Citrix Analytics - Usage
## Contents

What's new 3

Citrix Analytics offerings 5

Data Sources 6

Data Governance 7

System Requirements 44

Getting started 44

Content Collaboration 46

Microapps 54

SaaS and Web Apps 60

FAQs 65

Glossary of terms 70
What’s new

February 15, 2023

Note

Attention: Removal of Citrix Usage Analytics
Starting April 1 2023, Citrix Usage Analytics offering will no longer be available to users.

March 15, 2022

Fixed issue

If your organization is onboarded to Citrix Cloud in the Asia Pacific South region, Citrix Analytics is unable to generate the Usage Analytics reports from December 02, 2021 to December 10, 2021. [CAS-63134]

January 06, 2022

Fixed issue

- If your organization is onboarded to Citrix Cloud in the Asia Pacific South region, you can’t view the Usage Analytics reports. This issue is now fixed. [CAS-62341]

December 20, 2021

What’s new

Access Control is renamed to Secure Workspace Access

On the Data Sources page, all the Access Control labels are now updated as Secure Workspace Access to align with the rebranded product name.

For more information, see SaaS and Web Apps.

June 29, 2020

Fixed issues

- The Usage Analytics charts such as line chart and pie chart display only 20 data points (records) for a selected time period. If data points exceed 20 for a selected time period, the exceeded data points are not visible on the charts. The line chart displays the 20 data points from the start date of the selected time period. This issue is not observed in the charts that are presented in tabular formats. This issue is now fixed. [CAS-36128]
New features

The Usage tab replaces the Operations tab

In the Analytics user interface, the Operations offering is renamed as Usage to emphasize the purpose of this offering. The Usage dashboards provide visibility into the basic usage data of the following Citrix products:

- Content Collaboration
- Microapps
- SaaS and Web Apps (Secure Workspace Access)

For more information, see Usage Analytics.

View Content Collaboration usage data

You can now view the basic usage reports of your Content Collaboration service. The Content Collaboration dashboard provides visibility into how users interact with the Content Collaboration service in your organization.

To view the dashboard:

Click Usage > Content Collaboration.

For more information, see the Content Collaboration usage reports.

View Microapps usage data

You can now view the basic usage reports of your Citrix Workspace Microapps service. The Microapps dashboard provides visibility into how users interact with Microapps in your organization.

To view the dashboard:

Click Usage > Microapps.

For more information, see the Microapps usage reports.

View SaaS and Web Apps usage data

You can now view the basic usage reports of the SaaS and Web applications accessed through the Citrix Secure Workspace Access service. The SaaS and Web Apps dashboard provides visibility into how users interact with these applications in your organization.
To view the dashboard:

Click Usage > SaaS and Web Apps.

For more information, see the SaaS and Web Apps usage reports.

Deprecated features

Deprecated dashboards- User Operations and App Operations

The User Operations and App Operations dashboards under the Operations tab are deprecated. The reports displayed by these deprecated dashboards are now consolidated and available through the SaaS and Web Apps dashboard, which is under Usage tab. For more information, see the SaaS and Web Apps usage reports.

Citrix Analytics offerings

August 1, 2023

Citrix Analytics for Security

Collates and provides visibility into user and application behavior. You can track every aspect of the behavior, and by leveraging advanced Machine Learning algorithms, you can distinguish between normal behavior and a malicious attacker. Thus, enabling you to proactively identify and manage internal and external threats. To get started, you can request a trial or buy a subscription.

Learn more: Citrix Analytics for Security

Citrix Analytics for Performance

Provides visibility into the performance of Citrix Virtual Apps and Desktop Sites across an organization. Performance is indicated by the User Experience Score which quantifies the factors that define the experience a user has while using a virtual app or desktop. To get started, you can request a trial or buy a subscription.

Learn more: Citrix Analytics for Performance

Citrix Analytics - Usage (End of Life)

Note

Attention: Citrix Usage Analytics has reached its end of life and is no longer available to users.
Data Sources

February 3, 2023

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

Supported data sources

The following table lists various Citrix data sources supported by Citrix Analytics- Usage.

<table>
<thead>
<tr>
<th>Citrix Product / Data Source</th>
<th>Deployment Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Private Access</td>
<td>Service</td>
</tr>
<tr>
<td>Content Collaboration</td>
<td>Service</td>
</tr>
<tr>
<td>Microapps</td>
<td>Service</td>
</tr>
</tbody>
</table>

Note

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

Supported home regions

Citrix Analytics- Usage 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.

<table>
<thead>
<tr>
<th>Data source</th>
<th>Supported in US Region</th>
<th>Supported in EU Region</th>
<th>Supported in APS region</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Secure Private Access</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Data Governance

August 28, 2023

This section provides information regarding the collection, storage, and retention of logs by the Citrix Analytics service. Any capitalized terms not defined in the Definitions section carry the meaning specified in the Citrix End User Services Agreement.

Citrix Analytics is designed to provide customers with insight into activities in their Citrix computing environment. Citrix Analytics enables security administrators to choose the logs they want to monitor and take directed action based on the logged activity. These insights help security administrators manage access to their computing environments and protect Customer Content in the customer’s computing environment.

Data residency

Citrix Analytics logs are maintained separately from the data sources and are aggregated in multiple Microsoft Azure Cloud environments, which are located in the United States, the European Union, and the Asia Pacific South regions. The storage of the logs depends on the home region selected by the Citrix Cloud administrators when onboarding their organizations to Citrix Cloud. For example, if you choose the European region when onboarding your organization to Citrix Cloud, Citrix Analytics logs are stored in Microsoft Azure environments in the European Union.

For more information, see Citrix Cloud Services Customer Content and Log Handling and Geographical Considerations.

Data collection

Citrix Cloud services are instrumented to transmit logs to Citrix Analytics. Logs are collected from the following data sources:

- Citrix ADC (on-premises) along with subscription for Citrix Application Delivery Management
Citrix Analytics - Usage

- Citrix Content Collaboration
- Citrix Endpoint Management
- Citrix Gateway (on-premises)
- Citrix Identity provider
- Citrix Secure Browser
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)
- Microsoft Active Directory
- Microsoft Graph Security

**Data transmission**

Citrix Cloud logs are transmitted securely to Citrix Analytics. When the administrator of the customer environment explicitly enables Citrix Analytics, these logs are analyzed and stored on a customer database. The same is applicable to Citrix Virtual Apps and Desktops data sources with Citrix Workspace configured.

For Citrix ADC data sources, log transmission is initiated only when the administrator explicitly enables Citrix Analytics for the specific data source.

**Data control**

Logs sent to Citrix Analytics can be turned on or off at any time by the administrator.

When turned off for Citrix ADC on-premises data sources, communication between the particular ADC data source and Citrix Analytics stops.

When turned off all for other data sources, the logs for the particular data source are no longer analyzed and stored in Citrix Analytics.

**Data retention**

Citrix Analytics logs are retained in identifiable form for a maximum of 13 months or 396 days. All logs and associated analytics data such as user risk profiles, user risk score details, user risk event details, user watch list, user actions, and user profile are retained for this period.

For example, if you have enabled Analytics on a data source on January 1, 2021, then by default, data collected on January 1, 2021, will be retained in Citrix Analytics until January 31, 2022. Similarly, the data collected on January 15, 2021, will be retained until February 15, 2022, and so on.
Citrix Analytics - Usage

This data is stored for the default data retention period even after you have turned off data processing for the data source or after you have removed the data source from Citrix Analytics.

Citrix Analytics deletes all Customer Content 90 days after the expiry of the subscription or the trial period.

Data export

This section explains the data exported from Citrix Analytics for Security and Citrix Analytics for Performance.

Citrix Analytics for Performance collects and analyzes performance metrics from the Data Sources.

You can download the data from the Self-service search page as a CSV file.

Citrix Analytics for Security collects user events from various products (data sources). These events are processed to provide visibility into the users’ risky and unusual behavior. You can export these processed data related to users’ risk insights and users’ events to your System Information and Event Management (SIEM) service.

Currently, the data can be exported in two ways from Citrix Analytics for Security:

- Integrating Citrix Analytics for Security with your SIEM service
- Downloading the data from the Self-service search page as a CSV file.

When you integrate Citrix Analytics for Security with your SIEM service, the data is sent to your SIEM service by using either the north-bound Kafka topic or a Logstash-based data connector.

Currently, you can integrate with the following SIEM services:

- Splunk (by connecting through Citrix Analytics Add-on)
- Any SIEM service that support Kafka topic or Logstash-based data connectors such as Elastic-search and Microsoft Azure Sentinel

You can also export the data to your SIEM service by using a CSV file. In the Self-service search page, you can view the data (user events) for a data source and download these data as a CSV file. For more information about the CSV file, see Self-service search.

Important

After the data is exported to your SIEM service, Citrix is not responsible for the security, storage, management, and the use of the exported data in your SIEM environment.

You can turn on or off data transmission from Citrix Analytics for Security to your SIEM service.

For information on the processed data and the SIEM integration, see Security Information and Event Management (SIEM) integration and Citrix Analytics data format for SIEM.
**Citrix Services Security Exhibit**

Detailed information concerning the security controls applied to Citrix Analytics, including access and authentication, security program management, business continuity, and incident management, is included in the Citrix Services Security Exhibit.

**Definitions**

*Customer Content* means any data uploaded to a customer account for storage or data in a customer environment to which Citrix is provided access to perform Services.

*Log* means a record of events related to the Services, including records that measure performance, stability, usage, security, and support.

*Services* means the Citrix Cloud Services outlined above for the purposes of Citrix Analytics.

**Data collection agreement**

By uploading your data to Citrix Analytics and by using the features of Citrix Analytics, you agree and consent that Citrix may collect, store, transmit, maintain, process and use technical, user, or related information about your Citrix products and services.

Citrix always treats the received information according to the [Citrix Privacy Policy](#).

**Appendix: logs collected**

- Citrix Analytics for Security logs
- Citrix Analytics for Performance logs

**Citrix Analytics for Security logs**

- General logs
- Citrix Content Collaboration logs
- Citrix Endpoint Management service logs
- Citrix Secure Private Access logs
- Citrix Virtual Apps and Desktops and Citrix DaaS logs
- Citrix ADC logs
- Citrix DaaS Standard for Azure logs
- Citrix Identity provider logs
Citrix Analytics - Usage

- Citrix Gateway logs
- Citrix Secure Browser logs
- Microsoft Graph Security logs
- Microsoft Active Directory logs

**General logs**

In general, Citrix Analytics logs contain the following header identification data points:

- Header Keys
- Device Identification
- Identification
- IP Address
- Organization
- Product
- Product Version
- System Time
- Tenant Identification
- Type
- User: Email, Id, SAM Account Name, Domain, UPN
- Version

**Citrix Content Collaboration logs**

The Citrix Content Collaboration logs contain the following data points:

- Account Id
- Account Info: API Control Plane, App Control Plane, Subdomain
- Add On Name
- Additional Bandwidth
- Additional Bandwidth Rate
- Additional Disk Space
- Additional Disk Space Rate
- Additional User Rate
• Additional Users
• Address1
• Address2
• Advanced Custom Branding Folder Name
• Alias Id
• App Code
• Associated Folder Template Id
• Bandwidth Max
• Base Bandwidth
• Base Billing Rate
• Base Disk Space
• Base Users
• Billing Contact Id
• Billing Cycle
• Billing Rate
• Billing Type
• Branding Styles
• Bytes Downloaded
• Bytes Total
• Cc Sender
• City
• Client Information: City, Client IP, Control Plane, Country, OAuth Client Id, Operating System, Tool Display Name, Tool Name, Tool Version
• Client Name
• Company
• Company Name
• Component Name
• Connector Type
• Contacts: Op Name, Values, Contact Id, Email
• Context: Resource Id, Resource Type
- Copied File Id
- Country
- Created By
- Creation Date
- Creator Id
- Default Zone Id
- Deleted Permanently
- Description
- Destination: File Path, Parent Id, Path, Zone Id
- Disk Space Limit
- Disk Space Max
- DLP Status
- Download By Service
- Download Id
- Email Addresses: Op Name, Values
- Encryption Rate
- End Time
- Entity Id
- Event Id
- Event Time
- Event User Email
- Event User Id
- Events: Operation Name, Resource Type
- Expiration Date
- Fields: Account Id, Account Information Type, API Control Plane, App Control Plane, Subdomain, Approval Context Type, Approval Id, Approval Step Id, Approval Step Status, Is Linked to Approval Step, Bytes Downloaded, Client Information Type, City, Client IP, Control Plane, Country, OAuth Client ID, Operating System, Tool Display Name, Tool Name, Tool Version, Completed Step Id, Connector Type, Created By Type, Created By Email Address, Created By First Name, Created By Id, Created By Last Name, Due, End Time Event User Id, File Extension, File Id, File
Name, File Path, File Size, Form Id, Last Ping Back, Name, Next Step Id, Participant Type, Participant Role, Participant Status, Participant User Id, Recipient Type, Recipient Op Name, Recipient Email Address, Recipient First Name, Recipient Id, Recipient Last Name, Role Type, Role Initiators Type, Role Initiators Op Name, Role Initiators Email Address, Role Initiators First Name, Role Initiators Id, Role Initiators Last Name, Role Instance Manager Type, Role Instance Manager Op Name, Role Instance Manager Email Address, Role Instance Manager First Name, Role Instance Manager Id, Role Instance Manager Last Name, Role Template Manager Type, Role Template Manager Op Name, Role Template Manager Email Address, Role Template Manager First Name, Role Template Manager Id, Role Template Manager Last Name, Role View Report Type, Role View Report Op Name, Role View Report Email Address, Role View Report First Name, Role View Report Id, Role View Report Last Name, Routing Key Type, Routing Key Account Id, Routing Key Component Name, Routing Key File Extension, Routing Key File Id, Routing Key File Name, Routing Key Form Id, Routing Key Operation Name, Routing Key Product Name, Routing Key Resource Type, Routing Key Storage Center Id, Routing Key Submission Id, Routing Key Template Id, Routing Key Workflow Id, Routing Key Zone Id, Routing Key Zone Version, Server Name, Start Time, State, Step Data Type, Step Data File Id, Step Data Status, Step Data Step Type, Steps Completed, Steps Remaining, Steps Type, Steps Approvers Type, Steps Approvers Email Address, Steps Approvers First Name, Steps Approvers Id, Steps Approvers Last Name, Steps Days To Complete, Steps Sequential, Steps Step Id, Steps To Type, Steps To Email Address, Steps To First Name, Steps To Id, Steps To Last Name, Steps Viewers Type, Steps Viewers Email Address, Steps Viewers First Name, Steps Viewers Id, Steps Viewers Last Name, Steps Viewers Name, Storage Center Id, Stream Id, Submission Id, Templated Id, Trigger Type, Trigger Folder Ids, Trigger Form Id, User Id, Workflow Type, Workflow Id, Workflow Initiator Type, Workflow Initiator User Id, Workflow Name, Workflow Template Id, Workflow Trigger Resource Id, Workflow Trigger Type, Workflow Initiator Info User Id, Workflow Status, Workflow Type, Zone Id, Zone Services, Zone Version

- File Extension
- File Id
- File Name
- File Path
- File Size
- File Size Bytes
- First Name
- Folder Id
- Folder Name
- Grant Types
Citrix Analytics - Usage

- Group Id
- Has Encryption
- Has Multiple Versions
- Has Power Tools
- Hash
- Integration OAuth Client Id
- Integration Provider Type
- IRM Classification Id
- Is Confirmed
- Is Disabled
- Is Employee
- Is Free Trial
- Is Shared
- Is Template Owned
- Is View Only
- Item Extension
- Item Extensions
- Last Any Login
- Last Name
- Lock Id
- Lock Type
- Logo URL
- Max Downloads
- Method
- Name
- New Stream Id
- Number Of Licenses
- Number Of Paid Licenses
- OAuth Client Id
Citrix Analytics - Usage

- Old Stream Id
- Operation Name
- Owner Id
- Parent Id
- Path
- Phone
- Plan Name
- Plan Track
- Power Tools Rate
- Price Per License
- Primary Email
- Primary Subdomain
- Product Code
- Product Name
- Recipient Id
- Recipient Ids
- Redirect URIs
- Required Login
- Required User Info
- Resource Type
- Root Item Id
- Routing Key: Account Id, Add On Name, App Code, Component Name, Connector Type, Entity Id, File Id, Folder Id, Group Id, Integration Provider Type, OAuth Client Id, Operation Name, Parent Id, Product Name, Resource Type, Share Id, Stream Id, User Id, Version, Zone Id
- Scope
- Semantic Path
- Server Name
- Share Id
- Share Info: Alias Id, Creator Id, Share Id, Share Sub Type Id
- Share Sub Type Id
Citrix Analytics - Usage

- Share Type
- Single Version
- Start Time
- State
- Storage Center Name
- Stream Id
- Subdomains: Op Name, Values
- Subscribed Resource Id
- Subscribed Resource Type
- Tax Area Code
- Title
- Update Date
- Upload Id
- URL Path
- Use Advanced Custom Branding
- User Email
- User Id
- User Max
- User Roles: Op Name, Values
- Version
- Webhook Subscription Id
- Webhook URL
- Zip
- Zone Id

Citrix Endpoint Management service logs

The Citrix Endpoint Management service logs contain the following data points:

- Compliance
- Corporate Owned
Citrix Analytics - Usage

- Device Id
- Device Model
- Device Type
- Geo Latitude
- Geo Longitude
- Host Name
- IMEI
- IP Address
- Jail Broken
- Last Activity
- Management Mode
- Operating System
- Operating System Version
- Platform Information
- Reason
- Serial Number
- Supervised

Citrix Secure Private Access logs

- AAA User Name
- Auth Policy Action Name
- Authentication Session ID
- Request URL
- URL Category Policy Name
- VPN Session ID
- Vserver IP
- AAA User Email ID
- Actual Template Code
- App FQDN
Citrix Analytics - Usage

- App Name
- App Name Vserver LS
- Application Flags
- Authentication Type
- Authentication Stage
- Authentication Status Code
- Back-end Server Dst IPv4 Address
- Back-end Server IPv4 Address
- Back-end Server IPv6 Address
- Category Domain Name
- Category Domain Source
- Client IP
- Client MSS
- Client Fast Retx Count
- Client TCP Jitter
- Client TCP Packets Retransmitted
- Client TCP RTO Count
- Client TCP Zero Window Count
- Clt Flow Flags Rx
- Clt Flow Flags Tx
- Clt TCP Flags Rx
- Clt TCP Flags Tx
- Connection Chain Hop Count
- Connection Chain ID
- Egress Interface
- Exporting Process ID
- Flow Flags Rx
- Flow Flags Tx
- HTTP Content Type
• HTTP Domain Name
• HTTP Req Authorization
• HTTP Req Cookie
• HTTP Req Forw FB
• HTTP Req Forw LB
• HTTP Req Host
• HTTP Req Method
• HTTP Req Rcv FB
• HTTP Req Rcv LB
• HTTP Req Referer
• HTTP Req URL
• HTTP Req XForwarded For
• HTTP Res Forw FB
• HTTP Res Forw LB
• HTTP Res Location
• HTTP Res Rcv FB
• HTTP Res Rcv LB
• HTTP Res Set Cookie
• HTTP Rsp Len
• HTTP Rsp Status
• HTTP Transaction End Time
• HTTP Transaction ID
• IC Cont Grp Name
• IC Flags
• IC No Store Flags
• IC Policy Name
• Ingress Interface Client
• NetScaler Gateway Service App ID
• NetScaler Gateway Service App Name
• NetScaler Gateway Service App Type
• NetScaler Partition ID
• Observation Domain ID
• Observation Point ID
• Origin Res Status
• Origin Rsp Len
• Protocol Identifier
• Rate Limit Identifier Name
• Record Type
• Responder Action Type
• Response Media Type
• Srv Flow Flags Rx
• Srv Flow Flags Tx
• Srvr Fast Retx Count
• Srvr TCP Jitter
• Srvr TCP Packets Retransmitted
• Srvr TCP Rto Count
• Srvr TCP Zero Window Count
• SSL Cipher Value BE
• SSL Cipher Value FE
• SSL Client Cert Size BE
• SSL Client Cert Size FE
• SSL Clnt Cert Sig Hash BE
• SSL Clnt Cert Sig Hash FE
• SSL Err App Name
• SSL Err Flag
• SSL FLags BE
• SSL FLags FE
• SSL Handshake Error Msg
• SSL Server Cert Size BE
• SSL Server Cert Size FE
• SSL Session ID BE
• SSL Session ID FE
• SSL Sig Hash Alg BE
• SSL Sig Hash Alg FE
• SSL Srvr Cert Sig Hash BE
• SSL Srvr Cert Sig Hash FE
• SSL iDomain Category
• SSL iDomain Category Group
• SSL iDomain Name
• SSL iDomain Reputation
• SSL iExecuted Action
• SSL iPolicy Action
• SSL iReason For Action
• SSL iURL Set Matched
• SSL iURL Set Private
• Subscriber Identifier
• Svr Tcp Flags Rx
• Svr Tcp Flags Tx
• Tenant Name
• Tracing Req Parent Span ID
• Tracing Req Span ID
• Tracing Trace ID
• Trans Clt Dst IPv4 Address
• Trans Clt Dst IPv6 Address
• Trans Clt Dst Port
• Trans Clt Flow End Usec Rx
• Trans Clt Flow End Usec Tx
Citrix Analytics - Usage

- Trans Clt Flow Start Usec Rx
- Trans Clt Flow Start Usec Tx
- Trans Clt IPv4 Address
- Trans Clt IPv6 Address
- Trans Clt Packet Tot Cnt Rx
- Trans Clt Packet Tot Cnt Tx
- Trans Clt RTT
- Trans Clt Src Port
- Trans Clt Tot Rx Oct Cnt
- Trans Clt Tot Tx Oct Cnt
- Trans Info
- Trans Srv Dst Port
- Trans Srv Packet Tot Cnt Rx
- Trans Srv Packet Tot Cnt Tx
- Trans Srv Src Port
- Trans Svr Flow End Usec Rx
- Trans Svr Flow End Usec Tx
- Trans Svr Flow Start Usec Rx
- Trans Svr Flow Start Usec Tx
- Trans Svr RTT
- Trans Svr Tot Rx Oct Cnt
- Trans Svr Tot Tx Oct Cnt
- Transaction ID
- URL Category
- URL Category Group
- URL Category Reputation
- URL Category Action Reason
- URL Set Matched
- URL set Private
Citrix Analytics - Usage

- URL Object ID
- VLAN Number

Citrix Virtual Apps and Desktops and Citrix DaaS logs

The Citrix Virtual Apps and Desktops and Citrix DaaS logs contain the following data points:

- App Name
- Browser
- Customer ID
- Details: Format Size, Format Type, Initiator, Result
- Device ID
- Device Type
- Feedback
- Feedback ID
- File Name
- File Path
- File Size
- Is like
- Jail Broken
- Job Details: File Name, Format, Size
- Location: Estimated, Latitude, Longitude

Note

The location information is provided at the city and the country level and does not represent a precise geolocation.

- Long CMD Line
- Module File Path
- Operation
- Operating System
- Platform Extra Information
- Printer Name
- Question
Citrix Analytics - Usage

- Question ID
- SaaS App Name
- Session Domain
- Session Server Name
- Session User Name
- Session GUID
- Timestamp
- Time Zone: Bias, DST, Name
- Total Copies Printed
- Total Pages Printed
- Type
- URL
- User Agent

Citrix ADC logs

The Citrix ADC logs contain the following data points:

- Container
- Files
- Format
- Type

Citrix DaaS Standard for Azure logs

The Citrix DaaS Standard for Azure logs contain the following data points:

- App Name
- Browser
- Details: Format Size, Format Type, Initiator, Result
- Device Id
- Device Type
- File Name
- File Path
Citrix Analytics - Usage

- File Size
- Jail Broken
- Job Details: File Name, Format, Size
- Location: Estimated, Latitude, Longitude

Note
The location information is provided at the city and the country level and does not represent a precise geolocation.

- Long CMD Line
- Module File Path
- Operation
- Operating System
- Platform Extra Information
- Printer Name
- SaaS App Name
- Session Domain
- Session Server Name
- Session User Name
- Session GUID
- Timestamp
- Time Zone: Bias, DST, Name
- Type
- URL
- User Agent

Citrix Identity provider logs

- User Login:
  - Authentication Domains: Name, Product, IdP Type, IdP Display Name
    - IdP Properties: App, Auth Type, Customer Id, Client Id, Directory, Issuer, Logo, Resources, TID
    - Extensions:
Citrix Analytics - Usage

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

Citrix Gateway logs

- Transaction events:
  - ICA App: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSi Client Cookie, Flow Id Rx, ICA Flags, Connection Id, Padding Octets Two, ICA Device Serial Number, IP Version 4, Protocol Identifier, Source IPv4 Address Rx, Destination IPv4 Address Rx, Source Transport Port Rx, Destination Transport Port Rx, ICA Application Start up Duration, ICA Launch Mechanism, ICA Application Start up Time, ICA Process ID Launch, ICA Application Name, ICA App Module Path, ICA Application Termination Type, ICA Application Termination Time, Application Name App Id, ICA App Process ID Terminate, ICA App
  - ICA Event: Record Type, Actual Template Code, Source IPv4 Address Rx, Destination IPv4 Address Rx, ICA Session Guid, MSi Client Cookie, Connection Chain Id, ICA Client Version, ICA Client Host Name, ICA User Name, ICA Domain Name, Logon Ticket Setup, Server Name, Server Version, Flow Id Rx, ICA Flags, Observation Point Id, Exporting Process Id, Observation Domain Id, Connection Id, ICA Device Serial Number, ICA Session Setup Time, ICA Client IP, NS ICA Session Status Setup, Source Transport Port Rx, Destination Transport Port Rx, ICA Client Launcher, ICA Client Type, ICA Connection Priority

© 1999–2023 Cloud Software Group, Inc. All rights reserved.
Citrix Analytics - Usage

- Setup, NS ICA Session Server Port, NS ICA Session Server IP Address, IPv4, Protocol Identifier, Connection Chain Hop Count, Access Type

- ICA Update: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx, ICA Flags, Connection Id, ICA Device Serial Number, IPv4, Protocol Identifier, Padding Octets Two, ICA RTT, Client Side RX Bytes, Client Side Packets Retransmit, Server Side Packets Retransmit, Client Side RTT, Client Side Jitter, Server Side Jitter, ICA Network Update Start Time, ICA Network Update End Time, Client Side SRTT, Server Side SRTT, Client Side Delay, Server Side Delay, Host Delay, Client Side Zero Window Count, Server Side Zero Window Count, Client Side RTO Count, Server Side RTO Count, L7 Client Latency, L7 Server Latency, App Name App Id, Tenant Name, ICA Session Update Begin Sec, ICA Session Update End Sec, ICA Channel Id 1, ICA Channel Id 2, ICA Channel Id 2 Bytes, ICA Channel Id 3, ICA Channel Id 3 Bytes, ICA Channel Id 4, ICA Channel Id 4 Bytes, ICA Channel Id 5, ICA Channel Id 5 Bytes


- AppFlow: Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, Transaction Id, Appfw Violation Occurred Time, App Name App Id, Appfw Violation Severity, Appfw Violation Type, Appfw Violation Location, Appfw Violation Threat Index, Appfw NS Longitude, Appfw NS Latitude, Source IPv4 Address Rx, Appfw HttpMethod, Appfw App Threat Index, Appfw Block Flags, Appfw Transform Flags, Appfw Violation Profile Name, Appfw Session Id, Appfw Req Url, Appfw Geo Location, Appfw Violation Type Name 1, Appfw Violation Name Value 1, Appfw Sig Category 1, Appfw Violation Type Name 2, Appfw Violation Name Value 2, Appfw Sig Category 2, Appfw Violation Type Name 3, Appfw Violation Name Value 3, Appfw Sig Category 3, Appfw Req X Forwarded For, Appfw App Name Ls, App Name Ls, Iprep Category, Iprep Attack Time,
Iprep Reputation Score, Iprep NS Longitude, Iprep NS Latitude, Iprep Severity, Iprep HTTP Method, Iprep App Threat Index, Iprep Geo Location, Tcp Syn Attack Cntr, Tcp Slow Ris Cntr, Tcp Zero Window Cntr, Appfw Log Expr Name, Appfw Log Expr Value, Appfw Log Expr Comment

- **VPN:** Actual Template Code, Observation Domain Id, Access Insight Flags, Observation Point Id, Exporting Process Id, Access Insight Status Code, Access Insight Timestamp, Authentication Duration, Device Type, Device ID, Device Location, App Name App Id, App Name App Id1, Source Transport Port Rx, Destination Transport Port Rx, Authentication Stage, Authentication Type, VPN Session ID, EPA Id, AAA User Name, Policy Name, Auth Agent Name, Group Name, Virtual Server FQDN, cSec Expression, Source IPv4 Address Rx, Destination IPv4 Address Rx, Cur Factor Policy Label, Next Factor Policy Label, App Name Ls, App Name 1 Ls, AAA User Email Id, Gateway IP, Gateway Port, Application Byte Count, VPN Session State, VPN Session Mode, SSO Auth Method, IIP Address, VPN Request URL, SSO Request URL, Backend Server Name, VPN Session Logout Mode, Logon Ticket File Info, STA Ticket, Session Sharing Key, Resource Name, SNIP Address, Temp VPN Session ID

Action, SSLi URL Set Matched, SSLi URL Set Private, URL Category, URL Category Group, URL Category Reputation, Responder Action Type, URL Set Matched, URL Set Private, Category Domain Name, Category Domain Source, AAA User Name, VPN Session ID, Tenant Name

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

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

- Memory Pool: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Interface, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer SSL, VServer User, Memory Pool: Mem Cur Alloc Size, Mem Err Alloc Failed, Mem Tot Available

- Monitoring Service Binding: Bind Entity Name, Entity Name, NetScalerId, SchemaType, Time, CPU, Gslb Server, Gslb VServer, Interface, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Mon Service Binding: RATE Mon Tot Probes, Mon Tot Probes

- Interface: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema
Citrix Analytics - Usage

Type, Time, CPU, Gslb Server, Gslb VServer, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Interface: RATE NIC Tot Rx Bytes, RATE NIC Tot Rx Packets, RATE NIC Tot Tx Bytes, RATE NIC Tot Tx Packets, NIC Tot Rx Bytes, NIC Tot Rx Packets, NIC Tot Tx Bytes, NIC Tot Tx Packets

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

Secure Browser logs

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

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

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

• Entitlement Create:
  – Logs before the entitlement creation: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
  – Logs after the entitlement creation: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type

• Entitlement Update:
  – Logs before the entitlement update: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
  – Logs after the entitlement update: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type

• Session Access Host: Accept Host, Client IP, Date Time, Host, Session, User Name

• Session Connect:
  – Logs before the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  – Logs after the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name

• Session Launch:
Citrix Analytics - Usage

- Logs before the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- Logs after the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  • Session Tick:
    - Logs before the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
    - Logs after the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name

**Microsoft Graph Security logs**

- Tenant Id
- User Id
- Indicator Id
- Indicator UUID
- Event Time
- Create Time
- Category of alert
- Logon Location
- Logon IP
- Logon Type
- User Account Type
- Vendor Information
- Vendor Provider Information
- Vulnerability States
- Vulnerability Severity

**Microsoft Active Directory logs**

- Tenant Id
- Collect Time
- Type
Citrix Analytics - Usage

- Directory Context
- Groups
- Identity
- User Type
- Account Name
- Bad Password Count
- City
- Common Name
- Company
- Country
- Days Until Password Expiry
- Department
- Description
- Display Name
- Distinguished Name
- Email
- Fax Number
- First Name
- Group Category
- Group Scope
- Home Phone
- Initials
- IP Phone
- Is Account Enabled
- Is Account Locked
- Is Security Group
- Last Name
- Manager
- Member of
Citrix Analytics - Usage

- Mobile Phone
- Pager
- Password Never Expires
- Physical Delivery Office Name
- Post Office Box
- Postal Code
- Primary Group Id
- State
- Street Address
- Title
- User Account Control
- User Group List
- User Principal Name
- Work Phone

**Citrix Analytics for Performance logs**

- actionid
- actionreason
- actiontype
- adminfolder
- agentversion
- allocationtype
- applicationid
- applicationname
- applicationpath
- applicationtype
- applicationversion
- associateduserfullnames
- associatedusername
• associatedusernames
• associateduserupns
• authenticationduration
• autoreconnectcount
• autoreconnecttype
• AvgEndpointThroughputBytesReceived
• AvgEndpointThroughputBytesSent
• blobcontainer
• blobendpoint
• blobpath
• brokerapplicationchanged
• brokerapplicationcreated
• brokerapplicationdeleted
• brokeringdate
• brokeringduration
• brokerloadindex
• brokerregistrationstarted
• browsername
• catalogchangeevent
• catalogcreatedevent
• catalogdeletedevent
• catalogid
• catalogname
• catalogsync
• clientaddress
• clientname
• clientplatform
• clientsessionvalidatedate
• clientversion
• collecteddate
• connectedviahostname
• connectedviaipaddress
• connectionid
• connectioninfo
• connectionstate
• connectiontype
• controllerdnsname
• cpu
• cpuindex
• createddate
• currentloadindexid
• currentpowerstate
• currentregistrationstate
• currentsessioncount
• datetime
• deliverygroupadded
• deliverygroupchanged
• deliverygroupdeleted
• deliverygroupid
• deliverygroupmaintenancemodechanged
• deliverygroupname
• deliverygroupsync
• deliverytype
• deregistrationreason
• desktopgroupdeletedevent
• desktopgroupid
• desktopgroupname
• desktopkind
Citrix Analytics - Usage

- disconnectcode
- disconnectreason
- disk
- diskindex
- dnsname
- domainname
- effectiveloadindex
- enddate
- errormessage
- establishmentdate
- eventreporteddate
- eventtime
- exitcode
- failurecategory
- failurecode
- failedata
- failedate
- failurereason
- failuretype
- faultstate
- functionallevel
- gpoenddate
- gpostartdate
- hdxenddate
- hdxstartdate
- host
- hostedmachineid
- hostedmachinename
- hostingservername
• hypervisorconnectionchangedevent
• hypervisorconnectioncreatedevent
• hypervisorid
• hypervisorname
• hypervisorsync
• icartt
• icarttms
• id
• idletime
• inputbandwidthavailable
• inputbandwidthused
• instancecount
• interactiveenddate
• interactivestartdate
• ipaddress
• isassigned
• isinmaintenancemode
• ismachinephysical
• ispendingupdate
• ispreparing
• isremotecp
• issecureica
• lastderegisteredcode
• launchedviahostname
• launchedviaipaddress
• lifecyclestate
• LinkSpeed
• logonduration
• logonenddate
Citrix Analytics - Usage

- logonscriptsenddate
- logonscriptssstartdate
- logonstartdate
- long
- machineaddedtodesktopgroupevent
- machineassignedchanged
- machinecatalogchangedevent
- machinecreatedevent
- machinedeletedevent
- machinederegistrationevent
- machinednsname
- machinefaultstatechangeevent
- machinehardregistrationevent
- machineid
- machinemaintenancemodechangeevent
- machinename
- machinepvdstatechanged
- machineregistrationendedevent
- machineremovedfromdesktopgroupevent
- machinerole
- machinesid
- machineupdatedevent
- machinewindowsconnectionsettingchanged
- memory
- memoryindex
- modifieddate
- NGSConnector.ICAConnection.Start
- NGSConnector.NGSSyntheticMetrics
- NGSConnector.NGSPassiveMetrics
- NGSConnector.NGSSystemMetrics
- network
- networkindex
- networklatency
- networkinfoperiodic
- NetworkInterfaceType
- ostype
- outputbandwidthavailable
- outputbandwidthused
- path
- percentcpu
- persistentuserchanges
- powerstate
- processname
- profileloadenddate
- profileloadstartdate
- protocol
- provisioningschemeid
- provisioningtype
- publishedname
- registrationstate
- serversessionvalidatedate
- sessioncount
- sessionend
- sessionfailure
- sessionid
- sessionidlesince
- sessionindex
- sessionkey
Citrix Analytics - Usage

- sessionstart
- sessionstate
- sessionsupport
- sessiontermination
- sessiontype
- sid
- SignalStrength
- siteid
- sitename
- startdate
- totalmemory
- triggerinterval
- triggerlevel
- triggerperiod
- triggervalue
- usedmemory
- userid
- userinputdelay
- username
- usersid
- vdialogonduration
- vdaprocessdata
- vdaresourcedata
- version
- vmstartenddate
- vmstartstartdate
- windowsconnectionsetting
- xd.SessionStart
System Requirements

April 4, 2022

Before you begin using Citrix Analytics - Usage, review the following requirements:

Subscription requirements

Citrix Analytics - Usage is available free of charge with the following Citrix products and packages:

- Citrix Content Collaboration
- Citrix Workspace packages - Standard, Premium, and Premium Plus

For more information, see Citrix Cloud services.

Data sources requirements

To view the usage reports, you must use at least one of the following Citrix products, which acts as a data source for Analytics:

- Citrix Secure Private Access
- Citrix Content Collaboration
- Citrix Workspace Microapps

Supported browsers

Your workstation must have the following supported web browser:

- Latest version of Google Chrome
- Latest version of Mozilla Firefox
- Latest version of Microsoft Edge
- Latest version of Apple Safari

Getting started

April 4, 2022

This document describes how to get started with Citrix Analytics - Usage for the first time.
Step 1: Sign in to Citrix Cloud

To use Citrix Analytics - Usage, 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 Usage Analytics

After signing in to your Citrix Cloud account, do the following:

1. In the Available Services section, click Manage on the Analytics tile. You are redirected to the Analytics overview page.

2. On the Usage tile, click Get Started.

Note
For an existing user, click Manage.

Gain insights with Citrix Analytics!

Predictive and prescriptive insights into user behavior, application performance, network operations, and user productivity spanning the entire Citrix portfolio.

Security
Proactively manage and mitigate threats based on user behavior.

Performance
Gain real-time visibility and improve apps and desktops performance.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.
Step 3: Manage Usage Analytics

When you click Get Started or Manage, Analytics displays the Usage dashboards for the supported Citrix products. Analytics automatically discovers the Citrix products (data sources) associated with your Citrix Cloud account. To view your discovered data sources, click Settings > Data Sources > Usage. To get insights into the usage data, you must turn on data processing for your products on the Data Sources page.

What’s next

- View the system requirements and the supported data sources.
- Use the following dashboards for the Citrix products:
  - Content Collaboration - Provides basic usage data of the Citrix Content Collaboration service.
  - Microapps - Provides basic usage data of the Citrix Workspace service.
  - SaaS and Web Apps - Provides basic usage data of the Citrix Secure Private Access service.

Content Collaboration

August 1, 2023

Note

This feature is in preview.

The Citrix Content Collaboration data source provides telemetry about how users interact with the Citrix Content Collaboration service in your organization.

Prerequisites

- Before you begin, you must subscribe to the Citrix Content Collaboration service offered on Citrix Cloud. To learn how to set up Content Collaboration, see A quick guide to getting started.
- Review the System requirements section and ensure that you meet the requirements.

View data source and turn on data processing

Citrix Analytics automatically discovers the Content Collaboration data source associated with your Citrix Cloud account.
To view the data source:

From the top bar, click **Settings > Data Sources > Usage**.

A site card for Content Collaboration appears on the Data Sources page. Click **Turn On Data Processing** to allow Analytics to begin processing data.

View received events

The site card displays the number of events received from the data source for the last one hour, which is the default time selection. You can also select 1 week (1W) and view the data.

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.

**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. To enable data processing again, click **Turn On Data Processing**.

**Content Collaboration dashboard**

The **Content Collaboration** dashboard provides insight into the usage data of your Citrix Content Collaboration service. Citrix Analytics processes telemetry received from the Citrix Content Collaboration service and displays the usage metrics such as active users, top users, and upload volume. You
get visibility into how the Content Collaboration service is being used in your organization and how the users are interacting with the service.

The dashboard provides the following metrics:

- Number of unique users using the Content Collaboration service
- Top Content Collaboration users
- Amount of data uploaded to the Content Collaboration service
- Amount of data downloaded from the Content Collaboration service
- Number of files uploaded to the Content Collaboration service
- Number of files downloaded from the Content Collaboration service
- Number of actions performed by users on the files
- Number of share events created by the users

How to access the dashboard

To access the dashboard, from the Usage tab, click Content Collaboration.

About the reports

The usage reports are categorized as user reports and product usage reports.

User report: Displays the usage metrics of the Content Collaboration users.

- **Active users**: This report shows the number of unique users using Content Collaboration for the selected period. Each node on the graph provides the unique user count. A unique user is a distinct person using the Content Collaboration service for the specific period. Each user is counted only once for the period, regardless of how many times the user logs on to the service. From the graph, you can identify any variation in the user count and determine when the maximum users are active for the period. Click See More to view the active user trend based on the activities such as file update, file delete, file upload, and file download.
• **Top users:** This report shows the users who are sharing maximum files using Content Collaboration for the selected period. The top users are determined based on the number of links created by the users to share files and folders. In addition to the share links, you can view the amount of data uploaded (in bytes) to and downloaded (in bytes) from the Content Collaboration service. Click **See More** to view the complete list of top users.

<table>
<thead>
<tr>
<th>User</th>
<th>Upload Volume</th>
<th>Download Volume</th>
<th>Shared Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>User1</td>
<td>73022399</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>User2</td>
<td>112143971</td>
<td>15608</td>
<td>7</td>
</tr>
<tr>
<td>User3</td>
<td>1034666</td>
<td>3482791</td>
<td>6</td>
</tr>
<tr>
<td>User4</td>
<td>3804869</td>
<td>165022794</td>
<td>5</td>
</tr>
<tr>
<td>User5</td>
<td>5056871</td>
<td>11239</td>
<td>4</td>
</tr>
</tbody>
</table>

**Product usage report:** Display the usage metrics of the Content Collaboration service.

• **Upload volume:** This report shows the amount of data uploaded to Content Collaboration for the selected period. This data includes files and folders uploaded from users’ hard drives or data storage services such as Google Drive, OneDrive, and Office 365. Each node on the graph indicates the uploaded volume. From the graph, you can identify any variation in the upload volume and determine when the users uploaded maximum data during the period. Click **See More** to view the upload volume trend based on the types of connectors used.
• **Uploaded files:** This report shows the number of files uploaded to Content Collaboration for the selected period. Users can upload files from their hard drives or various data storage services such as Google Drive, OneDrive, and Office 365. Each node on the graph indicates the number of files uploaded. From the graph, you can identify any variation in the upload file count and determine when the users uploaded maximum files during the period.

• **Download volume:** This report shows the amount of data downloaded from Content Collaboration for the selected period. This data includes files and folders downloaded by the users from the Content Collaboration service to their hard drives or data storage services such as Google Drive, OneDrive, and Office 365.
Drive, OneDrive, and Office 365. Each node on the graph indicates the download volume. From the graph, you can identify any variation in the download volume and determine when the users have downloaded maximum data.

- **Download files**: This report shows the number of files downloaded from Content Collaboration for the selected period. Users can download files from the Content Collaboration service to their hard drives or data storage services such as Google Drive, OneDrive, and Office 365. Each node on the graph indicates the number of files downloaded. From the graph, you can identify any variation in the download file counts and determine when the users have downloaded maximum files during the period.
• **User actions**: This report shows the number of actions performed by the users on the files shared on Content Collaboration for the selected period. Users perform various actions on the files such as create, delete, copy, download, and upload. Each node on the graph indicates the number of user actions. From the graph, you can identify any variation in user actions and determine when the users are most actively working on the files. Click **See More** to view the trend based on the user actions.

• **Share events**: This report shows the number of share events for the selected period. When a user creates or modifies links for sharing files or folders, share events are triggered. From the
graph, you can identify any variation in the share event count and determine when the users triggered maximum share events for the period. Click See More to view the share events based on the type of links such as created links, shared links, and updated links.

Microapps

December 3, 2020

Note
This feature is in preview.

The Workspace Microapps data source provides telemetry about how users interact with the microapps service and its notifications.

Prerequisites

- Before you begin, you must have a subscription to use the Citrix Workspace Microapps service offered on Citrix Cloud. To learn how to get started, see the Getting started article in the Microapps documentation.
- Review the System requirements section and ensure that you meet the requirements.
Citrix Analytics - Usage

View data source and turn on data processing

Citrix Analytics automatically discovers the **Workspace Microapps** data source associated with your Citrix Cloud account.

**To view the data source:**

From the top bar, click **Settings > Data Sources > Usage**.

A site card for **Workspace Microapps** appears on the **Data Sources** page. Click **Turn On Data Processing** to allow Analytics to begin processing data.

View received events

The site card displays the number of 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.

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.

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. To enable data processing again, click Turn On Data Processing.

Microapps dashboard

The Microapps dashboard provides insight into the usage data of your Citrix Workspace Microapps service. The Microapps service delivers actions and notifications from users’ applications to their Citrix Workspace. Citrix Analytics processes the telemetry data received from the Microapps service and displays the usage metrics such as total active users, user-initiated actions, and notification actions. You get visibility into how the microapps are being used in your organization and how the users are interacting with the microapps and their notifications.

The dashboard provides the following metrics:
Citrix Analytics - Usage

- Number of unique users using the microapps
- Top microapps users
- Most used microapps
- Number of actions initiated by the users using the microapps
- Number of actions taken by the users on the notifications delivered by the microapps

How to access the dashboard

To access the dashboard, from the Usage tab, click Microapps.

About the reports

The usage reports are categorized as user reports and product usage reports.

User report: Displays the usage metrics of the microapps users.

- **Active users**: This report shows the Workspace app users using the microapps for the selected period. Each node on the graph indicates the unique user count. A unique user is a distinct person using the microapps for the specific period. Each user is counted only once for the period, regardless of the number of microapps the person is using. From the graph, you can identify any variation in the user count and determine when the users are most active during the period. Click See More to view the active user trend based on the activities such as the notifications actions, user-initiated actions, and page views.

- **Top users**: This report shows the Workspace app users using maximum microapps for the selected period. The top users are measured by the following metrics:
- **Notification-actions**: Number of actions taken on the microapp notifications by the users. For example, microapp notifications such as *New Expense Report for Approval* and *New Course Available for Registration* require actions from the users.

- **User-initiated actions**: Number of actions initiated by the users using the microapps. For example, *Request PTO*, *Submit a Help Desk Ticket* and *Search the Directory* are the activities initiated by the users through the corresponding microapps.

- **Page views**: Number of microapp pages viewed by the users.

Click **See More** to view the complete list of the top users. You can filter the users by microapps and view the top users for each microapp.

### Product usage report:
Displays the usage metrics of your Citrix Workspace Microapps service.

- **Top microapps**: This report shows the most used microapps in your organization for the selected period. The top microapps are determined by the following metrics:
  - **Unique users**: A unique user is a distinct person using the microapp for the specific period. Each user is counted only once for the period, regardless of the number of times the person uses the microapp for the selected period. For example, if a person uses the “Request PTO” microapp three times during the period, Analytics counts the user as one unique user.
  - **Notification actions**: Number of actions taken on the microapp notifications by the users.
  - **User-initiated actions**: Number of actions initiated by the users using the microapp.

Click **See More** to get the complete list of the top microapps for your organization.

### Top microapps

<table>
<thead>
<tr>
<th>Microapp</th>
<th>Unique Users</th>
<th>Notification Actions</th>
<th>User-Initiated Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test App 1</td>
<td>9</td>
<td>122</td>
<td>117</td>
</tr>
<tr>
<td>Test App 2</td>
<td>4</td>
<td>50</td>
<td>1</td>
</tr>
<tr>
<td>Test App 3</td>
<td>4</td>
<td>30</td>
<td>18</td>
</tr>
<tr>
<td>Test App 4</td>
<td>3</td>
<td>66</td>
<td>0</td>
</tr>
<tr>
<td>Test App 5</td>
<td>3</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

- **Notification activity**: This report shows the number of actions taken by the users on the microapp notifications for the selected period. Each node on the graph represents the number of
user actions. From the graph, you can view the variation in the user actions and identify the period when the user actions are maximum. Click **See More** to view the trend based on the user actions such as page views, dismissed notifications, and expired notifications and view its trend.

- **Client OS versions**: This report shows the percentage distribution of operating systems across the client endpoints. From the chart, you can determine the operating systems that are mostly used by the users in your organization.
SaaS and Web Apps

April 4, 2022

Note
This feature is in preview.

The SaaS and Web Apps (Secure Private Access Service) data source provides telemetry about how users interact with the SaaS and Web applications in your organization.

Prerequisites

- Before you begin, you must have a subscription to use the Citrix Secure Private Access service offered on Citrix Cloud. To learn how to get started with Secure Private Access, see Secure Private Access service.
- Review the System requirements section and ensure that you meet the requirements.

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 > Usage.

A site card for SaaS and Web Apps (Secure Private Access Service) appears on the Data Sources page. Click Turn On Data Processing to allow Analytics to begin processing data.
View received events

The site card displays the number of 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.

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.
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. To enable data processing again, click **Turn On Data Processing**.

SaaS and Web Apps (Secure Private Access) dashboard

The **SaaS and Web Apps** dashboard provides insight into the usage data of your published SaaS and enterprise Web applications in your organization. Citrix Analytics processes telemetry received from the Citrix Secure Private Access service and displays the usage metrics such as active users, top users, and total applications. You get visibility into how the users are interacting with the SaaS and Web applications and identify the most used applications in your organization.

The dashboard provides the following information about your published SaaS and Web applications:

- Number of unique users using the SaaS and Web applications
- Top SaaS and Web application users
- Number of SaaS and Web applications launched
Citrix Analytics - Usage

- Top SaaS and Web applications
- Top domains accessed by the users
- Total amount of data uploaded and downloaded (in bytes) across users, applications, and domains

How to access the dashboard

To access the dashboard, from the Usage tab, click SaaS and Web Apps.

About the reports

The usage reports are categorized as user reports, application reports, and domain reports.

User report: Displays the usage metrics of the users using the SaaS and Web applications.

- **Active users**: This report shows the number of unique users using the SaaS and Web applications for the selected period. Each node on the graph provides the unique user count. A unique user is a distinct person using the applications for the selected period. Each user is counted only once, regardless of how many applications the user is using during the period. For example, if a user A is using two SaaS applications at 10 AM, the user is counted as one. From the graph, you can identify any variation in the user count and determine when maximum users are active during a period. Click See More to view the active users' trend based on the application type such as SaaS or Web.

- **Top users**: This report shows the users launching maximum SaaS or Web applications for the selected period. The top users are determined by the number of application instances launched by them. If a user is using two instances of the same application, the number of applications launched is counted as two. You can view the data upload volume (in bytes), data download volume (in bytes), and the total amount of the data used (in bytes) by each user. Click See More.
to get the complete list of the top users. You can also view the top users based on the application type such as SaaS or Web.

<table>
<thead>
<tr>
<th>User</th>
<th>Total Apps Launched</th>
<th>Total Download Volume</th>
<th>Total Upload Volume</th>
<th>Total Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>User A</td>
<td>4</td>
<td>3528</td>
<td>41661</td>
<td>45189</td>
</tr>
<tr>
<td>User B</td>
<td>1</td>
<td>1532</td>
<td>9523</td>
<td>81355</td>
</tr>
<tr>
<td>User C</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>User D</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Application reports**: Displays the usage metrics of your published SaaS and Web applications.

- **App launched**: This report shows the number of SaaS applications and Web applications launched by the users for the selected period. Each node on the graph indicates the number of unique applications running during the specific time. Each distinct application or multiple instances (sessions) of the same application is counted only once for the selected period. For example, if two instances of Office 365 are running at 10 AM, it is counted as one. From the graph, you can detect any variation in the application count and determine when the users are using maximum applications. Click **See More** to view the trend based on the application type such as SaaS or Web.

- **Top apps**: This report shows the most used SaaS and Web applications. The top applications are determined by the number of instances (sessions) running for each application. You can view the data upload volume (in bytes), data download volume (in bytes), and total amount of the data used (in bytes) by the application instances. Click **See More** to get more details about the applications. You can view the top applications based on the application type such as SaaS or Web.
Citrix Analytics - Usage

Domain report: Displays the usage metrics of the domains accessed by the users.

- Top domains: This report shows the most accessed domains by the users in your organization. For each domain, you can view the sessions launched, the unique user count, data upload volume (in bytes), data download volume (in bytes), and the total amount of the data used (in bytes). Click See More to view the top domains based on the application type such as SaaS or Web.

FAQs

October 4, 2023

Data source

What is a data source?

Data sources are Citrix services and products that send data to Citrix Analytics.

Learn more: Data Source

How do I add a data source?

After you log on to Citrix Analytics, on the Welcome screen, select Get Started to add a data source to Citrix Analytics. Alternatively, you can also add a data source by navigating to Settings > Data Sources.
Citrix Analytics - Usage

Citrix ADM agent

What are the minimum resource requirements to install an agent on a hypervisor on-premises?

8 GB RAM, 4 Virtual CPU, 120 GB Storage, 1 Virtual Network Interfaces, 1 Gbps Throughput

Do I need to assign an additional disk to Citrix ADM agent while provisioning?

No, you do not have to add an additional disk. The agent is used only as an intermediary between Citrix Analytics and the instances in your enterprise data center. It does not store inventory or analytics data that would require an additional disk.

What are the default credentials to log on to an agent?

The default credentials to log on to the agent is `nsrecover/nsroot`. This logs you on to the shell prompt of the agent.

How do I change the network settings of an agent if I have entered an incorrect value?

Log on to the agent console on your hypervisor and access the shell prompt by using the credentials `nsrecover/nsroot`, and then run the command `networkconfig`.

Why do I need a service URL and an activation code?

The agent uses the service URL to locate the service and the activation code to register the agent with the service.

How can I reenter service URL if I have typed it incorrectly in the agent console?

Log on to the shell prompt of the agent by using the credentials `nsrecover/nsroot`, and then type: `deployment_type.py`. This script lets you reenter the Service URL and activation code.

How do I get a new activation code?

You can get a new activation code from Citrix ADM service. Log on to Citrix ADM service and navigate to Networks > Agents. On the Agents page, from the Select Action list, select Generate Activation Code.

Can I reuse my activation code with multiple agents?

No, you cannot.
How many Citrix ADM agents do I need to install?

The number of agents depends on the number of managed instances in a data center and the total throughput. Citrix recommends that you install at least one agent for every data center.

How do I install multiple Citrix ADM agents?

On the Data Sources page, click the plus (+) sign next to Citrix Gateway and follow the instructions to install another agent.

Alternatively, you can access the Citrix ADM GUI and navigate to Networks > Agents and click **Set Up Agent** to install multiple agents.

Can I install two agents in a high availability setup?

No, you cannot.

What do I do if my agent registration fails?

- Make sure that your agent has access to the Internet (configure DNS).
- Make sure you have copied the activation code correctly.
- Make sure you have entered the service URL correctly.
- Make sure you have the required ports open.

Registration is successful, but how do I know if the agent is running fine?

You can do the following to check if the agent is running fine:

- After the agent is successfully registered, access Citrix ADM and navigate to **Networks > Agents**. You can view the discovered agents on this page. If the agent is running fine, the status is indicated by a green icon. If it is not running, the state is indicated by a red icon.

- Log on to the agent's shell prompt and run the following commands: `ps -ax | grep mas` and `ps -ax | grep ulfd`. Ensure that the following processes are running.
• If any of the processes is not running, run the command **masd restart**. This might take some time to start all the daemons (1 minute or so).

• Make sure **agent.conf** is created in `/mpsconfig` after successful registration of agent.

### Onboarding Citrix Gateway instances

**Citrix Gateway Instances are added to Citrix Analytics, but how do I know if Analytics is enabled on the Agent?**

You can verify if analytics is enabled on the agent using the agent's shell prompt. If analytics is successfully enabled on the agent, the **turnOnEvent** parameter would be set to **Y** in the `/mpsconfig/telemetry_cloud.conf` file.

Log on to the agent's shell prompt and run the following command: `cat /mpsconfig/telemetry_cloud.conf` and verify the value of the **turnOnEvent** parameter.
I accidentally closed the Citrix Gateway onboarding wizard. Do I have to start my configuration from the beginning?

No. Citrix Analytics saves the progress and displays the incomplete configuration as a tile in the Data Sources > Settings page. Click Continue setup to complete the configuration.

Onboarding Virtual Apps and Desktops Site

How do I turn data processing off?

If you want to temporarily disable data processing from your Site to Citrix Analytics, simply click the Site card and then click Turn off data processing.

When I add my Site to Workspace and click “Test STA,” the test fails. What do I do?

There might be a connectivity issue between your Citrix Gateway and Cloud Connectors. To troubleshoot, see CTX232517 in the Citrix Support Knowledge Center.

Where can I get help with Citrix Analytics?

You can ask questions and connect with Citrix Analytics experts in the Citrix Analytics Discussion Forum at https://discussions.citrix.com/forum/1710-citrix-analytics/.

To participate in the forum, you must sign in with your Citrix ID.

Access assurance – Geolocation

How are geolocation details derived by Analytics?

Citrix Analytics uses the IP address of the device from where the workspace client is launched. Citrix Analytics leverages a third party IP geolocation data provider to derive a user’s location from their IP address. When you perform a session logon, it resolves your location (IPv4 address) to a country or city, and the mapping is updated periodically. Organizations can use these locations defined by countries to monitor access patterns from where they don’t do business.

What is the accuracy level of deriving a user’s location?

Citrix Analytics leverages a third party IP geolocation data provider to derive a user’s location from their IP address. GeoIP services are able to resolve to the right city or location most of the time, but GeoIP look-ups are never completely accurate. Sometimes the location shown for a user might be different from their precise location of access.
Based on IP GeoPoint documentation, the coverage level is about 99.99% of allocated IP addresses worldwide (IPv4 routable IP addresses). In terms of location accuracy, it accompanies each of the essential location fields (country, state, city, postal code) with a Confidence Factor.

**In which cases are the determination of location inaccurate?**

The accuracy of geolocation data depends on how the device connects to the internet. A device can connect to the internet through:

- Mobile gateways
- VPN or hosting facility
- Regional or international proxies/anonymizer server

In such cases, geolocation data is not accurate regardless of using the IP geolocation provider software.

**What is the supported Citrix Workspace app versions?**

There are minimum versions of Citrix Workspace app required for the operating system to send the IP address attribute to Citrix Analytics for Security. Refer the matrix table or Locations identified as not available for more details.

**In which cases do we not receive the geological details?**

To view the geolocation details, refer Locations identified as not available section for details.

**What Geolocation service does Citrix Analytics use to report a user’s location? How to report a wrong location for an IP?**

Citrix Analytics uses Neustar file-based geolocation services to provide geolocation data for incoming accesses. It has a public facing IP correction page which can be used to self-submit a correction request. Once a correction request is submitted, the request is reviewed by Neustar for accuracy and processed.

The GeoIP provider helps to show as accurate information as possible. Unfortunately, there might be cases where the GeoIP data is inaccurate due to the innate nature of GeoIP.

**Glossary of terms**

September 28, 2023
• **Actions**: Closed loop responses to suspicious events. Actions are applied to prevent future anomalous events from occurring. [Learn more.]

• **Cloud Access Security Broker (CASB)**: On-premises or cloud-based security policy enforcement point placed between cloud service consumers and cloud service providers. CASBs combine and interject enterprise security policies as cloud-based resources are accessed. They also help organizations to extend security controls of their on-premises infrastructure to cloud.

• **Citrix ADC (Application Delivery Controller)**: Network device that lives in a data center, located strategically between the firewall, and one or more application servers. Handles load balancing between servers and optimizes end-user performance and security for enterprise applications. [Learn more.]

• **Citrix ADM (Application Delivery Management)**: Centralized network management, analytics, and orchestration solution. From a single platform, administrators can view, automate, and manage network services for scale-out application architectures. [Learn more.]

• **Citrix ADM agent**: Proxy that enables communication between Citrix ADM and the managed instances in a data center. [Learn more.]

• **Citrix Analytics**: Cloud service that collects data across services and products (on-premises and cloud), and generates actionable insights, enabling administrators to proactively handle user and application security threats, improve app performance, and support continuous operations. [Learn more.]

• **Citrix Cloud**: Platform that connects to resources through the Citrix Cloud Connector on any cloud or infrastructure (on-premises, public cloud, private cloud, or hybrid cloud). [Learn more.]

• **Citrix Gateway**: Consolidated remote access solution that consolidates remote access infrastructure to provide single sign-on across all applications whether in a data center, in the cloud, or delivered as SaaS. [Learn more.]

• **Citrix Hypervisor**: Virtualization management platform optimized for application, desktop, and server virtualization infrastructures. [Learn more.]

• **Citrix Workspace App** (formerly known as Citrix Receiver): Client software that provides seamless, secure access to applications, desktops and data from any device, including smartphones, tablets, PCs, and Macs. [Learn more.]

• **DLP (Data Loss Prevention)**: Solution that describes a set of technologies and inspection techniques to classify information contained in an object such as file, email, packet, application, or a data store. Also, the object can also be in storage, in use, or across a network. DLP tools can dynamically apply policies such as log, report, classify, relocate, tag, and encrypt. DLP tools can also apply enterprise data rights management protections. [Learn more.]

• **DNS (Domain Name System)**: Network service that is used to locate internet domain names and translate them to internet protocol (IP) addresses. DNS maps website names that users pro-
vide, to their corresponding IP-addresses that machines provide, to locate a website regardless of the physical location of the entities.

- **Data processing**: Method of processing data from a data source to Citrix Analytics. [Learn more.](#)
- **Data source**: Product or service that sends data to Citrix Analytics. A data source can be internal or external. [Learn more](https://en-us/citrix-analytics/data-sources.html).
- **Data export**: Product or service that receives data from Citrix Analytics and provides insights. [Learn more.](#)
- **Discovered users**: Total number of users in an organization that use data sources. [Learn more.](#)
- **FQDN (Fully Qualified Domain Name)**: Complete domain name for internal (StoreFront) and external (Citrix ADC) access.
- **Machine learning**: Type of data analysis technology that extracts knowledge without being explicitly programmed to do so. Data from a wide variety of potential sources such as applications, sensors, networks, devices, and appliances are fed into a machine learning system. The system uses the data and applies algorithms to build its own logic to solve a problem, derive insight, or make a prediction.
- **Microsoft Graph Security**: Gateway that connects customer security and organizational data. Provides easy-to-review alerts and remediation options when an action must be taken. [Learn more.](#)
- **Performance Analytics**: Service that provides visibility into user session details across an organization. [Learn more.](#)
- **Policy**: Set of conditions to be met for an action to be applied on a user’s risk profile. [Learn more.](#)
- **Risk indicator**: Metric that provides information about the level of exposure to a business risk that the organization has at a given time. [Learn more.](#)
- **Risk score**: Dynamic value that indicates the aggregate level of risk a user or an entity poses to an IT infrastructure over a pre-determined monitoring period. [Learn more.](#)
- **Risk timeline**: Record of a user’s or an entity’s risky behavior that allows administrators to probe into a risk profile and understand the data usage, device usage, application usage, and location usage. [Learn more.](#)
- **Risky user**: User that has acted in a risky manner or presented risky behavior. [Learn more.](#)
- **Security Analytics**: Advanced analysis of data that is used to achieve compelling security outcomes such as security monitoring and threat hunting. [Learn more.](#)
- **Secure Private Access**: Service that provides integration of single sign-on, remote access, and content inspection into a single solution for end-to-end access control. [Learn more.](#)
• **Splunk**: SIEM (Security Information and Event Management) software that receives intelligent data from Citrix Analytics and provides insights about the potential business risks. [Learn more.]

• **UBA (User Behavior Analytics)**: Process of baselining user activity and behavior combined with peer group analysis, to detect potential intrusions, and malicious activity.

• **Watchlist**: List of users or entities whom administrators want to monitor for suspicious activities. [Learn more.]