Citrix Analytics for Security™

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

新增功能 37

April 15, 2024 37

新增执行摘要报告 37

January 29, 2024 37

Workspace 应用程序状态字段更新 37

January 25, 2024 37

CAS UI 中的不一致之处已得到简化 37

January 24, 2024 38

SIEM 环境中增强的用户配置文件事件 38

December 01, 2023 38

用于每周电子邮件和 SIEM 警报的管理员电子邮件设置页面 38

用户仪表板 - 新增活动用户计数时间筛选器并更新了“概述”部分 38

增强型自定义报告 38

November 30, 2023 39

移除 Citrix Analytics 中的所有 ShareFile 功能 39

September 22, 2023 39

自定义指示器中的 Citrix Secure Browser 数据源 39

增强每周电子邮件与 SIEM 数据导出功能 39

在电子邮件中消耗自定义管理员的通知首选项 40

July 04, 2023 40

自助搜索和自定义指标中支持 OR 运算符 40

June 15, 2023 40

启用 VDA 剪贴板遥测 40

June 14, 2023 41

Citrix Analytics for Security 中提供会话录制应用程序生命周期和注册表事件 41

June 08, 2023 41

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复的问题 41
May 29, 2023 42
适用于 Splunk 的 Citrix Analytics 附加组件现已在 Splunk Cloud 平台上推出 42
SIEM 中的会话录制事件 42
May 24, 2023 42
通知最终用户全局操作 42
May 04, 2023 42
测试事件生成 42
SIEM 电子邮件警报生成 43
April 13, 2023 43
已修复的问题 43
March 31, 2023 44
Citrix Analytics for Security 中的会话录制事件 44
自助搜索中的应用保护事件 44
March 30, 2023 44
自定义角色支持 44
SIEM UI 故障排除面板 45
March 24, 2023 45
用户配置文件视图更改 45
从所有搜索视图中移除动态自动建议 46
March 21, 2023 46
建议面板，帮助加入本地 StoreFront™ 数据源 46
February 23, 2023 46
已修复的问题 46
February 22, 2023 46
每周电子邮件通知的增强功能 46
为 App.SaaS.File.Download 事件类型添加了“下载文件格式”字段 47
浏览器派生字段的更改 47

© 1997–2026 Citrix Systems, Inc. All rights reserved.

February 16, 2023 47
已修复问题 47
February 03, 2023 48
适用于欧盟和亚太南部地区的 Citrix Secure Private Access™ 服务的分析支持 48
January 11, 2023 48
从 Secure Private Access 中移除 Web 过滤功能 48
December 27, 2022 48
自助搜索中数据源下拉列表的更改 48
December 13, 2022 49
用户仪表板增强功能 49
December 05, 2022 49
访问保障仪表板 - 登录网络 49
November 18, 2022 49
已修复问题 49
November 08, 2022 49
重命名操作 49
已修复的问题 50
October 19, 2022 50
数据源事件选择和导出 50
October 18, 2022 50
允许管理员在 Citrix DaaS™ 站点上运行动态会话录制操作 50
October 14, 2022 51
为用户风险指标提供反馈 51
September 26, 2022 51
访问保障支持地理围栏阻止列表 51
已修复的问题 51
September 13, 2022 52
共享链接仪表板增强功能 52

© 1997–2026 Citrix Systems, Inc. All rights reserved.

September 09, 2022 52
异常行程 RI 增强功能 52
August 19, 2022 52
启用 VDA 打印遥测 52
August 18, 2022 53
已修复的问题 53
August 17, 2022 53
按策略自定义最终用户电子邮件 53
August 11, 2022 53
已修复的问题 53
June 17, 2022 53
新付费授权默认启用数据处理 53
June 09, 2022 54
已修复的问题 54
June 02, 2022 54
已修复问题 54
May 24, 2022 54
推出适用于内容协作、Citrix DaaS 和 Citrix Virtual Apps and Desktops 以及 Gateway 数据源的不可能的行程风险指标 54
May 17, 2022 54
虚拟应用和桌面已重命名为应用和桌面 54
已修复问题 55
April 05, 2022 55
新增功能 55
安全工作区访问 已更名为 安全私有访问 55
March 21, 2022 55
已修复问题 55
March 10, 2022 56

© 1997–2026 Citrix Systems, Inc. All rights reserved.

新增功能 56
通知管理员电子邮件增强功能 56
已修复的问题 56
March 03, 2022 56
新增功能 56
手动应用请求最终用户响应 56
策略的请求最终用户响应增强功能 56
February 23, 2022 58
新增功能 58
风险指标的建议操作 58
已修复问题 59
February 17, 2022 59
新增功能 59
改进了 Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源的数据收集和报告 59
支持内容协作中会话事件和应用程序事件的上下文模板 59
February 10, 2022 60
新增功能 60
自定义风险指标中维度的自动建议值 60
February 09, 2022 61
新增功能 61
管理员的新自定义角色 61
支持自定义访问管理员的电子邮件通知 61
January 28, 2022 62
新增功能 62
为内容协作和网关数据源引入可疑登录风险指标 62
January 20, 2022 62
新增功能 62
微软 Azure 活动目录集成 62

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 18, 2022 63
最新功能 63
支持对所有内容协作风险指标执行共享链接操作 63
与 SIEM 的集成现已正式发布 63
December 23, 2021 64
新增功能 64
共享链接风险指标增强功能 64
December 21, 2021 64
新增功能 64
向非 Citrix Cloud 管理员发送有关风险指标的通知 64
December 20, 2021 65
新增功能 65
向您的内容协作用户发送用户响应通知 65
访问控制 已更名为 安全工作区访问 65
已修复问题 65
December 09, 2021 65
新增功能 65
使用模板轻松创建自定义风险指标 65
December 07, 2021 66
已修复问题 66
December 02, 2021 66
新增功能 66
检测到恶意文件风险指标 66
Content Collaboration 数据源的新操作 66
November 29, 2021 67
新增功能 67
用户通知的电子邮件设置增强功能 67
November 26, 2021 68

© 1997–2026 Citrix Systems, Inc. All rights reserved.

新增功能 68
自定义风险指标和策略菜单更改 68
November 25, 2021 69
新增功能 69
安全信息和事件管理 (SIEM) 集成增强功能 69
November 09, 2021 69
已修复问题 69
November 02, 2021 69
新增功能 69
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 69
在内容协作的自助服务搜索页面上查看恶意软件日志 70
已修复的问题 71
October 20, 2021 71
新增功能 71
会话录制服务器集成 71
October 19, 2021 72
新增功能 72
通知管理员电子邮件模板增强功能 72
用户登录摘要增强功能 72
已修复的问题 73
October 01, 2021 73
新增功能 73
在 Content Collaboration 的自助搜索中查看审核日志 73
已修复的问题 74
September 29, 2021 74
新增功能 74
访问保障位置控制板现已正式发布 74
September 15, 2021 74

© 1997–2026 Citrix Systems, Inc. All rights reserved.

新增功能 74
自定义风险指标增强功能 74
September 14, 2021 74
新增功能 74
推出可疑登录风险指标 74
SIEM 消息增强 75
已修复问题 75
August 19, 2021 75
新增功能 75
推出适用于 Splunk 的 Citrix Analytics 应用程序 75
SIEM 的自定义风险指示器架构 76
支持 Citrix Director 作为数据源 76
访问保障位置控制板中对地理围栏的支持 76
“用户”页面上的 Workspace 应用程序状态 76
支持 IS EMPTY 运算符 77
改进的风险评分 77
July 29, 2021 78
已弃用的功能 78
与 Citrix Endpoint Management™ 相关的已弃用操作 78
July 14, 2021 78
新增功能 78
支持 IS NOT EMPTY 运算符 78
July 06, 2021 79
新增功能 79
在用户仪表板上查看非风险用户 79
July 01, 2021 79
新增功能 79
访问保障位置仪表板增强功能 79

© 1997–2026 Citrix Systems, Inc. All rights reserved.

更新了适用于 Virtual Apps and Desktops 的自助服务搜索中的操作系统分面 80
June 30, 2021 80
新增功能 80
在 Apps and Desktops 的自定义风险指标条件中添加了 Workspace 应用程序版本 80
June 23, 2021 81
新增功能 81
SIEM 消息增强功能 81
June 07, 2021 81
新增功能 81
对通知管理员操作的增强 81
增加了对只读共享操作的支持 81
May 18, 2021 81
新增功能 81
将默认风险指标迁移到自定义风险指标 81
Gateway 自助搜索的增强功能 82
已修复的问题 83
April 29, 2021 83
新增功能 83
自定义风险指标的事件详细信息 83
已修复问题 83
April 16, 2021 83
新增功能 83
SIEM 消息增强功能 83
March 26, 2021 84
新增功能 84
SIEM 消息限制 84
在 SIEM 消息中添加了数据源 ID 和指标类别 ID 字段 84
March 18, 2021 85

© 1997–2026 Citrix Systems, Inc. All rights reserved.

新增功能 85
访问保障位置控制板 85
支持 NOT LIKE (!~) 运算符 86
已翻译的操作系统版本 86
更新了 Apps and Desktops 的数据字段 86
已弃用的功能 86
从自助服务搜索页面中删除了 VPN_AF 和 VPN_SU 事件 86
March 11, 2021 87
新增功能 87
用户风险评分架构的当前时间戳 87
March 03, 2021 87
新增功能 87
可疑 IP 登录风险指标的增强功能 87
异常位置访问风险指示器增强功能 88
适用于 SIEM 的 Citrix Analytics 数据格式 88
已修复的问题 88
February 18, 2021 88
新增功能 88
自定义风险指示器中首次从新实体访问的支持 88
创建自定义风险指示器的最大限制 89
来自 Citrix Virtual Apps and Desktops 和 Citrix DaaS 的用户位置数据 89
多列排序 89
已弃用的功能 90
“授权失败过多”风险指标已弃用 90
January 27, 2021 90
新增功能 90
异常位置访问风险指标的增强功能 90
January 20, 2021 91

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复的问题 91
January 19, 2021 91
已修复问题 91
January 13, 2021 91
新增功能 91
Citrix Analytics Add-on for Splunk 的新版本已发布 91
新增对 Splunk Cloud Inputs Data Manager (IDM) 和 Splunk 8.1 64 位版本的支持 91
已弃用的支持 92
已移除对 Splunk 7.1 64 位版本的支持 92
January 11, 2021 92
已修复问题 92
December 17, 2020 92
新增功能 92
使用预配置的自定义风险指示器和策略阻止来自异常位置的访问（地理围栏） 92
在用户响应电子邮件中查看访问位置 92
已重命名内容协作风险指示器 - 首次从新位置访问 93
已弃用功能 93
风险指示器反馈 93
December 07, 2020 93
新增功能 93
潜在数据渗漏风险指示器的改进 93
对内容协作风险指示器 - 首次从新位置访问的改进 93
November 30, 2020 94
新增功能 94
自助搜索页面改进 94
策略改进 95
November 04, 2020 95
新增功能 95

© 1997–2026 Citrix Systems, Inc. All rights reserved.

异常身份验证失败 - Citrix Gateway 风险指示器 95
October 20, 2020 96
已修复问题 96
October 15, 2020 96
新功能 96
从异常位置访问 – Citrix Virtual Apps and Desktops 和 Citrix DaaS 风险指示器 96
共享链接仪表板增强功能 97
共享链接风险时间线增强功能 97
已弃用的功能 98
已弃用从具有不受支持的操作系统 (OS) 的设备访问风险指示器 98
September 10, 2020 98
新功能 98
StoreFront 清单 98
自助搜索 - 支持不等于 (!=) 运算符 98
September 08, 2020 99
新功能 99
用户关联 99
已修复问题 99
August 11, 2020 100
已修复问题 100
July 31, 2020 100
已修复的问题 100
July 09, 2020 100
新增功能 100
Virtual Apps and Desktops 站点卡显示使用受支持和不受支持客户端的用户 100
来自异常位置的访问风险指示器 101
用户仪表板数据 102
重新设计的用户页面 102

© 1997–2026 Citrix Systems, Inc. All rights reserved.

风险用户窗格增强功能 103

观察列表中的用户窗格增强功能 104

特权用户窗格增强功能 104

已弃用的功能 105

警报 105

风险用户和观察列表页面 105

风险用户窗格 106

风险指标窗格 107

趋势视图 108

用户组页面 108

June 26, 2020 109

已弃用的功能 109

应用程序访问异常时间 (虚拟/SaaS) 风险指标已弃用 109

June 02, 2020 109

已修复的问题 109

May 11, 2020 110

已修复的问题 110

April 29, 2020 110

已修复的问题 110

April 02, 2020 110

新增功能 110

未添加 StoreFront 时禁用数据处理 110

已修复的问题 111

March 04, 2020 111

已修复问题 111

February 20, 2020 111

新增功能 111

Citrix Analytics for Security 所提供的产品 111

© 1997–2026 Citrix Systems, Inc. All rights reserved.

风险类别控制板 112

自定义指标页面上的风险类别列 113

风险指标名称变更 113

已修复的问题 114

January 09, 2020 114

新功能 114

持续风险评估 114

策略配置 115

锁定用户和解锁用户操作 118

访问摘要控制板 119

策略和操作控制板 120

策略的自助搜索 121

已弃用的功能 121

已删除基于风险评分更改策略的条件 121

已删除多个基于策略的操作 121

已修复的问题 122

December 12, 2019 122

新增功能 122

Splunk 版本支持 122

December 04, 2019 122

新增功能 122

Citrix Gateway 的自定义风险指标 122

November 22, 2019 123

新增功能 123

首次从新设备访问 – Citrix Virtual Apps and Desktops 风险指标 123

首次从新 IP 访问 - Citrix Gateway 风险指标 123

从可疑 IP 登录 - Citrix Gateway 风险指标 124

Citrix Gateway 事件的自助搜索 124

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Remote Browser Isolation™ 事件的自助搜索 125
从监视列表中删除操作 125
配置 StoreFront 部署时改进的入门消息 125
已弃用的功能 126
风险指示器 - 从新设备访问已移除 126
已修复的问题 126
November 08, 2019 126
已修复的问题 126
October 21, 2019 126
新增功能 126
分析代理的名称已修改 126
自定义报告支持时间维度 127
审核日志增强功能 128
已修复的问题 129
September 23, 2019 129
已修复的问题 129
August 30, 2019 129
新增功能 129
仪表板默认时间段的更改 129
已修复问题 129
August 20, 2019 130
新增功能 130
自助搜索增强功能 130
自定义报告增强功能 130
风险指标控制板 130
风险用户控制板增强功能 131
共享链接风险指标 - 过度下载 132
身份验证数据的自助搜索 132

© 1997–2026 Citrix Systems, Inc. All rights reserved.

July 11, 2019 133
新增功能 133
自定义风险指标 133
风险时间轴上的特权状态 133
共享链接过期操作 133
自助搜索增强功能 133
站点卡上的数据错误状态 134
已修复问题 134
June 19, 2019 134
已修复问题 134
June 17, 2019 134
新功能 134
StoreFront 配置 134
May 30, 2019 135
新功能 135
登录失败次数过多 135
已修复问题 135
May 09, 2019 135
新增功能 135
创建自定义报告 135
特权用户监控 136
每周电子邮件摘要 136
April 26, 2019 136
新增功能 136
委派管理员 136
已修复的问题 136
February 19, 2019 137
新增功能 137

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Splunk 集成 137
动态会话录制 137
共享链接仪表板和风险指示器 137
微软 Active Directory 集成 138
January 04, 2019 138
新增功能 138
为现有风险指标添加 SOURCE 列 138
高级用户配置文件 138
Microsoft Graph Security 风险指标 139
进入自助搜索页面的方法 139
内容协作的自助搜索 139
应用程序和桌面的自助搜索 140
将自助搜索事件导出到 CSV 文件 140
改进了 Citrix Virtual Apps and Desktops 的入门体验 140
November 29, 2018 140
新增功能 140
微软安全图谱数据源 140
在数据源的站点卡片上查看事件详细信息和发现的用户 141
November 16, 2018 142
新功能 142
访问数据的自助搜索 142
风险指示器反馈 143
已修复问题 143
已知问题 144
分析产品 145
数据源 146
Citrix 数据源 146
外部数据源 148

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持的区域 149
Citrix Workspace 应用程序版本矩阵 150
数据治理 152
系统要求 153
Citrix 安全分析订阅 153
数据源要求 153
支持的浏览器 153
管理 Security Analytics 的管理员角色 154
自定义角色的权限 154
管理员的安全警报通知 155
开始使用 157
步骤 1：登录 Citrix Cloud™ 157
步骤 2：访问 Security Analytics 157
步骤 3: 管理安全分析 158
后续步骤 159
Citrix 端点管理™ 数据源 160
先决条件 160
查看数据源并开启数据处理 161
查看用户和接收到的事件 161
开启或关闭数据处理 163
Citrix Gateway（本地部署）数据源 165
Citrix 远程浏览器隔离™ 数据源 165
思杰安全私有访问™ 数据源 165
先决条件 165
查看数据源并开启数据处理 165
查看用户和接收到的事件 166
开启或关闭数据处理 168
Citrix 虚拟应用和桌面™ 和 Citrix DaaS 数据源 168

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持的客户端版本 169
在 Citrix DaaS 上启用分析 169
先决条件 169
查看数据源并开启数据处理 169
查看云站点、用户和接收到的事件 170
在本地 Citrix Virtual Apps and Desktops 上启用分析 172
先决条件 172
使用 StoreFront 载入 Citrix Virtual Apps and Desktops 本地站点 173
使用 Workspace 载入 Citrix Virtual Apps and Desktops 本地站点 173
连接到本地站点的 Citrix Director 177
先决条件和配置步骤 177
查看已连接的站点和收到的事件 177
连接到会话录制部署 179
先决条件 179
配置您的 Session Recording 服务器 179
查看已连接的部署 182
查看收到的事件 182
添加会话录制服务器 183
删除会话录制服务器 183
为 Citrix DaaS 启用打印遥测 184
先决条件 184
在电源管理计算机中启用打印遥测 184
在新的主映像中启用打印遥测 186
在未进行电源管理的计算机中启用打印遥测 186
为新建物理 VDA 启用打印遥测 187
创建注册表项 187
为组织单位启用打印跟踪 195
启用 Citrix DaaS 的剪贴板遥测 196

© 1997–2026 Citrix Systems, Inc. All rights reserved.

先决条件 196

开启或关闭数据源上的数据处理 197

微软活动目录和 Azure 活动目录集成 197

先决条件 198

连接微软活动目录 198

连接微软 Azure 活动目录 199

查看用户信息 199

Microsoft Graph 安全集成 200

先决条件 200

载入 Microsoft Graph Security 实例 200

启用或禁用数据处理 202

安全信息和事件管理 (SIEM) 集成 204

优势 204

SIEM 集成架构 204

开启或关闭数据传输 205

设置 SIEM 环境 205

SIEM 导出帐户设置 206

SIEM 配置和环境设置 206

从 Citrix Analytics for Security 导出到您的 SIEM 服务的数据事件 207

SIEM 集成故障排除 208

Splunk 集成 209

实现 Citrix Analytics for Security™ 与 Splunk 的集成 209

数据导出 209

重置密码功能 211

启用或禁用数据传输 212

适用于 Splunk 的 Citrix Analytics 附加组件 213

适用于 Splunk 的 Citrix Analytics 附加组件（本地/企业版） 213

支持的版本 213

© 1997–2026 Citrix Systems, Inc. All rights reserved.

先决条件 214

下载并安装适用于 Splunk 的 Citrix Analytics 附加组件 214

配置适用于 Splunk 的 Citrix Analytics 附加组件 215

适用于 Splunk 的 Citrix Analytics 附加组件（云） 218

先决条件 218

下载并安装适用于 Splunk 的 Citrix Analytics 附加组件 219

配置适用于 Splunk 的 Citrix Analytics 附加组件 219

如何在您的 Splunk 环境中消费事件 220

排除 Splunk 版 Citrix Analytics 附加组件故障 221

Splunk 版 Citrix Analytics 应用程序 221

支持的 Splunk 版本 222

Splunk 版 Citrix Analytics 应用程序的先决条件 222

安装和配置 222

Splunk 架构与 Citrix Analytics 附加应用程序 224

适用于 Splunk 的 Citrix Analytics 控制板 226

先决条件 226

用户风险评分概览 226

风险指标概述 227

选择类别以查看报告 228

查看报告 228

风险指标详细信息 229

选择类别以查看报告 230

查看报告 230

实体详细信息 231

查看报告 232

用户配置文件概述 233

查看事件 233

收到的事件 234

© 1997–2026 Citrix Systems, Inc. All rights reserved.

查看报告 234
事件关联示例 235
先决条件 235
关联事件 235
无事件故障排除 236
适用于 Splunk 的 Citrix Analytics 附加组件的配置问题 236
微软 Sentinel 集成 237
先决条件 237
与 Microsoft Sentinel 集成 238
开启或关闭数据传输 242
适用于 Microsoft Sentinel 的 Citrix Analytics 工作簿 244
先决条件 244
查看 Citrix Analytics 事件 244
查看 Citrix Analytics 工作簿 245
用户风险评分概览 247
用户详细信息 247
用户配置文件 247
接收到的事件 248
风险指标详细信息 249
风险指标概览 250
通过 Logstash 集成 Sentinel 的故障排除指南 250
检查 Logstash 服务器日志 250
常见错误：使用捆绑的 JDK 251
检查 Microsoft Sentinel 工作簿 253
使用 KQL 检查 Log Analytics 工作区日志 254
Elasticsearch 集成 255
先决条件 255
与 Elasticsearch 集成 255

© 1997–2026 Citrix Systems, Inc. All rights reserved.

开启或关闭数据传输 258
使用 Kafka 或 Logstash 数据连接器进行 SIEM 集成 258
先决条件 258
使用 Kafka 与 SIEM 服务集成 259
数据流 261
身份验证 262
使用 SSL 进行加密，并使用 SASL/SSL 和 SASL/PLAINTEXT 进行身份验证 262
使用 Logstash 进行 SIEM 集成 263
使用 Logstash 与 SIEM 服务集成 263
开启或关闭数据传输 266
Citrix Analytics 适用于 SIEM 的数据导出格式 268
适用于 SIEM 的风险洞察数据 269
风险洞察事件的架构详细信息 270
用户配置文件数据架构 271
用户风险评分架构 275
风险评分变更架构 276
风险指标架构 277
Citrix Secure Private Access 风险指标架构 281
Citrix Endpoint Management 风险指标架构 289
Citrix Gateway 风险指标架构 295
Citrix DaaS 和 Citrix Virtual Apps and Desktops 风险指标架构 318
微软活动目录指标 332
自定义风险指标架构 334
数据源事件 354
数据源事件的架构详细信息 355
思杰虚拟应用和桌面事件 355
安全私有访问事件 356
设备姿态服务事件 356

© 1997–2026 Citrix Systems, Inc. All rights reserved.

利用 Citrix Analytics SIEM 数据模型进行威胁分析和数据关联 356
自定义风险指标洞察 357
在 Citrix Analytics 中设置自定义风险指标 357
Splunk 上的风险指标事件 - 原始查询 360
Splunk 上的风险指标事件 - 仪表板应用程序 361
数据源事件 362
故障排除数据导出 363
摘要选项卡 364
Citrix Analytics 中的可用数据 364
可供 SIEM 使用的事件 366
SIEM 的数据消耗 366
数据导出快速指南 371
测试事件生成 376
SIEM 电子邮件警报 378
如何启用电子邮件通知? 379
SIEM 电子邮件警报类型 379
安全洞察的 Sigma 签名示例 385
如何使用这些示例 385
查看数据源并开启数据处理 385
使用 CAS 查询 385
使用 Sigma 签名 386
受感染的端点 386
未经授权的浏览器 386
详细信息 386
CAS 查询 387
Sigma 签名 387
未经授权的操作系统 388
详细信息 388

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CAS 查询 388
Sigma 签名 388
未经授权的 IP 地址或子网 389
详细信息 389
CAS 查询 389
Sigma 签名 389
允许列表之外的未经授权的操作系统 390
详细信息 390
CAS 查询 390
Sigma 签名 390
未经批准的 Workspace 应用程序版本 391
详细信息 391
CAS 查询 391
Sigma 签名 392
内部威胁 393
异常桌面名称 393
详细信息 393
CAS 查询 393
Sigma 签名 393
监控特定进程 394
详细信息 394
CAS 查询 394
Sigma 签名 394
未经授权的虚拟应用程序 395
详细信息 395
CAS 查询 395
Sigma 签名 395
数据外泄 396

© 1997–2026 Citrix Systems, Inc. All rights reserved.

从 SaaS 应用程序打印 396
详细信息 396
CAS 查询 396
Sigma 签名 396
SaaS 应用程序上的剪贴板使用情况 397
详细信息 397
CAS 查询 397
Sigma 签名 397
用户仪表板 399
概述 399
用户活动状态 399
筛选条件 400
搜索框 400
最新评分 400
用户 400
发现的数据源 400
已触发的指标 401
已应用的操作 401
已处理的事件 402
用户风险分布 403
风险用户 403
高风险 403
中风险 404
低风险 404
热门用户 404
观察列表用户 405
风险类别 406
用例 407

© 1997–2026 Citrix Systems, Inc. All rights reserved.

如何分析风险类别仪表板? 408

风险类别类型 410

数据渗漏 410

内部威胁 410

受损用户 411

受损端点 411

风险指标和操作 412

访问摘要 413

策略和操作 414

热门策略 414

所有策略 415

热门操作 415

操作 415

风险指标 416

访问保障仪表板 417

查看仪表板 417

访问摘要 417

登录位置 418

未识别的位置 420

启用地理围栏 421

地理围栏：唯一用户登录 424

登录网络 426

查看用户网络详细信息 426

查看用户的访问配置文件 427

分面 428

查看用户登录详细信息 429

搜索栏 431

筛选条件 432

© 1997–2026 Citrix Systems, Inc. All rights reserved.

用户风险时间线和配置文件 433
风险时间线 434
风险摘要 437
用户配置文件 438
Citrix® 用户风险指标 439
思杰终端管理™ 风险指标 441
检测到黑名单应用程序的设备 441
何时触发检测到黑名单应用程序的设备风险指标? 441
如何分析检测到黑名单应用程序的设备风险指标? 441
您可以对用户执行哪些操作? 443
检测到越狱或已获得 root 权限的设备 443
何时触发检测到越狱或已获得 root 权限的设备风险指标? 444
如何分析检测到越狱或已获得 root 权限的设备风险指标? 444
您可以对用户执行哪些操作? 445
检测到非托管设备 445
何时会触发检测到非托管设备风险指标? 446
如何分析检测到非托管设备的风险指标? 446
您可以对用户执行哪些操作? 448
Citrix Gateway 风险指标 448
端点分析 (EPA) 扫描失败 448
EPA 扫描失败风险指标何时触发? 449
如何分析 EPA 扫描失败风险指标? 449
您可以对用户执行哪些操作? 450
身份验证失败过多 451
身份验证失败过多风险指示器何时触发? 451
如何分析身份验证失败过多风险指示器? 451
您可以对用户执行哪些操作? 453
不可能行程 453

© 1997–2026 Citrix Systems, Inc. All rights reserved.

何时会触发“不可能行程”风险指标? 454

如何分析“不可能行程”风险指标 454

您可以对用户执行哪些操作? 456

从可疑 IP 登录 456

何时触发“从可疑 IP 登录”风险指示器? 457

如何分析来自可疑 IP 的登录风险指标? 457

您可以对用户执行哪些操作? 459

可疑登录 460

何时触发“可疑登录”风险指示器? 460

如何分析可疑登录风险指标 461

您可以对用户执行哪些操作? 463

异常身份验证失败 463

异常身份验证失败指标何时触发? 463

如何分析异常身份验证失败指标? 464

您可以对用户执行哪些操作? 466

思杰安全私有访问™ 风险指标 467

危险网站访问 467

尝试访问黑名单 URL 467

何时触发“尝试访问黑名单 URL”风险指标? 467

如何分析“尝试访问黑名单 URL”风险指标? 467

您可以对用户执行哪些操作? 469

异常上传量 469

何时触发异常上传量风险指示器? 470

如何分析异常上传量风险指示器? 470

您可以对用户执行哪些操作? 471

数据下载过多 472

何时触发数据下载过多风险指标? 472

如何分析数据下载过多风险指标? 472

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以对用户执行哪些操作? 474

Citrix 虚拟应用和桌面™ 和 Citrix DaaS 风险指标 474

不可能的行程 474

何时会触发“不可能的行程”风险指标? 475

如何分析“不可能的行程”风险指标 475

您可以对用户执行哪些操作? 477

潜在数据泄露 477

潜在数据泄露风险指标何时触发? 478

如何分析潜在数据泄露风险指标? 478

您可以对用户应用哪些操作? 480

可疑登录 481

何时触发可疑登录风险指示器? 481

如何分析可疑登录风险指标 482

您可以对用户执行哪些操作? 485

提供用户风险指标的反馈 485

查看筛选器 487

Microsoft Graph Security 风险指标 491

如何分析 Microsoft Graph Security 风险指标 491

如何获取有关风险指标的更多信息 492

您可以对用户执行哪些操作 492

自定义风险指标 493

预配置的自定义风险指标 493

自定义风险指标页面 493

分析自定义风险指标 494

可应用于用户的操作 495

自定义风险指标模板 495

创建自定义风险指标 496

为自定义风险指标定义条件 497

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用高级选项 498
选择风险类别 501
选择严重性 501
定义条件支持的运算符 501
修改自定义风险指标 504
删除自定义风险指标 504
持续风险评估 505
用例 505
主要功能 506
支持多种条件 506
在应用操作前通知用户 506
应用操作后通知用户 506
强制执行和监控模式 506
访问和策略控制板的可见性 506
默认策略 507
策略和操作 510
什么是策略? 510
默认策略 511
如何添加或删除条件? 511
默认和自定义风险指标 512
什么是操作? 512
预配置的自定义风险指标和策略 516
针对地理围栏场景的预配置自定义风险指标 516
用于地理围栏场景的预配置策略 517
使用预配置的地理围栏自定义风险指标创建您自己的策略 518
首次访问场景的预配置自定义风险指标 519
终端用户电子邮件设置 522
修改电子邮件设置 522

© 1997–2026 Citrix Systems, Inc. All rights reserved.

监视列表 525
如何将用户添加到监视列表 525
如何将用户从监视列表移除 526
如何监控观察列表中的用户 527
每周电子邮件通知 528
启用电子邮件通知 528
您何时会收到来自 Citrix Analytics 的电子邮件? 528
账户摘要 530
数据摘要 530
用户信息 531
热门风险指标 531
热门操作 532
收到电子邮件后需要执行哪些操作? 533
审计日志 535
生成审计事件的活动 535
如何查看审计日志 536
如何使用审计日志 536
自定义报告 538
自定义报告中支持的字段 538
报告 539
创建自定义报告 540
使用模板创建自定义报告 540
创建无模板的自定义报告 543
保存报告 543
查看报告 545
导出报告 545
删除报告 546
编辑报告 546

© 1997–2026 Citrix Systems, Inc. All rights reserved.

执行摘要报告 546
它包含哪些报告? 547
编辑执行报告 548
自助搜索 552
用于身份验证的自助搜索 552
选择身份验证数据源 552
选择筛选条件以筛选事件 552
指定搜索查询以筛选事件 553
Gateway 的自助搜索 555
选择 Gateway 数据源 555
使用分面筛选事件 555
指定搜索查询以筛选事件 557
搜索查询支持的值 559
访问洞察标志 559
应用程序字节消耗 560
认证服务器IP 560
认证阶段 560
身份验证类型 560
后端服务器名称 561
浏览器 561
城市 561
客户端 IP 561
客户端 IP 类型 561
客户端端口 562
国家/地区 562
事件类型 562
网关-FQDN 563
网关 IP 563

© 1997–2026 Citrix Systems, Inc. All rights reserved.

网关端口 563
注销模式 563
NetScaler-IP 564
操作系统 564
记录类型 564
SSO-认证方法 564
服务器 IP 565
服务器端口 565
会话状态 565
状态码 565
用户代理 566
VPN-会话-ID 566
VPN-会话-模式 566
策略的自助搜索 567
选择策略数据集 567
选择方面以筛选事件 567
指定搜索查询以筛选事件 568
远程浏览器隔离（安全浏览器）的自助搜索 570
先决条件 570
选择远程浏览器隔离数据源 570
指定搜索查询以筛选事件 571
查看用户事件详情 572
Secure Private Access 的自助搜索 572
选择 Secure Private Access 数据源 573
选择方面以筛选事件 573
指定搜索查询以筛选事件 575
应用程序和桌面的自助搜索 576
选择应用程序和桌面数据源 576

© 1997–2026 Citrix Systems, Inc. All rights reserved.

选择方面以筛选事件 577
指定搜索查询以筛选事件 577
事件类型和支持的字段 579
搜索查询支持的值 584
操作系统命名格式 592
Citrix Analytics for Security and Performance 故障排除 594
将匿名用户验证为合法用户 594
排查数据源的事件传输问题 594
触发 Virtual Apps and Desktops 事件、SaaS 事件并验证事件传输 594
未从受支持的 Citrix Workspace™ 应用程序版本接收到用户事件 594
已配置的 Session Recording 服务器无法连接 594
无法将 StoreFront™ 服务器连接到 Citrix Analytics 594
常见问题 595
术语表 596

© 1997–2026 Citrix Systems, Inc. All rights reserved.

新增功能

Citrix 的目标是在新功能和产品更新可用时将其交付给 Citrix Analytics 客户。新版本提供更多价值，因此没有理由延迟更新。

对您（客户）而言，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。分阶段增量地交付更新有助于确保产品质量并最大限度地提高可用性。

April 15, 2024

新增执行摘要报告

您现在可以选择将多个报告整合为一份执行报告，该报告可按所需时间段进行安排。借助此新功能，您只需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。

January 29, 2024

Workspace 应用程序状态字段更新

- **自助搜索**：您现在可以利用针对 **Citrix Apps and Desktops** 数据源新引入的 **Workspace 应用程序状态**字段，执行查询以查找 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，请参阅适用于 Apps and Desktops 的自助搜索。

January 25, 2024

CAS UI 中的不一致之处已得到简化

针对 **Apps and Desktops** 数据源的**自助搜索**功能中已解决以下问题：

- 以前在会话中乱序显示的事件现在已正确显示。
- 默认列已更新。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 24, 2024

SIEM 环境中增强的用户配置文件事件

导出到 SIEM 环境的用户配置文件事件现在包括：

- IP 地址洞察
- Citrix Virtual Apps and Desktops™ 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）位置洞察

这些新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。

December 01, 2023

用于每周电子邮件和 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接收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。

用户仪表板 - 新增活动用户计数时间筛选器并更新了“概述”部分

用户仪表板中的新时间筛选器允许您查看和修改组织中特定时间段内的活动用户总数，同时考虑已启用 Citrix Analytics 的数据源。

用户仪表板中增强的**概述**部分显示了组织中的用户总数，以及当前登录的活动和非活动用户数。

有关详细信息，请参阅用户仪表板。

增强型自定义报告

- 您现在可以使用 Citrix Analytics for Security 中提供的事件和洞察来创建和安排自定义报告。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。
- 您现在可以使用增强型自定义报告平台功能，其中包括基于自助服务搜索查询的报告、模板、更好的可视化效果、涵盖所有数据源和指标、安排报告以及导出 PDF。

有关详细信息，请参阅自定义报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

November 30, 2023

移除 Citrix Analytics 中的所有 ShareFile 功能

以下 ShareFile 检测功能已移除：

- 共享链接
- 关联风险指标
- 及其出现次数的策略
- 内容协作数据导出配置
- 内容协作报告
- 搜索中的内容协作数据源
- 内容协作已保存搜索
- 内容协作数据源。

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

了解 ShareFile 如何直接简化对安全控制的访问，来自 <ShareFile.com>。

September 22, 2023

自定义指示器中的 Citrix Secure Browser 数据源

您现在可以为 Citrix Secure Browser 数据源创建风险指示器，以跟踪用户在安全浏览器中的活动。有关更多信息，请参阅 (/zh-cn/security-analytics/custom-risk-indicators.html)。

增强每周电子邮件与 SIEM 数据导出功能

每周电子邮件已得到增强，通过启用 SIEM 数据导出，可更深入地了解组织的安全状况。您现在可以加入并激活更多数据源，以发现围绕用户的各种事件。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。
- 根据数据导出消耗状态提供数据导出建议。

有关更多信息，请参阅 (/zh-cn/security-analytics/weekly-email.html)。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在电子邮件中消耗自定义管理员的通知首选项

Citrix Analytics for Security 现在遵守自定义管理员在 Citrix Cloud 中设置的通知首选项。此增强功能为自定义管理员提供了更大的灵活性来管理其通知首选项。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。

有关更多信息，请参阅 (/zh-cn/security-analytics/manage-security-admins.html)。

July 04, 2023

自助搜索和自定义指标中支持 OR 运算符

OR 运算符现已在**自助搜索**和**自定义风险指标**功能中可用。您可以在自助搜索和自定义指标查询等搜索视图中使用 **OR** 运算符。

有关详细信息，请参阅搜索查询中支持的运算符。

June 15, 2023

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，会触发一个名为 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剪贴板操作是否被允许。VDA 剪贴板事件属性也可在自助搜索和自定义风险指标工作流中使用。

- **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。
- **自定义风险指标**：VDA 剪贴板事件的属性可用于自定义指标工作流。您可以使用这些事件键/值对来配置自定义指标触发器并设置带操作的自动化策略。

您可以使用**用于安全监控的剪贴板位置元数据收集**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”页面并禁用它，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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

June 14, 2023

Citrix Analytics for Security 中提供会话录制应用程序生命周期和注册表事件

以下来自**会话录制**的**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。

有关更多信息，请参阅事件类型和支持的字段。

June 08, 2023

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。这导致在自助服务搜索和访问保障用户登录页面上，某些事件的用户名列显示为 **NA**。有时，当查看 **Last 1 Hour** 或 **Last 1 Day** 等小时间范围的数据时，即使访问保障 IP 注册组织图表中的总登录计数不为零，唯一用户计数也显示为零。此问题现已修复。
- 在应用程序和桌面自助服务搜索中，对于 Session.Logon 和 Session.end 用户事件，搜索查询中的 App-Name 维度填充的是交付组名称，而不是启动的应用程序或桌面名称，这可能会误导管理员。App-Name 维度对于 App.Start/App.End 事件的查询更有用，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自助服务搜索。此问题现已修复。
- 如果您的组织在 **Asia Pacific South** 主区域加入 Citrix Cloud，则内容协作事件在您的 Citrix Analytics 租户中不可见。此问题现已修复。
- Citrix Workspace 应用程序和 Citrix Receiver 客户端的某些版本不会向 Citrix Analytics 发送特定事件。因此，Citrix Analytics 无法为这些事件提供洞察并生成风险指标。此问题现已修复。有关更多信息，请参阅检查 6：虚拟应用程序和桌面事件是否传输到 Analytics？。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

May 29, 2023

适用于 Splunk 的 Citrix Analytics 附加组件现已在 Splunk Cloud 平台上推出

Citrix Analytics 的 Splunk 集成利用适用于 Splunk 的 Citrix Analytics 附加组件连接到分析环境，并将业务关键数据引入您的 Splunk 环境。

此前，该附加组件仅由 Splunk 审查，用于在 Splunk Enterprise 层上安装，客户负责在其本地 Splunk 环境中配置该附加组件。借助最新版本 2.1.2，该附加组件增加了与 Splunk Cloud 的 Splunk 平台兼容性。使用带有 IDM 的 **Classic** 实例或 **Victoria** 实例的客户可以利用此平台兼容性增强功能。现在，客户在考虑部署我们的附加组件以促进 Splunk 集成时，可以灵活选择 Splunk Enterprise 或 Splunk Cloud。

有关详细信息，请参阅 Splunk Integration。

SIEM 中的会话录制事件

现在，**会话录制**事件可以以适用于应用程序和桌面的**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在**数据导出**页面下的“用于导出阶段的数据事件”中找到。

有关详细信息，请参阅 Policies and Actions。

May 24, 2023

通知最终用户全局操作

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，该操作可与内置或自定义风险指示器触发器配对使用。管理员可以使用**通知最终用户**操作创建策略，该操作仅为最终用户生成电子邮件通知。此操作可用于各种合规性用例，例如通知用户未经授权的应用程序使用情况，或在不采取任何破坏性操作的情况下，就其 Citrix 帐户上的可疑行为发出警报。管理员可以根据具体情况自定义电子邮件正文和主题行。

有关详细信息，请参阅 Notify End User。

May 04, 2023

测试事件生成

测试事件生成功能旨在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，则需要等待数据源载入和用户活动，以检查事件是否由 Citrix Analytics 生成并因此由其

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SIEM 环境接收。这不再是必需的。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，并使用提供的查询检查 Citrix Analytics SIEM 集成是否按预期设置。这对于尝试调试中断数据流的管理员也适用，因为它可以帮助隔离故障点。

有关详细信息，请参阅 Test Event Generation。

SIEM 电子邮件警报生成

SIEM 电子邮件警报生成功能将数据导出的故障排除过程提升到一个新的便捷水平。Citrix Analytics 会针对可能导致或指示 SIEM 数据流中断的活动发送系统警报。此电子邮件将分发给 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**

   当从“数据导出”页面重置帐户密码时，会触发此电子邮件。如果仅在 Citrix Analytics for Security GUI 上执行此操作，可能会导致数据流中断。此警报包含执行密码重置的时间，从而使恢复成功的数据流变得更加容易。

2. **SIEM 数据导出警报 - 数据流已停止**

当客户遇到数据流中断时，会触发此电子邮件

- **超过 24 小时** - 关键时间，可通过使用警报中提供的有用故障排除提示或利用带有**快速指南**的**数据导出摘要**选项卡来快速恢复成功的数据流。
- **超过 7 天** - 每个客户主题的 Kafka 保留策略为七天，这意味着某些安全态势数据可能已过期。必须使用故障排除工具将数据流恢复到 SIEM。
- **超过 30 天** - 这意味着客户的数据存在安全问题，需要立即关注将数据流从 Citrix Analytics 恢复到 SIEM 环境。

有关详细信息，请参阅 SIEM 电子邮件警报生成。

April 13, 2023

已修复的问题

Windows Citrix Workspace™ 应用程序从 Citrix Workspace 应用程序版本 2203 及更高版本发送空的文件名、路径和格式属性。因此，Citrix Analytics for Security GUI 在“下载文件名”、“下载文件路径”和“下载文件格式”列中显示 NA 值。此问题现已修复。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

March 31, 2023

Citrix Analytics for Security 中的会话录制事件

在 Citrix Apps and Desktops 中，已添加两种新的事件类型，以帮助识别和评估基于会话录制的事件。

- 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的描述。此外，这些事件还可以在**自定义风险指标**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。
- **自定义风险指标**：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。

自助搜索中的应用保护事件

当您尝试在 Citrix Apps and Desktops 数据源下的受保护会话中捕获屏幕截图时，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 > 用于导出的数据事件 >** 从“数据源事件（可选）”类别中选择 **Apps and Desktops**。

您还可以查看 **Session.Logon** 事件的新属性，称为**应用保护策略**。

有关详细信息，请参阅事件类型和支持的字段。

March 30, 2023

自定义角色支持

管理员可以使用 Active Directory 或 Azure Active Directory 中的组，或者通过为 Citrix Analytics for Security 设置 Okta 集成来添加自定义角色。此集成提供了一种简化的方法来管理所有组管理员的服务访问权限。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。如果管理员同时是这两个组的成员，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 UI 故障排除面板

数据导出 UI 进行了以下增强：

- **摘要选项卡**：摘要选项卡描述了 SIEM 事件指标、数据源载入状态和以下场景中的数据消耗状态：
  - **Citrix Analytics 中的可用数据**：提供不同数据源的载入状态。
  - **可供 SIEM 消耗的事件**：提供发送到 SIEM 环境的洞察数量。
  - **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**，这使得设置和维护 SIEM 集成变得更简单。**数据导出快速指南**链接可从**摘要**和**配置**选项卡访问。

有关更多信息，请参阅数据导出故障排除。

March 24, 2023

用户配置文件视图更改

与应用程序、位置、设备和 ShareFile 数据使用相关的**用户配置文件数据**在用户时间线中的**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 -

- 职位
- 地址
- 电子邮件
- 电话
- 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，请参阅用户配置文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

从所有搜索视图中移除动态自动建议

针对基于租户历史数据的维度的自动建议功能现已弃用，适用于以下页面：

- 自助搜索
- 自定义风险指标

但是，针对 **Event-Type** 和 **Clipboard-Operations** 等维度的静态建议仍在搜索框中可用。

有关详细信息，请参阅如何使用自助搜索。

March 21, 2023

建议面板，帮助加入本地 StoreFront™ 数据源

数据源页面中引入了一个新的**建议**面板。**数据源**页面上的**建议**面板向用户介绍了加入本地 StoreFront 数据源的重要性。它帮助用户轻松加入本地 StoreFront 数据源，并为用户提供了一个选项，以审查并确保加入所有可用的数据源。

有关更多详细信息，请参阅连接到 StoreFront 部署。

February 23, 2023

已修复的问题

对于 Citrix Apps and Desktop 版本 > 1912 的本地 Citrix Apps and Desktop 部署，操作失败。在手动和基于策略的操作中都发现了此问题。此问题现已修复。

当虚拟应用程序仅启动一次时，“应用程序和桌面自助服务搜索”页面会显示多个应用程序启动和应用程序结束事件。此问题发生在适用于 Linux 客户端版本的 Citrix Workspace 应用程序上。此问题现已修复。

2022 年 4 月 4 日之后至 2022 年 5 月底，来自 Secure Private Access 服务的用户事件可能在您的 Citrix Analytics 租户中不可用。此问题现已修复。

February 22, 2023

每周电子邮件通知的增强功能

Citrix Analytics 会发送每周电子邮件通知，帮助您总结组织的安全风险敞口。每周电子邮件通知已通过以下更新得到改进：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 提供用户风险分布视图 - 一周内发现的用户总数、高风险用户数和非风险用户数
- 一周内处理的事件总数
- 一周内触发的指标总数
- 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“自助服务搜索”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标，还可以将该字段作为“导出到 CSV”格式的一部分进行导出。

有关更多信息，请参阅应用程序和桌面自助服务搜索。

浏览器派生字段的更改

以前，“自助服务搜索”页面包含“**浏览器**”、“**浏览器主要版本**”和“**浏览器次要版本**”字段，用于表示浏览器名称和版本。但是，为了确保清晰度和准确性，现在这三个字段已被弃用，并在“自助服务搜索”、“自定义指标模板”以及“应用程序和桌面数据源”的 CSV 下载中替换为“**浏览器名称**”和“**浏览器版本**”。

有关详细信息，请参阅应用程序和桌面的自助服务搜索。

February 16, 2023

已修复问题

在为租户获取用户名掩码状态时，某些欧盟和亚太南部客户的每周电子邮件受到影响。因此，由于异常，管理员收到了 10 封相同的每周电子邮件。一旦发生异常，后续租户将不会收到每周电子邮件。此问题现已修复。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

February 03, 2023

适用于欧盟和亚太南部地区的 Citrix Secure Private Access™ 服务的分析支持

Citrix Analytics for Security 现在处理来自欧盟地区和亚太南部地区可用的 Citrix Secure Private Access 的用户事件。如果您的组织从欧盟地区或亚太南部地区加入 Citrix Cloud，则可以查看正在使用 Secure Private Access 服务的用户的风险洞察。

有关详细信息，请参阅数据源。

January 11, 2023

从 Secure Private Access 中移除 Web 过滤功能

Web 过滤功能已从 Secure Private Access 类别中移除。由于 Secure Private Access 弃用了基于类别的 Web 过滤，Citrix Analytics for Security 上的以下功能受到影响：

1. “类别组”、“类别”和“URL 信誉”等数据字段在 Citrix Analytics for Security 控制板上不再可用。
2. 依赖相同数据的“高风险网站访问”指标也已弃用，并且不会为客户触发。
3. 任何使用数据字段（类别组、类别和 URL 信誉）及其相关策略的现有自定义风险指标将不再触发。
4. “**用户访问**”和“**应用程序访问**”选项卡。
5. SIEM 导出将继续在一段时间内包含 urlcategory、urlcategorygroup 和 urlcategoryreputation 属性，并带有以下虚拟值：
    - 类别和类别组为 99999
    - 信誉为 0

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

December 27, 2022

自助搜索中数据源下拉列表的更改

自助搜索页面中的数据源列表已更改，默认显示为**会话**而不是**应用程序和桌面**。此外，性能部分已移至顶部，后跟安全部分，因为性能数据源之前不可见。

有关详细信息，请参阅 自助搜索。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

December 13, 2022

用户仪表板增强功能

用户仪表板已通过摘要和图表进行了改进，以帮助管理员监控组织的安全状况。此视图不仅提供已发现用户、触发的风险指标和已应用操作的详细信息，还提供关键指标的基于时间的趋势线，以便更好地评估风险。管理员可以深入查看感兴趣的数据，并导航到具有正确上下文的相关仪表板，以进行更快的风险分析。

有关详细信息，请参阅 用户仪表板。

December 05, 2022

访问保障仪表板 - 登录网络

新增了“登录网络”部分，提供以下用户详细信息：

- 与用户登录所用的 IP 地址相关的组织。
- 用户登录所用的唯一公共子网和私有子网总数。
- 用户使用代理和专用 VPN 服务登录的详细信息。

利用这些额外详细信息，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预期。

有关更多详细信息，请参阅访问保障仪表板。

November 18, 2022

已修复问题

- 已修复在没有任何源事件的情况下被错误触发的地理围栏指示器。

November 08, 2022

重命名操作

Citrix Analytics for Security 中使用的一些操作已重命名以提供更清晰的说明。这些操作包括：

- **通知管理员** - 通知管理员
- **锁定用户** - 锁定用户帐户

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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，请参阅什么是操作？

已修复的问题

- 如果从时间线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。此情况发生在最新版本的 Firefox 中。此问题现已修复。
- **HardDrive**、**harddrive** 和 **HDD** 类别合并为一个类别，即 **Hard Disk Drive**，用于 Apps and Desktops 数据源的自助服务搜索中的 Download-Device-Type 字段。
- 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。应用程序中已实施重复数据删除机制以防止此问题。

October 19, 2022

数据源事件选择和导出

您现在可以利用新的数据事件导出工作流，除了机器学习生成的风险洞察事件和相关数据之外，还可以导出数据源事件。

这使安全和安全运营 (SOC) 管理员能够：

- 将 Citrix Analytics 中的数据与其他聚合在安全信息和事件管理 (SIEM) 系统上的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

数据事件将传递到您现有的 SIEM 集成和数据连接器，并且与我们的自助服务事件搜索视图中可用的内容保持一致。

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

October 18, 2022

允许管理员在 Citrix DaaS™ 站点上运行动态会话录制操作

管理员现在可以在 Citrix DaaS 站点上运行动态会话录制操作，并动态录制用户的虚拟会话。他们可以配置一个策略，以便在 Citrix Analytics for Security 检测到特定用户的危险活动时自动开始录制用户会话。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关详细信息，请参阅 什么是操作？

October 14, 2022

为用户风险指标提供反馈

Citrix Analytics for Security 管理员现在可以通过在指标详细信息面板上提供反馈，将用户风险指标报告为有用或无用。此功能使管理员能够报告误报、减少频繁触发指标的干扰，并与其他管理员共享更多上下文。此外，无用的风险指标将从用户的时间线中隐藏，并且用户风险评分将重新校准。

有关详细信息，请参阅 为用户风险指标提供反馈。

September 26, 2022

访问保障支持地理围栏阻止列表

“**安全**”和“**危险位置**”选项卡已添加到地理围栏设置中。

- 安全位置地理围栏有助于识别和限制对已定义地理围栏区域之外的访问。
- 危险位置地理围栏有助于根据组织的已知行为检测并缩小危险用户访问范围。

安全和危险地理围栏都由其各自预配置的自定义风险指标提供支持。

有关详细信息，请参阅 启用地理围栏。

已修复的问题

- Citrix Cloud API 在电子邮件正文中显示**客户名称**。现在，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**。
- Citrix Gateway 数据源卡在 **Citrix Analytics for Security** 和 **Citrix Analytics for Performance™** 之间是通用的。数据处理不断调用 Citrix Analytics for Security 端点，并且对于仅拥有 **Citrix Analytics for Performance** 权利的客户而言已损坏。
- 当 Citrix Cloud 同时收到多个权利消息时，在更新 Redis 缓存时会出现争用情况。在这种情况下，一个权利消息会更新到缓存中，其余的则会丢失。此问题现已修复，可更新缓存中的所有权利消息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

September 13, 2022

共享链接仪表板增强功能

共享链接仪表板已通过摘要视图和详细视图进行了改进。摘要视图包含最活跃的共享和风险最高的共享。详细视图通过引入创建者、活动计数、身份验证类型、权限、共享类型和内容等属性，为管理员提供了更多信息。管理员可以根据需要深入钻取和进一步筛选，并更改/提供时间范围以查看感兴趣的数据。

有关详细信息，请参阅共享链接仪表板。

September 09, 2022

异常行程 RI 增强功能

异常行程风险指标已得到增强，可报告客户端 IP 地址的注册组织和路由类型。这些新字段在用户时间线指标详细视图和发送到 SIEM 的指标详细信息中均可用。

有关默认策略的更多信息，请参阅以下文章：

- 持续风险评估。
- 策略和操作

August 19, 2022

启用 VDA 打印遥测

当在 Citrix Apps and Desktops 中启动打印作业时，会触发一个名为 VDA.Print 的事件。VDA 打印事件也可在**自助搜索**和**自定义风险指标**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。
- **自定义风险指标**：通过 EventHub 为 VDA 打印遥测提供了新事件，并且这些事件也可在自定义指标中使用。您可以使用这些事件键/值对来配置自定义指标触发器。

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

有关详细信息，请参阅为 Citrix DaaS 启用打印遥测。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

August 18, 2022

已修复的问题

- 在 Apps and Desktops 的自助搜索以及访问保障位置控制板下的用户登录页面中，下载的 CSV 文件中 Workspace 应用程序版本值显示为 **NA**（不可用），而页面视图中则可用。此问题现已修复。

August 17, 2022

按策略自定义最终用户电子邮件

您现在可以按策略自定义发送给最终用户的电子邮件内容。具体来说，当您创建包含“请求最终用户响应”操作或对用户帐户执行破坏性操作（例如“注销用户”和“锁定用户”）的策略时，应用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。

August 11, 2022

关于 **访问保障 – 地理位置** 的新问题已添加到 **常见问题** 文章中。有关更多详细信息，请参阅 常见问题。

已修复的问题

- “**查看所有通知**”按钮将管理员重定向到存在拼写错误的 `https://citrix.cloud.com/notifications` 每周电子邮件链接。

June 17, 2022

新付费授权默认启用数据处理

以前，拥有 Citrix Analytics for Security 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，当预配 Citrix Analytics for Security 的新付费授权时，以下 Citrix Cloud 服务将默认开启数据处理：

- 思杰安全私有访问
- Citrix 内容协作™
- 思杰 DaaS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关详细信息，请参阅 入门。

June 09, 2022

已修复的问题

- 由 Azure AD 身份保护和 Microsoft Defender for Endpoint 生成的 Microsoft Graph 风险指标可能会在 Security Analytics 中多次显示。此问题现已修复。

June 02, 2022

已修复问题

- 在策略的自助搜索中，当在搜索查询中选择 **策略名称** 维度以筛选事件时，系统会建议无效策略列表以及安全分析的有效策略。
- 在自助搜索中，Windows Citrix Receiver 的 **文件下载** 事件的下载文件大小显示不正确。出现此问题的原因是实际值以 KB 为单位，而 UI 将该值视为字节，导致向用户显示的值不正确。

May 24, 2022

推出适用于内容协作、Citrix DaaS 和 Citrix Virtual Apps and Desktops 以及 Gateway 数据源的不可能的行程风险指标

如果用户从两个相距太远而无法在规定时间内到达的位置登录，Citrix Analytics 会将此活动检测为不可能的行程场景，并触发**不可能的行程**风险指标。有关不可能的行程风险指标的更多信息，请参阅以下文章：

- Citrix 内容协作风险指标
- Citrix Gateway 风险指标
- 思杰虚拟应用和桌面和思杰DaaS风险指标

May 17, 2022

虚拟应用和桌面已重命名为应用和桌面

在安全分析控制板和报告中以及安全分析发送到 SIEM 服务的数据中，所有 Virtual Apps and Desktops 标签现已更新为 Apps and Desktops，以与重塑品牌后的产品名称保持一致。

例如，在“数据源”页面上，Virtual Apps and Desktops 标签已重命名为 Apps and Desktops。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Apps and Desktops 标签代表您组织中的 Citrix 本地 Citrix Virtual Apps and Desktops 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）。

已修复问题

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。

April 05, 2022

新增功能

安全工作区访问 已更名为 安全私有访问

在 Analytics 控制板和报告中，所有 **Secure Workspace Access** 标签现已更新为 **Secure Private Access**，以与更名后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** 标签已更名为 **Secure Private Access**。

March 21, 2022

已修复问题

- 在 **创建风险指标** 页面中，如果搜索查询的先前条件包含由空格分隔的维度值，则维度和运算符的自动建议不起作用。

  例如，在以下查询中，在您选择城市为 `San Jose` 后，自动建议将停止工作。此问题现已修复。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

March 10, 2022

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策略关联的多个风险指标的详细信息。
- 您可以查看与策略关联的每个风险指标的名称、严重性级别和触发日期。
- 单击“**查看风险详细信息**”可在 Citrix Analytics 中打开用户时间线页面，并查看触发策略的最新风险指标。在用户时间线页面上，您还可以查看为该用户触发的所有风险指标。

通知管理员电子邮件增强功能(/en-us/citrix-analytics/media/notify-email-enhancements.png)

有关“**通知管理员**”操作的更多信息，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，您在相应的自助搜索页面中看不到用户事件。此外，您无法为 Secure Workspace Access 数据源创建自定义风险指标。

March 03, 2022

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来对用户帐户应用“**请求最终用户响应**”操作。 在此版本中，您可以从用户时间线上的“**操作**”列表中选择该操作，并手动将此操作应用于风险指标。

有关该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。

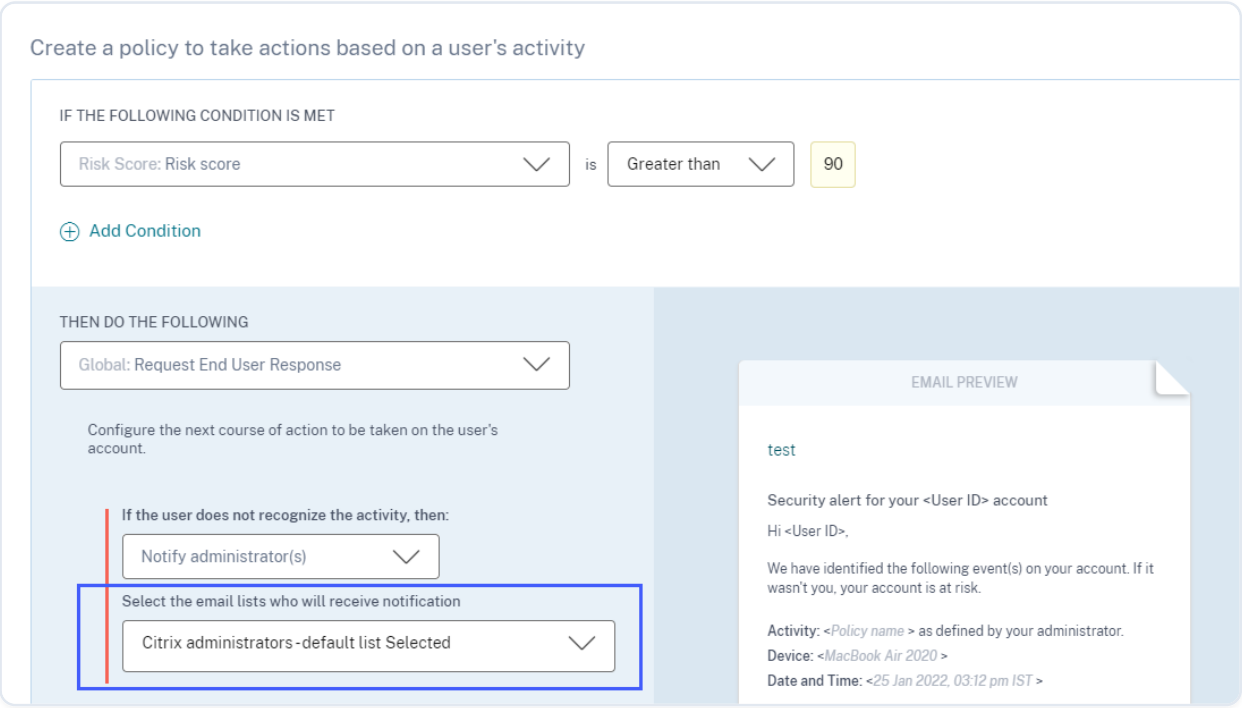
请求最终用户响应手动(/en-us/citrix-analytics/media/request-user-manual-action.png)

策略的请求最终用户响应增强功能

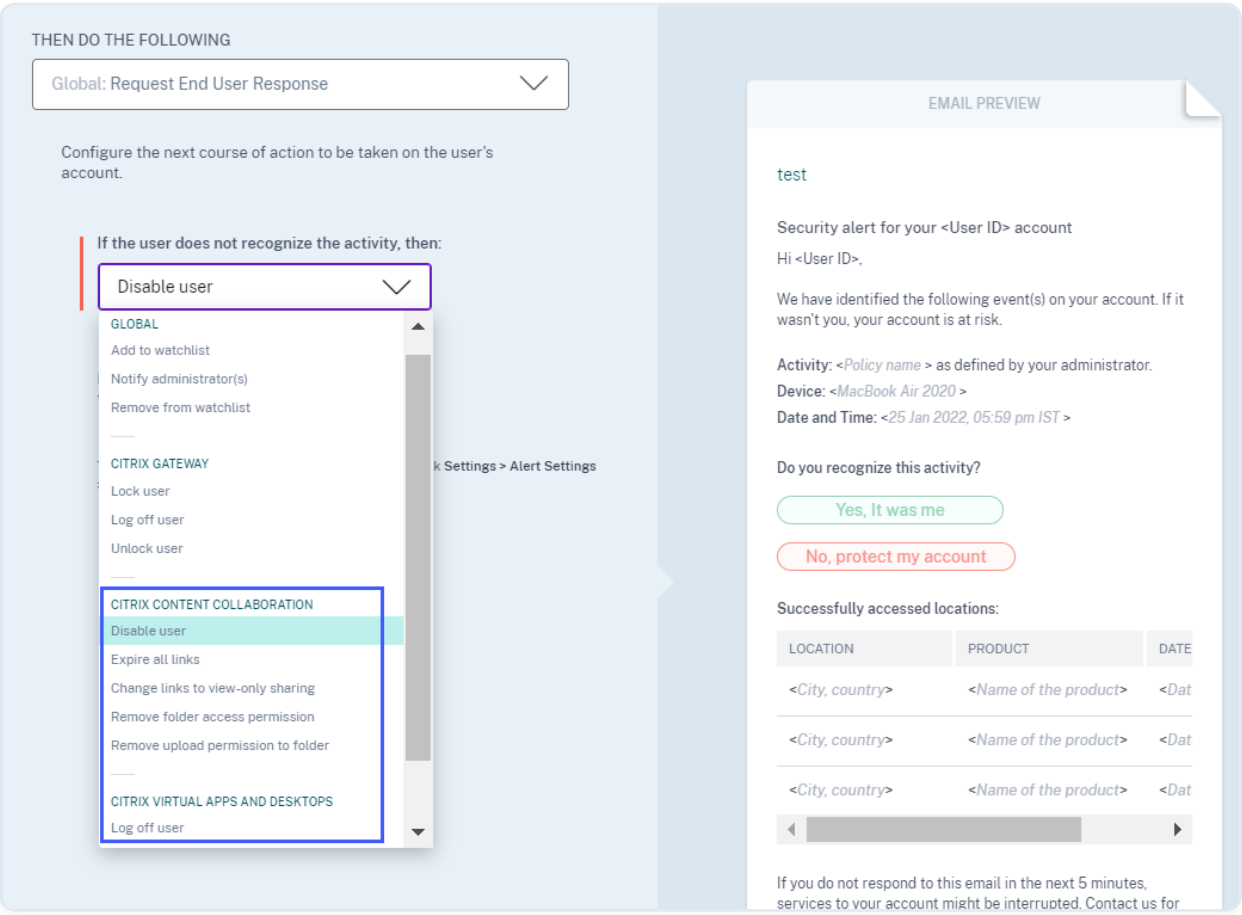
当您创建包含“**请求最终用户响应**”操作的策略时，您会看到以下增强功能：

- 选择“**通知管理员**”作为下一个操作后，您现在可以查看可供选择的默认和已创建的电子邮件通讯组列表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 您现在可以将 Citrix Content Collaboration 或 Citrix Virtual Apps and Desktops 和 Citrix DaaS 中的某个操作选为下一个操作。以前，您只能选择全局操作或 Citrix Gateway 操作之一。



有关操作的更多信息，请参阅 策略和操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

February 23, 2022

新增功能

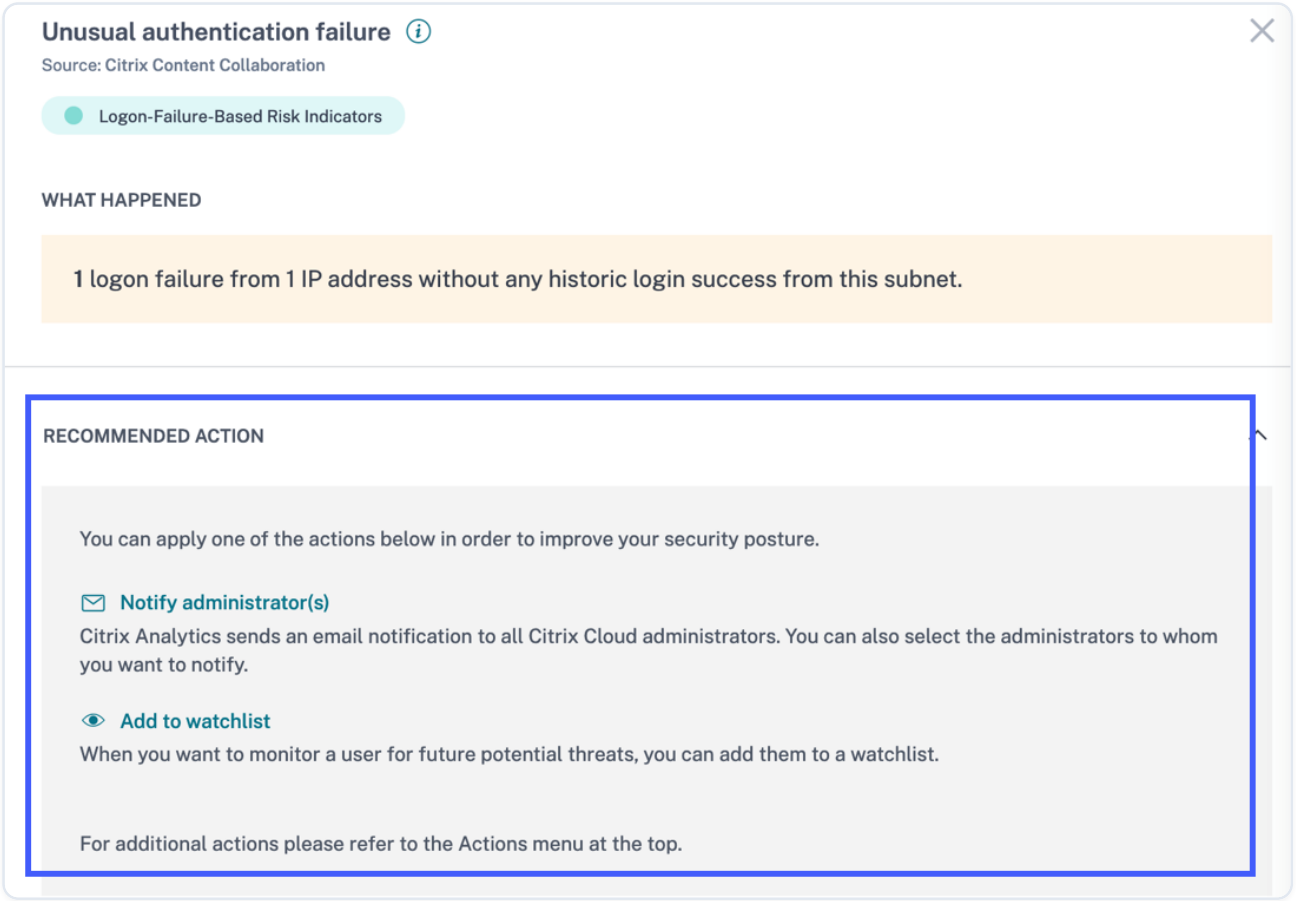
风险指标的建议操作

Citrix Analytics 建议您在为用户触发以下风险指标时应用以下操作：**通知管理员**、**添加到观察列表**和**创建策略**：

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

当您转到用户时间线并选择风险指标时，您可以在“**建议操作**”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标中，您可以查看以下建议操作：



此功能提供指导，帮助您根据用户带来的风险严重程度选择可采取的操作。但是，您也可以根据风险分析采取建议列表之外的适当操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复问题

- 如果您的组织在**亚太南部**主区域加入 Citrix Cloud，则 Citrix Analytics 可能无法从身份验证数据源接收用户事件。因此，您可能无法在相应的自助服务搜索页面中看到用户事件。此问题已修复。

February 17, 2022

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 服务的事件的数据收集、关联和报告。
- 改进了从用户和客户端版本接收的事件质量，可用于自助服务搜索、自定义风险指标和整体风险检测。

支持内容协作中会话事件和应用程序事件的上下文模板

在自助服务搜索页面上，您现在可以查看仅与文件、文件夹、会话、共享和用户事件相关的字段的详细信息。事件的不适用字段已删除。

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

这些详细信息有助于您在对与危险行为相关的用户帐户进行风险调查和分析时。您可以深入查看看似危险的事件的特定属性。

有关这些字段的更多信息，请参阅《内容协作自助搜索》。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

February 10, 2022

新增功能

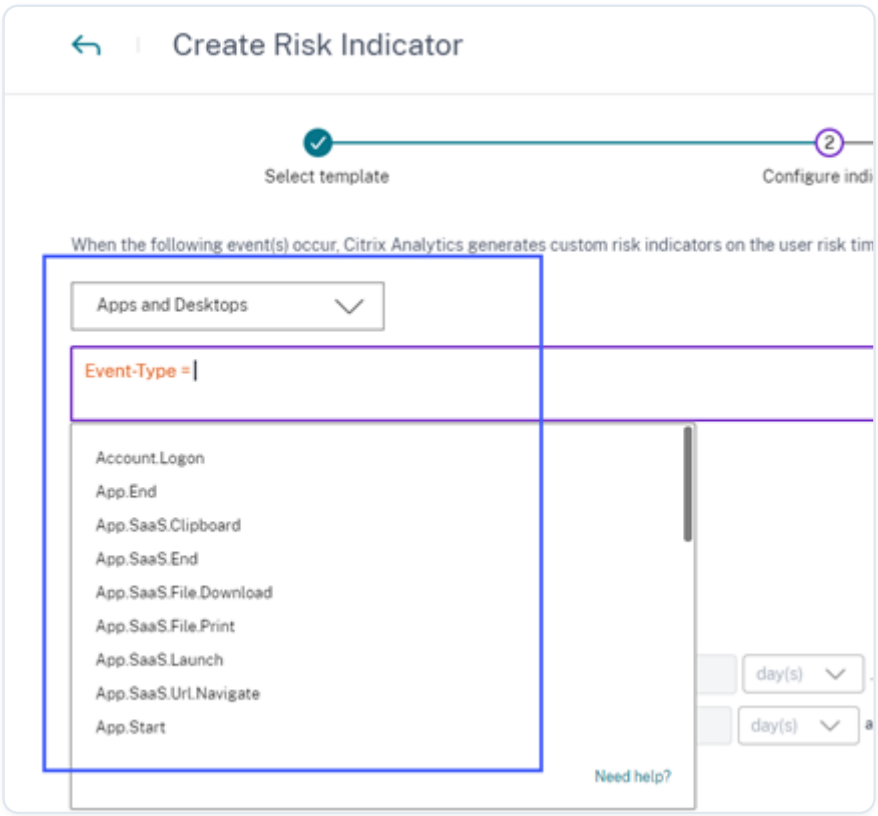
自定义风险指标中维度的自动建议值

在自定义风险指标页面中，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。您可以从自动建议列表中选择一个值，或根据您的用例手动输入一个值。当您键入值时，记录中可用的匹配值将自动建议。

为维度建议的值列表要么是数据库中预定义（已知值）的，要么是基于历史事件的。

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

有关更多信息，请参阅自定义风险指标。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

February 09, 2022

新增功能

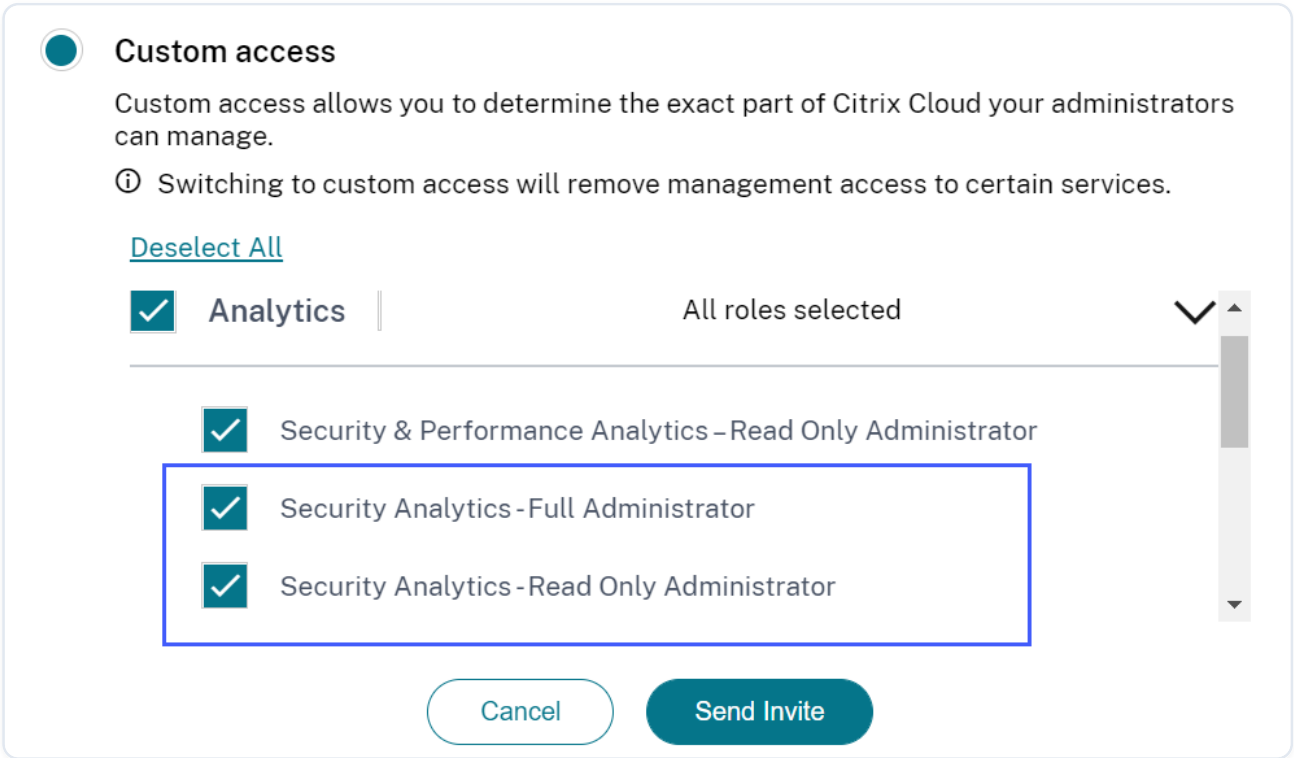
管理员的新自定义角色

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在您的组织中管理 Security Analytics。您现在可以将以下自定义角色分配给受邀管理员：

- Security Analytics - 完全管理员
- Security Analytics - 只读管理员

使用自定义角色，您可以为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

如果您是具有自定义访问（只读或完全访问）权限以管理 Security Analytics 的 Citrix Cloud 管理员，您现在将收到以下通知：

- 关于您的组织中检测到的安全风险的每周通知。有关更多信息，请参阅每周电子邮件通知。
- 当手动应用或由策略触发**通知管理员**操作时，关于风险指标的通知。有关更多信息，请参阅策略和操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 28, 2022

新增功能

为内容协作和网关数据源引入可疑登录风险指标

Citrix Analytics for Security 现在根据多种上下文因素（例如）检测本质上可疑的用户登录：

- 该位置相对于用户和组织历史记录被视为异常
- 根据用户和组织历史，该设备被认为是不寻常的。
- 根据用户和组织历史，该网络被认为是不寻常的。
- 根据 IP 威胁情报源，该 IP 地址被认为是可疑的。

当用户基于这些因素的组合从可疑上下文中登录时，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“从异常位置访问”风险指示器。任何基于“从异常位置访问”风险指示器的现有策略都将自动链接到新的风险指示器——“可疑登录”。

有关风险指示器的更多信息，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更多信息，请参阅 Citrix Analytics SIEM 数据格式。

January 20, 2022

新增功能

微软 Azure 活动目录集成

您现在可以将 Azure Active Directory 与 Citrix Analytics for Security 连接，以：

- 将您组织域中的用户详细信息和用户组导入到 Citrix Analytics for Security。
- 使用其他详细信息（例如职位、组织、办公地点、电子邮件和联系方式）丰富用户配置文件，这有助于您进行风险调查和分析。

有关更多信息，请参阅 Azure Active Directory 集成。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 18, 2022

最新功能

支持对所有内容协作风险指标执行共享链接操作

以前，您可以对与内容协作服务关联的以下基于共享链接的风险指标应用共享链接操作——**使所有链接过期**和**将链接更改为仅查看共享**：

- 匿名敏感共享链接下载
- 过多的共享链接下载
- 过多的文件共享

在此版本中，您现在可以对与内容协作服务关联的以下基于用户的风险指标应用共享链接操作：

- 从异常位置访问
- 对敏感文件的过度访问
- 过多的文件上传
- 过多的文件下载
- 过多的文件或文件夹删除
- 检测到恶意软件文件
- 怀疑有勒索软件活动
- 异常身份验证失败

您还可以对与内容协作服务关联的自定义风险指标应用共享链接操作。

有关操作和风险指标的更多信息，请参阅以下文章：

- 策略和操作
- 内容协作风险指标
- 自定义风险指标

与 SIEM 的集成现已正式发布

您可以将 Citrix Analytics for Security 与您的安全信息和事件管理 (SIEM) 服务集成，并将用户数据从 Citrix IT 环境导出到您的 SIEM。此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状况。

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 思普朗克
- 微软 Sentinel
- 弹性搜索
- 其他 SIEM 服务（通过使用基于 Kafka 或 Logstash 的数据连接器）

有关详细信息，请参阅安全信息和事件管理 (SIEM) 集成。

December 23, 2021

新增功能

共享链接风险指标增强功能

已进行以下增强功能：

- 您现在可以使用**匿名敏感共享链接下载**风险指标创建策略。
- **匿名敏感共享下载**风险指标已重命名为**匿名敏感共享链接下载**，以将其区分为共享链接风险指标。
- **过度下载**风险指标已重命名为**过度共享链接下载**，以将其区分为共享链接风险指标，并将其与基于用户的**过度文件下载**风险指标区分开来。

有关详细信息，请参阅 Citrix 共享链接风险指标。

December 21, 2021

新增功能

向非 Citrix Cloud 管理员发送有关风险指标的通知

您现在可以使用**通知管理员**操作来通知组织中的非 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 的外部域中选择电子邮件通讯组列表中的管理员，或者直接使用他们的电子邮件地址。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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

December 20, 2021

新增功能

向您的内容协作用户发送用户响应通知

除了 Active Directory 用户之外，您现在还可以将**请求最终用户响应**操作应用于您的 Content Collaboration 用户。

当 Citrix Analytics 检测到用户的 Citrix 帐户中有任何异常活动时，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 已更名为 安全工作区访问

在 **Security** Analytics 控制板和报告中，所有 **Access Control** 标签现已更新为 **Secure Workspace Access**，以与更名后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，Access Control 标签已更名为 Secure Workspace Access。

已修复问题

- 对于 Apps and Desktops 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显示为不可用 (N/A)，尽管它们的值是可用的。例如，`Download File Name`、`Session Launch Type` 和 `Workspace App Version` 等字段的值显示在**自助搜索**页面上，但在下载的 CSV 文件中，您会看到这些值显示为不可用 (N/A)。此问题现已修复。

December 09, 2021

新增功能

使用模板轻松创建自定义风险指标

您现在可以根据您的用例选择一个模板并创建自定义风险指标。这些模板通过提供预定义查询和参数来指导您。这在您创建自定义风险指标时减轻了您的工作量。

有关更多信息，请参阅自定义风险指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

December 07, 2021

已修复问题

- 在 Citrix Analytics for Security 中，您不会收到使用 2021 年 9 月发布的 Citrix Secure Browser 的用户的事件。出现此问题的原因是，在 2021 年 9 月发布后，**主机名跟踪**策略在 Citrix Secure Browser 中不可见，因此无法启用以与 Citrix Analytics for Security 集成。此问题现已修复。

December 02, 2021

新增功能

检测到恶意文件风险指标

现在，当用户在 Content Collaboration 中上传受感染文件时，您可以收到警报。

此风险指标可检测受恶意软件（例如木马、病毒或任何其他恶意威胁）感染的文件。它提供恶意文件的详细信息，例如文件所有者、病毒名称和文件位置。

与**检测到恶意文件**风险指标关联的风险因素是基于文件的风险指标。

有关风险指标以及您可以应用的操作的更多信息，请参阅检测到恶意文件风险指标。

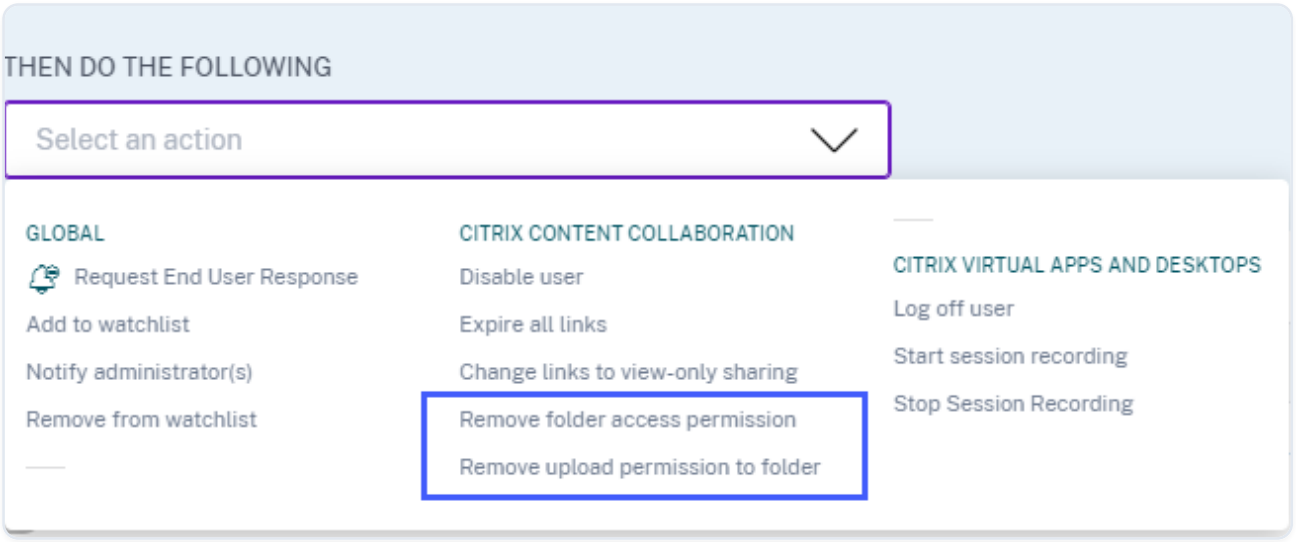
Content Collaboration 数据源的新操作

当针对用户触发**检测到恶意文件**风险指标时，您可以应用以下操作：

- **删除文件夹访问权限**。您可以阻止上传受感染文件的用户的访问权限。该用户无法访问上传受感染文件的文件夹。
- **删除文件夹上传权限**。您可以阻止上传受感染文件的用户的上传权限。该用户无法将文件上传到上传受感染文件的文件夹。

有关 Content Collaboration 操作的更多信息，请参阅策略和操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



November 29, 2021

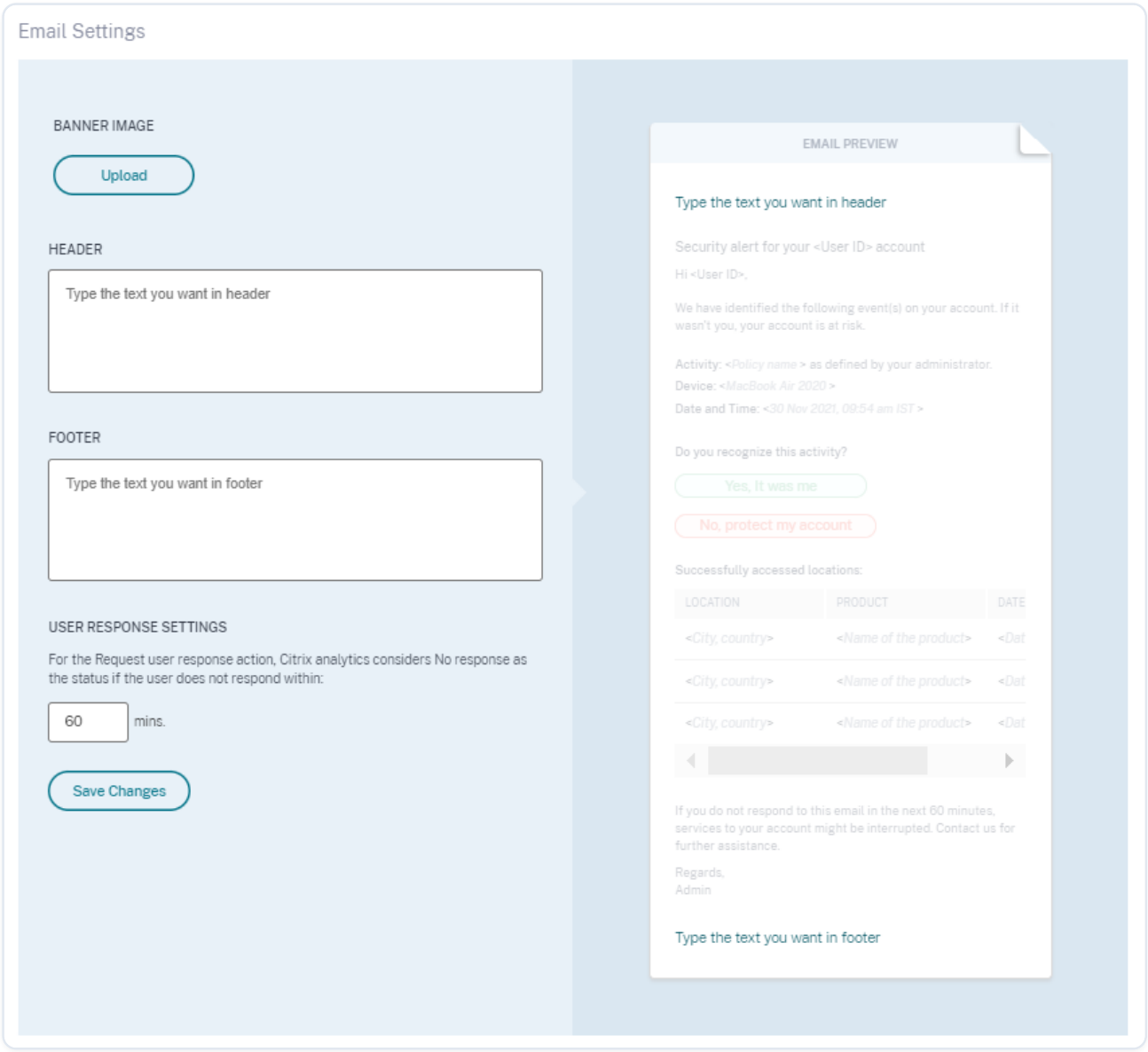
新增功能

用户通知的电子邮件设置增强功能

作为管理员，您现在可以在用户响应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，从而提高了用户对您的电子邮件的关注度和响应。

有关更多信息，请参阅最终用户电子邮件设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



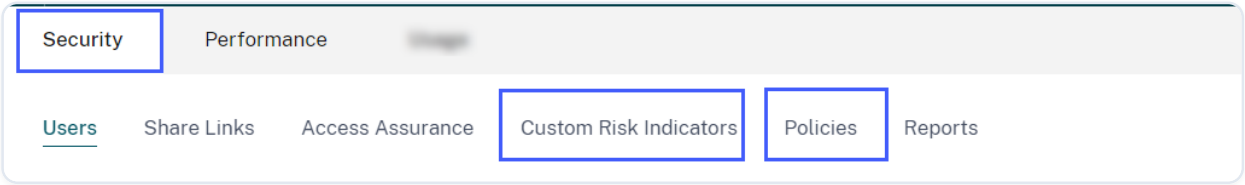
November 26, 2021

新增功能

自定义风险指标和策略菜单更改

以下功能的导航链接已更新：

- 自定义风险指标：通过单击 **安全 > 自定义风险指标** 使用此功能。
- 策略：通过单击 **安全 > 策略** 使用此功能。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

November 25, 2021

新增功能

安全信息和事件管理 (SIEM) 集成增强功能

注意

此集成处于预览阶段。

您现在可以将 Citrix Analytics for Security 与以下 SIEM 服务集成：

- 微软 Sentinel
- 带有可视化服务（如 Kibana）和 SIEM 服务（如 LogRythm）的 Elasticsearch
- 任何其他使用 Logstash 数据收集引擎的 SIEM 服务

根据您的业务需求，将用户数据从 Citrix Analytics for Security 导入到您的 SIEM 服务。此集成使您的安全运营团队能够关联、分析和搜索组织内 SIEM 服务中不同日志的数据，从而帮助他们识别并快速补救安全风险。

有关更多信息，请参阅 安全信息和事件管理 (SIEM) 集成。

November 09, 2021

已修复问题

- 在少数租户中，用户策略不起作用。当虚拟应用程序的警报域具有空字符串值时，会出现此问题。此问题现已修复。

November 02, 2021

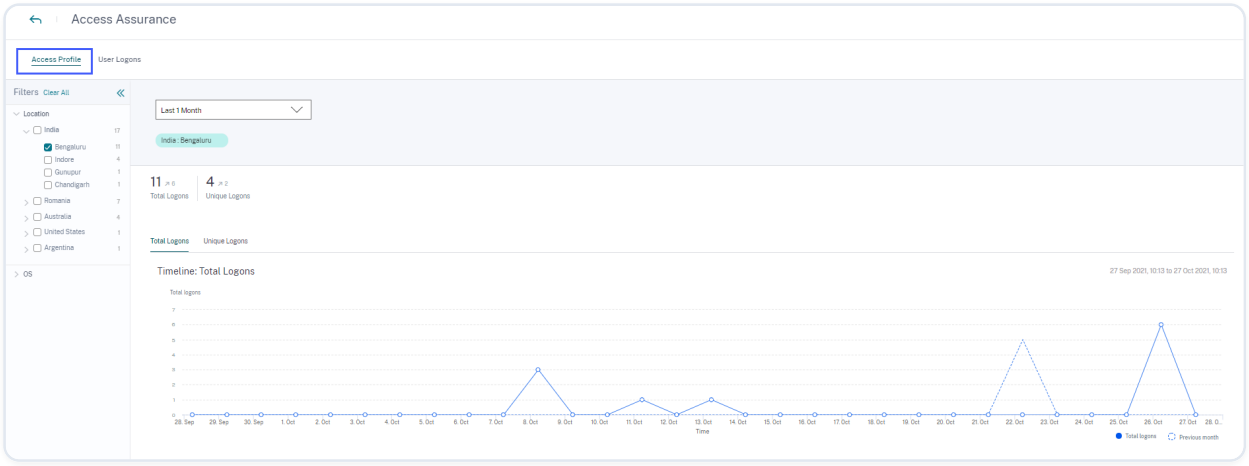
新增功能

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

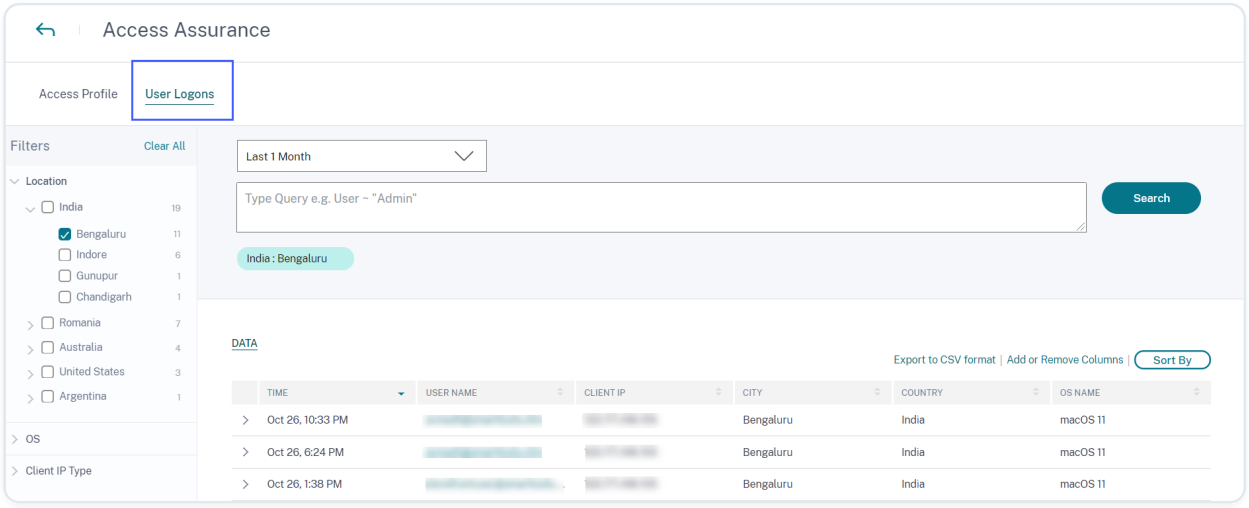
在 **访问保障位置** 仪表板上，您可以查看已登录虚拟应用程序和虚拟桌面的用户的访问配置文件和登录详细信息。此信息有助于您进行威胁调查和分析。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **访问配置文件** 页面提供了所选位置的用户访问摘要。您可以查看总用户和唯一用户登录的趋势分析和热门访问事件。



- **用户登录**页面提供从选定位置登录到虚拟应用和虚拟桌面的用户登录详细信息。

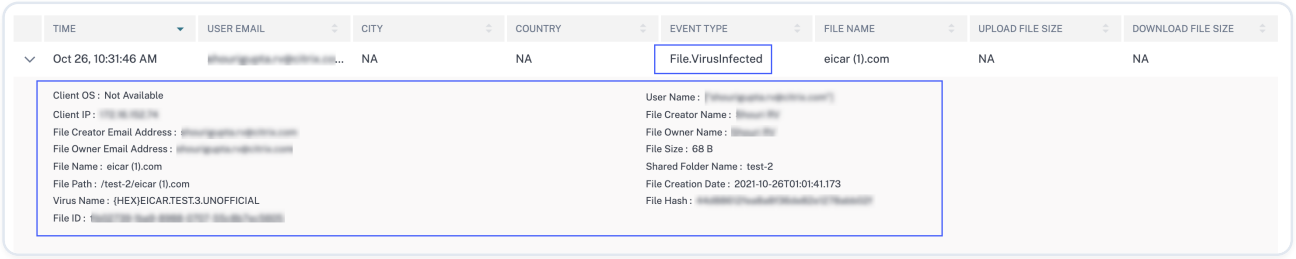


有关详细信息，请参阅访问保障位置控制板。

在内容协作的自助服务搜索页面上查看恶意软件日志

在内容协作的自助服务页面上，您现在可以查看恶意软件事件 `File.VirusInfected` 及其关联日志。当内容协作用户上传感染恶意软件的文件时，会触发此事件。

有关详细信息，请参阅内容协作的自助服务搜索



© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复的问题

- 在处理 Citrix Analytics 中的事件时，一些内容协作用户被错误地设置为非员工。因此，这些用户未被识别为已发现用户。此问题现已修复。

October 20, 2021

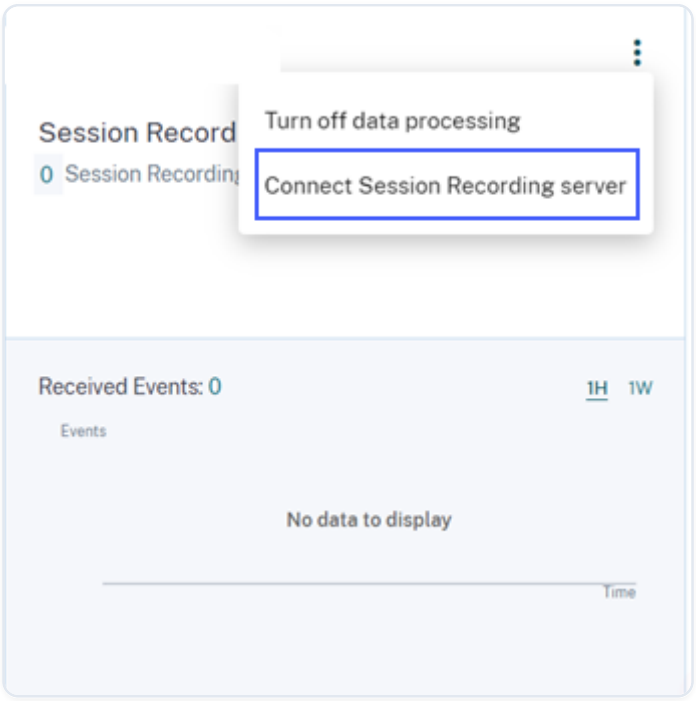
新增功能

会话录制服务器集成

对于您的 Citrix Virtual Apps and Desktops 和 Citrix DaaS 部署，您现在可以配置会话录制服务器以将用户事件发送到 Citrix Analytics for Security。这些用户事件经过处理，可提供有关用户行为的可操作见解。

在**数据源 > 安全**页面上，转到**虚拟应用和桌面**站点卡。在**会话录制**站点卡上，单击垂直省略号 (⋮)，然后选择**连接会话录制服务器**。

有关详细信息，请参阅 连接到会话录制部署。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

October 19, 2021

新增功能

通知管理员电子邮件模板增强功能

管理员在应用**通知管理员**操作后收到的电子邮件通知已得到增强，可更好地洞察用户风险事件。

- 通知现在提供有关触发的风险指标或应用的策略的详细信息。例如，您可以查看默认和自定义风险指标的严重性以及触发时间。内容结构已改进，以提高可读性。
- 管理员现在可以直接从电子邮件通知中访问用户时间线，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，并根据回复持续改进通知内容。

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

- 您现在可以查看全球总用户登录和全球唯一用户登录的用户登录趋势（上升或下降）。



- **唯一登录位置**表中的**偏差**列显示了特定位置的唯一用户登录的上升或下降变化。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



这些指标可帮助您了解用户登录与上一期间相比的变化（积极或消极）。它提供了用户与您的 Citrix Virtual Apps and Desktops 和 Citrix DaaS 部署交互的可见性。

有关详细信息，请参阅访问保障位置控制板。

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外登录时，**用户登录摘要**卡无法显示用户登录指标（全球用户登录总数、全球唯一用户登录数以及有用户登录的国家/地区）。此问题现已修复。

October 01, 2021

新增功能

在 Content Collaboration 的自助搜索中查看审核日志

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 Content Collaboration 管理员对用户帐户应用的权限和操作的见解。利用这些数据，您可以验证 Content Collaboration 管理员是否对其用户帐户执行了有效操作。作为安全管理员，这有助于您进行风险调查和分析。

有关审核日志的更多信息，请参阅 Content Collaboration 的自助搜索。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复的问题

当旧的过期会话 ID 与新的会话 ID 一起出现时，使用 Azure AD 登录 Citrix Cloud 的管理员无法访问 Citrix Analytics 服务。此问题现已修复。

September 29, 2021

新增功能

访问保障位置控制板现已正式发布

该控制板提供了您的 Citrix Virtual Apps and Desktops 和 Citrix DaaS 用户位置的可见性。您可以通过启用地理围栏来识别位置异常的用户，并采取适当措施来防止任何威胁。

要查看仪表板，请单击 **安全 > 访问保障**。选择您要查看位置详细信息的时间段。

有关更多信息，请参阅访问保障位置仪表板。

September 15, 2021

新增功能

自定义风险指标增强功能

- 当自定义风险指标被触发时，它会立即显示在用户时间线上。但是，用户的风险摘要和风险评分会在几分钟后（大约 15-20 分钟）更新。
- 如果您修改现有自定义风险指标的属性，例如条件、风险类别、严重性和名称，您仍然可以在用户时间线上查看为该用户触发的自定义风险指标的先前出现情况（带有旧属性）。
- 如果您删除自定义风险指标，您仍然可以在用户时间线上查看为该用户触发的自定义风险指标的先前出现情况。

有关更多信息，请参阅自定义风险指标。

September 14, 2021

新增功能

推出可疑登录风险指标

Citrix Analytics for Security 现在根据以下多个上下文因素检测本质上可疑的用户登录：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 该位置相对于用户和组织历史记录被视为异常
- 该设备相对于用户和组织历史记录被视为异常
- 网络被认为对用户和组织历史来说是不寻常的
- 根据 IP 威胁情报源，IP 地址被认为是可疑的

当 Citrix Virtual Apps and Desktops 和 Citrix DaaS 用户根据这些因素的组合从可疑上下文登录时，将触发风险指示器。

此风险指示器取代了与 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“**从异常位置访问**”风险指示器的现有策略都将自动链接到新的风险指示器 - “**可疑登录**”。

有关风险指示器的更多信息，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 现在将“**可疑登录**”风险指示器的架构详细信息发送到您的 SIEM 服务。您可以查看指示器摘要的架构以及“**可疑登录**”风险指示器的事件详细信息。有关更多信息，请参阅 Citrix Analytics SIEM 数据格式。

已修复问题

- 对于 Apps and Desktops 自助服务搜索，下载的 CSV 文件中缺少客户端 IP 值。此问题现已修复。

August 19, 2021

新增功能

推出适用于 Splunk 的 Citrix Analytics 应用程序

> **注意**
>
> 该应用程序处于预览阶段。

适用于 Splunk 的 Citrix Analytics 应用程序使您能够在 Splunk 上以富有洞察力的仪表板形式查看从 Citrix Analytics for Security 收集的数据。这些仪表板提供了对用户风险事件的洞察。您还可以将 Citrix Analytics 数据与从各种其他数据源收集的日志关联起来。关联有助于您发现事件之间的关系并及时采取行动以保护您的 IT 环境。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要下载此应用程序，请转到 Splunkbase。在您的 Splunk 搜索头中安装此应用程序。

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

SIEM 的自定义风险指示器架构

在您的 SIEM 服务中，您现在可以查看为 Citrix Virtual Apps and Desktops 和 Citrix DaaS 创建的自定义风险指示器的架构。此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详细信息，请参阅 适用于 SIEM 的 Citrix Analytics 数据格式。

支持 Citrix Director 作为数据源

您现在可以在 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，在发现站点后启用数据处理。在“**监控**”卡上，您可以查看所有连接的站点。

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。

访问保障位置控制板中对地理围栏的支持

您现在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，地图会显示地理围栏区域（国家/地区）以及来自地理围栏外部和内部的用户登录。此功能使用“**CVAD-会话在地理围栏外部启动**”风险指示器来监控用户登录。

有关详细信息，请参阅 访问保障位置控制板。

“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：

- 受支持
- 部分支持
- 不支持
- 不可用
- 非活动

此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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

要查看 Citrix Workspace 应用程序状态，您必须载入 Citrix Director 数据源。否则，每个 Citrix Virtual Apps and Desktops 和 Citrix DaaS 用户的状态都显示为**非活动**。

有关详细信息，请参阅用户仪表板。

支持 IS EMPTY 运算符

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

注意

此运算符仅适用于字符串类型维度，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示器。

改进的风险评分

在用户时间线上，您现在可以查看用户的风险摘要。风险摘要提供与用户事件相关的风险因素信息。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：

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

在用户时间轴上，您现在可以应用筛选器，根据风险因素查看用户事件。

有关详细信息，请参阅以下主题：

- Citrix 用户风险指标
- 用户风险时间轴和配置文件

© 1997–2026 Citrix Systems, Inc. All rights reserved.

July 29, 2021

已弃用的功能

与 Citrix Endpoint Management™ 相关的已弃用操作

以下操作已从 Citrix Endpoint Management 数据源中移除。您不能再将这些操作应用于风险指标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

在您现有策略中，如果这些操作已在使用中，它们将自动替换为**添加到观察列表**操作。您可以从观察列表中监控此类用户。

July 14, 2021

新增功能

支持 IS NOT EMPTY 运算符

创建自定义风险指标时，您现在可以在条件中使用 **IS NOT EMPTY** 运算符来检查维度是否不为空（非空白）。

注意

该运算符仅适用于字符串类型维度，例如 App-Name、Browser 和 Country。

例如，以下条件检测来自任何国家/地区的用户登录事件，其中国家/地区值不为空。换句话说，指定了国家/地区名称。

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

有关更多信息，请参阅自定义风险指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

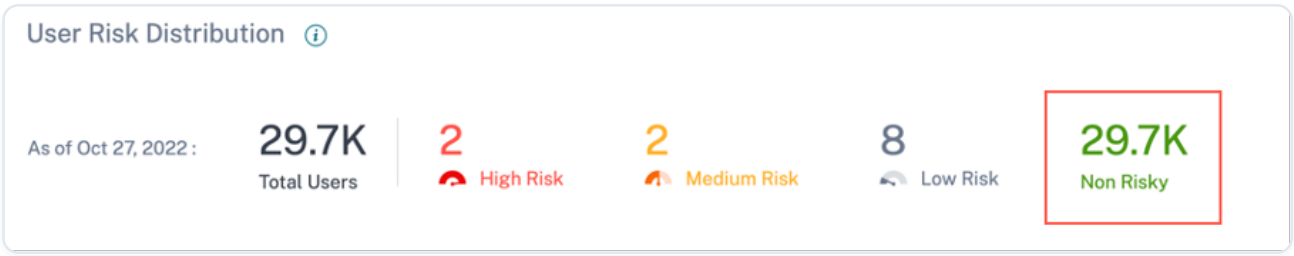
July 06, 2021

新增功能

在用户仪表板上查看非风险用户

在**用户**仪表板上，您现在可以查看所选时间段内非风险用户的数量。这些发现的用户根据所选时间段的零风险评分被识别为非风险用户。单击**非风险用户**卡片可查看所有风险评分为零的用户。

有关更多信息，请参阅用户仪表板。



July 01, 2021

新增功能

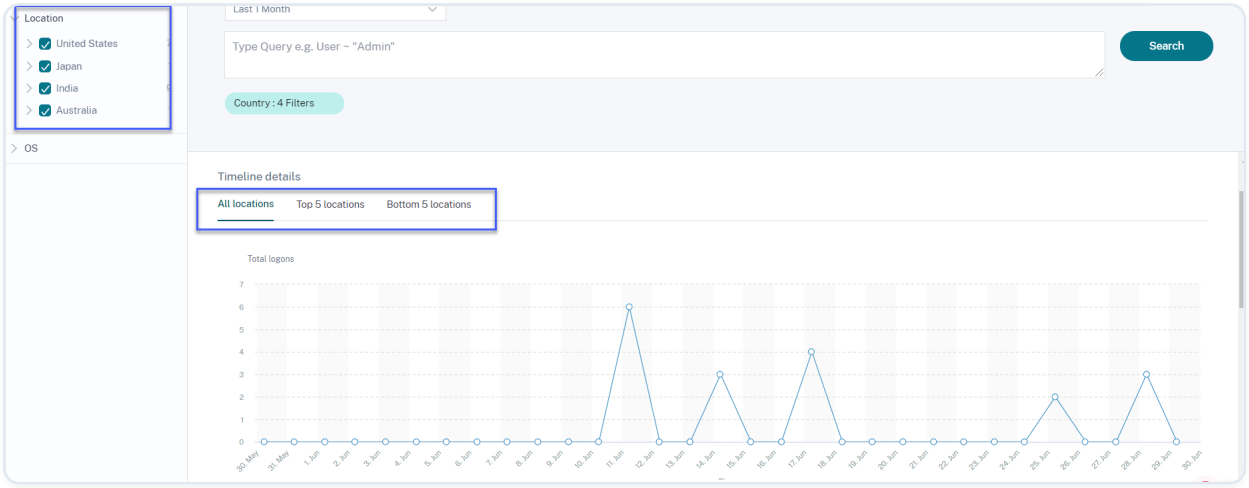
访问保障位置仪表板增强功能

- 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数量。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，您可以查看和比较来自所有位置、前五个位置和后五个位置的用户登录时间线详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 在**访问位置**页面上，您可以使用嵌套分面，例如国家/地区及其城市、操作系统（主要和次要版本）。这些分面使您能够以精细的方式筛选事件。

  嵌套分面(/en-us/citrix-analytics/media/access-assurance-nested-facets.png)

有关详细信息，请参阅访问保障位置。

更新了适用于 Virtual Apps and Desktops 的自助服务搜索中的操作系统分面

您现在可以使用嵌套的操作系统分面筛选 Apps and Desktops 事件。选择与操作系统关联的主要版本和次要版本，并以精细方式筛选事件。有关详细信息，请参阅适用于 Apps and Desktops 的自助服务搜索。

操作系统嵌套分面(/en-us/citrix-analytics/media/virtual-apps-desktops-nested-facets.png)

June 30, 2021

新增功能

在 Apps and Desktops 的自定义风险指标条件中添加了 Workspace 应用程序版本

对于 **Apps and Desktops** 数据源，您现在可以使用 **Workspace-App-Version** 维度在创建自定义风险指标时定义条件。有关该维度的详细信息，请参阅适用于 Apps and Desktops 的自助服务搜索。

CWA 版本(/en-us/citrix-analytics/media/cwa-ci-cvad.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

June 23, 2021

新增功能

SIEM 消息增强功能

以下字段现已添加到风险指标的架构中：

- `indicator_vector_name` - 指示与风险指标关联的风险向量。风险向量包括基于设备的风险指标、基于位置的风险指标、基于登录失败的风险指标、基于 IP 的风险指标、基于数据的风险指标、基于文件的风险指标以及其他风险指标。
- `indicator_vector_id` - 与风险向量关联的 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 IP 的风险指标，ID 6 = 基于数据的风险指标，ID 7 = 其他风险指标，以及 ID 999 = 不可用。

有关详细信息，请参阅Citrix Analytics SIEM 数据格式。

June 07, 2021

新增功能

对通知管理员操作的增强

当您将**通知管理员**操作应用于风险指标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通知的管理员。有关该操作的详细信息，请参阅策略和操作。

增加了对只读共享操作的支持

如果用户过度共享文件，Citrix Analytics 会触发**文件过度共享**风险指标。从用户的风险时间线中，您现在可以将**将链接更改为只读共享**操作应用于**文件过度共享**风险指标。您还可以在共享链接风险时间线上的特定共享链接上应用此操作。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。有关该操作的详细信息，请参阅策略和操作。

May 18, 2021

新增功能

将默认风险指标迁移到自定义风险指标

以下默认风险指标已迁移到预配置的自定义风险指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

默认风险指标	数据源	预配置的自定义风险指标
首次从新设备访问	Citrix 虚拟应用和桌面 和 Citrix DaaS	CVAD-首次从新设备访问
首次从新 IP 访问	Citrix 网关	Gateway-首次从新 IP 访问

随着迁移到自定义风险指标，默认风险指标和相关的机器学习算法已被弃用。

相应的自定义风险指标根据以下预配置条件触发：

- 当用户首次从新设备访问，或从已至少 90 天未使用的现有设备访问时。
- 当用户首次从新 IP 地址登录，或从已至少 90 天未使用的现有 IP 地址登录时。

除了预配置条件外，您现在还可以为这些自定义风险指标添加自己的条件，以识别 Citrix 环境中的威胁。此选项使您可以灵活地根据安全需求配置自定义风险指标。您还可以创建策略，对这些自定义风险指标检测到的风险事件应用操作。

但是，在用户的时间线中，您仍然可以查看之前触发的默认风险指标及其事件。

与这些默认风险指标关联的策略会自动链接到相应的预配置自定义风险指标。

有关更多信息，请参阅预配置的自定义风险指标和策略。

Gateway 自助搜索的增强功能

- **事件类型**筛选器现已重命名为**记录类型**。选择以下记录类型之一来筛选您的事件：VPN_AI、VPN_IF 和 VPN_ST。
- 在**数据**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之一：身份验证、ICA® 文件或会话注销。

下表描述了记录类型和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，请参阅网关自助搜索。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复的问题

- 自定义风险指示器根据条件值的大小写敏感性触发。例如，在包含允许列表中设备 ID 的用户事件中，您会看到以下行为：
  - 如果您输入`Device-ID`维度的小写值，自定义指示器将触发。

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

  - 如果您为同一设备输入`Device-ID`维度的大写值，则不会触发自定义指标。

    ```
    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标。

April 29, 2021

新增功能

自定义风险指标的事件详细信息

在用户的风险时间线页面上，您现在可以查看触发自定义风险指标的事件。以前，您只能查看自定义风险指标的定义条件、描述和触发频率。单击 **事件搜索** 以查看与用户和风险指标关联的事件详细信息。 有关更多信息，请参阅自定义风险指标。

已修复问题

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

April 16, 2021

新增功能

SIEM 消息增强功能

您可以在风险指标架构格式中查看以下增强功能：

- 客户端 IP 地址现在可用于所有批处理风险指标的架构中。以前，客户端 IP 地址仅适用于少数批处理风险指标：
  - EPA 扫描失败

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 身份验证失败次数过多
- 来自可疑 IP 的登录
- 从异常位置访问
- 异常身份验证失败
- 匿名敏感共享下载
- 潜在数据泄露

- 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 Citrix Analytics SIEM 数据格式。

March 26, 2021

新增功能

SIEM 消息限制

Citrix Analytics 会将每个风险指标事件最多 1000 个事件详细信息发送到您的 SIEM 服务。这些事件按发生的时间顺序发送。有关详细信息，请参阅 Citrix Analytics SIEM 数据格式。

在 SIEM 消息中添加了数据源 ID 和指标类别 ID 字段

以下字段已添加到指标摘要架构和指标事件详细信息架构中。

字段	描述
`data_source_id`	与数据源关联的 ID。ID 0 = Citrix 内容协作，ID 1 = Citrix 网关，ID 2 = Citrix 端点管理，ID 3 = Citrix 虚拟应用和桌面，ID 4 = Citrix 访问控制™
`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 = 受感染用户

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

March 18, 2021

新增功能

访问保障位置控制板

注意

此功能处于预览阶段。

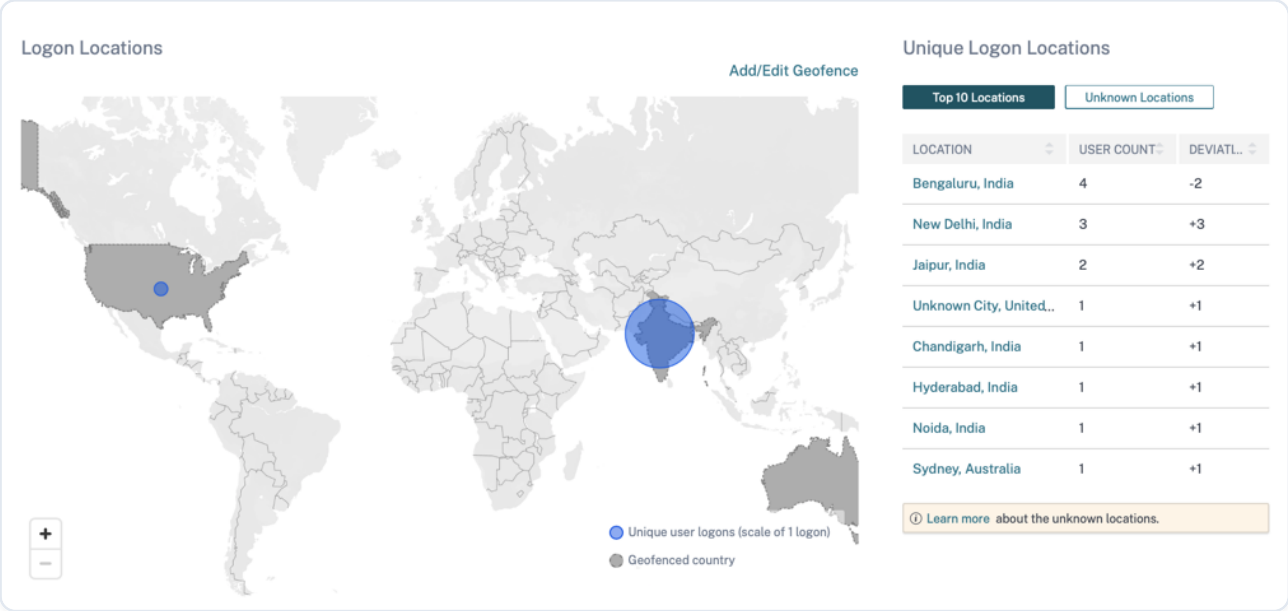
“**访问保障位置**”控制板概述了 Citrix Virtual Apps and Desktops 和 Citrix DaaS 用户在选定时间段内登录的位置。Citrix Analytics 从用户设备上安装的 Citrix Workspace 应用程序接收这些用户登录事件。

要查看仪表板，请单击 **安全 > 访问保障**。

您可以查看所选时间段的以下信息：

- 来自特定位置和所有位置的用户登录总数。
- 所有位置的唯一用户登录总数。
- 用户登录的国家/地区总数。
- 唯一用户登录次数最多的 10 个位置。

有关详细信息，请参阅 访问保障位置。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。该运算符检查用户事件中是否包含您指定的匹配模式。它返回事件字符串中不包含指定模式的事件。

例如，查询 `User-Name !~ “John”` 显示除 John、John Smith 或任何包含匹配名称“John”的用户之外的事件。

有关详细信息，请参阅 自助搜索。

已翻译的操作系统版本

对于 Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源，**平台**维度现在被翻译为 **OS-Major-Version**、**OS-Minor-Version** 和 **OS-Extra-Details** 维度。根据用户的操作系统详细信息，Citrix Analytics 会在自助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标，如果您已将 **Platform** 维度用作条件，Citrix Analytics 会自动将 **Platform** 维度替换为 **OS-Major-Version**、**OS-Minor-Version** 和 **OS-Extra-Details**。此更新不会影响您定义的条件的完整性。

有关新维度的更多信息，请参阅 适用于 Virtual Apps and Desktops 的自助服务搜索。

更新了 Apps and Desktops 的数据字段

在适用于 Apps and Desktops 的自助服务搜索中，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 适用于 Apps and Desktops 的自助服务搜索。

已弃用的功能

从自助服务搜索页面中删除了 VPN_AF 和 VPN_SU 事件

在 Citrix Gateway 数据源的自助服务搜索页面上，以下记录类型现已删除。

记录类型	记录名称
VPN_SU	会话更新记录
VPN_AF	应用程序启动失败记录

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标都将停止运行。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关详细信息，请参阅 Gateway 的自助搜索。

March 11, 2021

新增功能

用户风险评分架构的当前时间戳

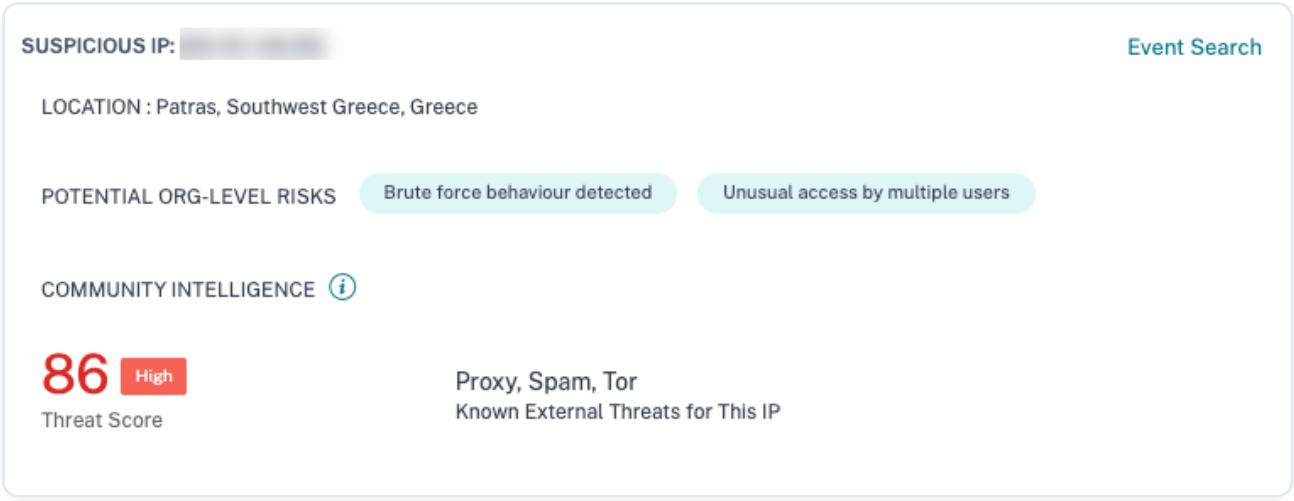
用户风险评分架构格式中添加了一个新字段 `last_update_timestamp`。此字段指示上次更新风险评分的时间。有关架构格式的更多信息，请参阅 用户风险评分架构。

March 03, 2021

新增功能

可疑 IP 登录风险指标的增强功能

在用户的风险时间线页面上，针对**可疑 IP 登录**风险指标显示了一个新部分**可疑 IP**。此部分提供以下信息：



- 检测到可疑登录活动的 IP 地址。
- 用户的位置。
- Citrix Analytics 最近在您的组织中检测到的任何可疑 IP 活动模式。
- 关于 IP 地址的社区级情报源。

有关详细信息，请参阅 可疑 IP 登录 风险指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

异常位置访问风险指示器增强功能

- 在 Citrix Content Collaboration 的异常位置访问风险指示器中，在事件表中添加了**工具名称**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 和 Citrix DaaS 的异常位置访问风险指示器中，在事件表中添加了**设备 ID** 和**接收器类型**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

文章 介绍了 Citrix Analytics 为您的 SIEM 服务生成的处理数据的架构。

已修复的问题

- 对于 Content Collaboration 用户，如果 `Is Employee` 值为 null，则该用户不会显示在发现的用户列表中。

February 18, 2021

新增功能

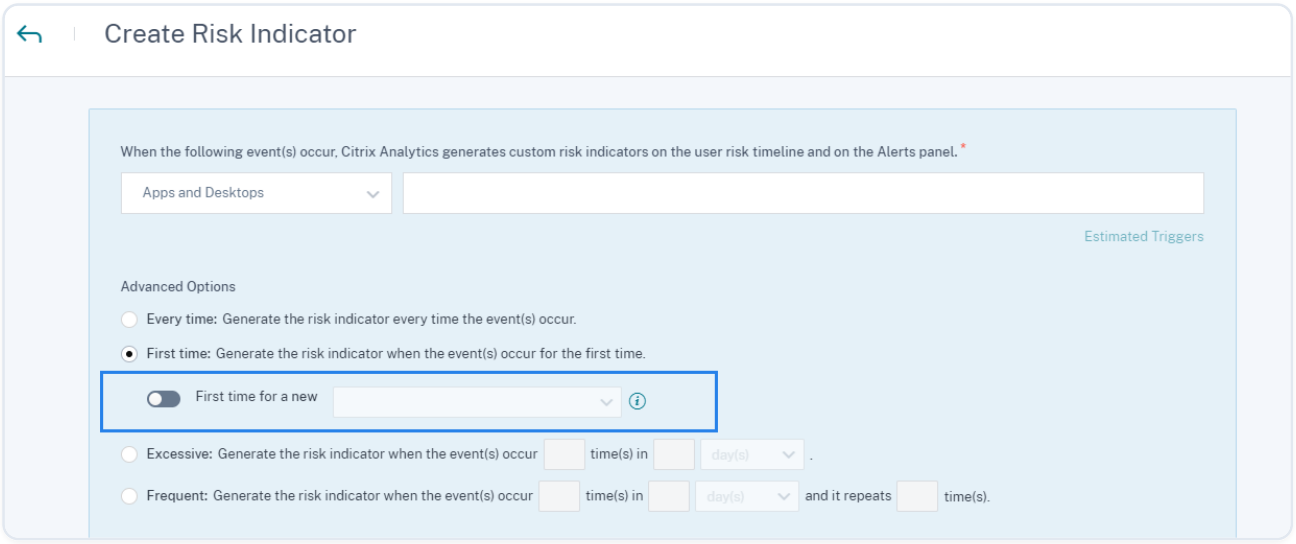
自定义风险指示器中首次从新实体访问的支持

您现在可以创建风险指示器，当 Citrix Analytics 首次从新实体接收事件时触发。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**首次针对新**按钮，并根据数据源从列表中选择一个有效实体。您无需为实体分配任何特定值。例如，如果您从列表中选择**城市**，则每当用户首次从新城市登录时，Citrix Analytics 都会触发风险指示器。

有关详细信息，请参阅 创建自定义风险指示器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



创建自定义风险指示器的最大限制

您现在最多可以创建 50 个自定义风险指标。如果达到此最大限制，则必须删除或编辑任何现有自定义风险指标才能创建新的自定义风险指标。

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

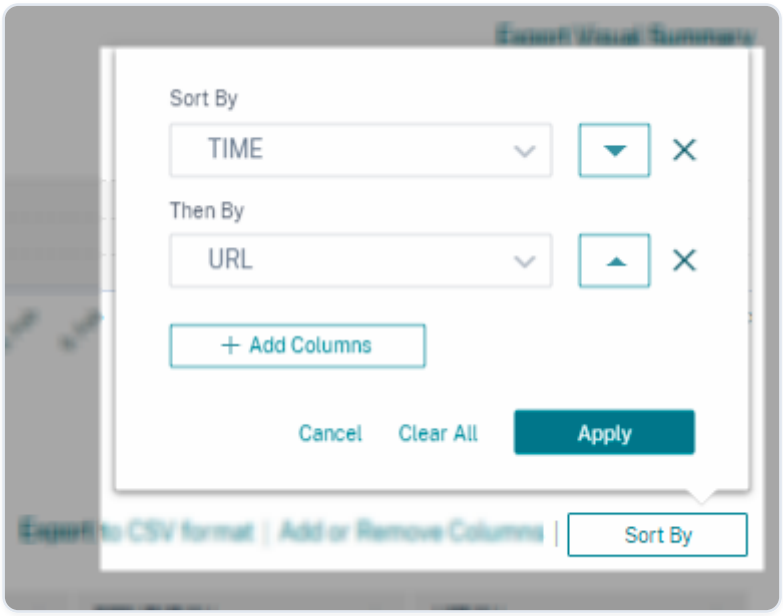
在“**用户信息**”页面上，Citrix Analytics 现在显示来自 Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源的用户位置。

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，您现在可以按多个列对用户事件进行排序。单击“**排序依据**”，添加列和排序顺序。单击“**应用**”以对用户事件进行排序。您最多可以添加六列以执行多列排序。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关详细信息，请参阅自助搜索。

已弃用的功能

“授权失败过多”风险指标已弃用

Citrix Gateway 风险指标 - **授权失败过多** 已弃用。您只能查看与此指标相关的历史数据。

以下更改适用于此弃用：

- Citrix Analytics 不再生成这些风险指标。
- Citrix Analytics 不再生成以这些风险指标作为条件的策略。
- 默认策略，如果以这些风险指标作为条件，则不再生效。

有关详细信息，请参阅 Citrix Gateway 风险指标。

January 27, 2021

新增功能

异常位置访问风险指标的增强功能

对于 Citrix Content Collaboration、Citrix Gateway 和 Citrix Virtual Apps and Desktops，当用户从与新国家/地区或与任何以前的登录位置异常遥远的新城市关联的 IP 地址登录时，将触发**异常位置访问**风险指标。其他因素包括用户的整体移动性水平以及您组织中所有用户从该城市登录的相对频率。在所有情况下，用户位置历史记录均基于过去 30 天的登录活动。

有关风险指标的更多信息，请参阅以下主题：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 思杰内容协作风险指标
- Citrix Gateway 风险指标
- Citrix 虚拟应用和桌面和 Citrix 桌面即服务风险指标

January 20, 2021

已修复的问题

- 对于使用本地 StoreFront 的 Apps and Desktops 数据源，即使 StoreFront 部署已成功连接，数据处理也会失败。

January 19, 2021

已修复问题

- 在自定义风险指标页面中，在搜索字段中更正无效条件后，**估计触发器**链接没有响应。

  例如，您输入了一个无效条件 *Client-IP = 10.10.10.10*。更正此条件并输入为 *Client-IP = "10.10.10.10"* 后，**估计触发器**链接没有响应。

  解决方法：刷新自定义指标页面，然后使用有效条件创建自定义指标。

January 13, 2021

新增功能

Citrix Analytics Add-on for Splunk 的新版本已发布

Citrix Analytics Add-on for Splunk 版本 2.1.0 现已推出。转到下载页面下载文件。

新增对 Splunk Cloud Inputs Data Manager (IDM) 和 Splunk 8.1 64 位版本的支持

您现在可以将 Citrix Analytics for Security 与 Splunk Cloud IDM 和 Splunk 8.1 64 位版本集成。有关更多信息，请参阅Splunk 集成。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已弃用的支持

已移除对 Splunk 7.1 64 位版本的支持

您无法再将 Citrix Analytics for Security 与 Splunk 7.1 64 位版本集成。有关支持的 Splunk 版本的信息，请参阅Splunk 集成。

January 11, 2021

已修复问题

- 在 Virtual Apps and Desktops 站点卡片上，标签 **支持的客户端用户** 已重命名为 **已接收来自用户的事件**。标签 **不支持的客户端用户** 已重命名为 **无法接收来自用户的事件**。

December 17, 2020

新增功能

使用预配置的自定义风险指示器和策略阻止来自异常位置的访问（地理围栏）

Citrix 提供了一系列预配置的自定义风险指示器和策略，可帮助您监控 Citrix 基础架构的安全性。通过这些指示器和策略，您可以阻止来自用户常用操作国家/地区以外的国家/地区的访问。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-会话在地理围栏外启动
- GW-地理围栏穿越
- CCC-地理围栏穿越
- 会话在地理围栏外启动

有关详细信息，请参阅预配置的自定义风险指示器和策略。

在用户响应电子邮件中查看访问位置

用户响应电子邮件现在显示用户在过去 15 分钟内访问的所有位置，而不是用户设备的 IP 地址。位置以 `<City>,<Country>` 格式显示。如果城市或国家/地区不可用，则相应的值显示为“未知”。

有关详细信息，请参阅 请求用户响应。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已重命名内容协作风险指示器 - 首次从新位置访问

Citrix 内容协作风险指示器 **首次从新位置访问** 已重命名为 **从异常位置访问**。

有关详细信息，请参阅从异常位置访问。

已弃用功能

风险指示器反馈

风险指示器反馈机制已移除。如果内容协作风险指示器 - 从异常位置访问被错误触发，您将无法再将其报告为误报并提供反馈。

December 07, 2020

新增功能

潜在数据渗漏风险指示器的改进

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。

有关风险指示器的详细信息，请参阅 潜在数据渗漏。

对内容协作风险指示器 - 首次从新位置访问的改进

在用户风险时间轴上，选择 **首次从新位置访问** 以查看以下信息：

- **登录位置**：显示用户登录的常见和异常位置的地理地图视图。
- **过去 30 天内从常见位置登录的次数**：显示用户在过去 30 天内登录的前 6 个常见位置的饼图视图。它还显示了从这些位置登录的事件数量。
- **异常位置的事件详细信息**：提供用户从异常位置登录的事件列表。

有关风险指标的更多信息，请参阅首次从新位置访问。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

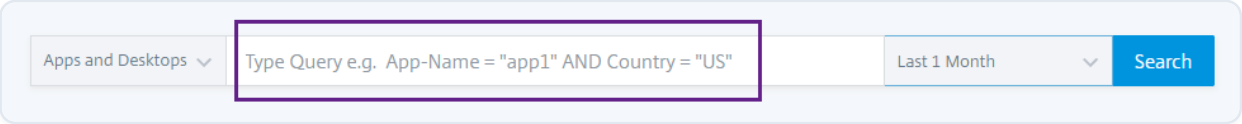
November 30, 2020

新增功能

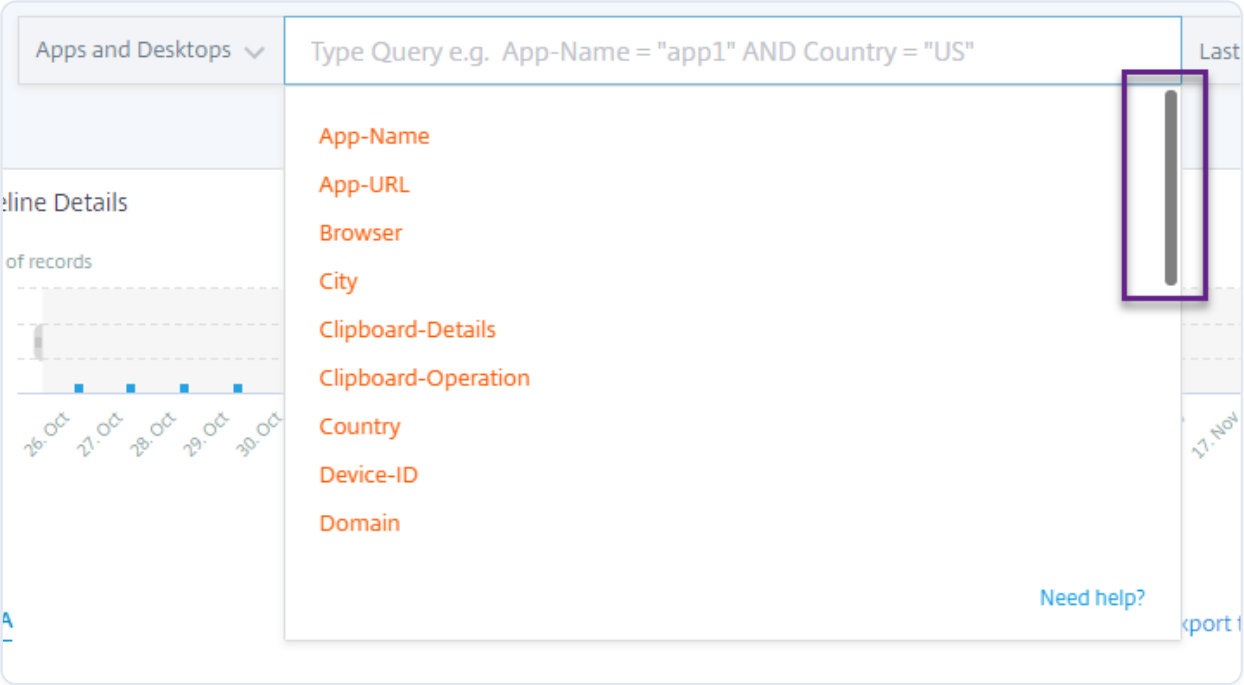
自助搜索页面改进

为增强自助搜索页面的可用性，进行了以下改进：

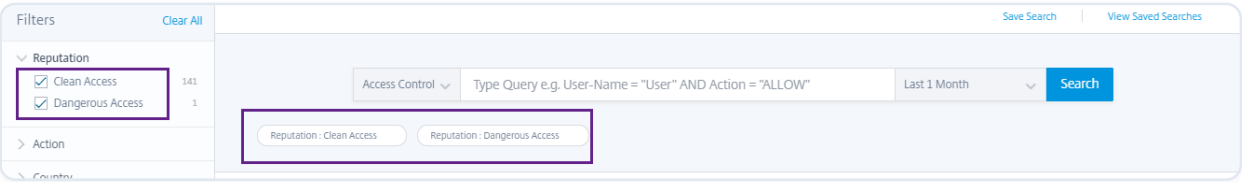
- 搜索框显示查询示例，以指示如何键入您自己的查询。



- 在 macOS 中，维度列表上的滚动条现在默认显示。

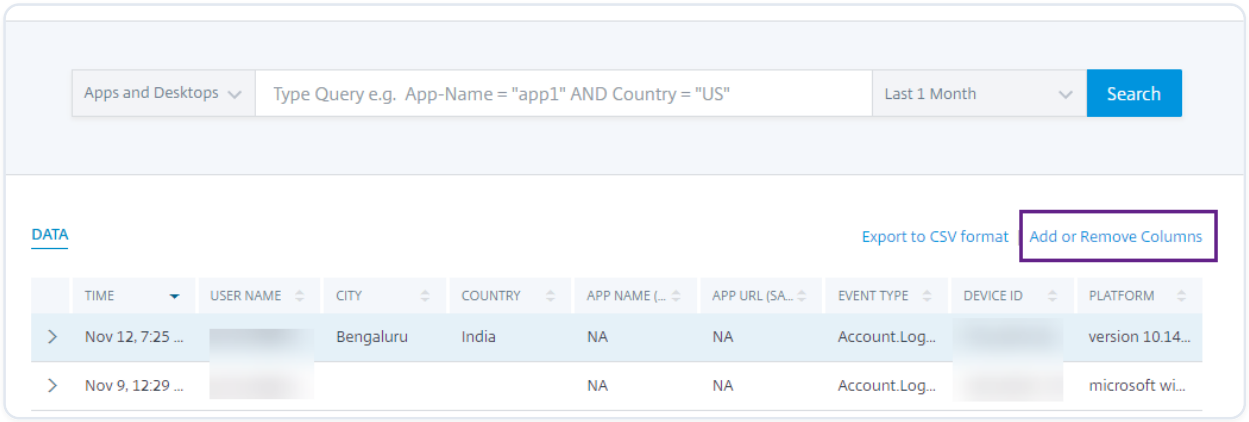


- 应用的筛选器现在显示为芯片。



- “**添加或删除列**”标签取代了“**+**”图标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关详细信息，请参阅 自助搜索。

策略改进

策略页面现在显示与已成功发现并连接到 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。

November 04, 2020

新增功能

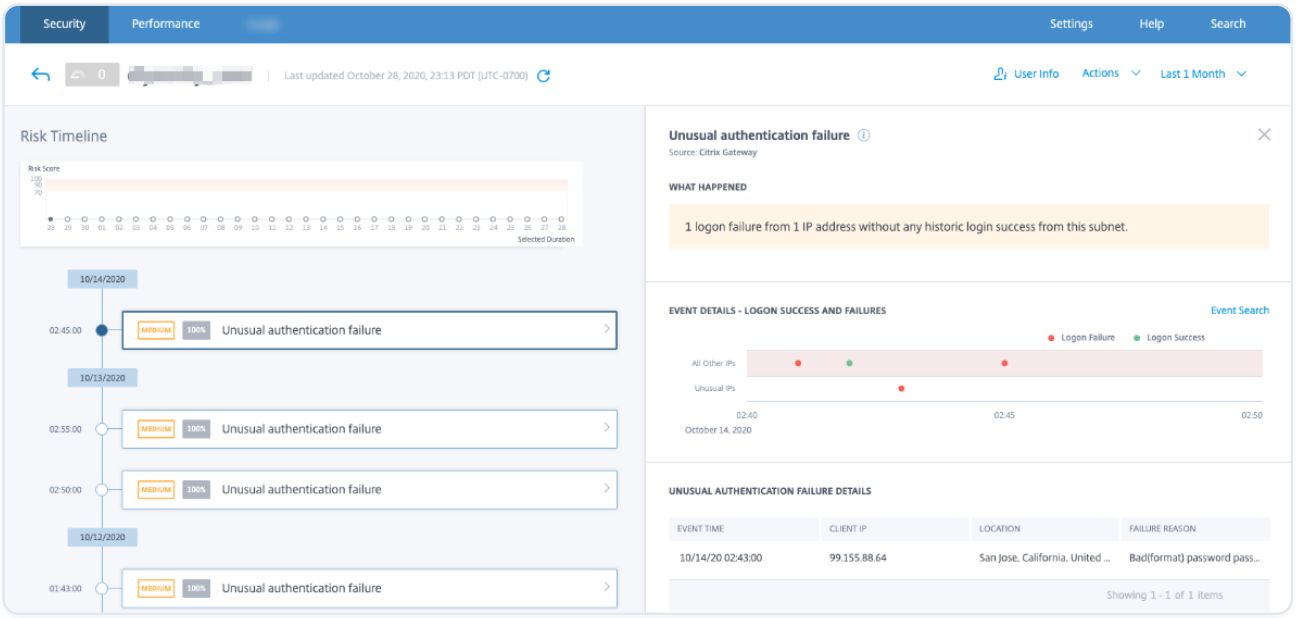
异常身份验证失败 - Citrix Gateway 风险指示器

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

当您组织中的用户从异常 IP 地址登录失败，且此行为与他们的常规行为不符时，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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



October 20, 2020

已修复问题

- 风险指示器 **首次从新设备访问** 应用了 **注销用户** 操作后未按预期工作。

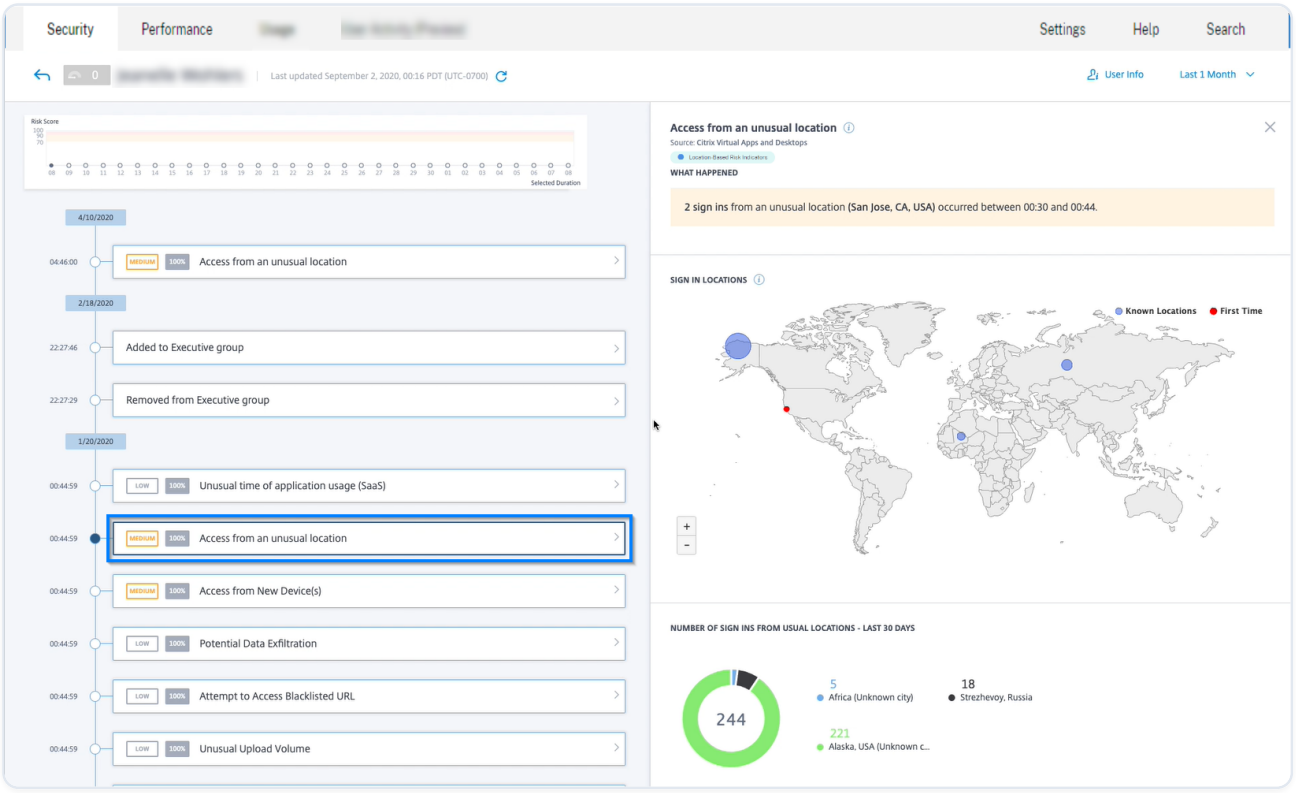
October 15, 2020

新功能

从异常位置访问 – Citrix Virtual Apps and Desktops 和 Citrix DaaS 风险指示器

Citrix Analytics 根据来自 Citrix Workspace 的异常登录检测基于访问的威胁，并触发相应的风险指示器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

共享链接仪表板增强功能

- “共享 URL”列现已替换为“共享 ID”列。每个共享 URL 现在都通过一个共享 ID 进行标识。
- 仪表板上的时间选择功能已移除。现在，此仪表板显示从活动状态到过期状态的所有共享链接，而不是选定期间的链接。
- 所有共享链接按活动链接在前、过期链接在后的顺序排序。默认情况下，风险指示器计数最高的共享链接显示在列表顶部。
- 风险链接现在显示具有风险行为的活动链接。它不显示已过期的链接。默认情况下，风险指示器计数最高的风险链接显示在列表顶部。
- “风险共享链接”卡和“所有共享链接”卡中的趋势视图已移除。

有关详细信息，请参阅共享链接仪表板。

共享链接风险时间线增强功能

风险时间线现在显示共享 ID 而不是共享 URL。有关详细信息，请参阅共享链接风险时间线。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已弃用的功能

已弃用从具有不受支持的操作系统 (OS) 的设备访问风险指示器

Citrix Virtual Apps and Desktops 风险指示器 - **从具有不受支持的操作系统 (OS) 的设备访问** 已弃用。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：

- Analytics 不再生成这些风险指示器。
- Analytics 不再生成以这些风险指示器作为条件的策略。
- 以这些风险指示器作为条件的默认策略不再生效。

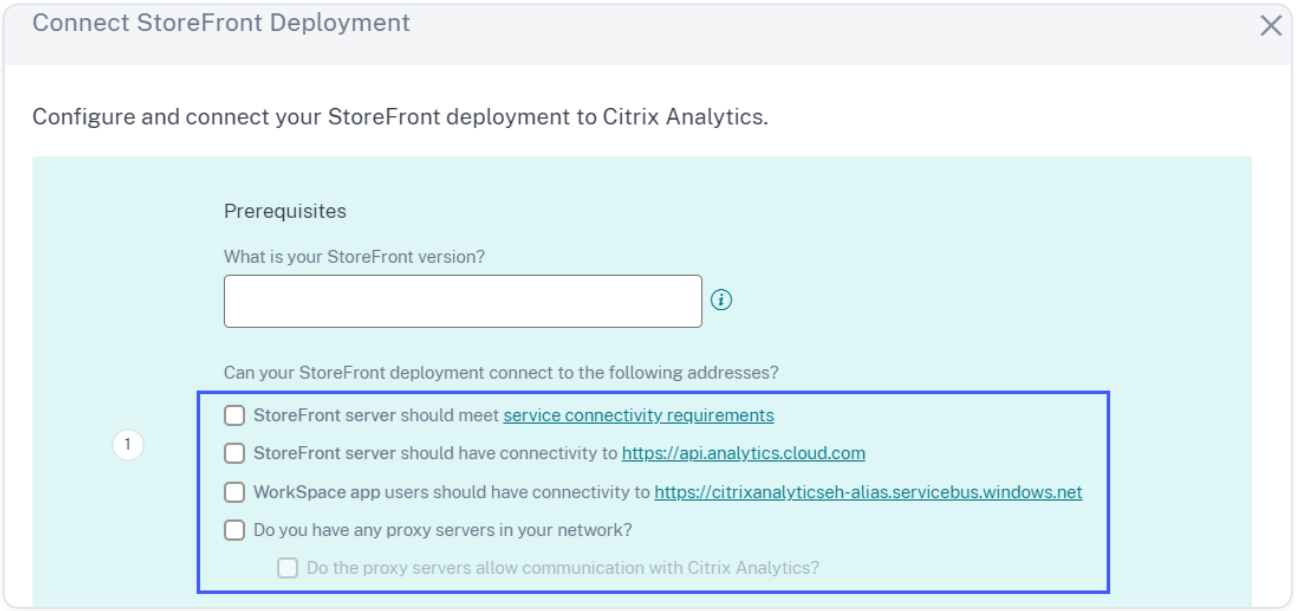
有关详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 风险指示器。

September 10, 2020

新功能

StoreFront 清单

Citrix Analytics 现在显示在下载 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 - 支持不等于 (!=) 运算符

您现在可以在以下功能中的查询中使用不等于 (!=) 运算符：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 自定义风险指标
- 自助搜索

您可以将此运算符用于以下条件：

数据源	维度
内容协作	国家/地区、城市、客户端操作系统
访问控制	国家/地区、城市、操作、URL、URL 类别、信誉、浏览器、操作系统、设备
应用程序和桌面	国家/地区、城市、应用程序名称、剪贴板操作、浏览器、操作系统
网关	身份验证阶段、客户端 IP

使用该运算符，创建具有单个值（例如“Country != XYZ”）的自定义指标表达式，并查看用户列表。然后创建策略以应用操作，例如添加到观察列表、通知管理员或禁用用户。 您还可以在指定数据源的自助服务搜索中使用该运算符来筛选用户事件。

在查询中输入维度值时，请使用数据源的自助服务搜索页面上显示的精确值。维度值区分大小写。

September 08, 2020

新功能

用户关联

Analytics 现在可以关联从各种数据源发现的用户。此机制消除了发现用户列表中的大多数重复用户。Analytics 中发现的用户现在会显示唯一用户列表及其数据源和风险指标。

例如，用户“Joe Smith”可以根据数据源拥有多个用户标识符：JosephSm、<joe.smith@citrix.com> 和 joe.smith。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已关联，并且从各种数据源收到的 Joe Smith 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

已修复问题

从“**操作**”列表中，选择操作选项并单击“**应用**”后，会显示错误消息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

August 11, 2020

已修复问题

- 您无法将 Microsoft Graph Security 与 Citrix Analytics 集成。出现此问题是因为 Microsoft 门户未能重定向到 Citrix Analytics。

July 31, 2020

已修复的问题

- 自定义风险指示器中的“**估计触发器**”选项无法预测过去一天的自定义风险指示器实例。

July 09, 2020

新增功能

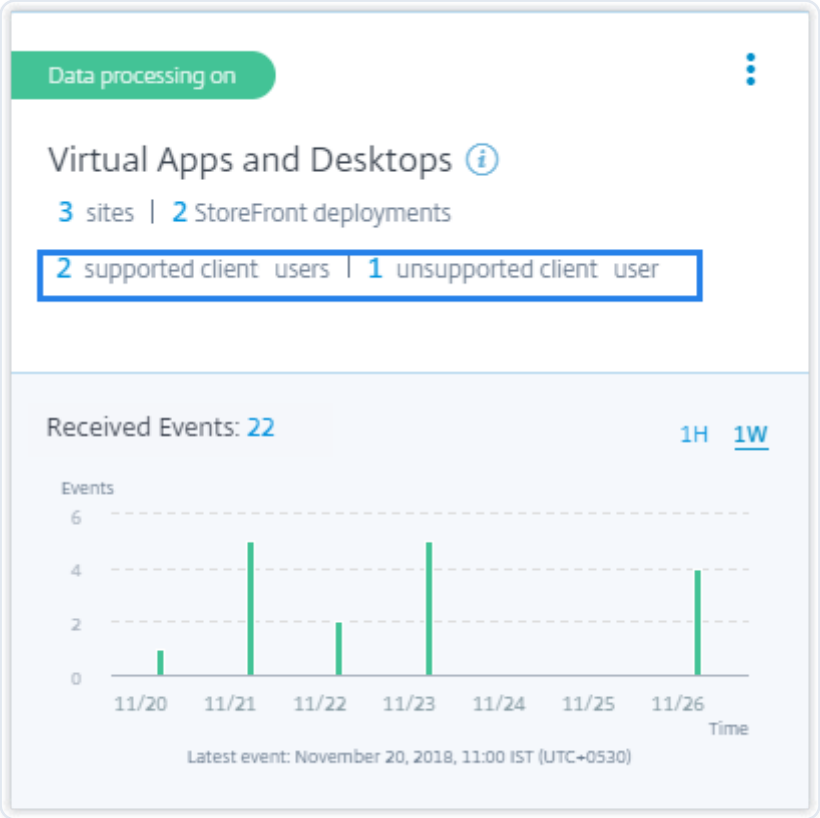
Virtual Apps and Desktops 站点卡显示使用受支持和不受支持客户端的用户

在站点卡上，您现在可以查看在其端点上使用受支持和不受支持版本的 Citrix Workspace 应用程序或 Citrix Receiver™ 客户端的用户数量。

- 单击受支持客户端的用户计数以查看显示所有已发现用户的“**用户**”页面。
- 单击不受支持客户端的用户计数以下载 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，因此不会将这些用户添加为已发现用户。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 可以提供对其行为的安全洞察。

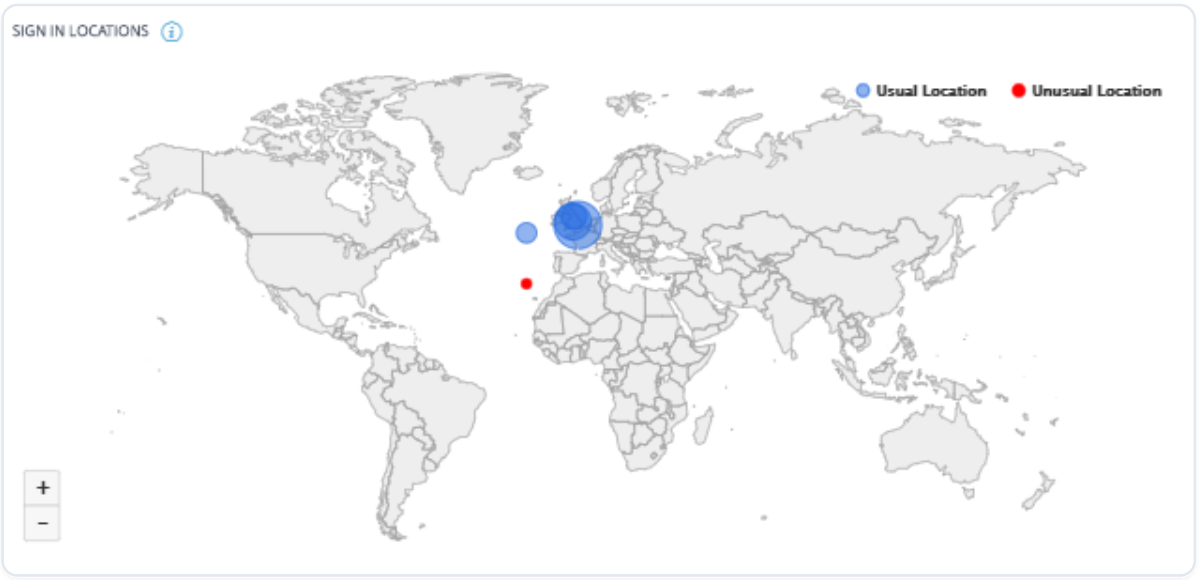
要查看受支持客户端的列表，请参阅Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



来自异常位置的访问风险指示器

- Citrix Gateway 风险指示器“**首次从新位置访问**”已重命名为“**来自异常位置的访问**”。
- 在用户风险时间线中，事件详细信息部分引入了地理地图和饼图。
  - **登录位置**：此部分显示用户常用和异常位置的地理地图视图。常用和异常位置通过地理地图右上角的颜色代码指示。您可以缩放地理地图以更近距离地查看位置。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **常用位置 - 最近 30 天**：此部分显示一个饼图，其中显示了用户登录过的排名前 6 位的常用位置。每个位置都用不同的颜色代码标记。您可以按位置对此部分进行排序，以获取所选位置的详细视图。

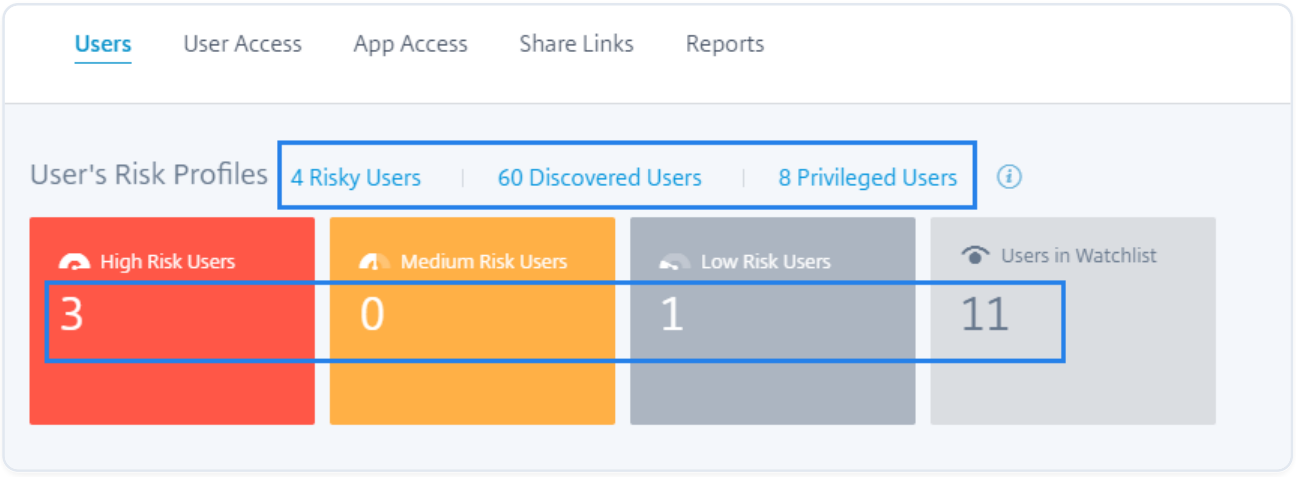


有关更多信息，请参阅来自异常位置的访问。

用户仪表板数据

无论在**用户**仪表板和**用户**页面上选择的时间段如何，都会显示过去 13 个月内的风险用户、已发现用户、特权用户和观察列表中的用户数量。当您选择时间段时，风险指标的出现次数会发生变化。

有关更多信息，请参阅用户仪表板。

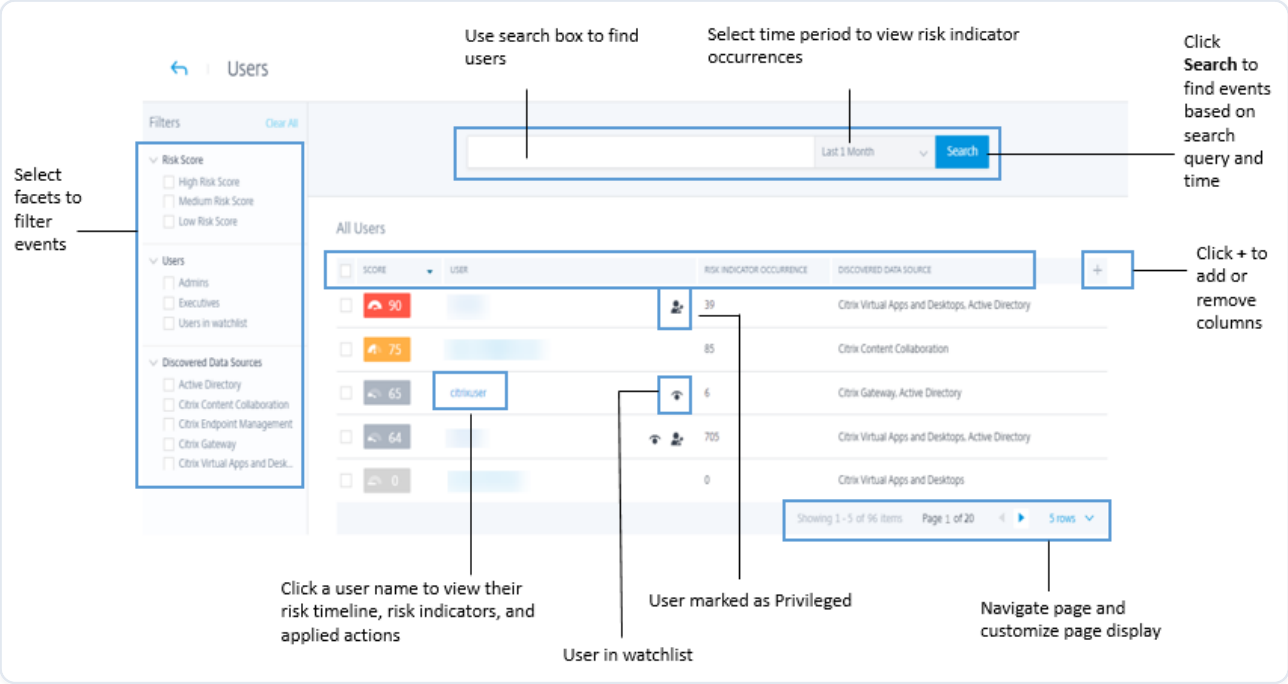


重新设计的用户页面

用户页面已得到增强，以提供更好的用户体验。它根据用户风险评分、数据源和用户类型提供用户事件的综合摘要。

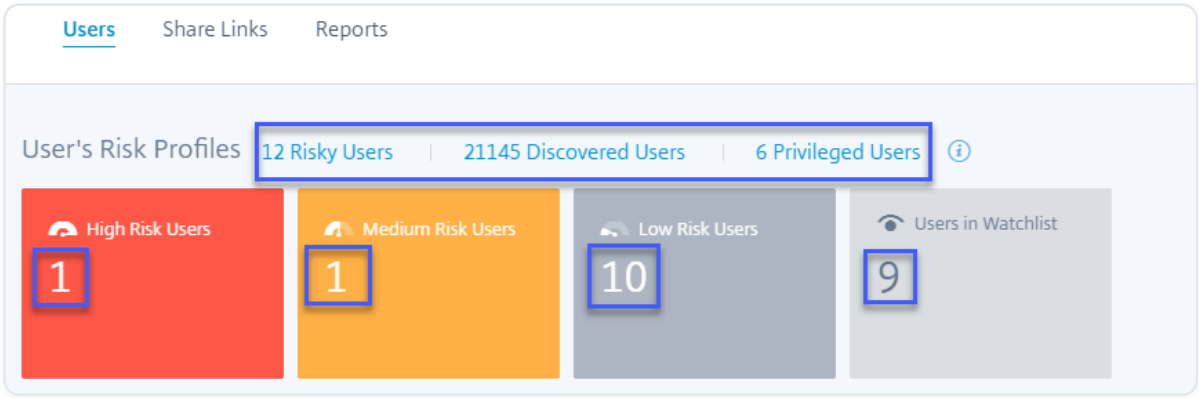
为了支持更集中的搜索，**用户**页面在左侧窗格中包含**筛选器**部分，顶部包含搜索栏。您可以搜索预设时间或自定义时间范围内的用户事件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



要查看**用户**页面：

- 转到**安全 > 用户**以查看**用户**仪表板并执行以下操作：
  - 单击以下链接或卡片之一。



  - 在**风险用户**窗格中，单击**查看更多**。
  - 在**观察列表中的用户**窗格中，单击**查看更多**。
  - 在**特权用户**窗格中，单击**查看更多**。
- 转到**设置 > 数据源 > 安全**。单击任何数据源站点卡片上的用户数量。

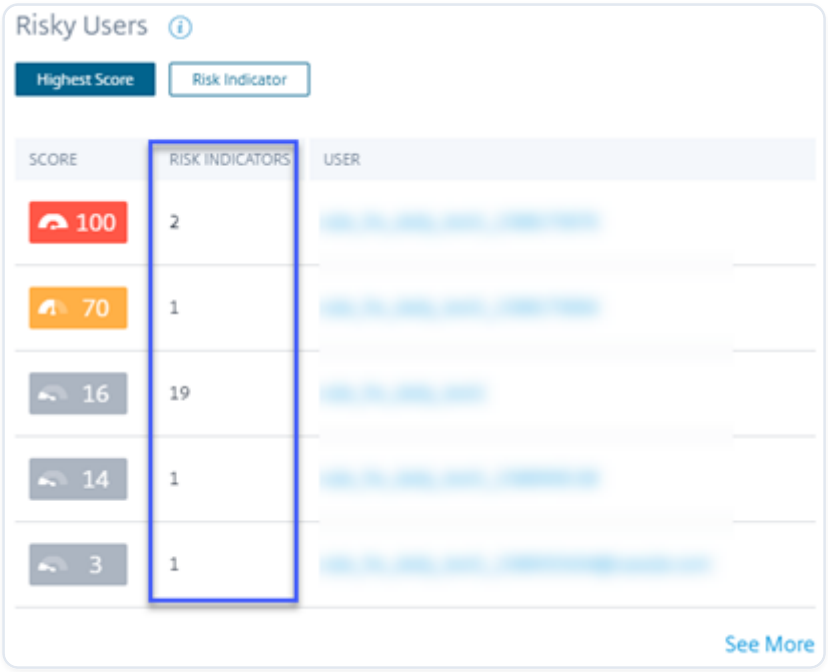
有关更多信息，请参阅用户仪表板。

风险用户窗格增强功能

更改列已替换为**风险指标**列。**风险指标**列显示用户在特定时间段内的总风险指标出现次数。

有关更多信息，请参阅风险用户。

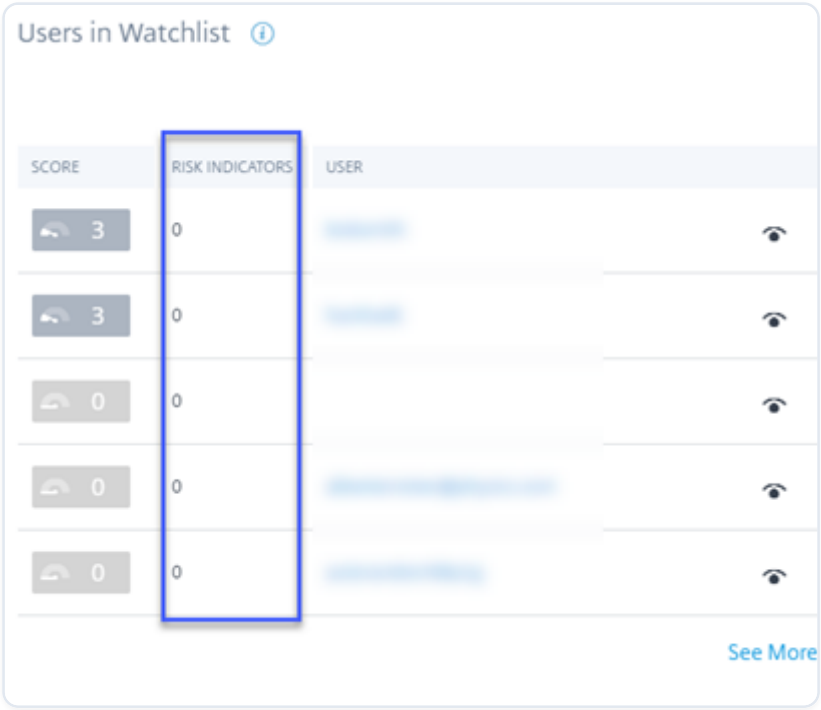
© 1997–2026 Citrix Systems, Inc. All rights reserved.



观察列表中的用户窗格增强功能

更改列已替换为**风险指标**列。**风险指标**列显示用户在特定时间段内的总风险指标出现次数。

有关更多信息，请参阅观察列表中的用户。

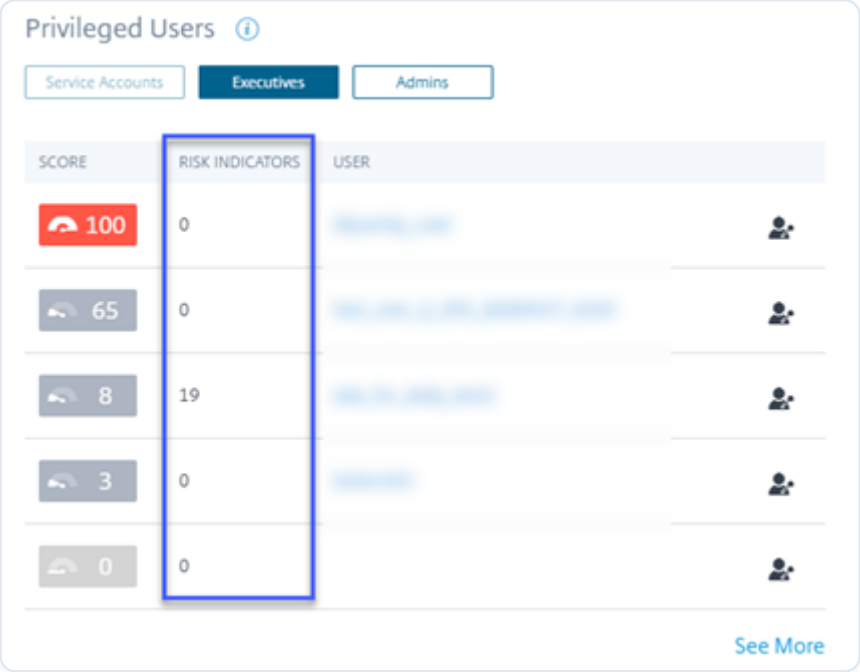


特权用户窗格增强功能

- “**更改**”列已替换为“**风险指标**”列。“**风险指标**”列显示用户在特定时间段内的总风险指标出现次数。
- 点击“**查看更多**”以查看“**用户**”页面。“**用户**”页面显示管理员和高管特权用户的列表。在此页面上，您可以添加或删除特权用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

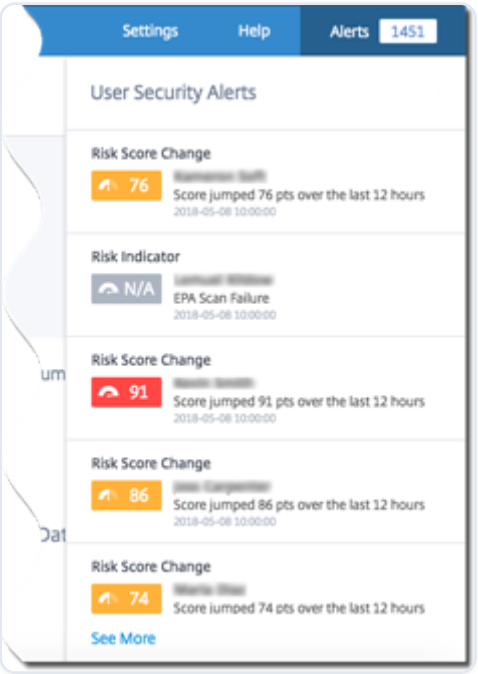
有关更多信息，请参阅特权用户。



已弃用的功能

警报

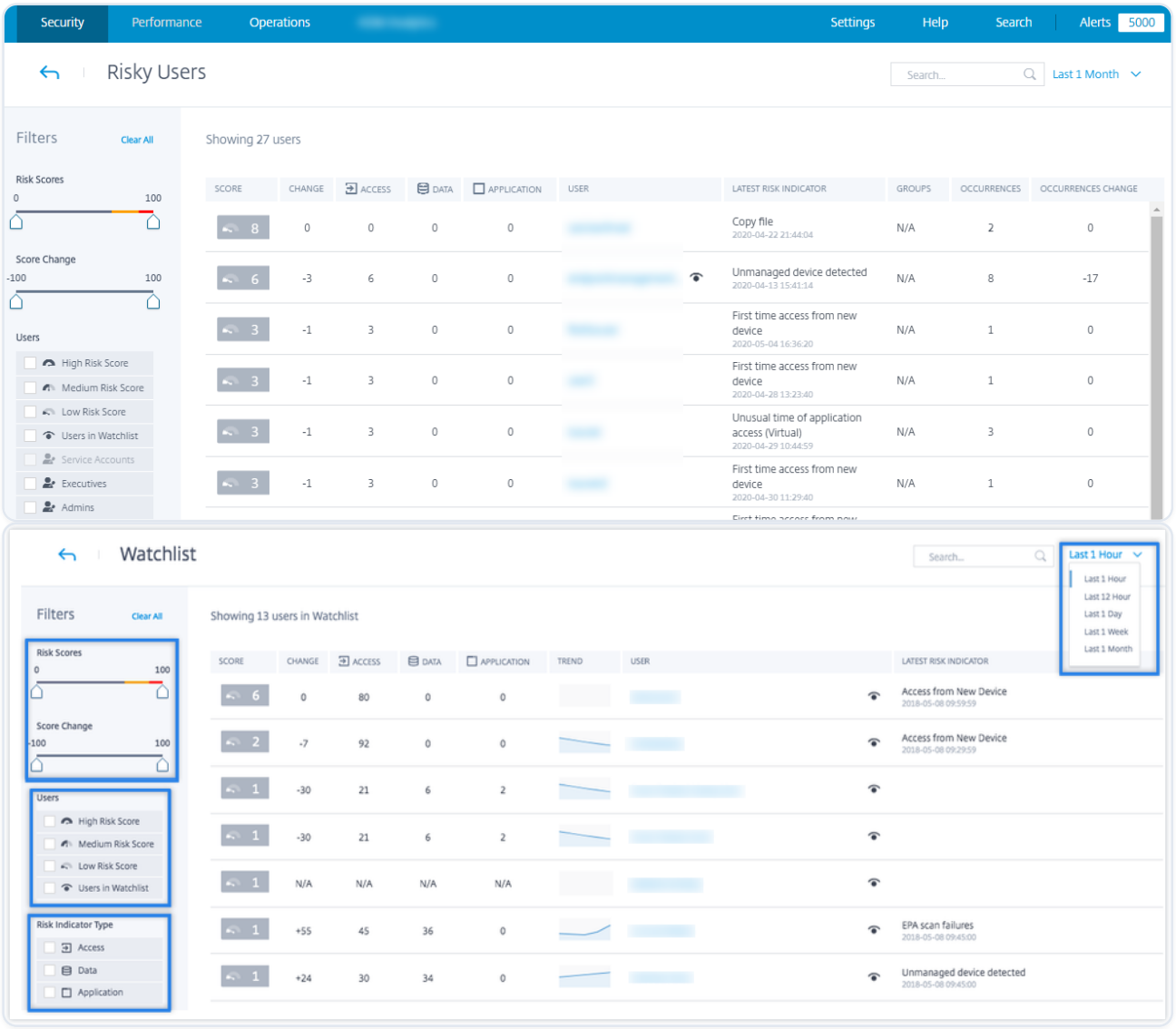
“**警报**”功能现已弃用，并且不再在 Analytics 用户界面上可用。



风险用户和观察列表页面

“**风险用户**”和“**观察列表**”页面已弃用。它们已替换为“**用户**”页面，该页面汇总了所有风险用户事件和观察列表中的用户。

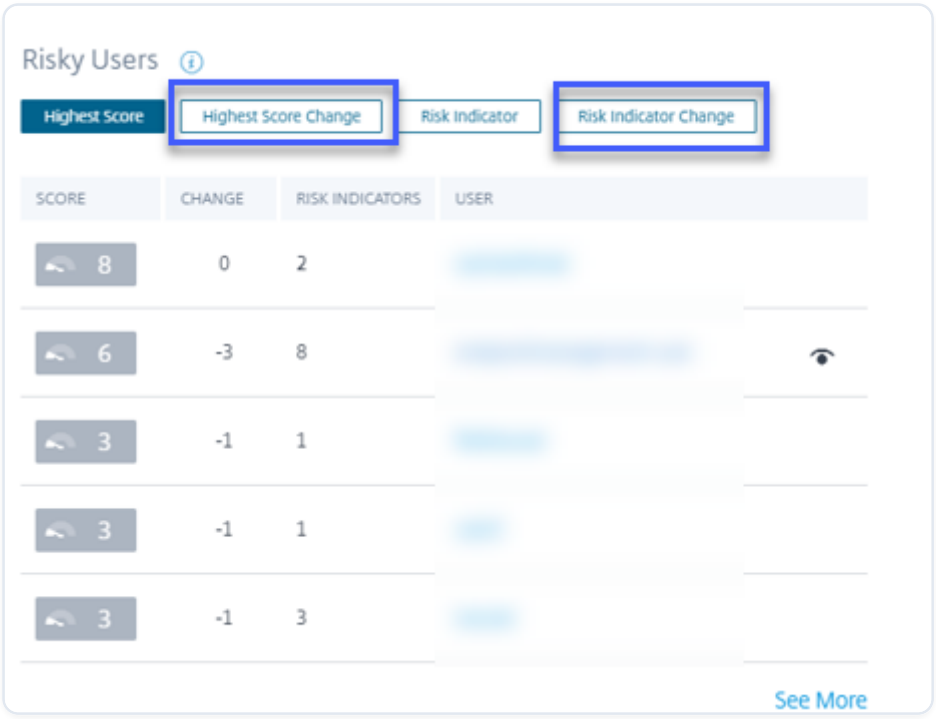
© 1997–2026 Citrix Systems, Inc. All rights reserved.



风险用户窗格

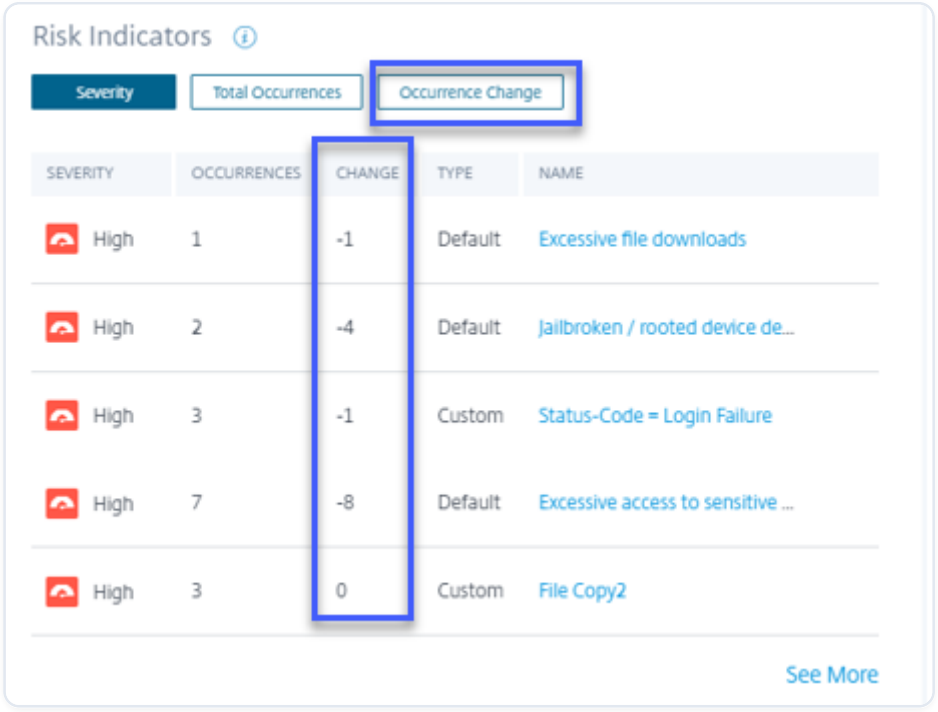
“**最高分数变化**”和“**风险指标变化**”选项卡已从“**风险用户**”窗格中移除。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



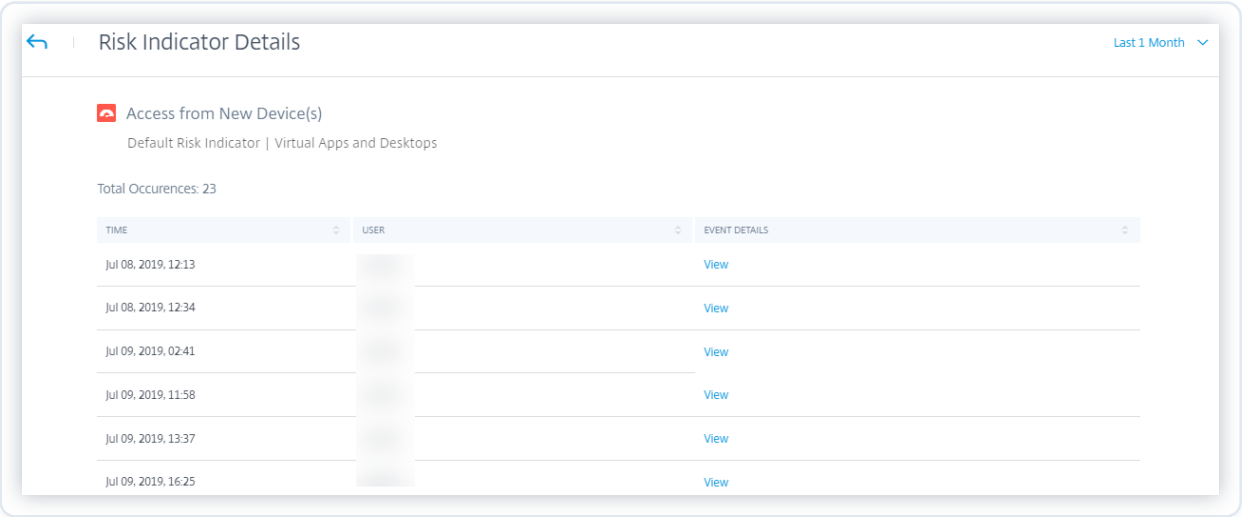
风险指标窗格

- “**发生变化**”选项卡和“**更改**”列已移除。



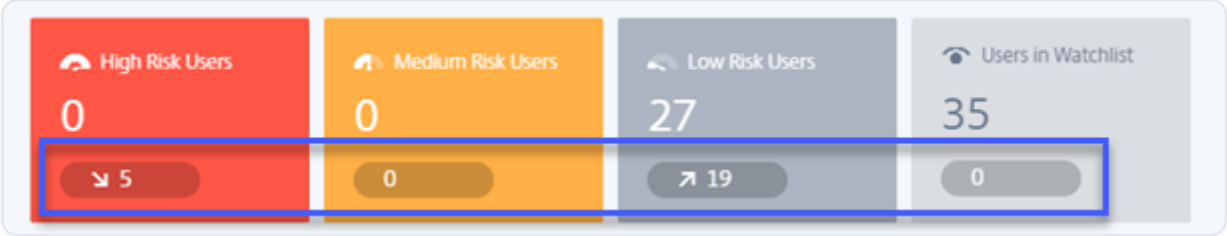
- “**风险指标详细信息**”页面已弃用。此前，当在“**风险指标**”窗格或“**风险指标概述**”页面上选择风险指标时，此页面会显示。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



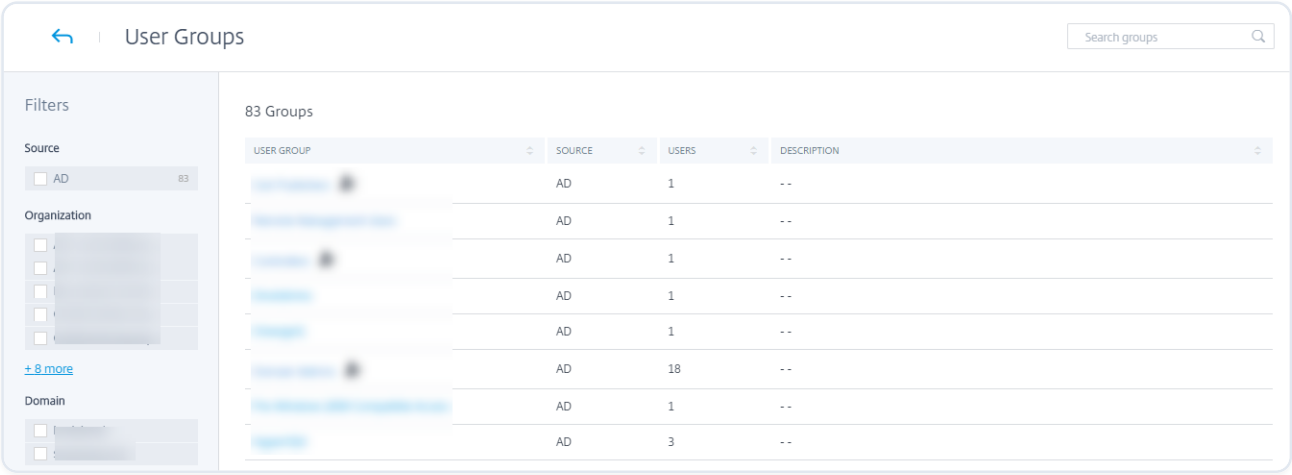
趋势视图

在“**用户**”控制面板上，已从“**高风险用户**”、“**中风险用户**”、“**低风险用户**”和“**观察列表中的用户**”卡片中移除用户计数的趋势视图。



用户组页面

“**设置**”选项下的“**用户组**”页面已弃用。您无法再将用户组添加或移除为特权组。但是，您可以将单个用户添加或移除为特权用户。有关更多详细信息，请参阅特权用户。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

June 26, 2020

已弃用的功能

应用程序访问异常时间 (虚拟/SaaS) 风险指标已弃用

Citrix Virtual Apps and Desktops 风险指标 - “**应用程序访问异常时间 (虚拟)**”和“**应用程序访问异常时间 (SaaS)**”已弃用。您只能查看与这些指标相关的历史数据。

以下更改适用于此弃用：

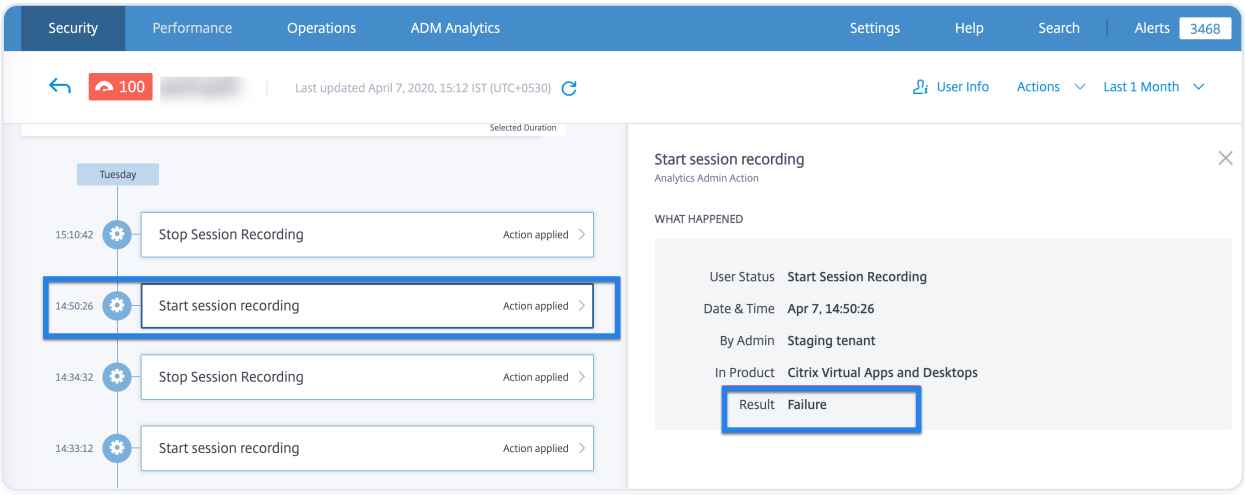
- Analytics 不再生成这些风险指标。
- Analytics 不再生成以这些风险指标作为条件的策略。
- 以这些风险指标作为条件的默认策略不再生效。

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

June 02, 2020

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”。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

May 11, 2020

已修复的问题

- 对于某些用户，基于策略的操作未触发，并且无法应用策略强制模式。当客户 ID 未采用小写形式时，会出现此问题。

  ,

- 无法为某些用户创建自定义风险指标。当客户 ID 未采用小写形式时，会出现此问题。

April 29, 2020

已修复的问题

- 应用于 Citrix Virtual Apps and Desktops 风险指标的操作未能生效，尽管 Analytics 显示操作已成功应用的消息。在 Citrix Virtual Apps and Desktops 7 1912 版本中观察到此问题。

April 02, 2020

新增功能

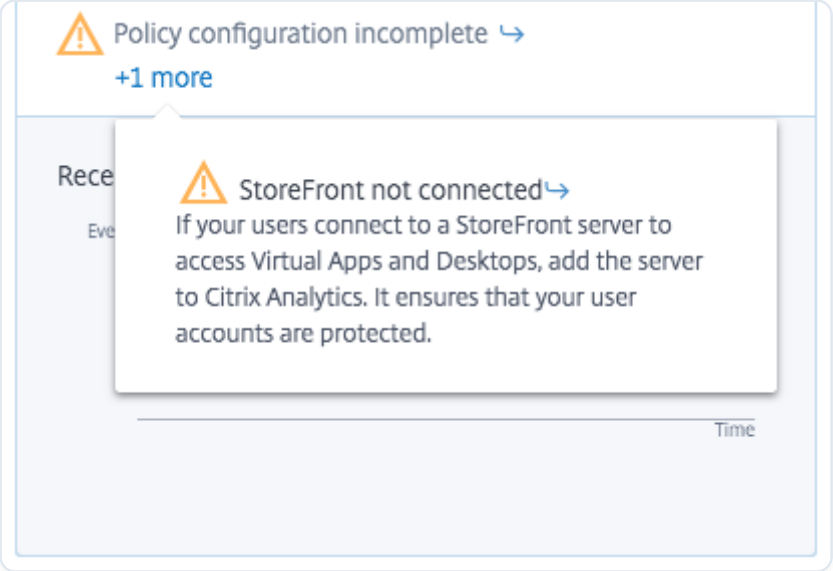
未添加 StoreFront 时禁用数据处理

在“**设置**”>“**数据源**”>“**安全**”>“**Virtual Apps and Desktops**”数据源站点卡上，如果您尚未载入 StoreFront，则“**启用数据处理**”按钮不会启用。您会在站点卡上看到“**StoreFront 未连接**”警告消息。如果您有一个活动的本地站点，并且希望 Analytics 从中接收数据，则必须验证您已将 StoreFront 载入 Citrix Analytics。这可确保您的用户帐户受到保护。

在“**Virtual Apps and Desktops**”站点卡上，选择垂直省略号 (⋮) 并单击“**连接 StoreFront 部署**”。在显示的屏幕上，按照说明完成 StoreFront 配置。

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



已修复的问题

- 对于 Citrix Content Collaboration 用户，在以下情况下，基于策略的操作未能生效：
  - 定义自定义风险指标条件时
  - 直到为用户生成风险指标

March 04, 2020

已修复问题

- 当 Gateway 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 **此 IP 地址的设备已存在**。

February 20, 2020

新增功能

Citrix Analytics for Security 所提供的产品

Citrix Analytics for Security 现已提供个人订阅。 您可以订阅 Citrix Analytics for Security 并获取此产品特有的见解。有关详细信息，请参阅 入门。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

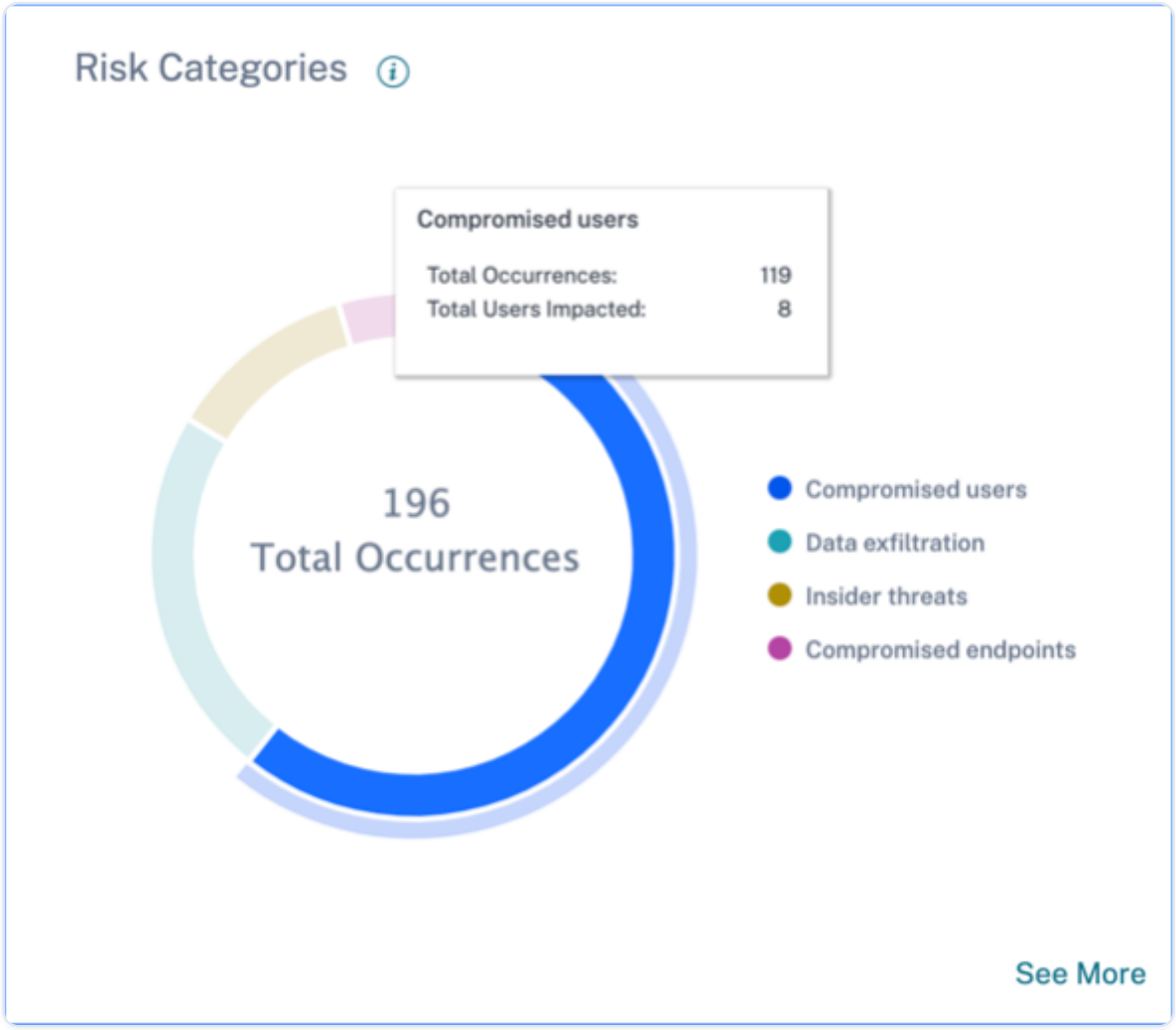
风险类别控制板

Citrix Analytics 引入了根据对组织安全方面具有类似影响的风险对风险指标进行分类的功能。此控制板提供了风险暴露和需要立即关注的关键风险的全面视图。对于默认风险指标，Analytics 会根据风险暴露自动分配风险类别。对于自定义风险指标，您必须根据风险暴露选择适当的风险类别。

Analytics 支持以下风险类别：

- 数据渗漏
- 内部威胁
- 受感染用户
- 受感染的端点

有关详细信息，请参阅风险类别。

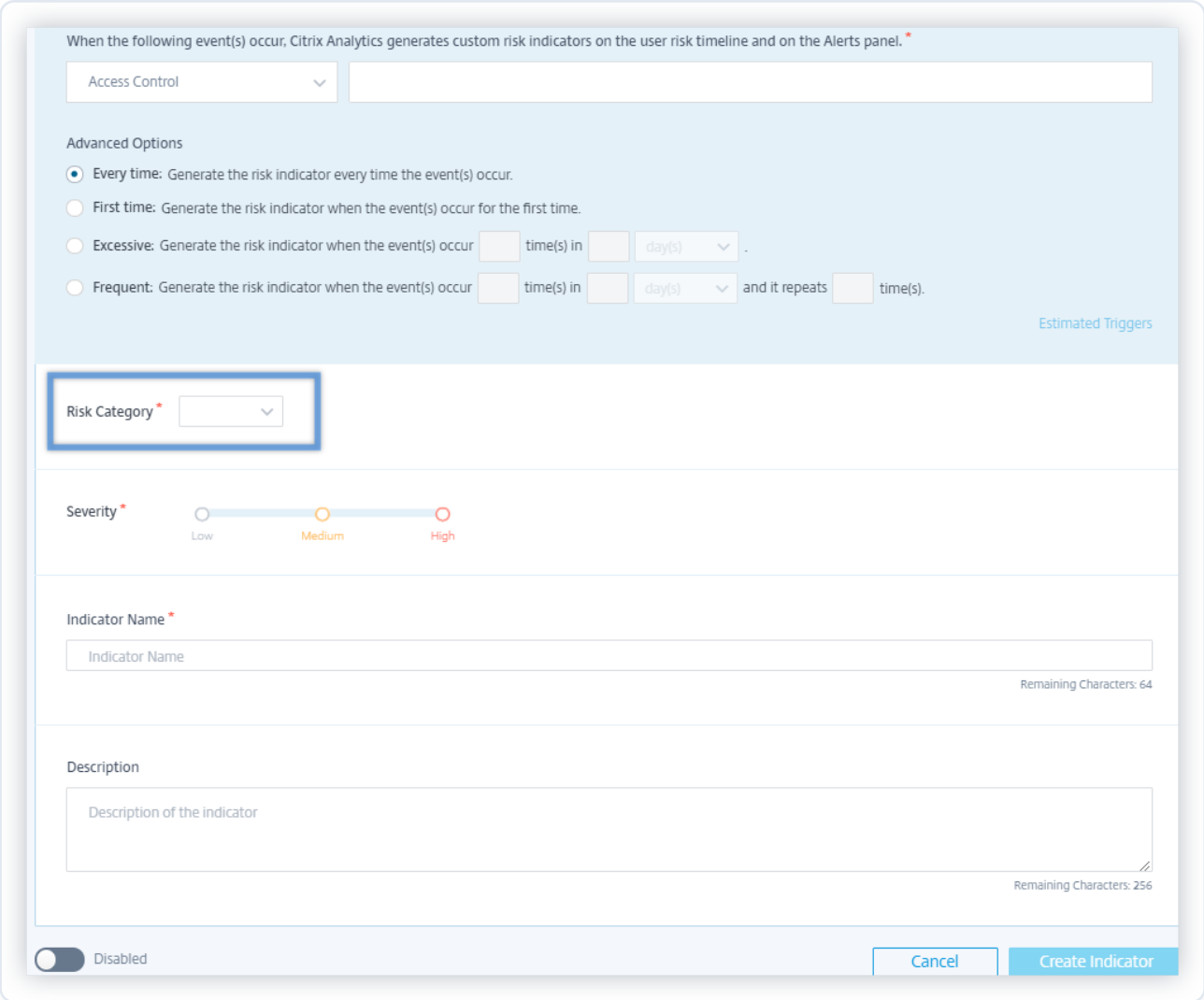


© 1997–2026 Citrix Systems, Inc. All rights reserved.

自定义指标页面上的风险类别列

在“自定义风险指标”页面上引入了**风险类别**列。您可以根据风险暴露类型为自定义风险指标选择风险类别。如果您通过选择风险类别来修改以前创建的自定义风险指标，它们将显示在“风险类别”仪表板上。

有关详细信息，请参阅自定义风险指标。



风险指标名称变更

以下风险指标名称已更改：

数据源	旧名称	新名称
Citrix 虚拟应用和桌面 和 Citrix 桌面即服务	异常应用程序使用情况（虚拟）	异常应用程序访问时间（虚拟）
Citrix 虚拟应用和桌面和 Citrix DaaS	异常应用程序使用情况 (SaaS)	异常应用程序访问时间 (SaaS)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

数据源	旧名称	新名称
Citrix 内容协作	过多的登录失败	过多的身份验证失败
Citrix 内容协作	异常登录访问	从新位置首次访问
Citrix 访问控制	异常下载量	过多的数据下载
Citrix 网关	登录失败	过多的身份验证失败
思杰网关	授权失败	过多授权失败
思杰网关	异常登录访问	首次从新位置访问

有关详细信息，请参阅风险指标。

已修复的问题

- 对于某些用户，即使数据源已成功载入且 StoreFront 已启用，Citrix Analytics 也无法从 Virtual Apps and Desktops 接收任何数据。
- Citrix Analytics 无法从 Citrix Content Collaboration 接收下载事件。因此，不会触发以下风险指标：
  - 匿名敏感共享下载
  - 过多共享链接下载
  - 过多敏感文件访问
  - 过多文件下载
- 对于新加入的用户，在 Citrix Gateway 风险指标上应用的手动和基于策略的操作不生效。
- 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。

January 09, 2020

新功能

持续风险评估

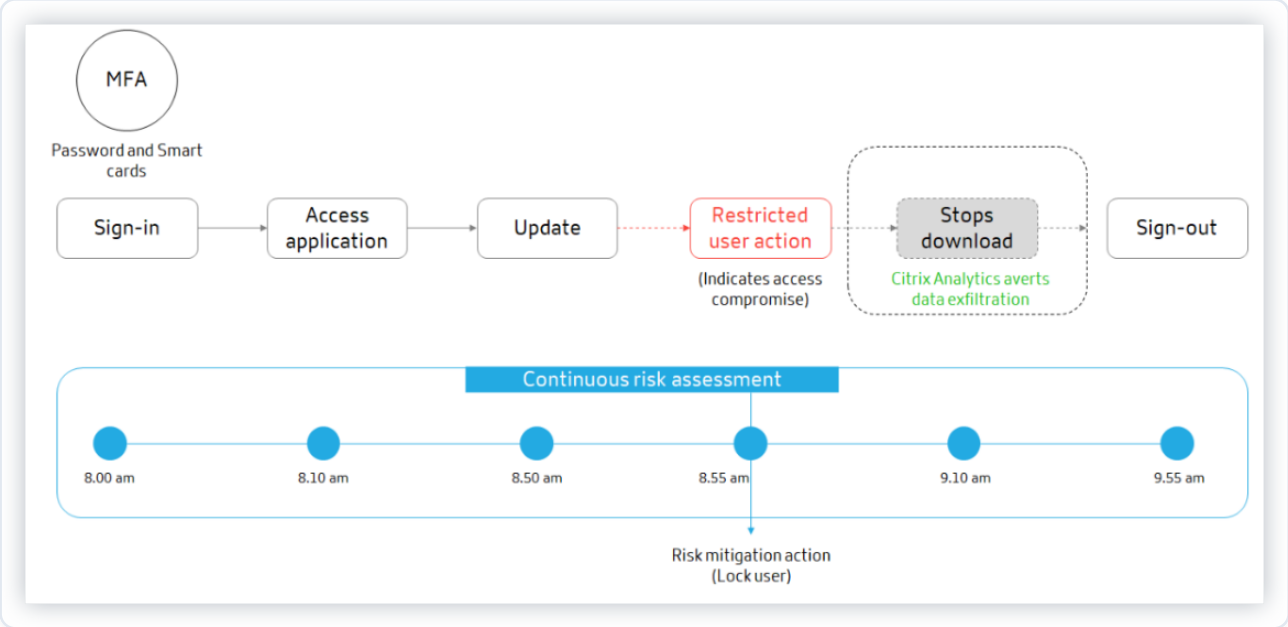
Citrix Workspace 用户面临的一些挑战是，远程访问通过数据泄露、盗窃、破坏和服务中断等网络犯罪活动，将敏感数据暴露给安全风险。组织内的员工也可能助长这种损害。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

解决这些风险的一些方法是实施多重身份验证、强制执行短登录超时等。尽管这些风险评估方法确保了更高的安全性，但它们在初始验证后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 引入了持续风险评估解决方案。此解决方案可帮助您持续监控用户配置文件，并在检测到风险事件时采取各种措施。

有关更多信息，请参阅持续风险评估。



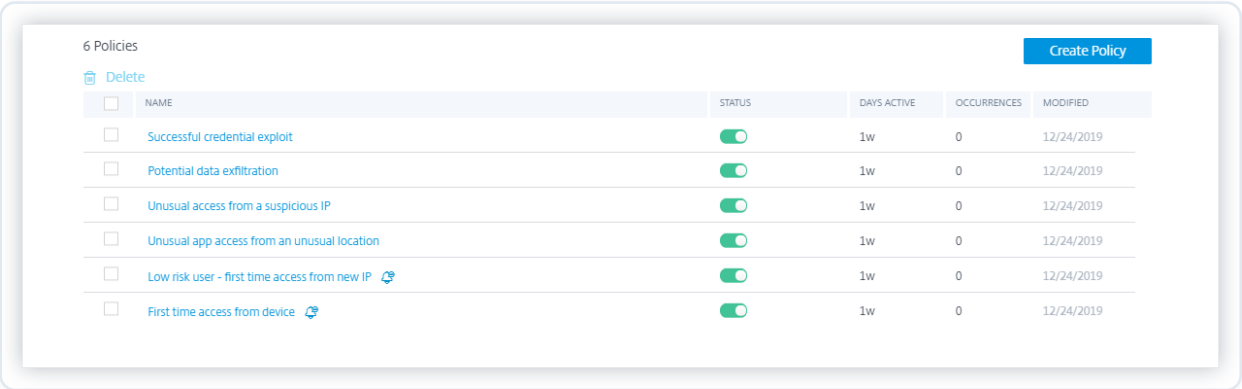
策略配置

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

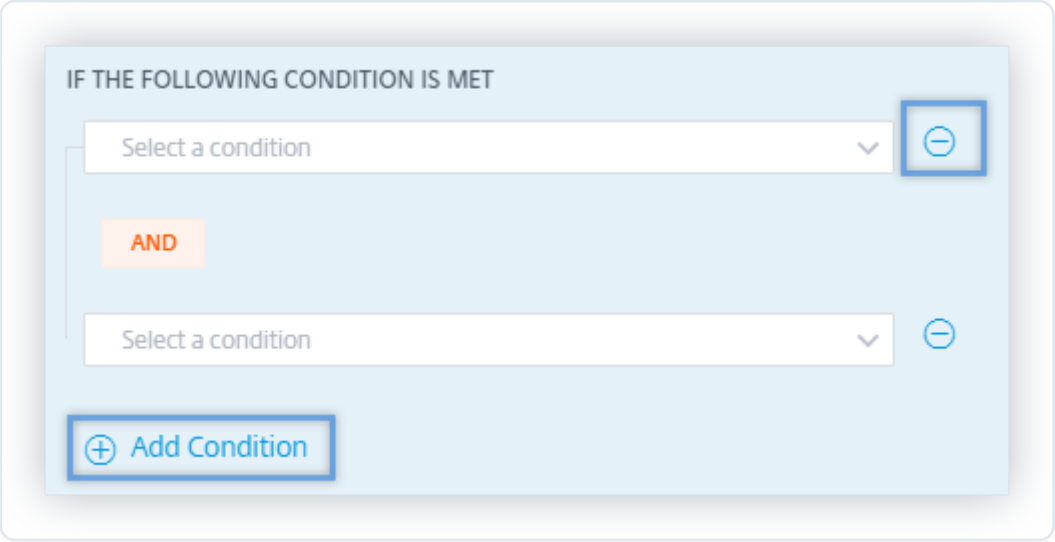
- **默认策略**：Citrix Analytics 支持以下默认策略：
  - 凭据成功利用
  - 潜在数据泄露
  - 来自可疑 IP 的异常访问
  - 来自异常位置的异常应用访问
  - 低风险用户 - 首次从新 IP 访问
  - 首次从设备访问

  您可以根据您的要求修改默认策略。

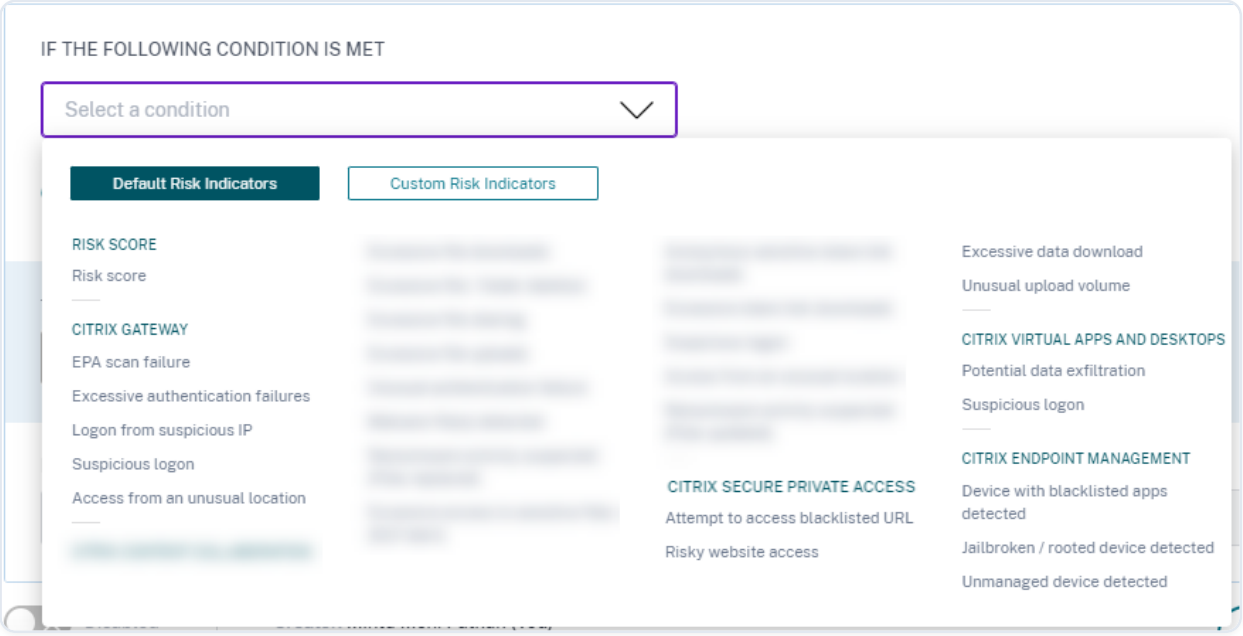
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **多个条件**：一个策略最多可以包含四个条件。这些条件可以通过风险评分和风险指标的组合或两者兼有来设置。

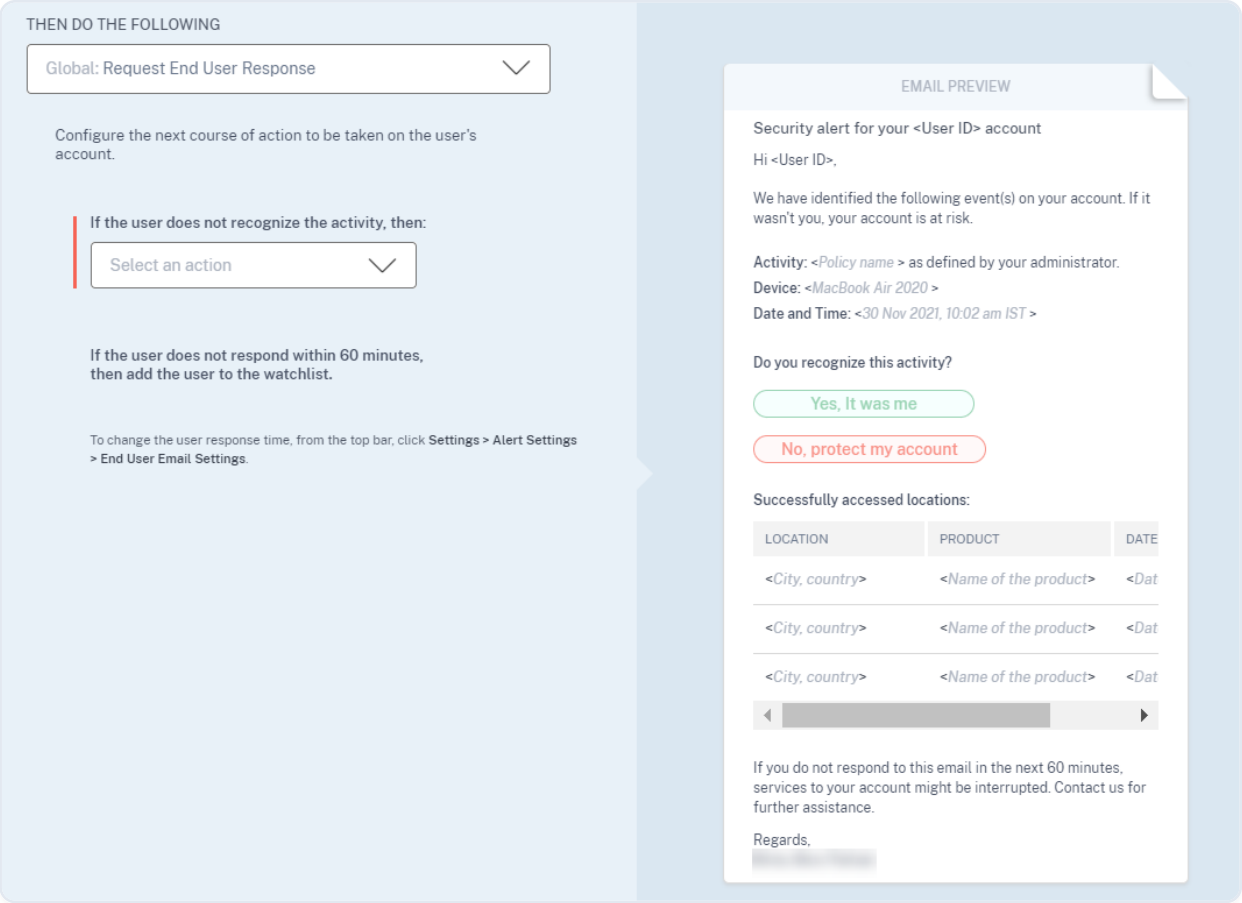


- **默认和自定义风险指标**：**创建策略**页面上的条件菜单现在根据默认和自定义风险指标进行区分。创建策略时，您可以在默认和自定义风险指标选项卡之间切换，并设置风险指标条件。



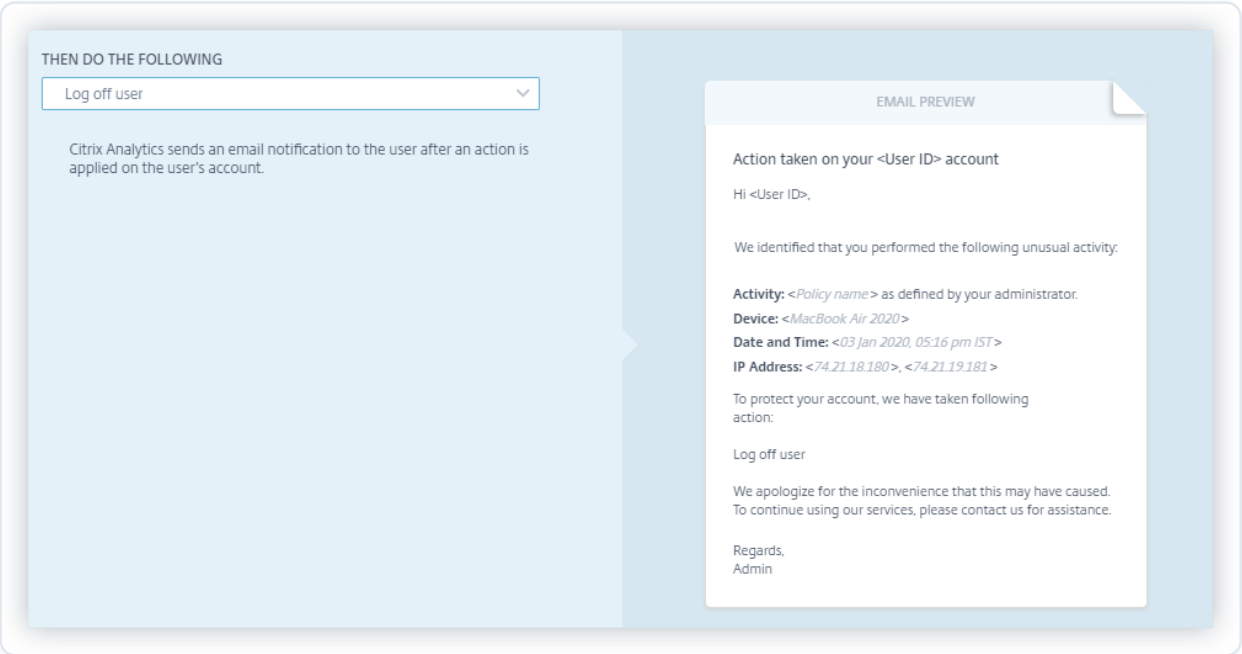
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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活动的电子邮件通知。一旦用户对活动做出响应，您就可以确定对其帐户采取的下一步措施。您还可以设置用户响应时间。如果未收到响应，Citrix Analytics 会将**无响应**视为状态。

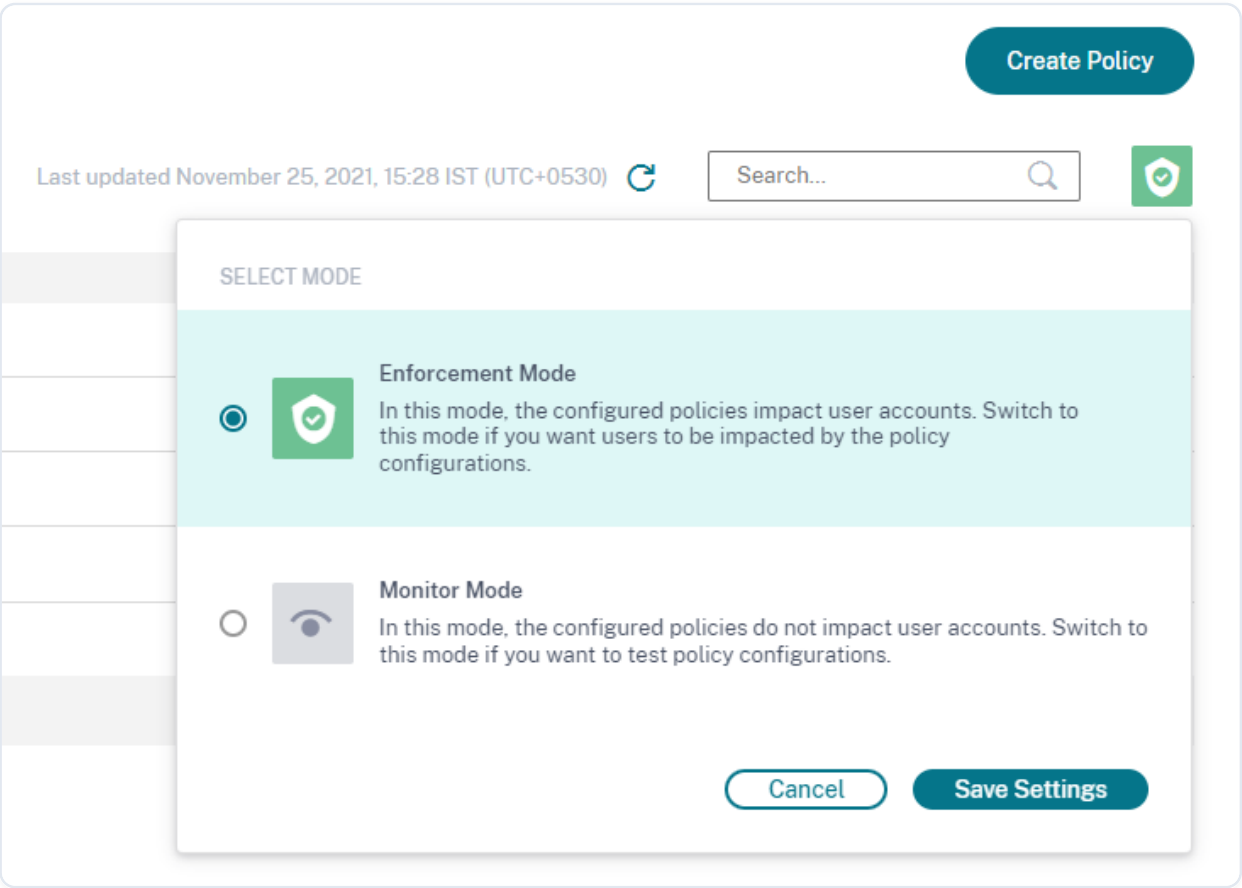


- **应用中断性操作**：当应用**注销用户**或**锁定用户**等中断性操作时，您可以通知用户。系统会向用户发送包含活动详细信息和所应用操作的通知。此操作会暂时中断用户帐户的服务，以防止进一步滥用。要继续访问帐户，用户必须联系管理员寻求帮助。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **强制和监视模式**：您可以为策略设置强制或监视模式。



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

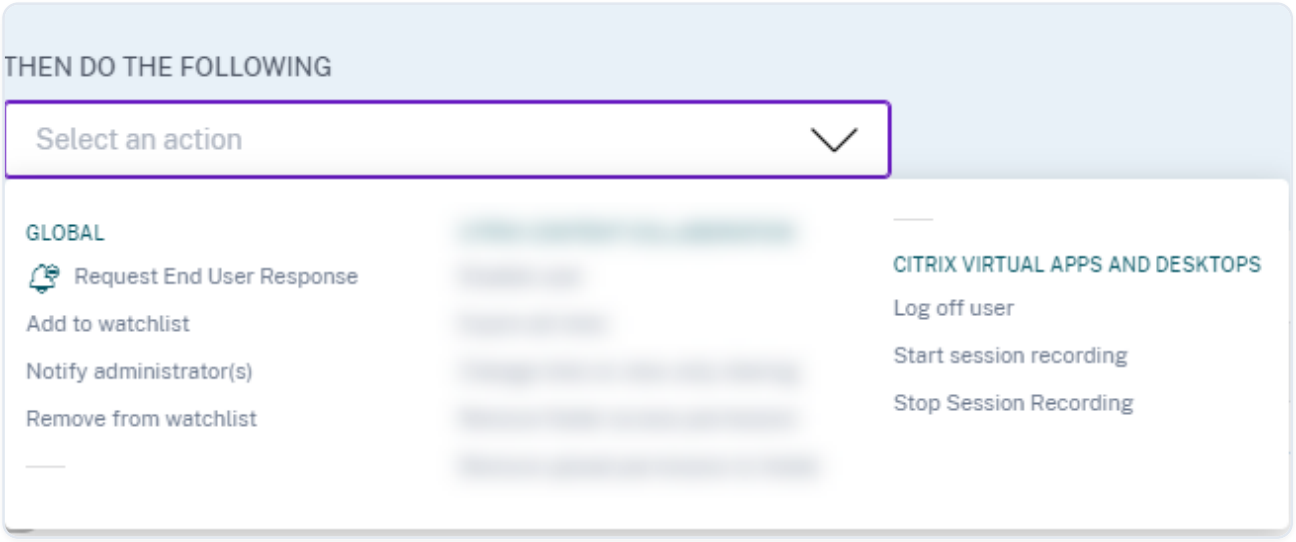
Citrix Analytics 引入了以下 Gateway 操作：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 锁定用户
- 解锁用户

您可以手动应用这些操作，也可以在配置策略时应用这些操作。

有关更多信息，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。它总结了用户尝试访问组织内资源的总次数。

有关更多信息，请参阅访问摘要。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

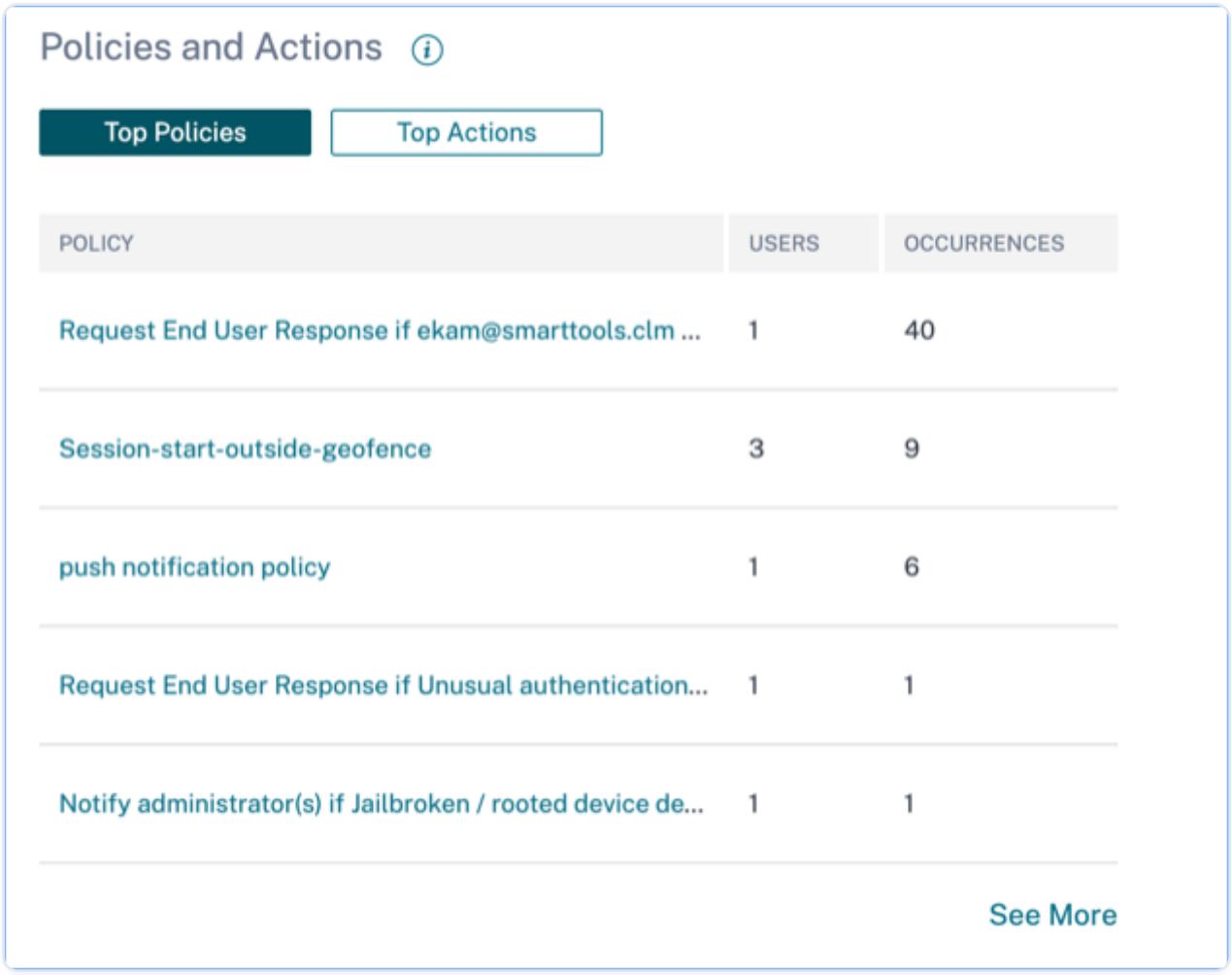


策略和操作控制板

Citrix Analytics 在**用户**控制板上引入了**策略和操作**面板。它显示了应用于用户配置文件的前五项策略和操作。您可以根据选定时间段内的热门策略和热门操作对数据进行排序。

有关详细信息，请参阅策略和操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



策略的自助搜索

使用自助搜索查看符合您定义的策略的用户事件。您还可以查看 Analytics 为这些异常事件应用的操作。使用分面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，请参阅策略的自助搜索。

已弃用的功能

已删除基于风险评分更改策略的条件

配置策略时，您不能再使用“**风险评分更改**”这一基于策略的条件。Citrix Analytics 不支持此条件。

有关详细信息，请参阅策略和操作。

已删除多个基于策略的操作

配置策略时，您不能再应用多个操作。Citrix Analytics 对每个策略仅支持一个操作。

有关详细信息，请参阅策略和操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**”仪表板时遇到错误。

December 12, 2019

新增功能

Splunk 版本支持

Citrix Analytics 支持以下 Splunk 版本：

- **Splunk 8.0 六十四位**
- **Splunk 7.3 六十四位**

为了获得 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。

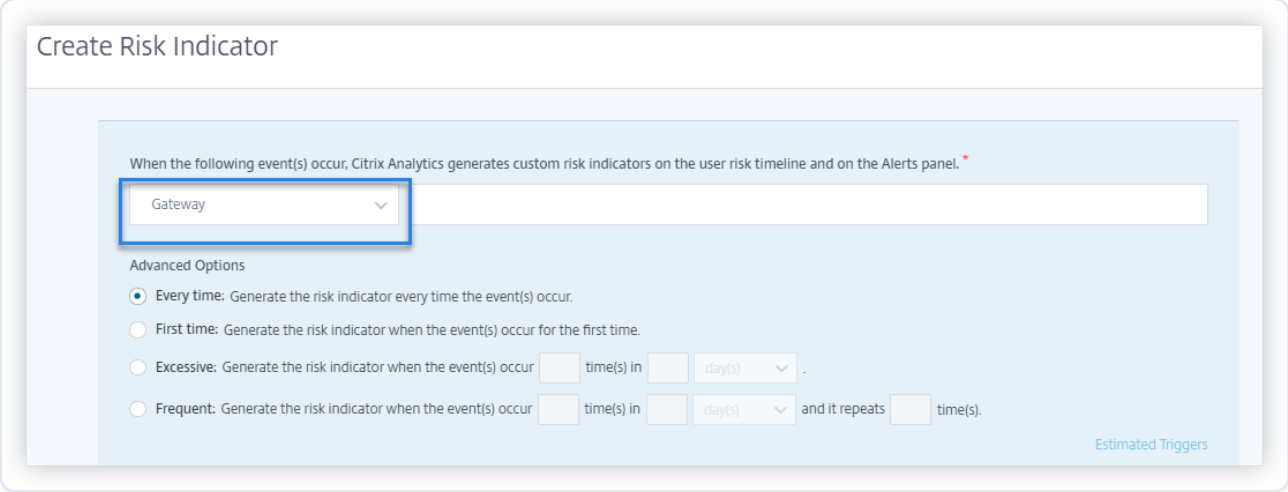
有关支持的 Splunk 版本的更多信息，请参阅 (/zh-cn/security-analytics/siem-integration/splunk-integration.html#supported-versions)。

December 04, 2019

新增功能

Citrix Gateway 的自定义风险指标

现在，您可以使用自定义风险指标来定义触发 Citrix Gateway 事件风险指标的条件和频率。当用户事件满足条件时，Analytics 会触发风险指标。有关如何创建自定义风险指标的更多信息，请参阅 (/zh-cn/security-analytics/custom-risk-indicators.html)。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

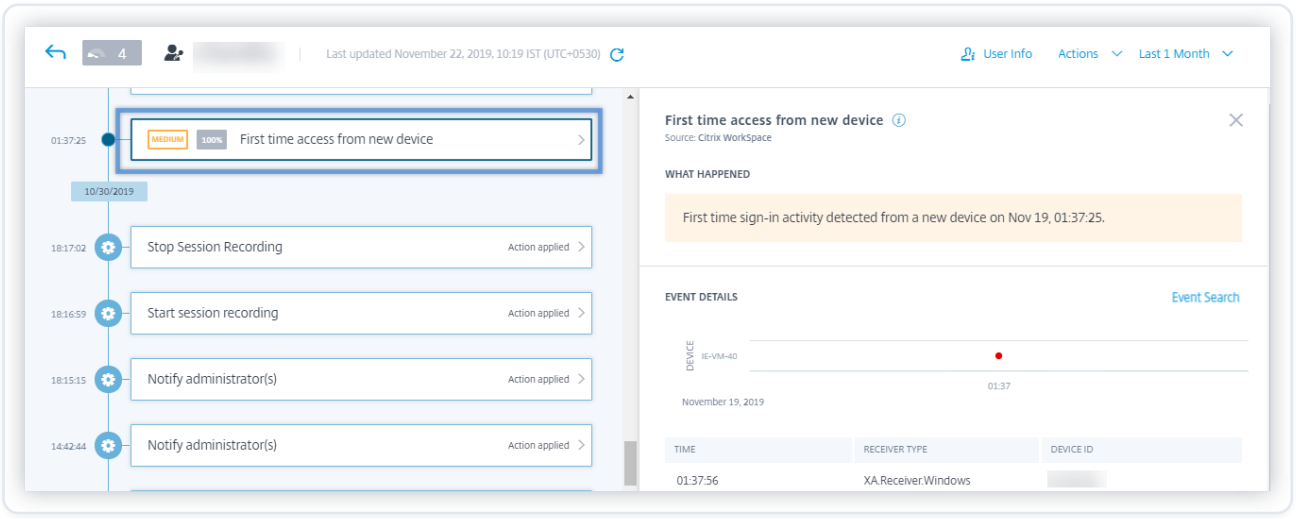
November 22, 2019

新增功能

首次从新设备访问 – Citrix Virtual Apps and Desktops 风险指标

Citrix Analytics 根据从新设备进行的访问检测访问威胁，并触发相应的风险指标。

当用户在 90 天后从设备登录时，将触发**首次从新设备访问**风险指标。触发此事件是因为 Citrix Receiver 在过去 90 天内没有来自此新设备或不熟悉设备的登录记录。有关更多信息，请参阅Citrix Virtual Apps and Desktops 和 Citrix DaaS 风险指标。



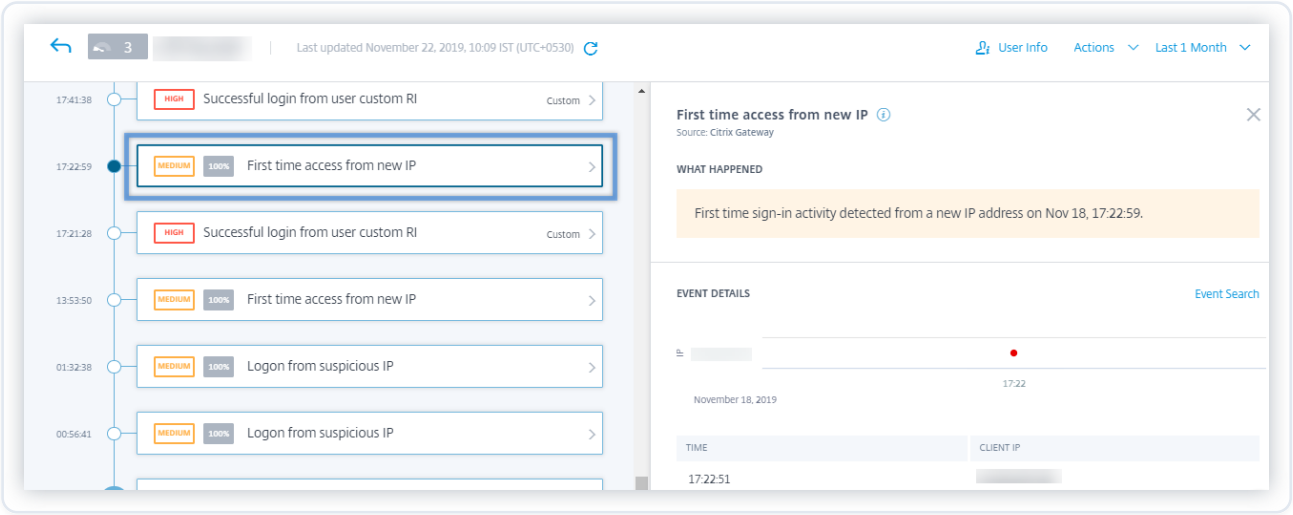
首次从新 IP 访问 - Citrix Gateway 风险指标

Citrix Analytics 根据从新 IP 地址进行的访问检测访问威胁，并触发相应的风险指标。

当用户在 90 天后从 IP 地址登录时，将触发**首次从新 IP 访问**风险指标。触发此事件是因为 Citrix Receiver 在过去 90 天内没有来自此新 IP 地址或不熟悉 IP 地址的登录记录。

有关更多信息，请参阅Citrix Gateway 风险指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



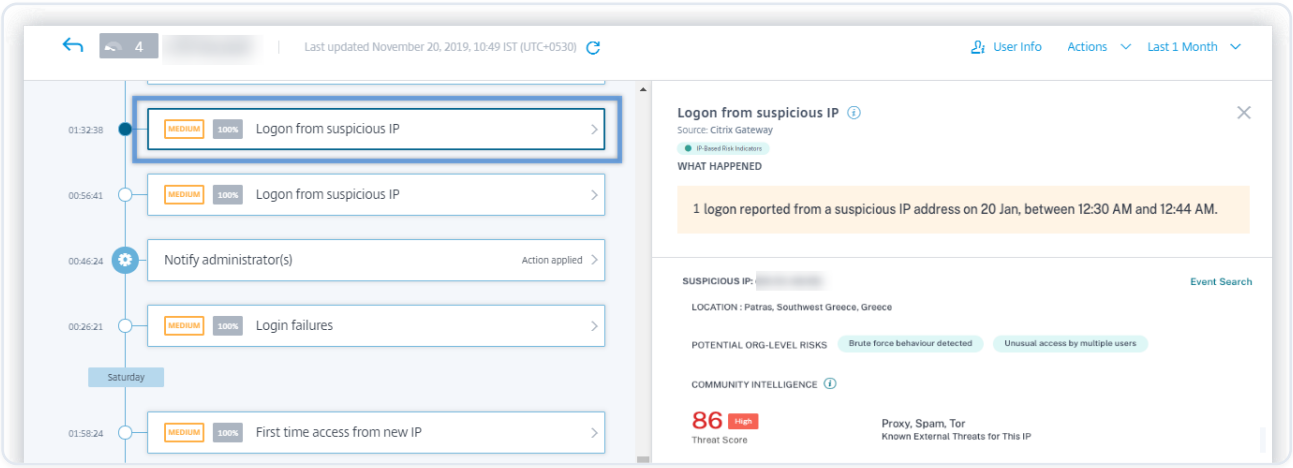
从可疑 IP 登录 - Citrix Gateway 风险指标

Citrix Analytics 根据可疑 IP 登录活动检测用户访问威胁，并触发**从可疑 IP 登录**风险指标。

当用户尝试从可疑 IP 地址访问网络时，将触发此风险指标。Analytics 根据以下任何条件将 IP 地址视为可疑：

- 列在外部 IP 威胁情报源中
- 具有来自异常位置的多个用户登录记录
- 具有过多的登录失败尝试，这可能表明存在暴力攻击

有关详细信息，请参阅 Citrix Gateway 风险指标。



Citrix Gateway 事件的自助搜索

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 用户的事件，例如身份验证阶段、授权类型、VPN 会话代码、VPN 会话状态。使用分面和搜索框搜索所需事件并探索基础数据。

要查看事件，请在搜索框中从列表中选择 **Gateway**，选择时间段，然后单击 **Search**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关详细信息，请参阅 Gateway 的自助搜索。

Citrix Remote Browser Isolation™ 事件的自助搜索

使用自助搜索功能深入了解从 Citrix Remote Browser Isolation Service 接收的浏览事件。Citrix Analytics 接收每个用户连接的事件，例如会话连接、会话启动、已发布的应用程序、已删除的应用程序。使用搜索框搜索所需事件并探索基础数据。

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 **Search**。

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

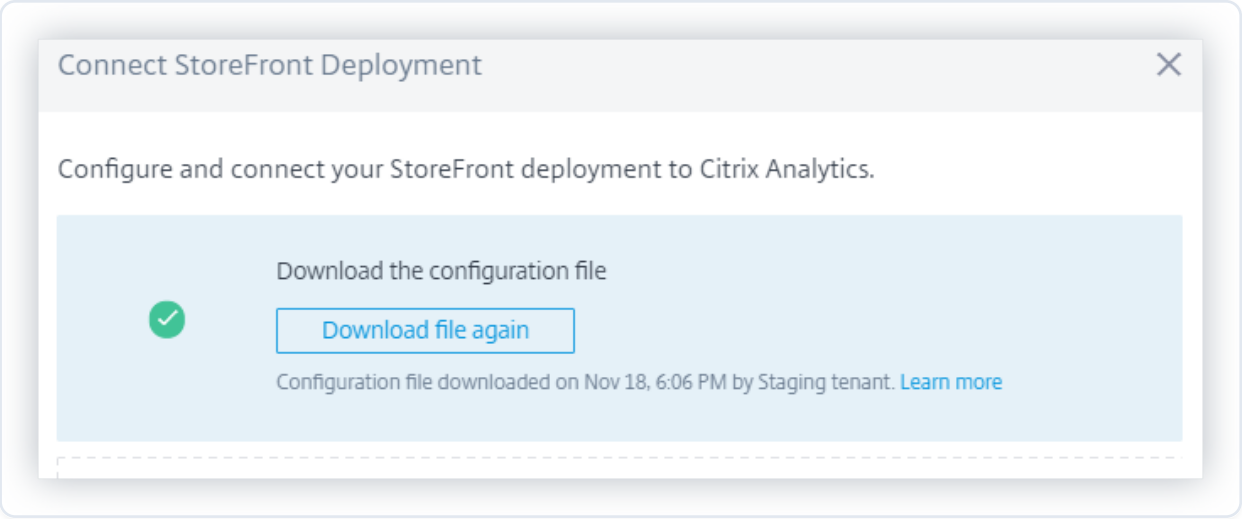
从监视列表中删除操作

您可以通过手动方法或基于策略的方法将用户从监视列表中删除。有关详细信息，请参阅 监视列表。

配置 StoreFront 部署时改进的入门消息

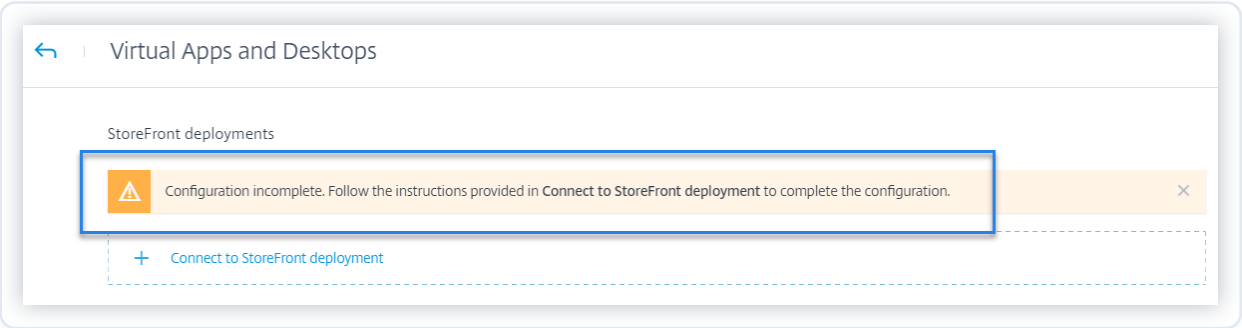
Citrix Analytics 现在提供以下消息，以帮助您配置 StoreFront 部署：

- 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，**Download file** 按钮会更改为 **Download file again**。



- 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您的 StoreFront 部署与 Analytics 连接。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关如何配置 StoreFront 部署的更多信息，请参阅 使用 StoreFront 载入 Citrix Virtual Apps and Desktops 本地站点。

已弃用的功能

风险指示器 - 从新设备访问已移除

Citrix Analytics 不再触发**从新设备访问**风险指示器。但是，在用户仪表板、用户时间线和策略仪表板上，您可以查看与此风险指示器相关的历史数据。

对于以前基于**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**首次从新设备访问**创建策略。

已修复的问题

- 身份验证的自助搜索无法显示事件。

November 08, 2019

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线上应用操作。
- 版本 1911 之前的适用于 Chrome 的 Citrix Workspace 应用程序无法将事件详细信息发送到 Citrix Analytics。

October 21, 2019

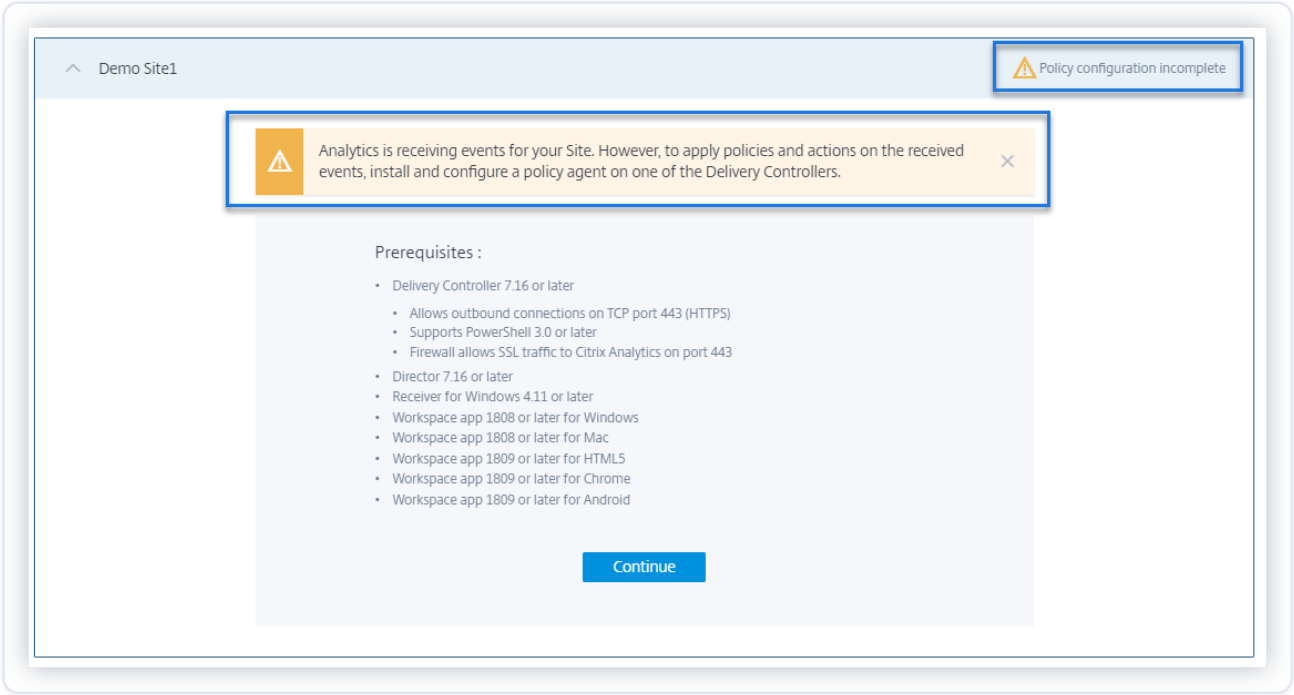
新增功能

分析代理的名称已修改

代理名称现在在用户界面上显示为**分析策略代理**，以表明其角色。在载入本地 Citrix Virtual Apps and Desktops 数据源时，Citrix Analytics 会明确通知，策略代理仅用于为您的站点配置策略和操

© 1997–2026 Citrix Systems, Inc. All rights reserved.

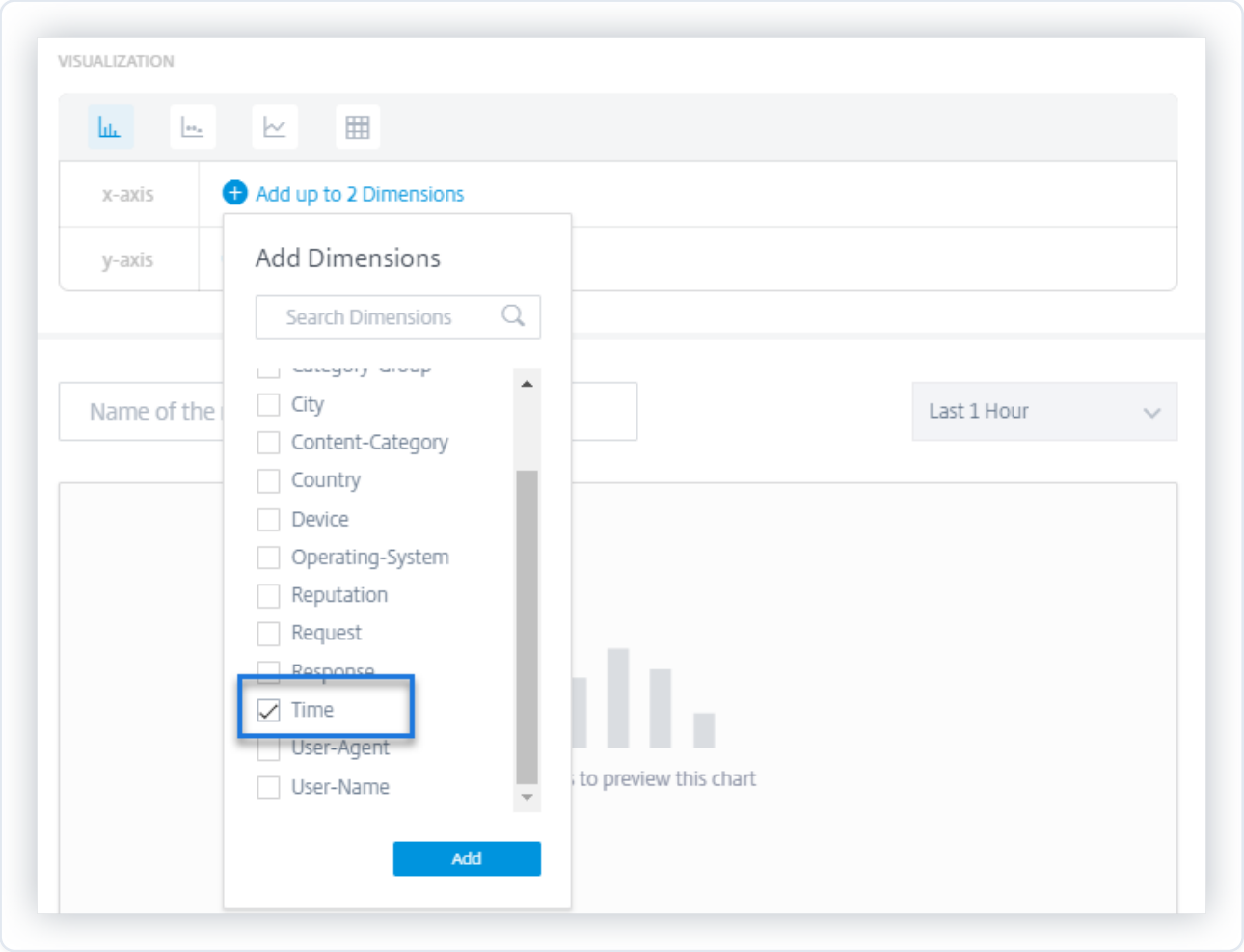
作。此代理在从数据源传输数据方面没有作用。有关详细信息，请参阅Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源。



自定义报告支持时间维度

您现在可以通过为 x 轴选择**时间**维度来根据时间对事件进行分组。报告会根据所选时间段的时间间隔显示收到的事件总数。有关如何创建报告的详细信息，请参阅自定义报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

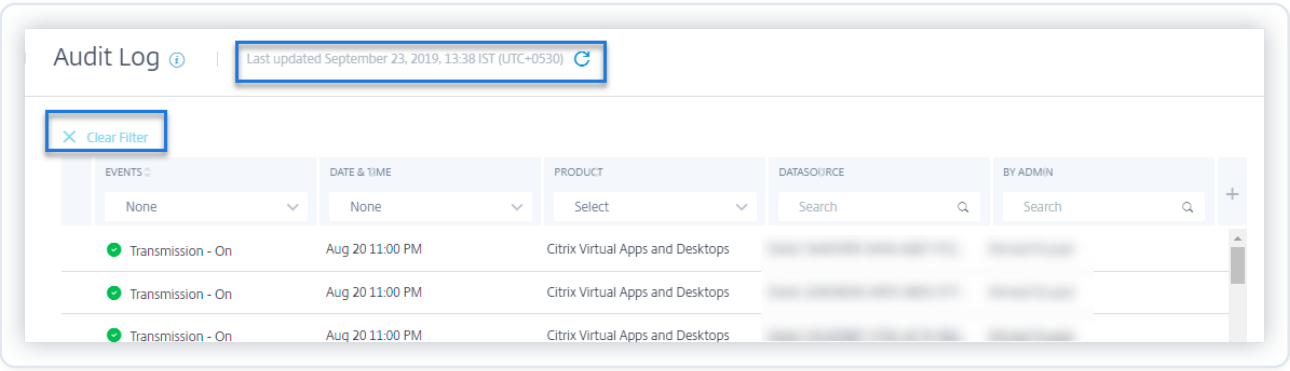


审核日志增强功能

审核日志页面的用户体验已得到增强。

- 您可以查看**审核日志**页面上次更新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。
- 您可以清除应用于审核日志的所有筛选器。

有关审核数据的详细信息，请参阅审核日志。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复的问题

- 即使 Microsoft Graph Security 已成功载入，Citrix Analytics 也无法生成**匿名 IP 地址**风险指示器。
- Citrix Workspace app for HTML5 版本 1910 之前无法将事件详细信息发送到 Citrix Analytics。

September 23, 2019

已修复的问题

- 在数据源站点卡片上，**最新事件**字段显示不正确的日期和时间信息。

August 30, 2019

新增功能

仪表板默认时间段的更改

以下仪表板的默认时间段已从**最近 1 小时**更改为**最近 1 个月**：

- 用户
- 风险时间线
- 用户访问
- 应用程序访问
- 共享链接
- 警报历史记录

现在，仪表板默认显示过去一个月的事件。使用这些仪表板时，您将获得更具吸引力的体验。例如，当您打开**应用程序访问**仪表板时，仪表板默认显示过去一个月的应用程序访问事件。

默认时间段选择(/en-us/citrix-analytics/media/default-time-change.png)

已修复问题

- 对于内容协作风险指示器，基于策略的**禁用用户**操作无法成功应用。
- 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 未能在发送到 Citrix Analytics 的登录事件中提供用户名。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

August 20, 2019

新增功能

自助搜索增强功能

- 自助服务页面的用户体验得到增强。您现在可以在用户风险时间线和自助服务搜索页面之间无缝切换。
- 您现在可以按时间对事件进行排序。默认情况下，最新事件显示在事件表中的最前面。单击**时间**列上的排序图标，可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更多信息，请参阅自助搜索。

自定义报告增强功能

- 为访问控制、内容协作以及应用程序和桌面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
  - **内容协作**：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已增强，支持分页和筛选器的“**全部清除**”选项。

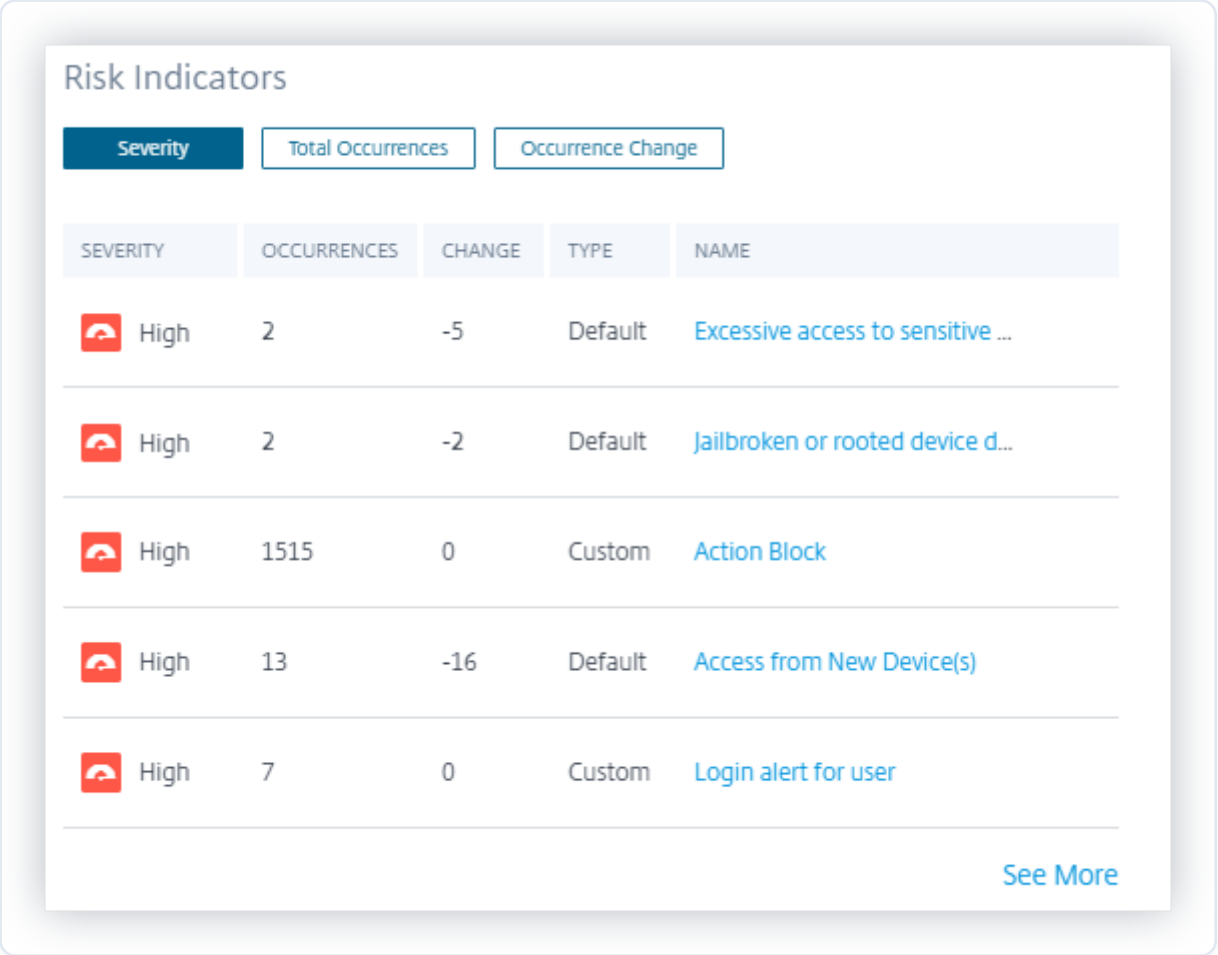
有关如何使用这些维度创建自定义报告的更多信息，请参阅自定义报告。

风险指标控制板

“**风险指标**”控制板已在“**用户**”页面上推出。它总结了用户的五大默认和自定义风险指标。“查看更多”链接会将您重定向到“**风险指标概述**”页面。此页面提供有关所选时间段内生成的风险指标的详细信息。

有关详细信息，请参阅用户控制板。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



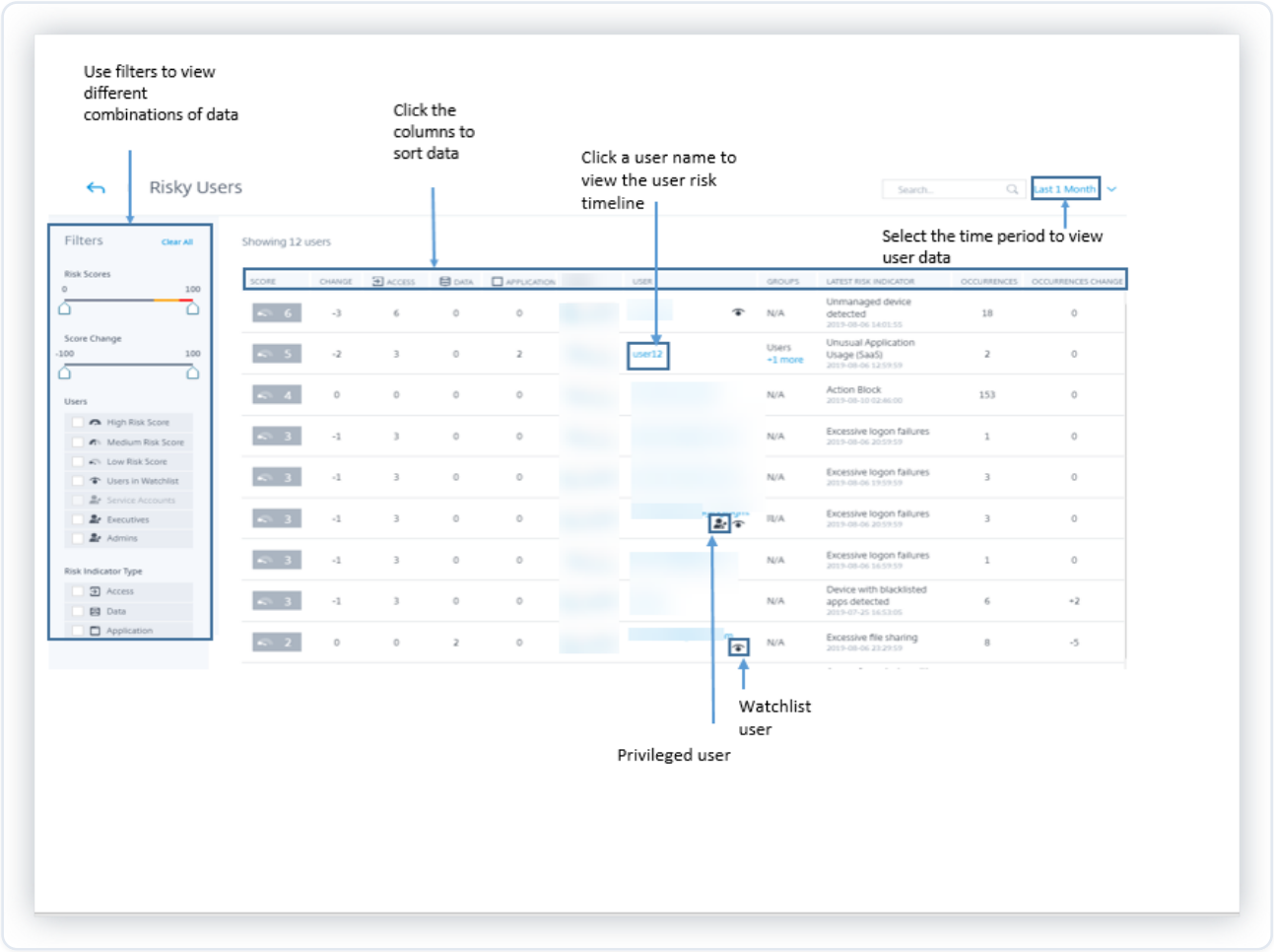
风险用户控制板增强功能

Citrix Analytics 在“**风险用户**”控制板上引入了“**风险指标**”和“**风险指标更改**”选项卡。您可以根据这些选项卡查看前五名风险用户。控制板还引入了“**风险指标**”列。它显示了用户的风险指标数量。

“**风险用户**”页面引入了“**发生次数**”和“**发生次数更改**”列。这些列汇总了自定义和默认风险指标的总发生次数以及发生次数的变化。

有关详细信息，请参阅用户控制板。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



共享链接风险指标 - 过度下载

Citrix Analytics 根据共享链接上的过度下载检测访问威胁，并触发“**过度下载**”风险指标。通过根据以前的行为识别过度下载的共享链接，您可以监控共享链接是否存在潜在攻击。此风险指标可帮助您识别过多的文件下载活动。

有关详细信息，请参阅过度下载。

身份验证数据的自助搜索

使用自助搜索获取有关身份验证事件的见解。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。该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您定义条件的事件。

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，请参阅身份验证的自助搜索。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

July 11, 2019

新增功能

自定义风险指标

Citrix Analytics 生成的默认风险指标基于机器学习算法。Citrix Analytics 现在允许您创建自定义风险指标。您可以根据用户事件定义条件并创建自定义风险指标。

当满足定义的条件时，Citrix Analytics 会生成类似于默认风险指标的自定义风险指标，并将其显示在用户的风险时间轴上。自定义风险指标在用户的风险时间轴上用标签表示。

有关详细信息，请参阅自定义风险指标。

风险时间轴上的特权状态

当用户的管理员或执行特权状态发生变化时，用户风险时间轴会显示以下事件：

- 已添加到执行组
- 已从执行组中移除
- 特权已提升为管理员
- 管理员特权已移除

当用户的风险指示器被触发时，您可以将其与指定的特权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线。

共享链接过期操作

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**共享链接过期**。

有关详细信息，请参阅 Citrix 共享链接风险指示器。

自助搜索增强功能

- **搜索查询中支持通配符 * **：在搜索查询中使用星号 (*\) 字符可匹配任意字符零次或多次。例如，搜索查询 User-Name = "John*" 会显示以 John 开头的所有用户名的事件。
- **为构面添加了“全部清除”选项**：单击**全部清除**可一次性删除所有选定的构面。
- **在事件列表中查看隐藏的列数据**：从事件表中删除列后，您可以在用户事件列表中查看相应数据。展开用户的事件行并查看数据。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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到事件时，站点卡会以红色显示**未收到数据**标签。它还会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，自助搜索仅适用于访问、内容协作以及应用程序和桌面数据源。

有关详细信息，请参阅在 Citrix 数据源上启用 Analytics。

已修复问题

- 对于访问控制数据源，站点卡上的事件数量与自助服务搜索结果不匹配。

June 19, 2019

已修复问题

- **审核日志**页面在每次发现 Active Directory 数据源时显示数据传输的开启或关闭状态。
- **用户**仪表板上的时间段菜单加载不准确。它显示超时错误消息。
- 用户在从 Splunk 连接到租户时，在 Citrix Analytics 上收到错误消息。偶尔，新数据源的载入会失败。

June 17, 2019

新功能

StoreFront 配置

如果您的组织使用本地 StoreFront，您现在可以配置 StoreFront 以连接到 Citrix Analytics。配置是使用从 Citrix Analytics 导入的配置文件执行的。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用户行为并主动处理组织中的安全威胁。有关更多信息，请参阅使用 StoreFront 载入本地 Citrix Virtual Apps and Desktops 站点。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

May 30, 2019

新功能

登录失败次数过多

Citrix Analytics 根据过多的登录活动检测访问威胁，并触发“登录失败次数过多”风险指标。当用户多次尝试登录 Content Collaboration 失败时，会触发此风险指标。通过根据以前的行为识别登录失败次数过多的用户，管理员可以监控用户的帐户是否存在暴力攻击。

注意

登录失败次数过多 现已更名为 **身份验证失败次数过多**。

已修复问题

- 对于 Citrix Workspace 应用程序传输的某些用户事件，数据源被错误地识别为 Endpoint Management 而不是 Citrix Virtual Apps and Desktops。
- **用户**控制板在“**最近 1 个月**”时间段内加载时间过长。当用户数量较多时，会出现此问题。在某些情况下，您甚至可能会遇到 601 错误。
- Citrix Content Collaboration 未被发现为数据源，尽管有些用户在 Citrix Cloud 上订阅了该服务。

May 09, 2019

新增功能

创建自定义报告

您现在可以根据您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标列表。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）来创建报告。创建报告有助于您以图形方式组织和分析数据。

要创建自定义报告，请在“**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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

特权用户监控

Citrix Analytics 使您能够密切监控组织中特权用户的行为异常。由于特权用户极易受到安全威胁，因此很难区分他们的日常活动和恶意活动。因此，特权用户的恶意活动长期以来一直未被发现。此功能使您能够主动监控此类活动，并对相应的用户帐户采取适当措施。特权用户在“**用户**”仪表板上以图标表示。

Citrix Analytics 支持监控以下类型的特权用户：

- **管理员** - 由相应的 Citrix 服务分配管理员权限的用户。目前，Citrix Analytics 支持监控在内容协作服务中具有管理员权限的特权用户。
- **高管** - 在 Citrix Analytics 上，您可以将 AD 组标记为高管组。将 AD 组标记为高管组会使该组中的所有用户都成为特权用户。如果不再需要支持 AD 组中用户的行为异常，您可以将该组从高管组中移除。

有关详细信息，请参阅特权用户。

每周电子邮件摘要

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，其中突出显示了前一周发生的安全事件。此电子邮件可确保管理员无需登录 Citrix Analytics 即可了解安全风险暴露。有关详细信息，请参阅每周电子邮件摘要。

April 26, 2019

新增功能

委派管理员

Citrix Analytics 现在支持委派管理员角色。此功能使您能够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您的 Citrix Cloud 帐户。这些额外的管理员称为委派管理员。您目前可以为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

使用数据流的数据源的少数风险指示器不会生成警报。如果触发以下任何风险指示器，您将不会收到任何警报通知，并且不会自动应用基于策略的操作：

- **Citrix Endpoint Management 风险指示器** - 未受管设备、越狱或已 root 设备以及具有黑名单应用程序的设备。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Citrix Virtual Apps and Desktops 风险指示器** - 从具有不受支持的操作系统 (OS) 的设备进行访问。
- **Citrix Content Collaboration 风险指示器** - 过度访问敏感文件。

February 19, 2019

新增功能

Splunk 集成

Citrix Analytics 与 Splunk 集成，以增强您的安全事件监控和故障排除体验。此集成利用 Citrix Analytics for Security 的风险分析功能和智能（例如风险指示器、风险评分和用户配置文件）来增强您现有的数据源。Citrix Analytics 将风险分析信息导出到通道。Splunk 从此通道中提取相同的信息。

Splunk 集成涉及 Citrix Analytics 上的配置、**Citrix Analytics Add-on for Splunk** 应用程序的安装以及应用程序的配置。请确保为至少一个数据源开启数据处理。这有助于 Citrix Analytics 启动 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。这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，例如断开会话和阻止用户。

有关详细信息，请参阅 策略和操作。

共享链接仪表板和风险指示器

Citrix Analytics 根据从 Citrix Content Collaboration 收集的数据，为共享链接引入了风险可见性。这有助于您通过共享链接触发的风险指示器来了解共享链接的风险暴露。

有关详细信息，请参阅共享链接仪表板。

目前，共享链接会触发匿名敏感共享下载风险指示器。当 Content Collaboration 检测到此风险行为时，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线中。

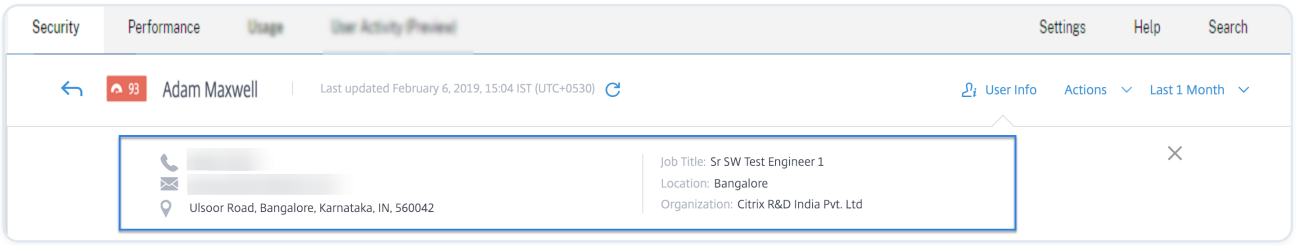
有关详细信息，请参阅 Share Link 风险时间线和 Citrix Share Link 风险指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

微软 Active Directory 集成

您现在可以将 Microsoft Active Directory 与 Citrix Analytics 集成。此集成通过职位、组织、办公地点、电子邮件和联系方式等附加信息增强了风险用户的上下文。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 Analytics 与 Microsoft Active Directory 集成。



January 04, 2019

新增功能

为现有风险指标添加 SOURCE 列

已在以下风险指标的 **EVENT DETAILS** 部分中引入 **SOURCE** 列：

- 文件上传过多
- 文件下载过多
- 文件共享过多
- 文件或文件夹删除过多

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

高级用户配置文件

用户配置文件上的“**用户信息**”视图已得到增强。“**趋势视图**”链接已引入到“**应用程序**”、“**设备**”和“**数据使用情况**”部分的右上角。“**地图视图**”链接已引入到“**位置**”部分的右上角。这些链接提供了用户在特定时间段内的历史行为的图形表示。您可以从用户的风险时间线或“**数据源**”页面导航到“**用户信息**”。

注意

目前，“**身份验证**”和“**域**”数据在“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线和配置文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Microsoft Graph Security 风险指标

已载入的 Microsoft Graph Security 可以从以下安全提供程序之一接收风险指标详细信息，并将其转发到 Citrix Analytics：

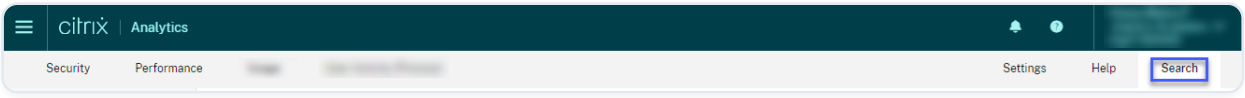
- Azure AD 身份保护
- 适用于终结点的 Microsoft Defender

有关详细信息，请参阅Microsoft Graph Security 风险指标。

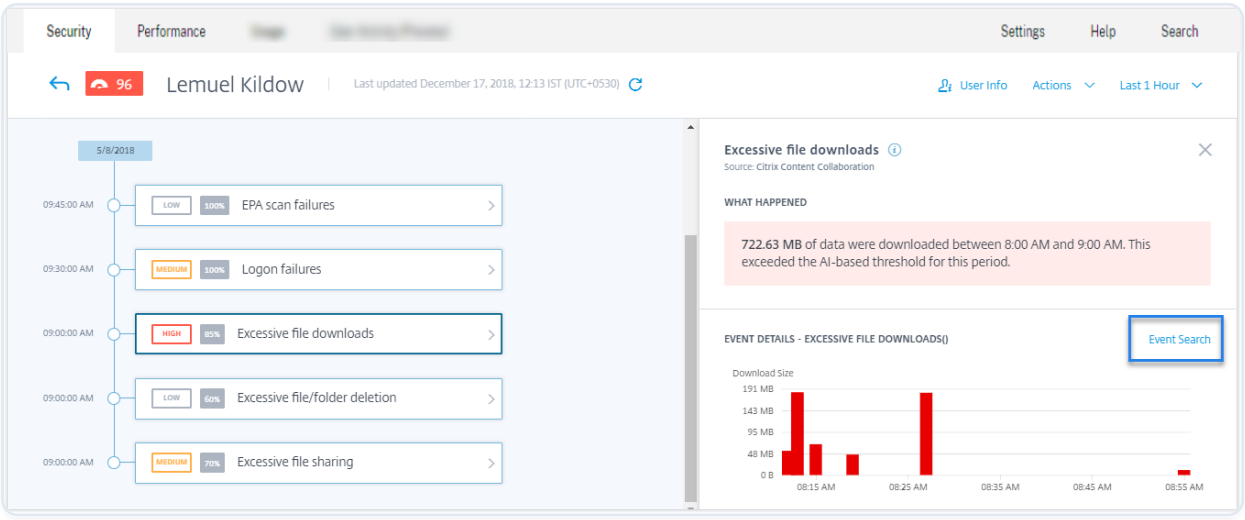
进入自助搜索页面的方法

您现在可以使用以下选项访问自助搜索页面：

- **顶部栏**：单击顶部栏上的“**搜索**”以直接访问搜索页面。



- **用户配置文件页面上的风险时间线**：单击“**事件搜索**”以访问搜索页面并查看与特定用户的风险指标和数据源相对应的事件。有关详细信息，请参阅自助搜索。



内容协作的自助搜索

使用自助搜索深入了解与内容协作数据源相关的事件。要查看事件，请从列表中选择“**内容协作**”，选择时间段，然后单击“**搜索**”。 有关详细信息，请参阅内容协作的自助搜索。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

应用程序和桌面的自助搜索

使用自助搜索深入了解与应用程序和桌面数据源相关的事件。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搜索。

将自助搜索事件导出到 CSV 文件

您现在可以将自助搜索事件导出到 CSV 文件并下载该文件以供将来使用。有关详细信息，请参阅自助搜索。

改进了 Citrix Virtual Apps and Desktops 的入门体验

Citrix Virtual Apps and Desktops 数据源的入门过程现已改进，以提供更好的用户体验。站点卡和入门步骤已修改。有关详细信息，请参阅Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源。

November 29, 2018

新增功能

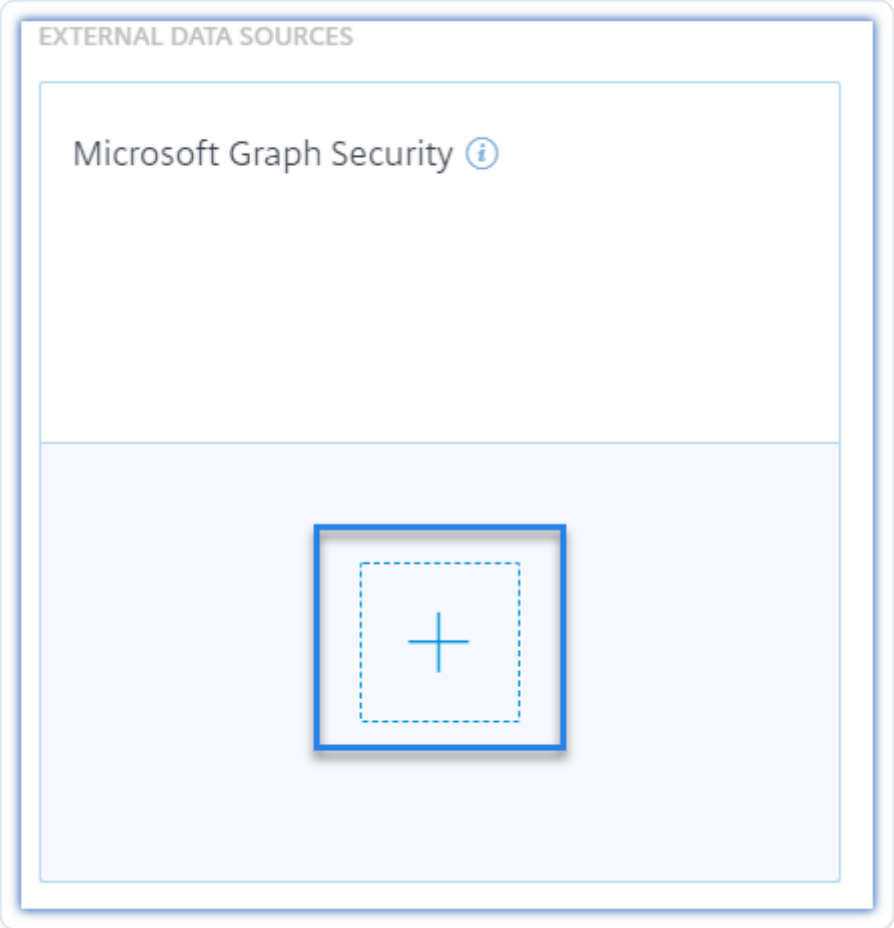
微软安全图谱数据源

Microsoft Graph Security 是一个外部数据源，它聚合来自多个安全提供程序的数据。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 identity protection** 和 **Microsoft Defender for Endpoint** 安全提供程序。

要载入此数据源，您必须从 Microsoft 身份平台获取权限。有关详细信息，请参阅Microsoft Graph Security。

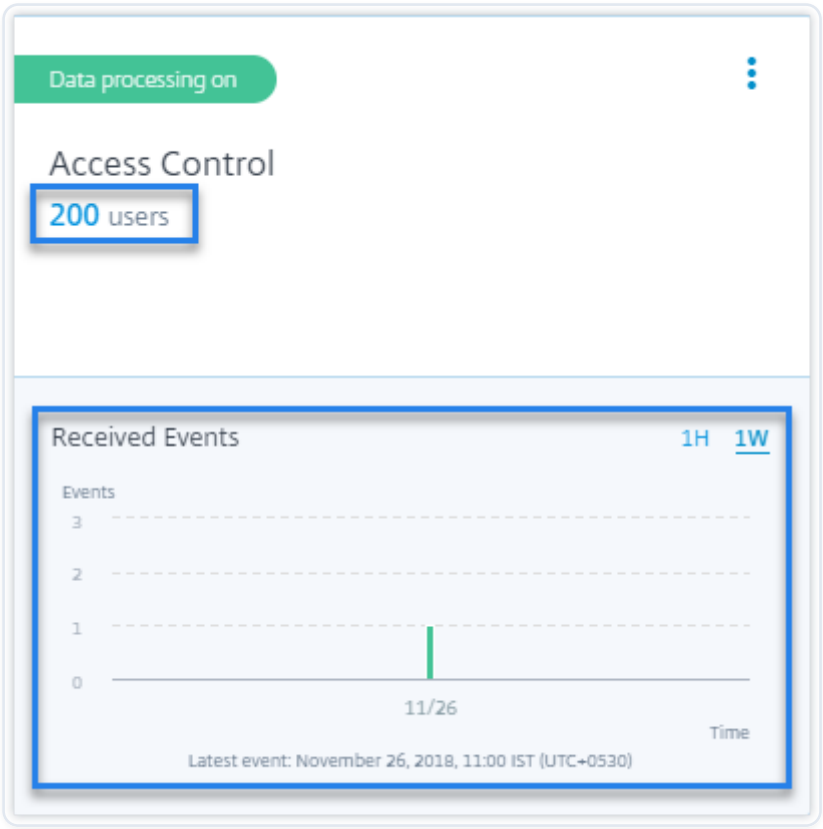
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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访问控制的事件详细信息和用户。有关详细信息，请参阅“在数据源上启用分析”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



November 16, 2018

新功能

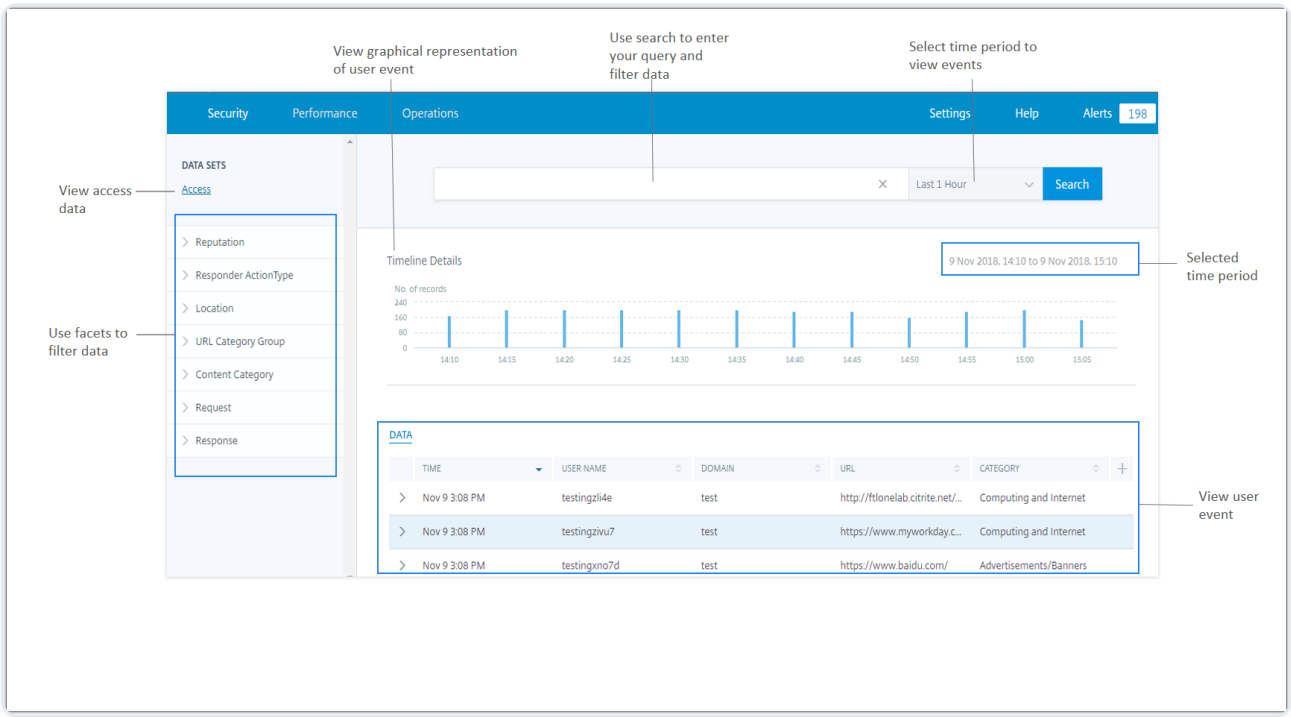
访问数据的自助搜索

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 Access Control 服务收集用户的访问详细信息。使用分面和搜索查询来缩小搜索结果范围。

要使用自助搜索页面，请从“**安全**”选项卡中单击“**事件搜索**”。

有关详细信息，请参阅访问的自助搜索。

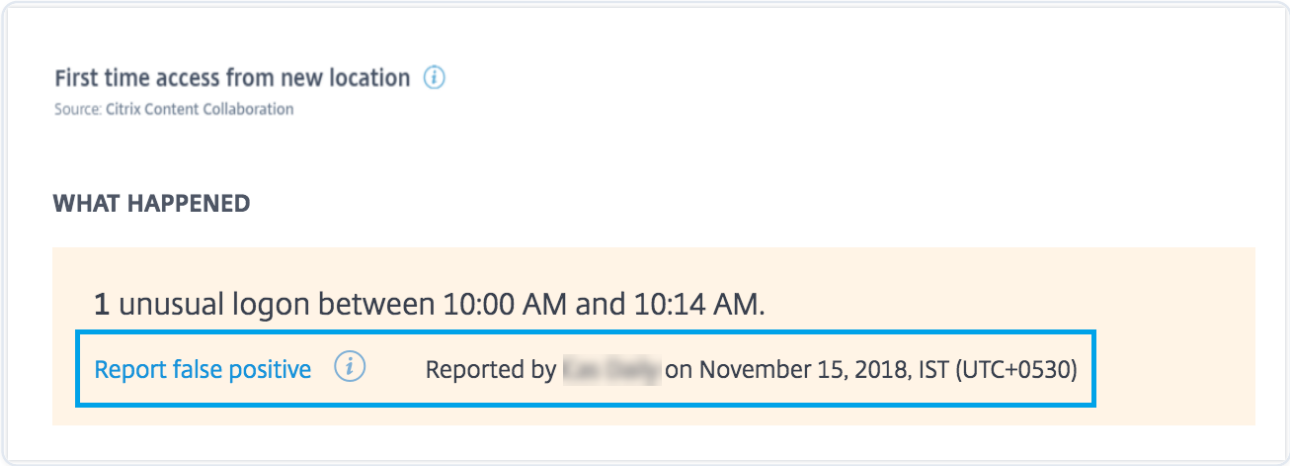
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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，此功能支持由内容协作数据源触发的“**异常登录访问**”风险指示器。如果此风险指示器触发不正确，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 会捕获您的反馈并验证预测信息，以优化异常行为检测。



已修复问题

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已知问题

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

- 当通过 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，Citrix Workspace™ app for Linux 无法将打印事件发送到 Citrix Analytics。

  注意

  有关所有平台上 Citrix Workspace 应用程序和 Citrix Receiver 的生命周期日期和生命周期阶段（全面上市、维护终止和生命周期终止）的更多信息，请参阅 Citrix Workspace 应用程序和 Citrix Receiver 的生命周期里程碑。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

分析产品

© 1997–2026 Citrix Systems, Inc. All rights reserved.

数据源

数据源是向 Citrix Analytics 发送数据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。有关详细信息，请参阅入门。

数据源	部署类型	所需代理	产品组件和版本
Citrix 端点管理	服务	不适用	Citrix 端点管理
网关	本地部署	应用交付管理代理	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 安全私有访问	服务	（不适用）不适用	Citrix 安全私有访问
Citrix 远程浏览器隔离	服务	不适用	Citrix 远程浏览器隔离
Citrix DaaS（以前称为 Virtual Apps and Desktops 服务）	服务	不适用	Citrix Workspace 应用程序：适用于 Windows 1907 或更高版本；适用于 Mac 1910.2 或更高版本；适用于 HTML5 2007 或更高版本；适用于 Chrome（Chrome 网上应用店中提供的最新版本）；适用于 Android（Google Play 中提供的最新版本）；适用于 iOS（Apple App Store 中提供的最新版

© 1997–2026 Citrix Systems, Inc. All rights reserved.

数据源	部署类型	所需代理	产品组件和版本
			本）；适用于 Linux 2006 或更高版本。
Citrix 虚拟应用和桌面	本地部署	虚拟应用和桌面代理	Citrix 虚拟应用和桌面 7 1808、Citrix XenApp 和 XenDesktop 7.16 或更高版本
		代理是高级功能（例如“操作”）所必需的。	Citrix Workspace 应用程序：适用于 Windows 1907 或更高版本；适用于 Mac 1910.2 或更高版本；适用于 HTML5 2007 或更高版本；适用于 Chrome（Chrome 网上应用店中提供的最新版本）；适用于 Android（Google Play 中提供的最新版本）；适用于 iOS（Apple App Store 中提供的最新版本）；适用于 Linux 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本地部署的 Virtual Apps and Desktops 站点添加到 Workspace。
			对于 StoreFront 用户：StoreFront 部署版本必须是 StoreFront 1906 或更高版本。必须使用

© 1997–2026 Citrix Systems, Inc. All rights reserved.

数据源	部署类型	所需代理	产品组件和版本
			以下客户端之一访问 StoreFront：HTML5 兼容浏览器中的 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，支持的 StoreFront 版本是 1912。

注意

请参阅 Citrix Cloud services 以了解 Citrix 产品及其订阅。

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	所需代理
微软图形安全	服务	不适用
微软活动目录	本地部署	思杰云连接器™

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持的区域

Citrix Analytics for Security 支持以下区域：

- 美国 (US)
- 欧盟 (EU)
- 亚太南部 (APS)

根据您组织的位置，您可以在其中一个主区域中加入 Citrix Cloud™。

如果您的组织已加入 Citrix Cloud，但在不支持数据源的主区域中，您将无法从该数据源获取用户事件。

使用下表查看数据源及其支持的区域。

数据源	在美国区域受支持	在欧盟区域受支持	在亚太南区域受支持
Citrix 端点管理™	是	是	是
Citrix 网关（本地）	是	是	是
Citrix 身份提供商	是	是	是
Citrix 安全私有访问™	是	是	是
Citrix 远程浏览器隔离™	是	是	是
Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）	是	是	是
Citrix 虚拟应用和桌面 本地部署	是	是	是
微软活动目录	是	是	是
微软图形安全	是	是	是

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace 应用程序版本矩阵

本节显示了 Citrix Workspace 应用程序支持的版本，这些版本发送所有遥测数据并包含所有必需的关键错误修复。

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
视窗	CU3 之后的所有 LTSR 2203 版本
	23.0.3.0 或更高版本
HTML5	21.5.0.0 或更高版本
麦金塔	21.0.4.0 或更高版本
林纳克斯	21.4.0.0 或更高版本
谷歌浏览器	21.5.0.0 或更高版本
iOS	21.4.0.0 或更高版本
安卓	21.5.0.0 或更高版本

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

事件属性	关联功能	视窗	MAC	琳纳克斯	HTML 5	谷歌浏览器	IOS	安卓
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 中提供的最新版本
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	Apple App Store 中提供	Google Play 中提供

© 1997–2026 Citrix Systems, Inc. All rights reserved.

事件属性	关联功能	视窗	MAC	琳纳克斯	HTML 5	谷歌浏览器	IOS	安卓
						的最新版本	的最新版本	的最新版本
操作系统名称、操作系统版本、操作系统附加信息	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 中提供的最新版本
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 中提供的最新版本
Web 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 中提供的最新版本

© 1997–2026 Citrix Systems, Inc. All rights reserved.

数据治理

© 1997–2026 Citrix Systems, Inc. All rights reserved.

系统要求

在使用 Citrix Analytics for Security™ 之前，请查看以下要求。

Citrix 安全分析订阅

此 Analytics 产品是基于订阅的服务。您必须拥有有效的订阅才能使用 Security Analytics。有关更多信息，请参阅产品概述页面。

数据源要求

Citrix Analytics for Security 从各种数据源接收事件。为了使 Analytics 准确运行，您必须拥有有效订阅才能使用以下至少一种产品，这些产品可作为 Analytics 的数据源：

- Citrix ADC（本地部署） 以及 Citrix Application Delivery Management 的订阅
- Citrix 端点管理服务
- Citrix 网关（本地）
- Citrix 身份提供商
- Citrix 远程浏览器隔离
- 思杰安全私有访问服务
- 思杰虚拟应用和桌面或思杰 DaaS（以前称为思杰虚拟应用和桌面服务）
- 微软活动目录
- 微软图形安全

支持的浏览器

要访问 Analytics，您的工作站必须安装以下受支持的 Web 浏览器：

- 最新版 Google Chrome
- 最新版 Mozilla Firefox
- 最新版 Microsoft Edge
- 最新版 Apple Safari

© 1997–2026 Citrix Systems, Inc. All rights reserved.

管理 Security Analytics 的管理员角色

注意：

自 2023 年 7 月起，Microsoft 已将 Azure Active Directory (Azure AD) 重命名为 Microsoft Entra ID。本文档中提及的 Azure Active Directory、Azure AD 或 AAD 均指 Microsoft Entra ID。

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，并为其分配以下自定义角色之一：

- **Security Analytics - 完全管理员**
- **Security Analytics - 只读管理员**

您可以通过两种方式添加新管理员：作为单个用户或使用 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

如果用户作为单个用户直接获得访问权限，并通过 Azure Active Directory 组获得访问权限，则单独授予用户的访问权限生效。

自定义角色的权限

具有 **Security Analytics - 完全管理员** 角色的管理员可以访问 Security Analytics 产品的所有功能和特性。他们可以根据组织要求使用和修改这些功能。例如，完全管理员可以创建自定义风险指标、启用地理围栏和创建策略。

具有 **Security Analytics - 只读管理员** 角色的管理员只能访问和查看安全控制板：用户、用户访问、应用程序访问、访问保障和报告。他们可以在这些控制板上监控用户行为和查看用户事件。但是，他们不允许执行任何关键任务，例如：

- 开启或关闭数据源的数据处理
- 创建或删除策略和操作
- 手动对用户风险时间线上显示的风险指标应用操作
- 创建、修改或删除自定义风险指标

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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（完全访问和只读访问）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：

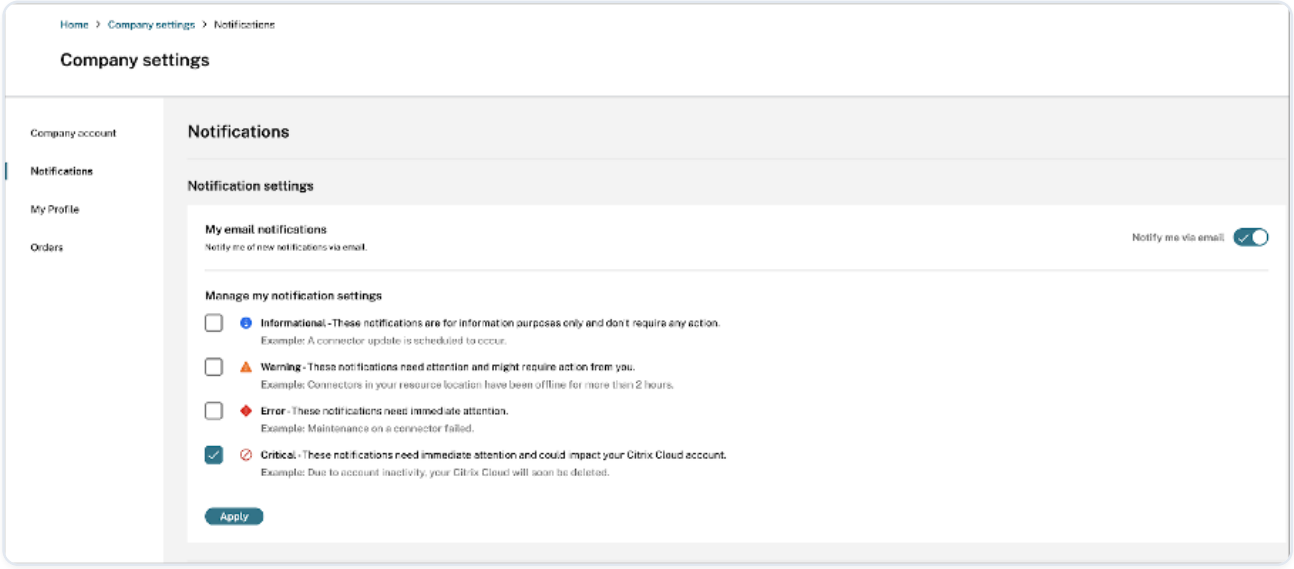
- 关于其组织中安全洞察的每周通知。有关详细信息，请参阅每周电子邮件通知。
- 基于“通知管理员”操作的通知。有关详细信息，请参阅策略和操作。

如果您是具有完全或自定义访问权限的 Citrix Cloud 管理员，则您的 Citrix Cloud 帐户中默认禁用电子邮件通知。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。通过 Active Directory/Azure AD 组添加的管理员无法使用通知首选项。

在发送通知时（例如每周电子邮件、“通知管理员”操作电子邮件以及数据导出警报），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 Security Analytics 完全访问权限的管理员必须将您从分发列表中删除。有关分发列表的详细信息，请参阅电子邮件分发列表。

注意

Citrix Cloud 管理员（具有完全或自定义访问权限）不会收到来自利用**通知首选项**的其他 Citrix Cloud 服务的任何通知。



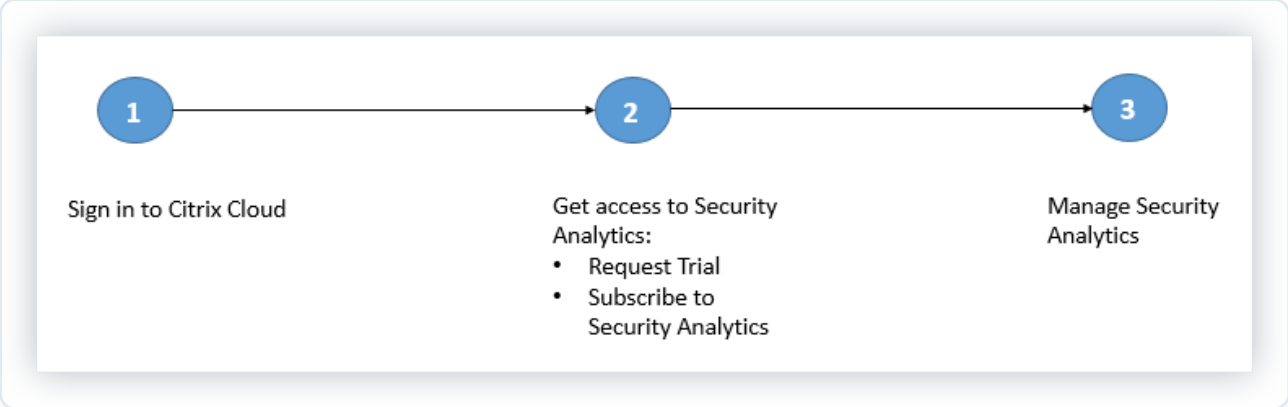
© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关详细信息，请参阅管理 Citrix Analytics 的管理员。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

开始使用

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



步骤 1：登录 Citrix Cloud™

要使用 Citrix Analytics for Security，您必须拥有一个 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，则必须首先创建一个 Citrix Cloud 帐户，或者加入组织中其他人创建的现有帐户。有关详细流程和操作说明，请参阅 注册 Citrix Cloud。

步骤 2：访问 Security Analytics

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

- **请求 Citrix Analytics for Security 试用版**。登录 Citrix Cloud 后，执行以下操作：
  a. 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。
  b. 在**安全**磁贴上，单击**请求试用**或直接联系您的 Citrix 客户经理或 Citrix 合作伙伴。
- **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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

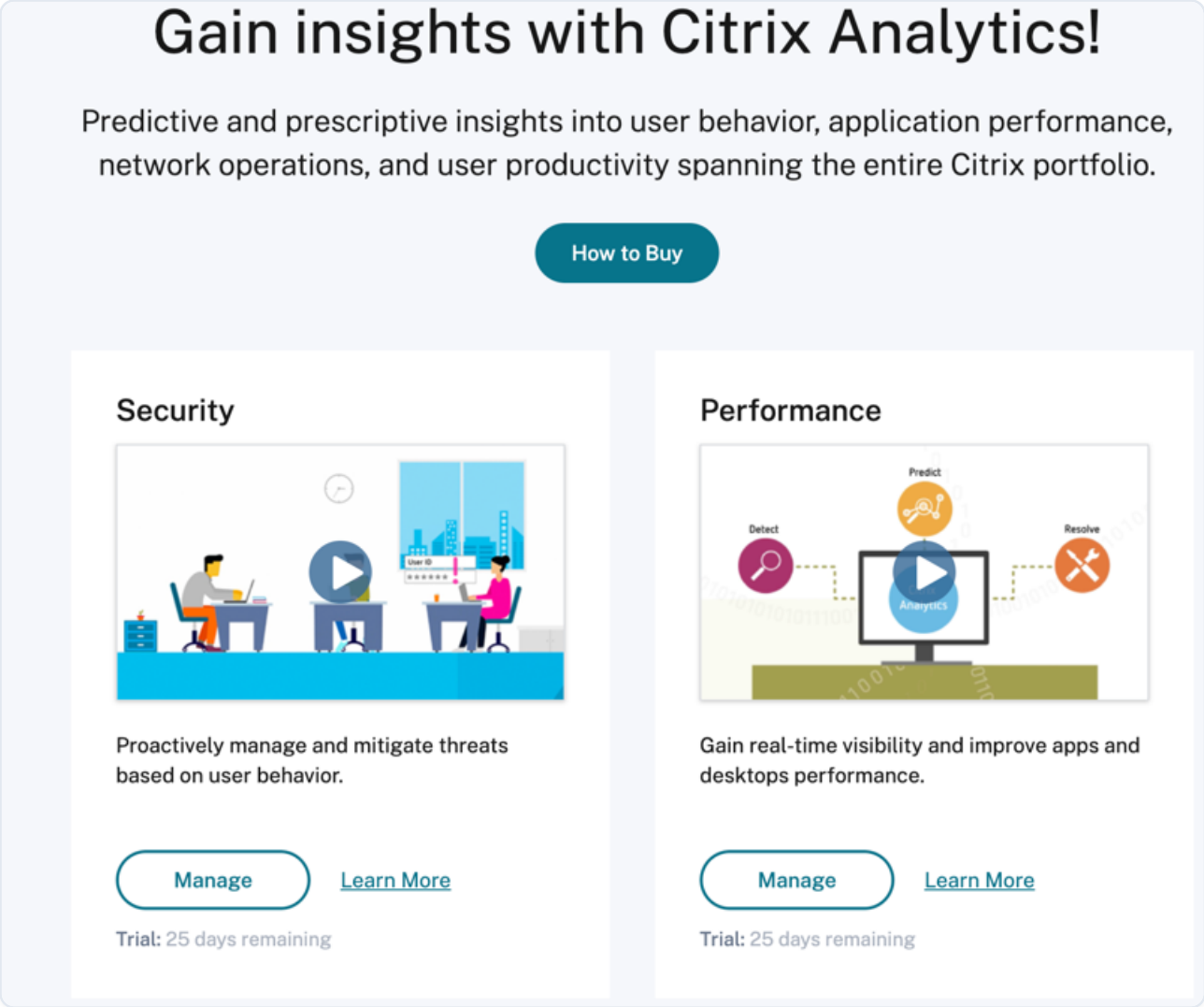
注意

- With effect from March 8, 2023, Citrix Analytics for Security 将不再作为 ShareFile/Citrix Content Collaboration 的独立产品提供购买。我们宣布 Citrix Analytics Service 独立附加组件（适用于 ShareFile/Citrix Content Collaboration）的销售终止 (EOS) 和续订终止 (EOR)。客户现有的 Citrix Analytics for Security 权益在其订阅到期前仍然有效。但是，Sharefile/Citrix Content Collaboration 集成将不再支持试用、续订和新购买。Citrix Analytics Service 与其他 Citrix 产品的集成将继续作为独立产品或捆绑产品提供，并与现有 Citrix DaaS 计划、Citrix Virtual Apps and Desktops 部署和 Citrix Workspace 部署一起提供。
- With effect from February 03, 2020, Citrix Analytics for Security 不再包含在 Workspace Premium 和 Workspace Premium Plus 订阅中。在 February 03, 2020 之前购买 Workspace Premium 或 Workspace Premium Plus 订阅的客户，可以在其订阅到期前，将 Citrix Analytics for Security 作为 Workspace 订阅的一部分进行访问。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。有关更多信息，请参阅 Citrix Cloud services。

步骤 3: 管理安全分析

在您拥有必要的订阅或获得试用授权后，在“分析”概览页面上，安全产品/服务的“**请求试用**”按钮会变为“**管理**”。单击“**管理**”以查看用户仪表板。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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。要从外部数据源接收数据，您需要将外部数据源与 Analytics 集成。要查看已发现的数据源，请单击“**设置 > 数据源 > 安全**”。

后续步骤

- 当以下云服务的 Citrix Analytics for Security 授权获得批准时，将启用数据处理：
  - Citrix 数据源
    - 思杰安全私有访问
    - 思杰虚拟应用和桌面和思杰 DaaS
- 要验证数据处理状态或了解如何手动开启它，请参阅以下文章：
  - Citrix 数据源：
    - 思杰端点管理

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - 思杰网关
  - 外部数据源：
    - 微软 Graph 安全
    - 微软活动目录
- 将 Analytics 中的已处理数据导出到以下产品：
  - 思普朗克
  - 微软 艾泽 哨兵
  - 弹性搜索
  - 使用基于 Kafka 或 Logstash 的数据连接器的其他 SIEM
- 使用 用户仪表板 查看已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预防的起点。

  注意

  如果您是首次使用 Analytics，用户风险配置文件需要一些时间才能显示在仪表板上。Analytics 使用机器学习来确定用户事件中的风险模式或异常，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 功能查看和筛选从数据源接收到的用户事件（原始数据）。

Citrix 端点管理™ 数据源

“**Endpoint Management**”数据源代表与您的 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活动相关的用户事件。系统会处理用户事件以检测任何安全威胁。

先决条件

- 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。
- **云站点和企业目录设置**。确保您有两台运行 Windows 2012 R2 或 Windows 2016 服务器的计算机来安装 Cloud Connector。
- **Cloud Connector 已安装**。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满足要求。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

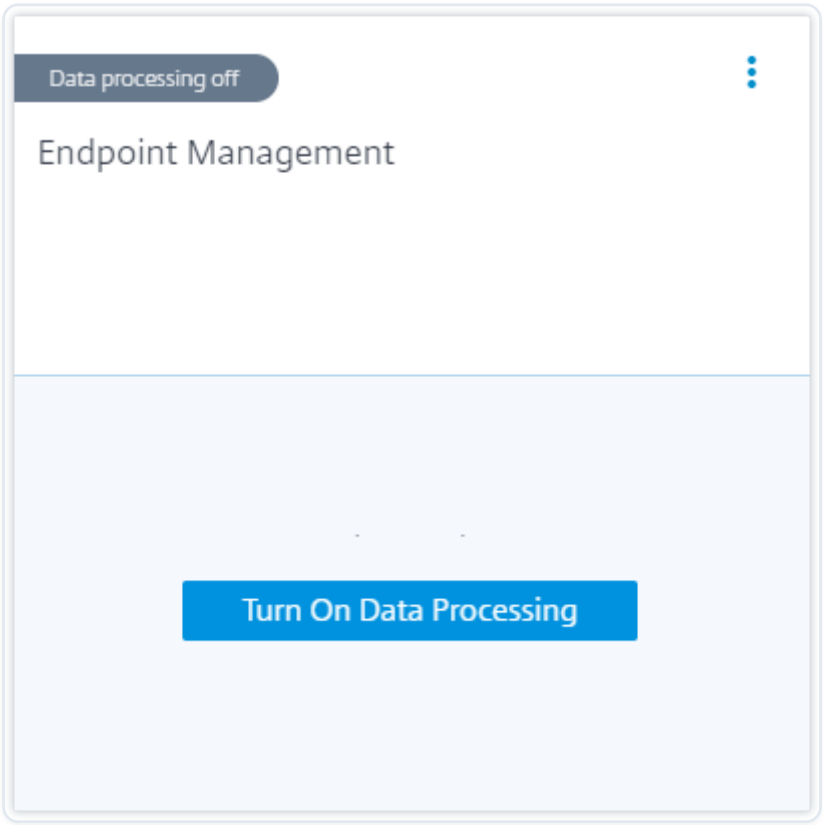
查看数据源并开启数据处理

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：

在顶部栏中，单击“**设置**”>“**数据源**”>“**安全**”。

Endpoint Management 数据源的站点卡片显示在“**数据源**”页面上。单击“**开启数据处理**”以允许 Citrix Analytics 开始处理此数据源的数据。

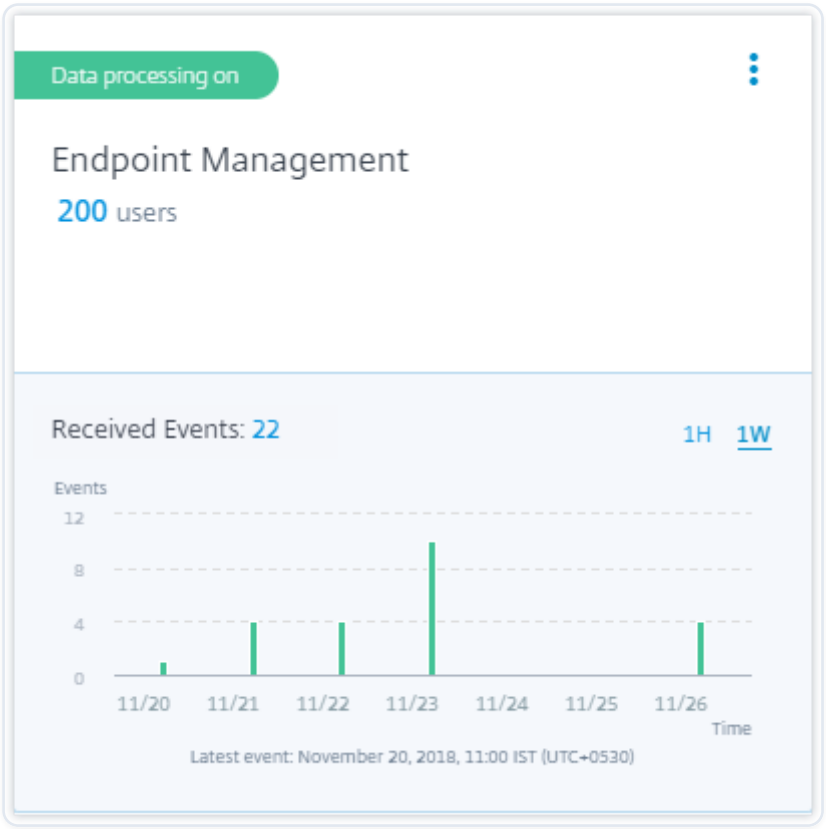


查看用户和接收到的事件

站点卡片显示了过去一小时内 Endpoint Management 用户、设备和接收到的事件数量，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。

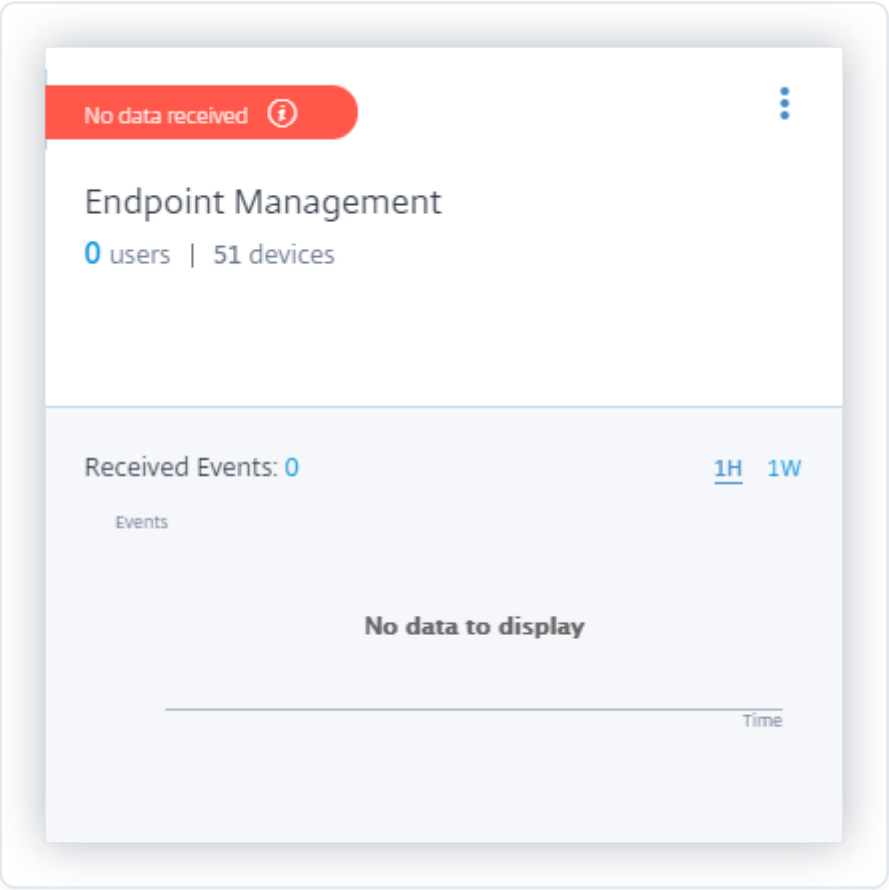
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

1. 如果您是首次开启数据处理，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“**数据处理已开启**”。如果一段时间后状态未更改，请刷新“**数据源**”页面。
2. Analytics 在过去一小时内未从数据源收到任何事件。

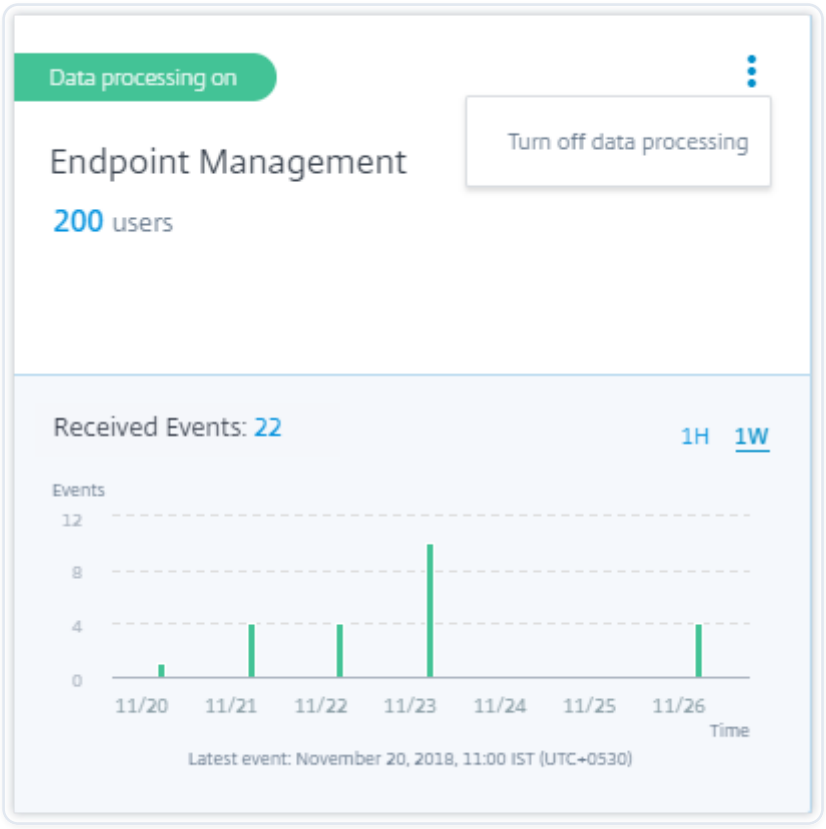
© 1997–2026 Citrix Systems, Inc. All rights reserved.



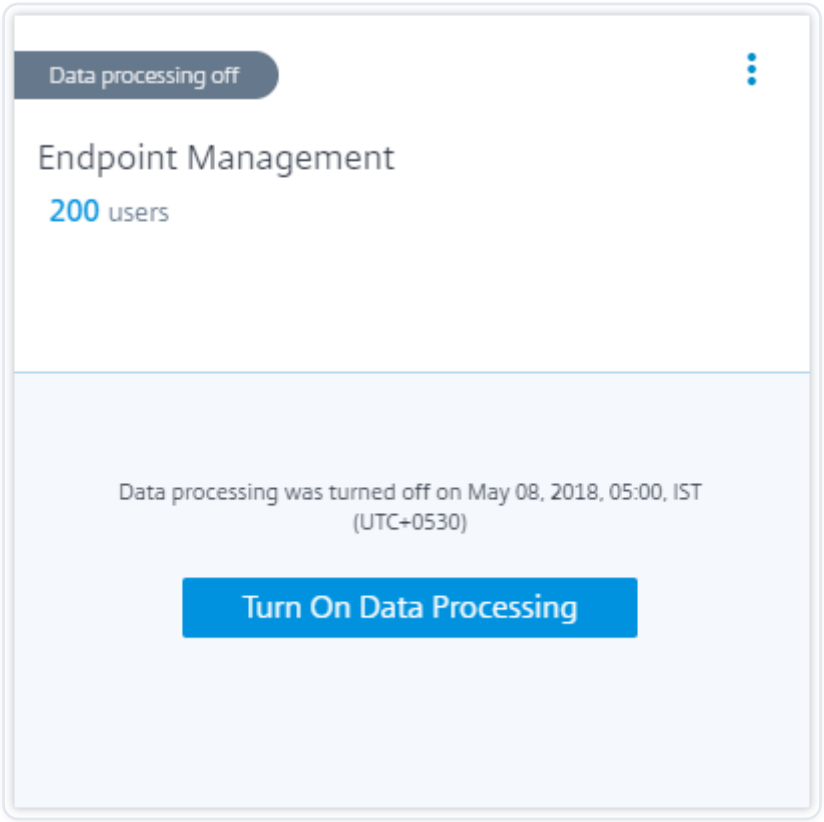
开启或关闭数据处理

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 将停止处理此数据源的数据。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



要再次启用数据处理，请单击“**开启数据处理**”。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Gateway（本地部署）数据源

Gateway 数据源代表您环境中本地部署的 Citrix Gateway 实例。Citrix Analytics 会自动发现 Citrix Application Delivery Management (ADM) 代理以及添加到 Citrix ADM 服务中的 Gateway 实例。

当用户通过 Gateway 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。这些用户事件会经过处理，以检测任何安全威胁。

有关先决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 远程浏览器隔离™ 数据源

Citrix Remote Browser Isolation Service (/zh-cn/citrix-cloud/secure-browser-service.html) 隔离网络浏览，以保护公司网络免受基于浏览器的攻击。它提供对互联网托管的 Web 应用程序的一致、安全的远程访问，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 Remote Browser Isolation 的自助搜索。

要接收来自已发布的 Remote Browser Isolation 会话的用户事件，请在 Remote Browser Isolation 中启用 **主机名跟踪** 策略。默认情况下，此策略处于禁用状态。

启用 **主机名跟踪** 策略后，Remote Browser Isolation 可以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。

思杰安全私有访问™ 数据源

Secure Private Access 数据源代表与您的 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）。用户事件经过处理以检测任何安全威胁。

先决条件

- 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。

查看数据源并开启数据处理

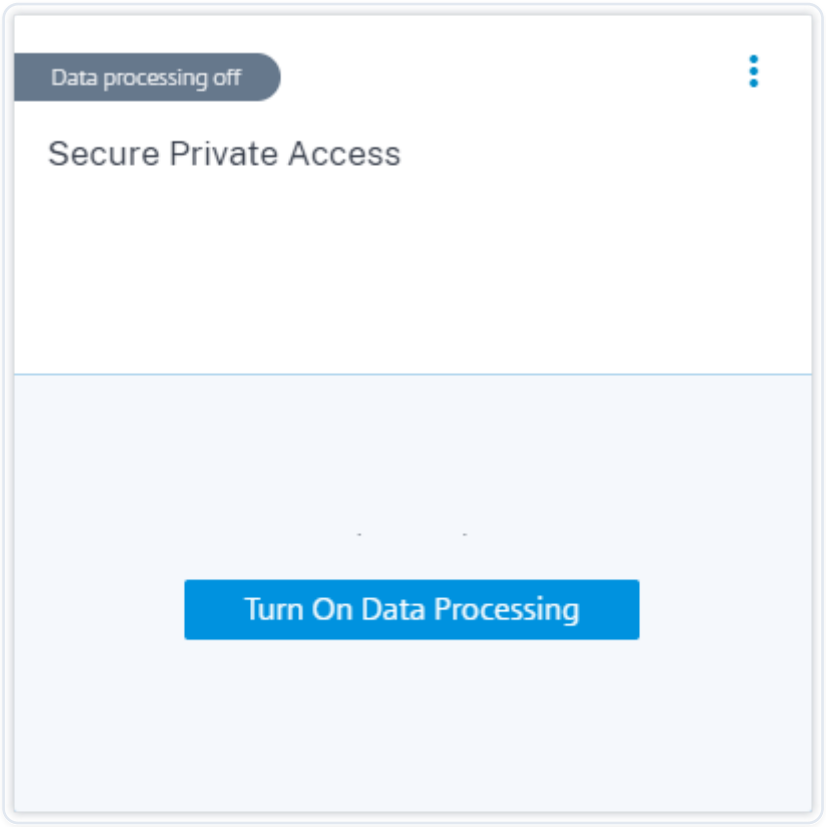
Citrix Analytics 会自动发现与您的 Citrix Cloud™ 帐户关联的 Secure Private Access 数据源。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要查看数据源：

在顶部栏中，单击“**设置**”>“**数据源**”>“**安全**”。

Secure Private Access 数据源的站点卡片显示在“**数据源**”页面上。单击“**开启数据处理**”以允许 Citrix Analytics 开始处理此数据源的数据。

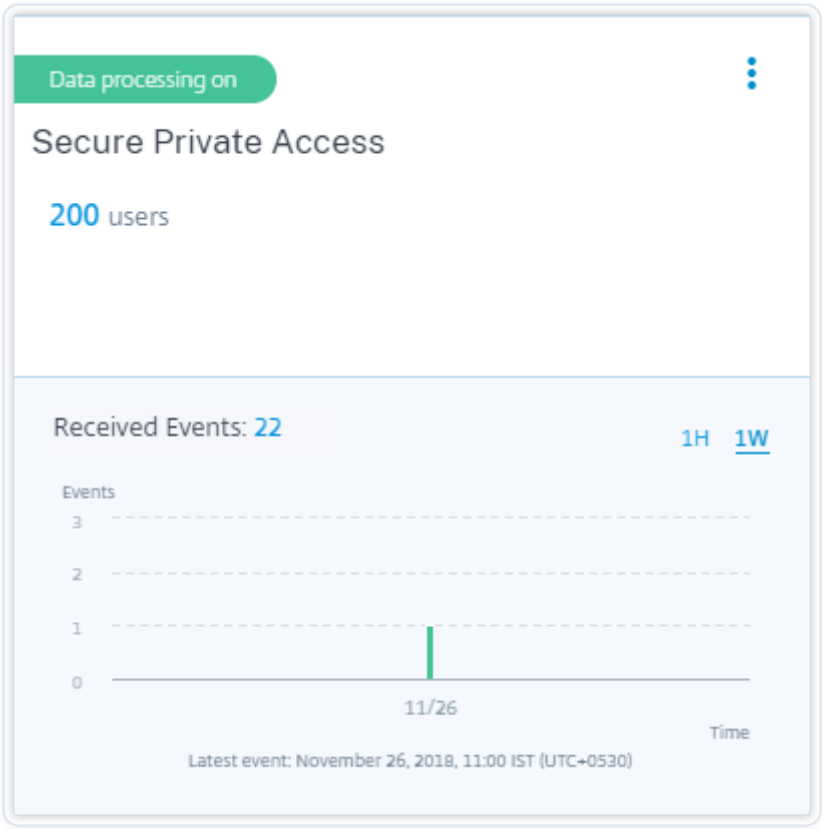


查看用户和接收到的事件

站点卡片显示过去一小时（默认时间选择）的活跃用户数以及从数据源接收到的事件。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。单击接收到的事件数可在 自助搜索 页面上查看事件详细信息。

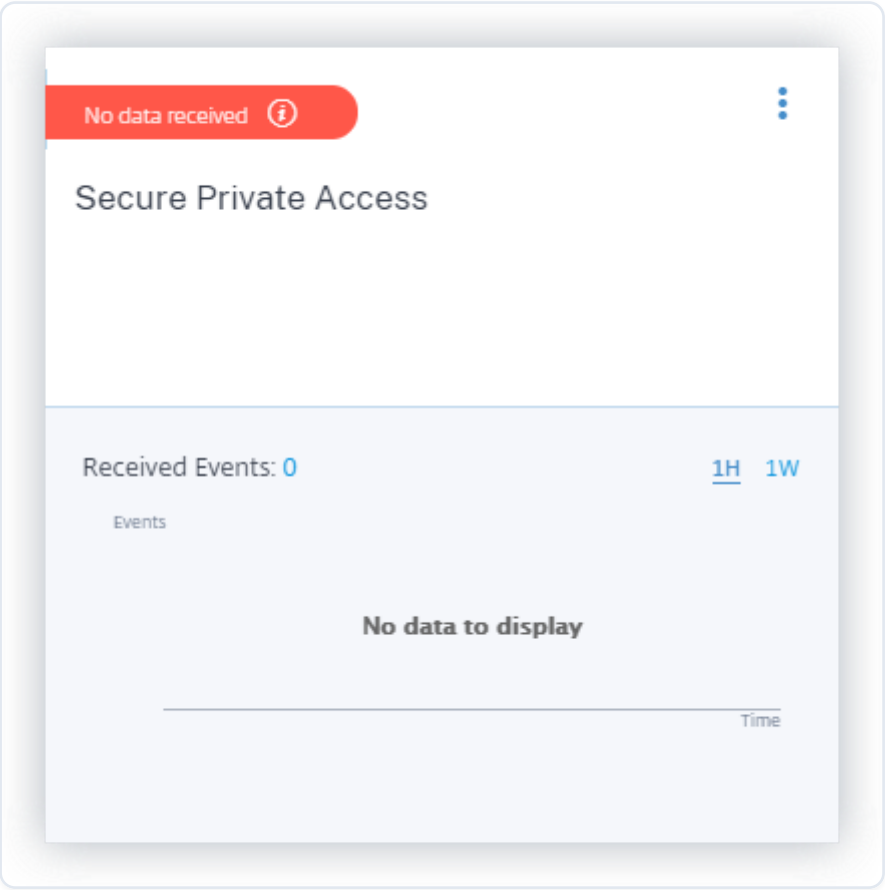
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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. 如果您是首次开启数据处理，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，状态将变为“**数据处理已开启**”。如果一段时间后状态未更改，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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



开启或关闭数据处理

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 将停止处理此数据源的数据。

清除数据处理(/en-us/citrix-analytics/media/access-control-turn-off-transmission.png)

要再次启用数据处理，请单击“**开启数据处理**”。

开启数据处理(/en-us/citrix-analytics/media/access-control-turn-on-again.png)

Citrix 虚拟应用和桌面™ 和 Citrix DaaS 数据源

Apps and Desktops 数据源代表您的组织中本地部署的 Citrix Virtual Apps and Desktops 和 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。本文将引导您了解在这两种产品上启用 Analytics 的先决条件和步骤。

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

- 安装在用户设备上的 Citrix Workspace™ 应用程序

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 用于本地部署的 Citrix Director
- Citrix 监控服务
- 会话录制服务器

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。

支持的客户端版本

当在用户端点上使用支持的客户端版本时，Citrix Analytics 会接收用户事件。如果用户正在使用任何不支持的客户端版本，他们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 应用程序 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 中提供的最新版本
- 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 2006 或更高版本的 Citrix Workspace 应用程序

在 Citrix DaaS 上启用分析

先决条件

- 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，并确保您已满足要求。

查看数据源并开启数据处理

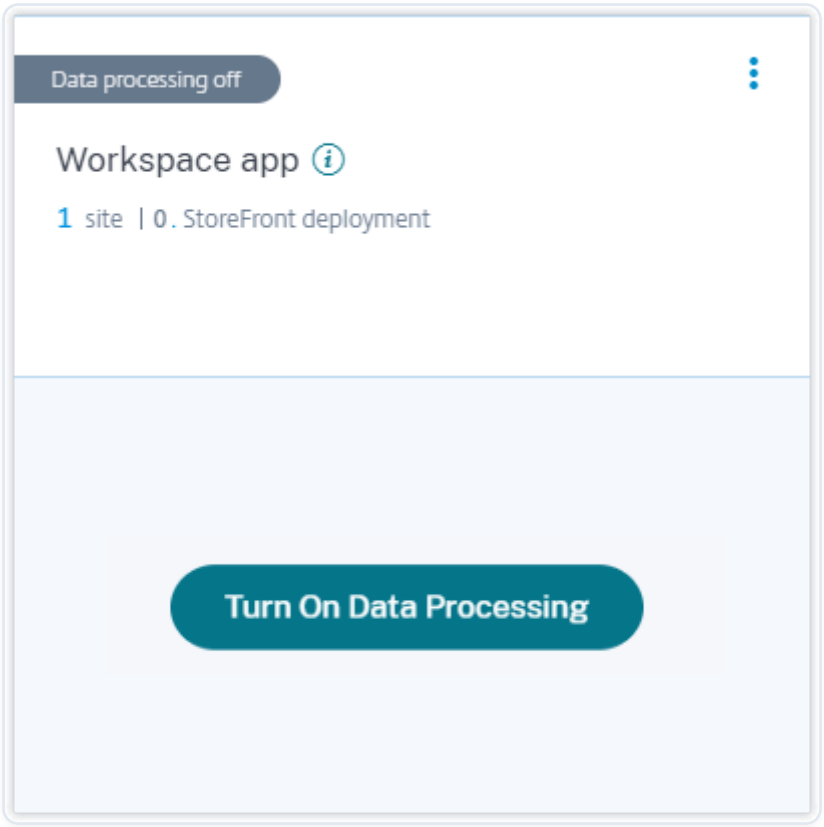
Citrix Analytics 会自动发现与您的 Citrix Cloud™ 帐户关联的 Citrix DaaS。

要查看数据源：

在顶部栏中，单击**设置** > **数据源** > **安全**。

应用程序和桌面 - Workspace 应用程序站点卡片显示在**数据源**页面上。单击**开启数据处理**以允许 Citrix Analytics 开始处理此数据源的数据。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

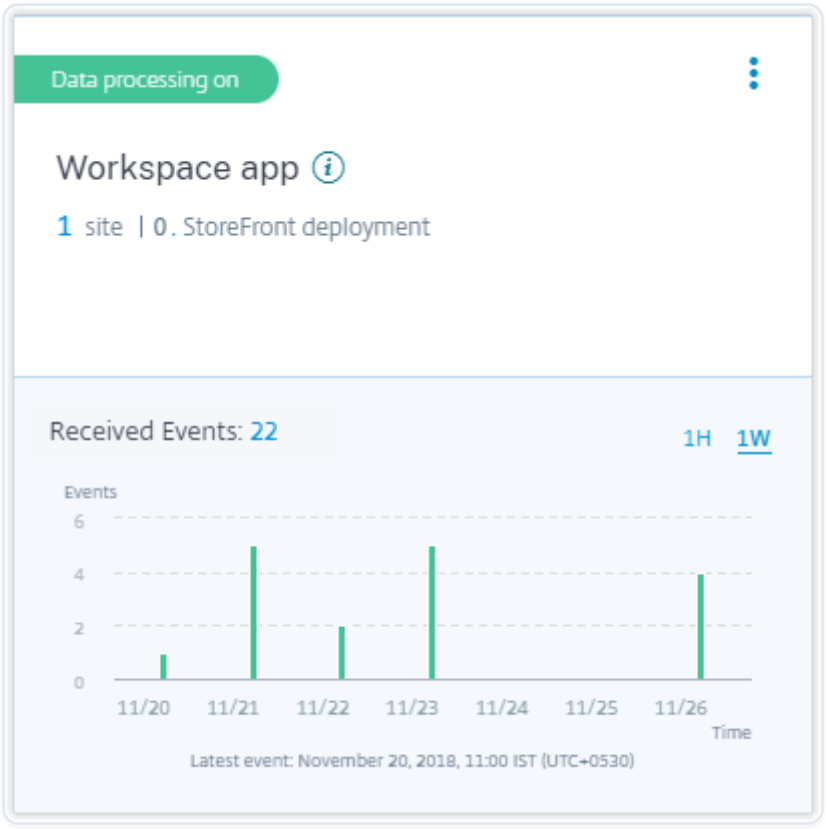


查看云站点、用户和接收到的事件

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

点击收到的事件数量，在 (/zh-cn/security-analytics/self-service-search/self-service-search-virtual-apps-desktops.html) 页面上查看事件。

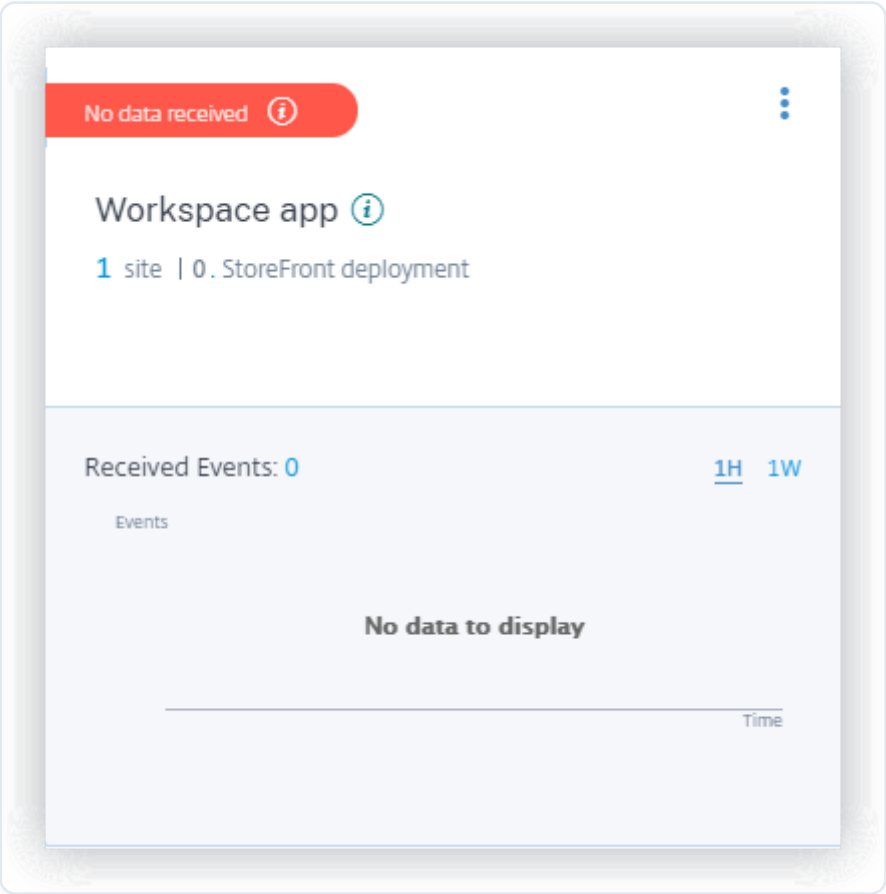
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

1. 如果您是首次开启数据处理，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，状态将变为“**数据处理已开启**”。如果一段时间后状态未更改，请刷新“**数据源**”页面。
2. 在过去一小时内，Analytics 未从数据源收到任何事件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在本地 Citrix Virtual Apps and Desktops 上启用分析

Citrix Analytics 从添加到 Workspace 的本地站点以及通过 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载入您的站点，以便 Analytics 发现这些站点：

- 使用 StoreFront 载入您的本地站点
- 使用 Workspace 载入您的本地站点

先决条件

- 您必须拥有使用 Citrix Virtual Apps and Desktops 本地解决方案的许可证。要了解如何开始使用 Citrix Virtual Apps and Desktops 本地解决方案，请参阅 (/zh-cn/citrix-virtual-apps-desktops/install-configure.html)。
- 查看 **系统要求** 部分，并确保您满足要求。
- 您的 Director 版本为 1912 CU2 或更高版本。有关详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/director/version-matrix.html)。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Citrix Workspace 订阅**。如果您想将站点添加到 Citrix Workspace，则必须拥有 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 会自动发现已添加到 Citrix Workspace 的站点。在继续在 Citrix Analytics 上进行载入之前，请将您的站点添加到 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。有关站点聚合的详细说明，请参阅 在工作区中聚合本地虚拟应用程序和桌面。

- **StoreFront 版本**。如果您正在为您的站点使用 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

有关先决条件和载入步骤的信息，请参阅 Citrix Analytics 平台文档中的 Citrix Virtual Apps and Desktops 数据源 文章。

使用 Workspace 载入 Citrix Virtual Apps and Desktops 本地站点

已添加到 Citrix Workspace 的站点

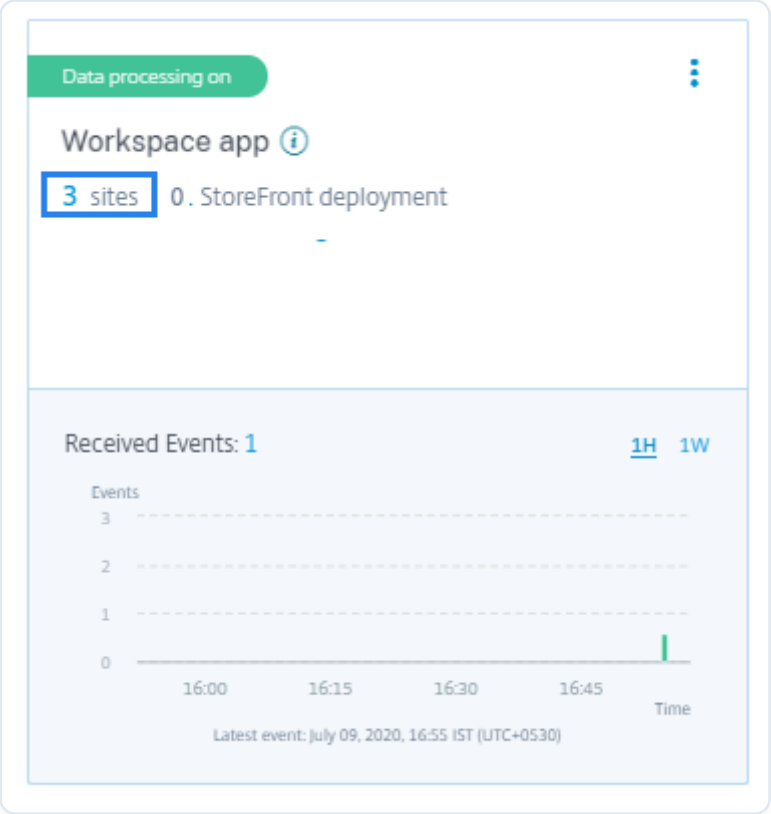
Citrix Analytics 会自动发现已添加到 Citrix Workspace 的本地站点，并将其显示在数据源站点卡上。

要查看数据源：

在顶部栏中，单击“**设置**”>“**数据源**”>“**安全**”。

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。单击站点计数可查看发现的站点。单击用户计数可在“**用户**”页面上查看发现的用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



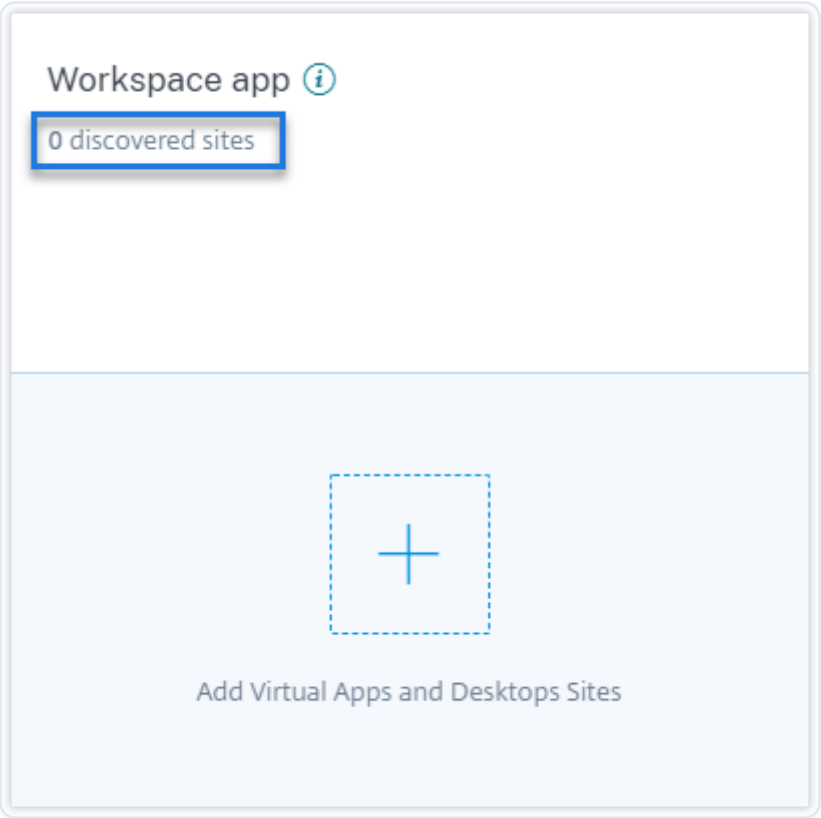
未添加到 Citrix Workspace 的站点

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

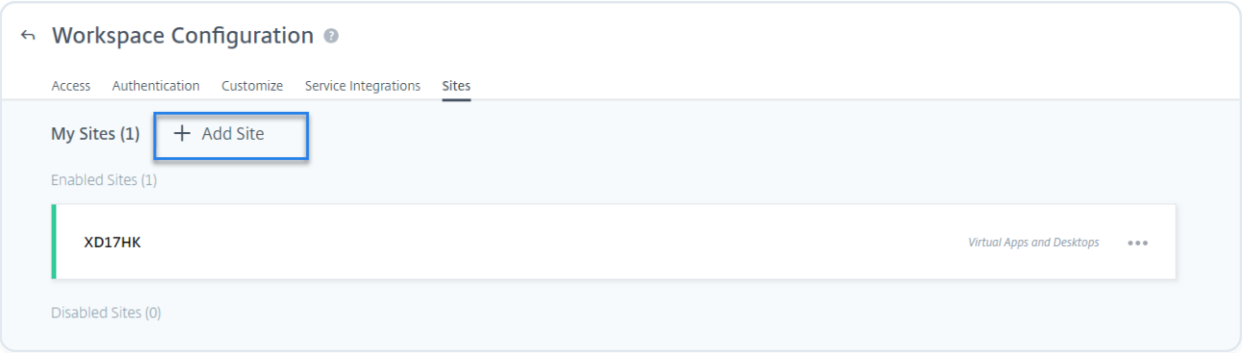
要将站点添加到 Workspace：

1. 单击站点卡片上的 +。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

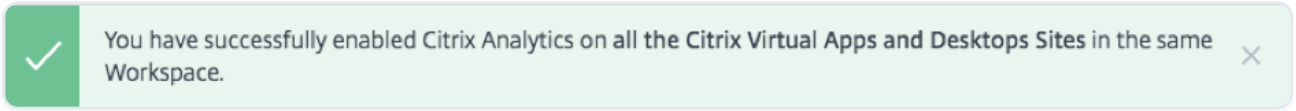


3. 按照屏幕上的说明添加站点。有关详细信息，请参阅在工作区中聚合本地虚拟应用程序和桌面。
4. 添加站点后，重新登录 Citrix Analytics 并刷新“**数据源**”页面，以在站点卡片上查看最近添加的站点。

开启数据处理并查看接收到的事件

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“**开启数据处理**”，然后按照屏幕上的提示操作。

如果您有多个站点添加到同一个 Workspace，Analytics 会处理并存储 Workspace 中所有站点的数据。当 Analytics 在所有站点上成功启用时，您会收到一条成功消息。

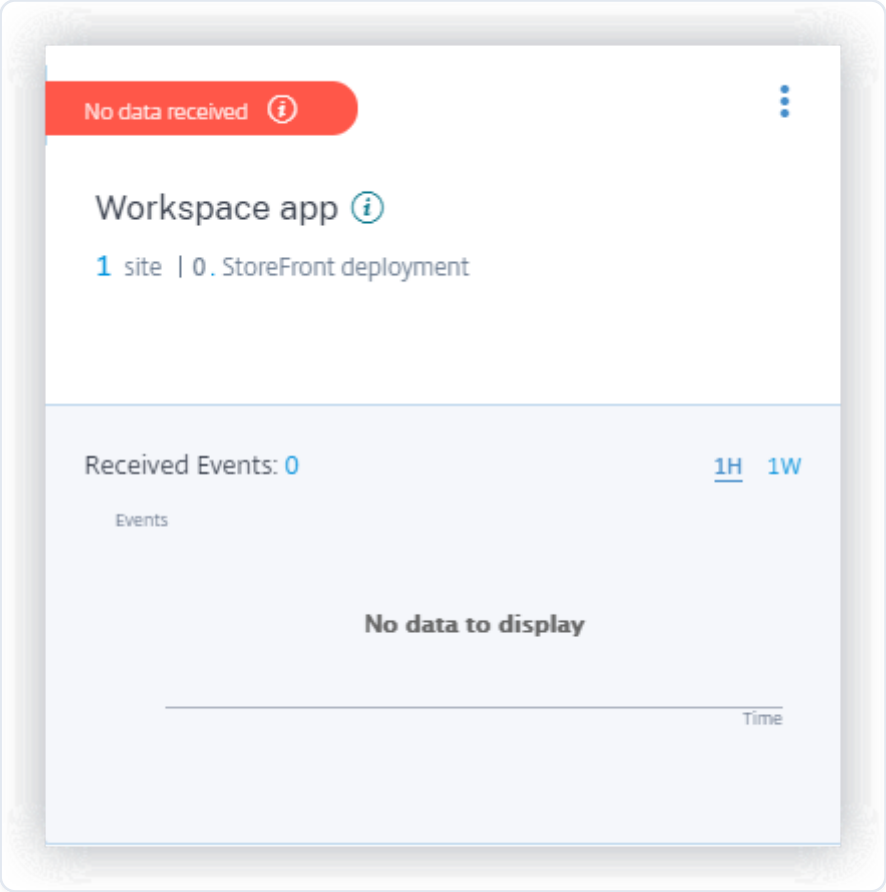


© 1997–2026 Citrix Systems, Inc. All rights reserved.

站点卡片显示过去一小时内接收到的事件，这是默认时间选择。您还可以选择 1 周 (1 W) 并查看数据。单击接收到的事件数量，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“**未接收到数据**”状态。此状态出现的原因有两个：

1. 如果您是首次开启数据处理，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，状态会变为“**数据处理已开启**”。如果一段时间后状态未更改，请刷新“**数据源**”页面。
2. Analytics 在过去一小时内未从数据源接收到任何事件。

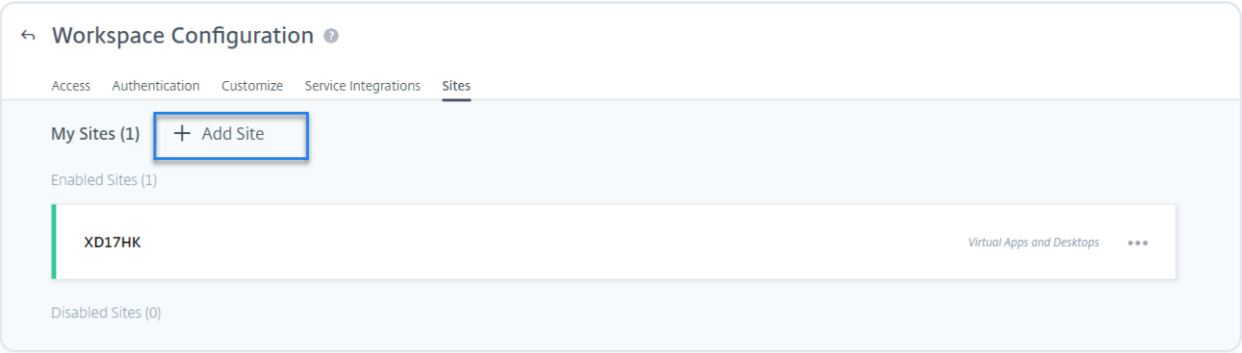


添加站点

如果要将另一个本地站点添加到 Workspace，可以从 Analytics 中添加它：

1. 在 Workspace 配置页面上，单击 **+添加站点**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 按照屏幕上的说明添加站点。有关详细信息，请参阅在工作区中聚合本地虚拟应用程序和桌面。
3. 添加站点后，转到 Citrix Analytics 并刷新**数据源**页面，以在站点卡上查看最近添加的站点。

连接到本地站点的 Citrix Director

Citrix Director 是 Citrix Virtual Apps and Desktops 的监控和故障排除控制台。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 会将监控事件发送到 Security Analytics。

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

在同时具有云部署和本地部署的混合环境中，Security Analytics 会从 Citrix Monitor 服务以及在 Citrix Director 上载入的站点接收事件。

先决条件和配置步骤

注意

- 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，则可以按照这些步骤连接到 Citrix Director。
- 如果您的 Citrix Cloud 帐户同时拥有 Security Analytics 和 Performance Analytics 的有效权利，并且您已经为 Performance Analytics 配置了站点，则无需再次为 Security Analytics 配置 Director。

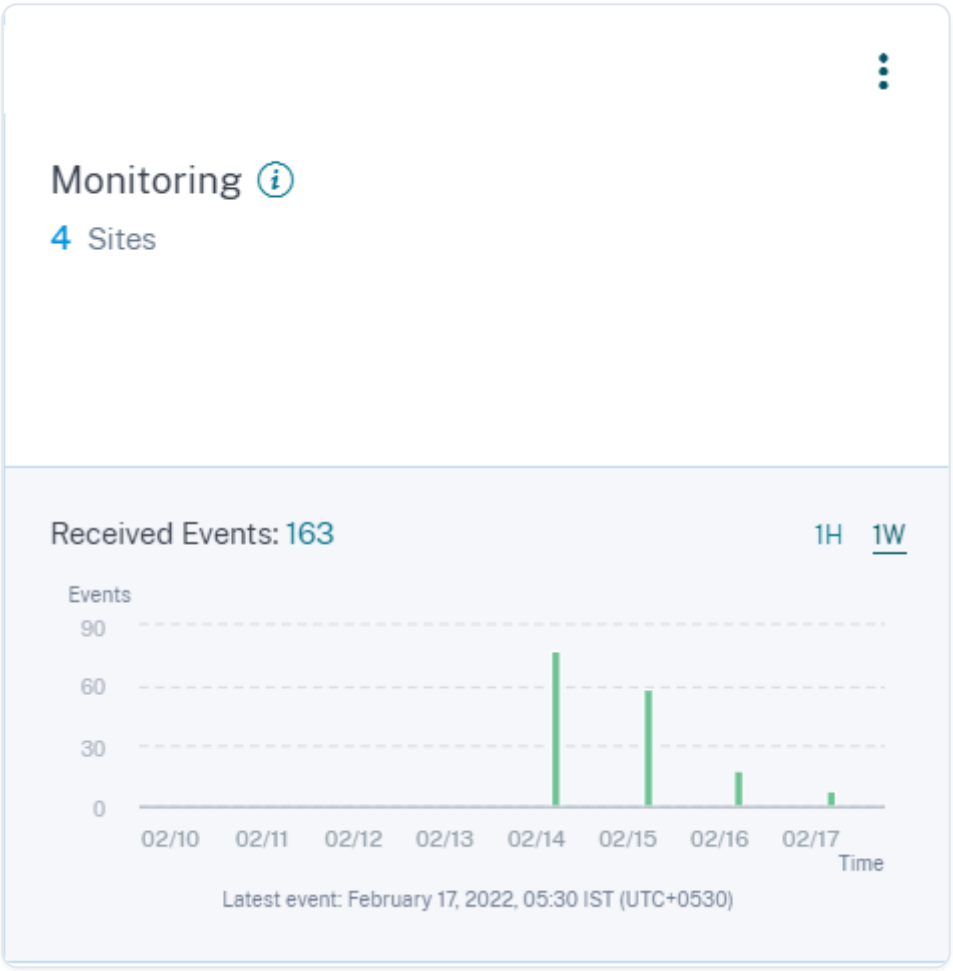
有关先决条件和配置步骤的信息，请参阅 (/zh-cn/performance-analytics/data-sources/onboarding.html)。

查看已连接的站点和收到的事件

1. 在 Citrix Analytics 中，转到**数据源**页面。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 单击**安全**选项卡。
3. 在**应用程序和桌面 - 监控**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收到的事件。

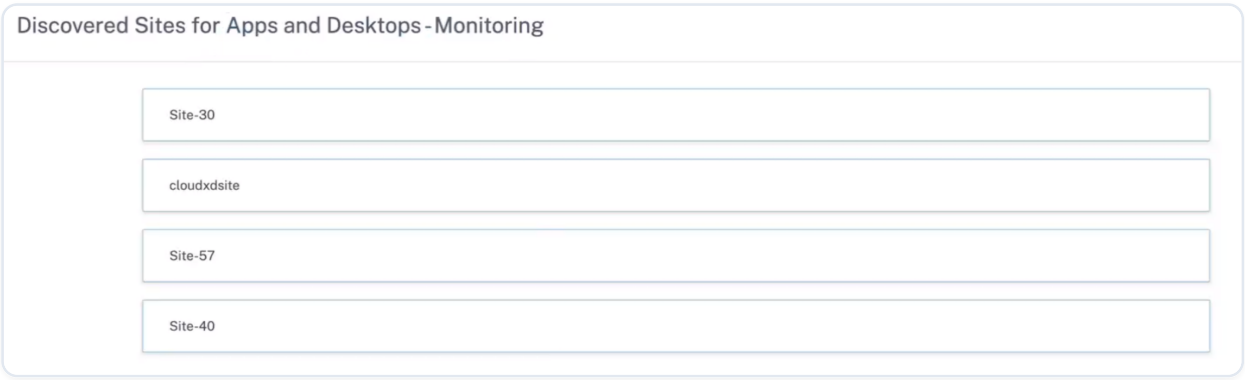


备注

- 首次在 Director 上配置本地站点时，来自站点的事件可能需要一些时间（大约一小时）才能处理完毕；这会导致**应用程序和桌面 - 监控**站点卡上显示连接站点时出现延迟。
- 在监控站点卡上，默认情况下会启用监控服务或 Director 数据源的数据处理。您也可以根据需要关闭数据处理。但是，建议保持数据处理开启，以从 Security Analytics 中获得最大收益。

4. 单击站点以查看详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



连接到会话录制部署

(/zh-cn/session-recording/current-release.html) 允许您录制 Citrix Virtual Apps and Desktops 和 Citrix DaaS 中任何用户会话的屏幕活动。您可以将会话录制服务器配置为将用户事件发送到 Citrix Analytics for Security。用户事件经过处理，可为用户的风险行为提供可操作的见解。

先决条件

开始之前，请确保满足以下条件：

- 您的 Session Recording 服务器和 VDA 代理必须是 2103 或更高版本。
- Session Recording 服务器必须能够连接到所需的地址。有关 URL 的更多信息，请参阅网络要求。
- Session Recording 部署必须打开端口 443 以进行出站 Internet 连接。网络上的任何代理服务器都必须允许此通信与 Citrix Analytics for Security 进行。
- 如果您使用的是 Citrix Virtual Apps and Desktops 7 1912 LTSR，则支持的 Session Recording 版本为 2103 或更高版本。

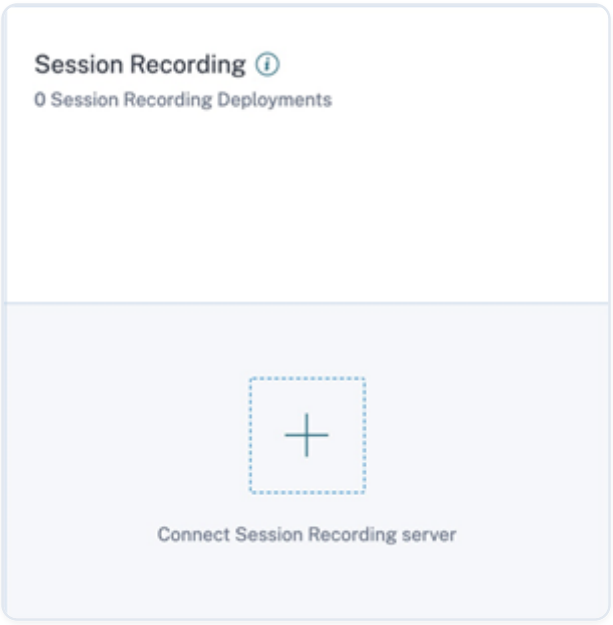
注意

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

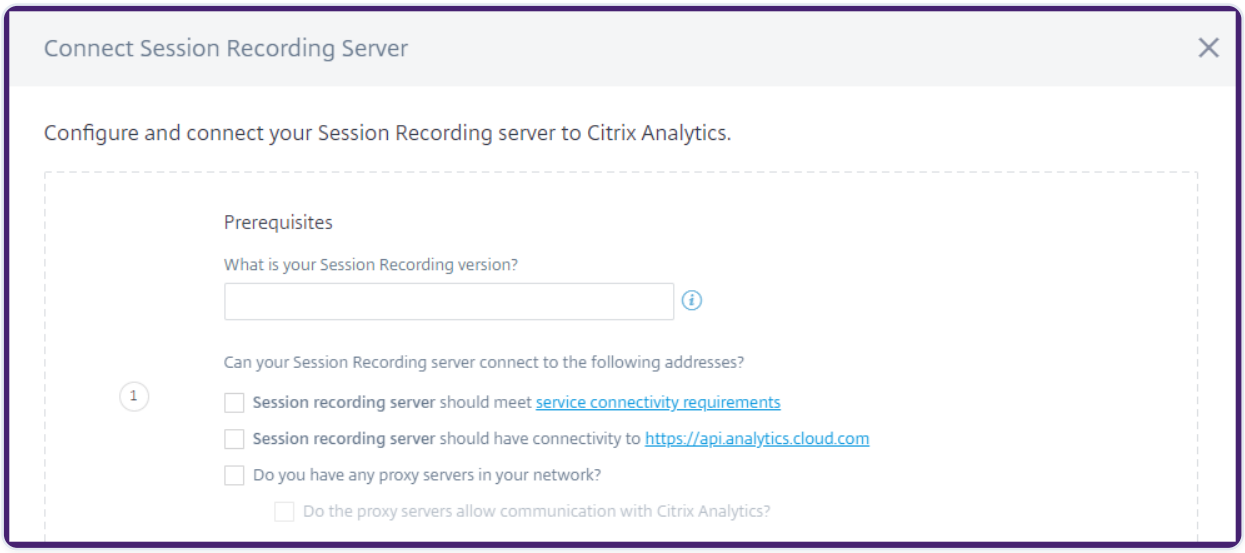
配置您的 Session Recording 服务器

1. 在 **Apps and Desktops- Session Recording** 站点卡上，单击**连接 Session Recording 服务器**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 在**连接 Session Recording 服务器**页面上，查看清单，并选择所有强制性要求。如果您未选择强制性要求，则“下载文件”选项将被禁用。



3. 如果您的网络中有代理服务器，请在 Session Recording 服务器的 *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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 点击**下载文件**以下载 *SessionRecordingConfigurationFile.json* 文件。

   注意

   该文件包含敏感信息。请将文件保存在安全可靠的位置。

5. 将文件复制到您要连接到 Citrix Analytics for Security 的会话录制服务器。
6. 如果您的部署中有多个会话录制服务器，则必须将文件复制到要连接的每个服务器中，并按照步骤配置每个服务器。
7. 在会话录制服务器上，运行以下命令以导入设置：

   ```
   &lt;Session Recording Server installation path>\bin\SsRecUtils.exe
   -Import_SRCasConfigurations &lt;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 会话录制分析服务
   - Citrix 会话录制存储管理器

9. 配置成功后，转到 Citrix Analytics for Security 以查看已连接的会话录制服务器。点击**启用数据处理**以允许 Citrix Analytics for Security 处理数据。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

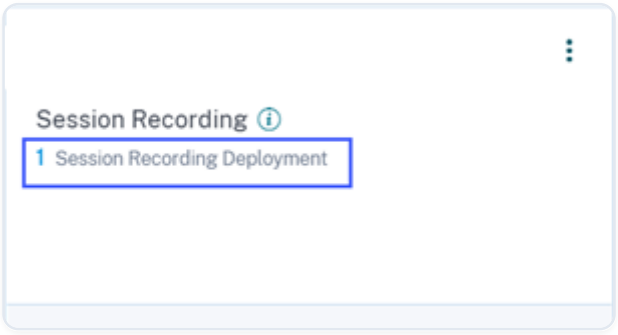
注意

如果您使用的是会话录制服务器版本 2103 或 2104，则必须首先启动一个 Apps and Desktops 会话才能在 Citrix Analytics for Security 上查看已连接的会话录制服务器。否则，已连接的会话录制服务器将无法显示。此要求不适用于会话录制服务器版本 2106 及更高版本。

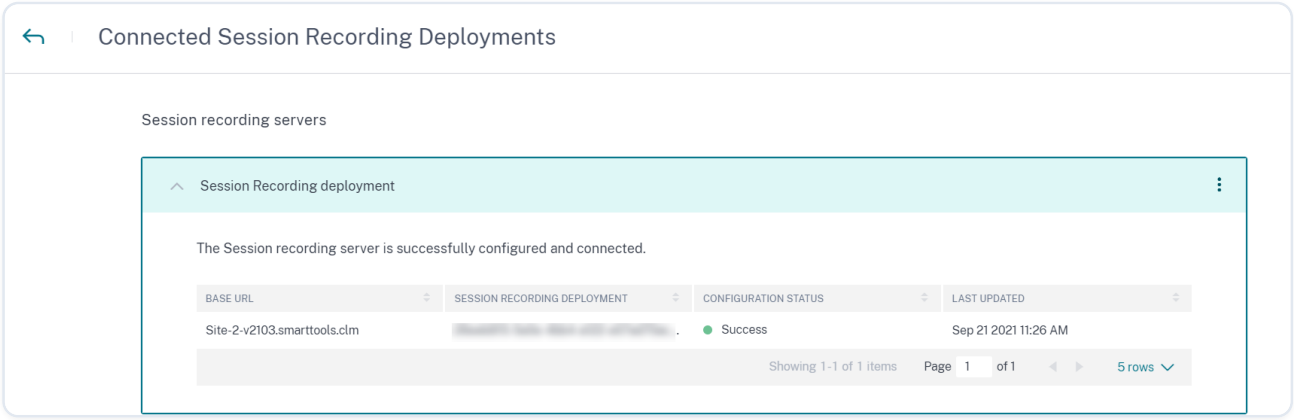
查看已连接的部署

仅当配置成功时，服务器部署才会显示在会话录制站点卡上。站点卡显示已与 Citrix Analytics for Security 建立连接的已配置服务器的数量。

如果即使配置成功后仍未看到会话录制服务器，请参阅故障排除文章。



在站点卡上，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 个会话录制部署**以查看已连接的服务器或服务器组。每个会话录制服务器都由一个基本 URL 和一个 ServerGroupID 表示。



查看收到的事件

站点卡显示已连接的会话录制部署以及在过去一小时内从这些部署收到的事件，这是一小时的默认时间选择。您还可以选择 1 周 (1 W) 并查看数据。单击收到的事件数量以在自助服务搜索页面上查看事件。

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

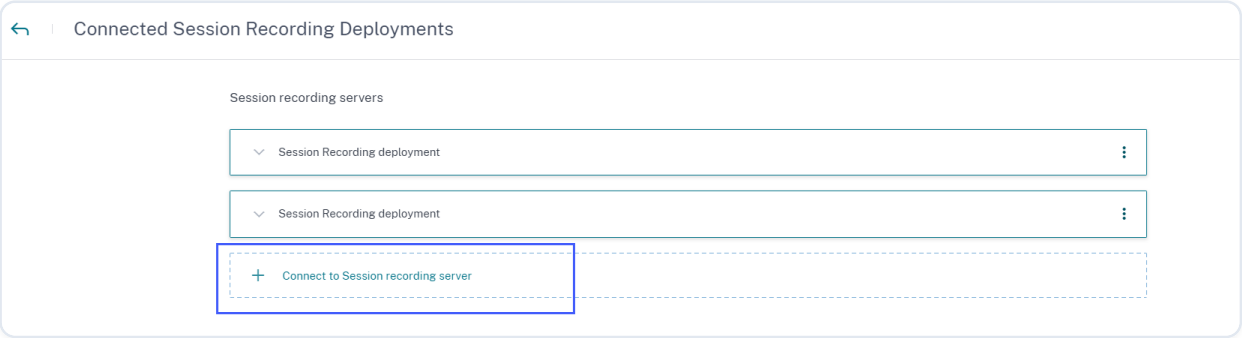
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 如果首次开启数据处理，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，状态将变为**数据处理开启**。如果一段时间后状态未更改，请刷新“数据源”页面。
2. Citrix Analytics 在过去一小时内未从数据源收到任何事件。

添加会话录制服务器

要添加会话录制服务器，请执行以下操作之一：

- 在**已连接的会话录制部署**页面上，单击**连接到会话录制服务器**。



- 在 **Apps and Desktops- Session Recording** 站点卡片上，单击垂直省略号 (⋮)，然后选择 **Connect Session Recording server**。

  会话录制连接(/en-us/citrix-analytics/media/sr-connect.png)

按照步骤下载配置文件并配置会话录制服务器。

删除会话录制服务器

要删除会话录制服务器，请执行以下操作：

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

   删除会话录制服务器(/en-us/citrix-analytics/media/sr-remove.png)
3. 在已从 Citrix Analytics 中删除的会话录制服务器上，运行以下命令：

   ```
   &lt;Session Recording Server installation path>\bin\SsRecUtils.exe
   -Remove_SRCasConfigurations
   ```

   例如：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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 service）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。这些打印日志提供了有关打印活动的重要信息，例如打印机名称、打印文件名和打印总份数。

注意

此功能仅支持 Citrix DaaS。

在 Citrix 安全分析中，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进行风险分析和用户调查。

默认情况下，在虚拟投递代理 (VDA) 上禁用打印遥测功能（即这些打印日志的收集和传输）。

要启用打印遥测并将打印日志传输到 Citrix 安全分析，您需要创建注册表项并配置您的 VDA。

重要

此配置仅适用于 Windows VDA。

先决条件

- 您的 VDA 版本必须与 Citrix Virtual Apps and Desktops 7 2203 LTSR 或更高版本的基线版本相同。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 7 2203 基线组件。
- 您必须具有执行注册表项更新的完全访问权限。

在电源管理计算机中启用打印遥测

电源管理计算机包括具有以下情况的虚拟机或刀片式 PC：

- 现有主映像
- 新主映像

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. 登录到主 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来启用打印服务日志：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 或更高版本的基线版本。有关详细信息，请参阅Citrix Virtual Apps and Desktops 7 2203 基线组件。
4. 关闭计算机电源并拍摄最新状态的快照。
5. 登录到 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。配置将在 24 小时内自动推送。如果配置已完成，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将在 Citrix Analytics for Security 的“**搜索**”页面上显示。

为 VDA 版本与 Citrix Virtual Apps and Desktops 7 2203 LTSR 或更高版本相同现有主映像启用打印遥测

选项 1：在主 VDA 中添加打印注册表项并更新虚拟桌面。

1. 登录到主 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 计算机并拍摄最新状态的快照。
4. 登录到 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。所有使用客户端打印机触发的打印事件都可在 Citrix Analytics for Security 的 **搜索** 页面上查看。

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，您必须遵循选项 1 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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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。所有使用客户端打印机触发的打印事件都可在 Citrix Analytics for Security 的 **搜索** 页面上查看。

在新的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. 确保主 VDA 已添加到所需域。
3. 登录到主 VDA 并通过添加以下注册表项来启用打印服务日志：

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   有关详细信息，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。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 基线组件。
5. 确保托管连接已添加到 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。配置将在 24 小时内由组策略引擎自动推送。
9. 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可在 Citrix Analytics for Security 的“**搜索**”页面上查看。

在未进行电源管理的计算机中启用打印遥测

未进行电源管理的计算机包括具有以下场景的物理计算机：

- 现有物理 VDA
- 新建物理 VDA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

   有关详细信息，请参阅 创建注册表项。
2. 将 VDA 升级到 Citrix Virtual Apps and Desktops 7 2203 LTSR 或更高版本的基线版本。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 7 2203 基线组件。
3. 等待 24 小时。配置将在 24 小时内自动推送。如果配置已完成，则无需等待。
4. 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可在 Citrix Analytics for Security 的“**搜索**”页面上查看。

为新建物理 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

   有关详细信息，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。安装 VDA 时，选择“远程 PC 访问”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

   必须选择计算机管理为**未进行电源管理的计算机（例如，物理计算机）**。
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。配置将在 24 小时内由组策略引擎自动推送。
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将在 Citrix Analytics for Security 的“**搜索**”页面中显示。

创建注册表项

在您的 VDA 中，执行以下任一操作：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 手动创建注册表项。此方法适用于主 VDA 以及部署中物理 VDA 数量较少的情况。
- 使用组策略对象 (GPO) 创建注册表项。当您的部署中有大量物理 VDA 计算机并且必须在所有这些计算机上启用打印遥测时，请使用此方法。

注册表项详细信息

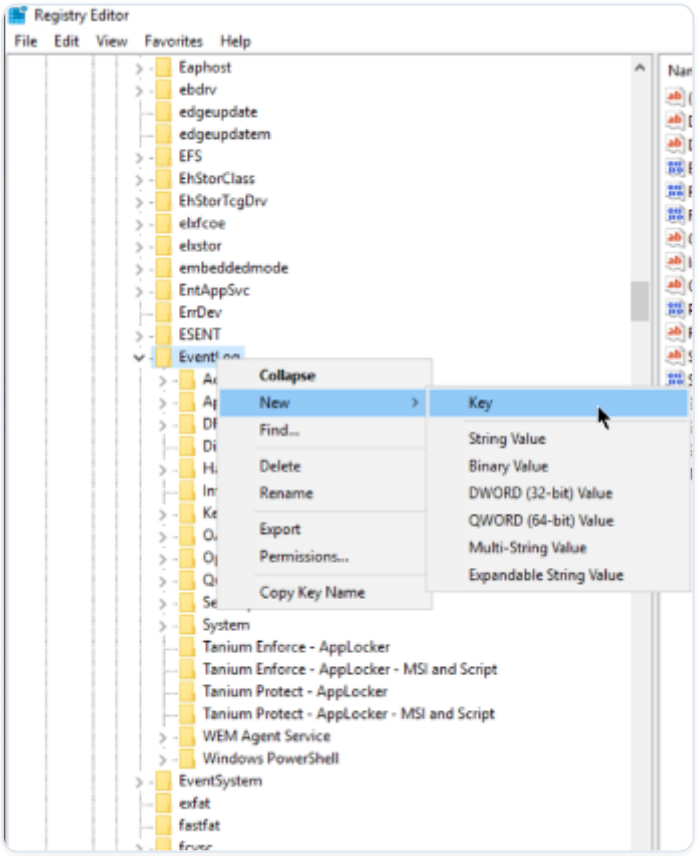
序号	注册表项名称	密钥用途	注册表详细信息
1	Microsoft-Windows-PrintService/Operational	在事件查看器中启用打印服务日志。	**注册表路径：**HKLM:\SYSTEM\CurrentControlSet\Services\EventLog
2	ShowJobTitleInEventLogs	控制打印作业名称是否包含在打印事件日志中，否则将使用通用作业名称“打印文档”。	**注册表配置单元：**HKEY_LOCAL_MACHINE
			注册表路径：Software\Policies\Microsoft\Windows NT\Printers
			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

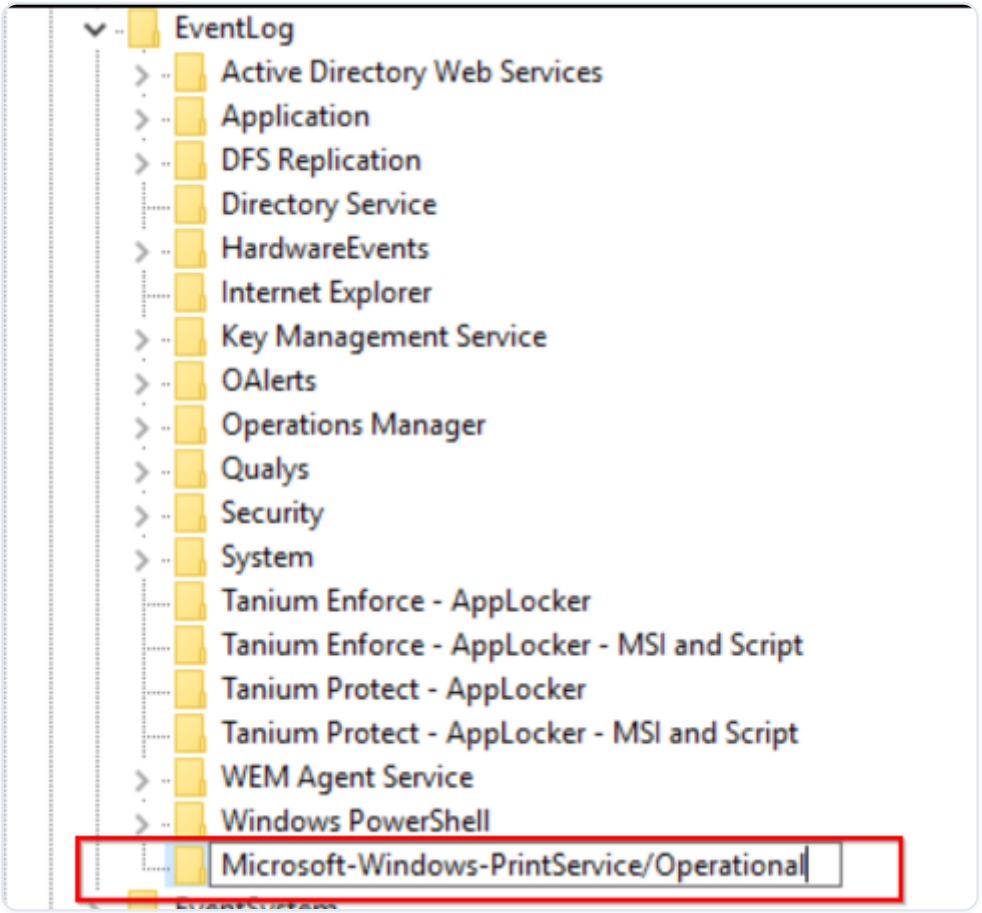
使用此方法在 VDA 主映像中创建注册表项。将项添加到主映像有助于使通过主映像创建的所有类型的 VDA 保持持久。

1. 登录到 VDA 主机。
2. 打开“运行”并键入 Regedit 以打开 Windows 注册表。
3. 转到位置 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog
4. 右键单击 **EventLog** 并选择 **新建 > 项**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 创建一个名为 **Microsoft-Windows-PrintService/Operational** 的项。此项启用打印服务日志。

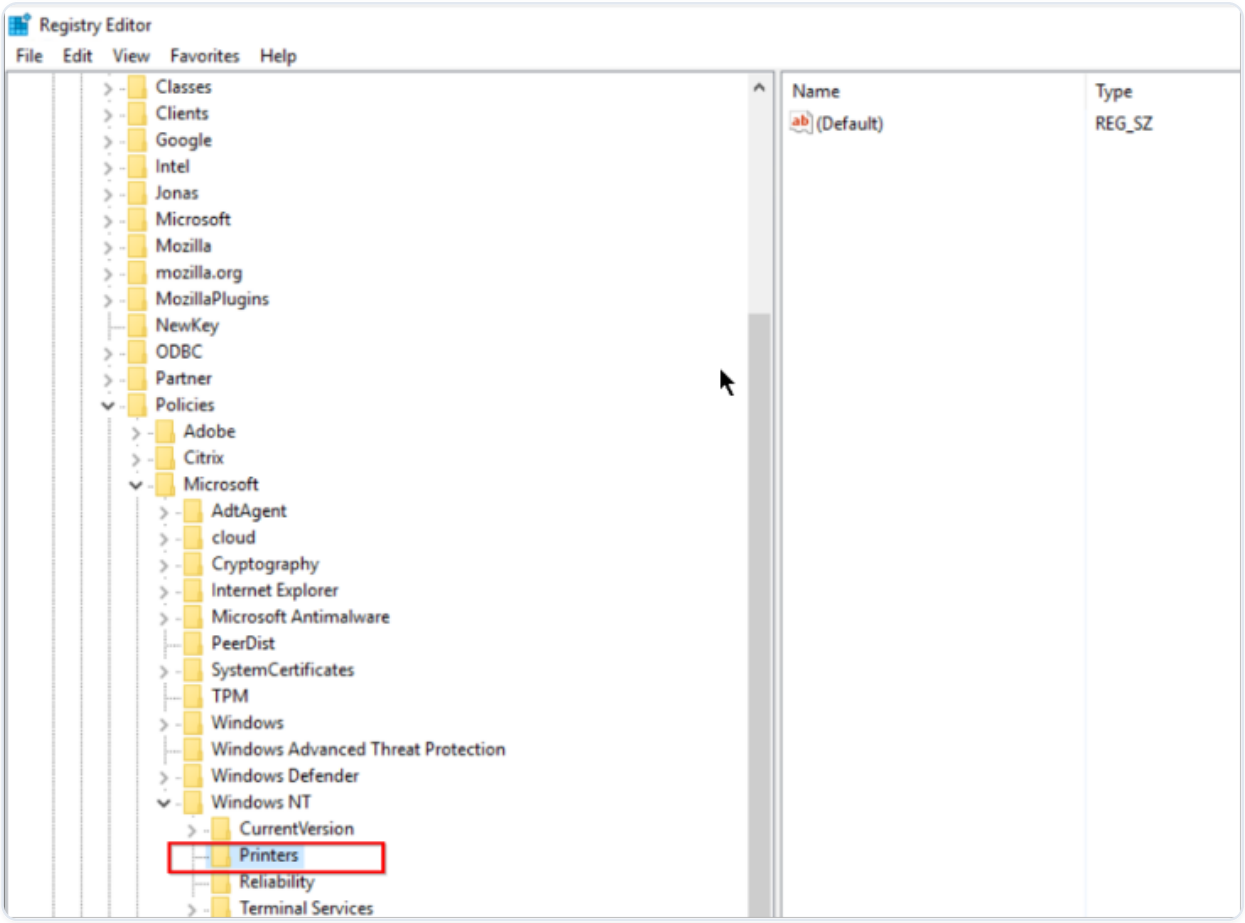


6. 转到位置 **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers**。

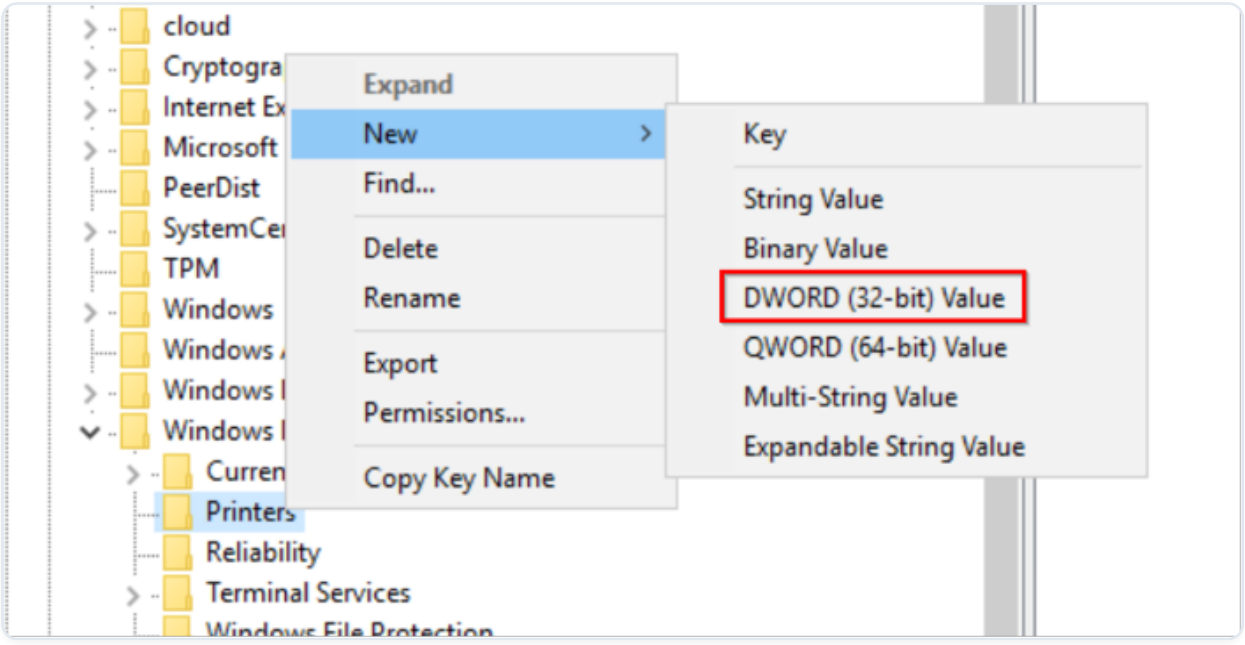
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

如果 Printers 文件夹不可用，请在 Windows NT 文件夹中创建一个名为 Printers 的项。

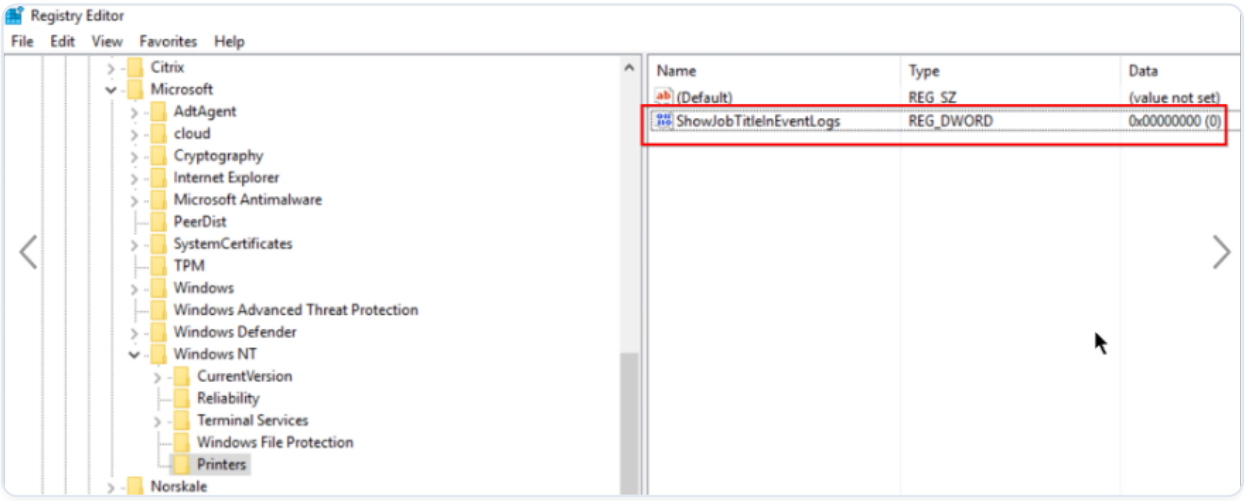


7. 右键单击 **Printers** 文件夹并选择 **新建 > DWORD（32 位）值**。

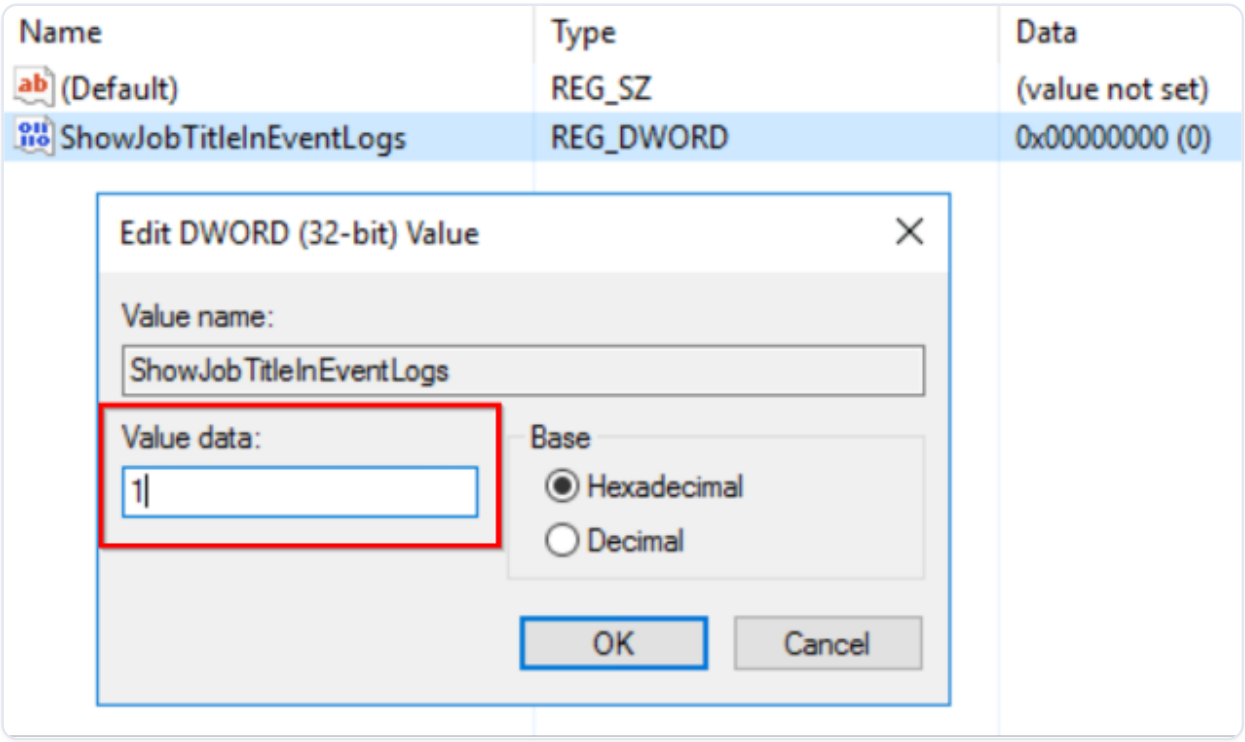


8. 创建一个名为 **ShowJobTitleInEventLogs** 的值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. 右键单击 **ShowJobTitleInEventLogs** 并选择“**修改**”。将“**值数据**”输入为 1，然后单击“**确定**”。



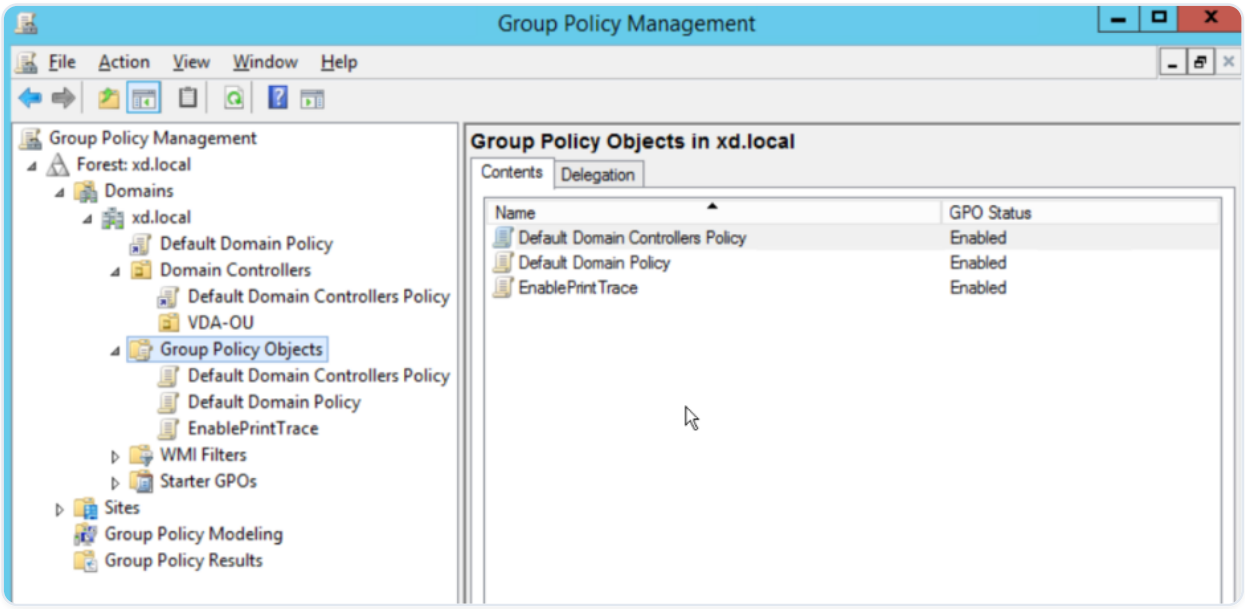
使用 GPO 在多个 VDA 中创建注册表项

此方法仅适用于持久性 VDA，并且在创建注册表项后需要重新启动 VDA。持久性 VDA 是一种在重新启动后仍能保持其状态的计算机。用户的资料在重新启动后不会丢失。

创建包含注册表项的注册表 GPO

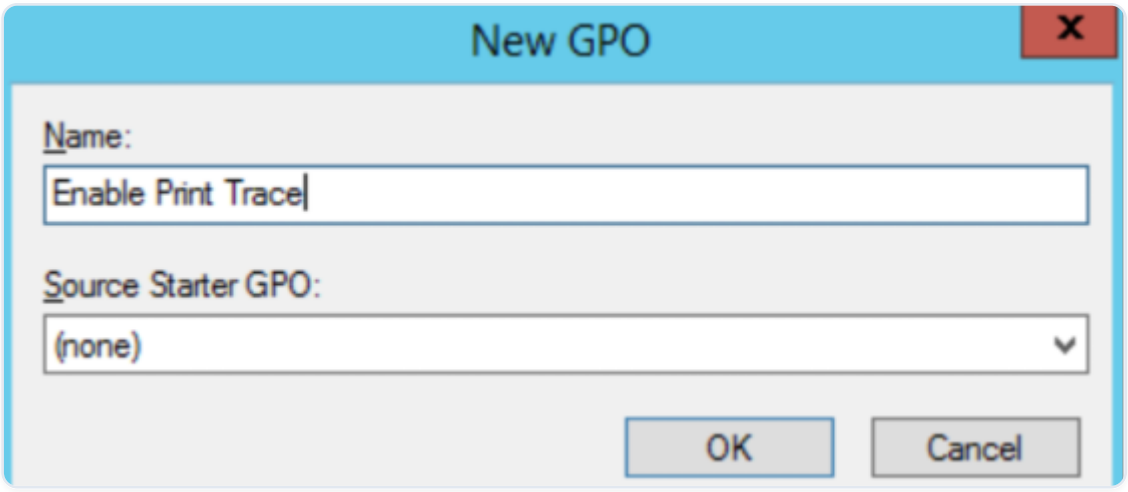
1. 打开组策略管理，然后右键单击“**组策略对象**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



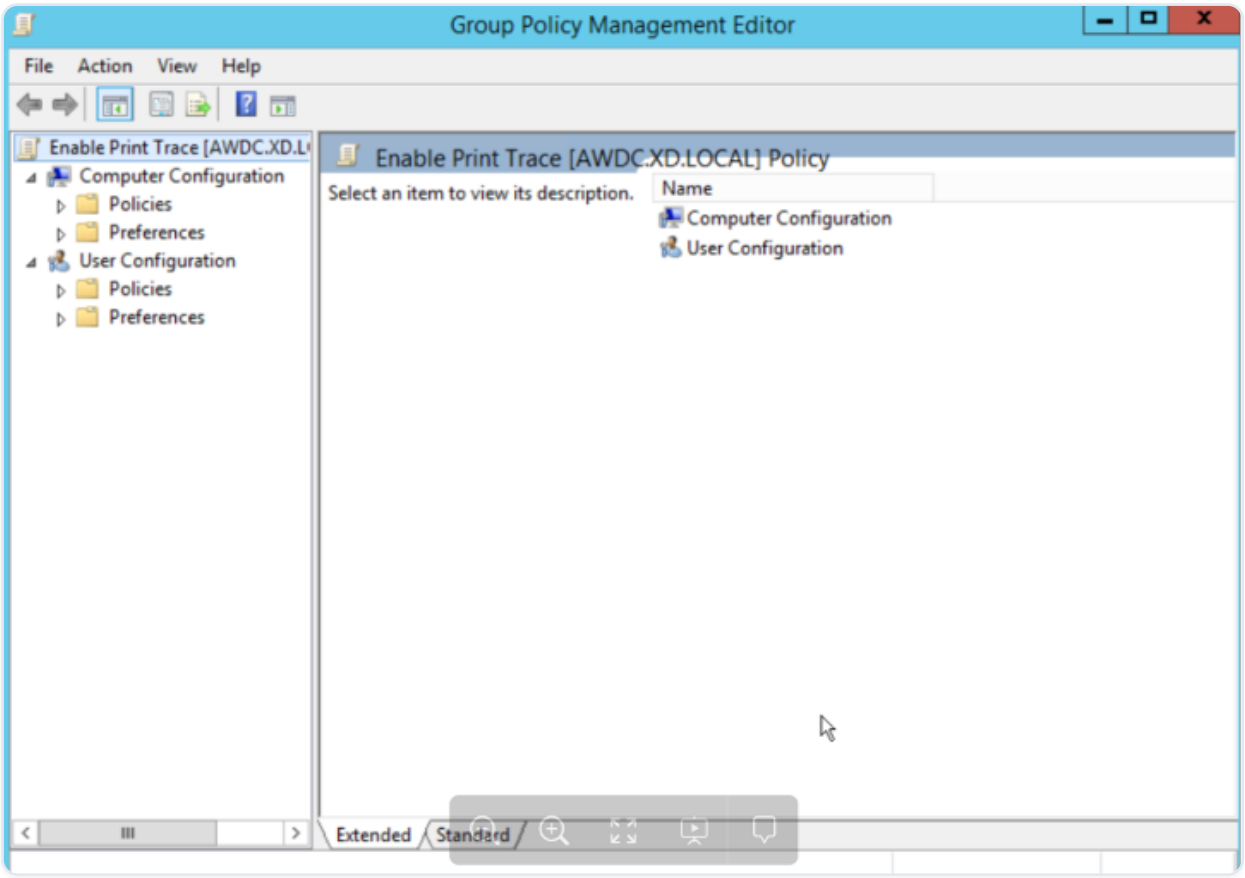
2. 在“**新建 GPO**”窗口中，在以下字段中输入值：

   - 名称：启用打印跟踪
   - 源启动 GPO：（无）



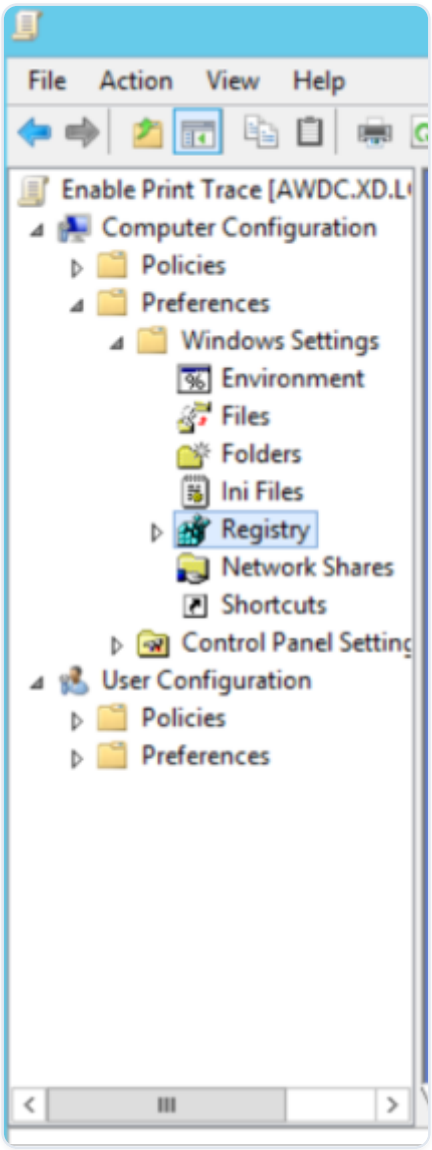
3. 选择“**确定**”。
4. 右键单击您创建的“**启用打印跟踪**”对象，然后选择“**编辑**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 在“**计算机配置**”列表中，选择“**首选项 > Windows 设置**”。

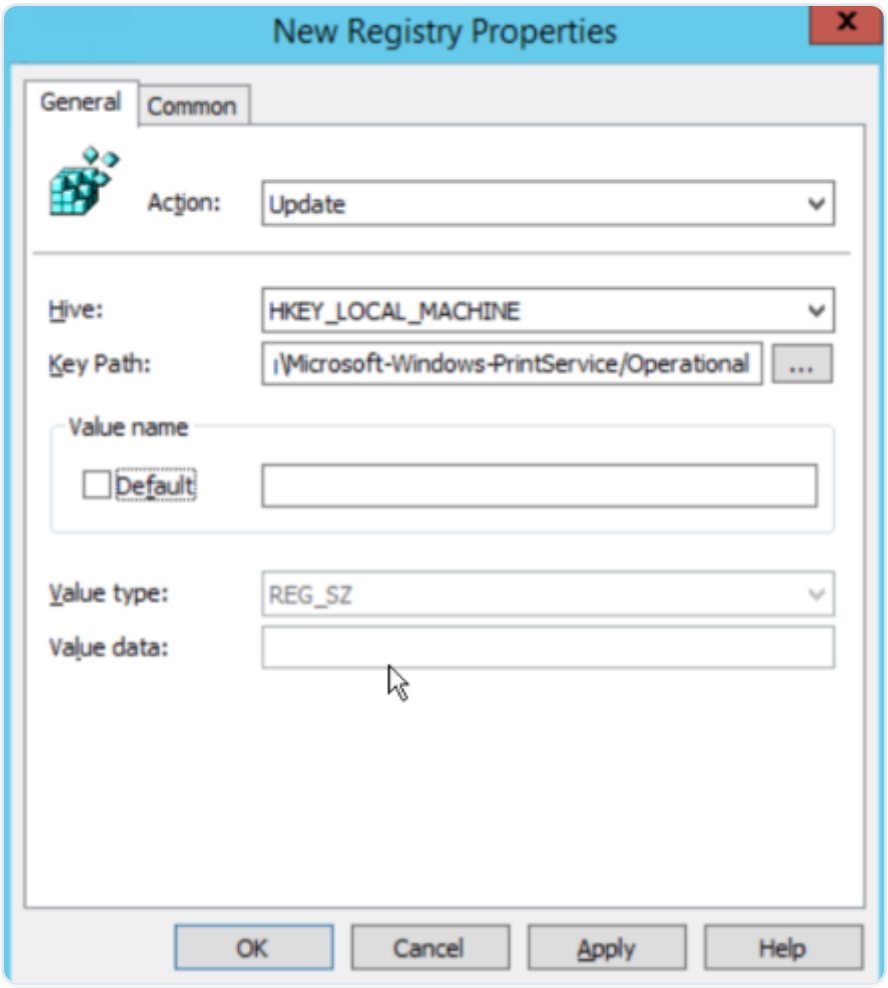
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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
   - 配置单元：HKEY_LOCAL_MACHINE
   - 密钥路径：SYSTEM\CurrentControlSet\Services\EventLog\Microsoft-Windows-PrintService/Operational

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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
    - 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

    注册表属性(/en-us/citrix-analytics/media/registry-attributes.png)

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），或者如果 VDA 是其一部分，则选择组织单位（例如 - VDA-OU）。
2. 右键单击域 (xd.local) 或组织单位 (VDA-OU) 并选择**链接现有 GPO**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

链接现有 GPO(/en-us/citrix-analytics/media/link-an-existing-gpo.png)

3. 在**选择 GPO** 对话框中，选择启用打印跟踪并选择**确定**。

   启用打印跟踪 GPO(/en-us/citrix-analytics/media/enable-print-trace-gpo.png)

4. 验证**启用打印跟踪 GPO**已链接到组织单位。

   已链接的启用打印跟踪 GPO(/en-us/citrix-analytics/media/enable-print-trace-gpo-linked.png)

注意

- 当您重新启动 VDA 时，队列中的任何事件都将丢失，并且在 Citrix Analytics 中不可用。
- 此重新启动对单会话 VDA 的影响较小，因为在给定时间只有一个会话可以处于活动状态，因此事件数量较少。
- 此重新启动对多会话 VDA 的影响较大，因为在重新启动期间所有活动会话都将终止，并且队列中的事件将丢失。

启用 Citrix DaaS 的剪贴板遥测

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剪贴板操作是否被允许。

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

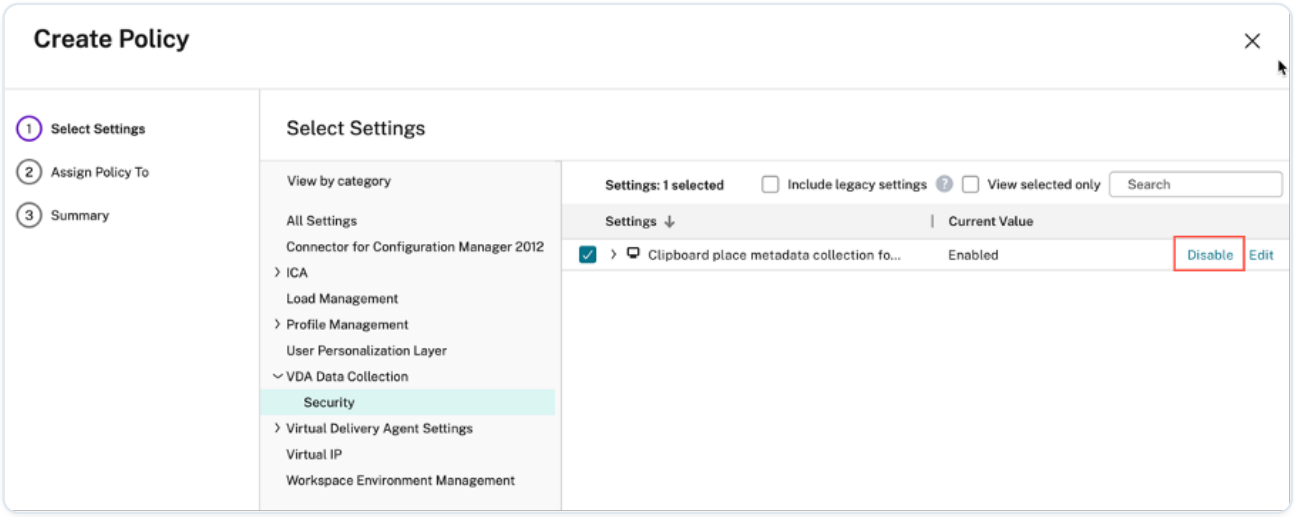
- 默认情况下，这些剪贴板日志的收集和传输在虚拟投递代理 (VDA) 上是启用的。
- 此配置仅适用于 Windows VDA。

先决条件

- 您的 VDA 版本必须与 Citrix Virtual Apps and Desktops 7 2305 或更高版本的基线版本相同。有关详细信息，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**”设置未配置为禁用状态。有关详细信息，请参阅 客户端剪贴板重定向。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以使用“**用于安全监控的剪贴板位置元数据收集**”策略来启用或禁用剪贴板遥测。默认情况下，此策略是启用的。要禁用，您必须转到“**策略**”页面 > 在“**VDA 数据收集**”下选择“**安全**”> 勾选该策略 > 单击“**禁用**”。



有关详细信息，请参阅 用于安全监控的剪贴板位置元数据收集。

开启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。您也可以从“应用程序和桌面”站点卡停止数据处理。此选项适用于 Director 和 Workspace 应用程序这两个数据源。

要再次启用数据处理，请单击“**开启数据处理**”。

微软活动目录和 Azure 活动目录集成

注意：

自 2023 年 7 月起，Microsoft 已将 Azure Active Directory (Azure AD) 更名为 Microsoft Entra ID。在本文档中，所有提及 Azure Active Directory、Azure AD 或 AAD 的地方均指 Microsoft Entra ID。

连接您的 Active Directory 或 Azure Active Directory，并将您组织域中的用户详细信息和用户组导入到 Citrix Analytics for Security。

此集成通过用户身份详细信息（例如职位、组织、办公地点、电子邮件和联系方式）增强了 Citrix Analytics for Security 中的用户配置文件。在用户配置文件页面上，您可以查看这些用户详细信息，这有助于您进行风险调查和分析。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

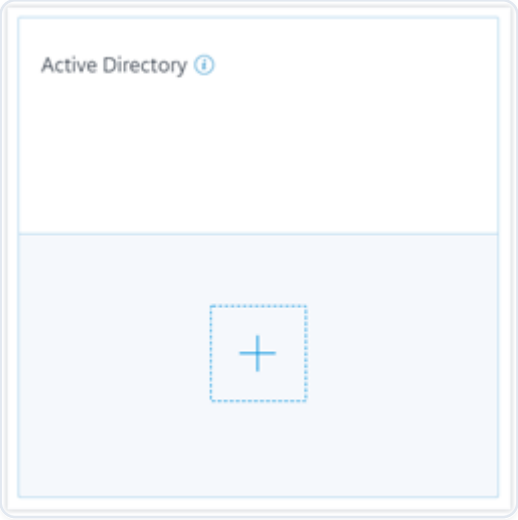
先决条件

- 如果您想将 Active Directory 与 Citrix Analytics for Security 连接，请确保您的 Active Directory 已首先连接到您的 Citrix Cloud 帐户。有关更多信息，请参阅将 Active Directory 连接到 Citrix Cloud。
- 如果您想将 Azure Active Directory 与 Citrix Analytics for Security 连接，请确保您的 Azure Active Directory 已首先连接到您的 Citrix Cloud 帐户。有关更多信息，请参阅将 Azure Active Directory 连接到 Citrix Cloud。

连接微软活动目录

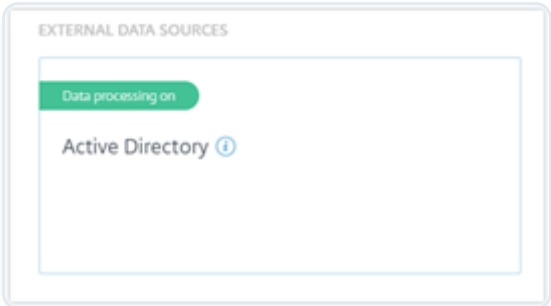
要将您的 Active Directory 连接到 Citrix Analytics for Security，请执行以下操作：

1. 转到 **设置** > **数据源** > **安全**，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 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，Active Directory 站点卡显示 **数据处理已开启**。



“**数据处理已开启**”状态表示已发现 Active Directory，并且正在从您的 Active Directory 中获取用户信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

连接微软 Azure 活动目录

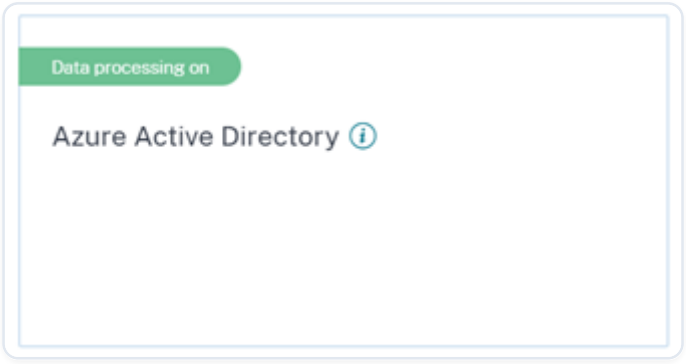
要将 Azure Active Directory 连接到 Citrix Analytics，请执行以下操作：

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



3. Citrix Analytics 提示您将 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。

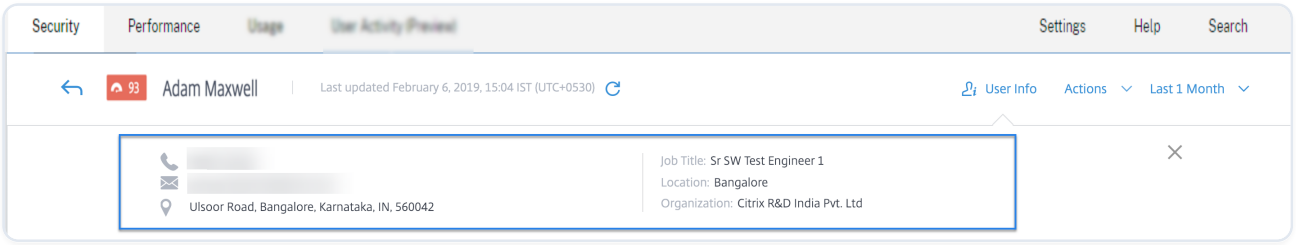
将 Azure Active Directory 连接到 Citrix Cloud 帐户后，Citrix Analytics 会自动发现此新数据源。在 **数据源** 页面上，**Azure Active Directory** 站点卡显示“**数据处理已开启**”。此状态表示已发现 Azure Active Directory，并且正在从您的 Azure Active Directory 中获取用户信息。



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，您可以在用户配置文件页面上查看其职位、组织、电子邮件和联系电话。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Microsoft Graph 安全集成

Microsoft Graph Security 是一个外部数据源，它聚合来自多个安全提供程序的数据。它还提供对用户清单数据的访问。

Citrix Analytics 目前支持 Microsoft Graph Security 中的以下安全提供程序：

- Azure AD 身份保护
- 适用于终结点的 Microsoft Defender

有关安全提供程序的更多信息，请参阅以下链接：

- 对于 **Azure AD 身份保护**：`<https://docs.microsoft.com/zh-cn/azure/active-directory/reports-monitoring/concept-risk-events>`
- 对于 **适用于终结点的 Microsoft Defender**：`<https://docs.microsoft.com/zh-cn/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection>`

要载入 Microsoft Graph Security 数据源，您需要从 Microsoft 身份平台代表租户获取所需的权限。

先决条件

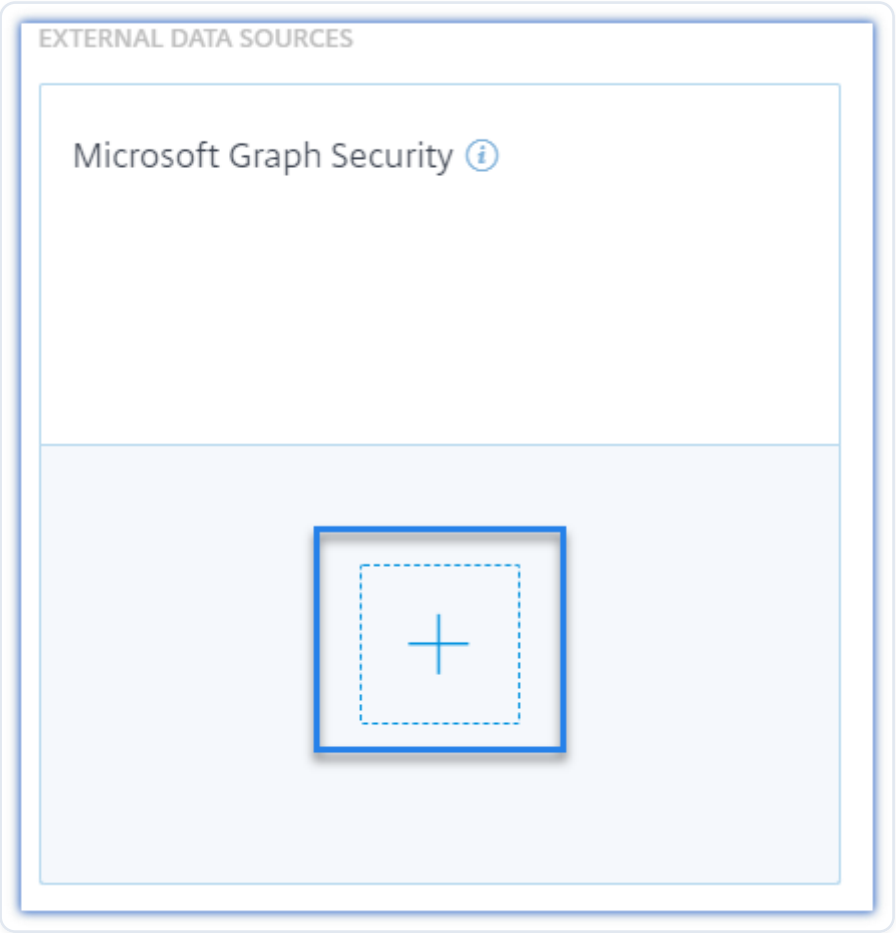
在开始载入 Microsoft Graph Security 数据源之前，请确保：

- 管理员正在使用 Azure AD Identity Protection（Azure AD Premium P2 的一部分）安全提供程序。
- 最终用户已使用工作或学校帐户登录到 Microsoft Store。

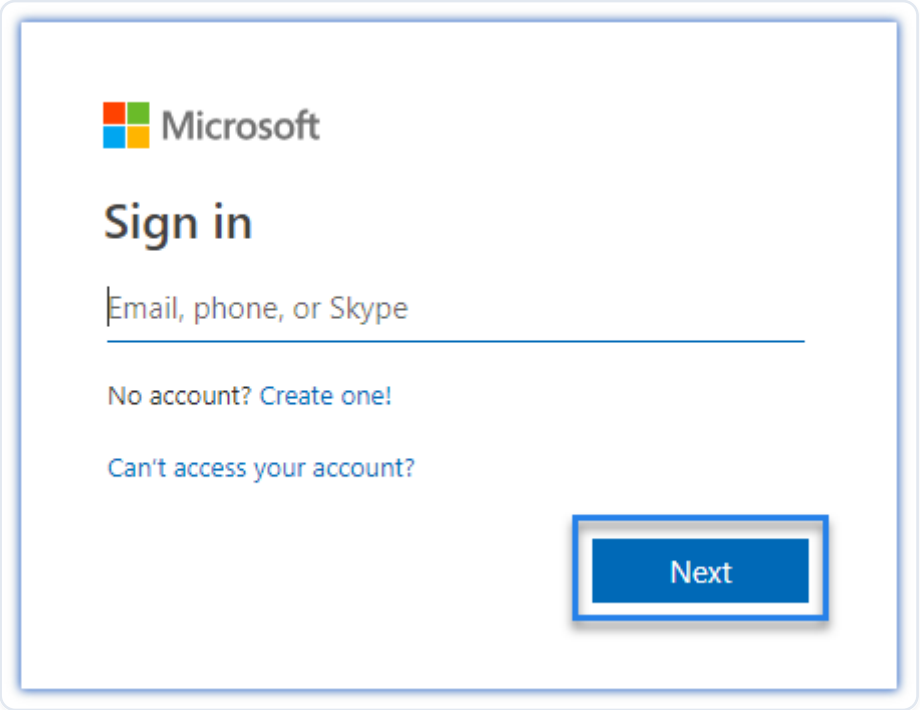
载入 Microsoft Graph Security 实例

1. 转到“**设置**”>“**数据源**”>“**安全**”，然后导航到“**外部数据源**”部分。
2. 点击 Microsoft Graph Security 站点卡上的加号 (**+**)。您将被重定向到授权端点。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

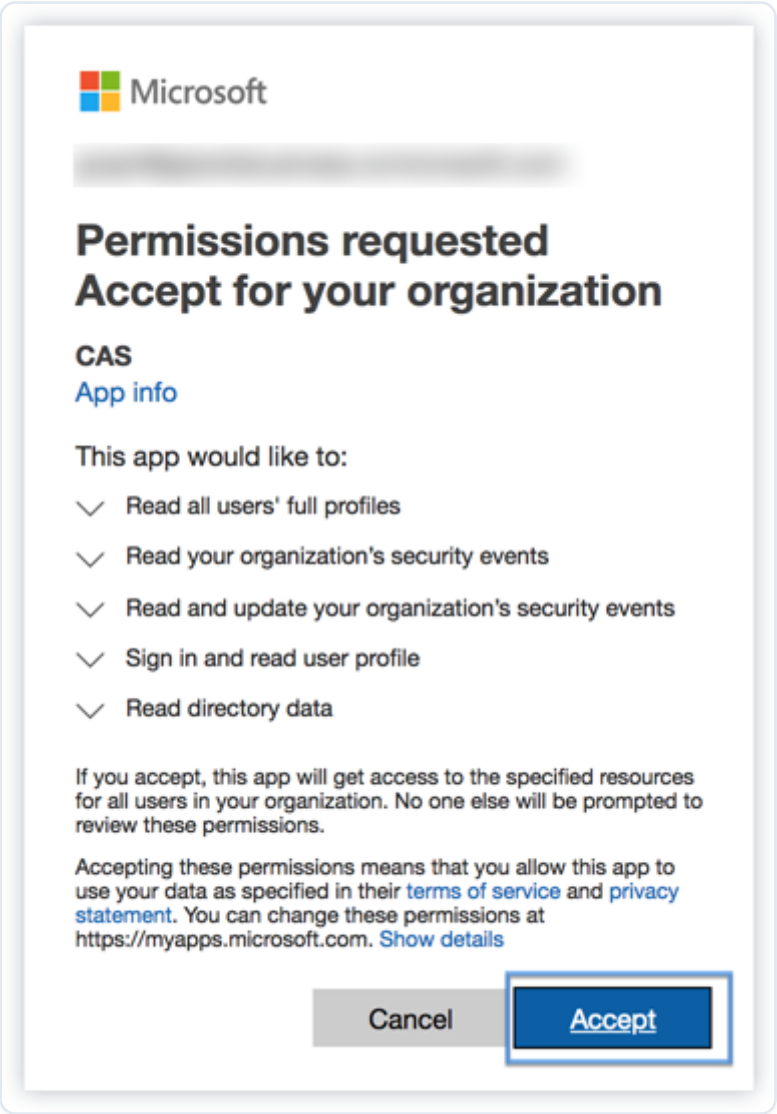


3. 在 **Microsoft** 窗口中，使用您的 Azure 登录凭据登录以注册帐户。或者，选择一个现有帐户。
4. 单击**下一步**。



5. 单击**接受**。您将被重定向到“数据源”页面。Microsoft Graph Security 数据源现在已链接到您的 Citrix Cloud™ 帐户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

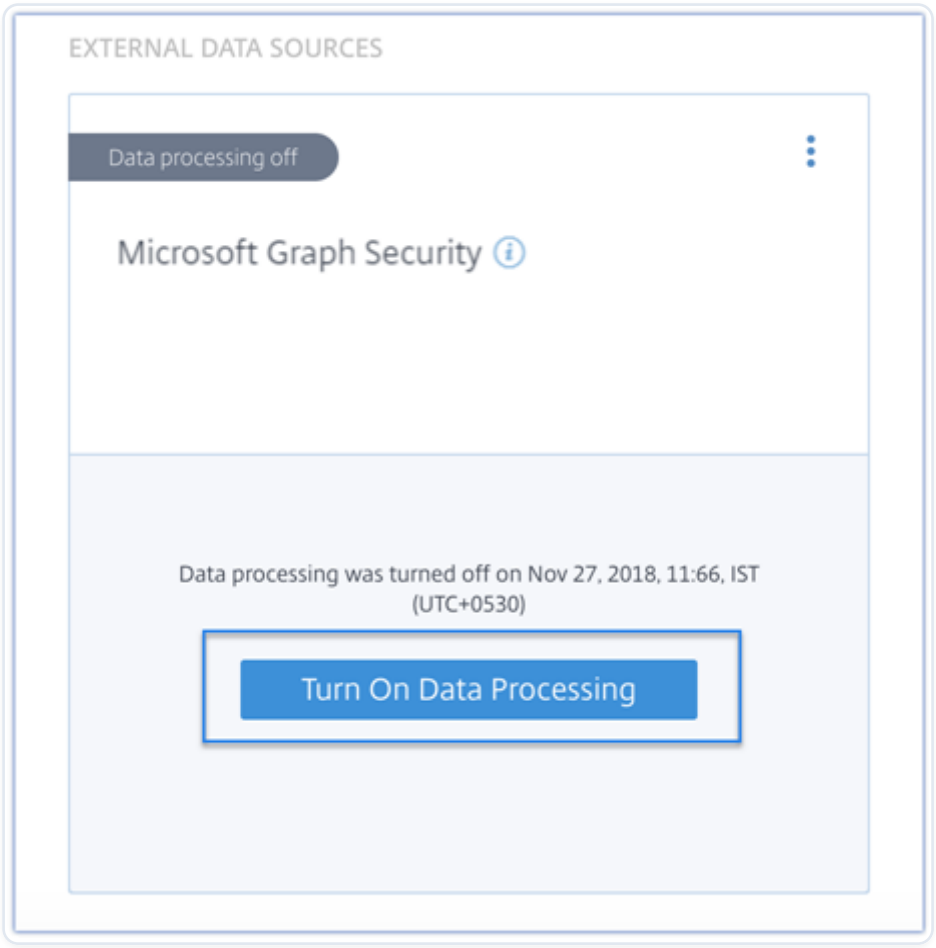


启用或禁用数据处理

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

您可以通过在站点卡上选择**启用数据处理**来再次启用数据处理。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关 Microsoft Graph Security 风险指标的信息，请参阅Microsoft Graph Security 风险指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全信息和事件管理 (SIEM) 集成

注意

联系 mailto:CAS-PM-Ext@cloud.com 以请求 SIEM 集成协助、将数据导出到 SIEM 并提供反馈。

将 Citrix Analytics for Security™ 与您的 SIEM 服务集成，并将用户数据从 Citrix IT 环境导出到您的 SIEM。将导出的数据与 SIEM 中可用的数据关联起来，以深入了解组织的安全状况。

此集成提升了您的 Citrix Analytics for Security 和您的 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。
- 在一个集中位置查看安全警报。
- 采用集中式方法检测潜在安全威胁，以实现组织风险分析功能，例如风险指标、用户配置文件和风险评分。
- 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。

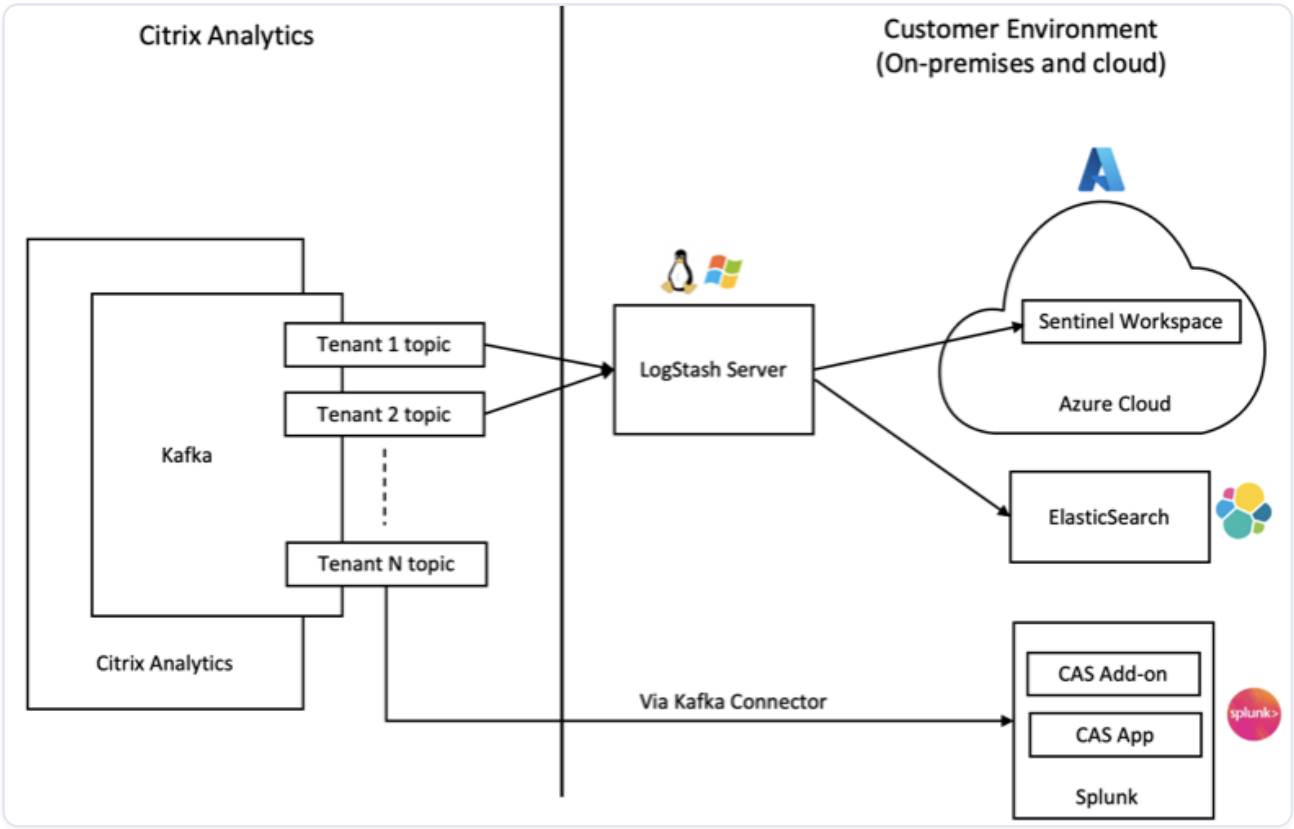
SIEM 集成架构

您的 SIEM 集成连接到部署在 Citrix Analytics for Security 云上的北向 Kafka。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，您可以连接并将数据拉取到所选的 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 Citrix Analytics for Security 中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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



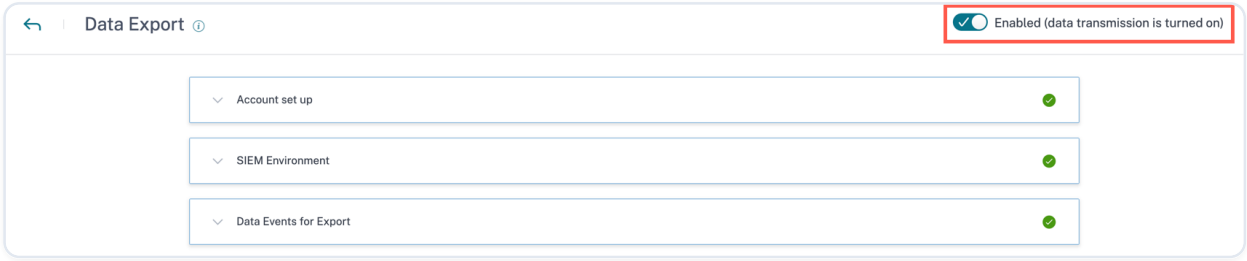
开启或关闭数据传输

要停止从 Citrix Analytics for Security 传输数据：

1. 转到 **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，请开启切换按钮。

设置 SIEM 环境

要将数据导出到 SIEM，您必须执行以下操作：

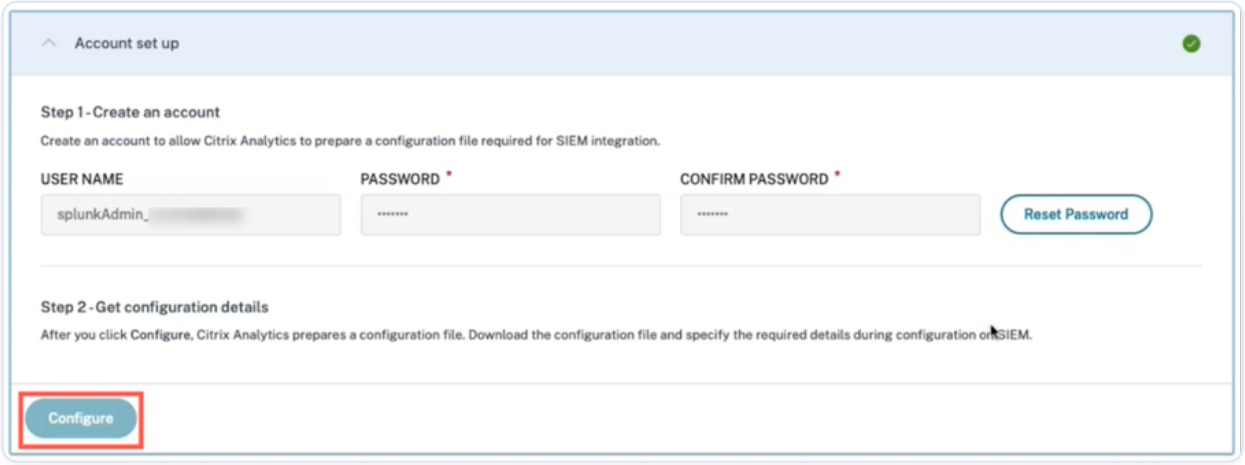
- 设置您的 Kafka 帐户和身份验证凭据

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 下载预填充配置并设置 SIEM 环境
- 用于导出的数据事件

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。设置帐户后，将生成您的 Kafka 详细信息。生成配置文件时，这些详细信息会自动嵌入。



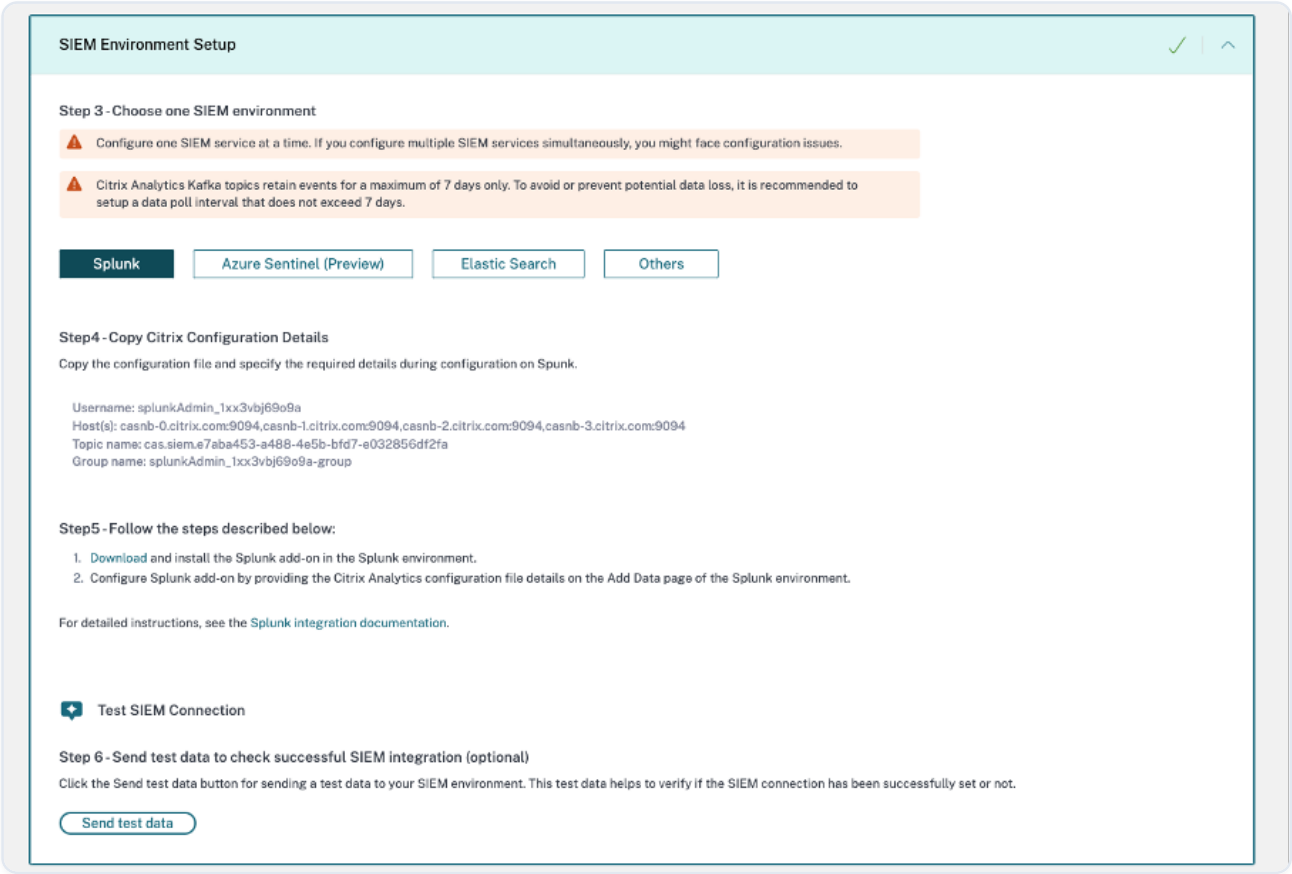
2. 单击**配置**以生成配置文件。配置文件包含 Kafka 端点、您的特定订阅主题和组 ID 等详细信息。此外，它还会预配置完成身份验证和数据流所需的 Kafka 和 SSL 属性。

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：

- 思普朗克
- 微软 Sentinel
- 弹性搜索
- 其他使用基于 Kafka 或 Logstash 的数据连接器的 SIEM

© 1997–2026 Citrix Systems, Inc. All rights reserved.



从 Citrix Analytics for Security 导出到您的 SIEM 服务的数据事件

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）将开始流向您的 SIEM 部署。风险洞察数据包含用户风险评分、用户配置文件和风险指标警报。这些数据由 Citrix Analytics 机器学习算法、用户行为分析以及用户事件生成。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，从启用了 Citrix Analytics for Security 的产品数据源导出用户事件。当您在 Citrix 环境中执行任何活动时，会生成数据源事件。导出的事件是自助服务视图中可用的未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进一步用于更深入的威胁分析、创建新仪表板，并与您的安全和 IT 基础设施中的其他非 Citrix 数据源事件相关联。

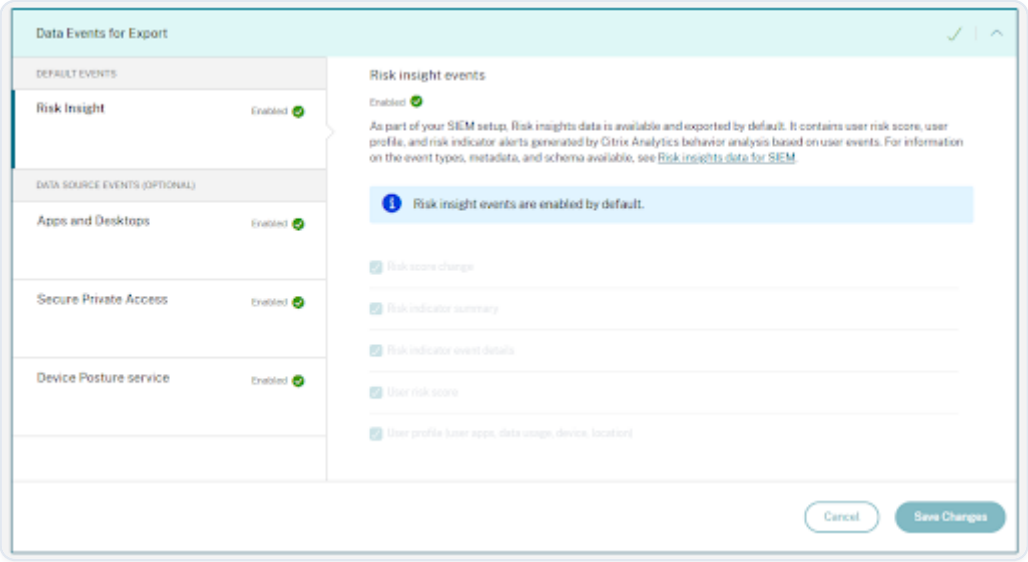
   目前，Citrix Analytics for Security 会将用户事件发送到您的 SIEM，用于以下数据源：Citrix Virtual Apps and Desktops™、Secure Private Access 和 Device Posture 服务。

   有关可用的事件类型、元数据和架构的信息，请参阅 数据源事件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

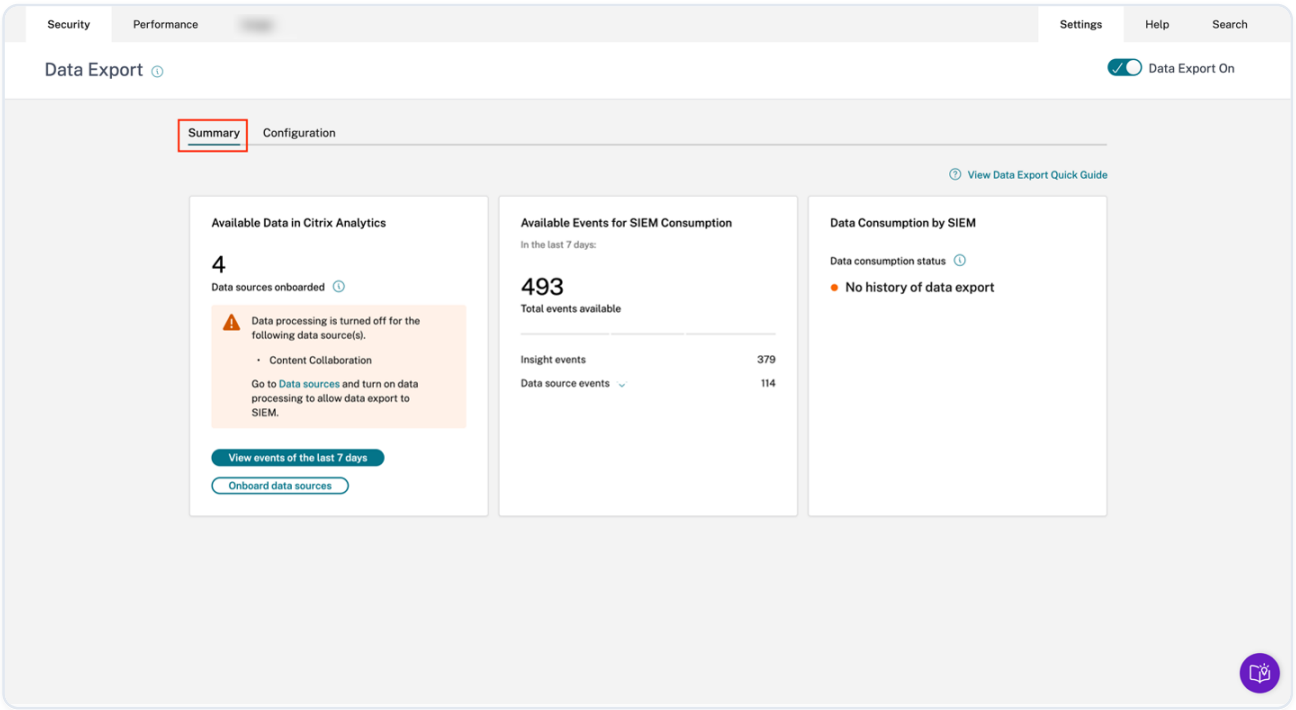
注意

使用 Logstash 数据代理的客户，建议从 Citrix Analytics for Security 门户下载最新的配置文件，并在 Logstash 服务部署上进行更新。这可确保创建正确的数据源事件表，并且事件现在可在 SIEM 索引中可用。



SIEM 集成故障排除

“安全数据导出”视图包含一个**摘要**选项卡，可帮助管理员排查其与 Citrix Analytics 的 SIEM 集成问题。**摘要**仪表板通过引导他们通过有助于故障排除过程的检查点，提供数据运行状况和流的可见性。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

要了解有关此功能的更多信息，请参阅 排查数据导出问题。

Splunk 集成

将 Citrix Analytics for Security 与 Splunk 集成，以导出并(/zh-cn/security-analytics/siem-integration/entity-data-model.html)您的 Citrix IT 环境中的用户数据到 Splunk，从而深入了解您组织的安全状况。

有关集成优势以及发送到 SIEM 的已处理数据类型，请参阅(/zh-cn/security-analytics/siem-integration.html)。

为了全面了解 Splunk 部署方法并采用有效的规划策略，请参阅 采用 Citrix® 托管在 Splunk 上的分析应用程序的 Splunk 架构 文档。

实现 Citrix Analytics for Security™ 与 Splunk 的集成

请遵循以下指南将 Citrix Analytics for Security 与 Splunk 集成：

- (#data-export)。Citrix Analytics for Security 创建一个 Kafka 通道，并导出风险洞察和数据源事件。Splunk 从该通道检索此风险情报。
- 获取 Citrix Analytics 上的配置。为您的预定义帐户创建身份验证密码。Citrix Analytics for Security 会准备一个配置文件，供您配置适用于 Splunk 的 Citrix Analytics 附加组件。
- (#download-and-install-citrix-analytics-add-on-for-splunk)。使用 Splunkbase 或 Splunk Cloud 下载 **Citrix Analytics Add-on for Splunk** 以完成安装过程。
- (#configure-citrix-analytics-add-on-for-splunk)。使用 Citrix Analytics for Security 提供的配置详细信息设置数据输入，并配置适用于 Splunk 的 Citrix Analytics 附加组件。

Citrix Analytics 配置文件准备好后，请参阅：

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

配置适用于 Splunk 的 Citrix Analytics 附加组件后，请参阅：

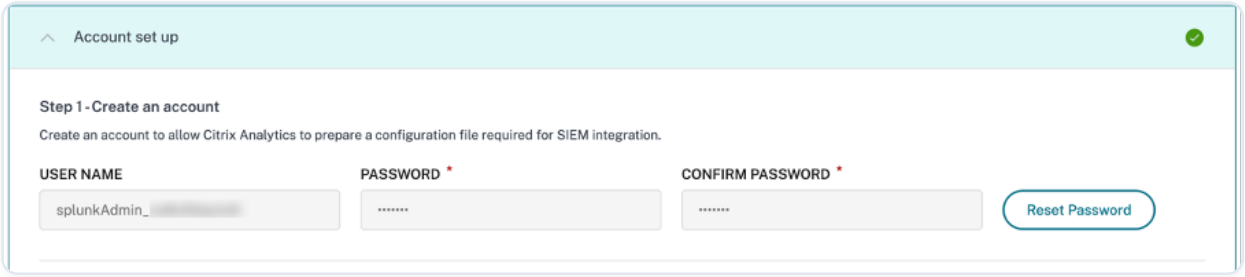
- (#how-to-consume-events-in-your-splunk-environment)
- 如何配置适用于 Splunk 的 Citrix Analytics 应用程序

数据导出

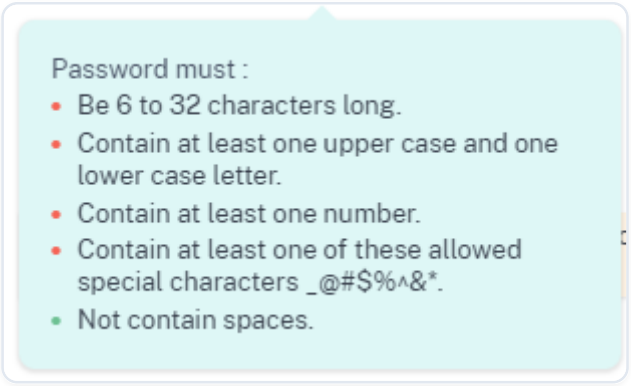
1. 转到“**设置**”>“**数据导出**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 在“**帐户设置**”部分中，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。

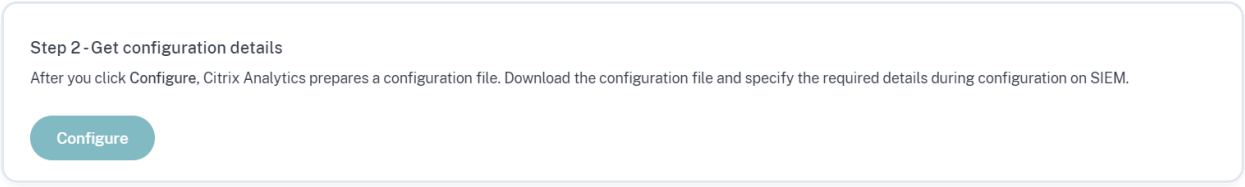


3. 确保密码满足以下条件：



4. 选择“**配置**”。

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



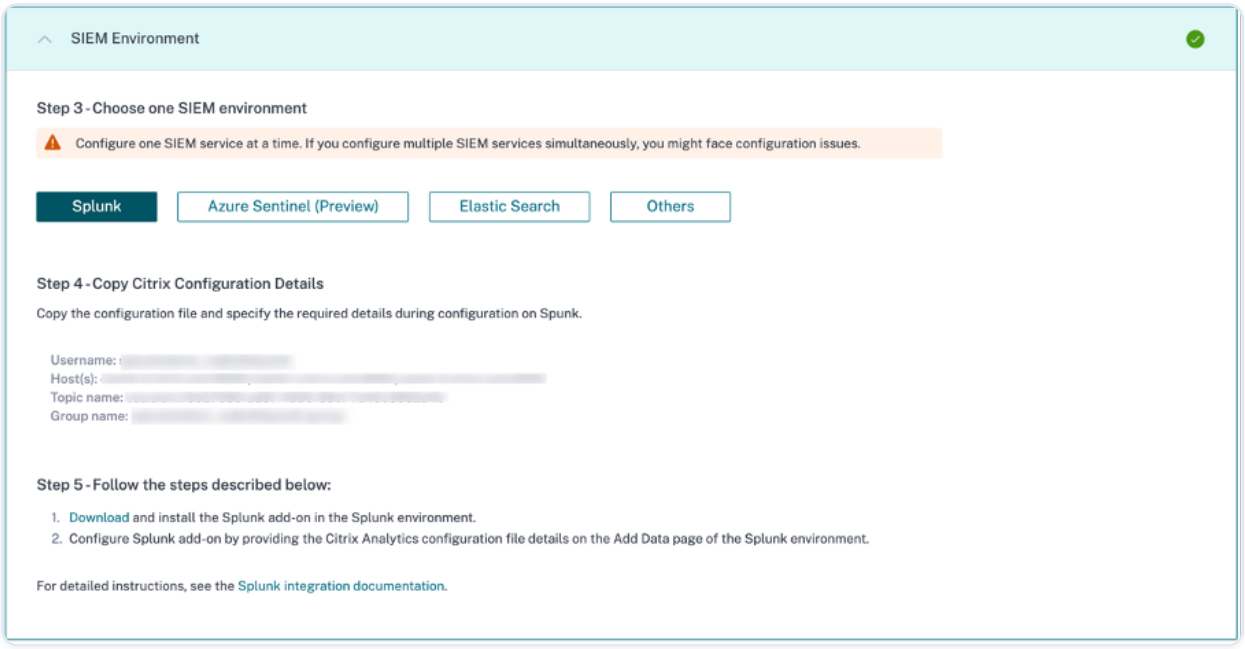
5. 选择“**Splunk**”。
6. 复制配置详细信息，其中包括用户名、主机、Kafka 主题名称和组名称。

   您需要这些详细信息才能在后续步骤中配置适用于 Splunk 的 Citrix Analytics 附加组件。

重要

这些详细信息很敏感，您必须将其存储在安全位置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

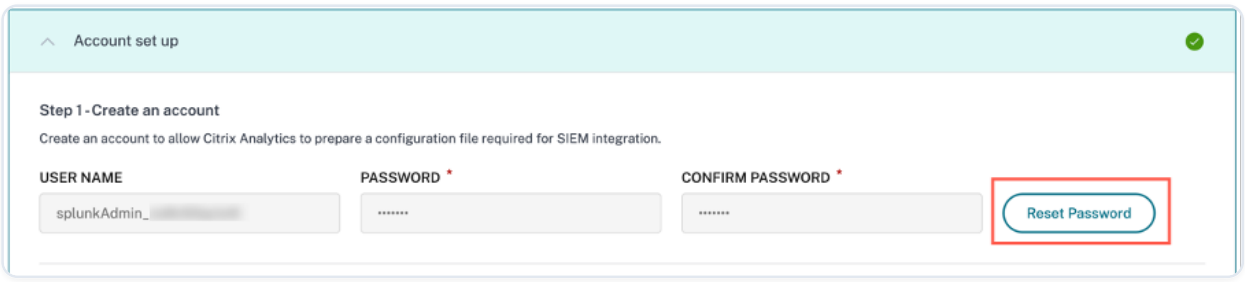


要为 Splunk 集成生成候选数据，请为至少一个数据源启用数据处理，或 使用测试事件生成功能。这有助于 Citrix Analytics for Security 启动 Splunk 集成过程。

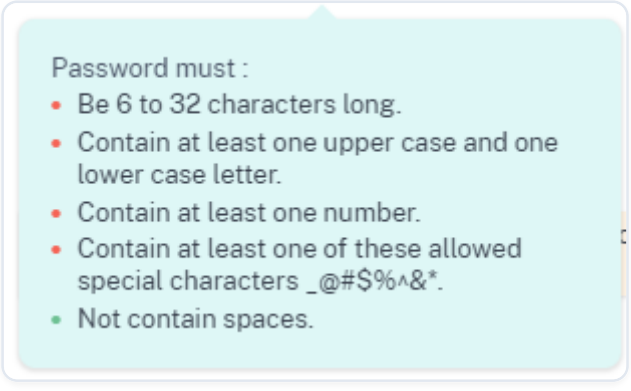
重置密码功能

如果您想在 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**”。

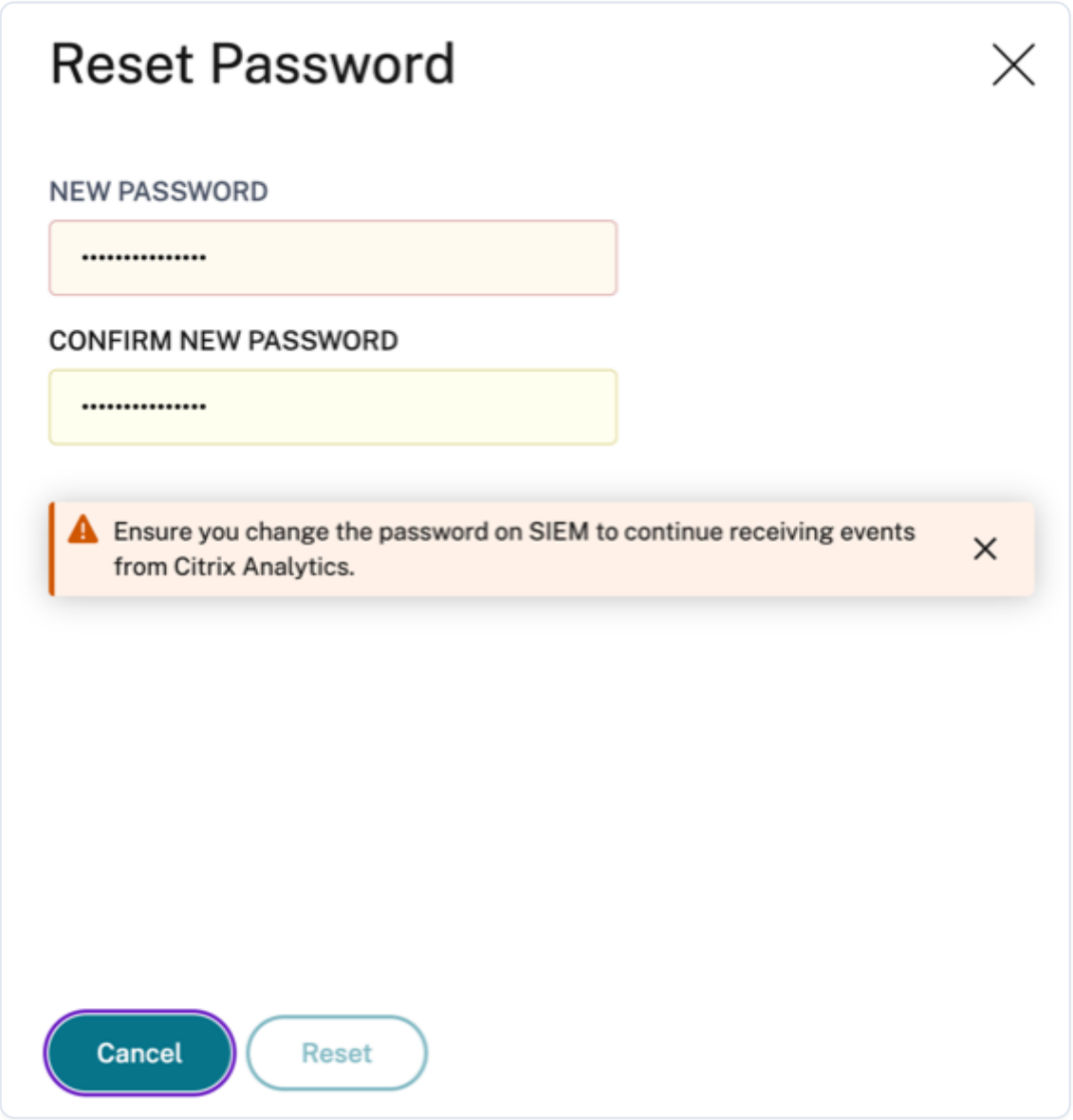


2. 在“**重置密码**”窗口中，在“**新密码**”和“**确认新密码**”字段中指定更新后的密码。请遵循显示的密码规则。



3. 单击“**重置**”。配置文件的准备工作已启动。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意

重置配置密码后，请务必在 Splunk 环境的“**添加数据**”页面上设置数据输入时更新新密码。这有助于 Citrix Analytics for Security 继续向 Splunk 传输数据。

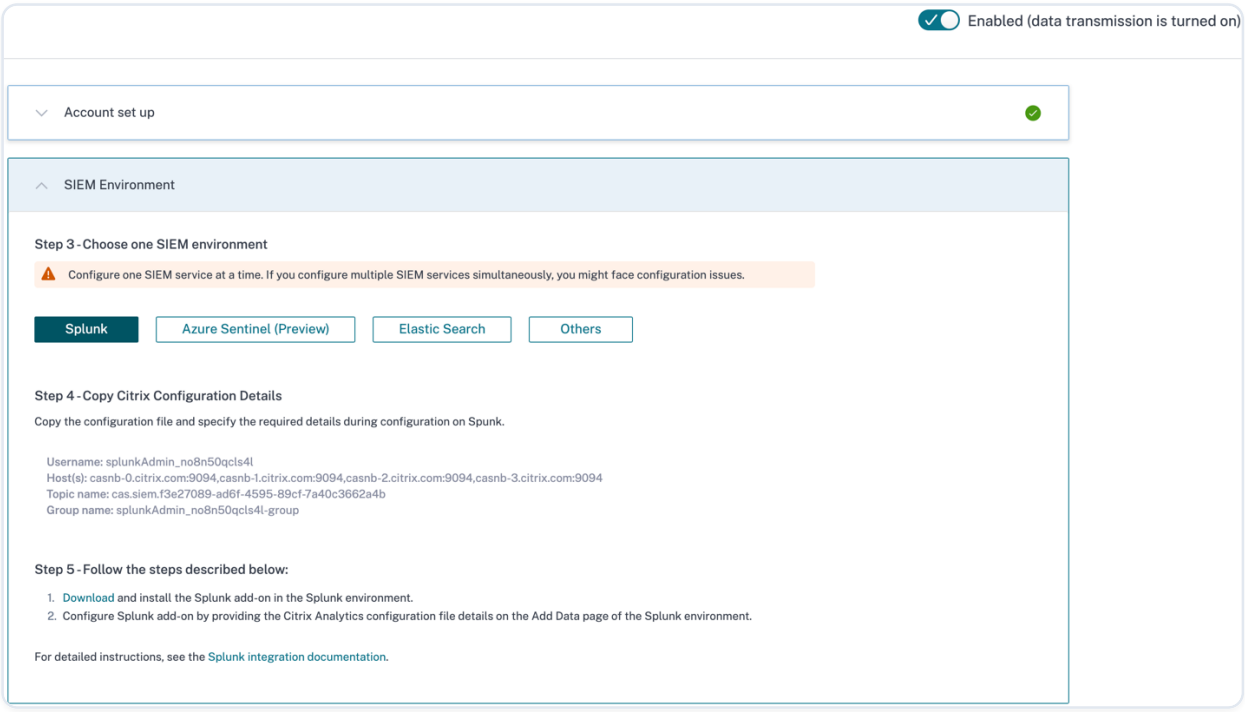
启用或禁用数据传输

Citrix Analytics 到 Splunk 数据导出的数据传输默认情况下处于启用状态。

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



要再次启用数据传输，请打开切换按钮。

适用于 Splunk 的 Citrix Analytics 附加组件

您可以选择在以下任一平台上安装附加应用程序：

- Splunk Enterprise（重型转发器）
- Splunk 云平台

适用于 Splunk 的 Citrix Analytics 附加组件（本地/企业版）

支持的版本

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

- CentOS Linux 7 及更高版本
- Debian GNU/Linux 10.0 及更高版本
- Red Hat Enterprise Linux Server 7.0 及更高版本
- Ubuntu 18.04 LTS 及更高版本

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

- Citrix 建议使用上述操作系统的最新版本，或 仍受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。

先决条件

- **适用于 Splunk 的 Citrix Analytics 附加组件**连接到 Citrix Analytics for Security 上的以下端点。请确保这些端点在您的网络允许列表中。

端点	美国区域	欧盟区域	亚太南部区域
Kafka 代理	`casnb-0.citrix.com:9094`	`casnb-eu-0.citrix.com:9094`	`casnb-aps-0.citrix.com:9094`
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`	`casnb-aps-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`		

注意

尝试使用端点名称而不是 IP 地址。端点的公共 IP 地址可能会更改。

下载并安装适用于 Splunk 的 Citrix Analytics 附加组件

您可以选择使用 **从文件安装应用程序** 或在 Splunk 环境中安装附加组件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

从文件安装应用程序

1. 转到 Splunkbase。
2. 下载适用于 Splunk 的 Citrix Analytics 附加组件文件。
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**
>
> - 如果您有旧版本的附加组件，请选择“**升级应用程序**”以覆盖它。
> - 如果您正在从早于 2.0.0 的版本升级 **Citrix Analytics Add-on for Splunk**，则必须删除附加组件安装文件夹的 */bin* 文件夹中包含的以下文件和文件夹，并重新启动您的 Splunk Forwarder 或 Splunk Standalone 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 内部安装应用程序

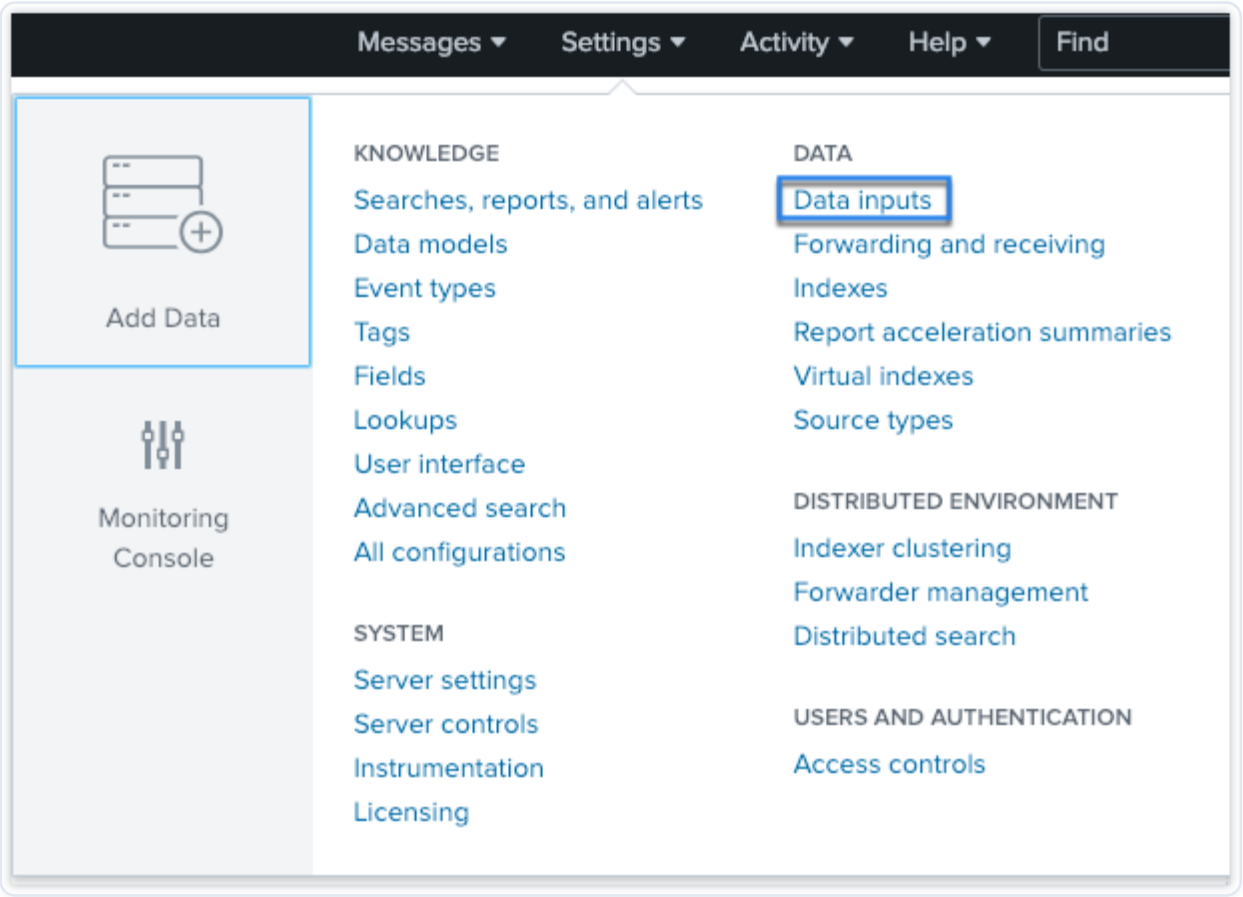
1. 在 Splunk Web 主页上，单击“**+查找更多应用程序**”。
2. 在“浏览更多应用程序”页面上，搜索 **Citrix Analytics Add-on for Splunk**。
3. 单击应用程序旁边的“**安装**”。
4. 验证应用程序是否显示在**应用程序**列表中。

配置适用于 Splunk 的 Citrix Analytics 附加组件

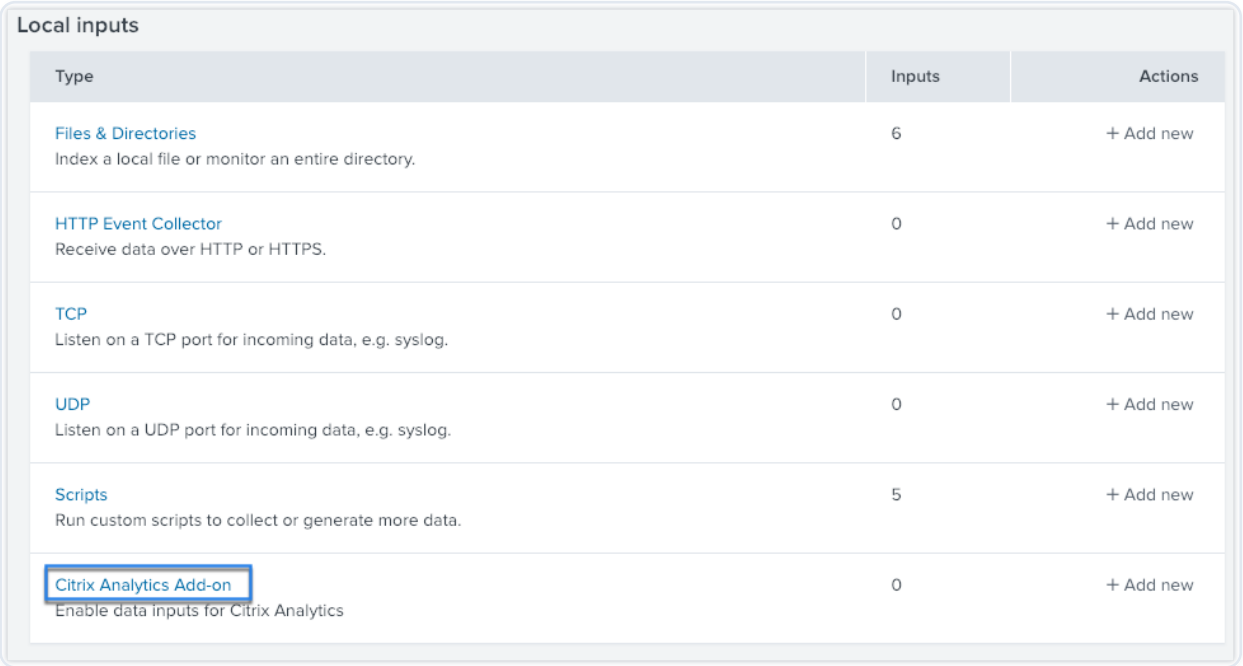
使用 Citrix Analytics for Security 提供的配置详细信息配置适用于 Splunk 的 Citrix Analytics 附加组件。成功配置附加组件后，Splunk 开始从 Citrix Analytics for Security 接收事件。

1. 在 Splunk 主页上，转到**设置** > **数据输入**。

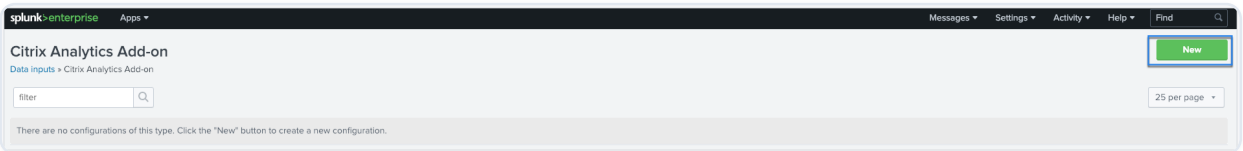
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 在**本地输入**部分中，单击**Citrix Analytics 附加组件**。

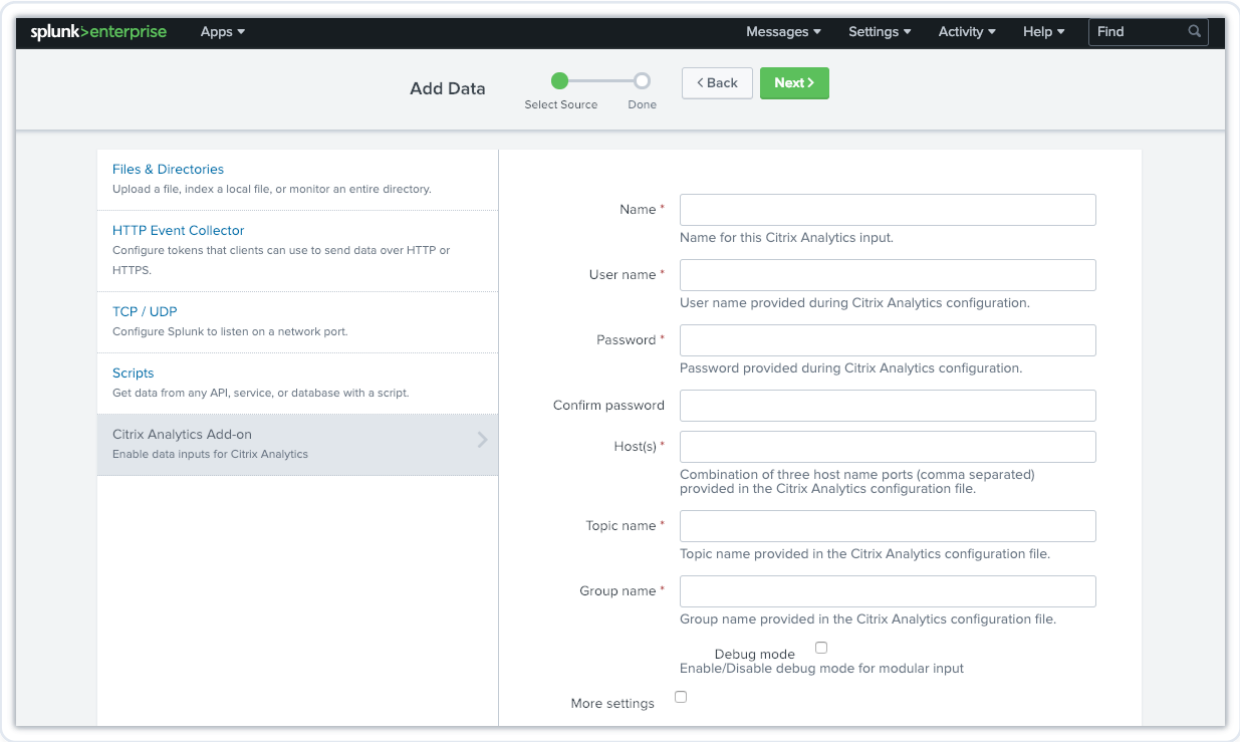


3. 单击**新建**。

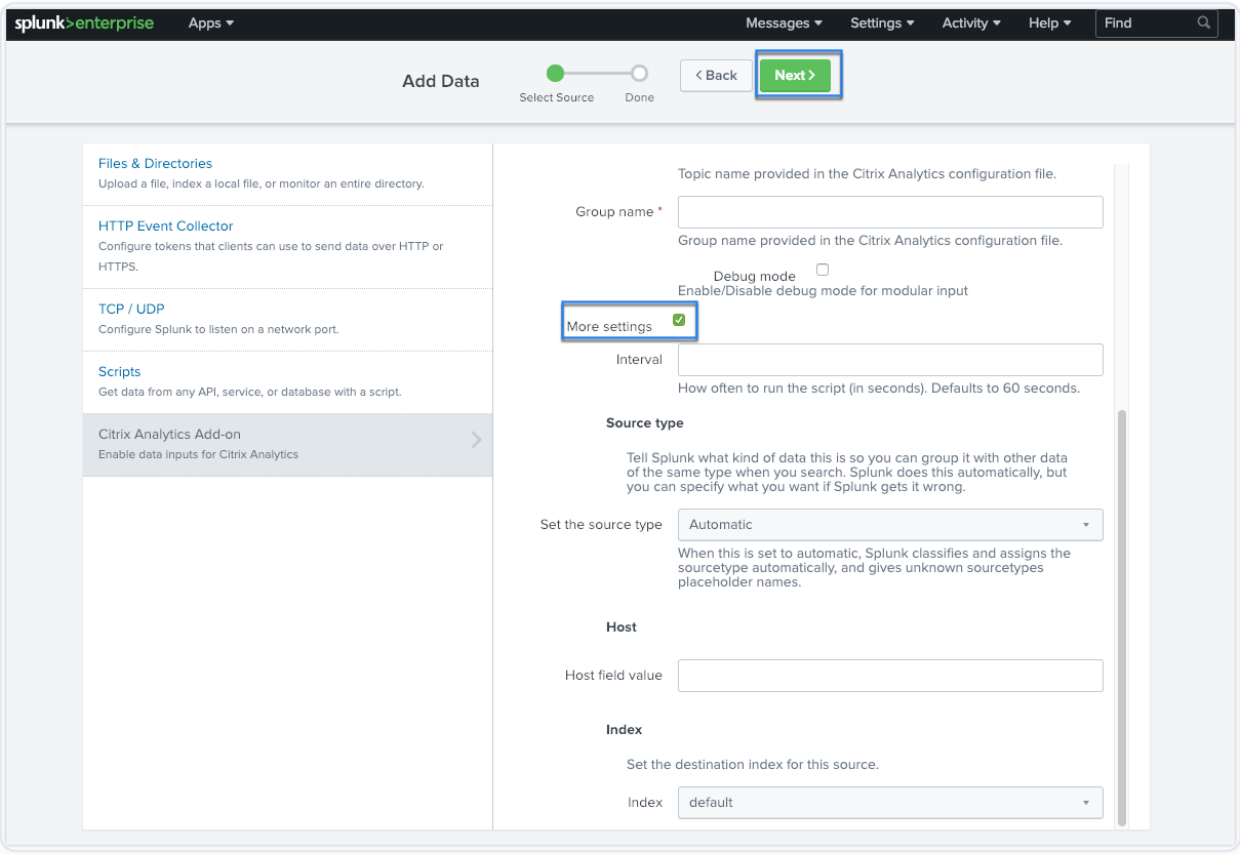


© 1997–2026 Citrix Systems, Inc. All rights reserved.

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，并且适用于 Splunk 的 Citrix Analytics 附加组件已成功配置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Splunk 的 Citrix Analytics 附加组件（云）

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。

先决条件

适用于 Splunk 的 Citrix Analytics 附加组件连接到以下 IP 和出站端口，以连接到 Citrix Analytics for Security。确保您的网络中允许以下 IP 和出站端口（取决于您的 Citrix Cloud™ 区域）。要配置这些 IP 和出站端口，请参阅“**使用管理配置服务 (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	欧盟地区	IP	出站端口	亚太南部地区	IP	出站端口
地址：casnb-0 citrix.com	20.242.21.84	9094	地址：casnb-eu-0 citrix.com	20.229.150.41	9094	域名：casnb-aps-0 citrix.com	20.211.0.214	9094
域名：casnb-1.citrix.com	20.98.232.61	9094	casnb-eu-1.citrix.com	20.107.97.59	9094	casnb-aps-1 citrix.com	20.211.38.102	9094
地址：casnb-2.citrix.com	20.242.21.108	9094	地址：casnb-eu-2.citrix.com	51.124.223.162	9094	域名：casnb-aps-2 citrix.com	20.211.36.180	9094
域名：casnb-3.citrix.com	20.242.57.140	9094						

注意

这些 IP 地址可能会轮换。请确保您的 IP 允许列表与 上面显示的最新的 IP 地址保持同步更新。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用管理配置服务 (ACS) 将 Citrix Analytics IP 地址和出站端口添加到 Splunk Cloud 允许列表

1. 根据您的 Citrix Cloud 区域，确定必须添加到允许列表中的 IP 地址。
2. 在 Splunk Cloud Platform 上启用管理配置服务 (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上的允许列表，并验证它们是否已成功添加。
5. 运行 cURL GET 和 POST 命令 以将出站端口添加到允许列表，并验证它们是否已成功添加。

下载并安装适用于 Splunk 的 Citrix Analytics 附加组件

1. 转到 **应用程序 > 查找更多应用程序 > 搜索适用于 Splunk 的 Citrix Analytics 附加组件**。

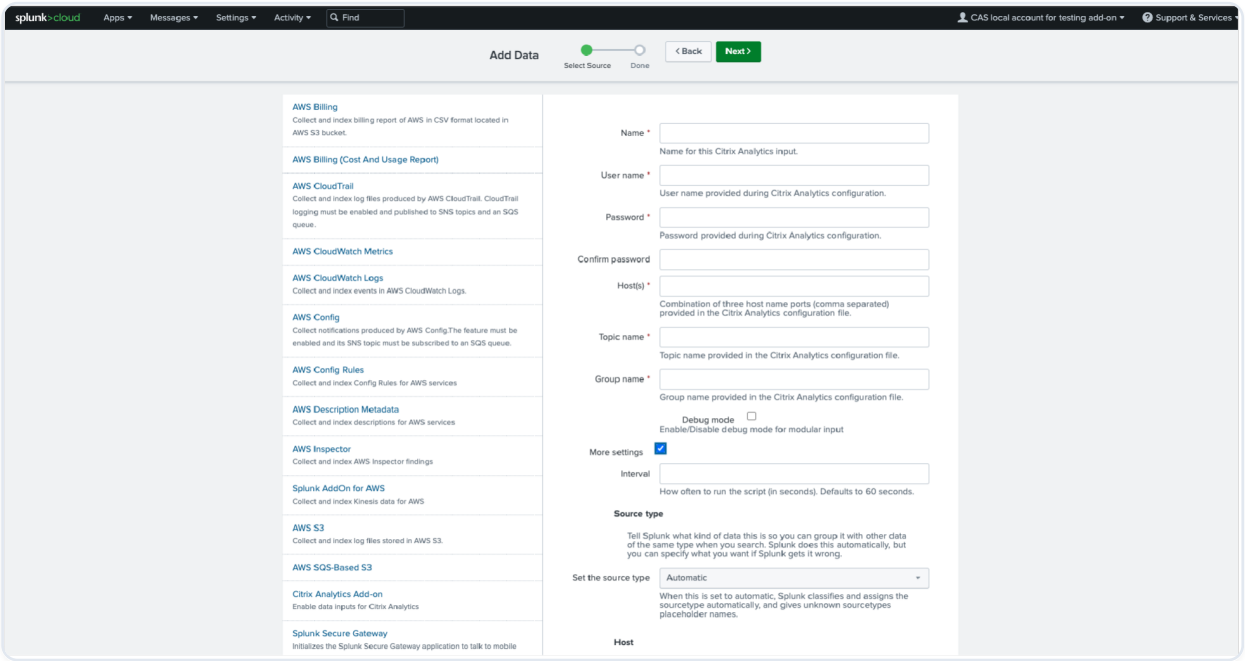
   (/en-us/citrix-analytics/media/add-on-for-splunk.png)
2. 安装应用程序。
3. 验证应用程序是否显示在“应用程序”列表中。

配置适用于 Splunk 的 Citrix Analytics 附加组件

1. 转到 **设置 > 数据输入 > Citrix Analytics 附加组件**。

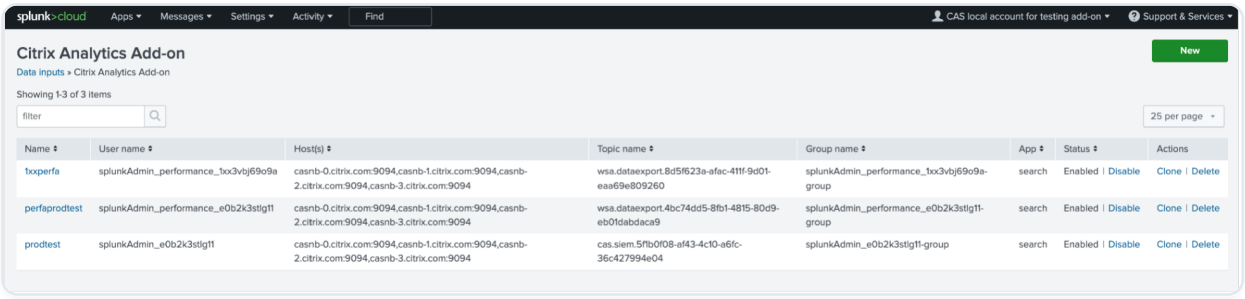
   (/en-us/citrix-analytics/media/citrix-analytics-add-on.png)
2. 添加输入：Splunk 集成 | Citrix Analytics for Security。单击 **添加新项**。

   (/en-us/citrix-analytics/media/splunk-integration-input.png)
3. 通过输入在 **Citrix Analytics 数据导出** 页面上配置的详细信息来配置数据输入。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

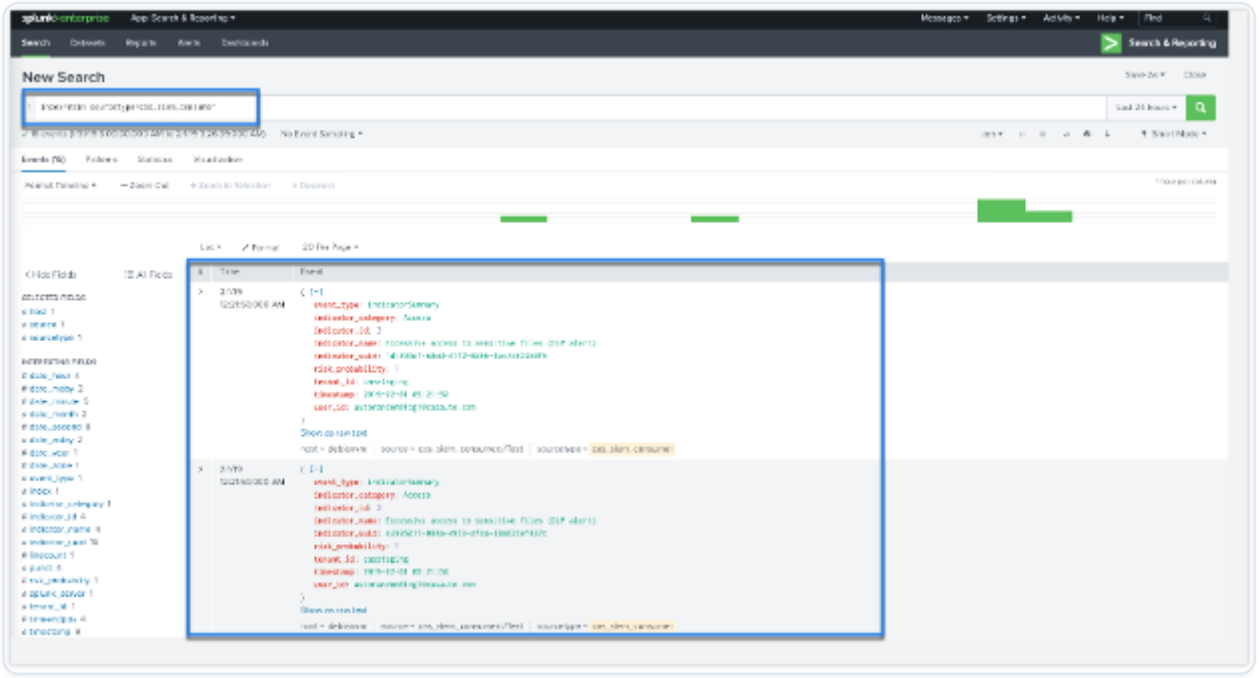
4. 验证您的数据输入是否已成功添加。



如何在您的 Splunk 环境中消费事件

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 搜索头中开始搜索您组织的事件。

搜索结果以以下格式显示：



示例输出：

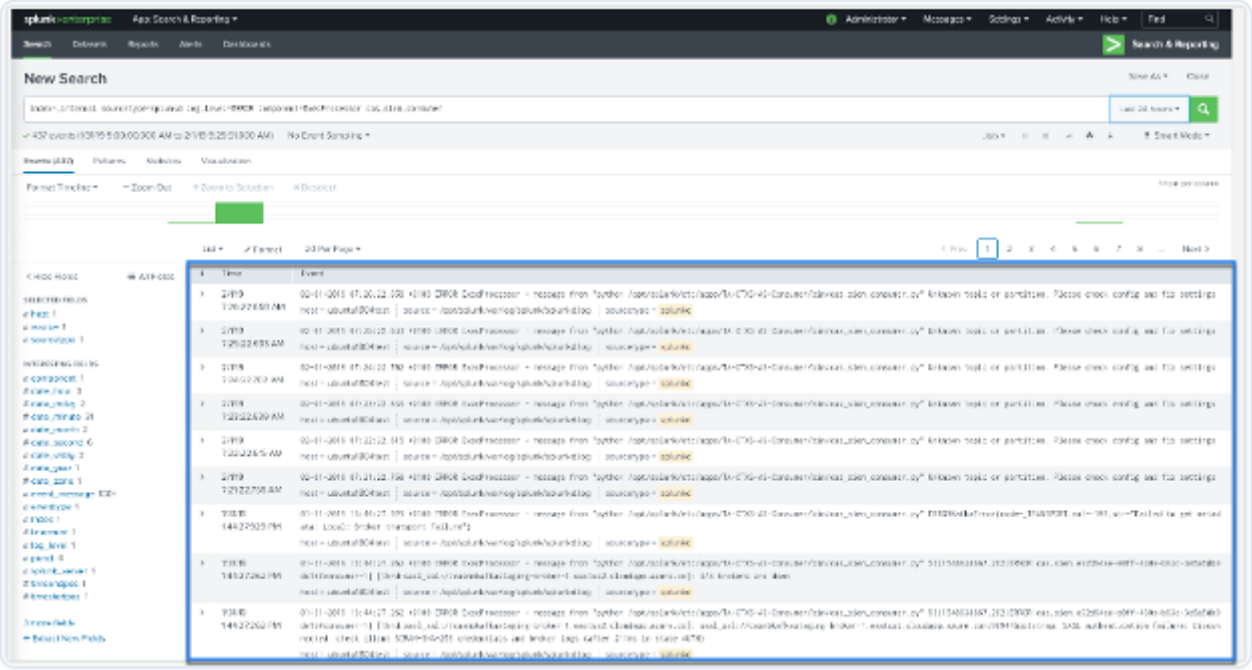
```
{"event_type": "indicatorSummary", "indicator_category": "Access",
"indicator_id": 200, "indicator_name": "Jailbroken / Rooted Device
Detected", "indicator_uuid": "1b97c3be-0000-000-0000-0000000000",
"risk_probability": 1.0, "tenant_id": "notcloud", "timestamp": "2017-11-16
23:59:59", "user_id": "testuser00001"}
```

要搜索和调试附加组件的问题，请使用以下搜索查询：

```
index=_internal sourcetype=splunkd log_level=ERROR component=ExecProcessor
cas_siem_consumer
```

结果以以下格式显示：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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。

排除 Splunk 版 Citrix Analytics 附加组件故障

如果您在 Splunk 控制板中看不到任何数据，或者在配置 Splunk 版 Citrix Analytics 附加组件时遇到问题，请执行调试步骤来解决该问题。有关更多信息，请参阅Splunk 版 Citrix Analytics 附加组件的配置问题。

注意

请联系 mailto:CAS-PM-Ext@cloud.com 以获取 Splunk 集成、将数据导出到 Splunk 或提供反馈方面的帮助。

Splunk 版 Citrix Analytics 应用程序

注意

此应用程序处于预览阶段。

Splunk 版 Citrix Analytics 应用程序使 Splunk Enterprise 管理员能够以富有洞察力且可操作的控制板形式在 Splunk 上查看从 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。这种关联使您能够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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持的 Splunk 版本

Splunk 版 Citrix Analytics 应用程序在以下 Splunk 版本上运行：

- Splunk 9.0 64 位版本
- Splunk 8.2 64 位版本
- 思普朗克 8.1 64位

Splunk 版 Citrix Analytics 应用程序的先决条件

- 安装 Splunk 版 Citrix Analytics 附加组件。
- 确保 Citrix Analytics for Splunk 附加组件的先决条件已满足。
- 确保数据正从 Citrix Analytics for Security 流向 Splunk。

安装和配置

在何处安装应用程序?

Splunk 搜索头

如何安装和配置应用程序?

您可以通过从 Splunkbase 下载或从 Splunk 内部安装来安装适用于 Splunk 的 Citrix Analytics 应用程序。

从文件安装应用程序

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 **Apps** 旁边的齿轮图标。
4. 单击 **从文件安装应用**。
5. 找到下载的文件，然后单击 **Upload**。

   注意

   如果您有旧版本的应用程序，请选择 **Upgrade app** 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 内部安装应用程序

1. 在 Splunk Web 主页上，单击“**+查找更多应用程序**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**”。



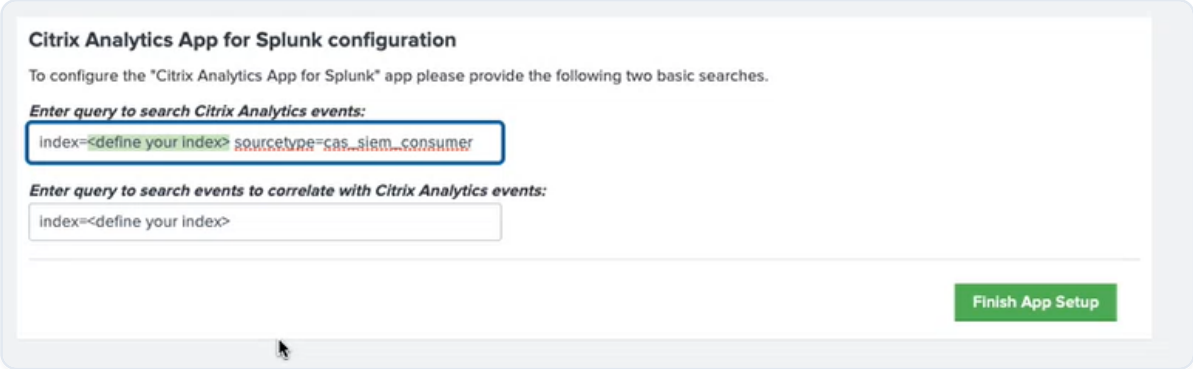
2. 输入以下查询：

   - 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 Splunk 的 Citrix Analytics 附加组件中指定的值相同。有关详细信息，请参阅配置 Splunk 的 Citrix Analytics 附加组件。

   - 您希望将数据与 Citrix Analytics for Security 关联的索引。



3. 单击“**完成应用程序设置**”以完成配置。

配置并设置 Splunk 的 Citrix Analytics 应用程序后，使用 Citrix Analytics 控制板 在 Splunk 上查看用户事件。

有关 Splunk 集成的更多信息，请参阅以下链接：

- 思杰分析与思普 克集成
- 适用于 Splunk 的 Citrix Analytics 应用程序，现已在 Splunkbase 中提供

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Splunk 架构与 Citrix Analytics 附加应用程序

Splunk 遵循包含以下三个层的架构：

- 收集
- 索引
- 搜索

Splunk 支持多种数据收集机制，有助于轻松将数据摄取到 Splunk 中，以便对其进行索引并使其可供搜索。此层就是您的重型转发器或通用转发器。

您必须将附加应用程序安装在重型转发器层，而不是通用转发器层。因为，除了少数结构化数据（例如 json、csv、tsv）的例外情况，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理解日志格式的操作。

它还附带一个精简版的 Python，这使得它与任何需要完整 Splunk 堆栈才能运行的模块化输入应用程序不兼容。重型转发器就是您的收集层。

通用转发器和重型转发器之间的主要区别在于，重型转发器包含完整的解析管道，执行与索引器相同的功能，而无需实际将事件写入磁盘并进行索引。这使得重型转发器能够理解并根据事件数据对单个事件进行操作，例如数据屏蔽、过滤和路由。由于附加应用程序具有完整的 Splunk Enterprise 安装，因此它可以托管需要完整 Python 堆栈才能进行正确数据收集的模块化输入，或者充当 Splunk HTTP 事件收集器 (HEC) 的端点。

数据收集后，会对其进行索引或处理，并以可搜索的方式存储。

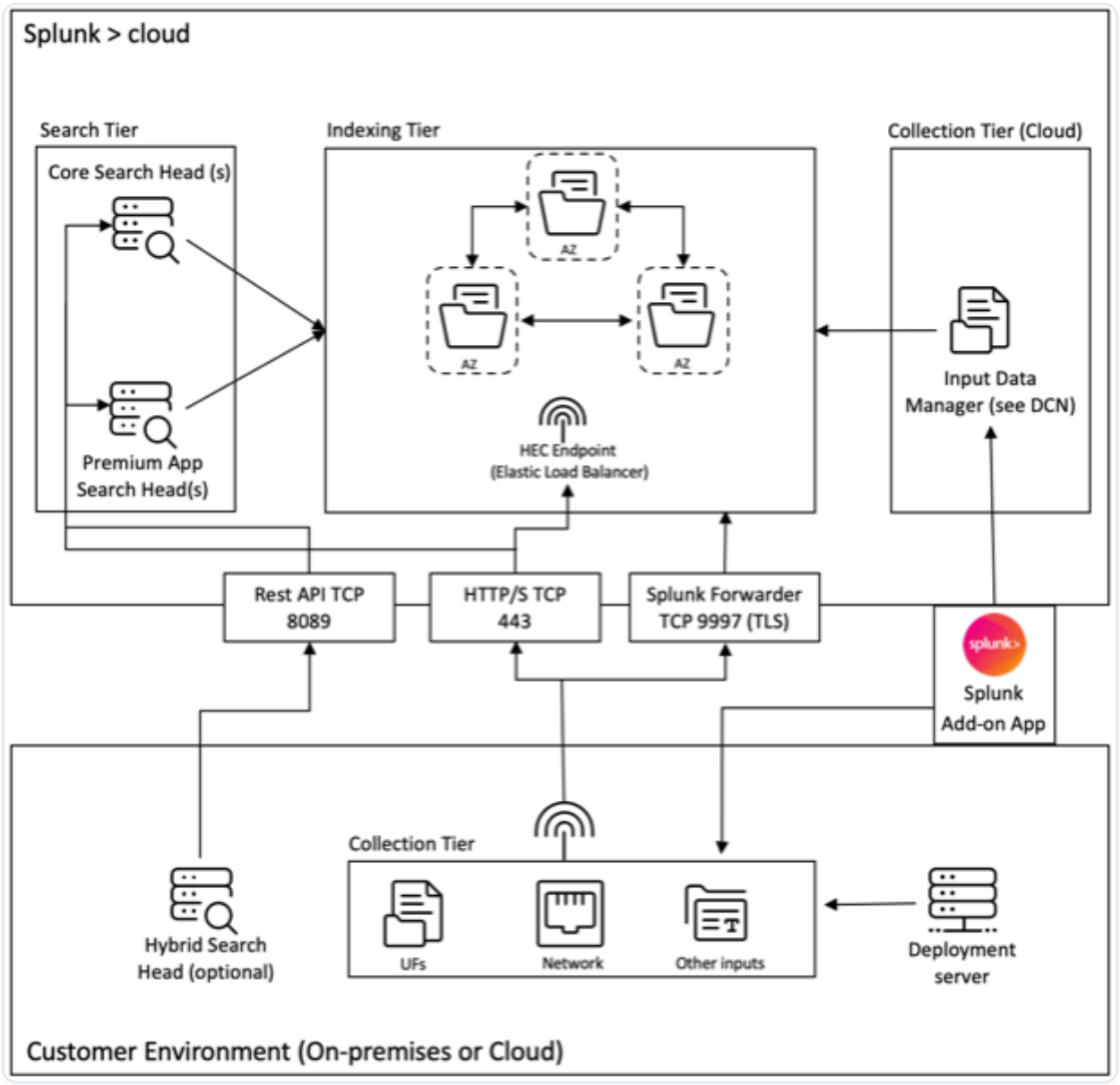
客户探索其数据的主要方式是通过搜索。搜索可以保存为报告，并用于驱动仪表板面板。搜索是从数据中提取信息。

通常，Splunk 附加应用程序部署在收集层（Splunk 企业级），而我们的仪表板应用程序部署在搜索层（Splunk Cloud 级）。在简单的本地部署中，您可以将所有这三个层部署在单个 Splunk 主机上（称为单服务器部署）。

收集层是使用 Splunk 附加应用程序的更好方式。有两种方法可以安装附加应用程序。您可以在客户环境下的收集层安装它，也可以在 **Splunk Cloud 实例**下的输入数据管理器中安装它。

请参阅下图以了解 Splunk 与我们的附加应用程序的部署架构：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



上述图中所示的输入数据管理器 (IDM) 是 Splunk Cloud 管理的数据收集节点 (DCN) 的实现，仅支持脚本化和模块化输入。对于超出此范围的数据收集需求，您可以使用 Splunk 重型转发器在您的环境中部署和管理 DCN。

Splunk 允许从各种来源收集、索引和搜索数据。一种数据收集方式是通过 API，这使得 Splunk 能够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都提供了一系列应用程序，这些应用程序通过 Splunk 模块化输入框架实现 API 交互。这些应用程序通常需要完整的 Splunk 企业软件安装才能正常运行。

为了方便通过 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功能更强大，因为它们包含完整的解析管道，并且能够理解和处理单个事件。这使它们能够通过 API 收集数据并在将其转发到 Splunk 实例进行索引之前进行处理。

要详细了解 Splunk Cloud 部署的高级架构，请参阅 Splunk Validated Architectures。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Splunk 的 Citrix Analytics 控制板

注意

注意：Citrix Content Collaboration™ 和 ShareFile 已达到其生命周期终止，不再对用户可用。

此功能处于预览阶段。

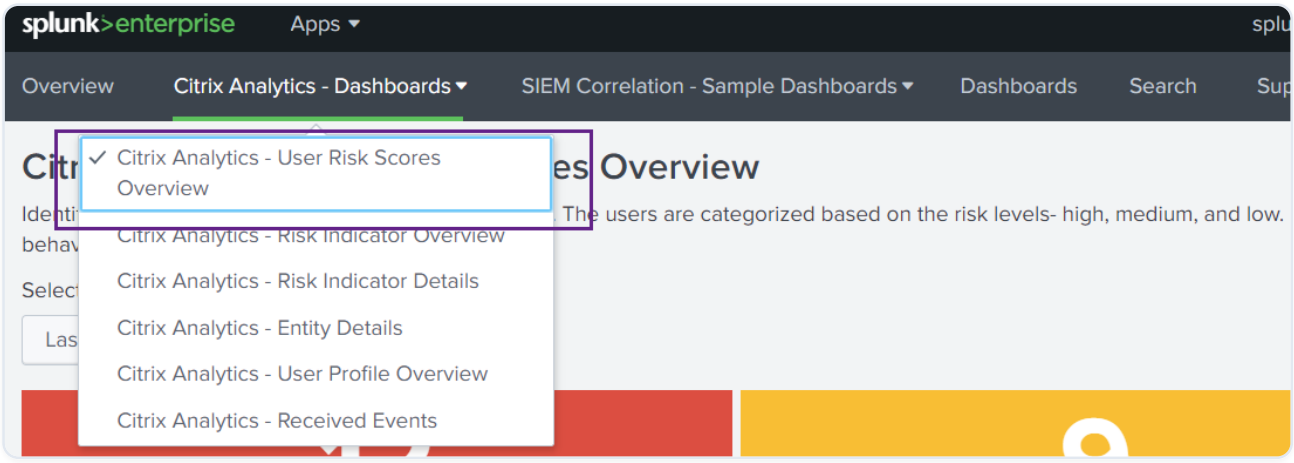
先决条件

要使用以下 Citrix Analytics 控制板，请确保您已配置并设置了 适用于 Splunk 的 Citrix Analytics 应用程序。

用户风险评分概览

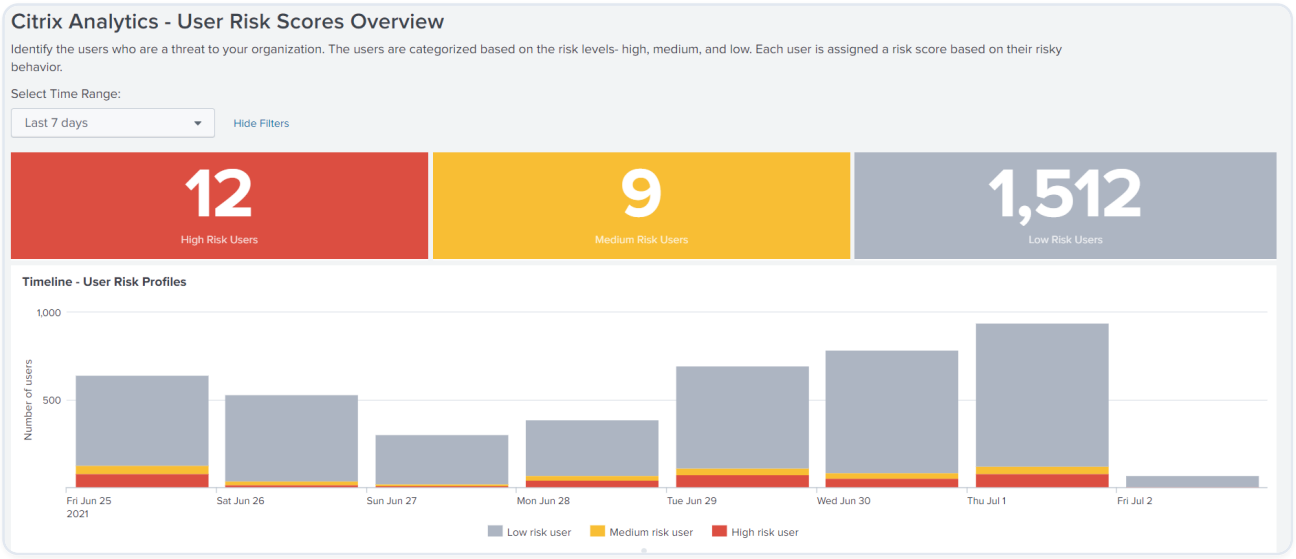
此控制板提供您组织中高风险用户的综合视图。用户按风险级别（高、中、低）进行分类。风险级别基于用户活动中的异常情况，并相应地分配风险评分。有关高风险用户类型的更多信息，请参阅用户控制板。

要查看此控制板，请单击 **Citrix Analytics- 控制板 > Citrix Analytics- 用户风险评分概览**。



选择预设时间范围或自定义时间范围，以查看高风险用户的时间线及其详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



高风险用户表提供以下信息：

- **用户**：指示用户名。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。
- **发现受损端点风险**：指示用户触发的属于受损端点风险类别的风险指标数量。
- **已泄露用户风险发现**：表示属于已泄露用户风险类别的用户触发的风险指标数量。
- **数据泄露风险发现**：表示属于数据泄露风险类别的用户触发的风险指标数量。
- **内部威胁风险发现**：表示属于内部威胁风险类别的用户触发的风险指标数量。
- **风险评分**：表示用户的风险评分。

您还可以通过用户名搜索用户并获取所需详细信息。

有关详细信息，请参阅风险类别。

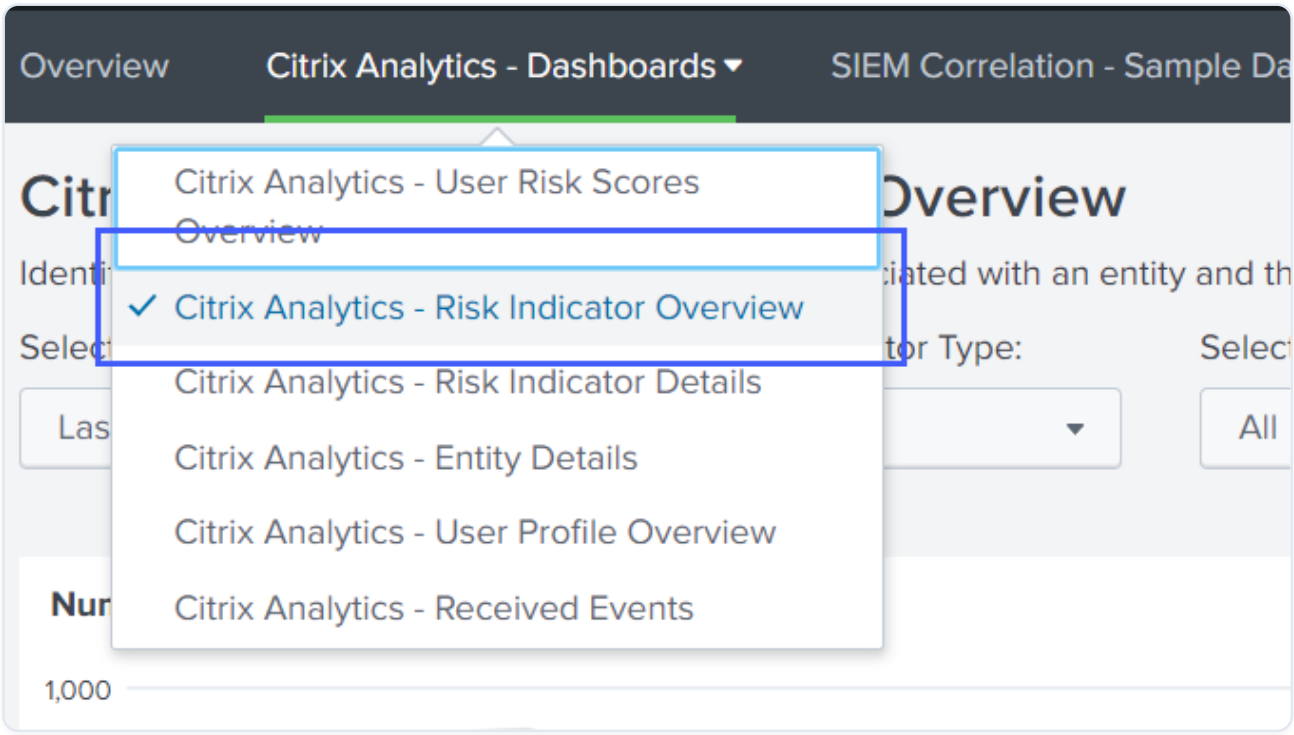


风险指标概述

此仪表板提供您组织中用户触发的风险指标的综合视图。

要查看仪表板，请单击 **Citrix Analytics- 仪表板 > Citrix Analytics- 风险指标概览**。

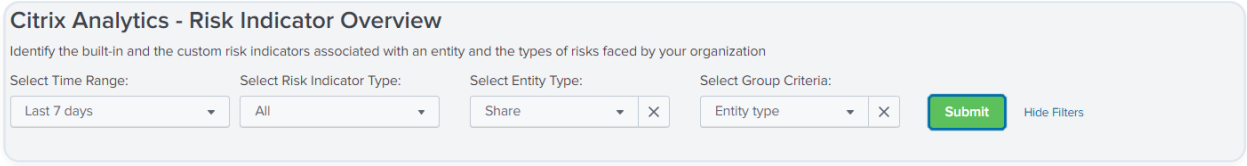
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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，以查看该期间触发的风险指标。
- **风险指标类型**：选择风险指标类型：内置或自定义。
- **实体类型**：选择一个用户以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，并查看相关的风险指标。



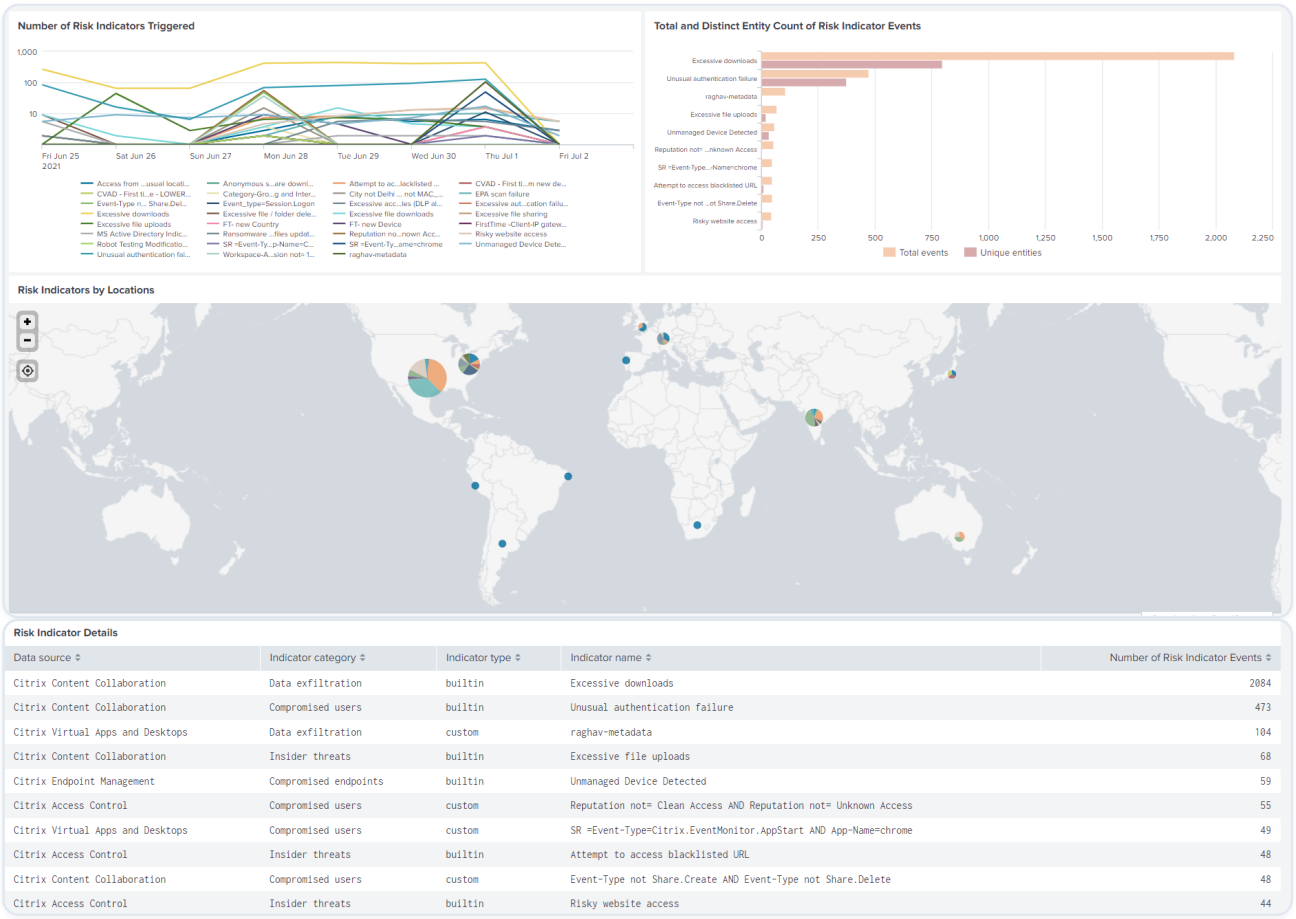
查看报告

使用以下报告，通过选择一个或多个类别来查看风险指标的详细信息：

- **触发的风险指标数量**：显示所选期间触发的风险指标数量。使用此报告可识别风险活动的模式和区域。此外，还可以识别组织中的主要风险活动。
- **风险指标事件的总实体计数和唯一实体计数**：显示与风险指标对应的总事件和唯一事件。使用此报告可识别每个风险指标的发生情况以及组织中的主要风险指标。您还可以识别有多少唯一用户触发了特定风险指标，并检查该风险指标是由较大还是较小的用户组触发的。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **按位置划分的风险指标**：显示用户在不同位置触发的风险指标数量。使用此报告可识别显示更多风险活动的地点，并检查这些地点是否在组织运营区域之外。
- **风险指标详细信息**：显示有关风险指标的详细信息，例如关联的数据源、指标类别、指标类型和发生次数。



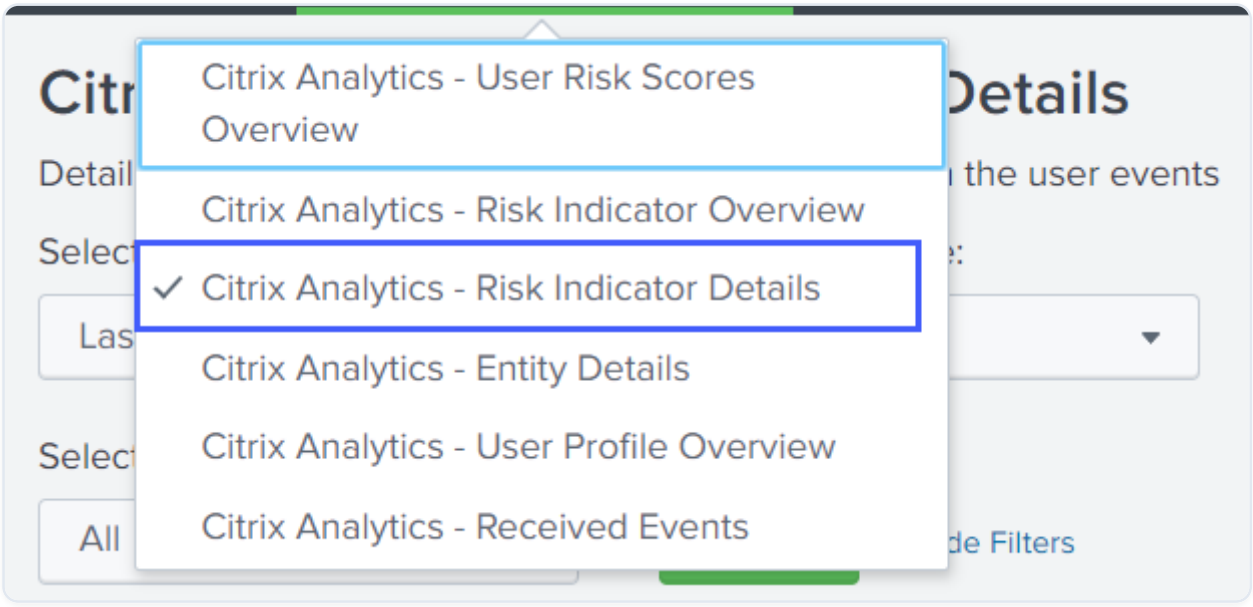
Data source	Indicator category	Indicator type	Indicator name	Number of Risk Indicator Events
Citrix Content Collaboration	Data exfiltration	builtin	Excessive downloads	2084
Citrix Content Collaboration	Compromised users	builtin	Unusual authentication failure	473
Citrix Virtual Apps and Desktops	Data 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

风险指标详细信息

此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 用户风险指标和自定义风险指标。

要查看仪表板，请单击 **Citrix Analytics- 仪表板 > Citrix Analytics- 风险指标详细信息**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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**：选择预设时间范围或自定义时间范围，以查看该期间触发的风险指标的详细信息。
- **实体类型**：选择一个用户以查看相关风险指标的详细信息。
- **风险指标类型** - 选择内置或自定义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标的详细信息。
- **风险指标类别** - 选择风险类别以查看相关风险指标的详细信息。
- **风险指标** - 选择风险指标以查看其详细信息。

查看报告

例如，从“选择风险指标”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：

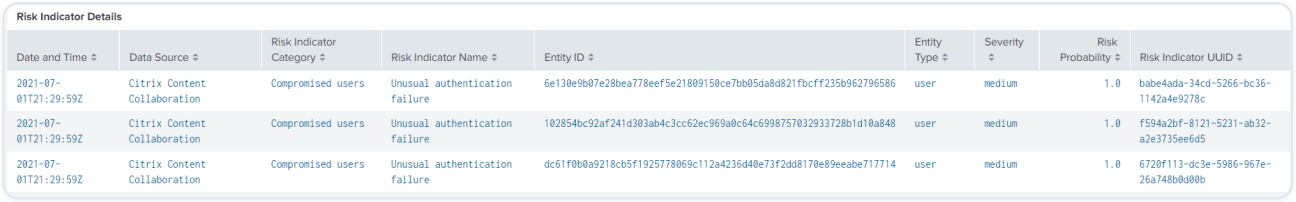
- 与风险指标关联的前 10 位用户
- 风险指标的详细信息，例如
  - 触发日期和时间
  - 相关数据源
  - 相关风险类别
  - 关联实体 ID 和用户实体类型
  - 风险严重性 - 高、中或低
  - 用户事件的风险概率

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 风险指标的唯一标识 (UUID)



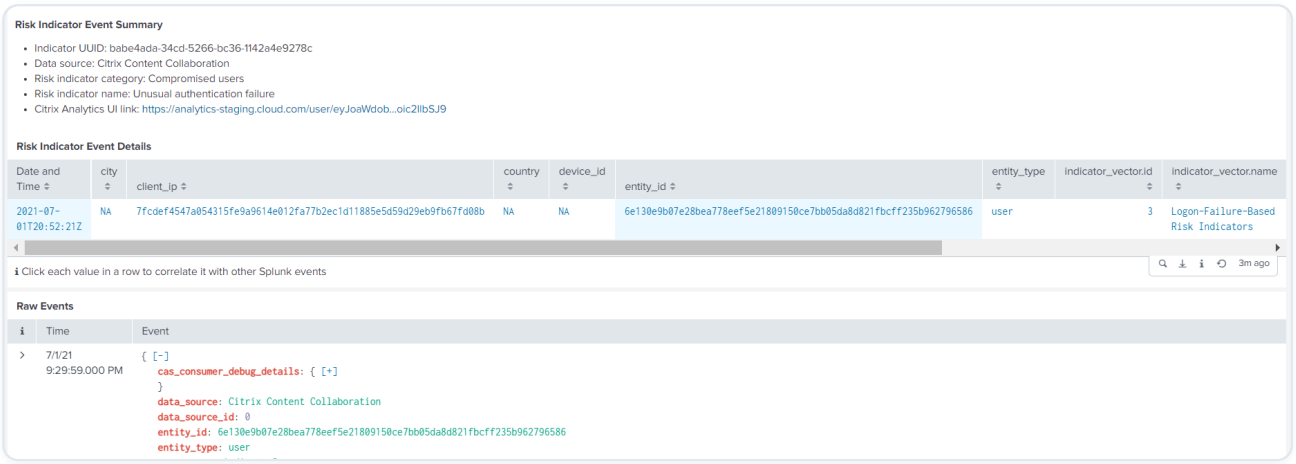
在“**按风险指标划分的前 10 个实体**”中，单击一个实体可在“**Citrix Analytics - 实体详细信息**”仪表板上查看其详细信息。



单击“**风险指标详细信息**”表中的每一行，可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“**风险指标事件摘要**”部分，单击“**Citrix Analytics UI 链接**”可直接从 Splunk 跳转到 Citrix Analytics for Security™ 上的用户时间线。在用户时间线上，查看风险指标、关联事件以及为该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，请参阅适用于 SIEM 的 Citrix Analytics 数据格式。

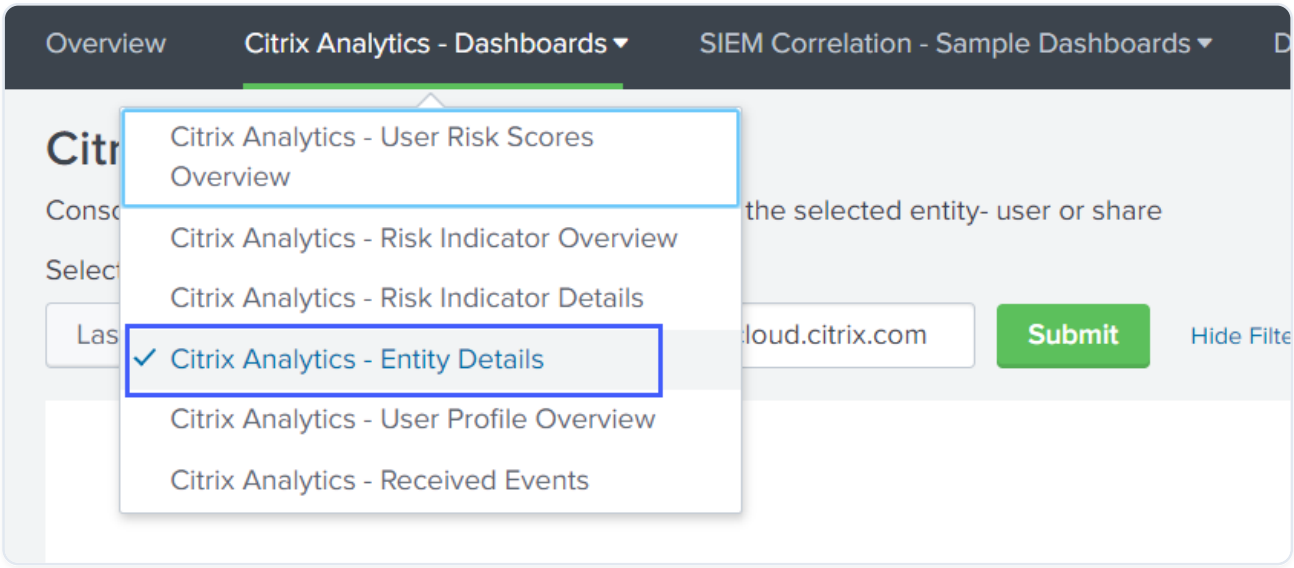


实体详细信息

使用此仪表板可查看用户实体用户及其风险行为的详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要查看仪表板，请单击“**Citrix Analytics - 仪表板 > Citrix Analytics - 实体详细信息**”。

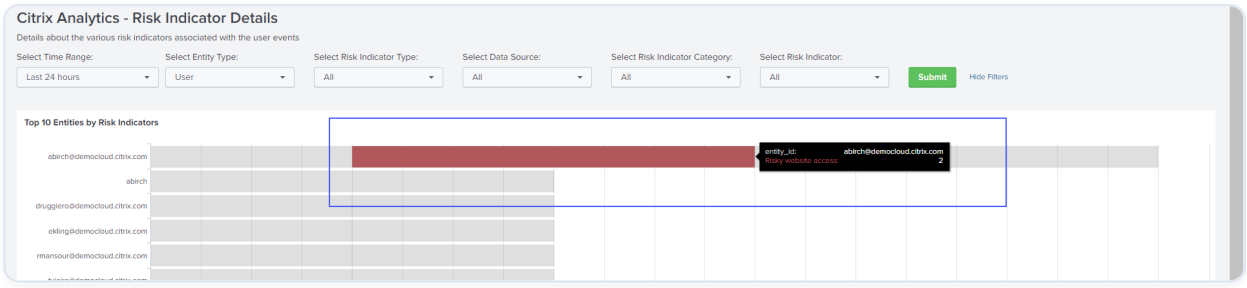


查看报告

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查看有关实体的详细信息：

- 在 **Citrix Analytics- 风险指标详细信息**中，转到**按风险指标排名前 10 的实体**，然后单击一个实体。



- 在 **Citrix Analytics- 风险评分概述**中，转到**高风险用户**，然后单击一个用户名。

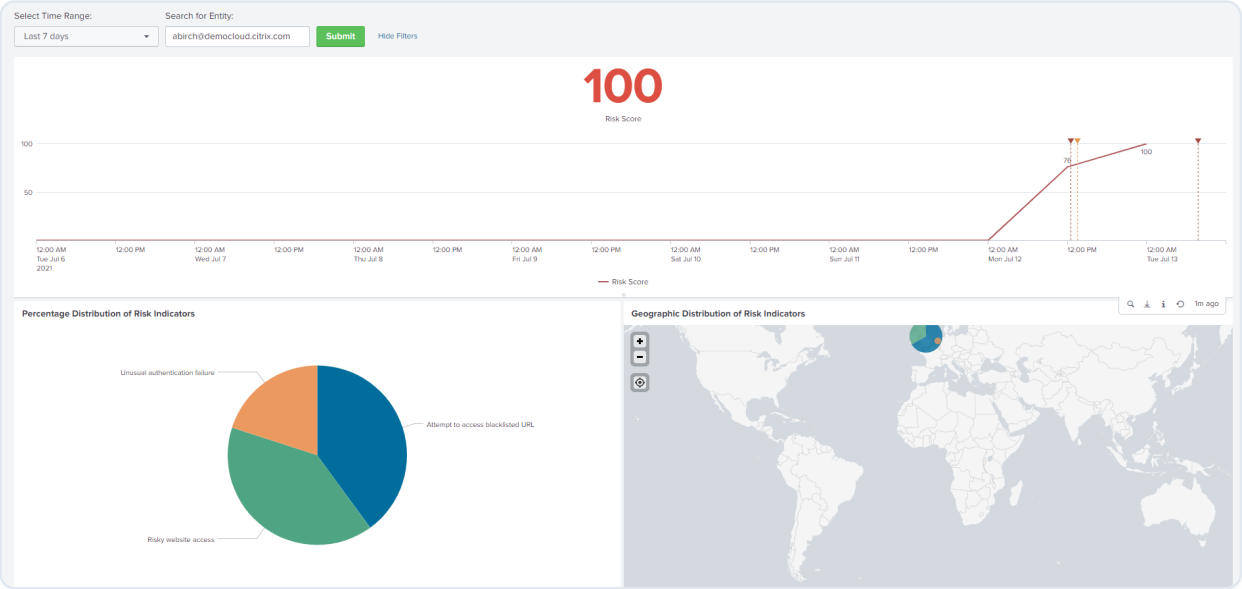


显示以下详细信息：

- 选定时间范围的当前风险评分和风险评分时间线。
- 风险指标的百分比分布。帮助您分析实体的风险活动模式。
- 风险指标的地理分布。帮助您识别异常和高风险位置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 与风险活动关联的客户端 IP 详细信息。
- 与风险活动关联的用户设备详细信息。
- 风险指标详细信息，例如关联的数据源、风险类别、风险严重性等。



实体详细信息视图 2(/en-us/citrix-analytics/media/entity-details-splunk-2.png)

将与危险活动相关的客户端 IP 和用户设备与从连接到 Splunk 的其他安全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。

客户端 IP 详细信息(/en-us/citrix-analytics/media/client-ip-details-splunk.png)

在“**Citrix Analytics 事件关联**”控制面板上，您可以查看与所选客户端 IP 关联的事件，这些事件是从其他安全数据源（基于索引和源类型）关联而来的。这些事件提供了对与客户端 IP 相关的恶意活动的更深入见解。

事件关联控制面板(/en-us/citrix-analytics/media/event-correlation-splunk-1.png)

用户配置文件概述

使用此控制面板可查看与组织中用户相关的事件指标。

要查看仪表板，请单击**Citrix Analytics- 仪表板 > Citrix Analytics- 用户配置文件概述**。

用户配置文件概述选择(/en-us/citrix-analytics/media/user-profile-overview-selection-splunk.png)

查看事件

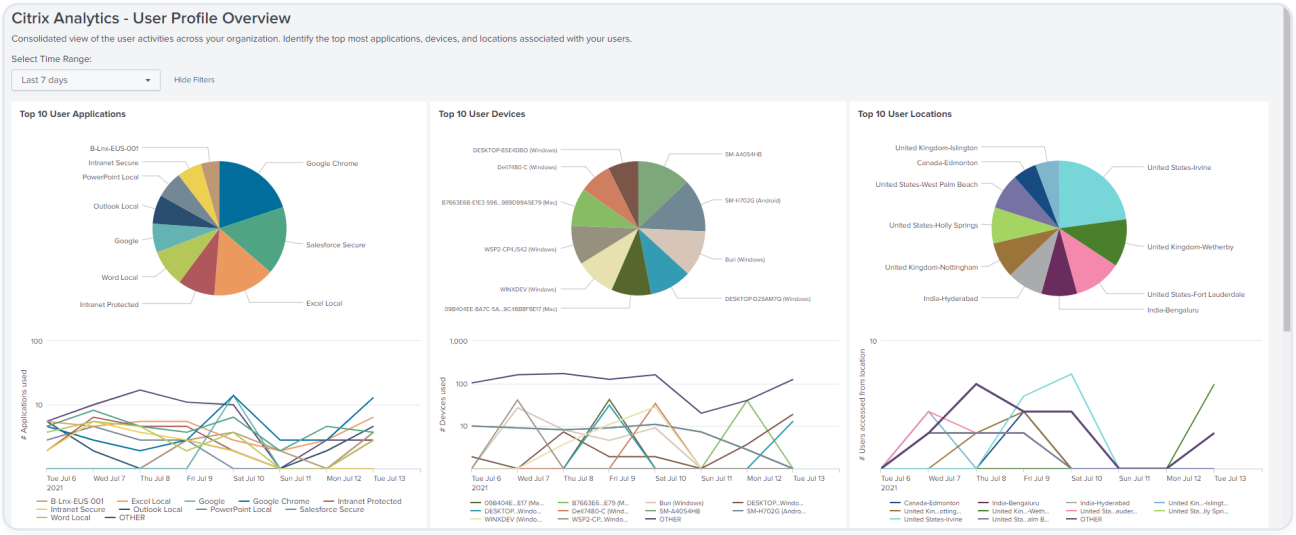
选择一个时间范围并查看以下指标：

- 用户使用的前 10 个应用程序

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 用户使用的前 10 个设备
- 用户使用的前 10 个位置
- 使用的 Web 和 SaaS 应用程序数量
- 使用的设备数量
- 跨位置访问的用户数量
- 数据使用情况指标，例如上传、下载、共享的文件

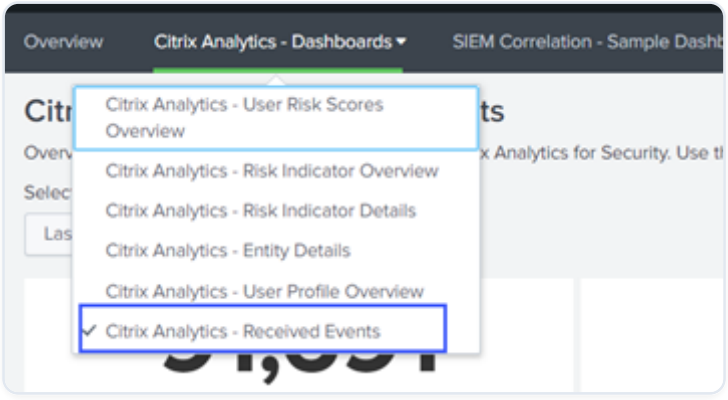
这些指标可让您深入了解组织中的用户活动。您可以识别最常用的应用程序和设备、使用模式、不合规的设备和应用程序、异常位置、有风险的访问以及异常文件活动。



收到的事件

使用控制面板查看从 Citrix Analytics for Security 收到的事件。事件表示一种用户活动。

要查看控制面板，请单击 **Citrix Analytics- Dashboards > Citrix Analytics- Received Events**。



查看报告

选择一个时间范围以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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 收到的事件总数：它是从 Citrix Analytics for Security 收到的所有事件的总和，包括以下内容：
    - 风险指示器事件总数：表示与用户触发的风险指示器相关的事件。
    - 风险指示器详细信息事件总数：表示与触发的风险指示器详细信息相关的事件。
    - 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。
    - 总用户配置文件风险评分事件：表示与用户风险评分相关的事件。
    - 总用户配置文件应用程序事件：表示与用户使用的应用程序相关的事件。
    - 总用户配置文件设备事件：表示与用户使用的设备相关的事件。
    - 总用户配置文件数据使用事件：表示与用户数据使用相关的事件。
    - 总用户配置文件位置事件：表示与用户访问的位置相关的事件。

      收到的事件仪表板(/en-us/citrix-analytics/media/received-events-report-splunk.png)

事件关联示例

使用此仪表板将从 Citrix Analytics for Security 接收的事件与从 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风险活动，发现事件之间的关系，并识别任何威胁。

要查看仪表板，请单击**SIEM Correlation- 示例仪表板 > Citrix Analytics 事件关联**。

事件关联选择(/en-us/citrix-analytics/media/event-correlation-selection-splunk.png)

先决条件

要执行关联，请确保满足以下条件：

- 您必须拥有来自其他安全数据源的事件才能进行关联。例如，从 Splunk 中配置的其他数据源接收到的与用户、设备和客户端 IP 地址相关的事件。
- 您必须在配置期间已定义关联索引。

关联事件

您可以查看由 Citrix Analytics for Security 检测到的高风险实体和高风险 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。

高风险事件(/en-us/citrix-analytics/media/event-correlation-splunk-2.png)

查询字段中显示的索引值是在配置应用程序时定义的。您可以根据需要将索引值更改为其他安全数据源。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

来自其他数据源的事件(/en-us/citrix-analytics/media/event-correlation-splunk-3.png)

无事件故障排除

如果您在所有仪表板上都找不到任何事件，这可能是由于 Citrix Analytics App for Splunk 和 Citrix Analytics add-on for Splunk 中的配置问题造成的。在这种情况下，请验证索引值和源类型值。确保索引和源类型的值在应用程序和附加组件中都相同。

要查看 Citrix Analytics App for Splunk 的配置设置：

1. 单击 **应用 > 管理应用**。

   配置应用程序(/en-us/citrix-analytics/media/manage-app-splunk.png)
2. 从列表中找到 Citrix Analytics App for Splunk。单击 **Set up**。

   设置(/en-us/citrix-analytics/media/splunk-app-setup.png)
3. 检查源类型和索引。

   源类型(/en-us/citrix-analytics/media/splunk-app-source-index.png)

要查看 Citrix Analytics add-on for Splunk 的配置设置：

1. 单击 **设置 > 数据输入**。

   数据输入(/en-us/citrix-analytics/media/data-inputs-splunk.png)
2. 点击 **Citrix Analytics 附加组件**。

   选择添加(/en-us/citrix-analytics/media/splunk-add-config.png)
3. 点击从中获取事件的租户。
4. 选择 **更多设置**。

   配置(/en-us/citrix-analytics/media/splunk-add-config-1.png)
5. 检查源类型和索引。

   源类型(/en-us/citrix-analytics/media/splunk-add-config-2.png)

有关配置的更多信息，请参阅 配置适用于 Splunk 的 Citrix Analytics 附加组件。

适用于 Splunk 的 Citrix Analytics 附加组件的配置问题

© 1997–2026 Citrix Systems, Inc. All rights reserved.

微软 Sentinel 集成

注意

- 请联系 mailto:CAS-PM-Ext@cloud.com 以获取 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 的功能处于预览阶段。此功能不提供服务级别协议，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™ 与您的 Microsoft Sentinel 集成。

此集成使您能够将 Citrix IT 环境中的用户数据导出并关联到 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仪表板。您还可以根据安全要求创建自定义视图。

有关集成优势以及发送到 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。

先决条件

- 为至少一个数据源开启数据处理。这有助于 Citrix Analytics for Security 启动 Microsoft Sentinel 集成过程。
- 确保以下端点在您的网络允许列表中。

端点	美国地区	欧盟地区	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`
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`	`casnb-aps-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`

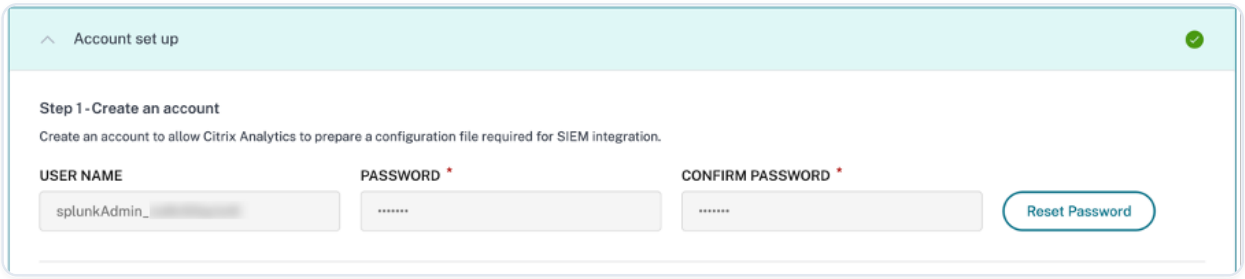
© 1997–2026 Citrix Systems, Inc. All rights reserved.

端点	美国地区	欧盟地区	亚太南部地区
	`casnb-3.citrix.com:9094`		

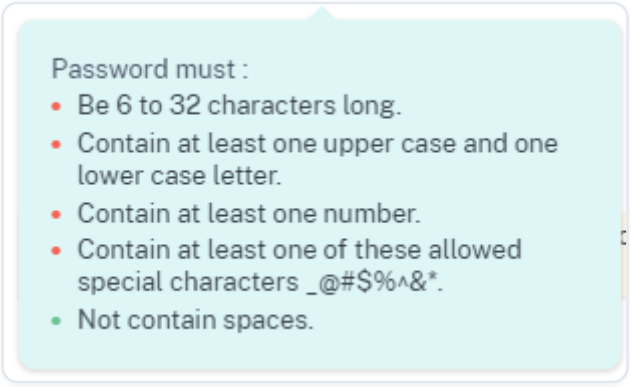
- 确保您使用 Logstash 7.17.7 或更高版本（与 Citrix Analytics for Security 兼容的测试版本：v7.17.7 和 v8.5.3）以及用于 Logstash 的 Microsoft Sentinel 输出插件。

与 Microsoft Sentinel 集成

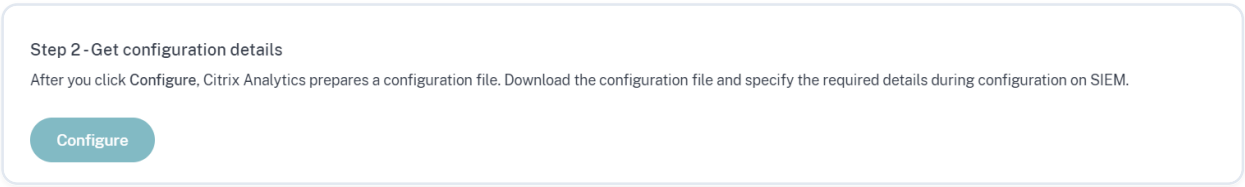
1. 转到 **设置 > 数据导出**。
2. 在“**帐户设置**”部分，通过指定用户名和密码来创建帐户。此帐户用于准备集成所需的配置文件。



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：

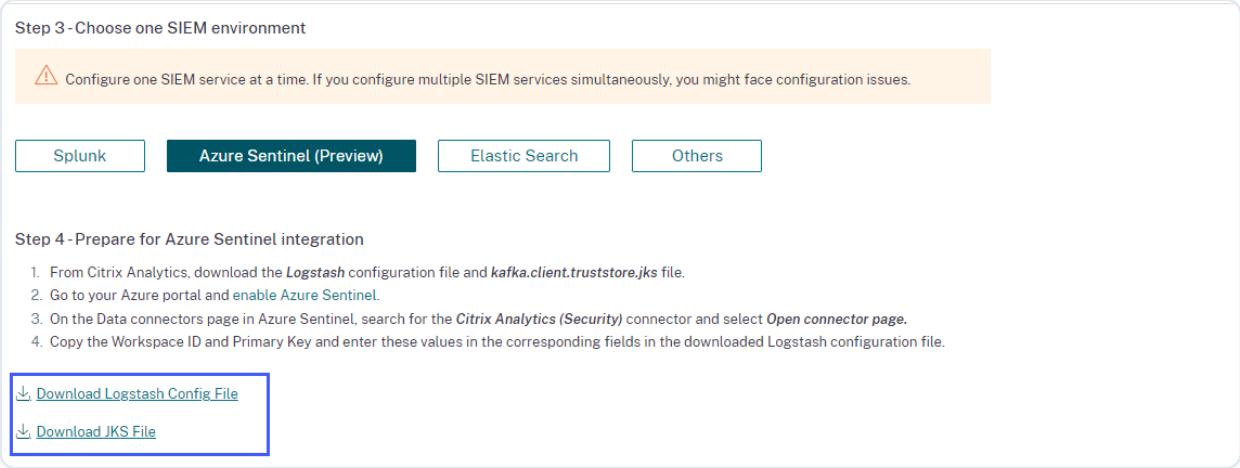
   - **Logstash 配置文件**：包含用于使用 Logstash 数据收集引擎将 Citrix Analytics for Security 中的事件发送到 Microsoft Sentinel 的配置数据（输入、筛选器和输出部分）。

     有关 Logstash 配置文件结构的信息，请参阅 Logstash 文档。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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。请将它们保存在安全的位置。



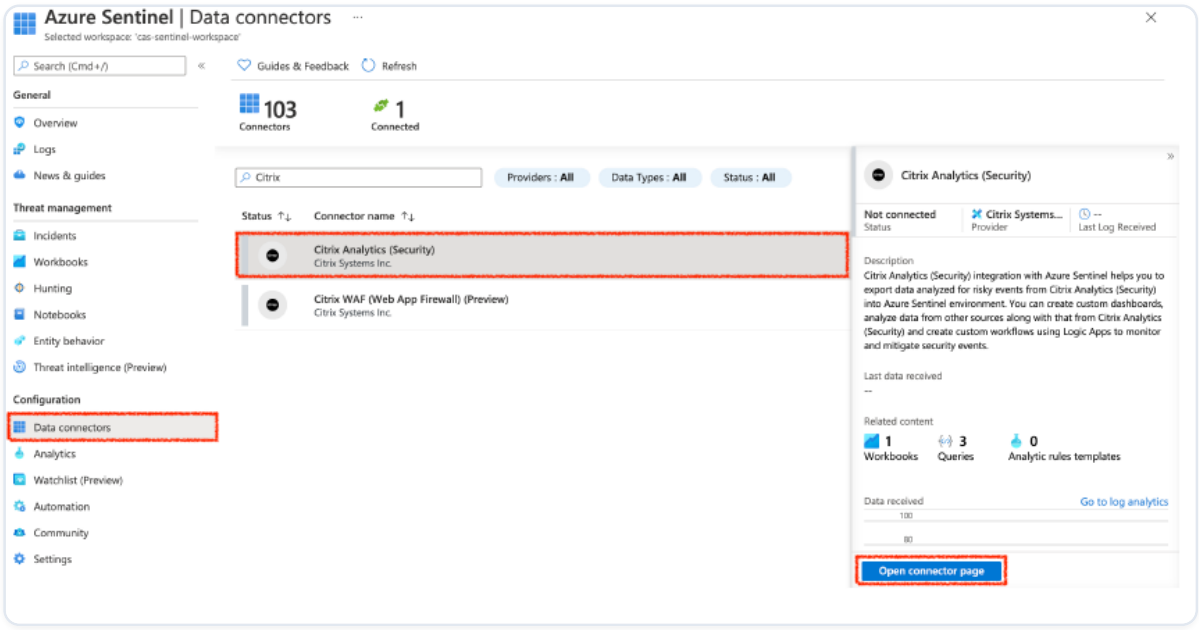
6. 准备 Azure Sentinel 集成：

   a. 在 Azure 门户上，启用 Microsoft Sentinel。您可以创建工作区或使用现有工作区来运行 Microsoft Sentinel。

   b. 从主菜单中，选择 **数据连接器** 以打开数据连接器库。

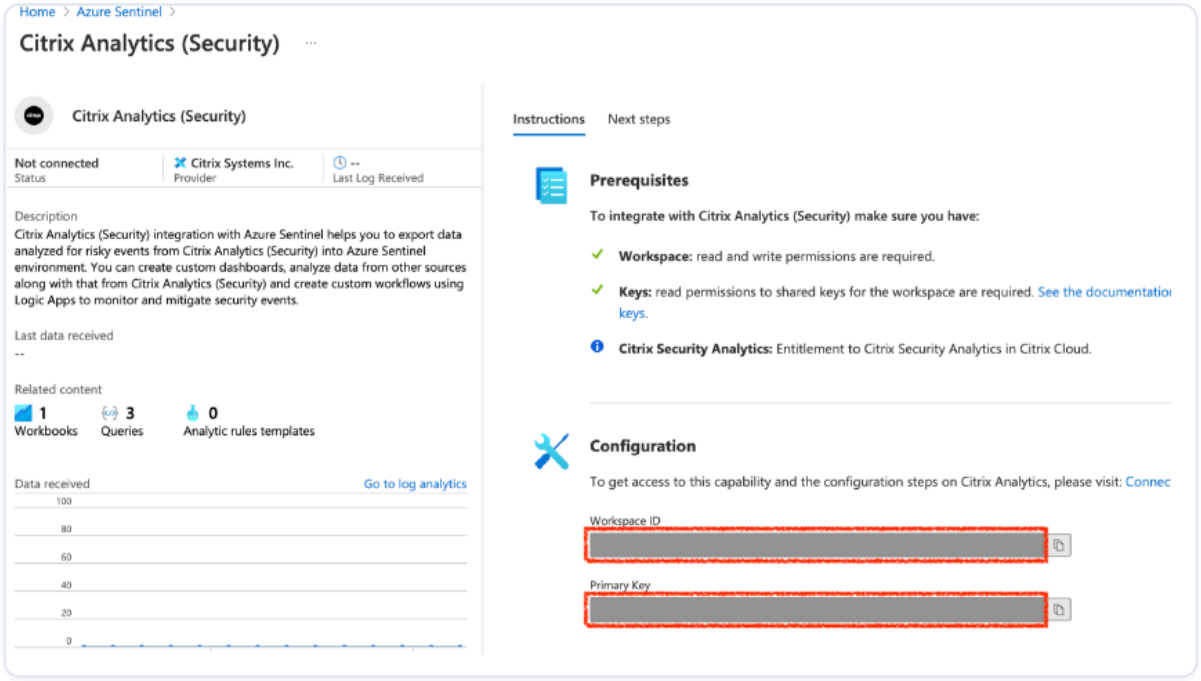
   c. 搜索 **Citrix Analytics (安全)**。

   d. 选择 **Citrix Analytics (Security)** 并选择 **打开连接器页面**。



   e. 在 **Citrix Analytics (Security)** 页面上，复制 **工作区 ID** 和 **主密钥**。您必须在后续步骤中将此信息输入到 Logstash 配置文件中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 Logstash 的 Microsoft Sentinel 输出插件。

ii. 在您安装了 Logstash 的主机上，将以下文件放置在指定目录中：

主机类型	文件名	目录路径
Linux 操作系统	CAS_AzureSentinel_LogStash_Config.config	对于 Debian 和 RPM 软件包：`/etc/logstash/conf.d/`
		对于 .zip 和 .tar.gz 归档文件：`{extract.path}/config`
	kafka.client.truststore.jks	对于 Debian 和 RPM 软件包：`/etc/logstash/ssl/`
		对于 .zip 和 .tar.gz 归档文件：`{extract.path}/ssl`
Windows 系统	CAS_AzureSentinel_LogStash_Config.config	`C:\logstash-7.xx.x\config`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

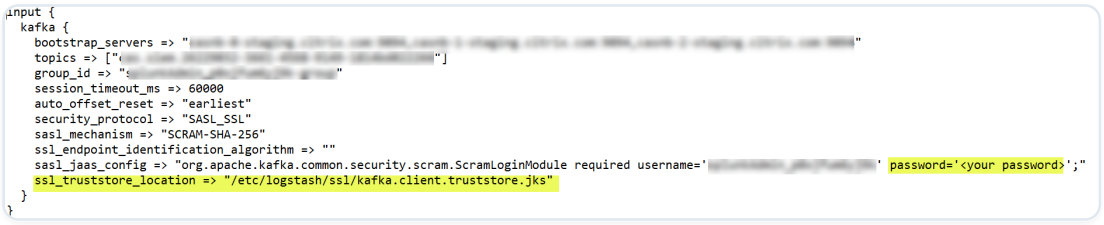
主机类型	文件名	目录路径
	kafka.client.truststore.jks	

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：

i. 在文件的输入部分中，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 信任库位置**：您的 SSL 客户端证书的位置。这是主机中 kafka.client.truststore.jks 文件的位置。



ii. 在文件的输出部分中，输入 **工作区 ID** 和 **主密钥**（您从 Microsoft Sentinel 复制的）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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，将处理后的数据从 Citrix Analytics for Security 发送到 Microsoft Sentinel。

g. 前往您的 Microsoft Sentinel 工作区，并在 Citrix Analytics 工作簿 中查看数据。

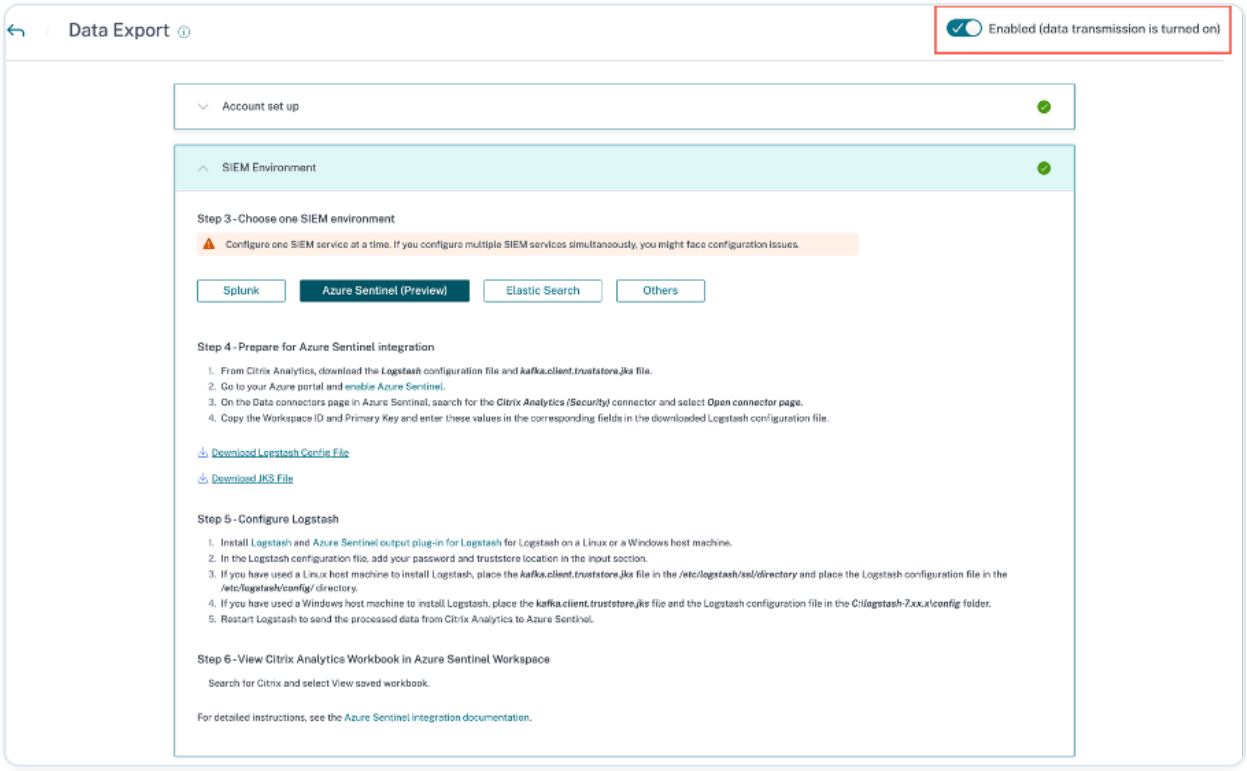
开启或关闭数据传输

Citrix Analytics for Security 准备好配置文件后，将为 Microsoft Sentinel 开启数据传输。

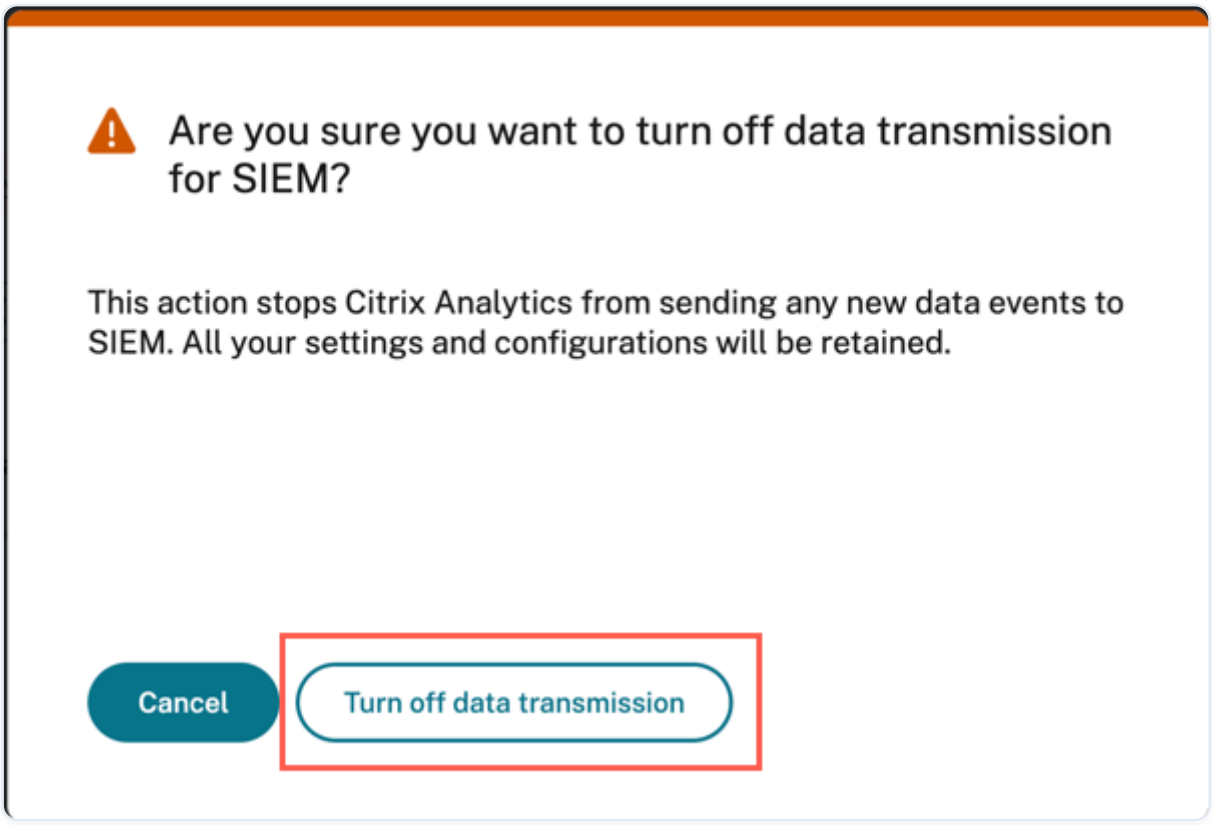
要停止从 Citrix Analytics for Security 传输数据，请执行以下操作：

1. 转到 **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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



将出现一个警告窗口，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，请开启切换按钮。

要了解有关 Microsoft Sentinel 集成的更多信息，请参阅以下链接：

- 思杰分析与微软哨兵集成

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 使用 Citrix Analytics for Security 和 Microsoft Sentinel 提升您的威胁搜寻能力

适用于 Microsoft Sentinel 的 Citrix Analytics 工作簿

注意

此功能为预览版。

本文介绍了 Microsoft Sentinel 工作区中提供的 Citrix Analytics 工作簿。

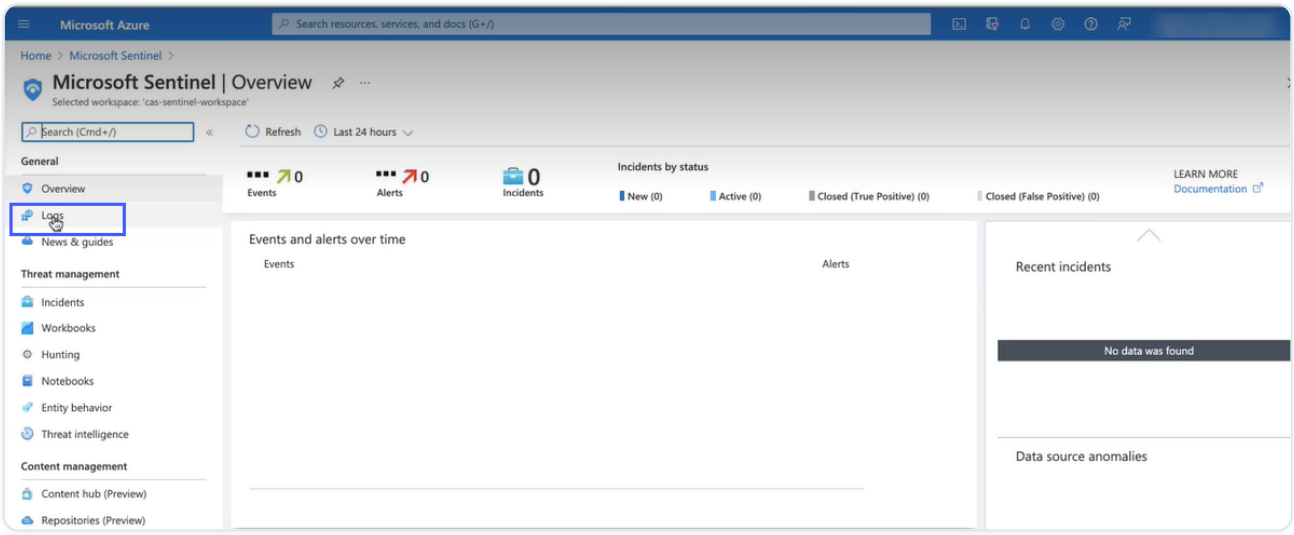
先决条件

要使用 Citrix Analytics 工作簿，请确保您已将 Microsoft Sentinel 与 Citrix Analytics for Security 集成。有关详细信息，请参阅Microsoft Sentinel 集成。

查看 Citrix Analytics 事件

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，打开您用于集成的 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**。

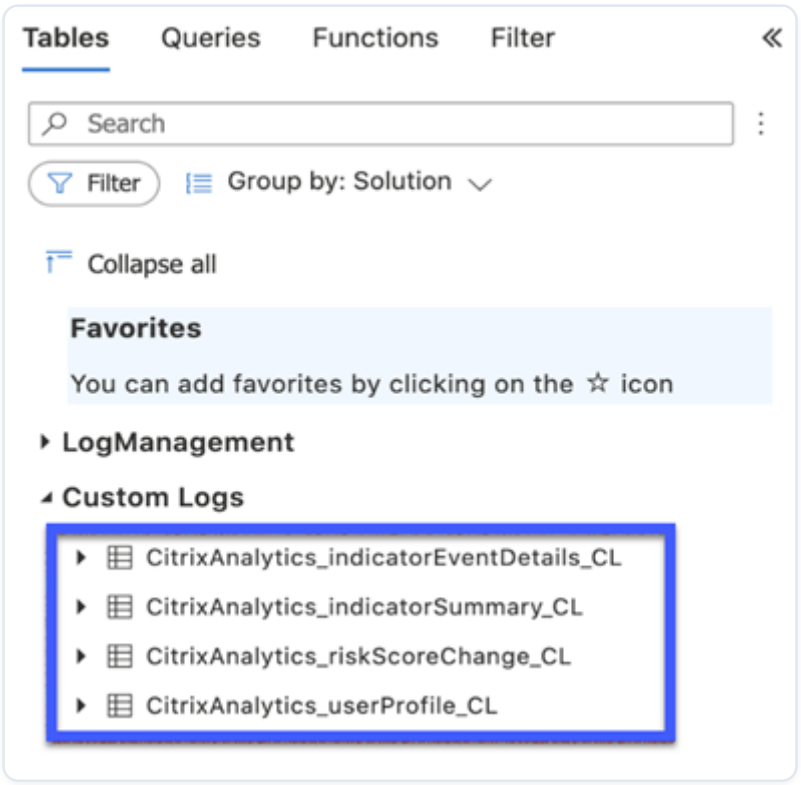


在“**自定义日志**”部分，您可以查看自动创建的日志表，这些日志表用于存储从 Citrix Analytics for Security 接收的事件。这些日志表是 Citrix Analytics 工作簿上仪表板的来源。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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，您可能会看到事件的日志表创建存在延迟。

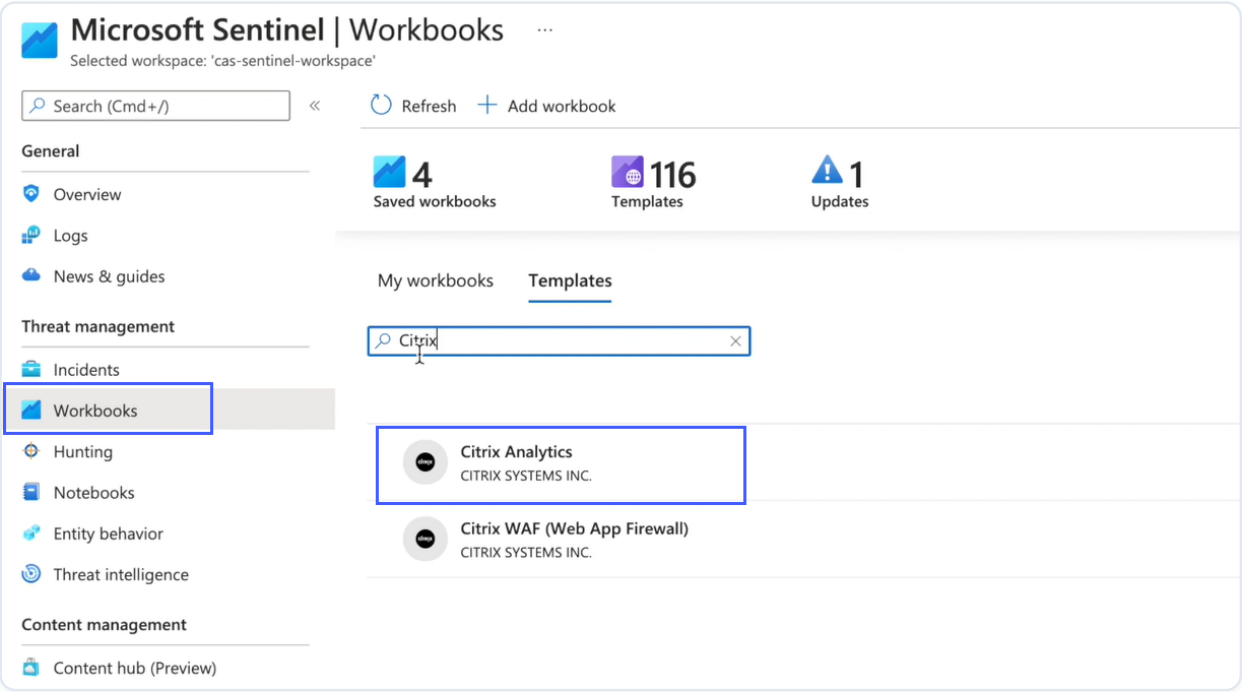


查看 Citrix Analytics 工作簿

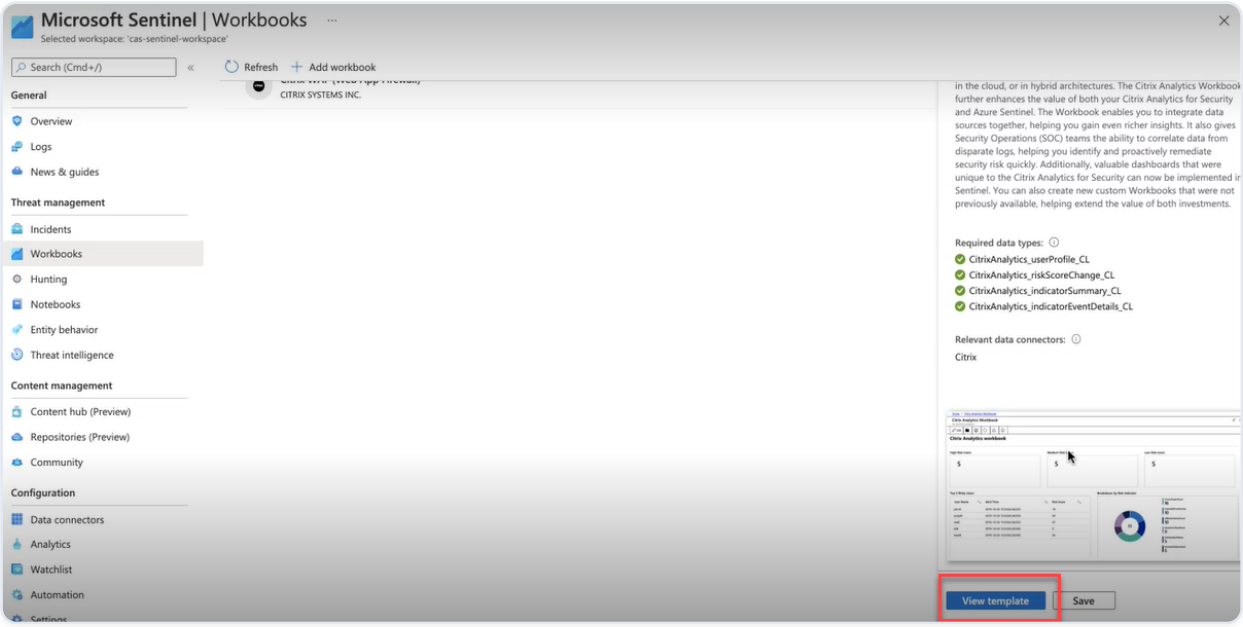
当日志表成功创建后，请执行以下操作：

1. 选择 **工作簿** 并搜索 **Citrix Analytics**。选择 **Citrix Analytics**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



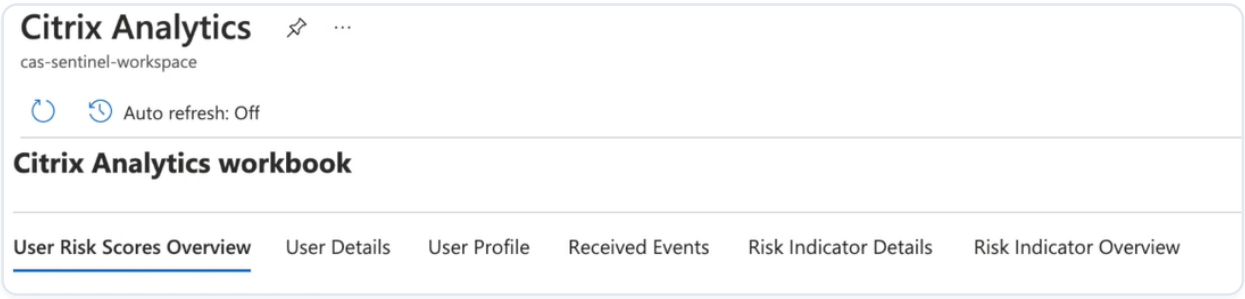
2. 选择 **查看模板** 以打开 Citrix Analytics 工作簿。



在 Citrix Analytics 工作簿中，您可以在以下仪表板中查看用户事件：

- **用户风险评分概览**：提供组织中高风险用户的综合视图。
- **用户详细信息**：提供用户的详细信息及其风险行为。
- **用户配置文件**：提供与用户相关的事件指标。
- **接收到的事件**：提供从 Citrix Analytics for Security 接收到的事件。
- **风险指标详细信息**：提供有关用户触发的内置和自定义风险指标的详细信息。
- **风险指标概览**：提供用户触发的风险指标的综合视图。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



用户风险评分概览

此仪表板提供组织中高风险用户的综合视图。用户按风险级别（高、中、低）进行分类。风险级别基于用户活动中的异常情况，并相应地分配风险评分。有关高风险用户类型的更多信息，请参阅用户仪表板。

选择一个时间段以查看组织中的风险用户。

用户风险评分概览(/en-us/citrix-analytics/media/risk-score-overview-sentinel-workbook.png)

用户详细信息

此仪表板提供与用户关联的风险评分和风险指标。

搜索用户并查看可能对您的组织构成威胁的风险活动。为了缓解威胁，您可以根据用户帐户的风险严重性采取适当措施。

用户详细信息(/en-us/citrix-analytics/media/user-details-sentinel-workbook.png)

用户配置文件

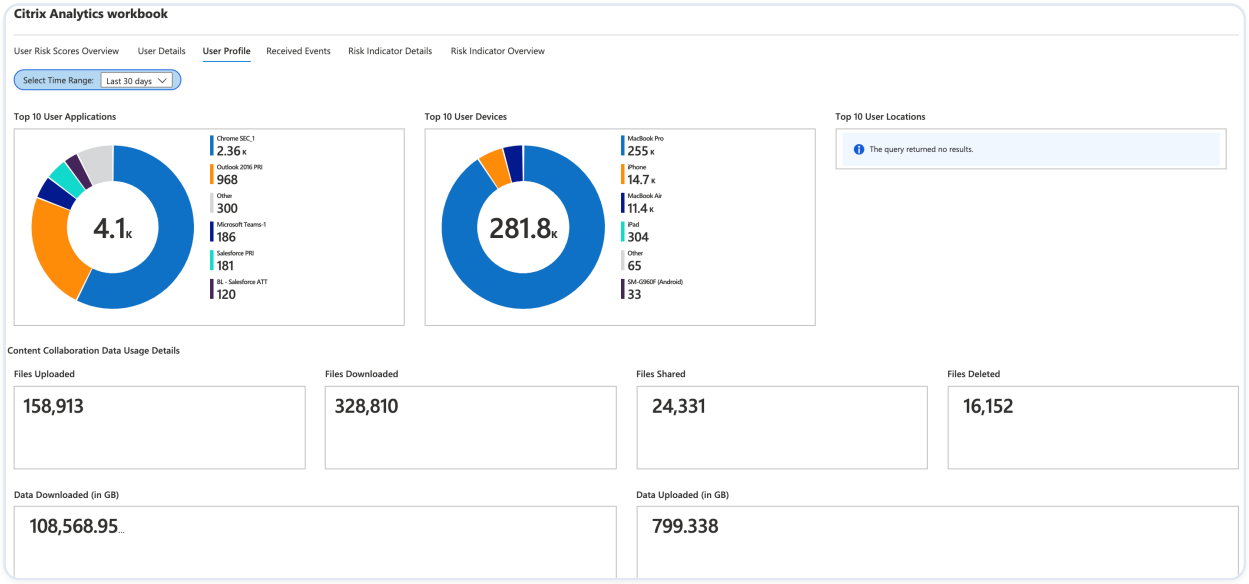
此仪表板提供所选时间段内与您的用户相关的事件指标详细信息。这些指标提供了对用户活动的深入了解，例如：

- 用户使用的前 10 个应用程序
- 用户使用的前 10 个设备
- 用户登录的前 10 个位置

使用这些报告，您可以：

- 识别用户的使用趋势
- 发现用于访问资源的非合规设备
- 检查您的用户是否存在任何潜在的风险访问

© 1997–2026 Citrix Systems, Inc. All rights reserved.



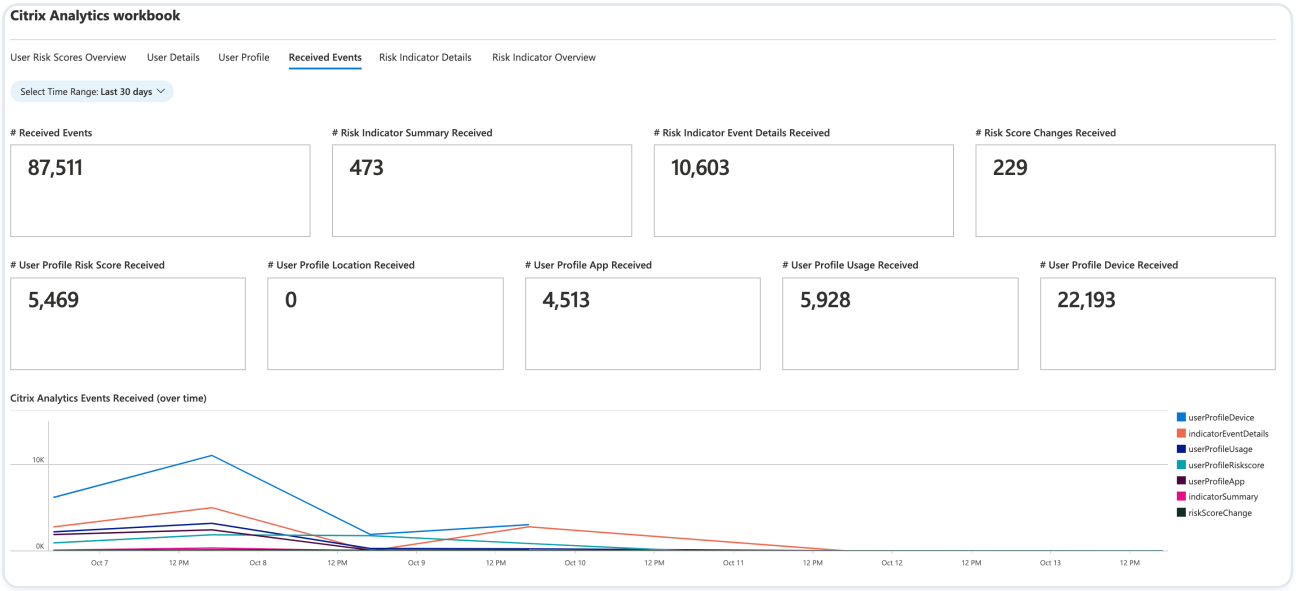
接收到的事件

在选定的时间段内，您可以查看从 Citrix Analytics for Security 接收到的事件总数。接收到的事件总数包括以下内容：

- 风险指标摘要：指示与用户风险指标摘要相关的事件。有关各种风险指标摘要事件的信息，请参阅 风险指标架构。
- 风险指标事件详细信息：指示与用户风险指标详细信息相关的事件。有关各种风险指标详细信息事件的信息，请参阅 风险指标架构。
- 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 用户仪表板。
- 风险评分更改：指示与用户风险评分更改相关的事件。有关信息，请参阅 用户仪表板。
- 用户配置文件位置：指示与用户登录位置相关的事件。
- 用户配置文件应用程序：指示与用户使用的应用程序相关的事件。
- 用户配置文件使用情况：指示与用户数据使用情况相关的事件。
- 用户配置文件设备：指示与用户使用的设备相关的事件。

通过定期查看仪表板，您可以确保事件是否正确流入您的 Microsoft Sentinel 工作区。接收到的事件总数中的任何差异都可能表明与 Citrix Analytics for Security 存在集成问题。您可以执行必要的步骤来调试这些问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

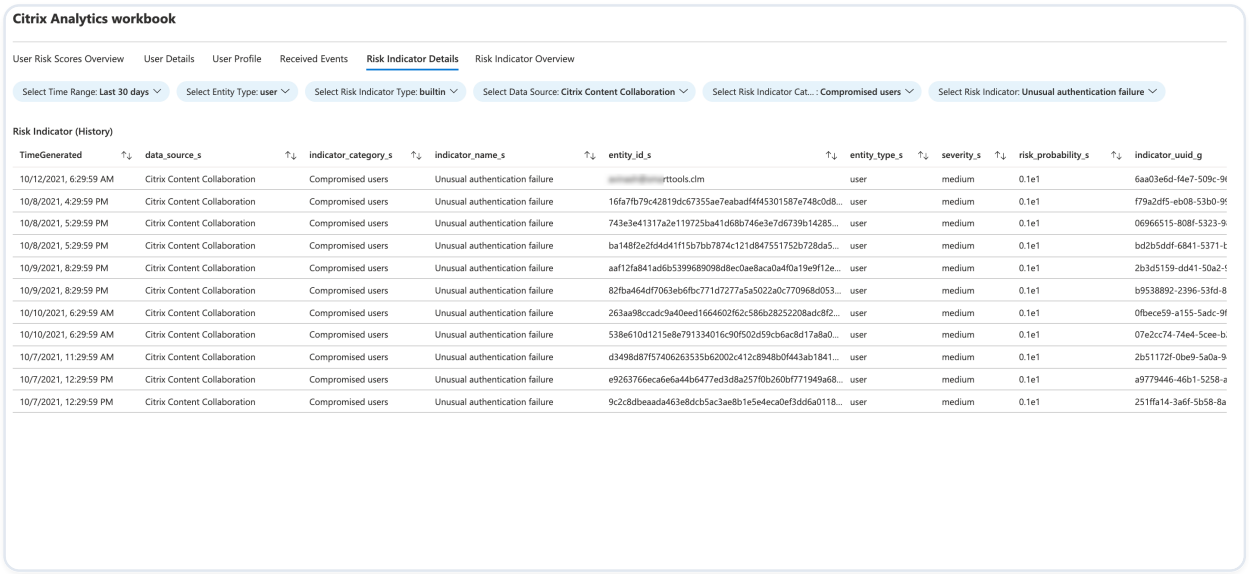


风险指标详细信息

此仪表板提供由您的用户触发的风险指标的详细信息。

您可以通过选择一个或多个类别来查看风险指标详细信息：

- 时间范围：选择一个时间范围以查看在此期间触发的风险指标的详细信息。
- 实体类型：选择一个用户以查看相关风险指标的详细信息。
- 风险指标类型：选择内置或自定义风险指标以查看其详细信息。
- 数据源：选择一个数据源以查看相关风险指标。
- 风险指标类别：选择风险类别以查看相关风险指标。
- 风险指标：按名称选择一个风险指标并查看其详细信息。



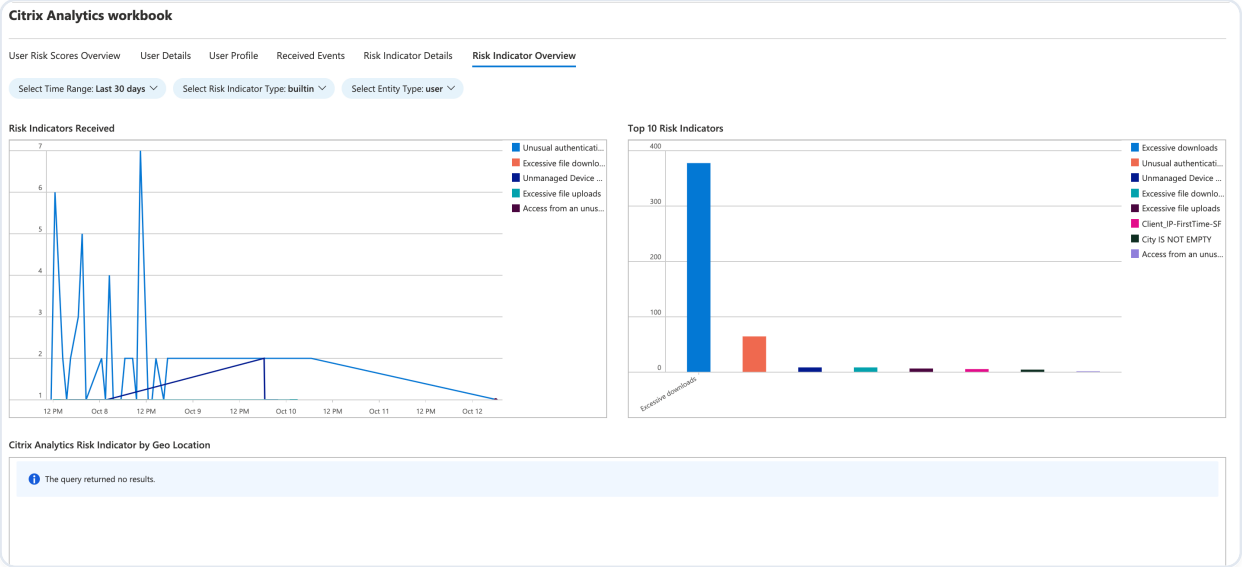
© 1997–2026 Citrix Systems, Inc. All rights reserved.

风险指标概览

此仪表板提供您的用户触发的所有风险指标的综合视图。

您可以通过选择一个或多个类别来查看风险指标：

- 时间范围：选择一个时间段以查看在此期间触发的风险指标。
- 风险指标类型：选择内置或自定义以查看相关风险指标。
- 实体类型：选择用户以查看相关风险指标。



通过 Logstash 集成 Sentinel 的故障排除指南

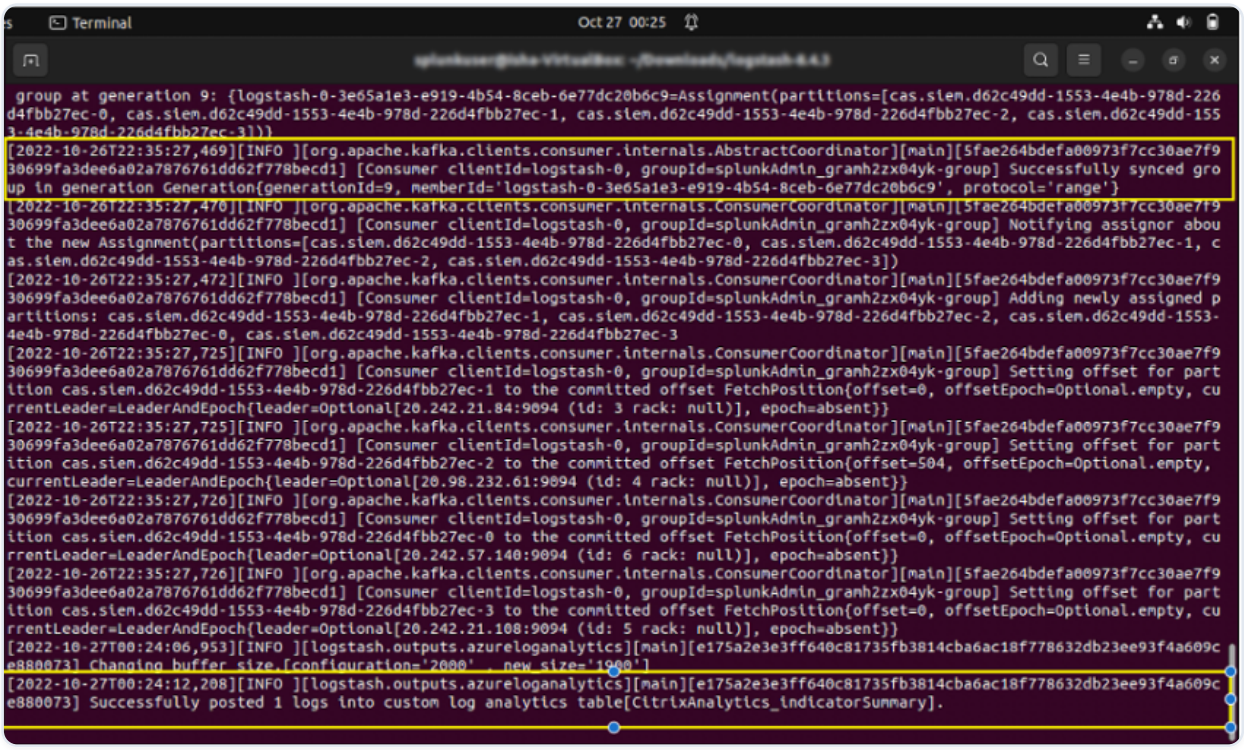
本文列出了在使用 Logstash 将 Microsoft Sentinel 与 Citrix Analytics 集成时可能遇到的问题的排查要点。要了解更多信息，请参阅 (/zh-cn/security-analytics/siem-integration/kafka-or-logstash-siem-integration.html)。

检查 Logstash 服务器日志

您可以检查终端窗口中显示的 Logstash 服务器日志，以验证数据是否已正确摄取到 Sentinel 工作区中的自定义日志表中。

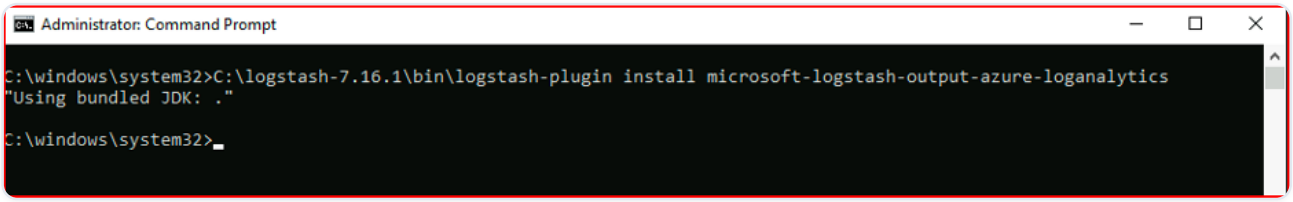
1. 要查看日志详细信息，您必须从 **Settings > Data Exports > Configuration** 选项卡下载 Logstash 配置文件 **>** 展开 **SIEM Environment**。在 **Azure Sentinel (Preview)** 下，单击 **Download Logstash Config File**。
2. 使用配置文件启动 Logstash 服务器后，您可以在同一终端窗口中查找以下日志，这些日志表示与 Microsoft Azure 托管的 Log Analytics 工作区成功连接。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

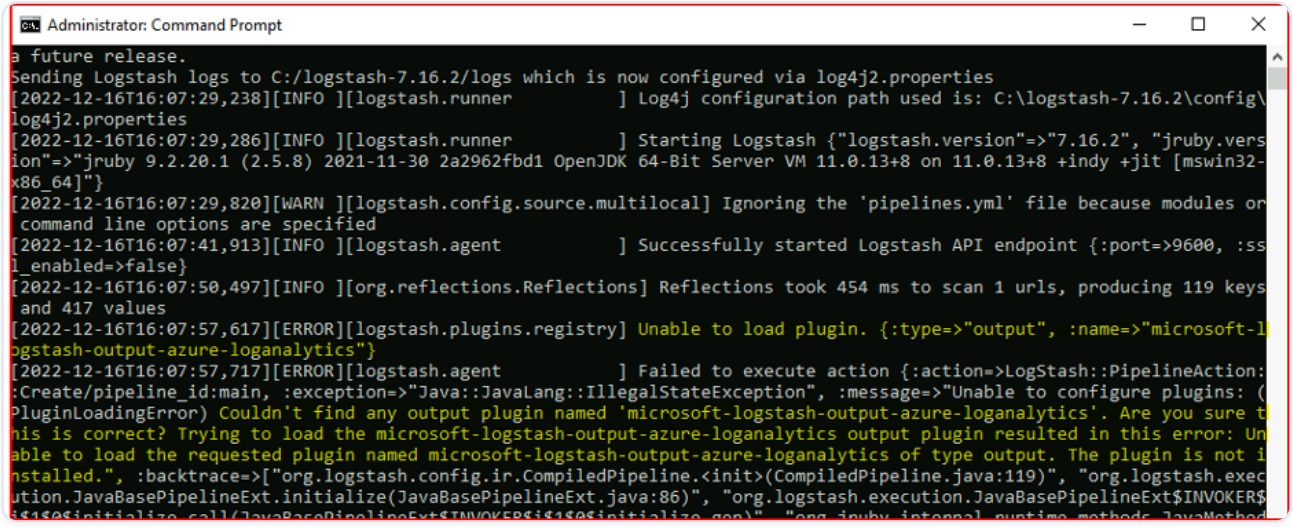


常见错误：使用捆绑的 JDK

尝试安装 Microsoft 日志分析插件时，报告的常见错误如下所示：



在此之后，尝试运行 Logstash 服务器时，您可能会看到以下错误：



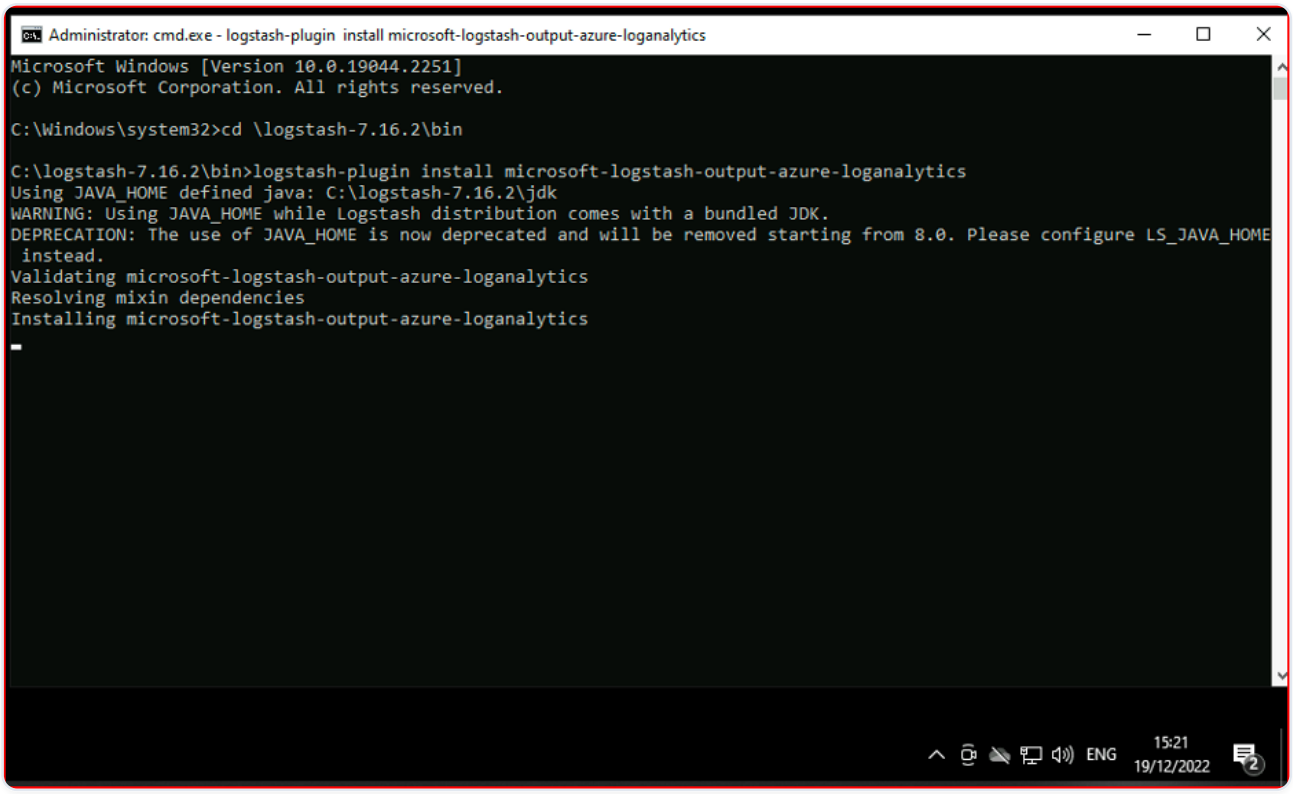
要解决此问题，请将 JAVA_HOME 设置为捆绑的 JDK：

1. 转到 Windows 环境变量
2. 创建一个名为“JAVA_HOME”的新系统变量

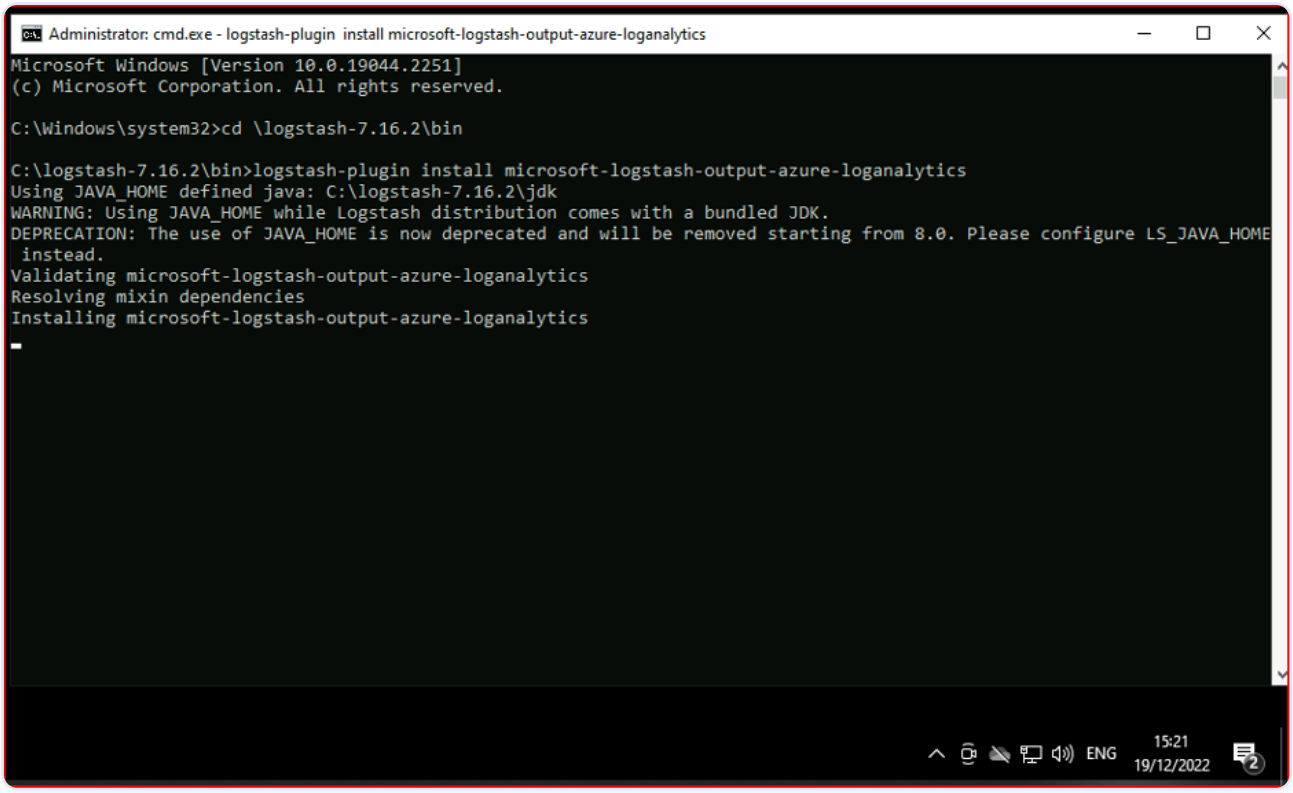
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 添加捆绑的 Logstash JDK 路径 (< path_to_logstash >/logstash-X.X.X/jdk)

完成上述步骤后，再次尝试安装插件时，将出现以下屏幕：

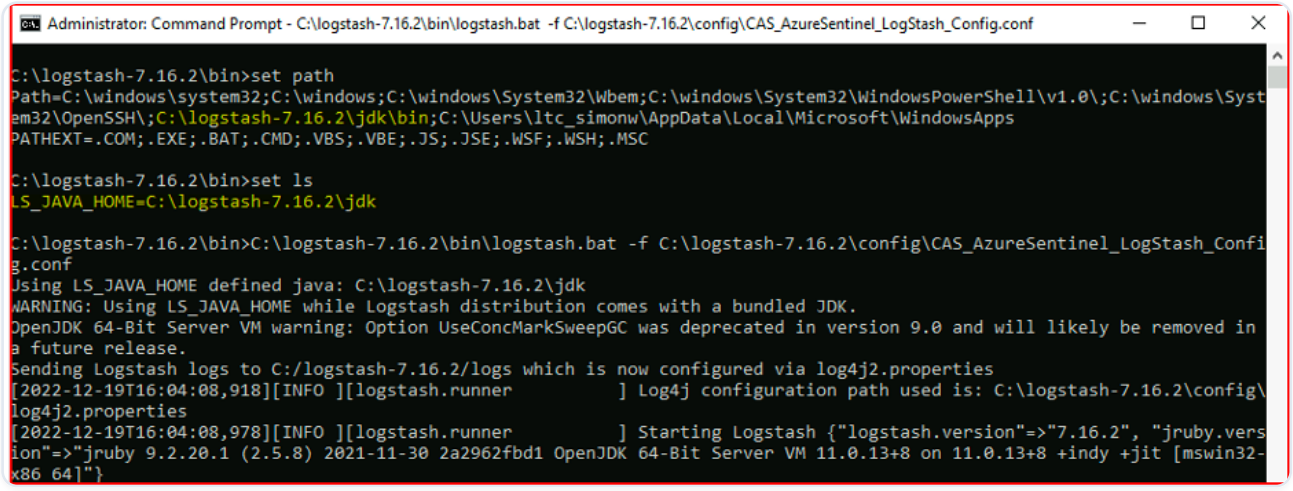


如果您使用 LS_JAVA_HOME（因为 JAVA_HOME 已弃用），您还必须在系统 PATH 变量中指定捆绑 JDK 的位置，并且此路径必须指向 **jdk\bin** 文件夹（与 LS_JAVA_HOME 变量不同）：



© 1997–2026 Citrix Systems, Inc. All rights reserved.

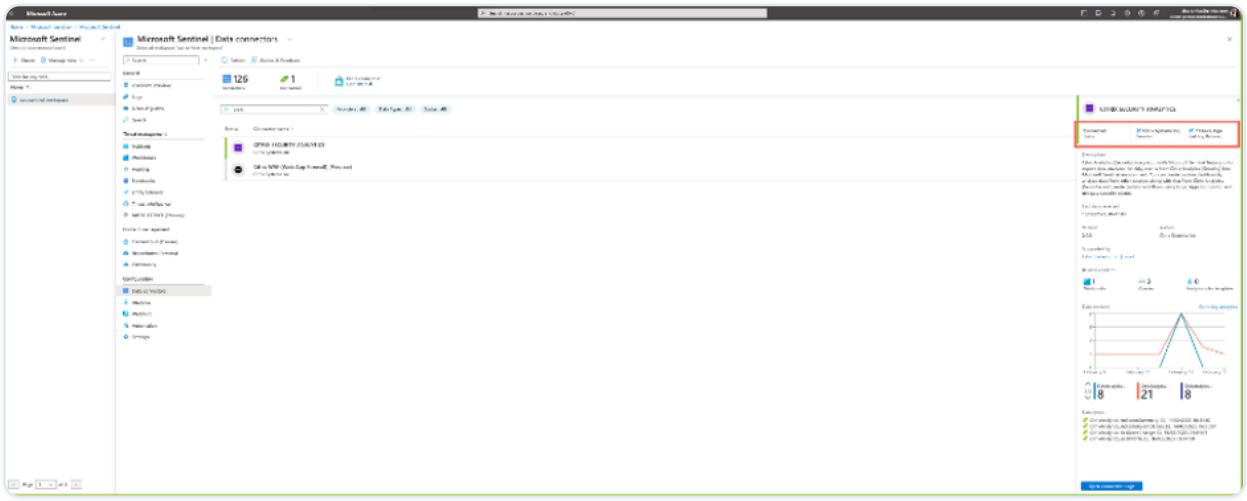
如果您使用 LS_JAVA_HOME（因为 JAVA_HOME 已弃用），您还必须在系统 PATH 变量中指定捆绑 JDK 的位置，并且此路径必须指向 **jdk\bin** 文件夹（与 LS_JAVA_HOME 变量不同）：



检查 Microsoft Sentinel 工作簿

要确认 Citrix Analytics 发送的数据是否已成功输入到 Log Analytics 工作区中相应的自定义日志表（要了解有关 Microsoft Sentinel 与 Citrix Analytics 集成的更多信息，请参阅 Microsoft Sentinel 集成）：

1. 导航到 **Azure 门户 > Microsoft Sentinel > 选择 appropriate_workspace > 数据连接器 >** 选择并单击 **Citrix Security Analytics**。
2. 检查顶部栏以验证连接状态。



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 > Microsoft Sentinel > 数据连接器 > CITRIX SECURITY ANALYTICS > 工作簿**。

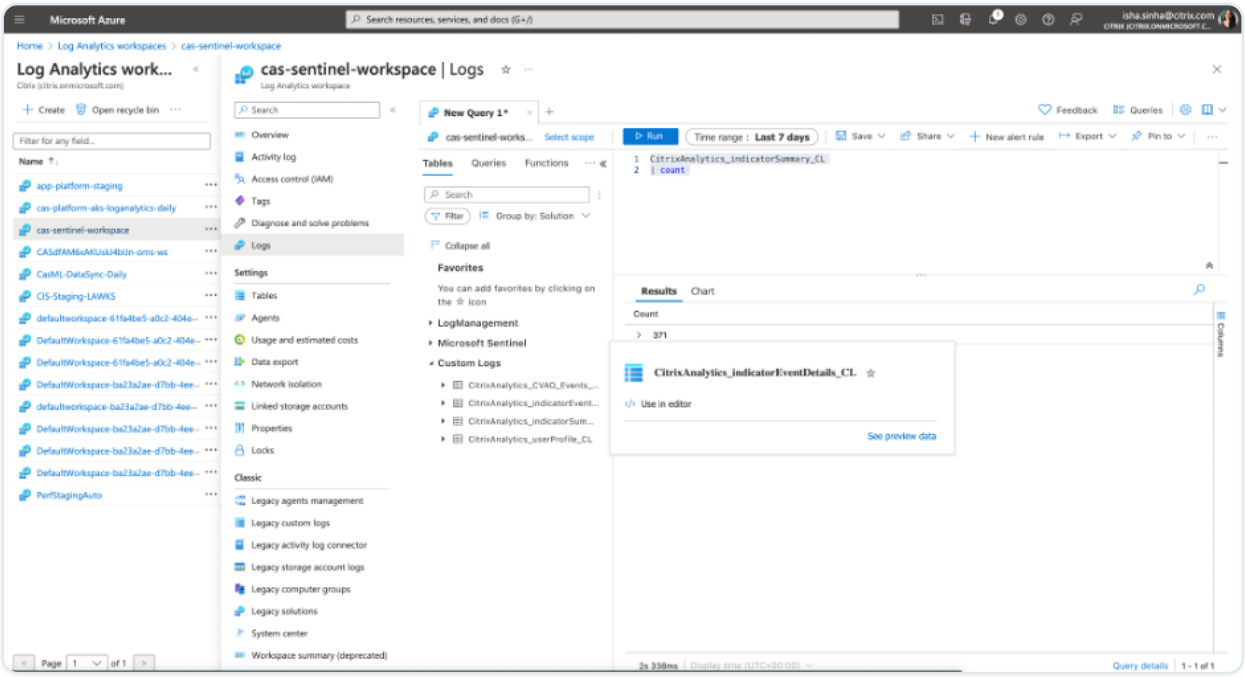
© 1997–2026 Citrix Systems, Inc. All rights reserved.



使用 KQL 检查 Log Analytics 工作区日志

您还可以通过对相应的自定义日志表运行 KQL 查询来检查正确的数据是否已进入您的 LogAnalytics 工作区。

1. 导航到 **Azure 门户 > Log Analytics 工作区** 并搜索正确的工作区。
2. 在左侧面板中，选择 **日志** 并在 **表** 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 Log Analytics 工作区上的 KQL 查询指南，请参阅 Log Analytics 教程）。
4. 单击 **运行**。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Elasticsearch 集成

注意

请联系 mailto:CAS-PM-Ext@cloud.com 以请求 Elasticsearch 集成、将数据导出到 Elasticsearch 或提供反馈方面的帮助。

使用 Logstash 引擎将 Citrix Analytics for Security 与 Elasticsearch 集成。此集成使您能够将 Citrix IT 环境中的用户数据导出并关联到 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）结合使用。

有关集成优势以及发送到 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。

先决条件

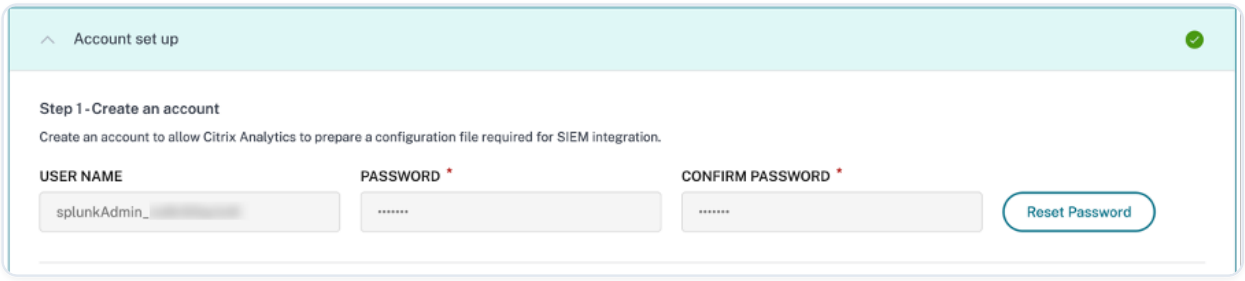
- 为至少一个数据源开启数据处理。这有助于 Citrix Analytics for Security™ 启动 Elasticsearch 集成过程。
- 确保以下端点在您的网络允许列表中。

端点	美国区域	欧盟区域	亚太南部区域
Kafka 代理	`casnb-0.citrix.com:9094`	`casnb-eu-0.citrix.com:9094`	`casnb-aps-0.citrix.com:9094`
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`	`casnb-aps-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`		

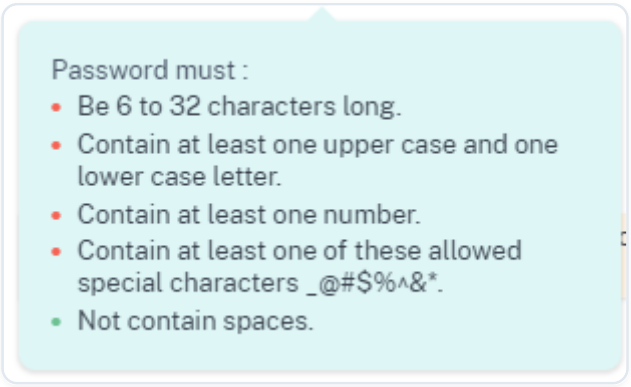
与 Elasticsearch 集成

1. 转到 **设置 > 数据导出**。
2. 在 **账户设置** 部分，通过指定用户名和密码来创建账户。此账户用于准备集成所需的配置文件。

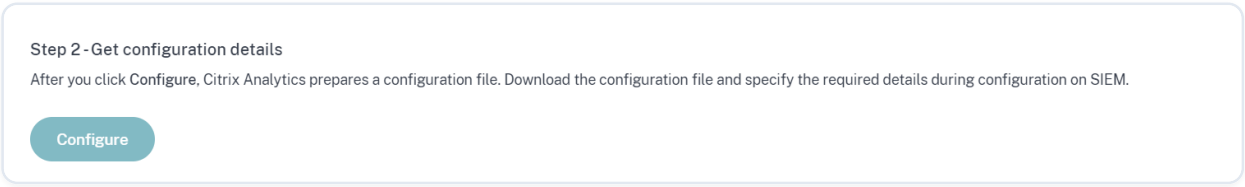
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 确保密码满足以下条件：



4. 点击 **配置** 以生成 Logstash 配置文件。



5. 从 SIEM 环境部分选择 **Elasticsearch** 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 Elasticsearch 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**：包含 SSL 连接所需的证书。

   注意

   这些文件包含敏感信息。请将其保存在安全的位置。

   选择 弹性搜索(/en-us/citrix-analytics/media/elasticsearch-select.png)

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，将以下文件放置在指定目录中：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

主机类型	文件名	目录路径
林纳克斯	CAS_Elasticsearch_LogStash_Config.config	对于 Debian 和 RPM 软件包：`/etc/logstash/conf.d/`
		对于 .zip 和 .tar.gz 归档文件：`{extract.path}/config`
	kafka.client.truststore.jks	对于 Debian 和 RPM 软件包：`/etc/logstash/ssl/`
		对于 .zip 和 .tar.gz 归档文件：`{extract.path}/ssl`
视窗	CAS_Elasticsearch_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。

c. 打开 Logstash 配置文件并执行以下操作：

i. 在该文件的输入部分中，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 信任库位置**：您的 SSL 客户端证书的位置。这是 kafka.client.truststore.jks 文件在您的主机中的位置。

```
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，输入您的主机或运行 Elasticsearch 的集群的地址。

Elasticsearch 输出部分(/en-us/citrix-analytics/media/elasticsearch-output-section.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. 重新启动您的主机，以将 Citrix Analytics for Security 处理的数据发送到 Elasticsearch。

配置完成后，验证您是否可以在 Elasticsearch 中查看 Citrix Analytics 数据。

开启或关闭数据传输

Citrix Analytics for Security 准备好配置文件后，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. 转到 **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。

   SIEM 传输关闭(/en-us/citrix-analytics/media/siem-turn-off.png)

   将出现一个警告窗口，供您确认。单击**关闭数据传输**按钮以停止传输活动。

   SIEM 传输关闭警告(/en-us/citrix-analytics/media/siem-turn-off-warning.png)

要再次启用数据传输，请打开切换按钮。

使用 Kafka 或 Logstash 数据连接器进行 SIEM 集成

Citrix Analytics for Security™ SIEM 集成使您能够将用户数据从 Citrix Analytics 导出并关联到您的 SIEM 环境，从而更深入地了解组织的安全状况。

有关集成优势以及发送到 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 与您的 SIEM 解决方案集成：

1. 通过 Kafka 端点连接
2. 通过 Logstash 数据代理连接，并使用基于 Kafka 的摄取

先决条件

- 为至少一个数据源开启数据处理。这有助于 Citrix Analytics for Security 开始与您的 SIEM 工具集成。
- 确保以下端点在您的网络允许列表中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

端点	美国区域	欧盟区域	亚太南部区域
Kafka 代理	`casnb-0.citrix.com:9094`	`casnb-eu-0.citrix.com:9094`	`casnb-aps-0.citrix.com:9094`
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`	`casnb-aps-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`		

使用 Kafka 与 SIEM 服务集成

Kafka 是一种开源软件，用于数据的实时流式传输。使用 Kafka，您可以分析实时数据以获得更快的洞察。通常，处理足够数据的大型组织会使用 Kafka。

北向 Kafka 是一个内部中间层，使 Citrix Analytics 能够通过 Kafka 端点与 SIEM 客户共享实时数据馈送。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 进行集成需要以下参数：

属性名称	描述	配置数据示例
用户名	Kafka 提供的用户名。	`'sasl.username': cas_siem_user_name,`
主机	您要连接的 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	您需要读取消费者共享消息的组名称。	`'group.id': cas_siem_group_id,`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

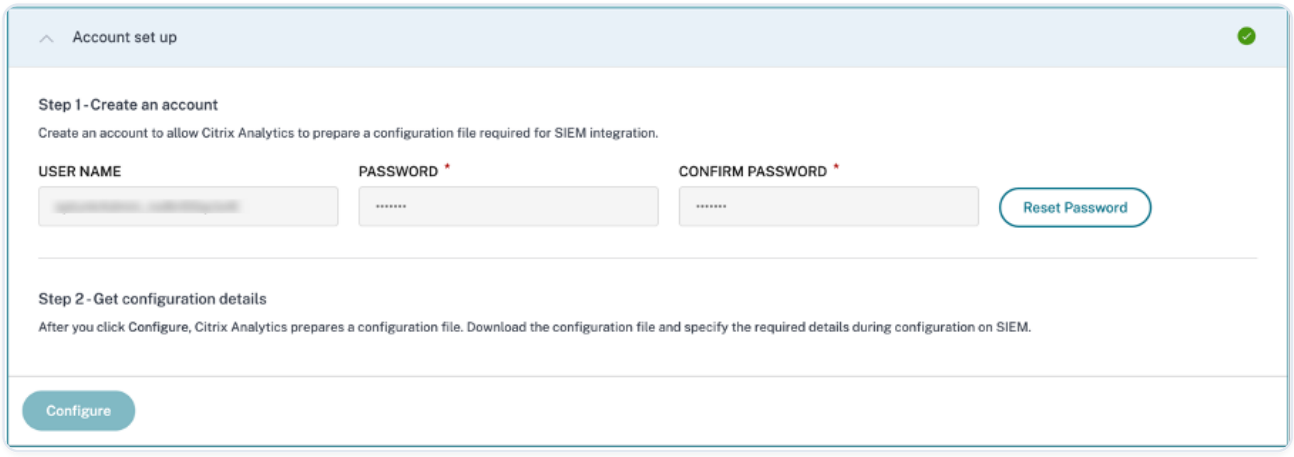
属性名称	描述	配置数据示例
安全协议	安全协议的名称。	`'security.protocol': 'SASL_SSL',`
SASL 机制	一种身份验证机制，通常用于加密以实现安全身份验证。	`'sasl.mechanisms': 'SCRAM-SHA-256',`
SSL 信任存储位置	存储证书文件的位置。客户端信任存储密码是可选的，通常留空。	`'ssl.ca.location': ca_location`
会话超时	使用 Kafka 时用于检测客户端故障的会话超时。	`'session.timeout.ms': 60000,`
自动偏移量重置	定义在没有初始偏移量时从主题分区消费数据时的行为。您可以设置诸如最新、最早或无等值。	`'auto.offset.reset': 'earliest',`

以下是配置输出示例：

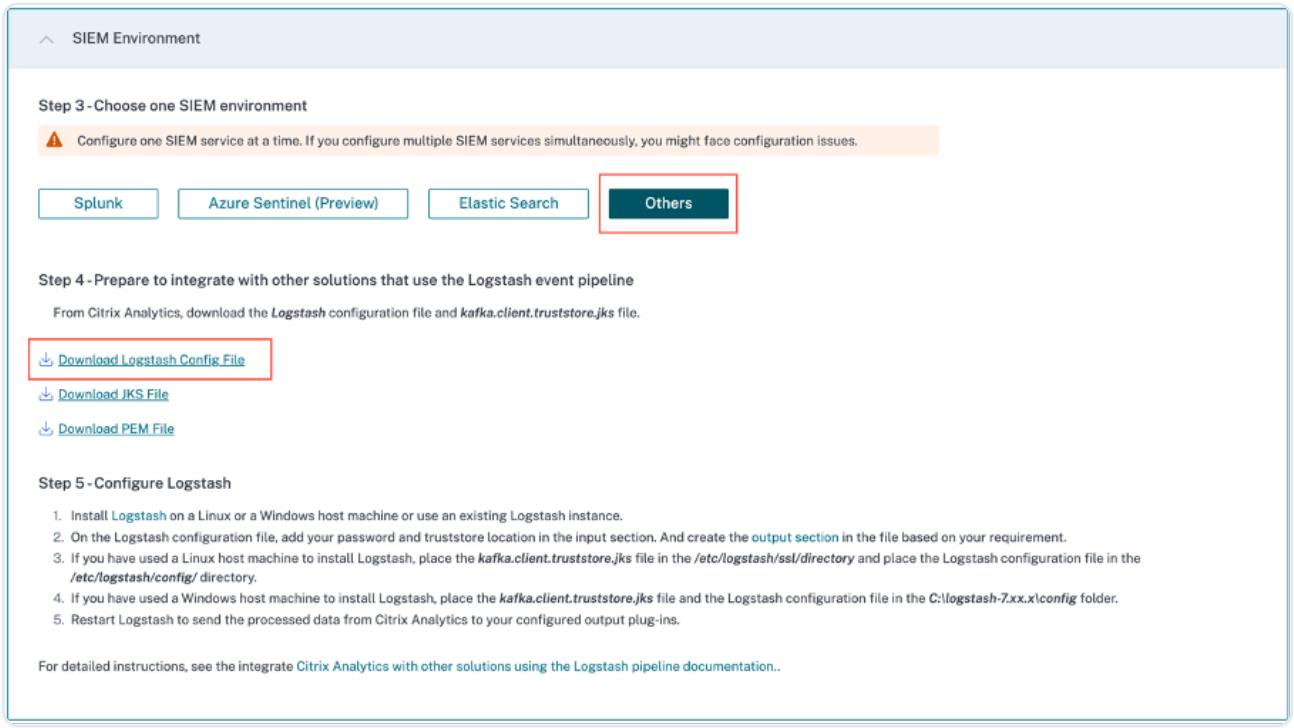
```
{'bootstrap.servers': cas_siem_host,
                    'client.id': cas_siem_topic,
                    'group.id': cas_siem_group_id,
                    'session.timeout.ms': 60000,
                    'auto.offset.reset': 'earliest',
                    'security.protocol': 'SASL_SSL',
                    'sasl.mechanisms': 'SCRAM-SHA-256',
                    'sasl.username': cas_siem_user_name,
                    'sasl.password': self.CLEAR_PASSWORD,
                    'ssl.ca.location': ca_location
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```



上述参数可在 Logstash 配置文件中找到。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已启用的 SASL_SSL 安全协议，并以 9094 端口进行公共访问。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Apache Kafka 具有一个安全组件，可使用 SSL 加密对传输中的数据进行加密。 启用加密并设置 SSL 证书后，通过网络传输的数据将进行加密和保护。只有第一台和最后一台机器能够解密通过 SSL 发送的数据包。

身份验证

身份验证分为以下两个级别：

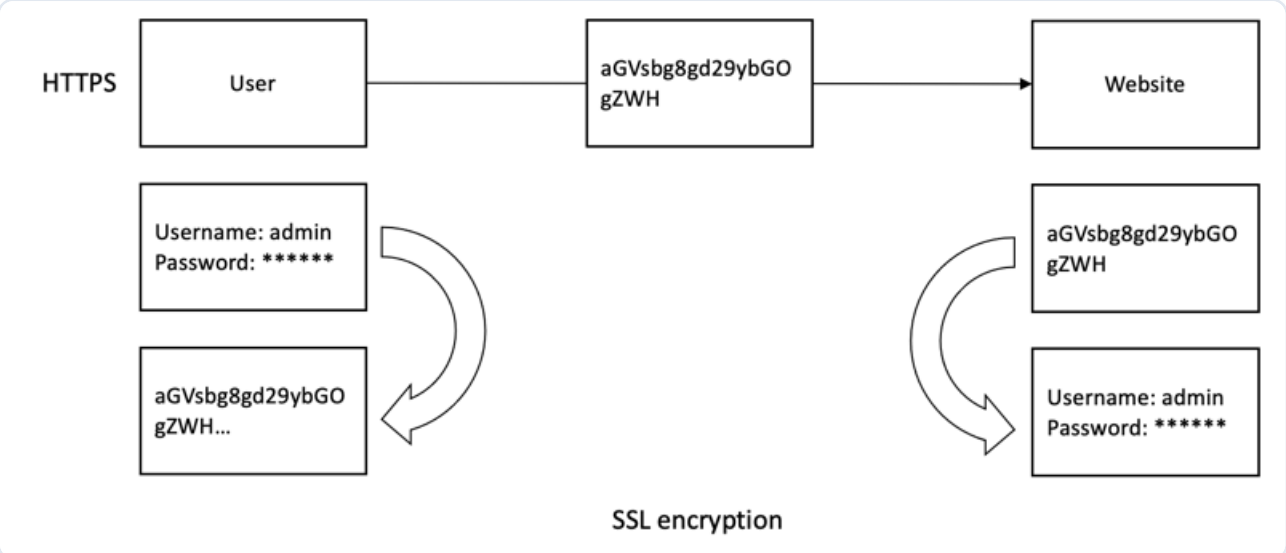
1. TLS/客户端与服务器之间。
    - 用于客户端和服务器之间 TLS 身份验证交换的服务器证书（公钥）。
    - 不支持基于客户端的身份验证或双向身份验证（需要客户端私钥证书）。
2. 用于对 TOPICS/端点进行访问控制的用户名/密码
    - 确保特定客户端只能从特定客户主题读取
    - SASL/SCRAM 用于用户名/密码身份验证机制，并结合 TLS 加密来实现安全身份验证。

使用 SSL 进行加密，并使用 SASL/SSL 和 SASL/PLAINTEXT 进行身份验证

默认情况下，Apache Kafka 以 PLAINTEXT 方式通信，所有数据都以明文形式发送，任何路由器都可以读取数据内容。Apache Kafka 具有一个安全组件，可使用 SSL 加密对传输中的数据进行加密。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。启用 SSL 加密后，只有第一台和最后一台机器才能解密正在发送的数据包。

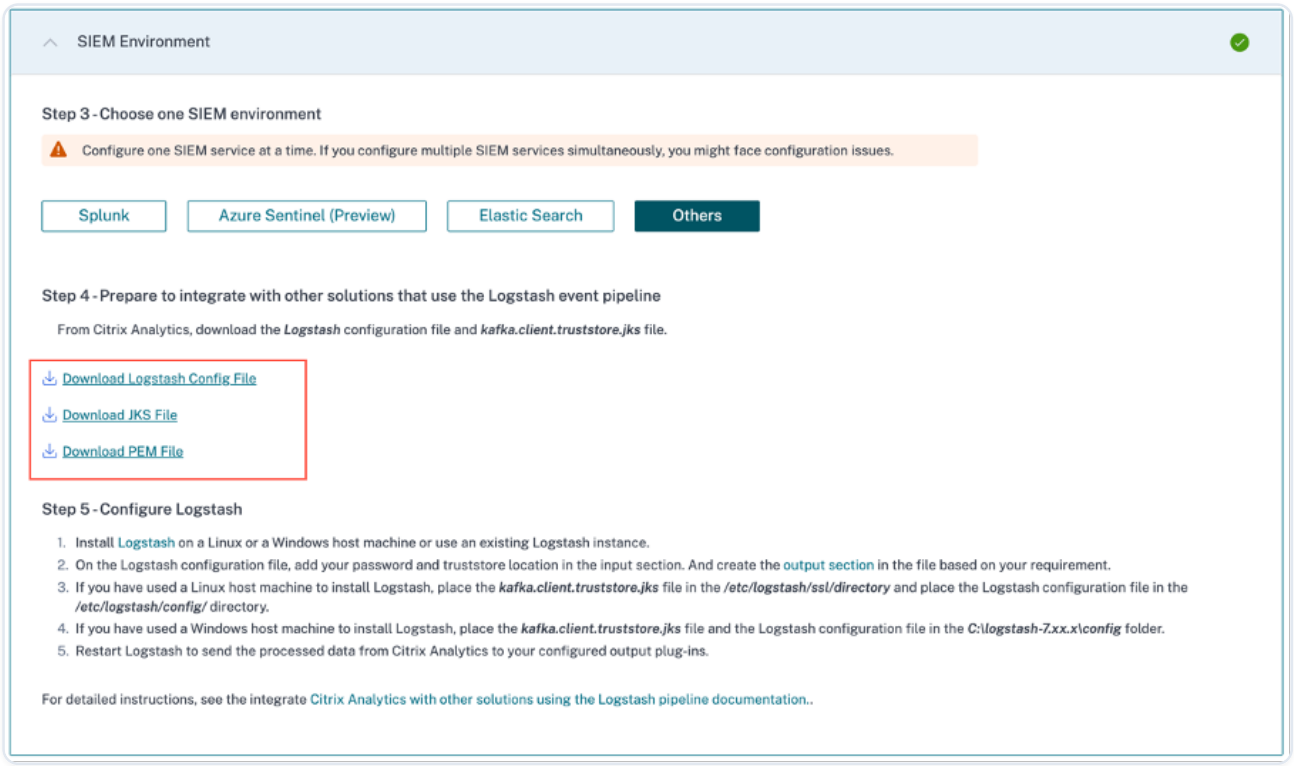
由于使用了双向 SSL 加密，用户名/密码登录对于外部通信是安全的。

加密仅在传输过程中进行，数据仍以未加密的形式存储在代理的磁盘上。



在客户端配置中，需要客户端信任库 JKS 文件和 PEM 文件（从信任库 JKS 文件转换而来）。您可以从 Citrix Analytics for Security GUI 下载这些文件，如以下屏幕截图所示：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



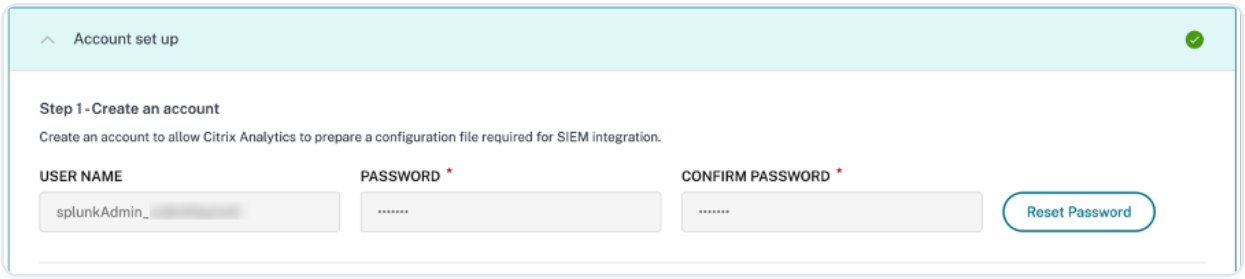
使用 Logstash 进行 SIEM 集成

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 Citrix Analytics for Security 中的数据事件发送到 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。

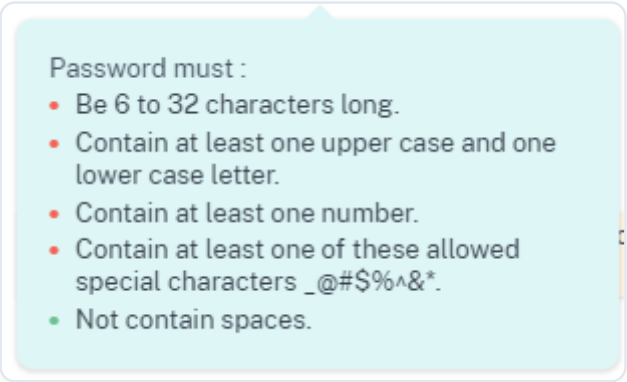
使用 Logstash 与 SIEM 服务集成

1. 转到 **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。

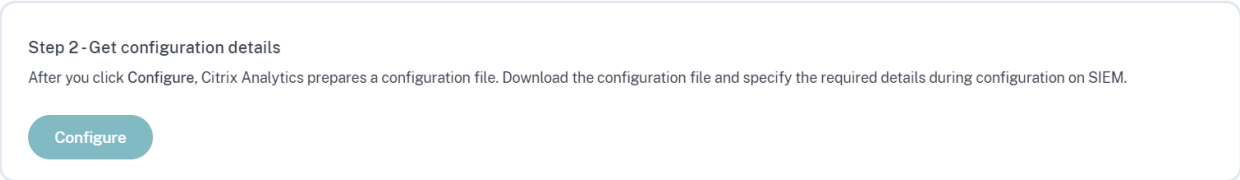


3. 确保密码满足以下条件：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 选择 **配置** 以生成 Logstash 配置文件。

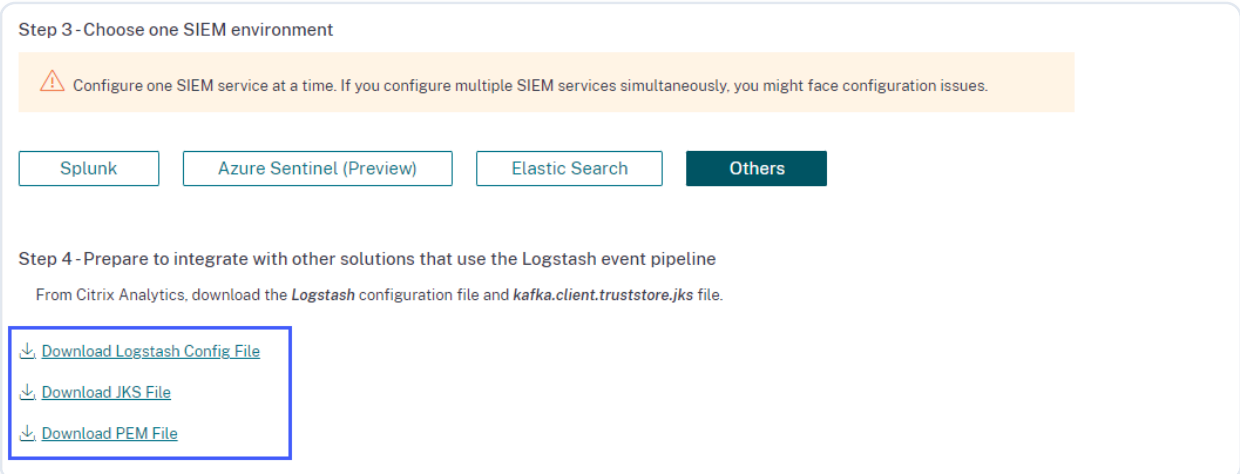


5. 选择**其他**选项卡以下载配置文件。

   - **Logstash 配置文件**：此文件包含配置数据（输入、筛选器和输出部分），用于使用 Logstash 数据收集引擎从 Citrix Analytics for Security 发送事件。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 SIEM 时需要此文件。
   - **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。请将其保存在安全的位置。



6. 配置 Logstash：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 在您的 Linux 或 Windows 主机上，安装 Logstash（与 Citrix Analytics for Security 兼容的测试版本：v7.17.7 和 v8.5.3）。您也可以使用现有的 Logstash 实例。

b. 在安装 Logstash 的主机上，将以下文件放置在指定目录中：

主机类型	文件名	目录路径
Linux 系统	CAS_Others_LogStash_Config.config	对于 Debian 和 RPM 软件包：`/etc/logstash/conf.d/`
		对于 .zip 和 .tar.gz 归档文件：`{extract.path}/config`
	kafka.client.truststore.jks	对于 Debian 和 RPM 软件包：`/etc/logstash/ssl/`
		对于 .zip 和 .tar.gz 归档文件：`{extract.path}/ssl`
Windows 系统	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 工作区 ID、主密钥。建议不要将这些敏感凭据以纯文本形式存储。为了保护集成安全，可以使用 Logstash 密钥库添加具有相应值的密钥，这些密钥反过来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 用于安全设置的密钥库。

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账户密码。
- **SSL 信任存储位置**：您的 SSL 客户端证书的位置。这是您的主机中 kafka.client.truststore.jks 文件的位置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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，输入您要发送数据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。

以下代码片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 中的已处理数据发送到 SIEM 服务。

配置完成后，登录您的 SIEM 服务并验证 SIEM 中的 Citrix Analytics 数据。

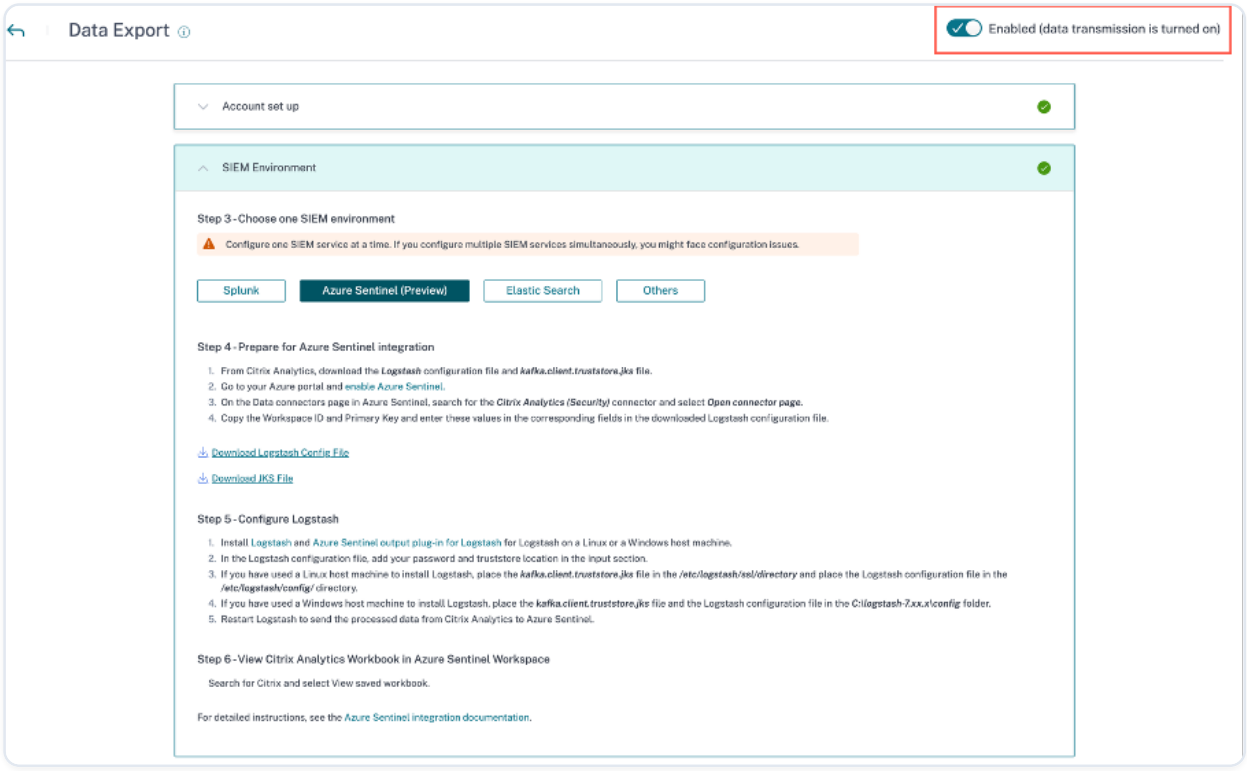
开启或关闭数据传输

Citrix Analytics for Security 准备好配置文件后，将为您的 SIEM 开启数据传输。

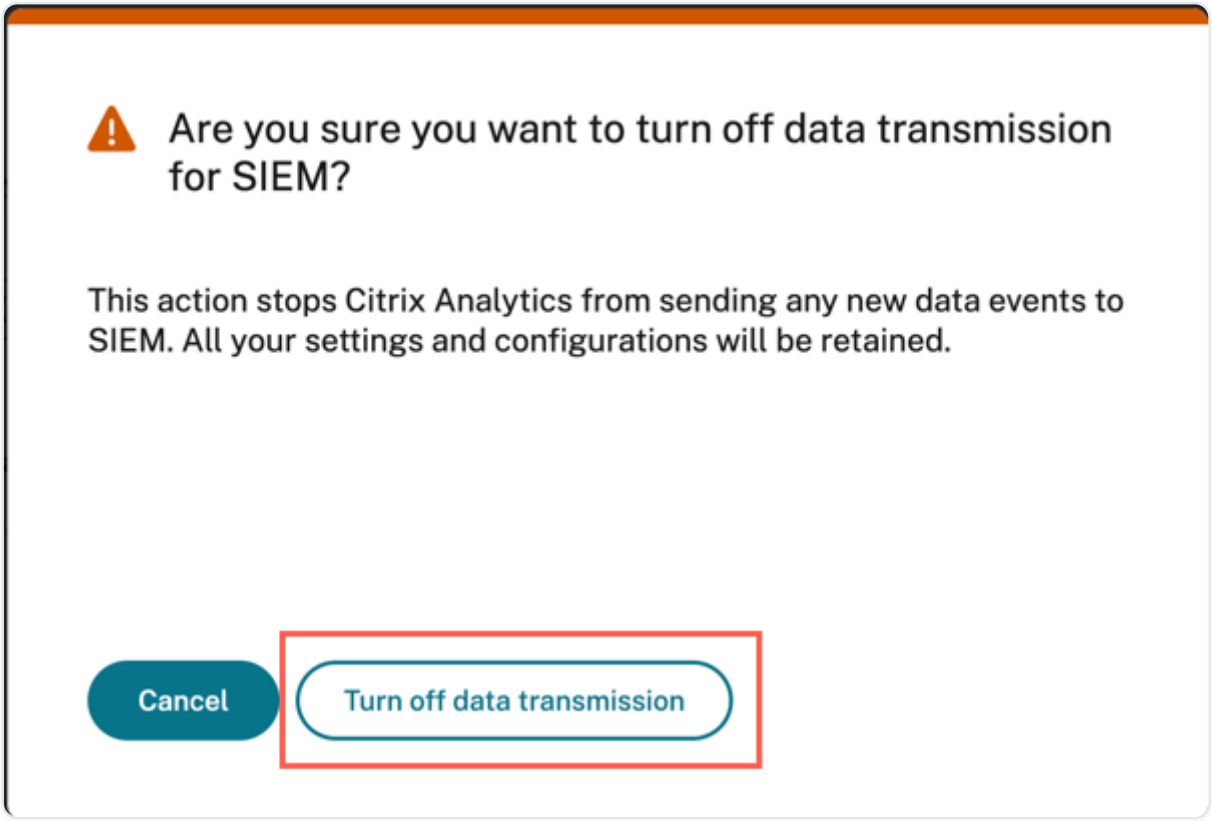
要停止从 Citrix Analytics for Security 传输数据：

1. 转到 **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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



将出现一个警告窗口以供您确认。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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

请联系 mailto:CAS-PM-Ext@cloud.com，以获取 SIEM 集成方面的帮助、将数据导出到您的 SIEM，或提供反馈。

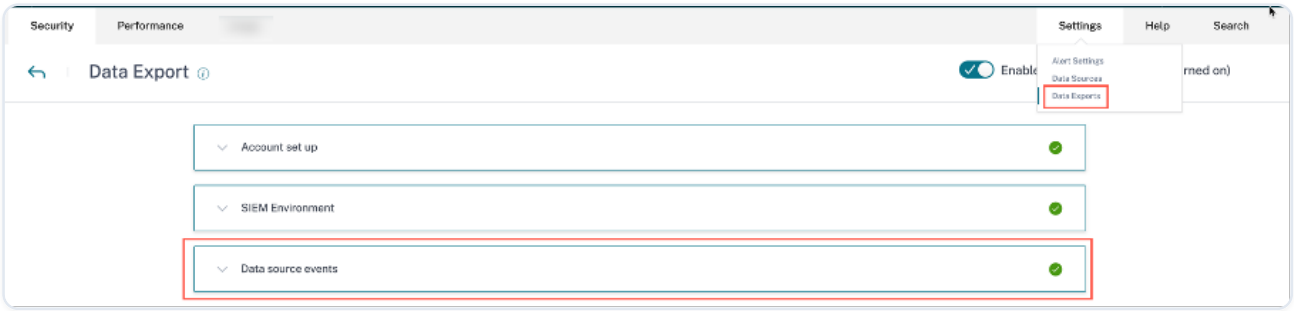
Citrix Analytics 适用于 SIEM 的数据导出格式

Citrix Analytics for Security™ 允许您与安全信息和事件管理 (SIEM) 服务集成。此集成使 Citrix Analytics for Security 能够将数据发送到您的 SIEM 服务，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：

- 斯普伦克
- 微软 Azure 哨兵
- 弹性搜索
- 使用基于 Kafka 或 Logstash 的数据连接器的其他 SIEM

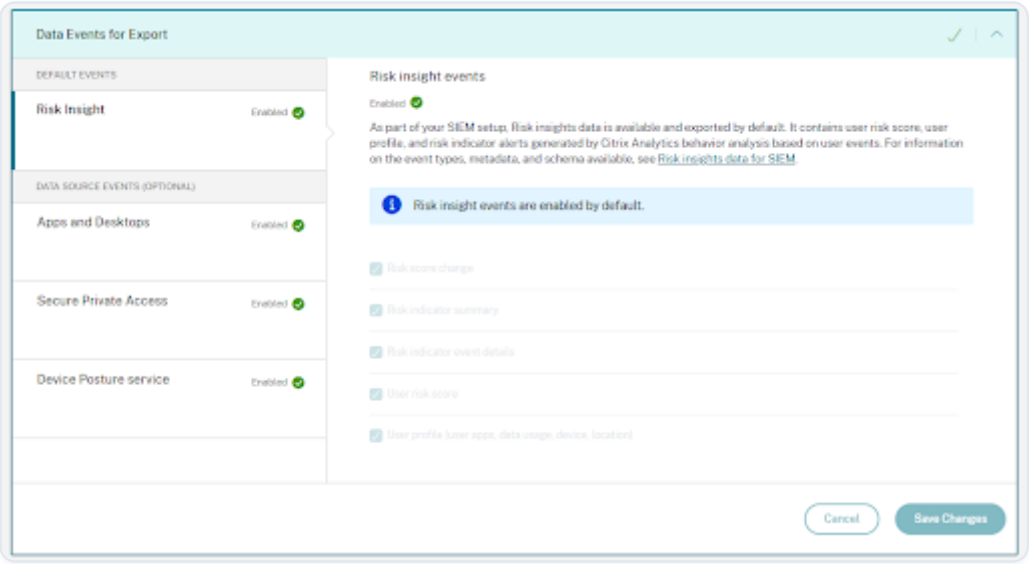
“**数据导出选项**”现已在全球范围内提供，位于“**设置**”下。要查看数据源事件，请导航到“**设置 > 数据导出 > 数据源事件**”。



Citrix Analytics for Security 发送到您的 SIEM 服务的风险洞察数据分为两种类型：

- 风险洞察事件 (默认导出)
- 数据源事件 (可选导出)

© 1997–2026 Citrix Systems, Inc. All rights reserved.



适用于 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）将开始流入您的 SIEM 部署。风险洞察数据集包括用户风险评分事件、用户配置文件事件和风险指标警报。这些由 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：

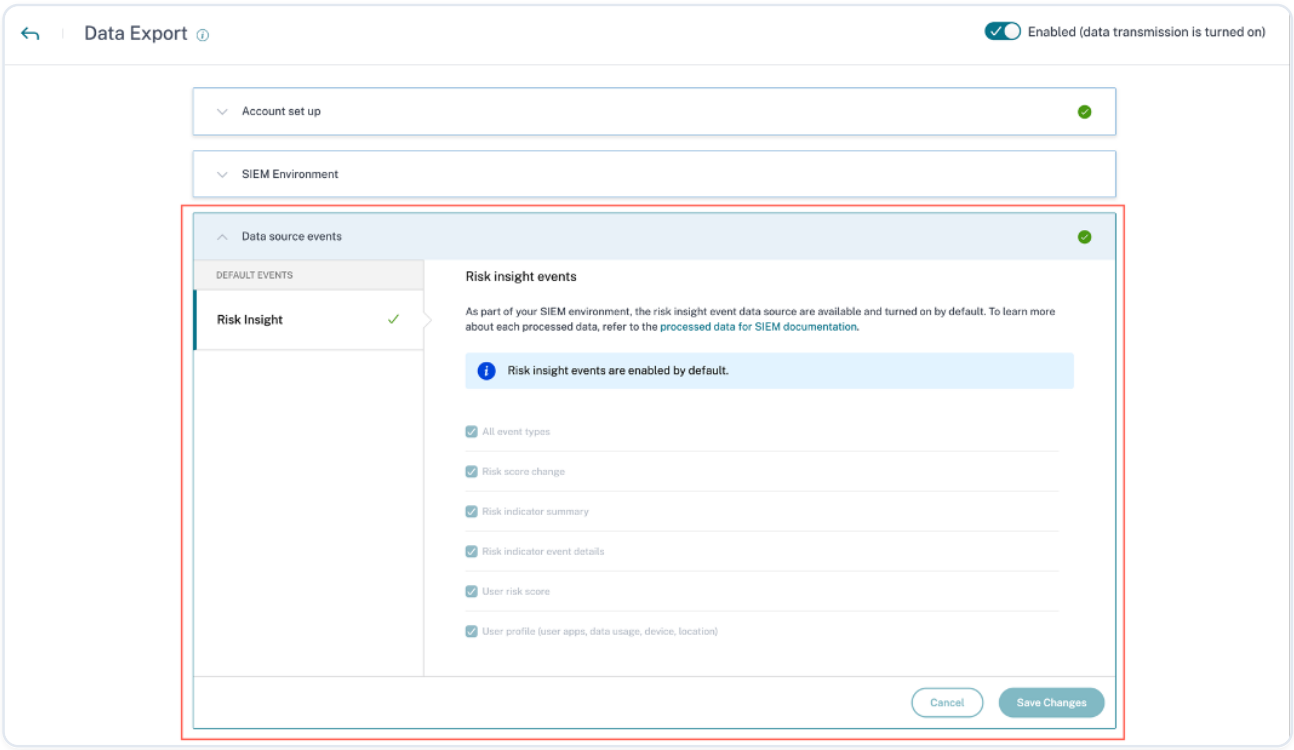
- **风险评分变化**：表示用户风险评分的变化。当用户风险评分变化等于或大于 3 且此变化以任何速率增加或下降超过 10% 时，数据将发送到 SIEM 服务。
- **风险指标摘要**：为用户触发的风险指标的详细信息。
- **风险指标事件详细信息**：与风险指标关联的用户事件。Citrix Analytics 会将每个风险指标事件最多 1000 个事件详细信息发送到您的 SIEM 服务。这些事件按发生的时间顺序发送。
- **用户风险评分事件**：用户的当前风险评分。Citrix Analytics for Security 每 12 小时将此数据发送到 SIEM 服务。
- **用户配置文件**：用户配置文件数据可分为：
  - **用户应用程序**：用户已启动和使用的应用程序。Citrix Analytics for Security 从 Citrix Virtual Apps™ 检索此数据，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 从 Citrix Virtual Apps 和 Citrix Endpoint Management™ 检索此数据，并每 12 小时将其发送到 SIEM 服务。
  - **用户位置**：上次检测到用户的城市。Citrix Analytics for Security 从 Citrix Virtual Apps and Desktops™ 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）检索此数据。Citrix Analytics for Security 每 12 小时将此信息发送到您的 SIEM 服务。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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™（以前称为 Citrix Virtual Apps and Desktops 服务）检索此数据，并每 12 小时将此信息发送到您的 SIEM 服务。

如果您只能查看但无法配置数据源事件首选项，则表示您没有必要的管理员权限。 要了解更多信息，请参阅 管理安全分析的管理员角色。

在以下示例中，**保存更改**按钮处于禁用状态。风险洞察事件默认启用。



风险洞察事件的架构详细信息

以下部分介绍了 Citrix Analytics for Security 生成的处理数据的架构。

注意

以下架构示例中显示的字段值仅用于表示目的。实际字段值会根据用户配置文件、用户事件和风险指标而异。

下表描述了所有用户配置文件数据、用户风险评分和风险评分更改的架构中通用的字段名称。

字段名称	描述
`entity_id`	与实体关联的身份。在此情况下，实体是用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`entity_type`	处于风险中的实体。在此情况下，实体是用户。
`event_type`	发送到 SIEM 服务的数据类型。例如：用户位置、用户数据使用情况或用户设备访问信息。
`tenant_id`	客户的唯一身份。
`timestamp`	最近用户活动的日期和时间。
`version`	已处理数据的架构版本。当前架构版本为 2。

用户配置文件数据架构

用户位置架构

```
{

  "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

  }
```

用户位置的字段描述

字段名称	描述
`event_type`	发送到 SIEM 服务的数据类型。在此情况下，事件类型是用户位置。
`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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

用户客户端 IP 架构

```
{
  "client_ip": "149.147.136.10",
  "cnt": 3,
  "entity_id": "r2_up_user_1",
  "entity_type": "user",
  "event_type": "userProfileClientIps",
  "tenant_id": "xaxddaily1",
  "timestamp": "2023-09-18T10:45:00Z",
  "version": 2
}
```

客户端 IP 的字段描述

字段名称	描述
`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。在此情况下，实体是用户。
`entity_type`	存在风险的实体。在此情况下，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：用户位置、用户数据使用情况或用户设备访问信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`tenant_id`	客户的唯一身份。
`timestamp`	最近用户活动的日期和时间..
`version`	已处理数据的架构版本。当前架构版本为 2。

用户数据使用情况架构


```
{

  "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

  }
```


用户数据使用情况的字段描述

字段名称	描述
`data_usage_bytes`	用户使用的数据量（以字节为单位）。它是用户下载和上传总量的聚合。
`deleted_file_cnt`	用户删除的文件数量。
`downloaded_bytes`	用户下载的数据量。
`downloaded_file_count`	用户下载的文件数量。
`event_type`	发送到 SIEM 服务的数据类型。在这种情况下，事件类型是用户的用法配置文件。
`shared_file_count`	用户共享的文件数量。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`uploaded_bytes`	用户上传的数据量。
`uploaded_file_cnt`	用户上传的文件数量。

用户设备架构


```
{

  "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

  }
```


用户设备的字段描述。

字段名称	描述
`cnt`	设备在过去 12 小时内被访问的次数。
`device`	设备的名称。
`event_type`	发送到 SIEM 服务的数据类型。在此情况下，事件类型是用户的设备访问信息。

用户应用程序架构


```
{

  "tenant_id": "demo_tenant", "entity_id": "demo", "entity_type": "user",
"timestamp": "2021-02-10T21:00:00Z", "event_type": "userProfileApp",
"version": 2, "session_domain":
"99e38d488136f62f828d4823edd120b4f32d724396a7410e6dd1b0",
"user_samaccountname": "testnameeikragz779", "app": "Chromeeikragz779",
"cnt": 189
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  }
```

用户应用程序的字段描述。

字段名称	描述
`event_type`	发送到 SIEM 服务的数据类型。在此情况下，事件类型是用户的设备访问信息。
`session_domain`	用户已登录的会话 ID。
`user_samaccountname`	适用于 Windows 早期版本（如 Windows NT 4.0、Windows 95、Windows 98 和 LAN Manager）的客户端和服务器的登录名称。此名称用于登录 Citrix StoreFront 以及登录远程 Windows 计算机。
`app`	用户访问的应用程序名称。
`cnt`	过去 12 小时内应用程序的访问次数。

用户风险评分架构

```
{

  "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

  }
```

用户风险评分的字段描述。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`cur_riskscore`	分配给用户的当前风险评分。风险评分根据与用户活动相关的威胁严重性在 0 到 100 之间变化。
`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`	用户风险评分上次更新的时间。
`timestamp`	用户风险评分事件被收集并发送到您的 SIEM 服务的时间。此事件每 12 小时发送到您的 SIEM 服务一次。

风险评分变更架构

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

  }
```


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":
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"2021-02-11T03:45:00Z", "version": 2

  }
```

风险评分变更的字段描述。

字段名称	描述
`alert_message`	风险评分变更显示的消息。
`alert_type`	指示警报是针对风险评分增加还是风险评分百分比显著下降。当用户的风险评分变化等于或大于三，并且此变化以任何速率增加或下降超过 10% 时，数据将发送到 SIEM 服务。
`alert_value`	为风险评分变更分配的数值。风险评分变更是一个用户当前风险评分与之前风险评分之间的差值。警报值范围为 -100 到 100。
`cur_riskscore`	分配给用户的当前风险评分。风险评分根据与用户活动相关的威胁严重性，范围从 0 到 100。
`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`	检测到用户风险评分最新变化的日期和时间。

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，架构中的字段及其值会相应地变化。

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	描述
`data source`	将数据发送到 Citrix Analytics for Security 的产品列表。例如：Citrix Secure Private Access™、Citrix Gateway 和 Citrix Apps and Desktops 等。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`data_source_id`	与数据源关联的 ID。ID 为 1 的是 Citrix Gateway，ID 为 2 的是 Citrix Endpoint Management，ID 为 3 的是 Citrix Apps and Desktops，ID 为 4 的是 Citrix Secure Private Access。
`entity_type`	处于风险中的实体。它可以是用户。
`entity_id`	与处于风险中的实体关联的 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`	指示风险指标的类别。风险指标分为以下风险类别之一：受感染的端点、受感染的用户、数据泄露或内部威胁。
`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 = 受感染的端点
`indicator_name`	风险指标的名称。对于自定义风险指标，此名称在创建指标时定义。
`indicator_type`	指示风险指标是默认（内置）还是自定义。
`indicator_uuid`	与风险指标实例关联的唯一 ID。
`indicator_vector_name`	指示与风险指标关联的风险向量。风险向量包括基于设备的风险指标、基于位置的风险指标、基于登录失败的风险指标、基于 IP 的风险指标、基于数据的风险指标、基于文件的风险指标以及其他风险指标。
`indicator_vector_id`	与风险向量关联的 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
	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。
`risk_probability`	指示与用户事件关联的风险几率。该值介于 0 到 1.0 之间。对于自定义风险指标，risk_probability 始终为 1.0，因为它是一个基于策略的指标。
`severity`	指示风险的严重性。可以是低、中或高。
`tenant_id`	客户的唯一身份。
`timestamp`	风险指标触发的日期和时间。
`ui_link`	Citrix Analytics 用户界面上用户时间线视图的链接。
`observation_start_time`	Citrix Analytics 开始监控用户活动到时间戳的时间。如果在此时间段内检测到任何异常行为，则会触发风险指示器。

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	描述
`data_source_id`	与数据源关联的唯一标识符。其中，标识符 1 代表 Citrix Gateway；标识符 2 代表 Citrix Endpoint Management；标识符 3 代表 Citrix Apps and Desktops；标识符 4 代表 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 = 内部威胁，ID 3 = 受感染用户，ID 4 = 受感染端点
`entity_id`	与处于风险中的实体关联的 ID。
`entity_type`	处于风险中的实体。可以是用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`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`	指示与风险指标关联的风险向量。风险向量包括基于设备的风险指标、基于位置的风险指标、基于登录失败的风险指标、基于 IP 的风险指标、基于数据的风险指标、基于文件的风险指标以及其他风险指标。
`indicator_vector_id`	与风险向量关联的 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。
`tenant_id`	客户的唯一身份。
`timestamp`	风险指标触发的日期和时间。
`version`	已处理数据的架构版本。当前架构版本为 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"`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Private Access 风险指标架构

尝试访问黑名单 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",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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"
  }
}
```

指标事件详细信息架构

```
{
  "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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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"
}
```

下表描述了尝试访问黑名单 URL 的摘要架构和事件详细信息架构特有的字段名称。

字段名称	描述
`observation_start_time`	Citrix Analytics 开始监控用户活动到时间戳的时间。如果在此期间检测到任何异常行为，将触发风险指标。
`executed_action`	对列入黑名单的 URL 执行的操作。操作包括允许和阻止。
`reason_for_action`	对该 URL 执行此操作的原因。

过量数据下载风险指标架构

指标摘要架构

```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 403,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"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"
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  }
}
```

指标事件详细信息架构

```
{
  "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": "2018-03-16T10:30:00Z",
  "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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

下表描述了过量数据下载的摘要架构和事件详细信息架构特有的字段名称。

字段名称	描述
`observation_start_time`	Citrix Analytics 开始监控用户活动到时间戳的时间。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`	下载数据的域的名称。
`downloaded_bytes`	下载的数据量（以字节为单位）。

异常上传量风险指示器架构

指示器摘要架构

```
{
  "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,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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"
  }
}
```

指示器事件详细信息架构

```
{
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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
}
```


下表描述了异常上传量的摘要架构和事件详细信息架构特有的字段名称。

字段名称	描述
`observation_start_time`	Citrix Analytics 开始监控用户活动到时间戳的时间。如果在此期间检测到任何异常行为，则会触发风险指示器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`data_volume_in_bytes`	上传的数据量（以字节为单位）。
`relevant_event_type`	指示用户事件的类型。
`domain_name`	上传数据的域的名称。
`uploaded_bytes`	上传的数据量（以字节为单位）。

Citrix Endpoint Management 风险指标架构

检测到越狱或已 Root 设备指标架构

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 },
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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
}
```


指标事件详细信息架构


```
{
  "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",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "id": 7 },
  "indicator_uuid": "9aaaa9e1-39ad-4daf-ae8b-2fa2caa60732",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T17:50:35Z",
  "version": 2
}
```


检测到带有黑名单应用程序的设备

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 },
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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
}
```


指标事件详细信息架构


```
{
  "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",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "id": 7 },
  "indicator_uuid": "743cd13a-2596-4323-8da9-1ac279232894",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T17:50:39Z",
  "version": 2
}
```


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 },
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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
}
```


指标事件详细信息架构


```
{
  "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",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "id": 7 },
  "indicator_uuid": "dd280122-04f2-42b4-b9fc-92a715c907a0",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T18:41:30Z",
  "version": 2
}
```

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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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"
  }
}
```

指标事件详细信息架构

```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 100,
  "indicator_uuid": "3c17454c-86f5-588a-a4ac-0342693d8a70",
  "indicator_category_id": 3,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"indicator_vector": {
  "name": "Other Risk Indicators",
  "id": 7 },
"data_source_id": 1,
"timestamp": "2017-12-21T07:12:00Z",
"event_type": "indicatorEventDetails",
"entity_type": "user",
"entity_id": "demo_user",
"version": 2,
"event_description": "Post auth failed, no quarantine",
"gateway_domain_name": "10.102.xx.xx",
"gateway_ip": "56.xx.xxx.xx",
"policy_name": "postauth_act_1",
"client_ip": "210.91.xx.xxx",
"country": "United States",
"city": "San Jose",
"region": "California",
"cs_vserver_name": "demo_vserver",
"device_os": "Windows OS",
"security_expression": "CLIENT.OS(Win12) EXISTS",
"vpn_vserver_name": "demo_vpn_vserver",
"vserver_fqdn": "10.xxx.xx.xx"
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

此表描述了 EPA 扫描失败风险指标的摘要架构和事件详细信息架构特有的字段名称。

字段名称	描述
`event_description`	描述了 EPA 扫描失败的原因，例如身份验证后失败和无隔离组。
`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`	在 Citrix Gateway 上配置的 EPA 扫描策略名称。
`country`	检测到用户活动的国家/地区。
`city`	检测到用户活动的城市。
`region`	检测到用户活动的区域。
`cs_vserver_name`	内容交换虚拟服务器的名称。
`device_os`	用户设备的操作系统。
`security_expression`	在 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。

过多的身份验证失败风险指标架构

指标摘要架构

```
{

  "tenant_id": "demo_tenant",

  "indicator_id": 101,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"indicator_uuid": "4bc0f759-93e0-5eea-9967-ed69de9dd09a",
"indicator_category_id": 3,
"indicator_vector": {
  "name": "Logon-Failure-Based Risk Indicators",
  "id": 3 },
"data_source_id": 1,
"timestamp": "2017-12-21T07:14:59Z",
"event_type": "indicatorSummary",
"entity_type": "user",
"entity_id": "demo_user",
"version": 2,
"risk_probability": 1,
"indicator_category": "Compromised users",
"indicator_name": "Excessive authentication failures",
"severity": "medium",
"data_source": "Citrix Gateway",
"ui_link": "https://analytics.cloud.com/user/”,
"indicator_type": "builtin",
"occurrence_details": {
  "observation_start_time": "2017-12-21T07:00:00Z",
  "relevant_event_type": "Logon Failure"
}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

指标事件详细信息架构

```
{
  "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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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
}
```

下表描述了特定于“过多的身份验证失败”的摘要架构和事件详细信息架构的字段名称。

字段名称	描述
`relevant_event_type`	指示事件类型，例如登录失败。
`event_description`	描述过多的身份验证失败事件的原因，例如密码不正确。
`authentication_stage`	指示身份验证阶段是主要、次要还是三级。
`authentication_type`	指示身份验证类型，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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`cs_vserver_name`	内容交换虚拟服务器的名称。
`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`	检测到用户活动的国家/地区。
`city`	检测到用户活动的城市。
`region`	检测到用户活动的区域。

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",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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

  }

}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标事件详细信息架构

```
{
  "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”,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "country": "Norway",
  "region": "Oslo",
  "city": "Oslo",
  "latitude": 59.9139,
  "longitude": 10.7522,
  "device_os": "Linux OS",
  "device_browser": "Chrome 62.0.3202.94"
}
```

下表描述了不可能旅行的摘要架构和事件详细信息架构特有的字段名称。

字段名称	描述
`distance`	不可能行程相关事件之间的距离（公里）。
`historical_logon_locations`	用户访问的位置以及在观察期内每个位置被访问的次数。
`historical_observation_period_in_days`	每个位置都会被监控 30 天。
`relevant_event_type`	指示事件类型，例如登录。
`observation_start_time`	Citrix Analytics 开始监控用户活动到时间戳的时间。如果在此时间段内检测到任何异常行为，则会触发风险指示器。
`country`	用户登录的国家/地区。
`city`	用户登录的城市。
`region`	指示用户登录的区域。
`latitude`	指示用户登录位置的纬度。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`longitude`	指示用户登录位置的经度。
`device_browser`	用户使用的网络浏览器。
`device_os`	用户设备的操作系统。
`ip_organization`	客户端IP地址的注册组织
`ip_routing_type`	客户端IP路由类型

可疑IP登录风险指示器架构

指示器摘要架构

```
{
  "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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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"
  }
}
```

指示器事件详细信息架构

```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 102,
  "indicator_uuid": "4ba77b6c-bac0-5ad0-9b4a-c459a3e2ec33",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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"
}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

下表描述了可疑 IP 登录的摘要架构和事件详细信息架构特有的字段名称。

字段名称	描述
`suspicious_reasons`	IP 地址被识别为可疑的原因。
`webroot_reputation`	由威胁情报提供商 Webroot 提供的 IP 信誉指数。
`webroot_threat_categories`	由威胁情报提供商 Webroot 为可疑 IP 识别的威胁类别。
`device_os`	用户设备的操作系统。
`device_browser`	使用的网络浏览器。
`country`	检测到用户活动的国家/地区。
`city`	检测到用户活动的城市。
`region`	检测到用户活动的区域。

异常身份验证失败风险指示器架构

指示器摘要架构

```
{
  "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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "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"
  }
}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

指示器事件详细信息架构

```
{
  "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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "region": "California",
  "device_os": "Windows OS ",
  "device_browser": "Chrome",
  "is_risky": "false"
}
```

下表描述了异常身份验证失败的摘要架构和事件详细信息架构特有的字段名称。

字段名称	描述
`relevant_event_type`	指示事件类型，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、次要还是第三级。
`authentication_type`	指示身份验证类型，例如 LDAP、本地或 OAuth。
`is_risky`	对于成功登录，is_risky 值为 false。对于不成功登录，is_risky 值为 true。
`device_os`	用户设备的操作系统。
`device_browser`	用户使用的网络浏览器。
`country`	检测到用户活动的国家/地区。
`city`	检测到用户活动的城市。
`region`	检测到用户活动的区域。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

可疑登录风险指示器

指示器摘要架构


```
{
  "tenant_id": "demo_tenant",
  "indicator_id": "110",
  "indicator_uuid": "67fd935-a6a3-5397-b596-636aa1588c",
  "indicator_category_id": 3,
  "indicator_vector": [
    {
      "name": "Location-Based Risk Indicators",
      "id": 2
    },
    {
      "name": "IP-Based Risk Indicators",
      "id": 4
    },
    {
      "name": "Other Risk Indicators",
      "id": 7
    }
  ],
  "data_source_id": 1,
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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}]",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "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
  }
}
```

指示器事件详细信息架构

```
{
  "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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "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,
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "device_browser": "Chrome",
  "device_os": "Windows OS",
  "device_id": "NA",
  "client_ip": "99.xxx.xx.xx"
}
```

下表描述了可疑登录的摘要架构和事件详细信息架构特有的字段名称。

字段名称	描述
`historical_logon_locations`	用户访问的位置以及在观察期内每个位置被访问的次数。
`historical_observation_period_in_days`	每个位置都会被监控 30 天。
`relevant_event_type`	指示事件类型，例如登录。
`observation_start_time`	Citrix Analytics 开始监控用户活动到时间戳的时间。如果在此时间段内检测到任何异常行为，则会触发风险指示器。
`occurrence_event_type`	指示用户事件类型，例如账户登录。
`country`	用户登录的国家/地区。
`city`	用户登录的城市。
`region`	指示用户登录的区域。
`latitude`	指示用户登录位置的纬度。
`longitude`	指示用户登录位置的经度。
`device_browser`	用户使用的网络浏览器。
`device_os`	用户设备的操作系统。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`device_id`	用户使用的设备名称。
`user_location_risk`	指示用户登录位置的可疑级别。低可疑级别：0–69，中可疑级别：70–89，高可疑级别：90–100
`user_device_risk`	指示用户登录设备的怀疑级别。低怀疑级别：0–69，中怀疑级别：70–89，高怀疑级别：90–100
`user_network_risk`	指示用户登录的网络或子网的可疑级别。低可疑级别：0–69，中可疑级别：70–89，高可疑级别：90–100
`suspicious_network_risk`	根据 Webroot IP 威胁情报源指示 IP 威胁级别。低威胁级别：0–69，中威胁级别：70–89，高威胁级别：90–100
`webroot_threat_categories`	根据 Webroot IP 威胁情报源指示从 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、扫描器、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": {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "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\":
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
\"United States\",
\"latitude\":37.0902,\"longitude\":-95.7129,\"count\":2}]",

    "historical_observation_period_in_days": 30

  }

}
```

指标事件详细信息架构

```
{

  "tenant_id": "demo_tenant",

  "indicator_id": "313",

  "indicator_uuid": "c78d1dd4-5e70-5642-ba6f-1cdf31bc6ab2",

  "pair_id": 2,

  "indicator_category_id": 3,

  "indicator_vector": {

    "name": "Location-Based Risk Indicators",

    "id": 2

  },

  "data_source_id": 3,

  "timestamp": "2020-06-06T05:05:00Z",

  "event_type": "indicatorEventDetails",

  "entity_type": "user",

  "entity_id": "demo_user",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "version": 2,
  "occurrence_event_type": "Account.Logon",
  "client_ip": "95.xxx.xx.xx",
  “ip_organization”: “global telecom ltd”,
  “ip_routing_type”: “mobile gateway”,
  "country": "Norway",
  "region": "Oslo",
  "city": "Oslo",
  "latitude": 59.9139,
  "longitude": 10.7522,
  "device_id": "device1",
  "receiver_type": "XA.Receiver.Linux",
  "os": "Linux OS",
  "browser": "Chrome 62.0.3202.94"
}
```

下表描述了与不可能的行程相关的摘要架构和事件详细信息架构特有的字段名称。

字段名称	描述
`distance`	与不可能的行程相关的事件之间的距离（公里）。
`historical_logon_locations`	用户访问的位置以及在观察期间每个位置被访问的次数。
`historical_observation_period_in_days`	每个位置都会被监控 30 天。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`relevant_event_type`	指示事件类型，例如登录。
`observation_start_time`	Citrix Analytics 开始监控用户活动到时间戳的时间。如果在此期间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`	指示用户登录的区域。
`latitude`	指示用户登录位置的纬度。
`longitude`	指示用户登录位置的经度。
`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`	客户端 IP 地址的注册组织
`ip_routing_type`	客户端 IP 路由类型

潜在数据泄露风险指标

指标摘要架构

```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 303,
  "indicator_uuid": "fb649ff7-5b09-5f48-8a04-12836b9eed85",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"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
}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

指标事件详细信息架构

```
{
  "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": "2018-04-02T10:57:36Z",
  "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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "receiver_type": "XA.Receiver.Windows",
  "app_url": "https://www.citrix.com",
  "client_ip": "10.xxx.xx.xxx",
  "entity_time_zone": "Pacific Standard Time"
}
```

下表描述了潜在数据泄露的摘要架构和事件详细信息架构特有的字段。

字段名称	描述
`observation_start_time`	Citrix Analytics 开始监控用户活动到时间戳的时间。如果在此期间检测到任何异常行为，则会触发风险指标。
`relevant_event_type`	指示用户活动，例如下载、打印或复制数据。
`exfil_data_volume_in_bytes`	数据渗漏量。
`occurrence_event_type`	指示数据渗漏的发生方式，例如 SaaS 应用程序中的剪贴板操作。
`file_size_in_bytes`	文件大小。
`file_type`	文件类型。
`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。
`app_url`	用户访问的应用程序的 URL。
`entity_time_zone`	用户的时区。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
    },
    {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "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",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "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

  }

}
```


指标事件详细信息架构


```
{

  "tenant_id": "tenant_1",

  "indicator_id": "312",

  "indicator_uuid": "1b97c3be-abcd-efgh-ijkl-1234567890",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"indicator_category_id": 3,
"indicator_vector":
[
  {
    "name": "Other Risk Indicators",
    "id": 7
  },
  {
    "name":"Location-Based Risk Indicators",
    "id":2
  },
  {
    "name":"IP-Based Risk Indicators",
    "id":4
  },
  {
    "name": "Device-Based Risk Indicators",
    "id": 1
  },
],
"data_source_id": 3,
"timestamp": "2020-06-06 12:02:30",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "user2",
  "version": 2,
  "occurrence_event_type": "Account.Logon",
  "city": "Some_city",
  "country": "United States",
  "region": "Some_Region",
  "latitude": 37.751,
  "longitude": -97.822,
  "browser": "Firefox 1.3",
  "os": "Windows OS",
  "device_id": "device2",
  "receiver_type": "XA.Receiver.Chrome",
  "client_ip": "99.xxx.xx.xx"
}
```

下表描述了可疑登录的摘要架构和事件详细信息架构特有的字段名称。

字段名称	描述
`historical_logon_locations`	用户访问的位置以及在观察期内每个位置被访问的次数。
`historical_observation_period_in_days`	每个位置都会被监控 30 天。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`relevant_event_type`	指示事件类型，例如登录。
`observation_start_time`	Citrix Analytics 开始监控用户活动到时间戳之间的时间。如果在此时间段内检测到任何异常行为，则会触发风险指示器。
`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`	指示用户登录的区域。
`latitude`	指示用户登录位置的纬度。
`longitude`	指示用户登录位置的经度。
`browser`	用户使用的 Web 浏览器。
`os`	用户的设备的操作系统。
`device_id`	用户使用的设备的名称。
`receiver_type`	安装在用户设备上的 Citrix Workspace 应用程序或 Citrix Receiver 的类型。
`user_location_risk`	指示用户登录位置的可疑级别。低可疑级别：0–69，中可疑级别：70–89，高可疑级别：90–100
`user_device_risk`	指示用户登录设备的的可疑级别。低可疑级别：0–69，中可疑级别：70–89，高可疑级别：90–100
`user_network_risk`	指示用户登录的网络或子网的可疑级别。低可疑级别：0–69，中可疑级别：70–89，高可疑级别：90–100

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`suspicious_network_risk`	指示基于 Webroot IP 威胁情报源的 IP 威胁级别。低威胁级别：0–69，中威胁级别：70–89，高威胁级别：90–100
`webroot_threat_categories`	根据 Webroot IP 威胁情报源，指示从 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、扫描器、拒绝服务、信誉、网络钓鱼、代理、未指定、移动威胁和 Tor 代理。

微软活动目录指标

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": {},
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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
}
```


指标事件详细信息架构


```
{
  "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
}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

自定义风险指标架构

以下部分描述了自定义风险指标的架构。

注意

目前，Citrix Analytics 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	描述
`data source`	向 Citrix Analytics for Security 发送数据的产品。例如，这些产品包括：Citrix Secure Private Access、Citrix Gateway 和 Citrix Apps and Desktops。
`data_source_id`	与数据源关联的 ID。ID 1 = Citrix 网关，ID 2 = Citrix 端点管理，ID 3 = Citrix 应用和桌面，ID 4 = Citrix 安全私有访问
`entity_id`	与风险实体关联的 ID。
`entity_type`	风险实体。在此情况下，实体是用户。
`event_type`	发送到 SIEM 服务的数据类型。在此情况下，事件类型是风险指标的摘要。
`indicator_category`	指示风险指标的类别。风险指标分为以下风险类别之一：受感染的端点、受感染的用户、数据泄露或内部威胁。
`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 = 受感染的端点。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`indicator_name`	风险指标的名称。对于自定义风险指标，此名称在创建指标时定义。
`indicator_type`	指示风险指标是默认（内置）还是自定义。
`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`	指示与用户事件相关的风险几率。该值介于 0 到 1.0 之间。对于自定义风险指标，risk_probability 始终为 1.0，因为它是一个基于策略的指标。
`severity`	指示风险的严重性。它可以是低、中或高。
`tenant_id`	客户的唯一身份。
`timestamp`	风险指标触发的日期和时间。
`ui_link`	Citrix Analytics 用户界面上用户时间线视图的链接。
`version`	已处理数据的架构版本。当前架构版本为 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	描述
`data_source_id`	与数据源关联的 ID。ID 1 = Citrix 网关，ID 2 = Citrix 端点管理，ID 3 = Citrix 应用和桌面，ID 4 = Citrix 安全私有访问
`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 = 受感染用户，ID 4 = 受感染端点
`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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`tenant_id`	客户的唯一身份。
`entity_id`	与风险实体关联的 ID。
`entity_type`	处于风险中的实体。在此情况下，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`	风险指标触发的日期和时间。
`version`	已处理数据的架构版本。当前架构版本为 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`	用户的设备的 IP 地址。
`session_user_name`	与 Citrix Apps and Desktops 会话关联的用户名。
`city`	检测到用户活动的城市名称。
`country`	检测到用户活动的国家/地区名称。
`device_id`	用户使用的设备名称。
`os_name`	安装在用户设备上的操作系统。有关详细信息，请参阅 Apps and Desktops 的自助服务搜索。
`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 应用程序和桌面自助搜索。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`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 应用程序和桌面自助搜索。

适用于 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",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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

}
```

适用于会话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": "Session.Logon",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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",
}
```


下表描述了适用于会话登录事件的事件详细信息架构特有的字段名称。

字段名称	描述
`app_name`	启动的应用程序或桌面的名称。
`launch_type`	指示是应用程序还是桌面。
`domain`	发送请求的服务器的域名。
`server_name`	服务器名称。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`session_guid`	活动会话的 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",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "os_name": "Windows NT 6.1",

  "os_version": "7601",

  "os_extra_info": "Service Pack 1",

  "app_name": "notepad",

  "launch_type": "Application",

}
```

下表描述了会话启动事件的事件详细信息架构特有的字段名称。

字段名称	描述
`app_name`	启动的应用程序或桌面名称。
`launch_type`	指示是应用程序还是桌面。

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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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",
}
```

下表描述了帐户登录事件的事件详细信息架构特有的字段名称。

字段名称	描述
`app_name`	启动的应用程序或桌面名称。

会话结束事件的指标事件详细信息架构

```
{
  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"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",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "server_name": "test_server",

  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",

}
```

下表描述了会话结束事件的事件详细信息架构特有的字段名称。

字段名称	描述
`app_name`	启动的应用程序或桌面名称。
`launch_type`	指示是应用程序还是桌面。
`domain`	发送请求的服务器的域名。
`server_name`	服务器名称。
`session_guid`	活动会话的 GUID。

应用程序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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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"
}
```


下表描述了应用程序启动事件的事件详细信息架构特有的字段名称。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`app_name`	启动的应用程序或桌面名称。
`launch_type`	指示是应用程序还是桌面。
`domain`	发送请求的服务器的域名。
`server_name`	服务器名称。
`session_guid`	活动会话的 GUID。
`module_file_path`	正在使用的应用程序的路径。

应用程序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",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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"
}
```


下表描述了应用程序结束事件的事件详细信息架构特有的字段名称。

字段名称	描述
`app_name`	启动的应用程序或桌面的名称。
`launch_type`	指示是应用程序还是桌面。
`domain`	发送请求的服务器的域名。
`server_name`	服务器名称。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`session_guid`	活动会话的 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",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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"
}
```


下表描述了文件下载事件的事件详细信息架构特有的字段名称。

字段名称	描述
`file_download_file_name`	下载文件的名称。
`file_download_file_path`	文件下载到的目标路径。
`launch_type`	指示是应用程序还是桌面。
`domain`	发送请求的服务器的域名。
`server_name`	服务器名称。
`session_guid`	活动会话的 GUID。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`device_type`	指示文件下载到的设备类型。

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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "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"
}
```

下表描述了打印事件的事件详细信息架构特有的字段名称。

字段名称	描述
`printer_name`	用于打印作业的打印机名称。
`launch_type`	指示应用程序或桌面。
`domain`	发送请求的服务器的域名。
`server_name`	服务器名称。
`session_guid`	活动会话的 GUID。
`job_details_size_in_bytes`	打印作业的大小，例如文件或文件夹。
`job_details_filename`	打印文件的名称。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

字段名称	描述
`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",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "os_name": "Windows NT 6.1",

  "os_version": "7601",

  "os_extra_info": "Service Pack 1",

  "launch_type": "Desktop",

}
```

下表描述了应用程序 SaaS 启动事件的事件详细信息架构特有的字段名称。

字段名称	描述
`launch_type`	指示应用程序或桌面。

应用程序 SAAS 结束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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   "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",
}
```

下表描述了应用程序 SaaS 结束事件的事件详细信息架构特有的字段名称。

字段名称	描述
`launch_type`	指示应用程序或桌面。

数据源事件

此外，您可以配置数据导出功能，从已启用 Citrix Analytics for Security 的产品数据源导出用户事件。当您在 Citrix 环境中执行任何活动时，会生成数据源事件。导出的事件是自助服务视图中可用的未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进一步用于更深入的威胁分析、创建新仪表板，并与您的安全和 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 会将 Citrix Virtual Apps and Desktops 数据源的用户事件发送到您的 SIEM。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

数据源事件的架构详细信息

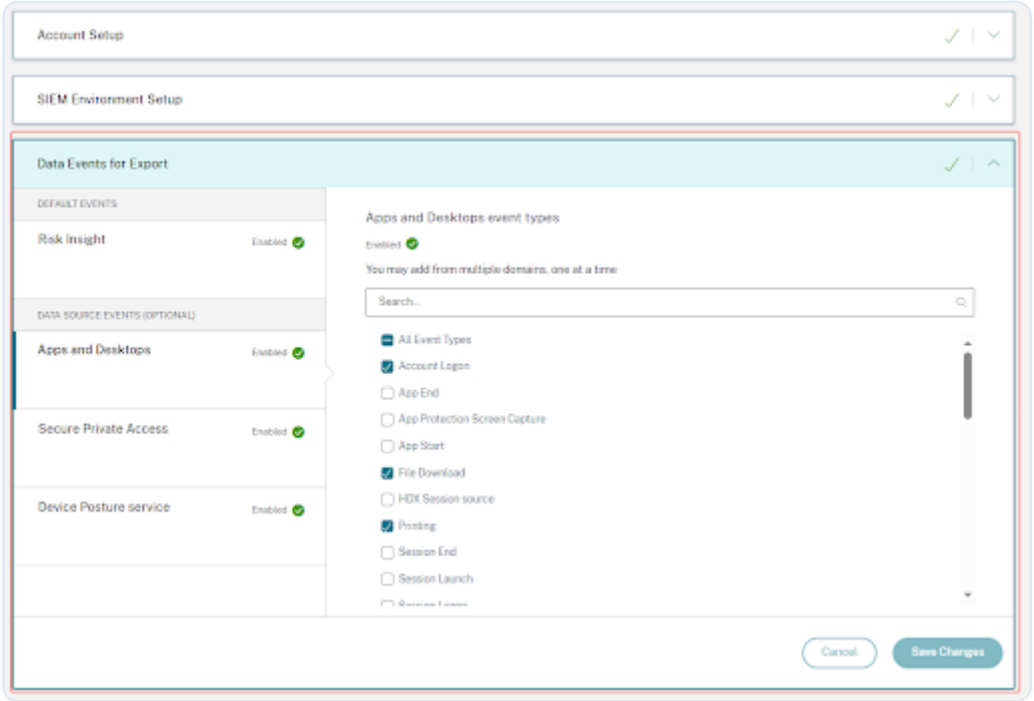
思杰虚拟应用和桌面事件

当用户使用虚拟应用程序或虚拟桌面时，用户事件会实时发送到 Citrix Analytics for Security。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 中查看与 Citrix Virtual Apps and Desktops 相关的以下用户事件：

- 所有事件类型
- 帐户登录
- 应用程序（启动、开始、结束）
- 剪贴板
- 文件（打印、下载）
- HDX™ 会话源
- 打印
- 会话（登录、启动、结束、终止）
- VDA 数据
- VDA 进程创建

有关事件及其属性的详细信息，请参阅Virtual Apps and Desktops 的自助搜索。

您可以查看已启用并流向 SIEM 的事件类型。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。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全私有访问事件

当用户通过 Citrix Secure Private Access（例如 Citrix Workspace App、Citrix Secure Access 客户端或 Citrix Enterprise Browser）访问应用程序时，用户事件会实时接收到 Citrix Analytics for Security 中。您可以在 SIEM 中查看与 Secure Private Access 相关的以下用户事件：

- 所有事件类型
- 账户登录
- 应用程序（连接、启动、结束、错误）
- 文件（打印、下载）
- 策略评估
- 剪贴板
- 会话（连接、启动）
- URL
- 用户登录
- SPA 服务日志

安全私有访问事件(/en-us/citrix-analytics/media/secure-private-access-events.png)

设备姿态服务事件

当 Citrix Endpoint Analysis (EPA) 客户端对尝试访问 Citrix Virtual Apps and Desktops 或 Citrix Secure Private Access 资源的设备执行姿态检查时，会生成用户事件。您可以在 SIEM 中查看与设备姿态服务相关的以下用户事件：

- 所有事件类型
- 设备姿态评估

设备姿态服务事件(/en-us/citrix-analytics/media/device-posture-service-events.png)

您可以查看为您的租户启用的事件类型，并确保它们正在流向 SIEM。您可以配置或删除适用的事件类型，然后点击“**保存更改**”按钮以应用您的设置。

利用 Citrix Analytics SIEM 数据模型进行威胁分析和数据关联

本文解释了发送到客户 SIEM 环境的事件所展示的实体数据关系。为了阐明这一点，我们以一个威胁搜寻场景为例，其中客户端 IP 和操作系统是焦点属性。将讨论以下将所述属性与用户关联的方法：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 使用自定义风险指标洞察
- 使用数据源事件

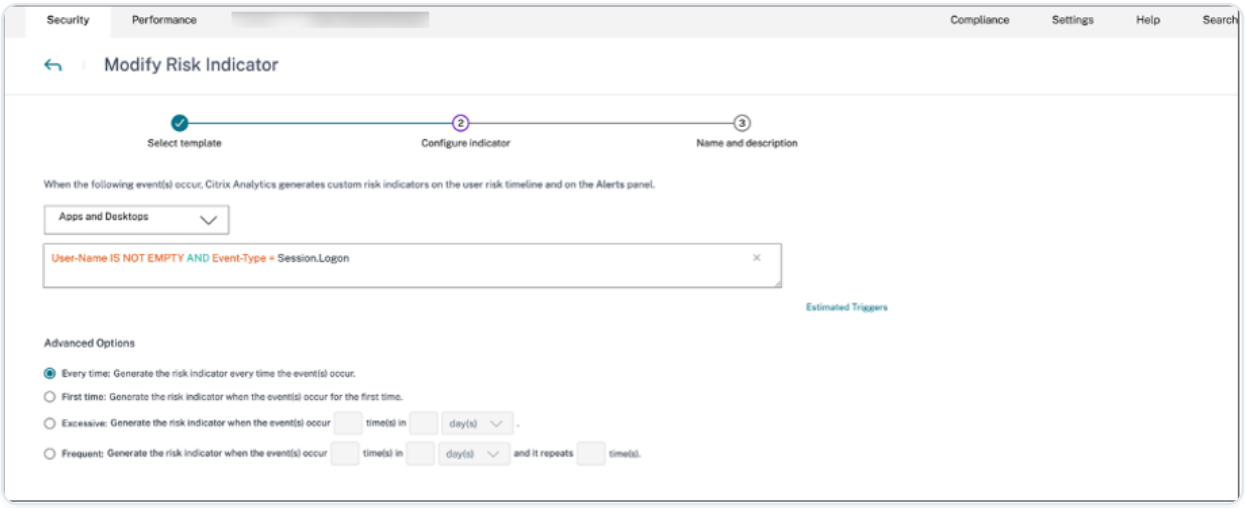
Splunk 是以下示例中选择展示的 SIEM 环境。Citrix Analytics 也可以使用工作簿模板在 Sentinel 上执行类似的数据关联。要进一步探索，请参阅 适用于 Microsoft Sentinel 的 Citrix Analytics 工作簿。

自定义风险指标洞察

如 Citrix Analytics SIEM 数据导出格式 中所述，指标摘要和事件详细信息洞察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，客户端 IP 和操作系统默认导出。因此，如果管理员设置了一个包含或不包含这些字段条件的自定义指标，则所述数据点将流入您的 Splunk 环境。

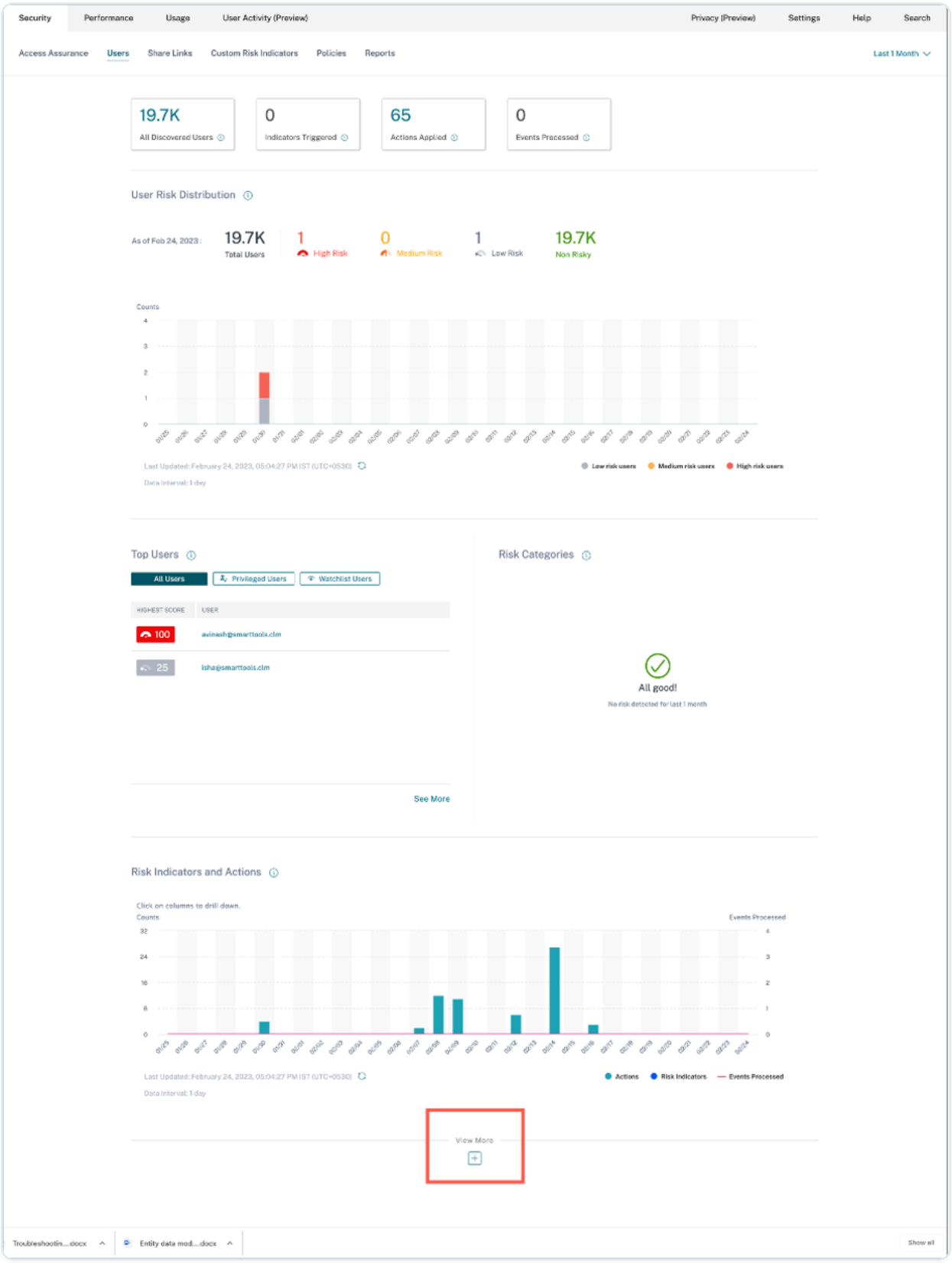
在 Citrix Analytics 中设置自定义风险指标

1. 导航到 **Citrix Analytics for Security™ 仪表板 > 自定义风险指标 > 创建指标**。您可以创建具有任何条件的自定义风险指标，以帮助您监控用户行为。设置自定义指标后，所有触发关联条件的用户都将在您的 Splunk 环境中可见。



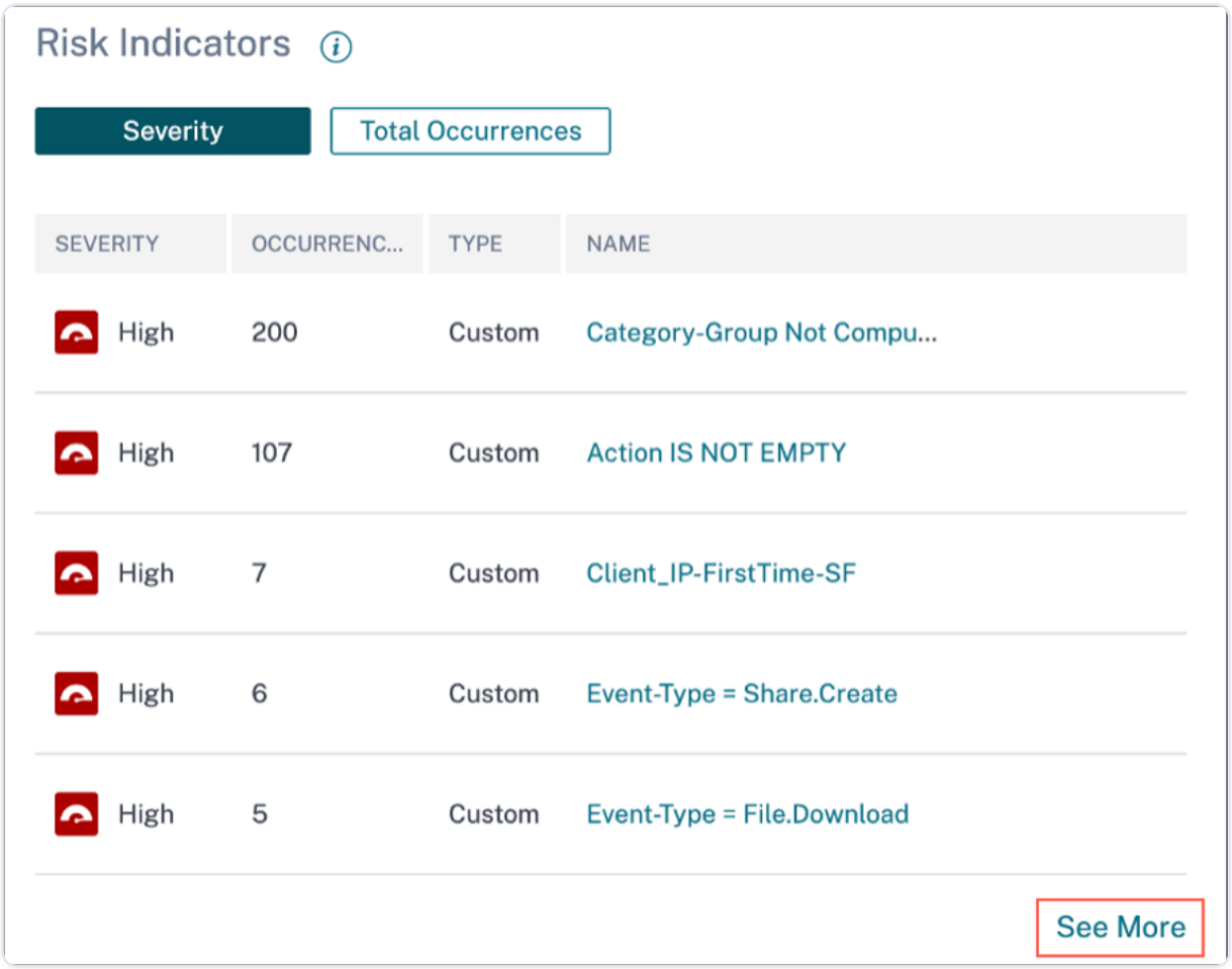
2. 要在 Citrix Analytics for Security 上查看已创建的风险指标事件，请导航到 **安全 > 用户。导航到页面底部并单击加号 (+) 图标**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

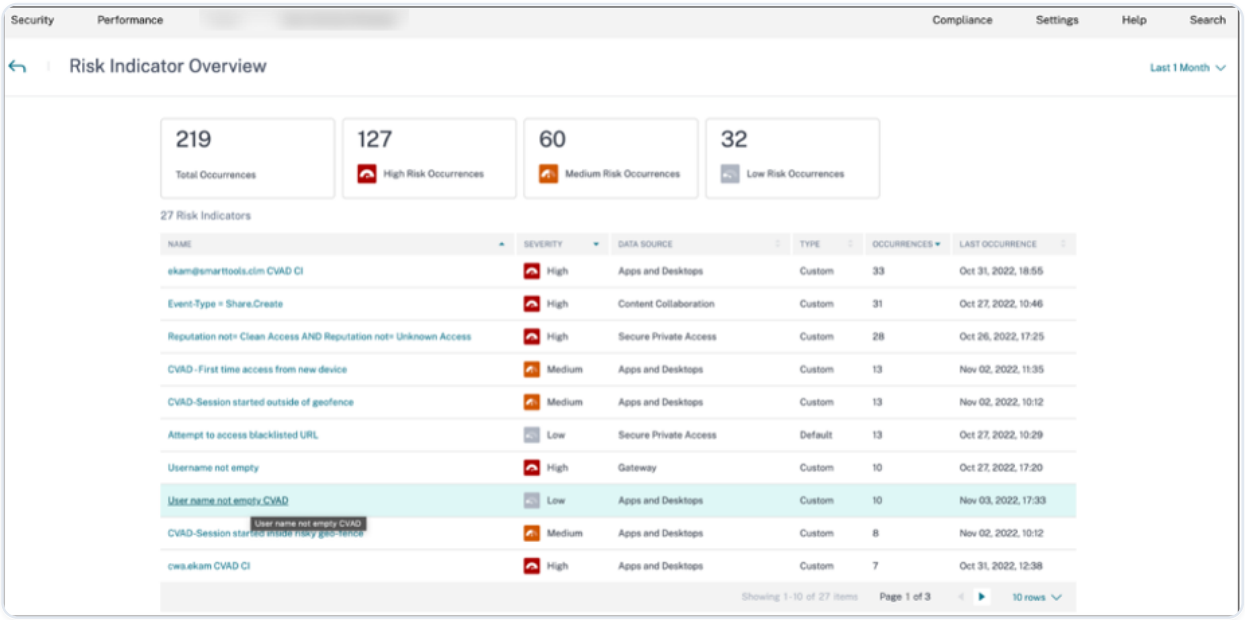


风险指标卡片出现。您可以查看风险指标的详细信息、严重性和发生次数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

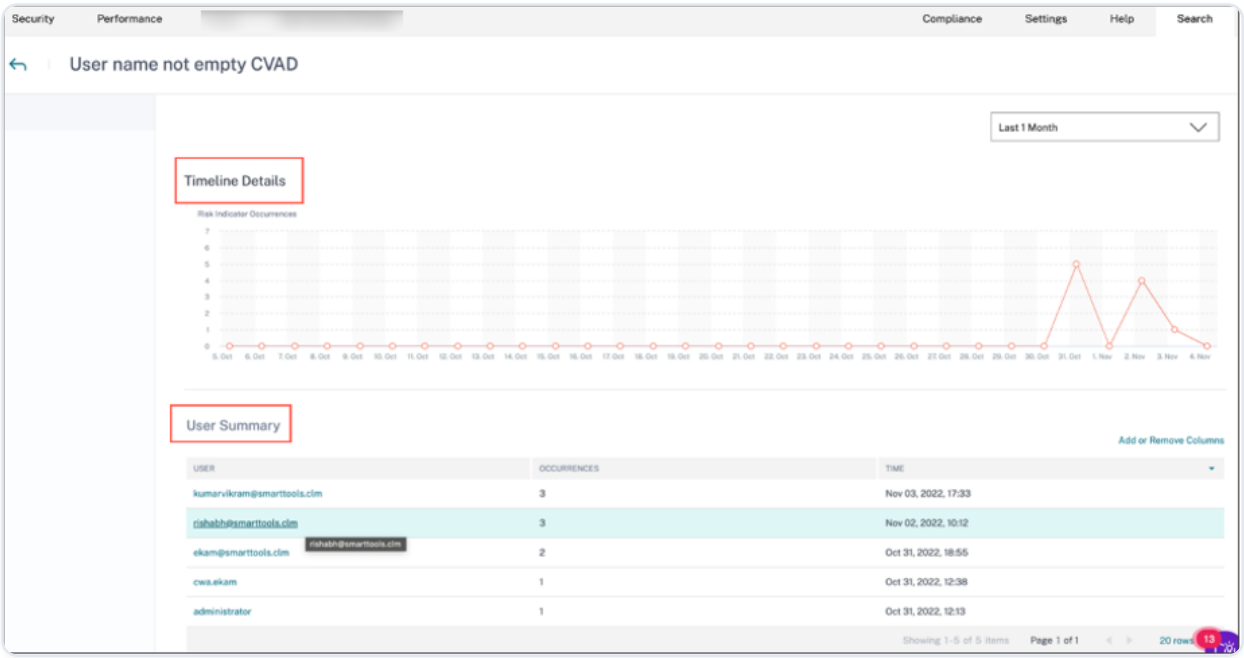


3. 单击 **查看更多**。风险指标 **概述** 页面出现。



在“风险指标概览”页面上，您可以查看触发该指标的用户的详细信息，包括详细的时间线视图和用户摘要。要了解有关时间线的更多信息，请参阅用户风险时间线和配置文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

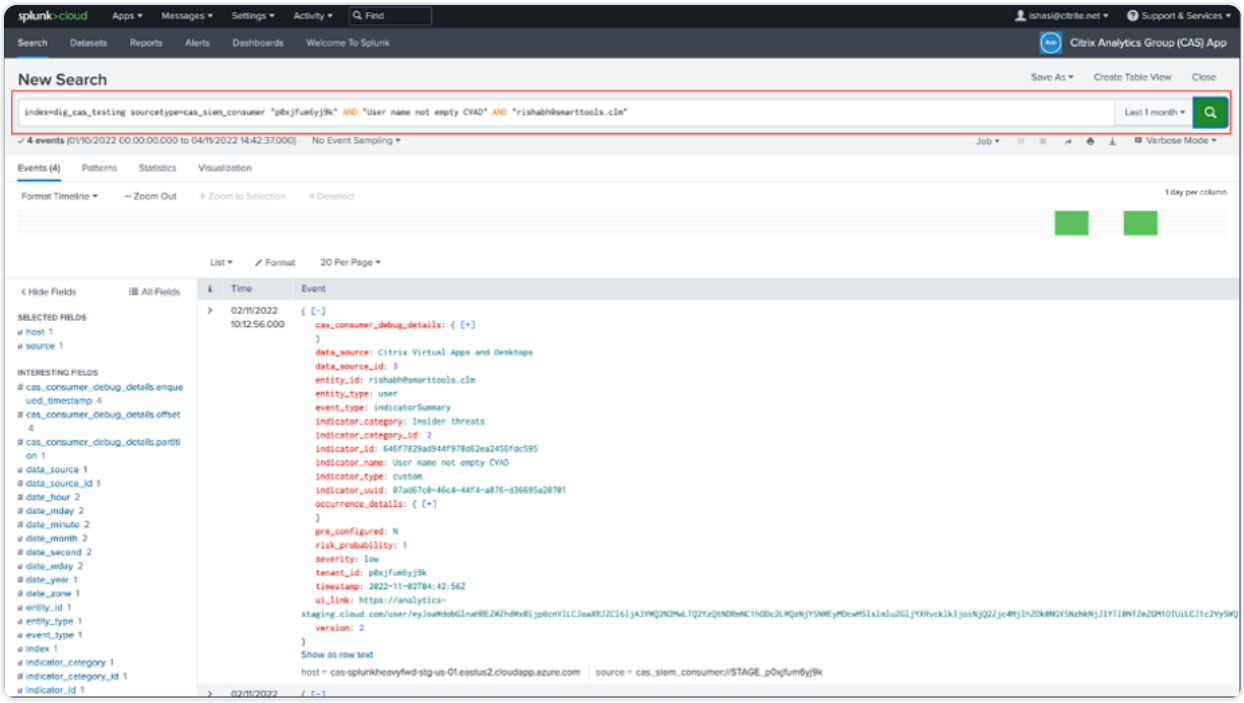


Splunk 上的风险指标事件 - 原始查询

您还可以通过使用 Splunk 基础架构管理员在 Splunk Enterprise 上为 Citrix Analytics for Security Add-on 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：

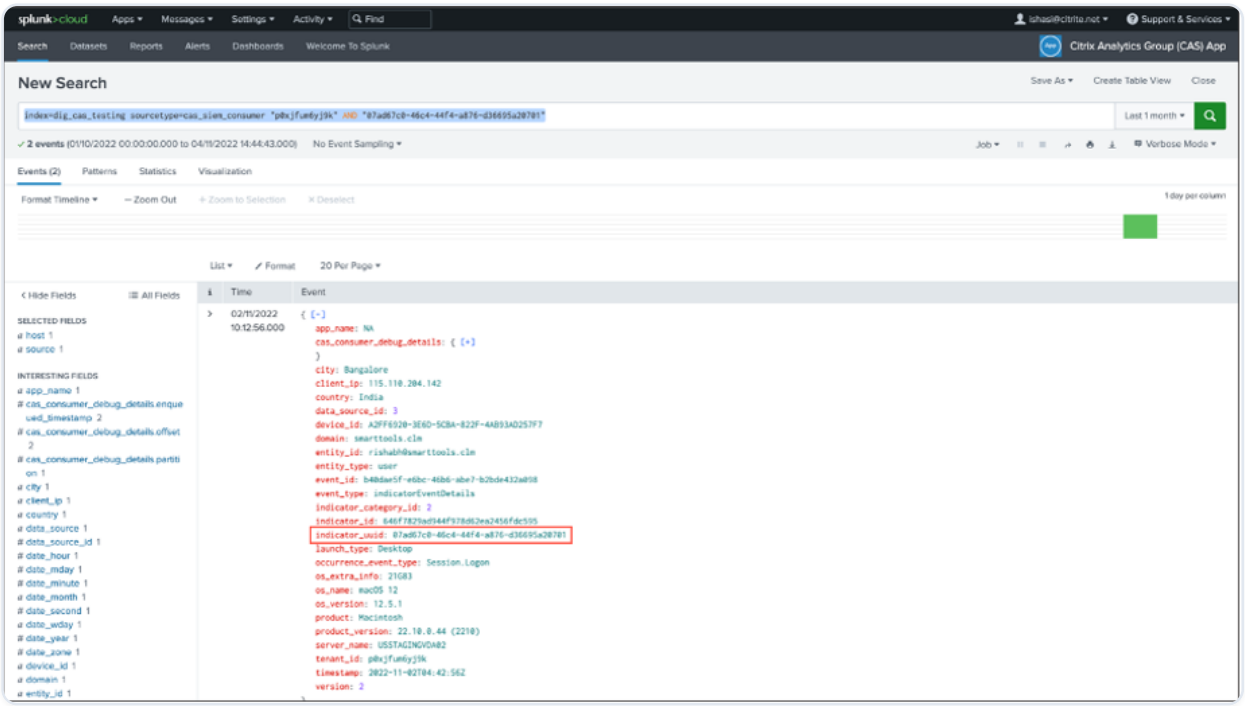
```
index=<index configured by you> sourcetype=<sourcetype configured by you> AND "<tenant_id>" AND "<indicator name configured by you on CAS>" AND "<user you are interested in>"
```



© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 获取 indicator_uuid 并运行以下查询：

```
index=<index configured by you> sourcetype=<sourcetype configured by
you> "<tenant_id>" AND "<indicator_uuid>"
```



事件结果包含**指标事件摘要**和**指标事件详细信息**（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Citrix Analytics SIEM 数据导出格式。

Splunk 上的风险指标事件 - 仪表板应用程序

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 应用程序
- 适用于 Splunk 的 Citrix Analytics 仪表板

1. 点击 **Citrix Analytics – Dashboard** 选项卡，然后从下拉列表中选择 **风险指标详细信息** 选项。

   风险指标详细信息选项(/en-us/citrix-analytics/media/risk-indicator-details-option.png)

2. 从下拉列表中适当筛选内容，然后点击 **提交**。

   风险指标详细信息选项筛选器(/en-us/citrix-analytics/media/risk-indicator-details-option-filter.png)

3. 点击用户实例以获取详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

风险指标用户实例(/en-us/citrix-analytics/media/risk-indicator-user-instance.png)

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、额外信息）：

   客户端 IP 和操作系统信息(/en-us/citrix-analytics/media/client-ip-and-os-information.png)

数据源事件

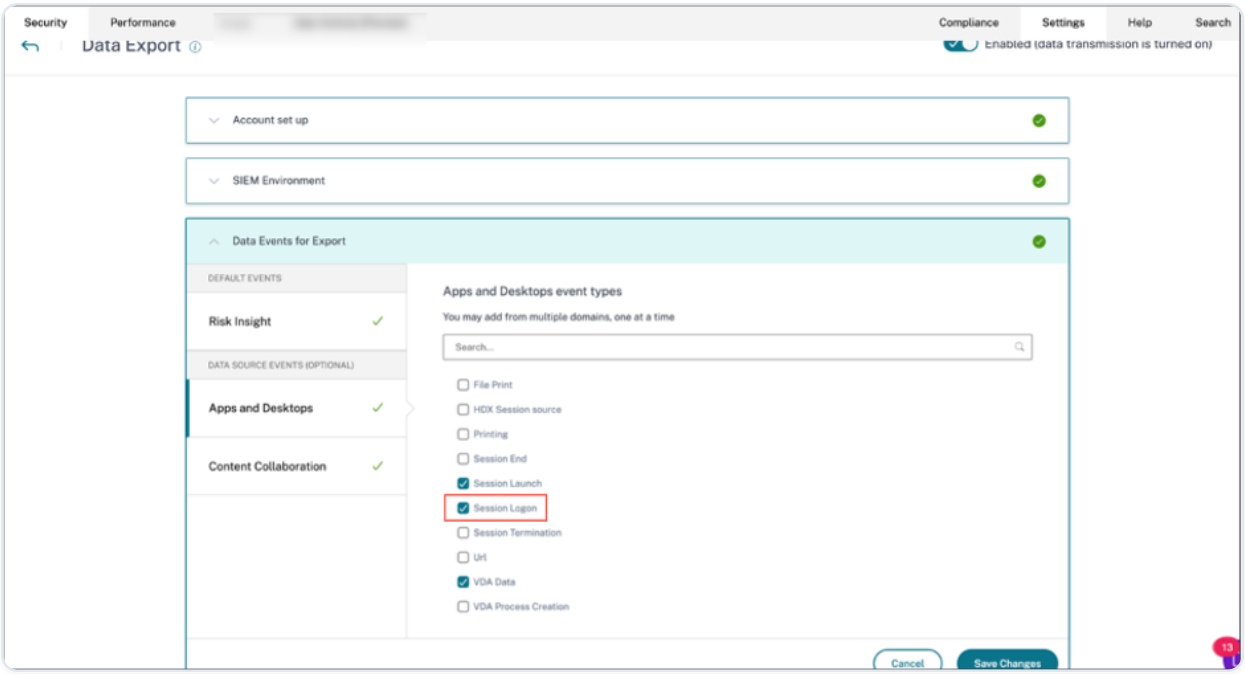
在 Splunk 环境中获取客户端 IP 和操作系统详细信息的另一种方法是配置用于导出的数据源事件。此功能允许自助服务搜索视图中存在的事件直接流入您的 Splunk 环境。有关如何配置要导出到 SIEM 的 Virtual Apps and Desktops 事件类型的更多信息，请参阅以下文章：

- 从 Citrix Analytics for Security 导出到 SIEM 服务的数据事件。
- 数据源事件

1. 导航到 **Citrix Analytic for Security 控制板 > 搜索**。在此自助服务搜索页面中，所有事件类型及其相关信息均可用。您可以在以下屏幕截图中看到 **Session.Logon** 事件类型作为示例：

   会话登录(/en-us/citrix-analytics/media/session-logon.png)

2. 在用于导出的数据源事件中配置 **Session.Logon**，然后点击 **保存** 以使其流入您的 Splunk 环境。

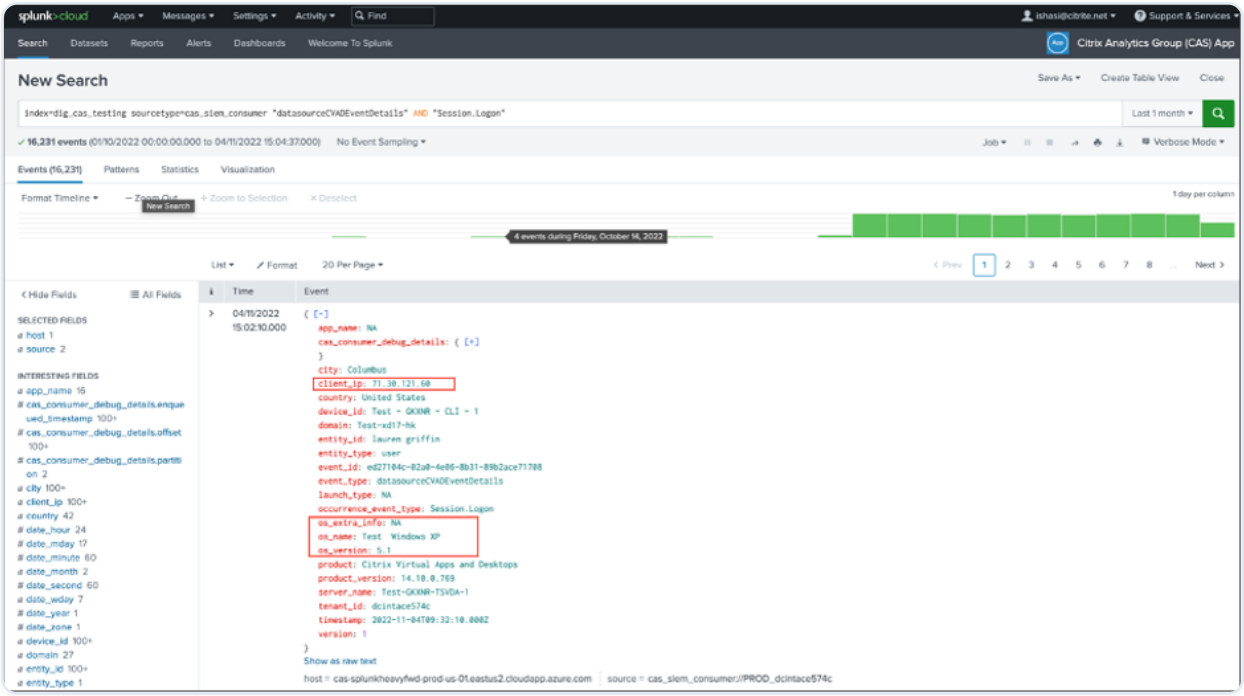


3. 前往 Splunk，然后输入并运行以下查询：

```
index="<index you configured>" sourcetype="<sourcetype you configured>"
"<tenant_id>" AND "datasourceCVADEventDetails" AND "Session.Logon"  AND
"<user you’re interested in>"
```

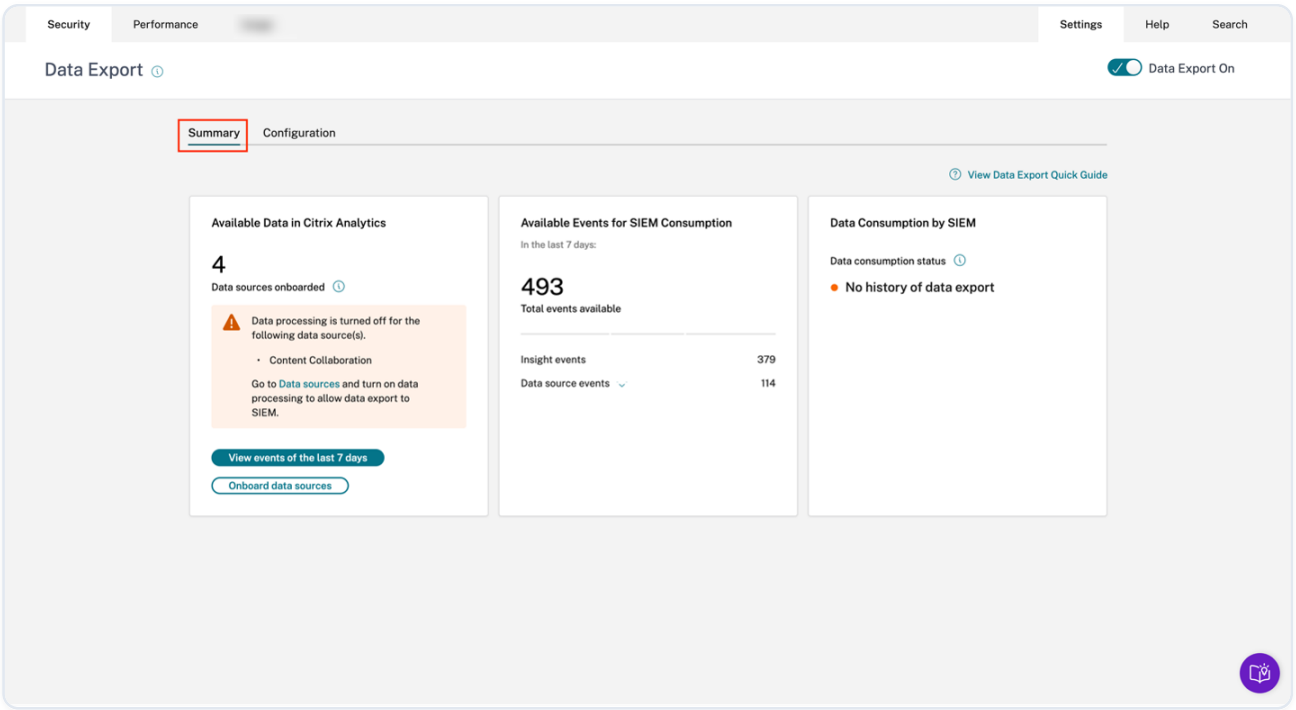
© 1997–2026 Citrix Systems, Inc. All rights reserved.

与客户端 IP 和操作系统相关的字段已突出显示。



故障排除数据导出

“安全数据导出”视图包含一个**摘要**选项卡，可帮助管理员排查其 SIEM 与 Citrix Analytics 的集成问题。**摘要**仪表板通过提供有助于故障排除过程的检查点，提供数据健康状况和流向的可见性。



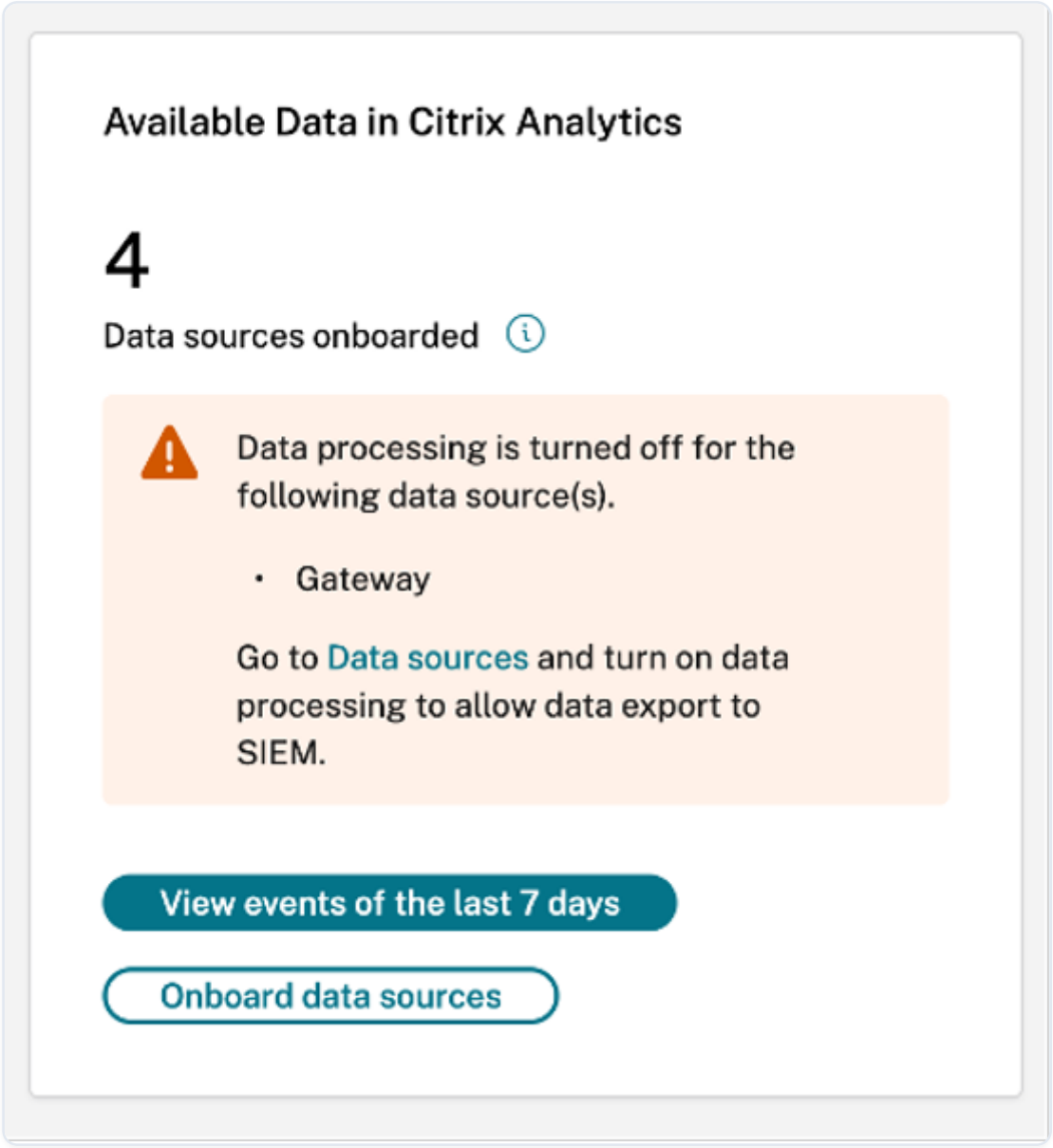
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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的基础。它通过以下三个卡片描述您的 SIEM 设置：

- **Citrix Analytics 中的可用数据**：此卡片显示数据源配置的状态。
- **可供 SIEM 使用的事件**：此卡片显示可供 SIEM 环境使用的事件数量。
- **SIEM 数据使用情况**：此卡片显示 SIEM 环境中数据流的状态。

Citrix Analytics 中的可用数据

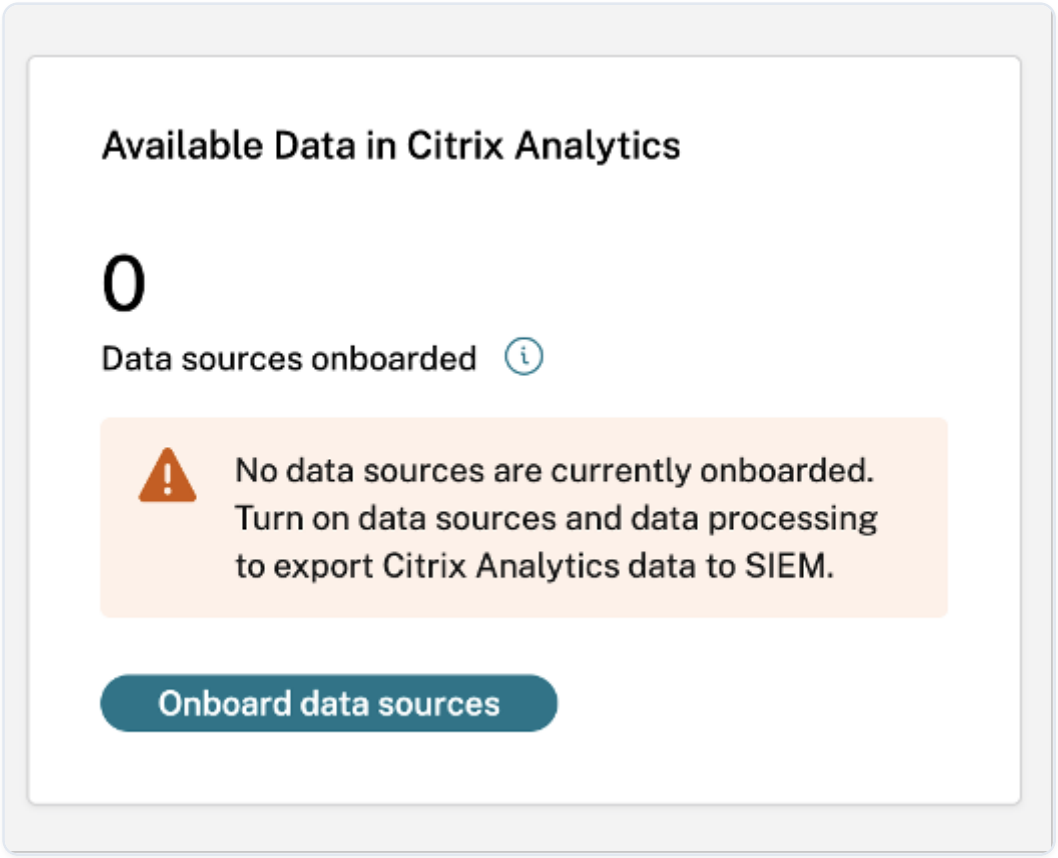


Citrix Analytics 中的可用数据卡片显示已载入 Citrix Analytics for Security 且最终可用于 SIEM 洞察的数据源数量。目前支持三种数据源用于数据导出：Apps and Desktops、Gateway 和 Secure Private Access。即使这些数据源已载入，对于数据处理已关闭的数据源，数据导出也将无法正常运行。当检测到此类数据源时，将显示如上图所示的相应警告消息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

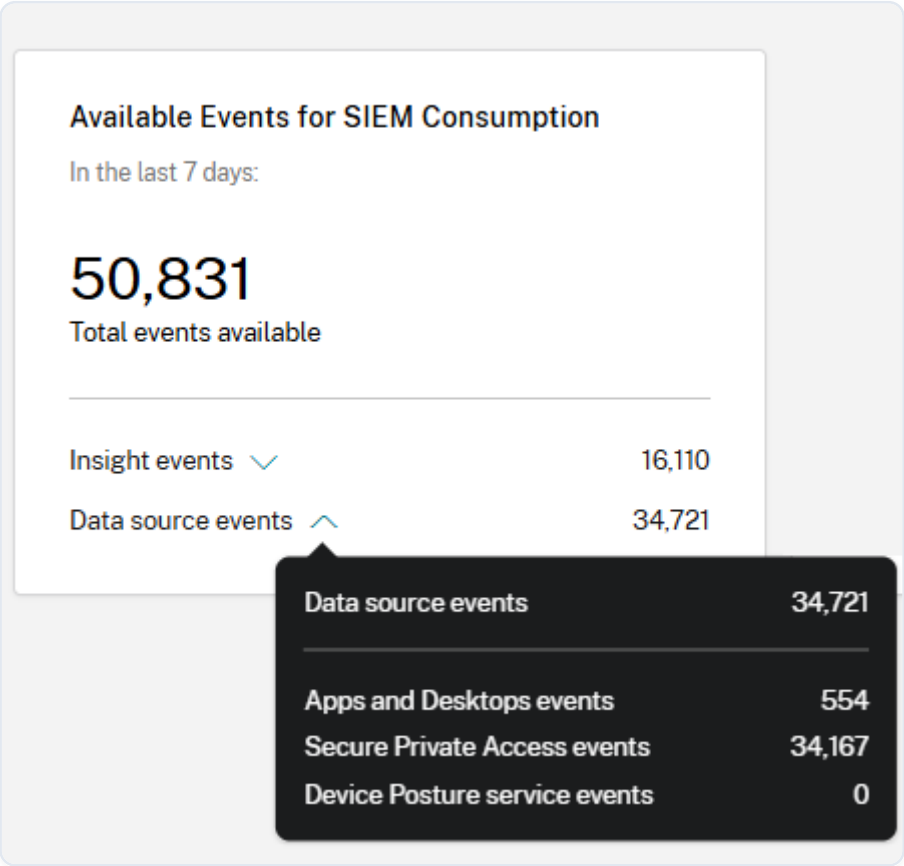
查看过去 7 天的事件按钮将管理员重定向到自助搜索视图，管理员可以通过该视图验证事件是否已流入 Citrix Analytics for Security。**载入数据源**按钮重定向到数据源视图，您可以在其中深入了解载入过程。

如果没有载入的数据源，将显示相应的警告消息，如以下屏幕截图所示：



© 1997–2026 Citrix Systems, Inc. All rights reserved.

可供 SIEM 使用的事件



“**可供 SIEM 消费的事件**”卡显示 Insight 和数据源事件的数量及其细分，这些事件预计将流入您的 SIEM 环境。展开后，还可以查看每种要导出的数据事件类型的进一步细分。

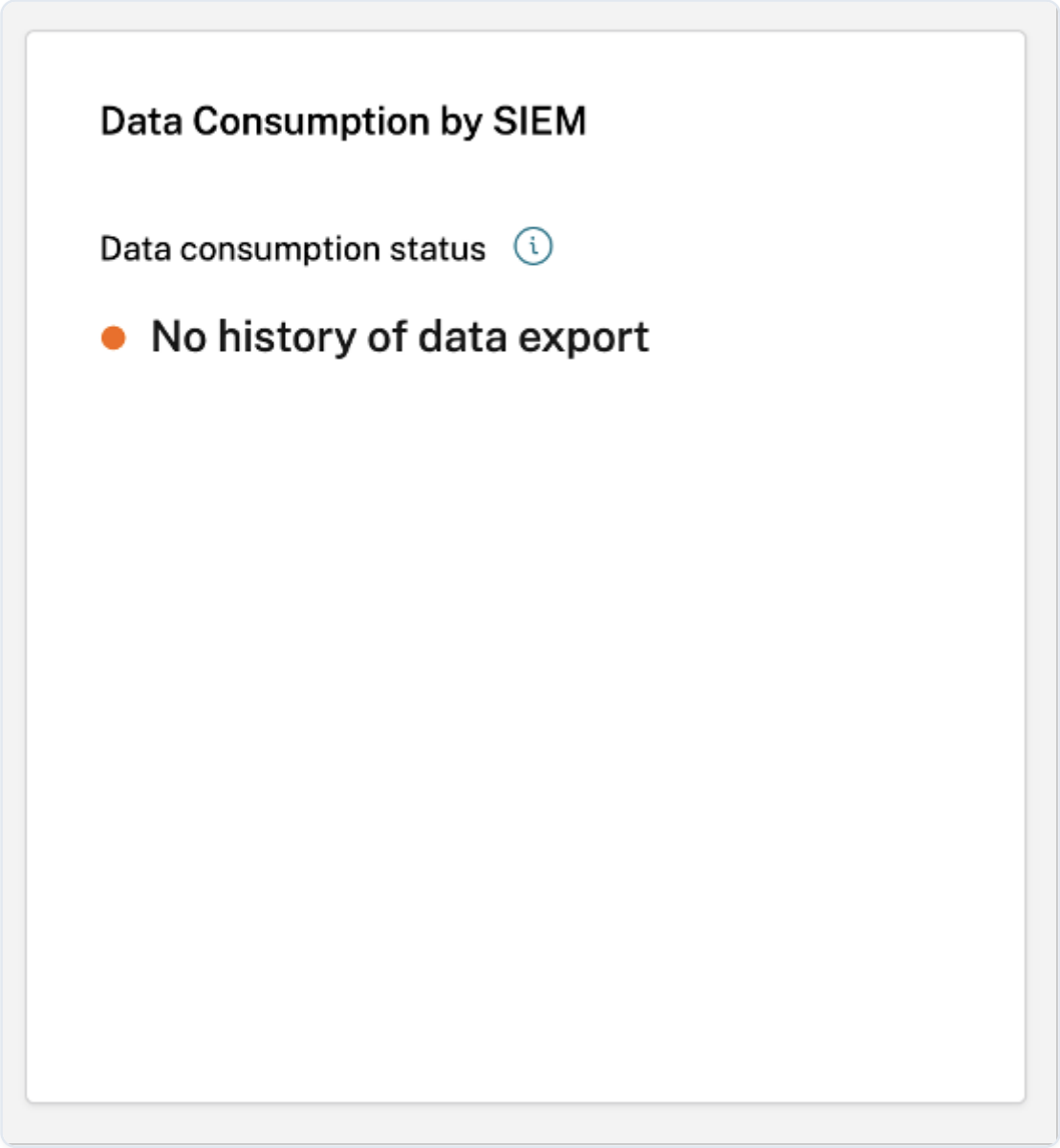
SIEM 的数据消耗

“**SIEM 的数据消耗**”卡显示了 Citrix Analytics 准备的数据流入 SIEM 环境的健康状况。数据消耗状态基于您的 **Kafka** 主题中的偏移量移动。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 10 分钟刷新一次。单击此处了解有关 Kafka 消费者组/偏移量管理的更多信息。

数据消耗状态可以采用以下状态：

1. **非活动消耗**
    - **无数据导出历史记录**：此状态由一个橙色点表示，表明 Citrix Analytics 准备的数据从未成功流入您的 SIEM 环境。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



这可能是由于以下原因造成的 -

- 数据源配置不正确/不完整。可以使用“**Citrix Analytics 中的可用数据**”卡来验证数据源是否充足，以及是否已启用数据处理以允许导出。
- 缺少用户活动。可以使用“**Citrix Analytics 中的可用数据**”卡中的“**查看过去 7 天的事件**”按钮来验证是否存在用户活动。此外，可以使用“**可供 SIEM 消费的事件**”卡来验证 Citrix Analytics 是否已准备好任何 Insight 或数据源事件以流入您的 SIEM。
- 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”阶段会显示一个绿色勾号。

  如果即使在成功设置帐户后状态仍未改变，请通过检查以下各项进行进一步故障排除：

  - 防火墙问题或 SIEM 设置错误 – 请参阅设置 SIEM 环境。
  - Kafka 帐户设置或 SIEM 环境的凭据问题 – 请参阅使用 Kafka 进行 SIEM 集成。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **未检测到活动消耗**：此状态表示在过去至少 10 分钟内，数据未能成功流入您的 SIEM 环境。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**可供 SIEM 消耗的可用事件**卡片来排查此问题。如果用户活动充足且可用事件计数增加，则最好关注上次成功的时间戳，以检查在该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**：此状态表示您的 SIEM 上次检测到活动消耗是在一周多以前。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**可供 SIEM 消耗的可用事件**卡片来排查您的 SIEM 设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



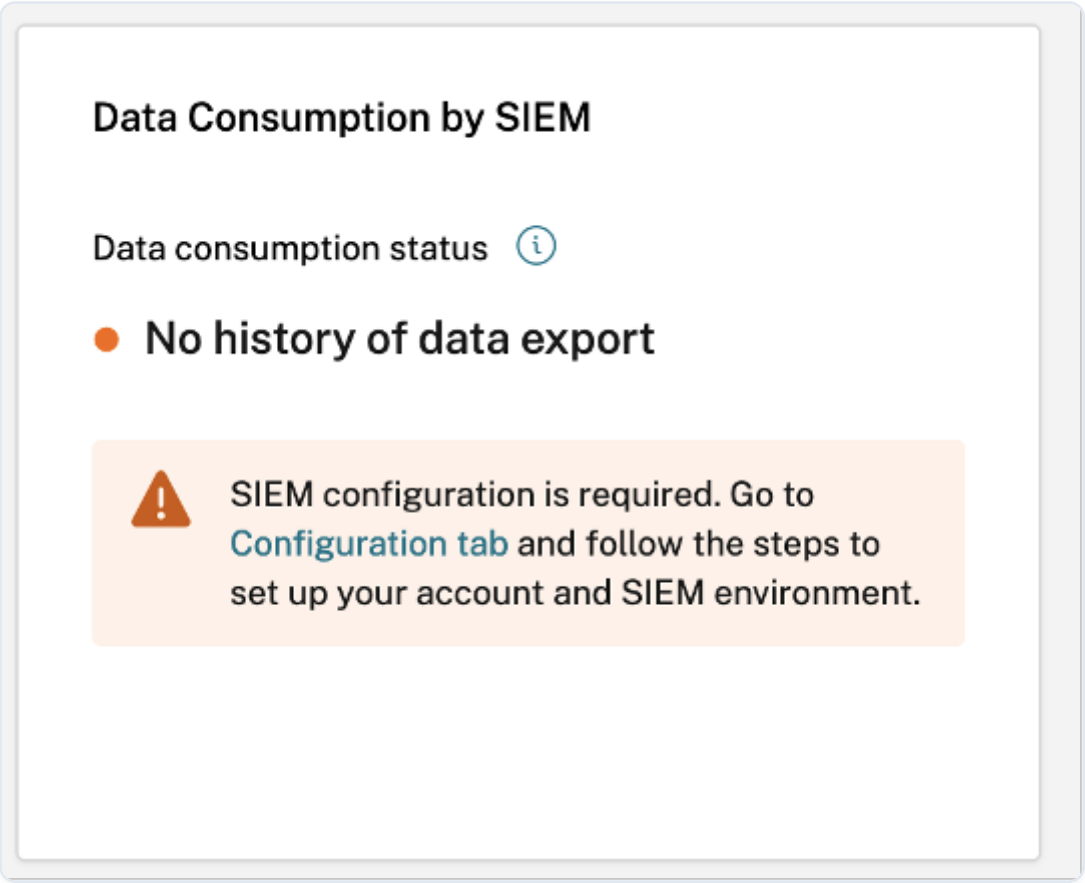
注意

Kafka 保留策略：Citrix Analytics Kafka 主题最多只保留事件 7 天。为避免或防止潜在的数据丢失，建议设置不超过 7 天的数据轮询间隔。

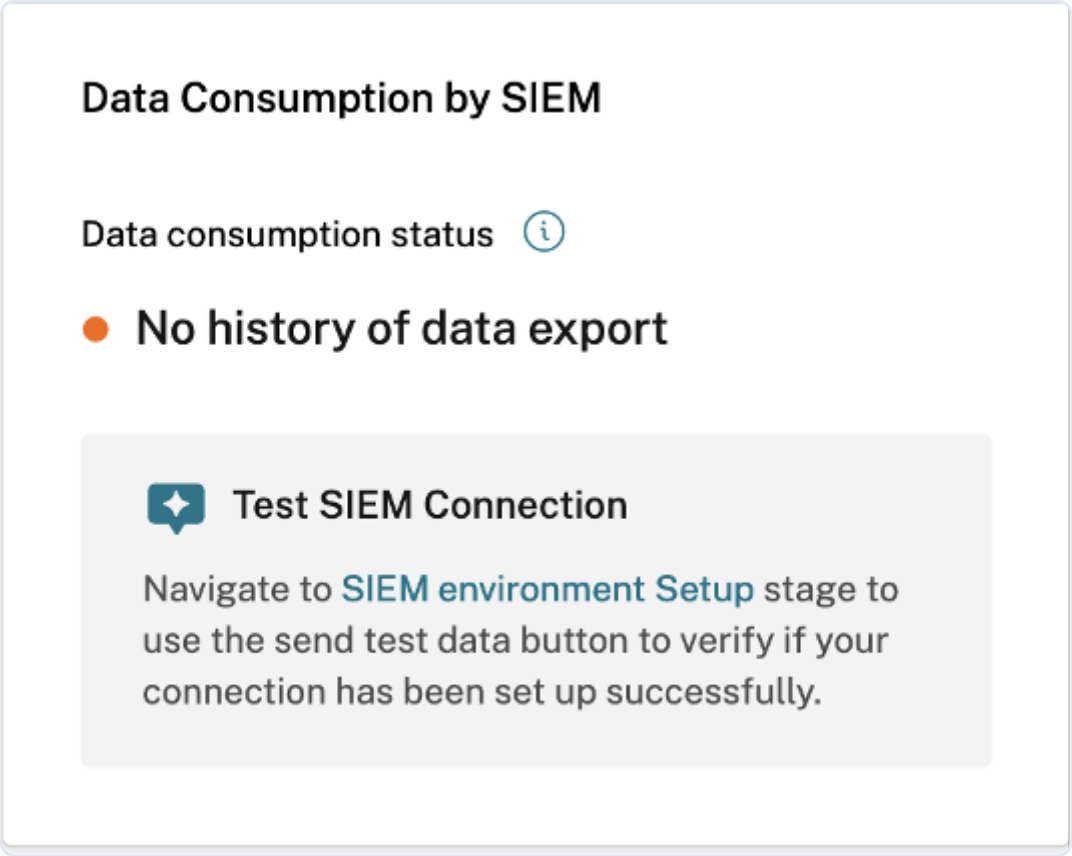
在非活动消耗中，您可以查看以下警告消息，以帮助您完成故障排除过程。

正如**无数据导出历史记录**案例中强调的那样，如果 SIEM 设置未完成，则数据永远不会流入 SIEM 环境。因此，用户将被重定向到**配置**选项卡以完成帐户设置，如以下屏幕截图所示：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



如果 SIEM 设置已完成，仍可能出现数据未主动流动的情况，如**未检测到活动消耗**或**7 天前导出**状态所示。因此，建议用户转到**测试事件生成**部分，以测试 SIEM 连接，如以下警告消息中突出显示的那样。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **活动消耗**

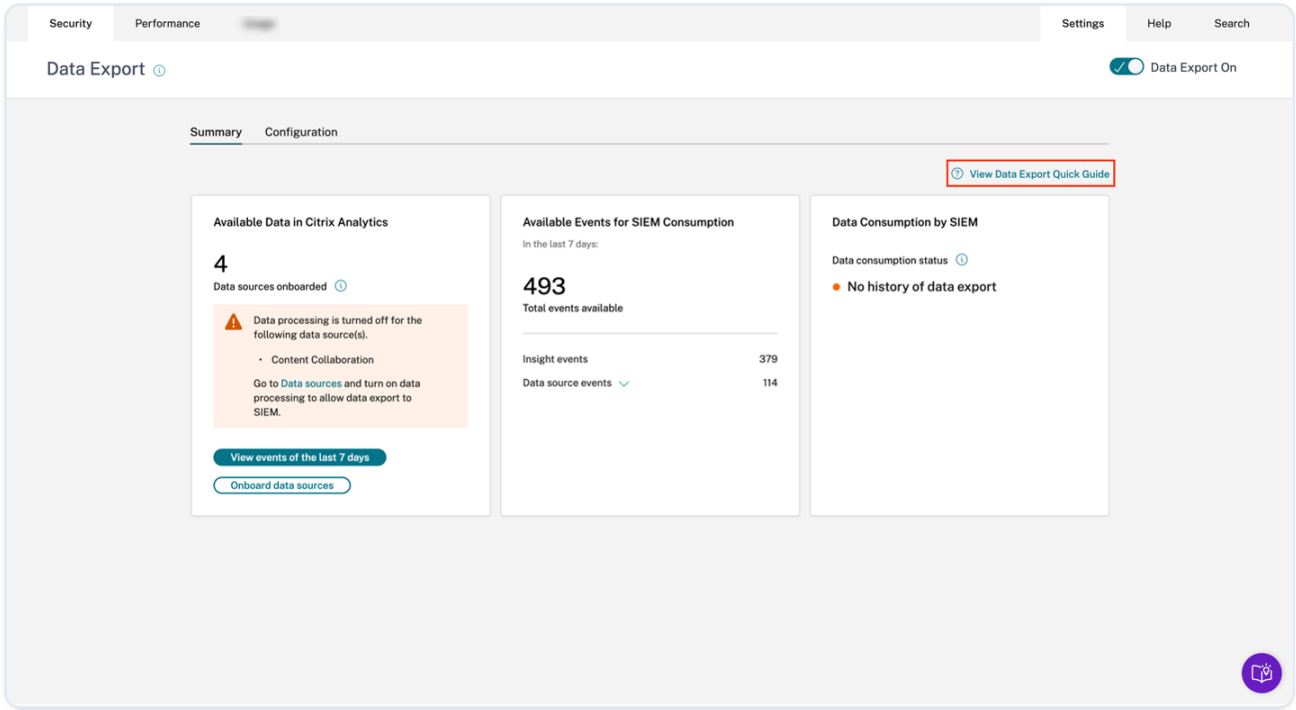
   - **检测到活动消耗**：此状态表示您的 SIEM 上已检测到活动消耗。

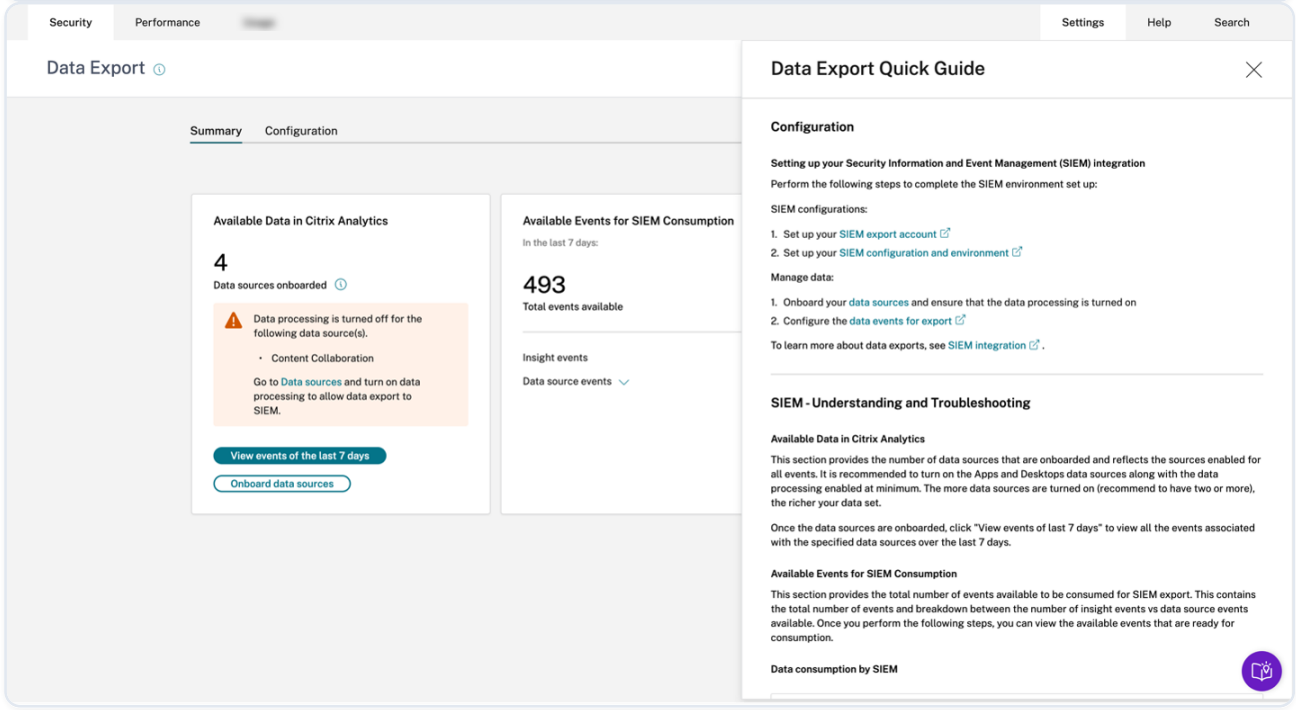


数据导出快速指南

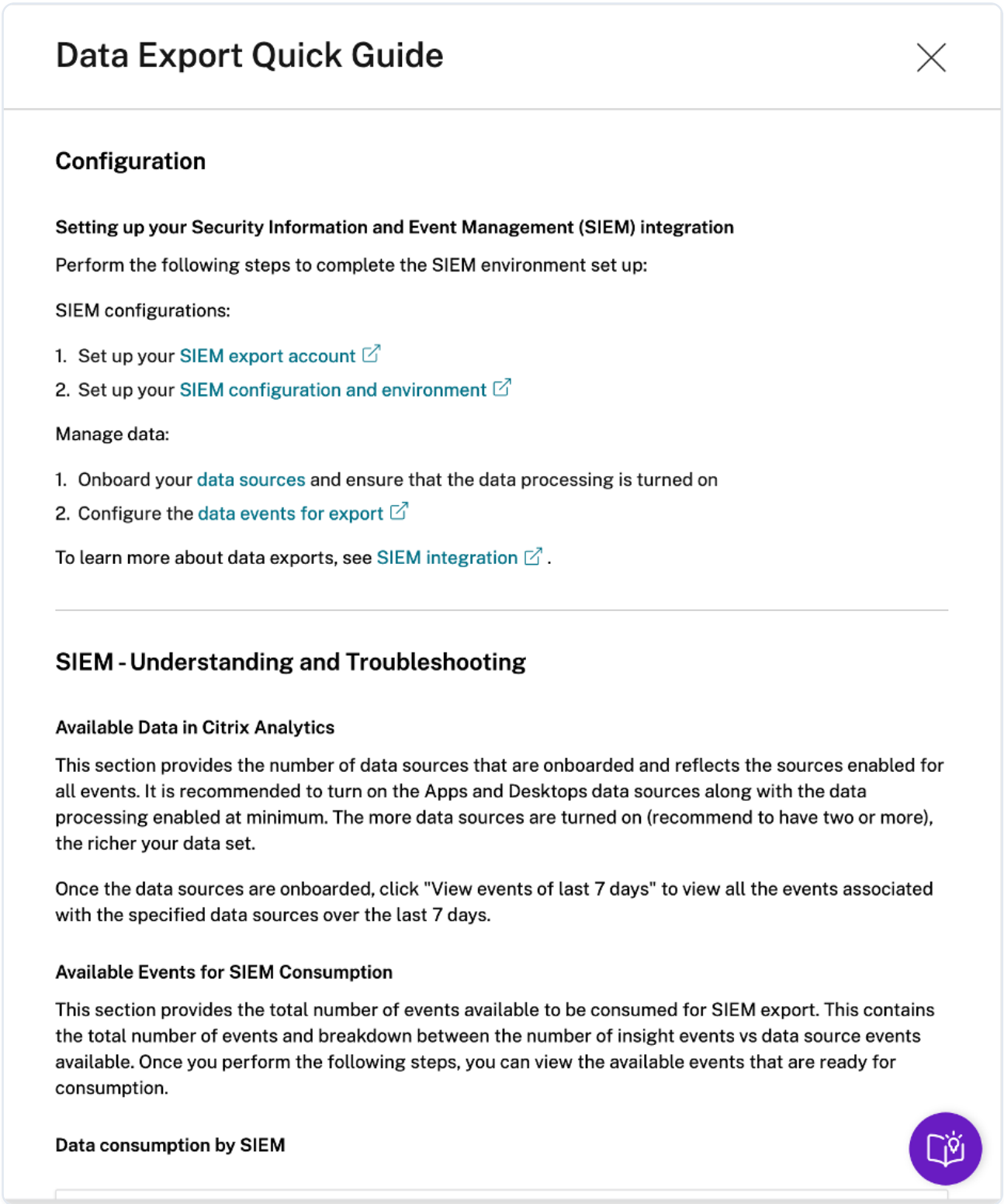
“**摘要**”选项卡补充了“**数据导出快速指南**”边栏，以简化 SIEM 设置的部署、管理和故障排除。除了提供“安全数据导出”视图的全面指南外，“快速指南”还通过提供相关文档的链接，包含有关如何设置和管理 SIEM 环境的有用提示。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



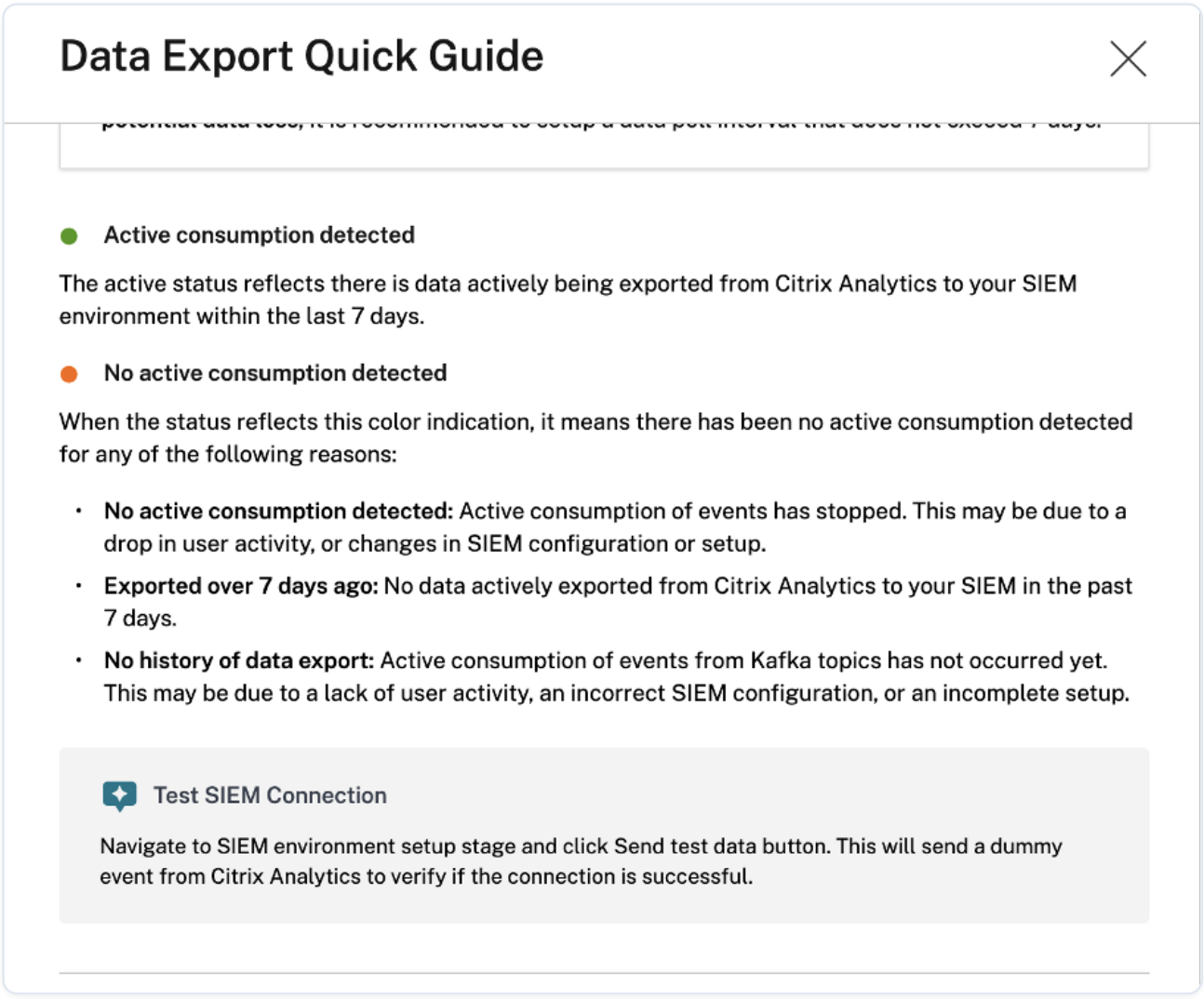


© 1997–2026 Citrix Systems, Inc. All rights reserved.



“快速指南”边栏中还有一个“**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 集成本身是否损坏，从而排除 Citrix Analytics for Security 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。

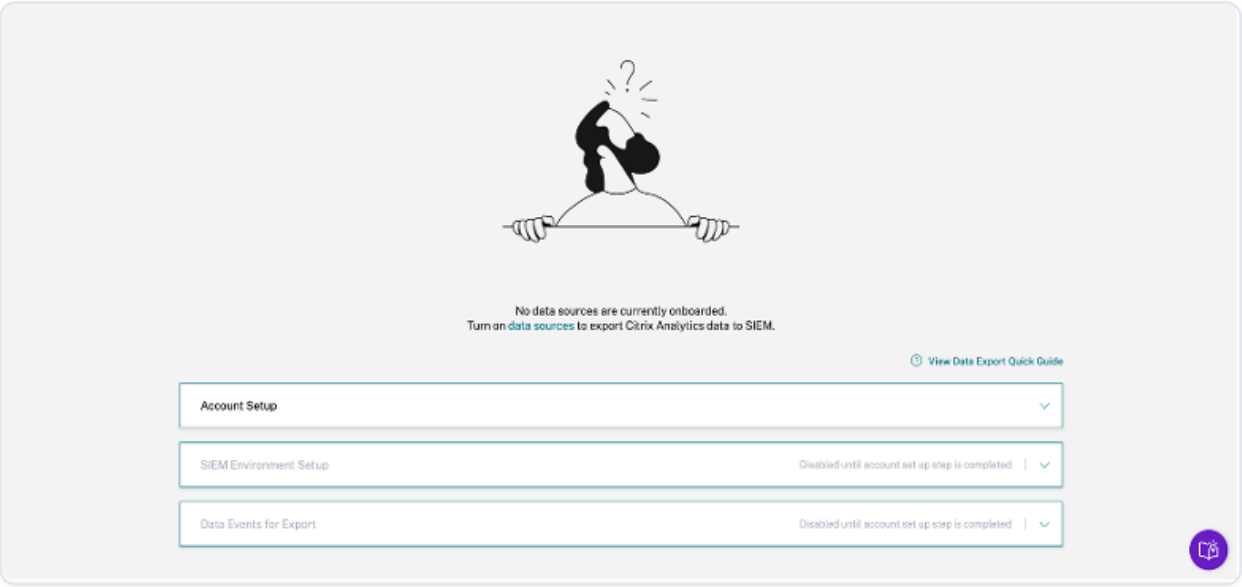
© 1997–2026 Citrix Systems, Inc. All rights reserved.



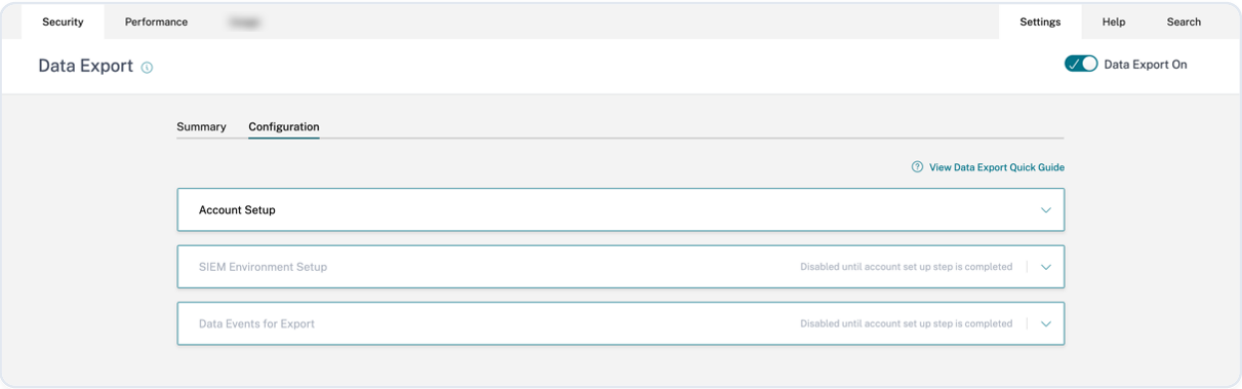
“**配置**”选项卡在指导部署设置的同时，还为管理员提供了有关设置 SIEM 时的有用提示、警告消息和常见陷阱。在以下情况下会显示相应的警告：

- Citrix Analytics 检测到没有数据源已载入。建议载入 Apps and Desktops 以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，也无法观察到数据流。

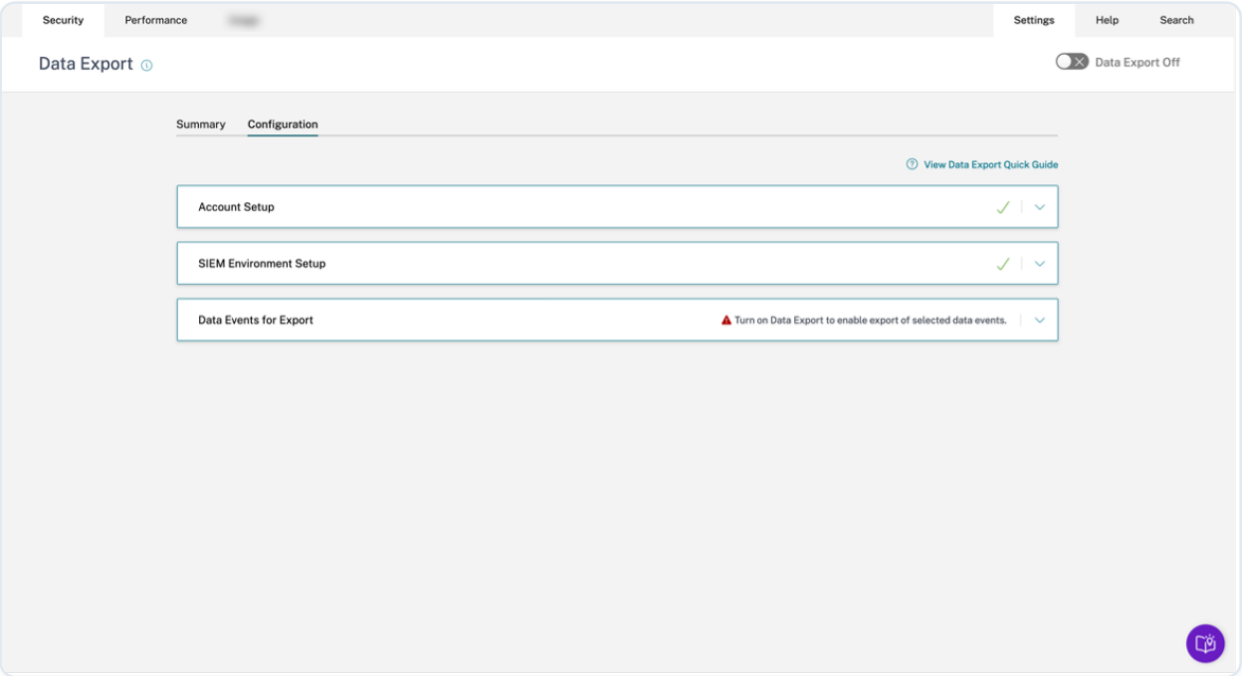
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 如下图所示，在成功完成帐户设置之前，“SIEM 环境设置”和“导出数据事件”阶段处于禁用状态。

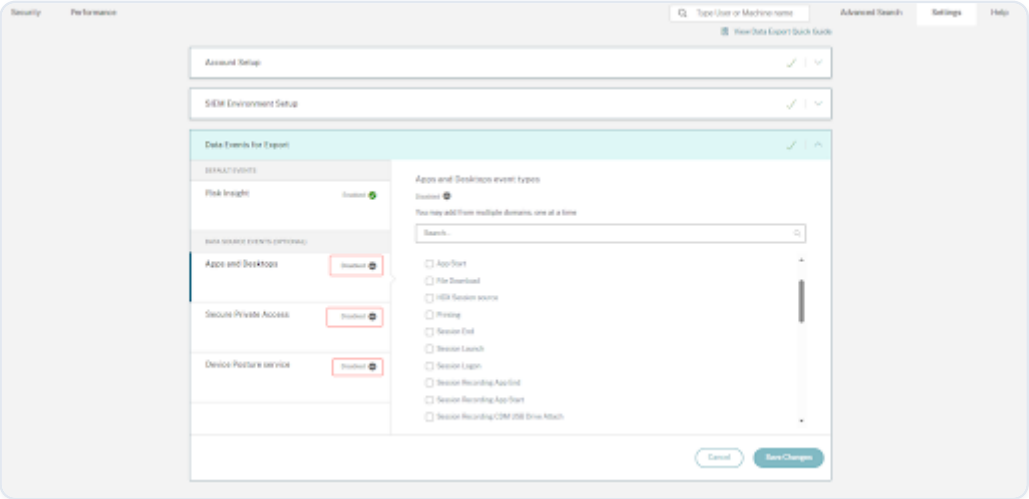


- 数据导出已关闭。“导出数据事件”阶段的警告提醒您启用数据导出以实现任何更改。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在“导出数据事件”阶段，如果特定数据源的数据导出被禁用，则没有数据源事件流向 SIEM。您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，请确保为相应数据源启用了数据处理，以确保数据到达 Citrix Analytics。

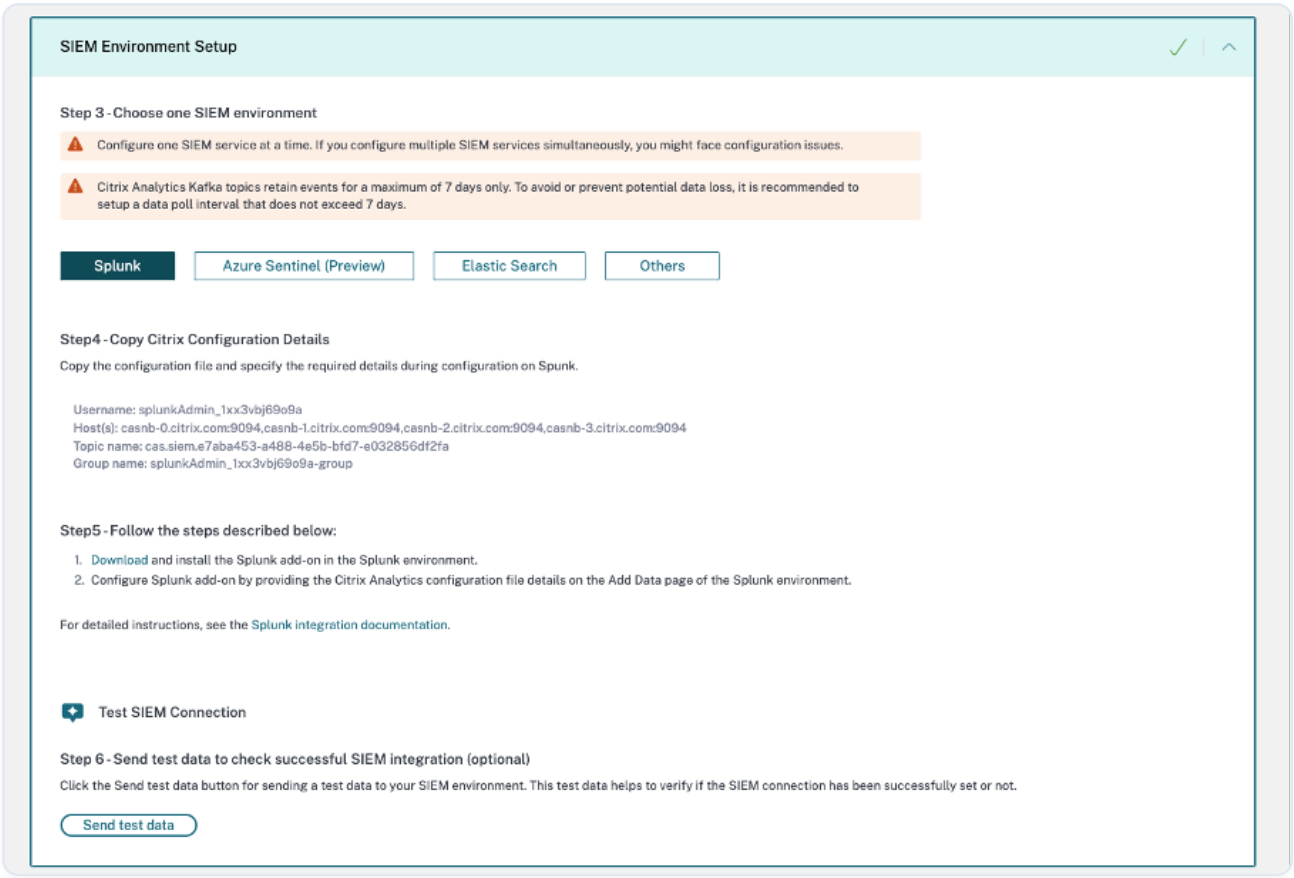


测试事件生成

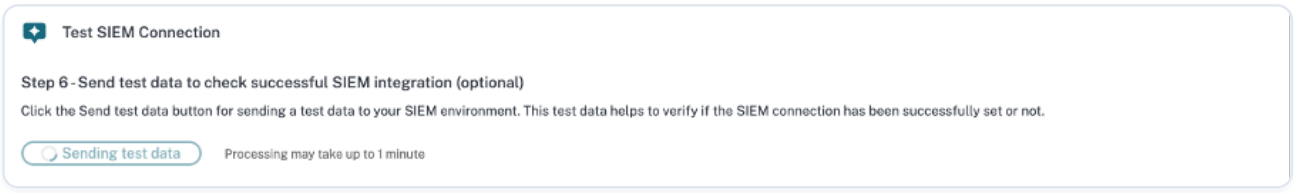
测试事件生成作为**SIEM 环境设置**阶段的一部分提供，旨在增强故障排除体验。用户完成 SIEM 设置后，测试事件生成提供了一种通过将测试事件直接发送到客户的 SIEM 数据导出 Kafka 主题来快速测试 SIEM 连接的方法。

它还使新用户能够快速测试其与 Citrix Analytics 的 SIEM 集成，而无需显式载入新的数据源并随后生成用户活动。

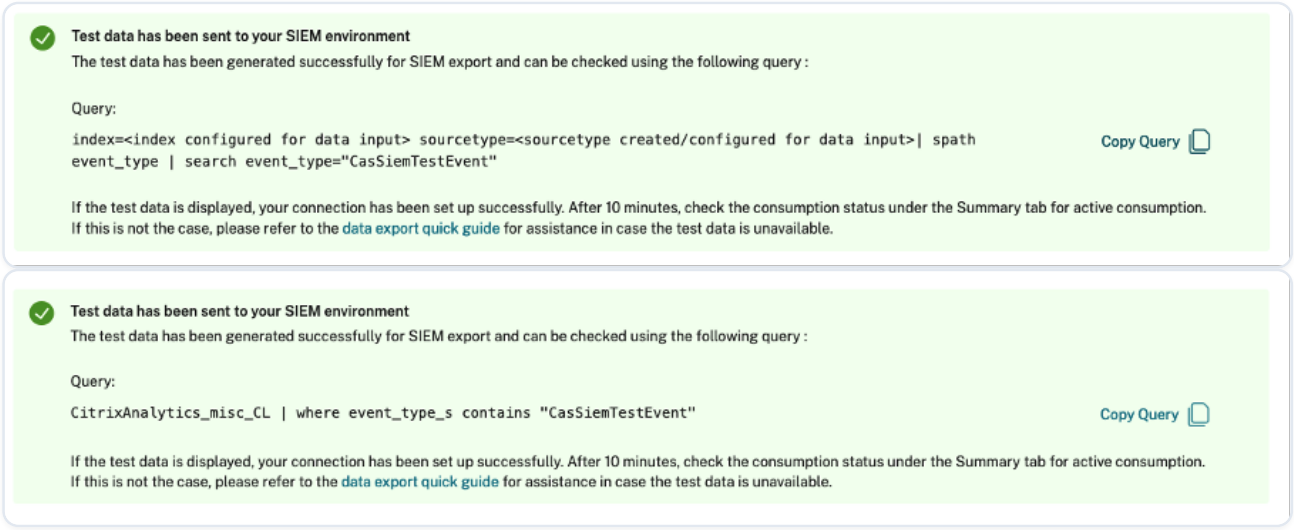
© 1997–2026 Citrix Systems, Inc. All rights reserved.



要测试此功能，用户需要单击**发送测试数据**按钮。这将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可能需要长达 1 分钟，如以下屏幕截图所示：

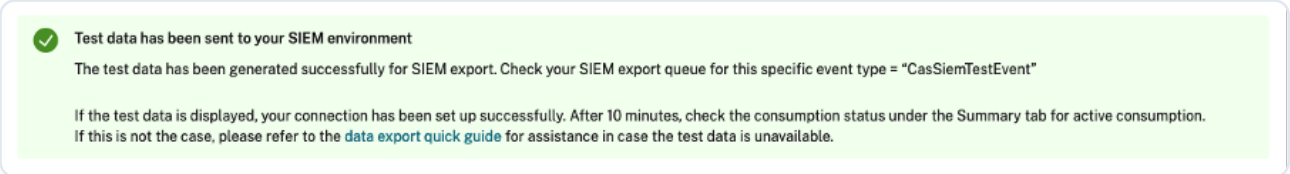


如果测试事件数据成功写入客户 Kafka 主题，则会显示一条成功消息，表明 SIEM 连接成功。根据您选择的环境（Splunk 和 Sentinel），管理员可以复制查询并检查其 SIEM 环境中的测试事件。



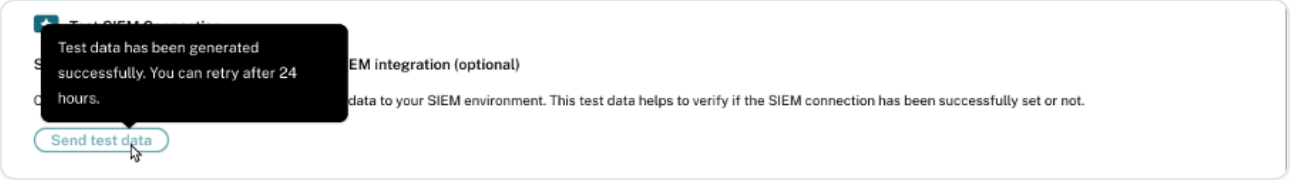
对于 Elasticsearch 和其他环境，将显示以下成功消息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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，并且用户将鼠标悬停在该按钮上时会看到以下弹出窗口。在最新成功时间戳后的 24 小时，该按钮将启用，供用户再次测试该功能。



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以测试连接。



SIEM 电子邮件警报

Citrix Analytics 会发送电子邮件警报，通知管理员可能导致数据流中断到其 SIEM 环境的场景。它包含有关可能导致临时/永久性安全态势数据丢失的活动的情境信息。它还有助于引导用户完成 SIEM 数据导出的自助故障排除过程。

此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它们：

- 此电子邮件将分发给 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。
- 发件人是 Citrix Cloud mailto:donotreplynotifications@citrix.com。
- 主题行是：
  - 对于密码重置电子邮件警报，主题行是：**SIEM 数据导出警报 - 密码已重置**。
  - 对于数据流中断电子邮件警报，主题行是：**SIEM 数据导出警报 - 数据流已停止**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

如何启用电子邮件通知?

如果您是具有自定义访问权限（安全完全管理员、安全只读管理员、安全和性能只读管理员）以管理 Security Analytics 的 Citrix Cloud 管理员，则您的 Citrix Cloud 帐户始终启用电子邮件通知。默认情况下，每周电子邮件通知会发送给 Citrix 安全管理员 - 默认列表。您还可以修改接收此警报的分发列表。有关更多信息，请参阅

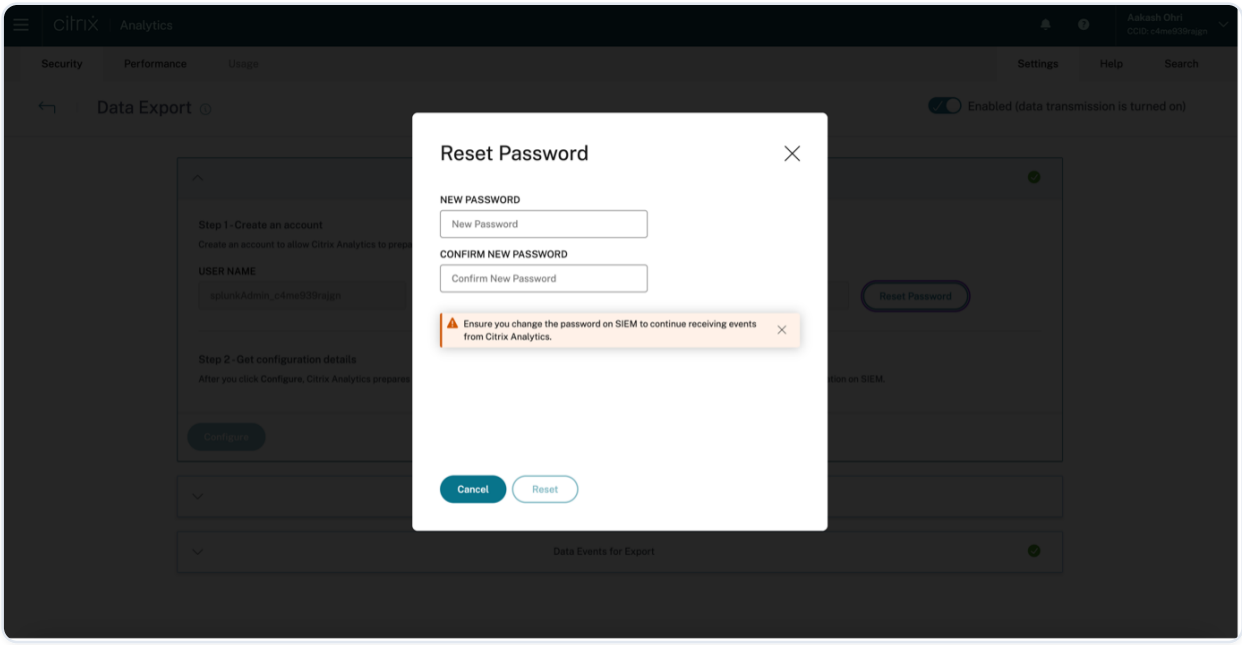
。

如果您是具有自定义访问权限（安全完全管理员、安全只读管理员、安全和性能只读管理员）以管理 Security Analytics 的 Citrix Cloud 管理员，则您的 Citrix Cloud 帐户始终启用电子邮件通知。

SIEM 电子邮件警报类型

1. **SIEM 密码重置电子邮件警报**

   当通过“数据导出”页面重置帐户密码时，会收到 SIEM 密码重置警报电子邮件。仅在 Citrix Analytics UI 上重置 SIEM 密码可能导致与 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，您可以转到“**摘要**”选项卡，检查“上次导出时间”时间戳是否与密码重置时间戳接近，从而传递必要的密码更改。这缩短了调试过程，并帮助您快速恢复到 SIEM 环境中的成功数据流。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 小时电子邮件警报**

   当 Citrix Analytics 服务到您的 SIEM 环境的数据流中断超过 24 小时时，会发送此电子邮件警报。电子邮件中包含上次事件导出的时间，以及可用于恢复数据流的有用故障排除快速提示。这是快速恢复数据流以避免丢失任何安全态势数据的正确时机。

3. **数据流中断 7 天电子邮件警报**

   当 Citrix Analytics 服务到您的 SIEM 环境的数据流中断超过 7 天时，会发送此电子邮件警报。由于客户 Kafka 主题的保留期为 7 天，因此务必遵循故障排除提示并参考“**数据导出**”页面上的快速指南，以避免丢失任何进一步的数据，因为此电子邮件警告的是安全态势信息永久丢失的情况。

4. **数据流中断 30 天电子邮件警报**

   当 Citrix Analytics 服务到您的 SIEM 环境的数据流中断超过 30 天时，会发送此电子邮件警报。此时，客户已丢失安全态势数据，因此必须尽快使用故障排除功能来恢复数据流。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

citrix | Analytics for Security

Data Flow Stopped 24 hours ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in the last 24 hours. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 24 hours, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 04 Apr, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

Regards,
Citrix Analytics for Security team

citrix | Analytics for Security

Data Flow Stopped 7 days ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in past 7 days. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 7 days, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 29 Mar, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

How can you benefit from the SIEM integration?

You can enhance the value of your SIEM by integrating it with Citrix Analytics for Security. This integration enables you to correlate your users' data with the data available in your SIEM environment along with deeper insights into your

citrix | Analytics for Security

Data Flow Stopped 30 days ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in past 30 days. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 30 days, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 06 Mar, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

How can you benefit from the SIEM integration?

You can enhance the value of your SIEM by integrating it with Citrix Analytics for Security. This integration enables you to correlate your users' data with the data available in your SIEM environment along with deeper insights into your organization's security posture.

Explore SIEM integration

Regards,

安全洞察的 Sigma 签名示例

此页面包含示例查询，可帮助管理员使用 Citrix Security Analytics 实现有意义的结果。

这些示例涵盖了以下类别的风险：

- 受感染的端点
- 内部威胁
- 数据渗漏

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**”站点卡片将显示在“**数据源**”页面上。单击“**开启数据处理**”以允许 Citrix Analytics 开始处理此数据源的数据。

Citrix Analytics for Security™ 会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并始终默认开启。有关详细信息，请参阅从 Citrix Analytics for Security 导出到 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接收的用户事件。从您的 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、开放的签名格式，用于创建分析师可用于描述日志事件的基于文本的查询，从而使检测更易于编写。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。

请参阅以下针对不同风险洞察的不同自定义指标用例：

- 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
- 允许列表之外的未经授权的操作系统
- 未经授权的 IP 地址或子网
- 未经授权的虚拟应用程序
- 异常桌面名称
- 监控特定应用程序
- 从SaaS应用打印
- SaaS应用上的剪贴板使用

受感染的端点

未经授权的浏览器

当用户尝试从组织 IT 策略不允许的浏览器类型或版本访问内容，或由于安全漏洞而访问内容时，会发生这种情况。

详细信息

数据源：应用程序和桌面 (Workspace App)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CAS 查询

```
Event-Type = "Session.Logon" AND Browser-Name !~ "<Browser-Name>"
```

当用户输入凭据并登录其应用程序或桌面会话时，会触发 Session.Logon 事件。

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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

未经授权的操作系统

当用户尝试访问的设备所使用的操作系统类型或版本不符合组织 IT 策略的规定，或存在安全漏洞时，会发生这种情况。

详细信息

数据源：应用程序和桌面 (Workspace App)

CAS 查询

```
Event-Type = "Session.Logon" AND OS-Name ~ "<OS-Name>" AND OS-Version =
"<OS-Version>" AND OS-Extra-Info = "<OS-Extra-Info>"
```

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:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  product: citrixanalytics

  service: security

title: Unauthorized operating systems in block list
```

未经授权的 IP 地址或子网

当用户尝试从被组织 IT 策略标记为未经授权的 IP 地址或范围进行访问时，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.*>"
```

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:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  - occurrence_event_type: Session.Logon

logsource:

  product: citrixanalytics

  service: security

title: Access from unauthorized IP
```

允许列表之外的未经授权的操作系统

当用户尝试从托管允许列表之外的操作系统服务器访问应用程序时，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>"
```

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:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  - os_version: '<OS Version>'

  filter_os_extra:

  - os_extra_info: '<OS Extra Info>'

  filter_null:

  - os_name: null

  - os_version: null

  - os_extra_info: null

  selection:

  - occurrence_event_type: Session.Logon

logsource:

  product: citrixanalytics

  service: security

title: Unauthorized operating systems outside allow list
```

未经批准的 Workspace 应用程序版本

当用户尝试访问不受支持的客户端版本的 Workspace 应用程序时，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受支持的版本。有关更多信息，请参阅支持的客户端版本。

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*"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

内部威胁

异常桌面名称

当用户尝试启动一个不被认为是常规的桌面时，会发生这种情况。

详细信息

数据源：应用程序和桌面 (Workspace App)

CAS 查询

```
Event-Type = "Session.Logon" AND Session-Launch-Type = "desktop" AND App-Name ~ "<Desktop Name>"
```

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'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
logsource:

  product: citrixanalytics

  service: security

title: Unusual desktop names
```

监控特定进程

当用户启动监视列表中的已发布应用程序时，会发生这种情况。其目的可能是监控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（会话录制）

CAS 查询

```
Event-Type = "Citrix.EventMonitor.AppStart" AND App-Name IN ("<App-Name-1>", "<App-Name-2>")
```

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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  selection:
  - occurrence_event_type: Citrix.EventMonitor.AppStart
logsource:
  product: citrixanalytics
  service: security
title: Monitor specific process
```

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，会发生这种情况。

详细信息

数据源：应用程序和桌面 (Workspace App)

CAS 查询

```
Event-Type = "App.Start" AND App-Name IN ("<App-Name1>", "<App-Name2>")
```

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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  selection:
  - occurrence_event_type: App.Start
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized virtual apps
```

数据外泄

从 SaaS 应用程序打印

当文件从不允许打印的 SaaS 应用程序中打印时，会发生这种情况。它通过监控 SaaS 应用程序中的打印操作来检测潜在的数据外泄。

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>"
```

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:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  - saas_app_name: '<App-Name>'
  filter_null:
  - saas_app_name: null
  selection:
  - occurrence_event_type: App.SaaS.File.Print
logsource:
  product: citrixanalytics
  service: security
title: Printing from SaaS apps
```

SaaS 应用程序上的剪贴板使用情况

当从任何 SaaS 应用程序执行剪切、复制或粘贴活动时，会发生这种情况。它通过监控剪贴板操作来检测组织中 SaaS 应用程序的潜在数据外泄。

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" )
```

Sigma 签名

```
author: Citrix
date: 2023/01/31
description: Clipboard usage on SaaS apps
detection:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

用户仪表板

概述

“**用户**”仪表板是用户行为分析和威胁预防的起点。

此仪表板可让您全面了解组织中的用户行为模式。利用这些数据，您可以主动监控、检测并标记异常行为，例如网络钓鱼或勒索软件攻击。

要查看用户仪表板，请转到“**安全 > 用户**”。用户仪表板包含以下部分：

用户仪表板(/en-us/citrix-analytics/media/users-dashboard.png)

- **用户活动状态**：总用户、活跃用户和非活跃用户的分布。
- **用户风险分布**：活跃用户、非活跃用户、总用户的分布，以及根据所选时间段内计算出的最高风险评分，将风险用户分为高、中、低配置文件的分布。
- **热门用户**：热门用户按其风险评分排序，并按所有用户、特权用户和观察列表用户进行细分。
- **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被分组到类别中。
- **风险指标和操作**：在选定持续时间内，组织中所有用户的风险指标和操作分布图。
- **访问摘要**：总结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项策略和操作。
- **风险指标**：显示组织中的前五项风险指标。

用户活动状态

您的组织中已启用分析功能的数据源所使用的用户总数。他们可能具有或不具有与其账户关联的风险评分。此磁贴显示活跃用户数量。活跃用户是指在选定时间段内检测到事件的用户。您可以点击用户活动状态下拉菜单，查看总用户在活跃用户和非活跃用户之间的分布。

- 总用户：在选定时间范围内用户总数。
- 活跃用户：在选定时间范围内检测到事件的用户。
- 非活跃用户：在选定时间范围内未检测到事件的用户。

用户仪表板上的用户总数可能多于风险用户数，因为并非所有用户都被认为是风险用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

在**用户**页面上，无论选择的时间段如何，都会显示过去 30 天的用户总数。

筛选条件

根据以下类别筛选用户事件：

- **风险评分**：基于高风险、中风险、低风险和零风险评分的用户事件。
- **用户**：基于管理员权限、高管权限和观察列表用户的用户事件。
- **已发现数据源**：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。

最新评分

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，并根据用户行为分析而变化。根据最新的风险评分，用户可分为以下几类：高风险用户、中风险用户、低风险用户和零风险评分用户。

用户

Analytics 发现的所有用户列表。选择一个用户名以查看该用户的用户信息和风险时间线。该用户可能触发或未触发任何风险指标。如果没有与此用户关联的风险事件，您将看到以下消息。

无风险事件(/en-us/citrix-analytics/media/no-risky-event.png)

如果存在与用户关联的风险事件，您将在其风险时间线上看到风险指标。选择该用户以查看其风险时间线。

用户可以标记为`privileged`并添加到观察列表。

发现的数据源

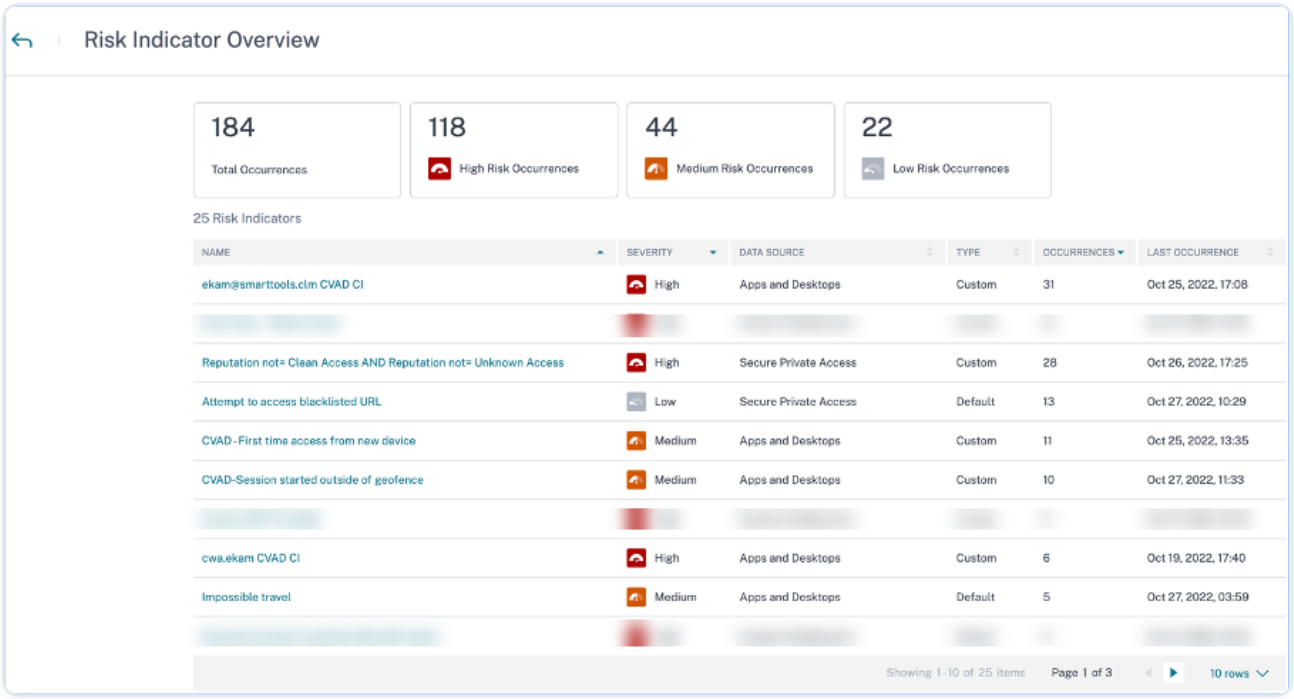
与用户关联的数据源。当用户主动使用数据源时，Analytics 会从该数据源接收用户事件。要接收用户事件，您必须在数据源站点卡上开启数据处理，该卡可在“**数据源**”页面上找到。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已触发的指标

指示在所选持续时间内跨用户触发的风险指标数量。单击“**已触发的指标**”磁贴以查看风险指标详细信息。风险指标表提供以下详细信息：

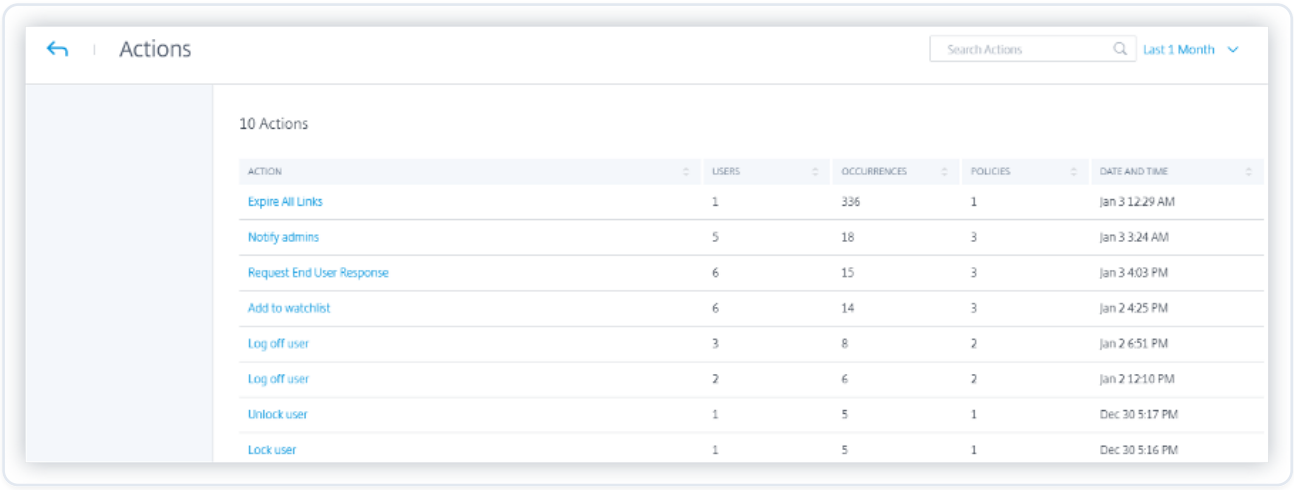
- **名称**：风险指标名称。
- **严重性**：与事件关联的风险严重性。风险可以是高、中或低。
- **数据源**：应用风险指标模板的数据源。
- **类型**：风险指标类型。风险指标可以是默认或自定义的。
- **发生次数**：风险指标为用户触发的次数。当您选择时间段时，风险指标的发生次数会根据时间选择而变化。
- **上次发生**：显示上次发生日期和时间。



已应用的操作

指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**”磁贴以查看操作详细信息。此部分不显示您手动应用于用户配置文件的操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

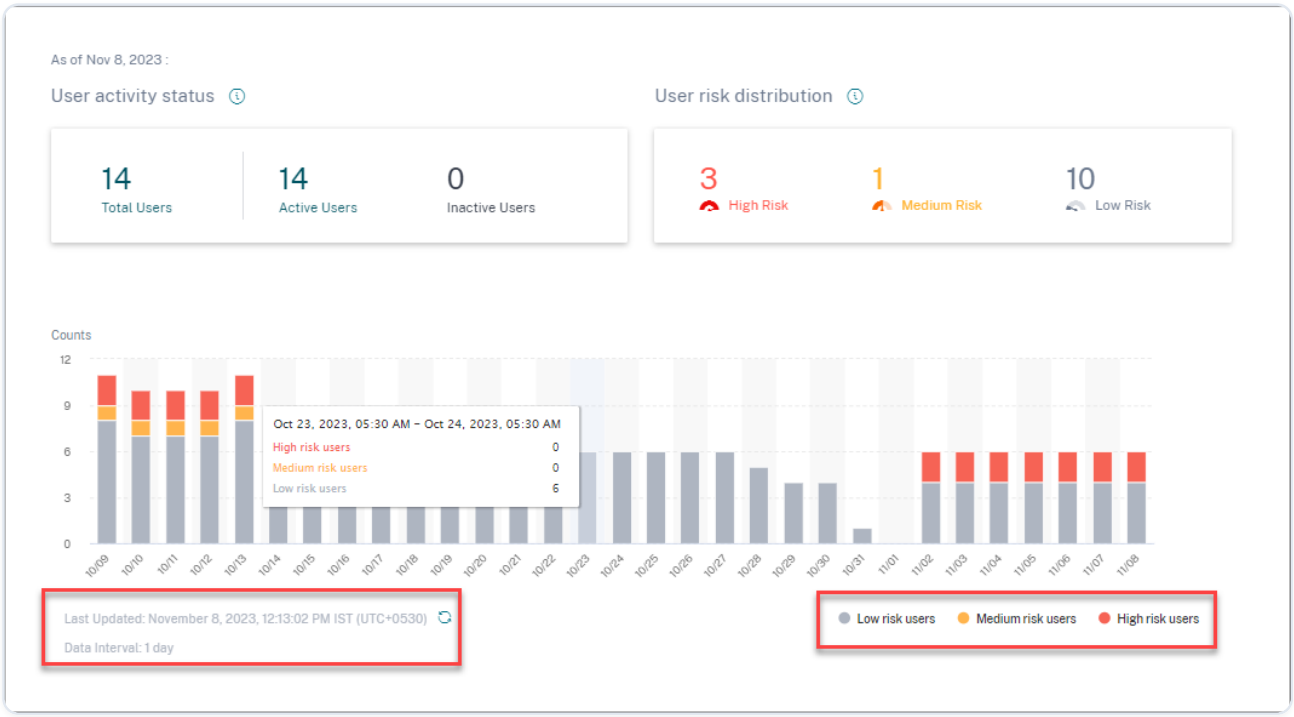


操作表提供以下信息：

- **操作**：根据策略应用的操作名称。
- **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

从您连接的数据源接收到的用户事件总数，并由 Analytics 处理。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

用户风险分布

您可以根据所选时间段内用户的最高计算风险评分，查看高、中、低风险配置文件中的用户数量。在总计数下方，条形图显示了低、中、高风险用户分布随时间的变化。

用户风险分布(/en-us/citrix-analytics/media/user-risk-distribution.png)

风险等级分为三种颜色代码。

- **红色** - 代表高风险用户。
- **橙色** – 代表中风险用户。
- **灰色** – 代表低风险用户。

您可以将鼠标悬停在颜色条上，根据特定时间段查看高、中、低风险用户的数量。您可以查看上次更新的详细信息（日期和时间）以及数据间隔信息。单击任意颜色条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。

风险用户

风险用户是指那些关联了风险事件并至少触发了一个风险指标的用户。用户在特定时间段内对网络造成的风险等级由与用户关联的风险评分决定。风险评分值是动态的，并基于用户行为分析。

每个用户的风险都会根据用户活动随时间定期更新。因此，用户可能在某个时间点处于中等或高风险，但随后会降至较低的风险级别。根据风险评分，风险用户可分为以下几类：

- 高风险
- 中风险
- 低风险

在“**风险用户**”页面上，您可以使用分面根据所选时间段关联的风险级别进行筛选，并使用搜索栏查询特定用户。

风险用户分面(/en-us/citrix-analytics/media/risky-users-facet.png)

单击用户的电子邮件 ID 可查看该特定所选用户的“**风险时间线**”页面。此页面会显示风险指标以及根据所选时间段的“**最新**”和“**最高风险评分**”详细信息。

最新和最高风险评分(/en-us/citrix-analytics/media/latest-and-highest-risk-score.png)

高风险

风险评分在 90 到 100 之间的用户。这些用户表现出多种与中度到重度风险因素一致的行为，并可能对组织构成直接威胁。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在**用户**仪表板上，您可以根据所选时间段内计算出的最高风险评分，查看高风险用户的数量。

高风险用户(/en-us/citrix-analytics/media/high-risk-users.png)

单击**高风险**选项以查看**风险用户**页面。该页面显示了有关高风险用户的详细信息。

中风险

风险评分在 70 到 89 之间的用户。这些用户通常有一个或多个看起来可能可疑和/或异常的活动，并且可能值得密切监控。

中风险用户(/en-us/citrix-analytics/media/medium-risk-users.png)

单击**中风险**选项以查看**风险用户**页面。该页面显示了有关中风险用户的详细信息。

低风险

风险评分在 1 到 69 之间的用户。这些用户至少有一个风险指标反映出一些不寻常或意外的行为，但不足以构成更严重的风险分类。

低风险用户(/en-us/citrix-analytics/media/low-risk-users.png)

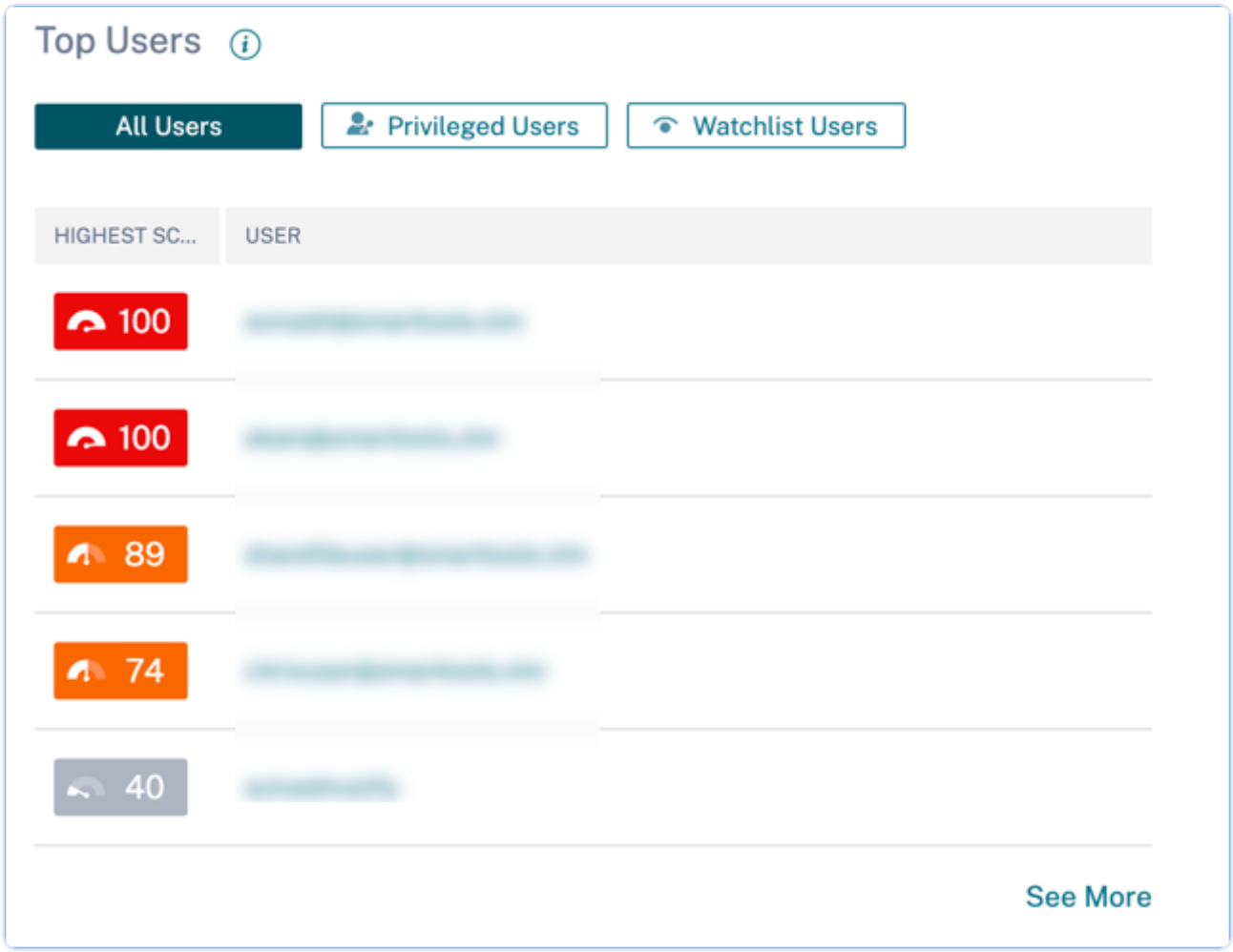
单击**低风险**选项以查看**风险用户**页面。该页面显示了有关低风险用户的详细信息。

低风险评分(/en-us/citrix-analytics/media/low-risk-score.png)

热门用户

您可以查看各种用户类别中的热门用户，这些用户按所选时间段内的最高风险评分进行排序。以下**热门用户**表显示了基于所选时间段内计算的风险评分（而非最新风险评分）的五位风险最高的（所有、特权和观察列表）用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意

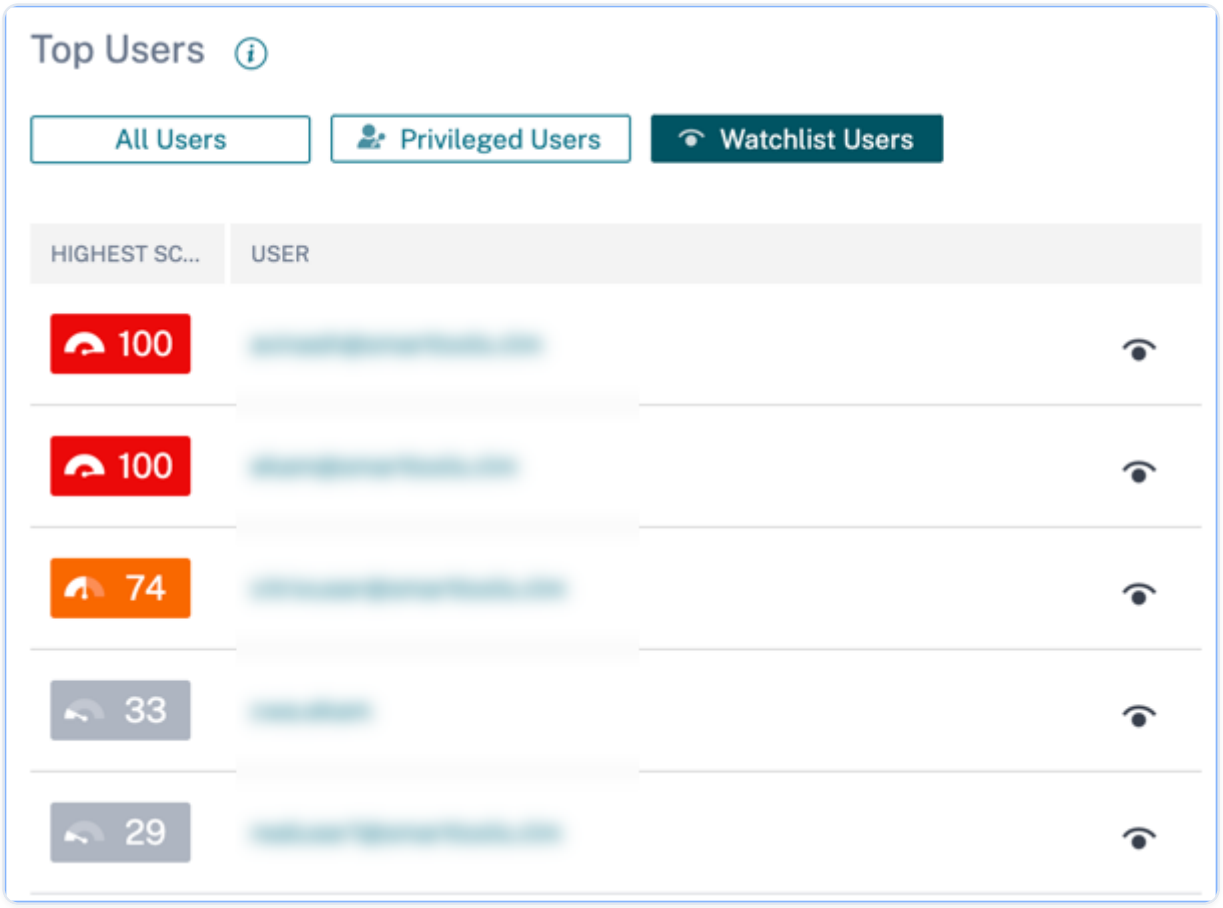
在早期版本中，“热门用户”表始终显示最新风险评分，无论所选时间段如何。

观察列表用户

密切监控潜在威胁的用户列表。例如，您可以通过将非组织全职员工的用户添加到观察列表来监控他们。您还可以监控频繁触发特定风险指标的用户。您可以手动将用户添加到观察列表，或定义策略以将用户添加到观察列表。

如果您已将用户添加到观察列表，则可以根据最高评分查看观察列表中的前五名用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



单击**所有用户**面板上的**查看更多**链接以查看**用户页面**。该页面显示观察列表中的所有用户列表。

注意

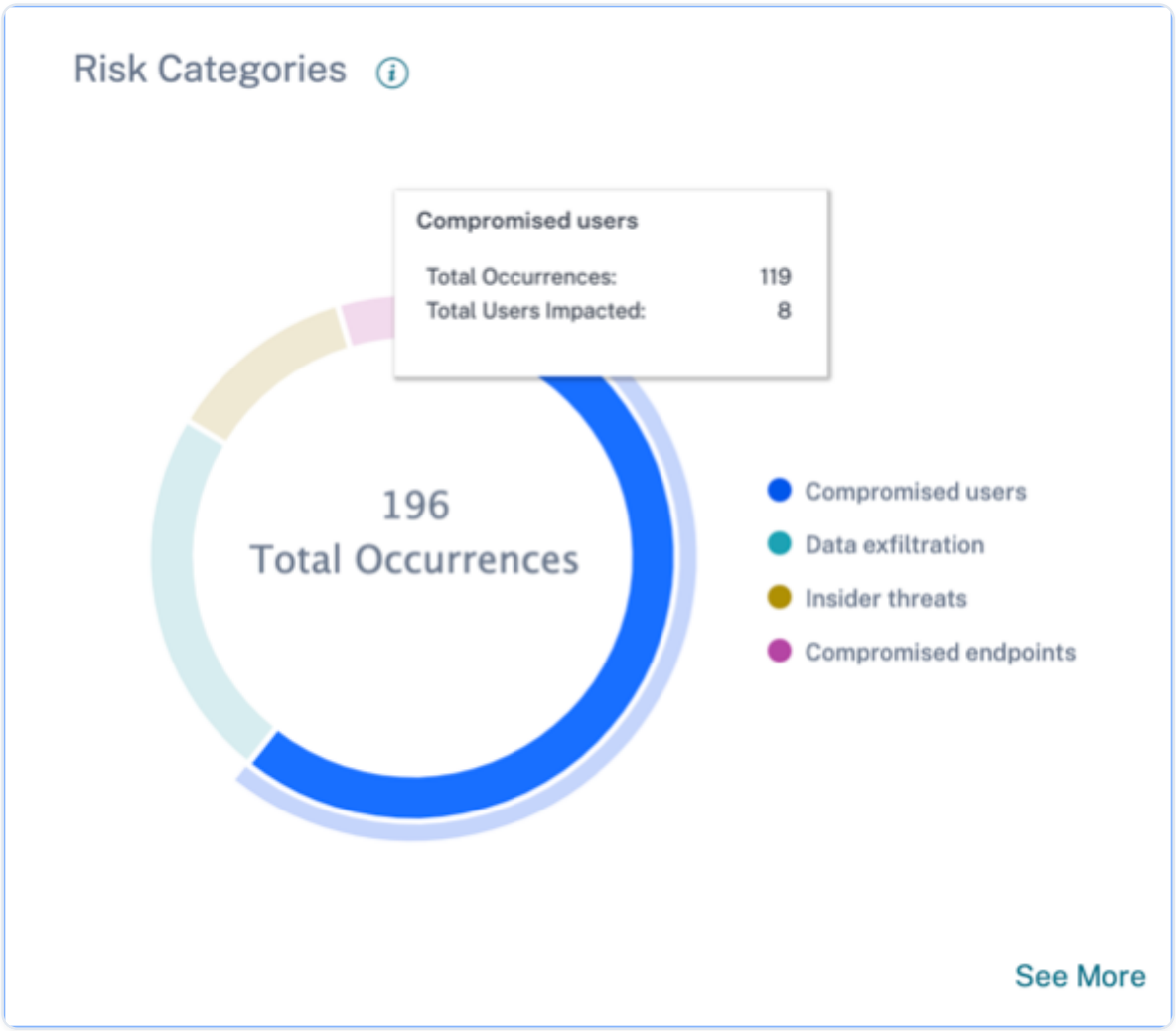
在**用户**仪表板和**用户**页面上，观察列表中的用户数量显示为过去 13 个月的数据，无论所选时间段如何。当您选择一个时间段时，风险指标出现次数会根据时间选择而变化。

了解更多：观察列表

风险类别

风险类别环形图按风险类别汇总了所选时间段内指标的出现次数。将鼠标悬停在每个图表段上会显示唯一用户计数，这反过来又链接到相应的**风险指标类别**概览页面。默认和自定义风险指标均支持风险分类。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

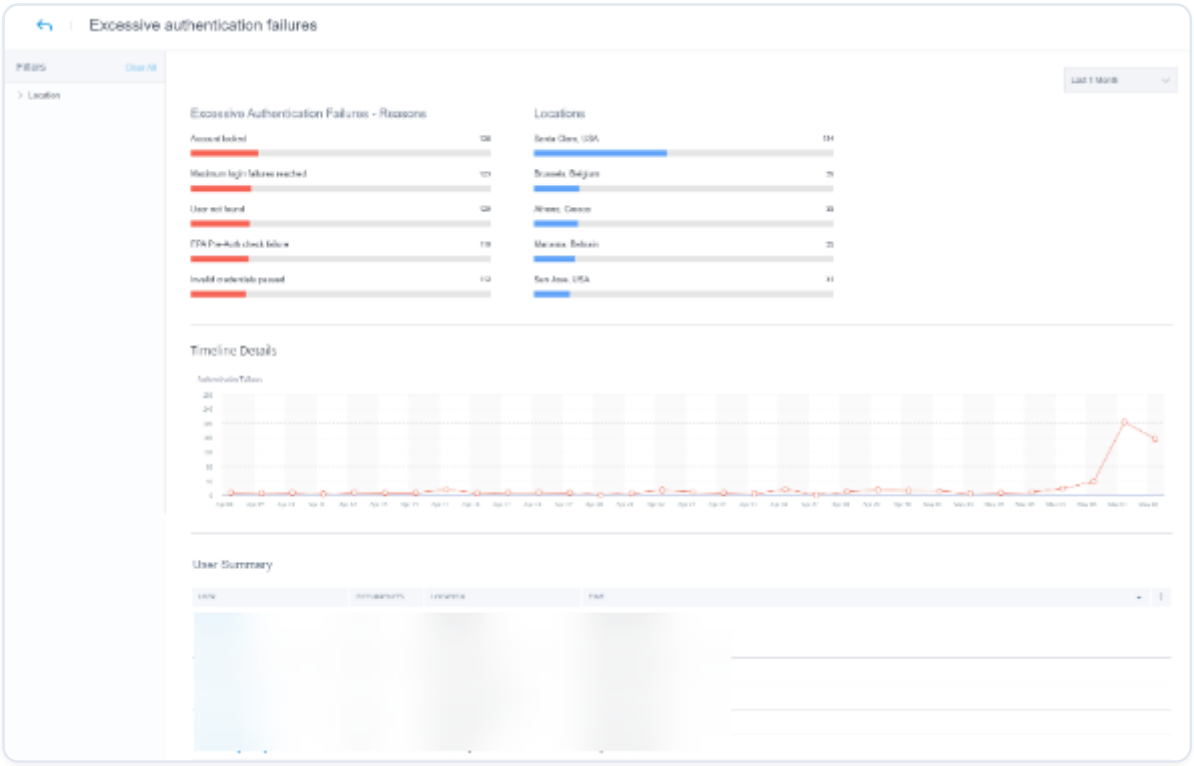


风险类别仪表板的目的是使 Citrix Virtual Apps and Desktops 和 Citrix DaaS 管理员能够管理用户风险，并与他们的安全同行进行简化讨论，而无需具备专家级的安全知识。它允许在组织层面实施安全强制执行，并且不限于安全管理员。

用例

假设您是 Citrix Virtual Apps and Desktops 管理员，负责管理组织中员工的应用程序访问权限。如果您转到“**风险类别**”>“**受损用户**”>“**身份验证失败过多 - Citrix Gateway**”风险指标部分，您可以评估您授予访问权限的员工是否已受损。如果您进一步导航，您可以获得有关此风险指标的更准确见解，例如失败原因、登录位置、时间线详细信息和用户摘要。如果您发现授予访问权限的用户与受损用户之间存在任何差异，您可以通知安全管理员。这种对安全管理员的及时通知有助于在组织层面强制执行安全。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



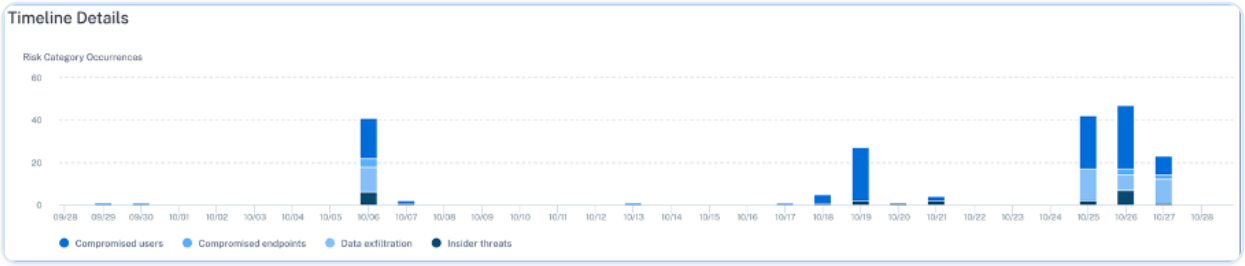
如何分析风险类别仪表板?

当您在“**风险类别**”仪表板上选择“**查看更多**”时，您将被重定向到总结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风险指标总发生次数。

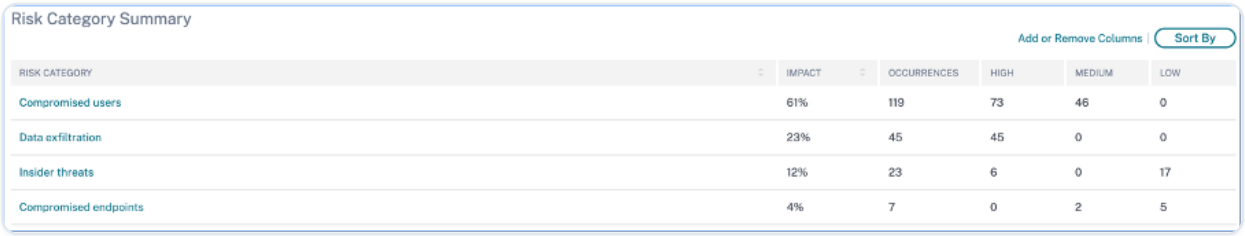


- **时间线详细信息**：提供在选定时间段内每个风险类别的风险指标总发生次数的图形表示。如果您导航到此部分的底部，您可以根据风险类别进行排序，以获取有关风险指标的更准确见解。



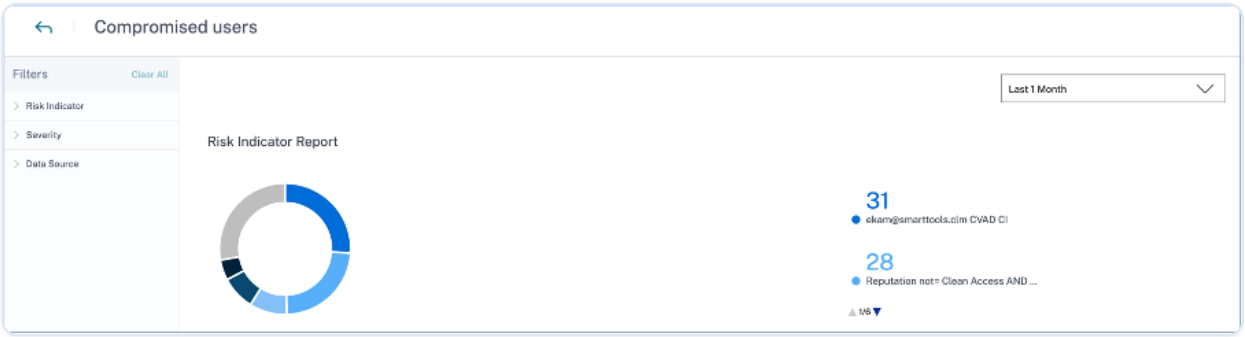
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **风险类别摘要**：本节提供与每个类别相关的风险指标的详细信息，例如影响、发生次数和严重性。选择任何风险类别以查看与该类别相关的风险指标的详细信息。例如，当您选择“**受损用户**”类别时，您将被重定向到“**受损用户**”页面。

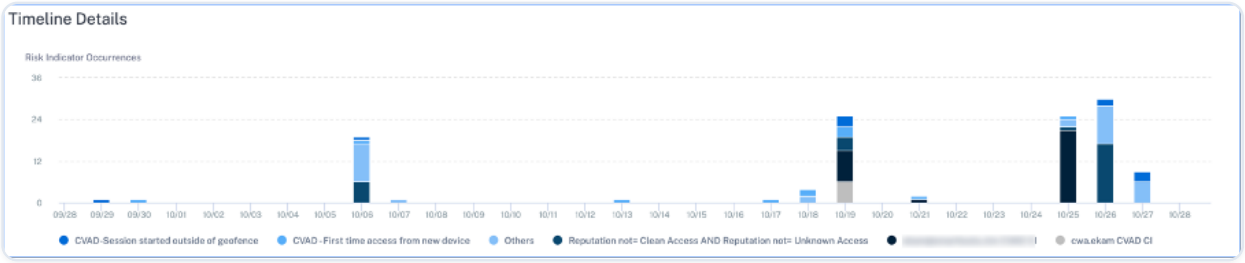


“**受损用户**”页面显示以下详细信息：

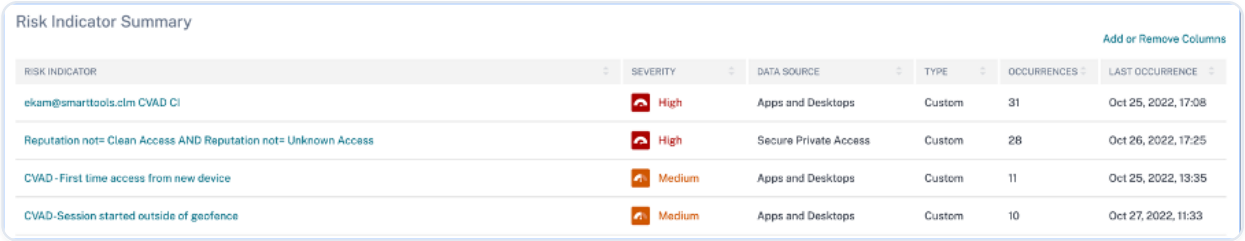
- **风险指标报告**：显示在选定时间段内属于受损用户类别的风险指标。它还显示在选定时间段内触发的风险指标的总发生次数。



- **时间线详细信息**：提供选定时间段内风险指标发生情况的图形表示。



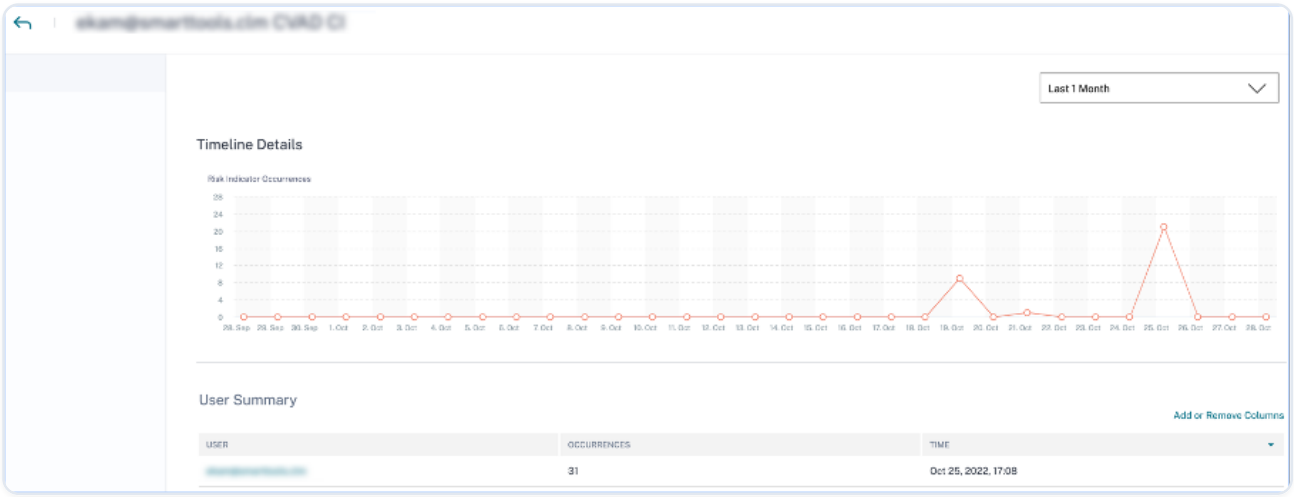
- **风险指标摘要**：显示在受损用户类别下生成的风险指标摘要。此部分还显示严重性、数据源、风险指标类型、发生次数和最后一次发生时间。



当您选择一个风险指标时，您将被重定向到汇总该指标详细信息的页面。例如，如果您选择**首次从新设备访问**风险指标，您将被重定向到汇总此指标详细信息的页面。摘要包括此事件发生的时间线

© 1997–2026 Citrix Systems, Inc. All rights reserved.

详细信息以及列出触发此风险指标的用户、风险指标发生次数和事件时间的的用户摘要。当您选择一个用户时，您将被重定向到该用户的风险时间线。



注意

Citrix Analytics 将默认风险指标归入相应的风险类别。对于自定义风险指标，您必须在**创建指标**页面上选择一个风险类别。有关详细信息，请参阅自定义风险指标。

风险类别类型

数据渗漏

此类别将由恶意软件或在组织中对设备执行未经授权的数据传输或数据盗窃的员工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渗漏活动，并通过主动对用户配置文件应用操作来缓解与此类别相关的风险。

数据渗漏风险类别包含以下风险指标：

数据源	用户风险指标
思杰虚拟应用和桌面和思杰 DaaS	潜在的数据泄露

内部威胁

此类别将组织内部员工触发的风险指标进行分组。由于员工对公司特定应用程序拥有更高级别的访问权限，因此组织面临更高的安全风险。风险活动可能是由恶意内部人员故意造成的，也可能是人为错误的结果。在任何一种情况下，对组织造成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配置文件应用操作来缓解与此类别相关的风险。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

内部威胁风险类别将以下风险指标分组在一起：

数据源	用户风险指标
思杰安全私有访问™	尝试访问列入黑名单的 URL
思杰安全私有访问	大量数据下载
思杰安全私有访问	有风险的网站访问
思杰安全私有访问	异常上传量

受损用户

此类别将用户显示异常行为模式（例如可疑登录和登录失败）的风险指标分组。另外，这些异常模式可能是用户帐户被盗用的结果。您可以深入了解在指定时间段内发生的所有受损用户事件，并通过主动对用户配置文件应用操作来缓解与此类别相关的风险。

受损用户风险类别将以下风险指标分组在一起：

数据源	用户风险指标
思杰网关	端点分析扫描失败
思杰网关	过多的身份验证失败
思杰网关	不可能旅行
思杰网关	从可疑 IP 登录
思杰网关	异常身份验证失败
Citrix 虚拟应用和桌面 和 Citrix 桌面即服务	可疑登录
Citrix 虚拟应用和桌面 和 Citrix 桌面即服务	不可能的行程
微软 Graph 安全	Azure AD 身份保护风险指标
微软 Graph 安全	适用于终结点的 Microsoft Defender 风险指标

受损端点

此类别将设备表现出可能表明存在入侵的不安全行为时触发的风险指标归类。

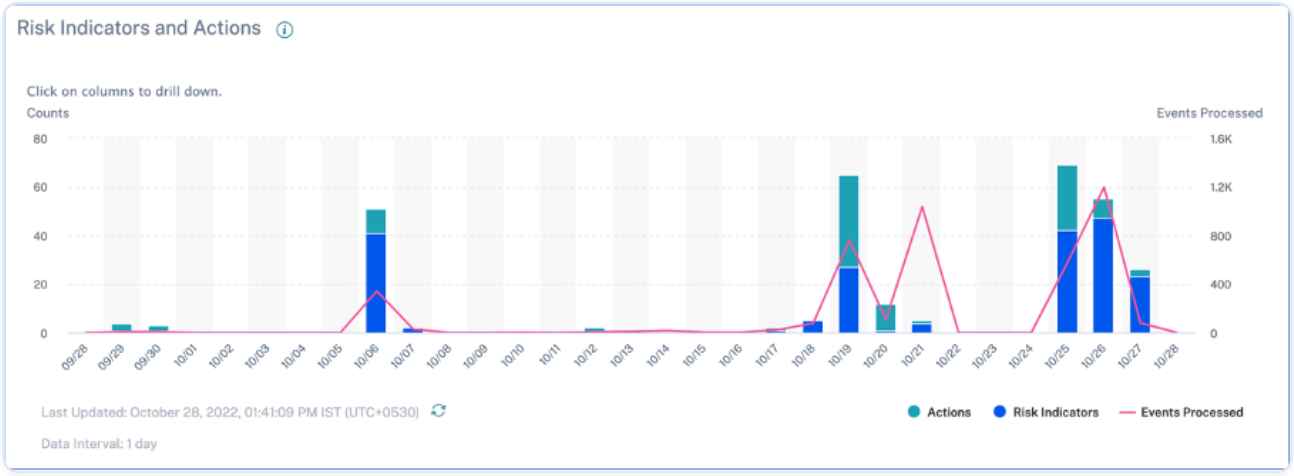
© 1997–2026 Citrix Systems, Inc. All rights reserved.

受损端点风险类别将以下风险指标归类在一起：

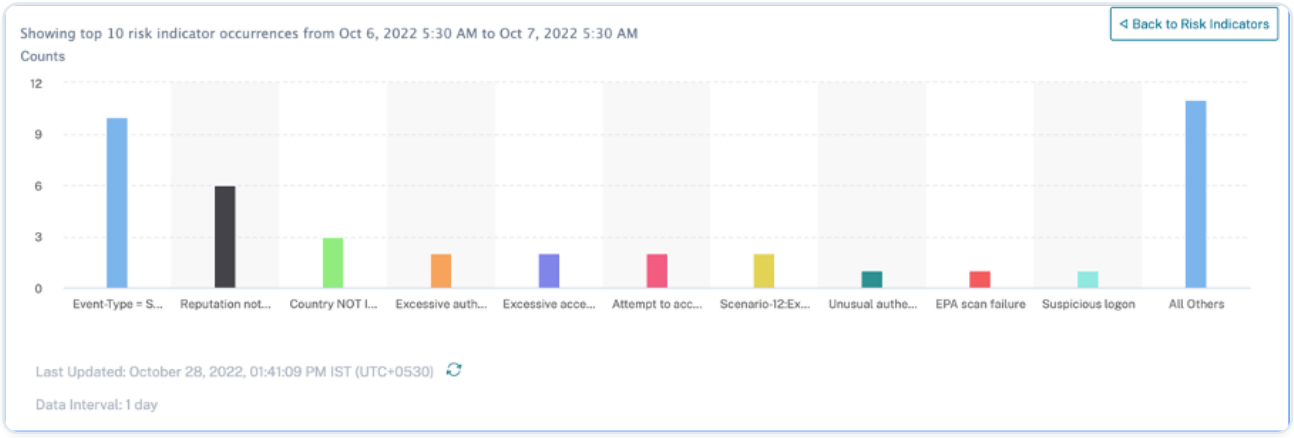
数据源	用户风险指标
思杰 端点管理™	检测到未受管设备
思杰端点管理	检测到越狱或已root的设备
思杰端点管理	检测到带有黑名单应用程序的设备

风险指标和操作

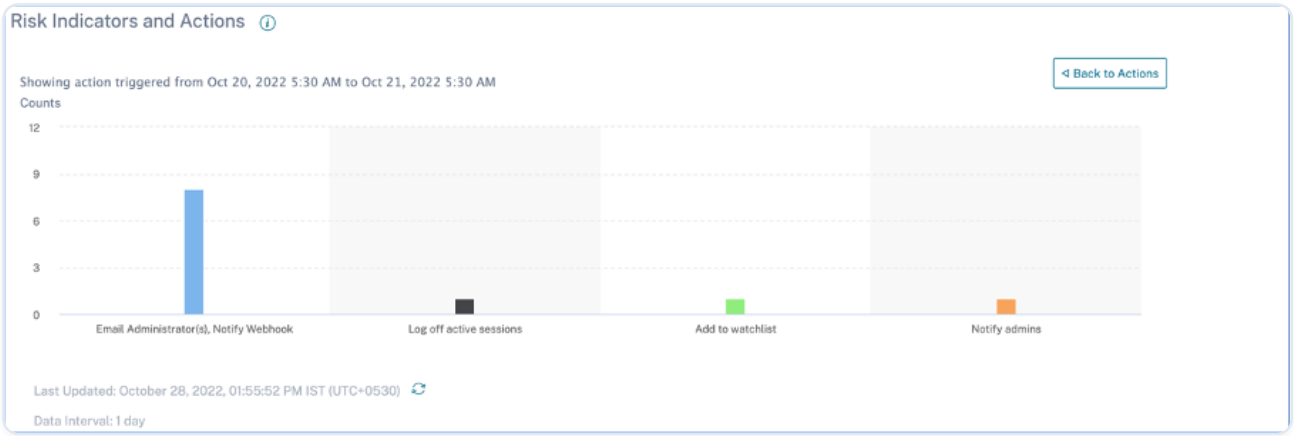
您可以查看所选时间段内为用户触发的风险指标和应用的操作。新的“**风险指标和操作**”条形图提供了指标、操作和事件随时间变化的详细计数，其中总体时间范围和条形间隔均来自所选时间段。



单击指标或操作的条形段会显示一个向下钻取的可视化，分别显示每个指标或操作的计数。



© 1997–2026 Citrix Systems, Inc. All rights reserved.



在指标向下钻取中，单击单个指标条会转到相应的风险指标页面，显示所选时间段的数据。

访问摘要

此控制板汇总了所选时间段内所有网关访问事件。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。

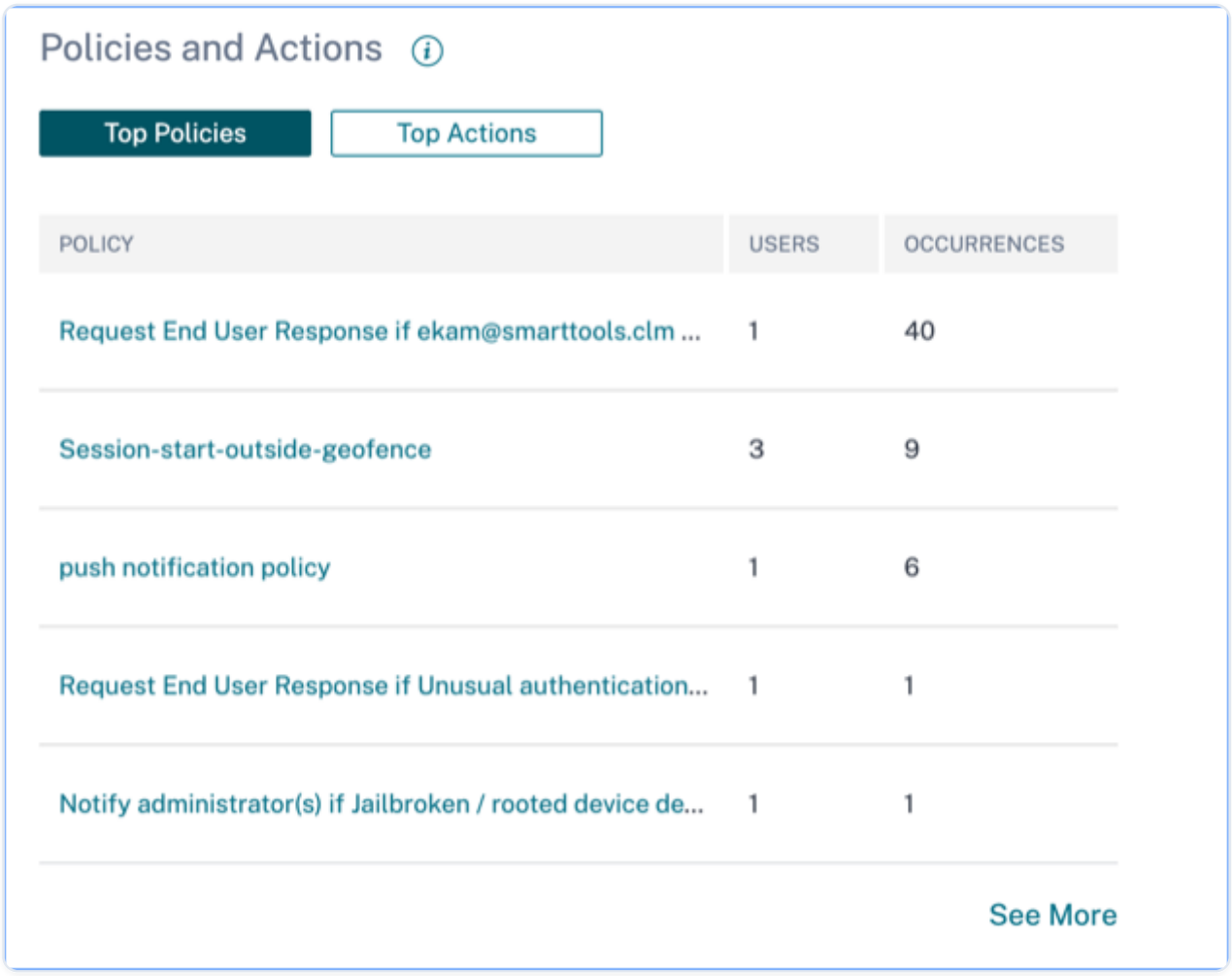
单击图表上的指针可查看 Gateway 自助搜索 页面。对于成功的登录场景，网关访问事件在该页面上按状态代码排序。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

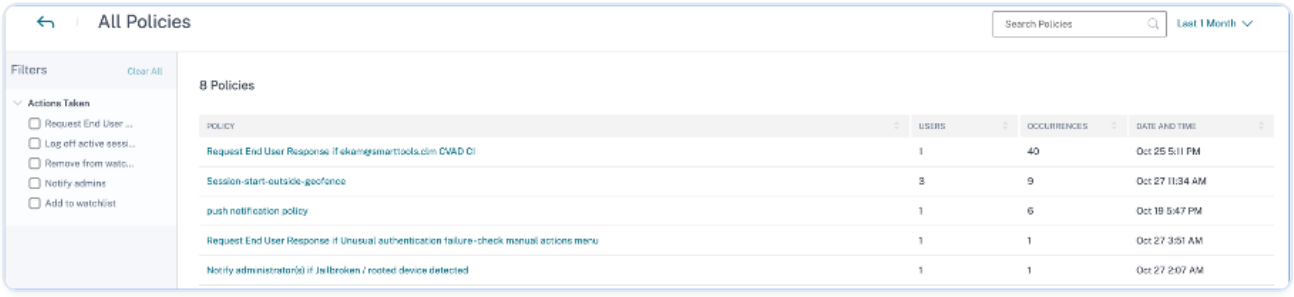
策略和操作

显示在选定时间段内应用于用户配置文件的前五项策略和操作。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。



热门策略

前五项已配置策略是根据出现次数确定的。当您位于仪表板的“**热门策略**”部分并选择“**查看更多**”时，您将被重定向到“**所有策略**”页面。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

所有策略

此页面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，您将被重定向到策略自助搜索页面。在左侧窗格中，您可以根据应用的操作进行筛选。

当您选择用户名时，您将被重定向到风险时间线。基于策略的操作将添加到用户的风险时间线中。当您选择该操作时，其详细信息将显示在风险时间线的右侧窗格中。

热门操作

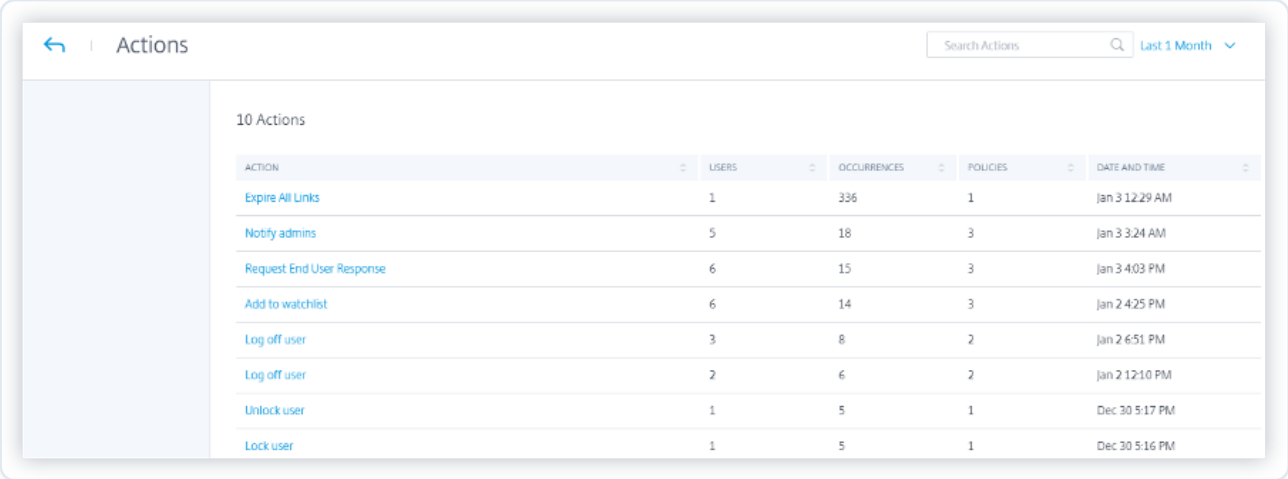
与应用于用户配置文件的策略相关联的前五项操作。本节不显示您手动应用于用户配置文件的操作。热门操作是根据出现次数确定的。

单击“**查看更多**”可在“**操作**”页面上查看所有基于策略的操作。

操作

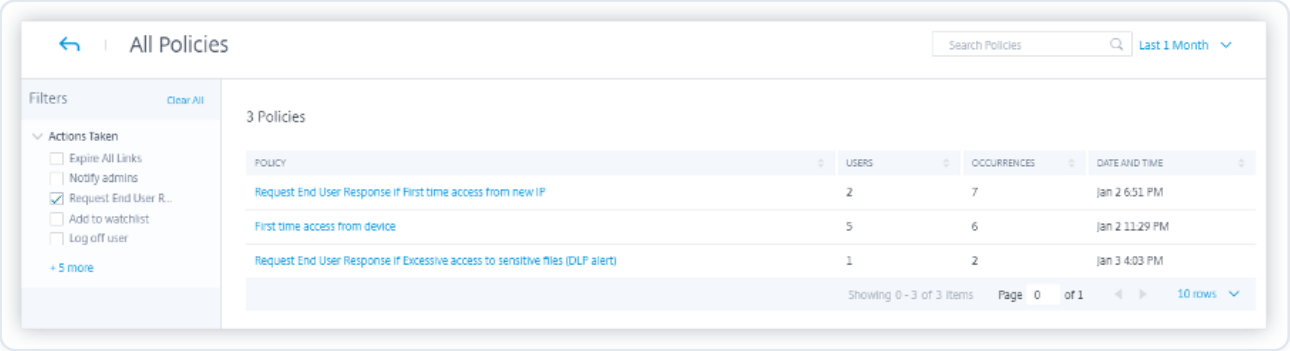
此页面提供在选定时间段内已应用于您的用户的所有基于策略的操作列表。您可以查看以下信息：

- 根据策略应用的操作名称
- 应用了该操作的用户数量
- 该操作的发生次数
- 与该操作关联的策略数量
- 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**”页面将显示与“**请求最终用户响应**”操作关联的所有策略。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在“**所有策略**”页面上，单击某个策略以查看已应用该操作的用户事件。

风险指标

总结了选定时间段内的前五名风险指标。风险指标可以是默认的或自定义的。对于默认风险指标，Citrix Analytics 从已发现的数据源收集数据，并对这些数据源启用了数据处理。

对于自定义风险指标，Citrix Analytics 根据生成的风险事件从以下数据源收集数据：

- Citrix 网关
- Citrix 安全私有访问
- Citrix 虚拟应用和桌面™
- Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）

在**风险指标**面板上，您可以查看前五个风险指标，并根据总出现次数或严重性对其进行排序。

风险指标面板(/en-us/citrix-analytics/media/risk-indicators-pane.png)

在**风险指标**面板上点击**查看更多**，以查看**风险指标概览**页面。

风险指标概览(/en-us/citrix-analytics/media/risk-indicator-overview.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

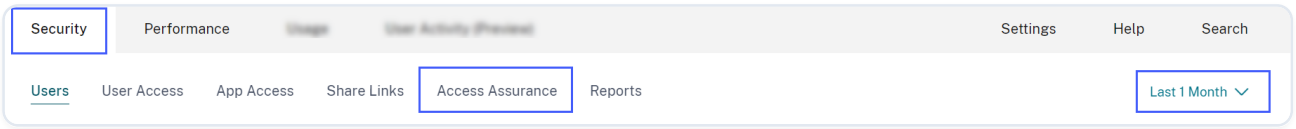
访问保障仪表板

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从其常用且安全的位置访问 Citrix Virtual Apps and Desktops 或 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）。如果任何用户从未知位置或新位置登录，您可以验证其登录详细信息并采取必要措施，以减轻对 Citrix IT 环境的任何威胁。

访问保障仪表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。

查看仪表板

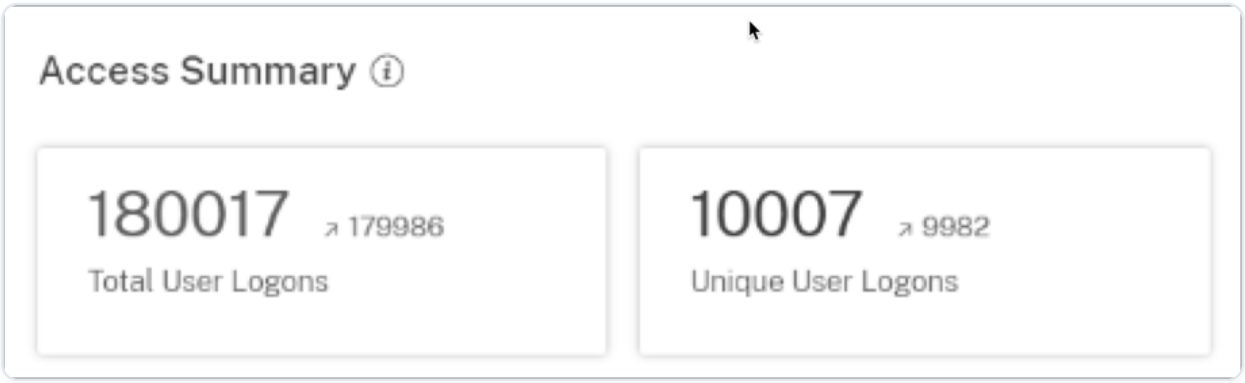
要查看仪表板，请单击 **安全 > 访问保障**。选择要查看登录详细信息的时间段。



访问摘要

仪表板的摘要部分提供所选时间段的以下信息：

1. 所有位置（全球）的用户登录总数。
2. 所有位置（全球）的唯一用户登录总数。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

登录位置

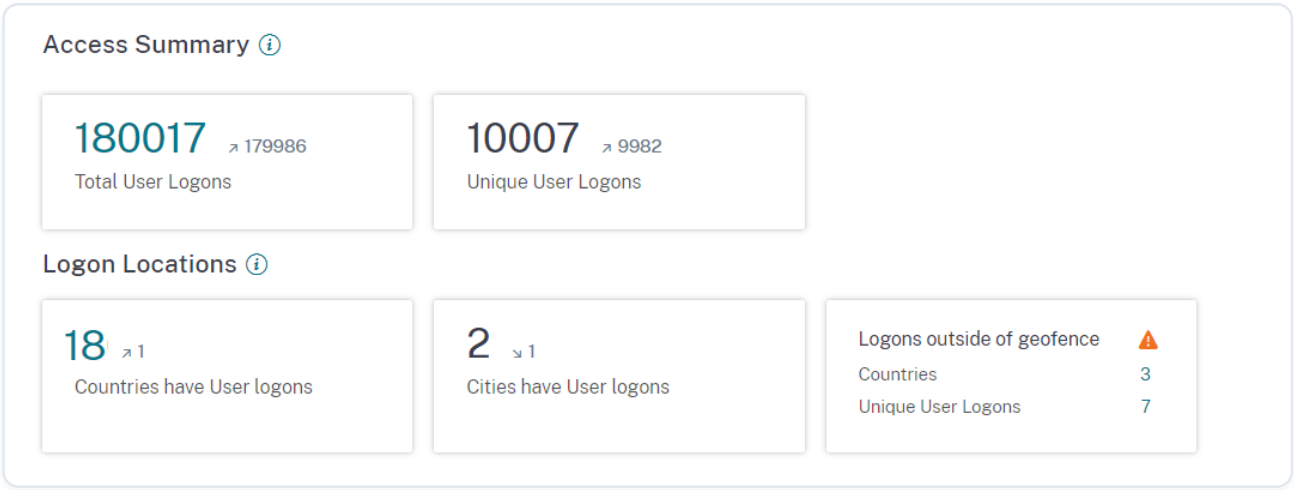
登录位置部分提供所选时间段的以下信息：

- 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总数和唯一用户登录数。要查看地理围栏区域的登录详细信息，请启用地理围栏。
- 唯一用户登录数排名前 10 的位置。有时，排名前列的唯一用户登录也来自未知城市和国家/地区，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。要了解某些位置未识别的原因，请参阅未识别的位置。

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。对于排名前 10 的位置，“**偏差**”列显示每个位置的用户登录变化（正 (+) 或负 (-)）。此比较基于选定的时间段和长度相等的上一个时间段。例如，如果您选择时间段“**上个月**”，则用户登录趋势和偏差将与上个月和上上个月进行比较。

注意

位置信息在城市和国家/地区级别提供，不代表精确的地理位置。有关访问保障、地理位置的更多详细信息，请参阅常见问题解答。

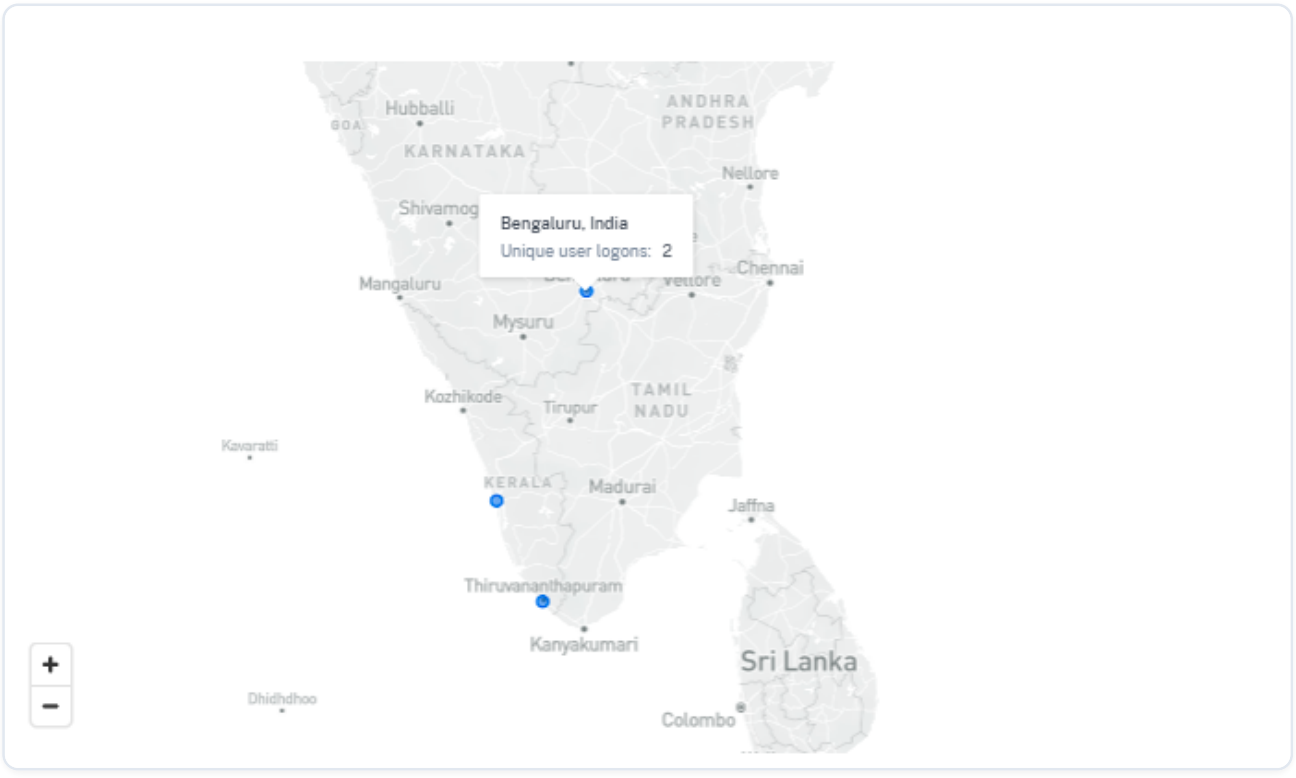


在“**前 10 个唯一登录位置**”表中，选择一个位置以查看用户及其访问配置文件和登录详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

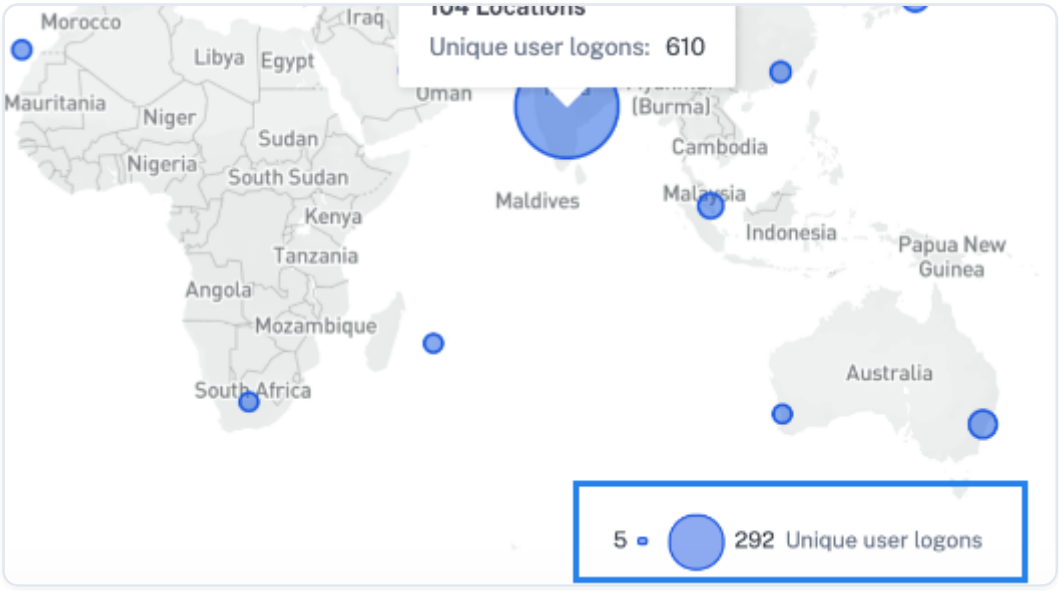


地图显示了选定时间段内来自不同位置的唯一用户数量。将鼠标悬停在蓝色气泡上或放大到某个位置，以查看该位置的唯一用户登录总数。单击蓝色气泡可查看某个位置的访问详细信息。



在地图的右下角，您可以查看唯一用户登录的范围。对于选定的时间段，小气泡表示所有位置中唯一用户登录的最小数量。大气泡表示所有位置中唯一用户登录的最大数量。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

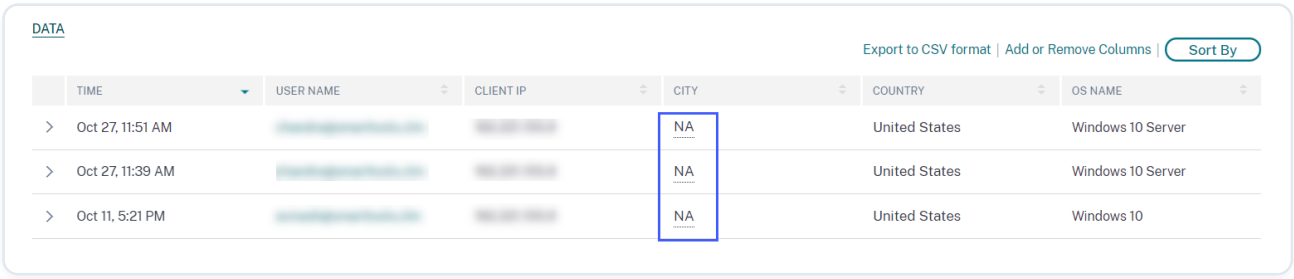


未识别的位置

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，如果任何国家/地区或城市信息不可用，“**数据**”表将显示“**NA**”标签。

将鼠标悬停在 **NA** 标签上，以查看位置信息不可用的原因。



您可能会看到以下导致位置不可用的情况之一：

场景	原因
城市名称和国家/地区名称不可用。	以下情况之一：
	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。

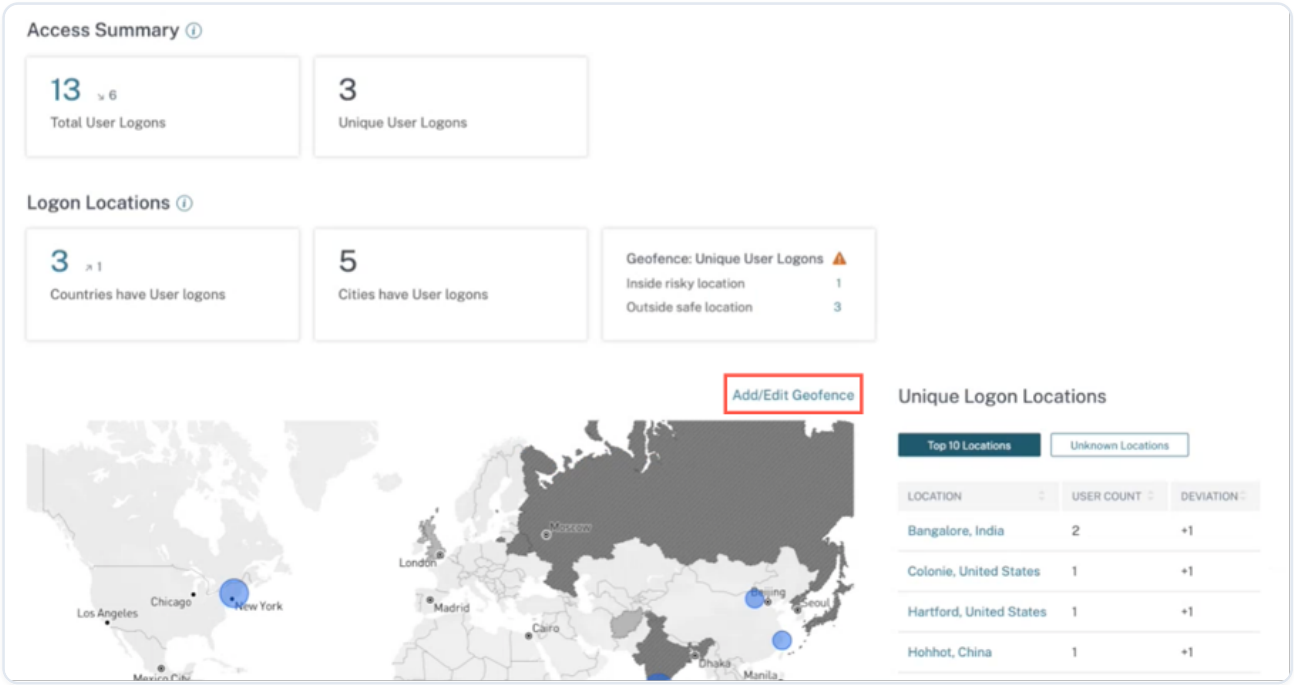
© 1997–2026 Citrix Systems, Inc. All rights reserved.

场景	原因
	1. 用户的网络公共 IP 地址不可用，因此 Citrix Analytics 无法找到位置。
	1. 外部地理位置服务无法将位置信息发送到 Citrix Analytics。
具有私有 IP 的位置	用户的设备位于专用网络中。在这种情况下，Citrix Analytics 无法获取位置信息。
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混淆。因此，Citrix Analytics 无法获取位置信息。

启用地理围栏

地理围栏有助于识别从安全地理围栏外部和危险地理围栏区域内部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**始终处于开启状态。要配置地理围栏，请单击**添加/编辑地理围栏**。

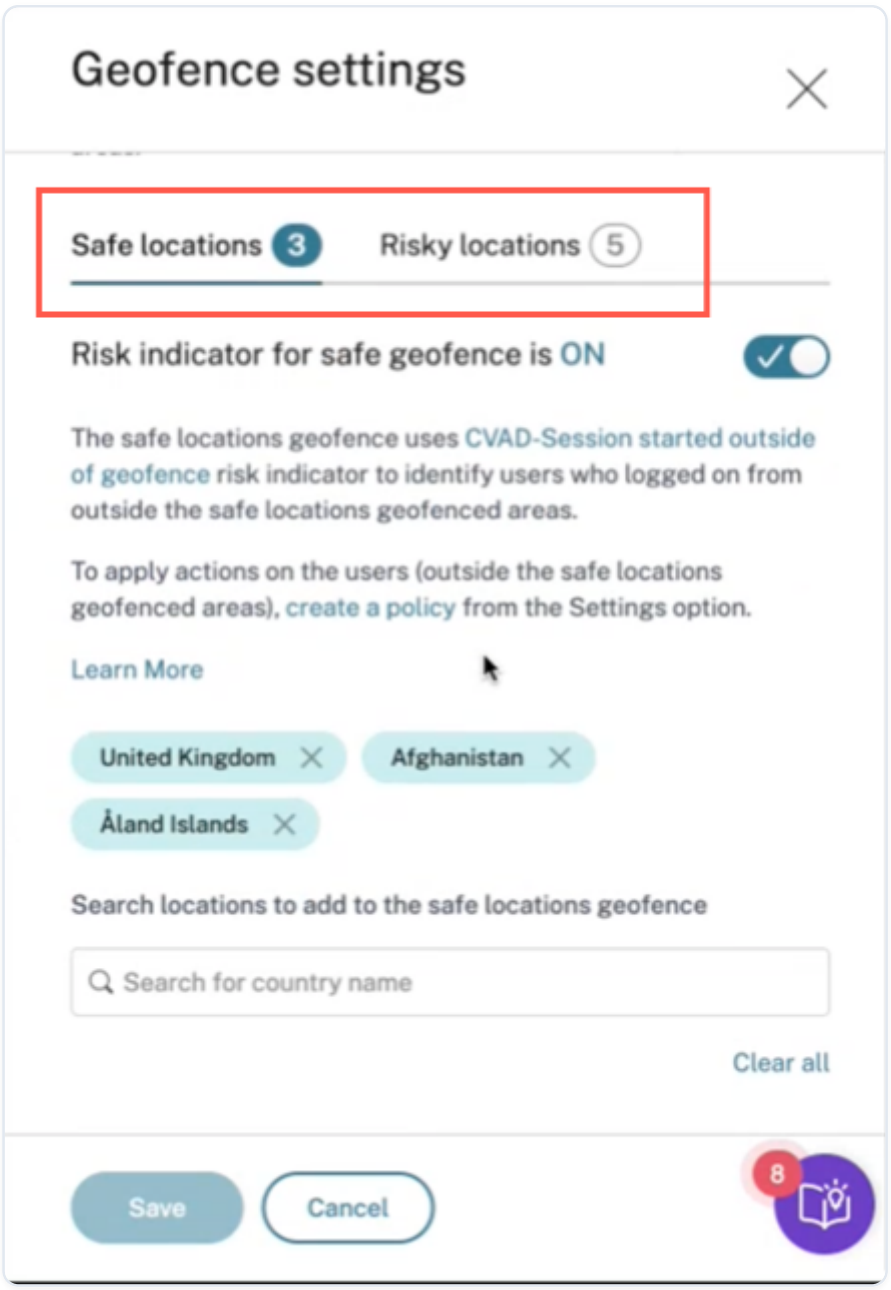


地理围栏设置窗口显示两个选项卡：

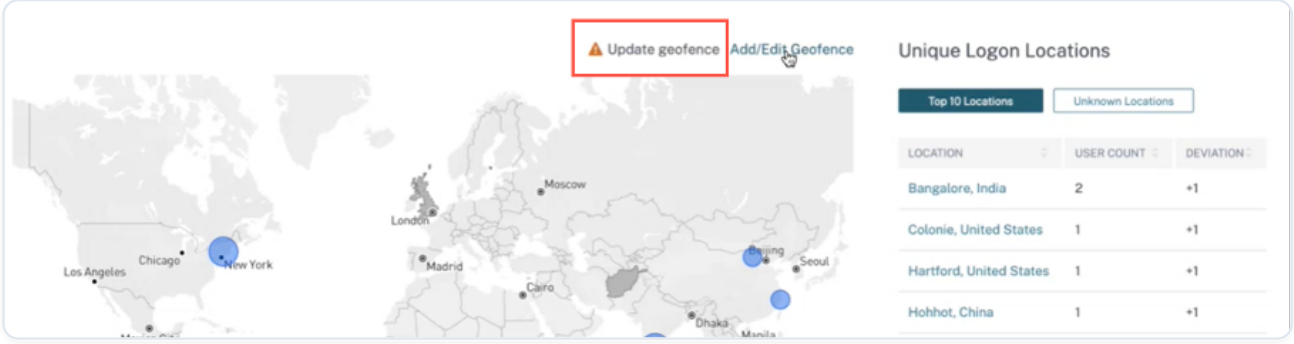
- **安全位置**：您可以配置或删除属于安全位置的国家/地区。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **危险位置**：您可以配置或删除属于危险位置的国家/地区。 您还可以查看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危险位置地理围栏中删除或移除某个国家/地区，请单击该国家/地区旁边的关闭 (X) 符号。单击**保存**以保存地理围栏设置。

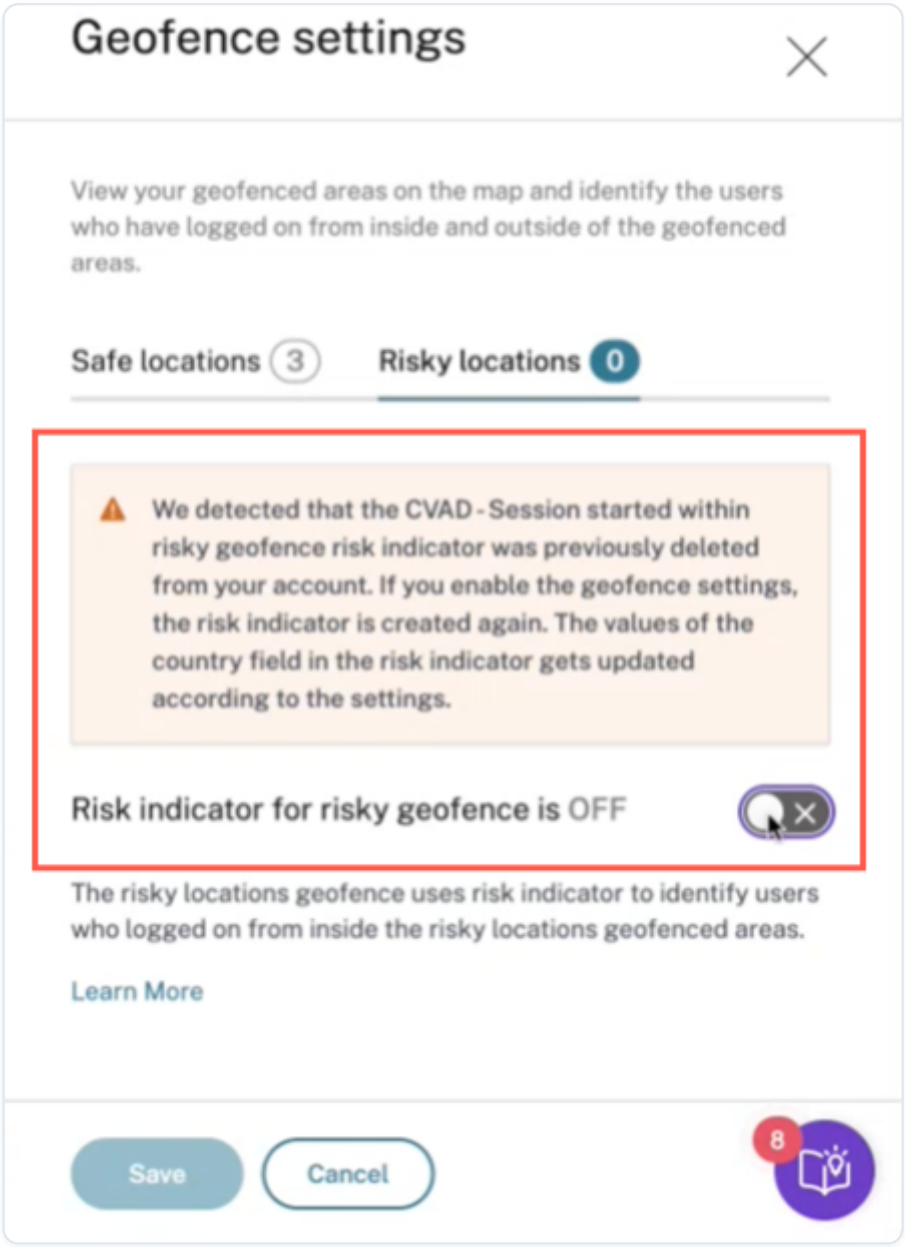


您可以配置属于危险位置地理围栏的国家/地区。如果未添加危险位置地理围栏的风险指示器或风险指示器已被删除，您将在**添加/编辑地理围栏**旁边看到**更新地理围栏**警告消息。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

要重新创建指示器，请导航到**危险位置**选项卡并打开**危险地理围栏的风险指示器**开关。

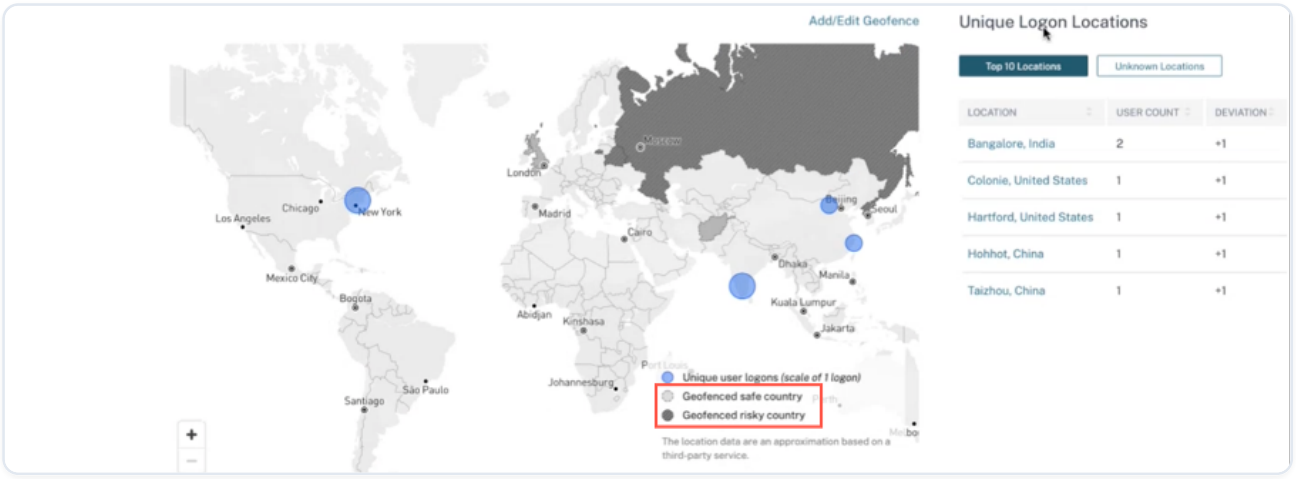


指示器是使用危险位置的默认列表创建的。

访问摘要页面还会显示地理围栏的安全和危险国家/地区。

- 地理围栏安全国家/地区用浅灰色圆圈标记。
- 地理围栏危险国家/地区用深灰色圆圈标记。

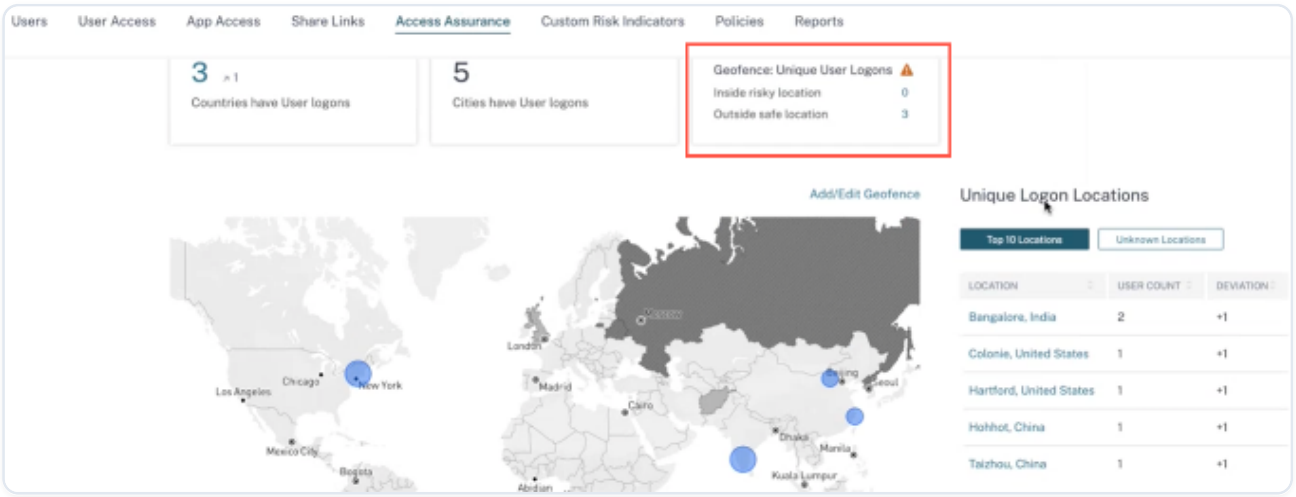
© 1997–2026 Citrix Systems, Inc. All rights reserved.



地理围栏：唯一用户登录

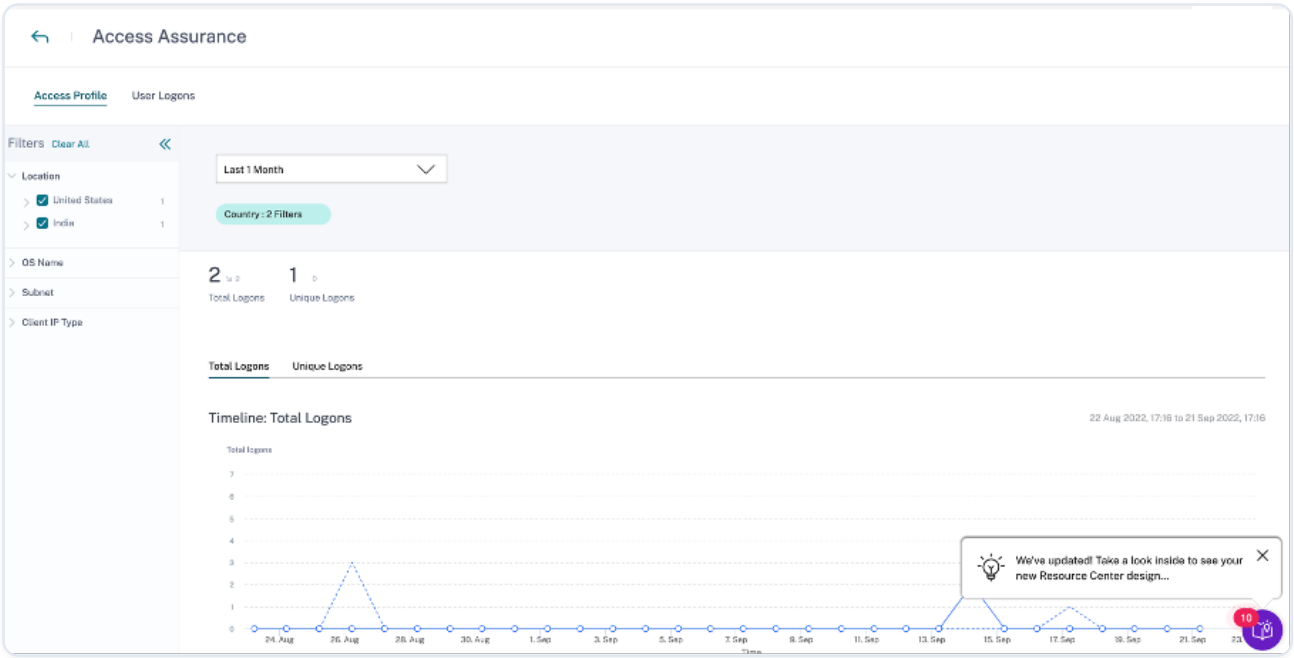
导航到“访问摘要”页面以查看“地理围栏：唯一用户登录”。该卡片显示了“危险区域内”和“安全区域外”的数量。

- **危险区域内**：识别从地理围栏的危险区域内登录的用户。
- **安全区域外**：识别从地理围栏的安全区域外登录的用户。



要查看总用户登录和唯一用户登录的详细摘要，请单击“危险区域内”或“安全区域外”旁边的数字。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



此功能使用以下预配置的自定义风险指示器：

- **CVAD-会话在地理围栏外启动**：用于监控安全地理围栏外的用户登录。
- **CVAD-会话在危险地理围栏内启动**：用于监控危险地理围栏内的用户登录。

如果检测到任何用户登录发生在地理围栏之外，则会触发风险指示器，并将“会话在地理围栏外启动”策略应用于这些用户。该策略会触发“*请求最终用户响应*”操作，并根据用户的响应，您可以采取适当的措施来防止任何可疑登录带来的威胁。有关更多信息，请参阅预配置的自定义风险指示器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

- 在**地理围栏设置**中，当您修改国家/地区时，*CVAD-会话在地理围栏外启动*风险指示器也会随之更新。
- 例如，如果您选择并保存澳大利亚和印度作为新的地理围栏国家/地区，则风险指示器的预配置条件将更新为这些新国家/地区，并保留美国（默认地理围栏）。您还可以删除默认的地理围栏国家/地区美国。

  风险指标的预配置条件：`Event-Type = \"Session.logon\" AND Country != \"\" AND Country ~ \"\" AND Country != \"United States\"`

  更新**地理围栏设置**后，风险指标的条件：

  `Event-Type = \"Session.logon\" AND Country != \"\" AND Country ~ \"\" AND Country NOT IN (\"Australia\", \"United States\", \"India\"`
- 如果 *CVAD 会话在地理围栏外启动* 风险指标之前已从您的帐户中删除，则启用**地理围栏设置**会再次创建该风险指标。风险指标的地理围栏国家/地区由**地理围栏设置**控制。

启用**地理围栏设置**后，地图会显示地理围栏区域以及来自这些区域的唯一用户登录。

登录网络

在访问保障控制板中，您现在可以查看以下其他用户详细信息：

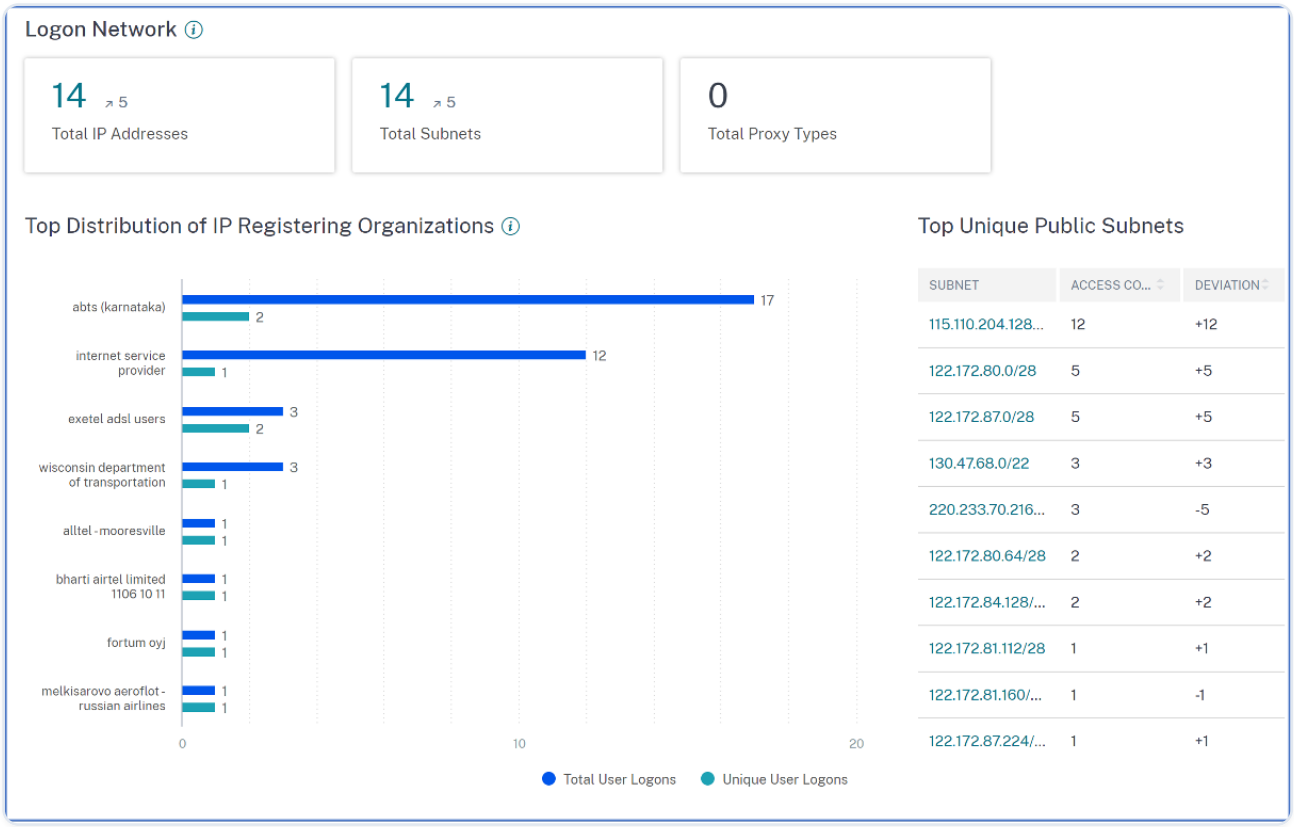
- 与用户登录所用的 IP 地址关联的组织。这些组织包括企业、政府、教育实体和互联网服务提供商等。
- 用户登录所用的总唯一公共子网和专用子网。
- 用户使用代理和专用 VPN 服务登录的详细信息。

作为管理员，您可以使用这些附加详细信息来验证用户登录详细信息，并确保用户登录符合组织的安全预期。

查看用户网络详细信息

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

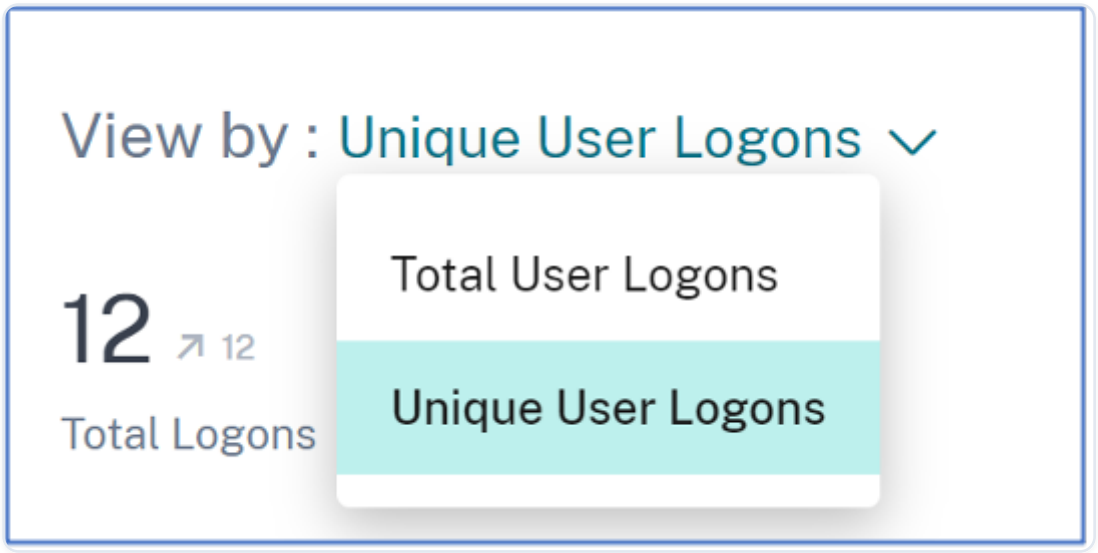


- **总 IP 地址**：指示用于登录虚拟会话的唯一 IP 地址总数。
- **总子网数**：表示用于登录虚拟会话的子网总数。
- **总代理类型**：表示服务器用于代理用户连接的网络或协议的总类型。
- 在“**IP 注册组织分布概览**”下，您可以查看每个组织 (ISP) 的总用户登录和唯一登录详细信息的概览。您可以单击图表以深入查看与所选组织关联的用户详细信息、其访问配置文件和登录详细信息。
- 在“**唯一公共子网总数**”下，您可以查看子网概览、每个子网的总用户登录数以及每个子网的偏差趋势。您可以单击每个子网以深入查看与所选子网关联的用户详细信息、其访问配置文件和登录详细信息。

查看用户的访问配置文件

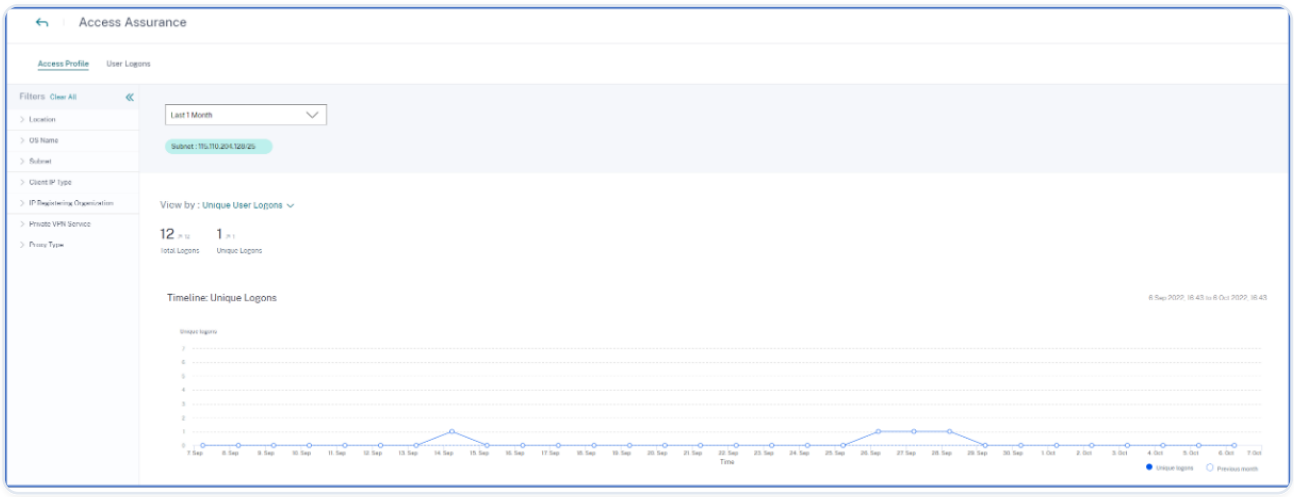
当您深入查看任何指标（位置、组织或子网）时，“**访问配置文件**”页面会提供您的用户从所选位置访问虚拟应用程序或虚拟桌面的摘要。您可以选择唯一登录或总登录选项，以查看所选时期的趋势分析。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以查看所选指标（位置、组织或子网）的顶级访问事件。此信息可帮助您查看访问模式以及用于威胁调查和分析的详细信息。

总用户登录和唯一用户登录的上升或下降趋势是根据所选时间段和长度相等的上一个时间段进行比较的。例如，如果您选择的时间段为**上个月**，则趋势将与上个月和上上个月进行比较。



分面

您可以对访问事件使用以下分面：

- **位置** - 按国家/地区及其城市筛选访问事件。
- **操作系统** - 按操作系统及其版本筛选访问事件。
- **子网** - 按子网筛选访问事件。
- **客户端 IP 类型**- 按公共或私有筛选访问事件。
- **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。

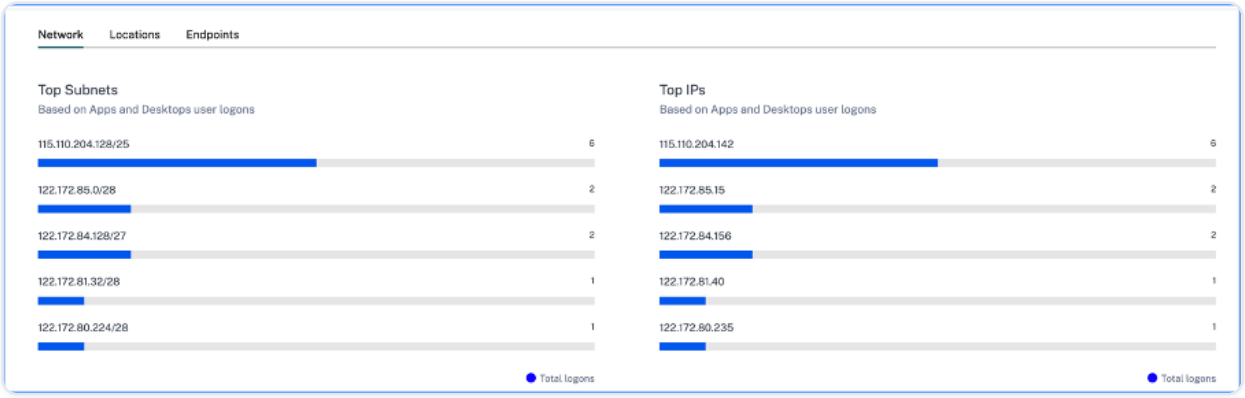
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

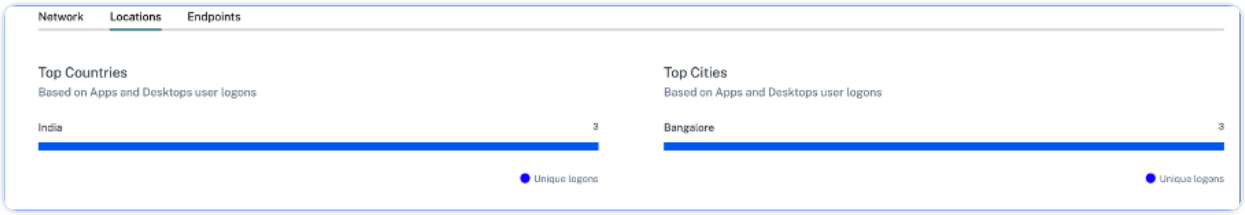
如果数据不可用或未识别，您可能还会看到“不可用”标签。

根据应用的筛选器，查看以下信息以了解总用户登录和唯一用户登录：

- **网络**- 用户登录到虚拟应用程序或虚拟桌面的热门子网和 IP 地址。



- **位置**- 用户登录到虚拟应用程序或虚拟桌面的热门国家/地区和城市。



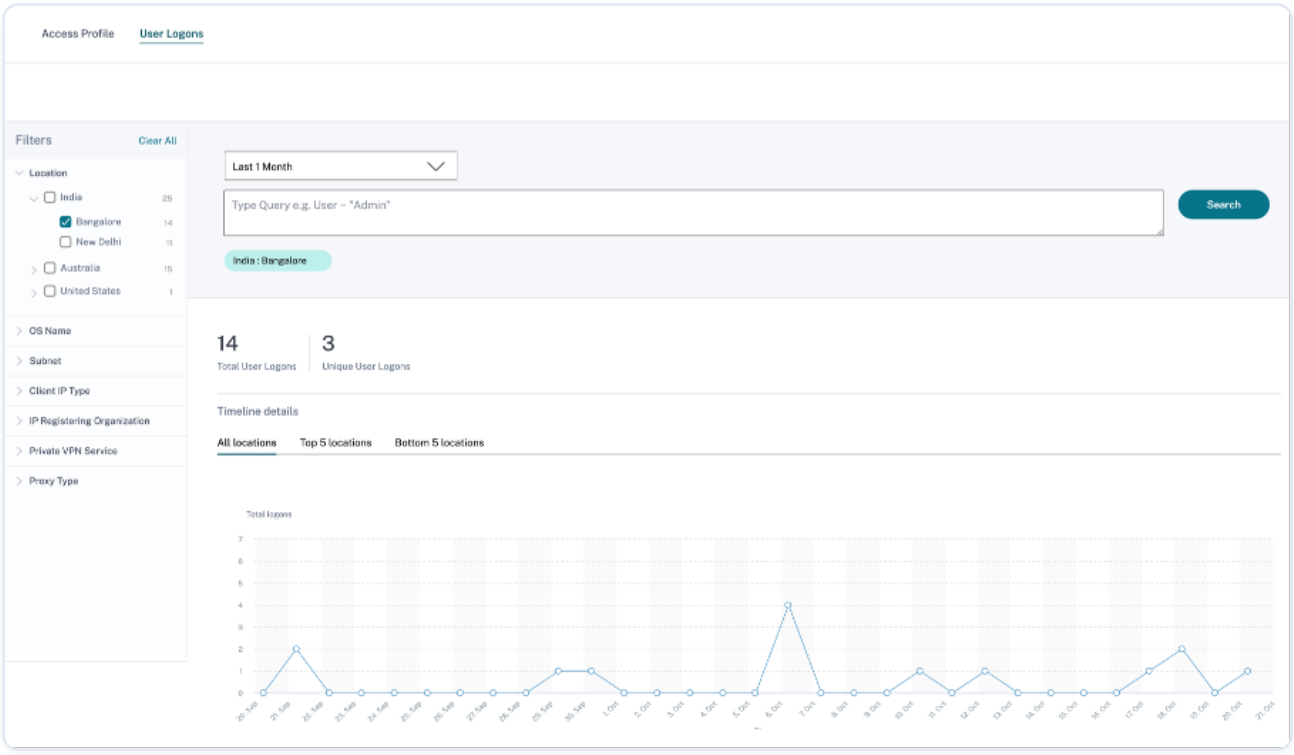
- **端点**- 根据应用程序和桌面用户登录情况排名前列的设备和操作系统名称。



查看用户登录详细信息

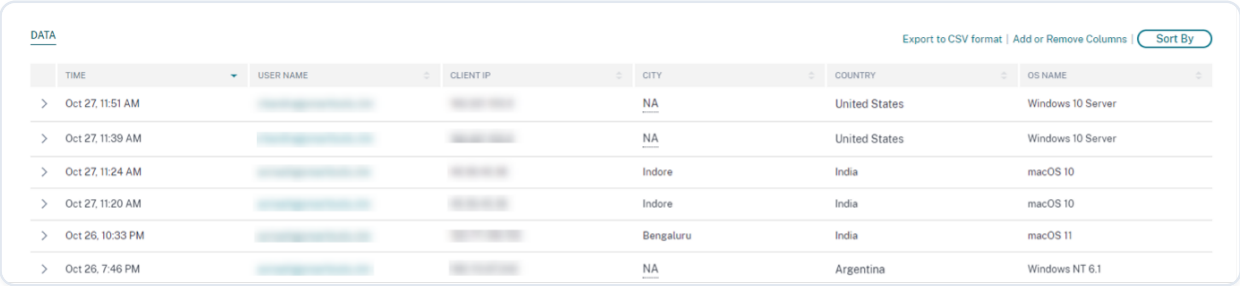
用户登录页面提供了用户从选定位置登录到虚拟应用程序或虚拟桌面的详细信息。此信息有助于您进行威胁调查和分析。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



数据表显示了所选位置和时间段的以下登录详细信息：

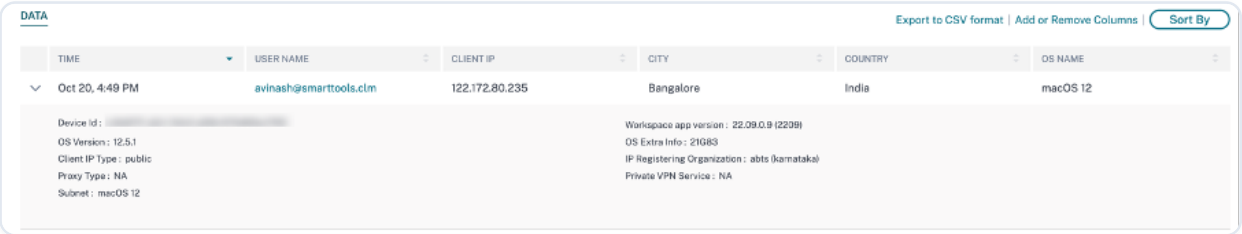
- **时间**。用户登录的日期和时间。
- **用户名**。用户的身份。
- **客户端 IP**。用户设备的 IP 地址。
- **客户端 IP 类型**。用户的 IP 地址类型，例如公共或私有。
- **城市和国家/地区**。用户登录虚拟应用或虚拟桌面的位置。
- **设备 ID**。用户设备的身份代码。
- **操作系统名称**。用户设备上的操作系统。有关详细信息，请参阅应用和桌面自助服务搜索。



如果展开每个事件，您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，请参阅应用和桌面自助服务搜索。
- **操作系统附加信息**- 操作系统的任何附加信息，例如内部版本号、Service Pack 和补丁。有关详细信息，请参阅应用和桌面自助服务搜索。
- **Workspace 应用程序版本**。Citrix Workspace™ 应用程序或 Citrix Receiver 的内部版本。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在**数据**表中，您可以执行以下操作：

- 单击**添加或删除列**以根据您希望查看数据的方式更新表列。
- 单击**排序依据**并选择数据元素以执行多列排序。有关更多信息，请参阅多列排序。
- 单击**导出为 CSV 格式**可将数据显示在数据表中的数据下载到 CSV 文件中，并用于您的分析。

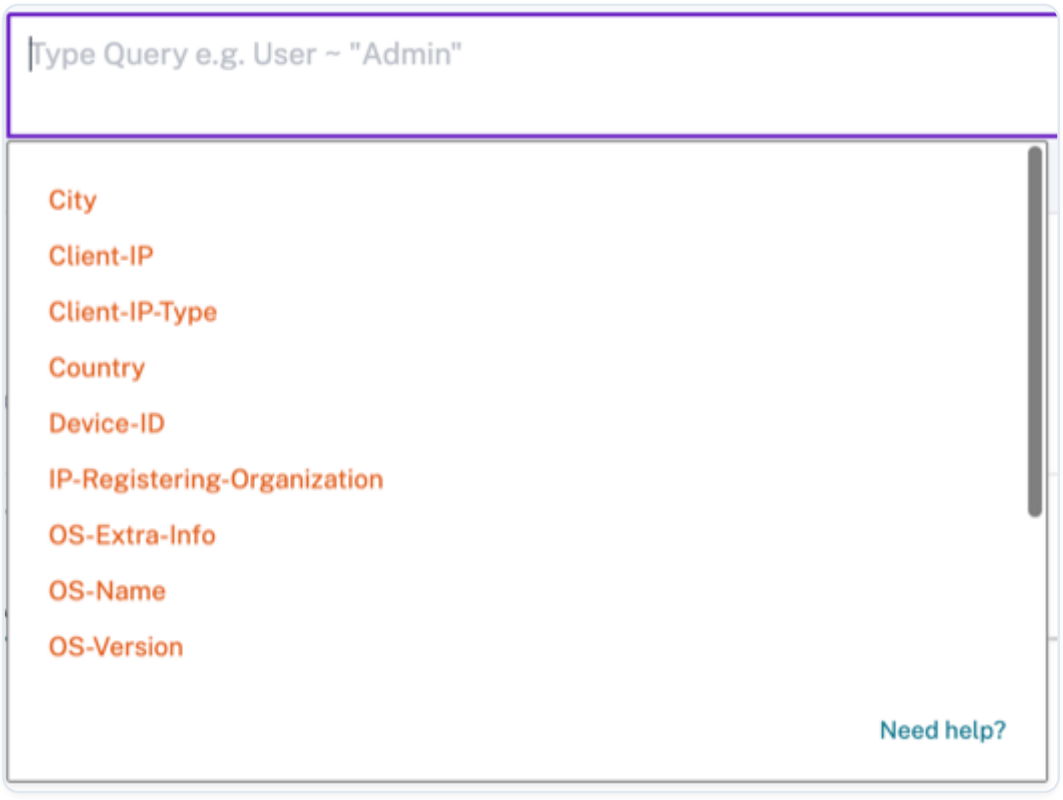
搜索栏

您还可以使用搜索栏，通过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
```



© 1997–2026 Citrix Systems, Inc. All rights reserved.

筛选条件

您可以对登录事件使用以下筛选条件：

- **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筛选登录事件。
- **子网**- 按子网筛选访问事件。
- **客户端 IP 类型**- 按公共和私有 IP 类型筛选访问事件。
- **IP 注册组织**- 按用户使用的 ISP 筛选访问事件。
- **私有 VPN 服务**- 按私有 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

如果数据不可用或无法识别，您可能还会看到“不可用”标签。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

用户风险时间线和配置文件

注意

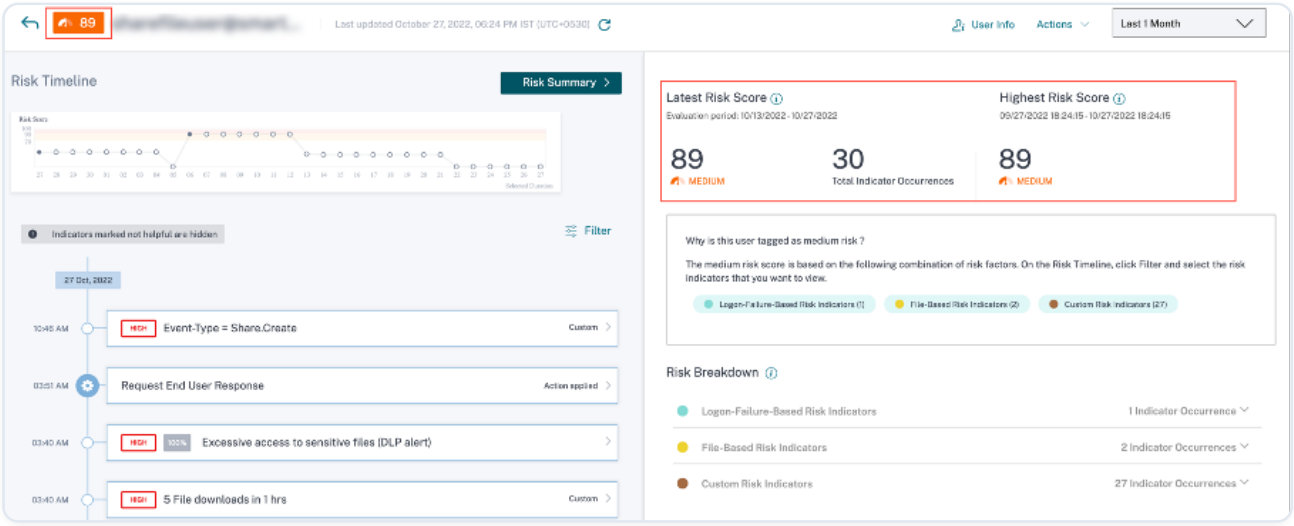
注意：Citrix Content Collaboration™ 和 ShareFile 已达到其生命周期终止，不再对用户可用。

用户配置文件上的用户风险时间线使您作为 Citrix Analytics 管理员能够更深入地了解用户的风险行为。默认情况下，用户风险时间线显示过去一个月的数据。您还可以查看在选定时间段内对其帐户执行的相应操作。通过用户风险时间线，您可以深入了解用户的配置文件，以了解以下内容：

- 应用程序使用情况
- 数据使用情况
- 设备使用情况
- 位置使用情况

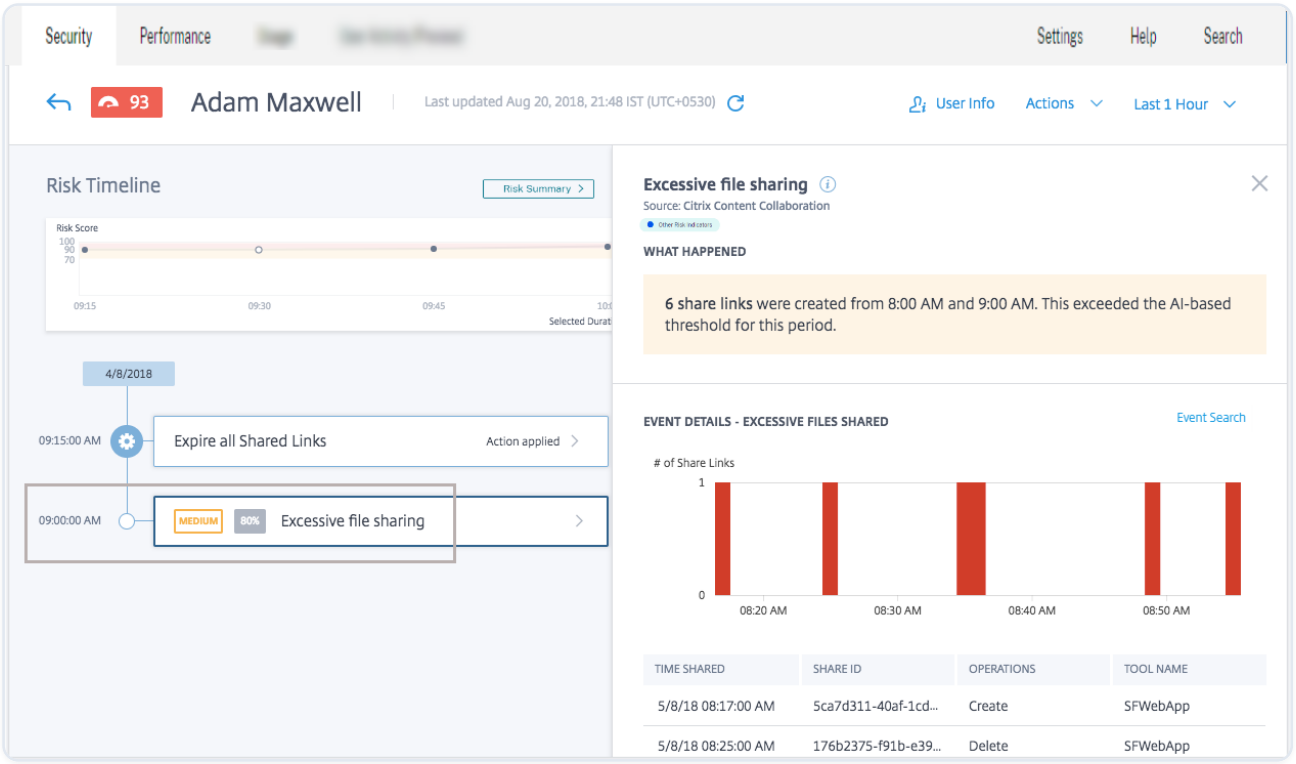
此外，您可以查看用户的风险评分和风险指标趋势，并确定该用户是否为高风险用户。

您可以在用户风险时间线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评分。



当您进入用户的风险时间线时，您可以选择一个风险指标或一个已应用于其帐户的操作。如果您选择其中之一，右侧窗格将显示风险指标部分或操作部分。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



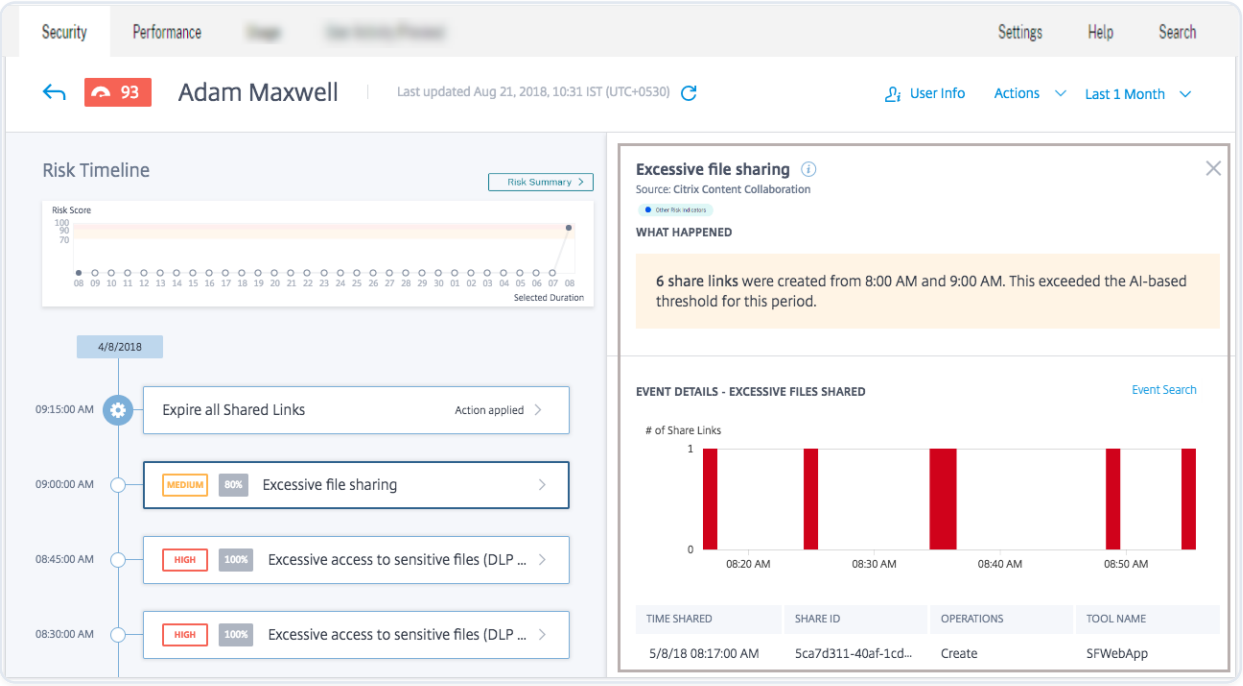
风险时间线

风险时间线显示以下信息：

- **风险指标**。风险指标是可疑的用户活动，可能对您的组织构成安全威胁。当用户行为偏离其正常行为时，会触发这些指标。风险指标可用于以下数据源：
  - Citrix 内容协作
  - Citrix 网关
  - Citrix 端点管理™
  - Citrix 虚拟应用和桌面 或 Citrix DaaS（以前称为 Citrix 虚拟应用和桌面服务）
  - Citrix 安全私有访问

  当您从用户时间线中选择风险指标时，右侧窗格中会显示风险指标信息部分。您可以查看风险指标的原因以及事件的详细信息。它们大致分为以下几个部分：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **发生了什么**。您可以在此处查看风险指标的摘要。例如，如果您选择了**文件共享过多**风险指标。在“发生了什么”部分，您可以查看发送给收件人的共享链接数量以及共享事件发生的时间。
- **事件详细信息**。您可以以图形和表格格式查看单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标对应的事件。有关更多信息，请参阅**自助搜索**。
- **其他上下文信息**。您可以在此部分查看事件发生期间共享的数据（如果有）。

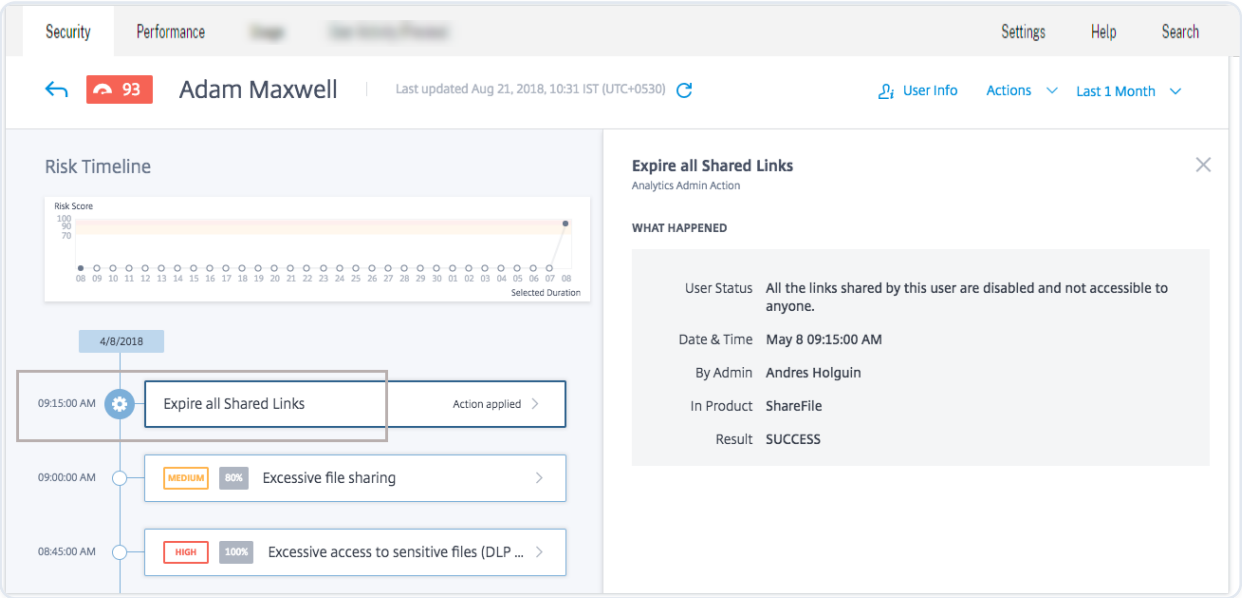
您可以手动将风险指标标记为有用或无用。有关更多信息，请参阅提供用户风险指标反馈。

了解更多：风险指标

- **操作**。操作可帮助您响应可疑事件并防止未来异常事件的发生。已应用于用户配置文件的操作会显示在风险时间线上。这些操作可以通过配置的策略自动应用于用户帐户，或者您可以手动应用特定操作。

  了解更多：策略和操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



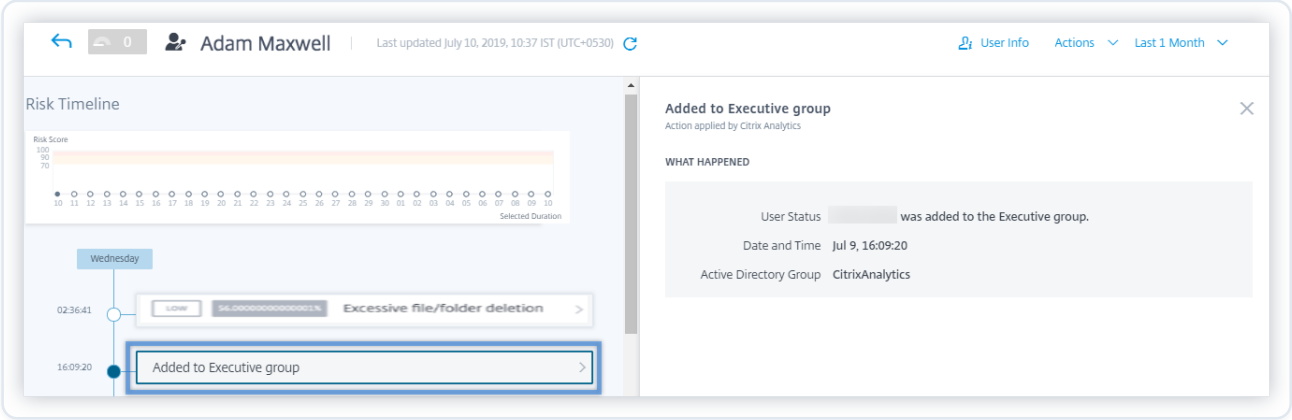
- **特权用户事件**。每当用户的管理员或高管特权状态发生变化时，都会触发特权用户事件。当用户的风险指标被触发时，您可以将其与指定的特权状态更改事件关联起来。如有必要，您可以对用户配置文件应用适当的操作。用户风险时间线上显示的管理员或高管特权事件如下：

  - 已添加到高管组
  - 已从高管组中移除
  - 特权已提升为管理员
  - 管理员特权已移除

  考虑用户 Adam Maxwell，他被添加到了高管特权组 **CitrixAnalytics**。**已添加到高管组**事件被添加到用户的风险时间线中。现在，Adam 开始过度删除文件和文件夹，并触发了检测异常行为的机器学习算法。**过度删除文件或文件夹**风险指标被添加到用户的风险时间线中。您可以在风险时间线上比较事件和风险指标。比较后，您可以确定风险指标是否是该事件的后果。如果是，您可以对 Adam 的配置文件应用适当的操作。有关特权用户的更多信息，请参阅特权用户。

当您从用户时间线中选择一个事件时，事件信息部分会显示在右侧窗格中。

对于高管，右侧窗格显示的信息包括**用户状态**、**日期和时间**以及**Active Directory 组**。

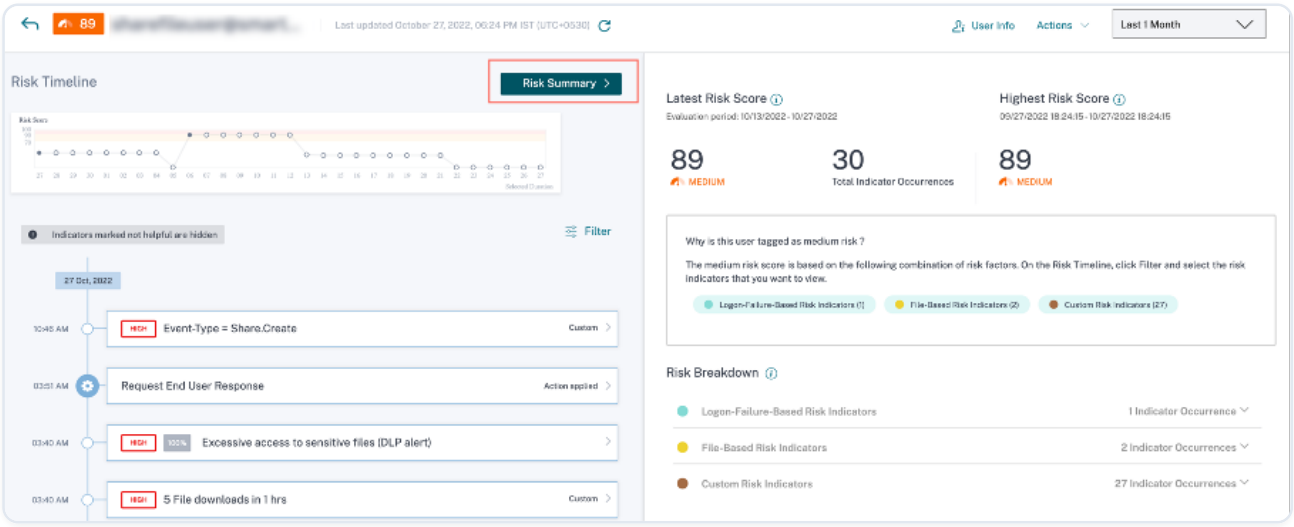


© 1997–2026 Citrix Systems, Inc. All rights reserved.

对于管理员特权事件，右侧窗格显示的信息包括**用户状态**、**日期和时间**以及**产品内**。

风险摘要

查看与用户相关的风险因素，这些因素导致了他们的风险评分。您可以查看在选定时间段内取最大值的风险评分详细信息，以及最新评分和相应的风险指标计数。从主登录页面或风险用户页面导航到用户时间线时，时间选择会从源页面保留。有关风险因素的更多信息，请参阅Citrix 用户风险指标。

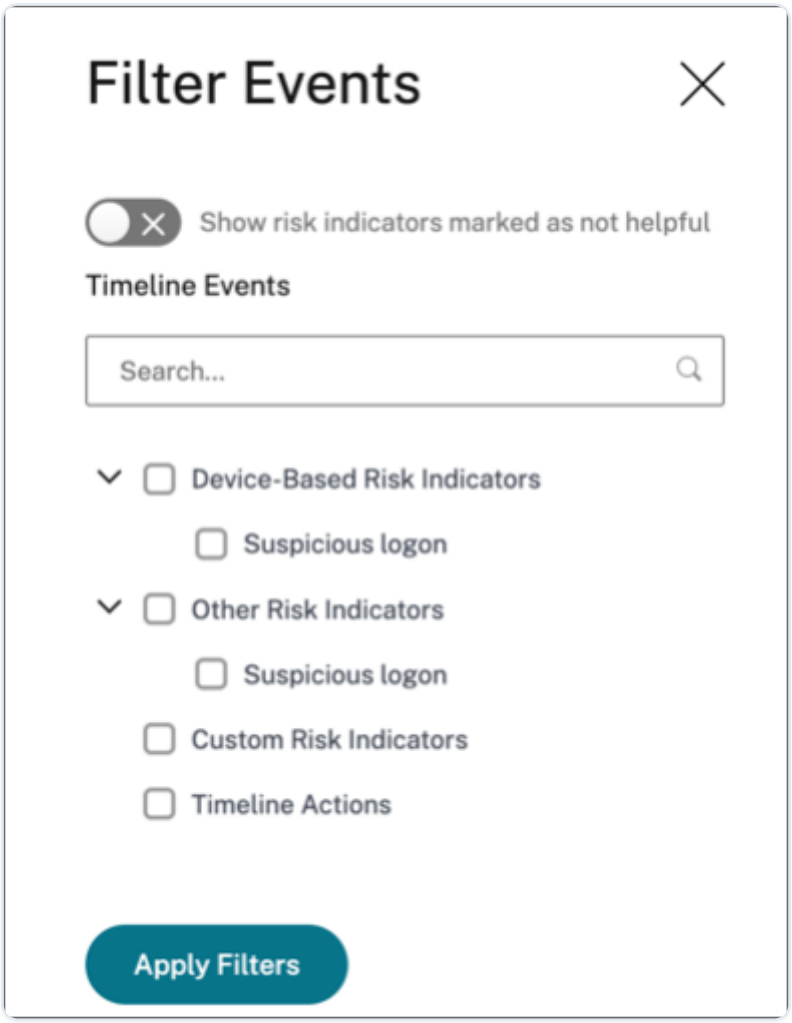


单击**风险摘要**以查看以下信息：

- **最新风险评分**：最新风险评分表示用户基于近期行为的当前风险。风险评分确定用户在过去两周内对组织构成的风险级别。风险评分值是动态的，并根据用户行为分析而变化。根据评分，用户可分为以下几类：高风险用户、中风险用户、低风险用户和零风险评分用户。有关用户类别的更多信息，请参阅用户仪表板。
    - **指标总发生次数**：表示用户在过去两周内触发的风险指标总数。这些触发的风险指标决定了用户的风险评分。
- **最高风险评分**：最高风险评分表示在选定时间段内为此用户计算的风险评分的最大值。它代表用户的总风险，可能不总是等于最新风险评分。
- **风险因素**：表示与导致风险评分的用户活动相关的一个或多个风险因素组合。
- **风险细分**：表示用户为每个风险因素触发的风险指标数量。展开行以查看详细信息。

在用户时间轴上，点击**筛选**并选择与用户相关的风险因素、已应用的操作或特权用户状态，并查看相应的事件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



用户配置文件

用户配置文件页面显示以下来自用户活动目录的用户信息：

- 职位
- 地址
- 电子邮件
- 电话
- 位置
- 组织



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix® 用户风险指标

注意

注意：Citrix Content Collaboration™ 和 ShareFile 已达到其生命周期结束，不再向用户提供。

用户风险指标是看起来可疑或可能对您的组织构成安全威胁的用户活动。这些风险指标涵盖您部署中使用的所有 Citrix 产品。当用户行为偏离正常时，会触发风险指标。每个风险指标可以有一个或多个与之关联的风险因素。这些风险因素可帮助您确定用户事件中的异常类型。风险指标及其关联的风险因素决定了用户的风险评分。

以下是与风险指标关联的风险因素：

- **基于设备的风险指标**：当用户从根据其设备历史记录被视为异常的设备登录时触发。
- **基于位置的风险指标**：当用户从与某个位置关联的 IP 地址登录时触发，该位置根据用户的地理位置历史记录被视为异常。
- **基于 IP 的风险指标**：当用户尝试从被识别为可疑的 IP 地址访问资源时触发，无论该 IP 地址对用户而言是否异常。
- **基于登录失败的风险指标**：当用户出现过多或异常登录失败模式时触发。
- **基于数据的风险指标**：当用户尝试从 Workspace 会话中窃取数据时触发。观察到的用户行为包括复制或粘贴事件、下载模式等等。
- **基于文件的风险指标**：当用户在 Content Collaboration 上访问文件的行为根据其历史访问模式被视为异常时触发。观察到的用户行为包括下载模式、访问敏感内容、勒索软件迹象的活动等等。
- **自定义风险指标**：当满足预配置条件或用户定义条件时触发。有关详细信息，请参阅以下文章：
  - 自定义风险指标
  - 预配置的自定义风险指标和策略
- 其他风险指标 - 不属于任何预定义风险因素（例如基于设备的、基于位置的和基于登录失败的）的风险指标。

风险指标也根据相似的风险分组到风险类别中。有关详细信息，请参阅风险类别。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

下表显示了风险指标、风险因素和风险类别之间的关联。

产品	用户风险指标	风险因素	风险类别
思杰端点管理	检测到具有黑名单应用程序的设备	其他风险指标	受损的端点
	检测到越狱或已root的设备	其他风险指标	受损的端点
	检测到非托管设备	其他风险指标	受感染的端点
Citrix 网关	端点分析 (EPA) 扫描失败	其他风险指标	受感染的用户
	过多的身份验证失败	基于登录失败的风险指标	受感染的用户
	不可能的行程	基于位置的风险指标	受感染的用户
	来自可疑 IP 的登录	基于 IP 的风险指标	受感染的用户
	可疑登录	基于设备的风险指标、基于IP的风险指标、基于位置的风险指标以及其他风险指标	受感染的用户
	异常身份验证失败	基于登录失败的风险指标	受感染的用户
Citrix 安全私有访问	尝试访问黑名单URL	其他风险指标	内部威胁
	过量数据下载	其他风险指标	内部威胁
	风险网站访问	其他风险指标	内部威胁
	异常上传量	其他风险指标	内部威胁
Citrix DaaS（以前称为 Citrix 虚拟应用和桌面 服务）和本地 Citrix 虚拟应用和桌面	不可能行程	基于位置的风险指标	受感染用户

© 1997–2026 Citrix Systems, Inc. All rights reserved.

产品	用户风险指标	风险因素	风险类别
	潜在数据渗漏	基于数据的风险指标	数据渗漏
	可疑登录	基于设备的风险指标、基于 IP 的风险指标、基于位置的风险指标和其他风险指标	受感染用户

您可以手动将风险指标标记为有用或无用。有关详细信息，请参阅 为用户风险指标提供反馈。

思杰终端管理™ 风险指标

检测到黑名单应用程序的设备

Citrix Analytics 根据带有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标。

检测到黑名单应用程序的设备风险指标在 Endpoint Management 服务在软件清点期间检测到黑名单应用程序时触发。此警报确保只有授权的应用程序在您组织网络中的设备上运行。

与检测到黑名单应用程序的设备风险指标关联的风险因素是其他风险指标。有关风险因素的更多信息，请参阅Citrix 用户风险指标。

何时触发检测到黑名单应用程序的设备风险指标?

检测到黑名单应用程序的设备风险指标在用户的设备上检测到黑名单应用程序时报告。当 Endpoint Management 服务在软件清点期间检测到设备上有一个或多个黑名单应用程序时，事件将发送到 Citrix Analytics。

Citrix Analytics 监控这些事件并更新用户的风险评分。此外，它还会将**检测到黑名单应用程序的设备**风险指标条目添加到用户的风险时间线中。

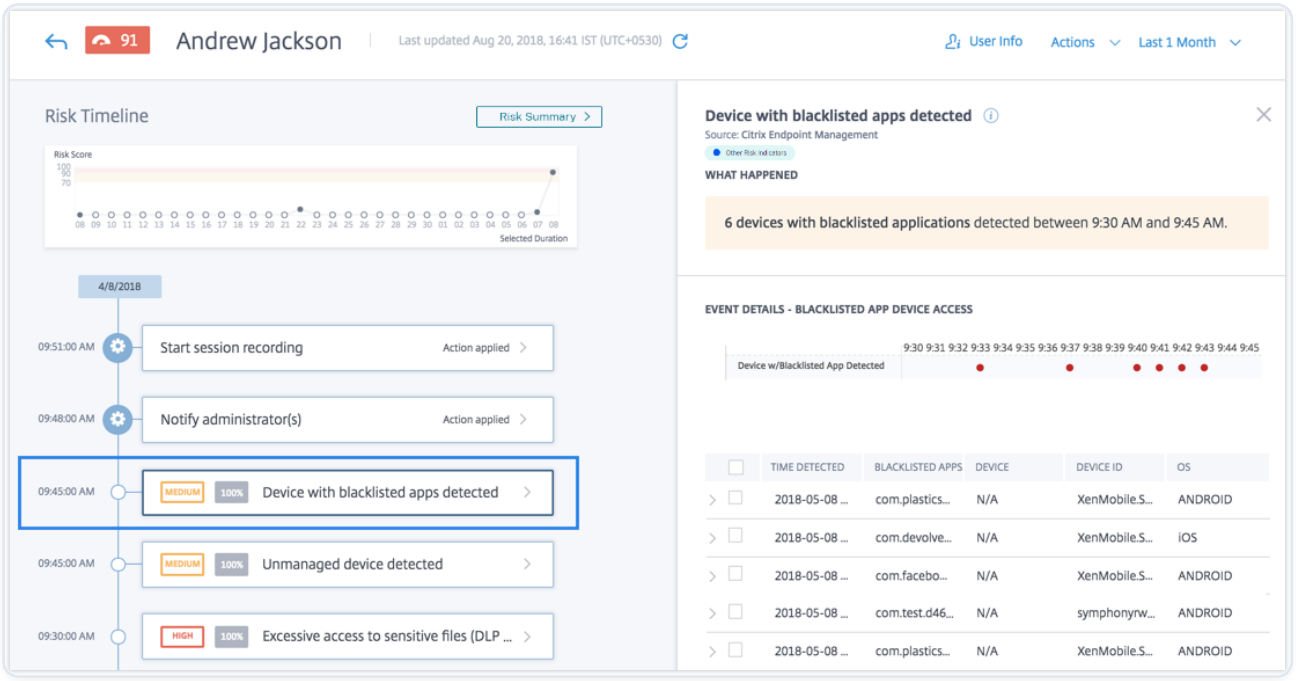
如何分析检测到黑名单应用程序的设备风险指标?

以用户 Andrew Jackson 为例，他使用的设备最近安装了黑名单应用程序。Endpoint Management 将此情况报告给 Citrix Analytics，后者为 Andrew Jackson 分配更新的风险评分。

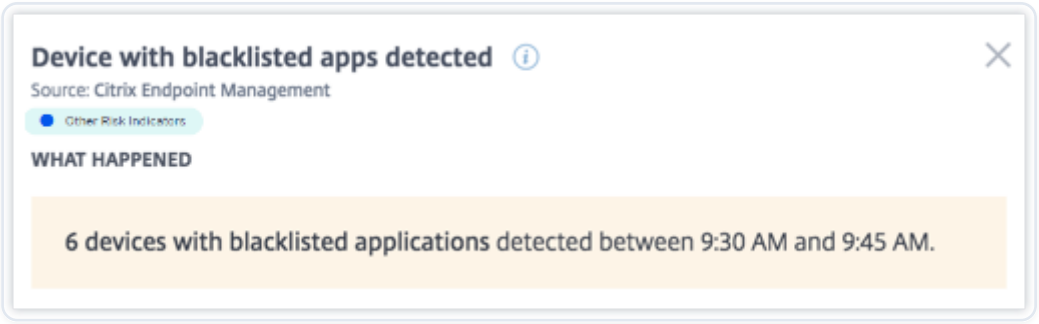
在 Andrew Jackson 的风险时间线中，您可以选择报告的**检测到黑名单应用程序的设备**风险指标。事件的原因以及详细信息（例如黑名单应用程序列表、Endpoint Management 检测到黑名单应用程序的时间等）都会显示。

要查看用户的**检测到黑名单应用程序的设备**风险指标，请导航到**安全 > 用户**，然后选择该用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

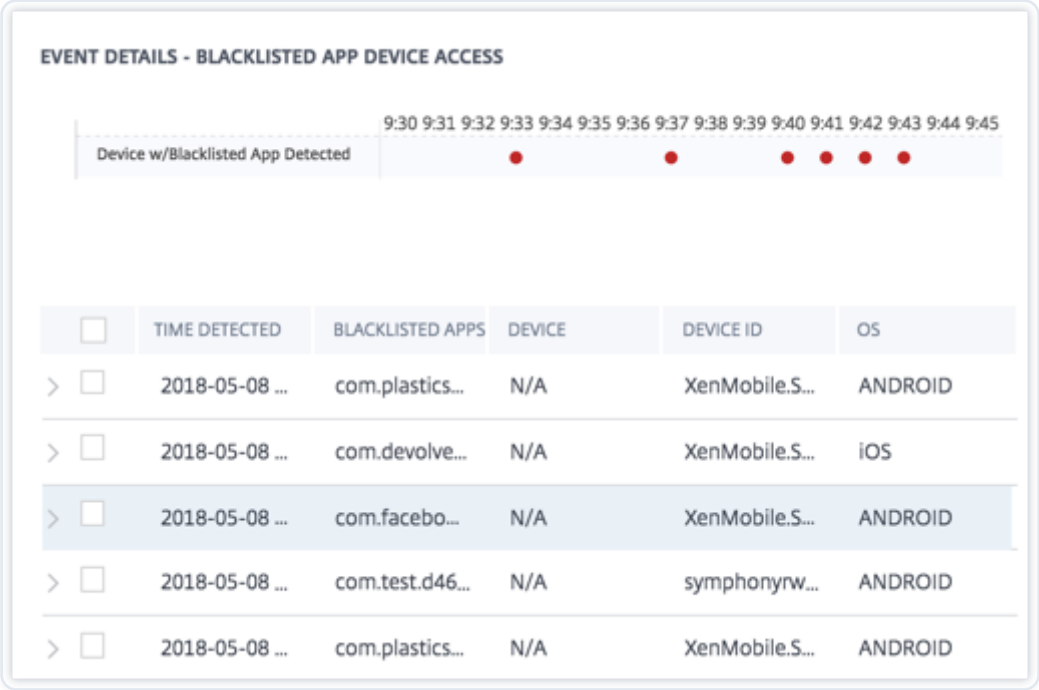


- 在**发生了什么**部分中，您可以查看事件摘要。您可以查看 Endpoint Management 服务检测到的带有黑名单应用程序的设备数量以及事件发生的时间。



- 在**事件详细信息 – 黑名单应用程序设备访问**部分，事件以图形和表格形式显示。事件也作为单个条目显示在图表中，表格提供以下关键信息：
  - **检测时间**- Endpoint Management 报告检测到黑名单应用程序的时间。
  - **黑名单应用程序**- 设备上的黑名单应用程序。
  - **设备**- 所使用的移动设备。
  - **设备 ID**- 用于登录会话的设备 ID 信息。
  - **操作系统**- 移动设备的操作系统。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意

除了以表格形式查看详细信息外，您还可以单击警报实例旁边的箭头以查看更多详细信息。

您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到监视列表**。当您希望监视用户以防范未来潜在威胁时，可以将其添加到监视列表。
- **通知管理员**。当用户帐户出现任何异常或可疑活动时，系统会向所有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它们的更多信息，请参阅策略和操作。

要手动对用户应用操作，请导航到用户配置文件并选择相应的风险指标。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是什么，都可以应用与其他数据源相关的操作。

检测到越狱或已获得 root 权限的设备

Citrix Analytics 根据越狱或已获得 root 权限的设备活动检测访问威胁，并触发相应的风险指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

越狱或已获得 root 权限的设备风险指标在用户使用越狱或已获得 root 权限的设备连接到网络时触发。Secure Hub 会检测到该设备并将事件报告给 Endpoint Management 服务。此警报可确保只有授权用户和设备才能连接到您的组织网络。

与越狱或已获得 root 权限的设备风险指标相关的风险因素是其他风险指标。有关风险因素的更多信息，请参阅Citrix 用户风险指标。

何时触发检测到越狱或已获得 root 权限的设备风险指标?

安全官员能够确保用户使用符合网络要求的设备进行连接非常重要。**检测到越狱或已获得 root 权限的设备**风险指标会提醒您注意使用越狱 iOS 设备或已获得 root 权限的 Android 设备的用户。

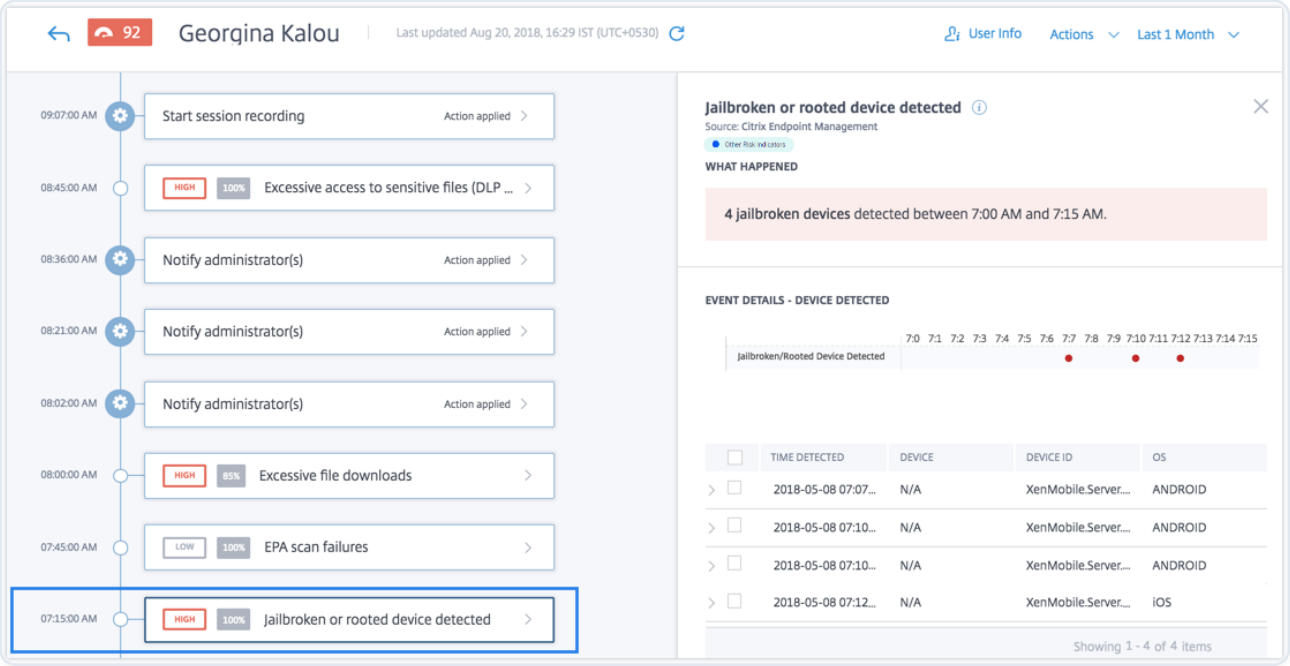
越狱或已获得 root 权限的设备风险指标在已注册设备越狱或获得 root 权限时触发。Secure Hub 会检测设备上的事件并将其报告给 Endpoint Management 服务。

如何分析检测到越狱或已获得 root 权限的设备风险指标?

考虑用户 Georgina Kalou，其已注册的 iOS 设备最近被越狱。Citrix Analytics 会检测到此可疑行为，并为 Georgina Kalou 分配风险评分。

从 Georgina Kalou 的风险时间线中，您可以选择报告的**检测到越狱或已获得 root 权限的设备**风险指标。事件原因将与风险指标触发时间、事件描述等详细信息一起显示。

要查看用户的**检测到越狱或已获得 root 权限的设备**风险指标，请导航到**安全 > 用户**，然后选择该用户。



- 在**发生了什么**部分，您可以查看事件摘要。您可以查看检测到的越狱或已获得 root 权限的设备数量以及事件发生的时间。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

检测到越狱或已获得 root 权限的设备发生了什么(/en-us/citrix-analytics/media/endpoint-management-jailbroken-rooted-device-what-happened.png)

- 在**事件详细信息 – 检测到的设备**部分，事件以图形和表格格式显示。事件也作为图表中的单个条目显示，表格提供以下关键信息：
  - **检测时间**。检测到越狱或已获得 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 ID 的信息。
  - **操作系统**。移动设备的操作系统。

  检测到越狱或已获得 root 权限的设备事件详细信息(/en-us/citrix-analytics/media/endpoint-management-jailbroken-rooted-device-event-details.png)

注意

除了以表格格式查看详细信息外，单击警报实例旁边的箭头可查看更多详细信息。

您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到监视列表**。当您想要监视用户以防范未来潜在威胁时，可以将其添加到监视列表。
- **通知管理员**。当用户帐户出现任何异常或可疑活动时，系统会向所有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。

要手动对用户应用操作，请导航到用户配置文件并选择相应的风险指标。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是什么，都可以应用与其它数据源相关的操作。

检测到非托管设备

Citrix Analytics 根据非托管设备活动检测访问威胁，并触发相应的风险指标。

当设备出现以下情况时，会触发**检测到非托管设备**风险指标：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 因自动化操作而被远程擦除。
- 由管理员手动擦除。
- 由用户取消注册。

与“检测到非托管设备”风险指标相关的风险因素是“其他风险指标”。有关风险因素的更多信息，请参阅Citrix 用户风险指标。

何时会触发检测到非托管设备风险指标?

当用户的设备变为非托管状态时，会报告**检测到非托管设备**风险指标。设备变为非托管状态的原因是：

- 用户执行的操作。
- Endpoint Management 管理员或服务器执行的操作。

在您的组织中，您可以使用 Endpoint Management 服务管理访问网络的设备和应用程序。有关更多信息，请参阅管理模式。

当用户的设备变为非托管状态时，Endpoint Management 服务会检测到此事件并将其报告给 Citrix Analytics。用户的风险评分会更新。**检测到非托管设备**风险指标会添加到用户的风险时间线中。

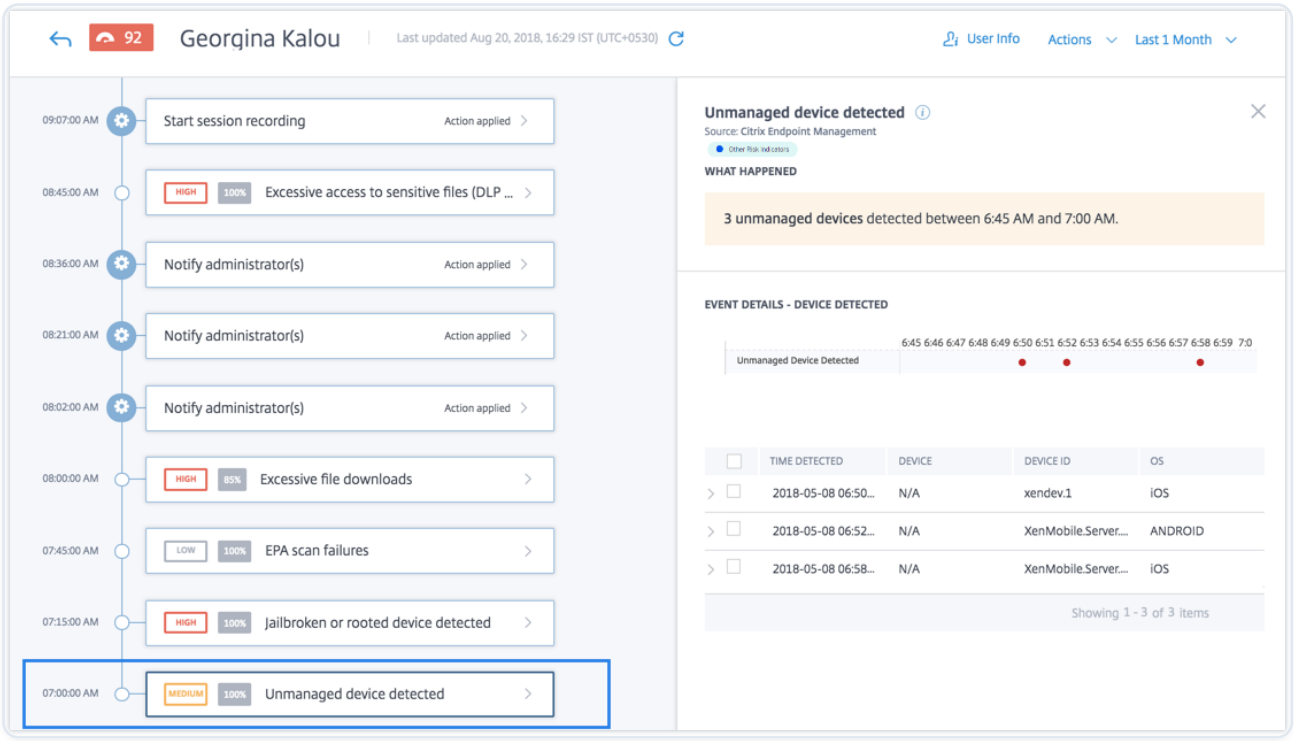
如何分析检测到非托管设备的风险指标?

考虑用户 Georgina Kalou，其设备被服务器上的自动化操作远程擦除。Endpoint Management 将此事件报告给 Citrix Analytics，后者为 Georgina Kalou 分配了更新的风险评分。

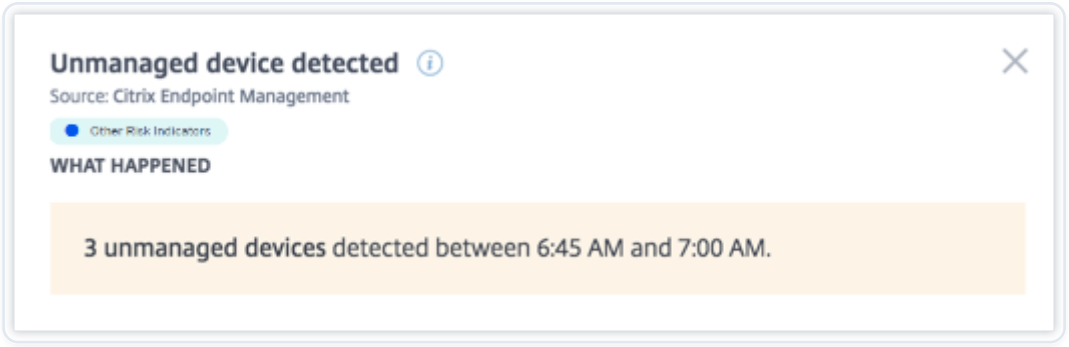
在 Georgina Kalou 的风险时间线中，您可以选择报告的“检测到非托管设备”风险指标。事件原因将与风险指标触发时间、事件描述等详细信息一起显示。

要查看用户的**检测到非托管设备**风险指标，请导航到**安全 > 用户**，然后选择该用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

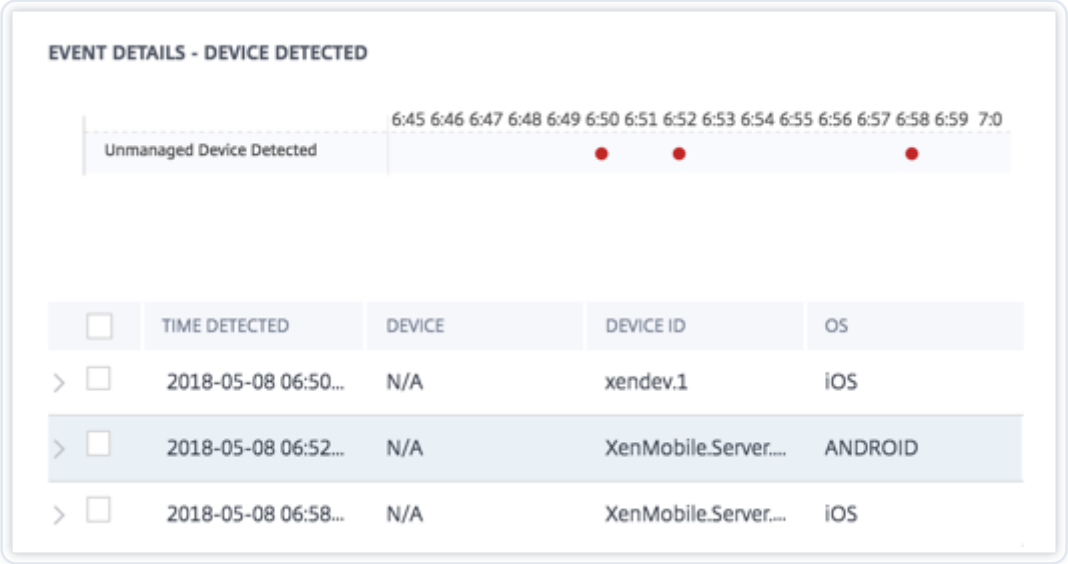


- 在**发生了什么**部分，您可以查看事件摘要。您可以查看检测到的非托管设备数量以及事件发生的时间。



- 在**事件详细信息 – 检测到设备**部分，事件以图形和表格形式显示。事件也作为单独的条目显示在图中，表格提供以下关键信息：
  - **检测时间**。事件被检测到的时间。
  - **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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到观察列表**。当您想要监控用户以防范未来潜在威胁时，可以将其添加到观察列表。
- **通知管理员**。当用户的账户出现任何异常或可疑活动时，系统会向所有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，请导航到用户配置文件并选择相应的风险指标。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是什么，都可以应用与其他数据源相关的操作。

Citrix Gateway 风险指标

端点分析 (EPA) 扫描失败

Citrix Analytics 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标。

与端点分析扫描失败风险指标相关的风险因素是其他风险指标。有关风险因素的更多信息，请参阅 Citrix 用户风险指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EPA 扫描失败风险指标何时触发?

当用户尝试使用未能通过 Citrix Gateway 的端点分析 (EPA) 扫描策略的设备进行预身份验证或后身份验证来访问网络时，会报告 EPA 扫描失败风险指标。

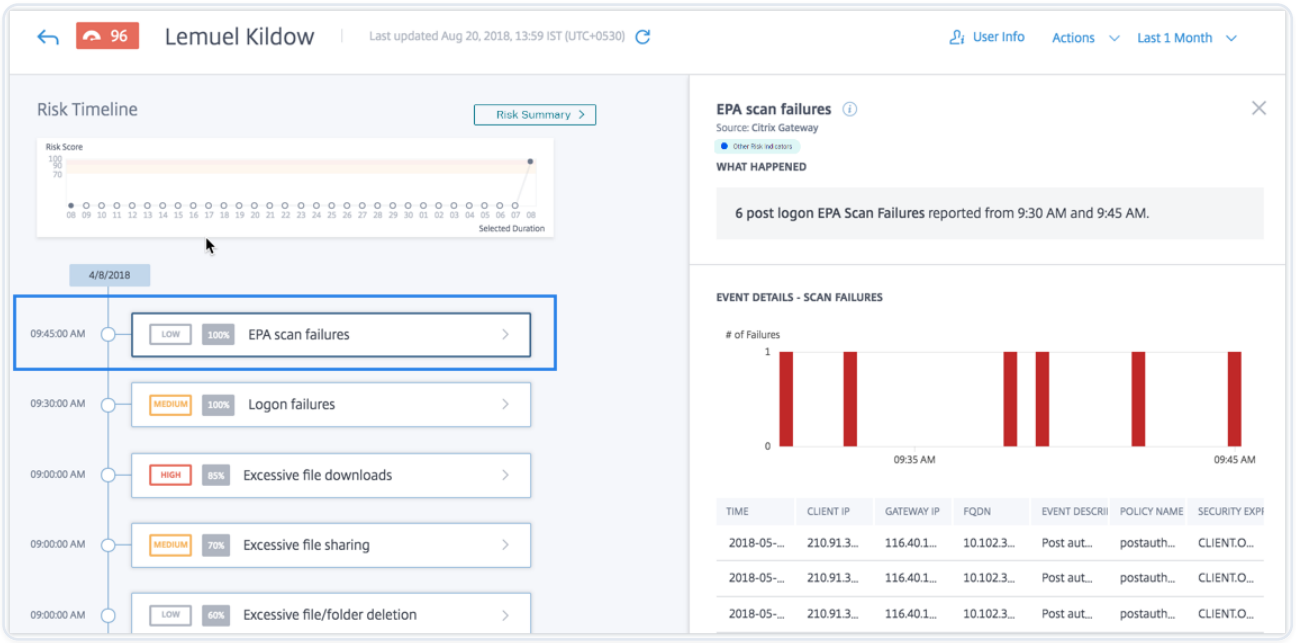
Citrix Gateway 检测到这些事件并将其报告给 Citrix Analytics。Citrix Analytics 监控所有这些事件，以检测用户是否发生了过多的 EPA 扫描失败。当 Citrix Analytics 确定用户存在过多的 EPA 扫描失败时，它会更新用户的风险评分，并将 EPA 扫描失败风险指标条目添加到用户的风险时间线中。

如何分析 EPA 扫描失败风险指标?

考虑用户 Lemuel，他最近多次尝试使用未能通过 Citrix Gateway EPA 扫描的设备访问网络。Citrix Gateway 将此失败报告给 Citrix Analytics，后者会为 Lemuel 分配更新的风险评分。EPA 扫描失败风险指标已添加到 Lemuel Kildow 的风险时间线中。

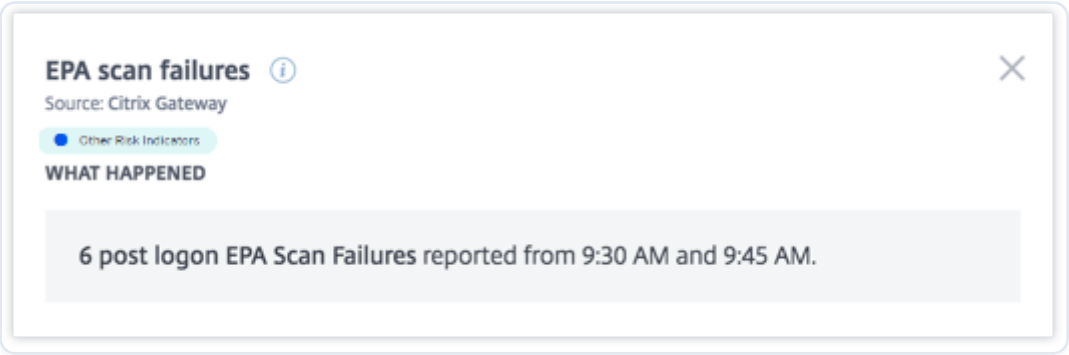
要查看用户的 **EPA 扫描失败** 条目，请导航到 **安全 > 用户**，然后选择该用户。

在 Lemuel Kildow 的风险时间线中，您可以选择为该用户报告的最新 **EPA 扫描失败** 风险指标。当您从时间线中选择一个 EPA 扫描失败风险指标条目时，右侧窗格中会显示相应的详细信息面板。

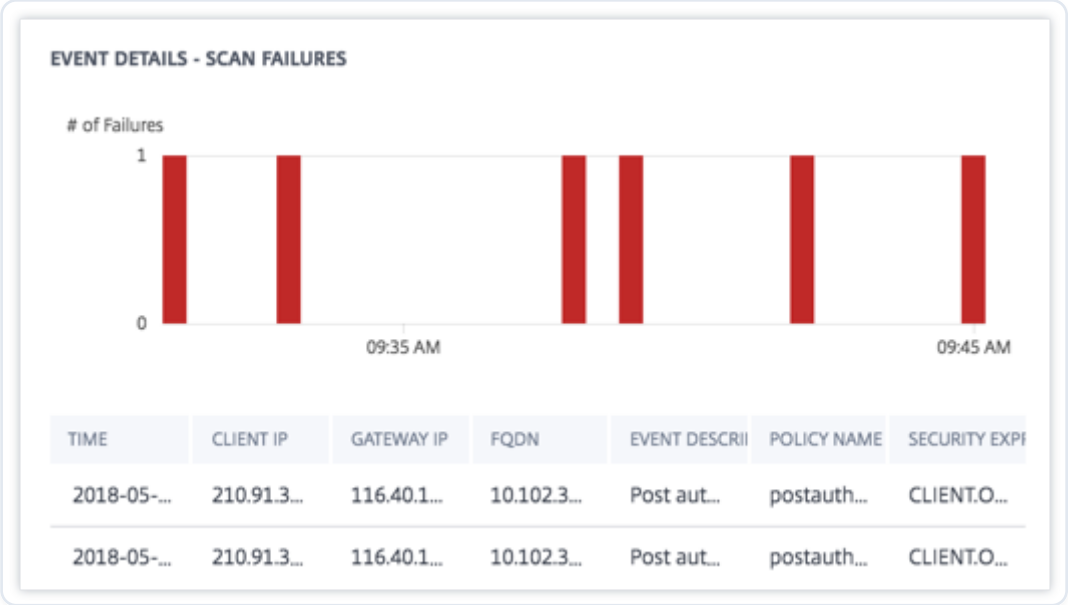


- **发生了什么** 部分提供了 EPA 扫描失败风险指标的简要摘要。此外，它还包括在选定期间报告的登录后 EPA 扫描失败次数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **事件详细信息 – 扫描失败** 部分包括在选定时间段内发生的各个 EPA 扫描失败事件的时间线可视化。此外，它还包括一个表格，提供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。
  - **完全限定域名**。Citrix Gateway 的完全限定域名。
  - **事件描述**。EPA 扫描失败原因的简要描述。
  - **策略名称**。在 Citrix Gateway 上配置的 EPA 扫描策略名称。
  - **安全表达式**。在 Citrix Gateway 上配置的安全表达式。



您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到监视列表**。当您想要监视用户以防范未来潜在威胁时，可以将其添加到监视列表。
- **通知管理员**。当用户帐户上出现任何异常或可疑活动时，会向所有或选定的管理员发送电子邮件通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **注销用户**。当用户从其帐户注销时，他们无法通过 Citrix Gateway 访问任何资源，直到 Citrix Gateway 管理员清除“注销用户”操作。
- **锁定用户**：当用户的帐户因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。

要了解有关操作以及如何手动配置它们的更多信息，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是什么，都可以应用与其他数据源相关的操作。

身份验证失败过多

Citrix Analytics 根据身份验证失败过多检测基于用户访问的威胁，并触发相应的风险指示器。

与身份验证失败过多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。

身份验证失败过多风险指示器何时触发？

当用户在给定时间内遇到多次 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、次要或三次身份验证失败，具体取决于是否为用户配置了多重身份验证。

Citrix Gateway 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 监控所有这些事件，以检测用户是否发生过多的身份验证失败。当 Citrix Analytics 确定身份验证失败过多时，它会更新用户的风险评分。身份验证失败过多风险指示器将添加到用户的风险时间线中。

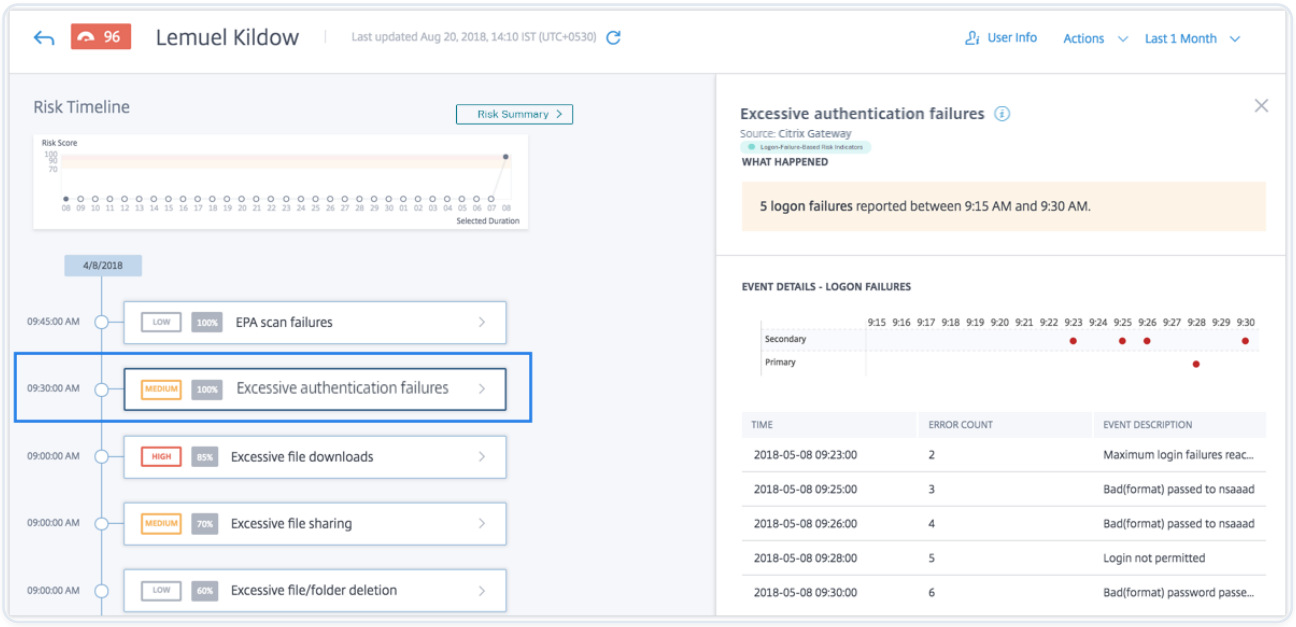
如何分析身份验证失败过多风险指示器？

考虑用户 Lemuel，他最近多次尝试验证网络失败。Citrix Gateway 将这些失败报告给 Citrix Analytics，并为 Lemuel 分配更新的风险评分。“**身份验证失败过多**”风险指示器将添加到 Lemuel Kildow 的风险时间线中。

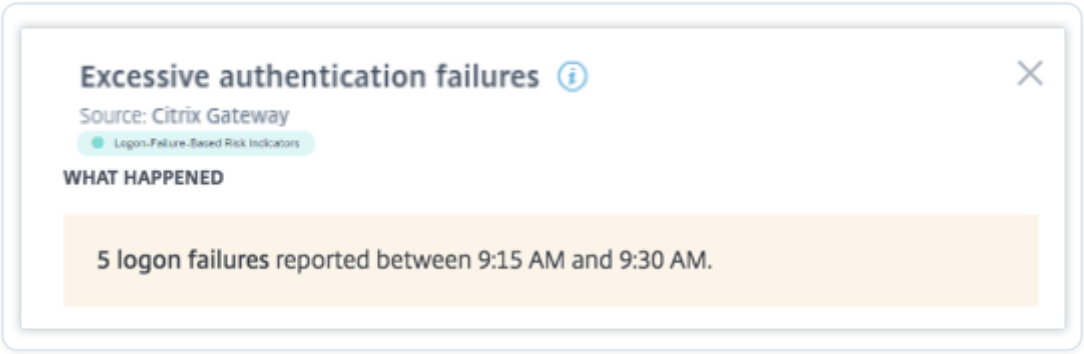
要查看用户的“**身份验证失败过多**”风险指示器条目，请导航到“**安全 > 用户**”，然后选择该用户。

从 Lemuel Kildow 的风险时间线中，您可以选择为用户报告的最新“**身份验证失败过多**”风险指示器。当您从风险时间线中选择“**身份验证失败过多**”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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

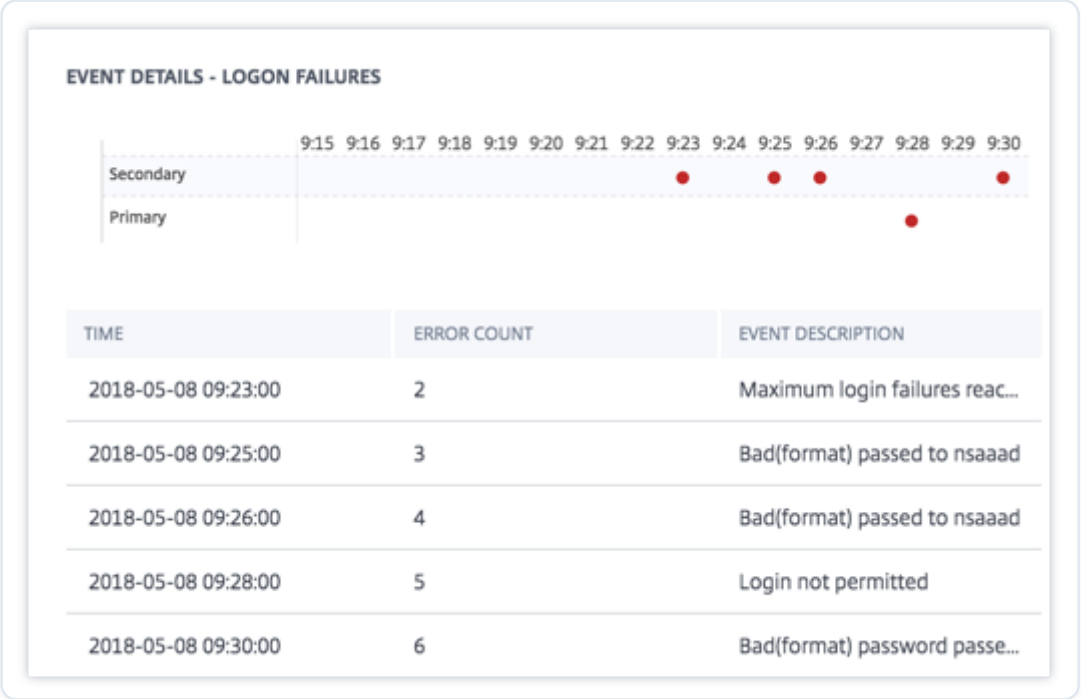


- “**发生了什么**”部分提供了风险指示器的简要摘要，包括在选定期间发生的身份验证失败次数。



- **事件详细信息**部分包含单个身份验证失败过多事件的时间线可视化，这些事件发生在选定的时间段内。此外，您可以查看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**。在事件发生时以及之前 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描述。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到监视列表**。当您想要监视用户以防范未来潜在威胁时，可以将其添加到监视列表。
- **通知管理员**。当用户帐户出现任何异常或可疑活动时，系统会向所有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，他们无法通过 Citrix Gateway 访问任何资源，直到 Citrix Gateway 管理员清除“注销用户”操作。
- **锁定用户**：当用户的帐户因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 Gateway 管理员解锁该帐户。

要了解有关操作以及如何手动配置它们的更多信息，请参阅策略和操作。

要手动将操作应用于用户，请导航到用户配置文件并选择相应的风险指标。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是什么，都可以应用与其它数据源相关的操作。

不可能行程

当用户连续两次登录来自两个不同国家，且两次登录之间的时间间隔小于两国之间的预期旅行时间时，Citrix Analytics 会将此登录检测为有风险。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

不可能行程时间场景表明存在以下风险：

- **凭据泄露**：远程攻击者窃取了合法用户的凭据。
- **共享凭据**：不同的用户正在使用相同的用户凭据。

何时会触发“不可能行程”风险指标?

不可能行程风险指标会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给定时间内可能旅行的距离时触发。

注意

此风险指标还包含用于减少以下不反映用户实际位置的场景的误报警报的逻辑：

- 用户通过 Citrix Gateway 从代理连接登录时。
- 用户通过 Citrix Gateway 从托管客户端登录时。

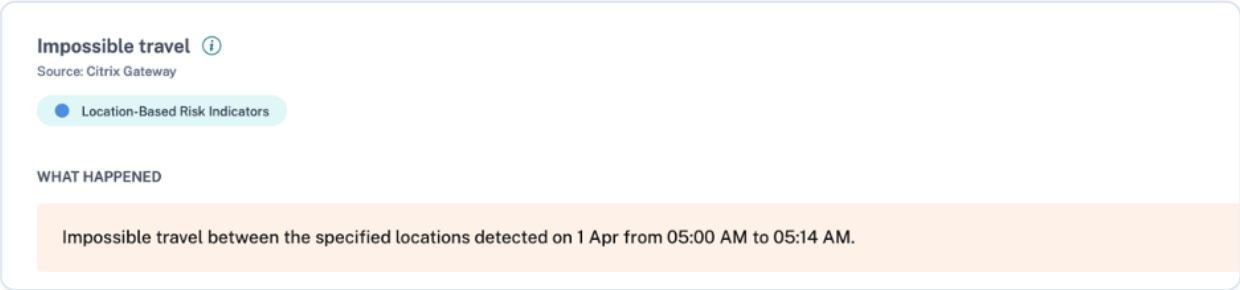
如何分析“不可能行程”风险指标

考虑用户 Adam Maxwell，他在一分钟内从两个位置登录：印度班加罗尔和挪威奥斯陆。Citrix Analytics 将此登录事件检测为不可能行程场景，并触发**不可能行程**风险指标。该风险指标将添加到 Adam Maxwell 的风险时间线中，并为其分配风险评分。

要查看 Adam Maxwell 的风险时间线，请选择**安全 > 用户**。从**有风险的用户**窗格中，选择用户 Adam Maxwell。

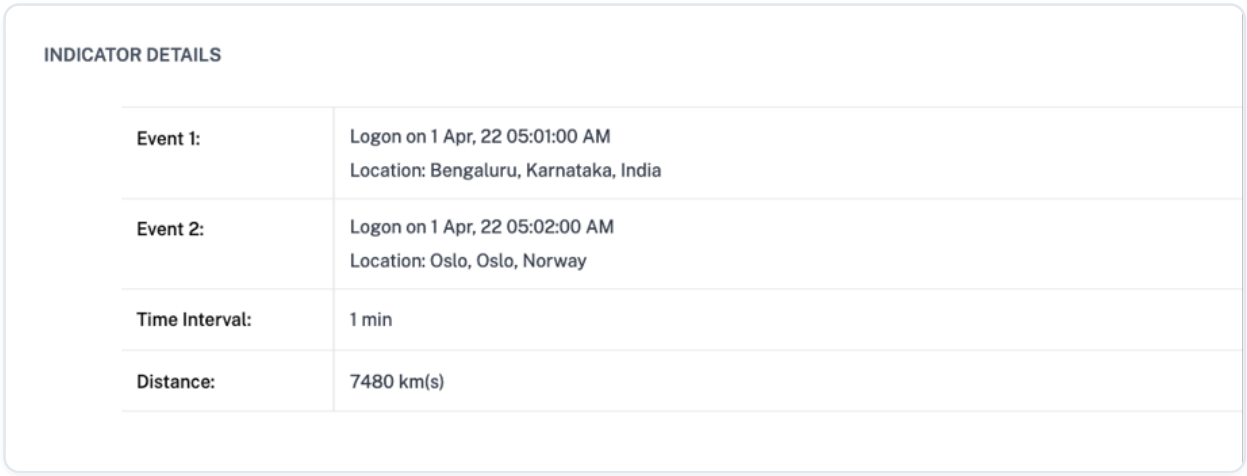
从 Adam Maxwell 的风险时间线中，选择“**不可能的行程**”风险指标。您可以查看以下信息：

- “**发生了什么**”部分提供了不可能的行程事件的简要摘要。



- “**指标详细信息**”部分提供了用户登录的地点、连续登录之间的时间间隔以及两个地点之间的距离。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

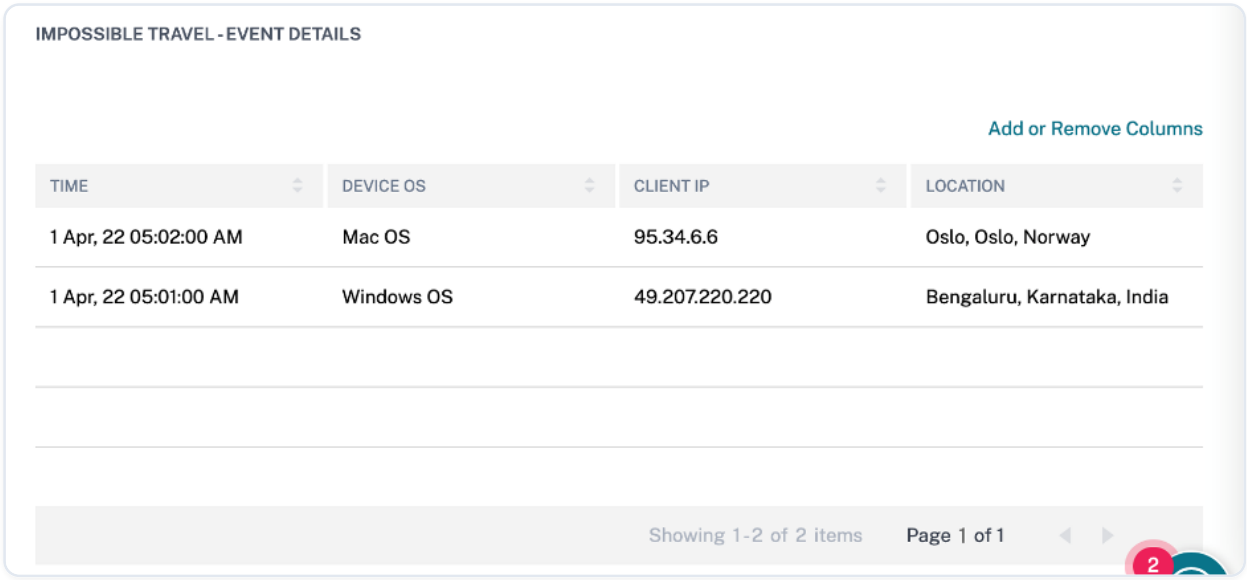


- “**登录地点 - 最近 30 天**”部分显示了不可能的行程地点和用户已知地点的地理地图视图。地点数据显示最近 30 天。您可以将鼠标悬停在地图上的指针上，以查看每个地点的总登录次数。



- “**不可能的行程 - 事件详细信息**”部分提供了有关不可能的行程事件的以下信息：
  - “**时间**”：指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**”：指示用户设备的 IP 地址。
  - “**地点**”：指示用户登录的地点。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到监视列表**。当您想要监视用户以防范未来潜在威胁时，可以将其添加到监视列表。
- **通知管理员**。当用户的帐户出现任何异常或可疑活动时，系统会向所有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，他们无法通过 Citrix Gateway 访问任何资源，直到 Citrix Gateway 管理员清除“注销用户”操作。
- **锁定用户**：当用户的帐户因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 Gateway 管理员解锁该帐户。

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是什么，都可以应用与其它数据源相关的操作。

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“从可疑 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

何时触发“从可疑 IP 登录”风险指示器?

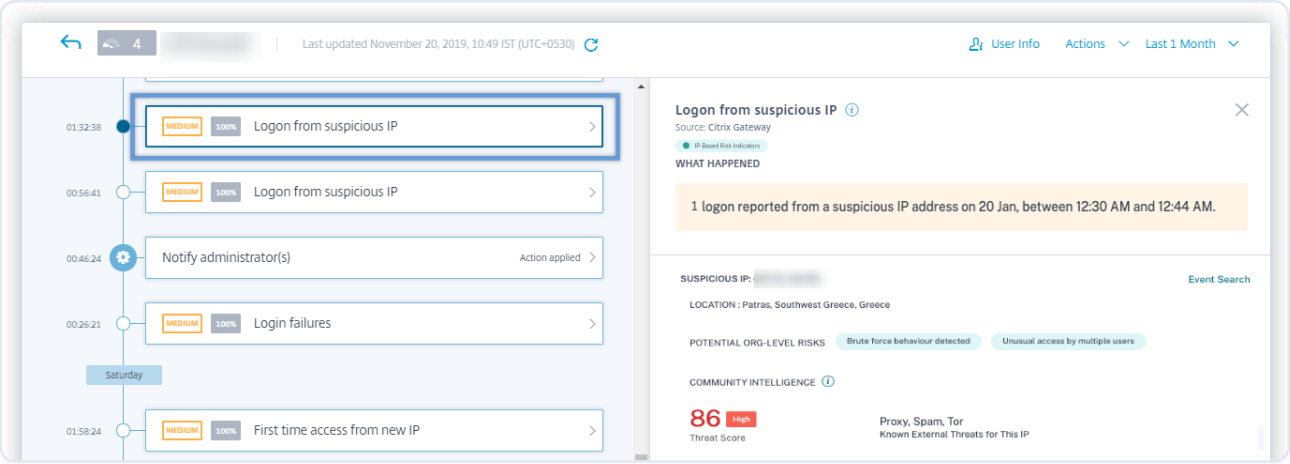
当用户尝试从 Citrix Analytics 识别为可疑的 IP 地址访问网络时，会触发**从可疑 IP 登录**风险指示器。IP 地址在以下任一条件下被视为可疑：

- 列在外部 IP 威胁情报源中
- 具有来自异常位置的多个用户登录记录
- 有过多失败的登录尝试，这可能表明存在暴力破解攻击

Citrix Analytics 监控从 Citrix Gateway 接收到的登录事件，并检测用户是否从任何可疑 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，并将一个**来自可疑 IP 的登录**风险指标条目添加到用户的风险时间线中。

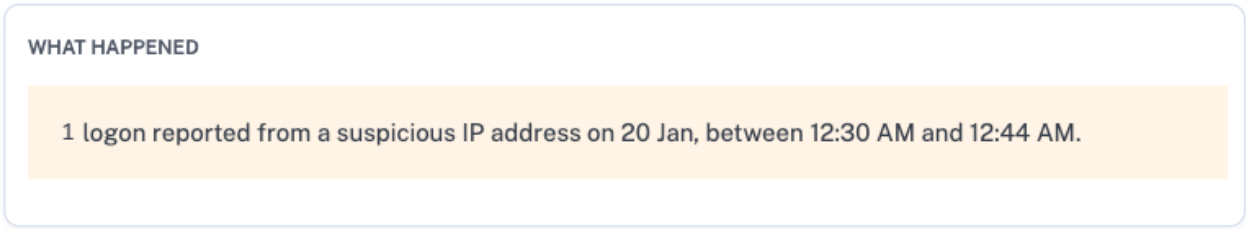
如何分析来自可疑 IP 的登录风险指标?

考虑用户 Lemuel，他尝试从 Citrix Analytics 识别为可疑的 IP 地址访问网络。Citrix Gateway 将登录事件报告给 Citrix Analytics，后者为 Lemuel 分配了更新的风险评分。**来自可疑 IP 的登录**风险指标已添加到 Lemuel Kildow 的风险时间线中。



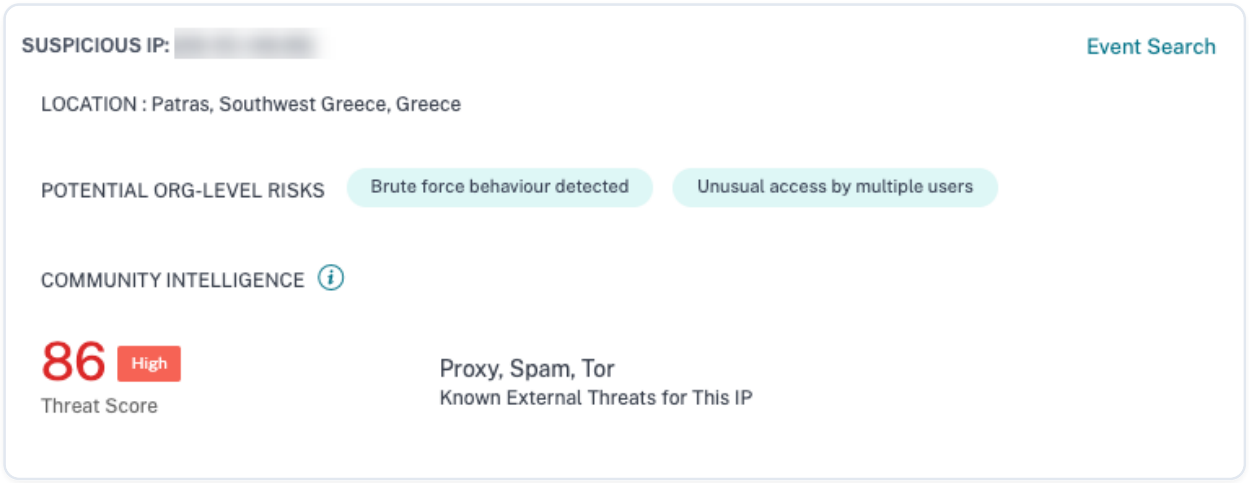
要查看为用户报告的来自可疑 IP 的登录风险指标，请导航到**安全** > **用户**，然后选择该用户。从 Lemuel Kildow 的风险时间线中，您可以选择为该用户报告的最新**来自可疑 IP 的登录**风险指标。当您从时间线中选择**来自可疑 IP 的登录**风险指标条目时，右侧窗格中会显示相应的详细信息面板。

- **发生了什么**部分提供了来自可疑 IP 的登录风险指标的简要摘要。并且，包括在选定期间报告的来自可疑 IP 地址的登录次数。

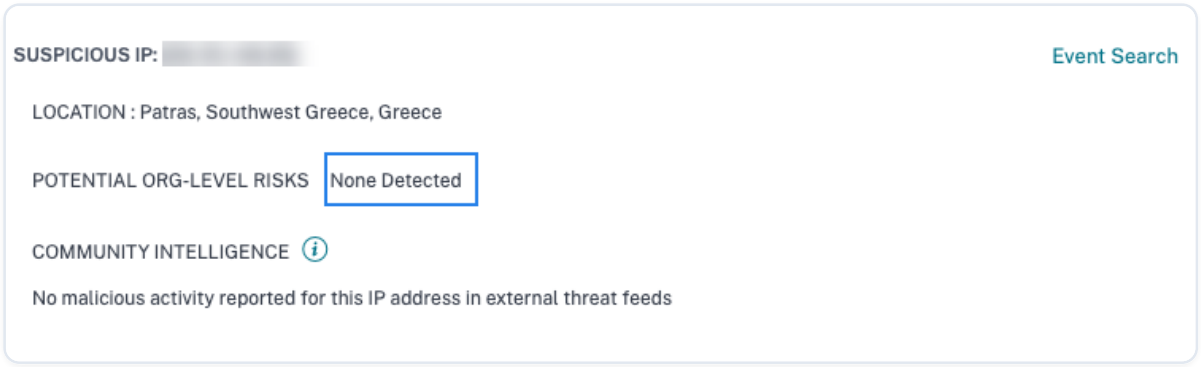
- **可疑 IP** 部分提供以下信息：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



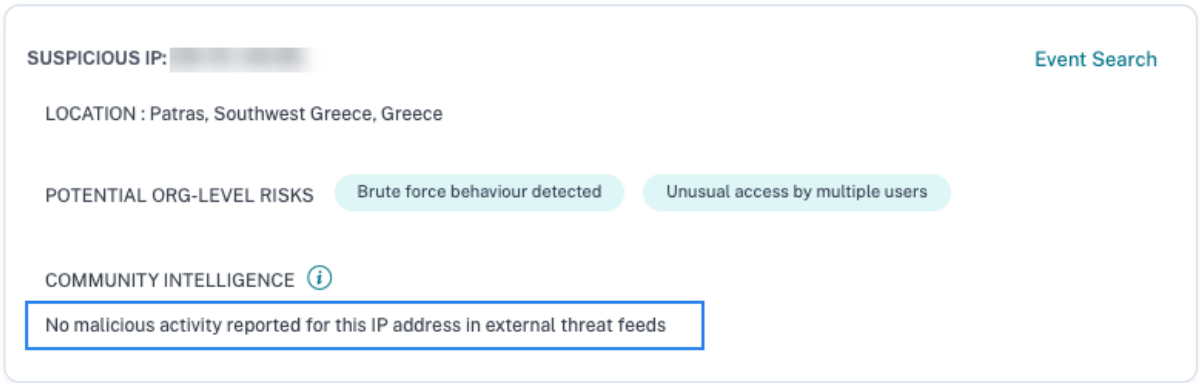
- **可疑 IP**。与可疑登录活动关联的 IP 地址。
- **位置**。用户的城市、地区和国家/地区。这些位置根据数据的可用性显示。
- **潜在的组织级别风险**。指示 Citrix Analytics 最近在您的组织中检测到的任何可疑 IP 活动模式。风险模式包括与潜在暴力破解尝试一致的过多登录失败以及多个用户的不寻常访问。

  如果在您的组织中未检测到 IP 地址的风险模式，您将看到以下消息。

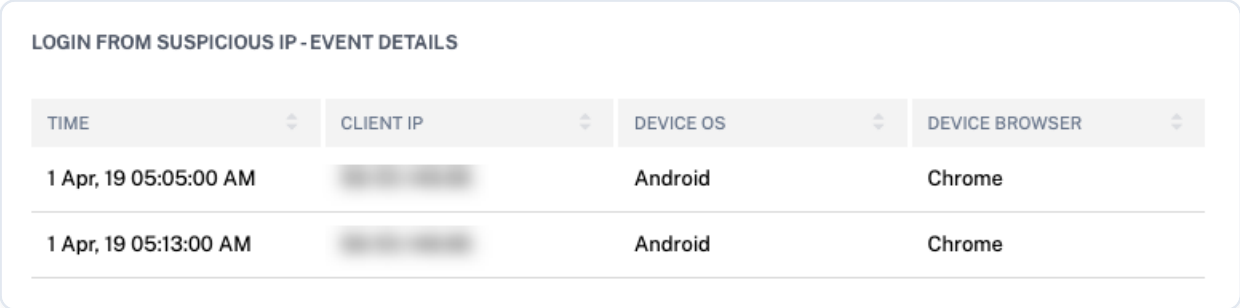
- **社区情报**。提供在外部 IP 威胁情报源中被识别为高风险的 IP 地址的威胁评分和威胁类别。Citrix Analytics 会为高风险 IP 地址分配风险评分。风险评分从 80 开始。

  如果 IP 地址在外部 IP 威胁情报源上没有可用的威胁情报，您会看到以下消息。

- **事件详细信息**部分提供有关可疑登录活动的以下信息：

© 1997–2026 Citrix Systems, Inc. All rights reserved.


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。

您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到监视列表**。当您想要监视用户以防范未来潜在威胁时，可以将其添加到监视列表。
- **通知管理员**。当用户帐户上出现任何异常或可疑活动时，电子邮件通知将发送给所有或选定的管理员。
- **注销用户**。当用户从其帐户注销时，他们无法通过 Citrix Gateway 访问任何资源，直到 Citrix Gateway 管理员清除“注销用户”操作。
- **锁定用户**：当用户帐户因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 Gateway 管理员解锁帐户。

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是什么，都可以应用与其他数据源相关的操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

可疑登录

注意

- 此风险指示器取代了“从异常位置访问”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 根据多个上下文因素检测用户看起来异常或有风险的登录，这些因素由用户使用的设备、位置和网络共同定义。

何时触发“可疑登录”风险指示器？

风险指示器由以下因素组合触发，其中每个因素都根据一个或多个条件被视为可能可疑。

因素	条件
异常设备	用户从签名与过去 30 天内使用的设备不同的设备登录。设备签名基于设备的操作系统和使用的浏览器。
异常位置	用户在过去 30 天内未曾登录过的城市或国家/地区登录。
	该城市或国家/地区在地理位置上远离最近（过去 30 天）的登录位置。
	在过去 30 天内，从该城市或国家/地区登录的用户为零或极少数。
异常网络	用户在过去 30 天内未曾使用过的 IP 地址登录。
	用户在过去 30 天内未曾使用过的 IP 子网登录。
	在过去 30 天内，从该 IP 子网登录的用户为零或极少数。
IP 威胁	该 IP 地址被社区威胁情报源 Webroot 识别为高风险。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

因素	条件
	Citrix Analytics 最近检测到其他用户从该 IP 地址进行的登录活动高度可疑。

如何分析可疑登录风险指标

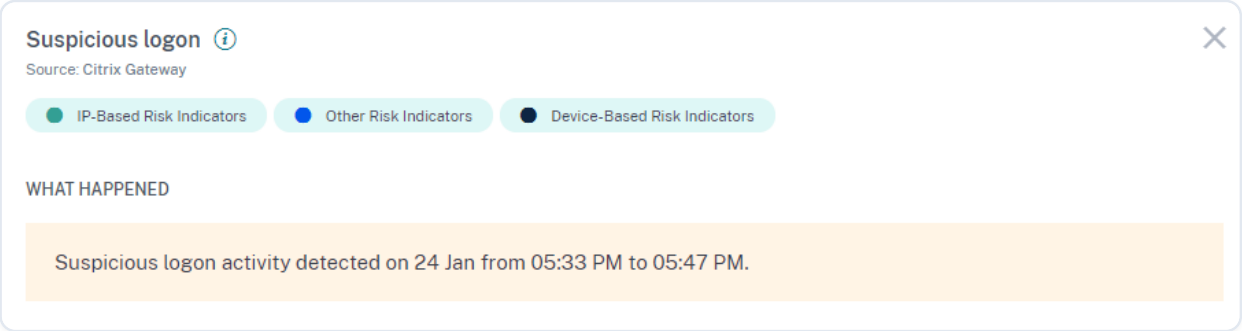
考虑用户 Adam Maxwell，他首次从印度安得拉邦登录。他使用具有已知签名的设备访问组织的资源。但他从一个在过去 30 天内未曾使用过的网络进行连接。

Citrix Analytics 将此登录事件检测为可疑，因为位置和网络因素偏离了他的常规行为，并触发了可疑登录风险指标。该风险指标被添加到 Adam Maxwell 的风险时间线中，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 的风险时间线中，选择**可疑登录**风险指标。您将看到以下信息：

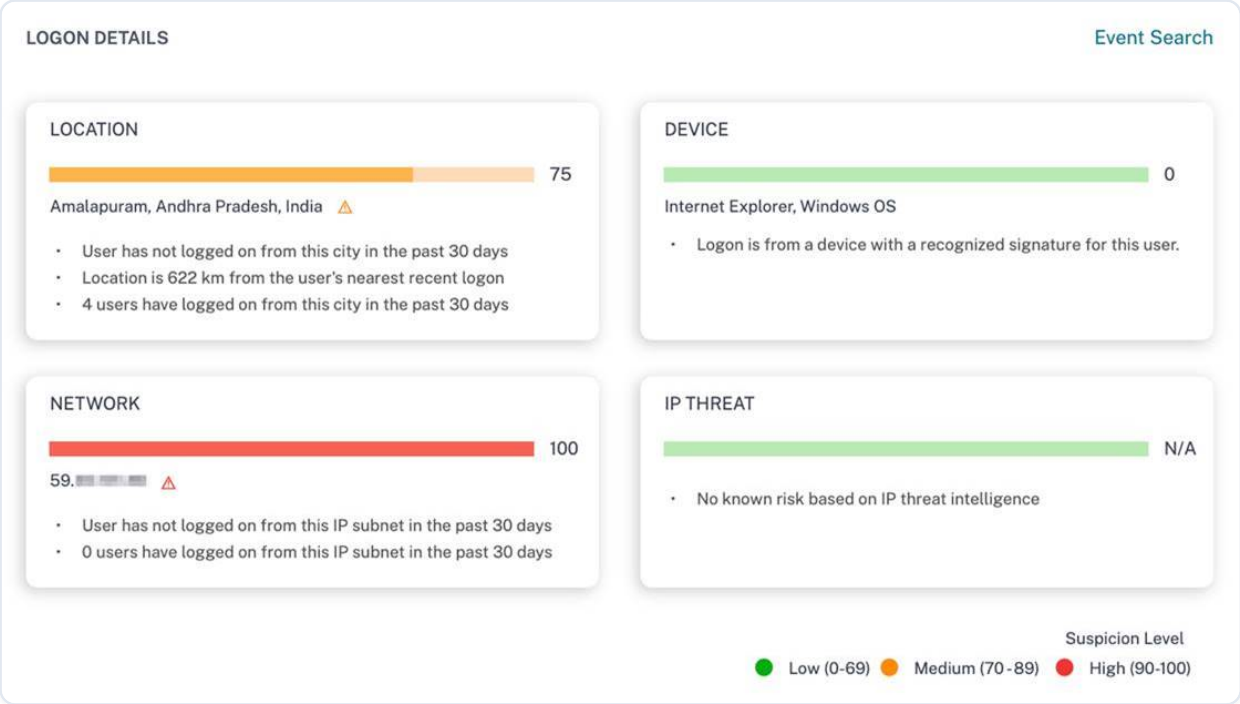
- **发生了什么**部分提供了可疑活动的简要摘要，其中包括风险因素和事件发生时间。



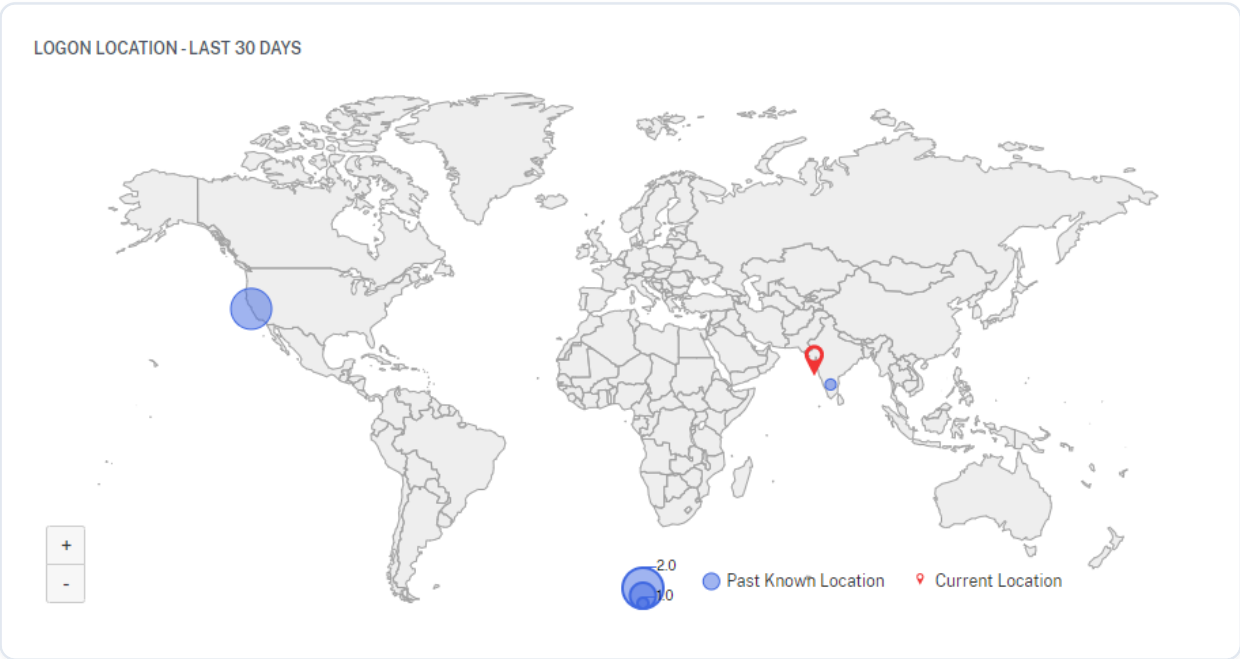
- **登录详细信息**部分提供了与每个风险因素对应的可疑活动的详细摘要。每个风险因素都被分配了一个分数，表示其可疑程度。任何单一风险因素都不表示用户存在高风险。总体风险是基于多个风险因素的关联性。

可疑程度	指示
0–69	该因素看起来正常，不被视为可疑。
70–89	该因素看起来略有异常，与其他因素一起被视为中度可疑。
90–100	该因素是全新的或异常的，与其他因素一起被视为高度可疑。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

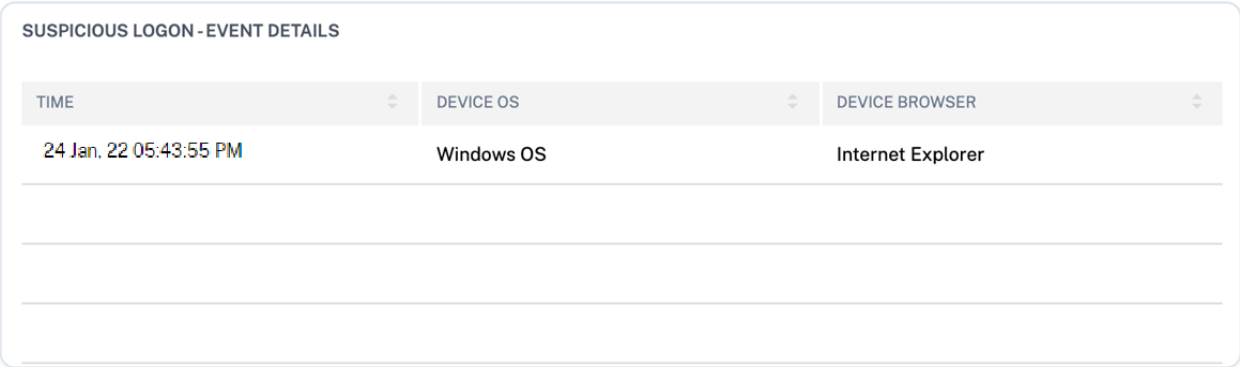


- **登录位置 - 最近 30 天**显示用户最后已知位置和当前位置的地理地图视图。位置数据显示最近 30 天的数据。您可以将鼠标悬停在地图上的指针上，以查看每个位置的总登录次数。



- “**可疑登录 - 事件详细信息**”部分提供有关可疑登录事件的以下信息：
  - **时间**：指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**：指示用于登录 Citrix Gateway 的 Web 浏览器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到观察列表**。当您想要监视用户以防范未来潜在威胁时，可以将其添加到观察列表。
- **通知管理员**。当用户帐户出现任何异常或可疑活动时，会向所有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，他们无法通过 Citrix Gateway 访问任何资源，直到 Citrix Gateway 管理员清除“注销用户”操作。
- **锁定用户**：当用户的帐户因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 Gateway 管理员解锁该帐户。

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。

要手动对用户应用操作，请导航到用户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是什么，都可以应用与其他数据源相关的操作。

异常身份验证失败

当用户从异常 IP 地址登录失败时，Citrix Analytics 会检测到基于访问的威胁并触发相应的风险指标。

与异常身份验证风险指标相关的风险因素是基于登录失败的风险指标。有关风险因素的更多信息，请参阅Citrix 用户风险指标。

异常身份验证失败指标何时触发?

当您组织中的用户从与其通常行为不符的异常 IP 地址登录失败时，您会收到通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

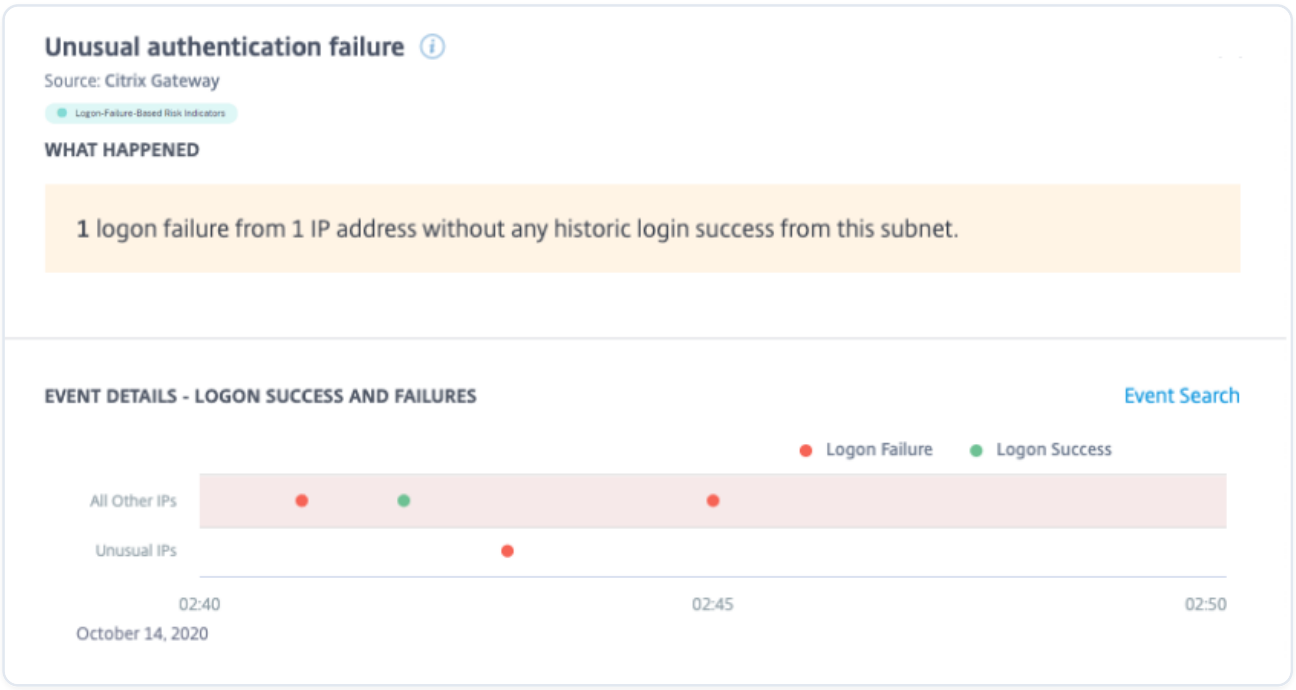
Citrix Gateway 会检测到这些事件并将其报告给 Citrix Analytics。Citrix Analytics 接收这些事件并提高用户的风险评分。**异常身份验证失败**风险指标将添加到用户的风险时间线中。

如何分析异常身份验证失败指标?

考虑用户 Georgina Kalou，她通常从家和办公室网络登录 Citrix Gateway。远程攻击者尝试通过猜测不同密码来验证 Georgina 的帐户，导致从不熟悉的网络进行身份验证失败。

在此场景中，Citrix Gateway 将这些事件报告给 Citrix Analytics，后者会为 Georgina Kalou 分配更新的风险评分。异常身份验证失败风险指标将添加到 Georgina Kalou 的风险时间线中。

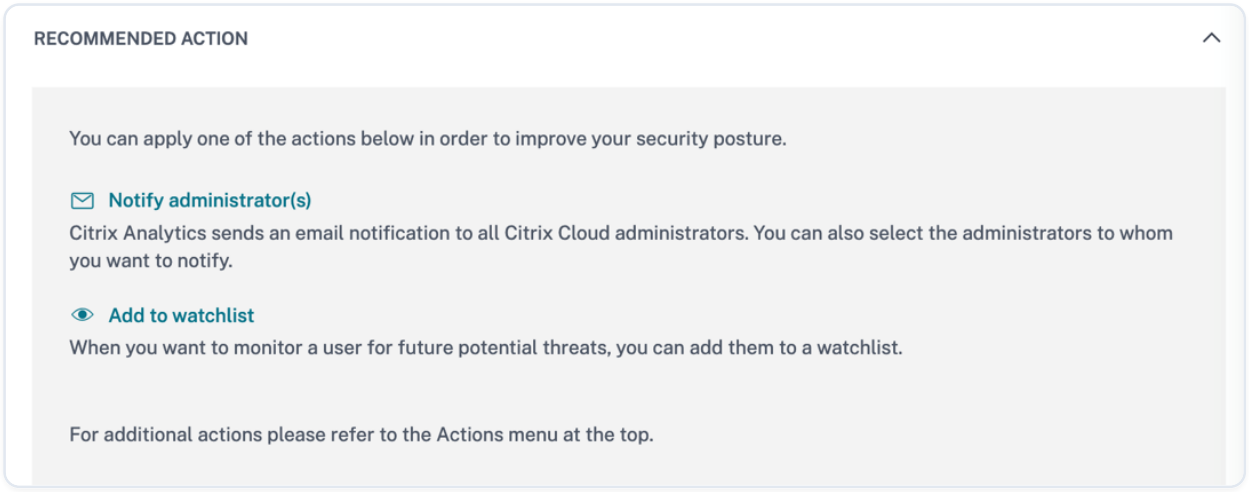
在 Georgina Kalou 的风险时间线中，您可以选择报告的异常身份验证失败风险指标。事件原因以及事件时间、位置等详细信息都会显示。



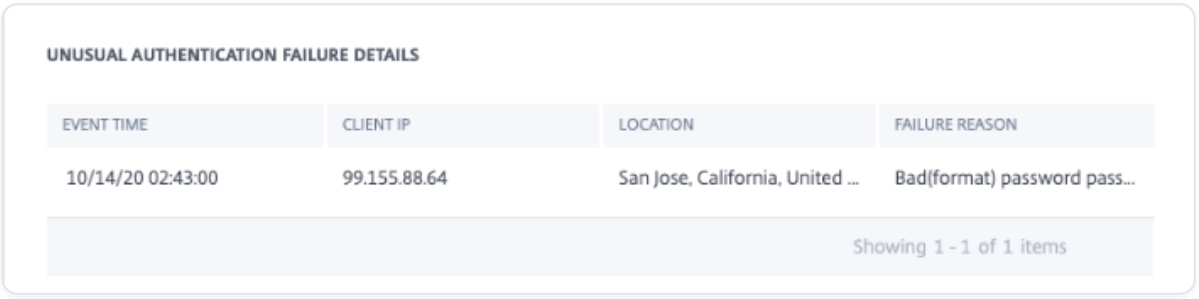
- 在**发生了什么**部分，您可以查看简要摘要，其中包括身份验证失败的总次数和事件发生时间。
- 在**建议操作**部分，您可以找到可应用于风险指标的建议操作。Citrix Analytics for Security™ 根据用户造成的风险严重程度推荐操作。建议可以是以下操作之一或组合：
  - 通知管理员
  - 添加到观察列表
  - 创建策略

  您可以根据建议选择一个操作。或者，您可以从“**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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

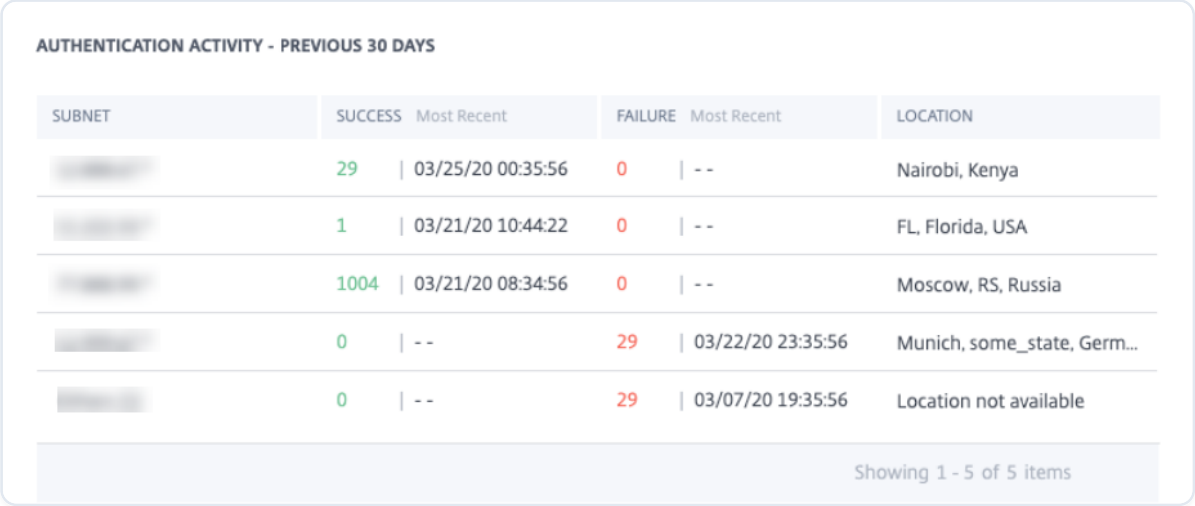


- 在“**事件详细信息 – 登录成功和失败**”部分，您可以查看一个图表，其中显示了异常身份验证失败以及在同一持续时间内检测到的任何其他登录活动。
- 在“**异常身份验证详细信息**”部分，表格提供了有关异常身份验证失败的以下信息：
  - **登录时间** – 事件的日期和时间
  - **客户端 IP** – 用户设备的 IP 地址
  - **位置** – 事件发生的位置
  - **失败原因** – 身份验证失败的原因



- 在“**用户身份验证活动 – 前 30 天**”部分，表格提供了有关用户过去 30 天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 – 成功身份验证事件的总数以及用户最近一次成功事件的时间。
  - 失败 – 失败身份验证事件的总数以及用户最近一次失败事件的时间。
  - 位置 – 身份验证事件发生的位置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到监视列表**。当您希望监视用户以防范未来潜在威胁时，可以将其添加到监视列表。
- **通知管理员**。当用户帐户出现任何异常或可疑活动时，系统会向所有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后，他们将无法通过 Citrix Gateway 访问任何资源，直到 Citrix Gateway 管理员清除“注销用户”操作。
- **锁定用户**：当用户的帐户因异常行为而被锁定时，他们将无法通过 Citrix Gateway 访问任何资源，直到 Gateway 管理员解锁该帐户。

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。

要手动对用户执行操作，请导航到用户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是什么，都可以应用与其他数据源相关的操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

思杰安全私有访问™ 风险指标

危险网站访问

注意

由于 Secure Private Access 弃用了基于类别的 Web 过滤，Citrix Analytics for Security™ 上的以下功能受到影响：

1. URL 的类别组、类别和信誉等数据字段在 Citrix Analytics for Security 控制板上不再可用。
2. 依赖相同数据的危险网站访问指标也已弃用，并且不会为客户触发。
3. 任何使用数据字段（URL 的类别组、类别和信誉）及其相关策略的现有自定义风险指标不再触发。

有关 Secure Private Access 弃用功能的详细信息，请参阅功能弃用。

尝试访问黑名单 URL

Citrix Analytics 根据用户访问的黑名单 URL 检测数据访问威胁，并触发相应的风险指标。

当用户尝试访问 Secure Private Access 中配置的黑名单 URL 时，Citrix Analytics 会报告**尝试访问黑名单 URL** 风险指标。

尝试访问黑名单 URL 风险指标的关联风险因素是其他风险指标。有关风险因素的更多信息，请参阅 Citrix 用户风险指标。

何时触发“尝试访问黑名单 URL”风险指标?

Secure Private Access 包含 URL 分类功能，可提供基于策略的控制以限制对黑名单 URL 的访问。当用户尝试访问黑名单 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**尝试访问黑名单 URL** 风险指标条目添加到用户的风险时间线中。

如何分析“尝试访问黑名单 URL”风险指标?

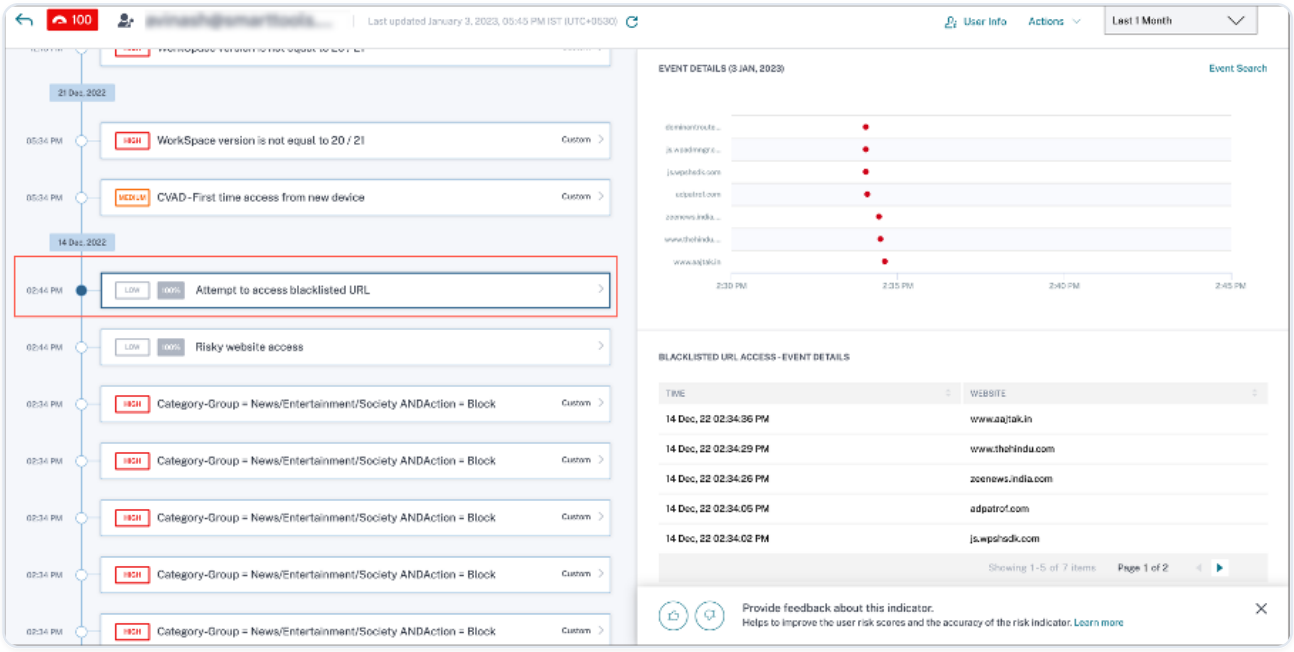
假设用户 Georgina Kalou 访问了 Secure Private Access 中配置的黑名单 URL。Secure Private Access 会向 Citrix Analytics 报告此事件，Citrix Analytics 会为 Georgina Kalou 分配更新的风险评分。**尝试访问黑名单 URL** 风险指标将添加到 Georgina Kalou 的风险时间线中。

从 Georgina Kalou 的风险时间线中，您可以选择报告的 **尝试访问黑名单 URL** 风险指标。事件的原因以及事件的详细信息（例如事件发生时间、网站详细信息）都会显示。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要查看用户的 **尝试访问黑名单 URL** 条目，请导航到 **安全 > 用户**，然后选择该用户。

当您从时间线中选择 **尝试访问黑名单 URL** 风险指标条目时，右侧窗格中会显示相应的详细信息面板。

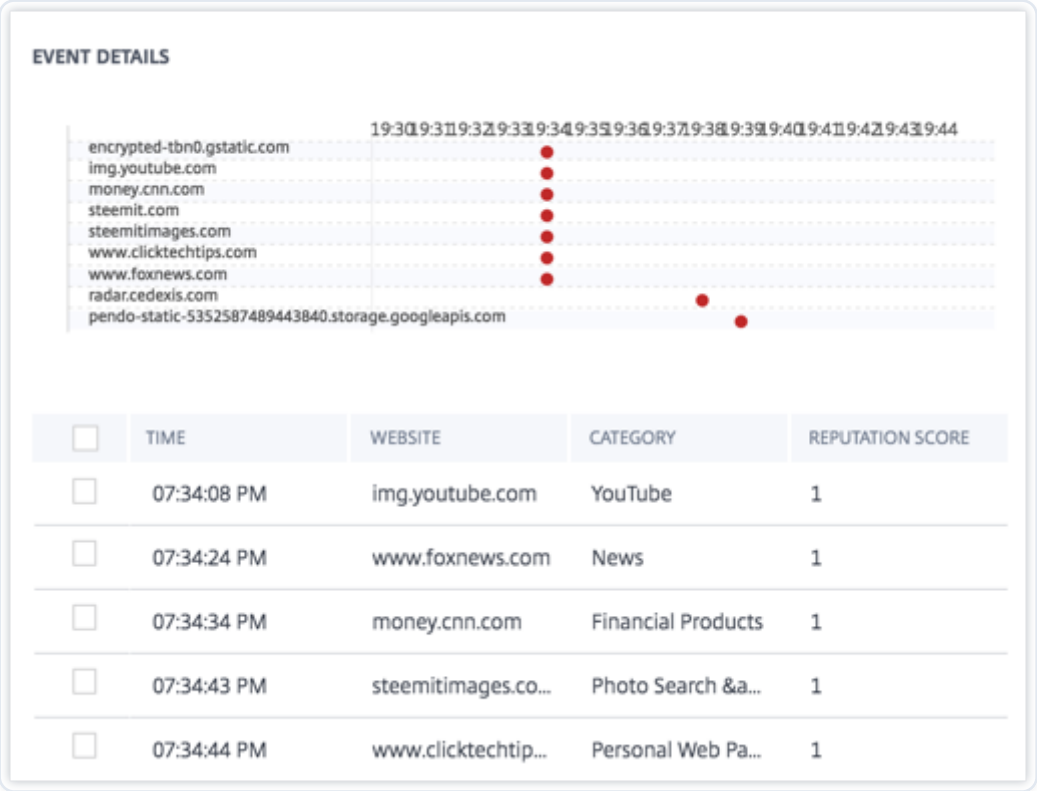


- “**发生了什么**”部分提供了风险指标的简要摘要。它包括用户在选定期间访问的黑名单 URL 的详细信息。



- “**事件详细信息**”部分包含在选定时间段内发生的各个事件的时间线可视化。此外，您还可以查看每个事件的以下关键信息：
  - **时间**。事件发生的时间。
  - **网站**。用户访问的风险网站。
  - **类别**。Secure Private Access 为黑名单 URL 指定的类别。
  - **信誉评级**。Secure Private Access 为黑名单 URL 返回的信誉评级。有关更多信息，请参阅 URL 信誉评分。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到监视列表**。当您希望监视用户以防范未来潜在威胁时，可以将其添加到监视列表。
- **通知管理员**。当用户的帐户出现任何异常或可疑活动时，电子邮件通知会发送给所有或选定的管理员。

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是什么，都可以应用与其他数据源相关的操作。

异常上传量

Citrix Analytics 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数据时，会报告“**异常上传量**”风险指示器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

何时触发异常上传量风险指示器?

您可以配置 Secure Private Access 以监控用户活动，例如访问恶意、危险或未知网站、消耗的带宽以及有风险的下载和上传。当组织中的用户将数据上传到应用程序或网站时，Secure Private Access 会将这些事件报告给 Citrix Analytics。

Citrix Analytics 监控所有这些事件，如果确定此用户活动与用户的常规行为不符，则会更新用户的风险评分。“**异常上传量**”风险指示器将添加到用户的风险时间线中。

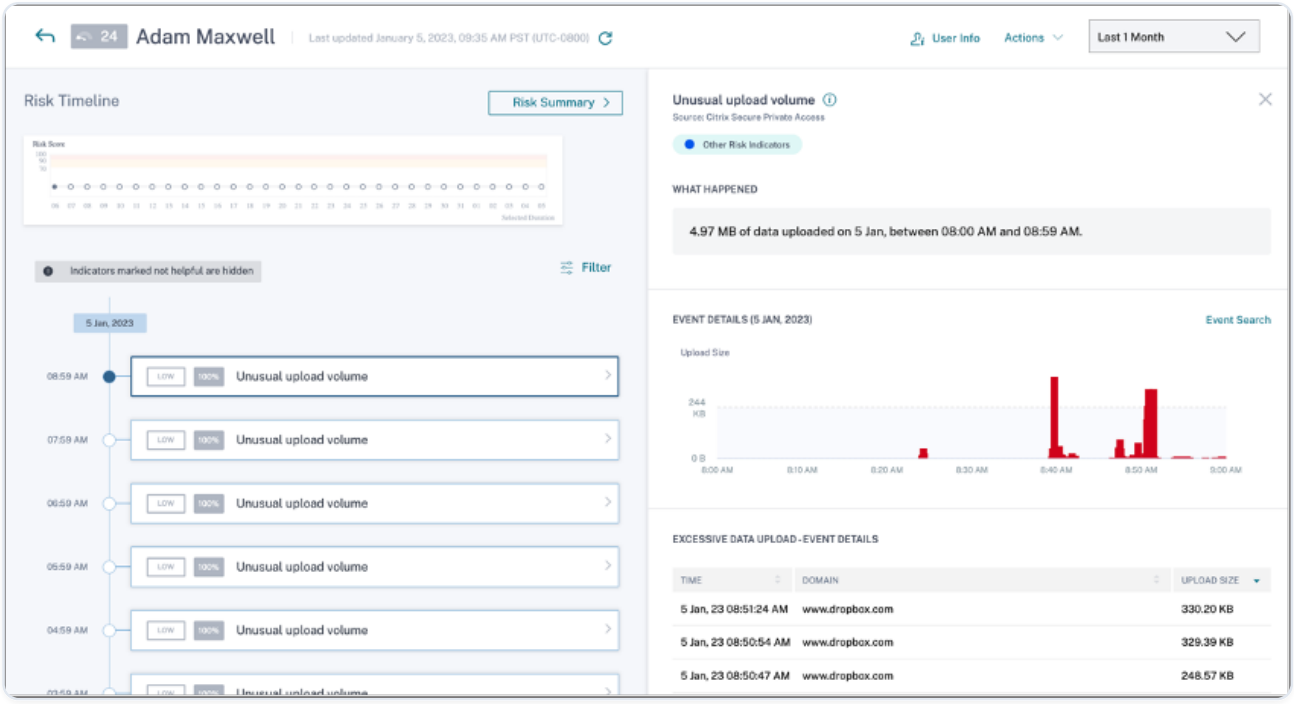
如何分析异常上传量风险指示器?

假设用户 Adam Maxwell 向应用程序或网站上传了过量数据。Secure Private Access 会将这些事件报告给 Citrix Analytics，后者会为 Adam Maxwell 分配更新的风险评分。“**异常上传量**”风险指示器将添加到 Adam Maxwell 的风险时间线中。

在 Adam Maxwell 的风险时间线中，您可以选择报告的“**异常上传量**”风险指示器。事件原因以及事件详细信息（例如事件时间和域）都会显示。

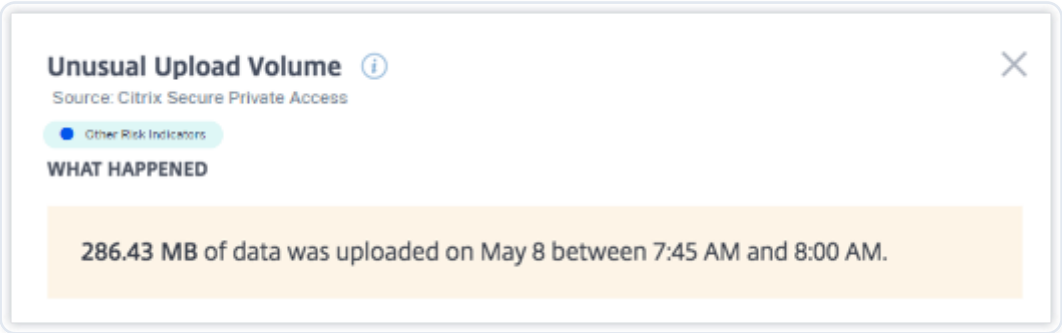
要查看**异常上传量**风险指标，请导航到**安全 > 用户**，然后选择该用户。

当您从时间线中选择**异常上传量**风险指标条目时，右侧窗格中会显示相应的详细信息面板。

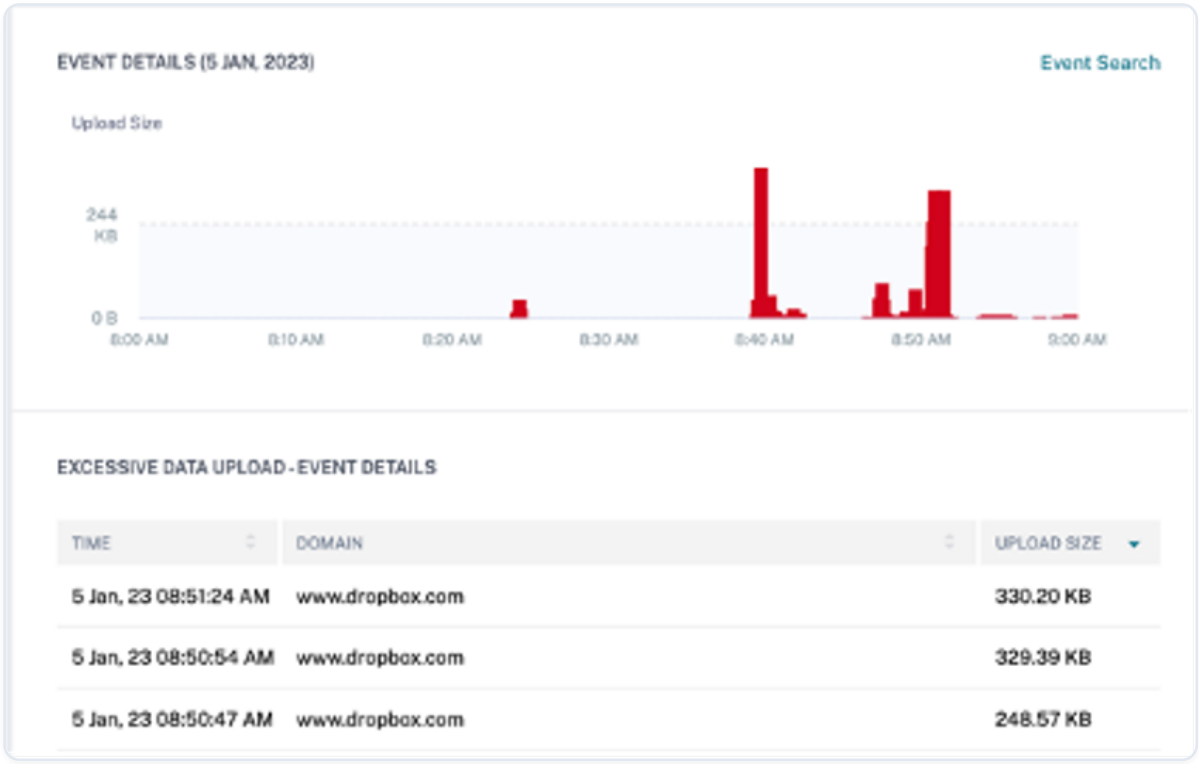


- **发生了什么**部分提供了风险指标的简要摘要，包括所选期间上传的数据量。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **事件详细信息**部分包括所选时间段内发生的单个数据上传事件的时间线可视化。此外，您还可以查看每个事件的以下关键信息：
  - **时间**。将过量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。



您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到监视列表**。当您想要监视用户以防范未来潜在威胁时，可以将其添加到监视列表。
- **通知管理员**。当用户帐户上出现任何异常或可疑活动时，会向所有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它们的更多信息，请参阅策略和操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要手动将操作应用于用户，请导航到用户配置文件并选择相应的风险指标。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是什么，都可以应用与其他数据源相关的操作。

数据下载过多

Citrix Analytics 根据用户在您的网络中下载的过多数据检测数据访问威胁，并触发相应的风险指标。

当您组织中的用户从应用程序或网站下载过量数据时，会报告此风险指标。

何时触发数据下载过多风险指标?

您可以配置 Secure Private Access 来监控用户活动，例如访问恶意、危险或未知网站、消耗的带宽以及有风险的下载和上传。当您组织中的用户从应用程序或网站下载数据时，Secure Private Access 会将这些事件报告给 Citrix Analytics。

Citrix Analytics 监控所有这些事件，如果它确定用户活动与用户的常规行为不符，它会更新用户的风险评分。数据下载过多风险指标将添加到用户的风险时间线中。

与数据下载过多风险指标相关的风险因素是其他风险指标。有关风险因素的更多信息，请参阅Citrix 用户风险指标。

如何分析数据下载过多风险指标?

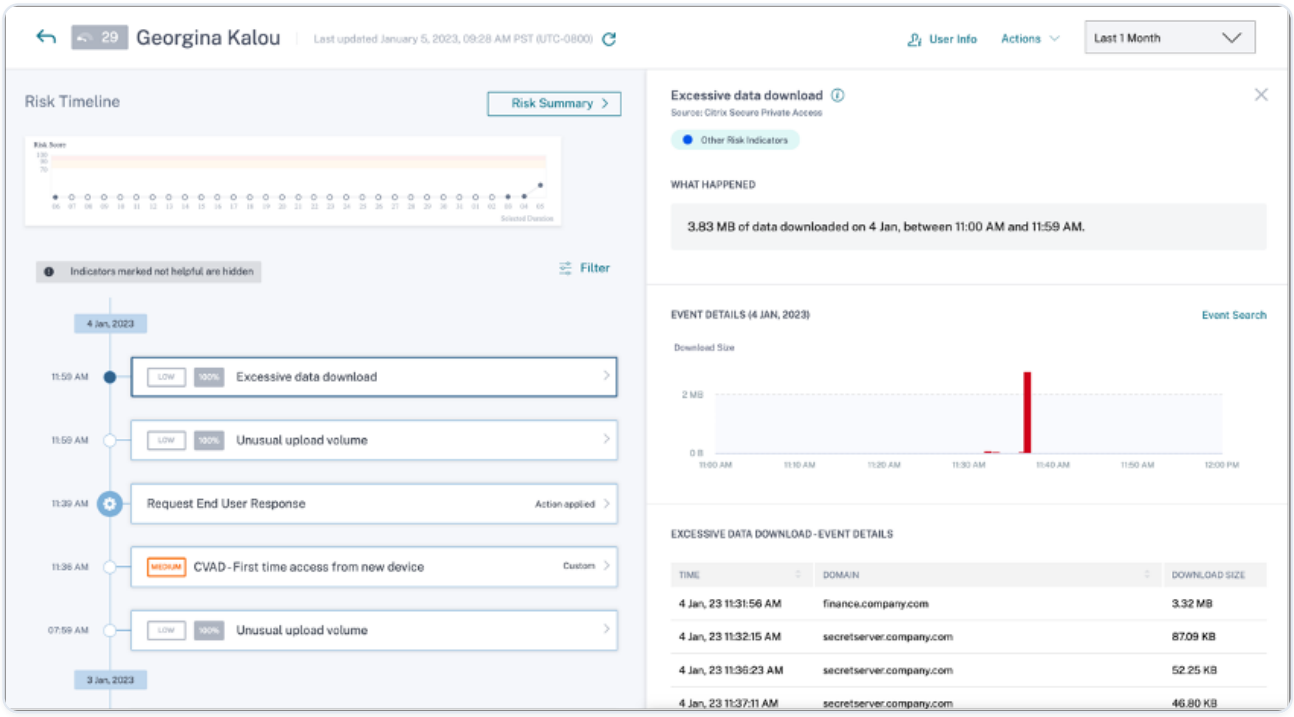
假设用户 Georgina Kalou 从应用程序或网站下载了过量数据。Secure Private Access 会将这些事件报告给 Citrix Analytics，后者会为 Georgina Kalou 分配更新的风险评分，并将**数据下载过多**风险指标条目添加到用户的风险时间线中。

从 Georgina Kalou 的风险时间线中，您可以选择报告的**数据下载过多**风险指标。事件的原因以及事件的详细信息（例如时间域详细信息）都会显示。

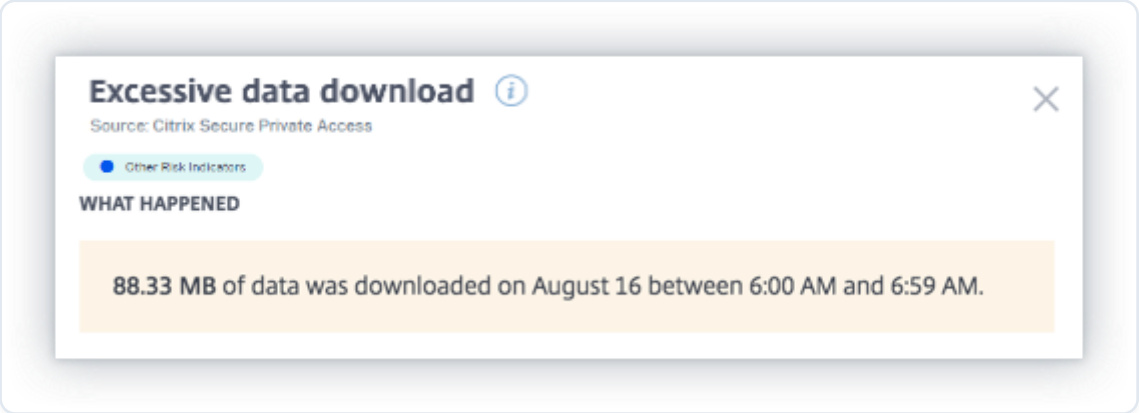
要查看**数据下载过多**风险指标，请导航到**安全 > 用户**，然后选择该用户。

当您从时间线中选择**数据下载过多**风险指标条目时，右侧窗格中会显示相应的详细信息面板。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

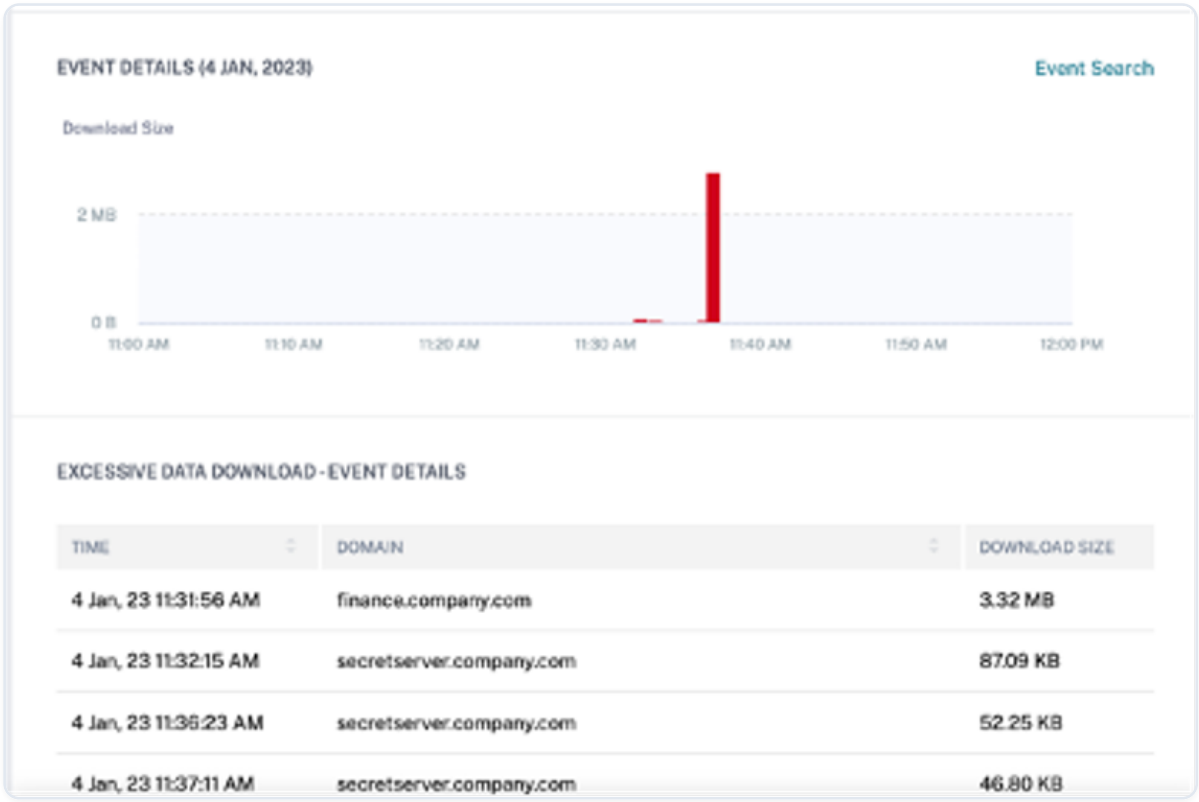


- **发生了什么**部分提供了风险指标的简要摘要，包括在选定期间上传/下载的数据量。



- **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线可视化。此外，您可以查看每个事件的以下关键信息：
  - **时间**。数据下载量过大到应用程序或网站的时间。
  - **域**。用户下载数据的域。
  - **下载大小**。下载到该域的数据量。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到监视列表**。当您想要监视用户以防范未来潜在威胁时，可以将其添加到监视列表。
- **通知管理员**。当用户帐户出现任何异常或可疑活动时，系统会向所有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。

要手动对用户执行操作，请导航到用户配置文件并选择相应的风险指标。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是什么，都可以应用与其他数据源相关的操作。

Citrix 虚拟应用和桌面™ 和 Citrix DaaS 风险指标

不可能的行程

当用户连续两次登录来自两个不同国家，且两次登录之间的时间间隔小于两国之间预期的旅行时间时，Citrix Analytics 会将用户的登录检测为高风险。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

不可能的行程时间场景表明存在以下风险：

- **凭据泄露**：远程攻击者窃取了合法用户的凭据。
- **共享凭据**：不同用户正在使用相同的用户凭据。

何时会触发“不可能的行程”风险指标？

不可能的行程风险指标会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给定时间内可能旅行的距离时触发。

注意

此风险指标还包含用于减少以下不反映用户实际位置的场景的误报警报的逻辑：

- 当用户通过代理连接登录虚拟应用程序和桌面时。
- 当用户通过托管客户端登录虚拟应用程序和桌面时。

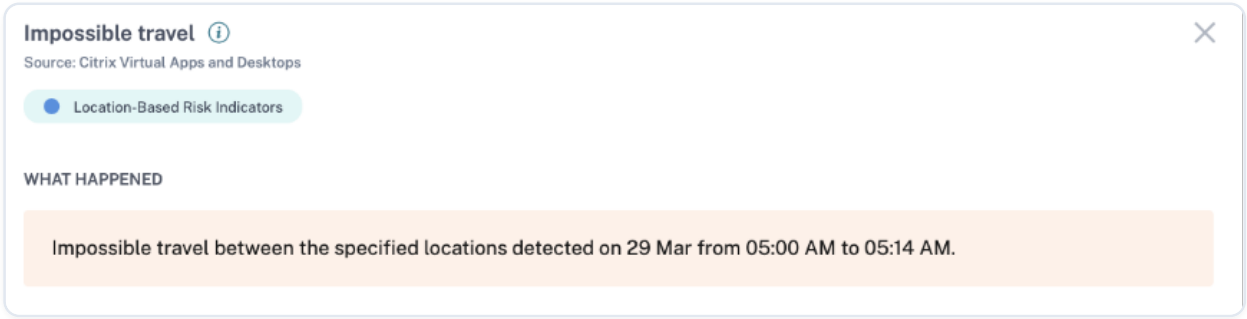
如何分析“不可能的行程”风险指标

考虑用户 Adam Maxwell，他在一分钟内从两个位置登录：俄罗斯莫斯科和中国呼和浩特。Citrix Analytics 会将此登录事件检测为不可能的行程场景，并触发**不可能的行程**风险指标。该风险指标会添加到 Adam Maxwell 的风险时间线中，并为其分配风险评分。

要查看 Adam Maxwell 的风险时间线，请选择“**安全 > 用户**”。在“**高风险用户**”窗格中，选择用户 Adam Maxwell。

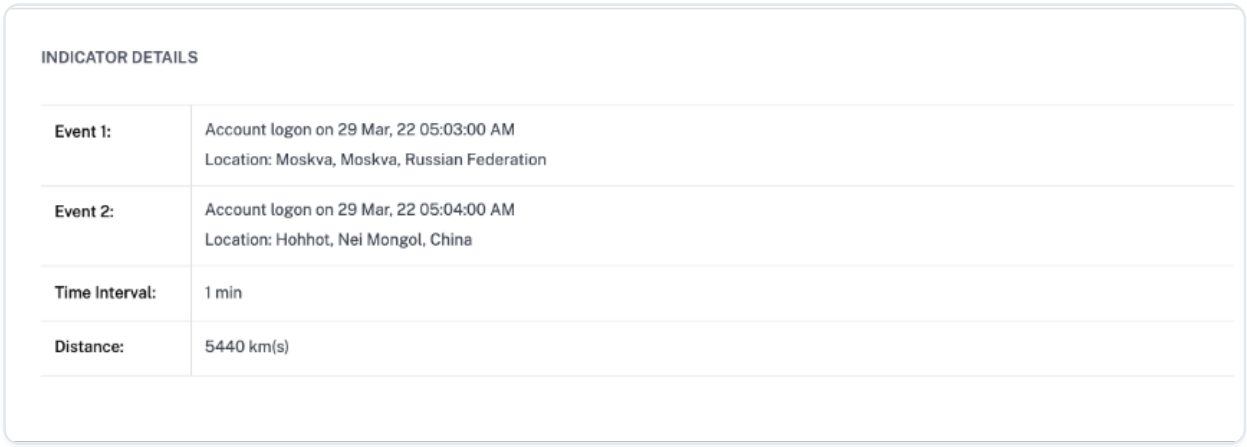
从 Adam Maxwell 的风险时间线中，选择**不可能的行程**风险指标。您可以查看以下信息：

- **发生了什么**部分提供了不可能的行程事件的简要摘要。

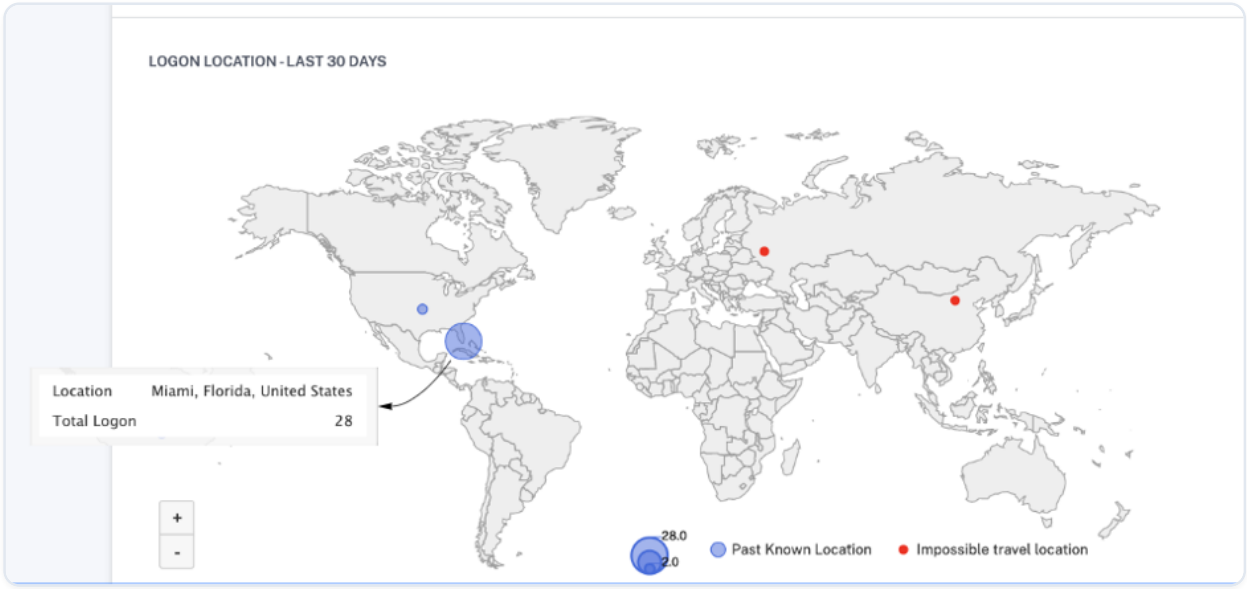


- **指标详细信息**部分提供了用户登录的位置、连续登录之间的时间间隔以及两个位置之间的距离。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

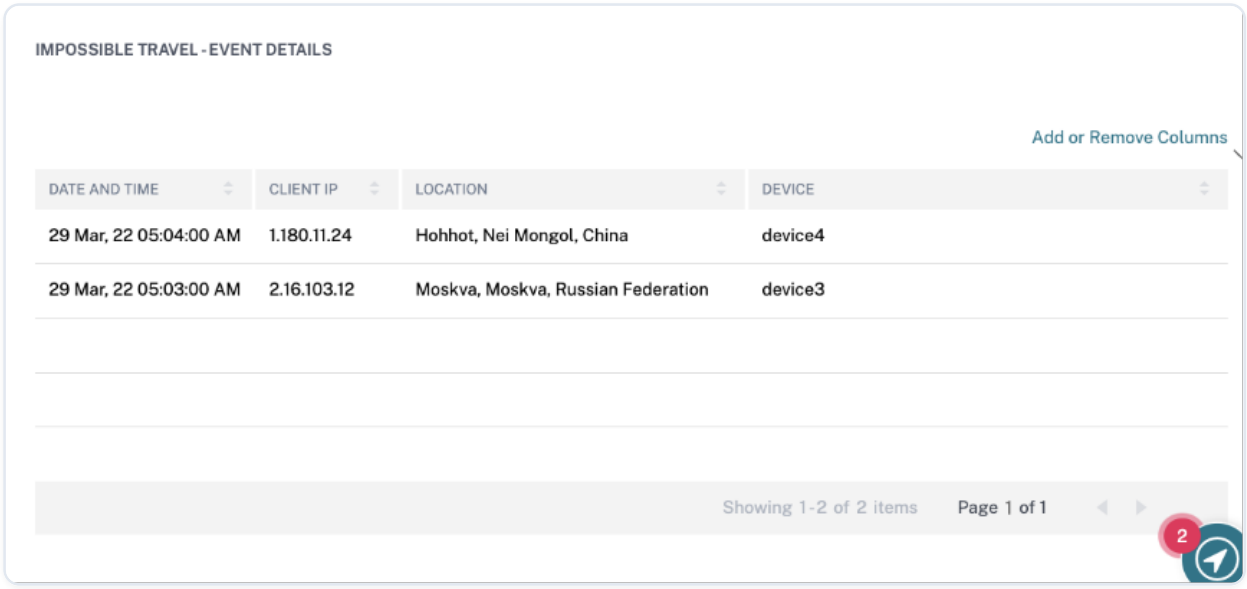


- **登录位置 - 最近 30 天**部分显示了不可能的行程位置和用户已知位置的地理地图视图。位置数据显示最近 30 天的数据。您可以将鼠标悬停在地图上的指针上，以查看每个位置的总登录次数。



- **不可能的行程 - 事件详细信息**部分提供了有关不可能的行程事件的以下信息：
  - **日期和时间**：指示登录的日期和时间。
  - **客户端 IP**：指示用户设备的 IP 地址。
  - **位置**：指示用户登录的位置。
  - **设备**：指示用户的设备名称。
  - **登录类型**：指示用户活动是会话登录还是帐户登录。当用户对其帐户的身份验证成功时，会触发帐户登录事件。而当用户输入其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。
  - **操作系统**：指示用户设备的操作系统。
  - **浏览器**：指示用于访问应用程序的 Web 浏览器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到监视列表**。当您想要监视用户以防范未来潜在威胁时，可以将其添加到监视列表。
- **通知管理员**。当用户帐户出现任何异常或可疑活动时，系统会向所有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，他们无法通过 Virtual Desktops 访问资源。
- **开始会话录制**。如果用户的 Virtual Desktops 帐户出现异常事件，管理员可以开始录制用户未来登录会话的活动。但是，如果用户使用的是 Citrix Virtual Apps and Desktops 7.18 或更高版本，管理员可以动态启动和停止录制用户当前的登录会话。

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。

要手动对用户应用操作，请导航到用户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是什么，都可以应用与其他数据源相关的操作。

潜在数据泄露

Citrix Analytics 根据过多的数据泄露尝试检测数据威胁，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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

当 Citrix Receiver 用户尝试将文件下载或传输到驱动器或打印机时，会触发“**潜在数据泄露**”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。数据也可以通过剪贴板或复制粘贴操作进行泄露。

注意

剪贴板操作仅由 SaaS 应用程序支持。

潜在数据泄露风险指标何时触发?

当用户在特定时间段内向驱动器或打印机传输了过多的文件时，您会收到通知。当用户在其本地计算机上使用复制粘贴操作时，也会触发此风险指标。

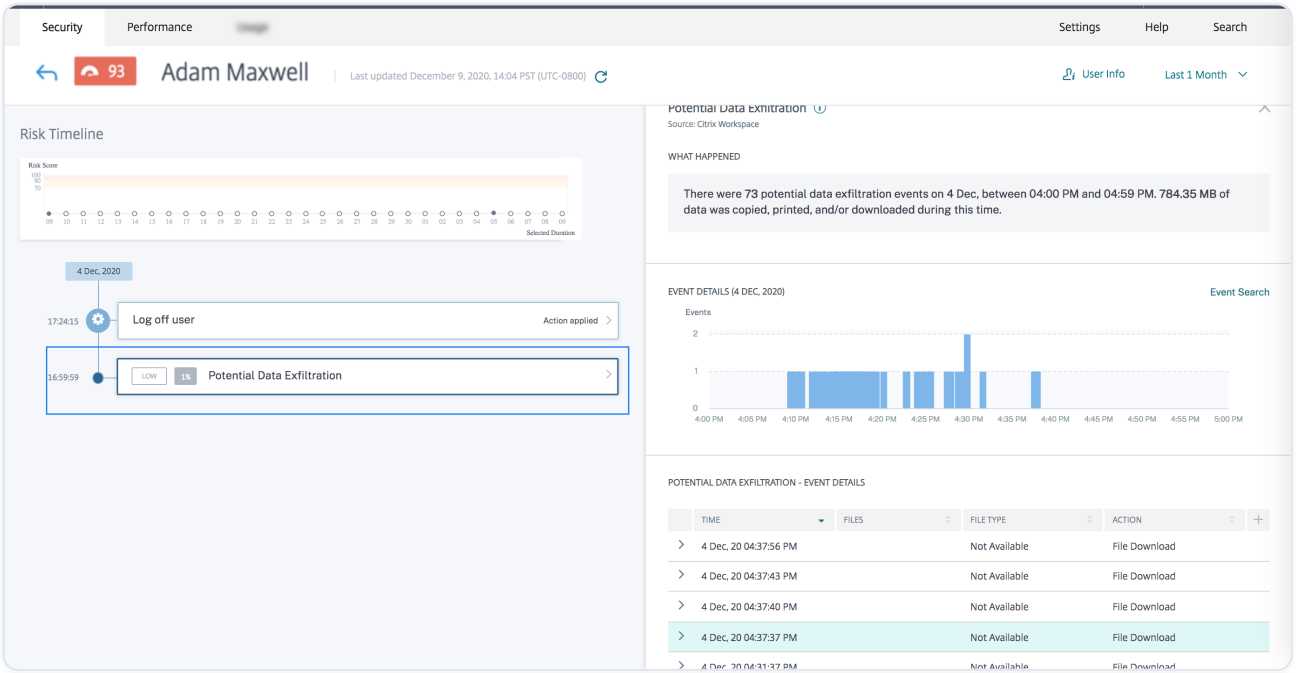
当 Citrix Receiver 检测到此行为时，Citrix Analytics 会收到此事件并为相应用户分配风险评分。**潜在数据泄露**风险指标将添加到用户的风险时间线中。

如何分析潜在数据泄露风险指标?

以用户 Adam Maxwell 为例，他登录到一个会话并尝试打印超出预定义限制的文件。通过此操作，Adam Maxwell 基于机器学习算法超出了其正常的文件传输行为。

在 Adam Maxwell 的时间线中，您可以选择**潜在数据泄露**风险指标。事件原因会与详细信息一起显示，例如传输的文件和用于传输文件的设备。

要查看为用户报告的**潜在数据泄露**风险指标，请导航到**安全 > 用户**，然后选择该用户。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **发生了什么**部分，您可以查看潜在数据泄露事件的摘要。您可以查看特定时间段内数据泄露事件的数量。

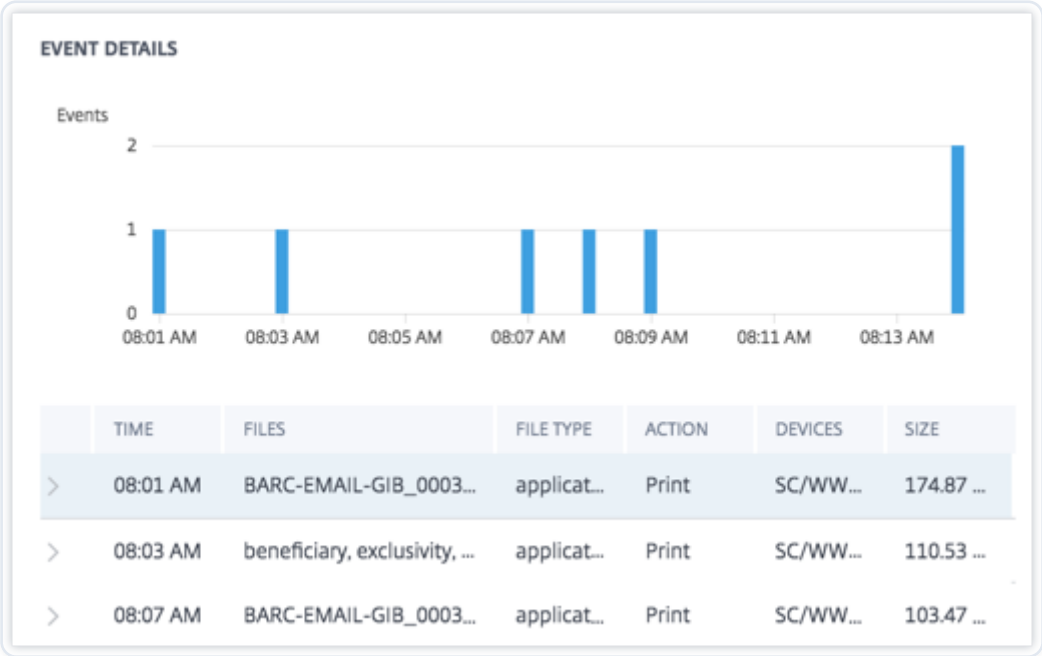


- **事件详细信息**部分，数据泄露尝试以图形和表格形式显示。事件在图中显示为单独的条目，表格提供以下关键信息：
  - **时间**。数据泄露事件发生的时间。
  - **文件**。已下载、打印或复制的文件。
  - **文件类型**。已下载、打印或复制的文件类型。

    注意

    打印的文件名仅在 SaaS 应用程序打印事件中可用。

  - **操作**。执行的数据外泄事件类型——打印、下载或复制。
  - **设备**。使用的设备。
  - **大小**。外泄文件的大小。
  - **位置**。用户尝试外泄数据的城市。



- 在事件发生期间，您可以在**附加上下文信息**部分查看以下内容：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 已外泄的文件数量。
- 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?

您可以对用户帐户执行以下操作：

- **添加到监视列表**。当您想要监视用户以防范未来潜在威胁时，可以将其添加到监视列表。
- **通知管理员**。当用户帐户上出现任何异常或可疑活动时，系统会向所有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上发生异常事件，管理员可以开始录制用户未来登录会话的活动。但是，如果用户使用的是 Citrix Virtual Apps and Desktops 7.18 或更高版本，管理员可以动态启动和停止录制用户当前的登录会话。

要了解有关操作以及如何手动配置它们的更多信息，请参阅策略和操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要手动将操作应用于用户，请导航到用户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是什么，都可以应用与其他数据源相关的操作。

可疑登录

Citrix Analytics 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）检测用户显示异常或有风险的登录。

何时触发可疑登录风险指示器?

风险指示器由以下因素组合触发，其中每个因素都根据一个或多个条件被视为潜在可疑。

因素	条件
异常设备	用户从过去 30 天内未使用的设备登录。
	用户从虚拟应用和桌面服务器未管理的设备登录。
	用户从 HTML5 客户端或 Chrome 客户端登录，其中设备签名与用户的历史记录不一致。
异常位置	从用户过去 30 天内未登录过的城市或国家/地区登录。
	该城市或国家/地区在地理上与最近（过去 30 天）的登录位置相距遥远。
	过去 30 天内，从该城市或国家/地区登录的用户为零或极少。
异常网络	从用户过去 30 天内未使用的 IP 地址登录。
	从用户过去 30 天内未使用的 IP 子网登录。
	过去 30 天内，从该 IP 子网登录的用户为零或极少。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

因素	条件
IP 威胁	该 IP 地址被社区威胁情报源 Webroot 识别为高风险。
	Citrix Analytics 最近检测到其他用户从该 IP 地址进行的极度可疑的登录活动。

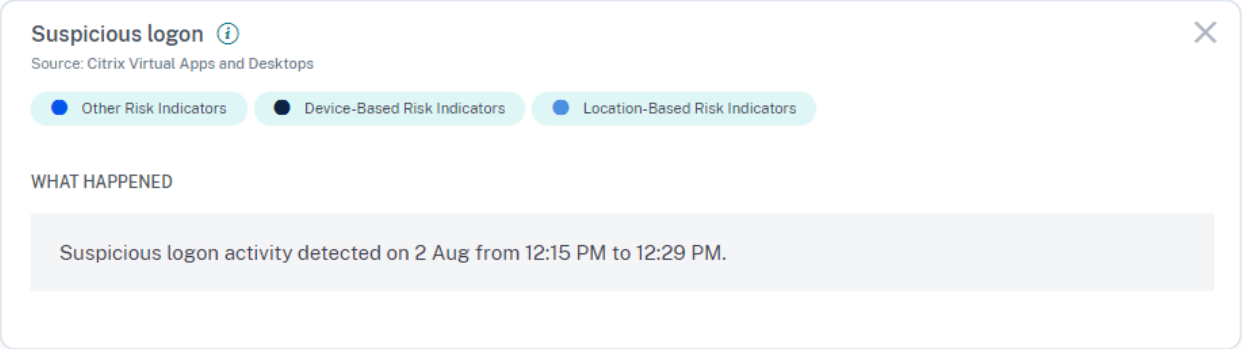
如何分析可疑登录风险指标

假设用户 Adam Maxwell 首次从印度孟买登录。他使用新设备或过去 30 天内未使用的设备登录 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、设备和网络等因素偏离了他的常规行为，并触发了**可疑登录**风险指标。该风险指标将添加到 Adam Maxwell 的风险时间线中，并为其分配风险评分。

要查看 Adam Maxwell 的风险时间，请选择 **安全 > 用户**。从**有风险的用户**窗格中，选择用户 Adam Maxwell。

从 Adam Maxwell 的风险时间线中，选择可疑登录风险指标。您可以查看以下信息：

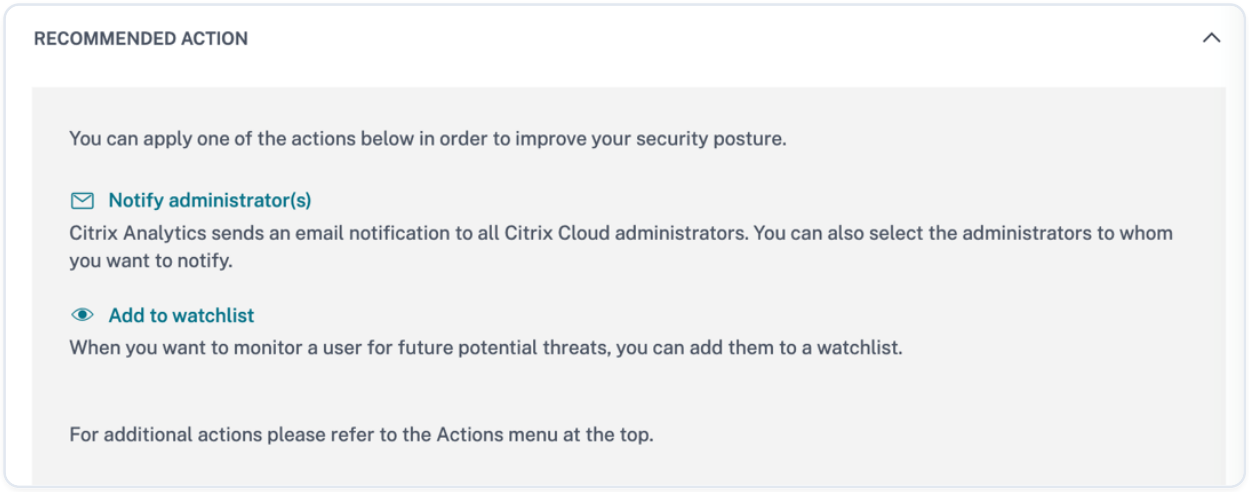
- **发生了什么**部分提供了可疑活动的简要摘要，其中包括风险因素和事件发生时间。



- 在**建议操作**部分中，您可以找到可应用于风险指标的建议操作。Citrix Analytics for Security™ 根据用户造成的风险严重程度推荐操作。建议可以是以下操作之一或组合：
  - 通知管理员
  - 添加到监视列表
  - 创建策略

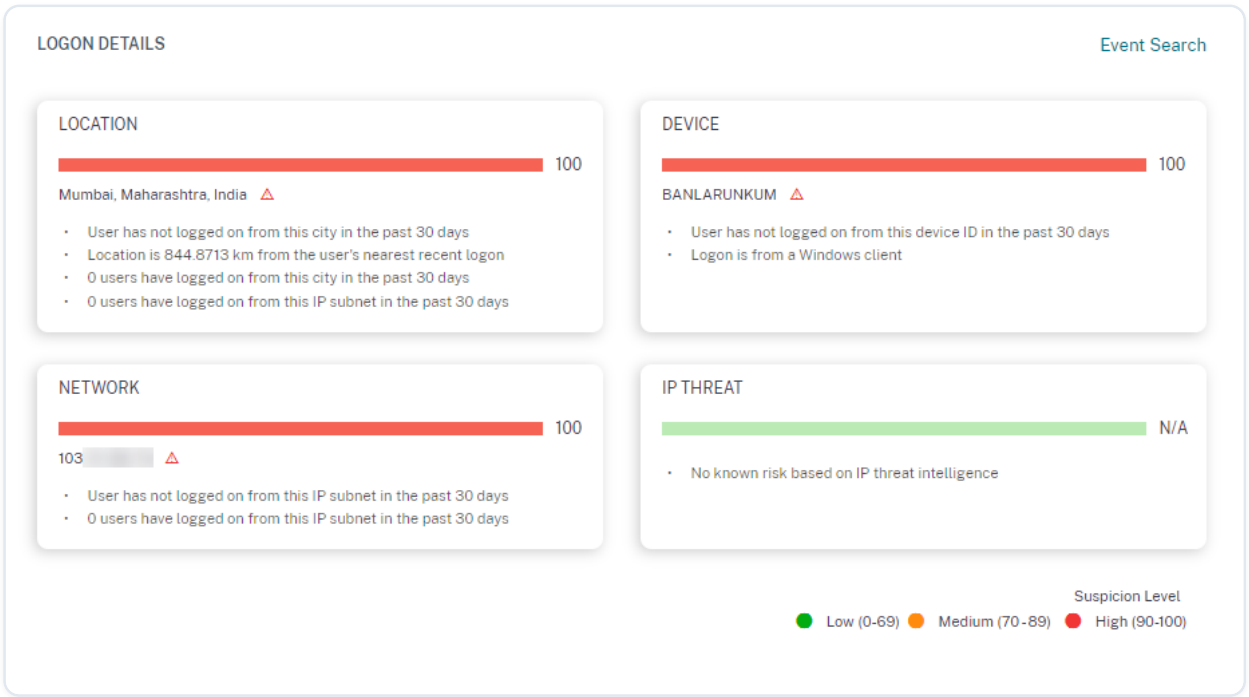
  您可以根据建议选择一个操作。或者，您可以根据自己的选择从**操作**菜单中选择要应用的操作。有关详细信息，请参阅手动应用操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **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。每个风险因素都分配有一个分数，表示可疑程度。任何单个风险因素都不表示用户存在高风险。总体风险基于多个风险因素的关联。

可疑程度	指示
0–69	该因素看起来正常，不被认为是可疑的。
70–89	该因素看起来略有异常，与其他因素一起被认为是中度可疑的。
90–100	该因素是全新的或异常的，与其他因素一起被认为是高度可疑的。



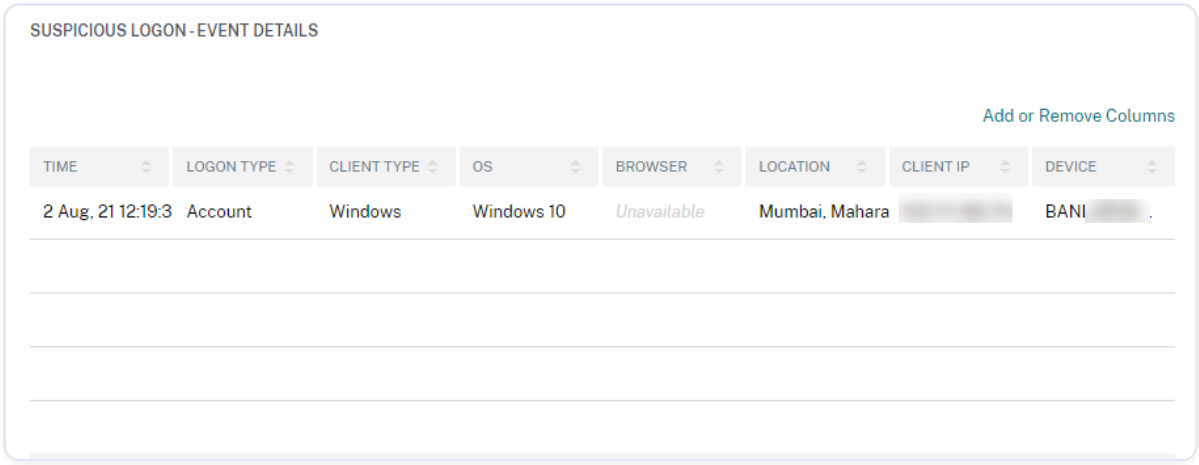
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- “**LOGON LOCATION- LAST 30 DAYS**”部分显示了用户最后已知位置和当前位置的地理地图视图。位置数据显示最近 30 天的数据。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。



- “**SUSPICIOUS LOGON- EVENT DETAILS**”部分提供了有关可疑登录事件的以下信息：
  - **时间**：指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。当用户对其帐户的身份验证成功时，会触发帐户登录事件。而当用户输入其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**：指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。
  - **操作系统**：指示用户设备的操作系统。
  - **浏览器**：指示用于访问应用程序的 Web 浏览器。
  - **位置**：指示用户登录的地点。
  - **客户端 IP**：指示用户设备的 IP 地址。
  - **设备**：指示用户的设备名称。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以对用户执行哪些操作?

您可以对用户帐户执行以下操作：

- **添加到监视列表**。当您希望监视用户以防范未来潜在威胁时，可以将其添加到监视列表。
- **通知管理员**。当用户帐户上出现任何异常或可疑活动时，系统会向所有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上出现异常事件，管理员可以开始录制用户未来登录会话的活动。但是，如果用户使用的是 Citrix Virtual Apps and Desktops 7.18 或更高版本，管理员可以动态启动和停止录制用户当前的登录会话。

要了解有关操作以及如何手动配置它们的更多信息，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是什么，都可以应用与其他数据源相关的操作。

提供用户风险指标的反馈

风险指标旨在检测并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。在实践中，尽管风险指标的某些出现对应着合法的潜在安全威胁，但其他情况则被证明是良性的。

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，标记为有用

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 如果您已确定不存在安全威胁，则标记为无用。在这种情况下，指标出现情况默认从用户时间线中隐藏，并且用户的风险评分会自动调整，以在后续计算中排除此指标出现情况。

此外，您的集体反馈将用于推动风险指标算法的未来改进。

提供反馈(/en-us/citrix-analytics/media/risk-indicator-feedback.png)

用户时间线中每个默认风险指标条目都会显示一个反馈横幅（带有竖起大拇指和朝下大拇指图标）。

- **竖起大拇指**图标 - 指标有用，并正确识别了风险活动。您可以单击竖起大拇指图标，并提供关于该指标如何有用及其益处的补充评论。

  您可以保存反馈并将指标标记为有用。您还可以通过单击“编辑反馈”来编辑评论。反馈横幅提供了上次提交反馈的时间线。

  编辑反馈(/en-us/citrix-analytics/media/risk-indicator-edit-feedback.png)

  当风险指标被标记为有用时，此反馈会显示在相应的用户时间线条目中，并报告给 Citrix Analytics。用户风险评分不受影响。

  已标记的反馈(/en-us/citrix-analytics/media/risk-indicator-marked-feedback.png)

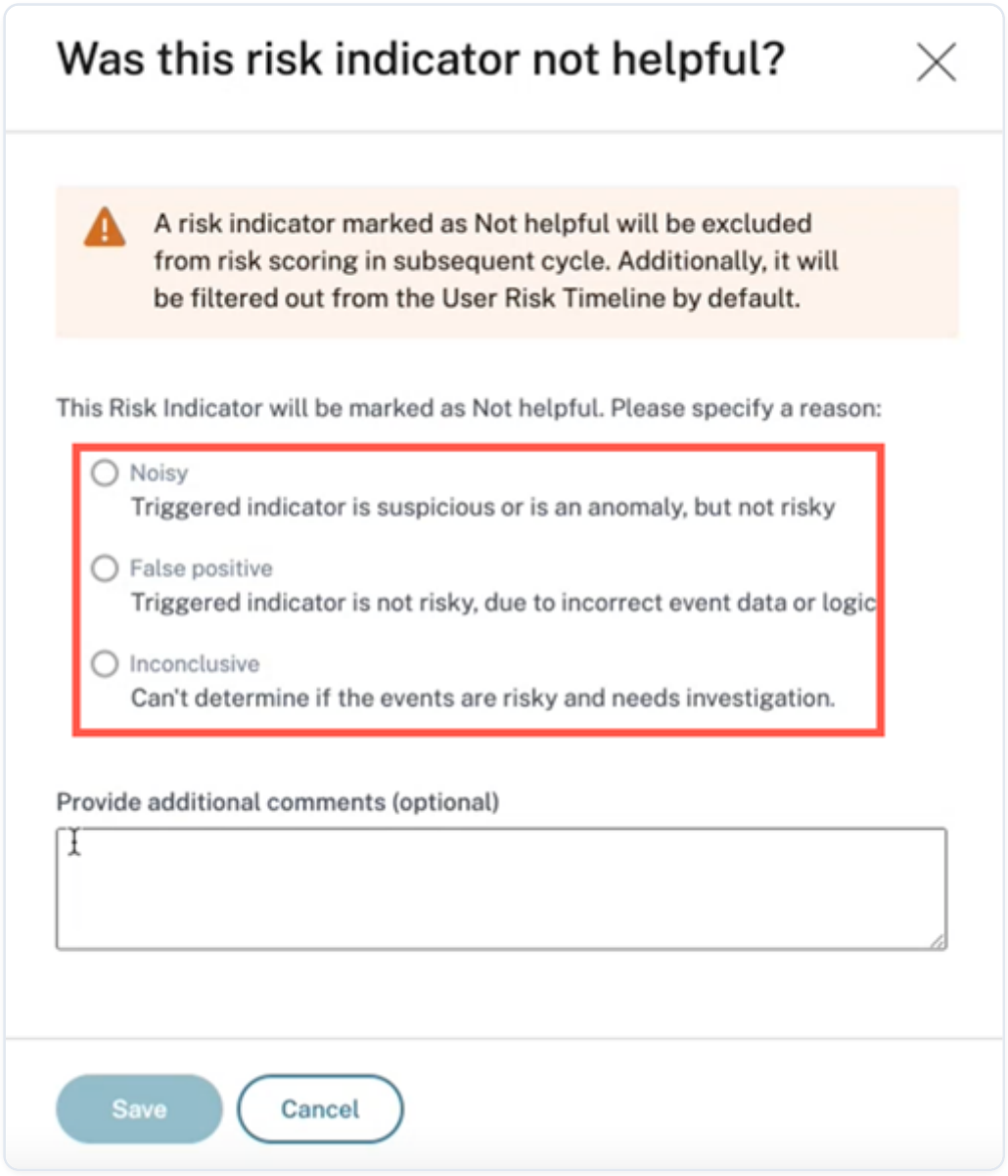
- **朝下大拇指**图标 - 指标无用或触发不正确。您可以将指标标记为无用，并将其归类为**噪音**、**误报**或**不确定**。此风险指标的出现情况将从用户风险评分的所有后续更新中排除。如有必要，您还可以提供补充评论。

  - **噪音** – 触发的指标可疑或异常，但无风险。
  - **误报** – 触发的指标没有风险，因为事件数据或逻辑不正确。
  - **不确定** – 无法确定事件是否有风险，并且需要调查。

    注意

    重新校准风险评分最多需要 15 分钟。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



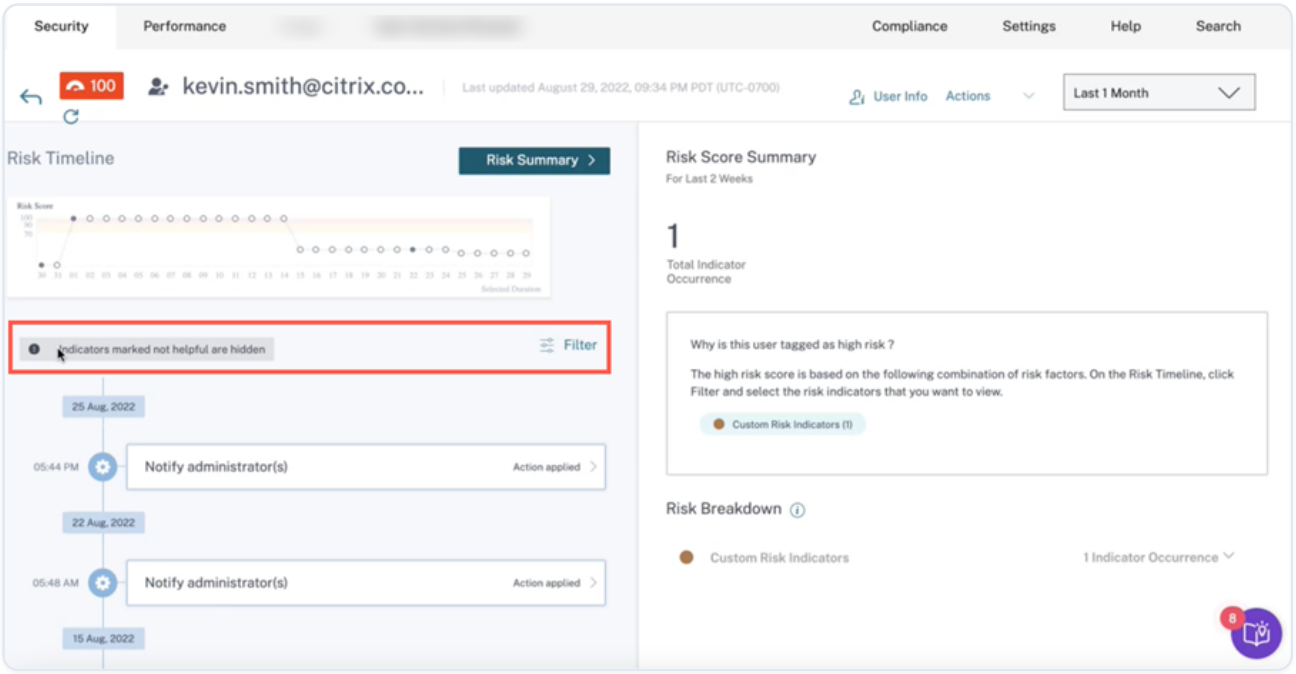
如果某个指标被标记为无用，您可以查看以下结果：

- 该特定指标将从时间线中隐藏。
- 风险评分将重新校准，因为在后续更新中，此指标的出现将从风险评分计算中排除。
- 作为文本反馈提供的任何附加信息将保留以供日后参考。

查看筛选器

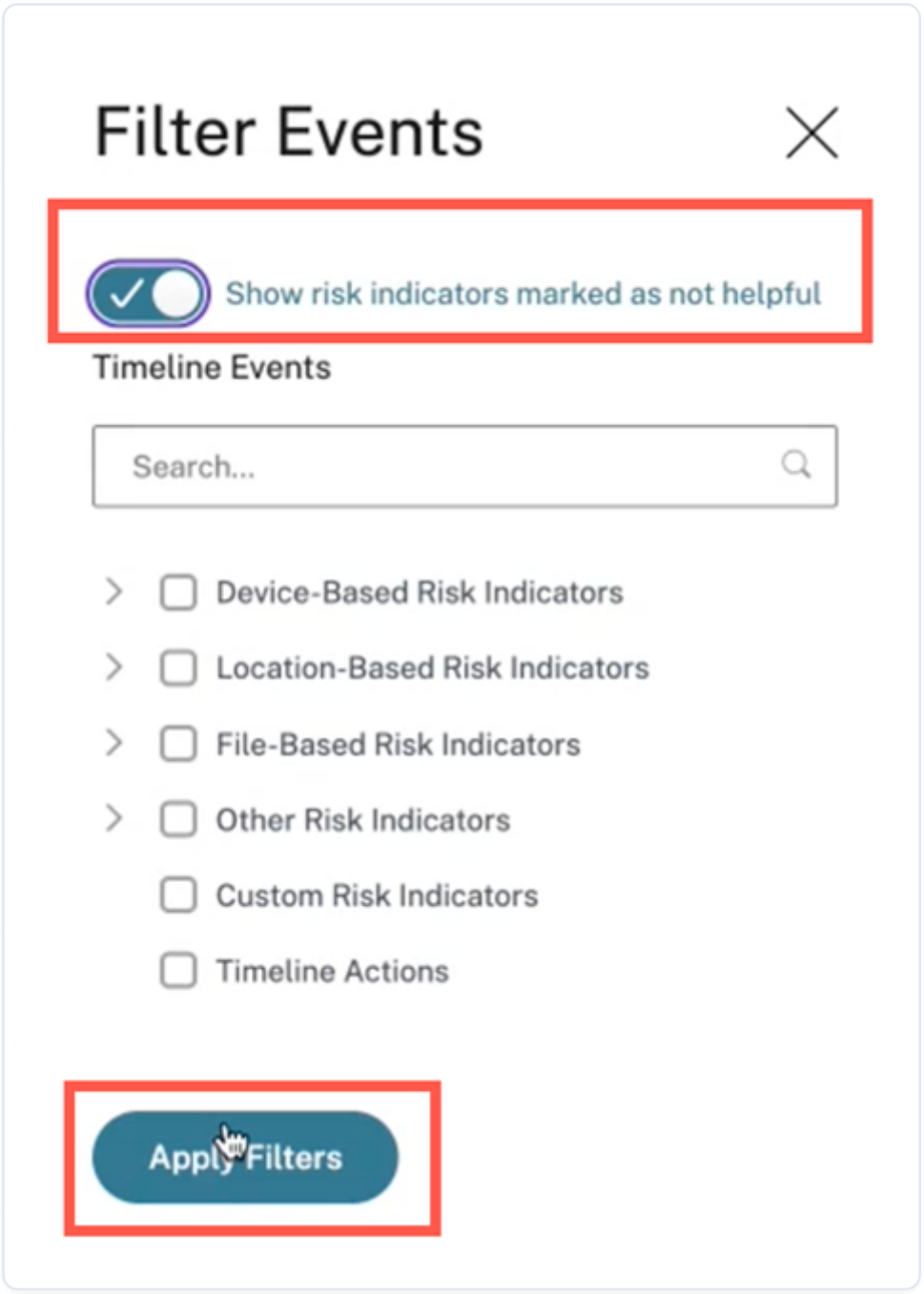
被标记为无用的指标默认情况下是隐藏的。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



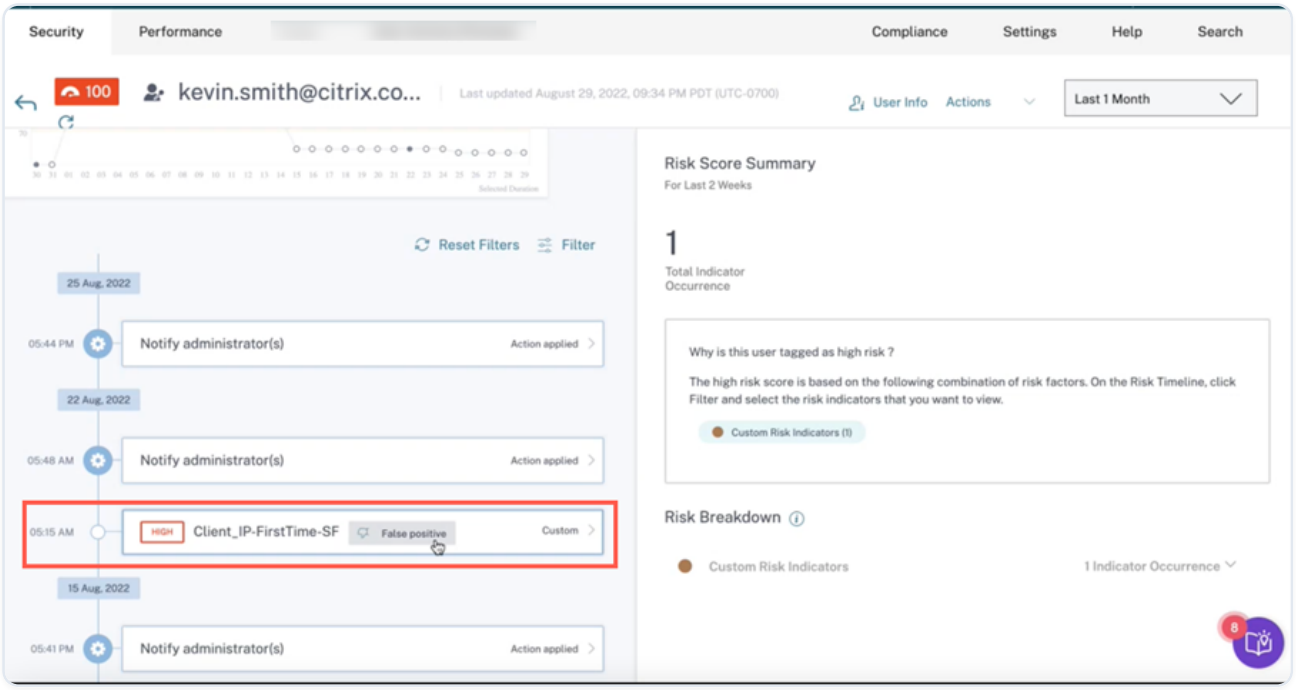
要查看隐藏的指标，请点击**筛选**。在出现的**筛选事件**窗口中，开启**显示标记为无用的风险指标**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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标，请选择类别并点击**应用筛选器**。您可以查看所有基于位置的无用指标及其反馈详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



作为管理员，您还可以根据需要执行以下操作：

- 更改反馈
- 查看之前的反馈以及相关的元数据
- 查看其他管理员提供的反馈以及相关的元数据

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Graph Security 风险指标

注意：

自 2023 年 7 月起，Microsoft 已将 Azure Active Directory (Azure AD) 重命名为 Microsoft Entra ID。本文档中，任何对 Azure Active Directory、Azure AD 或 AAD 的引用现在均指 Microsoft Entra ID。

Microsoft Graph Security 从 **Azure AD Identity Protection** 或 **Microsoft Defender for Endpoint** 安全提供程序接收数据，并将信息发送到 Citrix Analytics。

Azure AD Identity Protection 触发以下风险指标并将信息发送到 Microsoft Graph Security：

- 匿名 IP 地址
- 不可能前往非典型位置
- 凭据泄露的用户
- 来自受感染设备的登录
- 来自有可疑活动的 IP 地址的登录
- 来自陌生位置的登录

如需了解 Defender for Endpoint 的信息，请参阅 Microsoft Defender for Endpoint。

与风险指标关联的风险因素是基于 IP 的风险指标。有关风险因素的更多信息，请参阅 Citrix 用户风险指标。

如何分析 Microsoft Graph Security 风险指标

假设用户 Maria Brown 表现出前面提到的一种危险行为。Microsoft 检测到此事件并生成警报。Citrix Analytics 检索此警报并为 Maria Brown 分配更新的风险评分。此外，相应的风险指标会添加到 Maria Brown 的风险时间线中。

要查看用户的 Microsoft Graph Security 风险指标条目，请导航到 **安全** > **用户**，然后选择该用户。

在 Maria 的时间线中，您可以从风险时间线中选择最新的风险指标条目。其对应的详细信息面板将显示在右侧窗格中。**发生了什么** 部分提供了风险指标的简要摘要。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

如何获取有关风险指标的更多信息

有关更多信息，请参阅 Azure Active Directory 风险事件。

您可以对用户执行哪些操作

目前，尚无法通过 Microsoft Graph Security 数据源对用户帐户执行适当的操作。

有关 Microsoft Graph Security 入门的信息，请参阅 Microsoft Graph Security。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

自定义风险指标

您在 Citrix Analytics for Security™ 中会看到两种类型的风险指标：

- **默认风险指标**：这些风险指标基于机器学习算法。有关更多信息，请参阅 Citrix 用户风险指标。
- **自定义风险指标**：这些风险指标由管理员手动创建。

创建自定义风险指标时，您可以根据用例定义触发条件和参数。如果用户事件与您定义的条件匹配，Citrix Analytics 将触发自定义风险指标并将其显示在用户的风险时间轴上。

为以下数据源创建自定义风险指标：

- 思杰网关
- 思杰安全私有访问™
- 思杰虚拟应用和桌面™ 本地部署
- Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）
- 思杰安全浏览器

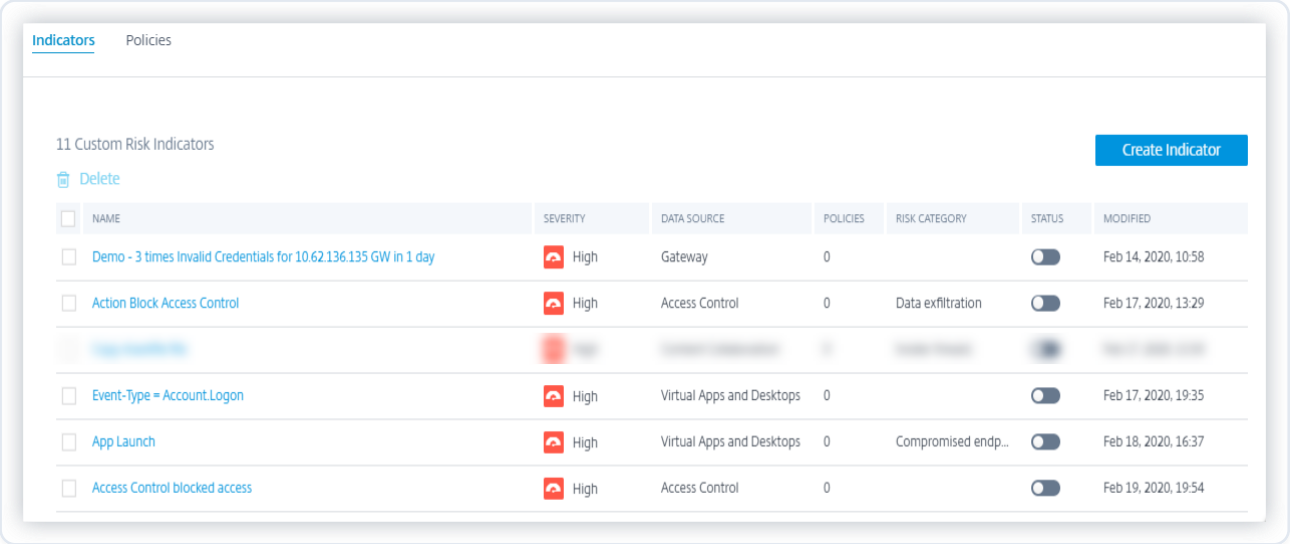
预配置的自定义风险指标

Citrix 还提供了一些具有预配置条件的自定义风险指标，可帮助您监控 Citrix 基础架构的安全性。您可以根据用例修改预配置条件。有关更多信息，请参阅 预配置的自定义风险指标。

自定义风险指标页面

自定义风险指标页面提供了针对用户、严重性、数据源、策略数量、风险类别、状态以及指标上次修改日期和时间生成的所有自定义风险指标的见解。要创建自定义风险指标，请参阅 创建自定义风险指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



当您选择风险指标时，您将被重定向到“**修改风险指标**”页面。有关详细信息，请参阅修改自定义风险指标。

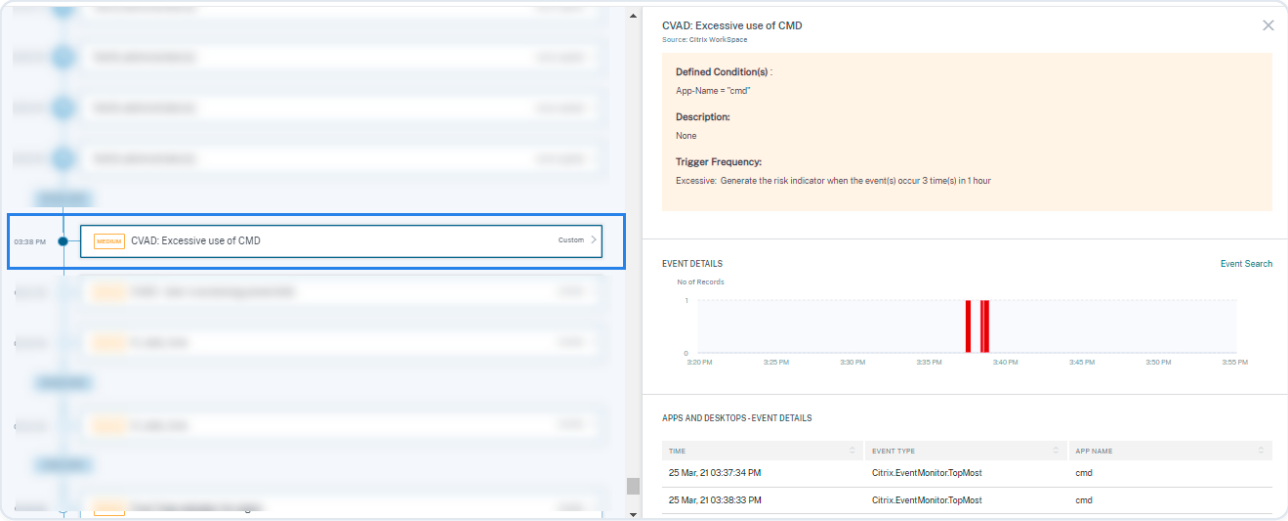
分析自定义风险指标

假设某个用户的操作触发了您定义的自定义风险指标。Citrix Analytics 会在用户的风险时间轴上显示该自定义风险指标。

当您在用户的风险时间轴上选择自定义风险指标时，右侧窗格会显示以下信息：

- **已定义条件**：显示您在创建自定义风险指标时定义的条件的摘要。
- **描述**：提供您在创建自定义风险指标时提供的描述摘要。如果未在创建自定义风险指标时提供描述，则此部分将显示“**无**”。
- **触发频率**：显示您在创建自定义风险指标时在“**高级选项**”部分中选择的选项。
- **事件详细信息**：显示触发自定义风险指标的用户事件的时间轴和详细信息。您可以单击“**事件搜索**”在自助搜索页面上查看用户事件。自助搜索页面会显示与用户和自定义风险指标相关的事件。搜索查询会显示为自定义风险指标定义的条件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意

自定义风险指标在用户风险时间轴上以标签形式显示。

可应用于用户的操作

当为用户触发自定义风险指标时，您可以手动应用操作或创建策略以自动应用操作。有关详细信息，请参阅策略和操作。

自定义风险指标模板

您可以使用预定义模板之一创建自定义风险指标，也可以不使用模板继续。

模板是创建自定义风险指标的起点。它通过提供预定义的查询和参数来指导您创建自定义风险指标，您可以根据自己的用例进行选择。

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。

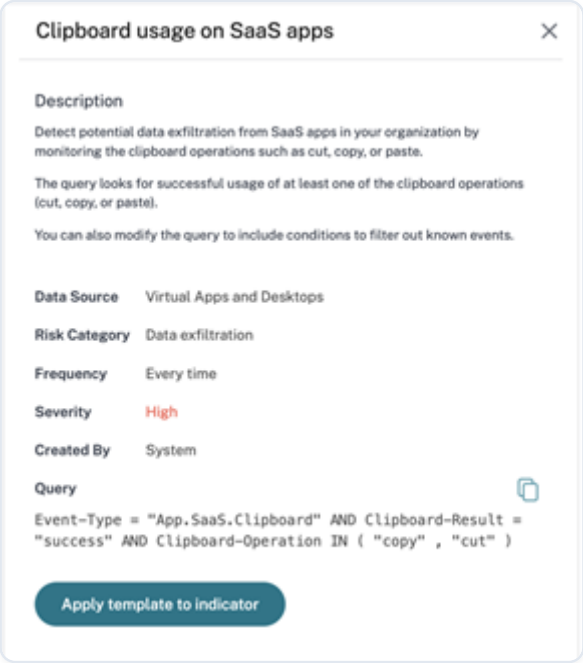
模板包含以下信息：

- **描述**：指示模板中定义的查询的目的。
- **数据源**：指示模板适用的数据源。
- **风险类别**：指示与查询搜索的事件相关的风险类别。风险事件分为四类：数据泄露、内部威胁、受感染用户和受感染端点。有关信息，请参阅风险类别。
- **频率**：指示查询触发的频率。
- **严重性**：指示与事件相关的风险严重性。风险可以是高、中或低。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **创建者**：指示模板的创建者。模板始终是系统定义的。
- **查询**：指示模板中定义的条件。查询检索满足条件的用户事件。

下图显示了 SaaS 应用中剪贴板使用情况的用例模板。

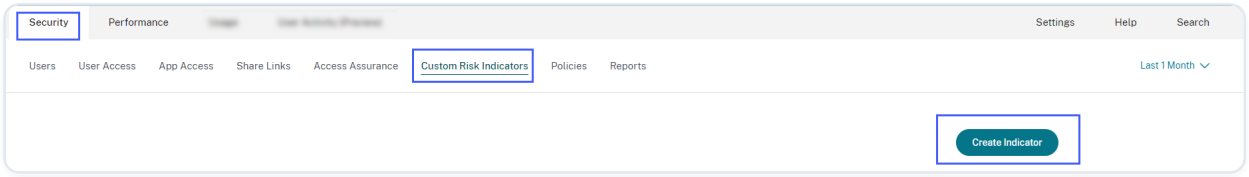


如果您没有找到适合您用例的模板，或者您想定义自己的查询，您可以不使用模板继续。

创建自定义风险指标

要创建自定义风险指标：

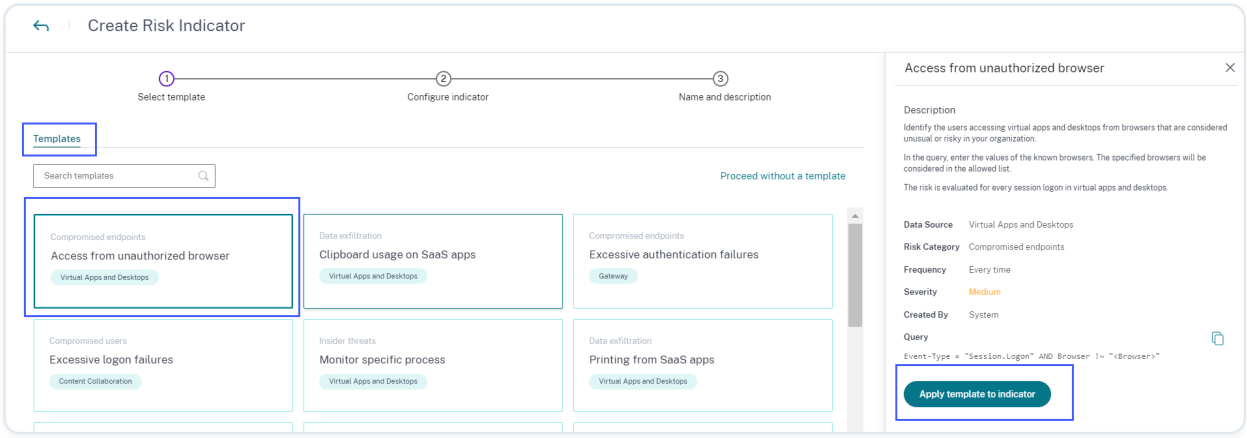
1. 导航到 **安全 > 自定义风险指标 > 创建指标**。



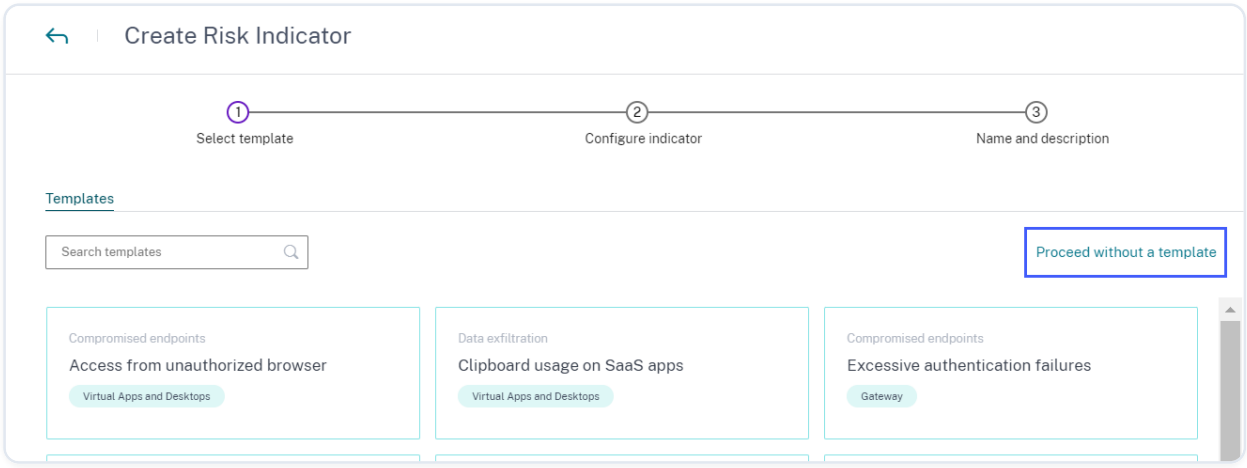
2. 选择一个模板以查看用例。如果它符合您的要求，请选择 **将模板应用于指标**。

> **注意**
>
> 您还可以修改模板的预定义条件和参数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 如果您没有找到所需的模板或想创建自己的条件，请选择 **不使用模板继续**。



4. 按照屏幕上的说明创建指标。

注意事项

- 您最多可以创建 50 个自定义风险指标。如果达到此最大限制，您必须删除或编辑任何现有的自定义风险指标才能创建新的自定义风险指标。
- 当自定义风险指标被触发时，它会立即显示在用户时间线上。但是，用户的风险摘要和风险评分会在几分钟后（大约 15-20 分钟）更新。

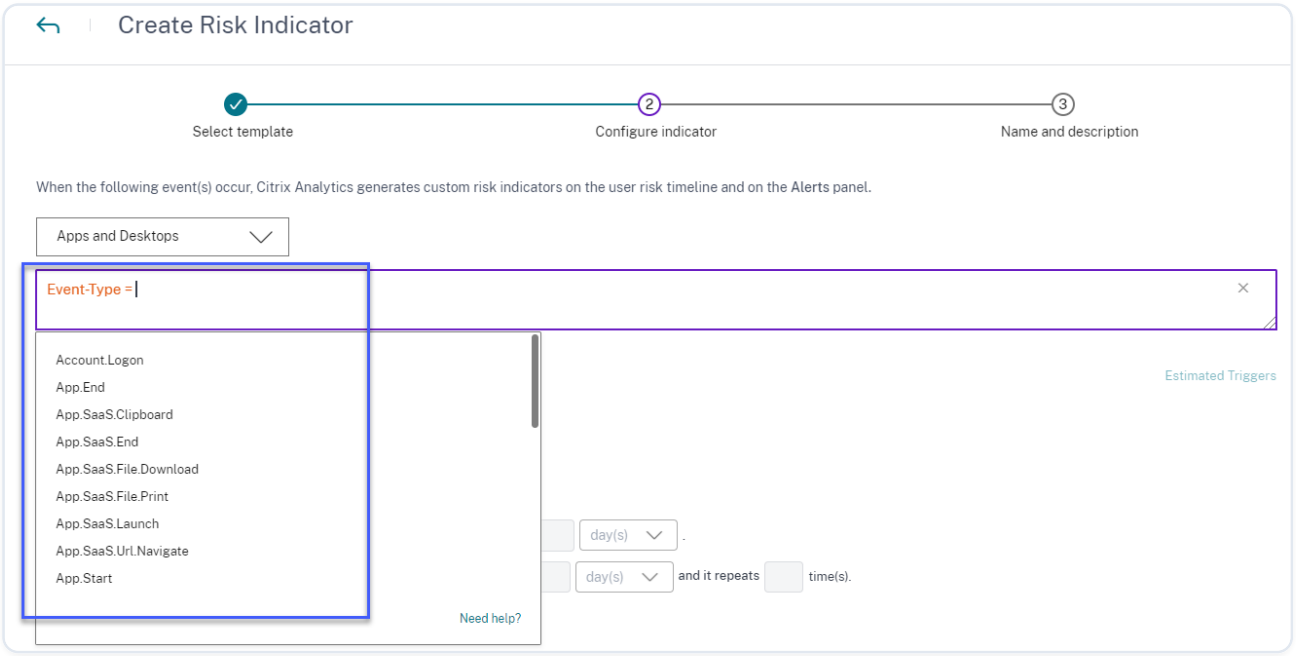
为自定义风险指标定义条件

使用查询框定义自定义风险指标的条件。根据所选数据源，您将获得相应的维度和有效运算符来定义您的条件。

当选择 `Event-Type` 和 `Clipboard-Operation` 等特定维度以及有效的运算符时，将自动显示维度的值。您可以从建议的选项中选择一个值，或根据您的要求输入一个新值。

下图显示了维度 `Event-Type` 的建议值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



如果您使用模板，则条件是预定义的。但是，您可以根据您的用例追加或修改预定义条件。

在查询框下方，您会看到“**预估触发器**”链接。单击该链接可预测将针对已定义条件触发的自定义风险指示器的近似实例。这些实例是根据 Citrix Analytics 维护并符合已定义条件的历史数据计算的。

请务必单击“**预估触发器**”以预测上次定义的条件的自定义风险指示器发生次数。

使用高级选项

在“**高级选项**”部分，选择事件触发自定义风险指示器的频率。如果您未选择任何选项，Citrix Analytics 会将“**每次：每次事件发生时生成风险指示器**”视为默认选项并生成自定义风险指示器。您可以选择以下选项之一：

- **每次**：每当事件满足定义的条件时，都会触发风险指示器。
- **首次**：当事件首次满足定义的条件时，会触发风险指示器。
    - **新实体的首次**：启用此选项可首次检测从新实体接收到的事件。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，而无需为实体指定显式值。例如，当您选择实体为“城市”时，您无需指定城市名称。当首次从新城市接收到事件时，会触发风险指示器。

      下表列出了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
安全私有访问	城市	当用户首次从新城市登录时。

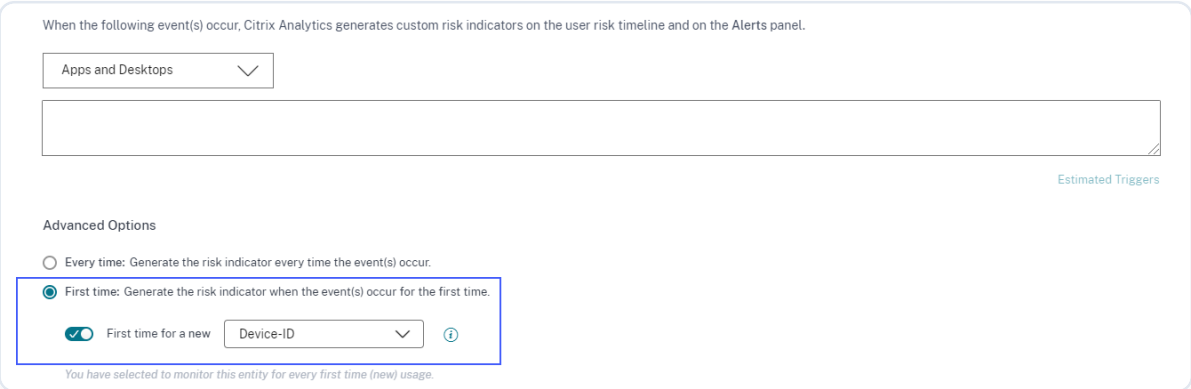
© 1997–2026 Citrix Systems, Inc. All rights reserved.

数据源	实体	触发条件
	客户端 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。
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上的浏览器中输入新的应用程序 URL 时。
	城市	当用户首次从新城市启动应用程序或桌面时。
	客户端 IP	当用户首次从新的 IP 地址登录时。
	国家/地区	当用户首次从新的国家/地区启动应用程序或桌面时。
	设备 ID	当用户首次从新设备（例如移动设备、笔记本电脑或台式机）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	所用打印机的名称。
	打印总份数	用户打印的总份数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

数据源	实体	触发条件
	打印总页数	用户打印的文档总页数。
网关	客户端 IP	用户首次从新的 IP 地址登录时。
安全浏览器	用户名	发起事件的用户的名称。
	允许访问	用户是否被允许或拒绝访问主机服务。
	客户端 IP	用户设备的 IP 地址。
	访问的主机名	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编号。

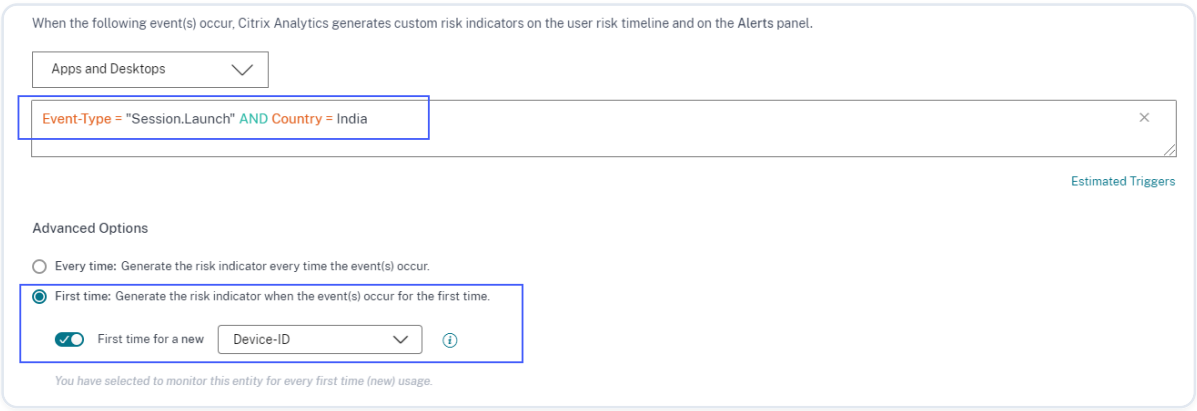
以下示例显示了为“应用程序和桌面”数据源创建的自定义风险指标。当用户首次从新设备启动虚拟桌面或虚拟应用程序时，将触发此风险指标。



您还可以添加一个条件以及“**首次针对新**”选项。在这种情况下，当风险指标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，将触发该风险指标。

以下示例显示了为自定义风险指标定义的条件以及启用的“**首次针对新设备 ID**”选项。当位于印度的用户首次从新设备启动虚拟桌面会话时，将触发此风险指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **过度**: 满足以下条件后，将触发风险指标：
  - 事件满足定义的条件。
  - 事件在指定期间内发生指定次数。
- **频繁**: 满足以下条件后，将触发风险指标：
  - 事件满足定义的条件。
  - 事件在指定期间内发生指定次数。
  - 事件模式重复指定次数。

选择风险类别

为您的自定义风险指标选择风险类别。

风险指标根据自定义风险指标的风险暴露类型进行分组。有关风险类别选择的帮助，请参阅风险类别。

选择严重性

严重性表示风险指标检测到的风险事件的严重程度。创建自定义风险指标时，请选择严重性——高、中或低。

如果您应用模板，严重性选项将预先选中。您可以根据您的用例修改此预选。

定义条件支持的运算符

定义条件时可以使用以下运算符。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

运算符	描述	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。
=	为搜索查询分配值。	用户名 = John	显示用户 John 的事件。
~	搜索相似值。	用户名 ~ test	显示具有相似用户名的事件。
""	括起由空格分隔的值。	用户名 = "John Smith"	显示用户 John Smith 的事件。
<, >	搜索关系值。	数据量 > 100	显示数据量大于 100 GB 的事件。
AND	搜索两个条件都为真的值。	用户名 : John 且 数据量 > 100	显示用户 John 的事件，其中数据量大于 100 GB。
*	搜索匹配该字符出现零次或多次的值。	用户名 = John*	显示所有以 John 开头的用户名的事件。
		用户名 = *John*	显示所有包含 John 的用户名的事件。
		用户名 = *Smith	显示所有以 Smith 结尾的用户名的事件。
!~	检查用户事件中是否存在您指定的匹配模式。此 NOT LIKE 运算符返回事件字符串中不包含指定匹配模式的事件。	用户名 !~ 约翰	显示除 John、John Smith 或任何包含匹配名称“John”的用户之外的用户事件。
!=	检查用户事件中是否存在您指定的精确字符串。此 NOT EQUAL 运算符返回事件字符串中不包含精确字符串的事件。	国家 != 美国	显示除 USA 之外的国家/地区的事件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

运算符	描述	示例	输出
IN	为维度分配多个值，以获取与一个或多个值相关的事件。	用户名 IN (约翰, 凯文)	查找与 John 或 Kevin 相关的所有事件。
NOT IN	为维度分配多个值，并查找不包含指定值的事件。	用户名 NOT IN (约翰, 凯文)	查找除 John 和 Kevin 之外的所有用户的事件。
为空	检查维度的空值或空字符串值。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 为空	查找国家/地区名称不可用或为空（未指定）的事件。
不为空	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 不为空	查找国家/地区名称可用或已指定的事件。
或	搜索满足任一或两个条件的真值。	(用户名 = `John*` 或 用户名 = `*Smith`) 并且 事件类型 = “Session.Logon”	显示 `Session.Logon` 事件，适用于所有以 John 开头或以 Smith 结尾的用户名。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

对于 **不等于** 运算符，在条件中输入维度值时，请使用数据源的 自助搜索 页面上提供的确切值。维度值区分大小写。

修改自定义风险指标

1. 导航到 **安全 > 自定义风险指标**。
2. 选择要修改的自定义风险指标。
3. 在**修改指标**页面上，根据需要修改信息。
4. 点击**保存更改**。

注意

如果您修改了现有自定义风险指标的属性，例如条件、风险类别、严重性和名称，在用户时间轴上，您仍然可以查看为用户触发的该自定义风险指标的先前发生情况（带有旧属性）。

例如，您创建了一个自定义风险指标，其条件为 *Country != India*。因此，当用户从印度境外登录时，会触发此自定义风险指标。现在，您将自定义风险指标的条件修改为 *Country != "United States"*。在这种情况下，您仍然可以在触发风险指标的用户时间轴上查看条件为 *Country != India* 的自定义风险指标的先前发生情况。

删除自定义风险指标

1. 导航到 **安全 > 自定义风险指标**。
2. 选择要删除的自定义风险指标。
3. 点击**删除**。
4. 在对话框中，确认删除自定义风险指标的请求。

注意

如果您删除了自定义风险指标，在用户时间轴上，您仍然可以查看为用户触发的该自定义风险指标的先前发生情况。

例如，您删除了一个现有自定义风险指标，其条件为 *Country != India*。在这种情况下，您仍然可以在触发风险指标的用户时间轴上查看条件为 *Country != India* 的自定义风险指标的先前发生情况。

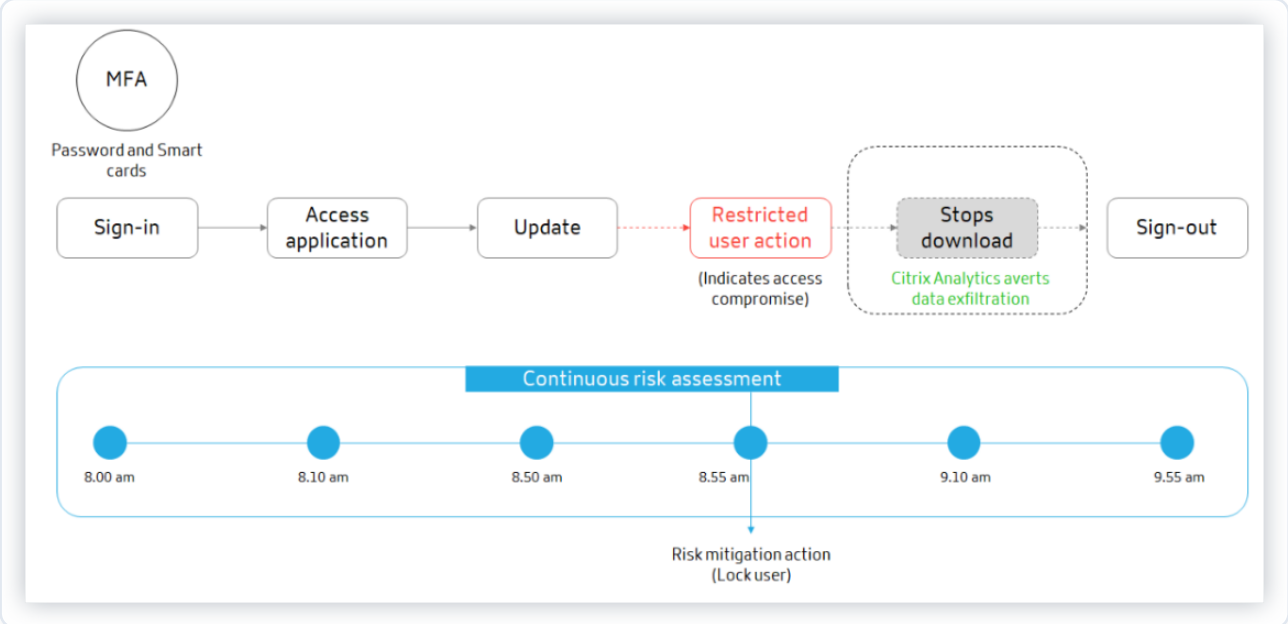
© 1997–2026 Citrix Systems, Inc. All rights reserved.

持续风险评估

便携式计算设备和互联网的日益普及，使 Citrix Workspace™ 用户几乎可以在任何地点、任何设备上工作。这种灵活性带来的挑战是，远程访问会通过数据泄露、盗窃、蓄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。组织内部的员工也可能助长这种损害。

解决此类风险的一些传统方法是实施多重身份验证、缩短登录会话等。尽管这些风险评估方法可确保更高水平的安全性，但在用户初始验证后，它们无法提供完整的安全性。如果恶意用户成功访问网络，他们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 引入了持续风险评估解决方案。此解决方案通过确保使用 Citrix Virtual Apps and Desktops 或 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops service）的用户的风险暴露与初始验证时保持一致，而无需用户每次都进行验证，从而保护您的数据免受外部网络犯罪分子和恶意内部人员的侵害。此解决方案通过在会话期间持续评估风险事件并自动应用操作来防止组织资源被进一步滥用。



用例

假设用户 Adam Maxwell 首次从一个与其通常行为不符的异常位置多次登录失败后，成功访问了网络。此外，该位置有网络攻击记录。在这种情况下，您需要立即采取行动，以避免 Adam 的帐户被

© 1997–2026 Citrix Systems, Inc. All rights reserved.

进一步滥用。您可以锁定 Adam 的帐户并通知他所采取的措施。此操作可能会暂时导致用户帐户的服务中断。用户可以联系管理员寻求帮助以恢复帐户。

考虑另一种情况，Adam 首次从新设备和新 IP 访问了网络。您可以联系 Adam，询问他是否确认此活动。如果是，则可能是 Adam 更改了其工作设备，并正在从其家庭网络工作。此活动不会对组织的安全造成任何损害，可以忽略。但是，如果用户未执行此活动，则其帐户很可能已被盗用。在这种情况下，您可以锁定用户帐户以防止进一步的损害。

主要功能

持续风险评估可自动执行与策略和可见性仪表板相关的一些功能：

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自定义风险指标、用户风险评分的组合，或两者兼有。

有关详细信息，请参阅什么是策略。

在应用操作前通知用户

在对用户帐户应用适当操作之前，您可以通知用户并评估已检测到的异常活动的性质。

有关更多信息，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帐户和组织的安全面临风险。在这种情况下，当您检测到异常活动时，可以应用破坏性操作，并通知用户。

有关更多信息，请参阅应用破坏性操作后通知用户。

强制执行和监控模式

您可以根据要求将策略设置为强制执行模式或监控模式。强制执行模式下的策略对用户帐户有直接影响。但是，如果您想在实施策略之前评估其影响或结果，可以将策略设置为监控模式。

有关更多信息，请参阅支持的模式。

访问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进行的访问尝试次数。有关更多信息，请参阅访问摘要。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用**策略和操作**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 引入了预定义策略，这些策略默认在**策略**控制板上启用。这些策略是使用风险指标和用户风险评分作为预定义条件创建的。每个默认策略都分配有一个全局操作。

注意

您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 的时间以及您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，也可以根据您的要求修改它们：

策略名称	条件	数据源	操作
凭据利用成功	当 (/zh-cn/security-analytics/risk-indicators/citrix-gateway-risk-indicators.html#excessive-authentication-failures) 和 (/zh-cn/security-analytics/risk-indicators/citrix-gateway-risk-indicators.html#suspicious-logon) 风险指标被触发时	思杰网关	锁定用户
潜在数据泄露	当 (/zh-cn/security-analytics/risk-indicators/citrix-virtual-apps-and-desktops-risk-indicators.html#potential-data-exfiltration) 风险指标被触发时	思杰虚拟应用和桌面以及思杰 DaaS	注销用户

© 1997–2026 Citrix Systems, Inc. All rights reserved.

策略名称	条件	数据源	操作
来自可疑 IP 的异常访问	当 (/zh-cn/security-analytics/risk-indicators/citrix-gateway-risk-indicators.html#suspicious-logon) 和 (/zh-cn/security-analytics/risk-indicators/citrix-gateway-risk-indicators.html#logon-from-suspicious-ip) 风险指标被触发时	Citrix 网关	锁定用户
首次从设备访问	当触发 (/zh-cn/security-analytics/preconf-custom-risk-indicators-policies.html#preconfigured-custom-risk-indicators-for-the-first-time-access-scenario) 风险指示器时	Citrix 虚拟应用和桌面和 Citrix DaaS	请求最终用户响应
访问时出现不可能的行程	当触发 (/zh-cn/security-analytics/risk-indicators/citrix-virtual-apps-and-desktops-risk-indicators.html#impossible-travel) 风险指示器时。	Citrix 虚拟应用和桌面和 Citrix DaaS	请求最终用户响应
身份验证时出现不可能的行程	当触发 (/zh-cn/security-analytics/risk-indicators/citrix-gateway-risk-indicators.html#impossible-traveld-desktops-risk-indicators.html#impo	Citrix 网关	请求最终用户响应

© 1997–2026 Citrix Systems, Inc. All rights reserved.

策略名称	条件	数据源	操作
	ssible-travel) 风险指示器时。		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

策略和操作

注意

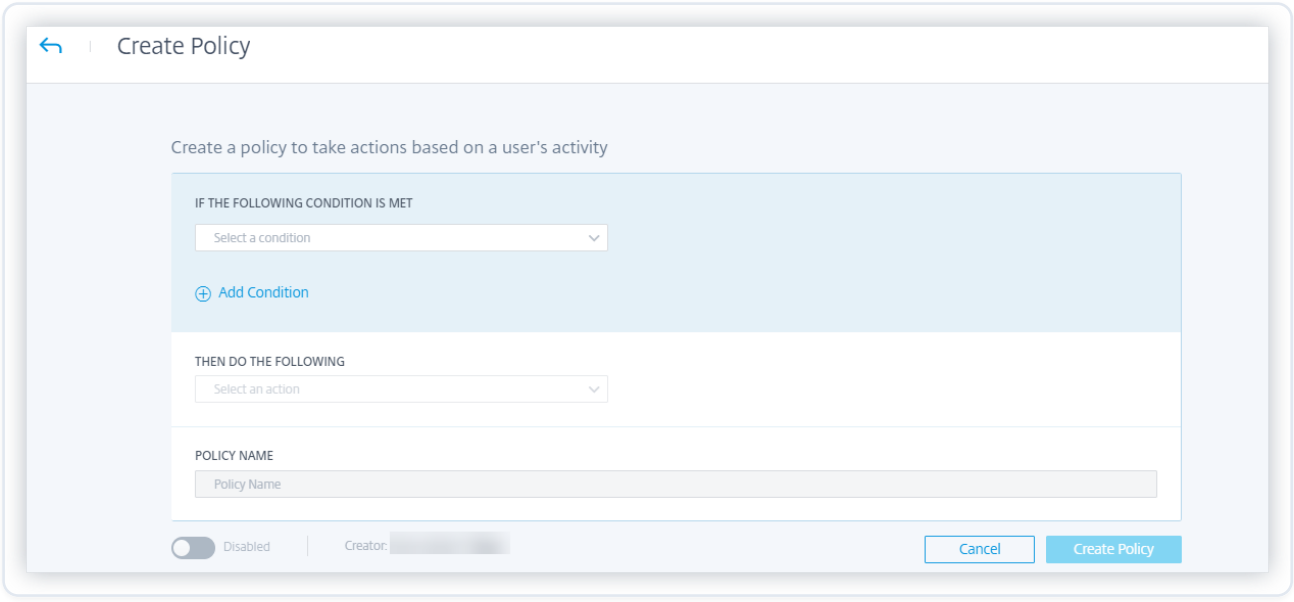
注意：Citrix Content Collaboration™ 和 ShareFile 已达到其生命周期终止，用户不再可用。

您可以在 Citrix Analytics 上创建策略，以帮助您在发生异常或可疑活动时对用户帐户执行操作。策略允许您自动化应用操作的过程，例如禁用用户和将用户添加到观察列表。当您启用策略时，在异常事件发生且满足策略条件后，将立即应用相应的操作。您还可以手动对具有异常活动的用户帐户应用操作。

什么是策略?

策略是必须满足才能应用操作的一组条件。策略包含一个或多个条件和一个操作。您可以创建包含多个条件和一个可应用于用户帐户的操作的策略。

风险评分是一个全局条件。全局条件可以应用于特定数据源的特定用户。您可以监视显示任何异常活动的用户帐户。其他条件特定于数据源及其风险指标。这些条件包含风险评分、默认风险指标和自定义风险指标的组合。创建策略时最多可以添加 4 个条件。



例如，如果您的组织使用敏感数据，您可能希望限制用户在内部共享或访问的数据量。但是，如果您的组织规模庞大，单个管理员管理和监视大量用户是不可行的。您可以创建一项策略，其中任何过度共享敏感数据的人都可以被添加到观察列表或立即禁用其帐户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

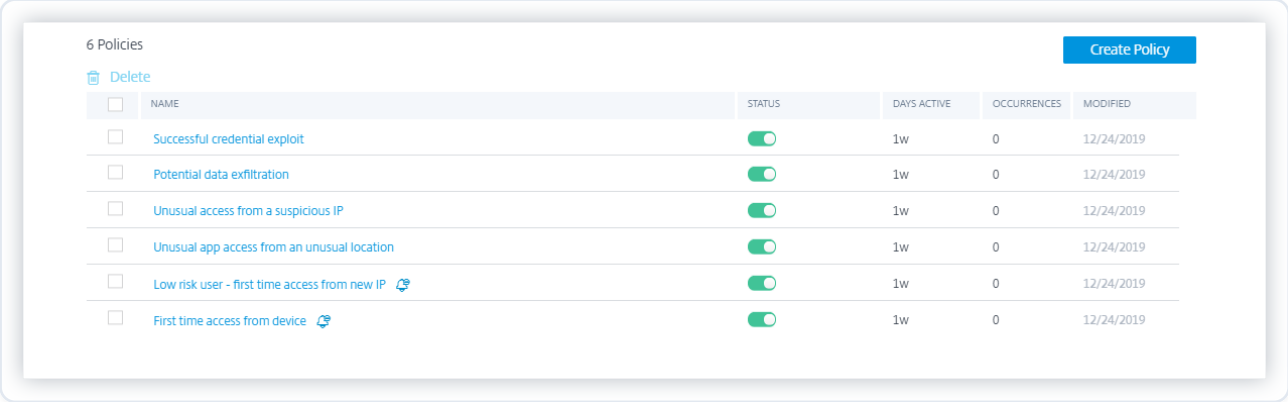
默认策略

默认策略在“**策略**”仪表板上预定义并启用。它们是根据预定义条件创建的，并且为每个默认策略分配了相应的操作。您可以根据自己的要求使用默认策略或修改它。

Citrix Analytics 支持以下默认策略：

- 凭据利用成功
- 潜在数据泄露
- 来自可疑 IP 的异常访问
- 设备首次访问
- Virtual Apps and Desktops 和 Citrix DaaS - 访问时不可能的行程
- Gateway - 身份验证时不可能的行程

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。

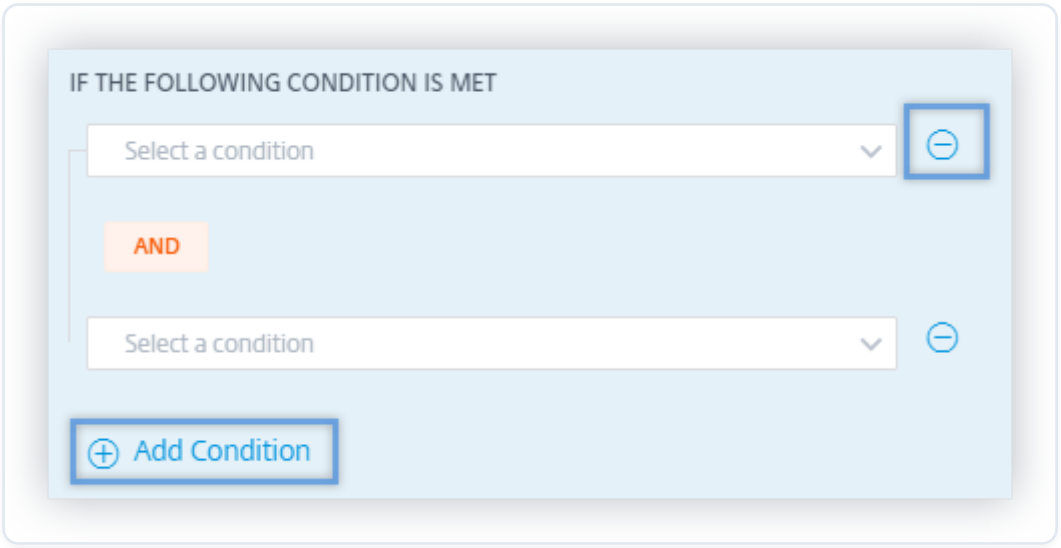


有关地理围栏用例的预定义策略的信息，请参阅预配置策略。

如何添加或删除条件?

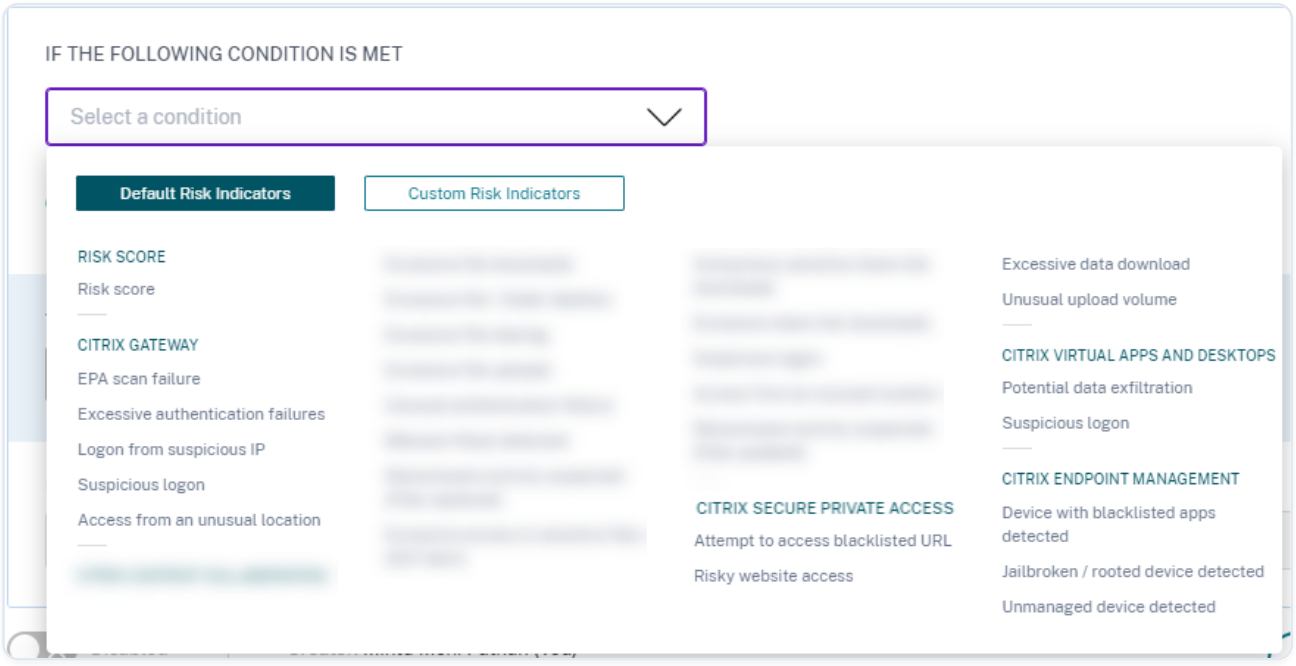
要添加更多条件，请在“**创建策略**”页面的“**如果满足以下条件**”部分中选择“**添加条件**”。要删除条件，请选择条件旁边显示的“**-**”图标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



默认和自定义风险指标

“**创建策略**”页面上的条件菜单根据“**默认风险指标**”和“**自定义风险指标**”选项卡进行区分。使用这些选项卡，您可以轻松识别在为策略配置选择条件时要选择的风险指标类型。



什么是操作?

操作是对可防止未来异常事件发生的异常事件的响应。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帐户应用操作，也可以从用户的风险时间线手动应用特定操作。

您可以查看全局操作或每个 Citrix 数据源的操作。您还可以随时禁用用户先前应用的操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

无论触发风险指标的数据源是什么，都可以应用适用于其他数据源的操作。

下表描述了您可以执行的操作。

操作名称	描述	适用数据源
全局操作		
添加到监视列表	当您想要监视用户以防范未来潜在威胁时，可以将他们添加到监视列表。	所有数据源
	“**监视列表中的用户**”窗格显示您希望根据其帐户上的异常活动监视以防范潜在威胁的所有用户。根据您组织的策略，您可以使用“添加到监视列表”操作将用户添加到监视列表。	
	要将用户添加到监视列表，请导航到用户配置文件，从“**操作**”菜单中选择“**添加到监视列表**”。单击“**应用**”以强制执行此操作。	
通知管理员	当为用户触发风险指标时，您可以手动通知管理员或创建自动通知策略。您可以从 Citrix Cloud 域和组织中的其他非 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，您的 Citrix Cloud 帐户的电子邮件通知处于禁用状态。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。如果您是具有自定义访问权限（只读和完全访问）以管理	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

操作名称	描述	适用数据源
	Security Analytics 的 Citrix Cloud 管理员，则您的 Citrix Cloud 帐户的电子邮件通知处于启用状态。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将您的姓名从通知管理员分发列表中删除。有关信息，请参阅电子邮件分发列表。	
请求最终用户响应	当用户帐户上出现任何异常或可疑活动时，您可以通知用户以确认用户是否识别该活动。根据该活动，您可以确定对用户帐户采取的下一步措施。有关详细信息，请参阅请求最终用户响应。	
通知最终用户	当用户帐户上发生任何异常或可疑活动时，您可以通过电子邮件通知最终用户。有关详细信息，请参阅通知最终用户。	
思杰网关操作		
注销活动会话	应用此操作后，它会注销当前处于活动状态的用户会话。它不会阻止任何未来的用户会话。	本地 思杰网关 和 思杰应用交付管理
锁定用户帐户	当用户的帐户因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 Gateway 管理员解锁该帐户。	本地部署 Citrix Gateway
解锁用户帐户	如果用户的帐户被意外锁定，即使未检测到异常行为，您也可以应用此操作来解锁它并恢复对帐户的访问。	本地部署 Citrix Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

操作名称	描述	适用数据源
Citrix 虚拟应用和桌面™ 和 Citrix 桌面即服务 操作		
注销活动会话	当应用此操作时，它会注销当前活动的用户会话。它不会阻止任何未来的用户会话。	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 帐户上发生异常事件，管理员可以开始录制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，并且已登录到虚拟会话，则管理员可以从 Citrix Analytics for Security 动态触发开始会话录制操作，从而开始录制用户当前的活动会话。	Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

预配置的自定义风险指标和策略

Citrix Analytics for Security 提供了一系列预配置的自定义风险指标和策略，以帮助您监控 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（例如受损用户、内部威胁和数据渗漏）进行定义。您还可以根据自己的安全要求修改这些预配置的条件或添加自己的条件，并使用自定义风险指标来缓解风险。

目前，预配置的自定义风险指标适用于以下场景：

- 地理围栏
- 首次访问

针对地理围栏场景的预配置自定义风险指标

使用以下预配置的自定义风险指标来检测地理围栏区域外的用户事件。

- CVAD-会话在地理围栏外启动
- GW-地理围栏穿越

当用户从其常用运营国家/地区或地理围栏之外访问 Citrix® 产品时，预配置的自定义风险指标会被触发。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

*CVAD-会话在地理围栏外启动*风险指标与 Access Assurance Location 功能的**地理围栏设置**相关联。因此，您无法直接修改风险指标条件中的地理围栏国家/地区。要更新风险指标中的地理围栏国家/地区，请在 Access Assurance Location 控制板的**地理围栏设置**中选择国家/地区。有关详细信息，请参阅访问保障位置控制板。

要查看预配置的自定义风险指标，请选择 **Security > Custom Risk Indicators**。

默认情况下，预配置的自定义风险指标处于禁用状态。使用**STATUS**按钮启用它们。

预配置的自定义风险指标(/en-us/citrix-analytics/media/preconfig-ci.png)

下表描述了地理围栏场景的各种预配置自定义风险指标。

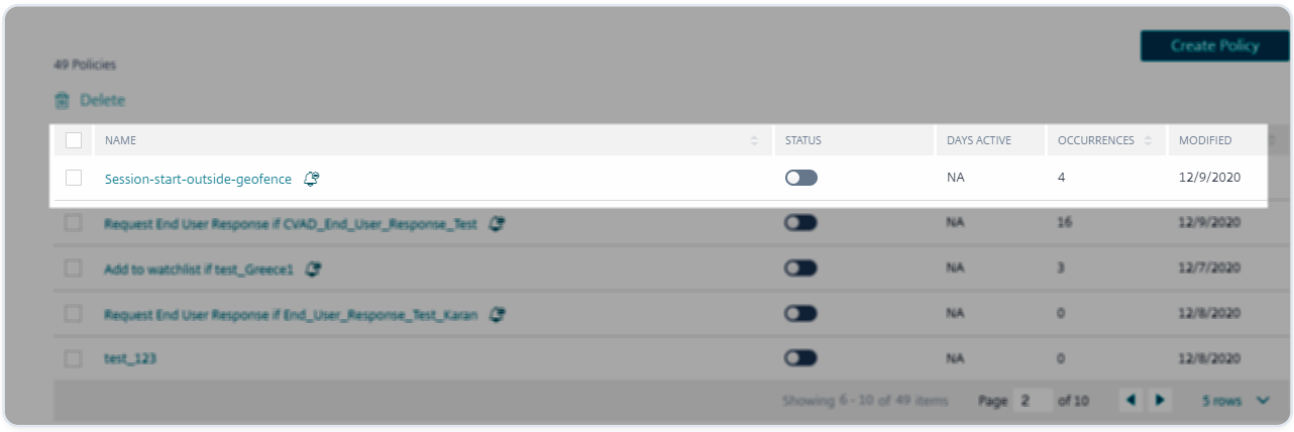
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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-会话在地理围栏外启动	用户在其运营国家/地区之外启动了虚拟会话	事件类型 = Session.logon 国家/地区 != "美国"	Citrix Workspace 应用程序	受感染的用户
GW-地理围栏穿越	用户在其运营国家/地区之外成功进行了身份验证	事件类型 = "VPN_AI" AND 国家/地区 != "美国"	Citrix Gateway（本地部署）	受感染的用户(/zh-cn/security-analytics/users-dashboard.html#types-of-risk-categories)

用于地理围栏场景的预配置策略

Citrix 提供了一个预配置策略，该策略在用户从其运营国家/地区之外启动虚拟会话时，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，并根据用户的响应，会采取适当的操作，例如将用户添加到观察列表或通知管理员采取进一步行动。有关详细信息，请参阅请求最终用户响应。

要查看预配置策略，请选择**安全 > 策略**。



下表描述了用于地理围栏的预配置策略。

策略名称	场景	策略条件	应用的操作
会话在地理围栏外启动	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	与预配置的自定义风险指标“CVAD-会话在地理围栏外启动”一起使用	请求最终用户响应

© 1997–2026 Citrix Systems, Inc. All rights reserved.

策略名称	场景	策略条件	应用的操作
	应”操作验证用户的合法性		
			根据以下用户的响应，将应用相应的操作：
			如果用户不识别该活动：**添加到观察列表**
			如果用户识别该活动：**无需采取任何操作**
			如果用户在收到电子邮件后 60 分钟内未响应：**将用户添加到观察列表**

注意

请求最终用户响应操作仅在美国地区受支持。因此，如果您的组织已加入 Citrix Cloud™ 的欧盟地区，则预配置策略不会应用于您的帐户。要使用预配置策略，请修改策略并选择您选择的其他操作。

使用预配置的地理围栏自定义风险指标创建您自己的策略

您还可以使用这些预配置的自定义风险指标创建自己的策略，并在指标触发时应用锁定用户或注销用户等操作。有关如何创建策略的信息，请参阅配置策略和操作。

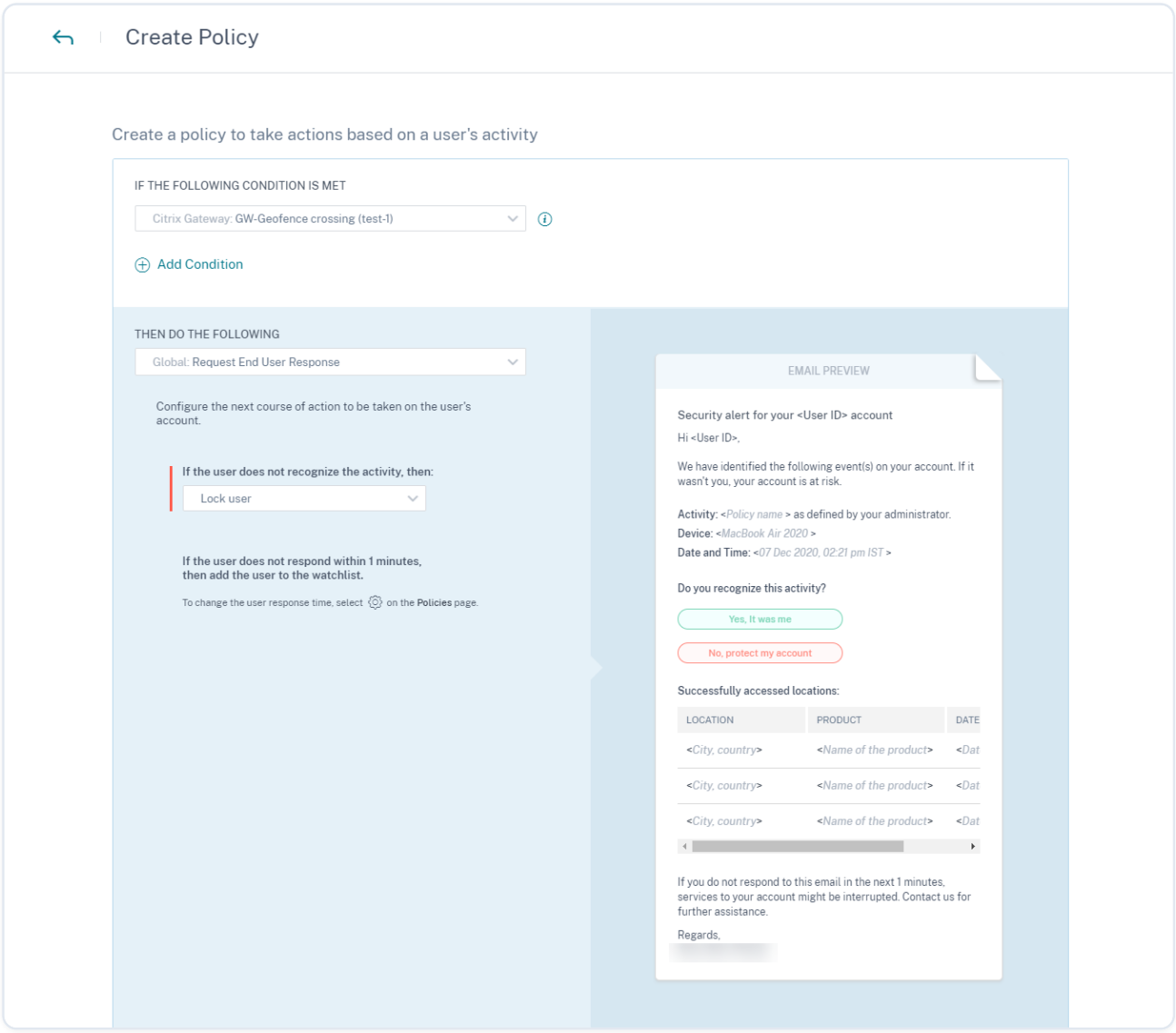
以下示例显示了一个策略，该策略会锁定尝试从美国境外访问 Citrix 服务的用户。如果用户不识别其访问活动，则用户访问将被锁定。

条件：GW-地理围栏越界

操作：请求最终用户响应

下一步操作：如果用户不识别该活动，则锁定用户

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意

请求最终用户响应操作仅在美国地区受支持。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。

首次访问场景的预配置自定义风险指标

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
- Gateway - 首次从新 IP 访问

默认情况下，这些预配置的自定义风险指标处于启用状态。如果要禁用它们，请使用 **STATUS** 按钮。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

首次访问 CI 列表(/en-us/citrix-analytics/media/custom-ci-first-time-access.png)

下表描述了首次访问的预配置自定义风险指标。

自定义指标名称	场景	预配置条件	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任一位置登录时：	默认情况下启用以下条件：	本地部署的 Citrix Virtual Apps and Desktops 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）	受感染的用户
	新设备	新设备 ID 的首次访问。		
	过去 90 天内未使用的现有设备。	`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")`		
网关 - 从新 IP 首次访问	当 Citrix Gateway 用户成功从以下任一位置登录时：	默认启用以下条件：	Citrix 网关	受感染的用户

© 1997–2026 Citrix Systems, Inc. All rights reserved.

自定义指标名称	场景	预配置条件	数据源	风险类别
	新的公共 IP 地址	新客户端 IP 的首次访问		
	过去 90 天内未使用的现有公共 IP 地址。	`Event-Type = "Authentication" AND Status-Code = "Successful login" AND Client-IP-Type != "private" AND Access-Insight-Flags = 1`		

在条件栏中，除了预配置的条件外，您还可以根据自己的要求添加自己的条件来识别威胁。

例如，如果您想识别来自特定国家/地区的用户事件，您可以添加国家/地区维度以及预配置条件：

- `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”`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

终端用户电子邮件设置

终端用户电子邮件设置控制与全局操作请求终端用户响应关联的电子邮件模板。您应用此操作是为了获取用户对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响应。

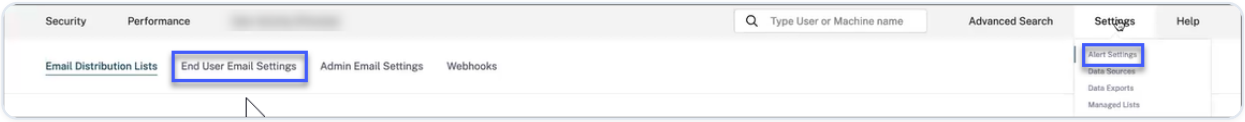
您可以使用电子邮件设置来执行以下操作：

- 添加适当的横幅、标题文本和页脚文本，以吸引用户注意力并获取他们的回复。这也会使您的电子邮件看起来更具合法性。
- 添加用户必须回复您的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回复，Citrix Analytics 会对该用户应用指定的操作。

修改电子邮件设置

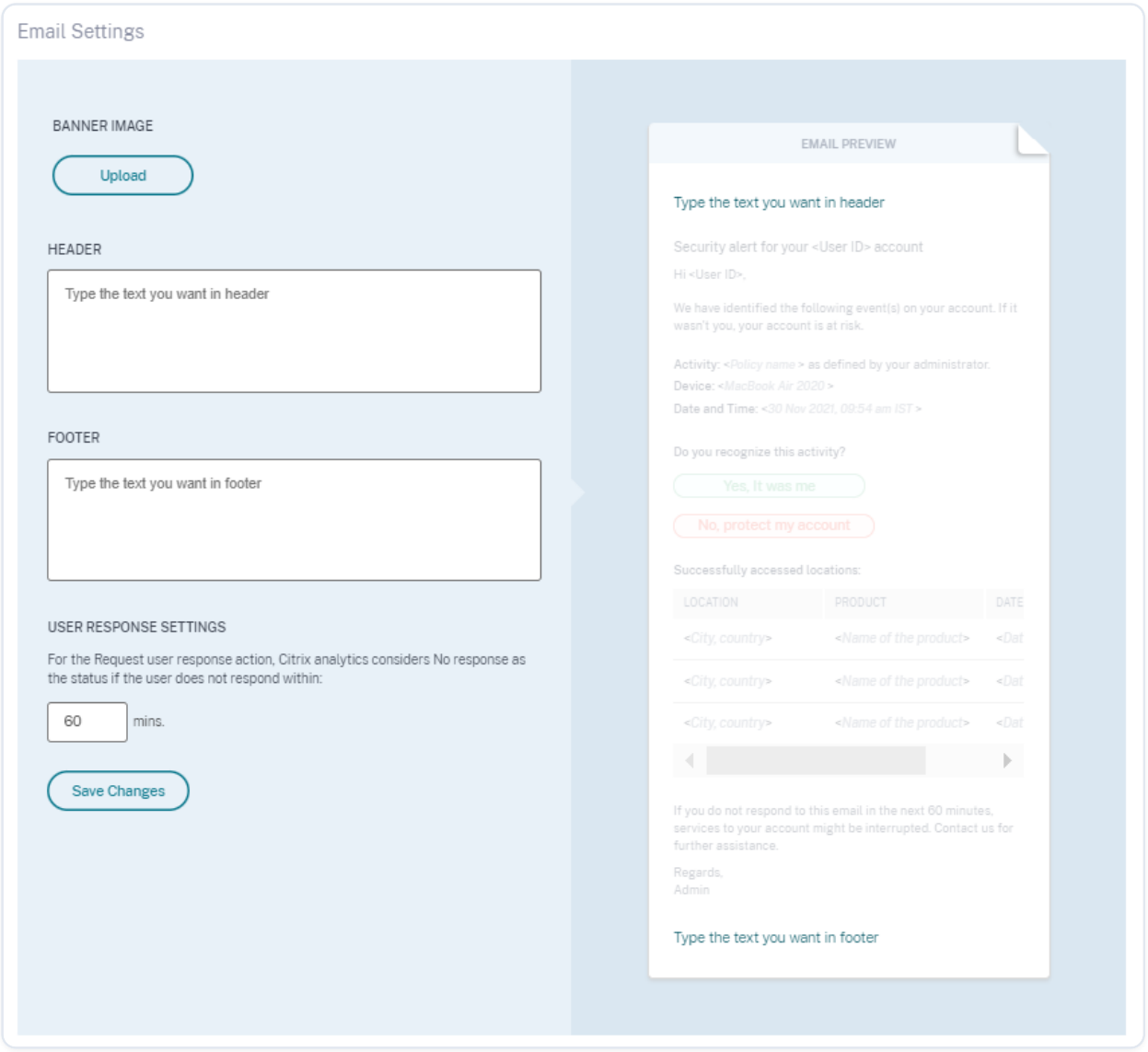
要修改电子邮件设置，请执行以下操作：

1. 在顶部栏上，单击 **“设置”>“警报设置”>“终端用户电子邮件设置”**。



2. 单击“编辑”以上传或浏览横幅图像。上传图像文件时，请确保图像满足以下要求：
    - 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 **“标题”** 和 **“页脚”** 字段中输入文本。这些字段是可选的。
4. 在用户响应设置中输入时间。
5. 预览电子邮件并点击**保存更改**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

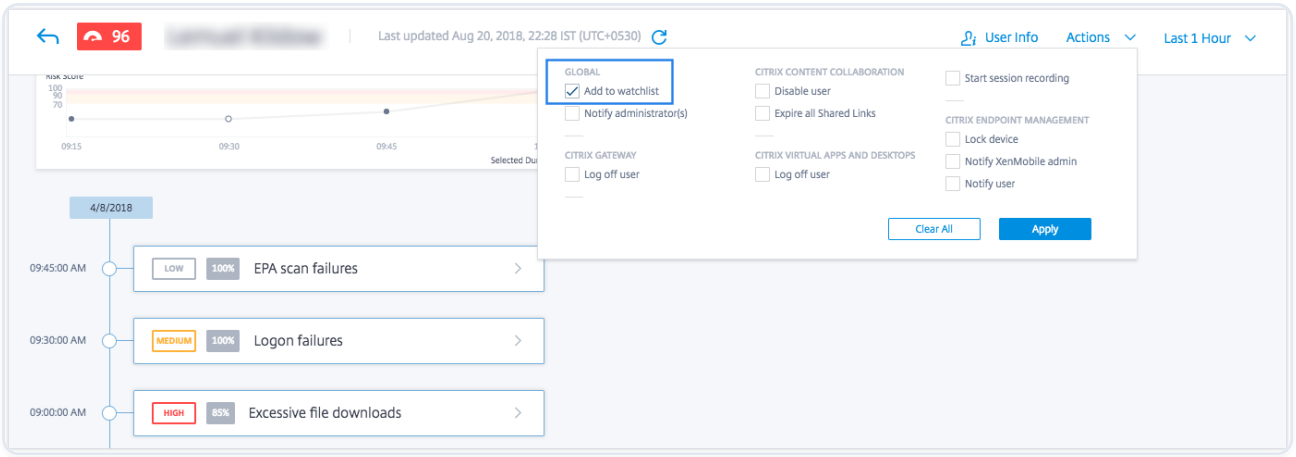
监视列表

使用监视列表监控特定用户的活动，以发现潜在威胁。例如，您可以监控组织中非全职员工的用户，或频繁触发特定风险指标的用户。

如何将用户添加到监视列表

您可以手动将用户添加到监视列表，也可以定义在触发时将用户添加到监视列表的策略。

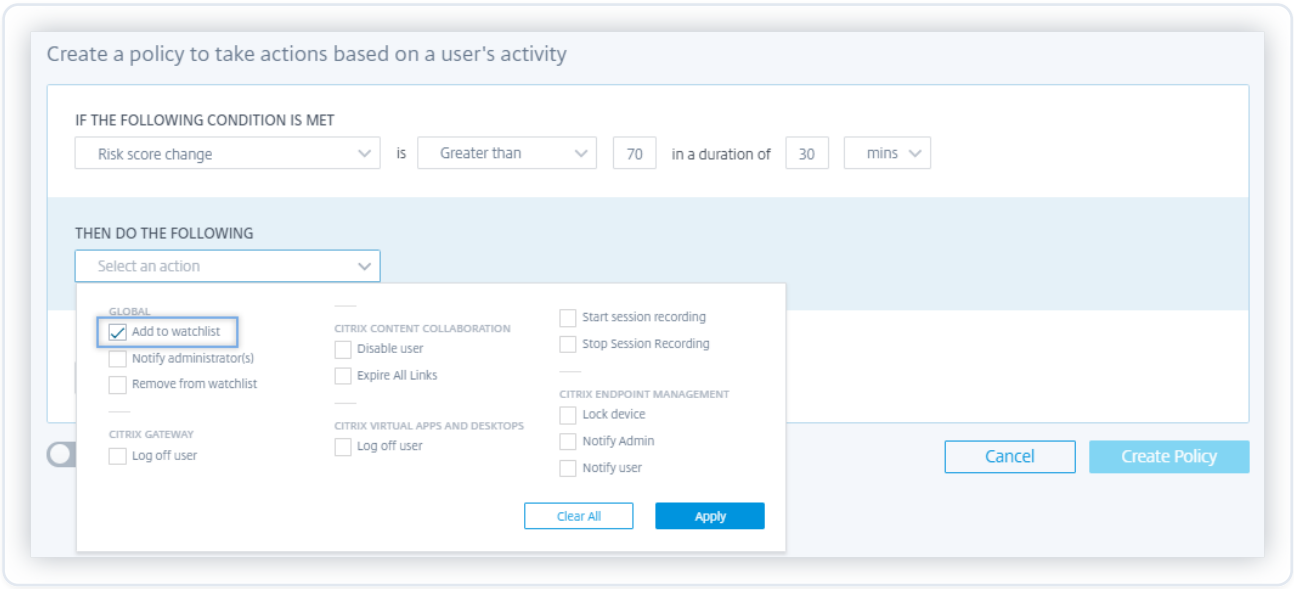
要手动将用户添加到监视列表，请导航到风险时间线上的用户个人资料。然后，从**操作**菜单中选择**添加到监视列表**。点击**应用**并按照提示执行此操作。



要使用策略将用户添加到监视列表，请创建包含一组必须满足的条件的策略。选择**添加到监视列表**操作。当条件满足时，用户将被添加到监视列表。例如，如果用户的风险评分在 30 分钟内变化大于 70，您可能希望将该用户添加到监视列表。

有关创建策略的更多信息，请参阅配置策略和操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



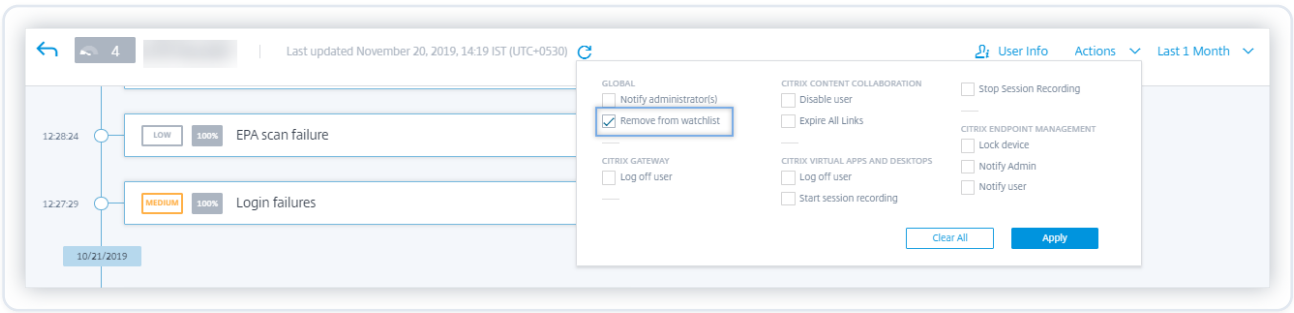
如何将用户从监视列表移除

您可以手动将用户从监视列表移除，也可以定义在触发时将用户从监视列表移除的策略。

要手动将用户从监视列表移除，请导航到风险时间线上的用户个人资料。然后，从**操作**菜单中选择**从监视列表移除**。点击**应用**并按照提示执行此操作。

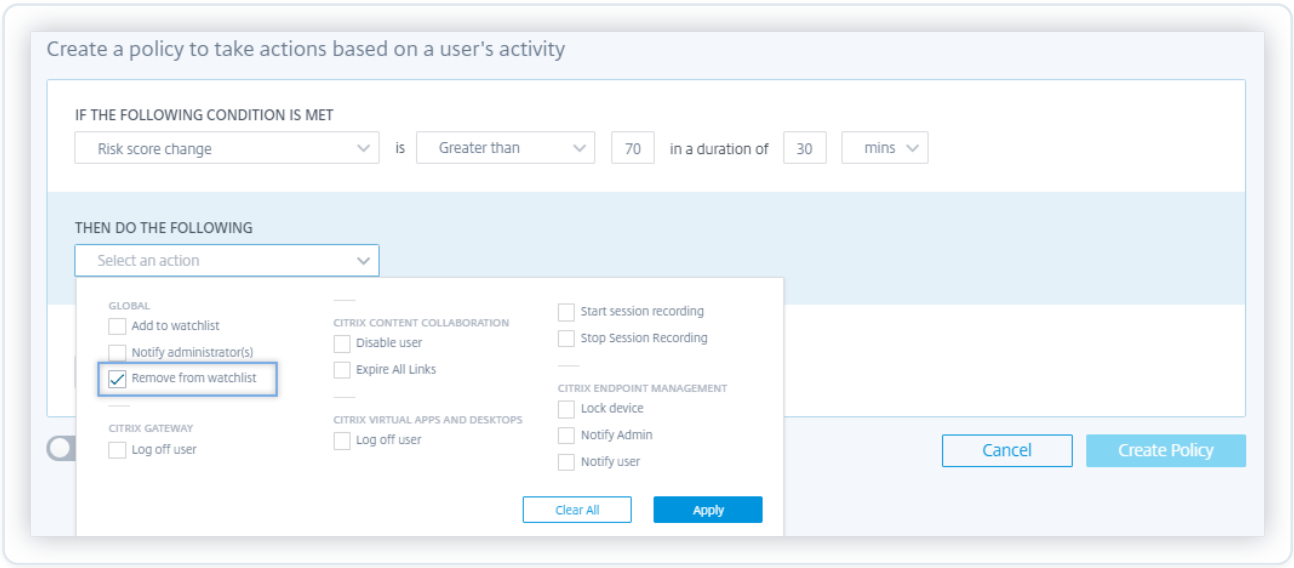
注意

当用户在监视列表中且您想移除他们时，您会在**操作**菜单中看到**从监视列表移除**选项。



使用策略将用户从观察列表中移除，请创建包含一组必须满足的条件的策略。选择“**从观察列表中移除**”操作。当条件满足时，用户将从观察列表中移除。例如，如果用户在 60 分钟内风险评分变化小于 70，您可能希望将该用户从观察列表中移除。要了解有关创建策略的更多信息，请参阅配置策略和操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



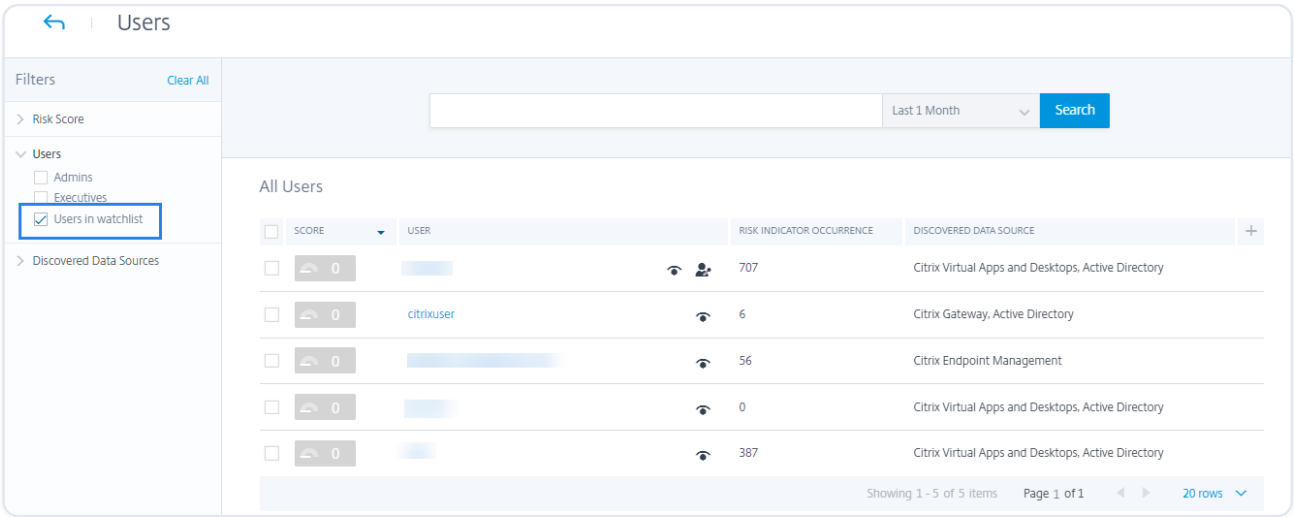
如何监控观察列表中的用户

在“**安全 > 用户**”仪表板上，查看以下内容：

- 过去 13 个月观察列表中的用户数量摘要。单击该框可在“**观察列表中的用户**”窗格中查看观察列表中所有用户的列表。
- 观察列表中根据风险评分列出的前五名用户。在“**观察列表中的用户**”窗格中，查看风险评分、风险指标发生次数以及用户名称。单击“**查看更多**”可在“**用户**”页面上查看观察列表中所有用户的列表。
- 观察列表中风险最高的用户。在“**风险用户**”窗格中，用户旁边的“眼睛”图标表示该用户在观察列表中。

在“**用户**”页面上，查看观察列表中所有用户的列表。查看用户的详细信息，例如风险评分、触发的风险指标数量以及关联的数据源。

使用搜索框查找用户及其事件详细信息。选择时间段以查看特定时间段内的风险指标发生次数。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

每周电子邮件通知

Citrix Analytics 会发送每周电子邮件通知，总结您组织 IT 基础设施中的安全风险暴露情况。每周通知让您了解并知晓上一周发生的风险事件及其发生情况。您无需登录 Citrix Analytics 即可了解是否有任何事件需要您的关注或采取行动。此信息让您随时了解 IT 安全领域中发生的情况。

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，则您的 Citrix Cloud 帐户中默认禁用电子邮件通知。要接收来自任何 Citrix Cloud 服务（例如 Citrix Analytics）的电子邮件通知，请在您的 Citrix Cloud 中启用通知选项。有关更多信息，请参阅接收电子邮件通知。通过 Active Directory/Azure AD 组添加的管理员无法使用通知首选项。
- 默认情况下，电子邮件通知会发送给 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分发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。

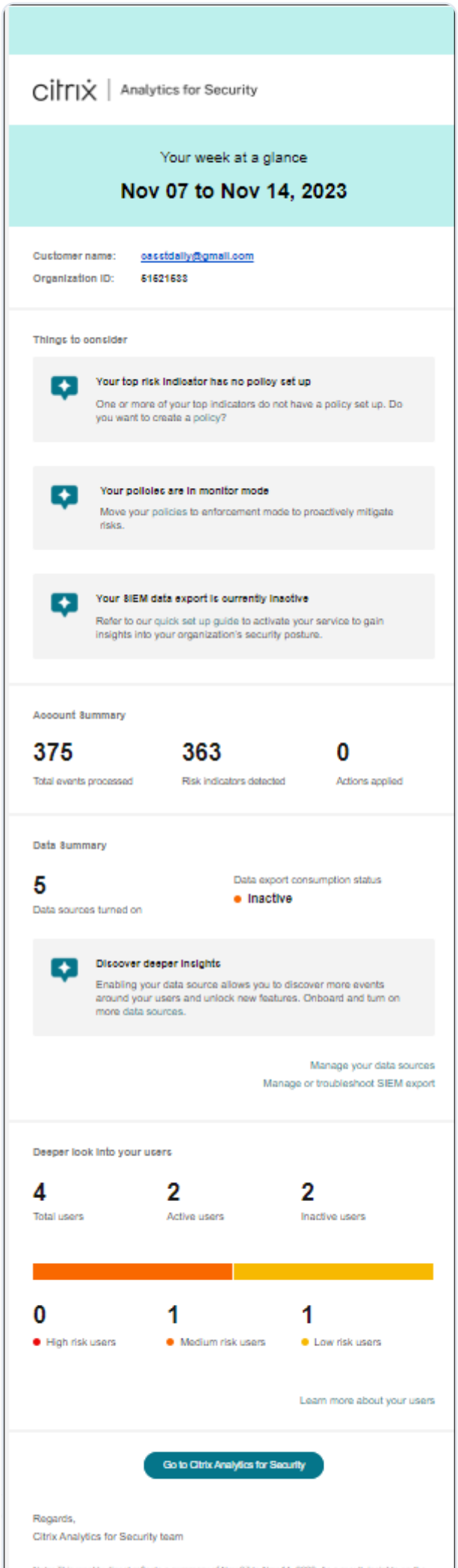
您何时会收到来自 Citrix Analytics 的电子邮件?

每个星期二，Citrix Cloud 都会向您发送一封电子邮件通知 mailto:donotreplynotifications@citrix.com。

电子邮件通知提供以下信息：

- 已处理事件总数、检测到的风险指标以及已应用操作的摘要
- 活动数据源总数和数据导出消耗状态的摘要
- 前三名风险指标
- 对风险指标采取的前三项操作
- 活动用户总数和风险用户总数
- 任何需要您关注的事件或操作

© 1997–2026 Citrix Systems, Inc. All rights reserved.



citrix | Analytics for Security

Your week at a glance

Nov 07 to Nov 14, 2023

Customer name: casstdaily@gmail.com
Organization ID: 51521633

Things to consider

Your top risk indicator has no policy set up

One or more of your top indicators do not have a policy set up. Do you want to create a policy?

Your policies are in monitor mode

Move your policies to enforcement mode to proactively mitigate risks.

Your SIEM data export is currently inactive

Refer to our quick set up guide to activate your service to gain insights into your organization's security posture.

Account Summary

375	363	0
Total events processed	Risk indicators detected	Actions applied

Data Summary

5
Data sources turned on

Data export consumption status
● Inactive

Discover deeper insights

Enabling your data source allows you to discover more events around your users and unlock new features. Onboard and turn on more data sources.

Manage your data sources
Manage or troubleshoot SIEM export

Deeper look into your users

4	2	2
Total users	Active users	Inactive users

0	1	1
● High risk users	● Medium risk users	● Low risk users

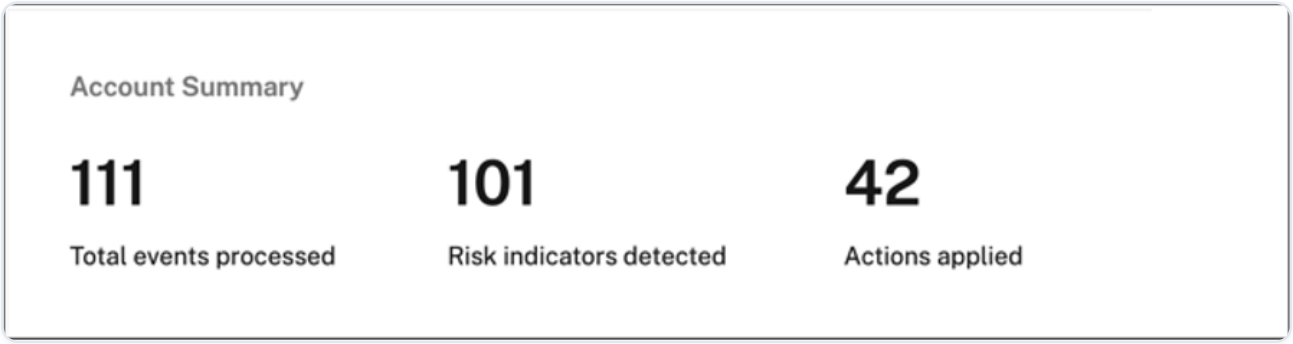
Learn more about your users

Go to Citrix Analytics for Security

Regards,
Citrix Analytics for Security team

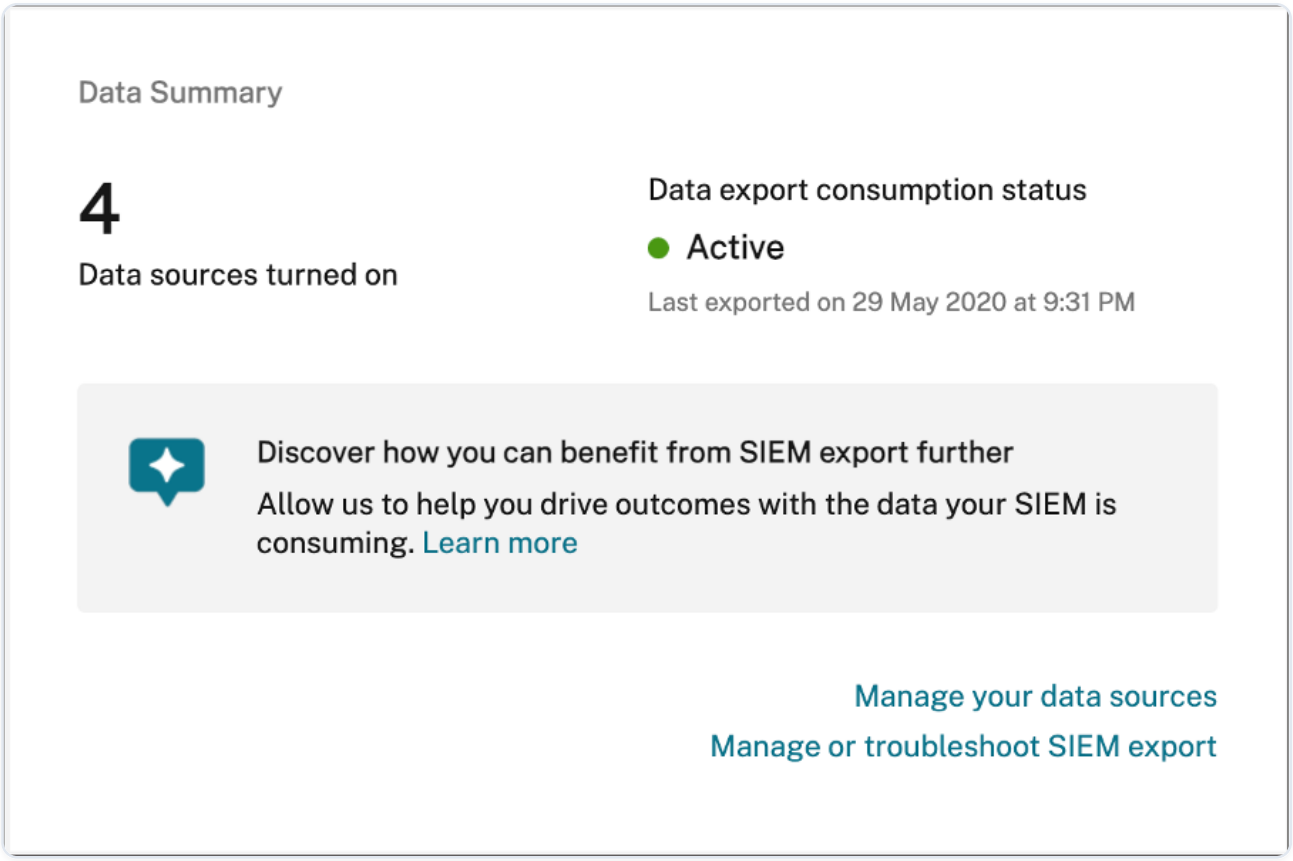
账户摘要

每周电子邮件提供已处理事件总数、检测到的风险指标以及已应用操作的摘要。



数据摘要

每周电子邮件还提供有关已启用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**”以在 Citrix Analytics 中查看“**数据源**”页面。您可以载入数据源并启用数据处理，以使 Citrix Analytics 能够处理数据。有关启用分析的更多信息，请参阅数据源上的启用分析。

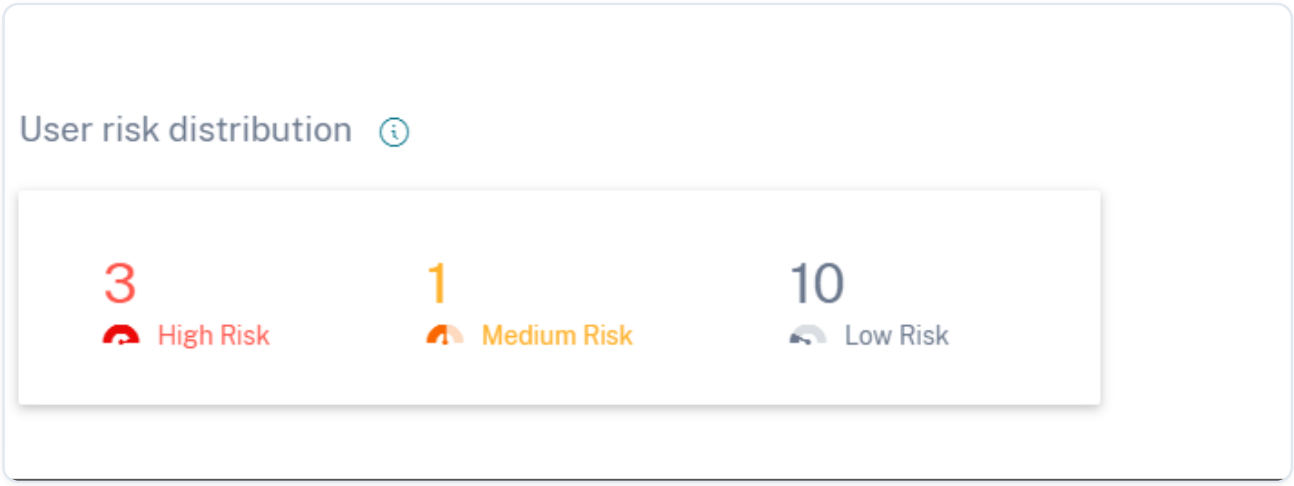
单击“**管理或排查 SIEM 导出**”以在 Citrix Analytics 中查看“数据导出”页面，从而排查您的环境并管理您的数据导出设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

用户信息

每周电子邮件提供有关用户总数以及行为存在风险的用户的见解。

- **高风险用户数** – 以红色标识。他们对组织构成直接威胁。
- **中风险用户数** – 以橙色标识。他们在所选周内其帐户存在多项严重违规行为，必须密切监控。
- **低风险用户数** – 以黄色标识。他们的帐户存在少量严重违规行为，但潜在地不被视为威胁。



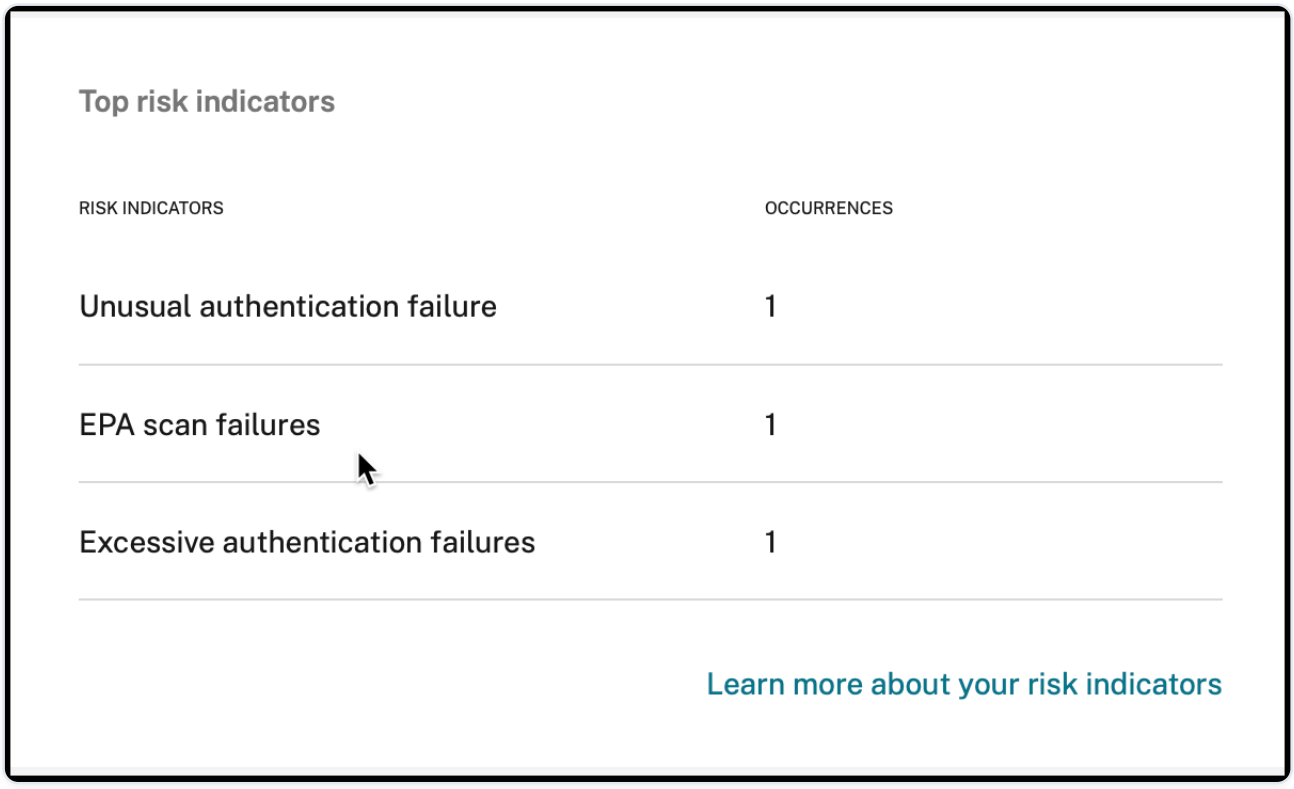
有关更多信息，请参阅风险用户。

点击“**了解有关您的用户的更多信息**”以在 Citrix Analytics 中查看“**风险用户**”页面。您可以深入了解活跃用户和风险分类。

热门风险指标

每周电子邮件提供有关所选周排名前三的风险指标及其出现次数的见解。根据出现次数，将显示所选周的默认和自定义风险指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



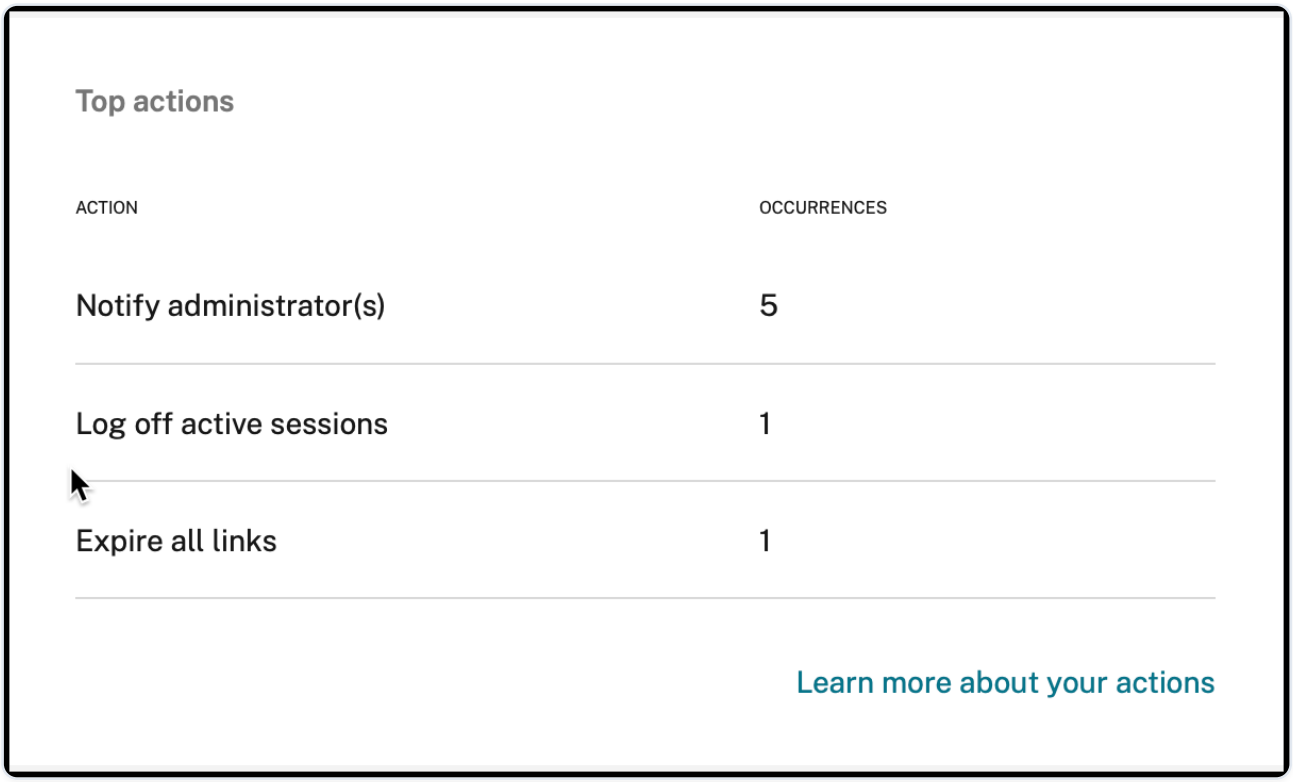
有关更多信息，请参阅风险指标。

点击电子邮件中的“**了解有关您的风险指标的更多信息**”以在 Citrix Analytics 中查看“**风险指标概述**”页面。

热门操作

每周电子邮件提供有关上周发生的异常和可疑威胁所采取的排名前三的操作的见解。根据出现次数，将显示所选周的全局操作和 Citrix Gateway 操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



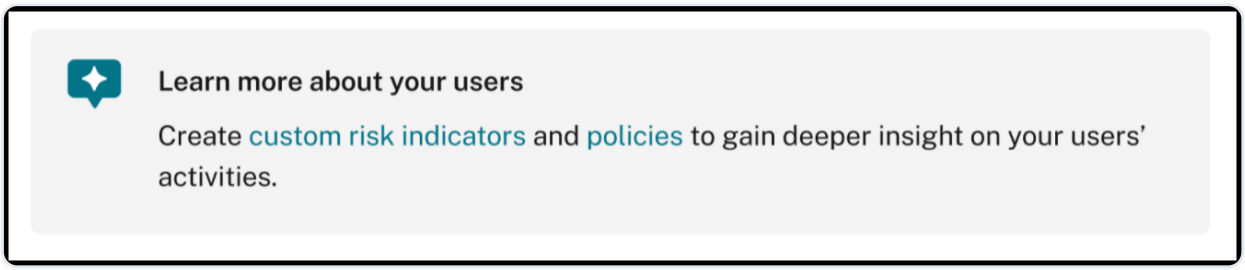
有关操作以及配置操作的更多信息，请参阅策略和操作。

点击电子邮件中的“**了解有关您的操作的更多信息**”以在 Citrix Analytics 中查看“**热门操作**”页面。

收到电子邮件后需要执行哪些操作?

每周电子邮件可让您了解是否有任何事件或操作需要您关注。

- 如果本周未检测到风险指标，您将收到以下消息，提示您创建更多自定义风险指标。



您可以登录 Citrix Analytics 以创建更多自定义风险指示器。

- 如果安全分析中未启用任何数据源，您将收到以下消息，提示您为数据源启用数据处理。

  未启用任何数据源(/en-us/citrix-analytics/media/turnon-data-sources-security-analytics.png)

- 如果没有策略处于监视模式，您将收到以下消息，提示您将策略移至强制模式。

  监视模式下的策略(/en-us/citrix-analytics/media/policies-monitoring-mode.png)

- 如果本周排名前 3 位的风险指示器没有设置任何策略，您将收到以下消息，提示您创建策略。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

未设置策略(/en-us/citrix-analytics/media/top-risk-indicator-no-policy.png)

- 如果您尚未为 Citrix Analytics 租户启用**数据导出**，以下建议将引导您了解有关我们的**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。

  启用数据导出(/en-us/citrix-analytics/media/enable-siem-dataexport.png)

- 如果数据导出消耗状态不活动，您将收到以下消息，提示您激活服务。

  数据导出消耗状态(/en-us/citrix-analytics/media/dataexport-consumption-status.png)

注意

仅当至少为一个数据源启用数据处理时，数据传输才会启用。如果所有数据源的数据处理都已关闭，您将收到以下警告消息，提示您启用数据源。

已启用数据传输(/en-us/citrix-analytics/media/action-req.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

审计日志

审计日志描述了在 Citrix Analytics 上生成的事件的审计信息。它们可以是系统事件（例如错误），也可以是 Citrix Analytics 管理员执行的配置操作的审计跟踪。

每当添加、删除或更新配置时，事件信息都会写入审计日志。此信息包括修改了什么、何时修改以及由谁修改。

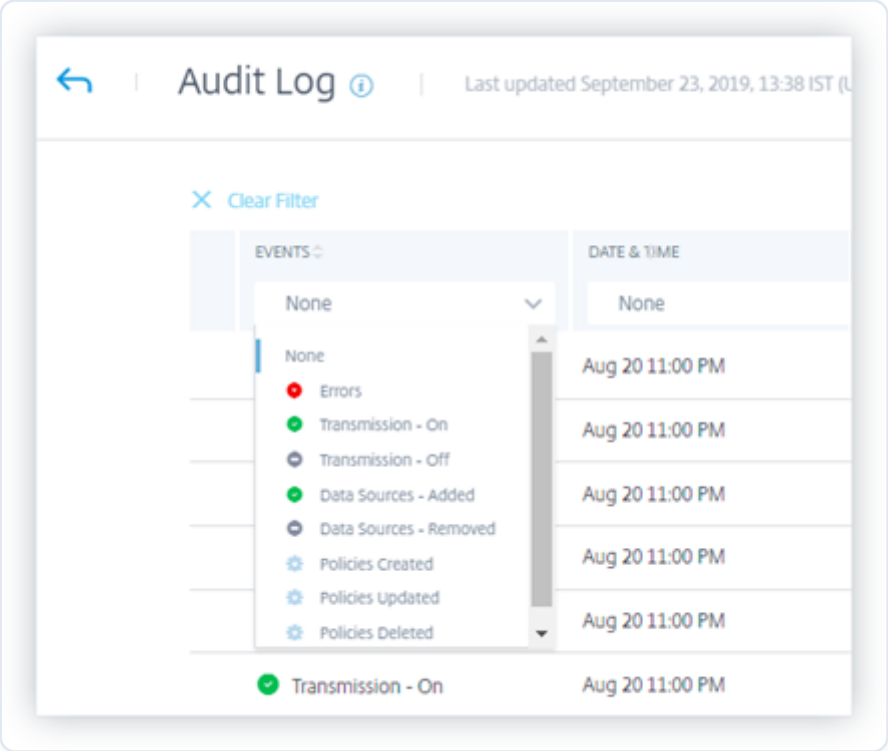
您可以查看过去三个月的审计日志信息。

生成审计事件的活动

以下事件在 Citrix Analytics 上注册：

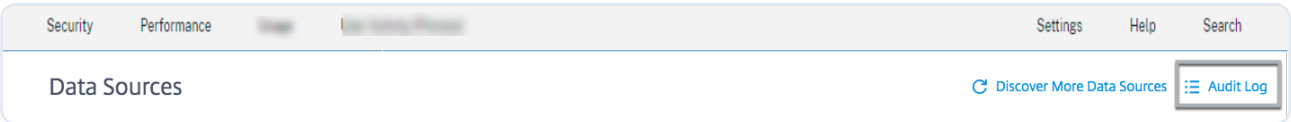
- 生成的错误
- 传输已开启
- 传输已关闭
- 已添加数据源
- 已删除数据源
- 已创建策略
- 已更新策略
- 已删除策略

© 1997–2026 Citrix Systems, Inc. All rights reserved.



如何查看审计日志

要查看审计日志，请登录 Citrix Analytics。导航到 **设置 > 数据源**。在 **数据源** 页面上，单击右上角的 **审计日志**。



如何使用审计日志

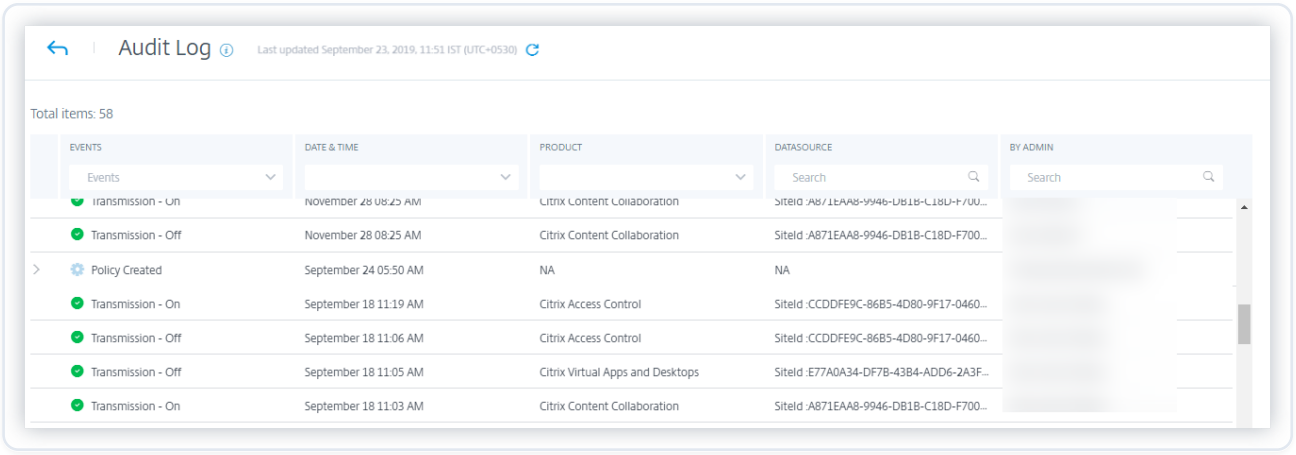
您可以使用审计日志来审查并了解 Citrix Analytics 上的任何事件。刷新 **审计日志** 页面以获取最新的审计数据。该页面显示审计数据上次更新的日期和时间。

您可以在 **审计日志** 页面上查看以下审计信息。您还可以根据这些字段筛选审计数据。

- **事件**。事件可以是系统生成的，也可以是管理员在 Citrix Analytics 上应用的配置。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，会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期间进行筛选。您可以查看当天、最近七天、最近 15 天、上个月和最近三个月的事件。
- **产品**。生成事件的产品。事件在产品上生成，并在 Citrix Analytics 上聚合显示。您可以根据一个或多个产品筛选日志。

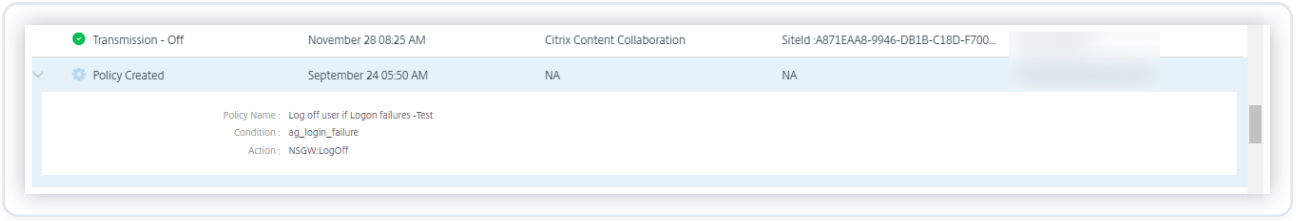
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **数据源**。与审计条目关联的产品实例名称。您可以搜索任何特定的数据源以查看其审计数据。
- **按管理员**。执行管理活动的 Citrix Analytics 管理员。您可以搜索由任何特定管理员执行的活动。



如果您注册的事件基于策略，您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
- 结果操作



© 1997–2026 Citrix Systems, Inc. All rights reserved.

自定义报告

您可以使用 Citrix Analytics for Security 中提供的事件和洞察来创建和安排自定义报告。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随时间推移的安全性。

自定义报告支持以下数据源：

- 应用程序和桌面
- 网关
- 安全私有访问
- 安全浏览器
- 策略
- 风险指标
- 风险评分

自定义报告中支持的字段

某些数据源也可用于自助搜索。要查看这些事件类型和支持的字段，请单击以下数据源。

- 应用程序和桌面
- 网关
- 安全私有访问
- 安全浏览器
- 策略

以下数据源仅在自定义报告中可用。下表列出了以下数据源在自定义报告中支持的字段：

- 风险指标
- 风险评分

© 1997–2026 Citrix Systems, Inc. All rights reserved.

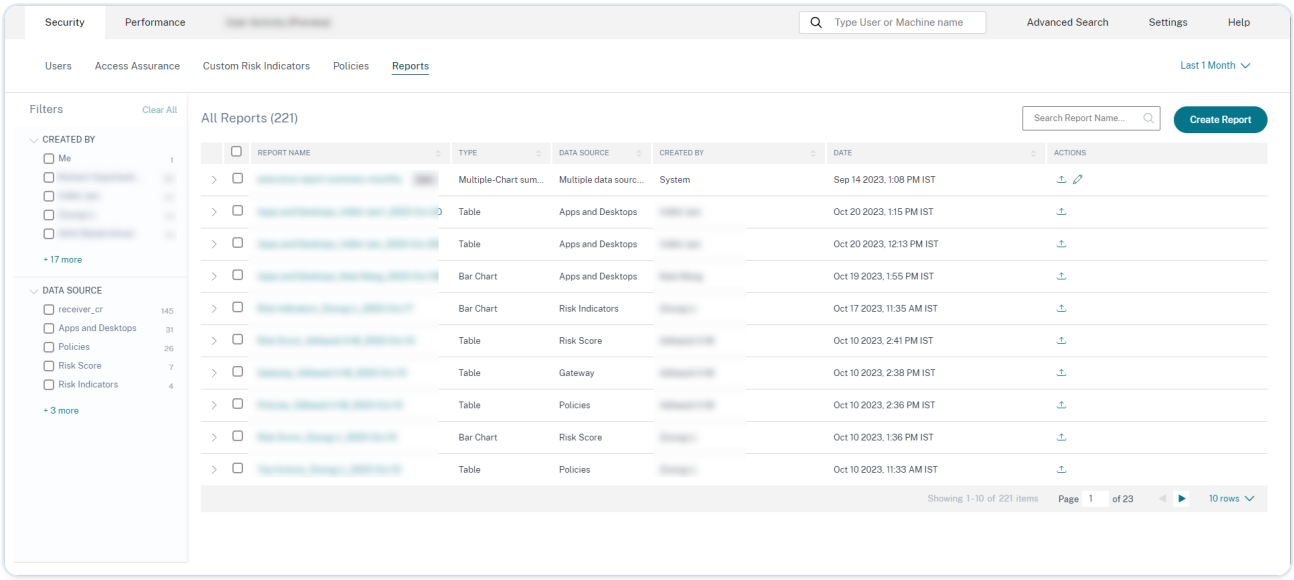
数据源	维度	描述
风险指标	类别	指示风险指标的类别。风险指标分为以下四类之一：受感染的端点、受感染的用户、数据泄露或内部威胁。
	风险指标名称	风险指标的名称。对于自定义风险指标，名称由管理员在创建指标时定义。
	严重性	指示风险的严重性。可以是低、中或高。
	用户名	用于登录的用户名或域\用户名。
风险评分	风险评分	分配给用户的风险评分。风险评分根据与用户活动相关的威胁严重性，在 0 到 100 之间变化。
	用户名	用于登录的用户名或域\用户名。
	风险评分类别	根据风险评分，有风险的用户可分为以下几类：高风险、中风险和低风险。

报告

您可以使用此视图对报告执行以下操作：

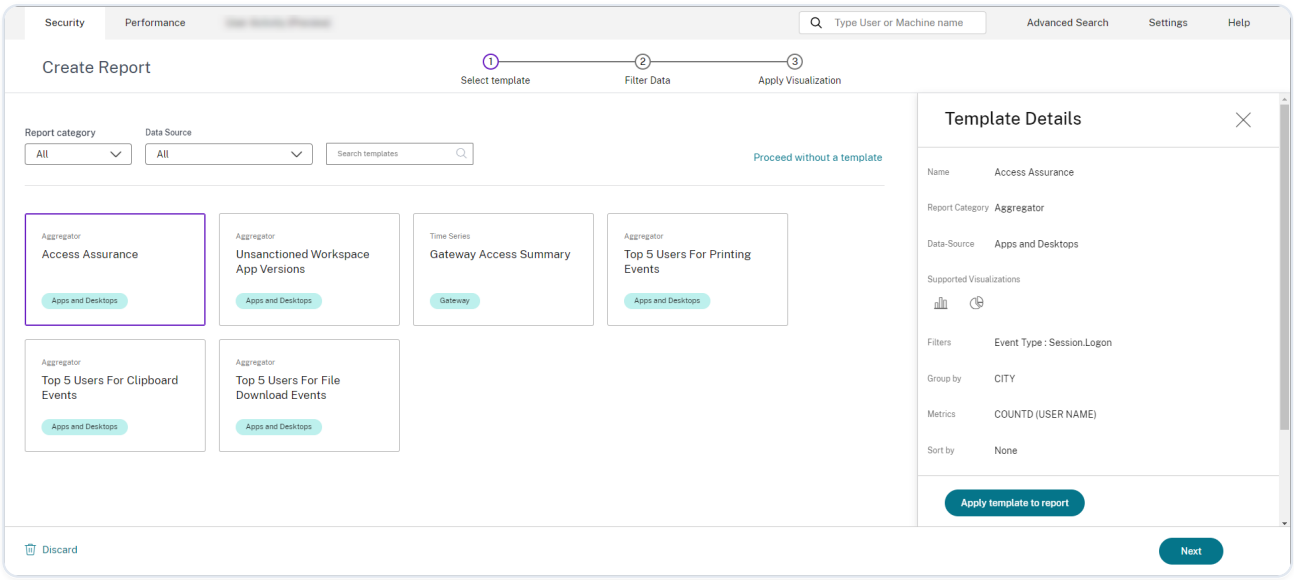
- 点击 **创建报告** 以创建自定义报告。
- 展开一行以查看现有自定义报告的预览。
- 点击报告名称以查看详细的报告可视化。
- 点击导出图标以 PDF 格式导出现有自定义报告。
- 点击编辑图标以编辑您已创建的报告。
- 点击删除图标以删除您已创建的报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



创建自定义报告

要创建自定义报告，请点击**创建报告**。在**创建报告**页面上，您可以选择创建带模板或不带模板的自定义报告。

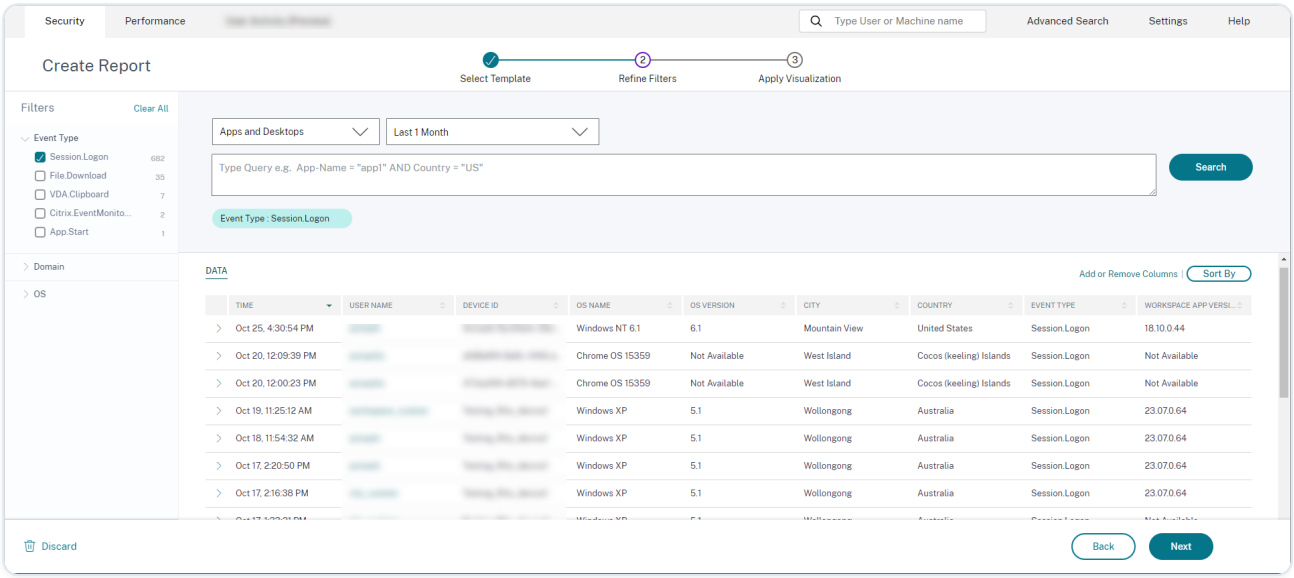


使用模板创建自定义报告

要使用模板创建自定义报告：

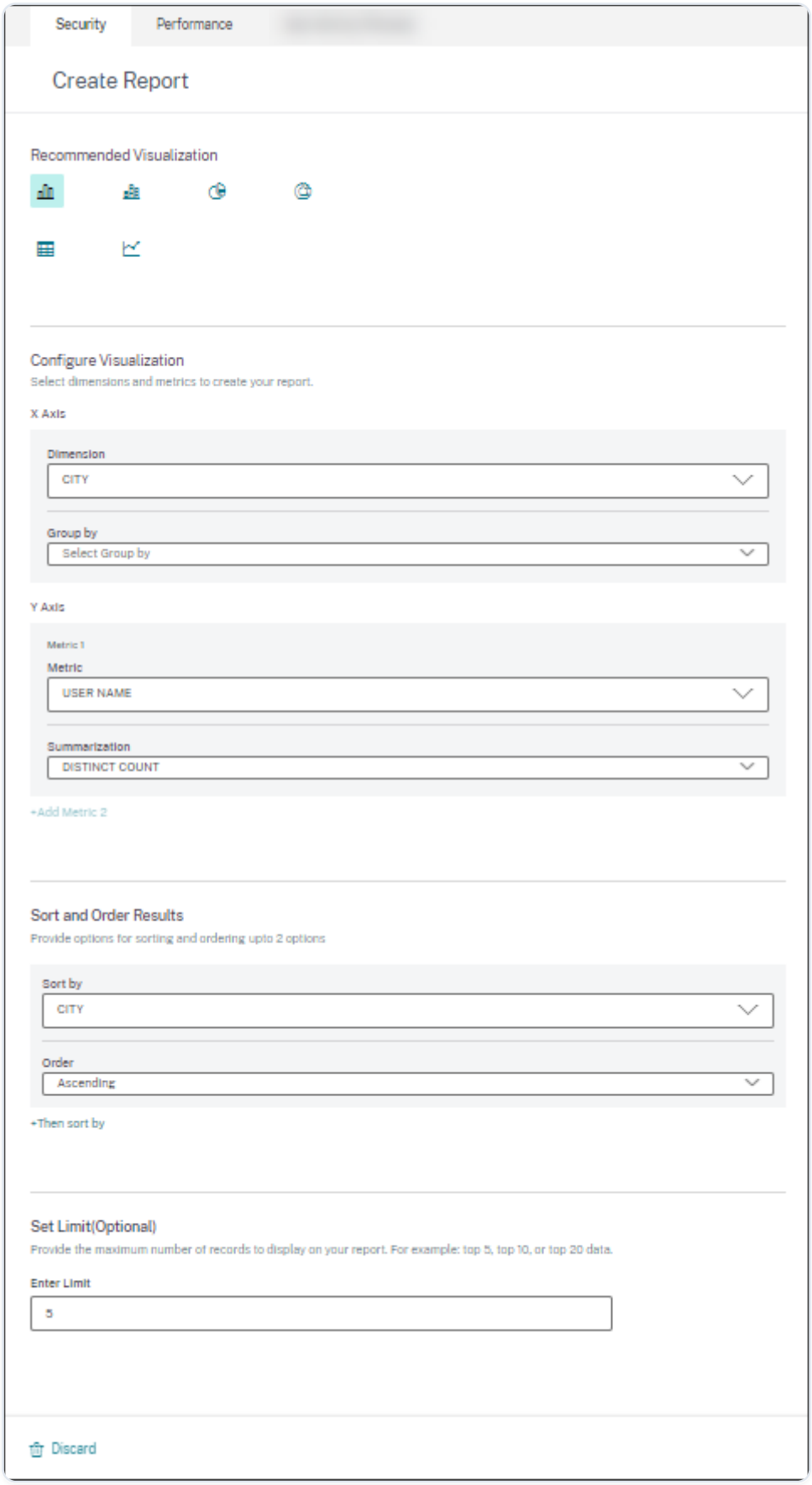
1. **选择模板**：点击模板后，模板详细信息将显示在右侧。点击**将模板应用于报告**以使报告使用所选模板。
2. **优化筛选器**：**优化筛选器**页面显示了为您选择的模板预定义的筛选器。进行必要的更改，然后点击**下一步**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. **应用可视化**：选择一个可用的可视化来显示报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **条形图**：以垂直矩形条形图显示数据，其高度与值成比例。用于比较事件。
- **堆叠柱状图**：以相互堆叠的条形图形式显示数据。用于可视化多个子类别数据的总和。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

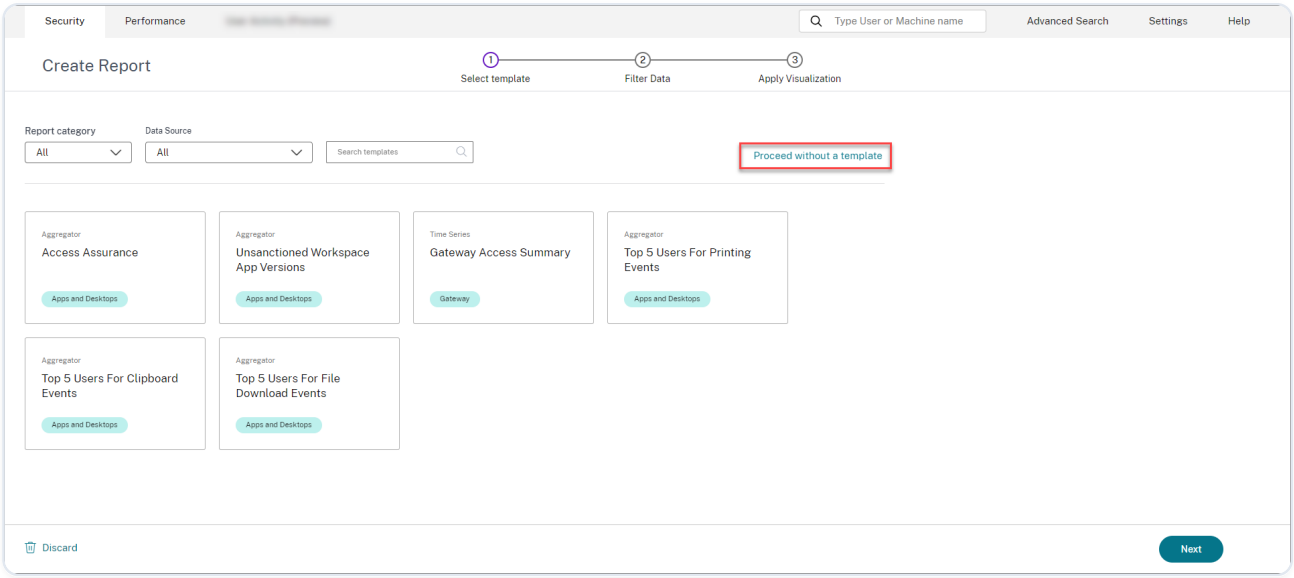
- **饼图**：以饼状形式呈现数据。用于可视化数据的相对大小或百分比。
- **甜甜圈图**：以甜甜圈形式呈现数据。用于可视化数据的相对大小或百分比。 - **表格**：以表格形式呈现数据。用于可视化所需的所有维度。
- **折线图**：以直线段连接的点来呈现数据。用于可视化一段时间内的数据趋势。

1. 现在使用以下参数配置可视化：

    - X 轴的维度
    - 要在 Y 轴中绘制的指标
    - 要应用于指标的汇总或聚合，例如平均值或计数
    - 排序和排列选项
    - 报告上显示的最大记录数的可选限制。

创建无模板的自定义报告

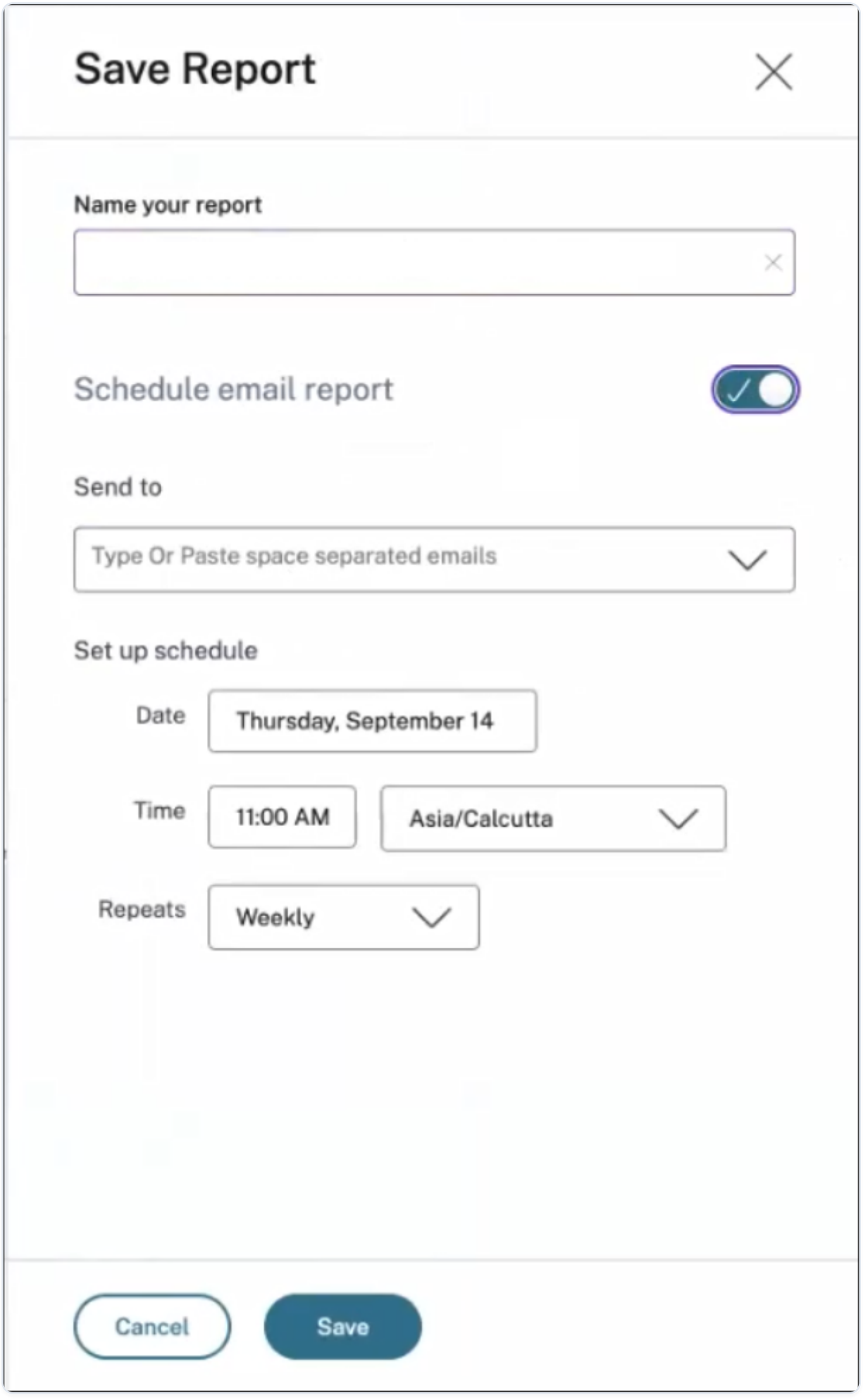
您还可以创建不带预定义模板的自定义报告。点击**创建无模板的自定义报告**。从下拉列表中选择一个数据源。按照步骤定义筛选器、应用可视化、保存并安排报告。



保存报告

1. 要保存报告，请点击**保存**。为您的报告指定一个标题。
2. 您可以安排在特定日期和时间或按重复计划将报告通过电子邮件发送给指定的电子邮件 ID 和分发列表。

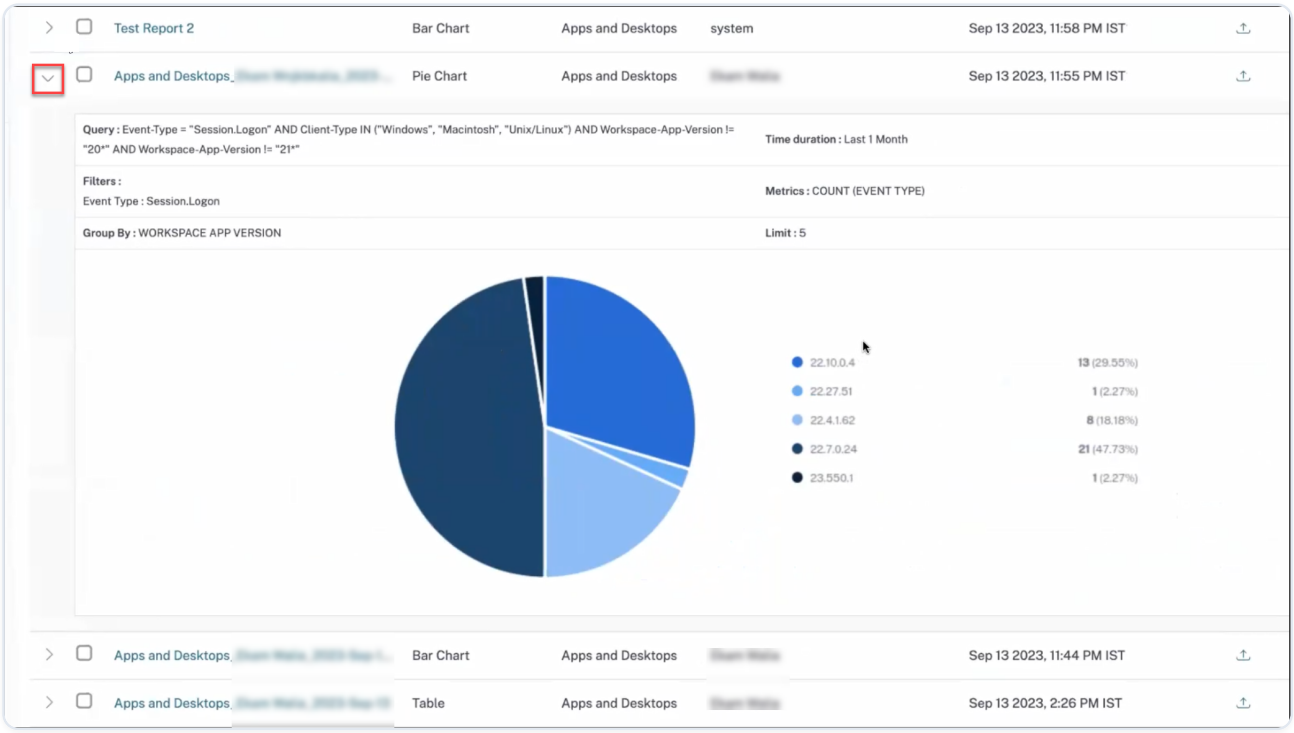
© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

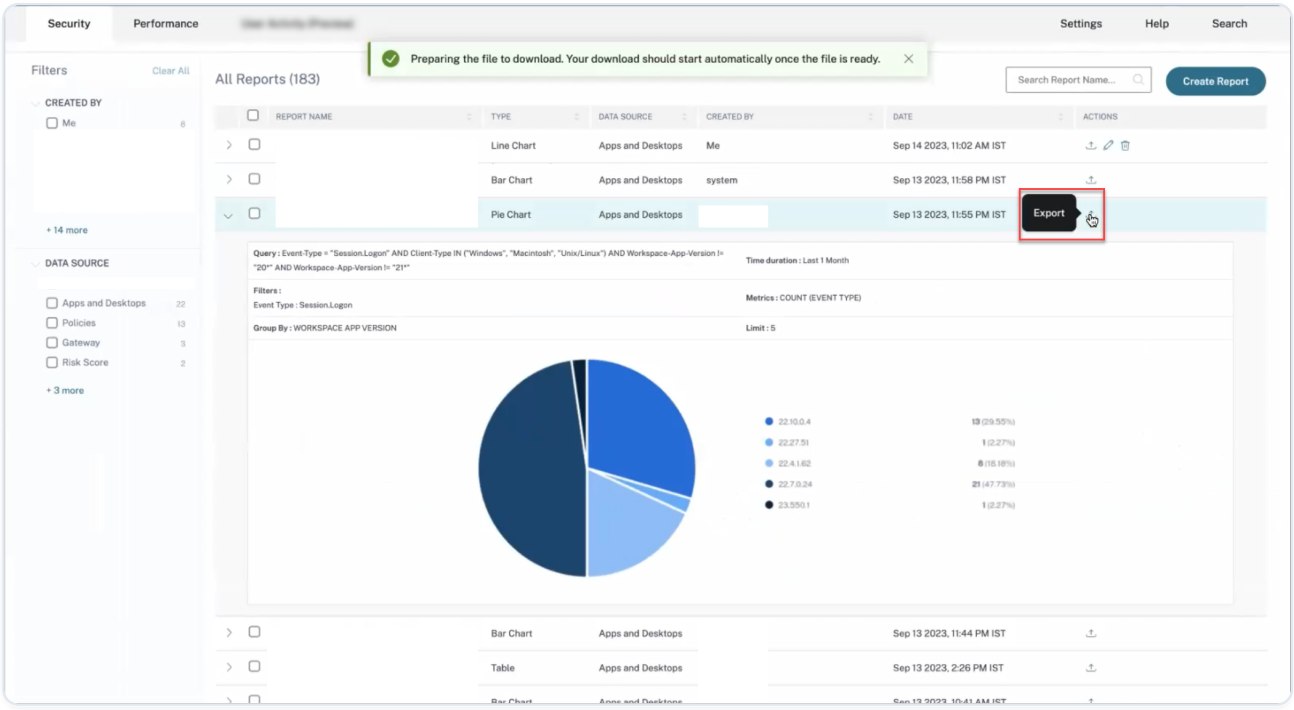
查看报告

1. 创建并保存报告后，您可以在**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. 点击下拉按钮预览报告。



导出报告

点击导出图标导出报告。



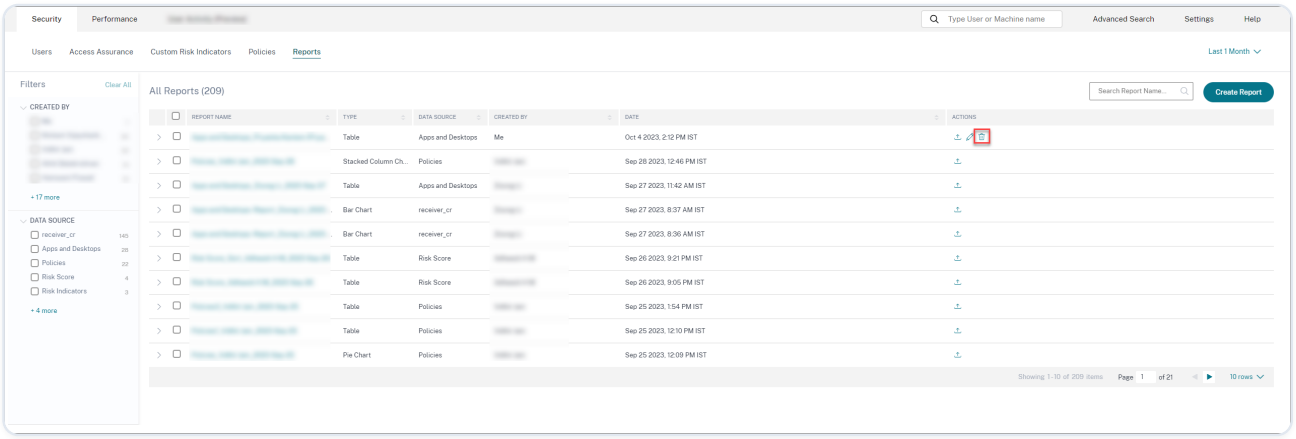
© 1997–2026 Citrix Systems, Inc. All rights reserved.

删除报告

点击删除图标删除报告。

注意：

> 只有创建报告的用户才能删除报告。

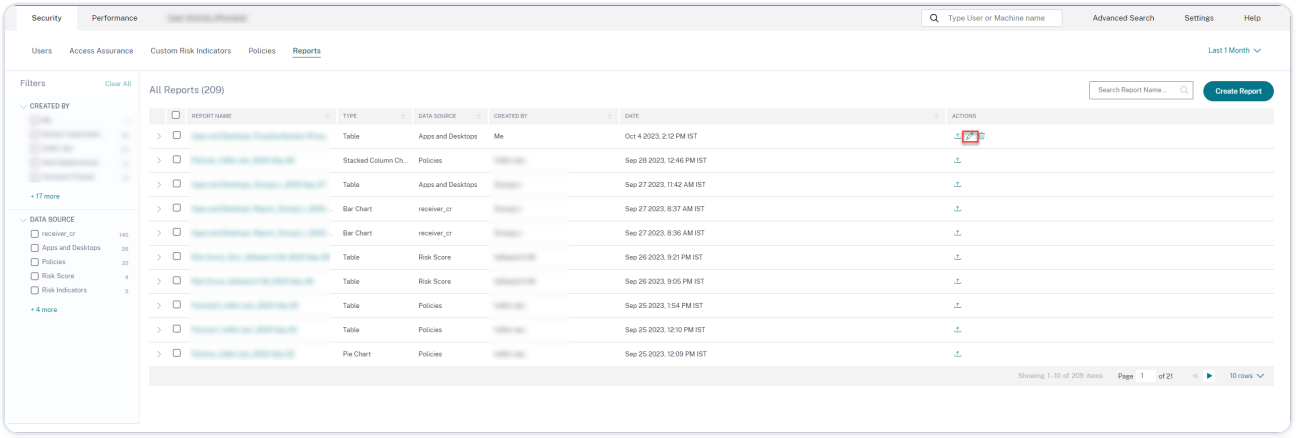


编辑报告

点击编辑图标编辑报告。

注意：

> 只有创建报告的用户才能编辑报告。



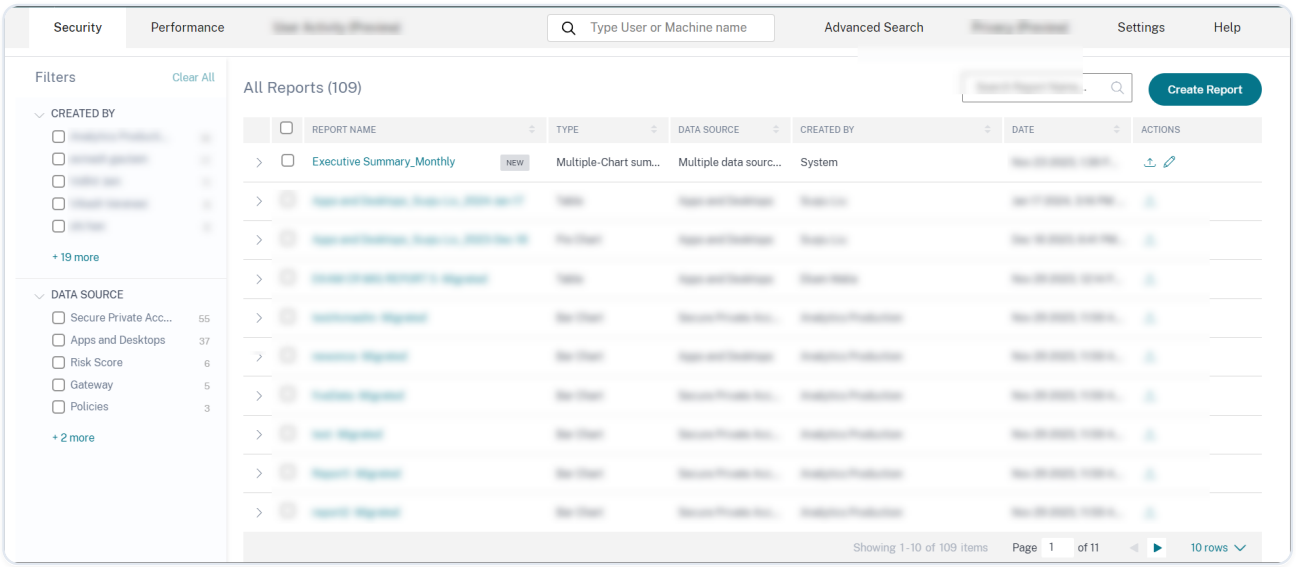
执行摘要报告

您可以安排通过电子邮件自动导出，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的集合，可在选定时间段内，为您选择的受众一目了然地描绘您企业的安全态势。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以为以下时间段的数据创建报告：

- 过去 1 小时
- 过去 12 小时
- 过去 1 天
- 过去 1 周
- 过去 1 个月



它包含哪些报告?

执行摘要报告包含以下报告：

- **用户风险分布**：根据用户在选定时间段内的最高计算风险评分，显示高、中、低风险配置文件的分布情况。
- 风险最高的用户：在选定时间段内，所有用户中按风险评分从高到低排序的风险最高的用户。
- **按类别划分的风险事件**：按风险类别提供的风险暴露类型和需要立即采取行动的关键风险的综合视图。风险指标分为以下几类：
  - 受感染用户
  - 受感染端点
  - 数据泄露
  - 内部威胁
- **风险指标**：在选定时间段内为用户触发的风险指标。
- **操作**：在选定时间段内对为用户触发的风险指标应用的操作。
- **热门策略**：在选定时间段内触发次数最多的前五项策略。

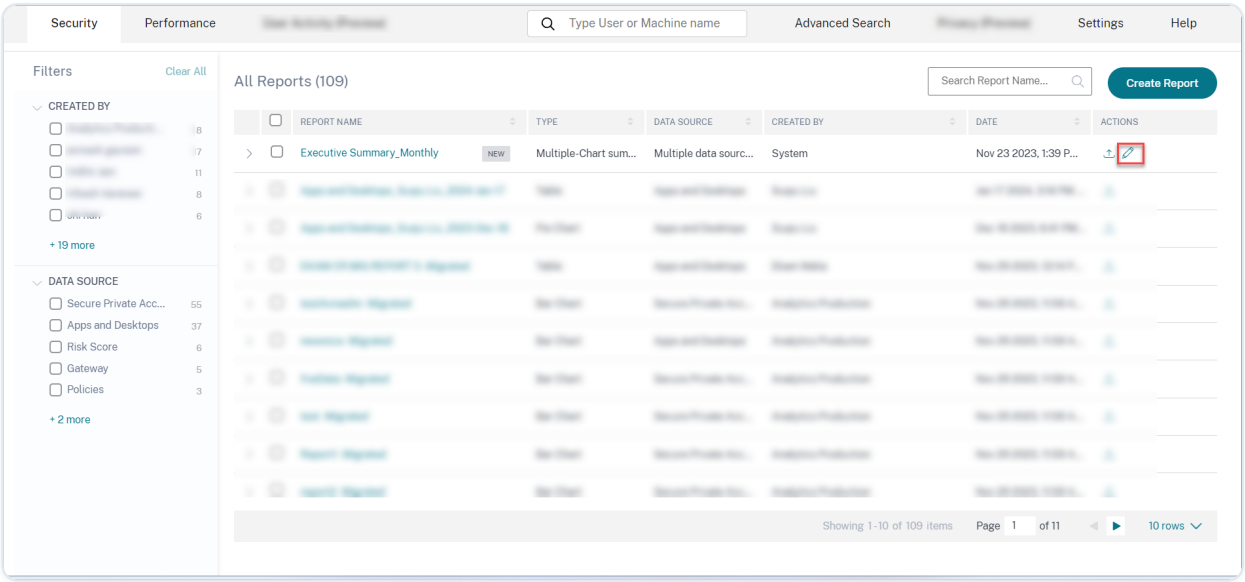
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **热门操作**：在选定时间段内触发次数最多的前五项操作。
- **按严重性划分的风险指标**：用户触发的默认和自定义风险指标，按严重性排序。
- **按总事件数划分的风险指标**：用户触发的默认和自定义风险指标，按事件数排序。

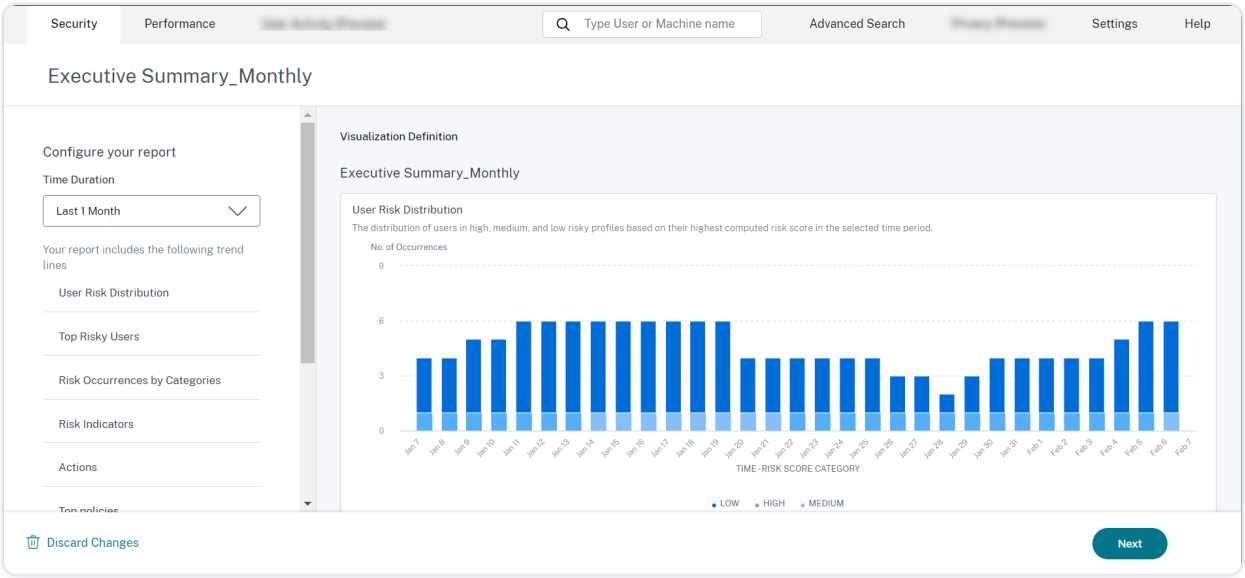
编辑执行报告

要编辑执行报告，请完成以下步骤：

1. 单击“**编辑**”符号。



2. 在 **配置报告** 窗格中，选择您想要查看数据的时间范围。



3. 点击 **下一步**。**保存报告** 窗格随即出现。

注意：

要放弃更改，请点击 **放弃更改**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

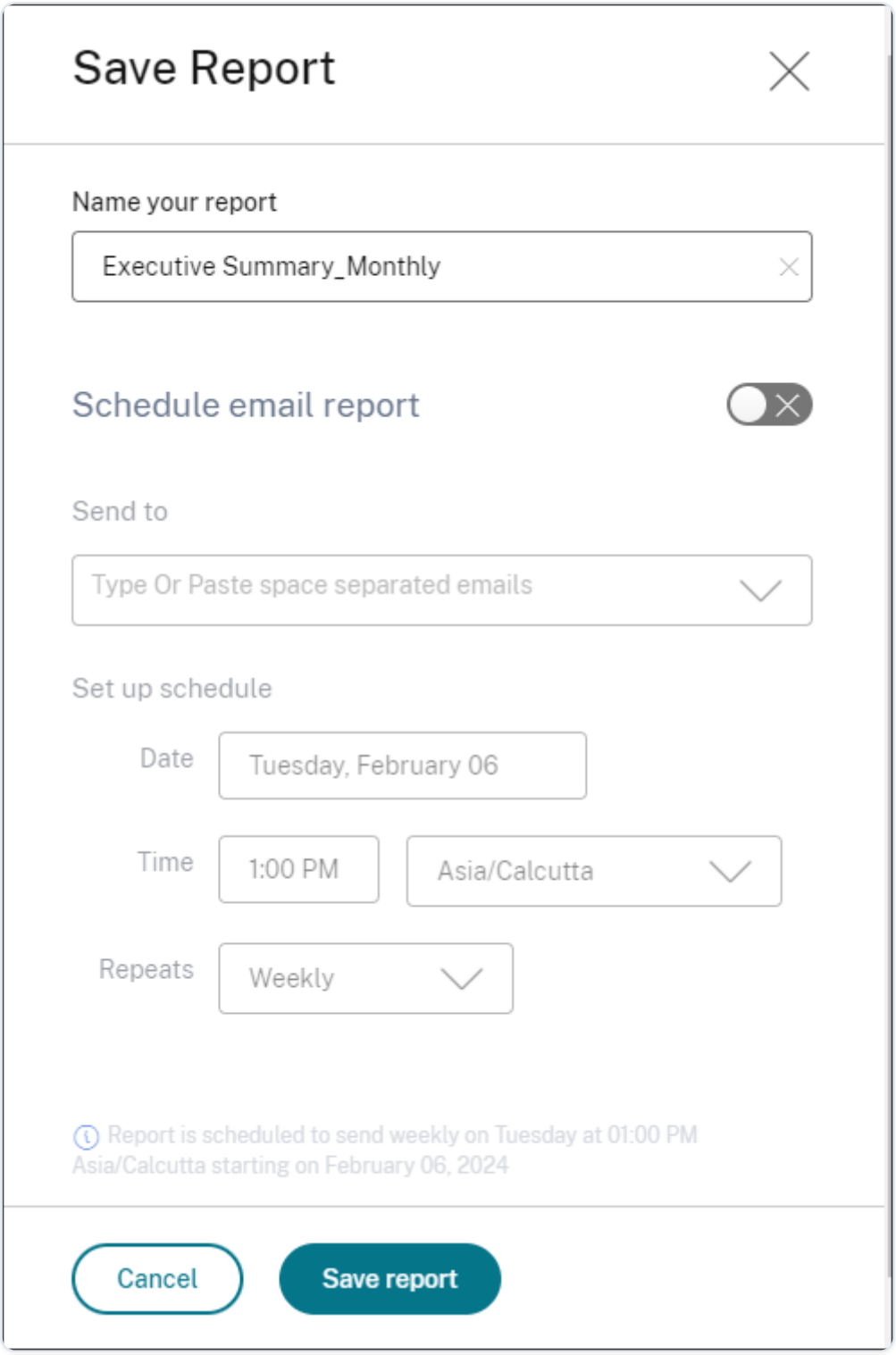
4. 在 **保存报告** 窗格中，输入以下详细信息：

   a. **报告名称**：高管报告的名称。

   b. **安排电子邮件报告**：打开此开关以安排报告。此开关默认关闭。

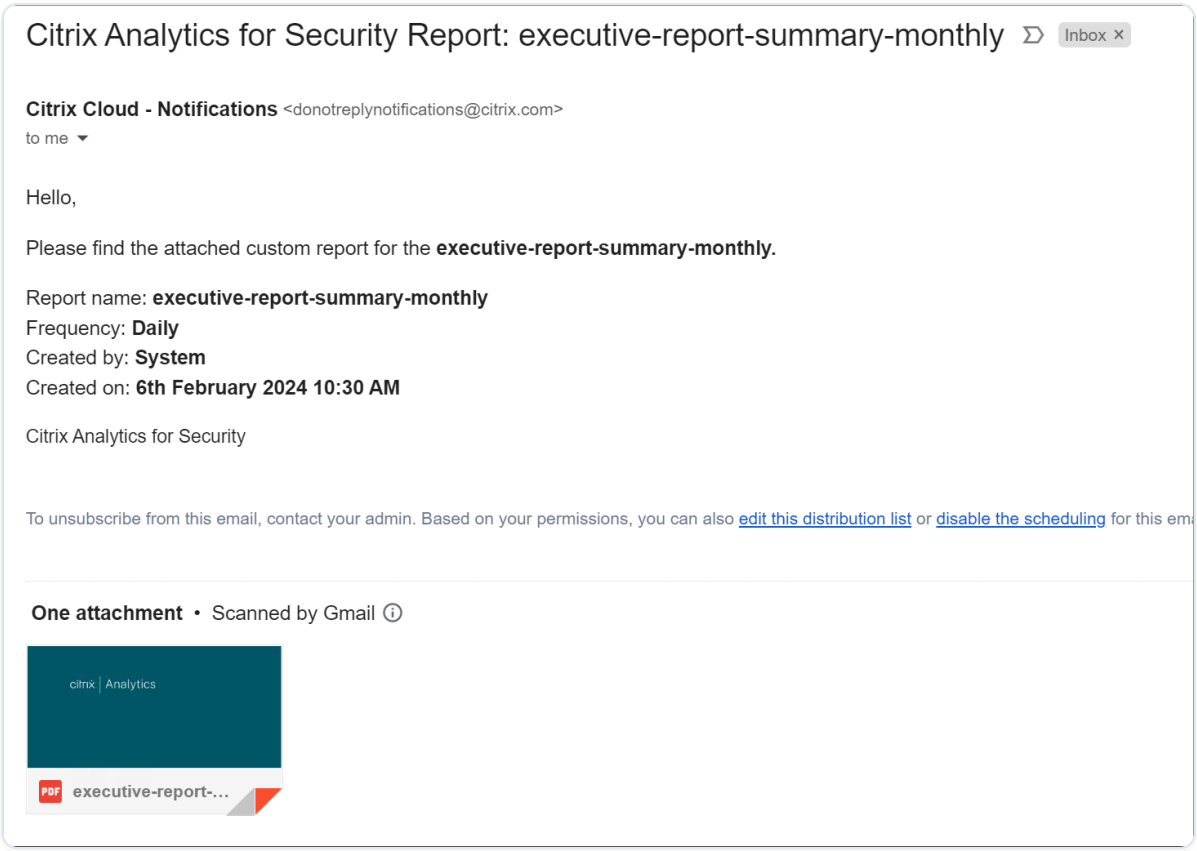
   c. **发送至**：从下拉列表中选择一个分发列表。您还可以添加分发列表和个人电子邮件地址的组合。要创建自定义分发列表，请参阅 管理员电子邮件设置。

   d. **设置日程**：选择报告首次发送给选定受众的所需时间以及重复发送的时间。

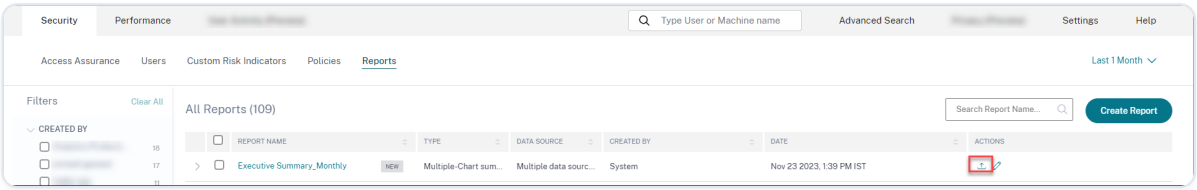


© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. 点击 **保存报告**。报告随后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** 符号将高管报告导出为 PDF。



以下屏幕截图显示了 PDF 输出示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

citrix | Analytics

Custom Report

executive-report-summary-monthly

From September 19, 2023 to October 19, 2023

Created by: **System**

Created on: **Oct 19, 2023 at 11:15 PM Asia/Singapore**

The custom report is generated for executive-report-summary-monthly for the period **19th Sep 2023 11:15 PM - 19th Oct 2023 11:15 PM**

User Risk Distribution

The distribution of users in high, medium, and low risky profiles based on their highest computed risk score in the selected time period.



自助搜索

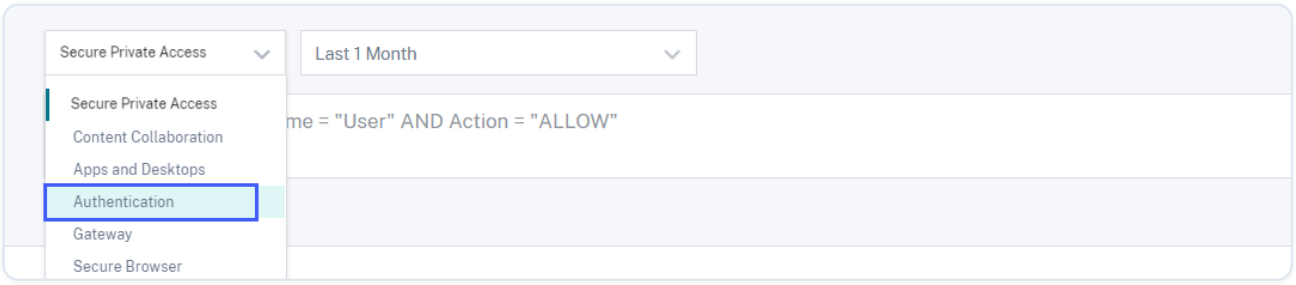
用于身份验证的自助搜索

使用自助搜索深入了解您企业中 Citrix Cloud 用户的身份验证详细信息。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。

有关搜索功能的更多信息，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 **Authentication**。默认情况下，自助服务页面显示过去一天的事件。您还可以选择要查看事件的时间段。

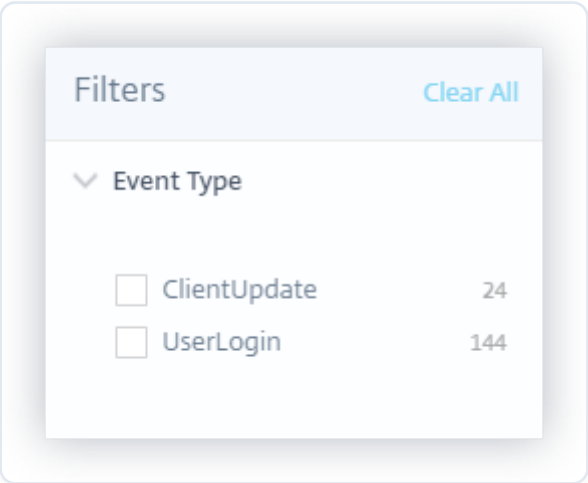


选择筛选条件以筛选事件

使用以下筛选器用于身份验证事件：

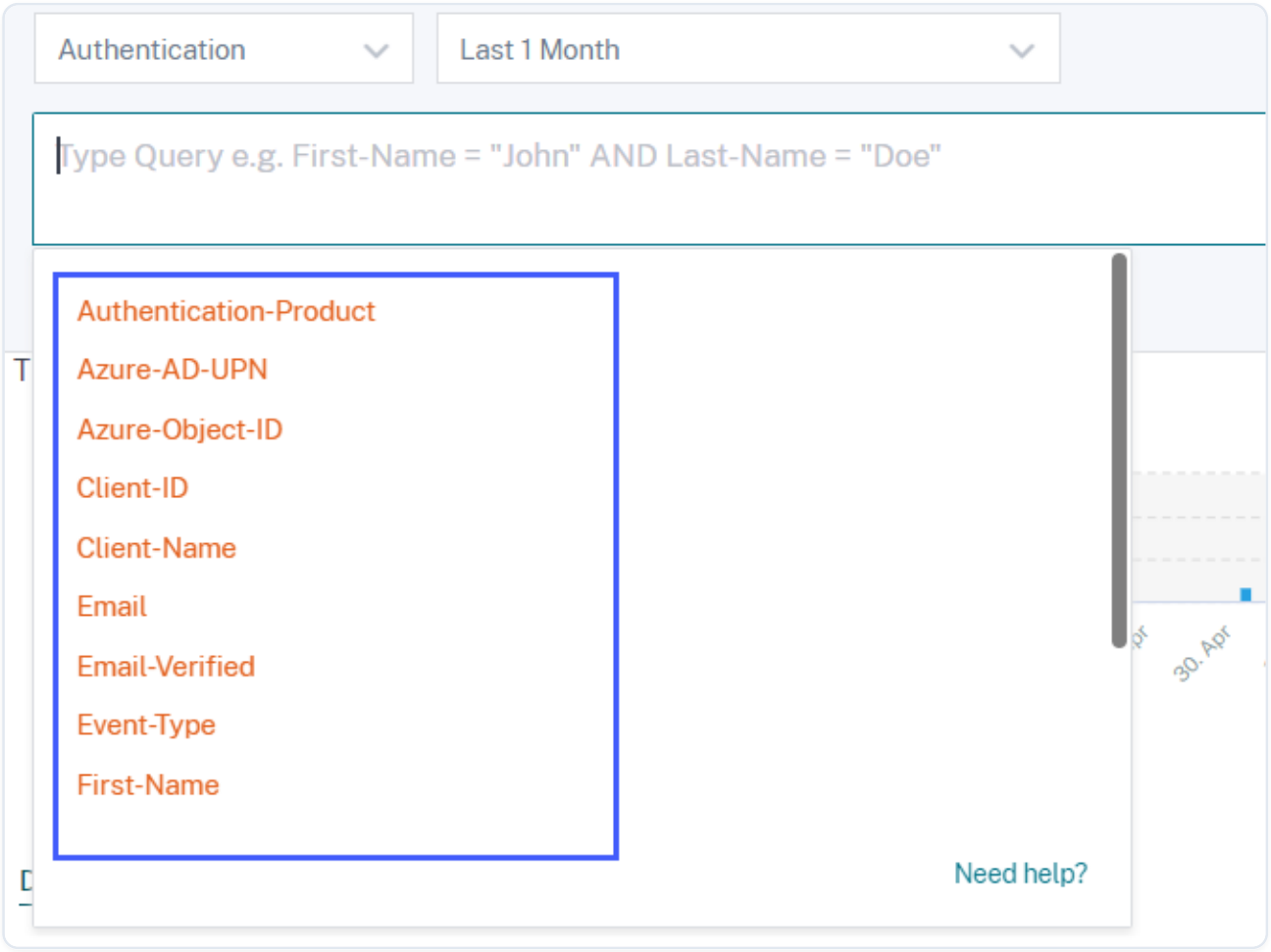
- **事件类型**- 根据用户事件类型（例如用户登录、用户注销和客户端更新）搜索事件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



指定搜索查询以筛选事件

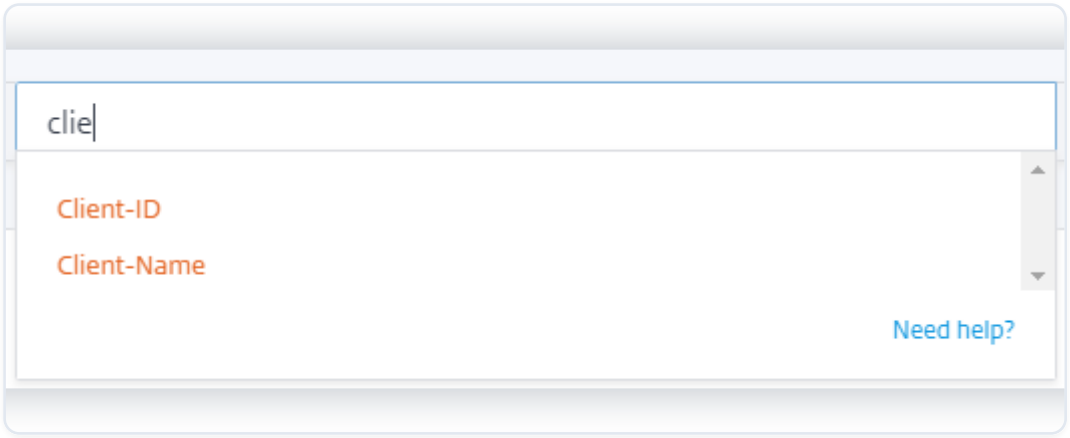
将光标置于搜索框中，以查看身份验证事件的维度列表。使用维度和 运算符 来指定查询并搜索所需事件。



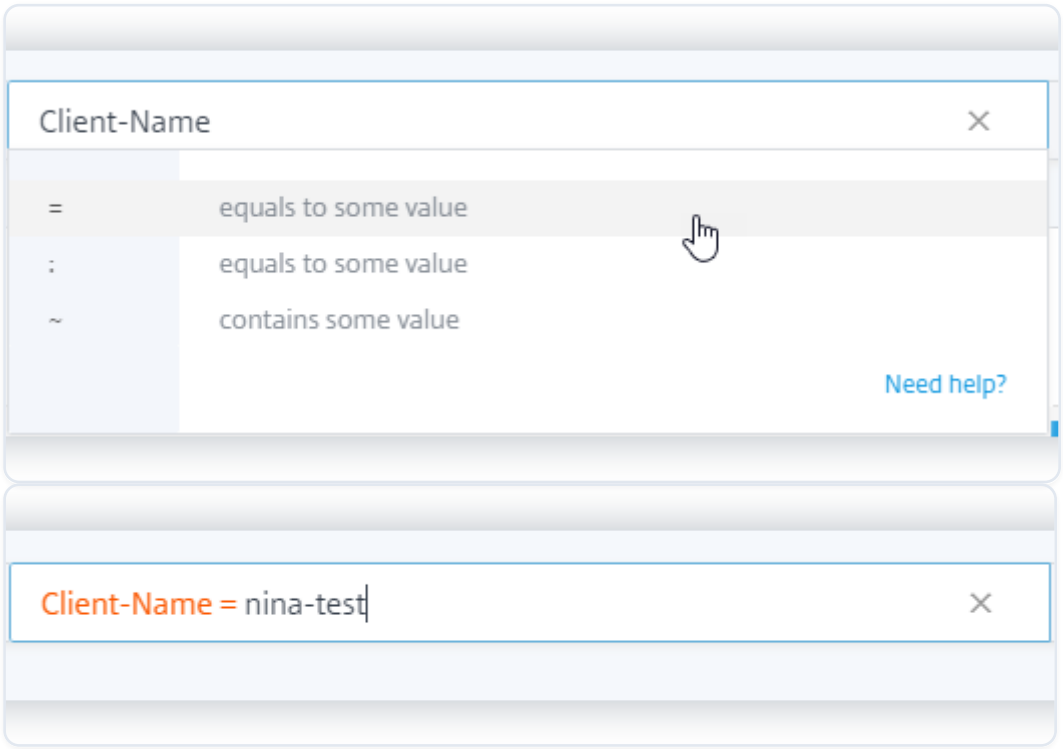
例如，您想要查看客户端“nina-test”的身份验证事件，其电子邮件状态已验证。

1. 在搜索框中输入“client”以获取相关维度。

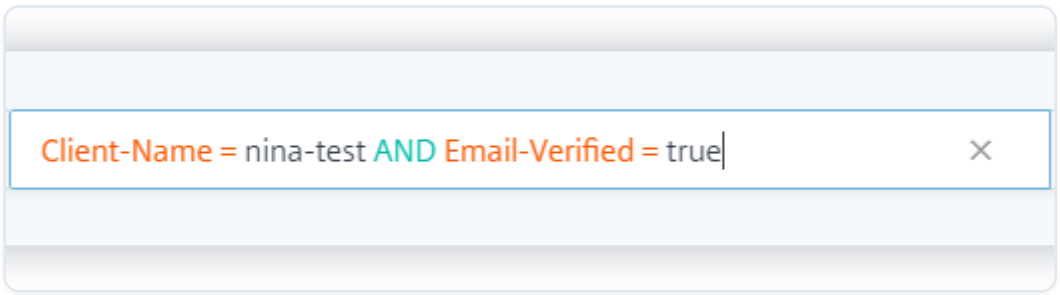
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 选择 **Client-Name**，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 **Email-Verified** 维度。使用等于运算符将值 "true" 分配给 **Email-Verified**。值 "true" 表示用户的电子邮件已验证。



4. 选择时间段，然后点击 **Search** 以在 **DATA** 表中查看事件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

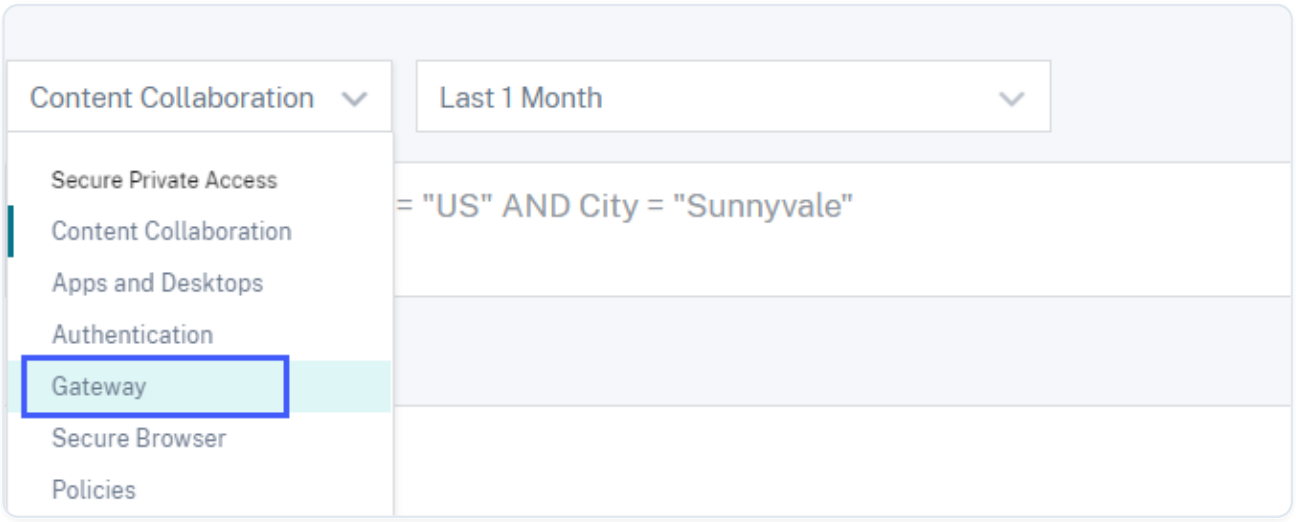
Gateway 的自助搜索

使用自助搜索功能深入了解从 Citrix Gateway 数据源接收到的用户事件。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，会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™ 接收这些事件并在自助搜索页面上显示它们。您可以查看用户及其访问详细信息。

有关搜索功能的更多信息，请参阅 **自助搜索**。

选择 Gateway 数据源

要查看 Gateway 事件，请从列表中选择 **Gateway**。默认情况下，自助服务页面显示过去一天的事件。您还可以选择要查看事件的时间段。



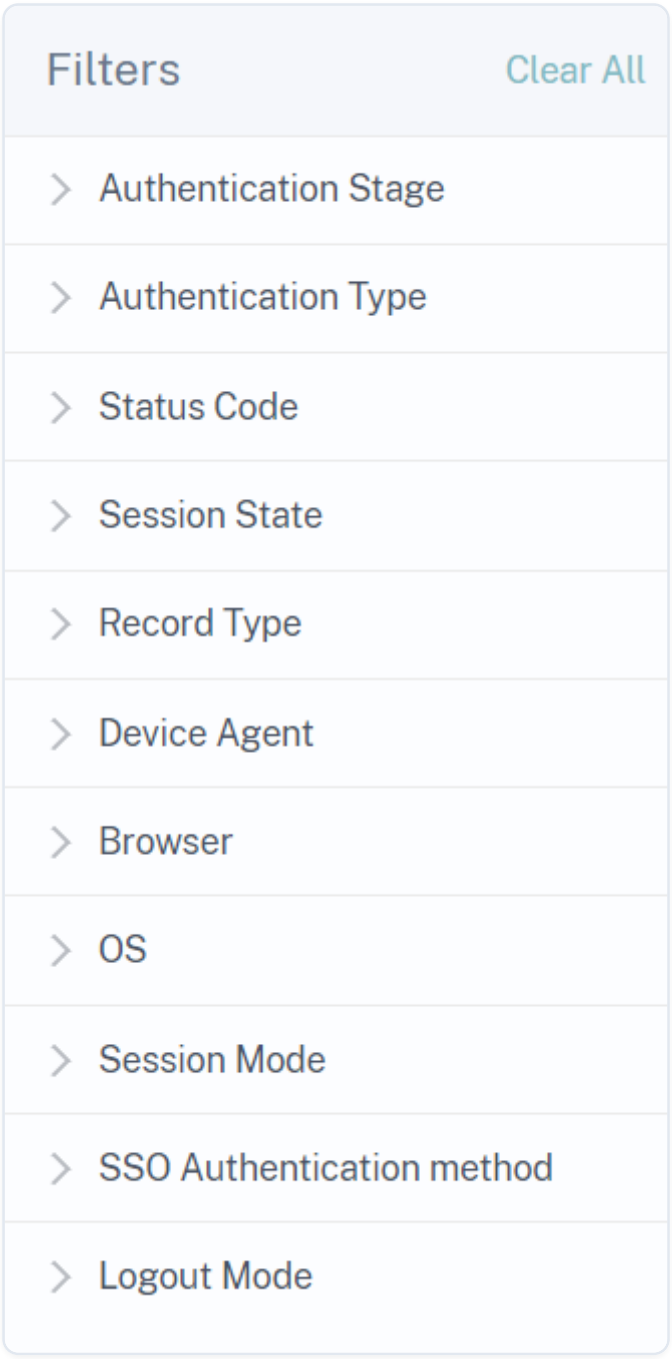
注意

此外，您可以从 **Security** > **Users** > **Access Summary** 仪表板访问 Gateway 的自助搜索页面。在成功登录场景中，您可以按状态代码访问数据。有关更多信息，请参阅 访问摘要 仪表板。

使用分面筛选事件

分面根据从数据源接收到的事件进行分类。使用以下分面筛选事件：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **身份验证阶段**- 根据客户端身份验证的不同阶段（例如主要、次要和三级）搜索事件。
- **身份验证类型**- 根据客户端身份验证类型（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）搜索事件。
- **设备代理**- 根据客户端设备（例如 iPhone、iPad、Windows Mobile）搜索事件。
- **记录类型**- 根据 VPN 记录类型搜索事件。提供以下 VPN 记录类型：

记录类型	描述
VPN_AI	筛选与身份验证相关的用户事件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

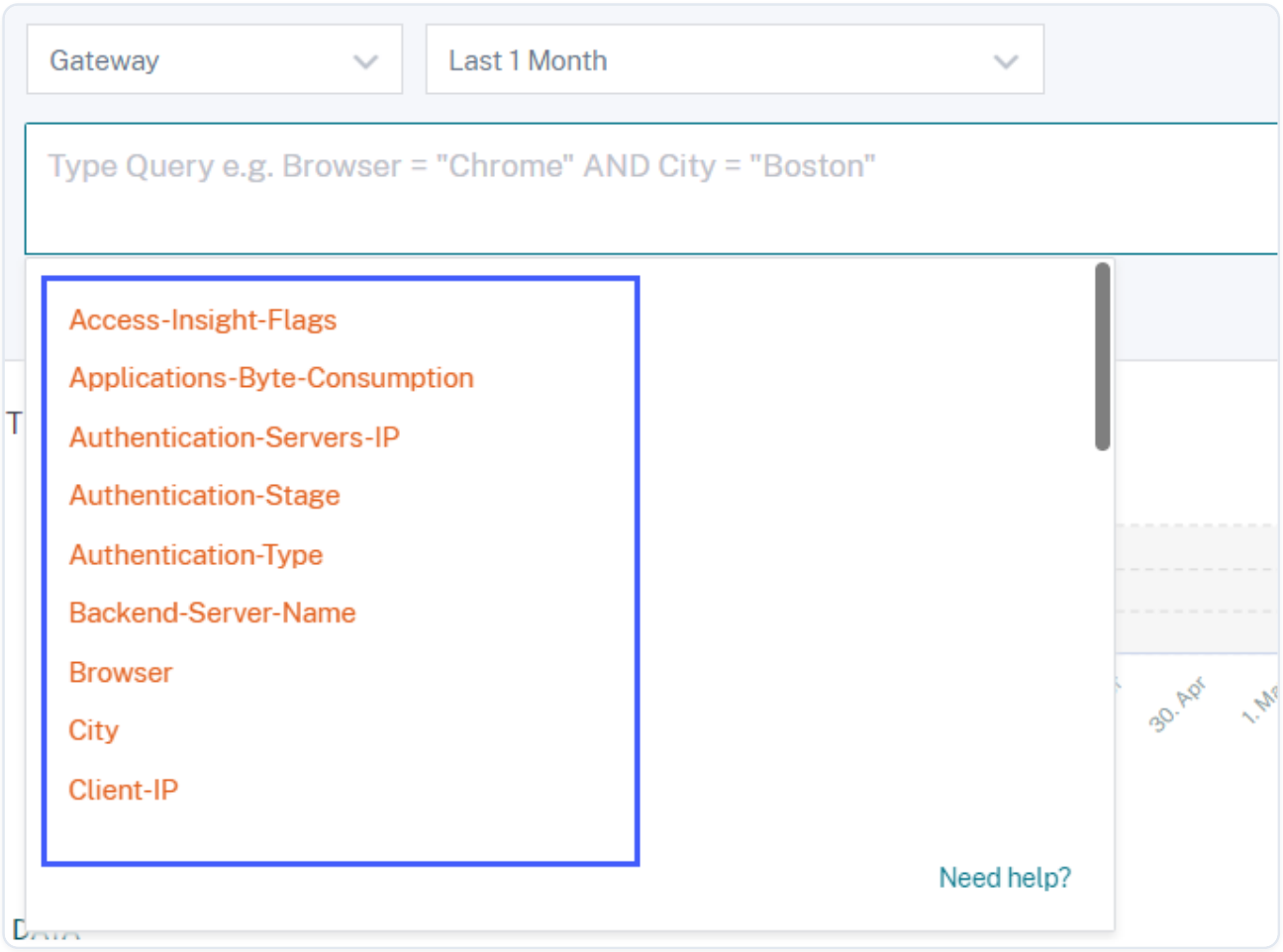
记录类型	描述
VPN_IF	筛选与 ICA® 文件相关的用户事件。
VPN_ST	筛选与会话注销相关的用户事件。

- **浏览器**- 根据浏览器（例如 Internet Explorer、Chrome、Firefox、Safari）搜索事件。
- **操作系统**- 根据客户端操作系统（例如 Windows、Mac、Linux、Android、iOS）搜索事件。
- **状态代码**- 根据 VPN 状态代码（例如 SSL 重定向响应失败、授权失败、单点登录失败）搜索事件。
- **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（例如全隧道、ICA 代理、无客户端）搜索事件。
- **SSO 身份验证方法**- 根据不同的单点登录身份验证方法（例如基本、摘要、NTLM、Kerberos、AG 基本、基于表单的 SSO）搜索事件。
- **注销模式**- 根据 VPN 注销模式（例如内部错误注销、会话超时注销、用户发起注销、管理员终止会话）搜索事件。

指定搜索查询以筛选事件

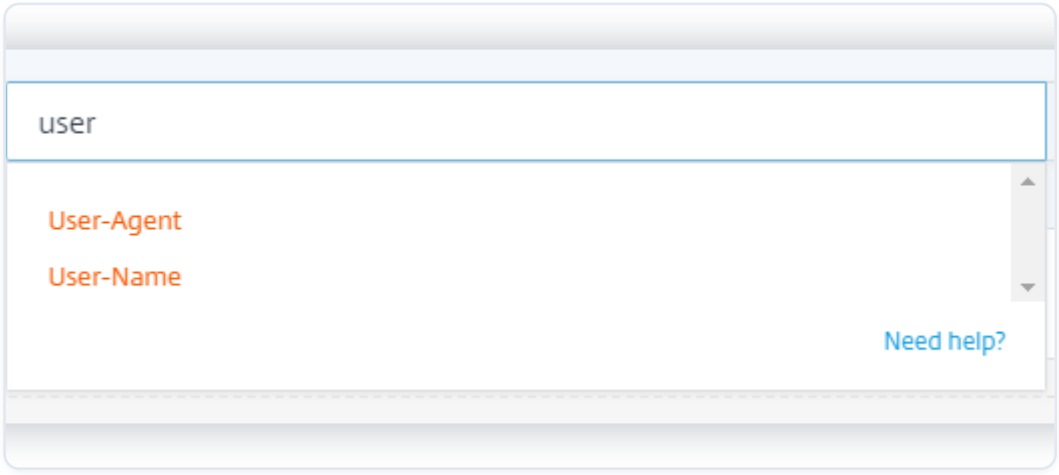
将光标置于搜索框中，以查看网关事件的维度列表。使用维度和运算符来指定查询并搜索所需的事件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

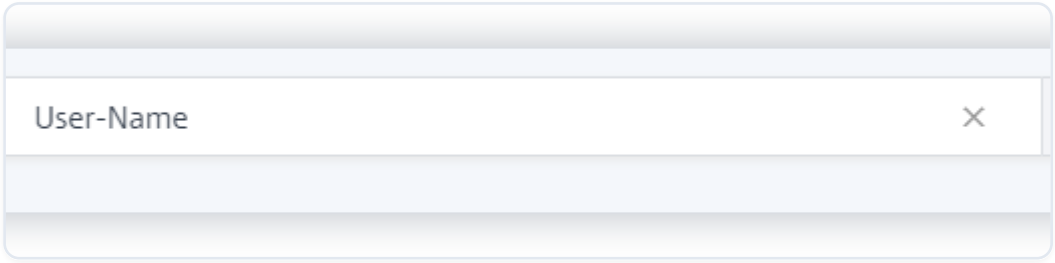


例如，您想查看用户“ns133”的事件，其中VPN状态码为“successful login”。

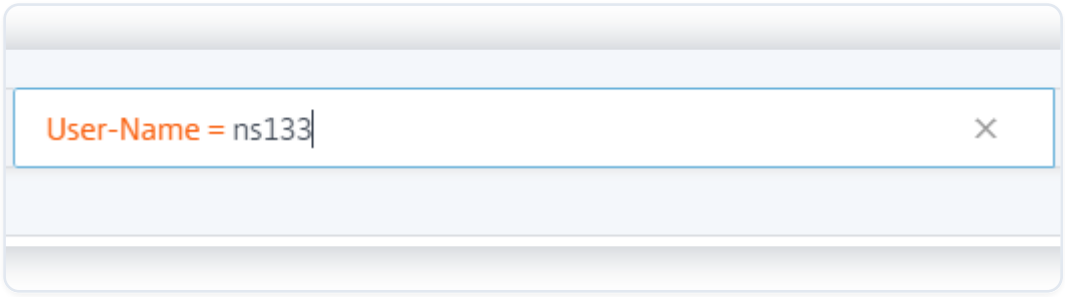
1. 在搜索框中输入“user”以选择相关维度。



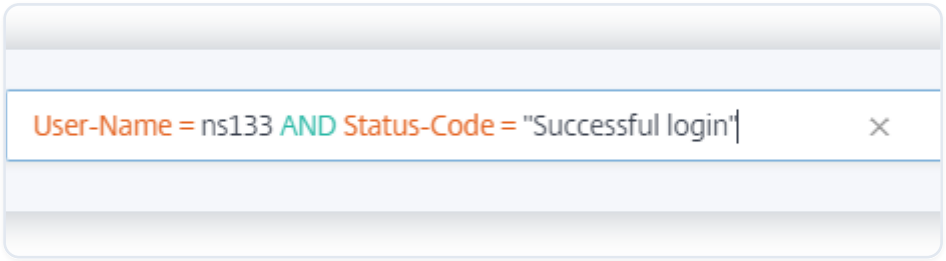
2. 选择 **User-Name** 并使用等号运算符输入值“ns133”。



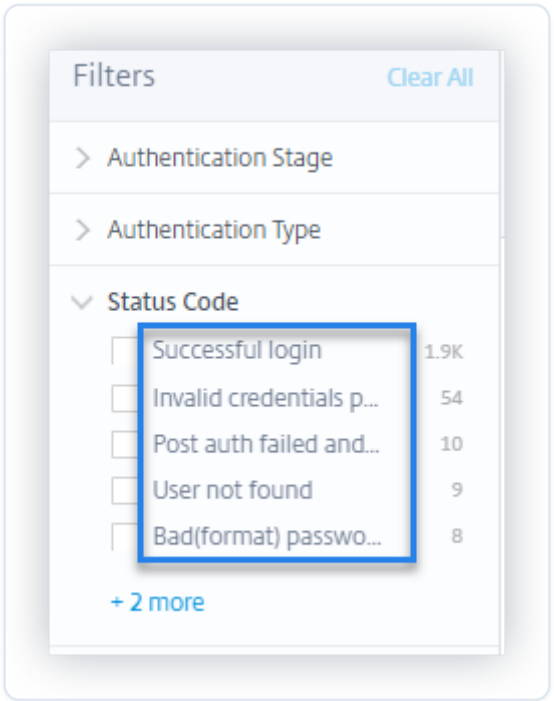
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 选择 **AND** 运算符，然后选择 **Status Code** 维度。使用等号运算符为 **Status Code** 输入字符串“Successful login”。



要识别 **Status Code** 的可能字符串值，请展开 **Status Code** 筛选列表，并将筛选器名称用作搜索查询中的字符串。



4. 选择时间段，然后点击 **Search** 以在 **DATA** 表中查看事件。

搜索查询支持的值

输入以下维度值以定义您的搜索查询。

访问洞察标志

指示 VPN 会话状态。输入以下标志值之一：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VPN 会话状态	标志值
预认证	2
nFactor（多因素）身份验证的最后或最终状态	1
后认证	4

注意

此标志仅适用于身份验证事件的上述 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，输入以下值：

值	类型	描述
示例：`40`、`100`	数字	您正在使用的应用程序消耗的数据（以字节为单位）。

认证服务器IP

对于 `Authentication-Servers-IP` 维度，请输入以下值：

值	类型	描述
示例：`10.xxx.xx.xx`	字符串	认证服务器的 IP 地址。

认证阶段

对于 `Authentication-Stage` 维度，输入以下值：

值	类型	描述
`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，输入以下值：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

值	类型	描述
`LDAP`、`SAML`、`Local`、`Radius`、`TACACS`、`SAMLIDP` 或 `OTP`。	字符串	通过其中一种可用方法验证您的用户。

后端服务器名称

对于 `Backend-Server-Name` 维度，输入以下值：

值	类型	描述
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，输入以下值：

值	类型	描述
`PN Agent`、`Edge`、`Firefox`、`Chrome` 或 `Safari`。	字符串	使用的浏览器。

城市

对于 `City` 维度，输入以下值：

值	类型	描述
示例：`Boston`、`Beijing`	字符串	用户登录的城市。

客户端 IP

对于 `Client-IP` 维度，输入以下值：

值	类型	描述
示例：`10.xxx.xxx.xx`	字符串	用户设备的 IP 地址。

客户端 IP 类型

对于 `Client-IP-Type` 维度，输入以下值:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

值	类型	描述
公共, 私有	字符串	指示用户 IP 地址是公共的还是私有的。

注意

这些值区分大小写。请输入小写值。

客户端端口

对于 `Client-Port` 维度，输入以下值:

值	类型	描述
示例：`45334`	数字	用户设备的端口号。

国家/地区

对于 `Country` 维度，输入以下值：

值	类型	描述
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，请将值用双引号引起来。**示例**：Country = "Unites States"。

事件类型

对于 `Event-Type` 维度，输入以下值：

值	类型	描述
身份验证、ICA 文件、会话注销	字符串	用户事件的类型。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

网关-FQDN

对于 `Gateway-FQDN` 维度，输入以下值：

值	类型	描述
示例：`Gateway-test`	字符串	您的 Citrix Gateway 的域名。

网关 IP

对于 `Gateway-IP` 维度，输入以下值：

值	类型	描述
示例：`10.xxx.xxx.xx`	字符串	您的 Citrix Gateway 的 IP 地址。

网关端口

对于 `Gateway-Port` 维度，输入以下值：

值	类型	描述
示例：`443`	字符串	您的 Citrix Gateway 的端口号。

注销模式

对于 `Logout-Mode` 维度，输入以下值：

值	类型	描述
`"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，请将值用双引号引起来。**示例**：Logout-Mode = `"Internal error"`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler-IP

对于 `NetScaler-IP` 维度，输入以下值：

值	类型	描述
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，输入以下值：

值	类型	描述
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，输入以下值：

值	类型	描述
`VPN_AI`	字符串	指示与身份验证相关的用户事件。
`VPN_IF`	字符串	指示与 ICA 文件相关的用户事件。
`VPN_ST`	字符串	指示与会话注销相关的用户事件。

SSO-认证方法

对于 `SSO-Authentication-Method` 维度，输入以下值：

值	类型	描述
`NSAUTH_BEARER`、`NSAUTH_FORM`、`NSAUTH_CITRIXAGBASIC`、`NSAUTH_NEGOTIATE`、`NSAUTH_NTLM` 或 `NSAUTH_BASIC`。	字符串	单点登录认证的不同方法。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

服务器 IP

对于 `Server-IP` 维度，输入以下值：

值	类型	描述
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，输入以下值：

值	类型	描述
示例：`47054`	数字	后端服务器的端口号。

会话状态

对于 `Session-State` 维度，输入以下值：

值	类型	描述
`"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，请将值用双引号引起来。**示例**：Session-State = `"Set Client State"`。

状态码

对于 `Status-Code` 维度，输入以下值：

值	类型	描述
`"Successful login"`、`"Invalid credentials passed"`、`"Post auth failed and connection`	字符串	VPN 状态码。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

值	类型	描述
`quarantined"`、`"Login not permitted"`、`"Maximum login failures reached"`		

注意

如果值包含空格，请将值用双引号引起来。**示例**：Session-Code = `"Successful login"`。

用户代理

对于 `User-Agent` 维度，输入以下值：

值	类型	描述
`IPHONE`、`IPAD` 或 `WINPHONE`	字符串	用于访问 VPN 的代理或设备。

VPN-会话-ID

对于 `VPN-Session-ID` 维度，输入以下值：

值	类型	描述
`c2c290c61dfe4e07247bde1e22142a12`	字符串	服务器为用户 VPN 会话分配的会话 ID。

VPN-会话-模式

对于 `VPN-Session-Mode` 维度，输入以下值：

值	类型	描述
`"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，请将该值用双引号引起来。**示例**：Session-Code = `"Full Tunnel"`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

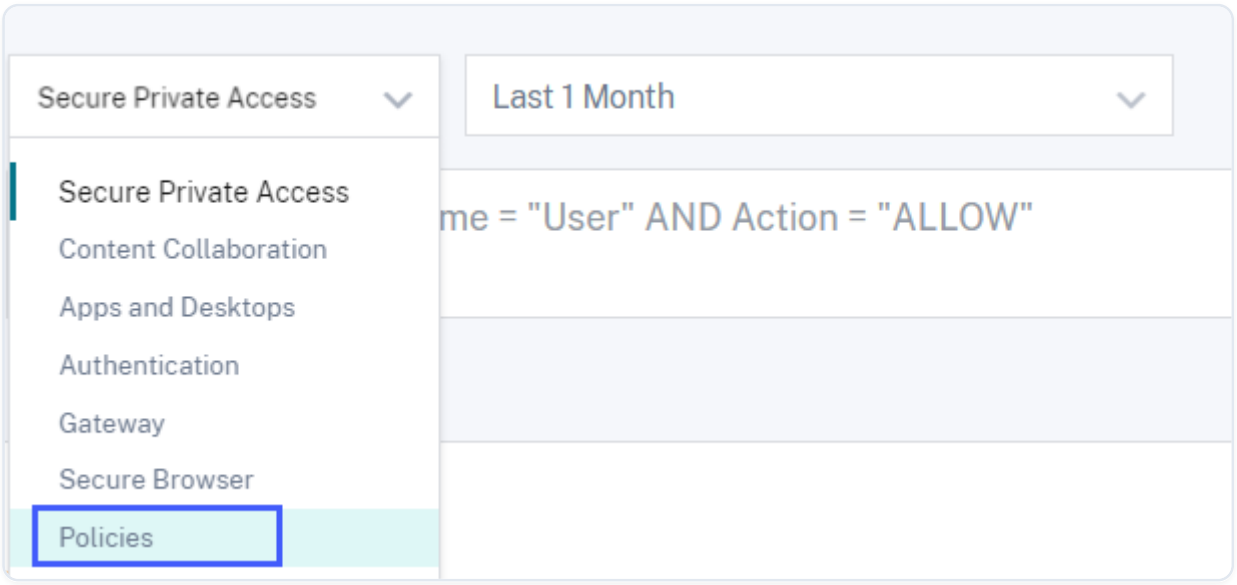
策略的自助搜索

Citrix Analytics for Security 允许您创建策略并在用户帐户上发生的异常或可疑事件上应用操作。当用户事件符合您定义的策略时，操作会自动应用于用户帐户，以隔离威胁并防止未来异常事件的发生。使用自助搜索，您可以查看符合您定义的策略的用户事件，并查看应用于这些异常事件的操作。

有关搜索功能的更多信息，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，自助服务页面显示过去一天的事件。您还可以选择要查看事件的时间段。



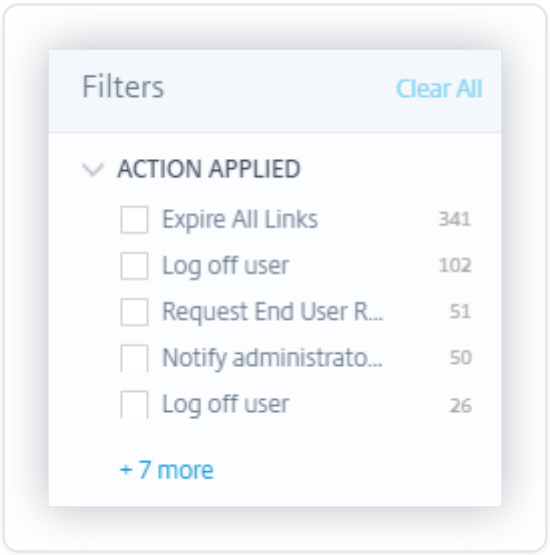
注意

您还可以从**安全** > **用户** > **策略和操作**控制板访问策略的自助搜索页面。在控制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。

选择方面以筛选事件

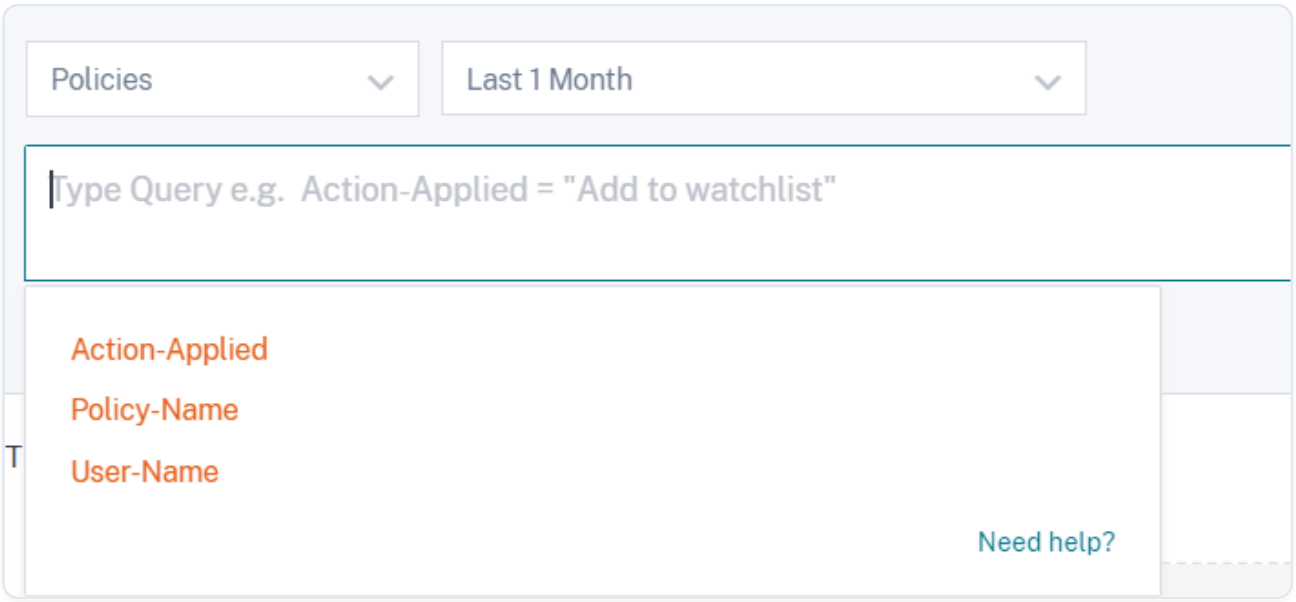
方面列表显示了应用于用户事件的操作。从方面列表中选择已应用的操作，并根据已应用的操作查看事件。有关配置策略时可以应用的操作的更多信息，请参阅什么是操作？。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



指定搜索查询以筛选事件

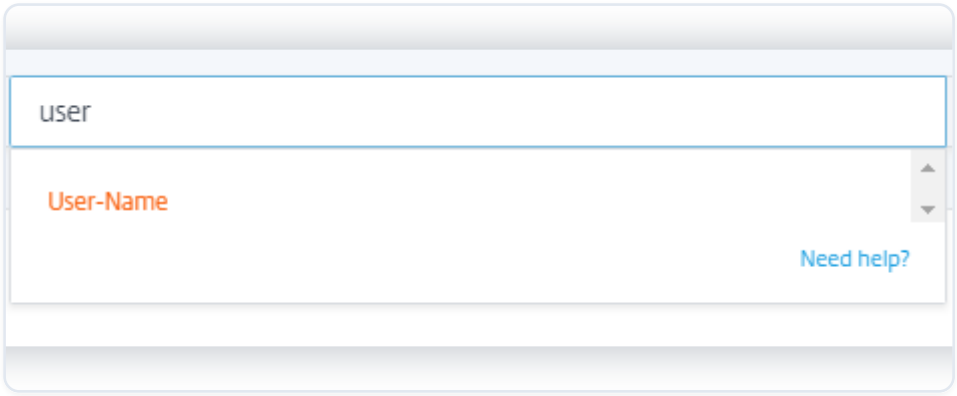
将光标置于搜索框中，以查看与策略相关的事件的维度列表。使用维度和运算符来指定您的查询并搜索所需事件。



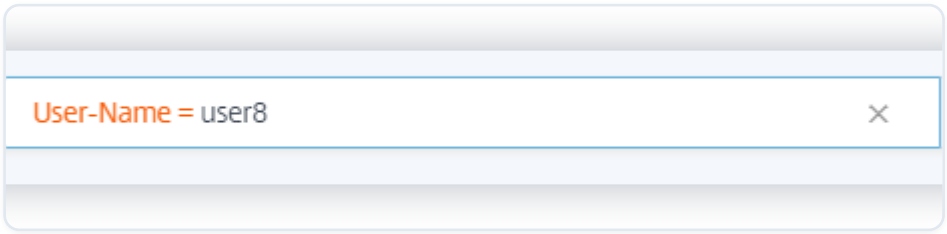
例如，您想要查看用户“user8”的异常事件，其中对这些事件应用的操作是“禁用用户”。

1. 在搜索框中输入“user”以获取相关维度。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

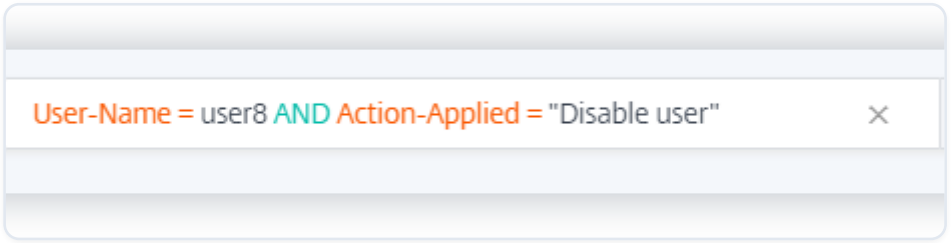


2. 选择 **User-Name** 并使用等号运算符输入值“user8”。



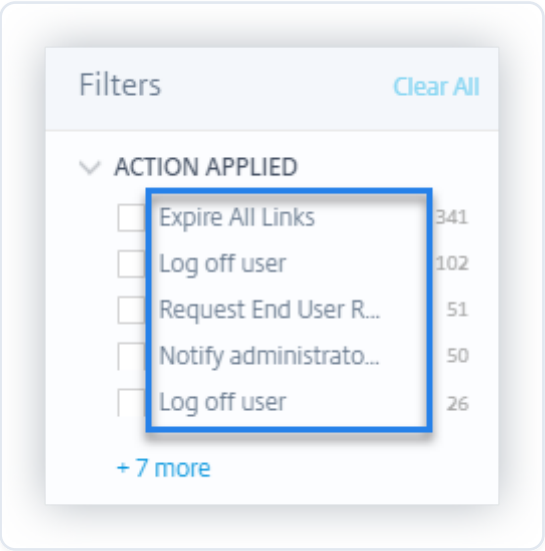
3. 选择 **AND** 运算符，然后选择 **Action-Applied** 维度。使用等号运算符为 **Action-Applied** 输入字符串“Disable user”。

> **注意**
>
> 如果字符串值包含两个或更多单词，则必须使用运算符 `“”` 将其括起来。例如，`“Disable user”`，“Stop Session Recording”。



要识别 **Action-Applied** 可能的字符串值，请展开分面列表并将筛选器名称用作搜索查询中的字符串。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 选择时间段，然后单击 **Search** 以在 **DATA** 表中查看事件。

远程浏览器隔离（安全浏览器）的自助搜索

使用自助搜索可深入了解正在使用 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，可在不损害企业网络安全的情况下提供安全的互联网浏览体验。当用户使用远程浏览器隔离访问 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。

有关搜索功能的更多信息，请参阅 **自助搜索**。

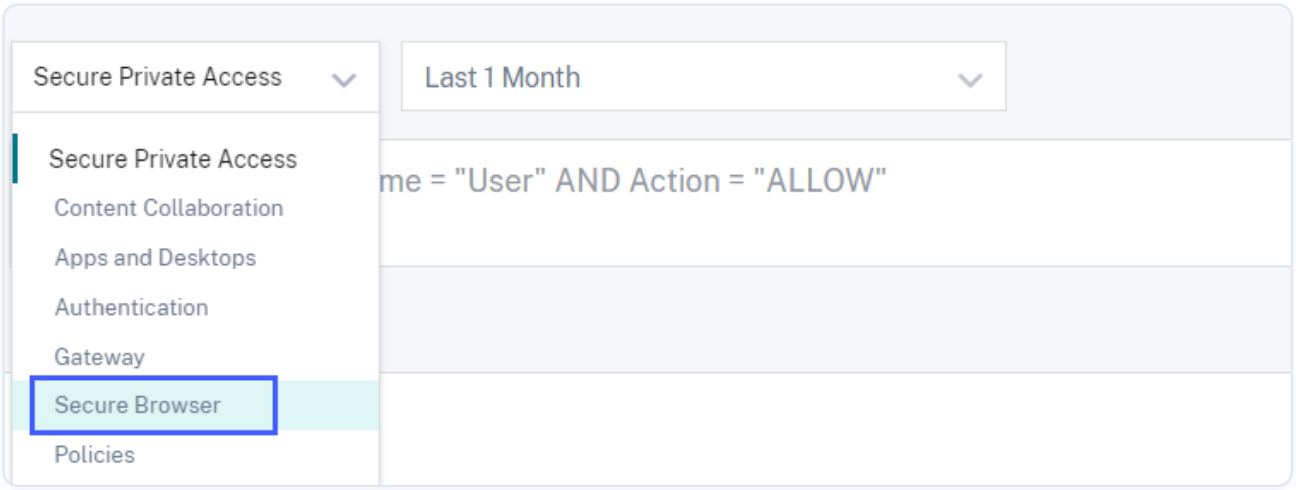
先决条件

要从远程浏览器隔离接收事件，请在远程浏览器隔离中启用 **主机名跟踪** 以记录用户会话的主机名。此信息将发送到 Citrix Analytics for Security。有关更多信息，请参阅 管理已发布的远程浏览器隔离。

选择远程浏览器隔离数据源

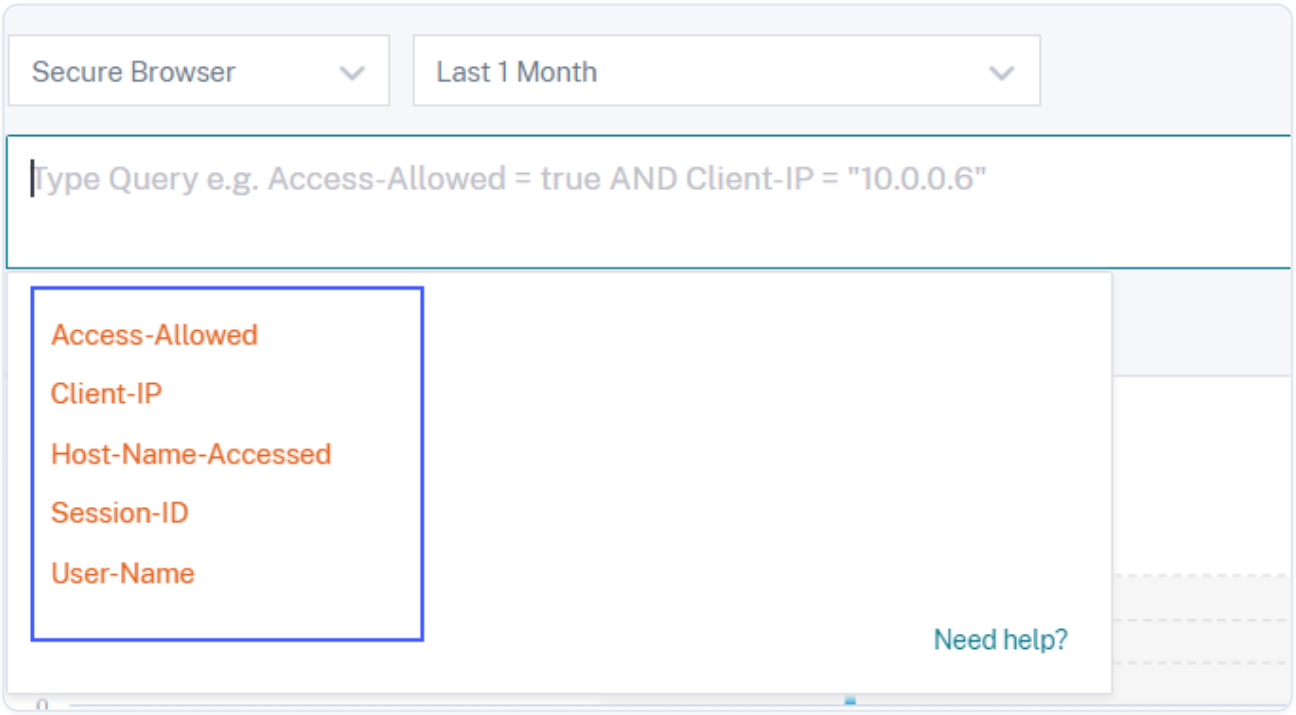
要查看远程浏览器隔离事件，请从列表中选择 **远程浏览器隔离**。默认情况下，自助服务页面显示过去一天的事件。您还可以选择要查看事件的时间段。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



指定搜索查询以筛选事件

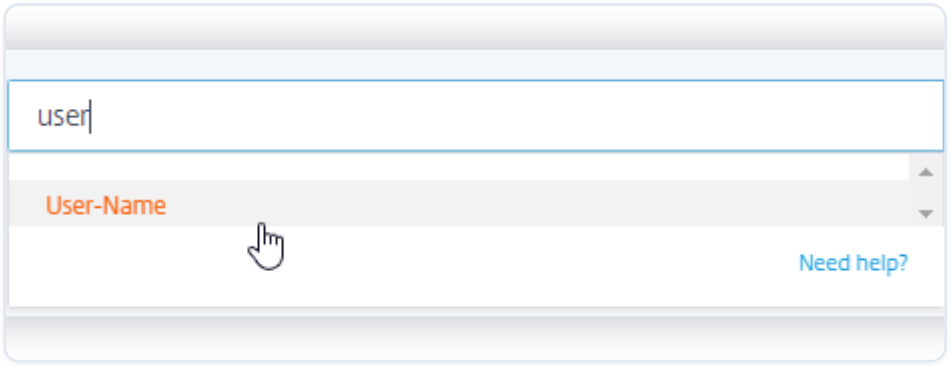
将光标置于搜索框中，以查看远程浏览器隔离事件的维度列表。使用维度和 运算符 来指定查询并搜索所需的事件。



例如，您想查看用户“aa”的浏览事件详细信息，该用户有权访问各种主机服务，例如 google.com、amazon.com。

1. 在搜索框中输入“user”以查看相关维度。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 单击 **User-Name** 并使用等号运算符输入值“aa”。

   远程浏览器隔离查询 2(/en-us/citrix-analytics/media/self-search-secure-browser-query-2.png)

3. 选择 **AND** 运算符和 **Allow-Access** 维度。使用等号运算符将值“true”分配给 **Allow-Access**。“true”值表示用户可以访问主机服务。

   远程浏览器隔离查询 4(/en-us/citrix-analytics/media/self-search-secure-browser-query-3.png)

4. 选择时间段并点击 **搜索** 以查看 **DATA** 表中的事件。

查看用户事件详情

您可以查看从远程浏览器隔离服务接收到的以下数据：

- **时间**- 用户事件发生时的日期和时间。
- **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**- 用户被允许或拒绝访问主机服务。

Secure Private Access 的自助搜索

使用自助搜索深入了解您组织中 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在自助搜索中显示它们。您可以跟踪用户及其访问详细信息。

有关搜索功能的更多信息，请参阅 **自助搜索**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

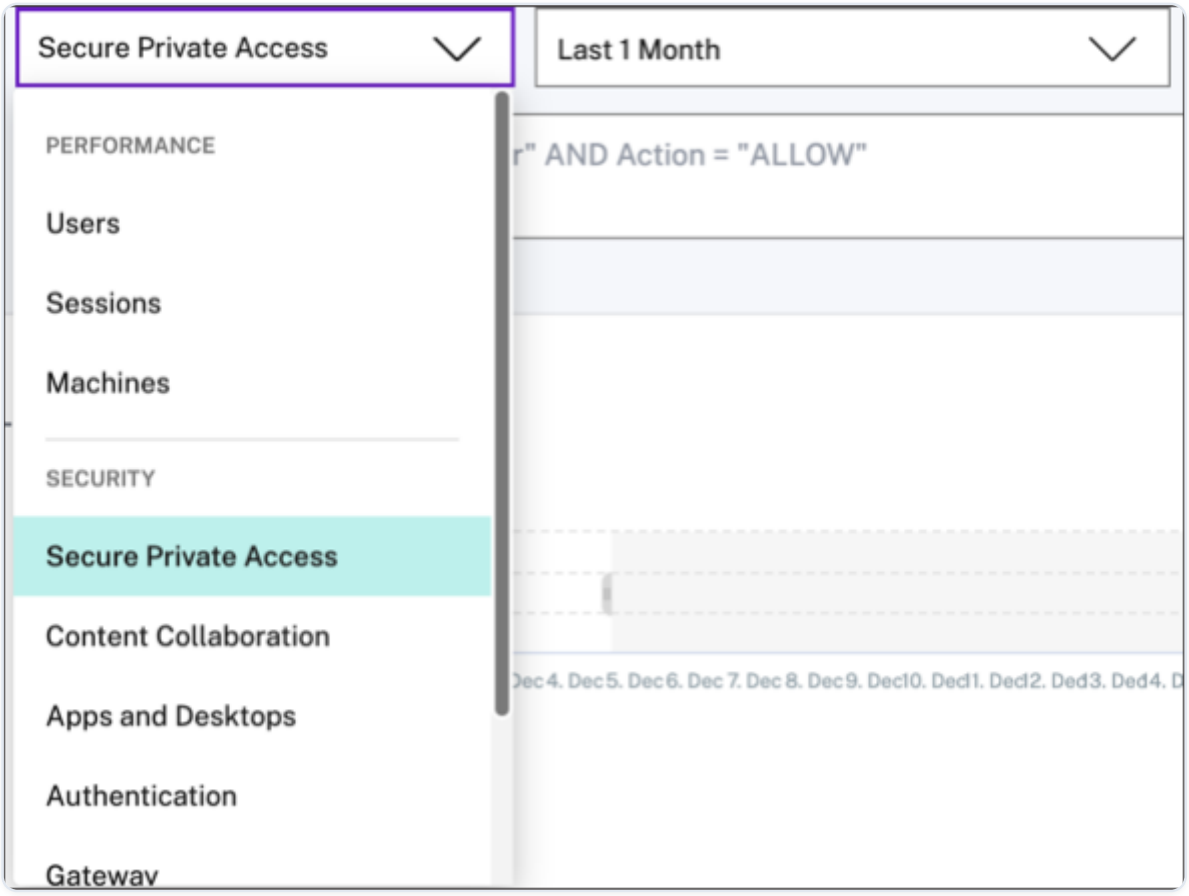
由于 Secure Private Access 弃用了基于类别的 Web 过滤，Citrix Analytics for Security 上的以下功能受到影响：

1. URL 的类别组、类别和信誉等数据字段在 Citrix Analytics for Security 控制板上不再可用。
2. 依赖相同数据的风险网站访问指示器也已弃用，并且不会为客户触发。
3. 任何使用数据字段（URL 的类别组、类别和信誉）的现有自定义风险指示器及其关联策略不再触发。

有关 Secure Private Access 弃用功能的详细信息，请参阅 功能弃用。

选择 Secure Private Access 数据源

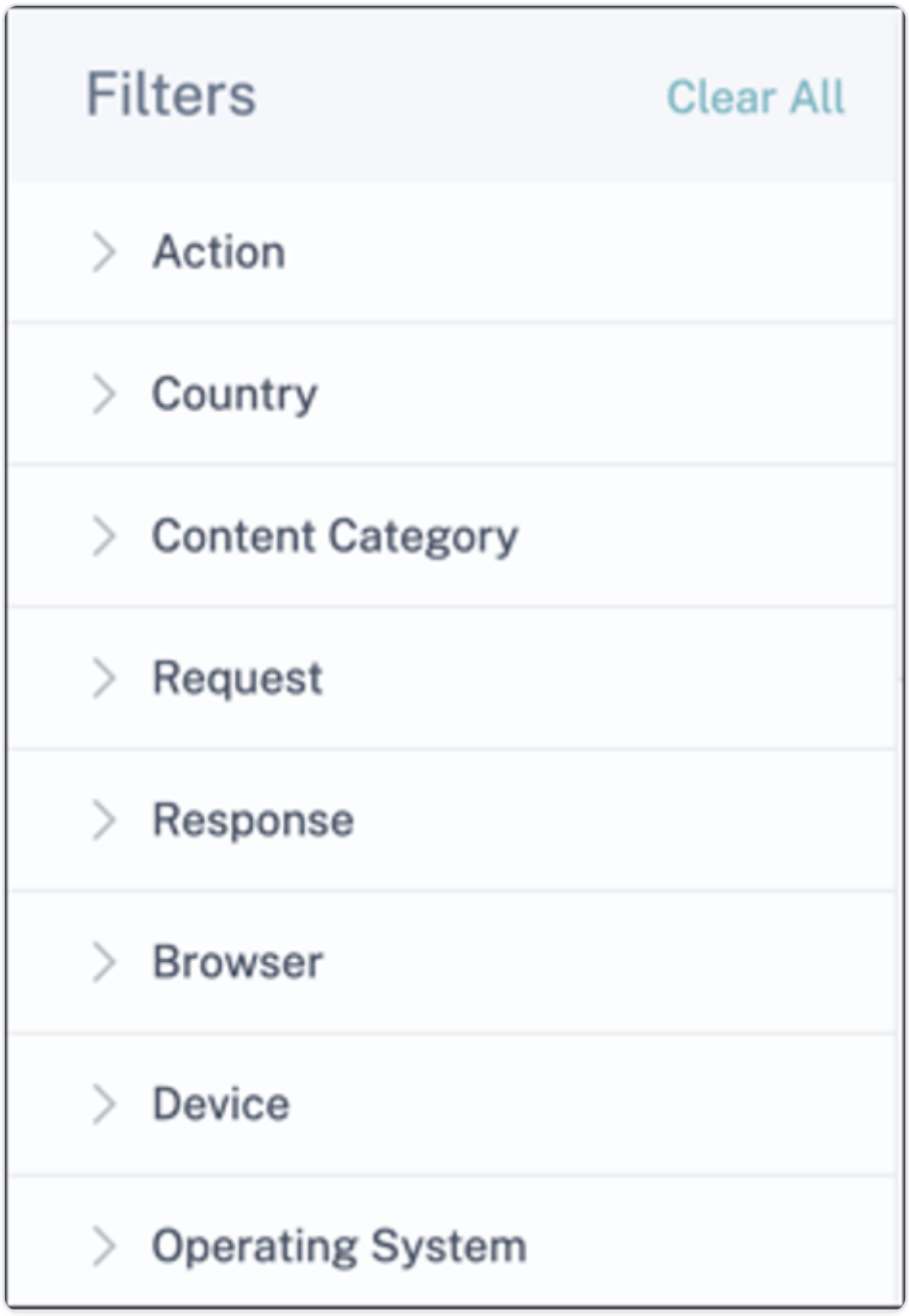
要查看 Secure Private Access 事件，请从列表中选择 **Secure Private Access**。默认情况下，自助服务页面显示过去一天的事件。您还可以选择要查看事件的时间段。



选择方面以筛选事件

使用以下与 Secure Private Access 事件相关联的方面。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

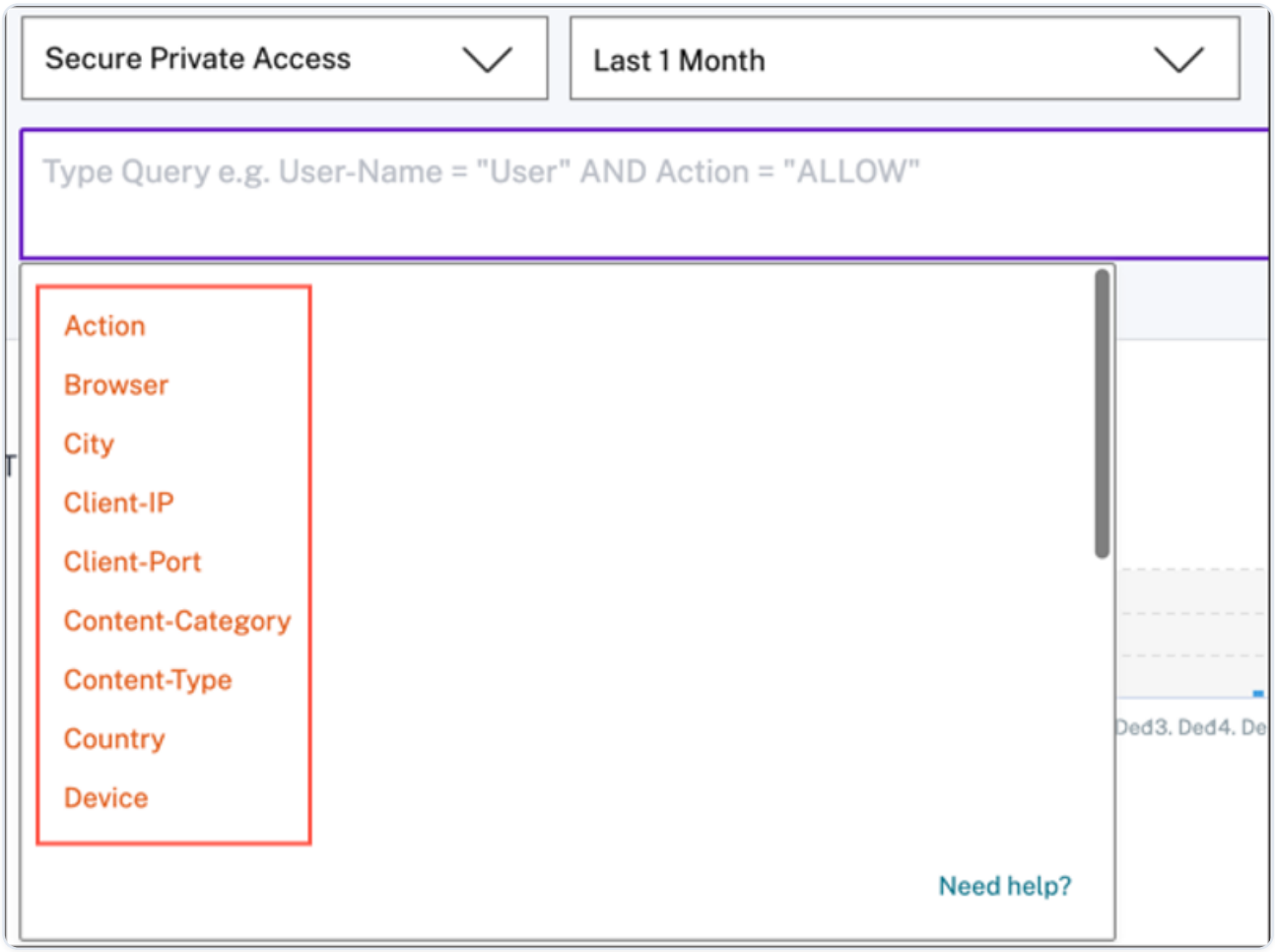


- **操作**- 根据用户应用程序上执行的操作（例如允许、阻止和重定向）搜索事件。
- **国家/地区**- 根据用户的访问位置搜索事件。
- **内容类别**- 根据访问内容的类别（例如应用程序、图像和文本）搜索事件。
- **请求**- 根据 HTTP 方法（例如 GET、POST、PUT、DELETE）搜索事件。
- **响应**- 根据 HTTP 响应搜索事件。
- **浏览器**- 根据用户使用的浏览器搜索事件。
- **设备**- 根据使用的设备（例如 Android 手机、iPhone、MacBook）搜索事件。
- **操作系统**- 根据设备上安装的操作系统搜索事件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

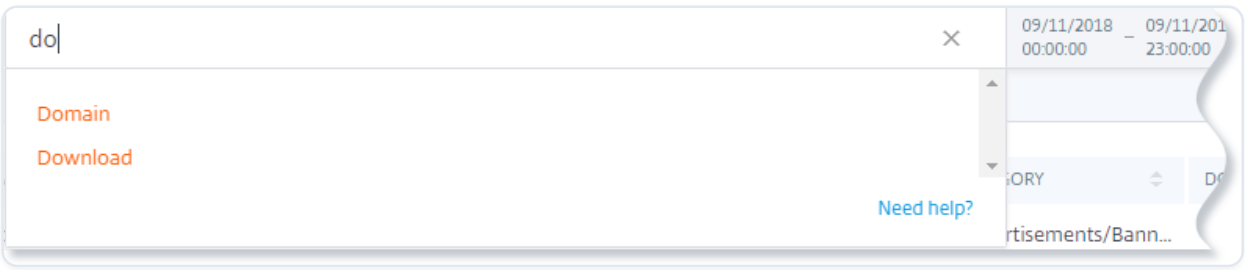
指定搜索查询以筛选事件

将光标置于搜索框中，以查看 Secure Private Access 事件的维度列表。使用维度和运算符来指定查询并搜索所需的事件。



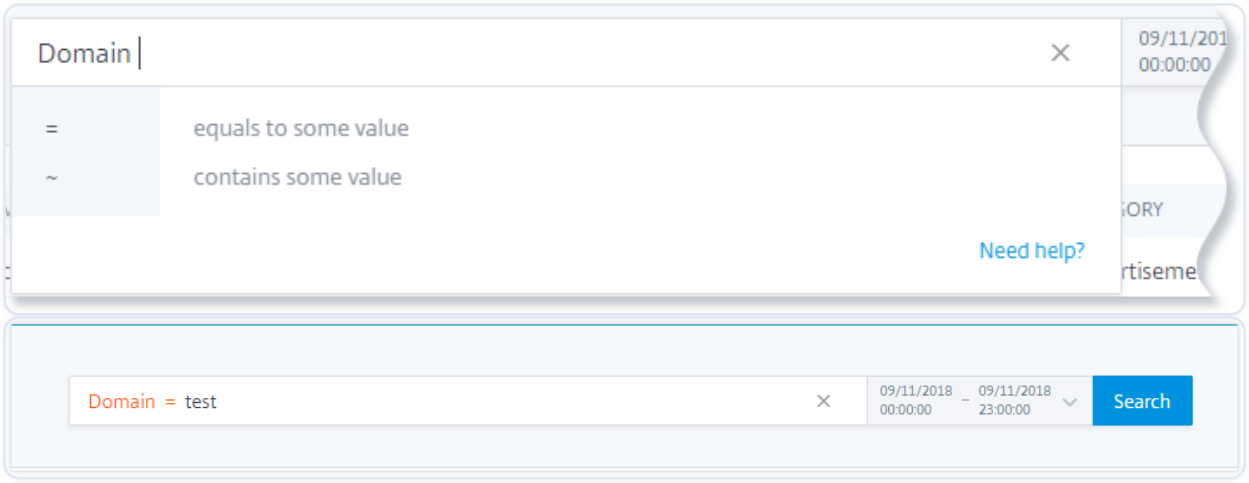
例如，您想要查看数据下载量超过 2,000 字节的测试域。请按如下方式指定搜索查询：

1. 在搜索框中输入“do”以获取相关建议。

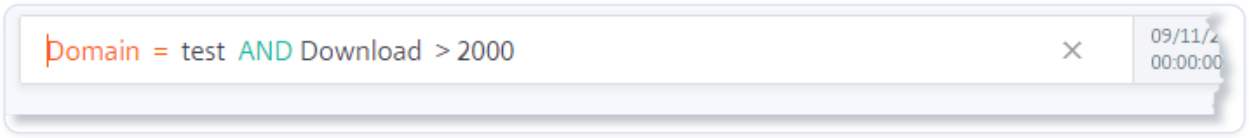


2. 单击**域**，然后使用等于运算符指定值“test”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 使用 **AND** 运算符，然后选择 **下载** 维度。选择 **>** 运算符，并输入以字节为单位的下载量。



4. 选择时间段，然后点击 **搜索** 以在 **数据** 表中查看事件。

应用程序和桌面的自助搜索

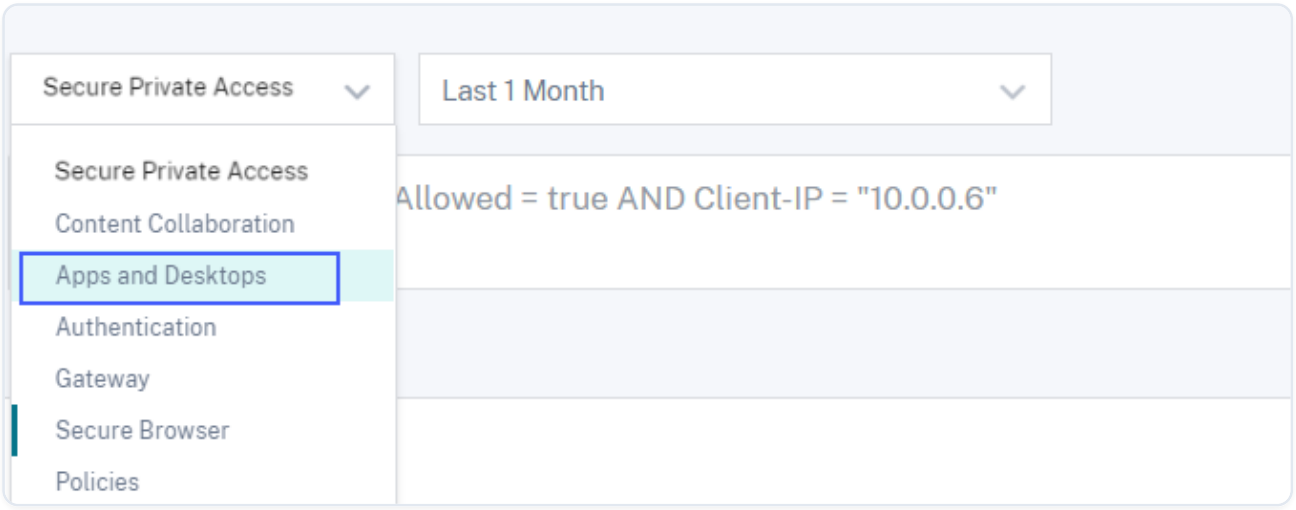
使用自助搜索功能，深入了解从 Citrix Virtual Apps and Desktops 数据源和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）数据源接收到的用户事件。当用户使用虚拟应用程序或虚拟桌面时，会生成与其活动和操作相对应的事件。用户事件的示例包括文件下载、帐户登录和应用程序启动。Citrix Analytics for Security 接收这些用户事件并将其显示在自助服务页面上。您可以跟踪用户及其活动。

有关搜索功能的更多信息，请参阅 **自助搜索**。

选择应用程序和桌面数据源

要查看 Citrix Virtual Apps and Desktops 或 Citrix DaaS 中的事件，请从列表中选择 **应用程序和桌面**。默认情况下，自助服务页面显示过去一天的事件。您还可以选择要查看事件的时间段。

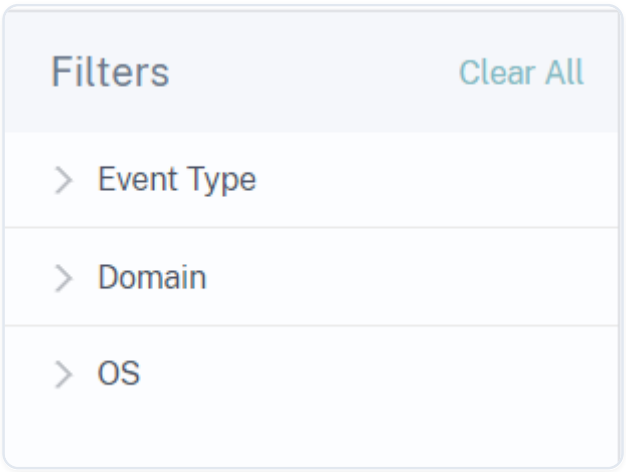
© 1997–2026 Citrix Systems, Inc. All rights reserved.



默认情况下，自助服务页面显示过去一个月的事件。该页面还提供了多个方面和一个搜索框，用于筛选和关注所需的事件。

选择方面以筛选事件

使用与应用程序和桌面事件关联的以下方面。

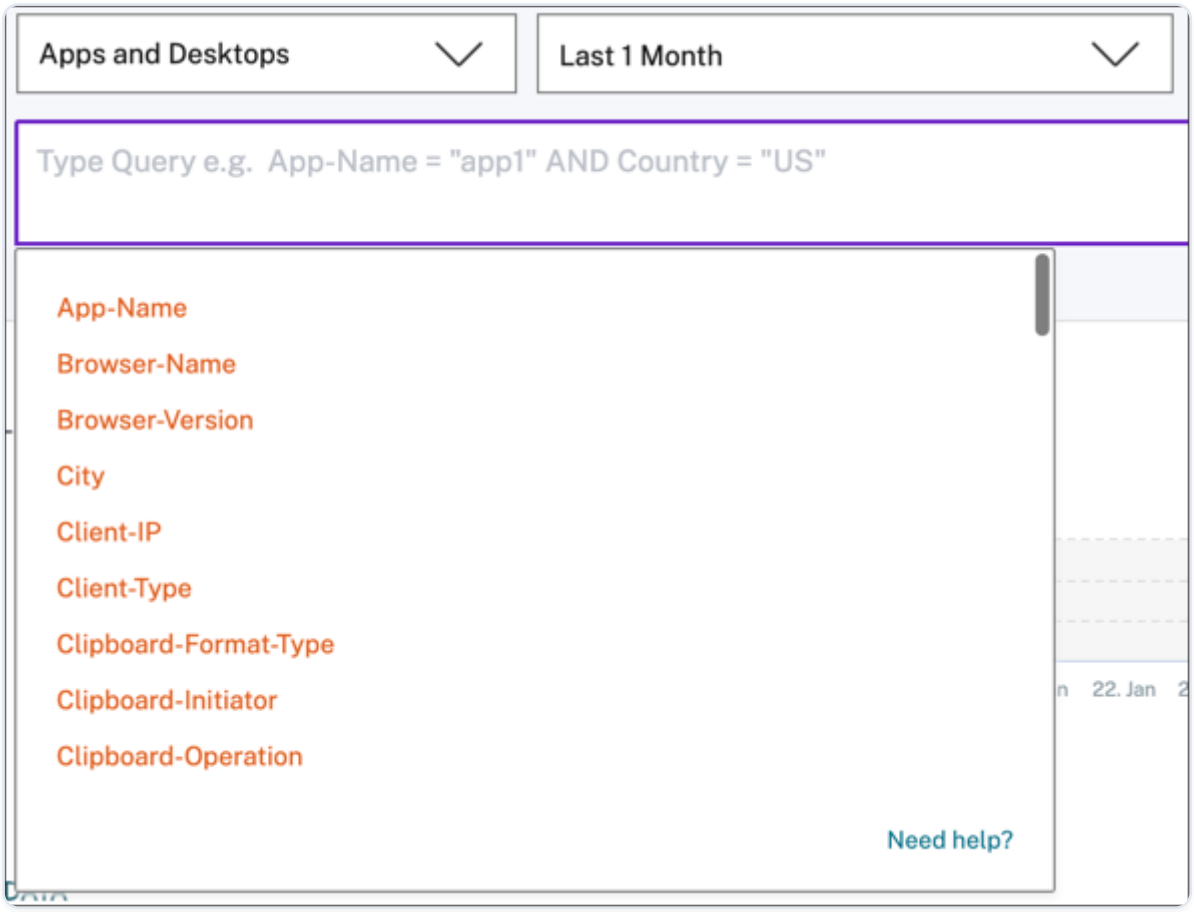


- **事件类型**- 根据事件类型（例如帐户登录、应用程序结束和会话结束）搜索事件。
- **域**- 根据域（例如 citrate.net）搜索事件。
- **操作系统**- 根据用户设备中使用的操作系统（例如 Chrome、iOS 和 Windows）搜索事件。选择操作系统名称和版本以筛选事件。有关操作系统版本的更多信息，请参阅 搜索查询支持的值。

指定搜索查询以筛选事件

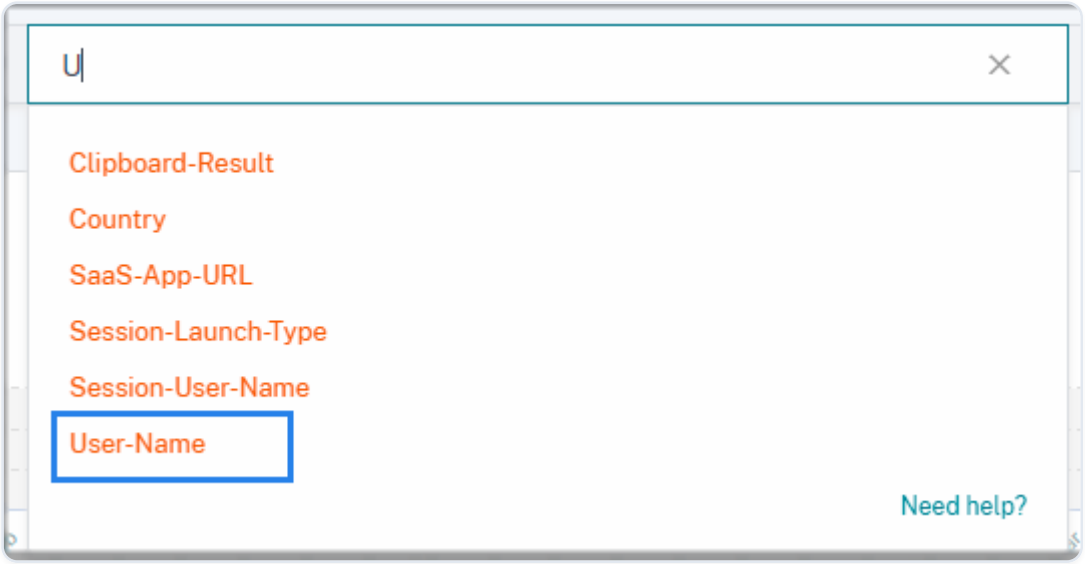
将光标置于搜索框中，以查看应用程序和桌面事件的维度列表。使用维度和 运算符 来指定查询并搜索所需的事件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



例如，您想搜索用户“John Doe”的事件，他正在使用 Windows 操作系统。

1. 在搜索框中输入“U”以获取相关建议。



2. 单击 **User-Name** 并使用等于运算符输入值“John”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 选择 **AND** 运算符和 **OS-Name** 维度。使用等于运算符分配值“Windows 7”。

```
User-Name = "John" AND OS-Name = "Windows 7"
```

4. 选择时间段并单击 **Search** 以查看基于 **DATA** 表的事件。

事件类型和支持的字段

以下字段适用于所有事件类型，VDA.Print 除外：

- 城市
- 客户端 IP
- 国家/地区
- 设备 ID
- 操作系统名称
- 操作系统版本
- 操作系统额外信息
- 时间
- 用户名
- Workspace 应用版本
- Workspace 应用状态

下表描述了适用于应用程序和桌面数据源的事件类型以及每个事件类型特有的字段。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

值	描述	字段
`Account.Logon`	当您通过 Citrix Workspace 应用程序登录到 Store 时触发。**注意**：HTML5 客户端不支持 Account.Logon。	检查如上所述的通用字段。
`Session.Logon`	当您登录到虚拟会话时触发。	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`	当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`	当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。对于在虚拟会话中发生的文件传输，它不会触发。**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
`Printing`	当您通过客户端打印机使用 Citrix Workspace 应用程序启动的会话打印文件时触发。**注意**：Citrix Workspace 应用程序存在两个影响打印事件的技术限制。首先，由于所有平台变体中都存在已知问题，打印文档名称遥测数据未包含在打	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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

值	描述	字段
	印事件中。其次，由于另一个已知技术限制，Windows 的打印文件大小遥测数据未包含在打印事件中。要收集这些数据集（文件名/文件大小），请使用 VDA.Print 事件。有关更多信息，请参阅 为 Citrix DaaS 启用打印遥测。	
`AppProtection.ScreenCapture`	当用户尝试在受保护的会话中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`	当在 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、剪贴板详细信息发起者、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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

值	描述	字段
`App.SaaS.Url.Navigate`	Citrix Enterprise Browser 导航到 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
`Citrix.EventMonitor.AppEnd`	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停止时触发。	应用程序名称
`Citrix.EventMonitor.Clipboard`	当会话录制中执行了剪贴板操作时触发。	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，客户端到主机）、源路径、目标路径
`Citrix.EventMonitor.RegistryChange`	当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`	当会话录制结束时触发。	描述
`Citrix.EventMonitor.SessionLaunch`	当会话录制开始时触发。	会话录制类型
`Citrix.EventMonitor.TopMost`	当最顶层窗口更改时触发。	应用程序名称
`Citrix.EventMonitor.IdleStart`	当会话变为空闲时触发。	检查上述通用字段。
`Citrix.EventMonitor.IdleEnd`	当空闲会话结束时触发。	检查上述通用字段。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

值	描述	字段
`Citrix.EventMonitor.WebBrowsing`	当用户在虚拟桌面会话中的浏览器上与网页交互时触发。	应用程序名称、URL
`Citrix.EventMonitor.FileCreate`	当在受监控的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`	当在受监控的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。	检查如上所述的通用字段。
`Citrix.EventMonitor.FileMove`	当受监控的文件系统路径中的文件或文件夹在虚拟桌面会话中或在会话主机 (VDA) 和客户端设备之间移动时触发。	检查如上所述的通用字段。
`Citrix.EventMonitor.FileDelete`	当受监控的文件系统路径内的文件或文件夹在虚拟桌面会话中被删除时触发。	文件名、文件路径、文件大小
`Citrix.EventMonitor.CDMUSBDriveAttach`	当客户端驱动器映射 (CDM) 映射的 USB 大容量存储设备插入到连接了虚拟应用程序和桌面会话的客户端时触发。	检查如上所述的通用字段。
`Citrix.EventMonitor.GenericUSBDriveAttach`	当通用重定向的 USB 大容量存储设备插入到连接了虚拟应用程序和桌面会话的客户端时触发。	检查如上所述的通用字段。
`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账户操作，包括账户创建、启用、禁用、删除、名称更改和密码修改。	描述、目标用户名
`VDA.Print`	当在 Apps and Desktops 中启动打印作业时触发。**注意**：此事件仅适用于 Citrix DaaS 数	文档用户名、计算机名称、打印文件名、打印文件大小、打

© 1997–2026 Citrix Systems, Inc. All rights reserved.

值	描述	字段
	据源。有关详细信息，请参阅启用 Citrix DaaS 的打印遥测。	印机名称、时间、打印总份数、打印总页数
`VDA.Clipboard`	当在 Apps and Desktops 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。有关详细信息，请参阅启用 Citrix DaaS 的剪贴板遥测。	剪贴板格式类型、剪贴板操作、剪贴板操作方向、剪贴板操作允许、剪贴板大小、计算机名称

注意

所有会话录制事件都需要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

输入以下维度值以定义您的搜索查询。

维度	值	类型	描述
`App-Name`	应用程序或桌面会话。	字符串	启动的应用程序或桌面的名称。
	示例应用程序会话：不带场名称的会话：`#Cloud - Excel 2016` 带场名称的会话：`XA65PROD#Concur`		
	示例桌面会话：不带场名称的会话：`#SINXIAP0616 $S1-1` 带场名称的会话：`XA65PROD#SINXIAP 0616 $S1-1`		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

维度	值	类型	描述
`App-Protection-Policies`	示例：`AntiScreenCaptureEnabled`	字符串	会话的活动应用程序保护策略。
`Browser-Name`	示例：谷歌浏览器、Citrix Enterprise Browser™、微软Edge浏览器、火狐浏览器、Safari浏览器	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、休斯顿、芝加哥	字符串	用户的城市名称。
`Client-IP`	IP 地址。示例：10.10.10.10	字符串	用户端点的 IP 地址。
`Client-Type`	安卓, Windows, Macintosh, Chrome, HTML5, Unix/Linux, iOS, 会话录制, 监控	字符串	指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：text, 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**：仅由 SaaS 应用程序支持。
`Clipboard-Operation`	复制、剪切、粘贴或放置	字符串	指示执行了哪个剪贴板操作。**注意**：**place** 操作表示数据被放置在剪贴板上。这不保证剪贴板中的数据是否被客户端粘贴或使用。此操作仅

© 1997–2026 Citrix Systems, Inc. All rights reserved.

维度	值	类型	描述
			支持 VDA.Clipboard 事件。
`Clipboard-Operation-Direction`	客户端到主机，主机到客户端	字符串	指示剪贴板操作的方向。**注意**：仅由应用程序和桌面 (Citrix DaaS™) 剪贴板操作支持。
`Clipboard-Operation-Permitted`	允许或拒绝	字符串	指示剪贴板操作是否在应用程序和桌面会话中被允许。**注意**：仅由应用程序和桌面 (Citrix DaaS) 剪贴板操作支持。
`Clipboard-Result`	成功或已阻止	字符串	指示剪贴板操作的结果。**注意**：仅由 SaaS 应用程序支持。
`Clipboard-Size`	示例：10, 20	数值	当前存储在剪贴板中的数据大小（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、尝试重置帐户密码。	字符串	描述用户帐户修改状态，例如帐户已创建、已删除、已重命名或尝试重置密码。
	对于 `Citrix.EventMonitor.SessionEnd` 事件：未知、注销、翻转、触发和不完整		描述会话录制结束的原因。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

维度	值	类型	描述
`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	文件传输完成后文件的最终路径。
`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、光盘或浏览器下载。	字符串	文件下载或传输到的设备类型。
`Download-File-Format`	示例：txt、PDF、xlsx、docx	字符串	下载文件的格式。
`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	数字	下载文件的大小（以千字节为单位）。
`Event-Type`	账户.登录, 会话.登录, 会话.结束, 应用.启动, 应用.结束, 文件.下载, 打印, 应用保护.屏幕捕获, SaaS应用.启动, SaaS应用.结束, SaaS应用.剪贴板, SaaS应用.文件.下载, SaaS应用.文件.打印,	字符串	有关更多详细信息，请参阅 Event types and supported fields.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

维度	值	类型	描述
	SaaS应用.URL.导航, Citrix.事件监控.应用启动, Citrix.事件监控.应用结束, Citrix.事件监控.置顶, Citrix.事件监控.网页浏览, Citrix.事件监控.文件创建, Citrix.事件监控.文件重命名, Citrix.事件监控.文件移动, Citrix.事件监控.文件删除, Citrix.事件监控.CDMUSBDrive连接, Citrix.事件监控.通用USBDrive连接, Citrix.事件监控.RDP连接, Citrix.事件监控.用户账户修改, VDA.打印, VDA.剪贴板, Citrix.事件监控.注册表更改, Citrix.事件监控.会话启动, Citrix.事件监控.会话结束, Citrix.事件监控.剪贴板, Citrix.事件监控.文件传输		
`Jail-Broken`	是或否	字符串	指示设备是否已获得 root 权限。**注意**：如果此维度不存在，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`	主机到客户端/客户端到主机	字符串	指示文件传输的方向。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

维度	值	类型	描述
`OS-Extra-Info`	示例：20G80，服务包 1，19043	字符串	指示操作系统的附加信息，例如内部版本号、Service Pack 和补丁。
`OS-Name`	示例：macOS 11，Windows 7，安卓 8.1，Windows 10 企业版	字符串	指示操作系统的名称。
`OS-Version`	示例：11.5.1、14.7.1、2009	字符串	指示操作系统的版本
`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：testprinter-1	字符串	使用的打印机名称。
`Process-ID`	示例：11248	字符串	指用于识别执行两个操作的特定进程的进程 ID：**创建新进程**和**建立远程桌面连接**。进程 ID 当前仅与 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`	修改后的注册表名称	字符串	已修改的注册表的名称。
`Registry-Operation`	重命名、创建、删除、设置值、删除值	字符串	指示执行了哪个注册表操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

维度	值	类型	描述
`Registry-Path`	修改后的注册表路径	字符串	已修改的注册表路径。
`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**：当 SaaS 应用程序首次启动时，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类型还是桌面类型。
`Session-Recording-Type`	传统录制/仅事件录制	字符串	指示启动的会话录制类型。
`Session-Server-Name`	示例：托管桌面、Cloud-VDA-1	字符串	从服务器接收到的所连接的应用程序或桌面名称。
`Session-User-Name`	示例：演示用户，测试用户	字符串	从服务器接收到的用户名。
`Source-Path`	示例：C:\Users\admin\Desktop\example.txt	字符串	文件传输前的初始路径。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

维度	值	类型	描述
`Target-User-Name`	示例：user01	字符串	目前，Target-User-Name 仅用于 Citrix.EventMonitor.UserAccountModification 事件，其中它是被修改的用户帐户。
`Total-Copies-Printed`	示例：1, 2	数字	用户打印的副本总数。
`Total-Pages-Printed`	示例：1,2	数字	用户打印的文档页数总计。
`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 应用程序进行的，则此值与从服务器接收到的值相同。
`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	指示执行剪贴板操作的窗口标题。
`Workspace-App-Version`	示例：20.8.0.3 (2008)	字符串	用户设备上安装的 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	指示用户设备上安装的 Citrix Workspace 应用程序或 Citrix Receiver 版本是否受

© 1997–2026 Citrix Systems, Inc. All rights reserved.

维度	值	类型	描述
			Citrix Analytics for Security 支持。当 Workspace 应用程序不受支持时，将鼠标悬停在 **Unsupported** 上。将出现一个弹出窗口，其中包含一个链接，可用于查看支持的版本列表。当 Workspace 应用程序版本即将进入不受支持状态时，自助服务搜索页面上会显示一个横幅，其中列出了可用的受支持版本，您可以启动升级。

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 OS 名称、OS 版本和 OS 额外信息。

- **OS 名称**指示操作系统的名称。
- **OS 版本**指示操作系统的发布 ID 或发布版本。
- **OS Extra Info** 指示操作系统的附加信息，例如内部版本号、服务包和补丁。

下表提供了操作系统版本编号格式的一些示例。

操作系统名称	操作系统版本	操作系统附加信息
macOS 11	11.5.1	20G80
iOS 14	14.7.1	不可用
Windows 10 企业版	2009	19043
视窗 7	6.1	服务包 1
安卓 8.1	8.1.0	不可用

© 1997–2026 Citrix Systems, Inc. All rights reserved.

备注

- 要获取 Mac 11.x 或更高版本的操作系统详细信息，建议的客户端版本是适用于 Mac 2108 或更高版本的 Citrix Workspace 应用程序。
- Windows 10 的操作系统详细信息目前不可用。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Analytics for Security and Performance 故障排除

将匿名用户验证为合法用户

排查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

未从受支持的 Citrix Workspace™ 应用程序版本接收到用户事件

已配置的 Session Recording 服务器无法连接

无法将 StoreFront™ 服务器连接到 Citrix Analytics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

常见问题

© 1997–2026 Citrix Systems, Inc. All rights reserved.

术语表

© 1997–2026 Citrix Systems, Inc. All rights reserved.