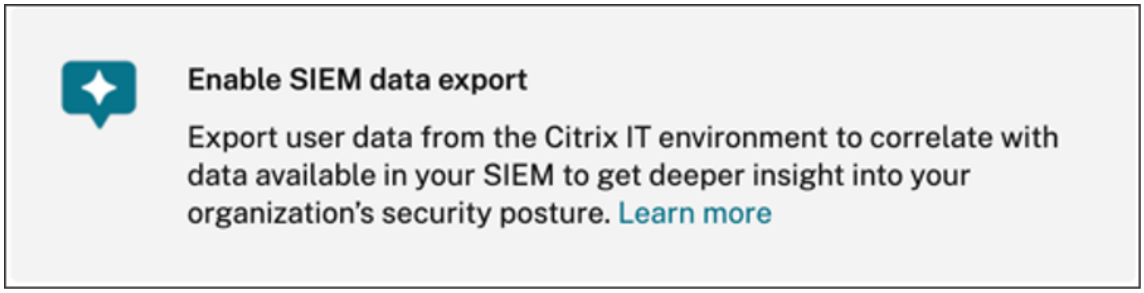
- 如果没有任何策略处于监控模式，则会收到以下消息，提示您将策略移至强制模式。



- 如果没有为本周前 3 个风险指示器中的任何一个设置策略，您将收到以下消息，提示您创建策略。



- 如果您尚未为 Citrix Analytics 租户启用 数据导 出，则以下建议将为您提供有关数据导出选项的更多详细信息，这些选项允许您将 Citrix 数据导 出到 SIEM 环境。



- 如果数据导出使用状态处于非活动状态，则会收到以下消息，提示您激活服务。

> 注意
>
> 仅当至少为一个数据源开启数据处理时，才会启用数据传输。如果所有数据源的数据处理均已关闭，则会收到以下警告消息，提示您启用数据源。

审核日志

June 23, 2021

审计日志描述了 Citrix Analytics 上生成的事件的审计信息。它们可以是错误之类的系统事件，也可以是 Citrix Analytics 管理员执行的配置操作的审计跟踪。

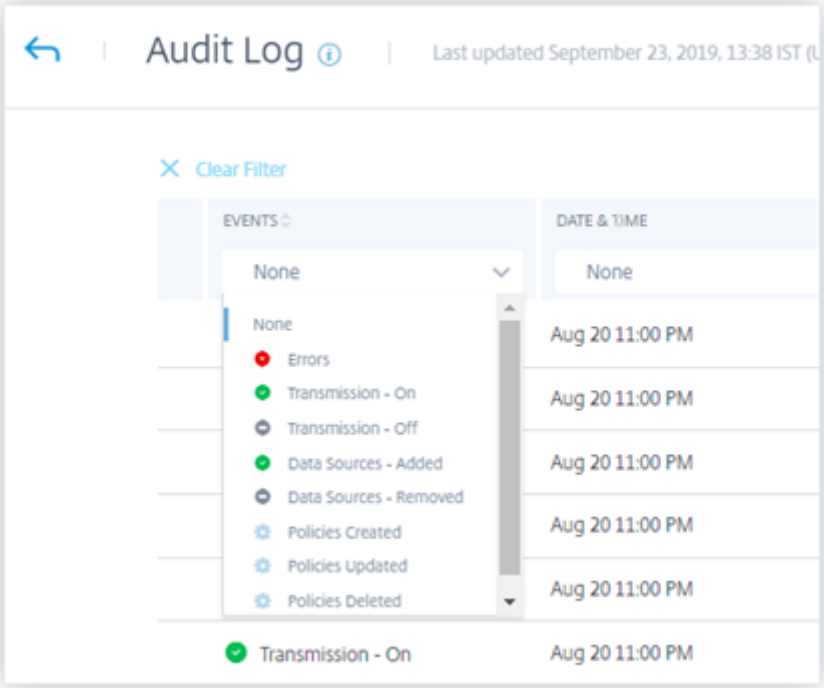
无论何时添加、删除或更新配置，事件信息都会写入审核日志。此信息是关于修改的内容、修改的时间以及谁修改的信息。

您可以查看过去三个月的审核日志信息。

生成审计事件的活动

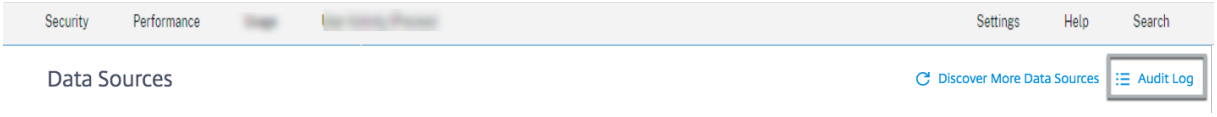
Citrix Analytics 上注册了以下事件：

- 生成的错误
- 传输已打开
- 变速器已关闭
- 已添加数据源
- 已删除数据源
- 已创建策略
- 更新策略
- 已删除策略



如何查看审核日志

要查看审核日志，请登录 Citrix Analytics。导航到设置 **>** 数据源。在数据源页上，单击右上角的审核日志。



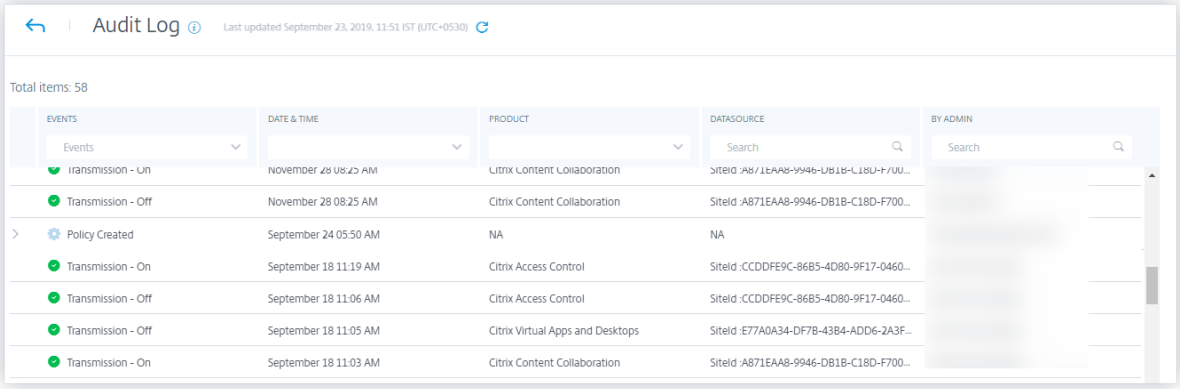
如何使用审核日志

您可以使用审核日志来查看并了解 Citrix Analytics 上的任何事件。刷新审核日志页面以获取最新的审核数据。该页面显示上次更新审计数据的日期和时间。

您可以在审核日志页面上查看以下审核信息。您还可以根据这些字段筛选审计数据。

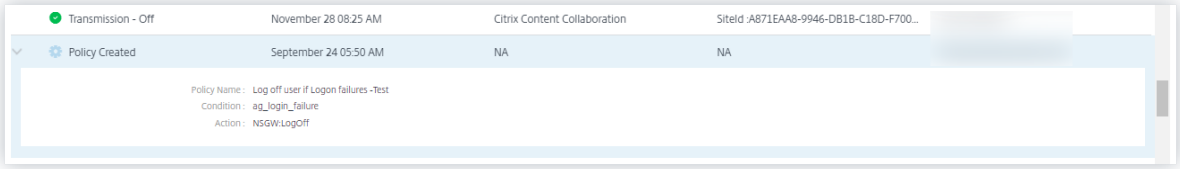
- 事件。事件可以由系统生成，也可以由管理员在 Citrix Analytics 上应用配置。事件还可以表示错误，例如未能应用操作或数据源。默认情况下，将显示所有事件的日志。您可以根据要查看的事件类型进行筛选。
- 日期和时间。事件发生的数据和时间。您可以根据要查看日志的时间段进行筛选。您可以查看当天、过去 7 天、过去 15 天、上月和过去三个月的事件。
- 产品。为其生成事件的产品。这些事件在产品上生成，并在显示它们的 Citrix Analytics 上进行汇总。您可以根据一个或多个产品筛选日志。
- 数据源。与审计条目关联的产品实例的名称。您可以搜索任何特定的数据源以查看其审计数据。

- 由管理员。执行管理员活动的 Citrix Analytics 管理员。您可以搜索任何特定管理员执行的活动。



如果您的注册活动基于策略，则可以单击箭头图标查看更多详细信息，例如：

- 策略名称
- 指定的条件
- 由此产生的操作



自定义报告

June 18, 2024

您可以使用 Citrix Analytics for Security 中提供的事件和见解来创建和计划定制报告。自定义报告可帮助您提取特定感兴趣的信息并以图形方式组织数据。它有助于分析您选择的数据源在一段时间内的安全性。

自定义报告支持以下数据源：

- Citrix Cloud Labs 应用程序和桌面
- 网关
- Secure Private Access
- Secure Browser
- 策略
- 风险指示器
- 风险分数

自定义报告中支持的字段

一些数据源也可以在自助搜索中找到。要查看这些事件类型和支持的字段，请单击以下数据源。

- Citrix Cloud Labs 应用程序和桌面
- 网关
- Secure Private Access
- Secure Browser
- 策略

以下数据源仅在自定义报告中可用。下表列出了自定义报告中支持以下数据源的字段：

- 风险指示器
- 风险分数

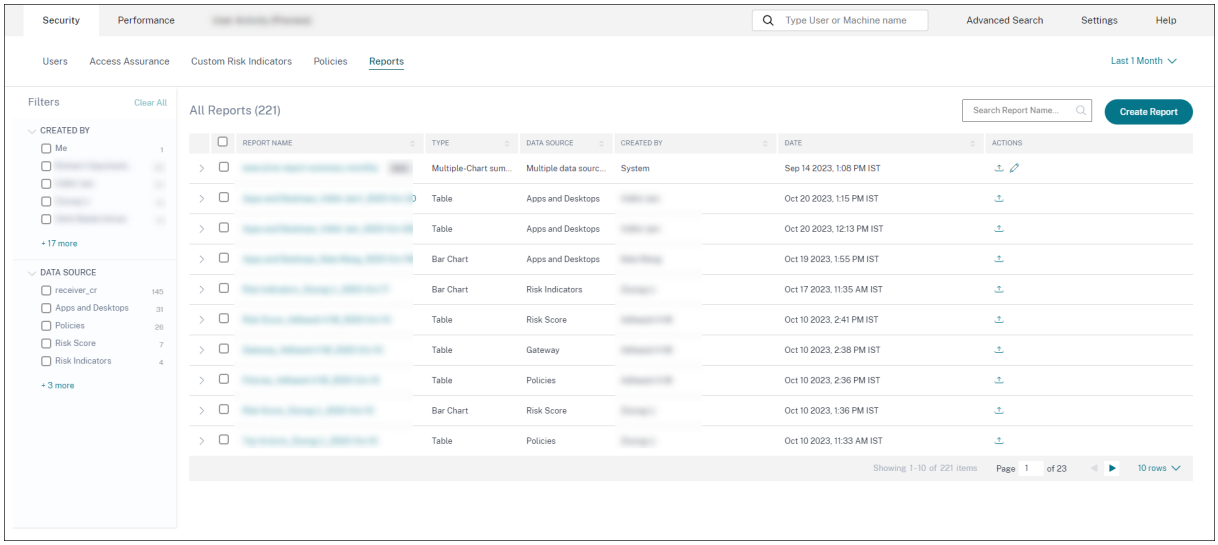
数据源	维度	说明
风险指示器	类别	表示风险指标的类别。风险指标分为四个类别之一——受感染的端点、受感染的用户、数据泄露或内部威胁。
	风险指标名称	风险指标的名称。对于自定义风险指标，名称由管理员在创建指标时定义。
	严重性	表示风险的严重程度。它可以是低、中或高。
	用户名称	用于登录的用户名或域\用户名。
风险分数	风险分数	分配给用户的风险分数。风险评分从 0 到 100 不等，具体取决于与用户活动相关的威胁严重程度。
	用户名称	用于登录的用户名或域\用户名。
	风险评分类别	根据风险评分，风险用户可能属于以下类别之一：高风险、中等风险和低风险。

报告

您可以使用此视图对报告执行以下操作：

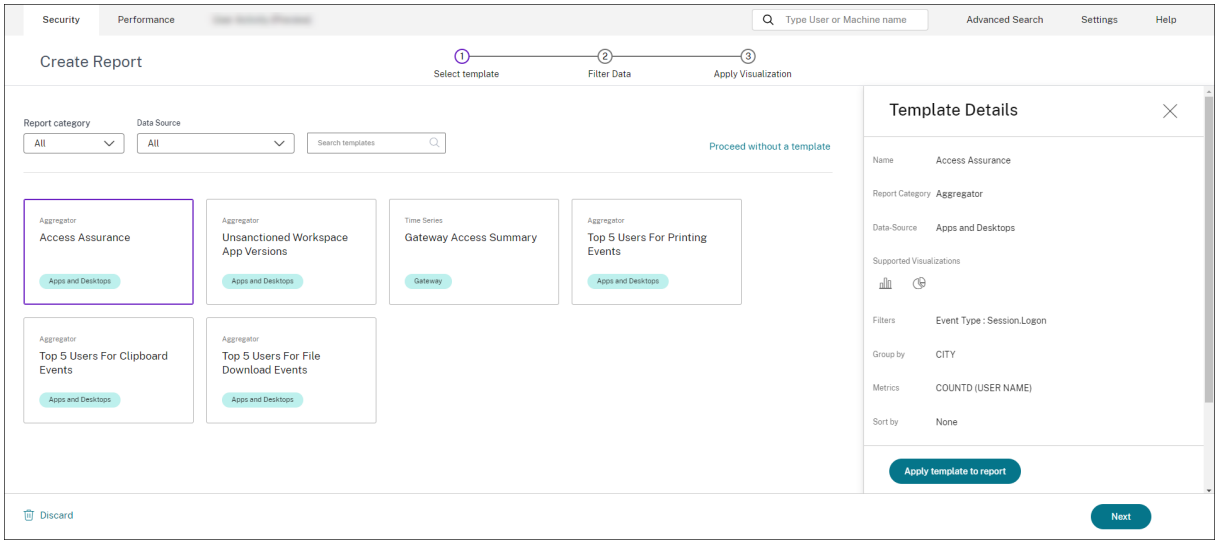
- 单击“创建报告”以创建自定义报告。
- 展开一行以查看现有自定义报告的预览。
- 单击报告名称可查看详细的报告可视化。
- 单击“导出”图标导出 PDF 格式的现有自定义报告。

- 单击“编辑”图标可编辑您创建的报告。
- 单击“删除”图标可删除您创建的报告。



创建自定义报告

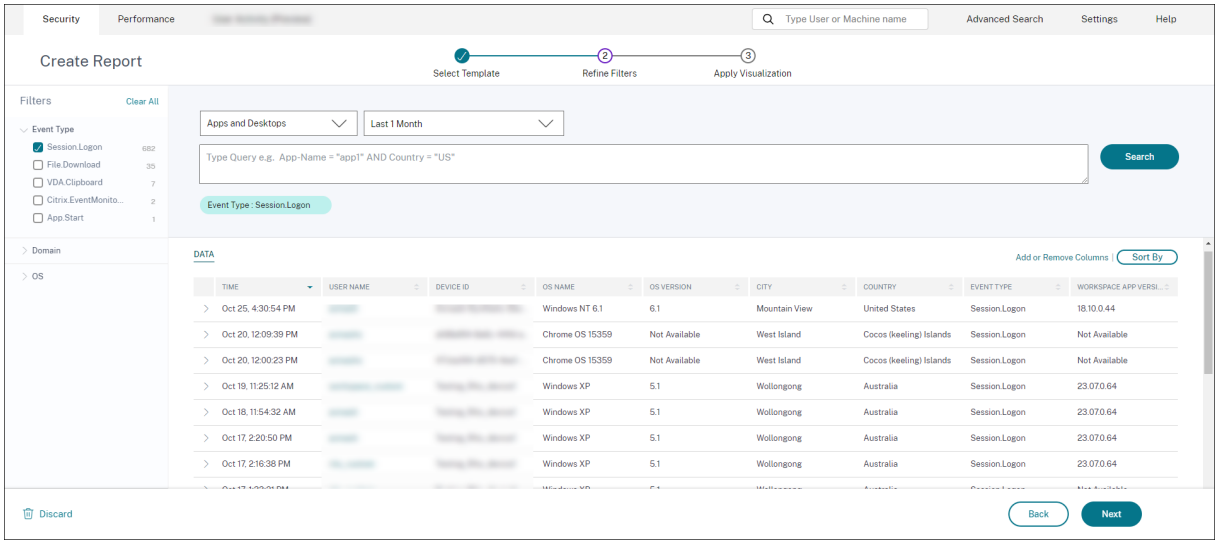
要创建自定义报告，请单击“创建报告”。在“创建报告”页面上，您可以选择创建带或不带模板的自定义报告。



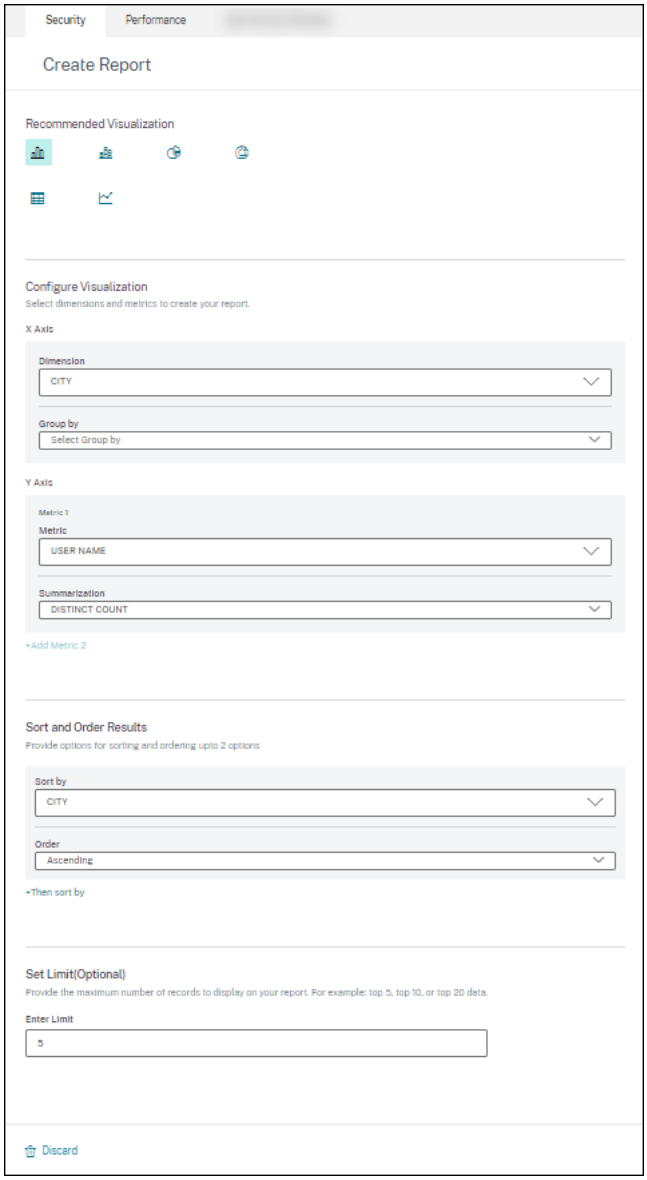
使用模板创建自定义报告

要使用模板创建自定义报告，请执行以下操作：

1. 选择模板：单击模板后，模板详细信息将在右侧列出。单击“将模板应用到报告”，使报告能够使用所选模板。
2. 细化筛选条件：“细化筛选器”页面显示为所选模板预定义的筛选器。进行所需的更改，然后单击“下一步”。



1. 应用可视化：选择一种可用的可视化效果来显示报告。



- 条形图：使用高度与值成比例的垂直矩形条来显示数据。用于比较事件。
- 堆叠柱状图：以条形图的形式呈现数据。用于可视化多个子类别的数据总和。
- 饼图：以饼状的形式显示数据。用于可视化数据或百分比的相对大小。
- 甜甜圈图：以甜甜圈的形式显示数据。用于可视化数据或百分比的相对大小。- 表：以表格的形式显示数据。用于根据需要对任意数量的维度进行可视化。
- 折线图：用直线段连接的点显示数据。用于可视化一段时间内的数据趋势。

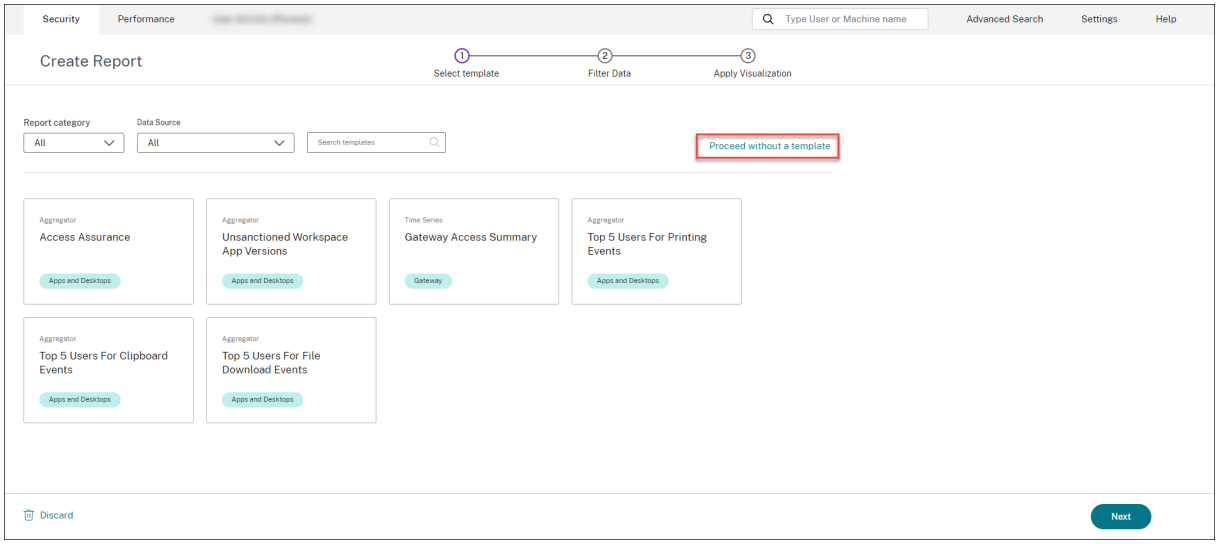
1. 现在使用以下参数配置可视化：

    - x 轴的尺寸
    - 要在 y 轴上绘制的指标
    - 要应用于指标的汇总或聚合，例如平均值或计数
    - 排序和订购选项

- 报告上显示的最大记录数的可选限制。

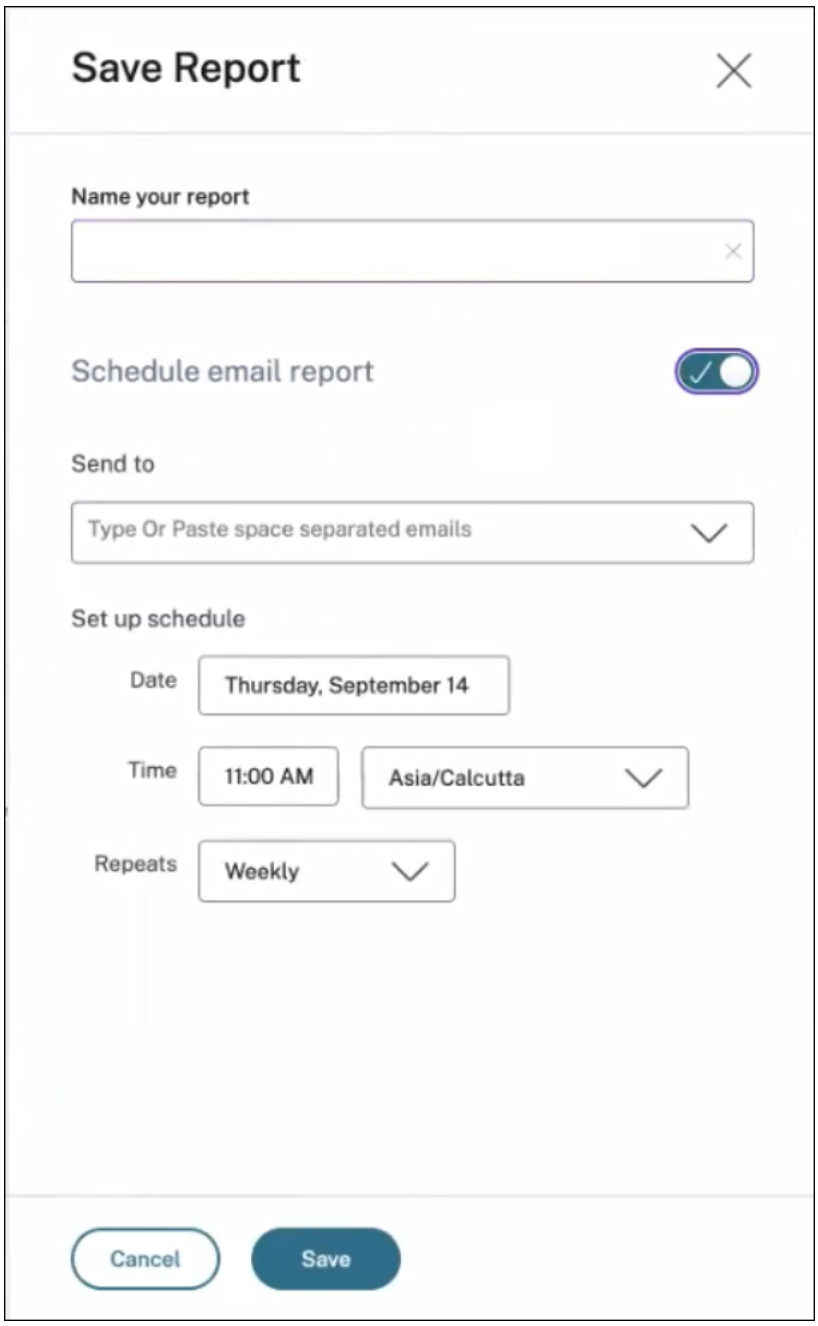
创建没有模板的自定义报告

您也可以在没有预定义模板的情况下创建自定义报告。单击“创建不带模板的自定义报告”。从下拉列表中选择一个数据源。按照步骤定义筛选器、应用可视化、保存和安排报告。



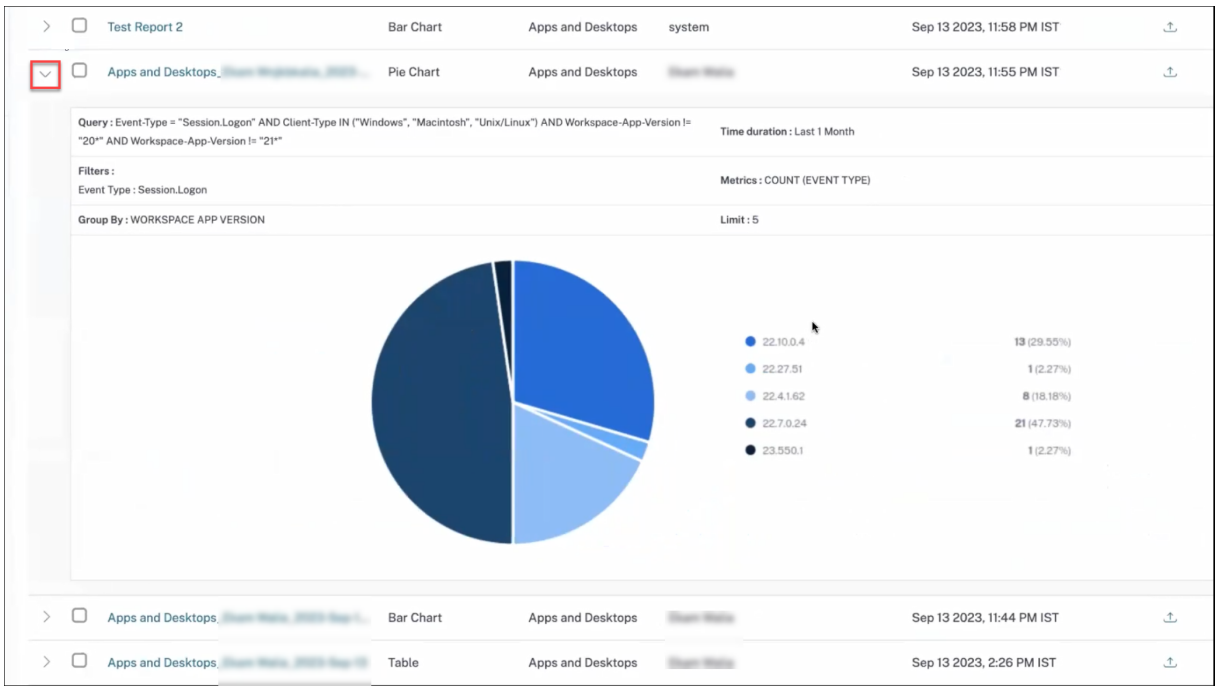
保存报告

1. 要保存报告，请单击“保存”。为报告指定标题。
2. 您可以安排在特定日期和时间或定期计划内通过电子邮件将报告发送到指定的电子邮件 ID 和通讯组列表。



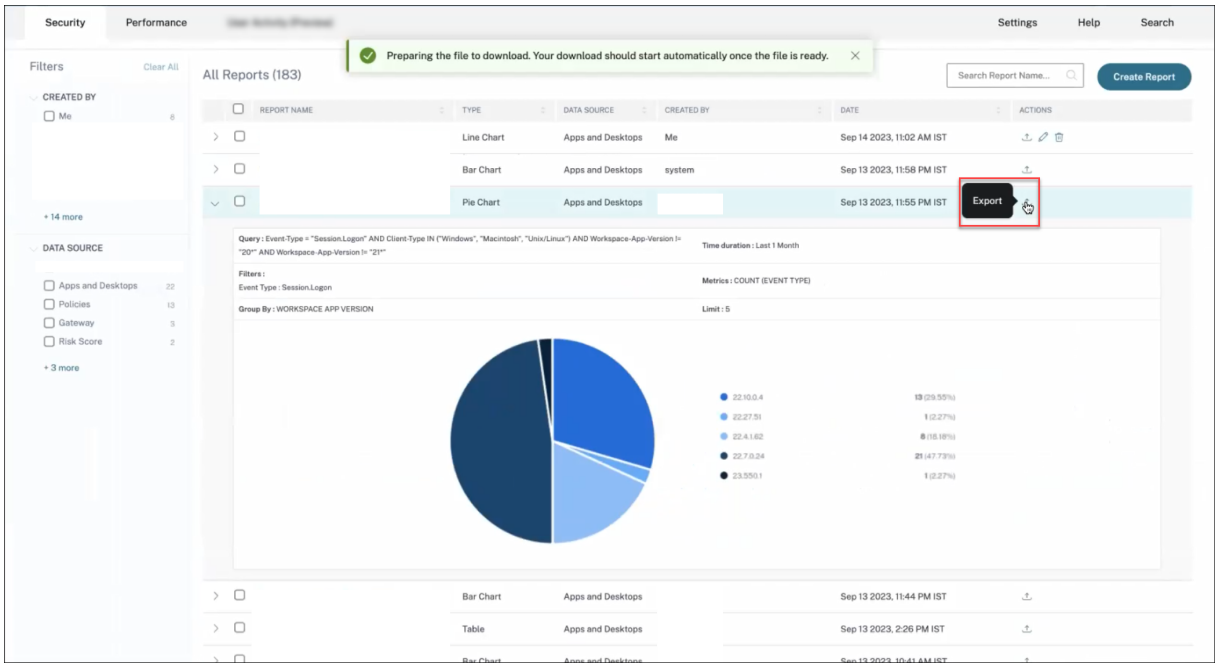
查看报告

1. 创建并保存报告后，可以在报告页面上查看该报告。您还可以修改或删除已保存的报告。
2. 单击下拉按钮预览报告。



导出报告

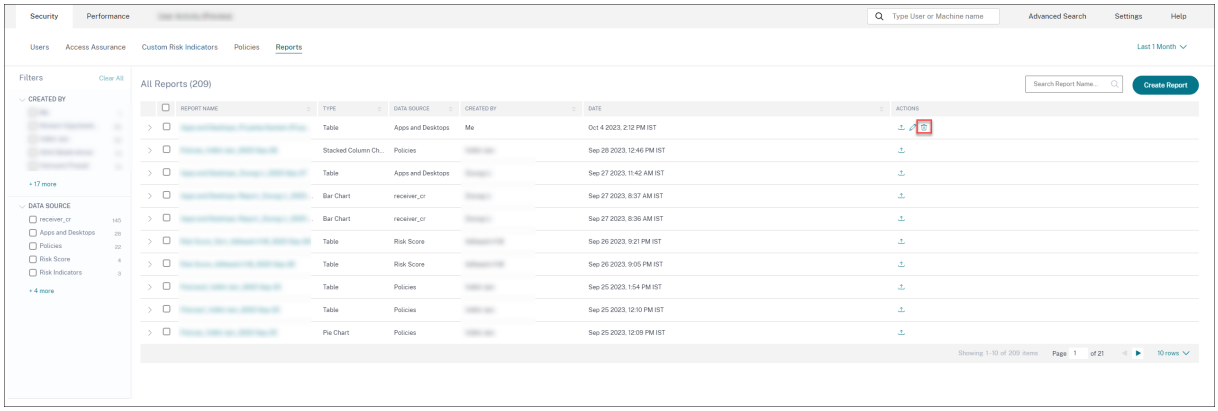
单击“导出”图标导出报告。



删除报告

单击“删除”图标删除报告。

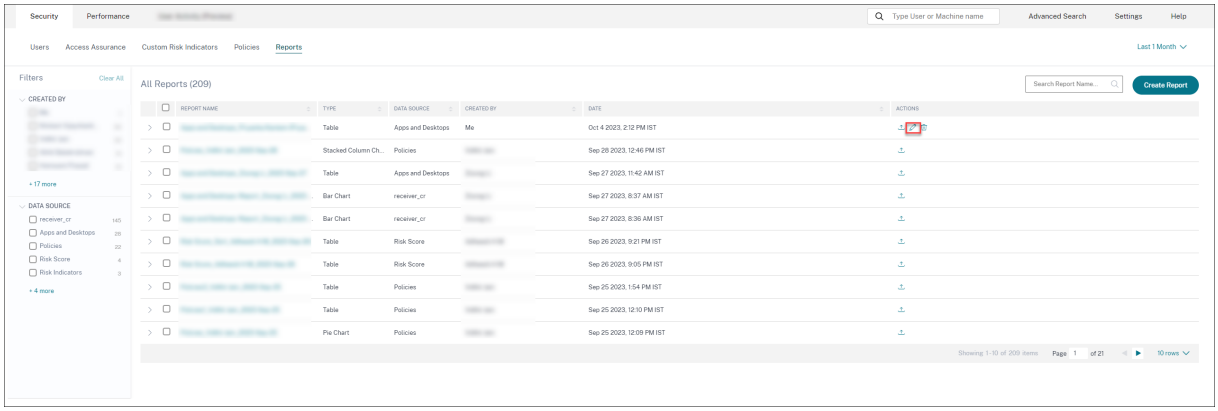
> 注意：
>
> 只有创建报告的用户才能将其删除。



编辑报告

单击“编辑”图标编辑报告。

> 注意：
>
> 只有创建报告的用户才能对其进行编辑。



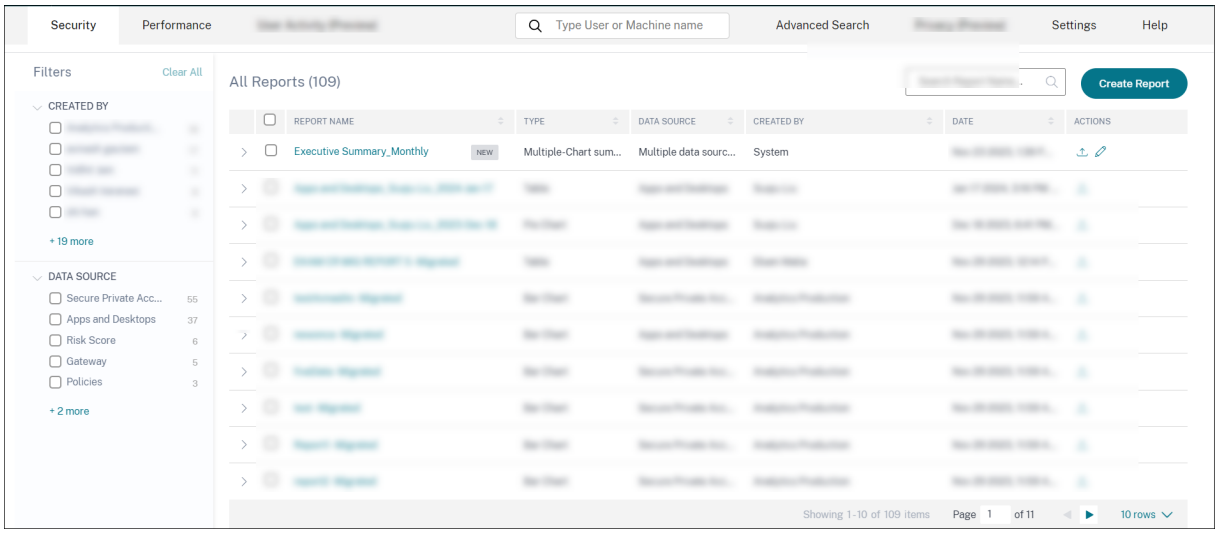
执行摘要报告

可以通过电子邮件安排自动导出，其中包含预先创建的执行摘要报告的 PDF。执行摘要报告是一系列报告，向您选择的受众一目了然地描述了企业在所选时间段内的安全状况。

可以为以下时间段的数据创建报告：

- 最近 1 小时
- 最近 12 小时

- 最近 1 天
- 最近 1 周
- 最近 1 个月



它包含哪些报告

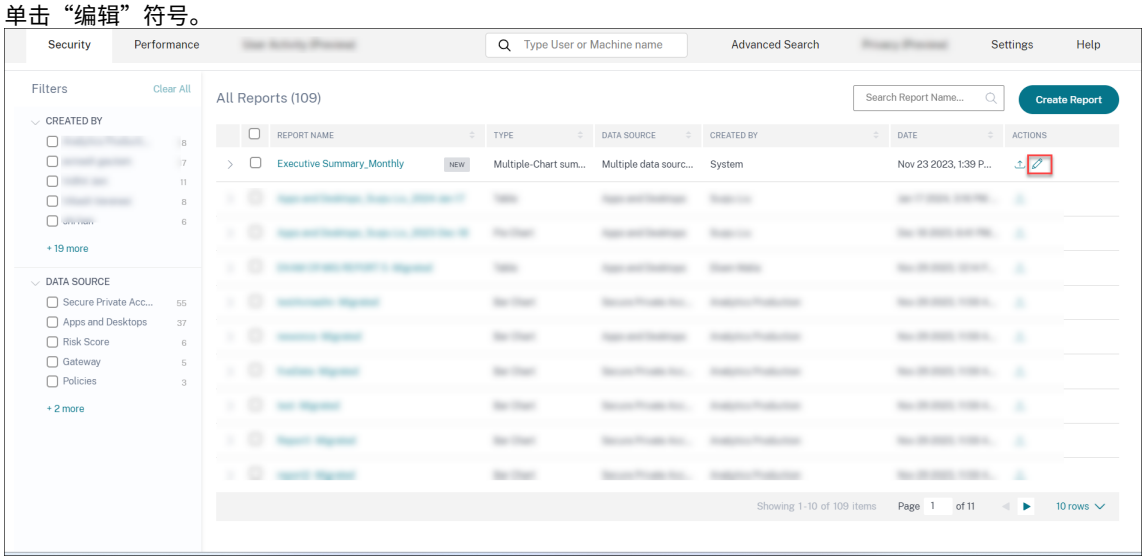
内容提要报告包含以下报告：

- 用户风险分布：基于所选时间段内最高计算风险分数的高、中和低风险分布。
- 最高风险用户：所有用户中风险最高的用户，按选定时间段内的最高风险分数排序。
- 按类别划分的风险发生次数：需要立即采取操作的风险类别提供的风险暴露类型和关键风险的全面视图。风险指标分为以下几类：
  - 受影响的用户
  - 受损的端点
  - 数据泄露
  - 内幕威胁
- 风险指标：选定时间段内用户触发的风险指标。
- 操作：对选定时间段内用户触发的风险指标的应用操作。
- 热门策略：在选定时间段内触发次数最多的前五个策略。
- 热门操作：在选定时间段内触发次数最多的前五个操作。
- 按严重性排序的风险指标：用户触发的默认和自定义风险指标，按严重性排序。
- 按总发生次数排序的风险指标：用户触发的默认和自定义风险指标，根据发生次数排序。

编辑执行报告

要编辑执行报告，请完成以下步骤：

1. 单击“编辑”符号。



2. 在“配置您的报告”窗格中，选择要查看数据的时长。

3. 单击下一步。将出现“保存报告”窗格。

> 注意：
>
> 要放弃更改，请单击“放弃更改”。

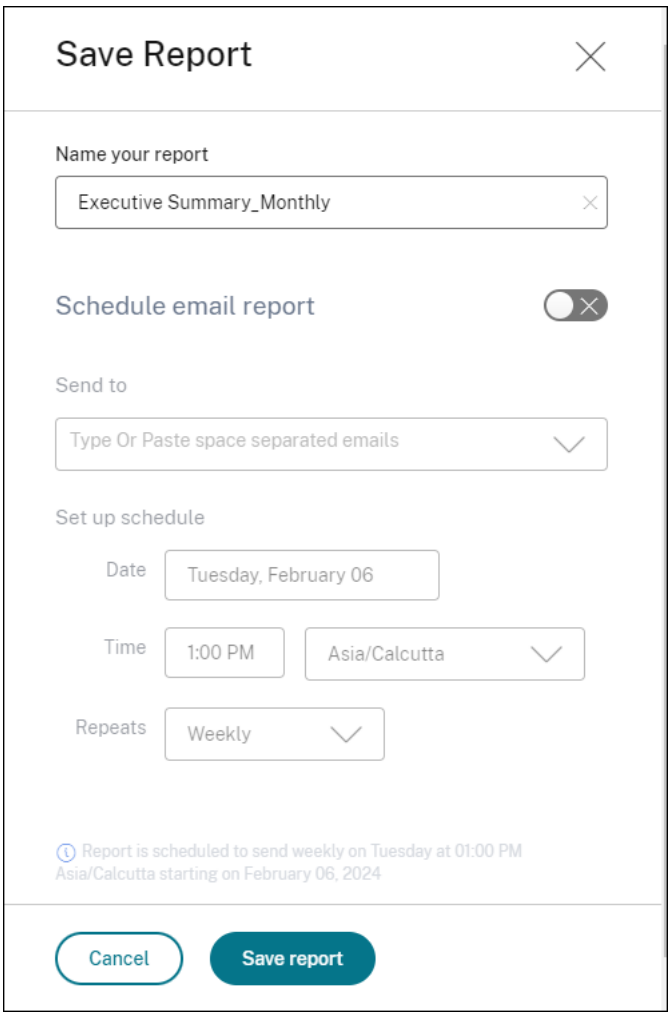
4. 在“保存报告”窗格中，输入以下详细信息：

   a) 为您的报告命名：执行报告的名称。

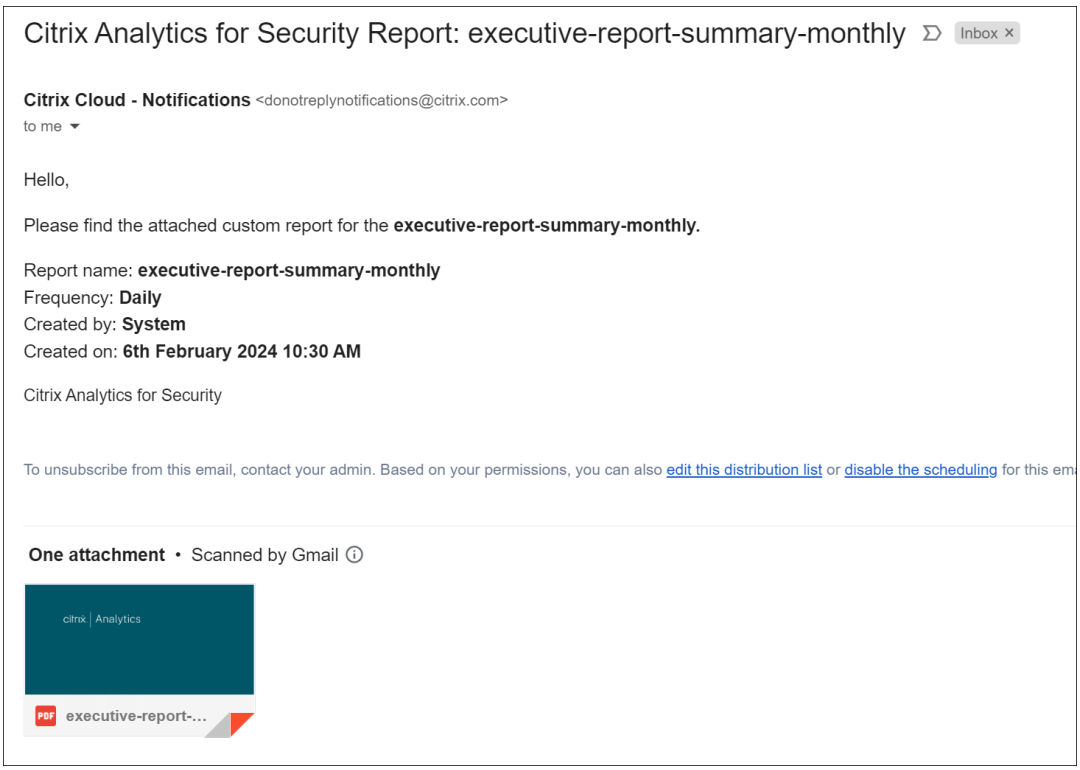
   b) 计划电子邮件报告：开启计划报告。默认情况下，该开关处于关闭状态。

   c) 发送至：从下拉列表中选择一个分发列表。您还可以添加分发列表和个人电子邮件地址的组合。要创建自定义的分发列表，请参阅管理员电子邮件设置。

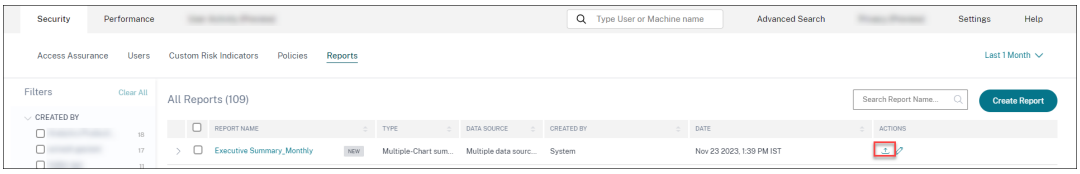
   d) 设置时间表：选择首次向选定受众发送报告的所需时间和重复发送报告的时间。



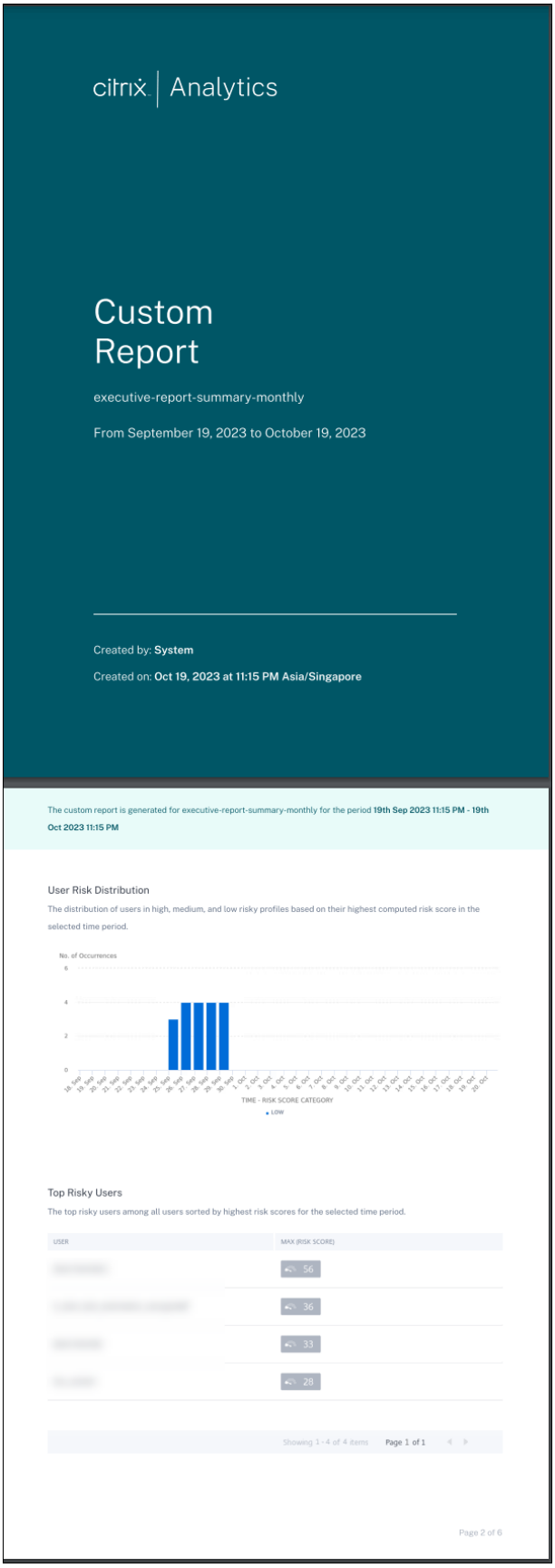
e) 单击“保存报告”。然后，该报告将以电子邮件形式发送给列出的收件人。



或者，您可以使用导出符号将执行报告导出为 PDF。



以下屏幕截图描述了示例 PDF 输出：



自助搜索

December 7, 2023

什么是自助搜索

自助搜索功能使您能够查找和筛选从数据源接收的用户事件。您可以探索底层用户事件及其属性。这些事件可帮助您识别任何数据问题并进行故障排除。搜索页面显示数据源的各个方面（维度）和量度。您可以定义搜索查询并应用筛选器来查看符合定义条件的事件。默认情况下，自助搜索页面显示最近一天的用户事件。

目前，自助搜索功能可用于以下数据源：

- Authentication
- Gateway
- Secure Browser
- Secure Private Access
- 应用程序和桌面
- 性能用户、计算机和会话

此外，您还可以对符合定义策略的事件执行自助搜索。有关详细信息，请参阅面向策略的自助搜索。

如何访问自助搜索

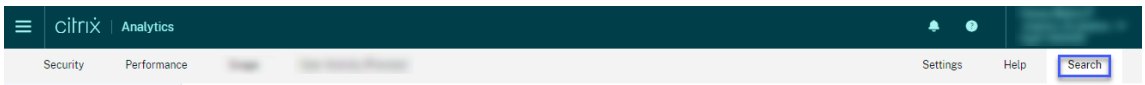
您可以使用以下选项访问自助搜索：

- 顶栏：单击顶栏中的 搜索 可查看所选数据源的所有用户事件。
- 用户个人资料页面上的风险时间表：单击 事件搜索 可查看相应用户的事件。

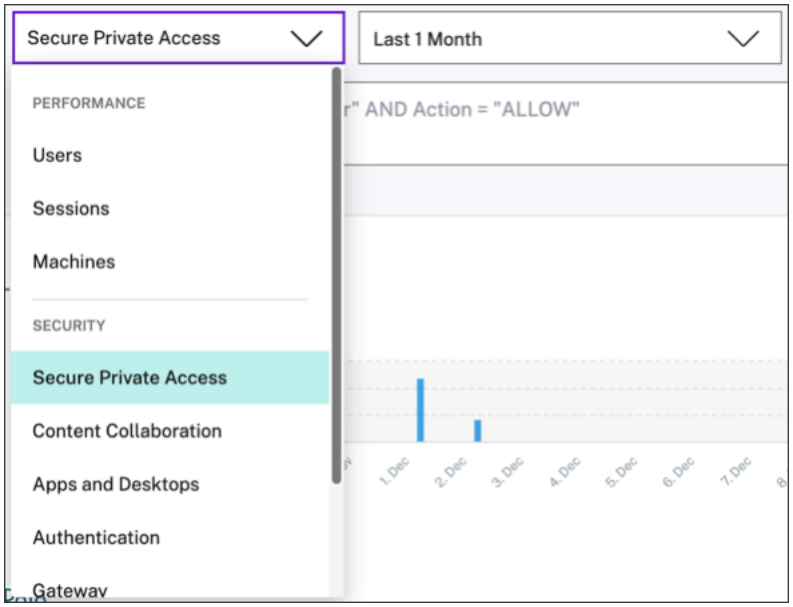
从顶部栏进行自助搜索

使用此选项可从用户界面中的任何位置转到自助搜索页面。

1. 单击 搜索 以查看自助服务页面。



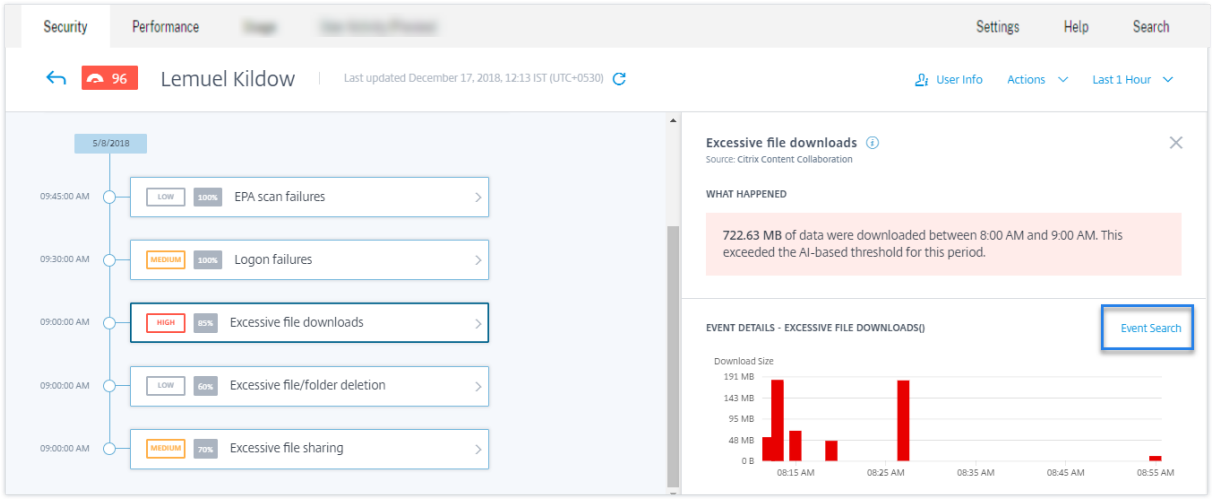
2. 选择数据源和时间段以查看相应的事件。



从用户的风险时间表进行自助搜索

如果要查看与风险指示器关联的用户事件，请使用此选项。

当您从用户的时间轴中选择风险指示器时，风险指示器信息部分将显示在右侧窗格中。单击 事件搜索 可在自助搜索页面上浏览与用户和数据源关联的事件（为其触发风险指示器）。



有关用户风险时间表的更多信息，请参阅 风险时间表。

如何使用自助搜索

使用自助搜索页面上的以下功能：

- 用于过滤事件的 Facets 。
- 用于输入查询和筛选事件的搜 索框。
- 用于选择时间 段的时间选择器。
- 查看事件图表的时间轴详细信息 。
- 用于查看事件的事件数据 。
- 导出为 CSV 格式 ，将搜索事件下载为 CSV 文件。
- 导出可视摘要 以下载搜索查询的可视摘要报告。
- 多列排序 ，按多列对事件进行排序。

使用 **Facets** 过滤事件

Facets 是构成事件的数据点的摘要。Facet 因数据源而异。例如，Secure Private Access 数据源的方面是信誉、操作、位置和类别组。而应用程序和桌面的方面是事件类型、域和平台。

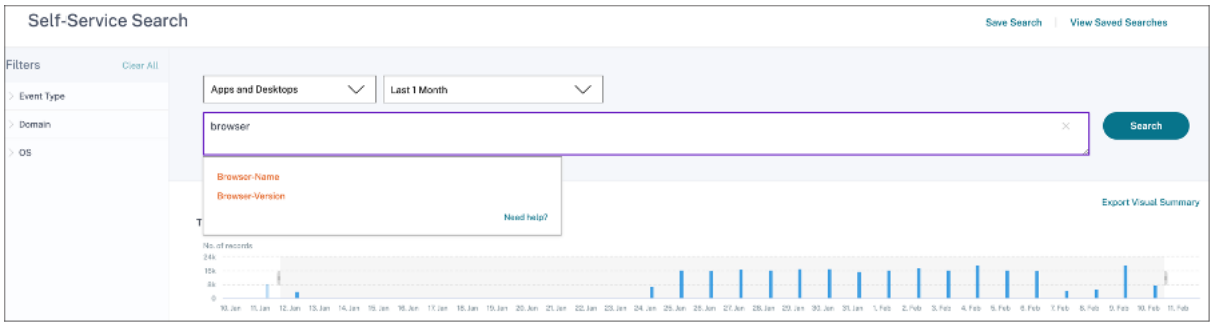
选择要过滤搜索结果的平面。选定的小平面显示为筹码。

有关与每个数据源相对应的方面的详细信息，请参阅本文前面提到的数据源的自助搜索文章。

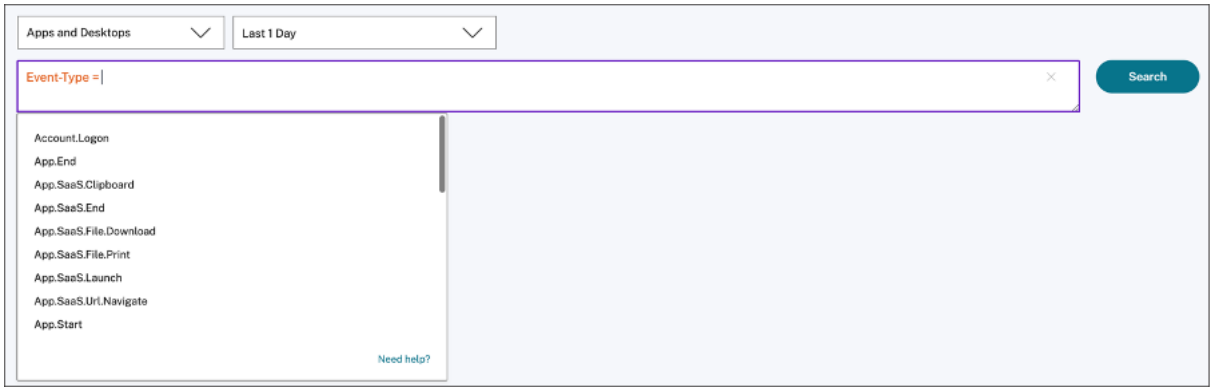
使用搜索框中的搜索查询过滤事件

将光标置于搜索框中时，搜索框会根据用户事件显示维度列表。这些维度因数据源而异。使用维度和有效 运算符 定义搜索条件并搜索所需的事件。

例如，在应用程序和桌面的自助搜索中，您将获得维度 `Browser` 的以下值。使用维度键入查询，选择时间段，然后单击 搜索。



当选择某些维度（例如 `Event-Type` 和 `Clipboard-Operation` 以及有效的运算符）时，维度的值会自动显示。您可以从建议的选项中选择一个值，也可以根据需要输入一个新值。



搜索查询中支持的运算符　在搜索查询中使用以下运算符来优化搜索结果。

操作员	说明	示例	输出
	为搜索维度分配一个值。	用户名：John	显示用户 John 的事件。
=	为搜索维度分配一个值。	用户名 = John	显示用户 John 的事件。
~	搜索具有相似值的事件。	用户名 ~ test	显示具有相似用户名的事件。
" "	用空格分隔的值括起来。	User-Name = “John Smith”	显示用户约翰·史密斯的事件。
< >	搜索关系价值。	数据量 > 100	显示数据量大于 100 GB 的事件。
AND	搜索指定条件为真的事件。	User-Name : John AND Data Volume > 100	显示用户 John 的事件，其中数据量大于 100 GB。
! ~	检查事件中指定的匹配模式。此 NOT LIKE 运算符返回事件字符串中任意位置不包含匹配模式的事件。	User-Name !~ John	显示除 John、John Smith 或包含匹配名称 “John” 的任何此类用户以外的用户的事件。
! =	检查事件是否确切指定的字符串。此 NOT EQUAL 运算符返回事件字符串中任意位置不包含确切字符串的事件。	Country != USA	显示除美国以外国家/地区的事件。
*	搜索与指定字符串匹配的事件。目前，只有以下运算符：、= 和 ! = 才支持 * 运算符。搜索结果区分大小写。	User-Name = John*	显示以 John 开头的所有用户名的事件。
		User-Name = *John*	显示包含 John 的所有用户名的事件。

操作员	说明	示例	输出
		User-Name = *Smith	显示以 Smith 结尾的所有用户名的事件。
		用户名：John*	显示以 John 开头的所有用户名的事件。
		用户名：*John*	显示包含 John 的所有用户名的事件。
		用户名：*Smith	显示以 Smith 结尾的所有用户名的事件。
		User-Name != John*	显示不以 John 开头的所有用户名的事件。
		User-Name != *Smith	显示不以 Smith 结尾的所有用户名的事件。
IN	为搜索维度分配多个值以获取与一个或多个值相关的事件。注意：目前，您可以将此运算符用于应用程序和桌面的以下维度：Device ID、Domain、Event-Type 和 User-Name。此运算符仅适用于字符串值。	User-Name IN (John, Kevin)	查找与约翰或凯文相关的所有事件。
NOT IN	为搜索维度分配多个值，然后查找不包含指定值的事件。注意：目前，您可以将此运算符用于应用程序和桌面的以下维度：Device ID、Domain、Event-Type 和 User-Name。此运算符仅适用于字符串值。	User-Name NOT IN (John, Kevin)	查找除 John 和 Kevin 之外的所有用户的事件。

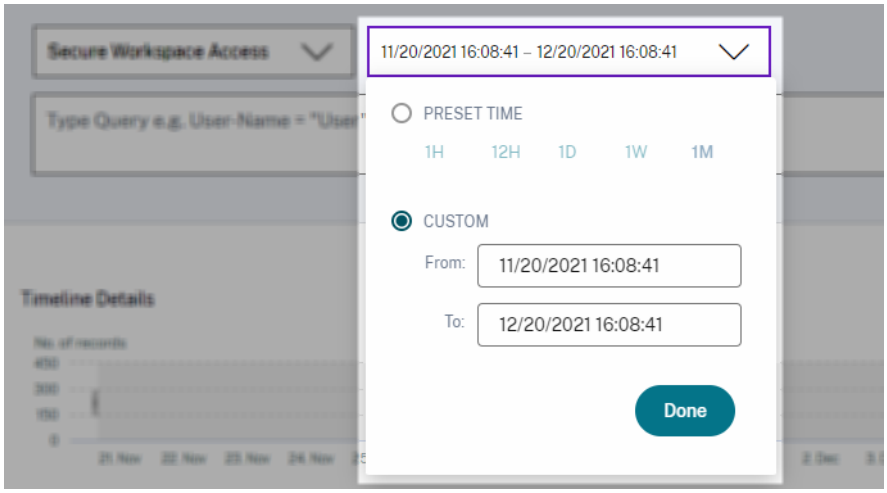
操作员	说明	示例	输出
IS EMPTY	检查维度的空值或空值。此运算符仅适用于字符串类型的维度，例如 App-Name、Browser 和 Country。它不适用于非字符串（数字）类型的维度，例如 Upload-File-Size、Download-File-Size 和 Client-IP。	国家/地区 IS EMPTY	查找国家名称不可用或为空（未指定）的事件。
IS NOT EMPTY	检查维度的非空值或特定值。此运算符仅适用于字符串类型的维度，例如 App-Name、Browser 和 Country。它不适用于非字符串（数字）类型的维度，例如 Upload-File-Size、Download-File-Size 和 Client-IP。	国家/地区 IS NOT EMPTY	查找可用或指定了国家/地区名称的事件。
OR	搜索其中一个或两个条件均为 true 时的值。	(User-Name = John* OR User-Name = *Smith) AND Event-Type = “Session.Logon”	显示所有以 John 开头或以 Smith 结尾的用户名的 Session.Logon 事件。

> 注意
>
> 对于 **NOT EQUAL** 运算符，在为查询中的维度输入值时，请使用自助搜索页面上提供的数据源的精确值。尺寸值区分大小写。

有关如何为数据源指定搜索查询的详细信息，请参阅本文前面提到的有关数据源的自助搜索文章。

选择查看活动的时间

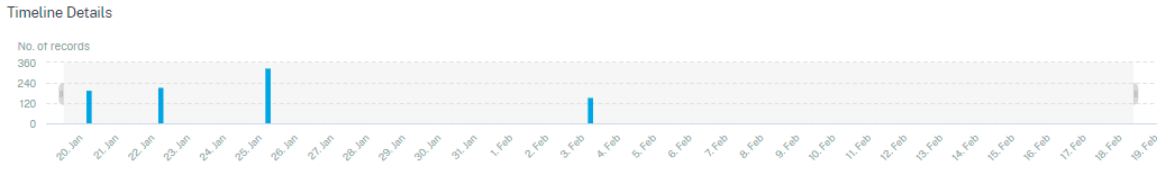
选择预设时间或输入自定义时间范围，然后单击 搜索 以查看事件。



查看时间轴详细信息

时间轴提供所选时间段内用户事件的图形表示。移动选择器栏以选择时间范围并查看与所选时间范围对应的事件。

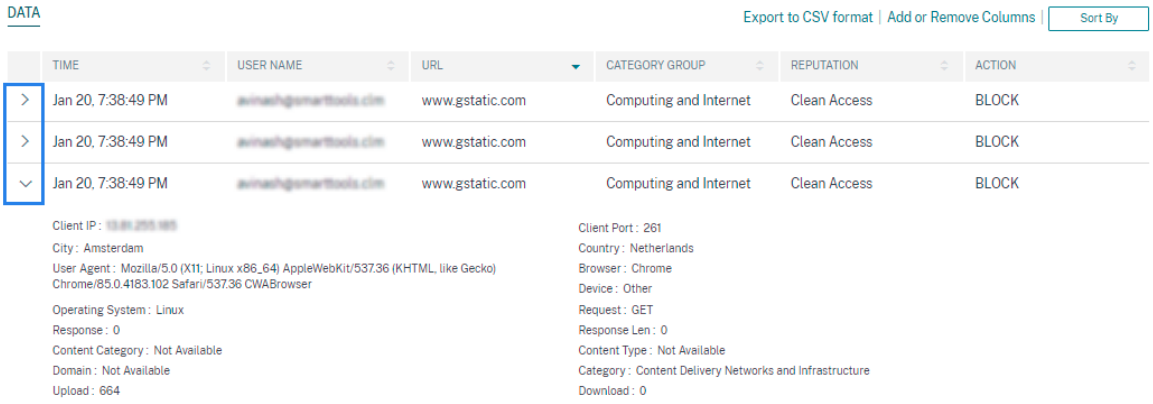
图中显示了访问数据的时间轴详细信息。



查看活动

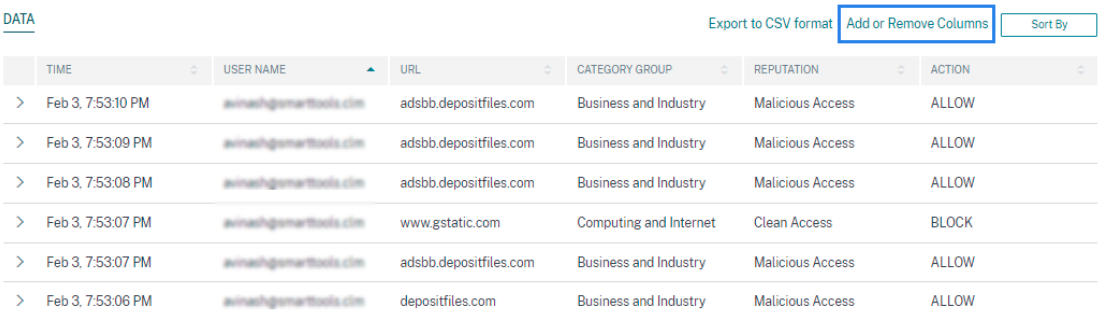
您可以查看有关用户事件的详细信息。在 **DATA** 表中，单击每列的箭头以查看用户事件详细信息。

图中显示了有关用户访问数据的详细信息。

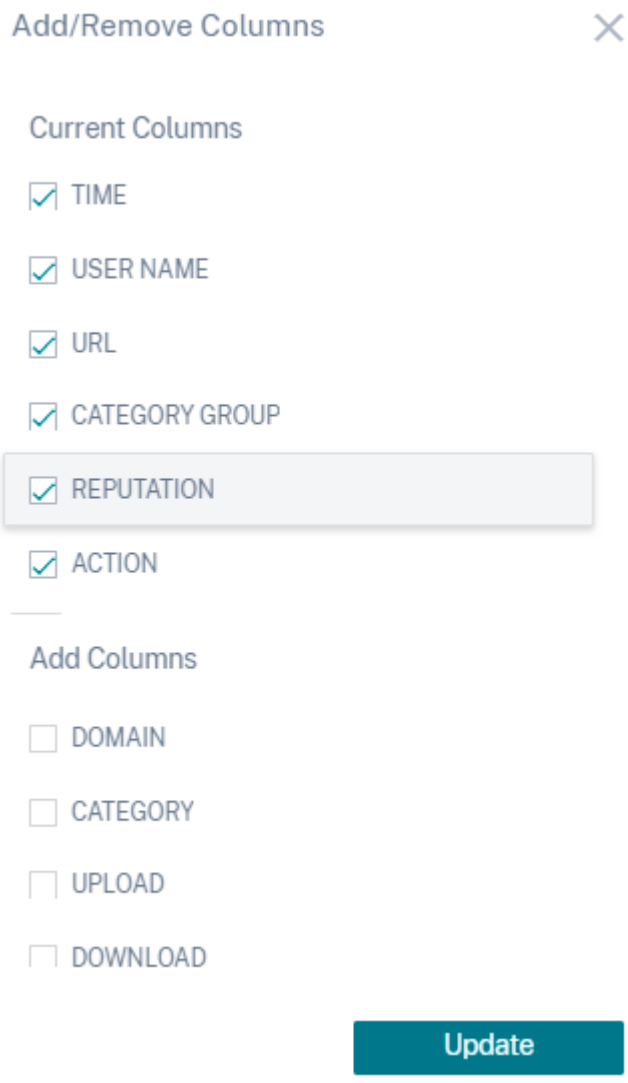


添加或删除列　您可以在事件表中添加或删除列以显示或隐藏相应的数据点。请执行以下操作：

1. 单击 添加或删除列。

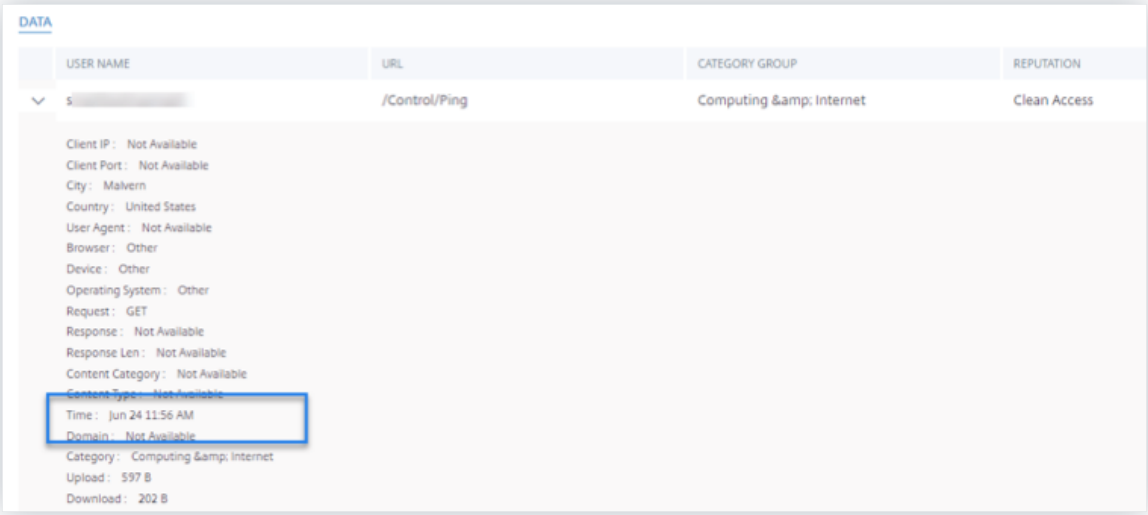


2. 从列表中选择或取消选择数据元素，然后单击“更新”。



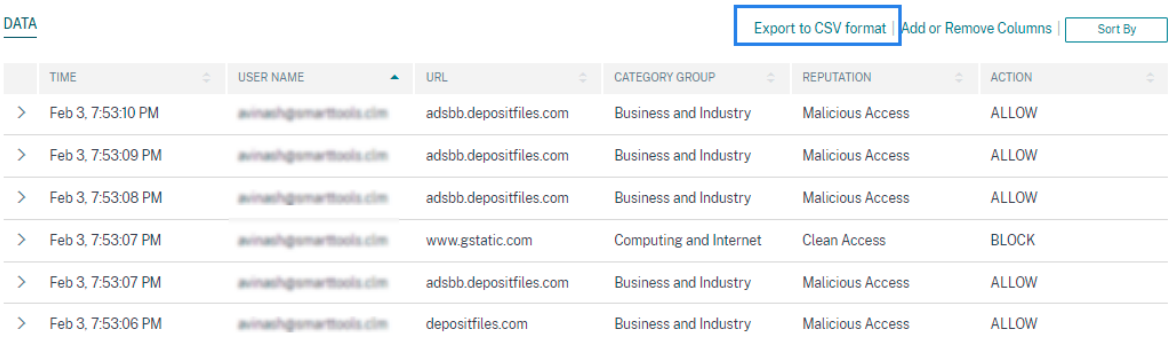
如果从列表中取消选择一个数据点，则会从事件表中删除相应的列。但是，您可以通过展开用户的事件行来查看该数据

点。例如，当您从列表中取消选择 **TIME** 数据点时，**TIME** 列将从事件表中移除。要查看时间记录，请展开用户的事件行。



将事件导出到 **CSV** 文件

将搜索结果导出为 CSV 文件并保存以供参考。单击 导出为 **CSV** 格式 以导出事件并下载生成的 CSV 文件。您可以使用导出为 **CSV** 格式功能导出 100K 行。



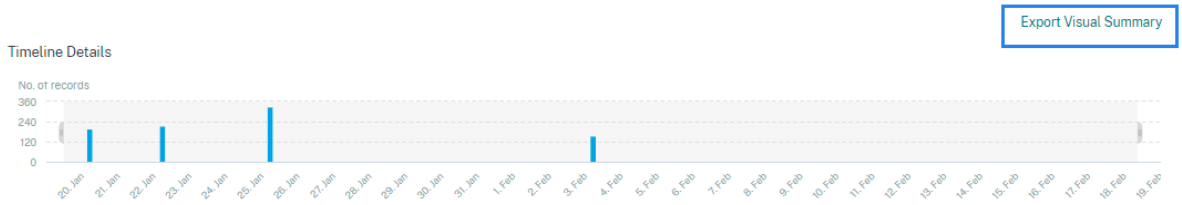
导出视觉摘要

您可以下载搜索查询的可视摘要报告，并与其他用户、管理员或管理团队共享副本。

单击 导出可视摘要 以 PDF 格式下载视觉摘要报告。该报告包含以下信息：

- 您为选定时间段内的事件指定的搜索查询。
- 在所选时间段内，您在事件上应用的方面（过滤器）。
- 可视摘要，例如时间轴图、条形图或选定时间段内搜索事件的图形。

对于数据源，只有在以条形图、时间线详细信息等视觉格式显示数据时，才能下载可视摘要报告。否则，此选项不可用。例如，您可以下载数据源的可视化摘要报表，例如应用程序和桌面、会话，您可以在其中查看时间轴详细信息和条形图的数据。对于用户和计算机等数据源，您只能看到表格格式的数据。因此，您无法下载任何视觉摘要报告。

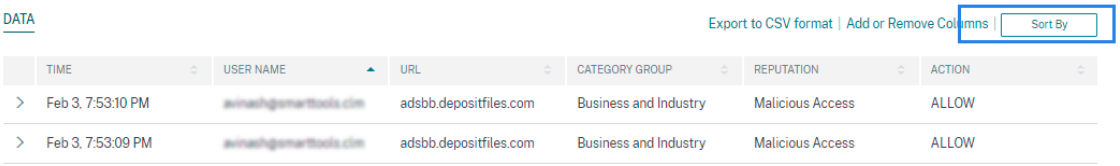


多列排序

排序有助于组织数据并提供更好的可见性。在自助搜索页面上，您可以按一列或多列对用户事件进行排序。这些列表示各种数据元素的值，例如用户名、日期和时间以及 URL。这些数据元素因选定的数据源而异。

要执行多列排序，请执行以下操作：

1. 单击“排序方式”。

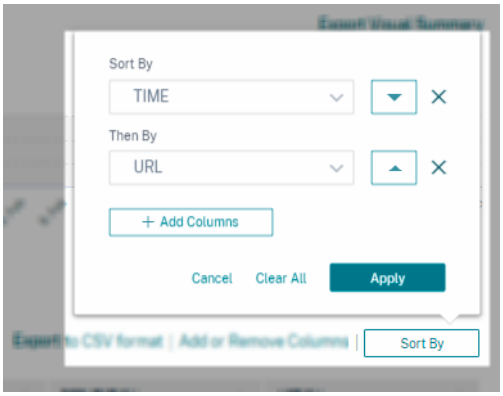


2. 从“排序方式”列表中选择一列。
3. 选择排序顺序-升序（向上箭头）或降序（向下箭头）以对列中的事件进行排序。
4. 单击 **+** 添加列。
5. 从“然后依 据”列表中选择另一列。
6. 选择排序顺序-升序（向上箭头）或降序（向下错误）以对列中的事件进行排序。

> 注意
>
> 您最多可以添加六列来执行排序。

7. 单击应用。
8. 如果不想应用上述设置，请单击“取消”。要删除所选列的值，请单击“全部清除”。

以下示例显示了对 Secure Private Access 事件的多列排序。事件按时间排序（从最新到最早的顺序），然后按 URL（按字母顺序）排序。



或者，您可以使用 **Shift** 键执行多列排序。按住 **Shift** 键并单击列标题以对用户事件进行排序。

如何保存自助搜索

作为管理员，您可以保存自助查询。此功能可节省重写经常用于分析或故障排除的查询的时间和精力。以下选项随查询一起保存：

- 应用的搜索筛选
- 选定的数据源和持续时间

执行以下操作以保存自助服务查询：

1. 选择所需的数据源和持续时间。
2. 在搜索栏中键入查询。
3. 应用所需的过滤器。
4. 单击“保存搜索”。
5. 指定用于保存自定义查询的名称。

   > 注意请
   >
   > 确保查询名称是唯一的。否则，查询不会保存。

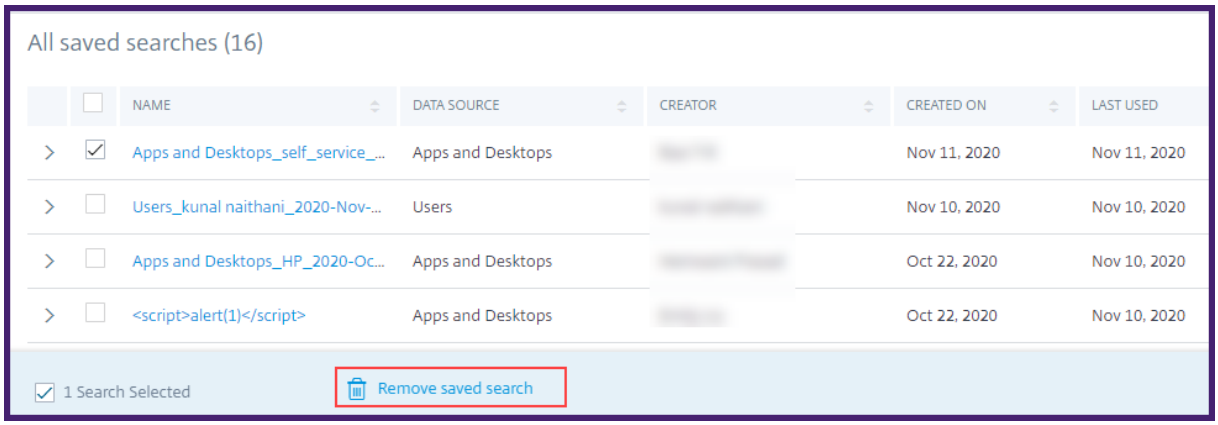
6. 如果要定期向自己和其他用户发送搜索查询报告的副本，请启用“计划电 子邮件报告”按钮。有关详细信息，请参阅为搜索查询安排电子邮件。
7. 单击保存。

要查看保存的搜索：

1. 单击查看保存的搜索。
2. 单击搜索查询的名称。

要删除已保存的搜索：

1. 单击查看保存的搜索。
2. 选择已保存的搜索查询。
3. 单击 删除保存的搜索。



要修改已保存的搜索：

1. 单击查看保存的搜索。
2. 单击已保存的搜索查询的名称。
3. 根据您的要求修改搜索查询或小平面选择。
4. 单击 更新搜索 **>** 保存 以更新和保存使用相同的搜索查询名称保存修改后的搜索。
5. 如果要使用新名称保存修改后的搜索，请单击向下箭头，然后单击 另存为新搜索 **>** 另存为。

如果用新名称替换搜索，则搜索将另存为新条目。如果在替换时保留现有搜索名称，则修改后的搜索数据将覆盖现有的搜索数据。

> 注意
>
> - 只有查询所有者可以修改或删除其保存的搜索。
> - 您可以复制保存的搜索链接地址以与其他用户共享。

为搜索查询安排电子邮件

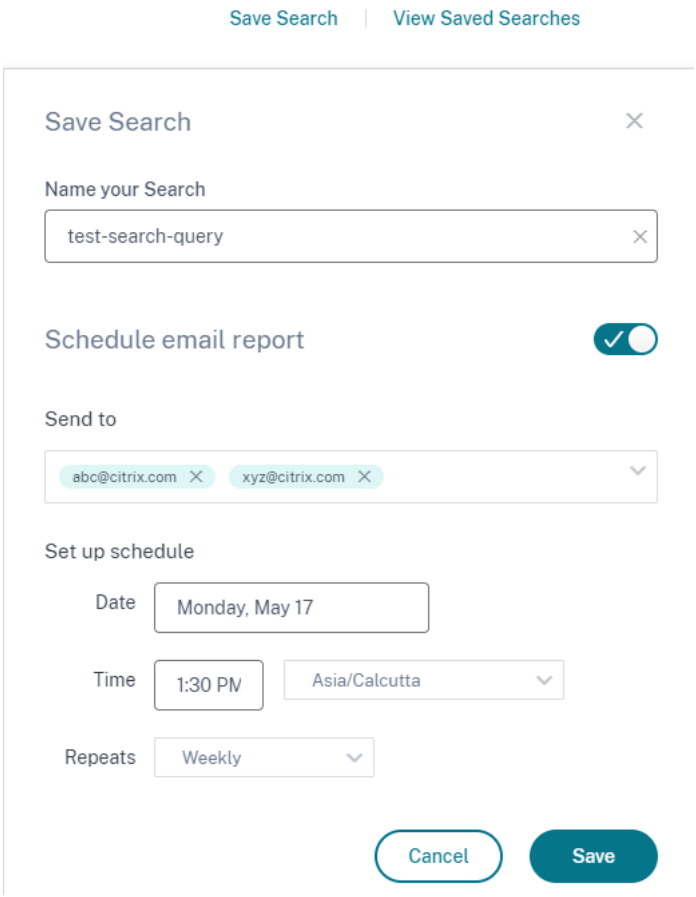
通过设置电子邮件发送计划，您可以定期向自己和其他用户发送搜索查询报告的副本。

仅当搜索查询报告包含条形图、时间线详细信息等视觉格式的数据时，此选项才可用。否则，您无法安排电子邮件发送。例如，您可以为数据源（例如应用程序和桌面、会话）安排电子邮件，在这些数据源中，您可以将数据视为时间轴详细信息和条形图。对于用户和计算机等数据源，您只能看到表格格式的数据。因此，您无法安排电子邮件。

在保存搜索查询的同时安排电子邮件

保存搜索查询时，请按如下方式设置电子邮件发送计划：

1. 在“保存搜索”对话框中，启用“计划电子邮件报告”按钮。



2. 输入或粘贴收件人的电子邮件地址。

> 注意
>
> 不支持电子邮件组。

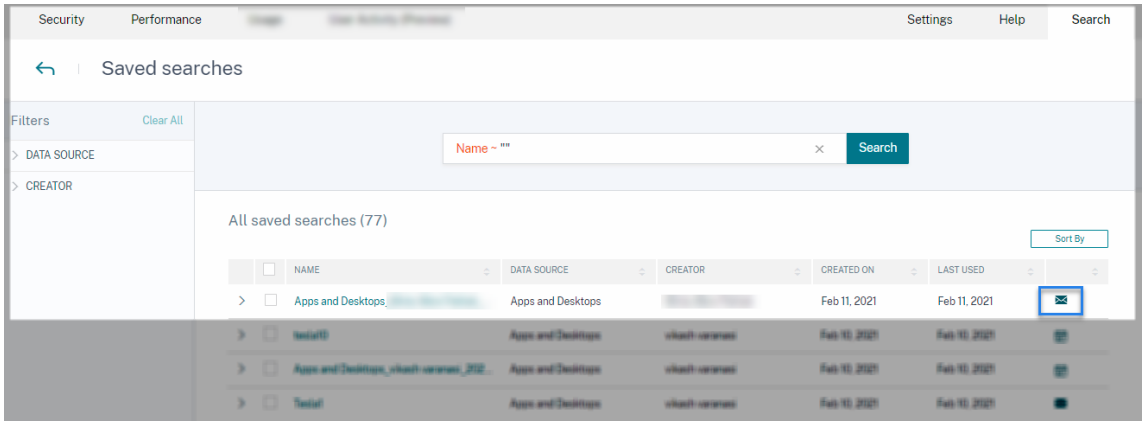
3. 设置电子邮件发送的日期和时间。
4. 选择配送频率-每天、每周或每月。
5. 单击保存。

为已保存的搜索查询安排电子邮件

如果要为之前保存的搜索查询设置电子邮件发送计划，请执行以下操作：

1. 单击查看保存的搜索。
2. 转到您创建的搜索查询。单击 电子邮件此查询 图标。

> 注意
>
> 只有查询所有者可以安排其保存的搜索查询的电子邮件发送。



3. 启用计 划电子邮件报告 按钮。
4. 输入或粘贴收件人的电子邮件地址。

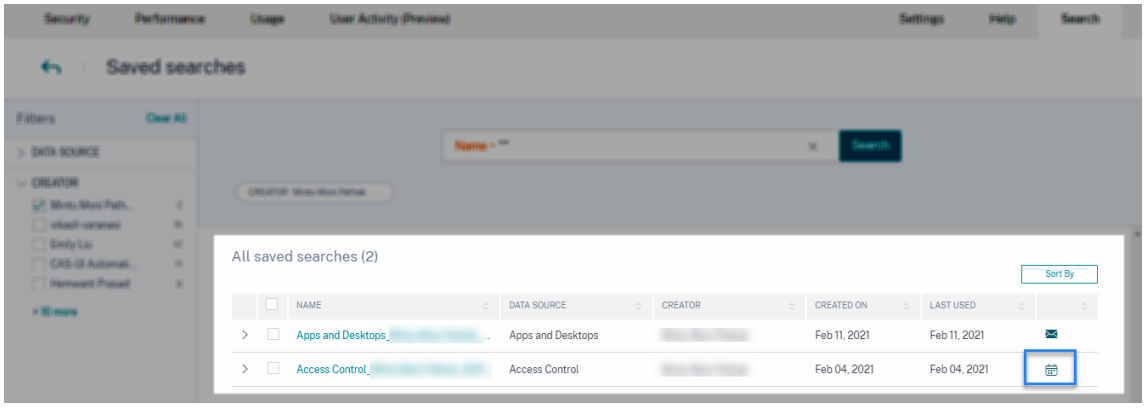
> 注意
>
> 不支持电子邮件组。

5. 设置电子邮件发送的日期和时间。
6. 选择配送频率-每天、每周或每月。
7. 单击保存。

停止搜索查询的电子邮件发送计划

1. 单击查看保存的搜索。
2. 转到您创建的搜索查询。单击查 看电子邮件发送计划 图标。

> 注意
>
> 只有查询所有者可以停止其保存的搜索查询的电子邮件计划。



3. 禁用计 划电子邮件报告 按钮。
4. 单击保存。

邮件内容

收件人会收到来自“Citrix Cloud - 通知 donotreplynotifications@citrix.com”的有关搜索查询报告的电子邮件。该报告作为 PDF 文档附件。电子邮件将按您在 计划电子邮件报告 设置中定义的定期间隔发送。

搜索查询报告包含以下信息：

- 您为选定时段内的事件指定的搜索查询。
- 您在事件上应用的方面（过滤器）。
- 视觉摘要，例如时间线图、条形图或搜索事件的图表。

完全访问权限和只读访问权限管理员的权限

- 如果您是具有完全访问权限的 Citrix Cloud 管理员，则可以使用 搜索 页面上的所有可用功能。
- 如果您是具有只读访问权限的 Citrix Cloud 管理员，则只能在 搜索 页面上执行以下活动：
  - 通过选择数据源和时间段来查看搜索结果。
  - 输入搜索查询并查看搜索结果。
  - 查看其他管理员保存的搜索结果。
  - 导出可视摘要并将搜索结果下载为 CSV 文件。

有关管理员角色的信息，请参阅 管理 Citrix Analytics 的管理员角色。

面向身份验证的自助搜索

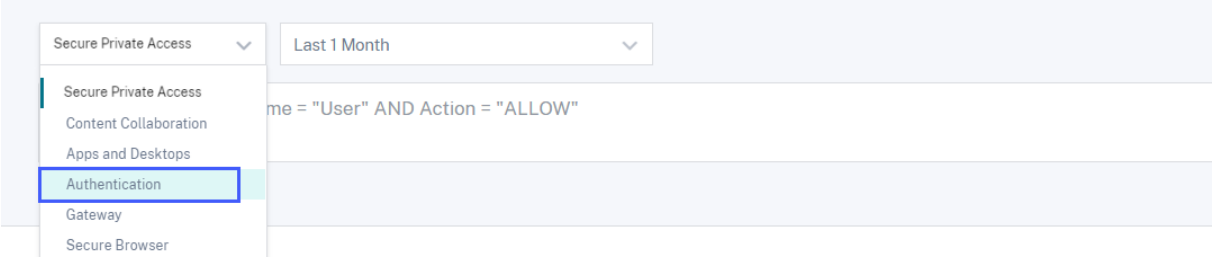
October 14, 2021

使用自助搜索可深入了解企业中 Citrix Cloud 用户的用户身份验证详细信息。Citrix Analytics for Security 从 Citrix Cloud 的身份和访问管理服务接收用户身份验证事件。用户登录、用户注销和客户端更新等身份验证事件显示在自助搜索页面上。

有关搜索功能的详细信息，请参阅 自助搜索。

选择身份验证数据源

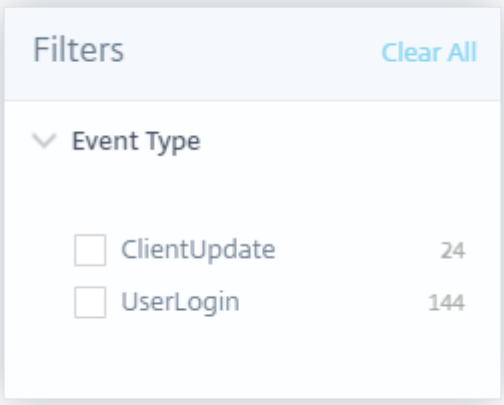
要查看身份验证事件，请从列表中选择 身份验证。默认情况下，自助服务页面显示最近一天的事件。您还可以选择要查看事件的时间段。



选择要过滤事件的平面

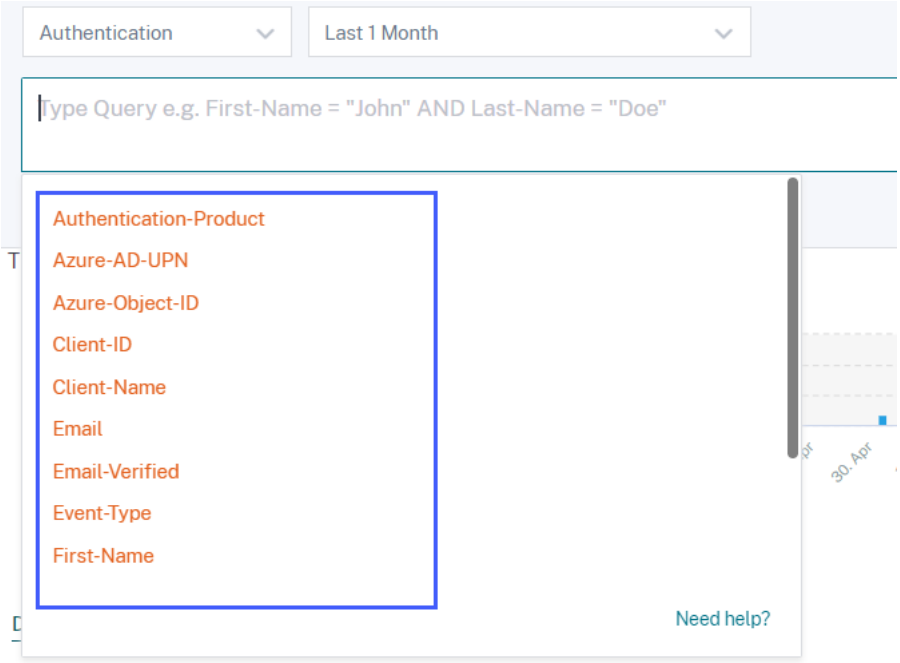
对身份验证事件使用以下过滤器：

- 事件类型-根据用户事件类型（如用户登录、用户注销和客户端更新）搜索事件。



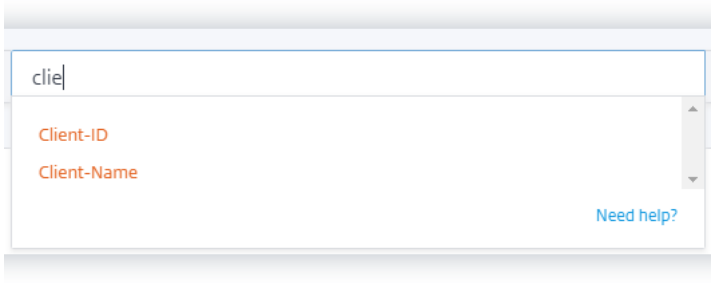
指定搜索查询以筛选事件

将光标置于搜索框中可查看身份验证事件的维度列表。使用维度和 运算符 指定查询并搜索所需的事件。

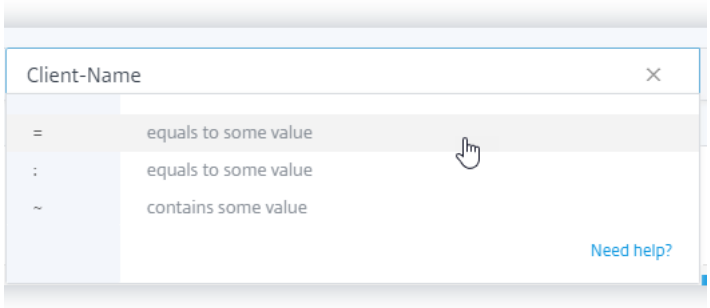


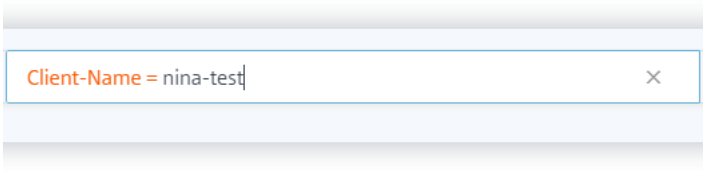
例如，您想查看电子邮件状态已验证的客户端“nina-test”的身份验证事件。

1. 在搜索框中输入“client”以获取相关维度。

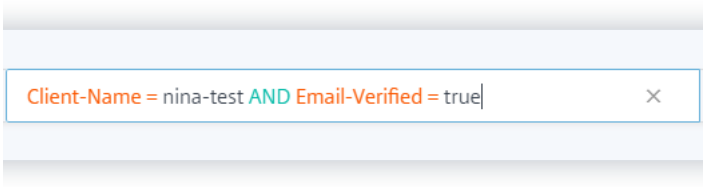


2. 选择 客户端名称，然后使用等于运算符指定值“nina-test”。





3. 选择 **AND** 运算符，然后选择 “电子邮件验证” 维度。使用等于运算符将值 “true” 分配给 “电子邮件验证”。“true” 值表示用户的电子邮件已通过验证。



4. 选择时间段，然后单击 “搜索” 以查看 数据 表上的事件。

面向网关的自助搜索

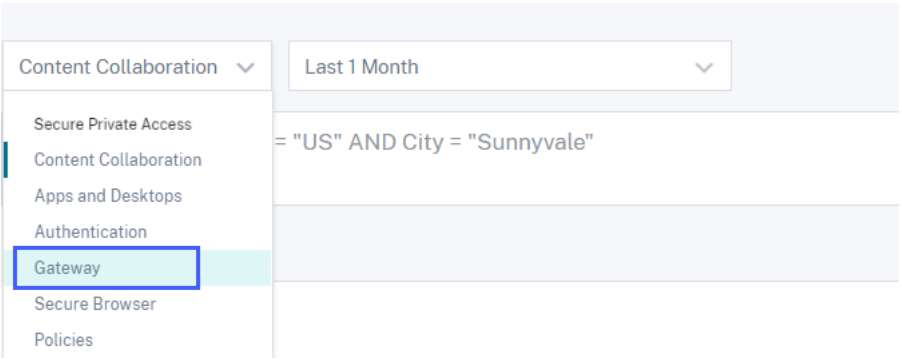
October 14, 2021

使用自助搜索功能深入了解从 Citrix Gateway 数据源接收的用户事件。当用户通过 Citrix Gateway 访问其网络资源（例如文件服务器、应用程序、网站）时，将为每个用户连接生成事件。用户事件的一些示例包括身份验证阶段、授权类型和 VPN 会话代码。Citrix Analytics for Security 接收这些事件并将其显示在自助搜索页面上。您可以查看用户及其访问详细信息。

有关搜索功能的详细信息，请参阅 自助搜索。

选择 **Gateway** 数据源

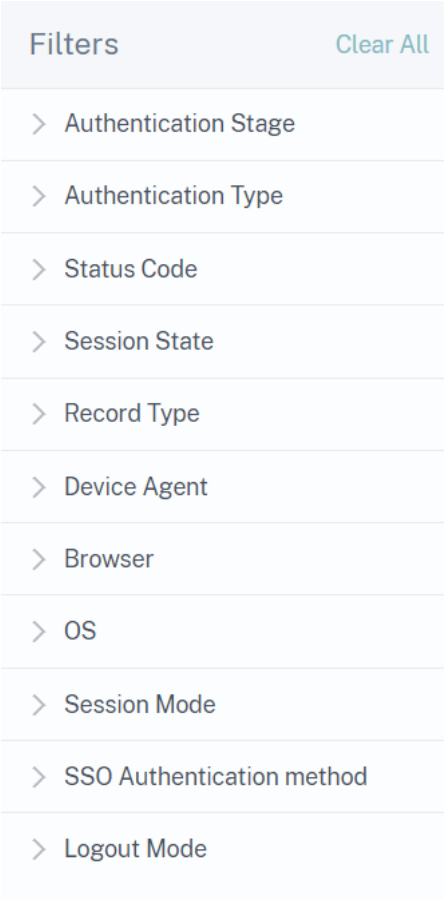
要查看网关事件，请从列表中选择 网关。默认情况下，自助服务页面显示最近一天的事件。您还可以选择要查看事件的时间段。



> 注意
>
> 或者，您可以从“安全”>“用户”>“访问 摘要”控制板访问“自助搜索网关”页面。在成功登录的情况下，您可以通过状态码访问数据。有关更多信息，请参阅“访问摘要”仪表板。

使用方面过滤事件

这些方面是根据从数据源接收到的事件进行分类的。使用以下方面过滤事件：



- 身份验证阶段-根据客户端身份验证的不同阶段（如主、辅助和第三阶段）搜索事件。
- 身份验证类型-根据客户端身份验证类型搜索事件，例如本地、RADIUS、LDAP、TACACS、客户端证书身份验证（包括智能卡身份验证）。
- 设备代理-基于 iPhone、iPad、Windows Mobile 等客户端设备搜索事件。
- 记录类型-根据 VPN 记录的类型搜索事件。以下 VPN 记录类型可用：

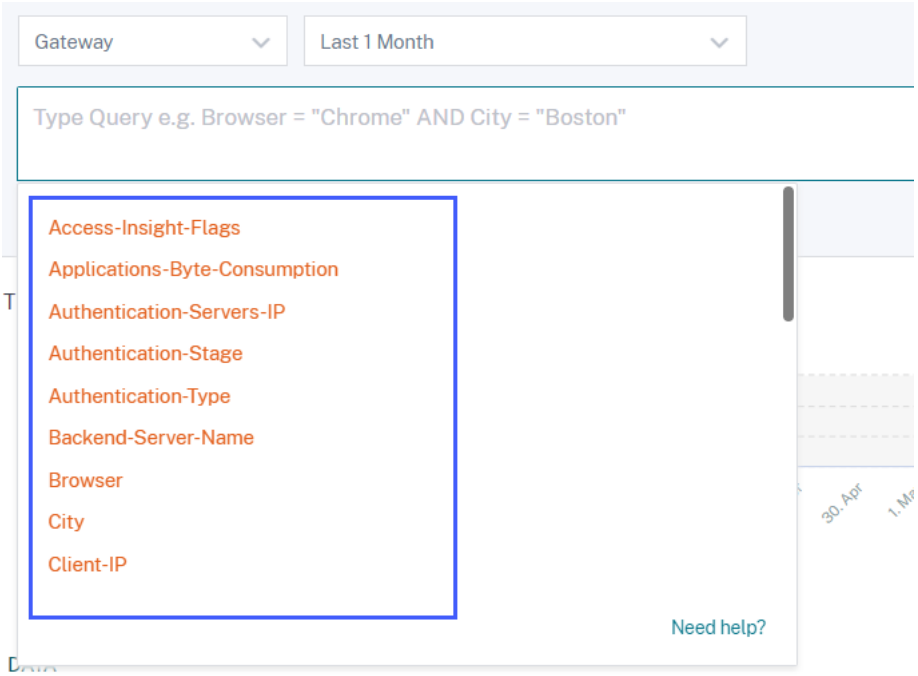
记录类型	说明
VPN_AI	筛选与验证相关的用户事件。

记录类型	说明
VPN_IF	筛选与 ICA 文件相关的用户事件。
VPN_ST	筛选与会话注销相关的用户事件。

- 浏览器 - 基于浏览器（例如 Internet Explorer、Chrome、Firefox、Safari）搜索事件。
- 操作系统-基于客户端操作系统（如 Windows、Mac、Linux、Android、iOS）搜索事件。
- 状态代码-根据 VPN 状态代码搜索事件，例如 SSL 重定向响应失败、授权失败、单点登录失败。
- 会话状态-根据 VPN 会话状态（例如客户端状态、授权状态、SSO 状态、应用程序带宽更新）搜索事件。
- 会话模式-根据 VPN 会话模式搜索事件，例如全通道、ICA 代理、无客户端。
- **SSO** 身份验证方法-根据不同的单点登录身份验证方法搜索事件，例如基本、摘要、NTLM、Kerberos、AG basic、基于表单的 SSO。
- 注销模式-根据 VPN 注销模式搜索事件，例如内部错误注销、会话超时注销、用户启动的注销、管理员终止的会话。

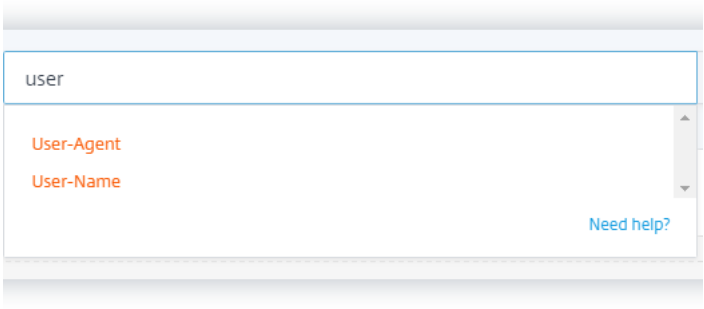
指定搜索查询以筛选事件

将光标置于搜索框中可查看 Gateway 事件的维度列表。使用维度和 运算符 指定查询并搜索所需的事件。

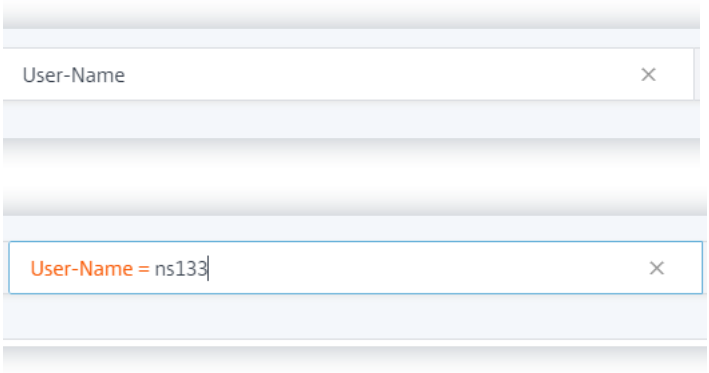


例如，您想查看 VPN 状态代码为“成功登录”的用户“ns133”的事件。

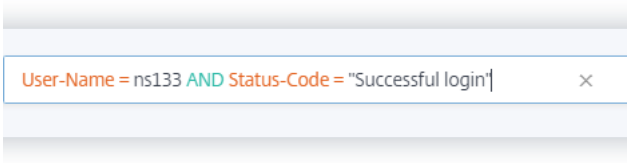
1. 在搜索框中输入“用户”以选择相关维度。



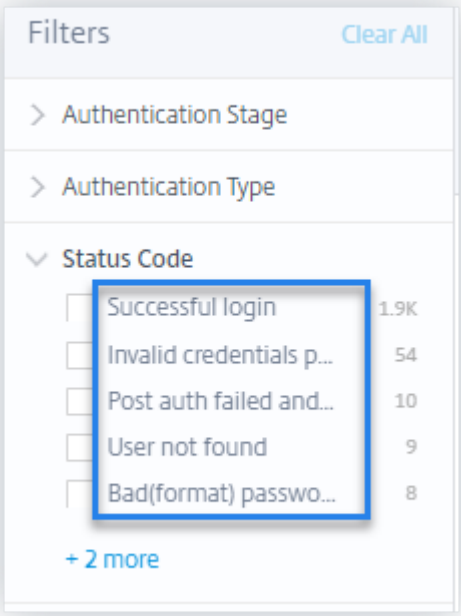
2. 选择用 户名 并使用等于运算符输入值“ns133”。



3. 选择 **AND** 运算符，然后选择 状态代码 维度。使用 equal 运算符为 状态码 输入字符串“成功登录”。



要识别“状态代码”的可能字符串值，请展开“状态代码”筛选器列表，然后在搜索查询中使用筛选器名称作为字符串。



4. 选择时间段，然后单击“搜索”以查看 数据 表上的事件。

搜索查询支持的值

为维度输入以下值以定义搜索查询。

访问洞察力标志

表示 VPN 会话状态。输入以下标志值之一：

VPN 会话状态	标记值
预身份验证	2
nFactor（多因素）身份验证的最后或最终状态	1
后身份验证	4

> 注意
>
> 此标志仅适用于验证事件的之前 VPN 会话状态。对于所有其他事件，标志值为零。

应用程序字节消耗

对于 `Applications-Byte-Consumption` 维度，请输入以下值：

值	类型	说明
示例：40、100	数量	您正在使用的应用程序消耗的数据（以字节为单位）。

身份验证-服务器-IP

对于 Authentication-Servers-IP 维度，请输入以下值：

值	类型	说明
示例：10.xxx.xx.xx	字符串	身份验证服务器的 IP 地址。

身份验证阶段

对于 Authentication-Stage 维度，请输入以下值：

值	类型	说明
Primary、Secondary、或 Tertiary	字符串	客户端身份验证的不同阶段。

身份验证类型

对于 Authentication-Type 维度，请输入以下值：

值	类型	说明
LDAP、SAML、Local、Radius、TACACS、SAMLIDP 或 OTP。	字符串	通过其中一种可用方法对用户进行身份验证。

后端服务器名称

对于 Backend-Server-Name 维度，请输入以下值：

值	类型	说明
示例：10.xxx.xxx.xx	字符串	后端服务器的 IP 地址。

浏览器

对于 Browser 维度，请输入以下值：

值	类型	说明
PN Agent、Edge、Firefox、Chrome 或 Safari。	字符串	使用的浏览器。

城市

对于 City 维度，请输入以下值：

值	类型	说明
示例：Boston、Beijing	字符串	用户登录的城市。

Client-IP

对于 Client-IP 维度，请输入以下值：

值	类型	说明
示例：10.xxx.xxx.xx	字符串	用户设备的 IP 地址。

Client-IP-Type

对于 Client-IP-Type 维度，请输入以下值：

值	类型	说明
公共、私人	字符串	指示用户 IP 地址是公有还是私有地址。

> 注意
>
> 这些值区分大小写。以小写字母输入值。

客户端口

对于 Client-Port 维度，请输入以下值：

值	类型	说明
示例：45334	数量	用户设备的端口号。

国家/地区

对于 Country 维度，请输入以下值：

值	类型	说明
示例：United States、India	字符串	用户登录的国家/地区。

> 注意
>
> 如果值包含空格，请将该值括在“”中。示例：国家 = “美国”。

活动类型

对于 Event-Type 维度，请输入以下值：

值	类型	说明
身份验证、ICA 文件、会话注销	字符串	用户事件的类型。

网关 **FQDN**

对于 Gateway-FQDN 维度，请输入以下值：

值	类型	说明
示例：Gateway-test	字符串	Citrix Gateway 关的域名。

网关 **IP**

对于 Gateway-IP 维度，请输入以下值：

值	类型	说明
示例：10.xxx.xxx.xx	字符串	Citrix Gateway 的 IP 地址。

网关端口

对于 Gateway-Port 维度，请输入以下值：

值	类型	说明
示例：443	字符串	Citrix Gateway 的端口号。

注销模式

对于 Logout-Mode 维度，请输入以下值：

值	类型	说明
"Internal error"、"Inactive time out"、"User initiated logout"、或 "Administrator killed session"。	字符串	VPN 会话超时或终止的原因。

> 注意
>
> 如果值包含空格，请将该值括在“”中。示例：注销模式 = "Internal error"。

NetScaler-IP

对于 NetScaler-IP 维度，请输入以下值：

值	类型	说明
示例：10.xxx.xx.xx	字符串	Citrix ADC 设备的 IP 地址。

操作系统

对于 OS 维度，请输入以下值：

值	类型	说明
示例：MAC_OS、WINDOWS	字符串	用户设备的操作系统。

记录类型

对于 Record Type 维度，请输入以下值：

值	类型	说明
VPN_AI	字符串	表示与验证相关的用户事件。
VPN_IF	字符串	表示与 ICA 文件相关的用户事件。
VPN_ST	字符串	表示与会话注销相关的用户事件。

SSO 身份验证方法

对于 SSO-Authentication-Method 维度，请输入以下值：

值	类型	说明
NSAUTH_BEARER、NSAUTH_FORM、NSAUTH_CITRIXAGBASIC、NSAUTH_NEGOTIATE、NSAUTH_NTLM 或 NSAUTH_BASIC。	字符串	单点登录身份验证的不同方法。

服务器 **IP**

对于 Server-IP 维度，请输入以下值：

值	类型	说明
示例：10.xx.xxx.xx	字符串	后端服务器的 IP 地址。

服务器端口

对于 Server-Port 维度，请输入以下值：

值	类型	说明
示例：47054	数量	后端服务器的端口号。

会话状态

对于 Session-State 维度，请输入以下值：

值	类型	说明
"Set Client State"、"Authorization State"、"SSO State" 和 "Application Bandwidth Update"	字符串	VPN 会话状态。

> 注意
>
> 如果值包含空格，请将该值括在“”中。示例：会话状态 = "Set Client State"。

状态代码

对于 Status-Code 维度，请输入以下值：

值	类型	说明
"Successful login"、"Invalid credentials passed"、"Post auth failed and connection quarantined"、"Login not permitted"、"Maximum login failures reached"	字符串	VPN 状态码。

> 注意
>
> 如果值包含空格，请将该值括在“”中。示例：会话代码 = "Successful login"。

用户代理

对于 User-Agent 维度，请输入以下值：

值	类型	说明
IPHONE、IPAD、或 WINPHONE	字符串	用于访问 VPN 的代理程序或设备。

VPN-会话 ID

对于 VPN-Session-ID 维度，请输入以下值：

值	类型	说明
c2c290c61dfe4e07247bde1e2a12	字符串	服务器为用户的 VPN 会话分配的会话 ID。

VPN 会话模式

对于 VPN-Session-Mode 维度，请输入以下值：

值	类型	说明
"Full Tunnel"、"ICA Proxy"或 Clientless	字符串	用户 VPN 会话的不同模式。

> 注意
>
> 如果值包含空格，请将该值括在“”中。示例：会话代码 = "Full Tunnel"。

面向策略的自助搜索

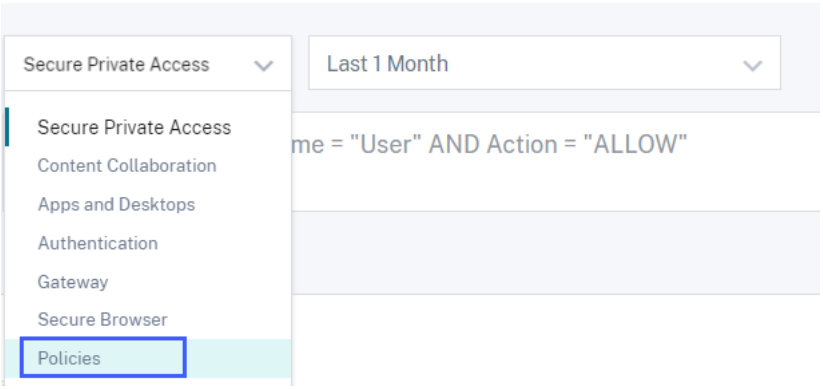
May 7, 2022

Citrix Analytics for Security 允许您创建策略并对用户帐户中的异常或可疑事件应用操作。当用户事件符合您定义的策略时，这些操作将自动应用于用户帐户，以隔离威胁并防止将来发生异常事件。使用自助搜索，您可以查看符合定义策略的用户事件，并查看对这些异常事件应用的操作。

有关搜索功能的详细信息，请参阅 自助搜索。

选择策略数据集

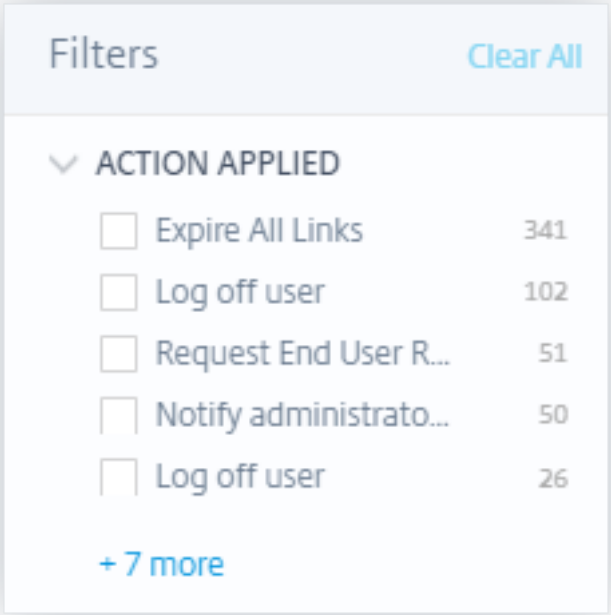
要查看与定义的策略相关的事件，请从列表中选择 策略。默认情况下，自助服务页面显示最近一天的事件。您还可以选择要查看事件的时间段。



> 注意
>
> 您还可以从“安全”>“用户”>“策略 和操作”控制板访问“自助搜索策略”页面。在控制面板上选择一个策略以查看与该策略相关的用户事件。有关更多信息，请参阅“策略和操作”控制板。

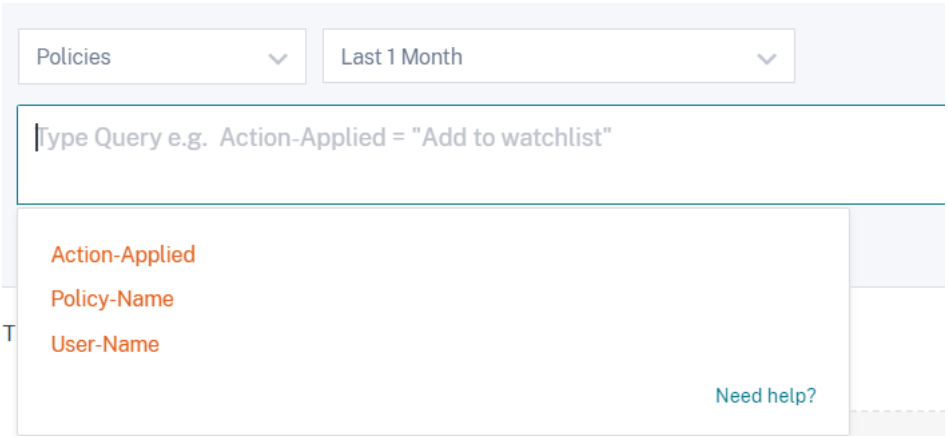
选择要过滤事件的平面

Facet 列表显示对用户事件应用的操作。从 Facet 列表中选择已应用的操作，然后根据应用的操作查看事件。有关在配置策略时可以应用的操作的更多信息，请参阅 什么是操作?



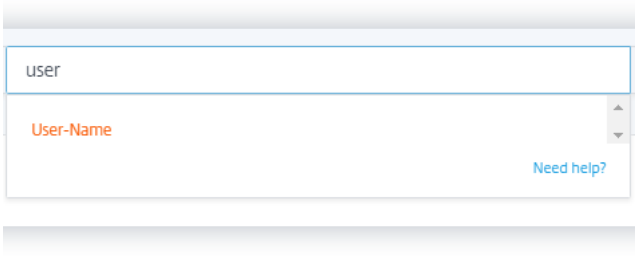
指定搜索查询以筛选事件

将光标置于搜索框中可查看与策略相关的事件的维度列表。使用维度和 运算符 指定查询并搜索所需的事件。

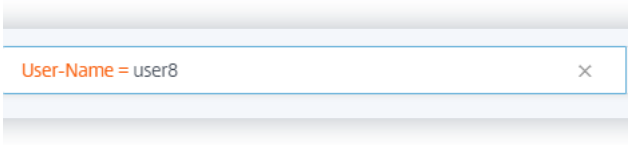


例如，您想查看用户“user8”的异常事件，其中应用于这些事件的操作是“禁用用户”。“

1. 在搜索框中输入“user”以获取相关维度。

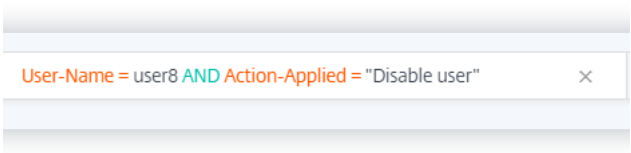


2. 选择用 户名，然后使用等于运算符输入值“user8”。

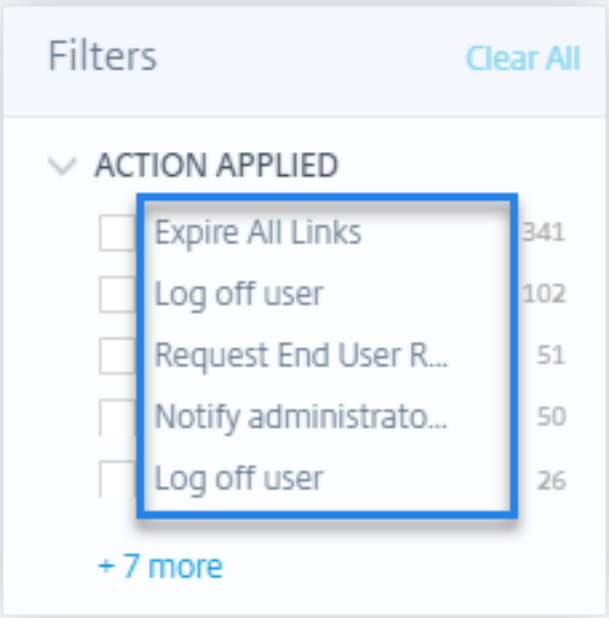


3. 选择 **AND** 运算符，然后选择“已应用操 作”维度。使用等于运算符为应用 操作输入字符串“禁用 用户”。

> 注意
>
> 如果字符串值包含两个或更多单词，则必须用运算符 “” <!--NeedCopy--> 将其括起来。例如 “Disable user” <!--NeedCopy-->，“停止会话录制”。



要确定 **ActionApplied** 的可能字符串值，请展开 Facet 列表，然后在搜索查询中使用筛选器名称作为字符串。



4. 选择时间段，然后单击“搜索”以查看 数据 表上的事件。

自助搜索远程浏览器隔离（**Secure Browser**）

December 7, 2023

使用自助搜索深入了解使用 Citrix Remote Browser Isolation 服务的 Citrix Workspace 用户的浏览会话。Citrix Remote Browser Isolation 是一项云服务，可在不影响企业网络安全的情况下提供安全的 Internet 浏览体验。当用户使用 Remote Browser Isolation 访问 Web 应用程序时，会为每个用户连接生成会话连接、会话启动、已发布的应用程序和已删除的应用程序等事件。Citrix Analytics for Security 接收这些事件并将其显示在自助服务页面上。您可以跟踪用户及其浏览会话。

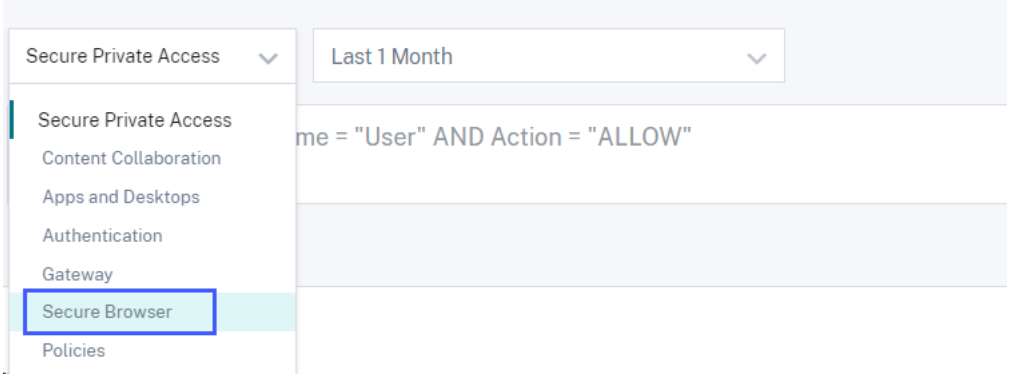
有关搜索功能的详细信息，请参阅 自助搜索。

必备条件

要接收来自 Remote Browser Isolation 的事件，请在 Remote Browser Isolation 中启用主机名跟踪以记录用户会话的主机名。此信息将发送给 Citrix Analytics for Security。有关更多信息，请参阅管理已发布的 Remote Browser Isolation。

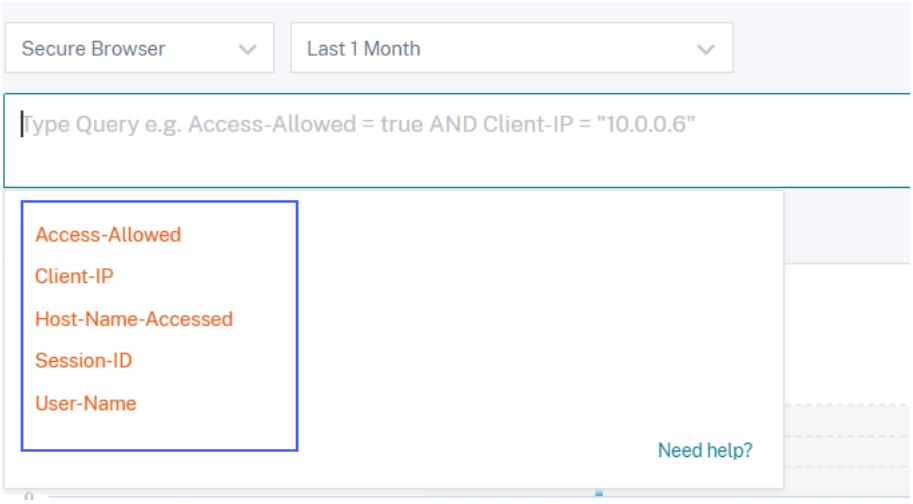
选择 **Remote Browser Isolation** 数据源

要查看 Remote Browser Isolation 事件，请从列表中选择“**Remote Browser Isolation**”。默认情况下，自助服务页面显示最近一天的事件。您还可以选择要查看事件的时间段。



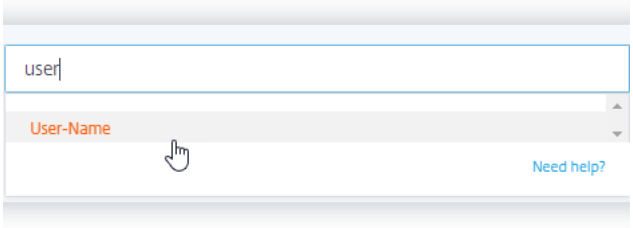
指定搜索查询以筛选事件

将光标置于搜索框中可查看 Remote Browser Isolation 事件的维度列表。使用维度和 运算符 指定查询并搜索所需的事件。

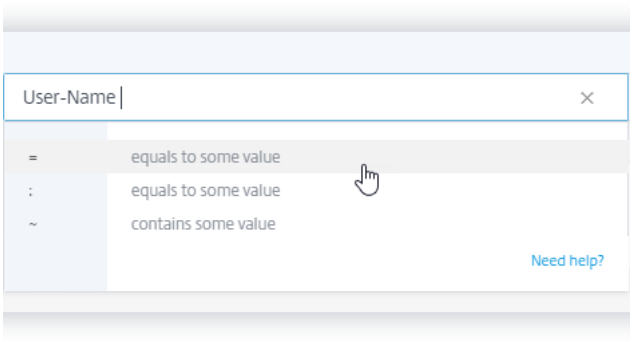


例如，您想查看有权访问各种主机服务（如 google.com、amazon.com）的用户“aa”的浏览事件详细信息。

1. 在搜索框中输入“user”以查看相关维度。



2. 单击用 户名，然后使用等于运算符输入值“aa”。



3. 选择 **AND** 运算符和 允许访问 维度。使用 equal 运算符将值“true”分配给允许访问。“true”值表示用户可以访问主机服务。

4. 选择时间段，然后单击“搜索”以查看 数据 表上的事件。

查看用户事件详情

您可以查看从 Remote Browser Isolation 服务收到的以下数据：

- 时间-用户事件发生的日期和时间。
- 用户名-发起事件的用户。
- 会话 **ID**-分配给用户会话的唯一编号。
- 客户端 **IP**-用户设备的 IP 地址。
- 主机名-用户通过网络访问的主机服务。
- 允许访问-允许或拒绝用户访问主机服务。

Secure Private Access 的自助搜索

April 12, 2024

使用自助搜索可深入了解组织中 Citrix Cloud 用户的访问事件。访问事件的示例包括 url 类别、内容类别、浏览器和设备。Citrix Analytics for Security 从 Secure Private Access 服务接收这些事件，并将其显示在自助搜索中。您可以跟踪用户及其访问详细信息。

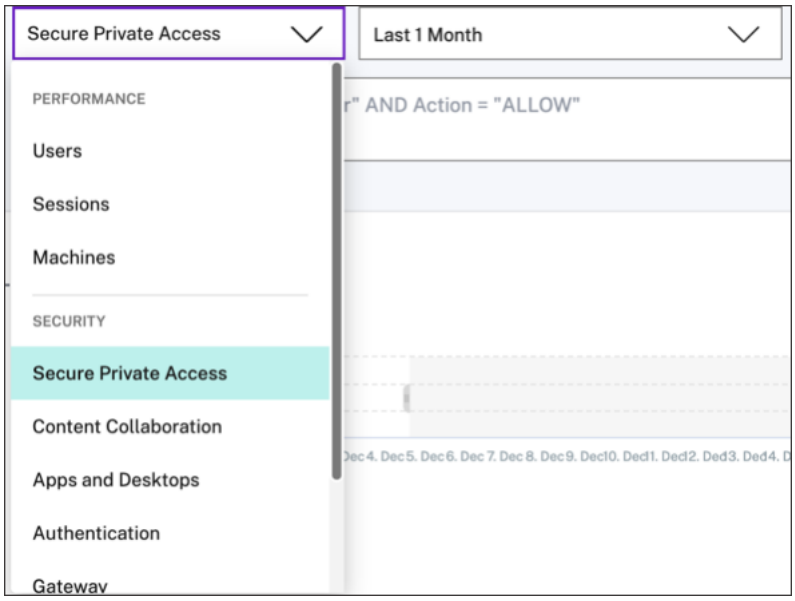
有关搜索功能的详细信息，请参阅 自助搜索。

> 注意
>
> 由于弃用了通过 Secure Private Access 进行的基于类别的 Web 筛选，Citrix Analytics for Security 的以下功能受到影响：
>
> 1. Citrix Analytics for Security 控制板上不再提供 URL 的类别组、类别和信誉等数据字段。
> 2. 依赖于相同数据的风险 Web 站点访问指示器也已弃用，不会为客户触发。
> 3. 任何使用数据字段（URL 的类别组、类别和信誉）及其关联策略的现有自定义风险指示器都不再触发。

有关 Secure Private Access 中的弃用的详细信息，请参阅功能弃用。

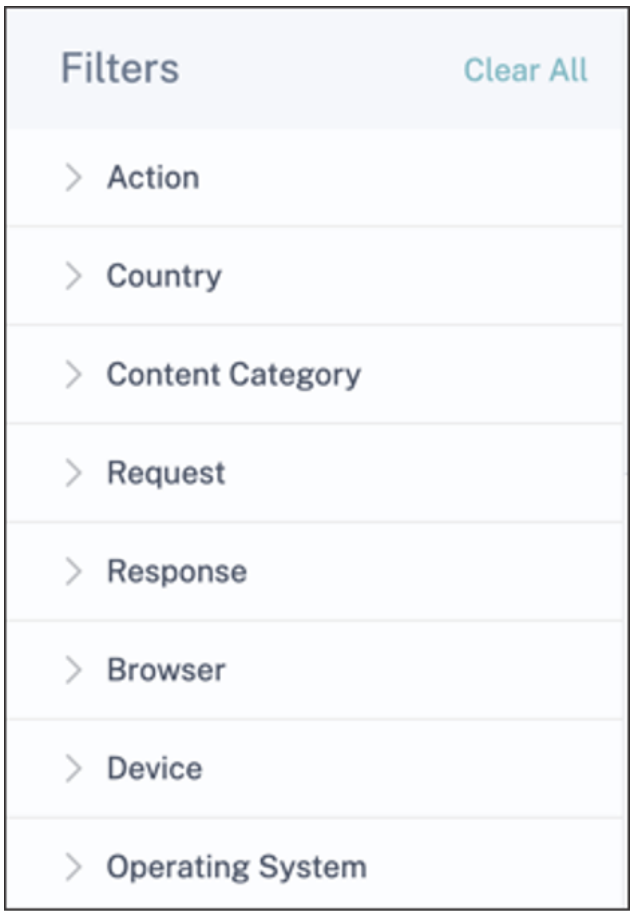
选择 **Secure Private Access** 数据源

要查看 Secure Private Access 事件，请从列表中选择“**Secure Private Access**”。默认情况下，自助服务页面显示最近一天的事件。您还可以选择要查看事件的时间段。



选择要过滤事件的平面

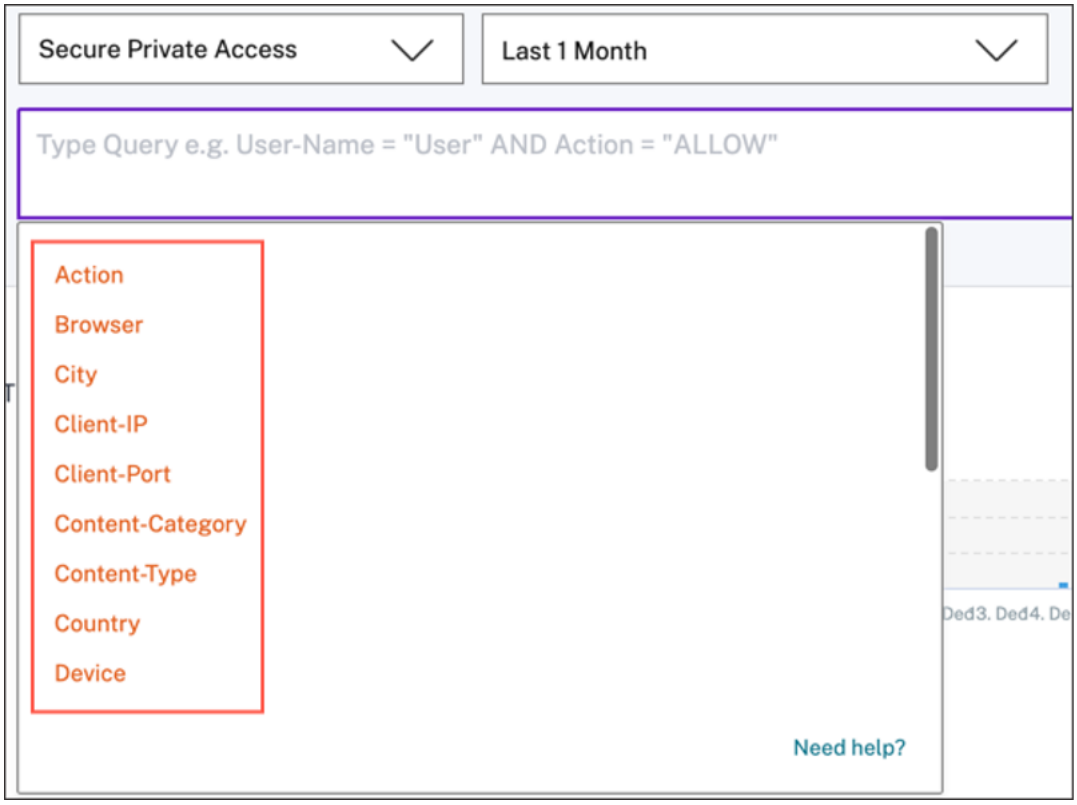
使用与 Secure Private Access 事件关联的以下方面。



- 操作-根据对用户应用程序执行的操作（例如允许、阻止和重定向）搜索事件。
- 国家/地区-根据用户的访问位置搜索事件。
- 内容类别-根据访问的内容类别（如应用程序、图像和文本）搜索事件。
- 请求-基于 HTTP 方法（例如 GET、POST、PUT、DELETE）搜索事件。
- 响应-根据 HTTP 响应搜索事件。
- 浏览器-根据用户使用的浏览器搜索事件。
- 设备-根据使用的设备（例如 Android 手机、iPhone、MacBook）搜索事件。
- 操作系统-根据设备上安装的操作系统搜索事件。

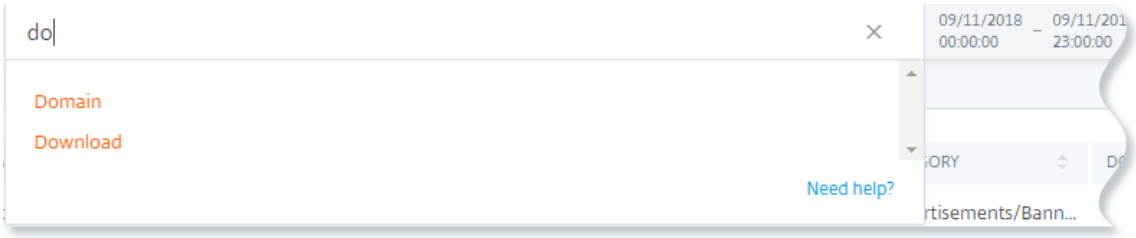
指定搜索查询以筛选事件

将光标置于搜索框中可查看 Secure Private Access 事件的维度列表。使用维度和 运算符 指定查询并搜索所需的事件。

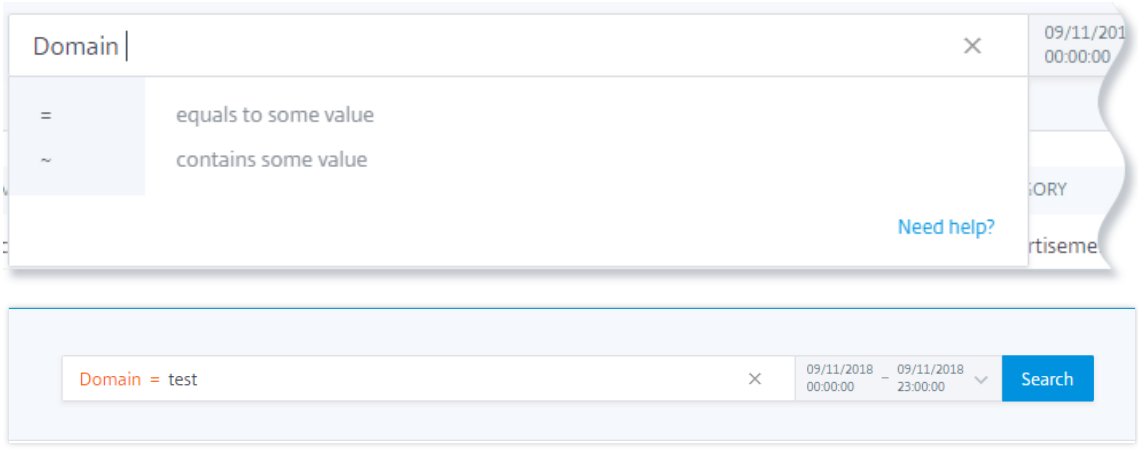


例如，您想查看数据下载量超过 2,000 字节的测试域。按以下方式指定搜索查询：

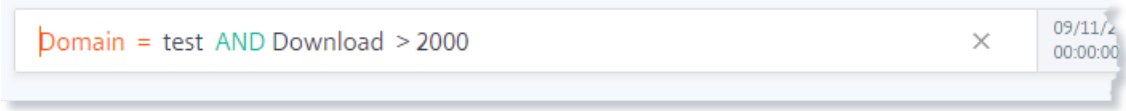
1. 在搜索框中输入“do”以获取相关建议。



2. 单击 域，然后使用等于运算符指定值“test”。



3. 使用 **AND** 运算符，然后选择“下 载”维度。选择 ** 运算符，然后输入下载量（以字节为单位）。



4. 选择时间段，然后单击“搜索”以查看 数据 表上的事件。

应用程序和桌面的自助式搜索

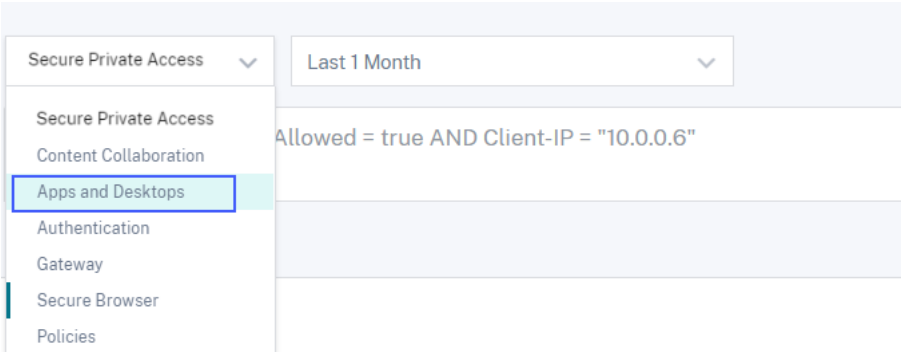
February 14, 2024

使用自助搜索深入了解从 Citrix Virtual Apps and Desktops 数据源和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）数据源收到的用户事件。当用户使用虚拟应用程序或虚拟桌面时，将生成与其活动和操作相对应的事件。用户事件的示例包括文件下载、帐户登录和应用程序启动。Citrix Analytics for Security 接收这些用户事件并将其显示在自助服务页面上您可以跟踪用户及其事件。

有关搜索功能的详细信息，请参阅 自助搜索。

选择应用程序和桌面数据源

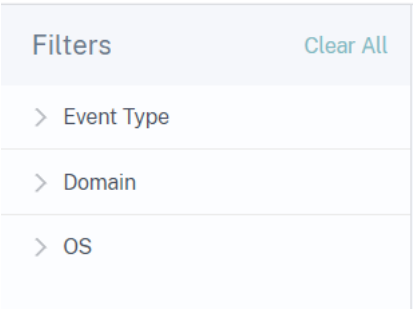
要查看来自 Citrix Virtual Apps and Desktops 或 Citrix DaaS 的事件，请从列表中选择应用程序和桌面。默认情况下，自助服务页面显示最近一天的事件。您还可以选择要查看事件的时间段。



默认情况下，自助服务页面会显示过去一个月的事件。该页面还为您提供了多个方面和一个搜索框，用于筛选和关注所需事件。

选择要过滤事件的平面

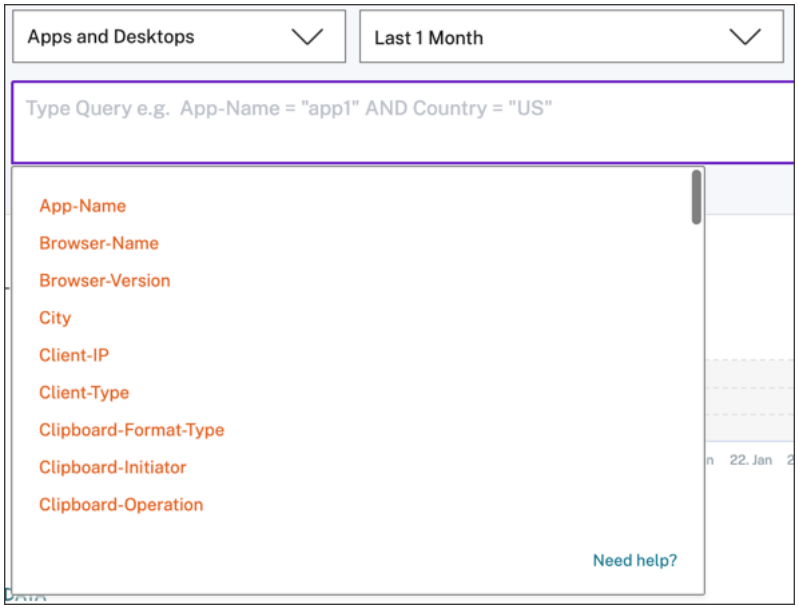
使用与应用程序和桌面事件关联的以下方面。



- 事件类型 - 根据帐户登录、应用程序结束和会话结束等事件类型搜索事件。
- 域-根据域（如 citrate.net）搜索事件。
- 操作系统-根据用户设备中使用的 **Chrome**、**iOS** 和 **Windows** 等操作系统搜索事件。选择操作系统名称和版本以筛选事件。有关操作系统版本的详细信息，请参阅 搜索查询支持的值。

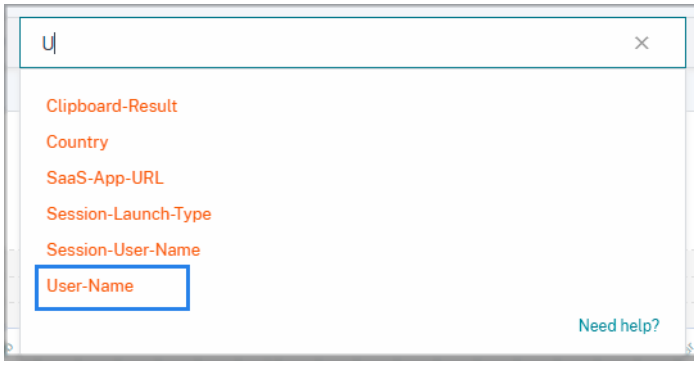
指定搜索查询以筛选事件

将光标置于搜索框中可查看应用程序和桌面事件的维度列表。使用维度和 运算符 指定查询并搜索所需的事件。

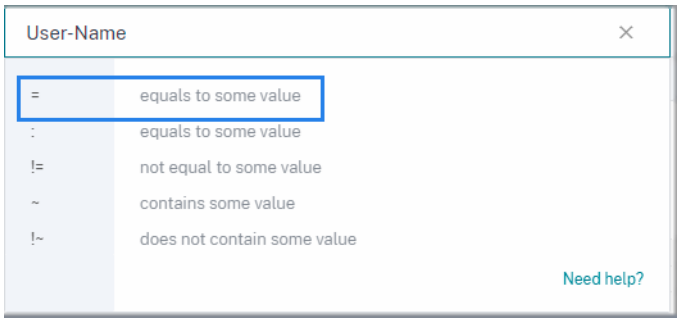


例如，您想要搜索正在使用 Windows 操作系统的用户“John Doe”的事件。

1. 在搜索框中输入“U”以获取相关建议。



2. 单击用 户名，然后使用等于运算符输入值“John”。



3. 选择 **AND** 运算符和操作 系统名称 维度。使用等于运算符分配值“Windows 7”。

```
User-Name = "John" AND OS-Name = "Windows 7"
```

4. 选择时间段，然后单击搜索以查看基于 **DATA** 表的事件。

事件类型和支持的字段

以下字段适用于除 vda.print 之外的所有事件类型：

- 城市
- 客户端 IP
- 国家/地区
- 设备 ID
- 操作系统名
- 操作系统版本
- OS 额外信息
- Time（时间）
- 用户名

- Workspace 应用程序版本
- Workspace 应用程序状态

下表描述了应用程序和桌面数据源中可用的事件类型以及每种事件类型的特定字段。

值	说明	字段
Account.Logon	当您通过 Citrix Workspace 应用程序登录应用商店时触发。注意：Account.Logon 不适用于 HTML5 客户端。	如上所述，检查常用字段。
Session.Logon	登录虚拟会话时触发。	应用程序保护策略、域、会话启动类型、会话服务器名称、会话用户名
Session.End	在您终止虚拟会话时触发。	域、会话启动类型、会话服务器名称、会话用户名
App.Start	当您启动虚拟应用程序会话时触发。注意：当应用程序在桌面会话中启动时，此事件类型不适用。	应用程序名称、域、会话启动类型、会话服务器名称、会话用户名
App.End	在您终止虚拟应用程序会话时触发。注意：当应用程序在桌面会话中启动时，此事件类型不适用。	应用程序名称、域、会话启动类型、会话服务器名称、会话用户名
File.Download	当用户将文件从远程虚拟会话复制到客户端设备时触发。虚拟会话中发生的文件传输不会被触发。注意：仅当服务器允许文件重定向（有关更多详细信息，请查看“文件重定向设置”）并且客户端工作区“文件访问”首选项设置为“读取和写入”时，才会发送此事件类型。	域、下载设备类型、下载文件名、下载文件路径、下载文件大小、会话服务器名称、会话用户名

值	说明	字段
Printing	当您使用 Citrix Workspace 应用程序通过客户端打印机启动的会话打印文件时触发。注意：Citrix Workspace 应用程序有两个影响打印事件的技术限制。首先，由于所有平台变体都存在已知问题，打印文档名称遥测未包含在打印事件中。其次，由于另一个已知的技术限制，打印文件大小遥测不包含在 Windows 的打印事件中。要收集这些数据集（文件名/文件大小），请使用 VDA.Print 事件。有关详细信息，请参阅为 Citrix DaaS 启用打印遥测。	浏览器名称、浏览器版本、域、打印机名称、打印文件格式、打印文件大小、会话服务器名称、会话用户名
AppProtection.ScreenCapture	当用户在受保护会话中尝试捕获屏幕截图时触发。注意：有关更多信息，请参阅 应用程序保护。	受保护的应用程序标题、屏幕捕获工具名称、屏幕捕获工具路径
App.SaaS.Launch	当 Citrix Workspace 应用程序在 Citrix Enterprise Browser 中启动 SaaS 应用程序时触发。	浏览器名称、浏览器版本、SaaS 应用程序名称、SaaS 应用程序 URL
App.SaaS.End	当 Citrix Workspace 应用程序在 Citrix Enterprise Browser 中关闭 SaaS 应用程序时触发。	浏览器名称、浏览器版本、SaaS 应用程序 URL
App.SaaS.Clipboard	在 Citrix Enterprise Browser 中执行剪贴板操作时触发。	浏览器名称、浏览器版本、剪贴板详细信息格式大小、剪贴板详细信息格式类型、剪贴板详细信息启动器、剪贴板详细信息结果、剪贴板操作、SaaS 应用程序 URL
App.SaaS.File.Download	在 Citrix Enterprise Browser 中下载文件时触发。	浏览器名称、浏览器版本、下载设备类型、下载文件路径、下载文件大小
App.SaaS.File.Print	在 Citrix Enterprise Browser 中启动打印时触发。	浏览器名称、浏览器版本、打印文件名、SaaS 应用程序名称、SaaS 应用程序 URL
App.SaaS.Url.Navigate	在 Citrix Enterprise Browser 浏览 URL 时触发。	浏览器名称、浏览器版本、SaaS 应用程序名称、SaaS 应用程序 URL
Citrix.EventMonitor.AppStart	当添加到会话录制服务器的 应用程序监视列表中的应用程序 在虚拟桌面会话中启动时触发。	应用程序名称

值	说明	字段
Citrix.EventMonitor.AppEnd	当添加到会话录制服务器的 应用程序监视列表）在虚拟桌面会话中停止时触发。	应用程序名称
Citrix.EventMonitor.Clipboard	在会话录制中执行剪贴板操作时触发。	剪贴板数据格式类型、进程名称、窗口标题
Citrix.EventMonitor.FileTransfer	当用户在虚拟桌面会话和用户计算机之间传输文件时触发。	文件大小、操作方向（主机到客户端、客户机到主机）、源路径、目标路径
Citrix.EventMonitor.RegistryChange	在执行注册表操作时触发。可能的注册表操作包括创建、删除、重命名、设置值和删除值。	注册表操作、注册表名称、注册表路径、进程 ID、进程文件路径
Citrix.EventMonitor.SessionEnd	会话录制结束时触发。	说明
Citrix.EventMonitor.SessionLaunch	会话录制开始时触发。	会话录制类型
Citrix.EventMonitor.TopMost	当最上面的窗口发生变化时触发。	应用程序名称
Citrix.EventMonitor.IdleStart	会话变为空闲时触发。	如上所述，检查常用字段。
Citrix.EventMonitor.IdleEnd	空闲会话结束时触发。	如上所述，检查常用字段。
Citrix.EventMonitor.WebBrowsing	当用户在虚拟桌面会话中与浏览器上的网页进行交互时触发。	应用程序名称、网址
Citrix.EventMonitor.FileCreate	在受监视文件系统路径内的虚拟桌面会话中创建文件或文件夹时触发。	文件名、文件路径、文件大小
Citrix.EventMonitor.FileRename	在受监视文件系统路径内的虚拟桌面会话中重命名文件或文件夹时触发。	如上所述，检查常用字段。
Citrix.EventMonitor.FileMove	在虚拟桌面会话中或会话主机 (vDA) 与客户端设备之间移动受监视文件系统路径中的文件或文件夹时触发。	如上所述，检查常用字段。
Citrix.EventMonitor.FileDelete	在虚拟桌面会话中删除受监视文件系统路径中的文件或文件夹时触发。	文件名、文件路径、文件大小
Citrix.EventMonitor.CDMUSBDriveAttach	在连接虚拟应用程序和桌面会话的客户端中插入客户端驱动器映射 (CDM) 映射的 USB 大容量存储设备时触发。	如上所述，检查常用字段。

值	说明	字段
Citrix.EventMonitor.GenericUSBDriveAttach	在连接虚拟应用程序和桌面会话的客户端中插入通用重定向 USB 大容量存储设备时触发。	如上所述，检查常用字段。
Citrix.EventMonitor.RDPConnection	当用户在 VDA 计算机中创建远程桌面连接时触发。	目标 IP，进程 ID
Citrix.EventMonitor.UserAccountModification	触发所有类型的用户帐户操作，包括帐户创建、启用、禁用、删除、名称更改和密码修改。	描述，目标用户名
VDA.Print	在应用程序和桌面中启动打印作业时触发。注意：此事件仅适用于 Citrix DaaS 数据源。有关详细信息，请参阅为 Citrix DaaS 启用打印遥测。	文档用户名、计算机名称、打印文件名、打印文件大小、打印机名称、时间、打印总份数、打印总页数
VDA.Clipboard	在应用程序和桌面中执行剪贴板操作时触发。注意：此事件仅适用于 Citrix DaaS 数据源。有关更多信息，请参阅为 Citrix DaaS 启用剪贴板遥测。	剪贴板格式类型、剪贴板操作、剪贴板操作方向、允许的剪贴板操作、剪贴板大小、计算机名称

> 注意
>
> 所有会话录制事件都要求在会话录制服务器上启用记录其事件的策略。有关详细信息，请参阅创建自定义事件检测策略。

搜索查询支持的值

为维度输入以下值以定义搜索查询。

维度	值	类型	说明
App-Name	应用程序或桌面会话。 示例应用程序会话：没有服务器场名称的会话：#Cloud - Excel 2016 以及具有服务器场名称的会话：XA65PROD#Concur	字符串	启动的应用程序或桌面的名称。

维度	值	类型	说明
	桌面会话示例：没有场名称的会话：#SINXIAP0616 $S1-1 以及带有场名称的会话：XA65PROD# SINXIAP0616 $S1 -1		
App-Protection-Policies	示例：AntiScreenCaptureEnabled	字符串	会话的有效应用程序保护策略。
Browser-Name	示例：Google Chrome、Citrix Enterprise Browser、Microsoft Edge、FIREFOX、SAFARI	字符串	浏览器名称
Browser-Version	示例：80.0.3987.122、101.0.9999.0	字符串	浏览器版本
City	示例：圣克拉拉、休斯敦、芝加哥	字符串	用户的城市名称。
Client-IP	一个 IP 地址。示例：10.10.10.10	字符串	用户终端节点的 IP 地址。
Client-Type	Android、Windows、Macintosh、Chrome、HTML5、Unix/Linux、iOS、SessionRecording、Monitor	字符串	表示基于操作系统或原始数据源的不同类型的 Citrix Workspace 应用程序。
Clipboard-Format-Type	示例：文本、html、CF_UNICODETEXT	字符串	复制到剪贴板的数据格式。
Clipboard-Initiator	示例：键盘、上下文菜单、JavaScript	字符串	指示剪贴板操作是如何启动的。注意：只有 SaaS 应用程序支持。

维度	值	类型	说明
Clipboard-Operation	复制、剪切、粘贴或置入	字符串	指示执行哪个剪贴板操作。注意：置 入操作表示数据已放置在剪贴板上。这不能保证剪贴板中的数据是否由客户端粘贴或使用。此操作仅支持 VDA.Clipboard 事件。
Clipboard-Operation-Direction	客户机到主机，主机到客户端	字符串	指示剪贴板的操作方向。注意：仅 Apps and Desktop (Citrix DaaS) 剪贴板操作支持。
Clipboard-Operation-Permitted	允许或拒绝	字符串	表示是否允许在应用程序和桌面会话中执行剪贴板操作。注意：仅 Apps and Desktop (Citrix DaaS) 剪贴板操作支持。
Clipboard-Result	成功或已阻止	字符串	表示剪贴板操作的结果。注意：只有 SaaS 应用程序支持。
Clipboard-Size	示例：10、20	数量	当前存储在剪贴板中的数据的大小（以字节为单位）。
Country	示例：美国、印度	字符串	用户的国家/地区名称。
Description	对于 **Citrix.EventMonitor.UserAccountModification** 事件：创建了用户帐户，启用了用户帐户，尝试重置帐户的密码。	字符串	描述用户帐户修改状态，例如帐户已创建、删除、重命名或尝试重置密码。
	适用于 **Citrix.EventMonitor.SessionEnd** 事件：未知、注销、翻转、触发和未完成		描述会话录制结束的原因。
Destination-IP	示例：10.60.110.xxx	字符串	远程桌面的 IP 地址。
Destination-Path	示例：\H$\Desktop\Folder\example.txt	字符串	传输完成后文件的最终路径。

维度	值	类型	说明
Device-ID	示例：cb781185-18ad-4f45-b75f	字符串	用于许可、客户端名称或操作系统硬件 ID 的设备 ID。
Domain	示例：example.com	结构	发送请求的服务器的域名。
Download-Device-Type	示例：USB、硬盘驱动器、RemoteDrive、cdrom 或浏览器下载。	字符串	下载或传输文件的设备类型。
Download-File-Format	示例：txt、PDF、xlsx、docx	字符串	下载的文件的格式。
Download-File-Name	示例：example-file.txt	字符串	下载文件的名称。
Download-File-Path	示例：C:\Users\admin\Desktop	字符串	下载文件的路径。
Download-File-Size	示例：8.05	数量	已下载文件的大小（以千字节为单位）。

维度	值	类型	说明
Event-Type	Account.Logon, Session.Logon, Session.End, App.Start, App.End, File.Download, Printing, AppProtection.ScreenCapture, App.SaaS.Launch, App.SaaS.End, App.SaaS.Clipboard, App.SaaS.File.Download, App.SaaS.File.Print, App.SaaS.Url.Navigate, Citrix.EventMonitor.AppStart, Citrix.EventMonitor.AppEnd, Citrix.EventMonitor.TopMost, Citrix.EventMonitor.WebBrowsing, Citrix.EventMonitor.FileCreate, Citrix.EventMonitor.FileRename, Citrix.EventMonitor.FileMove, Citrix.EventMonitor.FileDelete, Citrix.EventMonitor.CDMUSBDriveAttach, Citrix.EventMonitor.GenericUSBDriveAttach, Citrix.EventMonitor.RDPConnection, Citrix.EventMonitor.UserAccountModification, VDA.Print, VDA.Clipboard, Citrix.EventMonitor.RegistryChange, Citrix.EventMonitor.SessionLaunch, Citrix.EventMonitor.SessionEnd,	字符串	有关更多详细信息，请参阅事件类型和支持的字段。

维度	值	类型	说明
Jail-Broken	是或否	字符串	指示设备是否已获得 root 用户权限。注意：如果不存在此维度，则设备未获得 root 权限。此密钥适用于适用于 iOS 和 Android 设备的 Citrix Workspace 应用程序。
Operation-Direction	主机到客户机/客户机对主机	字符串	表示文件传输的方向。
OS-Extra-Info	示例：20G80，Service Pack 1，19043	字符串	表示操作系统的其他信息，例如内部版本号、服务包和补丁。
OS-Name	示例：macOS 11、Windows 7、Android 8.1、Windows 10 Enterprise	字符串	表示操作系统的名称。
OS-Version	示例：11.5.1、14.7.1、2009	字符串	表示操作系统的版本
Print-File-Format	示例：PDF、PS、DOCX	字符串	打印文件的格式。
Print-File-Name	示例：example-file.pdf	字符串	打印文件的名称。
Print-File-Size	示例：10、20	字符串	打印文件的大小（以字节为单位）。
Printer-Name	示例：testprester-1	字符串	使用的打印机的名称。
Process-ID	示例：11248	字符串	指进程 ID，用于识别执行以下两项操作的特定进程：创建新进程 和 建立远程桌面连接。Process-ID 目前仅与 Citrix.EventMonitor.RDPConnection 事件相关联。
Protected-App-Titles	示例：管理员桌面-Citrix Workspace	字符串	在受保护会话中运行的应用程序的名称。
Registry-Name	修改后的注册表的名称	字符串	修改后的注册表的名称。
Registry-Operation	重命名、创建、删除、设置值、删除值	字符串	表示执行了哪个注册表操作。

维度	值	类型	说明
Registry-Path	修改后的注册表的路径	字符串	修改后的注册表的路径。
SaaS-App-Name	示例：Workday	字符串	SaaS 应用程序的名称。
SaaS-App-URL	示例：https://xyz.com|String	字符串	SaaS 应用程序的 URL 或网关/代理 URL。注意：最初启动 SaaS 应用程序时，网关/代理 URL 会出现在 App.SaaS.Launch 事件中。
Screen-Capture-Tool-Name	示例：ScreenShotTool.exe	字符串	屏幕捕获工具的名称。
Screen-Capture-Tool-Path	示例：c:\Program files (x86)\ScreenContent Client	字符串	屏幕捕获工具的路径。
Session-Launch-Type	应用程序或桌面	字符串	指示启动的会话是应用程序还是桌面类型。
Session-Recording-Type	传统录制/仅限活动录制	字符串	表示已启动的会话录制的类型。
Session-Server-Name	示例：托管桌面、云 VDA-1	字符串	从服务器接收到的应用程序或桌面的名称。
Session-User-Name	示例：演示用户、测试用户	字符串	从服务器收到的用户名。
Source-Path	示例：C:\Users\admin\Desktop\example.txt	字符串	文件传输前的初始路径。
Target-User-Name	示例：user01	字符串	目前，Target-User-Name 仅用于 Citrix.EventMonitor.UserAccountModif 事件，在该事件中，修改的是用户帐户。
Total-Copies-Printed	示例：1、2	数量	用户打印的总份数。
Total-Pages-Printed	示例：1,2	数量	用户打印的文档总页数。

维度	值	类型	说明
User-Name	用户名或域\ 用户名	字符串	用户名或域\ 用户名。用于 StoreFront 登录。如果 StoreFront 登录不是通过适用于 HTML5 或 Chrome 的 Citrix Workspace 应用程序，则此值与从服务器接收的值相同。
VDA-Name	示例：TSVDA-19-01.xd.local	字符串	指示 VDA 计算机的名称。
Window-Title	示例：管理员 - 01 命令提示符	字符串	表示执行剪贴板操作的窗口的标题。
Workspace-App-Version	示例：20.8.0.3 (2008)	字符串	安装在用户设备上的 Citrix Workspace 应用程序或 Citrix Receiver 版本，用于启动远程虚拟应用程序和桌面会话。
Workspace-App-Status	支持或不支持	字符串	指示 Citrix Analytics for Security 是否支持用户设备上安装的 Citrix Workspace 应用程序或 Citrix Receiver 版本。当不支持 Workspace 应用程序时，将鼠标悬停在“不支持”上。将出现一个弹出窗口，其中包含查看支持版本列表的链接。当 Workspace 应用程序版本接近其不支持状态时，自助搜索页面上会显示一个横幅，列出您可以启动升级的可用支持版本。

操作系统命名格式

Citrix Analytics 接收用户设备的操作系统 (OS) 详细信息，并将其转换为操作系统名称、操作系统版本和操作系统额外信息。

- 操作系统名 称表示操作系统的名称。
- 操作系统版本 表示操作系统的发行 ID 或发行版本。
- **OS Extra Info** 表示操作系统的其他信息，例如内部版本号、服务包和修补程序。

下表提供了操作系统版本编号格式的几个示例。

操作系统名	操作系统版本	OS 额外信息
macOS 11	11.5.1	20G80
iOS 14	14.7.1	不可用
Windows 10 Enterprise	2009	19043
Windows 7	6.1	Service Pack 1
Android 8.1	8.1.0	不可用

> 备注
>
> - 要获取 Mac 版本 11.x 或更高版本的操作系统详细信息，建议使用适用于 Mac 2108 或更高版本的 Citrix Workspace 应用程序的客户端版本。
> - Windows 10 的操作系统详细信息目前不可用。

Citrix Analytics for Security 和 Citrix Analytics for Performance 故障排除

December 7, 2023

本节介绍了如何解决在使用 Citrix Analytics for Security 时可能遇到的以下问题。

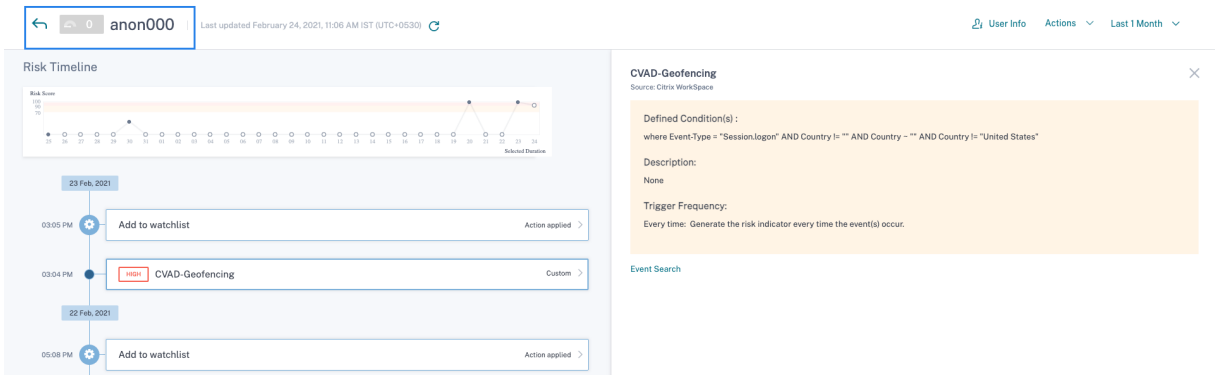
- 将匿名用户验证为合法用户。
- 排查来自数据源的事件传输问题。
- 触发 Virtual Apps and Desktops 事件、SaaS 事件，并验证事件传输到 Citrix Analytics for Security。
- Session Recording 服务器无法连接。
- 适用于 Splunk 的 Citrix Analytics 加载项存在配置问题

验证匿名用户为合法用户

July 12, 2022

作为管理员，您可能会注意到某些 Citrix Virtual Apps and Desktops
用户和 Citrix DaaS（以前是 Citrix Virtual Apps and Desktops 服务）用户在 Citrix Analytics for Security 上显示为匿名用户。这些用户被标识为已发现的用户。但是他们的用户名在以下页面上显示为 anonXYZ（其中“XYZ”表示三位数字）：

- 用户
- 用户的时间表
- 有风险的用户
- 自助搜索 Apps and Desktops 数据源



当你看到这样的用户时，你可能想知道：

- 这些用户是谁?
- 这些用户本质上是合法还是恶意的?
- 如何验证它们?
- 我必须为这些用户申请哪些操作?

在以下情况下，您可以在 Citrix IT 环境中看到匿名用户：

- 当用户使用已发布的安全浏览器应用程序时

- 当用户使用未经身份验证的商店时

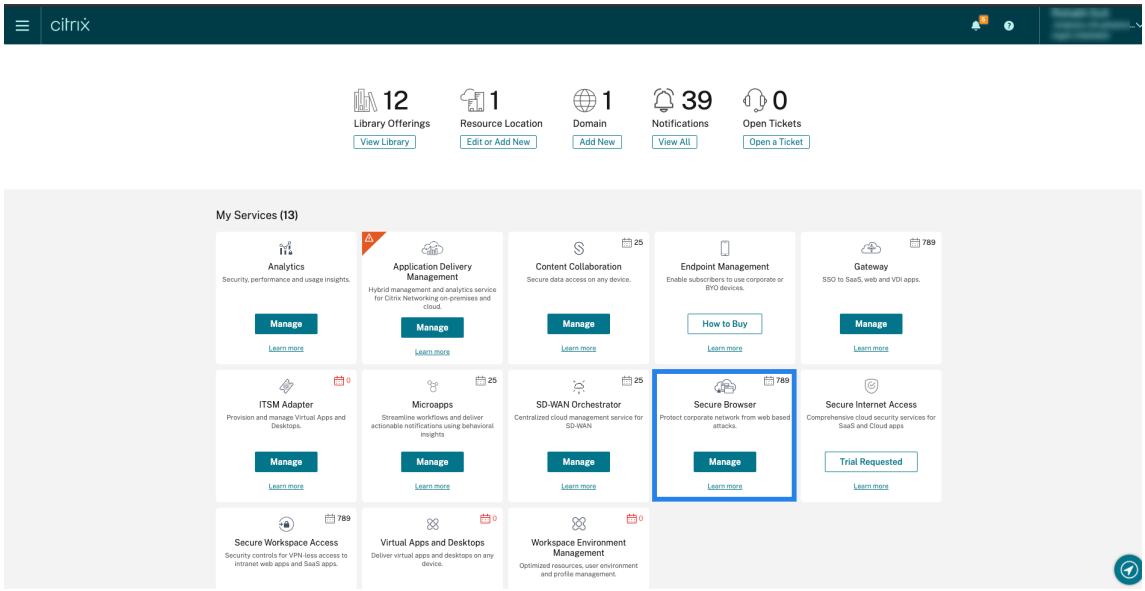
使用已发布的安全浏览器应用

安全浏览器应用程序是使用 Citrix Secure Browser 服务发布的 Web 应用程序。这些应用程序隔离您的 Web 浏览事件，保护您的公司网络免受基于浏览器的攻击。有关详细信息，请参阅 安全浏览器服务。

安全浏览器应用程序使用 Citrix DaaS 的匿名会话功能。

要验证 Citrix Cloud 帐户是否配置了安全浏览器，请执行以下操作：

1. 登录 Citrix Cloud。
2. 在 安全浏览器 卡上，单击 管理。



3. 在 管 理页面上，检查已发布的安全浏览器应用程序。

如果用户使用 Web 浏览器通过 Citrix Receiver for Web 站点访问 StoreFront 应用商店并使用已发布的安全浏览器应用程序，则该用户的身份将隐藏。因此，Citrix Analytics 会将用户显示为匿名。

如果用户通过安装在其设备上的 Citrix Receiver 或 Citrix Workspace 应用程序访问 StoreFront 应用商店并使用已发布的安全浏览器应用程序，Citrix Analytics 将该用户显示为 StoreFront 中指定的用户名。

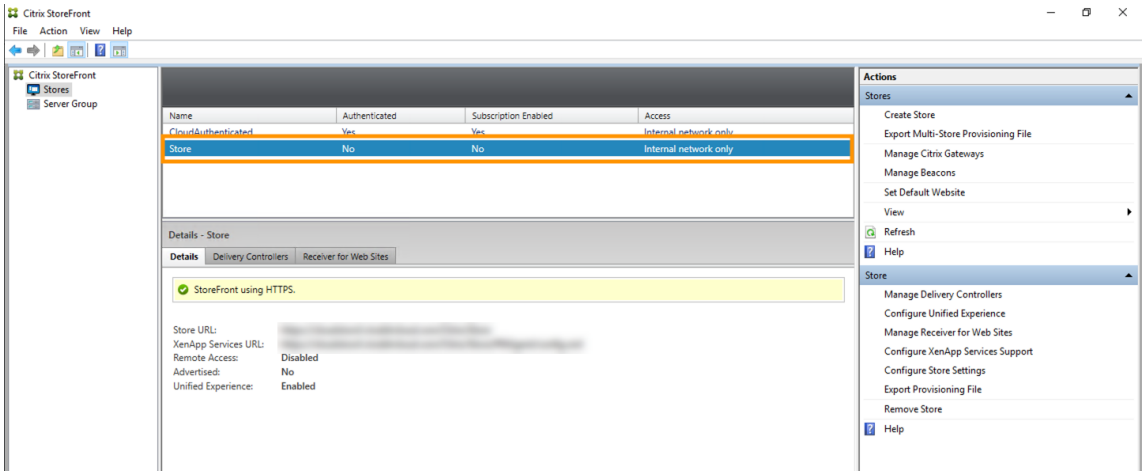
因此，您可以将该用户视为组织的合法用户。如果没有与用户相关的危险行为，则无需应用任何操作。

用户使用未经身份验证的商店

未经身份验证的应用商店是 Citrix StoreFront 的一项功能，适用于客户管理的商店。此功能支持未经身份验证（匿名）用户的访问权限。

要验证组织是否有未经身份验证的商店，请执行以

1. 启动 Citrix Studio。
2. 点击 商店。
3. 对于您的商店，请在已验证列中检查身份验证状态。



如果商店未经过身份验证且用户正在访问该未经身份验证的应用商店，则用户身份将保持匿名。因此，Citrix Analytics 会将用户显示为匿名。您可以将此用户视为组织的合法用户。如果没有与用户相关的危险行为，则无需应用任何操作。

解决数据源的事件传输问题

April 12, 2024

本节帮助您解决 Citrix Analytics for Security 中的数据传输问题。当数据源无法准确传输用户事件时，您可能会遇到未发现用户和风险指示器等问题。

清单

序列	检查
1	您是否拥有使用 Security Analytics 的正确权利?
2	您所在的区域是否支持该数据源?
3	您的环境是否满足所有系统要求?
4	是否在 Analytics 上发现了所有数据源并启用了数据处理?
5	数据源上的用户活动是否将事件准确地传输到 Analytics?
6	虚拟应用程序和桌面事件是否会传输到 Analytics?
7	用户事件是否显示在 Analytics 的自助搜索页面上?
8	用户是否被 Analytics 发现?

检查 **1 -** 您是否拥有使用 **Security Analytics** 的正确权利

Citrix Analytics for Security 是一项基于订阅的产品。有关更多信息，请参阅 入门。

检查 **2-**您的本地区域是否支持数据源

以下主区域支持 Citrix Analytics for Security：

- 美国 (US)
- 欧洲联盟（EU）
- 亚太南部 (APS)

根据组织所在的位置，您可以在其中一个主区域加入 Citrix Cloud。

但是，并非所有主区域都支持某些数据源。[数据源](/en-us/security-analytics/data-sources.html)）是 Citrix Analytics for Security 从中接收用户事件的产品。

如果您的组织在不支持数据源的主区域中加入了 Citrix Cloud，则不会从数据源获取用户事件。

使用下表查看数据源及其受支持的区域。

数据源	在美国地区受支持	在欧盟地区受支持	APS 区域支持
Citrix Endpoint Management	是	是	是
Citrix Gateway（本地）	是	是	是

数据源	在美国地区受支持	在欧盟地区受支持	APS 区域支持
Citrix 身份提供程序	是	是	是
Citrix Secure Browser	是	是	是
Citrix Secure Private Access	是	否	否
Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）	是	是	是
Citrix Virtual Apps and Desktops 本地	是	是	是
Microsoft Active Directory	是	是	是
Microsoft Graph 安全性	是	是	是

检查 **3-**您的环境是否满足所有系统要求

Citrix Analytics 可能需要几分钟时间才能从数据源接收用户事件。如果在数据源站点卡上看不到任何用户事件，请确保您的环境满足必备条件和 系统要求。

必备条件

1. 您的所有 Citrix Cloud 订阅都必须处于活动状态。在 Citrix Cloud 页面上，确保所有 Citrix Cloud 服务均处于活动状态。
2. 如果使用本地部署 Citrix Virtual Apps and Desktops，则必须将站点添加到 Citrix Workspace 并配置站点聚合。Citrix Analytics 会自动发现添加到 Citrix Workspace 的站点。有关更多信息，请参阅 聚合工作区中的本地虚拟应用程序和桌面。
3. 如果要为站点使用 StoreFront 部署，请将 StoreFront 服务器配置为使 Citrix Workspace 应用程序能够向 Citrix Analytics 发送用户事件。确保 StoreFront 版本为 1906 或更高版本。如果不配置 StoreFront 服务器，Citrix Analytics 将无法从本地 Citrix Virtual Apps and Desktops 接收用户事件。要配置 StoreFront 部署，请参阅 StoreFront 文档中的 Citrix Analytics Service 一文。
4. Citrix Virtual Apps and Desktops 用户和 Citrix DaaS 用户必须在其端点使用指定版本的 Citrix Workspace 应用程序或 Citrix Receiver。否则，Analytics 不会从用户端点接收用户事件。Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源中提供了受支持的 Citrix Workspace 应用程序或 Citrix Receiver 版本列表。
5. 要从已发布的安全浏览器会话中接收用户的事件，请在安全浏览器中启用 主机名跟踪 设置。默认情况下，禁用此设置。有关更多信息，请参阅管理已发布的安全浏览器。

6. 如以下文章所述，载入数据源：

   - Citrix Endpoint Management 数据源
   - Citrix Gateway 数据源
   - Citrix Secure Private Access 数据源
   - Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源
   - Microsoft Active Directory 集成
   - Microsoft Graph 安全性集成

检查 **4-Analytics** 上是否发现了所有数据源并启用了数据处理

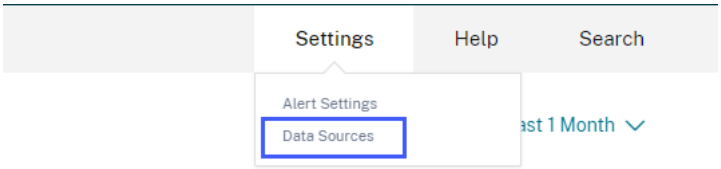
确保已发现所有数据源，并且已为它们启用了数据处理。如果不为数据源启用数据处理，则不会发现使用该数据源的用户。这种情况可能会造成潜在的安全风险。

启用数据处理可确保 Citrix Analytics 正在处理您的用户事件。只有在用户主动使用数据源时，才会将事件发送到 Citrix Analytics。

> 注意
>
> Citrix Analytics 不会主动从您的环境中提取数据。

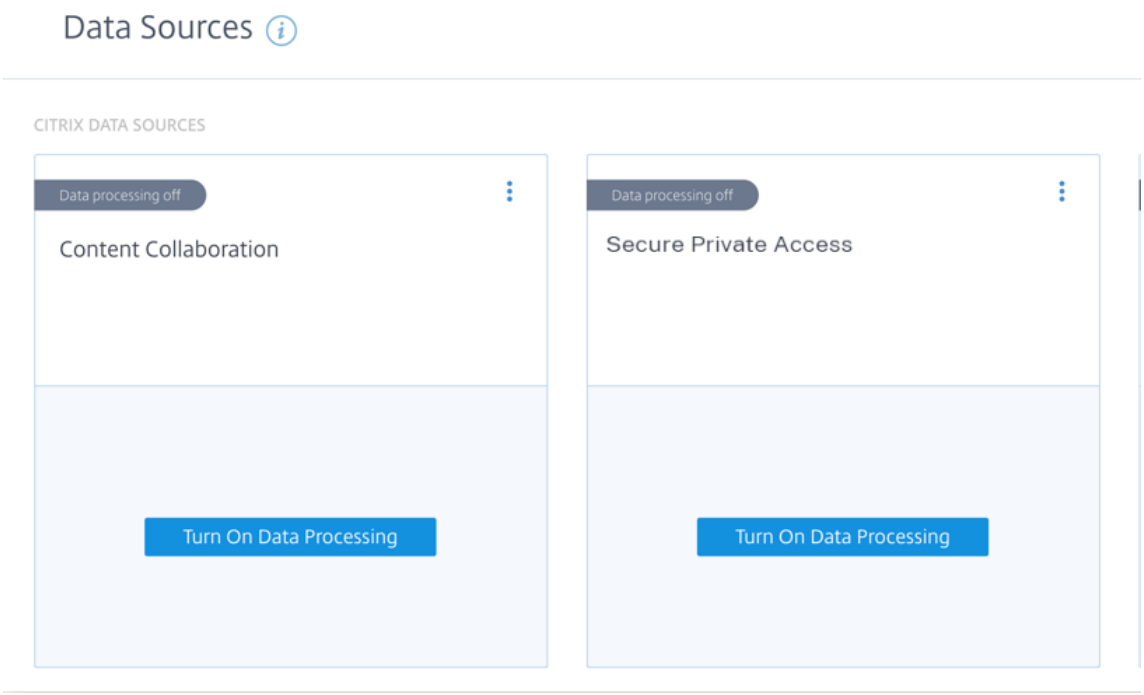
要发现数据源并启用分析，请执行以下操作：

1. 单击“设置”>“数据源”>“安全”以查看发现的数据源。Citrix Analytics 会自动发现您已订阅 Citrix Cloud 账户的数据源。

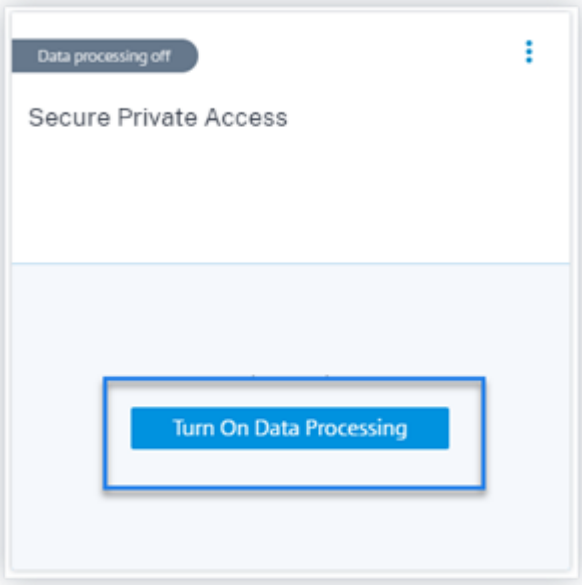


2. 在“数据源”页面上，发现的数据源将显示为站点卡。默认情况下，数据处理处于关闭状态。

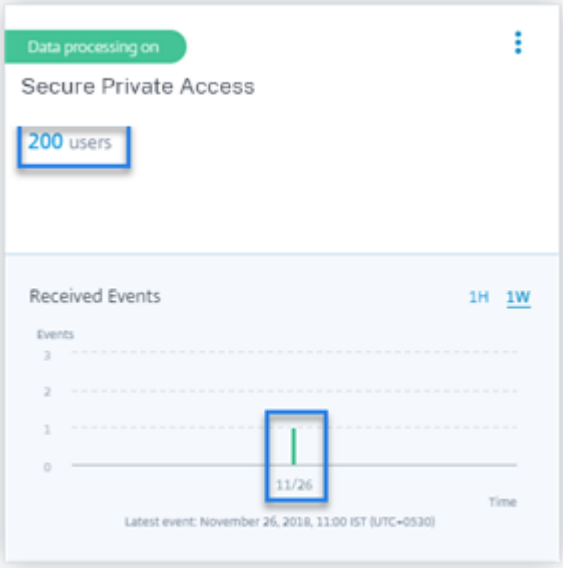
   > 重要提示
   >
   > Citrix Analytics 会在您同意后处理您的数据。



3. 在希望 **Citrix Analytics** 为其处理事件的站点卡片上，单击打开数据 处理。例如，在 Citrix Secure Private Access 站点卡片上，单击“打开数据处理”。



4. 打开数据处理功能后，Citrix Analytics 将处理数据源的事件。网站卡的状态更改为数据处理。您可以根据所选时间段查看用户数量和接收的事件。



5. 对于所有发现的数据源，请按照 入门 中指定的步骤启用分析。

检查 **5-**数据源上的用户活动是否将事件准确地传输到 **Analytics**

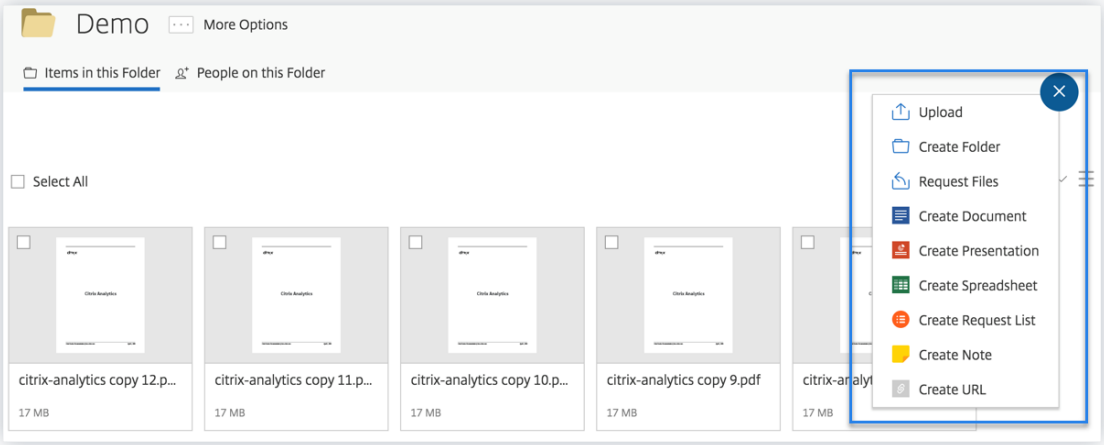
当用户主动使用数据源时，Citrix Analytics 会从数据源接收用户事件。用户必须在数据源上执行某些活动才能生成事件。例如，要接收来自应用程序和桌面数据源的事件，应用程序和桌面用户必须共享、上传或下载某些文件。

> 注意
>
> Citrix Analytics 不会主动从您的环境中提取数据。

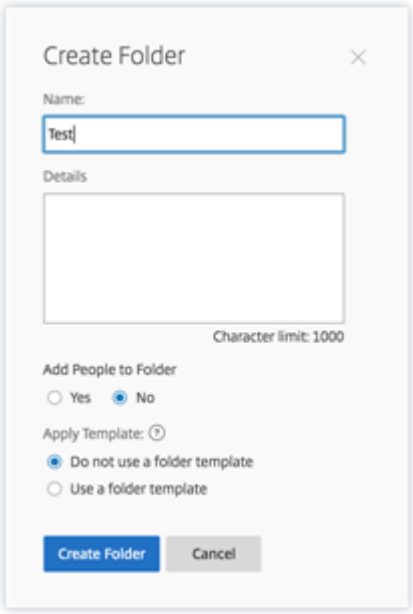
如果您在 Citrix Analytics 中看不到数据源的任何用户事件，则用户很有可能此时未处于活动状态。

要验证 Citrix Analytics 是否准确地接收了用户事件，请执行以下活动。此活动使用 Citrix 应用程序和桌面数据源。您可以根据您的订阅使用其他 Citrix 产品（数据源）执行类似的活动。

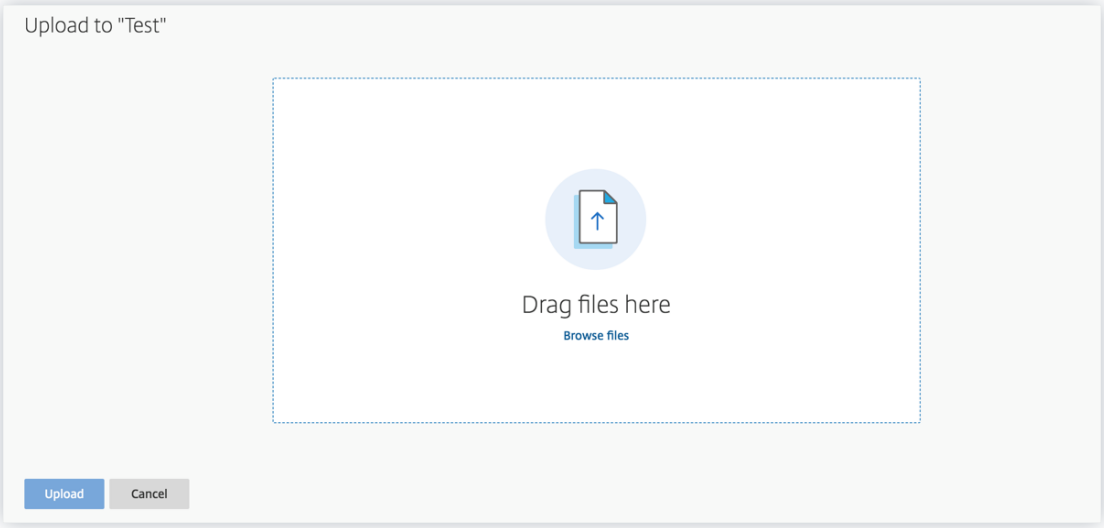
1. 登录 Citrix 应用程序和桌面服务。
2. 执行一些常见的用户活动，例如创建文件夹、下载文件、上传文件或删除文件。



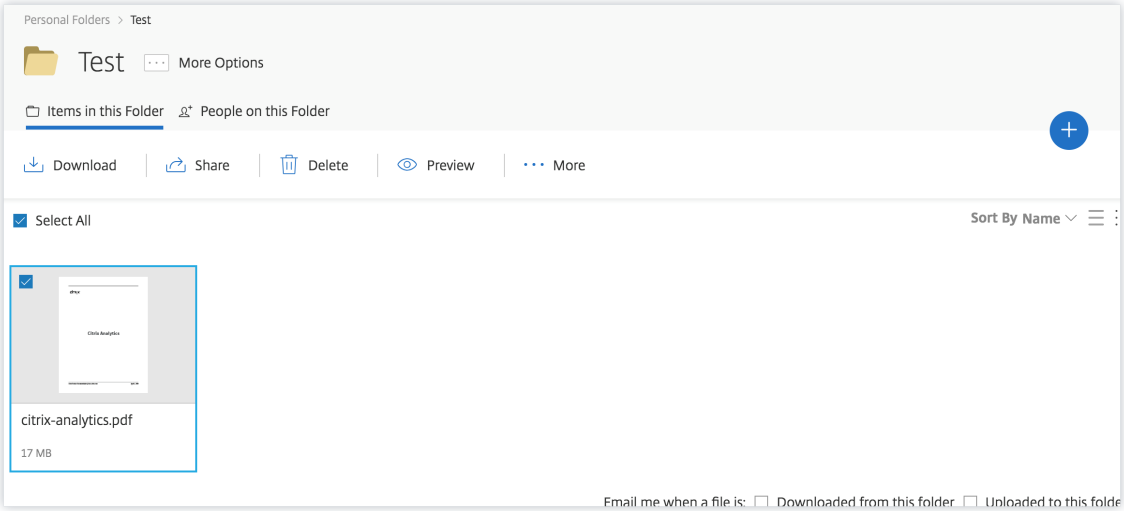
3. 例如，创建一个 Test 文件夹。



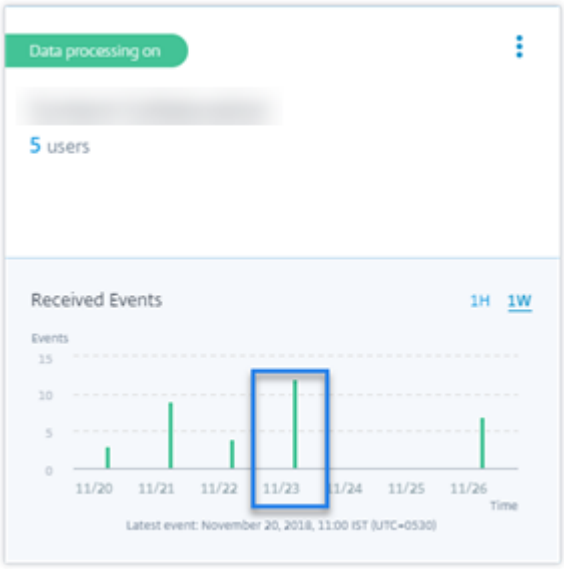
4. 上载一些本地文件。



5. 删除文件夹中的一些文件。



6. 返回 Citrix Analytics，在“数据源”页面上查看“应用程序和桌面”侧卡。Citrix Analytics 接收来自应用程序和桌面数据源的用户事件，并将其显示在网站卡上。



检查 **6**：虚拟应用程序和桌面事件是否传输到 **Analytics**

某些版本的 Citrix Workspace 应用程序或 Citrix Receiver 客户端无法向 Citrix Analytics 发送用户事件。当用户通过这些客户端启动虚拟应用程序和桌面时，Citrix Analytics 无法发现用户，直到他们执行受支持的事件。

例如，适用于 Linux 2006 或更高版本的 Citrix Workspace 应用程序不会将 ***SaaS*** 应用程序启动 和 ***SaaS*** 应用程序结束 事件发送到 Citrix Analytics。Citrix Analytics 上未发现使用适用于 Linux 的 Citrix Workspace 应用程序启动 SaaS 应用程序的用户。

支持的事件

请参阅下表以查看每个客户端版本支持的用户事件。

- 是-事件由客户端发送给 Citrix Analytics。
- 否-客户端不会将事件发送给 Citrix Analytics。
- 不适用-该事件不适用于客户端。

事件	适用于 Windows 的 Workspace 应用程序 1907 或更高版本	适用于 Mac 的 Workspace 应用程序 1910.2 或更高版本	适用于 Linux 的 Workspace 2006 或更高版本	适用于 Android 的 Workspace 应用程序 - Google Play 中提供的最新版本	适用于 iOS 的 Workspace 应用程序 - Apple App Store 中提供的最新版本	适用于 Chrome 的 Workspace 应用程序 - Chrome 网上应用店中提供的最新版本	适用于 HTML5 的 Workspace 2007 或更高版本
帐户登录	是	是	是	是	是	否	否
会话登录	是	是	是	是	是	是	是
会话启动	是	是	是	是	是	是	是
会话结束	是	是	是	是	是	是	是
应用程序启动	是	是	是	否	是	是	是
应用程序结束	是	是	是	否	是	是	是
文件下载	是	是	是	否	否	是	是
打印	否	是	是	否	否	是	是
SaaS 应用程序启动	是	是	否	否	否	否	否
SaaS 应用程序结束	是	是	否	否	否	否	否
SaaS 应用程序 URL 导航	是	是	否	否	否	否	否
SaaS 应用剪贴板访问	是	是	否	否	否	否	否
SaaS 应用程序文件下载	是	是	否	否	否	否	否
SaaS 应用程序文件打印	是	是	否	否	否	否	否

根据事件传输状态，您可能会遇到以下问题：

- 当用户使用其客户端连接到 Citrix Virtual Apps and Desktops 或 Citrix DaaS 时，在执行受支持的事件（活

动）之前，用户可能不会在 Citrix Analytics 中被发现。例如，考虑两个用户事件-应用程序启动和 SaaS 应用程序启动。使用适用于 iOS 的 Citrix Workspace 应用程序的用户，Citrix Analytics 会收到应用程序启动事件，但不接收 SaaS 应用程序启动事件。因此，当用户启动任何虚拟应用程序时，应用程序启动事件都会传输到 Citrix Analytics，然后发现该用户。但是，如果用户启动 SaaS 应用程序，Citrix Analytics 将不会收到 SaaS 应用程序启动事件，也不会发现该用户。有关已发现用户的信息，请参阅 发现的用户。

- 表格上标记为“否”的事件不会显示在自助搜索页面上。有关如何使用自助服务页面的信息，请参阅 关于自助搜索。

建议

为了获得分析的最大优势，Citrix 建议采取以下措施：

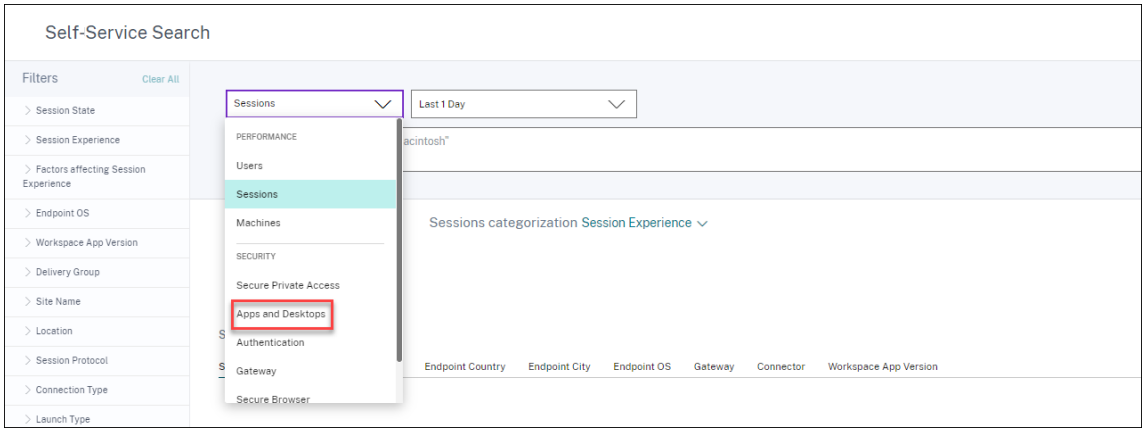
- **Windows** 用户：使用适用于 Windows 的 Citrix Workspace 应用程序 1907 或更高版本连接到您的 Citrix Virtual Apps and Desktops 和 Citrix DaaS。
- **Mac** 用户：Citrix Virtual Apps and Desktops 和 Citrix DaaS 使用适用于 Mac 1910.2 或更高版本的 Citrix Workspace 应用程序连接到你的。

检查 **7-**用户事件是否显示在 **Analytics**（分析）的自助搜索页面上

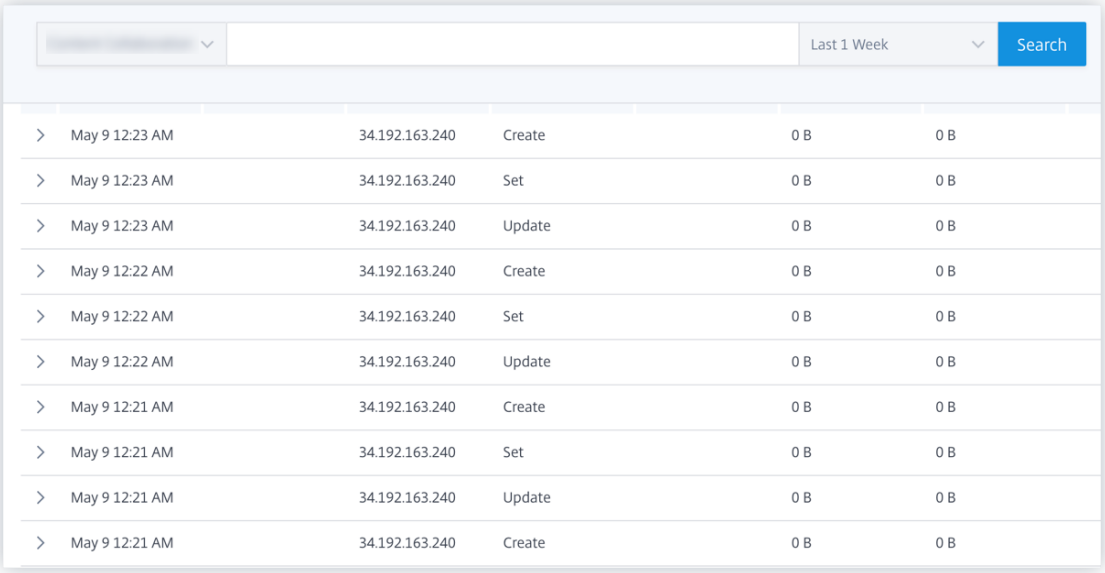
执行最后一次检查以确保事件准确地传输到 Citrix Analytics。

1. 在顶部栏上，单击“高级搜索”以转到自助服务搜索页面。

2. 选择数据源以查看相应的搜索页面和事件。



3. 要查看与应用程序和桌面事件相关的数据，请从列表中选择 应用程序和桌面，选择时间段，然后单击 搜索。

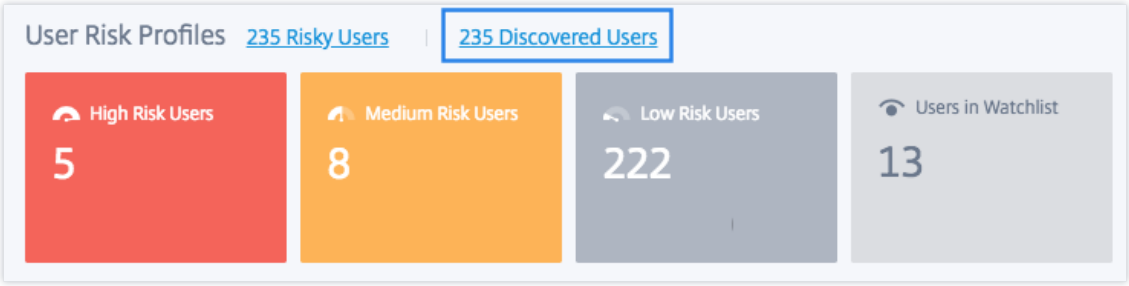


有关详细信息，请参阅 自助搜索。

检查 **8-**分析是否发现了用户

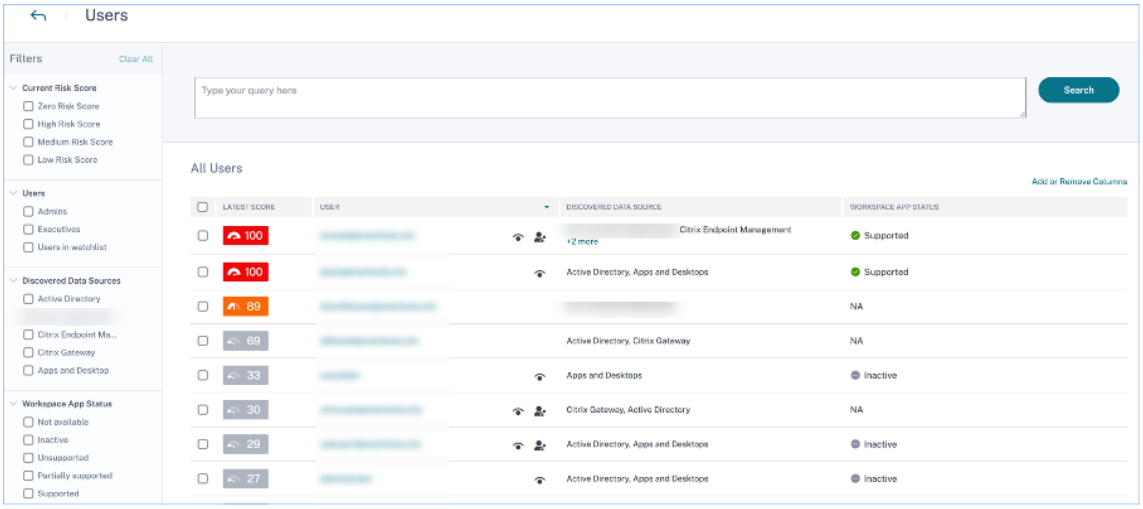
当事件开始流向 Citrix Analytics 时，系统会发现生成事件的用户并将其显示在用户控制板上。此过程通常需要大约几分钟时间，然后您才能在控制板上查看它们。

1. 单击“用户”控制板上的“已发现用户”链接，以查看 Citrix Analytics 发现的用户的完整列表。



2. “用户”页面显示过去 31 天内发现的所有用户的列表。选择时间段以查看风险指示器发生次数。

> 注意
>
> 如果您尝试设置的值大于 31 天，系统会显示一条错误消息，指出 - 日期范围无效。开始日期和结束日期之间的最大允许范围为 **31** 天。



如果事件成功传输，则表明您的 Citrix Analytics 环境将按预期执行。当发现异常时，会生成风险指示器。

触发 **Virtual Apps and Desktops** 事件、**SaaS** 事件并验证事件传输

April 12, 2024

本节介绍触发应用程序和桌面事件、SaaS 事件以及验证 Citrix Analytics for Security 是否正在主动接收这些用户事件的过程。

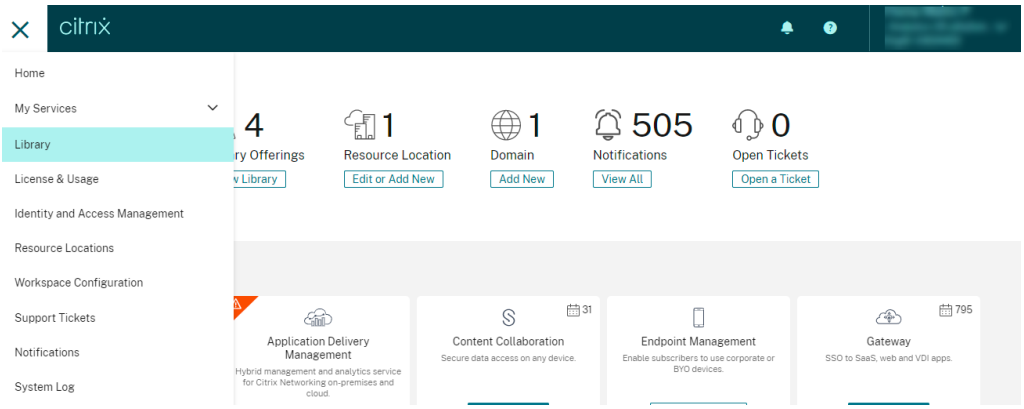
必备条件

- 如果您使用本地 Citrix Virtual Apps and Desktops，请将本地站点加载到 Citrix Analytics，然后从站点卡启用数据处理。如果您使用的是 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务），请直接从站点卡启用数据处理。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源。
- 在用户的终端设备中使用正确版本的 Citrix Workspace 应用程序或 Citrix Receiver，以便将事件准确发送到 Citrix Analytics。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源。
- 在从虚拟桌面触发打印事件之前，请确保在应用程序和桌面环境中配置和配置了打印机。有关管理打印机的详细信息，请参阅 打印。
- 要触发 SaaS 应用程序启动、SaaS 应用程序 URL 导航、SaaS 应用程序文件下载等 SaaS 事件，必须使用 Workspace 中已配置的 SaaS 应用程序。常用的 SaaS 应用程序包括 Salesforce、Workday、Concur、GoToMeeting。
  - 如果没有已配置 SaaS 应用程序，则必须配置和发布 SaaS 应用程序。有关详细信息，请参阅 对软件即服务应用程序的支持。配置 SaaS 应用程序时，请确保禁用以下安全选项：
    - 限制剪贴板访问

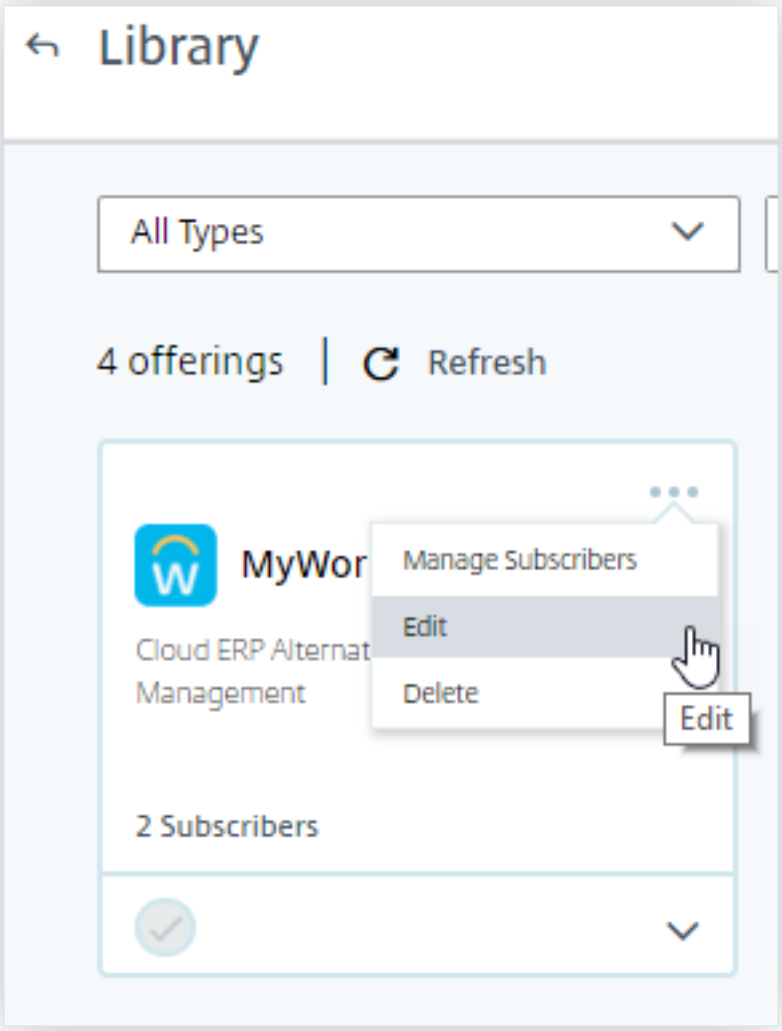
* 限制打印
* 限制导航
* 限制下载

– 如果要使用 Workspace 中已配置的 SaaS 应用来触发事件，请确保为 SaaS 应用程序禁用指定的增强安全选项：

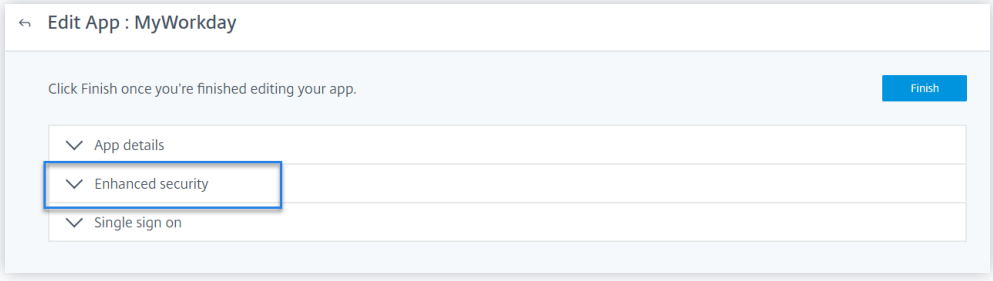
1. 转到您的 Citrix Cloud 帐户，然后选择 库。



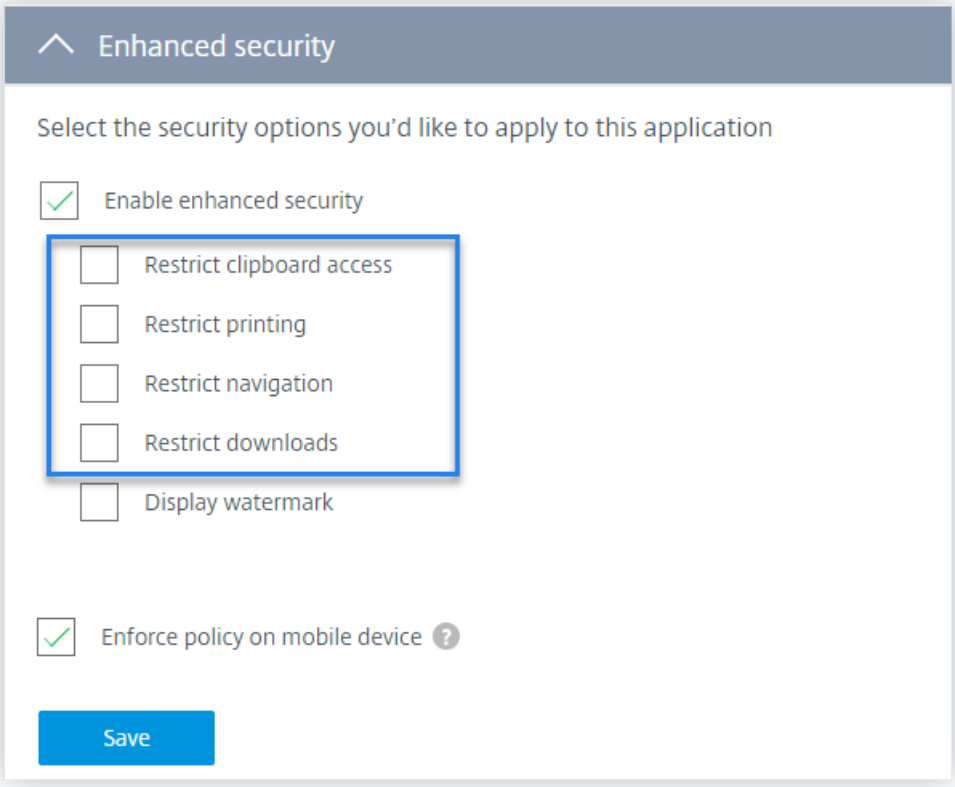
2. 在 资源库 页面上，确定要用于验证事件的 SaaS 应用程序。例如，Workday。
3. 单击省略号，然后选择 编辑。



4. 在 编辑应用程序 页面上，单击增强安全性的向下箭头。



5. 确保未选择以下安全选项。



已知问题

很少有版本的 Citrix Workspace 应用程序和 Citrix Receiver 无法将某些事件发送给 Citrix Analytics 因此，Citrix Analytics 无法为这些事件提供见解并生成风险指示器。有关此问题及其解决方法的更多信息，请参阅已知问题-CAS-16151。

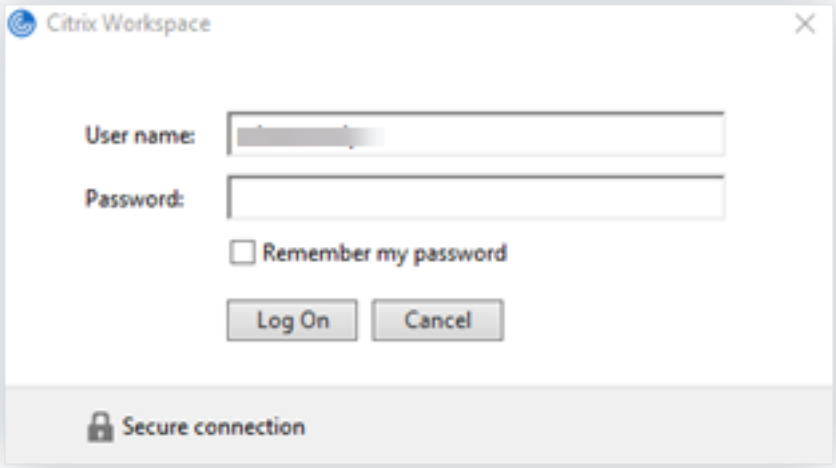
过程

按顺序执行以下步骤以触发应用程序和桌面环境中的事件，并验证 Citrix Analytics for Security 是否正在主动接收这些事件。

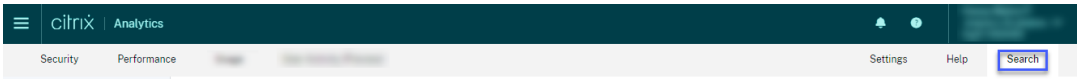
> 注意
>
> - 这些活动可能需要一些时间才能到达 Citrix Analytics。如果看不到触发的事件，请刷新 Citrix Analytics 页面。
> - 为了触发 SaaS 事件，此过程以 Workday 应用程序为例。您可以使用工作区中任何已配置的 SaaS 应用程序来触发 SaaS 事件。

- 帐户登录

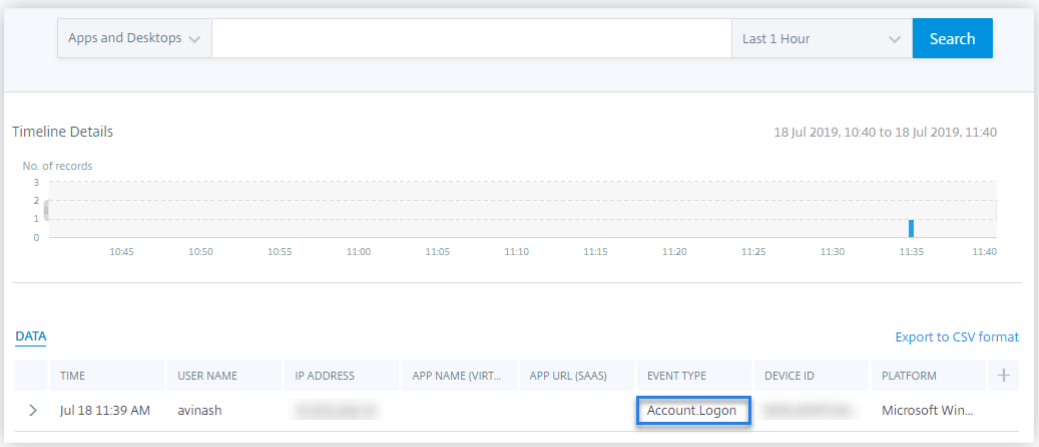
1. 启动 Citrix Workspace 应用程序或 Citrix Receiver 以访问您的 Workspace 或 StoreFront
2. 输入您的凭据以登录 Citrix Workspace 应用程序或 Citrix Receiver。



3. 转到 Citrix Analytics。
4. 单击 搜索，然后从列表中选择 应用程序和桌面。



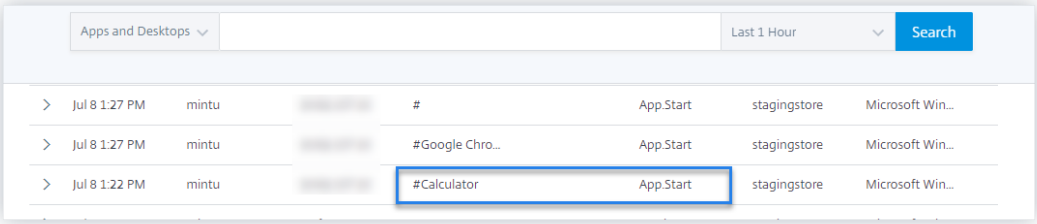
5. 在搜索页面中，查看 **Account.Logon** 事件的数据。展开该行以查看事件详细信息。



- 应用程序启动

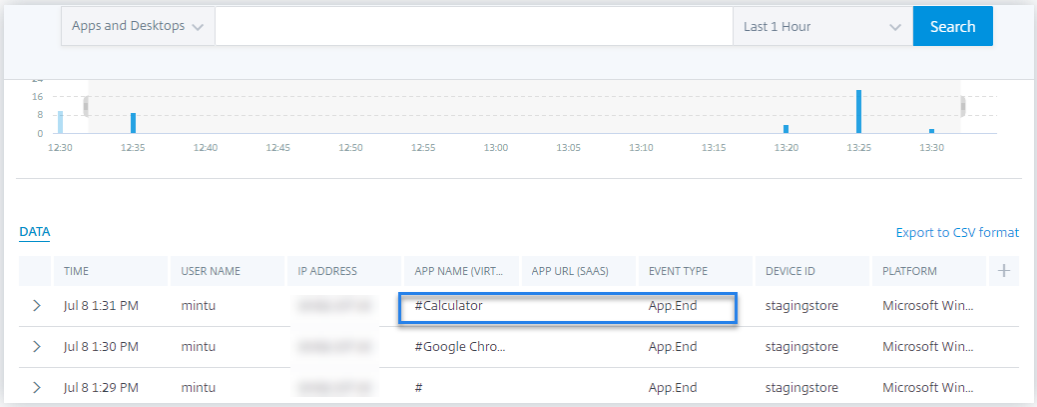
1. 启动 Citrix Workspace 应用程序或 Citrix Receiver 以访问您的 Workspace 或 StoreFront
2. 启动计算器之类的应用程序。
3. 转到 Citrix Analytics。

4. 单击“搜索”，然后选择“应用程序和桌面”。
5. 在搜索页面中，查看 **App.Start** 事件数据的数据。展开该行以查看事件详细信息。



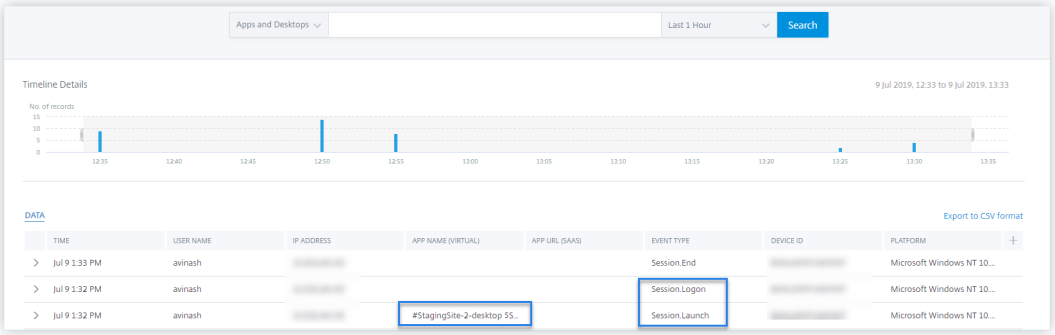
- 应用程序结束

1. 关闭已在工作区或 StoreFront 中启动的计算器。
2. 转到 Citrix Analytics。
3. 单击“搜索”，然后选择“应用程序和桌面”。
4. 在搜索页面中，查看 **App.End** 事件数据的数据。展开该行以查看事件详细信息。



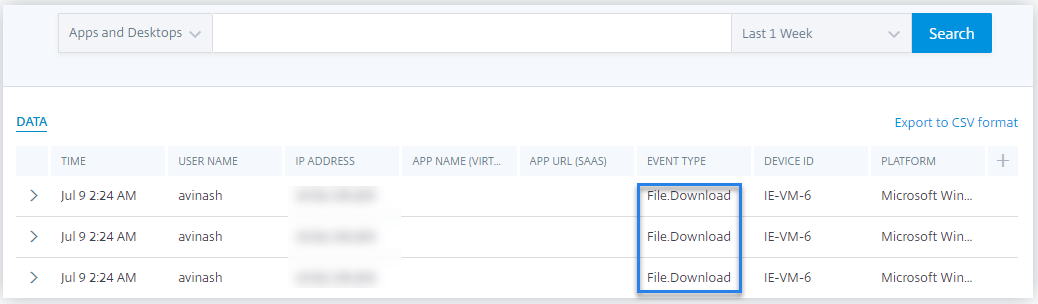
- 会话登录和会话启动

1. 启动 Citrix Workspace 应用程序或 Citrix Receiver 以访问您的 Workspace 或 StoreFront
2. 启动虚拟桌面。
3. 转到 Citrix Analytics。
4. 单击“搜索”，然后选择“应用程序和桌面”。
5. 在搜索页面中，查看 Session.L **ogon** 和 **Session.Launch** 事件的数据。展开该行以查看事件详细信息。



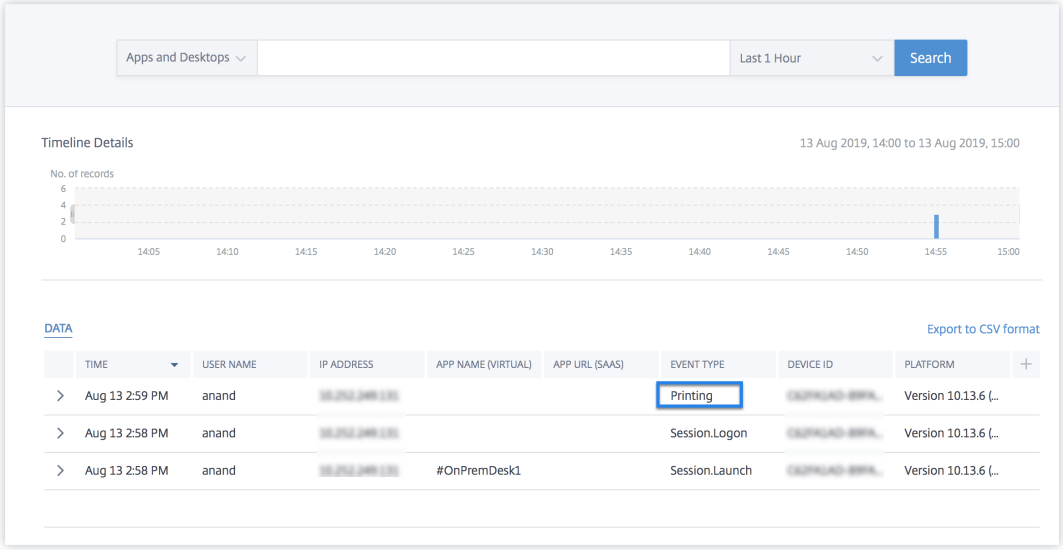
- 文件下载

  1. 启动 Citrix Workspace 应用程序或 Citrix Receiver 以访问您的 Workspace 或 StoreFront
  2. 启动虚拟桌面。
  3. 将文件从虚拟桌面复制到本地计算机。
  4. 转到 Citrix Analytics。
  5. 单击“搜索”，然后选择“应用程序和桌面”。
  6. 在搜索页面中，查看 **File.Download** 事件的数据。展开该行以查看事件详细信息。



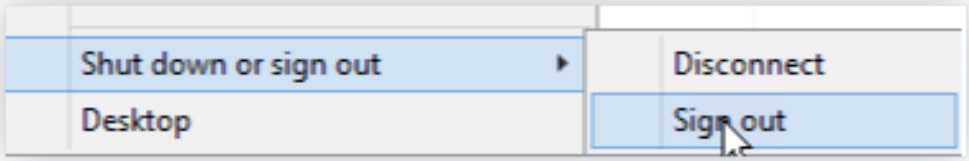
- 打印

  1. 启动 Citrix Workspace 应用程序或 Citrix Receiver
  2. 启动虚拟桌面。
  3. 使用配置有虚拟桌面的打印机打印文档。
  4. 转到 Citrix Analytics。
  5. 单击“搜索”，然后选择“应用程序和桌面”。
  6. 在“搜索”页面中，查看“打印”事件的数据。展开该行以查看事件详细信息。

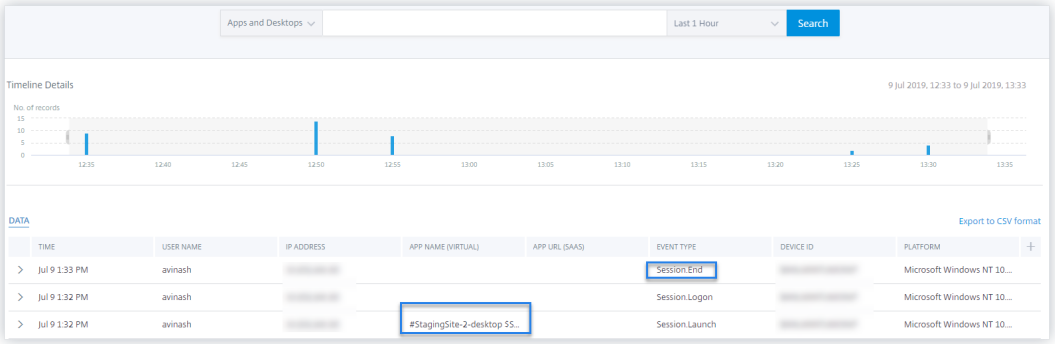


- 会话结束

  1. 从虚拟桌面注销。例如，如果您使用的是 Windows 虚拟桌面，请选择“注销”选项。



  2. 转到 Citrix Analytics。
  3. 单击“搜索”，然后选择“应用程序和桌面”。
  4. 在搜索页面中，查看 S **ession.End** 事件的数据。展开该行以查看事件详细信息。



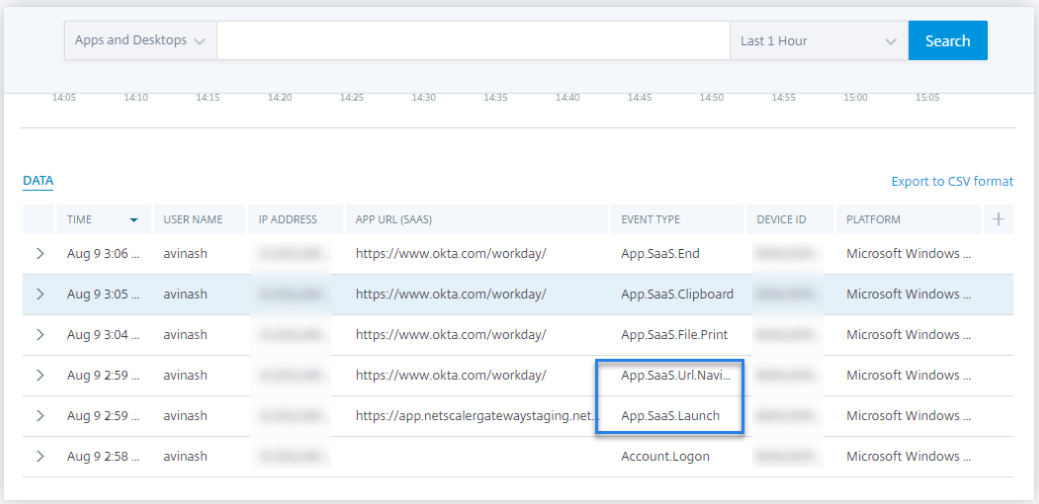
- **SaaS** 应用程序启动和 **SaaS** 应用程序 **URL** 导航

  1. 启动 Citrix Workspace 应用程序或 Citrix Receiver 以访问您的 Workspace 或 StoreFront

2. 启动诸如 Workday 之类的 SaaS 应用程序，然后等待 Workday 页面加载完毕。在 Workday 中浏览网页。

   > 注意
   >
   > 确保在“增强的安全性”部分中禁用了 限制导航 选项。有关更多信息，请参阅 先决条件。

3. 转到 Citrix Analytics。
4. 单击“搜索”，然后选择“应用程序和桌面”。
5. 在搜索页面中，查看 **App.SaaS.Launch** 和 **App.SaaS.URL.Navigation** 事件的数据。展开该行以查看事件详细信息。

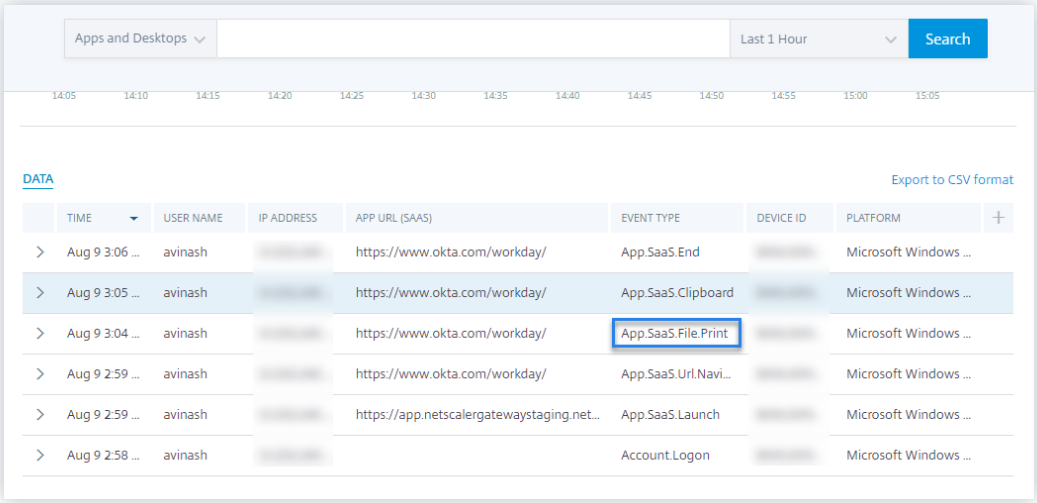


- **SaaS** 应用程序文件打印

1. 打印当前正在查看的 Workday 页面。

   > 注意
   >
   > 确保在增强的安全性部分禁用了 限制打印 选项。有关详细信息，请参阅必备条件。

2. 转到 Citrix Analytics。
3. 单击“搜索”，然后选择“应用程序和桌面”。
4. 在搜索页面中，查看 **App.SaaS.File.Print** 事件的数据。展开该行以查看事件详细信息。

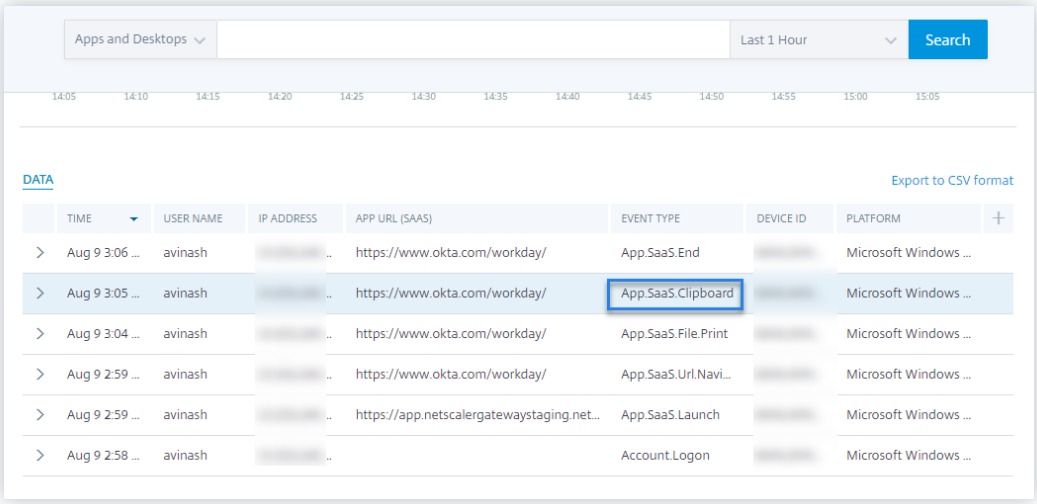


- **SaaS** 应用剪贴板访问

  1. 在 Workday 页面上，将一些文本复制到系统剪贴板。

     > 注意
     >
     > 确保在增强的安全性部分中禁用了 限制剪贴板访问 选项。有关详细信息，请参阅必备条件。

  2. 转到 Citrix Analytics。
  3. 单击“搜索”，然后选择“应用程序和桌面”。
  4. 在搜索页面中，查看 **App.SaaS.Clipboard** 事件的数据。展开该行以查看事件详细信息。

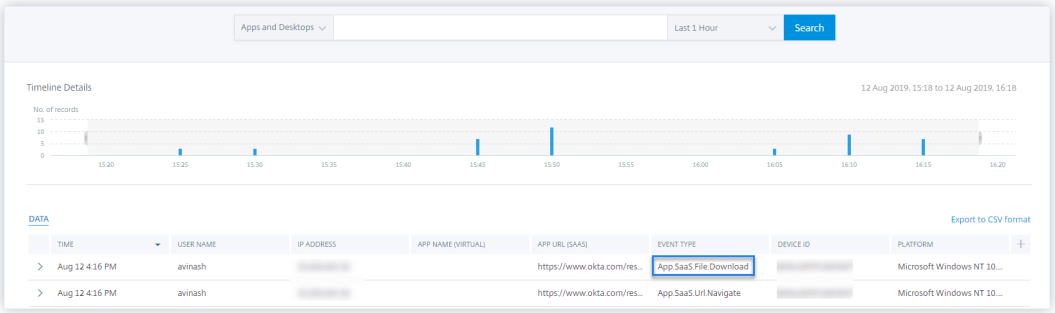


- **SaaS** 应用程序文件下载

  1. 在 Workday 页面上，搜索诸如白皮书之类的公开文档，然后下载该文档。

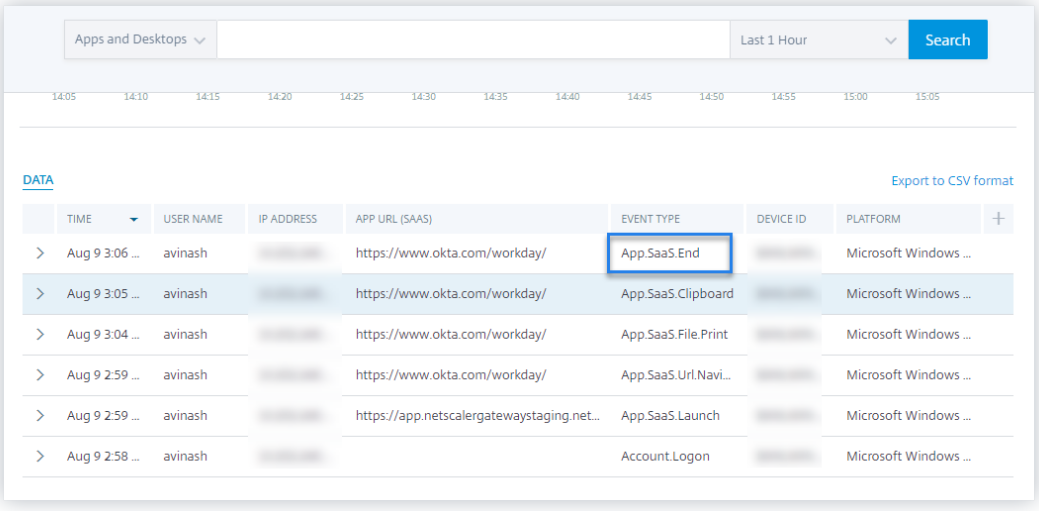
> 注意
>
> 确保在增强的安全性部分禁用了 限制下载 选项。有关详细信息，请参阅必备条件。

2. 转到 Citrix Analytics。
3. 单击“搜索”，然后选择“应用程序和桌面”。
4. 在搜索页面中，查看 **App.SaaS.File.Download** 事件的数据。展开该行以查看事件详细信息。



- **SaaS** 应用程序结束

1. 关闭“工作日”页面。
2. 转到 Citrix Analytics。
3. 单击“搜索”，然后选择“应用程序和桌面”。
4. 在搜索页面中，查看 **App.SaaS.End** 事件的数据。展开该行以查看事件详细信息。



- **VDA.Print**

  必备条件

  在触发打印事件之前，请参阅为 Citrix DaaS 启用打印遥测。

要触发打印事件，请执行以下操作：

1. 使用记事本或任何其他允许打印的应用程序打开文本文档。
2. 单击“文件”**>**“打印”或按 **Ctrl + P**。
3. 在“选择打印机”中，选择您的打印机，然后单击“应用”，然后打印。

- **VDA.Clipboard**

  必备条件

  在触发打印事件之前，请参阅为 Citrix DaaS 启用剪贴板遥测。

  要触发剪贴板事件，请执行以下操作：

  1. 使用记事本或任何文本编辑器打开文本文档。
  2. 选择要复制的内容。
  3. 右键单击“复制”或按 Ctrl+c。

未收到来自受支持的 **Citrix Workspace** 应用程序版本的

October 13, 2022

如果您没有看到来自使用 Citrix Analytics 支持的 Citrix Workspace 应用程序版本的用户发生的任何事件，则问题可能出在以下情况之一：

- StoreFront 配置
- Web 启动要求

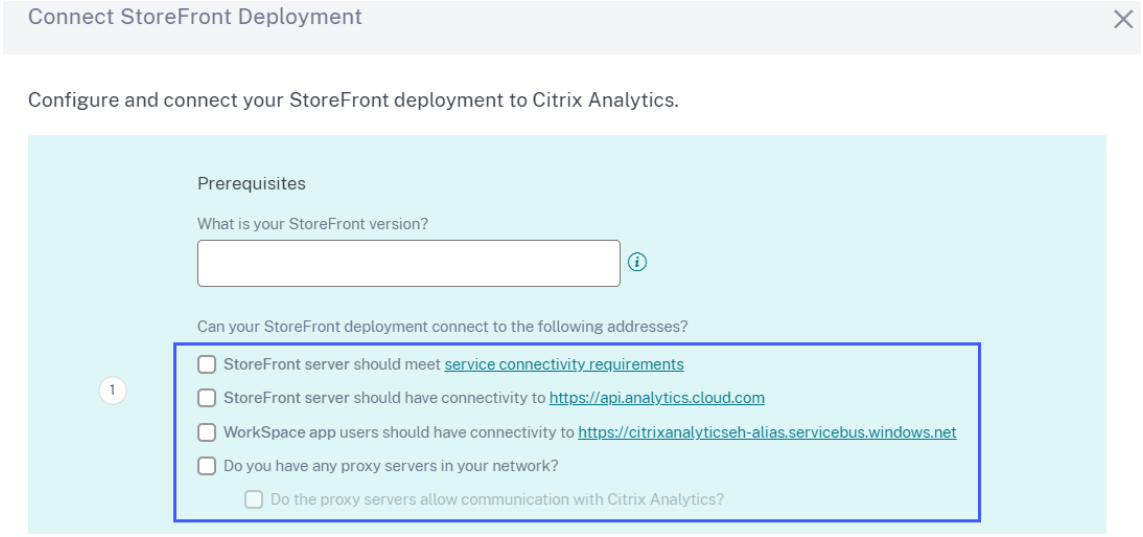
StoreFront 配置

如果 StoreFront 部署已连接到 Citrix Analytics，请检查上 次更新的时间戳。如果用户正在积极访问 StoreFront，则必须每周至少更新一次时间。频繁的时间更新表示 StoreFront 部署和 Citrix Analytics 之间的连接正常。否则，存在一些连接问题。

检查以下连接要求：

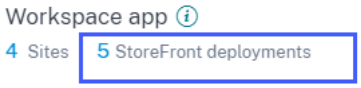
- StoreFront 服务器必须满足 系统和连接要求。
- StoreFront 服务器必须能够连接到 `https://api.analytics.cloud.com`
- Workspace 应用程序用户必须能够连接到 `https://citrixanalyticseh-alias.servicebus.windows.net`
- 您的代理服务器必须允许连接到 Citrix Analytics 事件中心：

- 美国地区：https://citrixanalyticseh-alias.servicebus.windows.net/
- 欧盟地区：https://citrixanalyticseheu-alias.servicebus.windows.net/
- 亚太南部地区：https://citrixanalyticsehaps-alias.servicebus.windows.net/

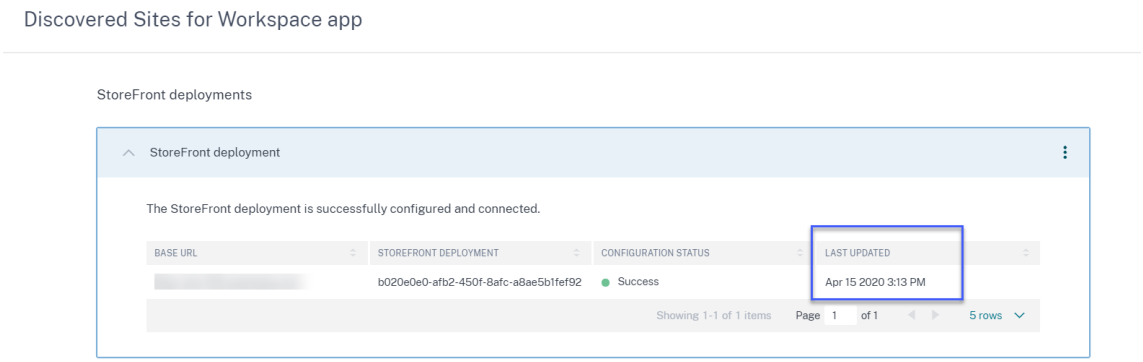


要查看上次更新的时间：

1. 单击 设置 > 数据源。
2. 在 Workspace 应用程序站点卡片上，单击已连接的 StoreFront 服务器的数量。



3. 在 StoreFront 部署上，检查上次更新时间。



如果即使在满足连接要求后，上次更新的时间戳也不经常更新，请重新配置 StoreFront。有关更多信息，请参阅使用 StoreFront 登录 Virtual Apps and Desktops 站点

Web 启动要求

用户可以通过以下方式之一启动虚拟应用程序和桌面：

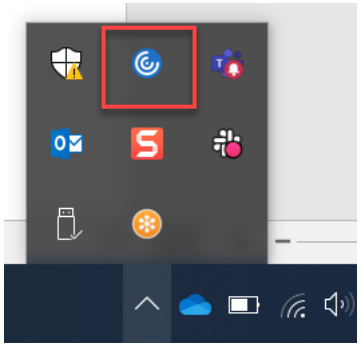
- 通过 Citrix 工作空间应用程序访问 Citrix 商店或 Citrix Workspace。这种方法称为本机启动。
- 在 Web 浏览器中打开 Citrix 应用商店 URL 或 Citrix Workspace URL。单击应用程序或虚拟桌面以下载相应的 ICA 文件。然后使用 Web 浏览器打开 ICA 文件以启动应用程序或虚拟桌面。这种方法称为网络启动。

对于 Web 启动，请确保用户设备必须具有以下基于设备操作系统的客户端之一。

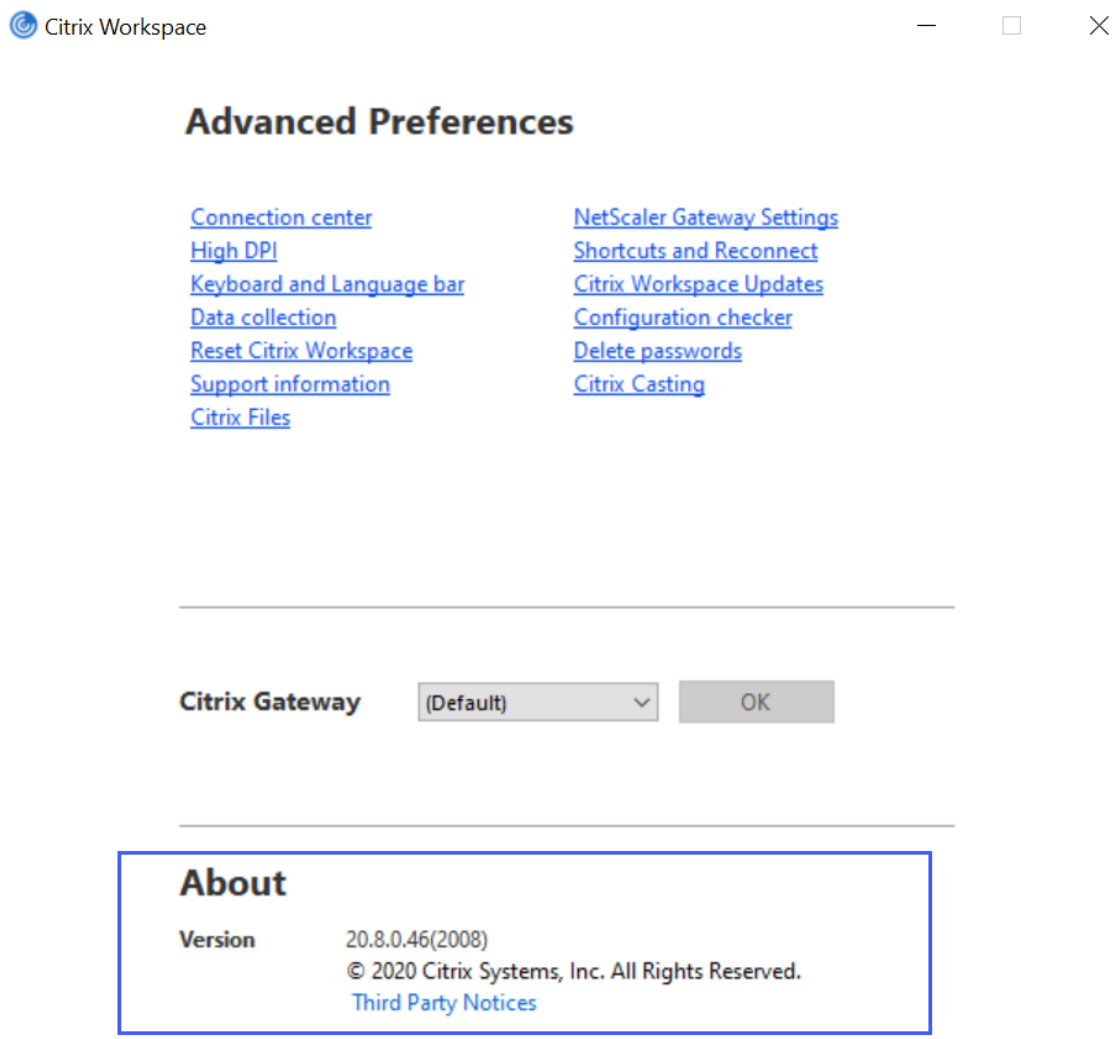
客户端	版本	内部版本
适用于 Windows 的 Citrix Workspace 应用程序	2006.1 或更高版本	20.6.0.38 或更高版本
适用于 Mac 的 Citrix Workspace 应用程序	2006 或更高版本	20.06.0.7 或更高版本

要检查 Citrix Workspace 应用程序版本：

1. 在用户的本地计算机上，右键单击 Citrix Workspace 应用程序图标。



2. 单击 高级首选项，然后选中 关于 部分以查看版本。



配置的 **Session Recording Server** 无法连接

July 12, 2022

配置后，Session Recording Server 无法连接到 Citrix Analytics。因此，在 **Session Recording** 站点卡片上看不到已配置的服务器。

要解决此问题，请执行以下操作：

1. 在配置的会话录制服务器上，运行以下 PowerShell 命令以检查客户端计算机标识 (CMID)。

```
Get-WmiObject -class SoftwareLicensingService | select
    Clientmachineid
```

2. 如果 CMID 为空，请在指定的路径中添加以下注册表文件。

注册表名称	注册表路径	注册表项类型	值
AuditorUniqueID	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\	字符串	输入您的 UUID。
EnableCASUseAuditorUniqueID	Computer\HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/SmartAuditor/Server/	REG_DWORD	1

3. 重新启动以下服务：
    - Citrix Session Recording Analytics Service
    - Citrix Session Recording Storage Manager

无法将 **StoreFront** 服务器与 **Citrix Analytics** 连接

January 5, 2023

将配置设置从 Citrix Analytics 导入到 StoreFront 服务器后，StoreFront 服务器无法连接到 Citrix Analytics。

有关如何将配置设置导入到 StoreFront 服务器的信息，请参阅 使用 StoreFront 的登录 Virtual Apps and Desktops 站点。

CAS 登录助手可帮助检查和解决本文中描述的问题。有关更多信息，请参阅 Citrix Analytics Service (CAS) 登录助手。

要解决此问题，请执行以下操作：

1. 在 StoreFront 服务器上，ping Citrix Analytics 的 特定于区域的端点 以测试 StoreFront 服务器与 Citrix Analytics 服务器之间的连接。此外，请确保 满足必备条件 。

    > 注意

> 在 StoreFront 服务器上，您可以通过直接 ping 区域特定的终端节点或打开 Web 浏览器并访问特定于区域的终端节点来测试连通性。

2. 在 StoreFront 服务器中启用详细日志记录以跟踪日志。有关详细日志记录的详细信息，请参阅文章-CTX139592。
3. 打开互联网信息服务 (IIS) 管理器并检查以下内容：
   - 如果 StoreFront 站点位于 IIS 默认站点下，则 IIS 会重新启动 StoreFront 站点。
   - 如果 StoreFront 站点位于其他驱动程序中或不在默认站点下，请打开命令窗口并键入 `iisreset`。
4. 运行以下命令以导入 Citrix Analytics 设置：

```
Import-STFCasConfiguration -Path "configuration file path"
```

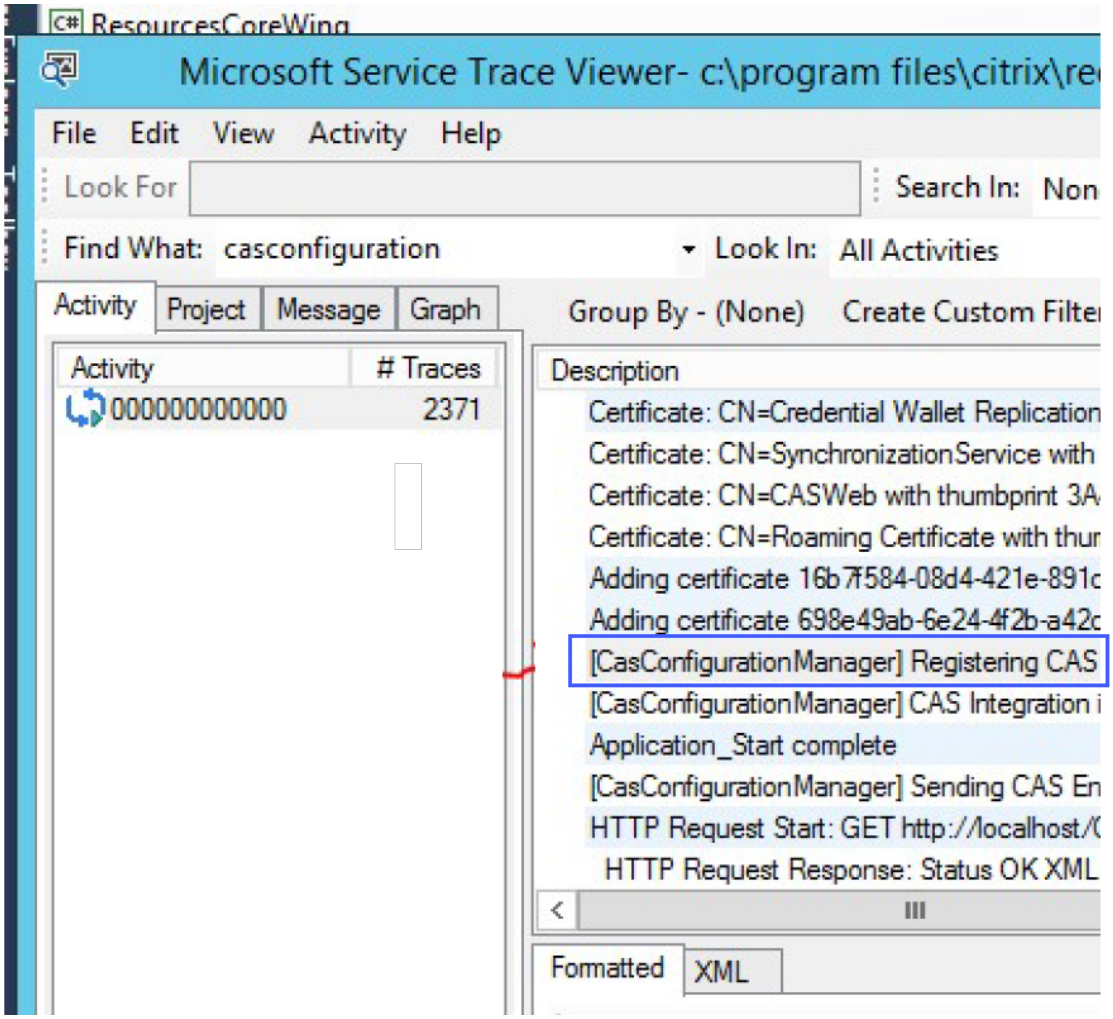
5. 运行以下命令验证导入的设置：

```
Get-STFCasConfiguration
```

6. 如果 StoreFront 站点位于其他驱动程序中或不在默认站点下，请打开命令窗口。键入 `iisreset` 以让 StoreFront 站点读取 Citrix Analytics
7. 从以下位置获取 StoreFront 详细日志文件：

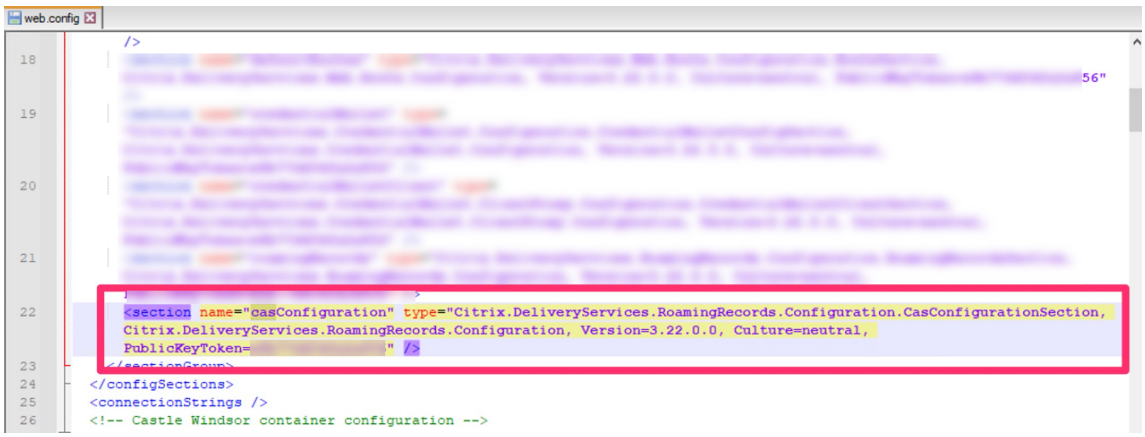
```
C:\Program Files\Citrix\Receiver StoreFront\Admin\trace
```

   在上述位置下，您可以找到多个 svclog 文件，这些文件可以在事件查看器中打开。
8. 使用 Microsoft 服务跟踪查看器打开以下日志：
   - StoreFront 日志
   - 漫游站点详细日志
9. 在日志中，确保 **casConfigurationManager** 部分和 Citrix Analytics 服务器信息可用。



10. 如果 casConfigurationManager 部分不可用，请打开在 `roaming site\folder` 中找到的漫游站点的 web.config 文件。

11. 在 `web.config` 文件中，找到 **casConfiguration** 部分，并确保 Citrix Analytics 服务器信息可用。



12. 在安装了 StoreFront 服务器的 Windows Server 计算机上，请确保满足以下条件：

- TLS 1.2 客户端已启用。
- 至少启用了以下密码套件之一：
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

有关如何配置 TLS 密码套件顺序的信息，请参阅 Microsoft 文档。

13. 如果您使用的是 Windows Server 2012 计算机，请确保已启用 Diffie-Hellman Exchange (ECDHE/DHE)。
14. 确保安装了 StoreFront 服务器的 Windows Server 计算机必须包含 Microsoft 文档中提到的注册表设置。

> 重要
>
> 说明使用组策略更新 TLS/SSL 密码套件。请勿手动修改 TLS/SSL 密码套件。有关如何使用组策略的更多信息，请参阅 Microsoft 文档。

例如，以下注册表设置必须在 Windows Server 计算机中可用：

TLS 1.2 客户端：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"Enabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000

<!--NeedCopy-->
```

Diffie-Hellman KEA：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman
   ]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

AES-128/AES-256 密码：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Ciphers\AES 128/128]
"Enabled"=dword:ffffffff
```



```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Ciphers\AES 256/256]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

SHA256/SHA384 哈希：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Hashes\SHA256]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Hashes\SHA384]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

常见问题解答

November 26, 2023

数据源

什么是数据源

数据源是向 Citrix Analytics 发送数据的 Citrix 服务和产品。

了解更多：数据源

如何添加数据源

登录 Citrix Analytics 后，在 欢迎屏幕上，选择入门以将数据源添加到 Citrix Analytics 中。或者，您也可以通过导航设置 **>** 数据源来添加数据源。

Citrix ADM 代理

在本地虚拟机管理程序上安装代理的最低资源要求是多少

8 GB RAM、4 个虚拟 CPU、120 GB 存储空间、1 个虚拟网络接口、1 Gbps 吞吐量

预配时是否需要向 **Citrix ADM** 代理分配额外的磁盘

不需要，您不必再添加磁盘。该代理仅用作 Citrix Analytics 与企业数据中心中的实例之间的中介。它不存储需要额外磁盘的库存或分析数据。

登录代理的默认凭据是什么

登录到代理的默认凭据是 `nsrecover`/`nsroot`。这会将您登录到代理的 shell 提示符。

如果我输入的值不正确，如何更改代理的网络设置

登录到虚拟机管理程序上的代理控制台，使用凭据 `nsrecover`/`nsroot` 访问 shell 提示符，然后运行命令 `networkconfig`。

为什么我需要服务 **URL** 和激活码

代理使用服务 URL 查找服务，使用激活码向服务注册代理。

如果我在代理控制台中输入的服务 **URL** 不正确，如何才能重新输入服务 **URL**

使用凭据 `nsrecover`/`nsroot` 登录到代理的 shell 提示符，然后键入 `deployment_type.py`。此脚本允许您重新输入服务 URL 和激活码。

如何获得新的激活码

您可以从 Citrix ADM 服务获取新的激活码。登录 Citrix ADM 服务并导航到网络 **>** 代理。在代理页上的选择操作列表中，选择生成激活码。

我可以使用多个代理重复使用激活码吗**?**

不，您不能。

我需要安装多少 **Citrix ADM** 代理

代理的数量取决于数据中心中托管实例的数量和总吞吐量。Citrix 建议您为每个数据中心至少安装一个代理。

如何安装多个 **Citrix ADM** 代理

在“数据源”页面上，单击 Citrix Gateway 旁边的加号 (+)，然后按照说明安装其他代理。

或者，您可以访问 Citrix ADM GUI 并导航到“网络”>“代理”，然后单击安装代理以安装多个代理。

我能否在高可用性设置中安装两个代理

不，您不能。

如果我的代理注册失败，我该怎么办**?**

- 确保您的代理可以访问互联网（配置 DNS）。
- 确保您已正确复制激活码。
- 确保您已正确输入服务 URL。
- 确保您已打开所需的端口。

注册成功，但如何知道代理是否正常运行呢

您可以执行以下操作来检查代理是否运行正常：

- 成功注册代理后，访问 Citrix ADM 并导航到网络 **>** 代理。您可以在此页面上查看发现的代理。如果代理运行正常，则状态由绿色图标表示。如果它未运行，则状态由红色图标表示。
- 登录到代理的 shell 提示符并运行以下命令：`ps -ax | grep mas` 和 `ps -ax | grep ulfd`。确保以下进程正在运行。

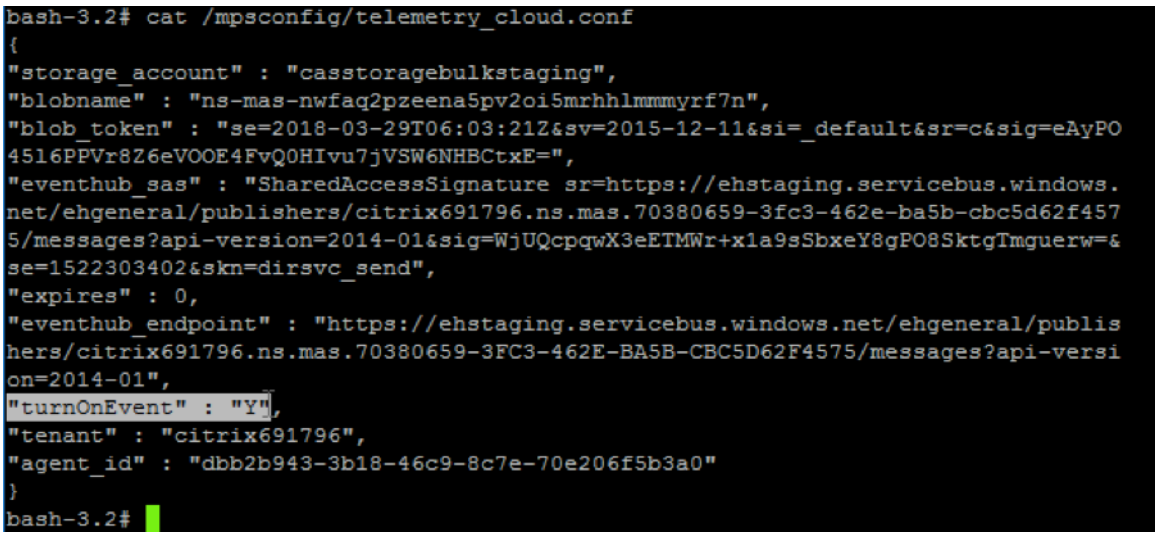
- 如果有任何进程未运行，请运行命令 **masd restart**。启动所有守护程序可能需要一些时间（1 分钟左右）。
- 成功注册代理后，确保在 `/mpsconfig` 中创建 `agent.conf`。

管理 **Citrix Gateway** 实例

Citrix Gateway 实例已添加到 **Citrix Analytics** 中，但我如何知道代理程序上是否启用了分析

您可以使用代理的 shell 提示符验证是否在代理上启用了分析。如果在代理上成功启用分析，则 /mpsconfig/telemetry_cloud.conf 文件中的 turnOnEvent 参数将设置为 Y。

登录到代理的 shell 提示符并运行以下命令：cat /mpsconfig/telemetry_cloud.conf 并验证 turnOnEvent 参数的值。



我不小心关闭了 **Citrix Gateway** 入门向导。我必须从头开始配置吗

不是。Citrix Analytics 会保存进度，并将未完成的配置显示为 数据源 **>** 设置 页面中的磁贴。单击继续设置以完成配置。

Virtual Apps and Desktops 入门网站

如何关闭数据处理

如果要暂时禁用从站点到 Citrix Analytics 的数据处理，只需单击 站点 卡，然后单击 关闭数据处理即可。

将站点添加到 **Workspace** 并单击“测试 **STA**”时，测试失败。我该怎么做

您的 Citrix Gateway 和 Cloud Connector 之间可能存在连接问题。要进行故障排除，请参阅 Citrix 支持知识中心中的 CTX232517 。

我在哪里可以获得有关 **Citrix Analytics** 的帮助

您可以在 Citrix Analytics 讨论论坛（网址为 https://discussions.citrix.com/forum/1710-citrix-analytics/）上提问并与 Citrix Analytics 专家联系。

要参与论坛，您必须使用您的 Citrix ID 登录。

访问保障-地理定位

Analytics 是如何推导出地理位置详细信息的

Citrix Analytics 使用从其启动 Workspace 客户端的设备的 IP 地址。Citrix Analytics 利用第三方 IP 地理位置数据提供商从用户的 IP 地址中获取用户的位置。当您执行会话登录时，它会将您的位置（IPv4 地址）解析为国家或城市，并且映射会定期更新。组织可以使用这些由国家/地区定义的地点来监视他们不开展业务的地方的访问模式。

推导用户位置的准确度是多少

Citrix Analytics 利用第三方 IP 地理位置数据提供商从用户的 IP 地址中获取用户的位置。大多数情况下，GeoIP 服务都能够解析到正确的城市或位置，但 GeoIP 查找从来都不是完全准确的。有时，为用户显示的位置可能与其访问的确切位置不同。

根据 IP GeoPoint 文档，覆盖级别约为全球分配的 IP 地址（IPv4 可路由 IP 地址）的 99.99%。就位置精度而言，它在每个基本位置字段（国家、州、城市、邮政编码）中都附有置信因子。

在哪些情况下，位置的确定不准确

地理位置数据的准确性取决于设备连接到互联网的方式。设备可以通过以下方式连接到互联网：

- 移动网关
- VPN 或托管设施
- 区域或国际代理/匿名服务器

在这种情况下，无论使用 IP 地理位置提供商软件如何，地理位置数据都不准确。

支持的 **Citrix Workspace** 应用程序版本是什么

将 **IP** 地址属性发送到 Citrix Analytics for Security 时，操作系统对 Citrix Workspace 应用程序的最低版本有要求。有关更多详细信息，请参阅 矩阵表 或 标识为不可用的位置 。

在哪些情况下，我们不会收到地质详细信息

要查看地理位置详细信息，请参阅 标识为不可用的位置 部分以了解详细信息。

Citrix Analytics 使用哪种地理位置服务来报告用户的位置？如何报告错误的 **IP** 位置

Citrix Analytics 使用 基于 Neustar 文件的地理定位服务 为传入访问提供地理位置数据。它有一个面向公众的 IP 更正页面，可用于自行提交更正请求。提交更正请求后，Neustar 将审核该请求的准确性并进行处理。

GeoIP 提供程序有助于显示尽可能准确的信息。遗憾的是，在某些情况下，由于 GeoIP 的固有特性，GeoIP 数据可能不准确。

术语表

April 12, 2024

- 操作：对可疑事件的闭环响应。应用操作以防止将来发生异常事件。了解更多。
- **Cloud Access** 安全代理 **(CASB)**：位于云服务使用者和云服务提供商之间的本地或基于云的安全策略执行点。在访问基于云的资源时，CASB 会合并和插入企业安全策略。它们还可以帮助组织将其内部基础设施的安全控制扩展到云中。
- **Citrix ADC**（应用程序 **Delivery Controller**）：位于数据中心的网络设备，战略性地位于防火墙与一台或多台应用程序服务器之间。处理服务器之间的负载平衡，并优化企业应用程序的最终用户性能和安全性。了解更多。
- **Citrix ADM**（应用程序交付管理）：集中式网络管理、分析和编排解决方案。管理员可以在单个平台上查看、自动化和管理横向扩展应用程序架构的网络服务。了解更多。
- **Citrix ADM** 代理：支持 Citrix ADM 与数据中心中的托管实例之间进行通信的代理。了解更多。
- **Citrix Analytics**：跨服务和产品（本地和云）收集数据并生成切实可行的见解的云服务，使管理员能够主动处理用户和应用程序安全威胁，提高应用性能并支持持续运营。了解更多。
- **Citrix Cloud**：通过任何云或基础架构（本地、公有云、私有云或混合云）上的 Citrix Cloud Connector 连接到资源的平台。了解更多。
- **Citrix Gateway**：整合了远程访问基础架构的整合远程访问解决方案，以提供跨所有应用程序的单点登录，无论是在数据中心、云中还是作为 SaaS 交付。了解更多.
- **Citrix Hypervisor**：针对应用程序、桌面和服务器虚拟化基础架构进行了优化的虚拟化管理平台。了解更多。
- **Citrix Workspace** 应用程序（以前称为 Citrix Receiver）：客户端软件，可通过任何设备（包括智能手机、平板电脑、个人电脑和 Mac）无缝、安全地访问应用程序、桌面和数据。了解更多。
- **DLP**（数据丢失防护）：描述一组技术和检查技术的解决方案，用于对对象（如文件、电子邮件、数据包、应用程序或数据存储）中包含的信息进行分类。此外，对象还可以在存储中、使用中或通过网络存储。DLP 工具可以动态应用日志、报告、分类、重新定位、标记和加密等策略。DLP 工具还可以应用企业数据权限管理保护。了解更多。
- **DNS**（域名系统）：用于查找互联网域名并将其转换为互联网协议（IP）地址的网络服务。DNS 将用户提供的网站名称映射到机器提供的相应的 IP 地址，以定位网站，而不管实体的物理位置如何。

- 数据处理：将数据源中的数据处理到 Citrix Analytics 的方法。了解更多。
- 数据源：向 Citrix Analytics 发送数据的产品或服务。数据源可以是内部数据源，也可以是外部数据源。[了解更多] /zh-cn/citrix-analytics/data-sources.html)。
- 数据导出：从 Citrix Analytics 接收数据并提供见解的产品或服务。了解更多。
- 发现的用户：组织中使用数据源的用户总数。了解更多。
- **FQDN**（完全限定域名）：用于内部 (StoreFront) 和外部 (Citrix ADC) 访问的完整域名。
- 机器学习：一种数据分析技术，无需明确编程即可提取知识。来自各种潜在来源（例如应用程序、传感器、网络、设备和设备）的数据被输入到机器学习系统中。系统使用数据并应用算法来构建自己的逻辑来解决问题、获得见解或做出预测。
- **Microsoft Graph** 安全性：连接客户安全和组织数据的网关。在必须采取措施时提供易于查看的警报和补救选项。了解更多。
- 性能分析：提供组织内用户会话详细信息可见性的服务。了解更多。
- 策略：对用户的风险配置文件应用操作所要满足的一组条件。了解更多。
- 风险指示器：提供有关组织在给定时间面临的业务风险程度的信息的指标。了解更多。
- 风险评分：动态值，表示用户或实体在预先确定的监视期内对 IT 基础架构构构成的总体风险水平。了解更多。
- 风险时间表：记录用户或实体的风险行为，允许管理员调查风险概况并了解数据使用情况、设备使用情况、应用程序使用情况和位置使用情况。了解更多。
- 有风险的用户：以危险方式行事或表现出危险行为的用户。了解更多。
- 安全分析：对数据进行高级分析，用于实现令人信服的安全成果，例如安全监视和威胁追踪。了解更多。
- **Secure Private Access**：该服务将单点登录、远程访问和内容检查集成到单个解决方案中，以实现端到端访问控制。了解更多。
- **Splunk**：SIEM（安全信息和事件管理）软件，用于接收来自 Citrix Analytics 的智能数据，并提供有关潜在业务风险的见解。了解更多。
- **UBA**（用户行为分析）：将用户活动和行为与对等组分析相结合的基准化过程，以检测潜在的入侵和恶意活动。
- 监视列表：管理员希望监视可疑活动的用户或实体的列表。了解更多。