Citrix Analytics

Contents

What's new

September 21, 2023

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. See 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 Performance

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

September 21, 2023

Simplify StoreFront On-boarding Using PowerShell Script

A new **PowerShell** script has been introduced that automates the process of checking prerequisites, installing, and configuring StoreFront. The customer must run this script in administrator mode on StoreFront to onboard, deboard, perform self-checks, troubleshoot, and verify whether onboarding to the Citrix Analytics Service GUI is successful.

For more information, see Connect to a StoreFront deployment.

August 28, 2023

Microapps service (End of Life)

Citrix Microapps service has reached its end of life and is no longer available to users.

August 01, 2023

Citrix Analytics - Usage (End of Life)

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

February 23, 2023

Fixed issues

Prior to the release of Citrix Virtual Apps and Desktops 2112, Citrix Analytics fails to discover the on-premises sites that are connected from Citrix Director and are recently registered on Citrix Cloud. So, you don't see these connected sites on your **Virtual Apps and Desktops- Monitoring** site card. This issue is fixed now. [CAS-63132]

September 28, 2022

Webhooks for Alert Notifications

You can use webhooks to send Citrix Analytics alert notifications to any third-party applications that have incoming webhook URLs configured. Webhooks are HTTP callbacks that enable real-time messaging between the service provider applications and consumer applications. Since the alert notifications are sent in real time, you get notified when the events occur. For more information, see Webhooks for Alert Notifications.

September 08, 2022

Export limit in CSV export increased

The limit on the number of rows that you can export using the **Export to CSV format** feature is now increased from 10K rows to 100K rows. For more information, see Export the events to a CSV file.

August 18, 2022

Fixed issue

- In the Self-Service search for Apps and Desktops, the Workspace app version value was populated as **NA** (not available) in the downloaded CSV file, while it was available in the page view. This issue is now fixed. [CAS-70361]

August 10, 2022

StoreFront onboarding without site aggregation

The site aggregation dependency for StoreFront has been removed from **Apps and Desktops- Workspace app** site card. You can see the **Connect Storefront Deployment** option on your workspace application, even if you do not have any site added to the site aggregation. For more details, refer Citrix Virtual Apps and Desktops data source.

April 05, 2022

Secure Workspace Access is renamed to Secure Private Access

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

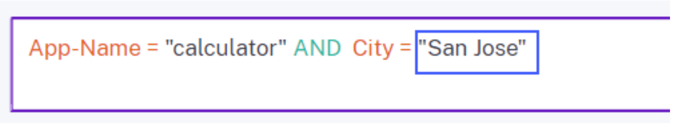
For example, on the **Data Sources** page and the **Self-service search page**, the **Secure Workspace Access** labels are renamed as **Secure Private Access**.

March 21, 2022

Fixed issue

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

  For example, in the following query, auto-suggestions stop working after you select the city as `San Jose`. This issue is now fixed. [CAS-64126]

  App-Name = "calculator" AND City = "San Jose"

February 10, 2022

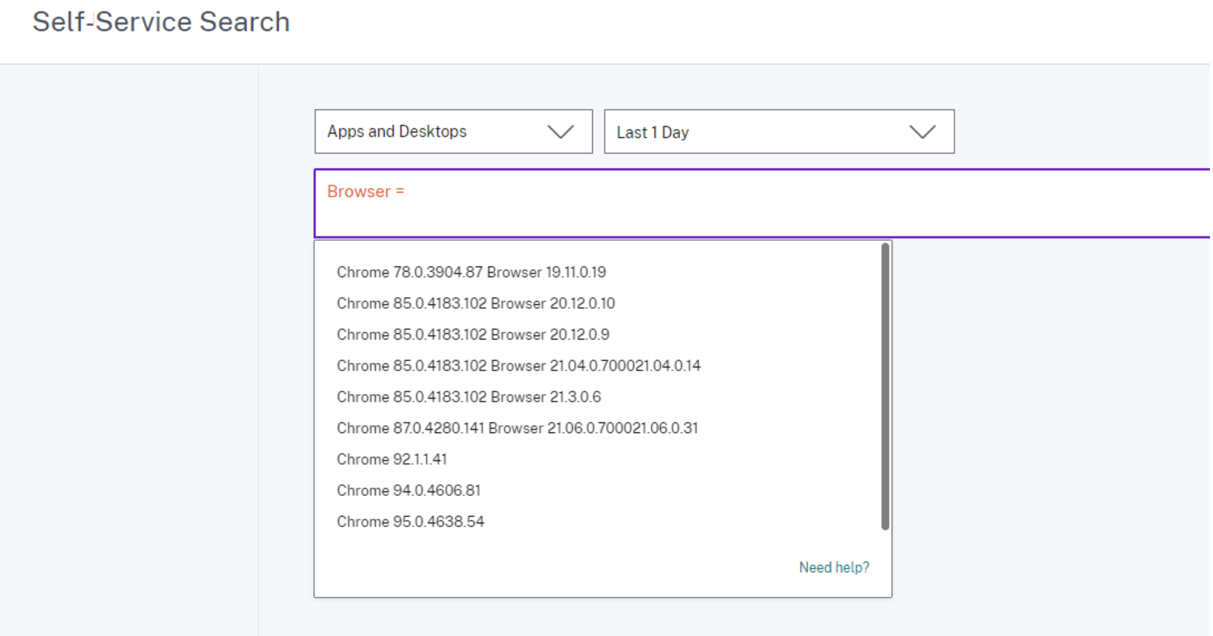
What's new

Auto suggested values for the dimensions in the self-service search box In the self-service search page, when you select a dimension and a valid operator in the search box, the values for the dimension are shown automatically. Select a value from the auto-suggested list or manually enter a value depending on your use cases. When you type a value, the matching values available in the records are auto-suggested.

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

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

For more information, see Self-service search.



Self-Service Search

Apps and Desktops

Last 1 Day

Browser =

Chrome 78.0.3904.87 Browser 19.11.0.19
Chrome 85.0.4183.102 Browser 20.12.0.10
Chrome 85.0.4183.102 Browser 20.12.0.9
Chrome 85.0.4183.102 Browser 21.04.0.700021.04.0.14
Chrome 85.0.4183.102 Browser 21.3.0.6
Chrome 87.0.4280.141 Browser 21.06.0.700021.06.0.31
Chrome 92.1.1.41
Chrome 94.0.4606.81
Chrome 95.0.4638.54

December 20, 2021

What's new

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

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

December 06, 2021

What's new

Citrix Analytics is now supported in the Asia Pacific South region

- You can now choose Asia Pacific South as a home region while onboarding your organization to Citrix Cloud and use the Citrix Analytics service. For more information, see Geographical Considerations.
- Citrix Analytics now stores the user events and metadata of your organization in the Asia Pacific South region when you choose it as your home region. For more information, see Data governance.

- For information about the network requirements for the Asia Pacific South region, see Technical security overview.
- For information about supported data sources in the Asia Pacific South region, see Data sources.

August 19, 2021

What's new

Support for the IS EMPTY operator In the self-service search, you can now use the **IS EMPTY** operator in your condition to check for null or empty dimension.

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

For more information, see Self-service search.

July 14, 2021

What's new

Support for the IS NOT EMPTY operator In the self-service search, you can now use the **IS NOT EMPTY** operator in your query to check if the dimension is not empty (not blank).

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

For more information, see Self-service search.

June 07, 2021

Deprecated feature

Removed Citrix Analytics demo environment The **Try Demo** links for Security Analytics and Performance Analytics are now removed from the Analytics overview page. You can no longer access the demo environment for each offering. For more information on how to get access to Citrix Analytics offerings, see Getting started.

May 18, 2021

What's new

Support for * operator with != operator In your search query, you can now use the * operator with the ! = operator to find the user events. For example:

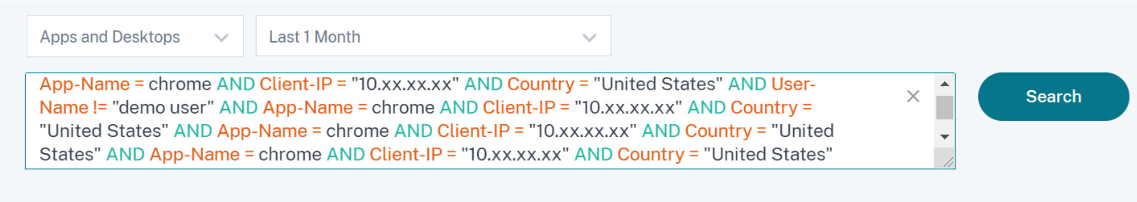
- To find all the user events that do not begin with the name "John", use the query: User-Name != John*
- To find all the user events that do not end with the name "Smith", use the query: User-Name != *Smith

> **Note**
>
> The search results are case-sensitive.

For more information, see Self-service search.

Enhanced search bar experience in the self-service search page

- The search bar now provides a better view of your queries when it extends to multiple lines. Use the scroll bar to scroll your multi-line queries. Previously, it was difficult to view the multi-line queries.



Apps and Desktops

Last 1 Month

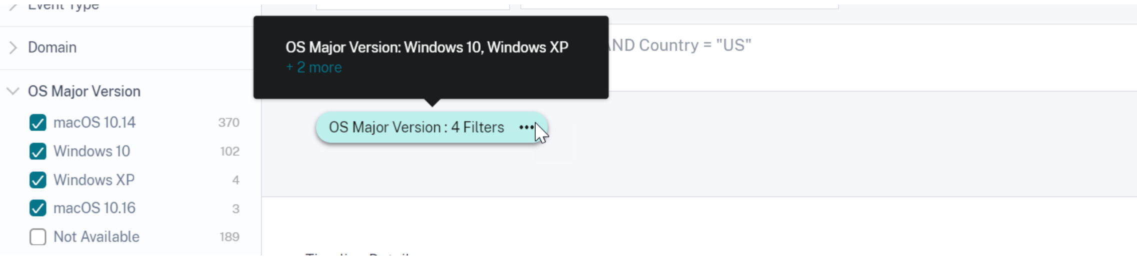
App-Name = chrome AND Client-IP = "10.xx.xx.xx" AND Country = "United States" AND User-Name != "demo user" AND App-Name = chrome AND Client-IP = "10.xx.xx.xx" AND Country = "United States" AND App-Name = chrome AND Client-IP = "10.xx.xx.xx" AND Country = "United States" AND App-Name = chrome AND Client-IP = "10.xx.xx.xx" AND Country = "United States"

- The cursor jumping issue that was observed in the Safari browser is now fixed.

For more information, see Self-service search.

Redesigned chips view in self-service search

- The redesigned chips now provide you a better view of the multiple facets that you have selected.



Domain

OS Major Version

☑ macOS 10.14	370
☑ Windows 10	102
☑ Windows XP	4
☑ macOS 10.16	3
□ Not Available	189

OS Major Version: Windows 10, Windows XP
+ 2 more

ND Country = "US"

OS Major Version : 4 Filters

- Click a chip to select or deselect the facets based on your requirements.

Fixed issue

- On Citrix Director, the **Go to Analytics** link is not working. This issue is observed for a user who has onboarded their organization in the European Union region of Citrix Cloud. [CAS-50224]

March 31, 2021

Support for the IN and NOT IN operators for Apps and Desktops search query

With the Apps and Desktops dimensions- `Device ID`, `Domain`, `Event-Type`, and `User-Name`, you can now use the following operators:

- **IN**: Assign multiple values to a dimension to get the events related to one or more values.
- **NOT IN**: Assign multiple values to a dimension and find the events that do not contain the specified values.

> **Note**
>
> These operators are applicable only for the string values.

For more information about the operators, see Self-service search.

March 18, 2021

What's new

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

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

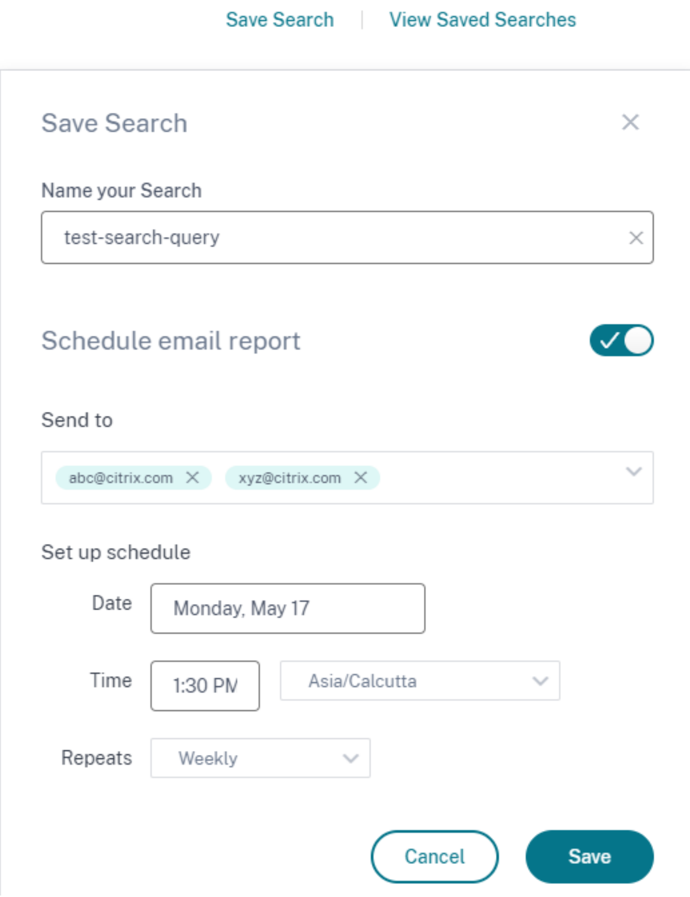
For more information, see Self-service search.

February 23, 2021

What's new

Schedule email delivery for a search query On the self-service search page, while saving a search query, you can also schedule an email delivery to send a copy of the saved search query and the corresponding visual summary report to yourself and other users. Set the date, time, and frequency-daily, weekly, or monthly to start sending an email. You can also schedule email delivery of the search queries that you previously saved.

For more information, see Self-service search.



Save Search

Name your Search: test-search-query

Schedule email report ✓

Send to: abc@citrix.com, xyz@citrix.com

Set up schedule

Date: Monday, May 17

Time: 1:30 PM Asia/Calcutta

Repeats: Weekly

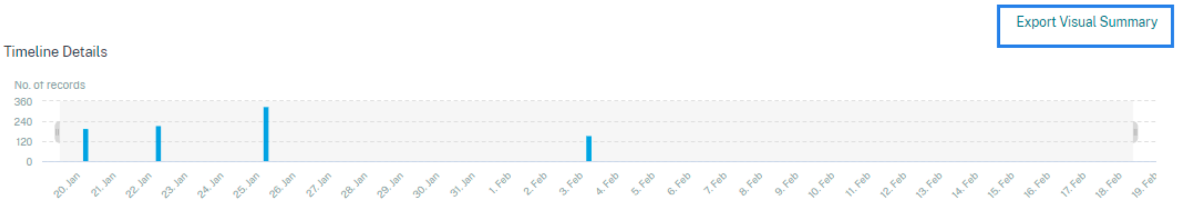
Download visual summary of a search query On the self-service page, you can now download the visual summary report of your search query for a selected time period and share a copy with other users. Click **Export Visual Summary** to download the visual summary report as a PDF.

The report contains the following information:

- The search query that you have specified for the events.
- The facets (filters) that you have applied on the events.

- The visual summary such as the timeline charts, bar charts, or graphs of the search events.

For more information, see Self-service search.

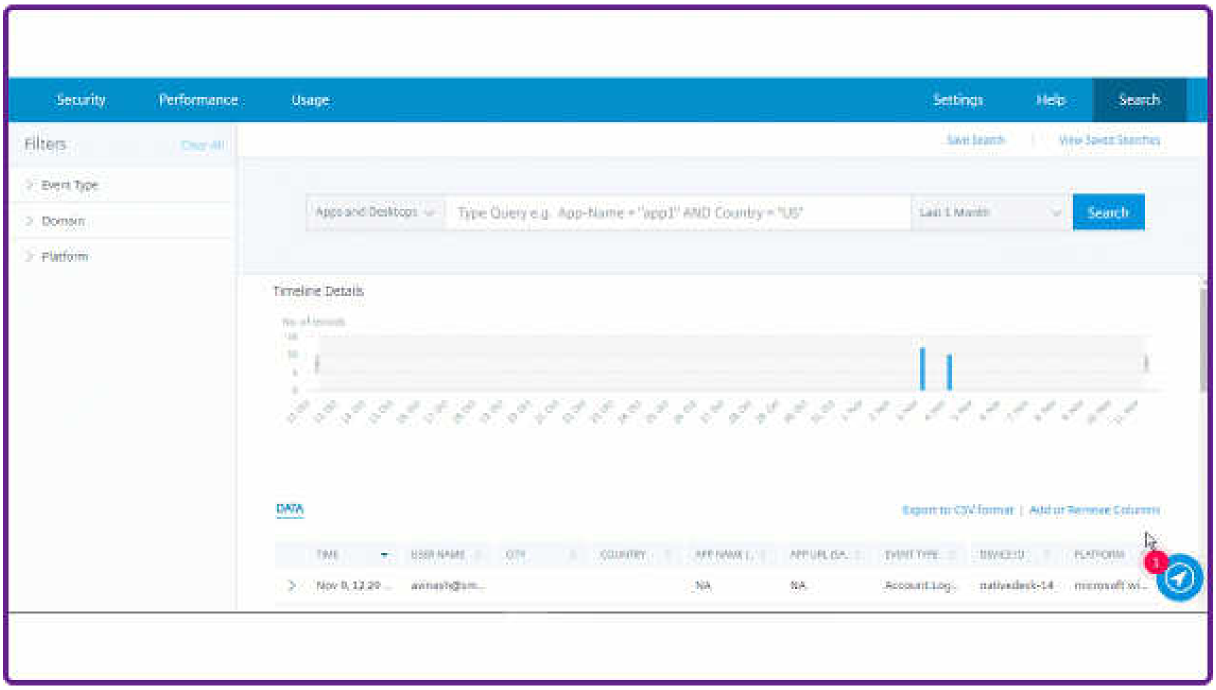


November 12, 2020

New feature

Save a self-service query After you create a self-service query, you can save it for later use. The following options are saved with the query:

- Applied search filters
- Selected data source and duration



TIME	USER NAME	CITY	COUNTRY	APP NAME (...	APP URL (SA...	EVENT TYPE	DEVICE ID	PLATFORM
Nov 8, 12:29 ...	avinash@sm...			NA	NA	Account Log...	nativedesk-14	microsoft wi...

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

October 20, 2020

New features

Support for Citrix Gateway in the European Union region Citrix Analytics now supports Citrix Gateway in the EU region. For more information, see Citrix Gateway data source.

July 09, 2020

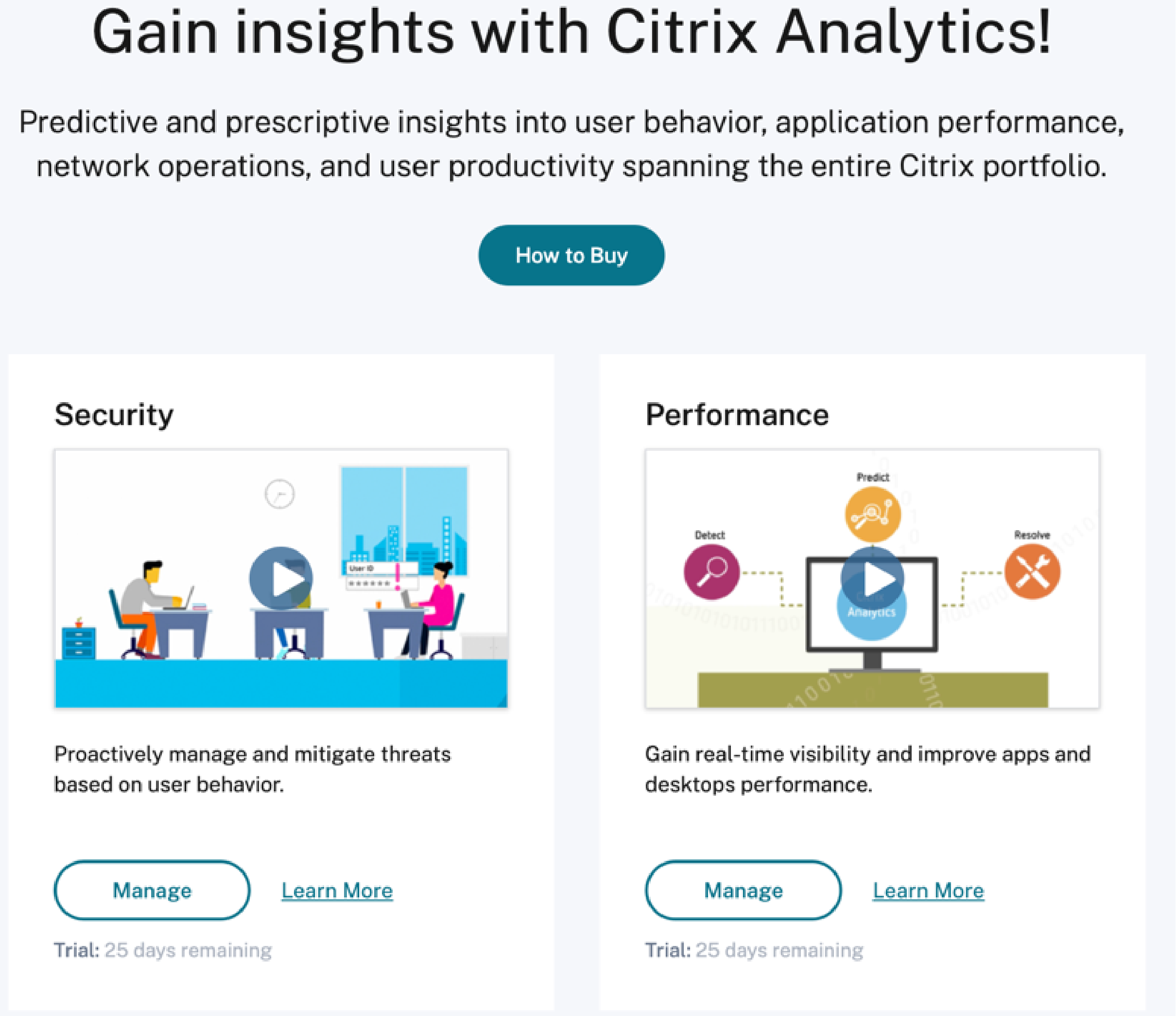
Deprecated support

Microsoft Internet Explorer 11 is now removed from the supported browsers list. This deprecation is because of the security vulnerability observed in the browser. For the list of supported browsers, see System requirements.

June 02, 2020

New features

Redesigned overview page and top bar in Analytics The Analytics overview page displays the **Usage** tile that replaces the previously existed **Operations** tile. Also, the **Productivity** tile is removed from this page. To view the overview page, select **Help** > **Overview**.



Gain insights with Citrix Analytics!

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

How to Buy

Security

Proactively manage and mitigate threats based on user behavior.

Manage Learn More

Trial: 25 days remaining

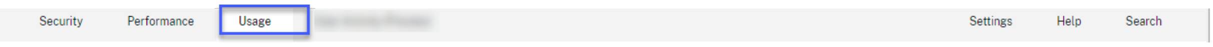
Performance

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

Manage Learn More

Trial: 25 days remaining

Similarly, on the top bar, the **Usage** tab replaces the **Operations** tab.



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
- 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

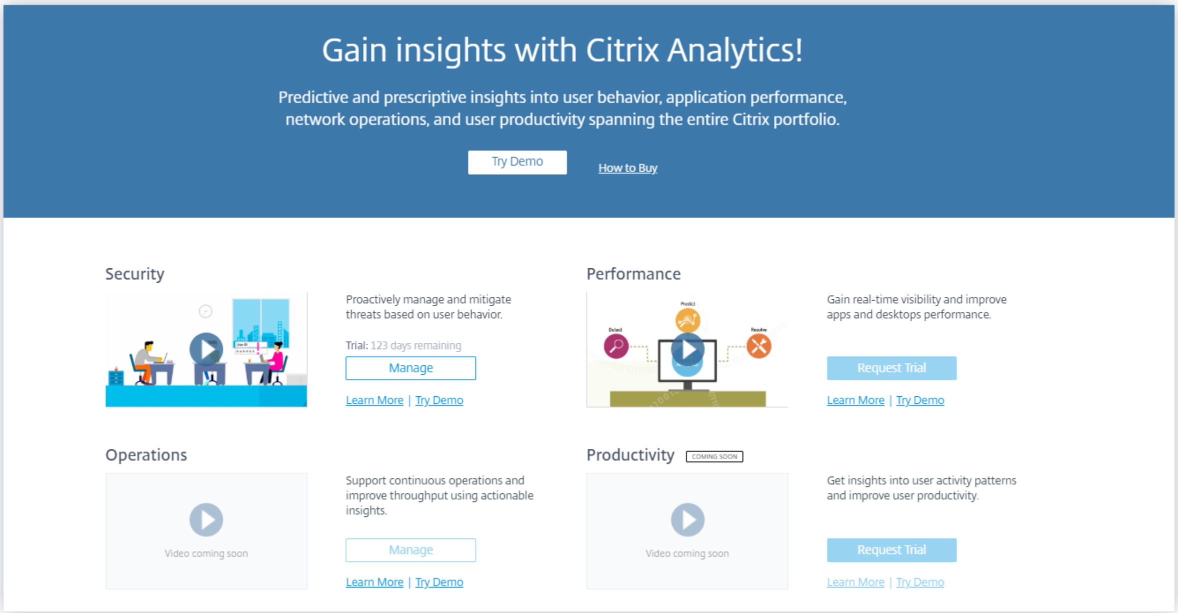
Some users in the Asia Pacific-South region are unable to sign in to Citrix Analytics although they have onboarded to Citrix Cloud by selecting **United States** as the home region. [CAS-27368]

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 the 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**.



Gain insights with Citrix Analytics!

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

Security

Proactively manage and mitigate threats based on user behavior.

Trial: 123 days remaining

Performance

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

Operations

Support continuous operations and improve throughput using actionable insights.

Productivity

Get insights into user activity patterns and improve user productivity.

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 rebranding 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.

- 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, screenshots, 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

August 2, 2023

This article highlights the known issues that are applicable across the Citrix Analytics offerings (Performance and Security).

For the issues specific to each offering, see the corresponding Known issues articles: Security and Performance.

- The **Gateway-First time access from new IP indicator** is triggered for users accessing services or applications through Gateway on the first time logging in. [CAS-57963]

Data Sources

August 1, 2023

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.

  For on-premises products such as Citrix Gateway and Citrix Virtual Apps and Desktops, you must perform a series of configurations to connect to Citrix Analytics. For example, the on-premises Gateway instances must be added to Application Delivery Management. And the on-premises

Virtual Apps and Desktops sites must be added to Workspace or the StoreFront servers must be configured.

- **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 Performance

Citrix Gateway, Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), and Citrix Virtual Apps and Desktops data sources are supported by both the offerings: Citrix Analytics for Security and Citrix Analytics for Performance. For information about the onboarding steps applicable for both the offerings, see the following articles:

- Citrix Gateway data source
- Citrix Virtual Apps and Desktops data source

Citrix Gateway data source

August 23, 2023

The **Gateway** data source represents the on-premises Citrix Gateway instances in your environment. Citrix Analytics automatically discovers the Citrix Application Delivery Management (ADM) agents and the Gateway instances added to the Citrix ADM service.

When users access any services or applications through Gateway, Citrix Analytics receives the user access events in real time. The user events are processed to detect any security threats.

This article describes the steps to add Citrix Gateway to Citrix Analytics. These steps are applicable for both the offerings: Citrix Analytics for Performance and Citrix Analytics for Security.

Prerequisites

- Subscribe to Citrix ADM offered on Citrix Cloud. To learn how to get started with Citrix ADM, see Getting Started.

- Verified Citrix ADM license. To know more about Citrix ADM Licensing, see Licenses.
- Review the system requirements and ensure that the requirements are met.

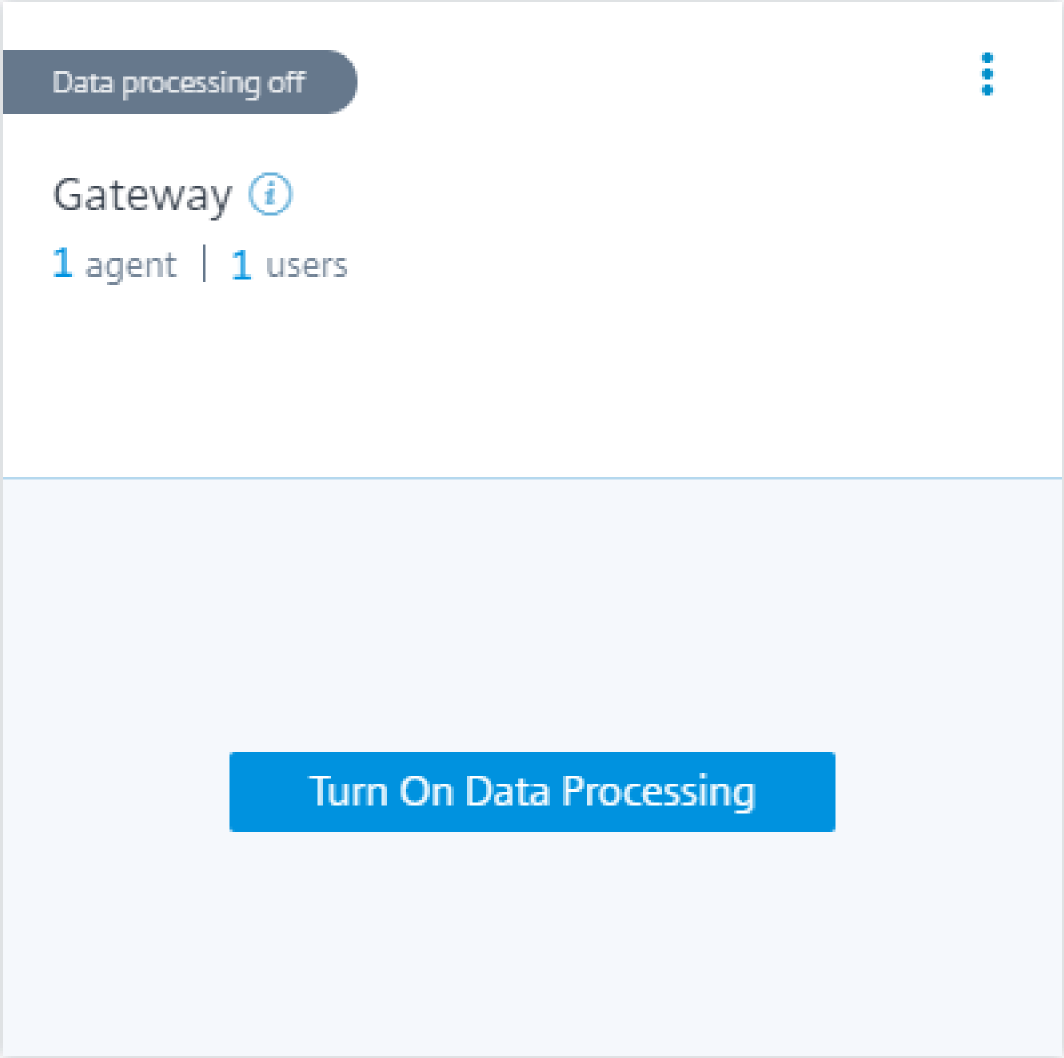
Gateway data sources added to Citrix ADM

Citrix Analytics automatically discovers the Citrix ADM agents and the Citrix Gateway instances that are already added to the Citrix ADM service.

To view the data source:

From the top bar, click **Settings** > **Data Sources**. Depending on your offering, select either **Security** or **Performance** to view the Gateway site card.

The discovered agents and the users are displayed on the Gateway site card. Click **Turn On Data Processing** to allow Citrix Analytics to begin processing data for this data source.

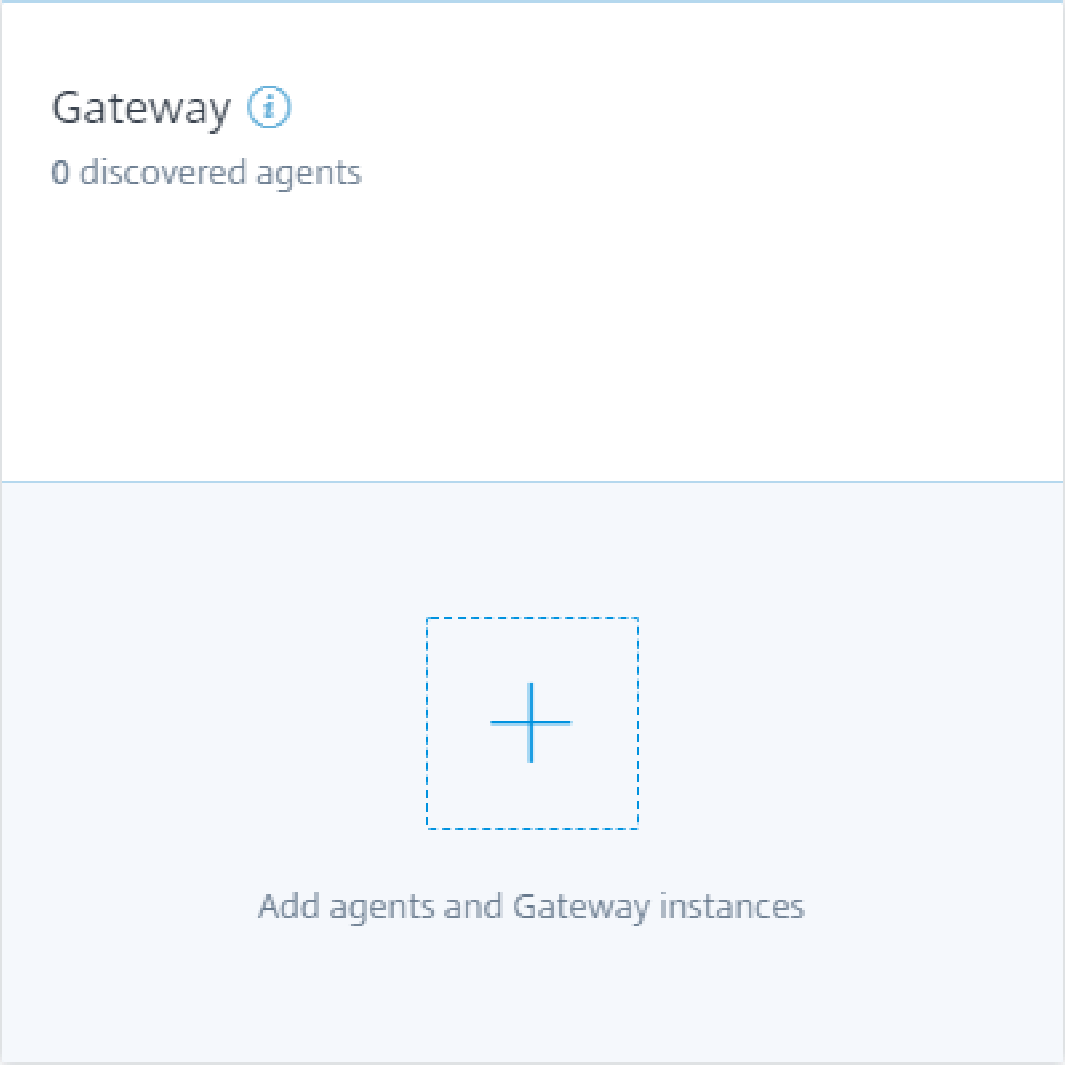


You can view the received events.

Refer A unified process to enable analytics on virtual servers to enable Citrix Analytics if not enabled already on the Citrix ADM Service.

Gateway data sources not added to Citrix ADM

The Gateway site card displays **0 discovered agents** when Citrix ADM agents and Citrix Gateway instances are not added to the Citrix ADM service.



To discover the agents and Gateway instances, do the following:

1. If you already have a Citrix ADM service subscription, click **+** on the site card to add the agents and the Gateway instances.

2. If you do not have a Citrix ADM service subscription, you must subscribe to it. Go to your Citrix Cloud account and do the following:

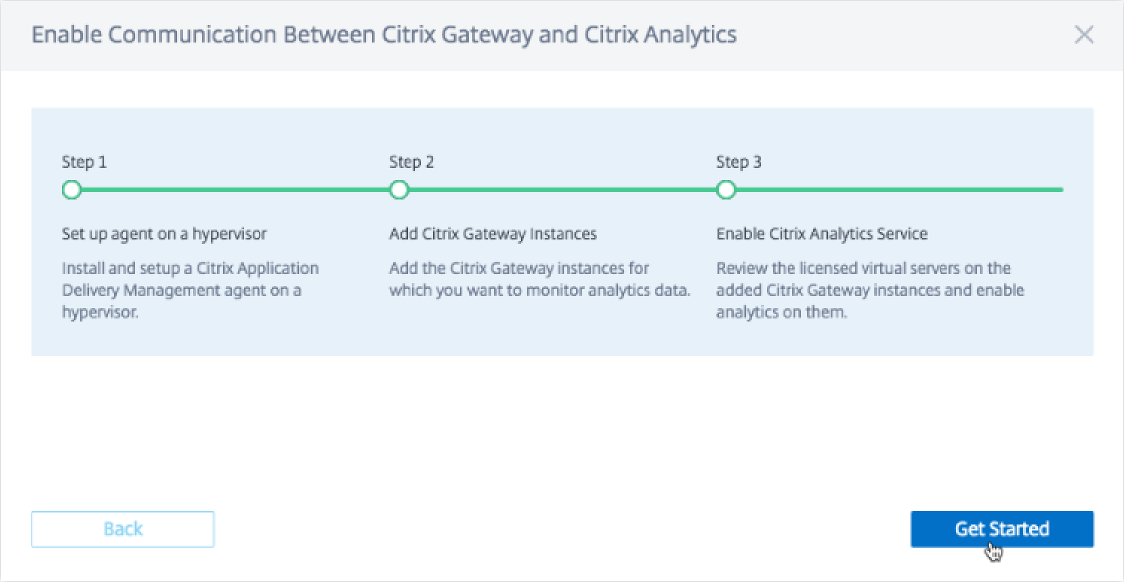
    a) Under **Available Services**, click **Manage** on the **Application Delivery Management** tile.

    b) Follow the on-screen instructions to create an Express account for Citrix ADM. For more information, see Getting started on the Citrix ADM documentation.

    c) After creating the Express account, log back to Analytics and click **Settings > Data Sources > Security**.

    d) On the Gateway site card, click **+** to add the agents and the Gateway instances.

3. On the following page, click **Get Started**.



Enable Communication Between Citrix Gateway and Citrix Analytics

Step 1

Set up agent on a hypervisor

Install and setup a Citrix Application Delivery Management agent on a hypervisor.

Step 2

Add Citrix Gateway Instances

Add the Citrix Gateway instances for which you want to monitor analytics data.

Step 3

Enable Citrix Analytics Service

Review the licensed virtual servers on the added Citrix Gateway instances and enable analytics on them.

4. Do the following tasks:

    - Install a Citrix ADM agent
    - Add your Gateway instances
    - Enable Analytics on virtual servers

Prerequisites

- **Citrix ADM agent installation requirement**: 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.

Component	Requirement
RAM	8 GB (32 GB recommended for better performance.)
Virtual CPU	4 (8 virtual CPUs recommended for better performance)
Storage space	120 GB
Virtual network interfaces	1
Throughput	1 Gbps

- **Port requirements**: Ensure that the following ports are open for the Citrix ADM agent to communicate with the Citrix Gateway instances.

Type	Port	Description
TCP	80/443	For NITRO communication from agent to Citrix Gateway instances
TCP	22	For SSH communication from agent to Citrix Gateway instance.
UDP	4739	For AppFlow communication from Citrix Gateway to agent
ICMP	No reserved port	To detect network reachability from agent to Citrix Gateway instances.
SNMP	161, 162	To receive SNMP events from Citrix Gateway instance to agent.
Syslog	514	To receive syslog messages in agent from Citrix Gateway instance.
TCP	5557	For log stream communication from Citrix Gateway instances to agent.

For communication between the Citrix ADM agent and Citrix Analytics, ensure that the following port is open:

Type	Port	Description
TCP	443	For NITRO communication between the agent and the Citrix Application Delivery Management service.

For communication between the Citrix ADM agent and Citrix Analytics, ensure that the following endpoint is whitelisted:

Endpoint	US region	EU region
Event Hub	`https://cas-eh-ns-alias.servicebus.windows.net/`	`https://cas-eh-ns-eu-alias.servicebus.windows.net/`

Install and set up an agent

Install and configure the Citrix ADM service agent in your network environment to enable communication between Analytics and the Gateway instances in your data center.

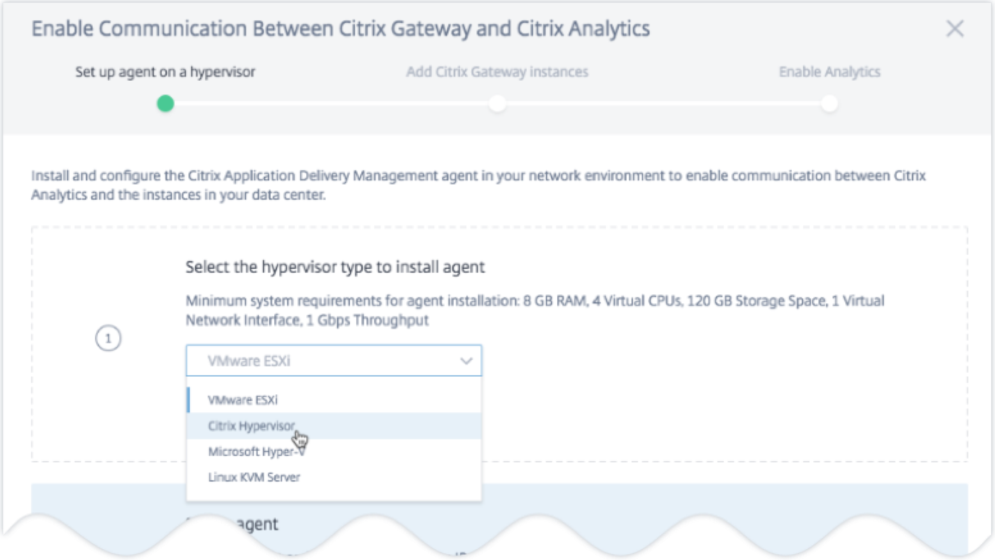
You can install an agent on the following hypervisors in your enterprise data center:

- Citrix Hypervisor
- VMware ESXi
- Microsoft Hyper-V
- Linux KVM Server

To install and set up an agent, do the following:

1. Download the agent image.

   On the **Set up agent on a hypervisor** page, select the hypervisor, and click **Download Image** to download the agent image to your local system.



Enable Communication Between Citrix Gateway and Citrix Analytics

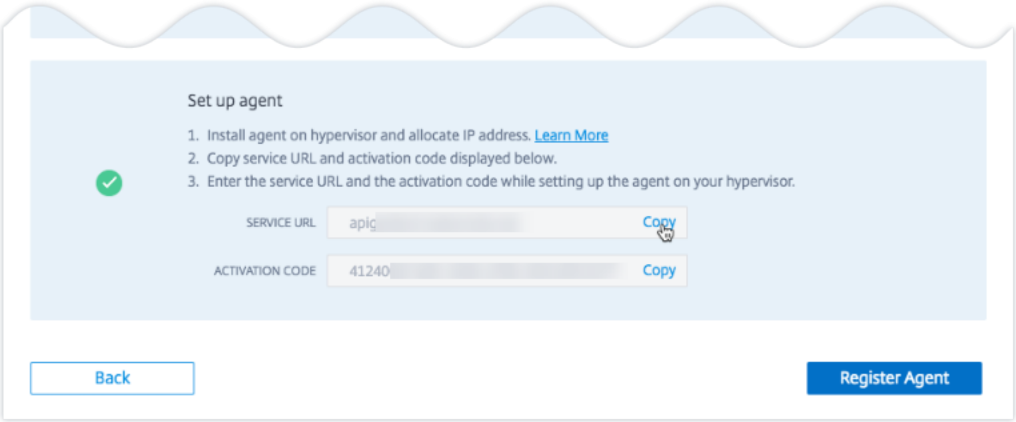
Install and configure the Citrix Application Delivery Management agent in your network environment to enable communication between Citrix Analytics and the instances in your data center.

Select the hypervisor type to install agent

Minimum system requirements for agent installation: 8 GB RAM, 4 Virtual CPUs, 120 GB Storage Space, 1 Virtual Network Interface, 1 Gbps Throughput

2. Copy service URL and activation code.

   A service URL and an activation code are generated and displayed on the UI as shown in the following image. (This process might take a few seconds.) The agent uses the service URL to locate the service and the activation code to register with the service. Enter the service URL and the activation code while installing the agent on your hypervisor.



Set up agent

1. Install agent on hypervisor and allocate IP address. Learn More
2. Copy service URL and activation code displayed below.
3. Enter the service URL and the activation code while setting up the agent on your hypervisor.

SERVICE URL apig[redacted]

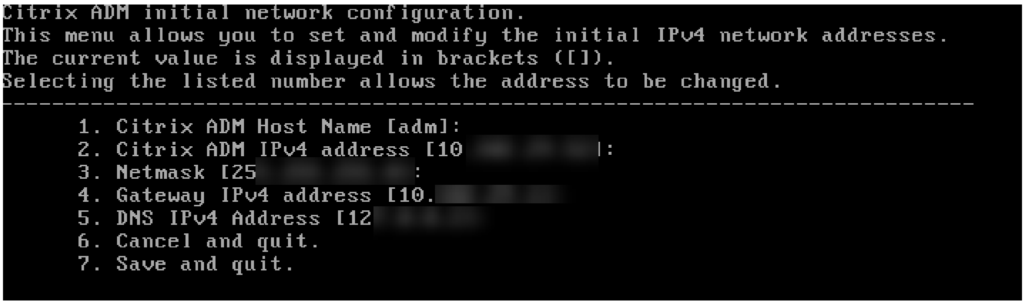
ACTIVATION CODE 41240[redacted]

3. Install the agent on a hypervisor.

   > **Note**
   >
   > Before you begin agent installation, ensure that:
   >
   > - You have the required virtual computing resources that the hypervisor must provide for each agent: RAM: 8 GB, vCPU: 4, storage space: 120 GB, virtual network interface: 1, and throughput: 1 Gbps
   > - You configure your DNS to allow internet access to your agent.

   - On a Citrix Hypervisor, perform the following:

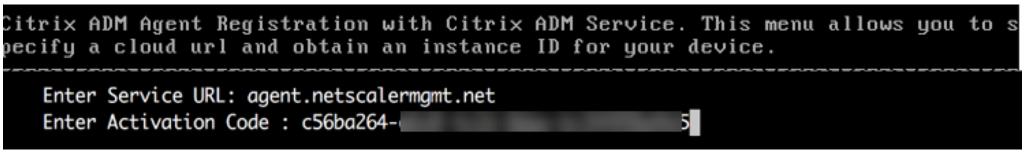
a) Import the agent image file to your hypervisor. From the **Console** tab configure the initial network configuration options as shown in the following example.



```
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-----------------------------------------------------------------------------
      1. Citrix ADM Host Name [adm]:
      2. Citrix ADM IPv4 address [10[redacted]]:
      3. Netmask [25[redacted]:
      4. Gateway IPv4 address [10.[redacted]
      5. DNS IPv4 Address [12[redacted]
      6. Cancel and quit.
      7. Save and quit.
```

If you have entered incorrect values or want to change any value, log on to the shell prompt by using the default credentials `nsrecover/nsroot`. Then run the command `networkconfig`.

b) Enter the **Service URL** and the **Activation Code** that you saved while downloading the agent image.

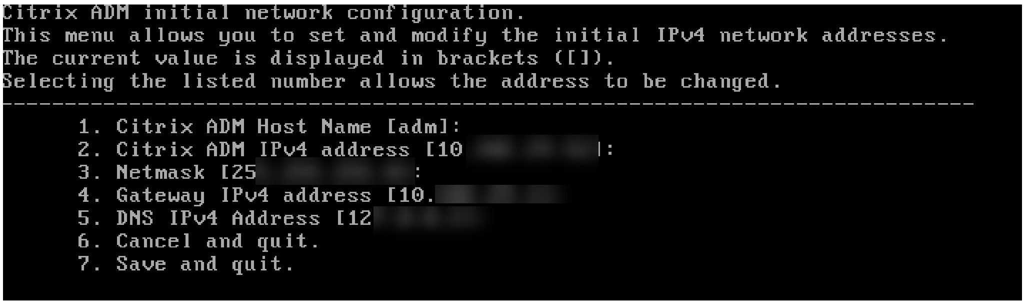


```
Citrix ADM Agent Registration with Citrix ADM Service. This menu allows you to s
pecify a cloud url and obtain an instance ID for your device.
---------------------------------------------------------------------------------
   Enter Service URL: agent.netscalermgmt.net
   Enter Activation Code : c56ba264-[redacted]5
```

If you entered the service URL or the activation code incorrectly, log on to the shell prompt of the agent and then run the script: `deployment_type.py`. This script lets you reenter the Service URL and activation code.

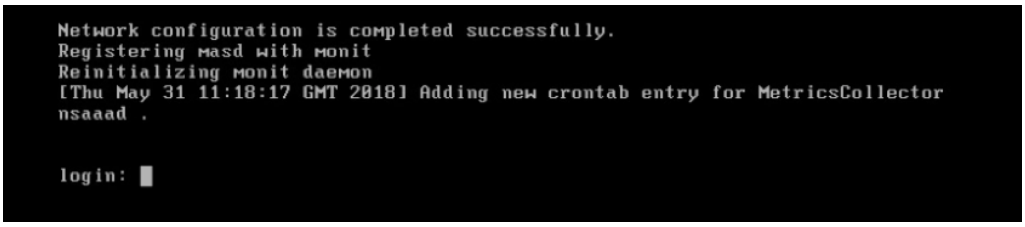
- On a VMware ESXi hypervisor, perform the following:

a) Import the agent image file to your hypervisor. From the **Console** tab configure the initial network configuration options as shown in the following example.



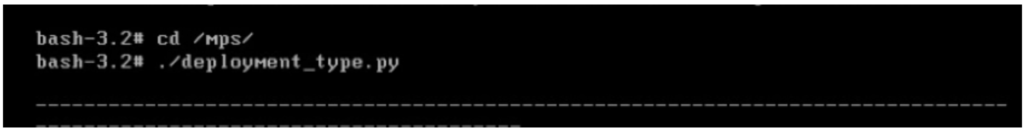
```
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-----------------------------------------------------------------------------
      1. Citrix ADM Host Name [adm]:
      2. Citrix ADM IPv4 address [10[redacted]]:
      3. Netmask [25[redacted]:
      4. Gateway IPv4 address [10.[redacted]
      5. DNS IPv4 Address [12[redacted]
      6. Cancel and quit.
      7. Save and quit.
```

b) After you configure the network, when prompted, log on to the shell prompt of the agent using the default credentials `nsrecover/nsroot`.

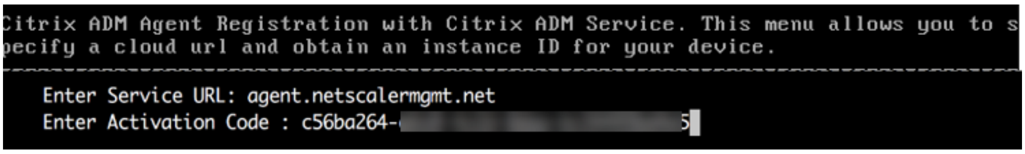


```
Network configuration is completed successfully.
Registering masd with monit
Reinitializing monit daemon
[Thu May 31 11:18:17 GMT 2018] Adding new crontab entry for MetricsCollector
nsaaad .

login: █
```

c) Navigate to the **/mps** directory, run the script, and enter the **Service URL** and the **Activation Code** that you saved when you while downloading the agent image.



```
bash-3.2# cd /mps/
bash-3.2# ./deployment_type.py

----------------------------------------------------------------------------------
```

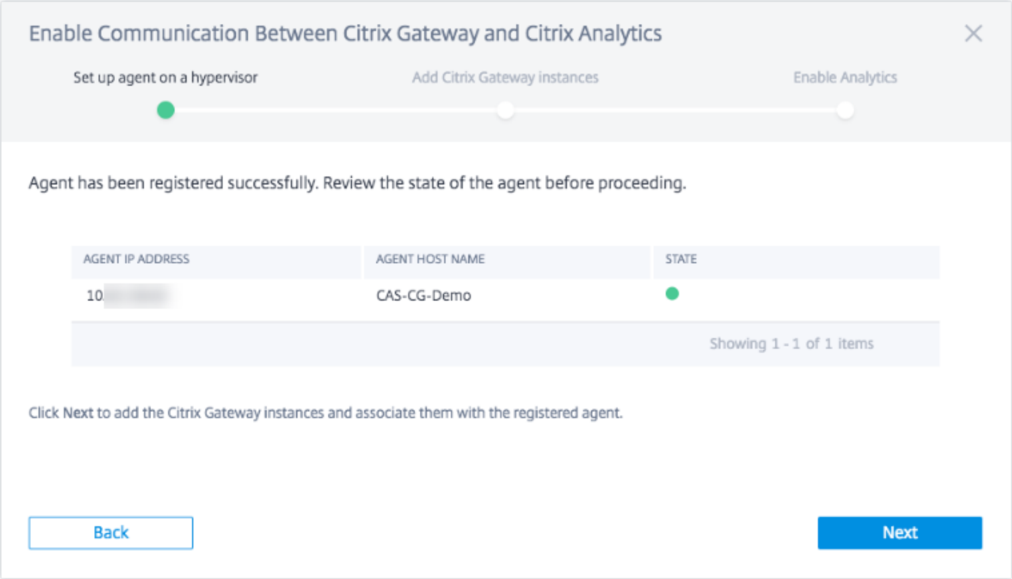


```
Citrix ADM Agent Registration with Citrix ADM Service. This menu allows you to s
pecify a cloud url and obtain an instance ID for your device.
---------------------------------------------------------------------------------
 Enter Service URL: agent.netscalermgmt.net
 Enter Activation Code : c56ba264-[redacted]5█
```

> **Note**
>
> You can use the same image file to install multiple agents. However, you cannot use the same activation code on more than one agent. To generate a new activation code, access Citrix Analytics, and on the Setup agent on a hypervisor step, click **Download Image** again. A new activation code is generated.

4. Register Agent.

   After agent registration is successful, the agent restarts to complete the installation process. After the agent has restarted, access Citrix Analytics and click **Register Agent**, and then verify the status of the agent.



Enable Communication Between Citrix Gateway and Citrix Analytics

Agent has been registered successfully. Review the state of the agent before proceeding.

AGENT IP ADDRESS	AGENT HOST NAME	STATE
10[redacted]	CAS-CG-Demo	●

Showing 1 - 1 of 1 items

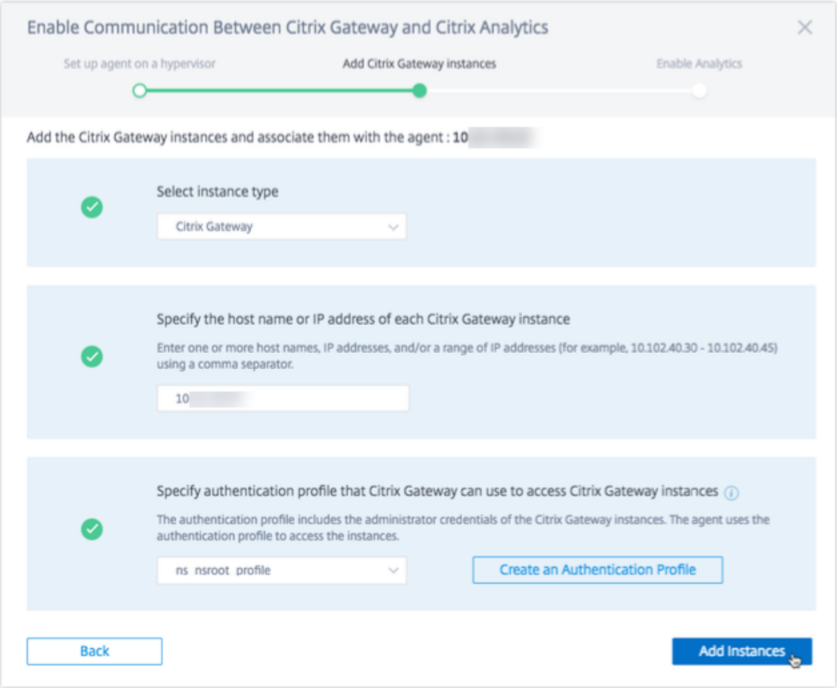
Click Next to add the Citrix Gateway instances and associate them with the registered agent.

When the agent status is in the UP state denoted by a green dot next to it, click **Next** to start adding instances to the service.

Add Citrix Gateway instances

Instances are Citrix Gateway appliances or virtual appliances that are the data sources for Citrix Analytics.

1. On the **Add Citrix Gateway Instances** page, select the instance type and specify host names or IP Addresses or range of IP addresses of Gateway instances to discover.
2. Create an authentication profile that the agent can use to access the Gateway instances. This profile is the administrator credentials of a Gateway instance. Then, click **Add Instances**.



Enable Communication Between Citrix Gateway and Citrix Analytics

Add the Citrix Gateway instances and associate them with the agent : 10[redacted]

Select instance type: Citrix Gateway

Specify the host name or IP address of each Citrix Gateway instance

Enter one or more host names, IP addresses, and/or a range of IP addresses (for example, 10.102.40.30 - 10.102.40.45) using a comma separator.

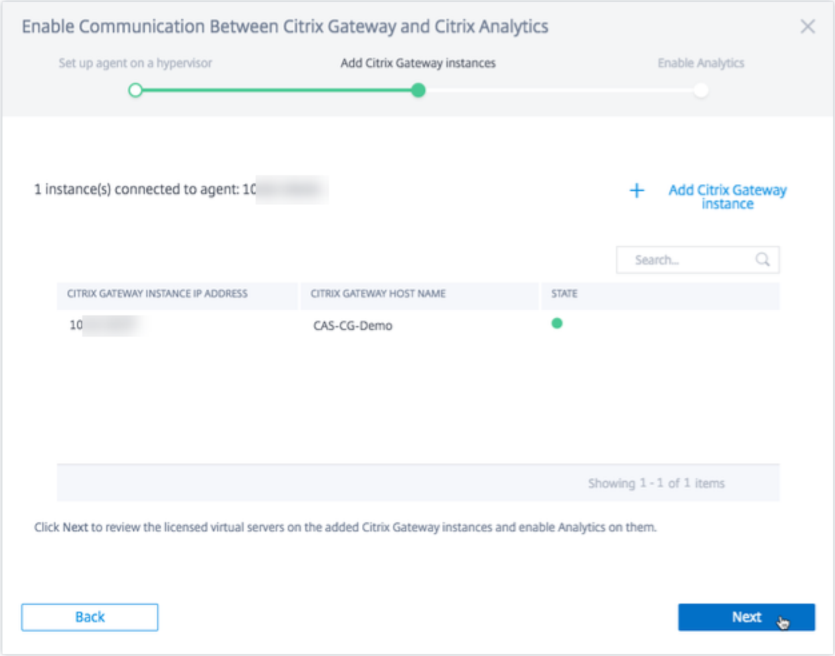
10[redacted]

Specify authentication profile that Citrix Gateway can use to access Citrix Gateway instances

The authentication profile includes the administrator credentials of the Citrix Gateway instances. The agent uses the authentication profile to access the instances.

ns_nsroot_profile

After the instances are added, you can view the number of instances that have been successfully discovered. To add more instances, click **Add Citrix Gateway Instance**.



Enable Communication Between Citrix Gateway and Citrix Analytics

Set up agent on a hypervisor
Add Citrix Gateway instances
Enable Analytics

1 instance(s) connected to agent: 10[redacted]

+ Add Citrix Gateway instance
Search...

CITRIX GATEWAY INSTANCE IP ADDRESS	CITRIX GATEWAY HOST NAME	STATE
10[redacted]	CAS-CG-Demo	●

Showing 1 - 1 of 1 items

Click Next to review the licensed virtual servers on the added Citrix Gateway instances and enable Analytics on them.

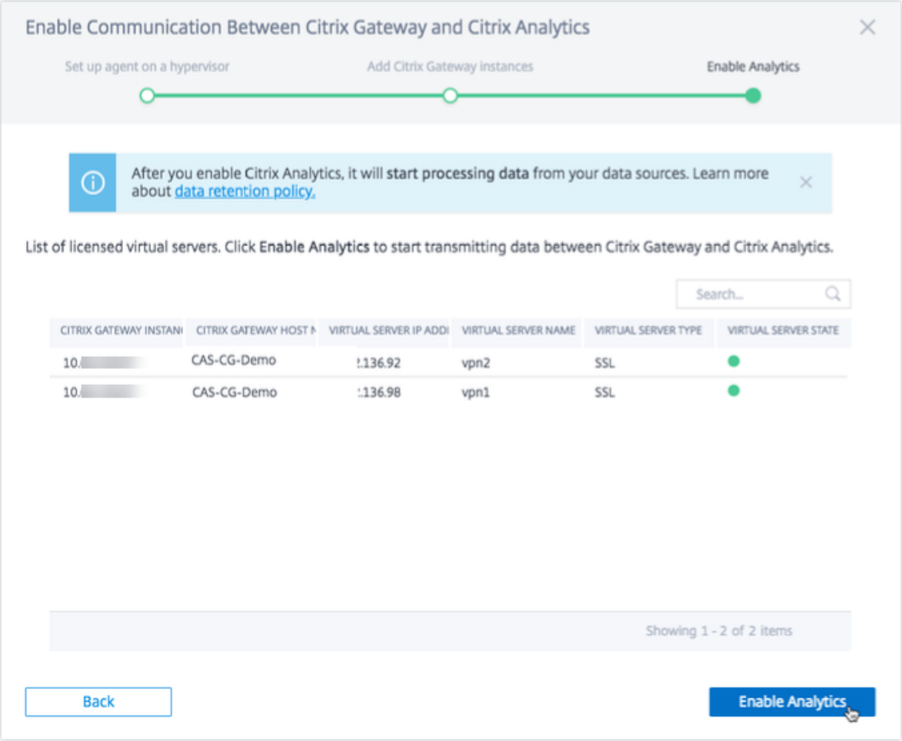
Click **Next** to enable analytics.

Enable analytics

Citrix Analytics automatically discovers the licensed virtual servers on the added Citrix Gateway Instances. Enable analytics on all the discovered virtual servers.

On the **Enable Analytics** page, by default, all the licensed virtual servers from the Gateway instances appear. Review the list of licensed virtual servers and click **Enable Analytics** to enable analytics on the virtual servers.

> **Note**
>
> The virtual servers might take some time, approximately 10 minutes, to appear on the page.



Enable Communication Between Citrix Gateway and Citrix Analytics

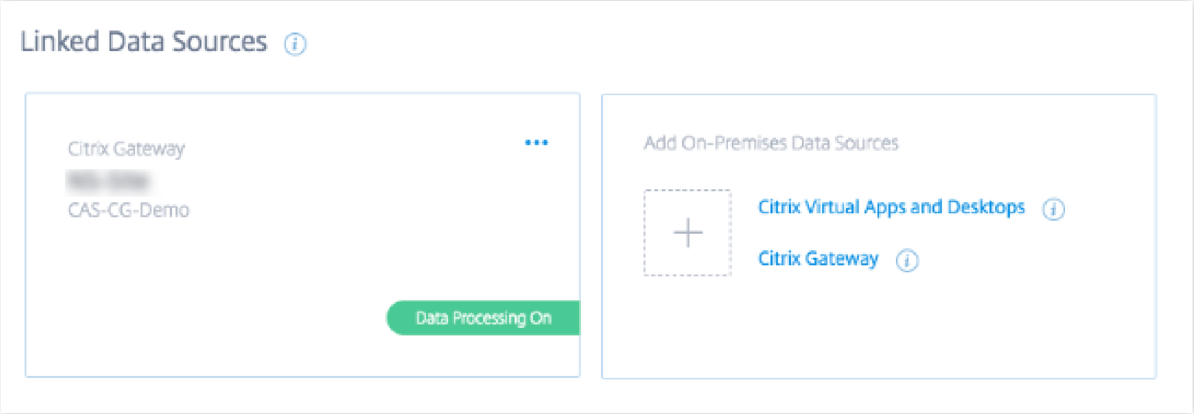
After you enable Citrix Analytics, it will **start processing data** from your data sources. Learn more about data retention policy.

List of licensed virtual servers. Click **Enable Analytics** to start transmitting data between Citrix Gateway and Citrix Analytics.

CITRIX GATEWAY INSTAN	CITRIX GATEWAY HOST N	VIRTUAL SERVER IP ADD	VIRTUAL SERVER NAME	VIRTUAL SERVER TYPE	VIRTUAL SERVER STATE
10.[redacted]	CAS-CG-Demo	:.136.92	vpn2	SSL	●
10.[redacted]	CAS-CG-Demo	:.136.98	vpn1	SSL	●

Showing 1 - 2 of 2 items

The status of the site card changes to **Data Processing On**. You can view the received events.



Watch the onboarding video

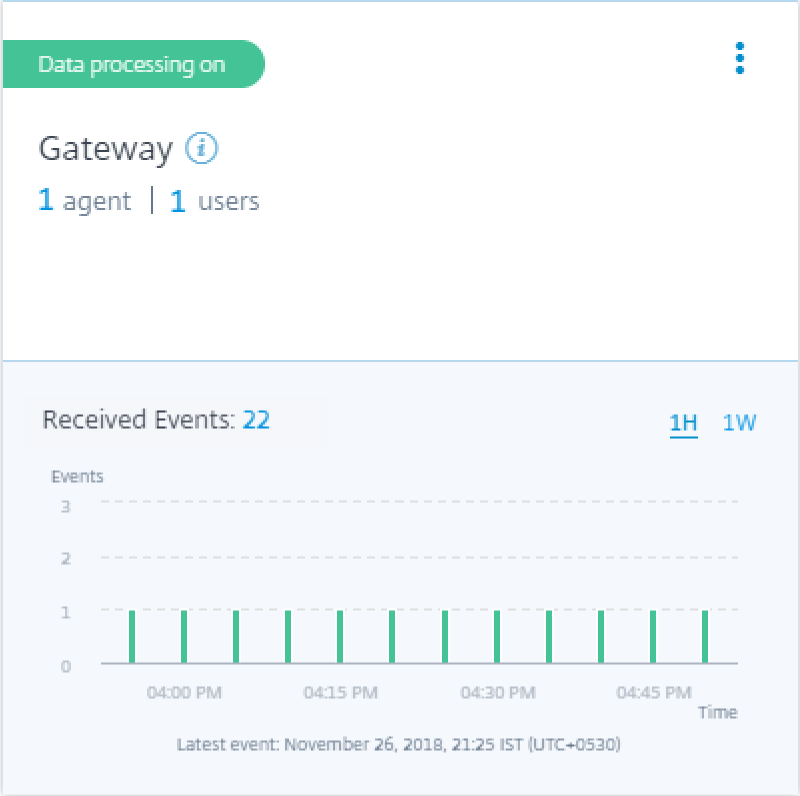
The following video shows the steps to onboard a Gateway instance:

This is an embedded video. Click the link to watch the video

View received events, users, and agents

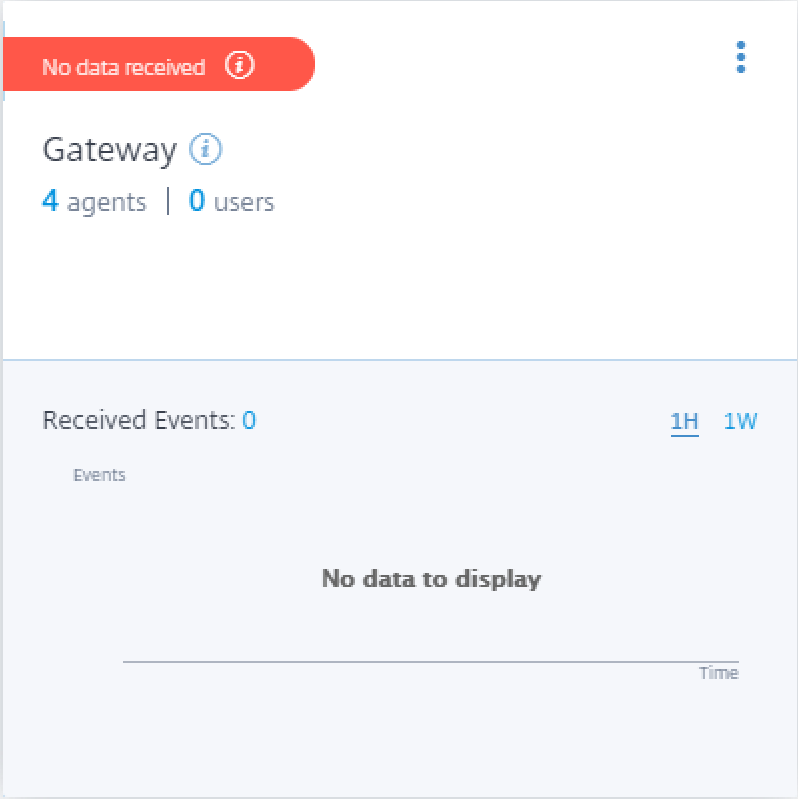
The site card displays the number of Gateway users, Citrix ADM agents, and the events received from the data source for the last one hour, which is the default time selection. You can also select 1 week

(**1W**) and view the data. Click the number of users to view on the **Users** page. Click the number of agents to view the Citrix Gateway instances and the agents.



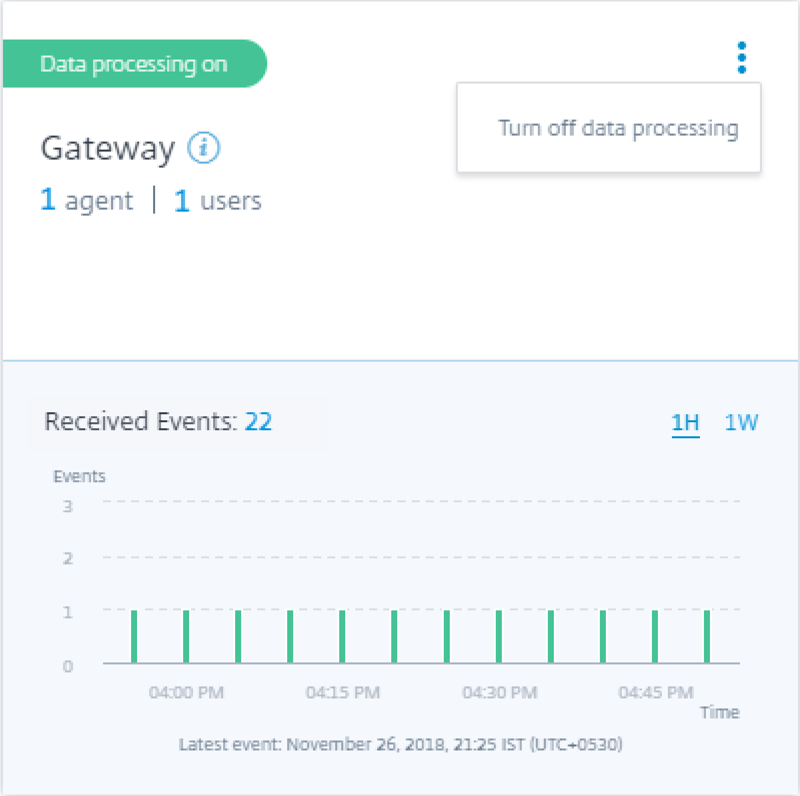
After you have enabled data processing, the site card might display the **No data received** status. This status appears for two reasons:

1. If you have turned on data processing for the first time, the events take some time to reach the event hub in Citrix Analytics. When Citrix Analytics receives the events, the status changes to **Data processing on**. If the status does not change after some time, refresh the **Data Sources** page.
2. Analytics has not received any events from the data source in the last one hour.

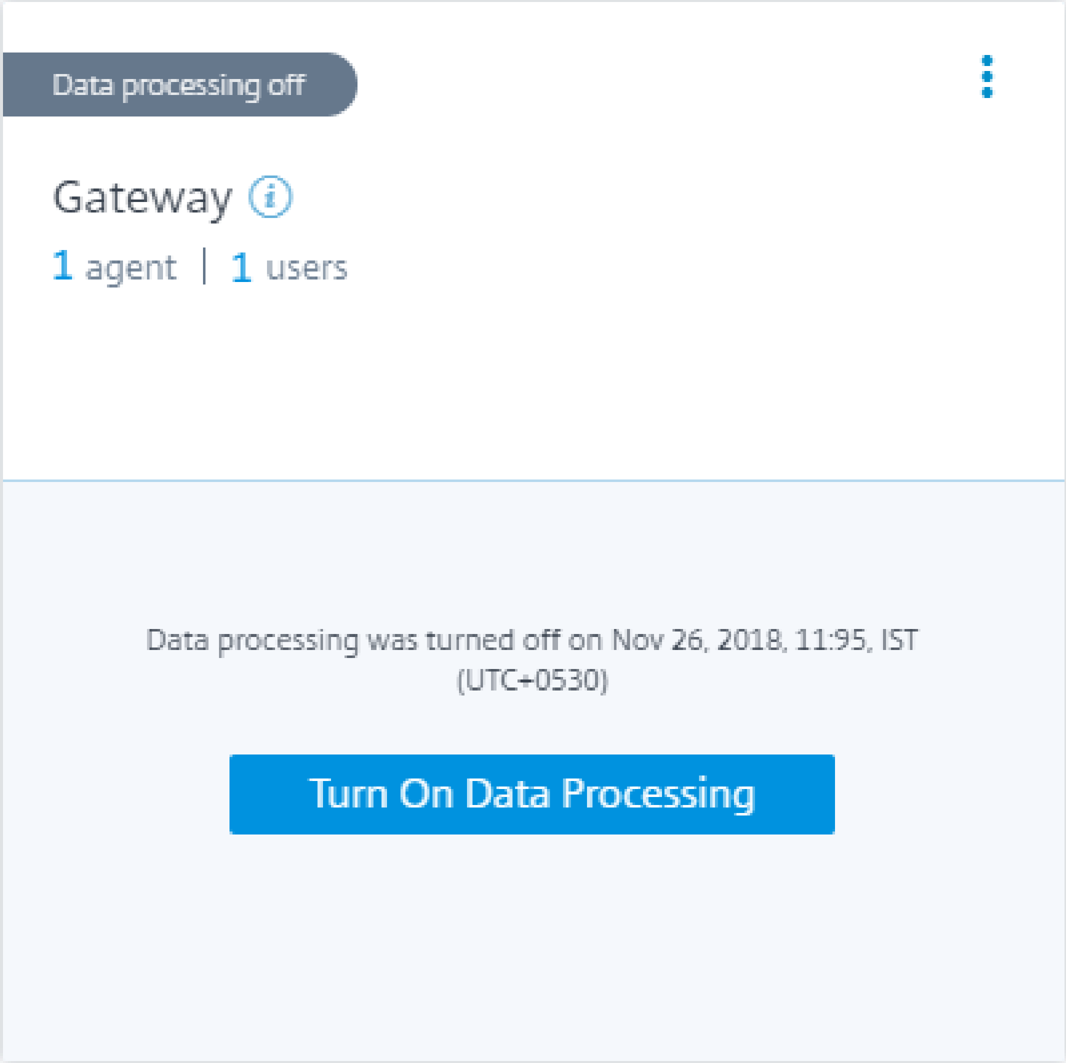


Turn on or off data processing

To stop data processing, click the vertical ellipsis (⋮) on the site card and then click **Turn off data processing**. Citrix Analytics stops processing data for this data source.



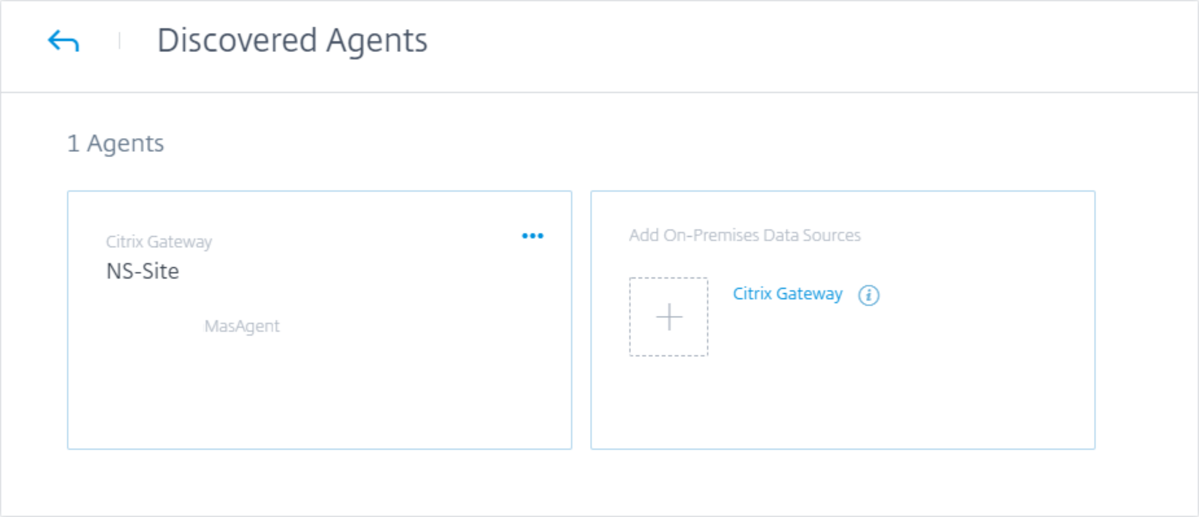
To enable data processing again, click **Turn On Data Processing**.



Data processing was turned off on Nov 26, 2018, 11:95, IST (UTC+0530)

Add more Gateway instances

If you want to add more Gateway instances, click the number of agents on the Gateway site card to view the **Discovered Agents** page. From the **Add On-Premises Data Sources** tile, click **Citrix Gateway**.



Discovered Agents

1 Agents

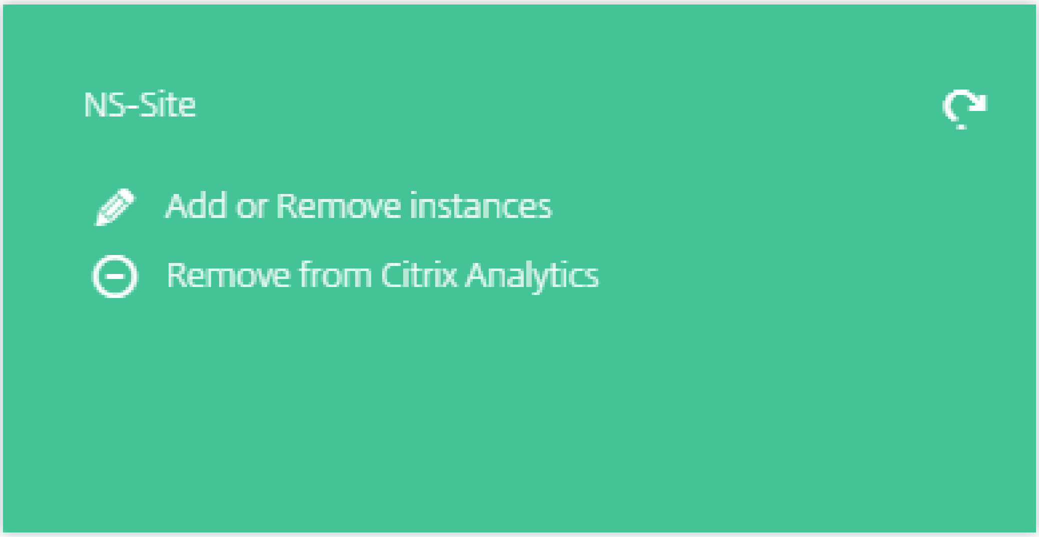
Citrix Gateway
NS-Site
MasAgent

Add On-Premises Data Sources
Citrix Gateway

Manage data source

You can also add more instances to an agent or remove instances associated with an agent. You can also remove the agent and it's associated instances from Citrix Analytics.

Flip an agent site card and do one of the following:



NS-Site
Add or Remove instances
Remove from Citrix Analytics

- **Add or Remove instances**. You can add more Gateway instances to an agent and enable Analytics on the virtual servers configured on those instances. You can also remove instances added to an agent. When you dissociate an instance from an agent, Citrix Analytics cannot communicate with that instance.
- **Remove from Citrix Analytics**. After you remove an agent site, Citrix Analytics stops collecting data from the instances associated with that agent. But all the previously processed data is

available during the retention period.

Citrix Virtual Apps and Desktops data source

March 22, 2024

This article describes the steps to connect your on-premises Citrix Virtual Apps and Desktops sites to Citrix Analytics using StoreFront. The onboarding steps mentioned in this article are applicable for both the offerings: Citrix Analytics for Performance (Performance Analytics) and Citrix Analytics for Security (Security Analytics).

For the onboarding steps specific to each offering, see the following articles:

- Configuring on-premises Citrix Virtual Apps and Desktops sites with Citrix Analytics for Performance
- Configuring Citrix Virtual Apps and Desktops and Citrix DaaS data source for Citrix Analytics for Security

Onboard Citrix Virtual Apps and Desktops on-premises sites using StoreFront

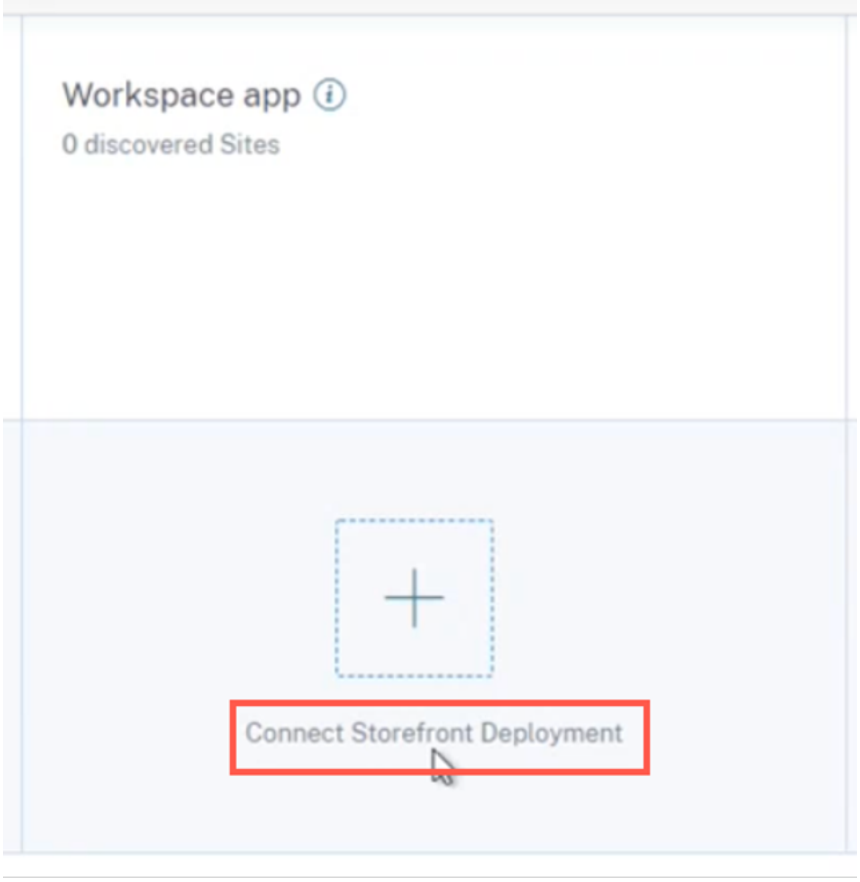
If your organization uses an on-premises StoreFront deployment, you must configure your StoreFront servers to enable Citrix Workspace app to send events to Citrix Analytics. Citrix Analytics processes events to provide actionable insights into the performance of your Citrix IT infrastructure and user behavior.

For more information on how to configure a StoreFront deployment for Citrix Analytics, see the Citrix Analytics service article in the StoreFront documentation.

Earlier, customers using the Citrix Apps and Desktops on-premises sites were enforced to use the site aggregation to onboard the on-premises sites for Citrix Analytics for Security and Performance.

You can now onboard Citrix Apps and Desktops on-premises sites without depending on the site aggregation.

You can see the **Connect Storefront Deployment** option on your workspace application, even if you do not have any site added to the site aggregation.



Prerequisites

Before you begin, ensure the following:

- Your StoreFront version must be 1906 or later.
- The StoreFront deployment must be able to connect to the following addresses:
  - https://*.cloud.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.
- If the StoreFront deployment is hosted on a webserver that uses a web proxy to connect to the Internet, the proxy for each store must be manually configured to allow outbound traffic. StoreFront does not automatically use the proxy setting of the host webserver. For more information, see Configure a StoreFront deployment hosted on a webserver that uses HTTP proxy.
- The StoreFront deployment must be accessed using one of the following clients:
  - Citrix Receiver for websites in HTML5-compatible browsers.

> **Note**
>
> If you are an HTML5 user, Citrix Virtual Apps and Desktops can launch events when certain configurations are enabled on StoreFront. For information about the configuration steps, see the Install article in the Citrix Workspace app for HTML5 documentation. For print-related events, extra policies must be configured on StoreFront. For more information, see the PDF Printing article in the Citrix Workspace app for HTML5 documentation.

  - Citrix Workspace app 1907 for Windows or later.
  - Citrix Workspace app 2006 for Linux or later.
  - Citrix Workspace app 2006 for Mac or later

- If you are using Citrix Virtual Apps and Desktops 7 1912 LTSR, the supported StoreFront version is 1912.

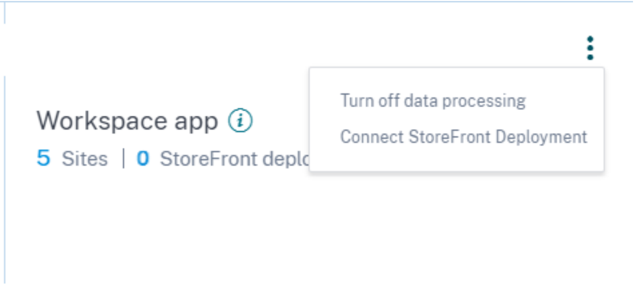
Connect to a StoreFront deployment

You can connect to a StoreFront deployment in the following ways –

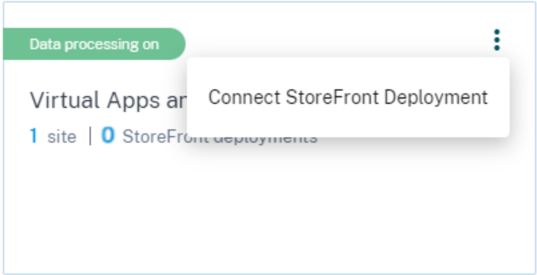
- Using the **Apps and Desktops –Workspace app** site card and the **Apps and Desktops –Monitoring** site card
- Using the **Recommendations** panel

Connect using Apps and Desktops –Workspace app site card and the Apps and Desktops – Monitoring site card

1. Navigate to **Settings > Data Sources > Security**. On the **Apps and Desktops- Workspace app** site card, click the vertical ellipsis (⋮) and then select **Connect StoreFront deployment**.

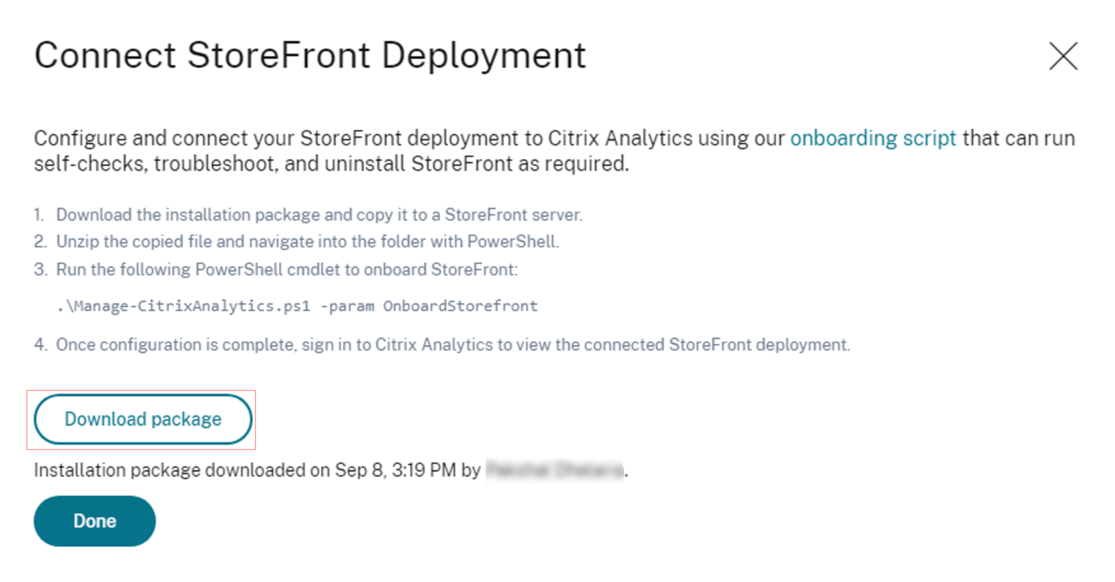


2. Navigate to **Settings > Data Sources > Performance**. On the **Apps and Desktops- Monitoring** site card, click the vertical ellipsis (⋮) and then select **Connect StoreFront deployment**.


Data processing on
Virtual Apps ar
Connect StoreFront Deployment
1 site | 0 StoreFront deployments

The StoreFront Onboarding wizard or the **Connect StoreFront Deployment** popup appears.

3. Click **Download package**.



Connect StoreFront Deployment

Configure and connect your StoreFront deployment to Citrix Analytics using our onboarding script that can run self-checks, troubleshoot, and uninstall StoreFront as required.

1. Download the installation package and copy it to a StoreFront server.
2. Unzip the copied file and navigate into the folder with PowerShell.
3. Run the following PowerShell cmdlet to onboard StoreFront:

```
.\Manage-CitrixAnalytics.ps1 -param OnboardStorefront
```

4. Once configuration is complete, sign in to Citrix Analytics to view the connected StoreFront deployment.

Installation package downloaded on Sep 8, 3:19 PM by [redacted].

> **Note**
>
> The file contains sensitive information. Keep the file in a safe and secure location.

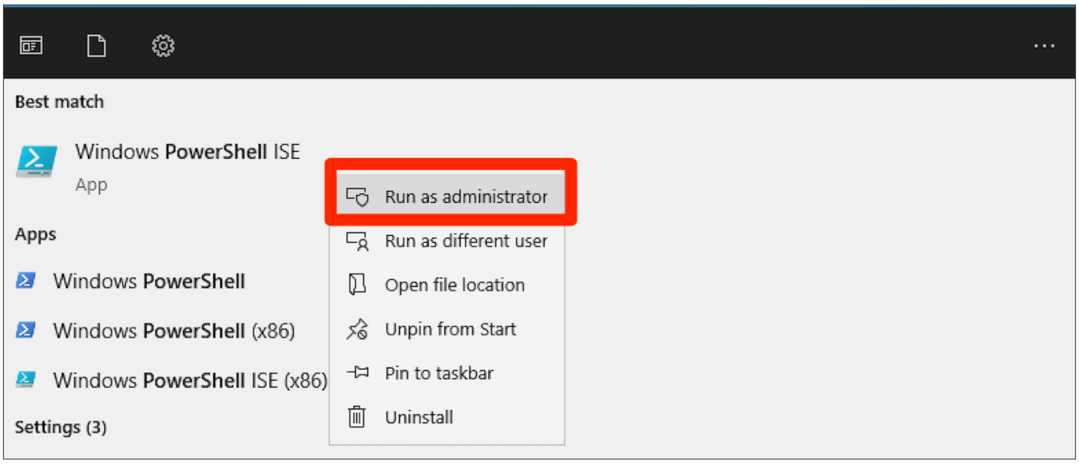
4. To configure the StoreFront deployment,

   a) Copy the installation package to the StoreFront server.

   b) Unzip the copied file and navigate into the folder within PowerShell.

   c) You must run the following command as an administrator to onboard the StoreFront:

   .\Manage-CitrixAnalytics.ps1 –param OnboardStorefront



For more options or parameters, refer to the PowerShell Script section.

d) Open the StoreFront server and execute the PowerShell script.

e) If the StoreFront site does not appear in the Citrix Analytics Service GUI even after running OnboardStorefront, run the iisreset command.

f) Log in to Citrix Analytics Service GUI and validate if the Cluster ID matches to the one logged in the console by the script.

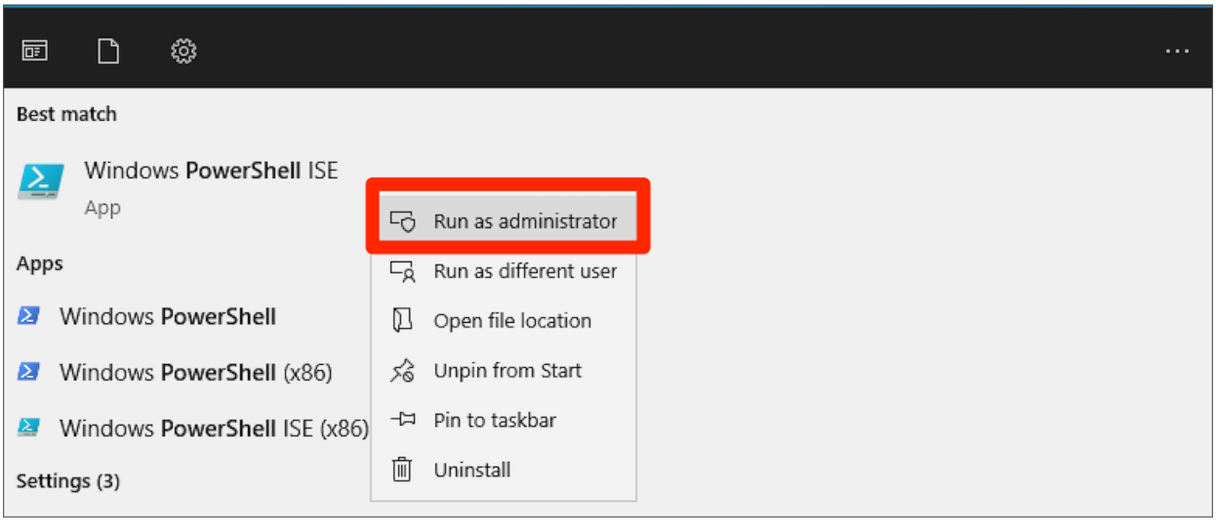
g) Once the configuration is done, log in to Citrix Analytics to view the connected StoreFront Deployment.

5. After the configuration is successful, click **Done**.

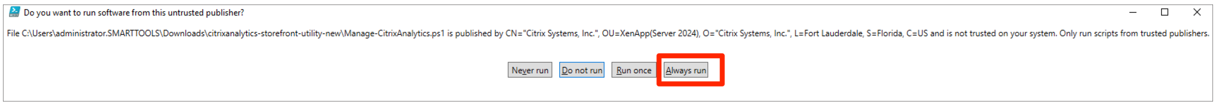
6. Click **Turn On Data Processing** to allow Citrix Analytics to process the data.

PowerShell Script

A new PowerShell script has been introduced to simplify the StoreFront onboarding process to Citrix Analytics Service. This PowerShell script automates the process of pre-requisites check, installing, and configuring StoreFront. The PowerShell script needs to run in administrator mode.



Customers can execute this PowerShell script on the StoreFront to onboard, deboard, perform self-checks, troubleshoot, and verify if the onboarding to Citrix Analytics Service GUI is successful. When a customer executes the script for the first time, a security warning message appears to confirm on the publisher. Select the Always run option if the publisher is trusted.



Do you want to run software from this untrusted publisher?

File C:\Users\administrator.SMARTTOOLS\Downloads\citrixanalytics-storefront-utility-new\Manage-CitrixAnalytics.ps1 is published by CN="Citrix Systems, Inc.", OU=XenApp(Server 2024), O="Citrix Systems, Inc.", L=Fort Lauderdale, S=Florida, C=US and is not trusted on your system. Only run scripts from trusted publishers.

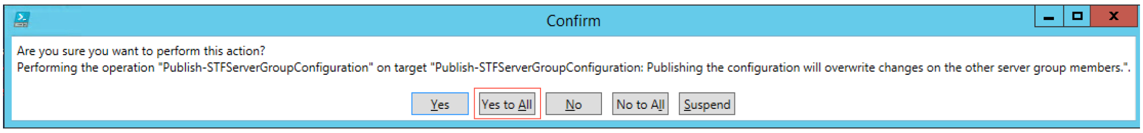
The PowerShell script is available on the **Connect StoreFront Deployment** page inside a zip file along with the StoreFrontConfiguration.json file, a few CCAuth, and dll files. The PowerShell script logs are saved in the cas-logs file under the **Downloads** folder.

The PowerShell script supports the following parameters:

- **SelfCheck**: The **SelfCheck** parameter is used to validate that the prerequisites for StoreFront onboarding have been met. It performs a check for StoreFront installation, required version, outbound connection, cURL Analytics server network connectivity, internet connectivity, server group configuration, and any existing Citrix Analytics Service configuration. Use the following command to run the **selfcheck**:

  ```
  .\Manage-CitrixAnalytics.ps1 –param SelfCheck
  ```

- **OnboardStorefront**: The **OnboardStoreFront** parameter quickly performs a self-check to verify setup readiness for Citrix Analytics Service configuration. If the setup is ready, it imports the Citrix Analytics Service configuration, and publishes the changes to other servers in the server group. For a server group, the PublishConfiguration command automatically runs from the script to publish the StoreFront configuration to all the servers within that StoreFront. You can see a pop-up to confirm `PublishConfiguration` action. Select the **Yes to All** button.



Are you sure you want to perform this action?
Performing the operation "Publish-STFServerGroupConfiguration" on target "Publish-STFServerGroupConfiguration: Publishing the configuration will overwrite changes on the other server group members.".

Once the configuration publishing is successfully completed, the script makes a call to Citrix Analytics Service API to check if the StoreFront is onboarded to the Citrix Analytics Service GUI. To invoke this API, a private key is required for authentication. To generate this private key, you need the CCAuth and dll files, and the credential that is available in your downloaded JSON file.

> **Note**
>
> Once the StoreFront onboarding process is complete, it might take two to five minutes for the StoreFront to appear in the Citrix Analytics Service GUI. If the StoreFront site does not appear in the Citrix Analytics Service GUI, you must perform an IISRESET to reset the internet information services.

Use the following command to run the **OnboardStoreFront**:

```
.\Manage-CitrixAnalytics.ps1 -param OnboardStorefront
```

- **IsOnboarded**: The **IsOnboarded** parameter is used to verify if the StoreFront is onboarded to Citrix Analytics Service GUI. The script waits for a minute before exiting, however, the StoreFront can take up to five minutes to appear in the GUI after successful onboarding. You must run this command to verify it. This command also has the CCAuth and dll files dependency. Use the following command to run the **IsOnboarded**:

  ```
  .\Manage-CitrixAnalytics.ps1 -param IsOnboarded
  ```

- **Troubleshoot**: After waiting for five minutes, if the StoreFront site does not appear in the Citrix Analytics Service GUI, you must perform an IISRESET to reset the internet information services. If the StoreFront site still does not appear in the GUI, use the **Troubleshoot** parameter. It helps you to troubleshoot any connectivity issues and collect logs. Use the following command to run the **Troubleshoot**:

  ```
  .\Manage-CitrixAnalytics.ps1 -param TroubleShoot
  ```

  The troubleshooting parameter is useful for the following two use cases:

  - **Use case 1**: As a part of self-check if the curlAnalytics failed, then a firewall rule gets created. This firewall rule opens a 443 port and verifies its connectivity to Analytics. If not, that means the Analytics server is not reachable and the script exits from here. Rerun the script once the connectivity to Citrix Analytics Service is restored.

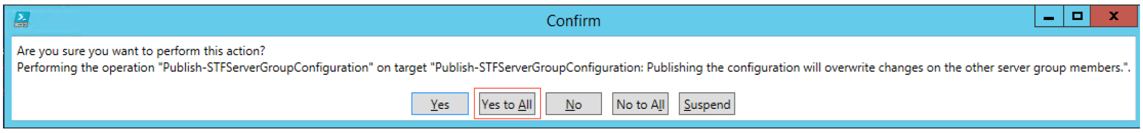
  - **Use case 2**: If the cURL went through fine and yet the StoreFront site is not getting reflected in the GUI, then the administrator must download the DebugView tool zip file from Download DebugView, unzip, and place it under the **Downloads** folder. The PowerShell script first uninstalls Citrix Analytics Service if it is already configured. It enables Verbose logging. Then, it starts the DebugView tool and reinstalls Citrix Analytics Service. Finally, it stops DebugView and disables Verbose logging.

The debug view logs can be captured and shared with Citrix Support. The Citrix administrator further debugs and tries to find out the issue and resolve it. The logs are generated and saved as a log file inside the DebugView folder.

You need to share the following three log files with the Citrix administrator:

- The DebugView log file (Downloads\DebugView\log)
- The StoreFront log file (C:\Program Files\Citrix\Receiver StoreFront\Admin\trace)
- The CAS logs file. These logs are generated as a part of the execution of the script and get saved under the **Downloads > cas-logs** folder.

For a server group, the `PublishConfiguration` command automatically runs when the script is trying to deboard or onboard StoreFront. The PublishConfiguration command helps to publish the StoreFront configuration to all the servers within that StoreFront. You can see a pop-up to confirm this action. Select the **Yes to All** button.



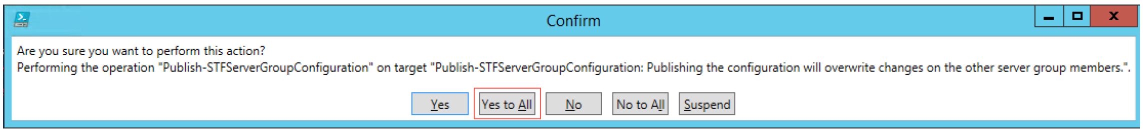
Are you sure you want to perform this action?
Performing the operation "Publish-STFServerGroupConfiguration" on target "Publish-STFServerGroupConfiguration: Publishing the configuration will overwrite changes on the other server group members.".

- **DeboardStoreFront**: The DeboardStoreFront parameter is used for deboarding the StoreFront server from Citrix Analytics Service. Use the following command to run the DeboardStoreFront:

```
.\Manage-CitrixAnalytics.ps1 -param DeboardStoreFront
```

The PowerShell script first removes all Citrix Analytics Service configurations from StoreFront and verify that the removal is successful. Then, it checks if the ServerGroup is present then publish the configuration so that the removed configurations are published to all the StoreFront. Finally, it invokes DeleteSiteOnboarded. If the site is not deleted from Citrix Analytics Service GUI then you need to manually delete the StoreFront site with StoreFront Deployment and from the Workspace Application site card under the StoreFront Deployment.

For a server group, the PublishConfiguration command automatically runs from the script to publish the StoreFront configuration to all the servers within that StoreFront. You can see a pop-up to confirm this action. Select the **Yes to All** button.

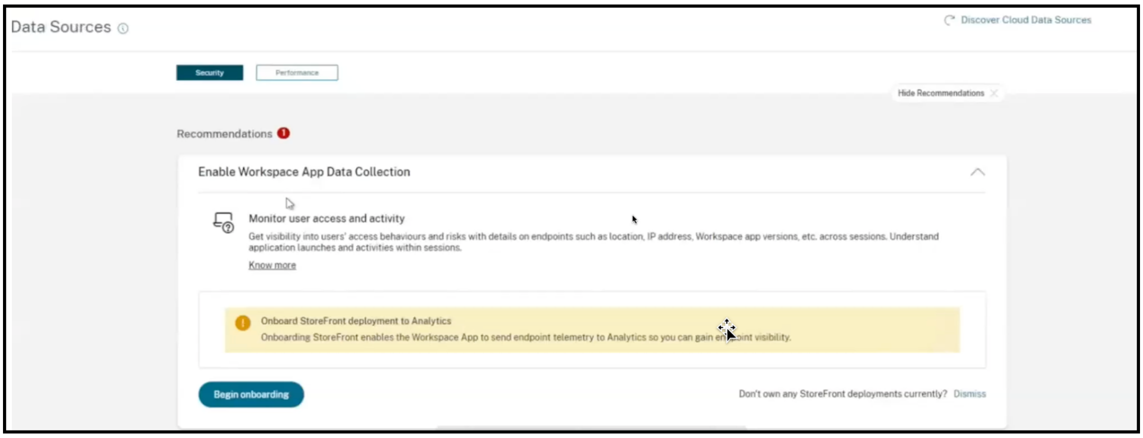


Are you sure you want to perform this action?
Performing the operation "Publish-STFServerGroupConfiguration" on target "Publish-STFServerGroupConfiguration: Publishing the configuration will overwrite changes on the other server group members.".

Connect using Recommendations panel

The **Recommendations** panel on the **Data Sources** page educates the user on the importance of onboarding data sources. It helps the user onboard the data sources easily and also provides an option to the user to review and ensure that he has onboarded all the available data sources.

1. If you are using the Security Analytics offering, select **Settings > Data Sources > Security**.
2. If you are using the Performance Analytics offering, navigate to **Settings > Data Sources > Performance**.
3. On the **Data Sources** page, review the information and recommendations on the **Recommendations** panel to onboard Storefront deployment.



Monitor user access and activity

Get visibility into users' access behaviours and risks with details on endpoints such as location, IP address, Workspace app versions, etc. across sessions. Understand application launches and activities within sessions.

Know more

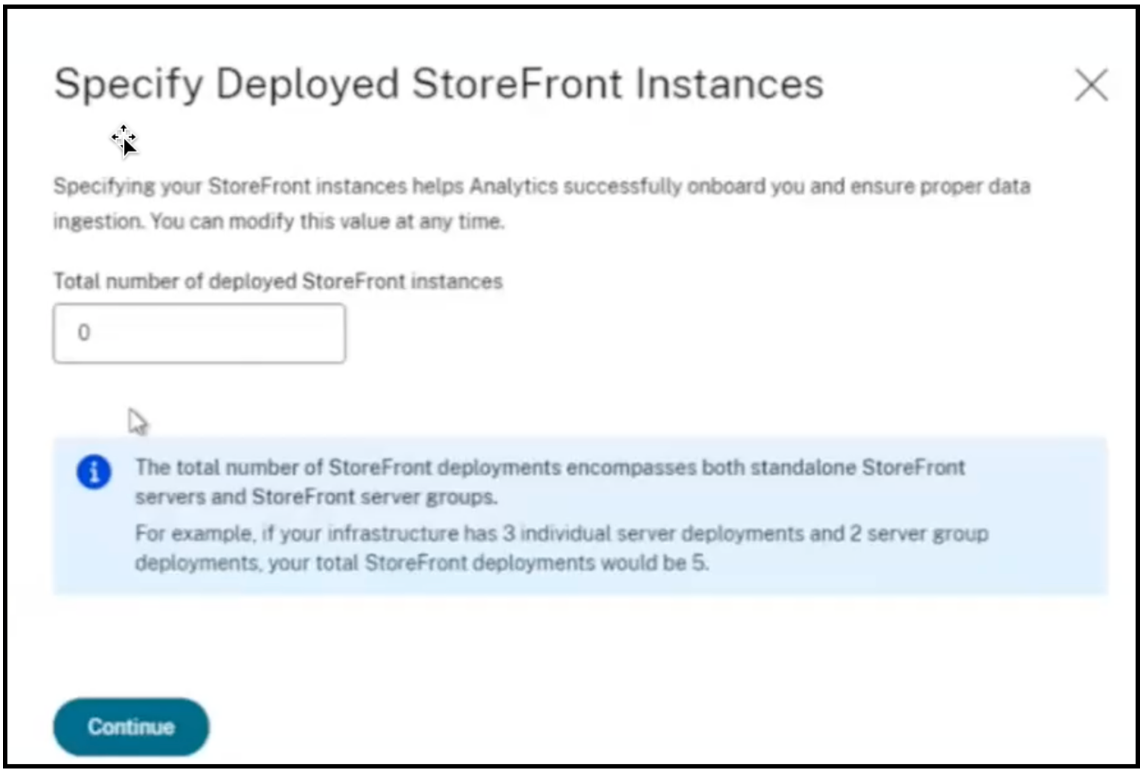
Onboard StoreFront deployment to Analytics

Onboarding StoreFront enables the Workspace App to send endpoint telemetry to Analytics so you can gain endpoint visibility.

Don't own any StoreFront deployments currently?

> **Note**
>
> Onboarding a StoreFront data source enables the Workspace app to send telemetry data on endpoint visibility to Analytics.

4. Click **Begin onboarding**. The **Specify Deployed Storefront Instances** page appears.



Specify Deployed StoreFront Instances

Specifying your StoreFront instances helps Analytics successfully onboard you and ensure proper data ingestion. You can modify this value at any time.

Total number of deployed StoreFront instances: 0

The total number of StoreFront deployments encompasses both standalone StoreFront servers and StoreFront server groups.

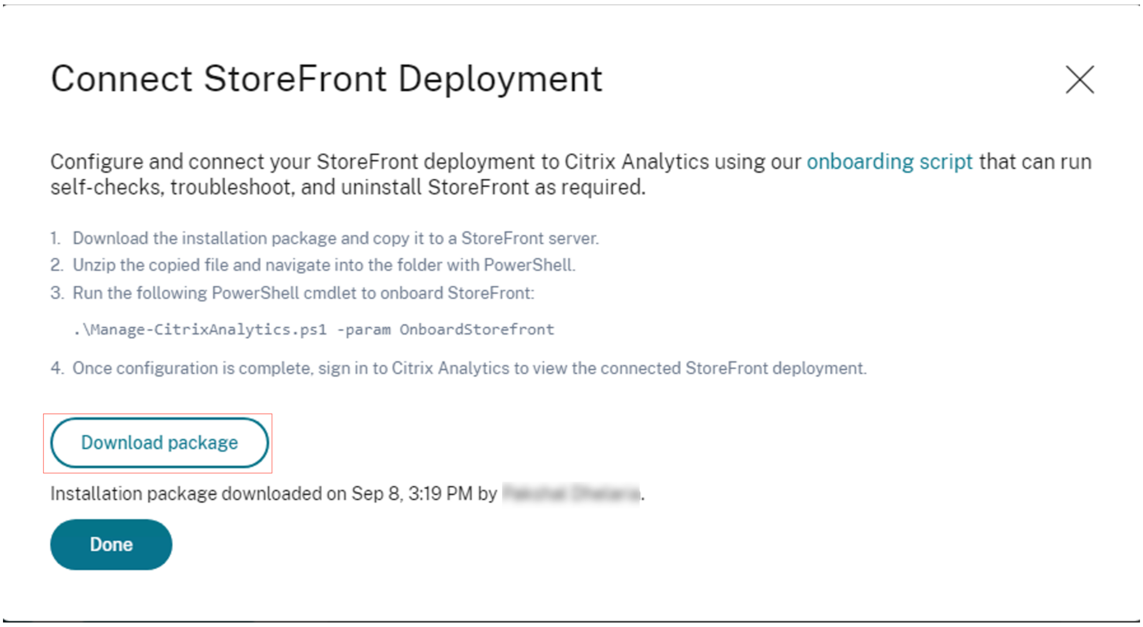
For example, if your infrastructure has 3 individual server deployments and 2 server group deployments, your total StoreFront deployments would be 5.

5. To ensure that Analytics successfully onboards the data source, specify the **Total number of deployed StoreFront instances**.

   > **Note:**
   >
   > The **Total number of deployed StoreFront instances** is the total number of StoreFront groups and it isn't the number of individual StoreFront servers.

6. Click **Continue**. The StoreFront Onboarding wizard or the **Connect StoreFront Deployment** popup appears.

7. On the **Connect StoreFront Deployment** page, click Download package to download the installation package.



Connect StoreFront Deployment

Configure and connect your StoreFront deployment to Citrix Analytics using our onboarding script that can run self-checks, troubleshoot, and uninstall StoreFront as required.

1. Download the installation package and copy it to a StoreFront server.
2. Unzip the copied file and navigate into the folder with PowerShell.
3. Run the following PowerShell cmdlet to onboard StoreFront:

```
.\Manage-CitrixAnalytics.ps1 -param OnboardStorefront
```

4. Once configuration is complete, sign in to Citrix Analytics to view the connected StoreFront deployment.

Installation package downloaded on Sep 8, 3:19 PM by [redacted].

> **Notes**
>
> The file contains sensitive information. Keep the file in a safe and secure location.
>
> You can download one package and use it to onboard one StoreFront group only. If you have multiple StoreFront groups, you must download the package separately for each StoreFront group. After one StoreFront group onboarding is finished using one package, download the package again and continue onboarding for the next StoreFront group.
>
> If the StoreFront onboarding isn't completed correctly within two days using one package due to some issue, you must re-download a new package after two days. Because the key within the package will be expired if not onboarded successfully within two days.

8. To configure the StoreFront deployment,

   a) Copy the installation package to the StoreFront server.

   b) Unzip the copied file and navigate into the folder within PowerShell.

   c) Run the following command to onboard the StoreFront:

   ```
   .\Manage-CitrixAnalytics.ps1 –param OnboardStorefront
   ```

   d) Open the StoreFront server and execute the PowerShell script.

   e) If the StoreFront site does not appear in the Citrix Analytics Service GUI, run the following command:

   ```
   Execute iisreset
   ```

   f) Log and verify the Cluster ID that is available in the PowerShell script.

  g) Once the configuration is done, log in to Citrix Analytics to view the connected StoreFront Deployment.

9. After the configuration is successful, click **Done**.

If you are onboarding through the **Recommendations** panel, the system fetches the number of StoreFront deployments that you have onboarded to Citrix Analytics service. The **Recommendations** panel appears and you can review the onboarded StoreFront deployments. You can review the message in the **Recommendations** panel and click **Mark as complete**.

> **Note**
>
> The **Recommendations** panel and the messages disappear only when all the declared Storefront deployments are onboarded.

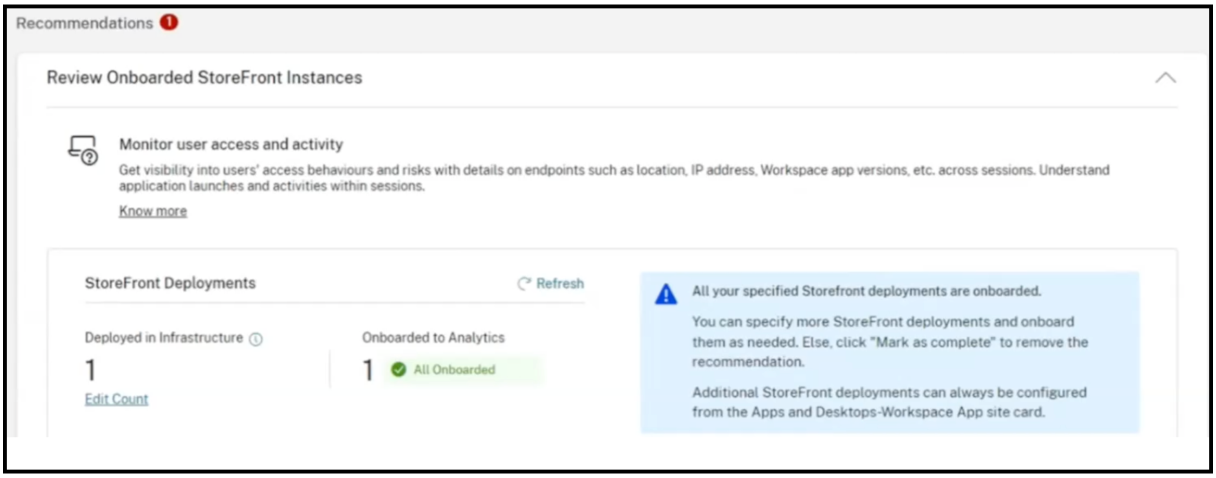
1. Click **Turn On Data Processing** to allow Citrix Analytics to process the data.

Review the Recommendations panel

You can compare the number of StoreFront deployments declared against the number of StoreFront deployments onboarded in the **Recommendations** panel.

If the number of StoreFront deployments declared is the same as the number of StoreFront deployments onboarded, a **All Onboarded** message appears indicating that all the StoreFront deployments are onboarded. You can review the message in the **Recommendations** panel and click **Mark as complete**.

> **Note**
>
> If you want to onboard more StoreFront deployments, click **View onboarding steps** and the StoreFront Onboarding wizard or the **Connect StoreFront Deployment** popup appears again.



Get visibility into users' access behaviours and risks with details on endpoints such as location, IP address, Workspace app versions, etc. across sessions. Understand application launches and activities within sessions.

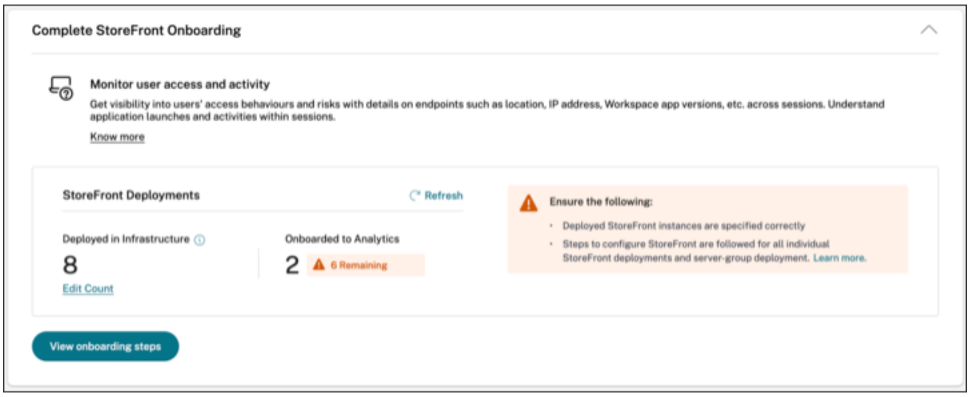
All your specified Storefront deployments are onboarded.

You can specify more StoreFront deployments and onboard them as needed. Else, click "Mark as complete" to remove the recommendation.

Additional StoreFront deployments can always be configured from the Apps and Desktops-Workspace App site card.

If the number of StoreFront deployments declared is less than the number of StoreFront deployments onboarded, click **Edit Count**, and the **Specify Deployed Storefront Instances** page appears. You can then enter the **Total number of deployed StoreFront instances**, and click **Continue**. The StoreFront Onboarding wizard or the **Connect StoreFront Deployment** popup appears again. Follow the steps to onboard more StoreFront deployments.

> **Note:**
>
> The **Total number of deployed StoreFront instances** is the total number of StoreFront groups and it isn't the number of individual StoreFront servers.



Complete StoreFront Onboarding

Monitor user access and activity

Get visibility into users' access behaviours and risks with details on endpoints such as location, IP address, Workspace app versions, etc. across sessions. Understand application launches and activities within sessions.

Know more

StoreFront Deployments

Refresh

Deployed in Infrastructure: 8

Edit Count

Onboarded to Analytics: 2 — 6 Remaining

Ensure the following:

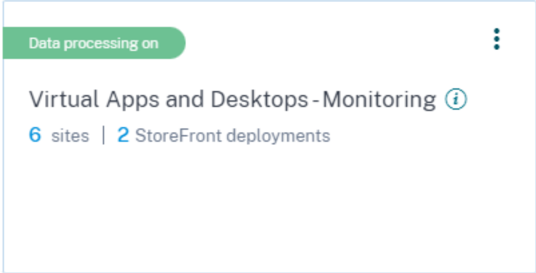
- Deployed StoreFront instances are specified correctly
- Steps to configure StoreFront are followed for all individual StoreFront deployments and server-group deployment. Learn more.

View onboarding steps

View connected StoreFront deployments

The StoreFront deployments appear on the site card only if the configuration is successful. The site card shows how many StoreFront deployments have established connections with Citrix Analytics.

- If you are using the Performance Analytics offering, you see the following information on the **Apps and Desktops- Monitoring** site card:

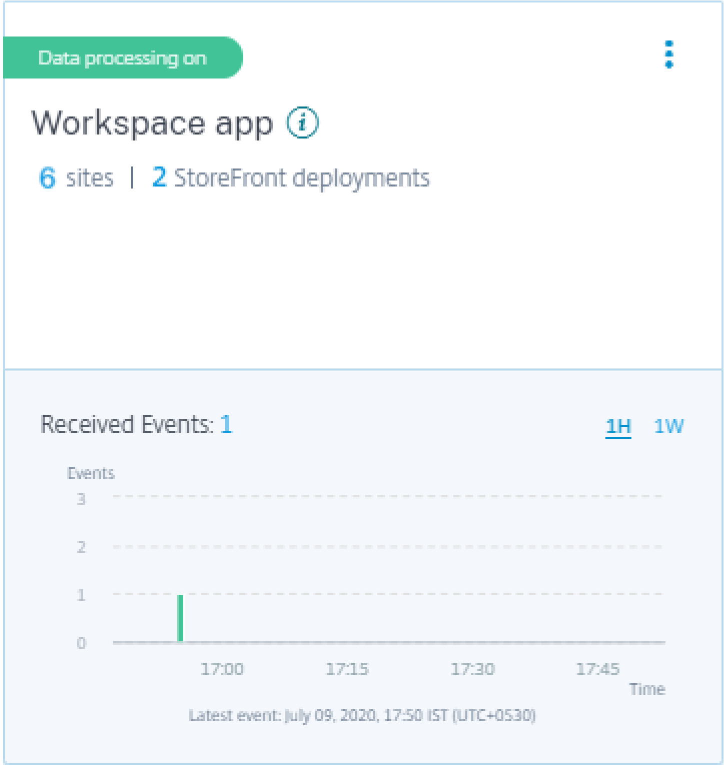


Data processing on

Virtual Apps and Desktops - Monitoring

6 sites | 2 StoreFront deployments

- If you are using the Security Analytics offering, you see the following information on the **Workspace app** site card:



Data processing on

Workspace app

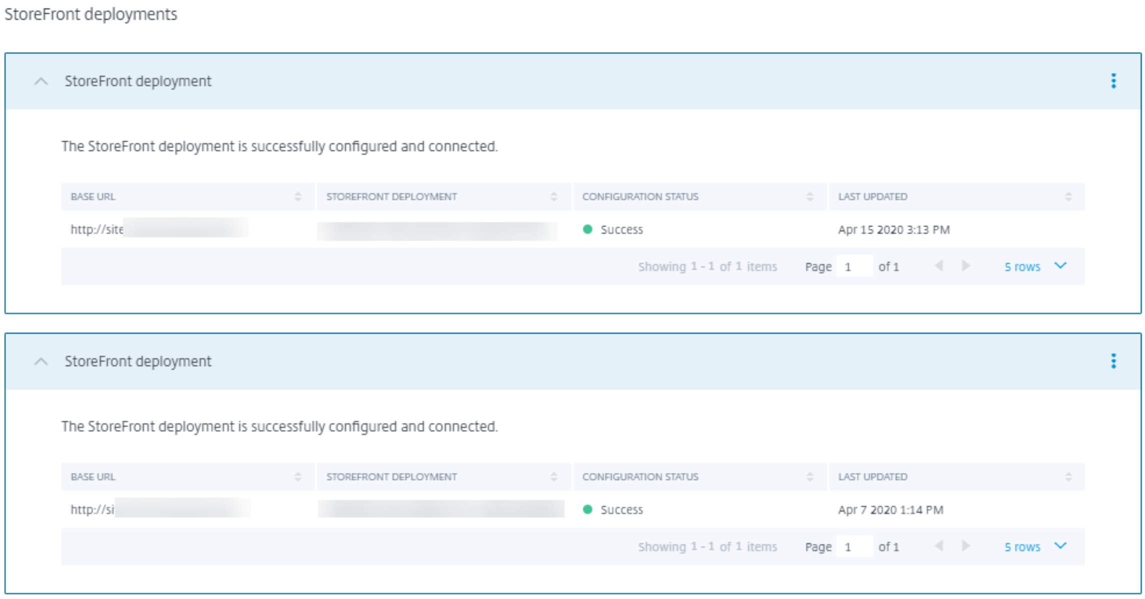
6 sites | 2 StoreFront deployments

Received Events: 1

Latest event: July 09, 2020, 17:50 IST (UTC+0530)

Click the number of StoreFront deployments on the site card to view the server groups.

Each StoreFront deployment is represented by a base URL and a ServerGroupID.



StoreFront deployments

StoreFront deployment

The StoreFront deployment is successfully configured and connected.

BASE URL	STOREFRONT DEPLOYMENT	CONFIGURATION STATUS	LAST UPDATED
http://site [redacted]	[redacted]	● Success	Apr 15 2020 3:13 PM

Showing 1 - 1 of 1 items Page 1 of 1 5 rows

StoreFront deployment

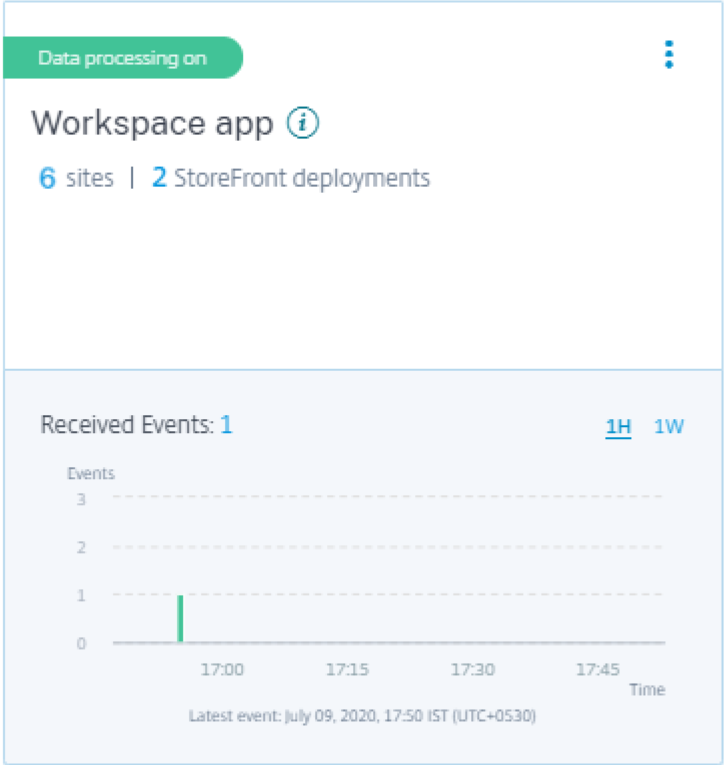
The StoreFront deployment is successfully configured and connected.

BASE URL	STOREFRONT DEPLOYMENT	CONFIGURATION STATUS	LAST UPDATED
http://si [redacted]	[redacted]	● Success	Apr 7 2020 1:14 PM

Showing 1 - 1 of 1 items Page 1 of 1 5 rows

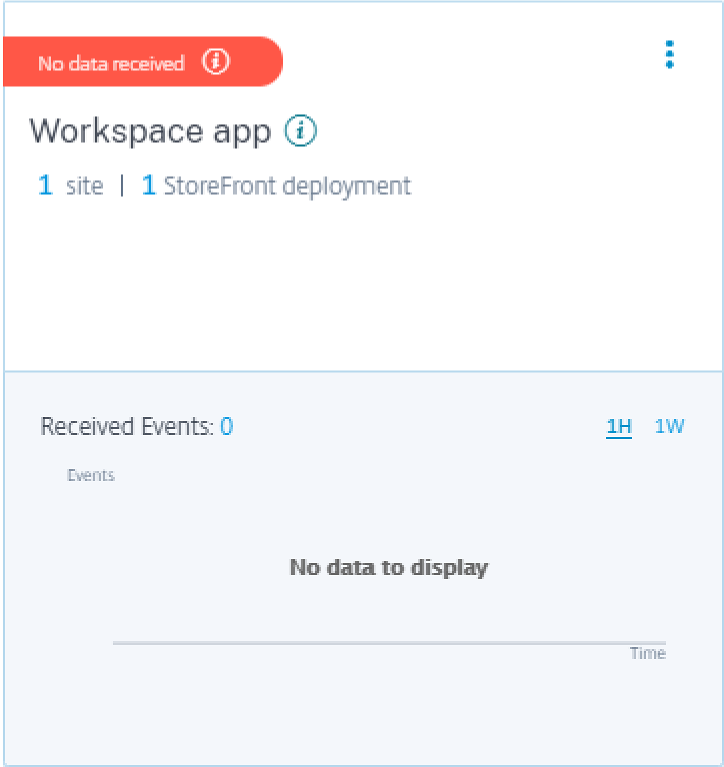
If you are using the Security Analytics offering, the site card also displays the following information about the received events:

- The events received from the StoreFront deployments for the last one hour, which is the default time selection. You can also select 1 week (1 W) and view the data. Click the number of received events to view the events on the self-service search page.



- After you have enabled data processing, the site card might display the **No data received** status. This status appears for two reasons:

  1. If you have turned on data processing for the first time, the events take some time to reach the event hub in Citrix Analytics. When Citrix Analytics receives the events, the status changes to **Data processing on**. If the status does not change after some time, refresh the **Data Sources** page.
  2. Citrix Analytics has not received any events from the data source in the last one hour.



No data received

Workspace app

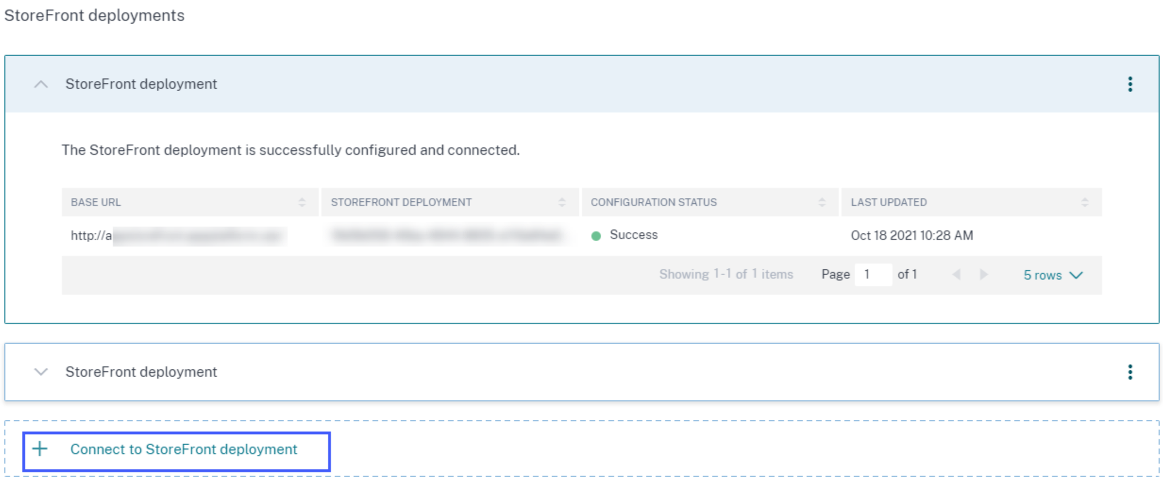
1 site | 1 StoreFront deployment

Received Events: 0

No data to display

Add or remove StoreFront deployments

To add a StoreFront deployment, click **Connect to StoreFront Deployments** on the **StoreFront deployments** section. Download the configuration file and follow the steps to configure a StoreFront deployment.



StoreFront deployments

StoreFront deployment

The StoreFront deployment is successfully configured and connected.

BASE URL	STOREFRONT DEPLOYMENT	CONFIGURATION STATUS	LAST UPDATED
http://a[redacted]	[redacted]	● Success	Oct 18 2021 10:28 AM

Showing 1-1 of 1 items   Page 1 of 1   5 rows

StoreFront deployment

To stop the event transmission from a configured StoreFront deployment and remove it from Citrix Analytics:

1. Go to the StoreFront deployment that you want to remove from Citrix Analytics. Run the following command to remove the configuration settings from your StoreFront server:

   ```
   Remove-STFCasConfiguration
   ```

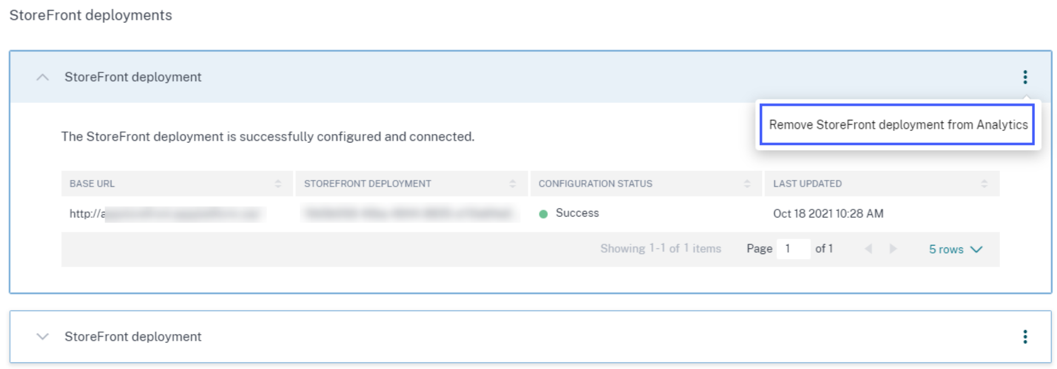
2. If you are using multiserver deployment, run the following command to propagate the changes and remove the configuration settings from all the servers in the StoreFront server group:

   ```
   Publish-STFServerGroupConfiguration
   ```

3. Run the following command to verify that the configuration settings have been successfully removed. The command returns nothing if the settings have been successfully removed.

   ```
   Get-STFCasConfiguration
   ```

4. Log back to Citrix Analytics and choose the StoreFront deployment on the **StoreFront deployments** section. Click the vertical ellipsis (⊠) and select **Remove StoreFront deployments from Analytics**.

   StoreFront deployments

   StoreFront deployment

   The StoreFront deployment is successfully configured and connected.

BASE URL	STOREFRONT DEPLOYMENT	CONFIGURATION STATUS	LAST UPDATED
http://a[redacted]	[redacted]	● Success	Oct 18 2021 10:28 AM

   Showing 1-1 of 1 items Page 1 of 1 5 rows

   StoreFront deployment

   > **Note**
   >
   > Run the specified commands on the StoreFront deployment before removing it from Citrix Analytics. If you fail to run the commands, Citrix Analytics continues to receive the events and the StoreFront deployment is added again at the next event pooling cycle.

Configure a StoreFront deployment hosted on a webserver that uses HTTP proxy

If a StoreFront is hosted on a webserver that uses a web proxy to connect to the Internet, the store must be manually configured to register with Citrix Analytics. This configuration requires you to add a `<system.net>` section to the store web.config file. You must configure every store on the StoreFront deployment that sends events to Citrix Analytics.

There are two methods by which you can add the `<system.net>` section to the store web.config file:

- Set the store proxy configuration via PowerShell for one or more stores (recommended method).
- Manually add a `<system.net>` section to the store web.config file.

For more information on these methods, see the Configure StoreFront to use a web proxy to contact Citrix Cloud and register with Citrix Analytics article in the StoreFront documentation.

Data Governance

November 30, 2023

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

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

Data residency

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

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

Data collection

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

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

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

Data transmission

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

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

Data control

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

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

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

Data retention

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

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

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

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

Data export

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

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

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

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

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

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

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

Currently, you can integrate with the following SIEM services:

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

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

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

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

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

Citrix Services Security Exhibit

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

Definitions

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

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

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

Data collection agreement

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

Citrix always treats the received information according to the Citrix Privacy Policy.

Appendix: logs collected

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

Citrix Analytics for Security logs

General logs

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 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 Secure Private Access logs

- AAA User Name
- Auth Policy Action Name
- Authentication Session ID
- Request URL
- URL Category Policy Name
- VPN Session ID
- Vserver IP
- AAA User Email ID
- Actual Template Code
- App FQDN
- App Name
- App Name Vserver LS
- Application Flags
- Authentication Type
- Authentication Stage
- Authentication Status Code
- Back-end Server Dst IPv4 Address
- Back-end Server IPv4 Address
- Back-end Server IPv6 Address
- Category Domain Name
- Category Domain Source
- Client IP
- Client MSS
- Client Fast Retx Count
- Client TCP Jitter
- Client TCP Packets Retransmited
- Client TCP RTO Count
- Client TCP Zero Window Count

- Clt Flow Flags Rx
- Clt Flow Flags Tx
- Clt TCP Flags Rx
- Clt TCP Flags Tx
- Connection Chain Hop Count
- Connection Chain ID
- Egress Interface
- Exporting Process ID
- Flow Flags Rx
- Flow Flags Tx
- HTTP Content Type
- HTTP Domain Name
- HTTP Req Authorization
- HTTP Req Cookie
- HTTP Req Forw FB
- HTTP Req Forw LB
- HTTP Req Host
- HTTP Req Method
- HTTP Req Rcv FB
- HTTP Req Rcv LB
- HTTP Req Referer
- HTTP Req URL
- HTTP Req XForwarded For
- HTTP Res Forw FB
- HTTP Res Forw LB
- HTTP Res Location
- HTTP Res Rcv FB
- HTTP Res Rcv LB
- HTTP Res Set Cookie

- HTTP Rsp Len
- HTTP Rsp Status
- HTTP Transaction End Time
- HTTP Transaction ID
- IC Cont Grp Name
- IC Flags
- IC No Store Flags
- IC Policy Name
- Ingress Interface Client
- NetScaler Gateway Service App ID
- NetScaler Gateway Service App Name
- NetScaler Gateway Service App Type
- NetScaler Partition ID
- Observation Domain ID
- Observation Point ID
- Origin Res Status
- Origin Rsp Len
- Protocol Identifier
- Rate Limit Identifier Name
- Record Type
- Responder Action Type
- Response Media Type
- Srv Flow Flags Rx
- Srv Flow Flags Tx
- Srvr Fast Retx Count
- Srvr TCP Jitter
- Srvr TCP Packets Retransmitted
- Srvr TCP Rto Count
- Srvr TCP Zero Window Count

- SSL Cipher Value BE
- SSL Cipher Value FE
- SSL Client Cert Size BE
- SSL Client Cert Size FE
- SSL Clnt Cert Sig Hash BE
- SSL Clnt Cert Sig Hash FE
- SSL Err App Name
- SSL Err Flag
- SSL FLags BE
- SSL FLags FE
- SSL Handshake Error Msg
- SSL Server Cert Size BE
- SSL Server Cert Size FE
- SSL Session ID BE
- SSL Session ID FE
- SSL Sig Hash Alg BE
- SSL Sig Hash Alg FE
- SSL Srvr Cert Sig Hash BE
- SSL Srvr Cert Sig Hash FE
- SSL iDomain Category
- SSL iDomain Category Group
- SSL iDomain Name
- SSL iDomain Reputation
- SSL iExecuted Action
- SSL iPolicy Action
- SSL iReason For Action
- SSL iURL Set Matched
- SSL iURL Set Private
- Subscriber Identifier

- Svr Tcp Flags Rx
- Svr Tcp Flags Tx
- Tenant Name
- Tracing Req Parent Span ID
- Tracing Req Span ID
- Tracing Trace ID
- Trans Clt Dst IPv4 Address
- Trans Clt Dst IPv6 Address
- Trans Clt Dst Port
- Trans Clt Flow End Usec Rx
- Trans Clt Flow End Usec Tx
- Trans Clt Flow Start Usec Rx
- Trans Clt Flow Start Usec Tx
- Trans Clt IPv4 Address
- Trans Clt IPv6 Address
- Trans Clt Packet Tot Cnt Rx
- Trans Clt Packet Tot Cnt Tx
- Trans Clt RTT
- Trans Clt Src Port
- Trans Clt Tot Rx Oct Cnt
- Trans Clt Tot Tx Oct Cnt
- Trans Info
- Trans Srv Dst Port
- Trans Srv Packet Tot Cnt Rx
- Trans Srv Packet Tot Cnt Tx
- Trans Srv Src Port
- Trans Svr Flow End Usec Rx
- Trans Svr Flow End Usec Tx
- Trans Svr Flow Start Usec Rx

- Trans Svr Flow Start Usec Tx
- Trans Svr RTT
- Trans Svr Tot Rx Oct Cnt
- Trans Svr Tot Tx Oct Cnt
- Transaction ID
- URL Category
- URL Category Group
- URL Category Reputation
- URL Category Action Reason
- URL Set Matched
- URL set Private
- URL Object ID
- VLAN Number

Citrix Virtual Apps and Desktops and Citrix DaaS logs

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

- App Name
- Browser
- Customer ID
- Details: Format Size, Format Type, Initiator, Result
- Device ID
- Device Type
- Feedback
- Feedbak ID
- File Name
- File Path
- File Size
- Is like
- Jail Broken

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

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

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

Citrix ADC logs

The Citrix ADC logs contain the following data points:

- Container

- Files
- Format
- Type

Citrix DaaS Standard for Azure logs

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

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

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

- Long CMD Line
- Module File Path
- Operation
- Operating System
- Platform Extra Information
- Printer Name
- SaaS App Name
- Session Domain
- Session Server Name

- Session User Name
- Session GUID
- Timestamp
- Time Zone: Bias, DST, Name
- Type
- URL
- User Agent

Citrix Identity provider logs

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

Citrix Gateway logs

- Transaction events:
  - ICA App: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx, ICA Flags, Connection Id, Padding Octets Two, ICA Device Serial Number, IP Version 4, Protocol Identifier, Source IPv4 Address Rx, Destination IPv4 Address Rx, Source Transport Port Rx, Destination Transport Port Rx, ICA Application Start up Duration, ICA Launch Mechanism, ICA Application Start up Time, ICA Process ID Launch, ICA Application Name, ICA App Module Path, ICA Application Termination Type, ICA Application Termination Time, Application Name App Id, ICA App Process ID Terminate, ICA App
  - ICA Event: Record Type, Actual Template Code, Source IPv4 Address Rx, Destination IPv4 Address Rx, ICA Session Guid, MSI Client Cookie, Connection Chain ID, ICA Client Version, ICA Client Host Name, ICA User Name, ICA Domain Name, Logon Ticket Setup, Server Name, Server Version, Flow Id Rx, ICA Flags, Observation Point Id, Exporting Process Id, Observation Domain Id, Connection Id, ICA Device Serial Number, ICA Session Setup Time, ICA Client IP, NS ICA Session Status Setup, Source Transport Port Rx, Destination Transport Port Rx, ICA Client Launcher, ICA Client Type, ICA Connection Priority Setup, NS ICA Session Server Port, NS ICA Session Server IP Address, IPv4, Protocol Identifier,Connection Chain Hop Count, Access Type
  - ICA Update: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx,ICA Flags, Connection Id, ICA Device Serial Number, IPv4, Protocol Identifier, Padding Octets Two, ICA RTT, Client Side RX Bytes, Client Side Packets Retransmit, Server Side Packets Retransmit, Client Side RTT, Client Side Jitter, Server Side Jitter, ICA Network Update Start Time, ICA Network Update End Time, Client Side SRTT, Server Side SRTT,Client Side Delay, Server Side Delay, Host Delay, Client Side Zero Window Count, Server Side Zero Window Count, Client Side RTO Count, Server Side RTO Count, L7 Client Latency, L7 Server Latency, App Name App Id, Tenant Name, ICA Session Update Begin Sec, ICA Session Update End Sec, ICA Channel Id 1, ICA Channel Id 2, ICA Channel Id 2 Bytes, ICA Channel Id 3, ICA Channel Id 3 Bytes, ICA Channel Id 4, ICA Channel Id 4 Bytes, ICA Channel Id 5, ICA Channel Id 5 Bytes
  - AppFlow Config: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, System Rule Flag 1, System Safety Index, AppFlow Profile Relaxed Flags, AppFlow Profile Block Flags, AppFlow Profile Log Flags, AppFlow Profile Learn Flags, AppFlow Profile Stats Flags, AppFlow Profile None Flags, AppFlow App Name Id, AppFlow Profile Sign Disabled, AppFlow Profile Sign Block Count, AppFlow Profile Sign Log Count, AppFlow Profile Sign Stat Count, AppFlow Incarnation Number,AppFlow Se-

quence Number, AppFlow Profile Sign Auto Update, AppFlow Safety Index, AppFlow App Safety Index, AppFlow Profile Sec Checks Safety Index, AppFlow Profile Type, Iprep App Safety Index, AppFlow Profile Name, AppFlow Sig Name, AppFlow App Name Ls, AppFlow Sig Rule ID1, AppFlow Sig Rule ID2, AppFlow Sig Rule ID3, AppFlow Sig Rule ID4, AppFlow Sig Rule ID5, AppFlow Sig Rule Enabled Flags, AppFlow Sig Rule Block Flags, AppFlow Sig Rule Log Flags, AppFlow Sig Rule File Name, AppFlow Sig Rule Category1, AppFlow Sig Rule Logstring1, AppFlow Sig Rule Category2, AppFlow Sig Rule Logstring2, AppFlow Sig Rule Category3, AppFlow Sig Rule Category4, AppFlow Sig Rule Logstring4, AppFlow Sig Rule Category5, AppFlow Sig Rule LogString5

- AppFlow: Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, Transaction Id, Appfw Violation Occurred Time, App Name App Id, Appfw Violation Severity, Appfw Violation Type, Appfw Violation Location, Appfw Violation Threat Index, Appfw NS Longitude, Appfw NS Latitude, Source IPv4 Address Rx, Appfw Http Method, Appfw App Threat Index, Appfw Block Flags, Appfw Transform Flags, Appfw Violation Profile Name, Appfw Session Id, Appfw Req Url, Appfw Geo Location, Appfw Violation Type Name 1, Appfw Violation Name Value 1, Appfw Sig Category 1, Appfw Violation Type Name 2, Appfw Violation Name Value 2, Appfw Sig Category 2, Appfw Violation Type Name 3, Appfw Violation Name Value 3, Appfw Sig Category3, Appfw Req X Forwarded For, Appfw App Name Ls,App Name Ls, Iprep Category, Iprep Attack Time, Iprep Reputation Score, Iprep NS Longitude, Iprep NS Latitude, Iprep Severity, Iprep HTTP Method, Iprep App Threat Index, Iprep Geo Location, Tcp Syn Attack Cntr, Tcp Slow Ris Cntr, Tcp Zero Window Cntr, Appfw Log Expr Name, Appfw Log Expr Value, Appfw Log Expr Comment
- VPN: Actual Template Code, Observation Domain Id, Access Insight Flags, Observation Point Id, Exporting Process Id, Access Insight Status Code, Access Insight Timestamp, Authentication Duration, Device Type, Device ID, Device Location, App Name App Id, App Name App Id1, Source Transport Port Rx, Destination Transport Port Rx, Authentication Stage, Authentication Type, VPN Session ID, EPA Id, AAA User Name, Policy Name, Auth Agent Name, Group Name, Virtual Server FQDN, cSec Expression, Source IPv4 Address Rx, Destination IPv4 Address Rx, Cur Factor Policy Label, Next Factor Policy Label, App Name Ls, App Name 1 Ls,AAA User Email Id, Gateway IP, Gateway Port, Application Byte Count, VPN Session State, VPN Session Mode, SSO Auth Method, IIP Address, VPN Request URL, SSO Request URL, Backend Server Name, VPN Session Logout Mode, Logon Ticket File Info, STA Ticket, Session Sharing Key, Resource Name, SNIP Address, Temp VPN Session ID
- HTTP: Actual Template Code, Http Req Method, Http Req Url, Http Req User Agent, Http Content Type, Http Req Host, Http Req Authorization, Http Req Cookie, Http Req Referer, Http Res Set Cookie, Ic Cont Grp Name, Ic Flags, Ic Nostore Flags, Ic Policy Name, Response Media Type, Ingress Interface Client, Origin Res Status, Origin Rsp Len, Srv Flow Flags Rx, Srv Flow Flags Tx, Flow Flags Rx, Flow Flags Tx, App Name, Observation Point Id, Exporting

Process Id, Observation Domain Id, Http Trans End Time, Transaction Id, Http Rsp Status, Trans Clt Ipv4 Address, Trans Clt Dst Ipv4 Address, Backend Svr Dst Ipv4 Address, Backend Svr Ipv4 Address, Http Rsp Len, Trans Svr RTT, Trans Clt RTT, Http Req Rcv FB, Http Req Rcv LB, Http Res Rcv FB, Http Res Rcv LB, Http Req Forw FB, Http Req Forw LB, Http Res Forw FB, Http Res Forw LB, Http Req X Forwarded For, Http Domain Name, Http Res Location, Protocol Identifier, Egress Interface, Backend Svr Ipv6 Address, SSL Flags BE, SSL Flags FE, SSL Session IDFE, SSL Session IDBE, SSL Cipher Value FE, SSL Cipher Value BE, SSL Sig Hash Alg BE, SSL Sig Hash Alg FE, SSL Srvr Cert Sig Hash BE, SSL Srvr Cert Sig Hash FE, SSL Clnt Cert Sig Hash FE, SSL Clnt Cert Sig Hash BE, SSL Server Cert Size FE, SSL Server Cert Size BE, SSL Client Cert Size FE, SSL Client Cert Size BE, SSL Err App Name, SSL Err Flag, SSL Handshake Error Msg, Client IP, Virtual Server IP, Connection Chain Id, Connection Chain Hop Count, Trans Clt Tot Rx Oct Cnt, Trans Clt TotTx Oct Cnt, Trans Clt Src Port, Trans Clt Dst Port, Trans Srv Src Port, Trans Srv Dst Port, VLAN Number, Client Mss, Trans Info, Trans Clt Flow End Usec Rx, Trans Clt Flow End Usec Tx, Trans Clt Flow Start Usec Rx, Trans Clt Flow Start Usec Tx, Trans Svr Flow End Usec Rx, Trans Svr Flow End Usec Tx, Trans Svr Flow Start Usec Rx, Trans Svr Flow Start Usec Tx, Trans Svr Tot Rx Oct Cnt, Trans Svr Tot Tx Oct Cnt, Clt Flow Flags Tx, Clt Flow Flags Rx, Trans Clt Ipv6 Address, Trans Clt Dst Ipv6 Address, Subscriber Identifier, SSLi Domain Name, SSLi Domain Category, SSLi Domain Category Group, SSLi Domain Reputation, SSLi Policy Action, SSLi Executed Action, SSLi Reason For Action, SSLi URL Set Matched, SSLi URL Set Private, URL Category, URL Category Group, URL Category Reputation, Responder Action Type, URL Set Matched, URL Set Private, Category Domain Name, Category Domain Source, AAA User Name, VPN Session ID, Tenant Name

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

- Server Service Group: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, Cc CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Service Group: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot_Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions,Si Tot Svr Tlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions
- Server SVC CFG: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Svc Cfg: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Svr Busy Err, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Cur Transport, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rcvd, Si Tot Pkt Sent, Si Tot Svr Busy Err, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions, Si Tot Svr Ttlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions
- NetScaler: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, GSLB Server, GSLB VServer, Interface, Memory Pool, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, NetScaler: RATE All Nic Tot Rx Mbits, RATE All Nic Tot Rx Mbits, RATE Dns Tot Queries, RATE Dns Tot Neg Nxdmn Entries,RATE Http Tot Gets, RATE Http Tot Others, RATE Http Tot Posts, RATE Http Tot Requests, RATE Http Tot Requests 1.0, RATE Http Tot Requests 1.1, RATE Http Tot Responses, RATE Http Tot Rx Request Bytes, RATE Http Tot Rx Response Bytes, RATE Ip Tot Rx Mbits, RATE Ip Tot Rx Bytes, RATE Ip Tot Rx Pkts, RATE Ip Tot Tx Mbits, RATE Ip Tot Tx Bytes, RATE Ip Tot Tx Pkts, RATE SSL Tot Dec Bytes, RATE SSL Tot Enc Bytes,RATE SSL Tot SSL Info Session Hits, RATE SSL Tot SSL Info Total Tx Count, RATE Tcp Err Rst, RATE Tcp Tot Client Open, RATE Tcp Tot Server Open, RATE Tcp Tot Rx Bytes, RATE Tcp Tot Rx Pkts, RATE Tcp Tot Syn, RATE Tcp Tot Tx Bytes, RATE Tcp Tot Tx Pkts, RATE Udp Tot Rx Bytes, RATE Udp Tot Rx Pkts, RATE Udp Tot Tx Bytes, RATE Udp Tot Tx Pkts, All Nic Tot Rx Mbits, All Nic Tot Tx Mbits, Cpu Use, Dns Tot Queries, Dns Tot Neg Nxdmn Entries, Http Tot Gets, Http Tot Others, Http Tot Posts, Http Tot Requests, Http Tot Requests1.0, Http Tot Requests1.1, Http Tot Responses, Http Tot Rx Request Bytes, Http

Tot Rx Response Bytes, Ip Tot Rx Mbits, Ip Tot Rx Bytes, Ip Tot Rx Pkts, Ip Tot Tx Mbits, Ip Tot Tx Bytes, Ip Tot Tx Pkts, Mem Cur Free size, Mem Cur Free size Actual, Mem Cur Used size, Mem Tot Available, Mgmt Additional Cpu Use, Mgmt Cpu 0 Use, Mgmt Cpu Use, SSL Tot Dec Bytes, SSL Tot Enc Bytes, SSL Tot SSL Info Session Hits, SSL Tot SSL Info Total Tx Count, Sys Cpus, Tcp Cur Client Conn, Tcp Cur Client Conn Closing, Tcp Cur Client Conn Est, Tcp Cur Server Conn, Tcp Cur Server Conn Closing, Tcp Cur Server Conn Est, Tcp Err Rst, Tcp Tot Client Open, Tcp Tot Server Open, Tcp Tot Rx Bytes, Tcp Tot Rx Pkts, Tcp Tot Syn, Tcp Tot Tx Bytes, Tcp Tot Tx Pkts, Udp Tot Rx Bytes, Udp Tot Rx Pkts, Udp Tot Tx Bytes, Udp Tot Tx Pkts

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

Secure Browser logs

- Application Post:

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

- Application Delete:
  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL
- Application Update:
  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL
- Entitlement Create:
  - Logs before the entitlement creation: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type

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

- Entitlement Update:
    - Logs before the entitlement update: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
    - Logs after the entitlement update: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
- Session Access Host: Accept Host, Client IP, Date Time, Host, Session, User Name
- Session Connect:
    - Logs before the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
    - Logs after the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- Session Launch:
    - Logs before the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
    - Logs after the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- Session Tick:
    - Logs before the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
    - Logs after the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name

Microsoft Graph Security logs

- Tenant Id
- User Id
- Indicator Id

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

Microsoft Active Directory logs

- Tenant Id
- Collect Time
- Type
- 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
- Street Address
- Title
- User Account Control
- User Group List

- User Principal Name
- Work Phone

Citrix Analytics for Performance logs

- actionid
- actionreason
- actiontype
- adminfolder
- agentversion
- allocationtype
- applicationid
- applicationname
- applicationpath
- applicationtype
- applicationversion
- associateduserfullnames
- associatedusername
- associatedusernames
- associateduserupns
- authenticationduration
- autoreconnectcount
- autoreconnecttype
- AvgEndpointThroughputBytesReceived
- AvgEndpointThroughputBytesSent
- blobcontainer
- blobendpoint
- blobpath
- brokerapplicationchanged
- brokerapplicationcreated

- brokerapplicationdeleted
- brokeringdate
- brokeringduration
- brokerloadindex
- brokerregistrationstarted
- browsername
- catalogchangeevent
- catalogcreatedevent
- catalogdeletedevent
- catalogid
- catalogname
- catalogsync
- clientaddress
- clientname
- clientplatform
- clientsessionvalidatedate
- clientversion
- collecteddate
- connectedviahostname
- connectedviaipaddress
- connectionid
- connectioninfo
- connectionstate
- connectiontype
- controllerdnsname
- cpu
- cpuindex
- createddate
- currentloadindexid

- currentpowerstate
- currentregistrationstate
- currentsessioncount
- datetime
- deliverygroupadded
- deliverygroupchanged
- deliverygroupdeleted
- deliverygroupid
- deliverygroupmaintenancemodechanged
- deliverygroupname
- deliverygroupsync
- deliverytype
- deregistrationreason
- desktopgroupdeletedevent
- desktopgroupid
- desktopgroupname
- desktopkind
- disconnectcode
- disconnectreason
- disk
- diskindex
- dnsname
- domainname
- effectiveloadindex
- enddate
- errormessage
- establishmentdate
- eventreporteddate
- eventtime

- exitcode
- failurecategory
- failurecode
- failuredata
- failuredate
- failurereason
- failuretype
- faultstate
- functionallevel
- gpoenddate
- gpostartdate
- hdxenddate
- hdxstartdate
- host
- hostedmachineid
- hostedmachinename
- hostingservername
- hypervisorconnectionchangedevent
- hypervisorconnectioncreatedevent
- hypervisorid
- hypervisorname
- hypervisorsync
- icartt
- icarttms
- id
- idletime
- inputbandwidthavailable
- inputbandwidthused
- instancecount

- interactiveenddate
- interactivestartdate
- ipaddress
- isassigned
- isinmaintenancemode
- ismachinephysical
- ispendingupdate
- ispreparing
- isremotepc
- issecureica
- lastderegisteredcode
- launchedviahostname
- launchedviaipaddress
- lifecyclestate
- LinkSpeed
- logonduration
- logonenddate
- logonscriptsenddate
- logonscriptsstartdate
- logonstartdate
- long
- machineaddedtodesktopgroupevent
- machineassignedchanged
- machinecatalogchangedevent
- machinecreatedevent
- machinedeletedevent
- machinederegistrationevent
- machinednsname
- machinefaultstatechangeevent

- machinehardregistrationevent
- machineid
- machinemaintenancemodechangeevent
- machinename
- machinepvdstatechanged
- machineregistrationendedevent
- machineremovedfromdesktopgroupevent
- machinerole
- machinesid
- machineupdatedevent
- machinewindowsconnectionsettingchanged
- memory
- memoryindex
- modifieddate
- NGSConnector.ICAConnection.Start
- NGSConnector.NGSSyntheticMetrics
- NGSConnector.NGSPassiveMetrics
- NGSConnector.NGSSystemMetrics
- network
- networkindex
- networklatency
- networkinfoperiodic
- NetworkInterfaceType
- ostype
- outputbandwidthavailable
- outputbandwidthused
- path
- percentcpu
- persistentuserchanges

- powerstate
- processname
- profileloadenddate
- profileloadstartdate
- protocol
- provisioningschemeid
- provisioningtype
- publishedname
- registrationstate
- serversessionvalidatedate
- sessioncount
- sessionend
- sessionfailure
- sessionid
- sessionidlesince
- sessionindex
- sessionkey
- sessionstart
- sessionstate
- sessionsupport
- sessiontermination
- sessiontype
- sid
- SignalStrength
- siteid
- sitename
- startdate
- totalmemory
- triggerinterval

- triggerlevel
- triggerperiod
- triggervalue
- usedmemory
- userid
- userinputdelay
- username
- usersid
- vdalogonduration
- vdaprocessdata
- vdaresourcedata
- version
- vmstartenddate
- vmstartstartdate
- windowsconnectionsetting
- xd.SessionStart

Technical security overview

April 8, 2024

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 extra configuration to integrate with Citrix Analytics. For example, you have to add your Citrix Virtual Apps and Desktops sites to Citrix Workspace before Citrix Analytics can discover the Sites. Similarly, on-premises Citrix Gateway requires you to configure a Citrix ADM agent. For more information on enabling Citrix 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 Citrix 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 a customer-owned Splunk environment. This integration requires deploying and configuring **Citrix Analytics Add-on for Spunk** 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 Citrix Analytics. In addition to the Citrix Cloud requirements, the following endpoint addresses must be accessible through the HTTPS port 443 to use the Citrix Analytics service.

Endpoint	United States region	European Union region	Asia Pacific South region
Admin UI	`https://analytics.cloud.com/`	`https://analytics-eu.cloud.com/`	`https://analytics-aps.cloud.com/`
Admin UI (CDN)	`https://cas-api-cdn-ep.azureedge.net/`	`https://cas-api-cdn-ep-eu.azureedge.net/`	`https://cas-api-cdn-ep-aps.azureedge.net/`
API Services	`https://api.analytics.cloud.com/`	`https://api.analytics-eu.cloud.com/`	`https://api.analytics-aps.cloud.com/`

Endpoint	United States region	European Union region	Asia Pacific South region
API Services (Performance Analytics)	https://api-a.was.cloud.com/	https://api-eu-a.was.cloud.com/	https://api-ap-s-a.was.cloud.com/
	https://api-b.was.cloud.com/	https://api-eu-b.was.cloud.com/	https://api-ap-s-b.was.cloud.com/
Get Public IP	https://locus.analytics.cloud.com/	https://locus.analytics.cloud.com/	https://locus.analytics.cloud.com/
Event Hub (Not applicable for Citrix ADM agent)	https://citrixanalyticseh-alias.servicebus.windows.net/	https://citrixanalyticseheu-alias.servicebus.windows.net/	https://citrixanalyticsehaps-alias.servicebus.windows.net/
	https://citrixanalyticseh2-alias.servicebus.windows.net/		
Event Hub (For Citrix ADM agent)	https://cas-eh-ns-alias.servicebus.windows.net/ and https://cas-eh-ns2-alias.servicebus.windows.net/	https://cas-eh-ns-eu-alias.servicebus.windows.net/	https://cas-eh-ns-aps-alias.servicebus.windows.net/
Bulk Upload	https://casstoragebulk.blob.core.windows.net/	https://casstorebulkeu.blob.core.windows.net/	https://casstorebulkaps.blob.core.windows.net/

> **Note**

> Citrix Analytics has discontinued the support for TLS 1.0 and TLS 1.1 for most of the preceding 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 endpoints for SIEM integration**: To integrate Citrix Analytics with your Security Information and Event Management (SIEM), ensure that the following endpoints are in the allow list in your network:

Endpoint	United States region	European Union region	Asia Pacific South region

Kafka brokers	`casnb-0.citrix.com:9094`
	`casnb-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`
		`casnb-eu-0.citrix.com:9094`
		`casnb-eu-1.citrix.com:9094`
		`casnb-eu-2.citrix.com:9094`
			`casnb-aps-0.citrix.com:9094`
			`casnb-aps-1.citrix.com:9094`
			`casnb-aps-2.citrix.com:9094`

Identity and access management

- To access Citrix 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 Manage administrator roles.

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, the European Union, and the Asia Pacific South 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. The received data is processed only if 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 micro services 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.
- 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 the 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 owned and managed by customers:
  - **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.
- Customer-provided administrator credentials for deploying and integrating the agents such as Citrix ADM agents. 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 documentation

- Technical security overview for Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)
- Security considerations for Citrix Virtual Apps and Desktops
- Secure your StoreFront deployment documentation
- Technical security overview for Citrix Endpoint Management
- Citrix Secure Private Access service documentation
- Secure deployment guide for Citrix ADC
- Citrix ADM system requirements

System Requirements

August 1, 2023

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

Citrix Analytics subscriptions

You must have valid subscriptions to use the following Analytics products:

- Citrix Analytics for Security
- Citrix Analytics for Performance

For more information, see Citrix Cloud services.

Data sources requirements

The data sources are the products that send events to Citrix Analytics. Based on the Citrix Analytics offerings that you are using, the 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 Performance

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
- Latest version of Apple Safari

Manage administrator roles for Citrix Analytics

March 30, 2023

By default, a Citrix Cloud administrator has full access permissions to all the subscribed services on their Citrix Cloud account. With the full access permissions, the administrator can use all the features and functionalities of a subscribed service.

As a Citrix Cloud administrator with full access, you can invite other administrators to your Citrix Cloud account for managing the subscribed services of your organization. You can then define their access permissions and allow them to manage specific features in the subscribed services.

New administrators can be added in two ways:

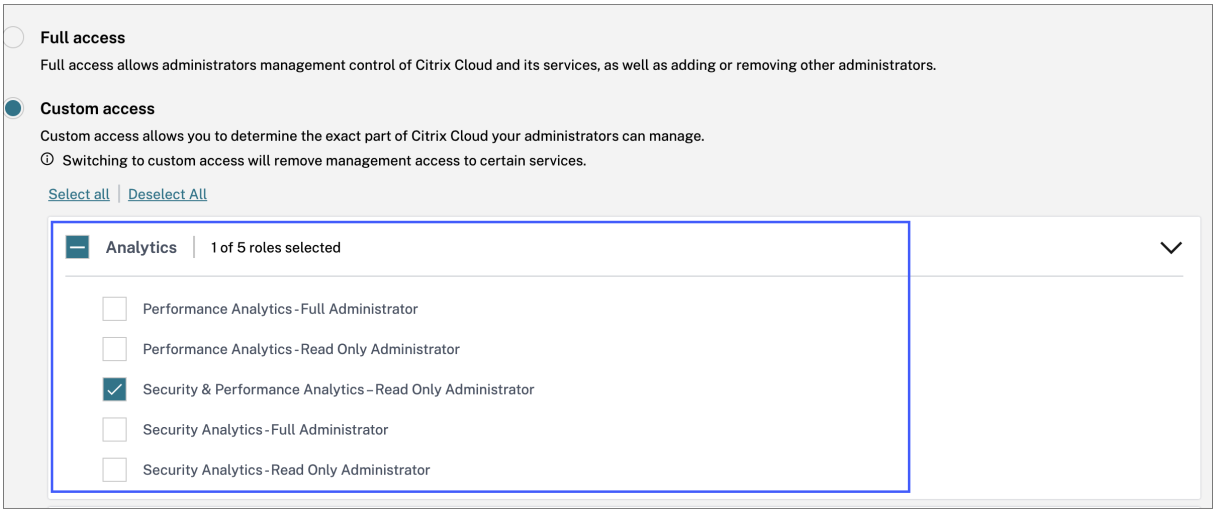
1. Individually as users from Citrix Identity and Azure AD/Active Directory. For more information, see Manage Citrix Cloud administrators.
2. Using groups in Azure Active Directory. For more information, see Manage administrator groups.

Administrators can log in to Citrix Cloud using their Citrix Cloud, Active Directory, or Azure Active Directory accounts, and access specific features and perform tasks depending on their roles.

For Citrix Analytics, you can assign the following custom roles to your administrators:

Role	Permission
Performance Analytics - Full Administrator	Assigns full access permission to the Citrix Cloud administrators of Performance Analytics.
Performance Analytics - Read Only Administrator	Assigns read-only access permission to the Citrix Cloud administrators of Performance Analytics.

Role	Permission
Security & Performance Analytics - Read Only Administrator	Assigns read-only access permissions to the Citrix Cloud administrators of both Security Analytics and Performance Analytics.
Security Analytics - Full Administrator	Assigns full access permission to the Citrix Cloud administrators of Security Analytics.
Security Analytics- Read Only Administrator	Assigns read-only access permission to the Citrix Cloud administrators of Security Analytics.



○ **Full access**
Full access allows administrators management control of Citrix Cloud and its services, as well as adding or removing other administrators.

● **Custom access**
Custom access allows you to determine the exact part of Citrix Cloud your administrators can manage.
ⓘ Switching to custom access will remove management access to certain services.

Analytics | 1 of 5 roles selected

- □ Performance Analytics - Full Administrator
- □ Performance Analytics - Read Only Administrator
- ☑ Security & Performance Analytics – Read Only Administrator
- □ Security Analytics - Full Administrator
- □ Security Analytics - Read Only Administrator

> ### Notes
>
> - If you select multiple roles for an administrator, the role with higher access takes effect.
> - If a user is granted access directly as a user and through an Azure Active Directory Group, the access granted individually to the user takes effect.
> - Azure Active Directory groups can only be added as Custom administrators. Full Access Administrator role is not available for groups.
> - The administrators with the **Read Only Administrator** role that was available earlier is renamed to **Security & Performance - Read Only Administrator**.
> - The administrators with the **Security & Performance Analytics - Read Only Administrator** role and the **Performance Analytics - Read Only Administrator** role do not receive any email notifications from Citrix Analytics.

For more information about the offering specific roles, see the following articles:

- Manage administrator roles for Performance Analytics

- Manage administrator roles for Security Analytics

Getting started

February 16, 2024

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** 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.

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

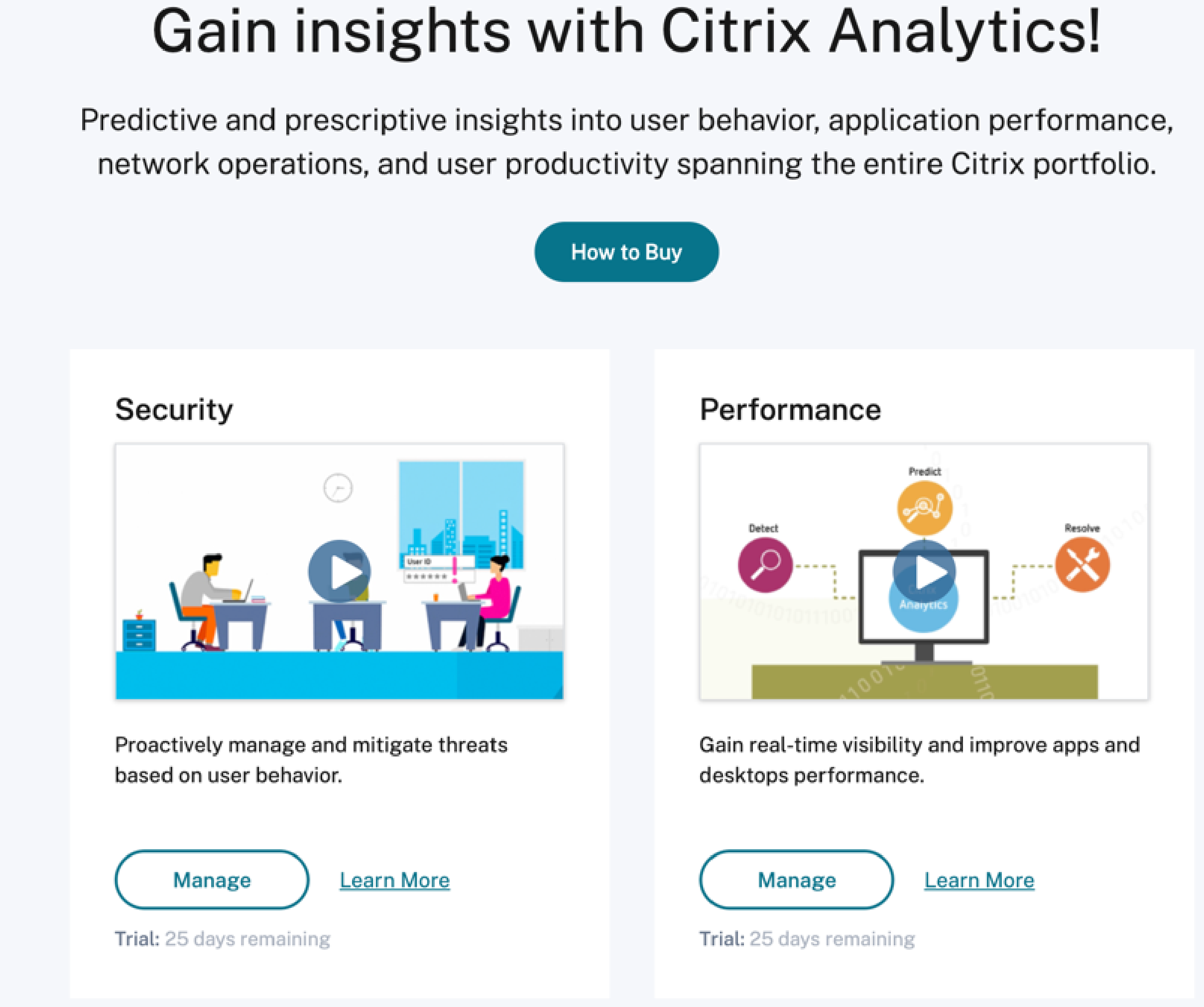
- **Subscribe to Citrix Analytics**. You can purchase the following Citrix Analytics subscriptions:

  - 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.

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.



Gain insights with Citrix Analytics!

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

How to Buy

Security

Proactively manage and mitigate threats based on user behavior.

Manage Learn More

Trial: 25 days remaining

Performance

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

Manage Learn More

Trial: 25 days remaining

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** and click the required tab- **Security** or **Performance**.

For more information on each Analytics offering, see

- Citrix Analytics for Security
- Citrix Analytics for Performance

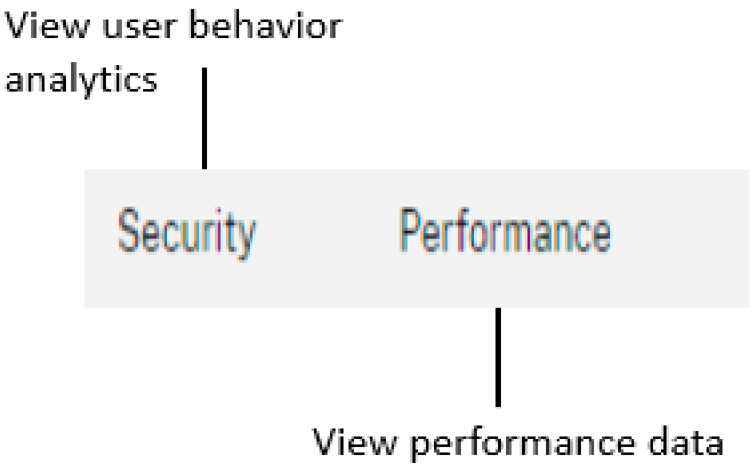
Find your way around

December 2, 2021

Familiarize yourself with the main controls on the Analytics user interface.

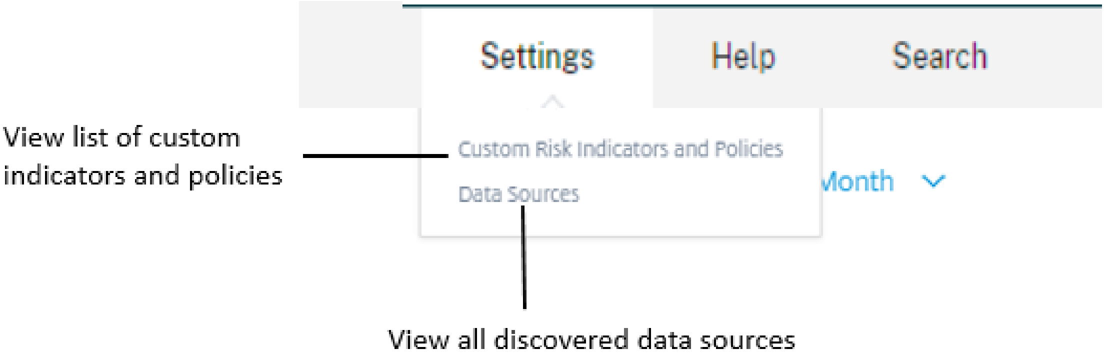
Top bar

Navigate to the various Analytics offerings from the top bar.

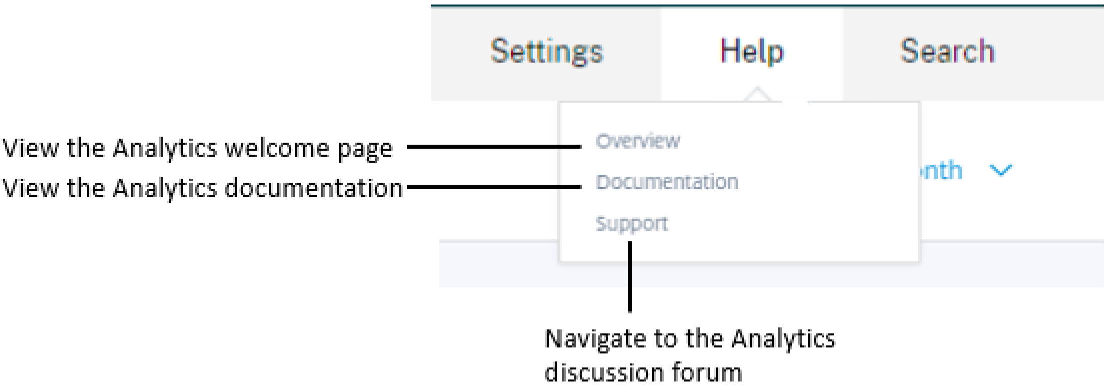


Settings menu

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

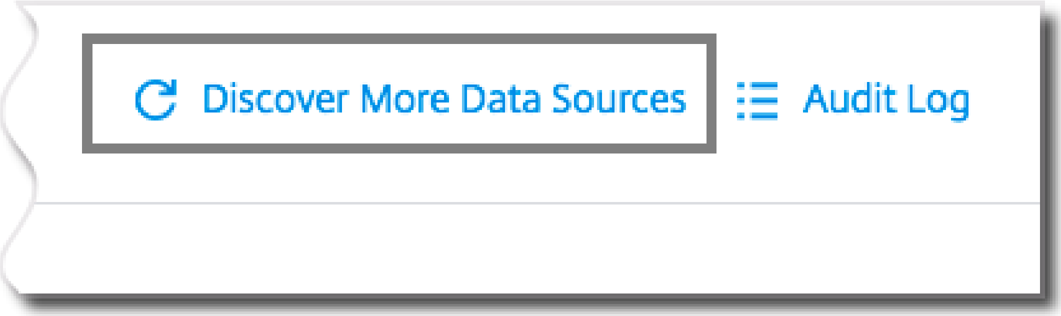

Settings
Help
Search
Custom Risk Indicators and Policies
Data Sources
Month
View list of custom indicators and policies
View all discovered data sources

Help menu


Settings
Help
Search
Overview
Documentation
Support
nth
View the Analytics welcome page
View the Analytics documentation
Navigate to the Analytics discussion forum

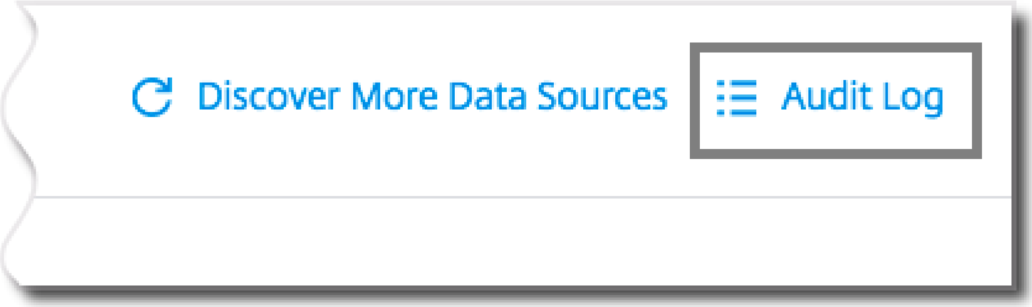
Discover more data sources

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

November 30, 2023

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 their 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 day.

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

- Authentication
- Gateway
- Secure Browser
- Secure Private Access
- Apps and Desktops
- Performance Users, Machines, 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

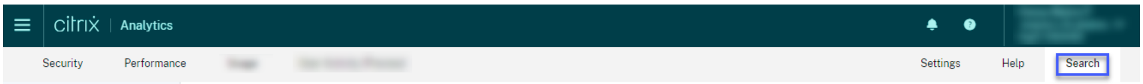
You can access the self-service search by using the following options:

- **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.

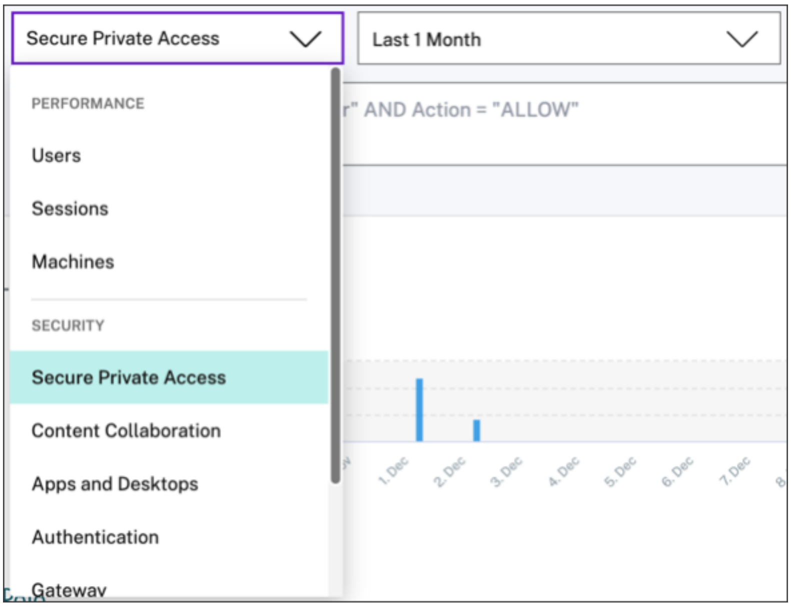
Self-service search from the top bar

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.



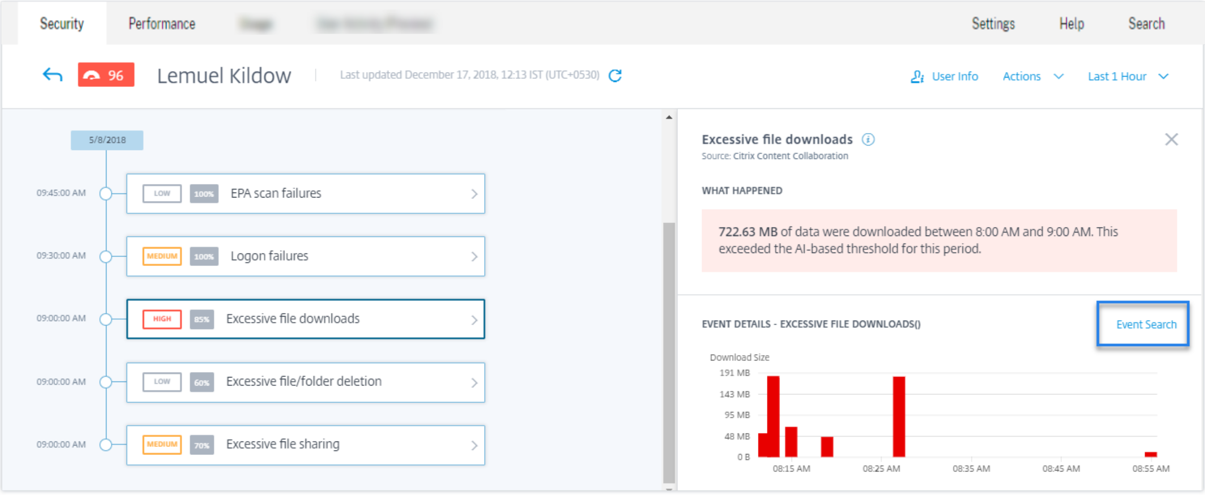
2. Select the data source and the time period to view the corresponding events.



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.



722.63 MB of data were downloaded between 8:00 AM and 9:00 AM. This exceeded the AI-based threshold for this period.

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.
- Export visual summary to download the visual summary report of your search query.
- Multicolumn sorting to sort the events by multiple columns.

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 Secure Private Access data source are reputation, actions, location, and category group. Whereas the facets for Apps and Desktops are event type, domain, and platform.

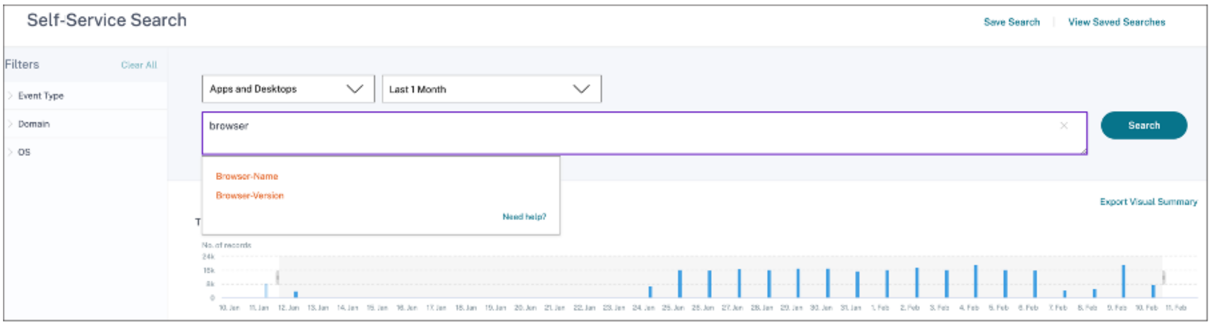
Select the facets to filter your search results. The selected facets are displayed as chips.

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 user events. These dimensions vary according to the data source. Use the dimensions and the valid operators to define your search criteria and search for the required events.

For example, in the self-service search for Apps and Desktops, you get the following values for the dimension `Browser`. Use the dimension to type your query, select the time period, and then click **Search**.

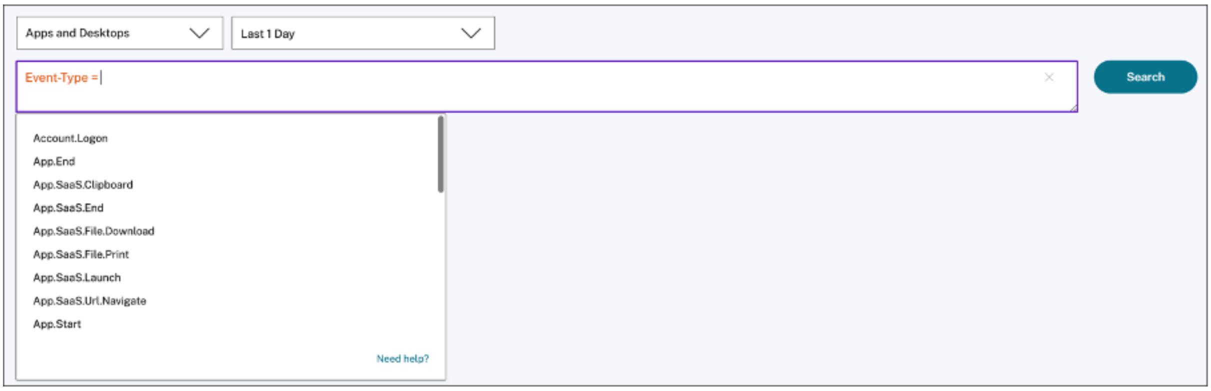


Apps and Desktops

Last 1 Month

browser

When selecting certain dimensions like `Event-Type` and `Clipboard-Operation` along with a valid operator, the values of the dimension are shown automatically. You can choose a value from the suggested options or enter a new value depending on your requirements.



Supported operators in search query Use the following operators in your search queries to refine your search results.

Operator	Description	Example	Output
	Assign a value to a search dimension.	User-Name : John	Displays events for the user John.
=	Assign a value to a search dimension.	User-Name = John	Displays events for the user John.
~	Search events with similar values.	User-Name ~ test	Displays events having similar user names.
""	Enclose values separated by spaces.	User-Name = "John Smith"	Displays events for the user John Smith.
< >	Search for relational value.	Data Volume > 100	Displays events where data volume is greater than 100 GB.
AND	Search events where the specified conditions are true.	User-Name : John AND Data Volume > 100	Displays events of user John where data volume is greater than 100 GB.

Operator	Description	Example	Output
`!~`	Checks events for the matching pattern that you specify. This NOT LIKE operator returns the events that do not contain the matching pattern anywhere in the event string.	User-Name !~ John	Displays events for the users except John, John Smith, or any such users that contain the matching name “John”.
`!=`	Checks events for the exact string that you specify. This NOT EQUAL operator returns the events that do not contain the exact string anywhere in the event string.	Country != USA	Displays events for the countries except USA.
`*`	Search events that match the specified strings. Currently, the `*` operator is supported only with the following operators `:`, =, and `!=`. The search results are case-sensitive.	User-Name = John*	Displays events for all user names that begin with John.
		User-Name = *John*	Displays events for all user names that contain John.
		User-Name = *Smith	Displays events for all user names that end with Smith.
		User-Name : John*	Displays events for all user names that begin with John.
		User-Name : *John*	Displays events for all user names that contain John.

Operator	Description	Example	Output
		User-Name : *Smith	Displays events for all user names that end with Smith.
		User-Name != John*	Displays events for all user names that do not begin with John.
		User-Name != *Smith	Displays events for all user names that do not end with Smith.
`IN`	Assign multiple values to a search dimension to get the events related to one or more values. **Note**: Currently, you can use this operator with the following dimensions of Apps and Desktops- `Device ID`, `Domain`, `Event-Type`, and `User-Name`. This operator is applicable only for the string values.	User-Name IN (John, Kevin)	Find all events related to John or Kevin.

Operator	Description	Example	Output
`NOT IN`	Assign multiple values to a search dimension and find the events that do not contain the specified values. **Note**: Currently, you can use this operator with the following dimensions of Apps and Desktops- `Device ID`, `Domain`, `Event-Type`, and `User-Name`. This operator is applicable only for the string values.	User-Name NOT IN (John, Kevin)	Find the events for all users except John and Kevin.
`IS EMPTY`	Checks for null value or empty value for a dimension. This operator works for only string type dimensions such as `App-Name`, `Browser`, and `Country`. It does not work for non-string (number) type dimensions such as `Upload-File-Size`, `Download-File-Size`, and `Client-IP`.	Country IS EMPTY	Find events where the country name is not available or empty (not specified).

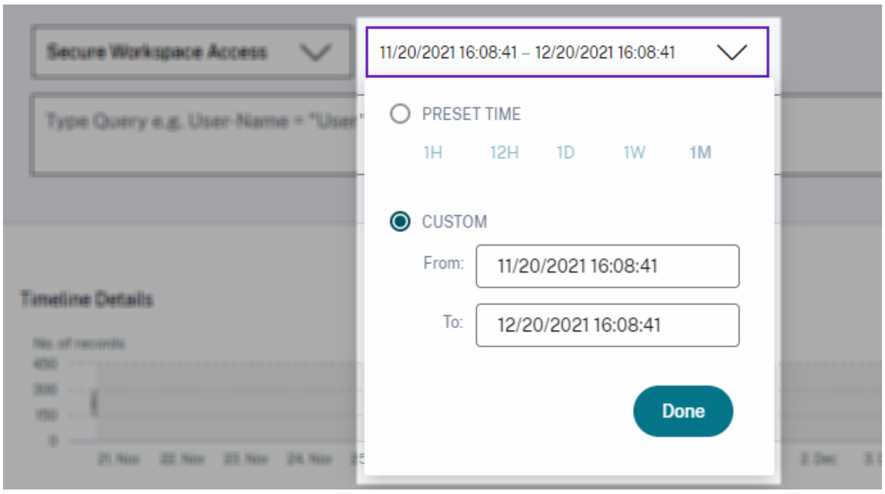
Operator	Description	Example	Output
`IS NOT EMPTY`	Checks for not null value or a specific value for a dimension. This operator works for only string type dimensions such as `App-Name`, `Browser`, and `Country`. It does not work for non-string (number) type dimensions such as `Upload-File-Size`, `Download-File-Size`, and `Client-IP`.	Country IS NOT EMPTY	Find events where the country name is available or specified.
`OR`	Searches for values where either or both conditions are true.	(User-Name = `John*` OR User-Name = `*Smith`) AND Event-Type = “Session.Logon”	Displays `Session.Logon` events for all user names that begin with John or end with Smith.

> **Note**
>
> For the **NOT EQUAL** operator, while entering the values for the dimensions in your query, use the exact values available on the self-service search page for a data source. The dimension values are case-sensitive.

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.



Secure Workspace Access

Type Query e.g. User-Name = "User"

11/20/2021 16:08:41 – 12/20/2021 16:08:41

○ PRESET TIME

1H 12H 1D 1W 1M

● CUSTOM

From: 11/20/2021 16:08:41

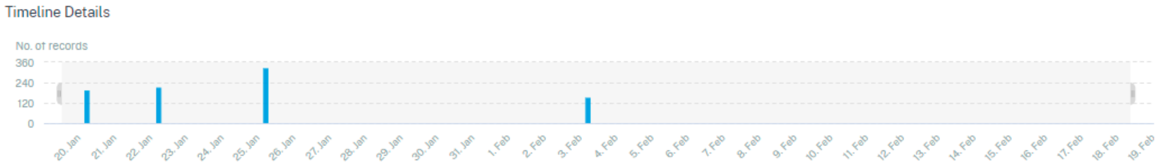
To: 12/20/2021 16:08:41

Done

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.

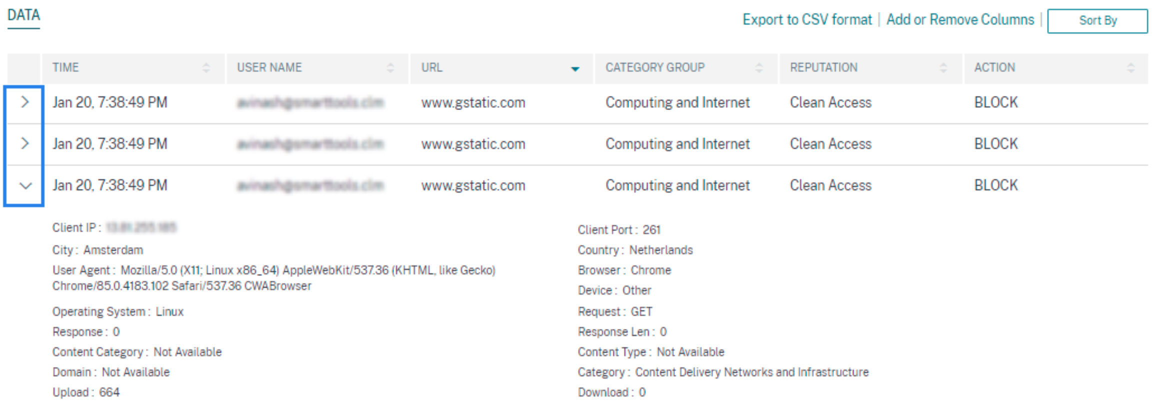
The figure shows timeline details for access data.



View the event

You can view the detailed information about the user event. On the **DATA** table, click the arrow for each column to view the user event details.

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



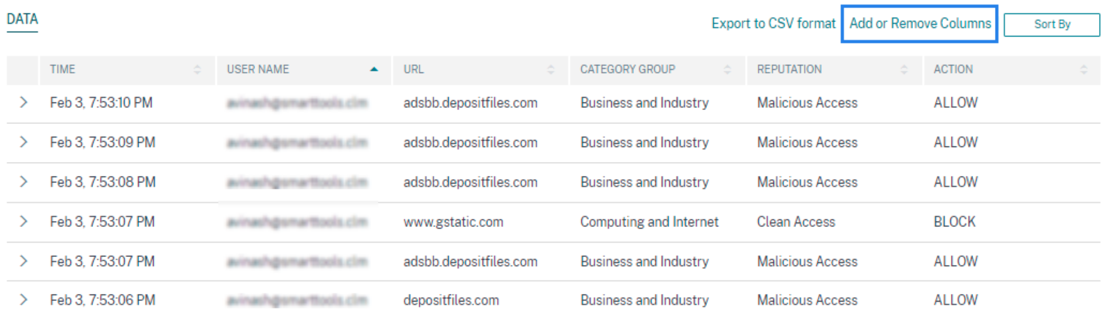
	TIME	USER NAME	URL	CATEGORY GROUP	REPUTATION	ACTION
>	Jan 20, 7:38:49 PM	[redacted]	www.gstatic.com	Computing and Internet	Clean Access	BLOCK
>	Jan 20, 7:38:49 PM	[redacted]	www.gstatic.com	Computing and Internet	Clean Access	BLOCK
∨	Jan 20, 7:38:49 PM	[redacted]	www.gstatic.com	Computing and Internet	Clean Access	BLOCK

Client IP : [redacted]
City : Amsterdam
User Agent : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36 CWABrowser
Operating System : Linux
Response : 0
Content Category : Not Available
Domain : Not Available
Upload : 664

Client Port : 261
Country : Netherlands
Browser : Chrome
Device : Other
Request : GET
Response Len : 0
Content Type : Not Available
Category : Content Delivery Networks and Infrastructure
Download : 0

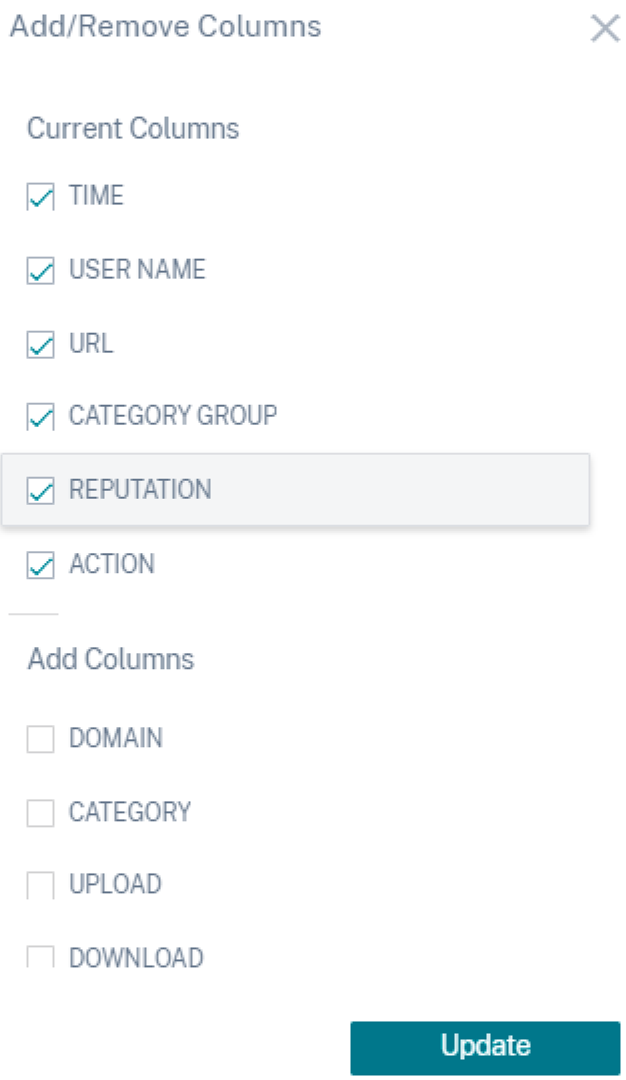
Add or remove columns You can either add or remove columns from the event table to display or hide the corresponding data points. Do the following:

1. Click **Add or Remove Columns**.



	TIME	USER NAME	URL	CATEGORY GROUP	REPUTATION	ACTION
>	Feb 3, 7:53:10 PM	[redacted]	adsbb.depositfiles.com	Business and Industry	Malicious Access	ALLOW
>	Feb 3, 7:53:09 PM	[redacted]	adsbb.depositfiles.com	Business and Industry	Malicious Access	ALLOW
>	Feb 3, 7:53:08 PM	[redacted]	adsbb.depositfiles.com	Business and Industry	Malicious Access	ALLOW
>	Feb 3, 7:53:07 PM	[redacted]	www.gstatic.com	Computing and Internet	Clean Access	BLOCK
>	Feb 3, 7:53:07 PM	[redacted]	adsbb.depositfiles.com	Business and Industry	Malicious Access	ALLOW
>	Feb 3, 7:53:06 PM	[redacted]	depositfiles.com	Business and Industry	Malicious Access	ALLOW

2. Select or deselect the data elements from the list and then click **Update**.



Add/Remove Columns

Current Columns

☑ TIME

☑ USER NAME

☑ URL

☑ CATEGORY GROUP

☑ REPUTATION

☑ ACTION

Add Columns

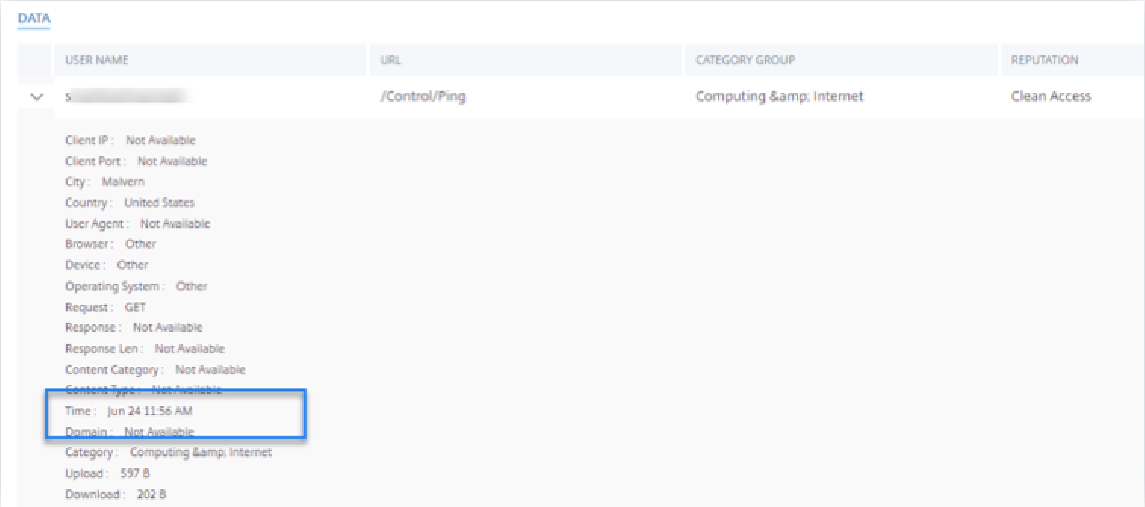
□ DOMAIN

□ CATEGORY

□ UPLOAD

□ DOWNLOAD

If you deselect a data point from the list, the corresponding column is removed from the event table. However, you can view that data point by expanding the event row for a user. For example, when you deselect the **TIME** data point from the list, the **TIME** column is removed from the event table. To view the time record, expand the event row for a user.



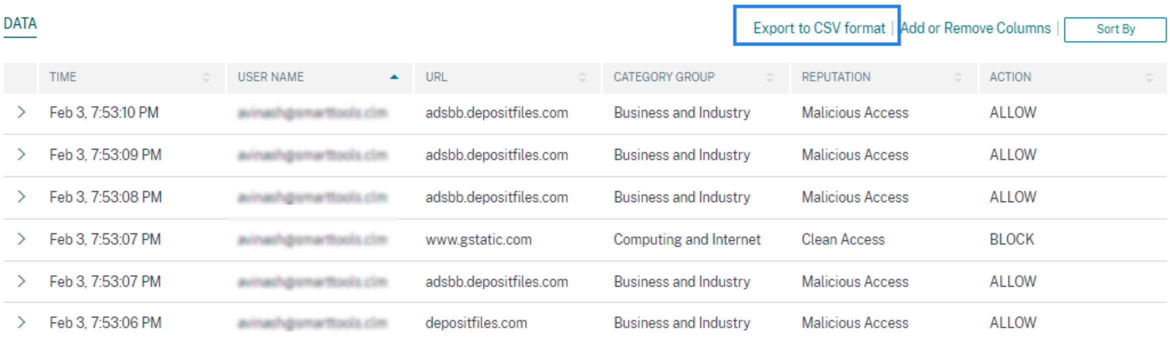
DATA

	USER NAME	URL	CATEGORY GROUP	REPUTATION
⌄	s[redacted]	/Control/Ping	Computing &amp; Internet	Clean Access

Client IP : Not Available
Client Port : Not Available
City : Malvern
Country : United States
User Agent : Not Available
Browser : Other
Device : Other
Operating System : Other
Request : GET
Response : Not Available
Response Len : Not Available
Content Category : Not Available
Content Type : Not Available
Time : Jun 24 11:56 AM
Domain : Not Available
Category : Computing &amp; Internet
Upload : 597 B
Download : 202 B

Export the events to a CSV file

Export the search results to a CSV file and save it for your reference. Click **Export to CSV format** to export the events and download the CSV file that is generated. You can export 100K rows using the **Export to CSV format** feature.



DATA

	TIME	USER NAME	URL	CATEGORY GROUP	REPUTATION	ACTION
>	Feb 3, 7:53:10 PM	[redacted]	adsbb.depositfiles.com	Business and Industry	Malicious Access	ALLOW
>	Feb 3, 7:53:09 PM	[redacted]	adsbb.depositfiles.com	Business and Industry	Malicious Access	ALLOW
>	Feb 3, 7:53:08 PM	[redacted]	adsbb.depositfiles.com	Business and Industry	Malicious Access	ALLOW
>	Feb 3, 7:53:07 PM	[redacted]	www.gstatic.com	Computing and Internet	Clean Access	BLOCK
>	Feb 3, 7:53:07 PM	[redacted]	adsbb.depositfiles.com	Business and Industry	Malicious Access	ALLOW
>	Feb 3, 7:53:06 PM	[redacted]	depositfiles.com	Business and Industry	Malicious Access	ALLOW

Export visual summary

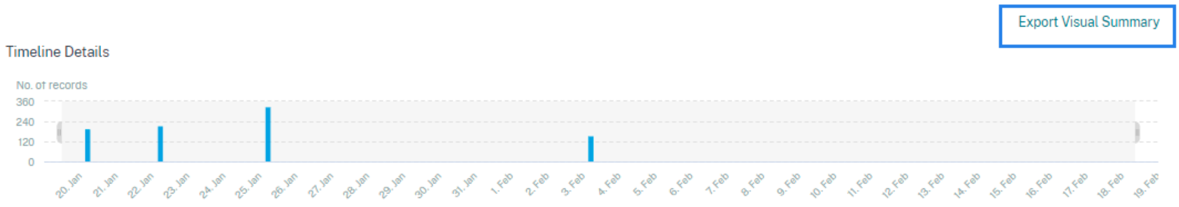
You can download the visual summary report of your search query and share a copy with other users, administrators, or your executive team.

Click **Export Visual Summary** to download the visual summary report as a PDF. The report contains the following information:

- The search query that you have specified for the events for the selected time period.
- The facets (filters) that you have applied on the events for the selected time period.

- The visual summary such as the timeline charts, bar charts, or graphs of the search events for the selected time period.

For a data source, you can download the visual summary report only if the data is displayed in visual formats such as bar charts, timeline details. Otherwise, this option is not available. For example, you can download the visual summary report of the data sources such as Apps and Desktops, Sessions, where you see data as timeline details and bar charts. For the data sources such as Users and Machines, you see data only in tabular format. Therefore, you cannot download any visual summary report.

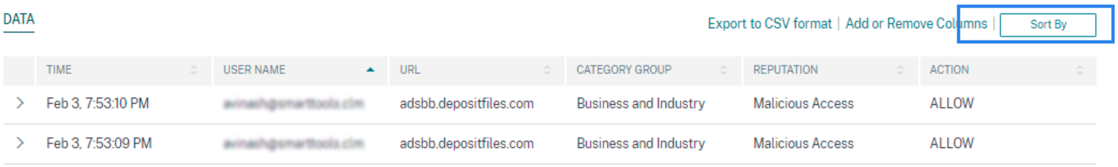


Multi-column sorting

Sorting helps to organize your data and provides better visibility. On the self-service search page, you can sort the user events by one or more columns. The columns represent the values of various data elements such as user name, date and time, and URL. These data elements vary based on the selected data sources.

To perform a multi-column sorting, do the following:

1. Click **Sort By**.



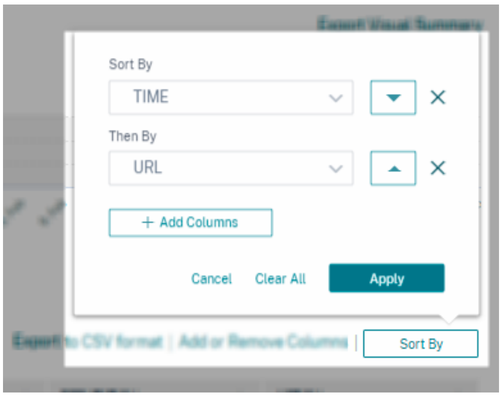
	TIME	USER NAME	URL	CATEGORY GROUP	REPUTATION	ACTION
>	Feb 3, 7:53:10 PM	[redacted]	adsbb.depositfiles.com	Business and Industry	Malicious Access	ALLOW
>	Feb 3, 7:53:09 PM	[redacted]	adsbb.depositfiles.com	Business and Industry	Malicious Access	ALLOW

2. Select a column from the **Sort By** list.
3. Select the sorting order- ascending (up arrow) or descending (down arrow) to sort the events in the column.
4. Click **+ Add Columns**.
5. Select another column from the **Then By** list.
6. Select the sorting order- ascending (up arrow) or descending (down error) to sort the events in the column.

> **Note**
>
> You can add up to six columns to perform the sorting.

7. Click **Apply**.
8. If you do not want to apply the preceding settings, click **Cancel**. To remove the values of the selected columns, click **Clear All**.

The following example shows a multi-column sort on the Secure Private Access events. The events are sorted by time (in latest to oldest order) and then by URL (in alphabetical order).



Sort By

TIME

Then By

URL

Alternatively, you can perform multi-column sorting by using the **Shift** key. Press the **Shift** key and click the column headers to sort the user events.

How to save the self-service search

As an administrator, you can save a self-service query. This feature saves the time and effort of rewriting the query that you use often for analysis or troubleshooting. The following options are saved with the query:

- Applied search filters
- Selected data source and duration

Do the following to save a self-service query:

1. Select the required data source and duration.
2. Type a query in the search bar.
3. Apply the required filters.
4. Click **Save Search**.
5. Specify the name to save the custom query.

> **Note**
>
> Ensure that the query name is unique. Otherwise, the query does not save.

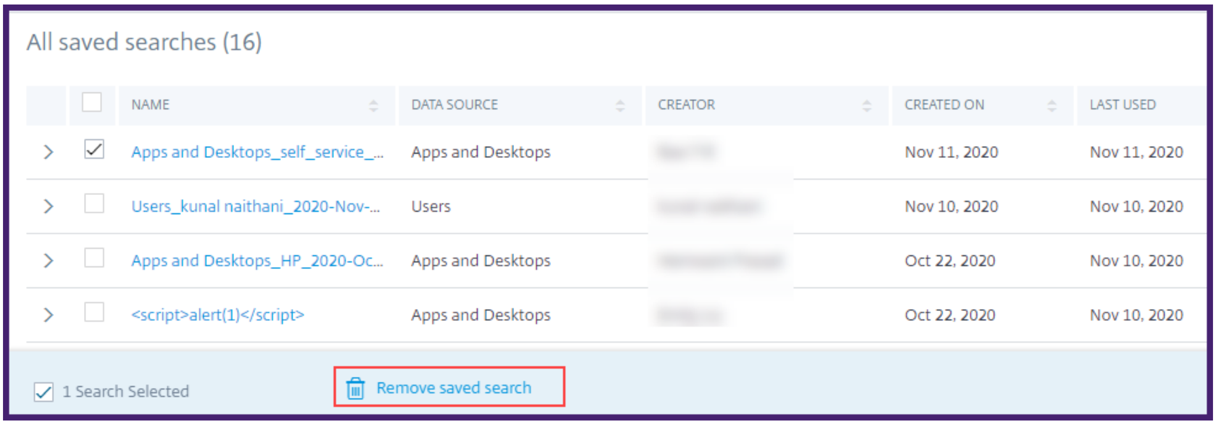
6. Enable the **Schedule email report** button if you want to send a copy of the search query report to yourself and other users at a regular interval. For more information, see Schedule an email for a search query.
7. Click **Save**.

To view the saved searches:

1. Click **View Saved Searches**.
2. Click the name of the search query.

To remove a saved search:

1. Click **View Saved Searches**.
2. Select the search query that you have saved.
3. Click **Remove saved search**.



All saved searches (16)

	□	NAME	DATA SOURCE	CREATOR	CREATED ON	LAST USED
>	☑	Apps and Desktops_self_service_...	Apps and Desktops	[redacted]	Nov 11, 2020	Nov 11, 2020
>	□	Users_kunal naithani_2020-Nov-...	Users	[redacted]	Nov 10, 2020	Nov 10, 2020
>	□	Apps and Desktops_HP_2020-Oc...	Apps and Desktops	[redacted]	Oct 22, 2020	Nov 10, 2020
>	□	<script>alert(1)</script>	Apps and Desktops	[redacted]	Oct 22, 2020	Nov 10, 2020

To modify a saved search:

1. Click **View Saved Searches**.
2. Click the name of the search query that you have saved.
3. Modify the search query or the facet selection based on your requirement.
4. Click **Update Search > Save** to update and save the modified search with the same search query name.
5. If you want to save the modified search with a new name, click the down arrow and click **Save as new search > Save As**.

If you replace the search with a new name, the search is saved as a new entry. If you retain the existing search name while replacing, then the modified search data overrides the existing search data.

> **Note**
>
> - Only a query owner can modify or remove their saved searches.
> - You can copy the saved search link address to share with another user.

Schedule an email for a search query

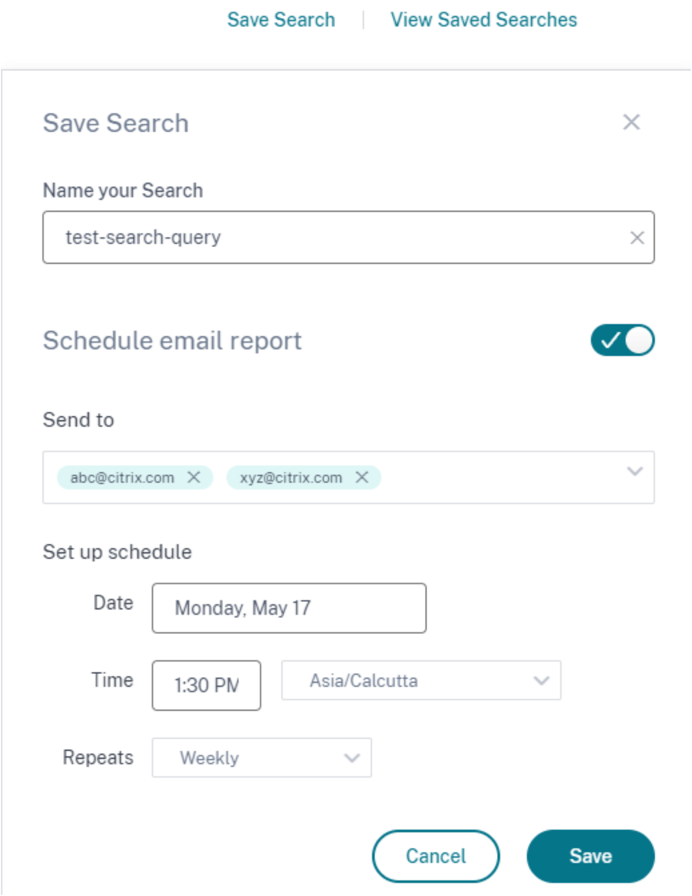
You can send a copy of the search query report to yourself and other users on regular intervals by setting up an email delivery schedule.

This option is available only if your search query report contains data in visual formats such as bar charts, timeline details. Otherwise, you cannot schedule an email delivery. For example, you can schedule an email for the data sources such as Apps and Desktops, Sessions, where you see data as timeline details and bar charts. For the data sources such as Users and Machines, you see data only in tabular format. Therefore, you cannot schedule an email.

Schedule an email while saving a search query

While saving a search query, set up an email delivery schedule as follows:

1. On the **Save Search** dialog box, enable the **Schedule email report** button.



Name your Search: test-search-query

Schedule email report ✓

Send to: abc@citrix.com, xyz@citrix.com

Set up schedule

Date: Monday, May 17

Time: 1:30 PM Asia/Calcutta

Repeats: Weekly

2. Enter or paste the email addresses of the recipients.

   > **Note**
   >
   > Email groups are not supported.

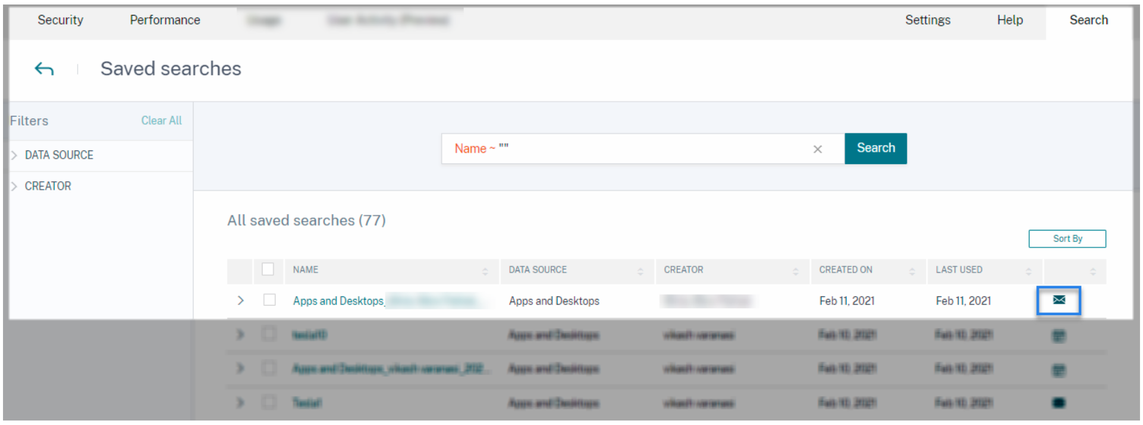
3. Set the date and time for the email delivery.
4. Select the delivery frequency- daily, weekly, or monthly.
5. Click **Save**.

Schedule an email for an already saved search query

If you want to set up an email delivery schedule for a search query that you previously saved, do the following:

1. Click **View Saved Searches**.
2. Go to the search query that you have created. Click the **Email this query** icon.

> **Note**
>
> Only a query owner can schedule email delivery of their saved search query.



All saved searches (77)

NAME	DATA SOURCE	CREATOR	CREATED ON	LAST USED
Apps and Desktops_[redacted]	Apps and Desktops	[redacted]	Feb 11, 2021	Feb 11, 2021

3. Enable the **Schedule email report** button.
4. Enter or paste the email addresses of the recipients.

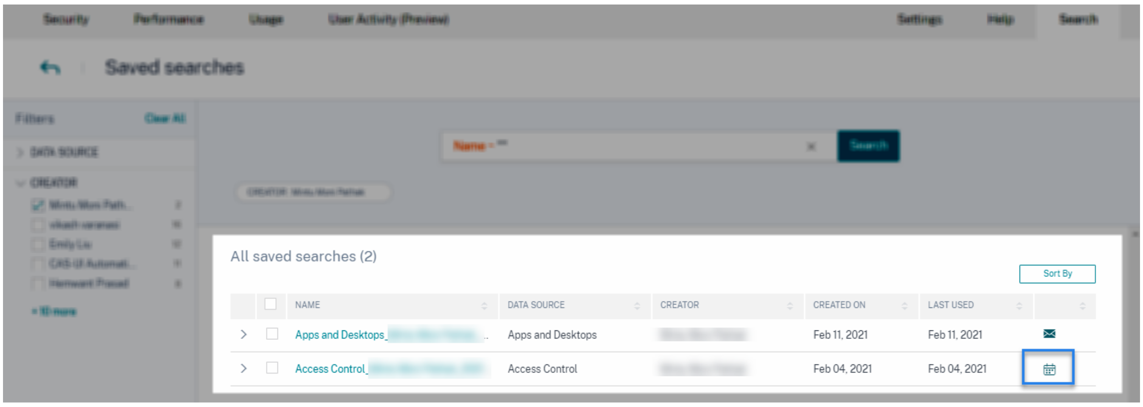
   > **Note**
   >
   > Email groups are not supported.

5. Set the date and time for the email delivery.
6. Select the delivery frequency- daily, weekly, or monthly.
7. Click **Save**.

Stop an email delivery schedule for a search query

1. Click **View Saved Searches**.
2. Go to the search query that you have created. Click the **View email delivery schedule** icon.

   > **Note**
   >
   > Only a query owner can stop the email schedule of their saved search query.



All saved searches (2)

NAME	DATA SOURCE	CREATOR	CREATED ON	LAST USED	
Apps and Desktops_[illegible]	Apps and Desktops	[illegible]	Feb 11, 2021	Feb 11, 2021	✉
Access Control_[illegible]	Access Control	[illegible]	Feb 04, 2021	Feb 04, 2021	📅

3. Disable the **Schedule email report** button.

4. Click **Save**.

Email content

The recipients receive an email from "Citrix Cloud - Notifications donotreplynotifications@citrix.com" about the search query report. The report is attached as a PDF document. The email is sent at a regular interval defined by you in the **Schedule email report** settings.

The search query report contains the following information:

- The search query that you have specified for the events for the selected period.
- The facets (filters) that you have applied on the events.
- The visual summary such as the timeline charts, bar charts, or graphs of the search events.

Permissions for full access and read-only access administrators

- If you are a Citrix Cloud administrator with full access, you can use all the features available on the **Search** page.
- If you are a Citrix Cloud administrator with read-only access, you can only do the following activities on the **Search** page:
  - View the search results by selecting a data source and the time period.
  - Enter a search query and view the search results.
  - View the saved search results of other administrators.
  - Export the visual summary and download the search results as a CSV file.

For information about the administrator roles, see Manage administrator roles for Citrix Analytics.

Alert settings

November 3, 2023

Citrix Analytics generates alerts based on the alert policy criteria. You can configure to receive alert notifications from Citrix Analytics for Security and Performance via email and Webhook.

- Email distribution list
- Webhook for Alert Notifications

You can format the email notification for alerts from Citrix Analytics for Security.

- End user email settings

Email distribution lists

November 3, 2023

When you apply the **Notify administrator(s)** action either manually or by creating a policy, a notification is sent to the selected administrators about the risk indicator.

> **IMPORTANT**
>
> You can select administrators from the Citrix Cloud domains and other non-Citrix Cloud domains in your organization.

To send notifications to the appropriate groups of administrators, create a distribution list using their email addresses.

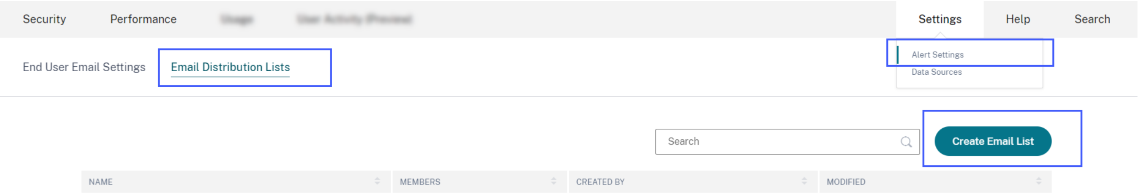
With the email distribution list, you can do the following:

- Create a common email distribution list with members from different domains in your organization.
- Notify all the members all at once.
- Save your time and effort of selecting the administrators from different domains.
- Manage and maintain the email distribution lists based on your requirements such as adding new members or removing existing members.

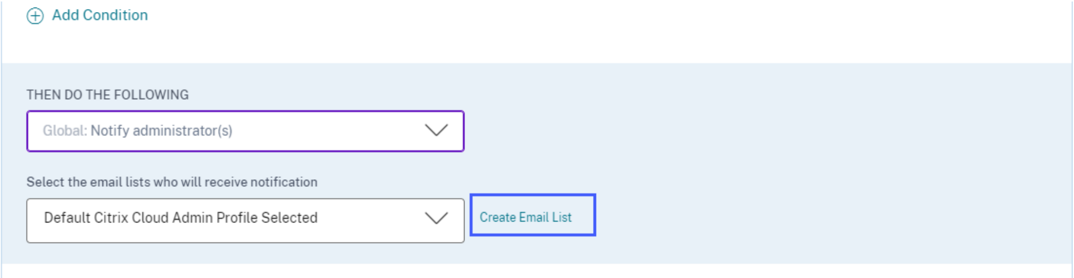
Create email distribution list

To create an email distribution list:

1. Click **Settings > Alert Settings > Email Distribution Lists > Create Email List**.

   Alternatively, you can also create an email distribution list from a policy. Modify an existing policy or create a policy and select the **Notify administrator(s)** action. Click the **Create Email List** link.

   
   Add Condition
   THEN DO THE FOLLOWING
   Global: Notify administrator(s)
   Select the email lists who will receive notification
   Default Citrix Cloud Admin Profile Selected
   Create Email List

2. Enter a name and a description of the email distribution list to identify its purpose.

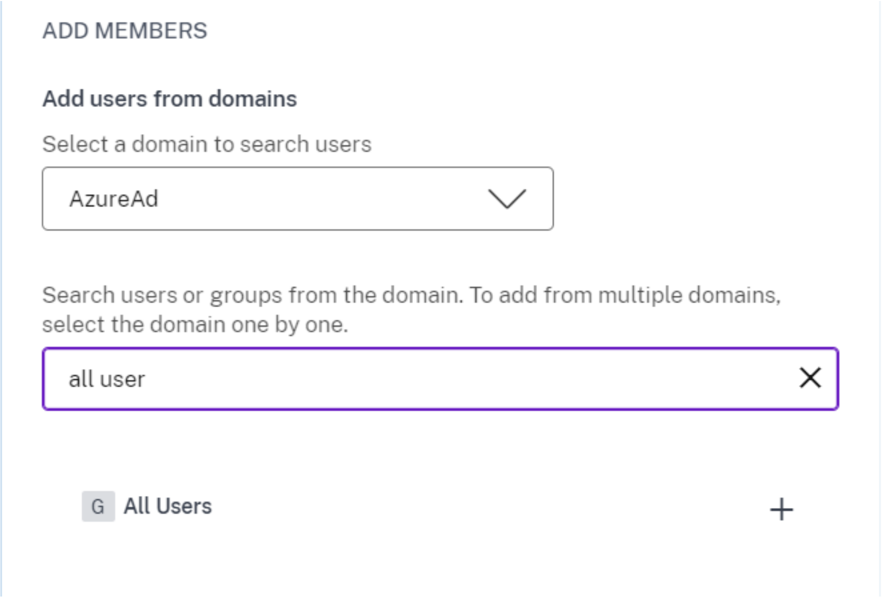
3. Use the following options to add members to the email distribution list:

   - **Add users from domains**. This option requires that your domains are connected with Citrix Cloud.
   - **Add users by email addresses**. Use this option if you want to add users that are outside your selected domains.

4. To add users from domains, select a domain and search the users or the user groups.

   > **Note**
   >
   > You can also add users and user groups from multiple domains by selecting the domains one by one. For each domain, search and add the users or the user group.

5. Click the **Add** icon beside the user or the user group.



ADD MEMBERS

Add users from domains

Select a domain to search users

AzureAd

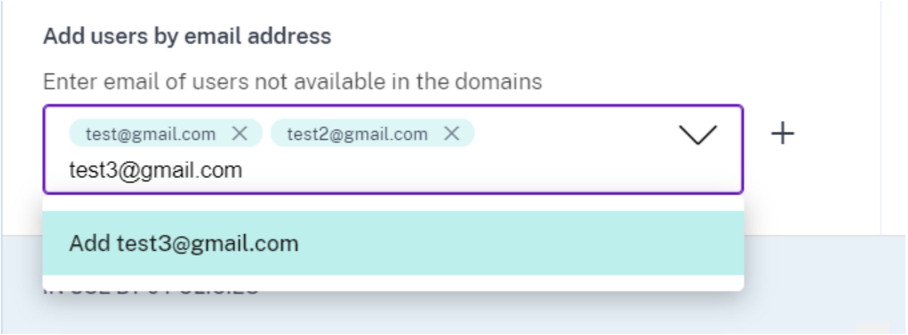
Search users or groups from the domain. To add from multiple domains, select the domain one by one.

all user

G All Users

6. To add users that are not available in your selected domain, enter either the users' email addresses or the email distribution lists.

> **Note**
>
> Before entering an email distribution list, ensure that you can access the email distribution list from outside your organization's network. If you add an email distribution list that is internal to your organization, the members of the list can't receive any notifications from Citrix Analytics.



Add users by email address

Enter email of users not available in the domains

test@gmail.com test2@gmail.com

test3@gmail.com

Add test3@gmail.com

7. Click **Create Email List**.

View email distribution list

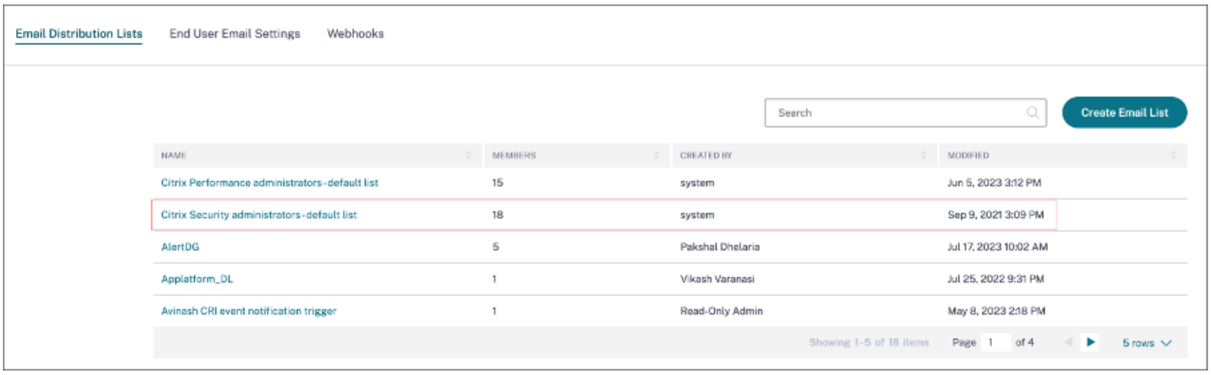
To view your email distribution lists, click **Settings > Alert Settings > Email Distribution Lists**.

The page displays all the email distribution lists created in your account. Select an email distribution list to view the members or modify the list.

You see an email distribution list created by default in your account. It contains the Citrix Cloud administrators whose **Email Notifications** option is enabled in their Citrix Cloud accounts. You can't delete or modify the default list.

> **Note**
>
> For the default email distribution list, Citrix Analytics caches the information about the administrators whose email notifications are enabled. The cache refreshes once in every 24 hours. So if any administrator changes the email notification preferences, this change gets updated in Citrix Analytics after 24 hours.
>
> For example, if a Citrix Cloud administrator enables their email notifications, they start receiving notifications after 24 hours, not instantly. Similarly, if a Citrix Cloud administrator disables their email notifications, they stop receiving notifications after 24 hours.

The default distribution list for security administrators now includes both full and custom administrators who have the **Email Notifications** option enabled in their Citrix Cloud accounts.



NAME	MEMBERS	CREATED BY	MODIFIED
Citrix Performance administrators-default list	15	system	Jun 5, 2023 3:12 PM
Citrix Security administrators-default list	18	system	Sep 9, 2021 3:09 PM
AlertDG	5	Pakshal Dhelaria	Jul 17, 2023 10:02 AM
Applatform_DL	1	Vikash Varanasi	Jul 25, 2022 9:31 PM
Avinash CRI event notification trigger	1	Read-Only Admin	May 8, 2023 2:18 PM

Showing 1-5 of 18 items Page 1 of 4 5 rows

Modify an email distribution list

To modify an email distribution list:

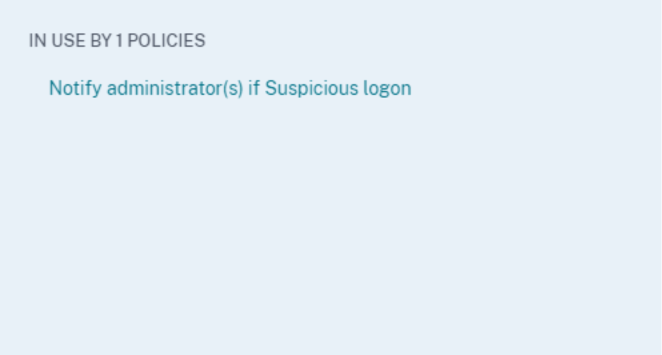
1. Click **Settings > Alert Settings > Email Distribution Lists**.
2. Click the email distribution list that you want to modify.
3. On the email distribution list, update the required details such as name, description, and add or remove members.
4. Click **Save Changes**.

Delete an email distribution list

You can delete an email distribution list only if it is not linked with any policies. If it is linked with some policies, you need to first remove the email distribution list from the associated policies.

To delete an email distribution list:

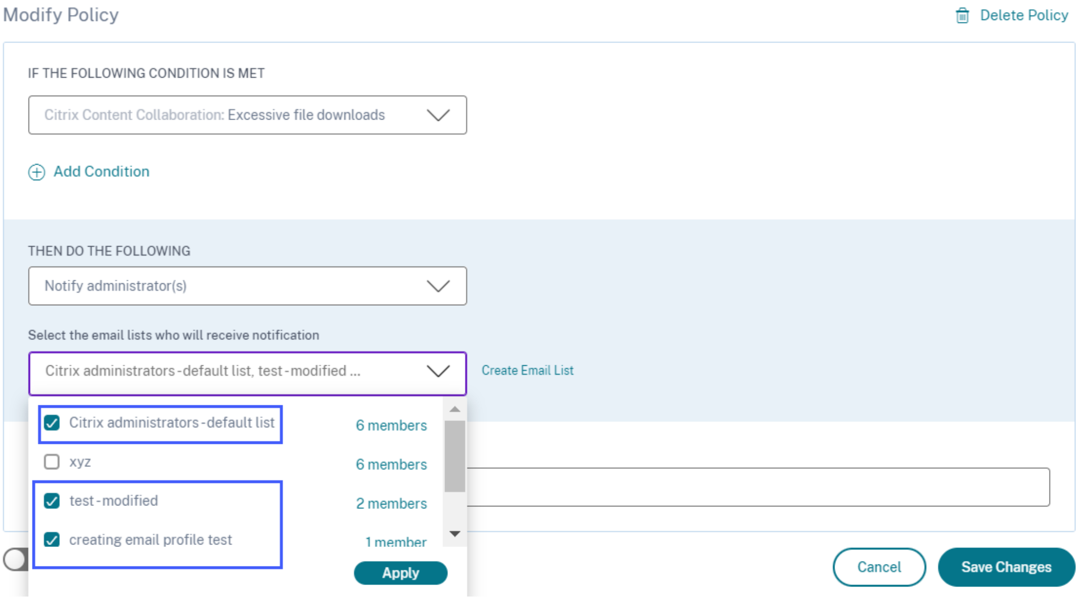
1. Click **Settings > Alert Settings > Email Distribution Lists**.
2. Click the email distribution list that you want to delete.
3. On the email distribution list, view the associated policies.



IN USE BY 1 POLICIES

Notify administrator(s) if Suspicious logon

4. Click the policy to open it and remove the email distribution lists. You can also delete the policy if you want.



Modify Policy

IF THE FOLLOWING CONDITION IS MET

Citrix Content Collaboration: Excessive file downloads

THEN DO THE FOLLOWING

Notify administrator(s)

Select the email lists who will receive notification

Citrix administrators-default list, test-modified ...

☑ Citrix administrators-default list 6 members

☐ xyz 6 members

☑ test-modified 2 members

☑ creating email profile test 1 member

5. Click **Save Changes** and go back to the email distribution list.
6. Open the email distribution list and click the **Delete** icon.

Webhook for Alert Notifications

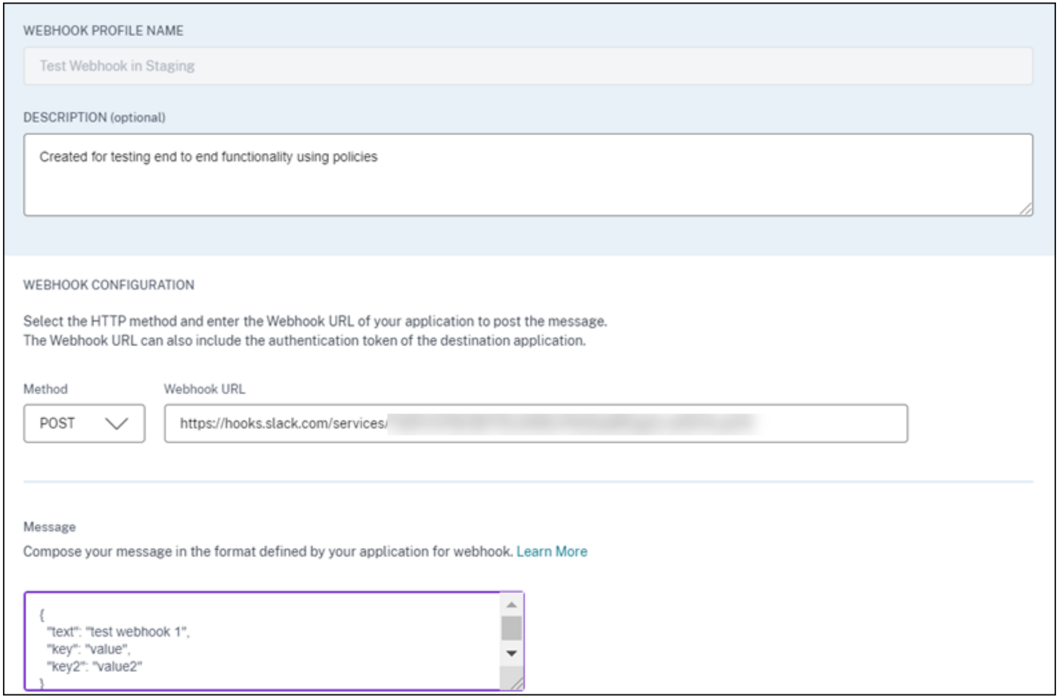
You can use webhooks to send Citrix Analytics alert notifications to any third-party applications that have incoming webhook URLs configured. Webhooks are HTTP callbacks that enable real-time messaging between the service provider applications and consumer applications. Since the alert notifications are sent in real time, you get notified when the events occur.

When Citrix Analytics triggers an alert, the associated webhook sends the alert message to the URL of the target application. The alert is sent in the form of a JSON payload through the HTTP POST or PUT request. For example, when a user triggers a risk indicator or the performance of a VDI machine goes down, you can set up a webhook to send the alert notifications to your Slack channel.
Setting up webhooks for alert management helps you to get real-time notifications in your applications. You can take timely actions to mitigate the security risk or improve the performance of your Citrix Virtual Apps and Desktops deployment.

Create Webhook Profile

To create the webhook profiles on Citrix Analytics:

1. Sign in to Citrix Analytics.
2. Depending on your subscribed offering, click **Manage** to access Security Analytics or Performance Analytics.
3. From the top bar, click **Settings > Alert Settings > Webhook**.
4. Select **Create Webhook**.



WEBHOOK PROFILE NAME

Test Webhook in Staging

DESCRIPTION (optional)

Created for testing end to end functionality using policies

WEBHOOK CONFIGURATION

Select the HTTP method and enter the Webhook URL of your application to post the message.
The Webhook URL can also include the authentication token of the destination application.

Method: POST

Webhook URL: https://hooks.slack.com/services/[redacted]

Message

Compose your message in the format defined by your application for webhook. Learn More

```
{
 "text": "test webhook 1",
 "key": "value",
 "key2": "value2"
}
```

5. Enter a profile name and a description of the webhook to identify its purpose.

6. Select the HTTP method and the webhook URL of your application to send the alert message.

   > **Note:**
   >
   > Usually the outgoing webhooks are sent through the HTTP POST request. You can also include an authentication token in the webhook URL of your application.

7. Enter the message about the alert that you want to send to the webhook URL. The message must be structured in the formats such as JSON or XML as defined by the target application. For more information, see the Webhook examples.
8. (Optional) Enter the header keys and values for the message. The header can include authentication tokens or other custom key-value pairs to securely send the payload to your application.
9. To validate the webhook configuration, click **Test**.
   The test validates the outgoing webhook URL, the payload structure, and the header keys. If no issues are found in your configuration, you get the "Test successful"message.

Webhook Configuration Examples

The section provides examples of configuring webhooks to send alerts to third-party applications such as Slack and Microsoft Teams.

> **Note:**
>
> Refer to the product documentation of the third-party applications on how to get the webhook URL and the required configurations for the webhook.

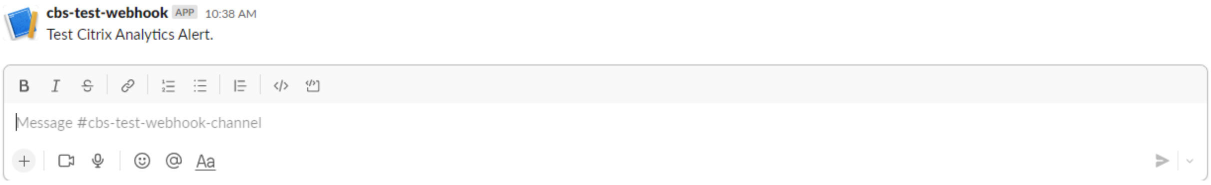
Sending alert message to Slack

On Slack, ensure that you have completed the following tasks before sending an alert:

1. Create a Slack app for Citrix Analytics if you don't have already one.
2. For the app, enable the Incoming Webhook feature and create an incoming Webhook.
3. Select a channel to which the app posts the message.
4. When you authorize the app, you get the Webhook URL for sending the message.
   For information, see Getting started with Incoming Webhooks.

Sample message format `curl --location --request POST 'WEBHOOK URL'--header 'Content-Type: application/json'--data-raw '{ "text": "Test Citrix Analytics Alert." }`

Output



cbs-test-webhook APP 10:38 AM
Test Citrix Analytics Alert.

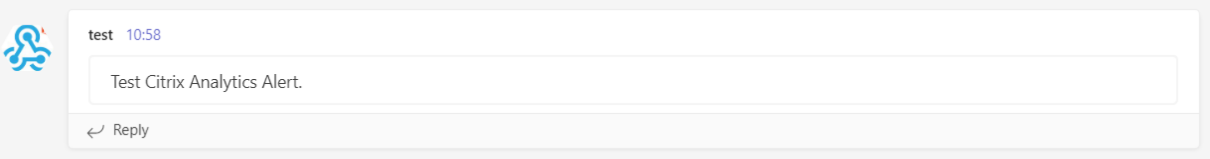
Sending alert message to Microsoft Teams

On Microsoft Teams, ensure that you have completed the following tasks before sending an alert:

1. Create a Teams group within Teams if you don't have already one.
2. Create a Webhook connecter. Refer to the steps described in the Create and send messages article.
3. Get the URL for the webhook.

Sample message format `curl --location --request POST 'WEBHOOK URL'--header 'Content-Type: application/json'--data-raw '{ "text": "Test Citrix Analytics Alert." }`

Output



test 10:58
Test Citrix Analytics Alert.

Citrix Analytics for Security (Security Analytics)

January 11, 2024

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.

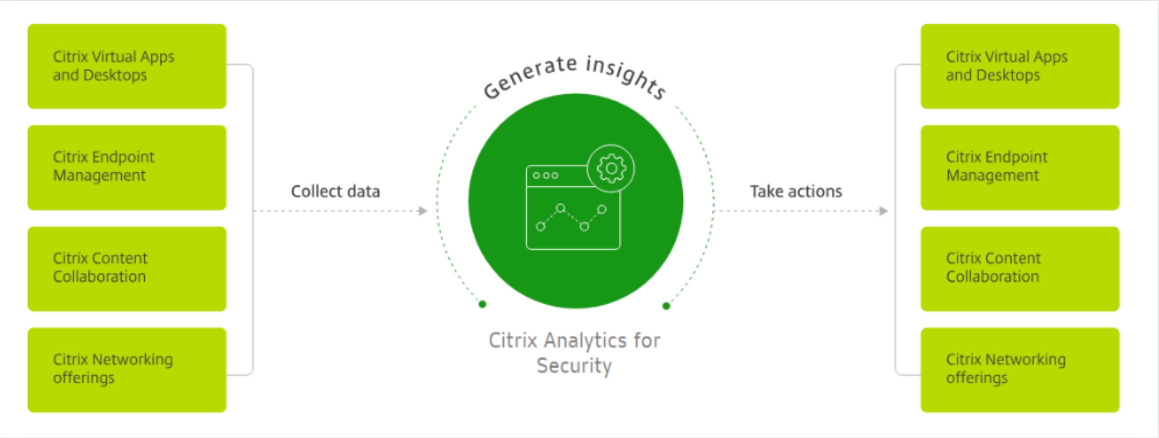
What is Security Analytics?

Citrix Analytics for Security continuously assesses the behavior of Citrix Virtual Apps and Desktops users, Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) users, and Citrix Workspace users.

It applies actions to protect sensitive corporate information. The aggregation and correlation of data across networks, virtualized applications and desktops 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. For more information, see Self-service search.
- Easy-to-consume dashboards provide a complete view of user behavior. For more information, see Users dashboard.
- Detect and mitigate malicious user behavior using machine learning and customized policies with automated actions. For more information, see Policies and actions.
- Continuous monitoring of user behavior after initial authentication to corporate networks balances thorough security and great user experience. For more information, see Continuous risk assessment.


Citrix Virtual Apps and Desktops
Citrix Endpoint Management
Citrix Content Collaboration
Citrix Networking offerings
Collect data
Generate insights
Citrix Analytics for Security
Take actions
Citrix Virtual Apps and Desktops
Citrix Endpoint Management
Citrix Content Collaboration
Citrix Networking offerings

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.

- Access Assurance Location: Summarizes the access details and the logon details of the Citrix Virtual Apps and Desktops users and Citrix DaaS users.
- Reports: Create custom reports based on the dimensions and metrics available from the onboarded data sources.

What's next

- System requirements: Minimum requirements that must be met before getting started.
- Data sources: Know about the products that Analytics supports.
- Data governance: Know about the collection, storage, and retention of logs by Analytics.
- Get started: How to start using Analytics in your organization.

Citrix Analytics for Performance (Performance Analytics)

August 17, 2023

What is Performance Analytics

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

- Performance Analytics aggregates site performance metrics into easy-to-view User Experience and Infrastructure dashboards. The dashboards help you analyze the user experience and optimize the usage of your 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 on 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 machines 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 machines is insufficient.
- If you see several cases of sessions failing to launch, drilldown to establish the cause for the failure. It might be a shortage in the number of licenses or issues with machine connection to the Delivery Controller.

> **Note:**
>
> **Infrastructure Analytics Dashboard** is currently under Preview.

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

Getting Started

Prerequisites

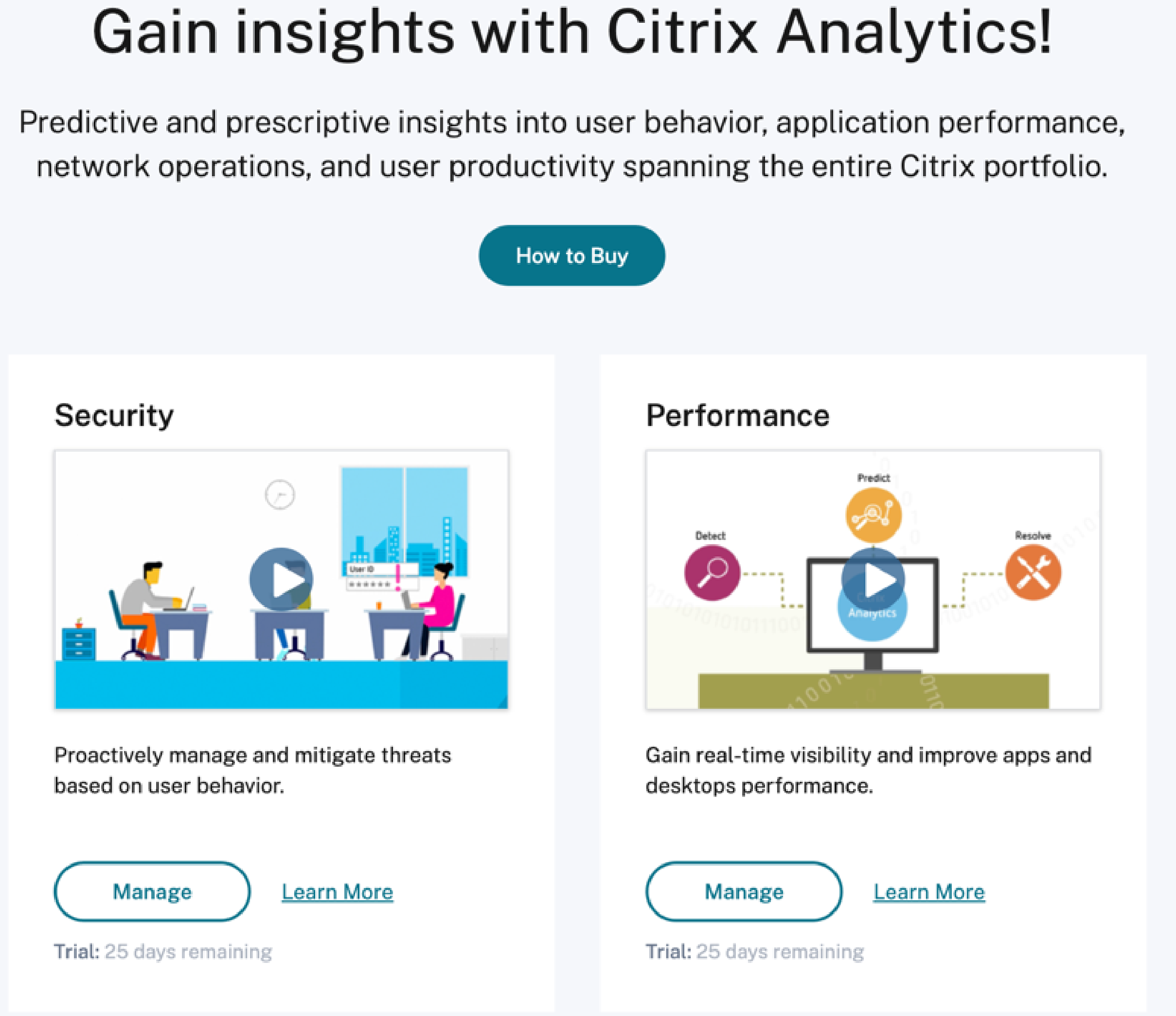
1. Check if your workstation has a supported web browser listed in the Supported browsers article. For information about the system requirements, see the Citrix Analytics System Requirements article.
2. You must have a Citrix Cloud account to use the Analytics service. For detailed instructions on how 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. Citrix Analytics for Performance is available as a subscription based offering, either as a standalone 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)`.
4. Supported versions of data sources is available in the Data Sources article.
5. Citrix Profile Management must be installed on all machines.
6. The End User Experience Monitoring (EUEM) service must be running and the corresponding policies must be configured on all machines. For more details see, End user monitoring policy settings.
7. The **VDA data collection for Performance Analytics** policy must be set to **Allowed** on machines to enable the Monitoring service to collect machine related performance metrics such as Bandwidth and latency statistics. For more information, see Policy for collecting data for Performance Analytics.
8. Enable the Process Monitoring policy from Citrix Studio to gain visibility into the high resource consuming processes in the **Machine Statistics > Process** tab.
   For more information, see Enable Process Monitoring.
9. Ensure accessibility to the following URLs from all endpoints (or proxies, if they are configured):

Endpoint	United States region	European Union region	Asia Pacific South region
Citrix Key Registration	`https://trust.citrixnetworkapi.net`	`https://trust.citrixnetworkapi.net`	`https://trust.citrixnetworkapi.net`
Citrix Cloud	`https://trust.citrixworkspacesapi.net`	`https://trust-eu.citrixworkspacesapi.net`	`https://trust-aps.citrixworkspacesapi.net`
Citrix Analytics	`https://api.was.cloud.com`	`https://api-eu.was.cloud.com`	`https://api-aps.was.cloud.com`
Bulk Upload	`https://citrixanalyticseh-alias.servicebus.windows.net/`	`https://citrixanalyticseheu-alias.servicebus.windows.net/`	`https://citrixanalyticsehaps-alias.servicebus.windows.net/`

Access

1. Log on to Citrix Cloud. Look for the Analytics service tile and click **Manage**. The overview page displays the offerings available in the Analytics portfolio.
2. 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.



Gain insights with Citrix Analytics!

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

Security

Proactively manage and mitigate threats based on user behavior.

Trial: 25 days remaining

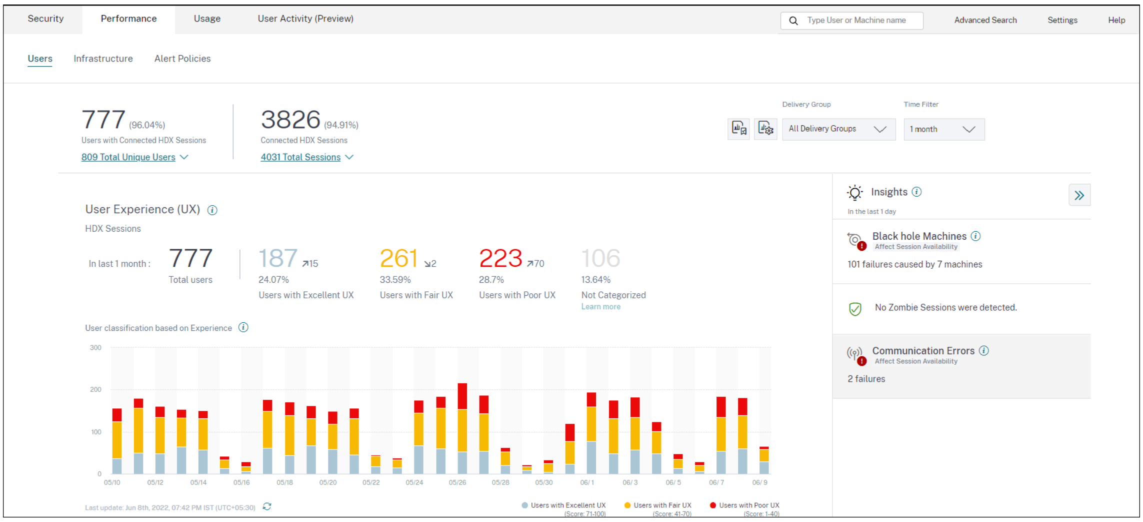
Performance

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

Trial: 25 days remaining

.

1. Citrix Analytics for Performance opens with dashboards displaying the User Experience and Infrastructure Performance Analytics.



777 (96.04%)
Users with Connected HDX Sessions
809 Total Unique Users

3826 (94.91%)
Connected HDX Sessions
4031 Total Sessions

User Experience (UX)
HDX Sessions

In last 1 month : 777 Total users

187 ↗15
24.07%
Users with Excellent UX

261 ↘2
33.59%
Users with Fair UX

223 ↗70
28.7%
Users with Poor UX

106
13.64%
Not Categorized
Learn more

User classification based on Experience

Last update: Jun 8th, 2022, 07:42 PM IST (UTC+05:30)

Insights
In the last 1 day

Black hole Machines
Affect Session Availability
101 failures caused by 7 machines

No Zombie Sessions were detected.

Communication Errors
Affect Session Availability
2 failures

Access from the Asia Pacific South region Citrix Analytics for Performance is now onboarded automatically for trial customers and subscription-based customers in the Asia Pacific South (APS) region. For more information on the regions supported in Citrix Cloud, see Geographical considerations.

To access Performance Analytics from the APS region, choose the Asia Pacific South region while onboarding your tenant to Citrix Cloud. Log on to Citrix Cloud, and select your tenant in the APS region of Citrix Cloud. Use the `https://analytics-aps.cloud.com` URL to access your Citrix Analytics Cloud Service.

- Citrix Analytics for Performance now stores the user events and metadata of your organization in the Asia Pacific South region when you choose it as your home region. For more information, see Data governance.
- For information about the network requirements for the Asia Pacific South region, see Technical security overview.

Configure Data Sources

You can 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.

Performance Analytics automatically detects your Citrix DaaS (formerly Citrix Virtual Apps and Desktops service).
If you are an on-premises customer,

- First onboard your Citrix Virtual Apps and Desktops Sites to Performance Analytics.
- To get network related information on Performance Analytics, you must also onboard your on-premises Citrix Gateway.

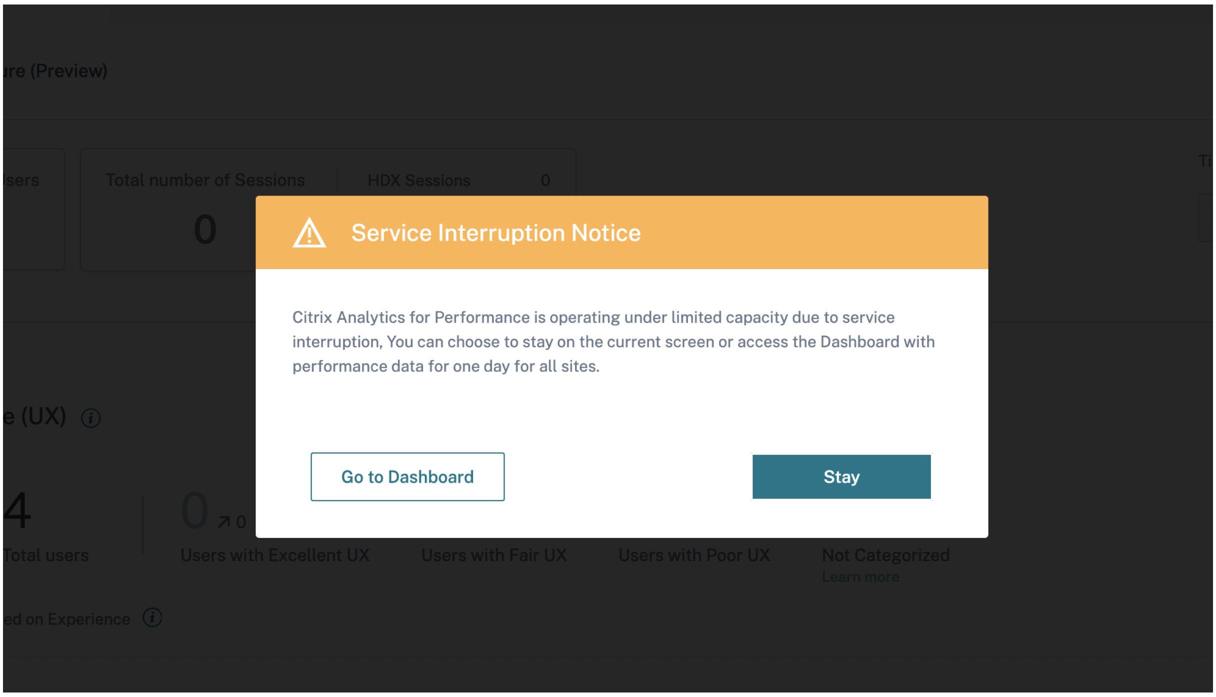
Configure the required data sources as described in the Data Sources article.

> **Note:**
>
> - Citrix Analytics for Performance collects and stores logs for data points as listed in Logs collected for Citrix Analytics for Performance.
> - Recommended limits for the Citrix Analytics for Performance service are listed in the Limits article.

Service Continuity

In the event of a service interruption, Citrix Analytics for Performance operates in a limited capacity.

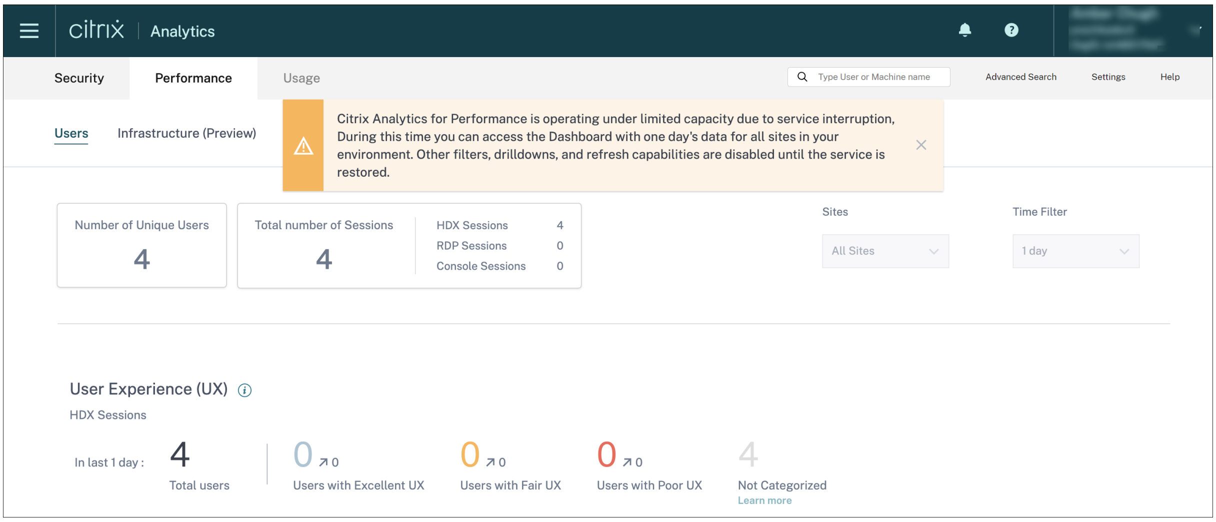
The admin can choose to **Stay** and view data available on the current screen or **Go to dashboard** in a downgraded mode.



Service Interruption Notice

Citrix Analytics for Performance is operating under limited capacity due to service interruption, You can choose to stay on the current screen or access the Dashboard with performance data for one day for all sites.

In the downgraded mode, the user is switched to the dashboard containing data of all sites for the past day.
All filters, and drilldowns are disabled until the service is restored to normal operation in either case.



Citrix Analytics for Performance is operating under limited capacity due to service interruption, During this time you can access the Dashboard with one day's data for all sites in your environment. Other filters, drilldowns, and refresh capabilities are disabled until the service is restored.

Number of Unique Users	4	
Total number of Sessions	4	
	HDX Sessions	4
	RDP Sessions	0
	Console Sessions	0

Sites: All Sites

Time Filter: 1 day

User Experience (UX)

HDX Sessions

In last 1 day : 4 Total users

0 ↗ 0 Users with Excellent UX

0 ↗ 0 Users with Fair UX

0 ↗ 0 Users with Poor UX

4 Not Categorized

Learn more

This update improves product resiliency and helps align with the Service Level Agreement.

Troubleshoot Citrix Analytics for Security and Performance

November 30, 2023

This section explains how to resolve the following issues that you might encounter when you use Citrix Analytics for Security.

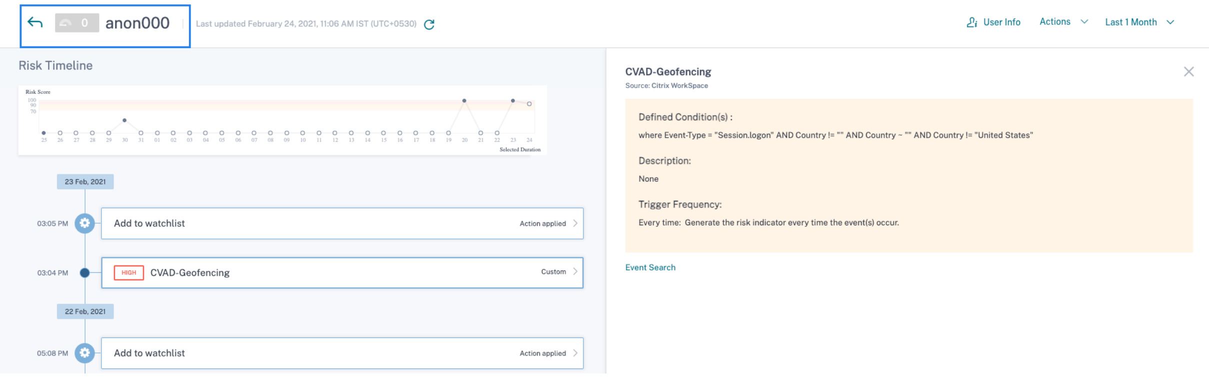
- Verify anonymous users as legitimate users.
- Troubleshoot event transmission issues from a data source.
- Trigger Virtual Apps and Desktops events, SaaS events, and verifying event transmission to Citrix Analytics for Security.
- Session recording server fails to connect.
- Configuration issues with Citrix Analytics add-on for Splunk

Verify the anonymous users as legitimate users

June 2, 2022

As an administrator, you might notice that some Citrix Virtual Apps and Desktops users and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) users are shown as anonymous on Citrix Analytics for Security. These users are identified as discovered users. But their user names appear as anonXYZ (where "XYZ"represents a three digit number) on the following pages:

- Users
- User's timeline
- Risky users
- Self-service search for the Apps and Desktops data source



23 Feb, 2021

03:05 PM Add to watchlist — Action applied

03:04 PM HIGH CVAD-Geofencing — Custom

22 Feb, 2021

05:08 PM Add to watchlist — Action applied

CVAD-Geofencing

Source: Citrix WorkSpace

Defined Condition(s) :

where Event-Type = "Session.logon" AND Country != "" AND Country ~ "" AND Country != "United States"

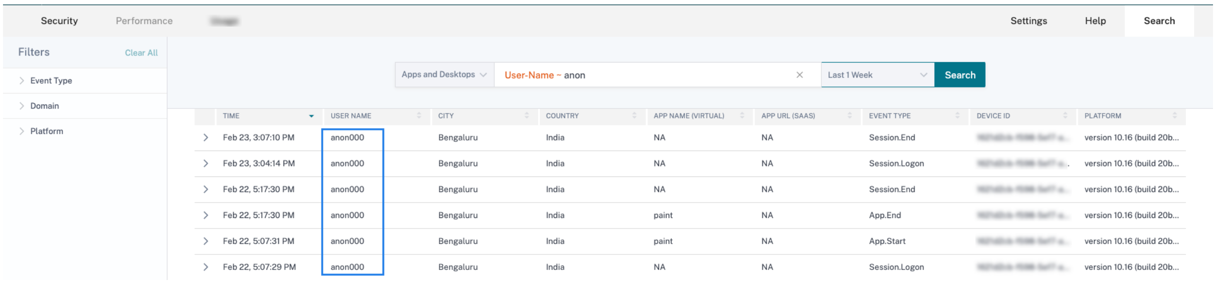
Description:

None

Trigger Frequency:

Every time: Generate the risk indicator every time the event(s) occur.

Event Search



User-Name ~ anon

TIME	USER NAME	CITY	COUNTRY	APP NAME (VIRTUAL)	APP URL (SAAS)	EVENT TYPE	DEVICE ID	PLATFORM
Feb 23, 3:07:10 PM	anon000	Bengaluru	India	NA	NA	Session.End	[redacted]	version 10.16 (build 20b...
Feb 23, 3:04:14 PM	anon000	Bengaluru	India	NA	NA	Session.Logon	[redacted]	version 10.16 (build 20b...
Feb 22, 5:17:30 PM	anon000	Bengaluru	India	NA	NA	Session.End	[redacted]	version 10.16 (build 20b...
Feb 22, 5:17:30 PM	anon000	Bengaluru	India	paint	NA	App.End	[redacted]	version 10.16 (build 20b...
Feb 22, 5:07:31 PM	anon000	Bengaluru	India	paint	NA	App.Start	[redacted]	version 10.16 (build 20b...
Feb 22, 5:07:29 PM	anon000	Bengaluru	India	NA	NA	Session.Logon	[redacted]	version 10.16 (build 20b...

When you see such users, you might want to know:

- Who are these users?
- Are these users legitimate or malicious in nature?
- How to verify them?
- What actions I must apply for these users?

You see anonymous users in your Citrix IT environment in the following scenarios:

- When a user is using a published secure browser app
- When a user is using an unauthenticated store

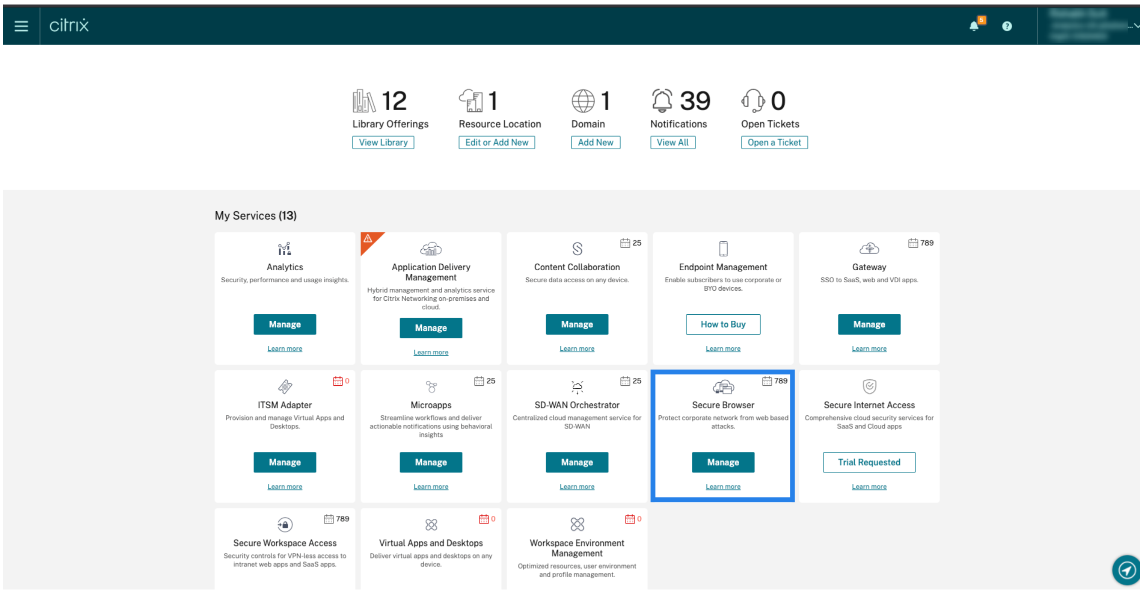
User using published secure browser apps

The secure browser apps are web apps that are published using the Citrix Secure Browser Service. These apps isolate your web browsing events and protect your corporate network from browser-based attacks. For more information, see Secure Browser Service.

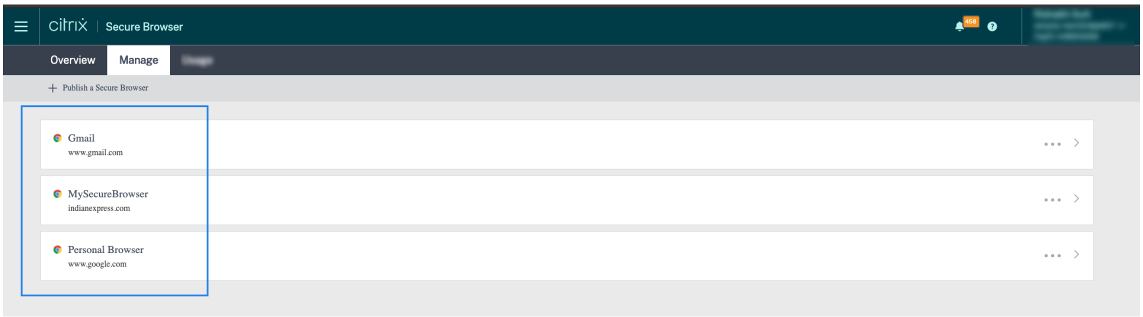
The secure browser apps use the anonymous session capability of Citrix DaaS.

To verify if Secure Browser is configured in your Citrix Cloud account:

1. Sign in to Citrix Cloud.
2. On the **Secure Browser** card, click **Manage**.


citrix
[redacted]
12 Library Offerings View Library
1 Resource Location Edit or Add New
1 Domain Add New
39 Notifications View All
0 Open Tickets Open a Ticket
My Services (13)
Analytics
Security, performance and usage insights.
Manage
Application Delivery Management
Hybrid management and analytics service for Citrix Networking on-premises and cloud.
Manage
Content Collaboration
Secure data access on any device.
Manage
Endpoint Management
Enable subscribers to use corporate or BYO devices.
How to Buy
Gateway
SSO to SaaS, web and VDI apps.
Manage
ITSM Adapter
Provision and manage Virtual Apps and Desktops.
Manage
Microapps
Streamline workflows and deliver actionable notifications using behavioral insights
Manage
SD-WAN Orchestrator
Centralized cloud management service for SD-WAN
Manage
Secure Browser
Protect corporate network from web based attacks.
Manage
Secure Internet Access
Comprehensive cloud security services for SaaS and Cloud apps
Trial Requested
Secure Workspace Access
Security controls for VPN-less access to intranet web apps and SaaS apps.
Virtual Apps and Desktops
Deliver virtual apps and desktops on any device.
Workspace Environment Management
Optimized resources, user environment and profile management.
Learn more

3. On the **Manage** page, check for published secure browser apps.



If a user accesses a StoreFront store through Citrix Receiver for Web sites by using a web browser and uses the published secure browser apps, the user's identity is hidden. Therefore, Citrix Analytics displays the user as anonymous.

If a user accesses a StoreFront store through a Citrix Receiver or Citrix Workspace app that is installed on their device and uses the published secure browser apps, Citrix Analytics displays the user as the user name specified in the StoreFront.

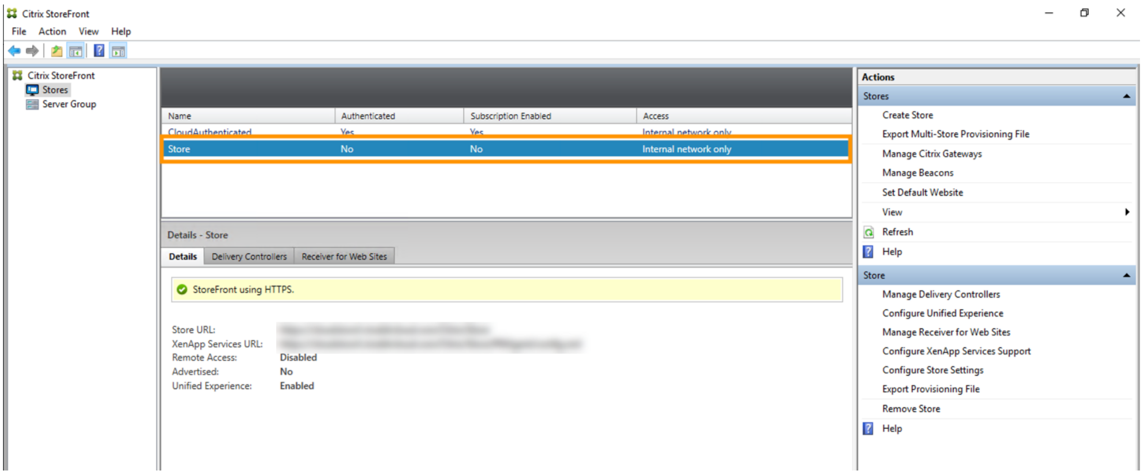
So, you can consider the user as a legitimate user of your organization. You need not apply any action if no risky behavior is associated with the user.

User using an unauthenticated store

The unauthenticated store is a feature of Citrix StoreFront and applies to the stores that are customer managed. This feature support access for unauthenticated (anonymous) users.

To verify if your organization has an unauthenticated store:

1. Launch Citrix Studio.
2. Click **Stores**.
3. For your stores, check the authentication status in the Authenticated column.



Name	Authenticated	Subscription Enabled	Access
CloudAuthenticated	Yes	Yes	Internal network only
Store	No	No	Internal network only

StoreFront using HTTPS.

Store URL: [redacted]
XenApp Services URL: [redacted]
Remote Access: Disabled
Advertised: No
Unified Experience: Enabled

If a store is not authenticated and the user is accessing that unauthenticated store, the user identity remains anonymous. Therefore, Citrix Analytics displays the user as anonymous. You can consider this user as a legitimate user of your organization. You need not apply any action if no risky behavior is associated with the user.

Troubleshoot event transmission issues from a data source

November 30, 2023

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

Checklist

Sequence	Checks
1	Do you have the correct entitlement to use Security Analytics?
2	Is the data source supported in your home region?
3	Does your environment meet all the system requirements?
4	Are all the data sources discovered and data processing enabled on Analytics?
5	Are the user activities on the data source transmitting events accurately to Analytics?
6	Are the virtual apps and desktops events transmitted to Analytics?
7	Are the user events appearing on the self-service search page in Analytics?
8	Are the users discovered by Analytics?

Check 1- Do you have the correct entitlement to use Security Analytics?

Citrix Analytics for Security is a subscription-based offering. For more information, see Getting started.

Check 2- Is the data source supported in your home region?

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

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

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

However, certain data sources are not supported in all home regions. The data sources are the products from which Citrix Analytics for Security receives user events.

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

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

Data source	Supported in US Region	Supported in EU Region	Supported in APS Region
Citrix Endpoint Management	Yes	Yes	Yes
Citrix Gateway (on-premises)	Yes	Yes	Yes
Citrix Identity provider	Yes	Yes	Yes
Citrix Secure Browser	Yes	Yes	Yes
Citrix Secure Private Access	Yes	No	No
Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)	Yes	Yes	Yes
Citrix Virtual Apps and Desktops on-premises	Yes	Yes	Yes
Microsoft Active Directory	Yes	Yes	Yes
Microsoft Graph Security	Yes	Yes	Yes

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

Citrix Analytics can take a few minutes to receive the user events from the data sources. 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, ensure 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. If you do not configure the StoreFront server, Citrix Analytics fails to receive user events from on-premises Citrix Virtual Apps and Desktops. To configure StoreFront deployment, see the Citrix Analytics service article in the StoreFront documentation.
4. The Citrix Virtual Apps and Desktops users and Citrix DaaS users must use the specified version of Citrix Workspace apps or Citrix Receiver on their end points. Otherwise, Analytics does 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 Citrix Virtual Apps and Desktops and Citrix DaaS data source.
5. To receive the users'events from a published Secure Browser session, enable the **Hostname Tracking** setting in the Secure Browser. By default, this setting is disabled. For more information, see Manage published secure browsers.
6. Onboard your data sources as mentioned in the following articles:

    - Citrix Endpoint Management data source
    - Citrix Gateway data source
    - Citrix Secure Private Access data source
    - Citrix Virtual Apps and Desktops and Citrix DaaS data source
    - Microsoft Active Directory integration
    - Microsoft Graph Security integration

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

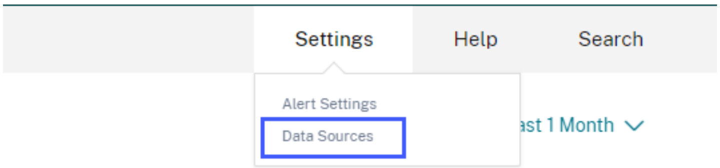
Ensure that all your data sources are discovered and you have enabled data processing for them. If you do not enable data processing for a data source, the users using the data source are not discovered. This situation might create a potential security risk.

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.

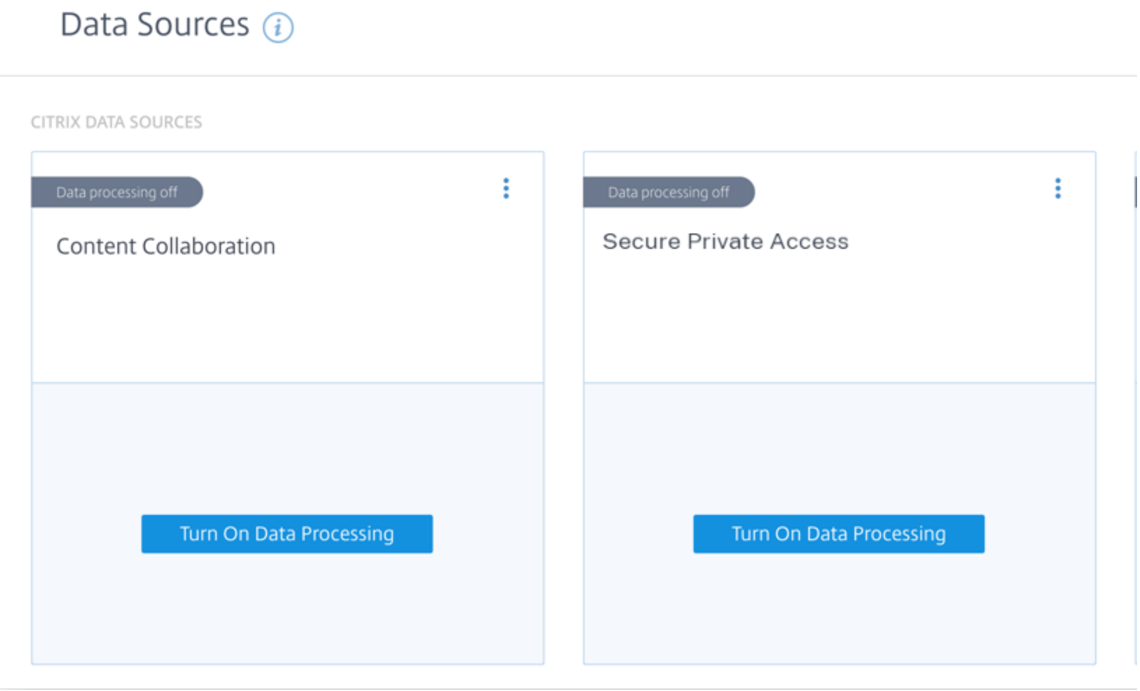
To discover your data sources and enable analytics, do the following:

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

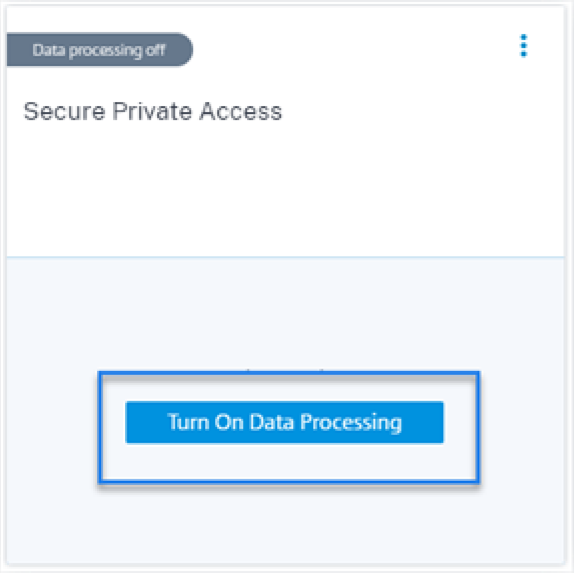


2. On the **Data Sources** page, the discovered data sources appear as site cards. By default, the data processing is off.

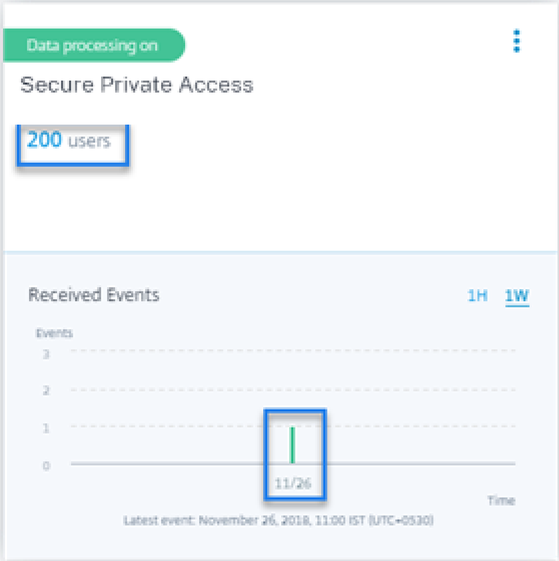
> **Important**
>
> Citrix Analytics processes your data after you have given your consent.



3. Click **Turn On Data Processing** on the site card for which you want Citrix Analytics to process events. For example, on the Citrix Secure Private Access 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. 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 steps specified in Getting started to enable analytics.

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

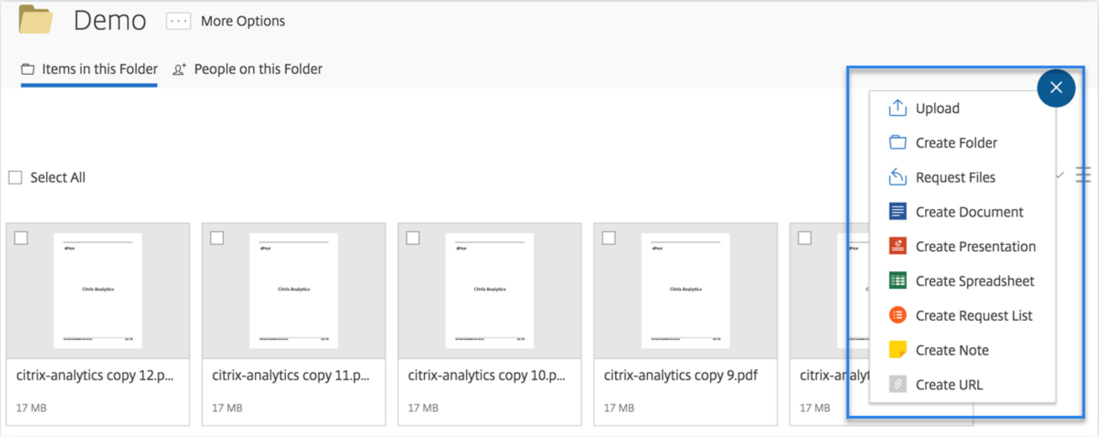
Citrix Analytics receives user events from the data sources when the users are actively using the data sources. The users must perform some activities on the data source to generate events. For example, to receive events from the Apps and Desktops data source, the Apps and Desktops users must share,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

> **Note**
>
> Citrix Analytics does not actively pull data from your environment.

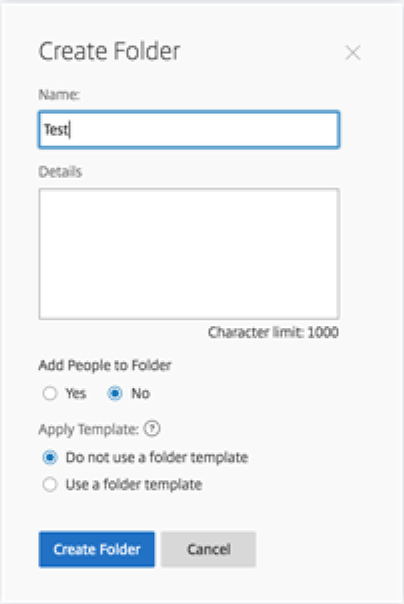
If you do not see any user events in Citrix Analytics for your data source, there is a high probability that the users are not active at that moment.

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

1. Log on to the Citrix Apps and Desktops service.
2. Perform some usual user activities such as create folder, download files, upload files, or delete files.



3. For example, create a Test folder.



Create Folder

Name: Test

Details

Character limit: 1000

Add People to Folder

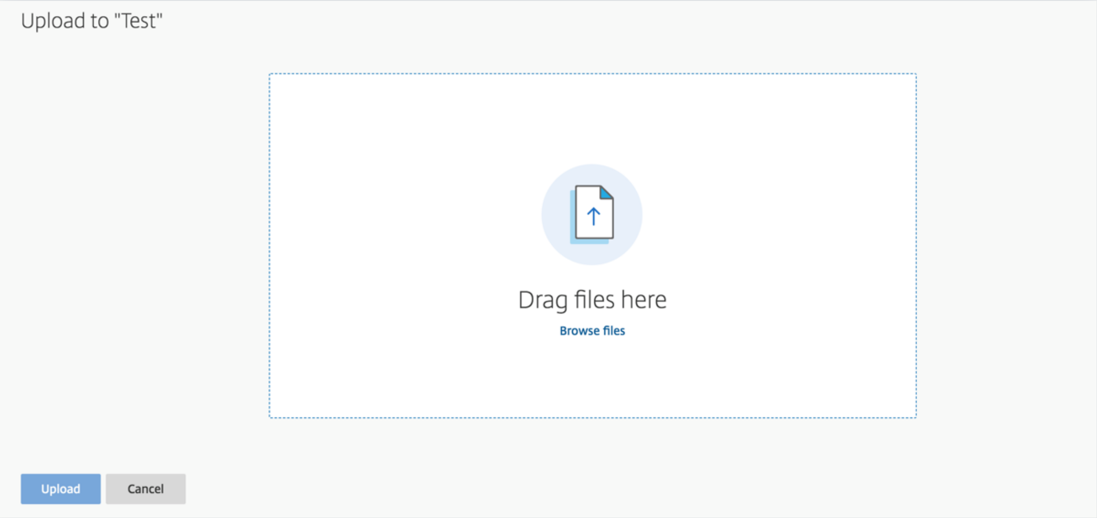
○ Yes ● No

Apply Template:

● Do not use a folder template

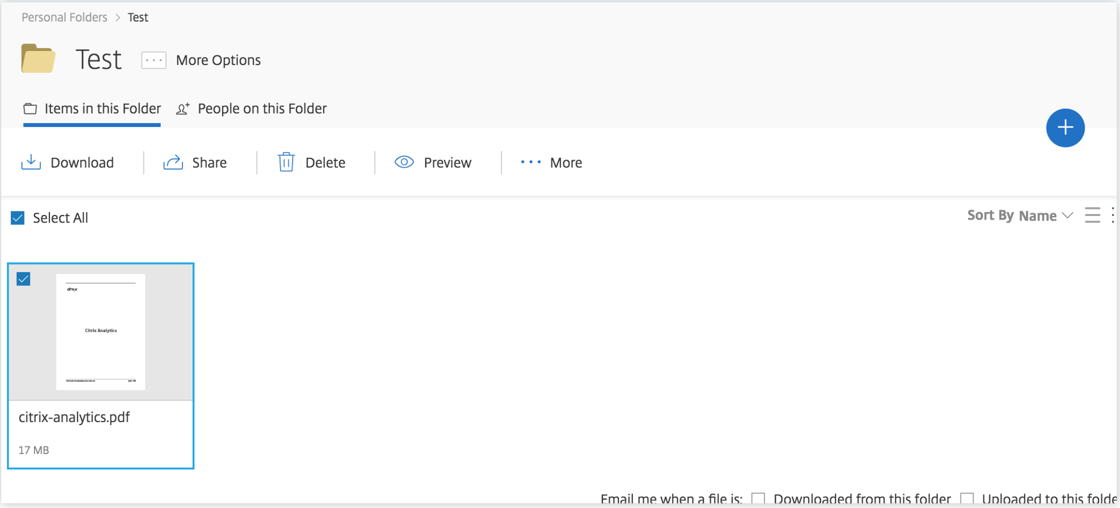
○ Use a folder template

4. Upload some local files.

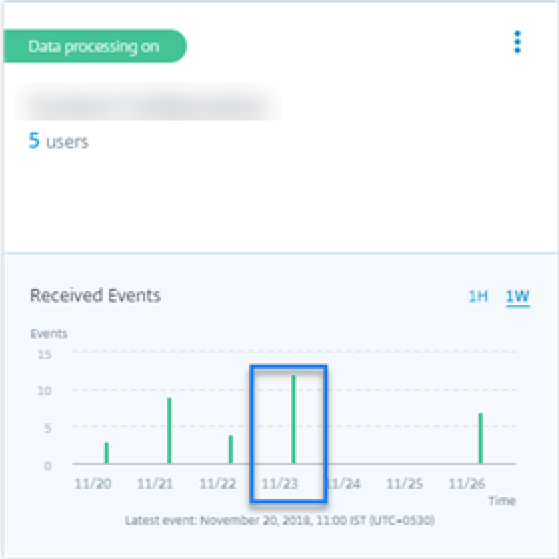


Upload to "Test"

5. Delete some files in the folder.



6. Go back to Citrix Analytics and view the **Apps and Desktops** side card on the Data Source page. Citrix Analytics receives the user events from the Apps and Desktops data source and displays them on the site card.



Check 6: Are the virtual apps and desktops events transmitted to Analytics?

Some versions of the 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 Linux 2006 or later does not send the ***SaaS App Launch*** and ***SaaS App End*** events to Citrix Analytics. A user who launches a SaaS app using the Citrix Workspace app for Linux is not discovered on 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 to the client.

Event	Workspace app for Windows 1907 or later	Workspace app for Mac 1910.2 or later	Workspace app for Linux 2006 or later	Workspace app for Android- Latest version available in Google Play	Workspace app for iOS- Latest version available in Apple App Store	Workspace app for Chrome- Latest version available in Chrome Web Store	Workspace app for HTML5 2007 or later
Account Logon	Yes	Yes	Yes	Yes	Yes	No	No
Session Logon	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Session Launch	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Session End	Yes	Yes	Yes	Yes	Yes	Yes	Yes
App Start	Yes	Yes	Yes	No	Yes	Yes	Yes
App End	Yes	Yes	Yes	No	Yes	Yes	Yes
File Download	Yes	Yes	Yes	No	No	Yes	Yes
Printing	No	Yes	Yes	No	No	Yes	Yes
SaaS App Launch	Yes	Yes	No	No	No	No	No
SaaS App End	Yes	Yes	No	No	No	No	No
SaaS App URL Navigation	Yes	Yes	No	No	No	No	No

Event	Workspace app for Windows 1907 or later	Workspace app for Mac 1910.2 or later	Workspace app for Linux 2006 or later	Workspace app for Android- Latest version available in Google Play	Workspace app for iOS- Latest version available in Apple App Store	Workspace app for Chrome- Latest version available in Chrome Web Store	Workspace app for HTML5 2007 or later
SaaS App Clipboard Access	Yes	Yes	No	No	No	No	No
SaaS App File Download	Yes	Yes	No	No	No	No	No
SaaS App File Print	Yes	Yes	No	No	No	No	No

Based on the event transmission state, you might encounter the following issues:

- When users connect to their Citrix Virtual Apps and Desktops or Citrix DaaS using the clients, the users might not get discovered in Citrix Analytics until they perform an event (activity) that is supported. For example, consider two user events - App Start and SaaS App Launch. A user who is using the Citrix Workspace app for iOS, Citrix Analytics receives the App Start event but not the SaaS App Launch event. So, when the user launches any virtual apps, the App Start event is transmitted to Citrix Analytics and the user is discovered. But if the user launches a SaaS app, Citrix Analytics does not receive the SaaS App Launch event and the user is not discovered. For information on discovered users, see Discovered users.
- Events marked as **No** on the table do not appear on the self-service search page. For information on how to use the self-service page, see About self-service search.

Recommendation

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

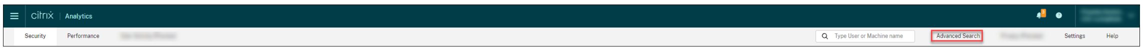
- **Windows user**: Connect to your Citrix Virtual Apps and Desktops and Citrix DaaS using Citrix Workspace app for Windows 1907 or later.

- **Mac user**: Connect to your Citrix Virtual Apps and Desktops and Citrix DaaS using the Citrix Workspace app for Mac 1910.2 or later.

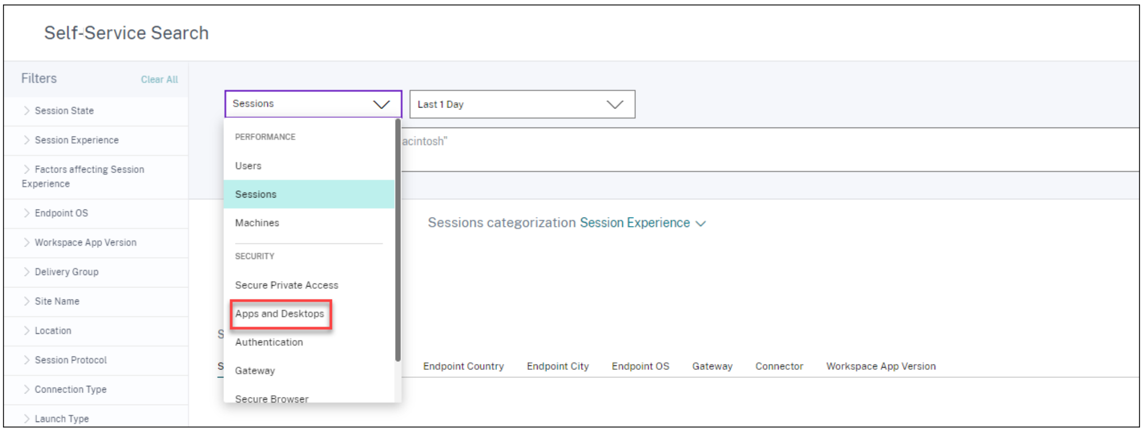
Check 7- Are the user events appearing on the self-service search page in Analytics?

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

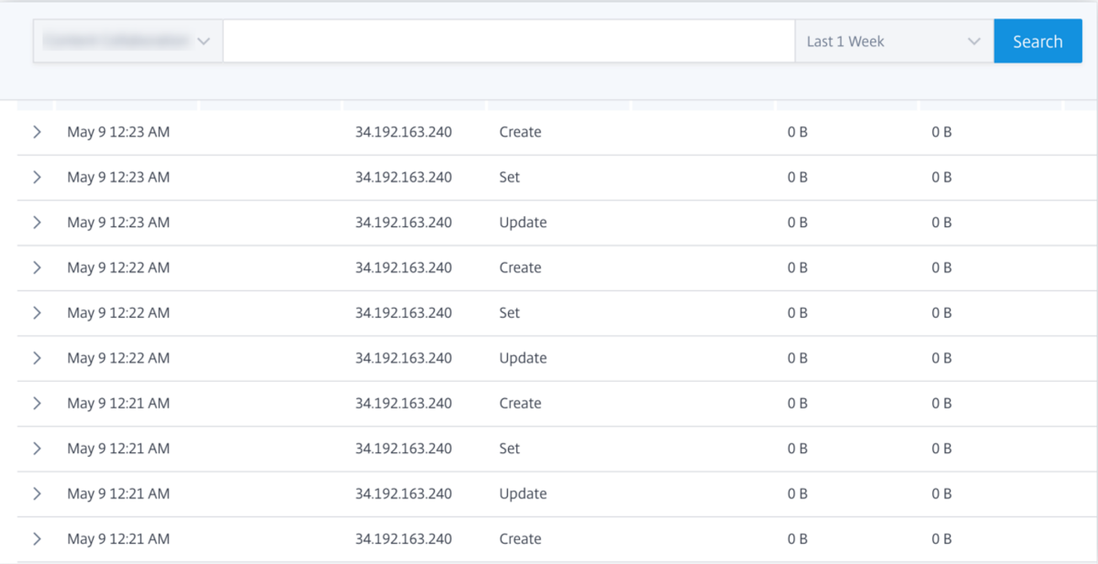
1. On the top bar, click **Advanced Search** to go to the self-service search page.



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



3. To view the data associated with the Apps and Desktops events, select **Apps and Desktops** from the list, select the time period, and then click **Search**.



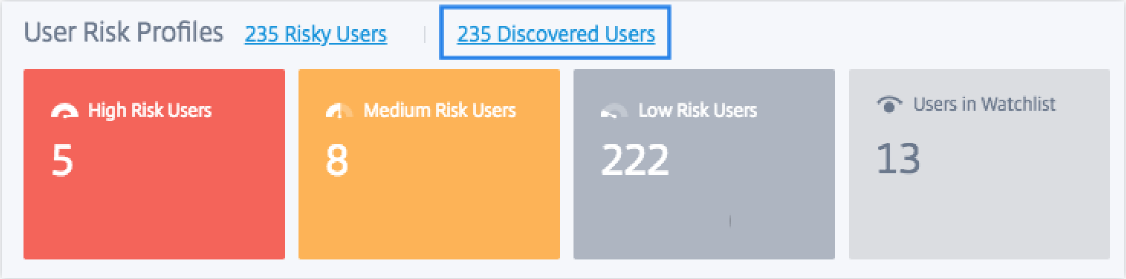
May 9 12:23 AM	34.192.163.240	Create	0 B	0 B
May 9 12:23 AM	34.192.163.240	Set	0 B	0 B
May 9 12:23 AM	34.192.163.240	Update	0 B	0 B
May 9 12:22 AM	34.192.163.240	Create	0 B	0 B
May 9 12:22 AM	34.192.163.240	Set	0 B	0 B
May 9 12:22 AM	34.192.163.240	Update	0 B	0 B
May 9 12:21 AM	34.192.163.240	Create	0 B	0 B
May 9 12:21 AM	34.192.163.240	Set	0 B	0 B
May 9 12:21 AM	34.192.163.240	Update	0 B	0 B
May 9 12:21 AM	34.192.163.240	Create	0 B	0 B

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 process 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.

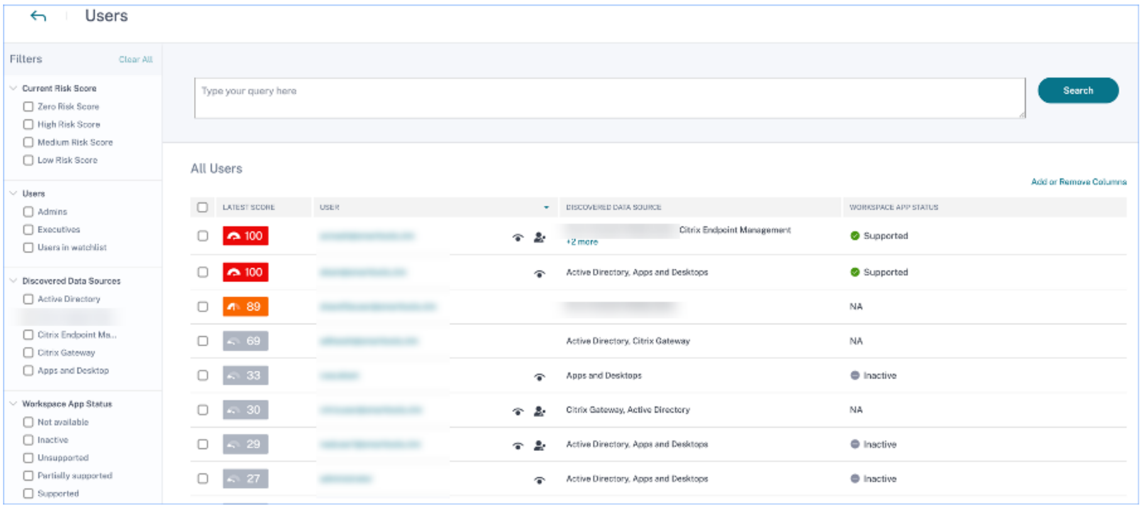


User Risk Profiles 235 Risky Users | 235 Discovered Users

High Risk Users	Medium Risk Users	Low Risk Users	Users in Watchlist
5	8	222	13

2. The **Users** page displays the list of all users discovered for the last 31 days. Select the time period to view the risk indicator occurrences.

> **Note**
>
> If you try to set a value higher than 31 days, the system displays an error message stating - **Invalid date range. The maximum allowed range between the start and the end date is 31 days**.



Users

Filters Clear All

Current Risk Score
☐ Zero Risk Score
☐ High Risk Score
☐ Medium Risk Score
☐ Low Risk Score

Users
☐ Admins
☐ Executives
☐ Users in watchlist

Discovered Data Sources
☐ Active Directory
[redacted]
☐ Citrix Endpoint Ma...
☐ Citrix Gateway
☐ Apps and Desktop

Workspace App Status
☐ Not available
☐ Inactive
☐ Unsupported
☐ Partially supported
☐ Supported

Type your query here

Search

All Users

Add or Remove Columns

☐	LATEST SCORE	USER	DISCOVERED DATA SOURCE	WORKSPACE APP STATUS
☐	100	[redacted]	[redacted] Citrix Endpoint Management +2 more	Supported
☐	100	[redacted]	Active Directory, Apps and Desktops	Supported
☐	89	[redacted]	[redacted]	NA
☐	69	[redacted]	Active Directory, Citrix Gateway	NA
☐	33	[redacted]	Apps and Desktops	Inactive
☐	30	[redacted]	Citrix Gateway, Active Directory	NA
☐	29	[redacted]	Active Directory, Apps and Desktops	Inactive
☐	27	[redacted]	Active Directory, Apps and Desktops	Inactive

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

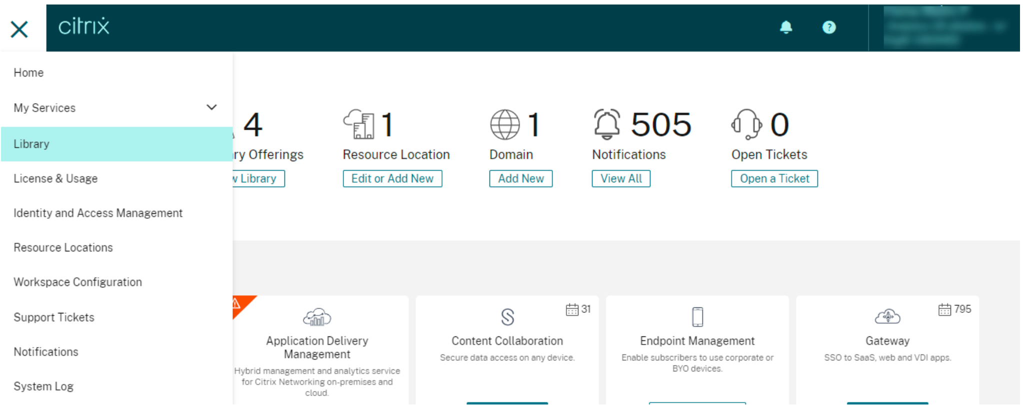
Trigger Virtual Apps and Desktops events, SaaS events, and verifying event transmission

February 21, 2023

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

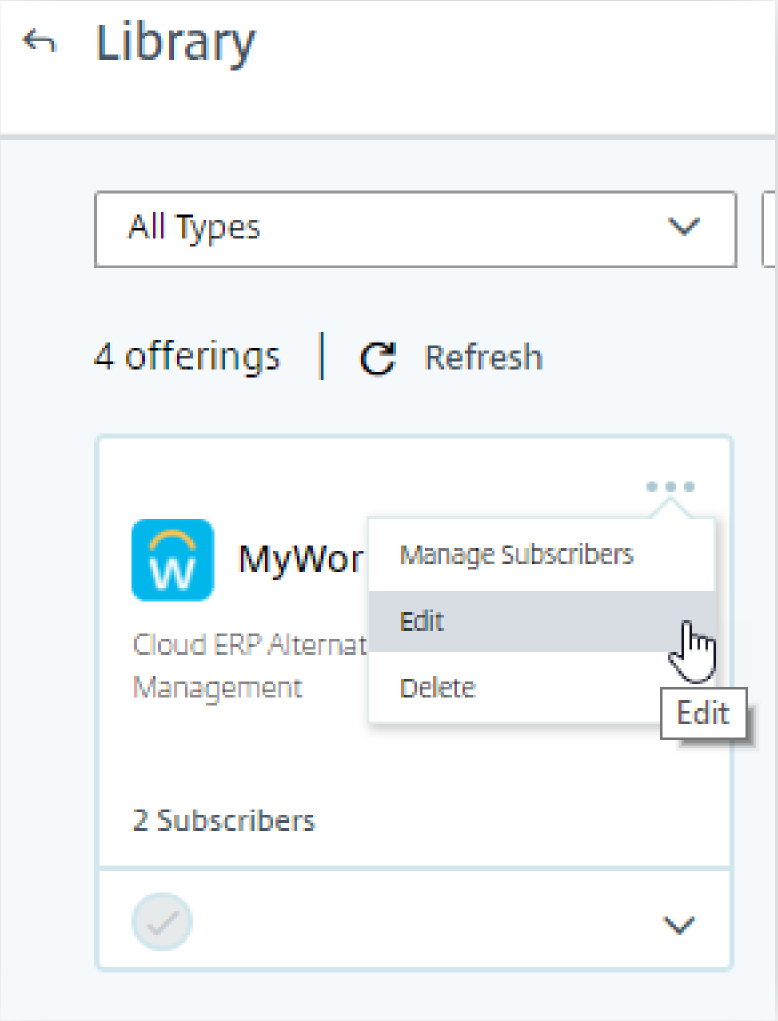
Prerequisites

- If you are using on-premises Citrix Virtual Apps and Desktops, then onboard your on-premises sites to Citrix Analytics, and enable data processing from the site card. If you are using Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), then enable data processing directly from the site card. For more information, see Citrix Virtual Apps and Desktops and Citrix DaaS 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 and Citrix DaaS data source.
- Before triggering the printing event from your virtual desktop, ensure that a printer is configured and provisioned in your 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**.

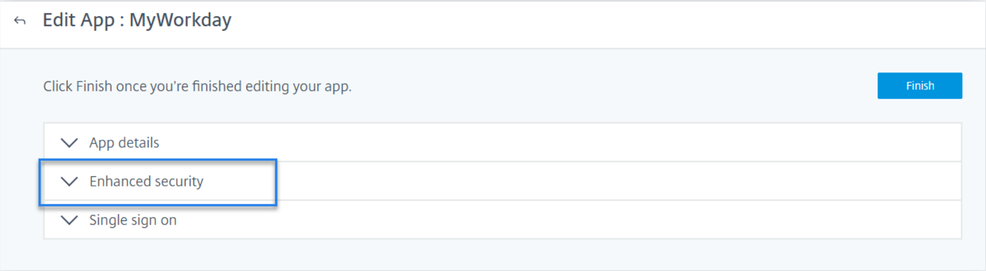


2. On the **Library** page, identify the SaaS app that you want to use for verifying the events. For example, Workday.

3. Click the ellipses, and select **Edit**.



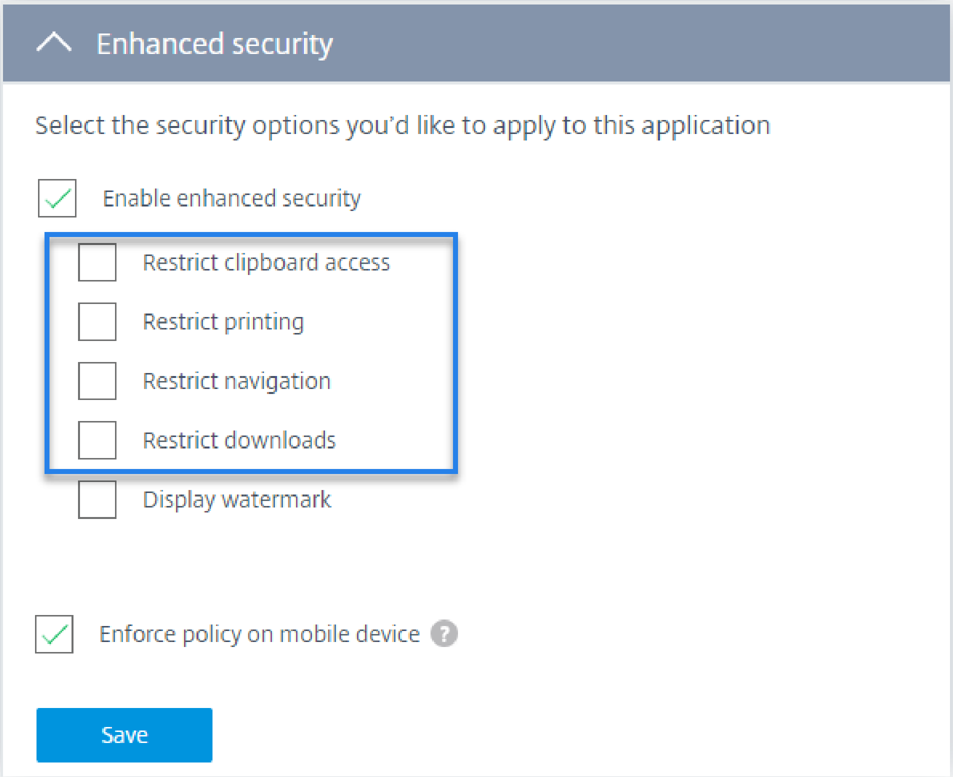
4. On the **Edit App** page, click the down arrow for Enhanced security.



Edit App : MyWorkday

Click Finish once you're finished editing your app.

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



Enhanced security

Select the security options you'd like to apply to this application

☑ Enable enhanced security

□ Restrict clipboard access

□ Restrict printing

□ Restrict navigation

□ Restrict downloads

□ Display watermark

☑ Enforce policy on mobile device

Known issue

Few versions of Citrix Workspace app and Citrix Receiver fail to send some 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.

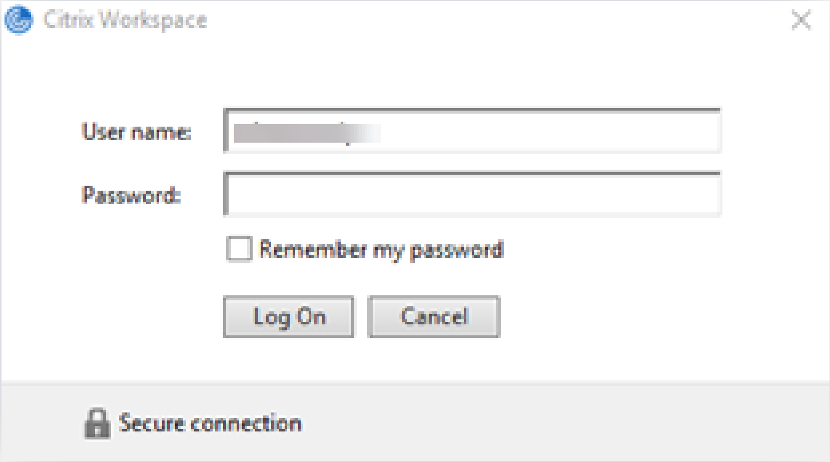
Procedure

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

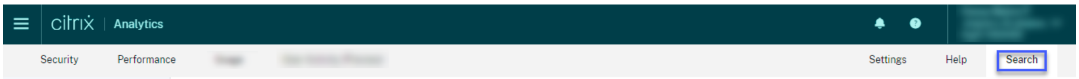
> **Note**
>
> - The events might take some time to reach Citrix Analytics. Refresh the Citrix Analytics page if you do not see the triggered events.
> - For triggering the SaaS events, this procedure uses the Workday app as an example. You can use any configured SaaS apps from your Workspace to trigger the SaaS events.

- **Account Logon**

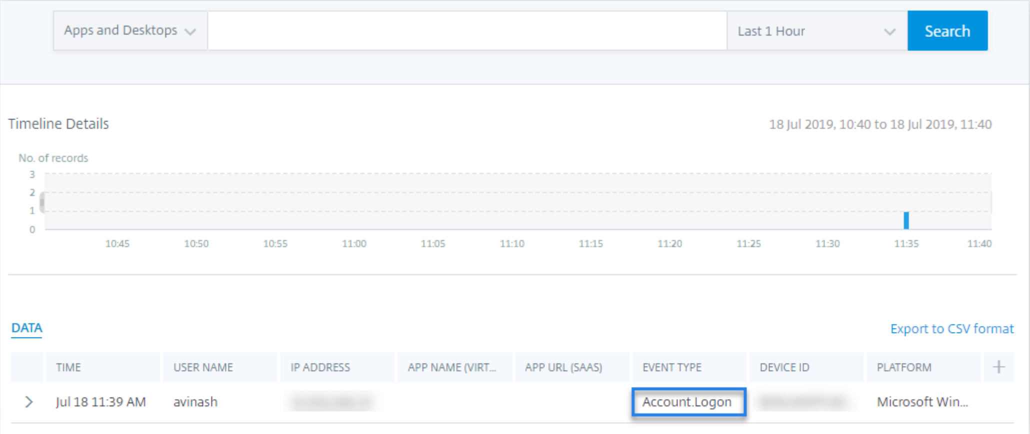
  1. Launch Citrix Workspace app or Citrix Receiver to access your Workspace or StoreFront.
  2. Enter your credentials to log on to the Citrix Workspace app or Citrix Receiver.



  3. Go to Citrix Analytics.
  4. Click **Search** and select **Apps and Desktops** from the list.



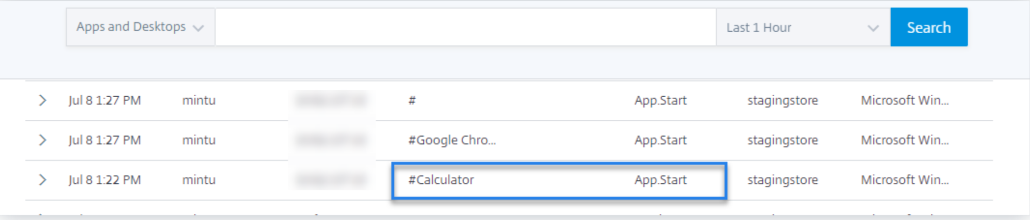
  5. In the search page, view the data for the **Account.Logon** event. Expand the row to view the event details.



TIME	USER NAME	IP ADDRESS	APP NAME (VIRT...	APP URL (SAAS)	EVENT TYPE	DEVICE ID	PLATFORM
Jul 18 11:39 AM	avinash	[redacted]			Account.Logon	[redacted]	Microsoft Win...

- **App Start**

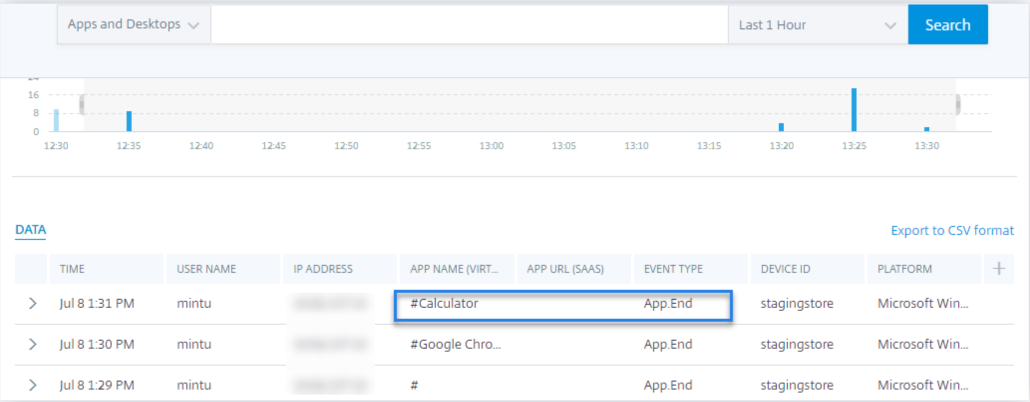
  1. Launch Citrix Workspace app or Citrix Receiver to access your Workspace or StoreFront.
  2. Launch an application such as the calculator.
  3. Go to Citrix Analytics.
  4. Click **Search** and select **Apps and Desktops**.
  5. In the search page, view the data for the **App.Start** event data. Expand the row to view the event details.



Jul 8 1:27 PM	mintu	[redacted]	#	App.Start	stagingstore	Microsoft Win...
Jul 8 1:27 PM	mintu	[redacted]	#Google Chro...	App.Start	stagingstore	Microsoft Win...
Jul 8 1:22 PM	mintu	[redacted]	#Calculator	App.Start	stagingstore	Microsoft Win...

- **App End**

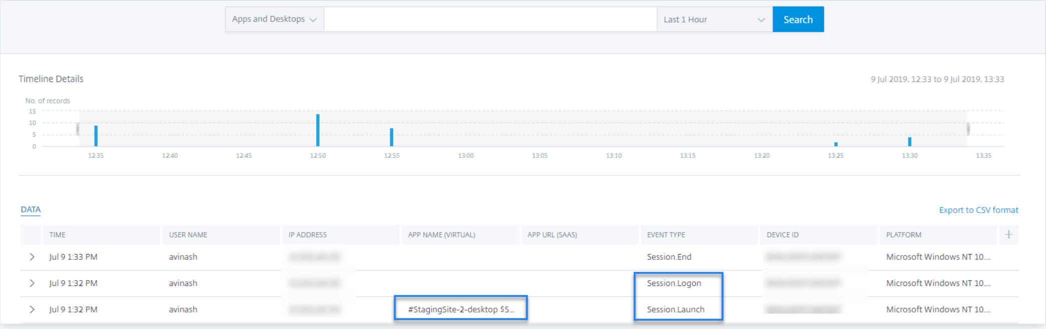
  1. Close the calculator that you have already launched in your Workspace or StoreFront.
  2. Go to Citrix Analytics.
  3. Click **Search** and select **Apps and Desktops**.
  4. In the search page, view the data for the **App.End** event data. Expand the row to view the event details.



TIME	USER NAME	IP ADDRESS	APP NAME (VIRT...	APP URL (SAAS)	EVENT TYPE	DEVICE ID	PLATFORM
Jul 8 1:31 PM	mintu	[redacted]	#Calculator		App.End	stagingstore	Microsoft Win...
Jul 8 1:30 PM	mintu	[redacted]	#Google Chro...		App.End	stagingstore	Microsoft Win...
Jul 8 1:29 PM	mintu	[redacted]	#		App.End	stagingstore	Microsoft Win...

- **Session Logon and Session Launch**

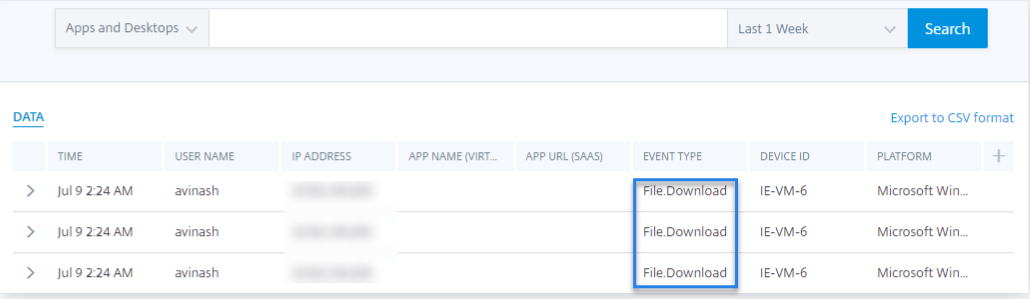
  1. Launch Citrix Workspace app or Citrix Receiver to access your Workspace or StoreFront.
  2. Launch your virtual desktop.
  3. Go to Citrix Analytics.
  4. Click **Search** and select **Apps and Desktops**.
  5. In the search page, view the data for the **Session.Logon** and **Session.Launch** events. Expand the row to view the event details.



TIME	USER NAME	IP ADDRESS	APP NAME (VIRTUAL)	APP URL (SAAS)	EVENT TYPE	DEVICE ID	PLATFORM
Jul 9 1:33 PM	avinash	[redacted]			Session.End	[redacted]	Microsoft Windows NT 10....
Jul 9 1:32 PM	avinash	[redacted]			Session.Logon	[redacted]	Microsoft Windows NT 10....
Jul 9 1:32 PM	avinash	[redacted]	#StagingSite-2-desktop $S...		Session.Launch	[redacted]	Microsoft Windows NT 10....

- **File Download**

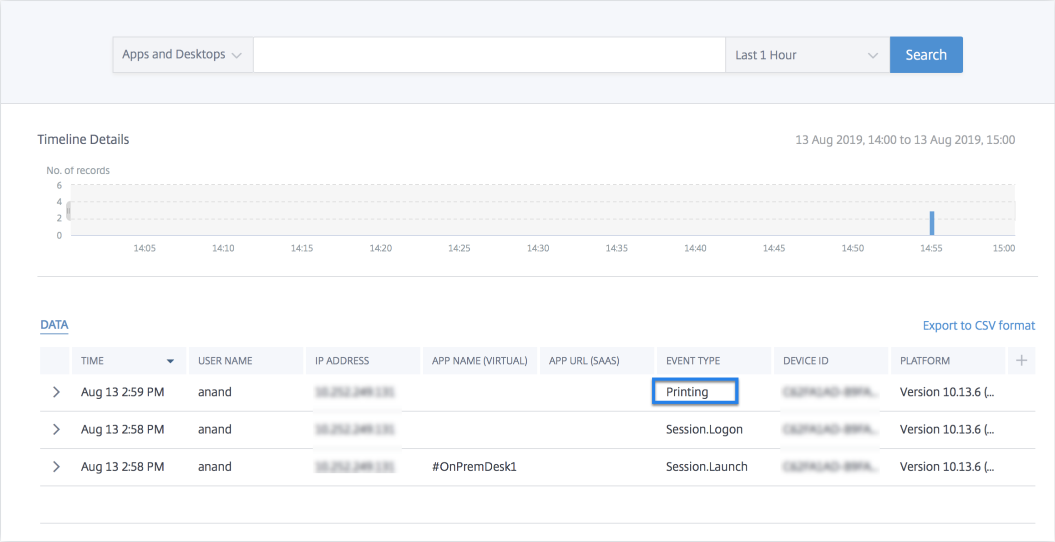
  1. Launch Citrix Workspace app or Citrix Receiver to access your Workspace or StoreFront.
  2. Launch your virtual desktop.
  3. Copy a file from your virtual desktop to your local computer.
  4. Go to Citrix Analytics.
  5. Click **Search** and select **Apps and Desktops**.
  6. In the search page,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



	TIME	USER NAME	IP ADDRESS	APP NAME (VIRT...	APP URL (SAAS)	EVENT TYPE	DEVICE ID	PLATFORM
>	Jul 9 2:24 AM	avinash	[redacted]			File.Download	IE-VM-6	Microsoft Win...
>	Jul 9 2:24 AM	avinash	[redacted]			File.Download	IE-VM-6	Microsoft Win...
>	Jul 9 2:24 AM	avinash	[redacted]			File.Download	IE-VM-6	Microsoft Win...

- **Printing**

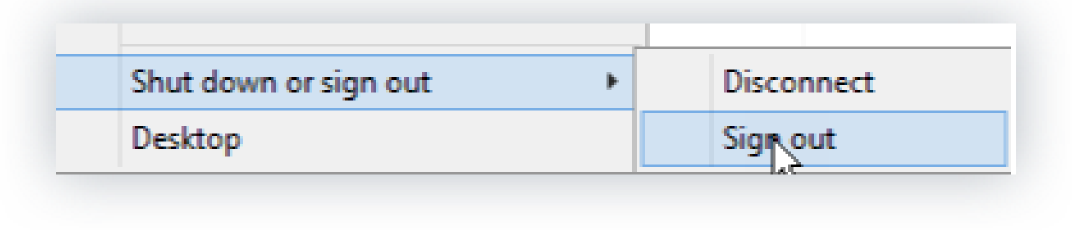
  1. Launch Citrix Workspace app or Citrix Receiver to access Workspace.
  2. Launch your virtual desktop.
  3. Print a document using a printer that is configured with your virtual desktop.
  4. Go to Citrix Analytics.
  5. Click **Search** and select **Apps and Desktops**.
  6. In the Search page, view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



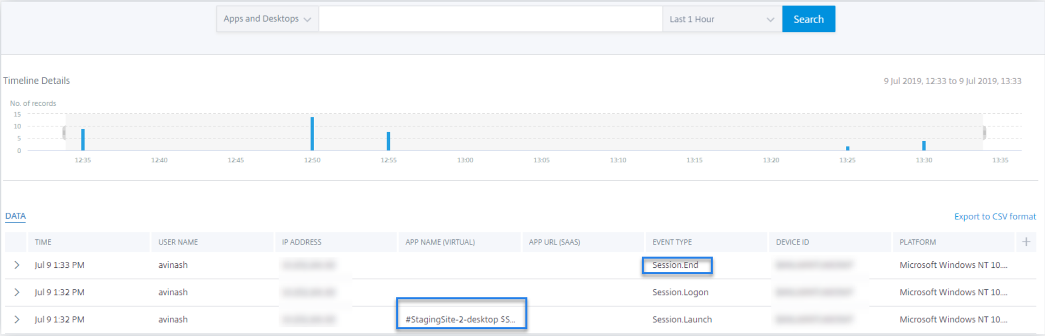
	TIME	USER NAME	IP ADDRESS	APP NAME (VIRTUAL)	APP URL (SAAS)	EVENT TYPE	DEVICE ID	PLATFORM
>	Aug 13 2:59 PM	anand	[redacted]			Printing	[redacted]	Version 10.13.6 (...
>	Aug 13 2:58 PM	anand	[redacted]			Session.Logon	[redacted]	Version 10.13.6 (...
>	Aug 13 2:58 PM	anand	[redacted]	#OnPremDesk1		Session.Launch	[redacted]	Version 10.13.6 (...

- **Session End**

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



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.



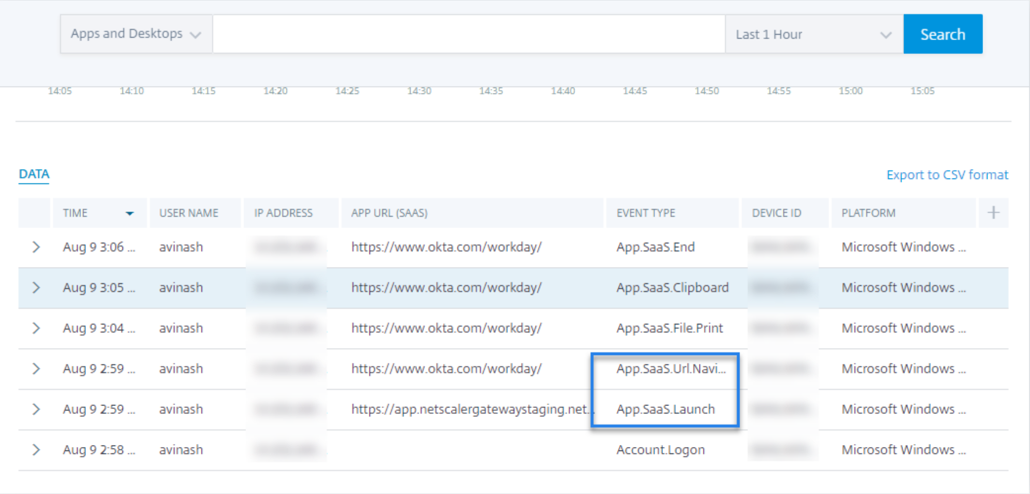
TIME	USER NAME	IP ADDRESS	APP NAME (VIRTUAL)	APP URL (SAAS)	EVENT TYPE	DEVICE ID	PLATFORM
Jul 9 1:33 PM	avinash	[redacted]			Session.End	[redacted]	Microsoft Windows NT 10....
Jul 9 1:32 PM	avinash	[redacted]			Session.Logon	[redacted]	Microsoft Windows NT 10....
Jul 9 1:32 PM	avinash	[redacted]	#StagingSite-2-desktop $S...		Session.Launch	[redacted]	Microsoft Windows NT 10....

- **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.



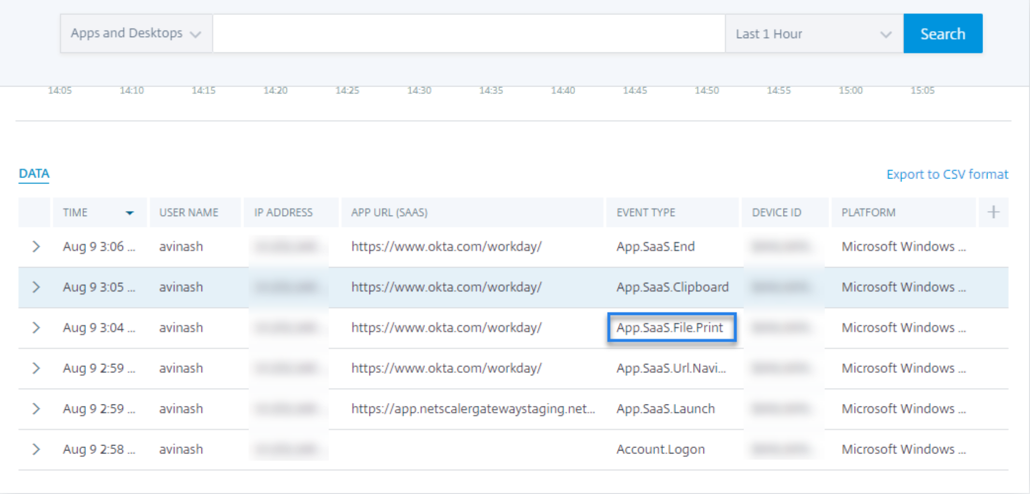
	TIME	USER NAME	IP ADDRESS	APP URL (SAAS)	EVENT TYPE	DEVICE ID	PLATFORM	+
>	Aug 9 3:06 ...	avinash	[redacted]	https://www.okta.com/workday/	App.SaaS.End	[redacted]	Microsoft Windows ...	
>	Aug 9 3:05 ...	avinash	[redacted]	https://www.okta.com/workday/	App.SaaS.Clipboard	[redacted]	Microsoft Windows ...	
>	Aug 9 3:04 ...	avinash	[redacted]	https://www.okta.com/workday/	App.SaaS.File.Print	[redacted]	Microsoft Windows ...	
>	Aug 9 2:59 ...	avinash	[redacted]	https://www.okta.com/workday/	App.SaaS.Url.Navi...	[redacted]	Microsoft Windows ...	
>	Aug 9 2:59 ...	avinash	[redacted]	https://app.netscalergatewaystaging.net...	App.SaaS.Launch	[redacted]	Microsoft Windows ...	
>	Aug 9 2:58 ...	avinash	[redacted]		Account.Logon	[redacted]	Microsoft Windows ...	

- **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.



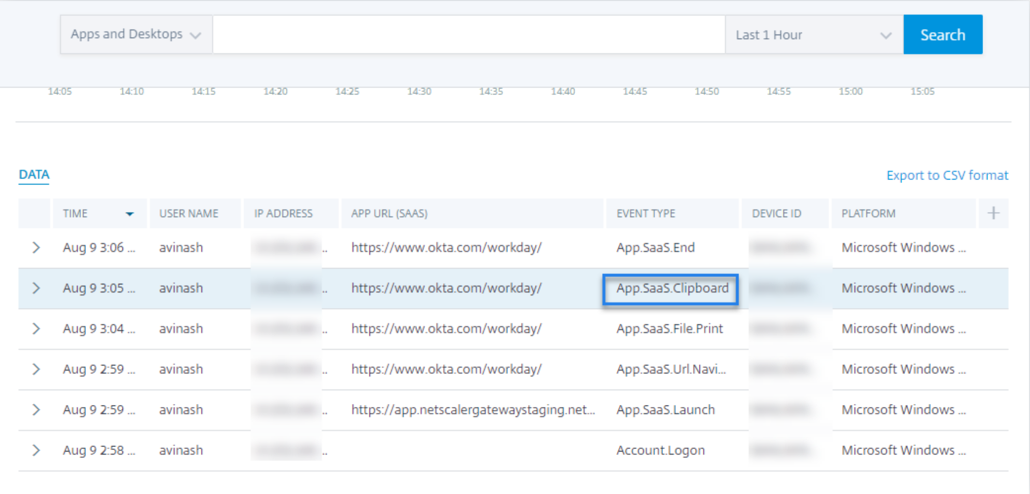
	TIME	USER NAME	IP ADDRESS	APP URL (SAAS)	EVENT TYPE	DEVICE ID	PLATFORM	+
>	Aug 9 3:06 ...	avinash	[redacted]	https://www.okta.com/workday/	App.SaaS.End	[redacted]	Microsoft Windows ...	
>	Aug 9 3:05 ...	avinash	[redacted]	https://www.okta.com/workday/	App.SaaS.Clipboard	[redacted]	Microsoft Windows ...	
>	Aug 9 3:04 ...	avinash	[redacted]	https://www.okta.com/workday/	App.SaaS.File.Print	[redacted]	Microsoft Windows ...	
>	Aug 9 2:59 ...	avinash	[redacted]	https://www.okta.com/workday/	App.SaaS.Url.Navi...	[redacted]	Microsoft Windows ...	
>	Aug 9 2:59 ...	avinash	[redacted]	https://app.netscalergatewaystaging.net...	App.SaaS.Launch	[redacted]	Microsoft Windows ...	
>	Aug 9 2:58 ...	avinash	[redacted]		Account.Logon	[redacted]	Microsoft Windows ...	

- **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.



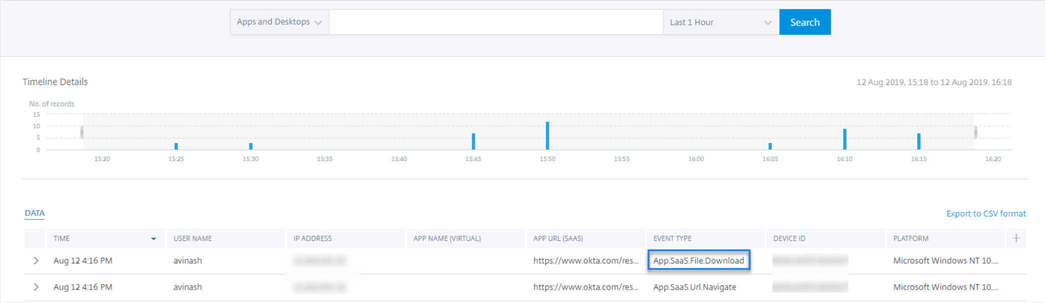
	TIME	USER NAME	IP ADDRESS	APP URL (SAAS)	EVENT TYPE	DEVICE ID	PLATFORM
>	Aug 9 3:06 ...	avinash	[redacted] ..	https://www.okta.com/workday/	App.SaaS.End	[redacted]	Microsoft Windows ...
>	Aug 9 3:05 ...	avinash	[redacted] ..	https://www.okta.com/workday/	App.SaaS.Clipboard	[redacted]	Microsoft Windows ...
>	Aug 9 3:04 ...	avinash	[redacted] ..	https://www.okta.com/workday/	App.SaaS.File.Print	[redacted]	Microsoft Windows ...
>	Aug 9 2:59 ...	avinash	[redacted] ..	https://www.okta.com/workday/	App.SaaS.Url.Navi...	[redacted]	Microsoft Windows ...
>	Aug 9 2:59 ...	avinash	[redacted] ..	https://app.netscalergatewaystaging.net...	App.SaaS.Launch	[redacted]	Microsoft Windows ...
>	Aug 9 2:58 ...	avinash	[redacted] ..		Account.Logon	[redacted]	Microsoft Windows ...

- **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**.

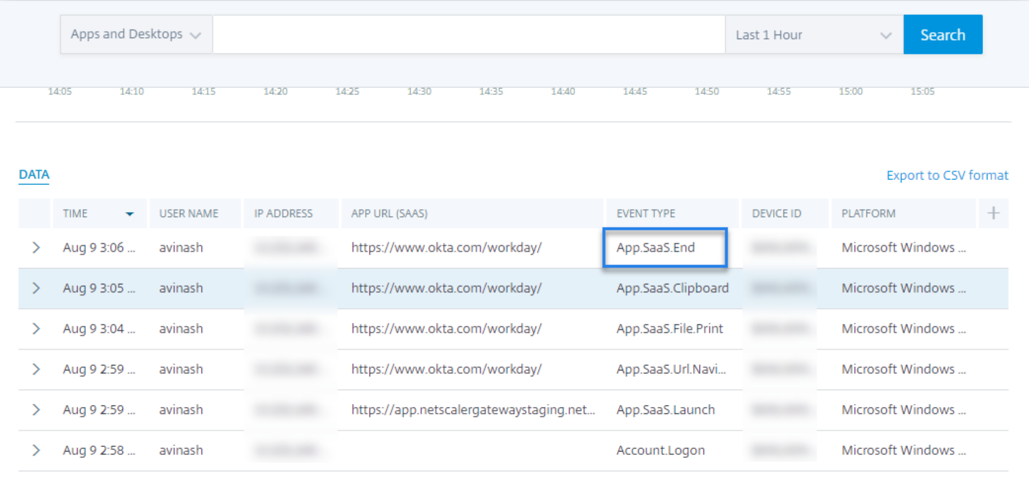
  2. Go to Citrix Analytics.
  3. Click Search and select **Apps and Desktops**.
  4. In the Search page, view the data for the **App.SaaS.File.Download** event. Expand the row to view the event details.



	TIME	USER NAME	IP ADDRESS	APP NAME (VIRTUAL)	APP URL (SAAS)	EVENT TYPE	DEVICE ID	PLATFORM
>	Aug 12 4:16 PM	avinash	[redacted]		https://www.okta.com/res...	App.SaaS.File.Download	[redacted]	Microsoft Windows NT 10....
>	Aug 12 4:16 PM	avinash	[redacted]		https://www.okta.com/res...	App.SaaS.Url.Navigate	[redacted]	Microsoft Windows NT 10....

- **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.



	TIME	USER NAME	IP ADDRESS	APP URL (SAAS)	EVENT TYPE	DEVICE ID	PLATFORM
>	Aug 9 3:06 ...	avinash	[redacted]	https://www.okta.com/workday/	App.SaaS.End	[redacted]	Microsoft Windows ...
>	Aug 9 3:05 ...	avinash	[redacted]	https://www.okta.com/workday/	App.SaaS.Clipboard	[redacted]	Microsoft Windows ...
>	Aug 9 3:04 ...	avinash	[redacted]	https://www.okta.com/workday/	App.SaaS.File.Print	[redacted]	Microsoft Windows ...
>	Aug 9 2:59 ...	avinash	[redacted]	https://www.okta.com/workday/	App.SaaS.Url.Navi...	[redacted]	Microsoft Windows ...
>	Aug 9 2:59 ...	avinash	[redacted]	https://app.netscalergatewaystaging.net...	App.SaaS.Launch	[redacted]	Microsoft Windows ...
>	Aug 9 2:58 ...	avinash	[redacted]		Account.Logon	[redacted]	Microsoft Windows ...

- **VDA.Print**

  Prerequisites

  Before triggering the print event, see Enabling print telemetry for Citrix DaaS.

  To trigger a print event, perform the following actions:

  1. Open a text document with notepad or any other app where print is allowed.
  2. Click **File > Print** or press **Ctrl + P**.
  3. In Select printer, choose your printer, then click **Apply**, and then print.

- **VDA.Clipboard**

Prerequisites

Before triggering the print event, see Enabling clipboard telemetry for Citrix DaaS.

To trigger a clipboard event, perform the following actions:

1. Open a text document with notepad or any text editor.
2. Select the content to copy.
3. Right click copy or press Ctrl+c.

Configured Session Recording server fails to connect

June 2, 2022

Your Session Recording server fails to connect to Citrix Analytics after configuration. Therefore, you don't see the configured server on the **Session Recording** site card.

To troubleshoot this issue, do the following:

1. On your configured Session Recording server, run the following PowerShell command to check the Client Machine Identification (CMID).

   ```
   Get-WmiObject -class SoftwareLicensingService | select
       Clientmachineid
   ```

2. If CMID is empty, add the following registry files in the specified paths.

Registry name	Registry path	Key type	Value
AuditorUniqueID	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\	String	Enter your UUID.
EnableCASUseAuditorUniqueID	Computer/HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/SmartAuditor/Server/	REG_DWORD	1

3. Restart the following services:

    - Citrix Session Recording Analytics Service
    - Citrix Session Recording Storage Manager

Configuration issues with Citrix Analytics add-on for Splunk

June 2, 2022

Citrix Analytics add-on settings unavailable

After installing Citrix Analytics Add-on for Splunk on your Splunk Forwarder or Splunk Standalone environment, you don't see the **Citrix Analytics Add-on** settings under **Settings > Data inputs**.

Reason

This issue occurs when you install Citrix Analytics Add-on for Splunk in an unsupported Splunk environment.

Fixes

Install the Citrix Analytics Add-on for Splunk in a supported Splunk environment. For information on the supported versions, see Splunk integration.

No data available on Splunk dashboards

After installing and configuring Citrix Analytics Add-on for Splunk on your Splunk Forwarder or Splunk Standalone environment, you don't see any data from Citrix Analytics in your Splunk dashboards.

Checks

To troubleshoot the issue, verify the following on your Splunk Forwarder or Splunk Standalone environment:

1. Ensure that the prerequisites for the Splunk integration are met.
2. Go to **Settings > Data inputs > Citrix Analytics Add-on**. Ensure that the Citrix Analytics configuration details are available.

3. If the configuration details are available, run the following query to check the logs for any errors related to Citrix Analytics add-on for Splunk:

```
index=_internal sourcetype=splunkd log_level=ERROR component=
    ExecProcessor cas_siem_consumer
```

4. If you don't find any errors, Citrix Analytics add-on for Splunk is working as expected. If you find any errors in the logs, it might be because of one of the following reasons:

   - Failed to established connection between your Splunk environment and Citrix Analytics Kafka endpoints. This issue might be because of the firewall settings.

     Fixes: Check with your network administrator to resolve this issue.

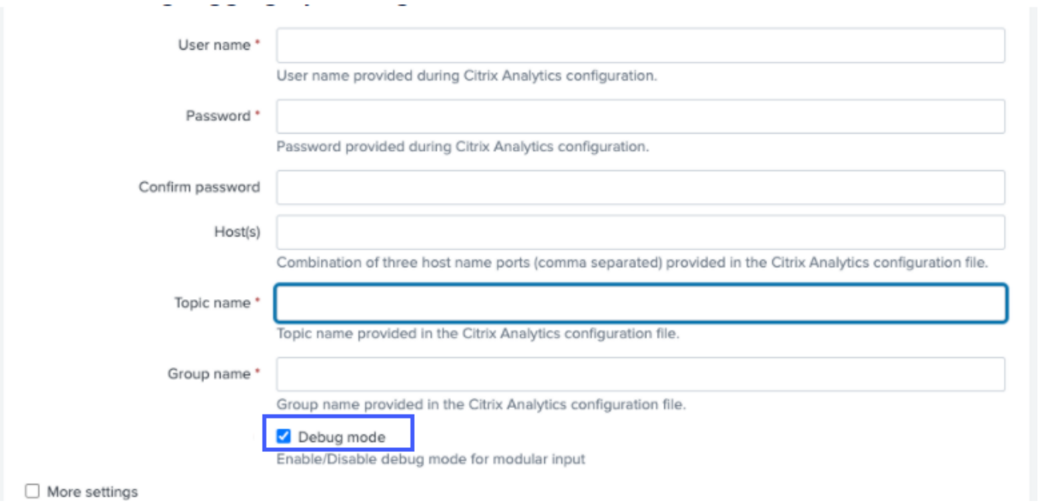
   - Incorrect configuration details in **Settings > Data inputs > Citrix Analytics Add-on**.

     Fixes: Ensure that the Citrix Analytics configuration details such as user name, password, host endpoints, topic, and consumer group are correctly entered as per the Citrix Analytics configuration file. For more information, see Configure Citrix Analytics add-on for Splunk.

5. If you are unable to find the cause of the issue from the preceding logs and want to investigate further:

   a) Enable the **Debug mode** in **Settings > Data inputs > Citrix Analytics Add-on**.

   > Note
   >
   > By default, the **Debug mode** is disabled. Enabling this mode generates too many logs. So, use this option only when required and disable it after completing your debugging task.



User name *

User name provided during Citrix Analytics configuration.

Password *

Password provided during Citrix Analytics configuration.

Confirm password

Host(s)

Combination of three host name ports (comma separated) provided in the Citrix Analytics configuration file.

Topic name *

Topic name provided in the Citrix Analytics configuration file.

Group name *

Group name provided in the Citrix Analytics configuration file.

☑ Debug mode

Enable/Disable debug mode for modular input

☐ More settings

   b) Locate the generated debug logs at the following location and check for any errors:

```
$SPLUNK_HOME$/var/log/splunk.Filename
    splunk_citrix_analytics_add_on_debug_connection.log
```

c) (Optional) Use the debug script `splunk cmd python cas_siem_consumer_debug.py` that is available with Citrix Analytics add-on for Splunk. This script generates a log file that contains the details of your Splunk environment and the connectivity checks. You can use the details to debug the issue. Run the script using the following command:

```
cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin/; /opt/splunk/bin/
    splunk cmd python cas_siem_consumer_debug.py
```

Error message

In the logs related to Citrix Analytics add-on for Splunk, you might see the following error:

`ERRORKafkaError{ code=_TRANSPORT,val=-195,str="Failed to get metadata: Local: Broker transport failure"}`

This error is because of either a network connectivity issue or an authentication issue.

To debug the issue:

1. On your Splunk Forwarder or Splunk Standalone environment, enable the **Debug mode** to get the debug logs. Refer to the preceding step 5.a.
2. Run the following query to find any authentication issues in the debug logs:

   ```
   index=_internal source="*
       splunk_citrix_analytics_add_on_debug_connection.log*" "
       Authentication failure"
   ```

3. If you don't find any authentication issues in the debug logs, the error is because of a network connectivity issue.
4. Find and resolve the issue by using telnet or the debug script mentioned in the preceding step 5.c.

Add-on upgrade fails from a version earlier than 2.0.0

On your Splunk Forwarder or Splunk Standalone environment, when you upgrade Citrix Analytics add-on for Splunk to the latest version from a version earlier than 2.0.0, the upgrade fails.

Fixes

1. Delete the following files and folders located within the `/bin` folder of the Citrix Analytics add-on for Splunk installation folder:

   - `cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin`

- `rm -rf splunklib`
- `rm -rf mac`
- `rm -rf linux_x64`
- `rm CARoot.pem`
- `rm certificate.pem`

2. Restart your Splunk Forwarder or Splunk Standalone environment.

Unable to connect StoreFront server with Citrix Analytics

December 20, 2022

After importing the configuration settings from Citrix Analytics to your StoreFront server, the StoreFront server fails to connect to Citrix Analytics.

For information on how to import configuration settings to a StoreFront server, see Onboard Virtual Apps and Desktops sites using StoreFront.

The CAS Onboarding Assistant helps check and troubleshoot the issues described in this article. For more information, see Citrix Analytics Service (CAS) Onboarding Assistant.

To troubleshoot the issue, do the following:

1. On the StoreFront server, ping the region-specific endpoints of Citrix Analytics to test connectivity between the StoreFront server and the Citrix Analytics server. Also, ensure that the prerequisites are met.

   > **Note**
   >
   > On your StoreFront server, you can test the connectivity by directly pinging the region-specific endpoints or by opening a web browser and accessing the region-specific endpoints.

2. Enable verbose logging in the StoreFront server to trace the logs. For more information on verbose logging, see the article- CTX139592.
3. Open the Internet Information Services (IIS) Manager and check the following:

   - If the StoreFront site is under IIS default site, then IIS restarts the StoreFront site.
   - If the StoreFront site is in other drivers or not under default site, then open the command window and type `iisreset`.

4. Run the following command to import the Citrix Analytics settings:

   ```
   Import-STFCasConfiguration -Path "configuration file path"
   ```

5. Run the following command to verify the imported settings:

   ```
   Get-STFCasConfiguration
   ```

6. If the StoreFront site is in other drivers or not under the default site, open the command window. Type `iisreset` to let StoreFront site read Citrix Analytics settings.
7. Get the StoreFront verbose log files from the following location:

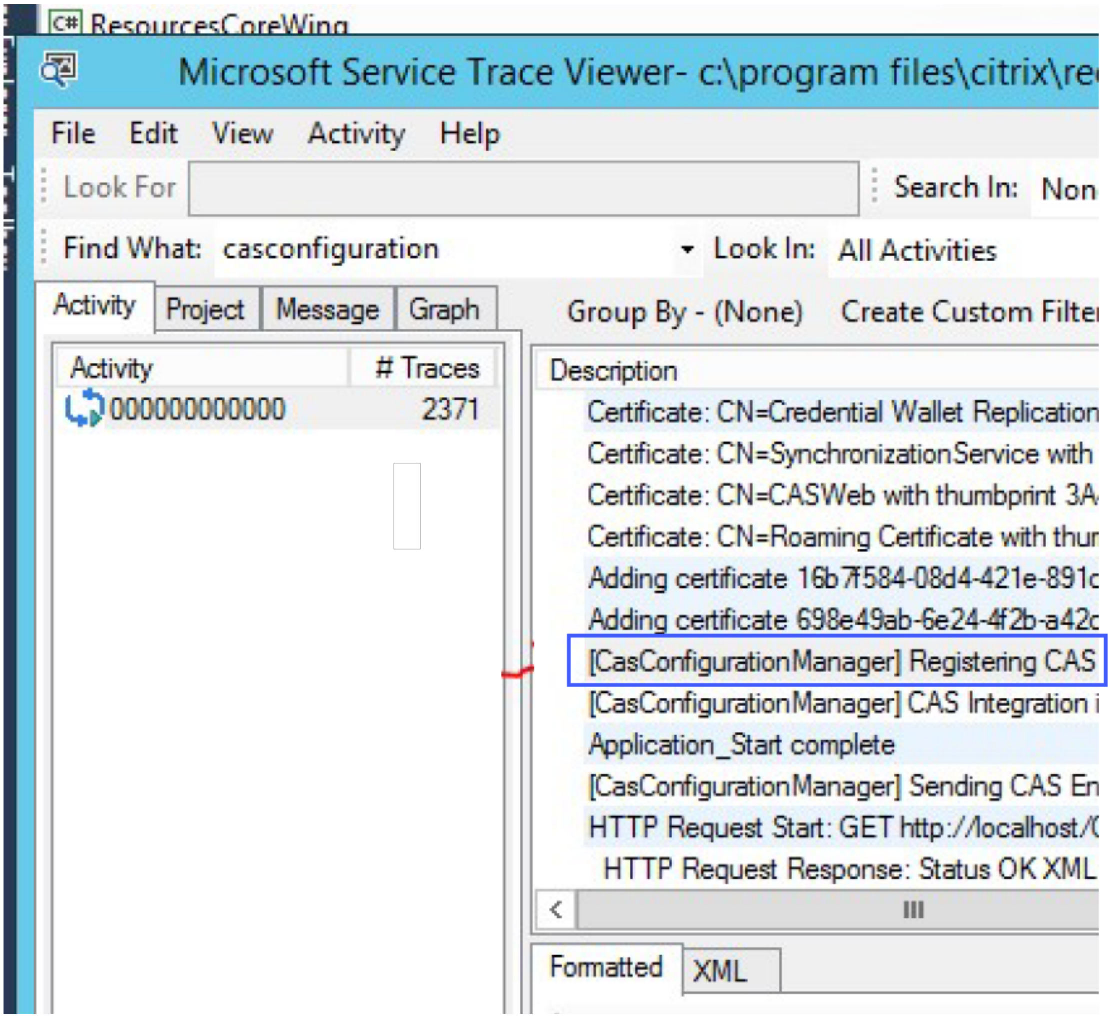
   ```
   C:\Program Files\Citrix\Receiver StoreFront\Admin\trace
   ```

   Under the above mentioned location, you can find multiple svclog files which can be opened in Event Viewer.

8. Use the Microsoft Service Trace Viewer to open the following logs:

   - StoreFront logs
   - Roaming site verbose logs

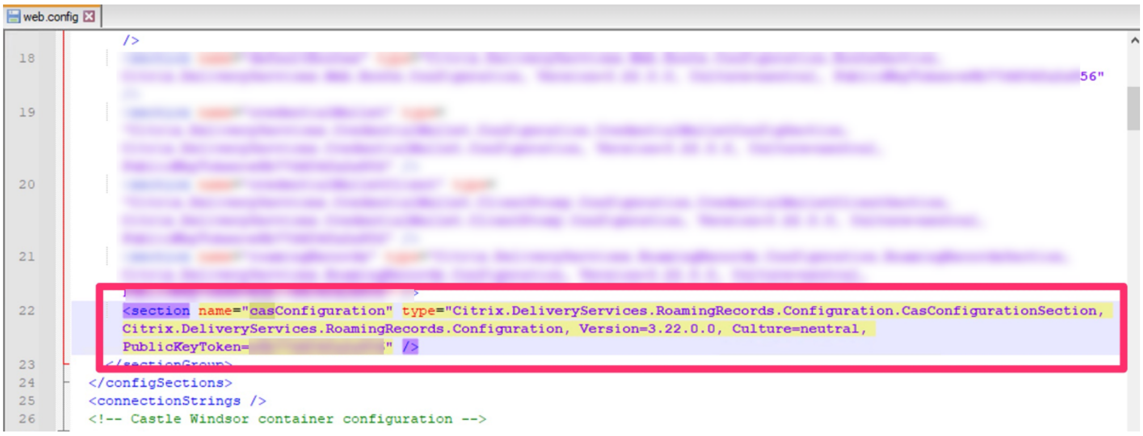
9. In the logs, ensure that the **CasConfigurationManager** sections and Citrix Analytics server information are available.



```
Certificate: CN=Credential Wallet Replication
Certificate: CN=SynchronizationService with
Certificate: CN=CASWeb with thumbprint 3A
Certificate: CN=Roaming Certificate with thur
Adding certificate 16b7f584-08d4-421e-891c
Adding certificate 698e49ab-6e24-4f2b-a42c
[CasConfigurationManager] Registering CAS
[CasConfigurationManager] CAS Integration i
Application_Start complete
[CasConfigurationManager] Sending CAS En
HTTP Request Start: GET http://localhost/(
HTTP Request Response: Status OK XML
```

10. If the CasConfigurationManager sections are unavailable, open the web.config file for the roaming site found in the `roaming site\folder`.

11. In the `web.config` file, locate the **casConfiguration** section and ensure that the Citrix Analytics server information is available.



```
            />
            [redacted]56"
            <section name="casConfiguration" type="Citrix.DeliveryServices.RoamingRecords.Configuration.CasConfigurationSection,
            Citrix.DeliveryServices.RoamingRecords.Configuration, Version=3.22.0.0, Culture=neutral,
            PublicKeyToken=[redacted]" />
          </sectionGroup>
        </configSections>
        <connectionStrings />
        <!-- Castle Windsor container configuration -->
```

12. On the Windows Server machines where the StoreFront server is installed, ensure the following:

- TLS 1.2 Client is enabled.
- At least one of the following cipher suites is enabled:
  - `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
  - `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
  - `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384`
  - `TLS_DHE_RSA_WITH_AES_128_GCM_SHA256`

For information on how to configure the TLS cipher suite order, see the Microsoft documentation.

13. If you are using Windows Server 2012 machines, ensure that the Diffie-Hellman Exchange (ECDHE/DHE) is enabled.
14. Ensure that the Windows Server machines where the StoreFront server is installed must contain the registry settings mentioned in the Microsoft documentation.

> **IMPORTANT**
>
> Update the TLS/SSL cipher suites by using group policy. Do not manually modify the TLS/SSL cipher suites. For more information on how to use group policy, see the Microsoft documentation.

For example, the following registry settings must be available in your Windows Server machine:

TLS 1.2 Client:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"Enabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000

<!--NeedCopy-->
```

Diffie-Hellman KEAs:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

AES-128/AES-256 ciphers:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

SHA256/SHA384 hashes:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA256]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA384]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

FAQs

October 4, 2023

Data source

What is a data source?

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

Learn more: Data Source

How do I add a data source?

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

Citrix ADM agent

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

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

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

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

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

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

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

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

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

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

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

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

How do I get a new activation code?

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

Can I reuse my activation code with multiple agents?

No, you cannot.

How many Citrix ADM agents do I need to install?

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

How do I install multiple Citrix ADM agents?

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

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

Can I install two agents in a high availability setup?

No, you cannot.

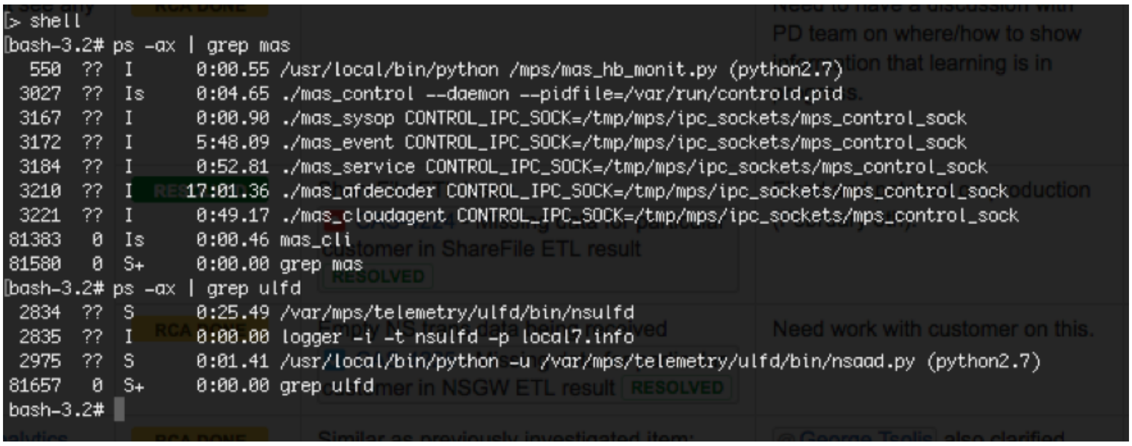
What do I do if my agent registration fails?

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

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

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

- After the agent is successfully registered, access Citrix ADM and navigate to **Networks > Agents**. You can view the discovered agents on this page. If the agent is running fine, the status is indicated by a green icon. If it is not running, the state is indicated by a red icon.
- Log on to the agent's shell prompt and run the following commands: `ps -ax | grep mas` and `ps -ax | grep ulfd`. Ensure that the following processes are running.



```
> shell
bash-3.2# ps -ax | grep mas
  550  ??  I       0:00.55 /usr/local/bin/python /mps/mas_hb_monit.py (python2.7)
 3027  ??  Is      0:04.65 ./mas_control --daemon --pidfile=/var/run/controld.pid
 3167  ??  I       0:00.90 ./mas_sysop CONTROL_IPC_SOCK=/tmp/mps/ipc_sockets/mps_control_sock
 3172  ??  I       5:48.09 ./mas_event CONTROL_IPC_SOCK=/tmp/mps/ipc_sockets/mps_control_sock
 3184  ??  I       0:52.81 ./mas_service CONTROL_IPC_SOCK=/tmp/mps/ipc_sockets/mps_control_sock
 3210  ??  I      17:01.36 ./mas_afdecoder CONTROL_IPC_SOCK=/tmp/mps/ipc_sockets/mps_control_sock
 3221  ??  I       0:49.17 ./mas_cloudagent CONTROL_IPC_SOCK=/tmp/mps/ipc_sockets/mps_control_sock
81383   0  Is      0:00.46 mas_cli
81580   0  S+      0:00.00 grep mas
bash-3.2# ps -ax | grep ulfd
 2834  ??  S       0:25.49 /var/mps/telemetry/ulfd/bin/nsulfd
 2835  ??  I       0:00.00 logger -i -t nsulfd -p local7.info
 2975  ??  S       0:01.41 /usr/local/bin/python -u /var/mps/telemetry/ulfd/bin/nsaad.py (python2.7)
81657   0  S+      0:00.00 grep ulfd
bash-3.2# 
```

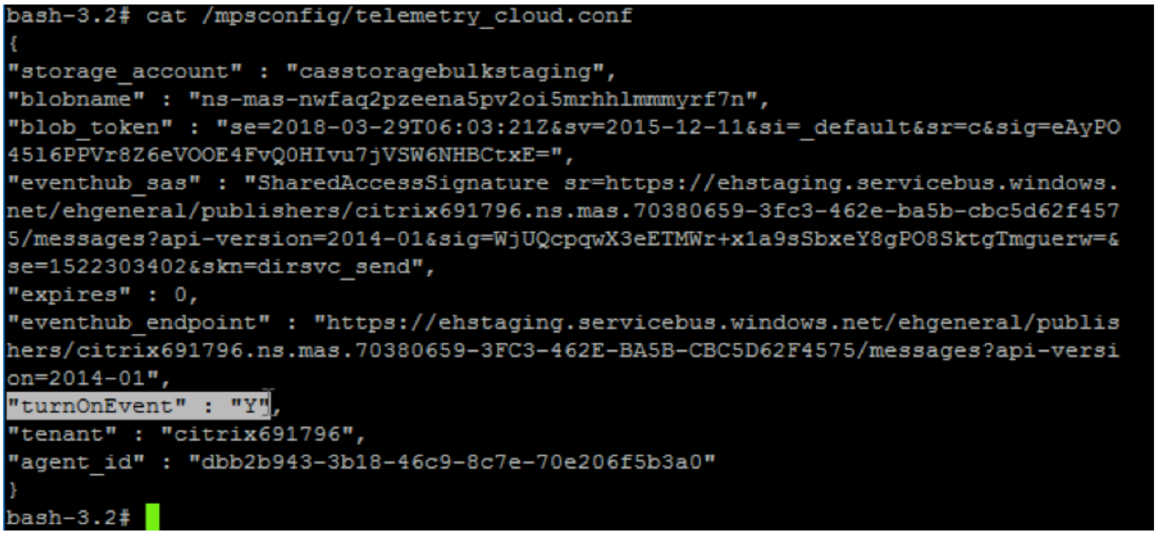
- If any of the processes is not running, run the command **masd restart**. This might take some time to start all the daemons (1 minute or so).
- Make sure `agent.conf` is created in `/mpsconfig` after successful registration of agent.

Onboarding Citrix Gateway instances

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

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

Log on to the agent's shell prompt and run the following command: cat `/mpsconfig/telemetry_cloud.conf` and verify the value of the `turnOnEvent` parameter.



```
bash-3.2# cat /mpsconfig/telemetry_cloud.conf
{
"storage_account" : "casstoragebulkstaging",
"blobname" : "ns-mas-nwfaq2pzeena5pv2oi5mrhhlmmmyrf7n",
"blob_token" : "se=2018-03-29T06:03:21Z&sv=2015-12-11&si=_default&sr=c&sig=eAyPO
4516PPVr8Z6eVOOE4FvQ0HIvu7jVSW6NHBCtxE=",
"eventhub_sas" : "SharedAccessSignature sr=https://ehstaging.servicebus.windows.
net/ehgeneral/publishers/citrix691796.ns.mas.70380659-3fc3-462e-ba5b-cbc5d62f457
5/messages?api-version=2014-01&sig=WjUQcpqwX3eETMWr+x1a9sSbxeY8gPO8SktgTmguerw=&
se=1522303402&skn=dirsvc_send",
"expires" : 0,
"eventhub_endpoint" : "https://ehstaging.servicebus.windows.net/ehgeneral/publis
hers/citrix691796.ns.mas.70380659-3FC3-462E-BA5B-CBC5D62F4575/messages?api-versi
on=2014-01",
"turnOnEvent" : "Y",
"tenant" : "citrix691796",
"agent_id" : "dbb2b943-3b18-46c9-8c7e-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

How do I turn data processing off?

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

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

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

Where can I get help with Citrix Analytics?

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

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

Access assurance –Geolocation

How are geolocation details derived by Analytics?

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

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

Citrix Analytics leverages a third party IP geolocation data provider to derive a user's location from their IP address. GeoIP services are able to resolve to the right city or location most of the time, but

GeoIP look-ups are never completely accurate. Sometimes the location shown for a user might be different from their precise location of access.

Based on IP GeoPoint documentation, the coverage level is about 99.99% of allocated IP addresses worldwide (IPv4 routable IP addresses). In terms of location accuracy, it accompanies each of the essential location fields (country, state, city, postal code) with a Confidence Factor.

In which cases are the determination of location inaccurate?

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

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

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

What is the supported Citrix Workspace app versions?

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

In which cases do we not receive the geological details?

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

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

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

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

Glossary of terms

September 28, 2023

- **Actions**: Closed loop responses to suspicious events. Actions are applied to prevent future anomalous events from occurring. Learn more.
- **Cloud Access Security Broker (CASB)**: On-premises or cloud-based security policy enforcement point placed between cloud service consumers and cloud service providers. CASBs combine and interject enterprise security policies as cloud-based resources are accessed. They also help organizations to extend security controls of their on-premises infrastructure to cloud.
- **Citrix ADC (Application Delivery Controller)**: Network device that lives in a data center, located strategically between the firewall, and one or more application servers. Handles load balancing between servers and optimizes end-user performance and security for enterprise applications. Learn more.
- **Citrix ADM (Application Delivery Management)**: Centralized network management, analytics, and orchestration solution. From a single platform, administrators can view, automate, and manage network services for scale-out application architectures. Learn more.
- **Citrix ADM agent**: Proxy that enables communication between Citrix ADM and the managed instances in a data center. Learn more.
- **Citrix Analytics**: Cloud service that collects data across services and products (on-premises and cloud), and generates actionable insights, enabling administrators to proactively handle user and application security threats, improve app performance, and support continuous operations. Learn more.
- **Citrix Cloud**: Platform that connects to resources through the Citrix Cloud Connector on any cloud or infrastructure (on-premises, public cloud, private cloud, or hybrid cloud). Learn more.
- **Citrix Gateway**: Consolidated remote access solution that consolidates remote access infrastructure to provide single sign-on across all applications whether in a data center, in the cloud, or delivered as SaaS. Learn more.
- **Citrix Hypervisor**: Virtualization management platform optimized for application, desktop, and server virtualization infrastructures. Learn more.
- **Citrix Workspace App** (formerly known as Citrix Receiver): Client software that provides seamless, secure access to applications, desktops and data from any device, including smartphones, tablets, PCs, and Macs. Learn more.
- **DLP (Data Loss Prevention)**: Solution that describes a set of technologies and inspection techniques to classify information contained in an object such as file, email, packet, application, or

a data store. Also, the object can also be in storage, in use, or across a network. DLP tools can dynamically apply policies such as log, report, classify, relocate, tag, and encrypt. DLP tools can also apply enterprise data rights management protections. Learn more.

- **DNS (Domain Name System)**: Network service that is used to locate internet domain names and translate them to internet protocol (IP) addresses. DNS maps website names that users 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.
- **Performance Analytics**: Service that provides visibility into user session details across an organization. Learn more.
- **Policy**: Set of conditions to be met for an action to be applied on a user's risk profile. Learn more.
- **Risk indicator**: Metric that provides information about the level of exposure to a business risk that the organization has at a given time. Learn more.
- **Risk score**: Dynamic value that indicates the aggregate level of risk a user or an entity poses to an IT infrastructure over a pre-determined monitoring period. Learn more.
- **Risk timeline**: Record of a user's or an entity's risky behavior that allows administrators to probe into a risk profile and understand the data usage, device usage, application usage, and location usage. Learn more.
- **Risky user**: User that has acted in a risky manner or presented risky behavior. Learn more.

- **Security Analytics**: Advanced analysis of data that is used to achieve compelling security outcomes such as security monitoring and threat hunting. Learn more.
- **Secure Private Access**: Service that provides integration of single sign-on, remote access, and content inspection into a single solution for end-to-end access control. Learn more.
- **Splunk**: SIEM (Security Information and Event Management) software that receives intelligent data from Citrix Analytics and provides insights about the potential business risks. Learn more.
- **UBA (User Behavior Analytics)**: Process of baselining user activity and behavior combined with peer group analysis, to detect potential intrusions, and malicious activity.
- **Watchlist**: List of users or entities whom administrators want to monitor for suspicious activities. Learn more.