Citrix Analytics for Security™

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

Contents

What's new 38
April 15, 2024 38
New Executive Summary report 38
January 29, 2024 38
Workspace App Status field updates 38
January 25, 2024 38
Inconsistencies in the CAS UI are streamlined 38
January 24, 2024 39
Enhanced user profile events on SIEM environments 39
December 01, 2023 39
Admin Email Settings page for Weekly email and SIEM alerts 39
Users dashboard - New active user count time filter and updated the Overview section 39
Enhanced custom reports 40
November 30, 2023 40
Removal of all ShareFile capabilities in Citrix Analytics 40
September 22, 2023 40
Citrix Secure Browser data source in Custom Indicator 40
Enhancement of Weekly Email with SIEM Data Export 41
Consumption of custom administrator's notification preferences in emails 41
July 04, 2023 41
OR operator support in Self-Service Search and Custom Indicator 41
June 15, 2023 41
Enable VDA clipboard telemetry 41
June 14, 2023 42
Availability of Session Recording App lifecycle and Registry events in Citrix Analytics for Security 42

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

June 08, 2023 42
Fixed issues 42
May 29, 2023 43
Citrix Analytics Add-On for Splunk Now Available on Splunk Cloud Platform 43
Session Recording events in SIEM 44
May 24, 2023 44
Notify End User Global Action 44
May 04, 2023 44
Test Event Generation 44
SIEM Email Alert Generation 45
April 13, 2023 45
Fixed issue 45
March 31, 2023 46
Session Recording Events in Citrix Analytics for Security 46
App Protection Events in Self-Service Search 46
March 30, 2023 47
Custom Roles support 47
Troubleshooting panel for SIEM UI 47
March 24, 2023 48
Change in User Profile view 48
Removal of Dynamic Auto-suggestions from all Search Views 48
March 21, 2023 48
Recommendations panel to help onboard on-premise StoreFront™ data source 48
February 23, 2023 49
Fixed issues 49
February 22, 2023 49
Enhancement in weekly email notifications 49
Added Download File Format field for App.SaaS.File.Download event type 49

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

Change in Browser-derived fields 50
February 16, 2023 50
Fixed issue 50
February 03, 2023 50
Analytics support for the Citrix Secure Private Access™ service available in the European Union and the Asia Pacific South regions 50
January 11, 2023 51
Removal of the Web filtering capability from Secure Private Access 51
December 27, 2022 51
Change in data source drop-down for Self-service Search 51
December 13, 2022 51
Users dashboard enhancement 51
December 05, 2022 52
Access assurance dashboard - Logon Network 52
November 18, 2022 52
Fixed issue 52
November 08, 2022 52
Rename actions 52
Fixed issues 53
October 19, 2022 53
Date Source events selection and export 53
October 18, 2022 54
Allow administrator to run dynamic session recording action on Citrix DaaS™ sites 54
October 14, 2022 54
Provide feedback for User Risk indicators 54
September 26, 2022 54
Access assurance to support geofence block list 54
Fixed issues 55

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

September 13, 2022 55
Sharelink dashboard enhancement 55
September 09, 2022 55
Impossible Travel RI Enhancement 55
August 19, 2022 56
Enable VDA Print telemetry 56
August 18, 2022 56
Fixed issue 56
August 17, 2022 56
Customization of end-user email per policy 56
August 11, 2022 57
Fixed issue 57
June 17, 2022 57
Data Processing is enabled by default for new paid entitlements 57
June 09, 2022 57
Fixed issue 57
June 02, 2022 58
Fixed issues 58
May 24, 2022 58
Introducing Impossible travel risk indicators for Content Collaboration, Citrix DaaS and Citrix Virtual Apps and Desktops, and Gateway data sources 58
May 17, 2022 58
Virtual Apps and Desktops is renamed to Apps and Desktops 58
Fixed issues 59
April 05, 2022 59
What's new 59
Secure Workspace Access is renamed to Secure Private Access 59
March 21, 2022 59

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

Fixed issue 59
March 10, 2022 59
What's new 59
Notify administrator email enhancements 59
Fixed issue 61
March 03, 2022 61
What's new 61
Apply request end user response manually 61
Request end user response enhancements for policy 61
February 23, 2022 63
What's new 63
Recommended actions for a risk indicator 63
Fixed issue 64
February 17, 2022 64
What's new 64
Improved data collection and reporting for the Citrix Virtual Apps and Desktops and Citrix DaaS data source 64
Support for contextual templates for the session events and the app events in Content Collaboration 64
February 10, 2022 65
What's new 65
Auto suggested values for the dimensions in the custom risk indicator 65
February 09, 2022 66
What's new 66
New custom roles for the administrators 66
Support for email notifications for custom access administrators 66
January 28, 2022 67
What's new 67

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

Introducing Suspicious Logon risk indicators for Content Collaboration and Gateway data sources 67
January 20, 2022 68
What's new 68
Microsoft Azure Active Directory integration 68
January 18, 2022 68
What's new 68
Support for the share link actions on all Content Collaboration risk indicators 68
Integration with SIEM is now generally available 69
December 23, 2021 69
What's new 69
Share link risk indicators enhancements 69
December 21, 2021 70
What's new 70
Send notifications about risk indicators to your non-Citrix Cloud administrators 70
December 20, 2021 70
What's new 70
Send user response notifications to your Content Collaboration users 70
Access Control is renamed to Secure Workspace Access 70
Fixed issue 71
December 09, 2021 71
What's new 71
Create your custom risk indicators easily with templates 71
December 07, 2021 71
Fixed issue 71
December 02, 2021 71
What's new 71
Malware files detected risk indicator 71

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

New actions for Content Collaboration data source 72
November 29, 2021 73
What's new 73
Email settings enhancements for user notifications 73
November 26, 2021 74
What's new 74
Custom risk indicators and policies menu changes 74
November 25, 2021 74
What's new 74
Security Information and Event Management (SIEM) integration enhancements 74
November 09, 2021 75
Fixed issue 75
November 02, 2021 75
What's new 75
View access profiles and logon details of the Citrix Virtual Apps and Desktops and Citrix DaaS users 75
View malware logs on the self-service search page for Content Collaboration 76
Fixed issue 76
October 20, 2021 77
What's new 77
Session Recording server integration 77
October 19, 2021 77
What's new 77
Notify administrator email template enhancements 77
User log on summary enhancements 78
Fixed issue 79
October 01, 2021 79
What's new 79

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

View audit logs on the self-service search for Content Collaboration 79
Fixed issue 80
September 29, 2021 80
What's new 80
Access assurance location dashboard is now generally available 80
September 15, 2021 80
What's new 80
Custom risk indicator enhancements 80
September 14, 2021 81
What's new 81
Introducing Suspicious Logon risk indicator 81
SIEM messages enhancement 81
Fixed issue 81
August 19, 2021 82
What's new 82
Introducing Citrix Analytics App for Splunk 82
Custom risk indicator schema for SIEM 82
Support for Citrix Director as a data source 82
Support for geofence in the Access assurance location dashboard 83
Workspace app status on the Users page 83
Support for the IS EMPTY operator 83
Improved risk scoring 84
July 29, 2021 85
Deprecated feature 85
Deprecated actions associated with Citrix Endpoint Management™ 85
July 14, 2021 85
What's new 85
Support for the IS NOT EMPTY operator 85

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

July 06, 2021 86
What's new 86
View non-risky users on the Users dashboard 86
July 01, 2021 86
What's new 86
Access assurance location dashboard enhancements 86
Updated the OS facet in self-service search for Virtual Apps and Desktops 87
June 30, 2021 88
What's new 88
Added Workspace app version in custom risk indicator condition for Apps and Desktops 88
June 23, 2021 89
What's new 89
SIEM messages enhancements 89
June 07, 2021 89
What's new 89
Enhancements to the notify administrator(s) action 89
Added support for the view-only sharing action 89
May 18, 2021 90
What's new 90
Migrating the default risk indicators to custom risk indicators 90
Enhancements in self-service search for Gateway 91
Fixed issue 91
April 29, 2021 92
What's new 92
Events details for a custom risk indicator 92
Fixed issue 92
April 16, 2021 92
What's new 92

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

SIEM messages enhancements 92
March 26, 2021 93
What's new 93
Restriction on the SIEM messages 93
Added the data source ID and the indicator category ID fields in the SIEM messages 93
March 18, 2021 93
What's new 93
Access assurance location dashboard 93
Support for the NOT LIKE (!~) operator 94
Translated operating system version 95
Updated the data fields for Apps and Desktops 95
Deprecated feature 95
Removed the VPN_AF and VPN_SU events from the self-service search page 95
March 11, 2021 96
What's new 96
Current timestamp for the user risk score schema 96
March 03, 2021 96
What's new 96
Enhancements to the Logon from suspicious IP risk indicator 96
Enhancements to Access from an unusual location risk indicator 97
Citrix Analytics data format for SIEM 97
Fixed issue 97
February 18, 2021 97
What's new 97
Support for the first time access from a new entity in the custom risk indicator 97
Maximum limit for creating custom risk indicator 98
User location data from Citrix Virtual Apps and Desktops and Citrix DaaS 98
Multi-column sorting 98

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

Deprecated features 99
Excessive authorization failure risk indicator deprecated 99
January 27, 2021 99
What's new 99
Enhancements to the Access from an unusual location risk indicator 99
January 20, 2021 100
Fixed issue 100
January 19, 2021 100
Fixed issue 100
January 13, 2021 100
What's new 100
New version of Citrix Analytics Add-on for Splunk is available 100
Added support for Splunk Cloud Inputs Data Manager (IDM) and Splunk 8.1 64-bit 101
Deprecated support 101
Removed support for Splunk 7.1 64-bit 101
January 11, 2021 101
Fixed issue 101
December 17, 2020 101
What's new 101
Use preconfigured custom risk indicators and a policy to block access from unusual locations (geofencing) 101
View accessed locations in the user-response email 102
Renamed Content Collaboration risk indicator- First time access from new location 102
Deprecated features 102
Risk indicator feedback 102
December 07, 2020 102
What's new 102
Improvements to the Potential data exfiltration risk indicator 102

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

Improvements to the Content Collaboration risk indicator- First time access from new location 102
November 30, 2020 103
What's new 103
Self-service search page improvements 103
Policy improvements 104
November 04, 2020 104
What's new 104
Unusual Authentication Failure - Citrix Gateway risk indicator 104
October 20, 2020 105
Fixed issue 105
October 15, 2020 105
New features 105
Access from an unusual location – Citrix Virtual Apps and Desktops and Citrix DaaS risk indicator 105
Share Link dashboard enhancements 106
Share Link risk timeline enhancements 106
Deprecated features 107
Access from device with unsupported operating system (OS) risk indicator deprecated 107
September 10, 2020 107
New features 107
Checklist for StoreFront 107
Self-service search - support for NOT EQUAL (!=) operator 108
September 08, 2020 108
New features 108
User Correlation 108
Fixed issue 109
August 11, 2020 109

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

Fixed issues 109
July 31, 2020 109
Fixed issues 109
July 09, 2020 109
New features 109
Virtual Apps and Desktops site card displays users with supported and unsupported clients 109
Access from an unusual location risk indicator 110
Users dashboard data 111
Redesigned Users page 112
Risky Users pane enhancements 113
Users in Watchlist pane enhancements 114
Privileged Users pane enhancements 114
Deprecated features 115
Alerts 115
Risky Users and Watchlist page 115
Risky Users pane 116
Risk Indicator pane 117
Trend view 118
User Groups page 118
June 26, 2020 119
Deprecated features 119
Unusual time of application access (Virtual/SaaS) risk indicators deprecated 119
June 02, 2020 119
Fixed issues 119
May 11, 2020 120
Fixed issues 120
April 29, 2020 120

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

Fixed issues 120
April 02, 2020 120
New features 120
Disable data processing when StoreFront is not added 120
Fixed issues 121
March 04, 2020 121
Fixed issues 121
February 20, 2020 121
New features 121
Citrix Analytics for Security offering 121
Risk Categories dashboard 122
Risk Category column on the Custom Indicators page 123
Change in risk indicator names 123
Fixed issues 124
January 09, 2020 125
New features 125
Continuous risk assessment 125
Policy configuration 125
Lock user and Unlock user actions 129
Access summary dashboard 130
Policies and actions dashboard 131
Self-service search for policies 131
Deprecated features 132
Risk score change policy-based condition removed 132
Multiple policy-based actions removed 132
Fixed issues 132
December 12, 2019 132
New features 132

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

Splunk version support 132
December 04, 2019 133
New features 133
Custom risk indicator for Citrix Gateway 133
November 22, 2019 133
New features 133
First time access from new device – Citrix Virtual Apps and Desktops risk indicator 133
First time access from new IP - Citrix Gateway risk indicator 134
Logon from suspicious IP - Citrix Gateway risk indicator 134
Self-service search for Citrix Gateway events 135
Self-service search for Citrix Remote Browser Isolation™ events 135
Remove from watch list action 135
Improved onboarding messages when configuring a StoreFront deployment 136
Deprecated features 136
Risk indicator - Access from new device remove 136
Fixed issues 137
November 08, 2019 137
Fixed issues 137
October 21, 2019 137
New features 137
Modified name for analytics agent 137
Support for the time dimension for custom report 138
Audit logs enhancements 139
Fixed issues 140
September 23, 2019 140
Fixed issues 140
August 30, 2019 140
New features 140

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

Change in default time period across dashboards 140
Fixed issues 141
August 20, 2019 141
New features 141
Self-service search enhancements 141
Custom report enhancements 141
Risk Indicators dashboard 142
Risky Users dashboard enhancements 143
Share link risk indicator - Excessive downloads 144
Self-service search for the Authentication data 144
July 11, 2019 145
New features 145
Custom risk indicators 145
Privileged status on risk timeline 145
Expire share link action 145
Self-service search enhancements 146
Data error status on the site cards 146
Fixed issues 146
June 19, 2019 146
Fixed issues 146
June 17, 2019 147
New features 147
StoreFront configuration 147
May 30, 2019 147
New features 147
Excessive logon failures 147
Fixed issues 147
May 09, 2019 148

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

New features 148

Creating custom reports 148

Privileged user monitoring 148

Weekly email summary 149

April 26, 2019 149

New features 149

Delegated administrators 149

Fixed issues 149

February 19, 2019 150

New features 150

Splunk integration 150

Dynamic session recording 150

Share Links dashboard and risk indicator 150

Microsoft Active Directory integration 151

January 04, 2019 151

New features 151

Addition of SOURCE column for existing risk indicators 151

Advanced user profile 151

Microsoft Graph Security risk indicators 152

Ways to enter the self-service search page 152

Self-service search for Content Collaboration 153

Self-service search for Apps and Desktops 153

Export self-service search events to CSV file 153

Improved onboarding for Citrix Virtual Apps and Desktops 153

November 29, 2018 153

New features 153

Microsoft Security Graph data source 153

View event details and discovered users on the site cards for data sources 154

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

November 16, 2018 155
New features 155
Self-service search for access data 155
Risk indicator feedback 156
Fixed issues 156
Known Issues 157
Analytics offerings 158
layout: doc replicate-from: commons/analytics-offerings.md 158
Data Sources 159
Citrix data sources 159
External data sources 162
Supported home regions 162
Citrix Workspace app version matrix 163
Data governance 166
layout: doc replicate-from: commons/data-governance.md 166
System Requirements 167
Citrix Analytics for Security subscription 167
Data sources requirements 167
Supported browsers 167
Manage administrator roles for Security Analytics 169
Permissions for the custom roles 169
Security alert notifications for the administrators 170
Getting started 172
Step 1: Sign in to Citrix Cloud™ 172
Step 2: Get access to Security Analytics 172
Step 3: Manage Security Analytics 173
What's next 174
Citrix Endpoint Management™ data source 175

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

Prerequisites 176
View data source and turn on data processing 176
View users and received events 177
Turn on or off data processing 178
Citrix Gateway (on-premises) data source 180
Citrix Remote Browser Isolation™ data source 180
Citrix Secure Private Access™ data source 180
Prerequisites 180
View data source and turn on data processing 181
View users and received events 181
Turn on or off data processing 183
Citrix Virtual Apps and Desktops™ and Citrix DaaS data source 185
Supported client versions 185
Enable Analytics on Citrix DaaS 186
Prerequisites 186
View the data source and turn on data processing 186
View cloud site, users, and received events 186
Enable Analytics on Citrix Virtual Apps and Desktops on-premises 188
Prerequisites 188
Onboard Citrix Virtual Apps and Desktops on-premises sites using StoreFront 189
Onboard Citrix Virtual Apps and Desktops on-premises sites using Workspace 189
Connect to Citrix Director for on-premises sites 193
Prerequisite and configuration steps 193
View your connected sites and received events 194
Connect to Session Recording deployment 195
Prerequisites 195
Configure your Session Recording server 196
View the connected deployments 198

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

View received events 199
Add Session Recording servers 199
Remove Session Recording servers 200
Enabling print telemetry for Citrix DaaS 201
Prerequisites 202
Enable print telemetry in power managed machines 202
Enable print telemetry in a new master image 204
Enable print telemetry in machines that are not power managed 204
Enable print telemetry for a new physical VDA 205
Create registry keys 206
Enable print trace for the organizational unit 215
Enabling clipboard telemetry for Citrix DaaS 218
Prerequisites 218
Turn on or off data processing on the data source 219
Microsoft Active Directory and Azure Active Directory integration 219
Prerequisites 220
Connect Microsoft Active Directory 220
Connect Microsoft Azure Active Directory 221
View user information 222
Microsoft Graph Security integration 222
Prerequisites 222
Onboarding Microsoft Graph Security instances 223
Turn on or off data processing 225
Security Information and Event Management (SIEM) integration 227
Benefits 227
SIEM integration architecture 227
Turn on or off data transmission 228
Setting up SIEM environment 229

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

SIEM export account setup 229
SIEM configuration and environment setup 230
Data events exported from Citrix Analytics for Security to your SIEM service 230
Troubleshooting SIEM Integration 231
Splunk integration 232
Integrate Citrix Analytics for Security™ with Splunk 232
Data export 233
Reset Password Capability 234
Turn on or off data transmission 236
Citrix Analytics Add-On for Splunk 237
Citrix Analytics Add-On for Splunk (On-prem/Enterprise) 237
Supported versions 237
Prerequisites 238
Download and install Citrix Analytics add-on for Splunk 239
Configure Citrix Analytics add-on for Splunk 240
Citrix Analytics Add-On for Splunk (Cloud) 242
Prerequisites 242
Download and install Citrix Analytics add-on for Splunk 244
Configure Citrix Analytics add-on for Splunk 244
How to consume events in your Splunk Environment 245
Troubleshoot Citrix Analytics add-on for Splunk 247
Citrix Analytics App for Splunk 247
Supported Splunk version 247
Prerequisites for Citrix Analytics App for Splunk 247
Installation and configuration 248
Splunk architecture with Citrix Analytics add-on application 249
Citrix Analytics dashboards for Splunk 252
Prerequisite 252

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

User risk score overview 252
Risk indicator overview 254
Select category to view report 254
View report 255
Risk indicator details 256
Select category to view the reports 256
View the reports 257
Entity details 258
View the report 258
User profile overview 261
View the events 261
Received events 262
View the reports 262
Sample event correlation 263
Prerequisites 264
Correlate the events 264
Troubleshooting for no events 264
Configuration issues with Citrix Analytics add-on for Splunk 267
layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/splunk-add-on-debugging.md 267
Microsoft Sentinel integration 268
Prerequisites 268
Integrate with Microsoft Sentinel 269
Turn on or off data transmission 273
Citrix Analytics workbook for Microsoft Sentinel 275
Prerequisite 275
View the Citrix Analytics events 275
View the Citrix Analytics workbook 276

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

User risk score overview 278
User details 278
User profile 279
Received events 280
Risk indicator details 281
Risk indicator overview 281
Troubleshooting guidance for Sentinel Integration via Logstash 282
Check Logstash Server Logs 282
Common Error: Using bundled JDK 283
Check Microsoft Sentinel Workbook 285
Check Log Analytics workspace logs using KQL 286
Elasticsearch integration 287
Prerequisites 287
Integrate with Elasticsearch 288
Turn on or off data transmission 291
SIEM integration using Kafka or Logstash based data connector 292
Prerequisites 293
Integrate with a SIEM service using Kafka 293
Data flow 296
Authentications 296
Encryption with SSL and Authentication with SASL/SSL&SASL/PLAINTEXT 297
SIEM integration using Logstash 298
Integrate with a SIEM service using Logstash 298
Turn on or off data transmission 301
Citrix Analytics data exports format for SIEM 303
Risk insights data for SIEM 304
Schema details of the risk insights events 305
User profile data schema 306

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

User risk score schema 311

Risk score change schema 312

Risk indicator schema 313

Citrix Secure Private Access risk indicators schema 317

Citrix Endpoint Management risk indicators schema 326

Citrix Gateway risk indicators schema 332

Citrix DaaS and Citrix Virtual Apps and Desktops risk indicators schema 356

Microsoft Active Directory Indicator 371

Custom risk indicator schema 372

Data source events 394

Schema details of the data source events 395

Citrix Virtual Apps and Desktops events 395

Secure Private Access events 396

Device Posture service events 397

Leveraging Citrix Analytics SIEM Data Model for Threat Analysis and Data Correlation 398

Custom Risk Indicator Insights 398

Setting Custom Risk Indicator In Citrix Analytics 398

Risk Indicator Occurrences on Splunk - Raw Queries 402

Risk Indicator Occurrences on Splunk - Dashboarding App 404

Data source events 405

Troubleshooting Data Exports 407

Summary tab 408

Available data in Citrix Analytics 408

Available events for SIEM consumption 410

Data consumption by SIEM 410

Data Export Quick Guide 416

Test Event Generation 421

SIEM Email Alert 423

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

How to enable email notifications? 424
Types of SIEM Email Alert 424
Example Sigma Signatures for Security Insights 431
How to use these examples 431
View the data source and turn on the data processing 431
Using CAS queries 432
Using Sigma signatures 432
Compromised endpoints 433
Unsanctioned browser 433
Details 433
CAS query 433
Sigma signature 433
Unsanctioned operating systems 434
Details 434
CAS query 434
Sigma signature 434
Unauthorized IP address or subnets 435
Details 435
CAS query 435
Sigma signature 435
Unauthorized operating systems outside allow list 436
Details 436
CAS query 436
Sigma signature 436
Unsanctioned Workspace app versions 437
Details 438
CAS query 438
Sigma signature 438

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

Insider threats 439
Unusual desktop names 439
Details 439
CAS query 439
Sigma signature 439
Monitor specific process 440
Details 440
CAS query 440
Sigma signature 440
Unauthorized virtual apps 441
Details 441
CAS query 441
Sigma signature 441
Data Exfiltration 442
Printing from SaaS apps 442
Details 442
CAS query 442
Sigma signature 442
Clipboard usage on SaaS apps 443
Details 443
CAS query 443
Sigma signature 444
Users dashboard 445
Overview 445
User activity status 446
Facets 446
Search box 446
Latest score 446

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

User 447

Discovered data source 447

Indicators triggered 447

Actions applied 448

Events processed 449

User risk distribution 449

Risky users 450

High risk 451

Medium risk 451

Low risk 452

Top users 452

Watchlist users 453

Risk Categories 454

Use case 455

How to analyze the Risk Categories dashboard? 456

Types of risk categories 458

Data exfiltration 458

Insider threats 459

Compromised users 459

Compromised endpoints 460

Risk indicators and actions 460

Access Summary 461

Policies and Actions 462

Top Policies 463

All policies 463

Top Actions 464

Actions 464

Risk Indicators 465

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

Access assurance dashboard 467
View the dashboard 467
Access summary 467
Logon location 468
Locations identified as not available 470
Enable geofencing 471
Geofence: Unique User Logons 475
Logon network 477
View user network details 478
View access profiles of the users 479
Facets 479
View logons details of users 481
Search bar 482
Facets 483
User risk timeline and profile 484
Risk timeline 485
Risk summary 488
User profile 489
Citrix® user risk indicators 491
Citrix Endpoint Management™ risk indicators 494
Device with blacklisted apps detected 494
When is the device with blacklisted apps detected risk indicator triggered? 494
How to analyze the device with blacklisted apps detected risk indicator? 494
What actions you can apply to the user? 496
Jailbroken or rooted device detected 497
When is the jailbroken or rooted device detected risk indicator triggered? 497
How to analyze the jailbroken or rooted device detected risk indicator? 497
What actions you can apply to the user? 499

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

Unmanaged device detected 500
When is the unmanaged device detected risk indicator triggered? 500
How to analyze unmanaged device detected risk indicator? 500
What actions you can apply to the user? 502
Citrix Gateway risk indicators 502
End Point Analysis (EPA) scan failures 502
When is the EPA scan failures risk indicator triggered? 503
How to analyze the EPA scan failures risk indicator? 503
What actions you can apply to the user? 504
Excessive authentication failures 505
When is the Excessive authentication failures risk indicator triggered? 505
How to analyze the Excessive authentication failures risk indicator? 506
What actions you can apply to the user? 507
Impossible travel 508
When is the Impossible travel risk indicator triggered? 508
How to analyze the Impossible risk indicator 508
What actions you can apply to the user? 510
Logon from suspicious IP 511
When is the Logon from suspicious IP risk indicator triggered? 511
How to analyze the Logon from suspicious IP risk Indicator? 511
What actions you can apply to the user? 514
Suspicious logon 514
When is the Suspicious logon risk indicator triggered? 514
How to analyze the Suspicious logon risk indicator 515
What actions you can apply to the user? 518
Unusual authentication failure 518
When is the unusual authentication failure indicator triggered? 519
How to analyze the unusual authentication failure indicator? 519

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

What actions you can apply to the user? 521
Citrix Secure Private Access™ risk indicators 522
Risky website access 522
Attempt to access blacklisted URL 522
When is the Attempt to access blacklisted URL risk indicator is triggered? 523
How to analyze the Attempt to access blacklisted URL risk indicator? 523
What actions you can apply to the user? 524
Unusual upload volume 525
When is the Unusual upload volume risk indicator triggered? 525
How to analyze the unusual upload volume risk indicator? 525
What actions you can apply to the user? 527
Excessive data download 528
When is the Excessive data download risk indicator triggered? 528
How to analyze the Excessive data download risk indicator? 528
What actions you can apply to the user? 530
Citrix Virtual Apps and Desktops™ and Citrix DaaS risk indicators 531
Impossible travel 531
When is the Impossible travel risk indicator triggered? 531
How to analyze the Impossible risk indicator 531
What actions you can apply to the users? 533
Potential data exfiltration 534
When is the Potential data exfiltration risk indicator triggered? 534
How to analyze the Potential data exfiltration risk Indicator? 535
What actions you can apply to the user? 537
Suspicious logon 538
When is the Suspicious logon risk indicator triggered? 538
How to analyze the Suspicious logon risk indicator 539
What actions you can apply to the users? 542

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

Provide feedback for User Risk indicators 543
View filters 545
Microsoft Graph Security risk indicators 549
How to analyze Microsoft Graph Security risk indicators 549
How to get more information about the risk indicators 550
What actions you can apply to the user 550
Custom risk indicators 551
Preconfigured custom risk indicators 551
Custom risk indicators page 551
Analyzing a custom risk indicator 552
Actions you can apply to the user 553
Custom risk indicator templates 553
Creating a custom risk indicator 554
Defining a condition for a custom risk indicator 556
Using the advanced options 556
Selecting the risk category 560
Selecting the severity 560
Supported operators for defining a condition 560
Modifying a custom risk indicator 563
Deleting a custom risk indicator 564
Continuous risk assessment 565
Use cases 566
Key features 566
Support multiple conditions 566
Notify users before applying actions 566
Notify users after applying actions 566
Enforcement and monitor modes 567
Visibility into access and policy dashboards 567

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

Default policies 567
Policies and actions 569
What are the policies? 569
Default policies 570
How to add or remove conditions? 571
Default and custom risk indicators 571
What are the actions? 572
Preconfigured custom risk indicators and policies 577
Preconfigured custom risk indicators for the geofencing scenario 577
Preconfigured policy for the geofencing scenario 578
Create your own policy with preconfigured custom risk indicators for geofencing 580
Preconfigured custom risk indicators for the first time access scenario 581
End user email settings 585
Modify email settings 585
Watchlist 588
How to add a user to the watchlist 588
How to remove a user from the watchlist 589
How to monitor users in a watchlist 590
Weekly email notification 592
Enable email notifications 592
When do you get an email from Citrix Analytics? 592
Account Summary 594
Data Summary 594
Users information 595
Top Risk Indicators 595
Top Actions 596
What action do you need to take after receiving the email? 597
Audit logs 600

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

Activities that generate audit events 600
How to view the audit log 601
How to use the audit log 601
Custom reports 603
Supported Fields in Custom Reports 603
Reports 605
Create a custom report 605
Creating a custom report with templates 606
Creating a custom report without templates 608
Save a report 609
View a report 611
Export a report 611
Delete a report 612
Edit a report 612
Executive Summary report 613
What reports does it contain? 613
Edit an Executive Report 614
Self-service search 619
layout: doc replicate-from: commons/self-service-search.md 619
Self-service search for Authentication 619
Select the Authentication data source 619
Select the facets to filter events 619
Specify search query to filter events 620
Self-service search for Gateway 622
Select the Gateway data source 622
Use the facets to filter events 622
Specify search query to filter events 624
Supported values for your search query 627

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

Access-Insight-Flags 627
Applications-Byte-Consumption 627
Authentication-Servers-IP 627
Authentication-Stage 628
Authentication-Type 628
Backend-Server-Name 628
Browser 628
City 628
Client-IP 629
Client-IP-Type 629
Client-Port 629
Country 629
Event-Type 630
Gateway-FQDN 630
Gateway-IP 630
Gateway-Port 630
Logout-Mode 631
NetScaler-IP 631
OS 631
Record Type 632
SSO-Authentication-Method 632
Server-IP 632
Server-Port 632
Session-State 633
Status-Code 633
User-Agent 634
VPN-Session-ID 634
VPN-Session-Mode 634

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

Self-service search for Policies 635
Select the Policies data set 635
Select the facets to filter events 635
Specify search query to filter events 636
Self-service search for Remote Browser Isolation (Secure Browser) 638
Prerequisite 638
Select the Remote Browser Isolation data source 638
Specify search query to filter events 639
View user event details 640
Self-service search for Secure Private Access 641
Select the Secure Private Access data source 641
Select the facets to filter events 642
Specify search query to filter events 644
Self-service search for Apps and Desktops 645
Select the Apps and Desktops data source 645
Select the facets to filter events 646
Specify search query to filter events 646
Event types and supported fields 648
Supported values for your search query 654
Operating system naming format 667
Troubleshoot Citrix Analytics for Security and Performance 669
layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance.md 669
Verify anonymous users as legitimate users 669
layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/anonymous-users-issue.md 669
Troubleshoot event transmission issues from a data source 669

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

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/datasource-events-transmission-issue.md 669

Trigger Virtual Apps and Desktops events, SaaS events, and verifying event transmission 669

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/virtual-apps-desktops-saas-events-verify.md 669

No user events received from supported Citrix Workspace™ app version 669

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/workspace-app-partially-supported.md 669

Configured Session Recording server fails to connect 670

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/session-recording-issue.md 670

Unable to connect StoreFront™ server with Citrix Analytics 670

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/storefront-issue.md 670

FAQs 671

layout: doc replicate-from: commons/faqs.md 671

Glossary of terms 672

layout: doc replicate-from: commons/glossary.md 672

Security Analytics Document History 673

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

What's new

A goal of Citrix is to deliver new features and product updates to Citrix Analytics customers when they are available. New releases provide more value, so there's no reason to delay updates.

To you, the customer, this process is transparent. Initial updates are applied to Citrix internal sites only, and are then applied to customer environments gradually. Delivering updates incrementally in waves helps to ensure product quality and to maximize the availability.

April 15, 2024

New Executive Summary report

You now have the option to consolidate multiple reports into a single executive report which can be scheduled for the required time period. With this new feature, you are only providing your audience with necessary graphical information. For more information, see Executive summary report.

January 29, 2024

Workspace App Status field updates

- **Self-Service Search**: You can now perform queries to find out the support status of a Workspace App version by utilizing the newly introduced **Workspace App status** field for the **Citrix Apps and Desktops** data source.
- **Users**: The **Workspace App Status** column has been removed.

For more information, see self-service search for Apps and Desktops.

January 25, 2024

Inconsistencies in the CAS UI are streamlined

The following problems have been resolved in the **Self-Service Search** feature for the **Apps and Desktops** data source:

- Events that were previously displayed out of order within a session now appear correctly.

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

- The default columns have been updated.

January 24, 2024

Enhanced user profile events on SIEM environments

The user profile events exported to your SIEM environments now include:

- IP address insights
- Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) location insights

These new enhancements enable you to identify the client's IP address used to access your organization's data and gather user location information from both Citrix Virtual Apps and Desktops, as well as Citrix DaaS.

For more information, see Risk insights data for SIEM.

December 01, 2023

Admin Email Settings page for Weekly email and SIEM alerts

The new **Admin Email Settings** feature allows you to configure custom distribution list recipients for system alerts. This enhancement ensures that administrators receive only the system alerts that are relevant to them.

For more information, see Admin email settings.

Users dashboard - New active user count time filter and updated the Overview section

The new time filter in the **Users** dashboard allows you to view and modify the total number of active users in your organization for a specific time period, considering the data sources for which you have enabled Citrix Analytics.

The enhanced **Overview** section in the **Users** dashboard displays the total number of users in your organization, as well as the number of active and inactive users who are currently logged on.

For more information, see Users dashboard.

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

Enhanced custom reports

- You can now create and schedule custom reports using the events and insights available in Citrix Analytics for Security. Custom reports help you to extract information of specific interest and organize the data graphically.
- You can now use the enhanced Custom Report platform capabilities that include Self-Service Search query-based reports, templates, better visualizations, coverage of all data sources and metrics, scheduling reports, and exporting PDFs.

For more information, see Custom reports.

November 30, 2023

Removal of all ShareFile capabilities in Citrix Analytics

The following ShareFile detection capabilities are removed:

- Share Links
- Associated Risk Indicators
- Policies with their occurrences
- Content Collaboration Data Export configurations
- Content Collaboration Reports
- Content Collaboration datasource on Search
- Content Collaboration Saved Searches
- Content Collaboration Data Source.

The removal of these capabilities might result in a temporary inconsistency in risk score and user timelines. All other Citrix Analytics capabilities remain the same.

Learn how ShareFile simplifies access to security controls directly from ShareFile.com.

September 22, 2023

Citrix Secure Browser data source in Custom Indicator

You can now create risk indicators for the Citrix Secure Browser data source to track a user's activity in the Secure browser. For more information, see Custom Indicators.

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

Enhancement of Weekly Email with SIEM Data Export

The Weekly email has been enhanced to provide deeper insight into your organization’s security posture by enabling the SIEM data export. You can now onboard and activate more data sources to discover a wide range of events around your users. The weekly email includes the following new additions:

- The data summary section shows the status of data consumption in the SIEM environment.
- Recommendations for Data Exports based on the data export consumption status.

For more information, see Weekly email notification.

Consumption of custom administrator's notification preferences in emails

Citrix Analytics for Security now honors the notification preferences set by custom administrators in Citrix Cloud. This enhancement provides custom administrators with greater flexibility in managing their notification preferences. This preference is also leveraged while sending notification emails such as weekly emails, Notify Administrators action emails, and alerts for data exports.

For more information, see Manage administrator roles for Security Analytics.

July 04, 2023

OR operator support in Self-Service Search and Custom Indicator

The **OR** operator is now available in the **Self-Service Search** and **Custom Risk Indicator** features. You can use the **OR** operator in search views such as Self-Service Search and Custom Indicator queries.

For more information, see Supported operators in search query.

June 15, 2023

Enable VDA clipboard telemetry

An event called VDA.Clipboard triggers when you initiate any clipboard operation in Citrix Apps and Desktops. These clipboard logs provide vital information such as the VDA name, clipboard size, clipboard format type, client IP, clipboard operation, clipboard operation direction, and whether the clipboard operation was permitted. The VDA Clipboard event attributes are also available on the Self-service search and Custom Risk Indicators workflows.

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

- **Self-service search**: You can generate reports, save queries and review the VDA.Clipboard events along with all its attribute details.
- **Custom Risk Indicators**: Attributes for the VDA clipboard events are available with Custom Indicators workflow. You can use these event key/value pairs to configure custom indicator triggers and setup automated policies with actions.

You can use the **Clipboard place metadata collection for Security monitoring** policy to enable the clipboard telemetry and transmission of clipboard logs to Citrix Analytics for Security. By default, this policy is enabled. To disable, navigate to the Policy page and disable it to stop the collection of data from the VDAs.

For more information, see Enabling clipboard telemetry for Citrix DaaS.

June 14, 2023

Availability of Session Recording App lifecycle and Registry events in Citrix Analytics for Security

The following **App Lifecycle** and **Registry** events from **Session Recording** are now available in Citrix Analytics for Security:

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

You can view these events, create custom indicators, and export these events to your SIEM environments.

For more information, see Event types and supported fields.

June 08, 2023

Fixed issues

- Some session logon events that are sent to Citrix Analytics for Security, do not have a username. This results in the username column showing as **NA** for some events on Self Service Search and Access Assurance User Logons page. Sometimes, It also results in having

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

a unique user count as zero although the total logon count is non-zero in the Access Assurance IP Registering Organizations chart when viewing the data for a small time range such as **Last 1 Hour** or **Last 1 Day**. This issue is fixed now.

- In Self-service search for Apps and Desktops, for Session.Logon and Session.end user events, the App-Name dimension in search queries is populated with Delivery Group names rather than the name of the application or desktop launched, which can be misleading to administrators. The App-Name dimension is more useful for queries on App.Start/App.End events, as it points to the applications which are being launched. For more details, refer Self-service search for Apps and Desktops. This issue is fixed now.
- If your organization is onboarded to Citrix Cloud in the **Asia Pacific South** home region, the Content Collaboration events are not visible in your Citrix Analytics tenants. This issue is fixed now.
- Few versions of the Citrix Workspace app and Citrix Receiver client do not send specific events to Citrix Analytics. Therefore, Citrix Analytics cannot provide insights and generate risk indicators for these events. This issue is fixed now. For more information, see Check 6: Are the virtual apps and desktops events transmitted to Analytics?.

May 29, 2023

Citrix Analytics Add-On for Splunk Now Available on Splunk Cloud Platform

Splunk Integration for Citrix Analytics utilizes Citrix Analytics Add-On for Splunk to connect to the analytics environment and bring in business critical data into your Splunk Environment.

Earlier, the add-on was vetted by Splunk only for installation on the Splunk Enterprise layer and the customers were responsible for configuring the add-on within their on-premises Splunk environment. With the latest version of 2.1.2, the add-on has the added Splunk platform compatibility with Splunk Cloud. Customers using **Classic** instances with IDM or **Victoria** instances can utilize this platform compatibility enhancement. Now, customers have the flexibility to choose between Splunk Enterprise or Splunk Cloud while considering the deployment of our add-on to facilitate Splunk integration.

For more information, see Splunk Integration.

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

Session Recording events in SIEM

The **Session Recording** events can now be exported to SIEM in the form of **Risk Insight** events and **Data Source** events for Apps and Desktops. The newly added event types can be found in the Data events for export stage under the **Data Exports** page.

For more information, see Policies and Actions.

May 24, 2023

Notify End User Global Action

The **Policies and Actions** feature in Citrix Analytics now supports the **Notify End User** global action which can be paired with built-in or custom risk indicator trigger(s). Administrators can create policies with the **Notify End User** action that generates email notifications for end users only. This action can be used for various of compliance use cases such as notifying the users for unsanctioned application usage, or alerting for suspicious behavior on their Citrix accounts without taking any disruptive actions. Administrators can customize the email message body and subject line depending upon the specific scenario.

For more information, see Notify End User.

May 04, 2023

Test Event Generation

The **Test event generation** feature is created to aid customers for quickly testing their Citrix Analytics - SIEM pipeline. Earlier, if the administrator had to test this integration, she/he would have to wait for data source onboarding and user activity to check if the events were being generated by Citrix Analytics and hence received by their SIEM environment. This is no longer a necessity. One can simply click the **Send test data** button to send a dummy event into the SIEM environment and use the query provided to check if the Citrix Analytics SIEM Integration is set as expected. This can also work for the administrator who's trying to debug disrupted data flow since it can help in isolating the point of failure.

For more information, see Test Event Generation.

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

SIEM Email Alert Generation

The SIEM Email Alert Generation capability takes the troubleshooting journey of Data Exports to a new level of ease. Citrix Analytics sends system alerts for activities that can lead to or indicate SIEM data flow disruption. The email gets distributed amongst Citrix Cloud administrators, Security full administrators, Security read-only administrators, and Security and Performance read-only administrators. The following are the different types of alerts that are sent:

1. **SIEM Data Export Alert - Password was reset**

   This email is triggered whenever the account password is reset from the Data Exports page. If only done on Citrix Analytics for Security GUI, it can lead to disruption in the data flow. This alert contains the time at which password reset was performed and hence makes getting back to successful data flow that much easier.

2. **SIEM Data Export Alert - Data Flow Stopped**

This email is triggered whenever the customer has faced data flow disruption form

- **More than 24 hours** - Critical time to quickly get back to successful data flow by using the helpful troubleshooting tips within the alert or utilizing the **Data Export Summary** tab with **Quick Guide**.
- **More than 7 days** - The Kakfa retention policy for each customer's topic is seven days which means there's a possibility that some security postured data has expired. Imperative to use the troubleshooting tools to reinstate data flow to SIEM.
- **More than 30 days** - This means that the customer has suffered from security-inclined data and needs to pay immediate attention to restoring the data flow from Citrix Analytics to the SIEM environment.

For more information, see SIEM Email Alert Generation.

April 13, 2023

Fixed issue

Windows Citrix Workspace™ App sends an empty file name, path, and format property from Citrix Workspace App Version 2203 and later versions. As a result, Citrix Analytics for Security GUI shows NA values for Download File Name, Download File Path, and Download File Format columns. This issue is fixed now.

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

March 31, 2023

Session Recording Events in Citrix Analytics for Security

In Citrix Apps and Desktops, two new event types have been added to help identify and assess session recording-based events.

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

Administrators can now easily identify and assess potential security risks. They can use these events to gather information on vital data such as process IDs, destination IP addresses and descriptions of user account operations. Additionally, these events can also be found on **Custom Risk Indicators** page and the **Self-Service Search** page.

- **Self-Service Search**: You can view these events along with their attribute details.
- **Custom Risk Indicators**: You can configure any custom indicator using these event types. For more information, see Event types and supported fields.

App Protection Events in Self-Service Search

A new event called **AppProtection.ScreenCapture** triggers when you try to capture a screenshot while being in a protected session under Citrix Apps and Desktops data source. The **AppProtection.ScreenCapture** events are also available on **Self-Service Search** and **Data Exports** pages.

- **Self-service search**: You can view the **AppProtection.ScreenCapture** results along with all its attribute details.
- **Data Exports**: You can view the **AppProtection.ScreenCapture** event type under the Data Exports section. Navigate to, **Settings > Data Exports > Configuration > Data Events for Export >** select **Apps and Desktops** from the Data Source Events (Optional) category.

You can also view a new attribute called **App Protection Policies** for the **Session.Logon** event.

For more information, see Event types and supported fields.

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

March 30, 2023

Custom Roles support

An administrator can be added for custom roles using groups in your Active Directory or Azure Active Directory or by setting up an Okta integration for Citrix Analytics for Security. This integration enables a streamlined approach to manage service access permissions for all group administrators.

After successfully adding an administrator to Active Directory or Azure Active Directory, the administrator can create groups and assign a custom role to a specific group. Individual permissions are given preference over group permissions if an administrator is a member of both.

For more information, see Custom Roles Support.

Troubleshooting panel for SIEM UI

The Data Exports UI is enhanced with the following changes:

- **Summary Tab**: The Summary tab describes the SIEM event metrics, data source onboarding status and the data consumption status in the following scenario:
  - **Available Data in Citrix Analytics**: Provides the onboarding status for the different data sources.
  - **Available Events for SIEM Consumption**: Provides the number of insights that are being sent to your SIEM environment.
  - **Data Consumption by SIEM**: Provides the data consumption status.
- **Configuration Tab**: The **Configuration** tab contains the information about your account setup, SIEM environment setup and data events selection.
- **Data Export Quick Guide**: Administrators can now make use of the **Quick Guide**, which makes it simpler to set up and maintain SIEM integrations. The **Data Export Quick Guide** link is accessible from both the **Summary** and **Configuration** tabs.

For more information, see Troubleshooting Data Exports.

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

March 24, 2023

Change in User Profile view

Users' profile data related to Applications, Locations, Devices, and ShareFile data usage are not available on the **User Info** page in User's Timeline. The following user information that comes from Active Directory is still available -

- Job Title
- Address
- Email
- Phone
- Location
- Organization

There are no changes in the user profile data that is exported to SIEM. For more information, see User profile.

Removal of Dynamic Auto-suggestions from all Search Views

The auto-suggestion functionality for dimensions based on the tenant's historical data is now deprecated for the following pages:

- Self-Service Search
- Custom Risk Indicator

However, static suggestions for dimensions such as **Event-Type** and **Clipboard-Operations** are still available in the search box.

For more information, see How to use self-service search.

March 21, 2023

Recommendations panel to help onboard on-premise StoreFront™ data source

A new **Recommendations** panel has been introduced on the **Data Sources** page. The **Recommendations** panel on the **Data Sources** page educates the user on the importance of onboarding on-premise StoreFront data sources. It helps the user onboard the on-premise

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

StoreFront data sources easily and also provides an option for the user to review and ensure onboarding of all the available data sources.

For more details, see Connect to a StoreFront Deployment.

February 23, 2023

Fixed issues

The actions are failing for the On-premises Citrix Apps and Desktop deployments where the Citrix Apps and Desktop version > 1912. This issue has been seen in both the manual and policy-based actions. This issue is fixed now.

The Self-service search for Apps and Desktops page displays multiple app start and app end events when virtual apps are launched only once. This issue occurs on Citrix Workspace app for Linux client versions. This issue is fixed now.

User events from the Secure Private Access service after 4th April 2022 and up to end of May 2022 might not be available in your Citrix Analytics tenants. This issue is fixed now.

February 22, 2023

Enhancement in weekly email notifications

Citrix Analytics sends weekly email notifications that help summarize your organization's security risk exposures. The weekly emails notification has been improved with the following updates:

- Provides a view of the users risk distribution - total discovered users, number of risky, and non-risky users for a week
- Total events processed for a week
- Total indicators triggered for a week
- Total actions performed for a week
- Total data sources that are turned on for data processing

For more details, see Weekly email notification.

Added Download File Format field for App.SaaS.File.Download event type

In the Self-Service Search page for the Apps and Desktops data source, a new **Download File Format** field has been added for the App.SaaS.File.Download event type. With this change, you

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

can now configure custom risk indicators for the **Download File Format** field and also export the field as part of the Export to CSV format.

For more information, see Self-service search for Apps and Desktops.

Change in Browser-derived fields

Previously, the Self-Service Search page featured the **Browser**, **Browser Major Version** and **Browser Minor Version** fields to represent the browser names and versions. However, to ensure clarity and accuracy, now these three fields are deprecated and replaced with **Browser Name** and **Browser Version** in Self-Service Search, Custom indicator template and CSV download for Apps and Desktops data source.

For more information, see Self-service search for Apps and Desktops.

February 16, 2023

Fixed issue

Weekly emails are affected for some of the EU and APS customers while fetching the Username Masking status for a tenant. As a result, the administrators are receiving 10 identical weekly emails because of the exception. Once the exception occurred, succeeding tenants did not receive the weekly email. This issue has been fixed now.

February 03, 2023

Analytics support for the Citrix Secure Private Access™ service available in the European Union and the Asia Pacific South regions

Citrix Analytics for Security now processes user events from Citrix Secure Private Access available in the European Union region and the Asia Pacific South region. If your organization is onboarded to Citrix Cloud from the European Union region or the Asia Pacific South region, you can view the risk insights of the users who are using the Secure Private Access service.

For more information, see Data Sources.

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

January 11, 2023

Removal of the Web filtering capability from Secure Private Access

The Web filtering capability has been removed from the Secure Private Access category. The following capabilities on Citrix Analytics for Security are impacted due to the deprecation of Category-based web filtering by Secure Private Access:

1. Data fields such as Category-Group, Category, and Reputation of URLs are no longer available on the Citrix Analytics for Security dashboard.
2. The Risky website access indicator which relies on the same data is also deprecated and is not triggered for customers.
3. Any existing custom risk indicators using the data fields (Category-Group, Category, and Reputation of URLs) and its associated policies are not triggered anymore.
4. The **User Access** and **App Access** tabs.
5. The SIEM exports continue to have the urlcategory, urlcategorygroup and urlcategoryreputation attributes for some time with the following dummy values:
    - 99999 for Category and Category-Group
    - 0 for Reputation

For more information, see Self-service search for Secure Private Access.

December 27, 2022

Change in data source drop-down for Self-service Search

The data source list is changed to reflect **Sessions** by default instead of **Apps and Desktops** in the Self-service Search page. Also, the Performance section is moved to the top followed by the Security section as the performance data sources were not visible.

For more information, see Self-service search.

December 13, 2022

Users dashboard enhancement

The Users dashboard is revamped with summaries and charts to help admins monitor the security posture of the organization. The view not only provides details of discovered users, risk indicators

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

triggered, and actions applied, but also provides time-based trend line of critical metrics for better assessment of risks. Administrators can drill down on data of interest and navigate to relevant dashboards with the right context for faster risk analysis.

For more information, see Users dashboard.

December 05, 2022

Access assurance dashboard - Logon Network

The Logon Network section is newly added and provides the following user details:

- The organizations associated with the IP addresses from which the users have logged on.
- The total unique public subnet and private subnet from where the users have logged on.
- The details that the user has logged on using proxies and private VPN services.

Using these additional details, an administrator can validate the user logon details and ensure that the user logon is within the security expectation of the organization.

For more details, see Access Assurance Dashboard.

November 18, 2022

Fixed issue

- The geofence indicators which were erroneously triggered without having any source events have been fixed.

November 08, 2022

Rename actions

Some of the actions used in Citrix Analytics for Security are renamed to provide more clarity. Those actions are:

- **Notify admins** - Notify administrator(s)
- **Lock user** - Lock user account
- **Log off user** - Log off active sessions
- **Unlock user** - Unlock user account

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

- **Disable user** - Disable User Account

For more information, see What are the actions?

Fixed issues

- If you select an option from the timeline actions dropdown, you cannot trigger any manual action as the Clear and Apply buttons are not visible. This condition occurs in the latest Firefox version. This issue is fixed now.
- The **HardDrive**, **harddrive**, and **HDD** categories are combined into a single category as **Hard Disk Drive** for the Download-Device-Type field in Self-Service Search for the Apps and Desktops data source.
- Sometimes, duplicated notifications are received from Microsoft Graph with the same alert ID, and that causes the creation of duplicated risk events. A deduplication mechanism is implemented within the applications to prevent this issue.

October 19, 2022

Date Source events selection and export

You can now leverage the new Data events export workflow to export data source events in addition to the machine-learning generated risk insights events and associated data.

This enables Security and Security operations (SOC) admins to:

- Correlate data from Citrix Analytics with other data source events aggregated on security information and event management (SIEMs)
- Control what data events flow to SIEMs for storage cost optimization

The data events are delivered to your existing SIEM integrations and data connectors and in parity to what is available on our Self-service event search view.

For more information, see Data events exported from Citrix Analytics for Security to your SIEM service.

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

October 18, 2022

Allow administrator to run dynamic session recording action on Citrix DaaS™ sites

Administrators can now run dynamic session recording actions on Citrix DaaS sites and dynamically record users' virtual sessions. They can configure the action with a policy to automatically start recording user sessions in case of a risky activity by a given user gets detected by Citrix Analytics for Security.

For more information, see What are the actions?

October 14, 2022

Provide feedback for User Risk indicators

Citrix Analytics for Security administrators can now report user risk indicators as helpful or not helpful by providing feedback on the indicators details panel. This feature enables administrators to report false positives, reduce noise for frequently triggered indicators, and share additional context with other administrators. As an additional outcome, the unhelpful risk indicator is hidden from the user’s timeline, and the user risk score is recalibrated.

For more information, see Provide feedback for User Risk indicators.

September 26, 2022

Access assurance to support geofence block list

The **Safe** and **Risky location** tabs are added under the Geofence settings.

- Safe location geofencing helps to identify and restrict access outside of a defined geofenced area.
- Risky location geofencing helps to detect and narrow down risky user access as per the organization’s known behavior.

Both Safe and Risky geofencings are backed by their own pre-configured custom risk indicators.

For more information, see Enable geofencing.

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

Fixed issues

- Citrix Cloud API to display the **Customer Name** in the email body. Now, the email uses the nickname to display the **Customer Name** in the email body sent to the admins.
- Citrix Gateway data source card is common among **Citrix Analytics for Security** and **Citrix Analytics for Performance™**. The data processing was constantly invoking Citrix Analytics for Security endpoint and was broken for customers having only **Citrix Analytics for Performance** entitlement.
- When more than one entitlement messages are received simultaneously from Citrix Cloud, there is a race condition that arises while updating the Redis Cache. In such scenario, one entitlement message is updated to the cache and remaining go missing. This issue is now fixed to update all the Entitlement messages in the cache.

September 13, 2022

Sharelink dashboard enhancement

The Sharelink dashboard is revamped with a summary and detailed view. The summary view consists of the top active shares and top risky shares. The detailed view provides more information to the admin with the introduction of attributes created by, activity count, authentication type, permission, share type, and content. The Admin can drill down and filter further as needed and change/provide the time frame to see the data of interest.

For more information, see Share Links dashboard.

September 09, 2022

Impossible Travel RI Enhancement

The Impossible Travel risk indicators have been enhanced to report the registering organization and routing type of client IP addresses. These new fields are available both in the user timeline indicator detail views and in indicator details sent to SIEM.

For more information on the default policies, see the following articles:

- Continuous risk assessment.
- Policies and actions

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

August 19, 2022

Enable VDA Print telemetry

An event called VDA.Print triggers when a printing job is initiated in Citrix Apps and Desktops. The VDA Print events are also available on **Self-service search** and **Custom Risk Indicators** pages.

- **Self-service search**: You can view the VDA.Print results along with all its attribute details.
- **Custom Risk Indicators**: New events are provided for VDA print telemetry via EventHub and are available within Custom Indicator as well. You can use these event key/value pairs to configure custom indicator triggers.

To enable the print telemetry and transmission of printing logs to Citrix Analytics for Security, you need to create registry keys and configure your VDA. These printing logs provide vital information about printing activities such as, printer names, print file names, and total printed copies. As a security administrator, you can use these logs to analyze the risk and investigate your users.

For more information, see Enabling print telemetry for Citrix DaaS.

August 18, 2022

Fixed issue

- In the Self-Service search for Apps and Desktops and in User Logons page under the Access assurance location dashboard, the Workspace app version value was populated as **NA** (not available) in the downloaded CSV file, while it was available in the page view. This issue is now fixed.

August 17, 2022

Customization of end-user email per policy

You can now customize the content of the email sent to end-users per policy. Specifically, when you create a policy with the Request End User Response action or a disruptive action on the user's account (such as Log Off user and Lock user), the email content sent to end-users when the policy is applied is customizable.

For more information on customizing the end-user mail per policy, see Policies and Actions.

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

August 11, 2022

New questions about **Access assurance – Geolocation** have been added under the **FAQ** article. For more details, refer FAQ.

Fixed issue

- The **View All Notifications** button redirected the administrator to `https://citrix.cloud.com/notifications` weekly email link that had a typo.

June 17, 2022

Data Processing is enabled by default for new paid entitlements

Previously, customers with new paid entitlement to Citrix Analytics for Security had to turn on Data Processing in the site card of specific data sources to begin processing data for those data sources.

With this release, when the new paid entitlement to Citrix Analytics for Security is provisioned, data processing is turned on by default for the following Citrix Cloud services:

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

For more information, see Getting started.

June 09, 2022

Fixed issue

- Microsoft Graph risk indicators generated by Azure AD identity protection and Microsoft Defender for Endpoint may be displayed multiple times in Security Analytics. This issue is now fixed.

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

June 02, 2022

Fixed issues

- In the Self-service search for Policies, when selecting **Policy-Name** dimension in your search query to filter events, a list of non-valid policies was suggested along with the valid policies for Security Analytics.
- The download file size of **File.Download** events from Windows Citrix Receiver was shown incorrectly in Self-service search. This issue surfaced because the actual value was in KBs and the UI treated the value as bytes leading to incorrect values being displayed to the users.

May 24, 2022

Introducing Impossible travel risk indicators for Content Collaboration, Citrix DaaS and Citrix Virtual Apps and Desktops, and Gateway data sources

If the user logs on from two locations that are too far apart to travel within the elapsed time, Citrix Analytics detects this activity as an impossible travel scenario and triggers the **Impossible travel** risk indicator. For more information about the Impossible travel risk indicators, see the following articles:

- Citrix Content Collaboration risk indicators
- Citrix Gateway risk indicators
- Citrix Virtual Apps and Desktops and Citrix DaaS risk indicators

May 17, 2022

Virtual Apps and Desktops is renamed to Apps and Desktops

On the Security Analytics dashboards and reports and in the data sent by Security Analytics to your SIEM service, all the Virtual Apps and Desktops labels are now updated as Apps and Desktops to align with the rebranded product name.

For example, on the Data Sources page, the Virtual Apps and Desktops labels are renamed as Apps and Desktops.

The Apps and Desktops label represents both Citrix on-premises Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) in your organization.

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

Fixed issues

Citrix Analytics does not automatically discover the Citrix DaaS Cloud Monitor or Director sites that are associated with your Citrix Cloud account.

April 05, 2022

What's new

Secure Workspace Access is renamed to Secure Private Access

On the Analytics dashboards and reports, all the **Secure Workspace Access** labels are now updated as **Secure Private Access** to align with the rebranded product name.

For example, on the **Data Sources** page and the **Self-service search page**, the **Secure Workspace Access** labels are renamed as **Secure Private Access**.

March 21, 2022

Fixed issue

- In the **Create Risk Indicator** page, auto-suggestions for dimensions and operators do not work if the previous condition of your search query contains a dimension value that is separated by a space.

  For example, in the following query, auto-suggestions stop working after you select the city as `San Jose`. This issue is now fixed.



March 10, 2022

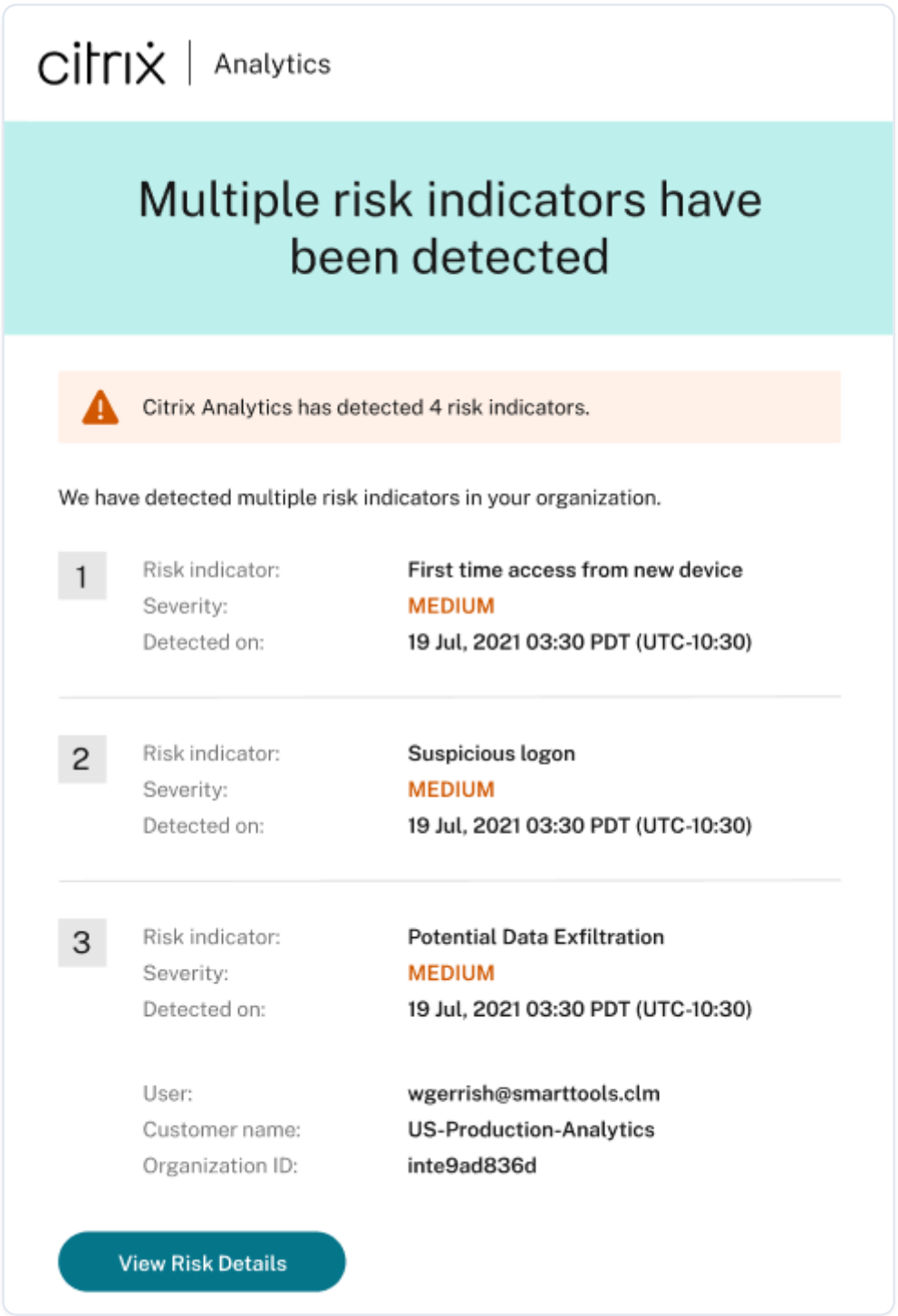
What's new

Notify administrator email enhancements

- The email notification for the **Notify administrator(s)** action now provides the details of the multiple risk indicators associated with a triggered policy.

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

- You can view the name, severity level, and the trigger date of each risk indicator associated with the policy.
- Click **View Risk Details** to open the user timeline page in Citrix Analytics and view the latest risk indicator that triggered the policy. On the user timeline page, you can also view all the risk indicators triggered for the user.



For more information about the **Notify administrator(s)** action, see Policies and actions.

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

Fixed issue

Citrix Analytics fails to receive user events from the Secure Workspace Access data source. Therefore, you don't see the user events in the corresponding self-service search page. Also, you can't create custom risk indicators for the Secure Workspace Access data source.

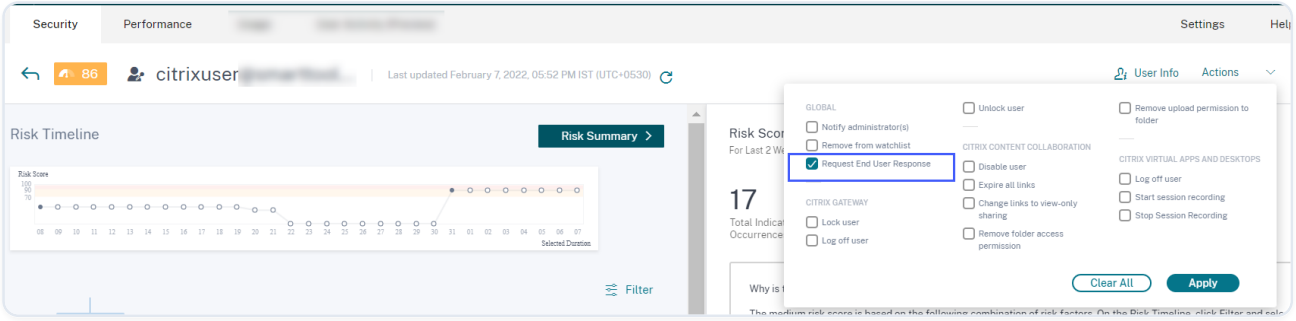
March 03, 2022

What's new

Apply request end user response manually

Previously you can apply the **Request End User Response** action on a user account only by creating a policy. With this release, you can select the action from the **Actions** list on the user timeline and manually apply this action on a risk indicator.

For more information about the action and how to apply actions manually, see Policies and actions.

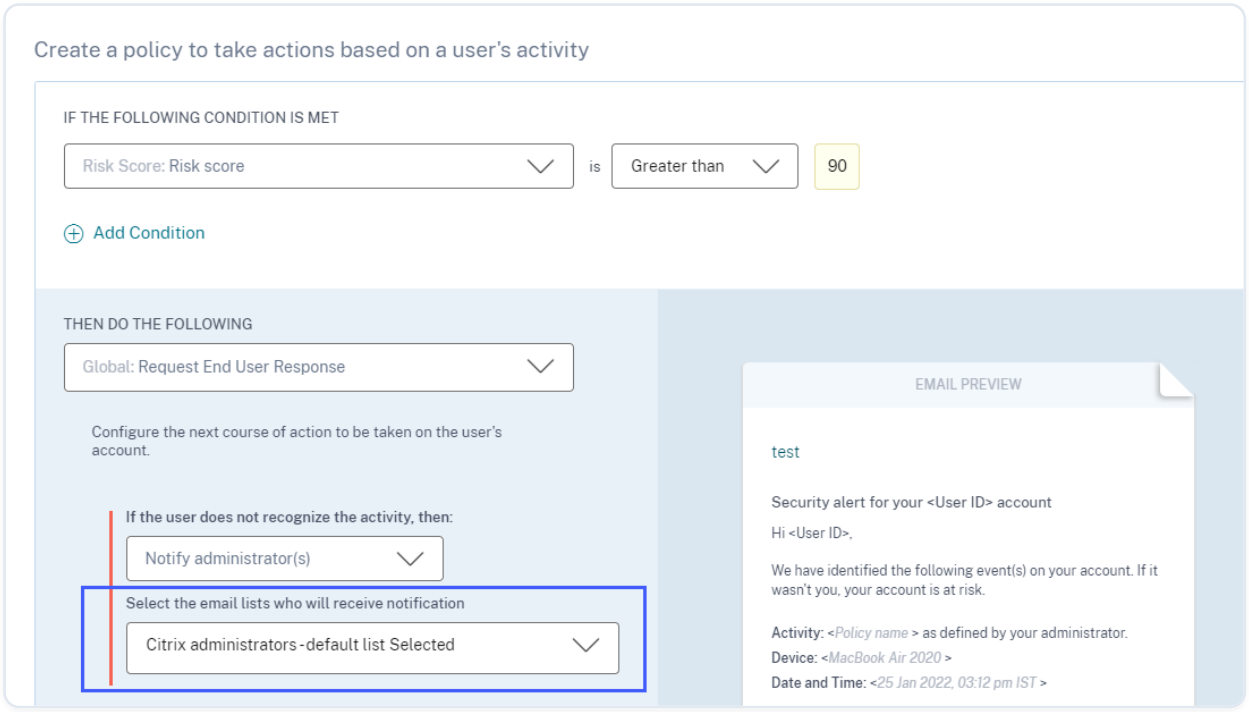


Request end user response enhancements for policy

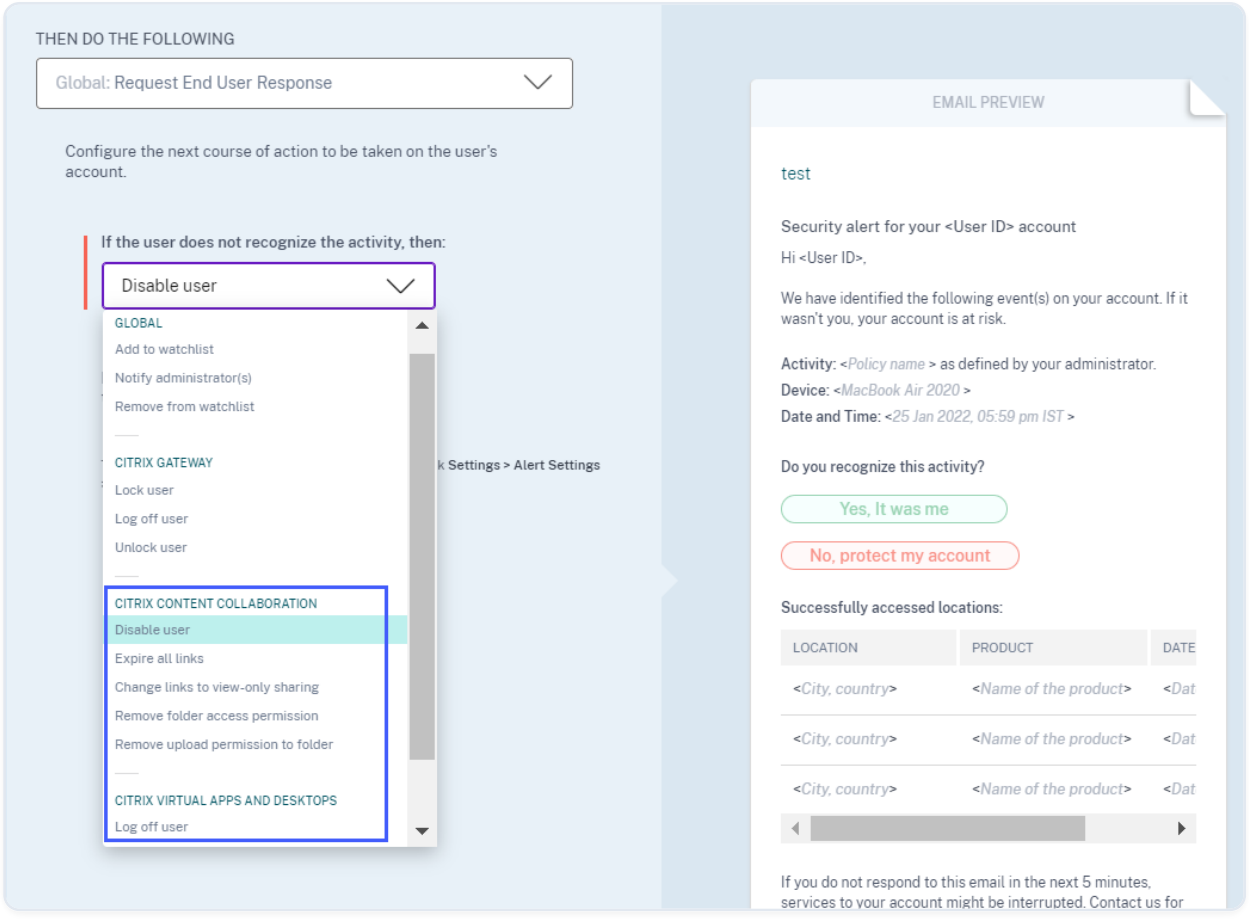
When you create a policy with the **Request End User Response** action, you see the following enhancements:

- After selecting **Notify administrator(s)** as the next action, you can now view the default and the created email distribution lists that you can choose from.

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



- You can now select one of the actions from Citrix Content Collaboration or {{page.cvad-and-daas-product-name}} as the next action. Previously, you can only select one of the Global actions or the Citrix Gateway actions.



For more information about the action, see Policies and actions.

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

February 23, 2022

What's new

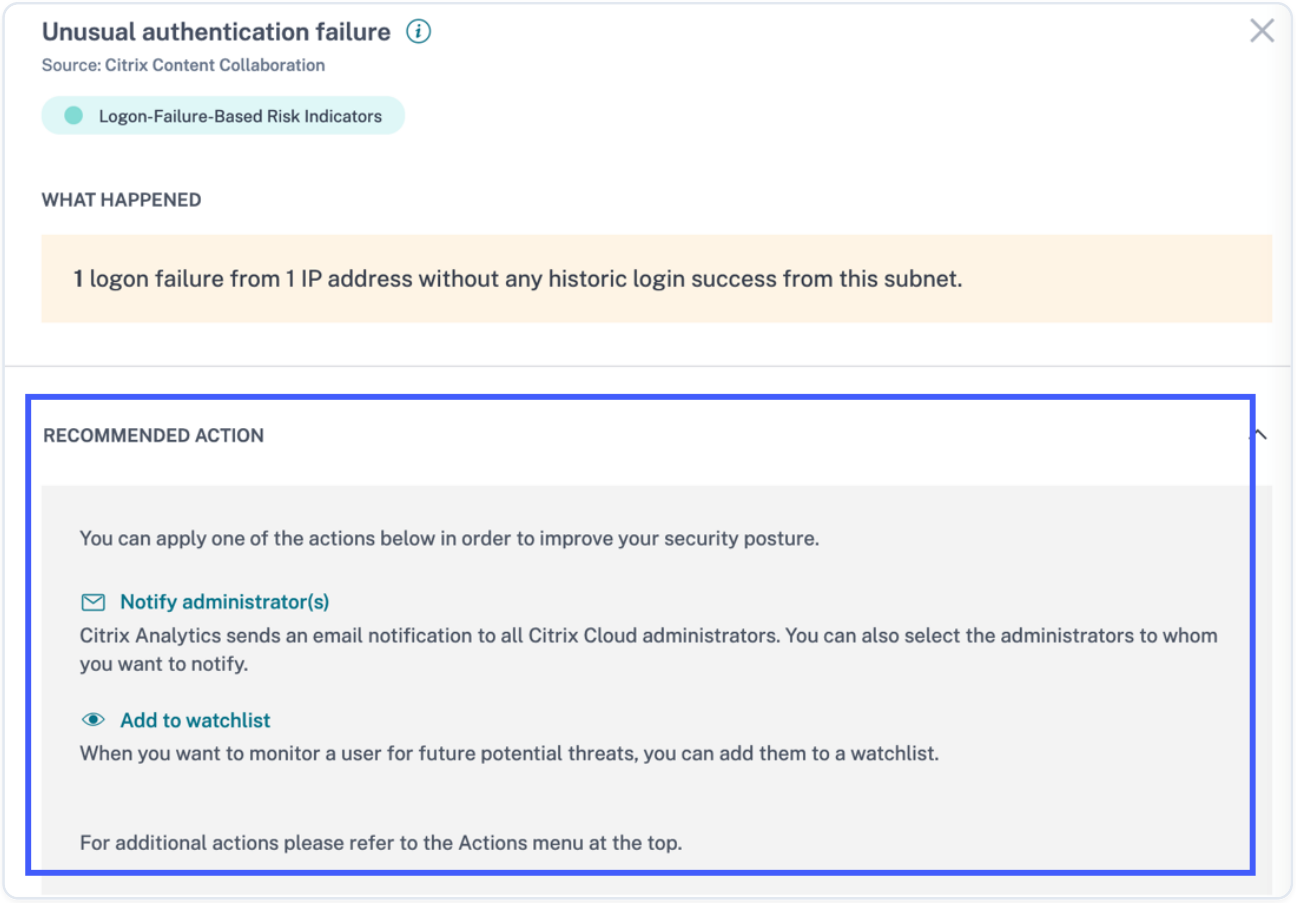
Recommended actions for a risk indicator

Citrix Analytics suggests you to apply actions such as **Notify administrator(s)**, **Add to watchlist**, and **Create a policy** when the following risk indicators are triggered for a user:

- Unusual authentication failure (Content Collaboration data source)
- Unusual authentication failure (Gateway data source)
- Suspicious logon ({{page.cvad-and-daas-product-name}} data source)

When you go to the user timeline and select the risk indicator, you can view all the suggested actions in the **RECOMMENDED ACTION** section.

For example, in the Unusual authentication failure risk indicator, you can view the following recommended actions:



This feature provides guidance to choose an action that you can take depending on the severity of the risk posed by the user. However, you can also take an appropriate action that is outside the recommended list and depending on your risk analysis.

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

Fixed issue

- If your organization is onboarded to Citrix Cloud in the **Asia Pacific South** home region, then Citrix Analytics might not receive user events from the Authentication data source. Therefore, you might not see the user events in the corresponding self-service search page. This issue is fixed.

February 17, 2022

What's new

Improved data collection and reporting for the Citrix Virtual Apps and Desktops and Citrix DaaS data source

With this release, you see the following changes:

- Improvements in data collection, correlation, and reporting of events from Citrix Workspace app clients and Citrix Monitor service.
- Improvements in the quality of events received from users and client versions, which can be used for the self-service search, custom risk indicators, and overall risk detection.

Support for contextual templates for the session events and the app events in Content Collaboration

On the self-service search page, you can now view the details of only the relevant fields associated with the file, folder, session, share, and user events. The non-applicable fields for the events are removed.

For example, you can view the following details of the `File.Copy` events:

- File ID
- File Copy ID
- File Path
- Destination File Path
- Stream ID
- Zone ID

These details help you during the risk investigation and analysis of a user account associated with a risky behavior. You can drill down to the specific attributes of an event that seems to be risky.

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

For more information about the fields, see Self-service search for Content Collaboration.

February 10, 2022

What's new

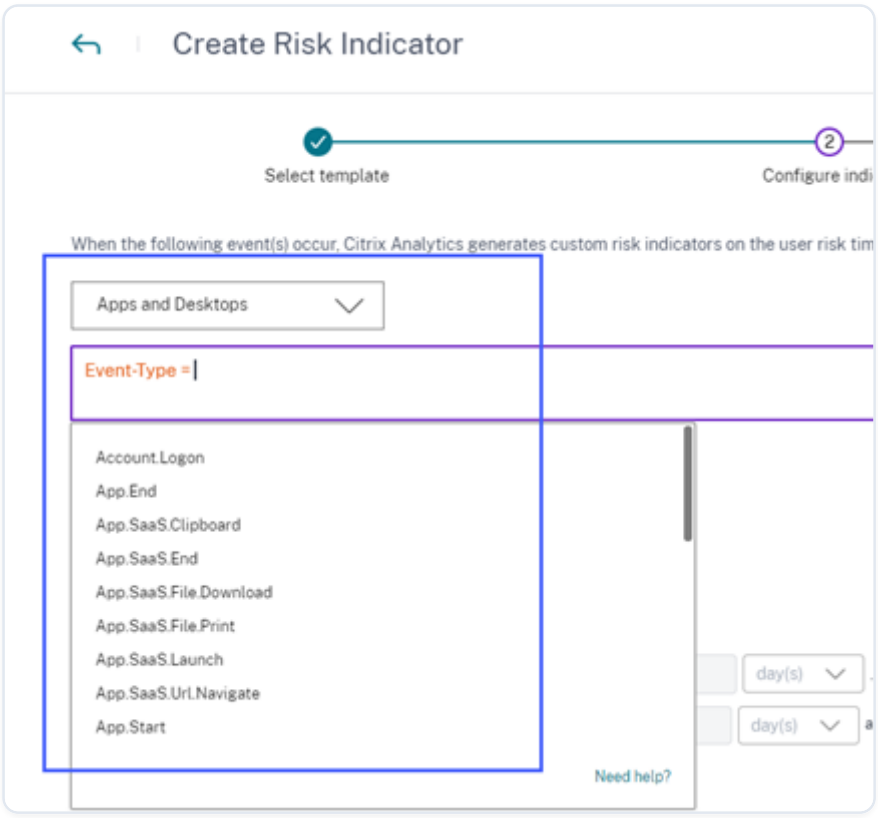
Auto suggested values for the dimensions in the custom risk indicator

In the custom risk indicator page, when you select a dimension and a valid operator in the condition bar, the values for the dimension are shown automatically. Select a value from the auto-suggested list or manually enter a value depending on your use cases. When you type a value, the matching values available in the records are auto-suggested.

The list of values suggested for a dimension is either predefined (known values) in the data base or based on historical events.

For example, when you select the dimension `Event-Type` and the assignment operator, the known values are auto-suggested. You can select a value depending on your requirement.

For more information, see Custom risk indicators.



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

February 09, 2022

What's new

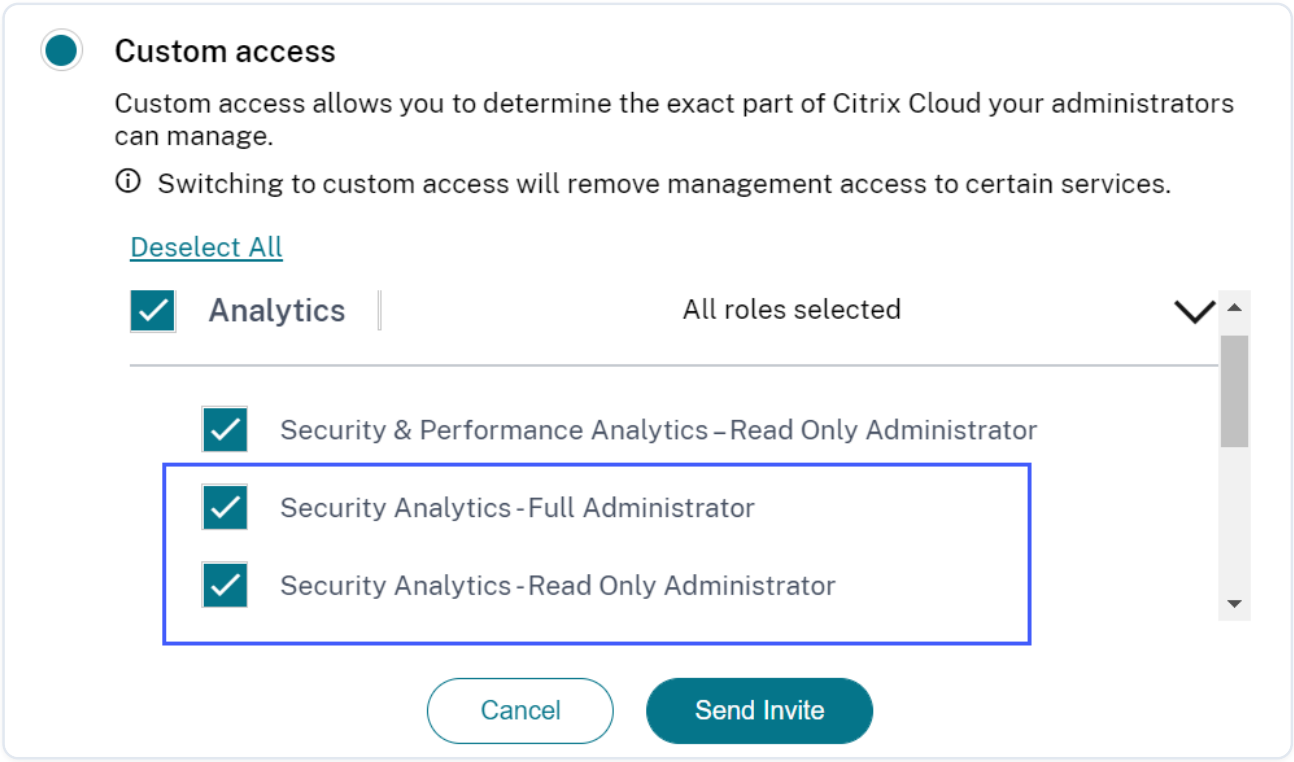
New custom roles for the administrators

As a Citrix Cloud administrator with full access permission, you can invite other administrators to manage Security Analytics in your organization. You can now assign the following custom roles to the invited administrators:

- Security Analytics- Full Administrator
- Security Analytics- Read Only Administrator

Using the custom role, you can provide either read-only or full access permissions to your administrators and allow them to manage the various features of Security Analytics.

For more information about the access permissions for these custom roles, see Manage administrator roles for Security Analytics.



Support for email notifications for custom access administrators

If you are a Citrix Cloud administrator with custom access (read-only or full access) permissions to manage Security Analytics, you now get the following notifications:

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

- Weekly notifications about the security risks detected in your organization. For more information, see Weekly email notification.
- Notifications about the risk indicators when the **Notify administrator(s)** action is applied manually or triggered by a policy. For more information, see Policies and action.

January 28, 2022

What's new

Introducing Suspicious Logon risk indicators for Content Collaboration and Gateway data sources

Citrix Analytics for Security now detects user logons that are suspicious in nature based on multiple contextual factors such as:

- The location is deemed unusual with respect to the user and the organization history
- The device is deemed unusual with respect to the user and the organization history
- The network is deemed unusual with respect to the user and the organization history
- The IP address is deemed suspicious based on the IP threat intelligence feeds

When a user logs on from a suspicious context based on the combination of these factors, the risk indicator is triggered.

This risk indicator replaces the Access from an unusual location risk indicator associated with the Citrix Content Collaboration and Citrix Gateway data sources. Any existing policies that are based on the Access from an unusual location risk indicator are automatically linked to the new risk indicator- Suspicious Logon.

For more information about the risk indicators, see Suspicious logon- Content Collaboration and Suspicious logon- Gateway.

For more information about the schema of the risk indicators, see Citrix Analytics data format for SIEM.

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

January 20, 2022

What's new

Microsoft Azure Active Directory integration

You can now connect your Azure Active Directory with Citrix Analytics for Security to:

- Import the user details and the user groups from your organization's domain to Citrix Analytics for Security.
- Enrich the user profiles with additional details such as job title, organization, office location, email, and contact details, which help you during risk investigation and analysis.

For more information, see Azure Active Directory integration.

January 18, 2022

What's new

Support for the share link actions on all Content Collaboration risk indicators

Previously, you can apply the share link actions- **Expire all links** and **Change link to view-only sharing** on the following share link-based risk indicators associated with the Content Collaboration service:

- Anonymous sensitive share link download
- Excessive share link downloads
- Excessive file sharing

With this release, you can now apply the share link actions on the following user-based risk indicators associated with the Content Collaboration service:

- Access from an unusual location
- Excessive access to sensitive files
- Excessive file uploads
- Excessive file downloads
- Excessive file or folder deletion
- Malware files detected
- Ransomware activity suspected

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

- Unusual authentication failures

You can also apply the share link actions on the custom risk indicators associated with the Content Collaboration service.

For more information about the actions and the risk indicators, see the following articles:

- Policies and actions
- Content Collaboration risk indicators
- Custom risk indicators

Integration with SIEM is now generally available

You can integrate Citrix Analytics for Security with your Security Information and Event Management (SIEM) services and export the users' data from the Citrix IT environment to your SIEM. The integration helps you to correlate the data collected from various sources and get a holistic view of your organization's security.

Currently, you can integrate Citrix Analytics for Security with the following services:

- Splunk
- Microsoft Sentinel
- Elasticsearch
- Other SIEM services by using Kafka or Logstash based data connector

For more information, see Security Information and Event Management (SIEM) integration.

December 23, 2021

What's new

Share link risk indicators enhancements

Following enhancements are made:

- You can now create a policy with the **Anonymous sensitive share link download** risk indicator.
- The **Anonymous sensitive share download** risk indicator is renamed as **Anonymous sensitive share link download** to distinguish it as a share link risk indicator.

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

- The **Excessive downloads** risk indicator is renamed as **Excessive share link downloads** to distinguish it as a share link risk indicator and to differentiate it from the user-based **Excessive file downloads** risk indicator.

For more information, see Citrix share link risk indicators.

December 21, 2021

What's new

Send notifications about risk indicators to your non-Citrix Cloud administrators

You can now notify the non-Citrix Cloud administrators in your organization with the **Notify administrator(s)** action.

To notify these administrators, create an email distribution list. Select the administrators in the email distribution list either from the external domains that are connected to Citrix Cloud or by using their email addresses directly. When applying the **Notify administrator(s)** action, select the email distribution list that contains the non-Citrix Cloud administrators.

For more information, see Email distribution list.

December 20, 2021

What's new

Send user response notifications to your Content Collaboration users

In addition to your Active Directory users, you can now apply the **Request End User Response** action to your Content Collaboration users.

This action sends email notifications to the users when Citrix Analytics detects any unusual activities in their Citrix accounts. For more information about the **Request End User Response** action, see Policies and actions.

Access Control is renamed to Secure Workspace Access

On the **Security** Analytics dashboards and reports, all the **Access Control** labels are now updated as **Secure Workspace Access** to align with the rebranded product name.

For example, on the **Data Sources** page, **Self-service search** page, and **Policies** page, the Access Control labels are renamed as Secure Workspace Access.

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

Fixed issue

- For the Apps and Desktops data source, when you download the search report as a CSV file, some field values in the CSV file are shown as not available (N/A) although their values are available. For example, the values of the fields such as `Download File Name`, `Session Launch Type`, and `Workspace App Version` are shown on the **Self-service search** page, but in the downloaded CSV file, you see these values as not available (N/A). This issue is now fixed.

December 09, 2021

What's new

Create your custom risk indicators easily with templates

You can now select a template based on your use case and create a custom risk indicator. The templates guide you by providing predefined queries and parameters. It eases your effort while creating a custom risk indicator.

For more information, see Custom risk indicators.

December 07, 2021

Fixed issue

- On Citrix Analytics for Security, you don't receive the events of the users who are using the Citrix Secure Browser that was released on September 2021. The issue exists because the **Hostname tracking** policy is not visible in the Citrix Secure Browser post release September 2021 and therefore can't be enabled to integrate with Citrix Analytics for Security. This issue is now fixed.

December 02, 2021

What's new

Malware files detected risk indicator

You can now get an alert when a user uploads an infected file in Content Collaboration.

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

The risk indicator detects a file that is infected by a malware such as trojan, virus, or any other malicious threats. It provides visibility into the details of the malicious file such as the file owner, virus name, and the file location.

The risk factor associated with the **Malware files detected** risk indicator is the File-based risk indicator.

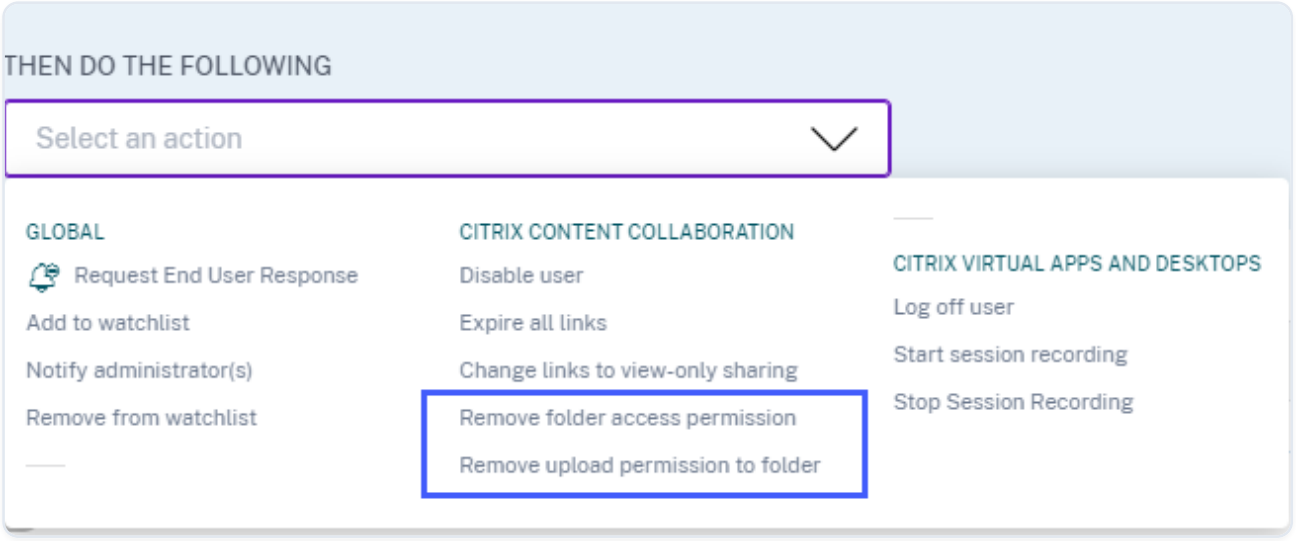
For more information on the risk indicator and the actions that you can apply, see the Malware files detected risk indicator.

New actions for Content Collaboration data source

You can apply the following actions when the **Malware files detected** risk indicator is triggered for a user:

- **Remove folder access permission**. You can block the access permission of the user who uploads the infected file. The user cannot access the folder where the infected file was uploaded.
- **Remove upload permission to folder**. You can block the upload permission of the user who uploads the infected file. The user cannot upload a file to the folder where the infected file was uploaded.

For more information about the actions for Content Collaboration, see Policies and actions.



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

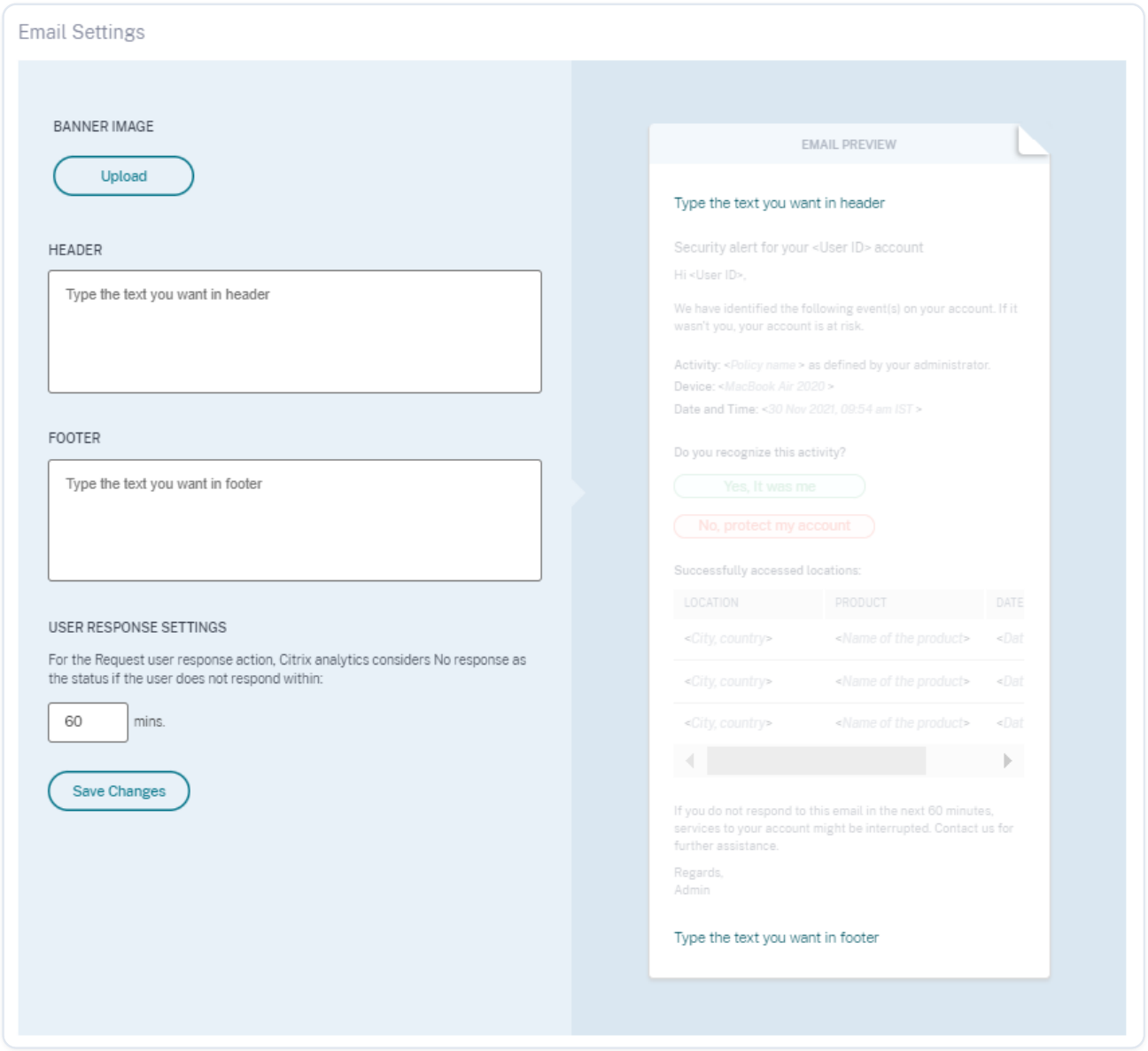
November 29, 2021

What's new

Email settings enhancements for user notifications

As an administrator, you can now add banner image, header, and footer text in the user-response email template. These fields enhance the legitimacy of your email, thus increasing the users' attention and responses towards your email.

For more information, see End user email settings.



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

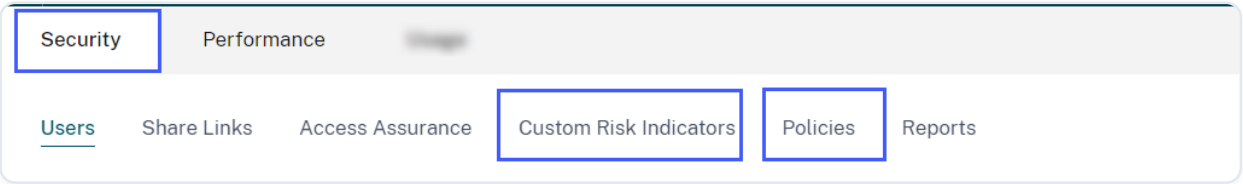
November 26, 2021

What's new

Custom risk indicators and policies menu changes

The navigation links of the following features are updated:

- Custom risk indicators: Use this feature by clicking **Security > Custom Risk Indicators**.
- Policies: Use this feature by clicking **Security > Policies**.



November 25, 2021

What's new

Security Information and Event Management (SIEM) integration enhancements

NOTE

This integration is in preview.

You can now integrate Citrix Analytics for Security with the following SIEM services:

- Microsoft Sentinel
- Elasticsearch with visualization services such as Kibana and SIEM service such as LogRythm
- Any other SIEM services using the Logstash data collection engine

Depending on your business needs, import the users' data from Citrix Analytics for Security to your SIEM service. This integration enables your Security Operations teams to correlate, analyze, and search data from disparate logs within the SIEM services in your organization, helping them to identify and quickly remediate the security risks.

For more information, see Security Information and Event Management (SIEM) integration.

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

November 09, 2021

Fixed issue

- On few tenants, the user policies are not working. This issue occurred when the alerts for the virtual apps have empty string values for the domains. This issue is now fixed.

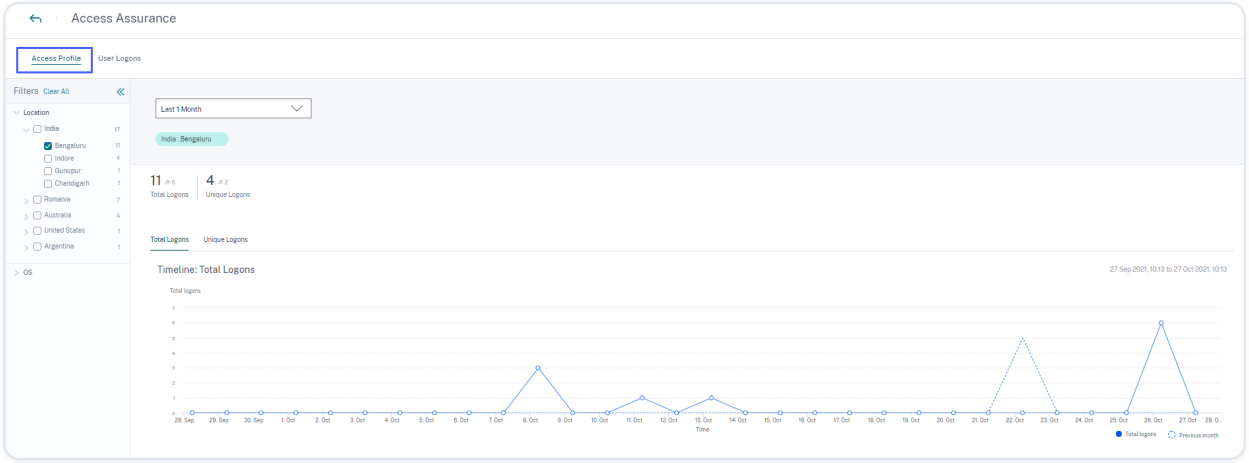
November 02, 2021

What's new

View access profiles and logon details of the Citrix Virtual Apps and Desktops and Citrix DaaS users

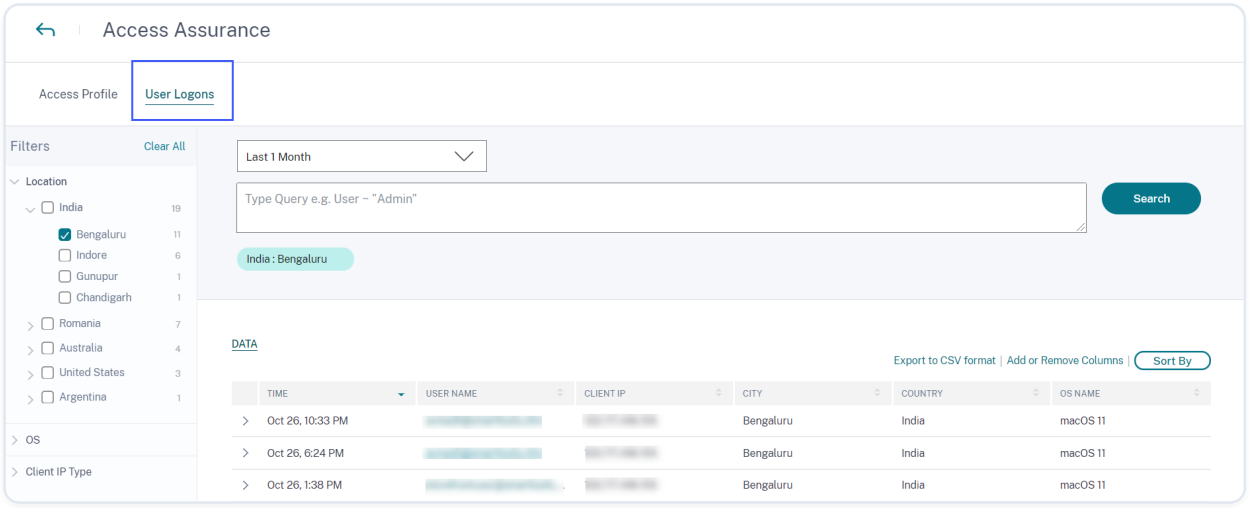
On the **Access Assurance Location** dashboard, you can view the access profiles and the logon details of the users who have logged on to virtual apps and virtual desktops. This information helps you during threat investigation and analysis.

- The **Access Profile** page provides the summary of the user accesses from the selected locations. You can view the trend analysis and top access events of the total users and the unique users logons.



- The **User Logons** page provides the details of the user logons to virtual apps and virtual desktops from the selected locations.

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

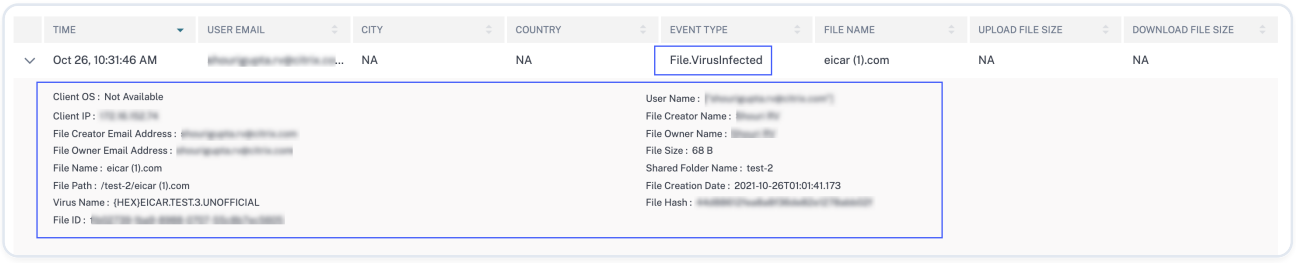


For more information, see the Access Assurance Location dashboard.

View malware logs on the self-service search page for Content Collaboration

On the self-service page for Content Collaboration, you can now view the malware event `File.VirusInfected` and its associated logs. This event is triggered when a Content Collaboration user uploads a file that is infected with a malware.

For more information, see Self-service search for Content Collaboration



Fixed issue

- A few Content Collaboration users are incorrectly set as non-employees while processing the events in Citrix Analytics. Therefore, the users are not identified as Discovered users. This issue is now fixed.

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

October 20, 2021

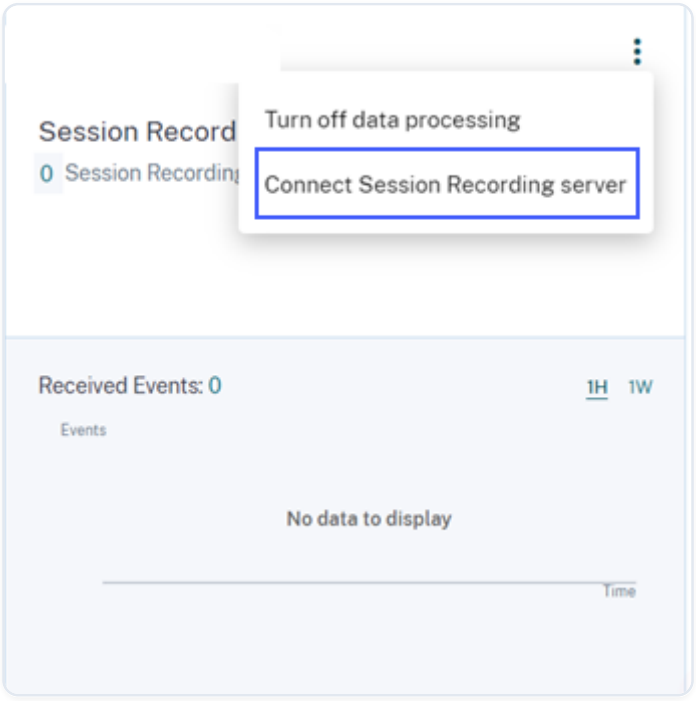
What's new

Session Recording server integration

For your {{page.cvad-and-daas-product-name}} deployment, you can now configure your Session Recording servers to send the user events to Citrix Analytics for Security. These user events are processed to provide actionable insights into users' behavior.

On the **Data Sources > Security** page, go to the **Virtual Apps and Desktops** site card. On the **Session Recording** site card, click vertical ellipsis (⋮) and then select **Connect Session Recording Server**.

For more information, see Connect to Session Recording deployment.



October 19, 2021

What's new

Notify administrator email template enhancements

The email notification that an administrator receives after applying the **Notify administrator(s)** action is enhanced to provide better insights into the user risky events.

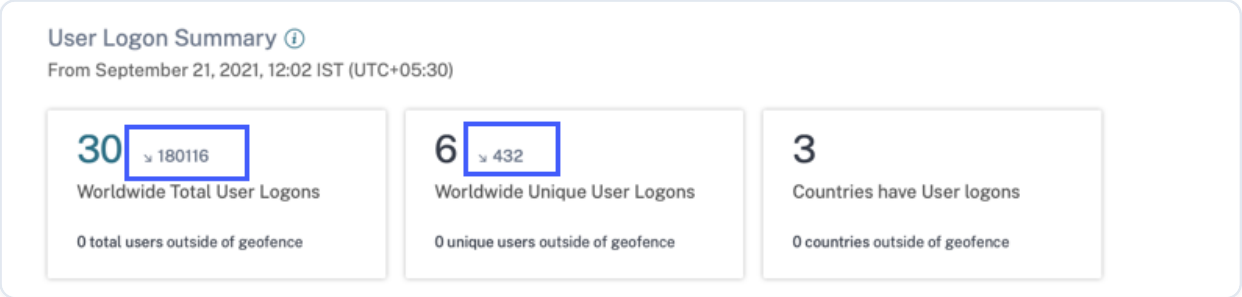
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The notification now provides detailed information about the triggered risk indicator or the applied policy. For example, you can view the severity and triggered time of the default and custom risk indicators. The content structure is improved for better readability.
- The administrators can now access the user timeline directly from the email notification and view details about the risky events.
- A feedback option is added in the notification. This option helps to collect the responses from the administrators and continuously improve the content of the notification based on the responses.

For more information about the **Notify administrator(s)** action, see Policies and actions.

User log on summary enhancements

- You can now view the upward or downward trend of the user logons for the world wide total user logons and world wide unique user logons.



- The **DEVIATION** column on the **Unique Logon Locations** table shows the upward or downward change in the unique user logons for a particular location.

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



These metrics help you to understand how the user logons have changed (positive or negative) from the previous period. It provides visibility into the user interactions with your {{page.cvad-and-daas-product-name}} deployments.

For more information, see Access assurance location dashboard.

Fixed issue

- On the **Access Assurance Location** dashboard, the **User Logon Summary** cards fail to display the user logon metrics (worldwide total user logons, worldwide unique user logons, and countries have user logons) when no users log on from outside the geofence areas. This issue is now fixed.

October 01, 2021

What's new

View audit logs on the self-service search for Content Collaboration

On the self-service search for Content Collaboration, you can now view the audit logs. These logs provide insights into the permissions and the actions applied on the user accounts by the Content Collaboration administrators. Using these data, you can verify if the Content Collaboration

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

administrators have taken valid actions on their user accounts. As a security administrator, it helps you during risk investigation and analysis.

For more information on audit logs, see Self-service search for Content Collaboration.

Fixed issue

The administrators who log on to Citrix Cloud by using Azure AD are unable to access the Citrix Analytics service when the previous expired session ID comes along with the new session ID. This issue is now fixed.

September 29, 2021

What's new

Access assurance location dashboard is now generally available

The dashboard provides visibility into the locations of your {{page.cvad-and-daas-product-name}} users. You can identify the users whose locations are unusual by enabling geofencing and apply appropriate actions to prevent any threats.

To view the dashboard, click **Security > Access Assurance**. Select the time period for which you want to view the location details.

For more information, see Access assurance location dashboard.

September 15, 2021

What's new

Custom risk indicator enhancements

- When a custom risk indicator is triggered, it gets displayed on the user timeline immediately. However, the risk summary and the risk score of the user get updated after a few minutes (approximately 15- 20 minutes).
- If you modify the attributes such as condition, risk category, severity, and name of an existing custom risk indicator, on the user timeline, you can still view the previous occurrences of the custom risk indicator (with the old attributes) that were triggered for the user.
- If you delete a custom risk indicator, on the user timeline, you can still view the previous occurrences of the custom risk indicator that were triggered for the user.

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

For more information, see Custom risk indicators.

September 14, 2021

What's new

Introducing Suspicious Logon risk indicator

Citrix Analytics for Security now detects user logons that are suspicious in nature based on multiple contextual factors such as:

- The location is deemed unusual with respect to the user and the organization history
- The device is deemed unusual with respect to the user and the organization history
- The network is deemed unusual with respect to the user and the organization history
- The IP address is deemed suspicious based on the IP threat intelligence feeds

When a {{page.cvad-and-daas-product-name}} user logs on from a suspicious context based on the combination of these factors, the risk indicator is triggered.

This risk indicator replaces the **Access from an unusual location** risk indicator associated with the Citrix Virtual Apps and Desktops data source. Any existing policies that are based on the **Access from an unusual location** risk indicator are automatically linked to the new risk indicator- **Suspicious Logon**.

For more information about the risk indicator, see Citrix Virtual Apps and Desktops and Citrix DaaS risk indicators.

SIEM messages enhancement

Citrix Analytics for Security now send the schema details of the **Suspicious logon** risk indicator to your SIEM service. You can view the schema of the indicator summary and the event details of the **Suspicious logon** risk indicator. For more information, see Citrix Analytics data format for SIEM.

Fixed issue

- For the Apps and Desktops self-service search, the client IP value is missing in the downloaded CSV file. This issue is now fixed.

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

August 19, 2021

What's new

Introducing Citrix Analytics App for Splunk

NOTE

The app is in preview.

Citrix Analytics App for Splunk enables you to view the data collected from Citrix Analytics for Security in the form of insightful dashboards on your Splunk. The dashboards provide insights into the risky events of your users. You can also correlate the Citrix Analytics data with logs collected from various other data sources. Correlation helps you to find relations between events and take timely actions to protect your IT environment.

To download the app, go to Splunkbase. Install the app on your Splunk search head.

For more information, see Citrix Analytics App for Splunk.

Custom risk indicator schema for SIEM

In your SIEM service, you can now view the schema of the custom risk indicators created for {{page.cvad-and-daas-product-name}}. This data helps you to gain insight into your organization's security risk posture.

For more information about the custom risk indicator schema, see Citrix Analytics data format for SIEM.

Support for Citrix Director as a data source

You can now configure your on-premises sites on the Citrix Director to send events to Security Analytics. These events are used to discover the users connected to Security Analytics and determine the Workspace app versions installed on the users' devices.

By default, the data processing is enabled after the discovery of the sites. On the **Monitoring** card, you can view all the connected sites.

For more information on how to configure your sites on the Director, see Citrix Virtual Apps and Desktops and Citrix DaaS data source.

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

Support for geofence in the Access assurance location dashboard

You can now use the **Geofence Settings** in the dashboard to select and enable the geofenced areas. After enabling the geofence, the map displays the geofenced areas (countries) and the user logons from outside and inside the geofence. This feature uses the **CVAD-Session started outside of geofence** risk indicator to monitor the user logons.

For more information, see Access assurance location dashboard.

Workspace app status on the Users page

On the **Users** page, you can now view the status of the Citrix Workspace app clients that are supported by Citrix Analytics. The page shows the following status:

- Supported
- Partially supported
- Unsupported
- Not Available
- Inactive

The status helps you to identify any unsupported client versions used by the users and recommend the users to upgrade their clients to a supported version. A supported client version sends the user events to Citrix Analytics.

NOTE

To view the Citrix Workspace app status, you must onboard your Citrix Director data source. Otherwise, the status for every {{page.cvad-and-daas-product-name}} user is shown as **Inactive**.

For more information, see the Users dashboard.

Support for the IS EMPTY operator

While creating a custom risk indicator, you can now use the **IS EMPTY** operator in your condition to check for null or empty dimension.

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

NOTE

The operator works for only string-type dimensions such as App-Name, Browser, and Country.

For more information, see Custom risk indicators.

Improved risk scoring

On the user's timeline, you can now view the risk summary of a user. The risk summary provides information about the risk factors associated with user events. The risk factor helps you to identify the type of anomalies in the user events and also determines the risk score. The following are the risk factors:

- Device-based risk indicators
- Location-based risk indicators
- IP-based risk indicators
- Logon-failure-based risk indicators
- Data-based risk indicators
- File-based risk indicators
- Custom risk indicators
- Other risk indicators

On the user's timeline, you can now apply the filter to view the user events based on the risk factors.

For more information, see the following topics:

- Citrix user risk indicators
- User risk timeline and profile

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

July 29, 2021

Deprecated feature

Deprecated actions associated with Citrix Endpoint Management™

The following actions are removed from the Citrix Endpoint Management data source. You can no longer apply these actions on the risk indicators or create policies using these actions.

- Lock device
- Notify Endpoint Management admin
- Notify user
- Revoke device
- Wipe device

In your existing policies, if these actions are already in use, they are automatically replaced by the **Add to watchlist** action. And you can monitor such users from the watchlist.

July 14, 2021

What's new

Support for the IS NOT EMPTY operator

While creating a custom risk indicator, you can now use the **IS NOT EMPTY** operator in your condition to check if the dimension is not empty (not blank).

NOTE

The operator works for only string-type dimensions such as App-Name, Browser, and Country.

For example, the following condition detects user logon events from any country where the country value is not null. In other words, the country name is specified.

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

For more information, see Custom risk indicators.

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

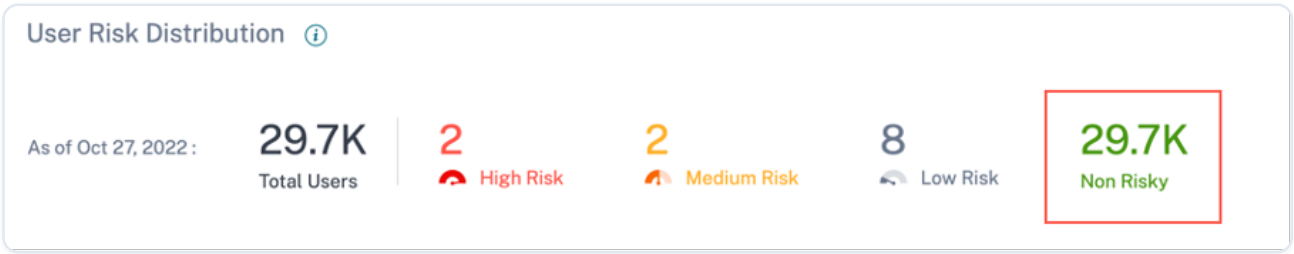
July 06, 2021

What's new

View non-risky users on the Users dashboard

On the **Users** dashboard, you can now view the number of non-risky users for the selected time period. These discovered users are identified as non-risky based on the zero risk score for the selected period. Click the **Non Risky Users** card to view all the users that have zero risk score.

For more information, see Users dashboard.



July 01, 2021

What's new

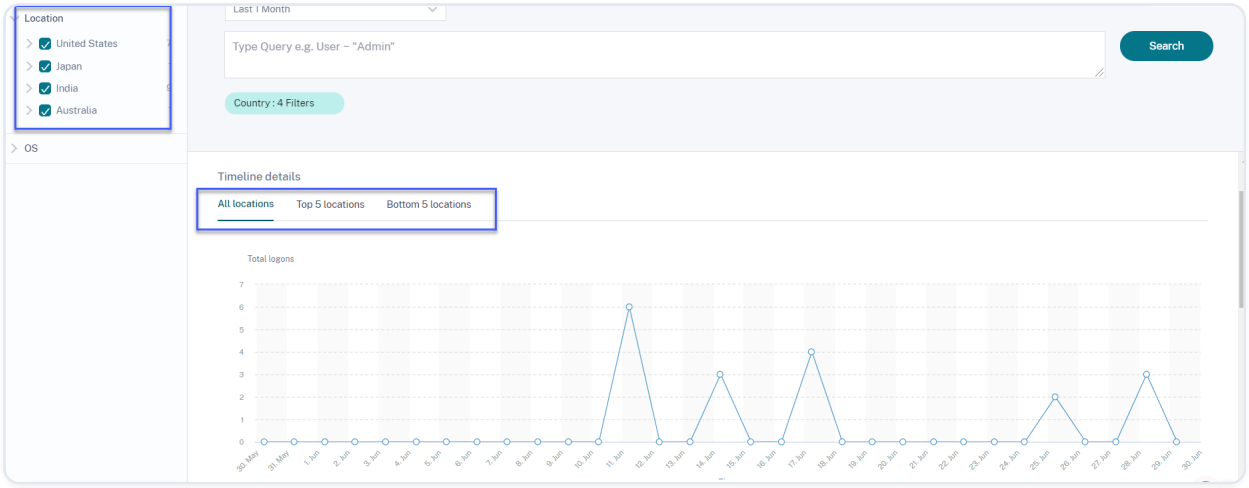
Access assurance location dashboard enhancements

- On the **Top 10 Unique Logon Locations** table, you can view the number of unique user logons from unknown locations. This list is a subset of the top 10 unique logon locations. You can also find the reasons why the locations are unknown and the possible ways to get the users' locations.

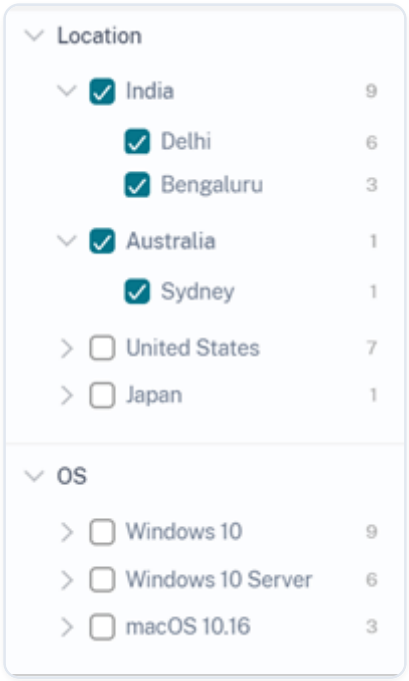


- On the **Access Location** page, if you select multiple locations, you can view and compare the timeline details of user logons from all locations, top five locations, and bottom five locations.

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



- On the **Access Location** page, you can use the nested facets such as country and their cities, operating systems- major and minor versions. These facets enable you to filter the events in a granular way.

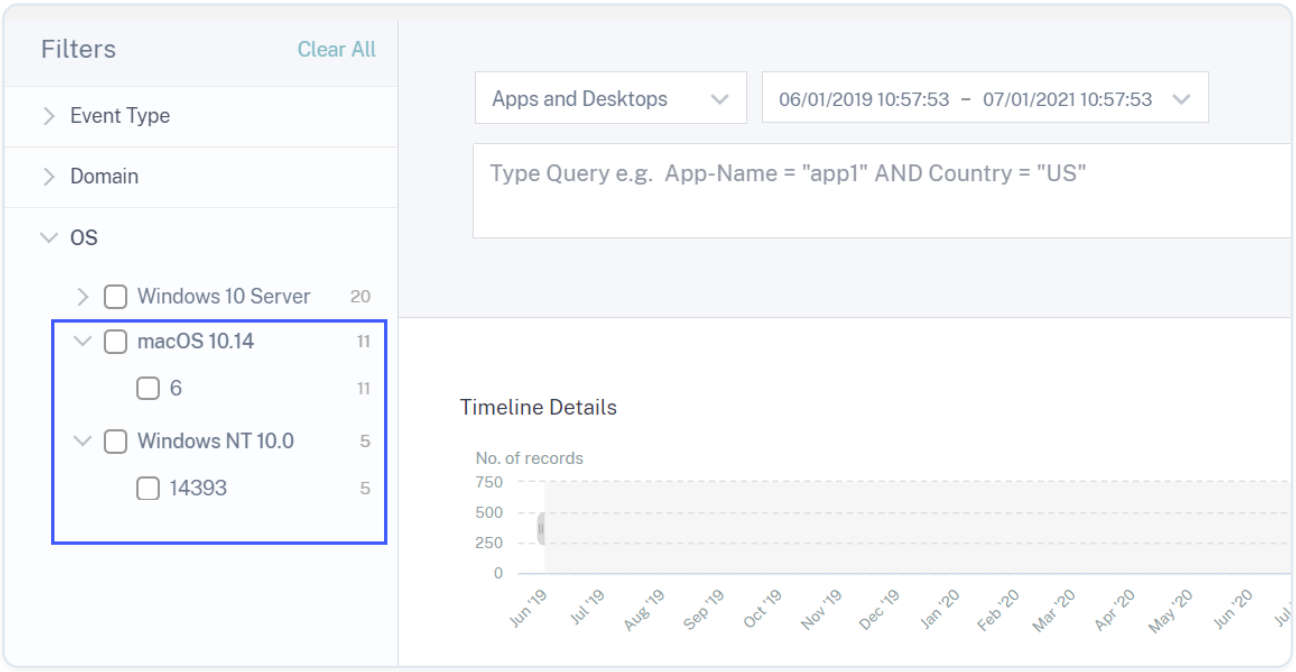


For more information, see Access assurance location.

Updated the OS facet in self-service search for Virtual Apps and Desktops

You can now filter the Apps and Desktops events using the nested OS facet. Select the major version and the minor version associated with an operating system and filter the events in a granular way. For more information, see Self-service search for Apps and Desktops.

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

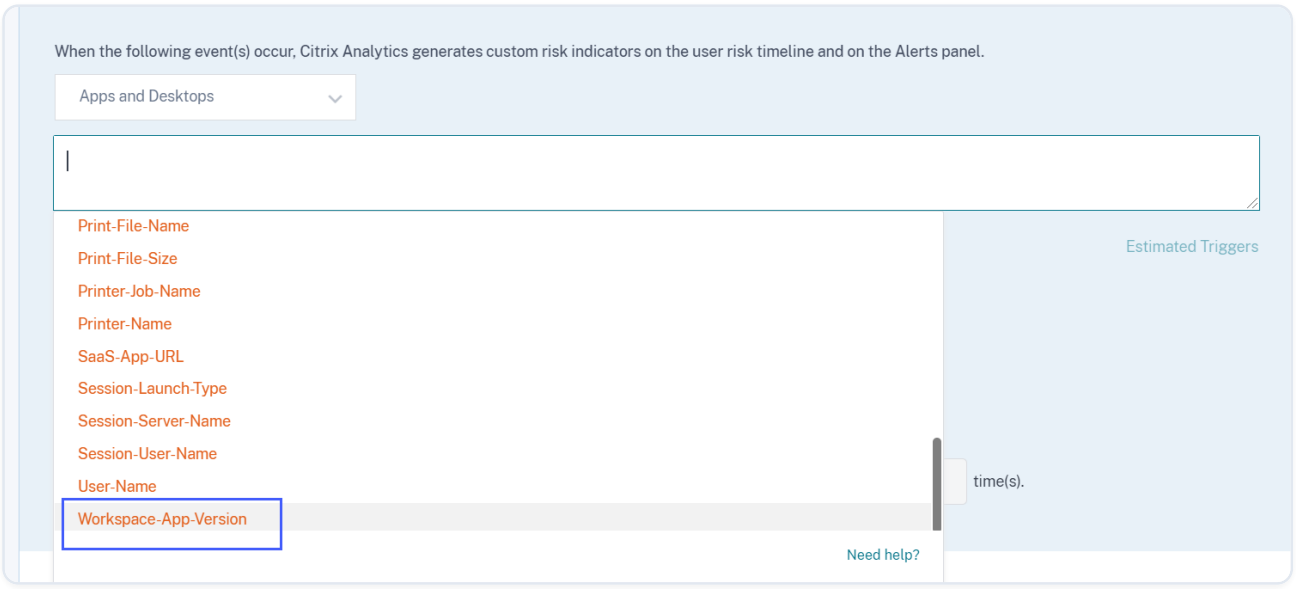


June 30, 2021

What's new

Added Workspace app version in custom risk indicator condition for Apps and Desktops

For the **Apps and Desktops** data source, you can now use the **Workspace-App-Version** dimension to define your condition while creating a custom risk indicator. For more information on the dimension, see Self-service search for Apps and Desktops.



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

June 23, 2021

What's new

SIEM messages enhancements

The following fields are now added to the schema of the risk indicators:

- `indicator_vector_name` - Indicates the risk vector associated with a risk indicator. The risk vectors are Device-based Risk Indicators, Location-based Risk Indicators, Logon-failure-based Risk Indicators, IP-based Risk Indicators, Data-based Risk Indicators, File-based Risk Indicators, and Other Risk Indicators.
- `indicator_vector_id` - The ID associated with a risk vector. ID 1 = Device-based Risk Indicators, ID 2 = Location-based Risk Indicators, ID 3 = Logon-failure-based Risk Indicators, ID 4 = IP-based Risk Indicators, ID 5 = IP-based Risk Indicators, ID 6 = Data-based Risk Indicators, ID 7 = Other Risk Indicators, and ID 999 = Not available.

For more information, see Citrix Analytics data format for SIEM.

June 07, 2021

What's new

Enhancements to the notify administrator(s) action

When you apply the **Notify administrator(s)** action to a risk indicator or create a policy with the action, you can now select the administrators who receive notification about the user's risky behavior. For more information on the action, see Policies and actions.

Added support for the view-only sharing action

If a user shares files excessively, Citrix Analytics triggers the **Excessive file sharing** risk indicator. From the user's risk timeline, you can now apply the **Change links to view-only sharing** action to the **Excessive file sharing** risk indicator. You can also apply the action on a particular share link on the share link risk timeline. This action prevents other users from downloading, copying, or printing the files associated with the share links. For more information about the action, see Policies and actions.

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

May 18, 2021

What's new

Migrating the default risk indicators to custom risk indicators

The following default risk indicators are migrated to preconfigured custom risk indicators.

DEFAULT RISK INDICATOR	DATA SOURCE	PRECONFIGURED CUSTOM RISK INDICATOR
First time access from new device	{{page.cvad-and-daas-product-name}}	CVAD-First time access from new device
First time access from new IP	Citrix Gateway	Gateway-First time access from new IP

With this migration to the custom risk indicators, the default risk indicators and the associated machine learning algorithms are deprecated.

The corresponding custom risk indicators are triggered based on the following preconfigured conditions:

- When a user access from a new device for the first time or an existing device that has not been used for a minimum 90 days.
- When a user signs in from a new IP address for the first time or an existing IP address that has not been used for a minimum 90 days.

Along with the preconfigured conditions, you can now add your own conditions for these custom risk indicators to identify the threats in your Citrix environment. This option gives you flexibility to configure the custom risk indicator based on your security needs. You can also create policies to apply actions on the risky events detected by these custom risk indicators.

However, on the user's time line, you can still view the previously triggered default risk indicators and their events.

The policies associated with these default risk indicators are automatically linked to the corresponding preconfigured custom risk indicators.

For more information, see Preconfigured custom risk indicators and policies.

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

Enhancements in self-service search for Gateway

- The **Event Type** filter is now renamed to **Record Type**. Select one of the following record types to filter your events- VPN_AI, VPN_IF, and, VPN_ST.
- On the **DATA** table, expand a row for a user event to view the corresponding event type. The event types can be one the following- Authentication, ICA® File, or Session Logout.

The following table describes the correlation between the record types and the event types.

RECORD TYPE	EVENT TYPE
VPN_AI	Authentication
VPN_IF	ICA File
VPN_ST	Session Logout

For more information, see Self-service search for Gateway.

Fixed issue

- Custom risk indicator gets triggered based on the case sensitivity of the conditional values. For example, in the user events containing device IDs in the allowed list, you see the following behavior:
  - If you enter the value of the `Device-ID` dimension in the lower case, the custom indicator gets triggered.

    `Event-Type = Session.Logon AND Device-ID NOTIN (“1621d2cb-f598-5ef7-a5bf-81747496ed2e”)`
  - If you enter the value of the `Device-ID` dimension in the upper case for the same device, the custom indicator does not get triggered.

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

  This issue is now fixed and the custom risk indicator gets triggered irrespective of the case-sensitivity of the conditional values.

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

April 29, 2021

What's new

Events details for a custom risk indicator

On the user's risk timeline page, you can now view the events that triggered a custom risk indicator. Previously, you were able to view only the defined conditions, description, and the trigger frequency for a custom risk indicator. Click **Event Search** to view the details of the events associated with the user and the risk indicator. For more information, see Custom risk indicators.

Fixed issue

- An administrator is unable to create custom risk indicators even after their access permission is changed from read-only admin to full admin.

April 16, 2021

What's new

SIEM messages enhancements

You can view the following enhancements on the risk indicator schema format:

- The client IP address is now available in the schema for all the batch risk indicators. Previously the client IP address was available only for a few batch risk indicators:
    - EPA scan failure
    - Excessive authentication failures
    - Logon from suspicious IP
    - Access from an unusual location
    - Unusual authentication failure
    - Anonymous sensitive share download
    - Potential data exfiltration
- If an integer data type field value is unavailable, the value assigned is **-999**. For example, `"latitide" = -999`.
- If a string data type field value is unavailable, the value assigned is **NA**. For example, `"city"= "NA"`.

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

For more information, see Citrix Analytics data format for SIEM.

March 26, 2021

What's new

Restriction on the SIEM messages

Citrix Analytics sends a maximum of 1000 events details for each risk indicator occurrence to your SIEM service. These events are sent in a chronological order of occurrence. For more information, see Citrix Analytics data format for SIEM.

Added the data source ID and the indicator category ID fields in the SIEM messages

Following fields are added in the indicator summary schema and the indicator event details schema.

FIELD	DESCRIPTION
`data_source_id`	The ID associated with a data source. ID 0 = Citrix Content Collaboration, ID1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Virtual Apps and Desktops, ID 4 = Citrix Access Control™
`indicator_category_id`	The ID associated with a risk indicator category. ID 1 = Data exfiltration, ID 2= Insider threats, ID 3 = Compromised users

For more information, see Citrix Analytics data format for SIEM.

March 18, 2021

What's new

Access assurance location dashboard

NOTE

The feature is in preview.

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

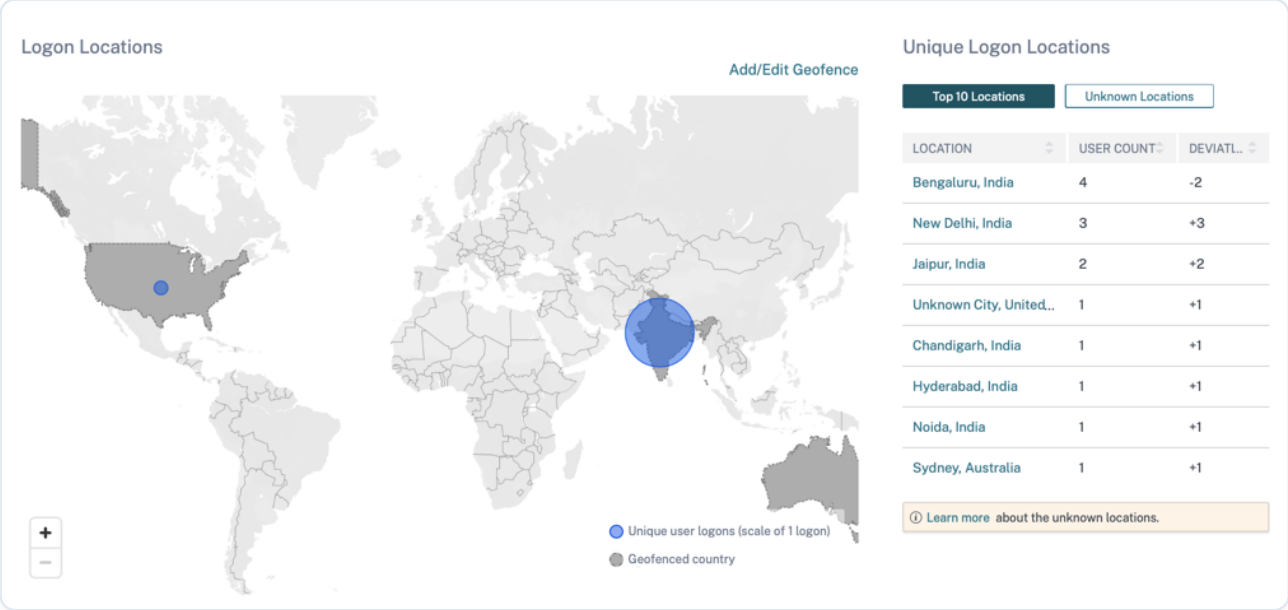
The **Access Assurance Location** dashboard provides an overview of the locations from where the {{page.cvad-and-daas-product-name}} users have logged on for a selected period. Citrix Analytics receives these user logon events from Citrix Workspace app installed on the users' devices.

To view the dashboard, click **Security > Access Assurance**.

You can view the following information for a selected period:

- Total number of user logons from a particular location and across the locations.
- Total number of unique user logons across the locations.
- Total number of countries from where the users have logged on.
- Top 10 locations with unique user logons.

For more information, see Access assurance location.



Support for the NOT LIKE (!~) operator

For the self-service search query and the custom risk indicator condition, you can now use the NOT LIKE (!~) operator. The operator checks for the user events for the matching pattern that you have specified. It returns the events that do not contain the specified pattern anywhere in the event string.

For example, the query `User-Name !~ “John”` displays events for the users except John, John Smith, or any such users that contain the matching name "John".

For more information, see Self-service search.

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

Translated operating system version

For the {{page.cvad-and-daas-product-name}} data source, the **Platform** dimension is now translated as the **OS-Major-Version**, **OS-Minor-Version**, and **OS-Extra-Details** dimensions. Based on the operating system details of a user, Citrix Analytics displays these dimensions on the self-service search page.

You can use these dimensions to define your conditions for a custom risk indicator.

For the previously created custom risk indicators, if you have used the **Platform** dimension as a condition, Citrix Analytics automatically replaces the **Platform** dimension with the **OS-Major-Version**, **OS-Minor-Version**, and **OS-Extra-Details**. This update does not affect the integrity of your defined condition.

For more information on the new dimensions, see Self-service search for Virtual Apps and Desktops.

Updated the data fields for Apps and Desktops

On the Self-service search for Apps and Desktops, view the updated data fields based on the contextual template.

For more information, see Self-service search for Apps and Desktops.

Deprecated feature

Removed the VPN_AF and VPN_SU events from the self-service search page

On the self-service search page for the Citrix Gateway data source, the following record types are now removed.

RECORD TYPE	RECORD NAME
VPN_SU	Session Update record
VPN_AF	Application Launch Failure record

So, you cannot filter and view your events based on these record types. Any custom risk indicators based on these record types stop functioning.

For more information, see Self-service search for Gateway.

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

March 11, 2021

What's new

Current timestamp for the user risk score schema

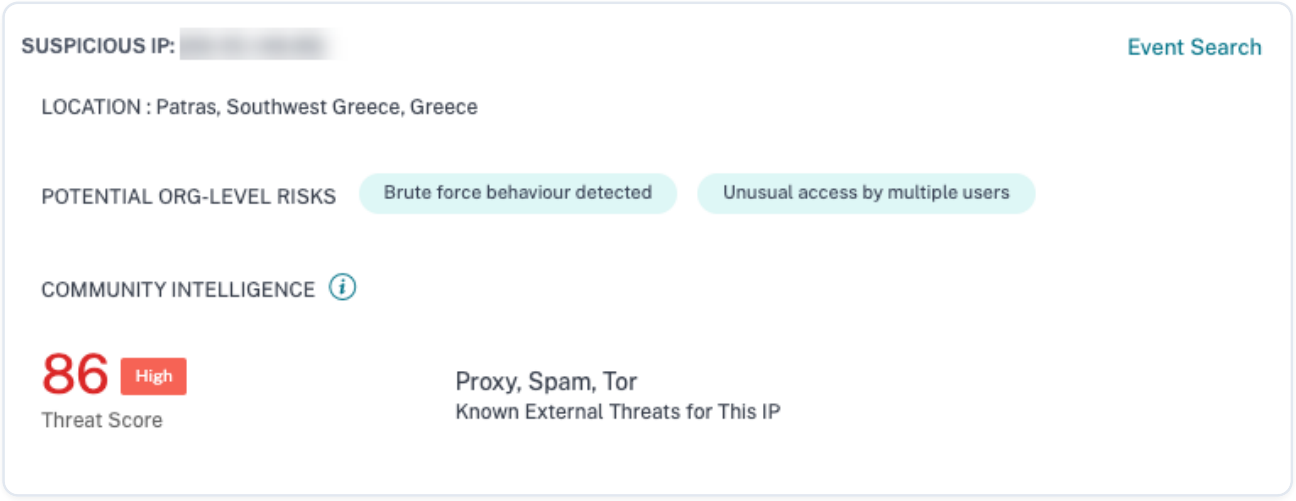
A new field `last_update_timestamp` is added in the user risk score schema format. This field indicates the time when the risk score was last updated. For more information on the schema format, see User risk score schema.

March 03, 2021

What's new

Enhancements to the Logon from suspicious IP risk indicator

On the user's risk timeline page, a new section **Suspicious IP** is displayed for the **Logon from suspicious IP** risk indicator. This section provides the following information:



- The IP address from which suspicious sign-in activity is detected.
- The location of the user.
- Any patterns of suspicious IP activity that Citrix Analytics has recently detected in your organization.
- Community-level intelligence feed about the IP address.

For more information, see the Logon from suspicious IP risk indicator.

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

Enhancements to Access from an unusual location risk indicator

- In the Access from an unusual location risk indicator for Citrix Content Collaboration, added the **TOOL NAME** column in the event table. Removed the **DEVICE BROWSER** column from the event table. For more information, see Citrix Content Collaboration risk indicators.
- In the Access from an unusual location risk indicator for {{page.cvad-and-daas-product-name}}, added the **DEVICE ID** and the **RECEIVER TYPE** columns in the event table. For more information, see Citrix Virtual Apps and Desktops risk indicators.

Citrix Analytics data format for SIEM

The article describes the schema of the processed data generated by Citrix Analytics for your SIEM service.

Fixed issue

- For a Content Collaboration user, if the `Is Employee` value is null, then the user is not displayed on the discovered users list.

February 18, 2021

What's new

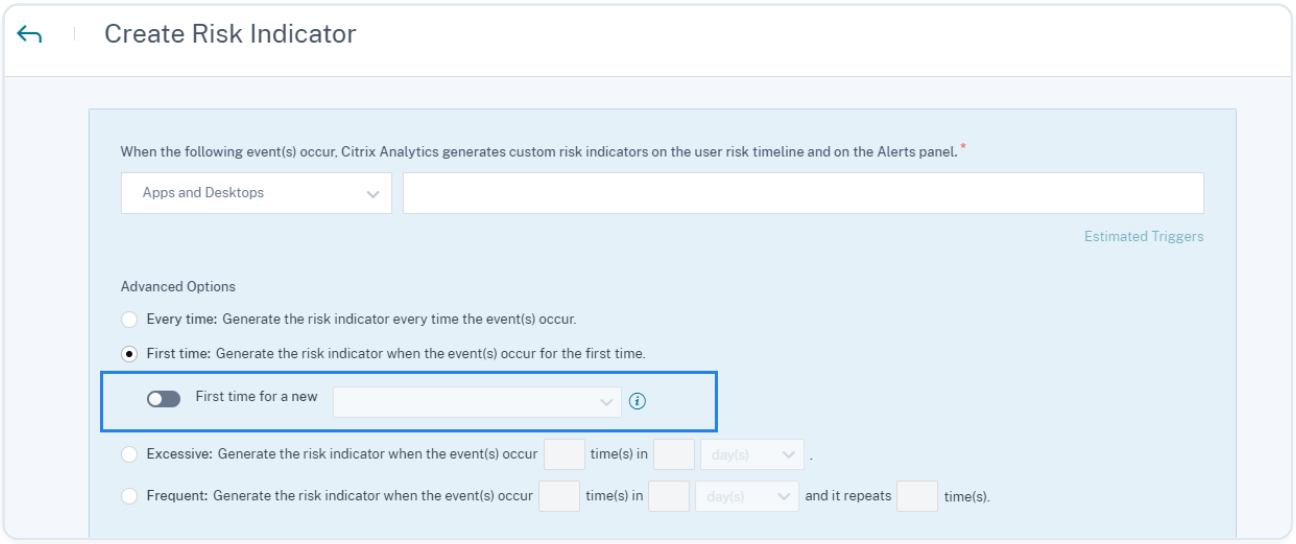
Support for the first time access from a new entity in the custom risk indicator

You can now create a risk indicator that triggers when Citrix Analytics receives events from a new entity for the first time. Some examples of entities are Client IP, City, and Country.

On the **Create Indicator** page, click the **First time** option. Enable the **First time for a new** button, and select a valid entity from the list based on the data source. You need not assign any specific value to the entity. For example, if you select **City** from the list, Citrix Analytics triggers a risk indicator whenever users sign in from a new city for the first time.

For more information, see Creating a custom risk indicator.

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



Maximum limit for creating custom risk indicator

You can now create custom risk indicators up to a maximum limit of 50. If you reach this maximum limit, you must either delete or edit any existing custom risk indicator to create a custom risk indicator.

For more information, see Custom risk indicators.

User location data from Citrix Virtual Apps and Desktops and Citrix DaaS

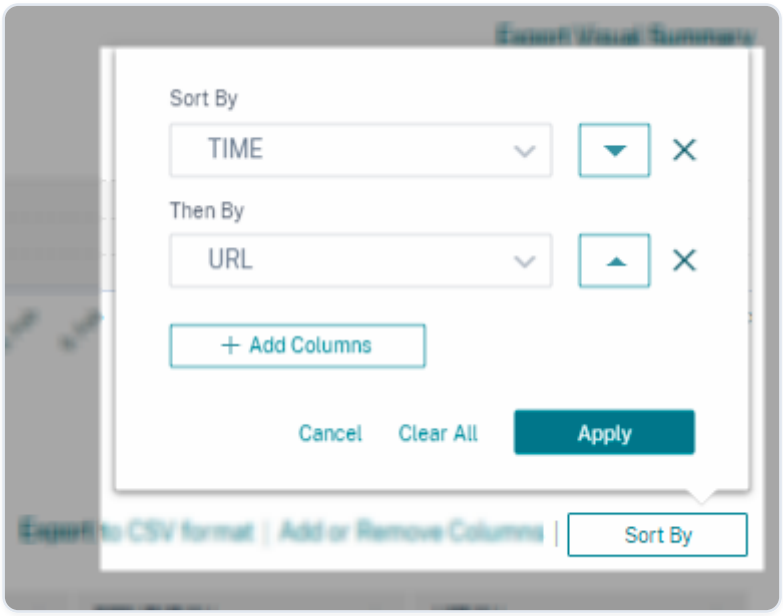
On the **User Info** page, Citrix Analytics now displays the user's location from the {{page.cvad-and-daas-product-name}} data source.

For more information about the user location, see User profile.

Multi-column sorting

On the self-service search page, you can now sort the user events by more than one column. Click **Sort By**, add the columns, and the sorting order. Click **Apply** to sort the user events. You can add up to six columns to perform a multi-column sorting.

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



For more information, see Self-service search.

Deprecated features

Excessive authorization failure risk indicator deprecated

The Citrix Gateway risk indicator - **Excessive authorization failure** has been deprecated. You can only view historic data related to this indicator.

The following changes are applicable as part of this deprecation:

- Citrix Analytics no longer generates these risk indicators.
- Citrix Analytics no longer generates policies with these risk indicators as the conditions.
- Default policies with these risk indicators as the conditions no longer take effect.

For more information, see Citrix Gateway risk indicators.

January 27, 2021

What's new

Enhancements to the Access from an unusual location risk indicator

For Citrix Content Collaboration, Citrix Gateway, and Citrix Virtual Apps and Desktops, the **Access from an unusual location** risk indicator is now triggered when the user signs in from an IP address associated with a new country, or a new city that is anomalously far away from any previous sign-in location. Other factors include the user's overall level of mobility and the relative

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

frequency of sign-ins from the city across all users in your organization. In all cases, user location history is based on the previous 30 days of sign-in activity.

For more information about the risk indicator, see the following topics:

- Citrix Content Collaboration risk indicators
- Citrix Gateway risk indicators
- Citrix Virtual Apps and Desktops and Citrix DaaS risk indicators

January 20, 2021

Fixed issue

- For the Apps and Desktops data source with on-premises StoreFront, the data processing fails although the StoreFront deployment is successfully connected.

January 19, 2021

Fixed issue

- In the custom risk indicator page, after correcting an invalid condition in the search field, the **Estimate Trigger** link does not respond.

  For example, you type an invalid condition *Client-IP = 10.10.10.10*. After you correct this condition and type as *Client-IP = "10.10.10.10"*, the **Estimate Trigger** link does not respond.

  Workaround: Refresh the custom indicator page and then create the custom indicator with a valid condition.

January 13, 2021

What's new

New version of Citrix Analytics Add-on for Splunk is available

Citrix Analytics Add-on version 2.1.0 for Splunk is now available. Go to the downloads page to download the file.

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

Added support for Splunk Cloud Inputs Data Manager (IDM) and Splunk 8.1 64-bit

You can now integrate Citrix Analytics for Security with Splunk Cloud IDM and Splunk 8.1 64-bit. For more information, see Splunk integration.

Deprecated support

Removed support for Splunk 7.1 64-bit

You can no longer integrate Citrix Analytics for Security with Splunk 7.1 64-bit. For information on supported Splunk versions, see Splunk integration.

January 11, 2021

Fixed issue

- On the Virtual Apps and Desktops site card, the label **Supported client users** is renamed to **Received events from users**. The label **Unsupported client users** is renamed to **Unable to receive events from users**.

December 17, 2020

What's new

Use preconfigured custom risk indicators and a policy to block access from unusual locations (geofencing)

Citrix provides a list of preconfigured custom risk indicators and a policy that help you monitor the security of your Citrix infrastructure. With these indicators and a policy, you can block the user access originating from countries that are outside their usual operating country. By default, the country is set to "United States". You can set your required country for geofencing.

The following are the preconfigured custom risk indicators and a policy:

- CVAD-Session started outside of geofence
- GW-Geofence crossing
- CCC-Geofence crossing
- Session start outside of geofence

For more information, see Preconfigured custom risk indicators and policies.

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

View accessed locations in the user-response email

Instead of a user device's IP address, the user-response email now displays all locations accessed by the user in the last 15 minutes. The location is displayed in the `<City>,<Country>` format. If the city or country is unavailable, the corresponding value is shown as "Unknown".

For more information, see Request user response.

Renamed Content Collaboration risk indicator- First time access from new location

The Citrix Content Collaboration risk indicator **First time access from new location** is renamed as **Access from an unusual location**.

For more information, see Access from an unusual location.

Deprecated features

Risk indicator feedback

The risk indicator feedback mechanism is removed. If the Content Collaboration risk indicator- Access from an unusual location is incorrectly triggered, you can no longer report it as a false positive and provide feedback.

December 07, 2020

What's new

Improvements to the Potential data exfiltration risk indicator

The following enhancements are made to the risk indicator:

- The information in the **WHAT HAPPENED** section is updated. The time format is updated to maintain consistency.
- The device location information appears in the event list.

For more information about the risk indicator, see Potential data exfiltration.

Improvements to the Content Collaboration risk indicator- First time access from new location

On the user risk timeline, select **First time access from new location** to view the following information:

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

- **Sign in locations**: Displays a geographical map view of the usual and unusual locations from where the user has signed in.
- **Number of sign-ins from usual locations - last 30 days**: Displays a pie chart view of the top 6 usual locations from where the user has signed in the last 30 days. It also displays the number of sign-in events from these locations.
- **Event details for unusual location**: Provides the list of the sign-in events from the unusual location for the user.

For more information about the risk indicator, see First time access from new location.

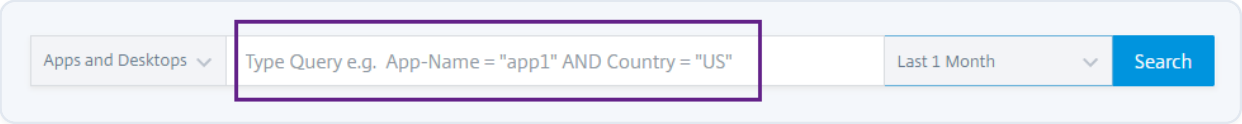
November 30, 2020

What's new

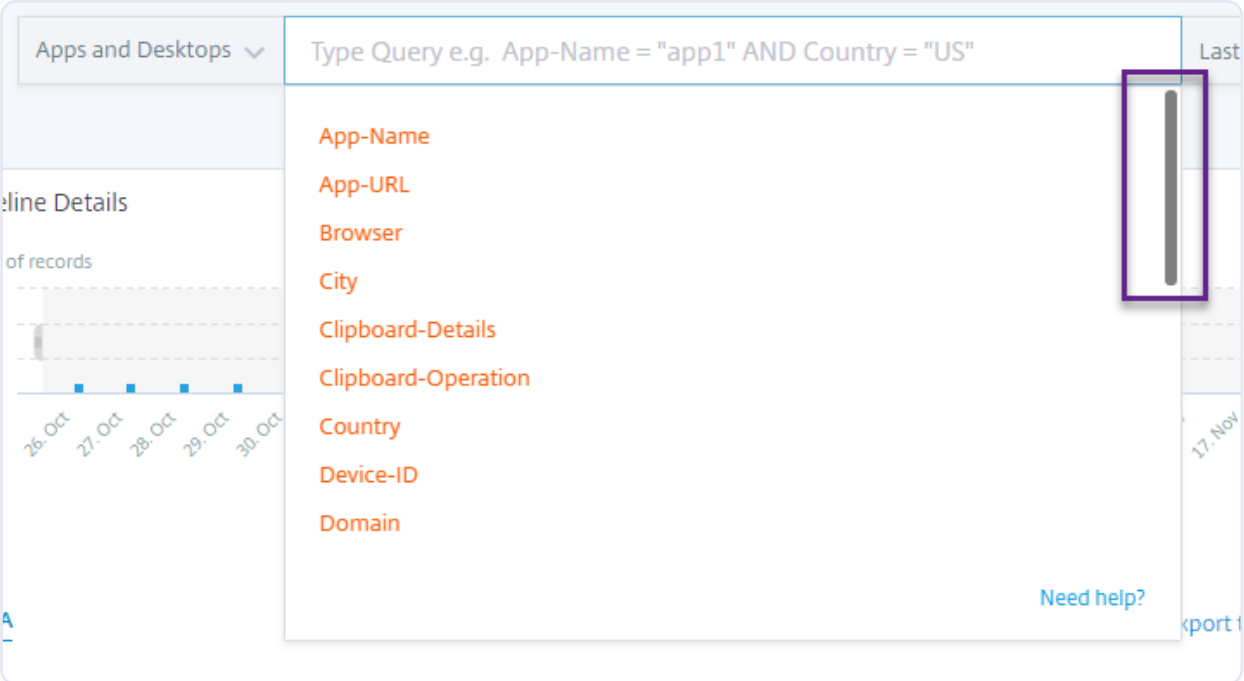
Self-service search page improvements

Following improvements are made to enhance the usability of the self-service search page:

- The search box displays an example of a query to indicate how to type your own query.

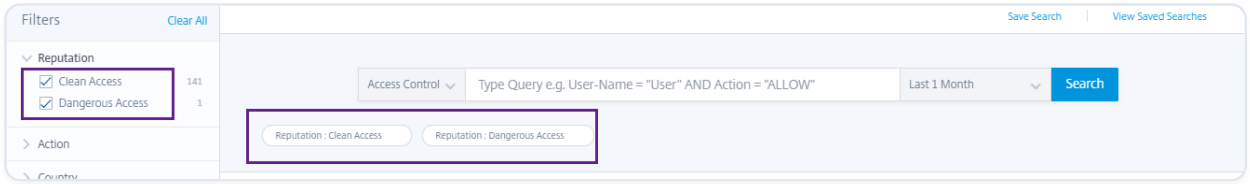


- In macOS, the scroll bar on the dimension list now appears by default.

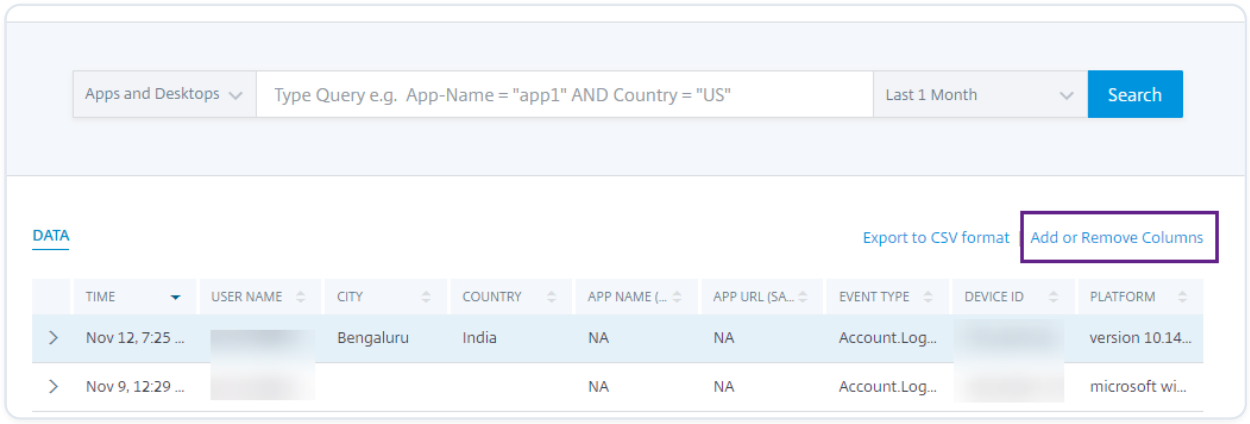


- The applied filters now appear as chips.

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



- The **Add or Remove Columns** label replaces the **+** icon.



For more information, see Self-service search.

Policy improvements

The **Policies** page now displays the policies associated with the data sources that are successfully discovered and connected to Citrix Analytics. This page does not display the policies that have a condition defined for the undiscovered data sources. Turning off data processing for an already connected data source does not affect the existing policies on the **Policies** page.

For more information, see Configure policies and actions.

November 04, 2020

What's new

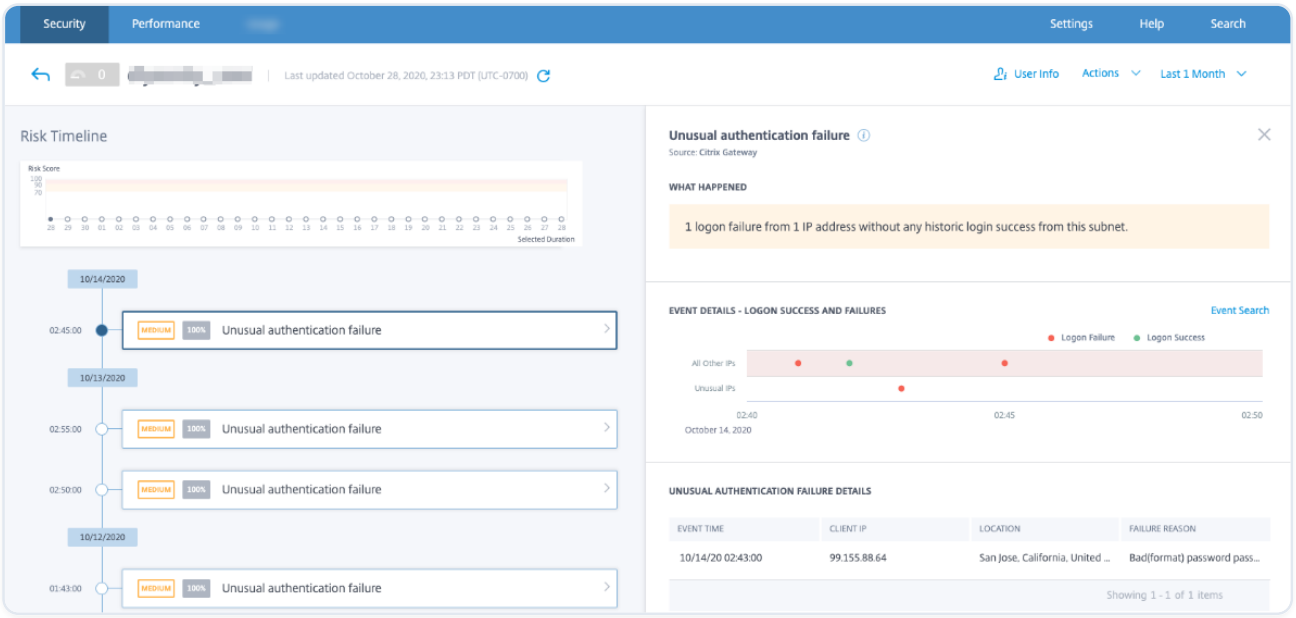
Unusual Authentication Failure - Citrix Gateway risk indicator

Citrix Analytics detects access-based threats when a user has logon failures from an unusual IP address and triggers the **Unusual Authentication Failure** risk indicator.

This risk indicator is triggered when a user in your organization has logon failures from an unusual IP address that is contrary to their usual behavior.

For more information, see Citrix Gateway risk indicators.

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



October 20, 2020

Fixed issue

- The risk indicator **First time access from new device** with **Log off user** action applied is not working as expected.

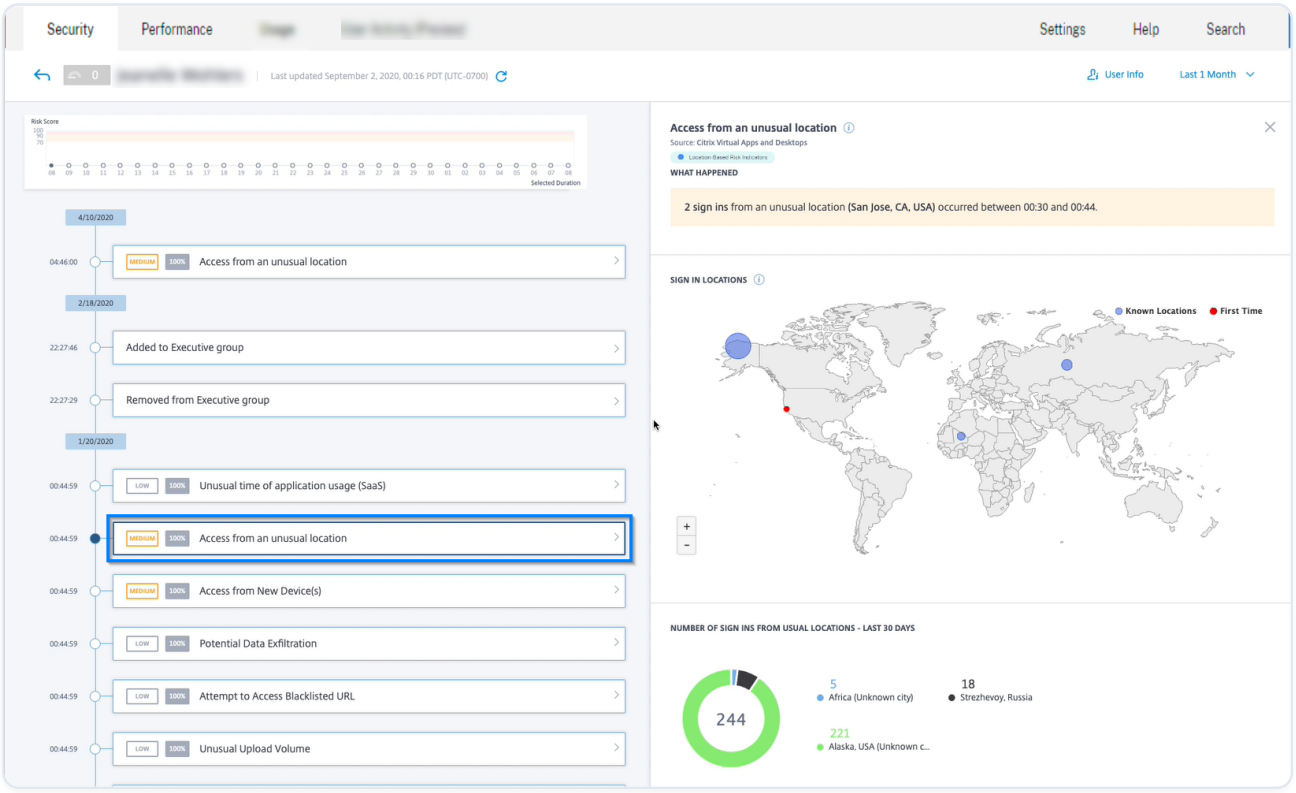
October 15, 2020

New features

Access from an unusual location – Citrix Virtual Apps and Desktops and Citrix DaaS risk indicator

Citrix Analytics detects access-based threats based on unusual sign-ins from Citrix Workspace and triggers the corresponding risk indicator.

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



For more information, see Citrix Virtual Apps and Desktops and Citrix DaaS risk indicators.

Share Link dashboard enhancements

- The SHARE URL column is now replaced by the SHARE ID column. Each share URL is now identified with a share ID.
- Time selection on the dashboard is removed. Now, this dashboard displays all share links from the active state to the expired state instead of a selected period.
- All share links are sorted in the order of active links first and then the expired links. By default, the share link with highest risk indicator count appears on the top of the list.
- The risky links now display the active links that have risky behavior. It does not show the expired links. By default, the risky link with highest risk indicator count appears on the top of the list.
- The trend view in the Risky Share Links card and the All Share Links card is removed.

For more information, see Share Links dashboard.

Share Link risk timeline enhancements

The risk timeline now displays the share ID instead of the share URL. For more information, see Share Link risk timeline.

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

Deprecated features

Access from device with unsupported operating system (OS) risk indicator deprecated

The Citrix Virtual Apps and Desktops risk indicator - **Access from device with unsupported operating system (OS)** has been deprecated. You can only view historic data related to this indicator.

The following changes are applicable as part of this deprecation:

- Analytics no longer generates these risk indicators.
- Analytics no longer generates policies with these risk indicators as the conditions.
- Default policies with these risk indicators as the conditions no longer take effect.

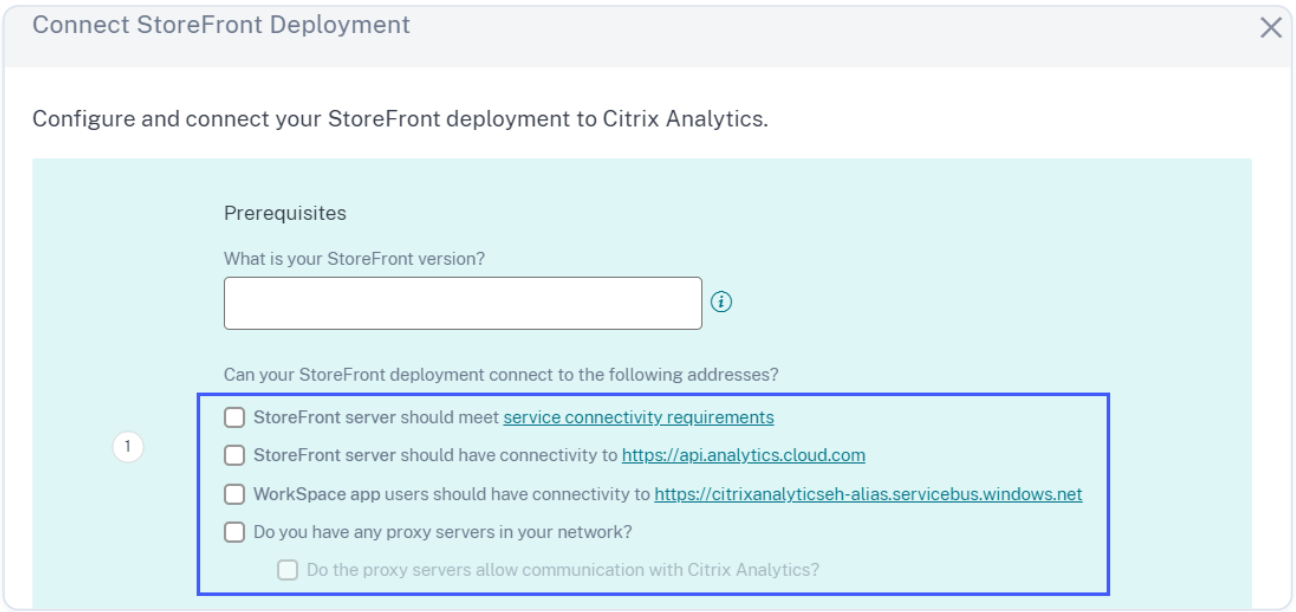
For more information, see Citrix Virtual Apps and Desktops and Citrix DaaS risk indicators.

September 10, 2020

New features

Checklist for StoreFront

Citrix Analytics now displays a list of prerequisites that you must meet before downloading the StoreFront configuration file. Review the checklist and ensure that all the minimum requirements are selected. If the minimum requirements are not selected, you cannot download the configuration file. For more information, see Citrix Virtual Apps and Desktops data source.



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

Self-service search - support for NOT EQUAL (!=) operator

You can now use the NOT EQUAL (!=) operator in your query in the following features:

- Custom risk indicator
- Self-service search

You can use this operator for the following conditions:

DATA SOURCE	DIMENSIONS
Content Collaboration	Country, City, Client OS
Access Control	Country, City, Action, URL, URL Category, Reputation, Browser, OS, Device
Apps and Desktops	Country, City, App Name, Clipboard operation, Browser, OS
Gateway	Authentication Stage, Client IP

Using the operator, create a custom indicator expression with a single value such as "Country != XYZ" and view the list of users. Then create a policy to apply actions such as Add to watchlist, Notify admin, or Disable user. You can also use the operator in the self-service search of the specified data sources to filter the user events.

While entering the values for the dimensions in your query, use the exact values that are shown on the self-service search page for a data source. The dimension values are case-sensitive.

September 08, 2020

New features

User Correlation

Analytics now correlates the users discovered from various data sources. This mechanism eliminates most of the duplicate users from the discovered users list. The discovered users in Analytics now display the list of unique users along with their data sources and the risk indicators.

For example, the user "Joe Smith" can have multiple user identifiers- JosephSm, <joe.smith@citrix.com>, and joe.smith based on the data sources. Analytics now identifies this user with a unique identifier name. All other user identifiers are correlated and events received for

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

Joe Smith from various data sources is linked to this unique name. For more information, see Discovered users

Fixed issue

From the **Actions** list, after selecting the action options and clicking **Apply**, an error message is displayed.

August 11, 2020

Fixed issues

- You are not able to integrate Microsoft Graph Security with Citrix Analytics. This issue occurred because the Microsoft portal failed to redirect to Citrix Analytics.

July 31, 2020

Fixed issues

- The **Estimated Triggers** option in the custom risk indicator does not predict the custom risk indicator instances for the last one day.

July 09, 2020

New features

Virtual Apps and Desktops site card displays users with supported and unsupported clients

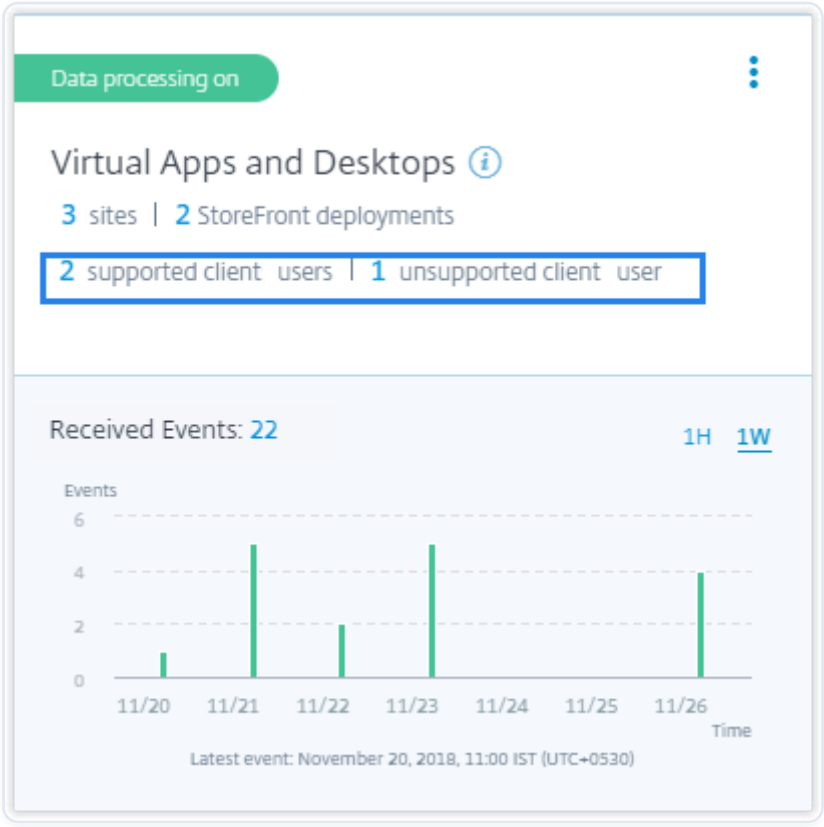
On the site card, you can now view the number of users who are using supported and unsupported versions of Citrix Workspace app or Citrix Receiver™ clients on their endpoints.

- Click the user count for the supported clients to view the **User** page that displays all the discovered users.
- Click the user count for the unsupported clients to download a CSV file. The file lists the users and their unsupported client versions. Analytics does not receive user events from the unsupported clients and therefore, does not add the users as discovered users. Using the CSV

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

file, you identify the users who must upgrade their clients to a supported version so that Analytics can provide security insight into their behavior.

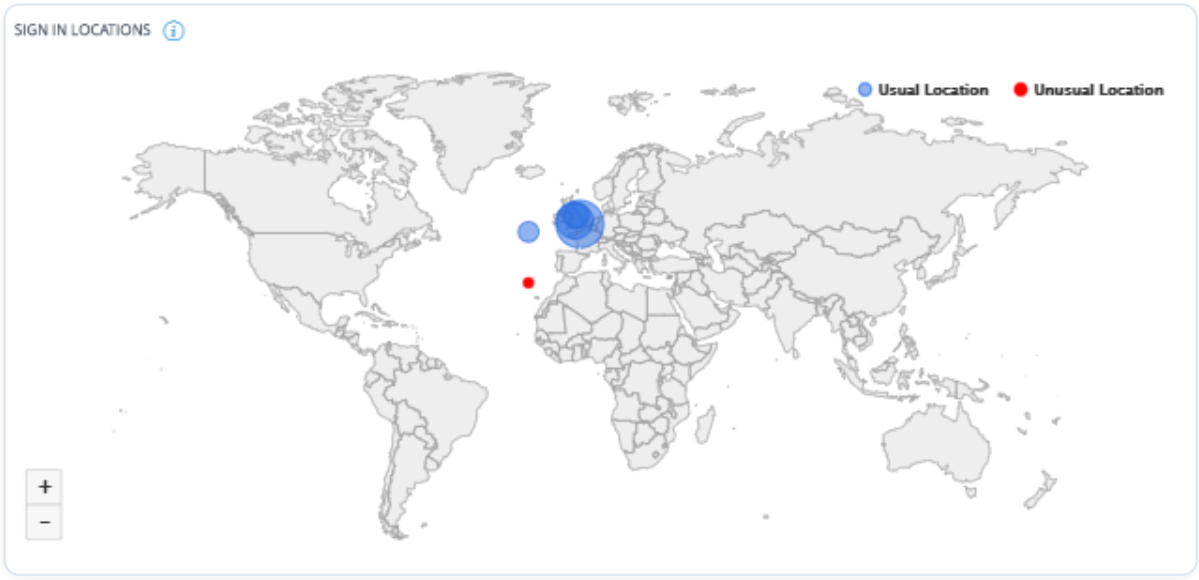
To view the list of supported clients, see Citrix Virtual Apps and Desktops and Citrix DaaS data source.



Access from an unusual location risk indicator

- The Citrix Gateway risk indicator **First time access from new location** is renamed as **Access from an unusual location**.
- On the user risk timeline, a geographical map and a pie chart are introduced in the event details section.
    - **Sign in locations**: This section displays a geographical map view of the user's usual and unusual locations. The usual and unusual locations are indicated by a color code on the top right section of the geo map. You can zoom the geo map to get a closer look of the location.

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



- **Usual locations - last 30 days**: This section displays a pie chart that gives a view of the top 6 usual locations that the user has signed in from. Each location is marked with a different color code. You can sort the section by the location to get a detailed view of the selected location.



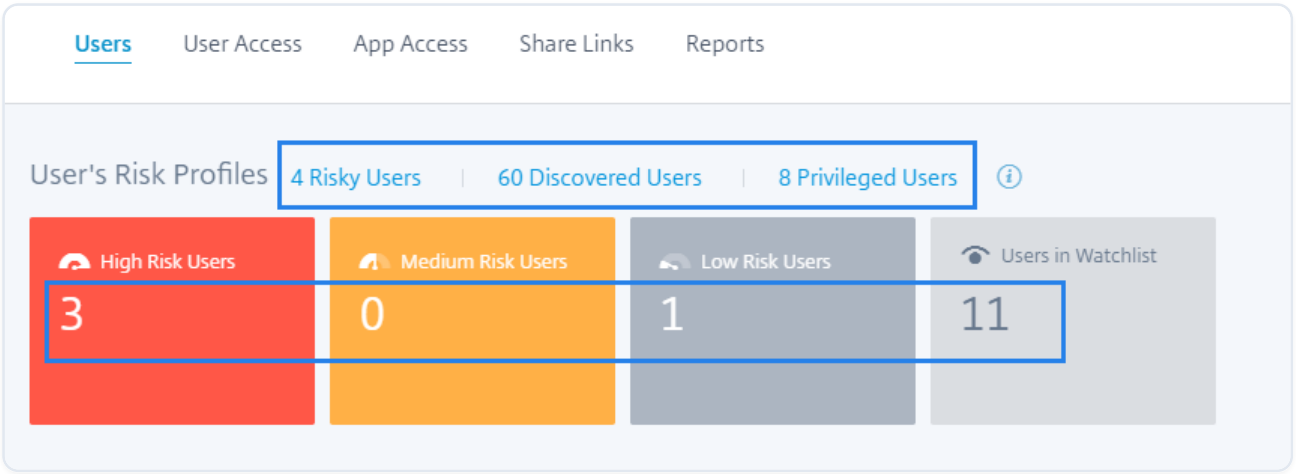
For more information, see Access from an unusual location.

Users dashboard data

The number of risky users, discovered users, privileged users, and users in the watchlist are displayed for the last 13 months irrespective of the time period selected on the **Users** dashboard and the **Users** page. When you select the time period, the risk indicator occurrences change.

For more information, see Users dashboard.

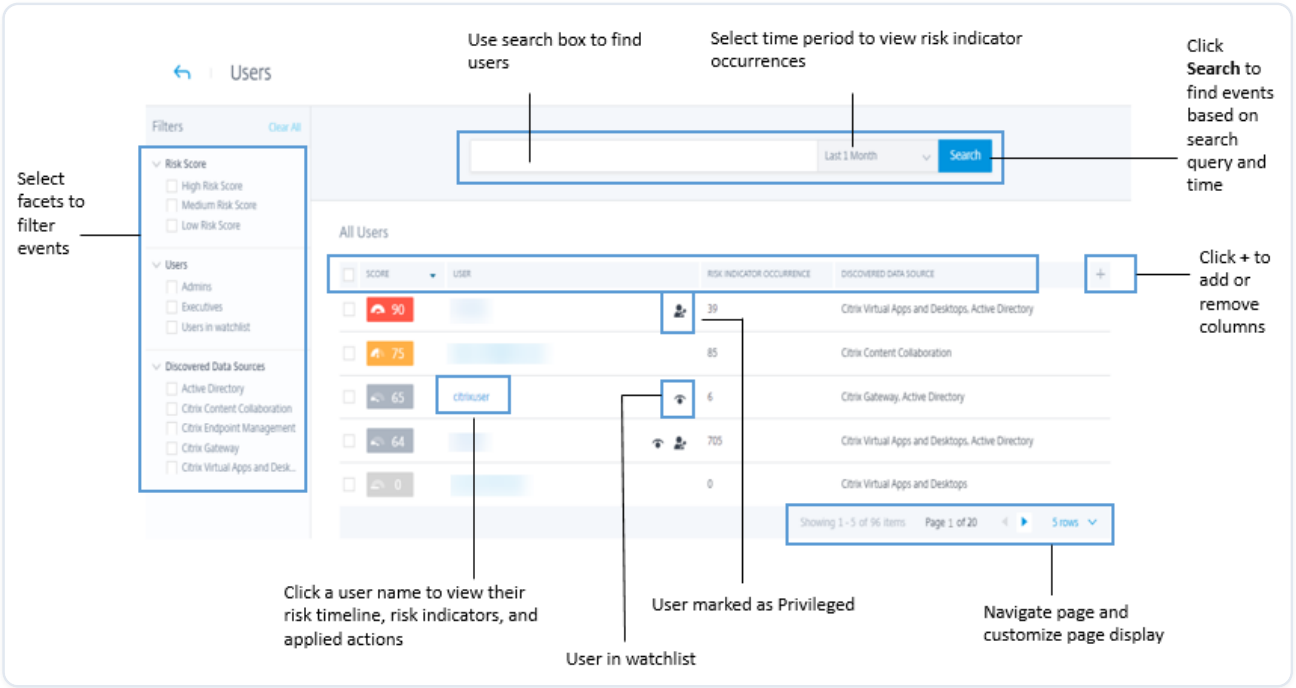
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Redesigned Users page

The **Users** page has been enhanced for a better user experience. It provides a consolidated summary of the user events based on the user risk scores, data source, and user type.

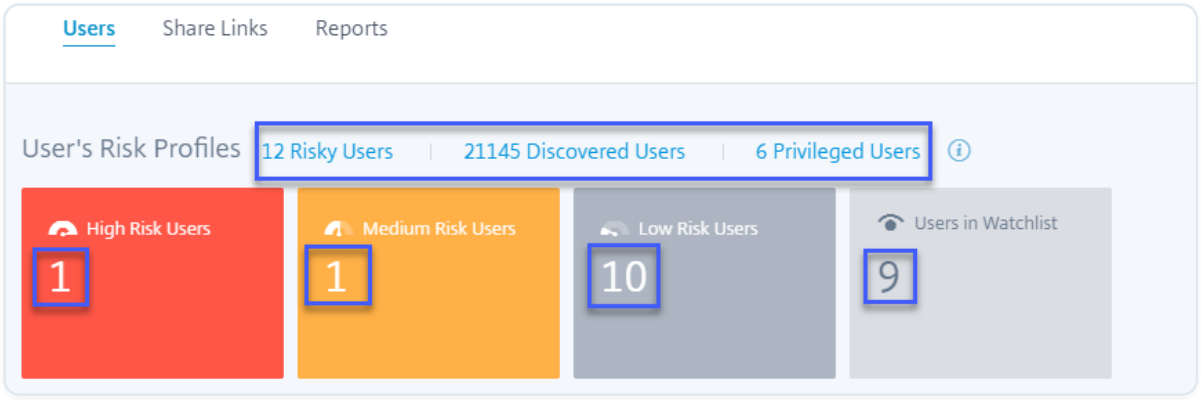
To support a more focused search, the **Users** page contains the **Filters** section on the left pane and the search bar on top. You can search for user events for a preset time or a customized time range.



To view the **Users** page:

- Go to **Security > Users** to view the **Users** dashboard and do the following:
  - Click one of the following links or the cards.

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



  - On the **Risky Users** pane, click **See More**.
  - On the **Users in Watchlist** pane, click **See More**.
  - On the **Privileged Users** pane, click **See More**.

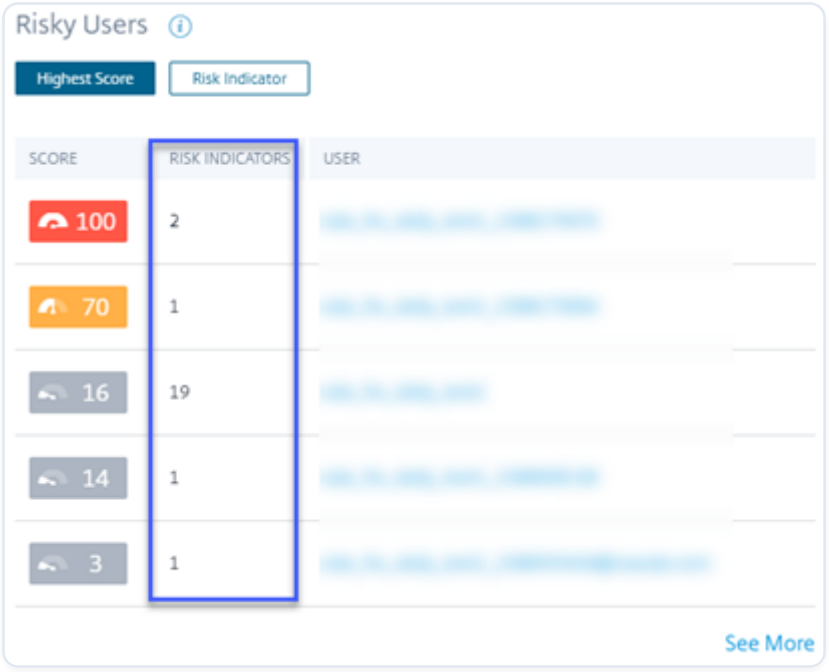
- Go to **Settings > Data Sources > Security**. Click the number of users on any data source site card.

For more information, see Users dashboard.

Risky Users pane enhancements

The **Change** column is replaced with the **Risk Indicators** column. The **Risk Indicators** column displays the total risk indicator occurrences of a user for a specific time period.

For more information, see Risky Users.

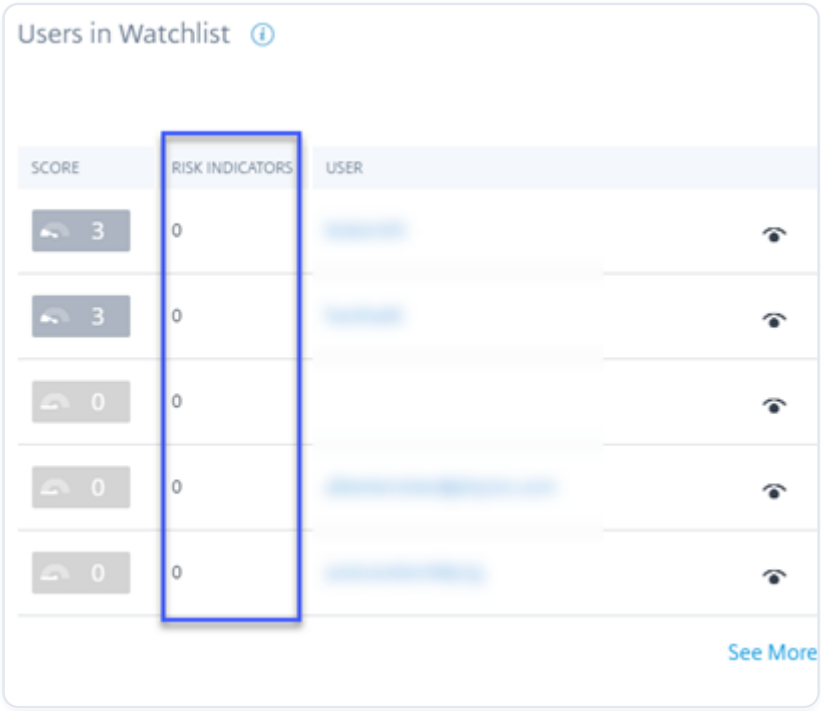


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Users in Watchlist pane enhancements

The **Change** column is replaced with the **Risk Indicators** column. The **Risk Indicators** column displays the total risk indicator occurrences of a user for a specific time period.

For more information, see Users in watchlist.

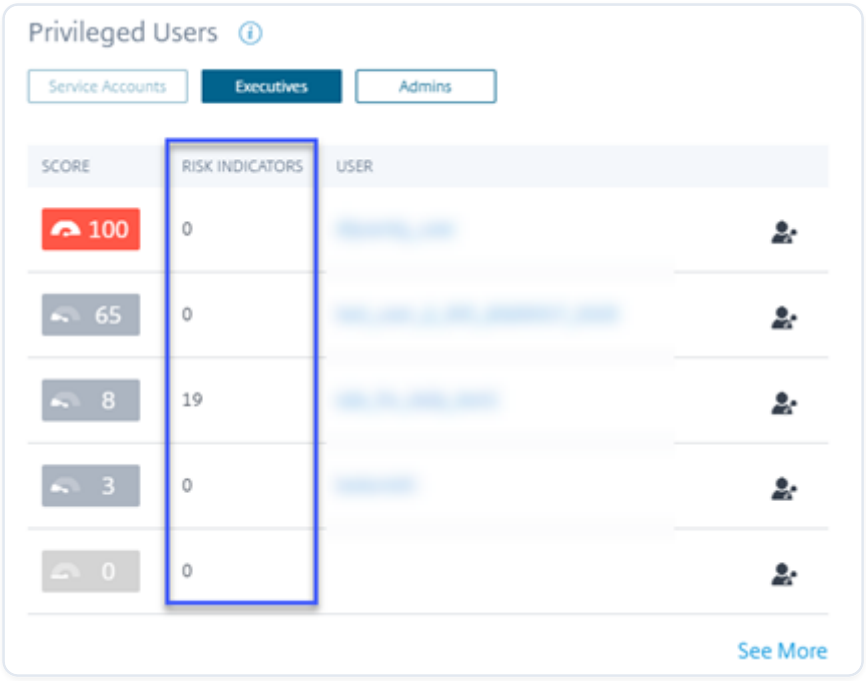


Privileged Users pane enhancements

- The **Change** column is replaced with the **Risk Indicators** column. The **Risk Indicators** column displays the total risk indicator occurrences of a user for a specific time period.
- Click **See More** to view the **Users** page. The **Users** page that displays the list of admin and executive privileged users. On this page, you can add or remove a user as a privileged user.

For more information, see Privileged users.

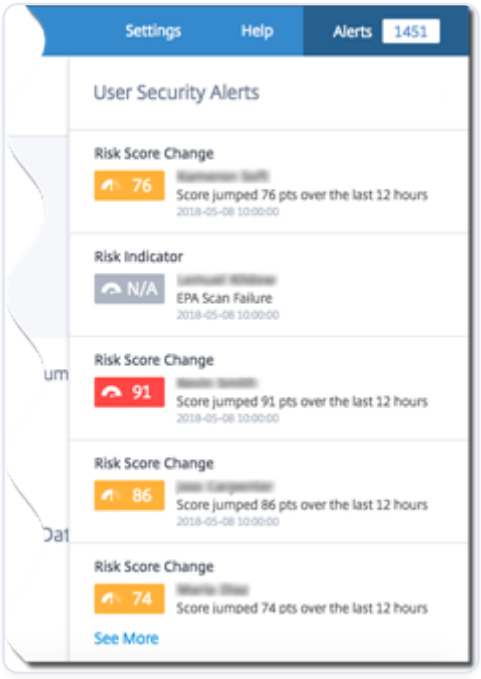
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Deprecated features

Alerts

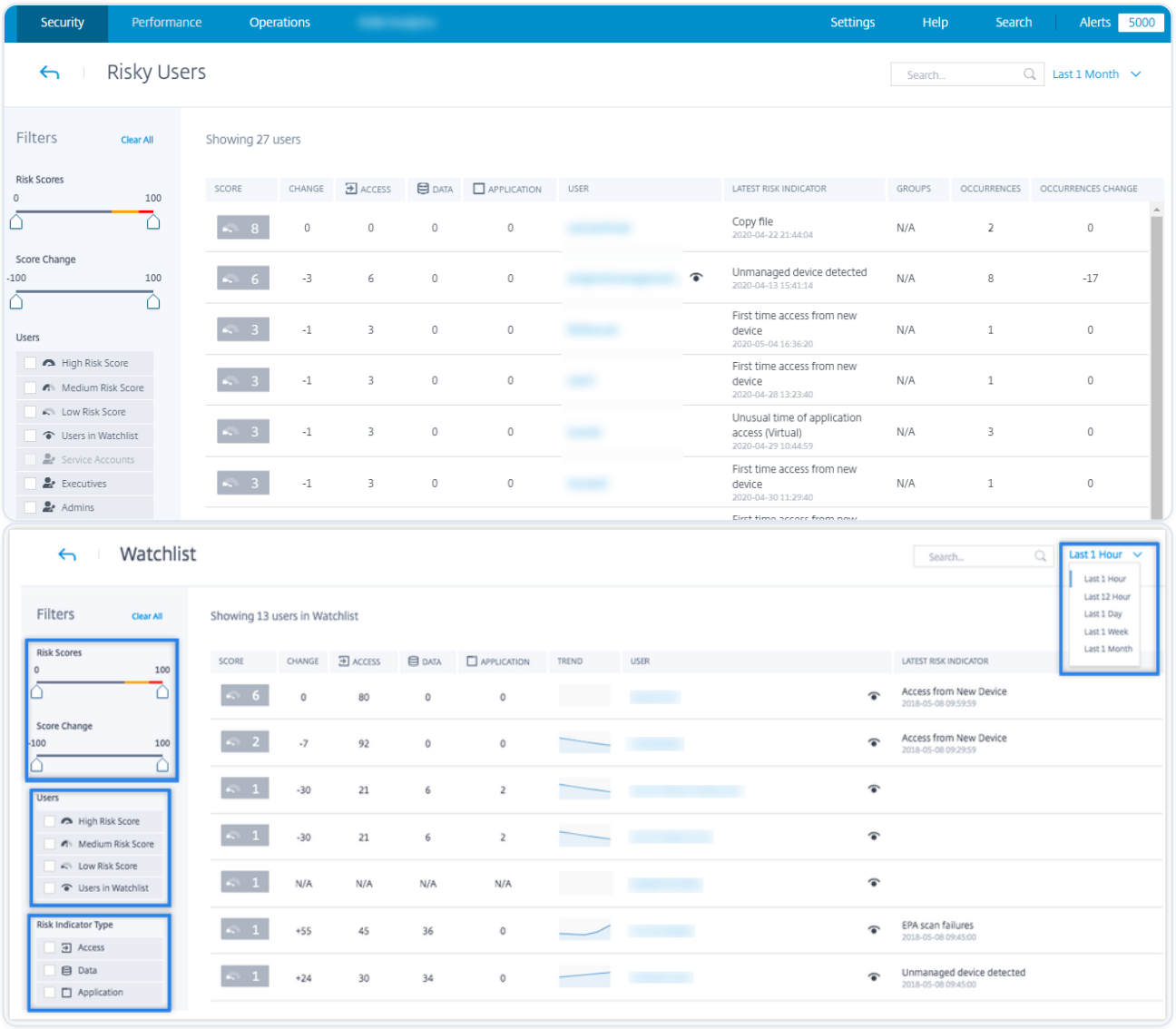
The **Alerts** feature is now deprecated and no longer available on the Analytics user interface.



Risky Users and Watchlist page

The **Risky Users** and **Watchlist** pages are deprecated. They are replaced with the **Users** page that summarizes all the risky user events and the users in the watchlist.

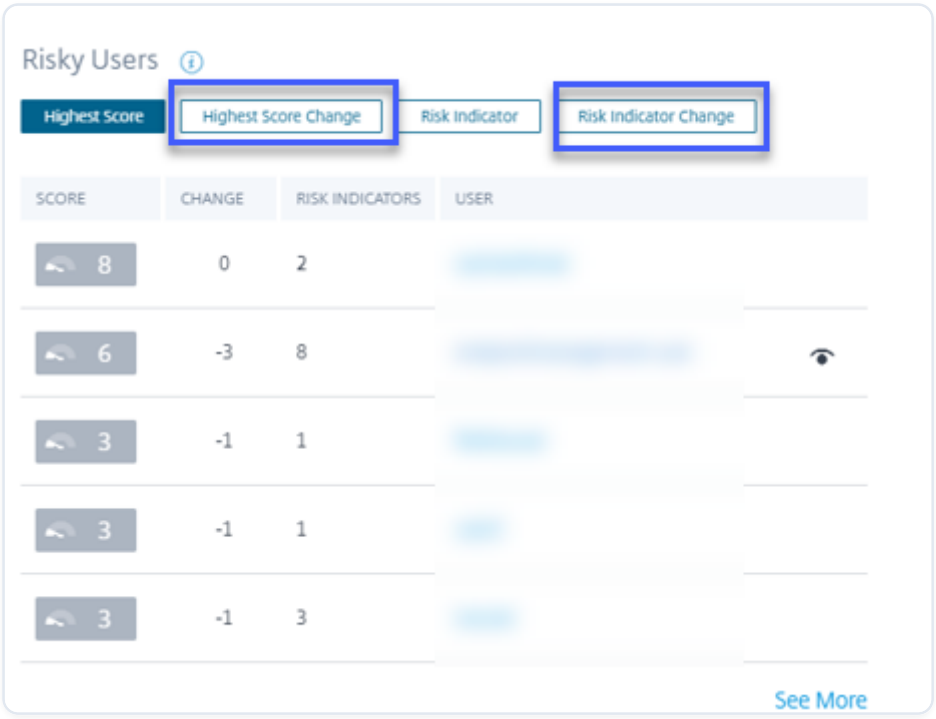
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Risky Users pane

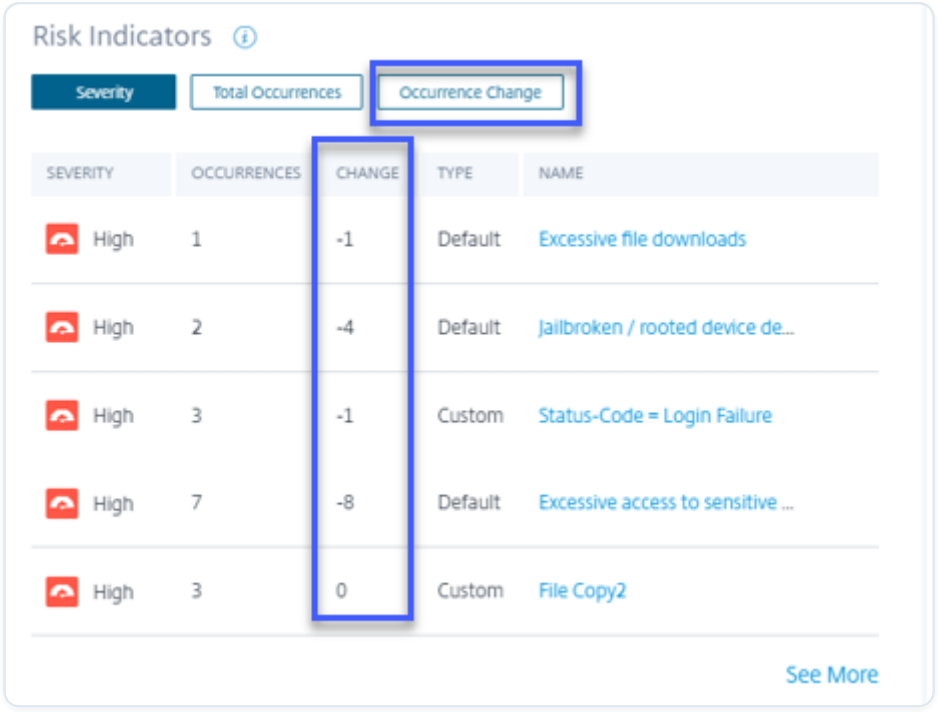
The **Highest Score Change** and **Risk Indicator Change** tabs are removed from the **Risky Users** pane.

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



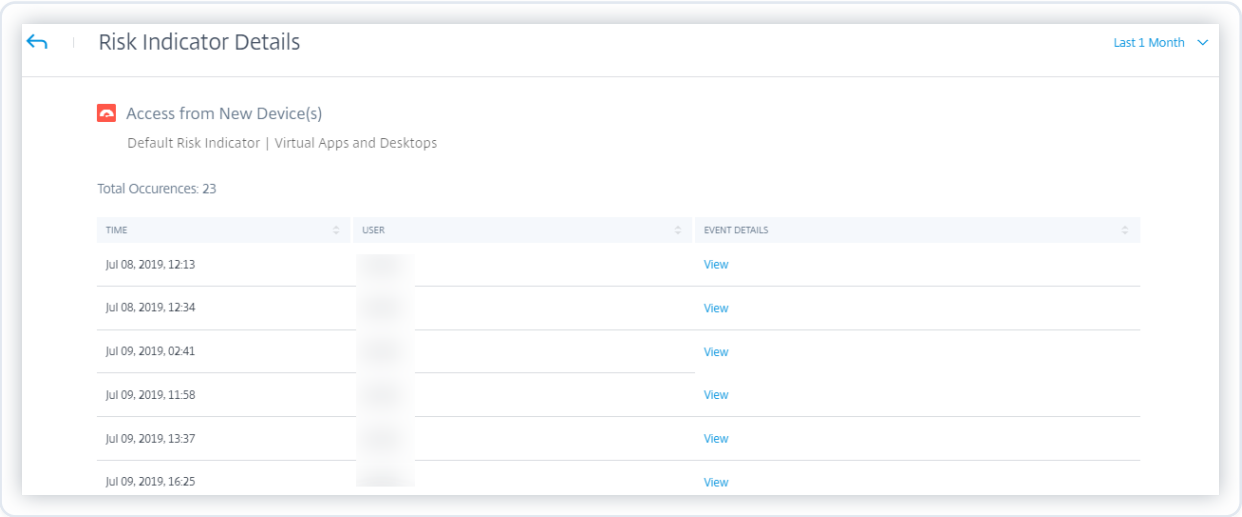
Risk Indicator pane

- The **Occurrence Change** tab and the **CHANGE** column are removed.



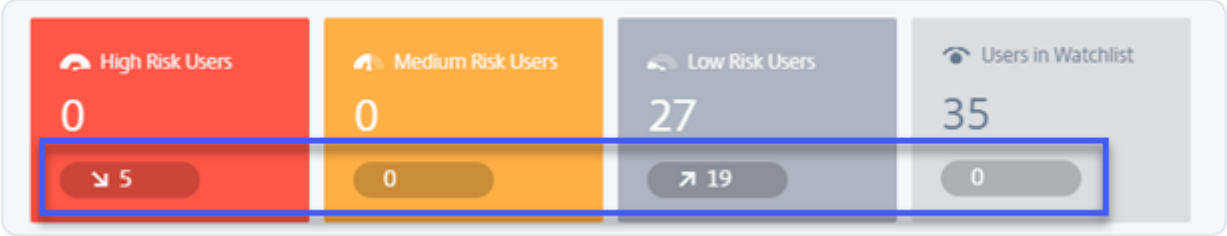
- The **Risk Indicator Details** page is deprecated. Previously, this page was displayed when a risk indicator was selected on the **Risk Indicators** pane or on the **Risk Indicator Overview** page.

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



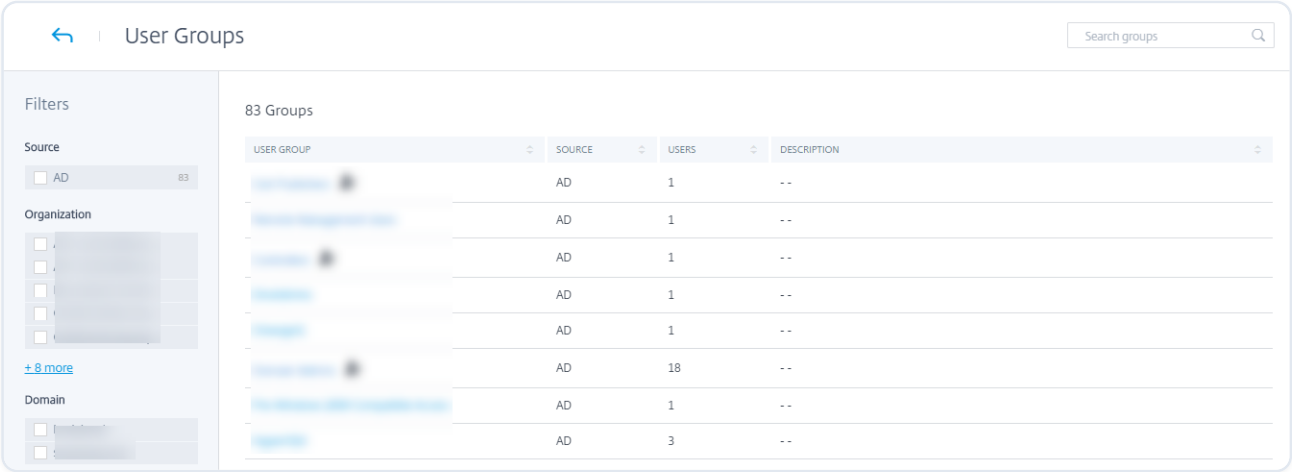
Trend view

On the **Users** dashboard, the trend view of user count is removed from the **High Risk Users**, **Medium Risk Users**, **Low Risk Users**, and **Users in Watchlist** cards.



User Groups page

The **User Groups** page under the **Settings** option is deprecated. You can no longer add or remove a user group as a privileged group. However, you can add or remove individual users as privileged users. For more details, see Privileged users.



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

June 26, 2020

Deprecated features

Unusual time of application access (Virtual/SaaS) risk indicators deprecated

The Citrix Virtual Apps and Desktops risk indicators - **Unusual time of application access (Virtual)** and **Unusual time of application access (SaaS)** have been deprecated. You can only view historic data related to these indicators.

The following changes are applicable as part of this deprecation:

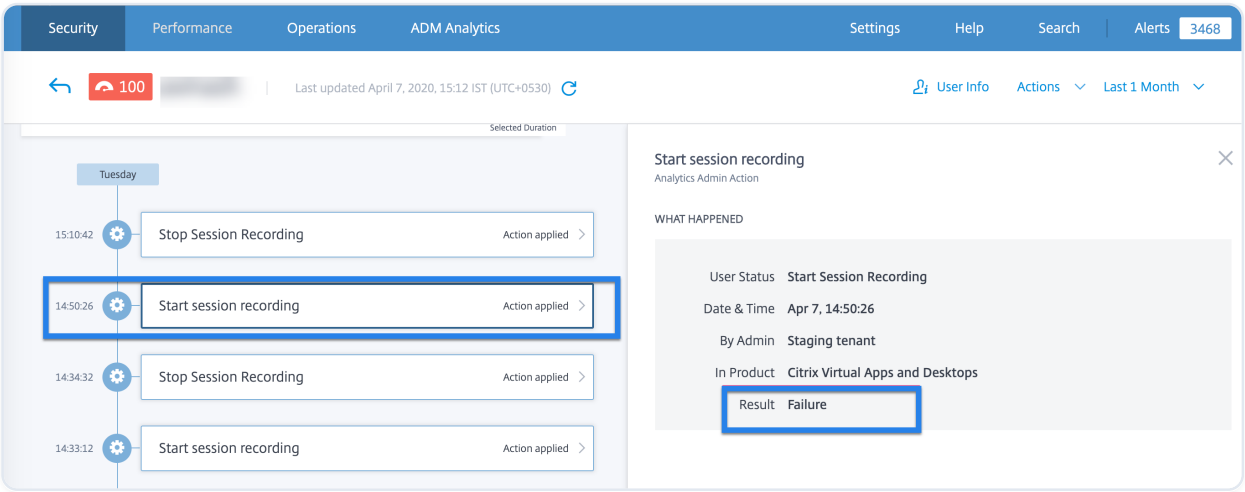
- Analytics no longer generates these risk indicators.
- Analytics no longer generates policies with these risk indicators as the conditions.
- Default policies with these risk indicators as the conditions no longer take effect.

For more information, see Citrix Virtual Apps and Desktops and Citrix DaaS risk indicators.

June 02, 2020

Fixed issues

- On the user risk timeline, the status of the Virtual Apps and Desktops actions (policy-based or manually applied) appears as "Failure" even though the actions are successfully applied on the user account. For example, the **Start session recording** action is successfully applied on the user account, but the result is shown as "Failure".



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

May 11, 2020

Fixed issues

- For some users, the policy-based actions are not triggered and the policy enforcement mode cannot be applied. This issue occurs when the customer IDs are not in lower case.

  ,

- Unable to create custom risk indicators for some users. This issue occurs when the customer IDs are not in lower case.

April 29, 2020

Fixed issues

- Actions applied on Citrix Virtual Apps and Desktops risk indicators fail to take effect although Analytics displays a message that the actions are successfully applied. This issue is observed in the Citrix Virtual Apps and Desktops 7 1912 version.

April 02, 2020

New features

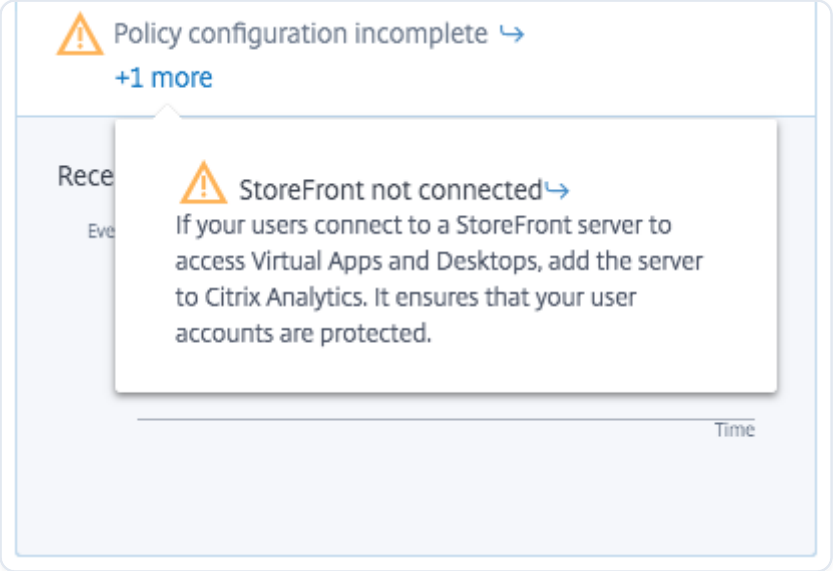
Disable data processing when StoreFront is not added

On the **Settings** > **Data Sources** > **Security** > **Virtual Apps and Desktops** data source site card, the **Turn on Data Processing** button does not get enabled if you have not onboarded StoreFront. You see the **StoreFront not connected** warning message on the site card. If you have an active on-premises site from where you want Analytics to receive data, you must verify that you have onboarded StoreFront to Citrix Analytics. It ensures that your user accounts are protected.

On the **Virtual Apps and Desktops** site card, select the vertical ellipsis (⋮) and click **Connect StoreFront deployment**. On the screen that is displayed, follow the instructions and complete the StoreFront configuration.

For more information, see Onboard Citrix Virtual Apps and Desktops on-premises sites using StoreFront.

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



Fixed issues

- For Citrix Content Collaboration users, policy-based actions fail to take effect under the following conditions:
  - When custom risk indicator conditions are defined
  - Until a risk indicator is generated for a user

March 04, 2020

Fixed issues

- When Gateway users onboard to Analytics for the first time, they see the error **Citrix ADC is unresponsive or credentials are incorrect**. Upon retrying, they see the error **Device with this IP address already exists**.

February 20, 2020

New features

Citrix Analytics for Security offering

Citrix Analytics for Security is now available for individual subscription. You can subscribe to Citrix Analytics for Security and get insights that are specific to this offering. For more information, see Get started.

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

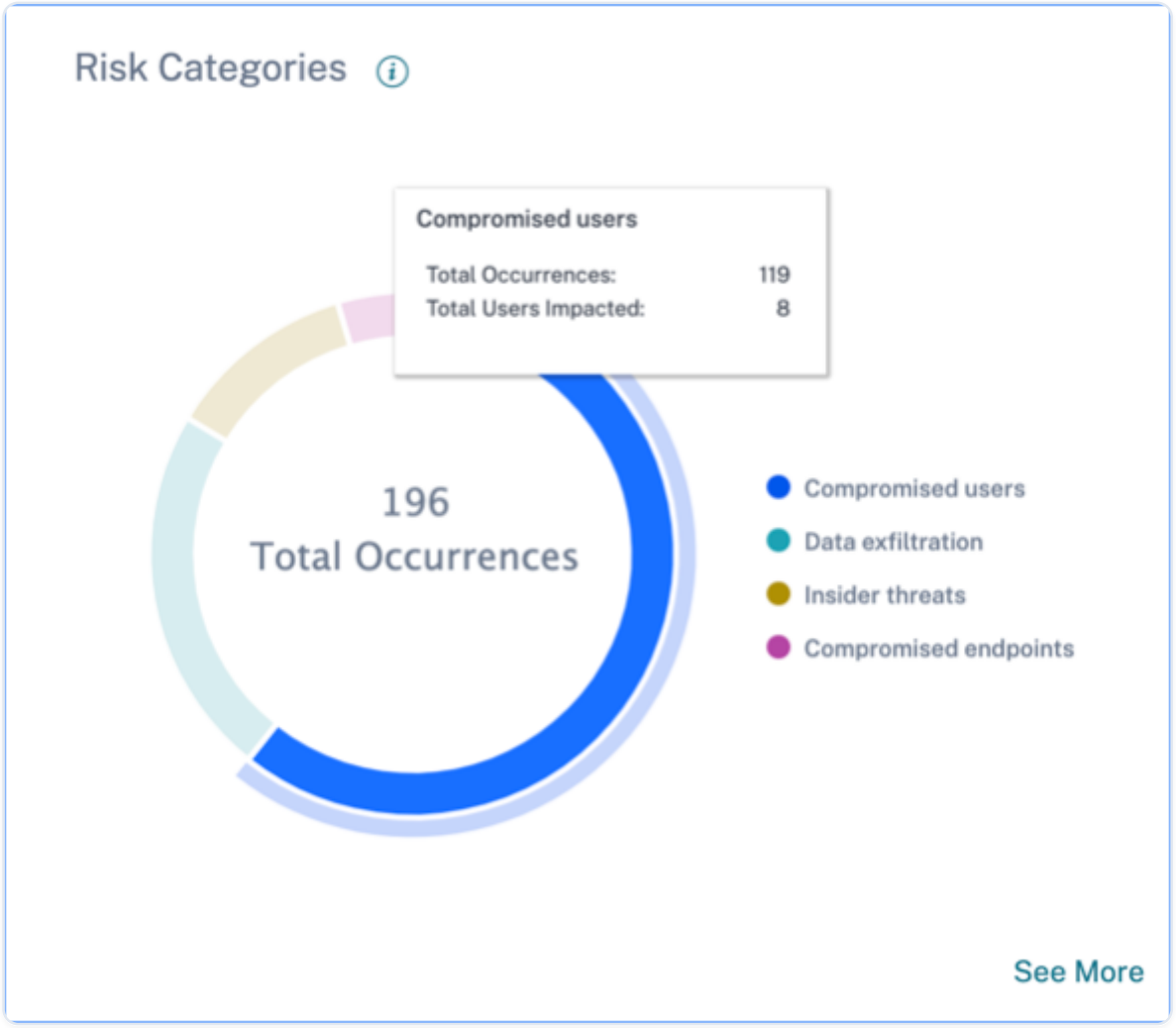
Risk Categories dashboard

Citrix Analytics introduces categorization of risk indicators based on risks that have a similar impact on the organization's security aspect. This dashboard provides a comprehensive view of the risk exposures and critical risks that require immediate attention. For default risk indicators, Analytics automatically assigns a risk category based on the risk exposure. For custom risk indicators, you must select an appropriate risk category based on the risk exposure.

Analytics supports the following risk categories:

- Data exfiltration
- Insider threats
- Compromised users
- Compromised endpoints

For more information, see Risk Categories.

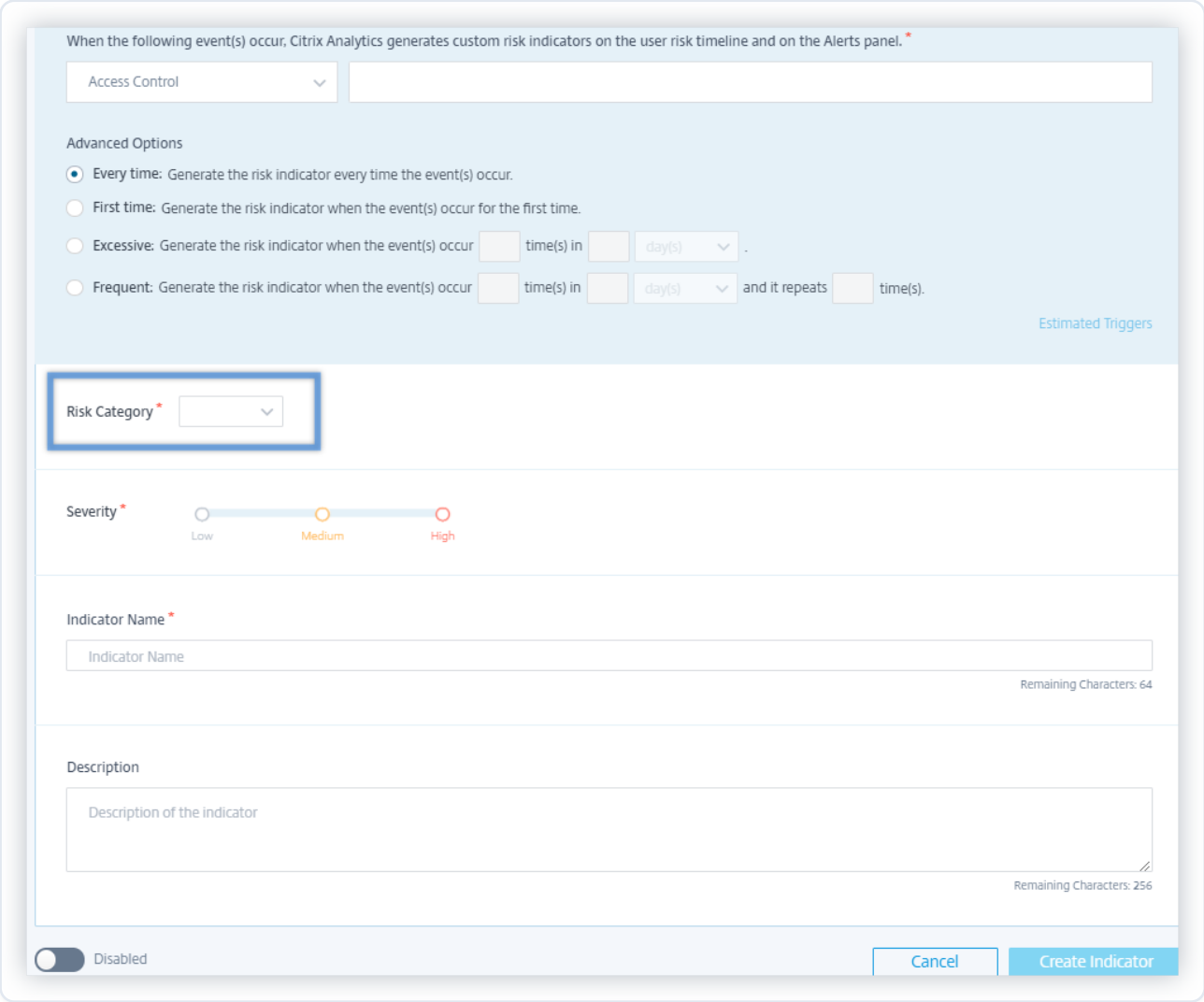


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Risk Category column on the Custom Indicators page

The **Risk Category** column is introduced on the Custom Risk Indicator page. Based on type of risk exposure, you can select a risk category for your custom risk indicator. Previously created custom risk indicators are displayed on the Risk Categories dashboard if you modify them by selecting a risk category.

For more information, see Custom risk indicators.



Change in risk indicator names

The following risk indicator names have been changed:

DATA SOURCE	OLD NAME	NEW NAME
{{page.cvad-and-daas-product-name}}	Unusual application usage (Virtual)	Unusual time of application access (Virtual)

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

DATA SOURCE	OLD NAME	NEW NAME
{{page.cvad-and-daas-product-name}}	Unusual application usage (SaaS)	Unusual time of application access (SaaS)
Citrix Content Collaboration	Excessive logon failures	Excessive authentication failures
Citrix Content Collaboration	Unusual logon access	First time access from new location
Citrix Access Control	Unusual download volume	Excessive data download
Citrix Gateway	Logon failures	Excessive authentication failures
Citrix Gateway	Authorization failures	Excessive authorization failures
Citrix Gateway	Unusual logon access	First time access from new location

For more information, see Risk indicators.

Fixed issues

- For some users, Citrix Analytics is unable to receive any data from Virtual Apps and Desktops even though the data source is successfully onboarded and StoreFront is enabled.
- Citrix Analytics is unable to receive download events from Citrix Content Collaboration. Therefore, the following risk indicators are not triggered:
  - Anonymous sensitive share download
  - Excessive share link downloads
  - Excessive access to sensitive files
  - Excessive file downloads
- For newly onboarded users, manual and policy-based actions applied on Citrix Gateway risk indicators do not take any effect.
- Some users are unable to view the site cards on the Data Sources page. This issue is resolved by repopulating the cache.

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

January 09, 2020

New features

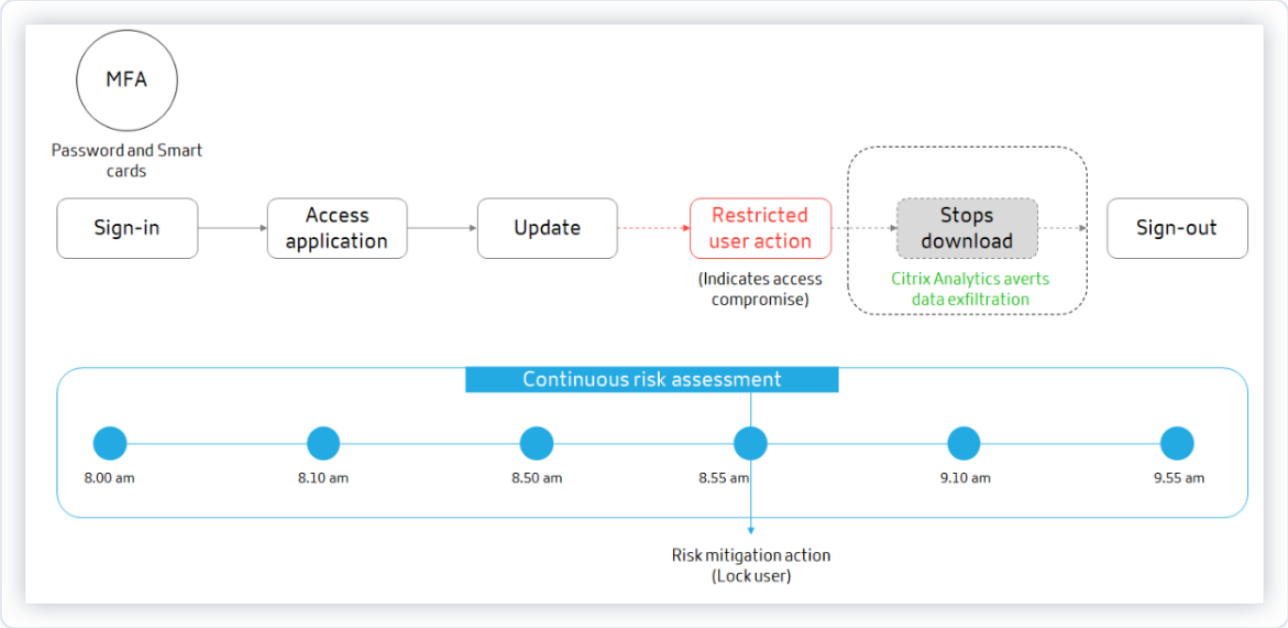
Continuous risk assessment

Some challenges Citrix Workspace users face are that, remote access exposes sensitive data to security risks through cyber-criminal activities like data exfiltration, theft, vandalism, and service disruptions. Employees within organizations are also likely to contribute to this damage.

Some ways of addressing these risks are to implement multifactor authentication, enforce short sign-in timeouts, and so on. Although these risk assessment methods ensure a higher level of security, they do not provide complete security after the initial validation.

To enhance the security aspect and to ensure a better user experience, Citrix Analytics introduces the solution of continuous risk assessment. This solution helps you to continuously monitor user profiles and take various actions when risky events are detected.

For more, information, see Continuous risk assessment.



Policy configuration

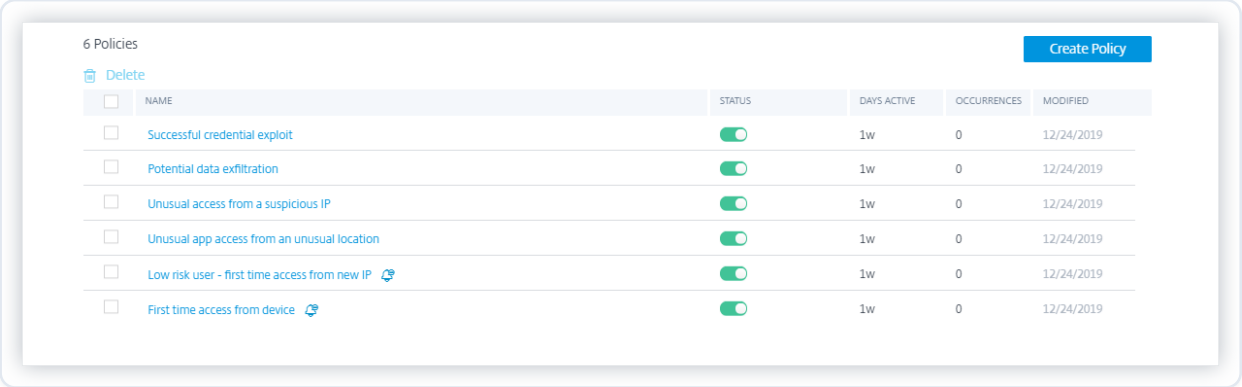
Citrix Analytics helps you to manage policy configurations more efficiently. You can protect user accounts from malicious attacks with the help of the following capabilities:

- **Default policies**: Citrix Analytics supports the following default policies:
  - Successful credential exploit

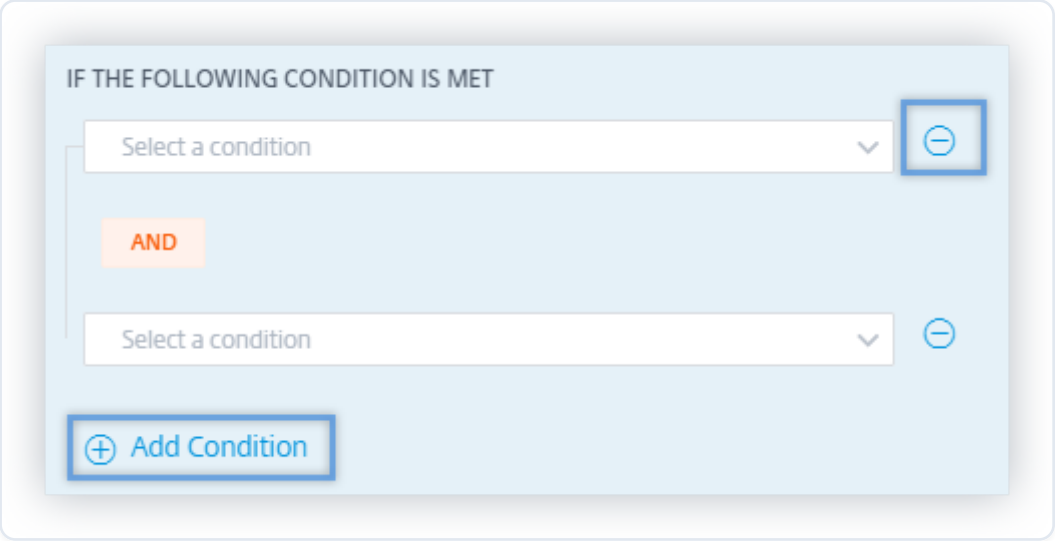
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Potential data exfiltration
- Unusual access from a suspicious IP
- Unusual app access from an unusual location
- Low risk user - first time access from new IP
- First time access from device

You can modify the default policies based on your requirements.

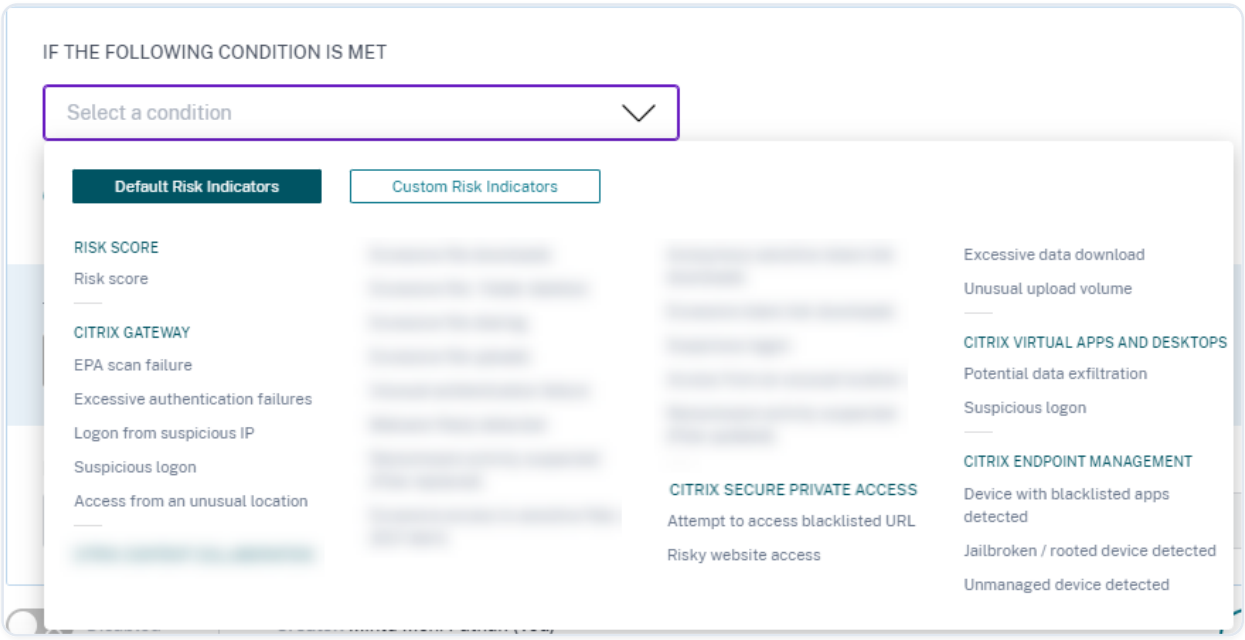


- **Multiple conditions**: A policy can contain up to four conditions. The conditions can be set with combinations of risk scores and risk indicators, or both.

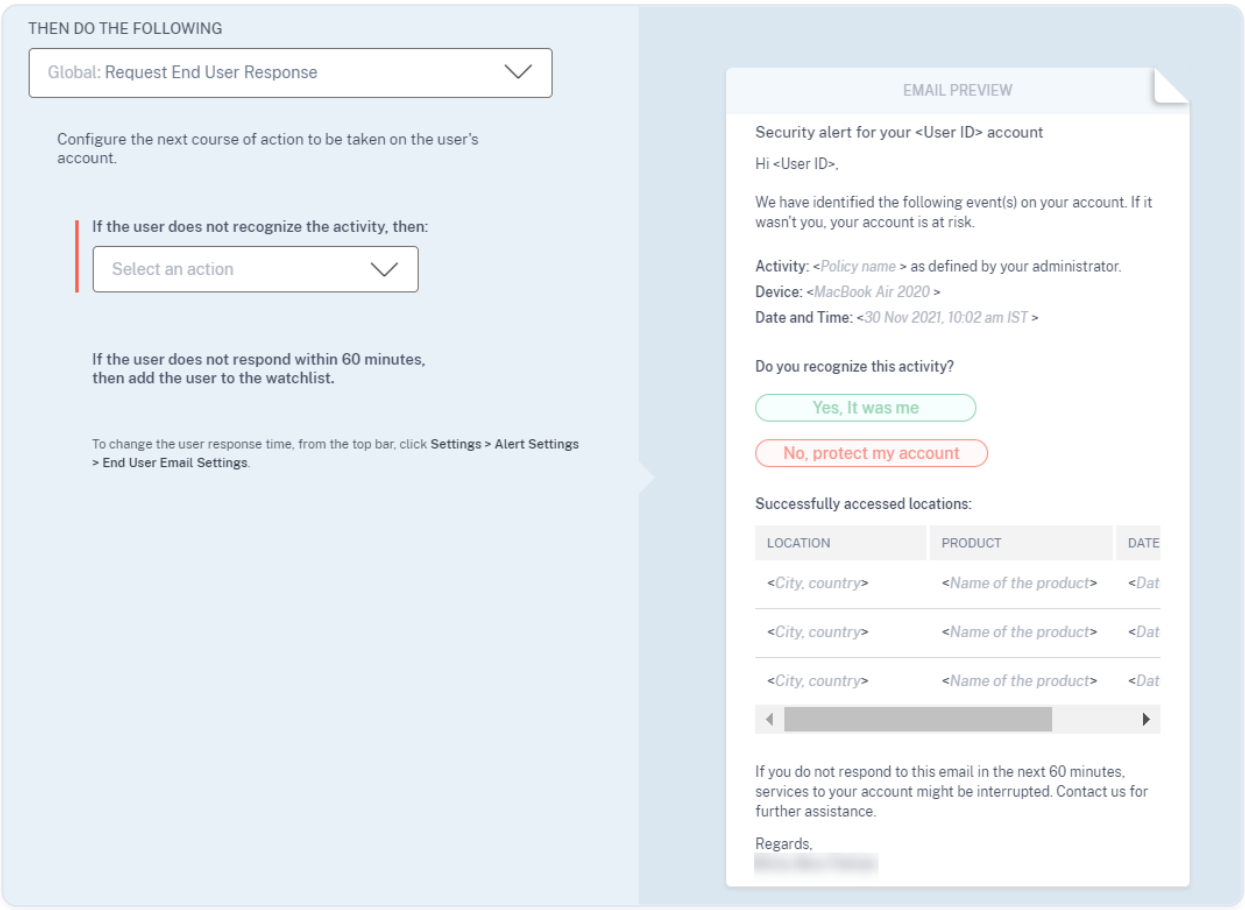


- **Default and custom risk indicators**: The conditions menu on the **Create Policy** page is now segregated based on default and custom risk indicators. When creating a policy, you can switch between the default and custom risk indicators tabs, and set the risk indicator conditions.

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

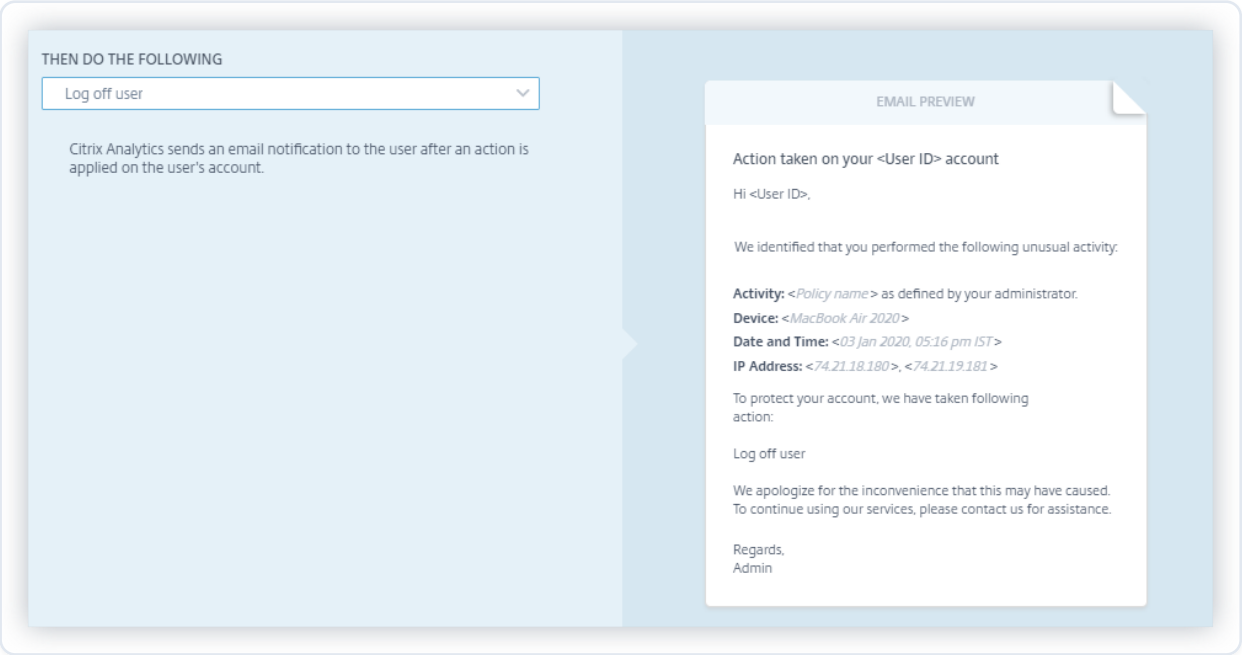


- **Request end user response**: Citrix Analytics introduces the **Request end user response** action. Using this action, you can send an email notification to the user regarding the risky activity detected. Once the user responds about the activity, you can determine the next course of action to be taken on their account. You can also set the user response time. If no response is received, Citrix Analytics considers **No response** as the status.



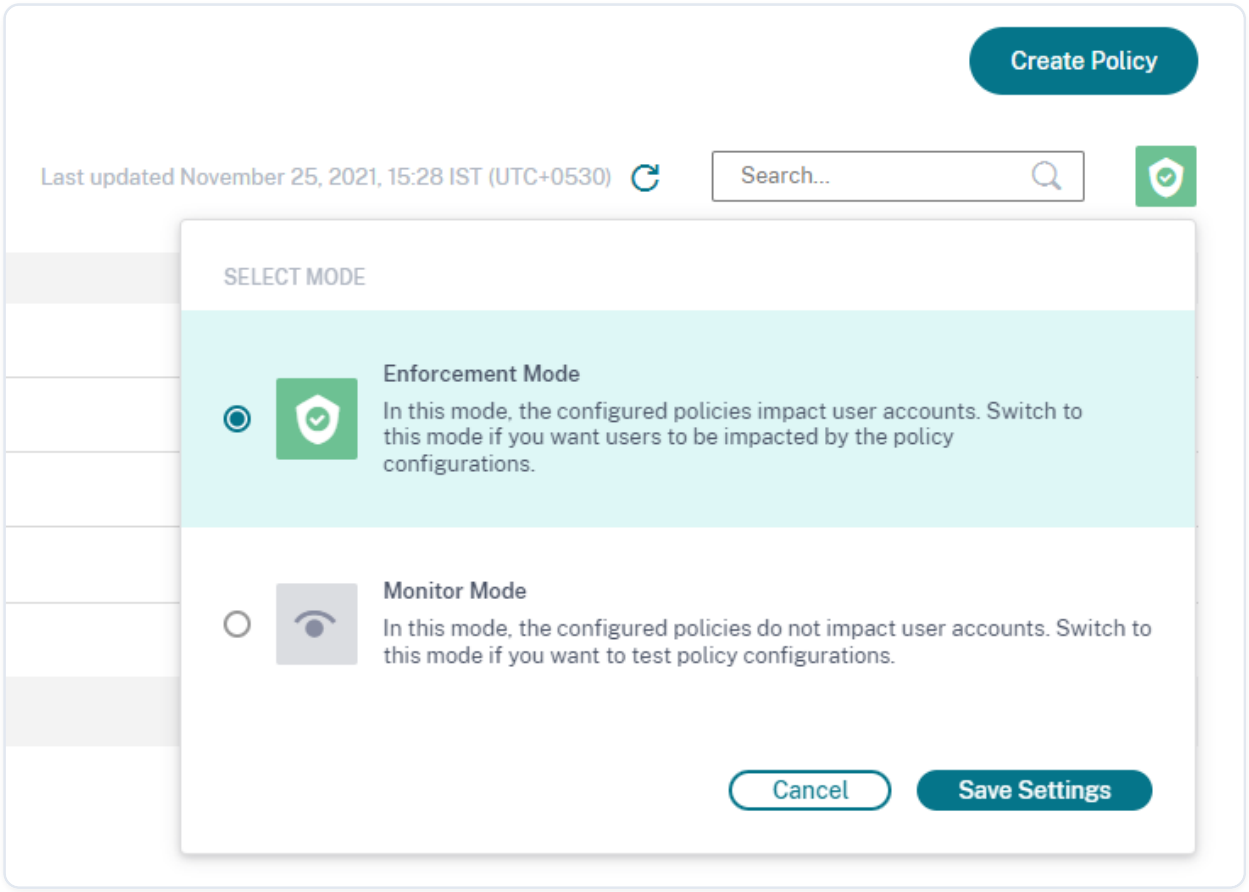
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Apply disruptive actions**: You can notify the users when a disruptive action such as **Log off user** or **Lock user**, is applied. A notification is sent to the user with details of the activity and the action applied. This action temporarily disrupts services to the user's account to prevent further misuse. To continue accessing the account, the user must contact the administrator for assistance.



- **Enforcement and monitor modes**: You can set enforcement or monitor modes to your policies.

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



For more information on policy enhancements, see Policies and actions.

Lock user and Unlock user actions

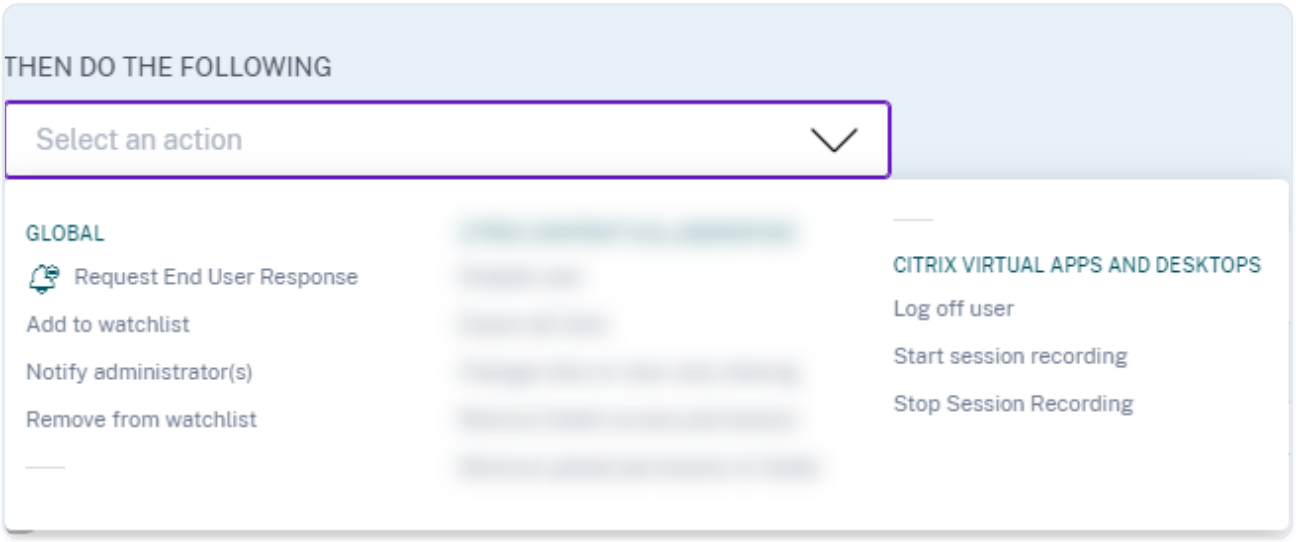
Citrix Analytics introduces the following Gateway actions:

- Lock user
- Unlock user

You can apply these actions either manually or when you configure policies.

For more information, see What are actions.

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



Access summary dashboard

Citrix Analytics introduces the **Access Summary** panel on the **Users** dashboard. It summarizes the total number of attempts that users have made to access the resources within an organization.

For more information, see Access summary.

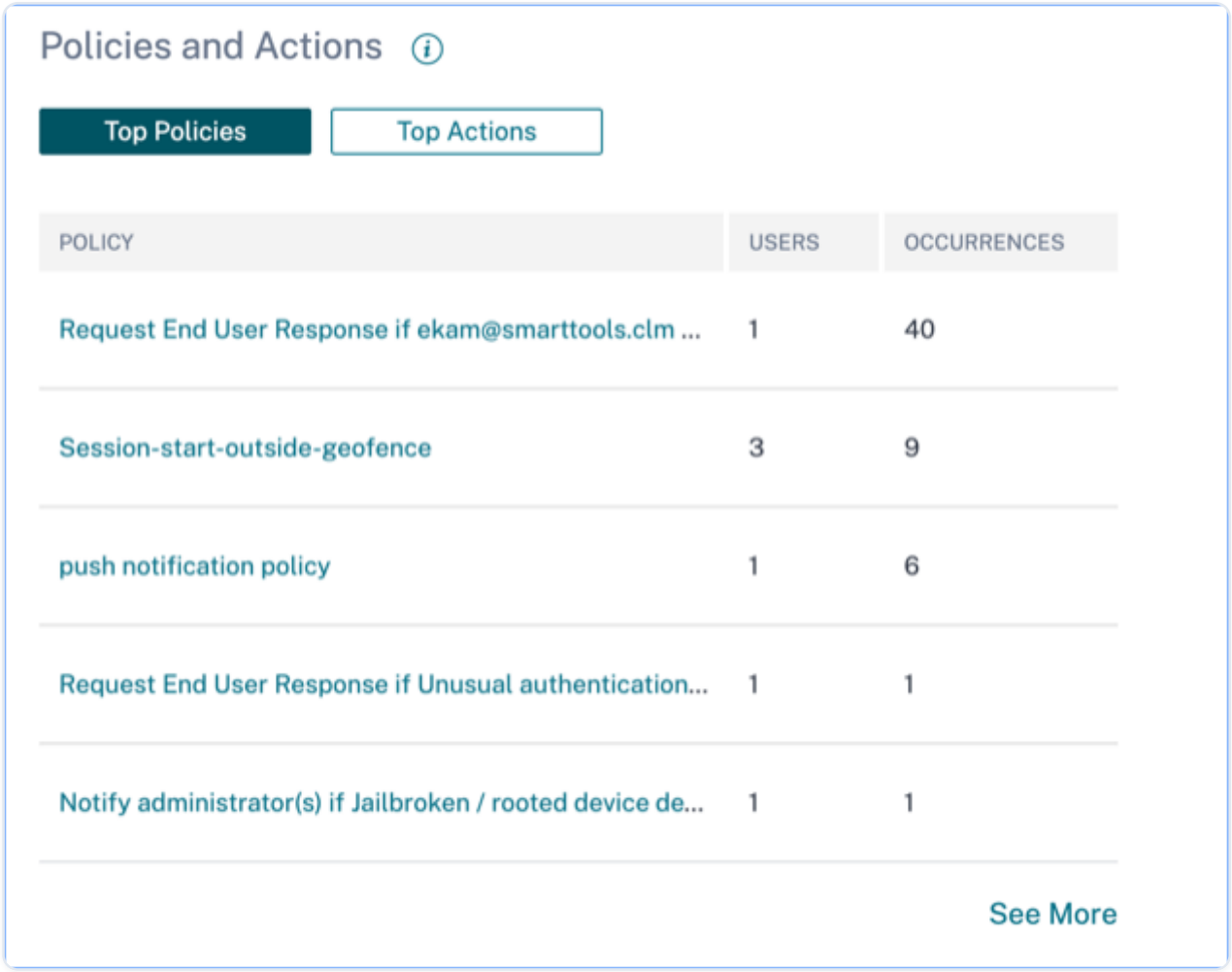


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policies and actions dashboard

Citrix Analytics introduces the **Policies and Actions** panel on the **Users** dashboard. It displays the top five policies and actions applied on user profiles. You can sort data based on the top policies and the top actions for a selected time period.

For more information, see Policies and actions.



Self-service search for policies

Use the self-service search to view the user events that met your defined policies. You can also view the actions that Analytics has applied for these anomalous events. Use the facets and the search box to search for the required events.

To view the events, in the search box, select **Policies** from the list, select the time period, and then click **Search**.

For more information, see Self-service search for Policies.

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

Deprecated features

Risk score change policy-based condition removed

When you configure policies, you cannot use the **Risk score change** policy-based condition anymore. Citrix Analytics does not support this condition.

For more information, see Policies and actions.

Multiple policy-based actions removed

When you configure policies, you cannot apply multiple actions anymore. Citrix Analytics supports only one action for each policy.

For more information, see Policies and actions.

Fixed issues

- Delegated read-only administrators encounter an error while accessing the **User Access** and **App Access** dashboards.

December 12, 2019

New features

Splunk version support

Citrix Analytics supports the following versions of Splunk:

- **Splunk 8.0 64-bit**
- **Splunk 7.3 64-bit**

To get the maximum security benefits of Splunk integration, upgrade to the latest version of the Splunk add-on app from the Download page.

For more information on supported Splunk versions, see Supported versions.

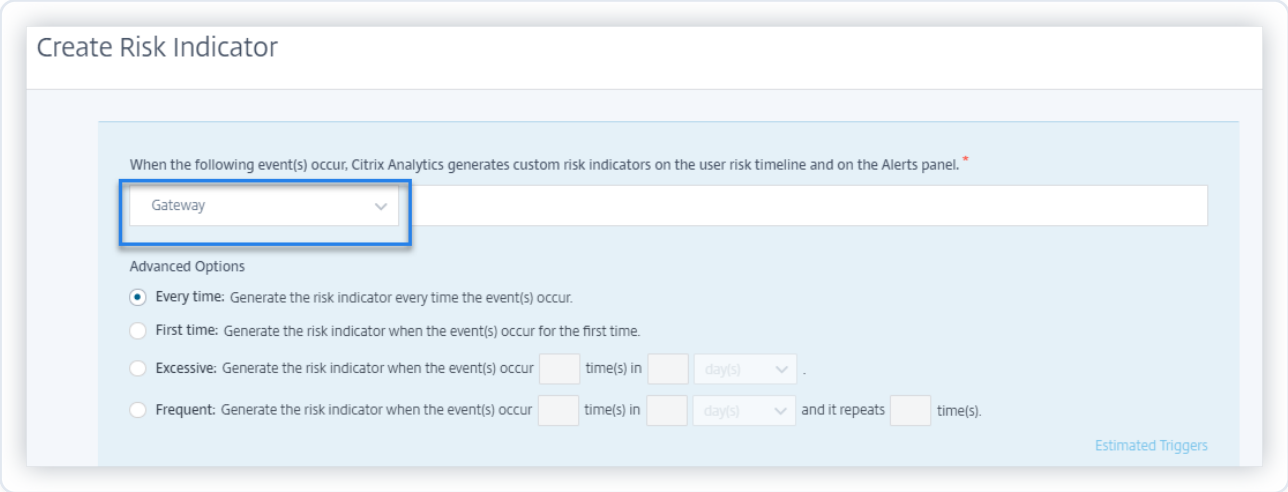
© 1997–2026 Citrix Systems, Inc. All rights reserved.

December 04, 2019

New features

Custom risk indicator for Citrix Gateway

Using custom risk indicators, you can now define the conditions and the frequency for triggering risk indicators for Citrix Gateway events. When a user event meets the conditions, Analytics triggers the risk indicators. For more information on how to create custom risk indicator, see Custom risk indicators.



November 22, 2019

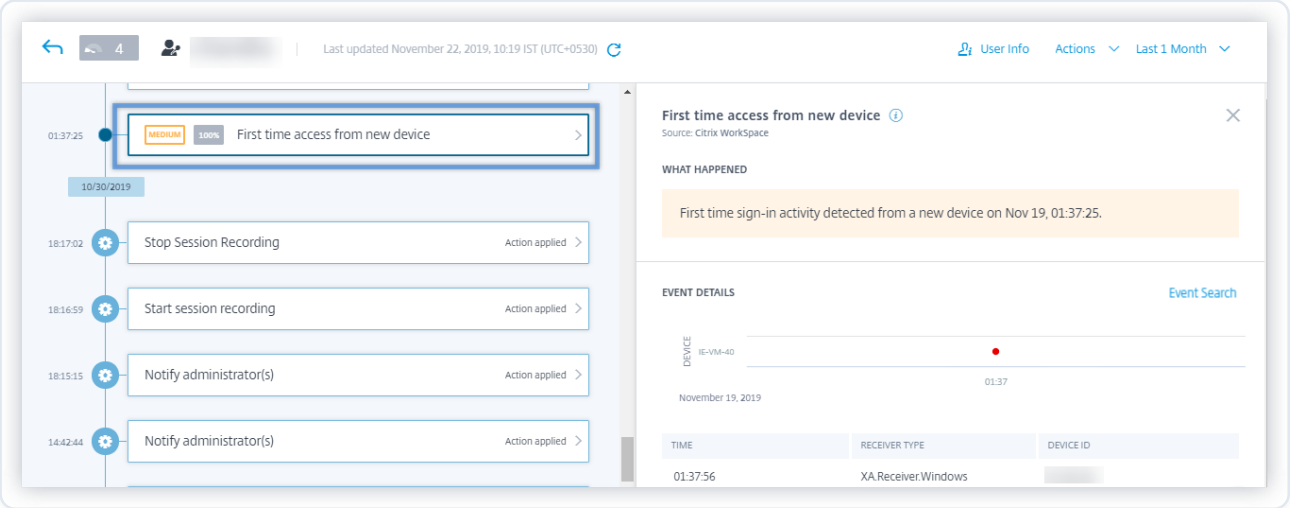
New features

First time access from new device – Citrix Virtual Apps and Desktops risk indicator

Citrix Analytics detects access threats based on access from a new device and triggers the corresponding risk indicator.

The **First time access from new device** risk indicator is triggered when a user signs in from a device after 90 days. This event is triggered because Citrix Receiver has no sign-in records from this new or unfamiliar device for the last 90 days. For more information, see Citrix Virtual Apps and Desktops and Citrix DaaS risk indicators.

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

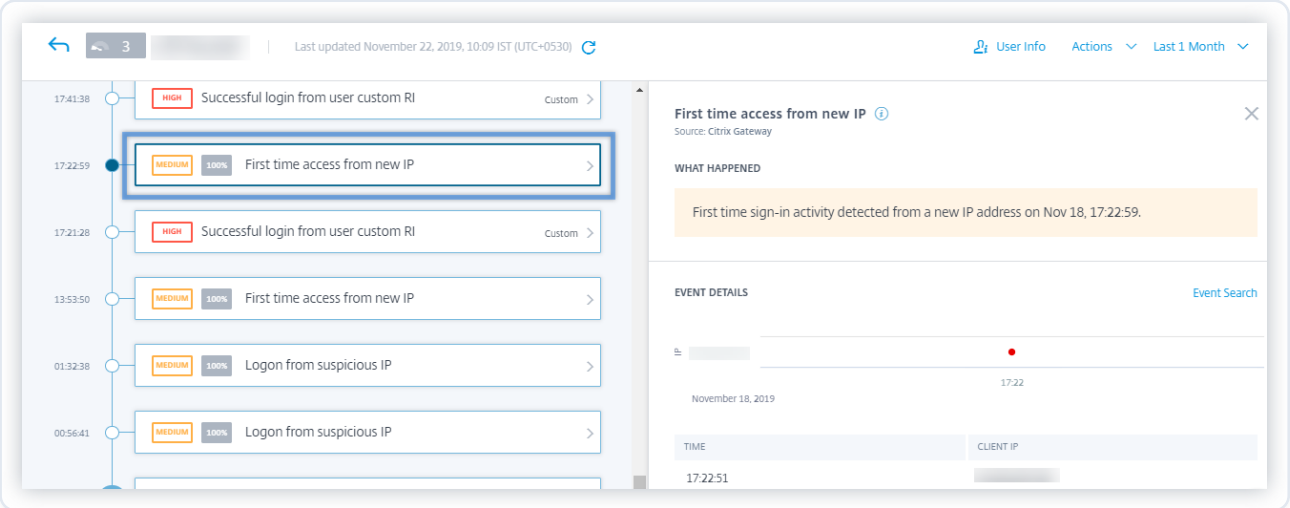


First time access from new IP - Citrix Gateway risk indicator

Citrix Analytics detects access threats based on access from a new IP address and triggers the corresponding risk indicator.

The **First time access from new IP** risk indicator is triggered when a user signs in from an IP address after 90 days. This event is triggered because Citrix Receiver has no sign-in records from the new or unfamiliar IP address for the last 90 days.

For more information, see Citrix Gateway risk indicators.



Logon from suspicious IP - Citrix Gateway risk indicator

Citrix Analytics detects user access threats based on the suspicious IP sign-in activity and triggers the **Logon from suspicious IP** risk indicator.

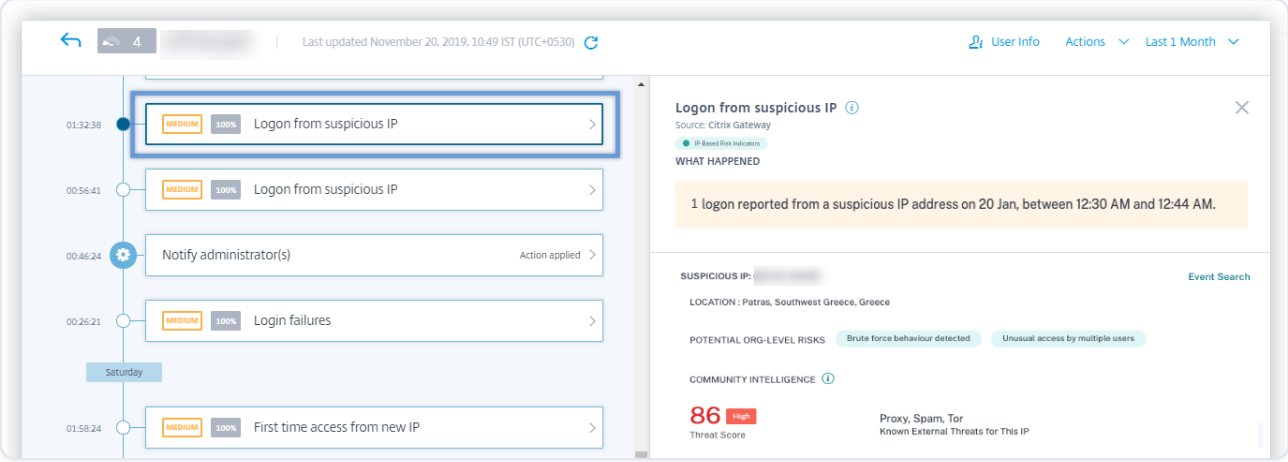
This risk indicator is triggered when a user attempts to access the network from a suspicious IP address. Analytics considers an IP address as suspicious based on any of the following conditions:

- Is listed on the external IP threat intelligence feed

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

- Has multiple user sign-in records from an unusual location
- Has excessive failed sign-in attempts that might indicate a brute-force attack

For more information, see Citrix Gateway risk indicators.



Self-service search for Citrix Gateway events

Use the self-service search feature to get insight into user events received from the Citrix Gateway data source. Citrix Analytics receives events such as authentication stage, authorization type, VPN session code, VPN session state for Citrix Gateway users. Use the facets and the search box to search for the required events and explore the underlying data.

To view the events, in the search box, select **Gateway** from the list, select the time period, and then click **Search**.

For more information, see Self-service search for Gateway.

Self-service search for Citrix Remote Browser Isolation™ events

Use the self-service search feature to get insight into the browsing events received from the Citrix Remote Browser Isolation Service. Citrix Analytics receives events such as session connect, session launch, published applications, deleted applications for each user connection. Use the search box to search for the required events and explore the underlying data.

To view the events, in the search box, select **Remote Browser Isolation** from the list, select the time period, and then click **Search**.

For more information, see Self-service search for Remote Browser Isolation.

Remove from watch list action

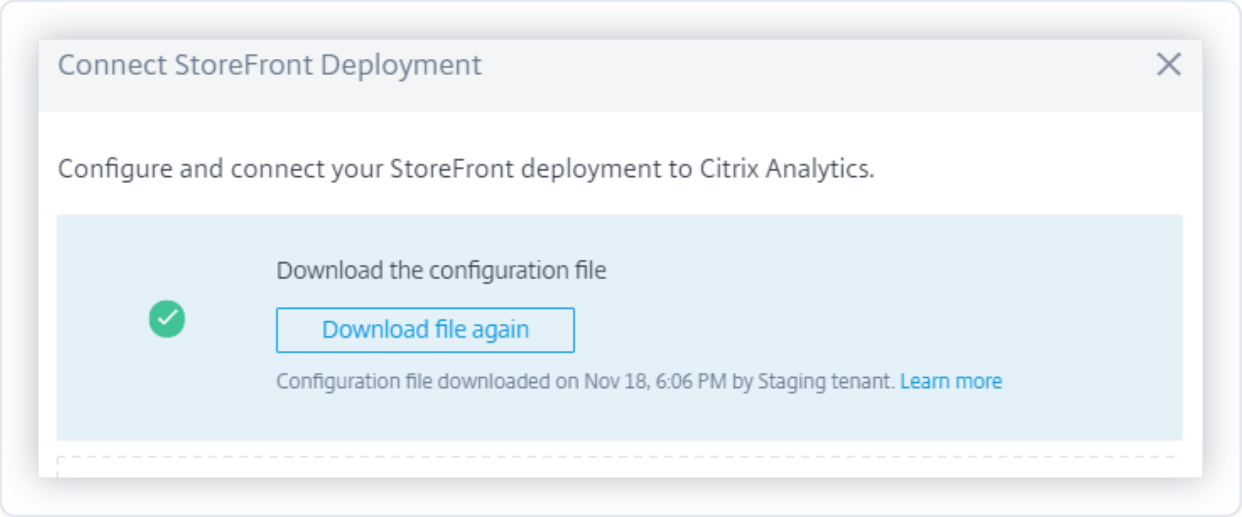
You can remove a user from the watchlist either by applying the manual method or by applying a policy-based method. For more information, see Watchlist.

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

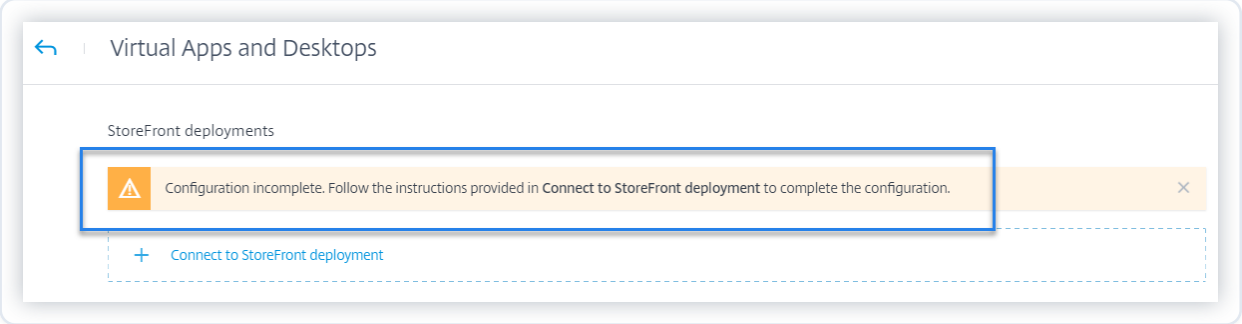
Improved onboarding messages when configuring a StoreFront deployment

Citrix Analytics now provides the following messages to help you configure your StoreFront deployments:

- After downloading the configuration file, you can see a message indicating the date and time of the download and the user name. When you refresh this page, the **Download file** button changes to **Download file again**.



- If your StoreFront configuration is incomplete, you see a warning message instructing you to follow configuration steps and connect your StoreFront deployment with Analytics.



For more information on how to configure your StoreFront deployment, see Onboard Citrix Virtual Apps and Desktops on-premises sites using StoreFront.

Deprecated features

Risk indicator - Access from new device remove

Citrix Analytics no longer triggers the **Access from new device** risk indicator. However, on the user dashboard, user timeline, and the policy dashboard, you can view historic data related to this risk indicator.

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

For previously created policies based on **Access from new device**, you must either modify the policy or create a policy with the new risk indicator **First time access from new device**.

Fixed issues

- The self-service search for authentication fails to display the events.

November 08, 2019

Fixed issues

- For Citrix Content Collaboration risk indicators, users are unable to apply actions on the risk timeline.
- Citrix Workspace app for Chrome prior to version 1911 fail to send event details to Citrix Analytics.

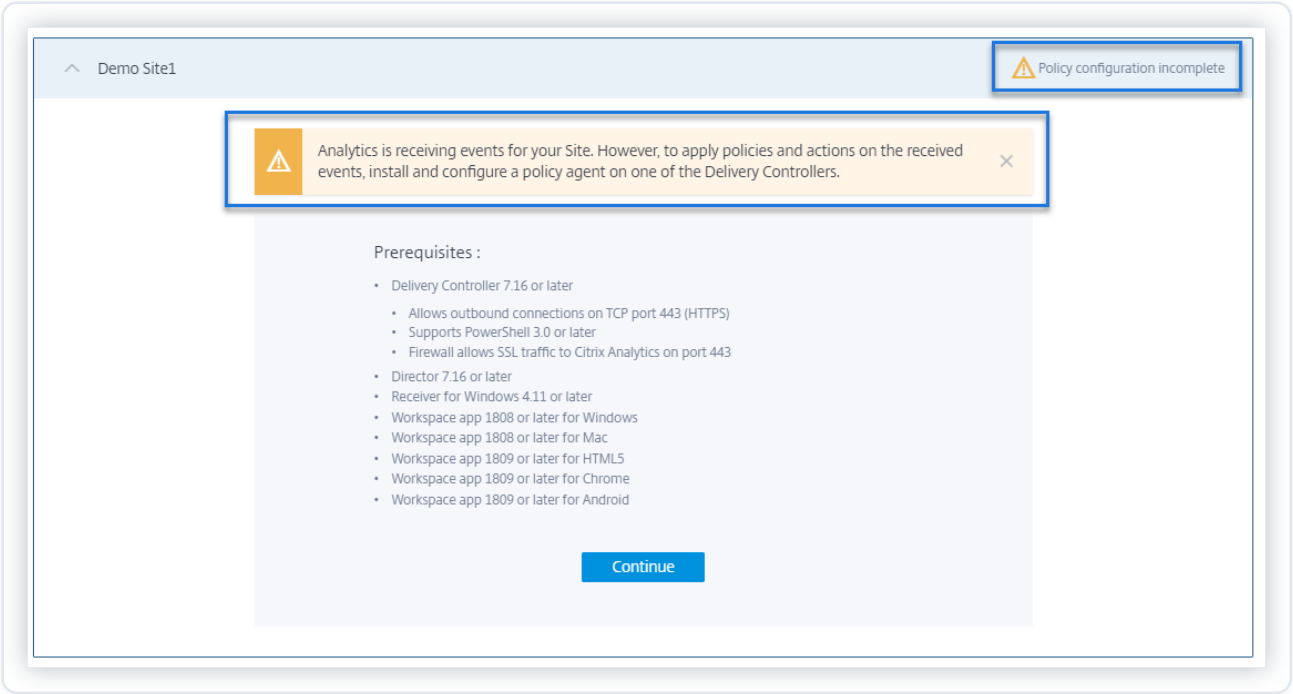
October 21, 2019

New features

Modified name for analytics agent

The agent name is now mentioned as **Analytics policy agent** on the user interfaces to indicate its role. When onboarding the on-premises Citrix Virtual Apps and Desktops data sources, Citrix Analytics clearly notifies that a policy agent is required only to configure policies and actions for your Site. This agent has no role in transmitting data from the data source. For more information, see Citrix Virtual Apps and Desktops and Citrix DaaS data source.

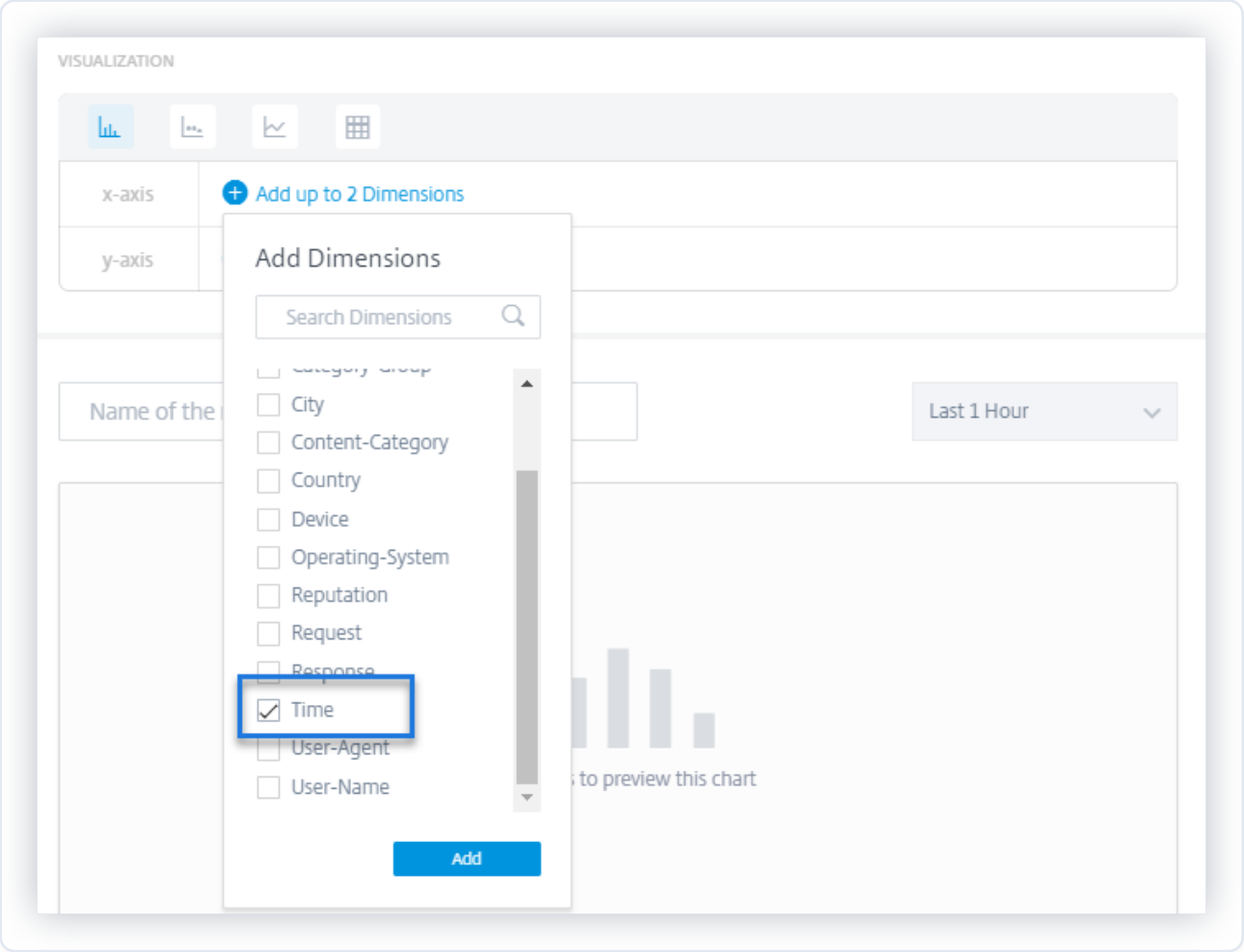
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Support for the time dimension for custom report

You can now group the events based on time by selecting the **Time** dimension for the x-axis. The report displays the total events received based on the time intervals for the selected period. For more information on how to create reports, see Custom reports.

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

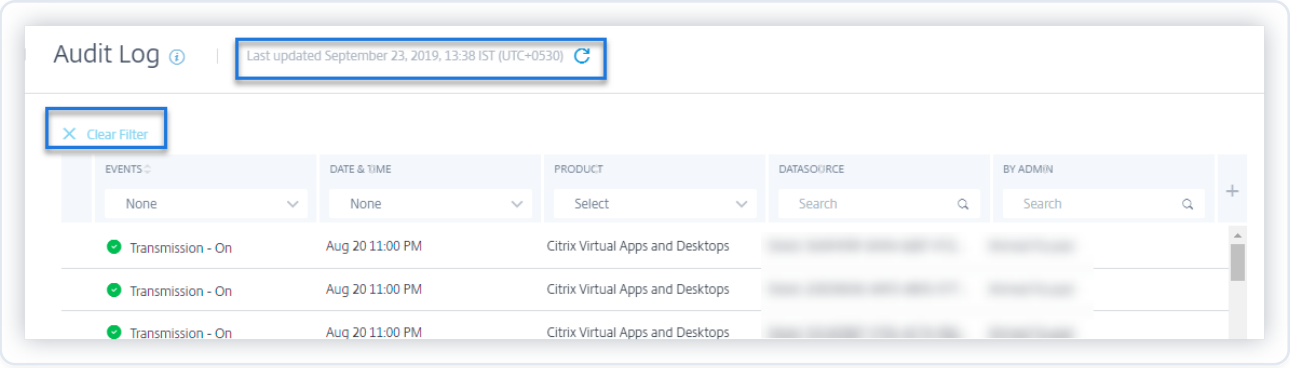


Audit logs enhancements

The user experience of the **Audit Log** page is enhanced.

- You can view the date and time details when the **Audit Log** page was last updated and refresh the page to view the latest audit logs.
- You can clear all the filters that were applied on the audit logs.

For more information on the audit data, see Audit logs.



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

Fixed issues

- Citrix Analytics is unable to generate the **Anonymous IP address** risk indicator even though Microsoft Graph Security is successfully onboarded.
- Citrix Workspace app for HTML5 prior to version 1910 fail to send event details to Citrix Analytics.

September 23, 2019

Fixed issues

- On the data sources site cards, the **Latest event** field displays incorrect date and time information.

August 30, 2019

New features

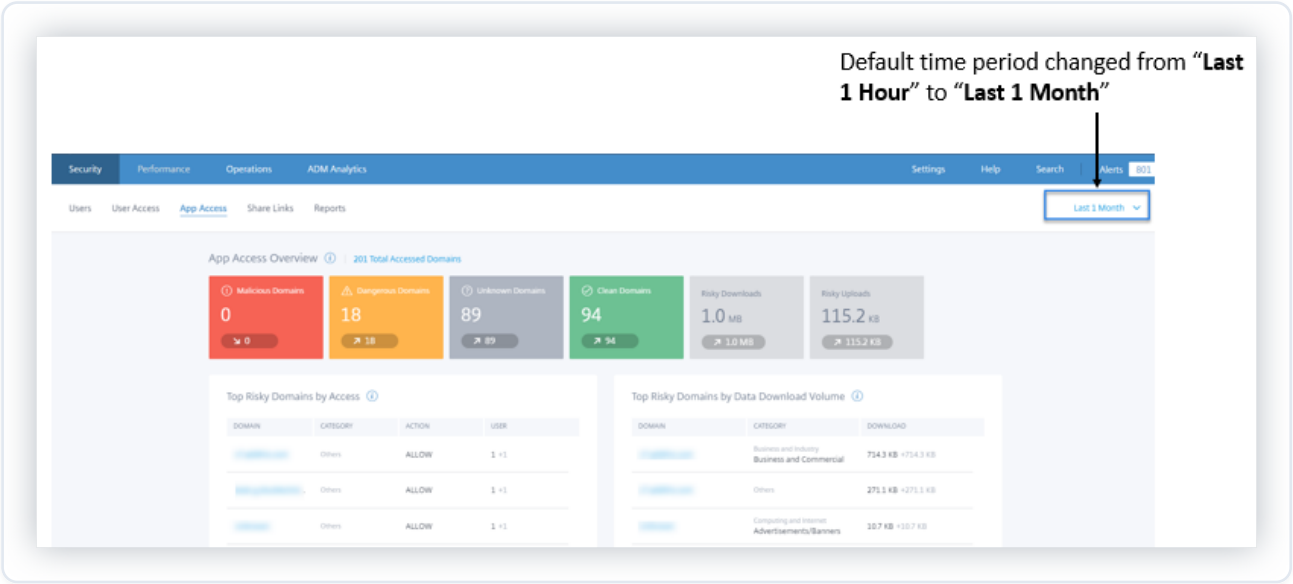
Change in default time period across dashboards

The default time period on the following dashboards is changed from **Last 1 Hour** to **Last 1 Month**:

- Users
- Risk Timeline
- User Access
- App Access
- Share Links
- Alerts History

Now the dashboards display the events for the last one month by default. You get a more engaging experience while using these dashboards. For example, when you open the **App Access** dashboard, the dashboard displays the app access events for the last one month by default.

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



Fixed issues

- For Content Collaboration risk indicators, the **Disable user** policy-based action cannot be applied successfully.
- Citrix Analytics cannot process events from Citrix Gateway 13.0. This issue occurs because Citrix Gateway 13.0 fails to provide user names in the logon events sent to Citrix Analytics.

August 20, 2019

New features

Self-service search enhancements

- The user experience of the self-service page is enhanced. You can now seamlessly switch back and forth between the user risk timeline and the self-service search page.
- You can now sort your events by time. By default, the latest events appear first in the event table. Click the sort icon on the **TIME** column to sort the events based on either latest time or earliest time.

For more information on how to use self-service search, see Self-service search.

Custom report enhancements

- New dimensions are added for the Access Control, Content Collaboration, and Apps and Desktops data sources. You can choose these dimensions to create reports. The following dimensions are added for the data sources:
    - **Access Control**: User Agent, User Name

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

    - **Content Collaboration**: User Email, User Name, Created by, Account Id, OAuth Client Id, Event Id, Folder Id, Folder Name, Resource Id, Form Id, Client IP
    - **Apps and Desktops**: User Name, IP Address, Device Id, Jail Broken, Session Launch Type, Session Server Name, Session User Name, Download File Name, Download File Path, Printing Printer Name, Printing Job Details File Name, SaaS App Launch URL, Clipboard Operation, Clipboard Details Result

- The custom report user interface is enhanced with support for pagination and a **Clear All** option for the filters.

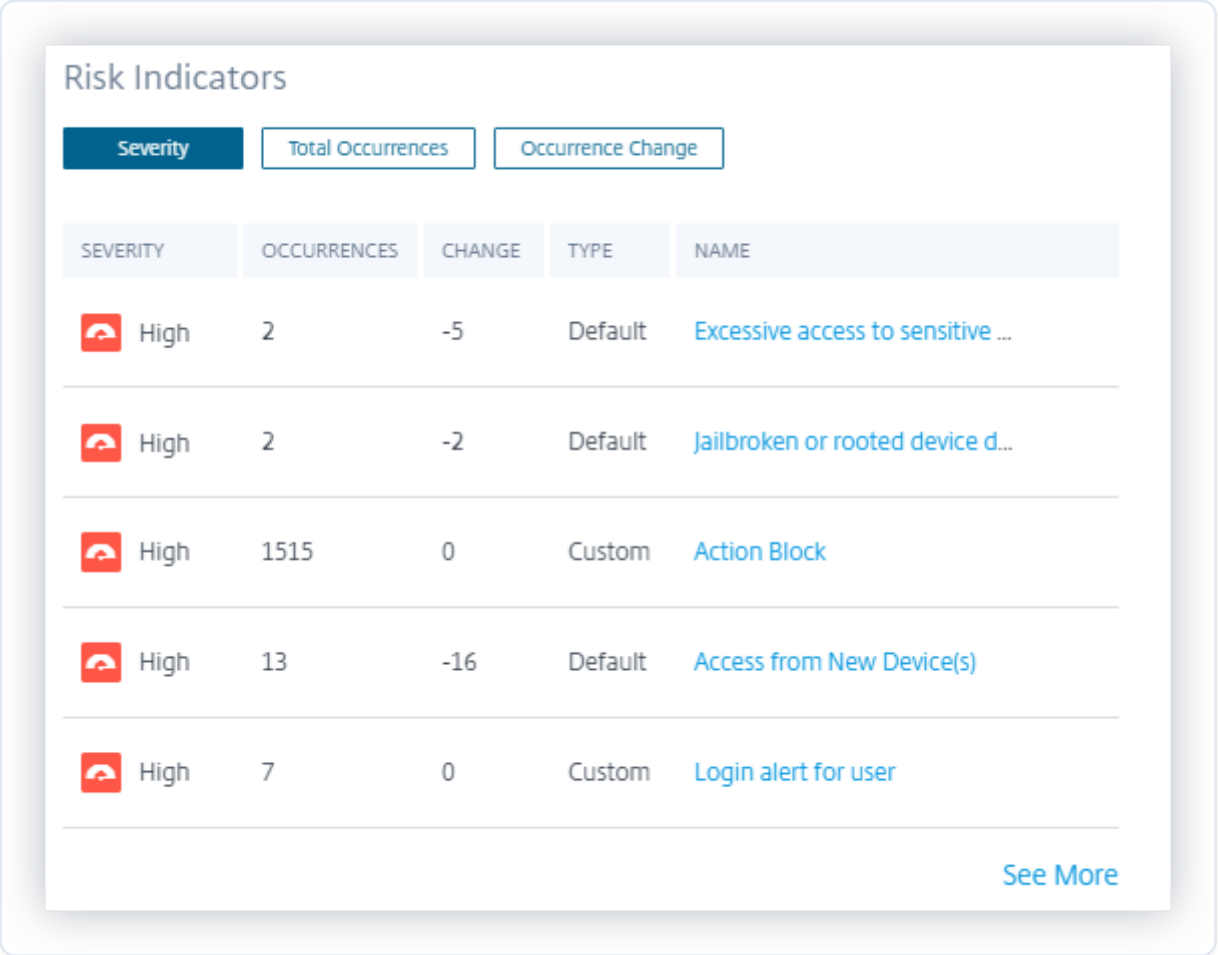
For more information on how to create a custom report using these dimensions, see Custom reports.

Risk Indicators dashboard

The **Risk Indicators** dashboard is introduced on the **Users** page. It summarizes the top five default and custom risk indicators for a user. A See More link redirects you to the **Risk Indicator Overview** page. This page provides detailed information about the risk indicators generated for a selected time period.

For more information, see Users dashboard.

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



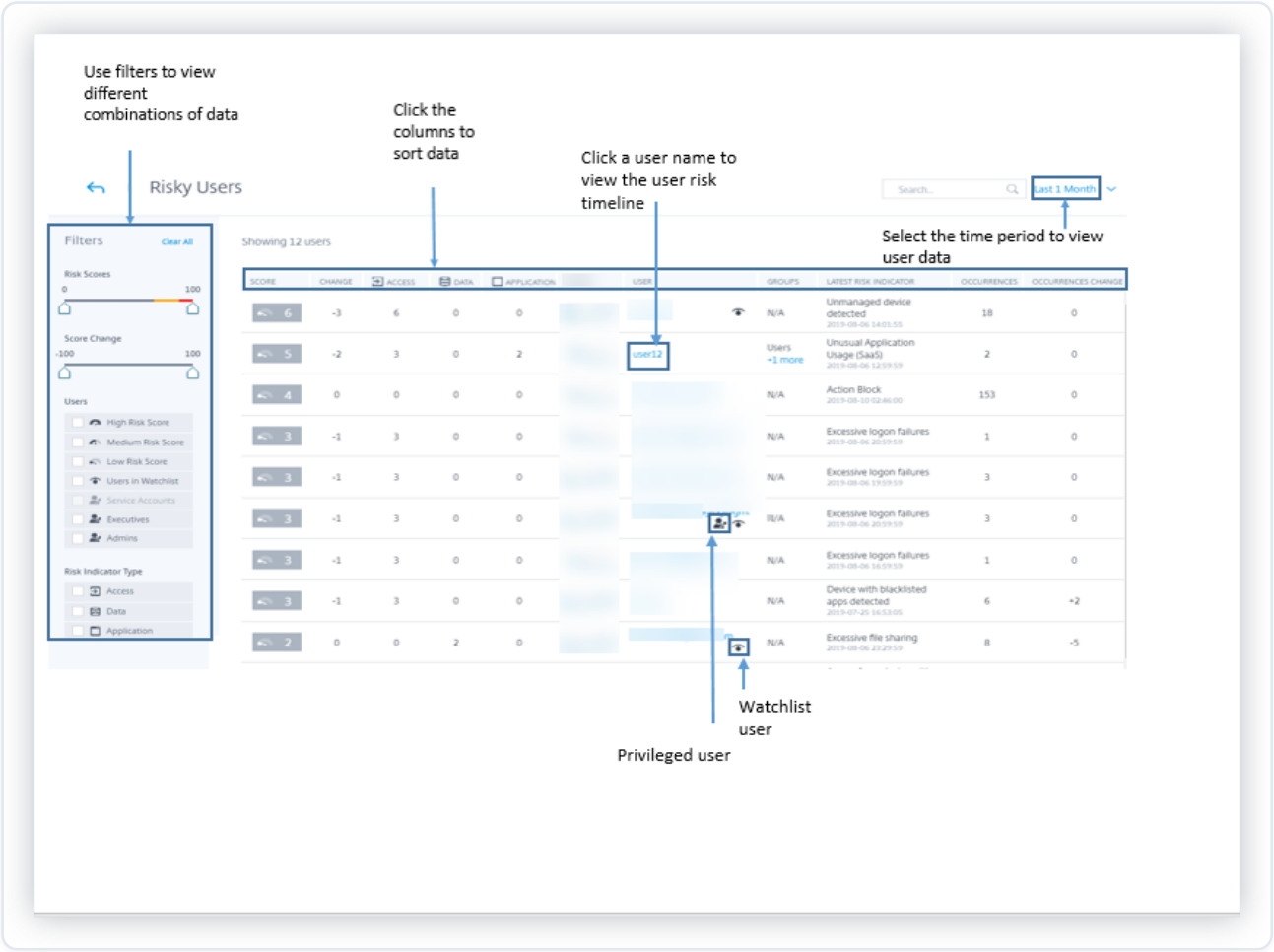
Risky Users dashboard enhancements

Citrix Analytics introduces the **Risk Indicators** and **Risk Indicators Change** tabs on the **Risky Users** dashboard. You can view the top five risky users based on these tabs. The dashboard also introduces the **Risk Indicators** column. It shows the number of risk indicators for a user.

The **Risky Users** page introduces the **Occurrences** and **Occurrences Change** columns. These columns summarize the total occurrences and the change in occurrences of the custom and the default risk indicators.

For more information, see Users dashboard.

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



Share link risk indicator - Excessive downloads

Citrix Analytics detects access threats based on excessive downloads on a share link and triggers the **Excessive downloads** risk indicator. By identifying share links with excessive downloads, based on previous behavior, you can monitor the share link for potential attacks. This risk indicator helps you identify an excessive file download activity.

For more information, see Excessive downloads.

Self-service search for the Authentication data

Use self-service search to get insights into the authentication events. Citrix Analytics receives the authentication events such as user login, user logoff, and client update from the Identity and Access Management service of Citrix Cloud. The search provides a detailed report on the authentication events, helps you to identify any authentication issues, and troubleshoot them. You can also define a search query to retrieve events that match your defined criteria.

To view the events, select **Authentication** from the list, select the time period, and then click **Search**.

For more information, see Self-service search for Authentication.

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

July 11, 2019

New features

Custom risk indicators

The default risk indicators that Citrix Analytics generates are based on machine learning algorithms. Citrix Analytics now allows you to create custom risk indicators. Based on user events, you can define the conditions and create custom risk indicators.

When the defined conditions are met, Citrix Analytics generates the custom risk indicators similar to default risk indicators, and displays them on the user's risk timeline. Custom risk indicators are denoted with a label on the user's risk timeline.

For more information, see Custom risk indicators.

Privileged status on risk timeline

The user risk timeline displays the following events whenever there is a change in the Admin or Executive privilege status of a user:

- Added to Executive group
- Removed from Executive group
- Privilege elevated to Admin
- Admin privilege removed

When a risk indicator is triggered for a user, you can co-relate it with the specified privilege status change event. If necessary, you can apply appropriate actions on the user profile.

For more information, see User risk timeline.

Expire share link action

Citrix Analytics enables you to apply actions on share link risk indicators. Currently, the supported action is **Expire share link**.

For more information, see Citrix share link risk indicators.

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

Self-service search enhancements

- **Support for wild card character * in search query**: Use the asterisk (*\) character in your search query to match any character zero or more times. For example, the search query User-Name = "John*" displays events for the all user names that begin with John.
- **Added the Clear All option for facets**: Click **Clear All** to remove all the selected facets at a time.
- **View hidden column data in the event list**: After removing a column from the event table, you can view the corresponding data in the user event list. Expand the event row for a user and view the data.

For more information, see Self-service search.

Data error status on the site cards

The Site cards display the **No data received** label in red when Citrix Analytics does not receive events for the last one hour from the data source. It also displays the number of events received and is linked to the corresponding self-service search page. This feature helps you view the corresponding events on the self-service search page and check for any data transmission issues.

NOTE

Currently, self-service search is available only for the Access, Content Collaboration, and Apps and Desktop data sources.

For more information, see Enable Analytics on Citrix data sources.

Fixed issues

- For the Access Control data source, the number of events on the site card does not match the self-service search results.

June 19, 2019

Fixed issues

- The **Audit Log** page displays the data transmission on or off status every time the Active Directory data source is discovered.
- The time period menu on the **Users** dashboard does not load accurately. It displays a timeout error message.

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

- Users get an error message on Citrix Analytics while connecting to a tenant from Splunk. Occasionally, onboarding of new data sources fails.

June 17, 2019

New features

StoreFront configuration

If your organization uses on-premises StoreFront, you can now configure StoreFront to connect to Citrix Analytics. Configuration is performed using a configuration file imported from Citrix Analytics. After the configuration is successful, Citrix Workspace app sends user events to Citrix Analytics for generating actionable insights into user behaviors. The insights help you to detect any anomalous user behaviors and proactively handle security threats in your organization. For more information, see Onboard Citrix Virtual Apps and Desktops on-premises sites using StoreFront.

May 30, 2019

New features

Excessive logon failures

Citrix Analytics detects access threats based on excessive logon activity and triggers the Excessive logon failures risk indicator. This risk indicator is triggered when a user experiences multiple failed logon attempts to access Content Collaboration. By identifying users with excessive logon failures, based on previous behavior, administrators can monitor the user's account for brute force attacks.

NOTE

Excessive logon failures is now renamed as **Excessive authentication failures**.

Fixed issues

- For some user events transmitted by Citrix Workspace apps, the data source is incorrectly identified as Endpoint Management instead of Citrix Virtual Apps and Desktops.

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

- The **Users** dashboard takes a long time to load for the **Last 1 Month** time period. This issue occurs when the number of users are high. In some instances, you might even encounter 601 errors.

- Citrix Content Collaboration is not discovered as a data source although some users subscribe to the service on Citrix Cloud.

May 09, 2019

New features

Creating custom reports

You can now create custom reports based on your operational requirements. Citrix Analytics provides a list of dimensions and metrics according to the selected data source. Choose the required parameters and the visualization types such as bar chart, event chart, line chart, or table to create your reports. Creating reports help you to organize and analyze your data graphically.

To create a custom report, from the **Security** tab, click **Reports** > **Create Report**. To view your previously created reports, from the **Security** tab, click **Reports**. For more information, see Custom reports.

Privileged user monitoring

Citrix Analytics enables you to closely monitor the behavior anomalies of privileged users in an organization. As privileged users are highly vulnerable to security threats, it becomes challenging to distinguish their daily activities from the malicious ones. Hence, the malicious activities of privileged users remain undetected for a long time. This feature enables you to proactively monitor such activities and take appropriate actions on the appropriate user accounts. Privileged users are represented with an icon on the **Users** dashboard.

Citrix Analytics supports monitoring for the following types of privileged users:

- **Admins** - Users who are assigned Admin privileges by the respective Citrix service. Currently, Citrix Analytics supports privileged user monitoring for users with Admin privileges in the Content Collaboration service.
- **Executives** - On Citrix Analytics, you can mark an AD group as an Executives group. Marking an AD group as an Executive group makes all the users in the group as privileged users. If

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

there is no need to further support the behavior anomalies of users in an AD group, you can remove the group as an Executive group.

For more information, see Privileged users.

Weekly email summary

Citrix Analytics sends a weekly email to the administrators summarizing the security risk exposures in their organization's IT environment. The email notification is sent every Tuesday to the administrators and it highlights the security events that have occurred in the previous week. This email ensures that the administrators are informed about the security risk exposures without signing in to Citrix Analytics. For more information, see Weekly email summary.

April 26, 2019

New features

Delegated administrators

Citrix Analytics now supports delegated administrator roles. This functionality enables you to invite other administrators to your Citrix Cloud account to manage Citrix Analytics for your organization. If you are a Citrix Analytics administrator with full access permission, you can add other administrators to your Citrix Cloud account. These additional administrators are called delegated administrators. You can currently assign read-only access to the delegated administrators. For more information, see Delegated administrators.

Fixed issues

Few risk indicators for the data sources that use data streaming do not generate alerts. You do not get any alert notifications and policy-based actions are not applied automatically if any one of the following risk indicators is triggered:

- **Citrix Endpoint Management risk indicators** - Unmanaged device, Jailbroken or rooted device, and Device with blacklisted apps.
- **Citrix Virtual Apps and Desktops risk indicator** - Access from device with unsupported operating system (OS).
- **Citrix Content Collaboration risk indicator** - Excessive access to sensitive files.

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

February 19, 2019

New features

Splunk integration

Citrix Analytics integrates with Splunk to enhance your security incident monitoring and troubleshooting experiences. This integration augments your existing data sources with the risk analysis capabilities and intelligence of Citrix Analytics for Security such as risk indicators, risk scores, and user profiles. Citrix Analytics exports risk analysis information to a channel. Splunk pulls the same from this channel.

Splunk integration involves configuration on Citrix Analytics, installation of the **Citrix Analytics Add-on for Splunk** app, and configuration of the app. Ensure to turn on data processing for at least one data source. It helps Citrix Analytics to begin the Splunk integration process.

For more information, see Splunk integration.

Dynamic session recording

Citrix Analytics introduces the ability to trigger session recording dynamically on the users' current Virtual Apps and Desktops sessions. It helps to capture evidences required for risk analysis and take appropriate incident response actions such as disconnect sessions and block user.

For more information, see Policies and actions.

Share Links dashboard and risk indicator

Citrix Analytics introduces the risk visibility to Share Links based on data collected from Citrix Content Collaboration. It helps you to understand the risk exposure of share links through the risk indicators that the share links trigger.

For more information, see Share Links dashboard.

Currently, the Anonymous sensitive share download risk indicator is triggered for a share link. When Content Collaboration detects this risky behavior, Citrix Analytics receives the events. You are notified in the **Alerts** panel and the Anonymous sensitive share download risk indicator is added to the share link's risk timeline.

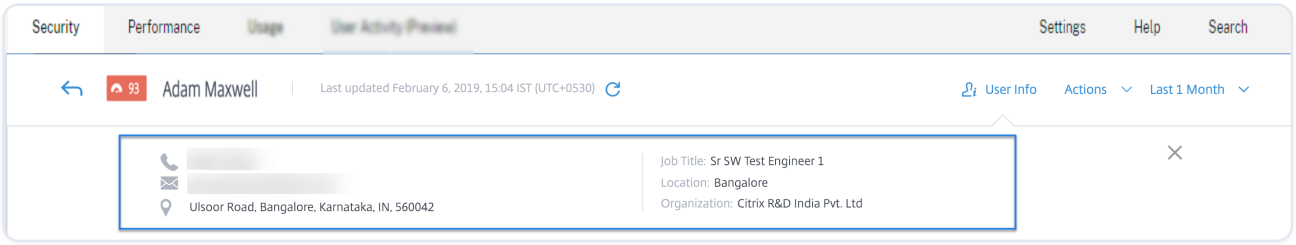
For more information, see Share Link risk timeline and Citrix Share Link risk indicators.

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

Microsoft Active Directory integration

You can now integrate Microsoft Active Directory with Citrix Analytics. This integration enhances the context of risky users with additional information such as job title, organization, office location, email, and contact details. You can get a better visibility of a user on the user profile page in Citrix Analytics.

For more information, see Integrate Analytics with Microsoft Active Directory.



January 04, 2019

New features

Addition of SOURCE column for existing risk indicators

The **SOURCE** column has been introduced in the **EVENT DETAILS** section for the following risk indicators:

- Excessive file uploads
- Excessive file downloads
- Excessive file sharing
- Excessive file or folder deletion

For more information, see Citrix Content Collaboration risk indicators.

Advanced user profile

The **User Info** view on the user profile has been enhanced. The **Trend View** link has been introduced at the top right corner of the **Application**, **Devices**, and **Data Usage** sections. The **Map View** link has been introduced at the top right corner of the **Locations** section. These links provide a graphic representation about the user's historical behavior during a specific time period. You can navigate to **User Info** from the user's risk timeline or from the **Data Sources** page.

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

NOTE

The **Authentication** and **Domains** data are currently not available on the User Info profile.

For more information, see User risk timeline and profile.



Microsoft Graph Security risk indicators

The onboarded Microsoft Graph Security can receive risk indicator details from one of the following security providers, and forwards it to Citrix Analytics:

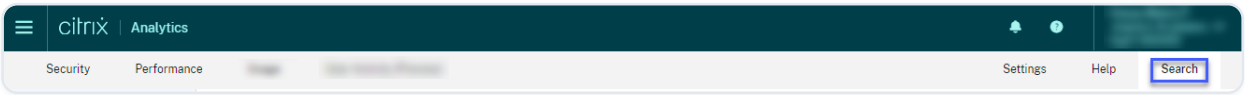
- Azure AD Identity Protection
- Microsoft Defender for Endpoint

For more information, see Microsoft Graph Security risk indicators.

Ways to enter the self-service search page

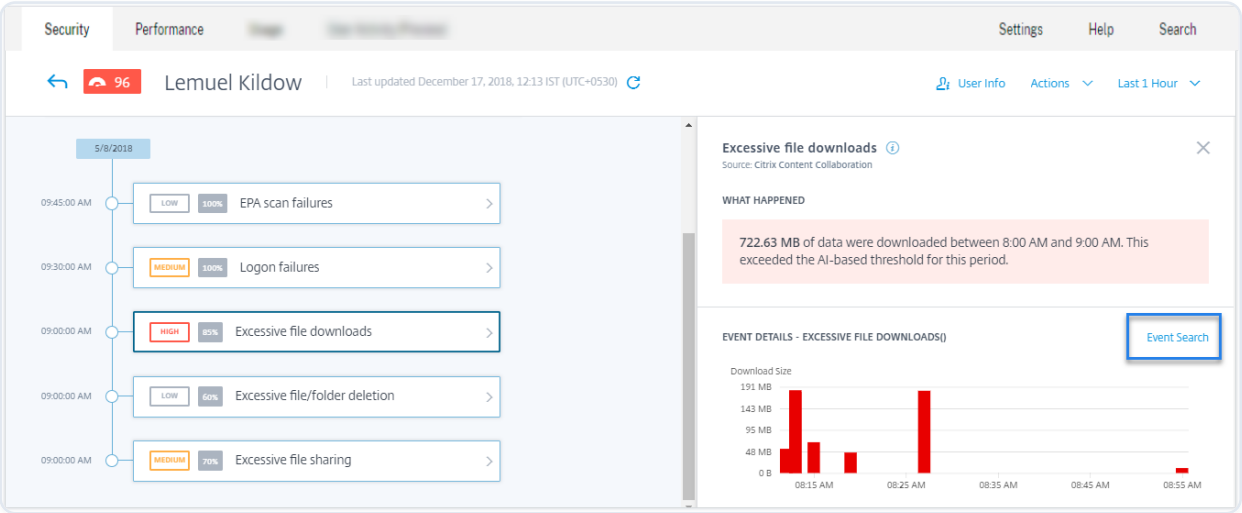
You can now access the self-service search page using the following options:

- **Top bar**: Click **Search** on the top bar to directly access the search page.



- **Risk timeline on user profile page**: Click **Event Search** to access the search page and view the events corresponding to a specific user's risk indicator and the data source. For more information, see Self-service search.

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



Self-service search for Content Collaboration

Use self-service search to get insight into the events associated with the Content Collaboration data source. To view the events, select **Content Collaboration** from the list, select the time period, and then click **Search**. For more information, see Self-service search for Content Collaboration.

Self-service search for Apps and Desktops

Use self-service search to get insight into the events associated with the Apps and Desktops data source. To view the events, select **Apps and Desktops** from the list, select the time period, and then click **Search**. For more information, see Self-service search for Apps and Desktops.

Export self-service search events to CSV file

You can now export the self-service search events to a CSV file and download the file for future use. For more information, see Self-service search.

Improved onboarding for Citrix Virtual Apps and Desktops

The onboarding process for the Citrix Virtual Apps and Desktops data source is now improved to provide a better user experience. The site cards and the on boarding steps have been modified. For more information, see Citrix Virtual Apps and Desktops and Citrix DaaS data source.

November 29, 2018

New features

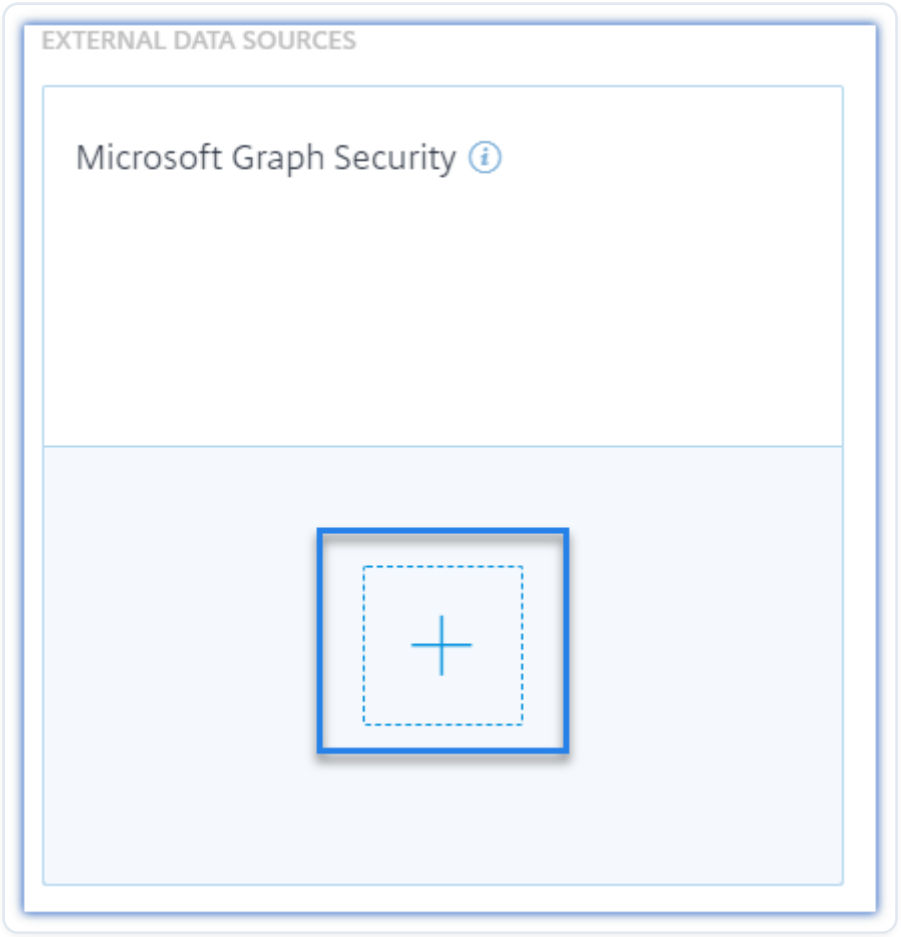
Microsoft Security Graph data source

Microsoft Graph Security is an external data source that aggregates data from multiple security providers. It also provides access to the user inventory data.

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

Citrix Analytics currently supports the **Azure AD identity protection** and **Microsoft Defender for Endpoint** security providers associated with this data source.

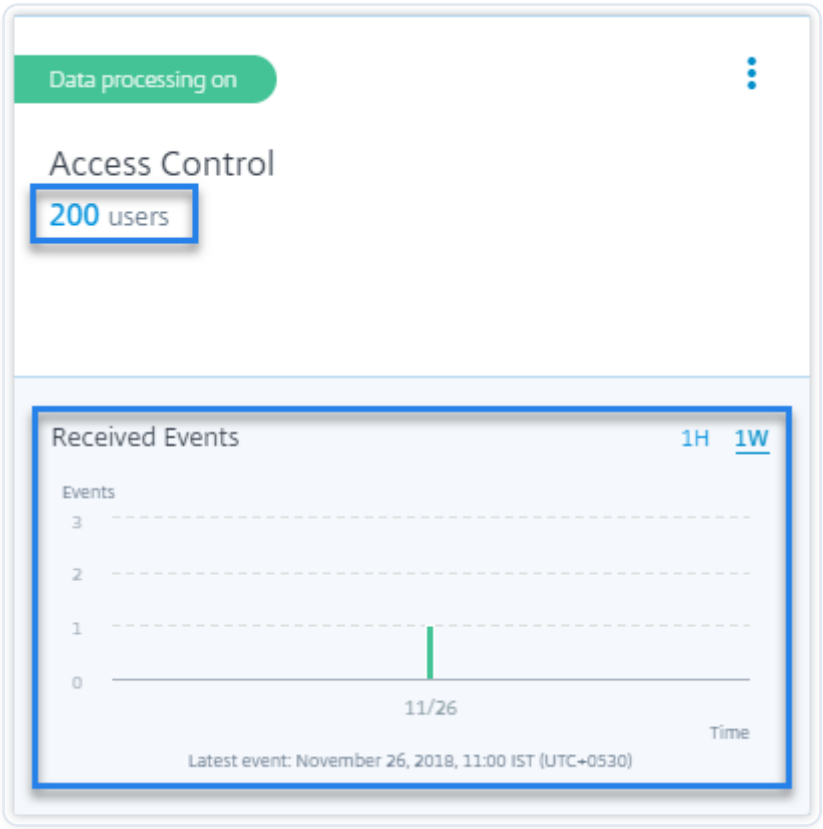
To onboard this data source, you must obtain permissions from the Microsoft identity platform. For more information, see Microsoft Graph Security.



View event details and discovered users on the site cards for data sources

The site cards for the data sources now display event details and the number of users. For example, you can view the event details and the users for Access Control on the site card. For more information, see Enable Analytics on data sources.

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



November 16, 2018

New features

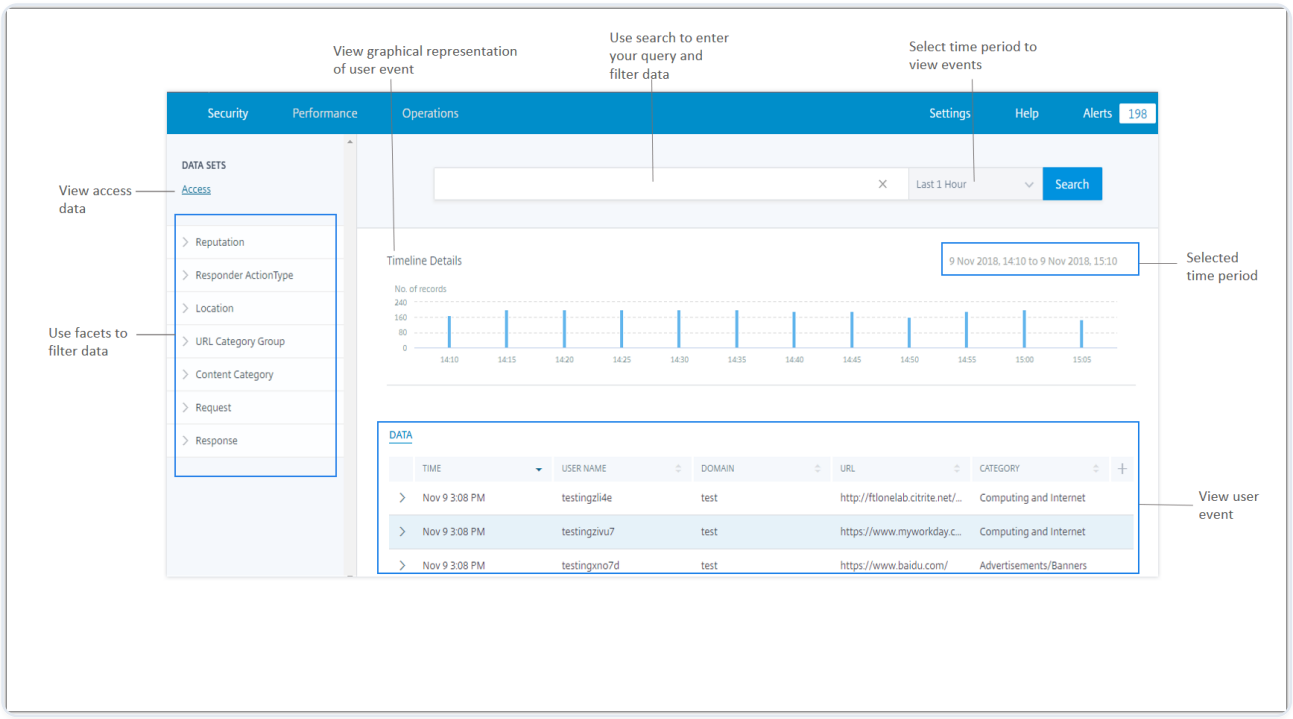
Self-service search for access data

You can use self-service search to get insight into the access details for the users in your enterprise. Citrix Analytics collects the users' access details from the Citrix Access Control service. Use the facets and the search query to narrow down your search results.

To use the self-service search page, from the **Security** tab, click **Event Search**.

For more information, see Self-service search for Access.

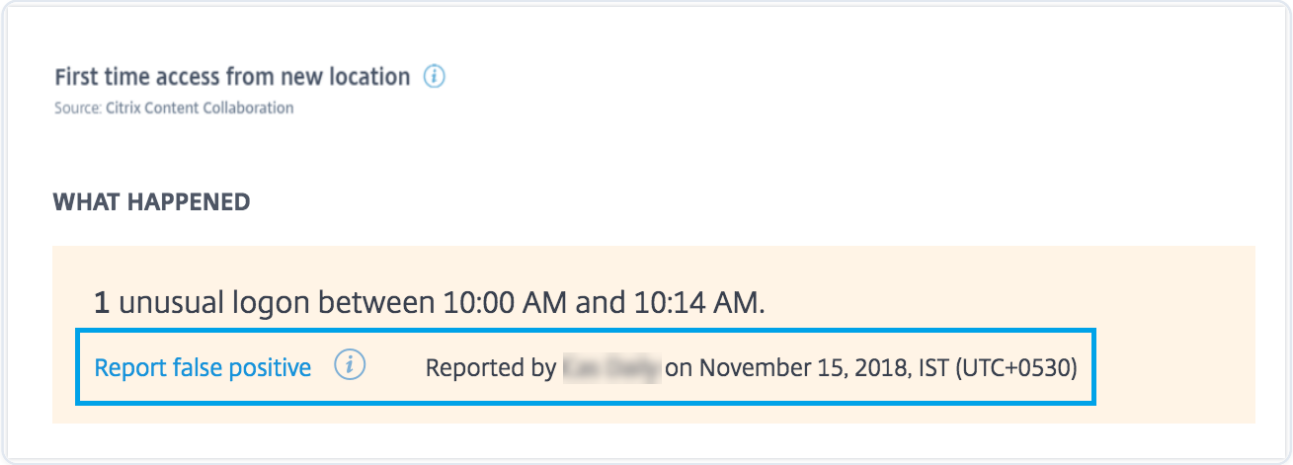
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Risk indicator feedback

Using the risk indicator feedback feature on Citrix Analytics, you can provide feedback regarding a risk indicator. Your feedback helps to confirm if the security incident reported is accurate or not.

Currently, this feature is supported on the **Unusual logon access** risk indicator triggered by the Content Collaboration data source. If this risk indicator triggered is incorrect, you can report it as a false positive and provide feedback. You can also edit feedback that you have previously submitted. Citrix Analytics captures your feedback and validates the predicted information to optimize the anomalous behavior detection.



Fixed issues

- You cannot edit and save a policy if you are accessing Citrix Analytics using Internet Explorer 11.0.

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

Known Issues

Citrix Analytics for Security™ has the following known issues:

- Citrix Workspace™ app for Linux fails to send printing events to Citrix Analytics when apps and desktops are opened through a web browser and launched from ICA® on the native client.

  NOTE

  For more information on the lifecycle dates and lifecycle phases (General Availability, End of Maintenance, and End of Life) of Citrix Workspace app and Citrix Receiver on all platforms, see Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

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

Analytics offerings

layout: doc replicate-from: commons/analytics-offerings.md

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

Data Sources

Data sources are the cloud services and the on-premises products that send data to Citrix Analytics.

Citrix data sources

The following table lists various Citrix data sources supported by Citrix Analytics for Security. For more information, see Getting started.

DATA SOURCE	DEPLOYMENT TYPE	REQUIRED AGENTS	PRODUCT COMPONENT AND VERSION
Citrix Endpoint Management	Service	N/A	Citrix Endpoint Management
Gateway	On-premises	Application Delivery Management agent	Citrix Gateway 12.0.56.16 or later
Citrix Identity provider	Service	N/A	Citrix Identity and Access Management
Citrix Secure Private Access	Service	(Not applicable) N/A	Citrix Secure Private Access
Citrix Remote Browser Isolation	Service	N/A	Citrix Remote Browser Isolation
Citrix DaaS (formerly Virtual Apps and Desktops service)	Service	N/A	Citrix Workspace app for Windows 1907 or later, Citrix Workspace app for Mac 1910.2 or later, Citrix Workspace app for HTML5 2007 or later, Citrix Workspace app for

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

DATA SOURCE	DEPLOYMENT TYPE	REQUIRED AGENTS	PRODUCT COMPONENT AND VERSION
			Chrome-Latest version available in Chrome Web Store, Citrix Workspace app for Android-Latest version available in Google Play, Citrix Workspace app for iOS-Latest version available in Apple App Store, Citrix Workspace app for Linux 2006 or later
Citrix Virtual Apps and Desktops	On-premises	Virtual Apps and Desktops agent	Citrix Virtual Apps and Desktops 7 1808, Citrix XenApp and XenDesktop 7.16 and later
		Agent is required for advanced features such as Actions.	Citrix Workspace app for Windows 1907 or later, Citrix Workspace app for Mac 1910.2 or later, Citrix Workspace app for HTML5 2007 or later, Citrix Workspace app for Chrome-Latest version available in Chrome Web Store, Citrix Workspace app for Android-Latest version available in Google Play, Citrix Workspace app for

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

DATA SOURCE	DEPLOYMENT TYPE	REQUIRED AGENTS	PRODUCT COMPONENT AND VERSION
			iOS-Latest version available in Apple App Store, Citrix Workspace app for Linux 2006 or later
			Citrix Director 7.16 or later
			For Workspace users: Virtual Apps and Desktops on-premises Sites must be added to Workspace using Site Aggregation.
			For StoreFront users: StoreFront deployment version must be StoreFront 1906 or later. StoreFront must be accessed using one of the clients: Citrix Receiver™ for Web sites in HTML5-compatible browsers, Citrix Workspace™ app 1907 for Windows or later, Citrix Workspace app 2006 for Linux or later, Citrix Workspace app 2006 for Mac or later.
			LTSR support: For Citrix Virtual Apps and Desktops™ 7

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

DATA SOURCE	DEPLOYMENT TYPE	REQUIRED AGENTS	PRODUCT COMPONENT AND VERSION
			1912 LTSR, the supported StoreFront version is 1912.

NOTE

Refer to Citrix Cloud services to know about the Citrix products and their subscriptions.

External data sources

The following table lists the external data sources (third-party products) that are supported by Citrix Analytics for Security.

DATA SOURCE	DEPLOYMENT TYPE	REQUIRED AGENTS
Microsoft Graph Security	Service	N/A
Microsoft Active Directory	On-premises	Citrix Cloud Connector™

Supported home regions

Citrix Analytics for Security is supported in the following home regions:

- United States (US)
- European Union (EU)
- Asia Pacific South (APS)

Depending on the location of your organization, you can onboard to Citrix Cloud™ in one of the home regions.

If your organization is onboarded to Citrix Cloud in a home region where a data source is not supported, you don't get user events from the data source.

Use the following table to view the data sources and the regions where they are supported.

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

DATA SOURCE	SUPPORTED IN US REGION	SUPPORTED IN EU REGION	SUPPORTED IN APS REGION
Citrix Endpoint Management™	Yes	Yes	Yes
Citrix Gateway (on-premises)	Yes	Yes	Yes
Citrix Identity provider	Yes	Yes	Yes
Citrix Secure Private Access™	Yes	Yes	Yes
Citrix Remote Browser Isolation™	Yes	Yes	Yes
{{page.daas-product-name}} (formerly Citrix Virtual Apps and Desktops service)	Yes	Yes	Yes
{{page.cvad-onprem-product-name}} on-premises	Yes	Yes	Yes
Microsoft Active Directory	Yes	Yes	Yes
Microsoft Graph Security	Yes	Yes	Yes

Citrix Workspace app version matrix

This section displays the supported versions of Citrix Workspace app which sends all telemetry and contains all critical bugfixes needed.

The following table lists the supported and unsupported versions for Citrix Workspace app.

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

PLATFORM	SUPPORTED VERSION
Windows	All the LTSR 2203 releases after CU3
	23.0.3.0 or above
HTML5	21.5.0.0 or above
Macintosh	21.0.4.0 or above
Linux	21.4.0.0 or above
Chrome	21.5.0.0 or above
iOS	21.4.0.0 or above
Android	21.5.0.0 or above

The following table lists the minimum version of Citrix Workspace app required for the operating system to receive the following user event attributes in Citrix Analytics for Security.

EVENT ATTRIBUTES	ASSOCIATED FEATURES	WINDOWS	MAC	LINUX	HTML5	CHROME	IOS	ANDROID
City, Country	Access assurance location, Self-service search - Apps and Desktops	2008 or above	2006 or above	2104 or above	2007 or above	Latest version available in Chrome Web Store	Latest version available in Apple App Store	Latest version available in Google Play

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

EVENT ATTRIBUTES	ASSOCIATED FEATURES	WINDOWS	MAC	LINUX	HTML5	CHROME	IOS	ANDROID
Client IP	Self-service search - Apps and Desktops	2008 or above	2006 or above	2104 or above	2007 or above	Latest version available in Chrome Web Store	Latest version available in Apple App Store	Latest version available in Google Play
OS name, OS version, OS extra info	Self-service search - Apps and Desktops	2109 or above	2108 or above	2104 or above	2007 or above	Latest version available in Chrome Web Store	Latest version available in Apple App Store	Latest version available in Google Play
Printer name	Self-service search - Apps and Desktops	2106 or later	1809 or later	2006 or later	1911 or later	Latest version available in Chrome Web Store	Latest version available in Apple App Store	Latest version available in Google Play
All user events for web launch	Self-service search - Apps and Desktops	2008 or later	2006 or later	2006 or later	Not applicable	Not supported	Latest version available in Apple App Store	Latest version available in Google Play

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

Data governance

layout: doc replicate-from: commons/data-governance.md

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

System Requirements

Before you begin using Citrix Analytics for Security™, review the following requirements.

Citrix Analytics for Security subscription

This Analytics product is a subscription-based offering. You must have a valid subscription to use the Security Analytics. For more information, see the product overview page.

Data sources requirements

Citrix Analytics for Security receives events from various data sources. For Analytics to function accurately, you must have a valid subscription to use at least one of the following products, which act as data sources for Analytics:

- Citrix ADC (on-premises) along with subscription for Citrix Application Delivery Management
- Citrix Endpoint Management service
- Citrix Gateway (on-premises)
- Citrix Identity provider
- Citrix Remote Browser Isolation
- Citrix Secure Private Access service
- Citrix Virtual Apps and Desktops or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)
- Microsoft Active Directory
- Microsoft Graph Security

Supported browsers

To access Analytics, your workstation must have the following supported web browser:

- Latest version of Google Chrome
- Latest version of Mozilla Firefox
- Latest version of Microsoft Edge

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

- Latest version of Apple Safari

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

Manage administrator roles for Security Analytics

NOTE:

Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

As a Citrix Cloud™ administrator with full access permissions, you can invite other administrators to manage the Security Analytics offering and assign them one of the following custom roles:

- **Security Analytics- Full Administrator**
- **Security Analytics- Read Only Administrator**

You can add new administrators in two ways - individually as users or using Azure Active Directory groups. For more information on adding new administrators, see Manage Administrator Roles.

NOTE

If a user is granted access directly as a user and through an Azure Active Directory Group, the access granted individually to the user takes effect.

Permissions for the custom roles

The administrators with the **Security Analytics- Full Administrator** role can access all the features and functionalities of the Security Analytics offering. They can use and modify the features according to their organizational requirements. For example, a full administrator can create custom risk indicators, enable geofence, and create policies.

The administrators with the **Security Analytics- Read Only Administrator** role can only access and view the Security dashboards- Users, User Access, App Access, Access Assurance, and Reports. They can monitor user behavior and view the user events on these dashboards. However, they are not allowed to perform any critical tasks such as:

- Turn on or off data processing for the data sources

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

- Create or remove policies and actions
- Apply actions manually on the risk indicators shown on the user risk timeline
- Create, modify, or delete custom risk indicators
- Create custom reports
- Add, modify, or delete another admin user
- Add or modify geo-fence for access assurance location

Security alert notifications for the administrators

Like the Citrix Cloud administrators with full access permissions, the administrators with the custom roles (Full access and Read-only access) receive email notifications from Security Analytics.

The administrators receive two types of email notifications:

- Weekly notification about the security insights in their organization. For more information, see Weekly email notification.
- Notifications based on the Notify administrators action. For more information, see Policies and actions.

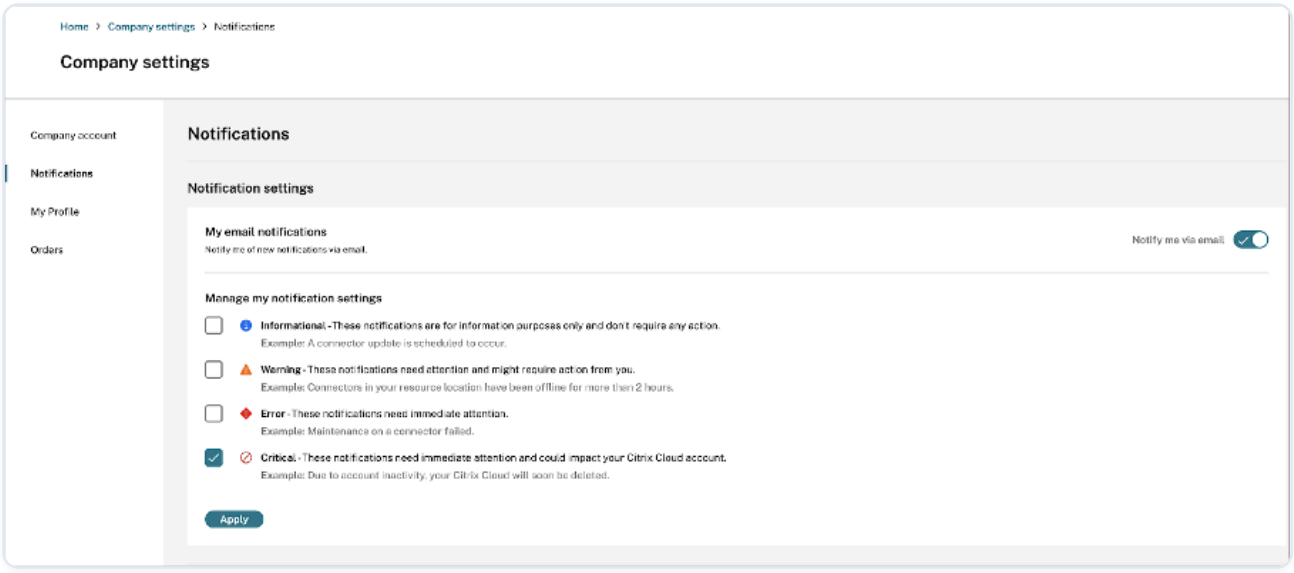
If you are a Citrix Cloud administrator with full or custom access permission, the email notifications are disabled by default in your Citrix Cloud account. To receive email notifications from any Citrix Cloud services such as Citrix Analytics, enable the notification option in your Citrix Cloud. For more information, see Received email notifications. Notification preferences are not available for administrators who are added through Active Directory/Azure AD Groups.

The notification preference is leveraged while sending notifications such as weekly emails, Notify Administrators action emails, and alerts for data exports. For the email notifications, if you wish to stop receiving emails, an administrator with Full access to Security Analytics must remove you from the distribution list. For more information about the distribution list, see Email distribution list.

NOTE

Citrix Cloud Administrators (with full or custom access permission) do not receive any notifications from other Citrix Cloud services that leverage **Notification Preferences**.

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

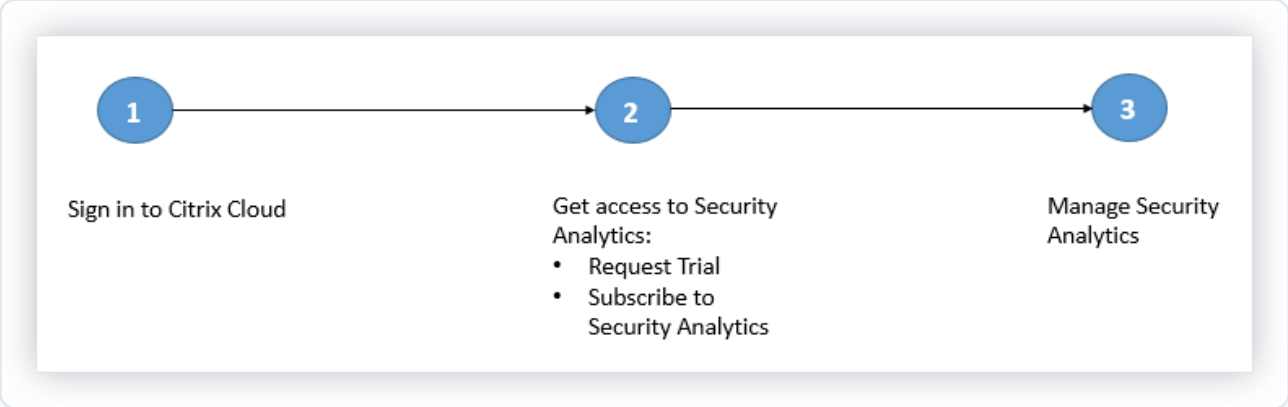


For more information, see Manage administrators for Citrix Analytics.

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

Getting started

This document describes how to get started with Citrix Analytics for Security™ for the first time.



Step 1: Sign in to Citrix Cloud™

To use Citrix Analytics for Security, you must have a Citrix Cloud account. Go to https://citrix.cloud.com and sign in with your existing Citrix Cloud account.

If you do not have a Citrix Cloud account, you must first create a Citrix Cloud account or join an existing account created by someone else in your organization. For detailed processes and instructions on how to proceed, see Sign Up for Citrix Cloud.

Step 2: Get access to Security Analytics

You can access Citrix Analytics for Security in one of the following ways:

- **Request a Citrix Analytics for Security trial**. After signing in to Citrix Cloud, do the following:
  a. In the **Available Services** section, click **Manage** on the **Analytics** tile. You are redirected to the Analytics overview page.
  b. On the **Security** tile, click **Request Trial** or directly get in touch with your Citrix Account or Citrix Partner.
- **Subscribe to Citrix Analytics for Security**. To purchase a Citrix Analytics for Security subscription, visit https://www.citrix.com/en-in/products/citrix-analytics/form/inquiry/ and contact a Citrix Analytics expert who can help you.

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

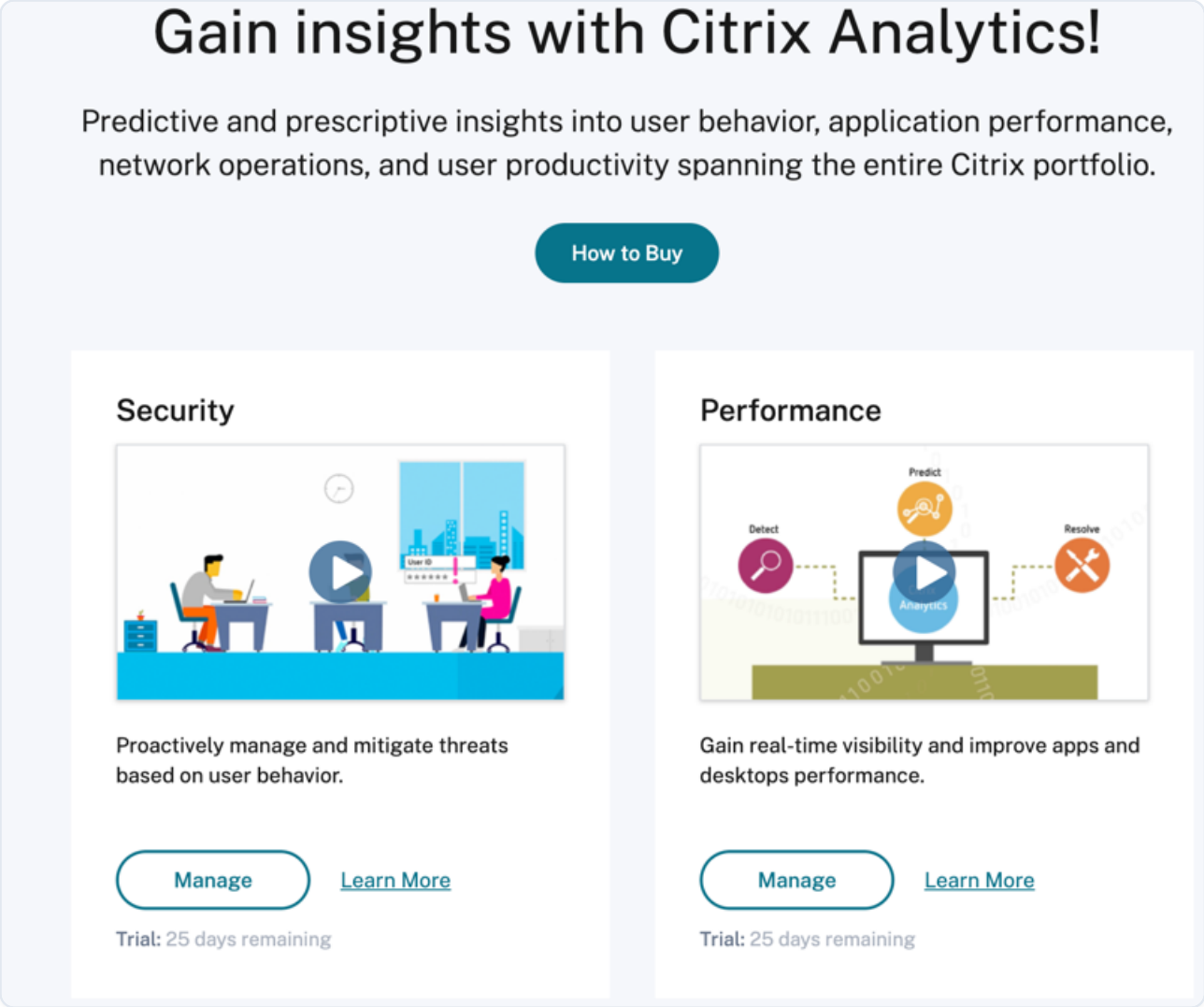
NOTE

- With effect from March 8, 2023, Citrix Analytics for Security will no longer be available for purchase as a standalone offering with ShareFile/Citrix Content Collaboration. We are announcing End of Sales (EOS) and End of Renewals (EOR) of Citrix Analytics Service stand-alone add-on for ShareFile/Citrix Content Collaboration. Customers' existing entitlements for Citrix Analytics for Security remains valid until their subscription expires. However, trials, renewals, and new purchases will not be supported for Sharefile/Citrix Content Collaboration integrations. Citrix Analytics Service integrations for other Citrix products continue to be offered as standalone or bundle offerings with existing Citrix DaaS plans, Citrix Virtual Apps and Desktops deployments and Citrix Workspace deployments.
- With effect from February 03, 2020, Citrix Analytics for Security is no longer included with the Workspace Premium and the Workspace Premium Plus subscriptions. Customers who have purchased the Workspace Premium or the Workspace Premium Plus subscription before February 03, 2020 can access Citrix Analytics for Security as a part of the Workspace subscription until their subscription expires. Citrix Analytics for Security is now offered as an add-on service with the Citrix Workspace packages- Workspace Standard, Workspace Premium, and Workspace Premium Plus. For more information, see Citrix Cloud services.

Step 3: Manage Security Analytics

After you have the necessary subscription or are authorized to access the trial, on the Analytics overview page, the **Request Trial** button for the Security offering changes to **Manage**. Click **Manage** to view the user dashboard.

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



Analytics supports both Citrix data sources and external data sources. It automatically discovers the Citrix data sources associated with your Citrix Cloud account. To receive data from external data sources, you need to integrate the external data sources with Analytics. To view your discovered data sources, click **Settings > Data Sources > Security**.

What's next

- Data processing is turned on for the following cloud services when their Citrix Analytics for Security entitlement is approved:
  - Citrix data sources
    - Citrix Secure Private Access
    - Citrix Virtual Apps and Desktops and Citrix DaaS
- To verify the data processing status or know how to turn it on manually, see the following articles:

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

    - Citrix data sources:
        - Citrix Endpoint Management
        - Citrix Gateway
    - External data sources:
        - Microsoft Graph Security
        - Microsoft Active Directory

- Export processed data from Analytics to the following products:
    - Splunk
    - Microsoft Azure Sentinel
    - Elasticsearch
    - Other SIEMs using Kafka or Logstash based data connector
- Use the Users dashboard to view the discovered users and their security risk profiles. The **Users** dashboard is the launching point for user behavior analysis and threat prevention.

  NOTE

  If you are using Analytics for the first time, the user risk profiles take some time to appear on the dashboard. Analytics uses machine learning to determine the risky pattern or anomalies in the user events and identifies the user profiles as high risk, medium risk, and low risk based on the severity of the risks.

- Use the self-service search feature to view and filter the user events (raw data) received from the data sources.

Citrix Endpoint Management™ data source

The **Endpoint Management** data source represents the Citrix Endpoint Management service associated with your Citrix Cloud account. When users use this service, Citrix Analytics receives the user events related to users' endpoints and their activities in real time. The user events are processed to detect any security threats.

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

Prerequisites

- Subscribe to Citrix Endpoint Management offered on Citrix Cloud. To learn how to set up your Endpoint Management service, see Onboarding and resource setup.
- **Cloud Site and Enterprise Directory set up**. Ensure that you have two machines running Windows 2012 R2 or Windows 2016 server to install the Cloud Connector.
- **Cloud Connector installed**. Download and install the Cloud Connector on a virtual machine that is part of Active Directory.
- Review the system requirements and ensure that your environment met the requirements.

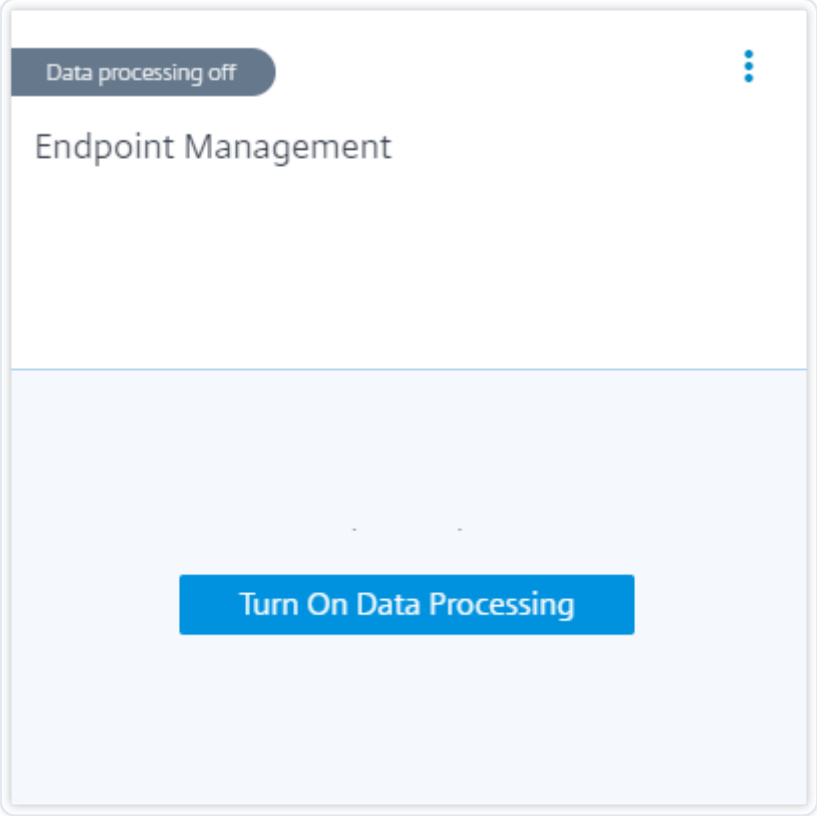
View data source and turn on data processing

Citrix Analytics automatically discovers all Endpoint Management data sources associated with your Citrix Cloud™ account.

To view the data source:

From the top bar, click **Settings** > **Data Sources** > **Security**.

A site card for the Endpoint Management data source appears on the **Data Sources** page. Click **Turn On Data Processing** to allow Citrix Analytics to begin processing data for this data source.

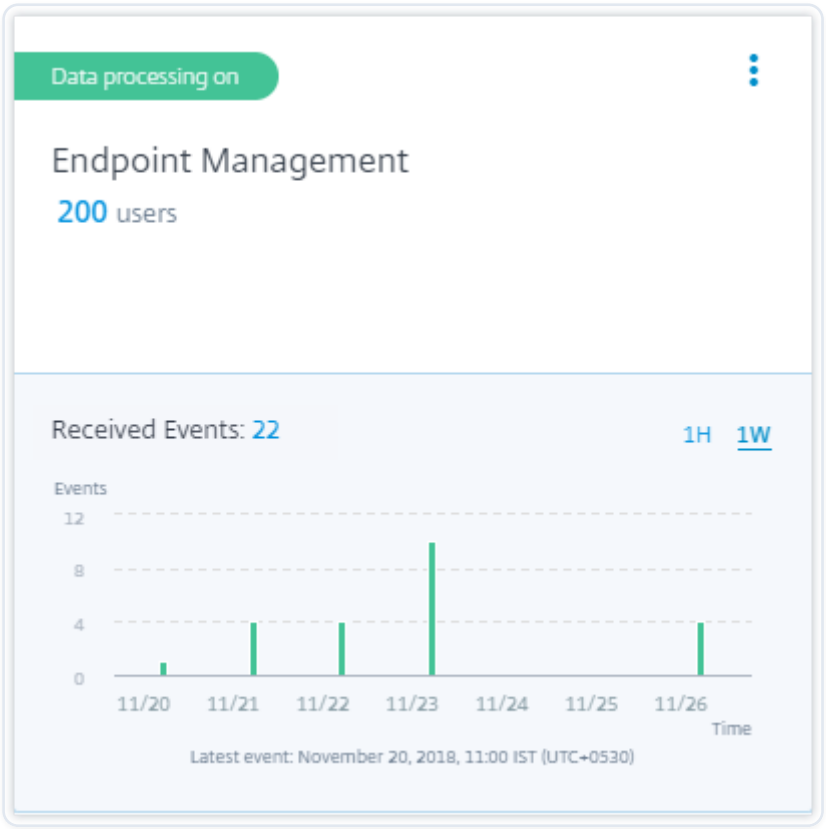


© 1997–2026 Citrix Systems, Inc. All rights reserved.

View users and received events

The site card displays the number of Endpoint Management users, devices, and the received events for the last one hour, which is the default time selection. You can also select 1 week (**1W**) and view the data.

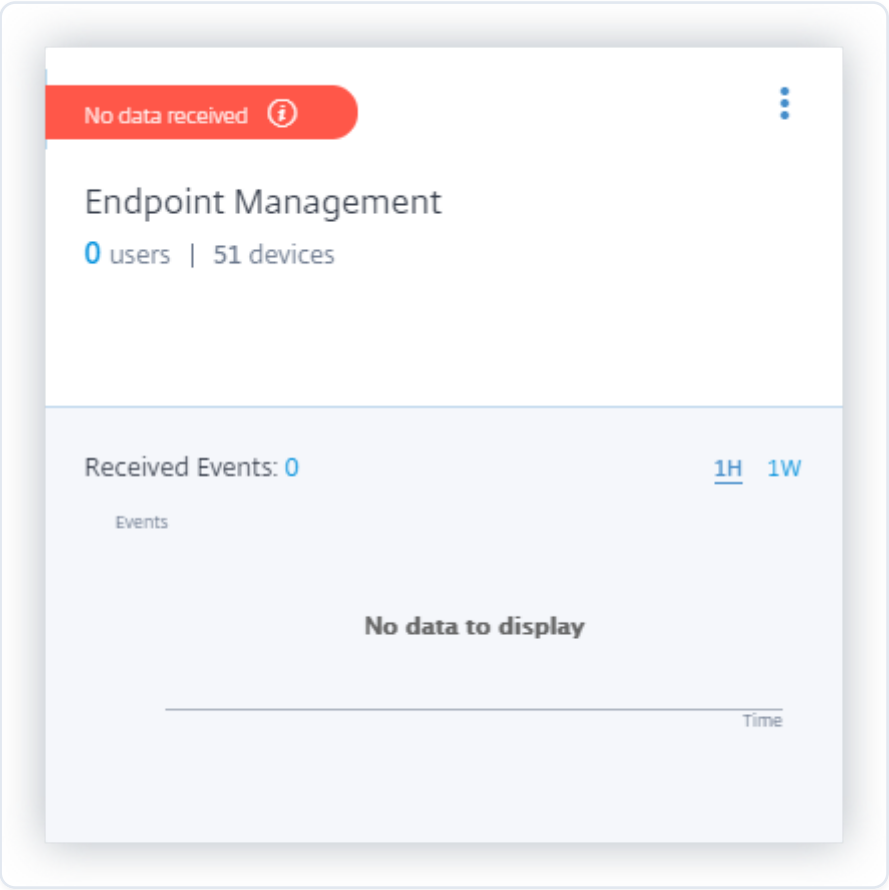
Click the number of users to view the user details on the **Users** page.



After you have enabled data processing, the site card might display the **No data received** status. This status appears for two reasons:

1. If you have turned on data processing for the first time, the events take some time to reach the event hub in Citrix Analytics. When Citrix Analytics receives the events, the status changes to **Data processing on**. If the status does not change after some time, refresh the **Data Sources** page.
2. Analytics has not received any events from the data source in the last one hour.

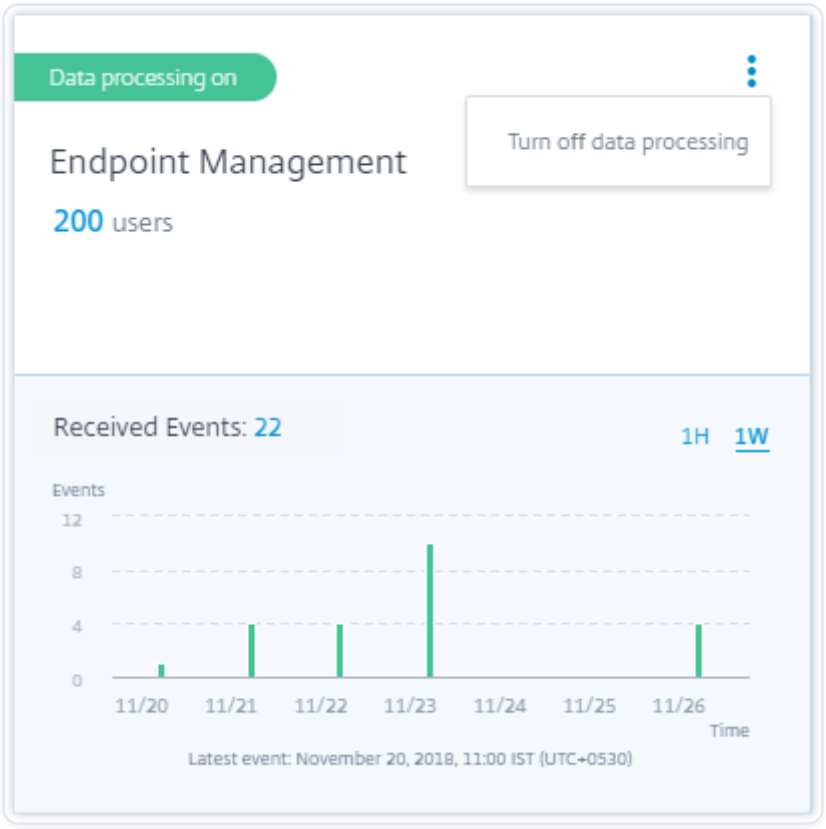
© 1997–2026 Citrix Systems, Inc. All rights reserved.



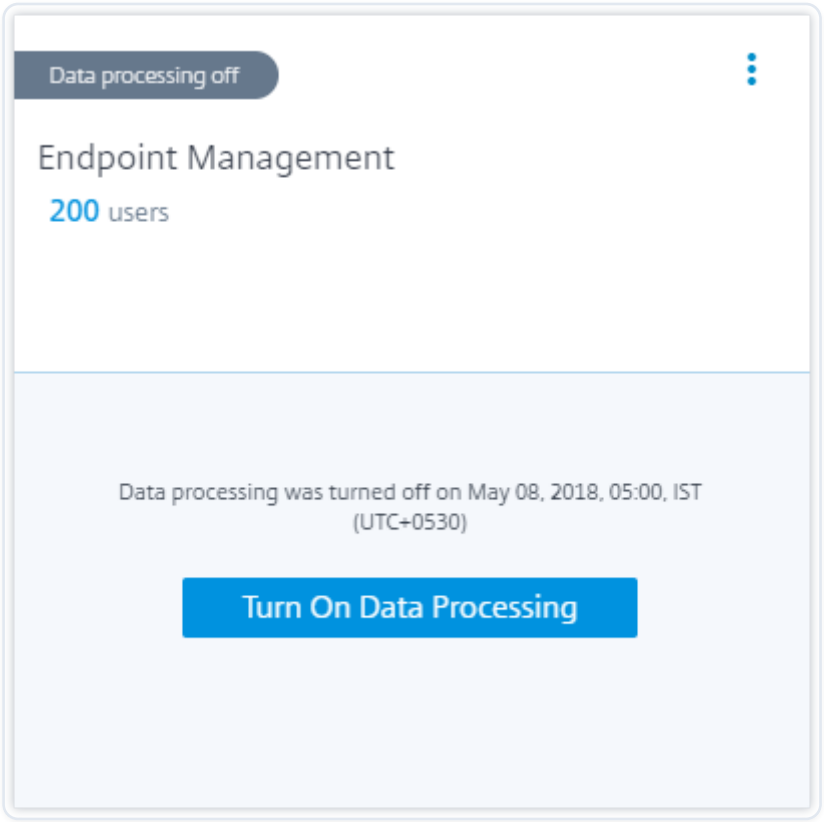
Turn on or off data processing

To stop data processing, click the vertical ellipsis (⋮) on the site card and then click **Turn off data processing**. Citrix Analytics stops processing data for this data source.

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



To enable data processing again, click **Turn On Data Processing**.



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

Citrix Gateway (on-premises) data source

The **Gateway** data source represents the on-premises Citrix Gateway instances in your environment. Citrix Analytics automatically discovers the Citrix Application Delivery Management (ADM) agents and the Gateway instances added to the Citrix ADM service.

When users access any services or applications through Gateway, Citrix Analytics receives the user access events in real time. The user events are processed to detect any security threats.

For information about the prerequisites and onboarding steps, see the Citrix Gateway data source article on Citrix Analytics platform documentation.

Citrix Remote Browser Isolation™ data source

The Citrix Remote Browser Isolation Service isolates web browsing to protect the corporate network from browser-based attacks. It delivers consistent, secure remote access to internet hosted web applications, with no need for user device configuration.

In Citrix Analytics for Security, you can view the user events of a published Remote Browser Isolation session. For more information about the user events, see Self-service search for Remote Browser Isolation.

To receive the user events from a published Remote Browser Isolation session, enable the **Hostname Tracking** policy in the Remote Browser Isolation. By default, the policy is disabled.

Enabling the **Hostname Tracking** policy allows Remote Browser Isolation to send host names used during the user session to Citrix Analytics for Security. For more information, see Manage published Remote Browser Isolations.

Citrix Secure Private Access™ data source

The **Secure Private Access** data source represents the {{page.secure-private-access-product-name}} service that is associated with your Citrix Cloud account. When users use this service, Citrix Analytics receives the user access events (logs) in real time. The user events are processed to detect any security threats.

Prerequisites

- Subscribe to {{page.secure-private-access-product-name}} service offered on Citrix Cloud. To learn how to get started, see Secure Private Access service.
- Review the system requirements and ensure that your environment met the requirements.

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

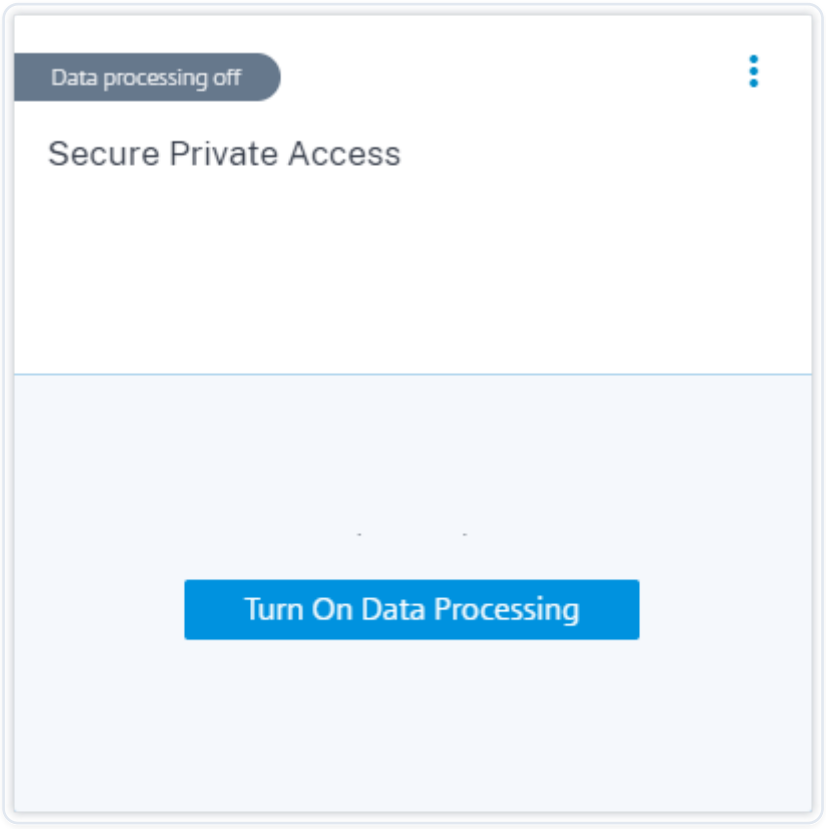
View data source and turn on data processing

Citrix Analytics automatically discovers the Secure Private Access data source associated with your Citrix Cloud™ account.

To view the data source:

From the top bar, click **Settings** > **Data Sources** > **Security**.

A site card for the **Secure Private Access** data source appears on the **Data Sources** page. Click **Turn On Data Processing** to allow Citrix Analytics to begin processing data for this data source.

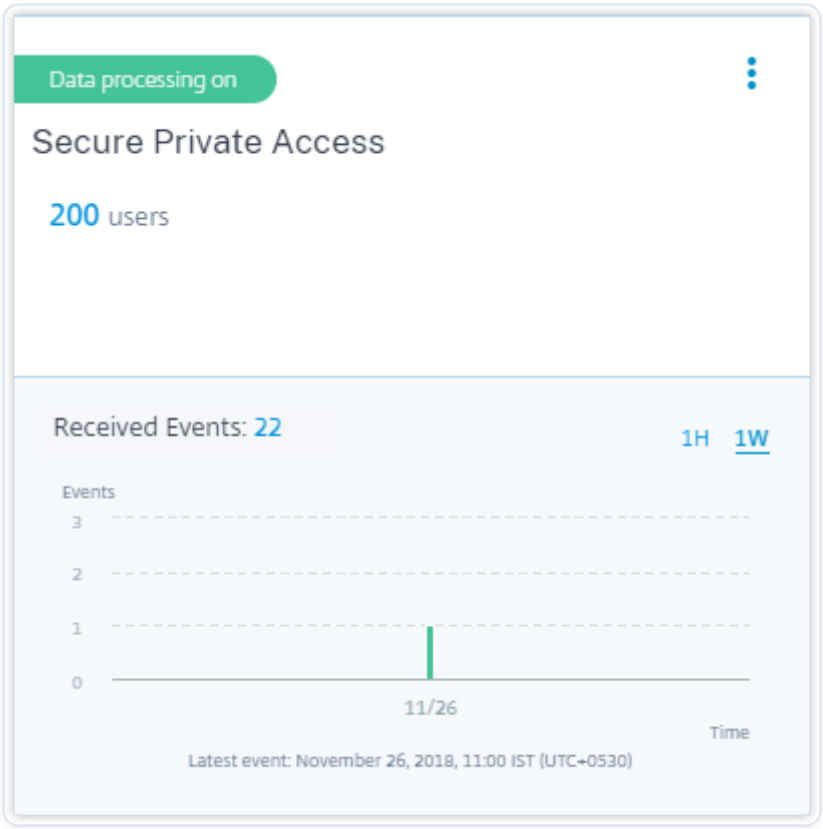


View users and received events

The site card displays the number of active users and the events received from the data source for the last one hour, which is the default time selection. You can also select 1 week (1 W) and view the data.

Click the number of users to view the user details on the **Users** page. Click the number of received events to view the event details on the self-service search page.

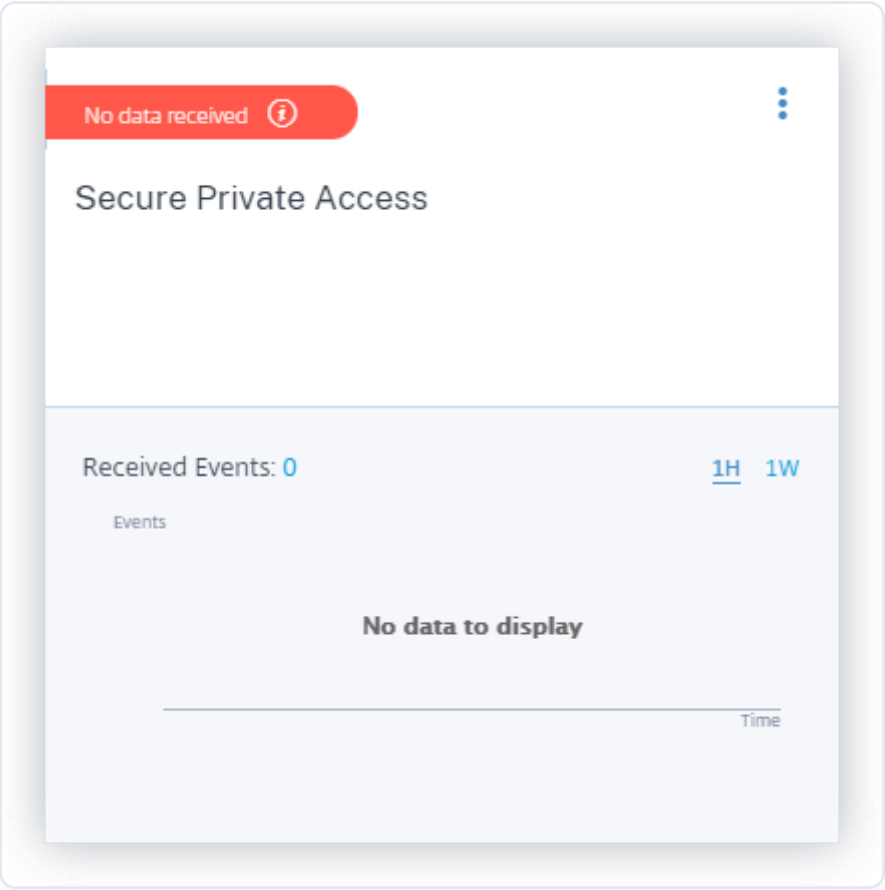
© 1997–2026 Citrix Systems, Inc. All rights reserved.



After you have enabled data processing, the site card might display the **No data received** status. This status appears for two reasons:

1. If you have turned on data processing for the first time, the events take some time to reach the event hub in Citrix Analytics. When Citrix Analytics receives the events, the status changes to **Data processing on**. If the status does not change after some time, refresh the **Data Sources** page.
2. Analytics has not received any events from the data source in the last one hour.

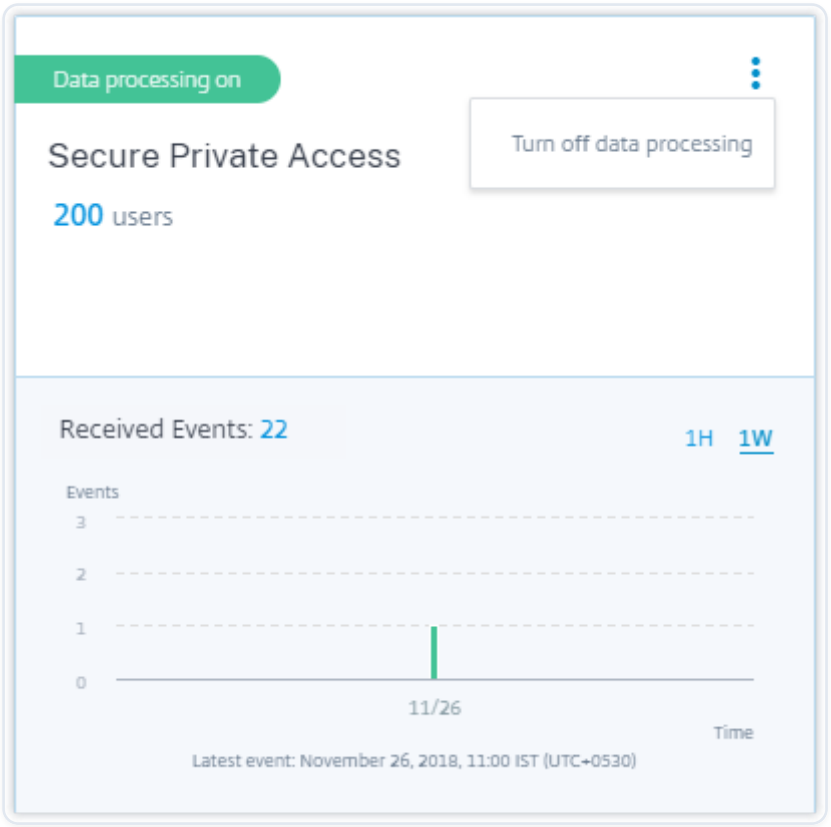
© 1997–2026 Citrix Systems, Inc. All rights reserved.



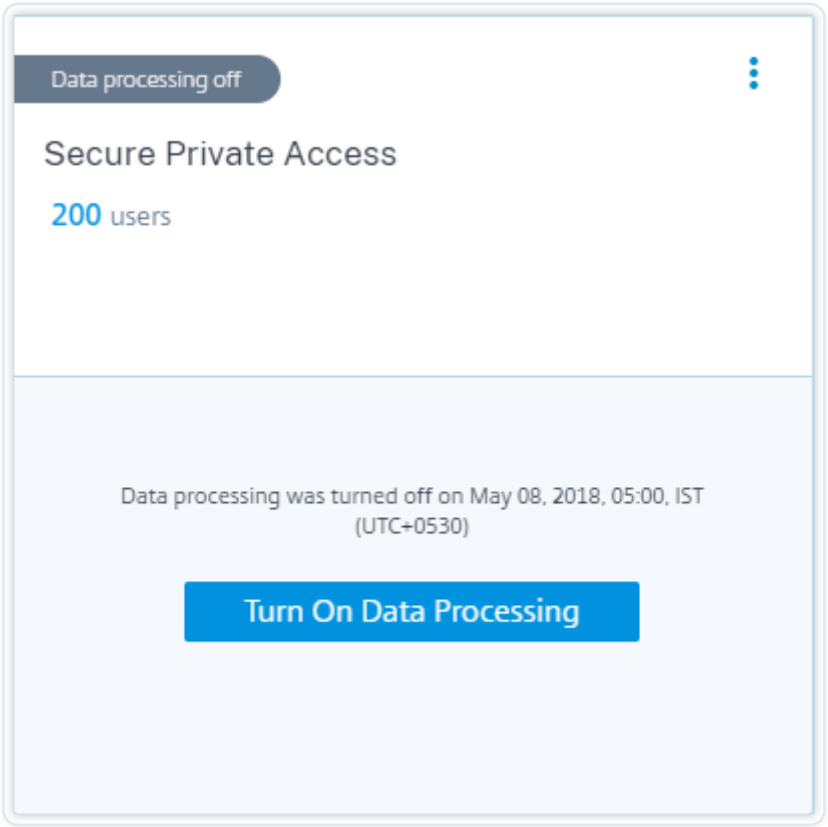
Turn on or off data processing

To stop data processing, click the vertical ellipsis (⋮) on the site card and then click **Turn off data processing**. Citrix Analytics stops processing data for this data source.

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



To enable data processing again, click **Turn On Data Processing**.



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

Citrix Virtual Apps and Desktops™ and Citrix DaaS data source

The **Apps and Desktops** data source represents on-premises Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) in your organization.

Citrix Analytics for Security™ supports both the offerings and receives user events from the data source. This article walks you through the prerequisites and the procedures to enable Analytics on both the offerings.

Citrix Analytics for Security receives user events from the following components of the Citrix Virtual Apps and Desktops and Citrix DaaS™ data source:

- Citrix Workspace™ app installed on the user devices
- Citrix Director for on-premises deployment
- Citrix Monitor service
- Session recording servers

The user events are received in real time in Citrix Analytics for Security when users use virtual apps or virtual desktops.

Supported client versions

Citrix Analytics receives user events when a supported client version is used on the user endpoints. If users are using any unsupported client versions, they must upgrade their clients to one of the following versions:

- Citrix Workspace app for Windows 1907 or later
- Citrix Workspace app for Mac 1910.2 or later
- Citrix Workspace app for HTML5 2007 or later
- Citrix Workspace app for Chrome-Latest version available in Chrome Web Store
- Citrix Workspace app for Android-Latest version available in Google Play
- Citrix Workspace app for iOS-Latest version available in Apple App Store
- Citrix Workspace app for Linux 2006 or later

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

Enable Analytics on Citrix DaaS

Prerequisites

- Subscribe to Citrix DaaS offered on Citrix Cloud. To learn how to get started with Citrix DaaS, see Install and configure.
- Review the **System Requirements** section and ensure that you met the requirements.

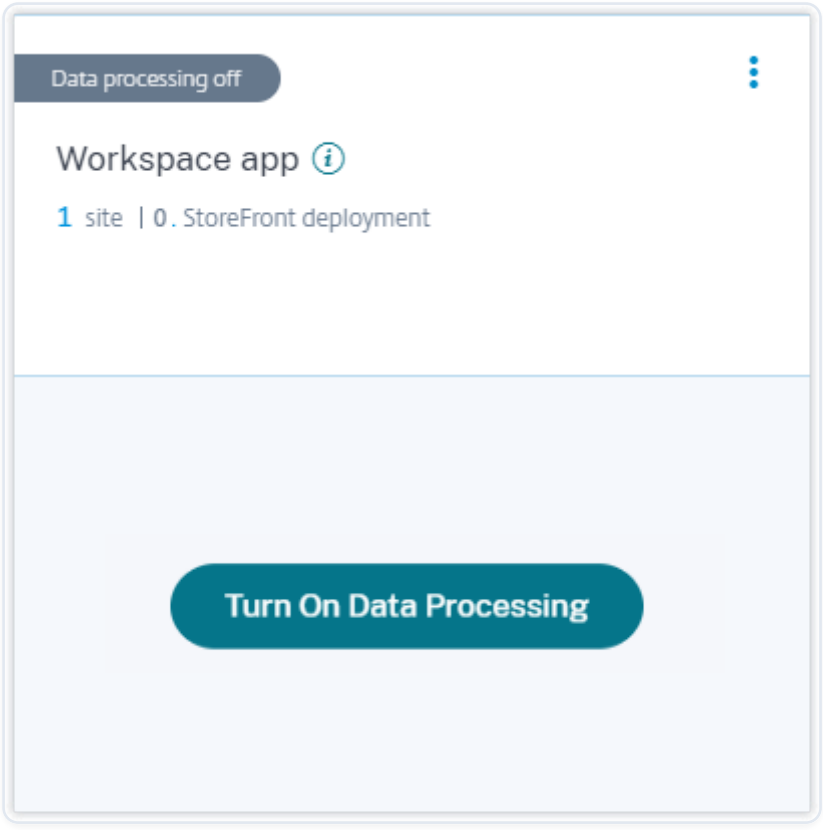
View the data source and turn on data processing

Citrix Analytics automatically discovers Citrix DaaS associated with your Citrix Cloud™ account.

To view the data source:

From the top bar, click **Settings** > **Data Sources** > **Security**.

The **Apps and Desktops- Workspace app** site card appears on the **Data Sources** page. Click **Turn On Data Processing** to allow Citrix Analytics to begin processing data for this data source.

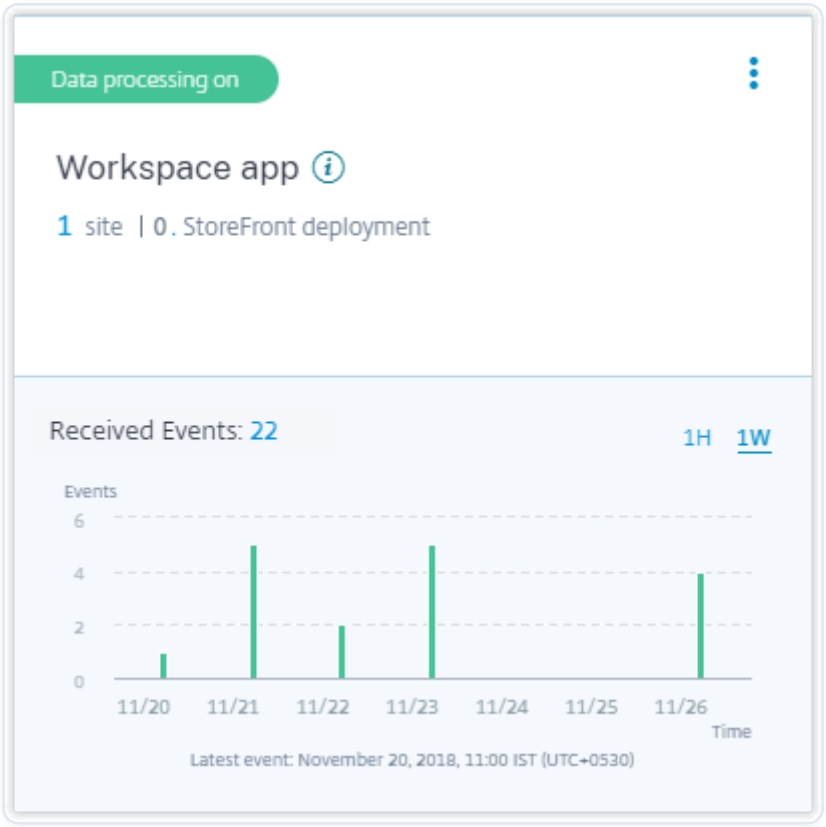


View cloud site, users, and received events

The site card displays the number of Apps and Desktops users, the discovered cloud site, and the received events for the last one hour, which is the default time selection. You can also select 1 week (1 W) and view the data.

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

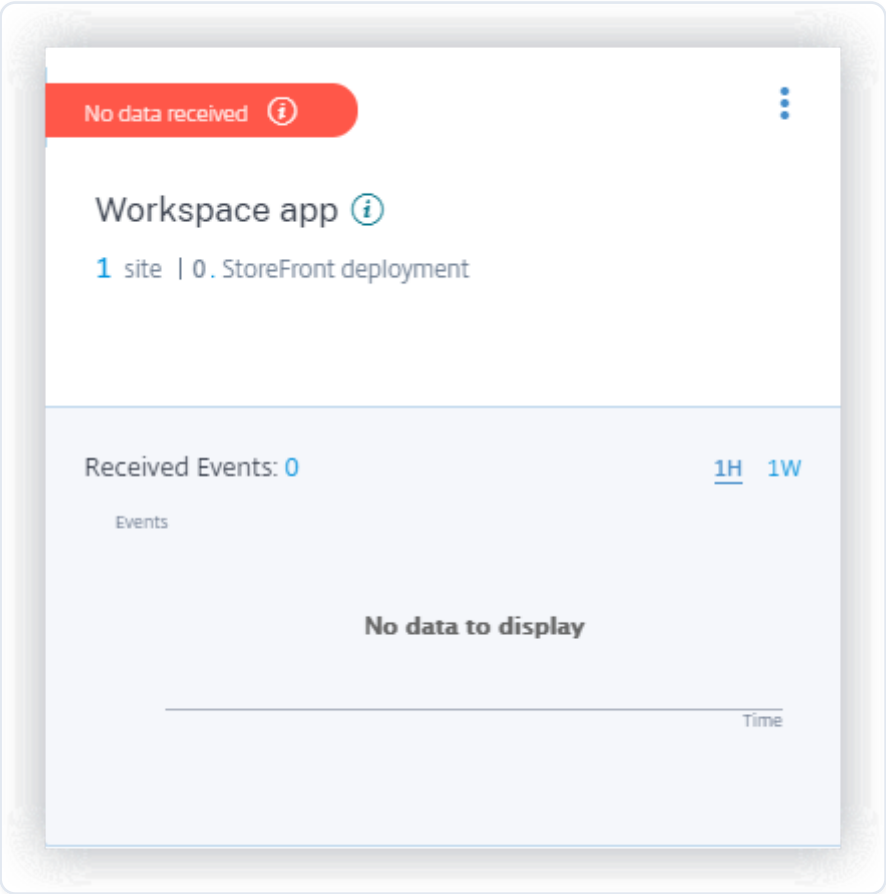
Click the number of received events to view the events on the self-service search page.



After you have enabled data processing, the site card might display the **No data received** status. This status appears for two reasons:

1. If you have turned on data processing for the first time, the events take some time to reach the event hub in Citrix Analytics. When Citrix Analytics receives the events, the status changes to **Data processing on**. If the status does not change after some time, refresh the **Data Sources** page.
2. Analytics has not received any events from the data source in the last one hour.

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



Enable Analytics on Citrix Virtual Apps and Desktops on-premises

Citrix Analytics receives user events from on-premises sites added to Workspace and sites accessed through StoreFront™ deployments.

If your organization is using on-premises sites, you must use one of the following methods to onboard your sites so that Analytics discovers the sites:

- Onboard your on-premises sites using StoreFront
- Onboard your on-premises sites using Workspace

Prerequisites

- You must have a license to use the Citrix Virtual Apps and Desktops on-premises solution. To learn how to get started with Citrix Virtual Apps and Desktops on-premises, see Install and configure.
- Review the **System Requirements** section and ensure that you met the requirements.
- Your Director is on version 1912 CU2 or later. For more information, see Feature compatibility matrix.

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

- **Subscription to Citrix Workspace**. If you want to add your sites to Citrix Workspace, you must require a Workspace subscription.

  To purchase a Citrix Workspace subscription, visit https://www.citrix.com/products/citrix-workspace/get-started.html and contact a Citrix Workspace expert who can help you.

- **Sites added to Workspace**. Citrix Analytics automatically discovers the sites added to Citrix Workspace. Add your sites to Citrix Workspace before proceeding with onboarding on Citrix Analytics. This process is known as **Site aggregation**.

  Site aggregation requires you to install Cloud Connector, configure NetScaler Gateway STA servers for internal and external connectivity to Workspace resources, and then add the sites to Workspace. For detailed instructions on site aggregation, see Aggregate on-premises virtual apps and desktops in workspaces.

- **StoreFront version**. If you are using a StoreFront deployment for your sites, ensure that the StoreFront version is 1906 or later.

Onboard Citrix Virtual Apps and Desktops on-premises sites using StoreFront

For information about the prerequisites and the onboarding steps, see the Citrix Virtual Apps and Desktops data source article on the Citrix Analytics platform documentation.

Onboard Citrix Virtual Apps and Desktops on-premises sites using Workspace

Sites already added to Citrix Workspace

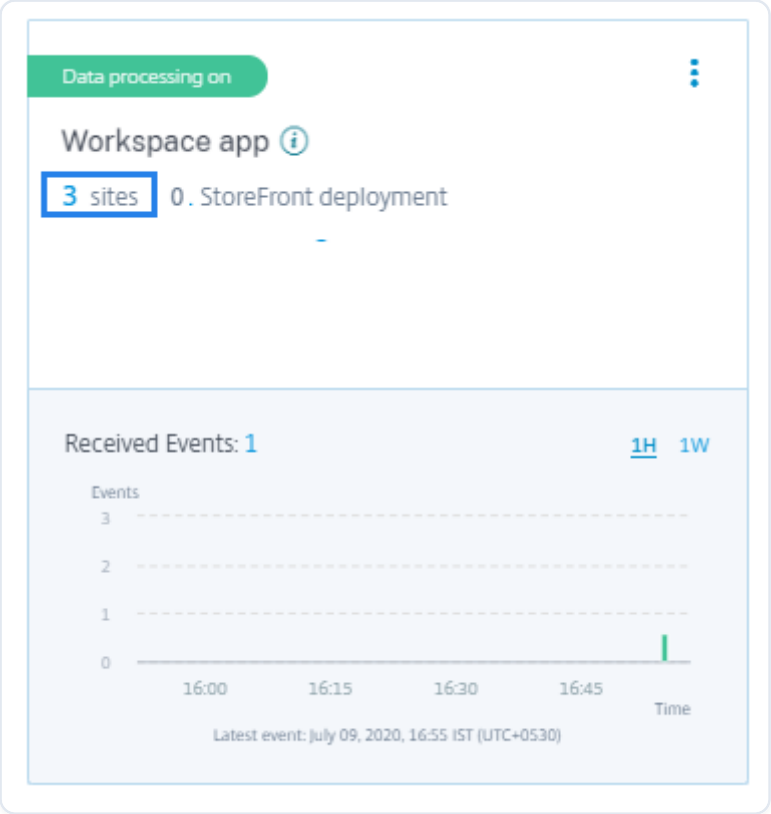
Citrix Analytics automatically discovers the on-premises sites that are already added to Citrix Workspace and displays them on the data source site card.

To view the data source:

From the top bar, click **Settings** > **Data Sources** > **Security**.

The **Apps and Desktops** site card displays the number of sites added to Workspace and the users connected to these sites. Click the site count to view the discovered sites. Click the user count to view the discovered users on the **Users** page.

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



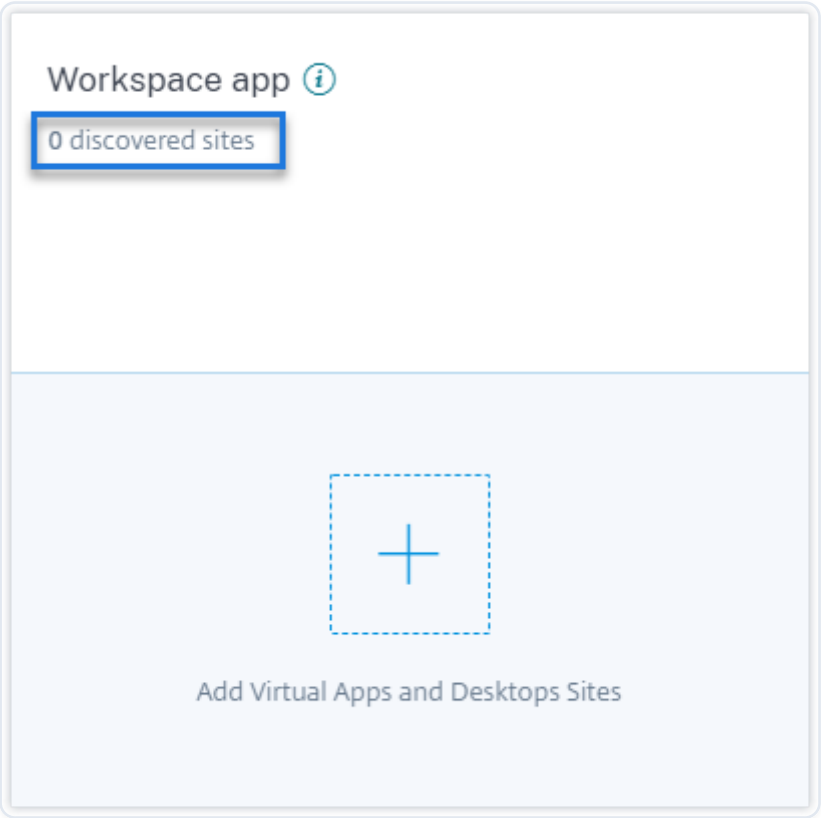
Sites not added to Citrix Workspace

If you have not already added your on-premises sites to Workspace, Analytics cannot discover your sites. The site card displays **0 discovered sites**.

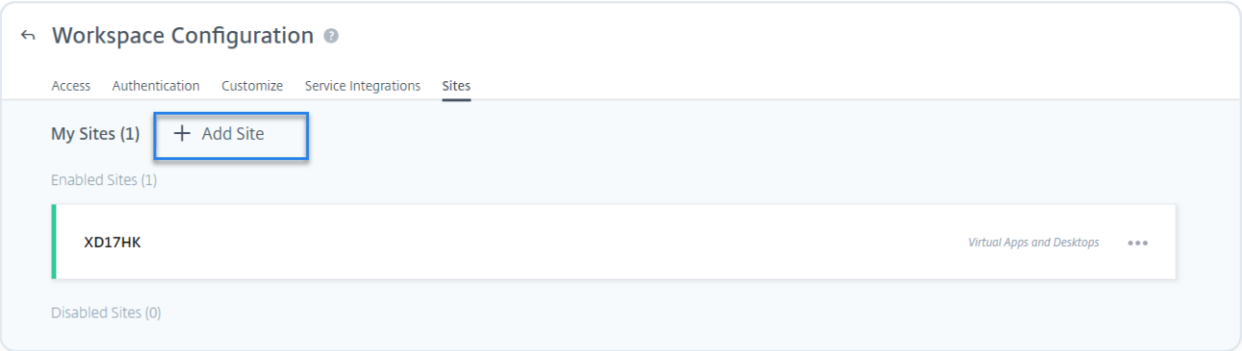
To add a site to Workspace:

1. Click + on the site card.

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



2. On the **Workspace Configuration** page, click **+Add Site**.



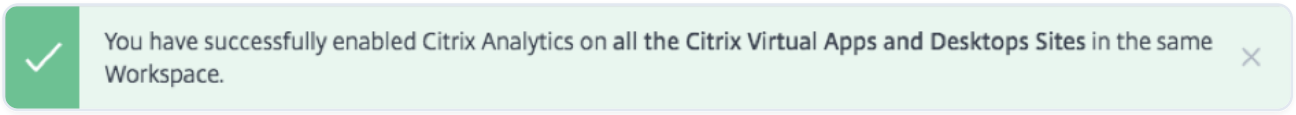
3. Follow the on-screen instructions to add a Site. For more information, see Aggregate on-premises virtual apps and desktops in workspaces.
4. After adding the site, log back to Citrix Analytics and refresh the **Data Sources** page to view the recently added site on the site card.

Turn on data processing and view received events

To allow Analytics to begin processing data for the discovered sites, click **Turn On Data Processing** on the site card and follow the prompts on the screen.

If you have multiple sites added to the same Workspace, Analytics processes and stores data for all the sites in the Workspace. You get a success message when Analytics is successfully enabled on all your sites.

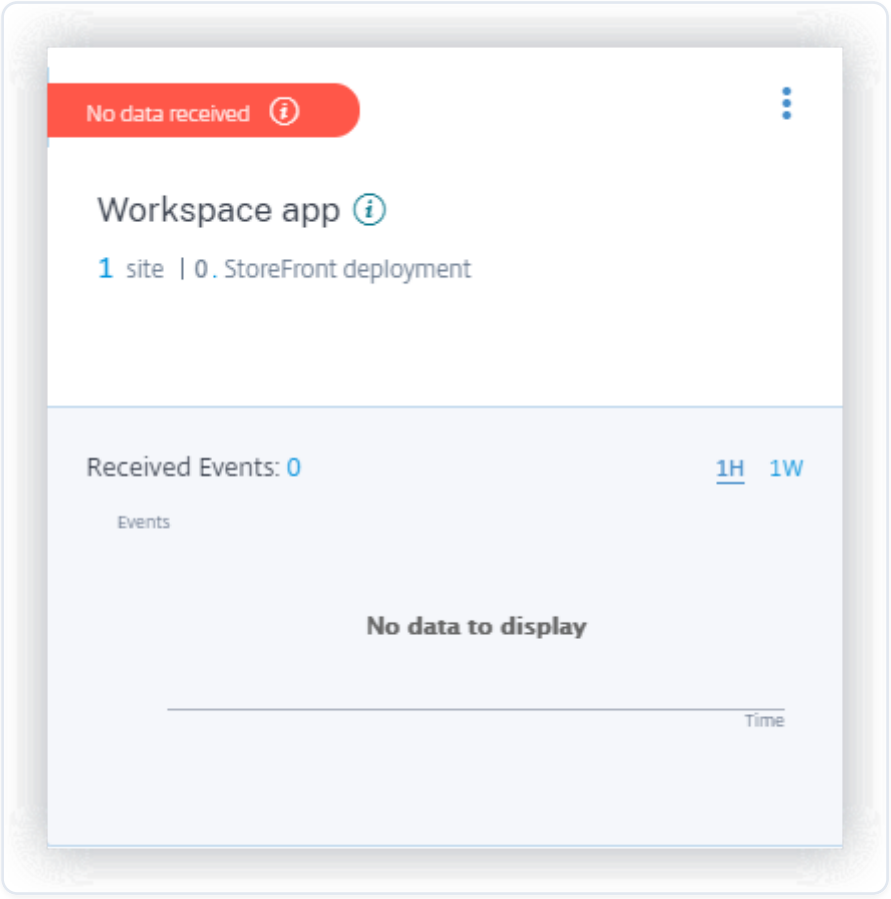
© 1997–2026 Citrix Systems, Inc. All rights reserved.



The site card displays the received events for the last one hour, which is the default time selection. You can also select 1 week (1 W) and view the data. Click the number of received events to view the events on the corresponding self-service search page.

After you have enabled data processing, the site card might display the **No data received** status. This status appears for two reasons:

1. If you have turned on data processing for the first time, the events take some time to reach the event hub in Citrix Analytics. When Citrix Analytics receives the events, the status changes to **Data processing on**. If the status does not change after some time, refresh the **Data Sources** page.
2. Analytics has not received any events from the data source in the last one hour.

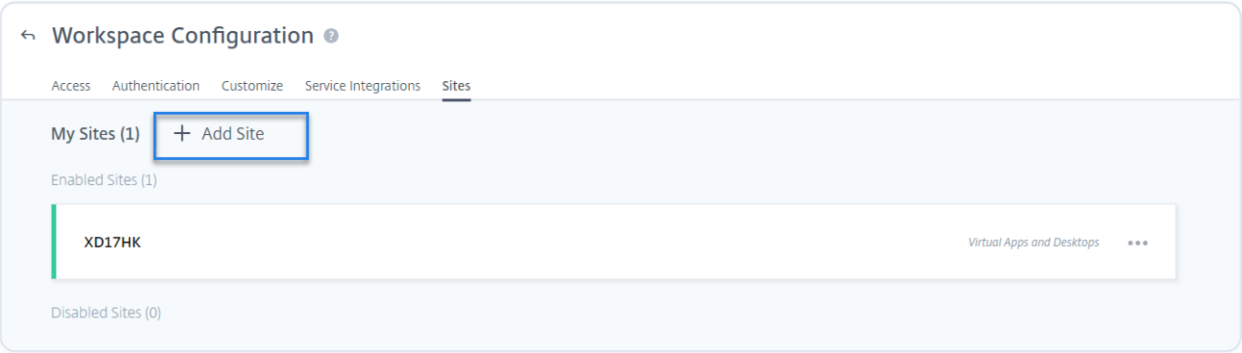


Add a site

If you want to add another on-premises site to Workspace, you can add it from Analytics:

1. On the Workspace Configuration page, click **+Add Site**.

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



2. Follow the on-screen instructions to add a site. For more information, see Aggregate on-premises virtual apps and desktops in workspaces.
3. After adding the site, go to Citrix Analytics and refresh the **Data Sources** page to view the recently added site on the site card.

Connect to Citrix Director for on-premises sites

Citrix Director is a monitoring and troubleshooting console for {{page.cvad-onprem-product-name}}. You can use Director to configure your on-premises sites for Citrix Analytics for Security (Security Analytics). After the sites are configured, Director sends monitoring events to Security Analytics.

If you are using {{page.daas-product-name}}, the Citrix Monitor service sends events from your cloud site to Security Analytics.

In a hybrid environment where you have both cloud and on-premises deployments, Security Analytics receives events from the Citrix Monitor service and the sites onboarded on Citrix Director.

Prerequisite and configuration steps

NOTES

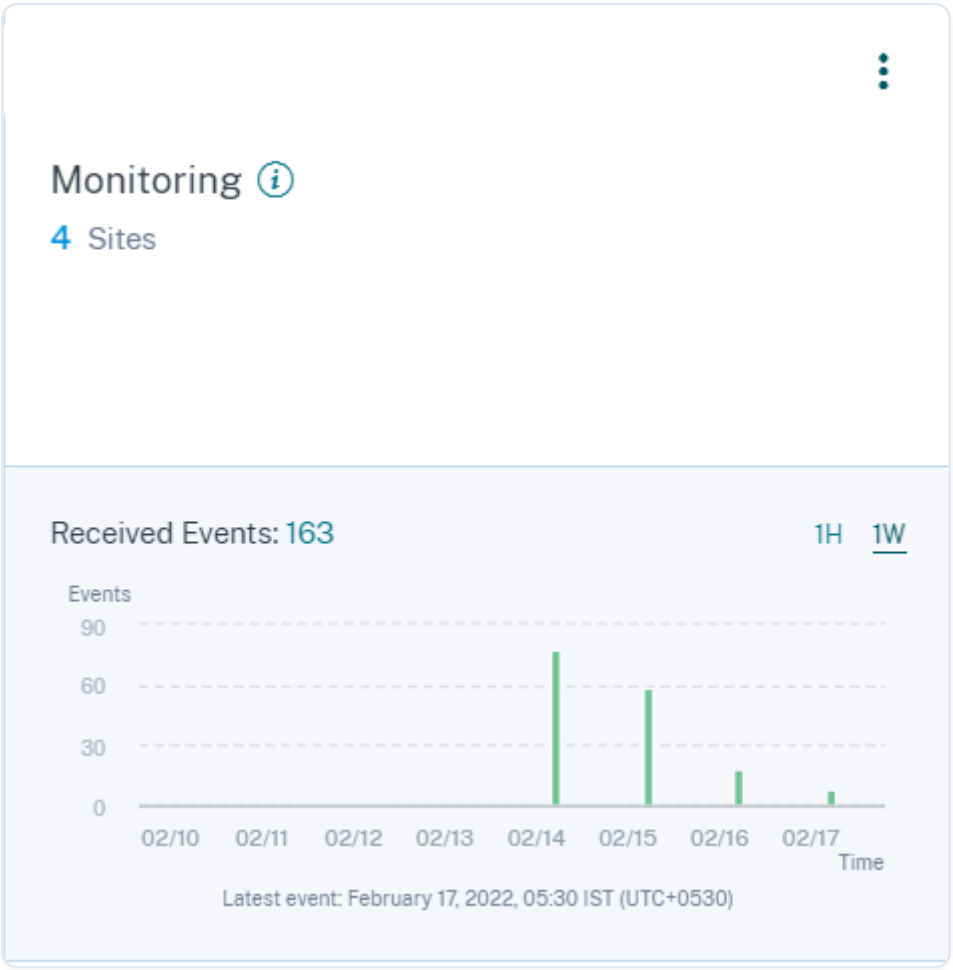
- Currently, the Director user interface displays the configuration steps related to Citrix Analytics for Performance™ (Performance Analytics). These configuration steps are also applicable for Citrix Analytics for Security (Security Analytics). If you have an active Citrix Cloud entitlement for Security Analytics, you can connect to Citrix Director by following those steps.
- If your Citrix Cloud account has active entitlements for both Security Analytics and Performance Analytics and you have already configured your site for Performance Analytics, you do not need to configure Director again for Security Analytics.

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

For information on the prerequisites and configuration steps, see Citrix Analytics for Performance documentation.

View your connected sites and received events

1. In Citrix Analytics, go to the **Data Sources** page.
2. Click the **Security** tab.
3. On the **Apps and Desktops- Monitoring** site card, you can view your on-premises sites or the cloud site (which ever is applicable). You also view the events received from the sites.

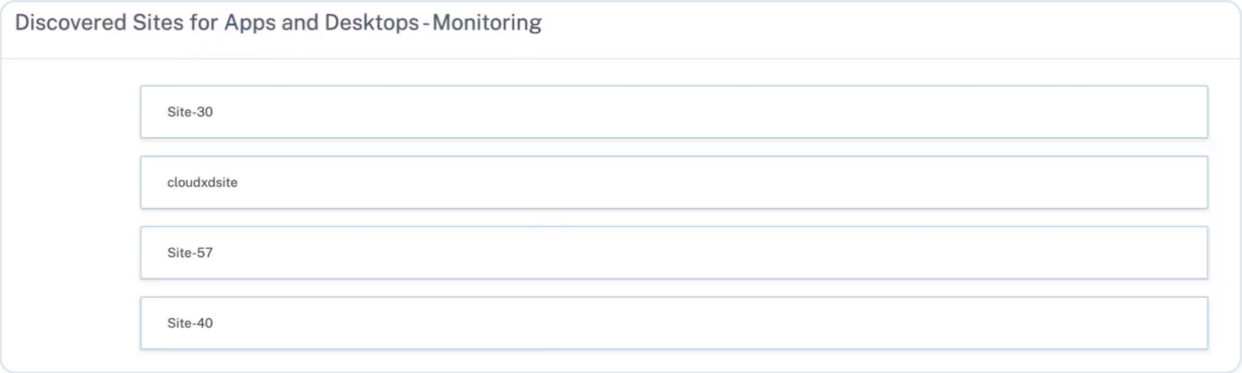


© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTES

- The first time you configure an on-premises site on Director, events from the site might take some time (approximately an hour) to get processed; causing a delay in the display of the connected site on the **Apps and Desktops- Monitoring** site card.
- On the Monitoring site card, the data processing for the Monitor service or the Director data source is enabled by default. You can also turn off the data processing depending on your requirement. However, it is recommended to keep the data processing on to get maximum benefits from Security Analytics.

4. Click the site to view the details.



Connect to Session Recording deployment

Session Recording allows you to record the on-screen activity of any user session in {{page.cvad-and-daas-product-name}}. You can configure the Session Recording servers to send the user events to Citrix Analytics for Security. The user events are processed to provide actionable insights into the users' risky behaviors.

Prerequisites

Before you begin, ensure the following:

- Your Session Recording server and the VDA agent must be 2103 or later.
- The Session Recording server must be able to connect to the required addresses. For more information on the URLs, see Network requirements.
- The Session Recording deployment must have port 443 open for outbound internet connections. Any proxy servers on the network must allow this communication with Citrix Analytics for Security.

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

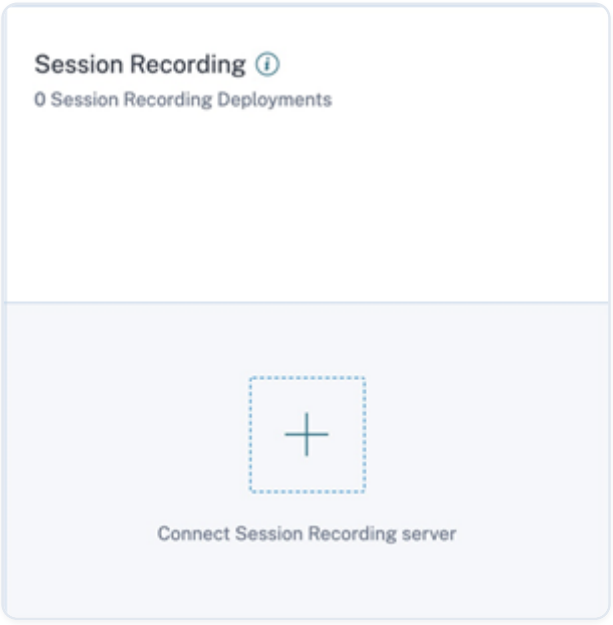
- If you are using {{page.cvad-onprem-product-name}} 7 1912 LTSR, the supported Session Recording version is 2103 or later.

NOTE

Ensure to verify the additional connectivity requirements while using the **Session Recording** service.

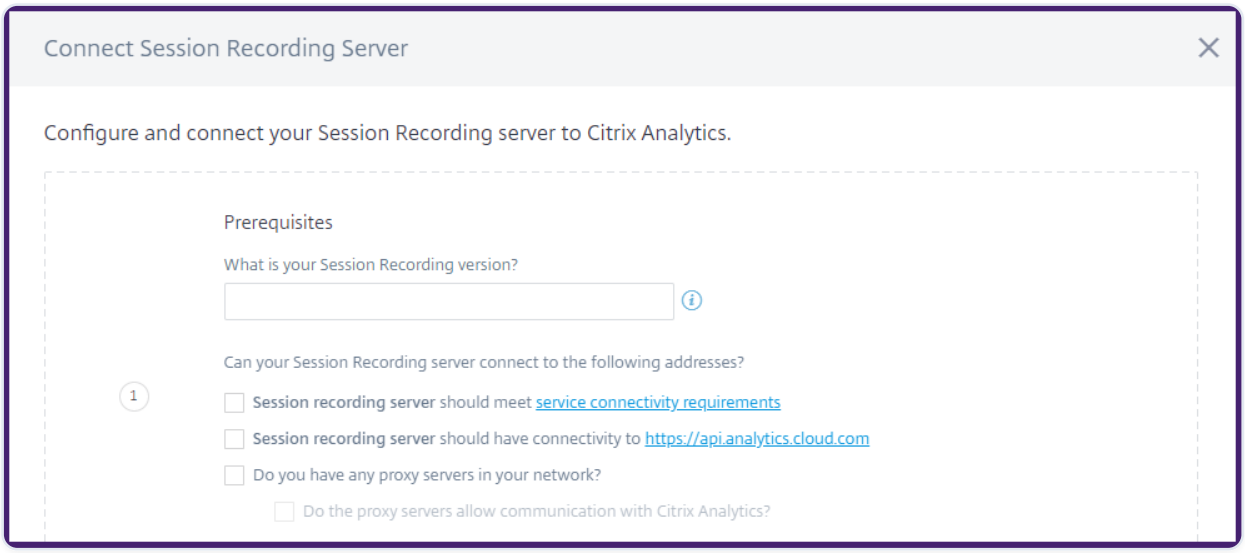
Configure your Session Recording server

1. On the **Apps and Desktops- Session Recording** site card, click **Connect Session Recording server**.



2. On the **Connect Session Recording Server** page, review the checklist, and select all the mandatory requirements. If you do not select a mandatory requirement, the Download File option is disabled.

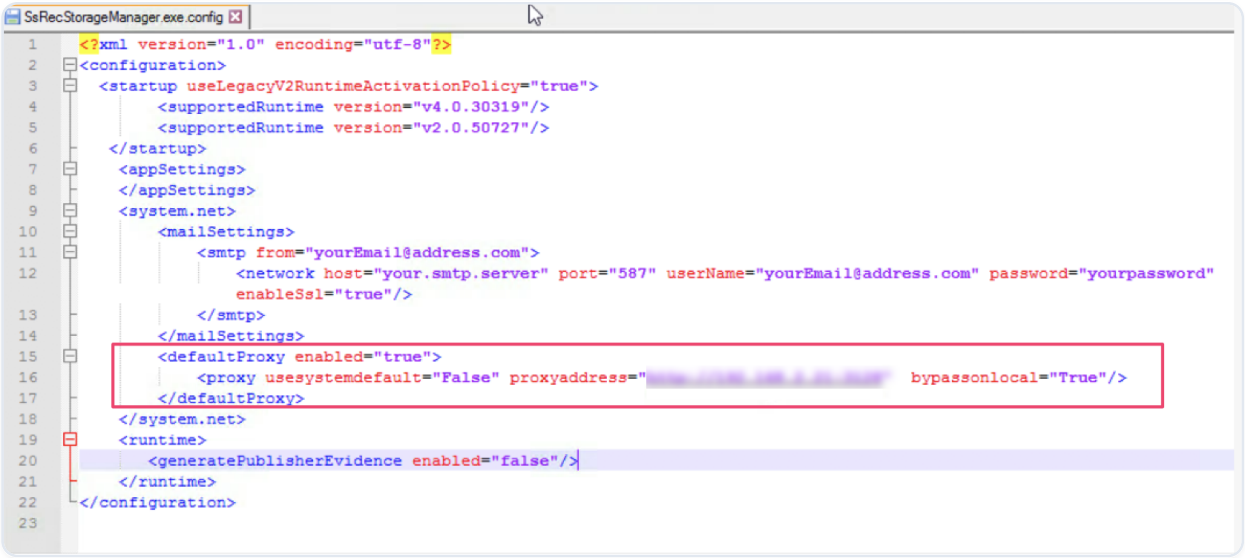
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. If you have proxy servers in your network, enter the proxy address in the *SsRecStorageManager.exe.config* file in your Session Recording server.

   The configuration file is located at `<Session Recording Server installation path>\bin\SsRecStorageManager.exe.config`

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



4. Click **Download File** to download the *SessionRecordingConfigurationFile.json* file.

> **NOTE**
>
> The file contains sensitive information. Keep the file in a safe and secure location.

5. Copy the file to the Session Recording server that you want to connect to Citrix Analytics for Security.

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

6. If you have multiple Session Recording servers in your deployment, you must copy the file in each server that you want to connect and follow the steps to configure each server.
7. On the Session Recording server, run the following command to import the settings:

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

   For example:

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

8. Restart the following services:
   - Citrix Session Recording Analytics Service
   - Citrix Session Recording Storage Manager
9. After configuration is successful, go to Citrix Analytics for Security to view the connected Session Recording server. Click **Turn On Data Processing** to allow Citrix Analytics for Security to process the data.

   NOTE

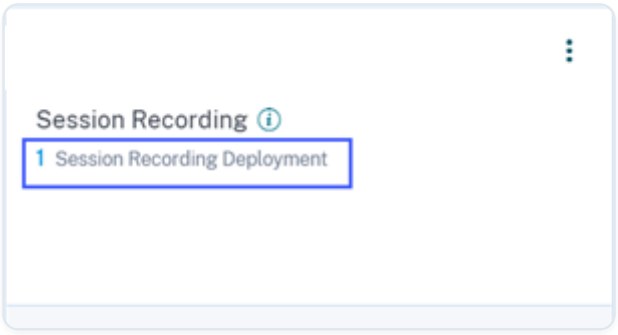
   If you are using Session Recording server version 2103 or 2104, you must first launch an Apps and Desktops session to view the connected Session Recording server on Citrix Analytics for Security. Otherwise the connected Session Recording server fails to get displayed. This requirement is not applicable for Session Recording server version 2106 and later.

View the connected deployments

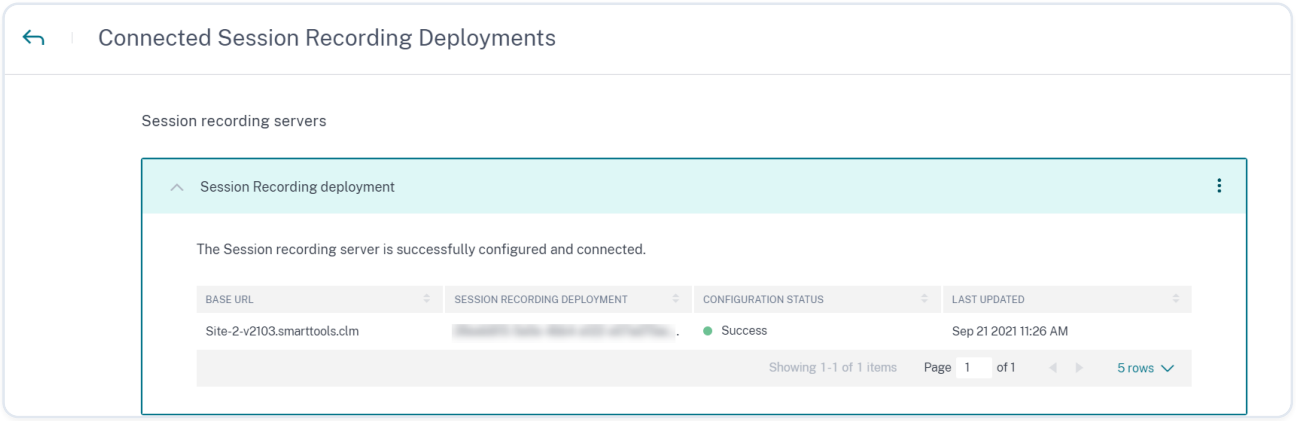
The server deployments appear on the Session Recording site card only if the configuration is successful. The site card shows the number of configured servers that have established connections with Citrix Analytics for Security.

If you don't see your Session Recording servers even after the configuration was successful, refer to the Troubleshooting article.

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



On the site card, click the number of deployments to view the connected server groups with Citrix Analytics for Security. For example, click **1 Session Recording Deployment** to view the connected server or server groups. Each Session Recording server is represented by a base URL and a ServerGroupID.



View received events

The site card displays the connected Session Recording deployments and the events received from these deployments for the last one hour, which is the default time selection. You can also select 1 week (1 W) and view the data. Click the number of received events to view the events on the self-service search page.

After you have enabled data processing, the site card might display the **No data received** status. This status appears for two reasons:

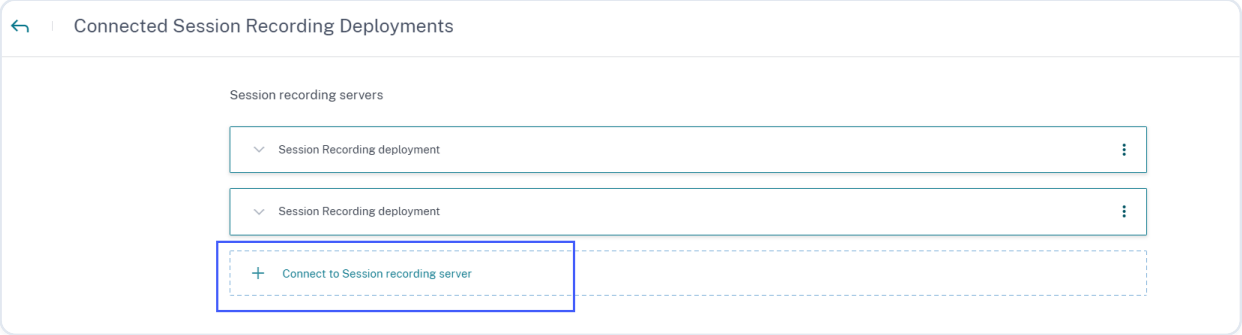
1. If you have turned on data processing for the first time, the events take some time to reach the event hub in Citrix Analytics. When Citrix Analytics receives the events, the status changes to **Data processing on**. If the status does not change after some time, refresh the Data Sources page.
2. Citrix Analytics has not received any events from the data source in the last one hour.

Add Session Recording servers

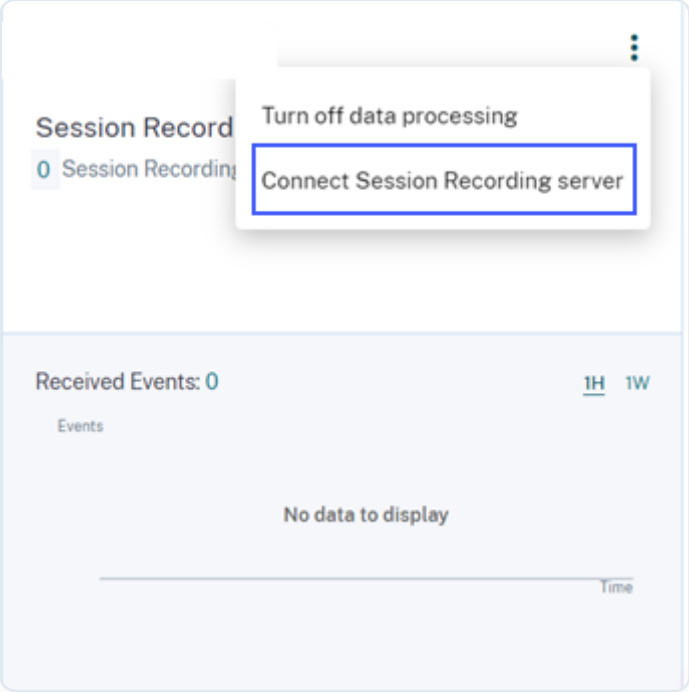
To add a Session Recording server, do one of the following:

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

- On the **Connected Session Recording Deployments** page, click **Connect to Session recording server**.



- On the **Apps and Desktops- Session Recording** site card, click the vertical ellipsis (⋮) and then select **Connect Session Recording server**.



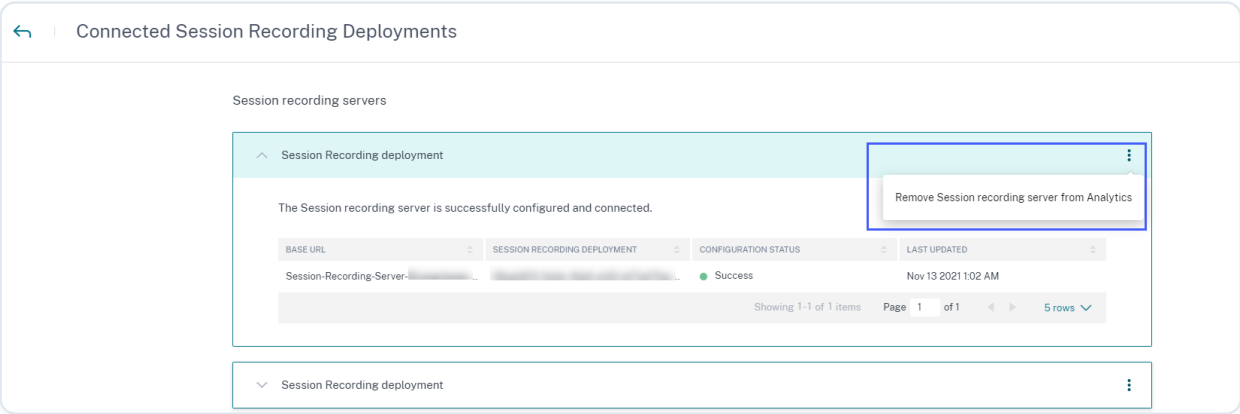
Follow the steps to download the configuration file and configure a Session Recording server.

Remove Session Recording servers

To remove a Session Recording server:

1. On Citrix Analytics for Security, go to the **Connected Session Recording Deployments** page and select the server deployment that you want to remove.
2. Click the vertical ellipses (⋮) and select **Remove Session Recording server from Analytics**.

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



3. On the Session Recording server that you have removed from Citrix Analytics, run the following command:

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

For example:

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

Enabling print telemetry for Citrix DaaS

When users perform printing jobs in Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), you can view the logs related to these printing jobs in Citrix Analytics for Security. These printing logs provide vital information about the printing activities such as printer names, print file names, and total printed copies.

NOTE

This feature is only supported for Citrix DaaS.

In Citrix Analytics for Security, on the **Search** page, you can select the **Apps and Desktops** data source to view the printing logs. As a security administrator, you can use these logs for risk analysis and investigation of your users.

By default, the print telemetry feature, which is the collection and transmission of these printing logs, is disabled on the Virtual Delivery Agents (VDAs).

To enable the print telemetry and transmission of printing logs to Citrix Analytics for Security, you need to create registry keys and configure your VDA.

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

IMPORTANT

This configuration is only applicable for the Windows VDAs.

Prerequisites

- Your VDA version must be the same as the baseline version for Citrix Virtual Apps and Desktops 7 2203 LTSR or later. For more information, see Citrix Virtual Apps and Desktops 7 2203 baseline components.
- You must have full access permissions to perform the registry key updates.

Enable print telemetry in power managed machines

The power-managed machines include virtual machines or blade PCs with the following scenarios:

- Existing master image
- New master image

Enable print telemetry for an existing master image where the VDA version is lower than Citrix Virtual Apps and Desktops 7 2203 LTSR

1. Log in to the master VDA machine and create a snapshot of the current state.
2. Enable print service logs by adding the following registry keys:
   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   For more information about the registry keys, see Create registry keys.
3. Upgrade the VDA to a baseline version for Citrix Virtual Apps and Desktops 7 2203 LTSR or later. For more information, see Citrix Virtual Apps and Desktops 7 2203 baseline components.
4. Power off the machine and take a snapshot of the latest state.
5. Log in to Citrix Cloud. Select the machine catalog, click **Update Machines**, and follow the on-screen instructions. For more information, see Create machine catalogs.
6. Wait for 24 hours. The configuration is pushed automatically within 24 hours. If the configuration is already completed, you need not wait.
7. Start a desktop session using Citrix Workspace app. All the triggered print events using the client printer are visible on the **Search** page in Citrix Analytics for Security.

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

Enable print telemetry for an existing master image where the VDA version is the same as Citrix Virtual Apps and Desktops 7 2203 LTSR or later

Option 1: Add the print registry keys in the master VDA and update virtual desktops.

1. Log in to the master VDA machine and create a snapshot of the current state.
2. Enable print service logs by adding the following registry keys:
   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   For more information about the registry keys, see Create registry keys.
3. Power off the VDA machine and take a snapshot of the latest state.
4. Log in to Citrix Cloud, select the machine catalog, click **Update Machines**, and follow the on-screen instructions.
5. Start a desktop session using Citrix Workspace app. All the triggered print events using the client printer are visible on the **Search** page in Citrix Analytics for Security.

Option 2: Move the virtual desktop to the organizational unit (OU) and create registry keys using GPO

NOTE

Option 2 method only works for static machines. For random machines, you must follow the option 1 method (as mentioned above).

1. Log in to the Domain Controller machine.
2. Enable print service logs by adding the following registry keys:
   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   For more information about the registry keys, see Create registry keys.

NOTE

In any domain controller, creating the registry keys is a one-time task.

1. Restart the VDA machine from Citrix Cloud.

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

2. Start a desktop session using Citrix Workspace app. All the triggered print events using the client printer are visible on the **Search** page in Citrix Analytics for Security.

Enable print telemetry in a new master image

1. Create a virtual machine (VM) by using the hypervisor's management tool. This VM is treated as a master VDA.
2. Ensure that the master VDA is added to the required domain.
3. Log in to the master VDA and enable the print service logs by adding the following registry keys:

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   For more information, see Create registry keys.
4. Install the VDA version for Citrix Virtual Apps and Desktops 7 2203 LTSR or later. While installing the VDA, select the **Master Image** option. For more information, see Citrix Virtual Apps and Desktops 7 2203 baseline components.
5. Ensure that the hosting connection is added to Citrix Cloud. For more information, see Create machine catalogs.
6. Create a machine catalog using the master image. For more information, see Create machine catalogs.
7. Create a delivery group and add the machine catalog. For more information, see Create delivery groups.
8. Wait for 24 hours. The configuration is pushed automatically within 24 hours by the group policy engine.
9. Start a desktop session using Citrix Workspace app. All the triggered print events using the client printer are visible on the **Search** page in Citrix Analytics for Security.

Enable print telemetry in machines that are not power managed

The non-power managed machines include the physical computers with the following scenarios:

- Existing physical VDA
- New physical VDA

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

Enable print telemetry for an existing physical VDA where the VDA version is lower than Citrix Virtual Apps and Desktops 7 2203 LTSR

1. Enable print service logs by adding the following registry keys:

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   For more information, see Create registry keys.
2. Upgrade the VDA to a baseline version for Citrix Virtual Apps and Desktops 7 2203 LTSR or later. For more information, see Citrix Virtual Apps and Desktops 7 2203 baseline components.
3. Wait for 24 hours. The configuration is pushed automatically within 24 hours. If the configuration is already completed, then you need not wait.
4. Start a desktop session using Citrix Workspace app. All the triggered print events using the client printer are visible on the **Search** page in Citrix Analytics for Security.

Enable print telemetry for a new physical VDA

1. Create a physical VM and change the domain to the required domain name.
2. Log in to the VM and enable the print service logs by adding the following registry keys:

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   For more information, see Create registry keys.
3. Install the VDA version for Citrix Virtual Apps and Desktops 7 2203 LTSR release or later. While installing VDA, select the Remote PC Access option.
4. Create a machine catalog. For more information, see Create machine catalogs.

   NOTE

   Machine management must be selected as **Machines that are not power managed (for example, physical machines)**.
5. Create a delivery group and add the machine catalog. For more information, see Create delivery groups.
6. Wait for 24 hours. The configuration is pushed automatically within 24 hours by the group policy engine.

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

7. Start a desktop session using Citrix Workspace app. All the triggered print events using the client printer are visible in the **Search** page in Citrix Analytics for Security.

Create registry keys

In your VDA, do one of the following options:

- Create registry keys manually. Use this method for master VDAs and having a smaller number of physical VDAs in your deployment.
- Create registry keys by using group policy object (GPO). Use this method when your deployment has a greater number of physical VDA machines and must enable the print telemetry in all of them.

Registry keys details

SL	REGISTRY KEY NAME	PURPOSE OF THE KEY	REGISTRY DETAILS
1	Microsoft-Windows-PrintService/Operational	Enables print service logs in the event viewer.	**Registry path**: HKLM:\SYSTEM\CurrentControlSet\Services\EventLog
2	ShowJobTitleInEventLogs	Controls whether the print job name is included in print event logs, otherwise considers the generic job name "Print Document.	**Registry Hive**: HKEY_LOCAL_MACHINE
			Registry Path: Software\Policies\Microsoft\Windows NT\Printers
			Value Name: ShowJobTitleInEventLogs
			Value Type: REG_DWORD

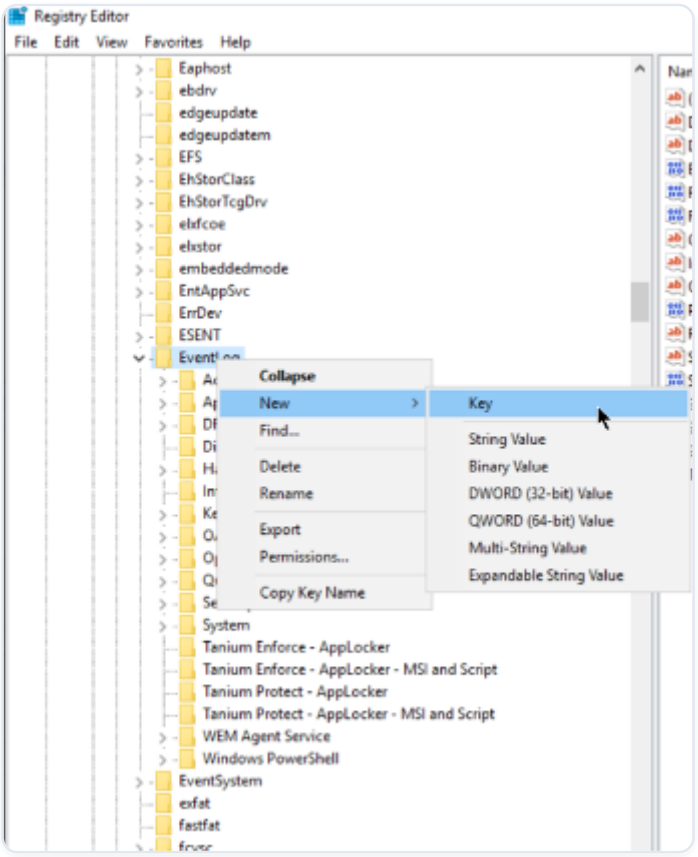
© 1997–2026 Citrix Systems, Inc. All rights reserved.

SL	REGISTRY KEY NAME	PURPOSE OF THE KEY	REGISTRY DETAILS
			Value: 1

Create registry keys manually in a VDA machine

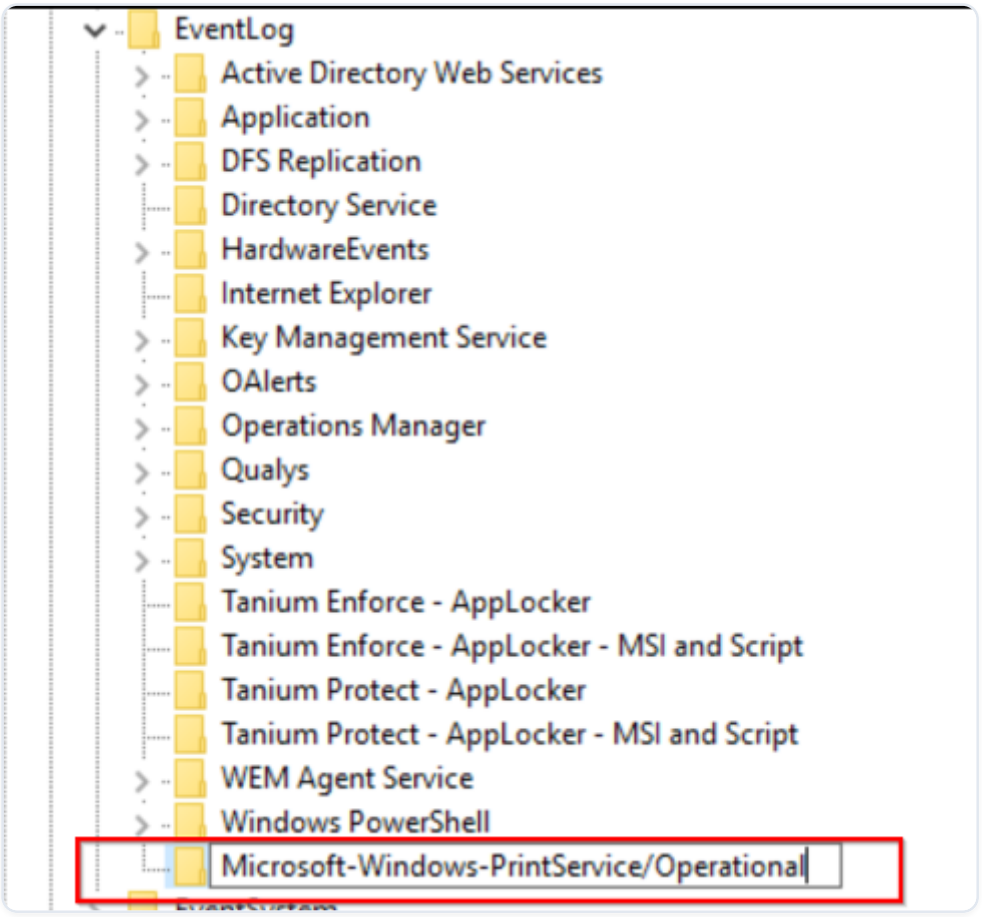
Use this approach to create the registry key in the VDA master image. Adding keys to the master image helps to keep the keys persistent for all types of VDAs that are created by using the master image.

1. Sign in to the VDA master machine.
2. Open Run and type Regedit to open the Windows registry.
3. Go to location HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog
4. Right-click **EventLog** and select **New > Key**.



5. Create a key with the name **Microsoft-Windows-PrintService/Operational**. This key enables the print service logs.

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

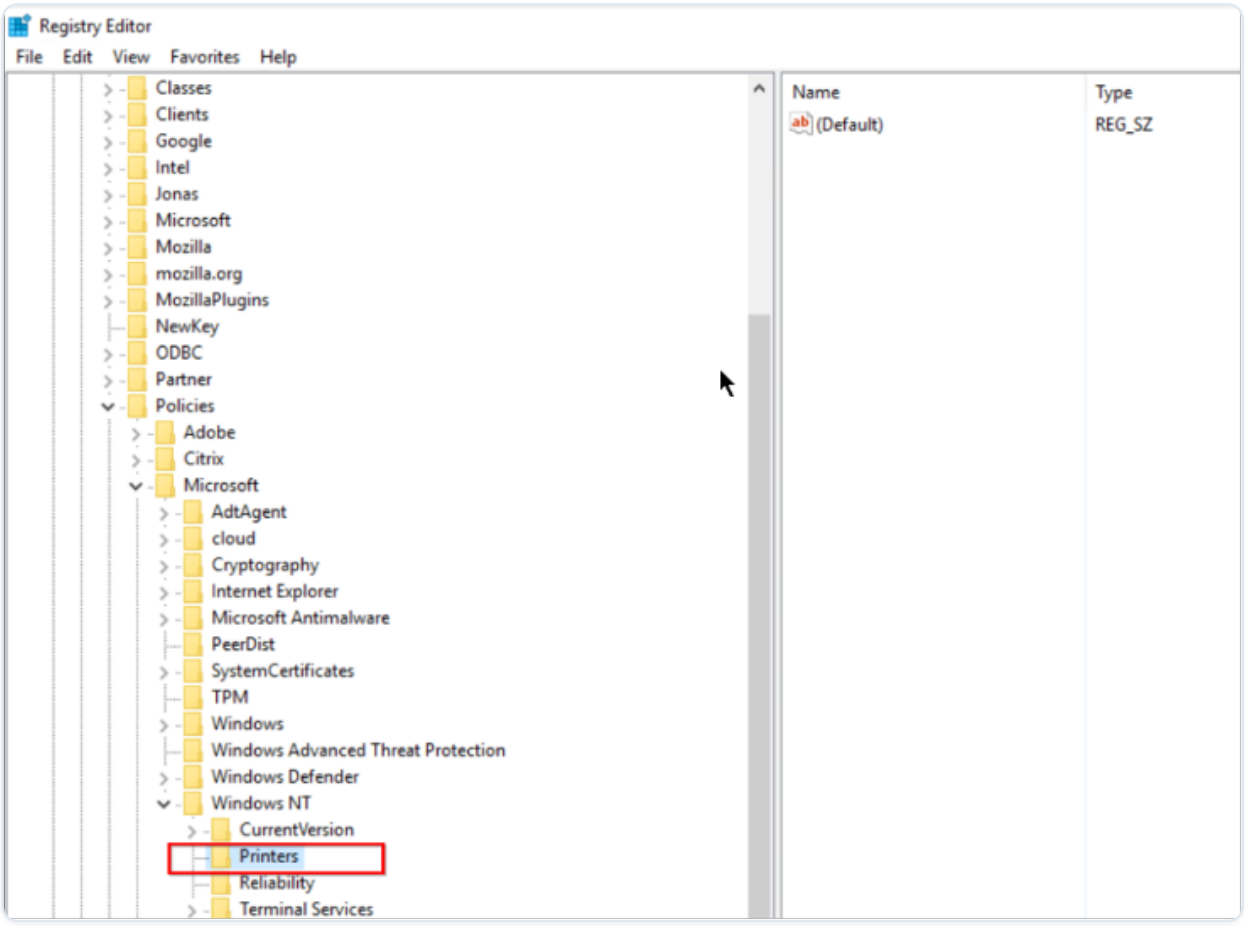


6. Go to the location **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers**.

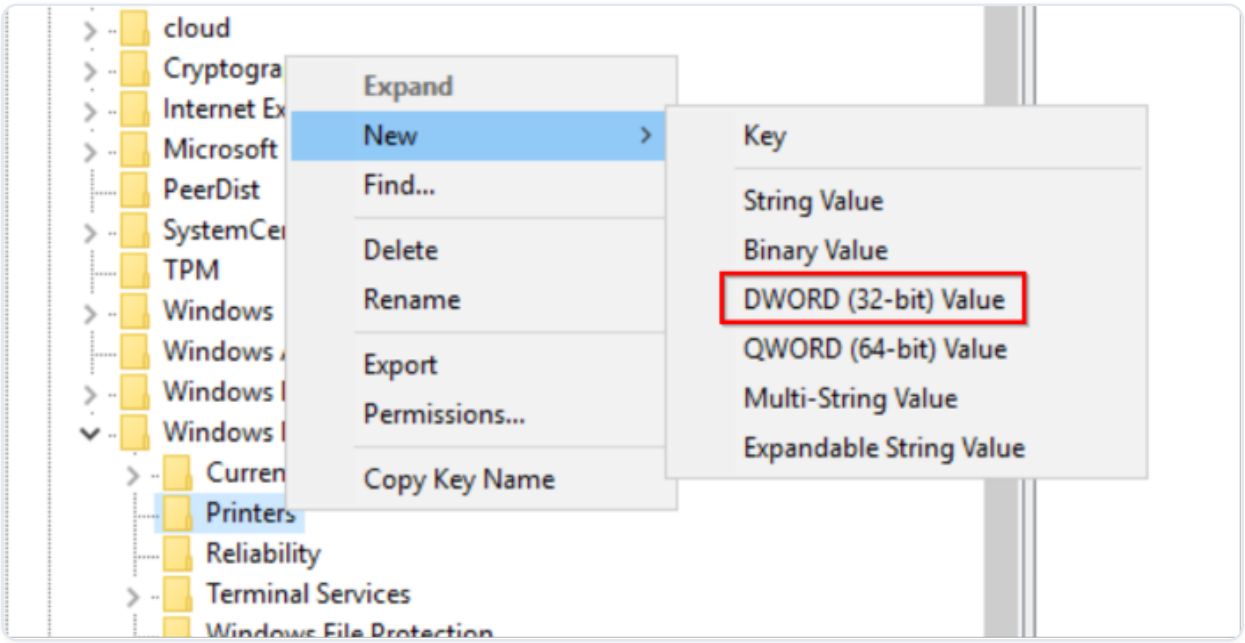
NOTE

If the Printers folder is not available, then create a key with the name Printers in the Windows NT folder.

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

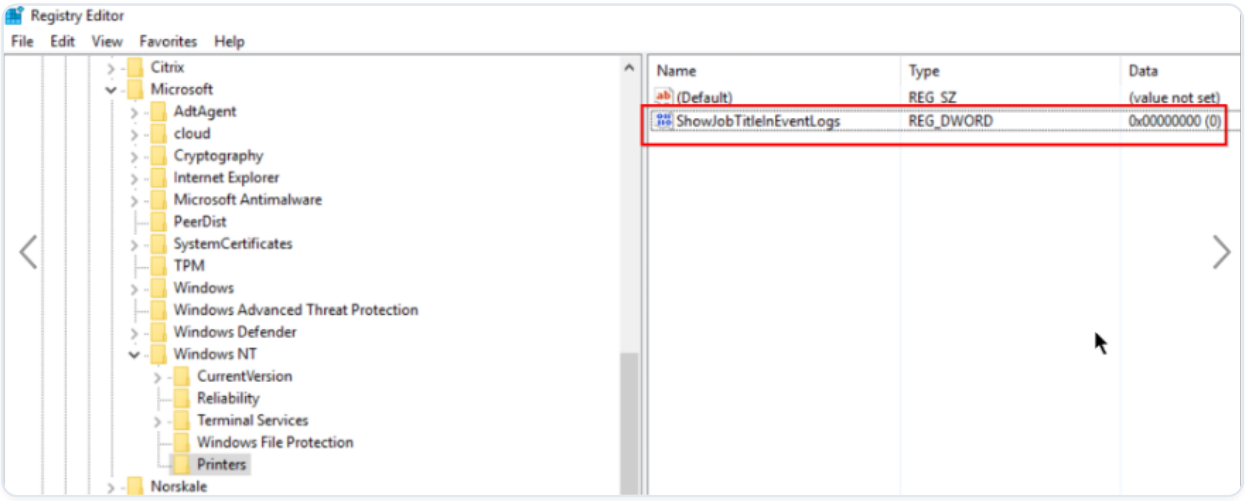


7. Right-click the **Printers** folder and select **New > DWORD (32-bit) Value**.

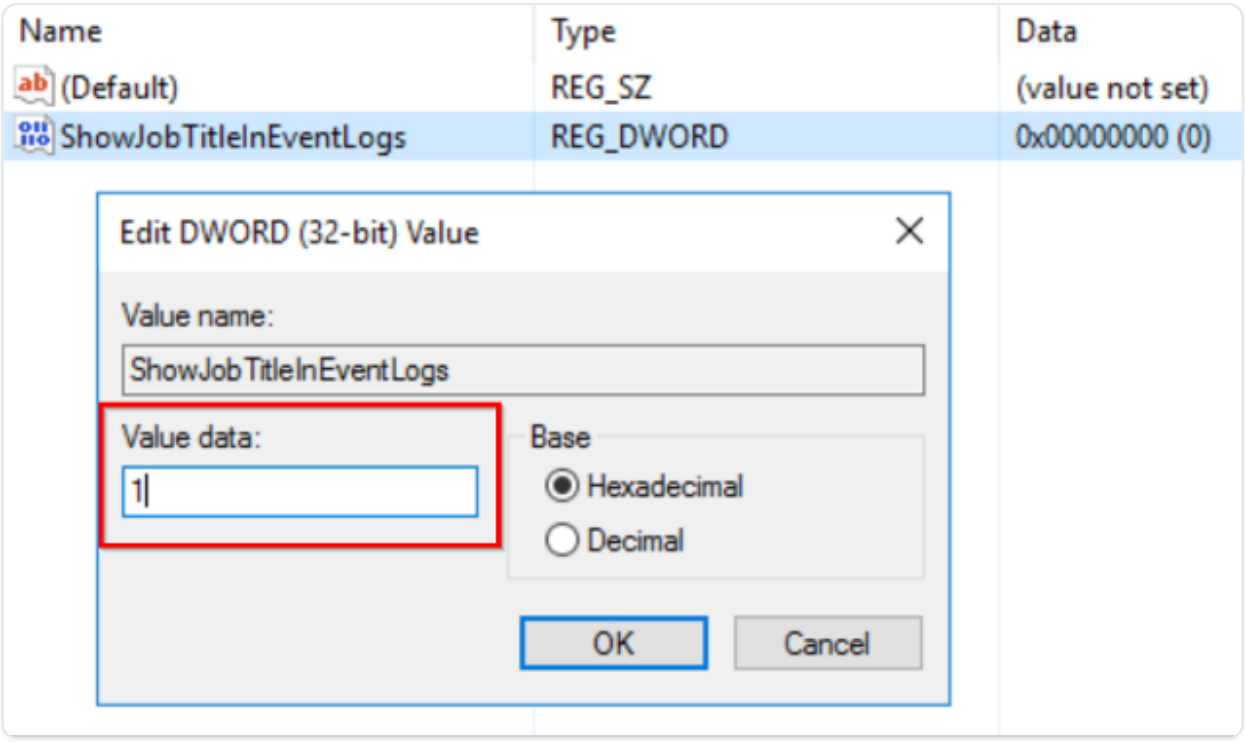


8. Create a value with the name **ShowJobTitleInEventLogs**.

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



9. Right-click **ShowJobTitleInEventLogs** and select **Modify**. Enter the **Value data** as 1 and click **OK**.



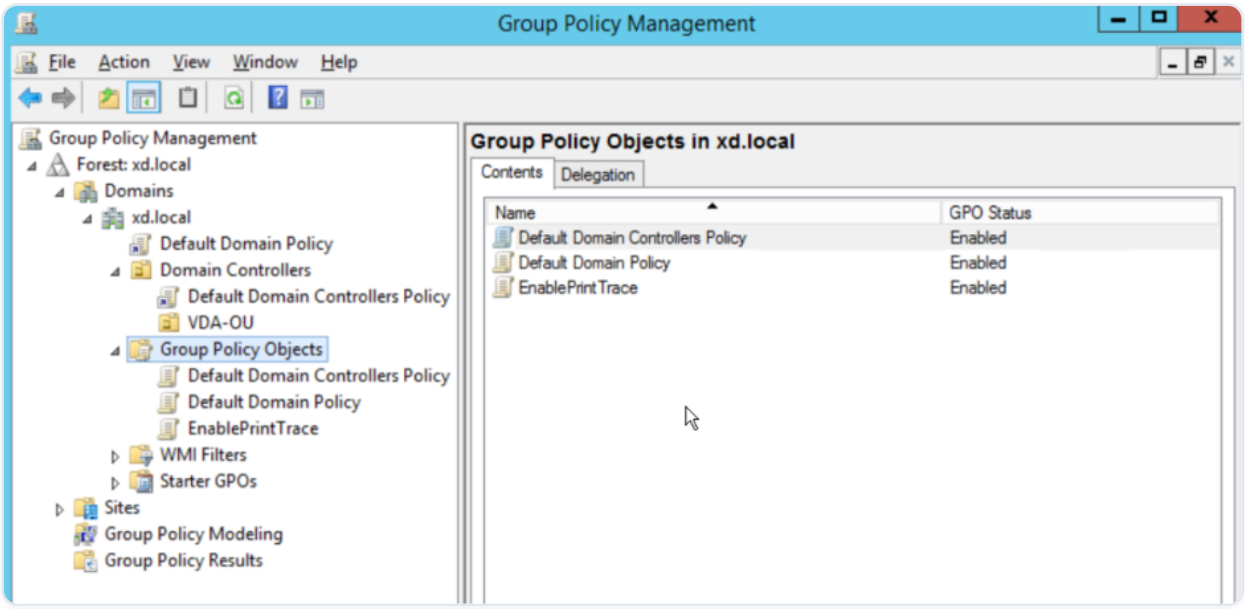
Create registry keys in multiple VDAs using GPO

This approach works only for the persistent VDAs and requires restart of the VDAs after creation of the registry keys. A persistent VDA is a machine that maintains its state after a restart. The users' data are not lost after the restart.

Create registry GPO with the registry keys

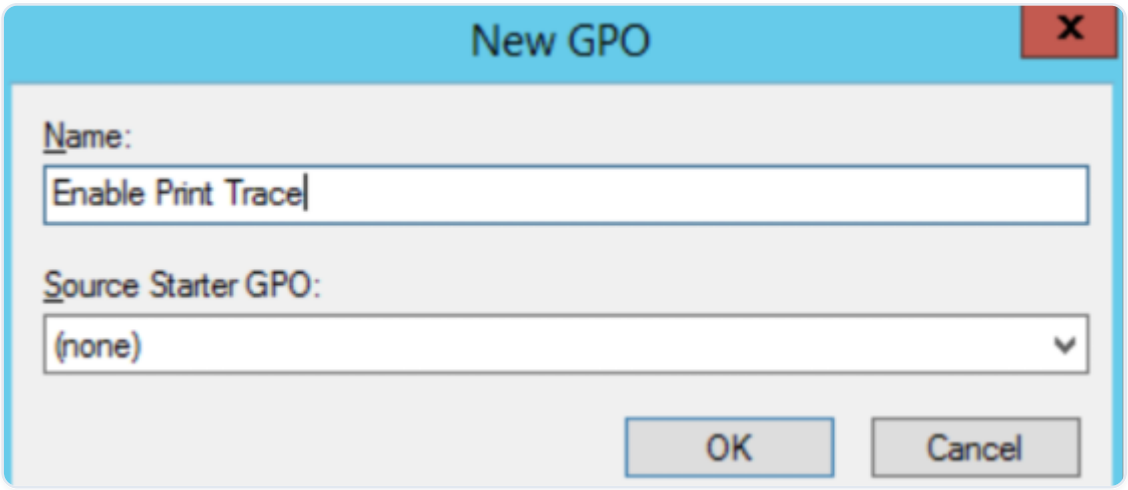
1. Open Group Policy Management and right-click **Group Policy Objects**.

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



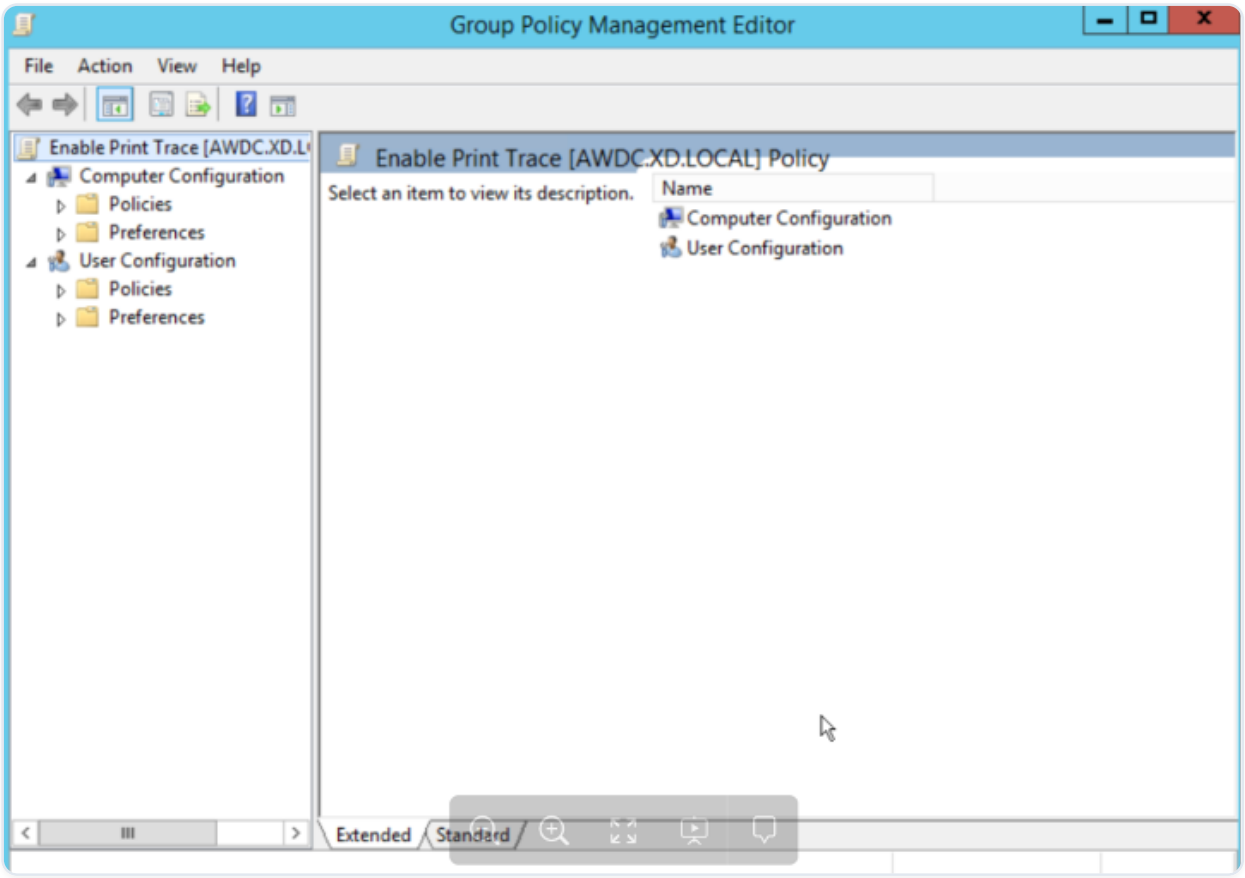
2. In the **New GPO** window, enter the values in the following fields:

   - Name: Enable Print Trace
   - Source Starter GPO: (none)



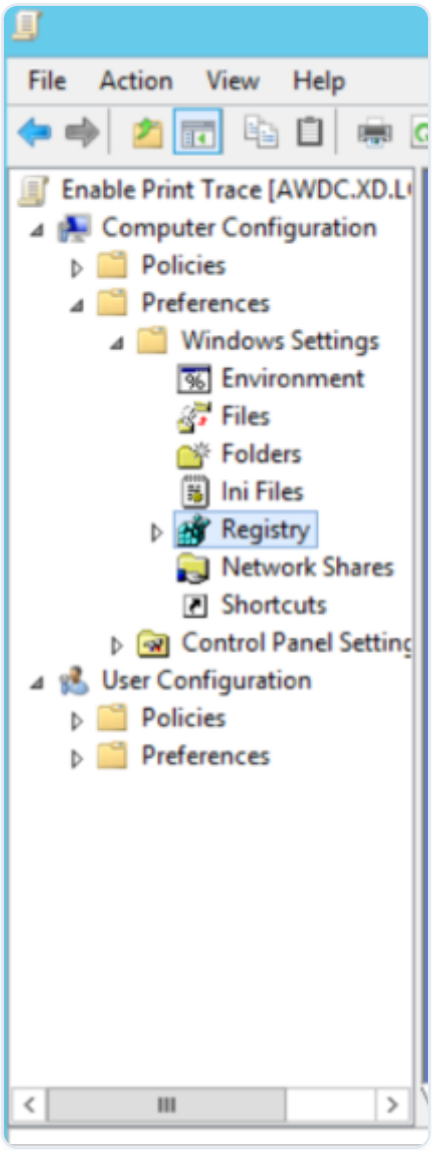
3. Select **OK**.
4. Right-click the **Enable Print Trace** object that you created and select **Edit**.

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



5. In the **Computer Configuration** list, select **Preferences > Windows Settings**.

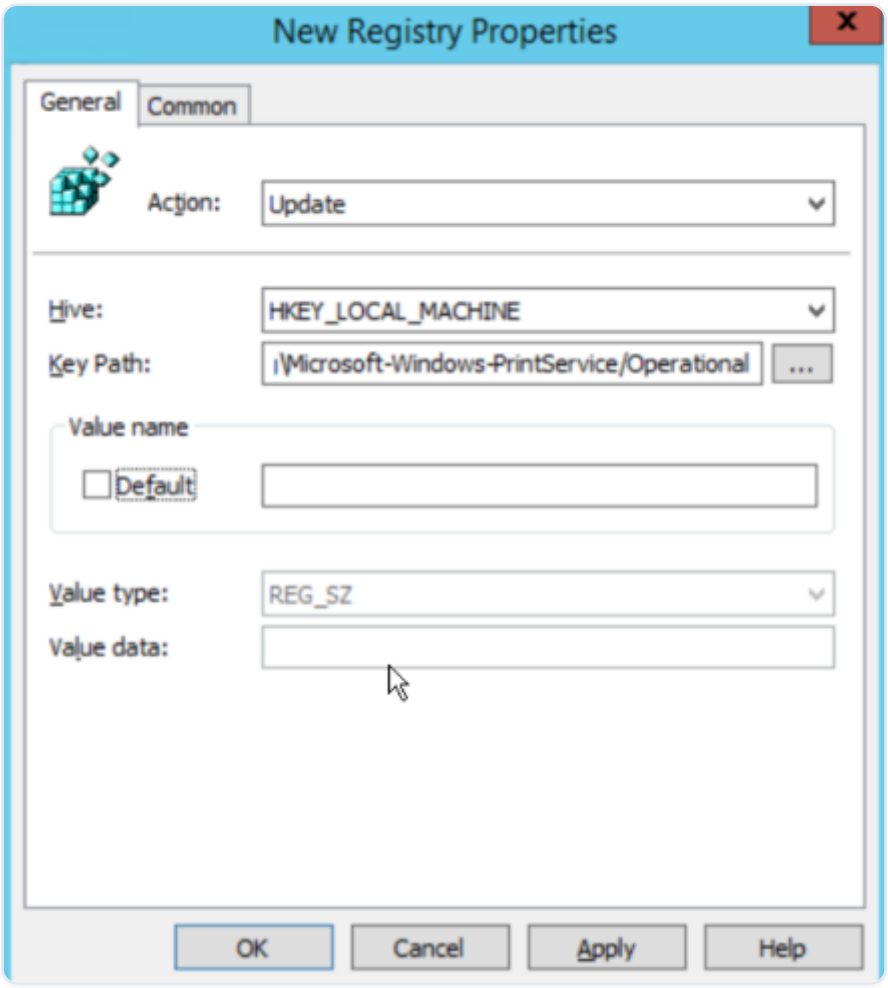
© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Right-click **Registry**, select **New > Registry Item**. Enter the following properties to enable print logs:

    - Action: Update
    - Hive: HKEY_LOCAL_MACHINE
    - Key Path: SYSTEM\CurrentControlSet\Services\EventLog\Microsoft-Windows-PrintService/Operational

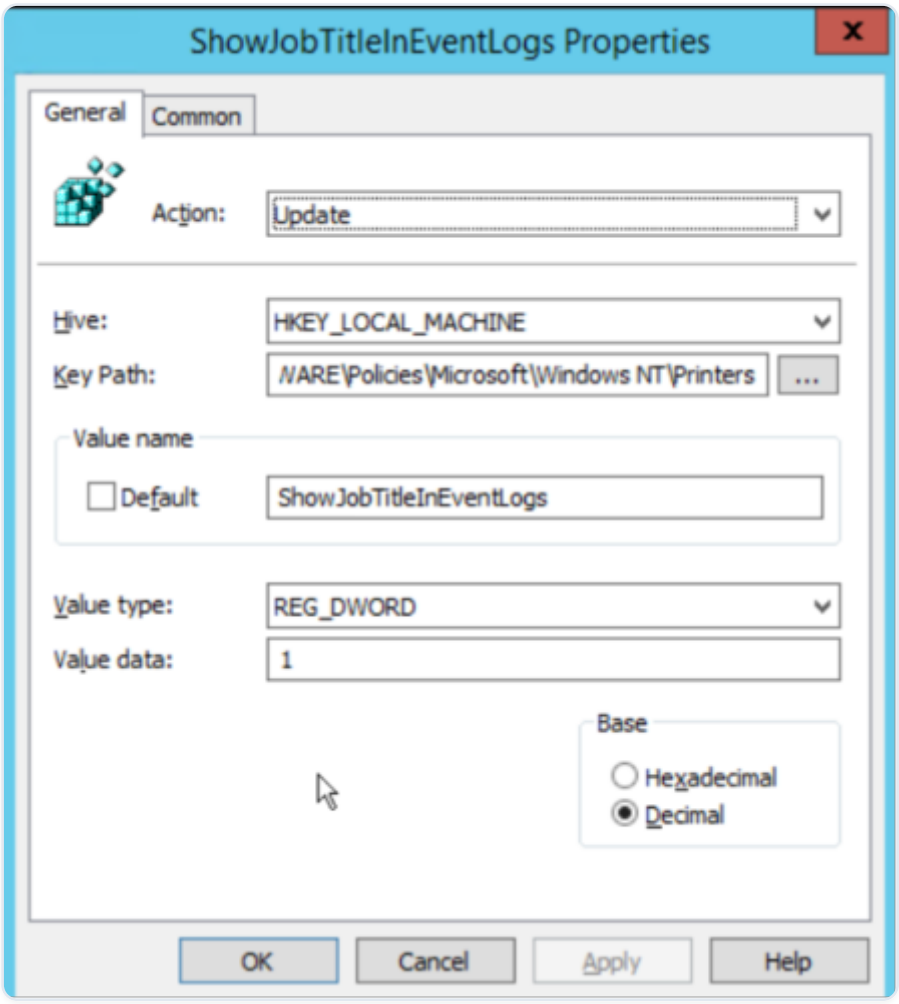
© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. Select **Apply** and then select **OK**.
8. Again, right-click **Registry**, select **New > Registry** Item. Enter the following properties to enable print job names:

    - Action: Update
    - Hive: HKEY_LOCAL_MACHINE
    - Key Path: SOFTWARE\Policies\Microsoft\Windows NT\Printers
    - Value Name: ShowJobTitleInEventLogs
    - Value Type: REG_DWORD
    - Value Data: 1
    - Base: Decimal

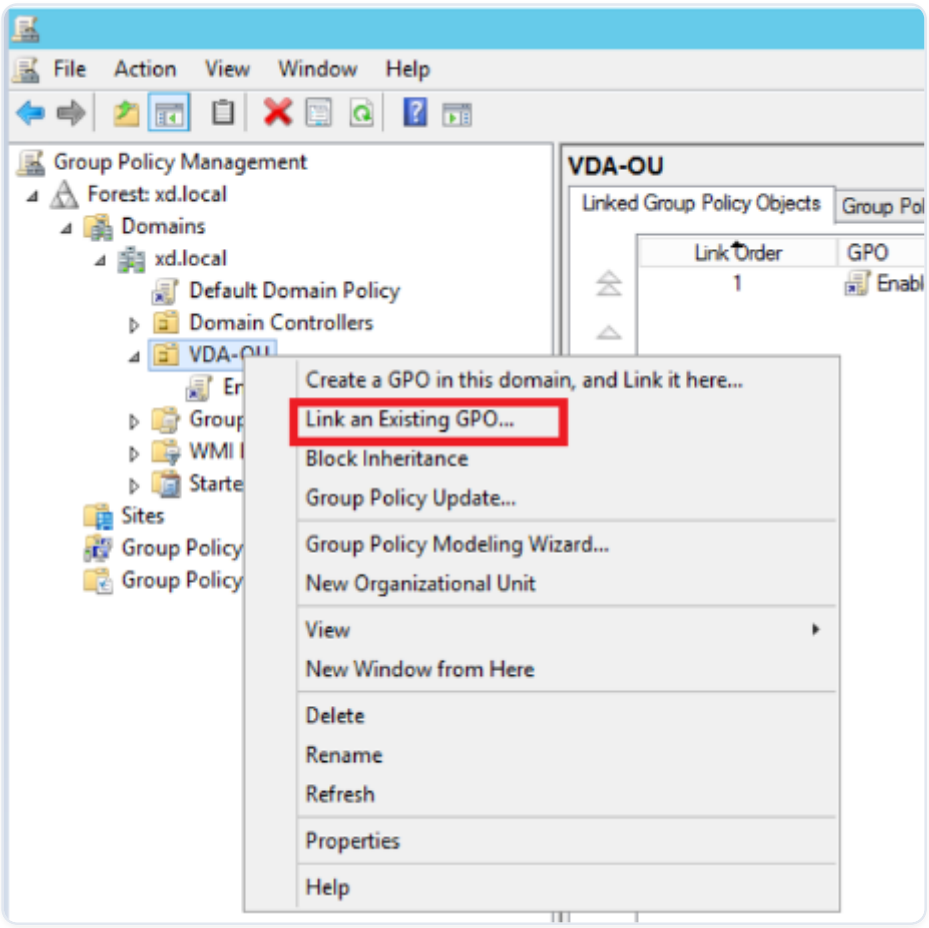
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Enable print trace for the organizational unit

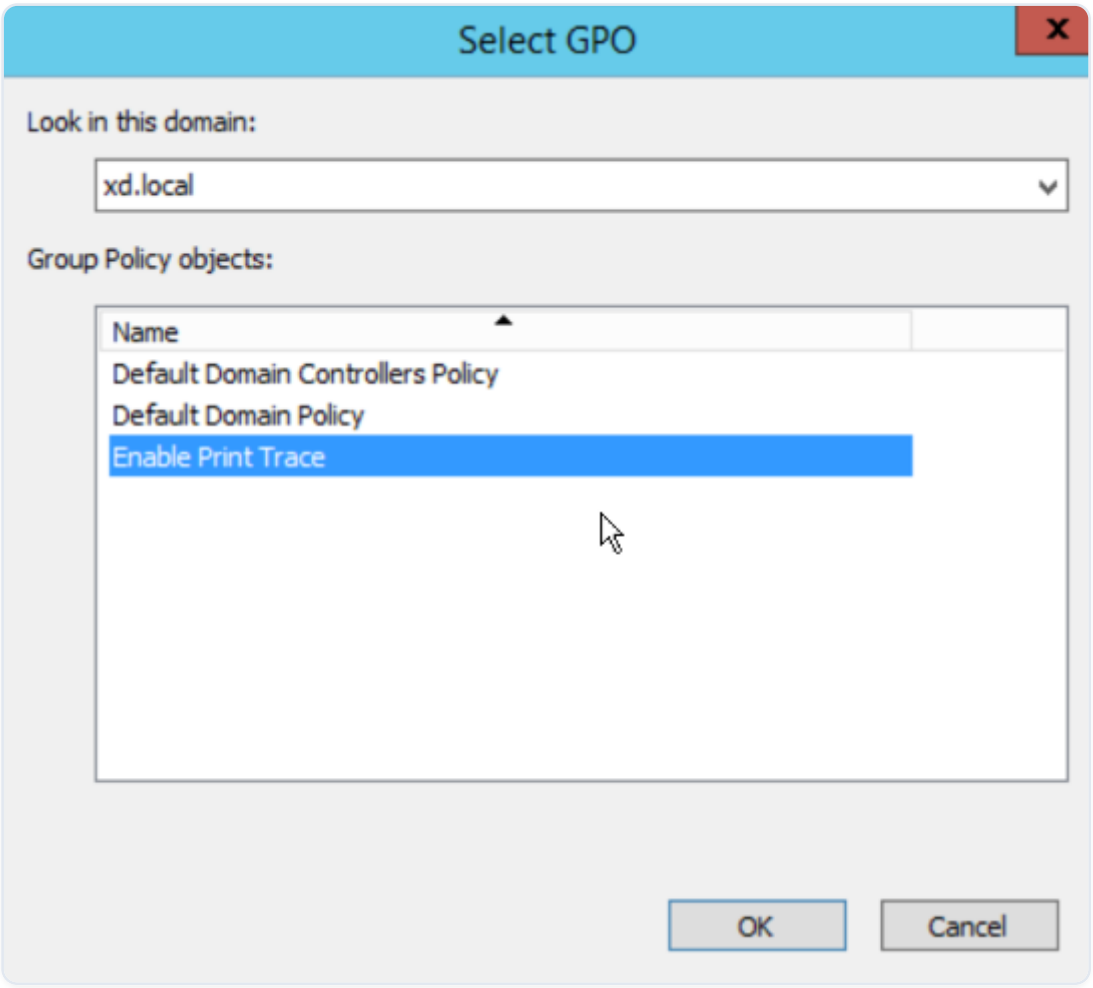
1. Open **Group Policy Management** and select the domain (for example - xd.local) or the OU if VDAs are part of it (for example - VDA-OU).
2. Right-click the domain (xd.local) or OU (VDA-OU) and select **Link an Existing GPO**.

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

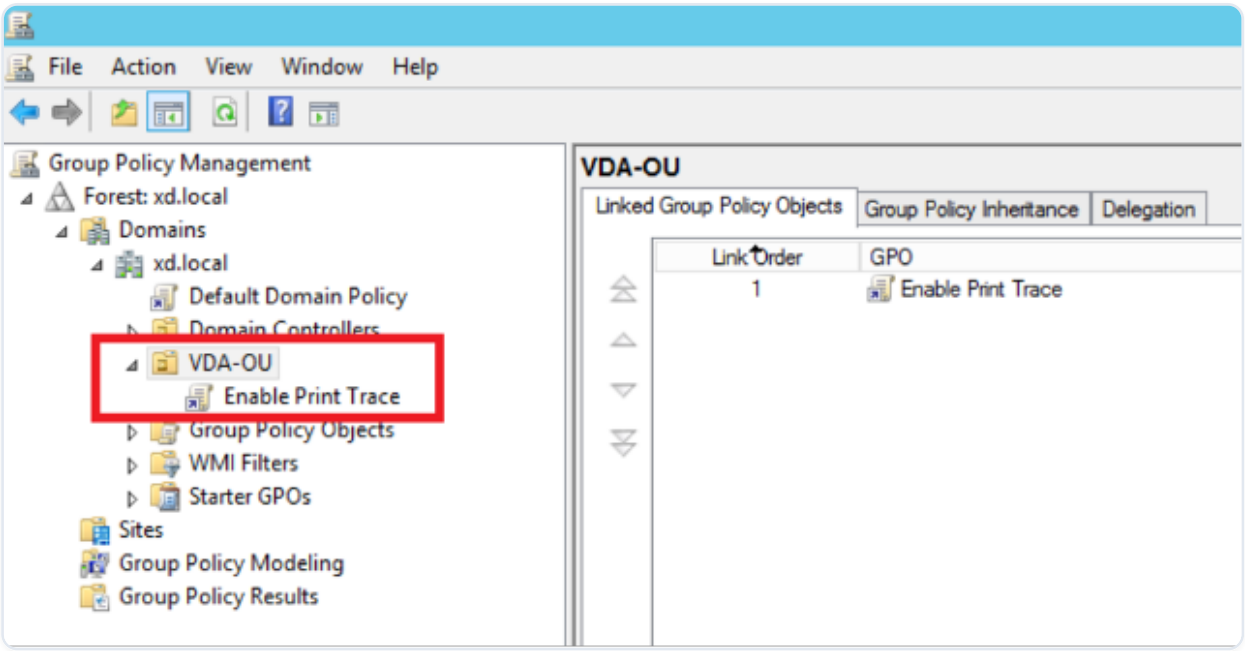


3. In the **Select GPO** dialog box, select Enable Print Trace and select **OK**.

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



4. Verify that the **Enable Print Trace GPO** is linked to the OU.



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

NOTE

- When you do a VDA restart, any events in the queue are lost and will not be available in Citrix Analytics.
- This restart has a low impact on a single session VDA because only one session can be active at a given time, accordingly the number of events are less.
- This restart has a high impact on a multi-session VDA as all the active sessions are terminated during the restart and the events that are in the queue are lost.

Enabling clipboard telemetry for Citrix DaaS

Citrix DaaS (formerly known as Citrix Virtual Apps and Desktops service) allows users to perform clipboard operations, and the related logs can be viewed in Citrix Analytics for Security. These clipboard logs provide valuable information such as the VDA name, clipboard size, clipboard format type, client IP, clipboard operation, clipboard operation direction, and whether the clipboard operation was permitted.

As a security administrator, you can use these logs for risk analysis and investigations by selecting the **Apps and Desktops** data source on the **Search** page in Citrix Analytics for Security.

NOTE

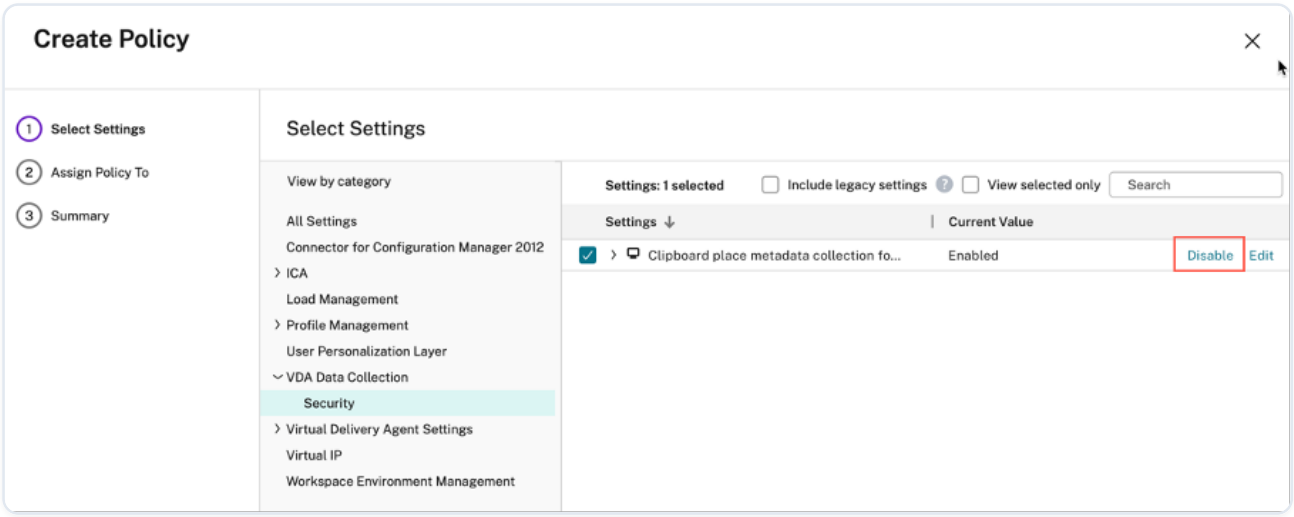
- By default, the collection and transmission of these clipboard logs is enabled on the Virtual Delivery Agents (VDAs).
- This configuration is only applicable for the Windows VDAs.

Prerequisites

- Your VDA version must be the same as the baseline version for Citrix Virtual Apps and Desktops 7 2305 or later. For more information, see Citrix Virtual Apps and Desktops 7 2305.
- Ensure that the **Client Clipboard Redirection** setting on the **Web Studio Policies** page is not configured to a prohibited state. For more information, see Client clipboard redirection.

You can use the **Clipboard place metadata collection for Security monitoring** policy to enable or disable the clipboard telemetry. By default, this policy is enabled. To disable, you must go to the **Policy** page > select **Security** under the **VDA Data Collection** > check the policy > click **Disable**.

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



For more information, see Clipboard place metadata collection for Security monitoring.

Turn on or off data processing on the data source

You can stop the data processing at any time for a particular data source- Director and Workspace app. On the data source site card, click the **vertical ellipsis (⋮) > Turn off data processing**. Citrix Analytics stops processing data for that data source. You can also stop the data processing from the Apps and Desktops site card. This option applies to both data sources- Director and Workspace app.

To enable data processing again, click **Turn On Data Processing**.

Microsoft Active Directory and Azure Active Directory integration

NOTE:

Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

Connect your Active Directory or your Azure Active Directory and import the user details and the user groups from your organization's domain to Citrix Analytics for Security.

This integration enhances the user profiles in Citrix Analytics for Security with user identity details such as job title, organization, office location, email, and contact details. On the User profile page, you can view these user details, which help you during risk investigation and analysis.

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

Prerequisites

- If you want to connect Active Directory with Citrix Analytics for Security, ensure that your Active Directory is first connected to your Citrix Cloud account. For more information, see Connect Active Directory to Citrix Cloud.
- If you want to connect Azure Active Directory with Citrix Analytics for Security, ensure that your Azure Active Directory is first connected to your Citrix Cloud account. For more information, see Connect Azure Active Directory to Citrix Cloud.

Connect Microsoft Active Directory

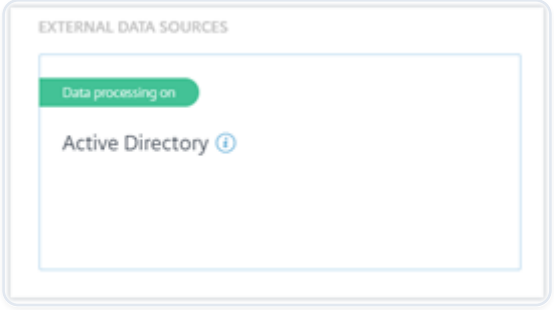
To connect your Active Directory to Citrix Analytics for Security, do the following:

1. Go to **Settings** > **Data Sources** > **Security** and then navigate to the **EXTERNAL DATA SOURCES** section.
2. On the **Active Directory** site card, click the plus **+** sign.



3. Citrix Analytics prompts you to connect Active Directory to your Citrix Cloud™ account. For more information, see Prerequisites.

After you have connected your Active Directory to your Citrix Cloud account, Citrix Analytics automatically discovers this new data source. On the **Data Sources** page, the Active Directory site card displays **Data processing on**.



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

The **Data processing on** status indicates that the Active Directory is discovered and user information is being fetched from your Active Directory.

Connect Microsoft Azure Active Directory

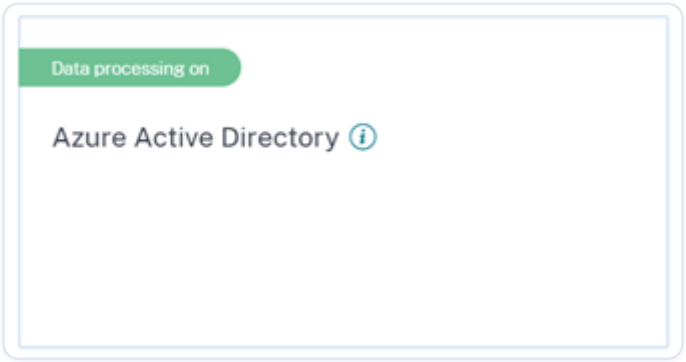
To connect your Azure Active Directory to Citrix Analytics, do the following:

1. Go to **Settings > Data Sources > Security** and then navigate to the **EXTERNAL DATA SOURCES** section.
2. On the **Azure Active Directory** site card, click the plus + sign.



3. Citrix Analytics prompts you to connect Azure Active Directory to your Citrix Cloud account. For more information, see Connect Azure Active Directory to Citrix Cloud.

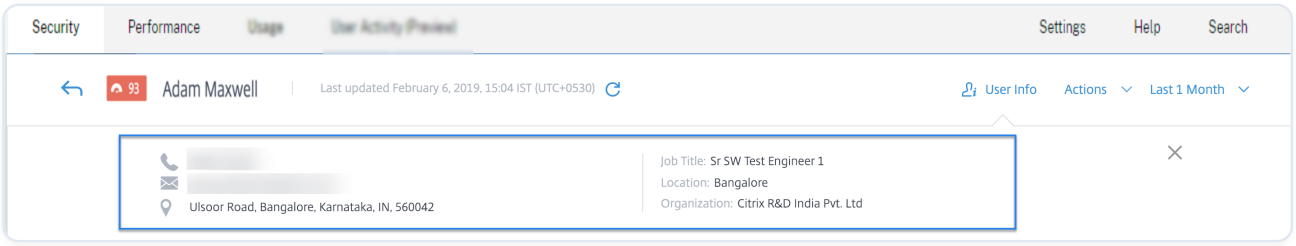
After you have connected your Azure Active Directory to your Citrix Cloud account, Citrix Analytics automatically discovers this new data source. On the **Data Sources** page, the **Azure Active Directory** site card displays **Data processing on**. This status indicates that the Azure Active Directory is discovered and the user information is being fetched from your Azure Active Directory.



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

View user information

From the **Security** tab, click a risky user to view the user profile page. If the user is available in Active Directory or Azure Active Directory, you can view their job title, organization, email, and contact number on the user profile page.



Microsoft Graph Security integration

Microsoft Graph Security is an external data source that aggregates data from multiple security providers. It also provides access to the user inventory data.

Citrix Analytics currently supports the following security providers from Microsoft Graph Security:

- Azure AD identity protection
- Microsoft Defender for Endpoint

For more information on the security providers, see the following links:

- For **Azure AD Identity Protection**: `<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events>`
- For **Microsoft Defender for Endpoint**: `<https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection>`

To onboard the Microsoft Graph Security data source, you need to obtain the required permissions on behalf of a tenant, from the Microsoft identity platform.

Prerequisites

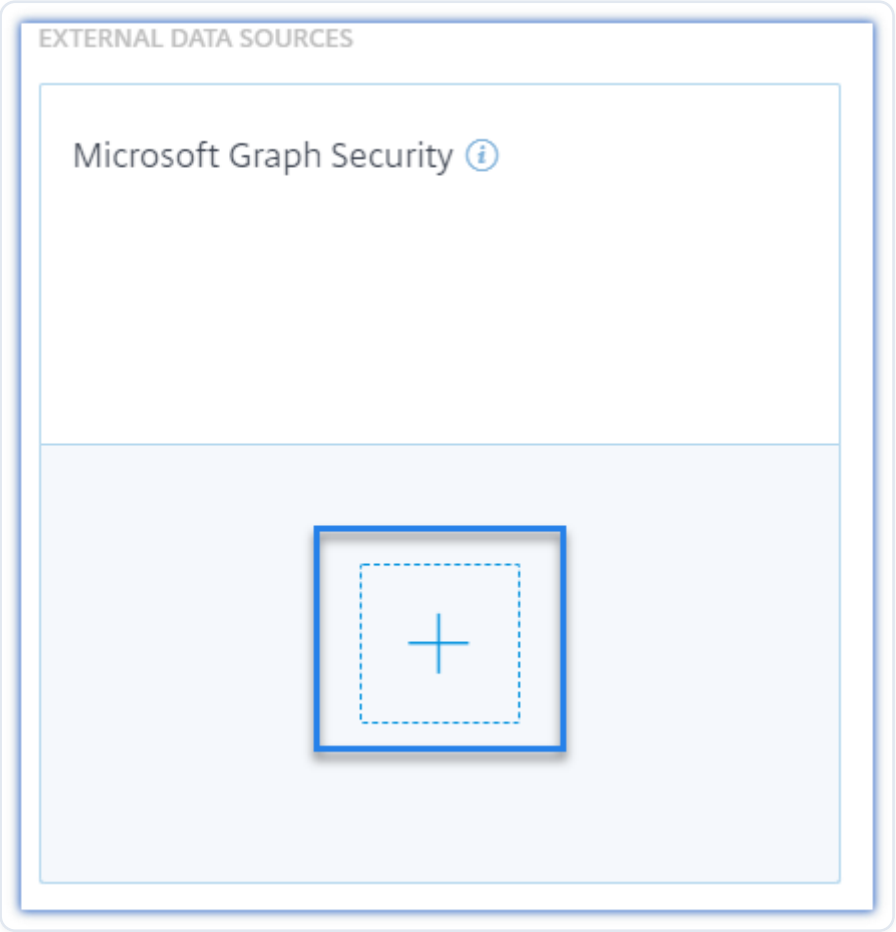
Before you begin onboarding the Microsoft Graph Security data source, ensure that:

- The administrator is using the Azure AD Identity Protection (part of the Azure AD Premium P2) security provider.
- The end user is signed in to Microsoft Store with Work or School accounts.

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

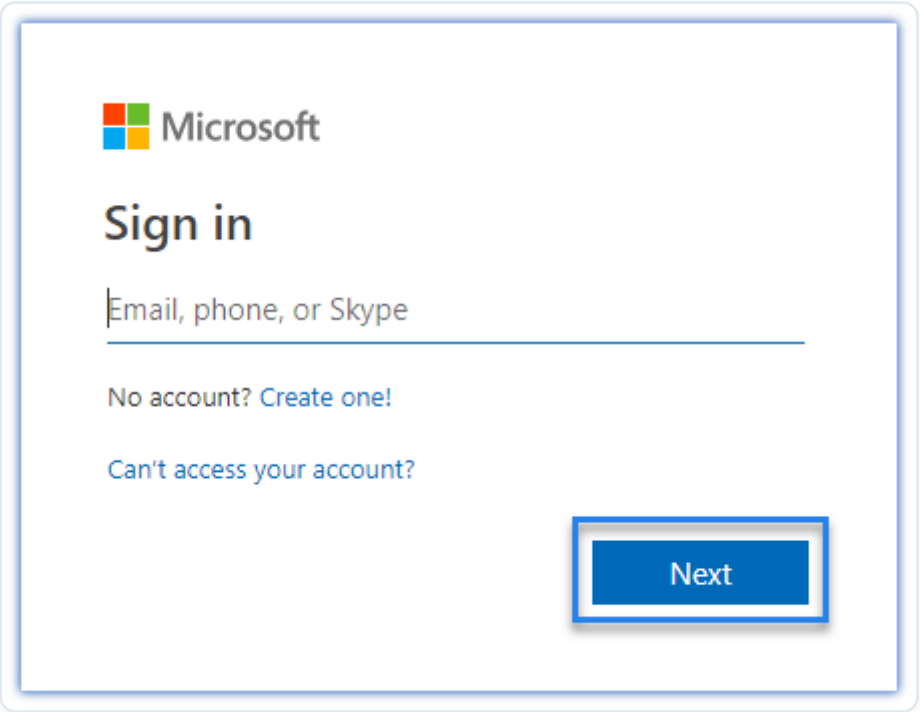
Onboarding Microsoft Graph Security instances

1. Go to **Settings** > **Data Sources** > **Security** and then navigate to the **EXTERNAL DATA SOURCES** section.
2. Click the plus (**+**) sign on the Microsoft Graph Security site card. You get redirected to the authorize endpoint.



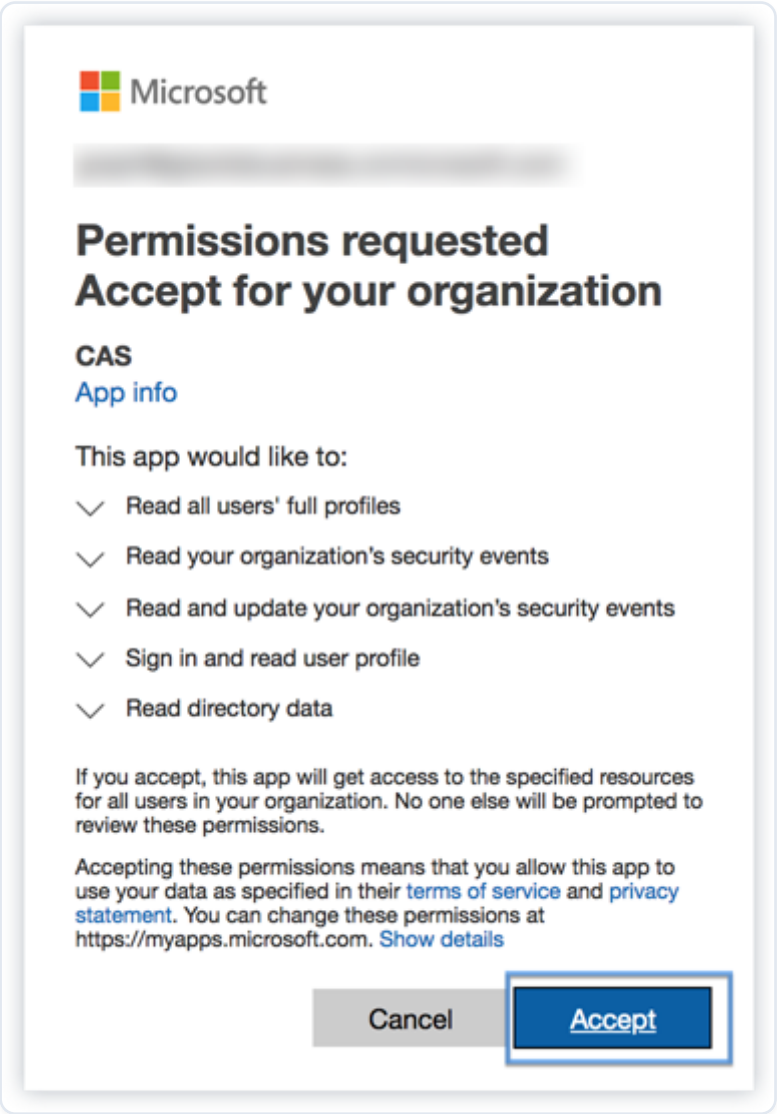
3. On the **Microsoft** window, sign in using your Azure logon credentials to register an account. Or, select an existing account.
4. Click **Next**.

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



5. Click **Accept**. You get redirected to the Data Sources page. The Microsoft Graph Security data source is now linked to your Citrix Cloud™ account.

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

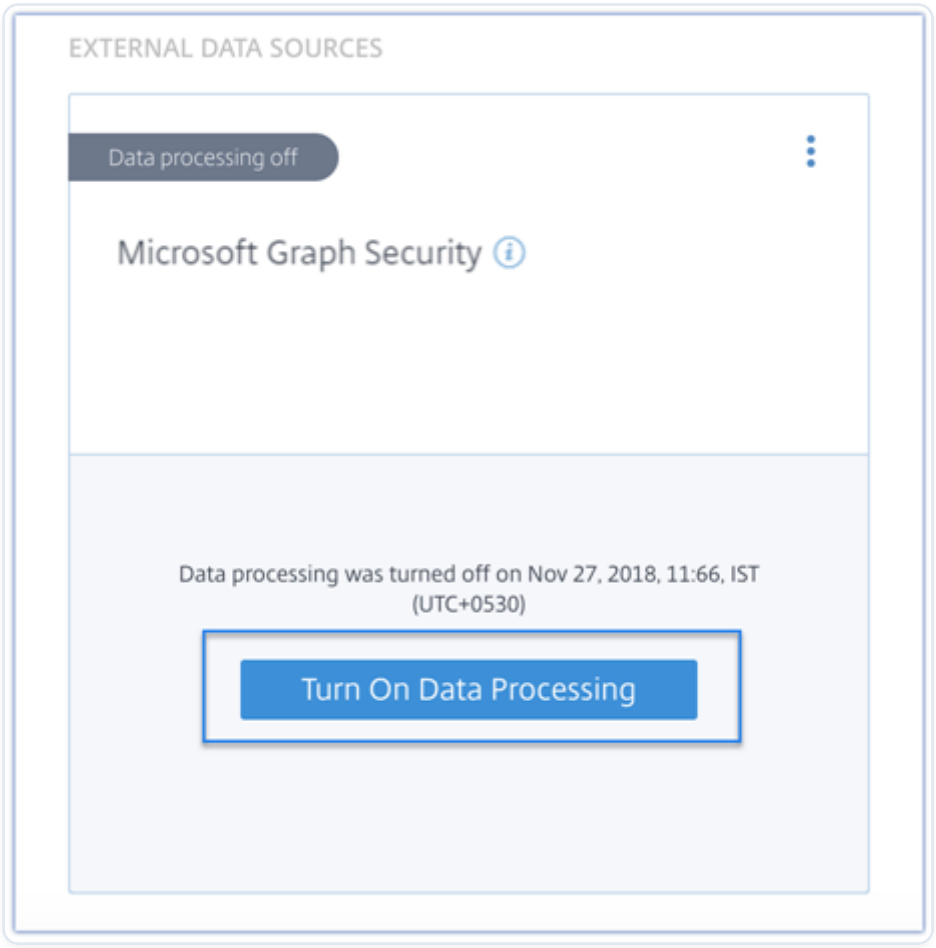


Turn on or off data processing

To disable data processing, click the vertical ellipsis (⋮) on the site card and select **Turn off data processing**. It stops Citrix Analytics from processing data for this data source.

You can turn on data processing again by selecting **Turn On Data Processing** on the site card.

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



For information on Microsoft Graph Security risk indicators, see Microsoft Graph Security risk indicators.

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

Security Information and Event Management (SIEM) integration

NOTE

Contact mailto:CAS-PM-Ext@cloud.com to request assistance for the SIEM integration, exporting data to SIEM, and provide feedback.

Integrate Citrix Analytics for Security™ with your SIEM services and export the users' data from the Citrix IT environment to your SIEM. Correlate the exported data with the data available in your SIEM to get deeper insights into your organization's security posture.

This integration enhances the value of both your Citrix Analytics for Security and your SIEM.

Benefits

- Enables your Security Operations teams to correlate, analyze, and search data from disparate logs.
- Helps your Security Operations teams to identify and quickly remediate the security risks.
- Visibility of security alerts in a centralized place.
- Centralized approach to detect potential security threats for organizational risk analysis capabilities such as risk indicators, user profiles, and risk scores.
- Ability to combine and correlate the Citrix Analytics risk intelligence information of a user account with the external data sources connected within your SIEM.

SIEM integration architecture

Your SIEM Integration connects with the north-bound Kafka deployed on Citrix Analytics for Security cloud. This can be achieved in the following two ways:

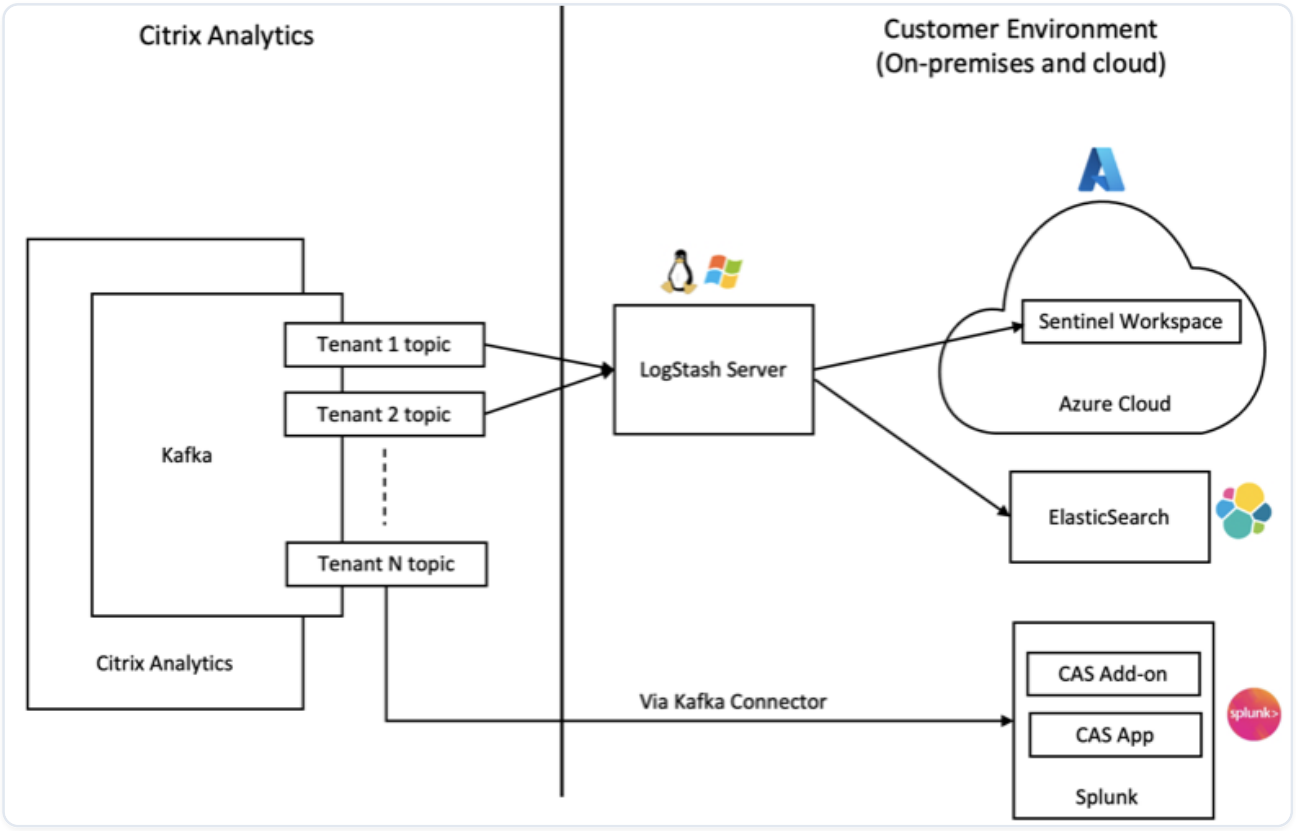
- **Kafka endpoints**: If your SIEM supports Kafka endpoints, use the parameters provided in the Logstash config file and the certificate details in the JKS file or the PEM file to integrate your

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

SIEM with Citrix Analytics for Security. Using the Kafka endpoints, you can connect and pull the data to the SIEM of choice.

- **Logstash engine**: If your SIEM does not support Kafka endpoints, then you can use the Logstash data collection engine. You can send the risk insights data from Citrix Analytics for Security to one of the output plug-ins that are supported by Logstash.

Refer to the following SIEM solution architecture diagram to understand how data flows from Citrix Analytics for Security to your SIEM service:



Turn on or off data transmission

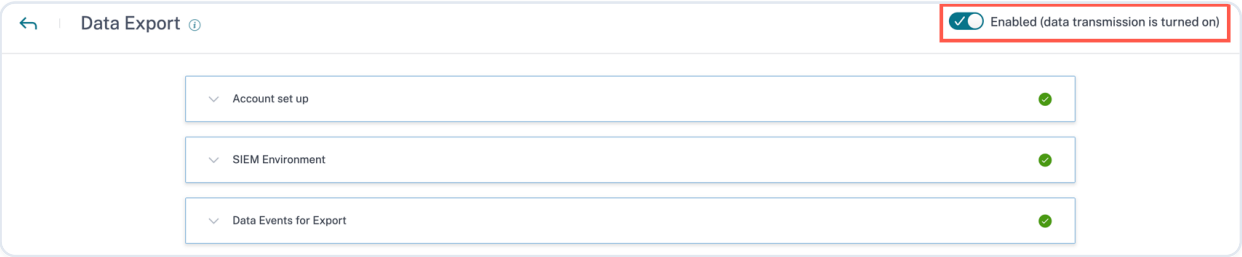
To stop transmitting data from Citrix Analytics for Security:

1. Go to **Settings > Data Exports**.
2. Turn off the toggle button to disable the **data transmission**.

NOTE

By default, the data transmission is always turned on/enabled for SIEM.

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



To enable data transmission again, turn on the toggle button.

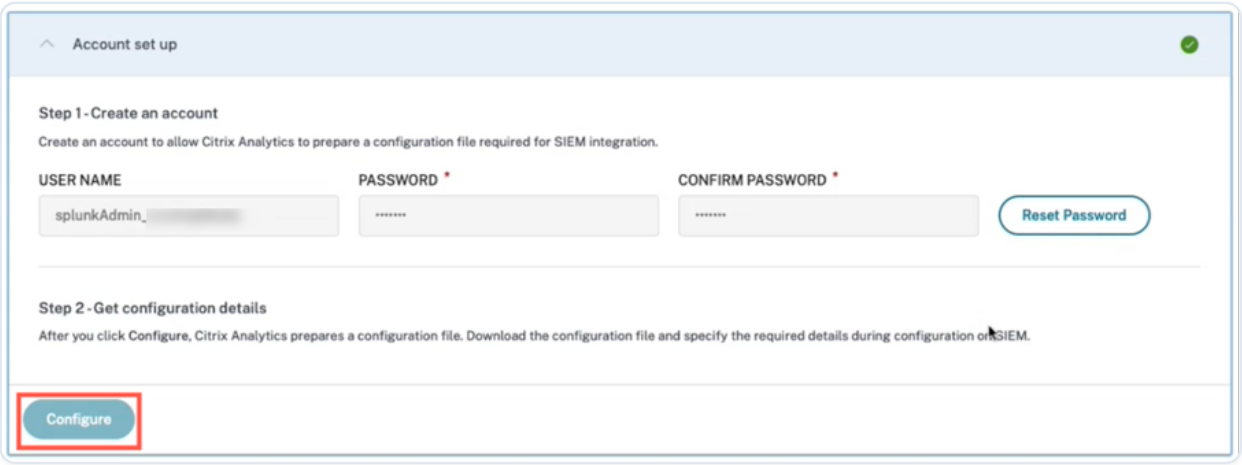
Setting up SIEM environment

To export data to SIEM, you must perform the following actions:

- Set up your Kafka account and authentication credentials
- Download the pre-populated configuration and set up the SIEM environment
- Data Events for Export

SIEM export account setup

1. For setting up your account, navigate to **Settings > Data Exports > expand Account set up**. Create an account by specifying the user name and password. Once you set up your account, your Kafka details are generated. These details are automatically embedded while generating the configuration file.



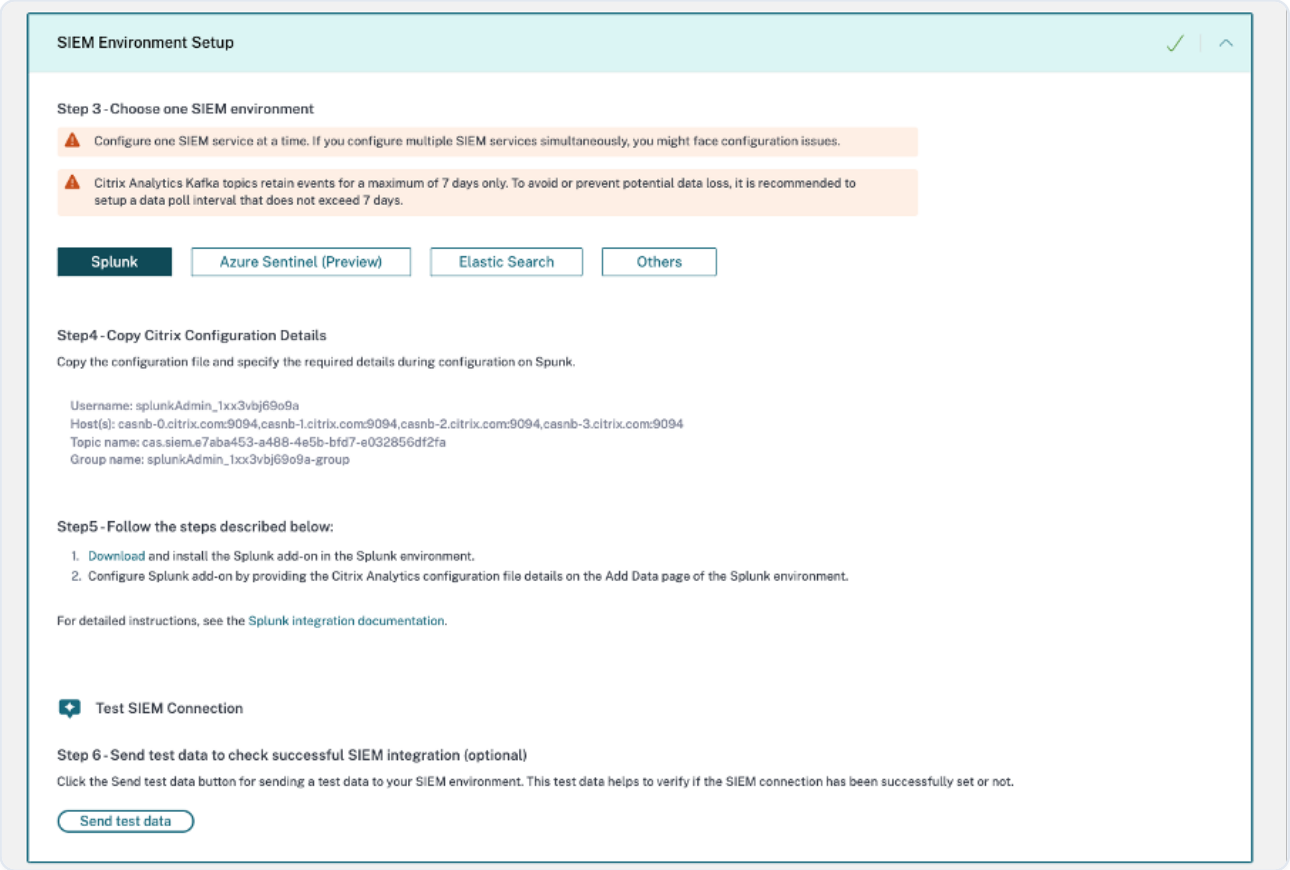
2. Click **Configure** to generate the configuration file. The configuration file contains details such as Kafka endpoints, your specific subscription topics, and group IDs. Also, it pre-configures the Kafka and SSL attributes which are required for completing authentication and data flow.

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

SIEM configuration and environment setup

Choose the SIEM environment as needed. You can integrate Citrix Analytics for Security with the following services. Refer the following links to get detailed information and SIEM specific configurations:

- Splunk
- Microsoft Sentinel
- Elasticsearch
- Other SIEMs using Kafka or Logstash based data connector



Data events exported from Citrix Analytics for Security to your SIEM service

As part of SIEM exports, there are two types of data sets:

1. **Risk insights events (Default exports)** – Once you have completed the account configuration and SIEM setup, default data (risk insights events) start flowing to your SIEM deployment. Risk insights data contains user risk score, user profile, and risk indicator alerts. These are generated by Citrix Analytics machine learning algorithm, user behavior analysis, and based on

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

user events. For information on the event types, metadata, and schema available, see Risk insights data for SIEM.

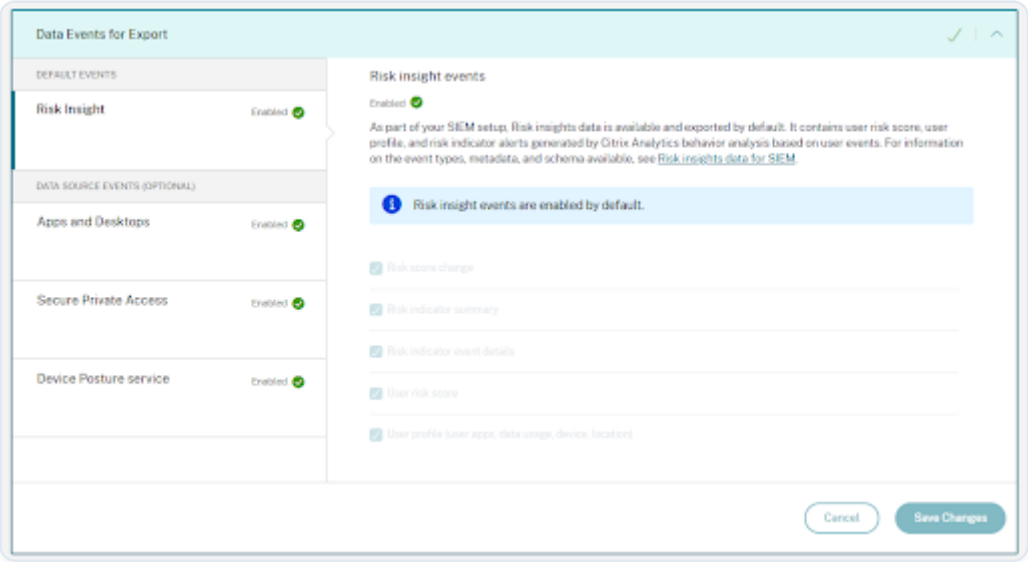
2. **Data Source events (Optional exports)** - Additionally, you can configure the Data exports feature to export user events from your Citrix Analytics for Security enabled products data sources. When you perform any activity in the Citrix environment, the data source events are generated. The exported events are unprocessed real time user and product usage data as available in self-service view. The meta data contained in these events can further be used for deeper threat analysis, creating new dashboards, and co related with other non-Citrix data source events across your security and IT infra.

   Currently, Citrix Analytics for Security sends user events to your SIEM for these data sources: Citrix Virtual Apps and Desktops™, Secure Private Access, and Device Posture service.

   For information on the event types, metadata, and schema available, see Data source events.

NOTE

Customers who are using a Logstash data broker, it is recommended that the latest configuration file is downloaded from Citrix Analytics for Security portal, and updated on the Logstash service deployment. This ensures that the correct data source event tables are created and the events are now available in SIEM indexes.

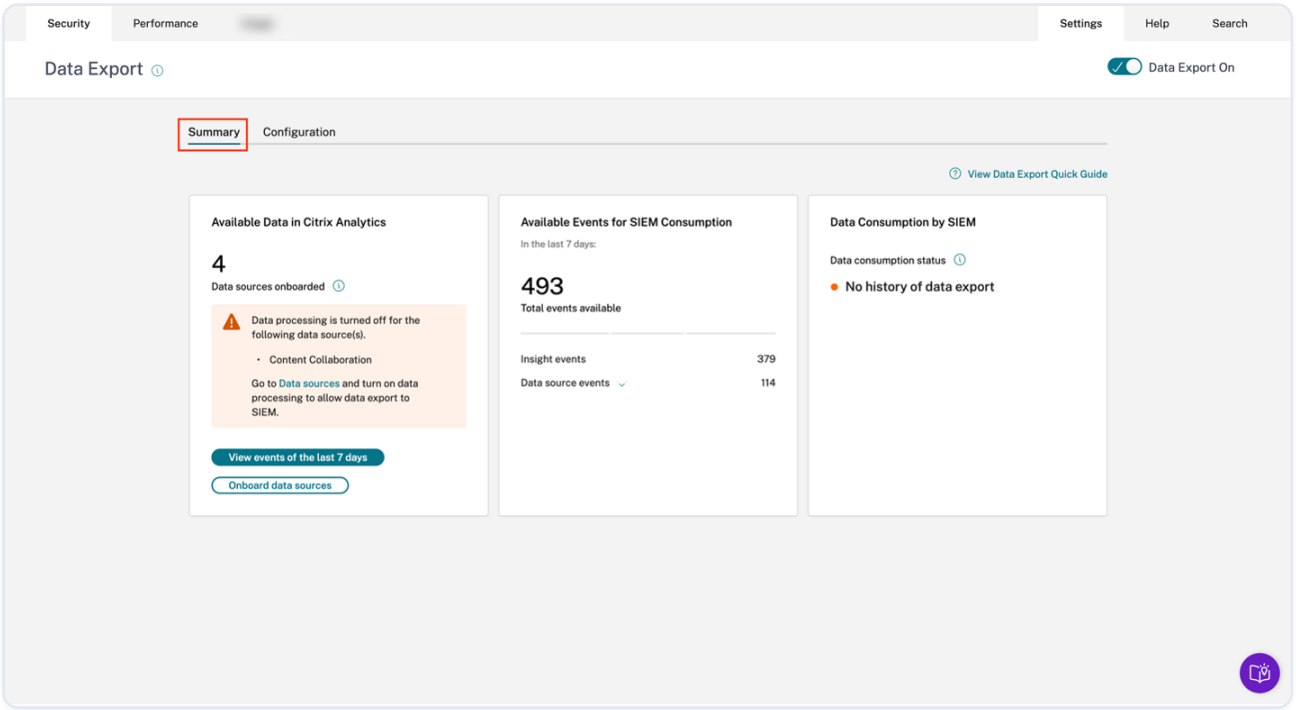


Troubleshooting SIEM Integration

The Data Exports for Security view includes a **Summary** tab to help administrators troubleshoot their SIEM integration with Citrix Analytics. The **Summary** dashboard provides visibility into the

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

health and flow of data by taking them through the checkpoints that aid the troubleshooting process.



To learn more about this capability, refer Troubleshooting Data Exports.

Splunk integration

Integrate Citrix Analytics for Security with Splunk to export and correlate the users' data from your Citrix IT environment to Splunk and get deeper insights into your organization's security posture.

For more information about the benefits of the integration and the type of processed data that is sent to your SIEM, see Security Information and Event Management integration.

To develop a comprehensive understanding of the Splunk Deployment Methodology and adopt the strategies for effective planning, refer Splunk architecture with Citrix® Analytics applications hosted on Splunk documentation.

Integrate Citrix Analytics for Security™ with Splunk

Follow the guidelines mentioned to integrate Citrix Analytics for Security with Splunk:

- Data export. Citrix Analytics for Security creates a Kafka channel and exports Risk Insights and Data source events. Splunk retrieves this risk intelligence from the channel.
- Get configuration on Citrix Analytics. Create a password for your pre-defined account for authentication. Citrix Analytics for Security prepares a configuration file required for you to configure the Citrix Analytics add-on for Splunk.

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

- Download and install Citrix Analytics add-on for Splunk. Download the **Citrix Analytics Add-on for Splunk** either using Splunkbase or Splunk Cloud to complete the installation process.
- Configure Citrix Analytics add-on for Splunk. Set up a data input by using the configuration details provided by Citrix Analytics for Security and configure the Citrix Analytics add-on for Splunk.

After the Citrix Analytics configuration file is prepared, see:

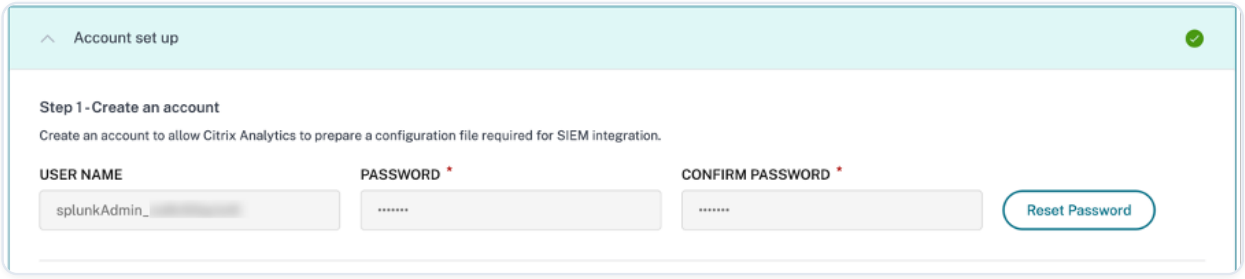
- Reset Password Capability
- Turn on or off data transmission

After the Citrix Analytics add-on for Splunk is configured, see:

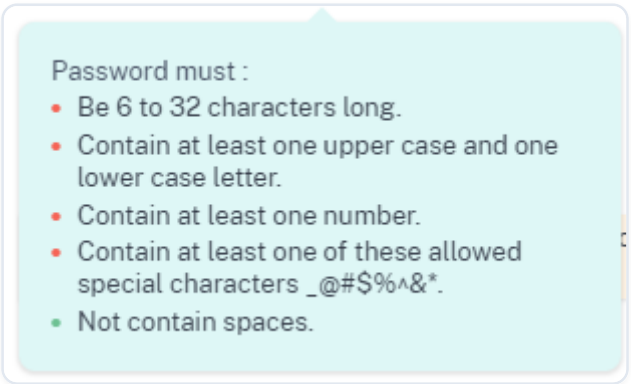
- How to consume events at Splunk Environment
- How to configure Citrix Analytics App for Splunk

Data export

1. Go to **Settings** > **Data Exports**.
2. On the **Account set up** section, create an account by specifying the user name and a password. This account is used to prepare a configuration file, which is required for the integration.



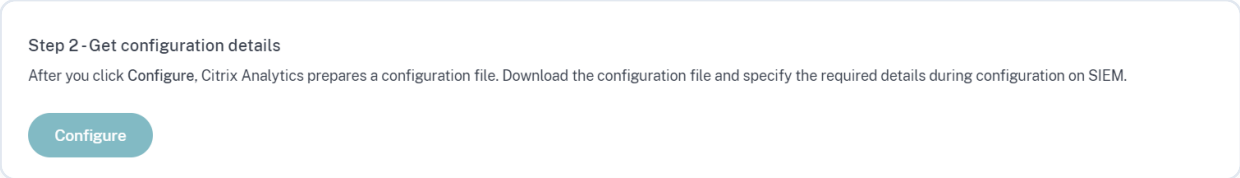
3. Ensure that the password meets the following conditions:



4. Select **Configure**.

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

Citrix Analytics for Security prepares the configuration details required for Splunk integration.

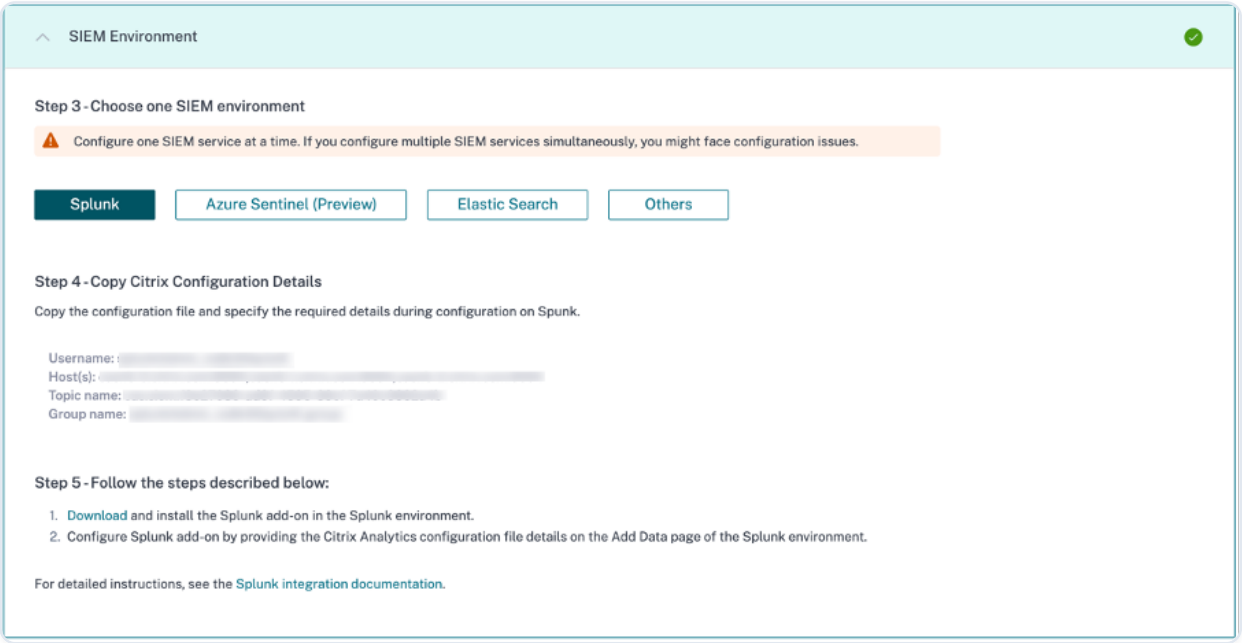


5. Select **Splunk**.
6. Copy the configuration details, which include the user name, hosts, Kafka topic name, and group name.

   You require these details to configure Citrix Analytics Add-on for Splunk in the subsequent steps.

   IMPORTANT

   These details are sensitive and you must store them in a secure location.



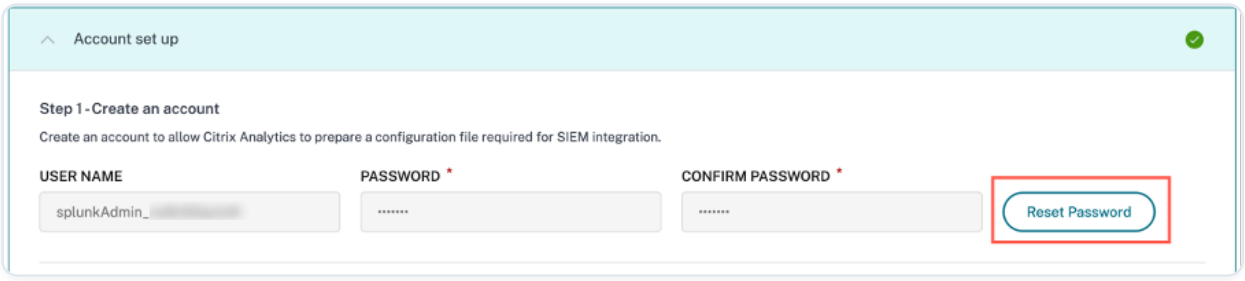
To generate candidate data for Splunk Integration, either turn on data processing for at least one data source or use test event generation capability. It helps Citrix Analytics for Security to begin the Splunk integration process.

Reset Password Capability

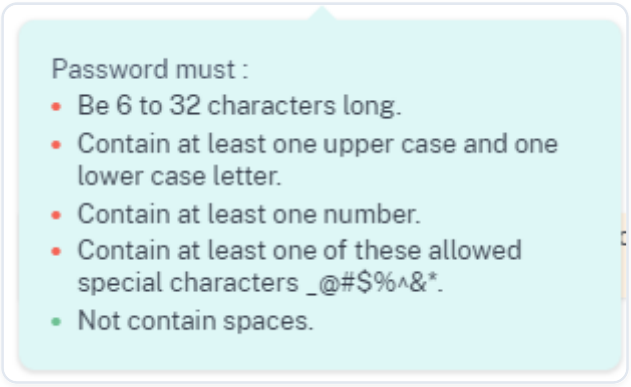
If you want to reset your configuration password on Citrix Analytics for Security, do the following steps:

1. On the **Account set up** page, click **Reset Password**.

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

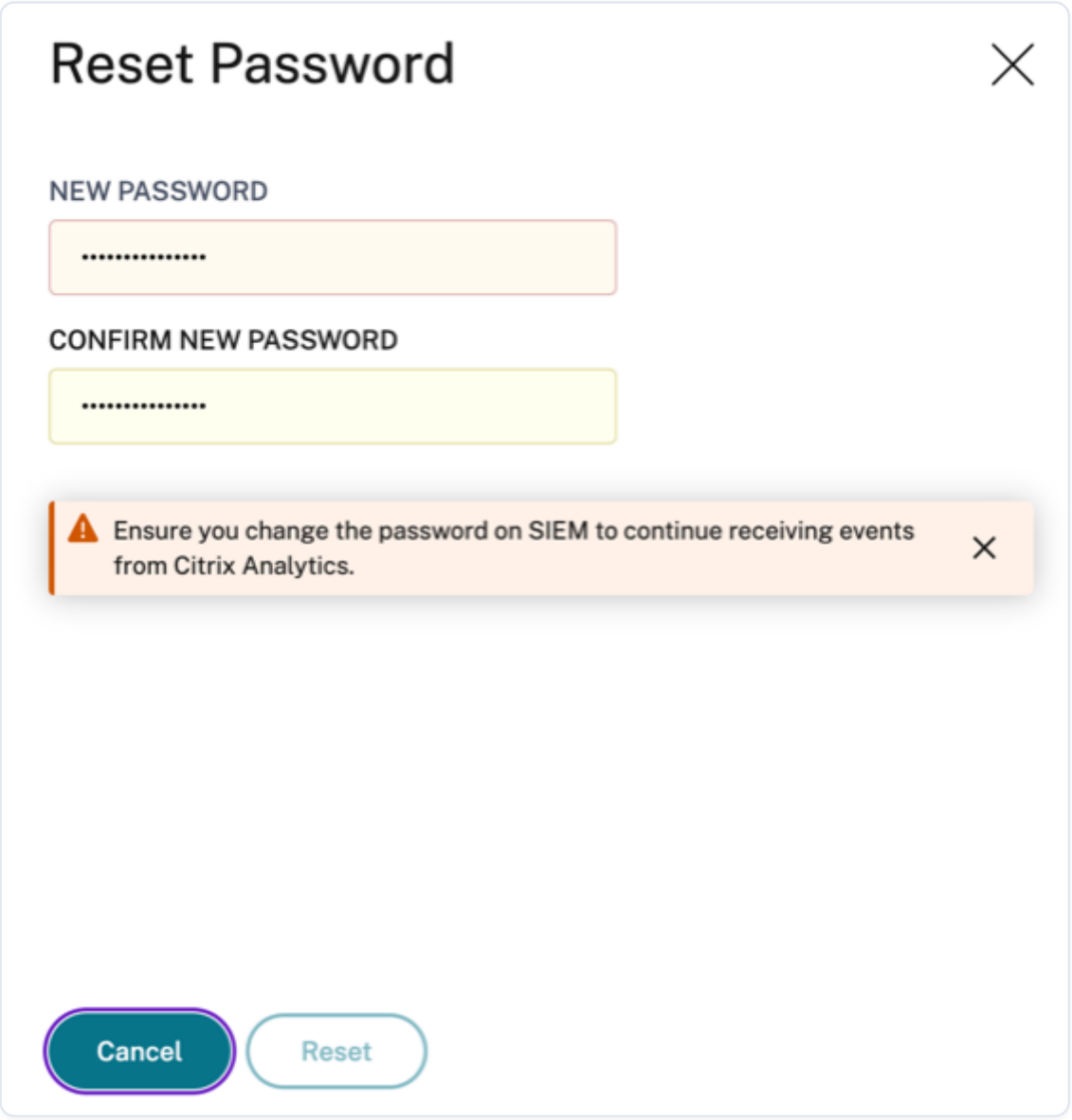


2. On the **Reset Password** window, specify the updated password on the **NEW PASSWORD** and **CONFIRM NEW PASSWORD** fields. Follow the password rules that are displayed.



3. Click **Reset**. The configuration file preparation is initiated.

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



NOTE

After you reset the configuration password, ensure you update the new password when you set up the data input on the **Add Data** page of your Splunk environment. It helps Citrix Analytics for Security to continue transmitting data to Splunk.

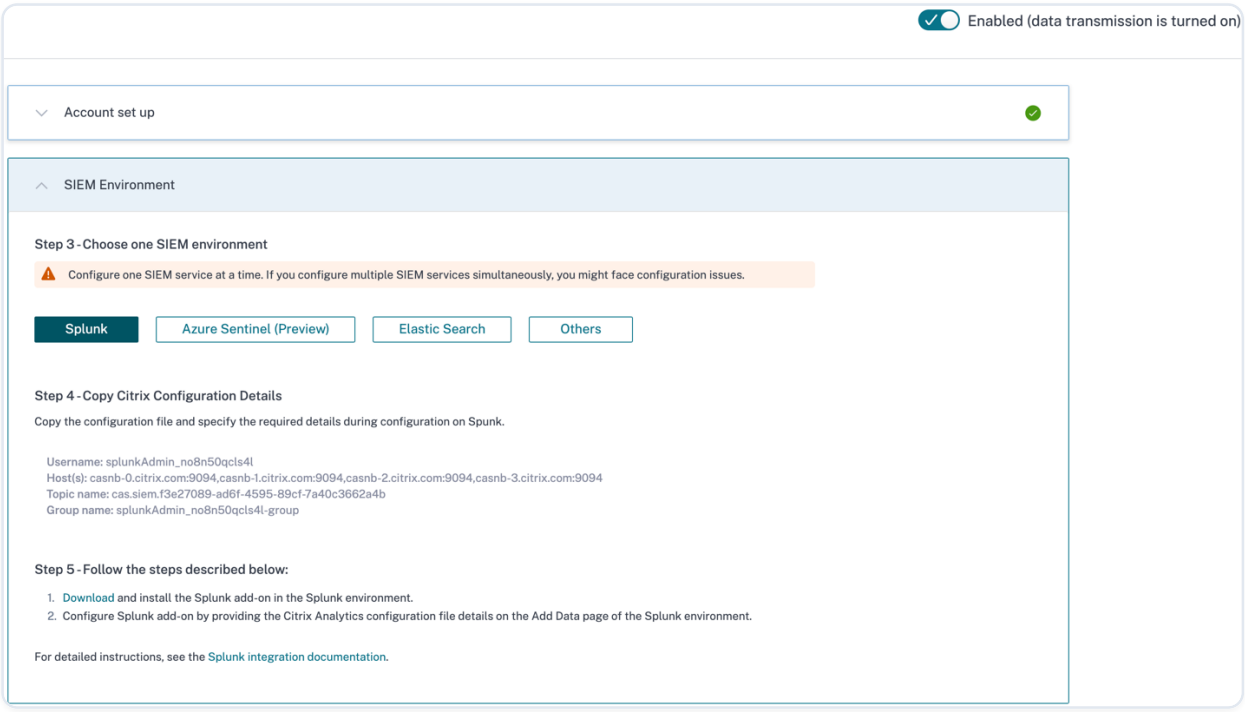
Turn on or off data transmission

Data Transmission for Splunk data export from Citrix Analytics is turned on by default.

To stop transmitting data from Citrix Analytics for Security:

1. Go to **Settings > Data Exports**.
2. Turn off the toggle button to disable the **data transmission**.

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



To enable data transmission again, turn on the toggle button.

Citrix Analytics Add-On for Splunk

You can choose to install the add-on application on either of the following platforms:

- Splunk Enterprise (Heavy Forwarder)
- Splunk Cloud

Citrix Analytics Add-On for Splunk (On-prem/Enterprise)

Supported versions

Citrix Analytics for Security supports Splunk integration on the following operating systems:

- CentOS Linux 7 and later
- Debian GNU/Linux 10.0 and later
- Red Hat Enterprise Linux Server 7.0 and later
- Ubuntu 18.04 LTS and later

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

NOTE

- Citrix recommends using the latest version of the preceding operating systems or the versions that are still under support from the respective vendors.
- For the Linux kernel (64-bit) operating systems, use a kernel version that is supported by Splunk. For more information, see Splunk documentation.

You can configure our Splunk integration on the following Splunk version: Splunk 8.1 (64-bit) and later.

Prerequisites

- The **Citrix Analytics add-on for Splunk** connects to the following endpoints on Citrix Analytics for Security. Ensure that the endpoints are in the allow list in your network.

ENDPOINT	UNITED STATES REGION	EUROPEAN UNION REGION	ASIA PACIFIC SOUTH REGION
Kafka brokers	`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`		

NOTE

Try using the endpoint names not the IP addresses. The public IP addresses of the endpoints might change.

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

Download and install Citrix Analytics add-on for Splunk

You can choose to install the add-on using **Install app from file** or from within the Splunk environment.

Install app from file

1. Go to Splunkbase.
2. Download the Citrix Analytics Add-on for Splunk file.
3. On the Splunk Web home page, click the gear icon next to **Apps**.
4. Click **Install app from file**.
5. Locate the downloaded file and click **Upload**.

NOTES

- If you have an older version of the add-on, select **Upgrade app** to overwrite it.
- If you are upgrading **Citrix Analytics Add-on for Splunk** from a version earlier than 2.0.0, you must delete the following files and folders located inside the */bin* folder of the add-on installation folder and restart your Splunk Forwarder or Splunk Standalone environment:
  - `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. Verify that the app appears in the **Apps** list.

Install app from within Splunk

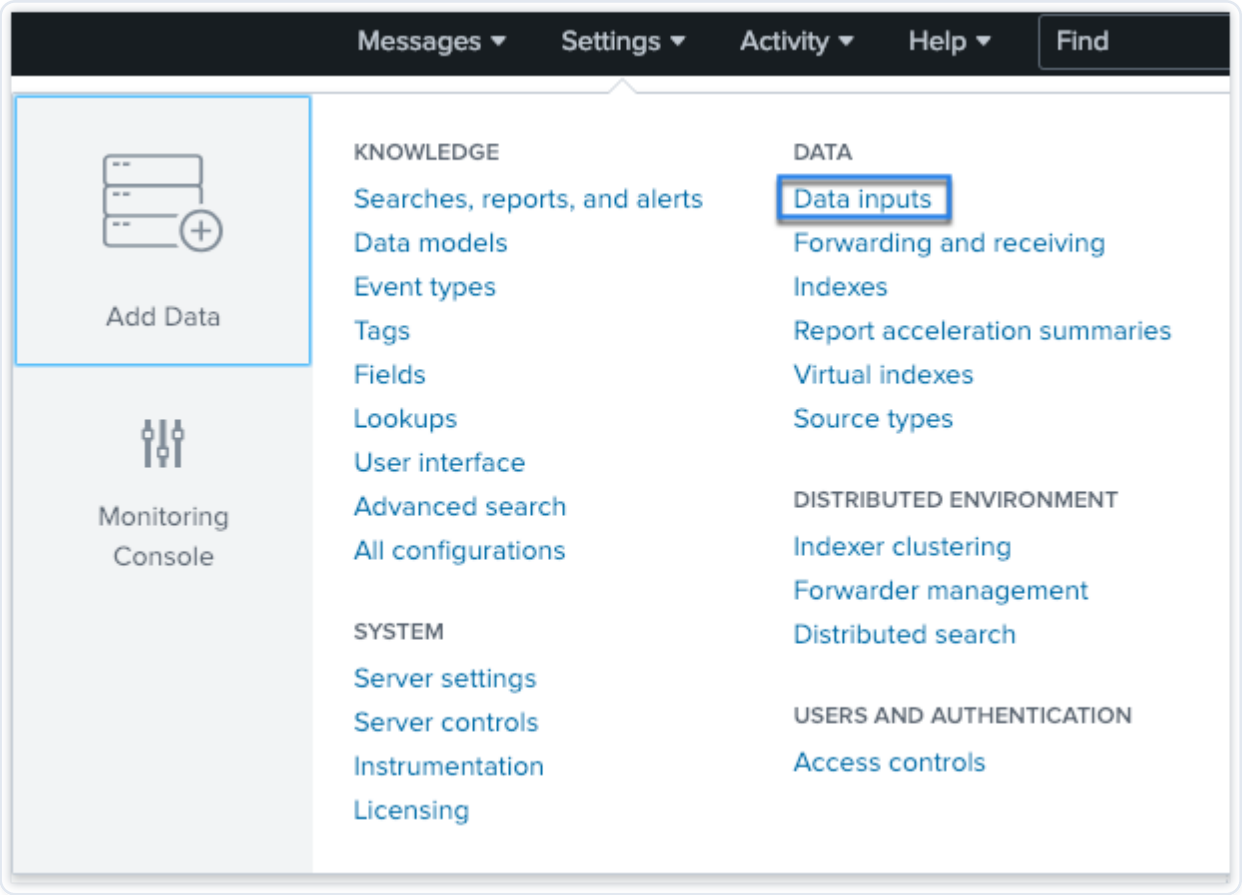
1. From the Splunk Web home page, click **+Find More Apps**.
2. On the Browse More Apps page, search **Citrix Analytics Add-on for Splunk**.
3. Click **Install** next to the app.
4. Verify that the app appears in the **Apps** list.

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

Configure Citrix Analytics add-on for Splunk

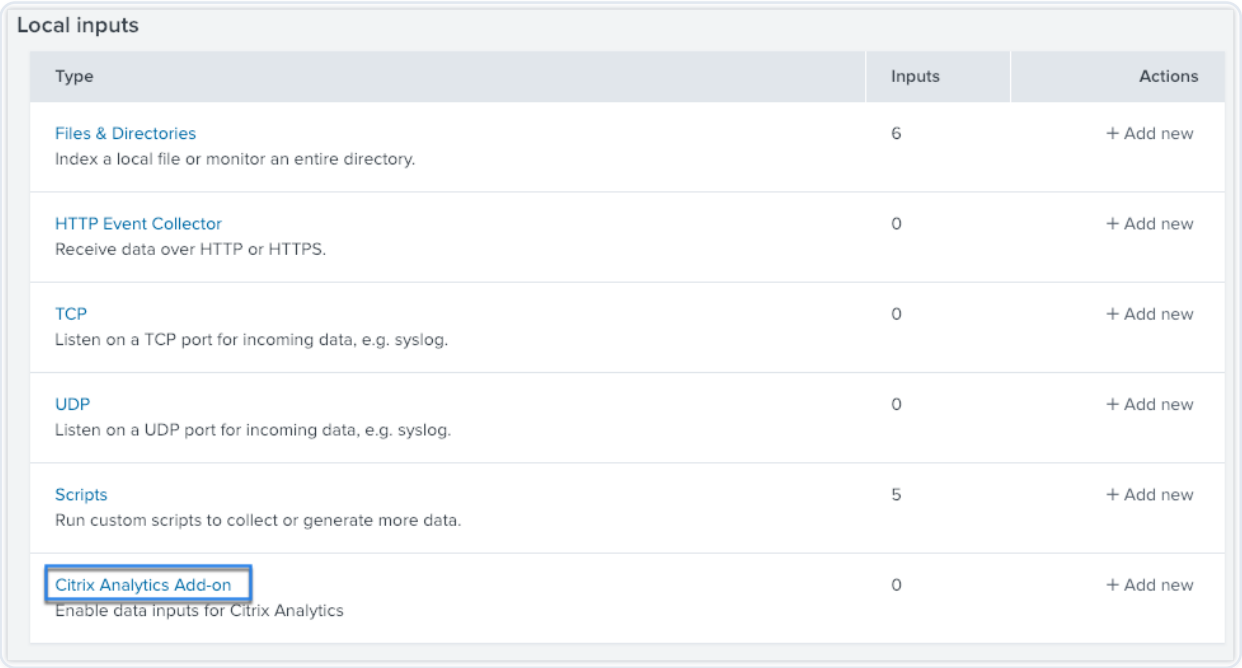
Configure the Citrix Analytics add-on for Splunk using the configuration details provided by Citrix Analytics for Security. After the add-on is successfully configured, Splunk starts consuming events from Citrix Analytics for Security.

1. On the Splunk home page, go to **Settings** > **Data inputs**.

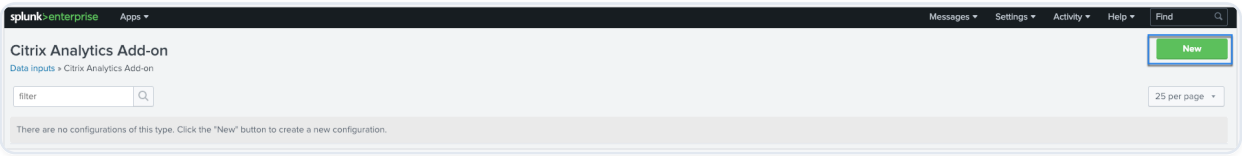


2. In the **Local inputs** section, click **Citrix Analytics Add-on**.

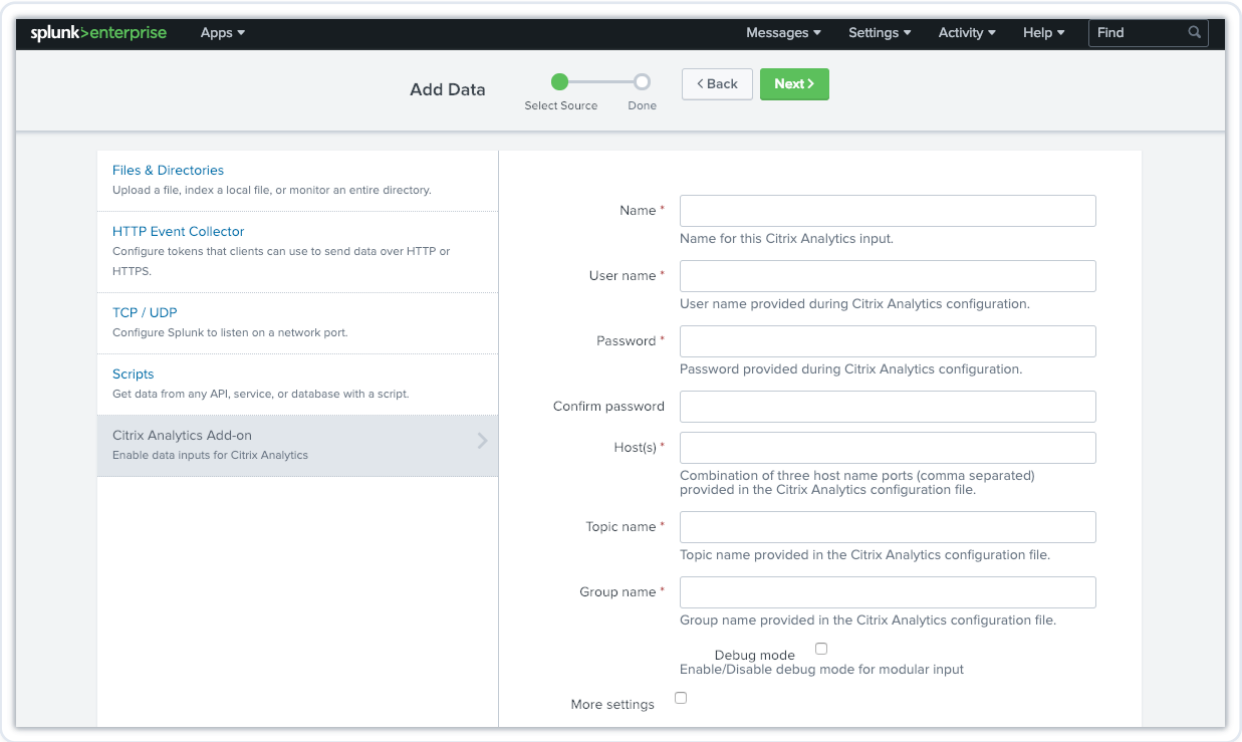
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Click **New**.

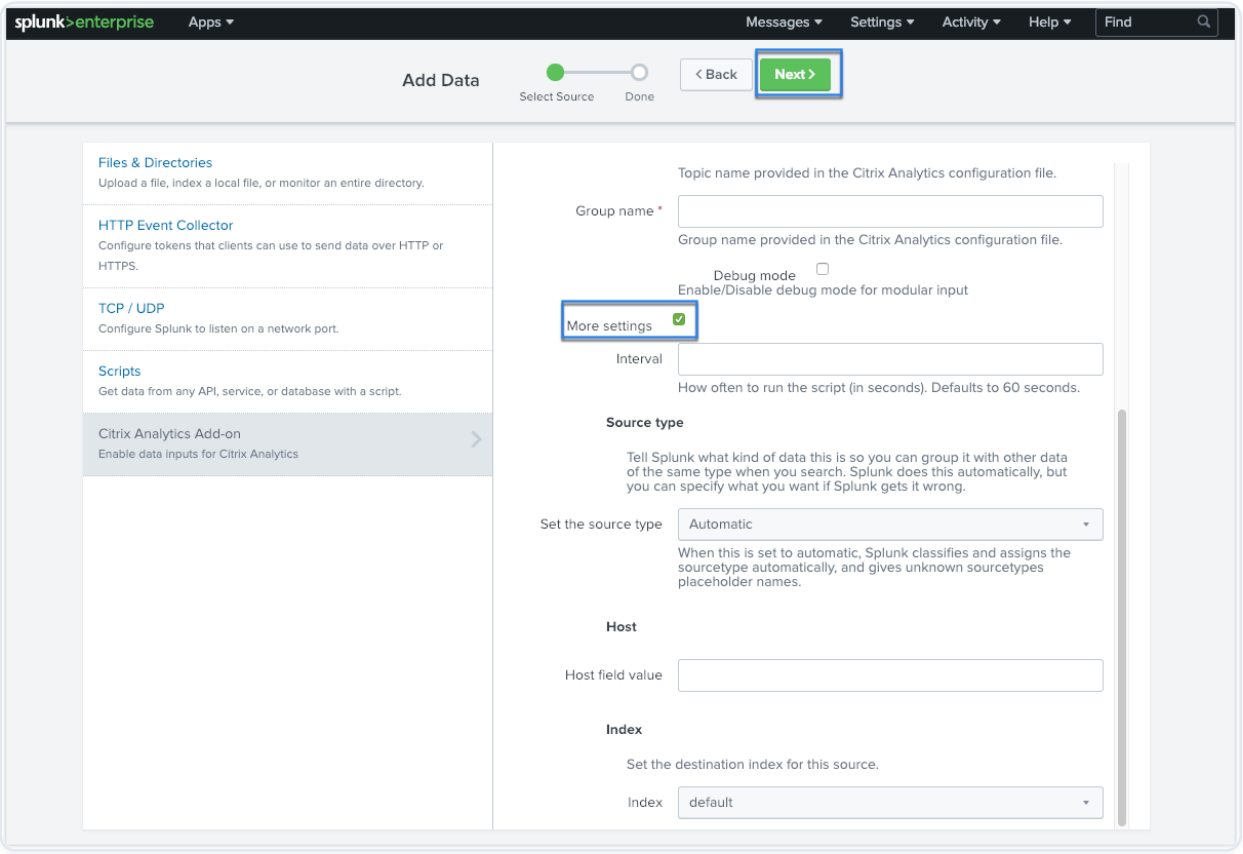


4. On the **Add Data** page, enter the details provided in the Citrix Analytics configuration file.



5. To customize your default settings, click **More settings** and set up the data input. You can define your own Splunk index, host name, and source type.

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



6. Click **Next**. Your Citrix Analytics data input is created and the Citrix Analytics add-on for Splunk is configured successfully.

Citrix Analytics Add-On for Splunk (Cloud)

You can configure our Splunk integration on the following Splunk version: Splunk 8.1 and later.

Prerequisites

The Citrix Analytics add-on for Splunk connects to the following IPs and outbound ports to connect to Citrix Analytics for Security. Ensure that the following IPs and outbound ports (depending upon your Citrix Cloud™ region) are in the allow list in your network. To configure these IPs and outbound ports, refer **Add Citrix Analytics IPs and Outbound Ports to Splunk Cloud Allow List using Admin Configuration Service (ACS)** section.

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

UNITED STATES REGION	IP	OUTBOUND PORT	EUROPEAN UNION REGION	IP	OUTBOUND PORT	ASIA PACIFIC SOUTH REGION	IP	OUTBOUND PORT
casnb-0 citrix.com	20.242.21.84	9094	casnb-eu-0 citrix.com	20.229.150.41	9094	casnb-aps-0 citrix.com	20.211.0.214	9094
casnb-1.citrix.com	20.98.232.61	9094	casnb-eu-1.citrix.com	20.107.97.59	9094	casnb-aps-1 citrix.com	20.211.38.102	9094
casnb-2.citrix.com	20.242.21.108	9094	casnb-eu-2.citrix.com	51.124.223.162	9094	casnb-aps-2 citrix.com	20.211.36.180	9094
casnb-3.citrix.com	20.242.57.140	9094						

NOTE

These IPs are subject to rotation. Make sure you keep your IP allow list updated with the most recent IPs as shown above.

Add Citrix Analytics IPs and Outbound Ports to Splunk Cloud Allow List using Admin Configuration Service (ACS)

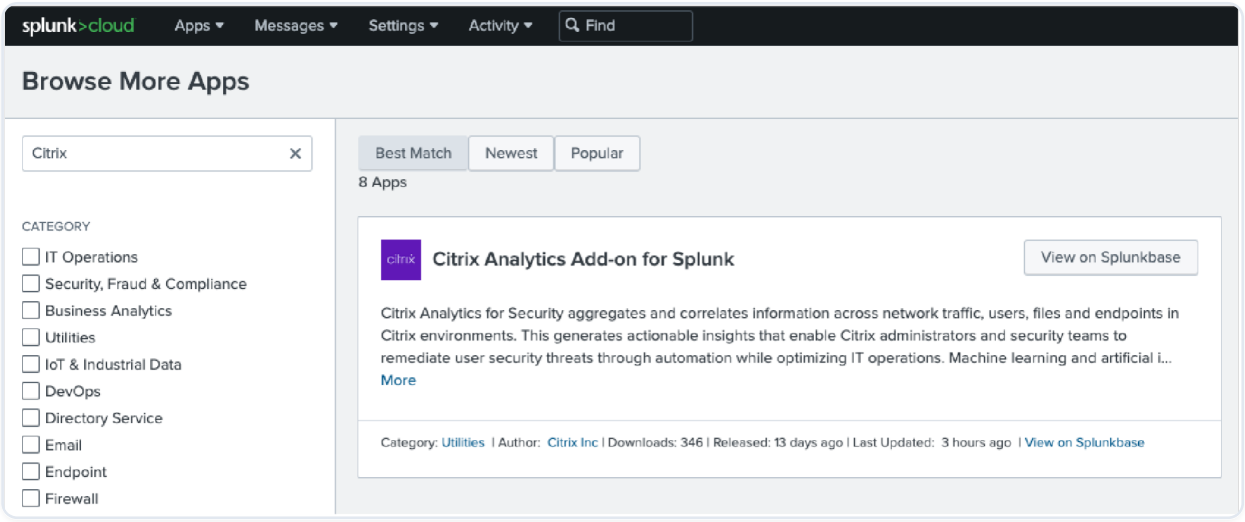
1. Depending upon your Citrix Cloud region, zero in on the IPs must be added in the allow list.
2. Enable Admin Configuration Service (ACS) on Splunk Cloud Platform.
3. Create token for the allow list using local account with admin privileges.
4. Run cURL GET and POST commands to add subnets to the allow list on respective ports and validate if they are successfully added.

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

5. Run cURL GET and POST commands to add outbound ports to the allow list and validate if they are successfully added.

Download and install Citrix Analytics add-on for Splunk

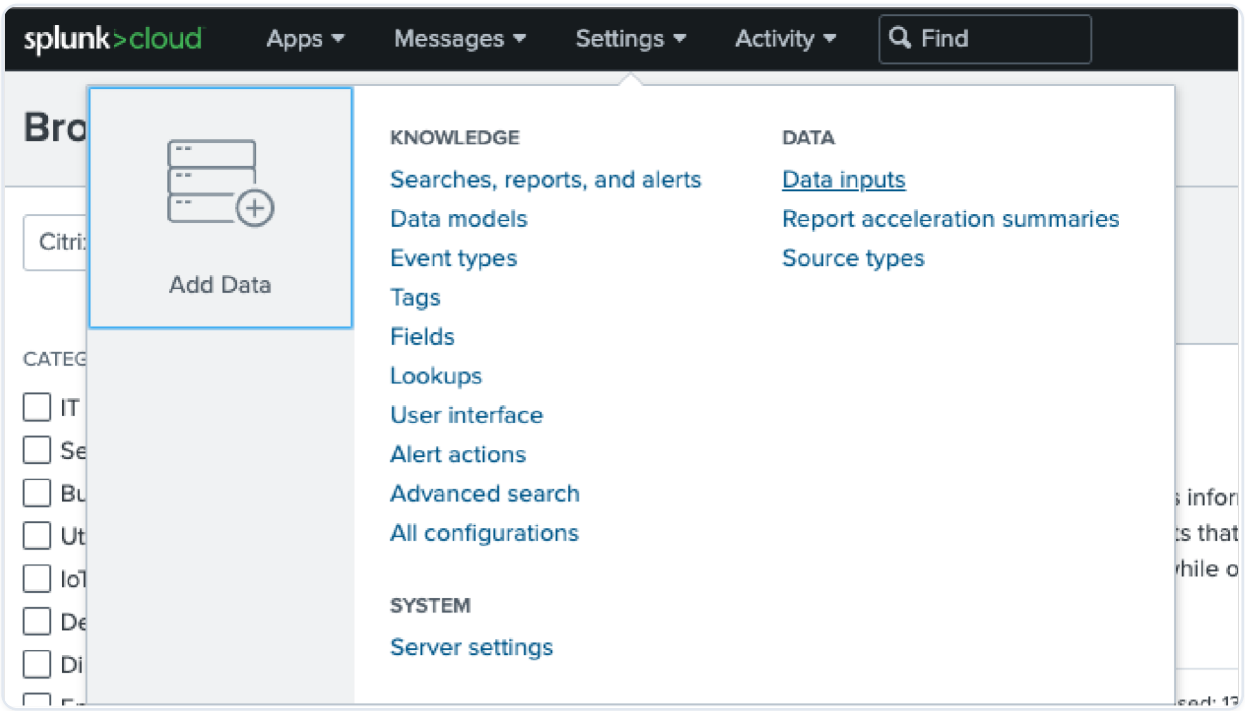
1. Go to **Apps > Find more Apps > Search for Citrix Analytics Add-on for Splunk**.



2. Install the app.
3. Verify that the app appears in the Apps list.

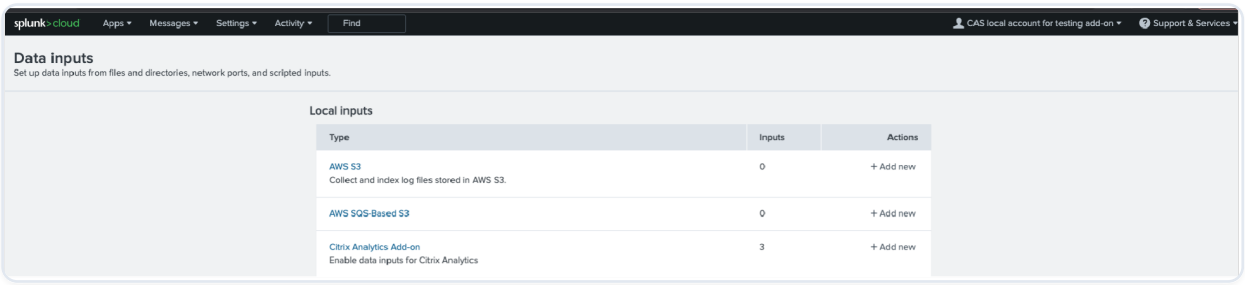
Configure Citrix Analytics add-on for Splunk

1. Go to **Settings > Data Inputs > Citrix Analytics Add-on**.

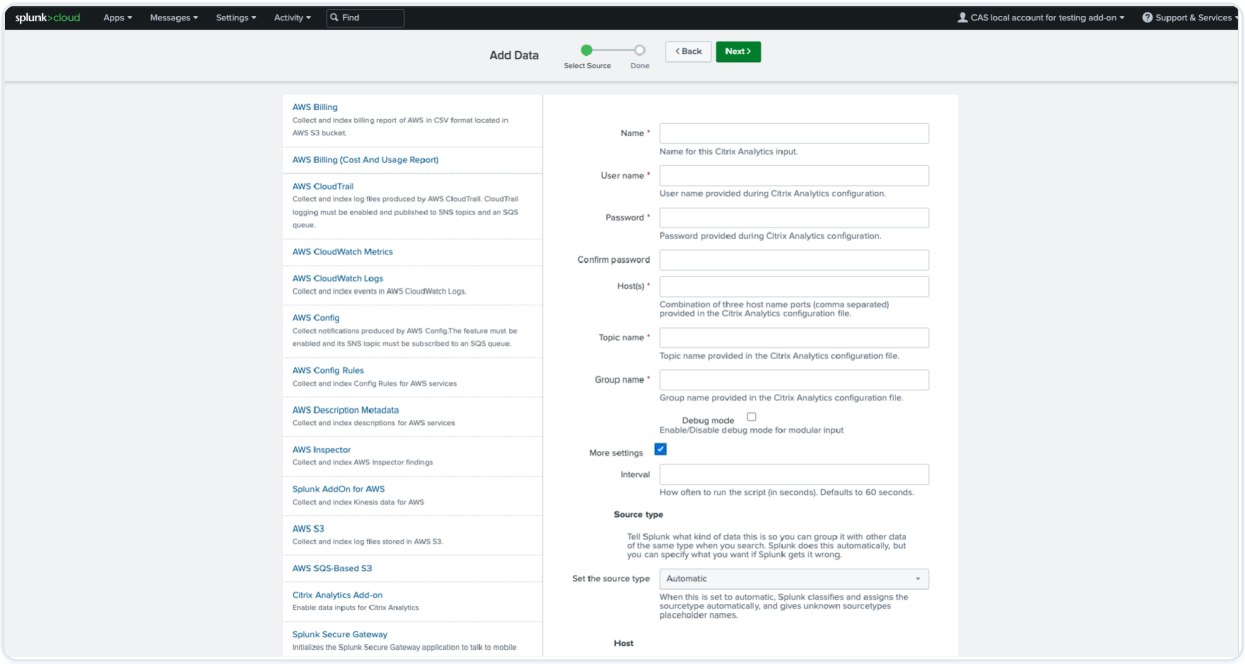


2. Add the input: Splunk integration | Citrix Analytics for Security. Click **Add New**.

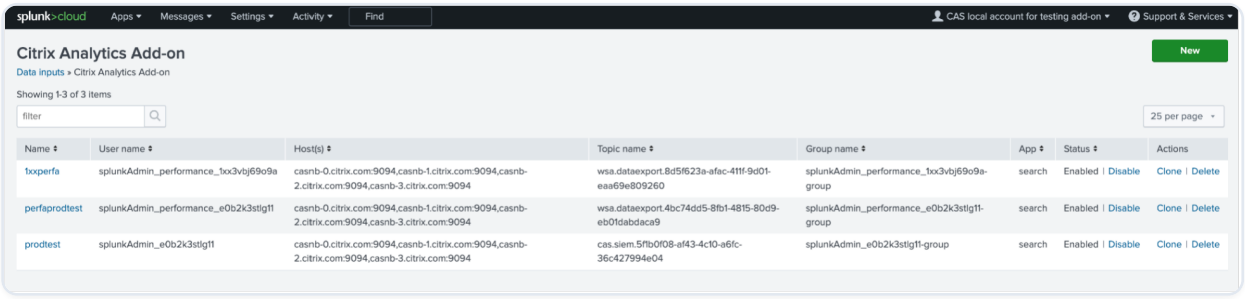
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Configure Data Input by entering the details configured on **Citrix Analytics Data Exports** page.



4. Verify if your data input has successfully been added.

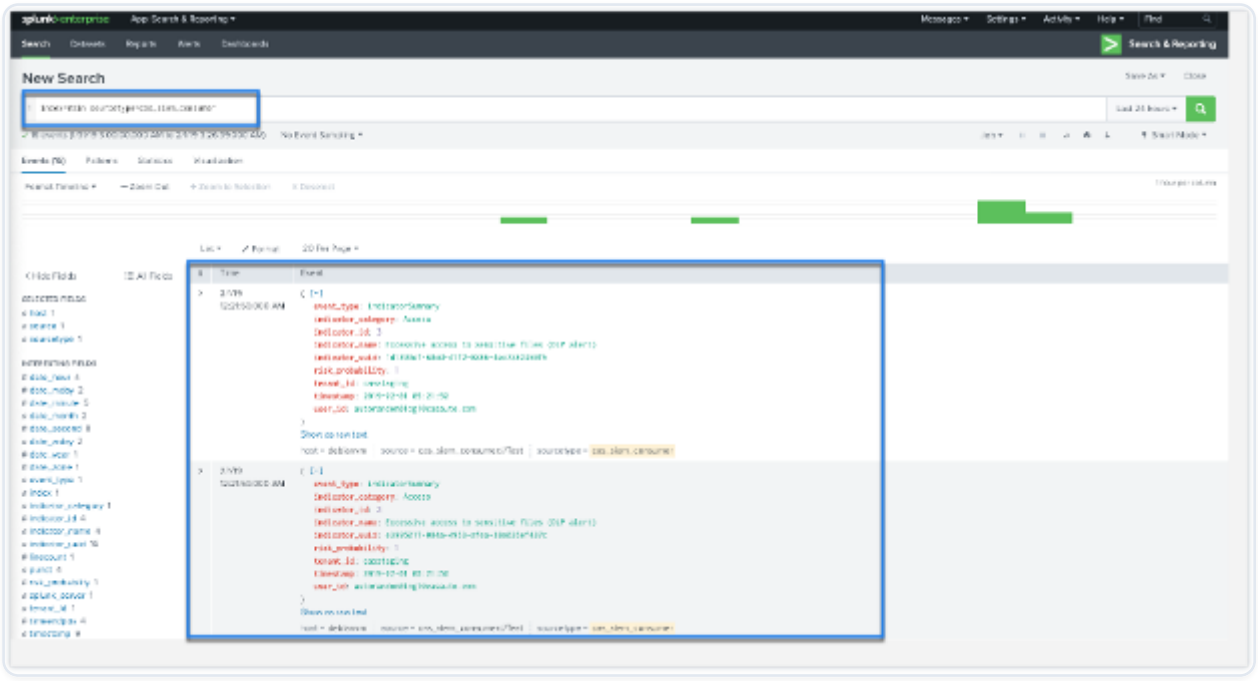


How to consume events in your Splunk Environment

After you configure the add-on, Splunk starts retrieving risk intelligence from Citrix Analytics for Security. You can start searching your organization's events on the Splunk search head based on the configured data input.

The search results are displayed in the following format:

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



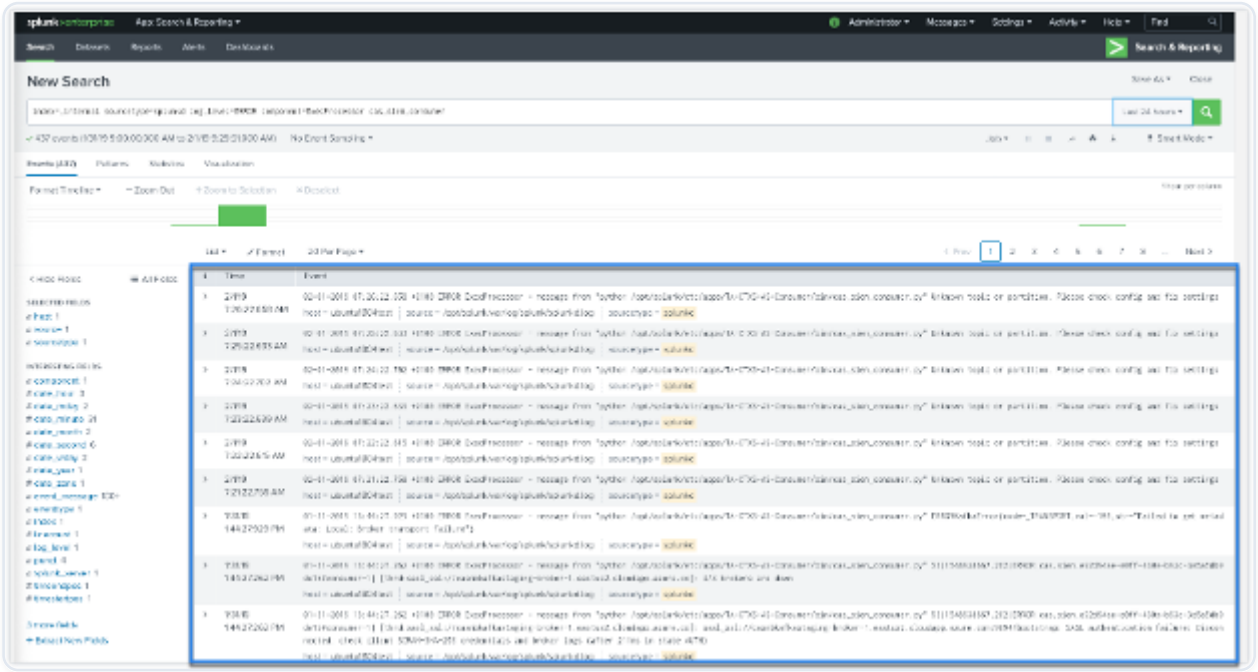
A sample output:


```
{"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"}
```


To search and debug issues with the add-on, use the following search query:

```
index=_internal sourcetype=splunkd log_level=ERROR component=ExecProcessor
cas_siem_consumer
```

The results are displayed in the following format:



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

For more information about the data format, see Citrix Analytics data format for SIEM.

Troubleshoot Citrix Analytics add-on for Splunk

If you don't see any data in your Splunk dashboards or encountered issues while configuring Citrix Analytics add-on for Splunk, perform the debugging steps to fix the issue. For more information, see Configuration issues with Citrix Analytics add-on for Splunk.

NOTE

Contact mailto:CAS-PM-Ext@cloud.com to request assistance for the Splunk integration, exporting data to Splunk, or provide feedback.

Citrix Analytics App for Splunk

NOTE

This app is in preview.

Citrix Analytics App for Splunk enables Splunk Enterprise administrators to view the user data collected from Citrix Analytics for Security in the form of insightful and actionable dashboards on Splunk. Using these dashboards, you get a detailed view of the users' risky behavior in your organization and taking timely actions to mitigate any insider threats. You can also correlate the data collected from Citrix Analytics for Security with other data sources configured on your Splunk. This correlation provides you with visibility into the users' risky activities from multiple sources and takes actions to protect your IT environment.

Supported Splunk version

The Citrix Analytics App for Splunk runs on the following Splunk versions:

- Splunk 9.0 64-bit
- Splunk 8.2 64-bit
- Splunk 8.1 64-bit

Prerequisites for Citrix Analytics App for Splunk

- Install the Citrix Analytics add-on for Splunk.
- Ensure the prerequisites mentioned for the Citrix Analytics add-on for Splunk are already met.

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

- Ensure that the data is flowing from Citrix Analytics for Security to Splunk.

Installation and configuration

Where to install the app?

Splunk search head

How to install and configure the app?

You can install the Citrix Analytics App for Splunk by downloading it from Splunkbase or by installing it from within Splunk.

INSTALL APP FROM FILE

1. Go to Splunkbase.
2. Download the Citrix Analytics App for Splunk file.
3. On the Splunk Web home page, click the gear icon next to **Apps**.
4. Click **Install app from file**.
5. Locate the downloaded file and click **Upload**.

> **NOTE**
>
> If you have an older version of the app, select **Upgrade app** to overwrite it.

6. Verify that the app appears in the **Apps** list.

INSTALL APP FROM WITHIN SPLUNK

1. From the Splunk Web home page, click **+Find More Apps**.
2. On the Browse More Apps page, search **Citrix Analytics App for Splunk**.
3. Click **Install** next to the app.

CONFIGURE YOUR INDEX AND SOURCE TYPE TO CORRELATE DATA

1. After you install the app, click **Set up now**.



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

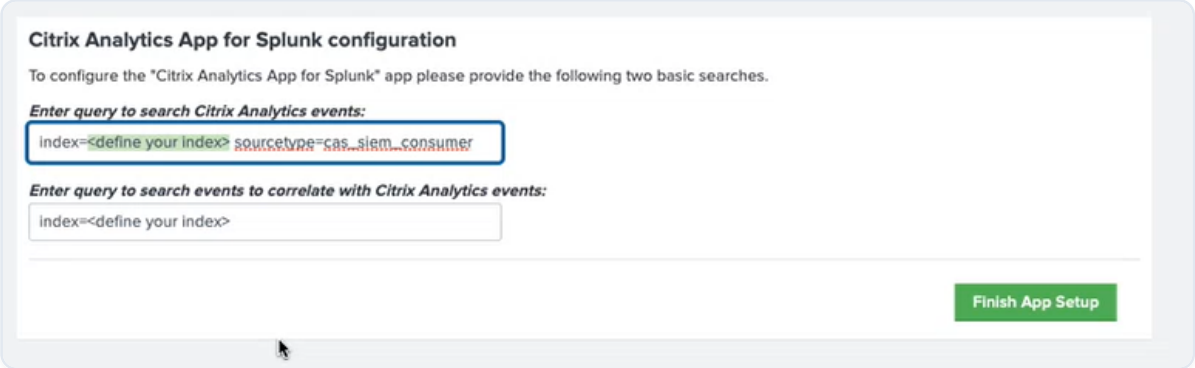
2. Enter the following queries:

   - Index and source type where the data from Citrix Analytics for Security are stored.

     NOTE

     These query values must be the same as specified in the Citrix Analytics add-on for Splunk. For more information, see Configure Citrix Analytics add-on for Splunk.

   - Index from which you want to correlate your data with Citrix Analytics for Security.



3. Click **Finish App Setup** to complete the configuration.

After you have configured and set up the Citrix Analytics App for Splunk, use the Citrix Analytics dashboards to view the user events on your Splunk.

For more information about Splunk integration, refer the following links:

- Citrix Analytics Integration with Splunk
- The Citrix Analytics app for Splunk, now in Splunkbase

Splunk architecture with Citrix Analytics add-on application

Splunk follows an architecture which contains the following three tiers:

- Collection
- Indexing
- Searching

Splunk supports a wide range of data collection mechanisms that helps ingest data into Splunk easily, such that it can be indexed and made available to search. This tier is nothing but your heavy forwarder or universal forwarder.

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

You must install the add-on application on the heavy forwarder layer instead of the universal forwarder layer. Because, with few exceptions for well-structured data (such as, json, csv, tsv), the universal forwarder does not parse log sources into events, so it cannot perform any action that requires understanding of the format of the logs.

It also ships with a stripped down version of Python, which makes it incompatible with any modular input applications that require a full Splunk stack to function. The heavy forwarder is nothing but your collection tier.

The key difference between a universal forwarder and a heavy forwarder is that the heavy forwarder contains the full parsing pipeline, performing the identical functions an indexer performs without actually writing and indexing events on disk. This enables the heavy forwarder to understand and act on individual events such as masking data, filtering, and routing based on event data. Since the add-on application has a full Splunk Enterprise installation, it can host modular inputs that require a full Python stack for proper data collection, or act as an endpoint for the Splunk HTTP Event Collector (HEC).

Once the data is collected, it is indexed or processed and stored in a way that makes it searchable.

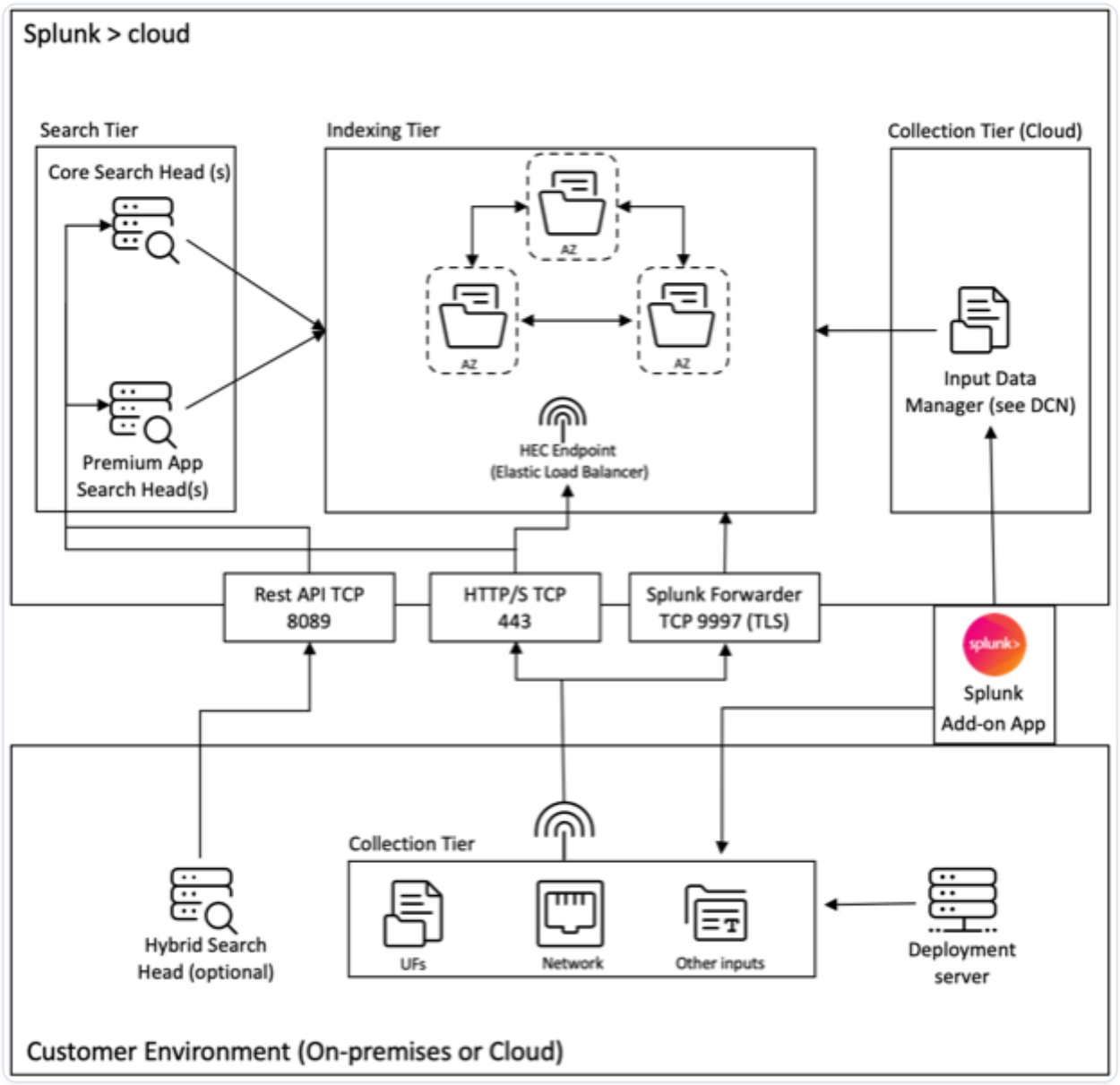
The primary way for customers to explore their data is through search. A search can be saved as a report and used to power dashboard panels. Searches are the extract information from your data.

In general, the Splunk add-on application is deployed in the Collection tier (at Splunk enterprise level), whereas our dashboarding application is deployed on the search layer (at Splunk Cloud level). On a simple on-prem setup, you can have all these three tiers on a single Splunk host (known as single server deployment).

The collection tier is much better way to use the add-on application for Splunk. There are two ways to install the add-on application. Either you can install it at the collection tier under the customer environment or you can install it at the inputs data manager under the **Splunk Cloud instance**.

Refer the following diagram to understand the Splunk deployment architecture with our add-on application:

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



The Inputs Data Manager (IDM) shown in the aforementioned diagram is the Splunk Cloud-managed implementation of a Data Collection Node (DCN) that supports scripted and modular inputs only. For data collection needs beyond that, you can deploy and manage a DCN in your environment using a Splunk heavy forwarder.

Splunk allows to collect, index, and search data from various sources. One way to collect data is through APIs, which allows Splunk to access data stored in other systems or applications. These APIs can include REST, web services, JMS and/or JDBC as the query mechanism. Splunk and any third-party developers offer a range of applications that enable API interactions through the Splunk modular input framework. These applications typically require a full Splunk enterprise software installation to function properly.

To facilitate the collection of data through APIs, it is common to deploy a heavy forwarder as a DCN. Heavy forwarders are more powerful agents than universal forwarders, as they contain the

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

full parsing pipeline and can understand and act on individual events. This enables them to collect data through APIs and process it before forwarding it to a Splunk instance for indexing.

To understand more about the high level architecture of a Splunk Cloud deployment, refer Splunk Validated Architectures.

Citrix Analytics dashboards for Splunk

NOTE

Attention: Citrix Content Collaboration™ and ShareFile has reached its end of life and is no longer available to users.

This feature is in preview.

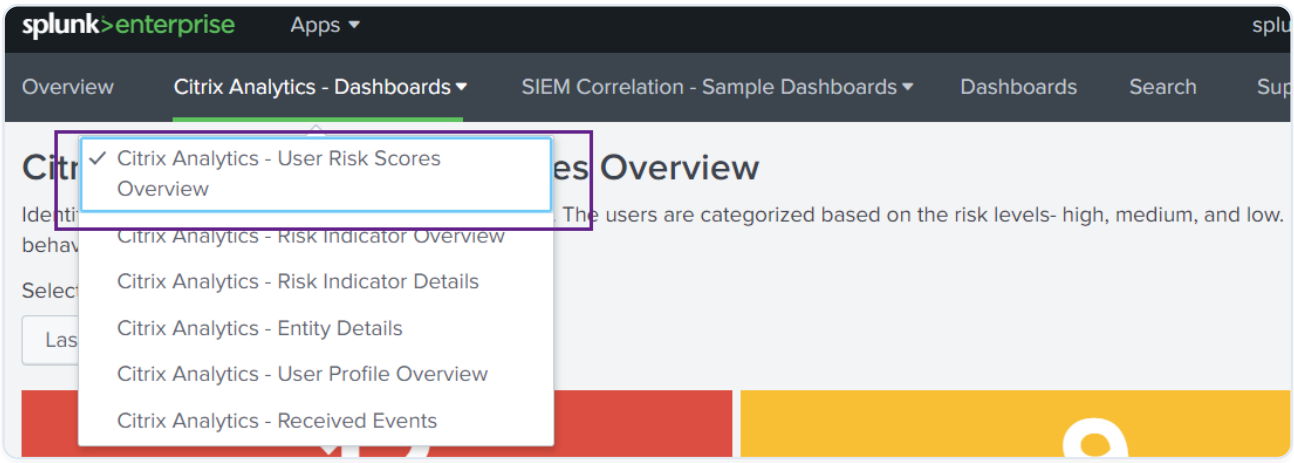
Prerequisite

To use the following Citrix Analytics dashboards, ensure that you have already configured and set up Citrix Analytics App for Splunk.

User risk score overview

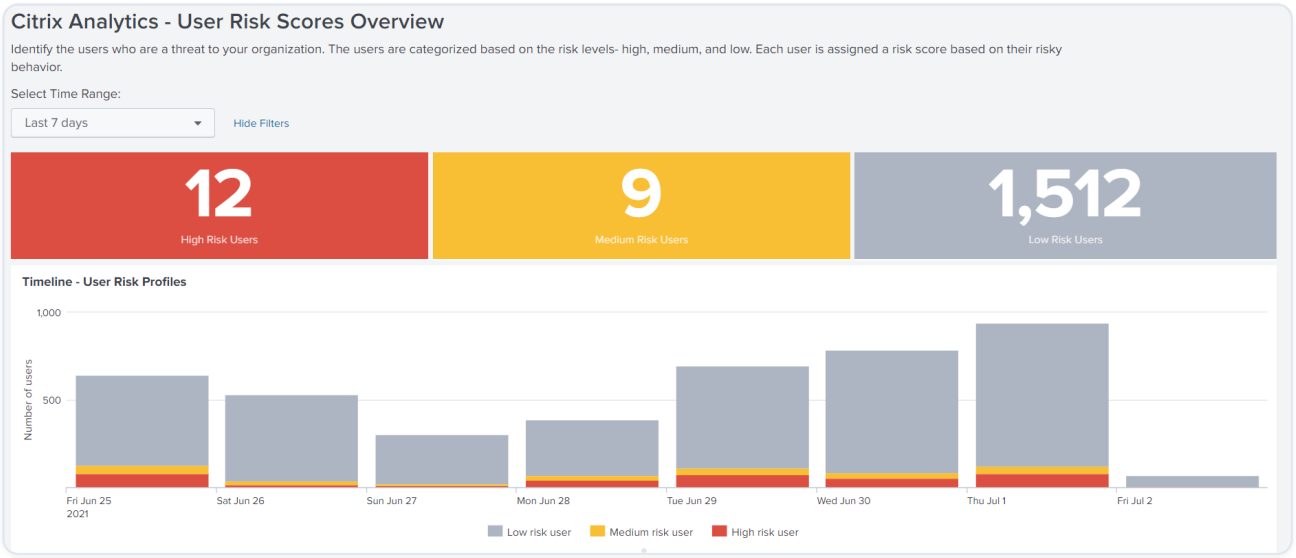
This dashboard provides a consolidated view of the risky users in your organization. The users are categorized by the risk levels- high, medium, and low. The risk levels are based on the anomalies in the user activities and accordingly a risk score is assigned. For more information about the types of risky users, see the Users dashboard.

To view this dashboard, click **Citrix Analytics- Dashboards > Citrix Analytics- User Risk Scores Overview**.



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

Select a preset time range or a custom time range to view the timeline of the risky users and their details.



The Risky Users table provides the following information:

- **User**: Indicates the user name. Click a user name to view the details about the user's risky behavior on the Citrix Analytics - Entity Details dashboard.
- **Compromised endpoints risks found**: Indicates the number of risk indicators triggered by the user that belongs to the compromised endpoints risk category.
- **Compromised users risks found**: Indicates the number of risk indicators triggered by the user that belongs to the compromised users risk category.
- **Data exfiltration risks found**: Indicates the number of risk indicators triggered by the user that belongs to the data exfiltration risk category.
- **Insider threats risks found**: Indicates the number of risk indicators triggered by the user that belongs to the insider threats risk category.
- **Risk Score**: Indicates the risk score of the user.

You can also search a user by the user name and get the required details.

For more information, see risk categories.

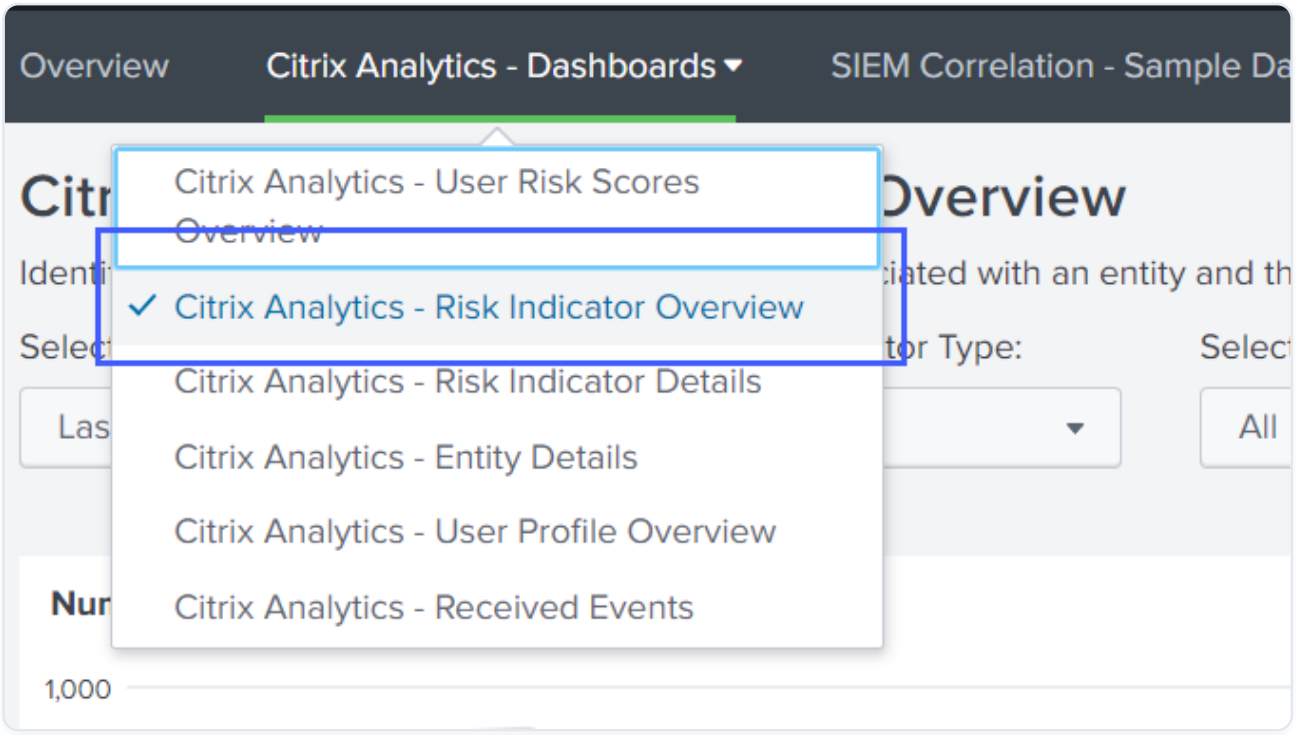
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Risk indicator overview

The dashboard provides a consolidated view of the risk indicators triggered by the users in your organization.

To view the dashboard, click **Citrix Analytics- Dashboards > Citrix Analytics- Risk Indicator Overview**.



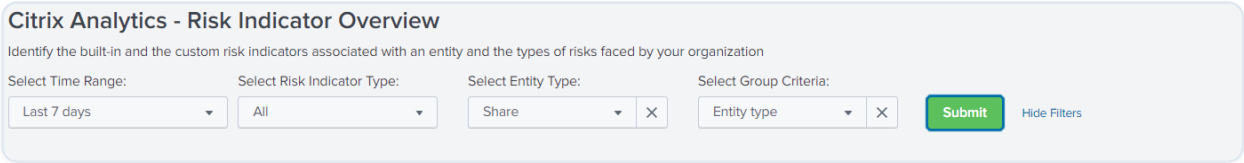
Select category to view report

Search the risk indicators by selecting one or more categories:

- **Time range**: Select a preset time range or a custom time range to view the triggered risk indicators for that period.
- **Risk indicator type**: Select the type of risk indicator: built-in or custom.
- **Entity type**: Select a user to view the associated risk indicators.

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

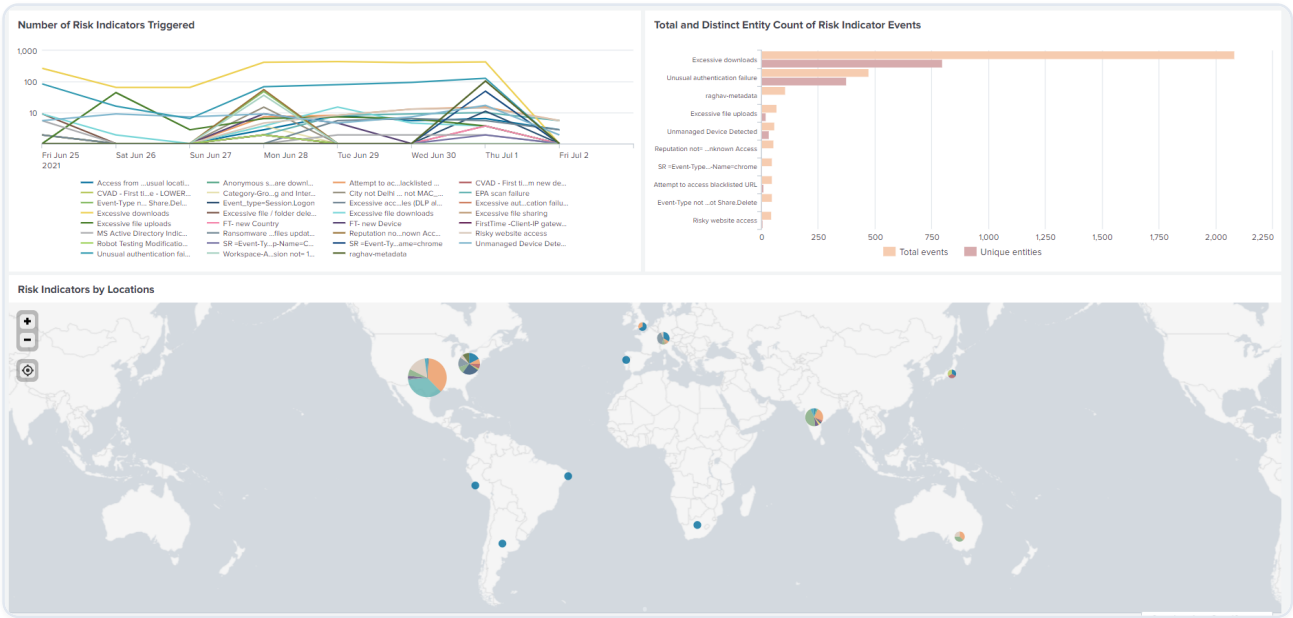
- **Group**: Select a criteria to group the user events by data source, indicator category, indicator name, indicator type, or entity type and view the associated risk indicators.



View report

Use the following reports to view details about the risk indicators by selecting one or more categories:

- **Number of risk indicators triggered**: Displays the number of risk indicators triggered for the selected period. Use this report to identify the pattern and areas of risky activities. Also, identify the top risky activities in your organization.
- **Total and distinct entity count of risk indicator events**: Displays the total events and the unique events corresponding to a risk indicator. Use this report to identify the occurrences of each risk indicator and the top risk indicators in your organization. You can also identify how many unique users triggered a particular risk indicator and check if the risk indicator is triggered by a larger or a smaller user group.
- **Risk indicators by locations**: Displays the number of risk indicators triggered by the users across locations. Use this report to identify the locations that show more risky activities and check if the locations are outside the area of operation of your organization.
- **Risk indicator details**: Displays the details about the risk indicator such as the associated data source, indicator category, indicator type, and number of occurrences.



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

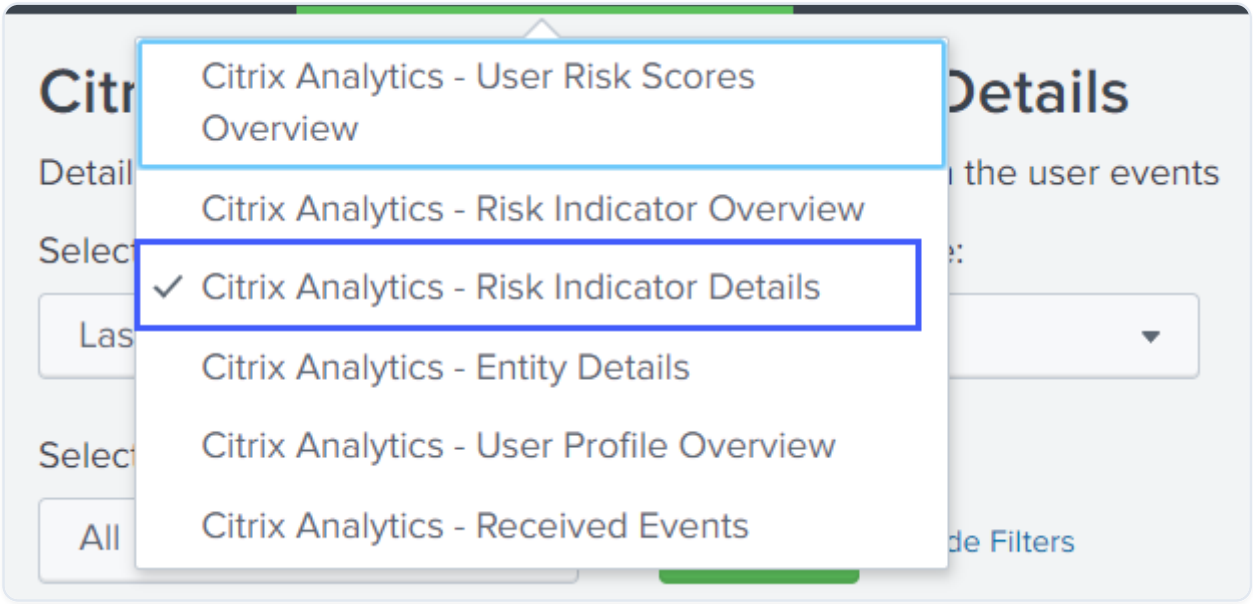
Risk Indicator Details

Data source	Indicator category	Indicator type	Indicator name	Number of Risk Indicator Events
Citrix Content Collaboration	Data exfiltration	builtin	Excessive downloads	2084
Citrix Content Collaboration	Compromised users	builtin	Unusual authentication failure	473
Citrix Virtual Apps and Desktops	Data exfiltration	custom	raghav-metadata	104
Citrix Content Collaboration	Insider threats	builtin	Excessive file uploads	68
Citrix Endpoint Management	Compromised endpoints	builtin	Unmanaged Device Detected	59
Citrix Access Control	Compromised users	custom	Reputation not= Clean Access AND Reputation not= Unknown Access	55
Citrix Virtual Apps and Desktops	Compromised users	custom	SR =Event-Type=Citrix.EventMonitor.AppStart AND App-Name=chrome	49
Citrix Access Control	Insider threats	builtin	Attempt to access blacklisted URL	48
Citrix Content Collaboration	Compromised users	custom	Event-Type not Share.Create AND Event-Type not Share.Delete	48
Citrix Access Control	Insider threats	builtin	Risky website access	44

Risk indicator details

The dashboard provides the detailed information about the built-in and custom risk indicators triggered by the users. For more information, see Citrix user risk indicators and Custom risk indicators.

To view the dashboard, click **Citrix Analytics- Dashboards > Citrix Analytics- Risk Indicator Details**.



Select category to view the reports

View the details of the risk indicators by selecting one or more categories:

- **Time range**: Select a preset time range or a custom time range to view the details of the triggered risk indicators for that period.
- **Entity type**: Select a user to view the details of the associated risk indicators.
- **Risk Indicator type**- Select the type of risk indicator-built-in or custom to view their details.
- **Data source**- Select the data source to view the details of the associated risk indicators.
- **Risk indicator category**- Select the risk category to view the details of the associated risk indicators.

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

- **Risk indicator**- Select the risk indicator to view its details.

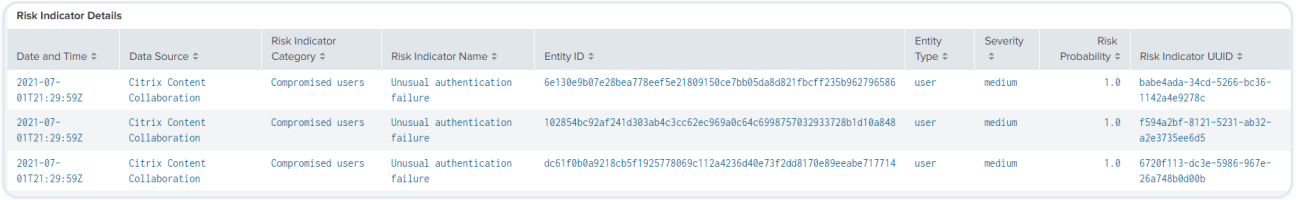
View the reports

For example, from the Select Risk Indicator list, select **Unusual authentication failure (Citrix Content Collaboration)**, click **Submit**, and view the following information:

- Top 10 users associated with the risk indicator
- Details about the risk indicator such as
  - Date and time of trigger
  - Associated data source
  - Associated risk category
  - Associated entity ID and user entity type
  - Risk severity-high, medium, or low
  - Risk probability of the user event
  - Unique identity of the risk indicator (UUID)



On **Top 10 Entities by Risk Indicators**, click an entity to view its details on the **Citrix Analytics-Entity Details** dashboard.



Risk Indicator Details

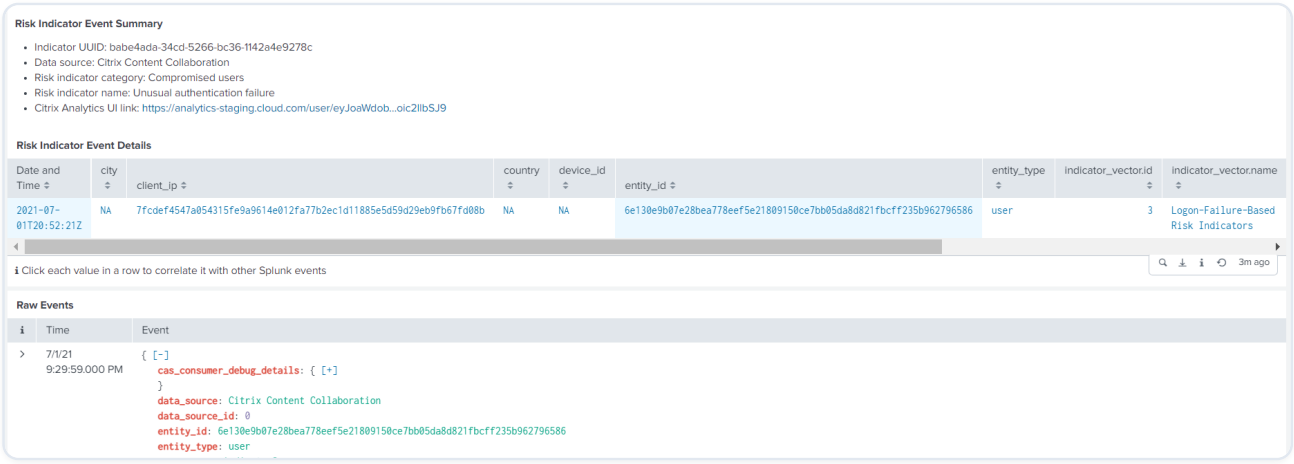
Date and Time	Data Source	Risk Indicator Category	Risk Indicator Name	Entity ID	Entity Type	Severity	Risk Probability	Risk Indicator UUID
2021-07-01T21:29:59Z	Citrix Content Collaboration	Compromised users	Unusual authentication failure	6e130e9b07e28bea778eef5e21809150ce7bb05da8d821fbcff235b962796586	user	medium	1.0	babe4ada-34cd-5266-bc36-1142a4e9278c
2021-07-01T21:29:59Z	Citrix Content Collaboration	Compromised users	Unusual authentication failure	102854bc92af241d303ab4c3cc62ec969a0c64c6998757032933728b1d10a848	user	medium	1.0	f594a2bf-8121-5231-ab32-a2e3735ee6d5
2021-07-01T21:29:59Z	Citrix Content Collaboration	Compromised users	Unusual authentication failure	dc61f0b0a9218cb5f1925778069c112a4236d40e73f2dd8170e89eeabe717714	user	medium	1.0	6720f113-dc3e-5986-967e-26a748b0d00b

Click each row of the **Risk Indicator Details** table to view the event summary, event details, and raw events of the selected risk indicator.

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

On the **Risk Indicator Event Summary** section, click the **Citrix Analytics UI link** to go directly to the user timeline on Citrix Analytics for Security™ from your Splunk. On the user timeline, view the risk indicator, associated events, and any applied actions for the user.

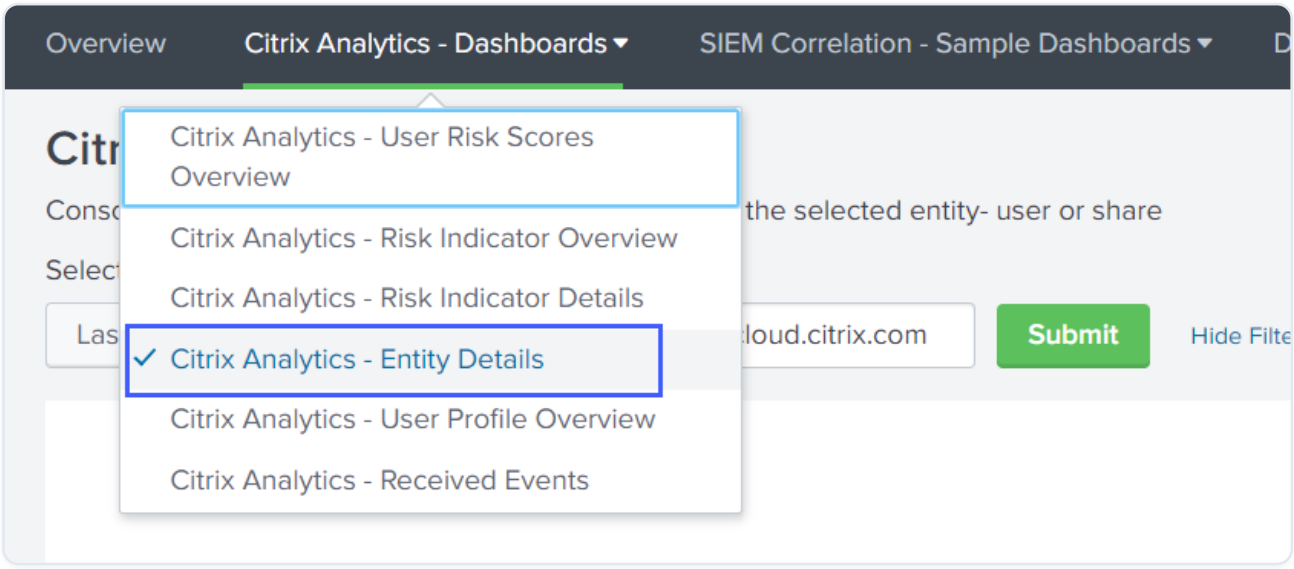
For more information about event summary and event details, see Citrix Analytics data format for SIEM.



Entity details

Use the dashboard to view the details about a user entity user and its risky behavior.

To view the dashboard, click **Citrix Analytics- Dashboards > Citrix Analytics- Entity Details**.



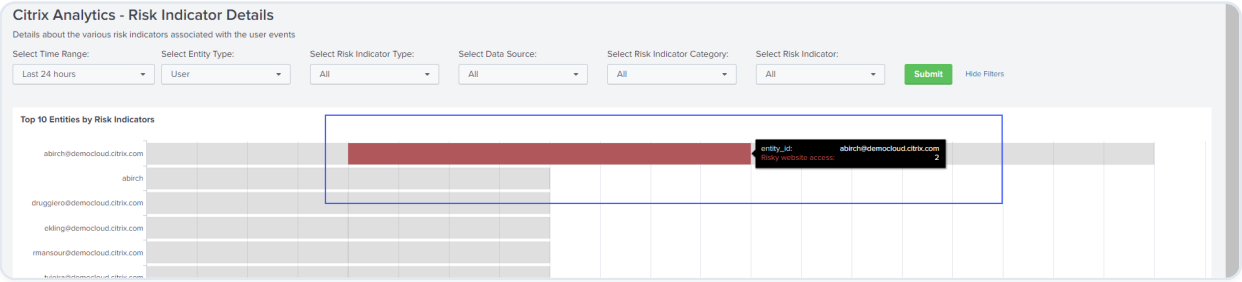
View the report

Enter a time range and the entity (user name) and click **Submit** to view the detailed information.

Alternatively, you can also view the detailed information about an entity from the following dashboards:

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

- On **Citrix Analytics- Risk Indicator Details**, go to **Top 10 Entities by Risk Indicators**, and click an entity.

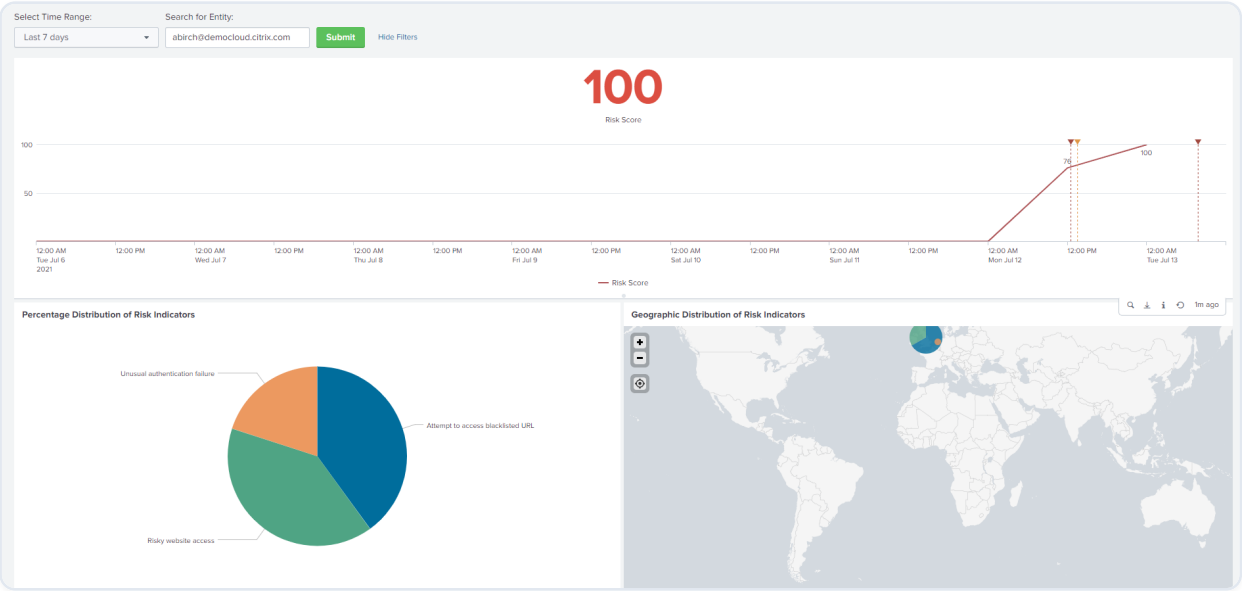


- On **Citrix Analytics- Risk Score Overview**, go to **Risky Users**, and click a user name.

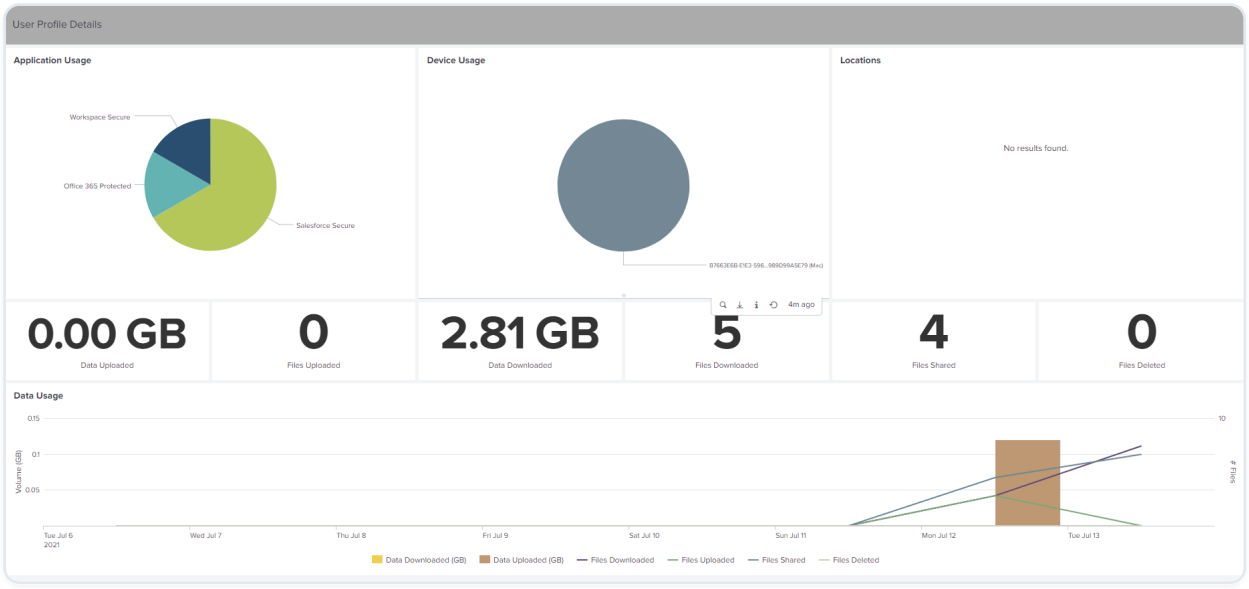


The following detailed information is displayed:

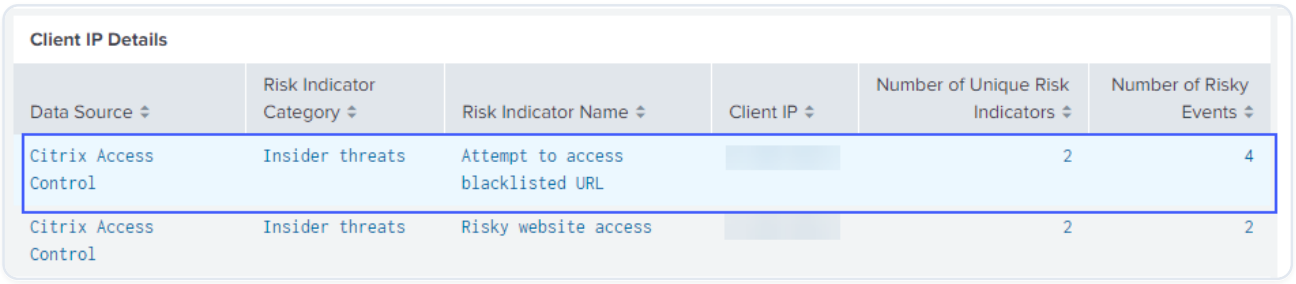
- Current risk score and the risk score timeline for the selected time range.
- Percentage distribution of the risk indicators. Helps you to analyze the pattern of risky activities of the entity.
- Geographic distribution of the risk indicators. Helps you to identify the unusual and high-risk locations.
- Client IP details associated with the risky activities.
- User device details associated with the risky activities.
- Risk indicator details such as associated data source, risk category, risk severity and so on.



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



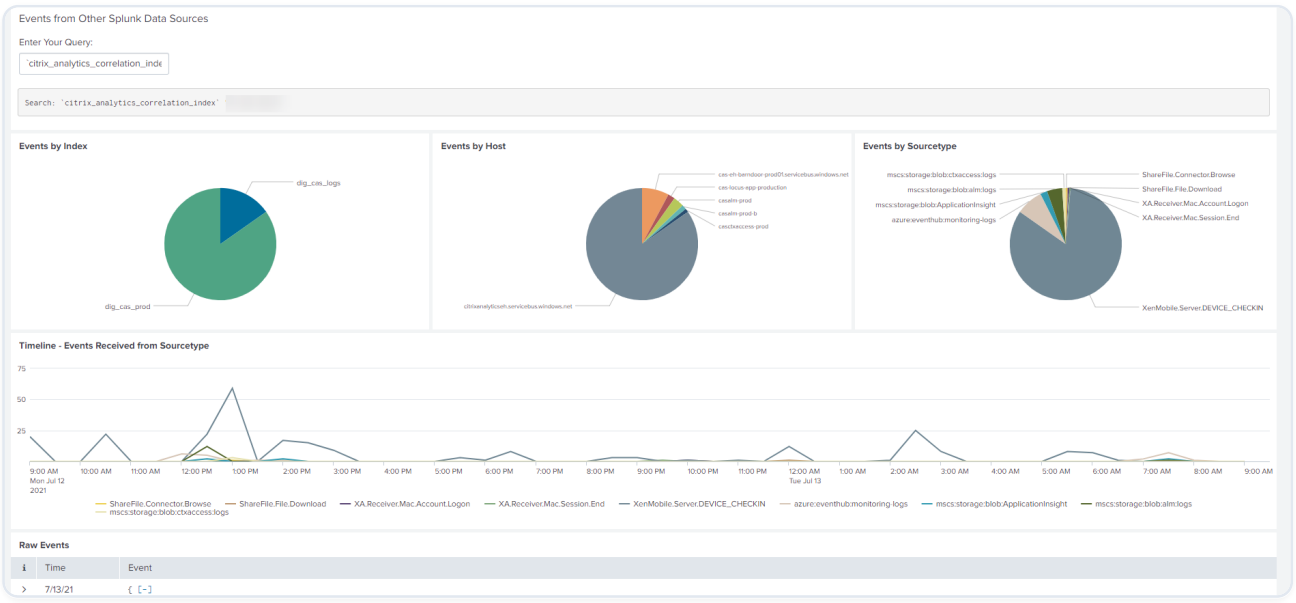
Correlate the client IPs and user devices associated with risky activities with the events collected from other security sources that are connected to your Splunk. For example, click a row on the **Client IP Details** table.



Client IP Details

Data Source	Risk Indicator Category	Risk Indicator Name	Client IP	Number of Unique Risk Indicators	Number of Risky Events
Citrix Access Control	Insider threats	Attempt to access blacklisted URL		2	4
Citrix Access Control	Insider threats	Risky website access		2	2

On the **Citrix Analytics Event Correlation** dashboard, you can view the events associated with the selected client IP that are correlated from your other security data sources (based on index and source type). These events provide deeper insights into the malicious activities associated with the client IP.

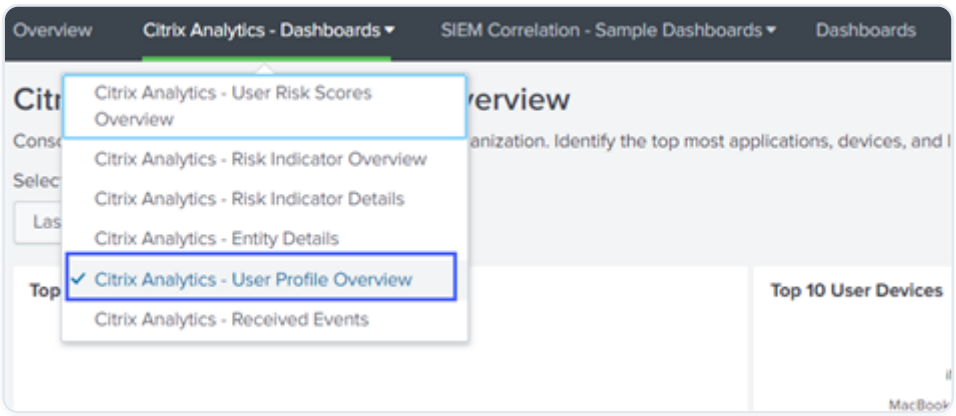


© 1997–2026 Citrix Systems, Inc. All rights reserved.

User profile overview

Use the dashboard to view the event metrics associated with the users in your organization.

To view the dashboard, click **Citrix Analytics- Dashboards > Citrix Analytics- User Profile Overview**.



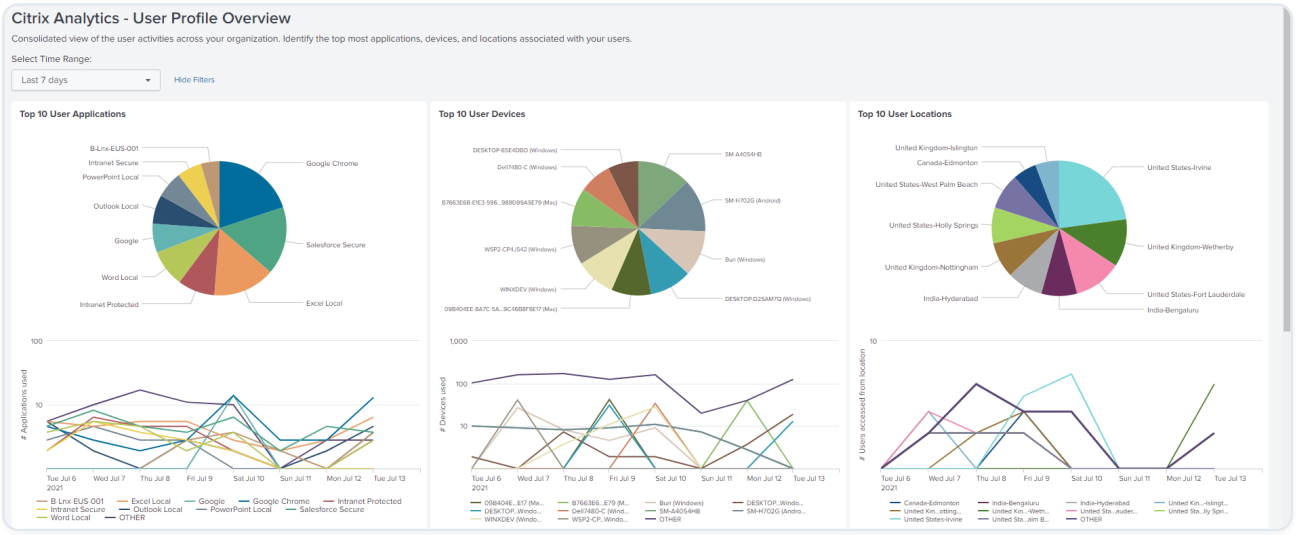
View the events

Select a time range and view the following metrics:

- Top 10 applications used by the users
- Top 10 devices used by the users
- Top 10 locations used by the users
- Number of Web and SaaS applications used
- Number of devices used
- Number of users who have accessed across locations
- Data usage metrics such as files uploaded, downloaded, shared

These metrics provide you insights into the user activities in your organization. You can identify the topmost applications and devices, usage patterns, non-compliant devices and applications, unusual locations, risky access, and unusual file activities.

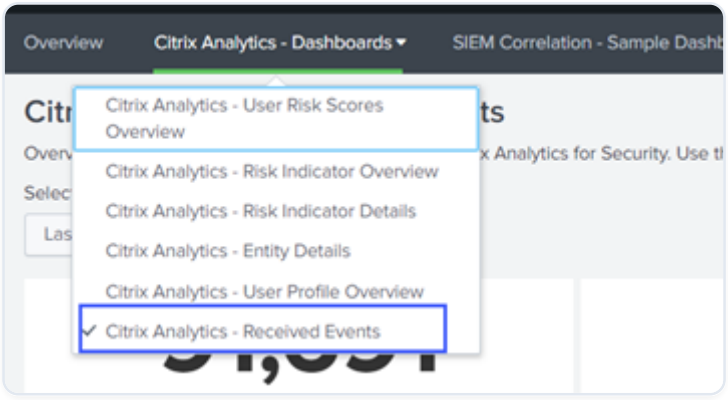
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Received events

Use the dashboard to view the events received from Citrix Analytics for Security. An event indicates a type of user activity.

To view the dashboard, click **Citrix Analytics- Dashboards > Citrix Analytics- Received Events**.



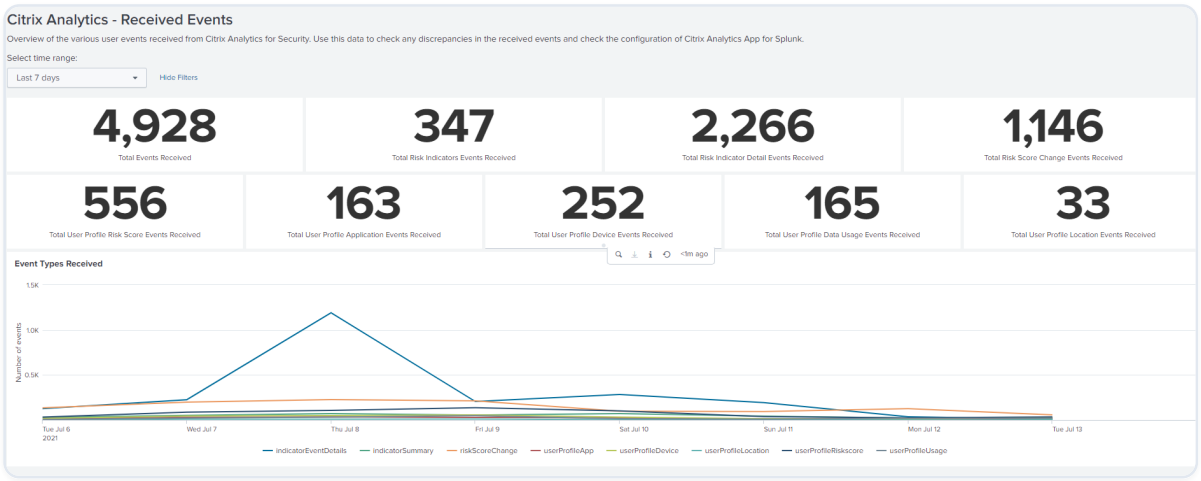
View the reports

Select a time range to view and compare the various types of events received. The dashboard provides the following information:

- Total events received: It is the aggregate of all the events received from Citrix Analytics for Security including the following:
  - Total risk indicator events: Indicates the events associated with the triggered risk indicators by the users.
  - Total risk indicator detail events: Indicates the events associated with the details of the triggered risk indicators.

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

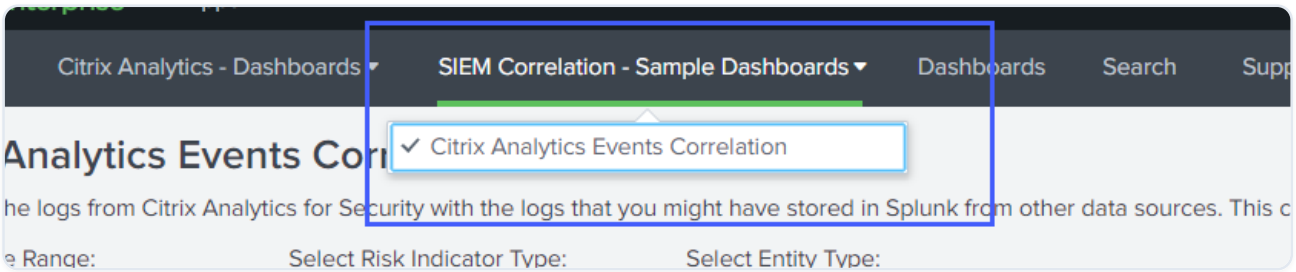
- Total risk score change events: Indicates the events associated with the user's risk score change.
- Total user profile risk score events: Indicates the events associated with users' risk scores.
- Total user profile application events: Indicates the events associated with the applications used by the users.
- Total user profile device events: Indicates the events associated with the devices used by the users.
- Total user profile data usage events: Indicates the events associated with the data usage of the users.
- Total user profile location events: Indicates the events associated with the locations accessed by the users.



Sample event correlation

Use the dashboard to correlate events received from Citrix Analytics for Security with the events collected from other security data sources configured in your Splunk. You get deeper insights into the user's risky activities collected from multiple data sources, find relations between the events, and identify any threats.

To view the dashboard, click **SIEM Correlation- Sample Dashboards > Citrix Analytics Event Correlation**.



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

Prerequisites

To perform correlation, ensure the following:

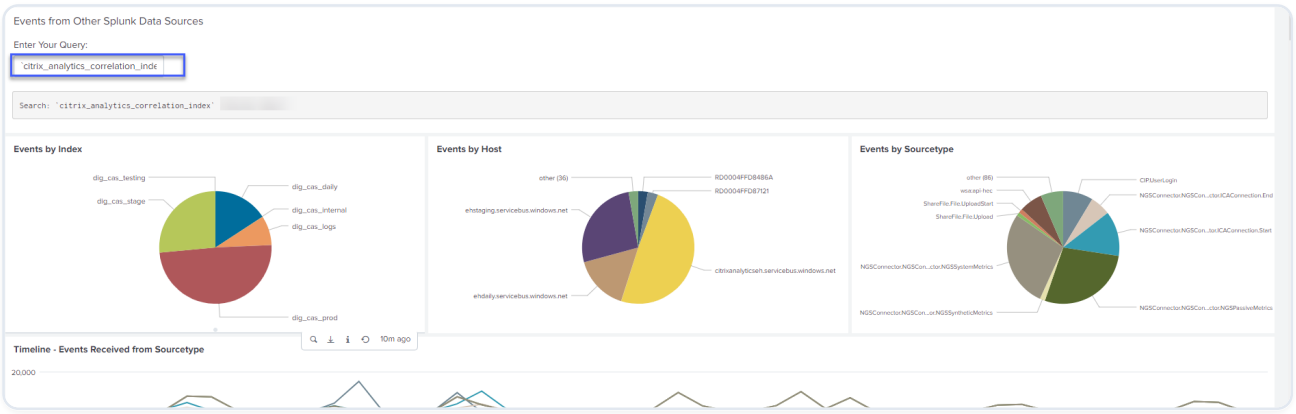
- You must have events from your other security data sources to correlate. For example, events associated with users, devices, and client IP addresses received from other data sources configured in your Splunk.
- You must have a correlation index already defined during configuration.

Correlate the events

You can view the top risky entities and the top risky IP addresses detected by Citrix Analytics for Security. To correlate these events with other data sources (defined in the index and the source type), click an entity or an IP address from the tables.



The index value shown in the query field is defined during the configuration of the app. You can change the index value to a different security data source based on your requirements.



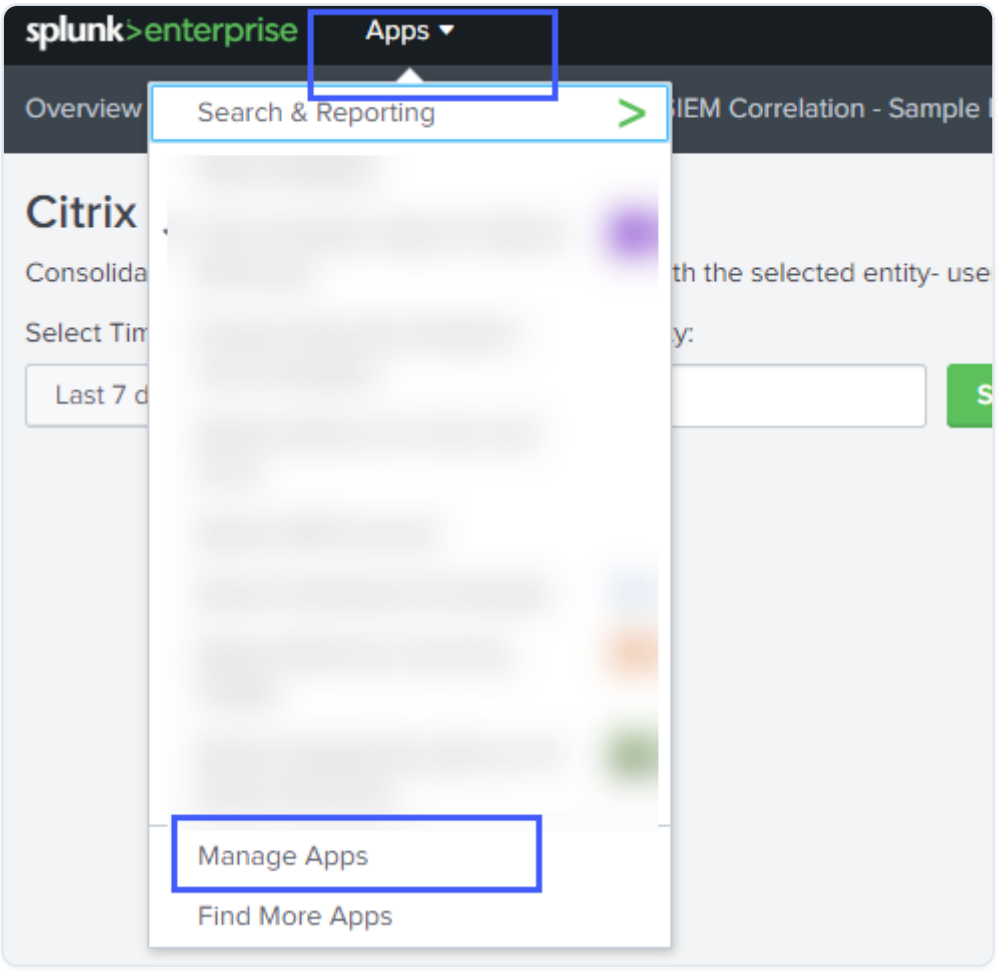
Troubleshooting for no events

If you do not find any events on all the dashboards, it might be because of the configuration issues in Citrix Analytics App for Splunk and Citrix Analytics add-on for Splunk. In such scenario, verify the index value and the source type value. Ensure that the values of the index and source type are the same in both the app and the add-on.

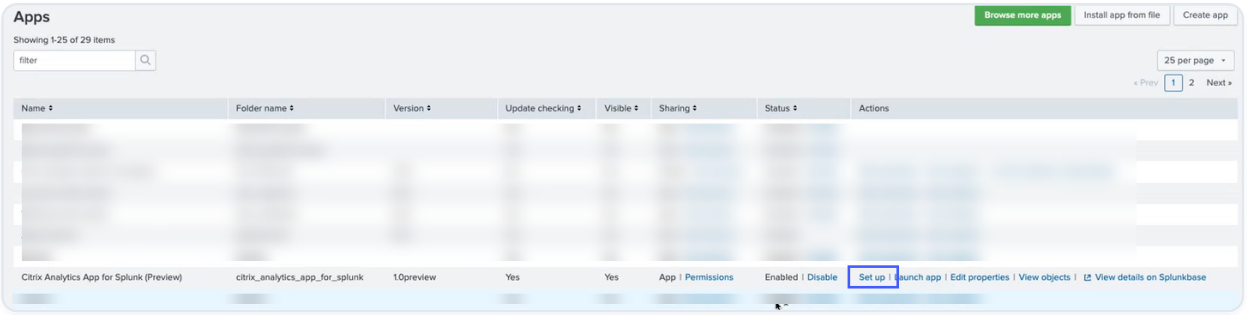
To view the configuration settings of the Citrix Analytics App for Splunk:

1. Click **Apps > Manage Apps**.

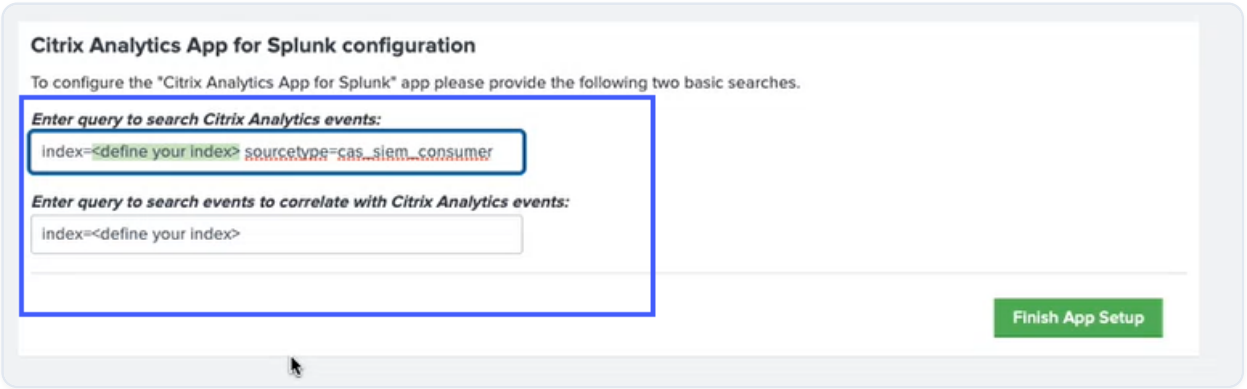
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Locate Citrix Analytics App for Splunk from the list. Click **Set up**.



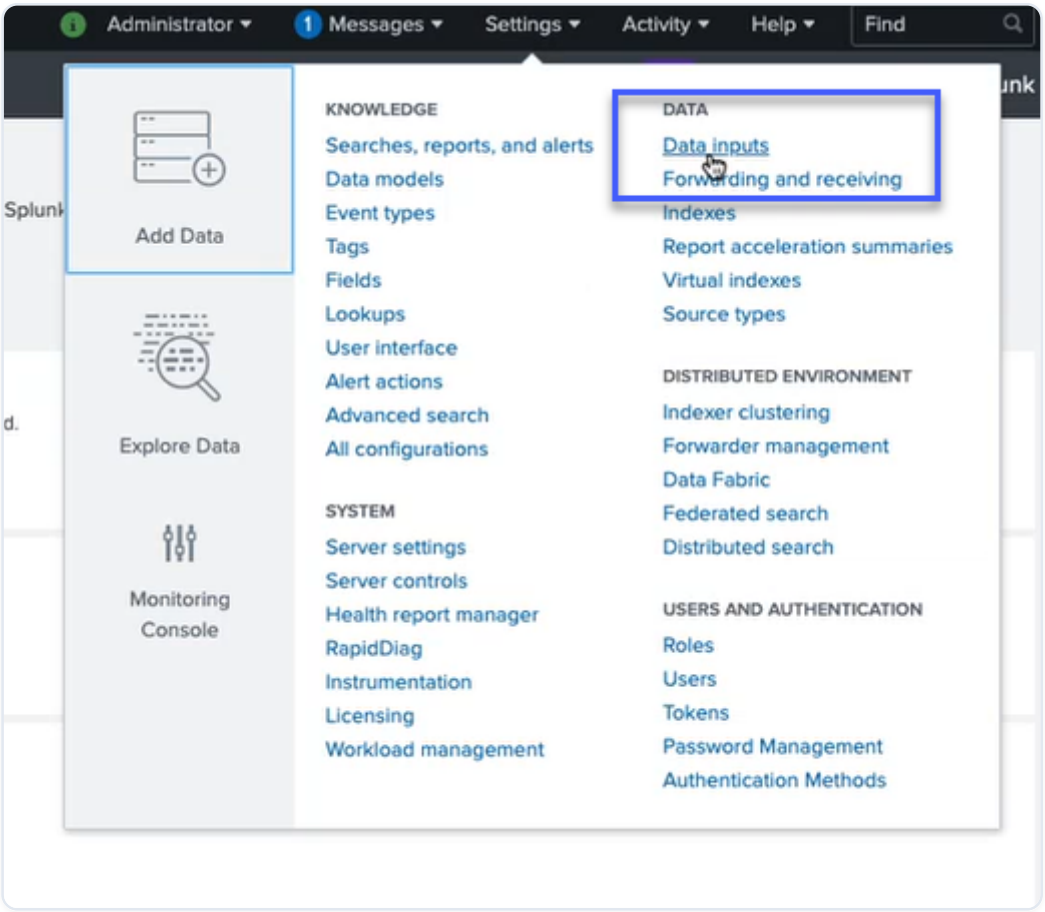
3. Check the source type and the index.



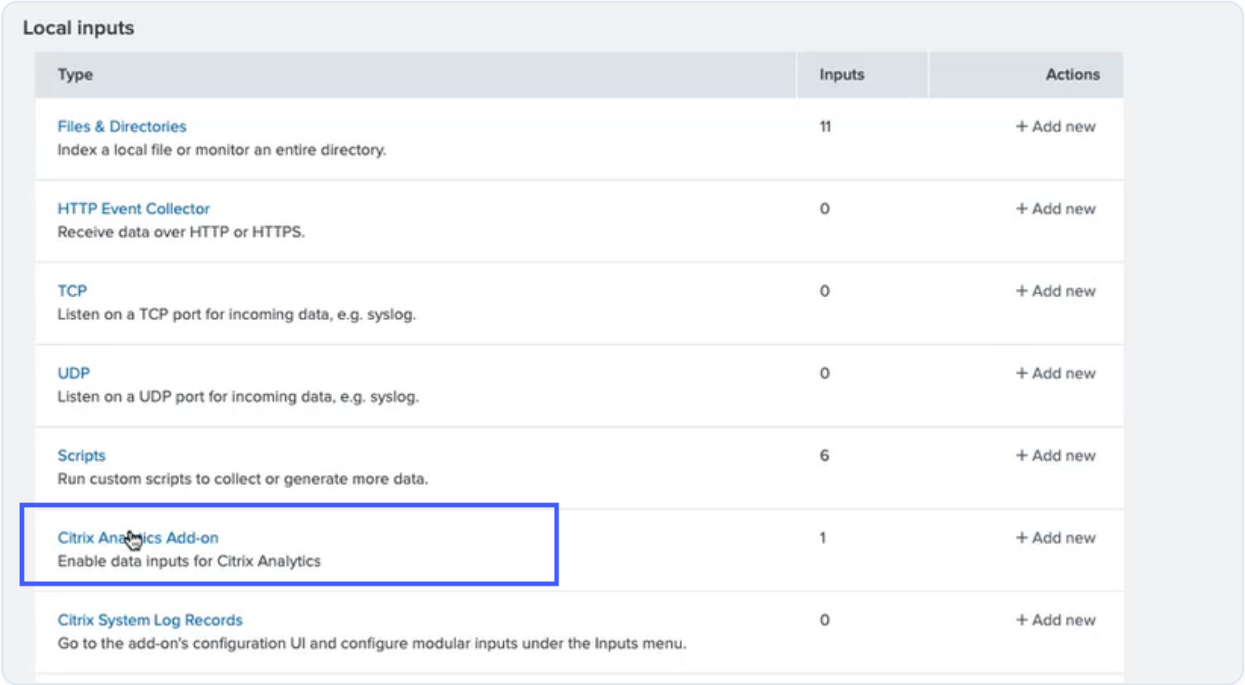
To view the configuration settings of the Citrix Analytics add-on for Splunk:

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

1. Click **Settings > Data inputs**.

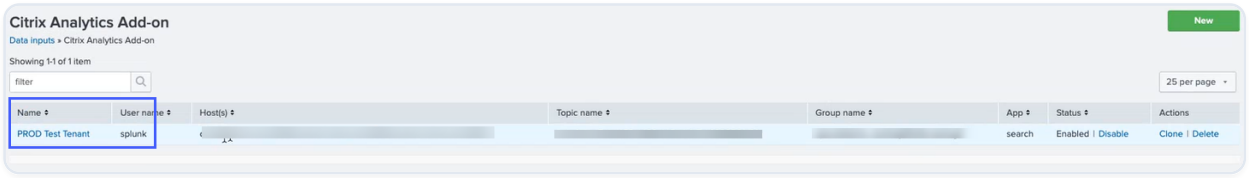


2. Click **Citrix Analytics Add-on**.

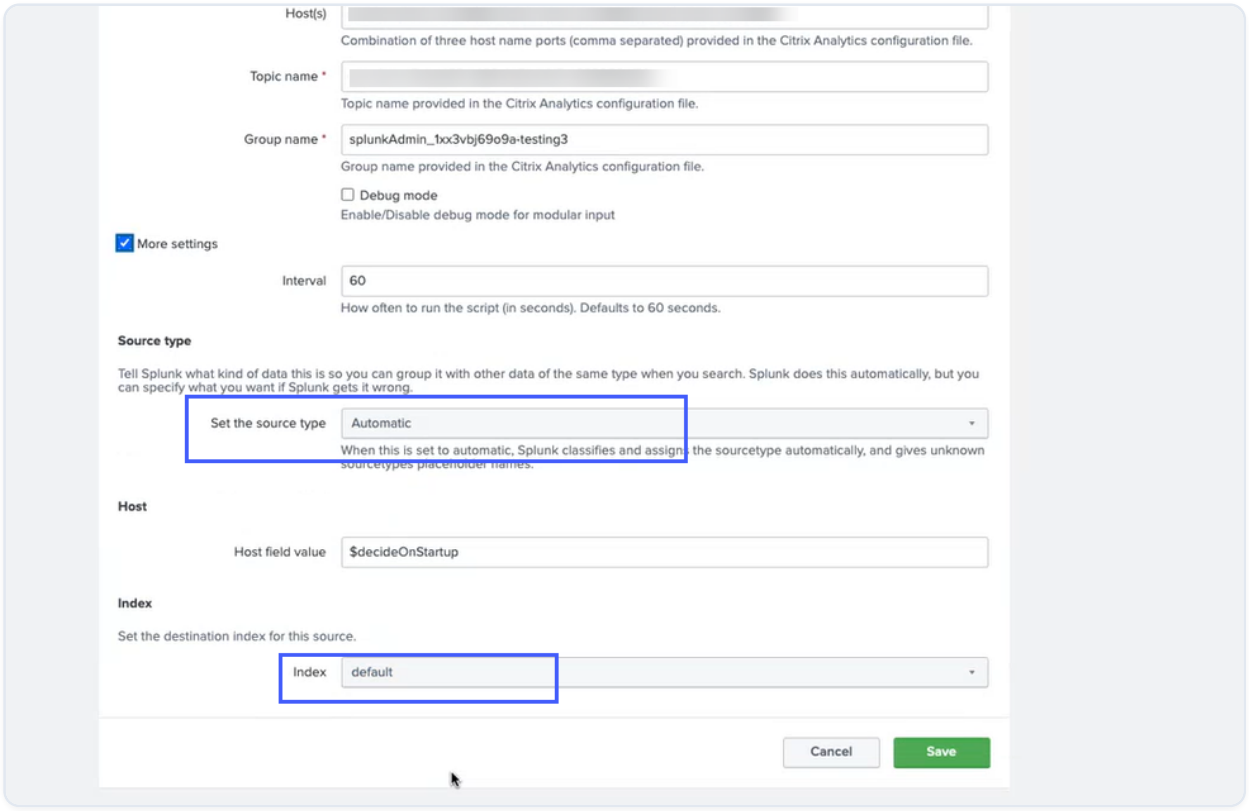


3. Click the tenant from which you get the events.
4. Select **More settings**.

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



5. Check the source type and the index.



For more information about configuration, see Configure Citrix Analytics add-on for Splunk.

Configuration issues with Citrix Analytics add-on for Splunk

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/splunk-add-on-debugging.md

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

Microsoft Sentinel integration

NOTES

- Contact mailto:CAS-PM-Ext@cloud.com to request assistance for the Microsoft Sentinel integration, exporting data to Microsoft Sentinel, or provide feedback.
- Data export to Microsoft Sentinel by using the Logstash engine is in preview. This feature is provided without a service level agreement and it's not recommended for production workloads. For more information, see the Microsoft Sentinel documentation.

Integrate Citrix Analytics for Security™ with your Microsoft Sentinel by using the Logstash engine.

This integration enables you to export and correlate the users' data from your Citrix IT environment to Microsoft Sentinel and get deeper insights into your organization's security posture. View the insightful dashboards that are unique to Citrix Analytics for Security in your Splunk environment. You can also create custom views based on your security requirements.

For more information about the benefits of the integration and the type of processed data that is sent to your SIEM, see Security Information and Event Management integration.

Prerequisites

- Turn on data processing for at least one data source. It helps Citrix Analytics for Security to begin the Microsoft Sentinel integration process.
- Ensure that the following endpoint is in the allow list in your network.

ENDPOINT	UNITED STATES REGION	EUROPEAN UNION REGION	ASIA PACIFIC SOUTH REGION
Kafka brokers	`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`

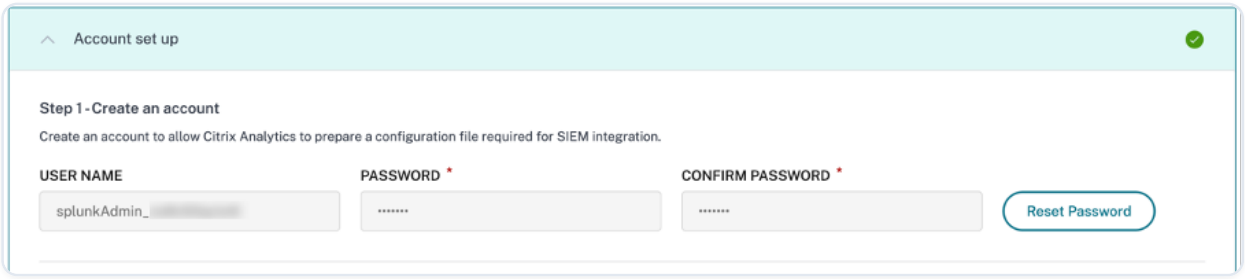
© 1997–2026 Citrix Systems, Inc. All rights reserved.

ENDPOINT	UNITED STATES REGION	EUROPEAN UNION REGION	ASIA PACIFIC SOUTH REGION
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`		

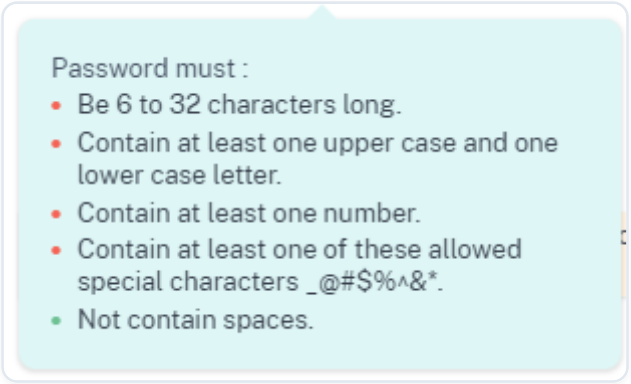
- Ensure that you use logstash versions 7.17.7 or later (tested versions for compatibility with Citrix Analytics for Security: v7.17.7 and v8.5.3) with the Microsoft Sentinel output plug-in for Logstash.

Integrate with Microsoft Sentinel

1. Go to **Settings > Data Exports**.
2. On the **Account set up** section, create an account by specifying the user name and a password. This account is used to prepare a configuration file, which is required for the integration.

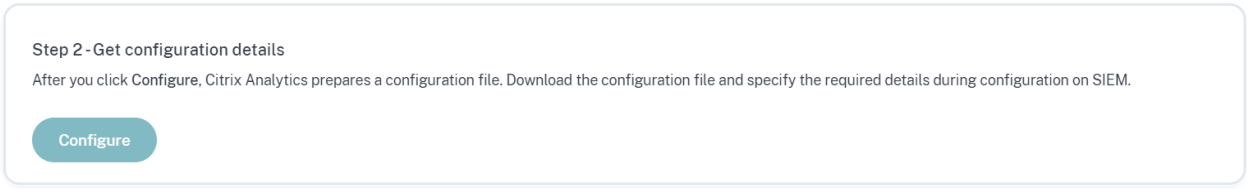


3. Ensure that the password meets the following conditions:



4. Click **Configure** to generate the Logstash configuration file.

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



5. Select the Azure Sentinel (Preview) tab to download the configuration files:

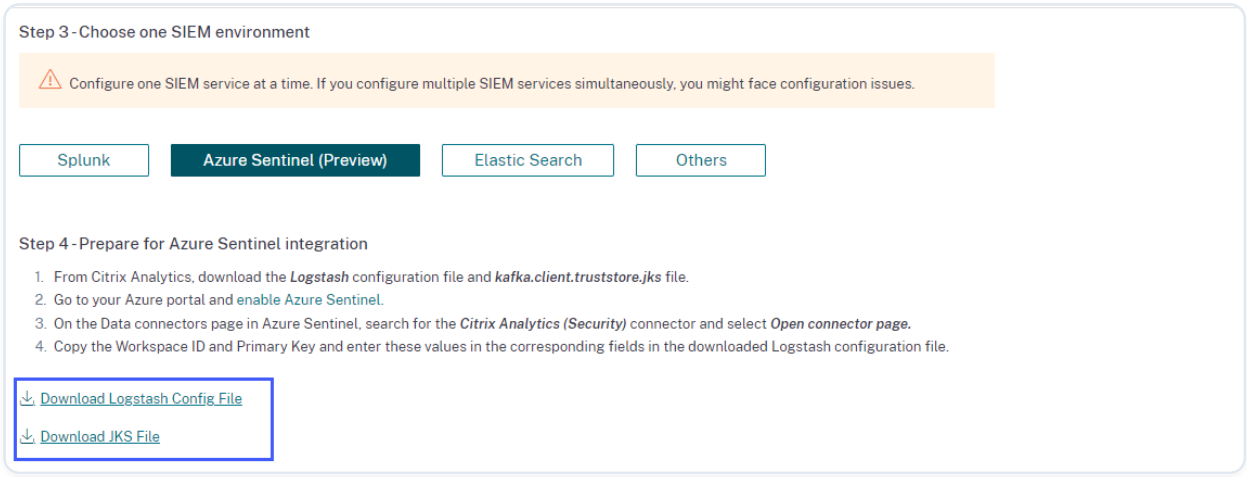
   - **Logstash config file**: Contains the configuration data (input, filter, and output sections) for sending events from Citrix Analytics for Security to Microsoft Sentinel using the Logstash data collection engine.

     For information on Logstash config file structure, see the Logstash documentation.

   - **JKS file**: Contains the certificates required for SSL connection.

NOTE

These files contain sensitive information. Keep them in a safe and secure location.



6. Prepare your Azure Sentinel integration:

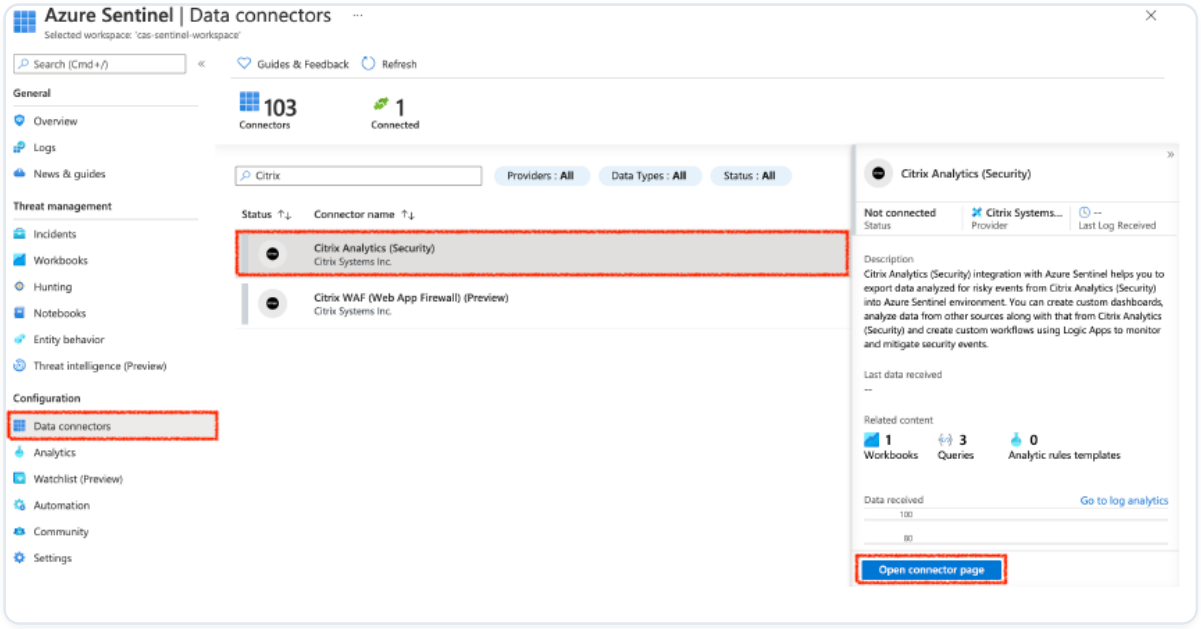
   a. On your Azure portal, enable Microsoft Sentinel. You can create a workspace or use your existing workspace to run Microsoft Sentinel.

   b. From the main menu, select **Data connectors** to open the data connectors gallery.

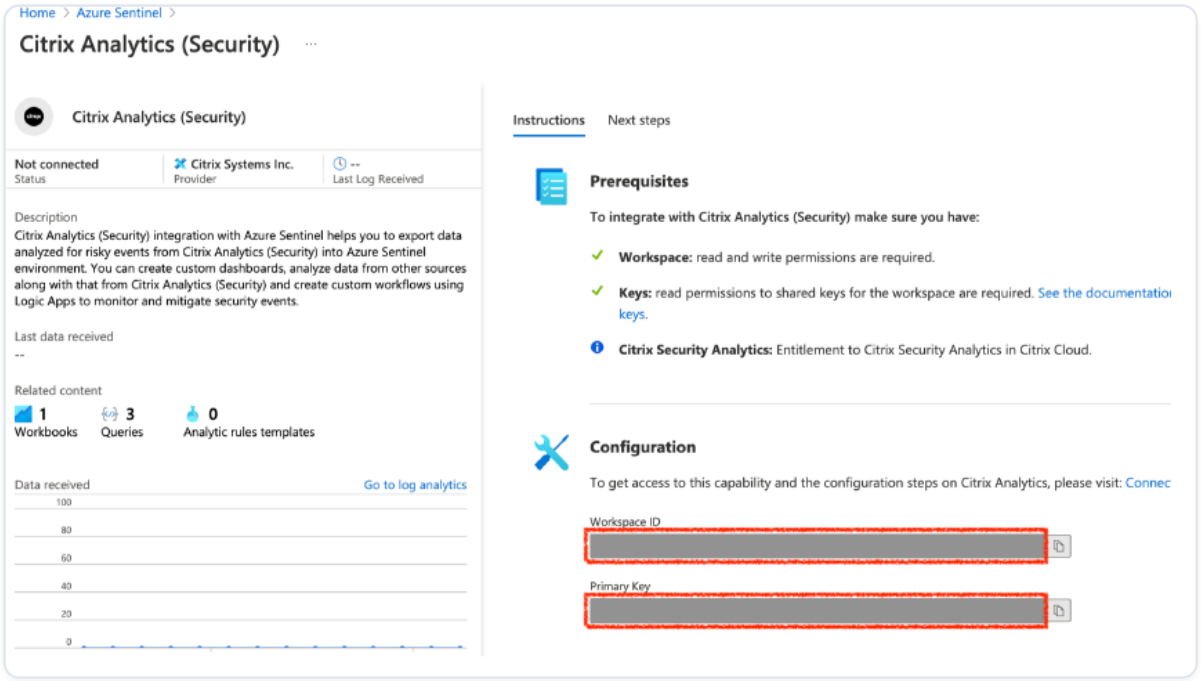
   c. Search for **Citrix Analytics (Security)**.

   d. Select **Citrix Analytics (Security)** and select **Open connector page**.

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



e. From the **Citrix Analytics (Security)** page, copy the **Workspace ID** and **Primary Key**. You must enter this information in the Logstash config file in subsequent steps.



f. Configure Logstash on your host machine:

   i. On your Linux or Windows host machine, install Logstash and Microsoft Sentinel output plug-in for Logstash.

   ii. On the host machine where you have installed Logstash, place the following files in the specified directory:

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

HOST MACHINE TYPE	FILE NAME	DIRECTORY PATH
Linux	CAS_AzureSentinel_LogStash_Config.config	For Debian and RPM packages: `/etc/logstash/conf.d/`
		For .zip and .tar.gz archives: `{extract.path}/config`
	kafka.client.truststore.jks	For Debian and RPM packages: `/etc/logstash/ssl/`
		For .zip and .tar.gz archives: `{extract.path}/ssl`
Windows	CAS_AzureSentinel_LogStash_Config.config	`C:\logstash-7.xx.x\config`
	kafka.client.truststore.jks	

For information on the default directory structure of Logstash installation packages, see Logstash documentation.

iii. Open the Logstash config file and do the following:

i. In the input section of the file, enter the following:

- **Password**: The password of the account that you have created in Citrix Analytics for Security to prepare the configuration file.
- **SSL truststore location**: The location of your SSL client certificate. This is the location of the kafka.client.truststore.jks file in your host machine.



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

ii. In the output section of the file, enter the **Workspace ID** and **Primary key** (that you have copied from Microsoft Sentinel) in the output section of the file.

```
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. Restart the Logstash host machine to send the processed data from Citrix Analytics for Security to Microsoft Sentinel.

g. Go to your Microsoft Sentinel Workspace and view the data in the Citrix Analytics workbook.

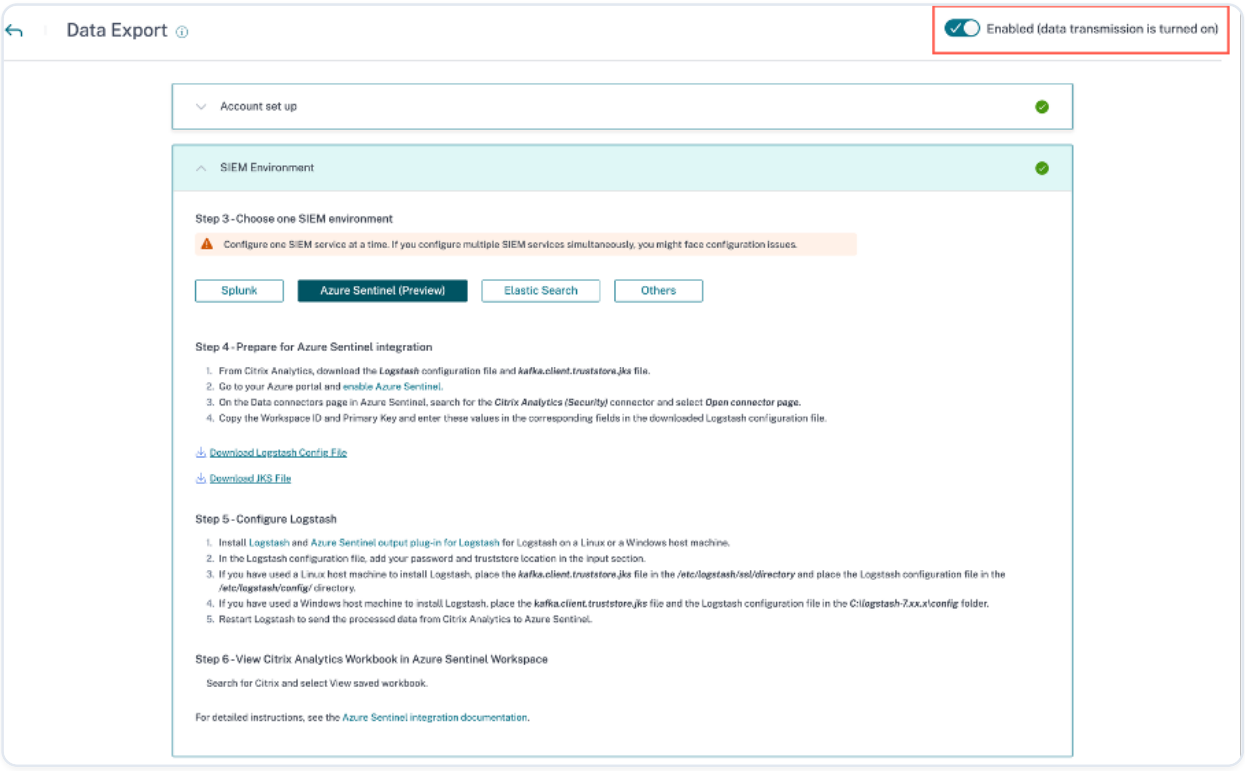
Turn on or off data transmission

After Citrix Analytics for Security prepares the configuration file, data transmission is turned on for Microsoft Sentinel.

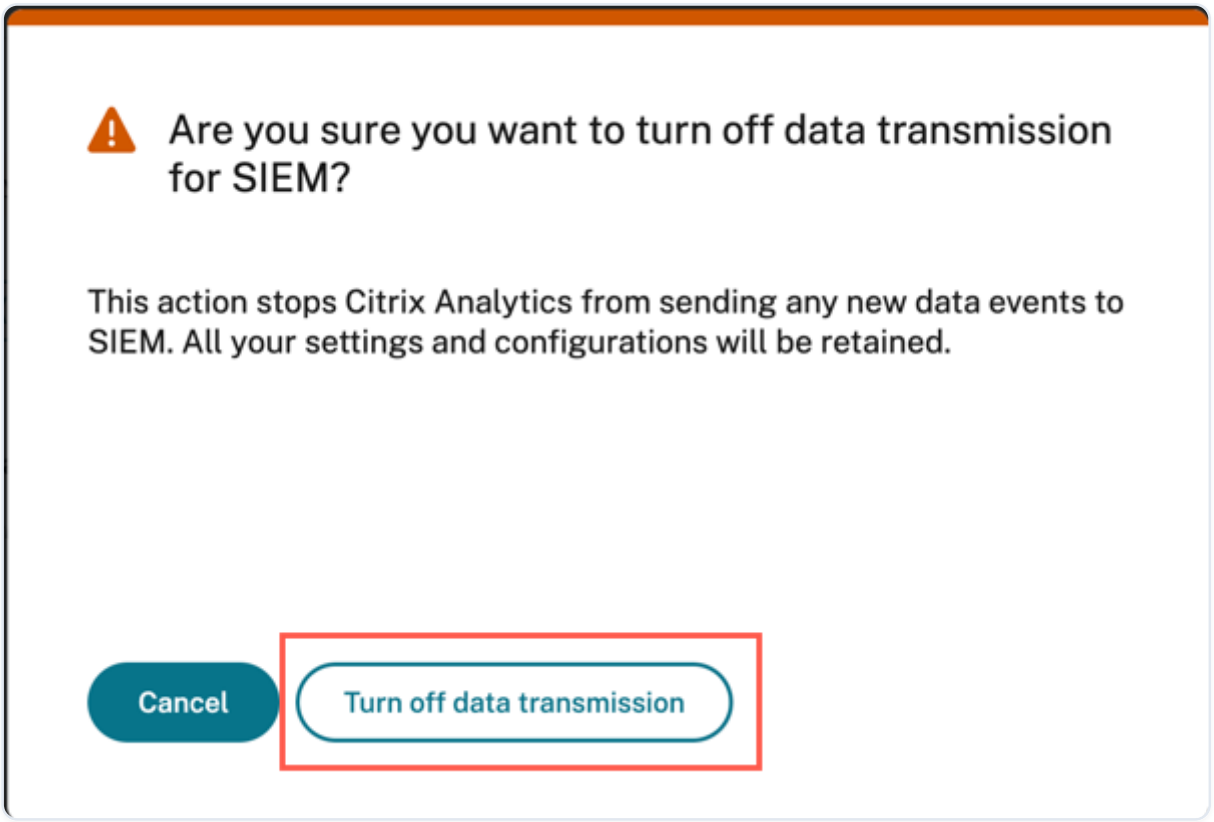
To stop transmitting data from Citrix Analytics for Security:

1. Go to **Settings > Data Exports**.
2. Turn off the toggle button to disable the **data transmission**. By default the data transmission always enabled..

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



A warning window appears for your confirmation. Click **Turn off data transmission** button to stop the transmission activity.



To enable data transmission again, turn on the toggle button.

For learn more about Microsoft Sentinel integration, refer the following links:

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

- Citrix Analytics Integration with Microsoft Sentinel
- Raise your threat-hunting game with Citrix Analytics for Security and Microsoft Sentinel

Citrix Analytics workbook for Microsoft Sentinel

NOTE

This feature is in preview.

This article describes the Citrix Analytics workbook that is available in your Microsoft Sentinel workspace.

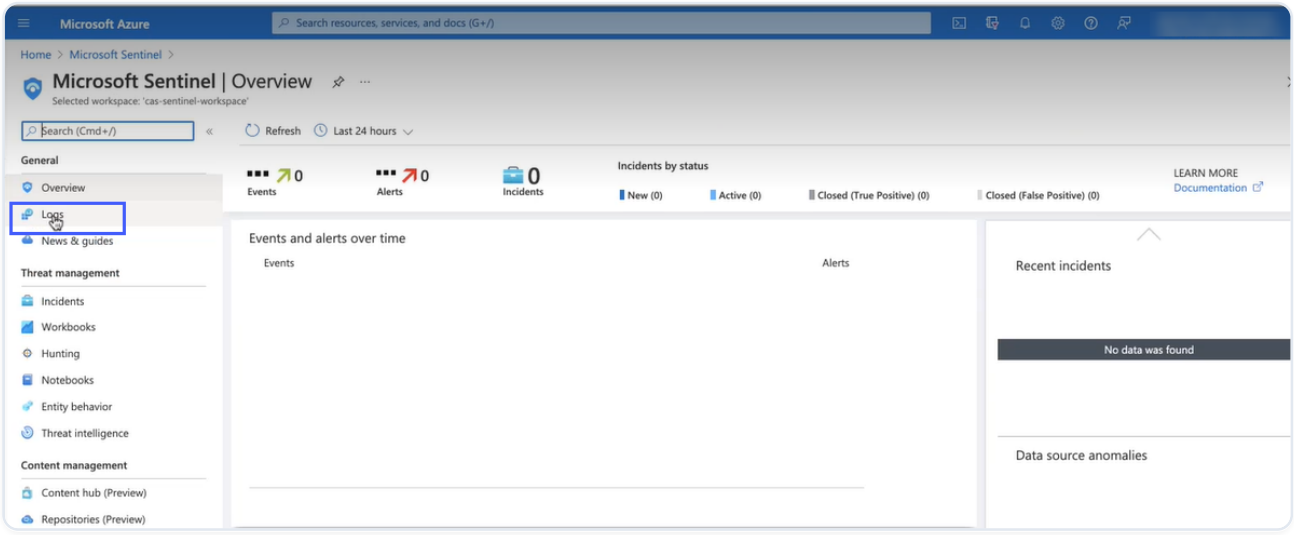
Prerequisite

To use the Citrix Analytics workbook, ensure that you have already integrated Microsoft Sentinel with Citrix Analytics for Security. For more information, see Microsoft Sentinel integration.

View the Citrix Analytics events

After integrating Citrix Analytics for Security™ with Microsoft Sentinel, the Logstash connector starts pushing events from Citrix Analytics for Security to the Microsoft Sentinel workspace. On your **Azure portal**, open the Microsoft Sentinel workspace that you have used for the integration.

To verify that Microsoft Sentinel is receiving the events from Citrix Analytics for Security, select **Logs > Custom Logs**.

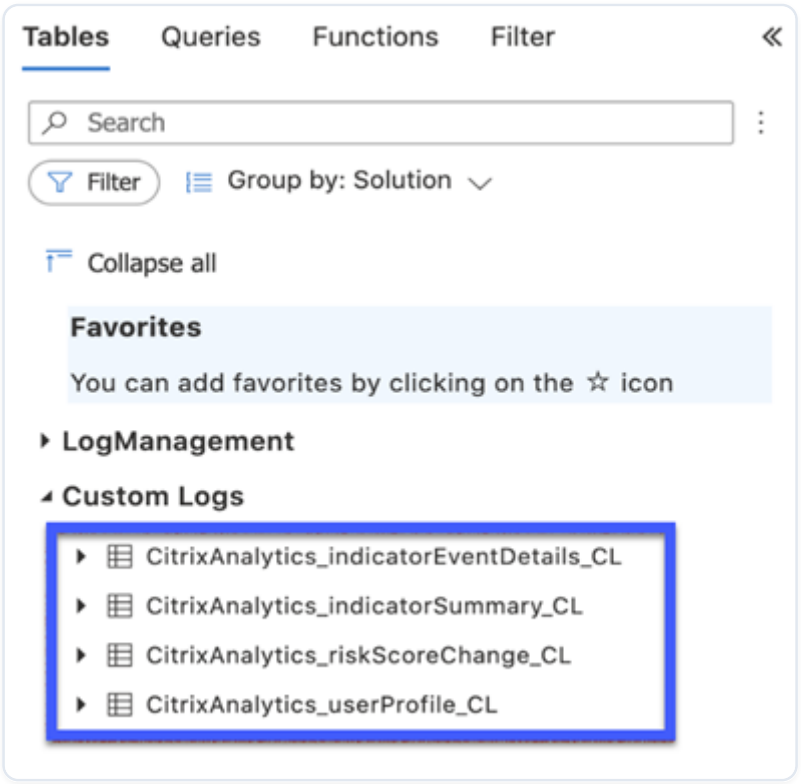


In the **Custom Logs** section, you can view the log tables that are created automatically to store the events received from Citrix Analytics for Security. These log tables serve as the source for the dashboards on the Citrix Analytics workbook.

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

NOTE

The events sent from Citrix Analytics for Security might take a few hours to appear in the Microsoft Sentinel workspace. So, you might see a delay in the creation of the log tables for the events.

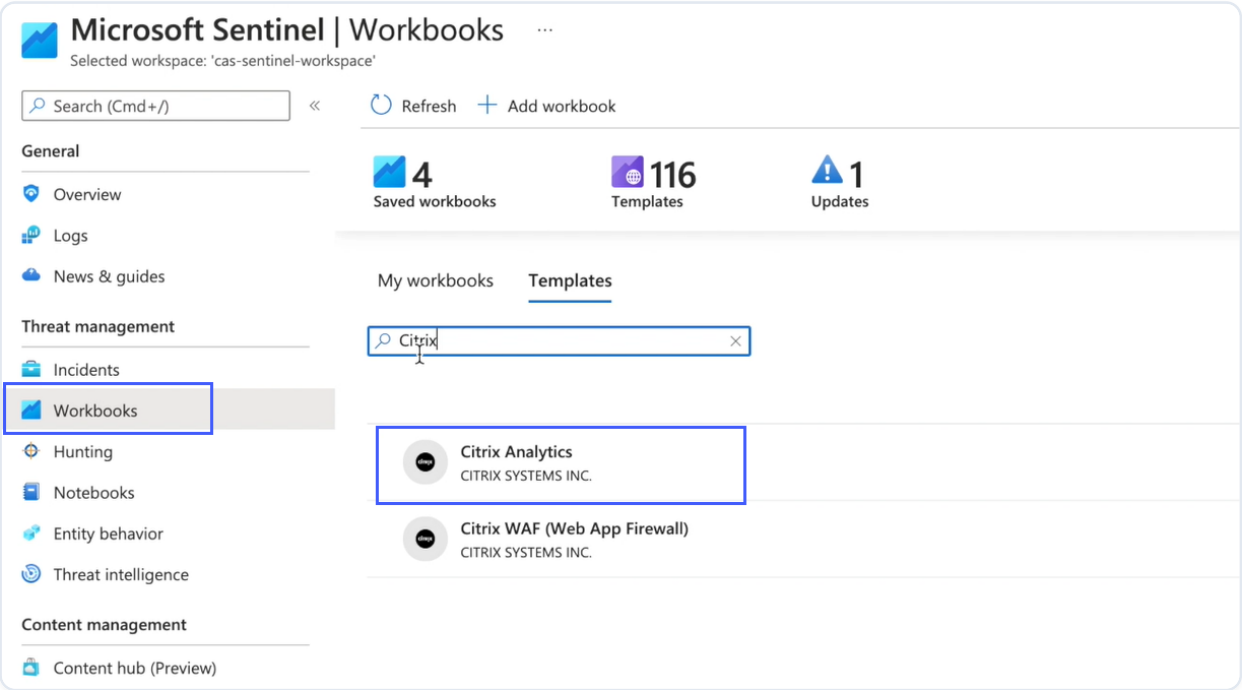


View the Citrix Analytics workbook

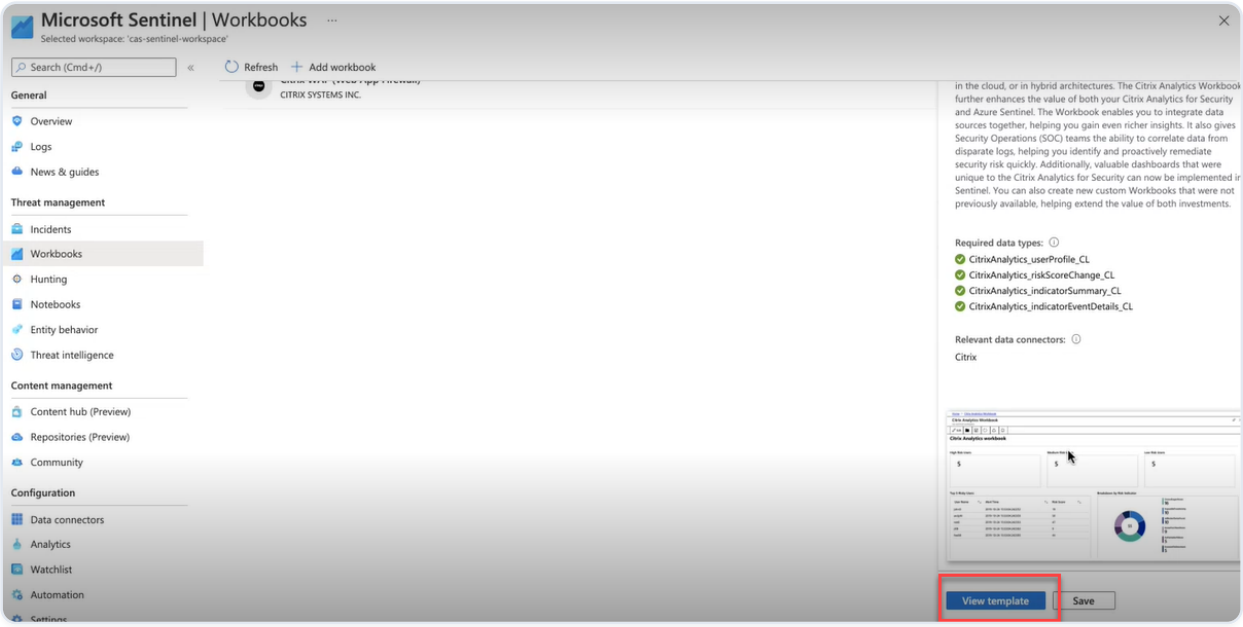
When the log tables are successfully created, do the following:

1. Select **Workbooks** and search **Citrix Analytics**. Select **Citrix Analytics**.

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



2. Select **View Template** to open the Citrix Analytics workbook.

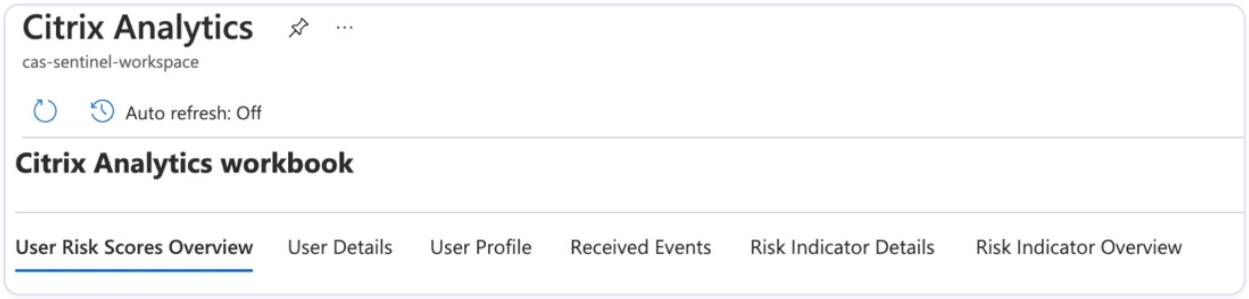


In the Citrix Analytics workbook, you can view the user events in the following dashboards:

- **User Risk Scores Overview**: Provides a consolidated view of the risky users in your organization.
- **User Details**: Provides details of the users and their risky behavior.
- **User Profile**: Provides the event metrics associated with the users.
- **Received Events**: Provides the events received from Citrix Analytics for Security.
- **Risk Indicator Details**: Provides details about the built-in and custom risk indicators triggered by the users.

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

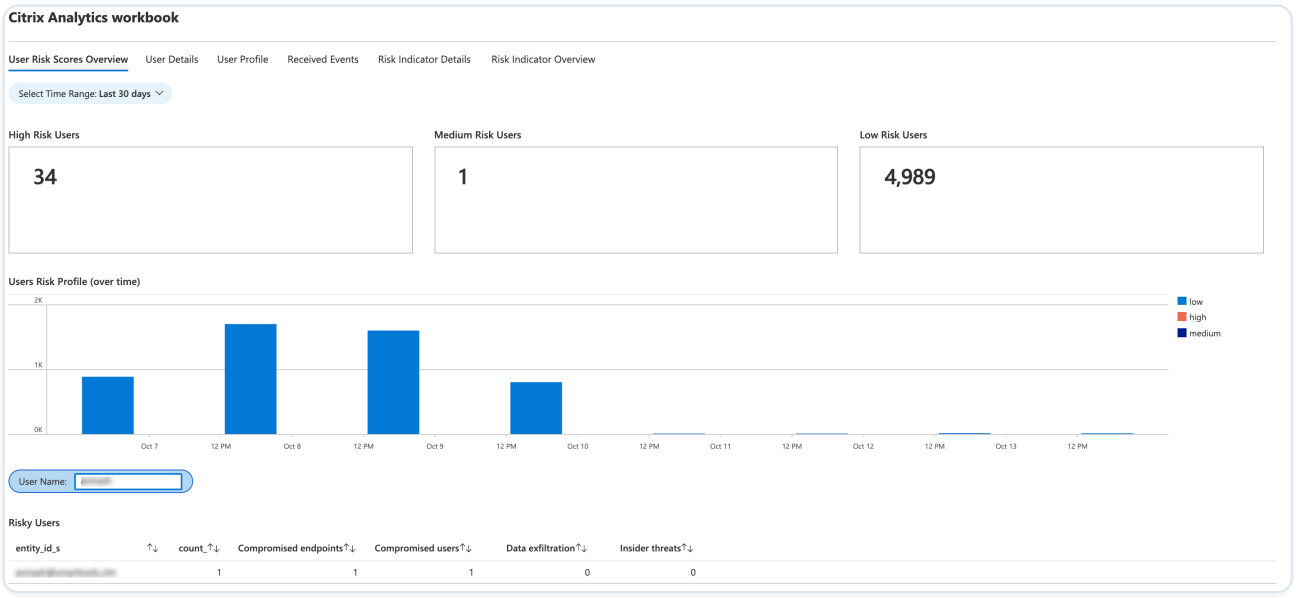
- **Risk Indicator Overview**: Provides a consolidated view of the risk indicators triggered by the users.



User risk score overview

This dashboard provides a consolidated view of the risky users in your organization. The users are categorized by the risk levels- high, medium, and low. The risk levels are based on the anomalies in the user activities and accordingly a risk score is assigned. For more information about the types of risky users, see the Users dashboard.

Select a time period to view the risky users in your organization.

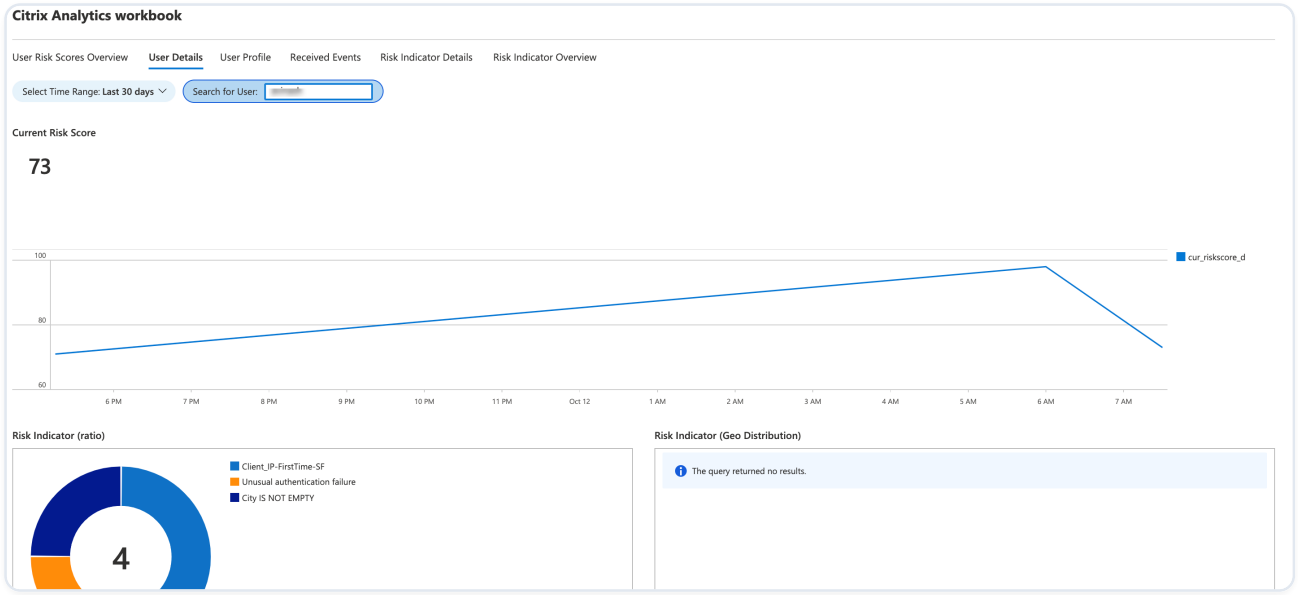


User details

This dashboard provides the risk score and the risk indicators associated with a user.

Search a user and view their risky activities that can pose a threat to your organization. To mitigate the threat, you can take appropriate actions on the user accounts based on their risk severity.

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



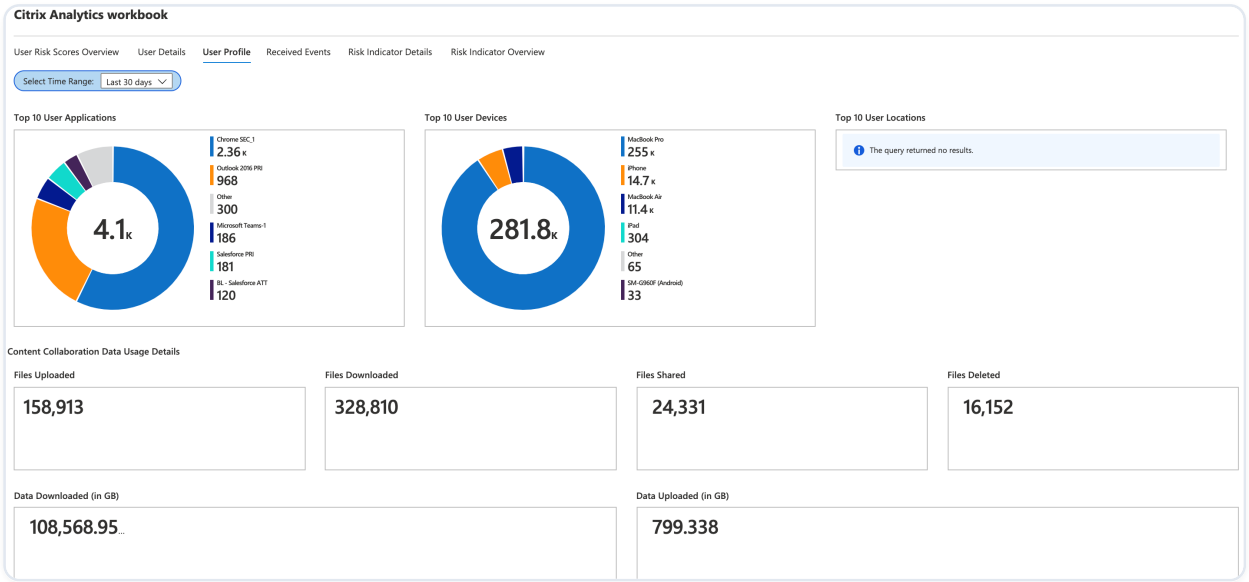
User profile

This dashboard provides the details of the event metrics associated with your users for a selected time period. The metrics provide insights into the user activities such as:

- Top 10 applications used by the users
- Top 10 devices used by the users
- Top 10 locations from where the users have logged on

Using the reports, you can:

- Identify the usage trend of your users
- Discover the non-compliant devices that are used to access the resources
- Check for any potential risky accesses from your users



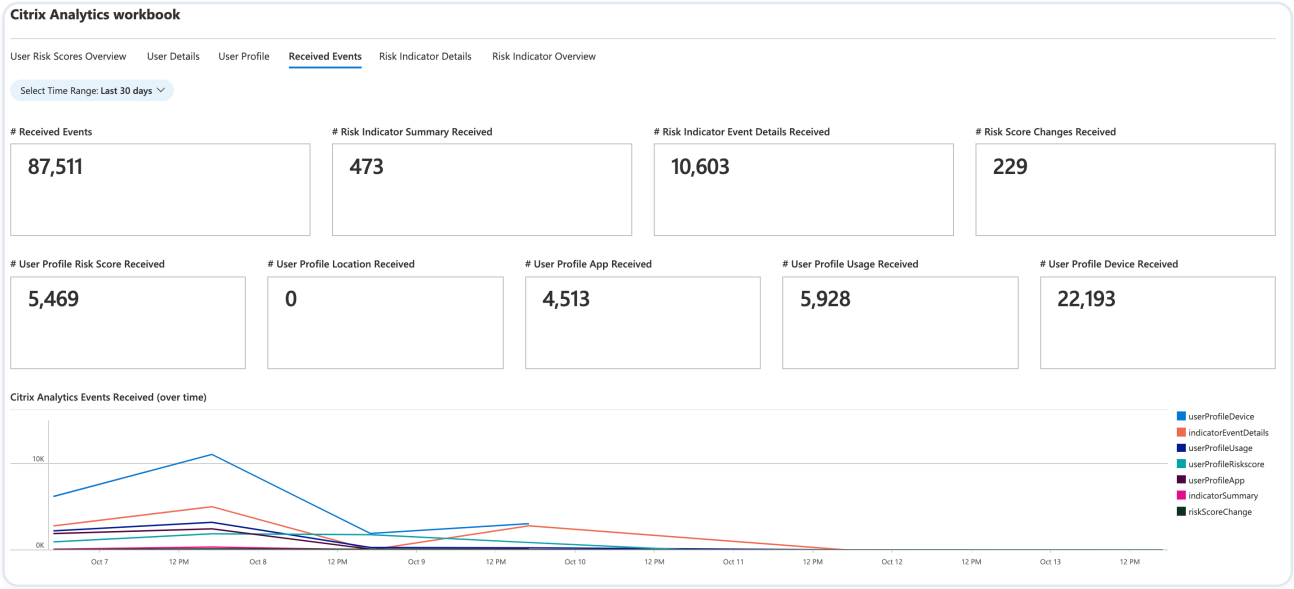
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Received events

For a selected time period, you can view the total number of events received from Citrix Analytics for Security. The total received events include the following:

- Risk indicator summary: Indicates the events associated with the user risk indicators' summary. For information on various risk indicator summary events, see Risk indicator schema.
- Risk indicator event details: Indicates the events associated with user risk indicators' details. For information on various risk indicator detail events, see Risk indicator schema.
- User profile risk score: Indicates the events associated with users' risk score. For information, see Users dashboard.
- Risk score changes: Indicates the events associated with users' risk score change. For information, see Users dashboard.
- User profile locations: Indicates the events associated with the locations from where the users have logged on.
- User profile app: Indicates the events associated with the applications used by the users.
- User profile usage: Indicates the events associated with the data usage of the users.
- User profile device: Indicates the events associated with the devices used by the users.

By reviewing the dashboard at regular intervals, you can ensure if events are properly flowing to your Microsoft Sentinel workspace. Any discrepancy in the total received events might indicate integration issues with Citrix Analytics for Security. You can perform the necessary steps to debug the issues.



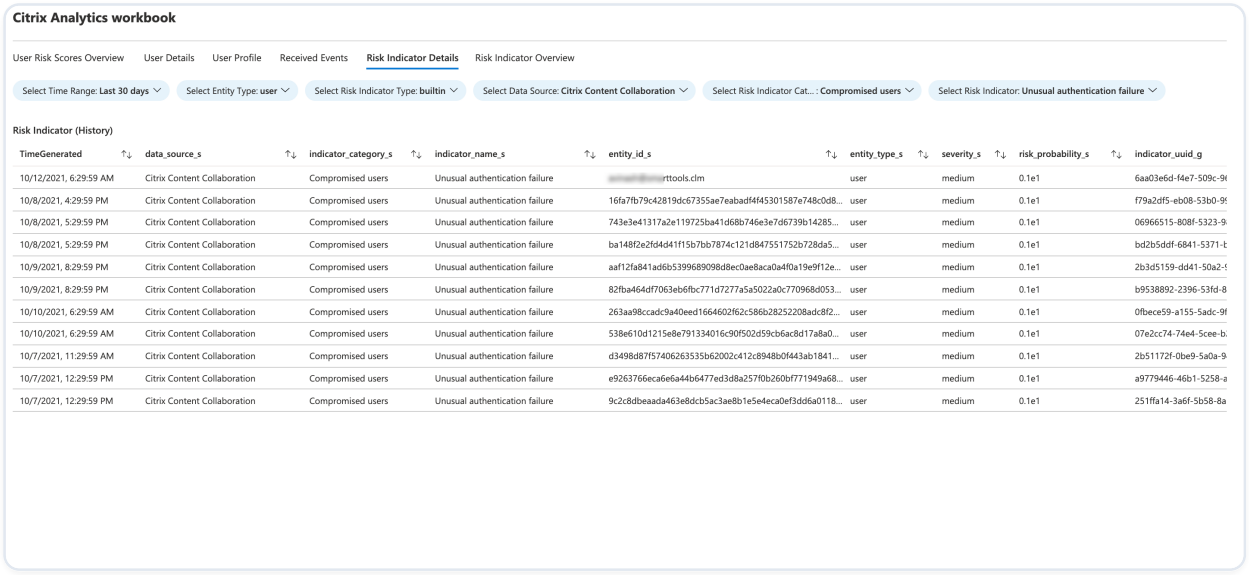
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Risk indicator details

This dashboard provides the details of the risk indicators triggered by your users.

You can view the risk indicator details by selecting one or more categories:

- Time range: Select a time range to view the details of the risk indicators triggered during the period.
- Entity type: Select a user to view the details of the associated risk indicators.
- Risk indicator type: Select either built-in or custom risk indicators to view their details.
- Data source: Select a data source to view the associated risk indicators.
- Risk indicator category: Select the risk category to view the associated risk indicators.
- Risk indicator: Select a risk indicator by name and view its details.



Risk indicator overview

This dashboard provides a consolidated view of all the risk indicators triggered by your users.

You can view the risk indicators by selecting one or more categories:

- Time range: Select a time period to view the risk indicators that are triggered during that period.
- Risk indicator type: Select either built-in or custom to view the associated risk indicators.
- Entity type: Select either user to view the associated risk indicators.

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



Troubleshooting guidance for Sentinel Integration via Logstash

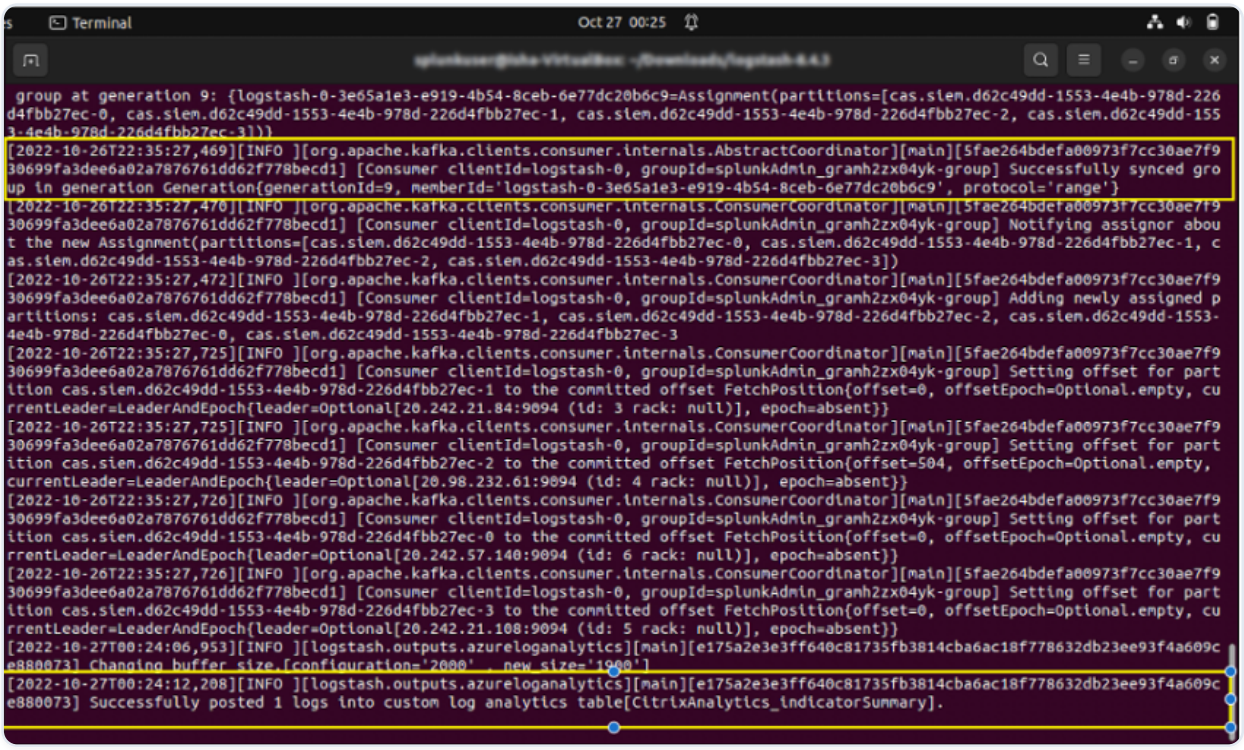
This article lists out pointers to spot in order to resolve an issue that you might encounter when you integrate Microsoft Sentinel with Citrix Analytics using Logstash. To know more about the same, refer SIEM integration using Kafka or Logstash based data connector.

Check Logstash Server Logs

You can check the Logstash server logs appearing on your terminal window to verify whether data has been correctly ingested into the custom log tables in your Sentinel workspace.

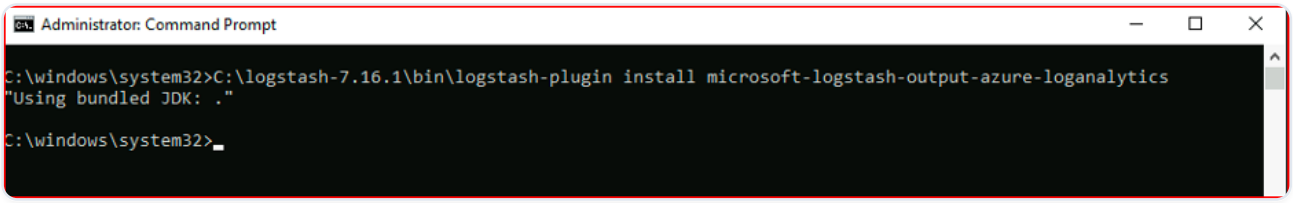
1. To view the log details, you must download the Logstash configuration file from **Settings > Data Exports > Configuration** tab **>** expand the **SIEM Environment**. Under the **Azure Sentinel (Preview)**, click **Download Logstash Config File**.
2. Once you start the Logstash server using the configuration file, you can look out for the following logs in the same terminal window that indicate a successful connection with Log Analytics workspace hosted by Microsoft Azure.

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

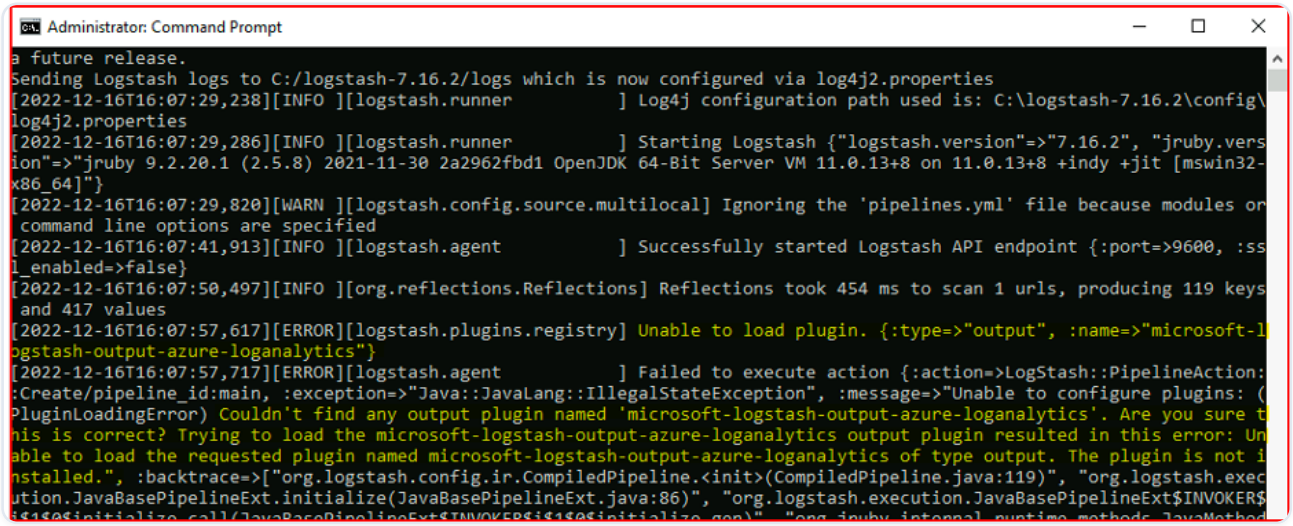


Common Error: Using bundled JDK

When trying to install the Microsoft log analytics plug-in, a common error reported is the one shown below:



After this, upon trying to run Logstash server, you might see the following error:



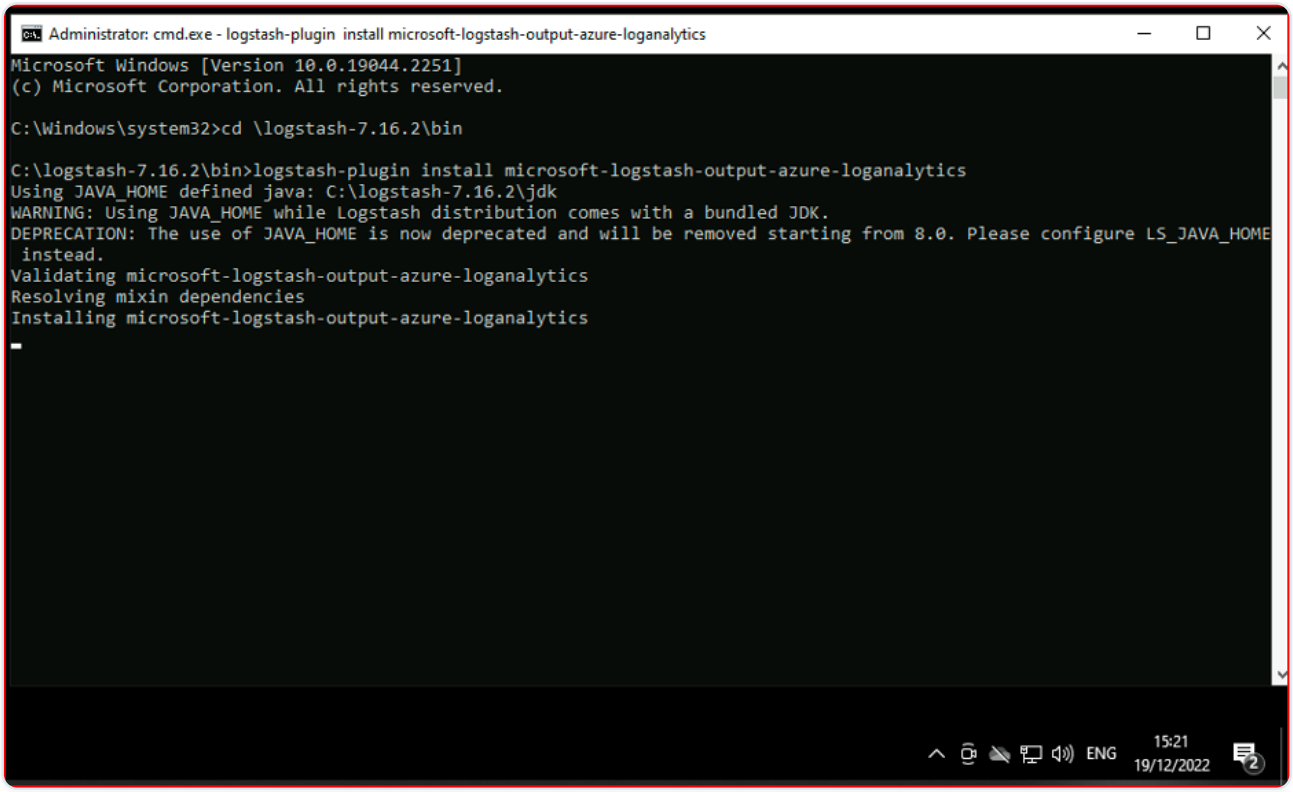
To resolve this, set JAVA_HOME to the bundled JDK:

1. Go to Windows Environment Variables

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

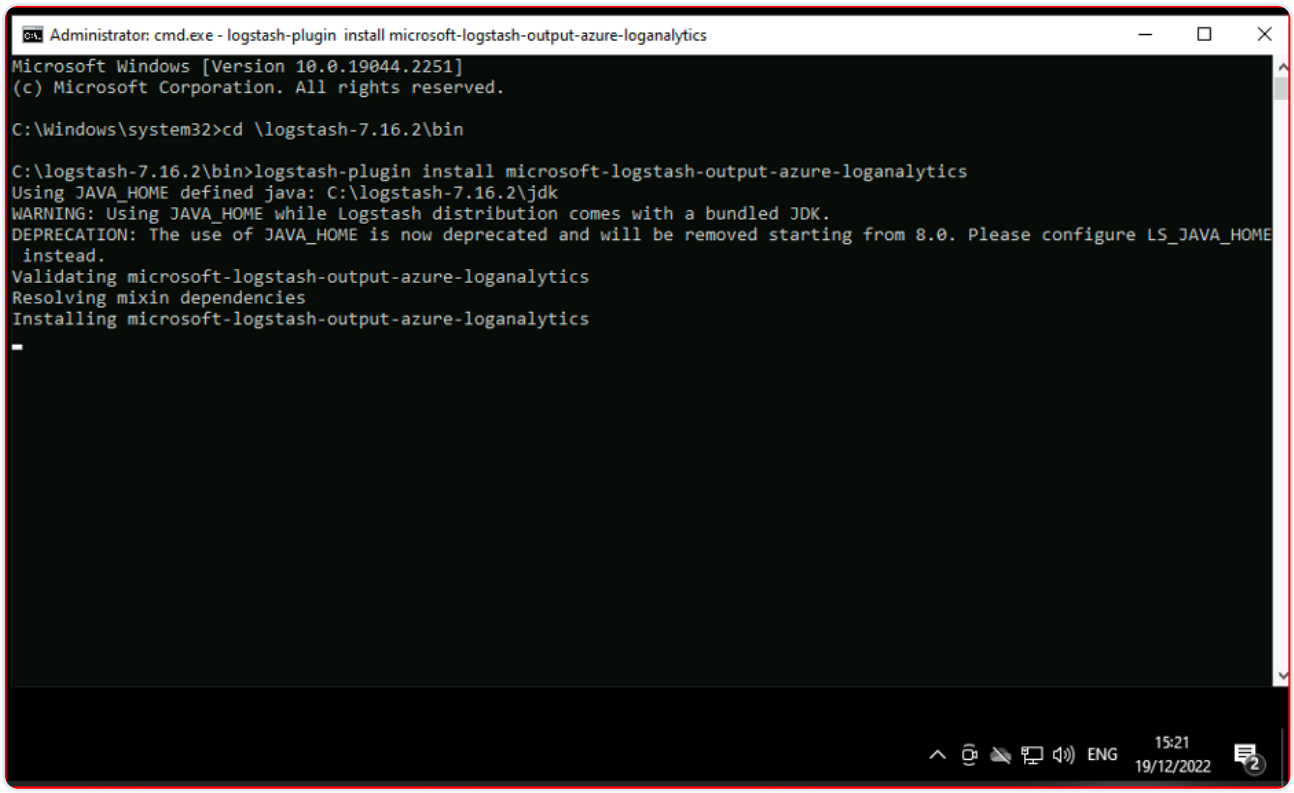
2. Create a new system variable with the name “JAVA_HOME”
3. Add the path to the bundled Logstash JDK (< path_to_logstash >/logstash-X.X.X/jdk)

After going through the above steps, upon trying to install the plug-in again, the following screen appears:

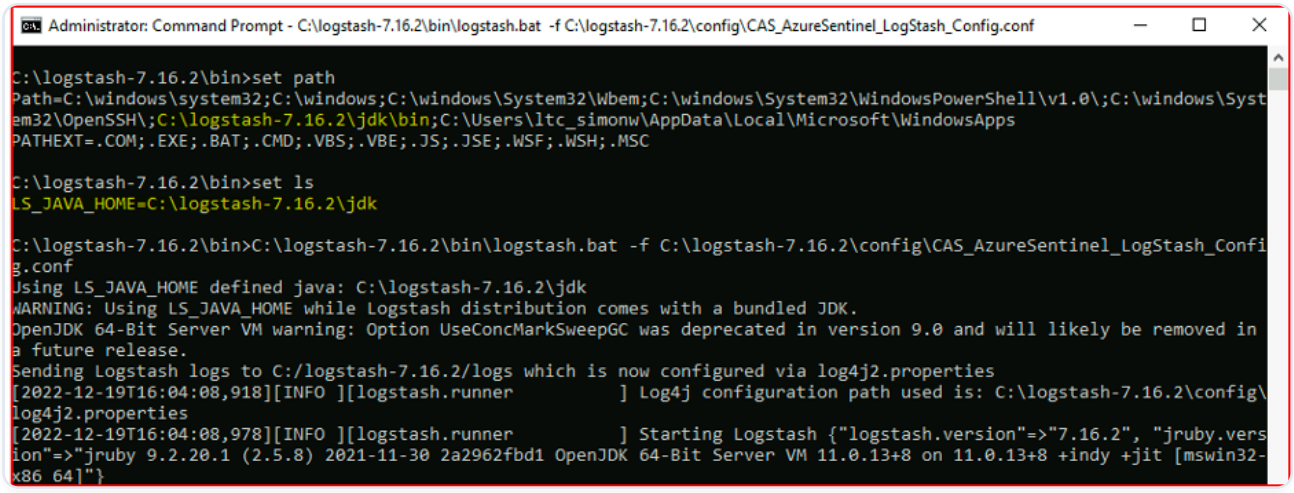


If you use LS_JAVA_HOME (as JAVA_HOME is deprecated), you also have to specify the location of the bundled JDK in the system PATH variable, and this path must point to the **jdk\bin** folder (unlike the LS_JAVA_HOME variable) :

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



If you use LS_JAVA_HOME (as JAVA_HOME is deprecated), you also have to specify the location of the bundled JDK in the system PATH variable, and this path must point to the **jdk\bin** folder (unlike the LS_JAVA_HOME variable):

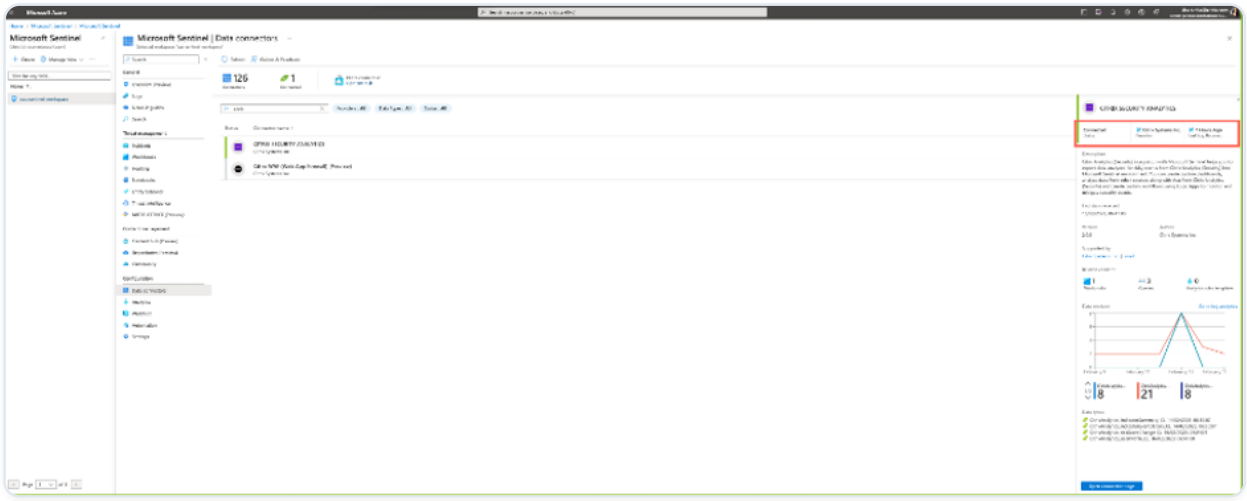


Check Microsoft Sentinel Workbook

To confirm whether data sent by Citrix Analytics has been successfully entered into the appropriate custom log table in the Log Analytics Workspace (To know more about Microsoft Sentinel integration with Citrix Analytics, refer Microsoft Sentinel integration):

1. Navigate to **Azure portal > Microsoft Sentinel > Select appropriate_workspace > Data connectors >** select and click **Citrix Security Analytics**.
2. Check the top bar to verify the connectivity status.

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



3. Under the Workbooks, you can use intuitive filters to further drill-down on the data to get the risk indicator information. To get the information, navigate to **Azure portal > Microsoft Sentinel > Data connectors > CITRIX SECURITY ANALYTICS > Workbooks**.

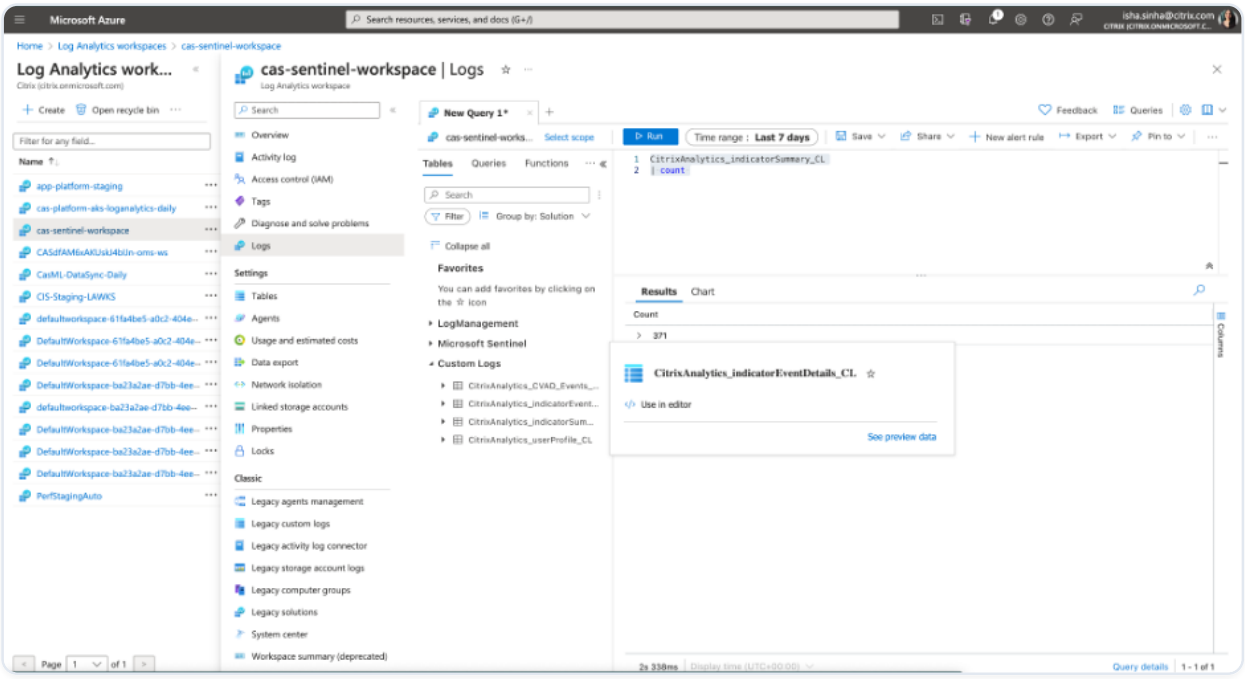


Check Log Analytics workspace logs using KQL

You can also check if the correct data made its way to your LogAnalytics workspace by running KQL queries on the respective custom log tables.

1. Navigate to **Azure portal > Log Analytics workspaces** and search for the correct workspace.
2. Under the left panel, select **Logs** and search for the custom log analytics table under the **Tables** tab.
3. Select the custom log analytics table and click **Use in editor**. (For guidance on KQL queries on Log Analytics workspace, refer Log Analytics tutorial).
4. Click **Run**.

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



Elasticsearch integration

NOTE

Contact mailto:CAS-PM-Ext@cloud.com to request assistance for the Elasticsearch integration, exporting data to Elasticsearch, or provide feedback.

Integrate Citrix Analytics for Security with Elasticsearch by using the Logstash engine. This integration enables you to export and correlate the users' data from your Citrix IT environment to Elasticsearch and get deeper insights into your organization's security posture. You can also use Elasticsearch with the visualization services and SIEMs like Kibana and LogRhythm respectively.

For more information about the benefits of the integration and the type of processed data that is sent to your SIEM, see Security Information and Event Management integration.

Prerequisites

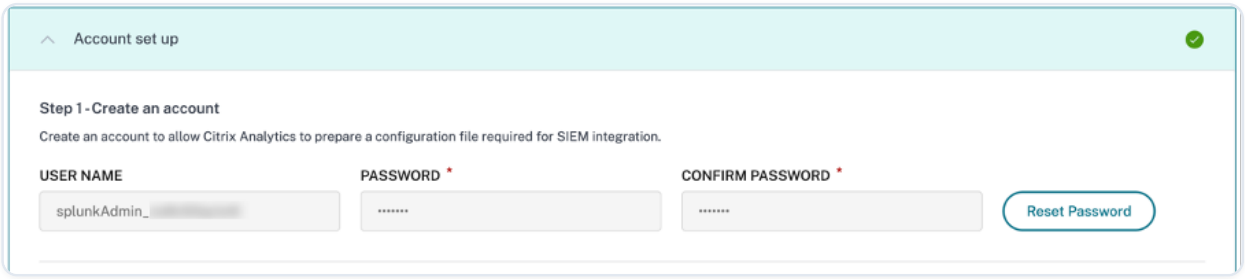
- Turn on data processing for at least one data source. It helps Citrix Analytics for Security™ to begin the Elasticsearch integration process.
- Ensure that the following endpoint is in the allow list in your network.

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

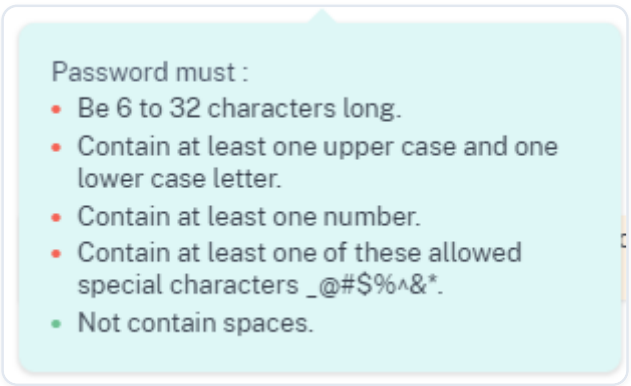
ENDPOINT	UNITED STATES REGION	EUROPEAN UNION REGION	ASIA PACIFIC SOUTH REGION
Kafka brokers	`casnb-0.citrix.com:9094`	`casnb-eu-0.citrix.com:9094`	`casnb-aps-0.citrix.com:9094`
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`	`casnb-aps-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`		

Integrate with Elasticsearch

1. Go to **Settings > Data Exports**.
2. On the **Account set up** section, create an account by specifying the user name and a password. This account is used to prepare a configuration file, which is required for integration.

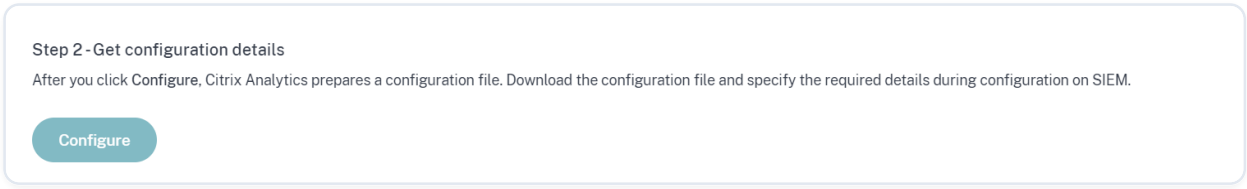


3. Ensure that the password meets the following conditions:



4. Click **Configure** to generate the Logstash configuration file.

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

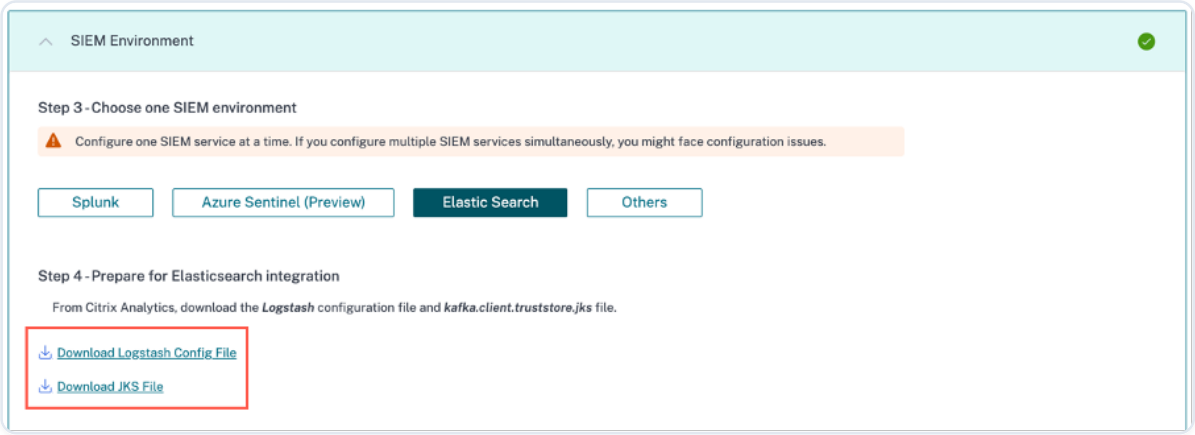


5. Select the **Elastic Search** tab from the SIEM Environment section to download the configuration files:

   - **Logstash config file**: Contains the configuration data (input, filter, and output sections) for sending events from Citrix Analytics for Security to Elasticsearch using the Logstash data collection engine. For information on Logstash config file structure, see the Logstash documentation.
   - **JKS file**: Contains the certificates required for SSL connection.

   NOTE

   These files contain sensitive information. Keep them in a safe and secure location.

6. Configure Logstash:

   a. On your Linux or Windows host machine, install Logstash. You can also use your existing Logstash instance.

   b. On the host machine where you have installed Logstash, place the following files in the specified directory:

HOST MACHINE TYPE	FILE NAME	DIRECTORY PATH
Linux	CAS_Elasticsearch_LogStash_Config.config	For Debian and RPM packages: `/etc/logstash/conf.d/`

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

HOST MACHINE TYPE	FILE NAME	DIRECTORY PATH
		For .zip and .tar.gz archives: `{extract.path}/config`
	kafka.client.truststore.jks	For Debian and RPM packages: `/etc/logstash/ssl/`
		For .zip and .tar.gz archives: `{extract.path}/ssl`
Windows	CAS_Elasticsearch_LogStash_Config.config	`C:\logstash-7.xx.x\config`
	kafka.client.truststore.jks	

For information on the default directory structure of Logstash installation packages, see Logstash documentation.

c. Open the Logstash config file and do the following:

   i. In the input section of the file, enter the following information:

   - **Password**: The password of the account that you have created in Citrix Analytics for Security to prepare the configuration file.
   - **SSL truststore location**: The location of your SSL client certificate. This is the location of the kafka.client.truststore.jks file in your host machine.

```
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. In the output section of the file, enter the address of your host machine or the cluster where Elasticsearch is running.

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

```
}
output {
  elasticsearch {
    hosts => ["<your logstash host : port>"]
    index => "citrixanalytics-%{+YYYY.MM.dd}"
  }
}
```

d. Restart your host machine to send processed data from Citrix Analytics for Security to Elasticsearch.

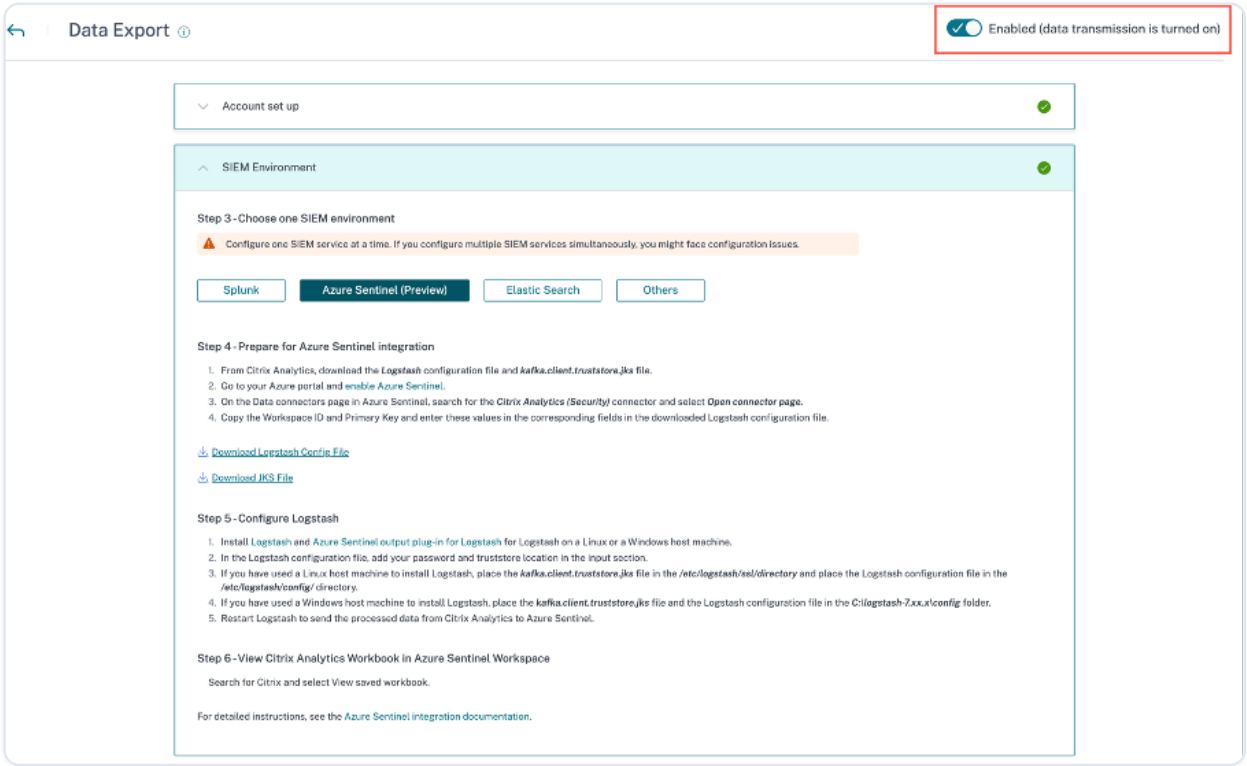
After configuration is complete, verify that you can view the Citrix Analytics data in your Elasticsearch.

Turn on or off data transmission

After Citrix Analytics for Security prepares the configuration file, data transmission is turned on for Elasticsearch.

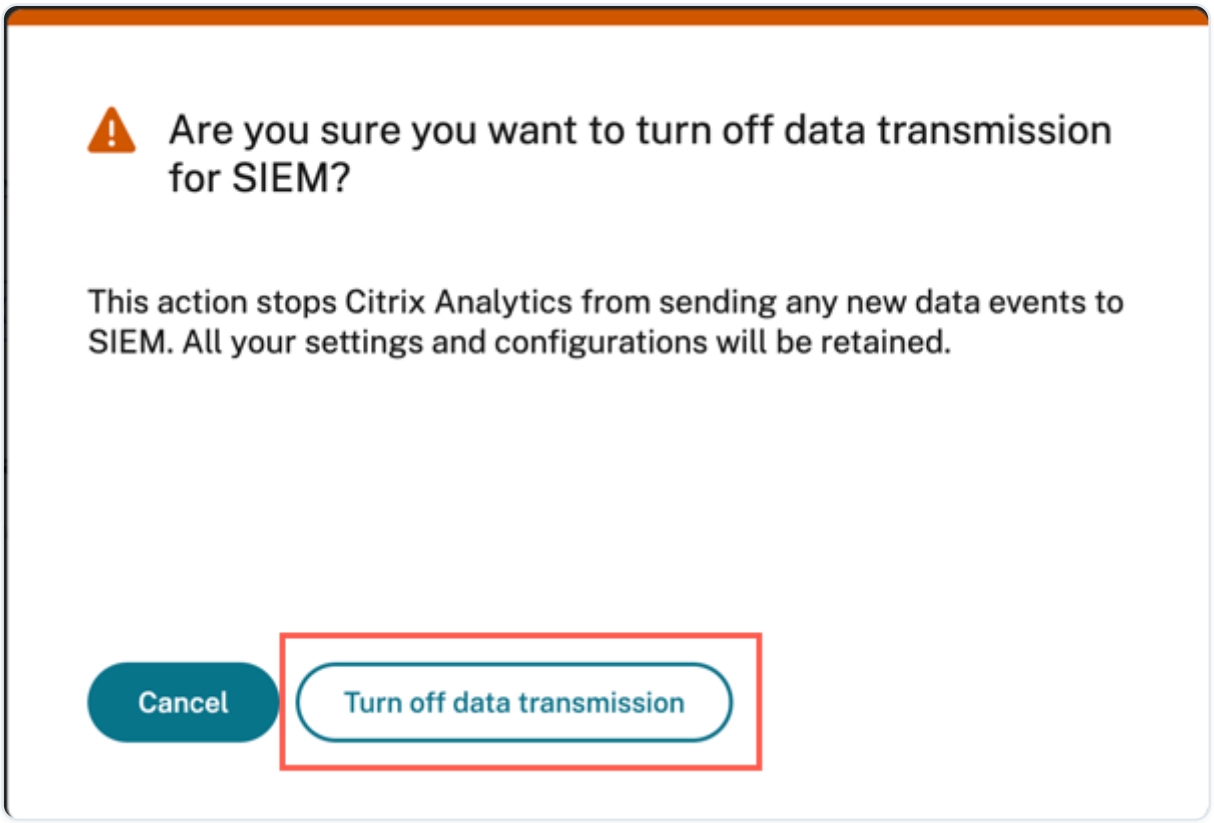
To stop transmitting data from Citrix Analytics for Security:

1. Go to **Settings > Data Exports**.
2. Turn off the toggle button to disable the data transmission. By default the **data transmission** always enabled..



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

A warning window appears for your confirmation. Click **Turn off data transmission** button to stop the transmission activity.



To enable data transmission again, turn on the toggle button.

SIEM integration using Kafka or Logstash based data connector

Citrix Analytics for Security™ SIEM integration enables you to export and correlate the users' data from the Citrix Analytics to your SIEM environment and get deeper insights into your organization's security posture.

For more information about the benefits of the integration and the type of data events (risk insights and data source events) that is sent to your SIEM, see Security Information and Event Management integration.

You can integrate Citrix Analytics for Security with your SIEM solutions through the following two mechanisms (supported by your SIEM and IT deployment):

1. Connect via Kafka endpoints
2. Connect via Logstash data broker with Kafka-based ingestion

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

Prerequisites

- Turn on data processing for at least one data source. It helps Citrix Analytics for Security to begin the integration with your SIEM tool.
- Ensure that the following endpoint is in the allow list in your network.

ENDPOINT	UNITED STATES REGION	EUROPEAN UNION REGION	ASIA PACIFIC SOUTH REGION
Kafka brokers	`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`		

Integrate with a SIEM service using Kafka

Kafka is an open source software and used for real-time streaming of data. Using Kafka, you can analyze the real-time data to gain faster insights. Mostly, the large organizations who handle adequate data, use Kafka.

Northbound Kafka is an internal middle layer enabling Citrix Analytics to share real-time data feeds with the SIEM customers through Kafka endpoints. If your SIEM supports Kafka endpoints, use the parameters provided in the Logstash config file and the certificate details in the JKS file or the PEM file to integrate your SIEM with Citrix Analytics for Security.

The following parameters are required to integrate using Kafka:

ATTRIBUTE NAME	DESCRIPTION	CONFIGURATION DATA SAMPLE
User name	User name provided by Kafka.	`'sasl.username': cas_siem_user_name,`

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

ATTRIBUTE NAME	DESCRIPTION	CONFIGURATION DATA SAMPLE
Host	Host name of the Kafka server to which you want to connect.	`'bootstrap.servers': cas_siem_host,`
Topic name/Client ID	Client ID assigned to each tenant.	`'client.id': cas_siem_topic,`
Group name/ID	Group name that you need to read the messages shared by the consumers.	`'group.id': cas_siem_group_id,`
Security protocol	Name of the security protocol.	`'security.protocol': 'SASL_SSL',`
SASL mechanisms	Authentication mechanism that is typically used for encryption to implement secure authentication.	`'sasl.mechanisms': 'SCRAM-SHA-256',`
SSL truststore location	Location where you can store the certificate file. The client truststore password is optional and is expected to be left empty.	`'ssl.ca.location': ca_location`
Session timeout	The session timeout used to detect client failures while using Kafka.	`'session.timeout.ms': 60000,`
Auto offset reset	Defines the behavior while consuming data from a topic partition when there is no initial offset. You can set the values such as, latest, earliest, or none.	`'auto.offset.reset': 'earliest',`

The following is a sample configuration output:

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

```
{'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',

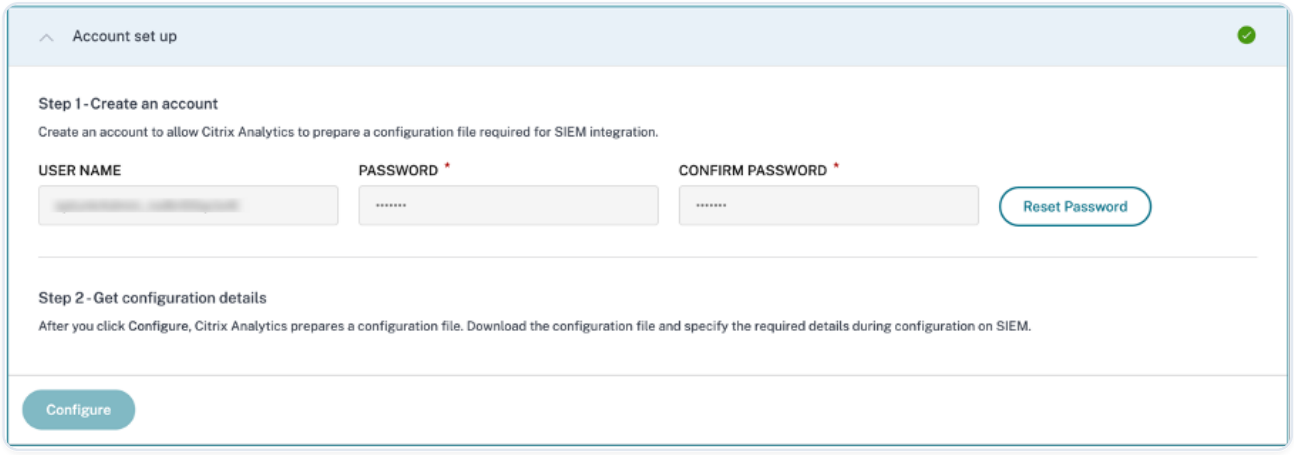
                    'sasl.mechanisms': 'SCRAM-SHA-256',

                    'sasl.username': cas_siem_user_name,

                    'sasl.password': self.CLEAR_PASSWORD,

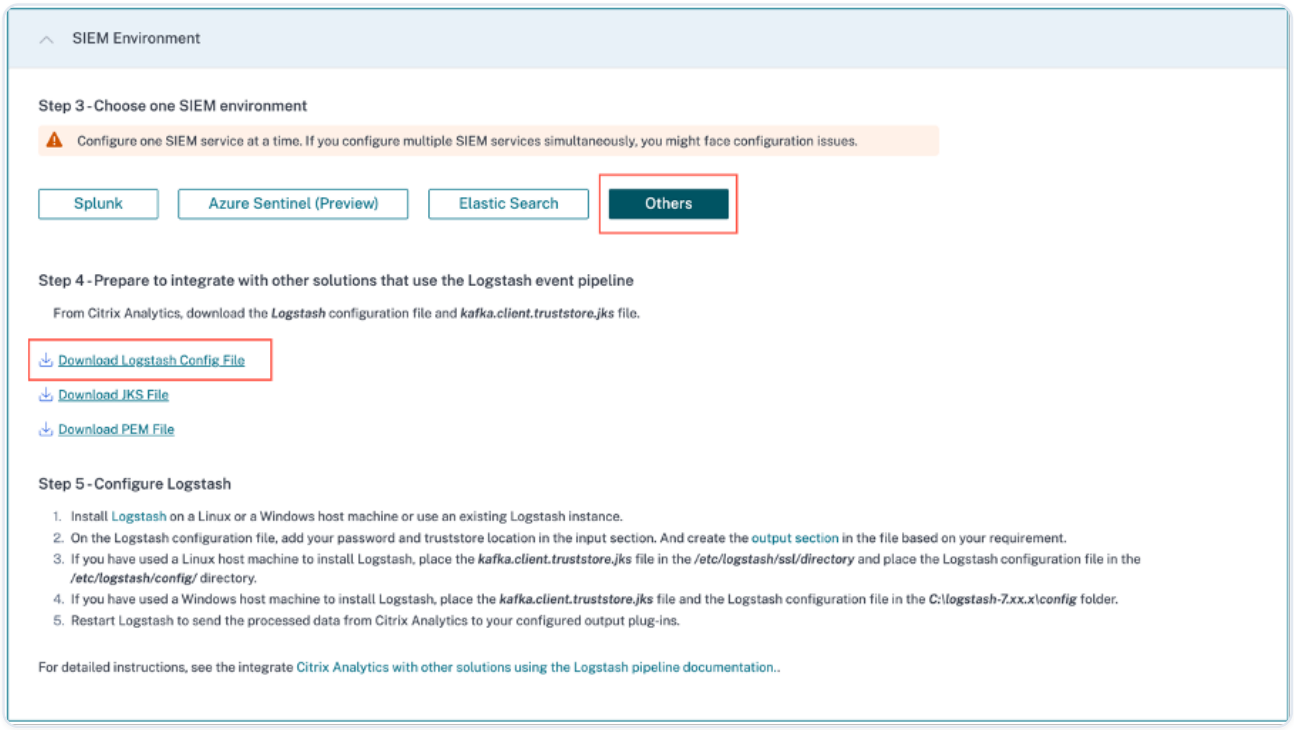
                    'ssl.ca.location': ca_location

            }
```



The aforementioned parameters are available in the Logstash configuration file. To download the configuration file, navigate to **Settings > Data Exports > SIEM Environment >** select **Others** tab > click **Download Logstash Config File**.

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



To understand/know more about the configuration values, refer Configuration.

Data flow

The authentication data communication happens between the Kafka server side Brokers (Citrix Analytics for Security cloud) and Kafka clients. All brokers/external clients' communication uses the enabled SASL_SSL security protocol and target 9094 port for public access.

Apache Kafka has a security component to encrypt the data in flight using SSL encryption. The data transmission over the network is encrypted and secured when encryption is enabled and SSL certificates are set. Only the first and the final machine possess the ability to decrypt the packets being sent through SSL.

Authentications

There are two levels of authentication available as below:

1. TLS/between client and server.
    - The server certificates (public keys) for TLS authentication exchange between client and server.
    - The client-based authentication or two way authentications are not supported (where client private key certificates is required).
2. Username/password for access control to TOPICS/endpoints
    - Ensures that specific client can read only from specific customer topic

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

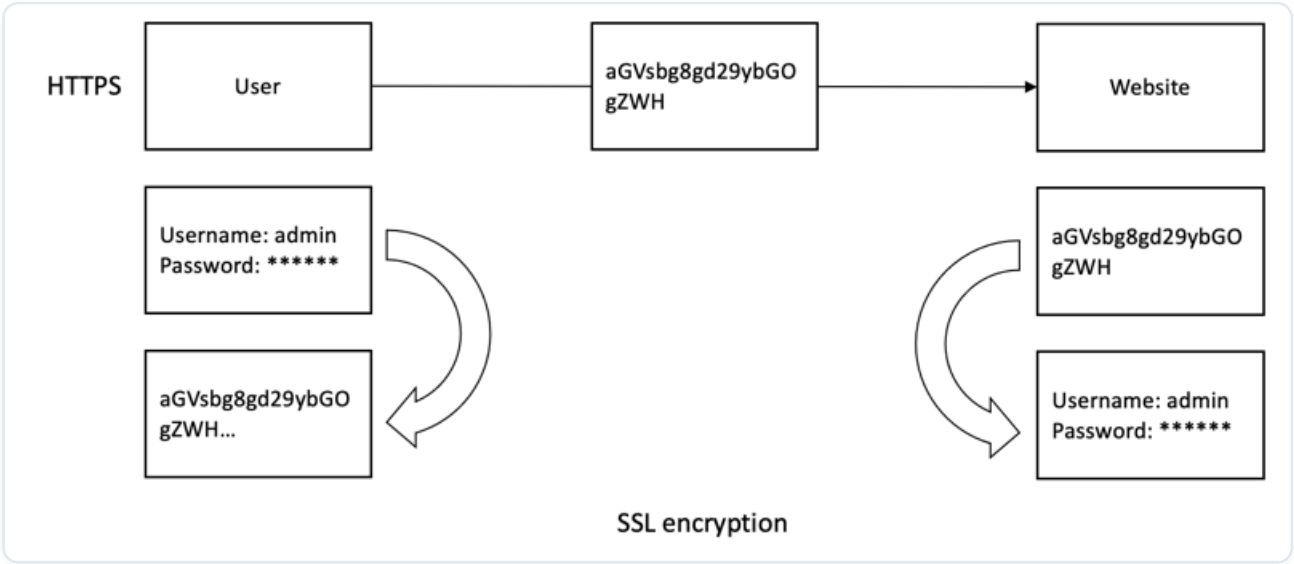
- SASL/SCRAM is used for username/password authentication mechanism along with TLS encryption to implement secure authentication.

Encryption with SSL and Authentication with SASL/SSL&SASL/PLAINTEXT

By default, Apache Kafka communicates in PLAINTEXT, where all data is sent in the clear and any of the routers can read the data content. Apache Kafka has a security component to encrypt the data in flight using SSL encryption. With encryption enabled and carefully setup SSL certificates, the data is now encrypted and securely transmitted over the network. With SSL encryption, only the first and the final machine possesses the ability to decrypt the packet being sent.

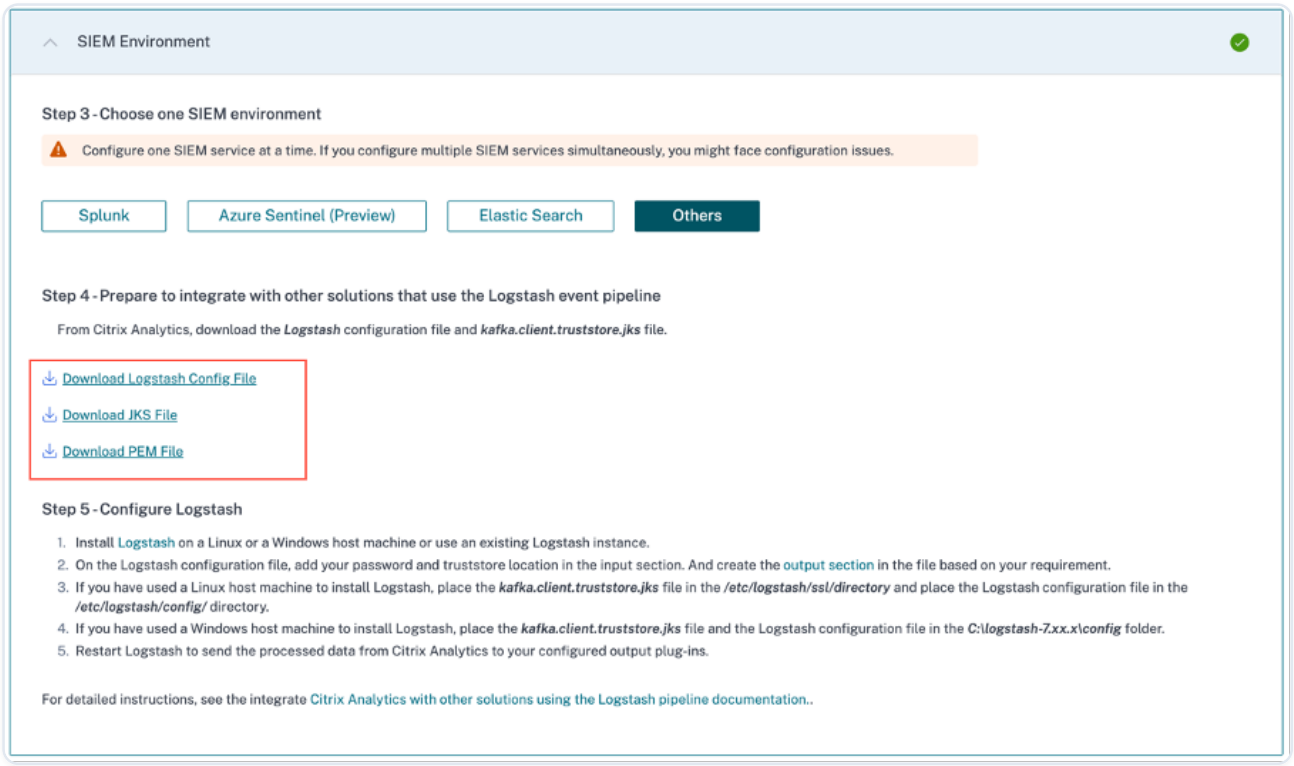
Since the two-way SSL encryption is used, user name/password login is safe for external communications.

The encryption is only in-flight and the data still sits unencrypted on broker’s disk.



In the client configuration, the client truststore JKS file and PEM file (converted from truststore jks file) are required. You can download these files from Citrix Analytics for Security GUI as shown in the following screenshot:

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



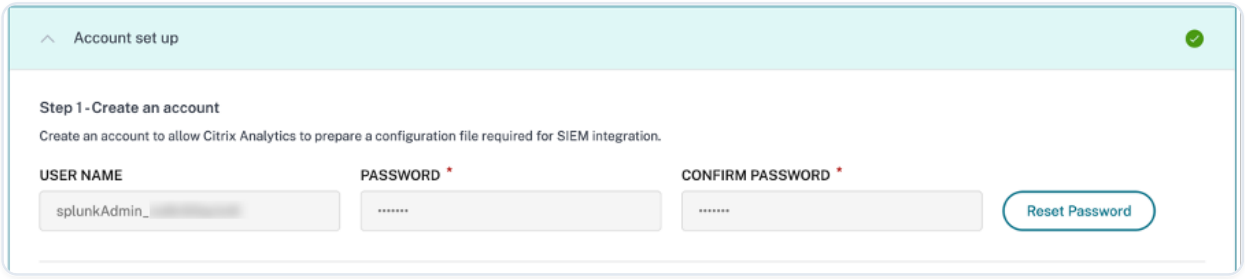
SIEM integration using Logstash

If your SIEM does not support Kafka endpoints, then you can use the **Logstash data** collection engine. You can send the data events from Citrix Analytics for Security to one of the output plug-ins that are supported by Logstash.

The following section describes the steps that you must follow to integrate your SIEM with Citrix Analytics for Security by using Logstash.

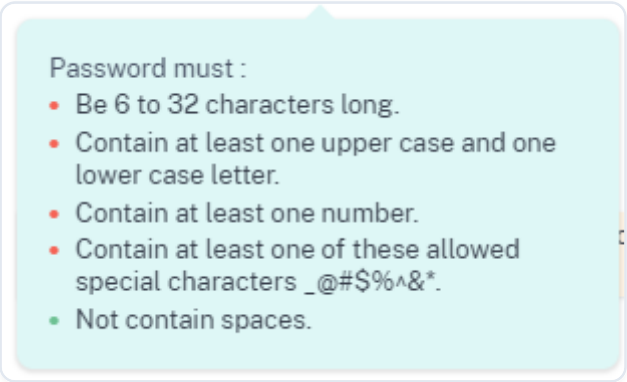
Integrate with a SIEM service using Logstash

1. Go to **Settings > Data Exports**.
2. On the **Account set up** page, create an account by specifying the user name and a password. This account is used to prepare a configuration file, which is required for integration.

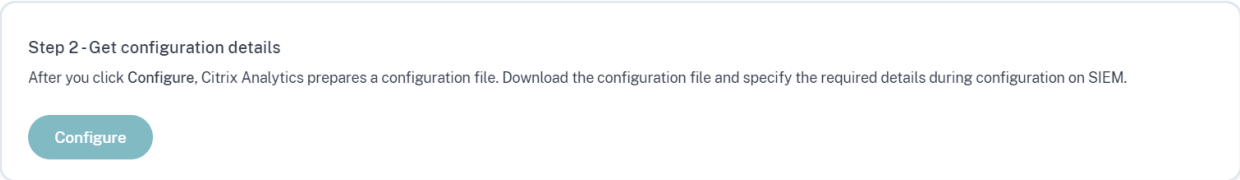


3. Ensure that the password meets the following conditions:

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



4. Select **Configure** to generate the Logstash configuration file.

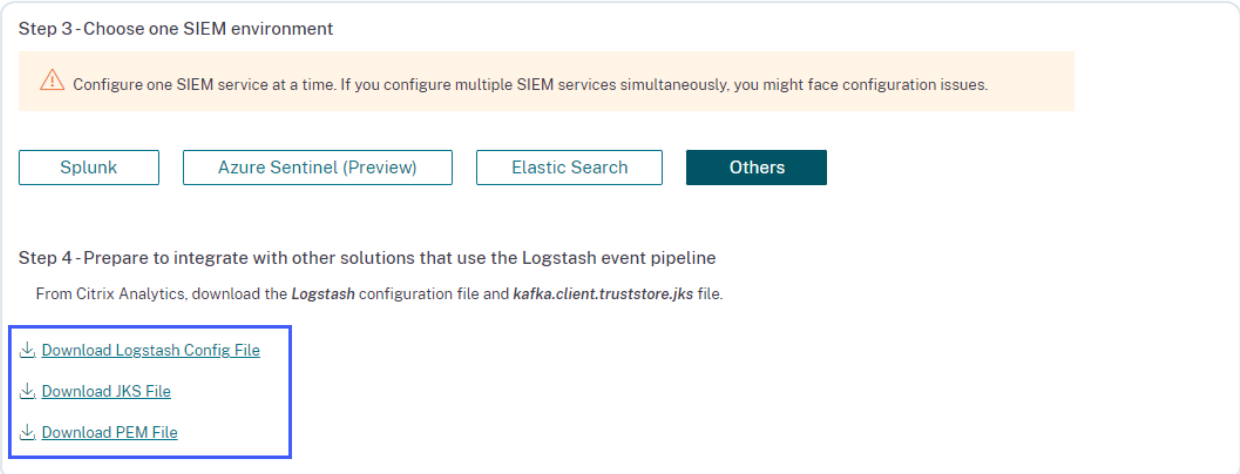


5. Select the **Others** tab to download the configuration files.

   - **Logstash config file**: This file contains the configuration data (input, filter, and output sections) for sending events from Citrix Analytics for Security using the Logstash data collection engine. For information on Logstash config file structure, see the Logstash documentation.
   - **JKS file**: This file contains the certificates required for SSL connection. This file is required when you integrate your SIEM using Logstash.
   - **PEM file**: This file contains the certificates required for SSL connection. This file is required when you integrate your SIEM using Kafka.

   NOTE

   These files contain sensitive information. Keep them in a safe and secure location.



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

6. Configure Logstash:

   a. On your Linux or Windows host machine, install Logstash (tested versions for compatibility with Citrix Analytics for Security: v7.17.7 and v8.5.3). You can also use your existing Logstash instance.

   b. On the host machine where you have installed Logstash, place the following files in the specified directory:

HOST MACHINE TYPE	FILE NAME	DIRECTORY PATH
Linux	CAS_Others_LogStash_Config.config	For Debian and RPM packages: `/etc/logstash/conf.d/`
		For .zip and .tar.gz archives: `{extract.path}/config`
	kafka.client.truststore.jks	For Debian and RPM packages: `/etc/logstash/ssl/`
		For .zip and .tar.gz archives: `{extract.path}/ssl`
Windows	CAS_Others_LogStash_Config.config	`C:\logstash-7.xx.x\config`
	kafka.client.truststore.jks	`C:\logstash-7.xx.x\config`

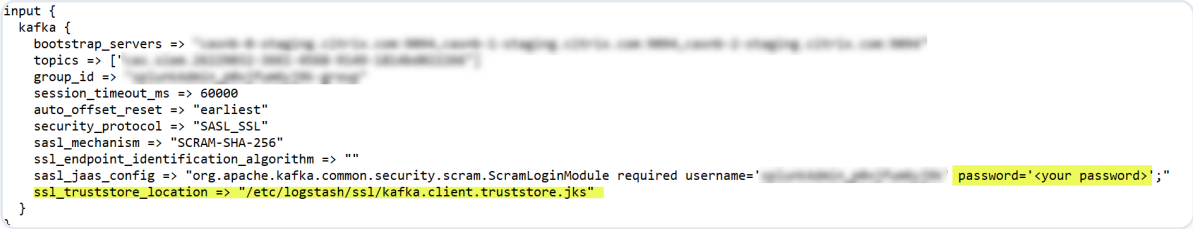
   c. Logstash configuration file contains sensitive information such as Kafka credentials, LogAnalytics Workspace IDs, Primary Keys. It is recommended that these sensitive credentials are not stored as a plaintext. To secure the integration, a Logstash keystore can be used to add keys with their respective values which can in turn be referenced using key names in the configuration file. For additional information on the Logstash keystore and how it enhances the security of your settings, see Secrets keystore for secure settings.

   d. Open the Logstash config file and do the following:

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

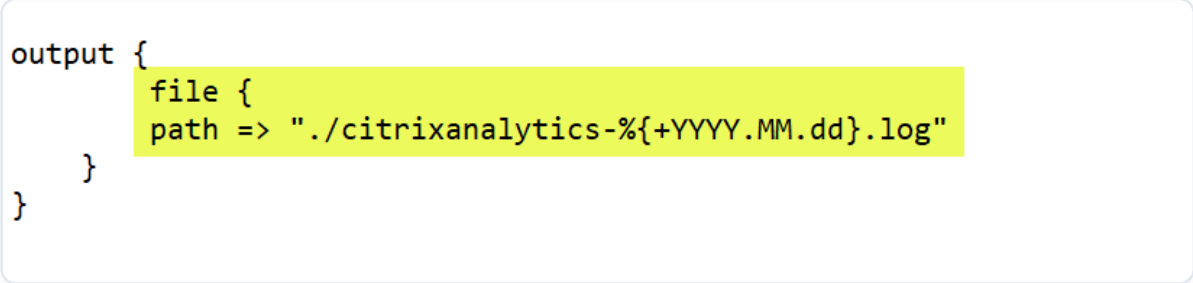
In the input section of the file, enter the following information:

- **Password**: The password of the account that you have created in Citrix Analytics for Security to prepare the configuration file.
- **SSL truststore location**: The location of your SSL client certificate. This is the location of the kafka.client.truststore.jks file in your host machine.



In the output section of the file, enter the destination path or details where you want to send the data. For information on the output plug-ins, see the Logstash documentation.

The following snippet shows that the output is written to a local log file.



e. Restart your host machine to send processed data from Citrix Analytics for Security to your SIEM service.

After configuration is complete, log in to your SIEM service and verify the Citrix Analytics data in your SIEM.

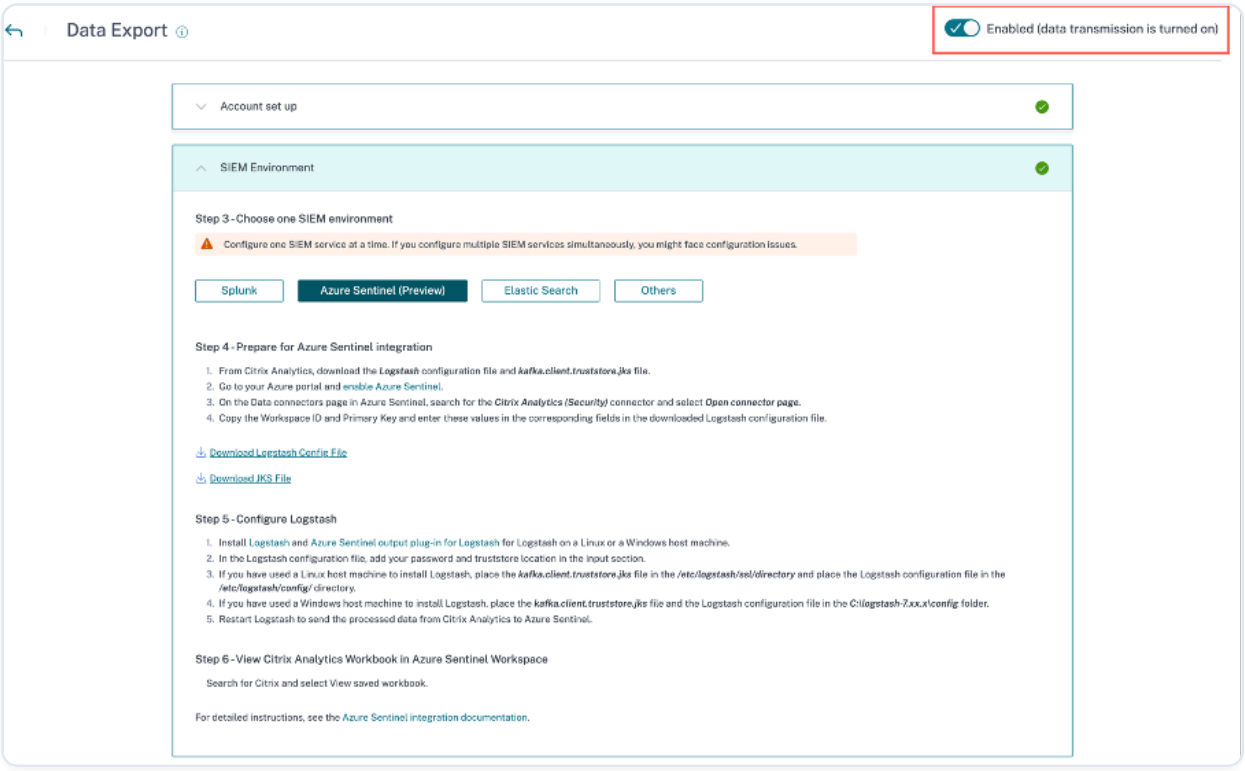
Turn on or off data transmission

After Citrix Analytics for Security prepares the configuration file, data transmission is turned on for your SIEM.

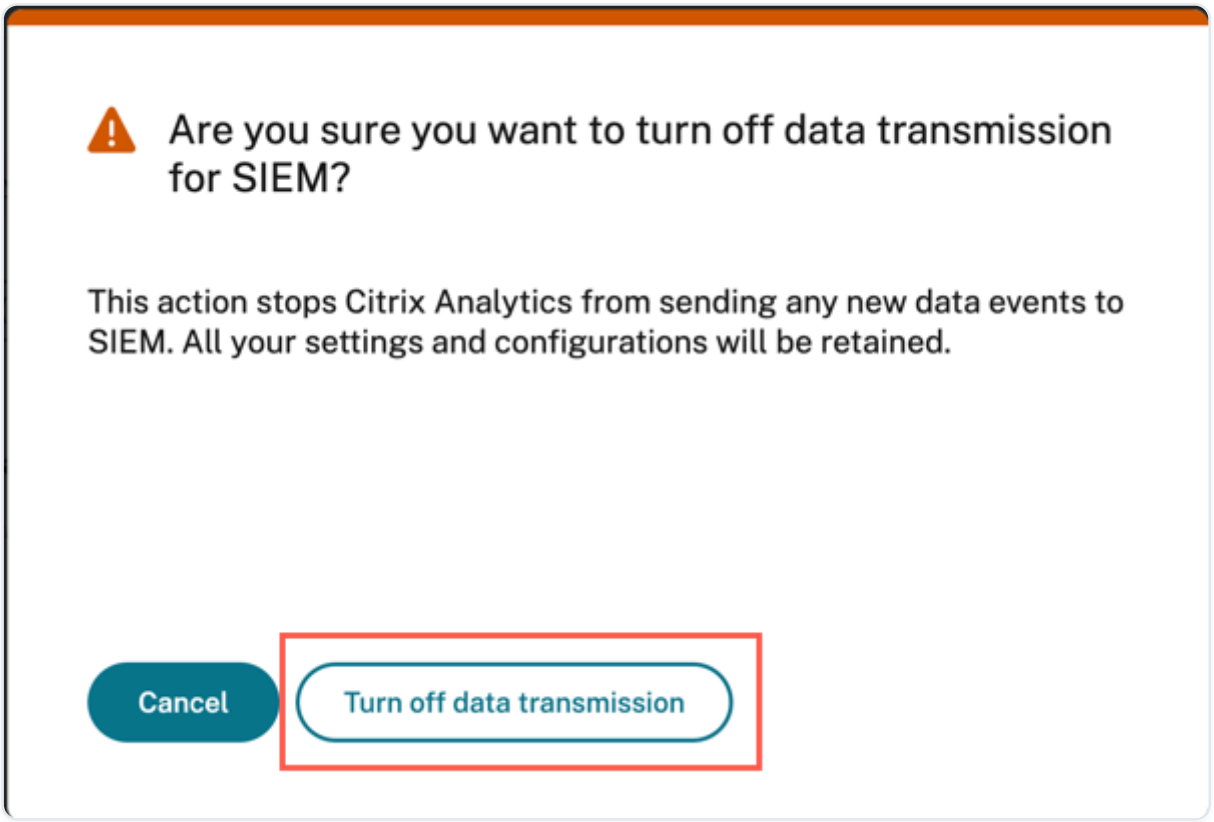
To stop transmitting data from Citrix Analytics for Security:

1. Go to **Settings > Data Exports**.
2. Turn off the toggle button to disable the **data transmission**. By default the data transmission always enabled.

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



A warning window appears for your confirmation. Click the **Turn off data transmission** button to stop the transmission activity.



To enable data transmission again, turn on the toggle button.

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

NOTE

Contact mailto:CAS-PM-Ext@cloud.com to request assistance for your SIEM integration, exporting data to your SIEM, or provide feedback.

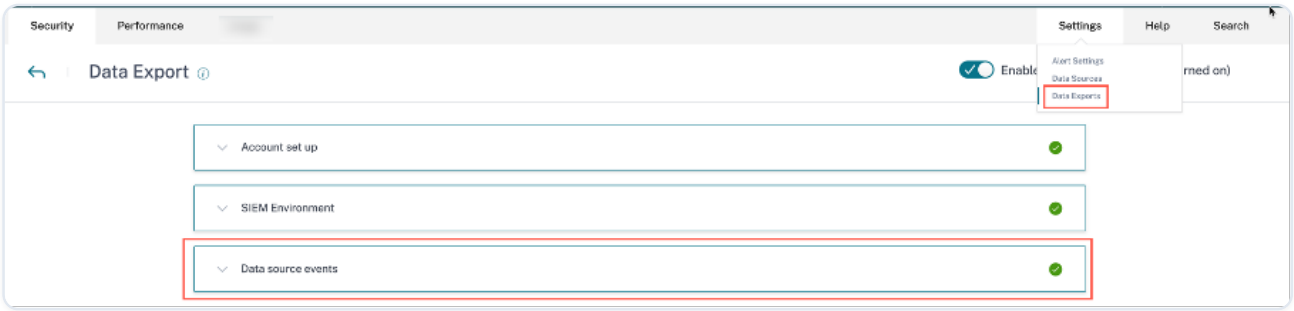
Citrix Analytics data exports format for SIEM

Citrix Analytics for Security™ allows you to integrate with your Security Information and Event Management (SIEM) services. This integration enables Citrix Analytics for Security to send data to your SIEM services and helps you gain insight into your organization's security risk posture.

Currently, you can integrate Citrix Analytics for Security with the following SIEM services:

- Splunk
- Microsoft Azure Sentinel
- Elasticsearch
- Other SIEMs using Kafka or Logstash based data connector

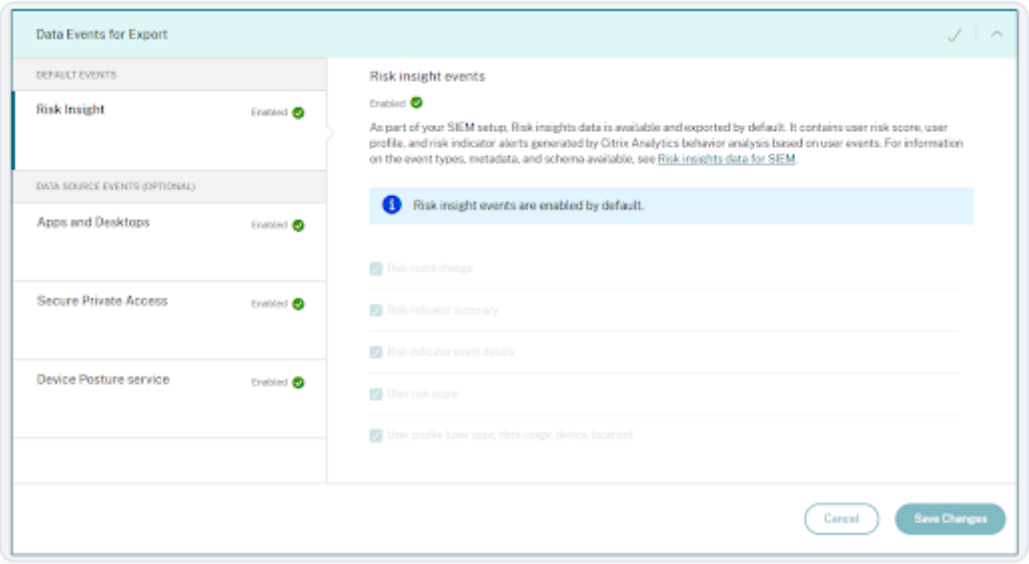
The **Data Exports option** is now globally available under **Settings**. To view the Data source events, navigate to **Settings > Data Exports > Data source events**.



The risk insights data sent by Citrix Analytics for Security to your SIEM service are of two types:

- Risk insights events (Default exports)
- Data Source events (Optional exports)

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



Risk insights data for SIEM

Once you have completed the account configuration and SIEM setup, default datasets (risk insights events) start flowing into your SIEM deployment. Risk insights datasets include user risk score events, user profile events, and risk indicator alerts. These are generated by Citrix Analytics machine learning algorithms and user behavior analysis, by leveraging user events.

The risk insights datasets of a user include the following:

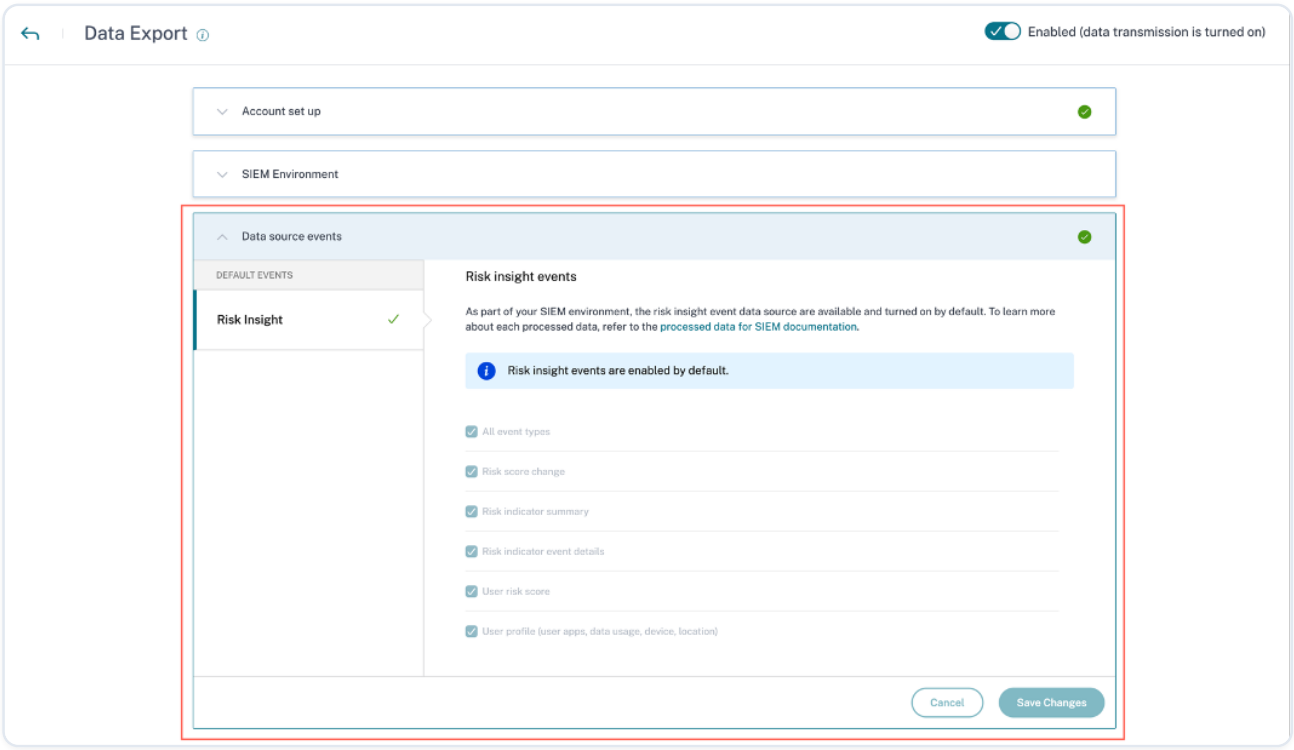
- **Risk score change**: Indicates a change in the user's risk score. When a user's risk score change is equal to or more than 3 and this change increases at any rate or drops by more than 10%, the data is sent to the SIEM service.
- **Risk indicator summary**: The details of the risk indicator triggered for a user.
- **Risk indicator event details**: The user events associated with a risk indicator. Citrix Analytics sends a maximum of 1000 event details for each risk indicator occurrence to your SIEM service. These events are sent in chronological order of occurrence.
- **User risk score event**: The current risk score of a user. Citrix Analytics for Security sends this data to the SIEM service every 12 hours.
- **User profile**: The user profile data can be categorized into:
    - **User apps**: The applications that a user has launched and used. Citrix Analytics for Security retrieves this data from Citrix Virtual Apps™ and sends it to the SIEM service every 12 hours.
    - **User device**: The devices associated with a user. Citrix Analytics for Security retrieves this data from Citrix Virtual Apps and Citrix Endpoint Management™ and sends it to SIEM service every 12 hours.

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

- **User location**: The city that a user was last detected in. Citrix Analytics for Security retrieves this data from Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). Citrix Analytics for Security sends this information to your SIEM service every 12 hours.
- **User client IP**: The client IP address of the user device. Citrix Analytics for Security retrieves this data from Citrix Virtual Apps and Desktops and Citrix DaaS™ (formerly Citrix Virtual Apps and Desktops service), and sends this information to your SIEM service every 12 hours.

If you are only able to view but unable to configure data source event preferences, then you do not have the necessary administrator permissions. To learn more, see Manage Administrator roles for Security Analytics.

In the following example, the **Save Changes** button is disabled. The risk insight events are enabled by default.



Schema details of the risk insights events

The following section describes the schema of the processed data generated by Citrix Analytics for Security.

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

NOTE

The field values shown in the following schema samples are only for representational purposes. The actual field values vary based on the user profile, user events, and the risk indicator.

The following table describes the field names that are common across the schema for all user profile data, user risk score, and risk score change.

FIELD NAME	DESCRIPTION
`entity_id`	The identity associated with the entity. In this case, the entity is the user.
`entity_type`	The entity at risk. In this case, the entity is the user.
`event_type`	The type of data sent to your SIEM service. For example: user's location, user's data usage, or user's device access information.
`tenant_id`	The unique identity of the customer.
`timestamp`	The date and time of the recent user activity.
`version`	The schema version of the processed data. The current schema version is 2.

User profile data schema

User location schema

```
{

  "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

  }
```

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

Field description for user location

FIELD NAME	DESCRIPTION
`event_type`	The type of data sent to the SIEM service. In this case, the event type is the user's location.
`country`	The country from where the user has logged in.
`city`	The city from where the user has logged in.
`cnt`	The number of times the location was accessed in the last 12 hours.

User client IP schema

```
{
  "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
}
```

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

Field description for client IP

FIELD NAME	DESCRIPTION
`client_ip`	The IP address of the user device.
`cnt`	The number of times the user has accessed the device in the last 12 hours.
`entity_id`	The identity associated with the entity. In this case, the entity is the user.
`entity_type`	The entity at risk. In this case, the event type is the user's client IP.
`event_type`	The type of data sent to your SIEM service. For example: the user's location, the user's data usage, or the user's device access information.
`tenant_id`	The unique identity of the customer.
`timestamp`	The date and time of the recent user activity..
`version`	The schema version of the processed data. The current schema version is 2.

User data usage schema


```
{

  "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

  }
```


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

Field description for user data usage

FIELD NAME	DESCRIPTION
`data_usage_bytes`	The amount of data (in bytes) used by the user. It is the aggregate of the downloaded and uploaded volume for a user.
`deleted_file_cnt`	The number of files deleted by the user.
`downloaded_bytes`	The amount of data downloaded by the user.
`downloaded_file_count`	The number of files downloaded by the user.
`event_type`	The type of data sent to the SIEM service. In this case, the event type is the user's usage profile.
`shared_file_count`	The number of files shared by the user.
`uploaded_bytes`	The amount of data uploaded by the user.
`uploaded_file_cnt`	The number of files uploaded by the user.

User device schema


```
{

  "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

  }
```


Field description for user device.

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

FIELD NAME	DESCRIPTION
`cnt`	The number of times the device is accessed in the last 12 hours.
`device`	The name of the device.
`event_type`	The type of data sent to the SIEM service. In this case, the event type is the user's device access information.

User app schema


```
{

  "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

  }
```


Field description for user app.

FIELD NAME	DESCRIPTION
`event_type`	The type of data sent to the SIEM service. In this case, the event type is the user's device access information.
`session_domain`	The ID of the session that the user has logged on.
`user_samaccountname`	The logon name for clients and servers from a previous version of Windows such as Windows NT 4.0, Windows 95, Windows 98, and LAN Manager. This name is used to log on to Citrix

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

FIELD NAME	DESCRIPTION
	StoreFront and also logon to a remote Windows machine.
`app`	The name of the application accessed by the user.
`cnt`	The number of times the application is accessed in the last 12 hours.

User risk score schema

```
{

  "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

  }
```

Field description for user risk score.

FIELD NAME	DESCRIPTION
`cur_riskscore`	The current risk score assigned to the user. The risk score varies from 0 to 100 depending on the threat severity associated with the user's activity.
`event_type`	The type of data sent to the SIEM service. In this case, the event type is the user's risk score.
`last_update_timestamp`	The time when the risk score was last updated for a user.

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

FIELD NAME	DESCRIPTION
`timestamp`	The time when the user risk score event is collected and sent to your SIEM service. This event is sent to your SIEM service after every 12 hours.

Risk score change schema

Sample 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

  }
```


Sample 2:


```
{

  "alert_message": "Risk score increase since last check", "alert_type":
"riskscore_increase", "alert_value": 39.0, "cur_riskscore": 76,
"entity_id": "demo_user", "entity_type": "user", "event_type":
"riskScoreChange", "tenant_id": "demo_tenant", "timestamp":
"2021-02-11T03:45:00Z", "version": 2

  }
```


Field description for risk score change.

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

FIELD NAME	DESCRIPTION
`alert_message`	The message displayed for the risk score change.
`alert_type`	Indicates whether the alert is for increase in risk score or significant drop in risk score percentage. When a user's risk score change is equal to or more than three and this change increases at any rate or drops by more than 10%, the data is sent to the SIEM service.
`alert_value`	A numerical value assigned for the risk score change. The risk score change is the difference between the current risk score and the previous risk score for a user. The alert value varies from -100 to 100.
`cur_riskscore`	The current risk score assigned to the user. The risk score varies from 0 to 100 depending on the threat severity associated with the user's activity.
`event_type`	The type of data sent to the SIEM service. In this case, the event type is the change in the user's risk score.
`timestamp`	The date and time when the latest change in the risk score is detected for the user.

Risk indicator schema

The risk indicator schema consists of two parts: indictor summary schema and indicator event details schema. Based on the risk indicator, the fields and their values in the schema change accordingly.

The following table describes the field names common across all indicator summary schema.

FIELD NAME	DESCRIPTION
`data source`	The products that send data to Citrix Analytics for Security. For example: Citrix Secure Private

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

FIELD NAME	DESCRIPTION
	Access™, Citrix Gateway, and Citrix Apps and Desktops.
`data_source_id`	The ID associated with a data source. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps and Desktops, ID 4 = Citrix Secure Private Access
`entity_type`	The entity at risk. It can be a user.
`entity_id`	The ID associated with the entity at risk.
`event_type`	The type of data sent to the SIEM service. In this case, the event type is the summary of the risk indicator.
`indicator_category`	Indicates the categories of risk indicators. The risk indicators are grouped into one of the risk categories- compromised endpoint, compromised users, data exfiltration, or insider threats.
`indicator_id`	The unique ID associated with the risk indicator.
`indicator_category_id`	The ID associated with a risk indicator category. ID 1 = Data exfiltration, ID 2 = Insider threats, ID 3 = Compromised users, ID 4 = Compromised endpoint
`indicator_name`	The name of the risk indicator. For a custom risk indicator, this name is defined while creating the indicator.
`indicator_type`	Indicates whether the risk indicator is default (built-in) or custom.
`indicator_uuid`	The unique ID associated with the risk indicator instance.
`indicator_vector_name`	Indicates the risk vector associated with a risk indicator. The risk vectors are Device-based

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

FIELD NAME	DESCRIPTION
	Risk Indicators, Location-based Risk Indicators, Logon-failure-based Risk Indicators, IP-based Risk Indicators, Data-based Risk Indicators, File-based Risk Indicators, and Other Risk Indicators.
`indicator_vector_id`	The ID associated with a risk vector. ID 1 = Device-based Risk Indicators, ID 2 = Location-based Risk Indicators, ID 3 = Logon-failure-based Risk Indicators, ID 4 = IP-based Risk Indicators, ID 5 = Data-based Risk Indicators, ID 6 = File-based Risk Indicators, ID 7 = Other Risk Indicators, and ID 999 = Not available
`occurrence_details`	The details about the risk indicator triggering condition.
`risk_probability`	Indicates the chances of risk associated with the user event. The value varies from 0 to 1.0. For a custom risk indicator, the risk_probability is always 1.0 because it is a policy-based indicator.
`severity`	Indicates the severity of the risk. It can be low, medium, or high.
`tenant_id`	The unique identity of the customer.
`timestamp`	The date and the time when the risk indicator is triggered.
`ui_link`	The link to the user timeline view on the Citrix Analytics user interface.
`observation_start_time`	The time from which Citrix Analytics starts monitoring the user activity until the time stamp. If any anomalous behavior is detected in this time period, a risk indicator is triggered.

The following table describes the field names common across all the indicator event details schema.

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

FIELD NAME	DESCRIPTION
`data_source_id`	The ID associated with a data source. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps and Desktops, ID 4 = Citrix Secure Private Access
`indicator_category_id`	The ID associated with a risk indicator category. ID 1 = Data exfiltration, ID 2 = Insider threats, ID 3 = Compromised users, ID 4 = Compromised endpoint
`entity_id`	The ID associated with the entity at risk.
`entity_type`	The entity that is at risk. It can be user.
`event_type`	The type of data sent to the SIEM service. In this case, the event type is the details of the risk indicator event.
`indicator_id`	The unique ID associated with the risk indicator.
`indicator_uuid`	The unique ID associated with the risk indicator instance.
`indicator_vector_name`	Indicates the risk vector associated with a risk indicator. The risk vectors are Device-based Risk Indicators, Location-based Risk Indicators, Logon-failure-based Risk Indicators, IP-based Risk Indicators, Data-based Risk Indicators, File-based Risk Indicators, and Other Risk Indicators.
`indicator_vector_id`	The ID associated with a risk vector. ID 1 = Device-based Risk Indicators, ID 2 = Location-based Risk Indicators, ID 3 = Logon-failure-based Risk Indicators, ID 4 = IP-based Risk Indicators, ID 5 = Data-based Risk Indicators, ID 6 = File-based Risk Indicators, ID 7 = Other Risk Indicators, and ID 999 = Not available
`tenant_id`	The unique identity of the customer.

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

FIELD NAME	DESCRIPTION
`timestamp`	The date and the time when the risk indicator is triggered.
`version`	The schema version of the processed data. The current schema version is 2.
`client_ip`	The IP address of the user's device.

NOTE

- If an integer data type field value is unavailable, the value assigned is -999. For example, `"latitude": -999`, `"longitude": -999`.
- If a string data type field value is unavailable, the value assigned is NA. For example, `"city": "NA"`, `"region": "NA"`.

Citrix Secure Private Access risk indicators schema

Attempt to access blacklisted URL risk indicator schema

INDICATOR SUMMARY SCHEMA

```
{
  "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 },
```

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

```
  "data_source_id": 4,
  "timestamp": "2018-03-15T10:59:58Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Attempt to access blacklisted URL",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {
    "observation_start_time": "2018-03-15T10:44:59Z",
    "relevant_event_type": "Blacklisted External Resource Access"
  }
}
```

INDICATOR EVENT DETAILS SCHEMA

```
{
```

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

```
  "tenant_id": "demo_tenant",
  "indicator_id": 401,
  "indicator_uuid": "c421f3f8-33d8-59b9-ad47-715b9d4f65f4",
  "indicator_category_id": 2,
  "indicator_vector": {
    "name": "Other Risk Indicators",
    "id": 7 },
  "data_source_id": 4,
  "timestamp": "2018-03-15T10:57:21Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "domain_name": "googleads.g.doubleclick.net",
  "executed_action": "blocked",
  "reason_for_action": "URL Category match",
  "client_ip": "157.xx.xxx.xxx"
}
```


The following table describes the field names specific to the summary schema and the event details schema for Attempt to access the blacklisted URL.

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

FIELD NAME	DESCRIPTION
`observation_start_time`	The time from which Citrix Analytics starts monitoring the user activity until the time stamp. If any anomalous behavior is detected in this time period, a risk indicator is triggered.
`executed_action`	The action applied on the blacklisted URL. The action includes Allow and Block.
`reason_for_action`	The reason for the applying the action for the URL.

Excessive data downloads risk indicator schema

INDICATOR SUMMARY SCHEMA


```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 403,
  "indicator_uuid": "67d21b81-a89a-531e-af0b-c5688c2e9d40",
  "indicator_category_id": 2,
  "indicator_vector": {
    "name": "Other Risk Indicators",
    "id": 7 },
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
```


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

```
  "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"
  }
}
```

INDICATOR EVENT DETAILS SCHEMA

```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 403,
  "indicator_uuid": "67d21b81-a89a-531e-af0b-c5688c2e9d40",
```

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

```
  "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
}
```


The following table describes the field names specific to the summary schema and the event details schema for Excessive data downloads.

FIELD NAME	DESCRIPTION
`observation_start_time`	The time from which Citrix Analytics starts monitoring the user activity until the time stamp. If any anomalous behavior is detected in this time period, a risk indicator is triggered.
`data_volume_in_bytes`	The amount of data in bytes that is downloaded.

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

FIELD NAME	DESCRIPTION
`relevant_event_type`	Indicates the type of the user event.
`domain_name`	The name of the domain from which data is downloaded.
`downloaded_bytes`	The amount of data in bytes that is downloaded.

Unusual upload volume risk indicator schema

INDICATOR SUMMARY SCHEMA


```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 402,
  "indicator_uuid": "4f2a249c-9d05-5409-9c5f-f4c764f50e67",
  "indicator_category_id": 2,
  "indicator_vector": {
    "name": "Other Risk Indicators",
    "id": 7 },
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
```


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

```
  "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"
  }
}
```

INDICATOR EVENT DETAILS SCHEMA

```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 402,
  "indicator_uuid": "c6abf40c-9b62-5db4-84bc-5b2cd2c0ca5f",
  "indicator_category_id": 2,
  "indicator_vector": {
```

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

```
    "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
}
```


The following table describes the field names specific to the summary schema and the event details schema for Unusual upload volume.

FIELD NAMES	DESCRIPTION
`observation_start_time`	The time from which Citrix Analytics starts monitoring the user activity until the time stamp. If any anomalous behavior is detected in this time period, a risk indicator is triggered.
`data_volume_in_bytes`	The amount of data in bytes that is uploaded.
`relevant_event_type`	Indicates the type of the user event.
`domain_name`	The name of the domain in which the data is uploaded.

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

FIELD NAMES	DESCRIPTION
`uploaded_bytes`	The amount of data in bytes that is uploaded.

Citrix Endpoint Management risk indicators schema

Jailbroken or rooted device detected indicators schema

INDICATOR SUMMARY SCHEMA


```
{
  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 200,
  "indicator_name": "Jailbroken / Rooted Device Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {
    "name": "Other Risk Indicators",
    "id": 7 },
  "indicator_type": "builtin",
  "indicator_uuid": "aa872f86-a991-4219-ad01-2a070b6e633d",
  "occurrence_details": {},
```


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

```
  "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
}
```


INDICATOR EVENT DETAILS SCHEMA


```
{
  "indicator_id": 200,
  "client_ip": "122.xx.xx.xxx",
  "data_source_id": 2,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {
    "name": "Other Risk Indicators",
    "id": 7 },
  "indicator_uuid": "9aaaa9e1-39ad-4daf-ae8b-2fa2caa60732",
  "tenant_id": "demo_tenant",
```


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

```
  "timestamp": "2021-04-09T17:50:35Z",
  "version": 2
}
```

Device with blacklisted apps detected

INDICATOR SUMMARY SCHEMA

```
{
  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 201,
  "indicator_name": "Device with Blacklisted Apps Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {
    "name": "Other Risk Indicators",
    "id": 7 },
  "indicator_type": "builtin",
  "indicator_uuid": "3ff7bd54-4319-46b6-8b98-58a9a50ae9a7",
  "occurrence_details": {},
```

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

```
  "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
}
```


INDICATOR EVENT DETAILS SCHEMA


```
{
  "indicator_id": 201,
  "client_ip": "122.xx.xx.xxx",
  "data_source_id": 2,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {
    "name": "Other Risk Indicators",
    "id": 7 },
  "indicator_uuid": "743cd13a-2596-4323-8da9-1ac279232894",
  "tenant_id": "demo_tenant",
```


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

```
  "timestamp": "2021-04-09T17:50:39Z",
  "version": 2
}
```

Unmanaged Device Detected

INDICATOR SUMMARY SCHEMA

```
{
  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 203,
  "indicator_name": "Unmanaged Device Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {
    "name": "Other Risk Indicators",
    "id": 7 },
  "indicator_type": "builtin",
  "indicator_uuid": "e28b8186-496b-44ff-9ddc-ae50e87bd757",
  "occurrence_details": {},
```

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

```
  "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
}
```


INDICATOR EVENT DETAILS SCHEMA


```
{
  "indicator_id": 203,
  "client_ip": "127.xx.xx.xxx",
  "data_source_id": 2,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {
    "name": "Other Risk Indicators",
    "id": 7 },
  "indicator_uuid": "dd280122-04f2-42b4-b9fc-92a715c907a0",
  "tenant_id": "demo_tenant",
```


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

```
  "timestamp": "2021-04-09T18:41:30Z",
  "version": 2
}
```

Citrix Gateway risk indicators schema

EPA scan failure risk indicator schema

INDICATOR SUMMARY SCHEMA

```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 100,
  "indicator_uuid": "3c17454c-86f5-588a-a4ac-0342693d8a70",
  "indicator_category_id": 3,
  "indicator_vector": {
    "name": "Other Risk Indicators",
    "id": 7 },
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
```

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

```
  "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"
  }
}
```

INDICATOR EVENT DETAILS SCHEMA

```
{
  "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 },
```

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

```
  "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"
}
```


The table describes the field names specific to the summary schema and the event details schema for the EPA scan failure risk indicator.

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

FIELD NAMES	DESCRIPTION
`event_description`	Describes the reasons for EPA scan failure such as post authentication failed and no quarantine group.
`relevant_event_type`	Indicates the type of the EPA scan failure event.
`gateway_domain_name`	The domain name of Citrix Gateway.
`gateway_ip`	The IP address of Citrix Gateway.
`policy_name`	The EPA scan policy name configured on the Citrix Gateway.
`country`	The country from which the user activity has been detected.
`city`	The city from which the user activity has been detected.
`region`	The region from which the user activity has been detected.
`cs_vserver_name`	The name of the content switch virtual server.
`device_os`	The operating system of the user's device.
`security_expression`	The security expression configured on the Citrix Gateway.
`vpn_vserver_name`	The name of the Citrix Gateway virtual server.
`vserver_fqdn`	The FQDN of the Citrix Gateway virtual server.

Excessive authentication failure risk indicator schema

INDICATOR SUMMARY SCHEMA

```
{

  "tenant_id": "demo_tenant",
```

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

```
"indicator_id": 101,

"indicator_uuid": "4bc0f759-93e0-5eea-9967-ed69de9dd09a",

"indicator_category_id": 3,

"indicator_vector": {

  "name": "Logon-Failure-Based Risk Indicators",

  "id": 3 },

"data_source_id": 1,

"timestamp": "2017-12-21T07:14:59Z",

"event_type": "indicatorSummary",

"entity_type": "user",

"entity_id": "demo_user",

"version": 2,

"risk_probability": 1,

"indicator_category": "Compromised users",

"indicator_name": "Excessive authentication failures",

"severity": "medium",

"data_source": "Citrix Gateway",

"ui_link": "https://analytics.cloud.com/user/”,

"indicator_type": "builtin",

"occurrence_details": {

  "observation_start_time": "2017-12-21T07:00:00Z",

  "relevant_event_type": "Logon Failure"
```


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

```
  }
}
```

INDICATOR EVENT DETAILS SCHEMA

```
{
  "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",
```

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

```
  "auth_server_ip": "10.xxx.x.xx",
  "client_ip": "24.xxx.xxx.xx",
  "gateway_ip": "24.xxx.xxx.xx",
  "vserver_fqdn": "demo-fqdn.citrix.com",
  "vpn_vserver_name": "demo_vpn_vserver",
  "cs_vserver_name": "demo_cs_vserver",
  "gateway_domain_name": "xyz",
  "country": "United States",
  "region": "California",
  "city": "San Jose",
  "nth_failure": 5
}
```


The following table describes the field names specific to the summary schema and the event details schema for Excessive authentication failure.

FIELD NAMES	DESCRIPTION
`relevant_event_type`	Indicates the type of event such as logon failure.
`event_description`	Describes the reason for the excessive authentication failure event such as an incorrect password.
`authentication_stage`	Indicates whether the authentication stage is primary, secondary, or tertiary.
`authentication_type`	Indicates the types of authentication such as LDAP, Local, or OAuth.

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

FIELD NAMES	DESCRIPTION
`auth_server_ip`	The IP address of the authentication server.
`gateway_domain_name`	The domain name of Citrix Gateway.
`gateway_ip`	The IP address of Citrix Gateway.
`cs_vserver_name`	The name of the content switch virtual server.
`vpn_vserver_name`	The name of the Citrix Gateway virtual server.
`vserver_fqdn`	The FQDN of the Citrix Gateway virtual server.
`nth_failure`	The number of times the user authentication has failed.
`country`	The country from which the user activity has been detected.
`city`	The city from which the user activity has been detected.
`region`	The region from which the user activity has been detected.

Impossible travel risk indicator

INDICATOR SUMMARY SCHEMA


```
{
  "tenant_id": "demo_tenant",
  "indicator_id": "111",
  "indicator_uuid": "83d68a6d-6588-5b77-9118-8a9e6a5b462b",
  "indicator_category_id": 3,
  "indicator_vector": {
```


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

```
    "name": "Location-Based Risk Indicators",
    "id": 2
  },
  "data_source_id": 1,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Impossible travel",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {
    "relevant_event_type": "Impossible travel",
    "distance": 7480.44718,
    "observation_start_time": "2020-06-06T12:00:00Z",
    "historical_logon_locations": "[{\"country\":\"United States\",
\"region\":\"Florida\",\"city\":\"Miami\",
\"latitude\":25.7617,\"longitude\":-80.191,\"count\":28},{\"country\":
```


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

```
\"United States\",
\"latitude\":37.0902,\"longitude\":-95.7129,\"count\":2}]",

    "historical_observation_period_in_days": 30

  }

}
```

INDICATOR EVENT DETAILS SCHEMA

```
{

  "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",
```

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

```
  "version": 2,
  "client_ip": "95.xxx.xx.xx",
  “ip_organization”: “global telecom ltd”,
  “ip_routing_type”: “mobile gateway”,
  "country": "Norway",
  "region": "Oslo",
  "city": "Oslo",
  "latitude": 59.9139,
  "longitude": 10.7522,
  "device_os": "Linux OS",
  "device_browser": "Chrome 62.0.3202.94"
}
```

The following table describes the field names specific to the summary schema and the event details schema for Impossible travel.

FIELD NAME	DESCRIPTION
`distance`	The distance (km) between the events associated with impossible travel.
`historical_logon_locations`	The locations accessed by the user and the number of times each location has been accessed during the observation period.
`historical_observation_period_in_days`	Each location is monitored for 30 days.
`relevant_event_type`	Indicates the type of event such as logon.

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

FIELD NAME	DESCRIPTION
`observation_start_time`	The time from which Citrix Analytics starts monitoring the user activity until the time stamp. If any anomalous behavior is detected in this time period, a risk indicator is triggered.
`country`	The country from which the user has logged on.
`city`	The city from which the user has logged on.
`region`	Indicates the region from which the user has logged on.
`latitude`	Indicates the latitude of the location from which the user has logged on.
`longitude`	Indicates the longitude of the location from which the user has logged on.
`device_browser`	The web browser used by the user.
`device_os`	The operating system of the user's device.
`ip_organization`	Registering organization of the client IP address
`ip_routing_type`	Client IP routing type

Logon from suspicious IP risk indicator schema

INDICATOR SUMMARY SCHEMA


```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 102,
  "indicator_uuid": "0100e910-561a-5ff3-b2a8-fc556d199ba5",
```


© 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": "2019-10-10T10:14:59Z",
"event_type": "indicatorSummary",
"entity_type": "user",
"entity_id": "demo_user",
"version": 2,
"risk_probability": 0.91,
"indicator_category": "Compromised users",
"indicator_name": "Logon from suspicious IP",
"severity": "medium",
"data_source": "Citrix Gateway",
"ui_link": "https://analytics.cloud.com/user/",
"indicator_type": "builtin",
"occurrence_details": {
  "relevant_event_type": "Logon",
  "client_ip": "1.0.xxx.xx",
  "observation_start_time": "2019-10-10T10:00:00Z",
  "suspicion_reasons": "brute_force|external_threat"
```


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

```
  }
}
```

INDICATOR EVENT DETAILS SCHEMA

```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 102,
  "indicator_uuid": "4ba77b6c-bac0-5ad0-9b4a-c459a3e2ec33",
  "indicator_category_id": 3,
  "indicator_vector": {
    "name": "IP-Based Risk Indicators",
    "id": 4 },
  "data_source_id": 1,
  "timestamp": "2019-10-10T10:11:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "suspicion_reasons": "external_threat",
  "gateway_ip": "gIP1",
  "client_ip": "128.0.xxx.xxx",
```

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

```
  "country": "Sweden",
  "city": "Stockholm",
  "region": "Stockholm",
  "webroot_reputation": 14,
  "webroot_threat_categories": "Windows Exploits|Botnets|Proxy",
  "device_os": "Windows OS",
  "device_browser": "Chrome"
}
```

The following table describes the field names specific to the summary schema and the event details schema for Login from a suspicious IP.

FIELD NAME	DESCRIPTION
`suspicious_reasons`	The reason for the IP address to be identified as suspicious.
`webroot_reputation`	The IP reputation index provided by the threat intelligence provider- Webroot.
`webroot_threat_categories`	The threat category identified for the suspicious IP by the threat intelligence provider- Webroot.
`device_os`	The operating system of the user device.
`device_browser`	The web browser used.
`country`	The country from which the user activity has been detected.
`city`	The city from which the user activity has been detected.

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

FIELD NAME	DESCRIPTION
`region`	The region from which the user activity has been detected.

Unusual authentication failure risk indicator schema

INDICATOR SUMMARY SCHEMA


```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 109,
  "indicator_uuid": "dc0174c9-247a-5e48-a2ab-d5f92cd83d0f",
  "indicator_category_id": 3,
  "indicator_vector": {
    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3 },
  "data_source_id": 1,
  "timestamp": "2020-04-01T06:44:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
```


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

```
  "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"
  }
}
```

INDICATOR EVENT DETAILS SCHEMA

```
{
  "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,
```

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

```
  "timestamp": "2020-04-01T06:42:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "event_description": "Success",
  "authentication_stage": "Secondary",
  "authentication_type": "LDAP",
  "client_ip": "99.xxx.xx.xx",
  "country": "United States",
  "city": "San Jose",
  "region": "California",
  "device_os": "Windows OS ",
  "device_browser": "Chrome",
  "is_risky": "false"
}
```


The following table describes the field names specific to the summary schema and the event details schema for Unusual authentication failure.

FIELD NAMES	DESCRIPTION
`relevant_event_type`	Indicates the type of event such as logon failure.

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

FIELD NAMES	DESCRIPTION
`event_description`	Indicates whether the logon is successful or unsuccessful
`authentication_stage`	Indicates whether the authentication stage is primary, secondary, or tertiary.
`authentication_type`	Indicates the types of authentication such as LDAP, Local, or OAuth.
`is_risky`	For a successful logon, the is_risky value is false. For an unsuccessful logon, the is_risky value is true.
`device_os`	The operating system of the user device.
`device_browser`	The web browser used by the user.
`country`	The country from which the user activity has been detected.
`city`	The city from which the user activity has been detected.
`region`	The region from which the user activity has been detected.

Suspicious logon risk indicator

INDICATOR SUMMARY SCHEMA

```
{
  "tenant_id": "demo_tenant",
  "indicator_id": "110",
  "indicator_uuid": "67fd935-a6a3-5397-b596-636aa1588c",
  "indicator_category_id": 3,
  "indicator_vector": [
```

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

```
    {
      "name": "Location-Based Risk Indicators",
      "id": 2
    },
    {
      "name": "IP-Based Risk Indicators",
      "id": 4
    },
    {
      "name": "Other Risk Indicators",
      "id": 7
    }
  ],
  "data_source_id": 1,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 0.71,
  "indicator_category": "Compromised users",
  "indicator_name": "Suspicious logon",
```


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

```
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {
    "observation_start_time": "2020-06-06T12:00:00Z",
    "relevant_event_type": "Logon",
    "event_count": 1,
    "historical_observation_period_in_days": 30,
    "country": "United States",
    "region": "Florida",
    "city": "Miami",
    "historical_logon_locations": "[{\"country\":\"United States\",
\"region\":\"New York\",\"city\":\"New York City\",
\"latitude\":40.7128,\"longitude\":-74.0060,\"count\":9}]",
    "user_location_risk": 75,
    "device_id": "",
    "device_os": "Windows OS",
    "device_browser": "Chrome",
    "user_device_risk": 0,
    "client_ip": "99.xxx.xx.xx",
    "user_network_risk": 75,
    "webroot_threat_categories": "Phishing",
```


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

```
    "suspicious_network_risk": 89
  }
}
```

INDICATOR EVENT DETAILS SCHEMA

```
{
  "tenant_id": "demo_tenant",
  "indicator_id": "110",
  "indicator_uuid": "67fd6935-a6a3-5397-b596-63856aa1588c",
  "indicator_category_id": 3,
  "indicator_vector": [
    {
      "name": "Location-Based Risk Indicators",
      "id": 2
    },
    {
      "name": "IP-Based Risk Indicators",
      "id": 4
    },
    {
      "name": "Other Risk Indicators",
```

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

```
      "id": 7
    }
  ],
  "data_source_id": 1,
  "timestamp": "2020-06-06T12:08:40Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "country": "United States",
  "region": "Florida",
  "city": "Miami",
  "latitude": 25.7617,
  "longitude": -80.1918,
  "device_browser": "Chrome",
  "device_os": "Windows OS",
  "device_id": "NA",
  "client_ip": "99.xxx.xx.xx"
}
```


The following table describes the field names specific to the summary schema and the event details schema for Suspicious logon.

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

FIELD NAME	DESCRIPTION
`historical_logon_locations`	The locations accessed by the user and the number of times each location has been accessed during the observation period.
`historical_observation_period_in_days`	Each location is monitored for 30 days.
`relevant_event_type`	Indicates the type of event such as logon.
`observation_start_time`	The time from which Citrix Analytics starts monitoring the user activity until the time stamp. If any anomalous behavior is detected in this time period, a risk indicator is triggered.
`occurrence_event_type`	Indicates the user event type such as account logon.
`country`	The country from which the user has logged on.
`city`	The city from which the user has logged on.
`region`	Indicates the region from which the user has logged on.
`latitude`	Indicates the latitude of the location from which the user has logged on.
`longitude`	Indicates the longitude of the location from which the user has logged on.
`device_browser`	The web browser used by the user.
`device_os`	The operating system of the user's device.
`device_id`	The name of the device used by the user.
`user_location_risk`	Indicates the suspicion level of the location from which the user has logged on. Low suspicion level: 0–69, Medium suspicion level: 70–89, and High suspicion level: 90–100

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

FIELD NAME	DESCRIPTION
`user_device_risk`	Indicates the suspicion level of the device from which the user has logged on. Low suspicion level: 0–69, Medium suspicion level: 70–89, and High suspicion level: 90–100
`user_network_risk`	Indicates the suspicion level of the network or the subnet from which the user has logged on. Low suspicion level: 0–69, Medium suspicion level: 70–89, and High suspicion level: 90–100
`suspicious_network_risk`	Indicates the IP threat level based on the Webroot IP threat intelligence feed. Low threat level: 0–69, Medium threat level: 70–89, and High threat level: 90–100
`webroot_threat_categories`	Indicates the types of threat detected from the IP address based on the Webroot IP threat intelligence feed. The threat categories can be Spam Sources, Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing, Proxy, Unspecified, Mobile Threats, and Tor Proxy

Citrix DaaS and Citrix Virtual Apps and Desktops risk indicators schema

Impossible travel risk indicator

INDICATOR SUMMARY SCHEMA

```
{

  "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

  }

}
```

INDICATOR EVENT DETAILS SCHEMA

```
{

  "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"
}
```

The following table describes the field names specific to the summary schema and the event details schema for Impossible travel.

FIELD NAME	DESCRIPTION
`distance`	The distance (km) between the events associated with impossible travel.
`historical_logon_locations`	The locations accessed by the user and the number of times each location has been accessed during the observation period.

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

FIELD NAME	DESCRIPTION
`historical_observation_period_in_days`	Each location is monitored for 30 days.
`relevant_event_type`	Indicates the type of event such as logon.
`observation_start_time`	The time from which Citrix Analytics starts monitoring the user activity until the time stamp. If any anomalous behavior is detected in this time period, a risk indicator is triggered.
`country`	The country from which the user has logged on.
`city`	The city from which the user has logged on.
`region`	Indicates the region from which the user has logged on.
`latitude`	Indicates the latitude of the location from which the user has logged on.
`longitude`	Indicates the longitude of the location from which the user has logged on.
`browser`	The web browser used by the user.
`os`	The operating system of the user's device.
`device_id`	The name of the device used by the user.
`receiver_type`	The type of the Citrix Workspace™ app or Citrix Receiver™ installed on the user's device.
`ip_organization`	Registering organization of the client IP address
`ip_routing_type`	Client IP routing type

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

Potential data exfiltration risk indicator

INDICATOR SUMMARY SCHEMA


```
{
  "tenant_id": "demo_tenant",
  "indicator_id": 303,
  "indicator_uuid": "fb649ff7-5b09-5f48-8a04-12836b9eed85",
  "indicator_category_id": 1,
  "indicator_vector": {
    "name": "Data-Based Risk Indicators",
    "id": 5 },
  "data_source_id": 3,
  "timestamp": "2018-04-02T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Data exfiltration",
  "indicator_name": "Potential data exfiltration",
  "severity": "low",
  "data_source": "Citrix Apps and Desktops",
```


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

```
  "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
  }
}
```

INDICATOR EVENT DETAILS SCHEMA

```
{
  "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",
```

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

```
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "occurrence_event_type": "App.SaaS.Clipboard",
  "file_size_in_bytes": 98000,
  "file_type": "text",
  "device_id": "dvc5",
  "receiver_type": "XA.Receiver.Windows",
  "app_url": "https://www.citrix.com",
  "client_ip": "10.xxx.xx.xxx",
  "entity_time_zone": "Pacific Standard Time"
}
```


The following table describes the fields specific to the summary schema and the event details schema for Potential data exfiltration.

FIELD NAME	DESCRIPTION
`observation_start_time`	The time from which Citrix Analytics starts monitoring the user activity until the time stamp. If any anomalous behavior is detected in this time period, a risk indicator is triggered.
`relevant_event_type`	Indicates the user activity such as download, print, or copy the data.
`exfil_data_volume_in_bytes`	The amount of data exfiltration.

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

FIELD NAME	DESCRIPTION
`occurrence_event_type`	Indicates how the data exfiltration has happened such as the clipboard operation in a SaaS app.
`file_size_in_bytes`	The size of the file.
`file_type`	The type of the file.
`device_id`	The ID of the user device.
`receiver_type`	The Citrix Workspace app or Citrix Receiver installed on the user device.
`app_url`	The URL of the application that is accessed by the user.
`entity_time_zone`	The time zone of the user.

Suspicious logon risk indicator schema

INDICATOR SUMMARY SCHEMA

```
{

  "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
```

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

```
    },
    {
      "name":"Location-Based Risk Indicators",
      "id":2
    },
    {
      "name":"IP-Based Risk Indicators",
      "id":4
    },
    {
      "name": "Device-Based Risk Indicators",
      "id": 1
    },
  ],
  "data_source_id": 3,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "user2",
  "version": 2,
  "risk_probability": 0.78,
  "indicator_category": "Compromised users",
```


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

```
  "indicator_name": "Suspicious logon",

  "severity": "medium",

  "data_source": "Citrix Apps and Desktops",

  "ui_link": "https://analytics.cloud.com/user/ ",

  "indicator_type": "builtin",

  "occurrence_details":

  {

    "user_location_risk": 0,

    "city": "Some_city",

    "observation_start_time": "2020-06-06T12:00:00Z",

    "event_count": 1,

    "user_device_risk": 75,

    "country": "United States",

    "device_id": "device2",

    "region": "Some_Region",

    "client_ip": "99.xx.xx.xx",

    "webroot_threat_categories": "'Spam Sources', 'Windows Exploits', 'Web
Attacks', 'Botnets', 'Scanners', 'Denial of Service'",

    "historical_logon_locations": "[{\"country\":\"United States\",
\"latitude\":45.0,\"longitude\":45.0,\"count\":12},{\"country\":\"United
States\",\"region\":\"Some_Region_A\",\"city\":\"Some_City_A\",
\"latitude\":0.0,\"longitude\":0.0,\"count\":8}]",

    "relevant_event_type": "Logon",

    "user_network_risk": 100,
```


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

```
    "historical_observation_period_in_days": 30,
    "suspicious_network_risk": 0
  }
}
```

INDICATOR EVENT DETAILS SCHEMA

```
{
  "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
    },
    {
```

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

```
      "name":"IP-Based Risk Indicators",
      "id":4
    },
    {
      "name": "Device-Based Risk Indicators",
      "id": 1
    },
  ],
  "data_source_id": 3,
  "timestamp": "2020-06-06 12:02:30",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "user2",
  "version": 2,
  "occurrence_event_type": "Account.Logon",
  "city": "Some_city",
  "country": "United States",
  "region": "Some_Region",
  "latitude": 37.751,
  "longitude": -97.822,
  "browser": "Firefox 1.3",
  "os": "Windows OS",
```


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

```
  "device_id": "device2",
  "receiver_type": "XA.Receiver.Chrome",
  "client_ip": "99.xxx.xx.xx"
}
```

The following table describes the field names specific to the summary schema and the event details schema for Suspicious logon.

FIELD NAME	DESCRIPTION
`historical_logon_locations`	The locations accessed by the user and the number of times each location has been accessed during the observation period.
`historical_observation_period_in_days`	Each location is monitored for 30 days.
`relevant_event_type`	Indicates the type of event such as logon.
`observation_start_time`	The time from which Citrix Analytics starts monitoring the user activity until the time stamp. If any anomalous behavior is detected in this time period, a risk indicator is triggered.
`occurrence_event_type`	Indicates the user event type such as account logon.
`country`	The country from which the user has logged on.
`city`	The city from which the user has logged on.
`region`	Indicates the region from which the user has logged on.
`latitude`	Indicates the latitude of the location from which the user has logged on.

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

FIELD NAME	DESCRIPTION
`longitude`	Indicates the longitude of the location from which the user has logged on.
`browser`	The web browser used by the user.
`os`	The operating system of the user's device.
`device_id`	The name of the device used by the user.
`receiver_type`	The type of the Citrix Workspace app or Citrix Receiver installed on the user's device.
`user_location_risk`	Indicates the suspicion level of the location from which the user has logged on. Low suspicion level: 0–69, Medium suspicion level: 70–89, and High suspicion level: 90–100
`user_device_risk`	Indicates the suspicion level of the device from which the user has logged on. Low suspicion level: 0–69, Medium suspicion level: 70–89, and High suspicion level: 90–100
`user_network_risk`	Indicates the suspicion level of the network or the subnet from which the user has logged on. Low suspicion level: 0–69, Medium suspicion level: 70–89, and High suspicion level: 90–100
`suspicious_network_risk`	Indicates the IP threat level based on the Webroot IP threat intelligence feed. Low threat level: 0–69, Medium threat level: 70–89, and High threat level: 90–100
`webroot_threat_categories`	Indicates the types of threat detected from the IP address based on the Webroot IP threat intelligence feed. The threat categories can be Spam Sources, Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing, Proxy, Unspecified, Mobile Threats, and Tor Proxy

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

Microsoft Active Directory Indicator

Indicator summary schema


```
{

  "data_source": "Microsoft Graph Security",

  "entity_id": "demo_user",

  "entity_type": "user",

  "event_type": "indicatorSummary",

  "indicator_category": "Compromised users",

  "indicator_id": 1000,

  "indicator_name": "MS Active Directory Indicator",

  "indicator_vector": {

    "name": "IP-Based Risk Indicators",

    "id": 4 },

  "indicator_type": "builtin",

  "indicator_uuid": "9880f479-9fbe-4ab0-8348-a613f9de5eba",

  "occurrence_details": {},

  "risk_probability": 1.0,

  "severity": "low",

  "tenant_id": "demo_tenant",

  "timestamp": "2021-01-27T16:03:46Z",

  "ui_link": "https://analytics-daily.cloud.com/user/",

  "version": 2
```


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

```
}
```

Indicator event details schema

```
{
  "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
}
```

Custom risk indicator schema

The following section describes the schema for the custom risk indicator.

NOTE

Currently, Citrix Analytics sends the data related to the custom risk indicators of Citrix DaaS and Citrix Virtual Apps and Desktops to your SIEM service.

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

The following table describes the field names for the custom risk indicator summary schema.

FIELD NAME	DESCRIPTION
`data source`	The products that send data to Citrix Analytics for Security. For example: Citrix Secure Private Access, Citrix Gateway, and Citrix Apps and Desktops.
`data_source_id`	The ID associated with a data source. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps and Desktops, ID 4 = Citrix Secure Private Access
`entity_id`	The ID associated with the entity at risk.
`entity_type`	The entity at risk. In this case, the entity is a user.
`event_type`	The type of data sent to the SIEM service. In this case, the event type is the summary of the risk indicator.
`indicator_category`	Indicates the categories of risk indicators. The risk indicators are grouped into one of the risk categories- compromised endpoint, compromised users, data exfiltration, or insider threats.
`indicator_id`	The unique ID associated with the risk indicator.
`indicator_category_id`	The ID associated with the risk indicator category. ID 1 = Data exfiltration, ID 2 = Insider threats, ID 3 = Compromised users, ID 4 = Compromised endpoints
`indicator_name`	The name of the risk indicator. For a custom risk indicator, this name is defined while creating the indicator.
`indicator_type`	Indicates whether the risk indicator is default (built-in) or custom.

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

FIELD NAME	DESCRIPTION
`indicator_uuid`	The unique ID associated with the risk indicator instance.
`occurrence_details`	The details about the risk indicator triggering condition.
`pre_configured`	Indicates whether the custom risk indicator is preconfigured.
`risk_probability`	Indicates the chances of risk associated with the user event. The value varies from 0 to 1.0. For a custom risk indicator, the risk_probability is always 1.0 because it is a policy-based indicator.
`severity`	Indicates the severity of the risk. It can be low, medium, or high.
`tenant_id`	The unique identity of the customer.
`timestamp`	The date and the time when the risk indicator is triggered.
`ui_link`	The link to the user timeline view on the Citrix Analytics user interface.
`version`	The schema version of the processed data. The current schema version is 2.

The following table describes the field names common across the custom risk indicator event details schema.

FIELD NAME	DESCRIPTION
`data_source_id`	The ID associated with a data source. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps and Desktops, ID 4 = Citrix Secure Private Access
`indicator_category_id`	The ID associated with the risk indicator category. ID 1 = Data exfiltration, ID 2 = Insider

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

FIELD NAME	DESCRIPTION
	threats, ID 3 = Compromised users, ID 4 = Compromised endpoints
`event_type`	The type of data sent to the SIEM service. In this case, the event type is the details of the risk indicator event.
`tenant_id`	The unique identity of the customer.
`entity_id`	The ID associated with the entity at risk.
`entity_type`	The entity that is at risk. In this case, it is the user.
`indicator_id`	The unique ID associated with the risk indicator.
`indicator_uuid`	The unique ID associated with the risk indicator instance.
`timestamp`	The date and the time when the risk indicator is triggered.
`version`	The schema version of the processed data. The current schema version is 2.
`event_id`	The ID associated with the user event.
`occurrence_event_type`	Indicates the type of user event such as session logon, session launch, and account logon.
`product`	Indicates the type of Citrix Workspace app such as Citrix Workspace app for Windows.
`client_ip`	The IP address of the user's device.
`session_user_name`	The user name associated with the Citrix Apps and Desktops session.
`city`	The name of the city from which the user activity is detected.

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

FIELD NAME	DESCRIPTION
`country`	The name of the country from which the user activity is detected.
`device_id`	The name of the device used by the user.
`os_name`	The operating system that is installed on the user's device. For more information, see Self-service search for Apps and Desktops.
`os_version`	The version of the operating system that is installed on the user's device. For more information, see Self-service search for Apps and Desktops.
`os_extra_info`	The extra details associated with the operating system that is installed on the user's device. For more information, see Self-service search for Apps and Desktops.

Custom risk indicator for Citrix DaaS and Citrix Virtual Apps and Desktops

INDICATOR SUMMARY SCHEMA

```
{
  "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,
```

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

```
  "indicator_id": "ca97a656ab0442b78f3514052d595936",

  "indicator_name": "Demo_user_usage",

  "indicator_type": "custom",

  "indicator_uuid": "8e680e29-d742-4e09-9a40-78d1d9730ea5",

  "occurrence_details": {

    "condition": "User-Name ~ demo_user", "happen": 0, "new_entities": "",
"repeat": 0, "time_quantity": 0, "time_unit": "", "type": "everyTime"},

  "pre_configured": "N",

  "risk_probability": 1.0,

  "severity": "low",

  "tenant_id": "demo_tenant",

  "timestamp": "2021-02-10T14:47:25Z",

  "ui_link": "https://analytics.cloud.com/user/ ",

  "version": 2

}
```


INDICATOR EVENT DETAILS SCHEMA FOR THE SESSION LOGON EVENT


```
{

  "event_type": "indicatorEventDetails",

  "data_source_id": 3,

  "indicator_category_id": 3,

  "tenant_id": "demo_tenant",
```


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

```
"entity_id": "demo_user",

"entity_type": "user",

"indicator_id": "9033b2f6a8914a9282937b35ce497bcf",

"timestamp": "2021-03-19T10:08:05Z",

"indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",

"version": 2,

"event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",

"occurrence_event_type": "Session.Logon",

"product": "XA.Receiver.Windows",

"client_ip": "103.xx.xxx.xxx",

"session_user_name": "user01",

"city": "Mumbai",

"country": "India",

"device_id": "5-Synthetic_device",

"os_name": "Windows NT 6.1",

"os_version": "7601",

"os_extra_info": "Service Pack 1",

"app_name": "notepad",

"launch_type": "Application",

"domain": "test_domain",

"server_name": "SYD04-MS1-S102",

"session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
```


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

```
}
```

The following table describes the field names specific to the event details schema for the session logon event.

FIELD NAME	DESCRIPTION
`app_name`	Name of an application or desktop launched.
`launch_type`	Indicates either application or desktop.
`domain`	The domain name of the server that sent the request.
`server_name`	Name of the server.
`session_guid`	The GUID of the active session.

INDICATOR EVENT DETAILS SCHEMA FOR THE SESSION LAUNCH EVENT

```
{
  "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,
```

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

```
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.Launch",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
}
```


The following table describes the field names specific to the event details schema for the session launch event.

FIELD NAME	DESCRIPTION
`app_name`	Name of an application or desktop launched.
`launch_type`	Indicates either application or desktop.

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

INDICATOR EVENT DETAILS SCHEMA FOR THE ACCOUNT LOGON EVENT


```
{

  "event_type": "indicatorEventDetails",

  "data_source_id": 3,

  "indicator_category_id": 3,

  "tenant_id": "demo_tenant",

  "entity_id": "demo_user",

  "entity_type": "user",

  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",

  "timestamp": "2021-03-19T10:08:05Z",

  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",

  "version": 2,

  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",

  "occurrence_event_type": "Account.Logon",

  "product": "XA.Receiver.Windows",

  "client_ip": "103.xx.xxx.xxx",

  "session_user_name": "user01",

  "city": "Mumbai",

  "country": "India",

  "device_id": "5-Synthetic_device",

  "os_name": "Windows NT 6.1",

  "os_version": "7601",
```


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

```
  "os_extra_info": "Service Pack 1",

  "app_name": "notepad",

}
```

The following table describes the field names specific to the event details schema for the account logon event.

FIELD NAME	DESCRIPTION
`app_name`	Name of an application or desktop launched.

INDICATOR EVENT DETAILS SCHEMA FOR THE SESSION END EVENT

```
{

  "event_type": "indicatorEventDetails",

  "data_source_id": 3,

  "indicator_category_id": 3,

  "tenant_id": "demo_tenant",

  "entity_id": "demo_user",

  "entity_type": "user",

  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",

  "timestamp": "2021-03-19T10:08:05Z",

  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",

  "version": 2,

  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",

  "occurrence_event_type": "Session.End",
```

© 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": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
}
```


The following table describes the field names specific to the event details schema for the session end event.

FIELD NAME	DESCRIPTION
`app_name`	Name of an application or desktop launched.
`launch_type`	Indicates either application or desktop.
`domain`	The domain name of the server that sent the request.

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

FIELD NAME	DESCRIPTION
`server_name`	Name of the server.
`session_guid`	The GUID of the active session.

INDICATOR EVENT DETAILS SCHEMA FOR THE APP START EVENT


```
{
  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.Start",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
```


© 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",
  "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"
}
```

The following table describes the field names specific to the event details schema for the app start event.

FIELD NAME	DESCRIPTION
`app_name`	Name of an application or desktop launched.
`launch_type`	Indicates either application or desktop.
`domain`	The domain name of the server that sent the request.
`server_name`	Name of the server.
`session_guid`	The GUID of the active session.
`module_file_path`	The path of the application that is being used.

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

INDICATOR EVENT DETAILS SCHEMA FOR THE APP END EVENT


```
{
  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
```


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

```
  "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"
}
```

The following table describes the field names specific to the event details schema for the app end event.

FIELD NAME	DESCRIPTION
`app_name`	Name of an application or desktop launched.
`launch_type`	Indicates either application or desktop.
`domain`	The domain name of the server that sent the request.
`server_name`	Name of the server.
`session_guid`	The GUID of the active session.
`module_file_path`	The path of the application that is being used.

INDICATOR EVENT DETAILS SCHEMA FOR THE FILE DOWNLOAD EVENT

```
{
  "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": "File.Download",

"product": "XA.Receiver.Windows",

"client_ip": "103.xx.xxx.xxx",

"session_user_name": "user01",

"city": "Mumbai",

"country": "India",

"device_id": "5-Synthetic_device",

"os_name": "Windows NT 6.1",

"os_version": "7601",

"os_extra_info": "Service Pack 1",

"file_download_file_name": "File5.txt",

"file_download_file_path": "/root/folder1/folder2/folder3",

"file_size_in_bytes": 278,
```


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

```
  "launch_type": "Desktop",

  "domain": "test_domain",

  "server_name": "test_server",

  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",

  "device_type": "USB"

}
```

The following table describes the field names specific to the event details schema for the file download event.

FIELD NAME	DESCRIPTION
`file_download_file_name`	Name of the download file.
`file_download_file_path`	The destination path where the file is downloaded.
`launch_type`	Indicates either application or desktop.
`domain`	The domain name of the server that sent the request.
`server_name`	Name of the server.
`session_guid`	The GUID of the active session.
`device_type`	Indicates the type of the device where the file is downloaded.

INDICATOR EVENT DETAILS SCHEMA FOR THE PRINTING EVENT

```
{

  "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": "Printing",

"product": "XA.Receiver.Windows",

"client_ip": "103.xx.xxx.xxx",

"session_user_name": "user01",

"city": "Mumbai",

"country": "India",

"device_id": "5-Synthetic_device",

"os_name": "Windows NT 6.1",

"os_version": "7601",

"os_extra_info": "Service Pack 1",

"printer_name": "Test-printer",

"launch_type": "Desktop",

"domain": "test_domain",
```


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

```
  "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"

}
```

The following table describes the field names specific to the event details schema for the printing event.

FIELD NAME	DESCRIPTION
`printer_name`	Name of the printer used for the printing job.
`launch_type`	Indicates either application or desktop.
`domain`	The domain name of the server that sent the request.
`server_name`	Name of the server.
`session_guid`	The GUID of the active session.
`job_details_size_in_bytes`	The size of the printed job such as file or folder.
`job_details_filename`	Name of the printed file.
`job_details_format`	The format of the printed job.

INDICATOR EVENT DETAILS SCHEMA FOR THE APP SAAS LAUNCH EVENT

```
{

  "event_type": "indicatorEventDetails",
```

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

```
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.SaaS.Launch",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "launch_type": "Desktop",
}
```


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

The following table describes the field names specific to the event details schema for the app SaaS launch event.

FIELD NAME	DESCRIPTION
`launch_type`	Indicates either application or desktop.

INDICATOR EVENT DETAILS SCHEMA FOR THE APP SAAS END EVENT


```
{
  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.SaaS.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
```


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

```
  "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",
}
```


The following table describes the field names specific to the event details schema for the app SaaS end event.

FIELD NAME	DESCRIPTION
`launch_type`	Indicates either application or desktop.

Data source events

Additionally, you can configure the Data exports feature to export user events from your Citrix Analytics for Security enabled product data sources. When you perform any activity in the Citrix environment, the data source events are generated. The exported events are unprocessed real-time user and product usage data as available in the self-service view. The metadata contained in these events can further be used for deeper threat analysis, creating new dashboards, and co-related with other non-Citrix data source events across your security and IT infra.

Currently, Citrix Analytics for Security sends user events to your SIEM for the Citrix Virtual Apps and Desktops data source.

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

Schema details of the data source events

Citrix Virtual Apps and Desktops events

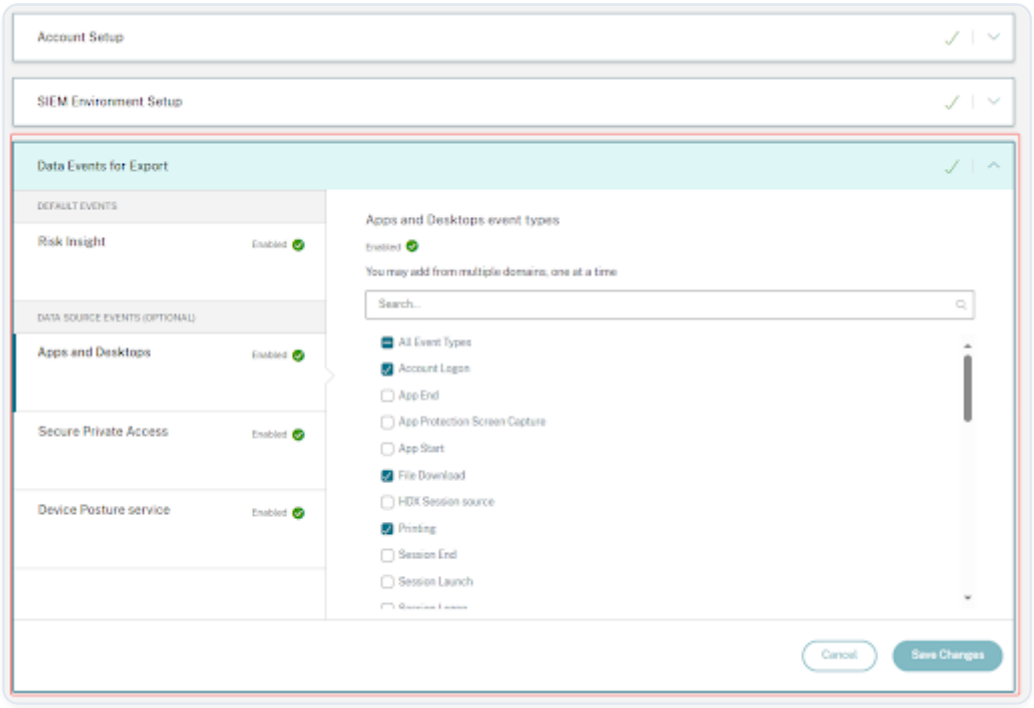
The user events are received in real-time in Citrix Analytics for Security when users use virtual apps or virtual desktops. For more information, see Citrix Virtual Apps and Desktops and Citrix DaaS data source. You can view the following user events associated with Citrix Virtual Apps and Desktops in your SIEM:

- All event types
- Account logon
- App (start, launch, end)
- Clipboard
- File (print, download)
- HDX™ session source
- Printing
- Session (logon, launch, end, termination)
- VDA data
- VDA process creation

For more information about the events and their attributes, see Self-service search for Virtual Apps and Desktops.

You can review what event types are enabled and flowing to SIEM. You can configure or remove the event type that is applicable for a tenant and click the **Save Changes** button to save your settings.

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

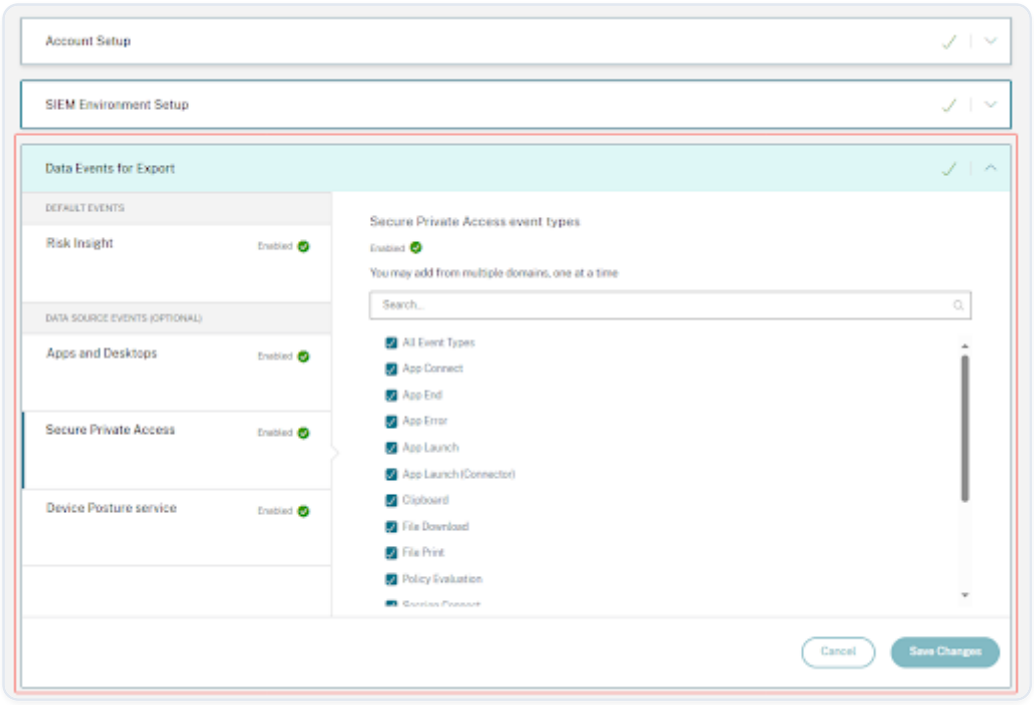


Secure Private Access events

The user events are received in real-time in Citrix Analytics for Security when users access applications through Citrix Secure Private Access, such as Citrix Workspace App, Citrix Secure Access clients, or Citrix Enterprise Browser. You can view the following user events associated with Secure Private Access in your SIEM:

- All event types
- Account logon
- App (connect, launch, end, error)
- File (print, download)
- Policy Evaluation
- Clipboard
- Session (connect, launch)
- Url
- User Login
- SPA Service Logs

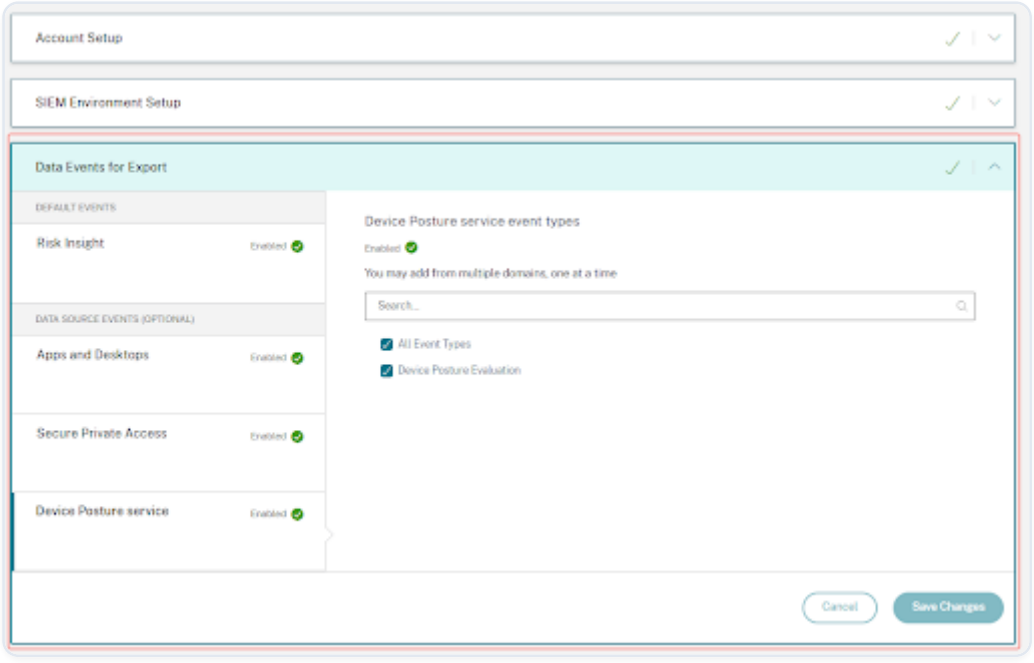
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Device Posture service events

The user events are generated when the Citrix Endpoint Analysis (EPA) client performs a posture check on a device attempting to access Citrix Virtual Apps and Desktops or Citrix Secure Private Access resources. You can view the following user events associated with Device Posture service in your SIEM:

- All event types
- Device Posture Evaluation



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

You can review the event types enabled for your tenant and ensure they are flowing to the SIEM. You can configure or remove applicable event types and click the **Save Changes** button to apply your settings.

Leveraging Citrix Analytics SIEM Data Model for Threat Analysis and Data Correlation

This article explains the entity data relationship that's exhibited by the events sent to a customer's SIEM environment. To elucidate this, let's take an example of a threat hunting scenario where the attributes - client IP and OS are the focal points. The following ways to correlate the said attributes to the user will be discussed:

- Using custom risk indicator insights
- Using data source events

Splunk is the SIEM environment chosen to be showcased in the following example. Similar data correlation can also be performed on Sentinel using workbook template by Citrix Analytics. To explore this further, refer Citrix Analytics workbook for Microsoft Sentinel.

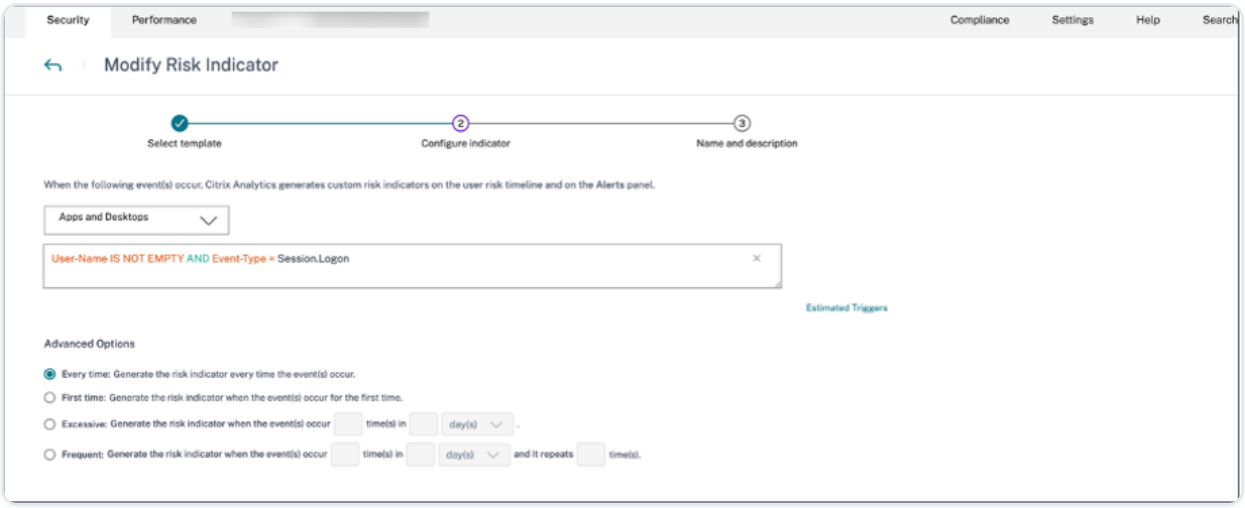
Custom Risk Indicator Insights

As mentioned in Citrix Analytics data exports format for SIEM, indicator summary and event details insights are part of the default risk insights data set. For Citrix Virtual Apps and Desktops indicator dataset, client IP and OS get exported by default. Hence, if an administrator sets up a custom indicator with or without the condition including these fields, the said data points would flow into your Splunk environment.

Setting Custom Risk Indicator In Citrix Analytics

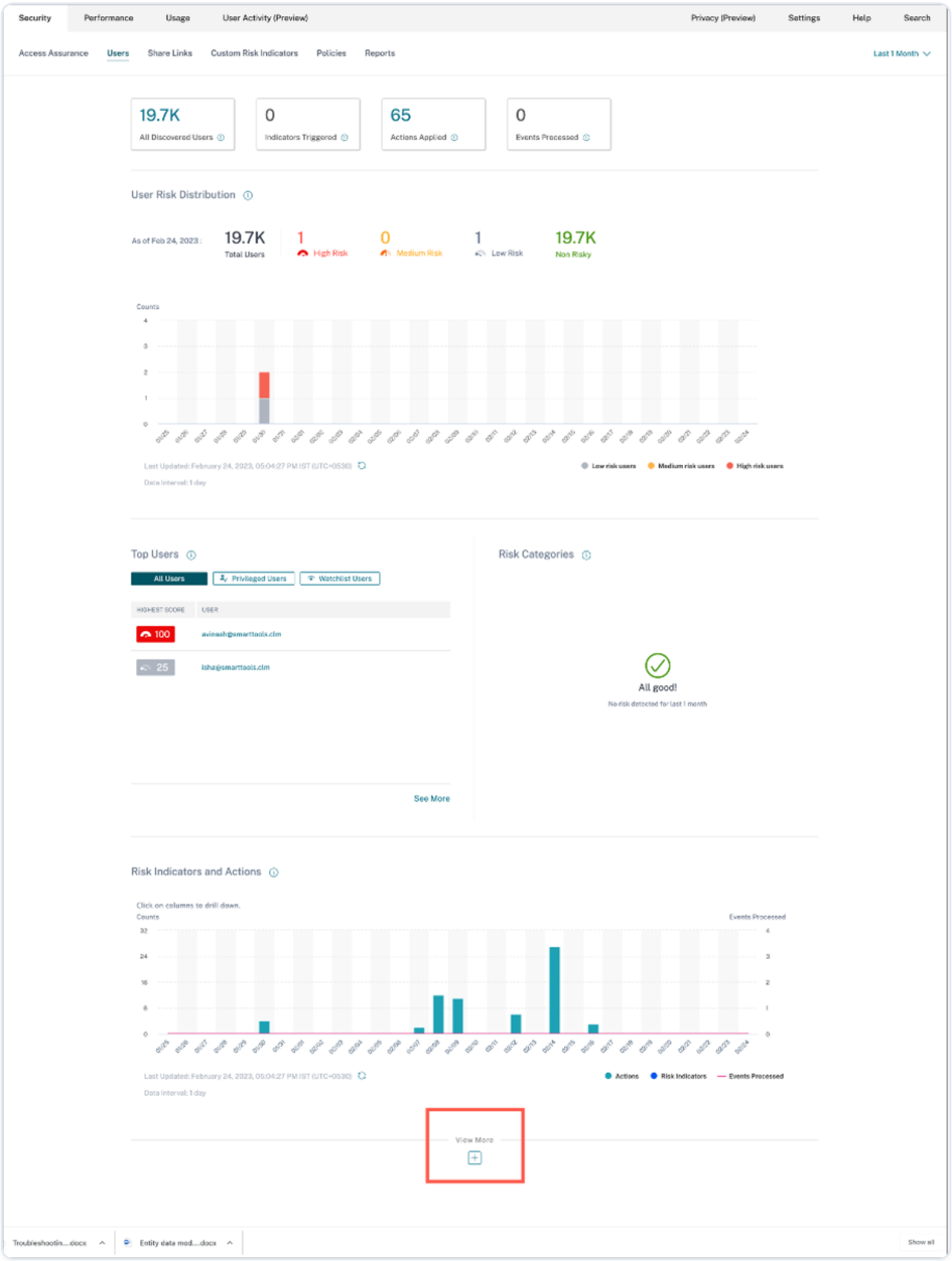
1. Navigate to **Citrix Analytics for Security™ dashboard > Custom Risk Indicators > Create Indicator**. You can create a custom risk indicator with any condition that assists you in monitoring the user's behavior. After you have set up the custom indicator, all the users who trigger the associated condition are visible in your Splunk environment.

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



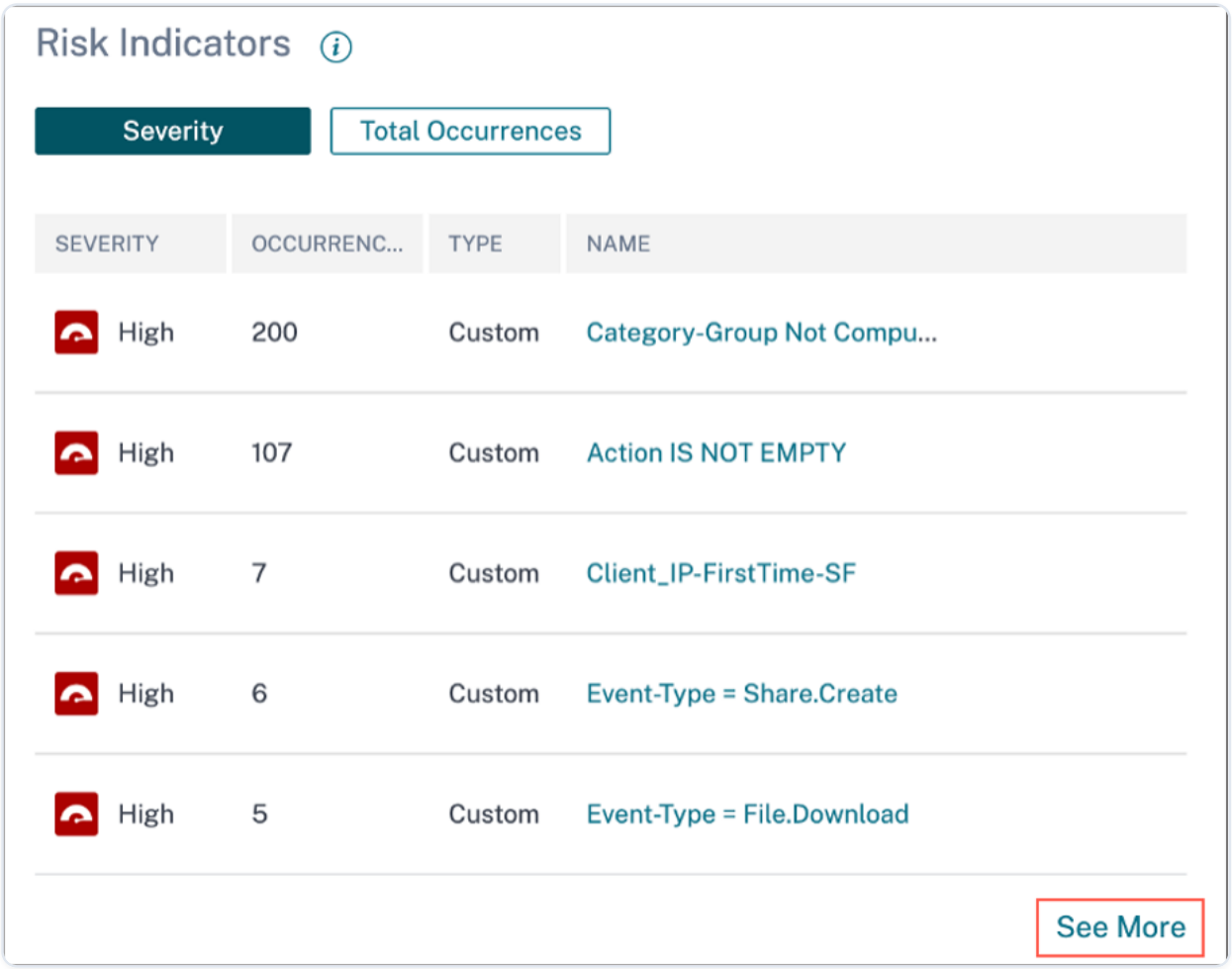
2. To view the created risk indicator occurrences on the Citrix Analytics for Security, navigate to **Security > Users. Navigate to the bottom of the page and click the plus (+) icon**.

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

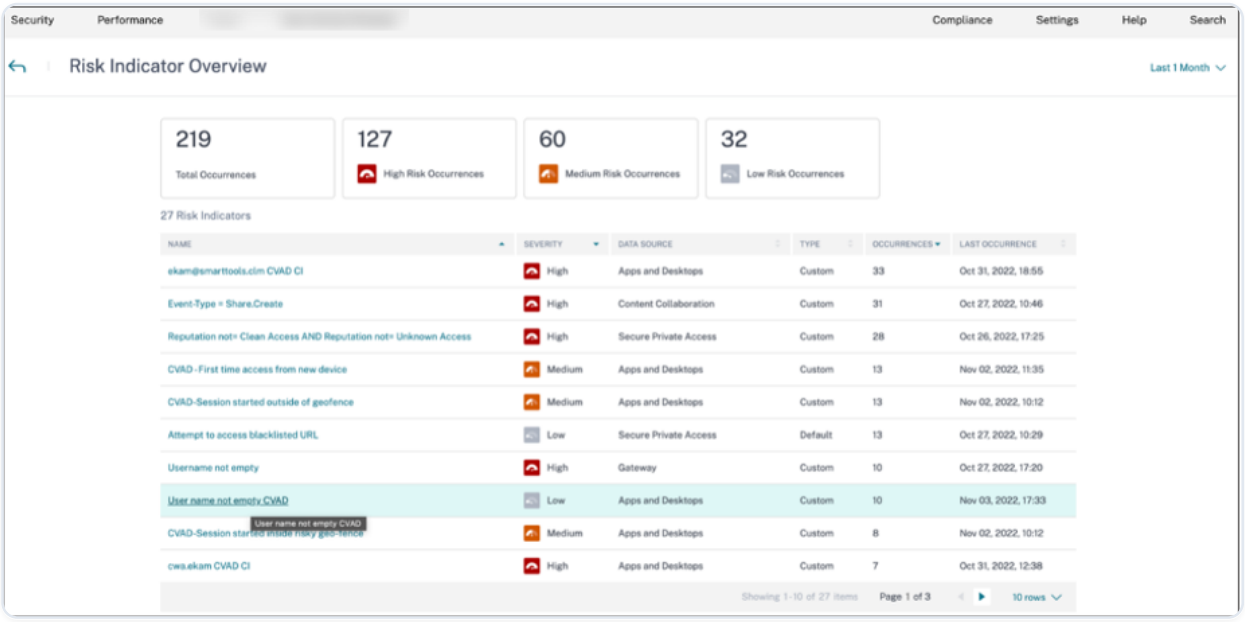


The Risk Indicators card appears. You can view the details of Risk Indicator, severity, and occurrence.

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

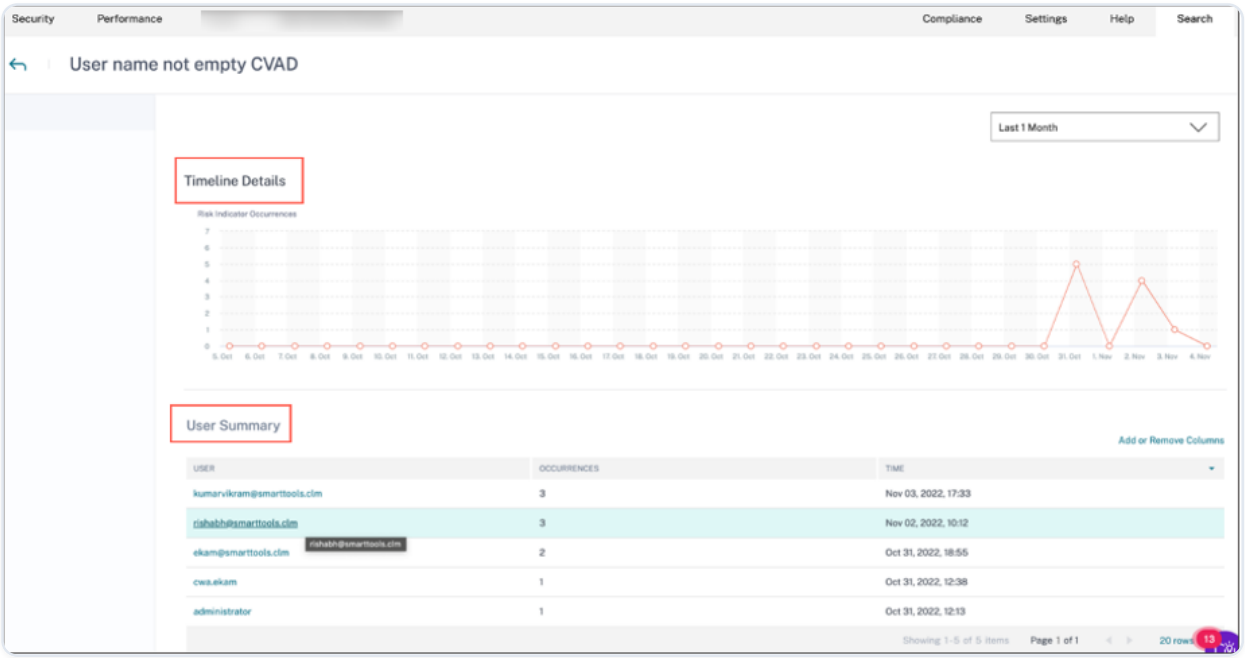


3. Click **See More**. The Risk Indicator **Overview** page appears.



In the Risk Indicator Overview page, you can view the user's details who have triggered the indicator with a detailed timeline view and user summary. To understand more about the timeline, see User risk timeline and profile.

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



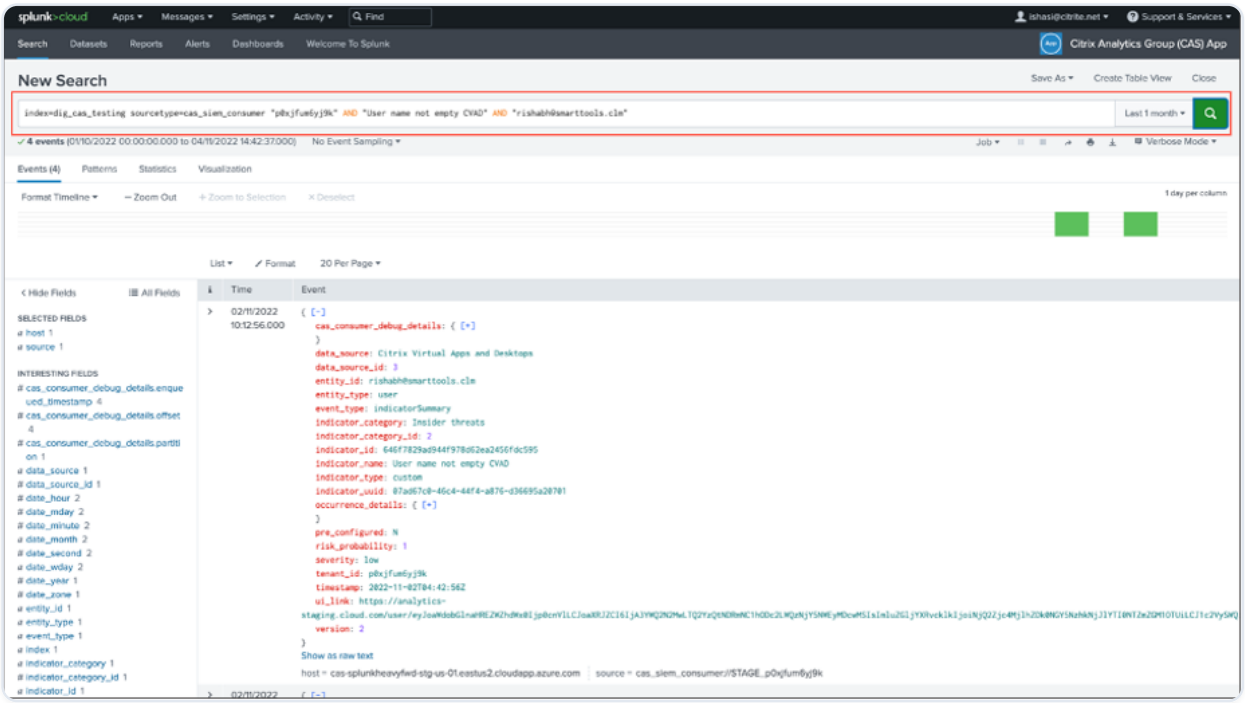
Risk Indicator Occurrences on Splunk - Raw Queries

You can also get the client IP and OS information by using the index and source type that was used by the Splunk infrastructure administrator while setting up the data input on Splunk Enterprise for Citrix Analytics for Security Add-on.

1. Navigate to **Splunk > New Search**. In the search query, enter and run the following query:

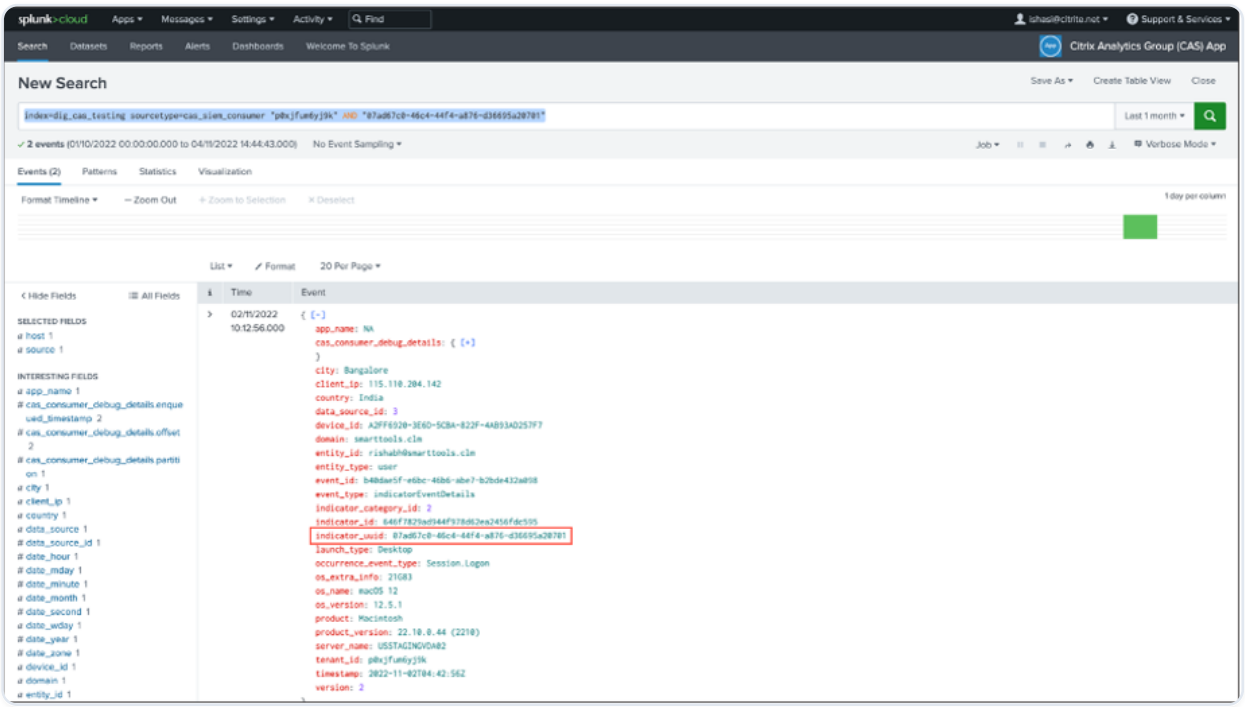
```
index=<index configured by you> sourcetype=<sourcetype configured by you> AND "<tenant_id>" AND "<indicator name configured by you on CAS>" AND "<user you are interested in>"
```

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



2. Pick up the indicator_uuid and run the following query:

```
index=<index configured by you> sourcetype=<sourcetype configured by you> "<tenant_id>" AND "<indicator_uuid>"
```



The event result contains the **Indicator Event Summary** and **Indicator Event Details** (the activity that is triggered by your indicator). The event detail contains the **Client IP** and **OS information** (name, version, extra information).

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

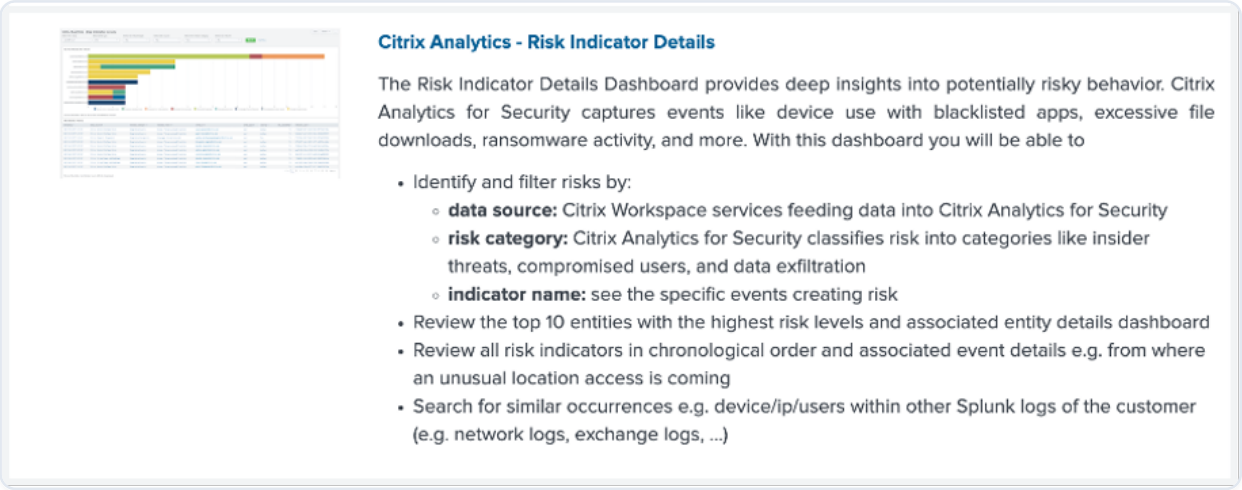
To understand more about the data format, refer Citrix Analytics data exports format for SIEM.

Risk Indicator Occurrences on Splunk - Dashboarding App

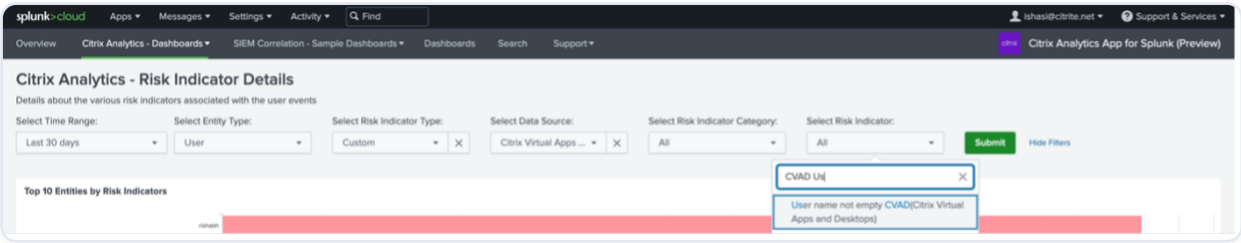
Refer the following articles for guidance on how to install Citrix Analytics App for Splunk:

- Citrix Analytics App for Splunk
- Citrix Analytics dashboards for Splunk

1. Click **Citrix Analytics – Dashboard** tab and select the **Risk Indicator Details** option from the drop-down list.

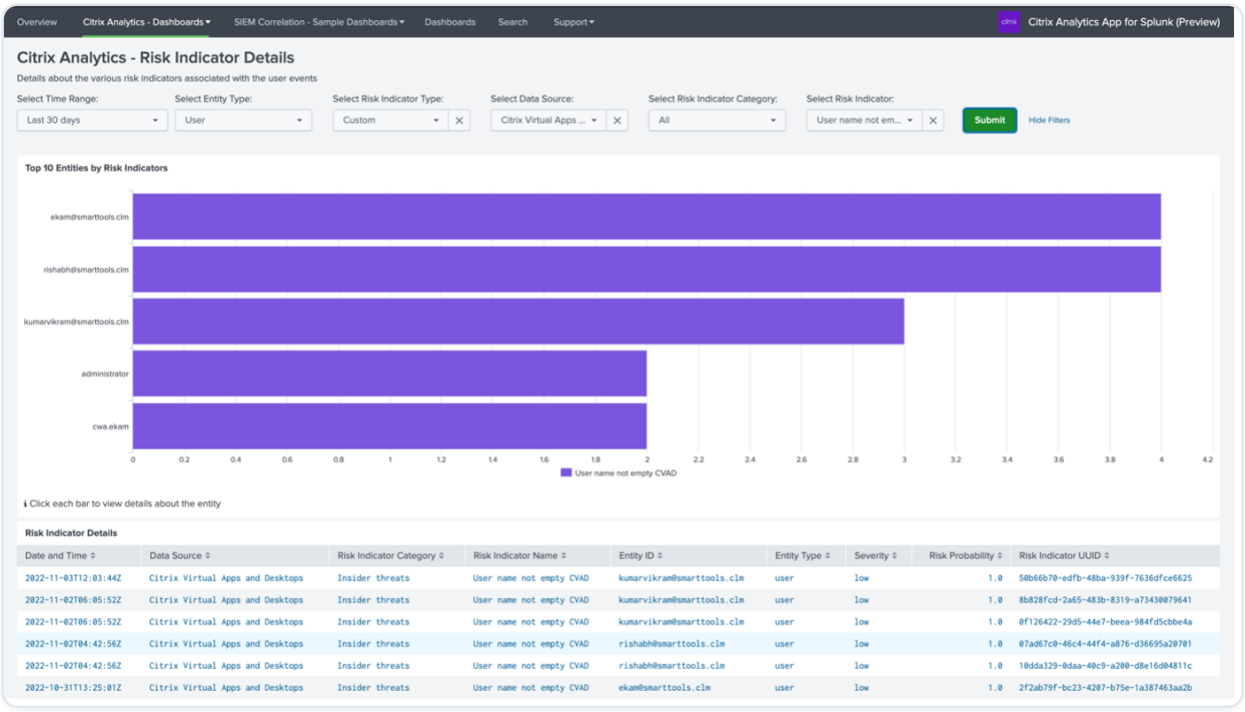


2. Filter the content appropriately from the drop-down list and click **Submit**.

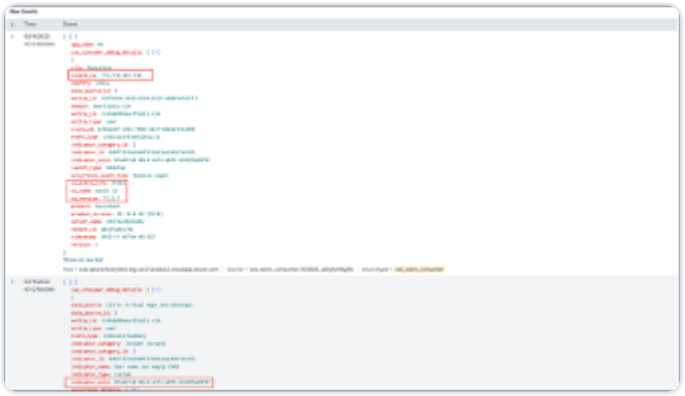


3. Click the user instance to get the details.

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



4. You can view the **Client IP** and **OS information** (name, version, extra information) at the bottom of this page:



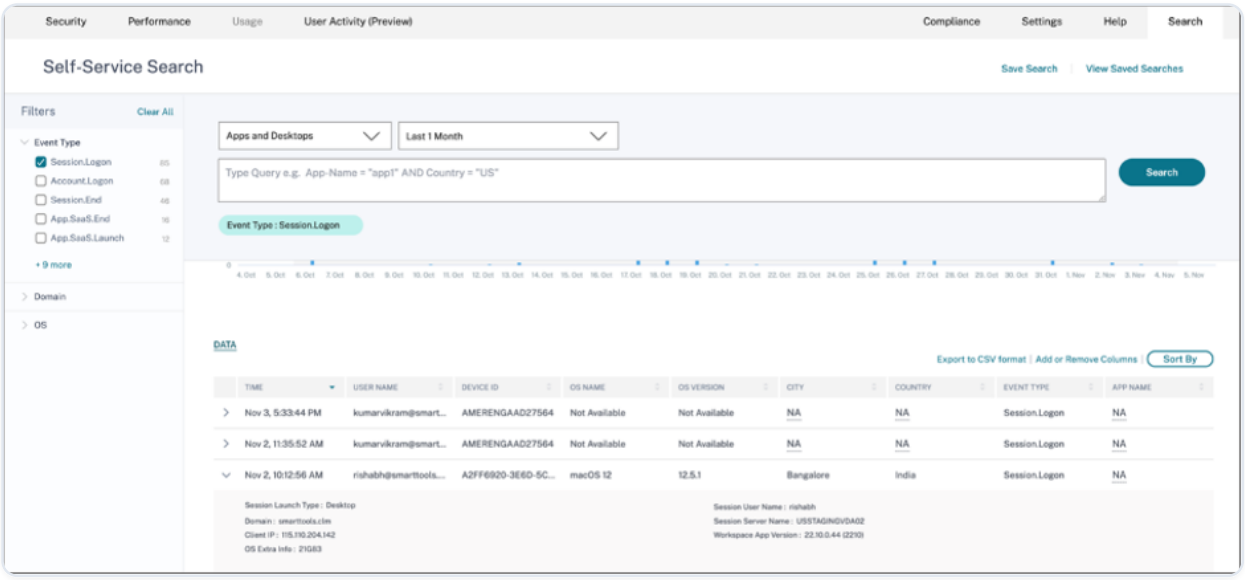
Data source events

Another method to get the Client IP and OS details in your Splunk environment is by configuring Data source events for export. This capability lets events present in the Self-Service Search view flow directly into your Splunk environment. For more information on how to configure event types for Virtual Apps and Desktops to be exported to SIEM, refer the following articles:

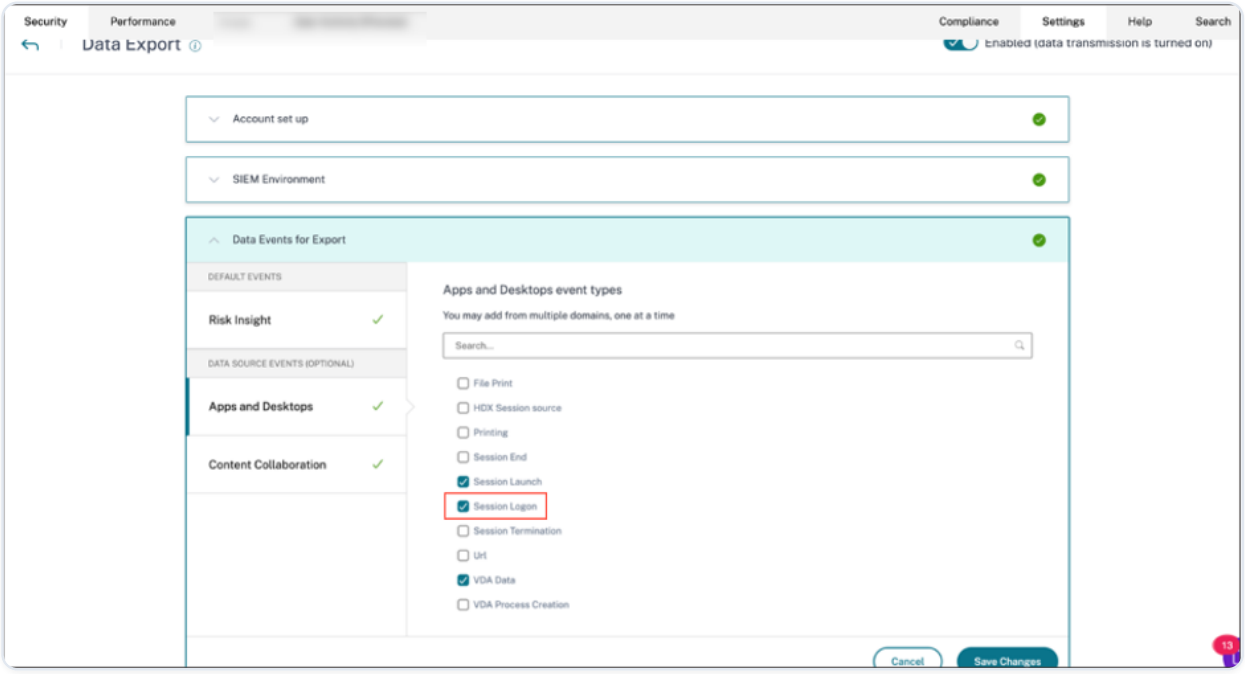
- Data events exported from Citrix Analytics for Security to your SIEM service.
- Data source events

1. Navigate to **Citrix Analytic for Security dashboard > Search**. In this Self-Service Search page, all the event types and its related information are available. You can see the **Session.Logon** event type as an example in the following screenshot:

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



2. Configure **Session.Logon** in Data source events for Export and hit **Save** to let it flow into your Splunk environment.

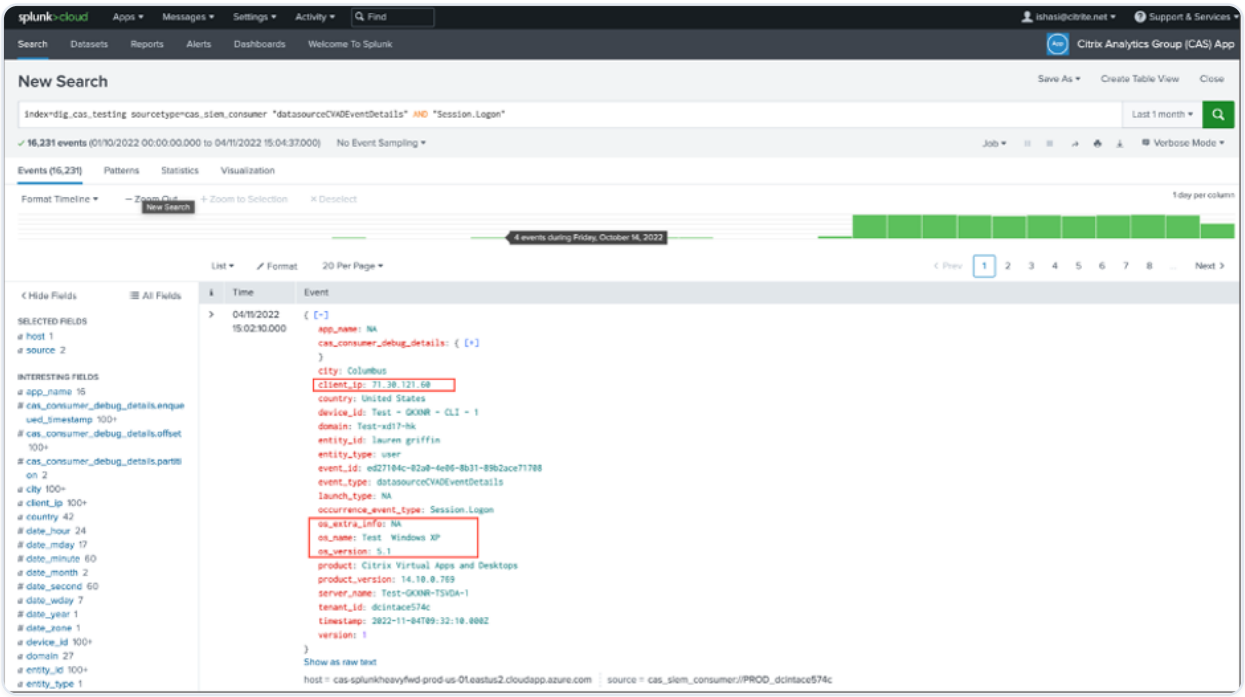


3. Go to Splunk then enter and run the following query:

```
index="<index you configured>" sourcetype="<sourcetype you configured>"
"<tenant_id>" AND "datasourceCVADEventDetails" AND "Session.Logon"  AND
"<user you're interested in>"
```

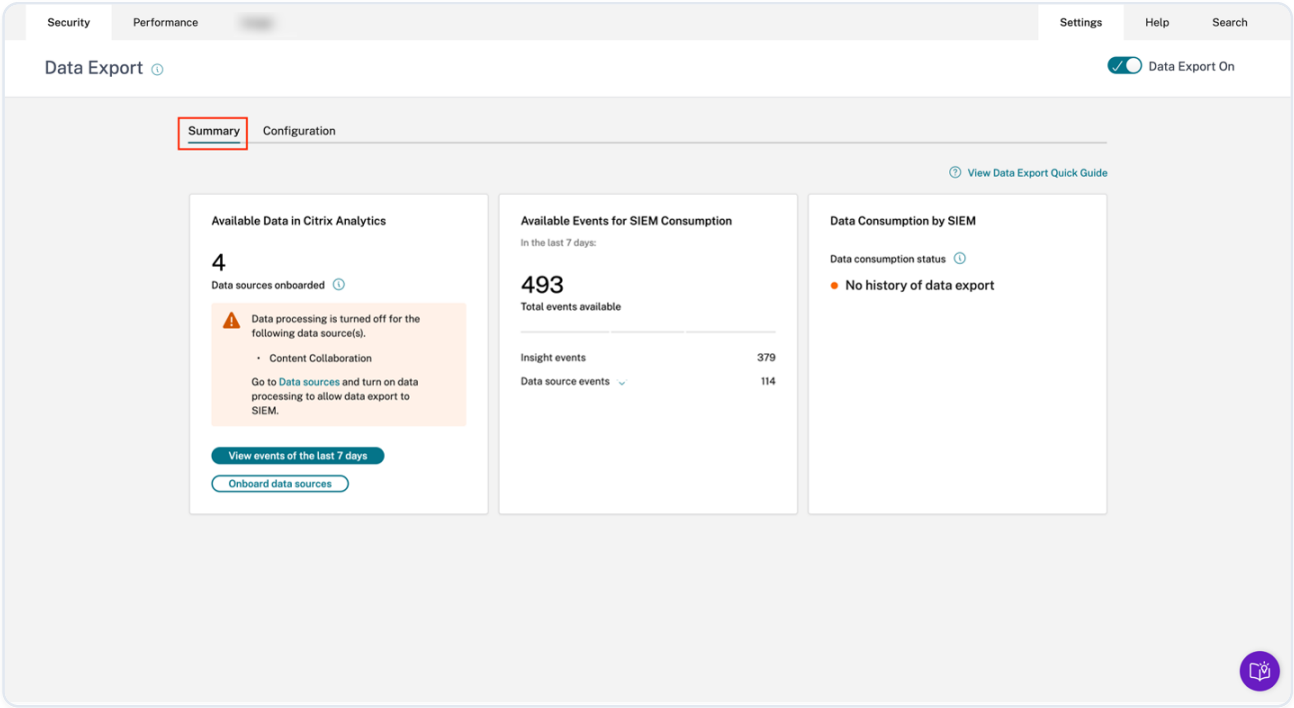
The fields pertaining to Client IP and OS are highlighted.

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



Troubleshooting Data Exports

The Data Exports for Security view includes a **Summary** tab to help administrators troubleshoot their SIEM integration with Citrix Analytics. The **Summary** dashboard provides visibility into the health and flow of data by taking them through the checkpoints that aid the troubleshooting process.



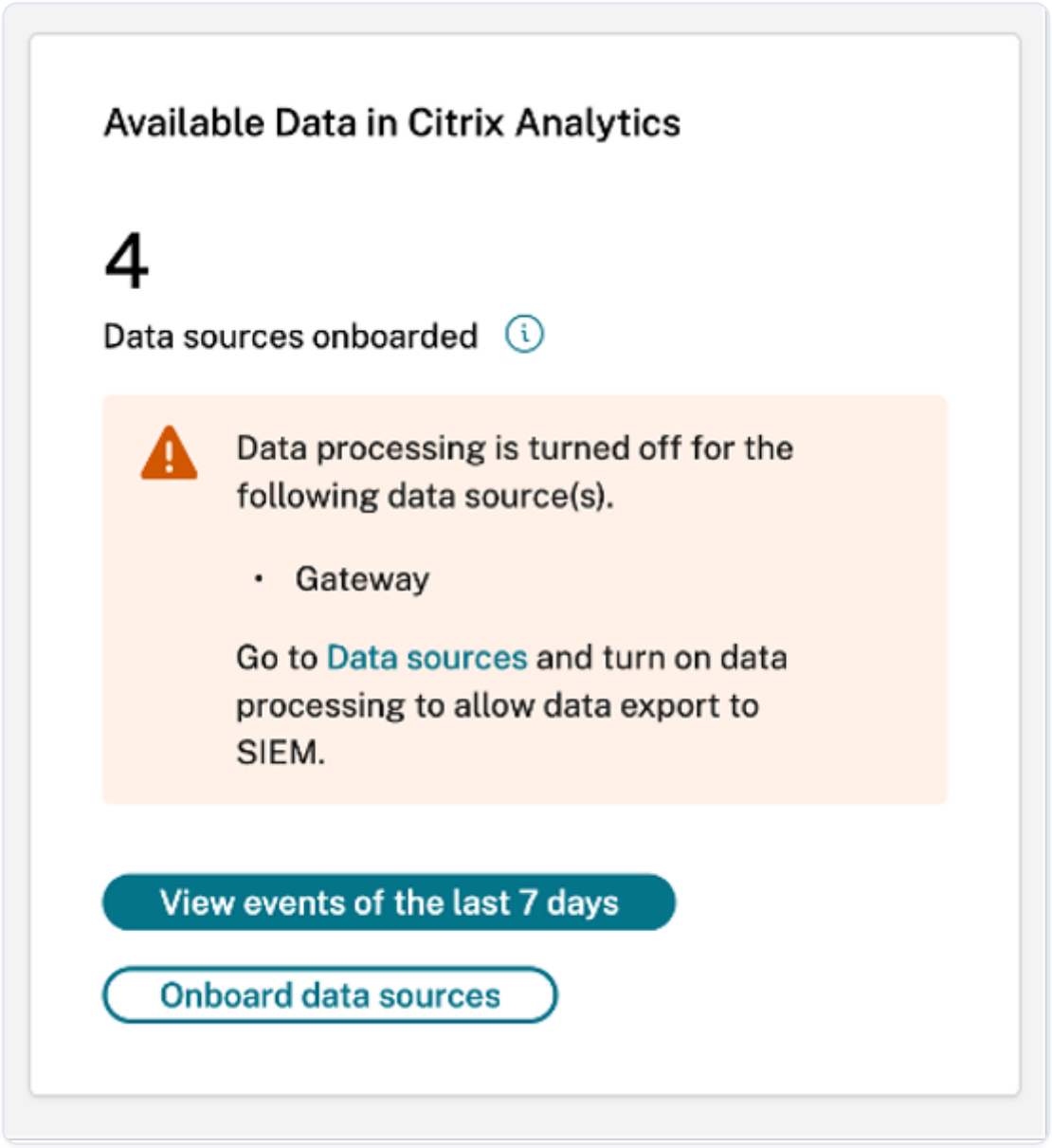
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Summary tab

The **Summary** tab forms the foundation of the self-service troubleshooting workflow in the Data Exports view. It describes your SIEM setup by using these three cards:

- **Available Data in Citrix Analytics**: This card shows the state of your data source configurations.
- **Available Events for SIEM Consumption**: This card displays the number of events that are ready to be consumed by your SIEM environment.
- **Data Consumption by SIEM**: This card displays the state of data flow in your SIEM environment.

Available data in Citrix Analytics

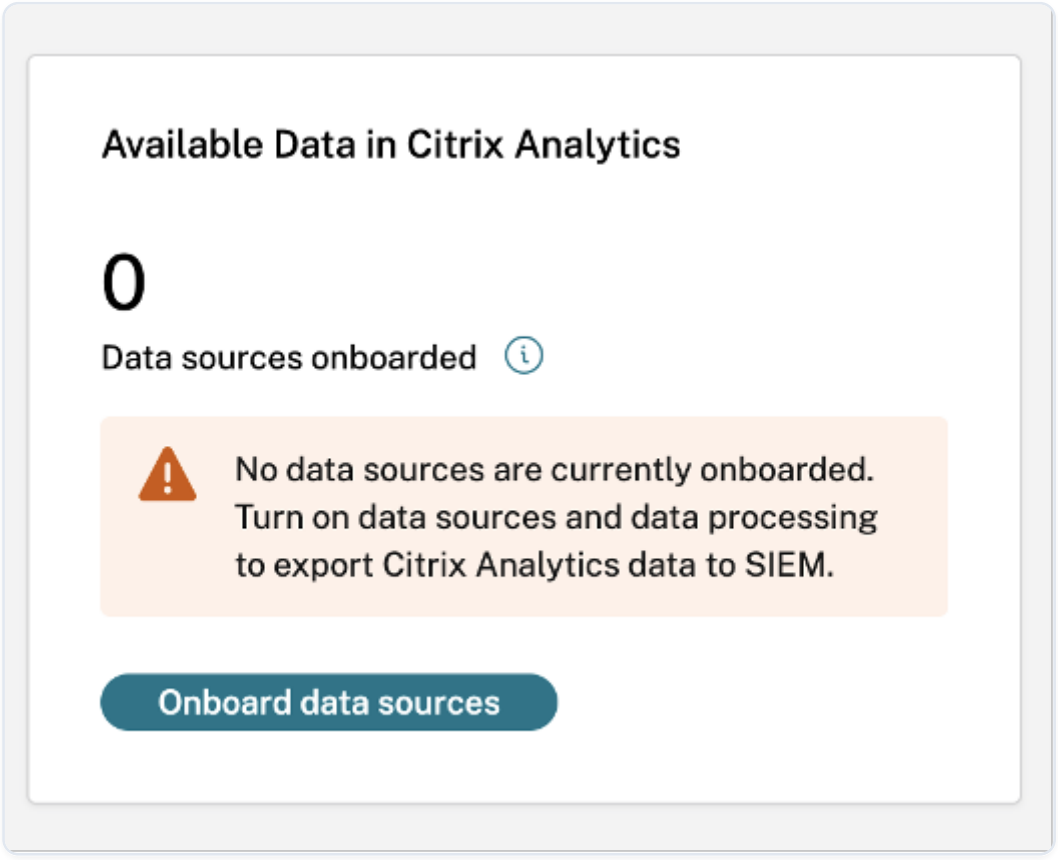


© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Available Data in Citrix Analytics** card shows the number of data sources that can eventually contribute to SIEM insights that have been onboarded to Citrix Analytics for Security. Three data sources are supported for data exports currently – Apps and Desktops, Gateway, and Secure Private Access. Even if these data sources have been onboarded, data export will not function for the data sources that have their data processing turned off. An appropriate warning message such as the one depicted in the image above is shown when such data sources are detected.

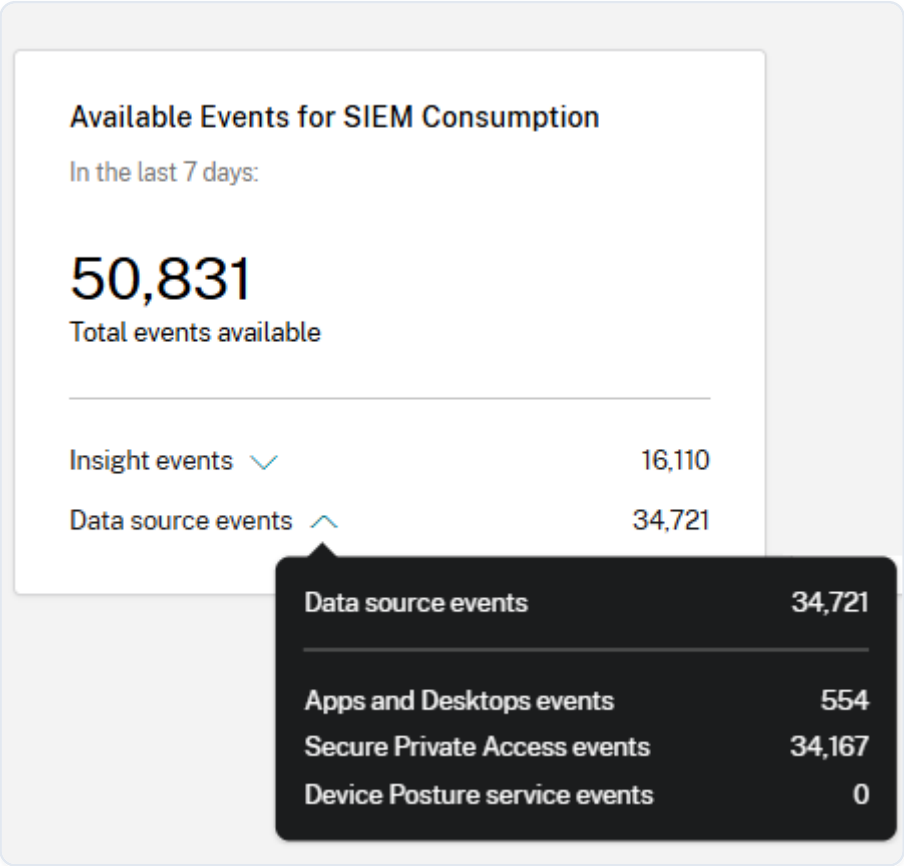
The **View events of the last 7 days** button redirects the administrator to the Self-Service Search view, through which administrators can verify that events have flowed into Citrix Analytics for Security. The **Onboard data sources** button redirects to the Data Sources view where you can be walked through the onboarding process in depth.

If there are no onboarded data sources, an appropriate warning message is displayed as shown in the following screenshot:



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

Available events for SIEM consumption



The **Available Events for SIEM Consumption** card displays the number of Insight and Data source events along with their breakdown that are expected to flow into your SIEM environment. Upon expanding, a further breakdown of each type of data event for export is also available.

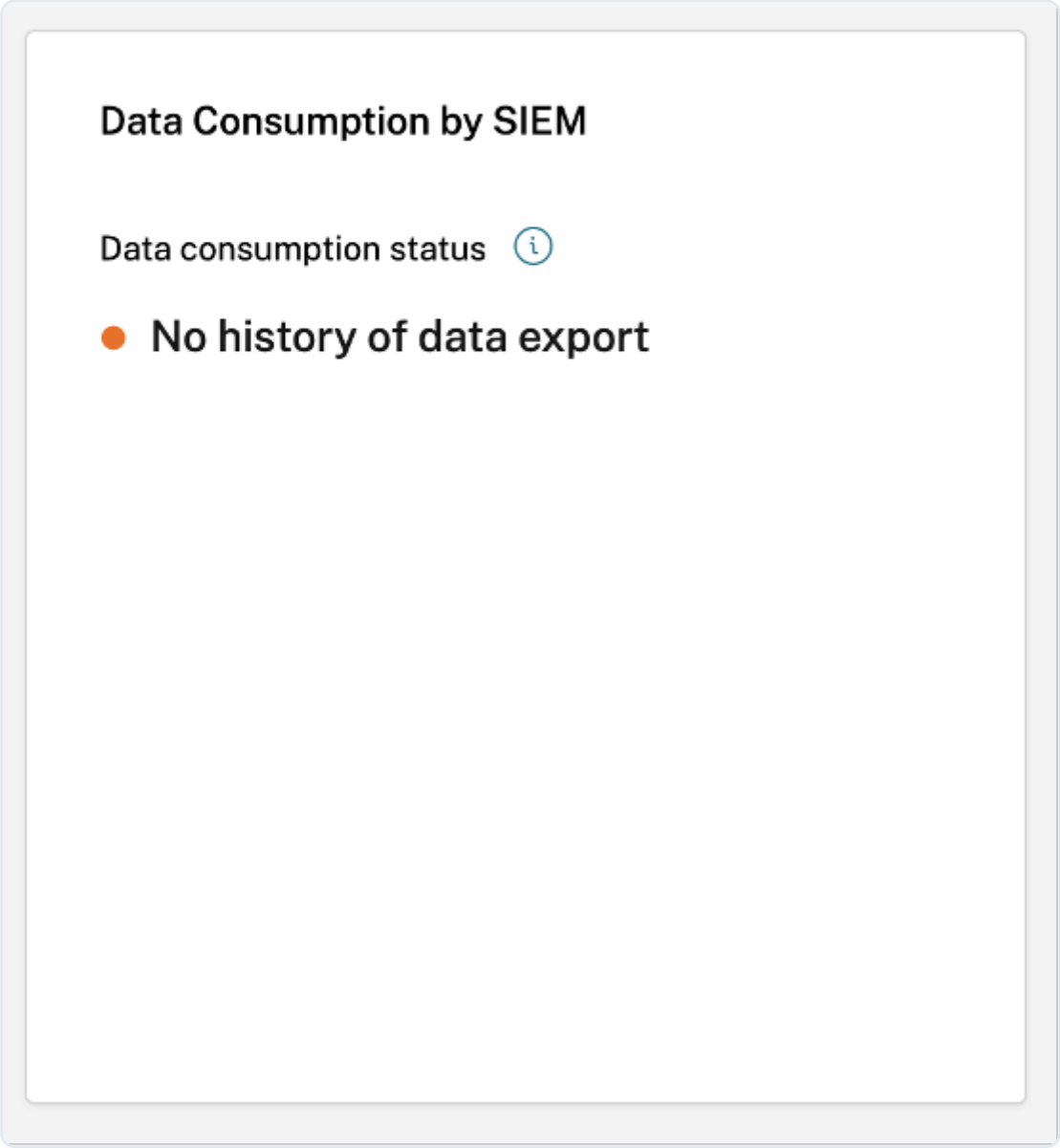
Data consumption by SIEM

The **Data Consumption by SIEM** card depicts the health of the flow of data prepared by Citrix Analytics into your SIEM environment. The data consumption status is based on the offset movement within your **Kafka** topic. When available, the card also shows the timestamp of when successful data consumption was last detected. Both the data consumption status and the timestamp are refreshed every 10 minutes. Click here to learn more about Kafka consumer group/ offset management.

The data consumption status can take on the following states:

1. **Inactive Consumption**
    - **No history of data export**: This state is represented by an orange dot to indicate that no data prepared by Citrix Analytics has ever flown successfully into your SIEM environment.

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



This can be due to -

- Incorrect/Incomplete data source configuration. The **Available Data in Citrix Analytics** card can be used to verify if there are enough data sources, and if they have their data processing turned on to allow for export.
- Lack of user activity. The **View events in the last 7 days** button in the **Available Data in Citrix Analytics** card can be used to verify the absence of user activity. Further, the **Available Events for SIEM Consumption** card can be used to verify if there are any Insight or Data source events readied by Citrix Analytics to flow into your SIEM.
- Incorrect/Incomplete SIEM setup. Verify that the Account Setup stage in the **Configuration** tab has been completed successfully. A green tick mark is visible in the Account Setup stage if the setup is complete.

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

If the state does not change even after a successful account setup, troubleshoot further by checking for:

- Firewall issues or misconfigured SIEM settings – refer Setting up SIEM environment.
- Credential issues with Kafka account setup or your SIEM environment – refer SIEM integration using Kafka.

- **No active consumption detected**: This state indicates that at least in the past 10 minutes, data has not flown successfully into your SIEM environment. The card will also display the timestamp of the last successful movement of data. As with **No history of data export**, you can troubleshoot this by using the **Available Data in Citrix Analytics** and **Available Events for SIEM Consumption** cards. If there is sufficient user activity along with the available events count increasing, it would be a good idea to focus on the last successful timestamp to check if any firewall changes or password rotations happened after the said timestamp.



- **Exported over 7 days ago**: This state indicates that active consumption on your SIEM was last detected over a week ago. Similar to the above two states, use the **Available Data in Citrix Analytics** and **Available Events for SIEM Consumption** cards to troubleshoot your SIEM setup if this is the detected data consumption state.

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



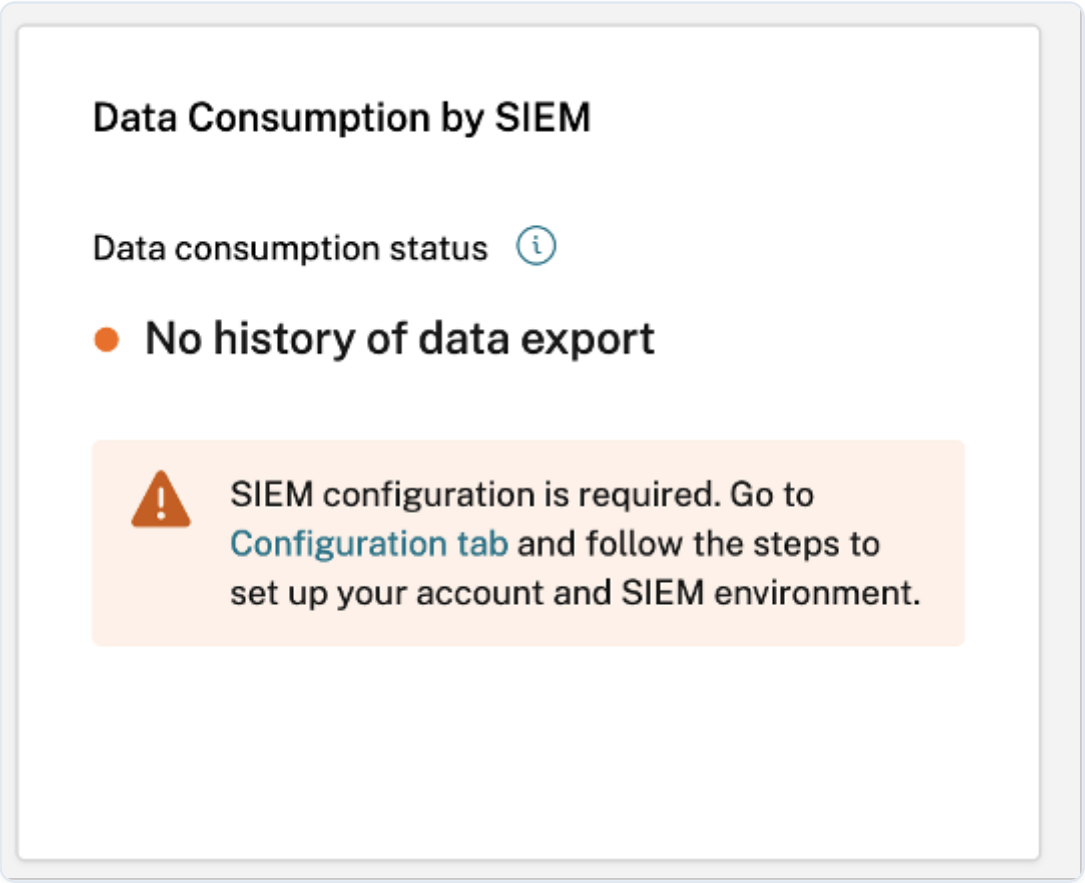
NOTE

Kafka Retention Policy: Citrix Analytics Kafka topics retain events for a maximum of 7 days only. To avoid or prevent potential data loss, it is recommended to set up a data poll interval that does not exceed 7 days.

In inactive consumption, you can view the following warning messages to help you navigate through the troubleshooting process.

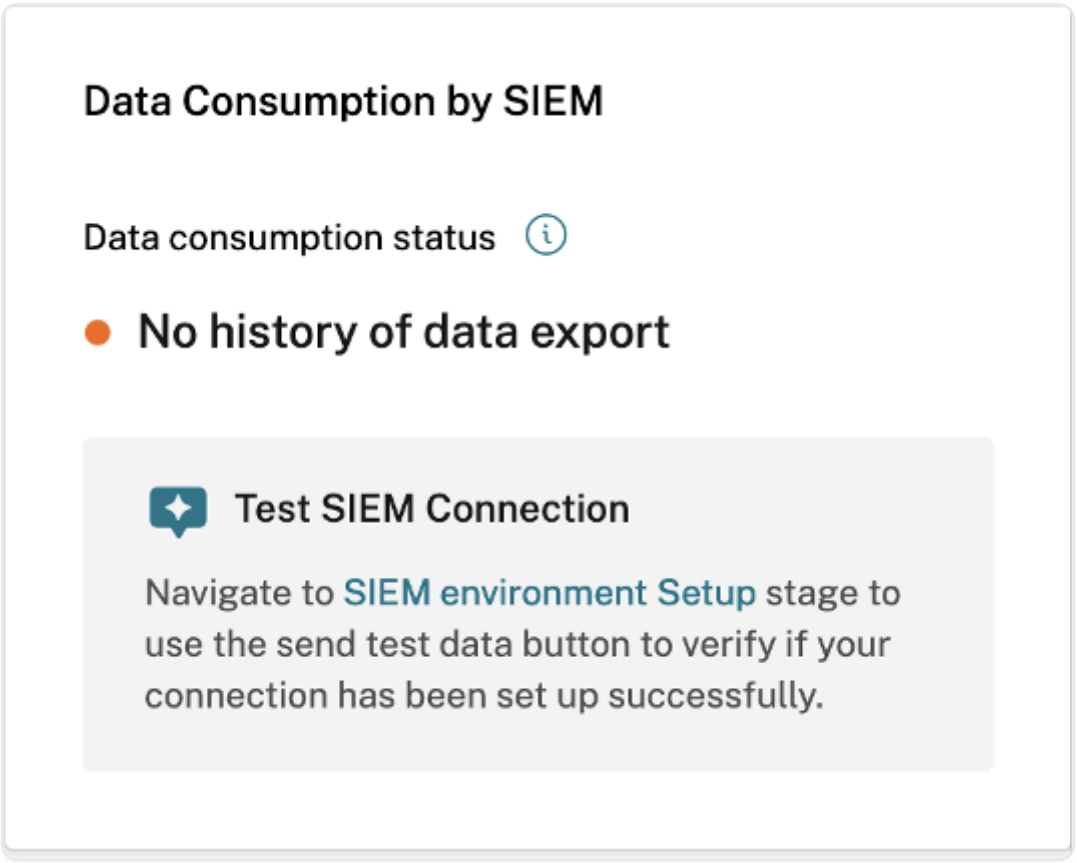
As highlighted in the **No history of Data Export** case, if the SIEM setup is not completed, no data ever flows into the SIEM Environment. Hence, the user is redirected to the **Configuration** tab to complete the account setup, as shown in the following screenshot:

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



If the SIEM setup is completed, it can still be the case that data is not actively flowing as depicted in the **No Active Consumption Detected** or **Exported over 7 days ago** state. Hence, the user is urged to go to the **Test Event Generation** section to test the SIEM connection as highlighted in the following warning message.

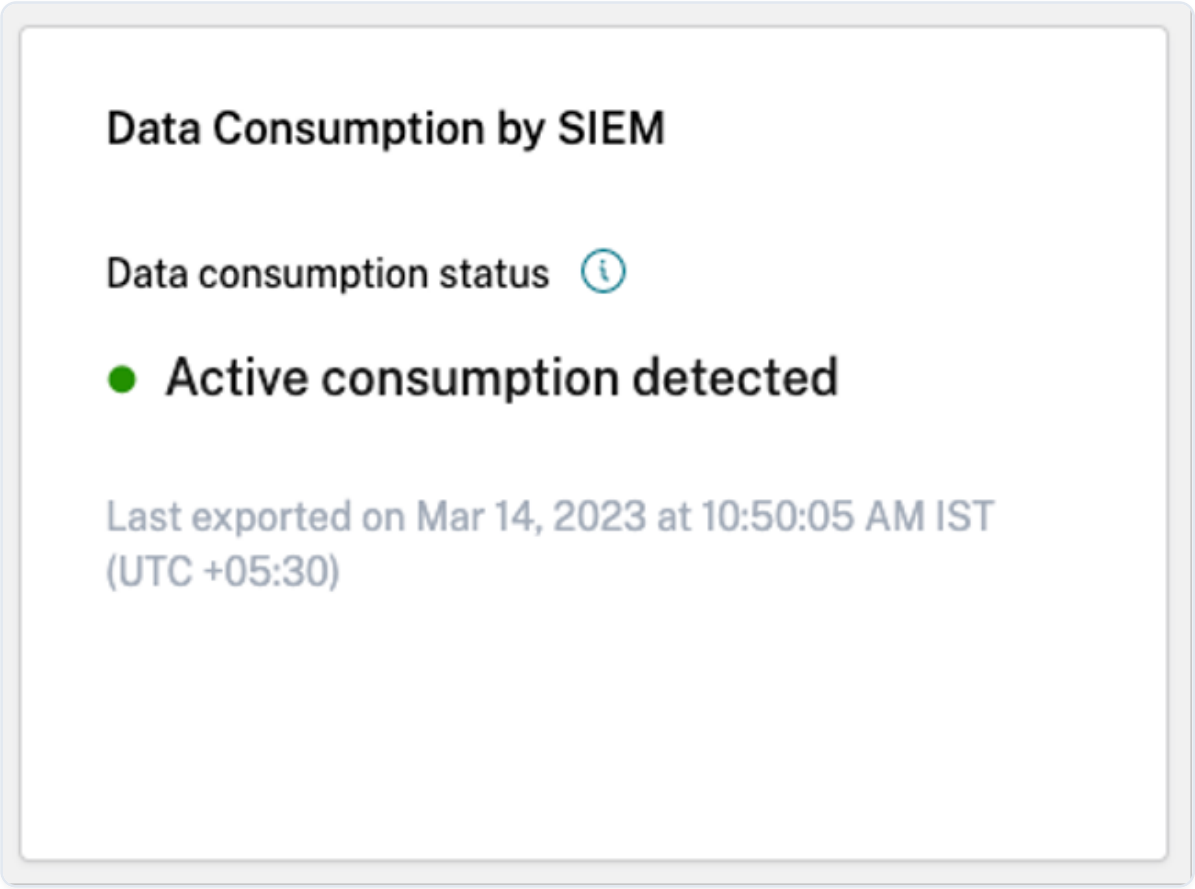
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. **Active Consumption**

    - **Active consumption detected**: This state indicates that active consumption has been detected on your SIEM.

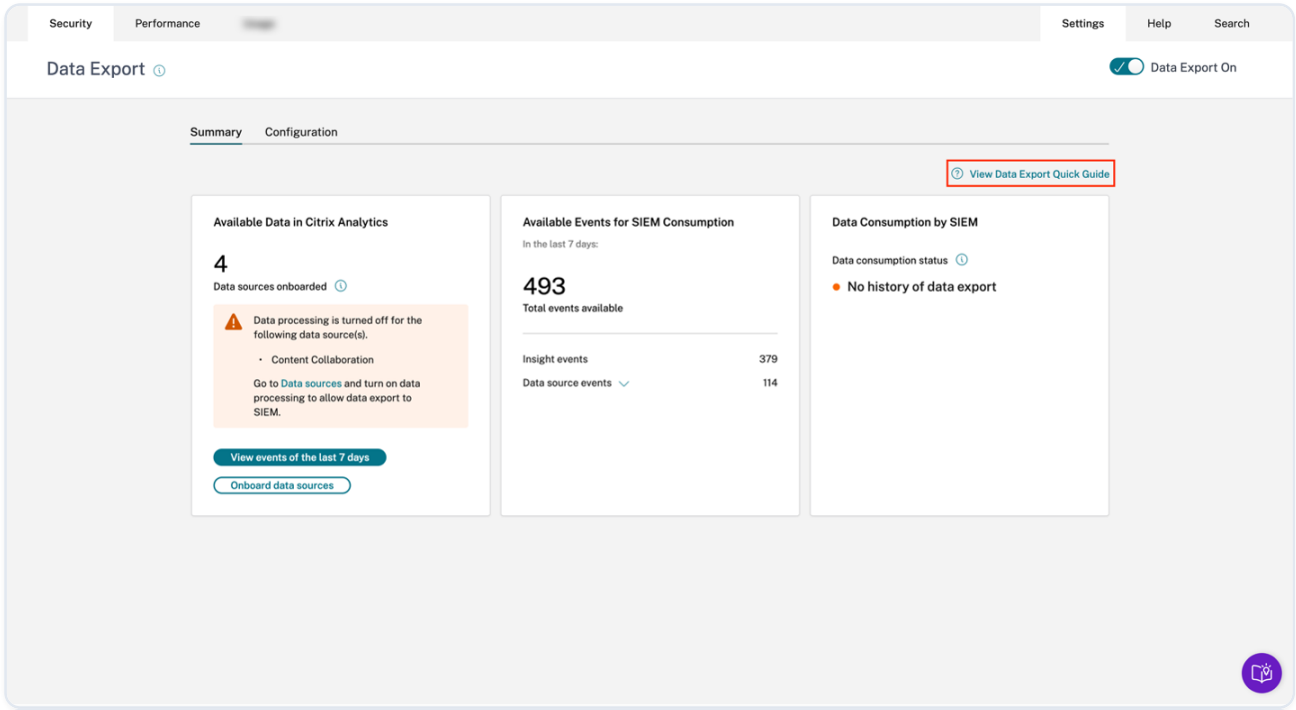
© 1997–2026 Citrix Systems, Inc. All rights reserved.

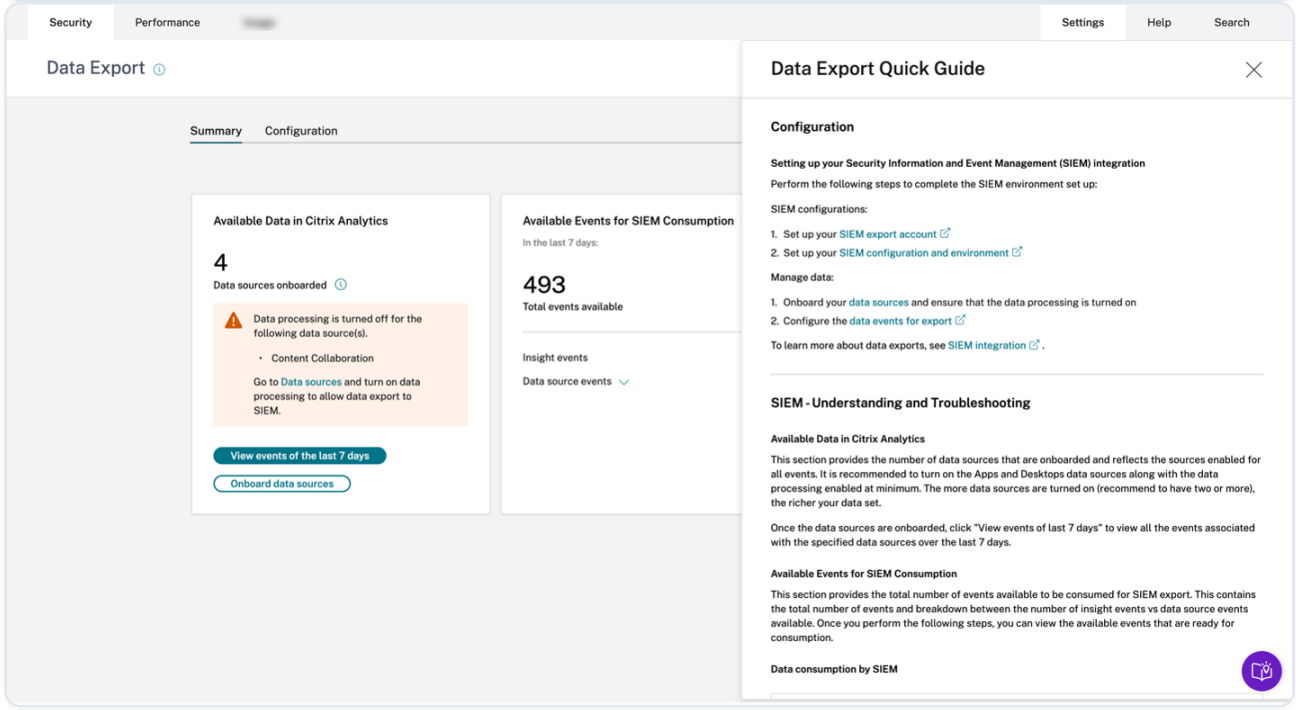


Data Export Quick Guide

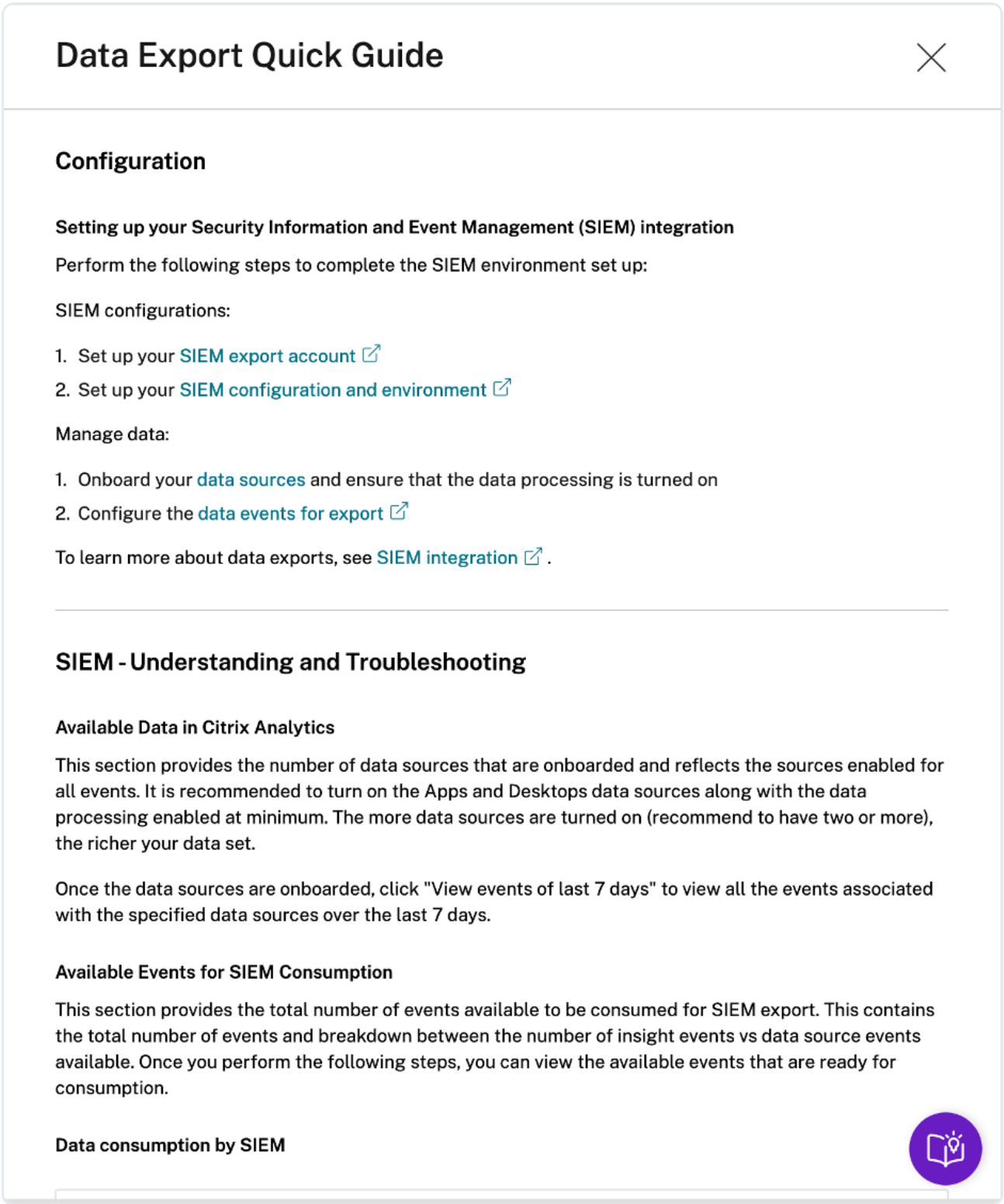
The **Summary** tab is supplemented with the **Data Export Quick Guide** blade to ease the deployment, management, and troubleshooting of your SIEM setups. In addition to providing a comprehensive guide to the Data Export for Security view, the Quick Guide also includes useful tips on how to set up and manage your SIEM environment by providing links to pertinent documentation.

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



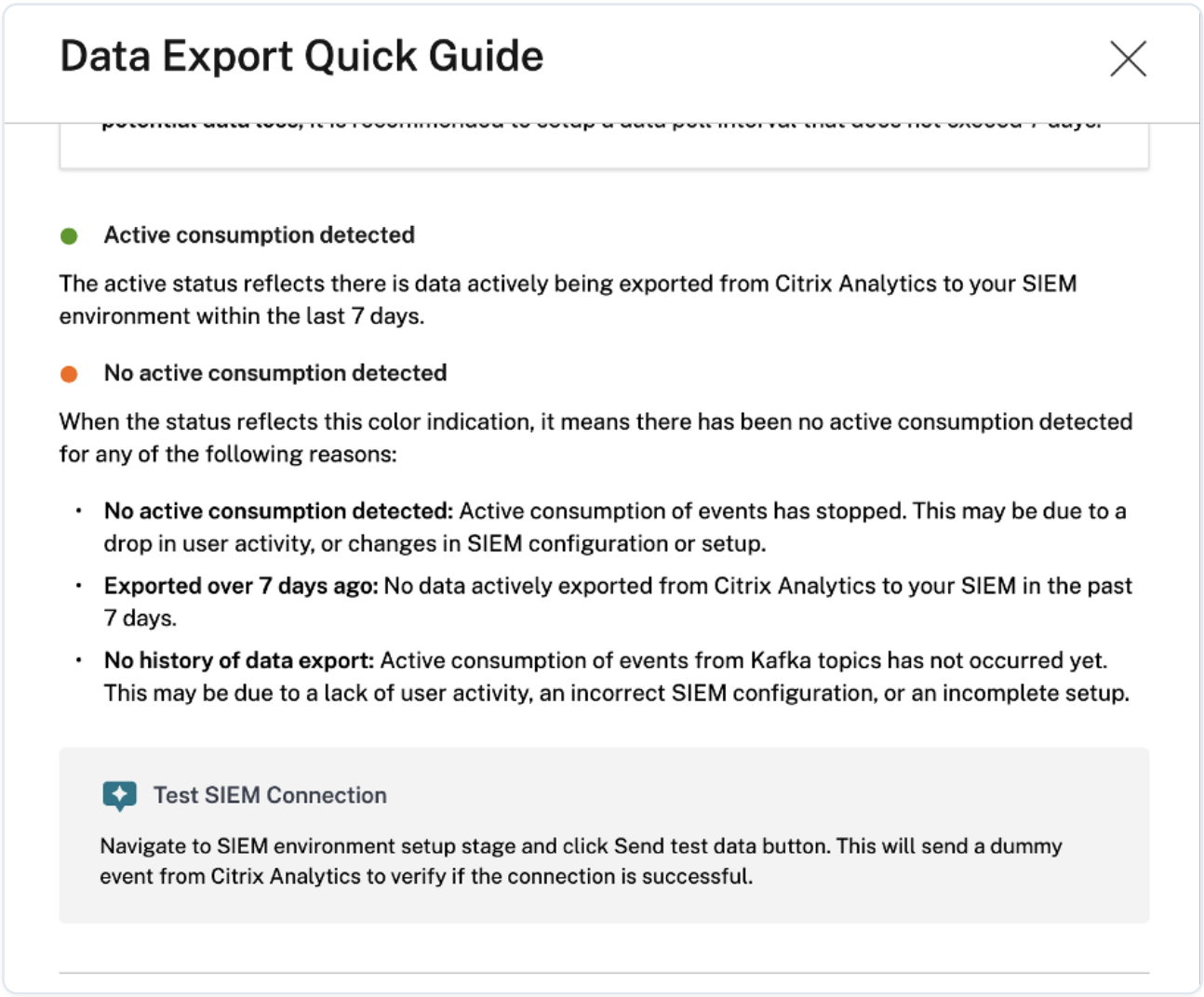


© 1997–2026 Citrix Systems, Inc. All rights reserved.



There is also a **Test SIEM Connection** section in the Quick Guide Blade that redirects the user to the Test SIEM Connection stage within the SIEM Environment setup stage. This enables the user to investigate if the SIEM Integration is itself broken, thereby ruling out the possibility of problems with Citrix Analytics for Security processing the events. The user can then fix the SIEM connection to enable data flow.

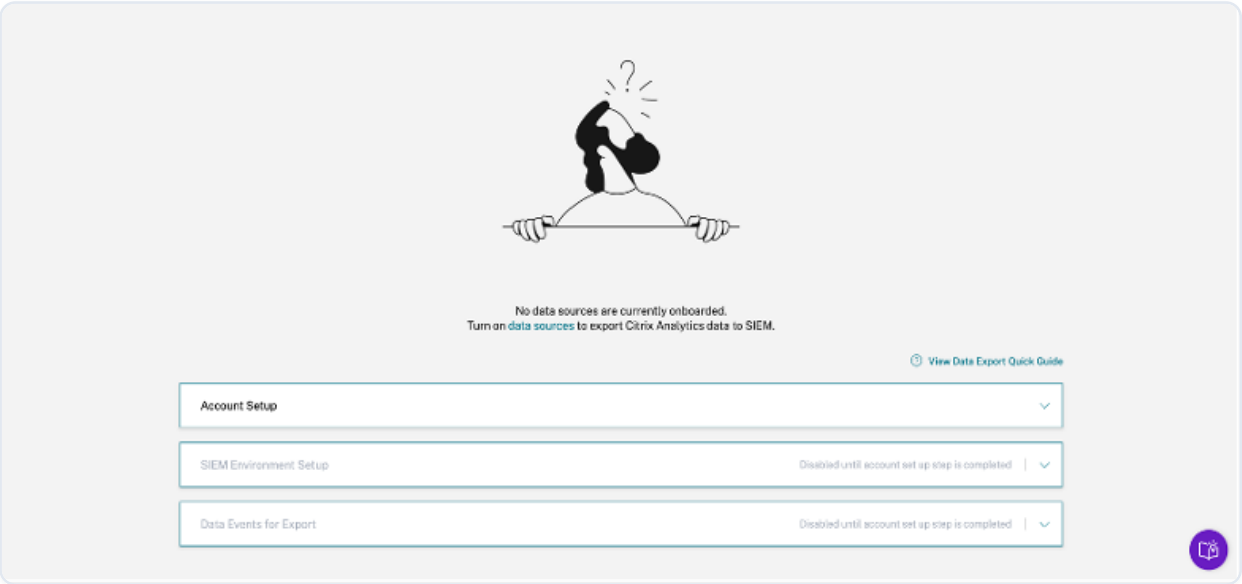
© 1997–2026 Citrix Systems, Inc. All rights reserved.



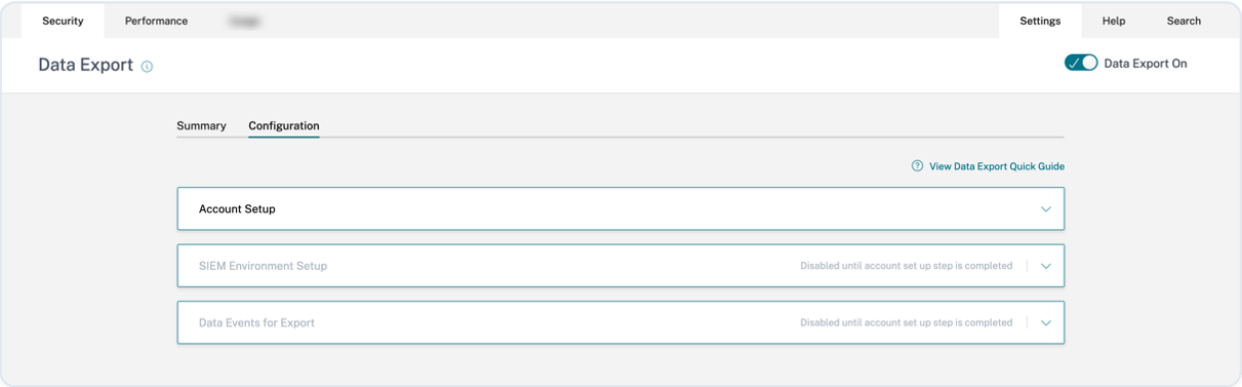
The **Configuration** tab, while guiding through deployment setup, also helps administrators with useful tips, warning messages, and common pitfalls while they set up their SIEM. Appropriate warnings are shown when:

- Citrix Analytics detects that no data sources have been onboarded. It is recommended that Apps and Desktops is onboarded to collect telemetry based on user activity. In the absence of the onboarded data source, no data flow is observed, even though your SIEM setup might have been done successfully.

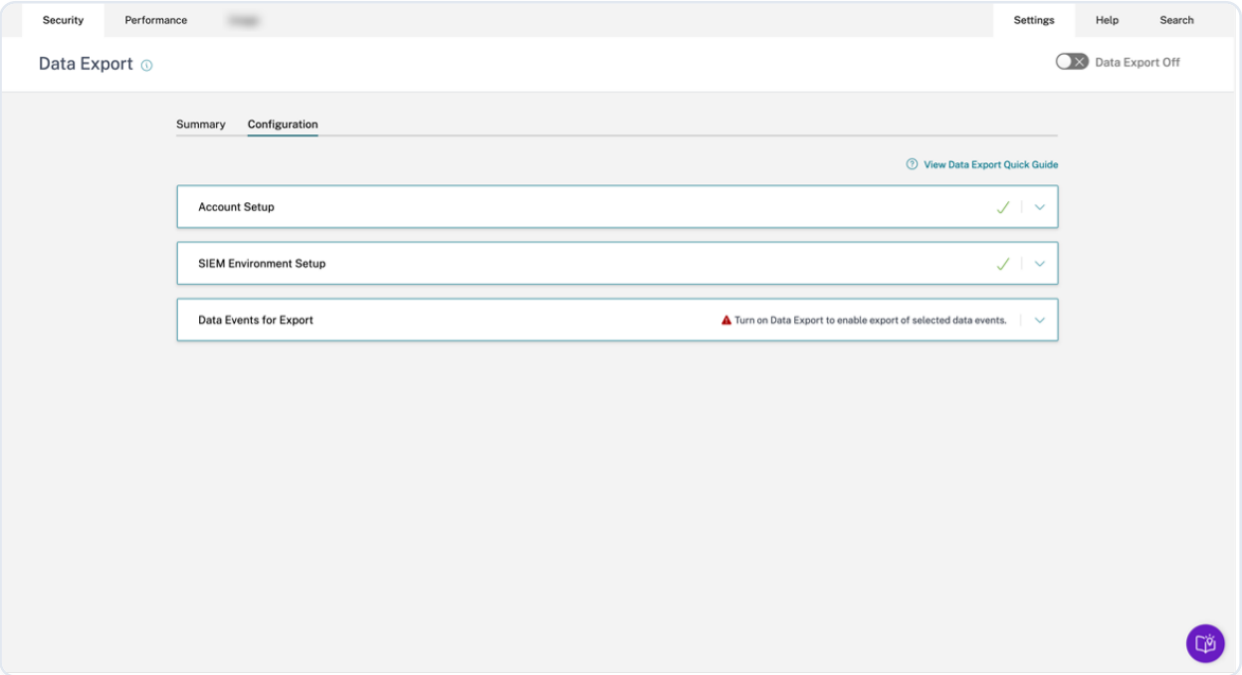
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- As illustrated by the following image, the SIEM Environment Setup and Data Events for Export stages are disabled until the account setup is completed successfully.

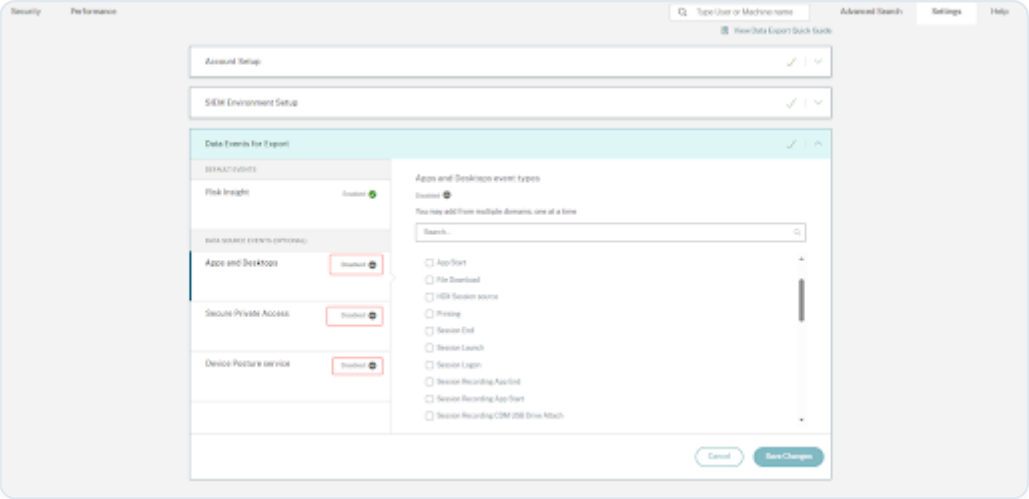


- Data Exports have been turned off. The warning on the Data Events for Export stage serves as a reminder to enable Data Exports to effectuate any changes.



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

- On the Data Events for Export stage, if data export for a particular data source is disabled, then no Data source events flow to SIEM. You must enable this by configuring and selecting the desired Data source events' types. Furthermore, make sure that Data processing for the respective data source is enabled to make sure data reaches Citrix Analytics.

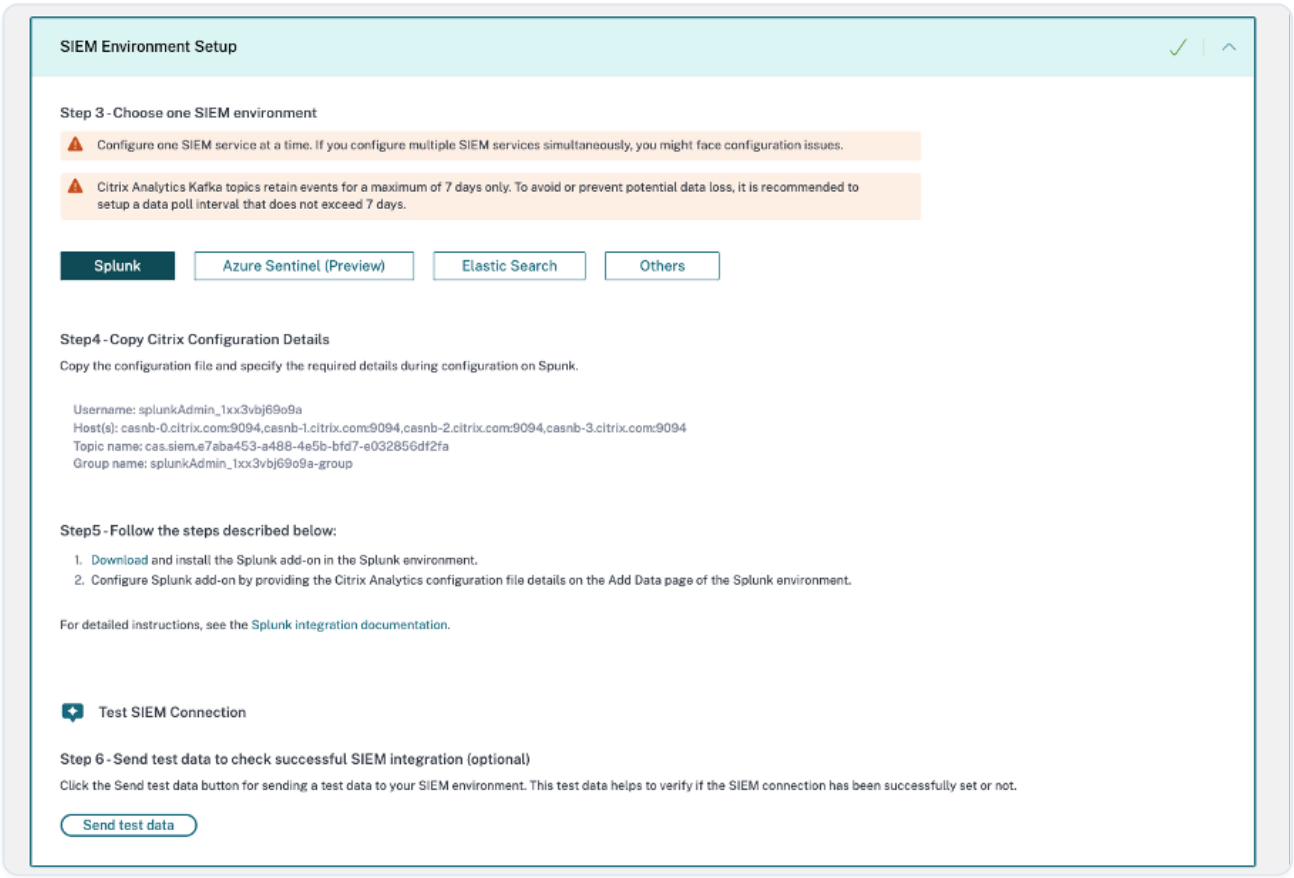


Test Event Generation

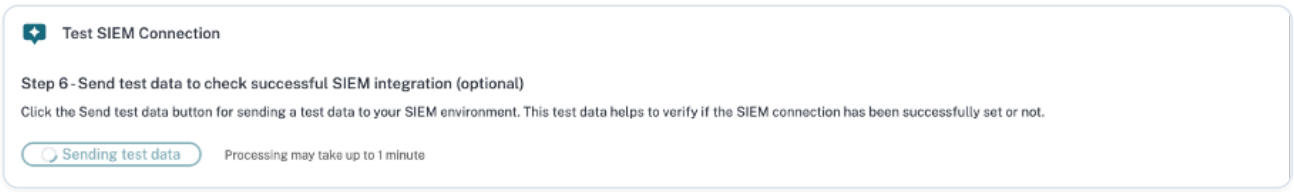
Test Event Generation is provided as a part of the **SIEM Environment Setup** stage to enhance the troubleshooting experience. Once a user completes the SIEM setup, Test Event generation provides a way to quickly test the SIEM connection by sending a test event directly into the customer's SIEM data export Kafka topic.

It also enables new users to quickly test their SIEM Integration with Citrix Analytics without having to explicitly onboard a new data source and subsequently generate user activity.

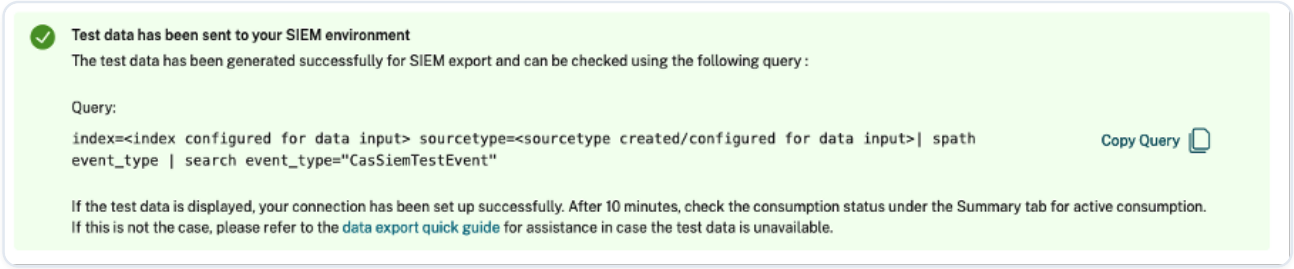
© 1997–2026 Citrix Systems, Inc. All rights reserved.



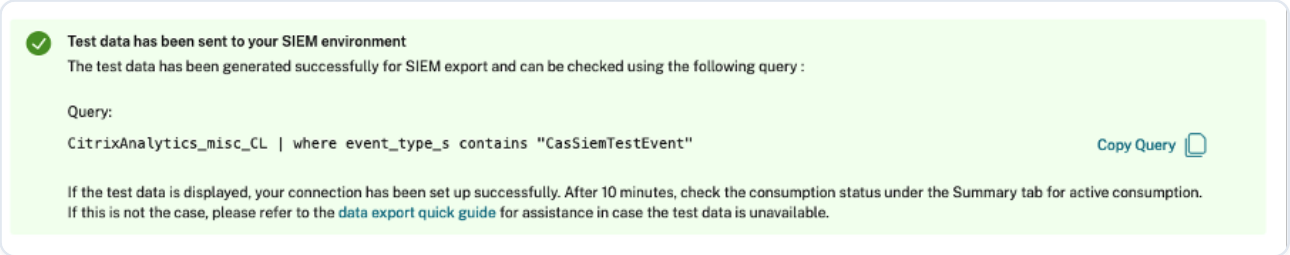
To test this functionality, the user needs to click the **Send Test Data** button. This generates a dummy test event and sends it to the customer's SIEM data export Kafka topic. This test event generation process might take up to 1 minute as shown in the following screenshot:



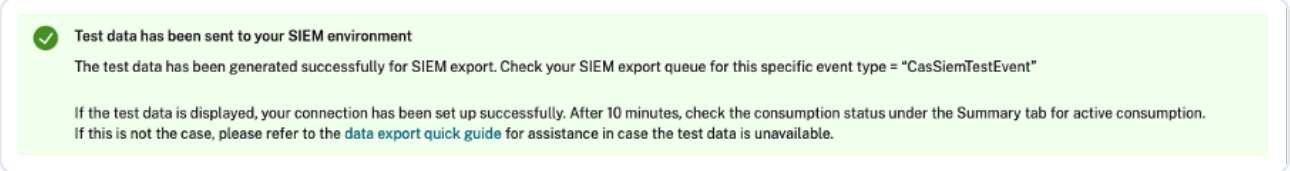
If the test event data is successfully written in the customer Kafka topic, a success message is displayed, indicating that the SIEM Connection is successful. Depending on your chosen environment (Splunk and Sentinel), admins can copy the query and check their SIEM environments for the test event.



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

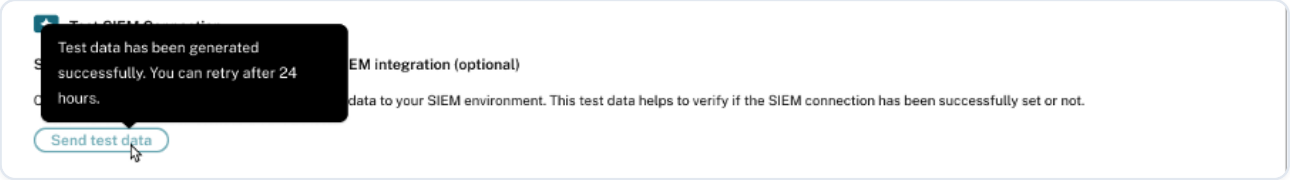


For Elasticsearch and other environments, the following success message is displayed.



NOTE

Once a test event is generated, the **Send test data** button is disabled for the next 24 hours, and the users see the following popup on hovering over the button. After 24 hours from the latest success timestamp, the button is enabled for the users to test the functionality again.



If the test event data is not successfully written in the customer Kafka topic, a failure message is shown as depicted in the following screenshot. The user can send the data again to test the connection.



SIEM Email Alert

Citrix Analytics sends email alerts to notify the administrators about scenarios that might lead to disruption of data flow to their SIEM environment. It contains situational information about activities that might lead to temporary/permanent security postured data loss. It also helps in navigating through the self-service troubleshooting journey for SIEM data export.

Some important properties of this set of email alerts to help locate the same in your inbox:

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

- The email gets distributed among Citrix Cloud™ admins, Security full admins, Security read-only admins, and Security and Performance read-only admins.
- The sender is Citrix Cloud mailto:donotreplynotifications@citrix.com.
- The subject line is:
  - **SIEM Data Export Alert - Password was reset** for Password reset email alerts.
  - **SIEM Data Export Alert - Data Flow Stopped** for Data Flow disruption email alerts.

How to enable email notifications?

If you are a Citrix Cloud administrator with custom access permissions (Security Full Admin, Security Read Only Admin, Security, and Performance Read Only) to manage Security Analytics, the email notifications are always enabled for your Citrix Cloud account. By default, the weekly email notifications are sent to the Citrix Security Administrators - default list. You can also modify the distribution list that receives this alert. For more information, see
.

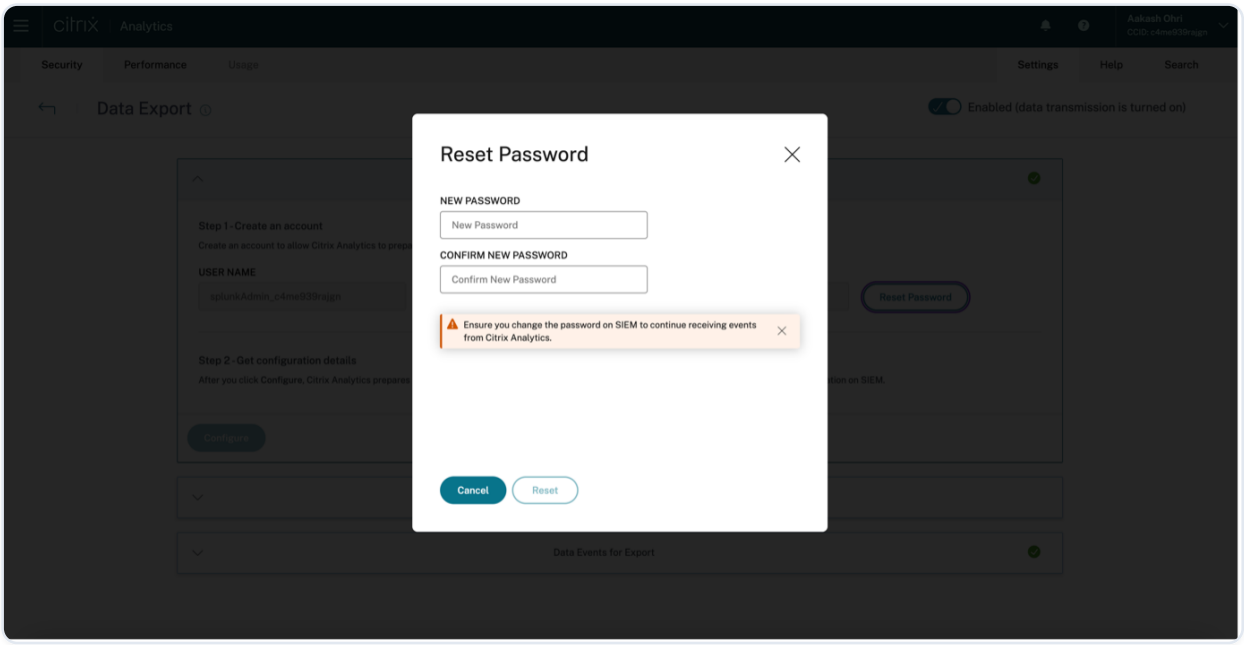
If you are a Citrix Cloud administrator with custom access permissions (Security Full Admin, Security Read Only Admin, Security and Performance Read Only) to manage Security Analytics, the email notifications are always enabled for your Citrix Cloud account.

Types of SIEM Email Alert

1. **SIEM Password Reset Email Alert**

   The SIEM password reset alert email is received when the account password is reset via the Data Exports page. Resetting the SIEM password on Citrix Analytics UI alone can lead to a password mismatch with the one configured on your SIEM. This leads to data flow disruption. This email alert contains the time at which the password was reset. If data flow stops, you can go to the **Summary** tab, check if the “last exported at” timestamp lies close to the password reset timestamp, and hence relay the necessary password changes. This shortens the debugging process and helps you get back to successful data flow into your SIEM environment in no time.

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



© 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. **Data Flow Disruption for 24 hours Email Alert**

   This email alert is sent when data flow from the Citrix Analytics service into your SIEM environment is disrupted for more than 24 hours. The email includes the time at which the last event was exported along with helpful troubleshooting quick tips that can be performed to bring back the data flow. This would be the correct time to quickly reinstate the data flow to not lose out on any security postured data.

3. **Data Flow Disruption for 7 days Email Alert**

   This email alert is sent when data flow from the Citrix Analytics service into your SIEM environment is disrupted for more than 7 days. Since the retention period of the customer’s Kafka topic is 7 days, it is critical to follow troubleshooting tips and take the help of the quick guide available on the **Data Exports** page to not lose any further data as this email warns of a situation of permanent loss of security postured information.

4. **Data Flow Disruption for 30 days Email Alert**

   This email alert is sent when data flow from the Citrix Analytics service into your SIEM environment is disrupted for more than 30 days. By now, the customer has lost security postured data and it's imperative to use the troubleshooting capabilities to reinstate the flow as soon as possible.

© 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,

Example Sigma Signatures for Security Insights

This page contains example queries to help administrators achieve meaningful outcomes using Citrix Security Analytics.

These examples cover risks under the following categories:

- Compromised endpoints
- Insider threats
- Data exfiltration

How to use these examples

View the data source and turn on the data processing

To view the data source, click **Settings > Data Sources > Security** in the Citrix Analytics GUI. The **Apps and Desktops- Workspace app** site card appears on the **Data Sources** page. Click **Turn On Data Processing** to allow Citrix Analytics to begin processing data for this data source.

Citrix Analytics for Security™ sends the following two types of risk insights data to your SIEM service:

- Risk insights events (Default exports)
- Data Source events (Optional exports)

As part of your SIEM environment, the risk insight event data sources are available and always turned on by default. For more information, see Data events exported from Citrix Analytics for Security to your SIEM service.

You can use either CAS or Sigma signatures to verify any particular user events within your data sources. CAS queries are accessible through the Self-Service Search page on your Citrix Analytics GUI. The Sigma signatures are written in a simple or user-friendly format, making them compatible with various SIEM environments.

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

Using CAS queries

You can use the CAS query under the **Self-Service Search** page to find and filter user events received from various data sources. Click **Search** from your Citrix Analytics GUI and enter the query in the search box. For more details, see How to use self-service search.

You can also create custom risk indicators with the existing templates. To create a custom risk indicator, navigate to **Security > Custom Risk Indicators > Create Indicator**. For more details, see Creating a Custom Risk Indicator.

Using Sigma signatures

Sigma is a user-friendly, open signature format for creating text-based queries that analysts can use to describe log events, making detections easier to write. There are a few different ways to convert a Sigma signature to your SIEM tool's query language.

- You can use the CLI tools and Python SDKs offered by Sigma. For more information on Sigma signature, see Rule Usage.
- You can use public tools such as uncoder.io's Sigma Translation Engine which offers a free tier.

Refer to the following different Custom Indicator use cases for the different risk insights:

- Unsanctioned browser
- Unsanctioned operating system
- Unsanctioned Workspace App Versions
- Unauthorized operating systems outside allow list
- Unauthorized IP address or subnets
- Unauthorized virtual apps
- Unusual desktop names
- Monitor specific application
- Printing from SaaS apps
- Clipboard usage on SaaS apps

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

Compromised endpoints

Unsanctioned browser

This occurs when a user attempts to access content from a browser type or version that is not allowed by the organization's IT policy or because of security vulnerabilities.

Details

Data Source: Apps and Desktops (Workspace App)

CAS query

```
Event-Type = "Session.Logon" AND Browser-Name !~ "<Browser-Name>"
```

The Session.Logon event triggers when a user enters their credentials and logs on to their app or desktop session.

Sigma signature

```
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
```

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

```
logsource:

  product: citrixanalytics

  service: security

title: Access from unauthorized browser
```

Unsanctioned operating systems

This occurs when a user attempts to access a device with an operating system type or version that is not allowed by your organization's IT policy or because of security vulnerabilities.

Details

Data Source: Apps and Desktops (Workspace App)

CAS query

```
Event-Type = "Session.Logon" AND OS-Name ~ "<OS-Name>" AND OS-Version =
"<OS-Version>" AND OS-Extra-Info = "<OS-Extra-Info>"
```

Sigma signature

```
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:
```

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

```
    occurrence_event_type: Session.logon

    os_name|contains: '<OS-Name>'

    os_version: '<OS-Version>'

    os_extra_info: '<OS-Extra-Info>'

logsource:

  product: citrixanalytics

  service: security

title: Unauthorized operating systems in block list
```

Unauthorized IP address or subnets

This occurs when a user attempts to access from an IP address or range which is marked as unauthorized by your organization's IT policy.

Details

Data Source: Apps and Desktops (Workspace App)

CAS query

```
Event-Type = "Session.Logon" AND Client-IP = "<XX.YY.ZZ.*>"
```

Sigma signature

```
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
```

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

```
  filter:
  - client_ip: '<IP>'
  filter_null:
  - client_ip: null
  selection:
  - occurrence_event_type: Session.Logon
logsource:
  product: citrixanalytics
  service: security
title: Access from unauthorized IP
```

Unauthorized operating systems outside allow list

This occurs when a user attempts to access applications from servers that host operating systems outside the allow list.

Details

Data Source: Apps and Desktops (Workspace App)

CAS query

```
Event-Type = "Session.Logon" AND OS-Name !~ "<OS-Name>" AND OS-Version !=
"<OS-Version>" AND OS-Extra-Info != "<OS-Extra-Info>"
```

Sigma signature

```
author: Citrix
date: 2023/01/31
description: Unauthorized operating systems outside allow list
```

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

```
detection:

  condition: selection and not filter_null and not filter_os and not
filter_os_version and not filter_os_extra

  filter_os:

  - os_name|contains: '<OS INFO>'

  filter_os_version:

  - os_version: '<OS Version>'

  filter_os_extra:

  - os_extra_info: '<OS Extra Info>'

  filter_null:

  - os_name: null

  - os_version: null

  - os_extra_info: null

  selection:

  - occurrence_event_type: Session.Logon

logsource:

  product: citrixanalytics

  service: security

title: Unauthorized operating systems outside allow list
```

Unsanctioned Workspace app versions

This occurs when a user attempts to access a Workspace app version that is not a supported client version. In such cases, users must upgrade their client to a supported version. For more information, see Support client versions.

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

Details

Data Source: Apps and Desktops (Workspace App)

CAS query

```
Event-Type = "Session.Logon" AND Client-Type IN ("Windows", "Macintosh",
"Unix/Linux") AND Workspace-App-Version != "20*" AND Workspace-App-
Version != "21*"
```

Sigma signature

```
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:
```

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

```
  product: citrixanalytics

  service: security

title: Unsupported Workspace app versions
```

Insider threats

Unusual desktop names

This occurs when the user attempts to launch a desktop that is not considered usual.

Details

Data Source: Apps and Desktops (Workspace App)

CAS query

```
Event-Type = "Session.Logon" AND Session-Launch-Type = "desktop" AND App-
Name ~ "<Desktop Name>"
```

Sigma signature

```
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
```

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

```
  selection1:
  - occurrence_event_type: Citrix.EventMonitor.AppStart
  selection2:
  - launch_type: 'desktop'
logsource:
  product: citrixanalytics
  service: security
title: Unusual desktop names
```

Monitor specific process

This occurs when the user launches a published application that is in the watch list. The purpose could be to monitor the usage of specific published applications.

Details

Data Source: Apps and Desktops (Session Recording)

CAS query

```
Event-Type = "Citrix.EventMonitor.AppStart" AND App-Name IN ("<App-Name-1>", "<App-Name-2>")
```

Sigma signature

```
author: Citrix
date: 2023/01/31
description: Monitor specific process
detection:
  condition: selection and not filter_null and filter_app_name
```

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

```
  filter_app_name:
  - app_name: ['<App-Name1>', '<App-Name2>']
  filter_null:
  - app_name: null
  selection:
  - occurrence_event_type: Citrix.EventMonitor.AppStart
logsource:
  product: citrixanalytics
  service: security
title: Monitor specific process
```

Unauthorized virtual apps

This occurs when the user accesses unauthorized virtual apps.

Details

Data Source: Apps and Desktops (Workspace App)

CAS query

```
Event-Type = "App.Start" AND App-Name IN ("<App-Name1>", "<App-Name2>")
```

Sigma signature

```
date: 2023/01/31
description: Unauthorized virtual apps
detection:
  condition: selection and not filter_null and filter_app_name
```

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

```
  filter_app_name:
  - app_name: ['<App-Name1>', '<App-Name2>']
  filter_null:
  - app_name: null
  selection:
  - occurrence_event_type: App.Start
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized virtual apps
```

Data Exfiltration

Printing from SaaS apps

This occurs when a file is printed from a SaaS application from which printing is not allowed. It detects potential data exfiltration by printing operations in SaaS applications.

Details

Data Source: Apps and Desktops (Citrix Enterprise Browser™)

CAS query

```
Event-Type = "App.SaaS.File.Print" AND SaaS-App-Name = "<App-Name>"
```

Sigma signature

```
author: Citrix
date: 2023/01/31
```

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

```
description: Printing from SaaS apps

detection:

  condition: selection and not filter_null and filter_saas_app_name

  filter_saas_app_name:

  - saas_app_name: '<App-Name>'

  filter_null:

  - saas_app_name: null

  selection:

  - occurrence_event_type: App.SaaS.File.Print

logsource:

  product: citrixanalytics

  service: security

title: Printing from SaaS apps
```

Clipboard usage on SaaS apps

This occurs when a cut, copy, or paste activity is done from any SaaS application. It detects potential data exfiltration from SaaS applications in your organization by monitoring the clipboard operations.

Details

Data Source: Apps and Desktops (Citrix Enterprise Browser)

CAS query

```
Event-Type = "App.SaaS.Clipboard" AND Clipboard-Result = "success" AND
Clipboard-Operation IN ( "copy" , "cut" )
```

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

Sigma signature

```
author: Citrix

date: 2023/01/31

description: Clipboard usage on SaaS apps

detection:

  condition: selection and not filter_null and
filter_clipboard_details_result and filter_clipboard_operation

  filter_clipboard_details_result:

  - clipboard_details_result: 'success'

  filter_clipboard_operation:

  - clipboard_operation: ['cut', 'copy', '<Other Operation>']

  filter_null:

  - clipboard_operation: null

  - clipboard_details_result: null

  selection:

  - occurrence_event_type: App.SaaS.Clipboard

logsource:

  product: citrixanalytics

  service: security

title: Clipboard usage on SaaS apps
```

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

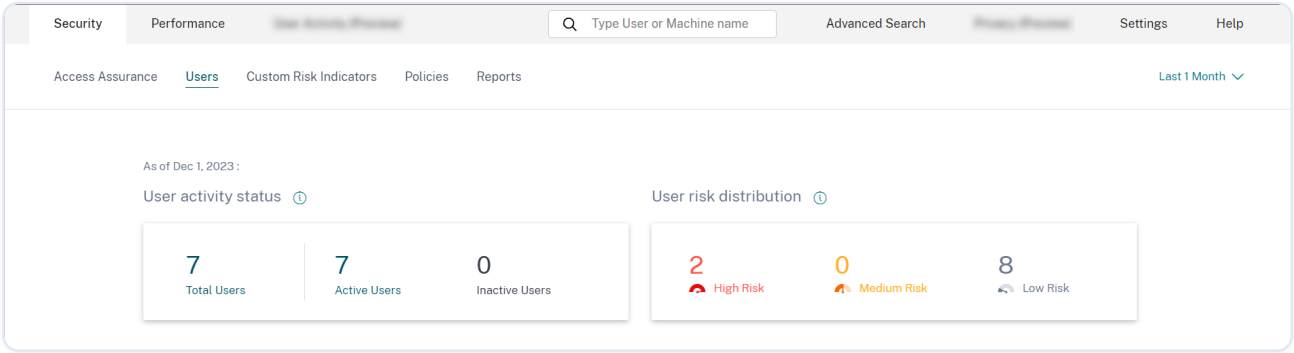
Users dashboard

Overview

The **Users** dashboard is the launching point for user behavior analysis and threat prevention.

This dashboard provides visibility into user behavior patterns across an organization. Using this data, you can proactively monitor, detect, and flag behavior that falls outside the norm, such as phishing or ransomware attacks.

To view the Users dashboard, go to **Security > Users**. The Users dashboard contains the following sections:



- **User active status**: Distribution of total, active, and inactive users.
- **User risk distribution**: Distribution of active, inactive, total users, and distribution of risk users in high, medium, and low profiles based on their highest computed risk score in the selected time period.
- **Top Users**: Top Users are sorted by their risk score and segmented by All Users, Privileged Users, and Watchlist Users.
- **Risk Categories**: Displays the risk categories that Citrix Analytics supports. Risk indicators with similar behavioral patterns are grouped into categories.
- **Risk Indicators and Actions**: Distribution of risk indicators and actions plotted over a selected duration across all users in your organization.
- **Access Summary**: Summarizes the total number of attempts that users have made to access the resources within your organization.
- **Policies and Actions**: Displays the top five policies and actions applied on user profiles.

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

- **Risk Indicators**: Displays the top five risk indicators in your organization.

User activity status

Total number of users in your organization using the data sources for which you have enabled Analytics. They might or might not have a risk score associated with their account. This tile shows the number of active users. Active users are the users with events detected within the selected time period. You can click the user activity status drop-down menu to view the distribution of total users into active and inactive users.

- Total users: Total number of users in the selected time frame.
- Active users: Users with events detected in the selected time frame.
- Inactive users: Users with no events detected in the selected time frame.

The total number of users on the **Users** dashboard might be more than the number of risky users since all users are not expected to be risky.

NOTE

On the **Users** page, the total number of users is displayed for the last 30 days irrespective of the selected time period.

Facets

Filter the user events based on the following categories:

- **Risk Score**: User events based on high-risk, medium-risk, low-risk, and zero-risk scores.
- **User**: User events based on admin privilege, executive privilege, and watchlist users.
- **Discovered Data Sources**: User events based on the data source that you have onboarded.

Search box

Use the search box to search events for the users. You can use operators in your query to narrow down the focus of your search. For information on the valid operators that you can use in your query, see Self-service search.

Latest score

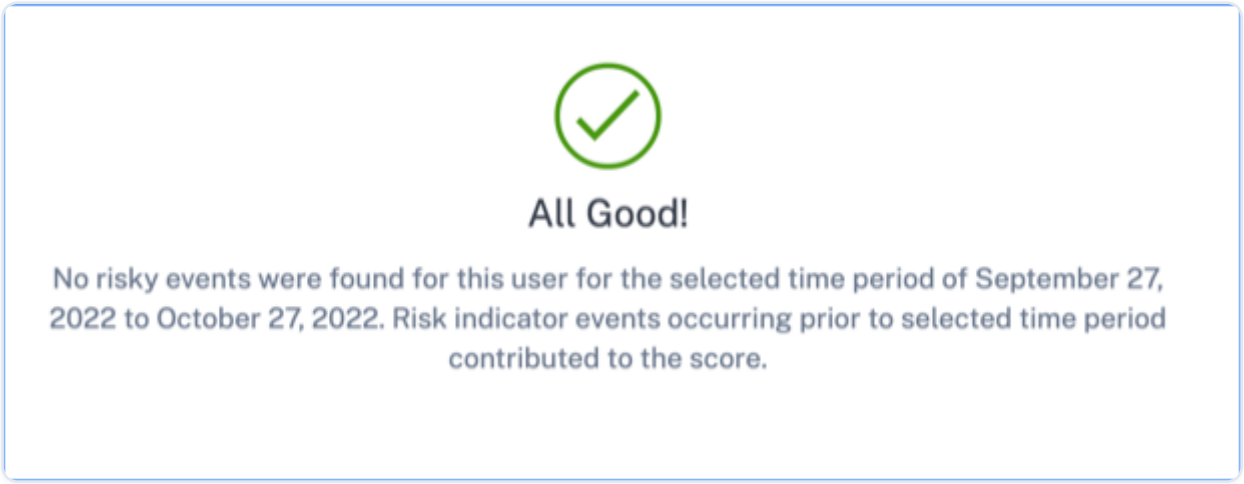
The risk score determines the level of risk a user poses to an organization for a specific time period. The risk score value is dynamic and varies based on user behavior analytics. Based on the

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

latest risk score, a user can fall under one of the categories: high-risk user, medium-risk user, low-risk user, and user with zero risk score.

User

List of all users discovered by Analytics. Select a user name to view the user information and risk timeline for the user. The user might or might not have triggered any risk indicator. If there are no risky events associated with this user, you see the following message.



If there are risky events associated with a user, you see the risk indicators on their risk timeline. Select the user to view their risk timeline.

A user can be marked as `privileged` and added to the watchlist.

Discovered data source

The data source associated with a user. When a user is actively using the data source, Analytics receives the user events from that data source. To receive user events, you must turn on data processing on the data source site card, which is available on the **Data Sources** page.

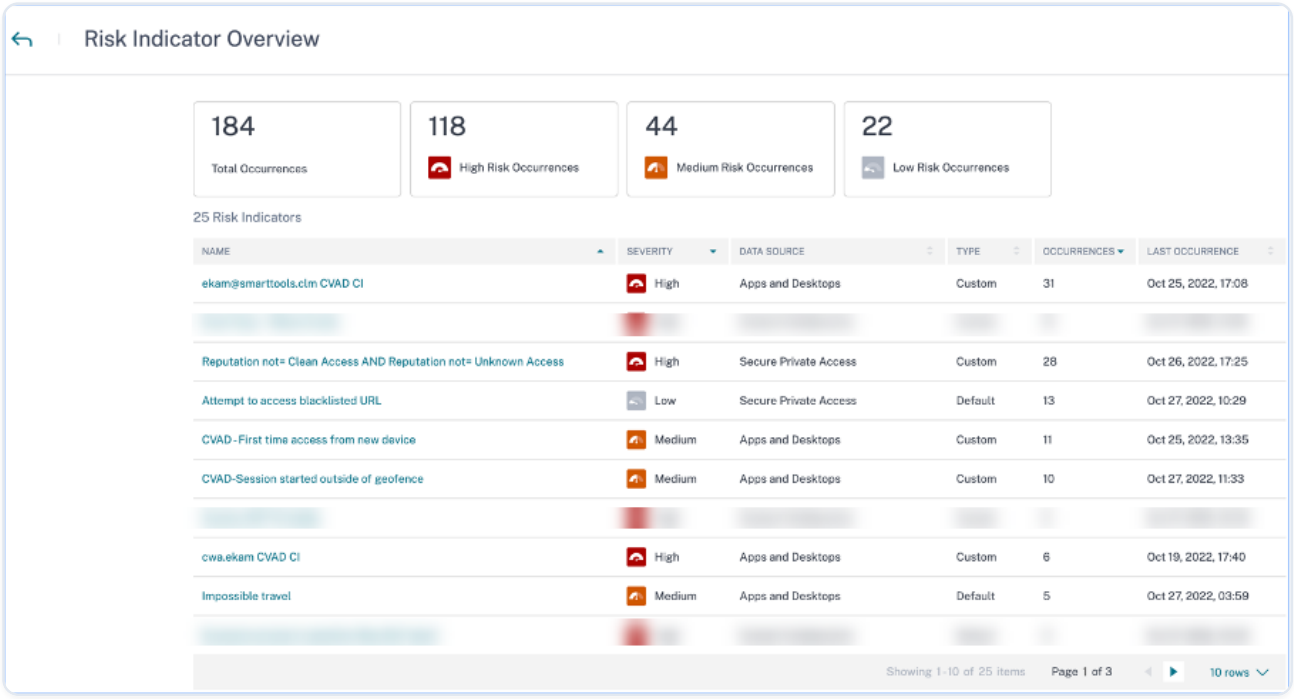
Indicators triggered

Indicates the number of risk indicators triggered across users for the selected duration. Click the **Indicators triggered** tile to view the risk indicators details. The risk indicator table provides the following details:

- **Name**: The risk indicator name.
- **Severity**: The severity of the risk associated with the event. The risk can be high, medium, or low.
- **Data source**: The data source on which the risk indicator template applies.
- **Type**: Type of risk indicator. A risk indicator can be default or custom.

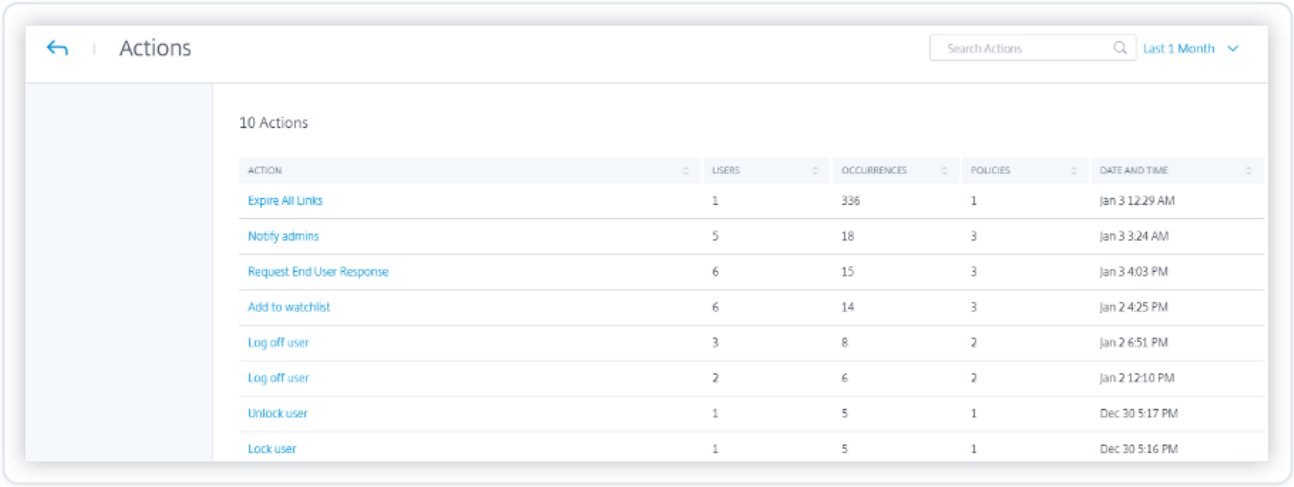
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Occurrences**: The number of times a risk indicator is triggered for a user. When you select the time period, the risk indicator occurrences change based on the time selection.
- **Last occurrence**: Shows the last occurrence date and time.



Actions applied

Indicates the number of actions applied across users for the selected duration. This includes the actions applied manually by the administrators and the policy-driven actions. Click the **Action applied** tile to view the action details. This section does not display the actions that you have applied manually on the user profiles.



The **Action** table provides the following information:

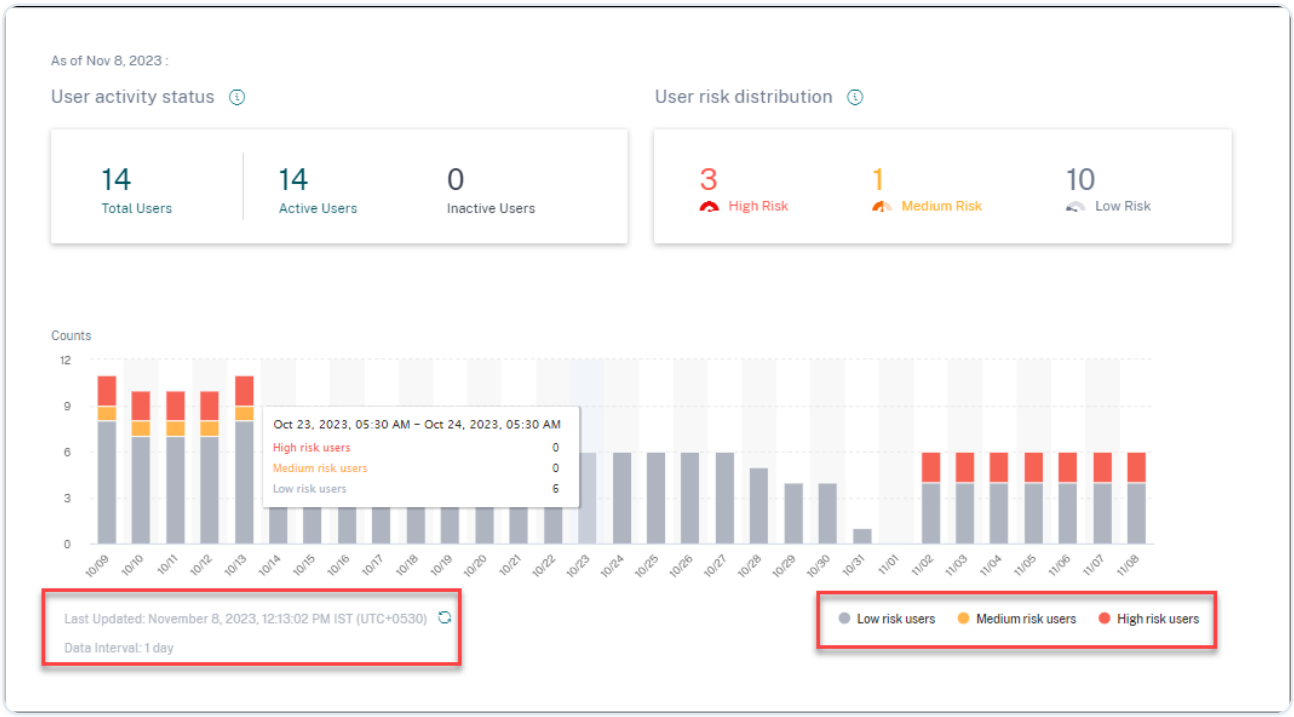
- **Action**: Name of the action applied as per the policy.
- **Users**: Number of users to which the action has been applied.

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

- **Occurrences**: Number of occurrences of the action.
- **Date and Time**: Date and time of the applied action.

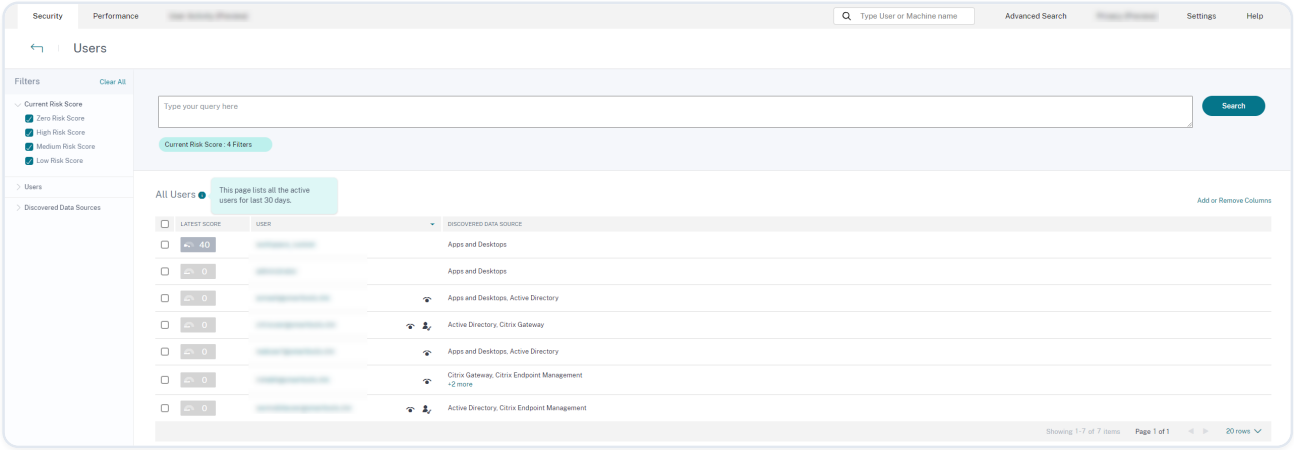
Events processed

Total number of user events received from your connected data sources and processed by Analytics.



User risk distribution

You can view the number of users in high, medium, and low profiles based on their highest computed risk score in the selected time period. Below the overall counts, a bar chart shows changes over time in the distribution of low, medium, and high-risk users.



The level of risk is categorized into three color codes.

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

- **Red** - Represents high-risk users.
- **Orange** – Represents medium-risk users.
- **Grey** – Represents low-risk users.

You can view the numbers of risky users (high, medium, and low) while hovering your mouse on the color bars based on a specific time period. You can view the last updated details (date and time) with the data interval information. Click any color bar to see the risk users in that duration. Click the refresh option to get the updated data.

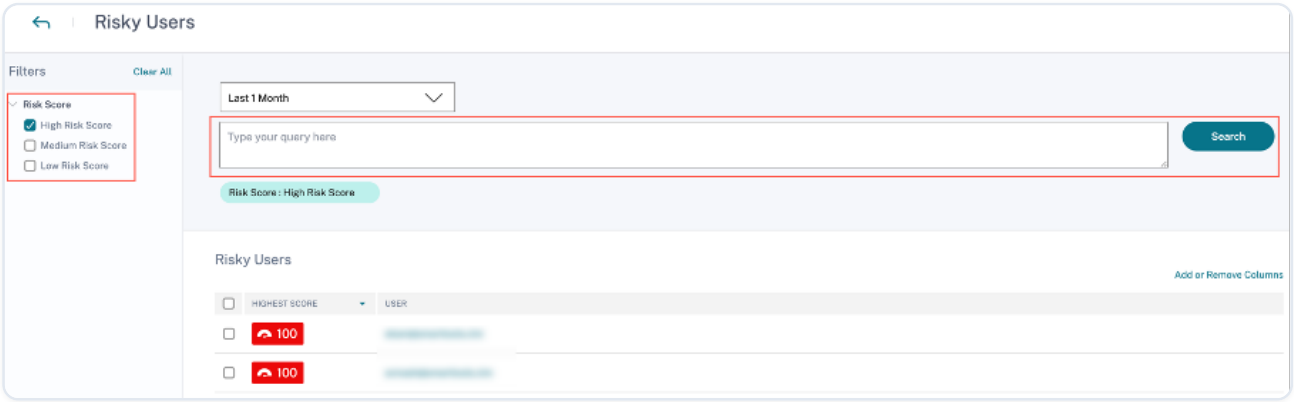
Risky users

Risky users are users who have risky events associated and have triggered at least one risk indicator. The level of risk a user poses to the network for a specific time period is determined by the risk score associated with the user. The risk score value is dynamic and is based on user behavior analytics.

Each user's risk is regularly updated over time based on user activity. Therefore a user might be medium or high risk at one point in time, but drop to a lower risk level later. Based on the risk score, a risky user can fall into one of the following categories:

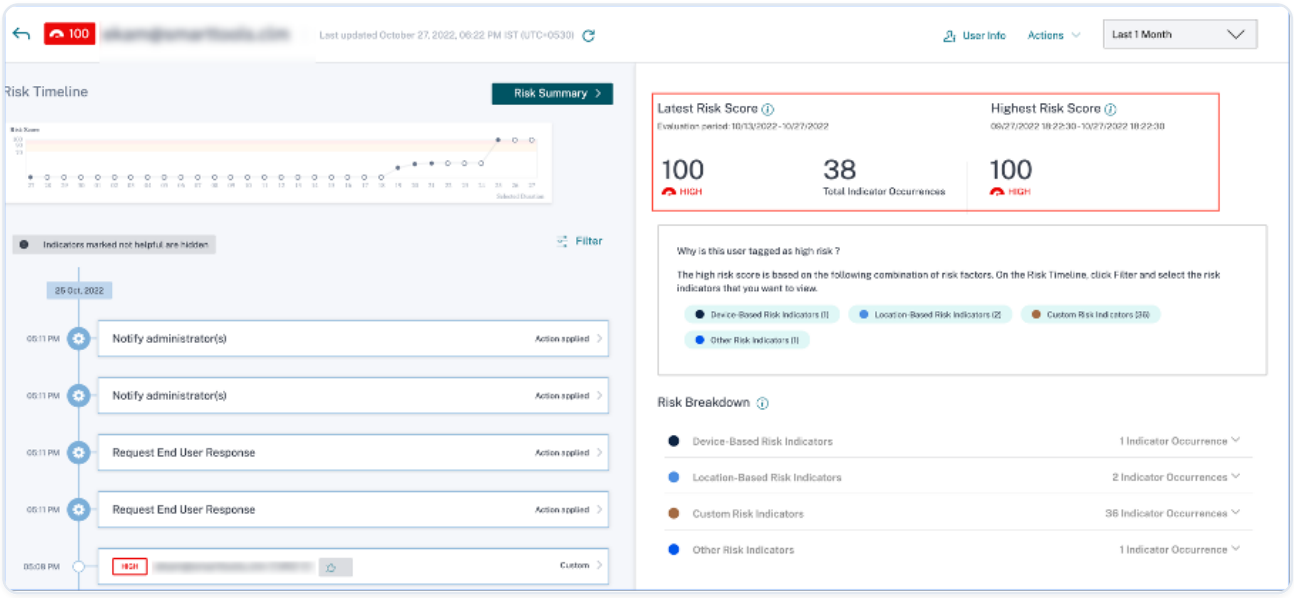
- High risk
- Medium risk
- Low risk

On the **Risky Users** page, you can use the facets to filter based on risk levels associated with the selected time period, and the search bar to query for a specific user or users.



Click the user’s email ID to view the **Risk timeline** page for that particular selected user. This page displays the risk indicators along with **Latest** and **Highest risk score** details based on the selected time period.

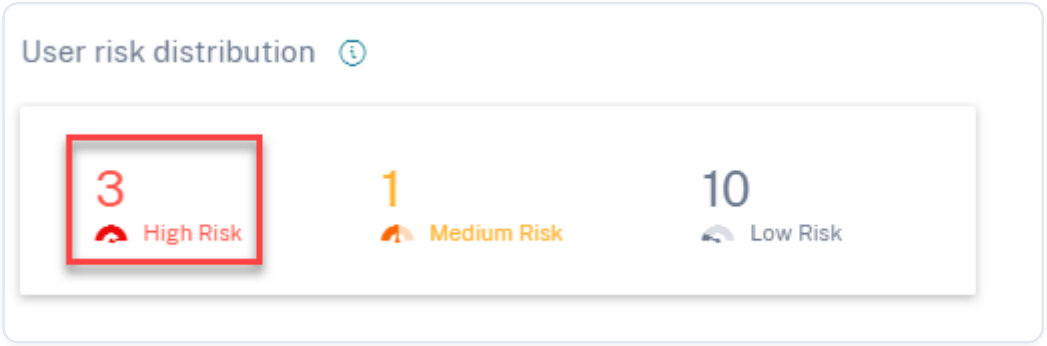
© 1997–2026 Citrix Systems, Inc. All rights reserved.



High risk

Users with risk scores between 90 and 100. These users have exhibited multiple behaviors consistent with moderate to severe risk factors and might represent immediate threats to the organization.

On the **Users** dashboard, you can view the number of high-risk users based on the highest computed risk score in the selected time period.

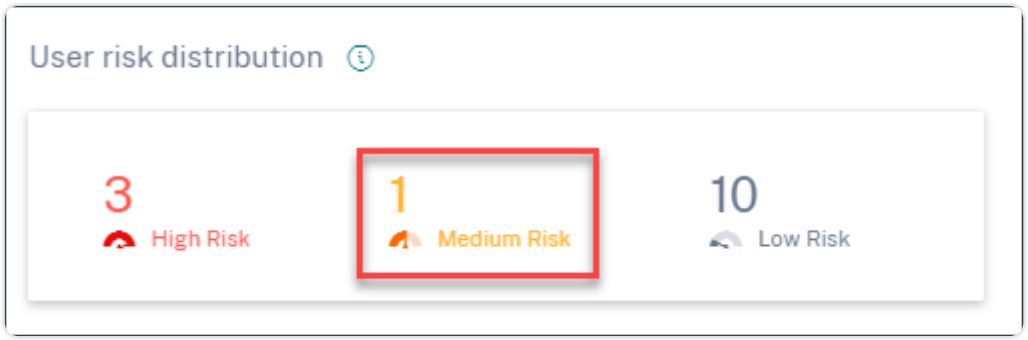


Click the **High Risk** option to view the **Risky users** page. The page displays the details about the high-risk users.

Medium risk

Users with risk scores between 70 and 89. These users have typically one or more activities that appear potentially suspicious and/or anomalous and might be worth monitoring closely.

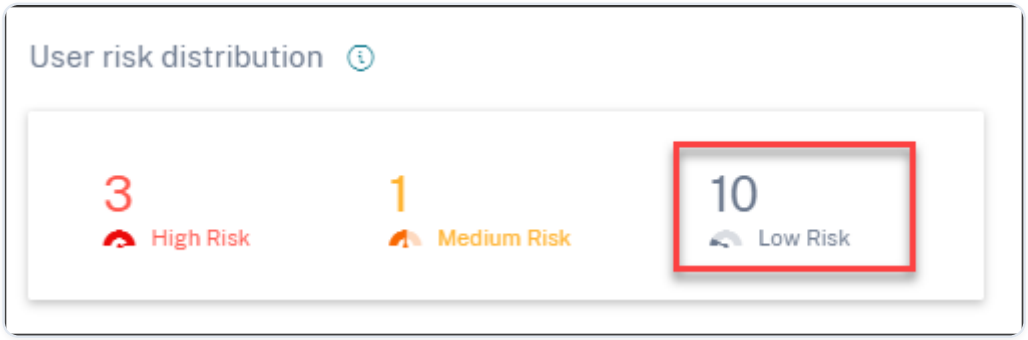
© 1997–2026 Citrix Systems, Inc. All rights reserved.



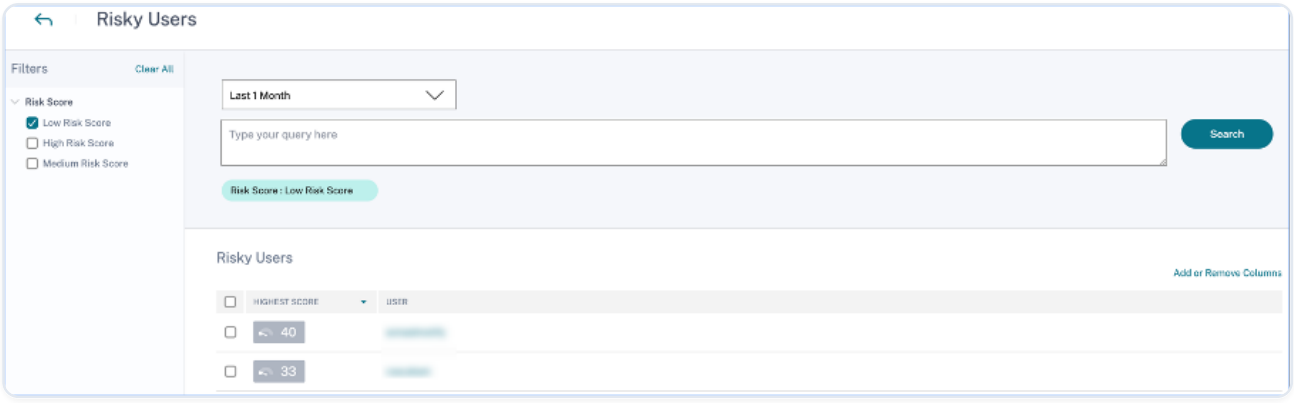
Click the **Medium Risk** option to view the **Risky users** page. The page displays the details about the medium-risk users.

Low risk

Users with risk scores between 1 and 69. These users have at least one risk indicator reflecting some unusual or unexpected behavior, but not enough to merit a more serious risk classification.



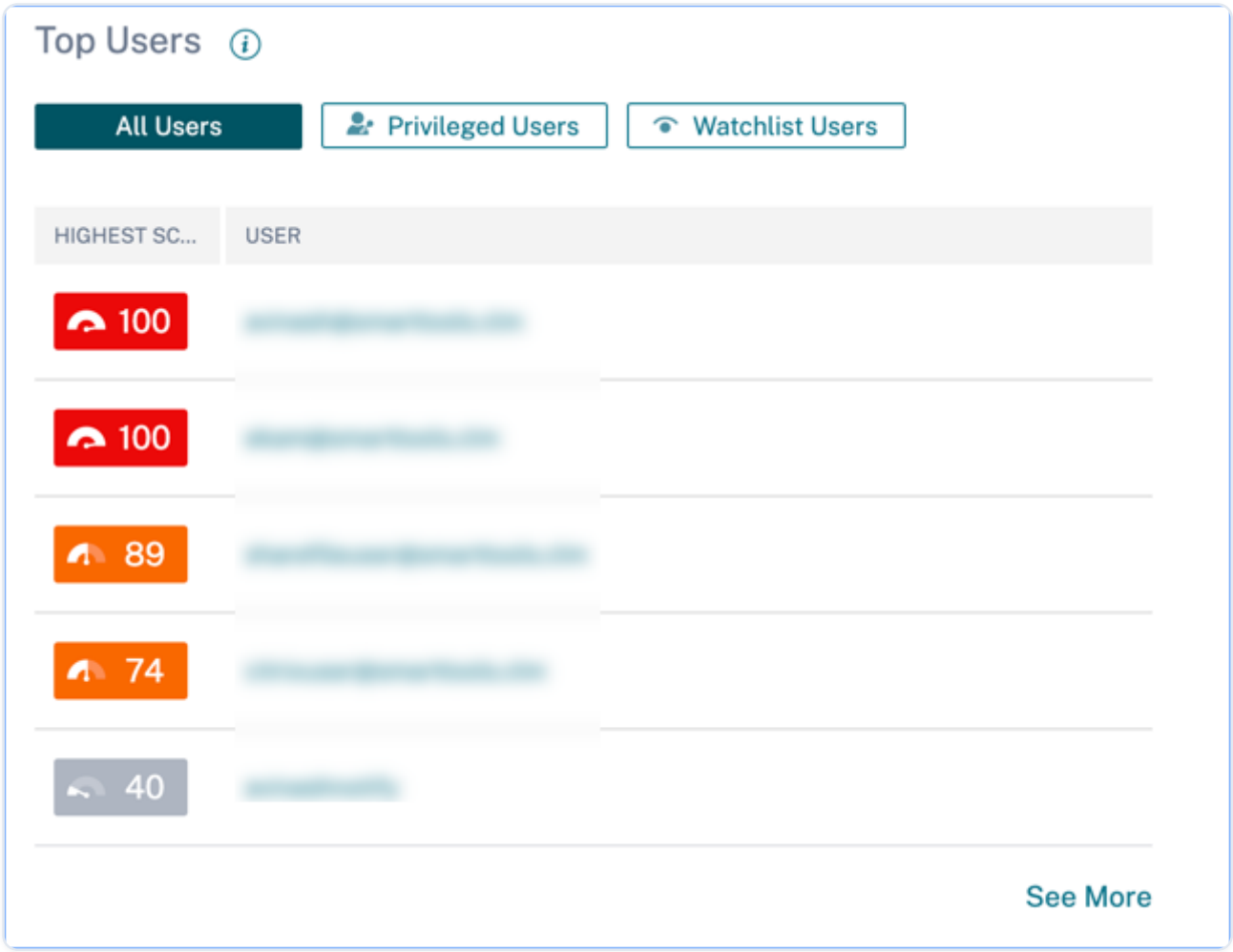
Click the **Low Risk** option to view the **Risky users** page. The page displays the details about the low risk users.



Top users

You can view the top users in various user categories sorted by highest risk scores for the selected time period. The following **Top users** table shows the top five highest risk users (all, privileged, and watchlist users) based on their risk score calculated over the selected time period, rather than the latest risk score.

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



NOTE

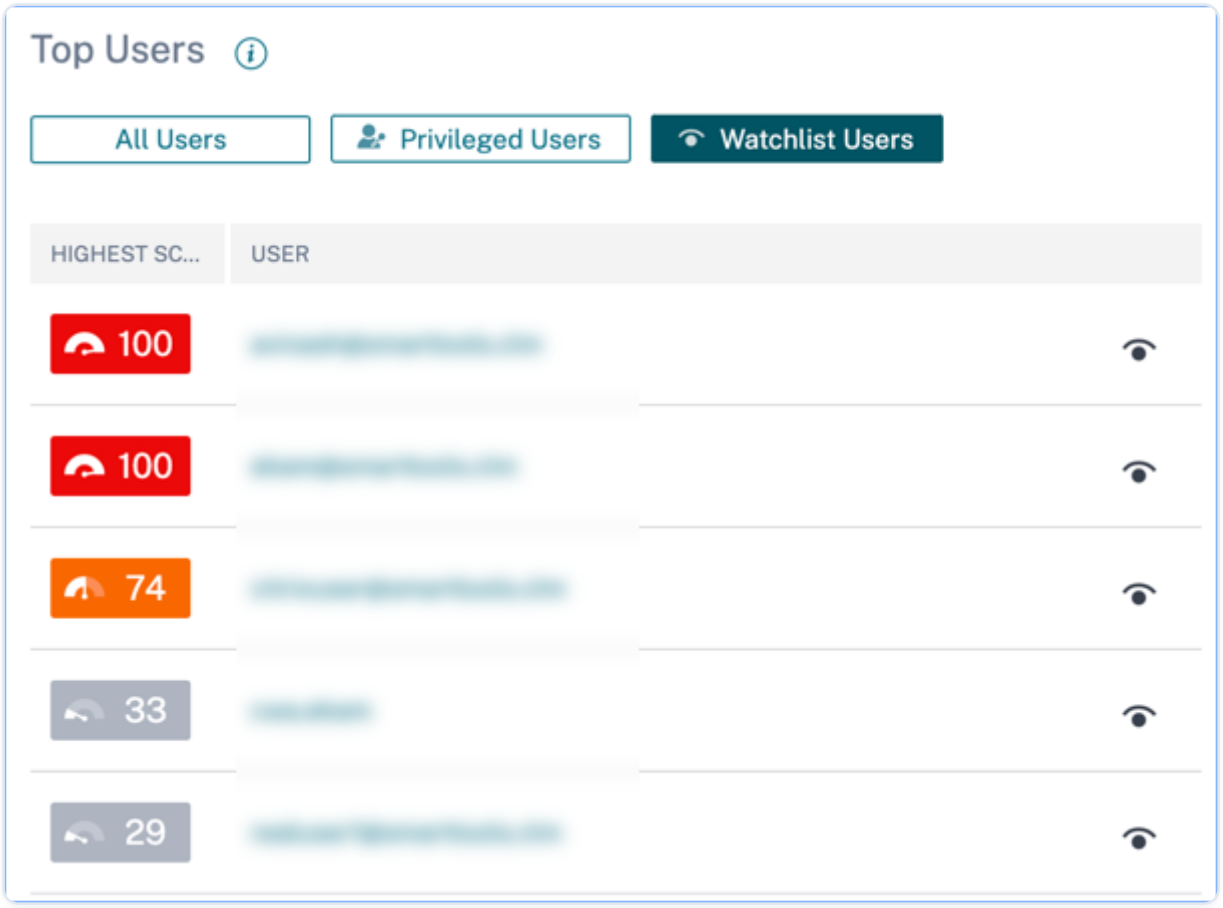
In earlier versions, the Top Users table always displayed the latest risk score, regardless of the time period selected.

Watchlist users

List of users monitored closely for potential threats. For example, you can monitor users who are not full-time employees within your organization by adding those users to the watchlist. You can also monitor users who trigger a specific risk indicator frequently. You either add a user to the watchlist manually or define policies to add users to the watchlist.

If you have added users to the watchlist, you can view the top five users in the watchlist based on the highest score.

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



Click the **See More** link on the **All Users** pane to view the **Users page**. The page displays the list of all users in the watchlist.

NOTE

On the **Users** dashboard and the **Users** page, the number of users in the watchlist are displayed for the last 13 months irrespective of the selected time period. When you select a time period, the risk indicator occurrences change based on the time selection.

Learn More: Watchlist

Risk Categories

The **Risk Categories** donut chart summarizes the number of indicator occurrences by risk category during the selected time period. Unique user counts are displayed on the hover over each chart segment, which in turn links to the corresponding **Risk Indicator Category** overview page. Risk categorization is supported by default and custom risk indicators.

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

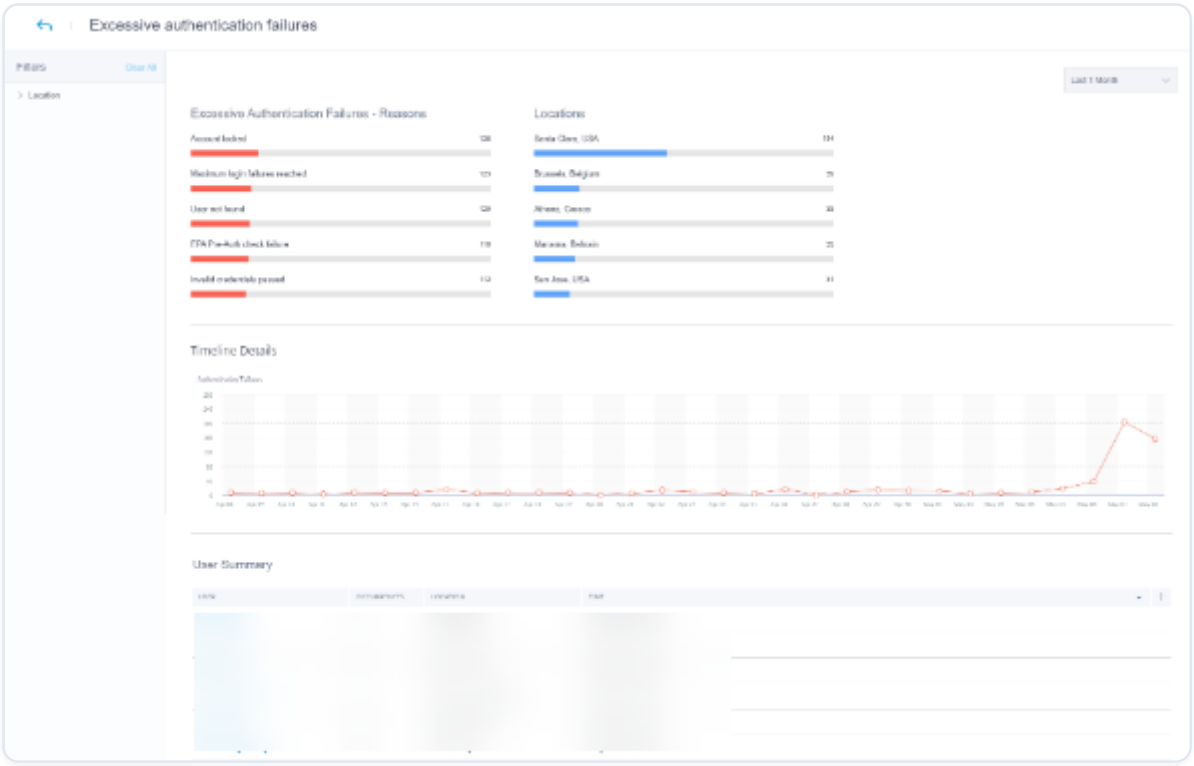


The purpose of the **Risk Categories** dashboard is to enable {{page.cvad-and-daas-product-name}} administrators manage user risks and have simplified discussions with their security counterparts without the need to have an expert-level security knowledge. It allows security enforcement to take effect at an organizational level and is not limited to security administrators alone.

Use case

Consider that you are a {{page.cvad-onprem-product-name}} administrator and you manage the application access rights of employees in your organization. If you go to the **Risk Categories** > **Compromised users** > **Excessive authentication failures - Citrix Gateway** risk indicator section, you can assess whether the employees to whom you had granted access have been compromised. If you navigate further, you can get more accurate insights into this risk indicator such as the failure reasons, sign-in locations, timeline details, and user summary. If you notice any discrepancies between the users that were granted access and the users that were compromised, you can notify the security administrator about it. This timely notification to the security administrator contributes towards enforcement of security at an organizational level.

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



How to analyze the Risk Categories dashboard?

When you select **See More** on the **Risk Categories** dashboard, you are redirected to the page that summarizes details about the risk categories. This page contains the following details:

- **Risk category report**: Represents the total risk indicator occurrences of each category for a selected time period.

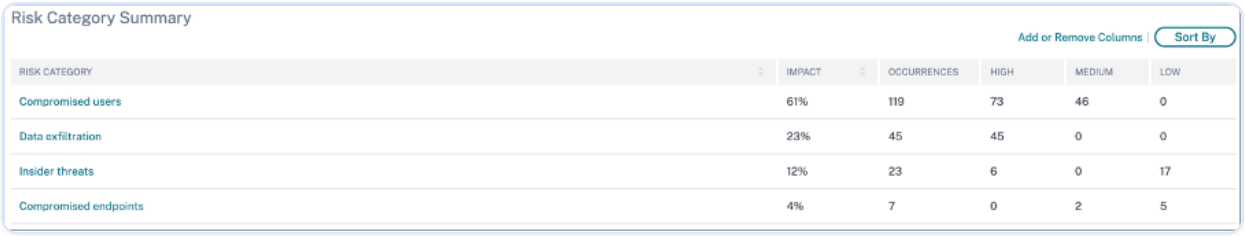


- **Timeline details**: Provides a graphical representation of the total risk indicator occurrences of every risk category for a selected time period. If you navigate to the bottom of this section, you can sort based on risk categories for more accurate insights about the risk indicators.



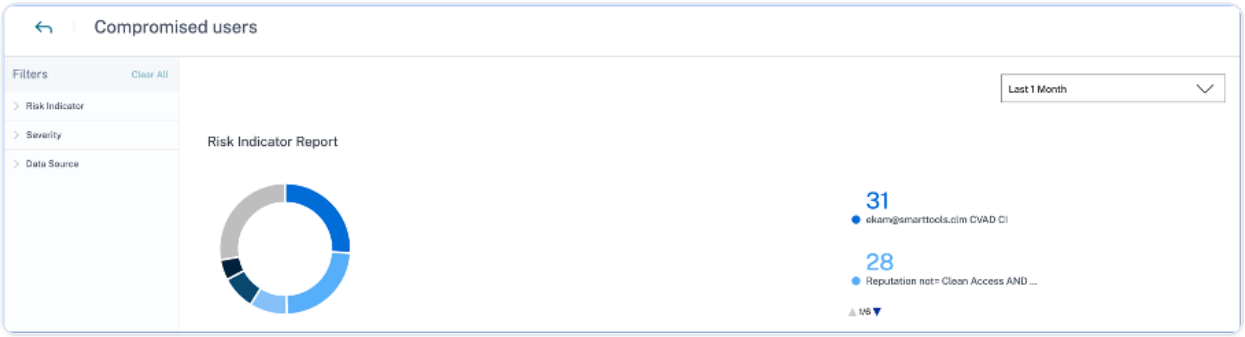
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Risk category summary**: This section provides details such as the impact, occurrences, and severity of the risk indicators associated with each category. Select any risk category to view details about the risk indicators associated with that category. For example, when you select the **Compromised users** category, you are redirected to the **Compromised users** page.

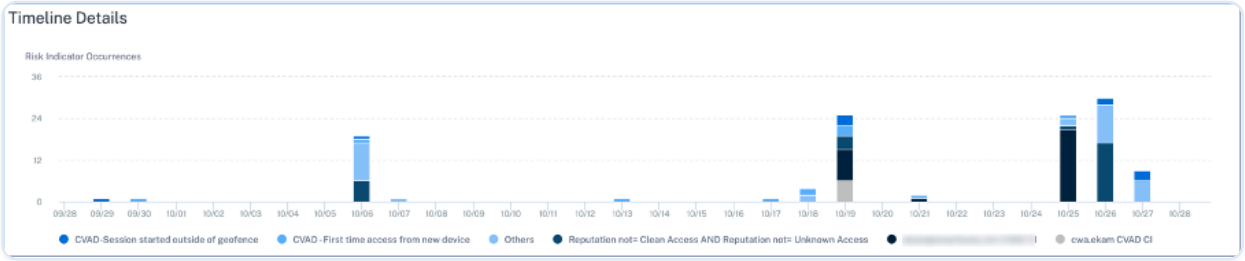


The **Compromised users** page displays the following details:

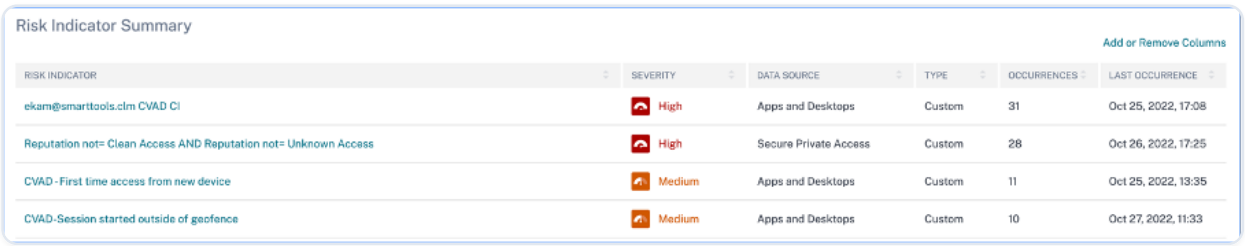
- **Risk Indicator Report**: Displays the risk indicators that belong to the Compromised users category for a selected time period. It also displays the total occurrences of the risk indicators that were triggered during the selected time period.



- **Timeline Details**: Provides a graphical representation of the risk indicator occurrences for a selected time period.

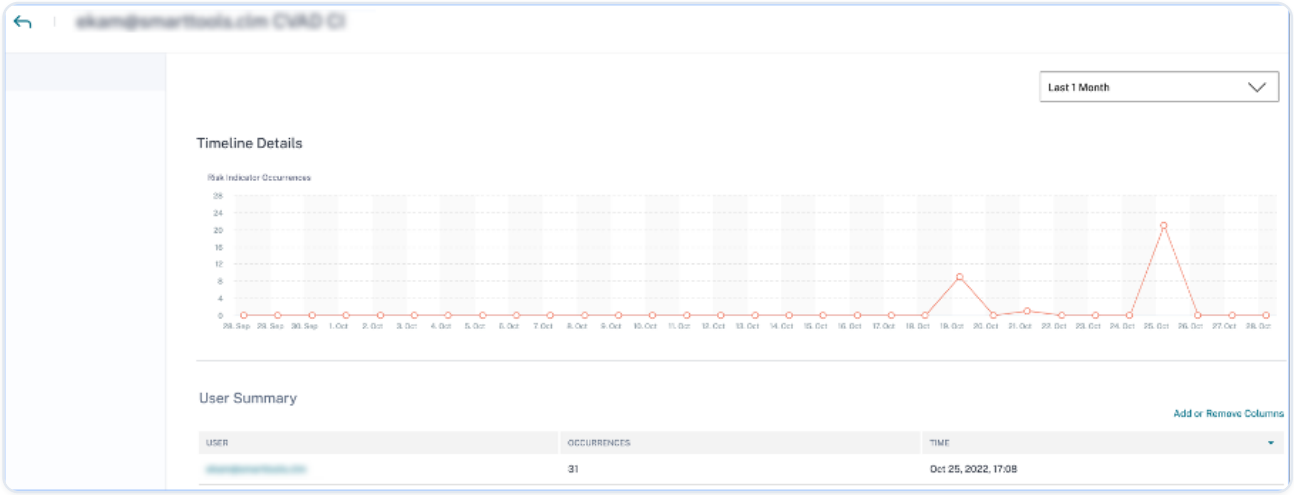


- **Risk Indicator Summary**: Displays a summary of the risk indicators generated under the compromised users category. This section also displays the severity, data source, risk indicator type, occurrences, and the last occurrence.



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

When you select a risk indicator, you are redirected to the page that summarizes the details of that indicator. For example, if you select the **First time access from new device** risk indicator, you are redirected to the page that summarizes details about this indicator. The summary includes timeline details about the occurrences of this event and a user summary that lists the users that triggered this risk indicator, risk indicator occurrences, and the time of the event. When you select a user, you are redirected to the user's risk timeline.



NOTE

Citrix Analytics groups default risk indicators under the appropriate risk category. For custom risk indicators, you must select a risk category on the **Create Indicator** page. For more information, see Custom risk indicators.

Types of risk categories

Data exfiltration

This category groups risk indicators triggered by malware or by employees who perform unauthorized data transfers or data thefts to or from a device in an organization. You can get insights into all the data exfiltration activities that have taken place during a specified time period, and mitigate the risks associated with this category by proactively applying actions on user profiles.

The Data exfiltration risk category groups the following risk indicator:

DATA SOURCES	USER RISK INDICATORS
{{page.cvad-and-daas-product-name}}	Potential data exfiltration

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

Insider threats

This category groups risk indicators triggered by employees within an organization. Since employees have higher levels of access to company-specific applications, organizations are at a higher chance of security risks. Risky activities might be intentionally caused by a malicious insider or might be a result of a human error. In either of the scenarios, the security impact on the organization is damaging. This category provides insights into all the insider threat activities that have taken place during a specified time period. With the help of these insights, you can mitigate the risks associated with this category by proactively applying actions on user profiles.

The Insider threats risk category groups the following risk indicators together:

DATA SOURCES	USER RISK INDICATORS
Citrix Secure Private Access™	Attempt to access the blacklisted URL
Citrix Secure Private Access	Excessive data download
Citrix Secure Private Access	Risky website access
Citrix Secure Private Access	Unusual upload volume

Compromised users

This category groups risk indicators in which users display unusual behavioral patterns such as suspicious sign-ins, and sign-in failures. Alternatively, the unusual patterns might be a result of the user accounts being compromised. You can get insights into all the compromised user events that have taken place during a specified time period, and mitigate risks associated with this category by proactively applying actions on user profiles.

The Compromised users' risk category groups the following risk indicators together:

DATA SOURCES	USER RISK INDICATORS
Citrix Gateway	End point analysis scan failure
Citrix Gateway	Excessive authentication failures
Citrix Gateway	Impossible travel
Citrix Gateway	Logon from suspicious IP
Citrix Gateway	Unusual authentication failure

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

DATA SOURCES	USER RISK INDICATORS
{{page.cvad-and-daas-product-name}}	Suspicious Logon
{{page.cvad-and-daas-product-name}}	Impossible travel
Microsoft Graph Security	Azure AD Identity Protection risk indicators
Microsoft Graph Security	Microsoft Defender for Endpoint risk indicators

Compromised endpoints

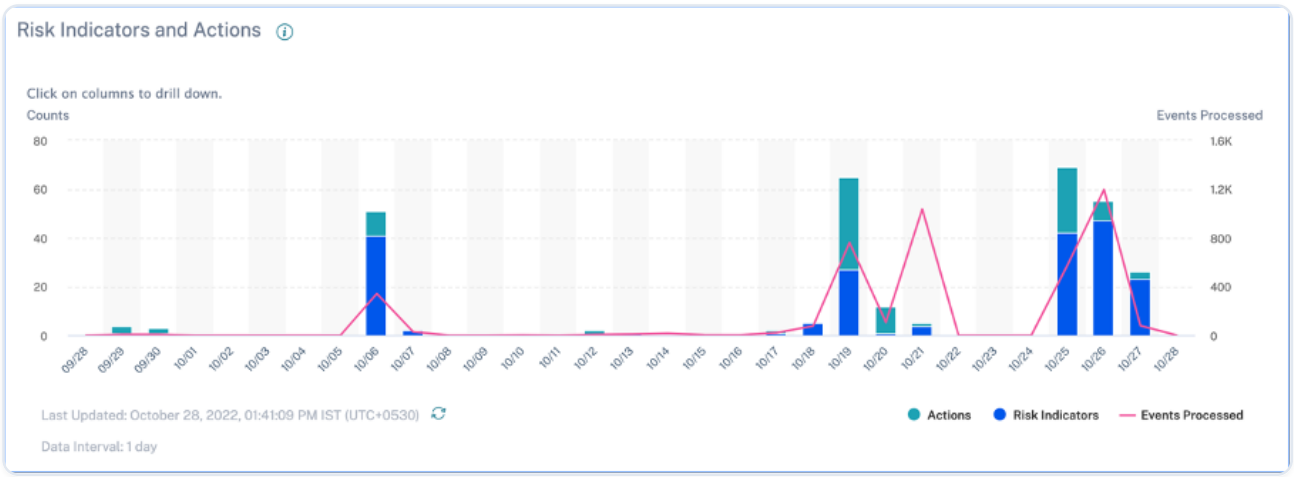
This category groups risk indicators that are triggered when devices exhibit unsecure behavior that might indicate a compromise.

The Compromised endpoints risk category groups the following risk indicators together:

DATA SOURCES	USER RISK INDICATORS
Citrix Endpoint Management™	Unmanaged device detected
Citrix Endpoint Management	Jailbroken or rooted device detected
Citrix Endpoint Management	Device with blacklisted apps detected

Risk indicators and actions

You can view the triggered risk indicators and the applied actions for your users for the selected time period. The new **Risk Indicators and Actions** bar chart provides the counts of indicators, actions, and events detail over time, with the overall time range and bar interval derived from the selected time period.



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

Clicking a bar segment for either indicators or actions yields a drill-down visualization of the counts per indicator or action, respectively.



In the indicator drill-down, clicking an individual indicator bar goes to the corresponding risk indicator page, for the selected time period.

Access Summary

This dashboard summarizes all the Gateway access events for a selected time period. It shows the number of total access, successful access, and failed access through Citrix Gateway.

Click the pointers on the graph to view the Self-service search for Gateway page. For successful sign-in scenarios, Gateway access events are sorted by the status code on the page.

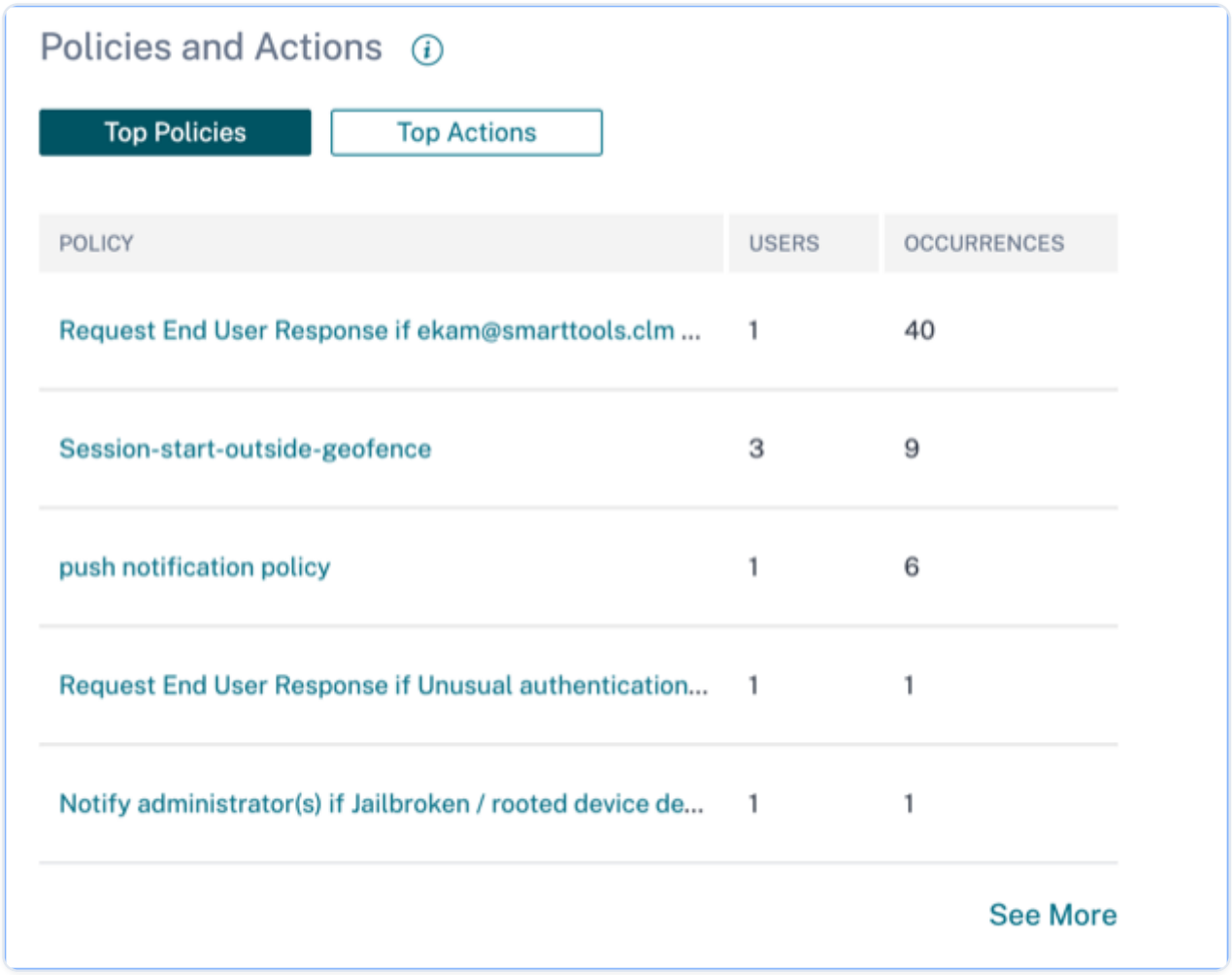
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Policies and Actions

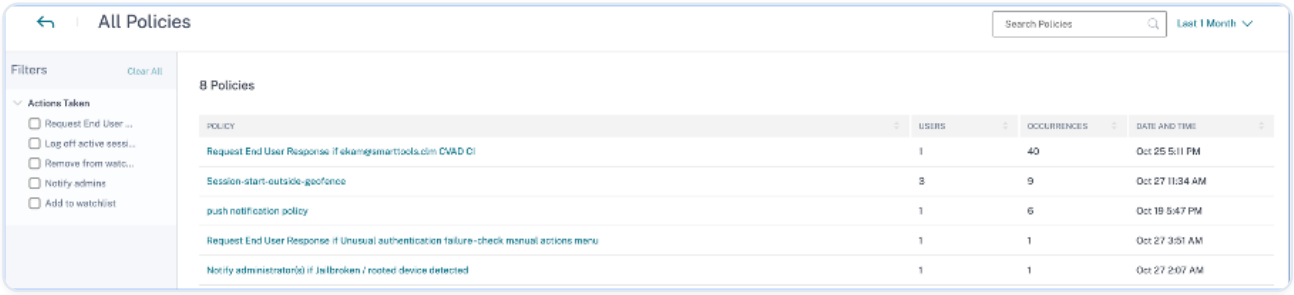
Displays the top five policies and actions applied on user profiles for a selected time period. Click the **See More** link on the **Policies and Actions** pane to get detailed information about the policies and actions.

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



Top Policies

The top five configured policies are determined based on the number of occurrences. When you are in the **Top Policies** section of the dashboard and select **See More**, you are redirected to the **All Policies** page.



All policies

This page provides detailed information about all the configured policies. When you select any policy, you are redirected to the Self-service search for Policies page. On the left pane, you can filter based on the actions applied.

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

When you select a user name, you are redirected to the risk timeline. The policy-based action is added to the user's risk timeline. When you select the action, its details are displayed on the right pane of the risk timeline.

Top Actions

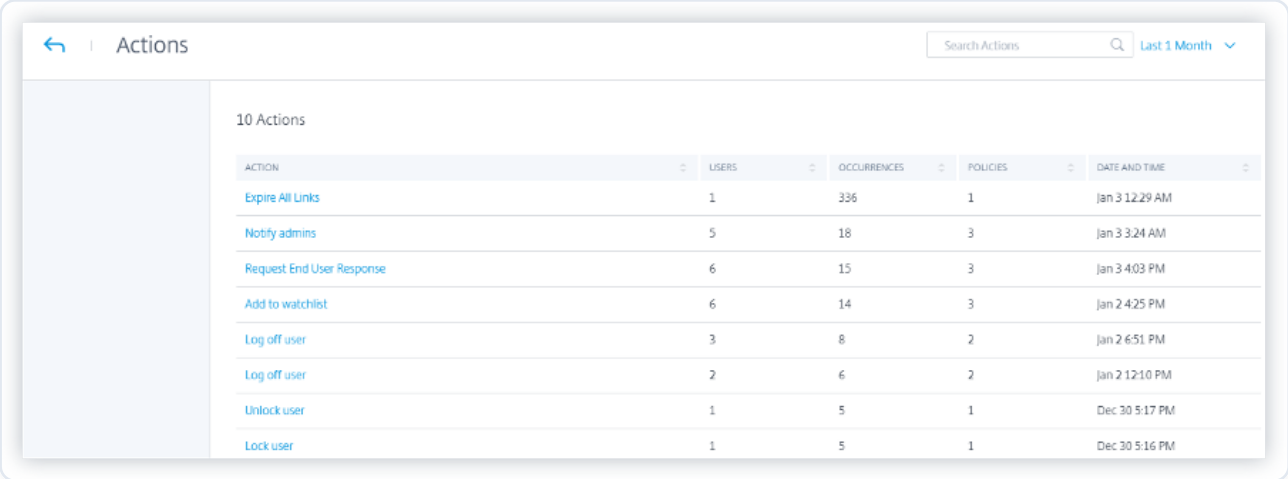
The top five actions associated with the policies that were applied to the user profiles. This section does not display the actions that you have applied manually on the user profiles. The top actions are determined by the number of occurrences.

Click **See More** to view all the policies-based actions on the **Actions** page.

Actions

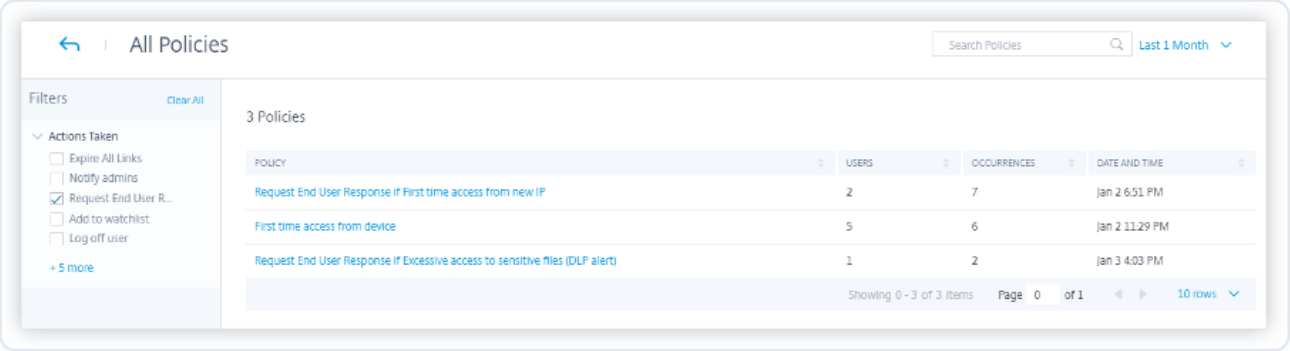
The page provides the list of all policies-based actions that have been applied to your users for the selected time period. You view the following information:

- Name of the action applied as per the policy
- Number of users on which the action has been applied
- Number of occurrences of the action
- Number of policies associated with the action
- Date and time of the applied action



Click an action to view all the associated policies. These policies are sorted based on the number of occurrences. For example, click **Request end user response** on the **Actions** page. The **All Policies** page displays all the policies associated with the **Request end user response** action.

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



On the **All Policies** page, click a policy to view the user events on which the action has been applied.

Risk Indicators

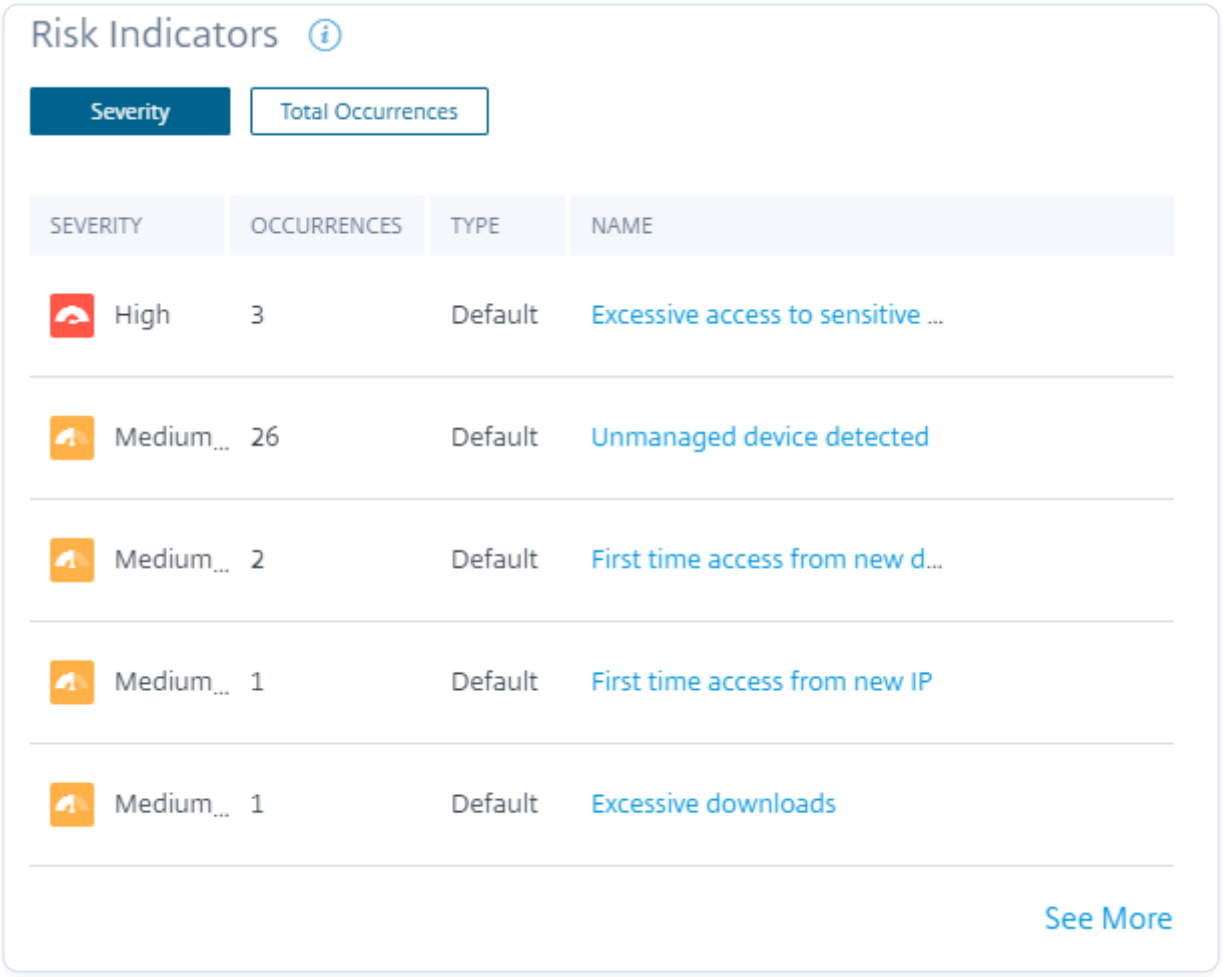
Summarizes the top five risk indicators for a selected time period. The risk indicators can be default or custom. For default risk indicators, Citrix Analytics collects data from the discovered data sources and on which the data processing is enabled.

For custom risk indicators, Citrix Analytics collects data from the following data sources based on the risky events generated:

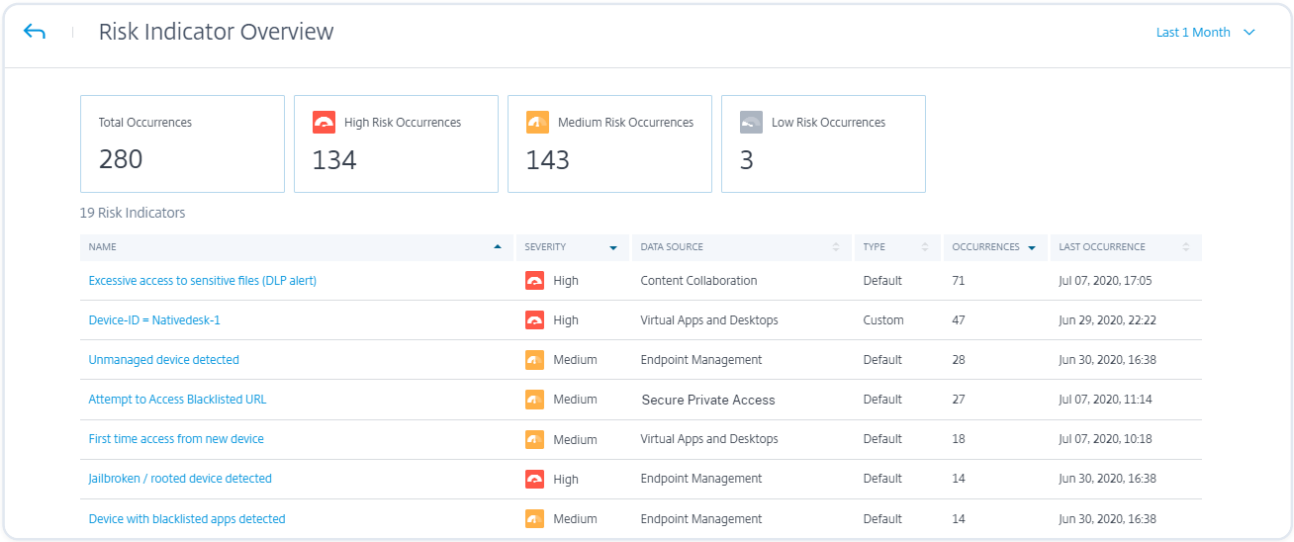
- Citrix Gateway
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops™
- Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)

On the **Risk Indicators** pane, you can view the top five risk indicators and sort them based on total occurrences or severity.

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



Click **See More** on the **Risk Indicators** pane to view the **Risk Indicator Overview** page.



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

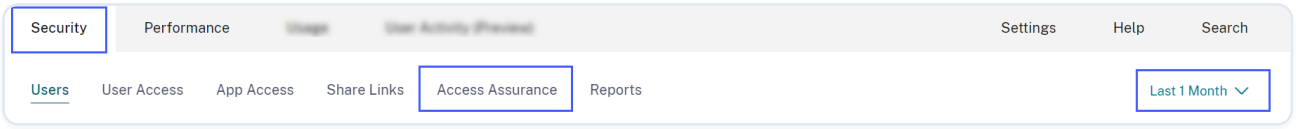
Access assurance dashboard

With an increase in remote working, as a Citrix IT administrator, you might want to get an assurance that your users are accessing {{page.cvad-onprem-product-name}} or {{page.daas-product-name}} (formerly Citrix Virtual Apps and Desktops service) from their usual and safe locations. If any users have logged on from unknown locations or new locations, you can validate their logon details and take necessary actions to mitigate any threats to your Citrix IT environment.

The Access Assurance dashboard provides an overview of the locations and networks from where your users are accessing virtual apps or virtual desktops. Citrix Analytics for Security receives these user logon events from Citrix Workspace app installed on the users' devices. For more details on supported versions, refer Citrix Workspace app version matrix.

View the dashboard

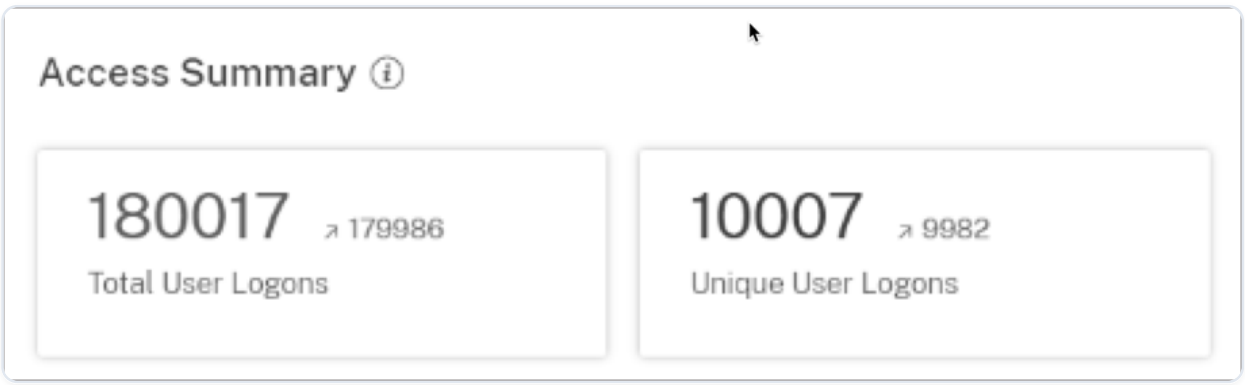
To view the dashboard, click **Security > Access Assurance**. Select the time period for which you want to view the logon details.



Access summary

The summary section of the dashboard provides the following information for a selected period:

1. Total number of user logons across the locations (worldwide).
2. Total number of unique user logons across the locations (worldwide).



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

Logon location

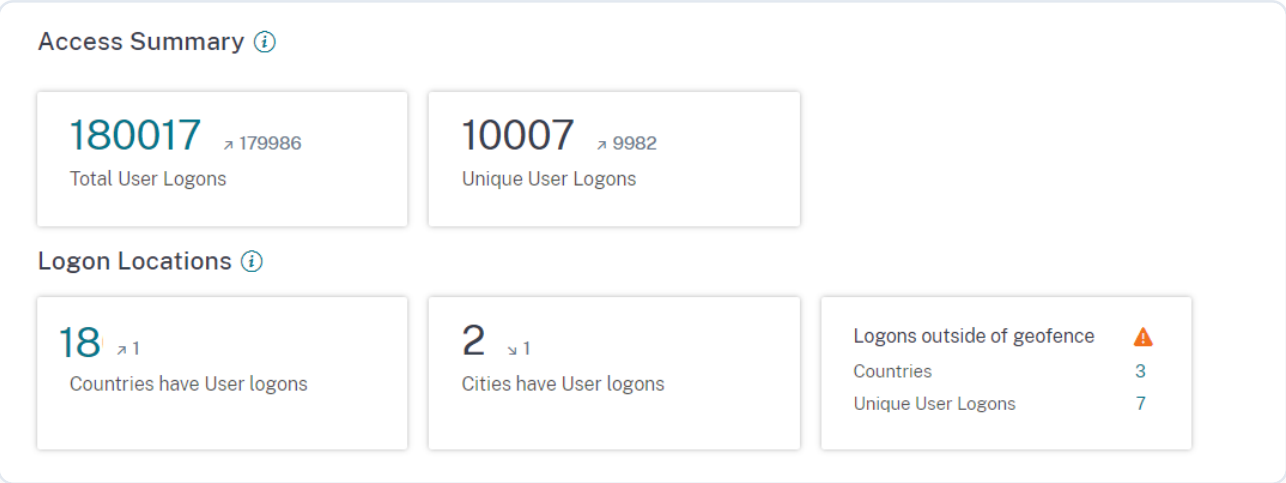
The **Logon Locations** section provides the following information for a selected period:

- Total number of countries from where the users have logged on.
- Total number of cities from where the users have logged on.
- Total number of countries and the unique user logons in the geofencing areas. To view the logon details from the geofencing areas, enable geofencing.
- Top 10 locations with unique user logons. Sometimes the top unique user logons are also from unknown cities and countries and these are listed under the **Unknown Locations** tab. The list of unknown locations is also a subset of the top 10 locations. To find the reasons why some locations are unidentified, see Locations identified as not available.

You can also view the upward or downward trend of the total user logons worldwide and the total unique user logons worldwide. For the top 10 locations, the **DEVIATION** column shows the change (positive (+) or negative (-)) in the user logons for each location. This comparison is based on the selected time period and the previous time period of equal length. For example, if you select the time period **Last 1 Month**, the user logon trend and the deviation are compared between the last 1 month and the previous to last 1 month.

NOTE

The location information is provided at the city and the country level and does not represent a precise geolocation. For more details on Access assurance, Geolocation, refer FAQ.

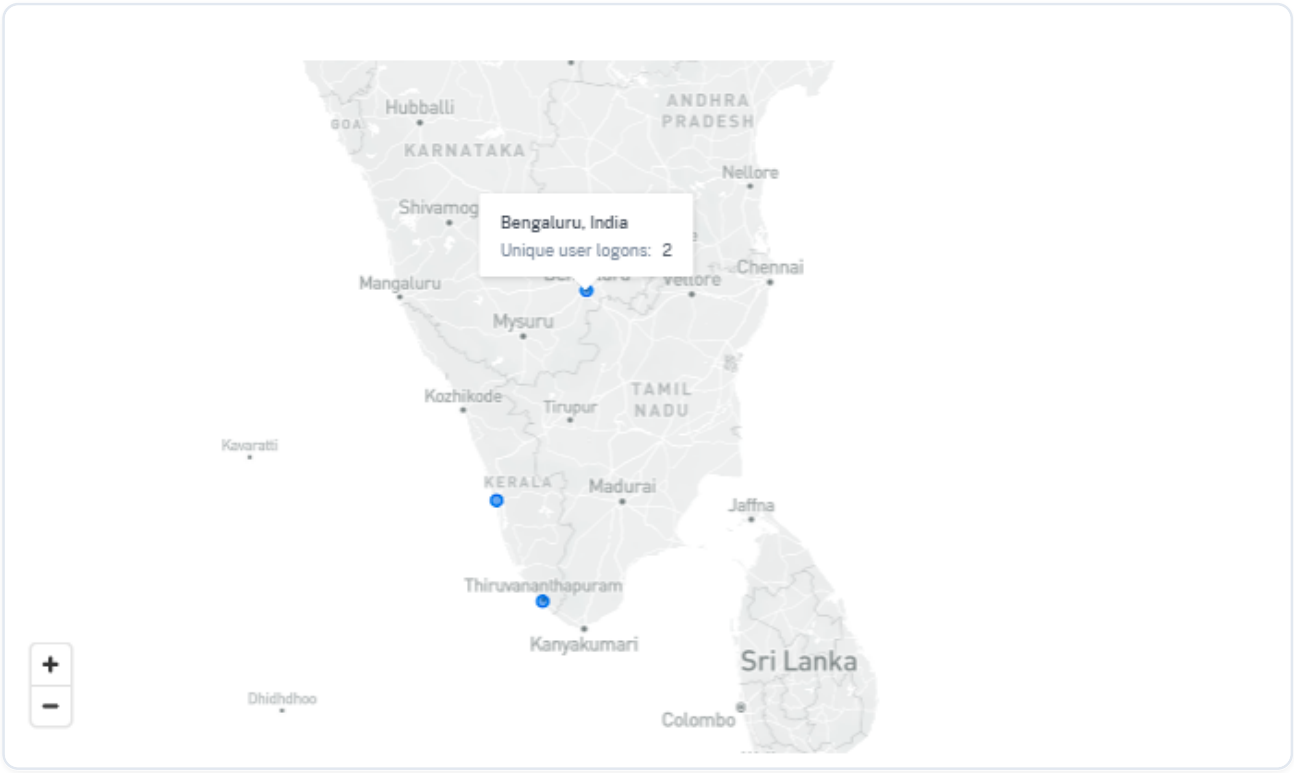


On the **Top 10 Unique Logon Locations** table, select a location to view the users and their access profiles and logon details.

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

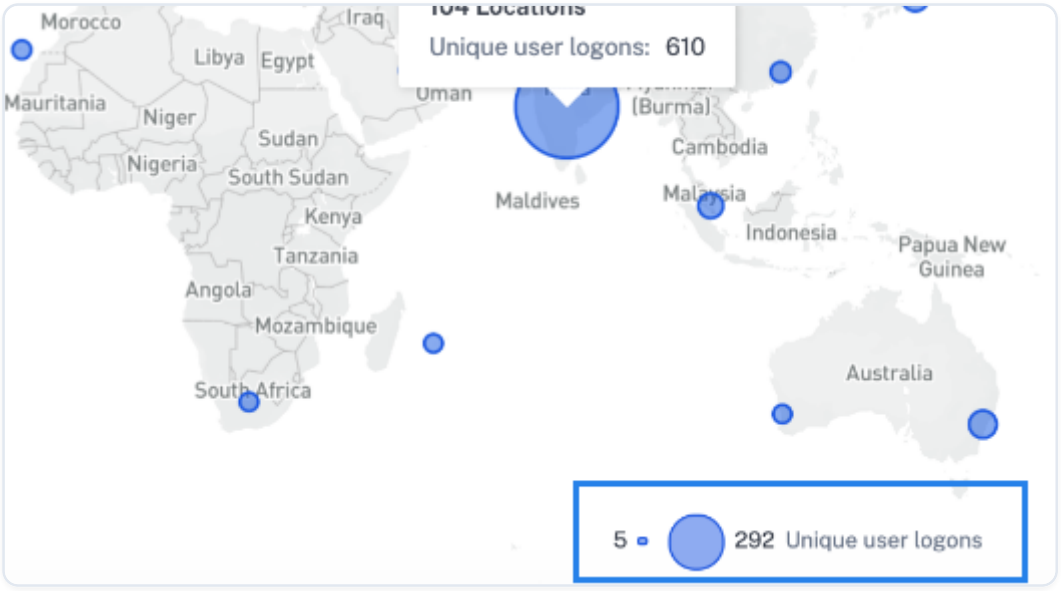


The map displays the number of unique users from various locations for a selected period. Hover over the blue bubble or zoom in to a location to view the total number of unique user logons from the location. Click the blue bubble to view the access details for a location.



On the bottom right corner of the map, you can view the range of the unique user logons. For a selected period, the small bubble indicates the minimum number of the unique user logons across the locations. The large bubble indicates the maximum number of the unique user logons across the locations.

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



Locations identified as not available

On the **Top 10 Unique Logon Locations** table, you might see that some locations are unknown or unavailable. Click an unknown location to view the corresponding user logon details on the **User Logons** page.

On the **User Logons** page, the **DATA** table displays the **NA** label if any country or city information is unavailable.

Hover over the **NA** label to view the reason why the location information is unavailable.



You might see one of the following scenarios for the unavailability of a location:

SCENARIO	REASONS
The city name and the country name are not available.	One of the following
	1. The users are using an unsupported version of Citrix Workspace app. To view

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

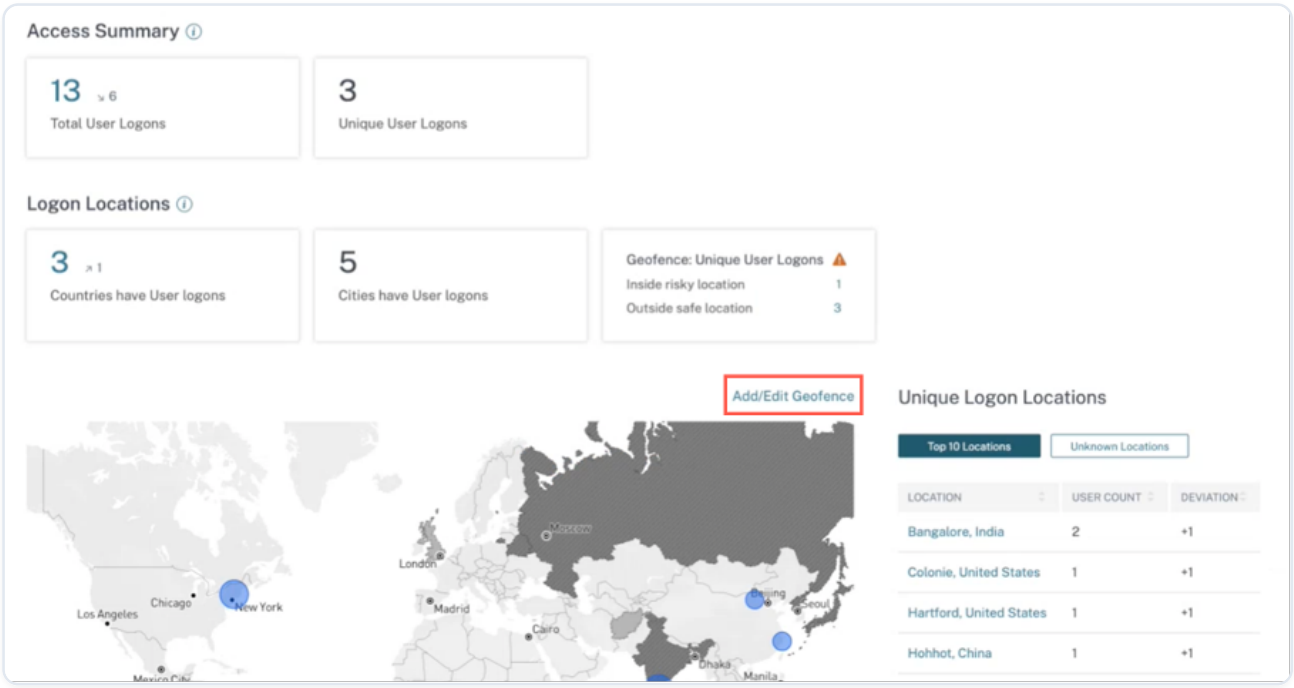
SCENARIO	REASONS
	the location information, update the client to a supported version.
	1. The user's network public IP address is unavailable and therefore Citrix Analytics cannot find the location.
	1. The external geo-location service is unable to send the location information to Citrix Analytics.
Locations with private IPs	The user's device is within a private network. In this case, the location information is unavailable to Citrix Analytics.
The country name is available but the city name is not available.	The user's device might be using a corporate IP. The corporate IP ranges are obfuscated in the external geo-location service. Therefore, the location information is unavailable to Citrix Analytics.

Enable geofencing

Geofencing helps you to identify the users who access virtual apps or virtual desktops from outside safe geofence and inside risky geofence areas. To view the **Access Summary** page, navigate to **Security > Access Assurance**.

By default, the **Geofence Settings** is always turned on. To configure your geofence, click **Add/Edit Geofence**.

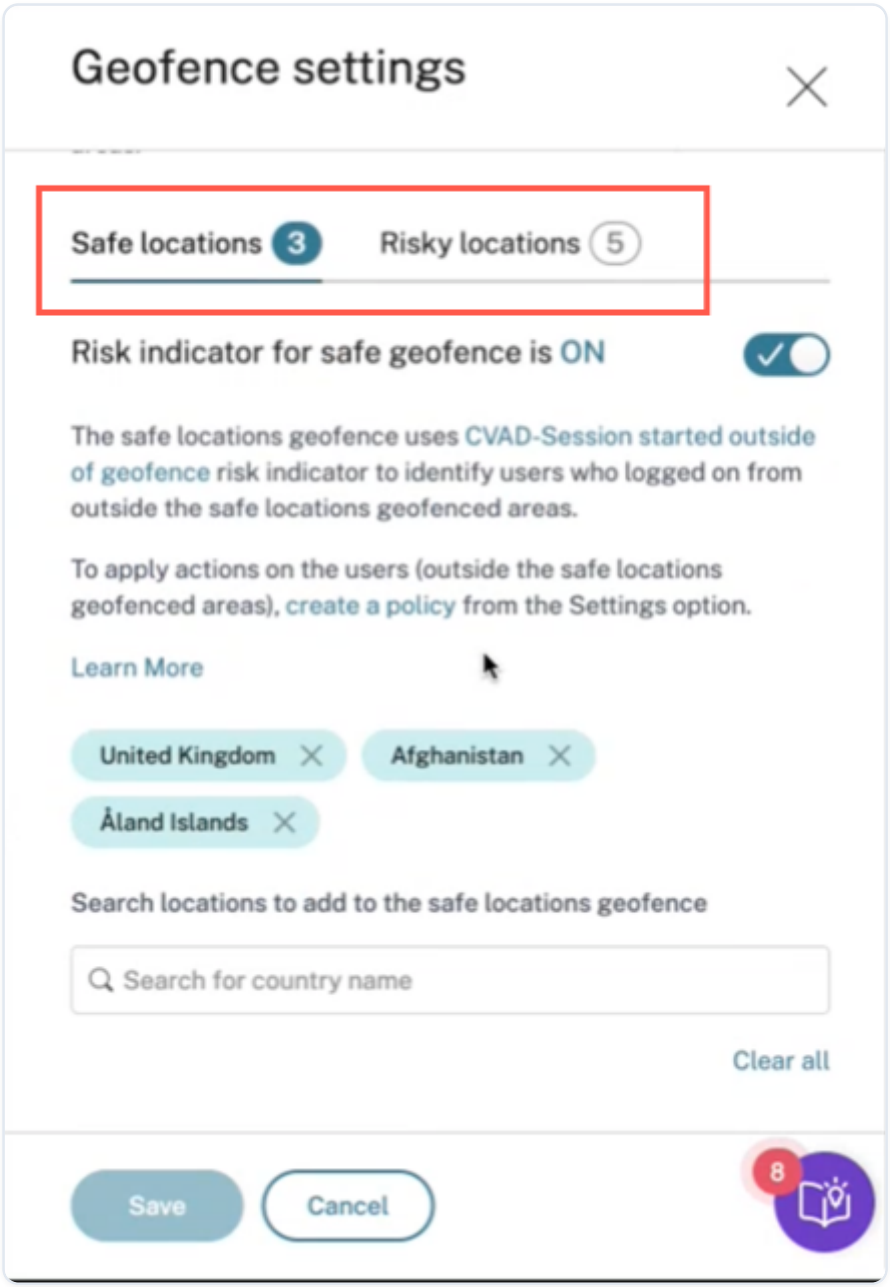
© 1997–2026 Citrix Systems, Inc. All rights reserved.



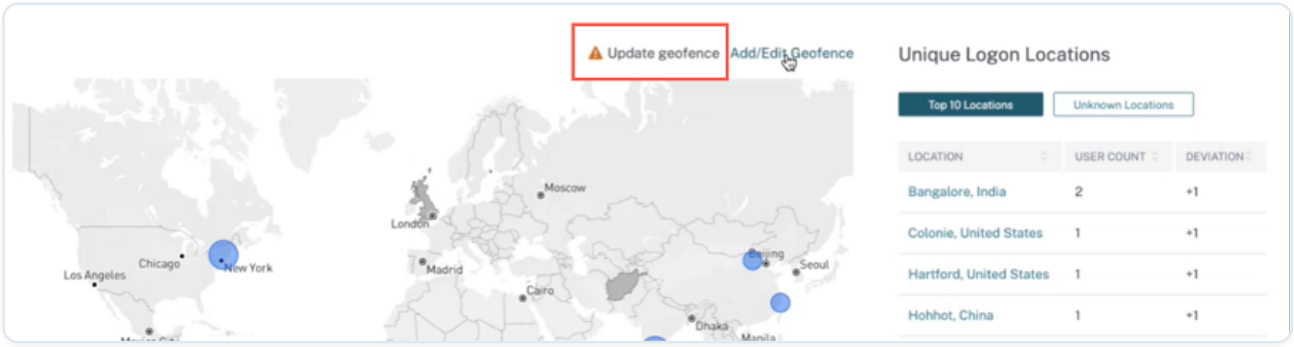
The **Geofence Settings** window appears with two tabs:

- **Safe locations**: You can configure or remove the countries that fall under safe location.
- **Risky locations**: You can configure or remove the countries that fall under risky location. You can also view the total number of safe and risky locations configured on each tab. To delete or remove a country from a Safe location geofence or Risk location geofence, click the close (X) sign next to the country. Click **Save** to save the Geofence settings.

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

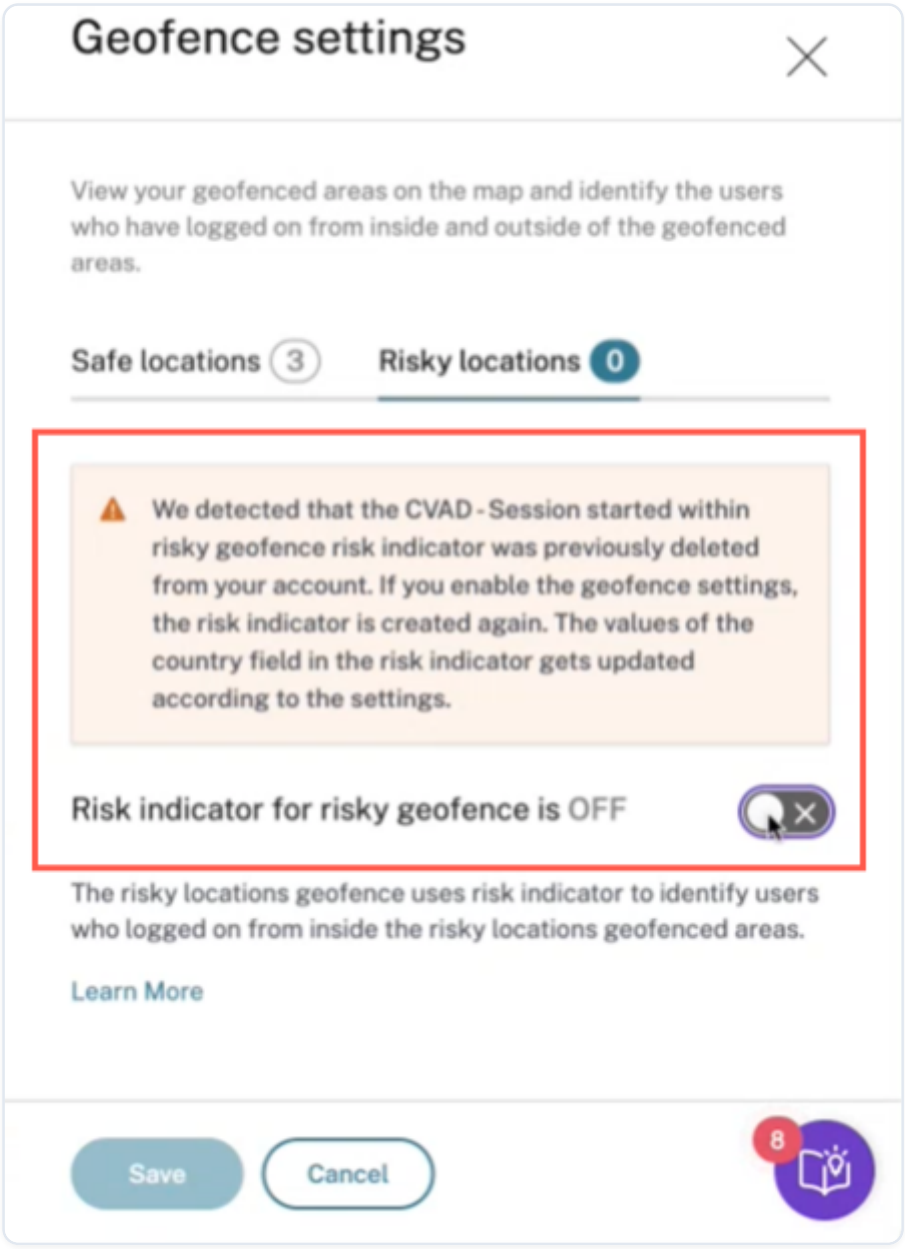


You can configure the countries that fall under Risky locations geofence. If there are no risk indicators added for Risky Locations geofence or the risk indicators are deleted, you can see a **Update geofence** warning message next to **Add/Edit Geofence**.



To recreate the indicator, navigate to **Risky locations** tab and turn on the **Risk indicator for risky geofence** toggle.

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

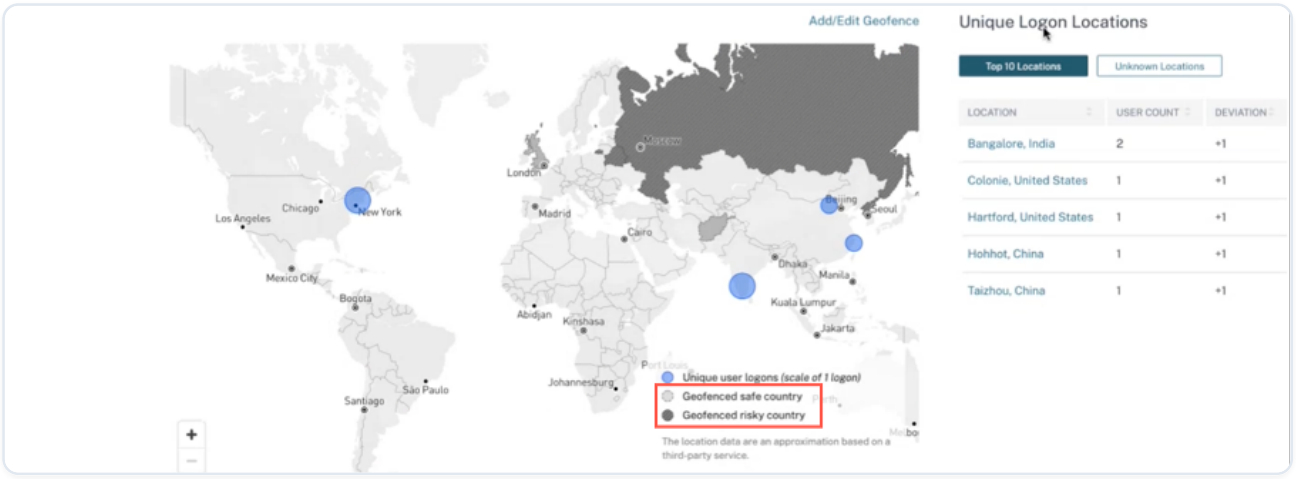


The indicator is created with the default list of risky locations.

The **Access Summary** page also displays the Geofenced safe and risky countries.

- Geofenced Safe countries are marked with the light gray circle.
- Geofenced Risky countries are marked with the dark gray circle.

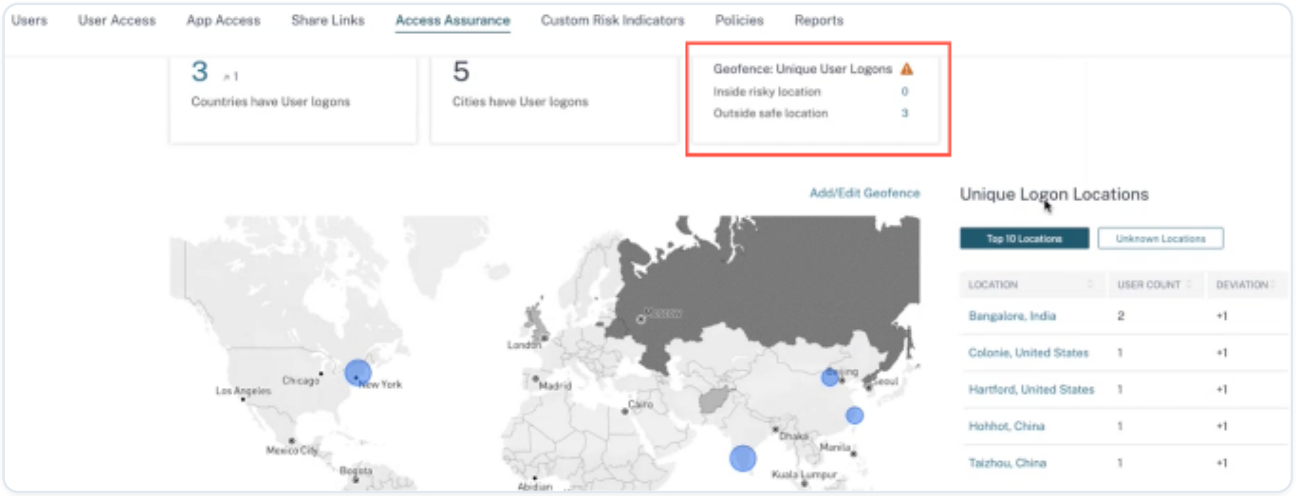
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Geofence: Unique User Logons

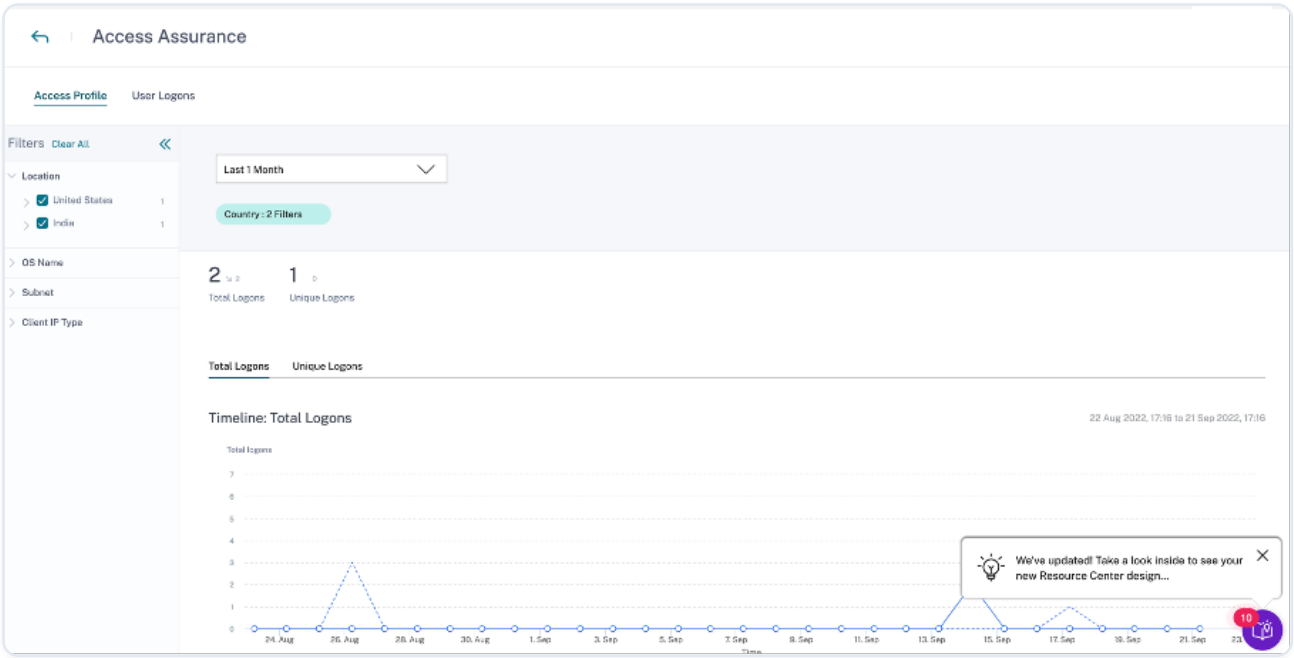
Navigate to Access Summary page to view Geofence: Unique User Logons. The card shows the number of Inside risky locations and Outside safe locations.

- **Inside risky location**: Identify users who logged on from inside the risky locations geofenced areas.
- **Outside safe location** Identify users who logged on from outside the safe locations geofenced areas.



For a detailed summary of the total and the unique user logons, click the number next to Inside risky location or Outside safe location.

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



This feature uses the following preconfigure custom risk indicator:

- **CVAD-Session started outside of geofence**: To monitor user logons outside safe geofence.
- **CVAD-Session started inside risky geofence**: To monitor user logons inside the risky geofence.

If any user logons are detected outside the geofence, the risk indicator is triggered and the Session started outside of geofence policy is applied on those users. The policy triggers the *Request End User Response* action and based on the user's response, you can take appropriate action to prevent threats from any suspicious logons. For more information, see preconfigured custom risk indicators.

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

NOTES

- In the **Geofence Settings**, when you modify the countries, the *CVAD-Session started outside of geofence* risk indicator also gets updated.
- For example, if you select and save the countries Australia and India as the new geofenced countries, the preconfigured condition of the risk indicator gets updated with the new countries, in addition to the United States (which is the default geofence). You can also remove the default geofenced country United States.

  Preconfigured condition of the risk indicator: `Event-Type = \"Session.logon\" AND Country != \"\" AND Country ~ \"\" AND Country != \"United States\"`

  After updating the **Geofenced Settings**, the condition of the risk indicator:

  `Event-Type = \"Session.logon\" AND Country != \"\" AND Country ~ \"\" AND Country NOT IN (\"Australia\", \"United States\", \"India\"`
- If the *CVAD-Session started outside of geofence* risk indicator is previously deleted from your account, enabling the **Geofence Settings** creates the risk indicator again. The geofenced countries of the risk indicator are controlled from the **Geofence Settings**.

After enabling the **Geofence Settings**, the map displays the geofenced areas and the unique user logons from these areas.

Logon network

In Access Assurance dashboard, you can now view the following additional user details:

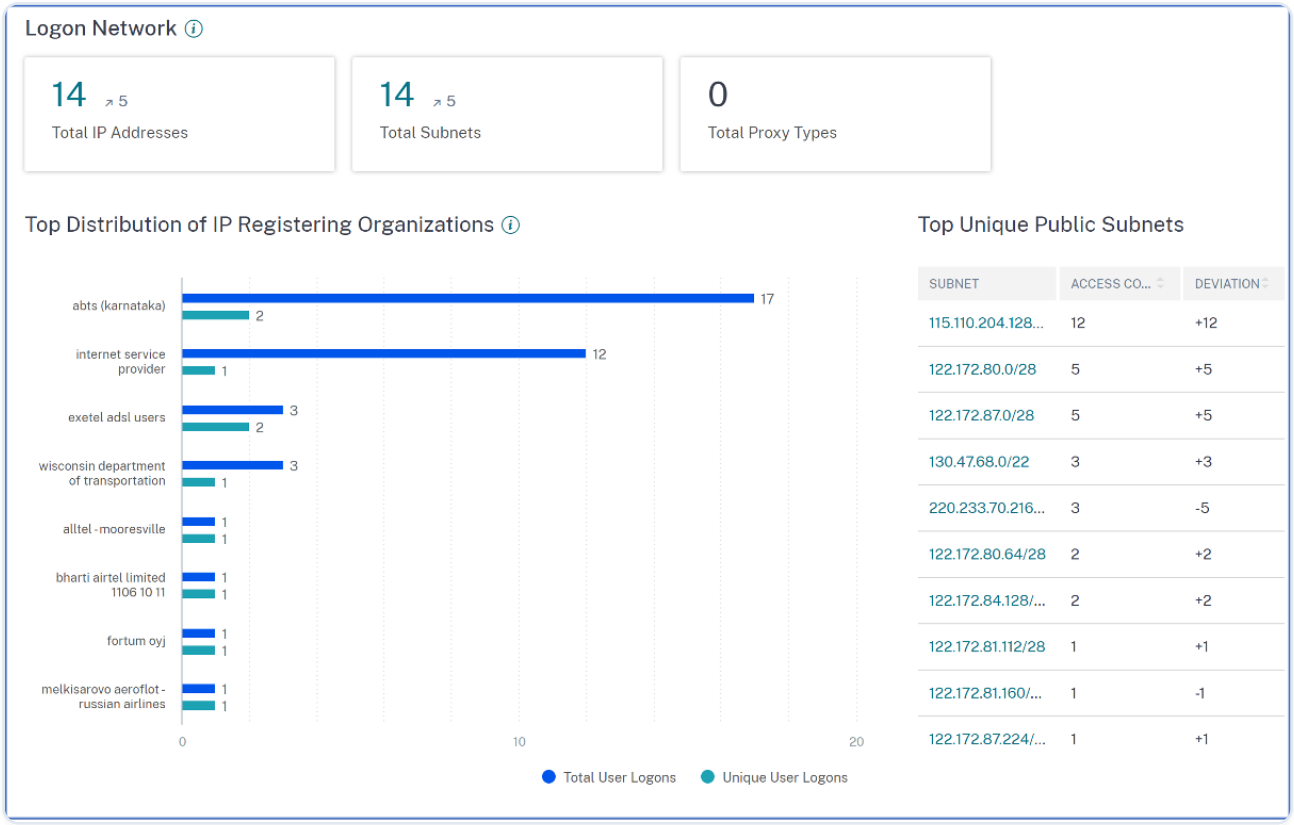
- The organizations associated with the IP addresses from which the users have logged on. These organizations include the entities such as corporate, government, educational entities, and internet service providers.
- The total unique public subnet and private subnet from where the users have logged on.
- The details that the user has logged on using proxies and private VPN services.

Using these additional details, as an administrator, you can validate the user logon details and ensure if the user logon is within the security expectation of the organization.

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

View user network details

Navigate to **Security > Access Assurance** and scroll down to view details under **Logon Network**.

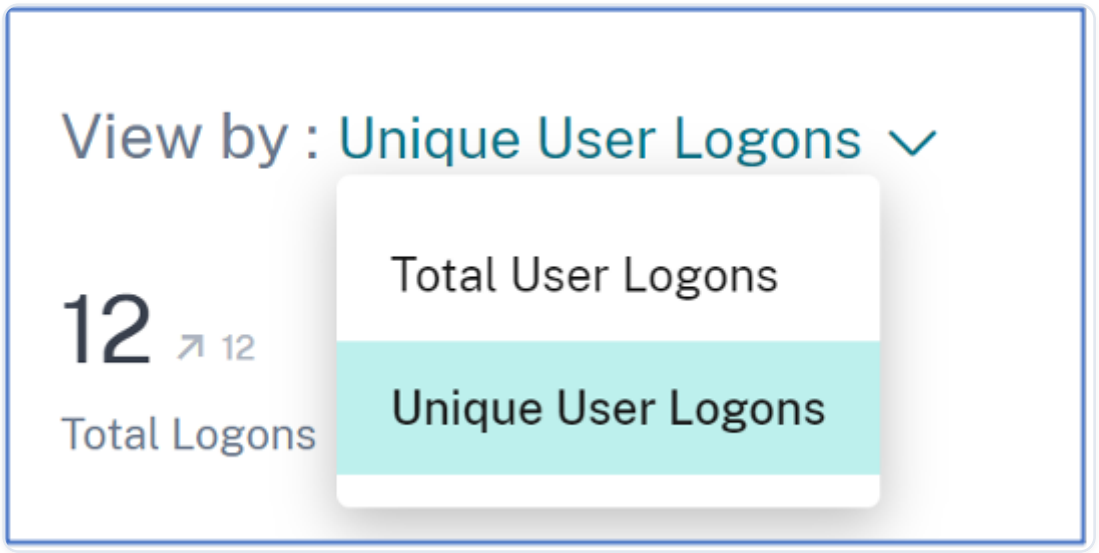


- **Total IP Addresses**: Indicates the total number of unique IP addresses used to log on to virtual sessions.
- **Total Subnets**: Indicates the total number of subnets used to log on to virtual sessions.
- **Total Proxy Types**: Indicates the total types of network or protocol utilized by the server to proxy the user connection.
- Under **Top Distribution of IP Registering Organizations**, you can visualize an overview of total user logons and unique logon details from each organization (ISP). You can click the chart to drill-down to view details of the users, and their access profiles and logon details associated with the selected organization.
- Under **Total Unique Public Subnets**, you can visualize an overview of the subnets, total user logons from each subnet, and the deviation trend in each subnet. You can click each subnet to drill-down to view details of the users, and their access profiles and logon details associated with the selected subnet.

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

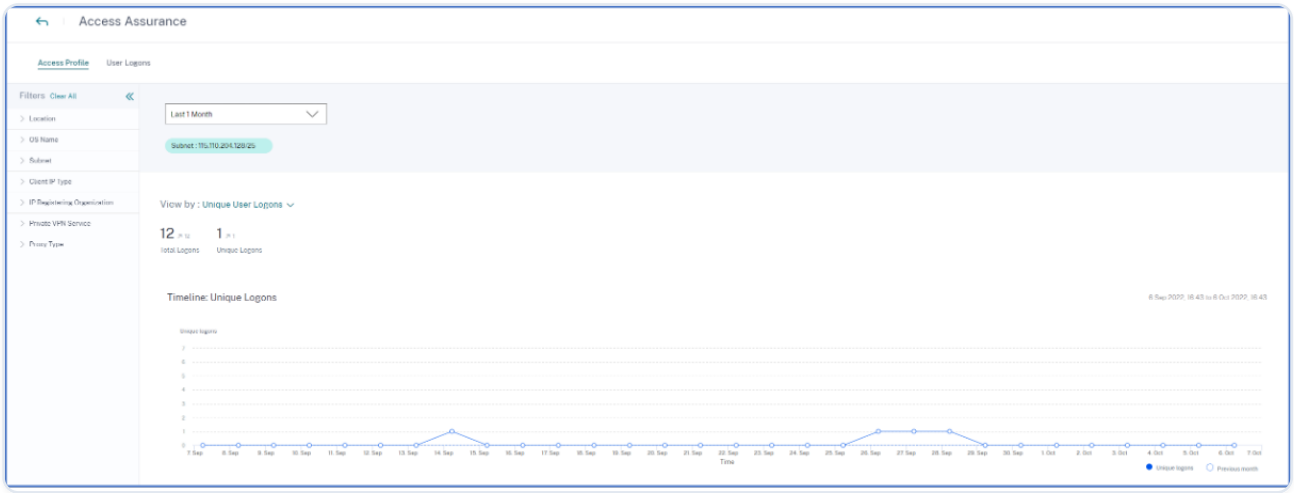
View access profiles of the users

When you drill-down any metric (location, organization, or subnet), the **Access Profile** page provides the summary of your users' accesses to virtual apps or virtual desktops from the selected locations. You can select the unique logon or total logon option to view the trend analysis for the selected period.



You can view the top access events for the selected metric (location, organization, or subnet). This information helps you to review the access patterns and the details for threat investigation and analysis.

The upward or downward trend for the total user logons and the unique user logons is compared based on the selected time period and previous time period of equal length. For example, if you select the time period as **Last 1 Month**, the trend is compared between last 1 month and previous to last 1 month.



Facets

You can use the following facets for the access events:

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

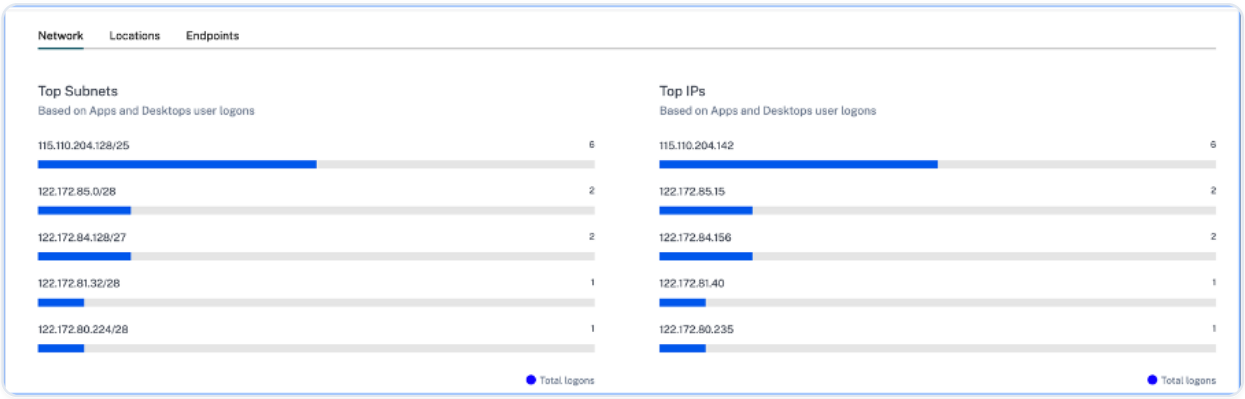
- **Location**- Filter the access events by countries and their cities.
- **OS**- Filter the access events by the operating systems and their versions.
- **Subnet**- Filter the access events by the subnets.
- **Client IP Type**- Filter the access events by public or private.
- **IP Registering Organization**- Filter the organization associated to the public IP address.
- **Private VPN Service**- Filter the access events by the private VPN network names.
- **Proxy Type**- Filter the access events by the proxy type classifications such as HTTP, web, Tor, and SOCKS.

NOTE

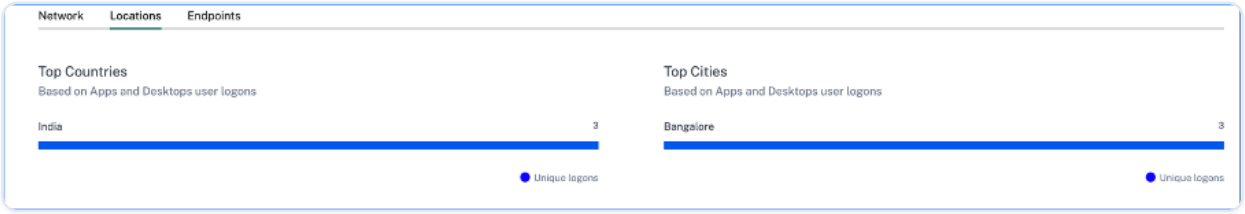
You might also see the not available label if data is either unavailable or unidentified.

Based on the applied filters, view the following information for total user logons and unique user logons:

- **Network**- The top subnets and the IP addresses from which the users have logged on to virtual apps or virtual desktops.

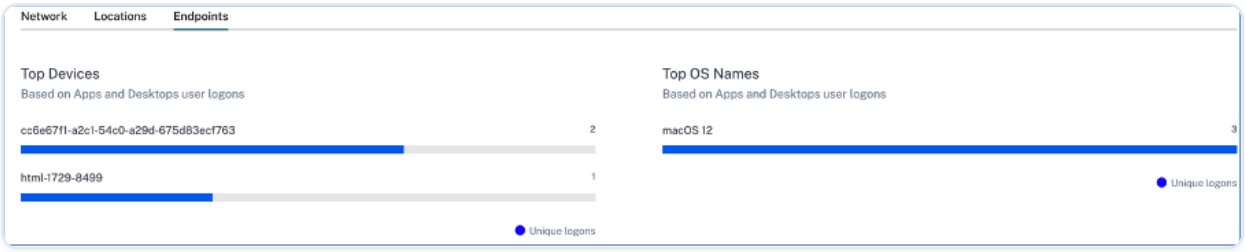


- **Locations**- The top countries and cities from which the users have logged on to virtual apps or virtual desktops.



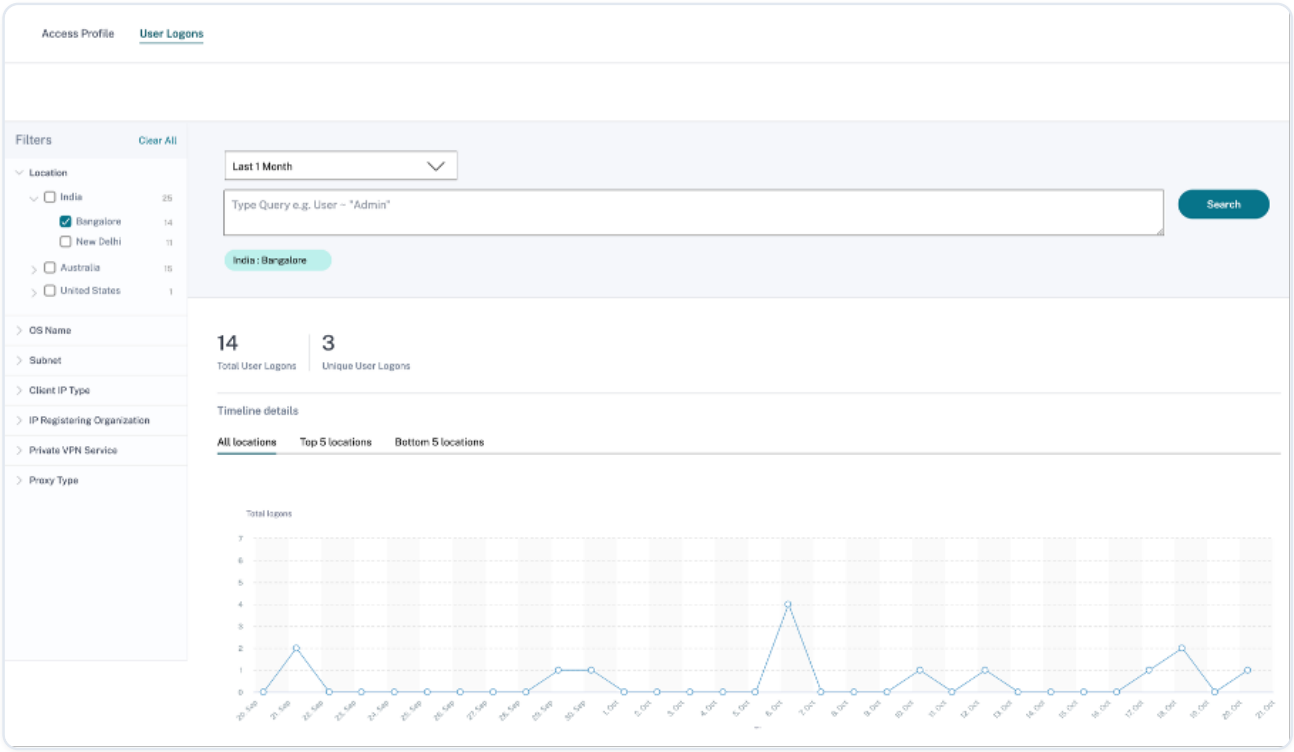
- **Endpoints**- The top device and OS names based on apps and desktops user logons.

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



View logons details of users

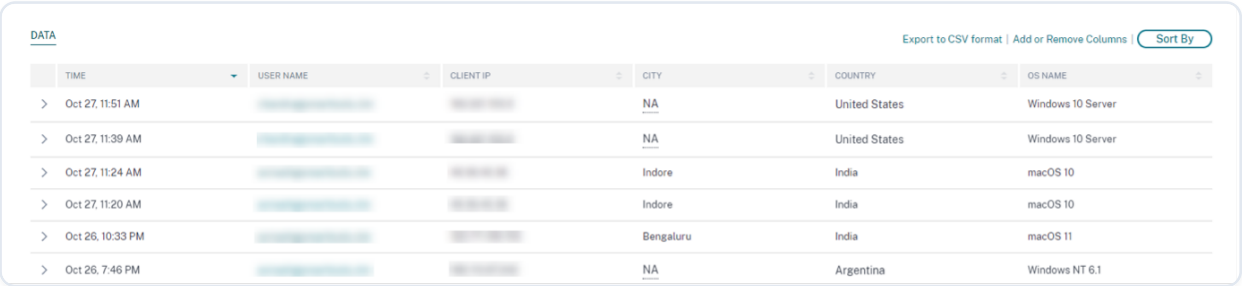
The **User Logons** page provides the details of the user logons to virtual apps or virtual desktops from the selected locations. This information helps you during threat investigation and analysis.



The **DATA** table displays the following logon details for the selected locations and the time period:

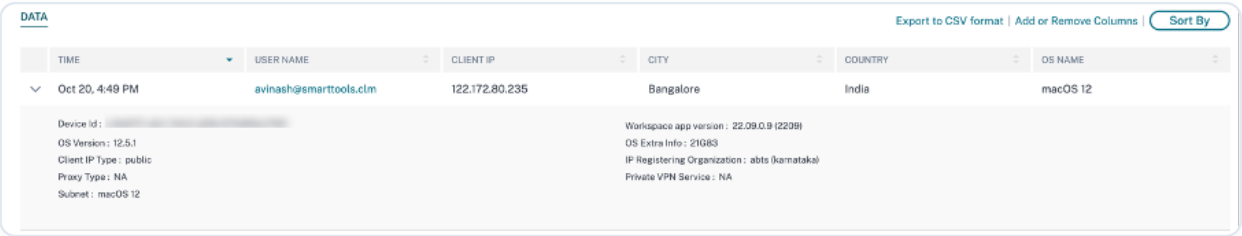
- **Time**. The date and time when the user logged on.
- **User name**. The identity of the user.
- **Client IP**. The IP address of the user device.
- **Client IP Type**. The type of IP address of the user such as public or private.
- **City and country**. The locations from where the user has logged on to virtual apps or virtual desktops.
- **Device ID**. The identity code of the user device.
- **OS name**. The operating system on the user device. For more information, see Self-service search for Apps and Desktops.

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



If you expand each event, you can see the following details:

- **OS version**. The version of the operating system on the user device. For more information, see Self-service search for Apps and Desktops.
- **OS extra information**- Any additional information of the operating system such as build numbers, service packs, and patches. For more information, see Self-service search for Apps and Desktops.
- **Workspace app version**. The build version of Citrix Workspace™ app or Citrix Receiver.



On the **DATA** table, you can do the following operations:

- Click **Add or Remove Columns** to update the table columns based on how you want to view the data.
- Click **Sort By** and select the data elements to perform a multi-column sort. For more information, see Multi-column sorting.
- Click **Export to CSV format** to download the data shown on the DATA table to a CSV file and use it for your analysis.

Search bar

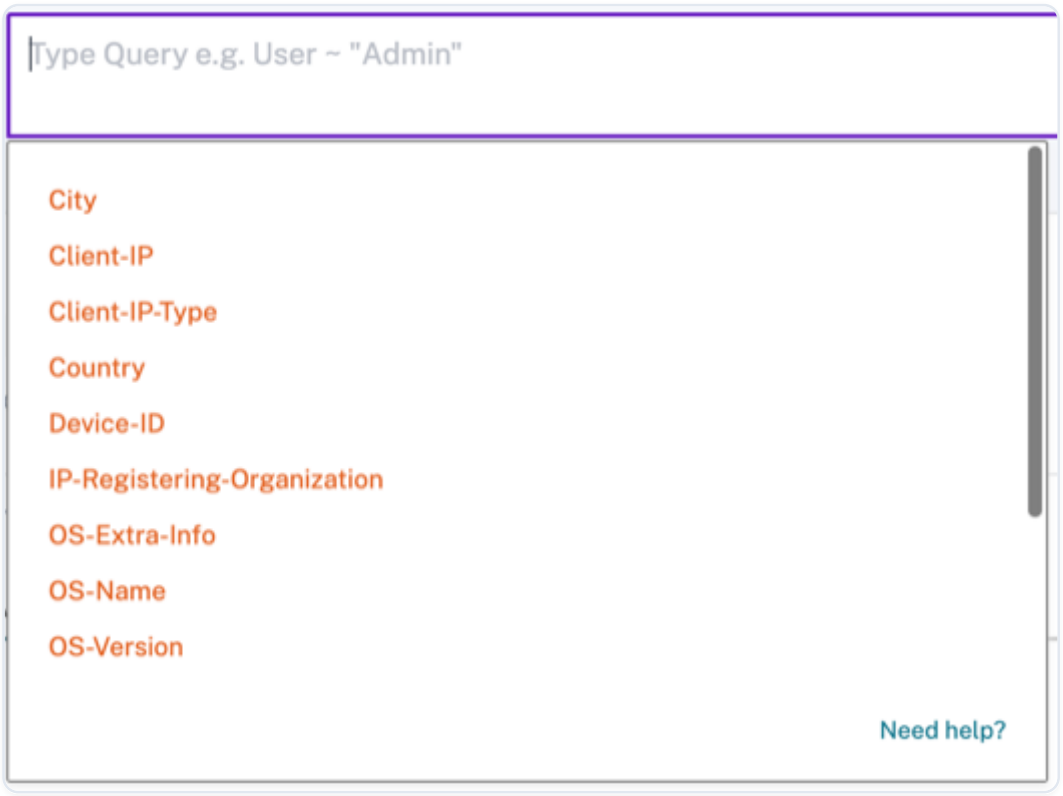
You can also use the search bar to define your query using the dimensions associated with a logon event.

For example:

```
User = “test user” AND Client-IP = “10.xx.xx.xx AND Client-IP-Type = public”
```

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

`User = “demo_user@citrix.com” AND OS-Major-Version = “macOS 10.13” AND OS-Minor-Version = 6`



Facets

You can use the following facets for the logon events:

- **Locations**- Filter the logon events by countries and their cities.
- **OS**- Filter the logon events by operating system and their versions.
- **Subnet**- Filter the access events by the subnets.
- **Client IP type**- Filter the access events by the public and the private IP types.
- **IP Registering Organization**- Filter the access events by user availed ISP.
- **Private VPN Service**- Filter the access events by the private VPN network names.
- **Proxy Type**- Filter the access events by the proxy type classifications such as HTTP, web, Tor, and SOCKS.

NOTE

You might also see the not available label if data is either unavailable or unidentified.

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

User risk timeline and profile

NOTE

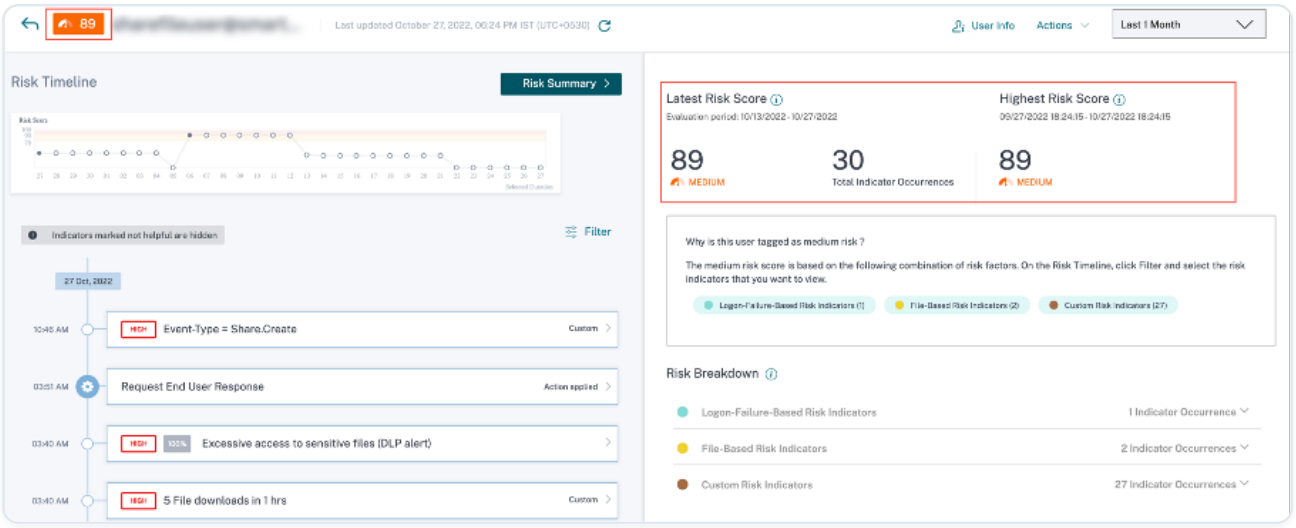
Attention: Citrix Content Collaboration™ and ShareFile has reached its end of life and is no longer available to users.

The User risk timeline on a user's profile enables you, as a Citrix Analytics administrator to gain deeper insights into a user's risky behavior. By default, the user risk timeline is displayed for the last one month. You can also see the corresponding actions taken on their account for a selected time period. From the User risk timeline, you can delve deeper into a user's profile to understand the following:

- Application Usage
- Data Usage
- Devices Usage
- Locations Usage

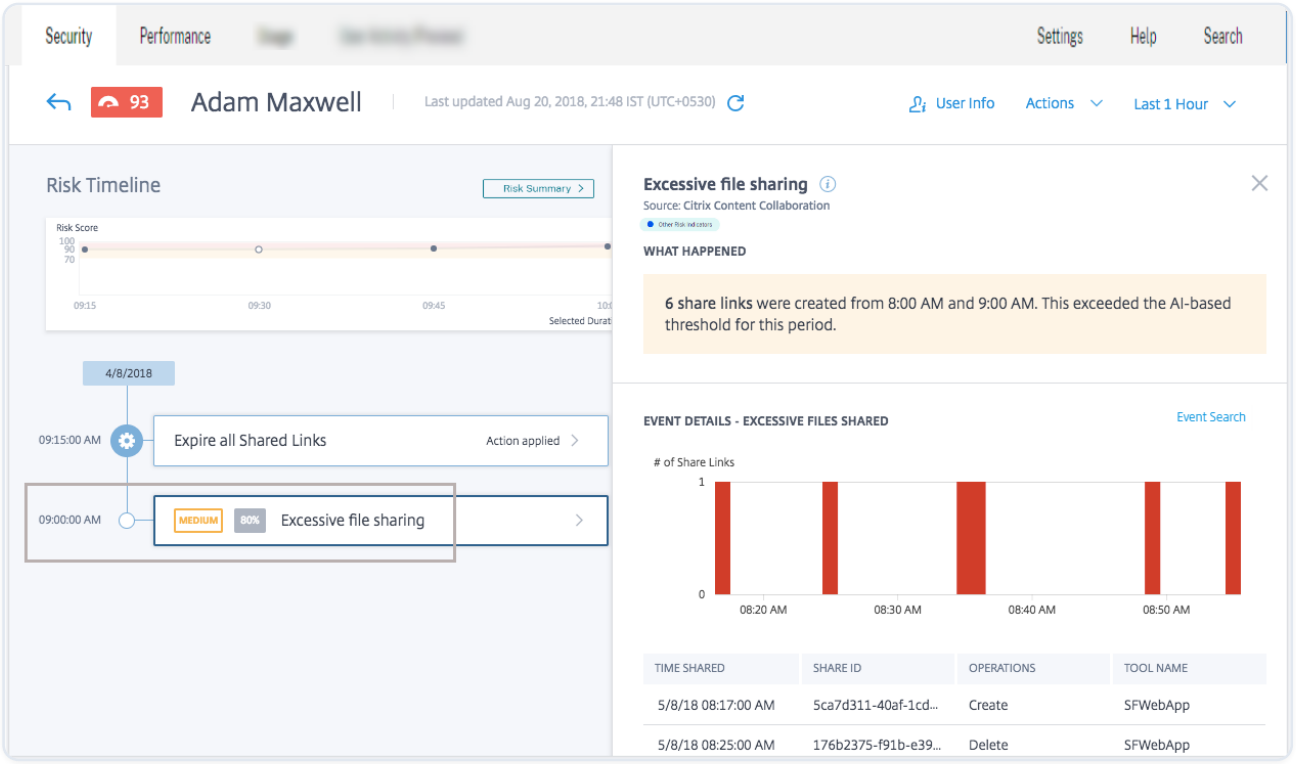
Also, you can view the risk score and risk indicator trends for the user and determine if the user is a high-risk user or not.

You can view the latest risk score of the user in the upper left corner of the User risk timeline page. The **Risk Summary** view reports show both the latest and historical maximum scores.



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

When you go to a user's risk timeline, you can select either a risk indicator or an action that has been applied to their account. If you choose one of the above, the right pane displays the risk indicator section or the action section.



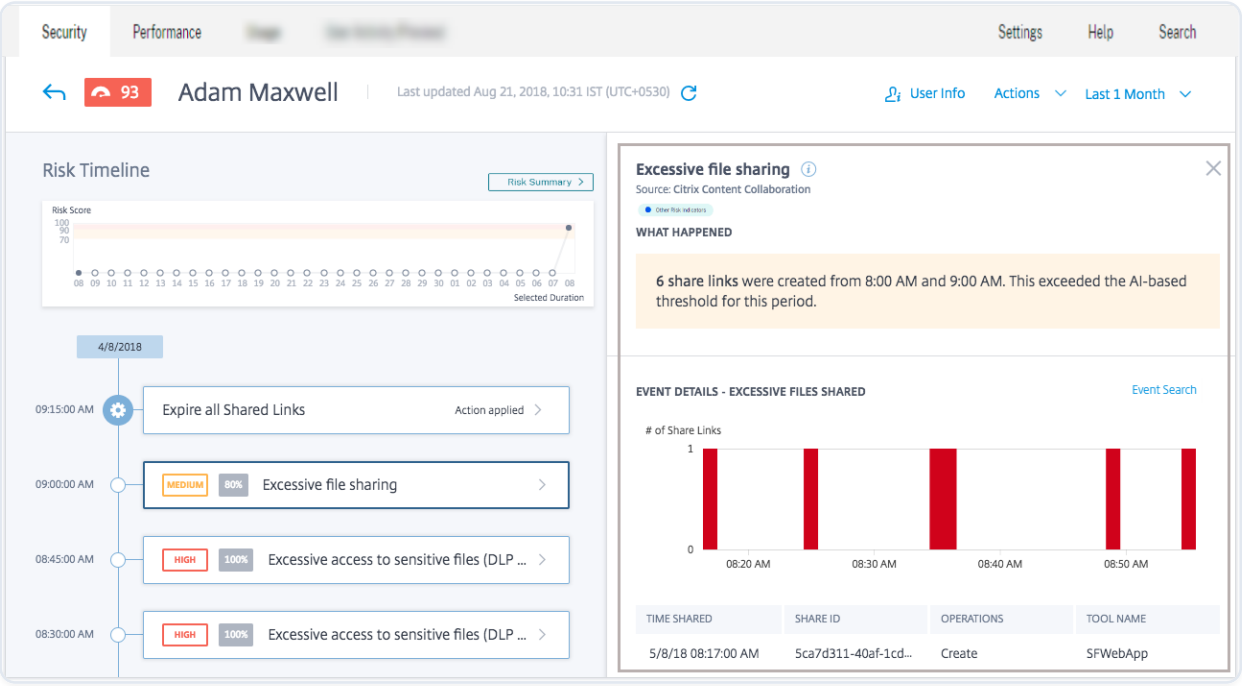
Risk timeline

The Risk Timeline displays the following information:

- **Risk indicators**. Risk Indicators are user activities that are suspicious or can pose a security threat to your organization. The indicators are triggered when the user's behavior deviates from their normal behavior. The risk indicators can be for the following data sources:
  - Citrix Content Collaboration
  - Citrix Gateway
  - Citrix Endpoint Management™
  - {{page.cvad-onprem-product-name}} or {{page.daas-product-name}} (formerly Citrix Virtual Apps and Desktops service)
  - {{page.secure-private-access-product-name}}

  When you select a risk indicator from the user's timeline, the risk indicator information section is displayed in the right pane. You can view the reason for the risk indicator along with details of the event. They are broadly categorized into the following sections:

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



- **What happened**. You can view a summary of the risk indicator here. For example, if you have selected the **Excessive file sharing** risk indicator. In the What happened section, you can view the number of share links sent to recipients and when the sharing event occurred.
- **Event details**. You can view individual event entries in graphical and tabular format along with details of the event. Click **Event Search** to access the self-service search page and view the events corresponding to the user's risk indicator. For more information, see **Self-service search**.
- **Additional contextual information**. You can view data shared, if any, during an event's occurrence in this section.

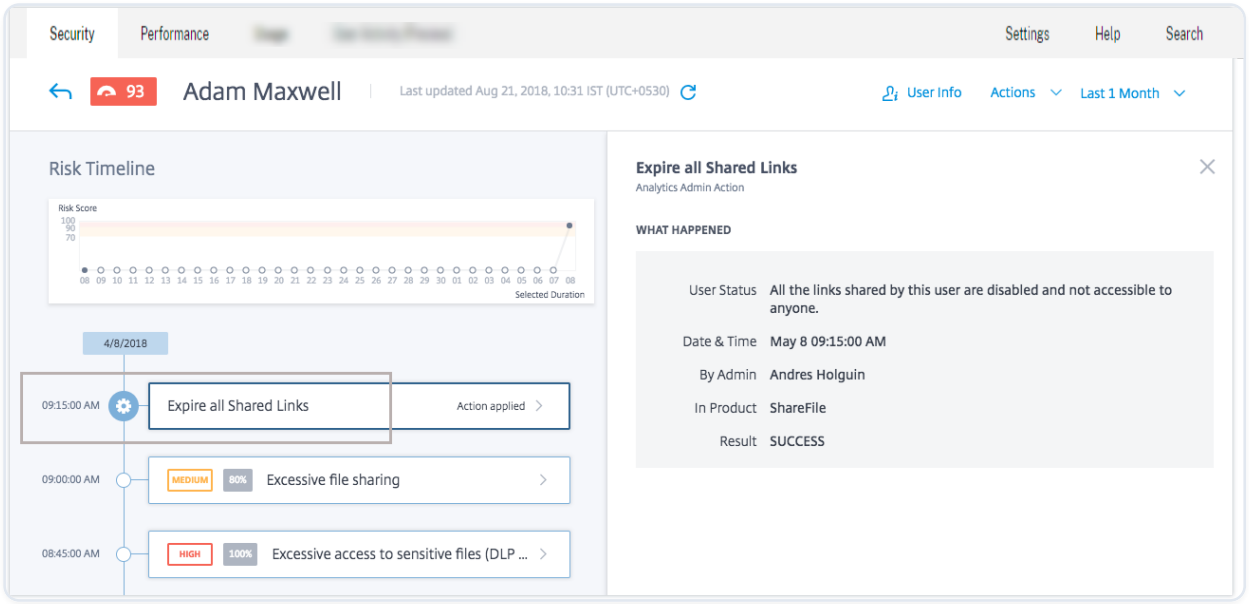
You can manually mark risk indicators as helpful or not helpful. For more information, see Provide feedback for User Risk indicators.

Learn more: Risk indicators

- **Actions**. Actions help you respond to suspicious events and prevent future anomalous events from occurring. Actions that have been applied to a user's profile are displayed on the risk timeline. These actions are either automatically applied to a user's account through configured policies or you can apply a specific action manually.

  Learn more: Policies and actions.

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



- **Privileged user events**. Privileged user events are triggered every time there is a change in the Admin or Executive privilege status of a user. When a risk indicator is triggered for a user, you can co-relate it with the specified privilege status change event. If necessary, you can apply the appropriate action on the user profile. The Admin or Executive privilege events displayed on the user risk timeline are as follows:

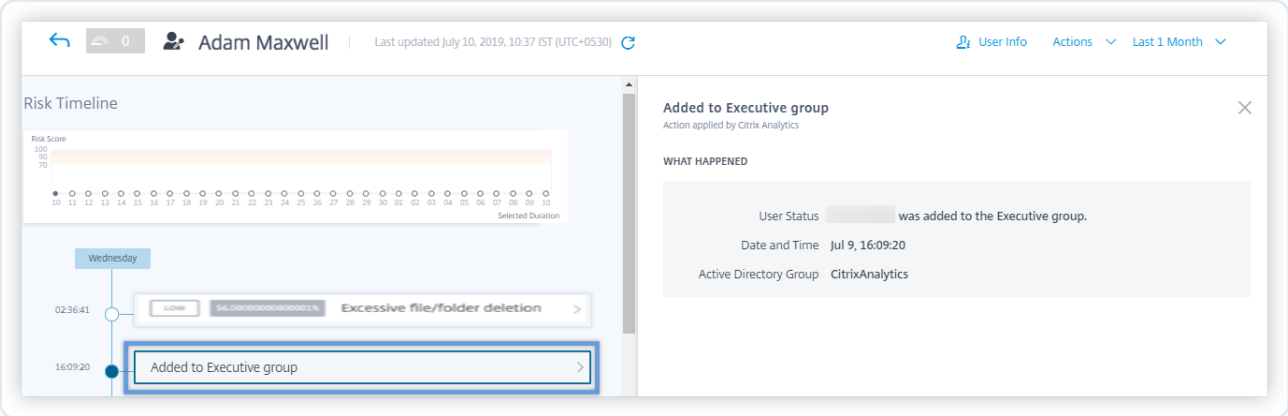
  - Added to Executive group
  - Removed from Executive group
  - Privilege elevated to Admin
  - Admin privilege removed

  Consider the user Adam Maxwell who was added to the Executive privileged group **CitrixAnalytics**. The **Added to Executive group** event is added to the user's risk timeline. Now, Adam starts excessively deleting files and folders and triggers the machine learning algorithm that detects unusual behavior. The **Excessive file or folder deletion** risk indicator is added to the user's risk timeline. You can compare the event and the risk indicator on the risk timeline. After the comparison, you can determine if the risk indicator was triggered as a consequence of the event. If so, you can apply appropriate actions to Adam's profile. For more information on privileged users, see Privileged users.

When you select an event from the user's timeline, the event information section is displayed in the right pane.

For an Executive, the right pane displays information such as **User status**, **Date and time**, and **Active Directory group**.

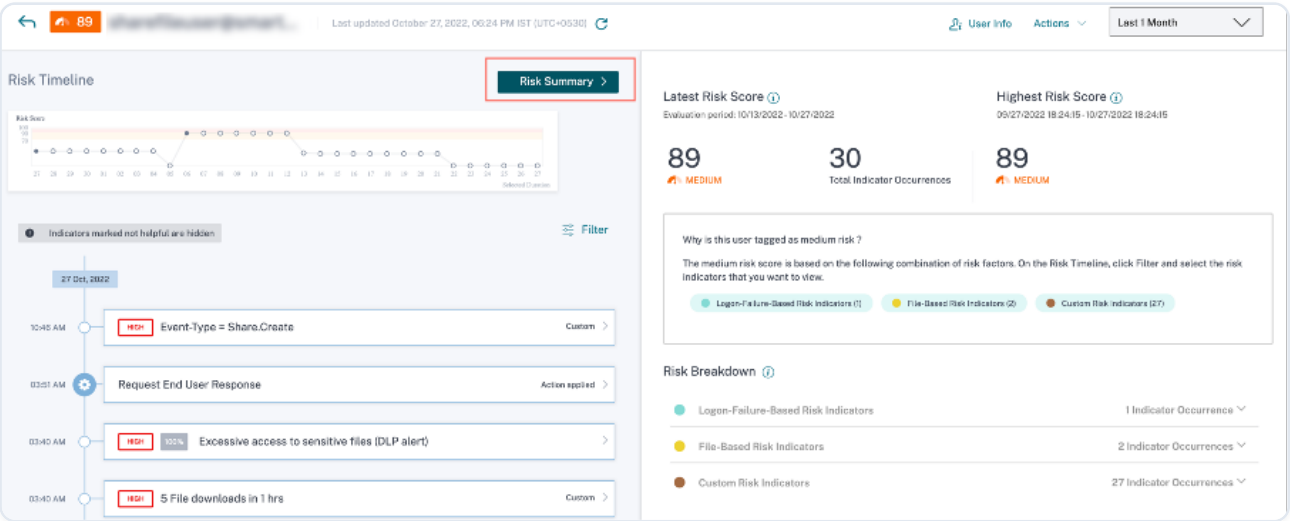
© 1997–2026 Citrix Systems, Inc. All rights reserved.



For an Admin privilege event, the right pane displays information such as **User status**, **Date and time**, and **In product**.

Risk summary

View the risk factors associated with the user that contributed to their risk score. You can see the risk score details taken as the maximum over the selected time period, along with the latest score and corresponding risk indicator count. Upon navigation to the User Timeline from either the main landing page or the Risky Users page, the time selection is preserved from the source page. For more information about the risk factors, see Citrix user risk indicators.



Click **Risk Summary** to view the following information:

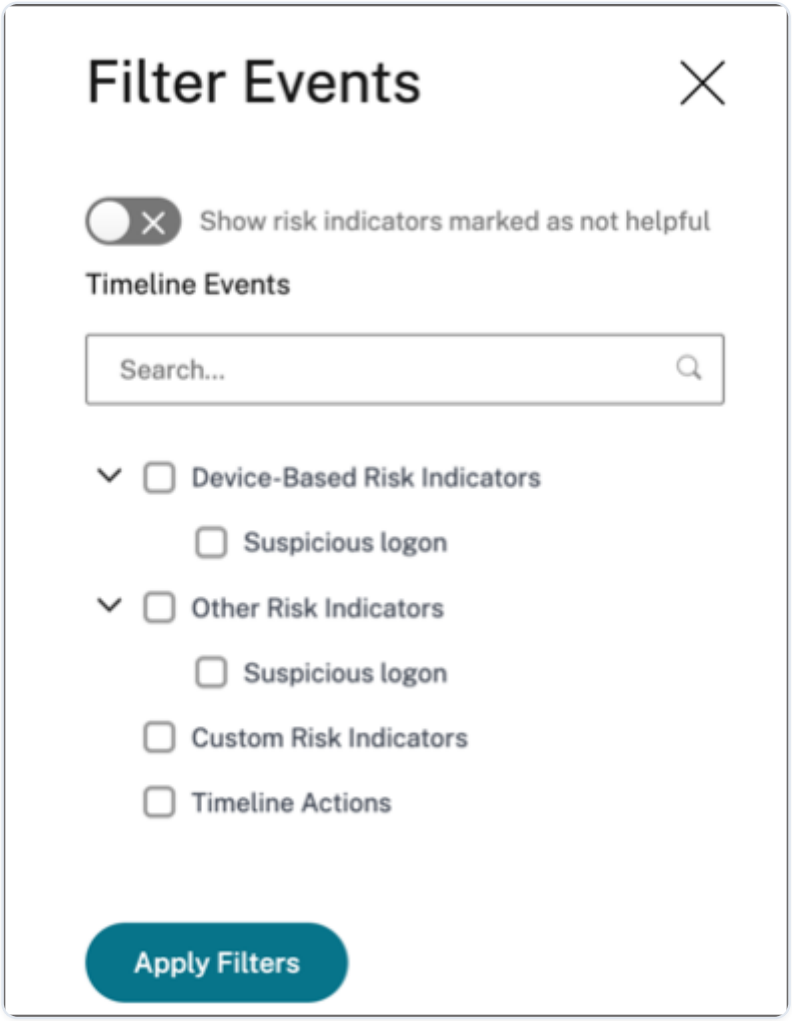
- **Latest risk score**: The latest risk score indicates the current risk of the user based on recent behavior. The risk score determines the level of risk a user poses to an organization over a trailing 2-week period. The risk score value is dynamic and varies based on user behavior analytics. Based on the score, a user can fall under one of the following categories: high-risk user, medium-risk user, low-risk user, and user with zero risk score. For more information about the user categories, see Users dashboard.

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

  - **Total indicator occurrences**: Indicates the total number of risk indicators triggered by the user in the last two weeks. These triggered risk indicators determine the user's risk score.

- **Highest Risk score**: The highest risk score indicates the maximum value of the risk scores calculated for this user within the selected time duration. It is representative of the aggregate risk for the user and may not always be equal to the latest risk score.
- **Risk factors**: Indicates one or more combinations of the risk factors associated with the user activities that contributed to the risk score.
- **Risk breakdown**: Indicates the number of risk indicators triggered by the user for each risk factor. Expand the row to view the details.

On the user timeline, click **Filter** and select the risk factors, the applied actions, or the privileged user status associated with the user and view the corresponding events.



User profile

The **User Profile** page displays the following user information that comes from the user's active directory:

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

- Job Title
- Address
- Email
- Phone
- Location
- Organization



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

Citrix® user risk indicators

NOTE

Attention: Citrix Content Collaboration™ and ShareFile have reached its end of life and is no longer available to users.

User risk indicators are user activities that look suspicious or can pose a security threat to your organization. These risk indicators span across all Citrix products used in your deployment. The risk indicators are triggered when the user's behavior deviates from the normal. Each risk indicator can have one or more risk factors associated with it. These risk factors help you to determine the type of anomalies in the user events. The risk indicators and their associated risk factors determine the risk score of a user.

The following are the risk factors associated with the risk indicators:

- **Device-based risk indicators**: Triggers when a user signs in from a device that is considered unusual based on the user's device history.
- **Location-based risk indicators**: Triggers when a user signs in from an IP address associated with a location that is considered unusual based on the user's location history.
- **IP-based risk indicators**: Triggers when a user attempts to access resources from an IP address that has been identified as suspicious, regardless of whether the IP address is unusual for the user.
- **Logon-failure-based risk indicators**: Triggers when a user has a pattern of excessive or unusual logon failures.
- **Data-based risk indicators**: Triggers when a user tries to exfiltrate data out of a Workspace session. The user behaviors under observation include copy or paste events, download patterns, and so on.
- **File-based risk indicators**: Triggers when a user's behavior regarding file access on Content Collaboration is considered unusual based on their historical access pattern. The user behaviors under observation include download patterns, access to sensitive content, activities indicative of ransomware, and so on.

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

- **Custom risk indicators**: Triggers when a pre-configured condition or a user-defined condition is met. For more information, see the following articles:
  - Custom risk indicators
  - Preconfigured custom risk indicators and policies
- Other risk indicators- The risk indicators that do not belong to any one of the predefined risk factors such as Device-based, Location-based, and Logon failure-based.

The risk indicators are also grouped into risk categories based on the risks that are similar. For more information, see Risk Categories.

The following table shows the correlation between the risk indicators, risk factors, and the risk categories.

PRODUCTS	USER RISK INDICATOR	RISK FACTOR	RISK CATEGORY
Citrix Endpoint Management	Device with blacklisted apps detected	Other risk indicators	Compromised endpoints
	Jailbroken or rooted device detected	Other risk indicators	Compromised endpoints
	Unmanaged device detected	Other risk indicators	Compromised endpoints
Citrix Gateway	End point analysis (EPA) scan failure	Other risk indicators	Compromised users
	Excessive authentication failures	Logon-failure-based risk indicators	Compromised users
	Impossible travel	Location-based risk indicators	Compromised users
	Logon from suspicious IP	IP-based risk indicators	Compromised users
	Suspicious logon	Device-based risk indicators, IP-based risk indicators,	Compromised users

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

PRODUCTS	USER RISK INDICATOR	RISK FACTOR	RISK CATEGORY
		Location-based risk indicators, and Other risk indicators	
	Unusual authentication failure	Logon-failure-based risk indicators	Compromised users
Citrix Secure Private Access	Attempt to access blacklisted URL	Other risk indicators	Insider threats
	Excessive data download	Other risk indicators	Insider threats
	Risky website access	Other risk indicators	Insider threats
	Unusual upload volume	Other risk indicators	Insider threats
Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) and on-premises Citrix Virtual Apps and Desktops	Impossible travel	Location-based risk indicators	Compromised users
	Potential data exfiltration	Data-based risk indicators	Data exfiltration
	Suspicious Logon	Device-based risk indicators, IP-based risk indicators, Location-based risk indicators, and Other risk indicators	Compromised users

You can manually mark risk indicators as helpful or not helpful. For more information, see Provide feedback for User Risk indicators.

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

Citrix Endpoint Management™ risk indicators

Device with blacklisted apps detected

Citrix Analytics detects access threats based on activity in a device with blacklisted apps and triggers the corresponding risk indicator.

The **Device with blacklisted apps detected** risk indicator is triggered when Endpoint Management service detects a blacklisted app during software inventory. The alert ensures that only authorized apps are run on devices that are on your organization's network.

The risk factor associated with the Device with blacklisted apps detected risk indicator is the Other risk indicators. For more information about the risk factors, see Citrix user risk indicators.

When is the device with blacklisted apps detected risk indicator triggered?

The **Device with blacklisted apps detected** risk indicator is reported when blacklisted apps are detected on a user's device. When Endpoint Management service detects one or more blacklisted apps on a device during software inventory, an event is sent to Citrix Analytics.

Citrix Analytics monitors these events and updates the user's risk score. Also, it adds a **Device with blacklisted apps detected** risk indicator entry to the user's risk timeline.

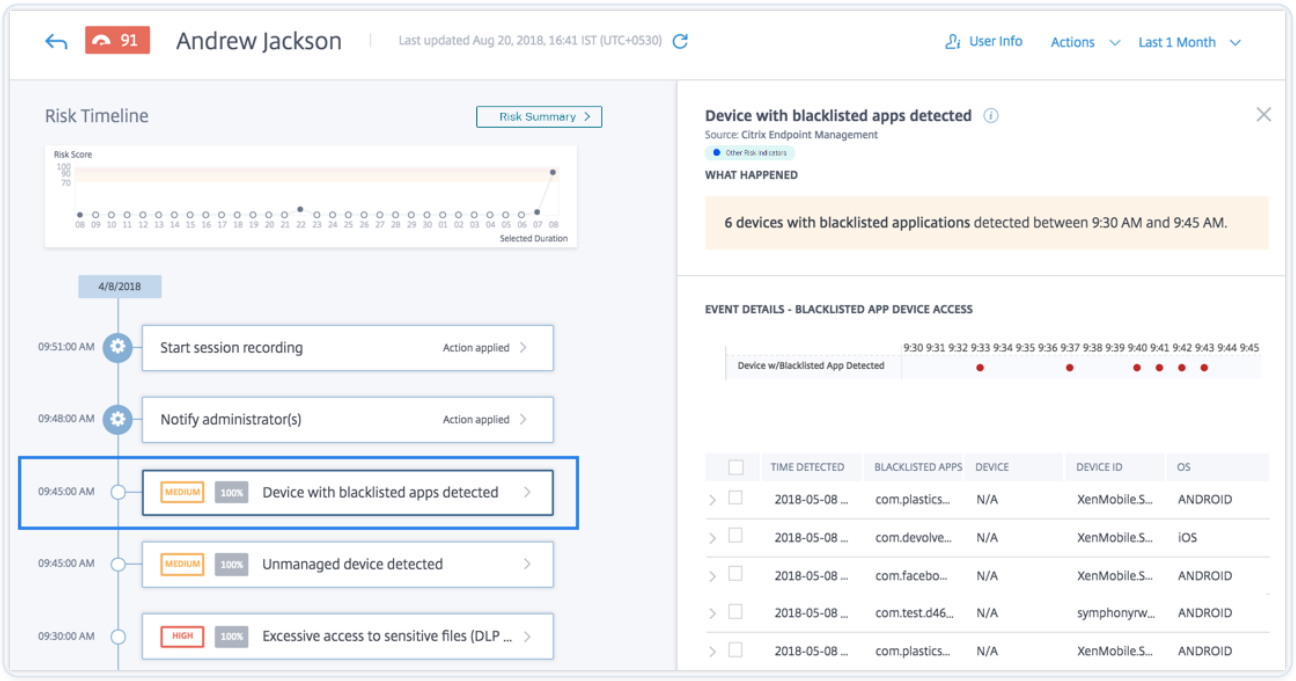
How to analyze the device with blacklisted apps detected risk indicator?

Consider the user Andrew Jackson, who used a device that had blacklisted apps recently installed. Endpoint Management reports this condition to Citrix Analytics, which assigns an updated risk score to Andrew Jackson.

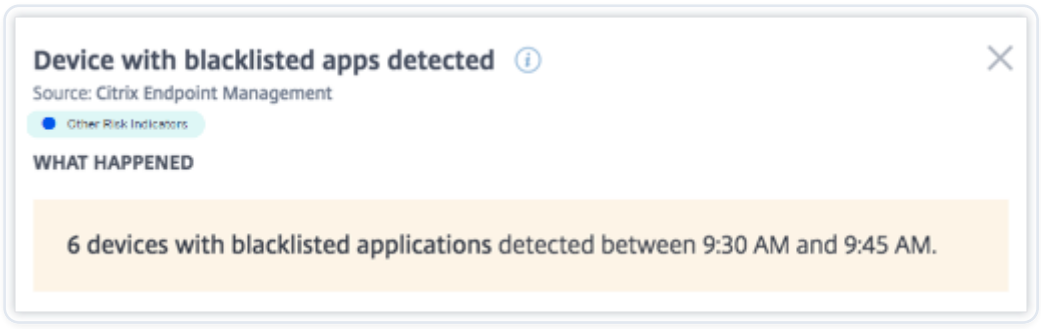
From Andrew Jackson's risk timeline, you can select the reported **Device with blacklisted apps detected** risk indicator. The reason for the event is displayed along with details such as the list of blacklisted apps, time Endpoint Management detected the blacklisted app, and so on.

To view the **Device with blacklisted apps detected** risk indicator for a user, navigate to **Security > Users**, and select the user.

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

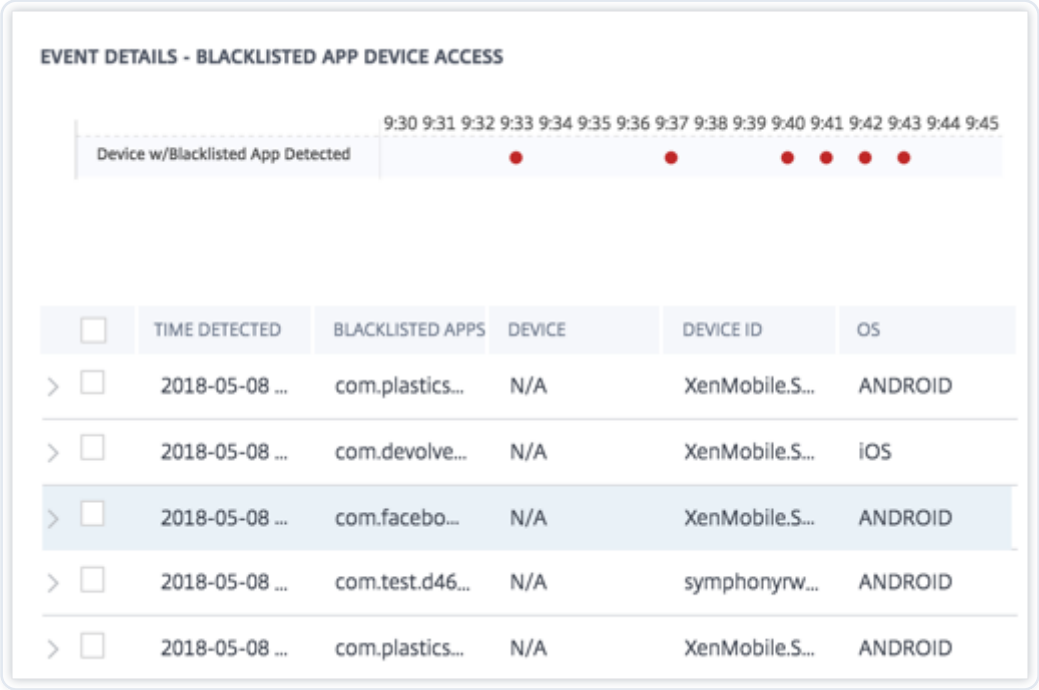


- In the **WHAT HAPPENED** section, you can view the summary of the event. You can view the number of devices with blacklisted applications detected by the Endpoint Management service and the time the events occurred.



- The **EVENT DETAILS – BLACKLISTED APP DEVICE ACCESS** section, the events are displayed in graphical and tabular format. The events are also displayed as individual entries in the graph, and the table provides the following key information:
  - **Time detected**- When the presence of blacklisted apps reported by Endpoint Management.
  - **Blacklisted apps**- The blacklisted apps on the device.
  - **Device**- The mobile device used.
  - **Device ID**- Information about the ID of the device that is used to log on to the session.
  - **OS**- The operating system of the mobile device.

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



NOTE

In addition to viewing the details in a tabular format, you can click the arrow against an alert's instance to see more details.

What actions you can apply to the user?

You can perform the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Actions** menu, select an action and click **Apply**.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

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

Jailbroken or rooted device detected

Citrix Analytics detects access threats based on jailbroken or rooted device activity and triggers the corresponding risk indicator.

The **Jailbroken or rooted device** risk indicator is triggered when a user uses a jailbroken or rooted device to connect to the network. Secure Hub detects the device and reports the incident to Endpoint Management service. The alert ensures that only authorized users and devices are on your organization's network.

The risk factor associated with the Jailbroken or rooted device risk indicator is the Other risk indicators. For more information about the risk factors, see Citrix user risk indicators.

When is the jailbroken or rooted device detected risk indicator triggered?

It is important for security officers to be able to ensure that users connect using network-compliant devices. The **Jailbroken or rooted device detected** risk indicator alerts you to users with iOS devices that are jailbroken or Android devices that are rooted.

The **Jailbroken or rooted device** risk indicator is triggered when an enrolled device becomes jailbroken or rooted. Secure Hub detects the event on the device and reports it to the Endpoint Management service.

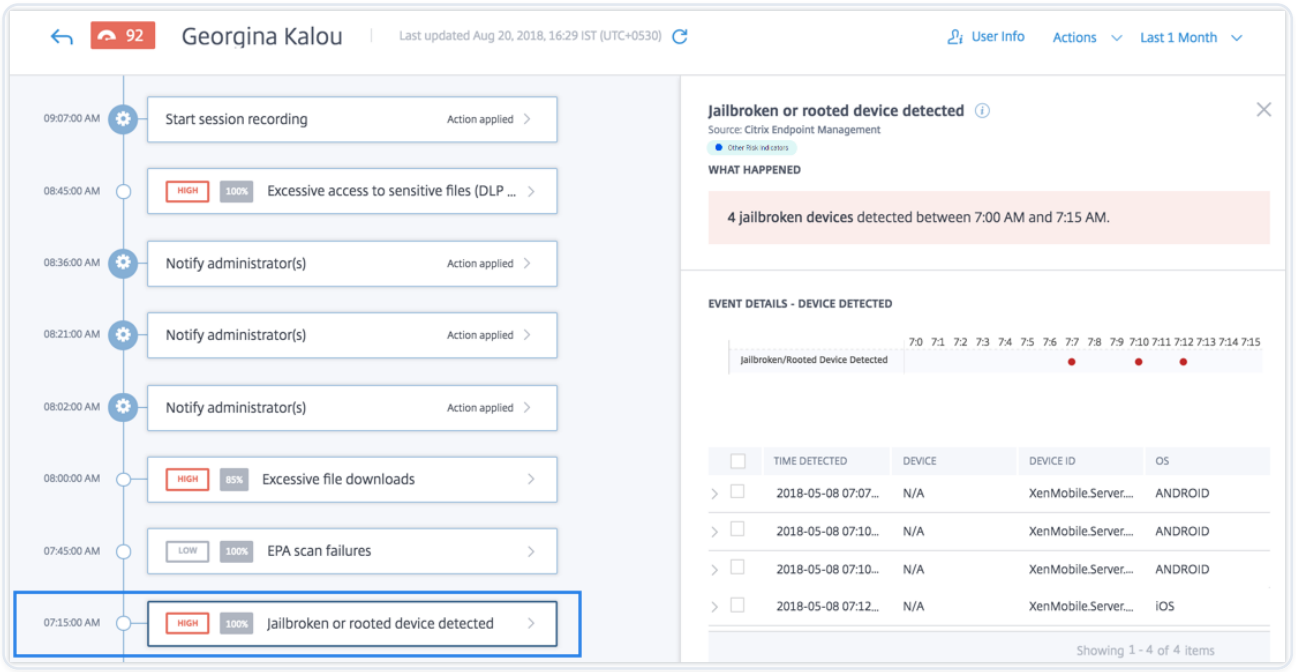
How to analyze the jailbroken or rooted device detected risk indicator?

Consider the user Georgina Kalou, whose enrolled iOS device recently became jailbroken. This suspicious behavior is detected by Citrix Analytics and a risk score is assigned to Georgina Kalou.

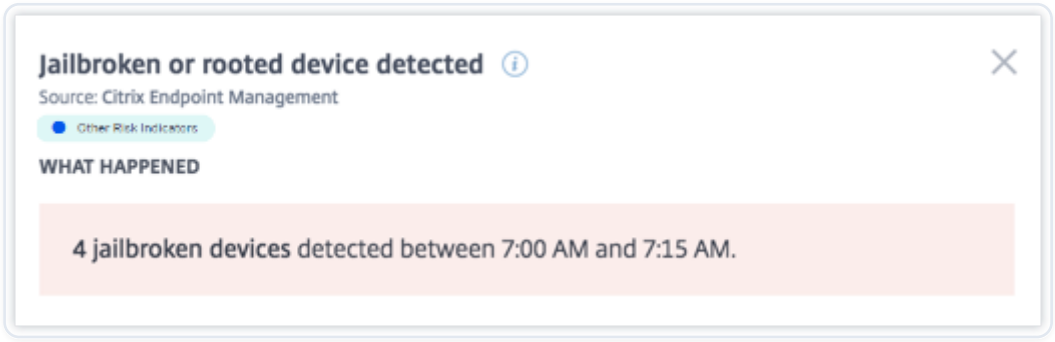
From Georgina Kalou's risk timeline, you can select the reported **Jailbroken or rooted device detected** risk indicator. The reason for the event is displayed along with the details such as time the risk indicator was triggered, description of the event, and so on.

To view the **Jailbroken or rooted device detected** risk indicator for a user, navigate to **Security > Users**, and select the user.

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

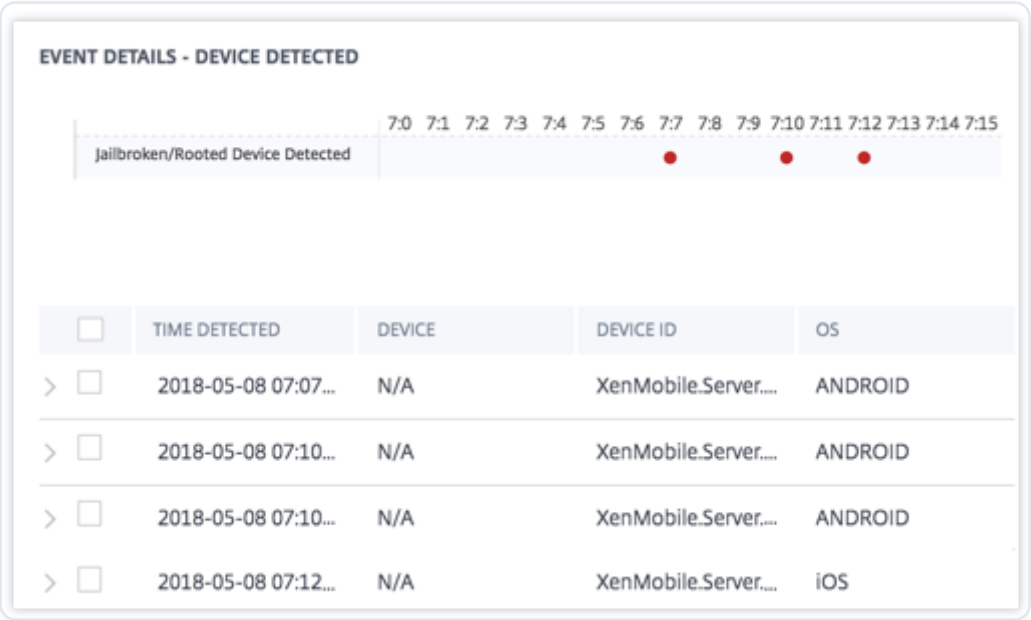


- The **WHAT HAPPENED** section, you can view the summary of the event. You can view the number of jailbroken or rooted devices detected and the time the events occurred.



- The **EVENT DETAILS – DEVICE DETECTED** section, the events are displayed in graphical and tabular format. The events are also displayed as individual entries in the graph, and the table provides the following key information:
  - **Time detected**. The time the jailbroken or rooted device is detected.
  - **Device**. The mobile device used.
  - **Device ID**. Information about the ID of the device that is used to log on to the session.
  - **OS**. The operating system of the mobile device.

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



NOTE

In addition to viewing the details in tabular format, click the arrow against an alert's instance to see more details.

What actions you can apply to the user?

You can perform the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Actions** menu, select an action and click **Apply**.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

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

Unmanaged device detected

Citrix Analytics detects access threats based on unmanaged device activity and triggers the corresponding risk indicator.

The **Unmanaged device detected** risk indicator is triggered when a device is:

- Remotely wiped due to an automated action.
- Manually wiped by the administrator.
- Unenrolled by the user.

The risk factor associated with the Unmanaged device detected risk indicator is the Other risk indicators. For more information about the risk factors, see Citrix user risk indicators.

When is the unmanaged device detected risk indicator triggered?

The **Unmanaged device detected** risk indicator is reported when a user's device has become unmanaged. A device changes to an unmanaged state due to:

- An action performed by the user.
- An action performed by the Endpoint Management administrator or the server.

In your organization, using Endpoint Management service you can manage the devices and apps that access the network. For more information, see Management Modes.

When a user's device changes to an unmanaged state, Endpoint Management service detects this event and reports it to Citrix Analytics. The user's risk score is updated. The **Unmanaged device detected** risk indicator is added to user's risk timeline.

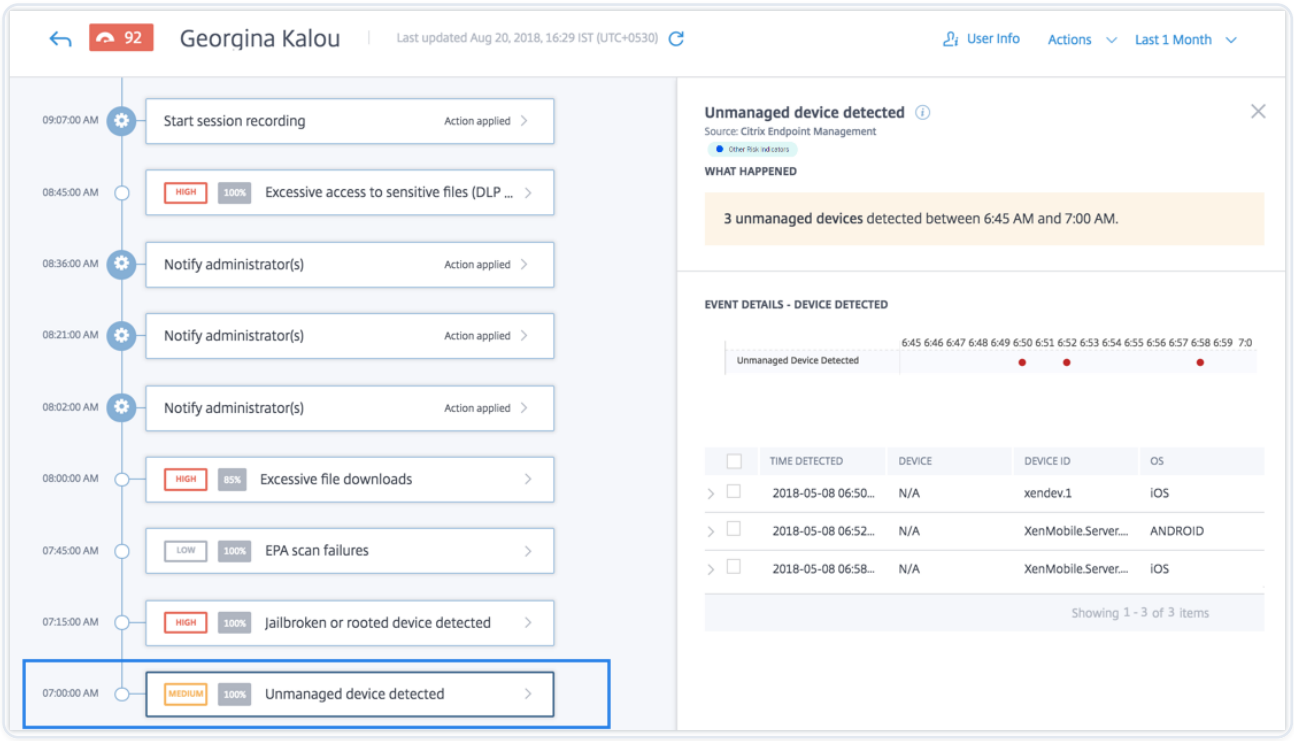
How to analyze unmanaged device detected risk indicator?

Consider the user Georgina Kalou, whose device is remotely wiped by an automated action on the server. Endpoint Management reports this event to Citrix Analytics, which assigns an updated risk score to Georgina Kalou.

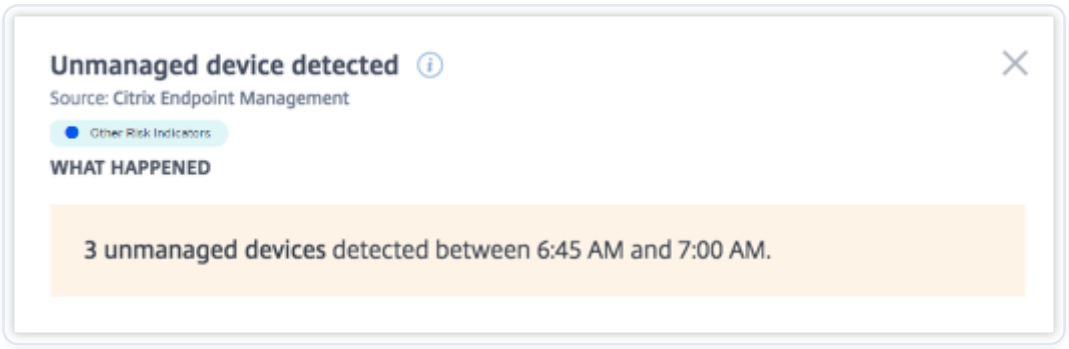
From Georgina Kalou's risk timeline, you can select the reported Unmanaged device detected risk indicator. The reason for the event is displayed along with details such as, time the risk indicator was triggered, description of the event, and so on.

To view the **Unmanaged device detected** risk indicator for a user, navigate to **Security > Users**, and select the user.

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

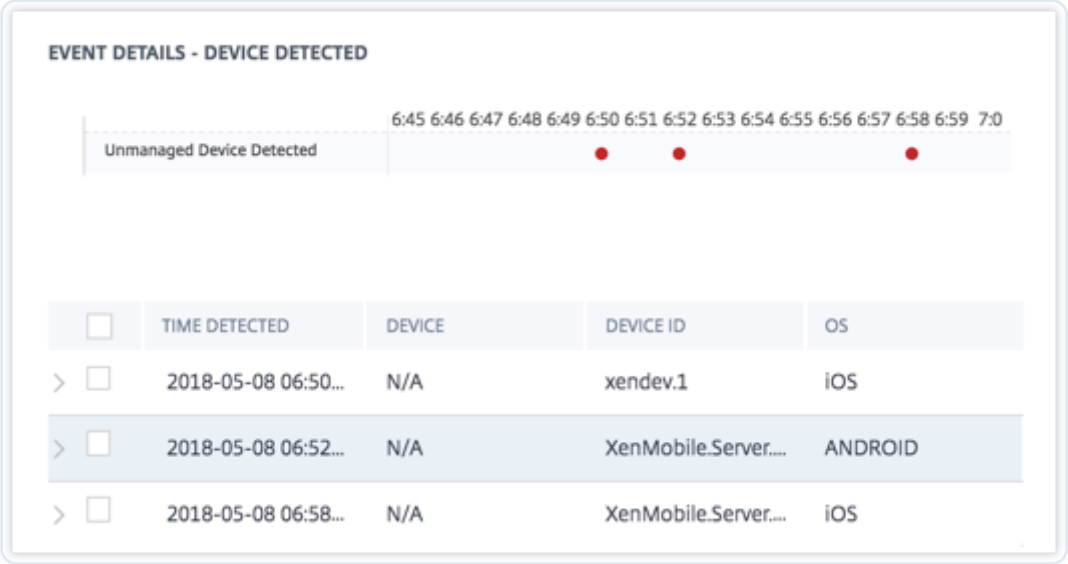


- The **WHAT HAPPENED** section, you can view a summary of the event. You can view the number of unmanaged devices detected and the time the events occurred.



- The **EVENT DETAILS – DEVICE DETECTED** section, the events are displayed in graphical and tabular format. The events are also displayed as individual entries in the graph, and the table provides the following key information:
  - **Time detected**. The time the event was detected.
  - **Device**. The mobile device used.
  - **Device ID**. The device ID of the mobile device.
  - **OS**. The operating system of the mobile device.

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



What actions you can apply to the user?

You can perform the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Actions** menu, select an action and click **Apply**.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

Citrix Gateway risk indicators

End Point Analysis (EPA) scan failures

Citrix Analytics detects user access-based threats based on EPA scan failures activity and triggers the corresponding risk indicator.

The risk factor associated with the End Point Analysis scan failure risk indicator is the Other risk indicators. For more information about the risk factors, see Citrix user risk indicators.

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

When is the EPA scan failures risk indicator triggered?

The EPA scan failure risk indicator is reported when a user tries to access the network using a device that has failed Citrix Gateway's End Point Analysis (EPA) Scan policies for pre-authentication or post authentication.

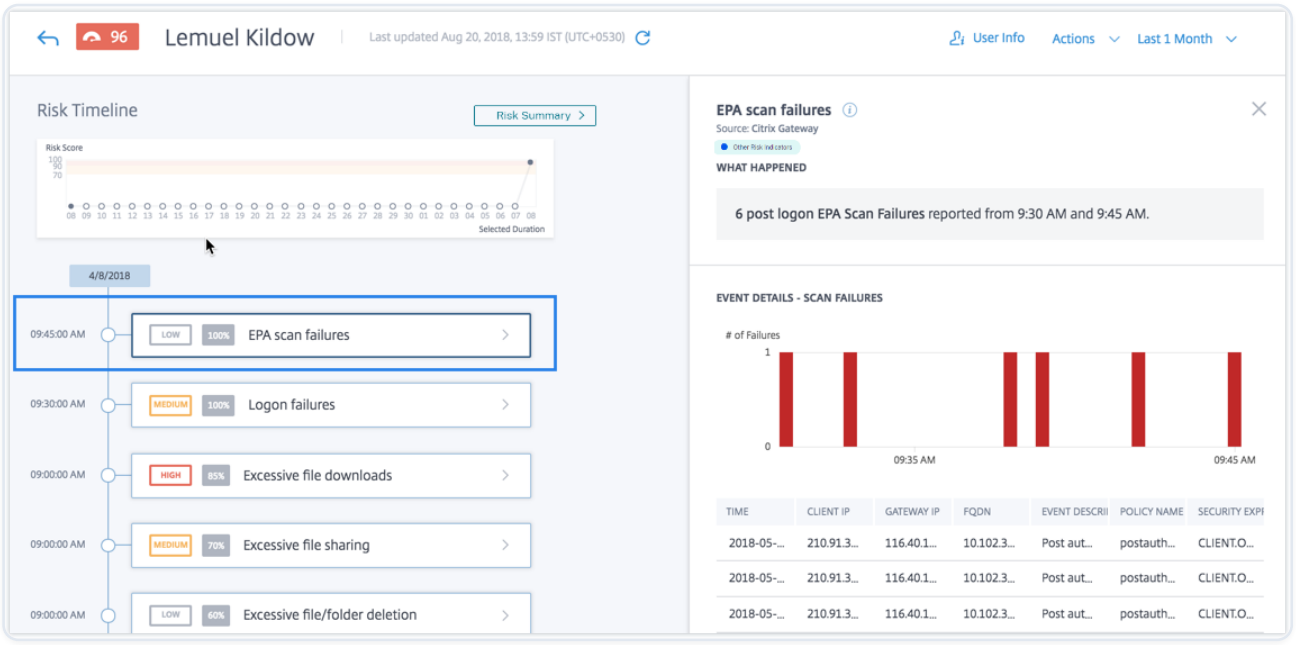
Citrix Gateway detects these events and reports them to Citrix Analytics. Citrix Analytics monitors all these events to detect whether the user has had too many EPA scan failures. When Citrix Analytics determines excessive EPA scan failures for a user, it updates the user's risk score and adds an EPA scan Failure risk indicator entry to the user's risk timeline.

How to analyze the EPA scan failures risk indicator?

Consider the user Lemuel, who recently tried multiple times to access the network using a device that has failed Citrix Gateway's EPA scan. Citrix Gateway reports this failure to Citrix Analytics, which assigns an updated risk score to Lemuel. The EPA scan failure risk indicator is added to Lemuel Kildow's risk timeline.

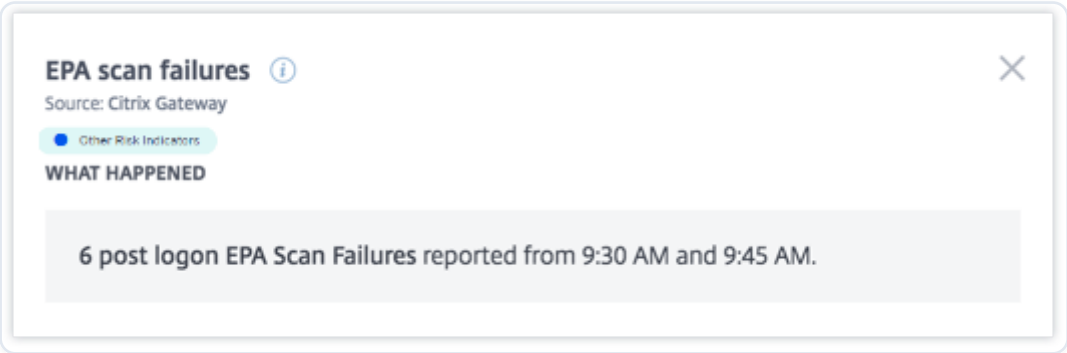
To view the **EPA scan failure** entry for a user, navigate to **Security > Users**, and select the user.

From Lemuel Kildow's risk timeline, you can select the latest **EPA scan failures** risk indicator reported for the user. When you select an EPA scan failure risk indicator entry from the timeline, a corresponding detailed information panel appears in the right pane.

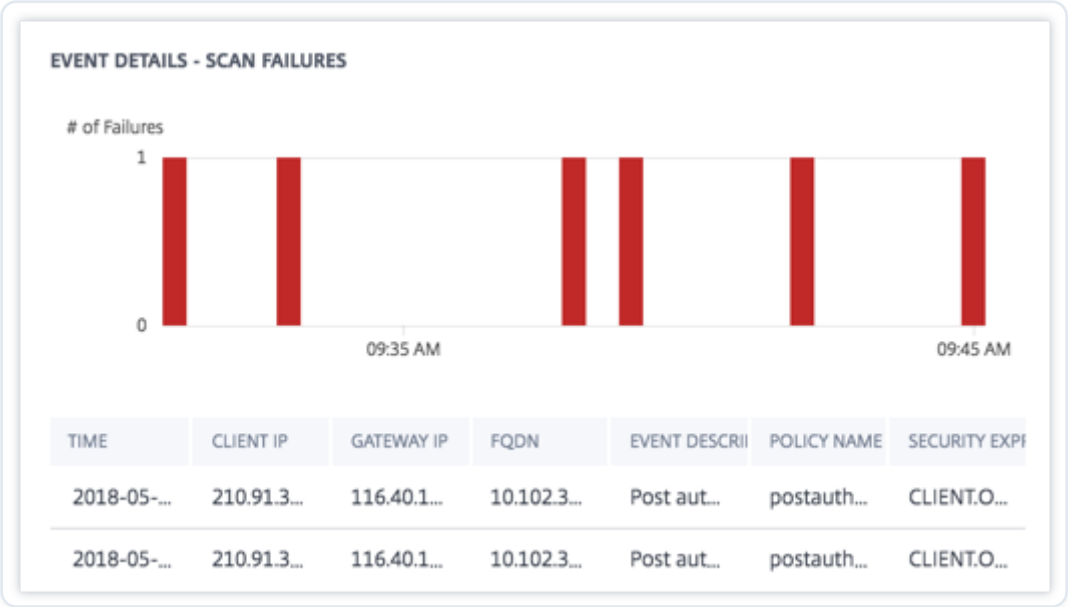


- The **WHAT HAPPENED** section provides a brief summary of the EPA scan failure risk indicator. And, includes the number of post logon EPA scan failures reported during the selected period.

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



- The **EVENT DETAILS – SCAN FAILURES** section, includes a timeline visualization of the individual EPA scan failure events that occurred during the selected time period. Also, it includes a table that provides the following key information about each event:
  - **Time**. The time the EPA scan failure occurred.
  - **Client IP**. The IP address of the client that causes the EPA scan failure.
  - **Gateway IP**. The IP address of Citrix Gateway that reported the EPA scan failure.
  - **FQDN**. The FQDN of Citrix Gateway.
  - **Event description**. Brief description of the reason for EPA scan failure.
  - **Policy name**. The EPA scan policy name configured on the Citrix Gateway.
  - **Security expression**. The security expression configured on the Citrix Gateway.



What actions you can apply to the user?

You can perform the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.

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

- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.
- **Log off user**. When a user is logged off from their account, they cannot access any resource through Citrix Gateway until the Citrix Gateway administrator clears the Log Off User action.
- **Lock user**: When a user's account is locked due to anomalous behavior, they cannot access any resource through Citrix Gateway until the Gateway administrator unlocks the account.

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Actions** menu, select an action and click **Apply**.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

Excessive authentication failures

Citrix Analytics detects user access-based threats based on Excessive authentication failures and triggers the corresponding risk indicator.

The risk factor associated with the Excessive authentication failures risk indicator is the Logon-failure-based risk indicators. For more information about the risk factors, see Citrix user risk indicators.

When is the Excessive authentication failures risk indicator triggered?

The Logon failure risk indicator is reported when the user encounters multiple Citrix Gateway authentication failures within a given period. The Citrix Gateway authentication failures can be primary, secondary, or tertiary authentication failures, depending on whether multifactor authentication is configured for the user.

Citrix Gateway detects all the user authentication failures and reports these events to Citrix Analytics. Citrix Analytics monitors all these events to detect whether the user has had too many authentication failures. When Citrix Analytics determines excessive authentication failures, it updates the user's risk score. The Excessive authentication failures risk indicator is added to the user's risk timeline.

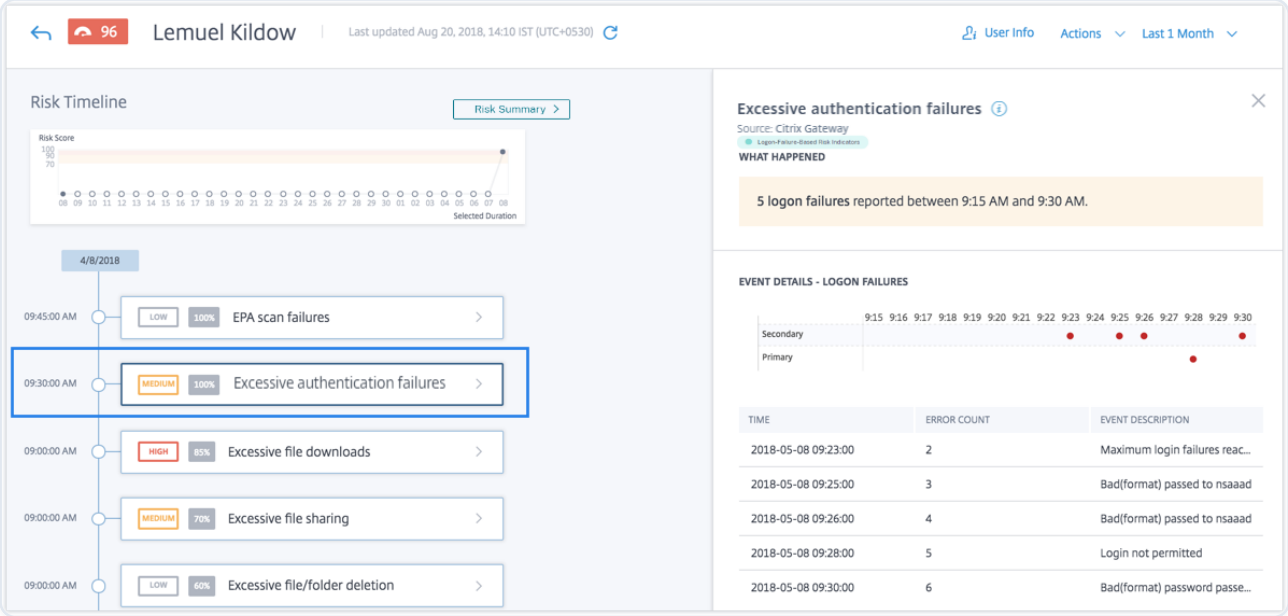
© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to analyze the Excessive authentication failures risk indicator?

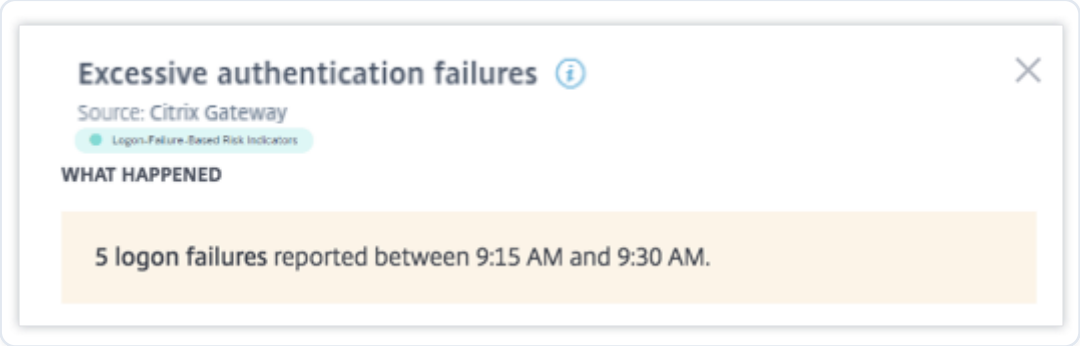
Consider the user Lemuel, who recently failed multiple attempts to authenticate the network. Citrix Gateway reports these failures to Citrix Analytics, and an updated risk score is assigned to Lemuel. The **Excessive authentication failures** risk indicator is added to Lemuel Kildow's risk timeline.

To view the **Excessive authentication failures** risk indicator entry for a user, navigate to **Security > Users**, and select the user.

From Lemuel Kildow's risk timeline, you can select the latest **Excessive authentication failures** risk indicator reported for the user. When you select the **Excessive authentication failures** risk indicator entry from the risk timeline, a corresponding detailed information panel appears in the right pane.



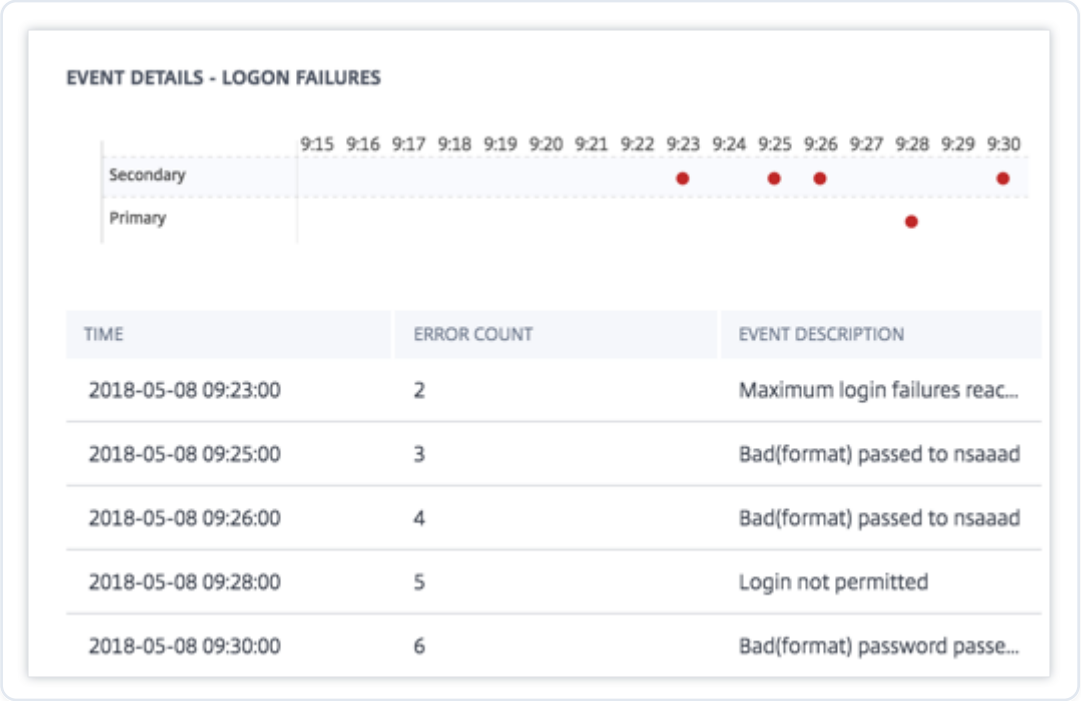
- The **WHAT HAPPENED** section provides a brief summary of the risk indicator, including the number of authentication failures that occurred during the selected period.



- The **EVENT DETAILS** section, includes a timeline visualization of the individual Excessive authentication failure events that occurred during the selected time period. Also, you can view the following key information about each event:

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

- **Time**. The time the logon failure occurred.
- **Error count**. The number of authentication failures detected for the user at the time of the event and for the previous 48 hours.
- **Event description**. Brief description of the reason for the logon failure.



What actions you can apply to the user?

You can perform the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.
- **Log off user**. When a user is logged off from their account, they cannot access any resource through Citrix Gateway until the Citrix Gateway administrator clears the Log Off User action.
- **Lock user**: When a user's account is locked due to anomalous behavior, they cannot access any resource through Citrix Gateway until the Gateway administrator unlocks the account.

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Actions** menu, select an action and click **Apply**.

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

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

Impossible travel

Citrix Analytics detects a user's logons as risky when the consecutive logons are from two different countries within a time period that is less than the expected travel time between the countries.

The impossible travel time scenario indicates the following risks:

- **Compromised credentials**: A remote attacker steals a legitimate user's credentials.
- **Shared credentials**: Different users are using the same user credentials.

When is the Impossible travel risk indicator triggered?

The **Impossible travel** risk indicator evaluates the time and estimated distance between each pair of consecutive user logons, and triggers when the distance is greater than an individual person can possibly travel in that amount of time.

NOTE

This risk indicator also contains logic to reduce false positive alerts for the following scenarios that do not reflect the users' actual locations:

- When users log on through Citrix Gateway from proxy connections.
- When users log on through Citrix Gateway from hosted clients.

How to analyze the Impossible risk indicator

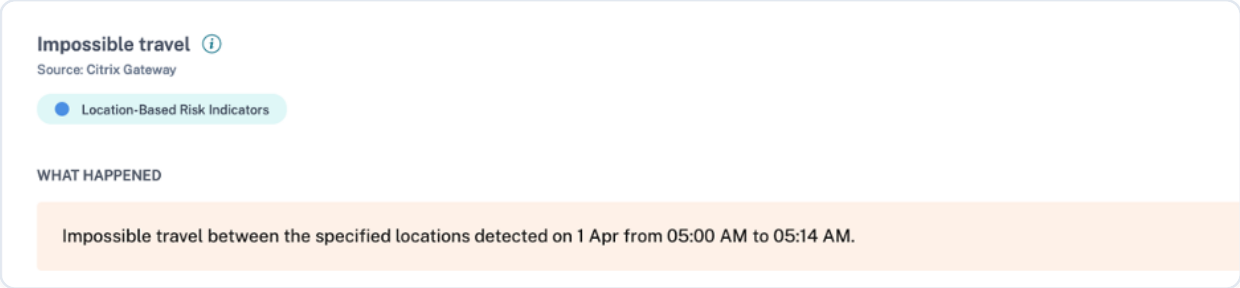
Consider the user Adam Maxwell, who logs on from two locations- Bengaluru, India and Oslo, Norway within a time duration of one minute. Citrix Analytics detects this logon event as an impossible travel scenario and triggers the **Impossible travel** risk indicator. The risk indicator is added to Adam Maxwell's risk timeline and a risk score is assigned to him.

To view Adam Maxwell's risk timeline, select **Security > Users**. From the **Risky Users** pane, select the user Adam Maxwell.

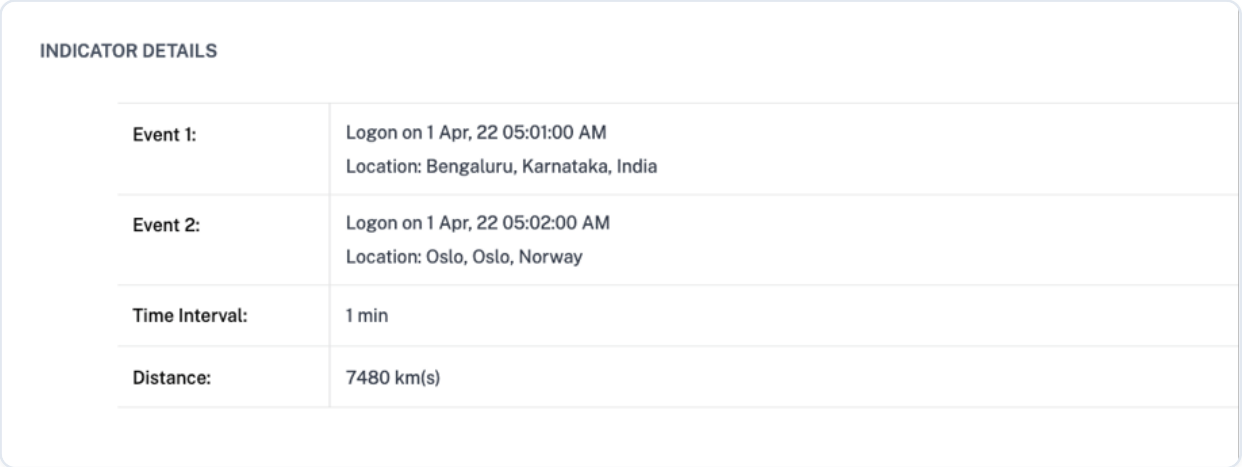
From Adam Maxwell's risk timeline, select the **Impossible travel** risk indicator. You can view the following information:

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

- The **WHAT HAPPENED** section provides a brief summary of the impossible travel event.



- The **INDICATOR DETAILS** section provides the locations from which the user has logged on, the time duration between the consecutive logons, and the distance between the two locations.



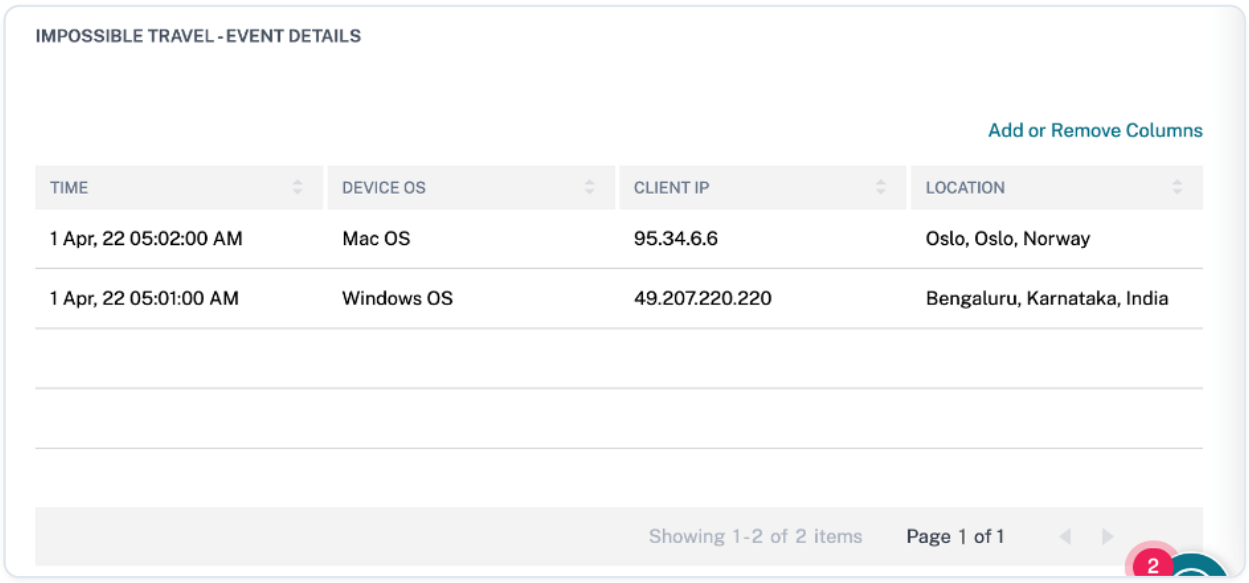
- The **LOGON LOCATION- LAST 30 DAYS** section displays a geographical map view of the impossible travel locations and known locations of the user. The location data is shown for the last 30 days. You can hover over the pointers on the map to view the total logons from each location.



- The **IMPOSSIBLE TRAVEL- EVENT DETAILS** section provides the following information about the impossible travel event:
  - **Time**: Indicates the date and the time of the logons.

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

- **Device OS**: Indicates the operating system of the user device.
- **Client IP**: Indicates the IP address of the user device.
- **Location**: Indicates the location from where the user has logged on.



What actions you can apply to the user?

You can do the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.
- **Log off user**. When a user is logged off from their account, they cannot access any resource through Citrix Gateway until the Citrix Gateway administrator clears the Log Off User action.
- **Lock user**: When a user's account is locked due to anomalous behavior, they cannot access any resource through Citrix Gateway until the Gateway administrator unlocks the account.

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Actions** menu, select an action and click **Apply**.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

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

Logon from suspicious IP

Citrix Analytics detects user access threats based on the sign-in activity from a suspicious IP and triggers this risk indicator.

The risk factor associated with the Logon from suspicious IP risk indicator is the IP-based risk indicators. For more information about the risk factors, see Citrix user risk indicators.

When is the Logon from suspicious IP risk indicator triggered?

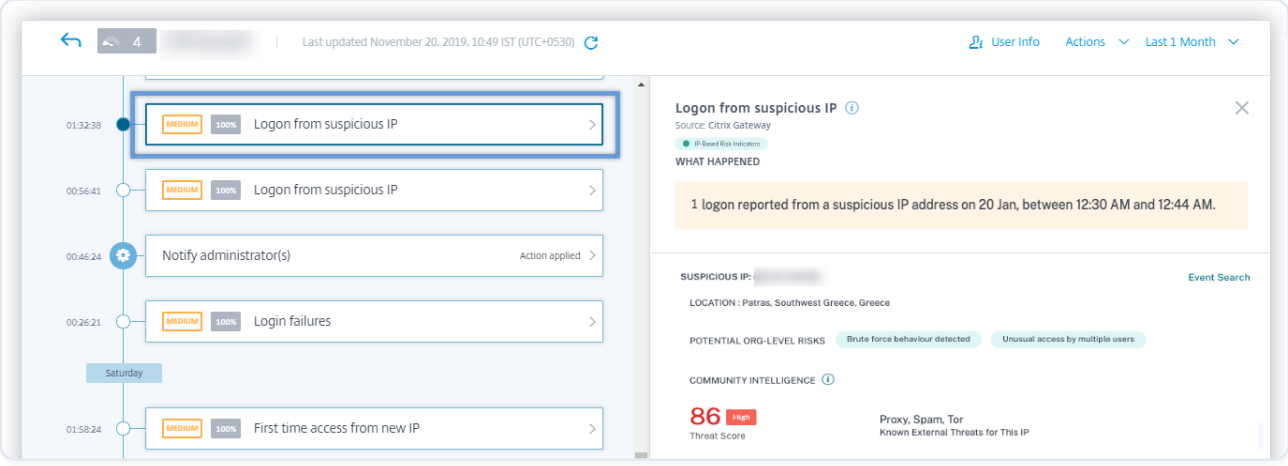
The **Logon from suspicious IP** risk indicator is triggered when a user attempts to access the network from an IP address that Citrix Analytics identifies as suspicious. The IP address is considered suspicious based on one of the following conditions:

- Is listed on the external IP threat intelligence feed
- Has multiple user sign-in records from an unusual location
- Has excessive failed sign-in attempts that might indicate a brute-force attack

Citrix Analytics monitors the sign-in events received from Citrix Gateway and detects whether a user has signed in from any suspicious IP. When Citrix Analytics detects a sign-in attempt from a suspicious IP, it updates the user's risk score and adds a **Logon from suspicious IP** risk indicator entry to the user's risk timeline.

How to analyze the Logon from suspicious IP risk Indicator?

Consider the user Lemuel, who attempted to access the network from an IP address that Citrix Analytics identifies as suspicious. Citrix Gateway reports the sign-in event to Citrix Analytics, which assigns an updated risk score to Lemuel. The **Logon from suspicious IP** risk indicator is added to Lemuel Kildow's risk timeline.

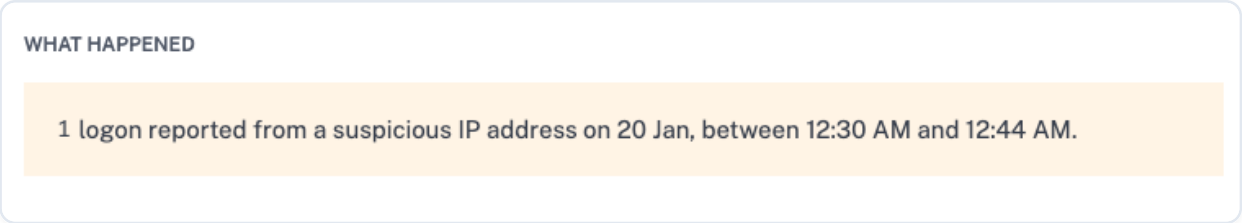


To view the Logon from suspicious IP risk indicator reported for a user, navigate to **Security** > **Users**, and select the user. From Lemuel Kildow's risk timeline, you can select the latest **Logon**

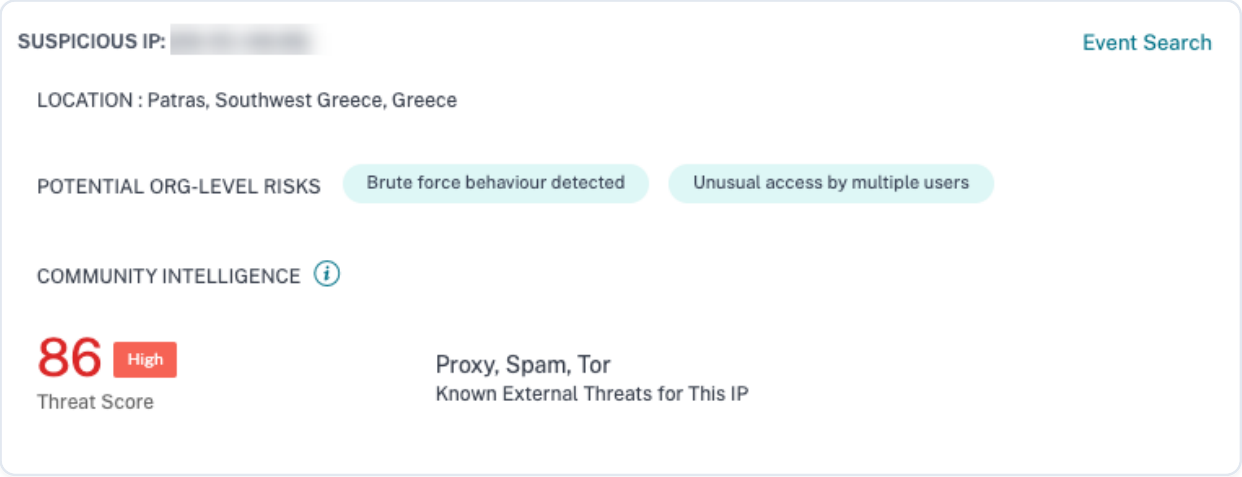
© 1997–2026 Citrix Systems, Inc. All rights reserved.

from suspicious IP risk indicator reported for the user. When you select the **Logon from suspicious IP** risk indicator entry from the timeline, a corresponding detailed information panel appears in the right pane.

- The **WHAT HAPPENED** section provides a brief summary of the Logon from suspicious IP risk indicator. And, includes the number of sign-ins from a suspicious IP address reported during the selected period.



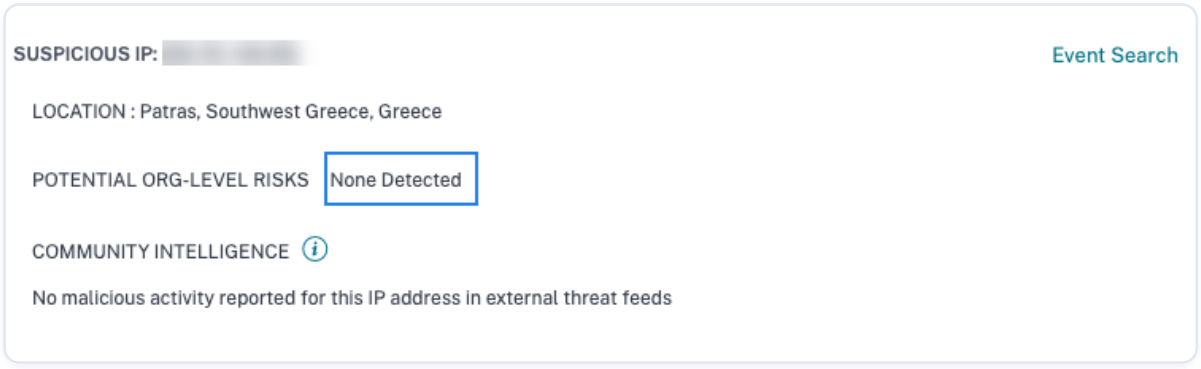
- The **Suspicious IP** section provides the following information:



  - **Suspicious IP**. The IP address associated with a suspicious sign-in activity.
  - **Location**. The city, region, and country of the user. These locations are displayed based on the availability of data.
  - **Potential organization level risk**. Indicates any patterns of suspicious IP activity that Citrix Analytics has recently detected in your organization. The risky patterns include excessive login failures consistent with potential brute force attempts and unusual access by multiple users.

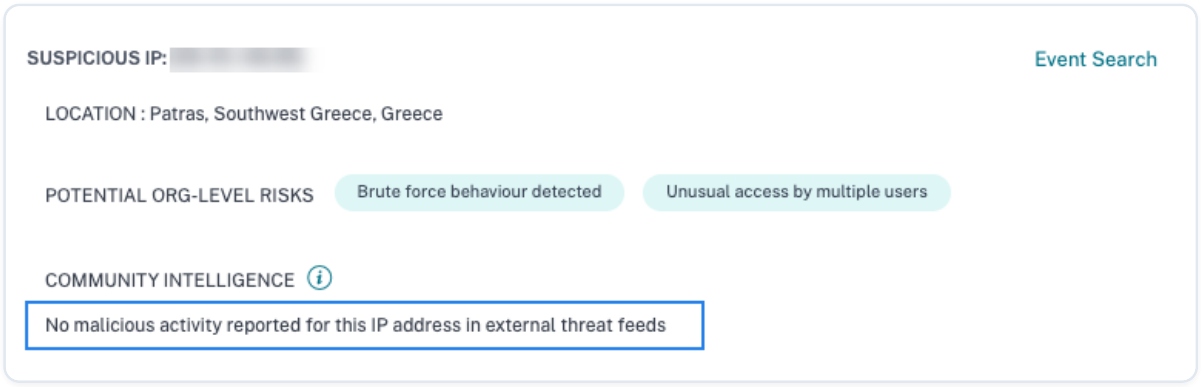
    If no risky pattern is detected for an IP address in your organization, you see the following message.

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

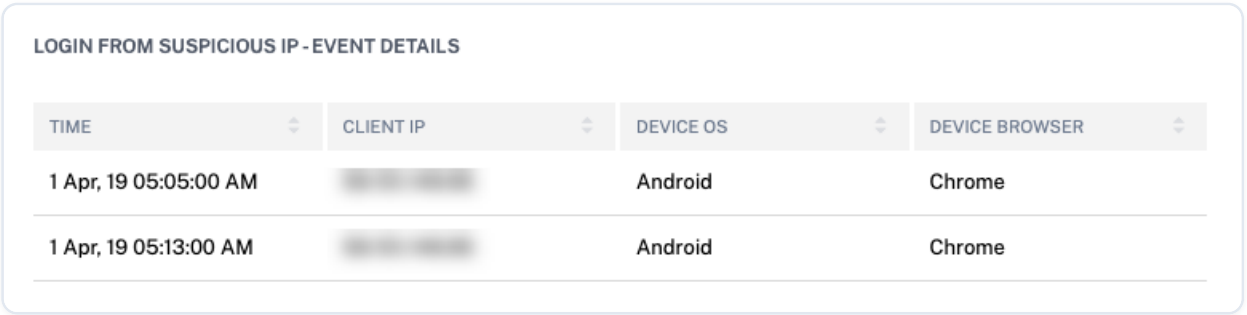


- **Community intelligence**. Provides the threat score and the threat categories of an IP address that is identified as high risk in the external IP threat intelligence feed. Citrix Analytics assigns a risk score to the high risk IP address. The risk score starts from 80.

  If an IP address does not have any threat intelligence available on the external IP threat intelligence feed, you see the following message.



- The **EVENT DETAILS** section provides the following information about the suspicious sign-in activity:



  - **Time**. The time of the suspicious sign-in activity.
  - **Client IP**. The IP address of the user's device that was used for the suspicious sign-in activity.
  - **Device OS**. The operating system of the browser.
  - **Device Browser**. The web browser used for the suspicious sign-in activity.

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

What actions you can apply to the user?

You can do the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.
- **Log off user**. When a user is logged off from their account, they cannot access any resource through Citrix Gateway until the Citrix Gateway administrator clears the Log Off User action.
- **Lock user**: When a user's account is locked due to anomalous behavior, they cannot access any resource through Citrix Gateway until the Gateway administrator unlocks the account.

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Actions** menu, select an action and click **Apply**.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

Suspicious logon

NOTES

- This risk indicator replaces the Access from an unusual location risk indicator.
- Any policies based on the Access from an unusual location risk indicator are automatically linked to the Suspicious logon risk indicator.

Citrix Analytics detects the user's logons that appear unusual or risky based on multiple contextual factors, which are defined jointly by the device, location, and network used by the user.

When is the Suspicious logon risk indicator triggered?

The risk indicator is triggered by the combination of the following factors, where each factor is regarded as potentially suspicious based on one or more conditions.

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

FACTOR	CONDITIONS
Unusual device	The user logs on from a device with a signature that is different from the devices used in the last 30 days. The device signature is based on the operating system of the device and the browser used.
Unusual location	Log on from a city or a country that the user has not logged on in the last 30 days.
	The city or country is geographically far from the recent (last 30 days) logon locations.
	Zero or minimum users have logged on from the city or the country in the last 30 days.
Unusual network	Log on from an IP address that the user has not used in the last 30 days.
	Log on from an IP subnet that the user has not used in the last 30 days.
	Zero or minimum users have logged on from the IP subnet in the last 30 days.
IP threat	The IP address is identified as high risk by the community threat intelligence feed- Webroot.
	Citrix Analytics recently detected highly suspicious logon activities from the IP address from other users.

How to analyze the Suspicious logon risk indicator

Consider the user Adam Maxwell, who signs in from the Andhra Pradesh, India for the first time. He uses a device with a known signature to access the organization's resources. But he connects from a network, which he has not used in the last 30 days.

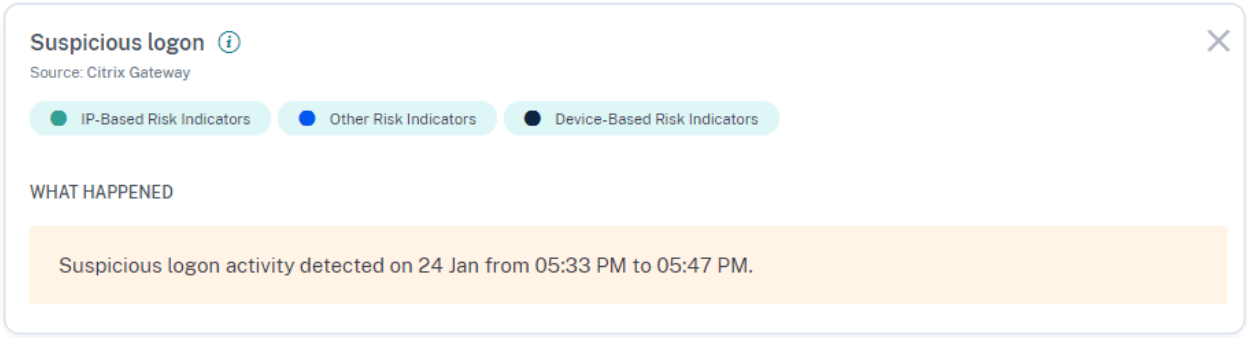
Citrix Analytics detects this logon event as suspicious because the factors- location and network deviate from his usual behavior and triggers the Suspicious logon risk indicator. The risk indicator is added to Adam Maxwell's risk timeline and a risk score is assigned to him.

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

To view Adam Maxwell's risk time, select **Security > Users**. From the **Risky Users** pane, select the user Adam Maxwell.

From Adam Maxwell's risk timeline, select the **Suspicious logon** risk indicator. You view the following information:

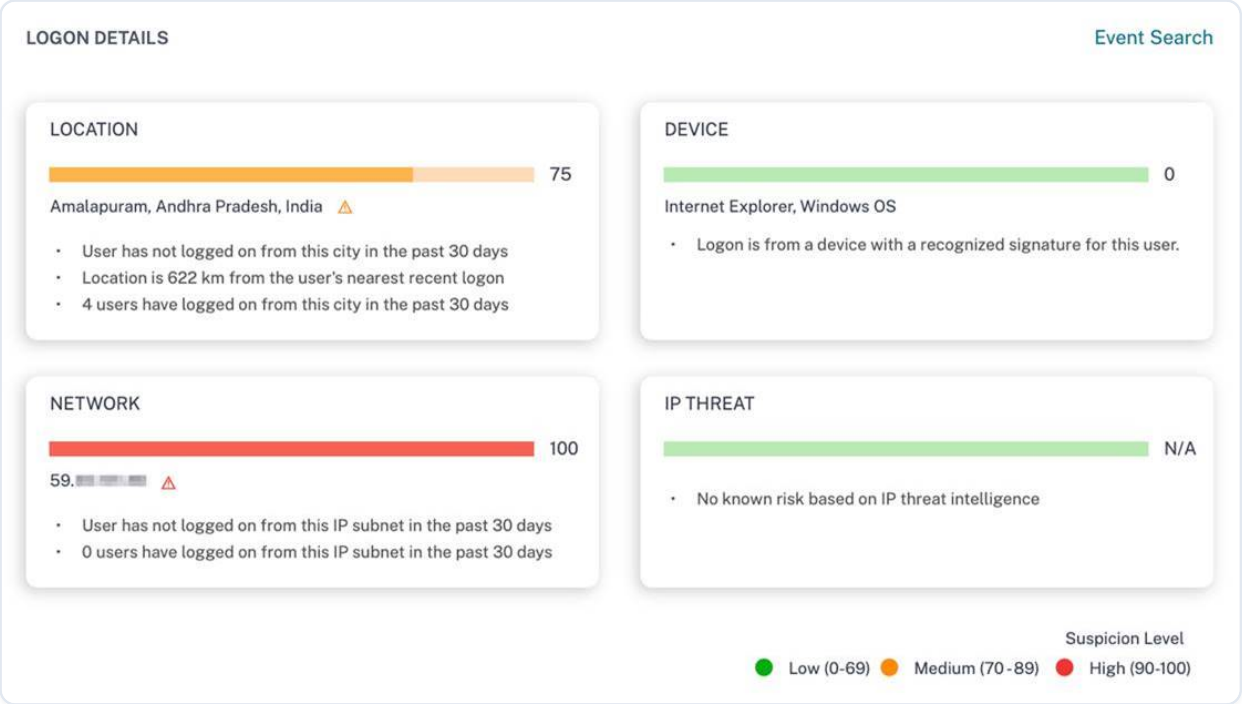
- The **WHAT HAPPENED** section provides a brief summary of the suspicious activities that include the risk factors and the time of the event.



- The **LOGON DETAILS** section provides detailed summary of the suspicious activities corresponding to each risk factor. Each risk factor is assigned a score that indicates the suspicion level. Any single risk factor does not indicate high risk from a user. The overall risk is based on the correlation of the multiple risk factors.

SUSPICION LEVEL	INDICATION
0–69	The factor appears normal and is not considered suspicious.
70–89	The factor appears slightly unusual and is considered moderately suspicious with other factors.
90–100	The factor is entirely new or unusual and is considered highly suspicious with other factors.

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

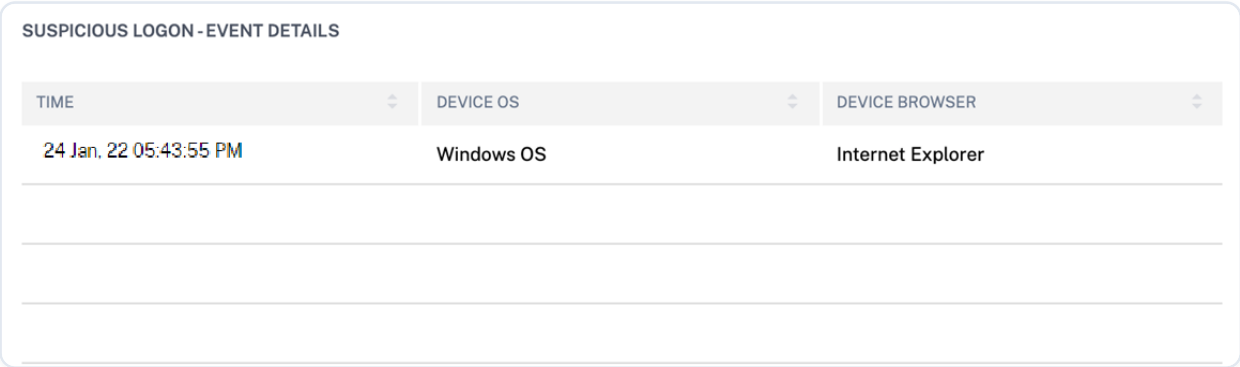


- The **LOGON LOCATION- LAST 30 DAYS** displays a geographical map view of the last known locations and the current location of the user. The location data is shown for the last 30 days. You can hover over the pointers on the map to view the total logons from each location.



- The **SUSPICIOUS LOGON- EVENT DETAILS** section provides the following information about the suspicious logon event:
  - **Time**: Indicates the date and time of the suspicious logon.
  - **Device OS**: Indicates the operating system of the user device.
  - **Device browser**: Indicates the web browser used to sign in to Citrix Gateway.

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



What actions you can apply to the user?

You can do the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.
- **Log off user**. When a user is logged off from their account, they cannot access any resource through Citrix Gateway until the Citrix Gateway administrator clears the Log Off User action.
- **Lock user**: When a user's account is locked due to anomalous behavior, they cannot access any resource through Citrix Gateway until the Gateway administrator unlocks the account.

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Actions** menu, select an action and click **Apply**.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

Unusual authentication failure

Citrix Analytics detects access-based threats when a user has logon failures from an unusual IP address and triggers the corresponding risk indicator.

The risk factor associated with the Unusual authentication risk indicator is the Logon-failure-based risk indicators. For more information about the risk factors, see Citrix user risk indicators.

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

When is the unusual authentication failure indicator triggered?

You can be notified when a user in your organization has logon failures from an unusual IP address that is contrary to their usual behavior.

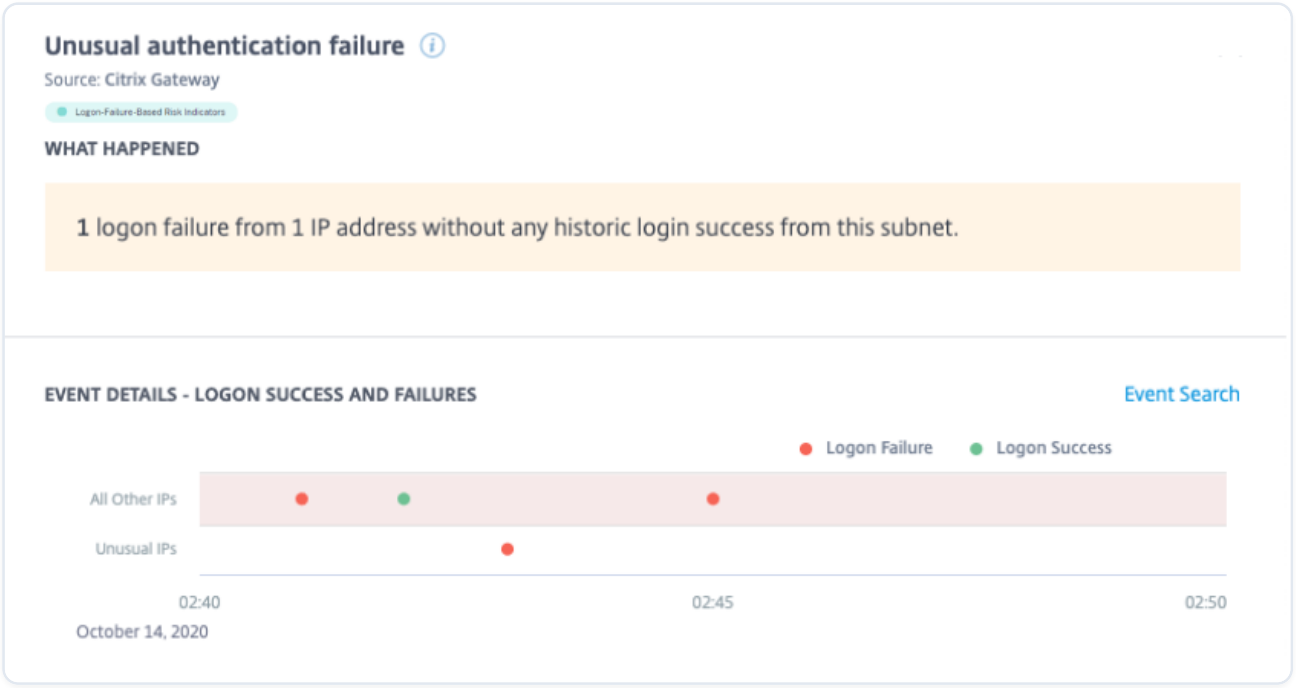
Citrix Gateway detects these events and reports them to Citrix Analytics. Citrix Analytics receives the events and increases the user's risk score. The **Unusual Authentication Failure** risk indicator is added to the user's risk timeline.

How to analyze the unusual authentication failure indicator?

Consider the user Georgina Kalou, who routinely signs into Citrix Gateway from her usual home and office networks. A remote attacker attempts to authenticate Georgina's account by guessing different passwords, resulting in authentication failures from an unfamiliar network.

In this scenario, Citrix Gateway reports these events to Citrix Analytics, which assigns an updated risk score to Georgina Kalou. The Unusual Authentication Failure risk indicator is added to Georgina Kalou's risk timeline.

From Georgina Kalou's risk timeline, you can select the reported Unusual Authentication Failure risk indicator. The reason for the event is displayed along with details such as the time of the event, and location.

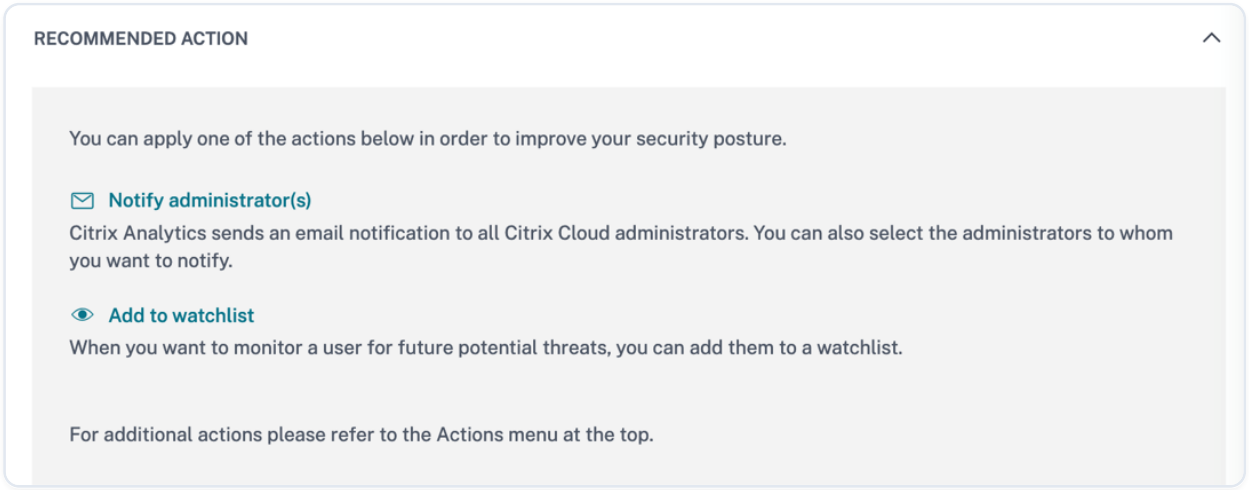


- In the **WHAT HAPPENED** section, you can view the brief summary that includes the total number of authentication failures and the time of the event.

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

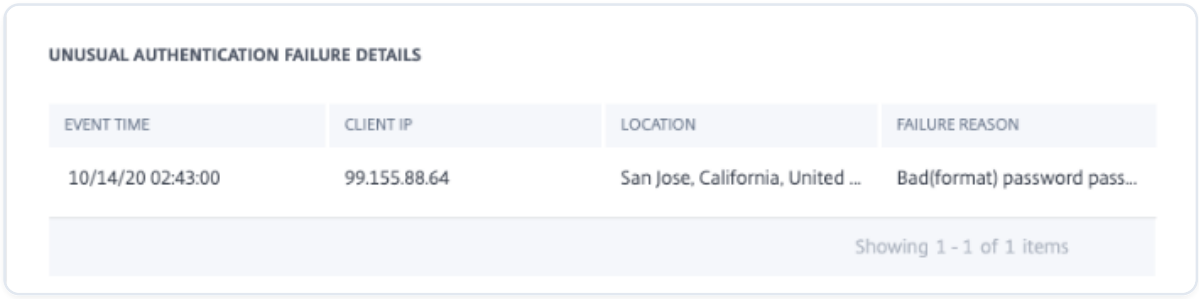
- In the **RECOMMENDED ACTION** section, you find the suggested actions that can be applied on the risk indicator. Citrix Analytics for Security™ recommends the actions depending on the severity of the risk posed by the user. The recommendation can be one or combination of the following actions:
  - Notify administrator(s)
  - Add to watchlist
  - Create a policy

  You can select an action based on the recommendation. Or you can select an action that you want to apply depending on your choice from the **Actions** menu. For more information, see Apply an action manually.

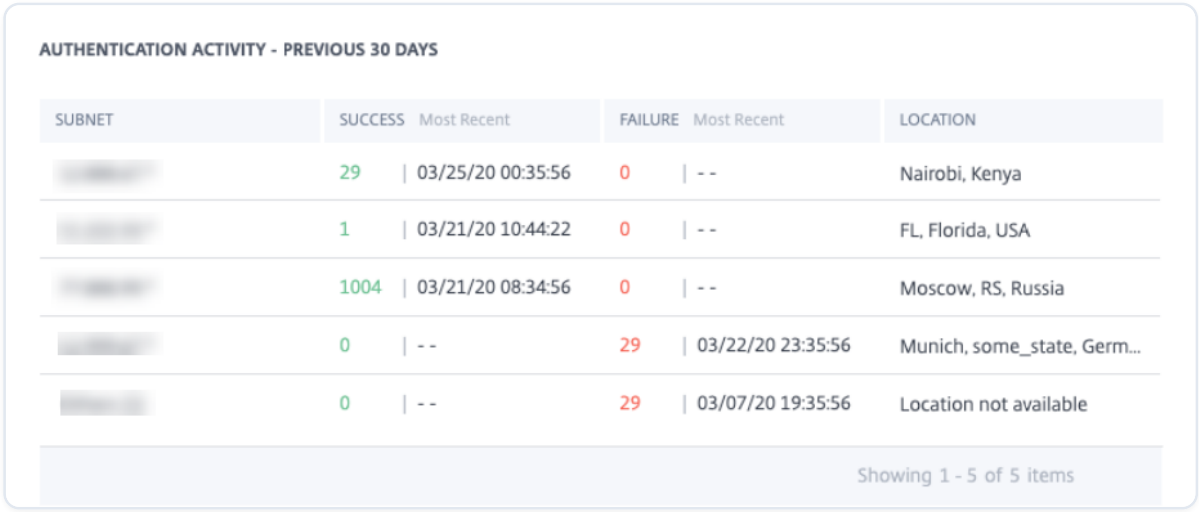


- In the **EVENT DETAILS – LOGON SUCCESS and FAILURES** section, you can view a graph indicating the unusual authentication failures, along with any other logon activity detected during the same duration.
- In the **UNUSUAL AUTHENTICATION DETAILS** section, the table provides the following information about the unusual authentication failures:
  - **Logon time** – The date and time of the event
  - **Client IP** – IP address of the user device
  - **Location** – The location from where the event has occurred
  - **Failure reason** – The reason for authentication failure

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



- In the **USER AUTHENTICATION ACTIVITY – PREVIOUS 30 DAYS** section, the table provides the following information about the previous 30-days of authentication activity for the user:
  - Subnet – The IP address from the user network.
  - Success – The total number of successful authentication events and the time of the most recent success event for the user.
  - Failure – The total number of failed authentication events and the time of the most recent failed event for the user.
  - Location – The location from where the authentication event has occurred.



What actions you can apply to the user?

You can perform the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.
- **Log off user**. When a user is logged off from their account, they cannot access any resource through Citrix Gateway until the Citrix Gateway administrator clears the Log Off User action.

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

- **Lock user**: When a user's account is locked due to anomalous behavior, they cannot access any resource through Citrix Gateway until the Gateway administrator unlocks the account.

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Actions** menu, select an action and click **Apply**.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

Citrix Secure Private Access™ risk indicators

Risky website access

NOTE

The following capabilities on Citrix Analytics for Security™ are impacted due to the deprecation of Category-based web filtering by Secure Private Access:

1. Data fields such as Category-Group, Category and Reputation of URLs are not available anymore on the Citrix Analytics for security dashboard.
2. The Risky website access indicator which relies on the same data is also deprecated and is not triggered for customers.
3. Any existing custom risk indicators using the data fields (Category-Group, Category and Reputation of URLs) and its associated policies are not triggered anymore.

For details on the deprecation from Secure Private Access, refer to Feature deprecations.

Attempt to access blacklisted URL

Citrix Analytics detects data access threats based on the blacklisted URLs accessed by the user and triggers the corresponding risk indicator.

The **Attempt to access blacklisted URL** risk indicator is reported in Citrix Analytics when a user attempts to access a blacklisted URL configured in Secure Private Access.

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

The risk factor associated with the **Attempt to access blacklisted URL** risk indicator is the Other risk indicators. For more information about the risk factors, see Citrix user risk indicators.

When is the Attempt to access blacklisted URL risk indicator is triggered?

Secure Private Access includes a URL categorization feature that provides policy-based control to restrict access to blacklisted URLs. When a user attempts to access a blacklisted URL, Secure Private Access reports this event to Citrix Analytics. Citrix Analytics updates the user's risk score and adds an **Attempt to access blacklisted URL** risk indicator entry to the user's risk timeline.

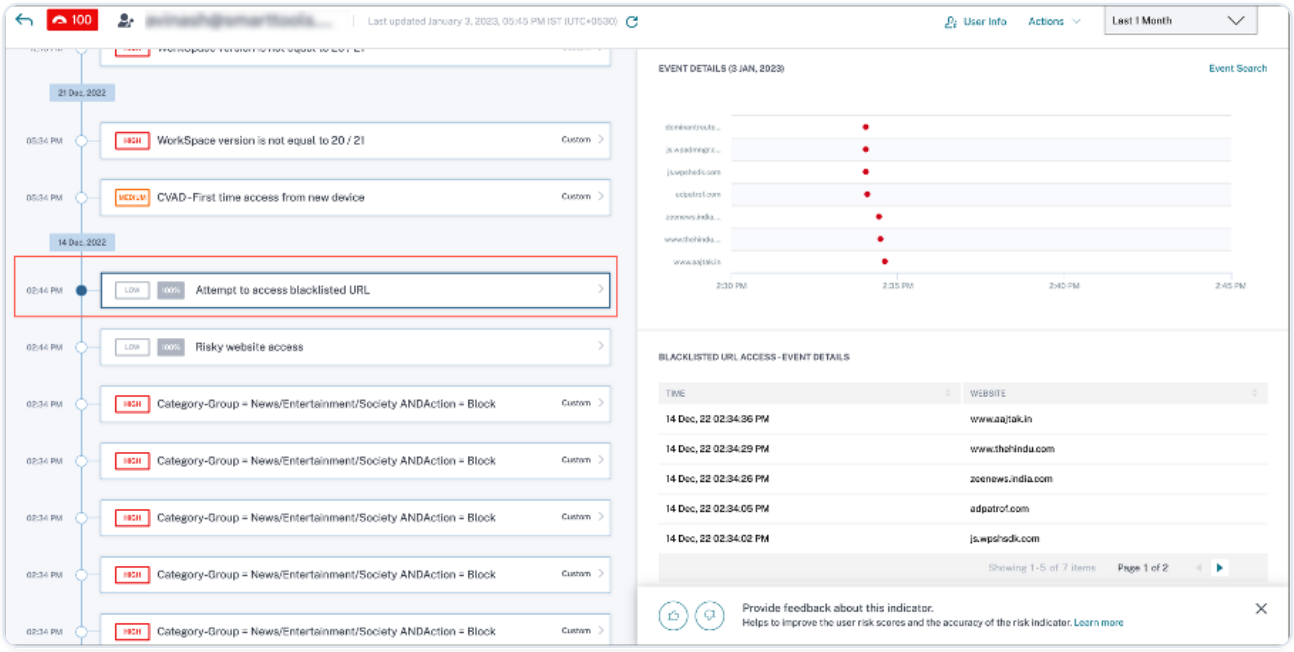
How to analyze the Attempt to access blacklisted URL risk indicator?

Consider a user Georgina Kalou, accessed a blacklisted URL configured in Secure Private Access. Secure Private Access reports this event to Citrix Analytics, which assigns an updated risk score to Georgina Kalou. The **Attempt to access blacklisted URL** risk indicator is added to Georgina Kalou's risk timeline.

From Georgina Kalou's risk timeline, you can select the reported **Attempt to access blacklisted URL** risk indicator. The reason for the event is displayed along with the details about the events, such as, time of the event, website details.

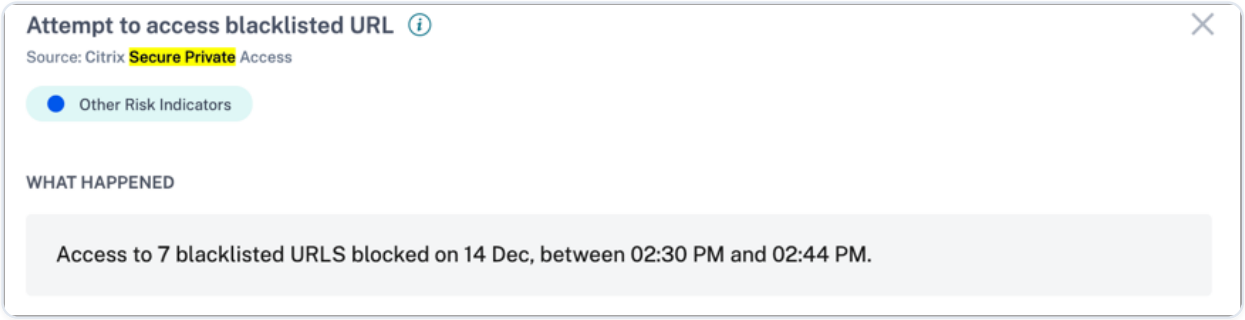
To view the **Attempt to access blacklisted URL** entry for a user, navigate to **Security > Users**, and select the user.

When you select the **Attempt to access blacklisted URL** risk indicator entry from the timeline, a corresponding detailed information panel appears in the right pane.

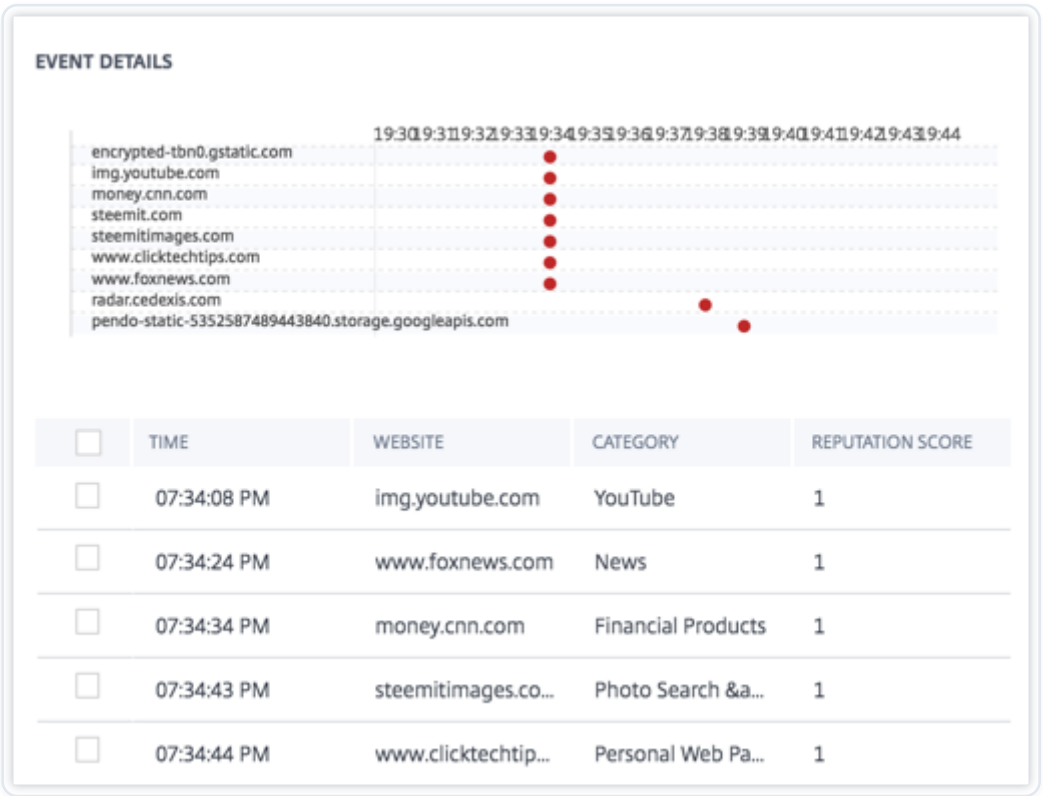


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The **WHAT HAPPENED** section provides a brief summary of the risk indicator. It includes the details of the blacklisted URL accessed by the user during the selected period.



- The **EVENT DETAILS** section, includes a timeline visualization of the individual events that occurred during the selected time period. Also, you can view the following key information about each event:
  - **Time**. The time the event occurred.
  - **Website**. The risky website accessed by the user.
  - **Category**. The category specified by Secure Private Access for the blacklisted URL.
  - **Reputation rating**. The reputation rating returned by Secure Private Access for the blacklisted URL. For more information, see URL reputation score.



What actions you can apply to the user?

You can perform the following actions on the user's account:

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

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Actions** menu, select an action and click **Apply**.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

Unusual upload volume

Citrix Analytics detects data access threats based on Unusual upload volume activity and triggers the corresponding risk indicator.

The **Unusual upload volume** risk indicator is reported when a user uploads excess volume of data to an application or website.

The risk factor associated with the Unusual upload volume risk indicator is the Other risk indicators. For more information about the risk factors, see Citrix user risk indicators.

When is the Unusual upload volume risk indicator triggered?

You can configure Secure Private Access to monitor user activities, such as malicious, dangerous, or unknown websites visited and the bandwidth consumed, and risky downloads and uploads. When a user in your organization uploads data to an application or website, Secure Private Access reports these events to Citrix Analytics.

Citrix Analytics monitors all these events and if it determines that this user activity is contrary to the user's usual behavior, it updates the user's risk score. The **Unusual upload volume** risk indicator is added to the user's risk timeline.

How to analyze the unusual upload volume risk indicator?

Consider a user Adam Maxwell, who uploaded excess volume of data to an application or website. Secure Private Access reports these events to Citrix Analytics, which assigns an updated risk

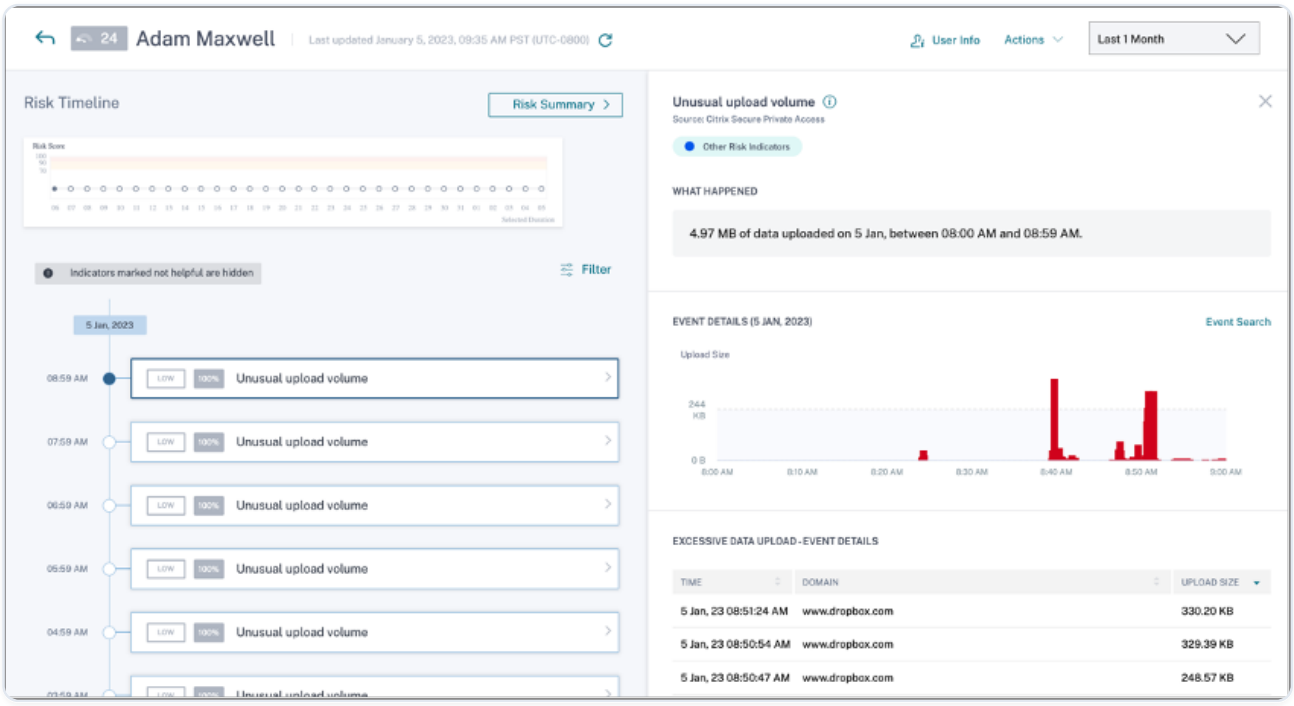
© 1997–2026 Citrix Systems, Inc. All rights reserved.

score to Adam Maxwell. The **Unusual upload volume** risk indicator is added to the Adam Maxwell's risk timeline.

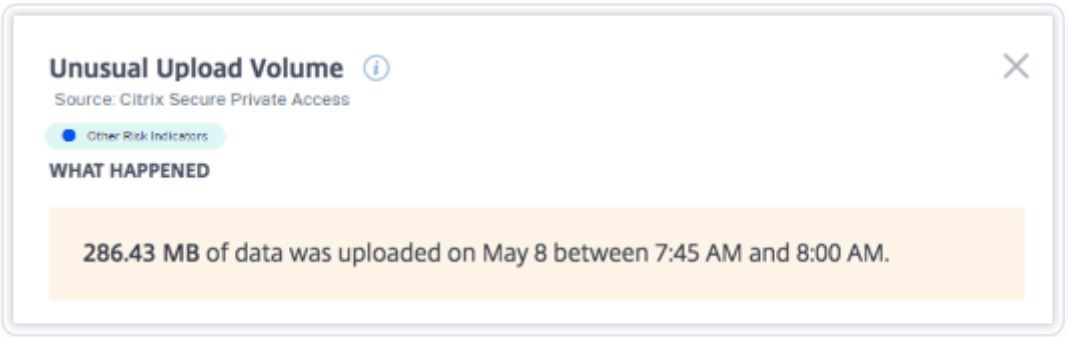
From Adam Maxwell's risk timeline, you can select the reported **Unusual upload volume** risk indicator. The reason for the event is displayed along with the details about the events, such as, time of the event and domain.

To view the **Unusual upload volume** risk indicator, navigate to **Security > Users**, and select the user.

When you select an **Unusual upload volume** risk indicator entry from the timeline, a corresponding detailed information panel appears in the right pane.



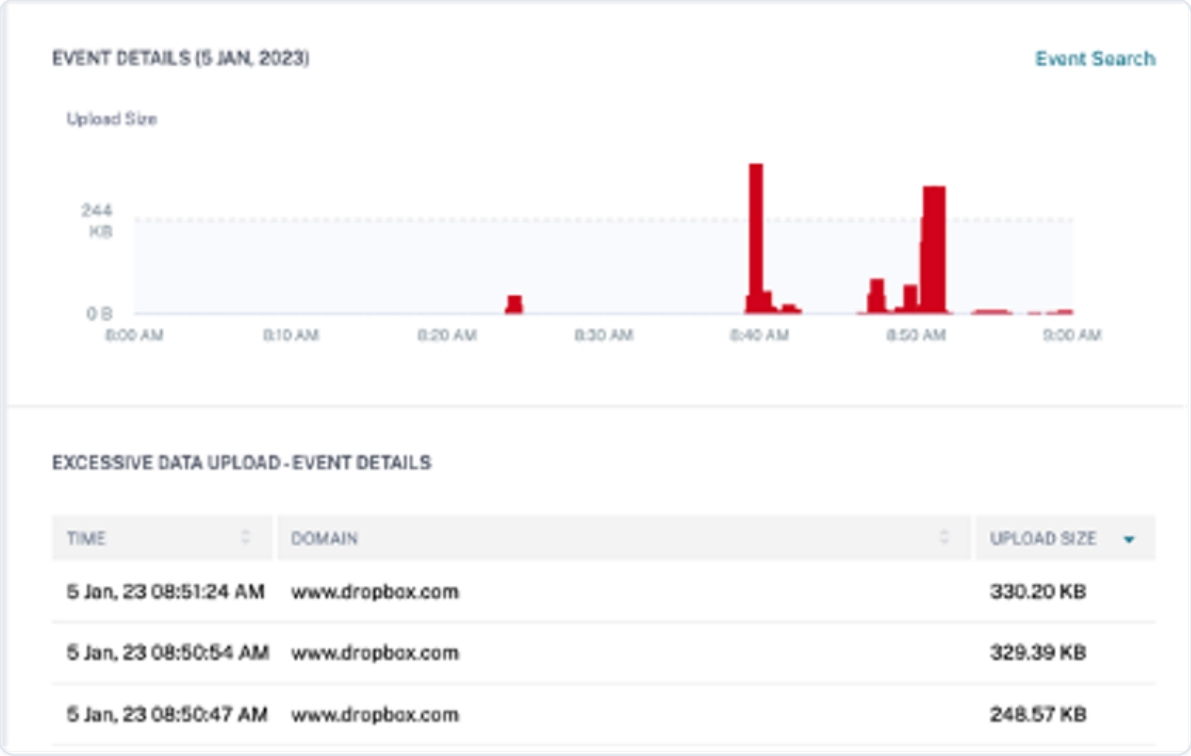
- The **WHAT HAPPENED** section provides a brief summary of the risk indicator, including the volume of data uploaded during the selected period.



- The **EVENT DETAILS** section, includes a timeline visualization of the individual data upload events that occurred during the selected time period. Also, you can view the following key information about each event:

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

- **Time**. The time the excessive data was uploaded to an application or a website.
- **Domain**. The domain to which the user uploaded the data.
- **Upload size**. Volume of data uploaded to the domain.



What actions you can apply to the user?

You can do the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Actions** menu, select an action and click **Apply**.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

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

Excessive data download

Citrix Analytics detects data access threats based on the excessive data downloaded by users in your network and triggers the corresponding risk indicator.

The risk indicator is reported when a user in your organization downloads excess volume of data from an application or website.

When is the Excessive data download risk indicator triggered?

You can configure Secure Private Access to monitor user activities, such as malicious, dangerous, or unknown websites visited and the bandwidth consumed, and risky downloads and uploads. When a user in your organization downloads data from an application or website, Secure Private Access reports these events to Citrix Analytics.

Citrix Analytics monitors all these events and if it determines that the user activity is contrary to the user's usual behavior, it updates the user's risk score. The Excessive data download risk indicator is added to the user's risk timeline.

The risk factor associated with the Excessive data download risk indicator is the Other risk indicators. For more information about the risk factors, see Citrix user risk indicators.

How to analyze the Excessive data download risk indicator?

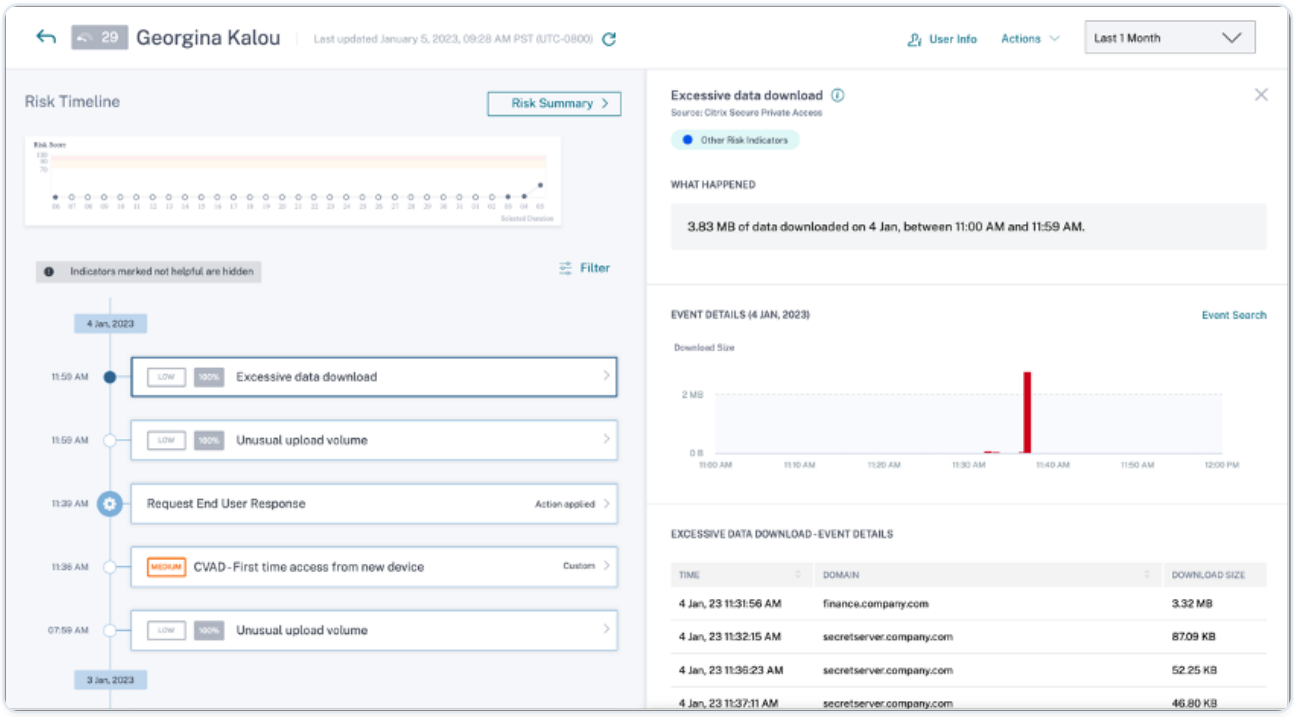
Consider a user Georgina Kalou, downloaded excess volume of data from an application or website. Secure Private Access reports these events to Citrix Analytics, which assigns an updated risk score to Georgina Kalou and adds the **Excessive data download** risk indicator entry to the user's risk timeline.

From Georgina Kalou's risk timeline, you can select the reported **Excessive data download** risk indicator. The reason for the event is displayed along with the details about the events, such as, time and domain details.

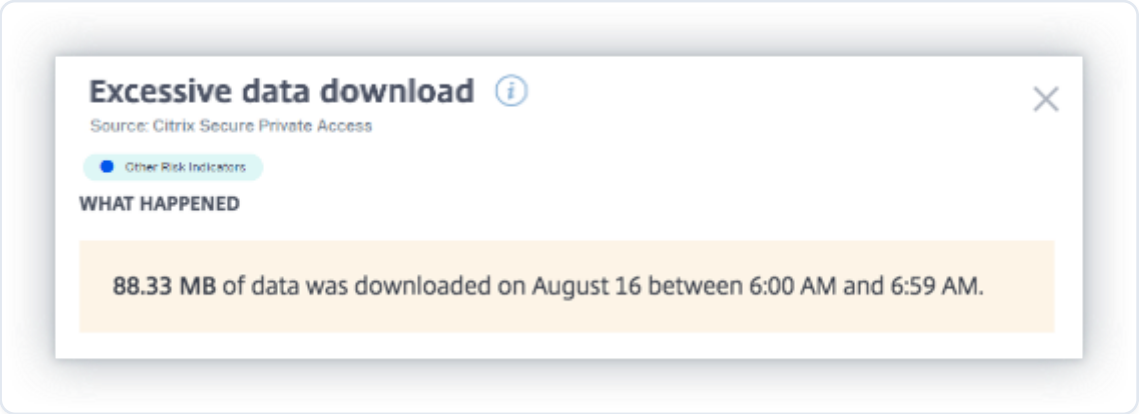
To view the **Excessive data download** risk indicator, navigate to **Security > Users**, and select the user.

When you select the **Excessive data download** risk indicator entry from the timeline, a corresponding detailed information panel appears in the right pane.

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

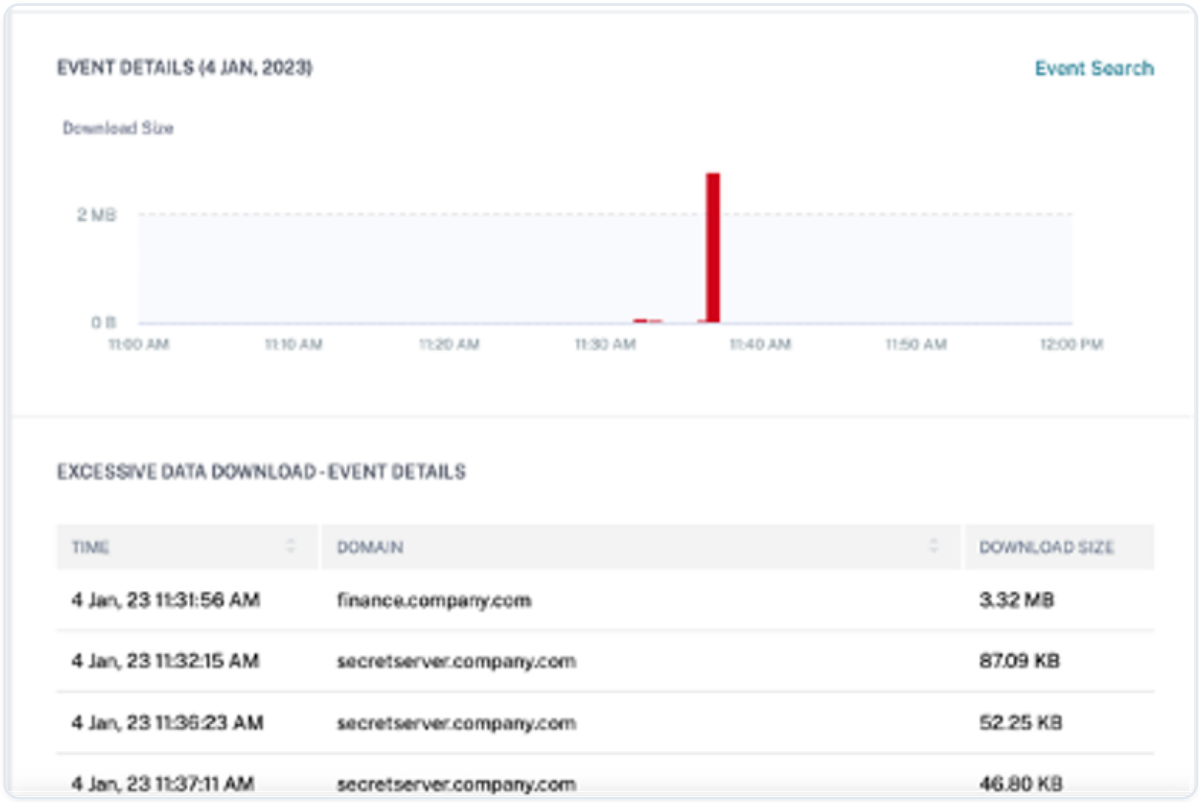


- The **WHAT HAPPENED** section provides a brief summary of the risk indicator, including the volume of data uploaded downloaded during the selected period.



- The **EVENT DETAILS** section, includes a timeline visualization of the individual data download events that occurred during the selected time period. Also, you can view the following key information about each event:
  - **Time**. The time the excessive data was downloaded to an application or a website.
  - **Domain**. The domain to which the user downloaded data.
  - **Download size**. Volume of data downloaded to the domain.

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



What actions you can apply to the user?

You can perform the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Actions** menu, select an action and click **Apply**.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

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

Citrix Virtual Apps and Desktops™ and Citrix DaaS risk indicators

Impossible travel

Citrix Analytics detects a user's logons as risky when the consecutive logons are from two different countries within a time period that is less than the expected travel time between the countries.

The impossible travel time scenario indicates the following risks:

- **Compromised credentials**: A remote attacker steals a legitimate user's credentials.
- **Shared credentials**: Different users are using the same user credentials.

When is the Impossible travel risk indicator triggered?

The **Impossible travel** risk indicator evaluates the time and estimated distance between each pair of consecutive user logons, and triggers when the distance is greater than an individual person can possibly travel in that amount of time.

NOTE

This risk indicator also contains logic to reduce false positive alerts for the following scenarios that do not reflect the users' actual locations:

- When users log on to virtual apps and desktops from proxy connections.
- When users log on to virtual apps and desktops from hosted clients.

How to analyze the Impossible risk indicator

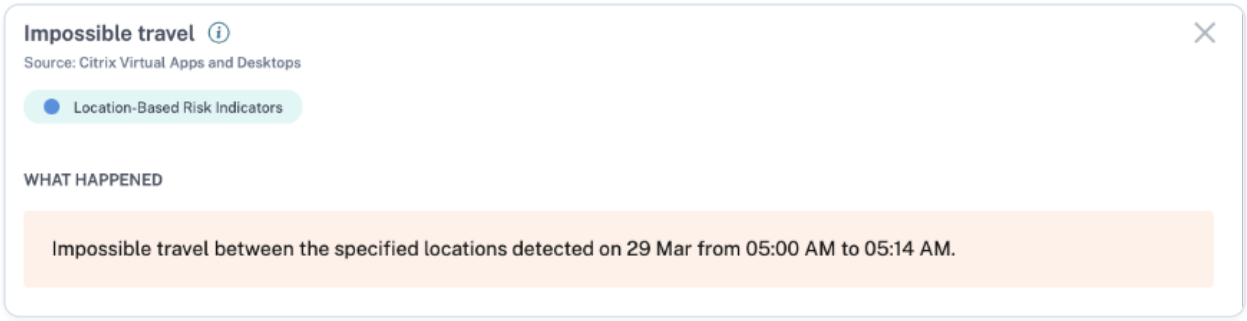
Consider the user Adam Maxwell, who logs on from two locations- Moskva, Russia and Hohhot, China within a time duration of one minute. Citrix Analytics detects this logon event as an impossible travel scenario and triggers the **Impossible travel** risk indicator. The risk indicator is added to Adam Maxwell's risk timeline and a risk score is assigned to him.

To view Adam Maxwell's risk timeline, select **Security > Users**. From the **Risky Users** pane, select the user Adam Maxwell.

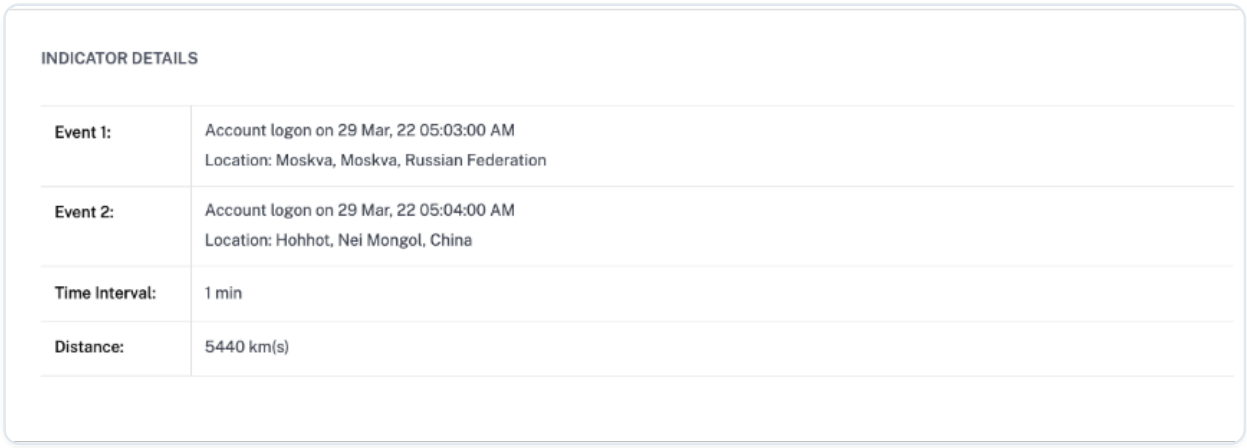
From Adam Maxwell's risk timeline, select the **Impossible travel** risk indicator. You can view the following information:

- The **WHAT HAPPENED** section provides a brief summary of the impossible travel event.

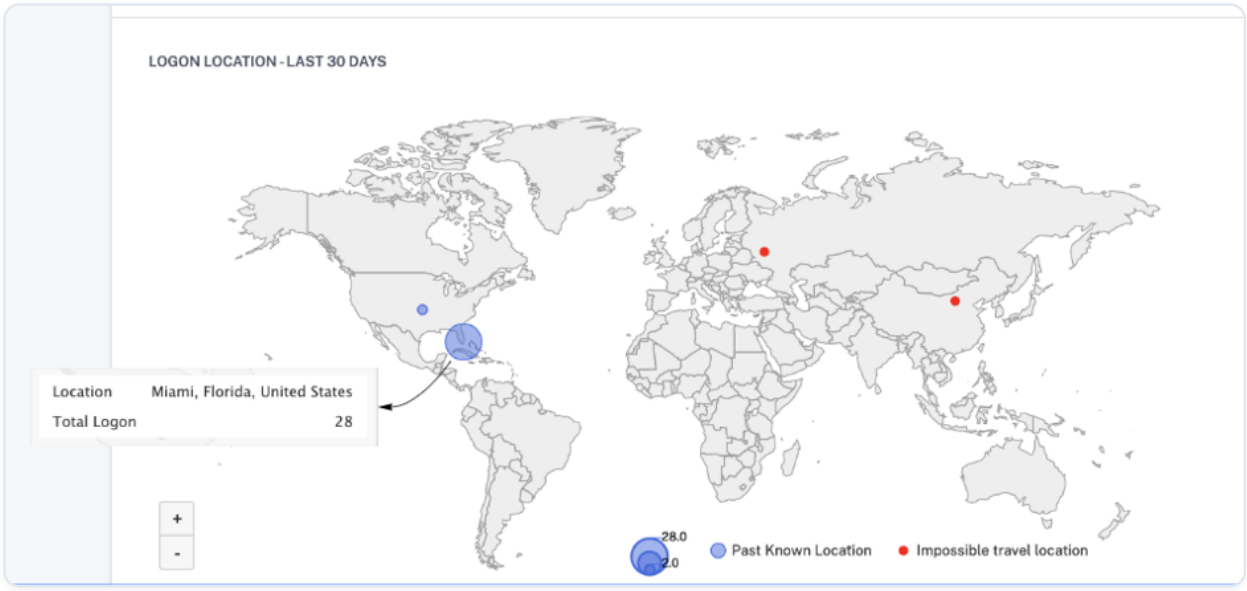
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- The **INDICATOR DETAILS** section provides the locations from which the user has logged on, the time duration between the consecutive logons, and the distance between the two locations.



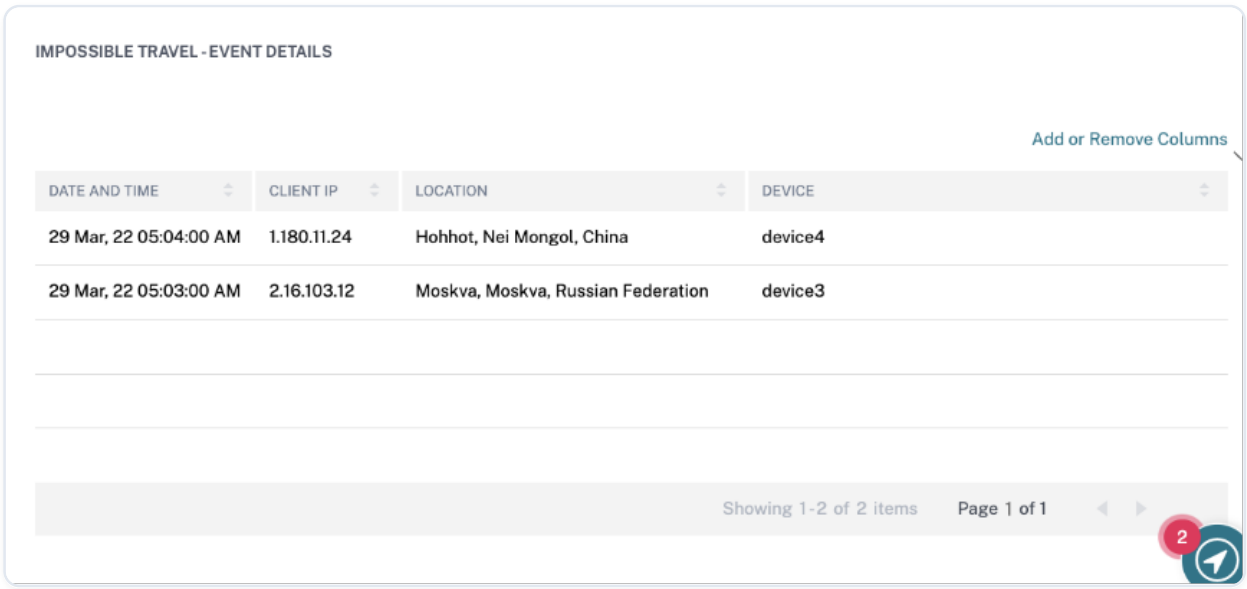
- The **LOGON LOCATION- LAST 30 DAYS** section displays a geographical map view of the impossible travel locations and known locations of the user. The location data is shown for the last 30 days. You can hover over the pointers on the map to view the total logons from each location.



- The **IMPOSSIBLE TRAVEL- EVENT DETAILS** section provides the following information about the impossible travel event:
  - **Date and time**: Indicates the date and the time of the logons.

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

- **Client IP**: Indicates the IP address of the user device.
- **Location**: Indicates the location from where the user has logged on.
- **Device**: Indicates the device name of the user.
- **Logon type**: Indicates whether the user activity is session logon or account logon. The account logon event is triggered when a user's authentication to their account is successful. Whereas the session logon event is triggered when a user enters their credential and logs on to their app or desktop session.
- **OS**: Indicates the operating system of the user device.
- **Browser**: Indicates the web browser that is used to access the application.



What actions you can apply to the users?

You can perform the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.
- **Log off user**. When a user is logged off from their account, they cannot access the resource through Virtual Desktops.
- **Start session recording**. If there is an unusual event on the user's Virtual Desktops account, the administrator can begin recording the user's activities of future logon sessions. However, if the user is on Citrix Virtual Apps and Desktops 7.18 or later, the administrator can dynamically start and stop recording the user's current logon session.

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

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Action** menu, select an action and click **Apply**.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

Potential data exfiltration

Citrix Analytics detects data threats based on excessive attempts to exfiltrate data and triggers the corresponding risk indicator.

The risk factor associated with the Potential data exfiltration risk indicator is the Data-based risk indicators. For more information about the risk factors, see Citrix user risk indicators.

The **Potential data exfiltration** risk indicator is triggered when a Citrix Receiver user attempts to download or transfer files to a drive or printer. This data might be a file-download event such as downloading a file to a local drive, mapped drives, or an external storage device. The data can also be exfiltrated using the clipboard or by the copy-paste action.

NOTE

The clipboard operations are supported only by the SaaS applications.

When is the Potential data exfiltration risk indicator triggered?

You can be notified when a user has transferred an excessive number of files to a drive or printer in a certain time period. This risk indicator is also triggered when the user uses the copy-paste action on their local computer.

When Citrix Receiver detects this behavior, Citrix Analytics receives this event and assigns a risk score to the respective user. The **Potential data exfiltration** risk indicator is added to the user's risk timeline.

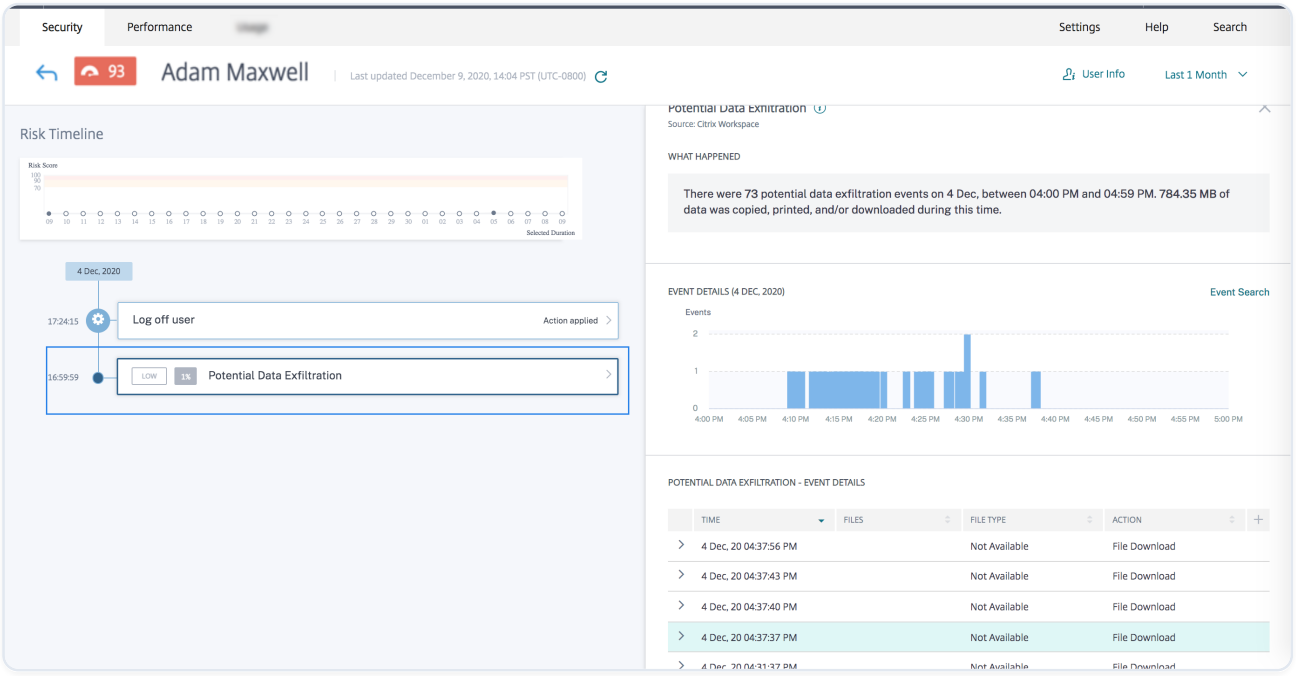
© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to analyze the Potential data exfiltration risk Indicator?

Consider the user Adam Maxwell, who is logged on to a session and attempts to print files that exceed the predefined limit. By this action, Adam Maxwell had exceeded his normal file transfer behavior based on machine learning algorithms.

From Adam Maxwell's timeline, you can select the **Potential data exfiltration** risk indicator. The reason for the event is displayed along with the details such as the files transferred and the device used to transfer the file.

To view the **Potential data exfiltration** risk indicator reported for a user, navigate to **Security > Users**, and select the user.



- The **WHAT HAPPENED** section, you can view the summary of the potential data exfiltration event. You can view the number of data exfiltration events during a specific time period.



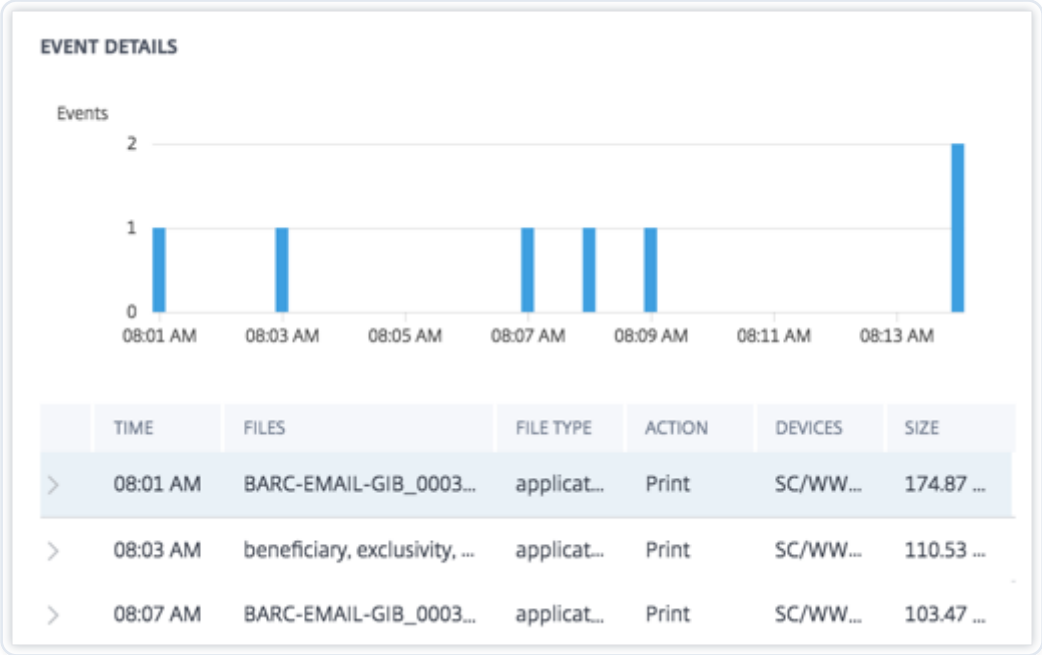
- The **EVENT DETAILS** section, the data exfiltration attempts appear in a graphical and tabular format. The events appear as individual entries in the graph and the table provides the following key information:
  - **Time**. The time the data exfiltration event occurred.
  - **Files**. The file that was either downloaded, printed, or copied.

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

- **File type**. The file type that was either downloaded, printed, or copied.

> **NOTE**
>
> The printed file name is available only from the SaaS apps printing event.

- **Action**. The kinds of data exfiltration event that was performed – print, download, or copy.
- **Devices**. The device used.
- **Size**. The size of the file that is exfiltrated.
- **Location**. The city from where the user is trying to exfiltrate data.



- The **ADDITIONAL CONTEXTUAL INFORMATION** section, during the event's occurrence, you can view the following:
  - The number of files that have been exfiltrated.
  - The actions performed.
  - The applications used.
  - Device used by the user.

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



What actions you can apply to the user?

You can perform the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.
- **Log off user**. When a user is logged off from their account, they cannot access the resource through Virtual Desktops.
- **Start session recording**. If there is an unusual event on the user's Virtual Desktops account, the administrator can begin recording the user's activities of future logon sessions. However, if the user is on {{page.cvad-onprem-product-name}} 7.18 or later, the administrator can dynamically start and stop recording the user's current logon session.

To learn more about actions and how to configure them manually, see Policies and Actions.

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Action** menu, select an action and click **Apply**.

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

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

Suspicious logon

Citrix Analytics detects the user's logons that appear unusual or risky based on multiple contextual factors, which are defined jointly by the device, location, and network used by the user.

When is the Suspicious logon risk indicator triggered?

The risk indicator is triggered by the combination of the following factors, where each factor is regarded as potentially suspicious based on one or more conditions.

FACTOR	CONDITIONS
Unusual device	The user logs on from a device that has not been used in the last 30 days.
	The user logs on from a device that is not managed by the virtual apps and desktops server.
	The user logs on from an HTML5 client or a Chrome client where the device signature is inconsistent with the user's history.
Unusual location	Log on from a city or a country that the user has not logged on in the last 30 days.
	The city or country is geographically far from the recent (last 30 days) logon locations.
	Zero or minimum users have logged on from the city or the country in the last 30 days.
Unusual network	Log on from an IP address that the user has not used in the last 30 days.
	Log on from an IP subnet that the user has not used in the last 30 days.

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

FACTOR	CONDITIONS
	Zero or minimum users have logged on from the IP subnet in the last 30 days.
IP threat	The IP address is identified as high risk by the community threat intelligence feed- Webroot.
	Citrix Analytics recently detected highly suspicious logon activities from the IP address from other users.

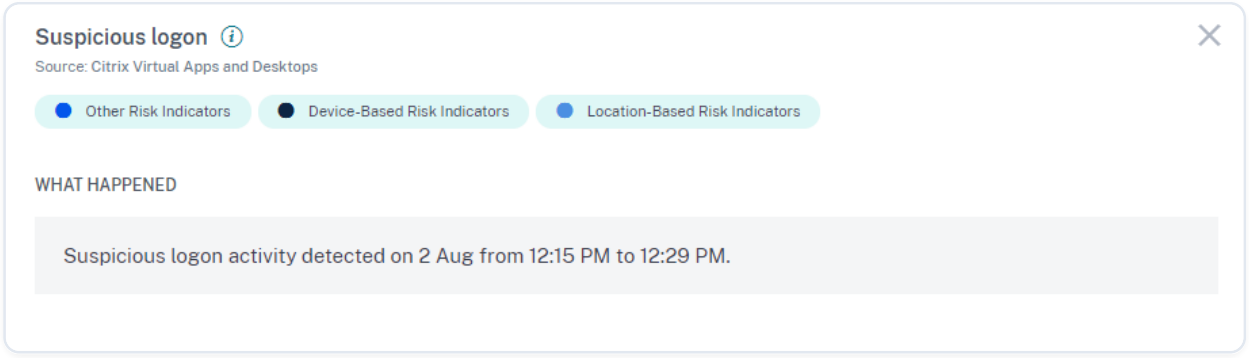
How to analyze the Suspicious logon risk indicator

Consider the user Adam Maxwell, who logs on from Mumbai, India for the first time. He uses a new device or a device that was not used for the last 30 days to log on to {{page.cvad-onprem-product-name}} and connected to a new network. Citrix Analytics detects this logon event as suspicious because the factors- location, device, and network deviate from his usual behavior and triggers the **Suspicious logon** risk indicator. The risk indicator is added to Adam Maxwell's risk timeline and a risk score is assigned to him.

To view Adam Maxwell's risk time, select **Security > Users**. From the **Risky Users** pane, select the user Adam Maxwell.

From Adam Maxwell's risk timeline, select the Suspicious logon risk indicator. You can view the following information:

- The **WHAT HAPPENED** section provides a brief summary of the suspicious activities that include the risk factors and the time of the event.



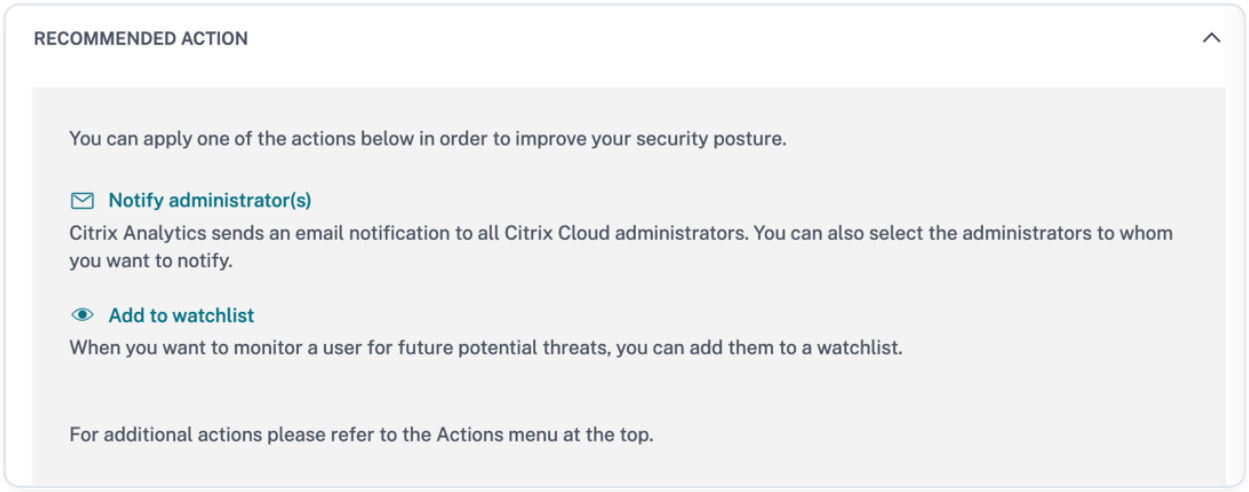
- In the **RECOMMENDED ACTION** section, you find the suggested actions that can be applied on the risk indicator. Citrix Analytics for Security™ recommends the actions depending on the

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

severity of the risk posed by the user. The recommendation can be one or combination of the following actions:

- Notify administrator(s)
- Add to watchlist
- Create a policy

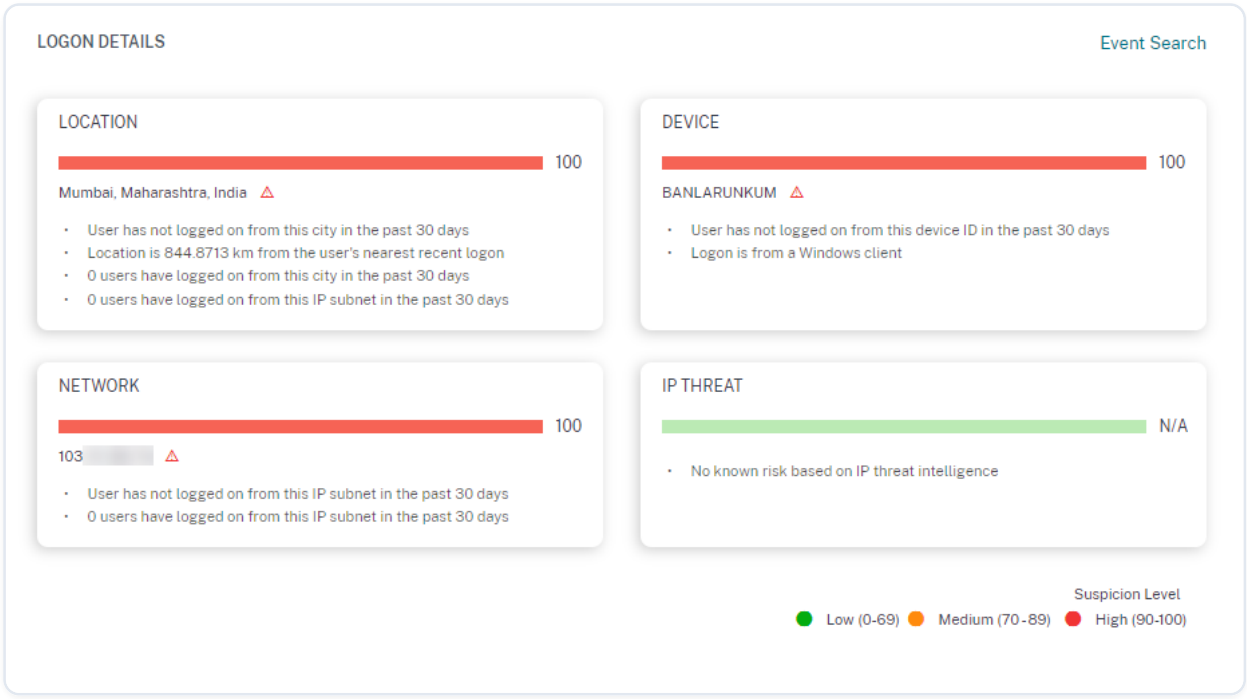
You can select an action based on the recommendation. Or you can select an action that you want to apply depending on your choice from the **Actions** menu. For more information, see Apply an action manually.



- The **LOGON DETAILS** section provides detailed summary of the suspicious activities corresponding to each risk factor. Each risk factor is assigned a score that indicates the suspicion level. Any single risk factor does not indicate high risk from a user. The overall risk is based on the correlation of the multiple risk factors.

SUSPICION LEVEL	INDICATION
0–69	The factor appears normal and is not considered suspicious.
70–89	The factor appears slightly unusual and is considered moderately suspicious with other factors.
90–100	The factor is entirely new or unusual and is considered highly suspicious with other factors.

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



- The **LOGON LOCATION- LAST 30 DAYS** section displays a geographical map view of the last known locations and the current location of the user. The location data is shown for the last 30 days. You can hover over the pointers on the map to view the total logons from each location.

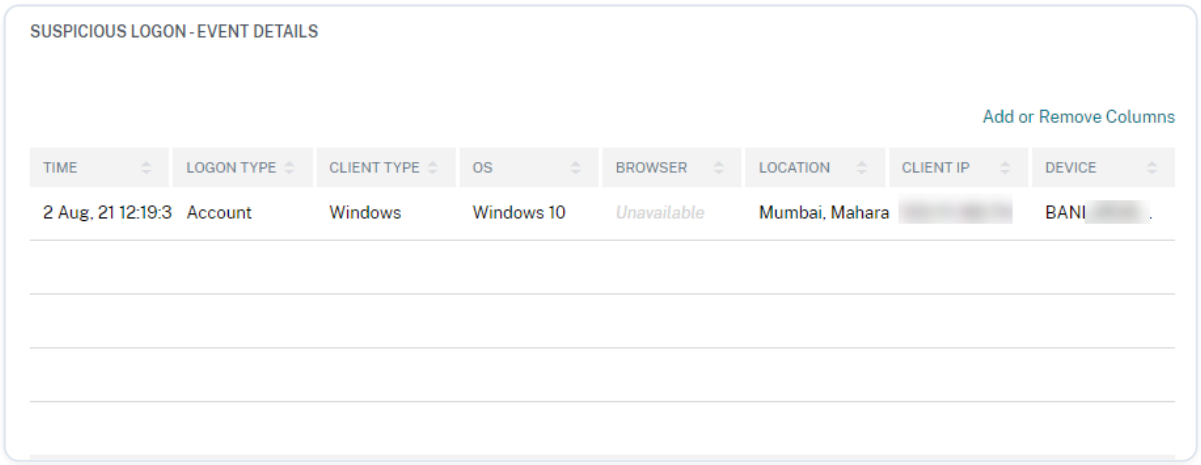


- The **SUSPICIOUS LOGON- EVENT DETAILS** section provides the following information about the suspicious logon event:
  - **Time**: Indicates the date and time of the suspicious logon.
  - **Logon type**: Indicates whether the user activity is session logon or account logon. The account logon event is triggered when a user's authentication to their account is successful.

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

Whereas the session logon event is triggered when a user enters their credential and logs on to their app or desktop session.

- **Client type**: Indicates the type of Citrix Workspace app installed on the user device. Depending on the operating system of the user device, the client type can be Android, iOS, Windows, Linux, Mac, and so on.
- **OS**: Indicates the operating system of the user device.
- **Browser**: Indicates the web browser that is used to access the application.
- **Location**: Indicates the location from where the user has logged on.
- **Client IP**: Indicates the IP address of the user device.
- **Device**: Indicates the device name of the user.



What actions you can apply to the users?

You can perform the following actions on the user's account:

- **Add to watchlist**. When you want to monitor a user for future potential threats, you can add them to a watchlist.
- **Notify administrator(s)**. When there is any unusual or suspicious activity on the user's account, an email notification is sent to all or selected administrators.
- **Log off user**. When a user is logged off from their account, they cannot access the resource through Virtual Desktops.
- **Start session recording**. If there is an unusual event on the user's Virtual Desktops account, the administrator can begin recording the user's activities of future logon sessions. However, if the user is on {{page.cvad-onprem-product-name}} 7.18 or later, the administrator can dynamically start and stop recording the user's current logon session.

To learn more about actions and how to configure them manually, see Policies and Actions.

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

To apply the actions to the user manually, navigate to the user's profile and select the appropriate risk indicator. From the **Action** menu, select an action and click **Apply**.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

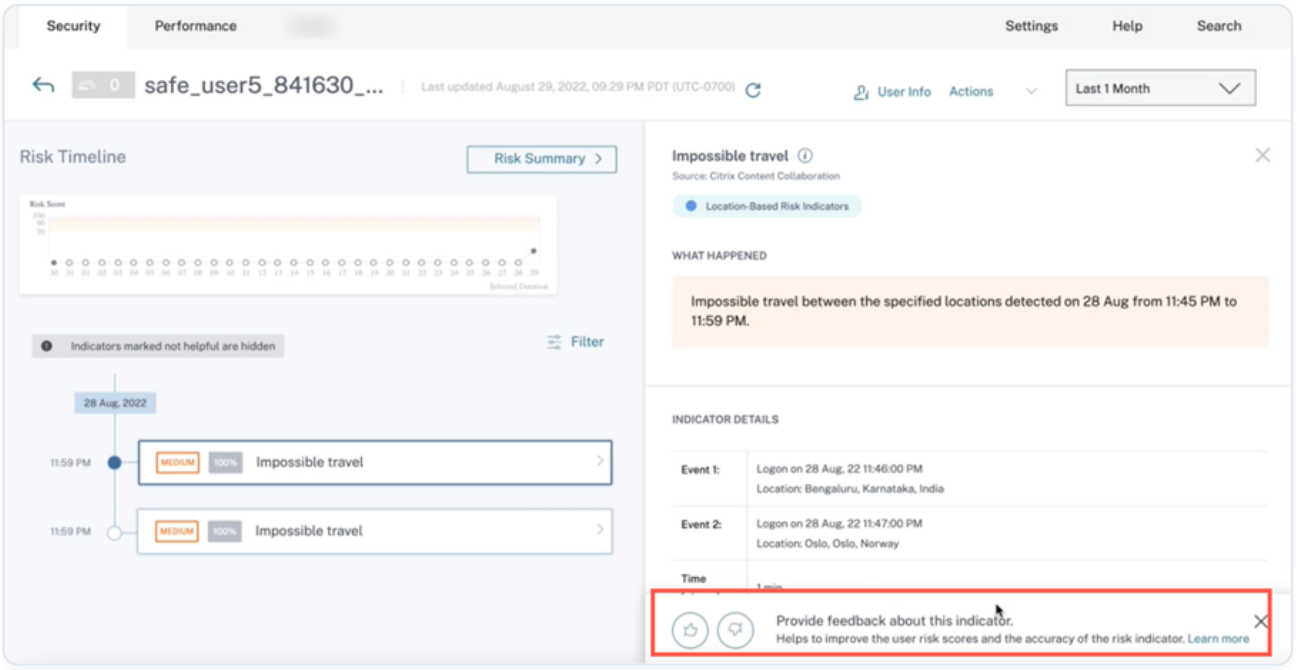
Provide feedback for User Risk indicators

Risk indicators are designed to detect and report potentially suspicious or anomalous user activity, while automatically increasing the user's risk score. In practice, although some occurrences of a risk indicator correspond to a legitimate underlying security threat, others turn out to be benign.

The indicator feedback feature allows you to explicitly flag risk indicator occurrences:

- As helpful when you believe there is true underlying user risk
- As not helpful if you have determined that there is no security threat. In this case, the indicator occurrence is hidden from the user timeline by default, and the user's risk score is automatically adjusted to exclude this indicator occurrence in subsequent calculations.

In addition, your collective feedback is used to drive future improvements in the risk indicator algorithms.

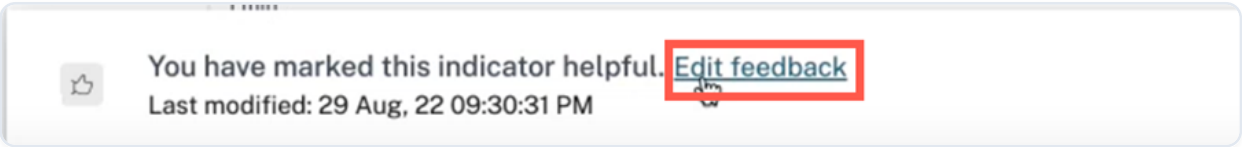


A feedback banner (with a thumbs-up and down icon) is displayed for each default risk indicator entry in the user timeline.

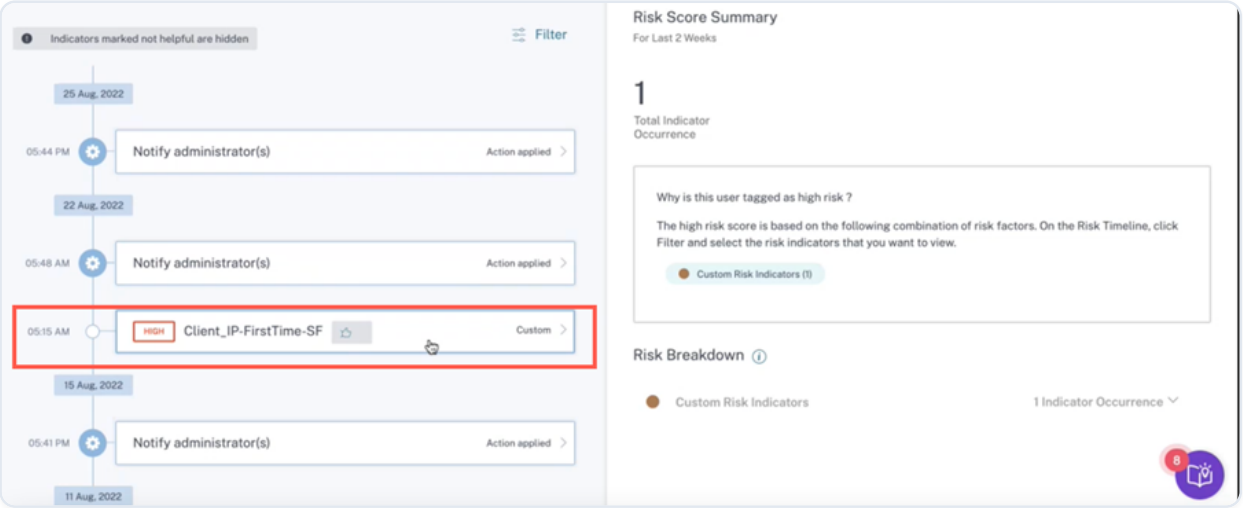
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Thumbs-up** icon - Indicator is helpful and has correctly identified risky activity. You can click the thumbs up icon and provide additional comments on how the indicator is helpful and its benefit.

  You can save your feedback and mark the indicator as helpful. You can also edit your comment by clicking Edit Feedback. The feedback banner provides the timeline of the last submitted feedback.



  When a risk indicator is marked helpful, this feedback is displayed in the corresponding user timeline entry, and reported to Citrix Analytics. The user risk score is not impacted.



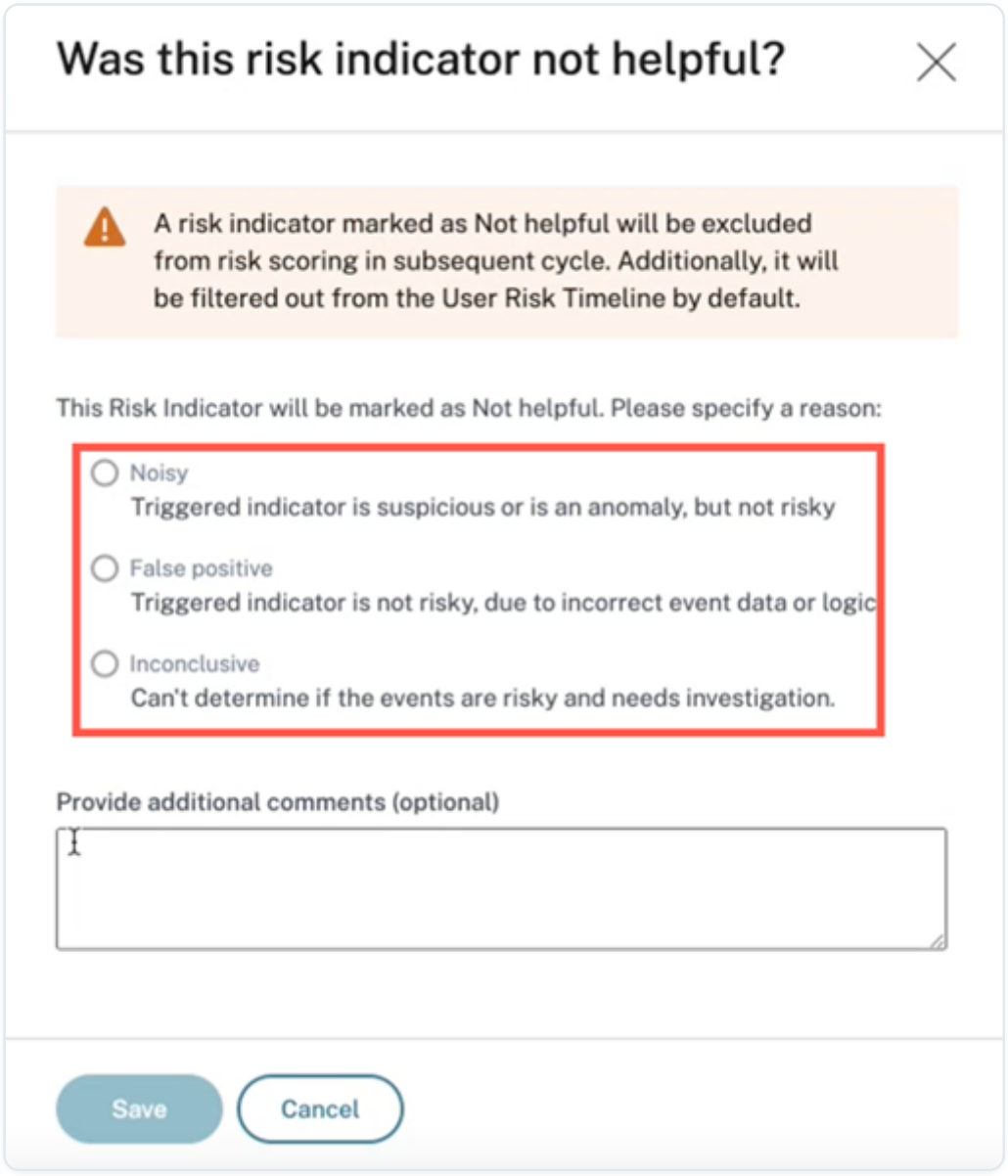
- **Thumbs-down** icon - Indicator is not helpful or incorrectly triggered. You can mark the indicator as not helpful and categorize it as **Noisy**, **False positive**, or **Inconclusive**. This occurrence of the risk indicator will be excluded from all subsequent updates to the user's risk score. You can also provide additional comments, if necessary.

  - **Noisy** – Triggered indicator is suspicious or is an anomaly, but not risky.
  - **False positive** – Triggered indicator is not risky, because of incorrect event data or logic.
  - **Inconclusive** – Can’t determine if the events are risky and needs investigation.

    NOTE

    It takes up to 15 minutes time to recalibrate the risk score.

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



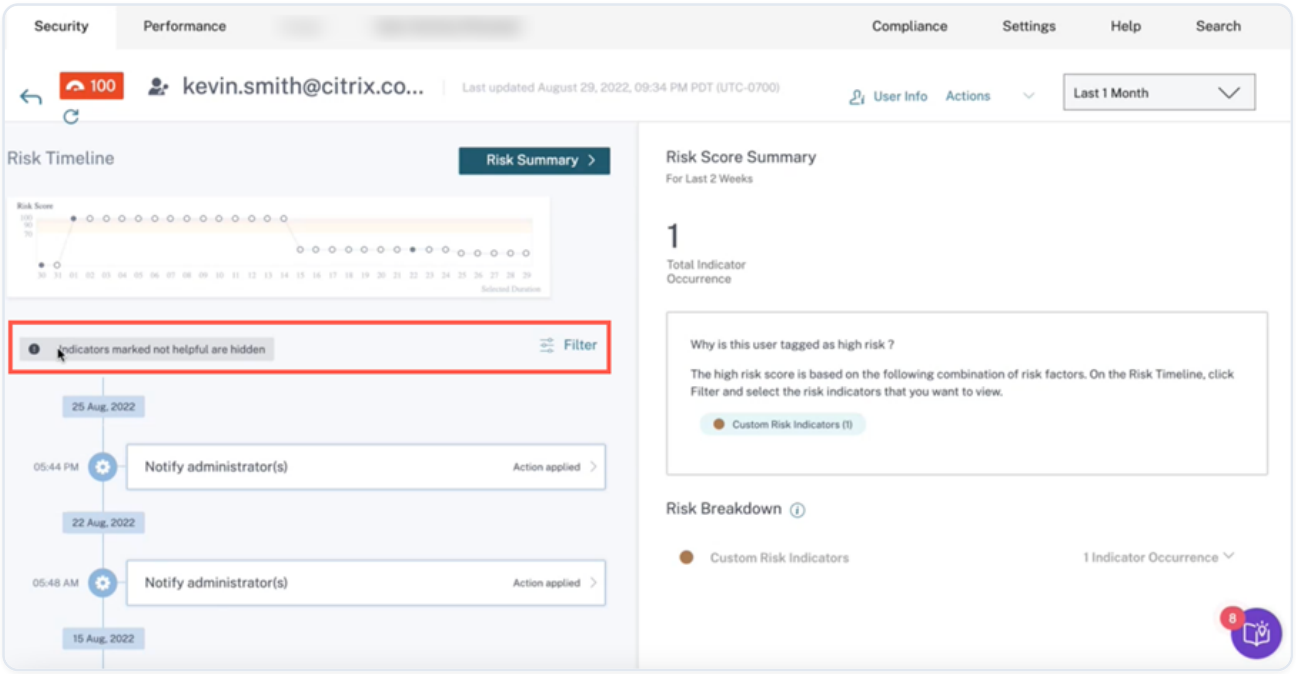
You can view the following results if an indicator is marked as not helpful:

- That particular indicator is hidden from timeline.
- The Risk score is recalibrated as a result of excluding this indicator occurrence from the risk score calculation in subsequent updates.
- Any additional information given as textual feedback is persisted for later reference.

View filters

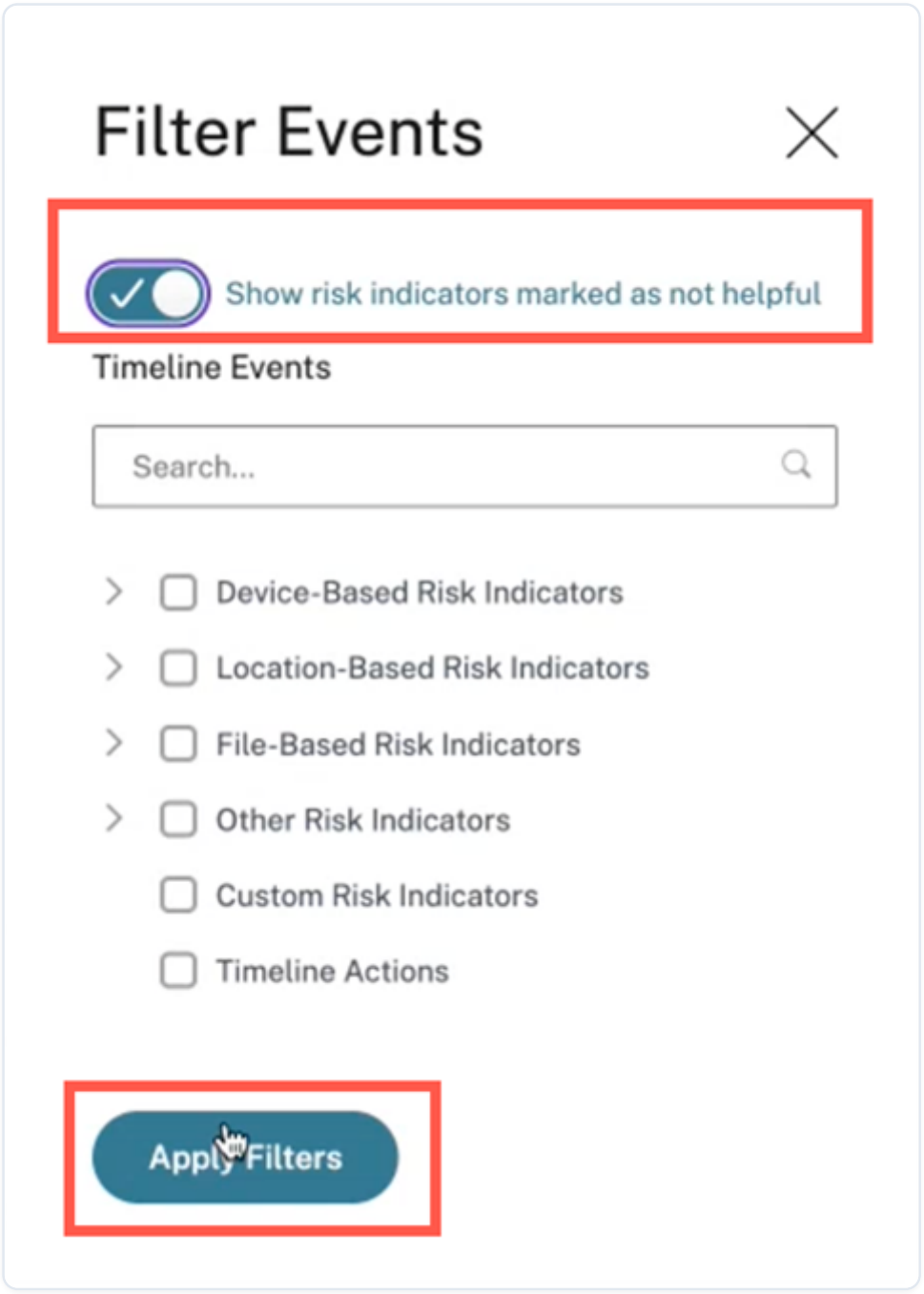
Indicators that are marked as not helpful are hidden by default.

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



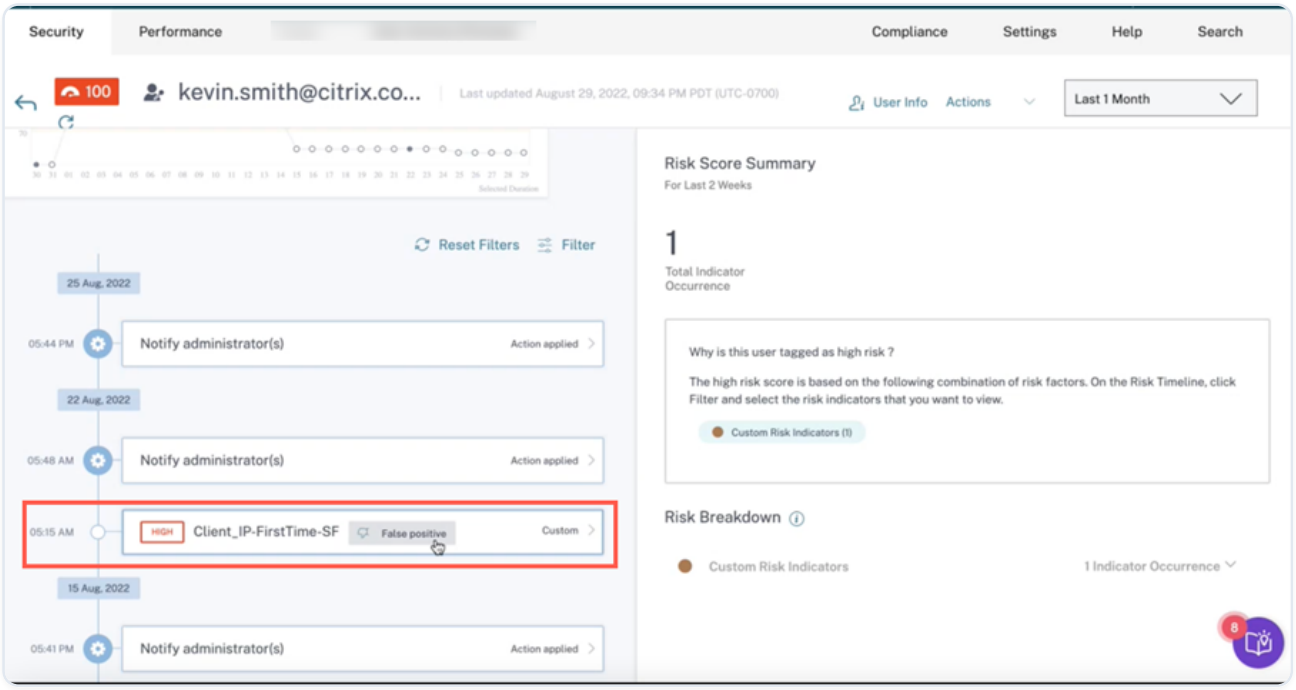
To view the hidden indicators, click **Filter**. In the **Filter Events** window that appears, turn on the **Show risk indicators marked as not helpful**.

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



You can search the indicators based on categories. For example, to view the location-based hidden risk indicators, select the category and click **Apply Filters**. You can view all the location-based indicators that are not helpful with the feedback details.

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



As an administrator, you can also perform the following actions as needed:

- Change the feedback
- Review previous feedback and the associated metadata
- Review the feedback provided by other administrator and the associated metadata

NOTE

- You can provide the feedback per user level not tenant level. The feedback for one risk indicator doesn't apply to all instances of that particular risk indicator.
- The feedback for one user doesn't apply to other users.

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

Microsoft Graph Security risk indicators

NOTE:

Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

Microsoft Graph Security receives data from the **Azure AD Identity Protection** or **Microsoft Defender for Endpoint** security providers, and sends the information to Citrix Analytics.

Azure AD Identity Protection triggers the following risk indicators and sends the information to Microsoft Graph Security:

- Anonymous IP address
- Impossible travel to atypical locations
- Users with leaked credentials
- Sign-ins from infected devices
- Sign-ins from IP addresses with suspicious activity
- Sign-ins from unfamiliar locations

For information about Defender for Endpoint, see Microsoft Defender for Endpoint.

The risk factor associated with the risk indicators is the IP-based risk indicators. For more information about the risk factors, see Citrix user risk indicators.

How to analyze Microsoft Graph Security risk indicators

Consider a user Maria Brown who exhibits one of the risky behaviors mentioned previously. Microsoft detects the incident and generates an alert. Citrix Analytics retrieves this alert and assigns an updated risk score to Maria Brown. Also, the appropriate risk indicator is added to Maria Brown's risk timeline.

To view the Microsoft Graph Security risk indicator entry for a user, navigate to **Security** > **Users**, and select the user.

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

From Maria’s timeline, you can select the latest risk indicator entry from the risk timeline. Its corresponding detailed information panel appears in the right pane. The **WHAT HAPPENED** section provides a brief summary of the risk indicator.

How to get more information about the risk indicators

For more information, see Azure Active Directory risk events.

What actions you can apply to the user

Currently, the ability to take appropriate actions on the user's account through the Microsoft Graph Security data source is not available.

For information on Microsoft Graph Security onboarding, see Microsoft Graph Security.

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

Custom risk indicators

There are two types of risk indicators that you see in Citrix Analytics for Security™:

- **Default risk indicators**: These risk indicators are based on the machine learning algorithm. For more information, see Citrix user risk indicators.
- **Custom risk indicators**: These risk indicators are created manually by the administrators.

When you create a custom risk indicator, you can define the triggering conditions and the parameters based on your use cases. If the user events match your defined criteria, Citrix Analytics triggers the custom risk indicator and displays it on the user's risk timeline.

Create custom risk indicators for the following data sources:

- Citrix Gateway
- Citrix Secure Private Access™
- Citrix Virtual Apps and Desktops™ on-premises
- Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)
- Citrix Secure Browser

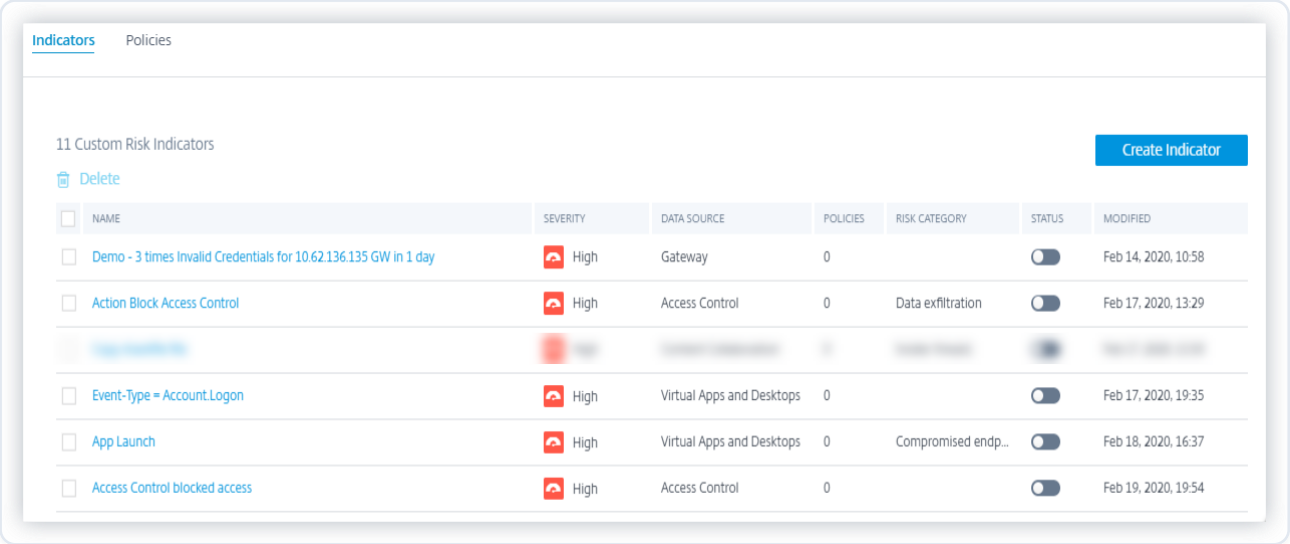
Preconfigured custom risk indicators

Citrix also provides a few custom risk indicators with preconfigured conditions to help you monitor the security of your Citrix infrastructure. You can modify the preconfigured conditions based on your use cases. For more information, see Preconfigured custom risk indicators.

Custom risk indicators page

The **Custom Risk Indicators** page provides insights into all the custom risk indicators generated for a user, severity, data source, number of policies, risk category, status, and the last modified date and time of the indicator. To create a custom risk indicator, see Creating a custom risk indicator.

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



When you select the risk indicator, you are redirected to the **Modify Risk Indicator** page. For more information, see Modifying a custom risk indicator.

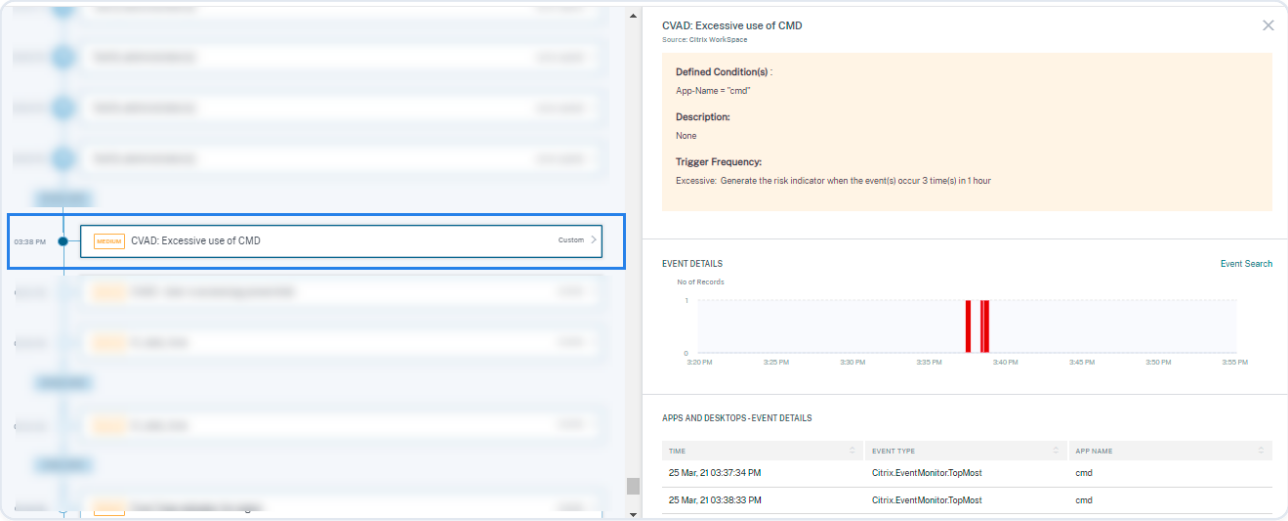
Analyzing a custom risk indicator

Consider a user whose action triggered a custom risk indicator that you have defined. Citrix Analytics displays the custom risk indicator on the user's risk timeline.

When you select the custom risk indicator on the user's risk timeline, the right pane displays the following information:

- **Defined Condition(s)**: Shows a summary of the conditions that you define while creating a custom risk indicator.
- **Description**: Provides a summary of the description you provide while creating the custom risk indicator. If no description is provided while creating the custom risk indicator, this section reflects **None**.
- **Trigger Frequency**: Displays the option that you select in the **Advanced options** section while creating the custom risk indicator.
- **Event Details**: Displays the timeline and the details of the user events that triggered the custom risk indicator. You can click **Event Search** to view the user events on the self-service search page. The self-service search page displays the events associated with the user and the custom risk indicator. The search query shows the conditions defined for the custom risk indicator.

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



NOTE

Custom risk indicators are represented with a label on the user risk timeline.

Actions you can apply to the user

When a custom risk indicator is triggered for a user, you can apply an action manually or create a policy to apply an action automatically. For more information, see Policies and actions.

Custom risk indicator templates

You can create a custom risk indicator by using one of the predefined templates or proceed without using a template.

The templates act as a starting point for creating a custom risk indicator. It guides you to create a custom risk indicator by providing predefined queries and parameters that you can select based on your use cases.

You can use a template as is or modify it to meet your requirements. Using the templates, administrators can create risk indicators of interest with no additional training.

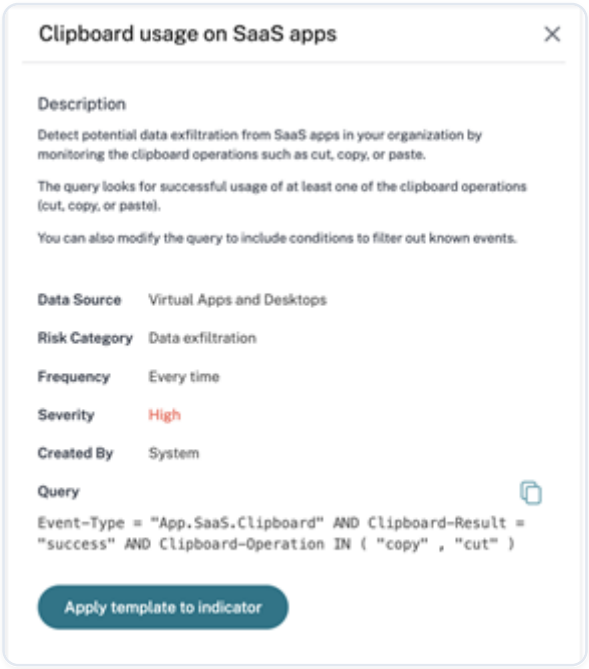
A template consists of the following information:

- **Description**: Indicates the purpose of the query defined in the template.
- **Data source**: Indicates the data source on which the template applies.
- **Risk category**: Indicates the risk category associated with the events searched by the query. There are four categories of risky events- Data exfiltration, Insider threats, Compromised users, and Compromise end points. For information, see risk categories.

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

- **Frequency**: Indicates the frequency at which the query triggers.
- **Severity**: Indicates the severity of the risk associated with the event. The risk can be high, medium, or low.
- **Created by**: Indicates the creator of the template. The templates are always system defined.
- **Query**: Indicates the conditions defined in the template. The query retrieves the user events that satisfy the conditions.

The following image shows the template for the use case-clipboard usage on SaaS apps.

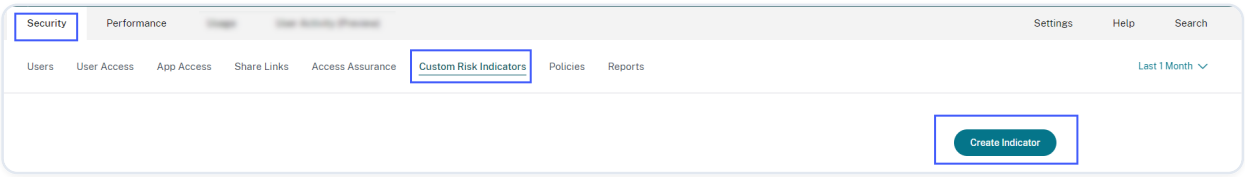


If you don't find a template for your use case or you want to define your own query, you can proceed without a template.

Creating a custom risk indicator

To create a custom risk indicator:

1. Navigate to **Security > Custom Risk Indicators > Create Indicator**.

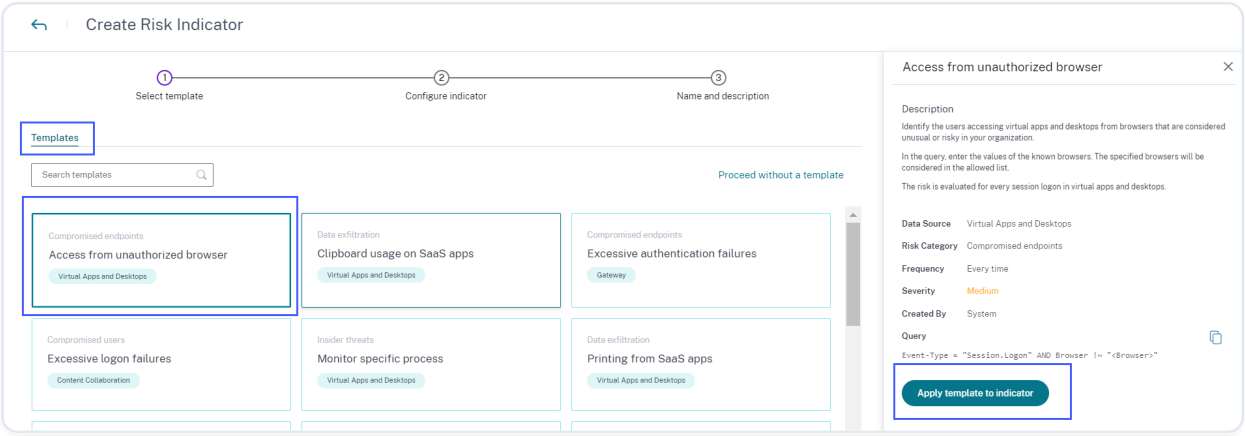


2. Select a template to view the use case. If it meets your requirement, select **Apply template to indicator**.

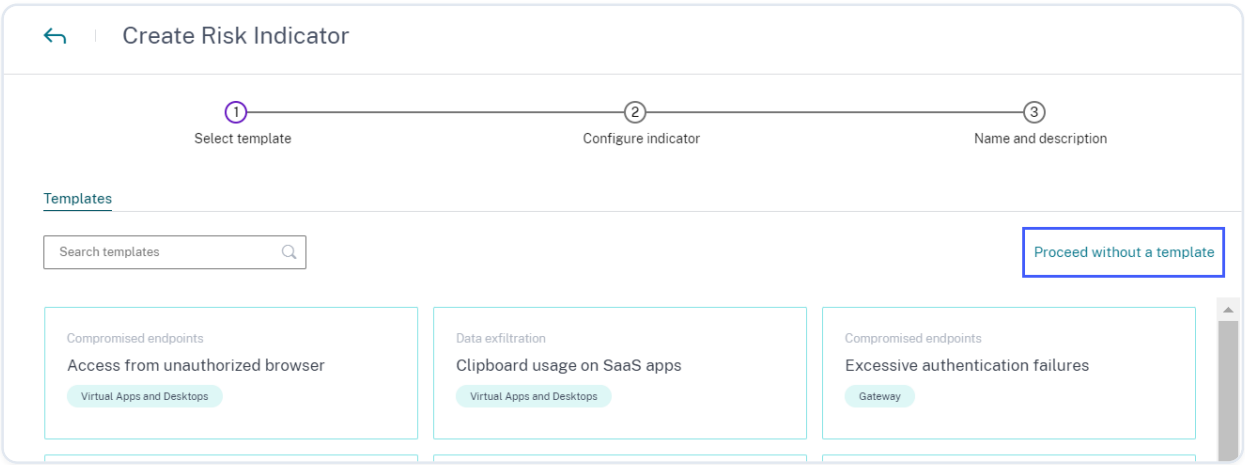
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

You can also modify the predefined conditions and the parameters of a template.



3. If you don't find a desired template or want to create your own condition, select **Proceed without a template**.



4. Follow the onscreen instructions to create an indicator.

NOTES

- You can create custom risk indicators up to a maximum limit of 50. If you reach this maximum limit, you must either delete or edit any existing custom risk indicator to create a custom risk indicator.
- When a custom risk indicator is triggered, it gets displayed on the user timeline immediately. However, the risk summary and the risk score of the user get updated after a few minutes (approximately 15- 20 minutes).

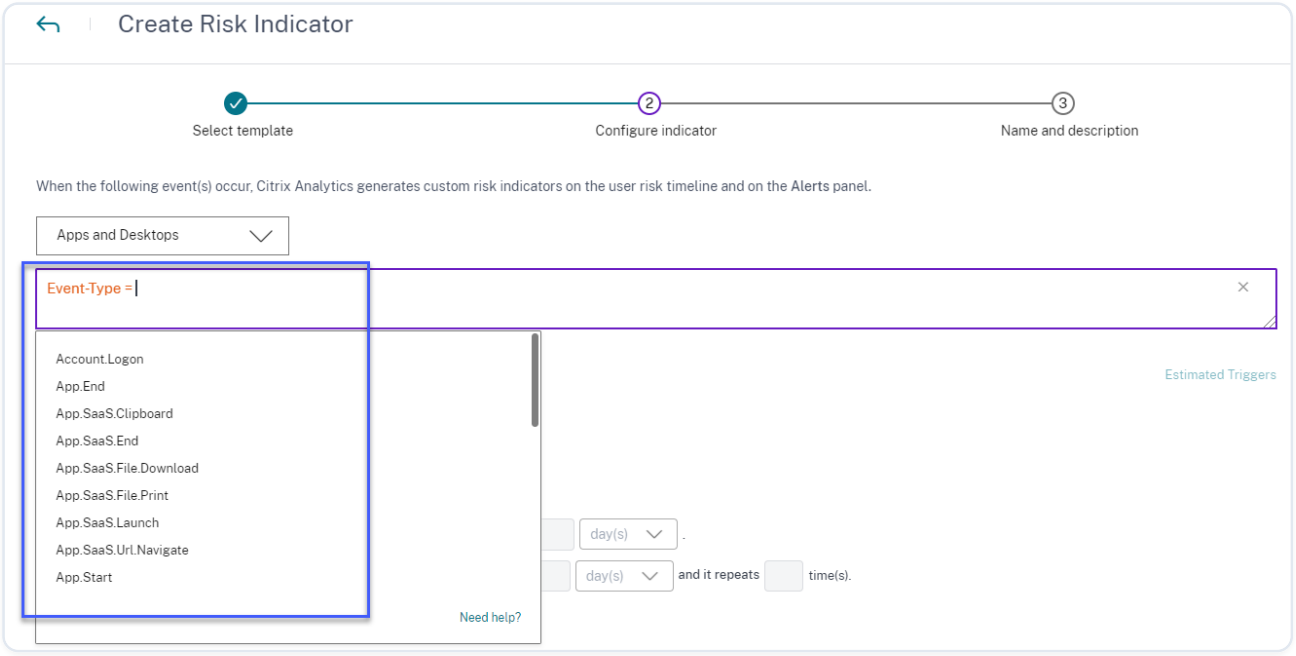
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Defining a condition for a custom risk indicator

Use the query box to define your conditions for the custom risk indicator. Depending on the selected data source, you get the corresponding dimensions and the valid operators for defining your conditions.

When selecting certain dimensions like `Event-Type` and `Clipboard-Operation` along with a valid operator, the values of the dimension are shown automatically. You can choose a value from the suggested options or enter a new value depending on your requirements.

The following image shows the suggested values of the dimension `Event-Type`.



If you use a template, the condition is predefined. However, you can append or modify the predefined condition based on your use case.

Below the query box, you see the **Estimated Triggers** link. Click the link to predict the approximate instances of the custom risk indicator that would be triggered for the defined conditions. These instances are calculated based on the historical data that Citrix Analytics maintains and meets the defined conditions.

Ensure to click **Estimated Triggers** to predict the number of custom risk indicator occurrences for the last defined condition.

Using the advanced options

On the **Advanced options** section, select the frequency of the event to trigger the custom risk indicator. When you do not select any option, Citrix Analytics considers **Every time: Generate the**

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

risk indicator every time the event(s) occur as the default option and generates the custom risk indicator. You can select one of the following options:

- **Every time**: The risk indicator is triggered whenever the events meet the defined conditions.
- **First time**: The risk indicator is triggered when the events meet the defined conditions for the first time.
    - **First time for a new**: Enable this option to detect events received from a new entity for the first time. Some examples of the entities are Client IP, Country, City, and Device-ID. You can select only one entity based on the data source. This option allows you to create a risk indicator without specifying an explicit value for the entities. For example, when you select the entity as "City", you need not specify the city name. The risk indicator is triggered when events are received from a new city for the first time.

      The following table lists the entities corresponding to each data source and describes the trigger conditions.

DATA SOURCE	ENTITY	TRIGGER CONDITION
Secure Private Access	City	When a user logs on from a new city for the first time.
	Client-IP	When a user logs on from a new IP address for the first time.
	Country	When a user logs on from a new country for the first time.
Apps and Desktops	App-Name	When a user opens a new virtual application or a SaaS application for the first time.
	App-URL	When a user enters a new app URL on a browser in their Virtual desktop for the first time.

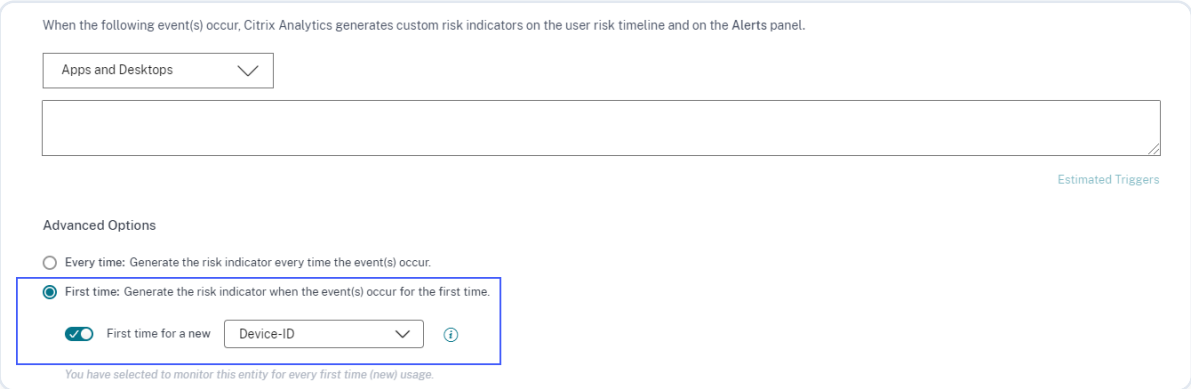
© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATA SOURCE	ENTITY	TRIGGER CONDITION
	City	When a user launches apps or desktops from a new city for the first time.
	Client-IP	When a user logs on from a new IP address for the first time.
	Country	When a user launches apps or desktops from a new country for the first time.
	Device-ID	When a user launches virtual apps or virtual desktops from a new device such as a mobile, laptop, or desktop machine for the first time.
	Download-Device-Type	When a user uses a new storage media such as a USB drive for the first time.
	Print-File-Format	Format of the printed file.
	Print-File-Size	Size of the printed file in bytes.
	Print-File-Name	Name of the printed file.
	Printer-Name	Name of the printer used.
	Total-Copies-Printed	Total number of copies printed by the user.
	Total-Pages-Printed	Total number of the document pages printed by the user.

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

DATA SOURCE	ENTITY	TRIGGER CONDITION
Gateway	Client-IP	When a user logs on from a new IP address for the first time.
Secure Browser	User-Name	The name of the user who initiated the event.
	Access-Allowed	Whether the user is allowed or denied access to the host service.
	Client-IP	The IP address of the user device.
	Host-Name-Accessed	The host service accessed by the user over the network.
	Session-ID	The unique number assigned to the user session.

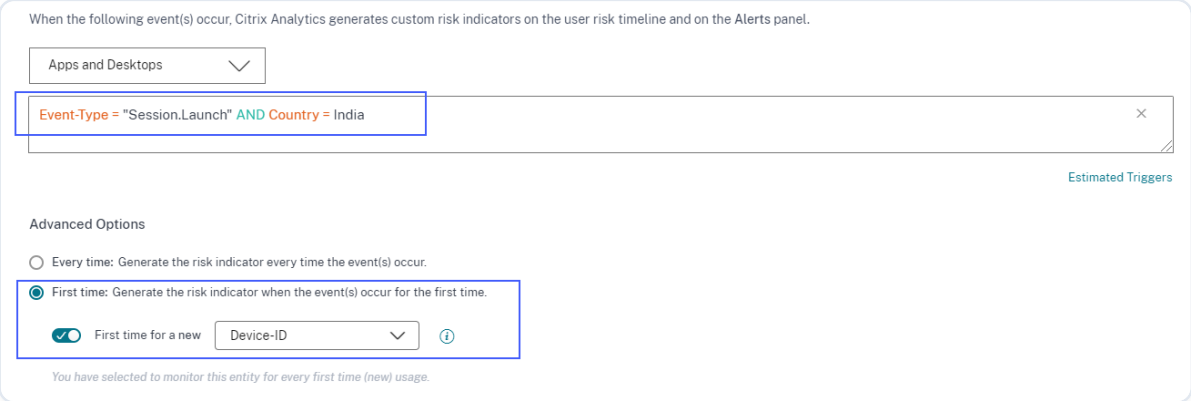
The following example shows a custom risk indicator created for the Apps and Desktops data source. The risk indicator is triggered when a user launches a virtual desktop or a virtual app from a new device for the first time.



You can also add a condition along with the **First time for a new** option. In this case, the risk indicator is triggered when it detects the events from the new entity for the first time and when the events meet the defined condition.

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

The following example shows a condition defined for the custom risk indicator and the **First time for a new Device-ID** option enabled. The risk indicator is triggered when a user located in India launches a virtual desktop session from a new device for the first time.



- **Excessive**: The risk indicator is triggered after the following conditions are met:
  - Events meet the defined conditions.
  - Events occur for a specified number of times during the specified period.
- **Frequent**: The risk indicator is triggered after the following conditions are met:
  - The events meet the defined conditions.
  - The events occur for the specified number of times during the specified period.
  - The event pattern repeats for the specified number of times.

Selecting the risk category

Select the risk category for your custom risk indicator.

Risk indicators are grouped based on the type of risk exposure of the custom risk indicator. For assistance on the risk category selection, see Risk Categories.

Selecting the severity

Severity indicates the level of seriousness of a risky event, which is detected by the risk indicator. When you create a custom risk indicator, select a severity-high, medium, or low.

If you apply a template, the severity option is preselected. You can modify this preselection depending on your use case.

Supported operators for defining a condition

You can use the following operators while defining a condition.

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

OPERATOR	DESCRIPTION	EXAMPLE	OUTPUT
	Assign a value to the search query.	User-Name : John	Displays events for the user John.
=	Assign a value to the search query.	User-Name = John	Displays events for the user John.
~	Search similar values.	User-Name ~ test	Displays events having similar user names.
""	Enclose values separated by spaces.	User-Name = "John Smith"	Displays events for the user John Smith.
<, >	Search for relational value.	Data Volume > 100	Displays events where data volume is greater than 100 GB.
AND	Search values where both conditions are true.	User-Name : John AND Data Volume > 100	Displays events of user John where data volume is greater than 100 GB.
*	Search values that match the character zero or more times.	User-Name = John*	Displays events for all user names that begin with John.
		User-Name = *John*	Displays events for all user names that contain John.
		User-Name = *Smith	Displays events for all user names that end with Smith.
!~	Checks the user events for the matching pattern that you specify. This NOT LIKE operator returns the events that do not contain	User-Name !~ John	Displays events for the users except John, John Smith, or any such users that contain the matching name "John".

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

OPERATOR	DESCRIPTION	EXAMPLE	OUTPUT
	the matching pattern anywhere in the event string.		
!=	Checks the user events for the exact string that you specify. This NOT EQUAL operator returns the events that do not contain the exact string anywhere in the event string.	Country != USA	Displays events for the countries except USA.
IN	Assign multiple values to a dimension to get the events related to one or more values.	User-Name IN (John, Kevin)	Find all events related to John or Kevin.
NOT IN	Assign multiple values to a dimension and find the events that do not contain the specified values.	User-Name NOT IN (John, Kevin)	Find the events for all users except John and Kevin.
IS EMPTY	Checks for null value or empty value for a dimension. This operator works for only string type dimensions such as `App-Name`, `Browser`, and `Country`. It does not work for non-string (number) type dimensions such as `Upload-File-Size`,	Country IS EMPTY	Find events where the country name is not available or empty (not specified).

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

OPERATOR	DESCRIPTION	EXAMPLE	OUTPUT
	`Download-File-Size`, and `Client-IP`.		
IS NOT EMPTY	Checks for not null value or a specific value for a dimension. This operator works for only string type dimensions such as `App-Name`, `Browser`, and `Country`. It does not work for non-string (number) type dimensions such as `Upload-File-Size`, `Download-File-Size`, and `Client-IP`.	Country IS NOT EMPTY	Find events where the country name is available or specified.
OR	Searches for values where either or both conditions are true.	(User-Name = `John*` OR User-Name = `*Smith`) AND Event-Type = “Session.Logon”	Displays `Session.Logon` events for all user names that begin with John or end with Smith.

NOTE

For the **NOT EQUAL** operator, while entering the values for the dimensions in your condition, use the exact values available on the self-service search page for a data source. The dimension values are case-sensitive.

Modifying a custom risk indicator

1. Navigate to **Security > Custom Risk Indicators**.

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

2. Select the custom risk indicator that you want to modify.
3. On the **Modify Indicator** page, modify the information as required.
4. Click **Save Changes**.

NOTE

If you modify the attributes such as condition, risk category, severity, and name of an existing custom risk indicator, on the user timeline, you can still view the previous occurrences of the custom risk indicator (with the old attributes) that were triggered for the user.

For example, you have created a custom risk indicator with the condition *Country != India*. So, this custom risk indicator is triggered when a user logs on from outside the country India. Now, you modify the condition of the custom risk indicator to *Country != "United States"*. In this case, you can still view the previous occurrences of the custom risk indicator with the condition *Country != India* on the user timelines who triggered the risk indicator.

Deleting a custom risk indicator

1. Navigate to **Security > Custom Risk Indicators**.
2. Select the custom risk indicator that you want to delete.
3. Click **Delete**.
4. In the dialog, confirm your request to delete the custom risk indicator.

NOTE

If you delete a custom risk indicator, on the user timeline, you can still view the previous occurrences of the custom risk indicator that were triggered for the user.

For example, you delete an existing custom risk indicator with the condition *Country != India*. In this case, you can still view the previous occurrences of the custom risk indicator with the condition *Country != India* on the user timelines who triggered the risk indicator.

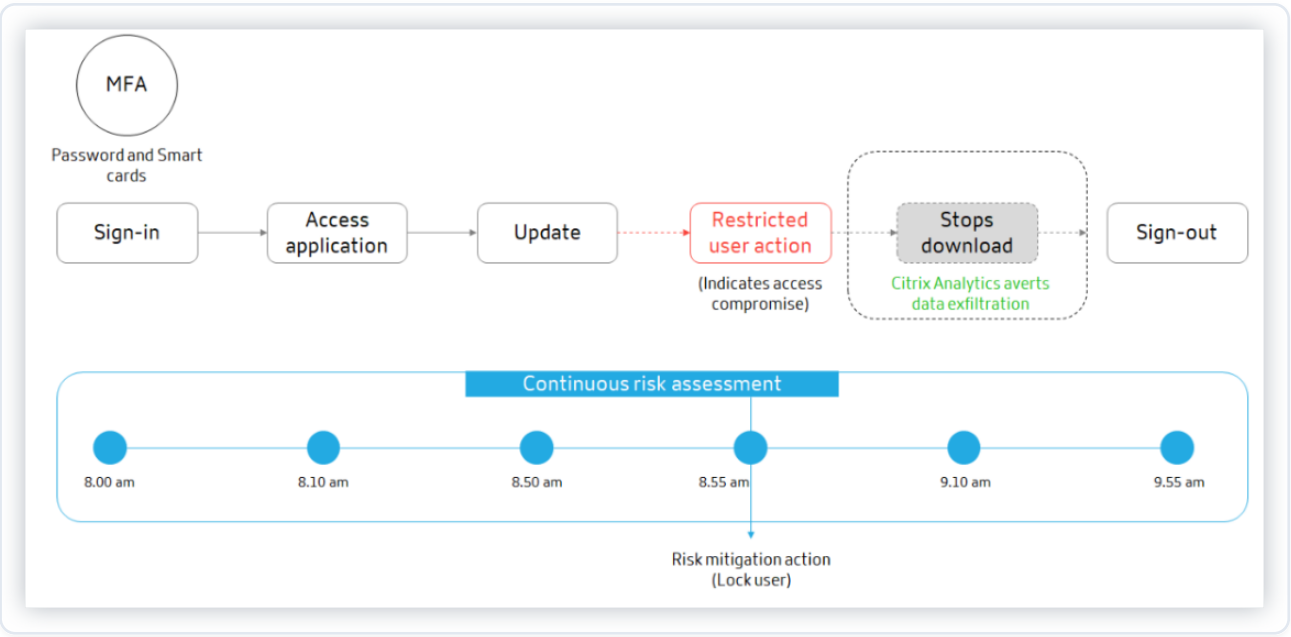
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Continuous risk assessment

An increased use of portable computing devices and the internet allows Citrix Workspace™ users to work from almost any location and on any device. The challenge with this flexibility is that, remote access exposes sensitive data to security risks through cyber-criminal activities like data exfiltration, theft, vandalism, and service disruptions. Employees within organizations are also likely to contribute to this damage.

Some conventional ways of addressing such risks are to implement multifactor authentication, short sign-in sessions, and so on. Although these risk assessment methods ensure a higher level of security, they do not provide complete security after the initial validation of users. If a malicious user is successful in gaining access to the network, they misuse sensitive data that is harmful to an organization.

To enhance the security aspect and to ensure a better user experience, Citrix Analytics introduces the solution of continuous risk assessment. This solution protects your data from both external cyber criminals and malicious insiders by ensuring that the risk exposure of the users who are using {{page.cvad-onprem-product-name}} or {{page.daas-product-name}} (formerly Citrix Virtual Apps and Desktops service) remains the same as it was when verified during the initial stage, without requiring the user to prove it every time. This solution is achieved by continuously assessing a risky event during a session and by automatically applying actions to prevent the organization's resources from further misuse.



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

Use cases

Consider a user Adam Maxwell, who was able to access a network for the first time after multiple failed sign-in attempts from an unusual location that is contrary to their usual behavior. Also, the location has a track record of cyber attacks. In this scenario, you are required to take immediate action to avoid Adam's account from further misuse. You can lock Adam's account and notify him about the action taken. This action might temporarily create service disruptions to the user's account. The user can contact the administrator for assistance to restore the account.

Consider another scenario where Adam has accessed a network from a new device and from a new IP for the first time. You can contact Adam asking to confirm if he identifies this activity. If so, it might be that Adam has changed his working device and is working from his home network. This activity does not cause any harm to your organization's security, and can be ignored. However, if the user did not perform this activity, it is likely that the account has been compromised. In this scenario, you can lock the user's account to prevent any further damage.

Key features

Continuous risk assessment automates some of the functionalities associated with policies and visibility dashboards:

Support multiple conditions

When you create or modify a policy, you can add up to four conditions. The conditions can contain combinations of default risk indicators and custom risk indicators, user risk scores, or both.

For more information, see What are policies.

Notify users before applying actions

Before applying an appropriate action on a user's account, you can notify the user and assess the nature of an unusual activity that has been detected.

For more information, see Request end user response.

Notify users after applying actions

For some activities, awaiting user response before applying an action can put the user's account and your organization's security at risk. In such scenarios, you can apply a disruptive action when you detect an unusual activity, and notify the user about the same.

For more information, see Notify user after applying disruptive action.

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

Enforcement and monitor modes

You can set policies to enforcement or monitor modes based on your requirements. Policies in enforcement mode have a direct impact on users' accounts. However, if you want to assess the impact or the outcome of your policies before implementing them, you can set your policies to monitor mode.

For more information, see Supported modes.

Visibility into access and policy dashboards

Using the **Access Summary** dashboard, you can gain insights into the number of access attempts made by users. For more information, see Access Summary.

Using the **Policies and Actions** dashboard, you can gain insights into the policies and actions applied on user accounts. For more information, see Policies and Actions.

Default policies

Citrix Analytics introduces pre-defined policies that are enabled on the **Policies** dashboard by default. These policies are created by using risk indicators and user risk scores as the pre-defined conditions. A global action is assigned to every default policy.

NOTE

The policies listed in your environment might vary depending on when you first started using Citrix Analytics, and whether you have made any local changes.

For more information, see What are policies.

You can use the following default policies or modify them based on your requirements:

POLICY NAME	CONDITION	DATA SOURCE	ACTION
Successful credential exploit	When the Excessive authentication failures and Suspicious logon risk indicators are triggered	Citrix Gateway	Lock user

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

POLICY NAME	CONDITION	DATA SOURCE	ACTION
Potential data exfiltration	When the Potential data exfiltration risk indicator is triggered	{{page.cvad-and-daas-product-name}}	Log off user
Unusual access from a suspicious IP	When the Suspicious logon and Logon from suspicious IP risk indicators are triggered	Citrix Gateway	Lock user
First time access from device	When the CVAD-First time access from new device risk indicator is triggered	{{page.cvad-and-daas-product-name}}	Request end user response
Impossible travel on access	When the Impossible Travel risk indicator is triggered.	{{page.cvad-and-daas-product-name}}	Request end user response
Impossible travel on authentication	When the Impossible Travel risk indicator is triggered.	Citrix Gateway	Request end user response

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

Policies and actions

NOTE

Attention: Citrix Content Collaboration™ and ShareFile has reached its end of life and is no longer available to users.

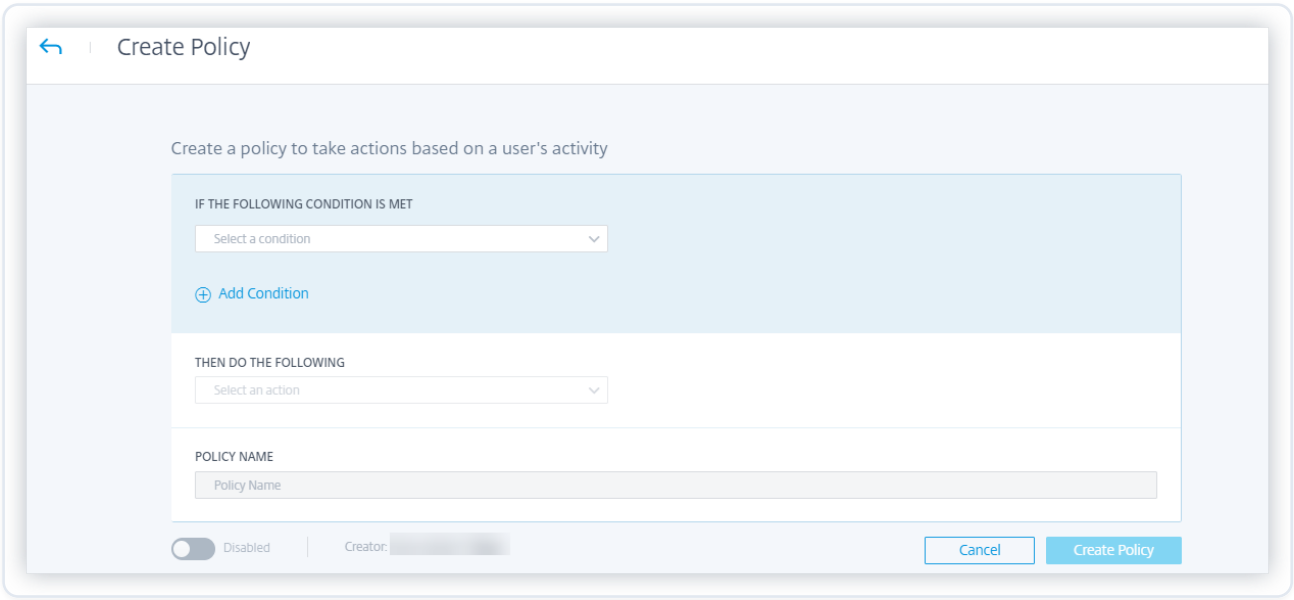
You can create policies on Citrix Analytics to help you perform actions on user accounts when unusual or suspicious activities occur. Policies let you automate the process of applying actions such as disabling a user and adding users to a watchlist. When you enable policies, a corresponding action is applied immediately after an anomalous event occurs and the policy condition is met. You can also manually apply actions on user accounts with anomalous activities.

What are the policies?

A policy is a set of conditions that must be met to apply an action. A policy contains one or more conditions and a single action. You can create a policy with multiple conditions and one action that can be applied to a user's account.

Risk score is a global condition. Global conditions can be applied to a specific user for a specific data source. You can keep a watch on user accounts that show any unusual activities. Other conditions are specific to data sources and their risk indicators. The conditions contain combinations of risk scores, default risk indicators, and custom risk indicators. You can add up to 4 conditions when creating a policy.

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



For example, if your organization uses sensitive data, you might want to restrict the amount of data shared or accessed by users internally. But if you have a large organization, it wouldn't be feasible for a single administrator to manage and monitor many users. You can create a policy wherein, anyone who shares sensitive data excessively can be added to a watchlist or have their account disabled immediately.

Default policies

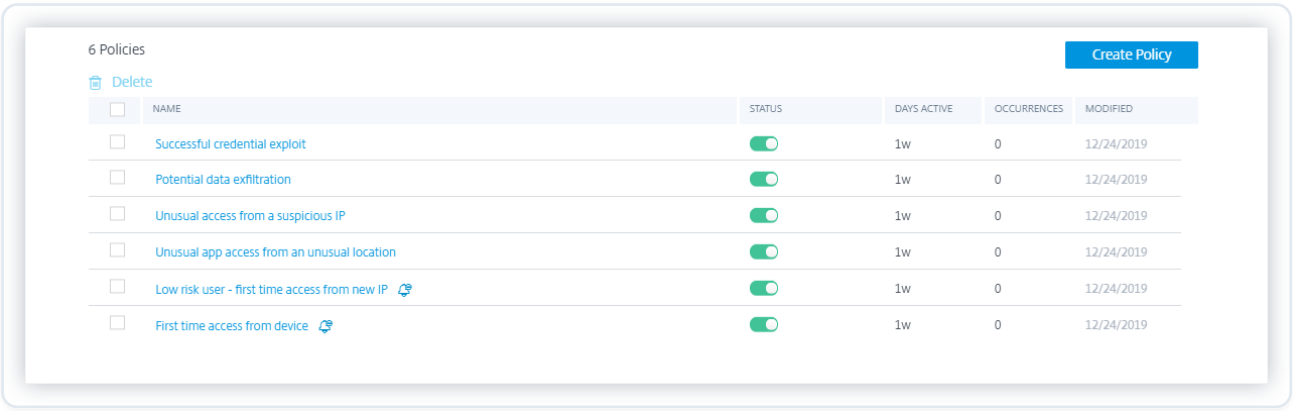
Default policies are predefined and enabled on the **Policies** dashboard. They are created based on pre-defined conditions and a corresponding action is assigned to every default policy. You can either use a default policy or modify it based on your requirements.

Citrix Analytics supports the following default policies:

- Successful credentials exploit
- Potential data exfiltration
- Unusual access from a suspicious IP
- First time access from device
- Virtual Apps and Desktops and Citrix DaaS- Impossible travel on access
- Gateway - Impossible travel on authentication

For information about the preset conditions and actions regarding the preceding default policies, see Continuous risk assessment.

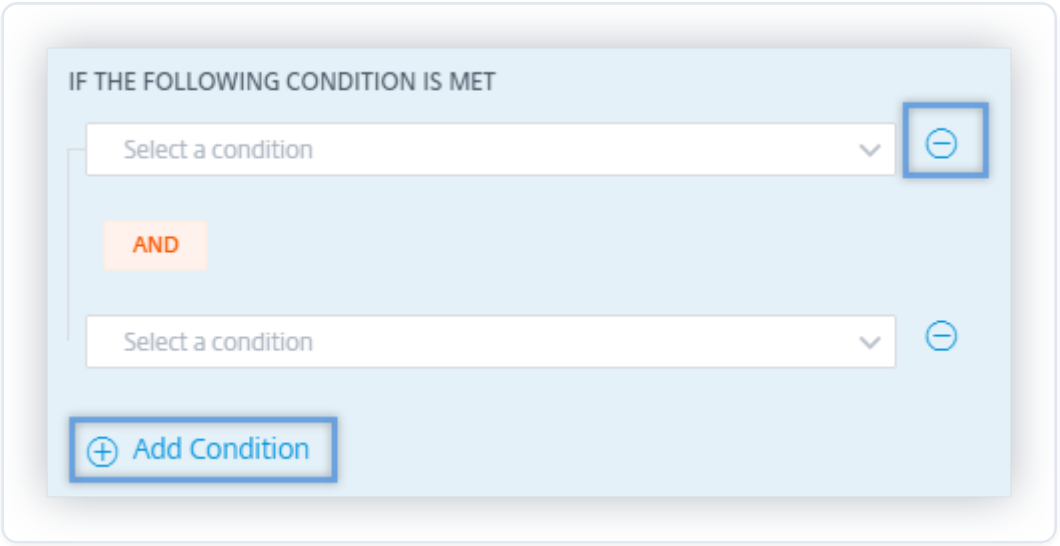
© 1997–2026 Citrix Systems, Inc. All rights reserved.



For information about the pre-defined policy for the geofencing use case, see Preconfigured policy.

How to add or remove conditions?

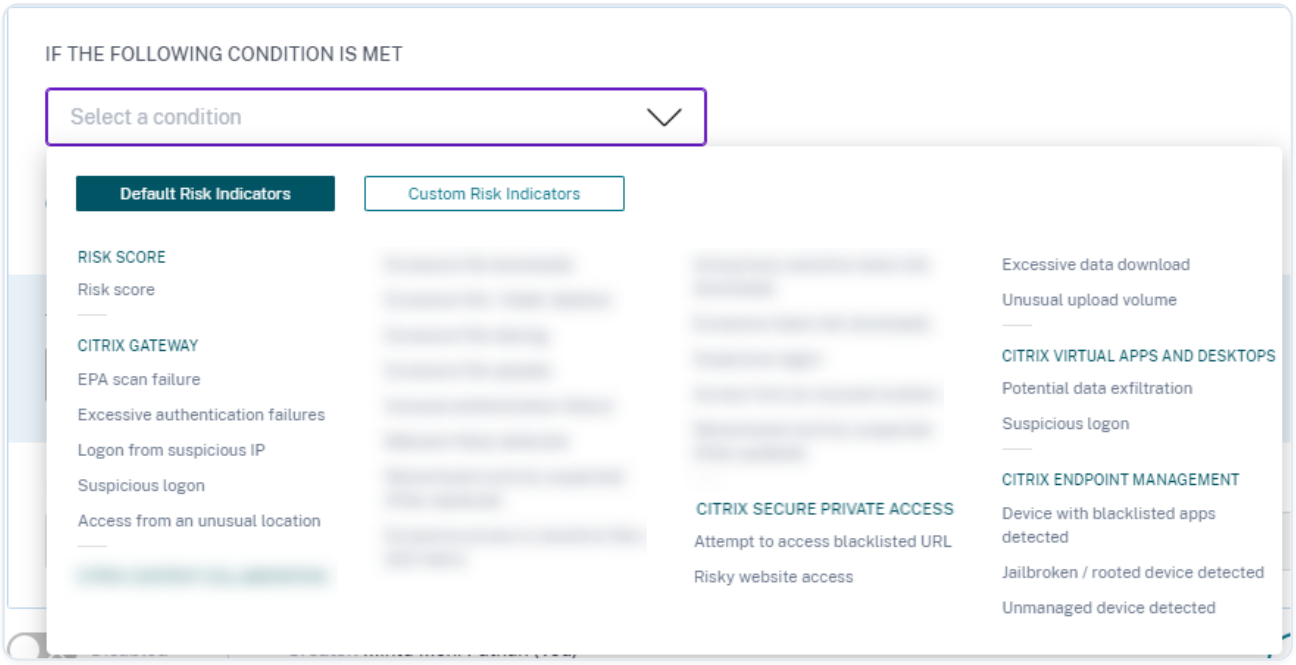
To add more conditions, select **Add condition** in the **IF THE FOLLOWING CONDITION IS MET** section of the **Create Policy** page. To remove a condition, select the **-** icon that is displayed next to the condition.



Default and custom risk indicators

The conditions menu is segregated based on **Default Risk Indicators** and **Custom Risk Indicators** tabs on the **Create Policy** page. Using these tabs, you can easily identify the type of risk indicator that you want to choose when selecting a condition for policy configuration.

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



What are the actions?

Actions are responses to suspicious events that prevent future anomalous events from occurring. You can apply actions on user accounts that display unusual or suspicious behavior. You can either configure policies to apply action on the user's account automatically or apply a specific action manually from the user's risk timeline.

You can view global actions or actions for each Citrix data source. You can also disable previously applied actions for a user at any time.

NOTE

Irrespective of the data source that triggers a risk indicator, actions pertaining to other data sources can be applied.

The following table describes the actions that you can take.

ACTION NAME	DESCRIPTION	APPLICABLE DATA SOURCES
Global actions		
Add to watchlist	When you want to monitor a user for future potential	All data sources

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

ACTION NAME	DESCRIPTION	APPLICABLE DATA SOURCES
	threats, you can add them to a watchlist.	
	The **Users in Watchlist** pane displays all the users that you want to monitor for potential threats based on the unusual activity on their account. Based on your organization's policy, you can add a user to the watchlist using the Add to watchlist action.	
	To add a user to the watchlist, navigate to the user's profile, from the **Actions** menu, select **Add to watchlist**. Click **Apply** to enforce the action.	
Notify administrator(s)	When a risk indicator is triggered for a user, you can manually notify to the administrators or create a policy for automatic notification. You can select the administrators from the Citrix Cloud domain and other non-Citrix Cloud domains in your organization. If you are a Citrix Cloud administrator with full access permissions, by default, the email notifications are disabled for your Citrix Cloud account. To receive email notifications, enable it on your Citrix Cloud account. For more information, see Receive emailed notifications. If you	

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

ACTION NAME	DESCRIPTION	APPLICABLE DATA SOURCES
	are a Citrix Cloud administrator with custom access permissions (read-only and full access) to manage Security Analytics, the email notifications are enabled for your Citrix Cloud account. To stop receiving email notifications from Citrix Analytics, request your Citrix Cloud full access administrator to remove your name from the notify administrators distribution list. For information about, see Email distribution list.	
Request end user response	When there is any unusual or suspicious activity on the user's account, you can notify the user to confirm if the user identifies the activity. Based on the activity, you can determine the next course of action to be taken on the user's account. For more information, see Request end user response.	
Notify End User	When any unusual or suspicious activity occurs on the user’s account, you can notify the end user via an email notification. For more information, see Notify End User.	
Citrix Gateway actions		

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

ACTION NAME	DESCRIPTION	APPLICABLE DATA SOURCES
Log off active sessions	When the action is applied, it logs off the user session that is currently active. It does not block any future user sessions.	Citrix Gateway on-premises and Citrix Application Delivery Management
Lock user account	When a user's account is locked due to anomalous behavior, they cannot access any resource through Citrix Gateway until the Gateway administrator unlocks the account.	Citrix Gateway on-premises
Unlock user account	When a user's account is accidentally locked although anomalous behavior was not detected, you can apply this action to unlock it and restore access to the account.	Citrix Gateway on-premises
Citrix Virtual Apps and Desktops™ and Citrix DaaS actions		
Log off active sessions	When the action is applied, it logs off the user session that is currently active. It does not block any future user sessions.	Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)
Start session recording	If there is an unusual event on the user’s Virtual Desktops account, the administrator can begin recording the user’s current active sessions. If the user is on Citrix Virtual Apps and Desktops 7.18 or a later version, and logged in to the	Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)

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

ACTION NAME	DESCRIPTION	APPLICABLE DATA SOURCES
	virtual session, an administrator can dynamically trigger start session recording action from Citrix Analytics for Security that starts the recording of the user's current active session.	

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

Preconfigured custom risk indicators and policies

Citrix Analytics for Security provides a list of preconfigured custom risk indicators and a policy to help you monitor the security of your Citrix infrastructure. The conditions of these preconfigured custom risk indicators and the policy are already defined according to specific security risk scenarios such as compromised users, insider threats, and data exfiltration. You can also modify these preconfigured conditions or add your own conditions according to your security requirements and use the custom risk indicators to mitigate the risks.

Currently, the preconfigured custom risk indicators are available for the following scenarios:

- Geofencing
- First time access

Preconfigured custom risk indicators for the geofencing scenario

Use the following pre-configured custom risk indicators to detect user events from outside the geofenced areas.

- CVAD-Session started outside of geofence
- GW-Geofence crossing

The preconfigured custom risk indicators are triggered whenever users access the Citrix® products from outside their usual country of operation or the geofence. By default, the geofence is set to "United States". You can set your required country as a geofence.

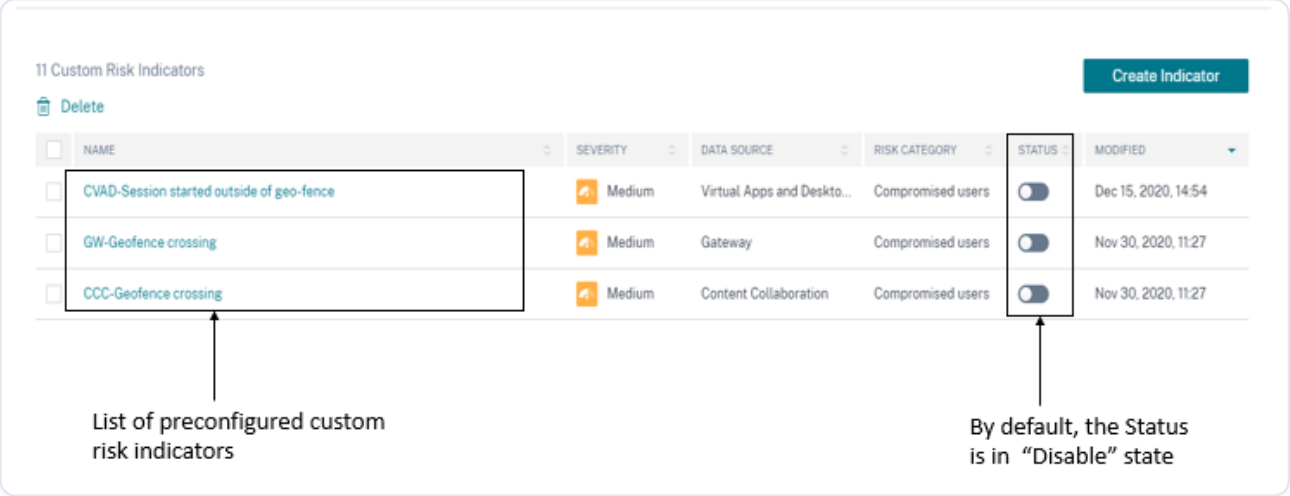
NOTE

The *CVAD-Session started outside of geofence* risk indicator is linked to the **Geofence Settings** of the Access Assurance Location feature. So, you cannot directly modify the geofenced countries in the condition of the risk indicator. To update the geofenced countries in the risk indicator, select the countries in the **Geofence Settings** of the Access Assurance Location dashboard. For more information, see the Access assurance location dashboard.

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

To view the preconfigured custom risk indicators, select **Security > Custom Risk Indicators**.

By default, the preconfigured custom risk indicators are disabled. Use the **STATUS** button to enable them.



The following table describes the various preconfigured custom risk indicators for geofencing.

CUSTOM RISK INDICATOR NAME	SCENARIO	CUSTOM INDICATOR CONDITIONS	DATA SOURCE	RISK CATEGORY
CVAD-Session started outside of geofence	User has started a virtual session outside their country of operation	Event-Type = Session.logon Country != "United States"	Citrix Workspace app	Compromised users
GW-Geofence crossing	User has successful authentication from outside their country of operation	Event-Type = "VPN_AI" AND Country != "United States"	Citrix Gateway (on-premises)	Compromised users

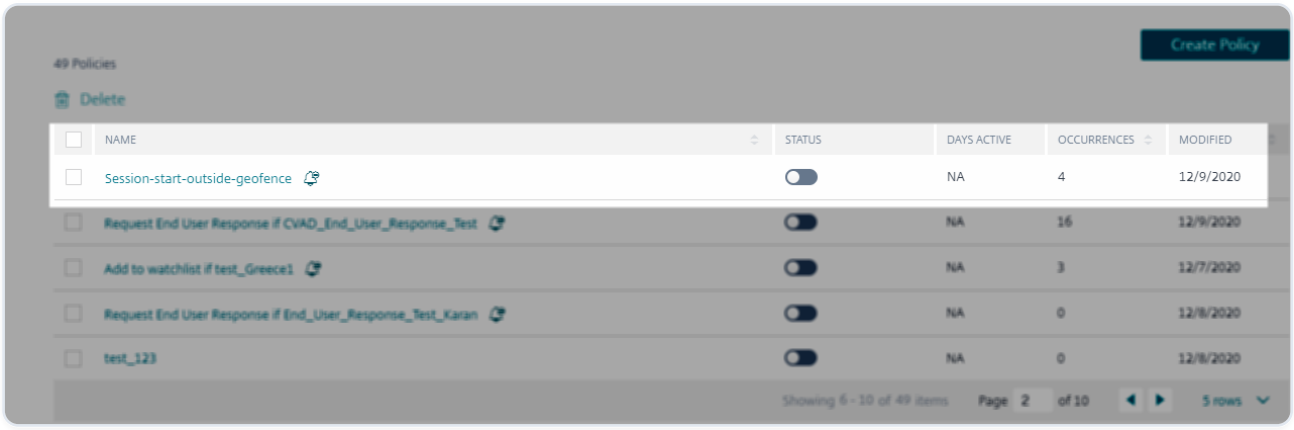
Preconfigured policy for the geofencing scenario

Citrix provides a preconfigured policy that applies the **Request End User Response** action to a user account whenever the user starts a virtual session from outside their country of operation. The user receives an email and based on the user's response, an appropriate action is taken such as

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

adding the user to the watchlist or notifying the administrator for further action. For more information, see Request end user response.

To view the preconfigured policy, select **Security > Policies**.



The following table describes the preconfigured policy for geofencing.

POLICY NAME	SCENARIO	POLICY CONDITION	APPLIED ACTION
Session start outside of geofence	Ability for an administrator to validate the user's legitimacy through the 'Request End-user Response' action when the user starts the virtual session outside their country of operation	Use with preconfigured custom risk indicator- "CVAD-Session started outside of geofence"	Request End-User Response
			Based on the following user's response, the corresponding action is applied
			If the user does not recognize the activity: **Add to watchlist**
			If the user recognizes the

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

POLICY NAME	SCENARIO	POLICY CONDITION	APPLIED ACTION
			activity: **No action required**
			If the user does not respond within 60 minutes of receiving the email: **Add the user to the watchlist**

NOTE

The **Request End User Response** action is supported only in the United States region. So, if your organization is onboarded to the European Union region in Citrix Cloud™, the preconfigured policy does not get applied to your account. To use the preconfigured policy, modify the policy and select another action of your choice.

Create your own policy with preconfigured custom risk indicators for geofencing

You can also create your own policies with these preconfigured custom risk indicators and apply actions such as locking users or logging off users whenever the indicators are triggered. For information on how to create policies, see Configure policies and actions.

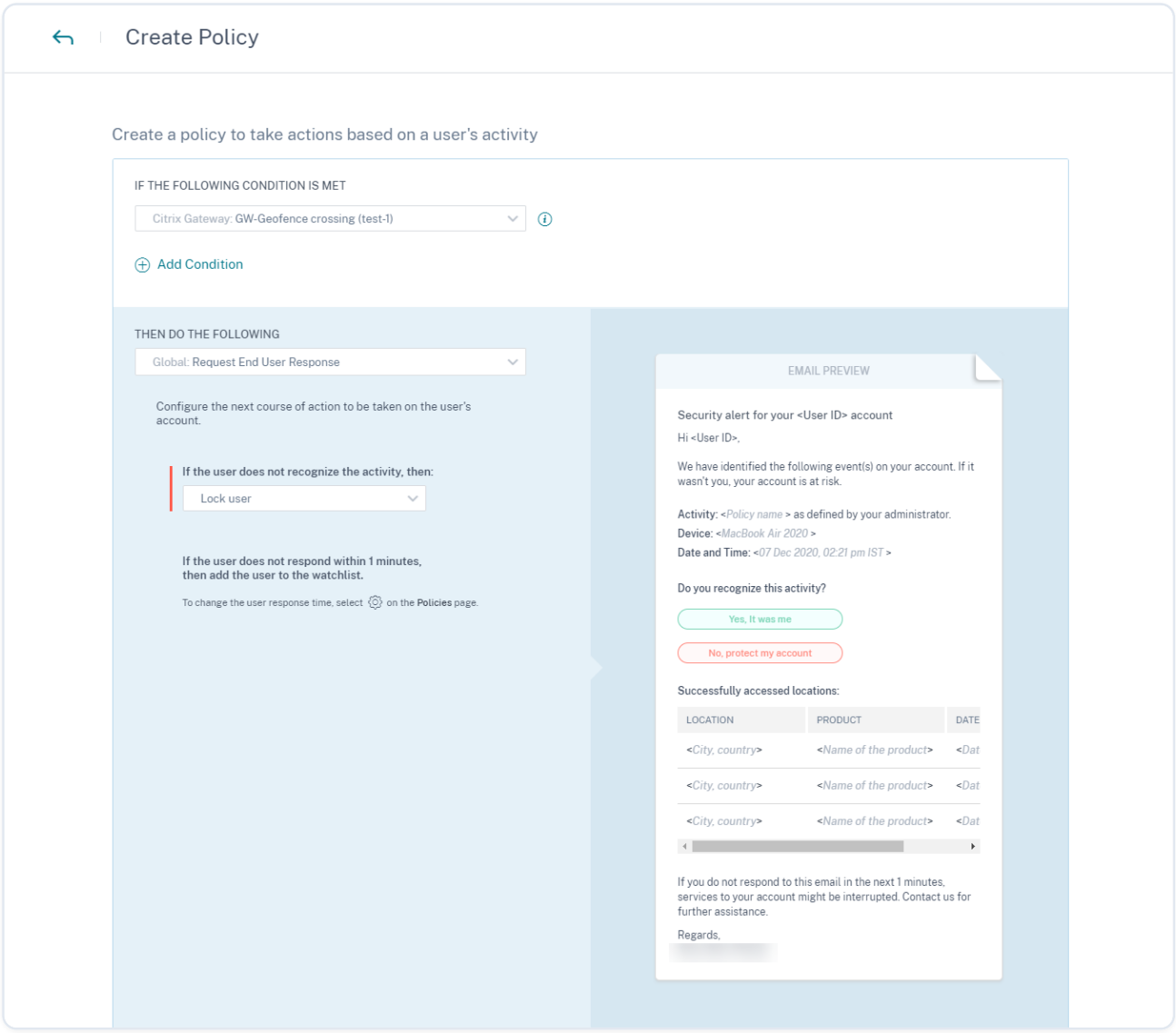
The following example shows a policy that locks users who try to access Citrix services from outside the United States. The user access is locked if the user does not recognize their access activity.

Condition: GW-Geofence crossing

Action: Request end user response

Next action: Lock the user if the user does not recognize the activity

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



NOTE

The **Request End User Response** action is supported only in the United States region. So, if your organization is onboarded to the European Union region, select another action of your choice instead of the **Request End User Response** action.

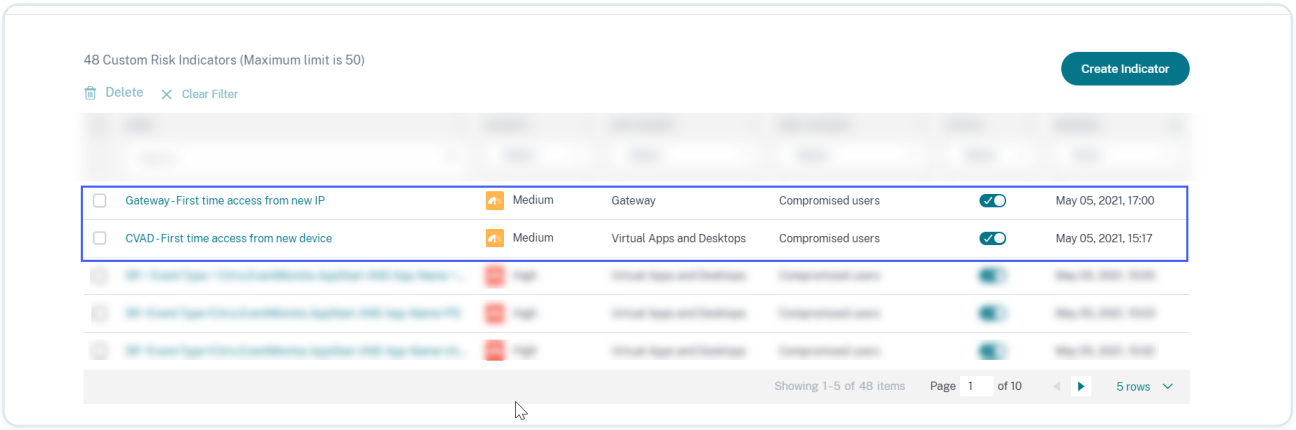
Preconfigured custom risk indicators for the first time access scenario

Use the following custom risk indicators to detect the user events for the first-time access scenarios:

- CVAD-First time access from new device
- Gateway-First time access from new IP

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

By default, these preconfigured custom risk indicators are in the enabled state. Use the **STATUS** button if you want to disable them.



The following table describes the preconfigured custom risk indicators for first-time access.

CUSTOM INDICATOR NAME	SCENARIO	PRECONFIGURED CONDITIONS	DATA SOURCE	RISK CATEGORY
CVAD-First time access from new device	When a Citrix Workspace app user signs in from one of the following	The following conditions are enabled by default	{{page.cvad-onprem-product-name}} on-premises and {{page.daas-product-name}} (formerly Citrix Virtual Apps and Desktops service)	Compromised users
	A new device	The First time for a new Device-ID.		
	An existing device that has not been used for the last 90 days.	`Event-Type = "Session.Logon" AND Client-Type IN ("XA.Receiver.Windows", "XA.Receiver.Mac",`		

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

CUSTOM INDICATOR NAME	SCENARIO	PRECONFIGURED CONDITIONS	DATA SOURCE	RISK CATEGORY
		`"XA.Receiver.Chrome", "XA.Receiver.Android", "XA.Receiver.Linux", "XA.Receiver.iOS")`		
Gateway-First time access from new IP	When a Citrix Gateway user successfully signs from one of the following	The following conditions are enabled by default	Citrix Gateway	Compromised users
	A new public IP address	The First time for a new Client-IP		
	An existing public IP address that has not been used for the last 90 days.	`Event-Type = "Authentication" AND Status-Code = "Successful login" AND Client-IP-Type != "private" AND Access-Insight-Flags = 1`		

On the condition bar, you can also add your own conditions in addition to the preconfigured conditions to identify threats as per your requirements.

For example, if you want to identify the user events from a particular country, you can add the country dimension along with the preconfigured condition:

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

- `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.

End user email settings

The end user email settings control the email template associated with the global action Request End User Response. You apply this action to get a response from the users for any unusual activity detected in their account. The users respond through the emails they receive from Citrix Analytics for Security.

You can use the email settings to:

- Add an appropriate banner, header text, and footer text to attract the user's attention and get their response. It also makes your email look more legitimate.
- Add time duration (in minutes) within which the user must respond to your email. If the user does not respond within the response time, Citrix Analytics applies the specified action to the user.

Modify email settings

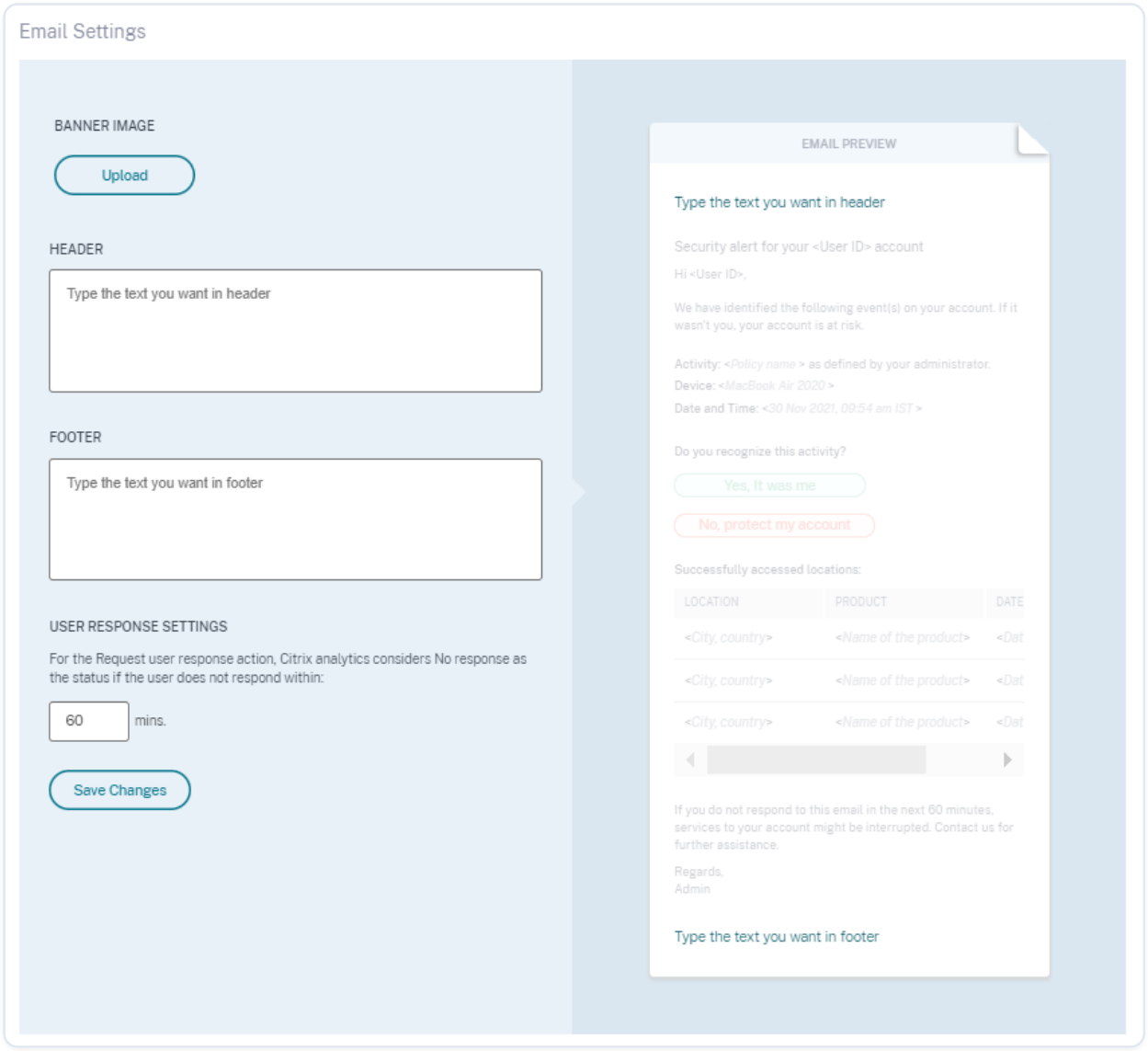
To modify the email settings:

1. On the top bar, click **Settings > Alert Settings > End User Email Settings**.



2. Click Edit to upload or browse a banner image. When uploading an image file, ensure that the image meets the following requirements:
    - Supported formats: JPEG or PNG
    - Maximum dimensions: 400* 100 pixels
    - Maximum file size: 5 MB
3. Enter your texts in the **HEADER** and the **FOOTER** fields. These fields are optional.
4. Enter the time in the user response settings.
5. Preview the email and click **Save Changes**.

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



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

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

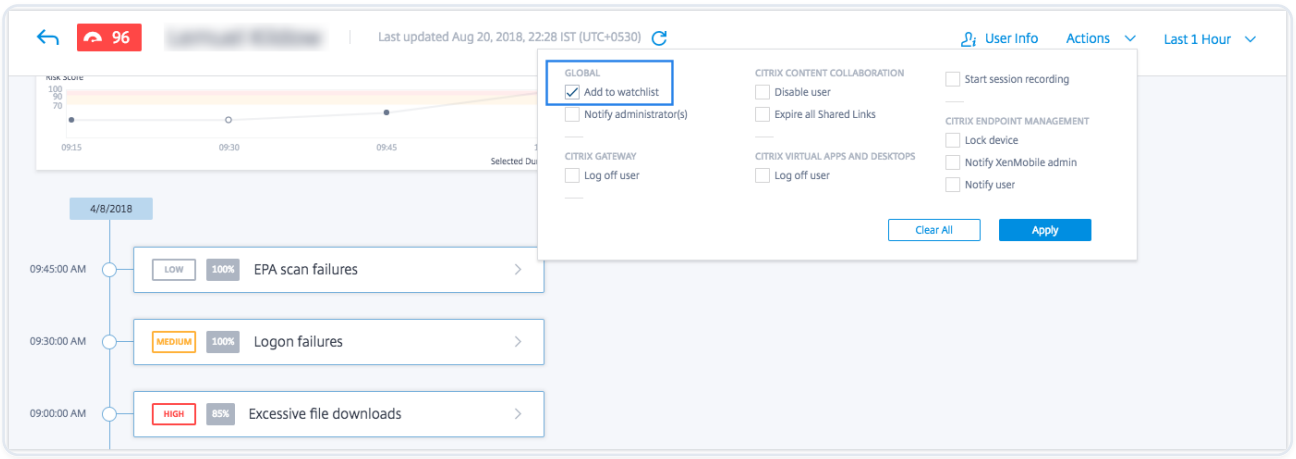
Watchlist

Use watchlists to monitor the activity of specific users for potential threats. For example, you can monitor users who are not full-time employees in your organization or users who trigger a specific risk indicator frequently.

How to add a user to the watchlist

You can either add a user to the watchlist manually, or you can define policies that when triggered adds a user to the watchlist.

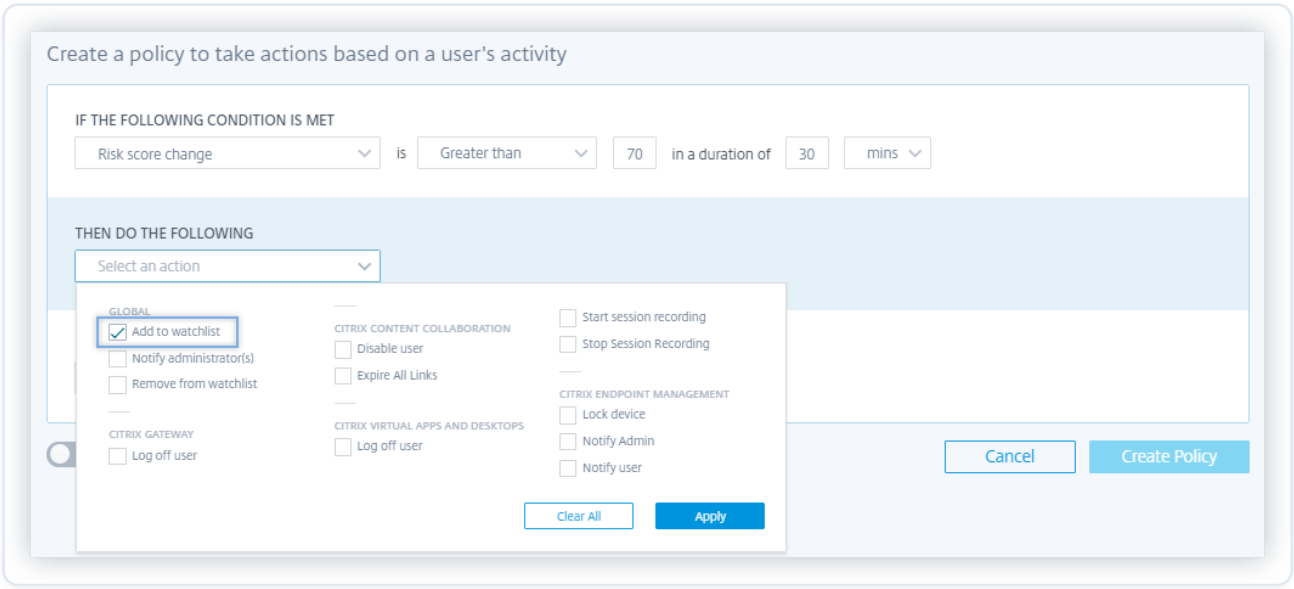
To add a user to the watchlist manually, navigate to the user's profile on the risk timeline. Then, from the **Actions** menu, select **Add to watchlist**. Click **Apply** and follow the prompts to enforce the action.



To add a user to the watchlist using policies, create a policy with a set of conditions that must be met. Select the **Add to watchlist** action. When the conditions are met, the user is added to the watchlist. For example, you might want to add a user to the watchlist if the user's risk score change is greater than 70 in 30 minutes.

For more information about creating policies, see Configure policies and actions.

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



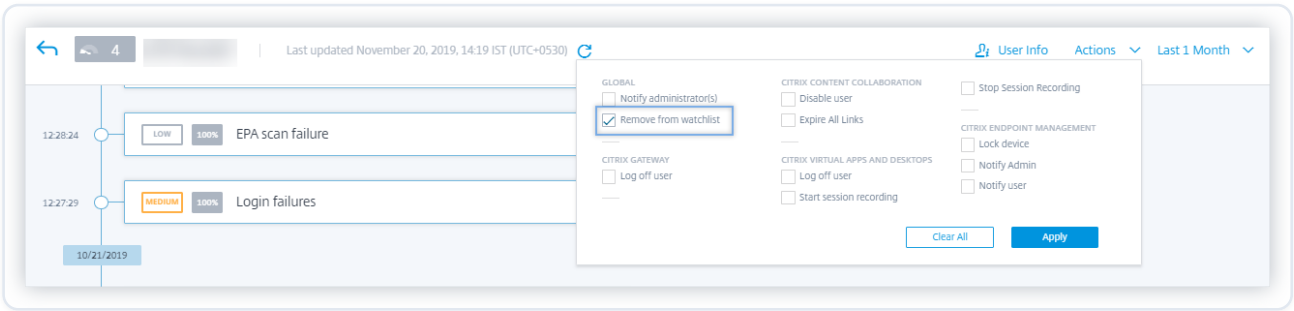
How to remove a user from the watchlist

You can either remove a user from the watchlist manually, or you can define policies that when triggered removes a user from the watchlist.

To remove a user from the watchlist manually, navigate to the user's profile on the risk timeline. Then, from the **Actions** menu, select **Remove from watchlist**. Click **Apply** and follow the prompts to enforce the action.

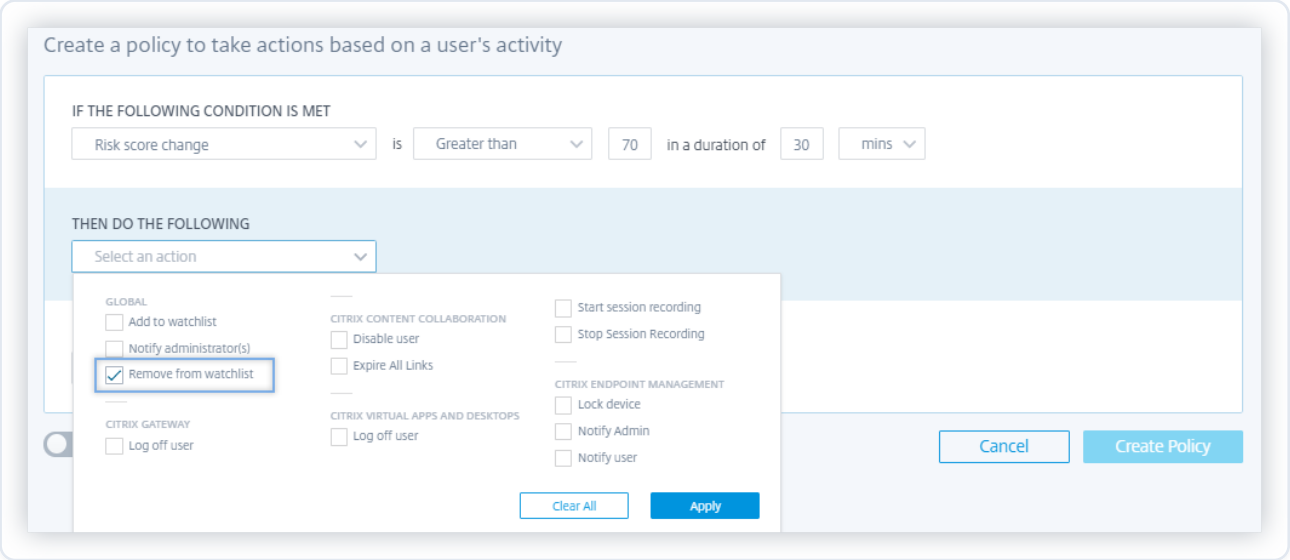
NOTE

When a user is on the watchlist, and you want to remove them, you see the **Remove from watchlist** option in the **Actions** menu.



To remove a user to the watchlist using policies, create a policy with a set of conditions that must be met. Select the **Remove from watchlist** action. When the conditions are met, the user is removed from the watchlist. For example, you might want to remove a user from the watchlist if the user's risk score change is lesser than 70 in 60 minutes. To learn more about creating policies, see Configure policies and actions.

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



How to monitor users in a watchlist

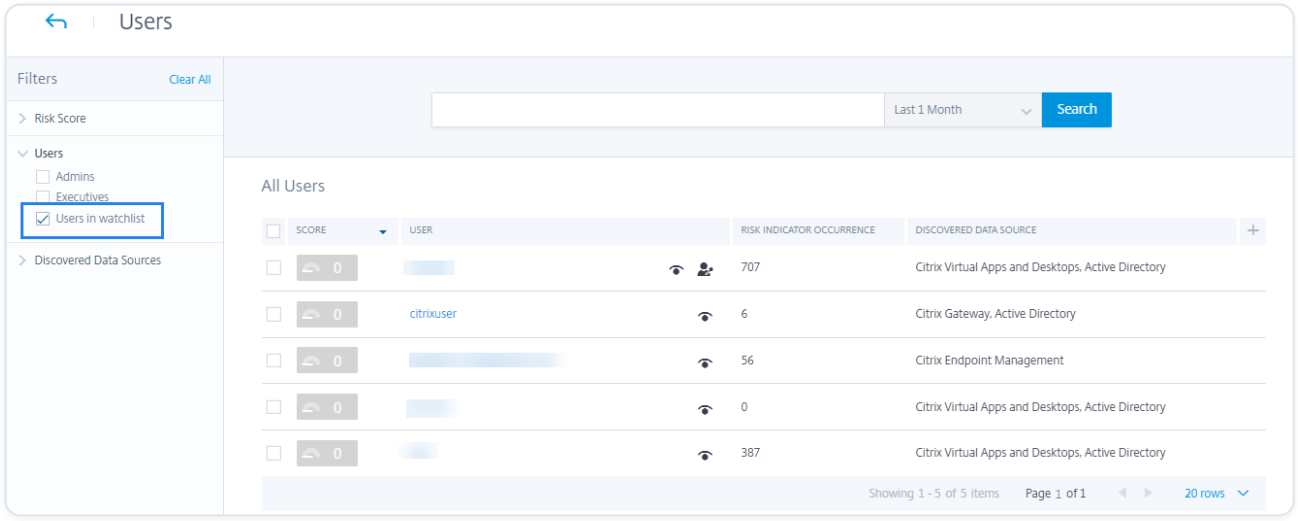
On the **Security > Users** dashboard, view the following:

- Summary of the number of users in the watchlist for the last 13 months. Click the box to view the list of all users in the watchlist on the **Users in Watchlist** pane.
- Top five users in the watchlist listed based on the risk score. In the **Users in Watchlist** pane, view the risk score, and risk indicator occurrences along with the name of the user. Click **See More** to view the list of all users in the watchlist on the **Users** page.
- Top risky users who are in the watchlist. In the **Risky Users** pane, the “eye” icon next to a user indicates that the user is in the watchlist.

On the **Users** page, view the list of all users in the watchlist. View details such as the risk score, number of risk indicators triggered, and associated data sources for a user.

Use the search box to find users and their event details. Select the time period to view the risk indicator occurrences for the specific period.

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



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

Weekly email notification

Citrix Analytics sends weekly email notifications summarizing the security risk exposures in your organization's IT infrastructure. The weekly notification keeps you aware and informed about the risky events and their occurrences in the previous week. You can find out if any events require your attention or actions without signing in to Citrix Analytics. This information keeps you informed about what is happening in your IT security domain.

Enable email notifications

- If you are a Citrix Cloud administrator with full or custom access permission, the email notifications are disabled by default in your Citrix Cloud account. To receive email notifications from any Citrix Cloud services such as Citrix Analytics, enable the notification option in your Citrix Cloud. For more information, see Receive emailed notifications. Notification preferences are not available for administrators who are added through Active Directory/Azure AD Groups.
- By default, the email notifications are sent to the Citrix Security Administrators - default list. You can change this by configuring custom distribution list recipients for weekly alerts. For more information, see Admin email settings.

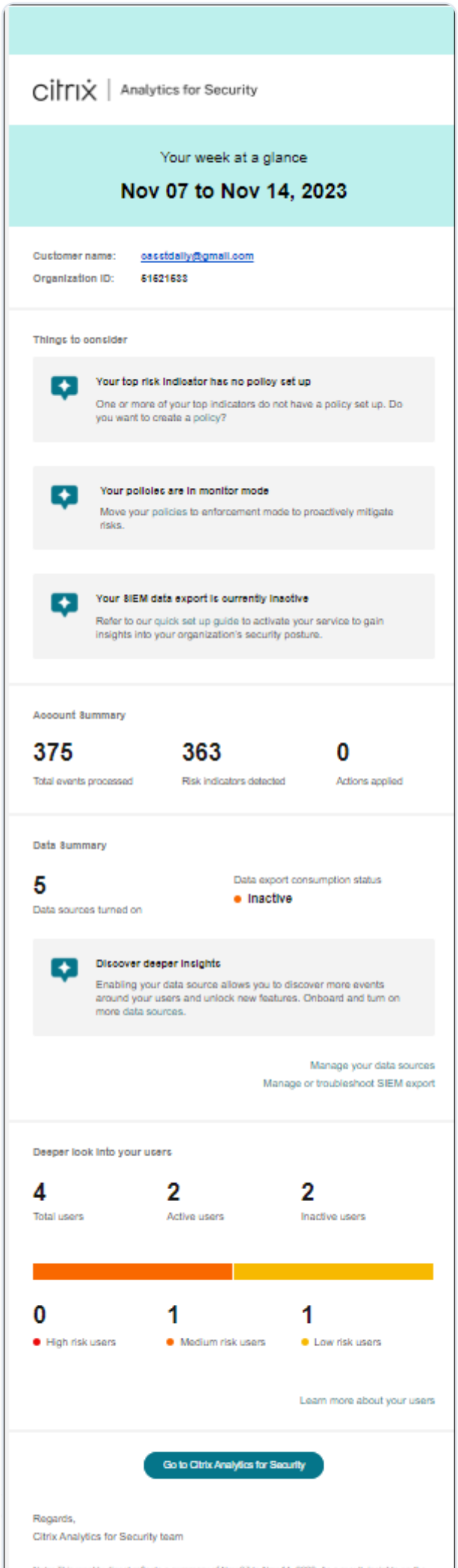
When do you get an email from Citrix Analytics?

Every Tuesday, an email notification is sent to you from Citrix Cloud mailto:donotreplynotifications@citrix.com.

The email notification provides the following information:

- Summary of the total number of events processed, risk indicators detected, and the actions applied
- Summary of the total number of active data sources and the data export consumption status
- Top three risk indicators
- Top three actions taken on the risk indicators
- Total number of active users and total number of risky users
- Any events or actions that require your attention

© 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

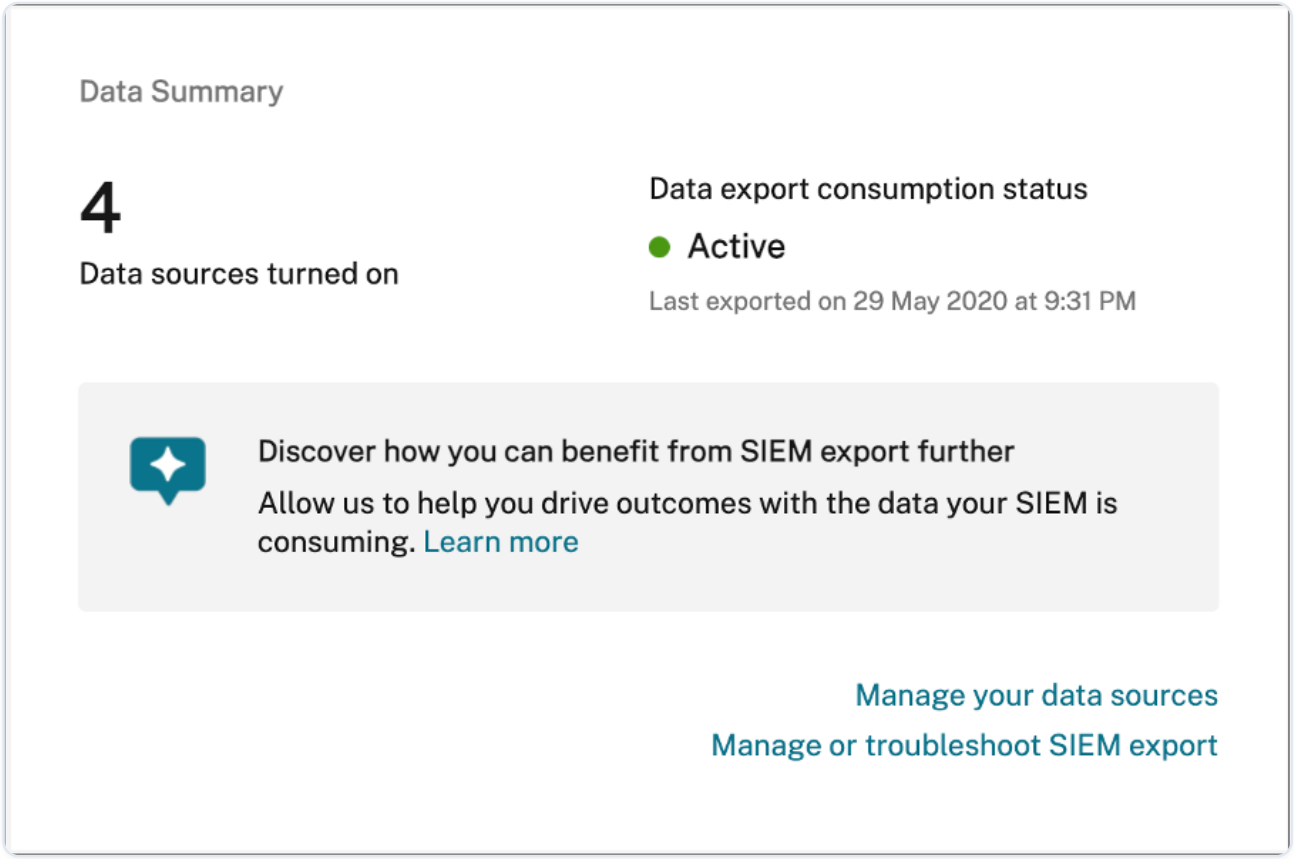
Account Summary

The weekly email provides a summary of the total number of events processed, risk indicators detected, and the actions applied.



Data Summary

The weekly email also provides insights on the data sources that have been turned on along with the data export consumption status.



Click **Manage your data sources** on the email to view the **Data Sources** page in Citrix Analytics. You can onboard the data source and turn on data processing to enable Citrix Analytics to allow the processing of data. For more information on enabling analytics, see Enable Analytics on data sources.

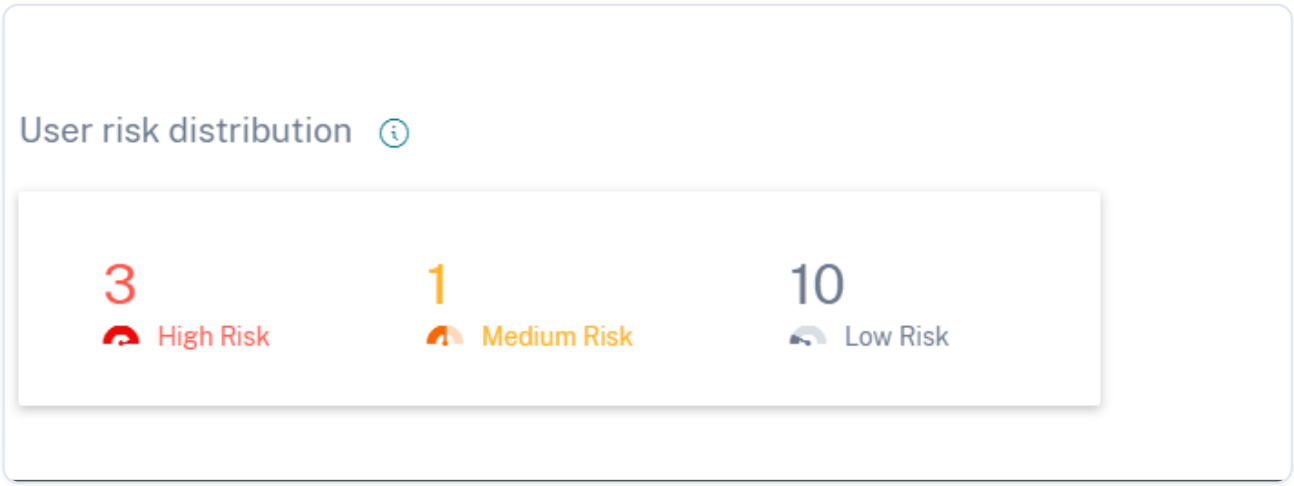
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Click **Manage or troubleshoot SIEM export** to view the Data Exports page in Citrix Analytics to troubleshoot your environment and manage your data export settings.

Users information

The weekly email provides insights into the total number of users and users who have acted in a risky manner.

- **Number of High risk users** – Identified in red. They represent an immediate threat to the organization.
- **Number of Medium risk** – Identified in orange. They have multiple serious violations on their account for the selected week and they must be monitored closely.
- **Number of Low risk users** – Identified in yellow. They have a few serious violations on their account, but potentially they are not considered a threat.



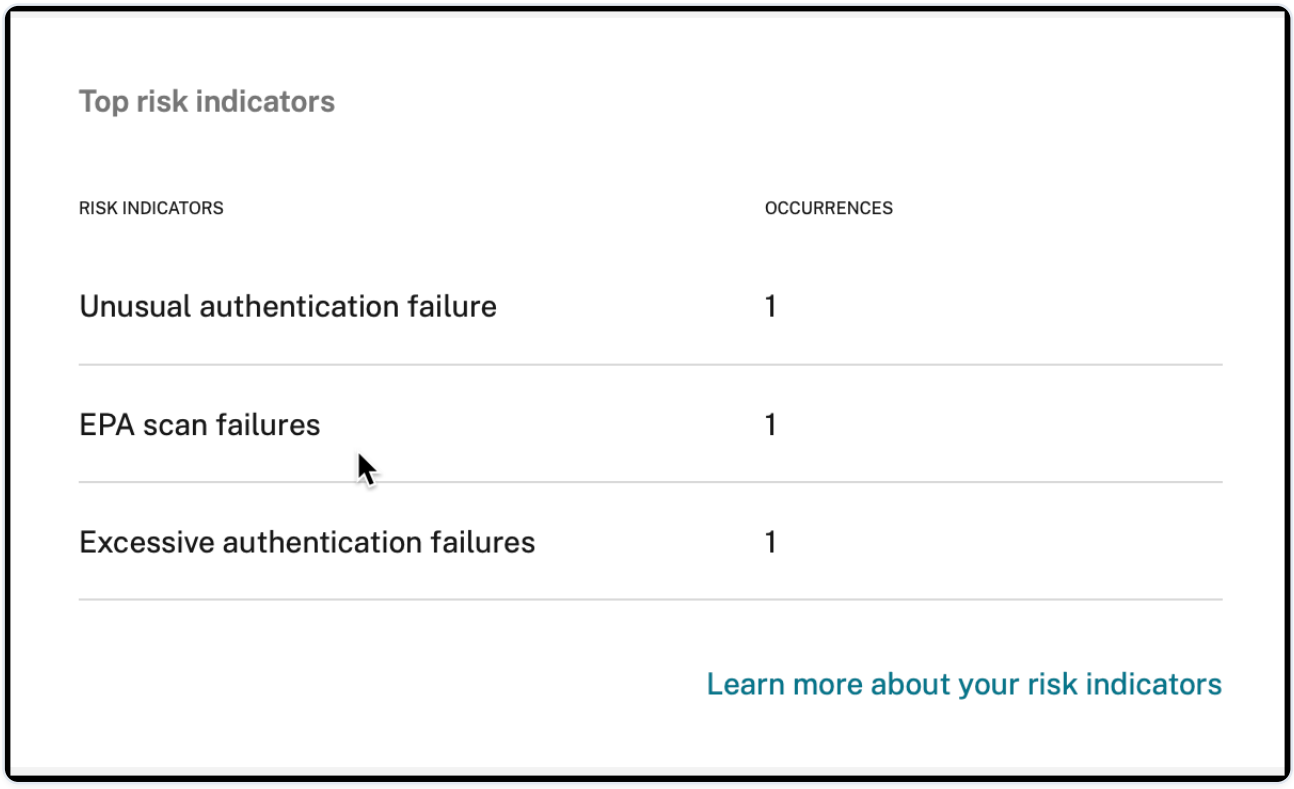
For more information, see risky users.

Click **Learn more about your users** to view the **Risky Users** page in Citrix Analytics. You can get deeper insights into the active users and the risk categorization.

Top Risk Indicators

The weekly email provides insights on the top three risk indicators and the number of occurrences for the selected week. Depending on the number of occurrences, both the default and custom risk indicators for the selected week are displayed.

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



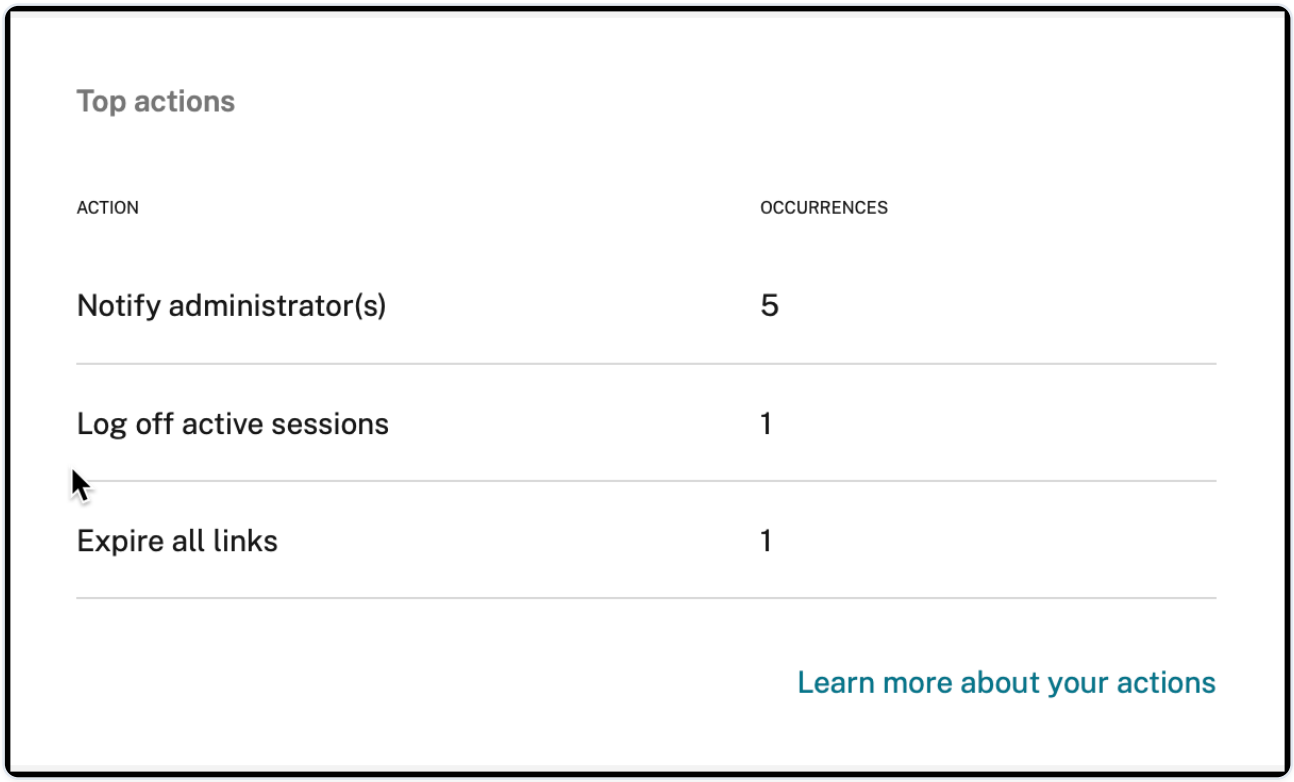
For more information, see risk indicators.

Click **Learn more about your risk indicators** on the email to view the **Risk Indicator Overview** page in Citrix Analytics.

Top Actions

The weekly email provides insights on the top three actions taken in response to the suspicious and anomalous threats that occurred in the last week. Depending on the number of occurrences, both Global actions and Citrix Gateway actions for the selected week are displayed.

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



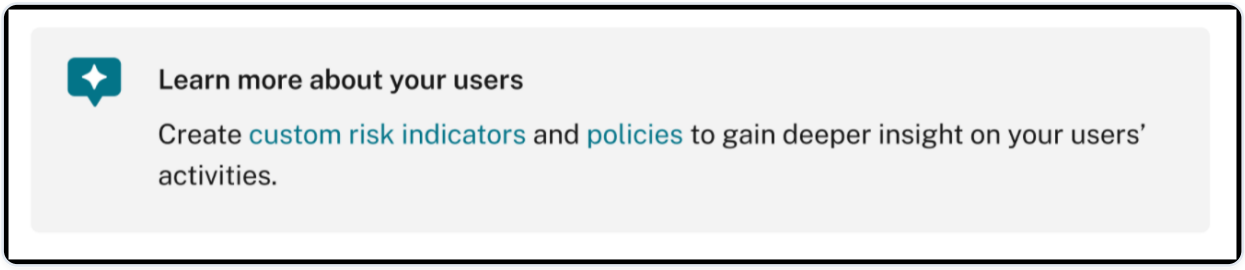
For more information on actions, and configuring an action, see policies and actions.

Click **Learn more about your actions** on the email to view the **Top Actions** page in Citrix Analytics.

What action do you need to take after receiving the email?

Weekly emails enable you to find out if any events or actions require your attention.

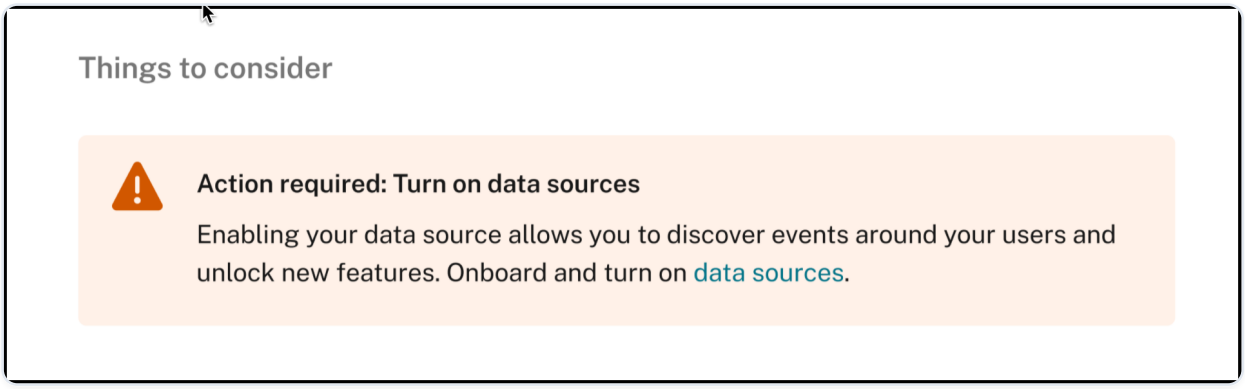
- If there are no risk indicators detected for the week, you get the following message which prompts you to create more custom risk indicators.



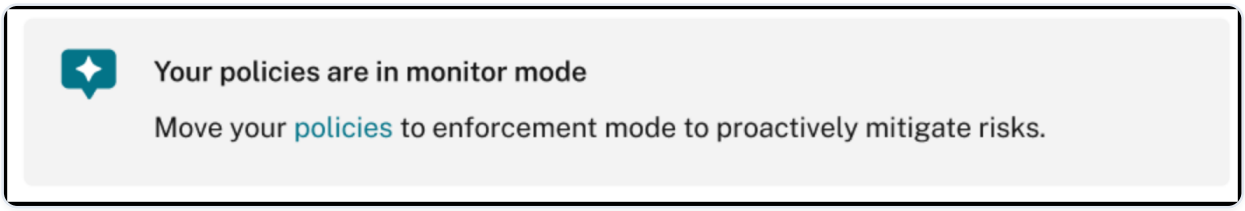
You can log in to Citrix Analytics to create more custom risk indicators.

- If none of the data sources are turned on in Security Analytics you get the following message which prompts you to turn on data processing for the data sources.

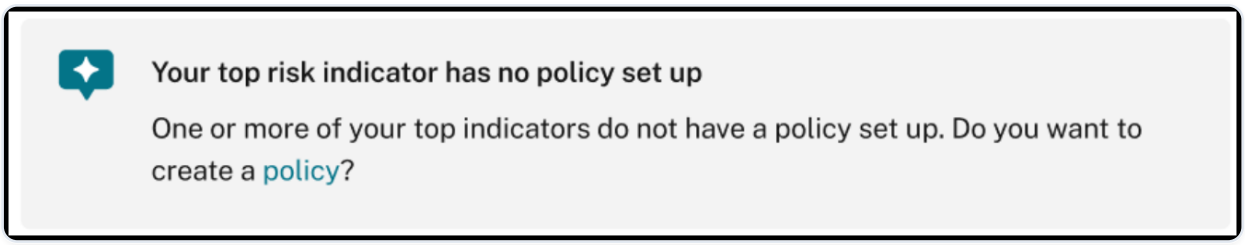
© 1997–2026 Citrix Systems, Inc. All rights reserved.



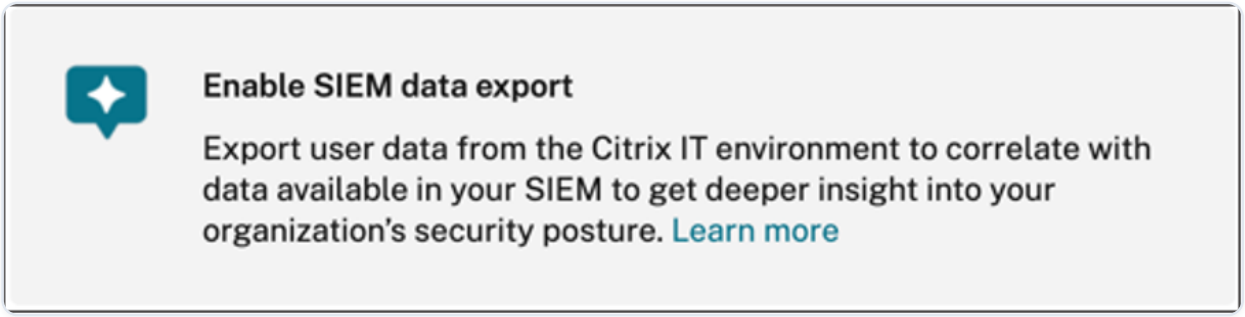
- If none of Policies are in monitor mode, you get the following message which prompts you to move the policies to enforcement mode.



- If there is no policy set up for any of the top 3 risk indicators for the week, you get the following message which prompts you to create a policy.



- If you have not enabled **Data Exports** for your Citrix Analytics tenant, the following recommendations point you to more details about our **Data Exports** options which allow you to export your Citrix data to a SIEM environment.



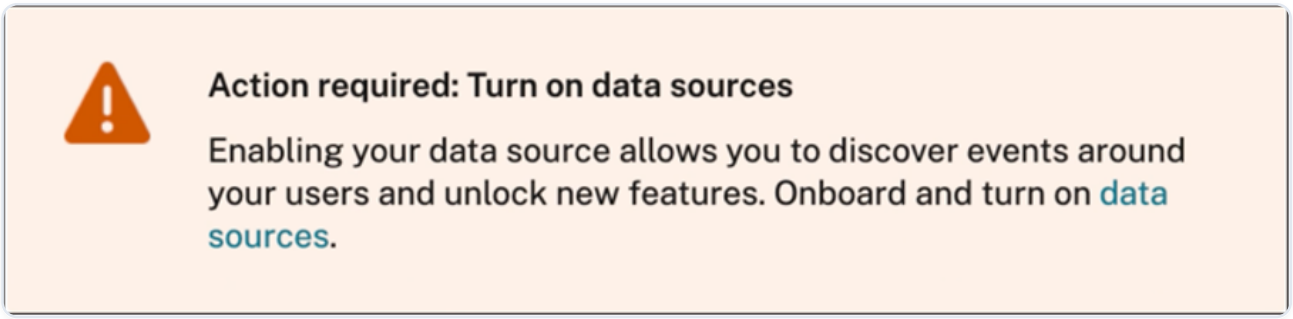
- If the data export consumption status is inactive, you get the following message which prompts you to activate your service.

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



NOTE

The data transmission is enabled only when the data processing is turned on at least for one data source. If the data processing is turned off for all the data sources, you get the following warning message to enable your data source.



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

Audit logs

An audit log describes audit information for events generated on Citrix Analytics. They can be system events such as errors, or an audit trail of configuration actions performed by the Citrix Analytics administrator.

Whenever a configuration is added, deleted, or updated, the event information is written to the audit log. This information is about what was modified, the time when it was modified, and who modified it.

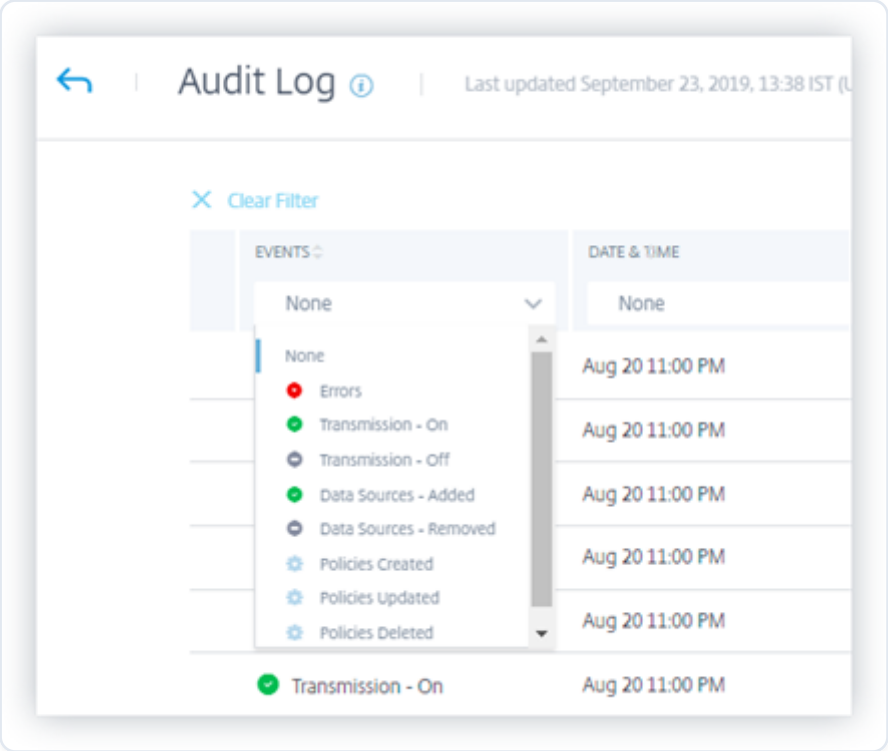
You can view audit log information for the last three months.

Activities that generate audit events

The following events are registered on Citrix Analytics:

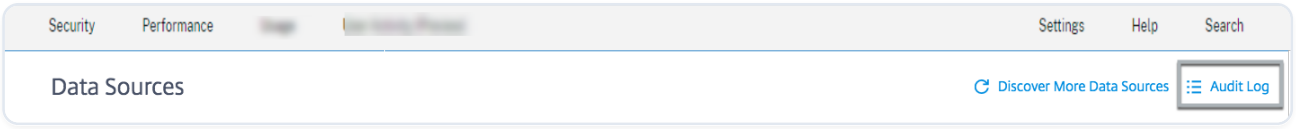
- Errors generated
- Transmission turned on
- Transmission turned off
- Data sources added
- Data sources removed
- Policies created
- Policies updated
- Policies deleted

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



How to view the audit log

To view audit logs, log on to Citrix Analytics. Navigate to **Settings > Data Sources**. On the **Data Sources** page, click **Audit Log** on the top right corner.



How to use the audit log

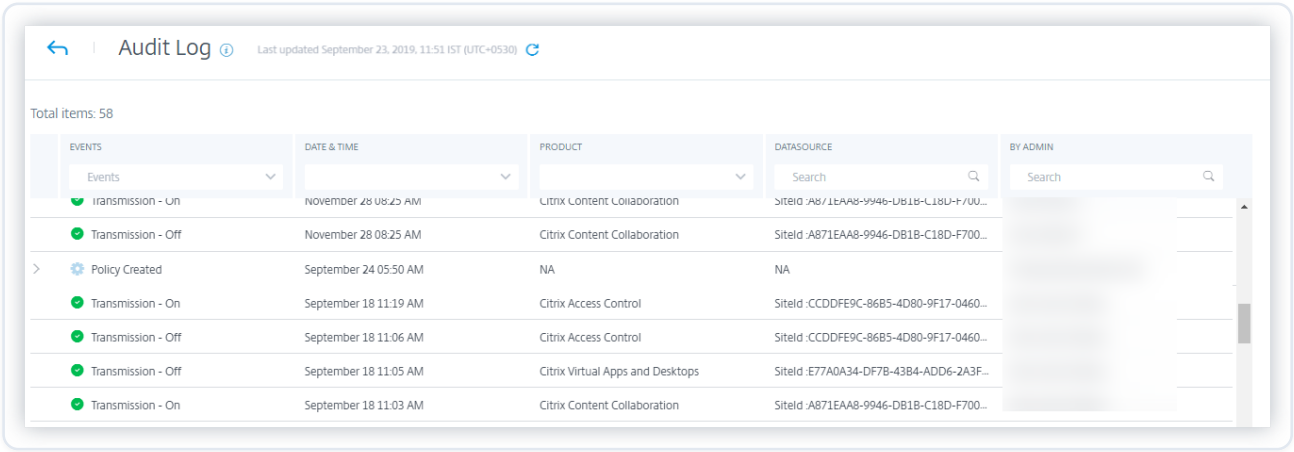
You can use the audit log to review and be aware of any event on Citrix Analytics. Refresh the **Audit Log** page to fetch the latest audit data. The page displays the date and time when the audit data was last updated.

You can view the following audit information on the **Audit Log** page. You can also filter the audit data based on these fields.

- **Events**. Events can be system generated or configurations applied by the administrator on Citrix Analytics. Events can also represent errors such as the failure to apply actions or a data source. By default, logs for all events are displayed. You can filter based on the type of event you want to view.

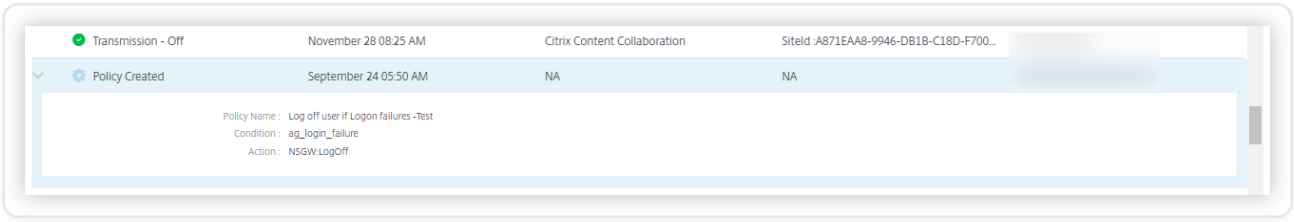
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Date and Time**. The data and time when the event occurred. You can filter based on the period for which you want to view the log. You can view events for the current day, last seven days, last 15 days, last month, and last three months.
- **Product**. The product for which the event was generated. The events are generated on the product and aggregated on Citrix Analytics where they are displayed. You can filter the log based on one or more products.
- **Data Source**. The name of the product instance associated with the audit entry. You can search for any specific data source to view its audit data.
- **By Admin**. The Citrix Analytics administrator who performed the admin activities. You can search for activities performed by any specific administrator.



If your registered event was based on a policy, you can click the arrow icon to view more details such as:

- Policy name
- The specified condition
- The resulting action



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

Custom reports

You can create and schedule custom reports using the events and insights available in Citrix Analytics for Security. Custom reports help you to extract information of specific interest and organize the data graphically. It helps analyze the security of the data source of your choice over time.

Custom reports support the following data sources:

- Apps and Desktops
- Gateway
- Secure Private Access
- Secure Browser
- Policies
- Risk Indicators
- Risk Score

Supported Fields in Custom Reports

Some data sources are also available in self-service search. To view these event types and supported fields, click the following data sources.

- Apps and Desktops
- Gateway
- Secure Private Access
- Secure Browser
- Policies

The following data sources are only available in Custom Reports. The following table lists the supported fields in the Custom reports for the following data sources:

- Risk Indicators
- Risk Score

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

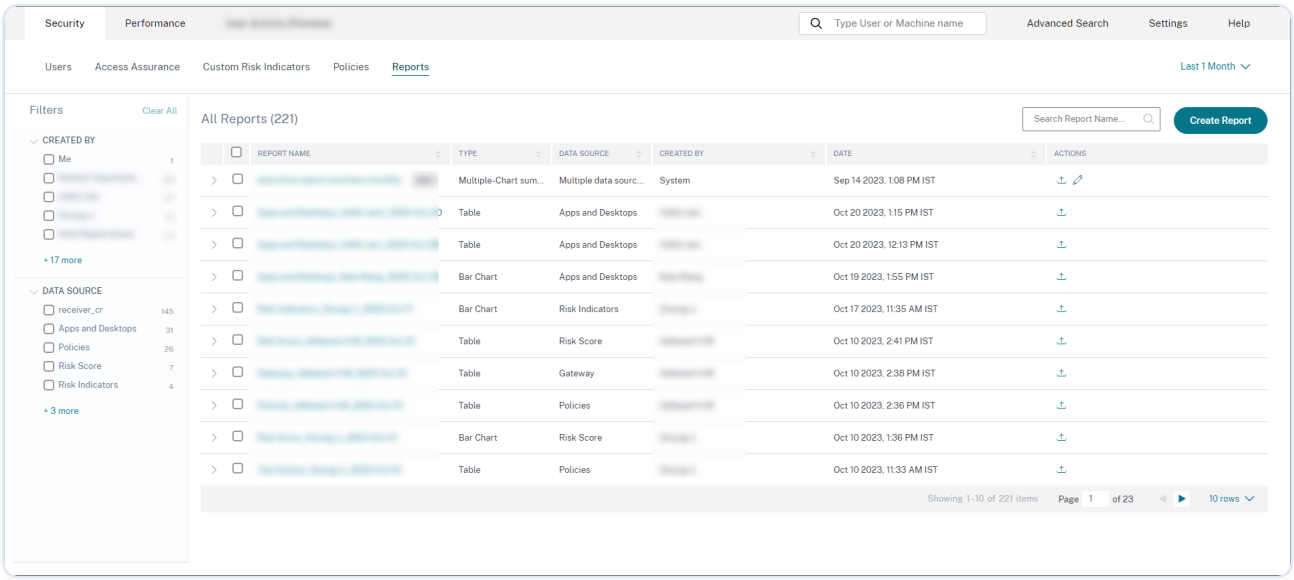
DATA SOURCE	DIMENSION	DESCRIPTION
Risk Indicators	Category	Indicates the category of risk indicators. The risk indicators are grouped into one of four categories - compromised endpoints, compromised users, data exfiltration, or insider threats.
	Risk-Indicator-Name	The name of the risk indicator. For a custom risk indicator, the name is defined by the admin while creating the indicator.
	Severity	Indicates the severity of the risk. It can be low, medium, or high.
	User-Name	The user name or domain\username that is used for logging in.
Risk Score	Risk-Score	The risk score assigned to the user. The risk score varies from 0 to 100 depending on the threat severity associated with the user’s activity.
	User-Name	The user name or domain\username that is used for logging in.
	Risk-Score-Category	Based on the risk score, a risky user can fall into one of the following categories: high risk, medium risk, and low risk.

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

Reports

You can perform the following actions on reports using this view:

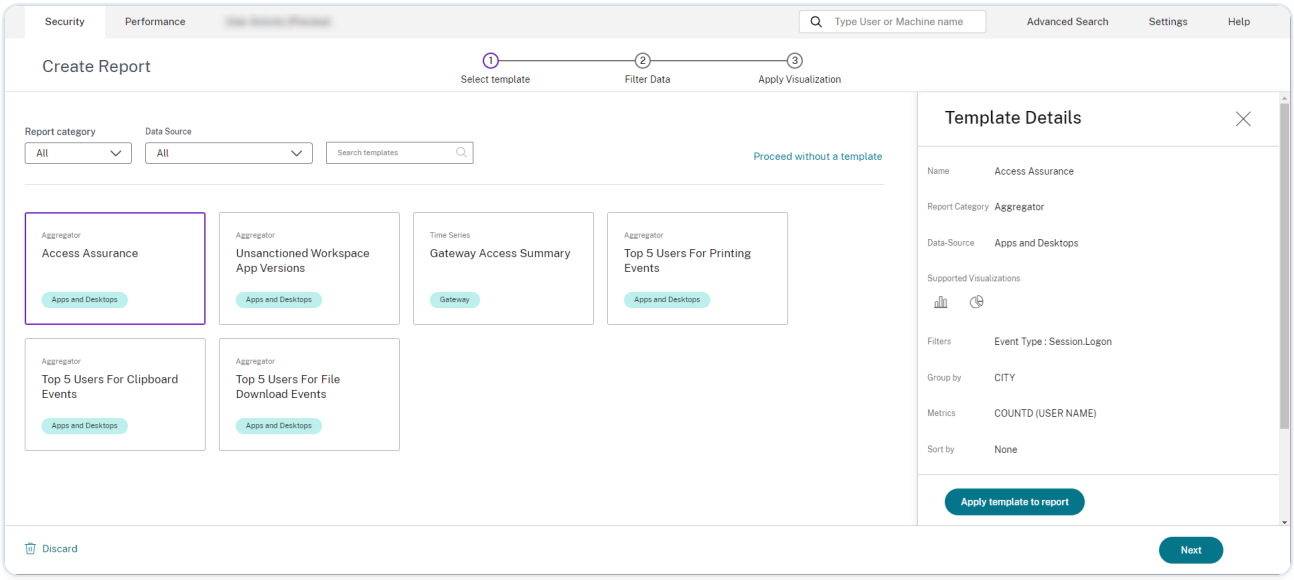
- Click **Create Report** to create a custom report.
- Expand a row to see the preview of an existing custom report.
- Click the report name to see the detailed report visualization.
- Click the export icon to export an existing custom report in PDF format.
- Click the edit icon to edit the reports you've created.
- Click the delete icon to delete the reports you've created.



Create a custom report

To create a custom report, click **Create Reports**. On the **Create Report** page, you can choose to create a custom report with or without templates.

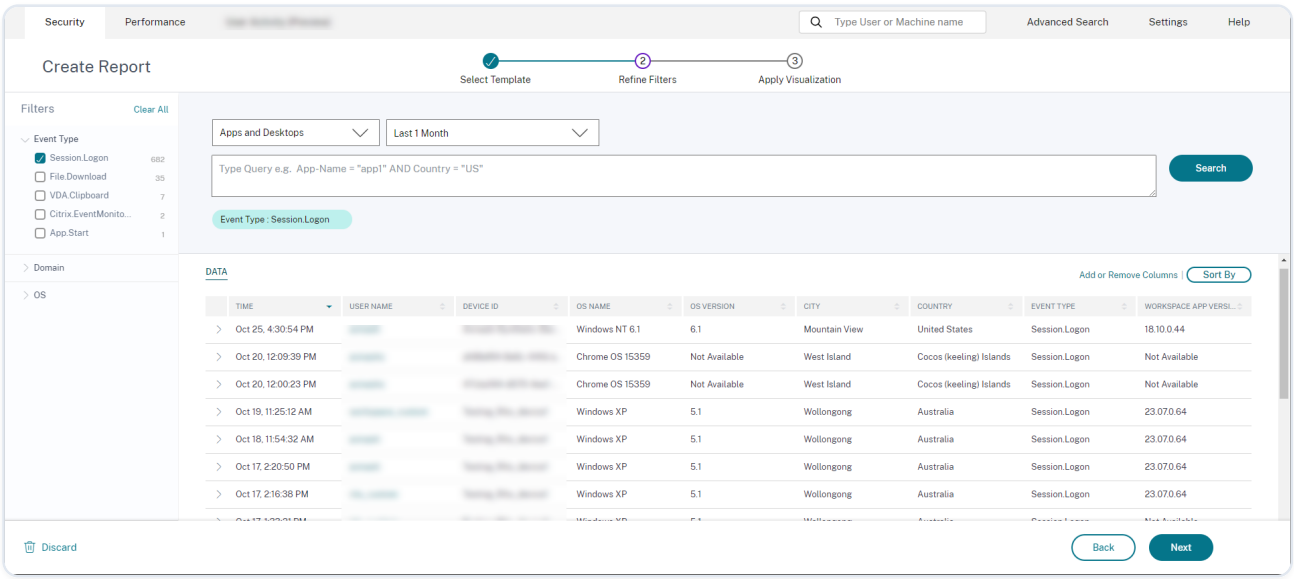
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Creating a custom report with templates

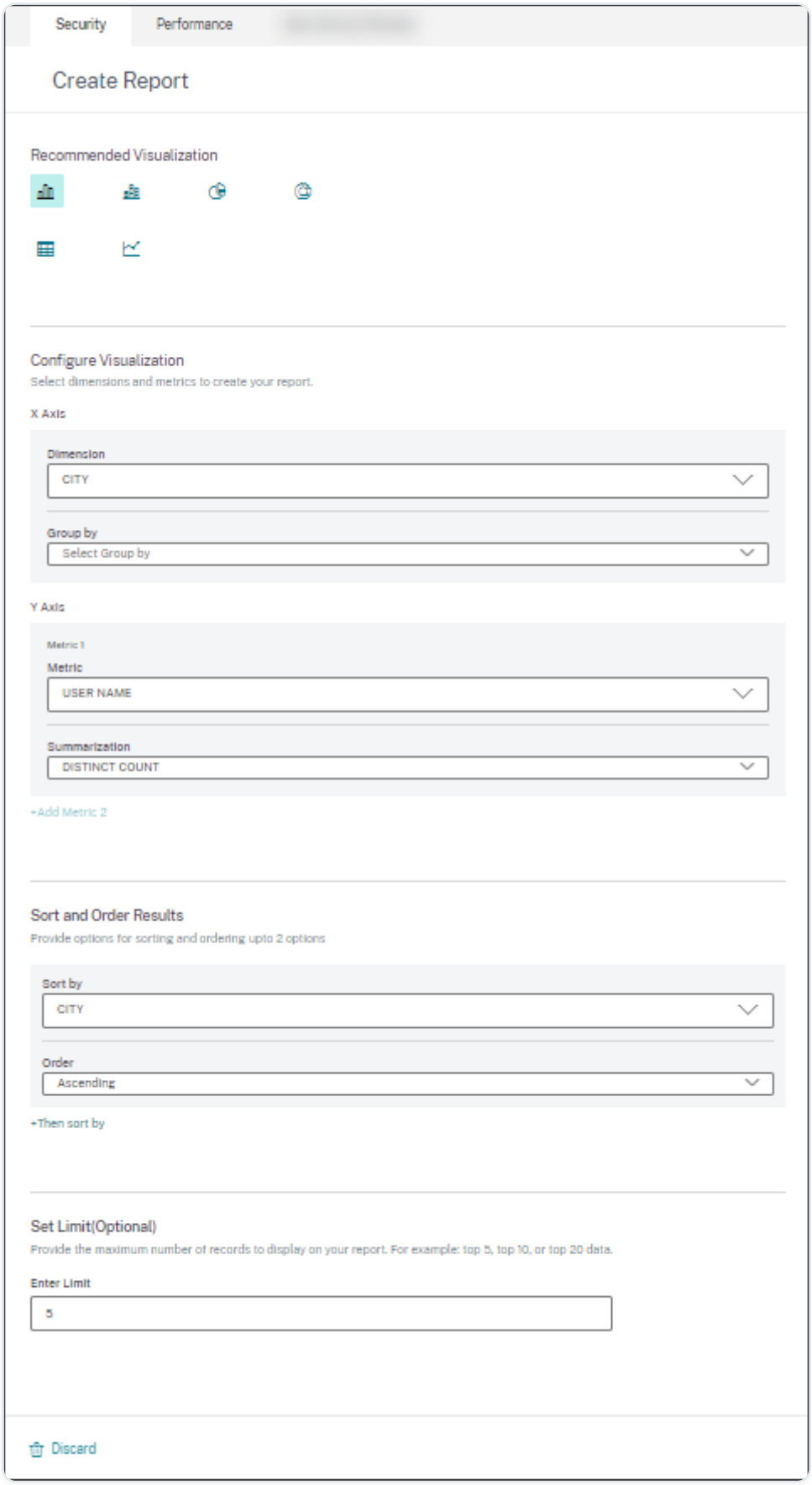
To create a custom report with a template:

1. **Select a template**: Once you click a template, the template details are listed on the right. Click **Apply Template to Report** to enable the report to use the selected template.
2. **Refine Filters**: The **Refine Filters** page shows the filters that were predefined for the template you selected. Make the required changes and then click **Next**.



1. **Apply Visualization**: Select one of the available visualizations for displaying the report.

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



- **Bar chart**: Presents data with vertical rectangular bars with height proportional to the values. Used for comparing events.

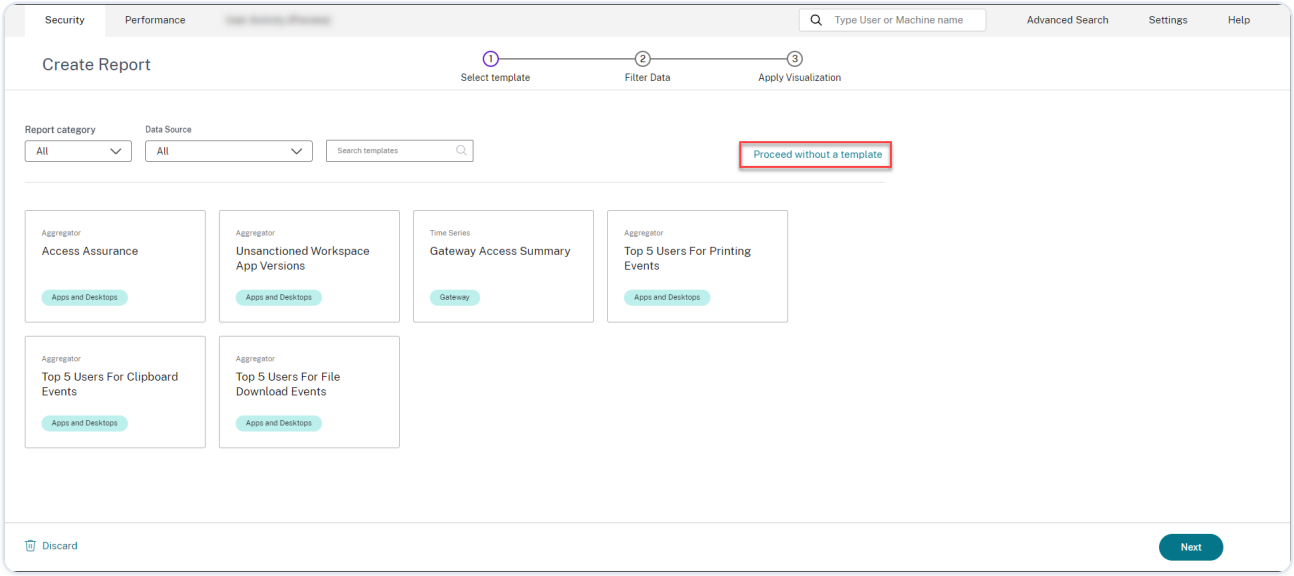
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Stacked-column chart**: Presents data in the form of bars stacked one over the other. Used to visualize the total sum of data over multiple sub-categories.
- **Pie chart**: Presents data in the form of a pie. Used to visualize the relative size of the data or percentages.
- **Donut chart**: Presents data in the form of a donut. Used to visualize the relative size of the data or percentages. - **Table**: Presents data in the form of a table. Used to visualize as many dimensions as needed.
- **Line chart**: Presents data with dots connected by straight line segments. Used to visualize data trends over a time period.

1. Now configure the visualization with the following parameters:
    - Dimension for the x-axis
    - Metrics to be plotted in the y-axis
    - Summarization or aggregations, such as average or count, to be applied to the metric
    - Options for sorting and ordering
    - An optional limit for the maximum number of records to be displayed on the report.

Creating a custom report without templates

You can also create a custom report without a predefined template. Click **Create Custom Report without Template**. Select a data source from the dropdown list. Follow the steps to define the filters, apply visualization, save, and schedule the report.

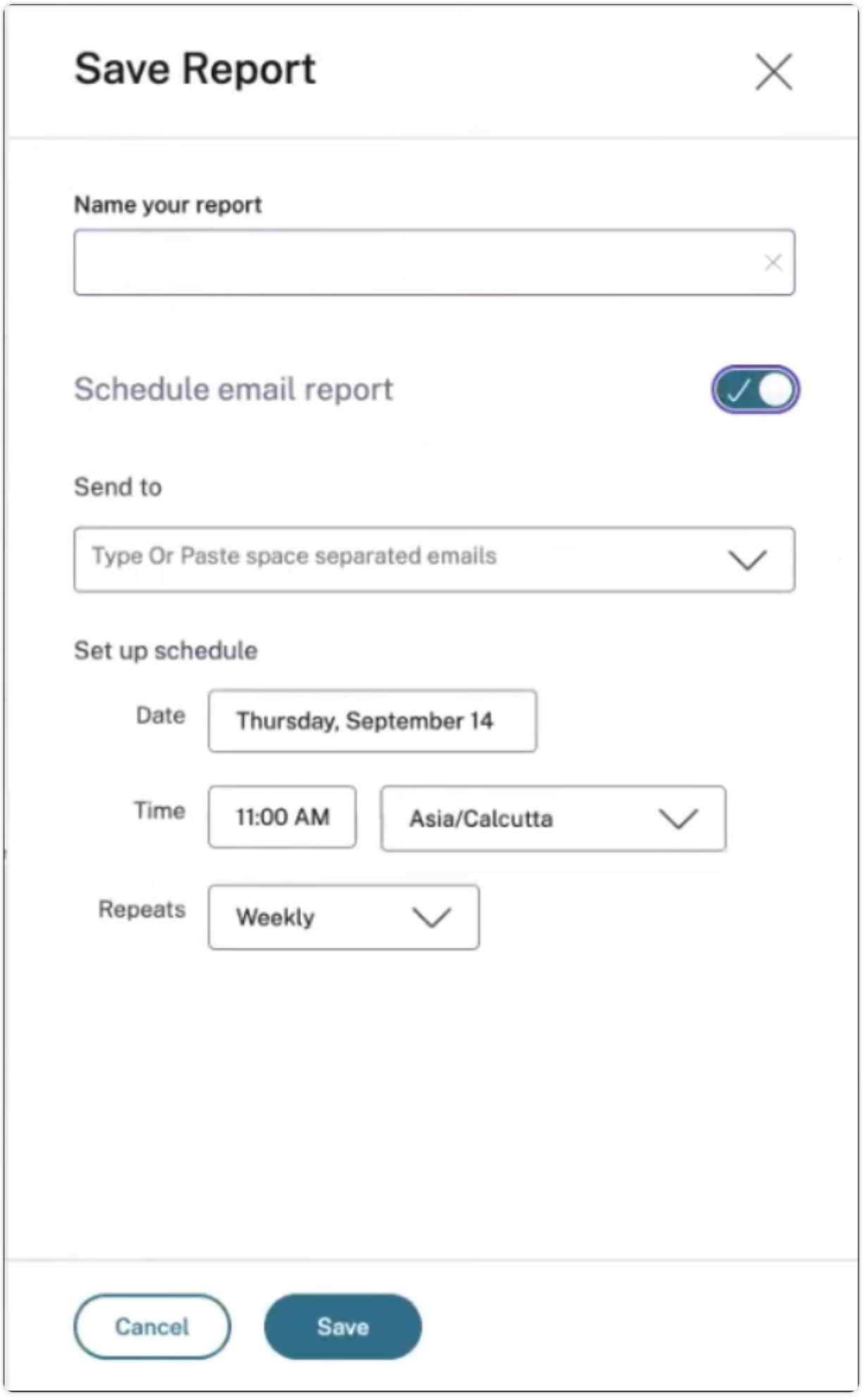


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Save a report

1. To save the report, click **Save**. Specify a title for your report.
2. You can schedule to email the report to the specified email IDs and distribution lists on a specific date and time or a recurring schedule.

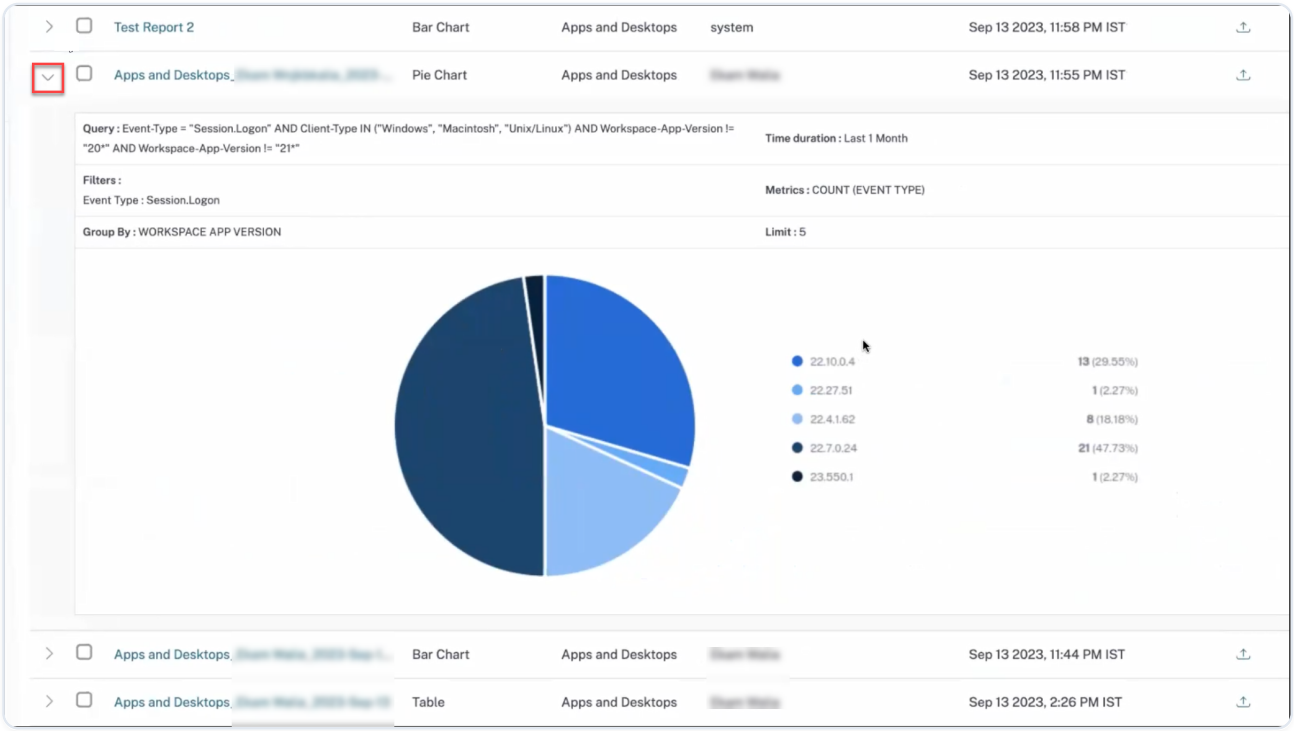
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

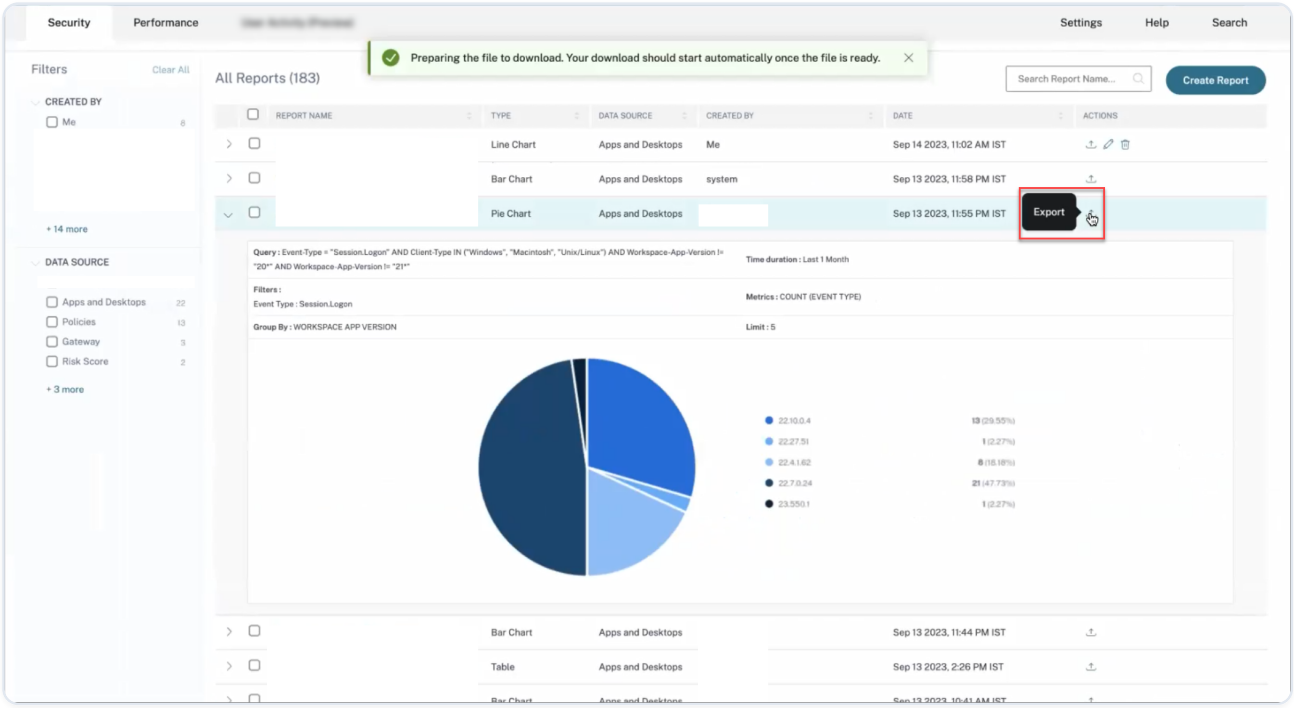
View a report

1. After you've created and saved a report, you can view the report on the **Reports** page. You can also modify or delete a saved report.
2. Click the dropdown button to preview the report.



Export a report

Click the export icon to export the report.



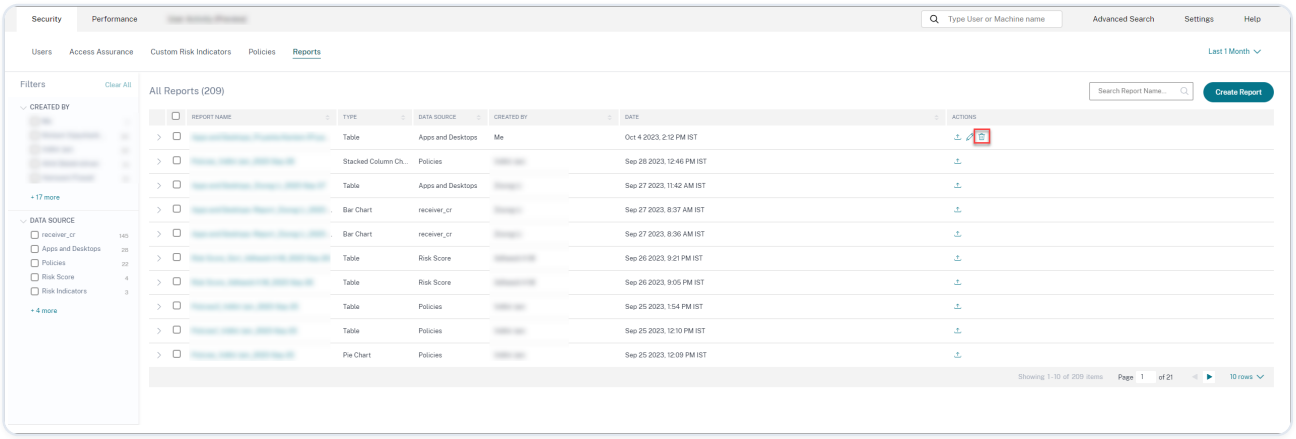
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Delete a report

Click the delete icon to delete the report.

Note:

> Only the user who creates the report can delete it.

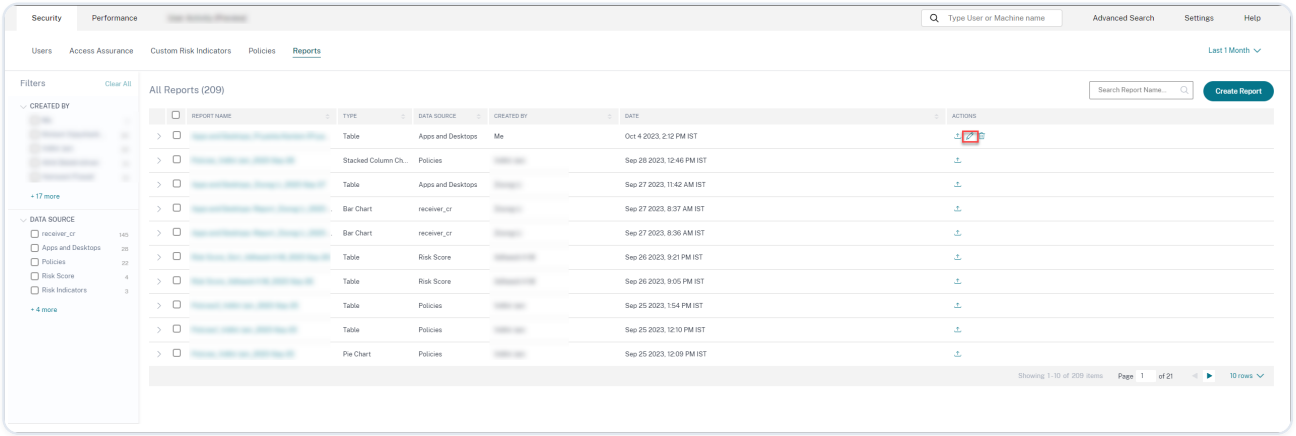


Edit a report

Click the edit icon to edit the report.

Note:

> Only the user who creates the report can edit it.



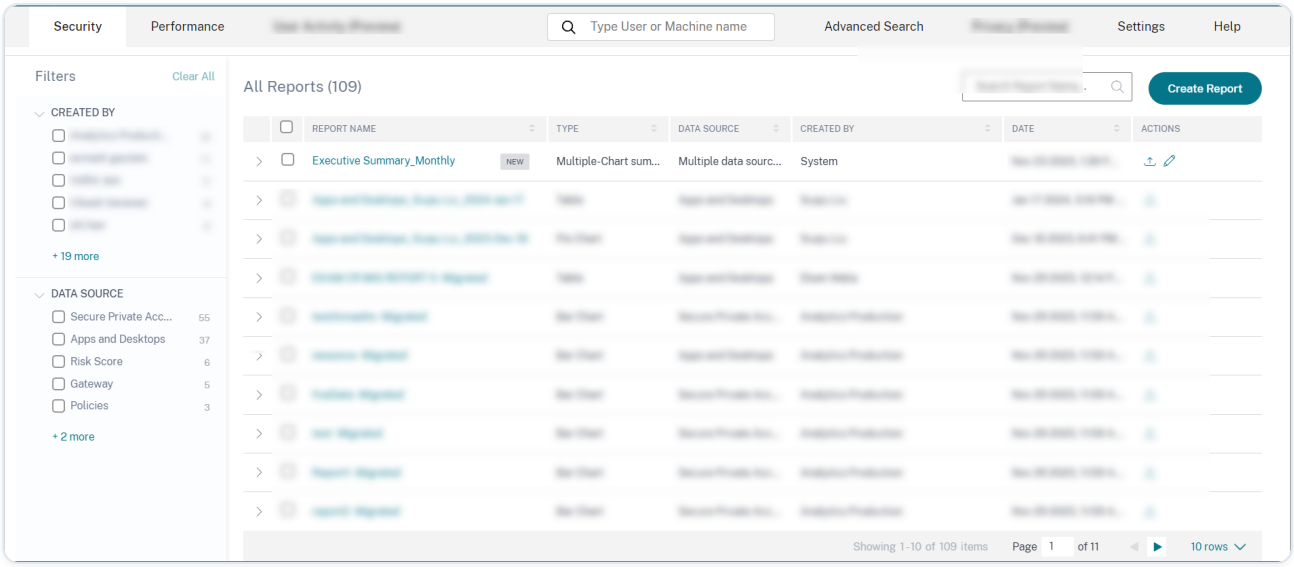
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Executive Summary report

You can schedule an automated export through email which contains a PDF of a pre-created executive summary report. The executive summary report is a collection of reports depicting your enterprise's security posture at one single glance for the selected time period to the audience of your choice.

You can create the report for data for the following time durations:

- Last 1 Hour
- Last 12 Hour
- Last 1 Day
- Last 1 Week
- Last 1 Month



What reports does it contain?

The Executive Summary report contains the following reports:

- **User Risk Distribution**: The distribution of high, medium, and low risky profiles based on their highest computed risk score in the selected time period.
- Top Risky Users: The top risky users among all users sorted by highest risk scores for the selected time period.
- **Risk Occurrences by Categories**: The comprehensive view of the types of risk exposures and critical risks provided by risk categories that require immediate action. The risk indicators are grouped under the following categories:

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

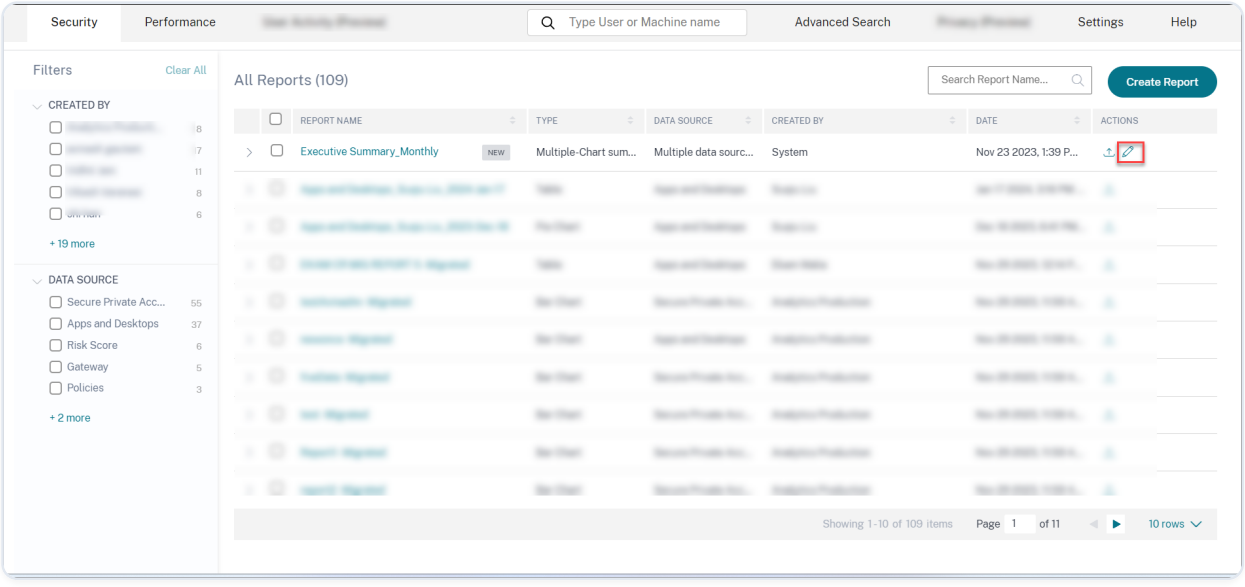
- Compromised users
- Compromised endpoints
- Data exfiltration
- Insider threats

- **Risk Indicators**: The triggered risk indicators for the users for the selected time period.
- **Actions**: The applied actions to the risk indicators triggered for the users for the selected time period.
- **Top policies**: The top five policies that got triggered the most in the selected time period.
- **Top Actions**: The top five actions that got triggered the most in the selected time period.
- **Risk Indicators by Severity**: Default and custom risk indicators triggered by the users sorted based on the severity.
- **Risk Indicators by Total Occurrences**: Default and custom risk indicators triggered by the users sorted based on the occurrences.

Edit an Executive Report

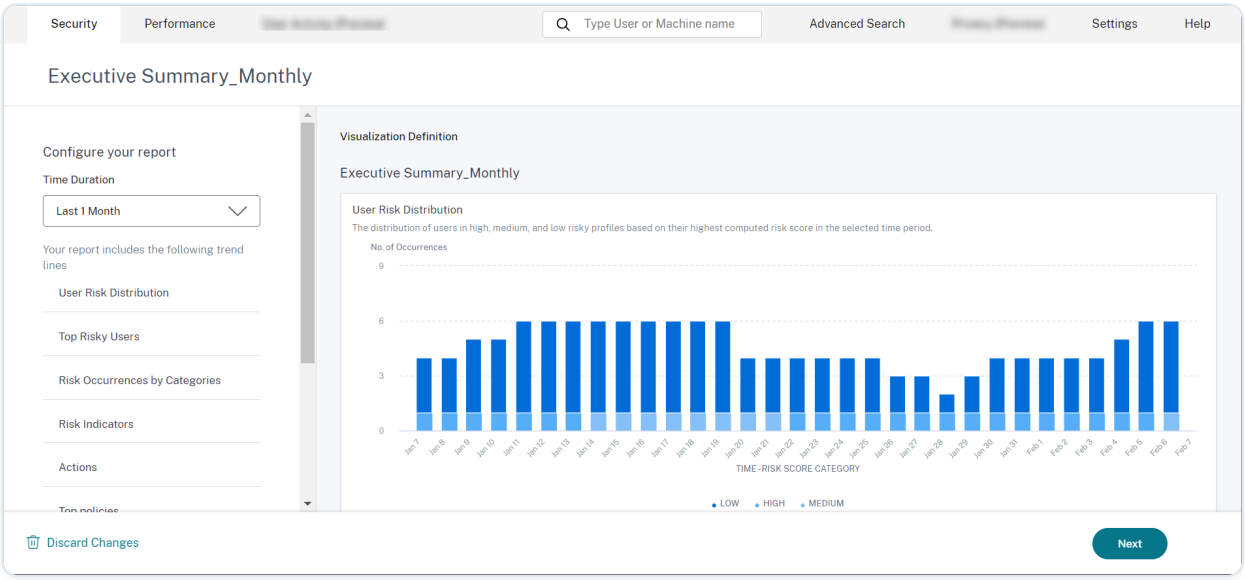
To edit an Executive Report, complete the following steps:

1. Click the **Edit** symbol.



2. In the **Configure your report** pane, select the time duration for which you want to see the data.

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



3. Click **Next**. The **Save Report** pane appears.

> **NOTE:**
>
> To discard the changes, click **Discard Changes**.

4. In the **Save Report** pane, enter the following details:

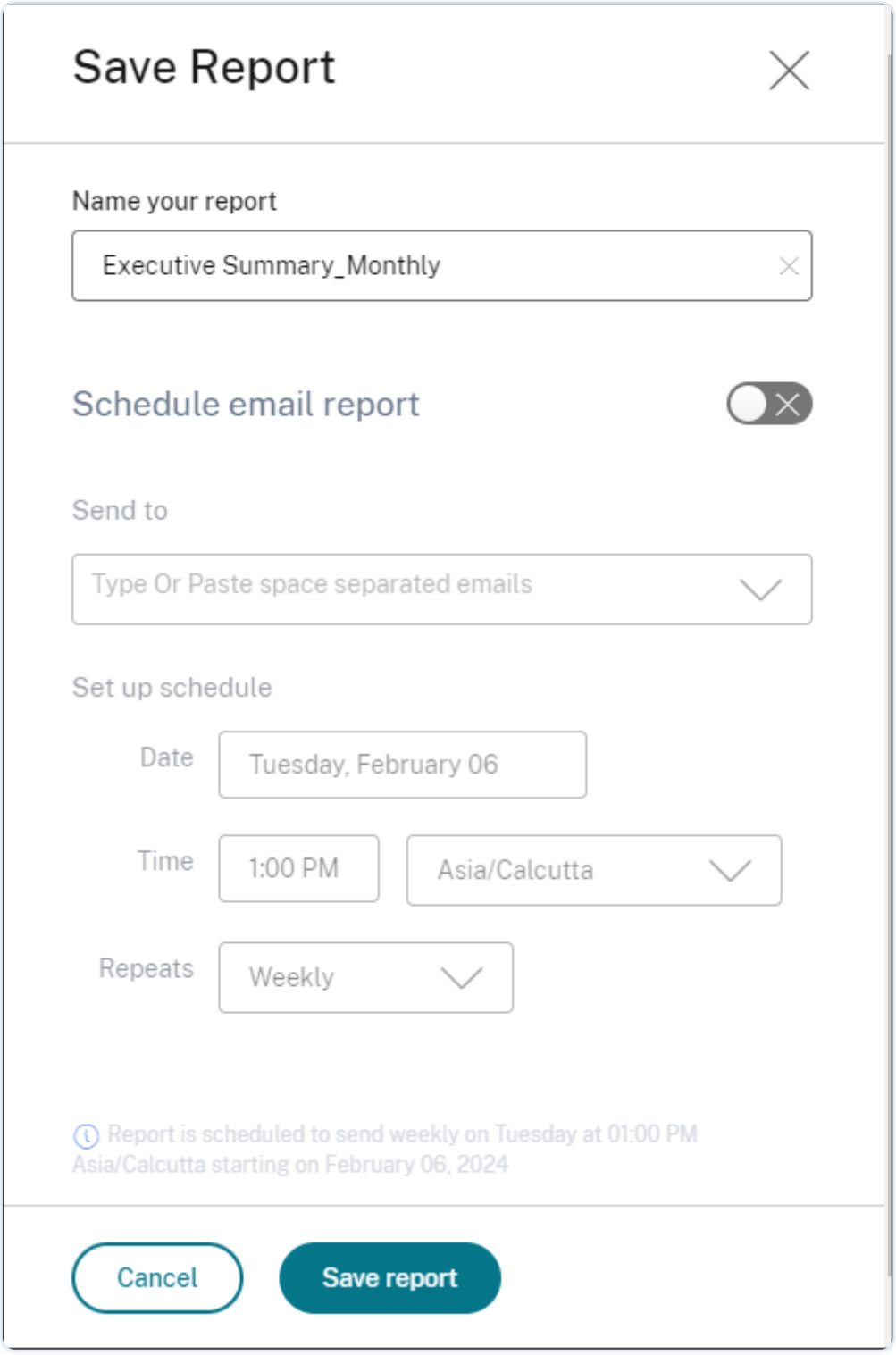
   a. **Name your report**: The name of the executive report.

   b. **Schedule email report**: Toggle on to schedule the report. The toggle is off by default.

   c. **Send to**: Select a distribution list from the dropdown. You can also add a combination of distribution lists and individual email addresses. To create a customized distribution list, see Admin Email Settings.

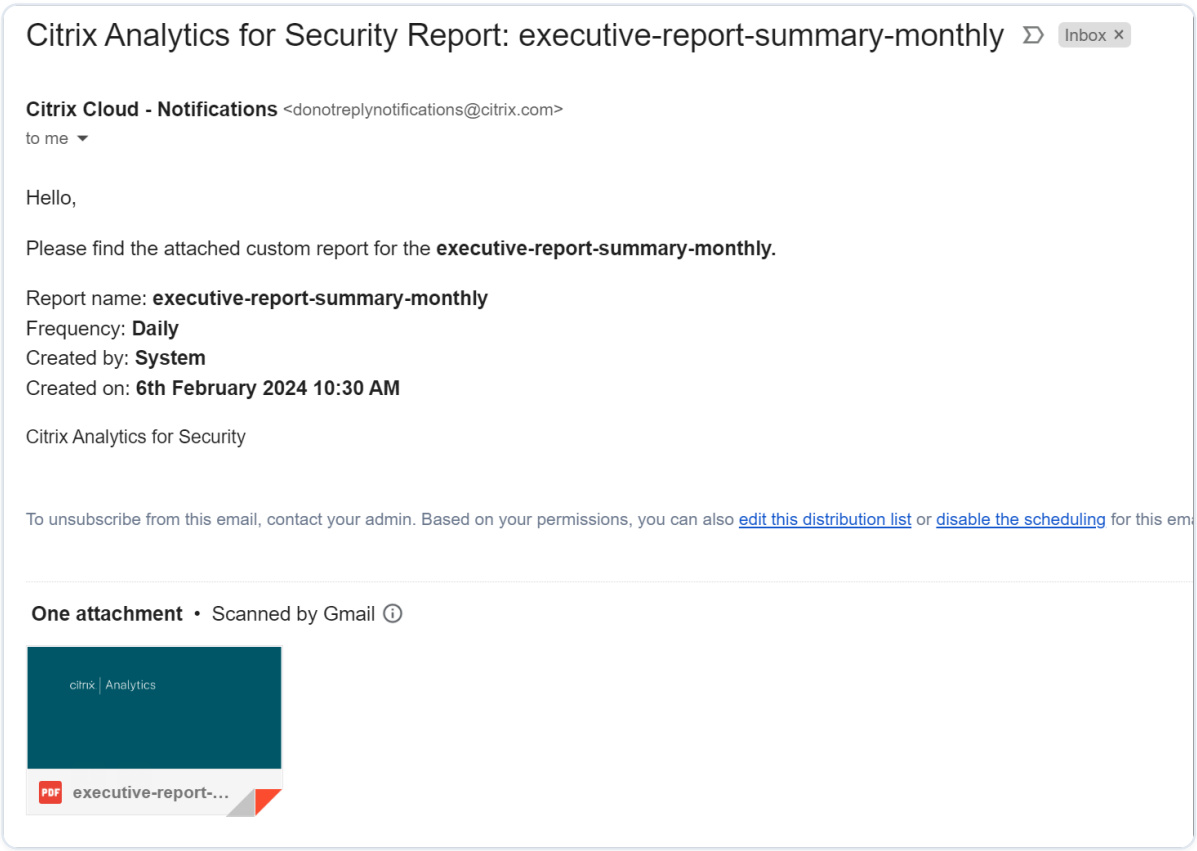
   d. **Set up schedule**: Select the desired time at which the report is first sent to the selected audience and the time it repeats.

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

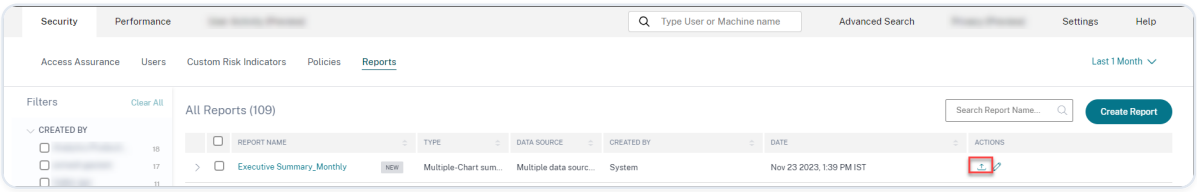


e. Click **Save report**. The report is then sent as an email to the listed recipients.

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



Alternatively, you can export the executive report as a PDF using the **Export** symbol.



The following screenshot depicts a sample PDF output:

© 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.



Self-service search

layout: doc replicate-from: commons/self-service-search.md

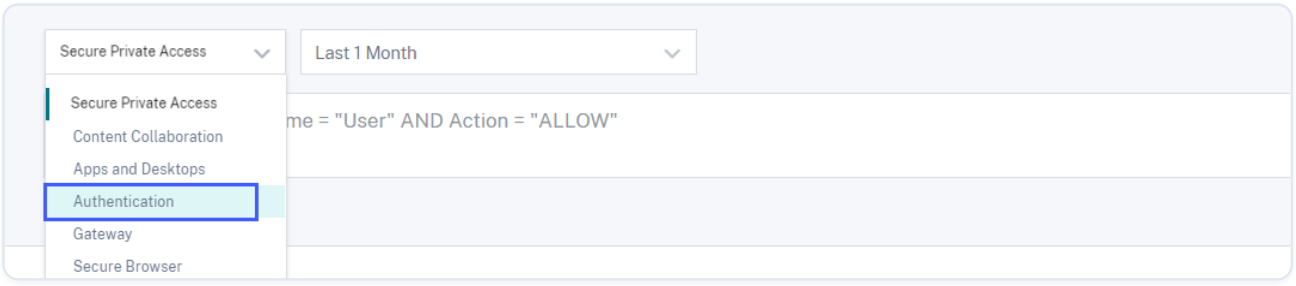
Self-service search for Authentication

Use the self-service search to get insights into the user authentication details of the Citrix Cloud users in your enterprise. Citrix Analytics for Security™ receives the user authentication events from the Identity and Access Management service of Citrix Cloud. Authentication events such as user login, user logoff, and client update are displayed on the self-service search page.

For more information on the search functionalities, see **Self-service search**.

Select the Authentication data source

To view the authentication events, select **Authentication** from the list. By default, the self-service page displays the events for the last one day. You can also select the time period for which you want to view the events.

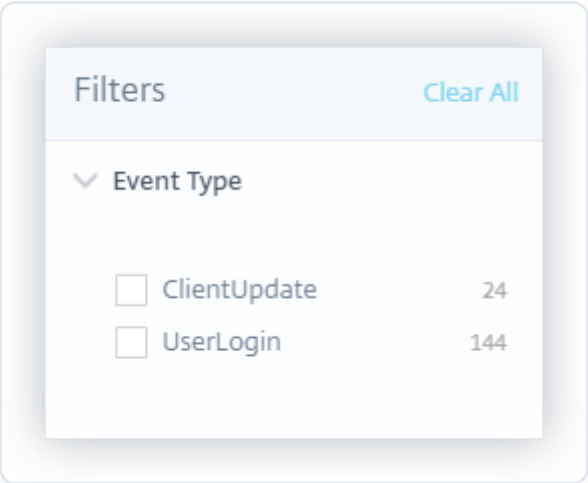


Select the facets to filter events

Use the following filter for the authentication events:

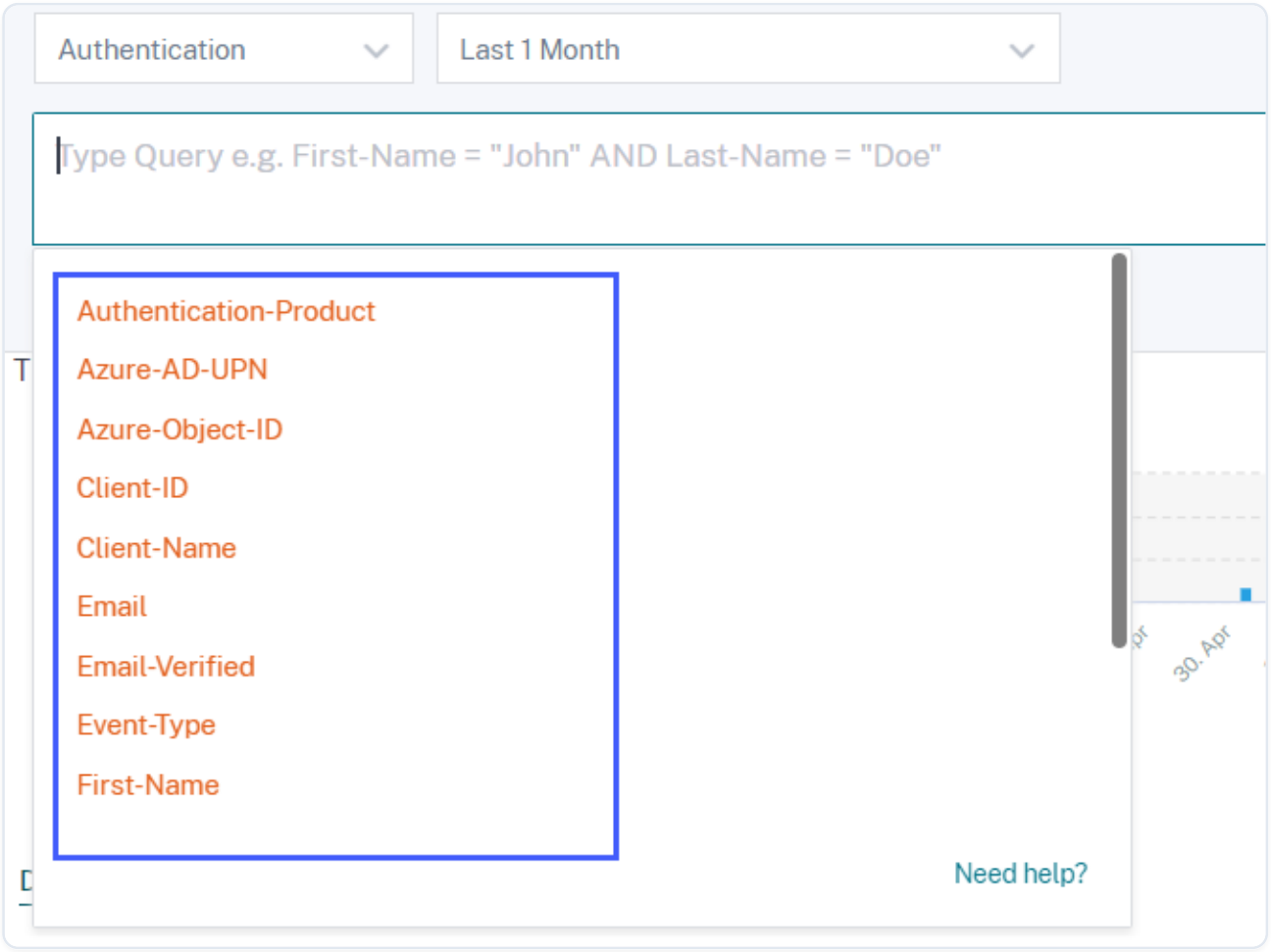
- **Event Type**- Search events based on the user event types such as user login, user logoff, and client update.

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



Specify search query to filter events

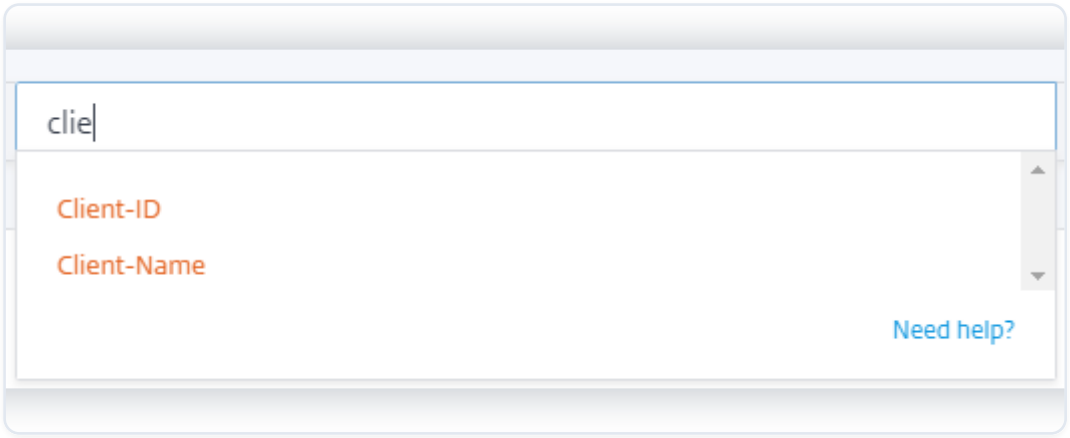
Place your cursor in the search box to view the list of dimensions for the authentication events. Use the dimensions and the operators to specify your query and search for the required events.



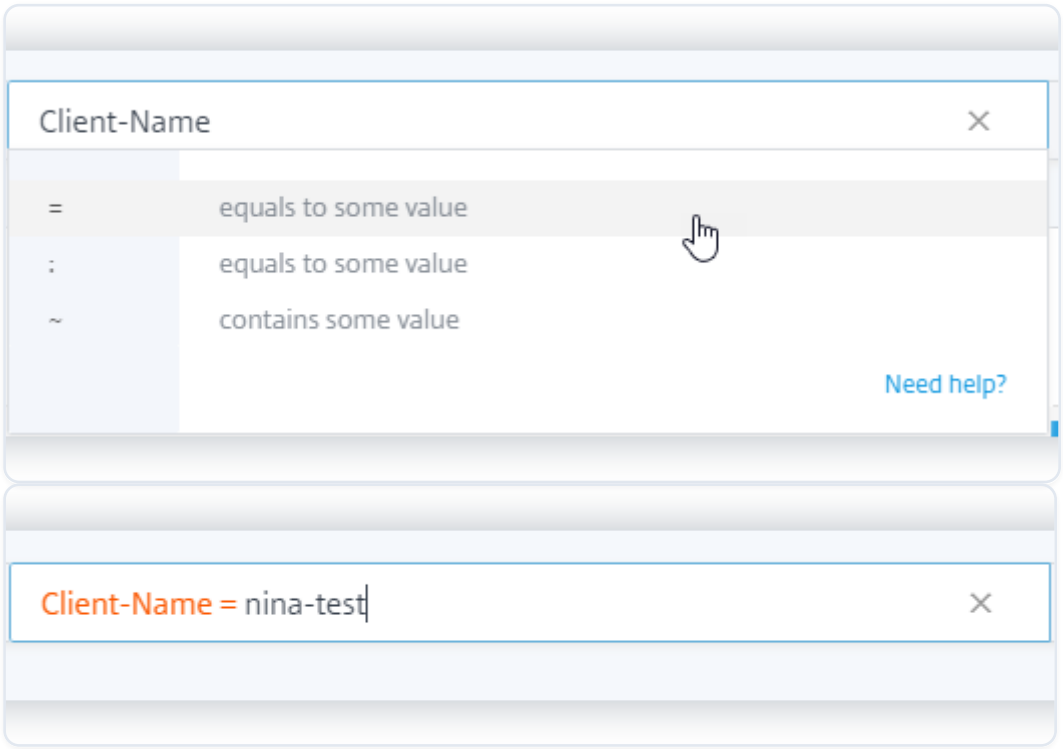
For example, you want to view the authentication events for a client "nina-test" with the email status verified.

1. Enter "client" in the search box to get the related dimensions.

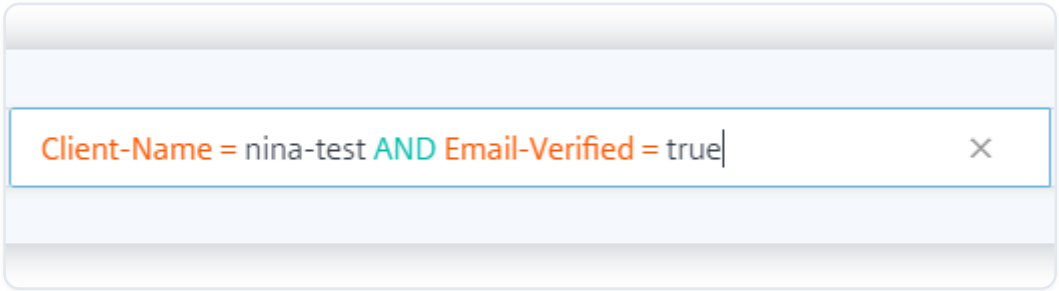
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Select **Client-Name** and then specify the value "nina-test" using the equal operator.



3. Select the **AND** operator and then select the **Email-Verified** dimension. Assign the value "true" to **Email-Verified** using the equal operator. The "true" value indicates that the user's email is verified.



4. Select the time period and click **Search** to view the events on the **DATA** table.

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

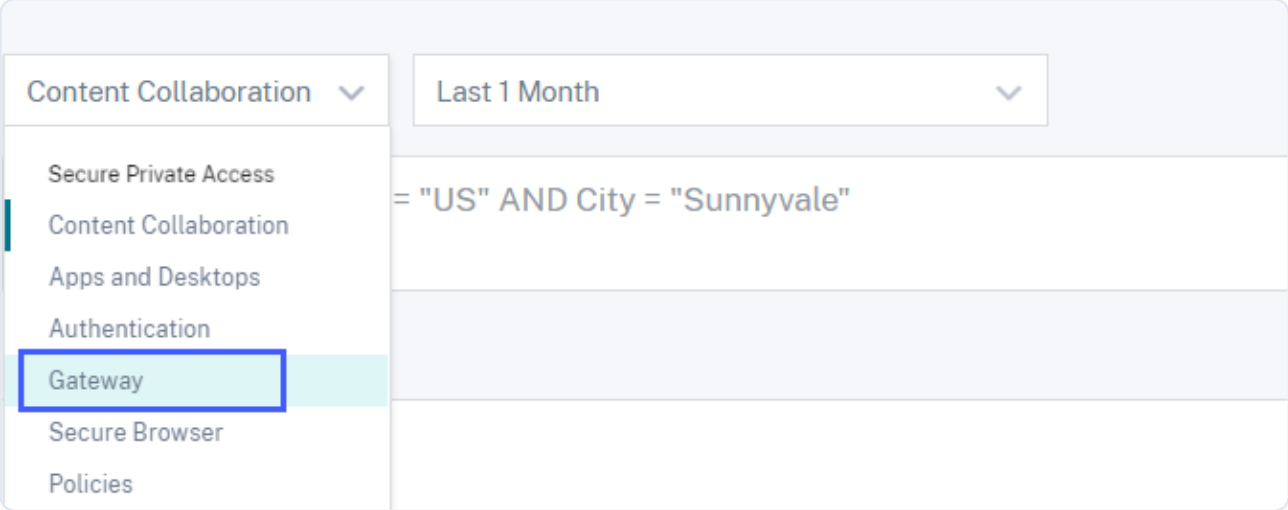
Self-service search for Gateway

Use the self-service search feature to get insights into the user events received from the Citrix Gateway data source. When users access their network resources such as file servers, applications, websites through Citrix Gateway, events are generated for each user connection. Some examples of user events are such as authentication stage, authorization type, and VPN session code. Citrix Analytics for Security™ receives these events and displays them on the self-service search page. You can view the users and their access details.

For more information on the search functionalities, see **Self-service search**.

Select the Gateway data source

To view the Gateway events, select **Gateway** from the list. By default, the self-service page displays the events for the last one day. You can also select the time period for which you want to view the events.



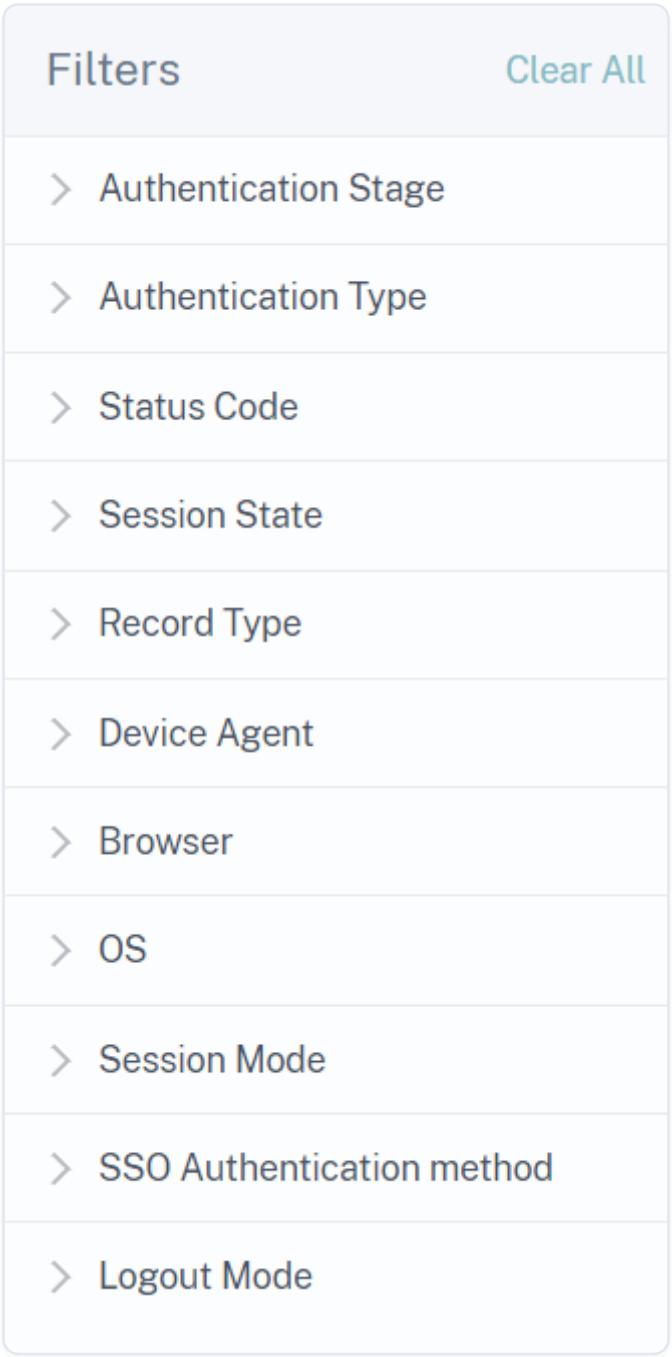
NOTE

Alternatively, you can access the Self-service search for Gateway page from the **Security** > **Users** > **Access Summary** dashboard. In successful login scenarios, you can access the data by the status code. For more information, see the Access Summary dashboard.

Use the facets to filter events

The facets are categorized based on the events received from your data source. Use the following facets to filter your events:

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



- **Authentication Stage**- Search events based on different stages of client authentication such as primary, secondary, and tertiary.
- **Authentication Type**- Search events based on the client authentication types such as Local, RADIUS, LDAP, TACACS, client certificate authentication including smart card authentication.
- **Device Agent**- Search events based on the client devices such as iPhone, iPad, Windows Mobile.
- **Record Type**- Search events based on the types of VPN records. Following VPN record types are available:

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

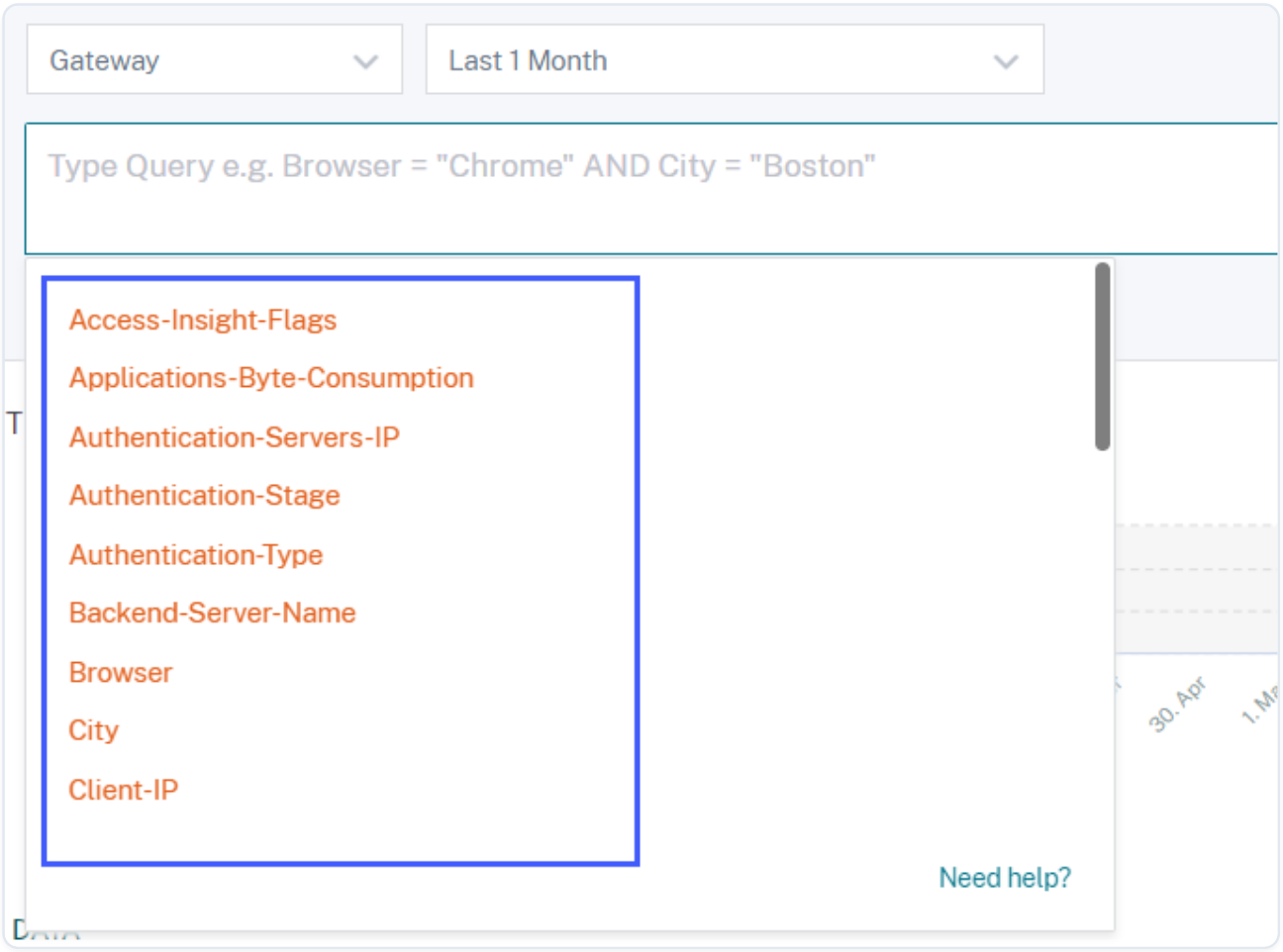
RECORD TYPE	DESCRIPTION
VPN_AI	Filters user events related to authentication.
VPN_IF	Filters user events related to ICA® file.
VPN_ST	Filters user events related to session logout.

- **Browser**- Search events based on the browsers such as Internet Explorer, Chrome, Firefox, Safari.
- **OS**- Search events based on the client operating systems such as Windows, Mac, Linux, Android, iOS.
- **Status Code**- Search events based on the VPN status codes such as SSL redirect response failure, authorization failure, single sign-on failed.
- **Session State**- Search events based on the VPN session states such as client state, authorization state, SSO state, application bandwidth update.
- **Session Mode**- Search events based on the VPN session modes such as Full tunnel, ICA Proxy, Clientless.
- **SSO Authentication Method**- Search events based on different methods of single sign-on authentication such as basic, digest, NTLM, Kerberos, AG basic, form-based SSO.
- **Logout Mode**- Search events based on the VPN logout modes such as internal error logout, session time-out logout, user-initiated logout, administrator terminated session.

Specify search query to filter events

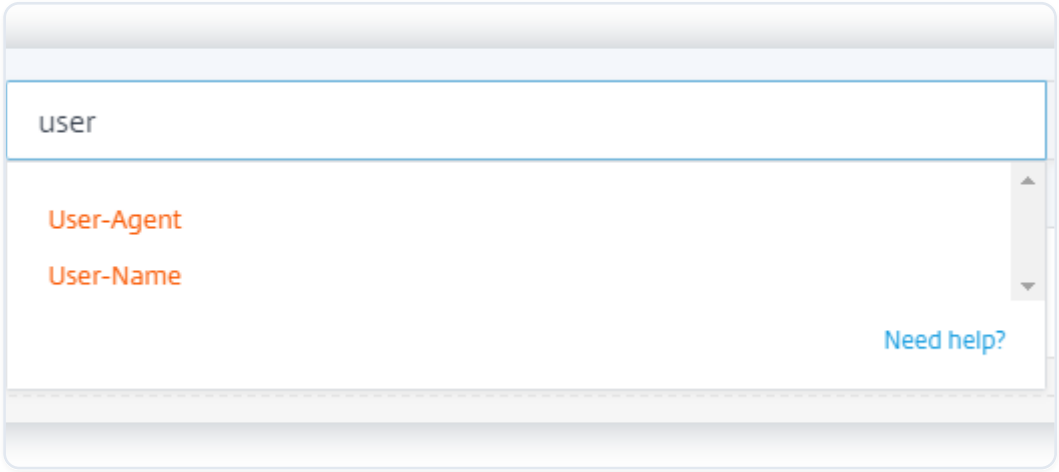
Place your cursor in the search box to view the list of dimensions for the Gateway events. Use the dimensions and the operators to specify your query and search for the required events.

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



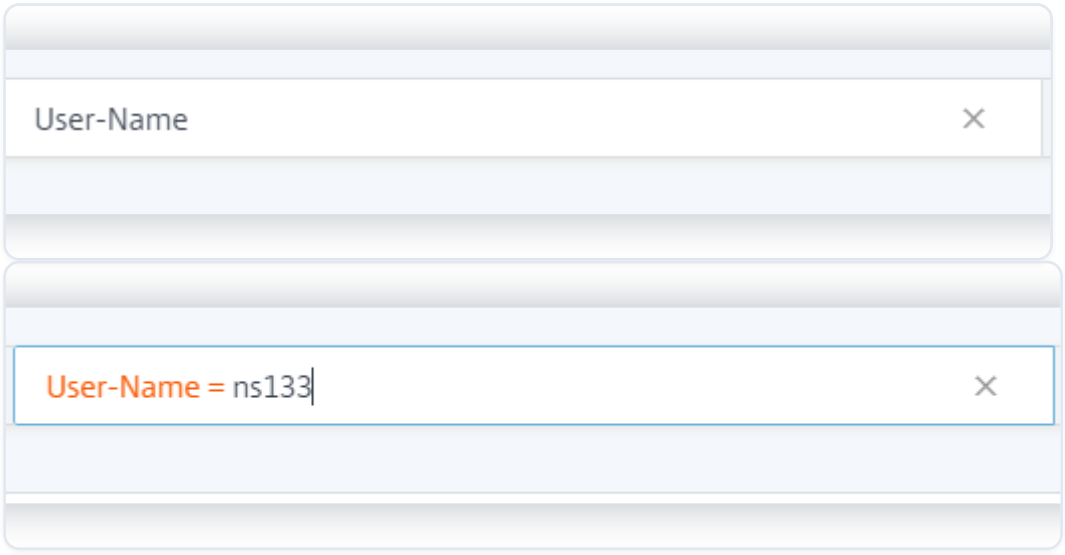
For example, you want to view the events for a user "ns133" where the VPN status code is "successful login".

1. Enter "user" in the search box to choose the related dimension.

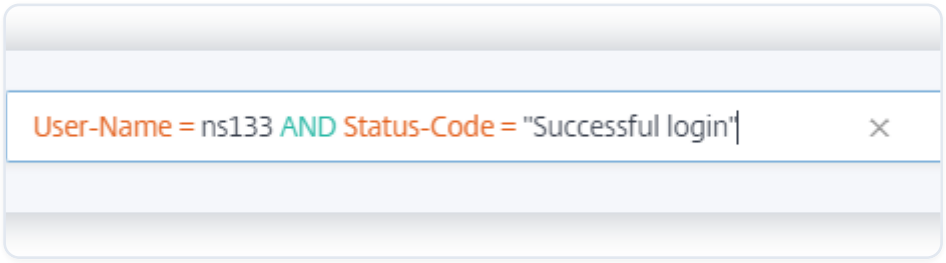


2. Select **User-Name** and enter the value "ns133" using the equal operator.

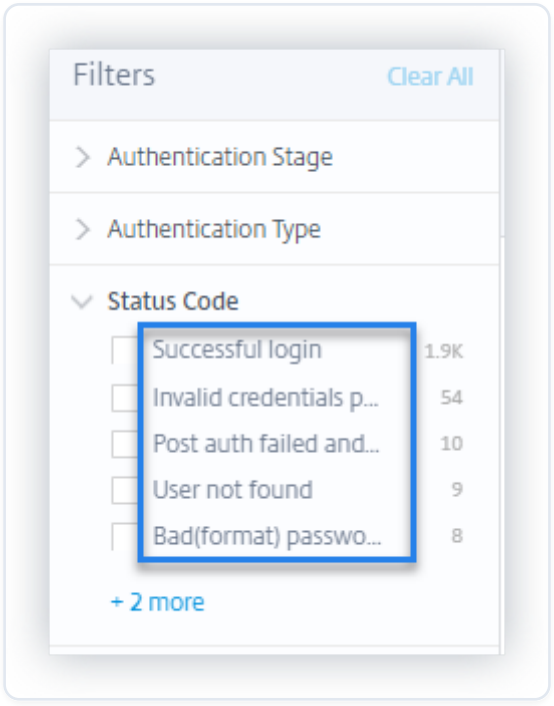
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Select the **AND** operator and then select the **Status Code** dimension. Enter the string "Successful login" for **Status Code** using the equal operator.



To identify the possible string values for **Status Code**, expand the **Status Code** filter list and use the filter name as the string in your search query.



4. Select the time period and click **Search** to view the events on the **DATA** table.

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

Supported values for your search query

Enter the following values for the dimensions to define your search query.

Access-Insight-Flags

Indicates the VPN session states. Enter one of the following flag values:

VPN SESSION STATE	FLAG VALUE
Pre-authentication	2
Last or final state of nFactor (multi-factor) authentication	1
Post authentication	4

NOTE

This flag is applicable only for the preceding VPN session states for the authentication events. For all other events, the flag value is zero.

Applications-Byte-Consumption

For the `Applications-Byte-Consumption` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
Examples: `40`, `100`	Number	Data (in Bytes) consumed by the application that you are using.

Authentication-Servers-IP

For the `Authentication-Servers-IP` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
Example: `10.xxx.xx.xx`	String	IP address of the authentication server.

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

Authentication-Stage

For the `Authentication-Stage` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
`Primary`, `Secondary`, or `Tertiary`	String	Different stages of client authentication.

Authentication-Type

For the `Authentication-Type` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
`LDAP`, `SAML`, `Local`, `Radius`, `TACACS`, `SAMLIDP`, or `OTP`.	String	Authenticate your users through one of the available methods.

Backend-Server-Name

For the `Backend-Server-Name` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
Example: `10.xxx.xxx.xx`	String	IP address of the back end server.

Browser

For the `Browser` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
`PN Agent`, `Edge`, `Firefox`, `Chrome`, or `Safari`.	String	Browser used.

City

For the `City` dimension, enter the following value:

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

VALUE	TYPE	DESCRIPTION
Examples: `Boston`, `Beijing`	String	City from where the user has logged on.

Client-IP

For the `Client-IP` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
Example: `10.xxx.xxx.xx`	String	IP address of the user device.

Client-IP-Type

For the `Client-IP-Type` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
public, private	String	Indicates whether the user IP address is public or private.

NOTE

The values are case-sensitive. Enter the values in lower case.

Client-Port

For the `Client-Port` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
Example: `45334`	Number	Port number of the user device.

Country

For the `Country` dimension, enter the following value:

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

VALUE	TYPE	DESCRIPTION
Examples: `United States`, `India`	String	Country from where the user has logged on.

NOTE

Enclose the value within "" if the value contains spaces. **Example**: Country = "Unites States".

Event-Type

For the `Event-Type` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
Authentication, ICA file, Session logout	String	Type of user events.

Gateway-FQDN

For the `Gateway-FQDN` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
Example: `Gateway-test`	String	Domain name of your Citrix Gateway.

Gateway-IP

For the `Gateway-IP` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
Example: `10.xxx.xxx.xx`	String	IP address of your Citrix Gateway.

Gateway-Port

For the `Gateway-Port` dimension, enter the following value:

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

VALUE	TYPE	DESCRIPTION
Example: `443`	String	Port number of your Citrix Gateway.

Logout-Mode

For the `Logout-Mode` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
`"Internal error"`, `"Inactive time out"`, `"User initiated logout"`, or `"Administrator killed session"`.	String	Reason for timeout or termination of VPN session.

NOTE

Enclose the value within "" if the value contains spaces. **Example**: Logout-Mode = `"Internal error"`.

NetScaler-IP

For the `NetScaler-IP` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
Example: `10.xxx.xx.xx`	String	IP address of your Citrix ADC appliance.

OS

For the `OS` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
Examples: `MAC_OS`, `WINDOWS`	String	Operating system of the user device.

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

Record Type

For the `Record Type` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
`VPN_AI`	String	Indicates user events related to authentication.
`VPN_IF`	String	Indicates user events related to ICA file.
`VPN_ST`	String	Indicates user events related to session logout.

SSO-Authentication-Method

For the `SSO-Authentication-Method` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
`NSAUTH_BEARER`, `NSAUTH_FORM`, `NSAUTH_CITRIXAGBASIC`, `NSAUTH_NEGOTIATE`, `NSAUTH_NTLM`, or `NSAUTH_BASIC`.	String	Different methods of single sign-on authentication.

Server-IP

For the `Server-IP` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
Example: `10.xx.xxx.xx`	String	IP address of the back end server.

Server-Port

For the `Server-Port` dimension, enter the following value:

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

VALUE	TYPE	DESCRIPTION
Example: `47054`	Number	Port number of the back end server.

Session-State

For the `Session-State` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
`"Set Client State"`, `"Authorization State"`, `"SSO State"`, and `"Application Bandwidth Update"`	String	The VPN session state.

NOTE

Enclose the value within "" if the value contains spaces. **Example**: Session-State = `"Set Client State"`.

Status-Code

For the `Status-Code` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
`"Successful login"`, `"Invalid credentials passed"`, `"Post auth failed and connection quarantined"`, `"Login not permitted"`, `"Maximum login failures reached"`	String	The VPN status code.

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

NOTE

Enclose the value within "" if the value contains spaces. **Example**: Session-Code = `"Successful login"`.

User-Agent

For the `User-Agent` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
`IPHONE`, `IPAD`, or `WINPHONE`	String	The agent or the device used to access the VPN.

VPN-Session-ID

For the `VPN-Session-ID` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
`c2c290c61dfe4e07247bde1e22142a12`	String	Session ID assigned by the server for a user's VPN session.

VPN-Session-Mode

For the `VPN-Session-Mode` dimension, enter the following value:

VALUE	TYPE	DESCRIPTION
`"Full Tunnel"`, `"ICA Proxy"`, or `Clientless`	String	Different modes of a user's VPN session.

NOTE

Enclose the value within "" if the value contains spaces. **Example**: Session-Code = `"Full Tunnel"`.

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

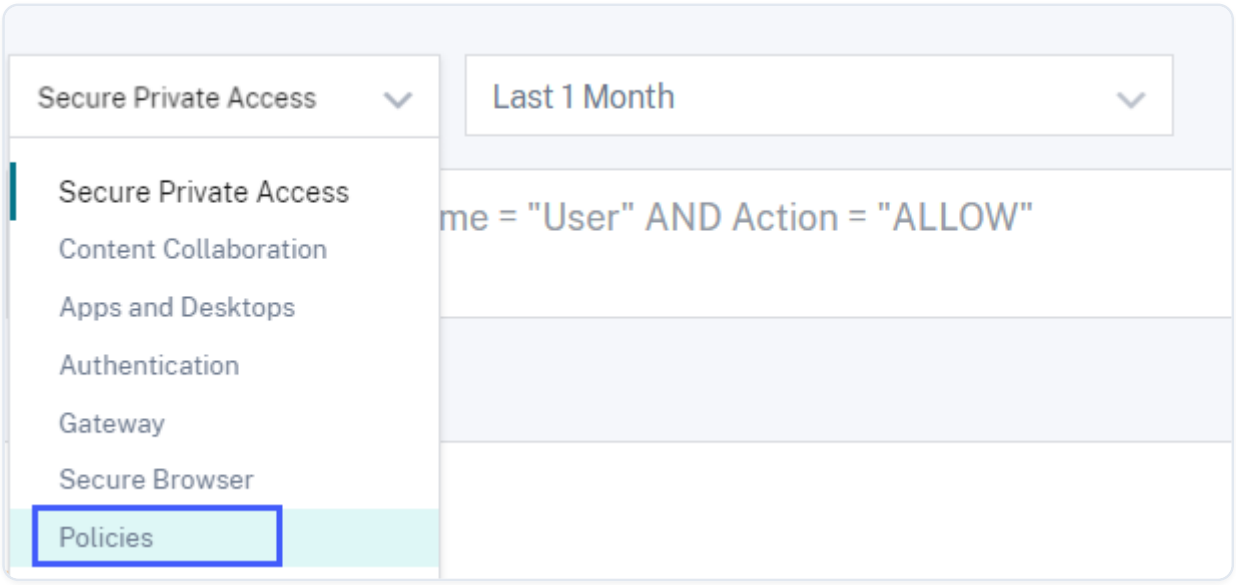
Self-service search for Policies

Citrix Analytics for Security allows you to create policies and apply actions on unusual or suspicious events on user accounts. When the user events meet your defined policies, the actions are automatically applied on the user accounts to isolate the threat and prevent future anomalous events from occurring. Using the self-service search, you can view the user events that have met your defined policies and view the actions applied on these anomalous events.

For more information on the search functionalities, see **Self-service search**.

Select the Policies data set

To view the events related to the defined policies, select **Policies** from the list. By default, the self-service page displays the events for the last one day. You can also select the time period for which you want to view the events.



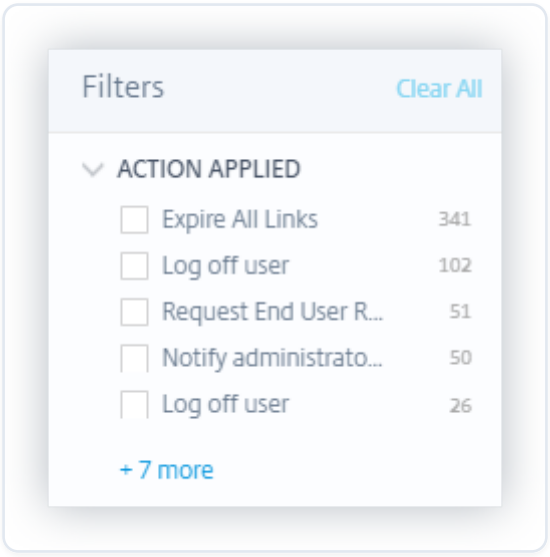
NOTE

You can also access the Self-service search for Policies page from the **Security** > **Users** > **Policies and Actions** dashboard. Select a policy on the dashboard to view the user events related to the policy. For more information, see the Policies and Actions dashboard.

Select the facets to filter events

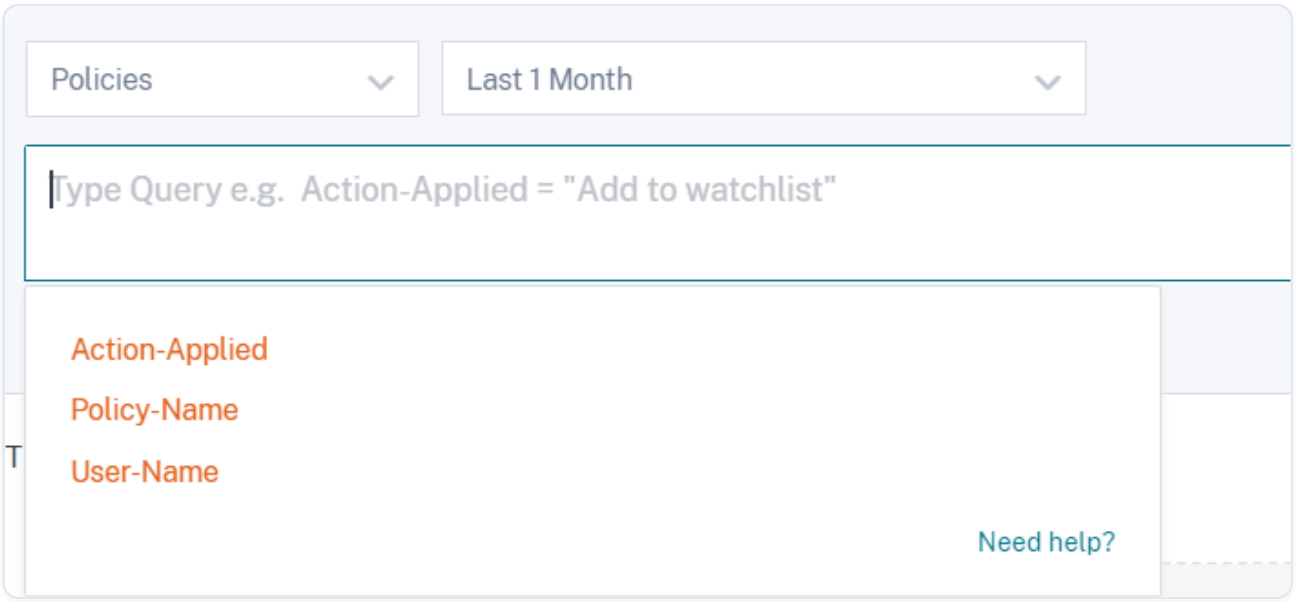
The facet list displays the applied actions on the user events. Select the applied actions from the facet list and view the events based on the applied actions. For more information on the actions that you can apply while configuring policies, see What are actions?

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



Specify search query to filter events

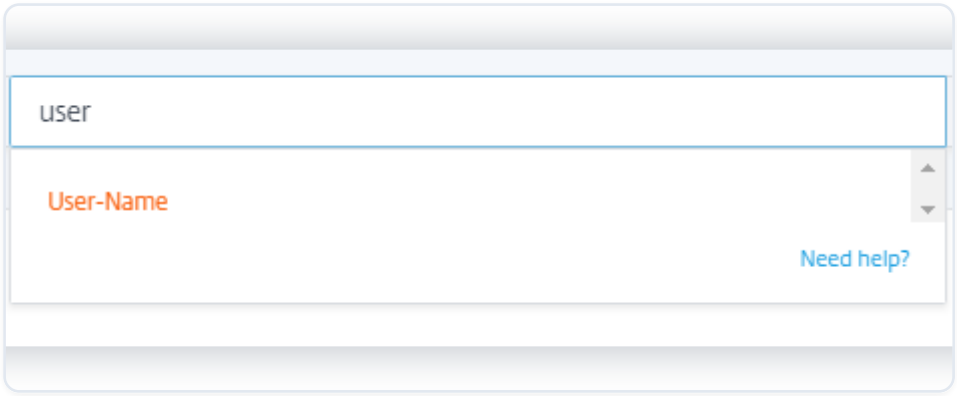
Place your cursor in the search box to view the list of dimensions for the events related to policies. Use the dimensions and the operators to specify your query and search for the required events.



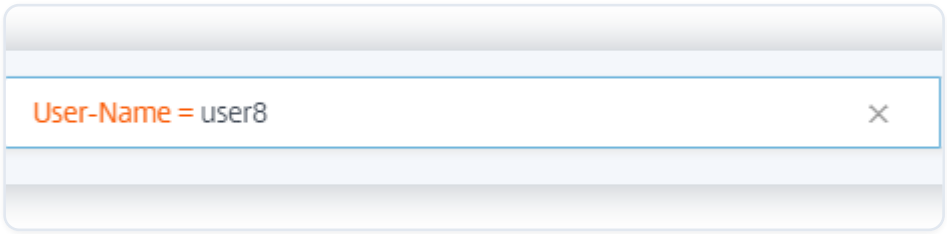
For example, you want to view the anomalous events of a user "user8" where the action applied for those events is "Disable user."

1. Enter "user" in the search box to get the related dimensions.

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



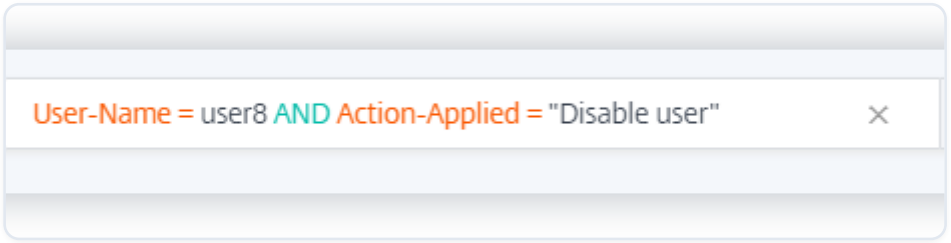
2. Select **User-Name** and enter the value "user8" using the equal operator.



3. Select the **AND** operator and then select the **Action-Applied** dimension. Enter the string "Disable user" for **Action-Applied** using the equal operator.

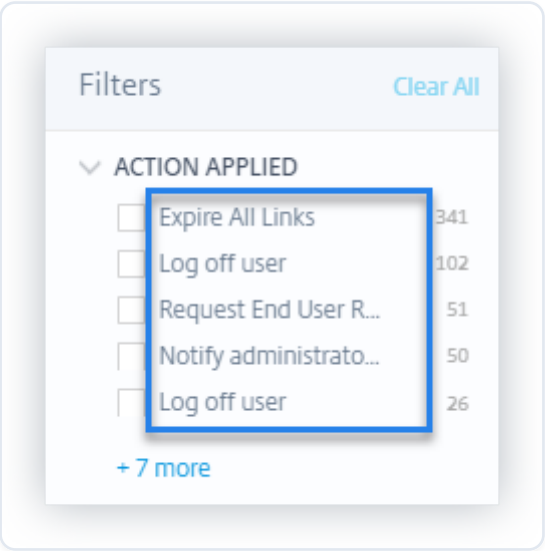
NOTE

If the string value contains two or more words, it must be enclosed with the operator `“”`. For example, `“Disable user”`, "Stop Session Recording".



To identify the possible string values for **Action-Applied**, expand the facet list and use the filter name as the string in your search query.

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



4. Select the time period and click **Search** to view the events on the **DATA** table.

Self-service search for Remote Browser Isolation (Secure Browser)

Use the self-service search to get insights into the browsing sessions of the Citrix Workspace™ users who are using the Citrix Remote Browser Isolation™ Service. Citrix Remote Browser Isolation is a cloud service that provides a safe internet browsing experience without compromising your corporate network security. When users access web applications using the Remote Browser Isolation, events such as session connect, session launch, published applications, and deleted applications are generated for each user connection. Citrix Analytics for Security receives these events and displays them on the self-service page. You can track the users and their browsing sessions.

For more information on the search functionalities, see **Self-service search**.

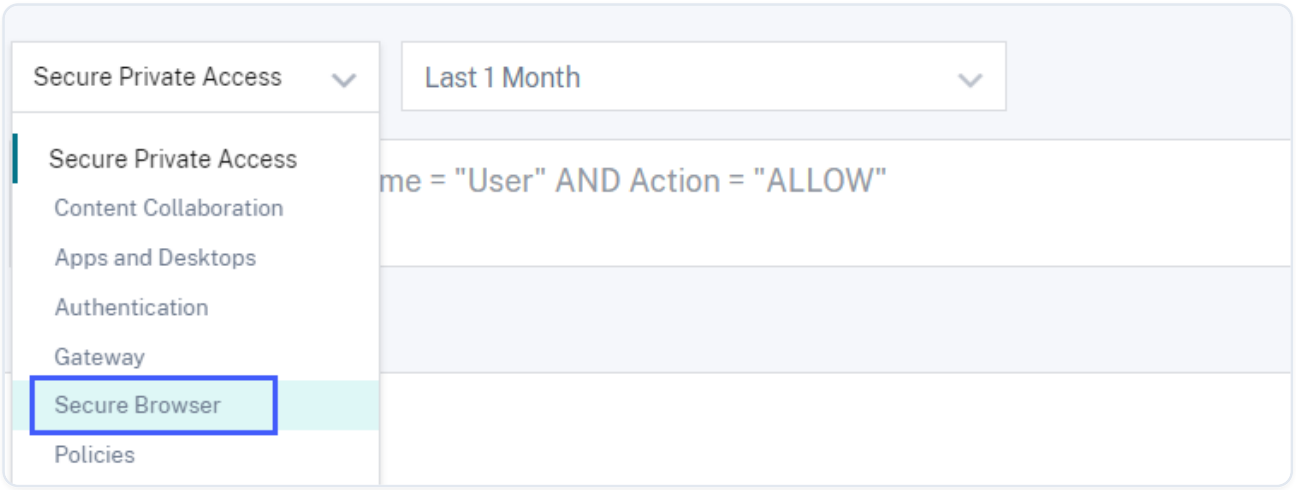
Prerequisite

To receive events from a Remote Browser Isolation, enable **Hostname tracking** in the Remote Browser Isolation to log host names for the user sessions. This information is sent to Citrix Analytics for Security. For more information, see Manage published Remote Browser Isolations.

Select the Remote Browser Isolation data source

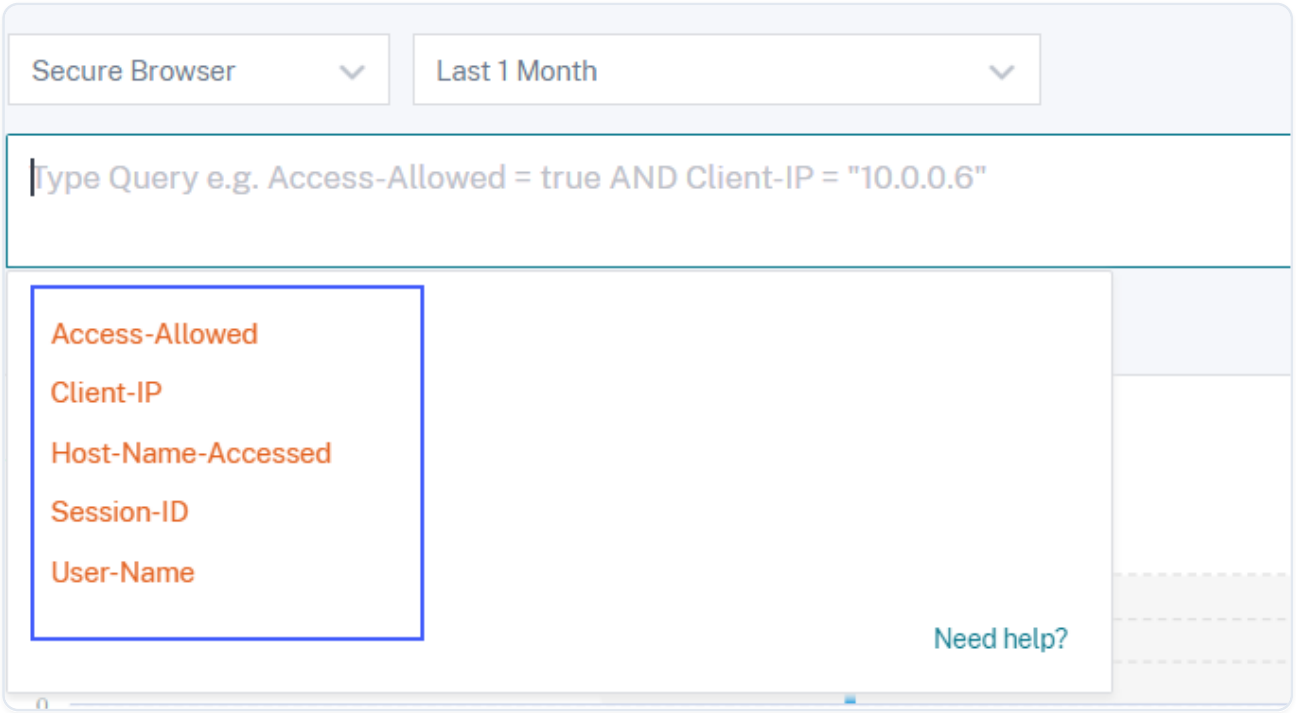
To view the Remote Browser Isolation events, select **Remote Browser Isolation** from the list. By default, the self-service page displays the events for the last one day. You can also select the time period for which you want to view the events.

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



Specify search query to filter events

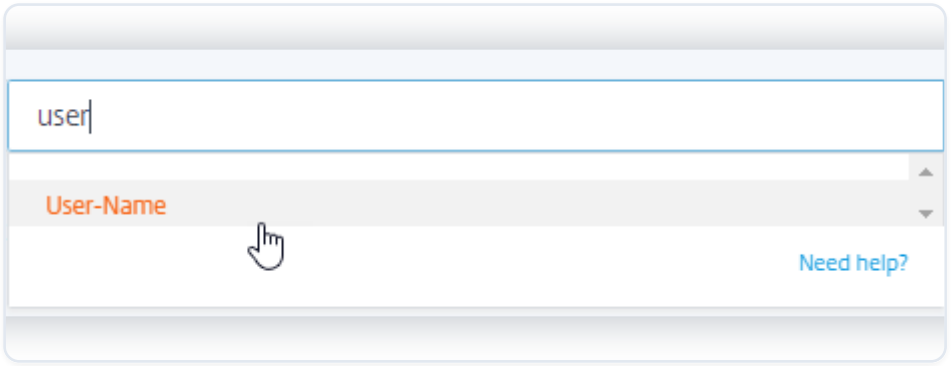
Place your cursor in the search box to view the list of dimensions for the Remote Browser Isolation events. Use the dimensions and the operators to specify your query and search for the required events.



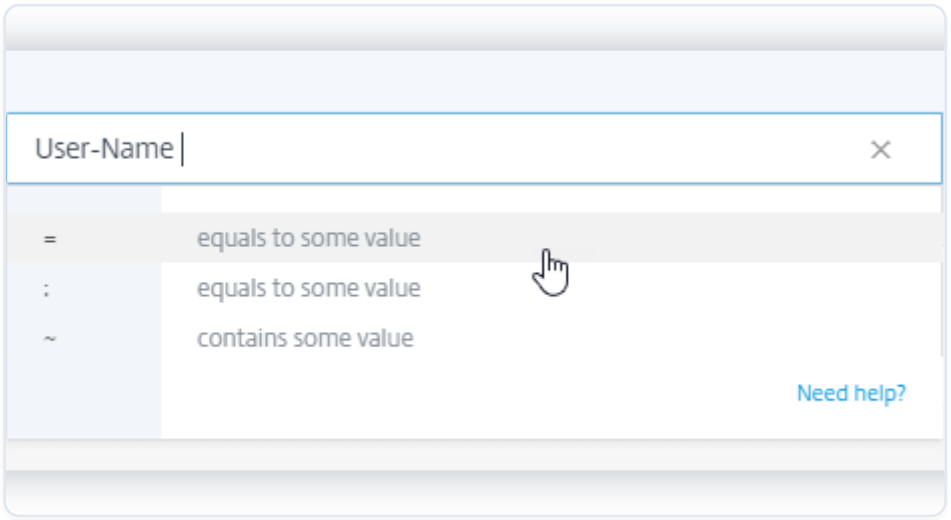
For example, you want to view the browsing event details for a user "aa" who has permission to access various host services such as google.com, amazon.com.

1. Enter "user" in the search box to view the related dimensions.

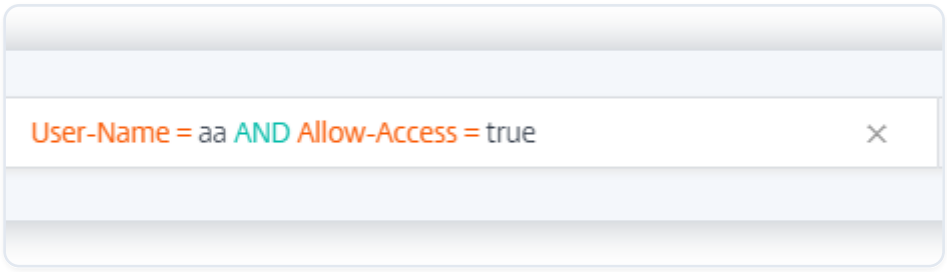
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Click **User-Name** and enter the value "aa" using the equal operator.



3. Select the **AND** operator and the **Allow-Access** dimension. Assign the value "true" to **Allow-Access** using the equal operator. The "true" value indicates that the user can access the host services.



4. Select the time period and click **Search** to view the events on the **DATA** table.

View user event details

You can view the following data received from the Remote Browser Isolation service:

- **Time**- Date and time when the user event occurred.
- **User name**- The user who initiated the event.
- **Session ID**- The unique number assigned to the user session.
- **Client IP**- IP address of the user device.

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

- **Host name**- The host service accessed by the user over the network.
- **Allow access**- The user is allowed or denied access to the host service.

Self-service search for Secure Private Access

Use the self-service search to get insights into the access events of the Citrix Cloud users in your organization. Examples of access events are url category, content category, browsers, and devices. Citrix Analytics for Security™ receives these events from the Secure Private Access service and displays them on the self-service search. You can track the users and their access details.

For more information on the search functionalities, see **Self-service search**.

NOTE

The following capabilities on Citrix Analytics for Security are impacted due to the deprecation of Category-based web filtering by Secure Private Access:

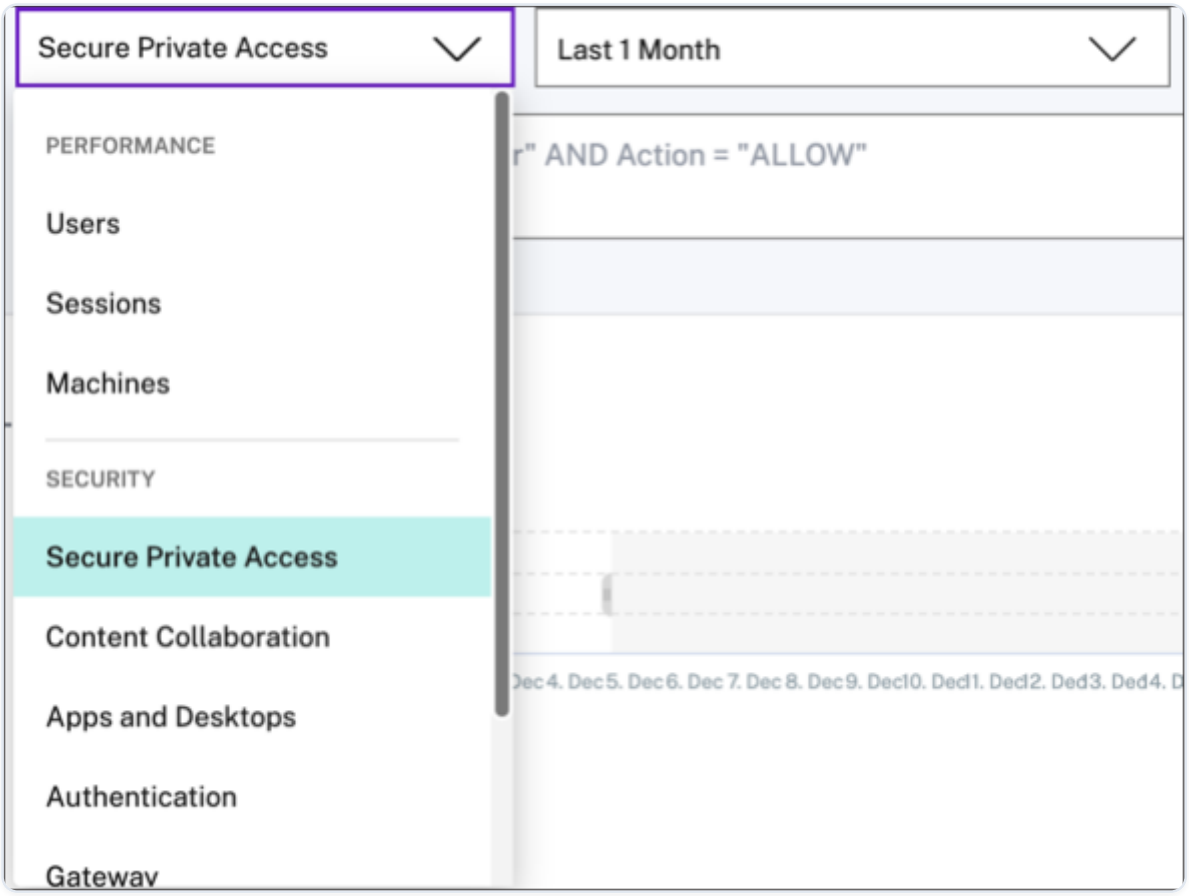
1. Data fields such as Category-Group, Category and Reputation of URLs are not available anymore on the Citrix Analytics for security dashboard.
2. The Risky website access indicator which relies on the same data is also deprecated and is not triggered for customers.
3. Any existing custom risk indicators using the data fields (Category-Group, Category and Reputation of URLs) and its associated policies are not triggered anymore.

For details on the deprecation from Secure Private Access, refer to Feature deprecations.

Select the Secure Private Access data source

To view the Secure Private Access events, select **Secure Private Access** from the list. By default, the self-service page displays the events for the last one day. You can also select the time period for which you want to view the events.

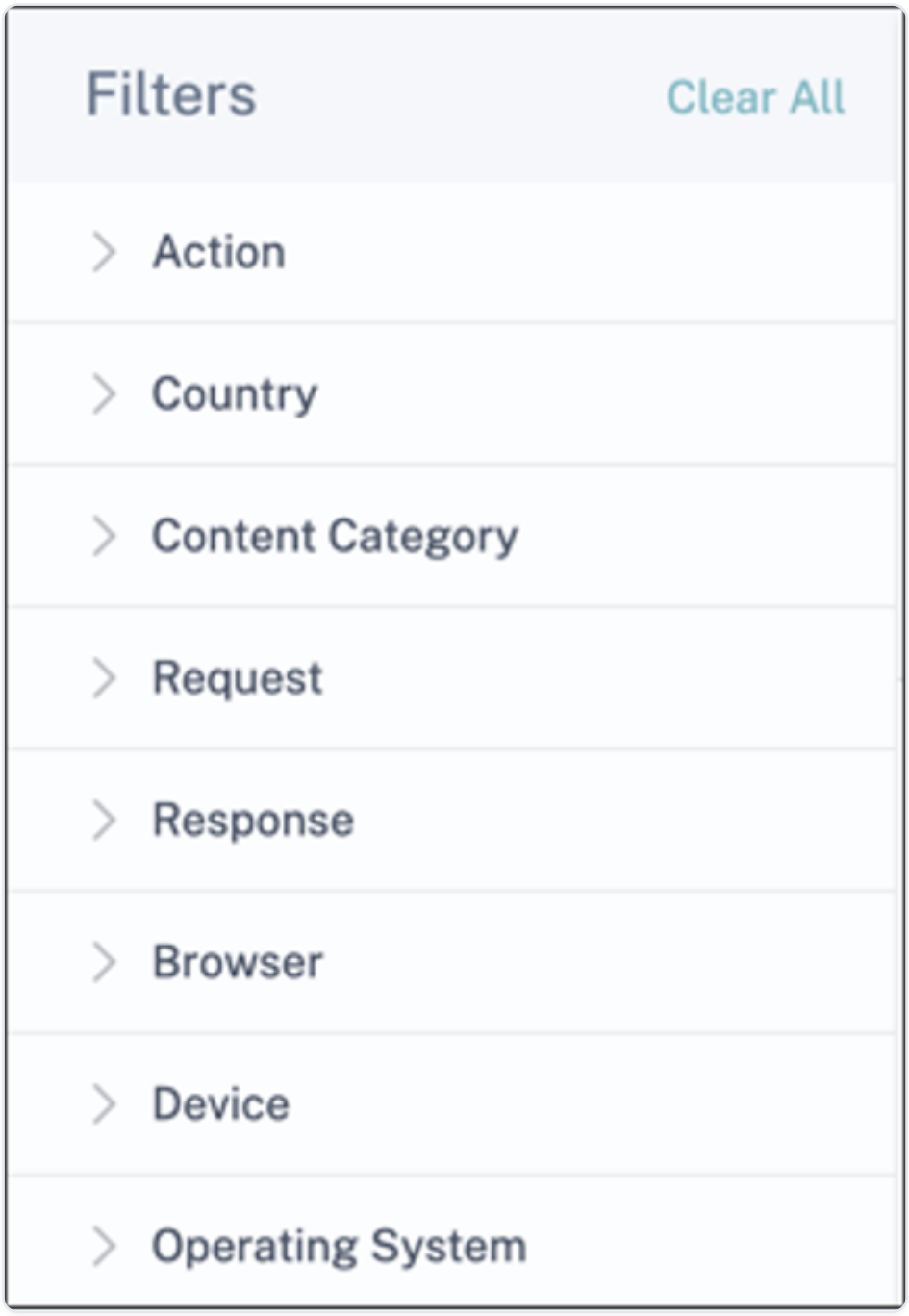
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Select the facets to filter events

Use the following facets that are associated to the Secure Private Access events.

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



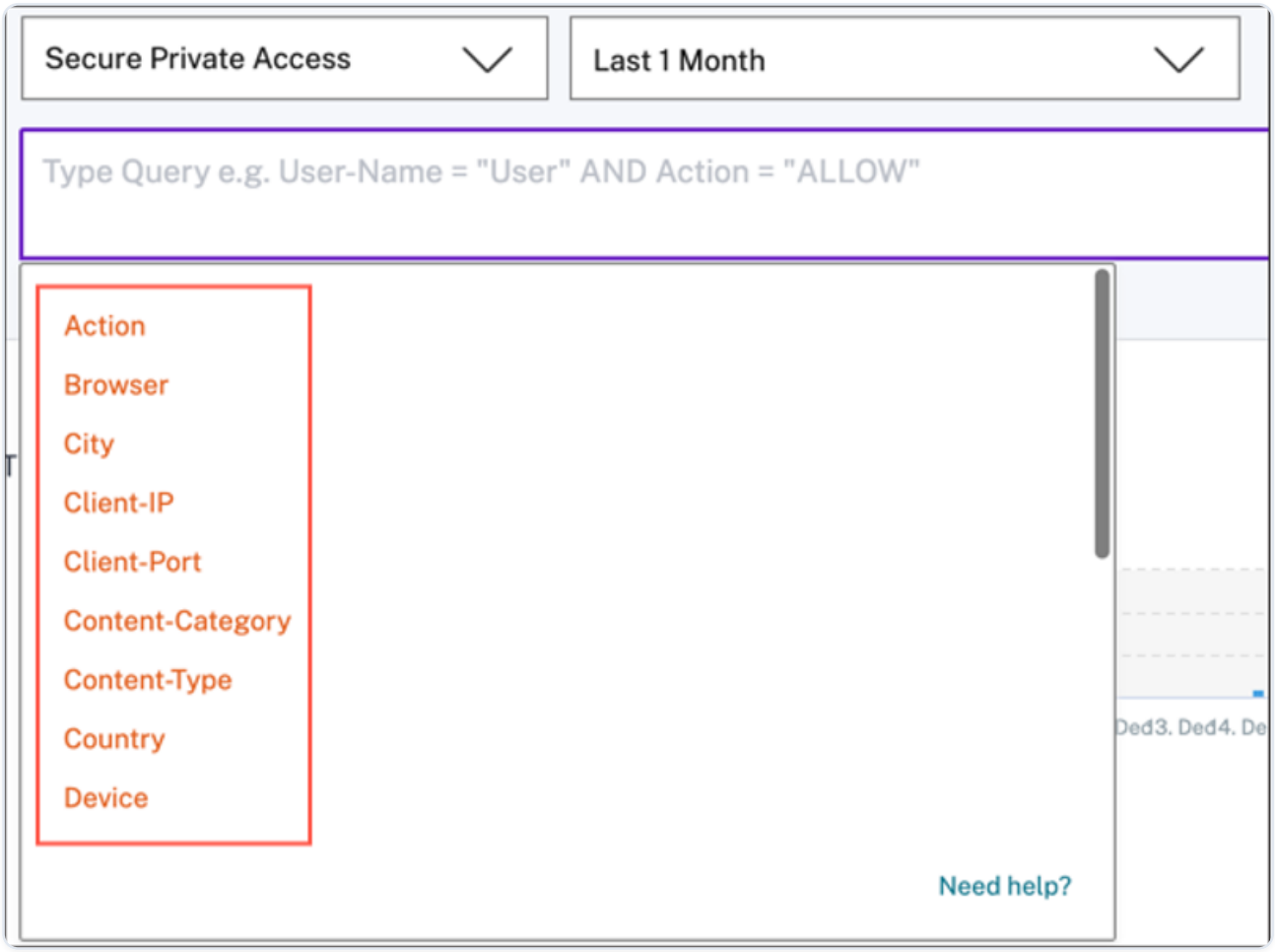
- **Action**- Search events based on the actions taken on users' applications such as allow, block, and redirect.
- **Country**- Search events based on the users' access locations.
- **Content Category**- Search events based on the categories of contents accessed such as application, image, and text.
- **Request**- Search events based on the HTTP methods such as GET, POST, PUT, DELETE.
- **Response**- Search events based on the HTTP response.
- **Browser**- Search events based on the browsers used by the users.

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

- **Device**- Search events based on the devices used such as Android phones, iPhones, MacBook.
- **Operating System**- Search events based on the operating systems installed on the devices.

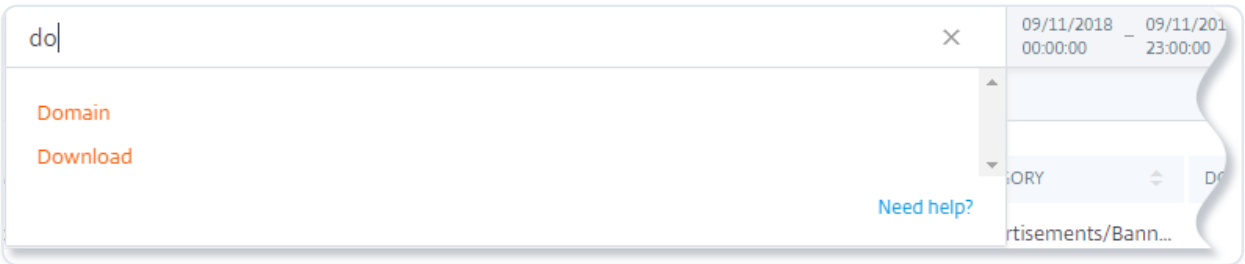
Specify search query to filter events

Place your cursor in the search box to view the list of dimensions for the Secure Private Access events. Use the dimensions and the operators to specify your query and search for the required events.



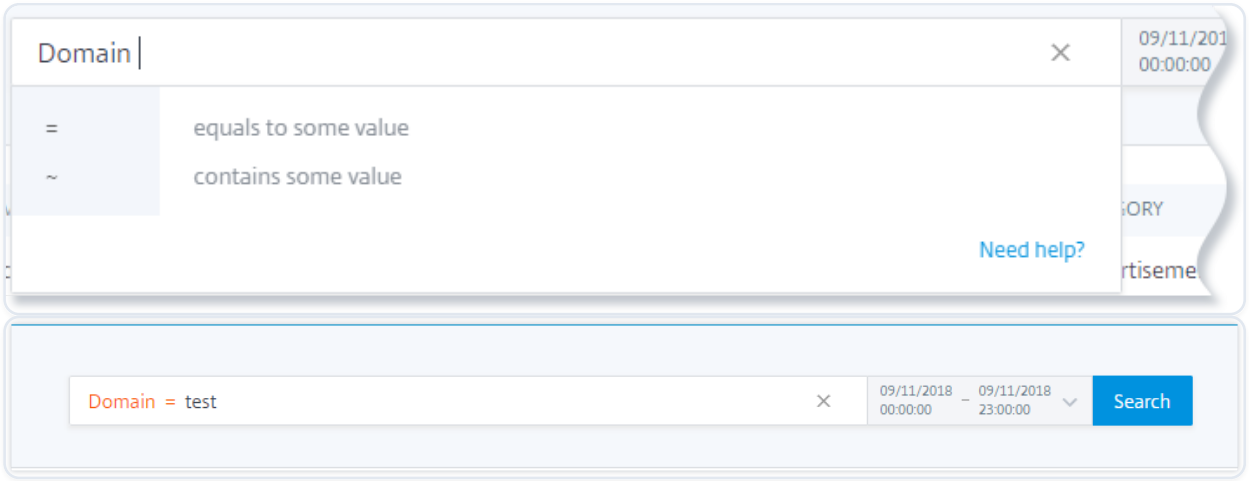
For example, you want to view the test domains where the data download volume is more than 2,000 Bytes. Specify your search query as the following:

1. Enter "do" in the search box to get the related suggestions.

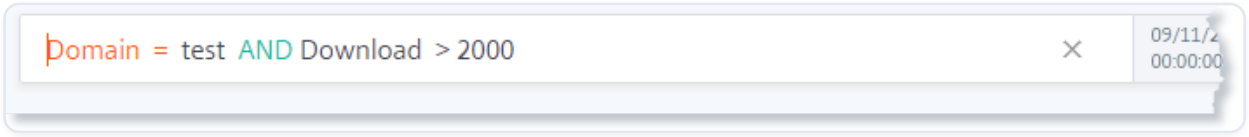


© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click **Domain** and then specify the value "test" using the equal operator.



3. Use the **AND** operator and then select the **Download** dimension. Select the **>** operator and enter the download volume in bytes.



4. Select the time period and click **Search** to view the events on the **DATA** table.

Self-service search for Apps and Desktops

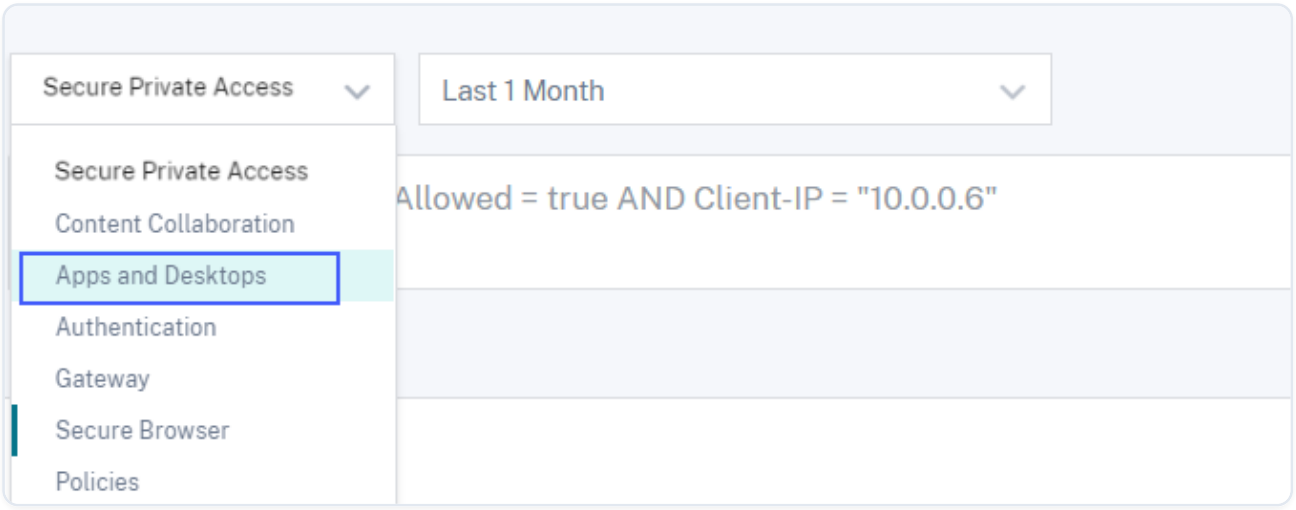
Use the self-service search to get insights into the user events received from the {{page.cvad-onprem-product-name}} data source and the {{page.daas-product-name}} (formerly Citrix Virtual Apps and Desktops service) data source. When users use virtual apps or virtual desktops, events corresponding to their activities and actions are generated. Examples of user events are file download, account logon, and app start. Citrix Analytics for Security receives these user events and displays them on the self-service page. You can track the users and their activities.

For more information on the search functionalities, see **Self-service search**.

Select the Apps and Desktops data source

To view the events from {{page.cvad-onprem-product-name}} or {{page.daas-product-name}}, select **Apps and Desktops** from the list. By default, the self-service page displays the events for the last one day. You can also select the time period for which you want to view the events.

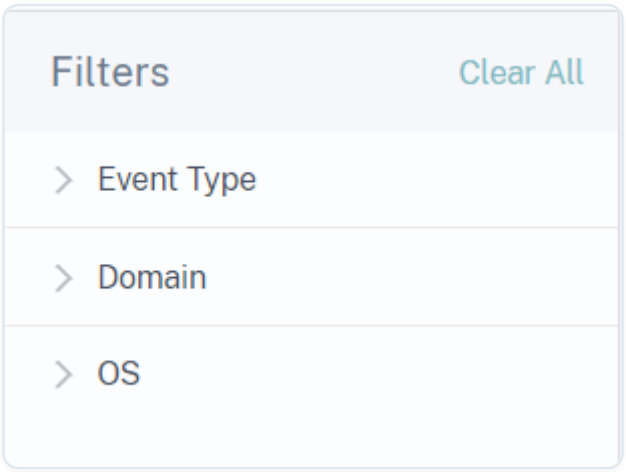
© 1997–2026 Citrix Systems, Inc. All rights reserved.



By default, the self-service page displays the events for the last one month. The page also provides you with several facets and a search box to filter and focus on the required events.

Select the facets to filter events

Use the following facets that are associated to the Apps and Desktops events.

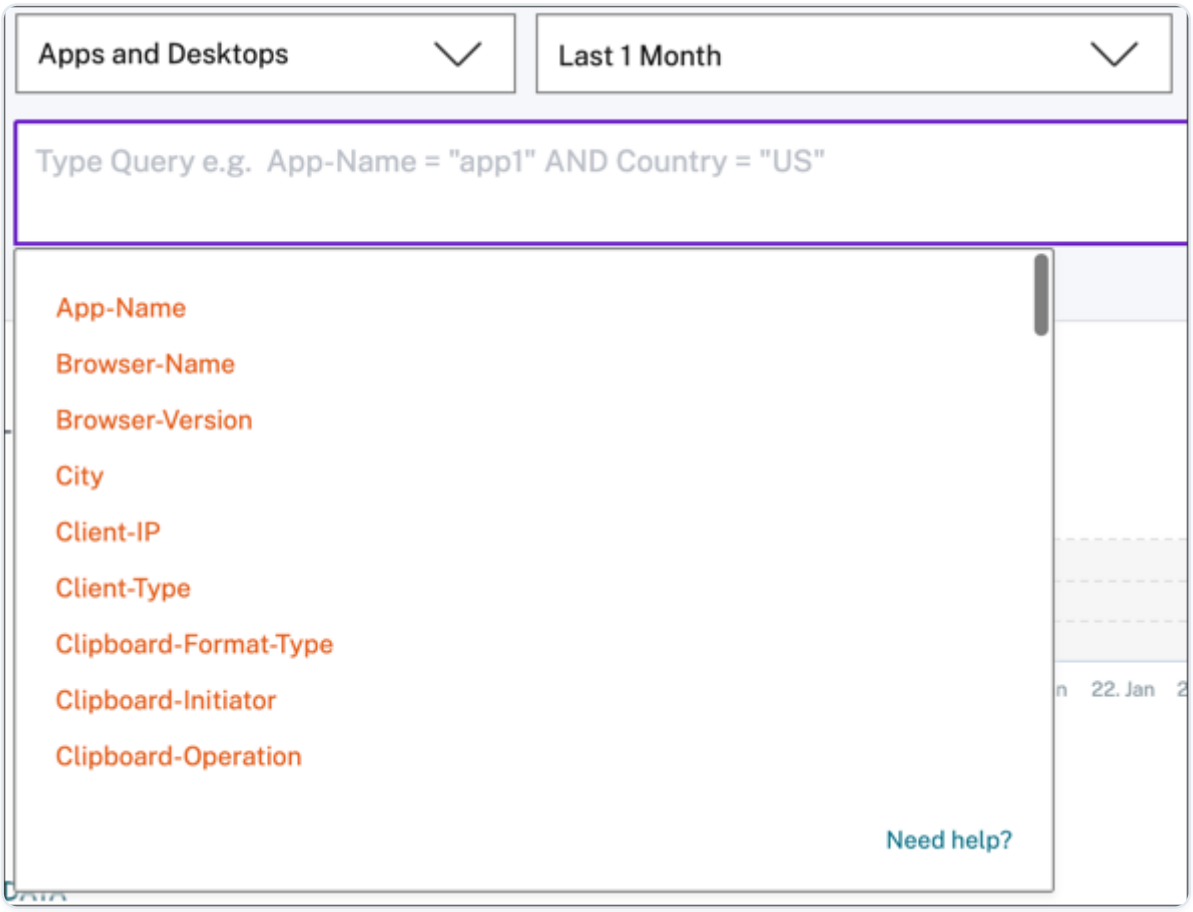


- **Event Type**- Search events based on the event type such as account logon, app end, and session end.
- **Domain**- Search events based on the domains such as citrate.net.
- **OS**- Search events based on the operating systems such as Chrome, iOS, and Windows used in the user's device. Select the operating system name and versions to filter the events. For more information on the operating system versions, see Supported values for your search query.

Specify search query to filter events

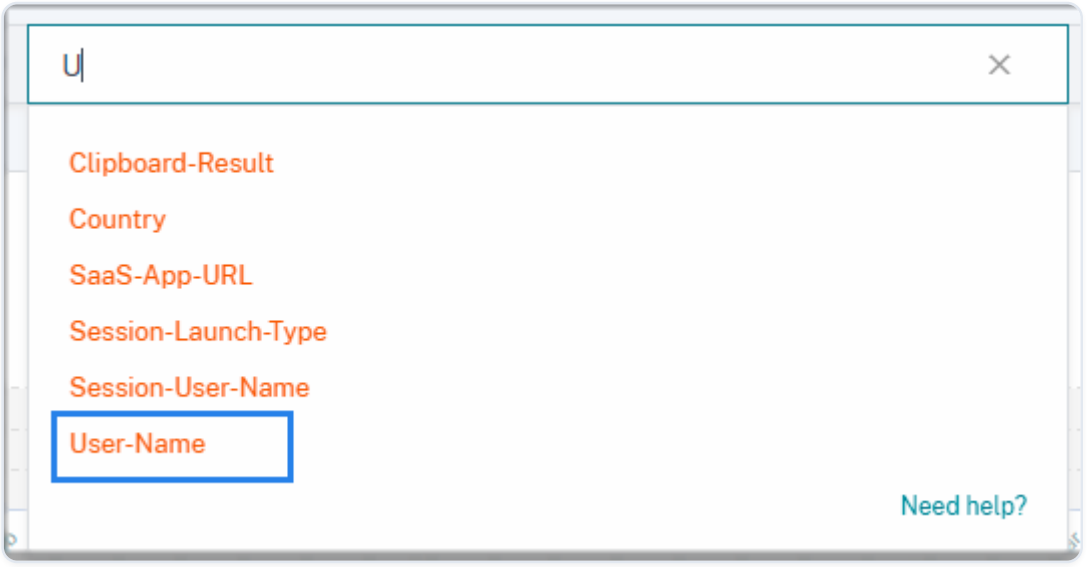
Place your cursor in the search box to view the list of dimensions for the Apps and Desktops events. Use the dimensions and the operators to specify your query and search for the required events.

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



For example, you want to search events for the user "John Doe" who is using the Windows operating system.

1. Enter "U" in the search box to get the related suggestions.



2. Click **User-Name** and enter the value "John" using the equal operator.

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



3. Select the **AND** operator and the **OS-Name** dimension. Assign the value "Windows 7" using the equal operator.

```
User-Name = "John" AND OS-Name = "Windows 7"
```

4. Select the time period and click **Search** to view the events based on the **DATA** table.

Event types and supported fields

The following fields are available for all the event types except VDA.Print:

- City
- Client IP
- Country
- Device ID
- OS Name
- OS Version
- OS Extra Info
- Time
- User Name
- Workspace App Version
- Workspace App Status

The following table describes the event types available for the Apps and Desktops data source and fields specific to each event type.

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

VALUE	DESCRIPTION	FIELDS
`Account.Logon`	Triggers when you log on to Store through Citrix Workspace app. **Note**: Account.Logon is not available for the HTML5 client.	Check common fields as described above.
`Session.Logon`	Triggers when you log on to your virtual session.	App Protection Policies, Domain, Session Launch Type, Session Server Name, Session User Name
`Session.End`	Triggers when you terminate your virtual session.	Domain, Session Launch Type, Session Server Name, Session User Name
`App.Start`	Triggers when you start a virtual app session. **Note**: This event type is not applicable when the application is launched within the desktop session.	App Name, Domain, Session Launch Type, Session Server Name, Session User Name
`App.End`	Triggers when you terminate a virtual app session. **Note**: This event type is not applicable when the application is launched within the desktop session.	App Name, Domain, Session Launch Type, Session Server Name, Session User Name
`File.Download`	Triggers when a user copies a file from remote virtual session to client device. It doesn't get triggered for file transfers happening within the virtual sessions. **Note**: This event type is sent only when the server allows file redirection (check File Redirection Settings for more details) and client workspace	Domain, Download Device Type, Download File Name, Download File Path, Download File Size, Session Server Name, Session User Name

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

VALUE	DESCRIPTION	FIELDS
	File Access preference is set to **Read and Write**.	
`Printing`	Triggers when you print a file with the Citrix Workspace app launched session through a client printer. **Note**: There are two technical limitations with Citrix Workspace app that affect printing events. First, the Printed Document Name telemetry is not included in the printing event due to a known issue across all platform variants. Second, the Printed File Size telemetry is not included in the printing event for Windows because of another known technical limitation. To collect these data sets (file name/file size) use VDA.Print event. For more information, see Enabling print telemetry for Citrix DaaS.	Browser Name, Browser Version, Domain, Printer Name, Print File Format, Print File Size, Session Server Name, Session User Name
`AppProtection.ScreenCapture`	Triggers when a user tries to capture a screenshot while in a protected session. **Note**: For more information, see App Protection.	Protected App Titles, Screen Capture Tool Name, Screen Capture Tool Path
`App.SaaS.Launch`	Triggers when Citrix Workspace app launches a SaaS app in Citrix Enterprise Browser.	Browser Name, Browser Version, SaaS App Name, SaaS App URL
`App.SaaS.End`	Triggers when Citrix Workspace app closes a SaaS app in Citrix Enterprise Browser.	Browser Name, Browser Version, SaaS App URL

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

VALUE	DESCRIPTION	FIELDS
`App.SaaS.Clipboard`	Triggers when a clipboard operation is performed in Citrix Enterprise Browser.	Browser Name, Browser Version, Clipboard Details Format Size, Clipboard Details Format Type, Clipboard Details Initiator, Clipboard Details Result, Clipboard Operation, SaaS App URL
`App.SaaS.File.Download`	Triggers when a file is downloaded in Citrix Enterprise Browser.	Browser Name, Browser Version, Download Device Type, Download File Path, Download File Size
`App.SaaS.File.Print`	Triggers when print is initiated in Citrix Enterprise Browser.	Browser Name, Browser Version, Print File Name, SaaS App Name, SaaS App URL
`App.SaaS.Url.Navigate`	Triggers when Citrix Enterprise Browser navigates a URL.	Browser Name, Browser Version, SaaS App Name, SaaS App URL
`Citrix.EventMonitor.AppStart`	Triggers when an application added into the Session recording server's app monitoring list is started within a virtual desktop session.	App Name
`Citrix.EventMonitor.AppEnd`	Triggers when an application added into the Session recording server's app monitoring list) is stopped within a virtual desktop session.	App Name
`Citrix.EventMonitor.Clipboard`	Triggers when a clipboard action has been performed within a session recording.	Clipboard Data Format Type, Process Name, Window Title

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

VALUE	DESCRIPTION	FIELDS
`Citrix.EventMonitor.FileTransfer`	Triggers when a user transfers a file between a virtual desktop session and the user's machine.	File Size, Operation Direction (Host to Client, Client to Host), Source Path, Destination Path
`Citrix.EventMonitor.RegistryChange`	Triggers when a registry operation is performed. The possible registry operations are create, delete, rename, set value, and delete value.	Registry Operation, Registry Name, Registry Path, Process ID, Process File Path
`Citrix.EventMonitor.SessionEnd`	Triggers when a session recording ends.	Description
`Citrix.EventMonitor.SessionLaunch`	Triggers when a session recording has started.	Session Recording Type
`Citrix.EventMonitor.TopMost`	Triggers when topmost window changes.	App Name
`Citrix.EventMonitor.IdleStart`	Triggers when session becomes idle.	Check common fields as described above.
`Citrix.EventMonitor.IdleEnd`	Triggers when idle session ends.	Check common fields as described above.
`Citrix.EventMonitor.WebBrowsing`	Triggers when user interacts with webpages on browsers within a virtual desktop session.	App Name, URL
`Citrix.EventMonitor.FileCreate`	Triggers when a file or a folder is created in virtual desktop session inside the monitored file system path.	File Name, File Path, File Size
`Citrix.EventMonitor.FileRename`	Triggers when a file or a folder is renamed in a virtual desktop session inside the monitored file system path.	Check common fields as described above.

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

VALUE	DESCRIPTION	FIELDS
`Citrix.EventMonitor.FileMove`	Triggers when a file or a folder from the monitored file system path is moved in a virtual desktop session or between session hosts (VDAs) and client devices.	Check common fields as described above.
`Citrix.EventMonitor.FileDelete`	Triggers when a file or a folder inside the monitored file system path is deleted in a virtual desktop session.	File Name, File Path, File Size
`Citrix.EventMonitor.CDMUSBDriveAttach`	Triggers when a Client Drive Mapping (CDM) mapped USB mass storage device is inserted in a client from which the virtual Apps and Desktop Session is connected.	Check common fields as described above.
`Citrix.EventMonitor.GenericUSBDriveAttach`	Triggers when a Generic redirected USB mass storage device is inserted in a client from which the virtual Apps and Desktop Session is connected.	Check common fields as described above.
`Citrix.EventMonitor.RDPConnection`	Triggers when a user creates a remote desktop connection within a VDA machine.	Destination IP, Process ID
`Citrix.EventMonitor.UserAccountModification`	Triggers for all type of user account operations that are - account creation, enablement, disablement, deletion, name changes, and password modification.	Description, Target User Name
`VDA.Print`	Triggers when a print job is initiated in Apps and Desktops. **Note**: This event is only applicable for Citrix	Document User Name, Machine Name, Print File Name, Print File Size, Printer

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

VALUE	DESCRIPTION	FIELDS
	DaaS data source. For more information, see Enabling print telemetry for Citrix DaaS.	Name, Time, Total Copies Printed, Total Pages Printed
`VDA.Clipboard`	Triggers when a clipboard operation is performed in Apps and Desktops. **Note**: This event is only applicable for Citrix DaaS data source. For more information, see Enabling clipboard telemetry for Citrix DaaS.	Clipboard Format Type, Clipboard Operation, Clipboard Operation Direction, Clipboard Operation Permitted, Clipboard Size, Machine Name

NOTE

All the session recording events require the policy for logging their events to be enabled on Session Recording server. For more information, see Create a custom event detection policy.

Supported values for your search query

Enter the following values for the dimensions to define your search query.

DIMENSION	VALUE	TYPE	DESCRIPTION	
`App-Name`	Application or desktop sessions.	String	Name of an application or desktop launched.	
	Example application sessions: A session without farm name: `#Cloud - Excel 2016` And a session with the farm name:			

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

DIMENSION	VALUE	TYPE	DESCRIPTION	
	`XA65PROD#Concur`			
	Example desktop sessions: A session without farm name: `#SINXIAP0616$S1-1` And a session with the farm name: `XA65PROD#SINXIAP0616$S1-1`			
`App-Protection-Policies`	Example: `AntiScreenCaptureEnabled`	String	Active application protection policies for the session.	
`Browser-Name`	Example: Google Chrome, Citrix Enterprise Browser™, Microsoft Edge, FIREFOX, SAFARI	String	Browser name	
`Browser-Version`	Example: 80.0.3987.122, 101.0.9999.0	String	Browser version	
`City`	Examples: Santa Clara, Houston, Chicago	String	The city name of a user.	

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

DIMENSION	VALUE	TYPE	DESCRIPTION	
`Client-IP`	An IP address. Example: 10.10.10.10	String	IP address of the user endpoint.	
`Client-Type`	Android, Windows, Macintosh, Chrome, HTML5, Unix/ Linux, iOS, SessionRecordi ng, Monitor	String	Indicates different types of Citrix Workspace app based on the operating systems or original data-source.	
`Clipboard-Format-Type`	Examples: text, html, CF_UNICODET EXT	String	The data format copied to the clipboard.	
`Clipboard-Initiator`	Examples: Keyboard, context menu, javascript	String	Indicates how the clipboard operation was initiated. **Note**: Supported only by the SaaS applications.	
`Clipboard-Operation`	Copy, cut, paste, or place	String	Indicates which clipboard operation is performed. **Note**: The **place** operation indicates data being placed on the clipboard. This does not guarantee if the data in the clipboard was pasted or used	

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

DIMENSION	VALUE	TYPE	DESCRIPTION	
			by the client. This operation is supported only for VDA.Clipboard Event.	
`Clipboard-Operation-Direction`	Client To Host, Host To Client	String	Indicates the direction of clipboard operation. **Note**: Supported only by Apps and Desktop (Citrix DaaS™) Clipboard Operation.	
`Clipboard-Operation-Permitted`	Allowed or Denied	String	Indicates whether the clipboard operation is permitted in Apps and Desktop Session. **Note**: Supported only by Apps and Desktop (Citrix DaaS) Clipboard Operation.	
`Clipboard-Result`	Success or Blocked	String	Indicates the result of the clipboard operation. **Note**: Supported only by the SaaS applications.	

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

DIMENSION	VALUE	TYPE	DESCRIPTION	
`Clipboard-Size`	Examples: 10, 20	Number	Size of the data (in bytes) that is currently stored in the clipboard.	
`Country`	Examples: USA, India	String	The country name of a user.	
`Description`	**For `Citrix.EventMonitor.UserAccountModification` events**: A user account was created, a user account was enabled, an attempt was made to reset an account's password.	String	Describes about user account modification status such as, the account was created, deleted, renamed, or an attempt was made to reset the password.	
	For `Citrix.EventMonitor.SessionEnd` events: Unknown, Logoff, Rollover, Trigger, and Incomplete		Describes the reason for end of the session recording.	
`Destination-IP`	Example: 10.60.110.xxx	String	IP address of the remote desktop.	
`Destination-Path`	Example: \H$ \Desktop\Folder \example.txt	String	The final path of the file after the transfer is completed.	

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

DIMENSION	VALUE	TYPE	DESCRIPTION	
`Device-ID`	Example: cb781185-18ad-4f45-b75f	String	Device ID used for licensing, client name, or operating system hardware ID.	
`Domain`	Example: example.com	Structure	The domain name of a server that sent a request.	
`Download-Device-Type`	Examples: USB, Hard Disk Drive, RemoteDrive, cdrom, or browser downloads.	String	The device type where the file is downloaded or transferred.	
`Download-File-Format`	Example: txt, PDF, xlsx, docx	String	The format of the file downloaded.	
`Download-File-Name`	Example: example-file.txt	String	Name of the downloaded file.	
`Download-File-Path`	Example: C:\Users\admin\Desktop	String	The path of the downloaded file.	
`Download-File-Size`	Example: 8.05	Number	The size of the downloaded file in kilobytes.	
`Event-Type`	Account.Logon, Session.Logon, Session.End, App.Start, App.End,	String	For more details, see Event types and supported fields.	

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

DIMENSION	VALUE	TYPE	DESCRIPTION	
	File.Download, Printing, AppProtection. ScreenCapture, App.SaaS.Launch, App.SaaS.End, App.SaaS.Clipboard, App.SaaS.File. Download, App.SaaS.File. Print, App.SaaS.Url.Navigate, Citrix.EventMonitor.AppStart, Citrix.EventMonitor.AppEnd, Citrix.EventMonitor.TopMost, Citrix.EventMonitor.WebBrowsing, Citrix.EventMonitor.FileCreate, Citrix.EventMonitor.FileRename, Citrix.EventMonitor.FileMove, Citrix.EventMonitor.FileDelete, Citrix.EventMonitor.CDMUSBDriveAttach, Citrix.EventMonitor.GenericUSBDriveAttach, Citrix.EventMonitor.RDPConne			

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

DIMENSION	VALUE	TYPE	DESCRIPTION	
	ction, Citrix.EventMonitor.UserAccountModification, VDA.Print, VDA.Clipboard, Citrix.EventMonitor.RegistryChange, Citrix.EventMonitor.SessionLaunch, Citrix.EventMonitor.SessionEnd, Citrix.EventMonitor.Clipboard, Citrix.EventMonitor.FileTransfer			
`Jail-Broken`	Yes or No	String	Indicates if the device is rooted or not. **Note**: If this dimension is absent, the device is not rooted. This key applies to Citrix Workspace™ app for iOS and Android devices.	
`Operation-Direction`	Host to Client/ Client to Host	String	Indicates the direction of the file transfer.	
`OS-Extra-Info`	Example: 20G80, Service Pack 1, 19043	String	Indicates the additional information of the operating	

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

DIMENSION	VALUE	TYPE	DESCRIPTION	
			system such as build numbers, service packs, and patches.	
`OS-Name`	Example: macOS 11, Windows 7, Android 8.1, Windows 10 Enterprise	String	Indicates the name of the operating system.	
`OS-Version`	Example: 11.5.1, 14.7.1, 2009	String	Indicates the version of the operating system	
`Print-File-Format`	Examples: PDF, PS, DOCX	String	Format of the printed file.	
`Print-File-Name`	Example: example-file.pdf	String	Name of the printed file.	
`Print-File-Size`	Examples: 10, 20	String	Size of the printed file in bytes.	
`Printer-Name`	Example: testprinter-1	String	Name of the printer used.	
`Process-ID`	Example: 11248	String	Refers to the process ID that is used to identify the specific process that performs two actions: **Creating a new process** and **Making a remote desktop**	

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

DIMENSION	VALUE	TYPE	DESCRIPTION	
			connection. Process-ID is currently associated only with Citrix.EventMonitor.RDPConnection event.	
`Protected-App-Titles`	Example: Admin Desktop - Citrix Workspace	String	Name of the application running in the protected session.	
`Registry-Name`	Name of the modified registry	String	The name of the registry that was modified.	
`Registry-Operation`	Rename, Create, Delete, SetValue, DeleteValue	String	Indicates which registry operation was performed.	
`Registry-Path`	Path of the modified registry	String	The path of the registry that was modified.	
`SaaS-App-Name`	Example: Workday	String	Name of the SaaS application.	
`SaaS-App-URL`	Example: `https://xyz.com	String`	String	URL of the SaaS application or gateway/proxy URL. **Note**: The gateway/proxy URL appears in the App.SaaS.Launch Event when

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

DIMENSION	VALUE	TYPE	DESCRIPTION	
				the SaaS application is launched initially.
`Screen-Capture-Tool-Name`	Example: ScreenShotTool.exe	String	Name of the screen capture tool.	
`Screen-Capture-Tool-Path`	Example: c:\Program files (x86)\ScreenContent Client	String	Path of the screen capture tool.	
`Session-Launch-Type`	Application or Desktop	String	Indicates if the launched session is an application or desktop type.	
`Session-Recording-Type`	Traditional recording/ Event only recording	String	Indicates the type of the launched session recording.	
`Session-Server-Name`	Examples: Hosted Desktop, Cloud-VDA-1	String	Name of the application or desktop connected to as received from a server.	
`Session-User-Name`	Examples: demo-user, test-user	String	User name received from the server.	
`Source-Path`	Example: C:\Users\admin\Desktop\example.txt	String	The initial path of the file before it was transferred.	

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

DIMENSION	VALUE	TYPE	DESCRIPTION	
`Target-User-Name`	Examples: user01	String	Currently, the Target-User-Name is only used for the Citrix.EventMonitor.UserAccountModification event, in which it's the user account which was modified.	
`Total-Copies-Printed`	Examples: 1, 2	Number	Total number of copies printed by the user.	
`Total-Pages-Printed`	Examples: 1,2	Number	Total number of the document pages printed by the user.	
`User-Name`	user name or Domain\username	String	The user name or domain\username. Used for StoreFront login. If the StoreFront logon is not through Citrix Workspace app for HTML5 or Chrome, then this value is same as the one received from server.	

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

DIMENSION	VALUE	TYPE	DESCRIPTION	
`VDA-Name`	Example: TSVDA-19-01.xd.local	String	Indicates the name of the VDA machine.	
`Window-Title`	Example: Administrator - 01 Command Prompt	String	Indicates the title of the window in which the clipboard operation was performed.	
`Workspace-App-Version`	Example: 20.8.0.3 (2008)	String	Citrix Workspace app or Citrix Receiver version installed on the user's device and used to launch remote virtual Apps and Desktop Sessions.	
`Workspace-App-Status`	Supported or Unsupported	String	Indicates whether the installed version of Citrix Workspace app or Citrix Receiver on the user's device is supported or not supported by Citrix Analytics for Security. Hover over **Unsupported** when the	

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

DIMENSION	VALUE	TYPE	DESCRIPTION	
			Workspace App is not supported. A pop-up window appears with a link to view the list of supported versions. When a Workspace App version is approaching its unsupported status, a banner is displayed on the self-service search page, listing the available supported versions to which you can initiate an upgrade.	

Operating system naming format

Citrix Analytics receives the operating system (OS) details of a user device and translates them into OS Name, OS Version, and OS Extra Info.

- **OS Name** indicates the name of the operating system.
- **OS Version** indicates the release ID or the release version of the operating system.
- **OS Extra Info** indicates the additional information of the operating system such as build numbers, service packs, and patches.

The following table provides a few examples of the version numbering format of operating systems.

OS NAME	OS VERSION	OS EXTRA INFO
macOS 11	11.5.1	20G80

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

OS NAME	OS VERSION	OS EXTRA INFO
iOS 14	14.7.1	Not Available
Windows 10 Enterprise	2009	19043
Windows 7	6.1	Service Pack 1
Android 8.1	8.1.0	Not Available

NOTES

- To get the OS details for Mac version 11.x or later, the recommended client version is Citrix Workspace app for Mac 2108 or later.
- The OS details for Windows 10 are currently not available.

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

Troubleshoot Citrix Analytics for Security and Performance

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance.md

Verify anonymous users as legitimate users

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/anonymous-users-issue.md

Troubleshoot event transmission issues from a data source

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/datasource-events-transmission-issue.md

Trigger Virtual Apps and Desktops events, SaaS events, and verifying event transmission

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/virtual-apps-desktops-saas-events-verify.md

No user events received from supported Citrix Workspace™ app version

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/workspace-app-partially-supported.md

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

Configured Session Recording server fails to connect

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/session-recording-issue.md

Unable to connect StoreFront™ server with Citrix Analytics

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/storefront-issue.md

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

FAQs

layout: doc replicate-from: commons/faqs.md

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

Glossary of terms

layout: doc replicate-from: commons/glossary.md

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

Security Analytics Document History

The following table describes important changes to the Security Analytics documentation. To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	REFERENCE
18 Jun 2024	Added Azure AD or Active Directory note related to Microsoft Entra	Added a note on Microsoft Entra.Learn more
15 Apr 2024	Added Executive Summary report	Added Executive Summary report.Learn more
29 Jan 2024	Updated Workspace App status fields	Updated the Workspace App status fields.Learn more
25 Jan 2024	Addressed data gaps and inconsistencies in the UI	Updated What's New.Learn more
24 Jan 2024	Updated user profile events on SIEM environments	Updated user profile events on SIEM environments.Learn more
01 Dec 2023	Updated weekly email and SIEM alerts	Updated weekly email and SIEM alerts.Learn more
01 Dec 2023	Updated Users dashboard	Added active user count time filter and updated the **Overview** section in the **Users** dashboard.Learn more
01 Dec 2023	Updated What's New	Updated **Custom reports**.Learn more
30 Nov 2023	Removed ShareFile detection capabilities.	Removed ShareFile detection capabilities. Learn more

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

DATE	CHANGE	REFERENCE
31 Oct 2023	Added examples of Sigma Signatures	Added examples of Sigma Signatures for Security Insights.Learn more
22 Sep 2023	Updated What's New.	Added Citrix Secure Browser data source in **Custom Indicator**.Learn more
22 Sep 2023	Updated What's New.	Citrix Analytics for Security now honors the notification preferences set by custom administrators in Citrix Cloud. Learn more. Also, the Weekly email has been enhanced to provide deeper insight into your organization's security posture by enabling the SIEM data export.Learn more
04 Jul 2023	Updated What's New.	Added **OR** operator support in **Self-Service Search** and **Custom Indicator**.Learn more
15 Jun 2023	Updated What's New.	Added **Clipboard place metadata collection for Security monitoring** policy to enable or disable the clipboard telemetry.Learn more
14 Jun 2023	Updated What's New.	Added **App Lifecycle** and **Registry** events from **Session Recording** for Apps and Desktops data source.Learn more
29 May 2023	Updated What's New.	Added details on Citrix Analytics add-on vetted for Splunk Cloud.Learn more

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

DATE	CHANGE	REFERENCE
24 May 2023	Updated What's New.	Added a new global action under the Policies and Action article.Learn more
04 May 2023	Updated What's New.	Added Test Event Genaration and SIEM Email Alert capabilties.Learn more
31 Mar 2023	Updated What's New.	Added new events for Session Recording and updated other event types in Self-Service Search.Learn more
30 Mar 2023	Updated What's New.	Added troubleshooting information for the Data Exports feature.Learn more
30 Mar 2023	Updated What's New.	Updated custom roles support with Azure Active Directory or Active Directory Group.Learn more
24 Mar 2023	Updated What's New.	The auto-suggestion functionality for dimensions based on the tenant's historical data is now deprecated for Self-Service Search and Custom Risk Indicator pages.Learn more
24 Mar 2023	Updated What's New and the User Profile section.	**Users' profile data** related to Applications, Locations, and Devices data usage are not available on the **User Info** page in User's Timeline.Learn more
21 Mar 2023	Updated What's New.	Recommendations panel to help onboard on-premise

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

DATE	CHANGE	REFERENCE
		StoreFront data source.Learn more
22 Feb 2023	Updated What's New.	Enhancement to the Weekly email digest feature.Learn more
21 Feb 2023	Updated What's New.	Added Download File Format field for App.SaaS.File.Download event type and updated Browser-derived fields. Also, added content for **Enable VDA clipboard telemetry**.Learn more
14 Feb 2023	Updated What's New.	Added the deprecation notice for on-premises Delivery Controller.Learn more
03 Feb 2023	Updated What's New.	Updated the Data Sources article with the supported home regions.Learn more
11 Jan 2023	Updated What's New.	Updated the impacted articles as the Web filtering capability has been removed from Secure Private Access.Learn more
27 Dec 2022	Updated What's New.	Captured data source list change for Self-service Search.Learn more
13 Dec 2022	Updated What's New.	Added Users dashboard feature.Learn more
05 Dec 2022	Added a Known Issue and updated What's New.	Added Network profile feature and a Known Issue: CAS-70954.Learn more

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

DATE	CHANGE	REFERENCE
18 Nov 2022	Added Fixed issue.	Added fixed issue: CAS-73222.Learn more
09 Nov 2022	Updated What's New	Revised the what's new content for CAS-59564 and CAS-67143.Learn more
08 Nov 2022	Updated What's New	Renamed few actions and added three fixed issues.Learn more
19 Oct 2022	Updated What's New	Updated the Event type selection for SIEM details.Learn more
18 Oct 2022	Updated What's New	Updated the **Start session recording** action details.Learn more
14 Oct 2022	Updated What's New	Added **Provide feedback for User Risk indicators** feature.Learn more
28 Sep 2022	Updated Known issues	Added Known issue - CAS-72051.Learn more.
26 Sep 2022	Updated What's New	Added **Access Assurance to support geofence blocklist** feature and three fixed issues.Learn more
22 Sep 2022	Removed 2 known issues and updated 1.	Removed CAS-65377 and CAS-65378 known issues as the impacted events will not be visible in customers' UI and updated CAS-66897.
13 Sep 2022	Updated What's New	Added **Sharelink dashboard enhancement** feature content.Learn more.

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

DATE	CHANGE	REFERENCE
09 Sep 2022	Updated defalut policies along with the Indicator event details schema.	Added three default policies and two new fields in the **Indicator event details schema** for impossible travel risk indicator.Learn more.
19 Aug 2022	Updated What's new	Added Enable VDA Print telemetry feature. Learn more.
18 Aug 2022	Updated What's new	Added fixed issue-CAS-70361. Learn more.
17 Aug 2022	Added new feature and updated What's new	Added Customization of end-user email per policy feature.Learn more.
11 Aug 2022	Added new section under FAQ	Added Access assurance – Geolocation FAQ section.Learn more.
10 Aug 2022	Updated Known issues	Added known issue-CAS-67968.Learn more.
04 Aug 2022	Updated Known issues	Added known issue-CAS-69098.Learn more.
17 Jun 2022	Updated What's new	Updated the data processing of specific data sources.Learn more.
09 Jun 2022	Updated What's new	Added fixed issue-CAS-66593, CAS-66731. Learn more.
02 Jun 2022	Updated What's new	Added fixed issue-CAS-67105, CAS-66838. Learn more.

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

DATE	CHANGE	REFERENCE
24 May 2022	Updated What's new	Virtual Apps and Desktops renamed as Apps and Desktop. Learn more.
17 May 2022	Updated What's new	Virtual Apps and Desktops renamed as Apps and Desktop. Learn more.
28 Apr 2022	Updated Known issues	Added known issue- CAS-66897. Learn more.
05 Apr 2022	Updated What's new	Secure Workspace Access labels renamed as Secure Private Access. Learn more.
21 Mar 2022	Updated What's new	Added fixed issue- CAS-64126. Learn more.
10 Mar 2022	Updated What's new	Updates about the **Notify administrator email enhancements**. Learn more.
03 Mar 2022	Updated What's new	Updates about the **Request End User Response action**. Learn more.
03 Mar 2022	Updated Policies and actions	Updates about the **Request End User Response action**. Learn more.
24 Feb 2022	Added Citrix Analytics workbook for Microsoft Sentinel	Added how to use the workbook. Learn more.
23 Feb 2022	Updated What's new	Updates about recommended actions for a risk indicator. And added a fixed issue- CAS-62300. Learn more.

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

DATE	CHANGE	REFERENCE
23 Feb 2022	Updated Citrix Content Collaboration risk indicators	Added recommended actions for Unusual authentication failures. Learn more.
23 Feb 2022	Updated Citrix Gateway risk indicators	Added recommended actions for Unusual authentication failure. Learn more.
23 Feb 2022	Updated Citrix Virtual Apps and Desktops and Citrix DaaS risk indicators	Added recommended actions for Suspicious logon. Learn more.
17 Feb 2022	Updated What's new	Updates about the Virtual Apps and Desktops events and Content Collaboration dimensions. Learn more.
17 Feb 2022	Updated Self-service search for Content Collaboration	Added new dimensions. Learn more.
10 Feb 2022	Updated Custom risk indicators	Added the auto-suggest feature in the condition bar. Learn more.
09 Feb 2022	Updated Manage administrator roles for Security Analytics	Added new custom roles. Learn more.
28 Jan 2022	Updated What's new	Updates about Suspicious logon for Content Collaboration and Gateway. Learn more.
28 Jan 2022	Updated Citrix Content Collaboration risk indicators	Added the Suspicious logon risk indicator. Learn more.
28 Jan 2022	Updated Citrix Gateway risk indicators	Added the Suspicious logon risk indicator. Learn more.
28 Jan 2022	Updated Citrix Analytics data format for SIEM	Added schema for Suspicious logon associated with

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

DATE	CHANGE	REFERENCE
		Content Collaboration and Gateway. Learn more.
27 Jan 2022	Updated Troubleshoot Citrix Analytics for Security	Added debugging steps for issues with Citrix Analytics add-on for Splunk. Learn more.
20 Jan 2022	Updated What's new	Support for Azure Active Directory integration. Learn more.
20 Jan 2022	Updated Microsoft Active Directory and Azure Active Directory integration	Added Azure Active Directory integration steps. Learn more.
18 Jan 2022	Updated What's new	Update about the Share link actions and SIEM integration. Learn more.
18 Jan 2022	Updated Content Collaboration risk indicators	Apply share link actions (Expire all links and Change link to view-only sharing) on all risk indicators. Learn more.
18 Jan 2022	Updated Policies and actions	Updated the descriptions of the *Expire all links* and *Change link to view-only sharing* actions. Learn more.
01 Jan 2022	Updated Known issues	Added the known issue-CAS-63093. Learn more.
24 Dec 2021	Updated Known issues	Added the known issue-CAS-62842. Learn more.
23 Dec 2021	Updated What's new	Share link risk indicator enhancements. Learn more.
23 Dec 2021	Updated Citrix share link risk indicators	Renamed share link risk indicators. Learn more.

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

DATE	CHANGE	REFERENCE
23 Dec 2021	Share Link risk timeline	Renamed share link risk indicators. Learn more.
21 Dec 2021	Updated What's new	Added a feature-email distribution list. Learn more.
21 Dec 2021	Added Email distribution list	Added information about the email distribution list. Learn more.
20 Dec 2021	Updated What's new	Update about the Request End User Response action and the Access Control labels. Learn more.
20 Dec 2021	Updated Policies and actions	Updated the prerequisites for the Request End User Response action. Learn more.
13 Dec 2021	Added Citrix Remote Browser Isolation data source	Added information about the Remote Browser Isolation integration. Learn more.
09 Dec 2021	Updated What's new	Added custom risk indicator templates. Learn more.
09 Dec 2021	Updated Custom risk indicators	Added how to use a template. Learn more.
09 Dec 2021	Updated Citrix Content Collaboration data source	Added prerequisite for the Asia Pacific South region. Learn more.
09 Dec 2021	Updated Known issues	Added Known issues- CAS-62317 and CAS-62299. Learn more.
08 Dec 2021	Updated Splunk integration	Updated the supported versions. Learn more.

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

DATE	CHANGE	REFERENCE
07 Dec 2021	Updated What's new	Added fixed issue - CAS-62254. Learn more.
06 Dec 2021	Updated SIEM integration-Elasticsearch, Azure Sentinel, Splunk, and Others	Added Kafka endpoints for the Asia Pacific South region. Learn more.
06 Dec 2021	Updated Data sources	Updated data sources supportability for the Asia Pacific South region. Learn more.
06 Dec 2021	Updated Known issues	Added known issue for Remote Browser Isolation (CAS-62254). Learn more.
03 Dec 2021	Updated Self-service search for Remote Browser Isolation	Added prerequisite to enable **Hostname Tracking** to send events. Learn more.
03 Dec 2021	Updated Citrix Analytics data format for SIEM	Added schema format of the Malware files detected risk indicator. Learn more.
02 Dec 2021	Updated What's new	Added new feature. Learn more.
02 Dec 2021	Updated Content Collaboration risk indicators	Added Malware files detected risk indicator. Learn more.
29 Nov 2021	Updated What's new	Added new feature. Learn more.
29 Nov 2021	Added End user email settings	Updated how to use the end user email settings. Learn more.
26 Nov 2021	Updated What's new	Added enhancements. Learn more.

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

DATE	CHANGE	REFERENCE
26 Nov 2021	Updated Custom risk indicators	Updated the navigation link to access the Custom risk indicators page. Learn more.
26 Nov 2021	Updated Policies and actions	Updated the navigation link to access the Policies page. Learn more.
25 Nov 2021	Updated What's new	Updated Security Information and Event Management (SIEM) integration enhancements. Learn more.
25 Nov 2021	Updated Security Information and Event Management (SIEM) integration	Added integration with Elasticsearch, Microsoft Azure Sentinel, and other SIEMs using Kafka or Logstash. Learn more.
09 Nov 2021	Updated What's new	Added fixed issue- CAS-60920. Learn more.
02 Nov 2021	Updated What's new	Added enhancements and fixed issue- CAS-59608. Learn more.
02 Nov 2021	Updated Access Assurance Location dashboard	Added **Access Profile** page and **User Logons** page. Learn more.
02 Nov 2021	Updated Self-service search for Content Collaboration	Added malware logs. Learn more.
20 Oct 2021	Updated What's new	Added Session recording server integration. Learn more.
20 Oct 2021	Updated Citrix Virtual Apps and Desktops and Citrix DaaS data source	Added Session recording server integration. Learn more.

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

DATE	CHANGE	REFERENCE
19 Oct 2021	Updated What's new	Updated Notify admin email template, Access assurance location dashboard enhancements, and added fixed issue- CAS-59595. Learn more.
19 Oct 2021	Updated Access Assurance location dashboard	Added user logon trend and deviation column. Learn more.
01 Oct 2021	Updated Self-service search for Content Collaboration	Added audit logs. Learn more.
01 Oct 2021	Updated What's new	Added audit logs for self-service search for Content Collaboration. Learn more.
29 Sep 2021	Updated Access assurance location dashboard	The dashboard is now generally available to all users. Learn more.
15 Sep 2021	Updated What's new	Added enhancement. Learn more.
15 Sep 2021	Updated Custom risk indicators	Enhancements to custom risk indicator modification and deletion process. Learn more.
14 Sep 2021	Updated What's new	Added features and known issue- CAS-58426. Learn more.
14 Sep 2021	Updated Citrix Analytics data format for SIEM	Added schema details for the Suspicious logon risk indicator. Learn more.
14 Sep 2021	Updated Citrix Virtual Apps and Desktops risk indicators	Added the Suspicious logon risk indicator and deprecated the Access from an unusual

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

DATE	CHANGE	REFERENCE
		location risk indicator. Learn more.
19 Aug 2021	Updated What's new	Added features and enhancements. Learn more.
19 Aug 2021	Updated Citrix Virtual Apps and Desktops data source	Added support for Citrix Director. Learn more.
19 Aug 2021	Updated Citrix Analytics data format for SIEM	Added custom risk indicators schema for Citrix Virtual Apps and Desktops. Learn more.
19 Aug 2021	Updated Access assurance location dashboard	Added geofencing feature. Learn more.
19 Aug 2021	Updated Users page	View Workspace app status. Learn more.
19 Aug 2021	Updated Custom risk indicators	Support for the IS EMPTY operator. Learn more.
19 Aug 2021	Updated Citrix users risk indicators	Added risky factors. Learn more.
19 Aug 2021	Updated User risk timeline and profile	Added risk summary. Learn more.
19 Aug 2021	Updated Splunk integration	Added Citrix Analytics App for Splunk. Learn more.
19 Aug 2021	Added Citrix Analytics dashboards at Splunk	Added new dashboards for Citrix Analytics App for Splunk. Learn more.
29 Jul 2021	Updated What's new	Deprecated feature. Learn more.
29 Jul 2021	Updated Citrix Endpoint Management risk indicators	Removed the following actions that an admin can apply- Lock device, Notify Endpoint Management

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

DATE	CHANGE	REFERENCE
		admin, Notify user, Revoke device, and Wipe device. Learn more.
14 Jul 2021	Updated What's new	Added enhancement. Learn more.
14 Jul 2021	Updated Custom risk indicator	Added IS NOT EMPTY operator. Learn more.
06 Jul 2021	Updated What's new	Added a feature. Learn more.
06 Jul 2021	Updated Users dashboard	Added non-risky users. Learn more.
01 Jul 2021	Updated What's new	Added access assurance location enhancements. Learn more.
01 Jul 2021	Updated Access assurance location dashboard.	Updated unknown locations tab, facets, and timeline views. Learn more.
01 Jul 2021	Updated Self-service search for Virtual Apps and Desktops	Updated the facet from OS Major to OS. Learn more.
30 Jun 2021	Updated What's new	Added enhancement. Learn more.
30 Jun 2021	Updated Splunk integration	Added supported versions for Splunk integration. Learn more.
07 Jun 2021	Updated What's new	Added a feature and enhancement. Learn more.
07 Jun 2021	Updated Policies and actions	Updated Notify administrator(s) action and added Change links to view-only sharing action. Learn more.

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

DATE	CHANGE	REFERENCE
18 May 2021	Updated What's new	Added a feature and a fixed issue- CAS-50153. Learn more.
18 May 2021	Updated Preconfigured custom risk indicators and policies	Added preconfigured custom risk indicators for first-time access. Learn more.
18 May 2021	Updated Citrix Gateway risk indicators	Removed the First time access from new IP risk indicator. Learn more.
18 May 2021	Updated Citrix Virtual Apps and Desktops risk indicators	Removed the First time access from new device risk indicator. Learn more.
29 Apr 2021	Updated What's new	Added a feature and a fixed issue- CAS-49628. Learn more.
29 Apr 2021	Updated Custom risk indicators	Added event details of the custom risk indicator. Learn more.
29 Apr 2021	Updated Self-service search for Virtual Apps and Desktops	Removed print size and print format from the `App.SaaS.File.Print` event. Learn more.
16 Apr 2021	Updated What's new	Added new features. Learn more.
16 Apr 2021	Updated Citrix Analytics data format for SIEM	Client IP added for all risk indicators. If data is not available, **-999** is assigned to integer data type fields and **NA** is assigned to string data type fields. Learn more.
26 Mar 2021	Updated What's new	Added new features. Learn more.

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

DATE	CHANGE	REFERENCE
26 Mar 2021	Updated Citrix Analytics data format for SIEM	Added a maximum threshold on the event details for each risk indicator that is sent to your SIEM service. Added new fields- `data_source_id` and `indicator_category_id` for the indicator summary schema and event details schema. Learn more.
18 Mar 2021	Updated What's new	Added new features and a deprecated feature. Learn more.
18 Mar 2021	Added Access assurance location	Added the topic- Access assurance location. Learn more.
18 Mar 2021	Updated Self-service search	Added support for the NOT LIKE (!~) operator. Learn more.
18 Mar 2021	Updated Custom risk indicators	Added support for the NOT LIKE (!~) operator. Learn more.
18 Mar 2021	Updated Self-service search for Gateway	Removed the record types Application Launch Failure record (VPN_AF) and Session Update record (VPN_SU). Learn more.
18 Mar 2021	Updated Self-service search for Virtual Apps and Desktops	Added dimensions based on the contextual template. Learn more.
11 Mar 2021	Updated What's new	Added a feature. Learn more.
11 Mar 2021	Updated Citrix Analytics data format for SIEM	Added the `last_update_timestamp`

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

DATE	CHANGE	REFERENCE
		field in the user risk score schema. Learn more.
03 Mar 2021	Updated What's new	Added new features. Learn more.
03 Mar 2021	Updated Citrix Content Collaboration risk indicators	Updated the Access from an unusual location and the Ransomware activity suspected risk indicators. Learn more.
03 Mar 2021	Updated Citrix Gateway risk indicators	Updated the Logon from suspicious IP risk indicator. Learn more.
03 Mar 2021	Updated Citrix Virtual Apps and Desktops risk indicators	Updated the event table of the Access from an unusual location risk indicator. Learn more.
03 Mar 2021	Added new topic- Citrix Analytics data format for SIEM	Describes the schema of the processed data for SIEM. Learn more.
18 Feb 2021	Updated What's new	Added new features and deprecated a Citrix Gateway risk indicator. Learn more.
18 Feb 2021	Updated Custom risk indicators	Added a new option- First time for a new. Learn more.
18 Feb 2021	Updated User profile	Citrix Analytics receives user location information from Citrix Virtual Apps and Desktops. Learn more.
18 Feb 2021	Updated Self-service search	Added multi-column sorting. Learn more.

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

DATE	CHANGE	REFERENCE
18 Feb 2021	Updated Citrix Gateway risk indicators	Deprecated Excessive authorization failures risk indicator. Learn more.
28 Jan 2021	Updated topic- Citrix Virtual Apps and Desktops data source	Added firewall exceptions for establishing a connection between a policy agent and an application server. Learn more.
27 Jan 2021	Updated topic- What's new	Enhancements to the Access from an unusual location risk indicator logic. Learn more.
27 Jan 2021	Updated topic- Citrix Content Collaboration risk indicators	Enhancements to the Access from an unusual location risk indicator logic. Learn more.
27 Jan 2021	Updated topic- Citrix Gateway risk indicators	Enhancements to the Access from an unusual location risk indicator logic. Learn more.
27 Jan 2021	Updated topic- Citrix Virtual Apps and Desktops and Citrix DaaS risk indicators	Enhancements to the Access from an unusual location risk indicator logic. Learn more.
20 Jan 2021	Updated topic- What's new	Added fixed issue CAS-46656. Learn more.
19 Jan 2021	Updated topic- What's new	Added fixed issue CAS-46316. Learn more.
13 Jan 2021	Updated topic- Known issues	Added known issue CAS-46316. Learn more.
13 Jan 2021	Updated topic- What's new	New version of the add-on for Splunk is available. Added support for Splunk Cloud IDM and Splunk 8.1 64-bit. Removed support for Splunk 7.1 64-bit. Learn more.

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

DATE	CHANGE	REFERENCE
13 Jan 2021	Updated topic- Splunk integration	Added support for Splunk Cloud IDM and Splunk 8.1 64-bit. Removed support for Splunk 7.1 64-bit. Learn more.
11 Jan 2021	Updated topic- What's new	Added fixed issue CAS-44773. Learn more.
11 Jan 2021	Updated topic- Citrix Virtual Apps and Desktops and Citrix DaaS data source	Updated Apps and Desktops site card images and updated the supported clients list. Learn more.
11 Jan 2021	Updated topic- Known issues	Updated the Citrix Workspace app events matrix table. Learn more.
11 Jan 2021	Updated topic- Troubleshoot Citrix Analytics for Security	Updated the Citrix Workspace app events matrix table. Learn more.
22 Dec 2020	Updated topic- Citrix Gateway data source	Added the Event hub endpoint in the allow list category. Learn more.
17 Dec 2020	Updated topic- What's new	Added Preconfigured custom risk indicators and a policy for geofencing use cases. Learn more.
17 Dec 2020	Added topic- Preconfigured custom risk indicators and policies	Added preconfigured custom risk indicators and a policy for the geofencing use cases. Learn more.
15 Dec 2020	Updated topic- What's new	Updated user-response email and renamed Content Collaboration risk indicator. Learn more.

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

DATE	CHANGE	REFERENCE
15 Dec 2020	Updated topic- Policies and actions	Added location information in the user-response email. Learn more.
15 Dec 2020	Updated topic- Citrix Content Collaboration risk indicators	Renamed **First time access from new location** to **Access from an unusual location**. Learn more.
07 Dec 2020	Updated topic- What's new	Improvements to Potential data exfiltration and First time access from new location risk indicators. Learn more.
07 Dec 2020	Updated topic- Citrix Virtual Apps and Desktops and Citrix DaaS risk indicators	Updated **WHAT HAPPENED** section for Potential data exfiltration. Learn more.
07 Dec 2020	Updated topic- Citrix Content Collaboration risk indicators	Added geo map and pie chart and modified event table for First time access from new location. Learn more.
30 Nov 2020	Updated What's new	Improvements to self-service search and policies. Learn more.
30 Nov 2020	Updated topic- Self-service search	Improved self-service search page. Learn more.
30 Nov 2020	Updated topic- Policies and actions	Updated policy display criteria on the **Policies** dashboard. Learn more.
12 Nov 2020	Updated topic- What's new	Added a feature. Learn more.
15 Oct 2020	Updated topic- What's new	Added a feature and a deprecated feature. Learn more.

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

DATE	CHANGE	REFERENCE
15 Oct 2020	Updated topic- Share Links dashboard	Improvements in Share links dashboard. Learn more.
30 Sep 2020	Updated topic - Splunk integration	Removed Splunk version 7.0 and lower. Learn more
10 Sep 2020	Updated topic - What's new	Added new features. Learn more.
08 Sep 2020	Updated topic - Microapps dashboard	Updated Client OS Version image that no longer displays the OS version.
08 Sep 2020	Updated topic- What's new	Added a feature and a fixed issue. Learn more.
01 Sep 2020	Renamed Citrix Managed Desktops logs to Citrix Virtual Apps and Desktops Standard for Azure logs	Learn more
31 Aug 2020	Updated topic- Citrix Virtual Apps and Desktops and Citrix DaaS data source	Added checklist for StoreFront configuration file. Learn more.
11 Aug 2020	Updated topic- What's new	Added the fixed issue CAS-38021. Learn more.
08 Aug 2020	Updated topic- What's new	Added new feature. Learn more.
31 Jul 2020	Updated topic- What's new	Added the fixed issue CAS-38129. Learn more.
09 Jul 2020	Updated topic- What's new	Added new features and deprecated features. Learn more.
09 Jul 2020	Updated topic- Users dashboard	Updated the Users dashboard data. Learn more.

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

DATE	CHANGE	REFERENCE
09 Jul 2020	Updated topic- Citrix Gateway risk indicators	Added the Access from an unusual location risk indicator. Learn more.
09 Jul 2020	Updated topic- System requirements	Removed Internet Explorer 11 from the supported browsers list. Learn more.
09 Jul 2020	Updated topic- Citrix Virtual Apps and Desktops and Citrix DaaS data source	Updated the site card data with supported and unsupported clients. Learn more.
01 Jul 2020	Updated topic- Known issues	Added the known issues CAS-36236 and CAS-36238. Learn more.
26 Jun 2020	Updated topic- What's new	**Unusual time of application access (Virtual/SaaS)** risk indicator deprecated. Learn more.
26 Jun 2020	Updated topic- Known issues	Added the known issue CAS-33767. Learn more.
02 Jun 2020	Updated topic- What's new	Added the fixed issue CAS-32773. Learn more.
02 Jun 2020	Updated topic- Known issues	Added the known issue CAS-35310. Learn more.
14 May 2020	Updated topic- System requirements	Updated the system requirements. Learn more.
14 May 2020	Updated topic- Citrix Gateway data source	Modified the content and added prerequisites. Learn more.
14 May 2020	Updated topic- Security Analytics home page	Added the What's next section. Learn more.

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

DATE	CHANGE	REFERENCE
14 May 2020	Updated topic- Citrix Virtual Apps and Desktops and Citrix DaaS data source	Modified the content and prerequisites. Learn more.
11 May 2020	Updated topic- What's new	Added the fixed issues CAS-34209, CAS-34141, and CAS-34139. Learn more.
04 May 2020	Updated topic- Known issues	Added the known issue CAS-33934. Learn more.
29 Apr 2020	Updated topic- What's new	Added the fixed issue CAS-31544. Learn more.
08 Apr 2020	Updated topic- Known issues	Added the known issue CAS-32773. Learn more.
02 Apr 2020	Updated topic- What's new	Added a feature and the fixed issue CAS-29226. Learn more.
02 Apr 2020	Updated topic- Citrix Virtual Apps and Desktops and Citrix DaaS data source	Added StoreFront specifications. Learn more.
18 Mar 2020	Updated topic- Known issues	Added the known issue CAS-31544. Learn more.
04 Mar 2020	Updated topic- What's new	Updated the fixed issue CAS-31180. Learn more.
04 Mar 2020	Updated topic- Known issues	Updated the supported events. Learn more.
04 Mar 2020	Updated topic- Troubleshoot Citrix Analytics	Updated the StoreFront configuration step. Learn more.
04 Mar 2020	Updated topic- System requirements	Updated the system requirements for Virtual Apps and Desktops. Learn more.

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

DATE	CHANGE	REFERENCE
03 Mar 2020	Updated topic- Known issues	Added the known issue CAS-31180. Learn more.
20 Feb 2020	Updated topic- What's new	Added new features and fixed issues CAS-24134, CAS-29207, CAS-29029, and CAS-28781. Learn more.
20 Feb 2020	Updated topic- Known issues	Added the known issue CAS-29583. Removed the known issue CAS-18536. Learn more.
20 Feb 2020	Updated topic- Users dashboard	Analytics introduces the risk categories dashboard. Learn more.
20 Feb 2020	Updated topic- Custom risk indicators	Analytics introduces the risk category column on the Custom risk indicators page. Learn more.
20 Feb 2020	Updated topic- Citrix user risk indicators	Updated new risk indicator names. Learn more.
17 Jan 2020	Updated topic- Known issues	Added the known issue CAS-29226. Learn more.
10 Jan 2020	Updated topic- Known issues	Added the known issue CAS-29207. Learn more.
09 Jan 2020	Updated topic- What's new	Added new features and the fixed issues CAS-26297. Learn more.
09 Jan 2020	Updated topic- Known issues	Added the known issue CAS-29029. Learn more.
09 Jan 2020	Added topic- Continuous risk assessment	Citrix Analytics supports continuous assessment. Learn more.

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

DATE	CHANGE	REFERENCE
09 Jan 2020	Updated topic- Policies and actions	Citrix Analytics introduces policy enhancements. Learn more.
09 Jan 2020	Updated topic- Users dashboard	**Access Summary** and **Policies and Actions** dashboards are introduced. Learn more.
09 Jan 2020	Added topic- Self-service search for Policies	Use the self-service search to view the events related to policies. Learn more.
12 Dec 2019	Updated topic- What's new	Added a feature. Learn more.
12 Dec 2019	Updated topic- Splunk integration	Added new Splunk versions. Learn more.
04 Dec 2019	Updated topic- What's new	Added a feature. Learn more.
04 Dec 2019	Updated topic- Custom risk indicators	Added support for Citrix Gateway data source. Learn more.
22 Nov 2019	Updated topic- What's new	Added new features and the fixed issue CAS-24959. Learn more.
22 Nov 2019	Updated topic- Citrix Virtual Apps and Desktops and Citrix DaaS risk indicators	Added the **First time access from new device** risk indicator and deprecated the **Access from new device** risk indicator. Learn more.
22 Nov 2019	Updated topic- Citrix Gateway risk indicators	Added the **First time access from new IP** and the **Logon from suspicious IP** risk indicators. Learn more.

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

DATE	CHANGE	REFERENCE
22 Nov 2019	Added topic- Self-service search for Gateway	Use self-service search to get insights into gateway events. Learn more.
22 Nov 2019	Added topic- Self-service search for Remote Browser Isolation	Use self-service search to get insights into Remote Browser Isolation events. Learn more.
22 Nov 2019	Updated topic- Watchlist	Remove a user from the watchlist. Learn more.
08 Nov 2019	Updated topic- What's new	Added the fixed issue CAS-24844. Learn more.
06 Nov 2019	Updated topic- Citrix Virtual Apps and Desktops and Citrix DaaS data source	Added the proxy configuration steps for a StoreFront deployment that is hosted on a webserver that uses an HTTP proxy. Learn more.
21 Oct 2019	Updated topic- Citrix Virtual Apps and Desktops data source	Modified the agent name as Analytics policy agent. Learn more.
21 Oct 2019	Updated topic- Audit logs	Refresh the Audit log page to view the latest audit data. Learn more.
21 Oct 2019	Updated topic- What's new	Added new features and fixed issues. Learn more.
21 Oct 2019	Updated topic- Known issues	Updated the known issues CAS-24938, CAS-24844, CAS-24959, and CAS-16151. Learn more.
18 Oct 2019	Updated topic- Overview	Updated the home page content. Learn more.

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

DATE	CHANGE	REFERENCE
14 Oct 2019	Updated topic- Known issues	Updated the version for Citrix Workspace app for Mac. Learn more.
30 Sep 2019	Updated topic- Known issues	Added the known issue CAS-24776 and updated the table with supported versions for the known issue CAS-16151. Learn more.
23 Sep 2019	Updated topic- What's new	Added the fixed issue CAS-24087. Learn more.
20 Aug 2019	Updated topic- What's new	Added new features. Learn more.
20 Aug 2019	Updated topic- Self-service search	Added self-service search enhancements. Learn more.
20 Aug 2019	Updated topic- Custom reports	Added custom report enhancements. Learn more.
20 Aug 2019	Updated topic- Users dashboard	**Risk Indicators** dashboard is introduced. **Risky Users** dashboard is enhanced. Learn more.
20 Aug 2019	Updated topic- Citrix share link risk indicators	**Excessive downloads** risk indicator is introduced. Learn more.
20 Aug 2019	Added topic- Self-service search for Authentication	Use self-service search to get insights into the authentication details of Citrix Cloud users. Learn more.
17 Jul 2019	Updated topic- Known issues	Added the known issues CAS-16297 and CAS-21329. Learn more.

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

DATE	CHANGE	REFERENCE
11 Jul 2019	Updated topic- What's new	Updated the list of new features. Learn more.
11 Jul 2019	Updated topic- Known issues	Added the known issues CAS-19466, CAS-20906, CAS-17304, and CAS-21339. Learn more.
11 Jul 2019	Added topic- Custom risk indicators	Create custom risk indicators. Learn more.
11 Jul 2019	Updated topic- User risk timeline	Updated the privileged user events displayed on the user risk timeline. Learn more.
11 Jul 2019	Updated topic- Citrix share link risk indicators	Updated the supported action of share link risk indicators. Learn more.
11 Jul 2019	Updated topic- Self-service search	Self-service search enhancements. Learn more.
11 Jul 2019	Updated topics - Citrix Content Collaboration data source, Citrix Access Control data source, Citrix Endpoint Management data source, Citrix Virtual Apps and Desktops and Citrix DaaS data source, and Citrix Gateway data source	Site cards display the **No data received** status. Learn more.
27 Jun 2019	Updated topic- Splunk integration	Updated the list of processed data sent to Splunk. Learn more.
19 Jun 2019	Updated topic- What's new	Added the fixed issues CAS-17575, CAS-19467, and CAS-19429. Learn more.

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

DATE	CHANGE	REFERENCE
17 Jun 2019	Updated topic- Citrix Virtual Apps and Desktops and Citrix DaaS data source	Configure StoreFront to send events to Citrix Analytics. Learn more.
12 Jun 2019	Updated topic - Known Issues	Added a known issue- CAS-19930. Learn more.
07 Jun 2019	Updated topic - Known Issues	Added a known issue- CAS-16151. Learn more.
04 Jun 2019	Updated topic- Data governance	Added Citrix Managed Desktops logs. Learn more.
30 May 2019	Updated topic - Known Issues	Added known issues. Learn more.
30 May 2019	Updated topic - What's new	Added new features and fixed issues. Learn more.
30 May 2019	Updated topic - Custom reports	Edit custom reports based on your requirements. Learn more.
09 May 2019	Updated topic - Known Issues	Self-service search does not work on Internet Explorer 11. Learn more.
09 May 2019	Added topic - Custom reports	Create custom reports based on your operational requirements. Learn more.
09 May 2019	Updated topic - Users dashboard	Citrix Analytics supports privileged user monitoring. Learn more.
09 May 2019	Added topic - Weekly email summary	Citrix Analytics sends a weekly email to administrators summarizing the security risk exposures. Learn more.

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

DATE	CHANGE	REFERENCE
26 Apr 2019	Updated topic - System Requirements	Subscription to Citrix ADM service is required for configuring an agent. Learn more.

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