



Citrix Analytics

Contents

What's new	10
September 21, 2023	10
Simplify StoreFront™ On-boarding Using PowerShell Script	10
August 28, 2023	10
Microapps service (End of Life)	10
August 01, 2023	11
Citrix Analytics - Usage (End of Life)	11
February 23, 2023	11
Fixed issues	11
September 28, 2022	11
Webhooks for Alert Notifications	11
September 08, 2022	11
Export limit in CSV export increased	11
August 18, 2022	11
Fixed issue	11
August 10, 2022	12
StoreFront onboarding without site aggregation	12
April 05, 2022	12
Secure Workspace Access is renamed to Secure Private Access	12
March 21, 2022	12
Fixed issue	12
February 10, 2022	13
What's new	13
Auto suggested values for the dimensions in the self-service search box	13
December 20, 2021	14
What's new	14

Access Control is renamed to Secure Workspace Access	14
December 06, 2021	14
What's new	14
Citrix Analytics is now supported in the Asia Pacific South region	14
August 19, 2021	14
What's new	14
Support for the IS EMPTY operator	14
July 14, 2021	15
What's new	15
Support for the IS NOT EMPTY operator	15
June 07, 2021	15
Deprecated feature	15
Removed Citrix Analytics demo environment	15
May 18, 2021	16
What's new	16
Support for * operator with != operator	16
Enhanced search bar experience in the self-service search page	16
Redesigned chips view in self-service search	16
Fixed issue	17
March 31, 2021	17
Support for the IN and NOT IN operators for Apps and Desktops search query	17
March 18, 2021	17
What's new	17
Support for the NOT LIKE (!~) operator	17
February 23, 2021	18
What's new	18
Schedule email delivery for a search query	18
Download visual summary of a search query	19

November 12, 2020	20
New feature	20
Save a self-service query	20
October 20, 2020	21
New features	21
Support for Citrix Gateway in the European Union region	21
July 09, 2020	21
Deprecated support	21
June 02, 2020	21
New features	21
Redesigned overview page and top bar in Analytics	21
February 20, 2020	22
New features	22
Citrix Analytics subscription offerings	22
Data governance logs updates	23
Fixed issues	23
January 09, 2020	23
Fixed issues	23
December 18, 2019	23
Fixed issues	23
December 12, 2019	24
New features	24
Support for Microapps service events in Asia Pacific South	24
December 04, 2019	24
Fixed issues	24
November 22, 2019	24
New features	24
Redesigned overview page for Analytics	24

October 21, 2019	25
New features	25
Technical security overview	25
September 11, 2019	25
Fixed issues	25
August 20, 2019	25
Fixed issues	25
July 31, 2019	26
New features	26
Support for the European Union region	26
June 26, 2019	26
Fixed issues	26
June 19, 2019	26
Fixed issues	26
November 16, 2018	26
Fixed issues	26
October 10, 2018	26
Architecture and platform enhancements	26
August 23, 2018	27
New product names	27
Known issues	28
Data Sources	29
Supported data sources	29
Citrix Gateway data source	30
Prerequisites	30
Gateway data sources added to Citrix ADM	30
Gateway data sources not added to Citrix ADM	31
Prerequisites	33

Install and set up an agent	35
Add Citrix Gateway instances	39
Enable analytics	41
Watch the onboarding video	42
View received events, users, and agents	43
Turn on or off data processing	44
Add more Gateway instances	46
Manage data source	46
Citrix Virtual Apps and Desktops™ data source	47
Onboard Citrix Virtual Apps and Desktops on-premises sites using StoreFront	47
Prerequisites	48
Connect to a StoreFront deployment	49
Connect using Apps and Desktops – Workspace app site card and the Apps and Desktops – Monitoring site card	49
PowerShell Script	52
Connect using Recommendations panel	55
Review the Recommendations panel	58
View connected StoreFront deployments	59
Add or remove StoreFront deployments	62
Configure a StoreFront deployment hosted on a webserver that uses HTTP proxy	64
Data governance	65
layout: doc replicate-from: commons/data-governance.md	65
Technical security overview	66
Data flow	66
Network requirements	66
Identity and access management	69
Data residency	69
Data protection	70

Security responsibility	71
Citrix responsibility	71
Customer responsibility	71
System Requirements	73
Citrix Analytics subscriptions	73
Data sources requirements	73
Supported browsers	73
Manage administrator roles for Citrix Analytics	74
Getting started	77
Step 1: Sign in to Citrix Cloud™	77
Step 2: Get access to Analytics	77
Step 3: Manage Analytics	78
Find your way around	79
Top bar	79
Settings menu	79
Help menu	80
Discover more data sources	80
Audit log	80
Self-service search	81
layout: doc replicate-from: /commons/self-service-search.md	81
Alert settings	82
Email distribution lists	82
Create email distribution list	83
View email distribution list	85
Modify an email distribution list	85
Delete an email distribution list	86
Webhook for Alert Notifications	87
Create Webhook Profile	87

Webhook Configuration Examples	88
Sending alert message to Slack	89
Sending alert message to Microsoft Teams	89
Citrix Analytics for Security™ (Security Analytics)	90
What is Security Analytics?	90
Features	90
Dashboards	91
What's next	91
Citrix Analytics for Performance™ (Performance Analytics)	92
What is Performance Analytics	92
How to use Performance Analytics	92
User Experience Dashboard	92
Infrastructure Dashboard	93
Getting Started	93
Prerequisites	93
Access	95
Access from the Asia Pacific South region	96
Configure Data Sources	96
Service Continuity	97
Troubleshoot Citrix Analytics for Security and Performance	99
layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance.md	99
Verify anonymous users as legitimate users	99
layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/anonymous-users-issue.md	99
Troubleshoot event transmission issues from a data source	99
layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/datasource-events-transmission-issue.md	99

Trigger Virtual Apps and Desktops events, SaaS events, and verifying event transmission	99
layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/virtual-apps-desktops-saas-events-verify.md	99
Configured Session Recording server fails to connect	99
layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/session-recording-issue.md	99
Configuration issues with Citrix Analytics add-on for Splunk	100
layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/splunk-add-on-debugging.md	100
Unable to connect StoreFront™ server with Citrix Analytics	100
layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/storefront-issue.md	100
FAQs	101
layout: doc replicate-from: commons/faqs.md	101
Glossary of terms	102
layout: doc replicate-from: commons/glossary.md	102
Citrix Analytics Document History	103

What's new

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

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

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.

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.

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.



```
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](#).

The screenshot displays the 'Self-Service Search' interface. At the top, there are two dropdown menus: 'Apps and Desktops' and 'Last 1 Day'. Below these, a search box contains the text 'Browser ='. A list of auto-suggested values is shown below the search box, including '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', and 'Chrome 95.0.4638.54'. A 'Need help?' link is located at the bottom right of the suggestions list.

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

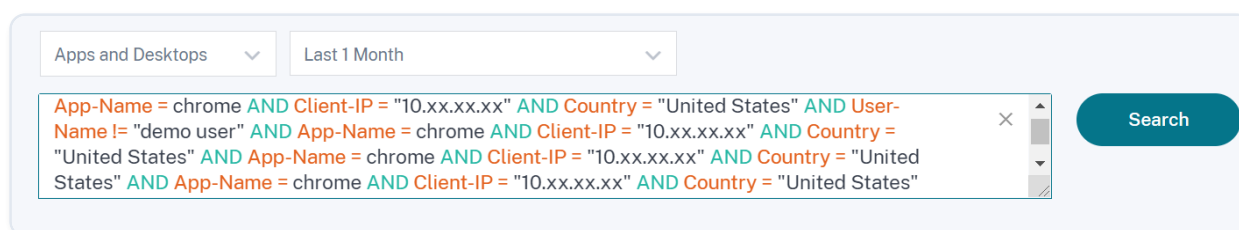
NOTE

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.

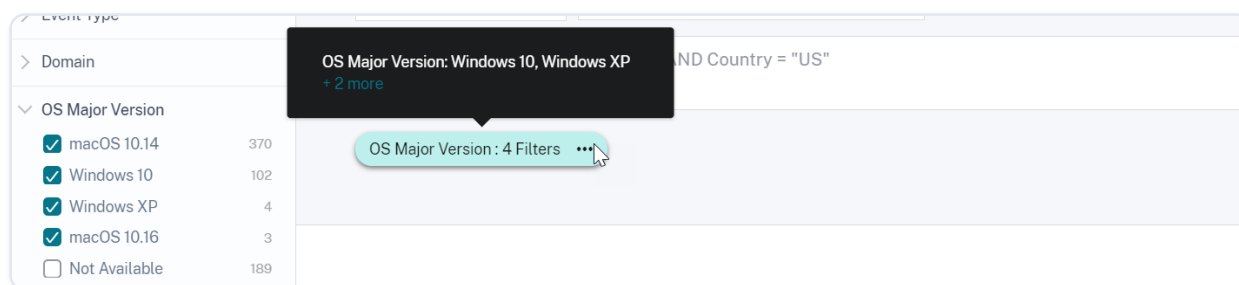


- The cursor jumping issue that was observed in the Safari browser is now fixed.

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.



- 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.

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](#) | [View Saved Searches](#)

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 ▼

Cancel

Save

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](#).



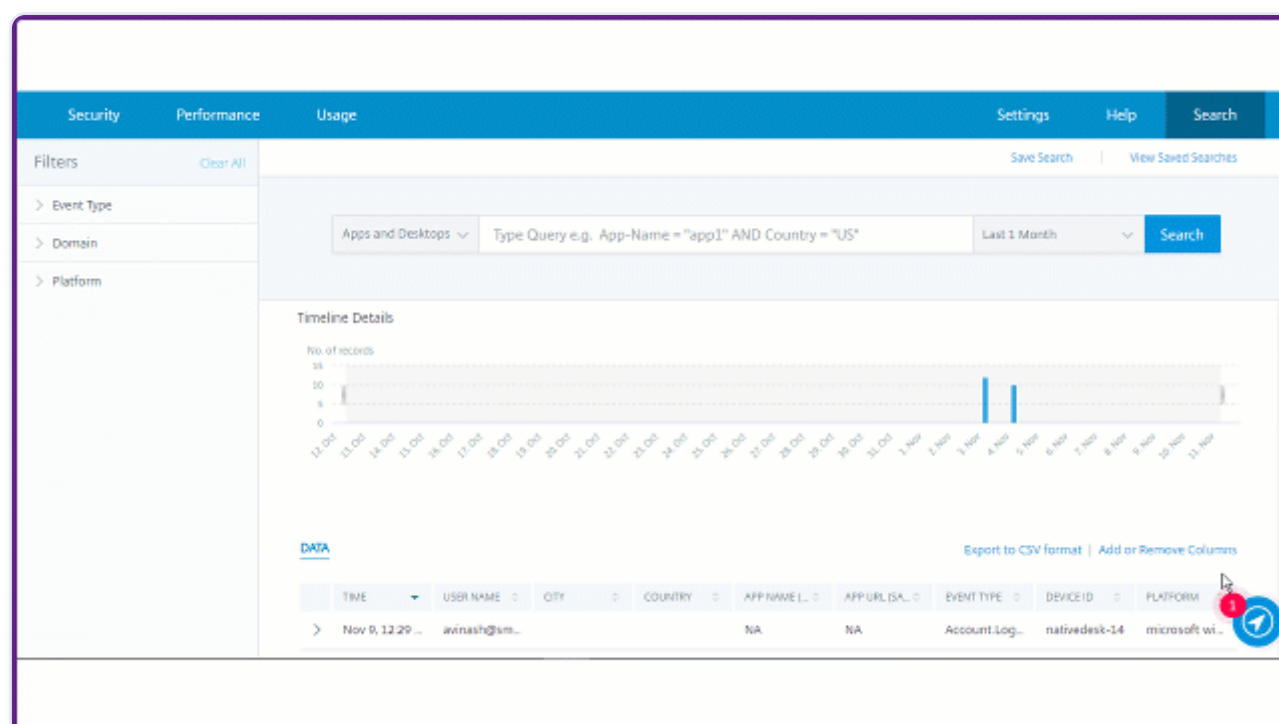
November 12, 2020

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



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

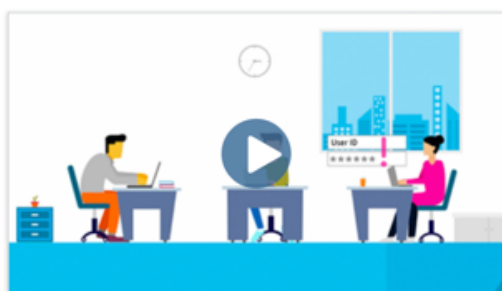
The Analytics overview page displays the **Usage** tile that replaces the previously existed **Operations** tile. Also, the **Productivity** tile is removed from this page. To view the overview page, select **Help > Overview**.

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.

Security

Performance

Usage

Settings

Help

Search

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.

January 09, 2020

Fixed issues

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

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.

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.

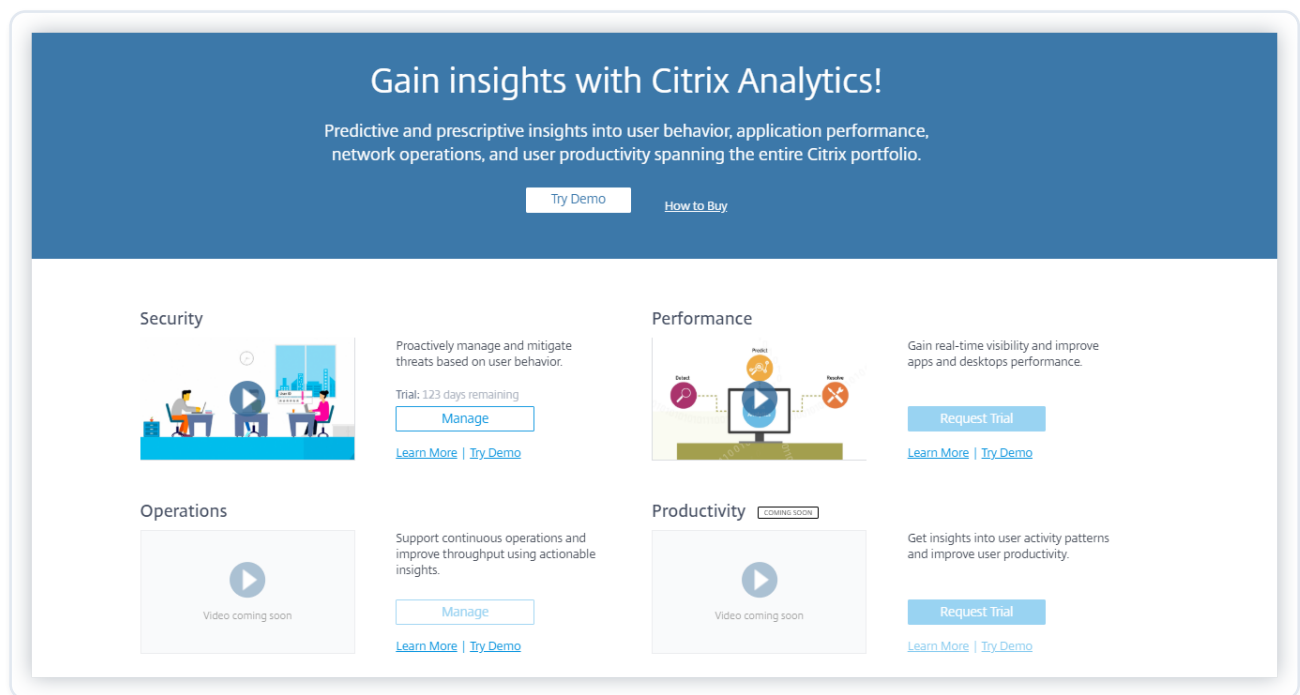
November 22, 2019

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**.



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.

August 20, 2019

Fixed issues

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

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.

June 19, 2019

Fixed issues

- Citrix Analytics does not load accurately on Microsoft Edge.

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

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.

Data Sources

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 {{page.gateway-onprem-product-name}} and {{page.cvad-onprem-product-name}}, 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](#)

{{page.gateway-onprem-product-name}}, {{page.daas-product-name}} (formerly Citrix Virtual Apps and Desktops service), and {{page.cvad-onprem-product-name}} 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

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.

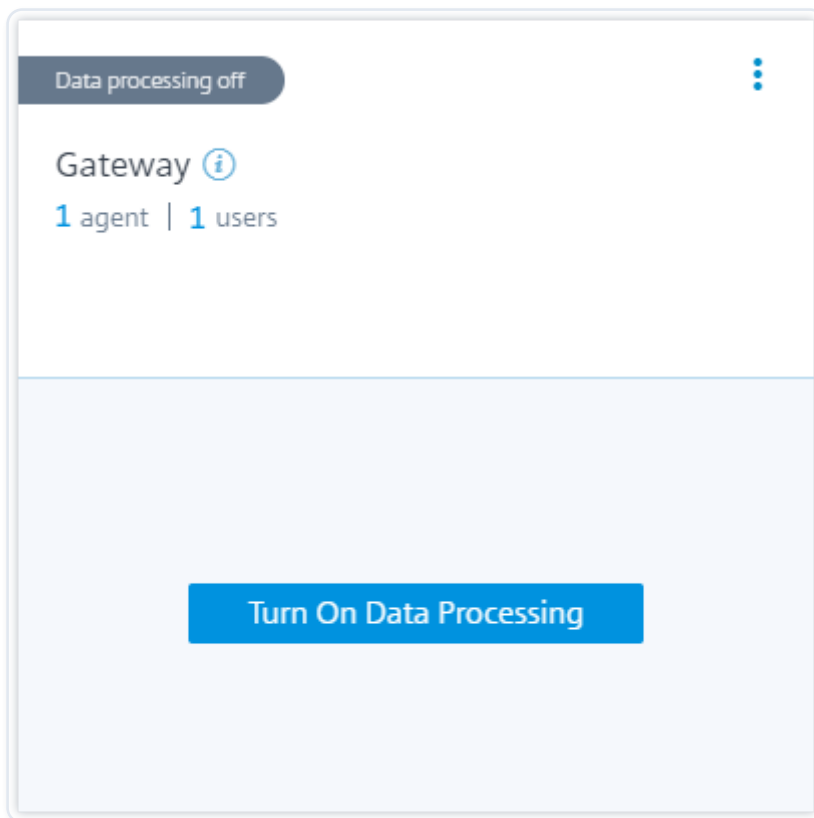
Gateway data sources added to Citrix ADM

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.

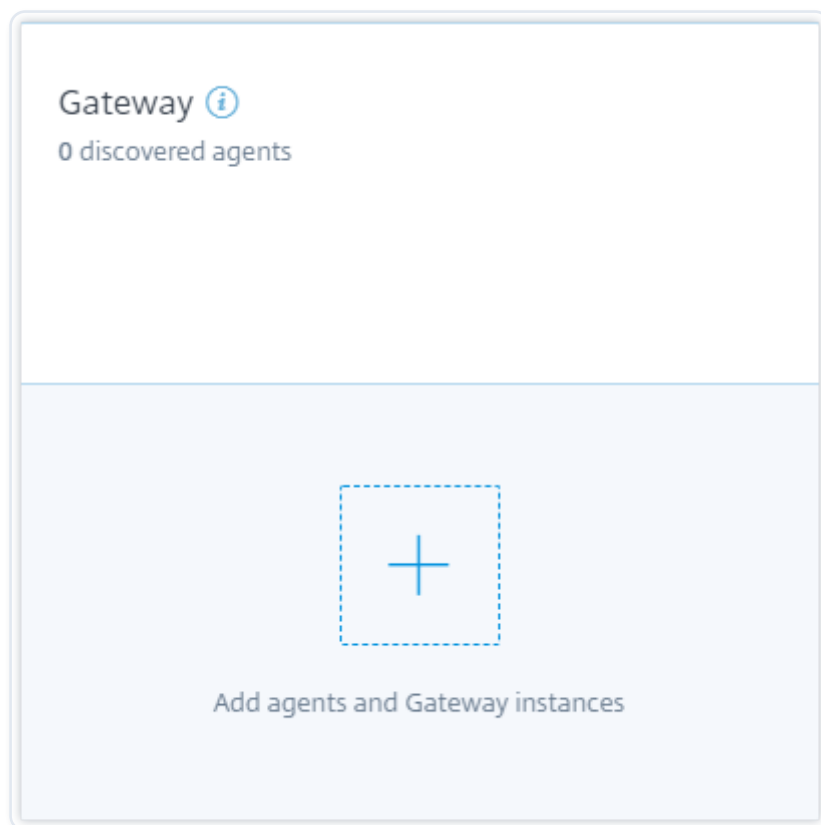


You can view the [received events](#).

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**.



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	APS REGION
Event Hub	<code>https://cas-eh-ns-alias.servicebus.windows.net/</code>	<code>https://cas-eh-ns-eu-alias.servicebus.windows.net/</code>	<code>https://cas-eh-ns-aps-alias.servicebus.windows.net/</code>

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.

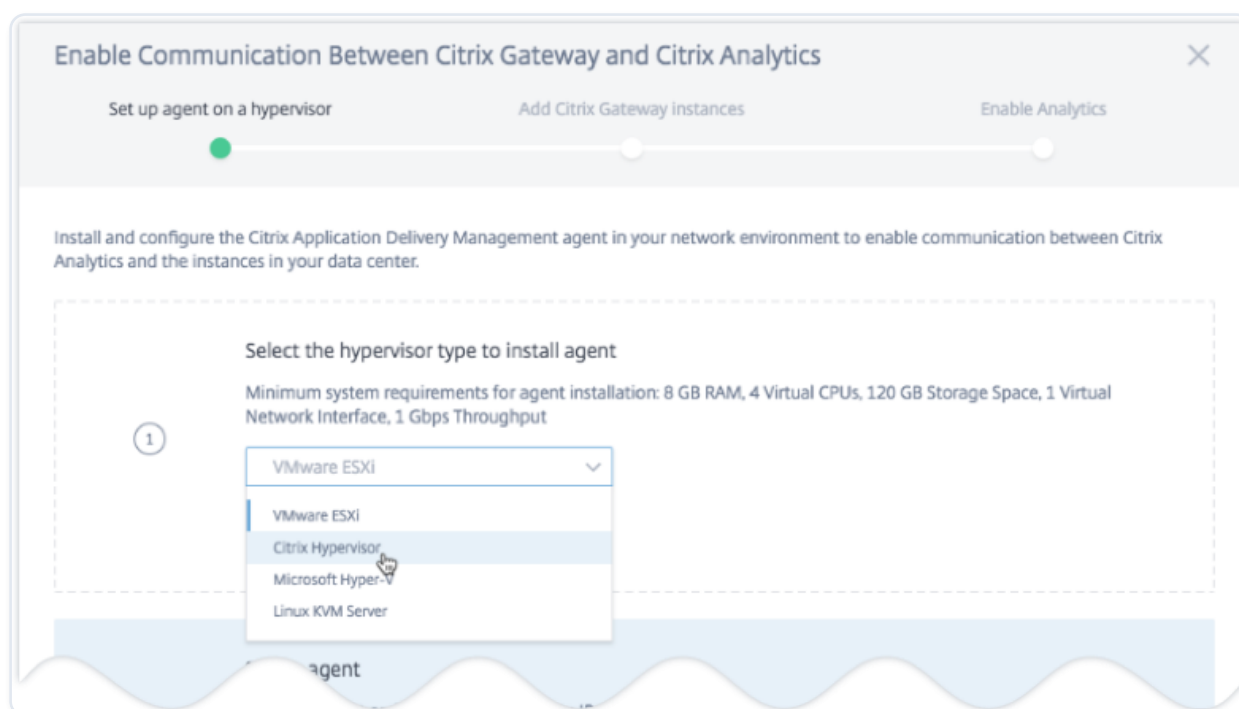
You can install an agent on the following hypervisors in your enterprise data center:

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

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

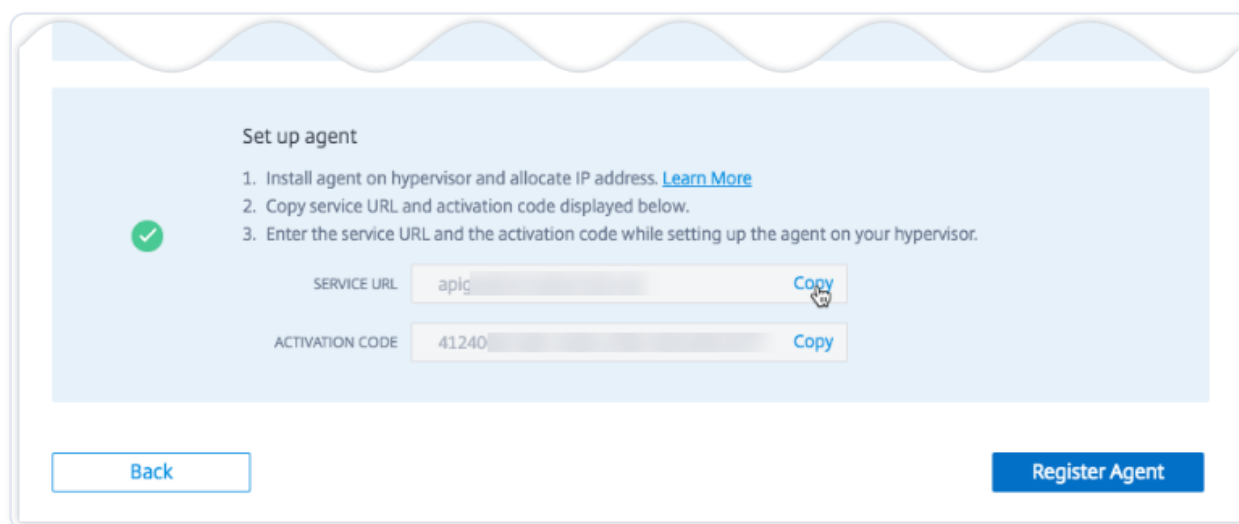
1. Download the agent image.

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.



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.



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 [10.10.10.1]:
3. Netmask [255.255.255.0]:
4. Gateway IPv4 address [10.10.10.1]:
5. DNS IPv4 Address [127.0.0.1]:
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 : c56ba264-5

```

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 [10.10.10.1]:
3. Netmask [255.255.255.0]:
4. Gateway IPv4 address [10.10.10.1]:
5. DNS IPv4 Address [127.0.0.1]:
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
nsaad .

```

```
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-██████████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

Set up agent on a hypervisor

Add Citrix Gateway instances

Enable Analytics

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

AGENT IP ADDRESS	AGENT HOST NAME	STATE
10	CAS-CG-Demo	

Showing 1 - 1 of 1 items

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

Back

Next

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

Set up agent on a hypervisorAdd Citrix Gateway instancesEnable Analytics

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

✓

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

✓

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

Create an Authentication Profile

BackAdd Instances

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

+ Add Citrix Gateway instance

Search...

CITRIX GATEWAY INSTANCE IP ADDRESS	CITRIX GATEWAY HOST NAME	STATE
10	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.

BackNext

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

Set up agent on a hypervisor
Add Citrix Gateway instances
Enable 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 A	VIRTUAL SERVER IP ADDI	VIRTUAL SERVER NAME	VIRTUAL SERVER TYPE	VIRTUAL SERVER STATE
10.136.92	CAS-CG-Demo	136.92	vpn2	SSL	●
10.136.98	CAS-CG-Demo	136.98	vpn1	SSL	●

Showing 1 - 2 of 2 items

Back
Enable Analytics

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

Linked Data Sources

Citrix Gateway
CAS-CG-Demo
Data Processing On

Add On-Premises Data Sources

Citrix Virtual Apps and Desktops
Citrix Gateway

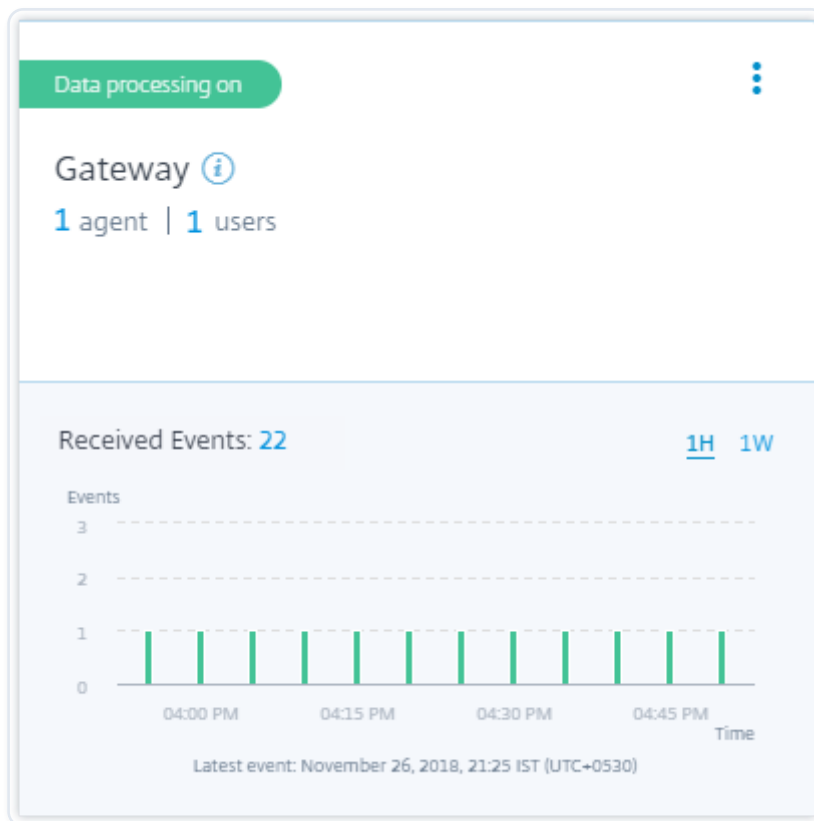
Watch the onboarding video

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

`<iframe src="https://www.youtube.com/embed/Bw_CXAUHINK" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>`

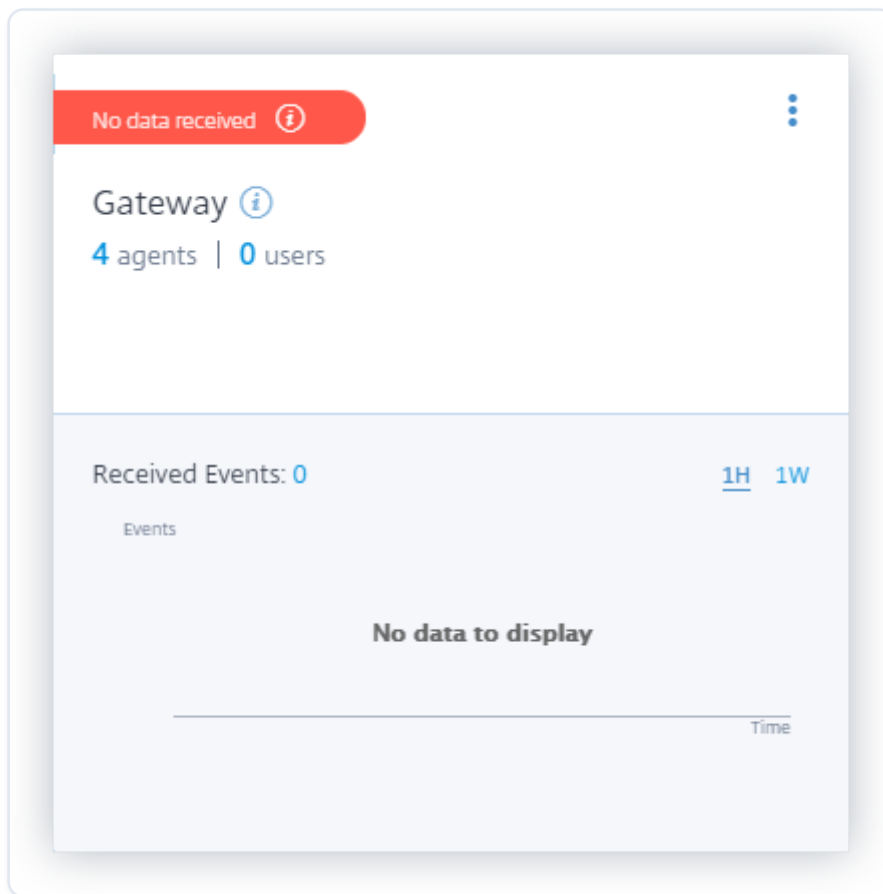
View received events, users, and agents

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.



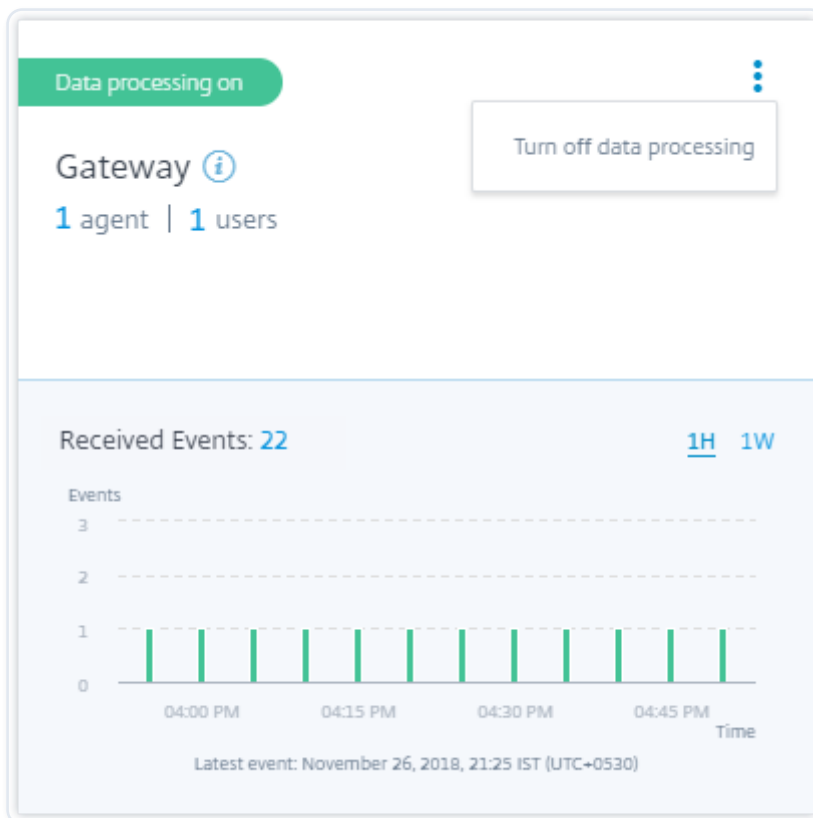
After you have enabled data processing, the site card might display the **No data received** status. This status appears for two reasons:

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.

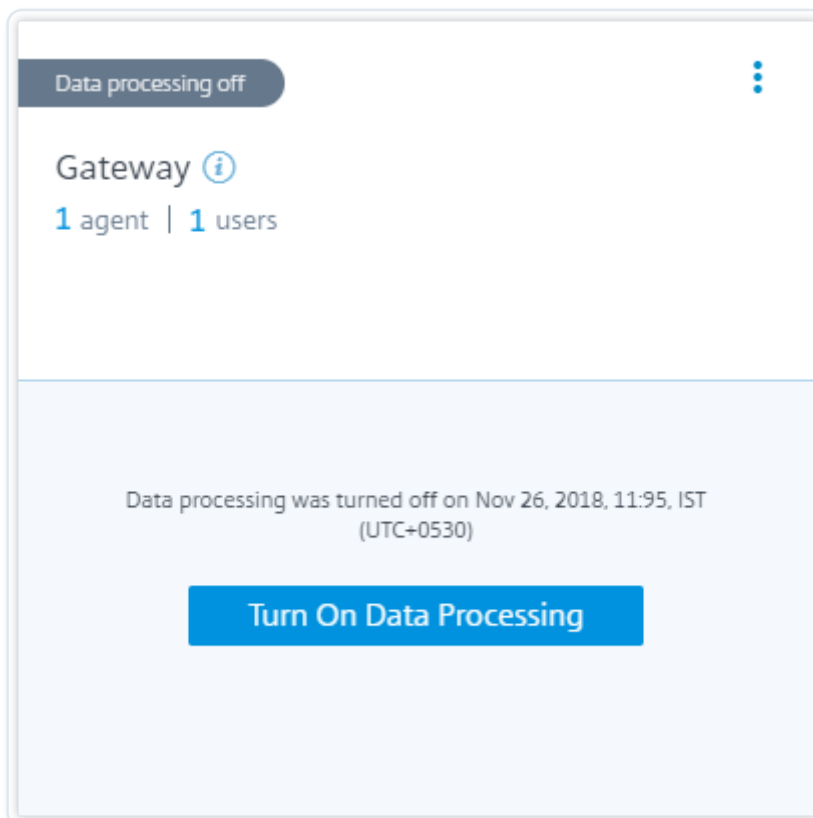


Turn on or off data processing

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.

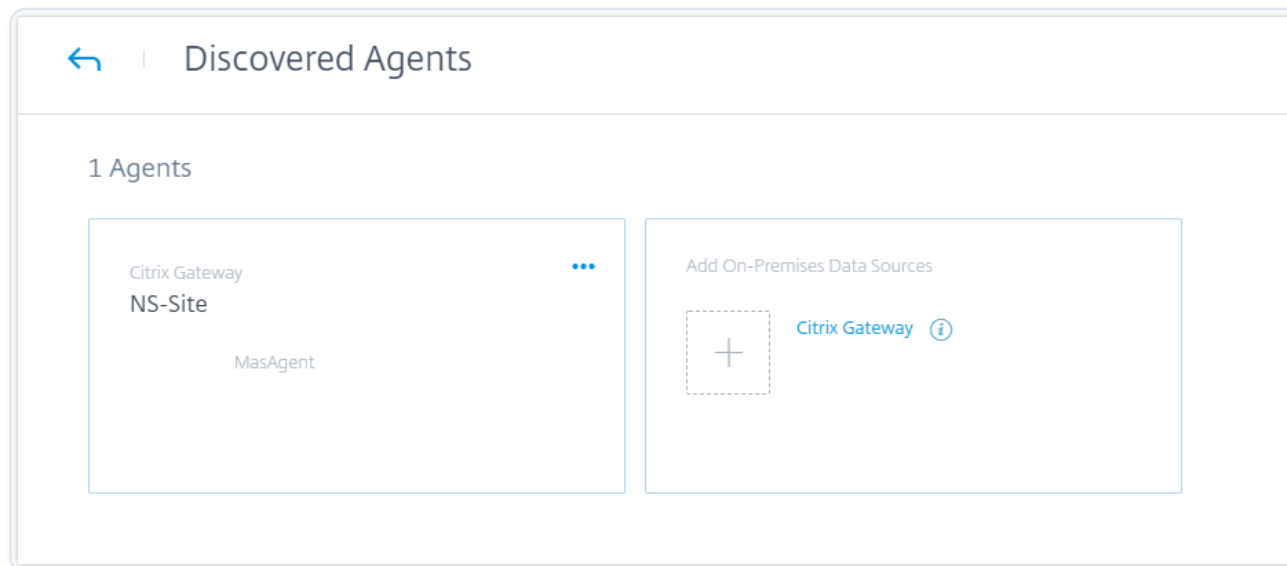


To enable data processing again, click **Turn On Data Processing**.



Add more Gateway instances

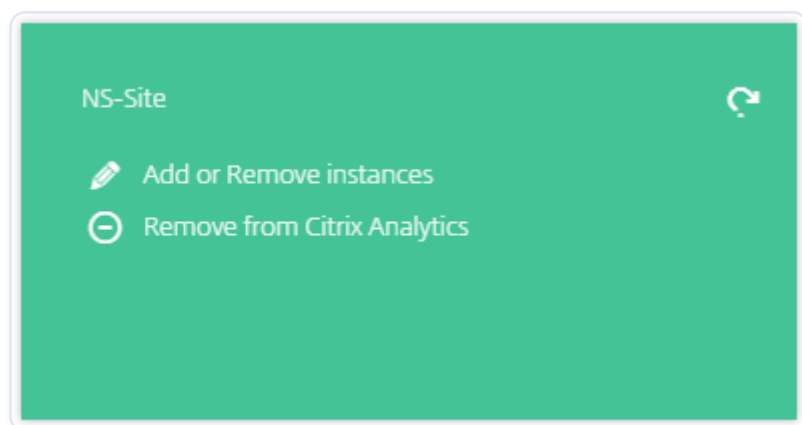
If you want to add more Gateway instances, click the number of agents on the Gateway site card to view the **Discovered Agents** page. From the **Add On-Premises Data Sources** tile, click **Citrix Gateway**.



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 its associated instances from Citrix Analytics.

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



- **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

This article describes the steps to connect your on-premises {{page.cvad-onprem-product-name}} 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 {{page.cvad-onprem-product-name}} sites with Citrix Analytics for Performance](#)
- [Configuring {{page.cvad-and-daas-product-name}} data source for Citrix Analytics for Security](#)

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

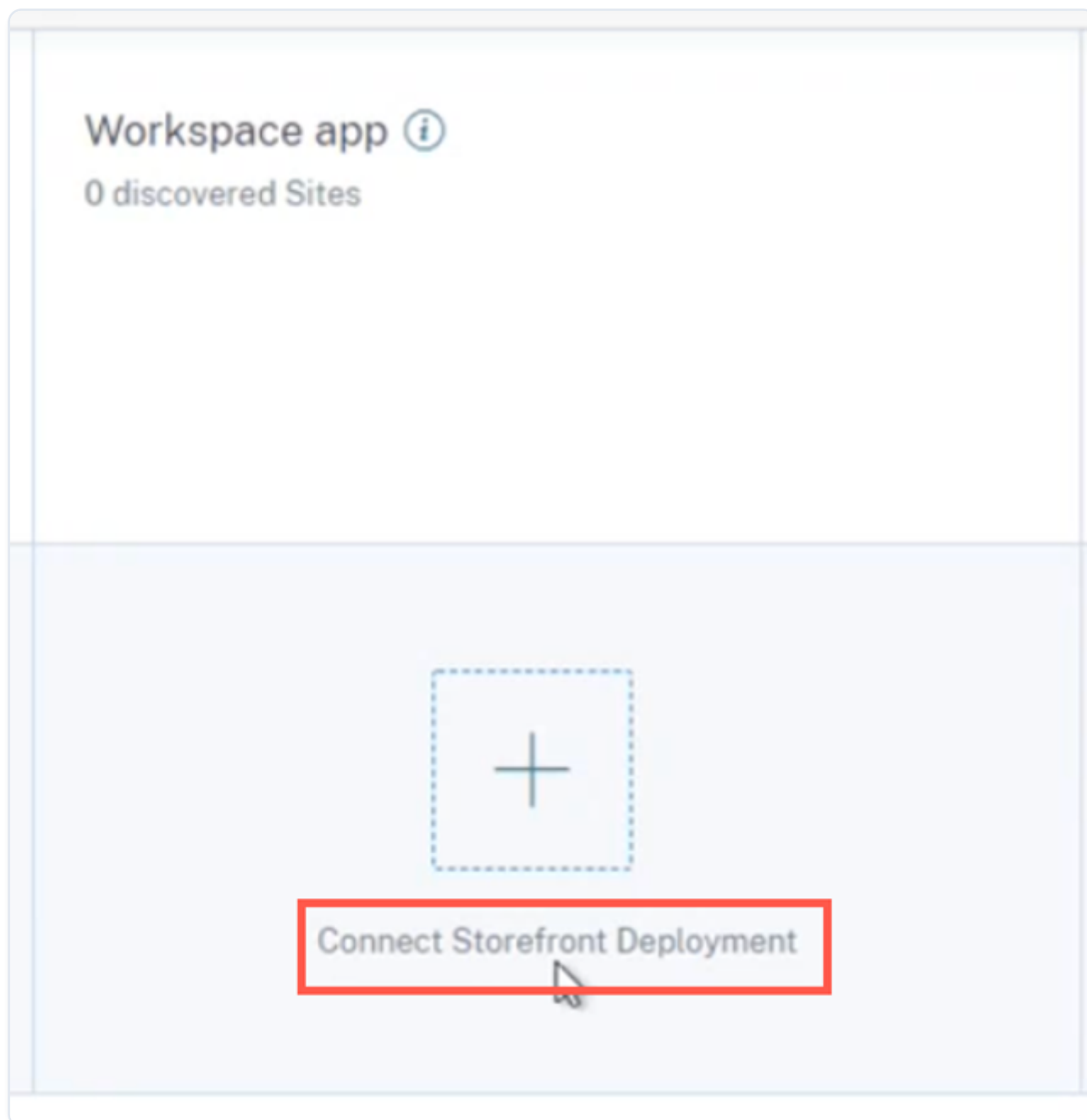
If your organization uses an on-premises StoreFront™ deployment, you must configure your StoreFront servers to enable Citrix Workspace™ app to send events to Citrix Analytics. Citrix Analytics processes events to provide actionable insights into the performance of your Citrix IT infrastructure and user 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, {{page.cvad-onprem-product-name}} 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 {{page.cvad-onprem-product-name}} 7 1912 LTSR, the supported StoreFront version is 1912.

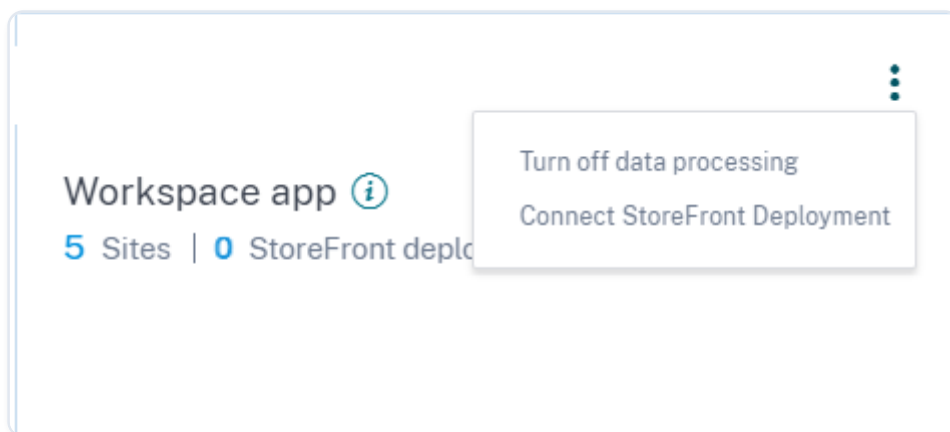
Connect to a StoreFront deployment

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

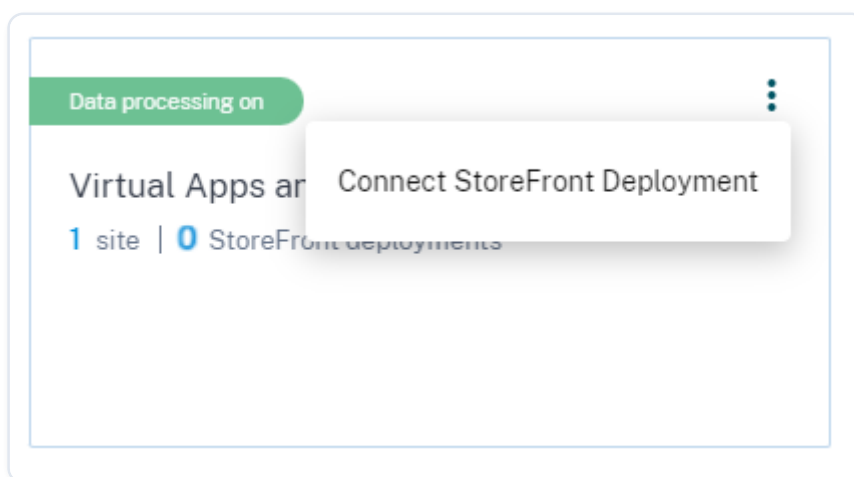
- Using the **Apps and Desktops – Workspace app** site card and the **Apps and Desktops – Monitoring** site card
- Using the **Recommendations** panel

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**.

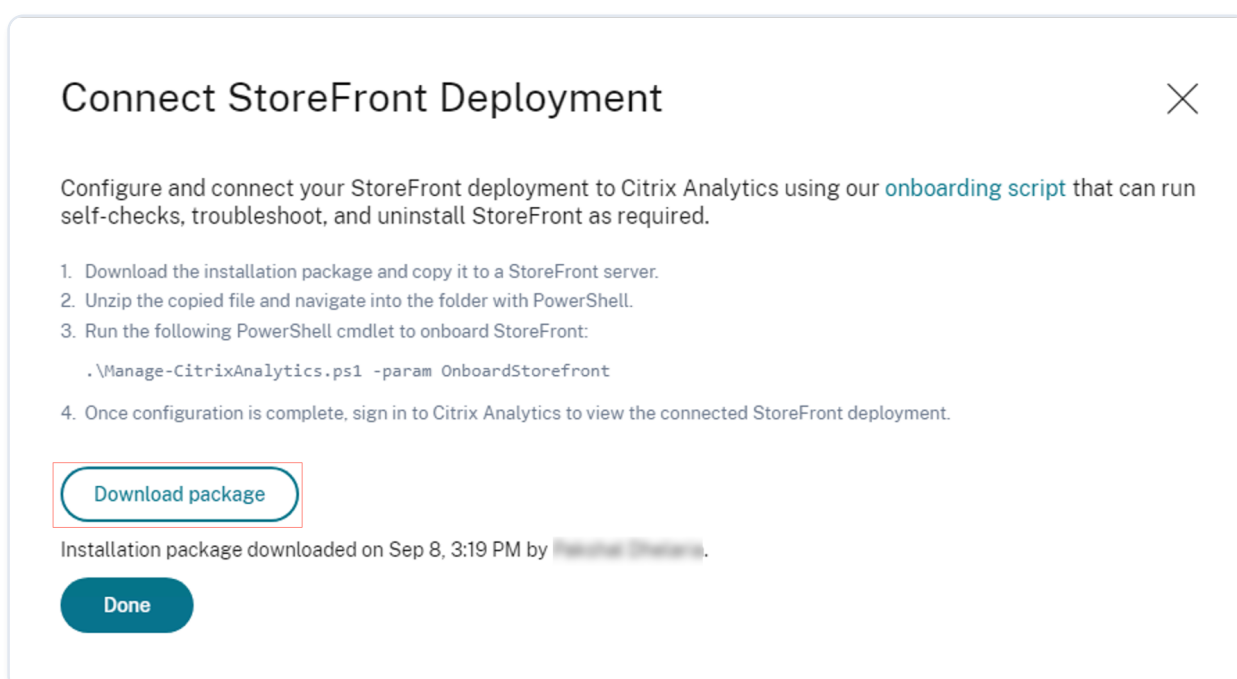


2. Navigate to **Settings > Data Sources > Performance**. On the **Apps and Desktops-Monitoring** site card, click the vertical ellipsis (:) and then select **Connect StoreFront deployment**.



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

3. Click **Download package**.

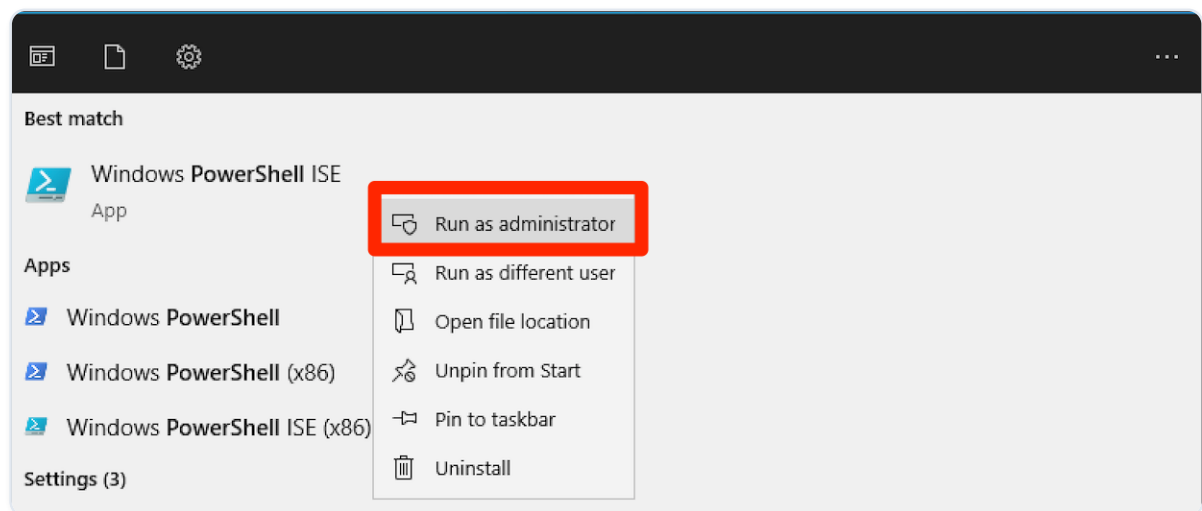


NOTE

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
```

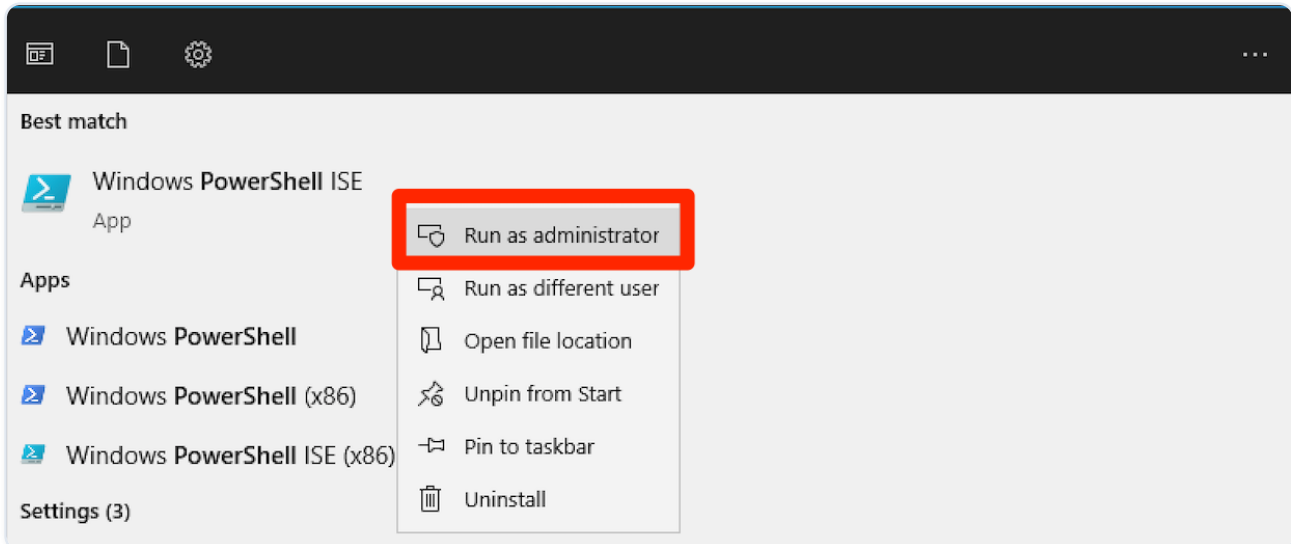


For more options or parameters, refer to the [PowerShell Script](#) section.

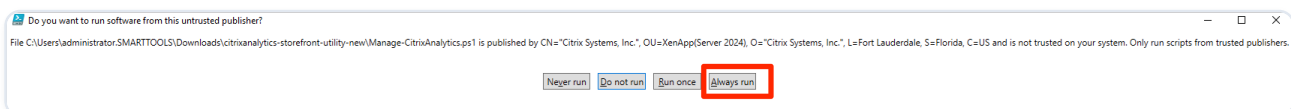
- d. Open the StoreFront server and execute the PowerShell script.
 - e. If the StoreFront site does not appear in the Citrix Analytics Service GUI even after running OnboardStorefront, run the iisreset command.
 - f. Log in to Citrix Analytics Service GUI and validate if the Cluster ID matches to the 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.



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.

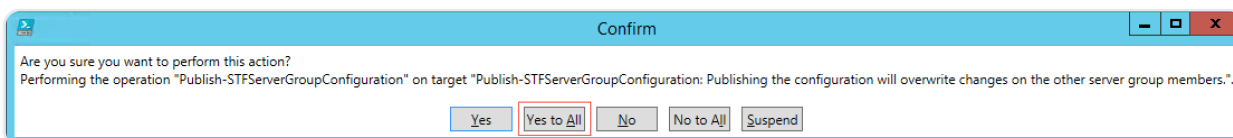
The PowerShell script supports the following parameters:

- **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.



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:

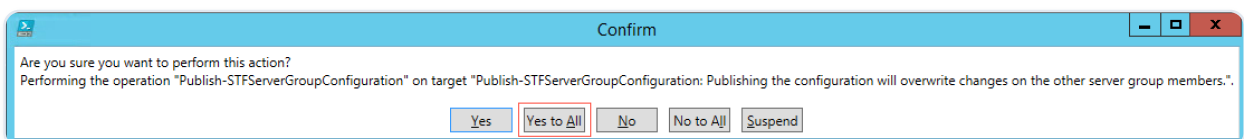
- **Use case 1:** As a part of self-check if the curlAnalytics failed, then a firewall rule gets created. This firewall rule opens a 443 port and verifies its connectivity to Analytics. If not, that means the Analytics server is not reachable and the script exits from here. Rerun the script once the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



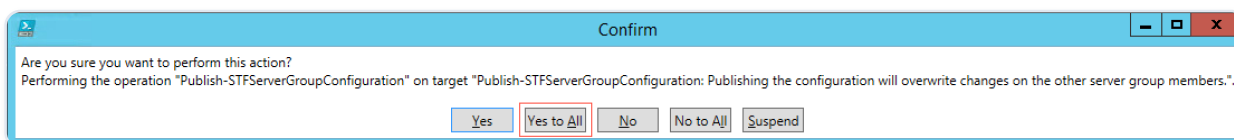
- **DeboardStoreFront:** The DeboardStoreFront parameter is used for deboarding the StoreFront server from Citrix Analytics Service. Use the following command to run the DeboardStoreFront:

```
.\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.

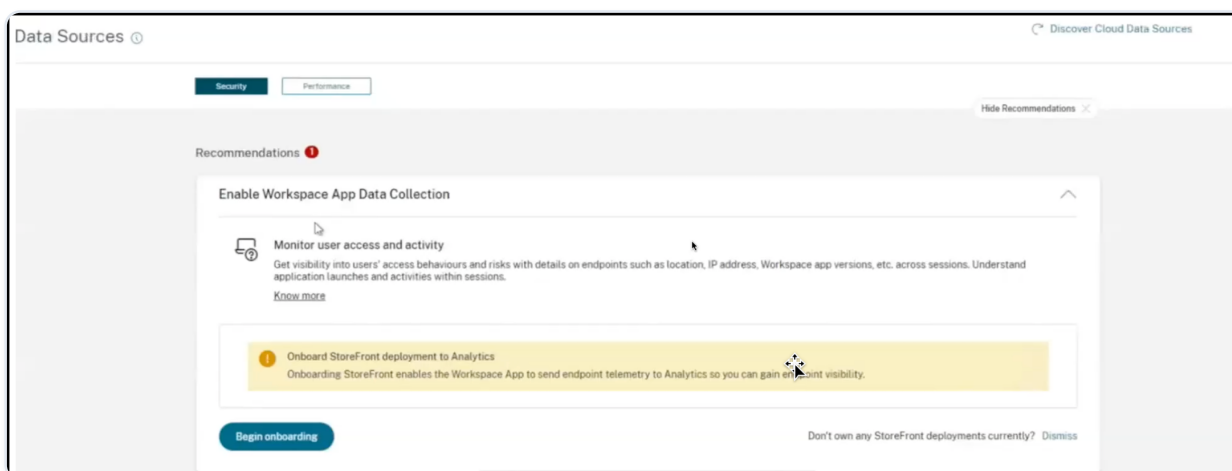
For a server group, the PublishConfiguration command automatically runs from the script to publish the StoreFront configuration to all the servers within that StoreFront. You can see a pop-up to confirm this action. Select the **Yes to All** button.



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.

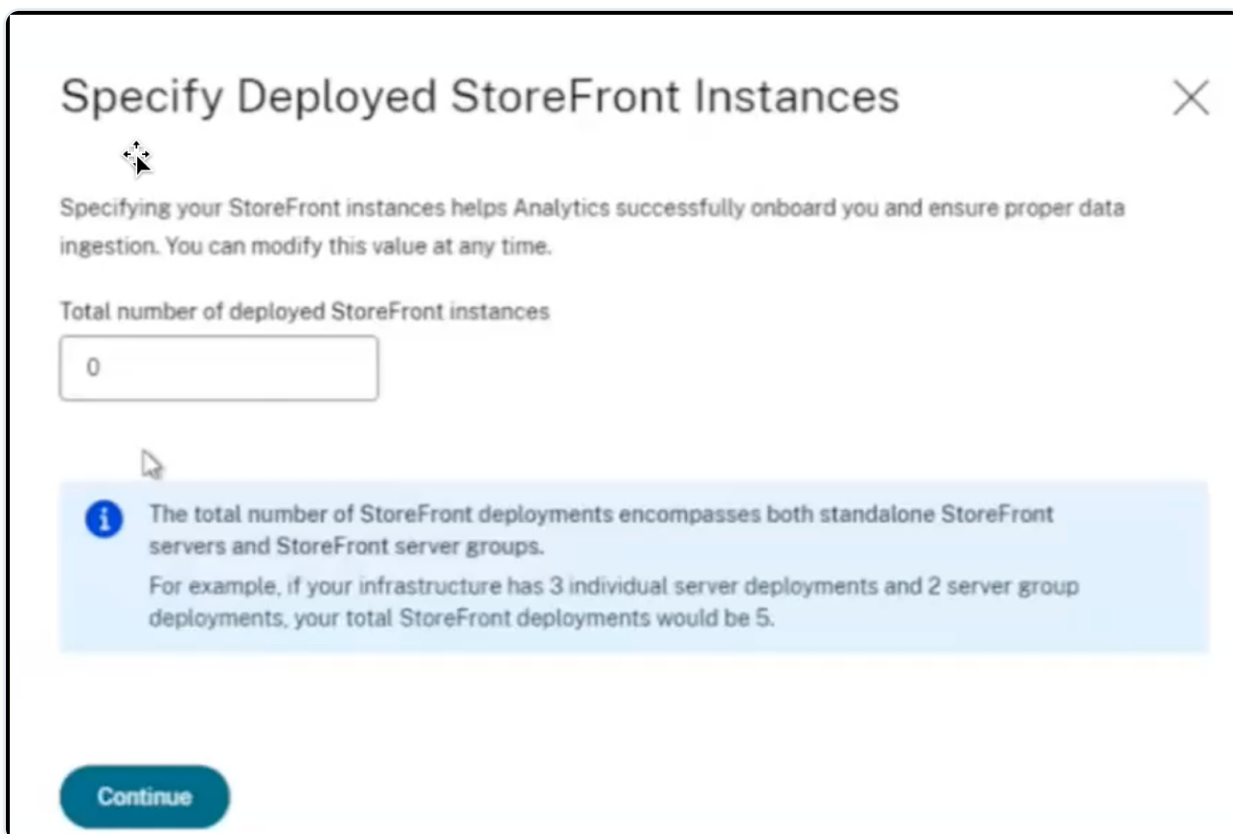
1. If you are using the Security Analytics offering, select **Settings > Data Sources > Security**.
2. If you are using the Performance Analytics offering, navigate to **Settings > Data Sources > Performance**.
3. On the **Data Sources** page, review the information and recommendations on the **Recommendations**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



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

i 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.

Continue

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.

Download package

Installation package downloaded on Sep 8, 3:19 PM by **Michael Stevens**.

Done

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.

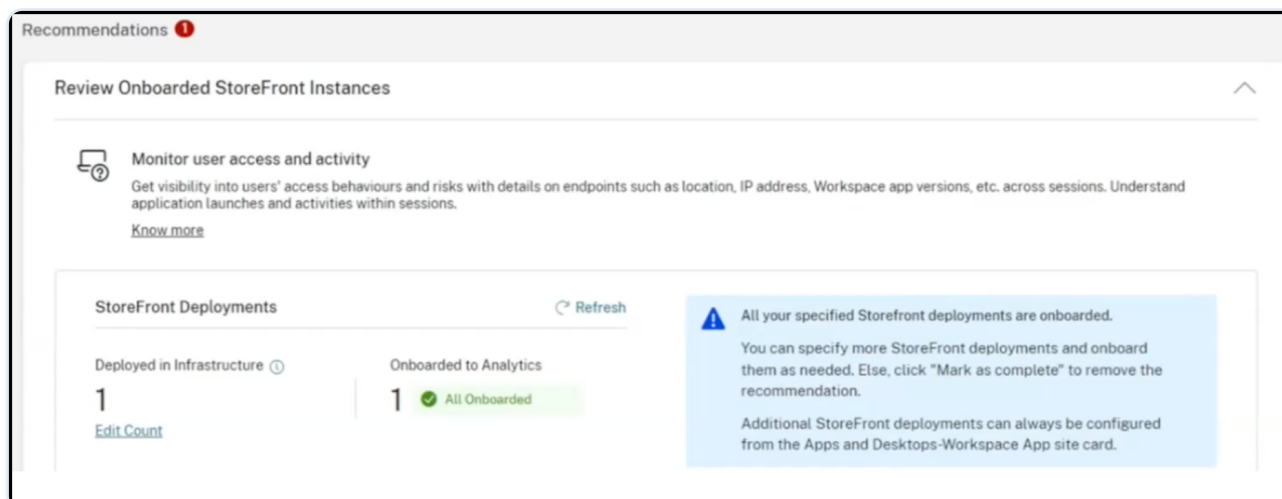
Review the Recommendations panel

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

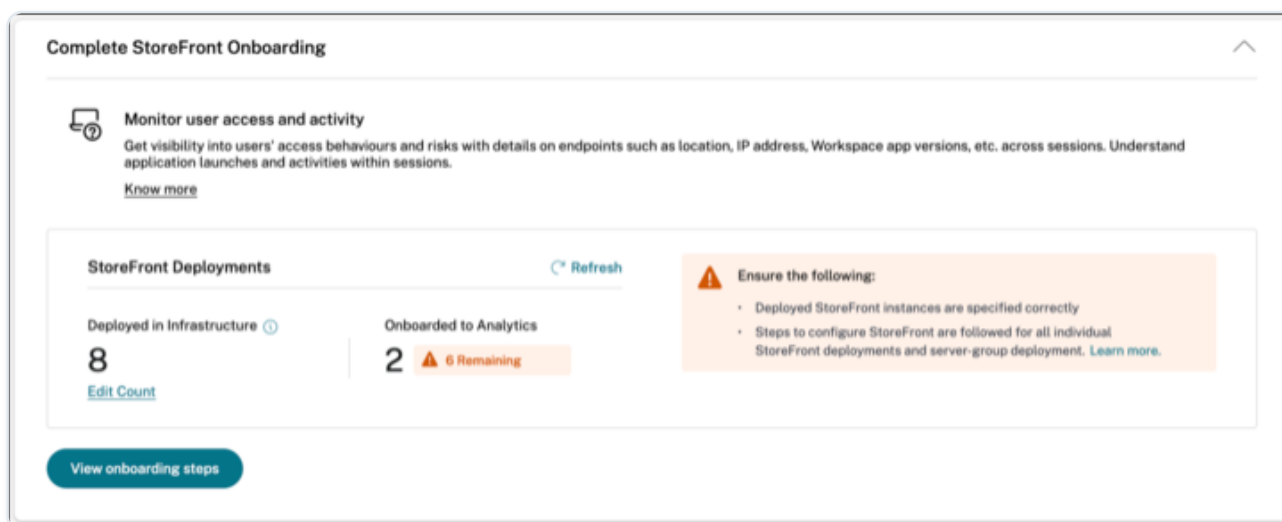
If you want to onboard more StoreFront deployments, click **View onboarding steps** and the StoreFront Onboarding wizard or the **Connect StoreFront Deployment** popup appears again.



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:

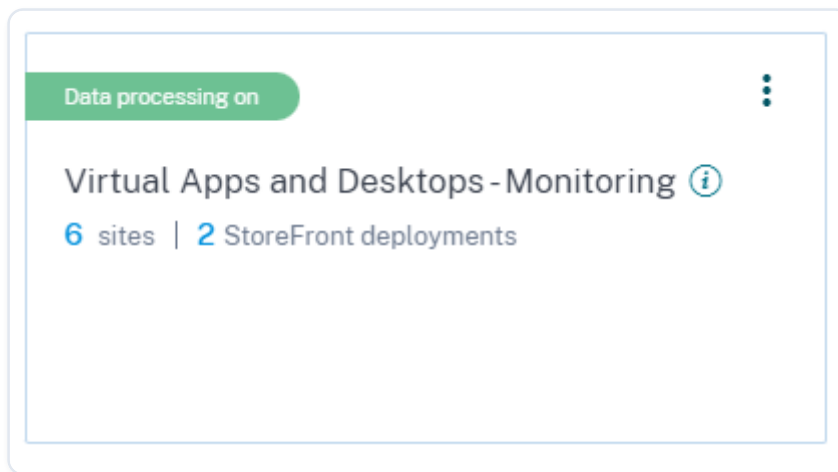
The **Total number of deployed StoreFront instances** is the total number of StoreFront groups and it isn't the number of individual StoreFront servers.



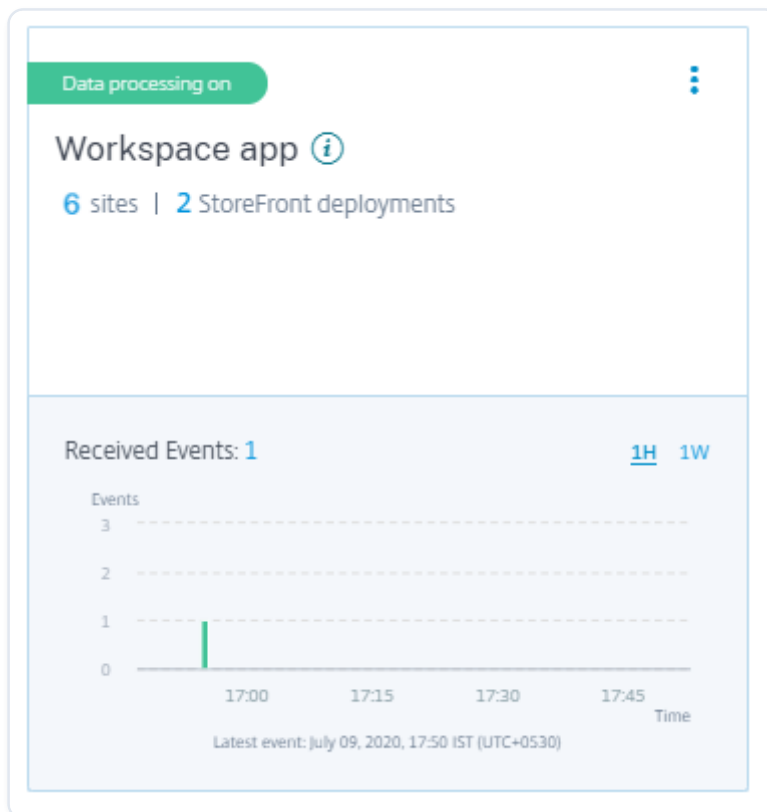
View connected StoreFront deployments

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:



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



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		Success	Apr 15 2020 3:13 PM

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

StoreFront deployment

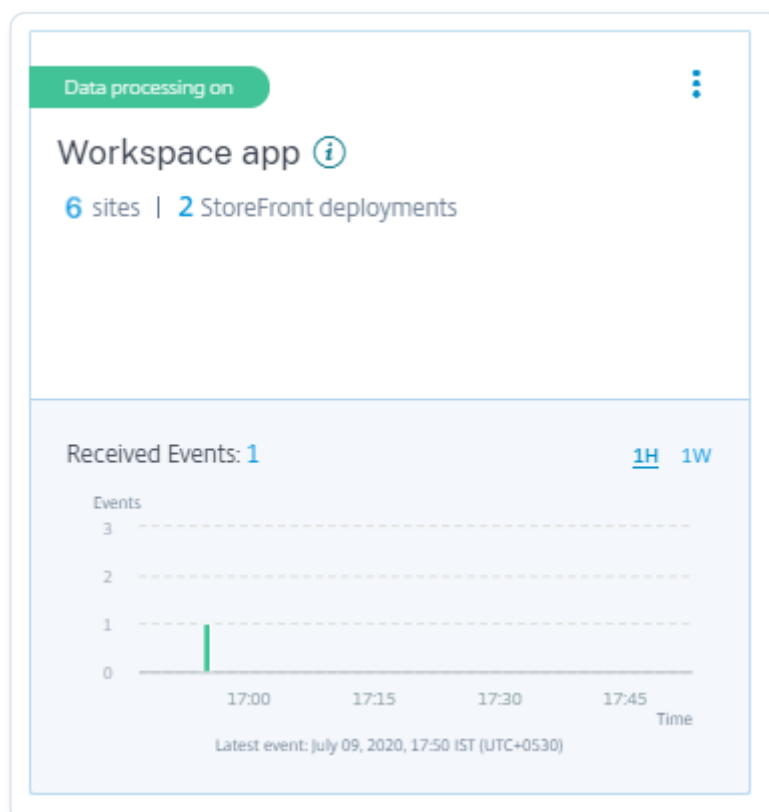
The StoreFront deployment is successfully configured and connected.

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

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

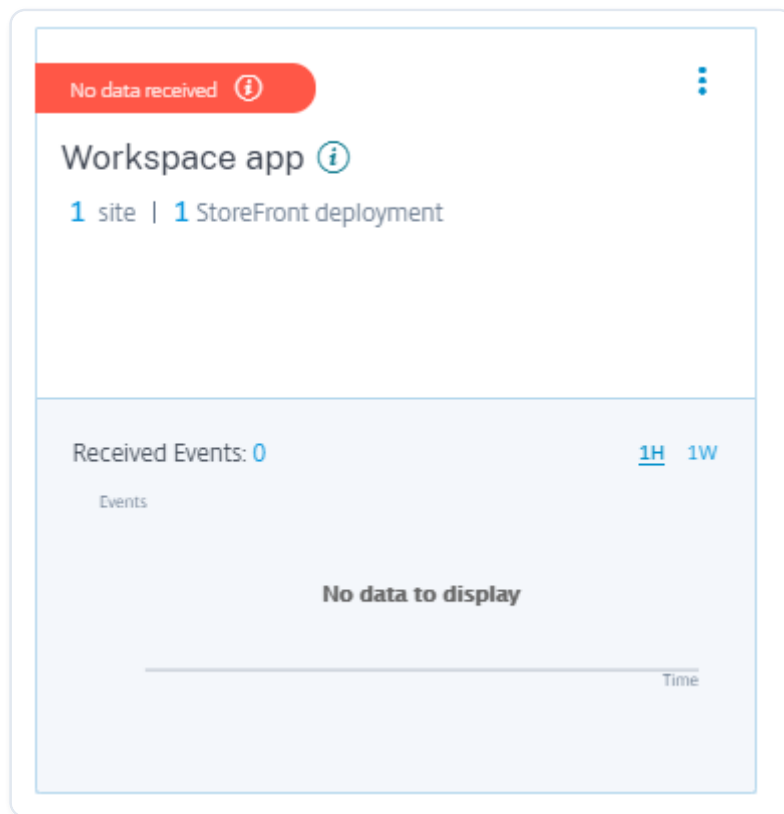
If you are using the Security Analytics offering, the site card also displays the following information about the received events:

- 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:

- a. 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.
- b. Citrix Analytics has not received any events from the data source in the last one hour.



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		Success	Oct 18 2021 10:28 AM

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

StoreFront deployment

+ Connect to 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**.

The screenshot shows the 'StoreFront deployments' section in Citrix Analytics. A message states: 'The StoreFront deployment is successfully configured and connected.' Below this is a table with the following columns: BASE URL, STOREFRONT DEPLOYMENT, CONFIGURATION STATUS, and LAST UPDATED. The table contains one row with the following data: BASE URL is 'http://...', STOREFRONT DEPLOYMENT is '...', CONFIGURATION STATUS is 'Success', and LAST UPDATED is 'Oct 18 2021 10:28 AM'. A button labeled 'Remove StoreFront deployment from Analytics' is highlighted with a red box. The table footer indicates 'Showing 1-1 of 1 items', 'Page 1 of 1', and '5 rows'.

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

layout: doc replicate-from: commons/data-governance.md

Technical security overview

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 {{page.cvad-onprem-product-name}} 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 Splunk** on the Splunk environment. For more information, see [Splunk integration](#).

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

Network requirements

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

- **Citrix Analytics requirements:** Review the [system requirements](#) before using 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	<code>https://analytics.cloud.com/</code>	<code>https://analytics-eu.cloud.com/</code>	<code>https://analytics-aps.cloud.com/</code>
Admin UI (CDN)	<code>https://cas-api-cdn-ep-h9apa4bsccg0gfe7.a02.azurefd.net/</code>	<code>https://cas-api-cdn-ep-eu-g5d6bhadh5gvd0fh.a02.azurefd.net/</code>	<code>https://cas-api-cdn-ep-aps-a0fwd8c3d7bbfxdt.a02.azurefd.net/</code>
API Services	<code>https://api.analytics.cloud.com/</code>	<code>https://api.analytics-eu.cloud.com/</code>	<code>https://api.analytics-aps.cloud.com/</code>
API Services (Performance Analytics)	<code>https://api-a.was.cloud.com/</code>	<code>https://api-eu-a.was.cloud.com/</code>	<code>https://api-aps-a.was.cloud.com/</code>
	<code>https://api-b.was.cloud.com/</code>	<code>https://api-eu-b.was.cloud.com/</code>	<code>https://api-aps-b.was.cloud.com/</code>
Get Public IP	<code>https://locus.analytics.cloud.com/</code>	<code>https://locus.analytics.cloud.com/</code>	<code>https://locus.analytics.cloud.com/</code>
Event Hub (Not applicable for Citrix ADM agent)	<code>https://citrixanalyticseh-alias.servicebus.windows.net/</code>	<code>https://citrixanalyticseheu-alias.servicebus.windows.net/</code>	<code>https://citrixanalyticsehaps-alias.servicebus.windows.net/</code>
	<code>https://citrixanalyticseh2-</code>	<code>https://citrixanalyticseh2eu-</code>	

ENDPOINT	UNITED STATES REGION	EUROPEAN UNION REGION	ASIA PACIFIC SOUTH REGION
	<code>alias.servicebus.windows.net/</code>	<code>alias.servicebus.windows.net/</code>	
	<code>https://citrixanalyticseh3-alias.servicebus.windows.net/</code>		
Event Hub (For Citrix ADM agent)	<code>https://cas-eh-ns-alias.servicebus.windows.net/</code> and <code>https://cas-eh-ns2-alias.servicebus.windows.net/</code>	<code>https://cas-eh-ns-eu-alias.servicebus.windows.net/</code>	<code>https://cas-eh-ns-aps-alias.servicebus.windows.net/</code>
Bulk Upload	<code>https://casstoragebulk.blob.core.windows.net/</code>	<code>https://casstorebulkeu.blob.core.windows.net/</code>	<code>https://casstorebulkaps.blob.core.windowss.net/</code>

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, {{page.cvad-onprem-product-name}}, 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	<code>casnb-0.citrix.com:9094</code>	<code>casnb-eu-0.citrix.com:9094</code>	<code>casnb-aps-0.citrix.com:9094</code>
	<code>casnb-1.citrix.com:9094</code>	<code>casnb-eu-1.citrix.com:9094</code>	<code>casnb-aps-1.citrix.com:9094</code>
	<code>casnb-2.citrix.com:9094</code>	<code>casnb-eu-2.citrix.com:9094</code>	<code>casnb-aps-2.citrix.com:9094</code>
	<code>casnb-3.citrix.com:9094</code>		

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, {{page.cvad-onprem-product-name}}, 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 {{page.daas-product-name}} \(formerly Citrix Virtual Apps and Desktops service\)](#)
- [Security considerations for {{page.cvad-onprem-product-name}}](#)

- [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

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

NOTE:

Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

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.

ROLE	PERMISSION
Performance Analytics - Read Only Administrator	Assigns read-only access permission to the Citrix Cloud administrators of Performance Analytics.
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.

[Select all](#) | [Deselect All](#)

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

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

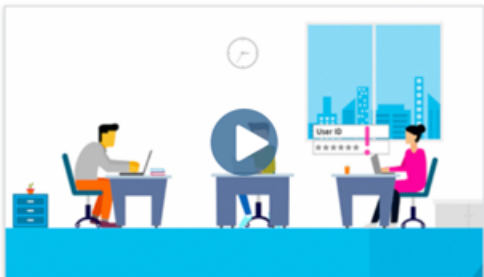
For Security Analytics and Performance Analytics, after you have the necessary subscriptions or are authorized to access the trial, on the Analytics overview page, the **Request Trial** button for the offering changes to **Manage**. Click **Manage** to view the user dashboard corresponding to each offering.

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

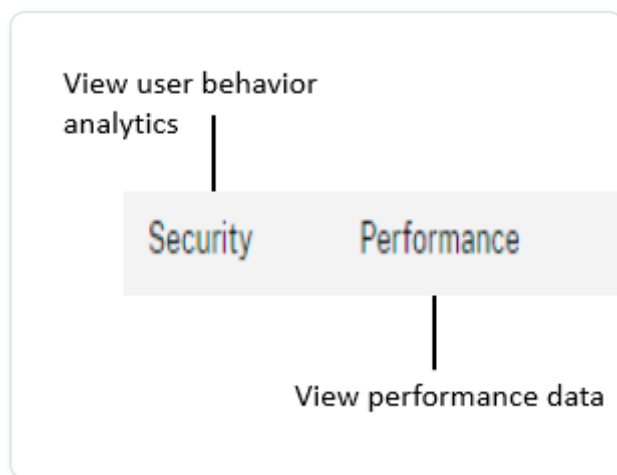
- [Citrix Analytics for Security](#)
- [Citrix Analytics for Performance](#)

Find your way around

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

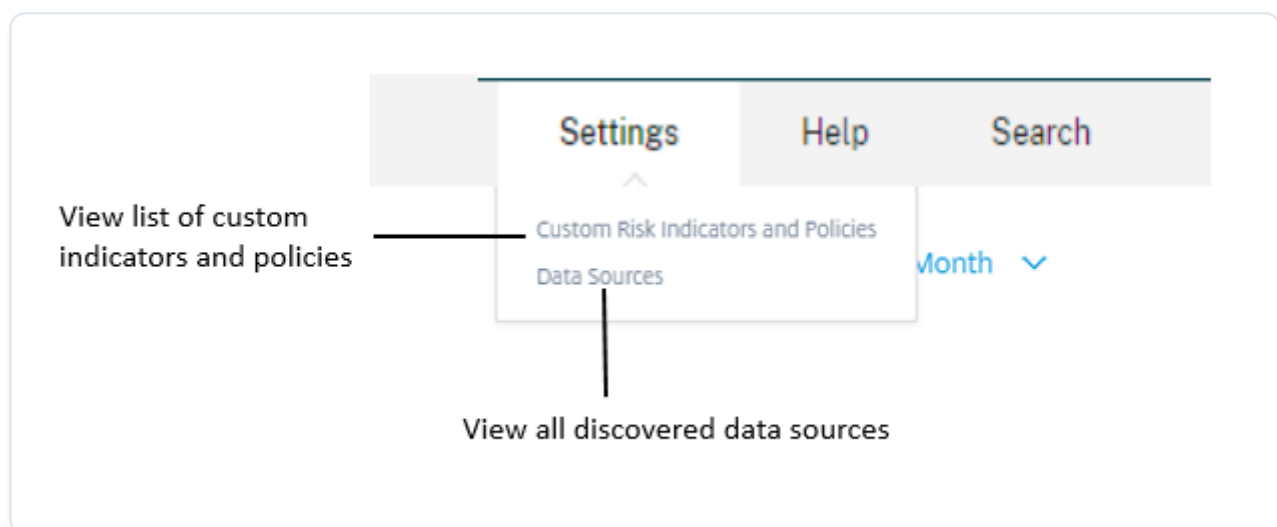
Top bar

Navigate to the various Analytics offerings from the top bar.

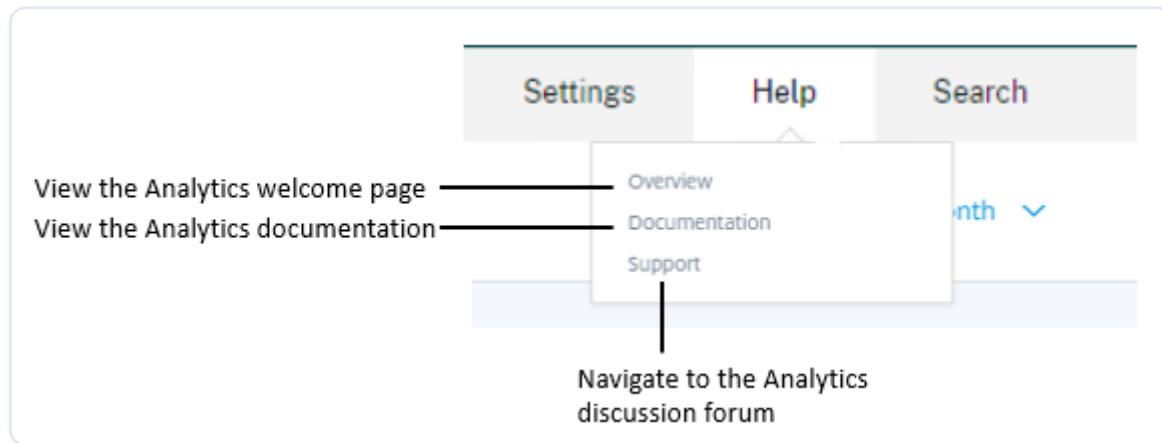


Settings menu

From the **Settings** menu, navigate to the [Indicators and Policies](#) page or the [Data Sources](#) page.

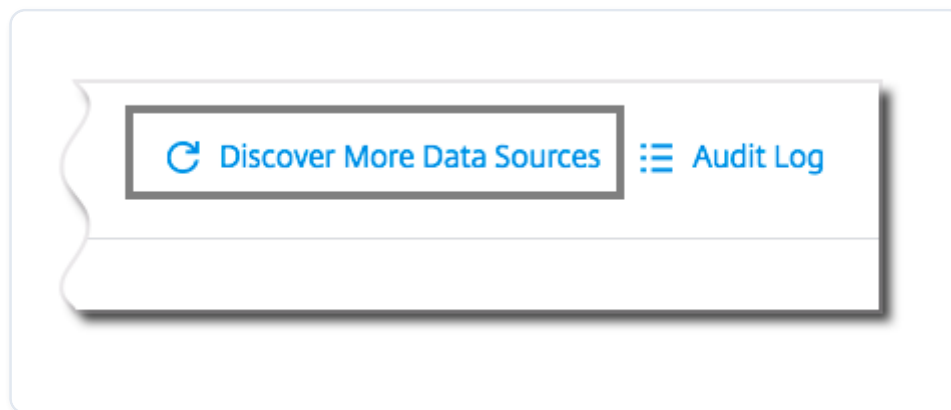


Help menu



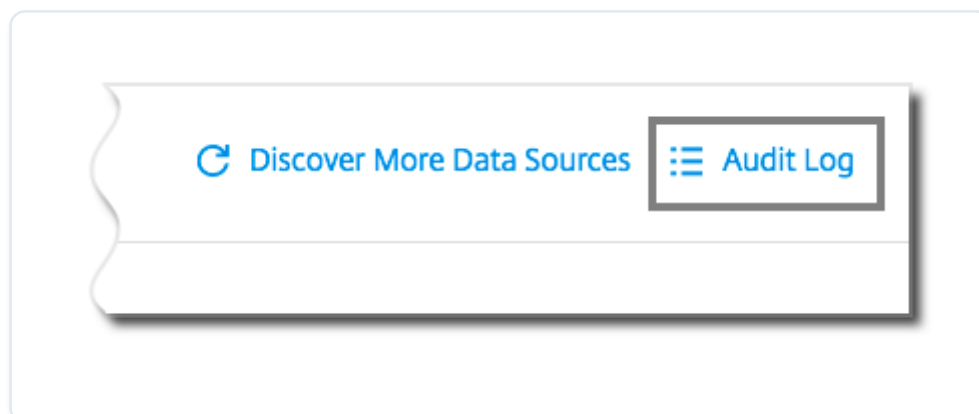
Discover more data sources

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

layout: doc replicate-from: /commons/self-service-search.md

Alert settings

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

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.

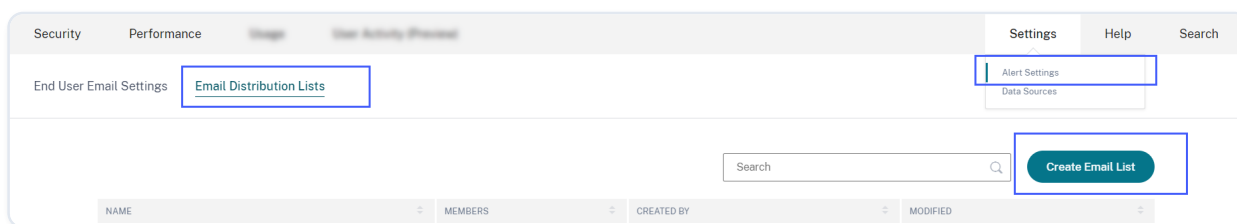
With the email distribution list, you can do the following:

- 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.

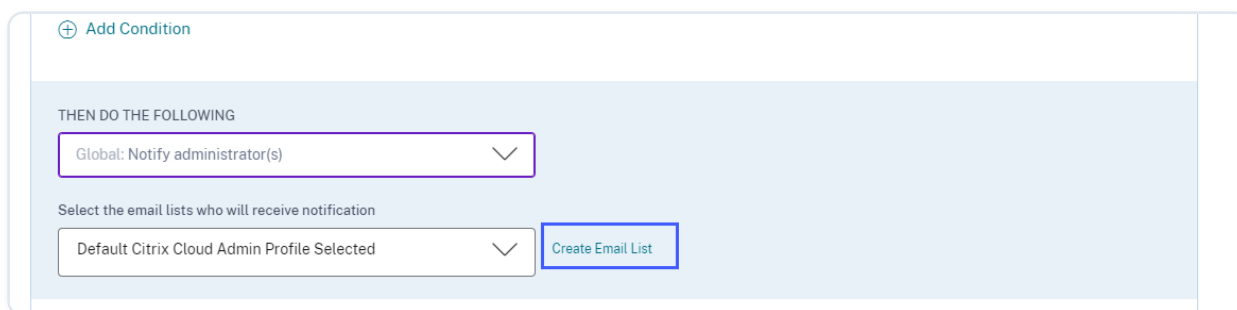
Create email distribution list

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.



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

+

- 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

- 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.

Email Distribution Lists			
End User Email Settings		Webhooks	
		Search	Create Email List
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 Dhalaria	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.

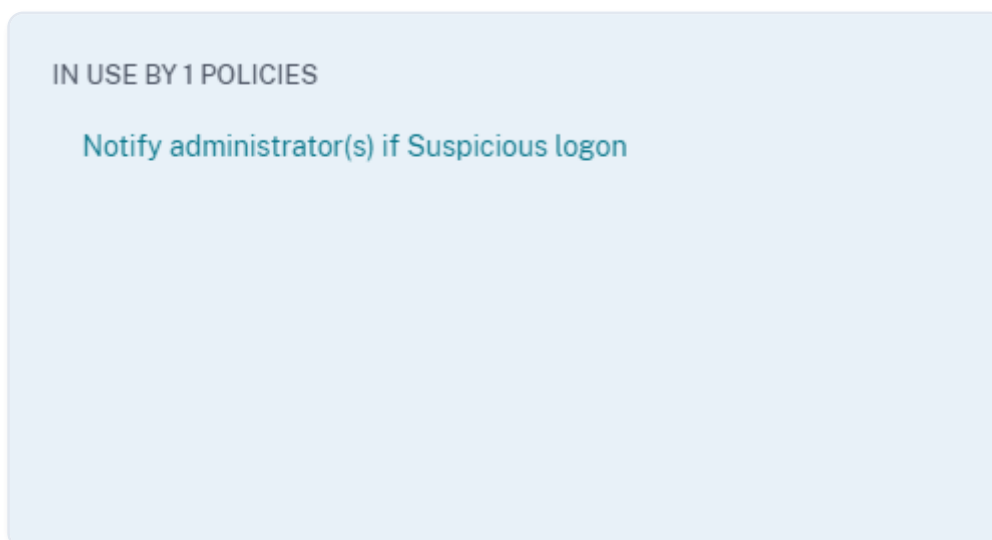
3. On the email distribution list, update the required details such as name, description, and add or remove members.
4. Click **Save Changes**.

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.



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

Modify Policy Delete Policy

IF THE FOLLOWING CONDITION IS MET

Citrix Content Collaboration: Excessive file downloads

[Add Condition](#)

THEN DO THE FOLLOWING

Notify administrator(s)

Select the email lists who will receive notification

Citrix administrators - default list, test - modified ... Create Email List

☒ Citrix administrators - default list	6 members
☐ xyz	6 members
☒ test - modified	2 members
☒ creating email profile test	1 member

[Apply](#) [Cancel](#) [Save Changes](#)

- Click **Save Changes** and go back to the email distribution list.
- 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:

- Sign in to Citrix Analytics.
- Depending on your subscribed offering, click **Manage** to access Security Analytics or Performance Analytics.

- From the top bar, click **Settings > Alert Settings > Webhook**.
- Select **Create Webhook**.

The screenshot shows a 'WEBHOOK CONFIGURATION' form. It has three main sections: 'WEBHOOK PROFILE NAME' with a text input containing 'Test Webhook in Staging'; 'DESCRIPTION (optional)' with a text area containing 'Created for testing end to end functionality using policies'; and 'WEBHOOK CONFIGURATION' which includes a 'Method' dropdown set to 'POST', a 'Webhook URL' input containing 'https://hooks.slack.com/services/', and a 'Message' section with a text area containing a JSON payload:

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

. A 'Learn More' link is present next to the message instruction.

- Enter a profile name and a description of the webhook to identify its purpose.
- Select the HTTP method and the webhook URL of your application to send the alert message.
- 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.
- (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.
- 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.

Sending alert message to Slack

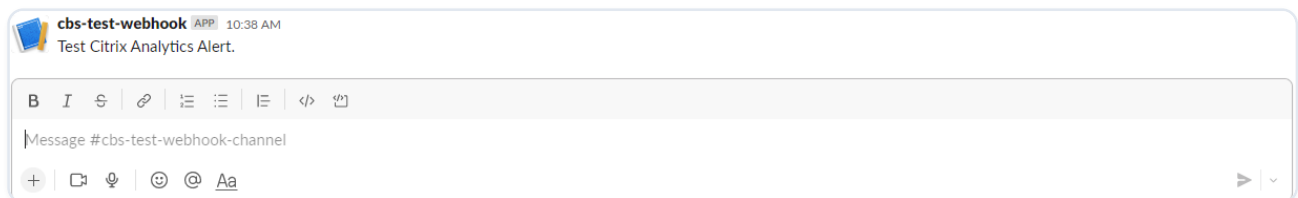
On Slack, ensure that you have completed the following tasks before sending an alert:

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



Sending alert message to Microsoft Teams

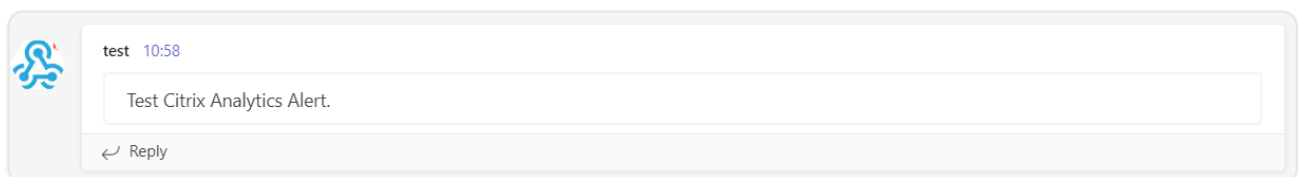
On Microsoft Teams, ensure that you have completed the following tasks before sending an alert:

1. Create a Teams group within Teams if you don't have already one.
2. Create a Webhook connector. 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



Citrix Analytics for Security™ (Security Analytics)

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](#).



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.
- [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)

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 stand-alone offering or bundled along with Citrix Analytics for Security. To subscribe to Citrix Analytics for Performance, see <https://www.citrix.com/products/citrix-analytics-performance.html>).
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	<code>https://trust.citrixnetworkapi.net</code>	<code>https://trust.citrixnetworkapi.net</code>	<code>https://trust.citrixnetworkapi.net</code>
Citrix Cloud	<code>https://trust.citrixworkspacesapi.net</code>	<code>https://trust-eu.citrixworkspacesapi.net</code>	<code>https://trust-aps.citrixworkspacesapi.net</code>
Citrix Analytics	<code>https://api.was.cloud.com</code>	<code>https://api-eu.was.cloud.com</code>	<code>https://api-aps.was.cloud.com</code>
Bulk Upload	<code>https://citrixanalyticseh-alias.servicebus.windows.net/</code>	<code>https://citrixanalyticseheu-alias.servicebus.windows.net/</code>	<code>https://citrixanalyticsehaps-alias.servicebus.windows.net/</code>
Bulk Upload	<code>https://citrixanalyticseh2-alias.servicebus.windows.net/</code>	<code>https://citrixanalyticseh2eu-alias.servicebus.windows.net/</code>	

ENDPOINT	UNITED STATES REGION	EUROPEAN UNION REGION	ASIA PACIFIC SOUTH REGION
Bulk Upload	https:// citrixanalyticse h3- alias.servicebus .windows.net/		

Access

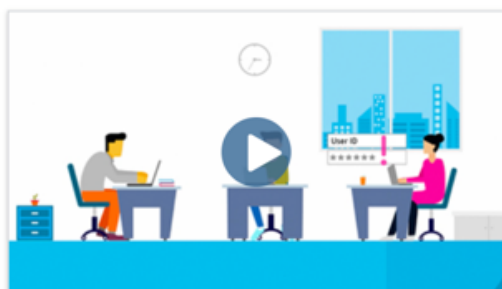
1. Log on to Citrix Cloud. Look for the Analytics service tile and click **Manage**. The overview page displays the offerings available in the Analytics portfolio.
2. In the **Performance** offering, to use the trial version of the offering, click **Request Trial**. If you have bought the Citrix Analytics 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.

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

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



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.

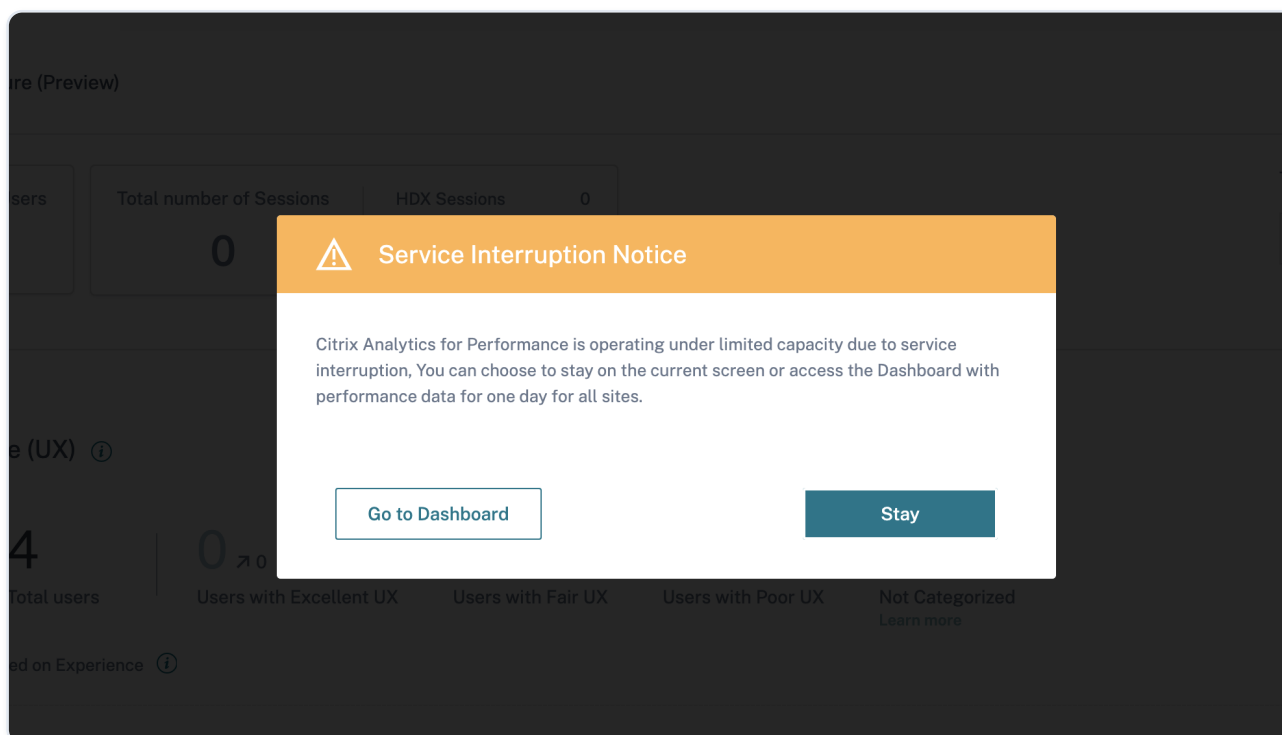
NOTE:

- 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.

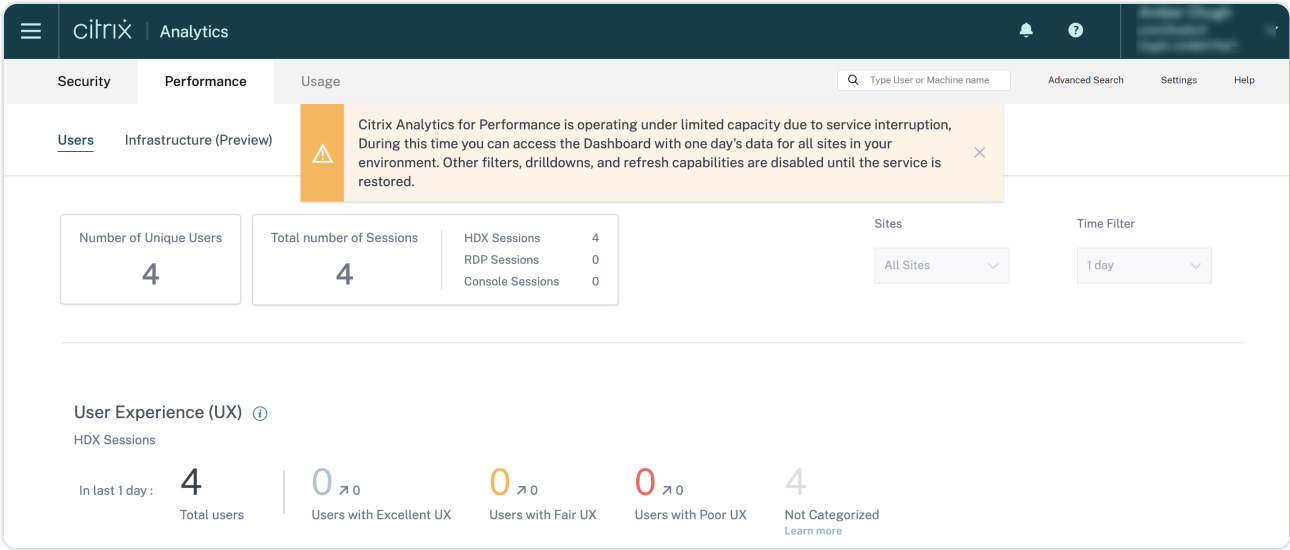
Service Continuity

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.



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.



This update improves product resiliency and helps align with the [Service Level Agreement](#).

Troubleshoot Citrix Analytics for Security and Performance

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

Verify anonymous users as legitimate users

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

Troubleshoot event transmission issues from a data source

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

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

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

Configured Session Recording server fails to connect

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

Configuration issues with Citrix Analytics add-on for Splunk

layout: doc replicate-from: /commons/troubleshoot-citrix-analytics-for-security-and-performance/splunk-add-on-debugging.md

Unable to connect StoreFront™ server with Citrix Analytics

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

FAQs

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

Glossary of terms

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

Citrix Analytics Document History

The following table describes important changes to the Citrix Analytics platform documentation. To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	DESCRIPTION
18 Jun 2024	Added Azure AD or Active Directory note related to Microsoft Entra	Added a note on Microsoft Entra. Learn more
21 Sep 2023	Updated What's New	A new PowerShell script has been introduced that automates the process and simplify StoreFront On-boarding. Learn more.
01 Aug 2023	Removal of Citrix Analytics - Usage	Citrix Analytics - Usage is no longer available for customers.
30 Nov 2022	Removed outdated information.	Removed outdated information of How to buy Citrix Analytics - Usage -DOCFB-15128.
28 Sep 2022	Updated What's new	Webhooks for Alert Notifications Learn more
22 Sep 2022	Removed a known issue.	Removed CAS-66973 known issue as that is fixed now.
16 Sep 2022	Removed dead link.	Removed the dead link for Analytics demo. Learn more.
14 Sep 2022	Added new log fields.	Added new fields in Citrix Virtual Apps and Desktops

DATE	CHANGE	DESCRIPTION
		and Citrix DaaS logs. Learn more.
08 Sep 2022	Updated What's new	Added 100 K rows support using Export to CSV format feature. Learn more.
18 Aug 2022	Updated Fixed issues	Added Fixed issue. Learn more.
10 Aug 2022	Updated Citrix Virtual Apps and Desktops data source	Added StoreFront onboarding without site aggregation information. Learn more.
06 May 2022	Updated Known issues	Added Known issues and updated the existing one. Learn more.
20 Apr 2022	Updated Manage administrator roles for Citrix Analytics	Added the custom roles specific to Performance Analytics. Learn more.
05 Apr 2022	Updated What's new	Secure Workspace Access labels renamed as Secure Private Access. Learn more.
21 Mar 2022	Updated What's new	Added fixed issue- CAS-64126. Learn more.
10 Feb 2022	Updated Self-service search	Added the auto-suggest feature in the search box. Learn more.
20 Dec 2021	Updated What's new	Access Control labels renamed as Secure Workspace Access. Learn more.
06 Dec 2021	Updated What's new	Announced Citrix Analytics general availability in the Asia Pacific region. Learn more.

DATE	CHANGE	DESCRIPTION
06 Dec 2021	Updated Technical security overview	Updated the network requirements for the Asia Pacific region. Learn more.
06 Dec 2021	Updated Data governance	Updated the data residency policy for the Asia Pacific region. Learn more.
19 Aug 2021	Updated What's new	Added feature. Learn more.
19 Aug 2021	Updated Self-service search	Added support for the IS EMPTY operator. Learn more.
07 Jun 2021	Updated What's new	Removed Try Demo link from Analytics overview page. Learn more.
07 Jun 2021	Updated Getting started	Removed Try Demo link from Analytics overview page. Learn more.
18 May 2021	Updated What's new	Added enhancements and a fixed issue- CAS-50224. Learn more.
18 May 2021	Updated Self-service search	Added support for * operator with != operator. Updated the new search bar. Learn more.
31 Mar 2021	Updated What's new	Added a feature. Learn more.
31 Mar 2021	Updated Self-service search	Added the IN and NOT IN operators. Learn more.
18 Mar 2021	Updated What's new	Added a feature. Learn more.
18 Mar 2021	Updated Self-service search	Added support for the NOT LIKE (!~) operator. Learn more.

DATE	CHANGE	DESCRIPTION
23 Feb 2021	Updated What's new	Added features. Learn more.
23 Feb 2021	Updated self-service search	Added email delivery schedule and export visual summary. Learn more.
03 Dec 2020	Updated topic- Technical security overview	Added Get Public IP endpoint and updated Kafka broker endpoints. Learn more.
12 Nov 2020	Updated topic- What's new	Added a feature. Learn more.
20 Oct 2020	Updated topic- What's new	Added a feature. Learn more.
09 Jul 2020	Updated topic- What's new	Added deprecated support. Learn more.
09 Jul 2020	Updated topic- System requirements	Removed Internet Explorer 11 from the supported browser list. Learn more.
09 Jul 2020	Updated topic- Find your way around	Removed the Alerts feature. Learn more.
02 Jul 2020	Updated topic- Citrix Analytics overview page	Added information about how to buy Citrix Analytics. Learn more.
02 Jun 2020	Updated topic- What's new	Redesigned the Analytics overview page and renamed the Operations tab to Usage on the top bar. Learn more.
14 May 2020	Updated topic- System requirements	Updated the system requirements. Learn more.
11 May 2020	Updated topic- Technical security overview	Corrected the endpoint URLs in the Network requirements section. Learn more.

DATE	CHANGE	DESCRIPTION
02 Apr 2020	Updated topic- Troubleshoot Citrix Analytics	Updated information about StoreFront onboarding. Learn more.
23 Mar 2020	Updated topic- Overview	Added Citrix Analytics - Fundamentals in the Analytics offerings list. Learn more.
20 Feb 2020	Updated topic- What's new	Updated the fixed issue CAS-18657. Learn more.
20 Feb 2020	Updated topic- Data governance	Updated the data governance logs. Learn more.
09 Jan 2020	Updated topic- What's new	Added the fixed issues CAS-26297. Learn more.
18 Dec 2019	Updated topic- What's new	Added the fixed issue CAS-27922. Learn more.
12 Dec 2019	Updated topic- Data governance	Analytics supports events from the Microapps service in Asia Pacific South.
12 Dec 2019	Updated topic- What's new	Added a feature. Learn more.
04 Dec 2019	Updated topic- What's new	Added the fixed issue CAS-27368. Learn more.
22 Nov 2019	Updated topic- Getting started	Redesigned Analytics overview page for easy access to each offering. Learn more.
22 Nov 2019	Updated topic- What's new	Added a feature. Learn more.
21 Oct 2019	Added topic- Technical security overview	Know about the security best practices, data flow, network requirements, and security

DATE	CHANGE	DESCRIPTION
		responsibilities when using Analytics. Learn more.
21 Oct 2019	Updated topic- What's new	Added a feature. Learn more.
11 Sep 2019	Updated topic- What's new	Added the fixed issue CAS-20559. Learn more.
20 Aug 2019	Updated topic- What's new	Added the fixed issue CAS-20906. Learn more.
31 Jul 2019	Updated topic- What's new	Added support for the European Union region. Learn more.
26 Jun 2019	Updated topic- What's new	Added the fixed issue CAS-19867. Learn more.
19 Jun 2019	Updated topic- What's new	Added the fixed issue CAS-19930. Learn more.