Citrix Analytics
## Contents

- **What's new** ........................................... 3
- **Known issues** ....................................... 8
- **Data Sources** ....................................... 8
- **Data Governance** .................................... 9
- **Technical security overview** ..................... 40
- **System Requirements** .............................. 44
- **Getting started** .................................... 48
- **Find your way around** ............................ 50
- **Self-service search** ............................... 54
- **Citrix Analytics for Security (Security Analytics)** 62
- **Citrix Analytics for Operations (Operations Analytics)** 64
- **Citrix Analytics for Performance (Performance Analytics)** 65
- **Troubleshoot Citrix Analytics** .................. 69
- **FAQs** .............................................. 94
- **Glossary of terms** .................................. 98
What’s new

April 17, 2020

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.

Citrix Analytics has the following products or offerings. Refer to the What’s new articles specific to each offering to know about the new features and product updates.

- Citrix Analytics for Security
- Citrix Analytics for Operations
- Citrix Analytics for Performance

This release notes highlight the new features and product updates specific to the Citrix Analytics platform.

February 20, 2020

New features

Citrix Analytics subscription offerings

Delivering flexible purchase options to users, Citrix now offers three individual subscription-based Citrix Analytics products. Citrix Analytics provides unique security or performance (or both) insights based on the offering that you subscribe to.

You can purchase the following Citrix Analytics subscription offerings:

- Citrix Analytics for Security
- Citrix Analytics for Performance
- Citrix Analytics for Security and Performance (bundle)

Data governance logs updates

Added new logs for the following data sources:

- Citrix Identity Provider
- Citrix Gateway
- Secure Browser
Citrix Analytics

- Microsoft Graph Security
- Microsoft Active Directory

For more information, see Data governance.

Fixed issues

- Self-service search does not work accurately on Internet Explorer 11. Therefore, you cannot type your search query and perform a search operation. [CAS-18657]

January 09, 2020

Fixed issues

- The Citrix Analytics walk-through functionality is not working for the users in the European Union home region. [CAS-26297]

December 18, 2019

Fixed issues

The Analytics tile on the Citrix Cloud page displayed the View Service button. This button is now changed to Manage for better user experience. [CAS-27922]

December 12, 2019

New features

Support for Microapps service events in Asia Pacific South

Citrix Analytics platform now processes notifications from the Microapps service in the Asia Pacific South region. However, records that measure performance, stability, usage, security, and support are aggregated and stored in the United States. For more information, see Data governance.

Note

Microapps service is offered as part of Citrix Workspace. For more information, see Microapps documentation.
December 04, 2019

Fixed issues

Some users in the Asia Pacific-South region are unable to sign into Citrix Analytics although they have onboarded to Citrix Cloud by selecting United States as the home region. [CAS-27368]

November 22, 2019

New features

Redesigned overview page for Analytics

The Analytics overview page is redesigned to allow access to all the Analytics offerings from this page. You can request for a trial, try demo, or manage your Analytics offering. Currently, only Security Analytics and Operations Analytics are generally available and therefore, active on this page.

To view the overview page, select Help > Overview.
October 21, 2019

New features

Technical security overview

The technical security overview provides you an understanding of the security best practices related to Citrix Analytics. This document describes the data flow, data protection, network requirements, and the security responsibilities that need to be considered when using Citrix Analytics.

September 11, 2019

Fixed issues

- Citrix Cloud is unable to redirect users to the region-specific Citrix Analytics page. [CAS-20559]

August 20, 2019

Fixed issues

- The Citrix Analytics walkthrough functionality does not load accurately on the Microsoft Edge and Safari browsers. [CAS-20906]

July 31, 2019

New features

Support for the European Union region

Citrix Analytics now supports the European Union region. You can choose European Union as a home region while onboarding your organization to Citrix Cloud and use the Citrix Analytics service. Citrix Analytics stores the user events and metadata for your organization in the European Union region. For more information on Citrix Cloud regions, see Geographical Considerations.

June 26, 2019

Fixed issues

- Citrix Analytics does not load accurately on Internet Explorer 11. [CAS-19867]
June 19, 2019

Fixed issues

- Citrix Analytics does not load accurately on Microsoft Edge. [CAS-19930]

November 16, 2018

Fixed issues

- If you are accessing Citrix Analytics using Internet Explorer version 11.0, the Citrix Cloud navigation bar fails to load and restricts you from accessing the hamburger menu.

October 10, 2018

Architecture and platform enhancements

Multiple architectural and platform improvements were done in this release to enhance performance, scale, monitoring, supportability, security, and user experience.

August 23, 2018

Citrix Analytics is a cloud service delivered through Citrix Cloud. It collects data across Citrix portfolio products and provides actionable insights, enabling administrators to proactively handle security threats, improve app performance, and support continuous operations. Currently, Citrix Analytics provides the following analytics offerings:

- **Security Analytics**: Collates and provides visibility into user and entity behavior. For more information, see Security Analytics.

- **Operations Analytics**: Collates and presents information on the activities of users, such as, websites visited, and the bandwidth spent. For more information, see Operations Analytics.

New product names

The Citrix products supported by Citrix Analytics are now renamed as part of the Citrix unified product portfolio.

You might notice new names in our products and product documentation. This is a result of the expansion of the Citrix portfolio and cloud strategy. For more details about the Citrix unified portfolio, see Citrix product guide.

Implementing this transition in our products and their documentation is an ongoing process.
Citrix Analytics

- In-product content and documentation might still contain former names. For example, you might see instances of earlier names in console text, messages, directory/file names, screen-shots, and diagrams.

- It is possible that some items (such as commands) might continue to retain their former names to prevent breaking existing customer scripts.

- Related product documentation and other resources (such as videos and blog posts) that are linked from this product's documentation might still contain former names.

Known issues

February 14, 2020

This article highlights the known issues specific to the Citrix Analytics platform. For issues specific to each offering, see the corresponding Known issues articles: Security, Operations, and Performance.

- The Launch Demo link for Citrix Analytics is not available when accessing Citrix Cloud using Safari.

  Workaround: Use a different web browser such as Google Chrome, Internet Explorer, or Microsoft Edge, or access the demo application https://analytics-demo.cloud.com directly after logging on to Citrix Cloud. [CAS-24776]

Data Sources

April 7, 2020

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

- **Citrix data sources.** Citrix Cloud services and on-premises products that send data to Citrix Analytics. Citrix Analytics automatically discovers the Citrix Cloud services such as Content Collaboration and Endpoint Management that are associated with your Citrix Cloud account. This also includes Citrix ADC instances added to Citrix Application Delivery Management (ADM) and on-premises Citrix Virtual Apps and Desktops added to Citrix Workspace.

- **External data sources.** Third party applications such as Microsoft Graph Security, Microsoft Active Directory that can be integrated with Citrix Analytics. Citrix Analytics collects data from these external data sources after successful integration.
**Supported data sources**

Depending on the Citrix Analytics offering that you are using, data sources vary. Refer to the following articles to view the data sources supported by each offering:

- Data sources supported by Citrix Analytics for Security
- Data sources supported by Citrix Analytics for Operations
- Data sources supported by Citrix Analytics for Performance

**Data Governance**

February 3, 2020

This section provides information regarding the collection, storage, and retention of logs by 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 and the European Union. 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 located 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 Analytics

- Citrix Access Control
- Citrix ADC (on-premises) along with subscription for Citrix Application Delivery Management
- Citrix Content Collaboration
- Citrix Endpoint Management
- Citrix Virtual Apps and Desktops (service and on-premises offerings)
- Microapps service

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 on-premises 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.

For the Microapps service, the administrator cannot explicitly enable Citrix Analytics to analyze and store the logs. The logs are transmitted to Citrix Analytics after Microapps is configured.

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, 2018, then by default, data collected on January 1, 2018, will be retained in Citrix Analytics until January 31, 2019, the data collected on January 15, 2018, will be retained until February 15, 2019, and so on.
Citrix Analytics

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 data 90 days after the expiry of subscription or trial period.

**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 customer account for storage or data in 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 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.

At all times, information received by Citrix are treated in accordance with Citrix’s Privacy Policy, which can be found at: [https://www.citrix.com/about/legal/privacy/](https://www.citrix.com/about/legal/privacy/).

**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 Analytics

- Citrix Virtual Apps and Desktops logs
- Citrix ADC logs
- Citrix Managed Desktops logs
- Microapps service logs
- Citrix Identity provider logs
- Citrix Gateway logs
- 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
Citrix Analytics

- 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
• 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
• 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
• 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
- 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 Virtual Apps and Desktops logs**

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

- App Name
- Browser
- Details: Format Size, Format Type, Initiator, Result
- Device Id
- Device Type
The Citrix ADC logs contain the following data points:

- Container
- Files
- Format
- Type
Citrix Analytics

Citrix Managed Desktops logs

The Citrix Managed Desktops logs contain the following data points:

- App Name
- Browser
- Details: Format Size, Format Type, Initiator, Result
- Device Id
- Device Type
- File Name
- File Path
- File Size
- Jail Broken
- Job Details: File Name, Format, Size
- Location: Estimated, Latitude, Longitude
- 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
Microapps service logs

- Microapp Name
- Microapp ID
- Notification Name
- Notification ID
- Notification Priority
- Integration (App) ID
- Integration (App) UUID
- Integration (App) Name
- Integration (App) Class
- Channel
- User Recipient/Enacting E-mail
- User Recipient/Enacting OID
- User Citrix Customer ID
- Subscribers User List
- Group Recipient OID
- Action ID
- Action Type
- Action Timestamp
- Action Duration
- Action Result
- Action Noun
- Action Verb
- Page/Card ID
- Page/Card UUID
- Page/Card Title
- Page/Card Entity
- Page/Card RecordId
- Event ID
Citrix Analytics

- Event UUID
- Event Title
- Event Type
- Event Channel
- Event Entity
- Button ID
- Button UUID
- Button Title
- Data Integration Provider API Call Average Duration
- Data Integration Provider API Call Peak Rate
- Data Integration Provider API Call Rate
- Data Integration Provider API Calls Total
- Data Integration Provider API Call Duration
- Data Integration Provider API Call Result

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:
      - 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
Citrix Analytics

* 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 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 Http Method, Appfw App Threat Index, Appfw Block Flags, Appfw Transform Flags, Appfw Violation Profile Name, Appfw Session Id, Appfw Req Url, Appfw Geo Location, Appfw Violation Type Name 1, Appfw Violation Name Value 1, Appfw Sig Category 1, Appfw Violation Type Name 2, Appfw Violation Name Value 2, Appfw Sig Category 2, Appfw Violation Type Name 3, Appfw Violation Name Value 3, Appfw Sig 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 Id 1, 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
Citrix Analytics

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


- 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 Responses, RATE Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Svrf Ttfb, RATE Si Tot Svrf Ttfb Transactions, RATE Si Tot Ttlb Tolerating Transactions, RATE Si Cur State, Si Tot Request Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, RATE Si Cur Transport

- Server SVC CFG: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Svc Cfg: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Svrf Busy Err, RATE Si Tot Svrf Ttfb, RATE Si Tot Ttlb Tolerating Transactions, RATE Si Tot Ttlb Tolerating Transactions, RATE 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 Svrf Busy Err, Si Tot Svrf Ttfb, Si Tot Ttlb Tolerating Transactions, Si Tot Ttlb Tolerating Transactions

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

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

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

- Interface: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema
Type, Time, CPU, Gslb Server, Gslb VServer, Interface, 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 Re-
quests, 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, IPAddress, Last Updated, Launch Source, User Name
  - Logs after the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IPAddress, Last Updated, Launch Source, User Name

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

• Session Tick
  - Logs before the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IPAddress, Last Updated, Launch Source, User Name
  - Logs after the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IPAddress, 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
- 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
• Mobile Phone
• Pager
• Password Never Expires
• Physical Delivery Office Name
• Post Office Box
• Postal Code
• Primary Group Id
• State
Citrix Analytics

- 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
- blobcontainer
- blobendpoint
- blobpath
- brokerapplicationchanged
- brokerapplicationcreated
- brokerapplicationdeleted
- brokeringdate
- brokeringduration
- brokerloadindex
- brokerregistrationstarted
- browsername
- catalogchangeevent
- catalogcreatedevent
- catalogdeletedevent
- catalogid
- catalogname
- catalogsync
- clientaddress
- clientname
- clientplatform
- clientsessionvalidatedate
- clientversion
- collecteddate
- connectedviahostname
- connectedviapaddress
- connectionid
- connectioninfo
- connectionstate
- connectiontype
- controllerdnsname
- cpu
- cpuindex
- createddate
- currentloadindexid
- currentpowerstate
- currentregistrationstate
- currentsessioncount
- datetime
- deliverygroupadded
- deliverygroupchanged
- deliverygroupdeleted
- deliverygroupid
- deliverygroupmaintenancemodechanged
- deliverygroupname
- deliverygroupsync
- deliverytype
- deregistrationreason
- desktopgroupdeletedevent
- desktopgroupid
- desktopgroupname
- desktopkind
- disconnectcode
- disconnectreason
- disk
- diskindex
- dnsname
- domainname
- effectiveloadindex
- enddate
- errormessage
- establishmentdate
• eventreporteddate
• eventtime
• exitcode
• failurecategory
• failurecode
• failedata
• failurereason
• failurereason
• faltstate
• functionallevel
• gpoenddate
• gpostartdate
• hdxenddate
• hdxstartdate
• host
• hostedmachineid
• hostedmachinename
• hostingservername
• hypervisorconnectionchangedevent
• hypervisorconnectioncreatedevent
• hypervisorid
• hypervisorname
• hypervisorsync
• icartt
• icarttms
• id
• idletime
• instancecount
- interactiveenddate
- interactivestartdate
- ipaddress
- isassigned
- isinmaintenancemode
- ismachinephysical
- ispendingupdate
- ispreparing
- isreconnect
- isremotepc
- issecureica
- lastderegisteredcode
- launchedviahostname
- launchedviaipaddress
- lifecyclestate
- logonduration
- logonenddate
- logonscriptsenddate
- logonscriptsstartdate
- logonstartdate
- long
- machineaddedtodesktopgroupevent
- machineassignedchanged
- machinecatalogchangedevent
- machinecreatedevent
- machinedeletedevent
- machinederegistrationevent
- machinednsname
- machinefaultstatechangeevent
• machinehardregistrationevent
• machineid
• machinemaintenancechangeevent
• machinename
• machinepvdstatechanged
• machineregistrationendedevent
• machineremovedfromdesktopgroupevent
• machinerole
• machinesid
• machineupdatedevent
• machinewindowsconnectionsettingchanged
• memory
• memoryindex
• modifieddate
• network
• networkindex
• ostype
• path
• percentcpu
• persistentuserchanges
• powerstate
• processname
• profileloadenddate
• profileloadstartdate
• protocol
• provisioningschemeid
• provisioningtype
• publishedname
• registrationstate
• serversessionvalidatedate
• sessioncount
• sessionend
• sessionid
• sessionidlesince
• sessionindex
• sessionkey
• sessionstart
• sessionstate
• sessionsupport
• sessiontype
• sid
• siteid
• sitename
• startdate
• totalmemory
• triggerinterval
• triggerlevel
• triggerperiod
• triggervalue
• usedmemory
• userid
• username
• usersid
• vdialogonduration
• version
• vmstartenddate
• vmstartstartdate
• windowsconnectionsetting
Technical security overview

March 30, 2020

The Analytics service hosted in Citrix Cloud collects data across Citrix portfolio products and third-party products. These products are called data sources. Citrix Analytics supports both cloud and on-premises data sources. The information in this document applies to Citrix Analytics and its data sources.

Data flow

Citrix Analytics automatically discovers the Citrix Cloud data sources that are subscribed to the customers. But the on-premises data sources require additional configuration to integrate with Analytics. For example, you have to add your on-premises Citrix Virtual Apps and Desktops Sites to Citrix Workspace before Analytics can discover the Sites. Similarly, on-premises Citrix Gateway requires you to configure a Citrix ADM agent. For more information on enabling Analytics on the data sources, see Enable Analytics on Citrix data sources.

You can integrate a few third-party products such as Microsoft Graph Security and Microsoft Active Directory with Analytics. For more information, see the following topics:

- Enable Analytics on Microsoft Graph Security
- Integrate Analytics with Microsoft Active Directory

Citrix Analytics can also send risk intelligence information to customer-owned Splunk environment. This integration requires deploying and configuring Citrix Analytics Add-on for Splunk on the Splunk environment. For more information, see Splunk integration.

Without customer consent, Citrix Analytics does not process any events received from the data sources. To process the events from the data sources, the Analytics administrator must enable data processing. For more information on data collection, storage, and retention by Analytics, see Data governance.

Network requirements

- **Citrix Cloud services requirements**: To use the Citrix Cloud services, you must be able to connect to the required Citrix addresses through the HTTPS port 443. For more information, see Internet Connectivity requirements.

- **Citrix Analytics requirements**: Review the system requirements before using Analytics. In addition to the Citrix Cloud requirements, the following endpoint addresses must be accessible to use the Analytics service.
### Citrix Analytics

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>US region</th>
<th>EU region</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin UI</td>
<td><a href="https://analytics.cloud.com">https://analytics.cloud.com</a></td>
<td><a href="https://analytics-eu-cloud.com">https://analytics-eu-cloud.com</a></td>
</tr>
<tr>
<td>Admin UI (Demo site)</td>
<td><a href="https://analytics-demo.cloud.com">https://analytics-demo.cloud.com</a></td>
<td>Not Available</td>
</tr>
<tr>
<td>API gateway</td>
<td><a href="https://apigw.analytics.cloud.com">https://apigw.analytics.cloud.com</a></td>
<td><a href="https://api.analytics-eu-cloud.com">https://api.analytics-eu-cloud.com</a></td>
</tr>
<tr>
<td>API micro services</td>
<td><a href="https://api.analytics.cloud.com">https://api.analytics.cloud.com</a></td>
<td><a href="https://api.analytics-eu-cloud.com">https://api.analytics-eu-cloud.com</a></td>
</tr>
<tr>
<td>Event Hub</td>
<td><a href="https://citrixanalyticseh.servicebus.windows.net">https://citrixanalyticseh.servicebus.windows.net</a></td>
<td><a href="https://citrixanalyticseheu.servicebus.windows.net">https://citrixanalyticseheu.servicebus.windows.net</a></td>
</tr>
</tbody>
</table>

**Note**

Citrix Analytics has discontinued the support for TLS 1.0 and TLS 1.1 for most of the above endpoints.

- **Citrix Cloud Connector installation**: Some data sources such as Citrix Endpoint Management, Citrix Virtual Apps and Desktops, and Microsoft Active Directory require you to install a Citrix Cloud Connector on your resource location. The Citrix Cloud Connector is a communication channel between Citrix Cloud and your resource locations. After installing the Citrix Cloud Connector, you must configure the web proxy settings. For more information, see [Cloud Connector Proxy and Firewall Configuration](#).

- **Citrix Analytics endpoint for Splunk**: To integrate Analytics with your Splunk environment, you must configure the **Citrix Analytics add-on for Splunk**. This add-on connects to the following endpoints on Citrix Analytics:

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>US region</th>
<th>EU region</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kafka brokers</td>
<td>casnbkafka-broker-0.eastus2.cloudapp.azure.com:9094</td>
<td>casnbkafka-broker-0.westeurope.cloudapp.azure.com:9094</td>
</tr>
<tr>
<td></td>
<td>casnbkafka-broker-1.eastus2.cloudapp.azure.com:9094</td>
<td>casnbkafka-broker-1.westeurope.cloudapp.azure.com:9094</td>
</tr>
</tbody>
</table>
Identity and access management

- To access Analytics, you must use your Citrix Cloud account. By default, Citrix Cloud uses the Citrix Identity provider to manage the identity information for all users in your Citrix Cloud account. You can also use other identity providers as mentioned in Identity and access management.
- Citrix Analytics supports delegated administrator permissions. You can assign a read-only admin permission to a user to manage Analytics in your enterprise. For more information, see Delegated administrators.

Data residency

Citrix Cloud manages the control plane for Citrix Analytics. Data received from the data sources are stored in multiple Microsoft Azure environments. These environments are located in the United States and the European Union regions. The storage location depends on the home region selected by the Citrix Cloud administrators when onboarding their organizations to Citrix Cloud. For more information, see the following topics:

- Geographical considerations
- Data governance

Data protection

Citrix Analytics receives data from the subscribed Citrix Cloud data sources, on-premises data sources, and the third-party products. Analytics does not process the received data unless the customer has a Citrix Cloud entitlement and the Analytics administrator has explicitly enabled data processing for each of the subscribed data sources.

Citrix Analytics protects the customers' data using the following security measures:

- Citrix Cloud authentication for the Analytics users. For information, see Identity and access management.
- Tenant-based data access controls enforced by the Data Service and Data Access Layer.
- Strong data isolation per customer or tenant in all data stores in the data lake and data warehouse.
- TLS-encrypted data transfer between the various microservices and data stores, applicable for the public endpoints (APTs/inputs/outputs) of the platform and within the platform.
- High standards in TLS endpoints. TLS 1.0 and TLS 1.1 are disabled.
- Encrypted data storage using encryption keys and secrets that are stored in appropriate key vaults.
Citrix Analytics

- Strong user management access controls for service operations and support while protecting customer logs.
- Vulnerability scanning, intrusion detection, anti-malware, rootkit scanning used along with Azure Security Center.

As with all Citrix Cloud services, data collection is strictly subject to the End User Service Agreement (EUSA). For more information, see the following agreements:

- User Agreements
- Citrix Privacy Policy
- Citrix Data Processing Agreement
- Citrix Services Security Exhibit
- Citrix Cloud Services: Customer Content and Log Handling
- Citrix Privacy and Compliance Information

Security responsibility

Citrix responsibility

Citrix is responsible for securing all infrastructure and data residing on the Citrix-managed cloud environments that host Citrix Analytics. Citrix is responsible for applying regular software updates and patches on cloud environment to address security vulnerabilities.

Customer responsibility

Citrix customers are responsible for securing their data sources, policy enforcement points, and Security Information and Event Management (SIEM) systems that are integrated with Citrix Analytics, which include:

- On-premises data sources: Citrix Gateway, Citrix Virtual Apps and Desktops, Microsoft Active Directory
- SIEM: Splunk and any other third party products that use the Kafka brokers to read events from Citrix Analytics.
- Customer-provided administrator credentials for managing Citrix Cloud services, including Citrix Analytics.
- Customer-owned administrator accounts that receive emails or notifications from Citrix Cloud services.
Citrix Analytics

- Customer-provided administrator credentials for deploying and integrating the agents such as Citrix ADM agents, Analytics policy agent. Access to these agents must be restricted because they store the keys locally to communicate with Citrix Analytics.
- Citrix Analytics-generated credentials for configuring **Citrix Analytics Add-on for Splunk**.
- End user devices running on Windows, Mac, Android, iOS to connect to Citrix Cloud or Citrix Workspace and integrated with data sources.

For more information on security provisions, see the following documents:

- Secure Deployment Guide for Citrix Cloud Platform
- Citrix Workspace platform
- Technical security overview for Citrix Virtual Apps and Desktops service
- Security considerations for on-premises Citrix Virtual Apps and Desktops
- Secure your StoreFront deployment
- Technical security overview for Citrix Endpoint Management
- Technical security overview for Citrix Content Collaboration
- Access Control service documentation
- Secure deployment guide for Citrix ADC
- Citrix ADM system requirements

**System Requirements**

February 3, 2020

Before you begin using Citrix Analytics, you must review the software requirements, browser requirements, port information, license information, and limitations.

**Supported browsers**

To access Citrix 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
- Microsoft Internet Explorer 11
- Latest version of Apple Safari
Citrix Virtual Apps and Desktops requirements

For Virtual Apps and Desktops service:

- Subscription to the Citrix Virtual Apps and Desktops service. Note that Virtual Apps and Desktops Essentials is not supported on Citrix Analytics.
- Receiver for Windows version 4.11 or later
- Citrix Workspace app for Windows 1808 or later
- Receiver for Mac version 12.9.1 or later (for Secure SaaS apps)
- Citrix Workspace app for Mac 1910 or later
- Citrix Workspace app for HTML5 1809 or later
- Citrix Workspace app for Chrome 1809 or later
- Citrix Workspace app for Android 1809 or later

  Note: Citrix Workspace app for Android does not support the App.Start and the App.End events. Hence, Unusual App Usage indicator is not supported.

For Virtual Apps and Desktops on-premises deployment:

- Delivery Controller version 7.16 or later
- Director version 7.16 or later
- Receiver for Windows version 4.11 or later
- Citrix Workspace app for Windows 1808 or later
- Receiver for Mac version 12.9.1 or later (for Secure SaaS apps)
- Citrix Workspace app for Mac 1910 or later
- Citrix Workspace app for HTML5 1809 or later
- Citrix Workspace app for Chrome 1809 or later
- Citrix Workspace app for Android 1809 or later

  Note: Citrix Workspace app for Android does not support the App.Start and the App.End events. Hence, Unusual App Usage indicator is not supported.

- Subscription to Citrix Workspace
- Sites added to Workspace

Learn more: Citrix Virtual Apps and Desktops data source.

For connecting to StoreFront deployment:
• The StoreFront deployment must be StoreFront 1906 or later.

• The StoreFront deployment must be able to connect to the following address:
  – https://*.cloud.com
  – https://*.citrixdata.com
  – https://api.analytics.cloud.com

• The StoreFront deployment must have port 443 open for outbound internet connections. Any proxy servers on the network must allow this communication with Citrix Analytics.

• The StoreFront deployment must be accessed using one of the following clients:
  – Citrix Receiver for Websites in HTML5-compatible browsers.
  – Citrix Workspace app 1903 for Windows or later.
  – Citrix Workspace app 1901 for Linux or later.

**LTSR support:**

• For Citrix Virtual Apps and Desktops 7 1912 LTSR, the supported StoreFront version is 1912.

**Citrix ADC requirements**

You must install and configure a Citrix Application Delivery Management (Citrix ADM) agent in your network environment to enable communication between Citrix Analytics and the managed ADC instances in your data center. To configure an agent, you must subscribe to Citrix Application Delivery Management, which is available as a service in the Citrix Cloud. For more information on the Citrix ADM agent, see [Getting started](#).

This section describes the various system components and ports required.

**Application Delivery Management agent installation requirements**

In your data center, you can install an agent on Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V, and Linux KVM Server. The following table lists the virtual computing resources that the hypervisor must provide for the agent.

The following table lists the virtual computing resources that the hypervisor must provide for the agent.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8 GB (32 GB recommended for better performance.)</td>
</tr>
</tbody>
</table>
### Component Requirement

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual CPU</td>
<td>4 (8 virtual CPUs recommended for better performance)</td>
</tr>
<tr>
<td>Storage space</td>
<td>120 GB</td>
</tr>
<tr>
<td>Virtual network interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

### Port requirements

Ensure the following ports are open for the Citrix Application Delivery Management agent to communicate with Citrix Gateway instances.

<table>
<thead>
<tr>
<th>Type</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>80/443</td>
<td>For NITRO communication from agent to Citrix Gateway instances</td>
</tr>
<tr>
<td>TCP</td>
<td>22</td>
<td>For SSH communication from agent to Citrix Gateway instance.</td>
</tr>
<tr>
<td>UDP</td>
<td>4739</td>
<td>For AppFlow communication from Citrix Gateway to agent.</td>
</tr>
<tr>
<td>ICMP</td>
<td>No reserved port</td>
<td>To detect network reachability from agent to Citrix Gateway instances.</td>
</tr>
<tr>
<td>SNMP</td>
<td>161,162</td>
<td>To receive SNMP events from Citrix Gateway instance to agent.</td>
</tr>
<tr>
<td>Syslog</td>
<td>514</td>
<td>To receive syslog messages in agent from Citrix Gateway instance.</td>
</tr>
<tr>
<td>TCP</td>
<td>5557</td>
<td>for log stream communication from Citrix Gateway instances to agent.</td>
</tr>
</tbody>
</table>
For communication between the Citrix Application Delivery Management agent and Citrix Analytics, ensure the following port is open:

<table>
<thead>
<tr>
<th>Type</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>443</td>
<td>For NITRO communication from the agent to the Citrix Application Delivery Management service.</td>
</tr>
</tbody>
</table>

**Getting started**

April 15, 2020

This document describes how to get started with Citrix Analytics for the first time.

**Step 1: Sign in to Citrix Cloud**

To use Citrix Analytics, 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 Analytics**

You can access Analytics in one of the following ways:
• **Request a Citrix Analytics offering trial.** After signing in to Citrix Cloud, in the Available Services section, on the Analytics tile, click Manage to view the Analytics overview page.

The overview page displays the Analytics offerings - Security, Operations, and Performance.

- For Security Analytics and Performance Analytics, click Request Trial to use the trial version of the offering. You receive an email when your request is approved and trial becomes available. You can use the trial for a maximum 60 days period. For more information on service trials, see Citrix Cloud Service Trials.

- Operations Analytics is available free of charge with the following subscriptions and therefore you do not need to request for a trial:
  * Citrix Workspace Standard
  * Citrix Workspace Premium
  * Citrix Workspace Premium Plus
  * Citrix Virtual Apps and Desktops stand-alone service
  * Citrix Content Collaboration stand-alone service

If you have one of these subscriptions, you can access this Analytics offering and view the basic operational reports of the Citrix services associated to your Citrix Cloud account.

On the Citrix Cloud page, the Analytics tile moves to the My Services section.

• **Subscribe to Citrix Analytics.** You can purchase the following Citrix Analytics subscriptions:

  - Citrix Analytics for Security
  - Citrix Analytics for Performance
  - Citrix Analytics for Security and Performance

Citrix Analytics for Security and Citrix Analytics for Performance are 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.

**Note**

You can view the Analytics demo anytime if you have a Citrix Cloud account. Click Manage on the Analytics tile in Citrix Cloud to go to the Analytics overview page. On the overview page, click the Try Demo link specific to each Analytics offering, or register for a demo on https://www.citrix.com/products/citrix-analytics.html.

**Step 3: Manage Analytics**

For Security Analytics and Performance Analytics, after you have the necessary subscriptions or are authorized to access the trial, on the Analytics overview page, the Request Trial button for the offering
changes to **Manage**. Click **Manage** to view the user dashboard corresponding to each offering.

For Operations Analytics, click **Manage** to view the operations dashboard for the Citrix services that you have subscribed to.

Analytics automatically discovers the Citrix Cloud services (data sources) associated to your Citrix Cloud account. To view your discovered data sources, click **Settings > Data Sources**.

For more information on each Analytics offering, see

- **Citrix Analytics for Security**
- **Citrix Analytics for Operations**
- **Citrix Analytics for Performance**

**Find your way around**

February 3, 2020

Familiarize yourself with the main controls on the Analytics UI.
Citrix Analytics

**Top bar**

Navigate to the various Analytics offerings from the top bar.

![Top bar diagram]

**Settings menu**

From the **Settings** menu, navigate to the **Indicators and Policies** page or the **Data Sources** page.

![Settings menu diagram]
Help menu

View the Welcome page
View Analytics documentation

Alerts

View list of alerts generated on Citrix Analytics to notify you of security events that require attention.
User Security Alerts

Risk Score Change

76
Score jumped 76 pts over the last 12 hours
2018-05-08 10:00:00

Risk Indicator

N/A
EPA Scan Failure
2018-05-08 10:00:00

Risk Score Change

91
Score jumped 91 pts over the last 12 hours
2018-05-08 10:00:00

Risk Score Change

86
Score jumped 86 pts over the last 12 hours
2018-05-08 10:00:00

Risk Score Change

74
Score jumped 74 pts over the last 12 hours

See More
Discover more data sources

Discover newly added data sources or previously deleted data sources.

Audit log

Navigate to the Audit Log page that lists all events generated on Analytics.

Self-service search

February 3, 2020
What is self-service search?

The self-service search feature enables you to find and filter user events received from your data sources. You can explore the underlying user events and its attributes. These events help you to identify any data issues and troubleshoot them. The search page displays various facets (dimensions) and metrics for a data source. You can define your search query and apply filters to view the events that match your defined criteria. By default, the self-service search page displays user events for the last one month.

Currently, the self-service search feature is available for the following data sources:

- Access Control
- Authentication
- Content Collaboration
- Gateway
- Secure Browser
- Virtual Apps and Desktops
- Performance Users and Sessions

Also, you can perform self-service search on the events that met your defined policies. For more information, see Self-service search for Policies.

How to access self-service search

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

- **Top bar**: Click Search from the top bar to view all user events for the selected data source.
- **Risk timeline on a user profile page**: Click Event Search to view the events for the respective user.

Self-service search from the top bar

Use this option to go to the self-service search page from any place in the user interface.

1. Click Search to view the self-service page.
2. Select the data source and the time period to view the corresponding events.

Self-service search from user’s risk timeline

Use this option if you want to view the user events associated with a risk indicator.

When you select a risk indicator from a user’s timeline, the risk indicator information section is displayed on the right pane. Click **Event Search** to explore the events associated to the user and the data source (for which the risk indicator is triggered) on the self-service search page.

For more information on the user risk timeline, see **Risk timeline**.

How to use self-service search

Use the following features on the self-service search page:

- Facets to filter your events.
- Search box to enter your query and filter events.
- Time selector to select the time period.
• Timeline details to view the event graphs.
• Event data to view the events.
• Export to CSV format to download your search events as a CSV file.

Use facets to filter events

Facets are the summary of data points that constitute an event. Facets vary depending on the data source. For example, the facets for the Access Control data source include reputation, actions, location, category group. Whereas facets for Virtual Apps and Desktops include event type, domain, platform.

Use the facets to filter and focus on the required user events. For more information on the facets corresponding to each data source, see the self-service search article for the data source mentioned earlier in this article.

Use search query in the search box to filter events

When you place your cursor in the search box, the search box displays a list of dimensions based on the events received from the data source. Use the dimensions to define your search criteria and search for the events.

For example, in self-service search for access, you get the following dimensions for the access events. Enter your query by using these dimensions, select the time period, and then click **Search**.
You can also use the following operators in your search queries.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>:</td>
<td>Assign a value to the search query</td>
<td>User-Name : John</td>
<td>Displays events for the user John</td>
</tr>
<tr>
<td>=</td>
<td>Assign a value to the search query</td>
<td>User-Name = John</td>
<td>Displays events for the user John</td>
</tr>
<tr>
<td>~</td>
<td>Search similar values</td>
<td>User-Name ~ test</td>
<td>Displays events having similar user names</td>
</tr>
<tr>
<td>&quot;&quot;&quot;</td>
<td>Enclose values separated by spaces</td>
<td>User-Name = “John Smith”</td>
<td>Displays events for the user John Smith</td>
</tr>
<tr>
<td>&lt;, &gt;</td>
<td>Search for relational value</td>
<td>Data Volume &gt; 100</td>
<td>Displays events where data volume is greater than 100 GB</td>
</tr>
<tr>
<td>AND</td>
<td>Search values where both conditions are true</td>
<td>User-Name : John AND Data Volume &gt; 100</td>
<td>Displays events of user John where data volume is greater than 100 GB</td>
</tr>
<tr>
<td>*</td>
<td>Search values that match the character zero or more times</td>
<td>User-Name = John*</td>
<td>Displays events for all user names that begin with John</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User-Name = <em>John</em></td>
<td>Displays events for all user names that contain John</td>
</tr>
</tbody>
</table>
For more information on how to specify your search query for the data source, see the self-service search article for the data source mentioned earlier in this article.

**Select time to view event**

Select a preset time or enter a custom time range and click **Search** to view the events.

**View the timeline details**

The timeline provides a graphical representation of user events for the selected time period. Move the selector bars to choose the time range and view the events corresponding to the selected time range.

The figure shows timeline details for access data.

For example, you want to view the events that have occurred between July 08, 2019 to July 10, 2019. Use the selector bars to select the required timeline area and view the events corresponding to the selected area.
View the event

You can view the detailed information about the user event. Click a user to get insight into their data.

The figure shows the details about the user’s access data.

Add columns in the event table

You can add columns and select the data points that you want to display in the event table. Do the following:

1. Click + to add columns for the data points.
2. In the Add Columns window, select the data points and then click Add Columns.

If you deselect a data point from the Add Columns list, the corresponding column is removed from the event table. However, you can view the data point after expanding the event row for a user. For example, if you deselect the TIME data point from the Add Columns list, the TIME column is removed from the event table. To view the time record, expand the event row for a user.
Export the events to a CSV file

You can export the searched events to a CSV file and save the report for future reference. Click Export to CSV format to export the events and download the CSV file that is generated.

Citrix Analytics for Security (Security Analytics)

February 3, 2020

With the advantage of work from anywhere, anytime, any device on any network, sensitive corporate data is exposed more than when users only worked from an isolated corporate office. Malicious users have a large attack surface to target. IT teams are charged with delivering a great user experience without compromising security. Citrix Analytics for Security can help bridge that gap with a focus on user security.
What is Security Analytics?

Citrix Analytics for Security continuously assesses the behavior of Citrix Virtual Apps and Desktops users and Citrix Workspace users and applies actions to protect sensitive corporate information. The aggregation and correlation of data across networks, virtualized applications and desktops, and content collaboration tools enables the generation of valuable insights and more focused actions to address user security threats. Also, machine learning supports highly predictive approaches to identifying malicious user behavior.

Features

- Streamlined insights from across Citrix products and partner integrations. Learn more.
- Easy-to-consume dashboards provide a complete view of user behavior. Learn more.
- Detect and mitigate malicious user behavior using machine learning and customized policies with automated actions. Learn more.
- Continuous monitoring of user behavior after initial authentication to corporate networks balances thorough security and great user experience. Learn more.

Dashboards

You can view details about user or entity behavior on the following security dashboards:

- **Users**: Provides visibility into user-behavior patterns across an organization.
- **User access**: Summarizes the number of risky domains accessed and the volume of data uploaded and downloaded by the users in your network.
- **App Access**: Summarizes the details of the domains, URLs, and apps accessed by users in your network.
Citrix Analytics

- **Share Links**: Summarizes the details of the share links’ patterns across an organization.
- **Reports**: This page allows you to create custom reports based on the dimensions and metrics available from the on-boarded data sources.

**Citrix Analytics for Operations (Operations Analytics)**

April 20, 2020

**What is Operations Analytics?**

To improve and optimize the operations of your existing Citrix infrastructure, you need to have an insight into what is happening in your Citrix environment. Citrix infrastructure includes the Citrix products running on cloud and on-premises to meet the needs of your mobile workforce, consistent application delivery, and securing your digital workspace. These services and products generate huge amount of user and application data, which can be analyzed to gain transparency into the operations and usage of the Citrix infrastructure. Citrix Analytics uses machine learning to analyze the incoming data from the data sources (Citrix products) and provides actionable insights into the operational data.

For example, if your enterprise is using the Citrix Access Control service, you can use the Operations dashboards to get insight into your user operations and application operations data. You have a comprehensive view of the usage data based on data downloads, data upload, domains accessed, and other available metrics according to the data sources.

**Why Operations Analytics?**

- The insight plays a pivotal role in capacity planning. Your Citrix infrastructure can consists of multiple products with different sets of workloads. Transparency into the consumption metrics for each product helps you to predict the infrastructure load and quickly respond to any operational issues.
- As an administrator, you can make better informed decisions in optimizing the resources and reducing the overall IT cost.

**Dashboards**

You can view the operational data in the following dashboards:
• **User Operations.** Provides an overview of the user operations data based on transactions and data usage volume.

• **App Operations.** Provides an overview of app operations data based on domains, categories, and download volume.

---

**Citrix Analytics for Performance (Performance Analytics)**

April 30, 2020

**What is Performance Analytics?**

Performance Analytics is a Citrix Analytics service (CAS) offering that enables you to track, aggregate, and visualize key performance indicators of your Citrix Virtual Apps and Desktops environment.

Broadly,

• Performance Analytics aggregates Site performance metrics into easy-to-view User Experience and Infrastructure dashboards. They help you analyze the user experience and optimize the usage of your Citrix Virtual Apps and Desktops Sites.

• Performance Analytics supports multi-Site aggregation and reporting. It aggregates performance metrics across your Cloud and on-premises setups. Hence, you can view data for all the Sites in your environment in a single console.
• Performance Analytics quantifies the user performance factors and classifies the users based on these factors. It provides actionable insights to troubleshoot failures, screen lags, delayed session logons, and other performance indicators.

• Performance Analytics allows you to find and filter metrics to narrow down to specific users or sessions facing performance issues.

How to use Performance Analytics

User Experience Dashboard

The User Experience dashboard shows the Site performance concerning factors such as session responsiveness, session logon duration, session failures, and session reconnects that together define the user experience.

If you are supporting several users of virtual apps and desktops in your organization, and they occasionally experience delay while launching apps or desktops, the logon duration metric can give you insights into the issue. Drilling down can help you identify the factors leading to the issues.

Infrastructure Dashboard

The Infrastructure dashboard displays the status and health of the VDAs in your Site. When used together, the User and Infrastructure dashboards can help you proactively check availability of resources and identify performance bottlenecks on the Sites.

• If user or session trends show a dip, indicating a reduction in the number of users or sessions logged into the Site, use this indicator to check if a hypervisor has been rebooted or the number of VDAs is insufficient.

• If you see several cases of session failing to launch, drilldown to establish the cause for the failure. It might be a shortage in the number of licenses or issues with VDA connection to the Delivery Controller.

Using Performance Analytics you can quickly analyze issues, troubleshoot and resolve them, and maintain an optimum level of service of apps and desktops.

For information about the system requirements, refer to the Citrix Analytics System Requirements article.

Citrix Analytics for Performance collects and stores logs for data points as listed in Logs collected for Citrix Analytics for Performance.
How to configure Data Sources

Use Performance Analytics to monitor on-premises or Cloud Sites. You can use this offering whether you are a pure on-premises customer, a Cloud customer, or a hybrid customer with a mix of on-premises and Cloud Sites.

Check the status of the Cloud data sources relevant to Performance Analytics from Citrix Analytics Service > Settings > Data Sources > Performance.

If you are an on-premises customer, you must first onboard your Citrix Virtual Apps and Desktops Sites to Performance Analytics. For network related information to be available on Performance Analytics, you must also onboard your on-premises Citrix Gateway.

Configure on-premises Citrix Virtual Apps and Desktops (CVAD) Sites

First configure your on-premises CVAD Sites with Performance Analytics using your Director console on-premises. The configuration helps Performance Analytics obtain the required metrics from your environment.

The versions of CVAD components supported for configuration with Citrix Analytics for Performance are as follows:

- Delivery Controller version 1909 and later
- Director version 1909 and later
- VDA version 7.15 LTSR and later
- Citrix Workspace app version 1909 and later for Chrome, HTML5, Linux, Mac, Windows, and Windows(Store). (Citrix Workspace app for iOS and Android are not supported).

For more information about the onboarding process, see Configuring on-premises CVAD Sites with Citrix Analytics for Performance.
Configure on-premises Citrix Gateway

For Performance Analytics to obtain network related statistics from your on-premises environment, you must configure your on-premises Citrix Gateway with Citrix Application Delivery Management (ADM) Service in Citrix Cloud. Citrix Gateway versions 12.1.x.x and later are supported.

1. Ensure that you are subscribed to the Citrix ADM Service.
2. Register your on-premises Citrix Gateway with the Citrix ADM Service. Follow the instructions as in the Citrix ADM Getting Started article.
3. Configure HDX insights on Citrix Gateway. Follow the instructions described in the HDXInsight article.
4. Enable Advanced analytics. Follow the instructions as in the Advanced analytics article.

How to access Performance Analytics

Citrix Analytics for Performance is available as a subscription based offering, either as a stand-alone offering or bundled along with Citrix Analytics for Security. To subscribe to Citrix Analytics for Performance, see https://www.citrix.com/products/citrix-analytics-performance.html).

1. Check if your workstation has have a supported web browser listed in the Supported browsers article.
2. You must have a Citrix Cloud account to use the Analytics service. For detailed instructions on how to create a Citrix Cloud account, see Sign Up for Citrix Cloud. Go to https://citrix.cloud.com and sign in with your Citrix Cloud account.
3. Look for the Analytics service tile and click Manage. The overview page displays the offerings available in the Analytics portfolio.
4. In the Performance offering, to use the trial version of the offering, click Request Trial. If you have bought the Citrix Analytics for Performance offering, click the Manage link instead.
5. Citrix Analytics for Performance is opened with dashboards displaying the User Experience and Infrastructure Performance Analytics.

Note:
Known issues specific to the CAS platform are listed in the CAS Known Issues article.

Troubleshoot Citrix Analytics

February 3, 2020

Troubleshooting events transmission issue from a data source

This section helps you to troubleshoot data transmission issues when using Citrix Analytics for Security. When a data source fails to transmit user events accurately, you can encounter issues such as non-discovery of users, absence of alerts, and risk indicators.

Checklist

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Is your organization in a supported geographic region- United States, European Union, or Asia Pacific South?</td>
</tr>
<tr>
<td>2</td>
<td>Do you have the correct entitlements to use Analytics?</td>
</tr>
<tr>
<td>Sequence</td>
<td>Checks</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>3</td>
<td>Does your environment meet all the system requirements?</td>
</tr>
<tr>
<td>4</td>
<td>Are all the data sources discovered and data processing enabled on Analytics?</td>
</tr>
<tr>
<td>5</td>
<td>Are the user activities on the data source transmitting events accurately to Analytics?</td>
</tr>
<tr>
<td>6</td>
<td>Are the virtual apps and desktops events transmitted to Analytics?</td>
</tr>
<tr>
<td>7</td>
<td>Are the user events appearing on the self-service search page in Analytics?</td>
</tr>
<tr>
<td>8</td>
<td>Are the users discovered by Analytics?</td>
</tr>
</tbody>
</table>

**Check 1- Is your organization in a supported geographic region?**

If you do not see user events in Citrix Analytics, your organization might have been onboarded in a home region that is currently not supported. Citrix Analytics does not receive events from the non-supported regions.

To use Citrix Analytics, you must select either **United States** or **European Union** as the home region to onboard your organization. If your organization is located in the Asia Pacific South region, you must select the **United States** region to onboard your organization. For more information, see [Geographical Considerations](#).

**To verify the Citrix Cloud region in which your organization is onboarded:**

On your Citrix Cloud account, select **Account Settings > Company Account**.
### Supported data sources based on their locations

Citrix Analytics supports the following data sources based on their geographic regions. Data sources are the products that send data to Analytics. For more information, see Data sources.

<table>
<thead>
<tr>
<th>Data source</th>
<th>Region</th>
<th>Supported by Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Access Control</td>
<td>US</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EU</td>
<td>No</td>
</tr>
<tr>
<td>Citrix Content Collaboration</td>
<td>US</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EU</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix Endpoint Management</td>
<td>US</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EU</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix Gateway</td>
<td>US</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EU</td>
<td>No</td>
</tr>
<tr>
<td>Citrix Virtual Apps and Desktops service</td>
<td>US</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EU</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix Virtual Apps and Desktops on-premises</td>
<td>US</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EU</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix Secure Browser</td>
<td>US</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Check 2- Do you have correct entitlements to use Analytics?

Citrix Analytics for Security is a subscription-based offering. You can either use a limited trial or buy a subscription to use this offering. For more information, see [Getting started](#).

### Check 3- Does your environment meet all the system requirements?

Citrix Analytics can take a few minutes to receive the user events. If you do not see any user events on the data source site cards, ensure that your environment meets the prerequisites and the system requirements.

#### Prerequisites

1. All your Citrix Cloud subscriptions must be active. On the Citrix Cloud page, make sure that all the Citrix Cloud services are active.

2. If you are using on-premises Citrix Virtual Apps and Desktops, you must add your Sites to Citrix Workspace and configure Site aggregation. Citrix Analytics automatically discovers the Sites added to Citrix Workspace. For more information, see [Aggregate on-premises virtual apps and desktops in workspaces](#).

3. If you are using a StoreFront deployment for your Sites, configure your StoreFront servers to enable Citrix Workspace app to send user events to Citrix Analytics. Ensure that the StoreFront version is 1906 or later. Failure to configure the StoreFront server results in Citrix Virtual Apps and Desktops not sending data to Analytics. To configure StoreFront deployment, see the [Citrix Analytics service](#) article in the StoreFront documentation.
4. Install and configure a Citrix Application Management agent in your network environment to enable communication between Citrix Analytics and managed Application Delivery Controller (ADC) instances. For more information, see Citrix ADC requirements.

5. Onboard your data sources as mentioned in the following articles:
   - Citrix Access Control data source
   - Citrix Content Collaboration data source
   - Citrix Endpoint Management data source
   - Citrix Gateway data source
   - Citrix Virtual Apps and Desktops data source
   - Enable Analytics on Microsoft Graph Security
   - Integrate Analytics with Microsoft Active Directory

6. The Citrix Virtual Apps and Desktops users must use the specified version of Citrix Workspace apps or Citrix Receiver on their end points. Otherwise, Analytics will not receive the user events from the user end points. The list of supported versions of Citrix Workspace app or Citrix Receiver is available in the System Requirements article.

Check 4- Are all data sources discovered and data processing enabled on Analytics?

Ensure that all data sources are discovered and you have enabled data processing for all of them. If you do not enable data processing for a specific data source, the users using the data source are not discovered. This might create a potential security risk.

Enabling data processing ensures that Citrix Analytics is processing your user events. Events are sent to Citrix Analytics only when the users are actively using the data source.

Note

Citrix Analytics does not actively pull data from your environment.

To discover your data sources and enable analytics, do the following:

1. Click Settings > Data Sources to view your discovered data sources. Citrix Analytics automatically discovers the data sources that you have subscribed on your Citrix Cloud account.

2. On the Data Sources page, the discovered data sources appear as site cards. By default, the data processing is off.
3. Click **Turn On Data Processing** on the site card for which you want Citrix Analytics to process events. For example, on the Access Control site card, click **Turn On Data Processing**.

4. After you have turned on data processing, Citrix Analytics processes the events for the data source. The status of the site card changes to Data processing on. You can view the number of users and the received events based on the selected time period.
5. For all discovered data sources, follow the specified steps to enable analytics. For more information, see Enable Analytics on Citrix data sources.

**Check 5- Are the user activities on the data source transmitting events accurately to Analytics?**

Citrix Analytics receives user events from the data sources when the users are actively using the data sources. The users must perform some activities on the data source to generate events. For example, to receive events from the Content Collaboration data source, the Content Collaboration users must share, upload, or download some files.

**Note**

Citrix Analytics does not actively pull data from your environment.

If you do not see any user events in Citrix Analytics for your data source, there is a high probability that the users are not active at that moment.

To verify that Citrix Analytics accurately receives the user events, perform the following activity. This activity uses the Citrix Content Collaboration data source. You can perform a similar activity using other Citrix products (data sources) based on your subscription.

1. Log on to the Citrix Content Collaboration service.
2. Perform some usual user activities such as create folder, download files, uploads files, or delete files.
3. For example, create a Test folder.

4. Upload some local files.
5. Delete some files in the folder.

6. Go back to Citrix Analytics and view the **Content Collaboration** side card on the Data Source page. Citrix Analytics receives the user events from the Content Collaboration data source and displays on the site card.
Check 6: Are the virtual apps and desktops events transmitted to Analytics?

Some versions of Citrix Workspace app or Citrix Receiver client fail to send user events to Citrix Analytics. When users launch virtual apps and desktops through these clients, Citrix Analytics fails to discover the users until they perform the supported events.

For example, the Citrix Workspace app for Mac prior to 1910 does not send the Account Logon event to Citrix Analytics. A user who logs on using such version of Citrix Workspace app for Mac is not discovered on Citrix Analytics. However, if the user later launches a SaaS app, the user is discovered as Citrix Workspace app for Mac prior to 1910 sends the SaaS App Launch event to Citrix Analytics.

**Supported events**

Refer to the following table to check the user events supported by each client version.

- **Yes** - The event is sent by the client to Citrix Analytics.
- **No** - The event is not sent by the client to Citrix Analytics.
- **NA** - The event is not applicable for the client.
| Account Logon | Yes | No | Yes | Yes | Yes | Yes | No | No | Yes | Yes | No |
| Session Logon | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Session Launch | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Session End | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| App Start | Yes | No | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No |
| App End | Yes | No | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No |
| File Download | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes |
| Printing | No | Yes | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes |
| SaaS App Launch | Yes | Yes | Yes | No | No | No | No | No | NA | NA | NA |
| SaaS App End | Yes | Yes | Yes | No | No | No | No | No | NA | NA | NA |
## Recommendation

To get maximum benefits of Analytics, Citrix recommends the following:

- **Windows user**: Connect to your Citrix Virtual Apps and Desktops environment using Citrix Workspace app for Windows 1808 or later.

- **Mac user**: Connect to your Citrix Virtual Apps and Desktops environment using Citrix Workspace app for Mac prior to version 1910 Workspace app for Mac 1910 or later Workspace app for Linux 1901 or later Workspace app for Android 1809 or later Workspace app for iOS 1811 or later Workspace app for Chrome 1809 to 1909 Workspace app for HTML5 1809 to 1909 Receiver for Windows 4.11 Receiver for Windows 4.12 Receiver for Mac 12.9.1

<table>
<thead>
<tr>
<th>SaaS App URL Navigation</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>No</th>
<th>No</th>
<th>No</th>
<th>No</th>
<th>No</th>
<th>NA</th>
<th>NA</th>
<th>NA</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS App Clipboard Access</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>SaaS App File Download</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>SaaS App File Print</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

© 1999-2020 Citrix Systems, Inc. All rights reserved.
app for Mac 1910 or later.

**Check 7 - Are the user events appearing on the self-service search page in Analytics?**

Perform this final check to ensure that the events are being transmitted accurately to Citrix Analytics.

1. On the top bar, click **Search** to go to the self-service search page.

2. Select the data source to view the corresponding search page and the events.

3. To view the data associated to the Content Collaboration events, select **Content Collaboration** from the list, select the time period, and then click **Search**.

For more information, see **Self-service search**.
Check 8- Are the users discovered by Analytics?

When events start flowing to Citrix Analytics, the users generating the events are discovered and shown on the Users dashboard. This usually takes approximately a few minutes before you can view them on the dashboard.

1. Click the Discovered Users link on the Users dashboard to view the complete list of users discovered by Citrix Analytics.

2. The Discovered Users page displays the list of all users discovered over a time period. You can view data for the last 1 hour, 12 hours, 1 day, 1 week, or 1 month.

If events are being transmitted successfully, your Citrix Analytics environment is performing as expected. Risk indicators are generated when anomalies are detected.

Triggering Virtual Apps and Desktops events, SaaS events, and verifying its transmission to Analytics

This section describes the procedures to trigger Virtual Apps and Desktops events, SaaS events, and verify that Citrix Analytics is actively receiving these user events.
Prerequisites

- Onboard your Citrix Virtual Apps and Desktops to Citrix Analytics and then enable data processing. For more information, see Citrix Virtual Apps and Desktops data source.

- Use the correct versions of Citrix Workspace app or Citrix Receiver in the users’ endpoint devices so that the events are accurately sent to Citrix Analytics. For more information, see Citrix Virtual Apps and Desktops requirements.

- Before triggering the printing event from your virtual desktop, ensure that a printer is configured and provisioned in your Citrix Virtual Apps and Desktops environment. For more information on managing a printer, see Print.

- For triggering the SaaS events such as SaaS App Launch, SaaS App URL Navigation, SaaS App File Download, you must use a configured SaaS app from Workspace. Commonly used SaaS apps include Salesforce, Workday, Concur, GoTo Meeting.
  
  - If there are no configured SaaS apps, you must configure and publish a SaaS app. For more information, see Support for Software as a Service apps. When configuring a SaaS app, ensure that the following security options are disabled:
    
    * Restrict clipboard access
    * Restrict printing
    * Restrict navigation
    * Restrict download
  
  - If you want to use an already configured SaaS app from your Workspace to trigger the events, ensure that the specified enhanced security options are disabled for the SaaS app:
    
    1. Go to your Citrix Cloud account and select Library.
2. On the **Library** page, identify the SaaS app that you want to use for verifying the events. For example, Workday.

3. Click the ellipses, and select **Edit**.
4. On the **Edit App** page, click the down arrow for Enhanced security.

5. Ensure that the following security options are not selected.
Known issue

Few versions of Citrix Workspace app and Citrix Receiver do not send specific events to Citrix Analytics. Therefore, Citrix Analytics cannot provide insights and generate risk indicators for these events. For more information about the issue and its workaround, see the known issue- CAS-16151.

Procedure

Perform the following steps in sequence to trigger the events in your Citrix Virtual Apps and Desktops deployment and verify that Citrix Analytics is actively receiving these events.

Note

- The events might take some time to reach Citrix Analytics. Refresh the Citrix Analytics page if you do not see the triggered events.
- For triggering the SaaS events, this procedure uses the Workday app as an example. You can use any configured SaaS apps from your Workspace to trigger the SaaS events.
- Account Logon
1. Launch Citrix Workspace app or Citrix Receiver to access your Workspace or StoreFront.

2. Enter your credentials to log on to the Citrix Workspace app or Citrix Receiver.

3. Go to Citrix Analytics.

4. Click Search and select Apps and Desktops from the list.

5. In the search page, view the data for the Account.Logon event. Expand the row to view the event details.

   - **App Start**
     1. Launch Citrix Workspace app or Citrix Receiver to access your Workspace or StoreFront.
     2. Launch an application such as calculator.
3. Go to Citrix Analytics.

4. Click **Search** and select **Apps and Desktops**.

5. In the search page, view the data for the **App.Start** event data. Expand the row to view the event details.

   ![App Start Event Data](image1)

### App End

1. Close the calculator that you have already launched in your Workspace or StoreFront.

2. Go to Citrix Analytics.

3. Click **Search** and select **Apps and Desktops**.

4. In the search page, view the data for the **App.End** event data. Expand the row to view the event details.

   ![App End Event Data](image2)

### Session Logon and Session Launch

1. Launch Citrix Workspace app or Citrix Receiver to access your Workspace or StoreFront.

2. Launch your virtual desktop.

3. Go to Citrix Analytics.

4. Click **Search** and select **Apps and Desktops**.

5. In the search page, view the data for the **Session.Logon** and **Session.Launch** events. Expand the row to view the event details.

   ![Session Logon and Launch Event Data](image3)
• **File Download**

1. Launch Citrix Workspace app or Citrix Receiver to access your Workspace or StoreFront.
2. Launch your virtual desktop.
3. Copy a file from your virtual desktop to your local computer.
4. Go to Citrix Analytics.
5. Click **Search** and select **Apps and Desktops**.
6. In the search page, view the data for the **File.Download** event. Expand the row to view the event details.

• **Printing**

1. Launch Citrix Workspace app or Citrix Receiver to access Workspace.
2. Launch your virtual desktop.
3. Print a document using a printer that is configured with your virtual desktop.
4. Go to Citrix Analytics.
5. Click **Search** and select **Apps and Desktops**.
6. In the Search page, view the data for the **Printing** event. Expand the row to view the event details.
• **Session End**

  1. Sign out from your virtual desktop. For example, if you are using a Windows virtual desktop, select the **Sign out** option.

  ![Sign out](image)

  2. Go to Citrix Analytics.

  3. Click **Search** and select **Apps and Desktops**.

  4. In the search page, view the data for the **Session.End** event. Expand the row to view the event details.

• **SaaS App Launch and SaaS App URL Navigation**

  1. Launch Citrix Workspace app or Citrix Receiver to access your Workspace or StoreFront.
2. Launch a SaaS application such as Workday and wait until the Workday page has loaded. Navigate around the webpages in Workday.

   Note
   Ensure that the `Restrict navigate` option is disabled in the Enhanced security section. For more information, see Prerequisites.

3. Go to Citrix Analytics.

4. Click **Search** and select **Apps and Desktops**.

5. In the search page, view the data for the **App.SaaS.Launch** and **App.SaaS.URL.Navigation** events. Expand the row to view the event details.

   ![Citrix Analytics screenshot](image)

   • **SaaS App File Print**

     1. Print the Workday page that you are currently viewing.

        Note
        Ensure that the `Restrict printing` option is disabled in the Enhanced security section. For more information, see the Prerequisites.

2. Go to Citrix Analytics.

3. Click **Search** and select **Apps and Desktops**.

4. In the search page, view the data for the **App.SaaS.File.Print** event. Expand the row to view the event details.
• SaaS App Clipboard Access

1. From the Workday page, copy some text to your system clipboard.

   **Note**
   
   Ensure that the **Restrict clipboard access** option is disabled in the Enhanced security section. For more information, see the **Prerequisites**.

2. Go to Citrix Analytics.

3. Click **Search** and select **Apps and Desktops**.

4. In the search page, view the data for the **App.SaaS.Clipboard** event. Expand the row to view the event details.

   ![SaaS App Clipboard Access Table](image)

• SaaS App File Download
1. On the Workday page, search for a public document such as whitepaper and download the document.

**Note**

Ensure that the **Restrict downloads** option is disabled in the Enhanced security section. For more information, see the **Prerequisites**.

2. Go to Citrix Analytics.

3. Click Search and select **Apps and Desktops**.

4. In the Search page, view the data for the **App.SaaS.File.Download** event. Expand the row to view the event details.

- **SaaS App End**

  1. Close the Workday page.

  2. Go to Citrix Analytics.

  3. Click **Search** and select **Apps and Desktops**.

  4. In the search page, view the data for the **App.SaaS.End** event. Expand the row to view the event details.
Citrix Analytics

Contact support

Citrix is committed to helping you be successful with our solutions. To ensure that your support request is routed to the correct resources, choose the options mentioned on our Contact Support page.

FAQs

February 3, 2020

This document provides frequently asked questions on Citrix Analytics.

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 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

Should I 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 Agents 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 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.
Citrix Analytics

- 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 onto the agent’s shell prompt and run the following command: `cat /mpsconfig/telemetry_cloud.conf` and verify the value of the `turnOnEvent` parameter.

```
bash-3.2$ cat /mpsconfig/telemetry_cloud.conf
{
"storage_account": "casstoragebulkstaging",
"blobname": "ns-mas-nwfaq2pzcenaspv2018smrhlmmmyrf7n",
"blobtoken": "se-2019-03-29T06:03:21Z__2019-12-11T23_defaultar-cisig-eAyPO4516F8PvS26eV00E4YqOMHvu7JVS69NNBtCye",
"eventhub_name": "SharedAccessSignature =https://ehstaging.servicebus.windows.net/ehgeneral/publishers/citrix691796.ns.mas.70380659-3fc3-462-eb5b-ccb5d62f5475/messages?api-version=2014-01&sig=WJUQopqquXeE1MNx-xla98SbxexYgP08SktgIqguerw=6=1522303402&skn=dirsve_send",
"expiration": 0,
"turnOnEvent": "Y",
"tenant": "citrix691796",
"agent_id": "aBB2B943-3B18-46C9-8C7E-70e206f5b3a0"
}
bash-3.2$
```

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

Can I add more agents on Delivery Controllers for Citrix Analytics?

Yes! Adding more agents ensures high availability for your Site, enabling Citrix Analytics to keep analyzing user behavior in the event one of your Delivery Controllers becomes unavailable.

To add more agents:

1. Click the Site card and then click **View Site details**. Citrix Analytics displays a list of the available Delivery Controllers in your Site.
2. Click **Install agent** for the Delivery Controllers you want to add. When the installation finishes, the Agent State changes to “online.”

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/](https://discussions.citrix.com/forum/1710-citrix-analytics/).

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

Glossary of terms

February 3, 2020

- **Access control**: 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](#).
- **Actions**: Closed loop responses to suspicious events. Actions are executed 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 datacenter, 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 provide, 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](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](#).

• **Operations Analytics**: Service that collates and presents information on user activities, such as, websites visited and the bandwidth consumed. [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 executed 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, threat hunting, and so on. [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.]