Citrix Analytics for Performance™

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

Contents

What's new 3

Known Issues 52

Data Sources 53

Configuring on-premises Citrix Virtual Apps and Desktops Sites with Citrix Analytics for Performance™ 59

Data Governance 66

Data Export to Observability Platform (Preview) 96

Splunk Integration with Citrix Analytics for Performance™ 99

Elasticsearch integration 108

Grafana integration 117

Data Structure of the Sessions Events 123

Data Structure of the Machines Events 140

Data export via REST APIs (Preview) 146

Citrix Analytics ODATA API 147

Data Structure of the users events 157

Data Structure of the Sessions Events 161

Data Structure of the Machines Events 169

Power BI integration for Citrix Performance Analytics 173

Limits 180

Manage Administrator Roles for Performance Analytics 181

User Experience Analytics 183

User Experience Score 193

User Experience (UX) Factors 197

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

Infrastructure Analytics **208**

Connector Statistics **213**

Session Details **216**

Machine Statistics **220**

N/A or Not Categorized Metrics **232**

Self-service search **243**

Self-Service Search for Performance **262**

Insights **284**

Alerts **297**

Custom Reports (Preview) **318**

Citrix Analytics offerings **324**

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

What's new

September 11, 2025

A goal of Citrix® is to deliver new features and product updates to customers as and 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 helps to ensure product quality and to maximize the availability.

It is possible that the updates mentioned in this documentation are being rolled out and are not accessible to all customers at the same time.

New features introduced in Citrix Analytics for Performance™ provide further insights into performance parameters affecting the user experience on Citrix Virtual Apps and Desktops on-premises sites and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) sites on cloud.

Dec 28, 2023

Custom Reports export in CSV format

You can now export raw data as CSV format attachments in Custom Report emails apart from the PDF format.
You can create various reports of sessions and machines and download the raw data from the Custom Reports (Preview) tab. You can download reports in PDF, CSV, or both formats.

This feature provides stakeholders periodical access to raw data without needing direct access to Citrix Analytics for Performance. For more information, see Custom Reports.

Endpoint Network telemetry of Citrix Workspace™ app for Windows version 2311 sessions launched in hybrid mode

Citrix Analytics for Performance now extends visibility into key Endpoint Network telemetry for virtual apps and desktops sessions that are launched in hybrid mode. The Endpoint Network telemetry is available in Citrix Analytics for Performance for sessions from Citrix Workspace app for Windows version 2311 and later. The Endpoint Network telemetry available are Network Interface Type (Ethernet/ WiFi), Endpoint Link Speed, Endpoint Throughput (Incoming and outgoing), and WiFi Signal Strength.

Virtual sessions are said to be launched in hybrid mode when you log on to Citrix Workspace app through the Citrix Workspace for Web browser and launch the applications or desktops through the native Citrix Workspace app.

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

For more information about the available metrics, see Self-service search for Sessions.

Dec 19, 2023

Endpoint Network telemetry of Citrix Workspace app for Linux version 2311 sessions launched in hybrid mode

Citrix Analytics for Performance now extends visibility into key Endpoint Network telemetry for virtual apps and desktops sessions that are launched in hybrid mode. The Endpoint Network telemetry is available in Citrix Analytics for Performance for sessions from Citrix Workspace app for Linux version 2311 and later. The Endpoint Network telemetry available are Network Interface Type (Ethernet/ WiFi), Endpoint Link Speed, Endpoint Throughput (Incoming and outgoing), and WiFi Signal Strength.

Virtual sessions are said to be launched in hybrid mode when you log on to Citrix Workspace app through the Citrix Workspace for Web browser and launch the applications or desktops through the native Citrix Workspace app.

For more information about the available metrics, see Self-service search for Sessions.

Dec 12, 2023

Simplified search for users and machines

You can now search for sessions or machines that were active over the last week from the dashboards using the user name or the machine name respectively. A new search box is provided on the top navigation bar of the User Experience and Infrastructure dashboards for this. Provision of this simplified search helps discover user or machine related information and triage issues easily. The existing search in the self-service view continues to provide advanced search facilities with filters to slice and dice the search results.

Machine Statistics view enhancements

You can now view the successful sessions running on the machine during the selected time period from the Machine Statistics view. A **Total Sessions** field is added in the **Machine Statistics** > **Sessions** tab. Clicking the Total Sessions number opens the Sessions self-service view with the corresponding set of sessions displayed. You can further drilldown and inspect the session metrics from the Session Details view.

Also, you can now click the **Session Failure** number, the bars in the chart displaying the session failures, and the categorized session counts to view the sessions. This feature makes the Machine Statistics a comprehensive view of all machine-related metrics required to triage and fix issues related

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

to the machine and the sessions running on the machine. For more information, see the Machine Statistics article.

Nov 15, 2023

Metrics relevant to session state displayed in Sessions self-service view

Expanding a row in the **Sessions self-service** view > **Data** table view displays the corresponding session metrics. Now only the metrics that are relevant for the session state are displayed. If the session was in a disconnected state during the selected time interval, session metrics related to responsiveness and bandwidth, that are not applicable for disconnected sessions are not displayed. For a failed session, the failure reason and type are displayed to help triage the reason for the session failure. Any columns added to the table that are not relevant for the session state is displayed as "–".

This feature ensures that displayed session metrics are relevant to the session state. For more information, see Self-service search for Sessions.

Oct 26, 2023

Additional metrics in Sessions self-service view

To support triaging session-related issues, the following session and failure related metadata are now available as optional columns in the Sessions based self-service view. This provides more visibility into the details of failure at individual session level.

- **Failure Type** –Indicates the kind of session failure from among the following values:
- **Failure Reasons** –Indicates the exact reason for the failure. You can resolve the failure using the corresponding recommended steps in Citrix Director failure reasons and troubleshooting.
- **Session Type** –Indicates if the session is an application or a desktop session.
- **Session State** –Indicates the state of the session.
- **Session End Time** –Indicates the time at which the session ended.

You can filter the view using these additional columns. The column values are included in export reports and are available as dimension parameters in during the creation of session-based Custom Reports.

The failure metrics help understand the reason for a session failure and the recommended steps to resolve the failure. This feature is especially helpful when you navigate from the failed session count on the dashboard to a filtered set of failed sessions in the Sessions self-service view. For more information, see Self-service search for Sessions.

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

Improved accuracy of Session Score and other session metrics

Session Score and the other session performance and factors metric charts in the Session Details view now take into account the disconnected duration of the session. This consideration enables the overall Session Score and associated metrics to be an accurate representation of the session performance. The session-disconnected interval is represented in the all charts and tooltips. For more information, see the Session Details article.

Sep 25, 2023

Customize Alert Parameters

Citrix Analytics for Performance now provides the ability to customize the alert parameters.

Alert policies are pre-built with default parameter values. To modify the alert parameters, click the alert policy name to open the **Modify Alert** window and modify the values of the listed parameters to suit your environment. Subsequent alert notifications are generated based on the custom conditions.

Updating the alert parameters also alters the calculation of the corresponding insight on the UX dashboard.

In alerts where re-alerting is supported, you can also control the re-alerting preference. Alert notifications are resent if the re-alert preference is set to **Enabled** and the conditions as specified in the re-alert preference persist.

Customized alerts are more relevant to your environment, they help identify anomalies easily, and are more dependable for proactive monitoring.

For more information, see Alerts.

Sep 14, 2023

Support for endpoint metrics from Citrix Workspace apps for Linux

Citrix Analytics for Performance now supports the availability of endpoint metrics from Citrix Workspace apps for Linux version 2308 and later launched in native mode. You can see metrics like Endpoint Link Speed, Endpoint Throughput Incoming, Endpoint Throughput Outgoing and WiFi Signal Strength, Endpoint Throughput Incoming, and Endpoint Throughput Outgoing coming from Citrix Workspace apps for Linux.

For more information, see the Citrix Workspace app versions matrix.

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

Sep 05, 2023

New Custom Report templates

Two new Custom Report templates based on users and machines data sources are now available in Citrix Analytics for Performance. You can access the new templates from the **Reports (Preview)** tab.

- The **User Experience Category Trends over Last Seven Days** template is based on the Users data source. Custom reports based on this template contain trends of Excellent, Fair and Poor users based on their User Experience Score plotted over the last seven days.
- The **Machine State Trends over Last Seven Days** template is based on the Machines data source. Custom reports based on this template contain trends of machines based on the Machine States - Ready for Use, Active, Maintenance, Unregistered, and Failed - plotted over the last seven days.

Also, you now have a wider choice of metrics to select as plotting parameters. For more information regarding the creation of Custom Reports using templates, see Custom Reports.

Exclude delivery groups from receiving alerts

You can now specify delivery groups to be excluded from receiving alert notifications. You can remove unused delivery groups or those created for testing purposes from the alerting process. This feature helps reduce alert fatigue and improve the relevance of alerts. For more information, see Alerts.

Aug 31, 2023

Anomalous Session Disconnects Baseline Insight and Alert

Anomalous Session Disconnects Baseline Insight is introduced to indicate the number of session disconnects and its deviation from the baseline value. The user-specific baseline value is calculated using the P80 count of session disconnects measured over the last 30 days. For more information, see Insights.

The Anomalous Session Disconnects out-of-the-box alert policy is introduced to track the number of session disconnects. If the number of session disconnects exceeds the baseline value by 30% or more and if more than 5% of the sessions are impacted by the disconnects, an alert notification is sent using the configured channel. For more information, see Alerts.

New alert policies based on Baseline Insights

New out-of-the-box alert policies based on the existing Baseline Insights are now defined for:

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

- Sessions with Poor Logon Duration
- Session with Poor Responsiveness
- Session Failures

The alerts are generated when the number of impacted sessions exceeds the 30-day baseline value by 30% or more and more than 5% of the sessions are impacted by this increase. The alerts can be configured to be notified by mail or webhook like the other Performance Analytics alerts. The alert policies are available in the Alert Policies tab.
For more information, see Alerts.

Aug 18, 2023

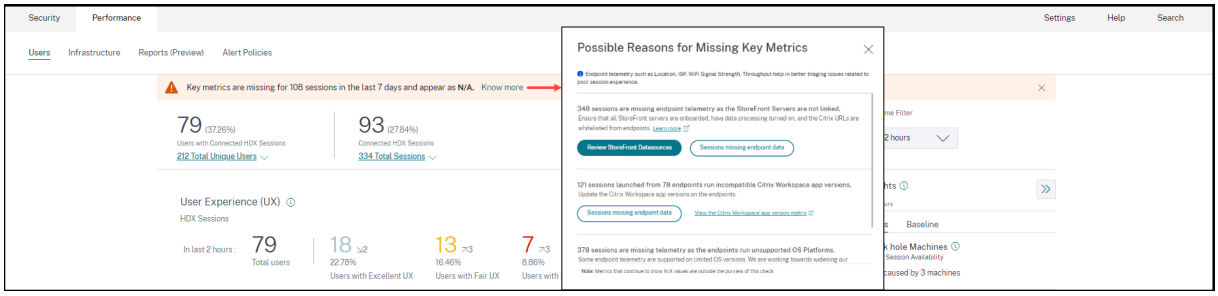
Discover reasons for missing endpoint metrics

Data availability is important to optimally analyze your Citrix Virtual Apps and Desktops™ environments. Endpoint metrics like Location, ISP, WiFi Strength and Throughput are important indicators that help triage poor session experience. Endpoint metric values might be missing if the appropriate prerequisites are not met.

This feature helps easily identify issues resulting in endpoint metrics having N/A values and suggests appropriate actions.

Drilldown from Dashboard The User Experience dashboard contains a banner displaying the number of sessions whose endpoint metrics have not been available during the last 7 days.

Clicking **Know more** displays a modal box with the key reasons for sessions missing endpoint metrics, the number of sessions affected by each reason during the last 7 days and the actions that you could take to fix them.



- One of the key reasons for missing endpoint telemetry is StoreFront™ onboarding. StoreFront must be onboarded correctly; data processing must be switched on and appropriate URLs must be whitelisted. Clicking **Review StoreFront Data Sources** takes you to the Data Sources page that leads you through the StoreFront onboarding process required for the Workspace App data collection. If you are using Citrix Workspace, the service is automatically discovered and does not require onboarding.

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

- Endpoint telemetry is not available for sessions launched from endpoints that run unsupported OS platforms or incompatible Citrix Workspace app versions. Clicking **Sessions missing endpoint data** opens the Sessions self-service view with the list of the sessions missing endpoint telemetry due to a specific listed reason. For more information, see the Version matrix that lists for each feature the OS versions and the required Workspace app version on which it is supported.

For more information, see the Not Categorized article.

Tooltips in the Sessions Self-service view Tooltips elaborating the reasons for N/A values are now available in the Sessions self-service view for the following endpoint-related metrics:

- Workspace App Version
- Endpoint Country (Last known)
- Endpoint City (Last known)
- Endpoint Link Speed (P95)
- Endpoint Throughput Incoming (P95)
- Endpoint Throughput Outgoing (P95)
- ISP (Internet Service Provider)

Tooltips are displayed on the N/A values of these metrics with the reasons as incorrect StoreFront onboarding, or sessions launched from endpoints that run unsupported OS platforms or incompatible Citrix Workspace app versions.
This feature helps to educate on the reasons for N/A values so that you can take the necessary action.
For more information about the metrics available in the Sessions self-service view, see Self-service view for sessions.

Aug 01, 2023

Alert information as CSV attachments in mailers

Black hole Machines, Overloaded Machine and Zombie Session alerts emails now have CSV attachments containing information about the affected machines and sessions.
The attachment has the following data:

- Machine Name
- Site ID
- Catalog Name
- Delivery Group Name
- Failure count (Number of failed machines or sessions as applicable).

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

The CSV attachments in alert mailers help identify faulting machines and sessions without having to log on to Citrix Analytics for Performance. This helps establish automation pipelines to create and forward tickets to stakeholders responsible for speedy resolution of issues. The feature helps improve communication and efficiency and is the next step to achieve proactive monitoring of your virtual apps and desktops environment.

For more information about available alerts, see Alerts.

Jun 06, 2023

Alert email notifications for non-administrator Citrix Cloud™ accounts

You can now enable the Citrix Analytics for Performance alert email notifications for stakeholders who don't have administrator access to your Citrix Cloud account. This enables members of your organization's security and auditing teams who do not hold Citrix Cloud accounts to be able to get alert notifications.

This update ensures that the alert notifications are available to administrators who take action to mitigate the alert condition. This helps speedy resolution of issues and ensures an optimal performance of the virtual apps and desktops environment. For more information, see the Email distribution list.

For more information regarding alerts from Citrix Analytics for Performance, see Alerts.

Jun 05, 2023

User count in Sessions Self-service view

The Visual Summary in the Sessions Self-service view now displays the user count along with the session count. This feature provides a quick overview of the number of users impacted during an incident or because of a specific issue. It also helps understand the number of unique users for a specific query. For more information, see the Sessions self-service article.

May 22, 2023

Connector-Gateway PoP Latency

Connector-Gateway PoP Latency is now displayed on the Connector Statistics page. The values represent the P95 values of the synthetic latency calculated for the available Gateway PoPs in your virtual apps and desktops environment.

This information helps you choose and configure the closest Gateway PoP to achieve the optimum session experience. For more information, see Connector Statistics.

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

Connector-Gateway PoP Latency is also available in the Sessions self-service view as an optional column. For more information about the metrics available on the Sessions Self-service view, see the Sessions self-service article.

May 16, 2023

Patterns detected in Black hole Machine Insights

Some machines in your environment though registered and appearing healthy might not service sessions brokered to them, resulting in failures. Machines that have failed to service four or more consecutive session requests are termed as Black hole machines. The Black hole machines insights show the number of black hole machines identified in your environment during the selected time period.

Now, top failure patterns detected with respect to the Delivery Group, single and multi-OS session machines is displayed on the Black hole machine insights panel and in the alert mail. These patterns are aimed to help you spot if there is a specific cohort of users experiencing the issue. In cases where the system is unable to highlight any pattern due to a distributed cohort, it is recommended to drill down to self-analyze.

For more information, see Diagnostic Insights: Black hole machines and Alert for Black Hole Machines.

Anomalous Latency Alerts based on user-specific baseline values

The **Sessions with Anomalous latency** alert that was based on a machine learning model to determine the latency value for all Delivery Group-Location pairs for a specific customer is now redeveloped to use a baseline latency value at a user level. The user-specific baseline is calculated using the P95 ICARTT values measured over the last 30 days.

Poor in-session responsiveness has been a common complaint for poor session experience among most users. The Anomalous Latency proactive alerts help administrators identify only those users with latency deviation from their own 30-day baseline latency. The user-specific baseline ensures meaningful comparison and appropriate alerting compared to checking against a static threshold.

You can now publish the Anomalous Latency alert notifications from Performance Analytics to a preferred Webhook listener in addition to receiving them via email.

For more information, see the Alerts article.

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

Apr 28, 2023

Data Availability

Accuracy of Performance Analytics depends on the data collected from various site infrastructure like the endpoints, machines, Gateway, and Delivery Controller. A good availability of the required metrics ensures that the data and insights provided by Performance Analytics closely represents the actual performance of the site.

The **Data Availability** feature helps identify sessions that do not have the data required to monitor the performance of your endpoints. Endpoint metrics like Endpoint Link Speed, Location, Throughput, ISP, Network Interface type, OS and Endpoint receiver version that are critical to analyze issues specific to endpoints.

Endpoint metrics require that the StoreFront/ Citrix Workspace be onboarded correctly, and the Citrix Workspace App versions installed on the endpoints are correct. Clicking the Data Availability icon on the User Experience (UX) Dashboard shows the number of sessions across all the onboarded sites which don't have endpoint metrics during the past seven days. Clicking the session number opens the Sessions Self-service view listing these sessions.

To improve Data Availability:

- Check if the corresponding StoreFront/Citrix Workspace has been onboarded correctly as described in Onboard Citrix Virtual Apps and Desktops on-premises sites using StoreFront.
- Check if the endpoints are on the correct Citrix Workspace app version for the Endpoint Network Statistics feature as per Citrix Workspace app version matrix.

For more information, see the Performance Analytics article.

Endpoint IP and Name

Endpoint IP and name are added as columns on the Sessions Self-service view. This provides more visibility into the client-side network. For more information, see Self-service search for Sessions.

Apr 13, 2023

Integration of Citrix Analytics for Performance with the Splunk Observability platform (Preview)

Citrix Analytics for Performance is now integrated with the Splunk Observability platform. You can use the **Data Export** feature to export performance data and events from Citrix Analytics for Performance to Splunk.

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

You can get a holistic view of the performance metrics of all on-premises Citrix Virtual Apps and Desktops sites and DaaS cloud services that have been onboarded to your Citrix Analytics for Performance service on the Observability platform. Further, you can combine and correlate performance metrics from Citrix Analytics for Performance data with the external data sources connected within your Splunk instance.

You can create dashboards and reports in a regular cadence and derive actionable business insights into the performance of your virtual apps and desktop sites.

For more information, see the Data Export article.

To leverage this functionality, sign up and enroll to the Technical Preview using this form.

Apr 04, 2023

Custom Roles Support for Citrix Cloud Administrator Groups

You can now assign Citrix Cloud administrator groups in your Azure Active Directory with custom roles to access Citrix Analytics for Performance. The administrator groups must be configured on Citrix Cloud using Identity and Access Management > Administrators. For more information, see Identity and access management.

This integration enables a streamlined approach to manage service access permissions for administrator users and groups.

For more information on managing roles, see Manage Administrator Roles for Performance Analytics.

Feb 20, 2023

Support for 100K machines

Citrix Analytics for Performance is now optimized to support 100K machines. To know the recommended configuration and usage limits of Citrix Analytics for Performance, see the Limits article.

Feb 01, 2023

ISP, Endpoint Link Speed, and Endpoint Location visibility

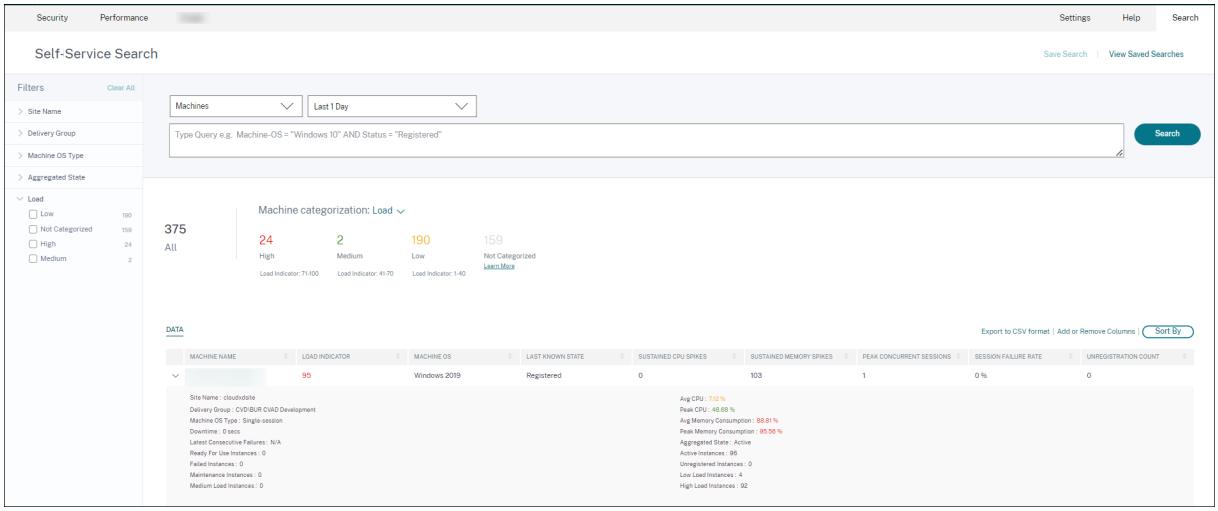
The Sessions Details page now contains the ISP, Endpoint Link Speed, and Endpoint Location information. These additional session attributes help easier triaging. This feature is valuable to help-desk administrators accessing the Citrix Analytics for Performance from Director to troubleshoot session-related issues. For more information about all the session attributes, see the Session Details article.

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

Jan 23, 2023

Machine Load Indicator in Machines Self-Service View

Machine Load metrics based on the Load Indicator are added in the Machines Self-Service View. These metrics help quickly check the load on machines without having to drill down to multiple machine parameters like the CPU usage, memory utilization, and the number of sessions on the machine.



1. The Machines self-service view now shows machine categorization based on the Load Indicator of the machines. Load Indicator for a machine is calculated based on the resource utilization, the overall user experience on the machine and the number of sessions hosted in the case of multi-session OS machines. The value is aggregated over the selected time period.
   In the Machines self-service view, select **Load** in the Machine categorization dropdown. The machines are categorized as follows:
   - High (red) - Machines with Load Indicator in the range 71-100
   - Medium (green) –Machines with Load Indicator in the range 41-70
   - Low (amber) –Machines with Load Indicator in the range 1-40.
   - Not Categorized - The machines might not be categorized if they are in shutdown, unregistered, or failed state or if the resource data is not available for the machine.
2. The **Load** facet with High, Medium, Low, and Not Categorized options help filter the machines to help further analysis.
3. Machines self-service view has a Load Indicator column that shows the load score of the machine. The machine performance parameters available upon expansion of the machine row now show the number of High, Medium and Low Load Instances for the selected period. This helps quantify and evaluate the load on the specific machine.

This feature helps identify machines that are underutilized or overloaded. This further enables proactive action to ensure optimal usage of the infrastructure and improve the overall machine perfor-

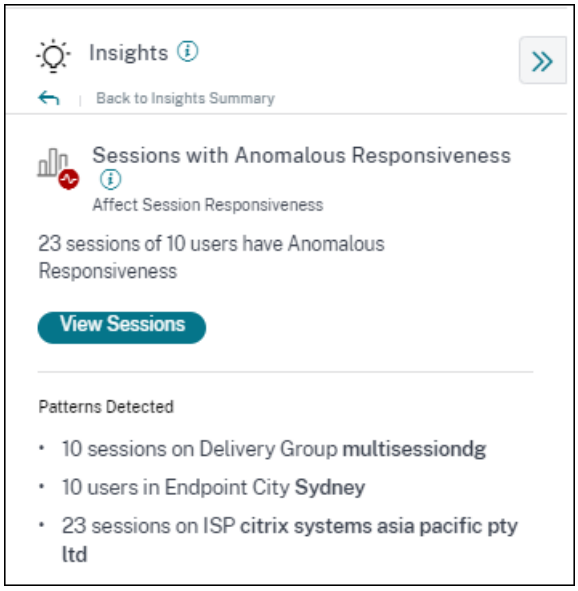
© 1997–2026 Citrix Systems, Inc. All rights reserved.

mance. For more information, see the Self-service article.

Jan 02, 2023

Baseline Insight on Sessions with Anomalous Responsiveness

The Sessions with Anomalous Responsiveness Baseline Insight shows the number of sessions that have recorded ICARTT values that are higher than the baseline ICARTT for the user. The user-specific baseline is calculated using the P95 ICARTT values measured over the last 30 days. Sessions with anomalous responsiveness are detected by comparing the current ICARTT measurements of the sessions with the user-specific baseline.



This insight helps quickly identify users experiencing poor in-session experience as compared to their own previous experience. The feature helps proactively monitor the environment and quickly troubleshoot issues related to session performance.

For more information, see the Insights article.

Dec 14, 2022

Custom Reports (Preview)

You can now create and schedule custom reports using the performance metrics in Citrix Analytics for Performance. Custom reports help you to extract information of specific interest and organize the data graphically. It helps create executive reports in a regular cadence and analyze the performance of your environment over time. For more information, see Custom Reports.

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

Nov 18, 2022

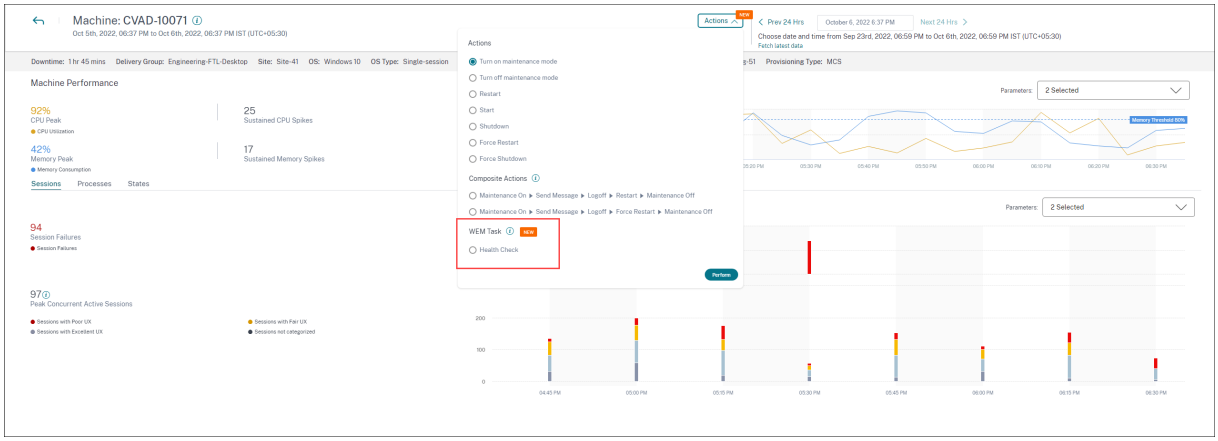
Machine Catalog, Hypervisor, and Provisioning Type visibility

The Machine Statistics page now displays the Hypervisor Name, Catalog Name, and Provisioning Type of the machine as a part of the key machine parameters. This data helps triage issues related to machine performance. Specifically, this data helps find similar machines which might have performance issues, using the Hypervisor, Catalog or Provisioning type attributes. For more information, see the Machine Statistics article.

Oct 13, 2022

WEM Health Check

You can now perform health checks on machines from Performance Analytics. Workspace Environment Management™ (WEM) is a user environment management tool that helps optimize desktops for the best possible user experience. The new WEM Task Health Check action introduced on the Machine Statistics page helps run WEM scripts to get information on the status of machines.



This helps root cause common machine issues easily without having to go to the WEM terminal.

A detailed report of the WEM Health Check and possible actions that can be performed to fix them is also provided.

WEM Actions are enabled for Cloud admins with full access and valid entitlement to WEM.

For more information regarding the usage of the WEM Task Health Check action in Performance Analytics, see WEM Tasks - Health Check.

For more information regarding the WEM Task Health Check, see the Scripted Tasks article in the Workspace Environment Management documentation.

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

Oct 11, 2022

Process Visibility Improvements

Now, processes running on single-session OS machines are also displayed in the **Process** tab of the Machine Statistics view along with processes running on multi-session OS machines. This feature is available for machines running on cloud and on-premises environments.
Up to 10 top resource consuming processes are displayed in the **Process** tab.
The top resource-consuming processes are displayed even if there are no memory or CPU spikes during the selected time period.
This feature requires that you enable the **Process Monitoring policy** from Citrix Studio for both, single-session and multi-session OS machines. This policy is disabled by default, and must be enabled explicitly to view the processes running on the machine. For more information, see the Machine Statistics article.

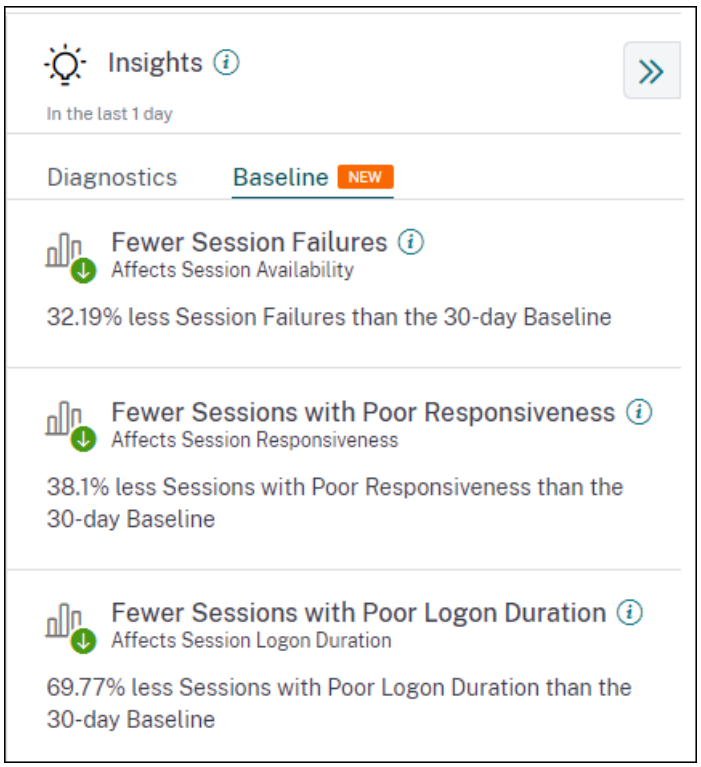
Sep 30, 2022

Baseline Insights

Insights are now displayed in two categories:

- **Diagnostic Insights:** The Blackhole Machines, Zombie Sessions, Overloaded Machines and Communication Error Diagnostic Insights are available on the Diagnostic sub-pane. These insights give crucial updates about failures that have occurred on the site.
- **Baseline Insights:** The Baseline Insights are introduced to show the deviation of key performance metrics from the historical baseline. These insights show if key metrics are improving or deteriorating in a glance. They help spot incident indicators quickly and take proactive steps to improve the performance of your environment.

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



Baseline Insights for Poor Session Failures, Session Responsiveness, and Session Logon Duration are available on the Baseline subpane.

Deviation from the baseline is also displayed on the User Experience dashboard. They are available for Session Failures under the User Sessions section and the Poor Sessions categorized under the Session Responsiveness and Session Logon Duration sections. Clicking the deviation displays the respective Baseline Insight.

For more information, see the Insights article.

Sep 28, 2022

Webhook Support for Alerts Notifications

You can now publish alert notifications from Performance Analytics to a preferred Webhook listener. This feature allows you to get notified on your chosen channel such as Slack, JIRA. This helps enterprise customers automate the flow from incident detection to closure, and hence easily drive workflows in response to Performance Analytics Alert notifications. For more information about configuring alert policies with webhook, see Webhook Support for Alerts Notifications.

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

Sep 07, 2022

Export limit in CSV export increased

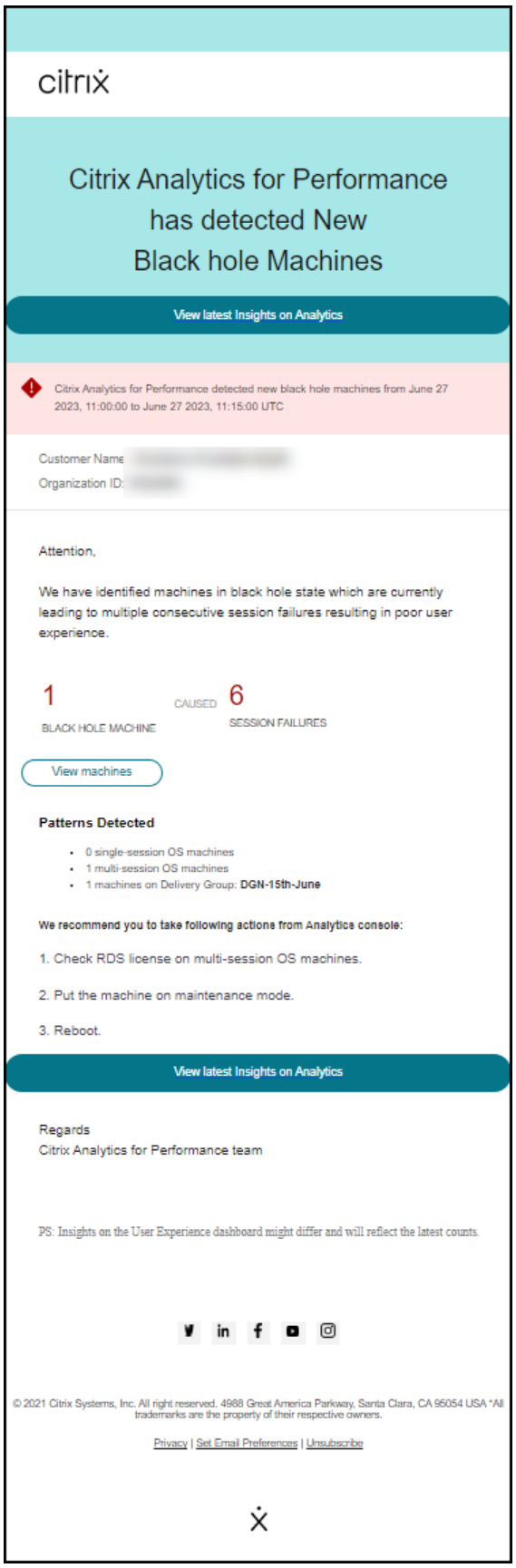
The limit on the number of rows that you can export using the **Export to CSV format** feature on the Self-service pages is now increased from 10K rows to 100 K rows. For more information regarding the export functionality, see the Self-service search article.

Aug 05, 2022

Black Hole Machines Alert

Citrix Analytics for Performance scans for black hole machines every 15 minutes and sends out an alert to enable administrators to proactively mitigate session failures faced by users due to black hole machines. Machines that have failed to service four or more consecutive session requests are termed as Black hole machines. With black hole failure alerting, administrators need not log into Performance Analytics to know the session failures that occurred due to black hole machines.
Details of the machines and the session failures caused by them are sent in the alert mails to administrators. The **Black Hole Machines** alert policy must be enabled to receive these mails.

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



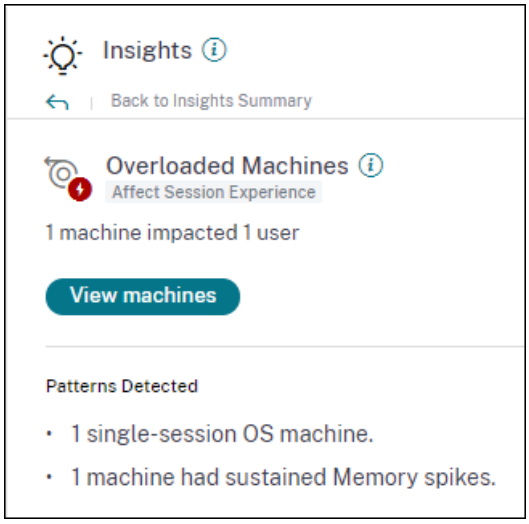
© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information about Black Hole Machine Alerts, see the Alerts article.

July 29, 2022

Overloaded Machines - Insights and Alerts

Insights on overloaded machines are available on the User Experience dashboard.

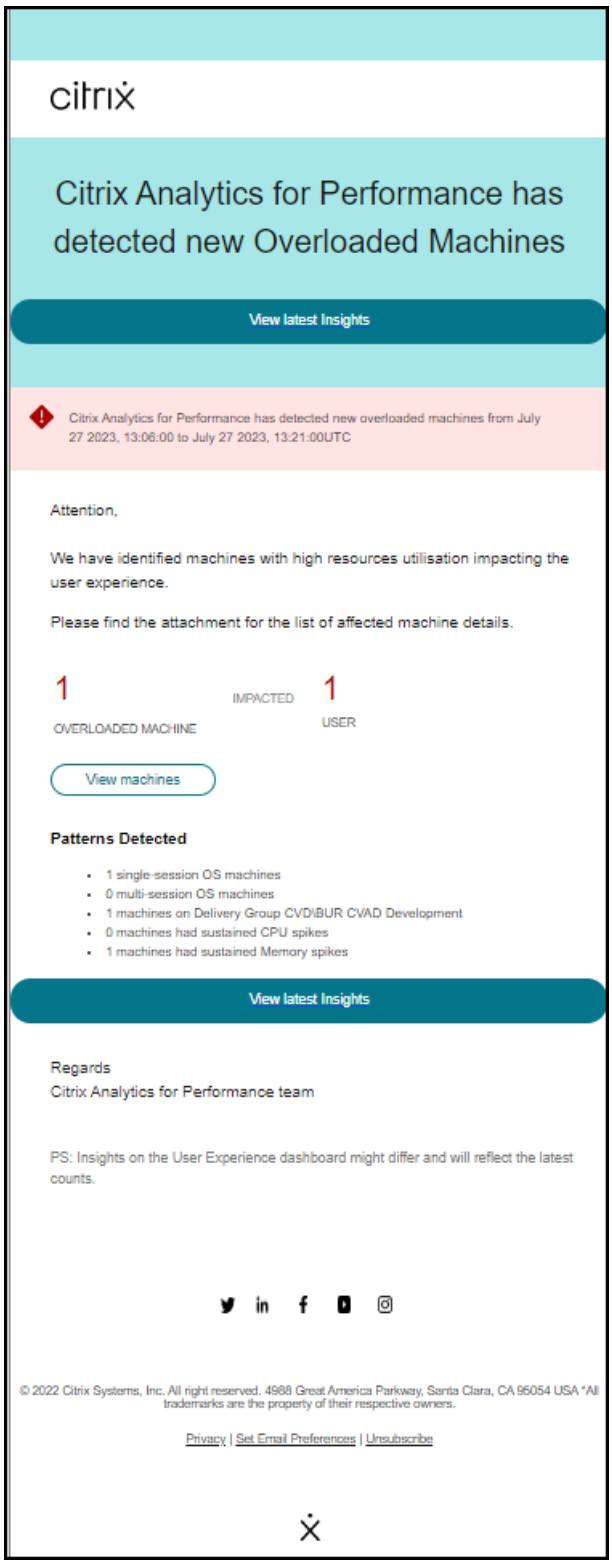


Machines that have experienced sustained CPU spikes, or high memory usage, or both, that have lasted for 5 minutes or more, resulting in a poor user experience are considered to be overloaded. The Overloaded Machines insight shows the number of overloaded machines causing poor user experience and the number of users affected during the selected duration.

For more information, see Overloaded Machine Insights.

An Overloaded Machines alert mail is sent to administrators when a new overloaded machine is detected in the environment in a 15 mins interval. A re-alert mail is sent if the same machine remains in the overloaded condition after 24 hours. The administrators are re-alerted up to three times regarding machines that continue to be overloaded. Pro-active alerting helps administrators who are not currently logged on to Citrix Analytics for Performance detect and handle overloaded resources.

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



For more information, see Overloaded Machine Alerts.

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

July 18, 2022

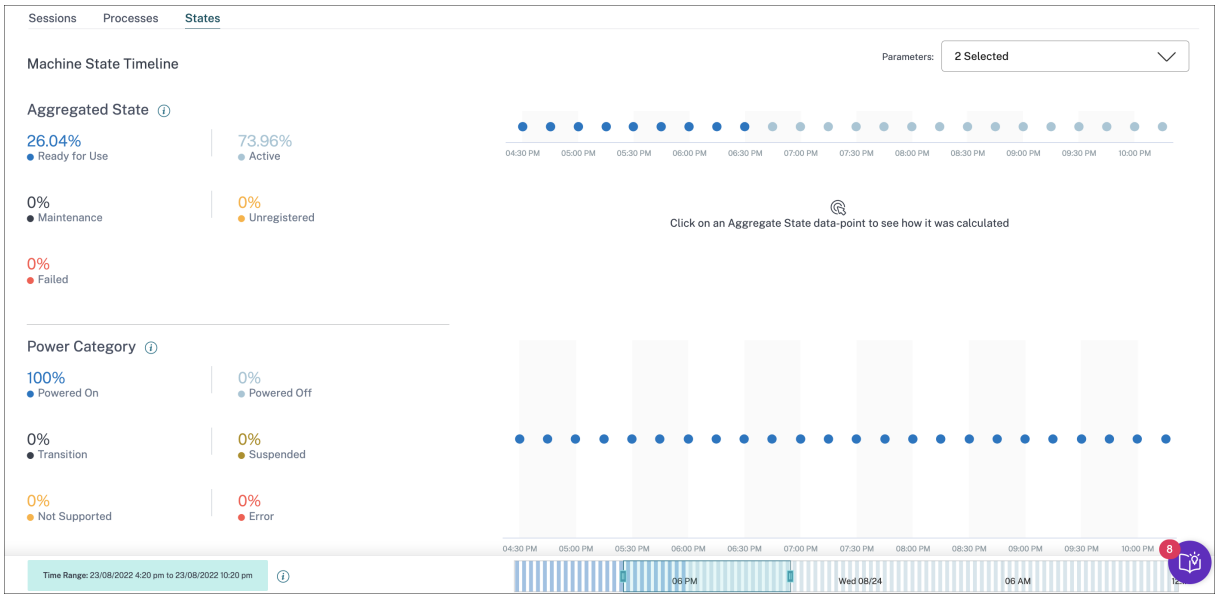
Machine States

The Machine Statistics page now includes information on Machine States. The **States** tab shows the timeline of **Machine Aggregated State** and **Machine Power Category** plotted at 15 min intervals for the last 24 hours.

Clicking an Aggregated State data point helps understand how it was calculated. A breakdown of the actual values of Machine State and Maintenance Mode that resulted in the plotted Aggregated State is displayed. This helps comprehend the machine's state changes over time. Failure Type and Deregistration Reason help debug machine issues.

Hover over the Power Category data point to see the actual Power State the machine has been in.

This feature helps slice and dice important parameters concerning the machines in the environment and spot inefficiencies easily. Along with the Sessions and Processes information already available in this view, the Aggregated State and Power Category transition over time gives in-depth information to troubleshoot machine issues.



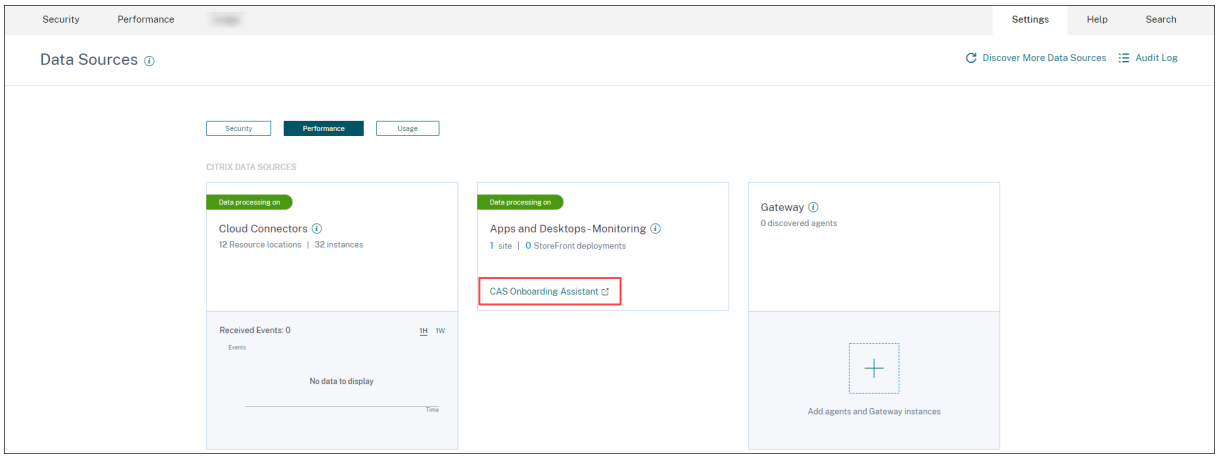
For more information, see the Machine Statistics article.

Citrix Analytics Service (CAS) Onboarding Assistant

The Citrix Analytics Service Onboarding Assistant tool helps troubleshoot issues while onboarding StoreFront with the Citrix Analytics service. The StoreFront server might fail to connect to Citrix Analytics after importing the configuration settings from Citrix Analytics to the StoreFront server. CAS Onboarding Assistant automates all the checks and prerequisites mentioned in the document, Unable to connect StoreFront server with Citrix Analytics. For more information on the usage and to download

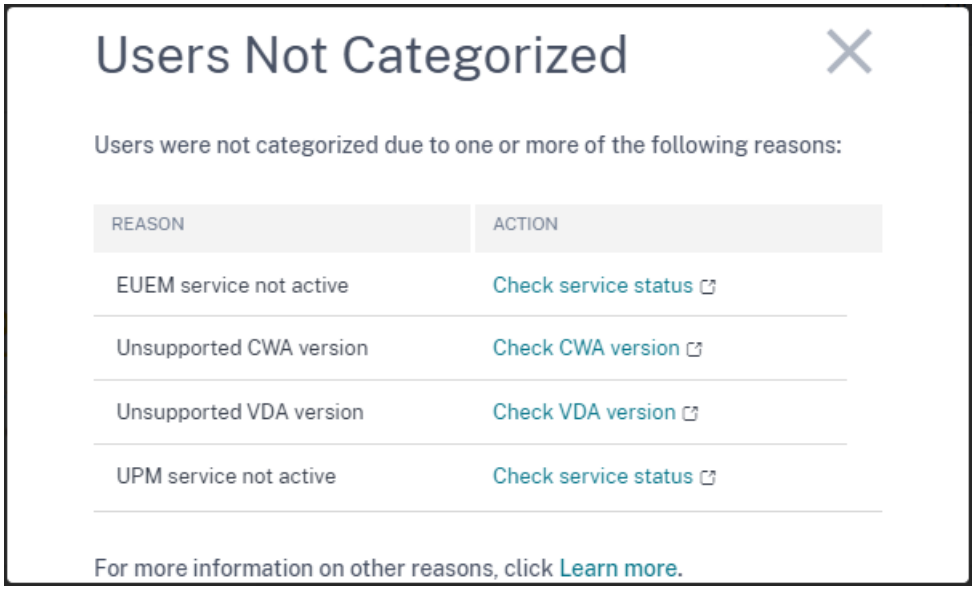
© 1997–2026 Citrix Systems, Inc. All rights reserved.

the tool, see the Knowledge Center article, Citrix Analytics Service Onboarding Assistant.



Reasons for Users or Sessions being Not Categorized

Users and sessions that cannot be classified into excellent, fair, or poor categories due to configuration issues or dependencies are classified as Not Categorized. The **Know more** link below the Not Categorized classification in the User Experience and Session Responsiveness trends displays the primary reasons for certain users and sessions not being categorized. This feature provides the clarity required to quickly discover and fix any configuration issues.



For more information, see the Not Categorized article.

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

Jun 08, 2022

User and Session Classification in Percentages

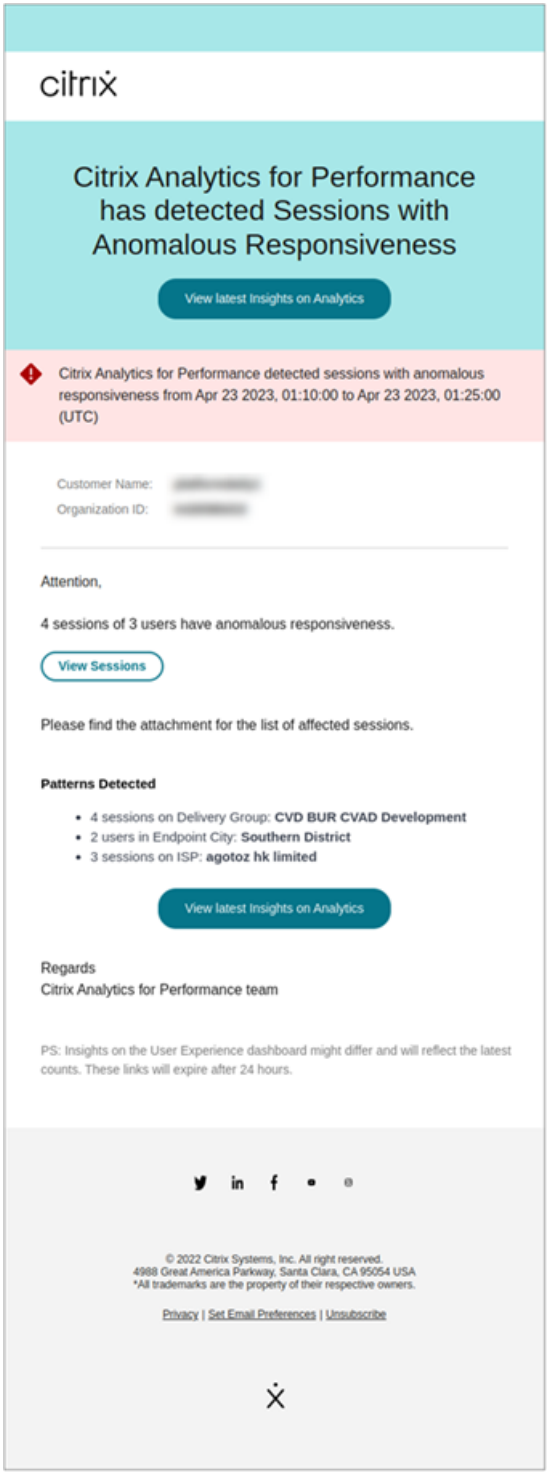
The User Experience dashboard shows the classification of connected HDX™ users and sessions as excellent, fair, and poor. These numbers are now displayed in percentages as well.

Apr 28, 2022

Anomalous Latency Alerts

Poor in-session responsiveness is the primary cause for poor session experience. The Anomalous Latency Alerts feature alerts administrators when there is a significant deviation in the session latency values. The proactive alerting helps administrators identify specific locations or Delivery Groups from which poor sessions might be originating.

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



A machine learning model is used to determine the baseline latency value for all Delivery Group-Location pairs for a specific customer. The baseline latency value is calibrated every day based on the ICARTT values from the last three days. Any outlier measurements of ICARTT are ignored. If the measured ICARTT has a deviation of 60% or more from the baseline latency value, an alert is generated.

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

For more information, see the Alerts article.

Apr 20, 2022

Performance Analytics specific Custom Access roles

Custom Access Roles specific to Citrix Analytics for Performance are now available. As a Citrix Cloud administrator with Full access permission, you can invite other administrators to manage Performance Analytics in your organization using the following roles.

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

You can provide read-only or full access permissions to your administrators and allow them to manage the various features of Performance Analytics. This update allows you to create administrators and provide access based on a specific Citrix Analytics offering.
The users with the Read Only Administrator role that was available earlier is now renamed to Security & Performance - Read Only Administrator.

Read Only Performance Analytics users can access and use the User Experience and Infrastructure Dashboards like the Full Administrators. However, Machine Actions on the Machine Statistics page are disabled for read-only users. Administrators with read-only access will not receive alert notifications from Citrix Analytics.

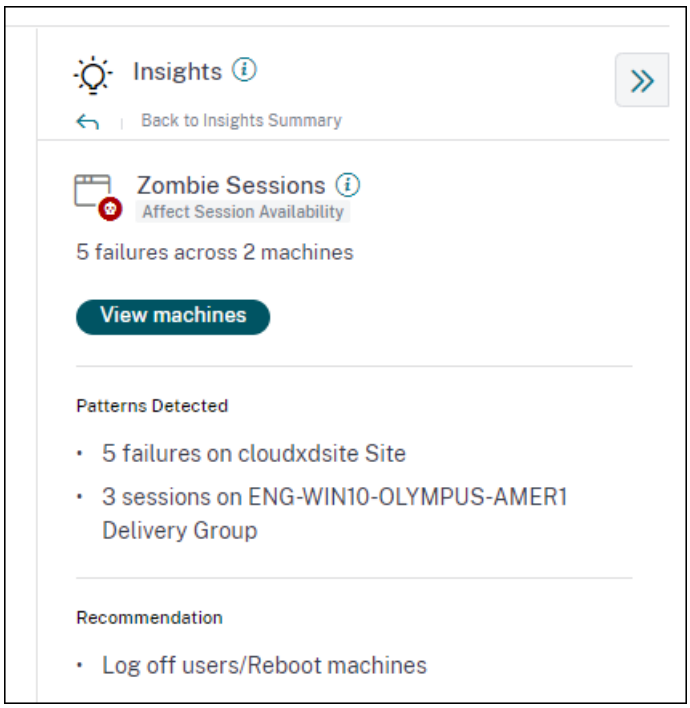
For more information on the actions allowed on the Self-service view, see the Self-Service article.

Apr 14, 2022

Zombie Insights and Alerts

The Zombie Sessions subpane shows information on session failures that have occurred due to zombie sessions in the environment. A zombie session is an abandoned session on a single-session OS machine resulting in new session launches on the machine to fail. Attempts to launch sessions on this machine fails with an Unavailable Capacity error until the abandoned session is terminated. Zombie Sessions insights aim to help spot these machines with abandoned sessions, thus enabling proactive mitigation of these failures.

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



A Zombie session alert mail is generated when a new machine with a zombie session is detected in the environment in a 15 mins interval. Alert mails are sent to full administrators who have enabled email notifications in Citrix Cloud.
Re-alerting on the same machine is done only if the same-abandoned session persists on the same machine for over 24 hours from the initial detection.

Clicking **View machines** displays the Self-service view filtered with the list of machines containing Zombie Sessions. Here, Failure Count represents the number of session failures that have occurred in the selected interval. The Last Failure Type and Reason help root cause reasons for machines containing zombie sessions.

You can disable the Machines with Zombie Sessions alert from the **Alert Policies** tab.



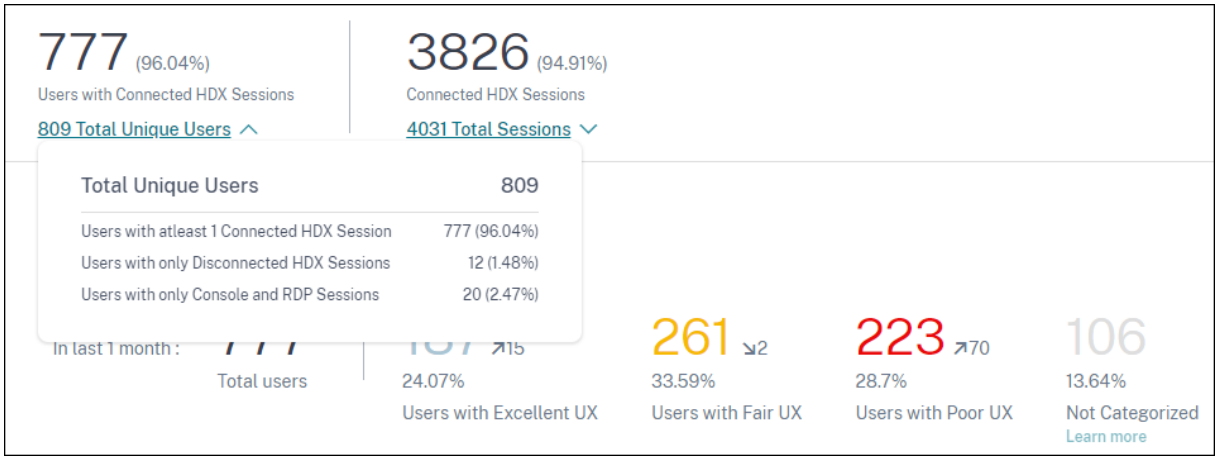
For more information, see Zombie sessions.

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

Apr 14, 2022

Breakup of Unique Users and Sessions Numbers

This feature brings more clarity to the **Not Categorized** numbers on the User Experience dashboard. The dashboard now shows the breakup of users and sessions in the virtual apps and desktops environment based on the session protocol and the connection status.



The dashboard provides performance metrics for only connected HDX sessions. Sessions that have been disconnected throughout during the selected period indicates that the user was not active for the entire selected period. Hence, Session and User Experience scores are not applicable for disconnected sessions.

With this feature, disconnected sessions and users are no longer in the Not Categorized classification. They are now available in the breakup. This reduces the number of users and sessions in the overall Not Categorized classification. For more information, see Breakup of Users and Sessions.

Apr 14, 2022

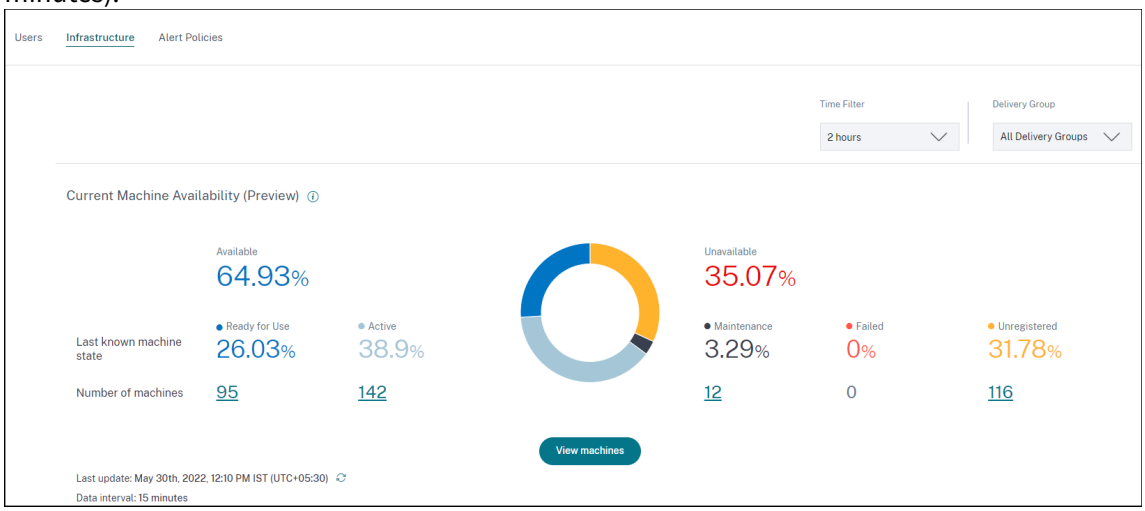
Infrastructure Dashboard Enhancements

The Infrastructure dashboard that shows the availability and performance analytics for virtual machines in your apps and desktops environment has the following enhancements.

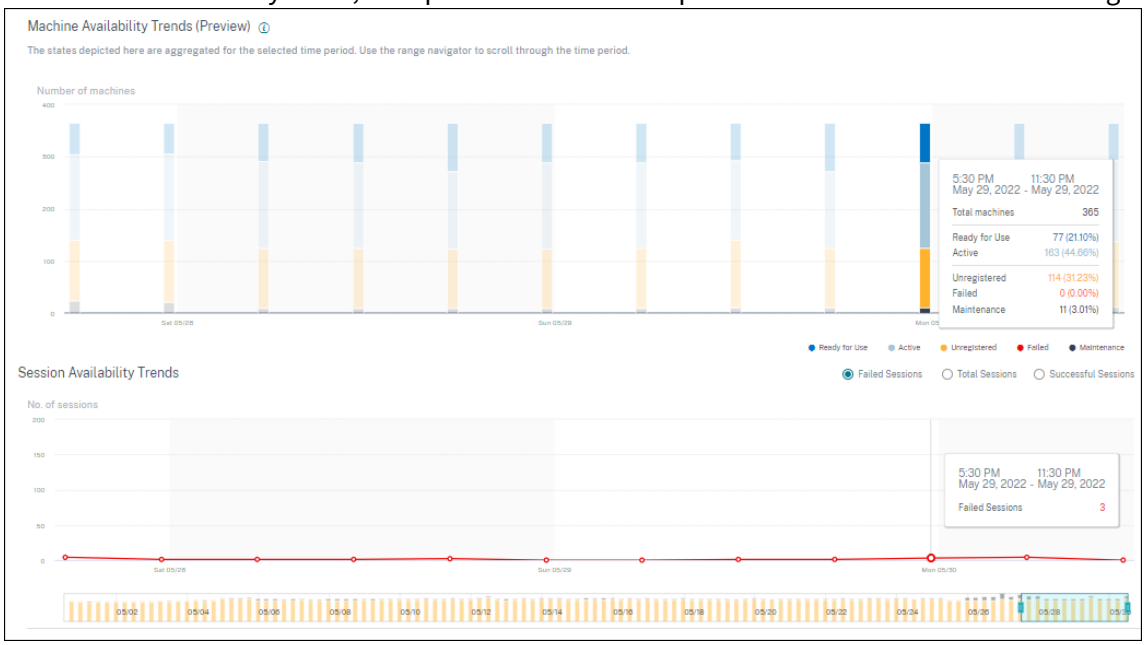
- The Infrastructure dashboard is now enhanced to show the **current availability** of virtual machines. This enhancement gives an overview of the number of machines currently serving users and the number of machines that are unavailable for various reasons. The machine counts in the last known Available machine states (Ready for Use, Active) and Unavailable machine states (Maintenance, Unregistered and Failed) is displayed for the last instance (15

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

minutes).



- Clicking the machine count opens the Machine Self-service view with the list of machines in the selected state for the last 15 minutes.
- The Machine Availability trend now plots machine counts in **aggregated states** for the selected period. The aggregated state is the least favorable state that the machine has been in, from among the Ready for Use, Active, Maintenance, Unregistered and Failed states. You can drill down from a specific section on the graph to view details of machines in a specific aggregated state on the Machine self-service view. The Machine Availability trend helps check the number of machines in an aggregated state at a point in time. When used alongside the Session Availability trend, it helps understand the impact of a resource crunch or an outage.



- Trends for one-month and one-week periods are now plotted with a 6-hour granularity. You can zoom into the one month Machine and Sessions Availability trends using the time navigator in

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

a 3–7 day range.

- The time navigator now reflects the Machine Availability trend. This helps identify time periods with a large number of unavailable machines, so you can easily navigate and zoom into the required period on the trend.
- The tool tips on Machines and Sessions Availability trends are synchronized to help understand the correlation between unavailable machines and failed sessions.
- The Machines Self-service view has a new facet called Aggregated State, to allow state-based filtering of machines. The view has the machine count displayed for the selected Aggregated States. You can now use the Aggregated State facet or click from the Availability trend, to see the list of machines that were in a specific aggregated state for the chosen time.
- New columns are added to the Machines self-service view - Last Known State, and the machine count in each of the selected Aggregated states.

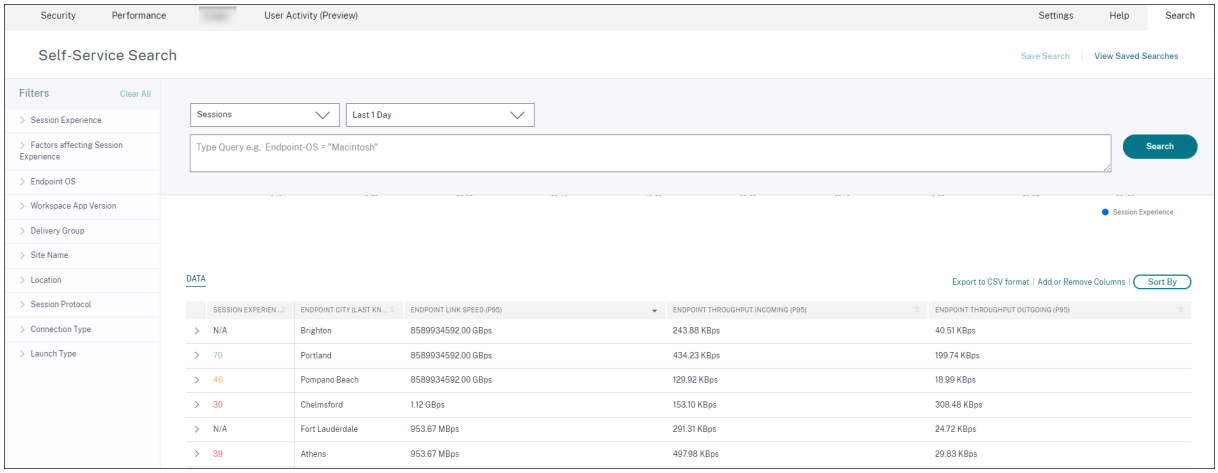
These enhancements help identify machines in a particular state currently or at a historical time period on the Machines Self-service view. They enable better troubleshooting of machines as they give higher granularity of data and help identify machines that need attention easily. For more information, see the Self-Service search for Machines and the Infrastructure Analytics articles.

Mar 08, 2022

Endpoint Network Statistics

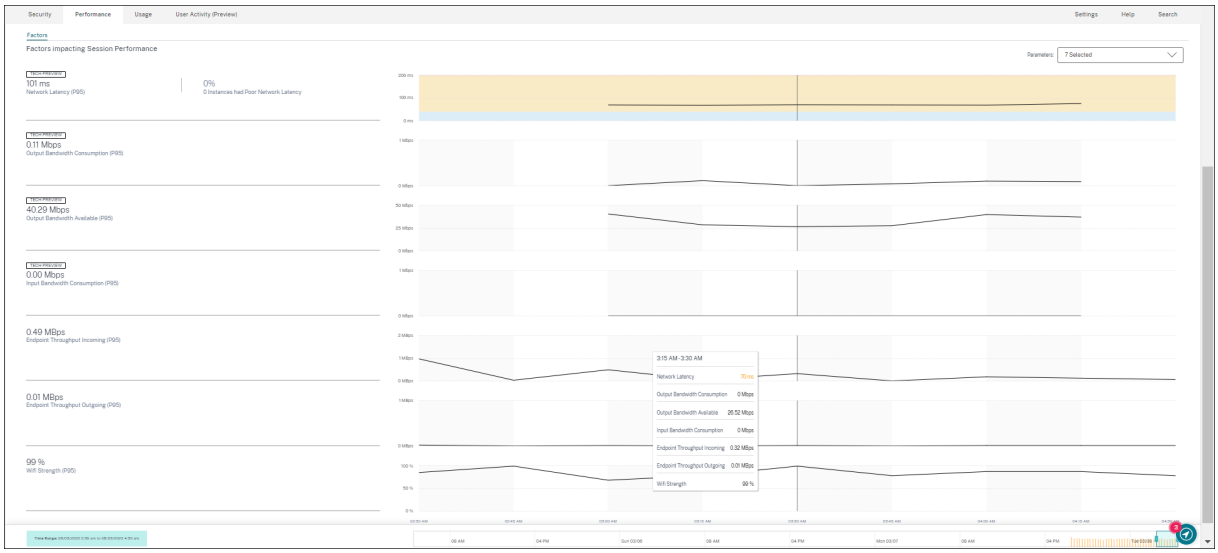
This feature provides more visibility into the client-side network, as several relevant metrics are added on the Sessions Self-service view and the Sessions Statistics view.

Endpoint Link Speed (P95), Endpoint Throughput Incoming (P95), Endpoint Throughput Outgoing (P95) are introduced as optional columns on the Sessions Self-service view.



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

The Session Statistics page now displays the **P95 values of WiFi Signal Strength, Endpoint Throughput Incoming, and Endpoint Throughput Outgoing** in the **Factors** tab. Graphs of these metrics are plotted through the session duration.



You need endpoints running Citrix Workspace app for Windows version 7 2108 or later to view Endpoint Network metrics.

These metrics along with existing values of Network Interface Type, ISP, Bandwidth, Network Latency, Gateway, Connector, and Connector performance statistics help better triage the root cause of poor session experience.

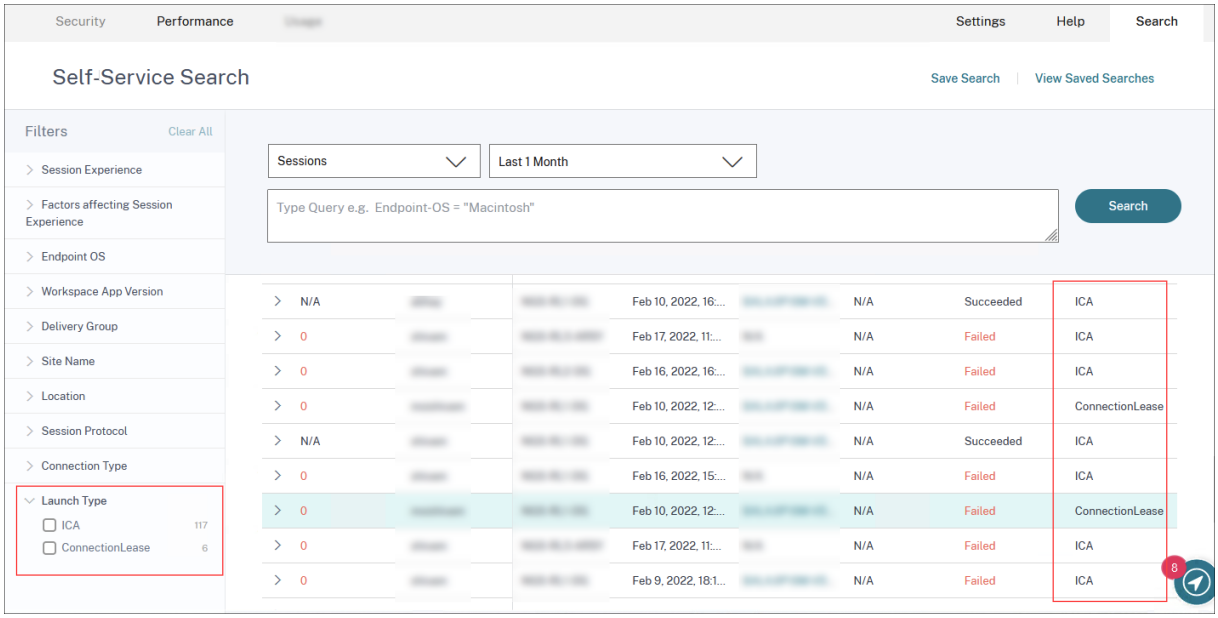
For more information, see the Self-Service search and the Session Details articles.

Mar 07, 2022

Visibility into Connection leased sessions

This feature provides visibility into sessions that were launched via a Connection lease. During Cloud service outages, Citrix DaaS™ supports sessions to be launched via a Connection lease to maintain service continuity.
Connection leased sessions are displayed under the **Not Categorized** classification on the **User Experience** Dashboard. ICA® RTT and logon duration metrics are not available for Connection leased sessions.

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



You can see the classification of sessions as ICA based or Connection leased using the Launch Type facet on the Sessions Self-service view.
The optional column, Launch Type on the Session Self-service table shows if sessions are ICA based or Connection leased.
This feature helps find the number of sessions that were launched via Connection Lease. You can use the failure reason to troubleshoot Connection leased sessions that have failed to launch.

Feb 21, 2022

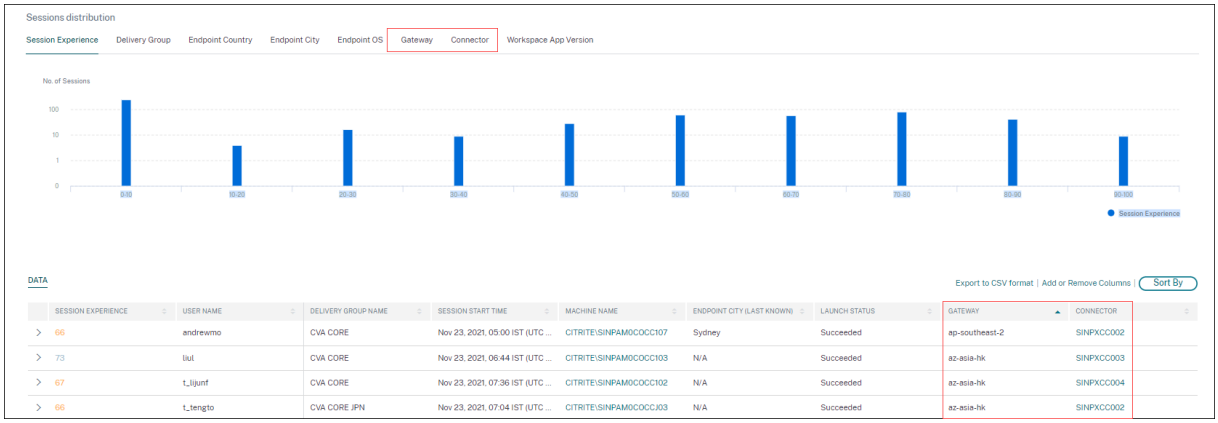
Connector and Gateway PoP Statistics

Citrix Analytics for Performance now has the **Connector and the Gateway Points of Presence (PoPs)** names displayed on the Session Self-service view as optional columns for all launched sessions.

This data helps identify Connectors and Gateway PoPs through which sessions are routed. This information helps check if sessions with poor responsiveness are routed through specific Connectors or Gateway PoPs. Based on the user location, you can further identify if the user session was routed through the right Gateway PoP for optimal performance. If the session has been routed through a Gateway PoP farther away from the location, you can check the DNS configuration.

The pivots for Connector and Gateway PoP on the Visual summary help triage poor sessions that might all be routed through a single Gateway PoP or Connector.

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



The value of the **Connector** might be N/A for any of the following reasons:

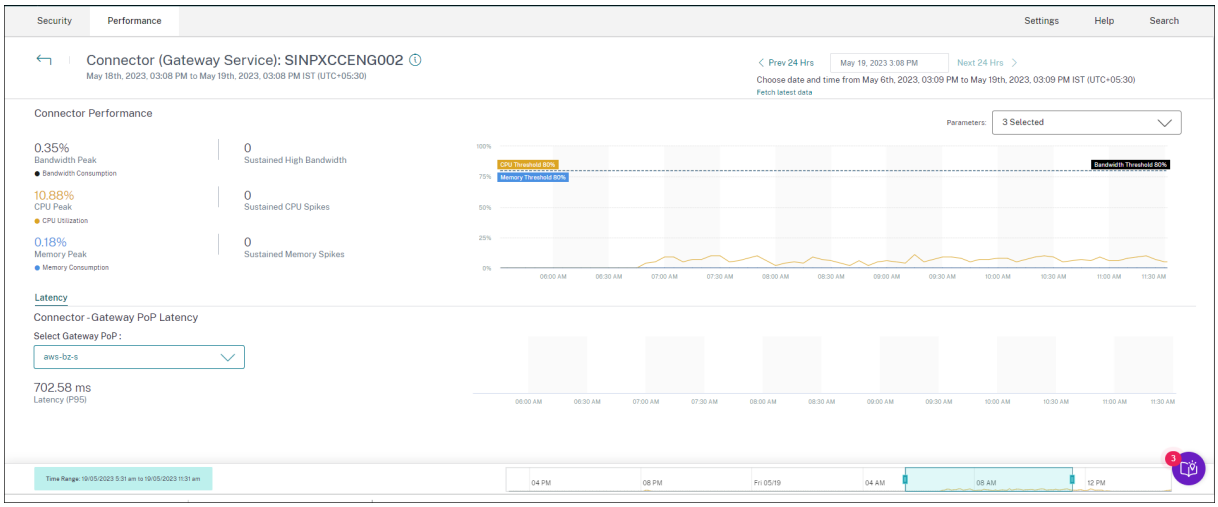
- There was a delay in receiving Connector events.
- Cloud Connector version is earlier than 16.0.0.7.

Also, ensure that the data processing via your Cloud Connectors is on. To do this, you can check the **Data processing on** state on the Cloud Connectors tile from the **Performance** tab in **Citrix Analytics** > **Data Sources**.

For more information, see the **Connector and Gateway** column descriptions in the Self-Service search article.

Connector Statistics View

A comprehensive view of the performance metrics of connectors is now available in Citrix Analytics for Performance. Clicking the connector name leads to the **Connector Statistics view**.



Connector Statistics view provides a summary of the connector performance in terms of its resources - bandwidth, CPU, and memory consumed for a selected connector in the last 24 hours. The peak

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

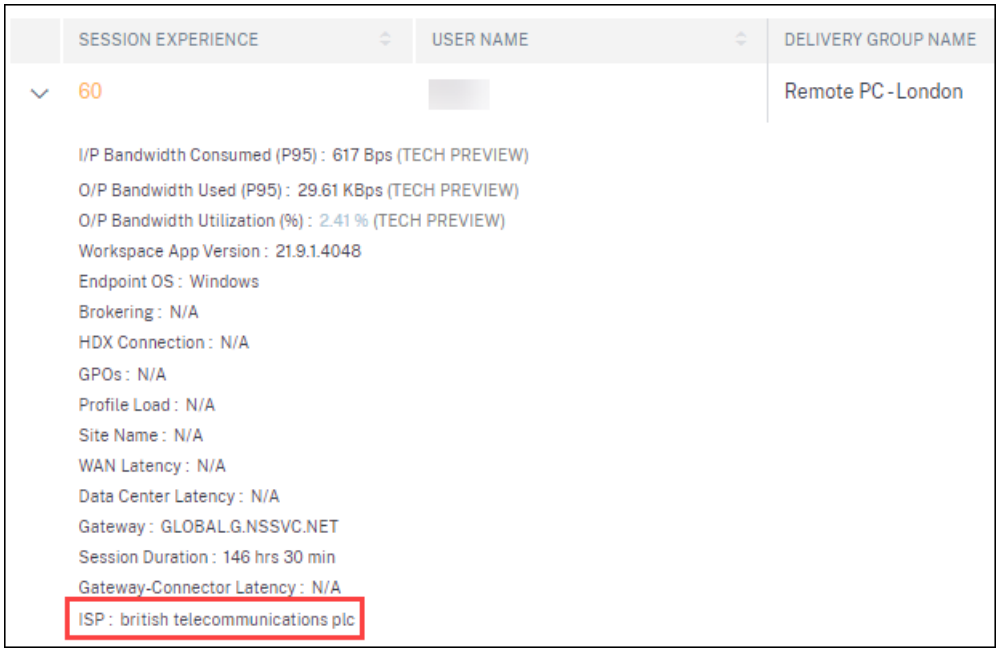
percentages of each metric consumed in the connector along with the number of instances when the metric crossed the threshold value is displayed. The graph plots this data over the 24 hour period available at a 15-minute granularity.

Resource consumption on the connector affects session launches and end user experience. This feature helps admins root cause issues of session failures and poor latency due to high resource consumption on the connector. For more information, see the Connector Statistics article.

Dec 20, 2021

Client Side statistics: Internet Service Provider (ISP)

The name of the ISP serving the endpoints is available on the Sessions self-service view when you expand a session row.



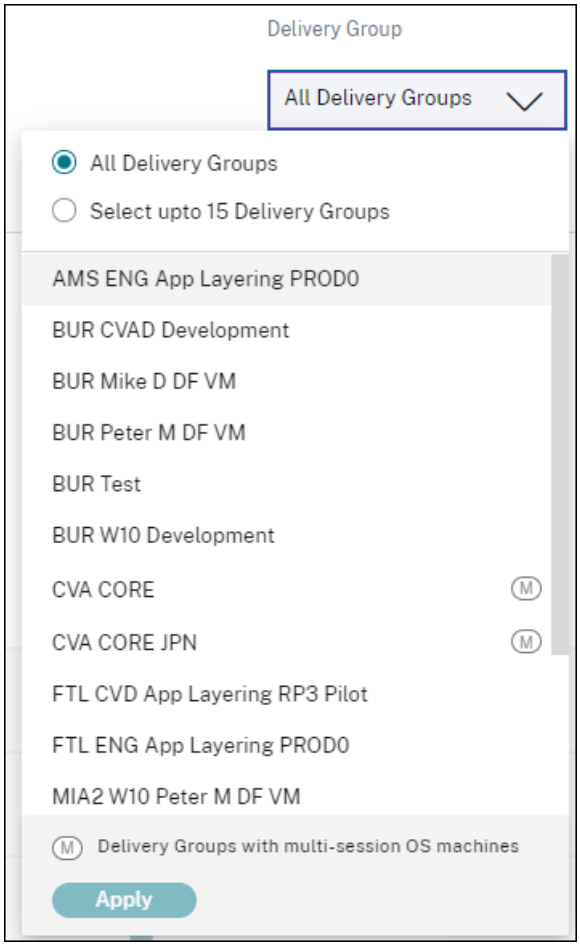
This feature helps you identify session performance issues that might be related to a specific ISP. This information is available with Citrix Workspace app for Windows versions 1912 and later. For more details regarding the availability of this feature with Citrix Workspace app for other OS, see the Workspace app matrix. For more information regarding the metrics available on the Session Self-service view, see the Sessions self-service article.

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

Dec 17, 2021

Delivery Group-Based Filtering

Citrix Analytics for Performance now has Delivery Group-based filtering in addition to the existing Site and Time period-based filters. Delivery group-based filtering enables you to view performance data belonging to the selected Delivery Groups. This filter helps focus on a specific selected set of Delivery Groups and hence, aids to root cause poor session experience in sessions running on them.



The **Delivery Group** drop-down list is available on the User Experience Dashboard. Here, the **All Delivery Groups** option is selected by default. You can also choose the **Select up to 15 Delivery Groups** option. The Search bar is available to search for specific Delivery Group names from the list.

Once the filter is applied, data relevant to these Delivery Groups is analyzed and displayed on the dashboard. The selection is retained upon drilling down from the dashboard into the factors page and then the self-service views. All views and reports show data belonging to the selected delivery groups.

To make any updates to the Delivery Groups - like, addition, deletion, or rename - available in the drop-down list, refresh the page at least 15 minutes after the change.

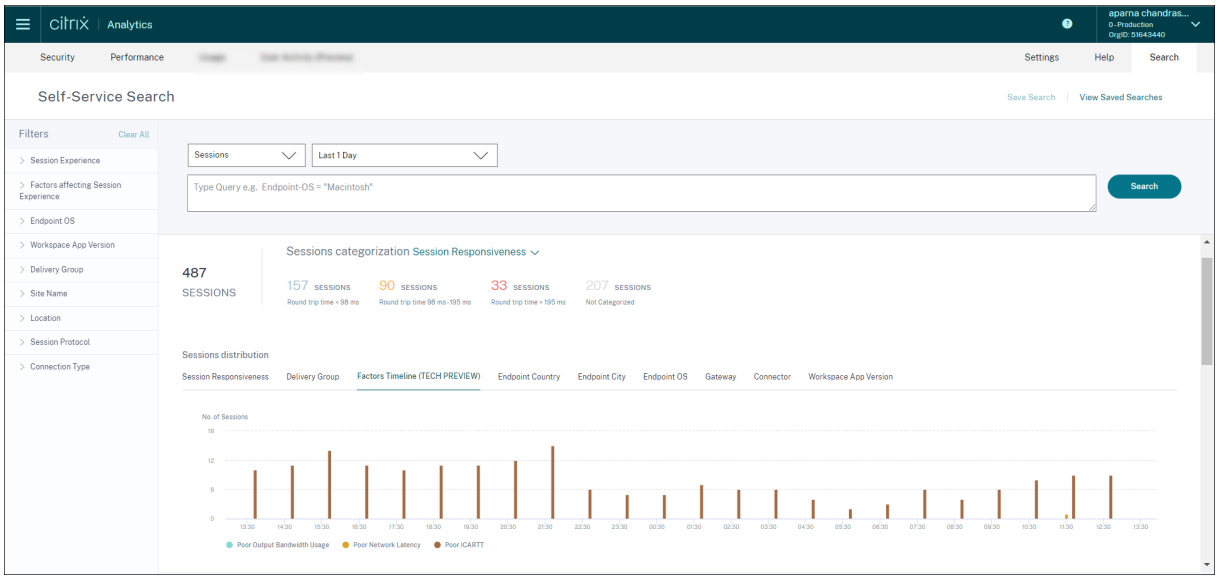
© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information about the usage of the User Experience Dashboard, see the User Experience Analytics article.

Bandwidth and Network Latency Metrics (Preview)

Granular bandwidth and latency-related metrics that compose Session Responsiveness of your Cloud environment are now available in Citrix Analytics for Performance.

The Factors Timeline pivot is added in the **Session Distribution** section of the Sessions self-service view under the **Session Responsiveness** category. This pivot helps analyze sessions based on Poor Output Bandwidth Usage, Poor Network Latency, and Poor ICARTT.

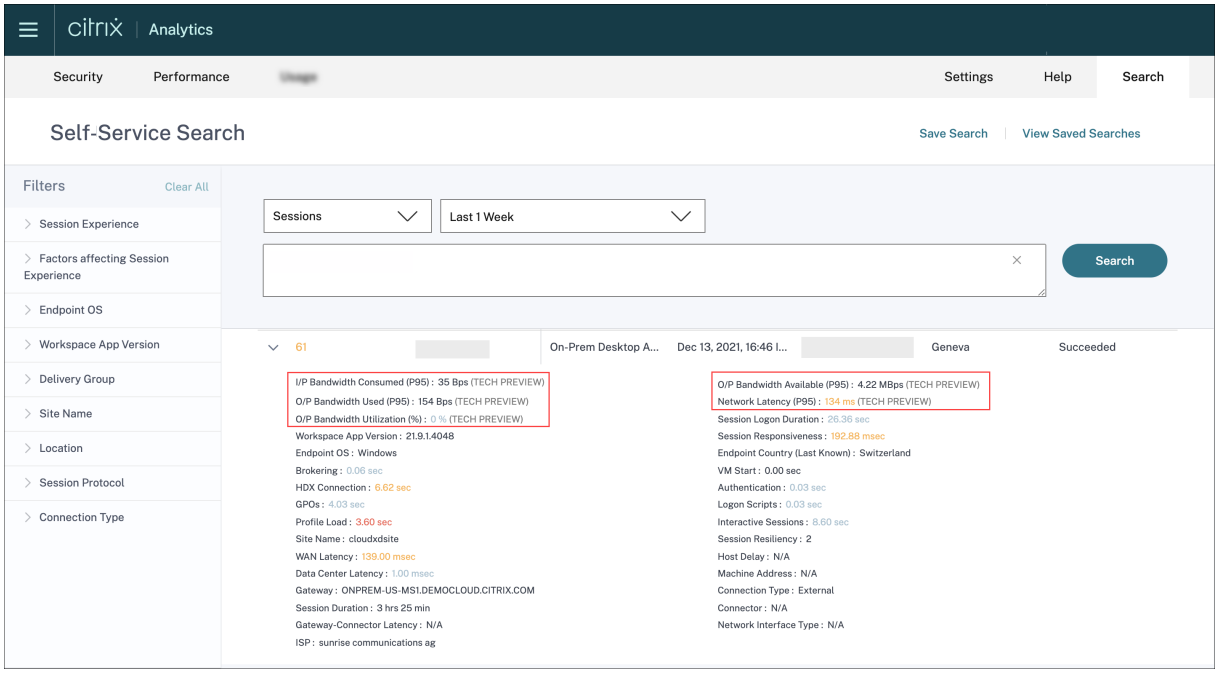


The following bandwidth and network latency metrics are available on the tabular view when you expand the selected session row on the Sessions self-service view.

- P95 values of the bandwidth metrics - Input Bandwidth Consumed, Output Bandwidth Available, Output Bandwidth Used,
- Percentage value of Output Bandwidth Utilization, and
- P95 value of the Network Latency

You need machines running Citrix Virtual Apps and Desktops 7 2112 or later. These metrics are available out-of-the-box for Citrix DaaS and do not require any specific configuration.

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



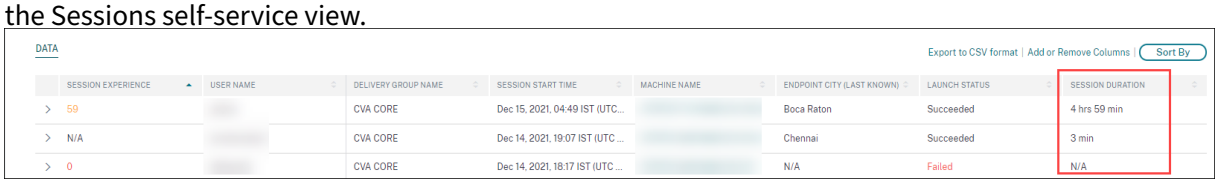
The Output Bandwidth Utilization and Network Latency metrics are color-coded based on whether they belong to the poor, fair, or excellent category.

The bandwidth and network latency metrics help analyze if a particular metric might be causing poor Session Responsiveness. The addition of these metrics helps Citrix Analytics for Performance serve as a single console of information to troubleshoot session performance issues.

For more information about the metrics available on the Sessions Self-service view, see the Sessions self-service article.

Session Duration in Sessions Self-Service View

Session Duration is now available on the Sessions self-service view. Use Add or Remove Columns to add Session Duration. The addition of this metric helps get a holistic view of the session metrics from the Sessions self-service view.

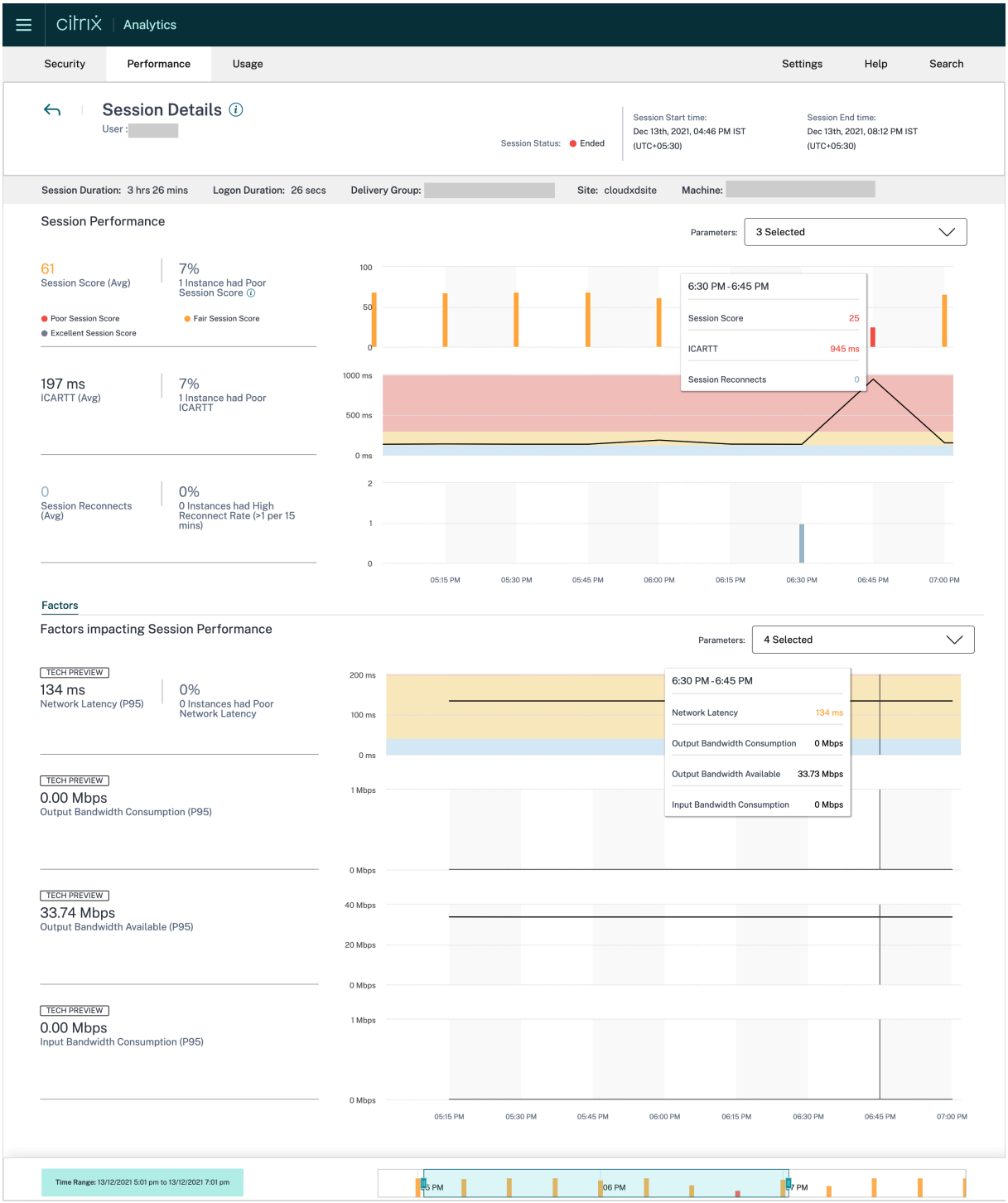


For more information about the metrics available on the Sessions Self-service view, see the Sessions self-service article.

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

Session Details

The Session Details page provides a holistic view of the session performance metrics. Comprehensive session details and factors affecting the session performance are displayed for the session duration.



This view gives visibility into session factors like ICARTT, Session Reconnects, bandwidth metrics, and network latency. These factors are plotted along with the Session Score for the selected period. The

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

Session Details view helps correlate the impact of available bandwidth and network latency on ICARTT and Session Score.

You need machines running Citrix Virtual Apps and Desktops 7 2112 or later to view the bandwidth and network latency metrics. For more information on the Session Details page see Session Details.

Dec 6, 2021

Automated onboarding for 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. The access does not require a request or manual onboarding by customers. 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. Once you log on to Citrix Cloud, select your tenant in the APS region of Citrix Cloud and 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.

For more information on accessing Performance Analytics see Access.

Nov 18, 2021

Overloaded Machines factor availability

The Overloaded Machines factor section is now available only for the 2 hours, 12 hours and 1 day ranges. The feature is disabled for 1 week and 1 month time periods for optimization. For more information, see Overloaded Machines.

Sep 13, 2021

Support for the Asia Pacific South region

Citrix Analytics for Performance now supports the Asia Pacific South (APS) region. For more information on the regions supported in Citrix Cloud, see Geographical considerations.

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

To access Performance Analytics from the APS region,

1. Choose the Asia Pacific South region while onboarding your tenant to Citrix Cloud.
2. Fill the Registration for Citrix Analytics for Performance in the APS Plane Podio form for a trial or a paid entitlement to Performance Analytics from your tenant in the APS region. You will be notified by mail upon successful allocation.
3. After you log on to Citrix Cloud, select your tenant in the APS region of Citrix Cloud and use the `https://analytics-aps.cloud.com` URL to access your Citrix Analytics Cloud Service.

For more information on accessing Performance Analytics see Access.

Aug 12, 2021

Client Side statistics: Network Interface Type

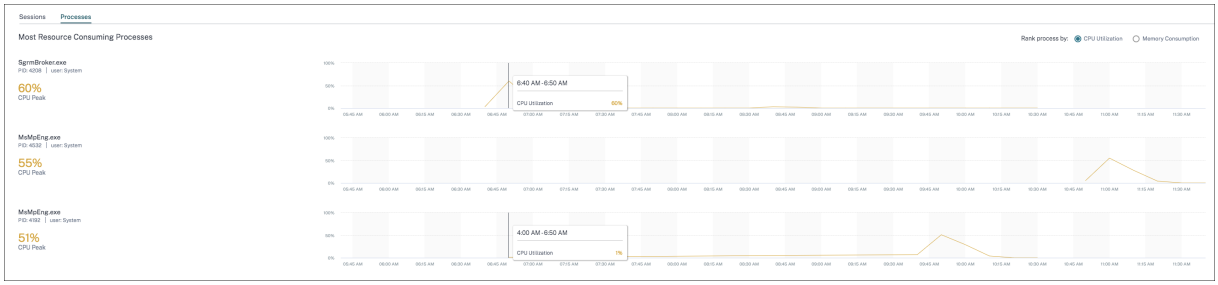
The **Network Interface Type** column is added to the tabular data on the Sessions self-service view. This field provides visibility into the client side network and helps root cause if poor session experience is due to issues at the endpoint device or the client side network. The value of this field is N/A for endpoints running Citrix Workspace app Windows version earlier than 2105. For more information, see the Self-service search for Sessions section.

July 29, 2021

Visibility into most resource consuming processes

Citrix Analytics for Performance provides visibility into processes contributing to high resource consumption. This is an important insight for admins to analyze the impact of these processes on user performance.
This feature is available for multi-session OS machines in the **Machine Statistics** page under the **Processes** tab. You can choose to view the processes ranked as per **CPU Utilization** or **Memory Consumption**. The three most resource consuming processes are displayed with percentage CPU or Memory Peak as selected. Charts plot CPU Utilization or Memory Consumption by the process across the selected time period. This feature requires that you enable the **Process Monitoring policy** from Citrix Studio.

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



For more information, see Process visibility.

June 10, 2021

Color coding on Session-based self-service view

Tabular data on the Session-based self-service view is color-coded to indicate the excellent, fair, or poor category the metrics belong to. This categorization is based on the individual threshold levels of the metrics. The thresholds are calculated dynamically. For more information, see [How are Dynamic Thresholds calculated?

Similar color coding is applied to the metrics available on expanding the rows in the Session-based self-service view.

Color coding visually aids in focusing on and identifying factors that are contributing to poor performance. It also gives an overview of the performance across various factors for the sessions that have been filtered to be seen in the current view.

Machine Actions and Composite Actions

Citrix Analytics for Performance provides actions you can perform on power managed machines in your Citrix DaaS Sites on Cloud. Admins with Full Administrator access can perform Machine Actions on identified machines. This capability helps simplify the task of admins having to monitor and take a sequence of actions on a machine with performance issues.
Machine Actions - start, restart, turn maintenance mode on or off, shut down the machine - are accessible from the Machines Analysis page of the respective machine. Also available are Composite Actions that combine more than one action to help admins bring affected machines back to availability with a single click.
This feature avoids admins shifting to other consoles, like the Web Studio or Citrix Director, to perform these actions. The feature is the key to close the loop when it comes to troubleshooting and solving issues related to machine performance.

For more information, see Machine Actions and Composite Actions.

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

May 12, 2021

Infrastructure Analytics Dashboard - Enhancements

In this release, Citrix Analytics for Performance provides an enhanced **Infrastructure Analytics Dashboard** to improve visibility into the overall availability of the machines. The new **Machine Availability** page displays the number of hours machines are available or unavailable across sites and Delivery Groups. Machine Availability displays information about machines that are **Available** and **Unavailable**. Available machines are further classified into **Ready for use** and **Active** states. Unavailable machines are classified into **Unregistered**, **Failed**, and **Maintenance** states. This information helps determine the availability of provisioned machines to serve sessions.

The Machine Availability trend shows the distribution of machines in various states across the selected time period. Also available is the sessions chart plotting the successful and failed sessions. This helps correlate unavailable machines with failed sessions.

The **Machine Performance** section provides information about the performance of Multi-session OS machines.

Additionally, you can use the custom time selection filter to zoom into the machine availability and machine performance for a specific duration within the selected time period.

For more information, see Infrastructure Analytics.

Apr 23, 2021

Failure Insights - Communication Error

In this release, Citrix Analytics for Performance provides insights into **Communication Error** as a part of **Failure Insights**.

The **Communication Error** sub-pane lists the number of session failures due to communication errors between the endpoint (where the user launches the session) and the machine. These errors can occur due to incorrect firewall configurations or other errors on the network path.

The two categories of communication errors are:

- Endpoint to machine —lists the sessions where communication errors have occurred between the endpoint and the machine.
- Gateway to machine —lists the sessions where communication errors have occurred between the gateway and the machine.

Additionally, the **Communication Error** sub-pane displays the following recommendations to resolve the errors.

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

- Check the firewall settings on the machine and gateway
- Check network connectivity between the machine and gateway

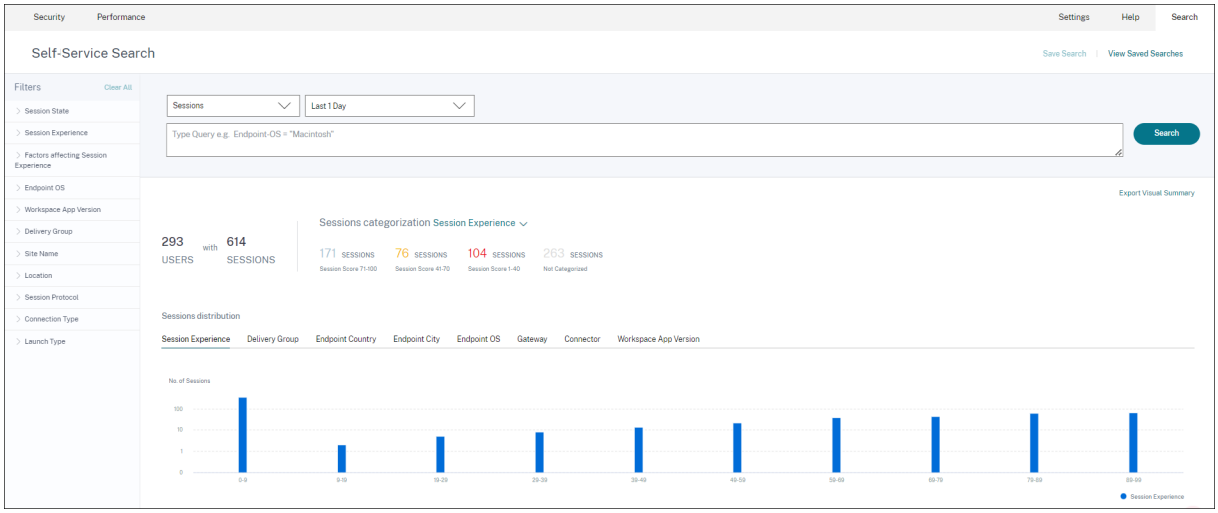
This feature is supported only on Citrix Workspace app 2103 and later.

For more information, see Communication Error.

Feb 2, 2021

Visual Summary io Sessions self-service view

Visual Summary of data is available on the Sessions self-service view. Visual Summary presents the raw data in the self-service tables as charts aimed at an improved visibility into the user experience.



The Visual Summary chart displays session categorization based on the chosen criteria. In addition, you can choose to view the session distribution pivoted on a specific parameter. This view helps identify session performance issues related to the pivots.

Use the visualization to identify patterns in data that can help troubleshoot specific issues.

For more information, see the Self-service search for Sessions section in the Self-service article.

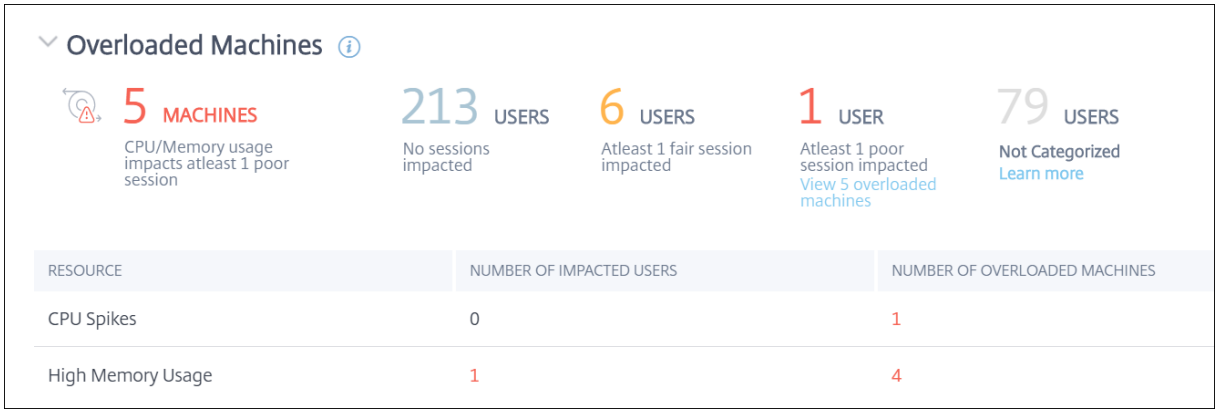
Jan 28, 2021

Overloaded Machines factor

Overloaded resources can cause high latency, high logon duration, and failures resulting in poor user experience. The **Overloaded Machines** factor, added on the User Experience (UX) factors page, gives visibility into the overloaded resources causing poor experience.

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

Machines that have experienced sustained CPU spikes, or high memory usage, or both, that have lasted for 5 minutes or more, resulting in a poor user experience in the selected duration are considered to be overloaded.



The **Overloaded Machines** section shows:

- The number of machines in which CPU or memory usage has impacted at least one poor session.
- The number of users affected due to the impact of overloaded CPU or memory on the session experience.
- Breakup of:
    - the number of machines affecting users with poor experience due to overloaded resources.
    - the number of users with poor experience impacted by CPU Spikes and High memory usage.

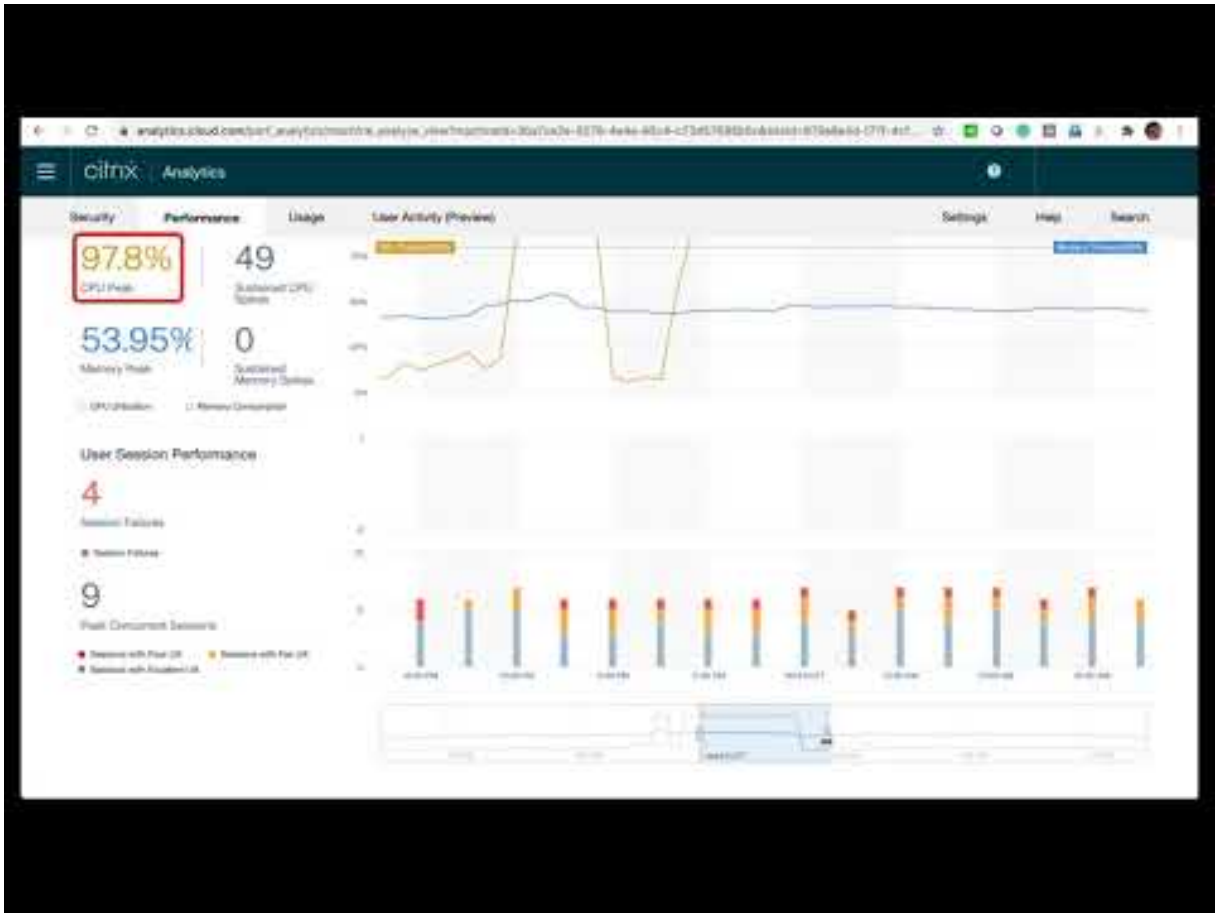
For more information, see the Overloaded Machines section in the User Experience Factors drilldown article.

- Clicking the number of overloaded users leads to the Users self-service view filtered to show users whose sessions are affected by the overloaded resources.
- Clicking the number of overloaded machines leads to the Machines self-service view filtered to show the chosen set of overloaded machines - based on classification, or based on the overloaded resource, CPU, or machine.

The Machines self-service view is enhanced with the Overloaded Machines and Overloaded CPU/Memory facets to help filter machines with overloaded resources. For more information, see Overloaded Machines in the Self-Service Search for Performance article.

This video shows a typical troubleshooting scenario using the Overloaded Machines factor.

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



Dec 16, 2020

User Experience Dashboard: Session count enhancements

A session breakup panel based on protocol is added to the User Experience dashboard. The breakup brings clarity into the total number of sessions launched on the Site versus the number of sessions analyzed in Performance Analytics.

The panel displays the following for the selected duration:

- the total number of unique users in the selected Sites,
- the total number sessions that have been active,
- individual HDX, Console, and RDP sessions.

Analytics relevant only to HDX sessions are available on the dashboard. For more information about the various sections on the dashboard, see the User Analytics article.

Performance metrics of all the sessions independent of protocol are available on the Users, and Sessions based self-service views. Use the Protocol facet to filter the results based on the session protocol.

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

For more information, see the Self-Service Search for Performance article.

User Experience Dashboard: Session classification clarity

Not Categorized users and sessions are displayed as a separate session category on the User Experience dashboard. This category in the User Experience Score, Session Responsiveness, and Session Logon Duration sections helps identify users and sessions that cannot be classified as experiencing excellent, fair, or poor performance. A session might not get classified if it is launched from a machine running an older Workspace app version, or if the session fails during the logon. For more information on specific reasons for **Not Categorized** sessions in individual sections on the dashboard, see,

- Users Not Categorized
- Sessions Not Categorized for Responsiveness
- Sessions Not Categorized for Logon Duration

Connection information

Connection failures are generally an important cause for performance degradation. Connection-related parameters are now available on the Self-service view for Sessions to help identify and troubleshoot connection failures easily.
The Self-Service view for Sessions includes **Connection Type** facet and column. Connection Type has values:

- **internal** –if the connection is direct without Gateway
- **external** –if the connection is through a Gateway

In addition, **Gateway FQDN** (for external connections) and **Machine Address** (for internal connections) are available as columns on the Self-service view for Sessions.

The Connection details are available for Endpoints running Citrix Workspace app version 20.12.0 or later for Windows. For all other endpoints, the Connection type is displayed as N/A.

For more information, see the Self-service search for Sessions article.

Endpoint Information enhancements

Endpoint parameters are added to the columns on the Users and Sessions based self-service views, in addition to the existing endpoint facets. This feature helps search users and sessions based on the endpoint parameters like the location, OS, and the Workspace app version. The parameters are also available in exported CSV files.
In addition, the location algorithm has been enhanced to return the last known location in cases where the latest location of the endpoint is not resolved.

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

- The Users and Sessions self-service view contains the location parameters Endpoint Country (last known), and Endpoint City (last known).
- The Sessions self-service view contains the location parameters Endpoint Country (last known), and Endpoint City (last known), Workspace app version, and Endpoint OS.

The addition of these columns helps define queries using the endpoint parameters. You can easily identify issues with performance that are endpoint specific like the location, Workspace app version, or OS.

For more information, see the Self-Service Search for Performance article.

Dec 15, 2020

Drilldown into Profile Load Insights

Profile load insights are updated with a drilldown to help identify users who have a poor logon experience due to large profile sizes.



The **View the correlation** link displays the average profile size of users, calculated using profile sizes of users who have had excellent and fair profile load experience. Users having profile sizes larger than the average are likely to have poor profile load times.

The **View analysis** link displays users whose profile size is larger than the average on the users based self-service view. Use facets to further filter this data to view users with both large profile size and poor logon duration experience.

The self-service views for both users and sessions include the **Profile Load** and the **Average Profile Size** fields. These fields help filter and identify users with large profile load times easily.

For more information, see the Profile load insights section in the User Experience (UX) Factors article.

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

Dec 11, 2020

Identification of user terminated sessions

Session failures are an important factor affecting user experience in most environments. Hence, its accuracy plays an important role in correctly measuring the overall user experience in the environment.

Identification of user-terminated sessions is a step forward in this direction. It identifies sessions voluntarily terminated by users separately from failed sessions. The **Launch Status** field on the Sessions self-service view shows a **`User Terminated`** status, apart from the existing `Succeeded`, and `Failed` statuses. Addition of the separate `User Terminated` status increases the accuracy of the session failure count.

This feature is supported with endpoints running:

- Citrix Workspace app 20.9.0 or later for Android
- Citrix Workspace app 20.8.0 or later for iOS
- Citrix Workspace app 20.8.0 or later for Windows

This feature does not support endpoints running Workspace on the web.

For more information, see Self-Service search for Sessions.

Oct 19, 2020

Machines based self-service search

A **Machines based self-service search** is now added to the existing Users and Sessions based self-service views in Citrix Analytics for Performance.

The machines based self-service view displays key performance indicators of your virtual machines. The metrics include the machine downtime, the latest consecutive failures, performance indicators of the machine resources (CPU and memory) - the peak usage, and the number of peaks for the selected time period. Overloaded resources can cause session failures, high latency, or high logon duration resulting in poor user experience. This view helps easily troubleshoot the performance issues related to machine resource utilization.

You can access the Machines based self-service view from the **Search** menu in your Citrix Analytics service. In the list of services on the **Search** tab, under the **Performance** section, select **Machines**. The Machines based self-service view is also available when you drill down from black hole machines. To access the view, on the User experience dashboard, in the **Failure Insights** section, click the **Black hole machines** number.

For more information on the Machines based self-service view, see Self-service search for Machines.

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

Machine Statistics view

Citrix Analytics for Performance provides a **Machine Statistics** view. This view displays a correlation between the resource load and the session experience on the selected machine for the selected time period. This information helps you understand if high CPU or memory usage is related to session failures. You can then explain a poor experience in your Apps and Desktops environment.

To access the Machine statistics page, on the **Machines self-service view**, click the machine name link.

Key data points available on this page are:

- Relevant machine attributes, such as the OS, Site, Delivery Group, and downtime of the machine during the last 24 hours.
- Machine performance statistics related to resource usage, such as CPU and memory peaks, and the number of spikes over the last 24 hours. Also displayed is a trend of the CPU and memory consumption.
- Session performance statistics, such as the number of session failures, and peak concurrent session count over the last 24 hours. Also displayed are trends of session failures and session classification.

You can choose to view machine statistics for any 24-hour duration from the last 14 days. The charts are displayed for a default 4-hour time period. A time navigator helps change this time period and also zoom into any duration within the chosen 24-hour time period.

The machine and session performance statistics displayed on the same view help analyze machine resources, their usage pattern and understand if the machine resources have been a possible bottleneck for poor performance.

For more information about this feature, see the Machine Statistics article.

Failure Insights - Black hole machines

Failure Insights in Citrix Analytics for Performance provides insights into session failures that occurred during the chosen time period. This feature is important in helping troubleshoot and resolve session failures faster. It eases the task of admins who need to troubleshoot session failures to improve session availability and hence, the user experience.
In this release, Citrix Analytics for Performance provides insights into **Black hole machines** as a part of Failure Insights.

Some machines in your environment, though registered and appearing healthy might not service sessions brokered to the them, resulting in failures. Machines that have failed to service four or more consecutive session requests are termed as **Black hole machines**. The reasons for these failures are

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

related to various factors that might affect the machine, such as, insufficient RDS licenses, intermittent networking issues, or instantaneous load on the machine.

The **Black hole machines** section of Failure Insights shows the number of black hole machines identified in your environment during the selected time period. The presence of black hole machines in the environment impacts session availability. Suggestions to reduce the number of black hole machines in your environment are provided. Clicking the number of black hole machines opens the Machines based self-service view that is filtered to show the black hole machines in your environment during the selected time period.
For more information, see Black hole machines.

July 21, 2020

GPO Insights

GPO Insights displays client-side extensions (CSEs) taking the longest processing time during the selected time period. **GPO Insights** are available in the Session Logon Duration subfactor table. Click the **Possible Reasons** link in the **GPOs** row, **Insights** column.

GPO Insights are based on the analysis of user sessions having high GPO execution times. Increased GPO execution times are due to CSEs with long processing time. Optimizing CSE processing improves the overall session logon experience of the user. Average CSE execution time depends on the number and type of policies applied with it. Review and tune policies associated with CSEs taking the longest processing time as indicated in the GPO insights. Further, consider deleting the ones that are not required. For more pointers to improve the processing time of CSEs, see GPOs.

June 16, 2020

Improved User Experience Score algorithm

The User Experience score calculation algorithm has been improved. The method for quantifying the experience based on the factors - Session Availability, Session Logon Duration, Session Responsiveness, and Session Resiliency has been optimized. Now, more emphasis is laid on the in-session experience factors.

This update results in a more appropriate classification of users having an excellent, a fair, or a poor experience. You might notice more users being classified as having a fair or a poor experience now. The improved score algorithm enables you to correctly identify poor sessions and resolve issues to improve the user experience. Starting June 2020, the new user classification data appears on your User Experience trend. This change does not affect any classification done earlier.

For more information on the User Experience Score calculation, see the User Experience article.

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

April 23, 2020

Location and Endpoint based Self-Service Search

Now, you can search events based on the Endpoint Country or City on the self-service view for User and Session performance data. The self-service view for Session performance data also has filters based on the Session Endpoint OS and Endpoint Version.

This information helps analyze if performance issues are localized to a specific geography, endpoint OS, or version. These filters are available for the Citrix Workspace app for Windows version 1912 and later.

For more information about the usage of these filters in self-service search, see Self-Service Search for Performance.

January 10, 2020

Citrix Analytics for Performance - Generally Available

The Citrix Analytics for Performance is a new subscription-based offering from Citrix Analytics. It allows you to track, aggregate, and visualize key performance indicators of your Apps and Desktops environment. You can use it to analyze performance issues of Apps and Desktops Sites both on-premises and on Cloud. For more information, see Performance Analytics.

Known Issues

September 1, 2025

Known issues specific to the Citrix Analytics service platform are listed in the Citrix Analytics service Known Issues article.

Performance analytics has the following known issue.

Onboarding on-premises Citrix Virtual Apps and Desktops version 2109 to Citrix Analytics for Performance™ from Citrix Director might fail.
Workaround: Upgrade Citrix Virtual Apps and Desktops™ to version 2112 and onboard to Citrix Analytics for Performance. [DIR-16070]

Data from on-premises Citrix Gateway that was onboarded to Citrix Analytics for Performance prior to 14th September 2022, might not be processed accurately. As a workaround, enable or onboard the on-premises Citrix Gateway data source again. Follow the On-premises Citrix Gateway onboarding guide [WSA-13616].

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

Data Sources

September 11, 2025

The data sources described here are cloud services and on-premises products that send data to Citrix Analytics for Performance.
You can use Performance Analytics to monitor on-premises and 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.

Supported data sources

The following table lists the Citrix data sources that Citrix Analytics for Performance supports.

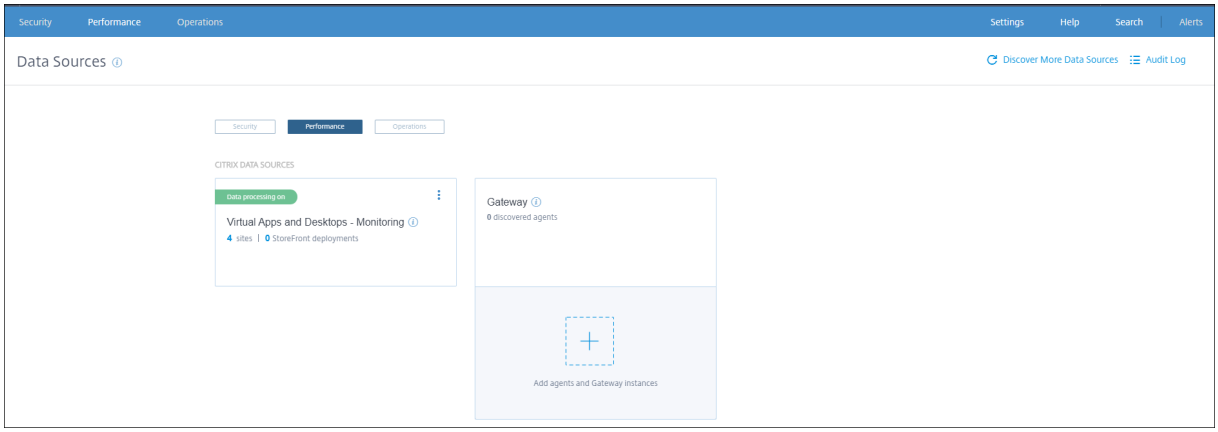
Data Source	Required Service Subscriptions	Product Component and version	Onboarding	Value-add
Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)	Citrix Cloud license, Citrix DaaS subscription	See Citrix Workspace app version matrix	Automatically detected. Ensure accessibility to URLs from all endpoints as described in Network Requirements	Performance analytics features
		End User Experience Monitoring (EUEM) service installed and running		Session Responsiveness, UX Score
		Citrix Profile Management installed and running		Logon Duration, UX Score

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

Data Source	Required Service Subscriptions	Product Component and version	Onboarding	Value-add
Citrix Virtual Apps and Desktops on-premises	Citrix Workspace service, Citrix Virtual Apps and Desktops	See Citrix Workspace app version matrix and Citrix VDA/Machine version matrix	Onboard from Director through a 3-step process	Performance analytics features
		End User Experience Monitoring (EUEM) service installed and running.		Session Responsiveness, UX Score
		Citrix Profile Management installed and running		Logon Duration, UX Score
		StoreFront 1906 and later (for StoreFront users) Citrix Workspace is automatically discovered and does not require onboarding.	Onboard Virtual Apps and Desktops sites using StoreFront	Endpoint Location, Failure Insights: Communication error, Failed Sessions: Endpoint OS, Workspace app Version, User Terminated Launch status
Citrix Gateway On-premises	Application Delivery Management agent	Citrix Gateway 12.1.x.x and later	Gateway data source	Session Responsiveness (Latency) breakdown
Cloud Connector			Automatically detected	Connector statistics

You can check the status of Cloud data sources relevant to Performance Analytics from **Citrix Analytics service > Settings > Data Sources > Performance**.

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



Citrix Workspace™ app version matrix

The following table lists the minimum required Citrix Workspace app version for Citrix Analytics for Performance features. Ensure accessibility to the `https://*.cloud.com/` and `https://*.windows.net/` URLs from all endpoints (or proxies, if they are configured)

Feature	UI Parameter	Windows	Linux	Android	iOS	Mac	HTML5
User Experience Score	User Experience Dashboard	1906	2104	2010.5	21.9	21.6.0	21.1

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

Feature	UI Parameter	Windows	Linux	Android	iOS	Mac	HTML5
Endpoint Location, ISP (ensure that the URL `https://locus.analytics.cloud.com/api/locateip` is accessible to the endpoints)	Sessions self-service view > Endpoint City, Endpoint Country	1912	2104	20.3.0	20.4.0	20.05.06	2004
Network Metrics	Sessions self-service view > Network Interface Type	2105, 2311 (Hybrid Launch)	2311 (Hybrid Launch)	Not supported	Not supported	Not supported	Not supported
Gateway information	Sessions self-service view > Connection Type, Machine FQDN, Gateway Address	2012	Not supported	Not supported	Not supported	Not supported	Not supported

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

Feature	UI Parameter	Windows	Linux	Android	iOS	Mac	HTML5
Session Launch Status	Sessions self-service view > Launch Status	2008	2101	20.9.0	20.8.0	2101	Not supported
Communication Error Insights	UX Dashboard > Failure Insights > Communication Errors	2103	Not supported	Not supported	Not supported	Not supported	Not supported

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

Feature	UI Parameter	Windows	Linux	Android	iOS	Mac	HTML5
Endpoint Network Statistics	Sessions self-service view > Endpoint Link Speed (P95), Endpoint Throughput Incoming (P95), Endpoint Throughput Outgoing (P95) and Sessions Details page > WiFi Signal Strength, Endpoint Throughput Incoming and Endpoint Throughput Outgoing	2108 (Native launch), 2311 (Hybrid Launch)	2308 (Native launch), 2311 (Hybrid Launch)	Not supported	Not supported	Mac 2409	Not supported

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

Citrix VDA version matrix

The following table lists the minimum required Citrix Virtual Apps and Desktops™ to be running on the machines for certain Citrix Analytics for Performance features.

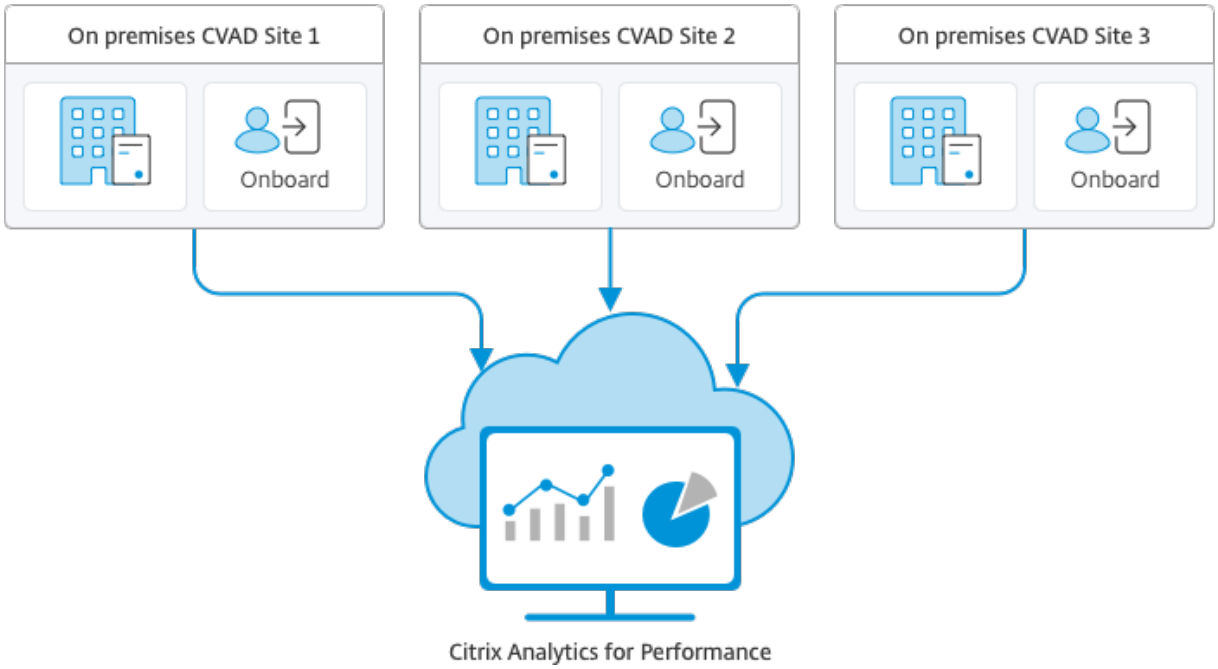
Feature	UI Parameter	Citrix VDA version
Citrix Analytics for Performance	—	Citrix Virtual Apps and Desktops 7.15 LTSR
Bandwidth and Network Latency Metrics	Bandwidth and Network Latency metrics in the Sessions self-service and Session Details views	Citrix Virtual Apps and Desktops 7 2112
Process Data in Machine Statistics	List of top resource consuming processes in Machine Statistics > Process tab	Citrix Virtual Apps and Desktops 7 2203 LTSR

Configuring on-premises Citrix Virtual Apps and Desktops Sites with Citrix Analytics for Performance™

September 1, 2025

You can send performance data from your on-premises Citrix Virtual Apps and Desktops site to Citrix Analytics for Performance on Citrix Cloud to leverage its advanced performance analytics capabilities. To view and use Performance Analytics, you must first configure your on-premises sites with Citrix Analytics for Performance from your on-premises monitoring tool, Citrix Director.

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



Performance Analytics accesses data in a secure manner and no data is transferred from Citrix Cloud™ to the on-premises environment.

Prerequisites

To configure Citrix Analytics for Performance from Director, no new components need to be installed. Ensure that the following requirements are met:

- Your Delivery Controller and Director are on version 1912 CU2 or later. For more information, see Feature compatibility matrix.

> **Note:**
>
> - Configuring your on-premises site with Citrix Analytics for Performance from Director might fail if the Delivery Controller is running a Microsoft .NET Framework version earlier than 4.8. As a workaround, upgrade the .NET Framework in your Delivery Controller to version 4.8. LCM-9255
> - When you configure your on-premises site running Citrix Virtual Apps and Desktops version 2012 with Citrix Analytics for Performance from Director, the configuration might fail after a couple of hours or after a restart of the Citrix Monitor Service in the Delivery Controller. The Analytics tab displays a Not Connected status in this case. As a workaround, create an Encryption folder in the registry on the Delivery Controller, Location: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor Folder Name: Encryption Ensure that the CitrixMonitor account has Full Control Access on the Encryption

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

> folder. Restart the Citrix Monitor Service.DIR-14324

- Access to the **Analytics** tab to perform this configuration is available for full administrators only.
- For Performance Analytics to access performance metrics, outbound internet access is available on all Delivery Controllers and the machines on which Director is installed. Specifically, ensure accessibility to the URLs as described in Network Requirements.

In case, Delivery Controllers and Director machines are within an intranet and outbound internet access is via a proxy server, ensure the following:

- The proxy server must allow the preceding list of URLs.
- Add the following configuration in the Director web.config and citrix.monitor.exe.config files. Ensure that you add this configuration within the **configuration** tags:

```
<system.net>
    <defaultProxy>
        <proxy  usesystemdefault = "false"  proxyaddress = "http
            ://<your_proxyserver_address>:80" bypassonlocal = "
            true"  />
    </defaultProxy>
</system.net>
```

  - The Director web.config is located at `C:\inetpub\wwwroot\Director\web.config` on the machine where director is installed.
  - The citrix.monitor.exe.config is located at `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` on the machine where the Delivery Controller is installed.

  This setting is provided by Microsoft on IIS. For more information, see `https://docs.microsoft.com/en-us/dotnet/framework/network-programming/proxy-configuration`.

  The **defaultproxy** field in the config file controls the outbound access of Director and Monitor Service. Configuration and communication with Performance Analytics requires the **defaultproxy** field to be set to **true**. It is possible that the policies in effect set this field to false. In this case, you must manually set the field to true. Take a backup of the config files before you make the changes. Restart the Monitoring service on the Delivery Controller™ for the changes to be affected.

  > **Note:**
  >
  > If you upgrade to a newer version of Citrix Virtual Apps and Desktops site, ensure that the proxy in the `citrix.monitor.exe.config` file of the Delivery Controllers is reconfigured.

- Ensure accessibility to the following URLs from all endpoints (or proxies, if they are configured):

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

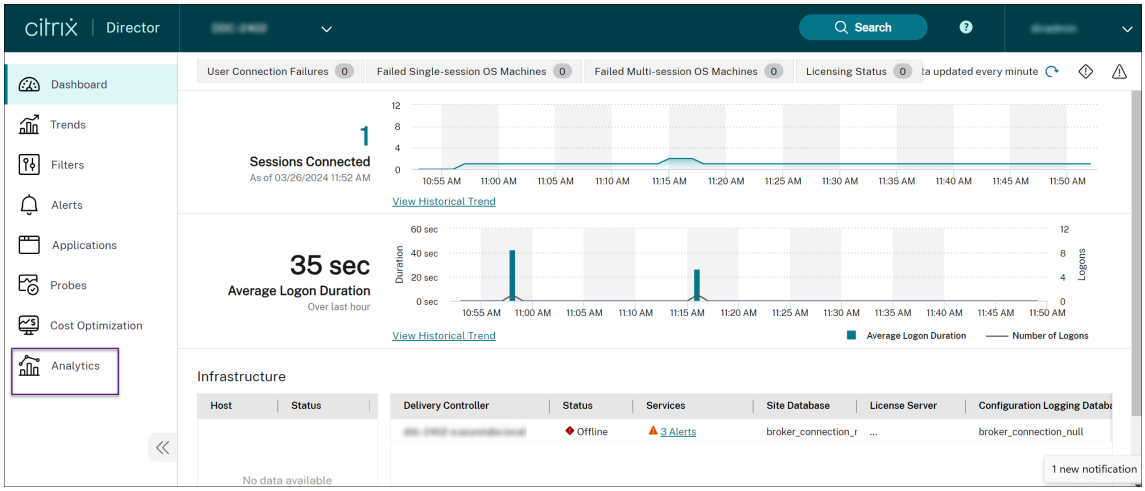
  - Citrix Analytics: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/`

- You have an active Citrix Cloud entitlement for Citrix Analytics for Performance.
- Your Citrix Cloud account is an Administrator account with rights to the Product Registration Experience. For more information about administrator permissions, see Modify Administrator Permissions.

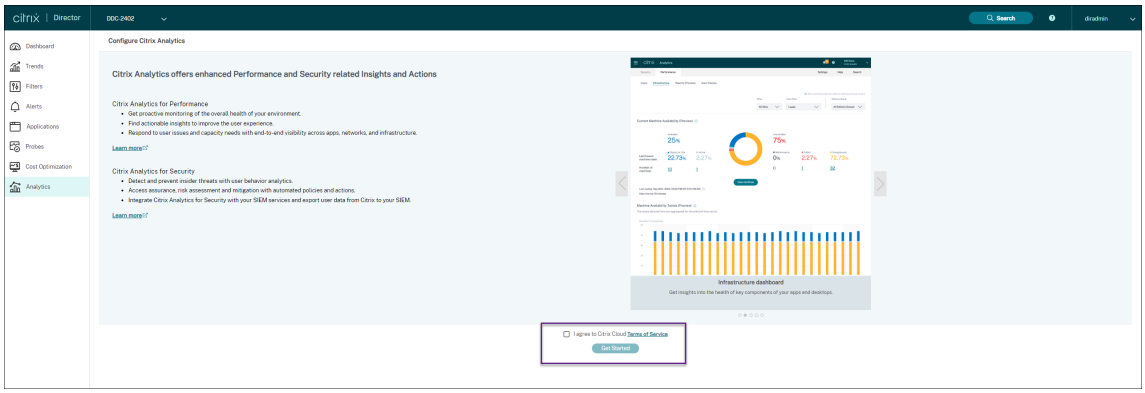
Configuration steps

After you have verified the prerequisites, do the following:

1. Sign in to Director as a full administrator and select the site which you want to configure with Performance Analytics. The Director Dashboard page appears.

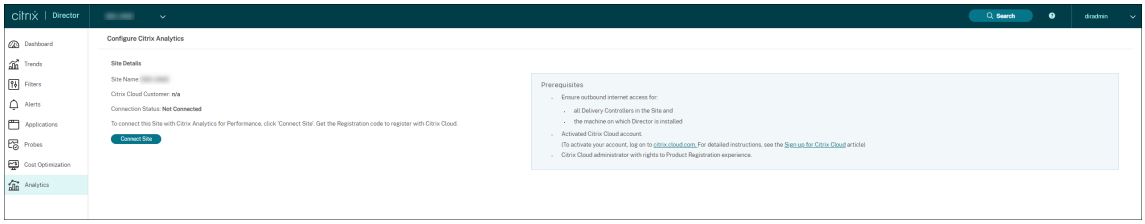


2. Click the **Analytics** tab. The **Configure Citrix Analytics** page appears.



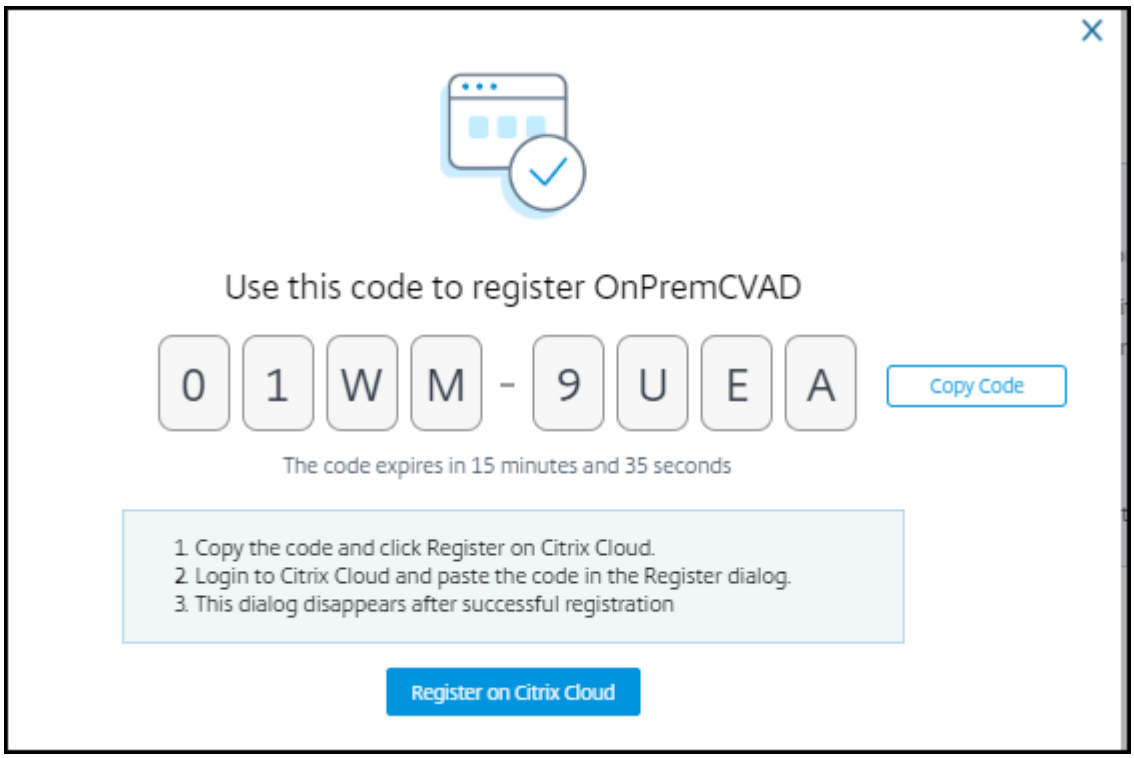
3. Review the steps, select the terms of service, and then click **Get Started**. The **Site Details** page appears.

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



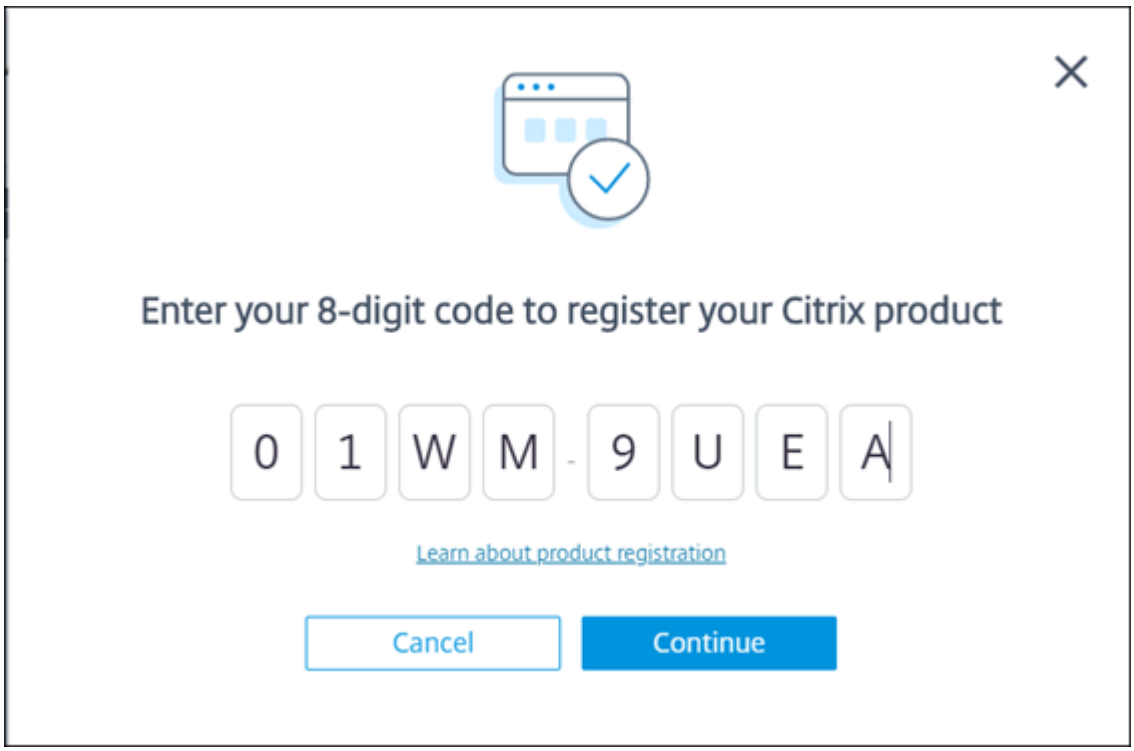
4. Review the prerequisites and ensure that they are met. Review the site details.
5. Click **Connect Site** to start the configuration process.

   A unique 8-digit registration code is generated to be used to register this site with Citrix Cloud.



6. Click **Copy Code** to copy the code and then click **Register on Citrix Cloud**. You are redirected to the registration URL in Citrix Cloud.
7. Sign in with your Citrix Cloud credentials and select your customer.
8. Paste the copied registration code in the Product Registrations page in Citrix Cloud. Click **Continue** to register. Review the registration details and click **Register**.

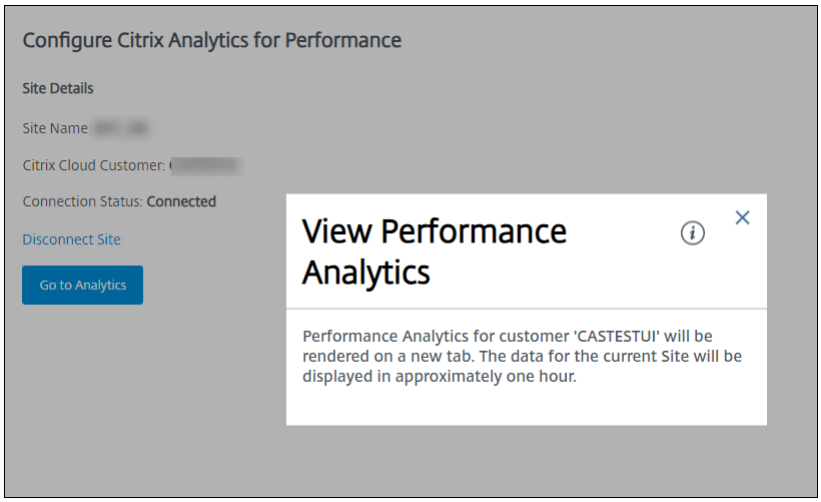
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Your on-premises site registers with Citrix Cloud.

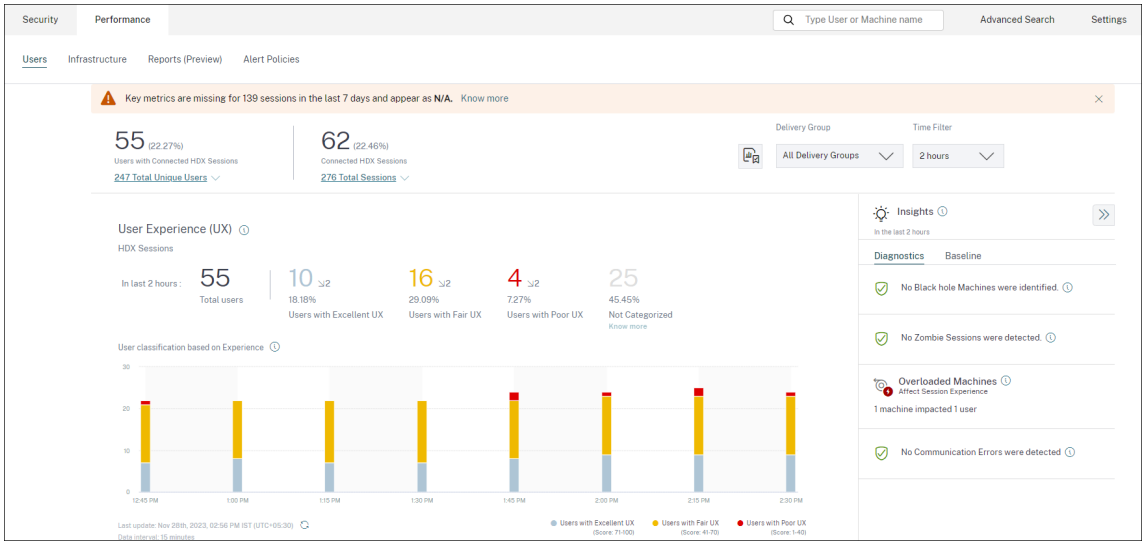
In case the registration input is not displayed, follow the steps decsribed in Register a product.

9. From **Director**, click **Go to Analytics** on the **Analytics** tab.



Performance Analytics opens on a new tab on your browser.

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



If your Citrix Cloud session has expired, you might be redirected to the Citrix.com or My Citrix account logon page.

10. To register multiple sites with Performance Analytics, repeat the preceding configuration steps for each site from Director. Metrics for all configured sites are displayed on the Performance Analytics dashboard.

    In case you have more than one Director instance running per site, configure from any one Director instance. All other Director instances connected to the site are updated at the next refresh after the configuration process.

11. To disconnect your site from Citrix Cloud, click **Disconnect Site**. This option deletes the existing configuration.

    > **Notes:**
    >
    > The first time you configure a site, events from the site might take some time (approximately an hour) to be processed; causing a delay in the display of metrics on the Performance Analytics dashboard. Thereafter, events refresh at regular intervals.
    >
    > Upon disconnect, data transmission from the old account continues for some time until the events from the new account are transmitted. For approximately one hour after data transmission stops, analytics related to the old account remain displayed on the Performance Analytics Dashboard.
    >
    > Upon expiry of entitlement to the Citrix Analytics service, it takes up to a day to stop sending the site metrics to Performance Analytics.

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

Data Governance

September 11, 2025

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

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

Data residency

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

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

Data collection

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

- Citrix ADC (on-premises) along with subscription for Citrix Application Delivery Management
- Citrix Endpoint Management™
- Citrix Gateway (on-premises)
- Citrix Identity provider
- Citrix Secure Browser
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops

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

- Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)
- Microsoft Active Directory
- Microsoft Graph Security

Data transmission

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

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

Data control

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

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

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

Data retention

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

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

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

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

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

Data export

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

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

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

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

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

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

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

Currently, you can integrate with the following SIEM services:

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

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

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

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

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

Citrix Services Security Exhibit

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

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

Definitions

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

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

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

Data collection agreement

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

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

Appendix: logs collected

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

Citrix Analytics for Security logs

General logs

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

- Header Keys
- Device Identification
- Identification
- IP Address
- Organization
- Product
- Product Version
- System Time
- Tenant Identification

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

- Type
- User: Email, Id, SAM Account Name, Domain, UPN
- Version

Citrix Endpoint Management service logs

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

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

Citrix Secure Private Access™ logs

- AAA User Name
- Auth Policy Action Name

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

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

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

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

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

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

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

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

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

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

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

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

Citrix Virtual Apps and Desktops™ and Citrix DaaS logs

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

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

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

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

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

Citrix ADC logs

The Citrix ADC logs contain the following data points:

- Container
- Files
- Format
- Type

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

Citrix DaaS Standard for Azure logs

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

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

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

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

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

- Type
- URL
- User Agent

Citrix Identity provider logs

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

Citrix Gateway logs

- Transaction events:

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

- ICA® App: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx, ICA Flags, Connection Id, Padding Octets Two, ICA Device Serial Number, IP Version 4, Protocol Identifier, Source IPv4 Address Rx, Destination IPv4 Address Rx, Source Transport Port Rx, Destination Transport Port Rx, ICA Application Start up Duration, ICA Launch Mechanism, ICA Application Start up Time, ICA Process ID Launch, ICA Application Name, ICA App Module Path, ICA Application Termination Type, ICA Application Termination Time, Application Name App Id, ICA App Process ID Terminate, ICA App
- ICA Event: Record Type, Actual Template Code, Source IPv4 Address Rx, Destination IPv4 Address Rx, ICA Session Guid, MSI Client Cookie, Connection Chain ID, ICA Client Version, ICA Client Host Name, ICA User Name, ICA Domain Name, Logon Ticket Setup, Server Name, Server Version, Flow Id Rx, ICA Flags, Observation Point Id, Exporting Process Id, Observation Domain Id, Connection Id, ICA Device Serial Number, ICA Session Setup Time, ICA Client IP, NS ICA Session Status Setup, Source Transport Port Rx, Destination Transport Port Rx, ICA Client Launcher, ICA Client Type, ICA Connection Priority Setup, NS ICA Session Server Port, NS ICA Session Server IP Address, IPv4, Protocol Identifier,Connection Chain Hop Count, Access Type
- ICA Update: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx,ICA Flags, Connection Id, ICA Device Serial Number, IPv4, Protocol Identifier, Padding Octets Two, ICA RTT, Client Side RX Bytes, Client Side Packets Retransmit, Server Side Packets Retransmit, Client Side RTT, Client Side Jitter, Server Side Jitter, ICA Network Update Start Time, ICA Network Update End Time, Client Side SRTT, Server Side SRTT,Client Side Delay, Server Side Delay, Host Delay, Client Side Zero Window Count, Server Side Zero Window Count, Client Side RTO Count, Server Side RTO Count, L7 Client Latency, L7 Server Latency, App Name App Id, Tenant Name, ICA Session Update Begin Sec, ICA Session Update End Sec, ICA Channel Id 1, ICA Channel Id 2, ICA Channel Id 2 Bytes, ICA Channel Id 3, ICA Channel Id 3 Bytes, ICA Channel Id 4, ICA Channel Id 4 Bytes, ICA Channel Id 5, ICA Channel Id 5 Bytes
- AppFlow® Config: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, System Rule Flag 1, System Safety Index, AppFlow Profile Relaxed Flags, AppFlow Profile Block Flags, AppFlow Profile Log Flags, AppFlow Profile Learn Flags, AppFlow Profile Stats Flags, AppFlow Profile None Flags, AppFlow App Name Id, AppFlow Profile Sign Disabled, AppFlow Profile Sign Block Count, AppFlow Profile Sign Log Count, AppFlow Profile Sign Stat Count, AppFlow Incarnation Number,AppFlow Sequence Number, AppFlow Profile Sign Auto Update, AppFlow Safety Index, AppFlow App Safety Index, AppFlow Profile Sec Checks Safety Index, AppFlow Profile Type, Iprep App Safety Index, AppFlow Profile Name, AppFlow Sig Name, AppFlow App Name Ls, AppFlow Sig Rule ID1, AppFlow Sig Rule ID2, AppFlow Sig Rule ID3, AppFlow Sig Rule ID4, AppFlow

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

Sig Rule ID5, AppFlow Sig Rule Enabled Flags, AppFlow Sig Rule Block Flags, AppFlow Sig Rule Log Flags, AppFlow Sig Rule File Name, AppFlow Sig Rule Category1, AppFlow Sig Rule Logstring1, AppFlow Sig Rule Category2, AppFlow Sig Rule Logstring2, AppFlow Sig Rule Category3, AppFlow Sig Rule Category4, AppFlow Sig Rule Logstring4, AppFlow Sig Rule Category5, AppFlow Sig Rule LogString5

- AppFlow: Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, Transaction Id, Appfw Violation Occurred Time, App Name App Id, Appfw Violation Severity, Appfw Violation Type, Appfw Violation Location, Appfw Violation Threat Index, Appfw NS Longitude, Appfw NS Latitude, Source IPv4 Address Rx, Appfw Http Method, Appfw App Threat Index, Appfw Block Flags, Appfw Transform Flags, Appfw Violation Profile Name, Appfw Session Id, Appfw Req Url, Appfw Geo Location, Appfw Violation Type Name 1, Appfw Violation Name Value 1, Appfw Sig Category 1, Appfw Violation Type Name 2, Appfw Violation Name Value 2, Appfw Sig Category 2, Appfw Violation Type Name 3, Appfw Violation Name Value 3, Appfw Sig Category3, Appfw Req X Forwarded For, Appfw App Name Ls,App Name Ls, Iprep Category, Iprep Attack Time, Iprep Reputation Score, Iprep NS Longitude, Iprep NS Latitude, Iprep Severity, Iprep HTTP Method, Iprep App Threat Index, Iprep Geo Location, Tcp Syn Attack Cntr, Tcp Slow Ris Cntr, Tcp Zero Window Cntr, Appfw Log Expr Name, Appfw Log Expr Value, Appfw Log Expr Comment
- VPN: Actual Template Code, Observation Domain Id, Access Insight Flags, Observation Point Id, Exporting Process Id, Access Insight Status Code, Access Insight Timestamp, Authentication Duration, Device Type, Device ID, Device Location, App Name App Id, App Name App Id1, Source Transport Port Rx, Destination Transport Port Rx, Authentication Stage, Authentication Type, VPN Session ID, EPA Id, AAA User Name, Policy Name, Auth Agent Name, Group Name, Virtual Server FQDN, cSec Expression, Source IPv4 Address Rx, Destination IPv4 Address Rx, Cur Factor Policy Label, Next Factor Policy Label, App Name Ls, App Name 1 Ls,AAA User Email Id, Gateway IP, Gateway Port, Application Byte Count, VPN Session State, VPN Session Mode, SSO Auth Method, IIP Address, VPN Request URL, SSO Request URL, Backend Server Name, VPN Session Logout Mode, Logon Ticket File Info, STA Ticket, Session Sharing Key, Resource Name, SNIP Address, Temp VPN Session ID
- HTTP: Actual Template Code, Http Req Method, Http Req Url, Http Req User Agent, Http Content Type, Http Req Host, Http Req Authorization, Http Req Cookie, Http Req Referer, Http Res Set Cookie, Ic Cont Grp Name, Ic Flags, Ic Nostore Flags, Ic Policy Name, Response Media Type, Ingress Interface Client, Origin Res Status, Origin Rsp Len, Srv Flow Flags Rx, Srv Flow Flags Tx, Flow Flags Rx, Flow Flags Tx, App Name, Observation Point Id, Exporting Process Id, Observation Domain Id, Http Trans End Time, Transaction Id, Http Rsp Status, Trans Clt Ipv4 Address, Trans Clt Dst Ipv4 Address, Backend Svr Dst Ipv4 Address, Backend Svr Ipv4 Address, Http Rsp Len, Trans Svr RTT, Trans Clt RTT, Http Req Rcv FB, Http Req Rcv LB, Http Res Rcv FB, Http Res Rcv LB, Http Req Forw FB, Http Req Forw LB, Http Res Forw

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

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

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

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

Requests, RATE Si Tot_Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions,Si Tot Svr Tlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions

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

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

Count, Sys Cpus, Tcp Cur Client Conn, Tcp Cur Client Conn Closing, Tcp Cur Client Conn Est, Tcp Cur Server Conn, Tcp Cur Server Conn Closing, Tcp Cur Server Conn Est, Tcp Err Rst, Tcp Tot Client Open, Tcp Tot Server Open, Tcp Tot Rx Bytes, Tcp Tot Rx Pkts, Tcp Tot Syn, Tcp Tot Tx Bytes, Tcp Tot Tx Pkts, Udp Tot Rx Bytes, Udp Tot Rx Pkts, Udp Tot Tx Bytes, Udp Tot Tx Pkts

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

Secure Browser logs

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

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

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

- Application Delete:

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

- Application Update:

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

- Entitlement Create:

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

- Entitlement Update:

    - Logs before the entitlement update: Approved, Customer Id, Data Retention Days, End Date, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type

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

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

- Session Access Host: Accept Host, Client IP, Date Time, Host, Session, User Name
- Session Connect:
    - Logs before the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
    - Logs after the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- Session Launch:
    - Logs before the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
    - Logs after the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- Session Tick:
    - Logs before the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
    - Logs after the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name

Microsoft Graph Security logs

- Tenant Id
- User Id
- Indicator Id
- Indicator UUID
- Event Time
- Create Time
- Category of alert
- Logon Location
- Logon IP
- Logon Type

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

- User Account Type
- Vendor Information
- Vendor Provider Information
- Vulnerability States
- Vulnerability Severity

Microsoft Active Directory logs

- Tenant Id
- Collect Time
- Type
- Directory Context
- Groups
- Identity
- User Type
- Account Name
- Bad Password Count
- City
- Common Name
- Company
- Country
- Days Until Password Expiry
- Department
- Description
- Display Name
- Distinguished Name
- Email
- Fax Number
- First Name
- Group Category

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

- Group Scope
- Home Phone
- Initials
- IP Phone
- Is Account Enabled
- Is Account Locked
- Is Security Group
- Last Name
- Manager
- Member of
- Mobile Phone
- Pager
- Password Never Expires
- Physical Delivery Office Name
- Post Office Box
- Postal Code
- Primary Group Id
- State
- Street Address
- Title
- User Account Control
- User Group List
- User Principal Name
- Work Phone

Citrix Analytics for Performance logs

- actionid
- actionreason
- actiontype

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

- adminfolder
- agentversion
- allocationtype
- applicationid
- applicationname
- applicationpath
- applicationtype
- applicationversion
- associateduserfullnames
- associatedusername
- associatedusernames
- associateduserupns
- authenticationduration
- autoreconnectcount
- autoreconnecttype
- AvgEndpointThroughputBytesReceived
- AvgEndpointThroughputBytesSent
- blobcontainer
- blobendpoint
- blobpath
- brokerapplicationchanged
- brokerapplicationcreated
- brokerapplicationdeleted
- brokeringdate
- brokeringduration
- brokerloadindex
- brokerregistrationstarted
- browsername
- catalogchangeevent

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

- catalogcreatedevent
- catalogdeletedevent
- catalogid
- catalogname
- catalogsync
- clientaddress
- clientname
- clientplatform
- clientsessionvalidatedate
- clientversion
- collecteddate
- connectedviahostname
- connectedviaipaddress
- connectionid
- connectioninfo
- connectionstate
- connectiontype
- controllerdnsname
- cpu
- cpuindex
- createddate
- currentloadindexid
- currentpowerstate
- currentregistrationstate
- currentsessioncount
- datetime
- deliverygroupadded
- deliverygroupchanged
- deliverygroupdeleted

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

- deliverygroupid
- deliverygroupmaintenancemodechanged
- deliverygroupname
- deliverygroupsync
- deliverytype
- deregistrationreason
- desktopgroupdeletedevent
- desktopgroupid
- desktopgroupname
- desktopkind
- disconnectcode
- disconnectreason
- disk
- diskindex
- dnsname
- domainname
- effectiveloadindex
- enddate
- errormessage
- establishmentdate
- eventreporteddate
- eventtime
- exitcode
- failurecategory
- failurecode
- failuredata
- failuredate
- failurereason
- failuretype

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

- faultstate
- functionallevel
- gpoenddate
- gpostartdate
- hdxenddate
- hdxstartdate
- host
- hostedmachineid
- hostedmachinename
- hostingservername
- hypervisorconnectionchangedevent
- hypervisorconnectioncreatedevent
- hypervisorid
- hypervisorname
- hypervisorsync
- icartt
- icarttms
- id
- idletime
- inputbandwidthavailable
- inputbandwidthused
- instancecount
- interactiveenddate
- interactivestartdate
- ipaddress
- isassigned
- isinmaintenancemode
- ismachinephysical
- ispendingupdate

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

- ispreparing
- isremotepc
- issecureica
- lastderegisteredcode
- launchedviahostname
- launchedviaipaddress
- lifecyclestate
- LinkSpeed
- logonduration
- logonenddate
- logonscriptsenddate
- logonscriptsstartdate
- logonstartdate
- long
- machineaddedtodesktopgroupevent
- machineassignedchanged
- machinecatalogchangedevent
- machinecreatedevent
- machinedeletedevent
- machinederegistrationevent
- machinednsname
- machinefaultstatechangeevent
- machinehardregistrationevent
- machineid
- machinemaintenancemodechangeevent
- machinename
- machinepvdstatechanged
- machineregistrationendedevent
- machineremovedfromdesktopgroupevent

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

- machinerole
- machinesid
- machineupdatedevent
- machinewindowsconnectionsettingchanged
- memory
- memoryindex
- modifieddate
- NGSConnector.ICAConnection.Start
- NGSConnector.NGSSyntheticMetrics
- NGSConnector.NGSPassiveMetrics
- NGSConnector.NGSSystemMetrics
- network
- networkindex
- networklatency
- networkinfoperiodic
- NetworkInterfaceType
- ostype
- outputbandwidthavailable
- outputbandwidthused
- path
- percentcpu
- persistentuserchanges
- powerstate
- processname
- profileloadenddate
- profileloadstartdate
- protocol
- provisioningschemeid
- provisioningtype

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

- publishedname
- registrationstate
- serversessionvalidatedate
- sessioncount
- sessionend
- sessionfailure
- sessionid
- sessionidlesince
- sessionindex
- sessionkey
- sessionstart
- sessionstate
- sessionsupport
- sessiontermination
- sessiontype
- sid
- SignalStrength
- siteid
- sitename
- startdate
- totalmemory
- triggerinterval
- triggerlevel
- triggerperiod
- triggervalue
- usedmemory
- userid
- userinputdelay
- username

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

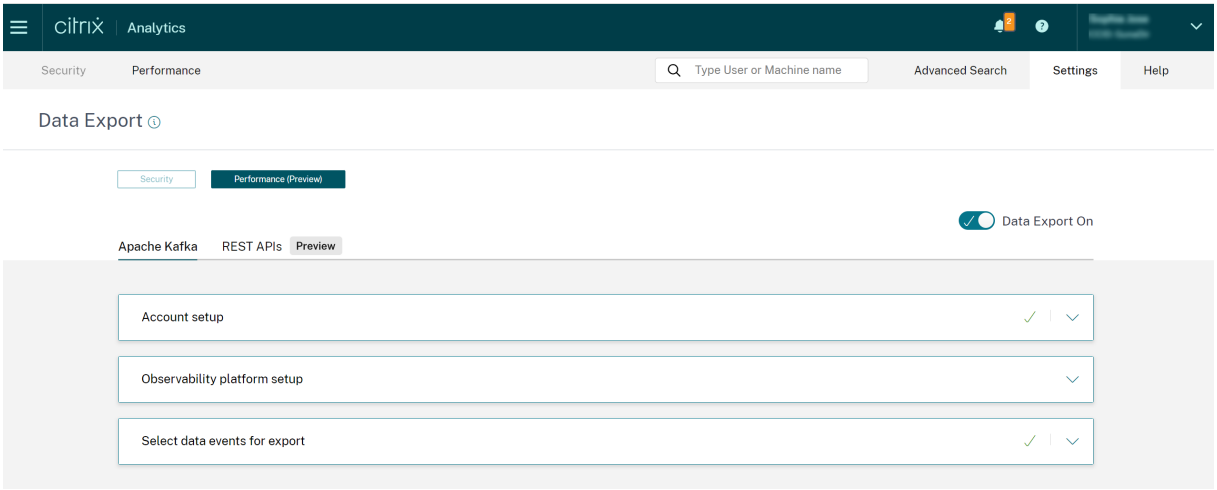
- usersid
- vdalogonduration
- vdaprocessdata
- vdaresourcedata
- version
- vmstartenddate
- vmstartstartdate
- windowsconnectionsetting
- xd.SessionStart

Data Export to Observability Platform (Preview)

September 1, 2025

Citrix Analytics for Performance™ is now integrated with the Splunk, Elasticsearch, and Grafana Observability platform. You can use the **Data Export** feature to export performance data and events from Citrix Analytics for Performance to Splunk, Elasticsearch, and Grafana.

> **Note:**
>
> You can export data to only one endpoint at a time.



The Observability platform gives you a holistic view of the performance metrics that belong to the on-premises Citrix Virtual Apps and Desktops™ sites and the DaaS cloud services that have been onboarded to your Citrix Analytics for Performance service. Further, you can combine and correlate per-

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

formance metrics from Citrix Analytics for Performance data with data from external data sources that are connected within your Observability platform.

Data available in the Observability platform can be used to derive value through continuous monitoring. It helps get actionable business insights into the performance of your virtual apps and desktop sites. Some ways in which you can use the data in the Observability platform are as follows:

- Create dashboards and reports in a regular cadence. These dashboards and reports help analyze the performance of your environment over time.
- Extract information of specific interest to your organization's KPIs and identify bottlenecks causing poor user performance.
- Identify machines in your sites that are underutilized and optimize consumption and usage to reduce overall costs.
- Triage and troubleshoot specific issues that users in your infrastructure are facing during connection and in-session.
- Easily root cause and pinpoint poor in-session experience to client-side network or end point device issues, or to issues on specific infrastructure components like the gateway or the connector.
- Identify patterns in session failures and high session latency to see if poor experience can be localized to a location or a specific service provider.
- Identify particular apps or processes that are causing a resource crunch.

To use this functionality, sign up and enroll to the Technical Preview using this form.

Integration with Observability Platform

Currently, the Observability platforms that Citrix Analytics for Performance support are Splunk, Elasticsearch, and Grafana. For more information on the features and usage of:

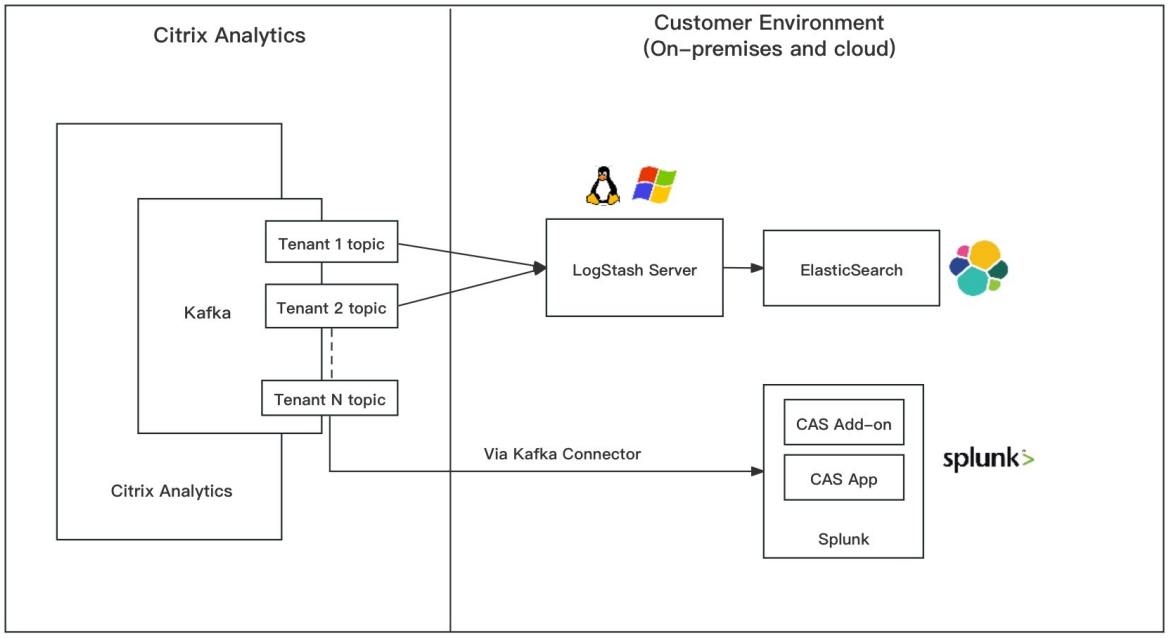
- Splunk, see the Splunk documentation.
- Elasticsearch, see the Elasticsearch documentation
- Grafana, see the Grafana documentation

Splunk connects with the north-bound Kafka deployed on Citrix Analytics for Performance cloud using Kafka endpoints. Use the parameters provided by Citrix Analytics for Performance to integrate Citrix Analytics for Performance with Splunk. Using the Kafka endpoints, you can connect and pull the data into Splunk.

Elasticsearch connects with the Kafka deployed on Citrix Analytics for Performance cloud using the Logstash engine. Use the parameters provided by Citrix Analytics for Performance to integrate Citrix Analytics for Performance with Elasticsearch. Using the Kafka endpoints, you can connect and pull the data into Elasticsearch and get deeper insights into your organization's performance posture.

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

The following architecture diagram explains how data flows from Citrix Analytics for Performance to Observability platform:



Getting Started with Data Export

The Data Export feature can be accessed and configured from **Citrix Analytics Service > Settings > Data Export > Performance**. Data export to the Observability platform is turned on by default with the **Data Export On** toggle. You can toggle **Data Export Off**, to stop sending new data events.

Data Export is configured in the following steps. For more information, see the Splunk Integration and the Elasticsearch integration articles.

1. **Account setup** - To create an account, specify a password. Once you configure your account, the Kafka details are generated. These details are used in the configuration with Splunk and Elasticsearch. Use this section to reset your password.
2. **Observability platform setup** - Install and configure Citrix Analytics Add-On for Splunk, Elasticsearch, and Grafana using the Kafka details generated in the previous step.
3. **Select data events for export** - This section lists the data exported to the Observability platform. You can select specific events you want to export from the Sessions and Machines data sources.

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

Splunk Integration with Citrix Analytics for Performance™

September 1, 2025

You can integrate Citrix Analytics for Performance with Splunk to export performance data from your virtual apps and desktops sites to Splunk and get deeper insights into the performance of your virtual apps and desktops environment.

For more information about the benefits of the integration and the type of processed data that is sent to your Observability platform, see Data Export.

Supported versions

Citrix Analytics for Performance supports Splunk integration on the following operating systems. Citrix recommends using the latest version of these operating systems or versions that are still under support from the respective vendors.

- CentOS Linux 7 and later
- Debian GNU/Linux 10.0 and later
- Red Hat Enterprise Linux Server 7.0 and later
- Ubuntu 18.04 LTS and later

> **Note**
>
> For the Linux Kernel (64-bit) operating systems, use a kernel version that Splunk supports. For more information, see Splunk documentation.

You can configure Splunk integration on the following Splunk versions:

- Splunk Cloud Inputs Data Manager (IDM)
- Splunk 8.1 (64-bit) and later

Prerequisites

Citrix Analytics add-on for Splunk connects to the following endpoints on Citrix Analytics for Performance. Ensure that the endpoints are in the allow list in your network. Use the endpoint names and not IP addresses, as the public IP addresses of the endpoints might change.

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

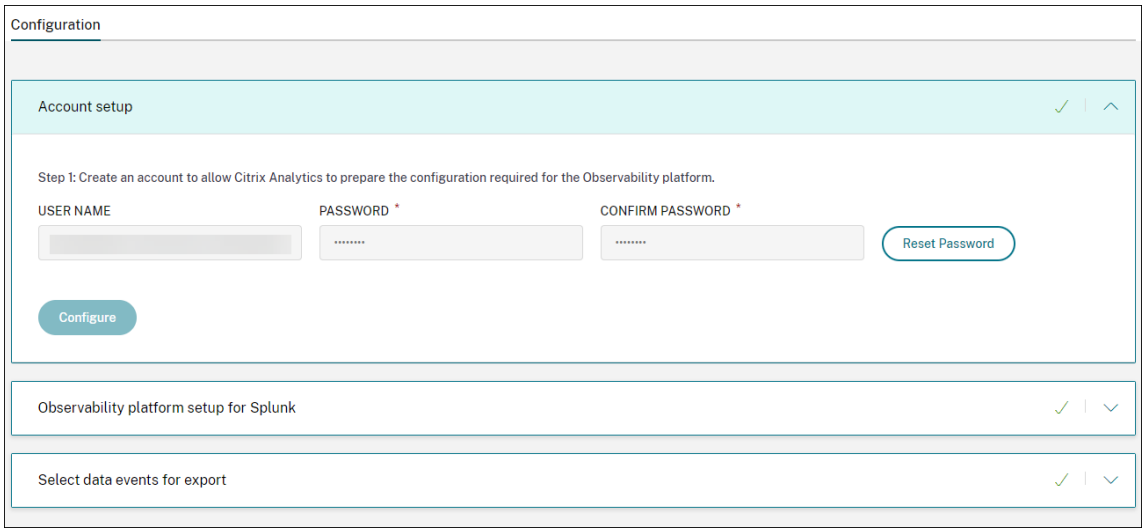
Endpoint	United States region	European Union region	Asia Pacific South region
Kafka brokers	casnb-0.citrix.com:9094 casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-0.citrix.com:9094 casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-0.citrix.com:9094 casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

Turn on data processing for at least one data source. It helps Citrix Analytics for Performance to begin the Splunk integration process.

Data Export Configuration

Account Setup

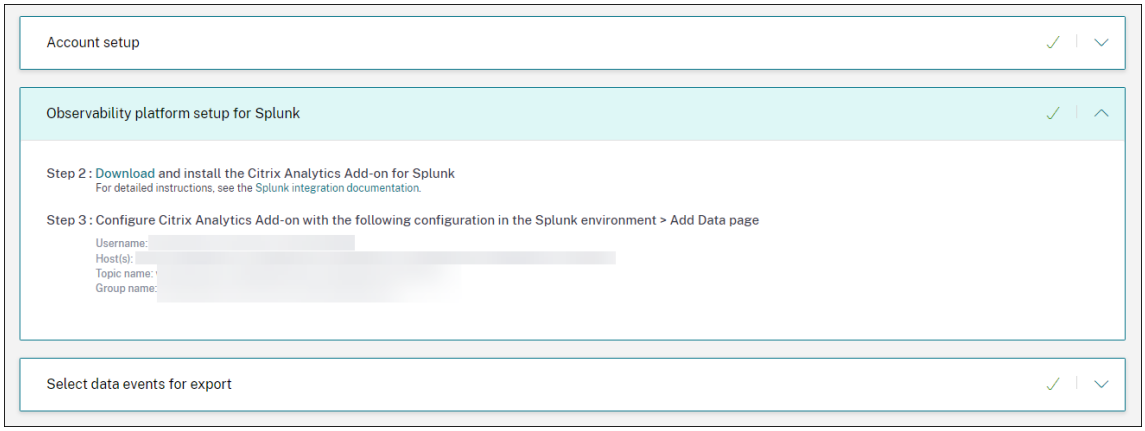
1. Go to **Settings** > **Data Exports** > **Performance**.
2. In the **Account setup** section, create an account by specifying a password. This account is used to prepare a configuration file required for Splunk integration.



3. Click **Configure**. Citrix Analytics for Performance prepares the configuration details - user name, hosts, Kafka topic name, and group name. Copy the details to help configure Citrix Analytics Add-on for Splunk in the subsequent steps.

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

> **Note**
>
> These details are sensitive and you must store them in a secure location.



Observability Platform setup for Splunk

Download and install Citrix Analytics Add-on for Splunk

> **Note**
>
> This app is in preview.

Citrix Analytics add-on for Splunk enables Splunk Enterprise administrators to view performance data collected from Citrix Analytics for Performance. You can also correlate the data collected from Citrix Analytics for Performance with data from other data sources configured on your Splunk. This correlation provides you visibility into performance from multiple sources and take actions to improve the usage and performance of your virtual apps and desktops environment.

1. Log on to your Splunk Forwarder or Splunk Standalone environment.
2. Install the Citrix Analytics Add-on for Splunk by either downloading it from Splunkbase or by installing it from within Splunk.

Install app from Splunkbase

1. Download the Citrix Analytics Add-on for Splunk file.
2. On the Splunk Web home page, click the gear icon next to **Apps**.
3. Click **Install app from file**.
4. Locate the downloaded file and click **Upload**.

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

> **Notes**
>
> - If you have an older version of the add-on, select **Upgrade app** to overwrite it.
> - If you are upgrading **Citrix Analytics Add-on for Splunk** from a version earlier than 2.0.0, you must delete the following files and folders located inside the */bin* folder of the add-on installation folder and restart your Splunk Forwarder or Splunk Stand-alone environment:
>   - `cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin`
>   - `rm -rf splunklib`
>   - `rm -rf mac`
>   - `rm -rf linux_x64`
>   - `rm CARoot.pem`
>   - `rm certificate.pem`

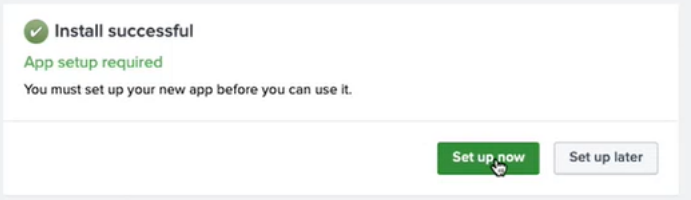
5. Verify that the app appears in the **Apps** list.

Install app from within Splunk

1. From the Splunk Web home page, click **+Find More Apps**.
2. On the Browse More Apps page, search **Citrix Analytics Add-on for Splunk**.
3. Click **Install** next to the app.
4. Verify that the app appears in the **Apps** list.

Configure index and source type to correlate data

1. After you install the app, click **Set up now**.

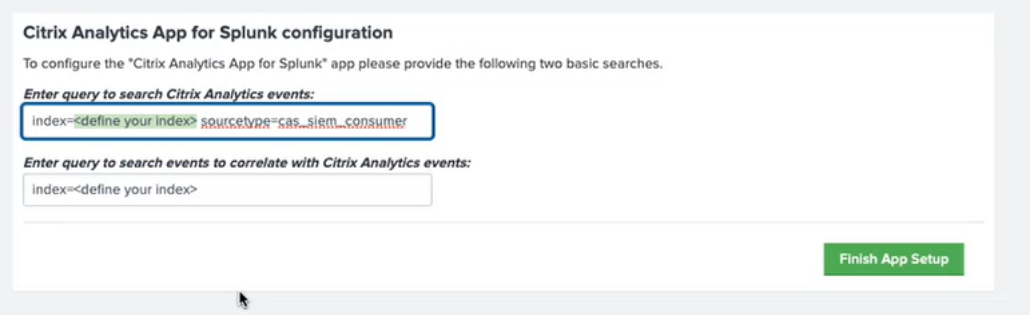


2. Enter the following queries:
   - Index and source type where the data from Citrix Analytics for Performance are stored.

     > **Note**
     >
     > These query values must be the same as specified in the Citrix Analytics Add-on for Splunk. For more information, see Configure Citrix Analytics Add-on for Splunk.

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

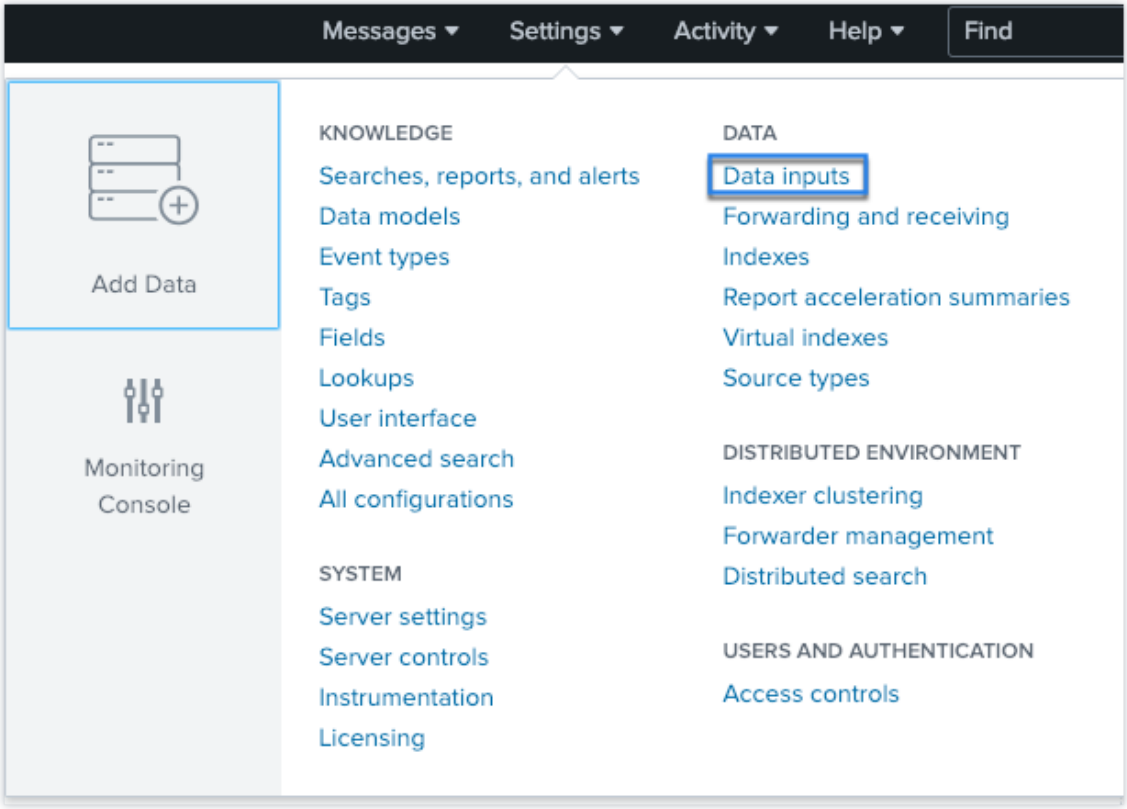
- Index from which you want to correlate your data with Citrix Analytics for Performance.



3. Click **Finish App Setup** to complete the configuration.

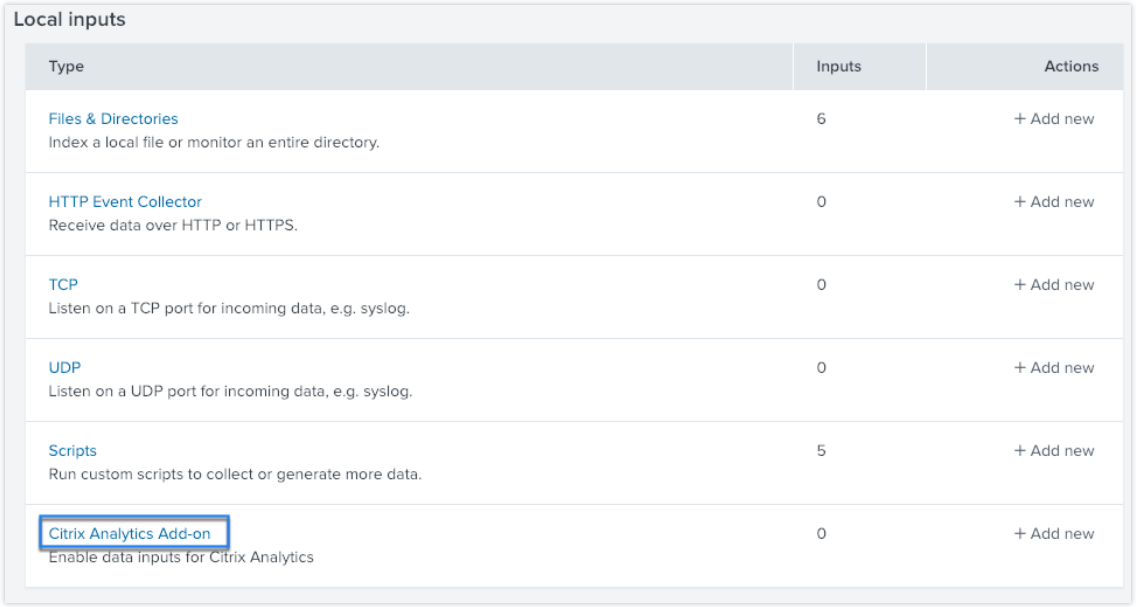
Configure Citrix Analytics Add-on for Splunk Configure the Citrix Analytics Add-on for Splunk using the configuration details provided by Citrix Analytics for Performance. After the add-on is successfully configured, Splunk starts consuming events from Citrix Analytics for Performance.

1. On the Splunk home page, go to **Settings** > **Data inputs**.

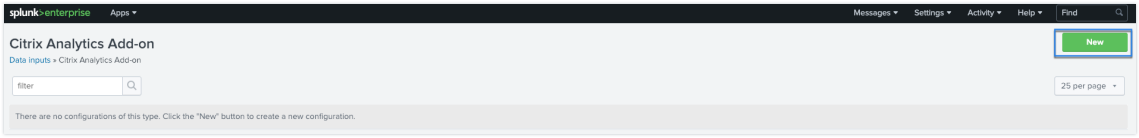


2. In the **Local inputs** section, click **Citrix Analytics Add-on**.

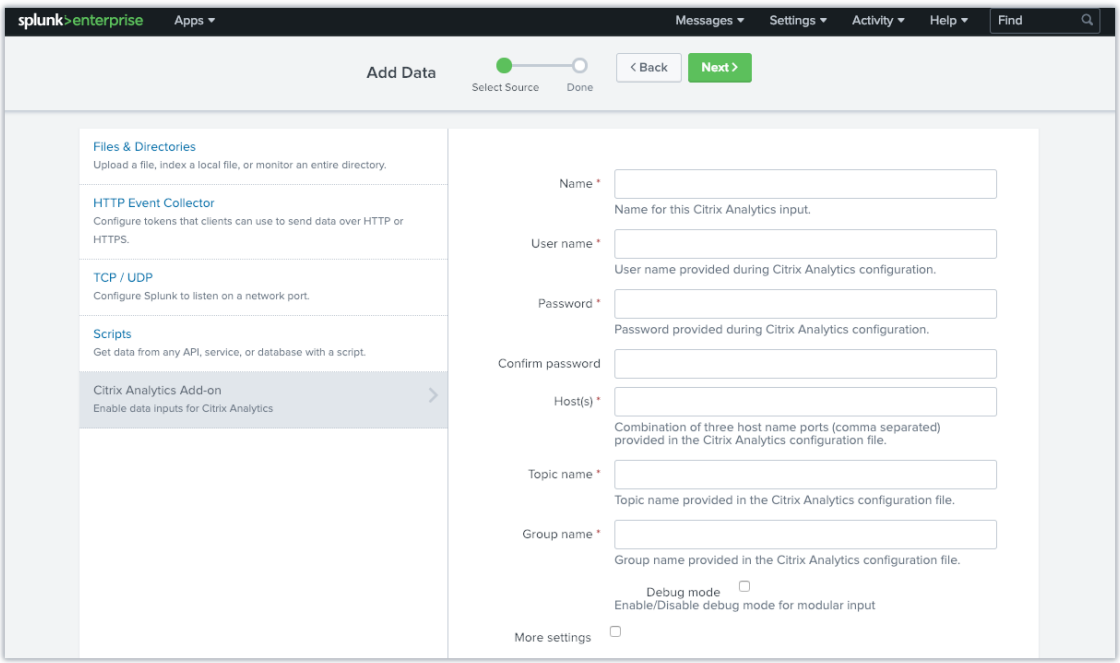
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Click **New**.

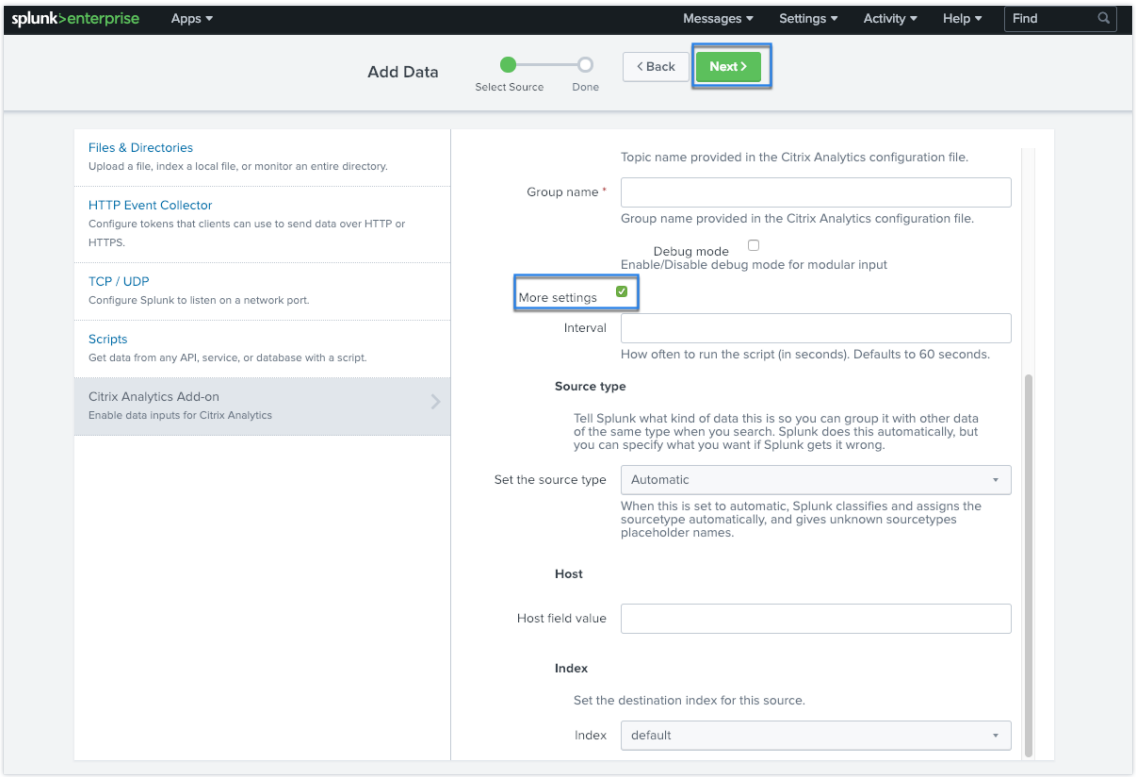


4. On the **Add Data** page, enter the details provided in the Citrix Analytics configuration file.



5. To customize your default settings, click **More settings** and set up the data input. You can define your own Splunk index, host name, and source type.

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



6. Click **Next**. Your Citrix Analytics data input is created and Citrix Analytics Add-on for Splunk is configured successfully.

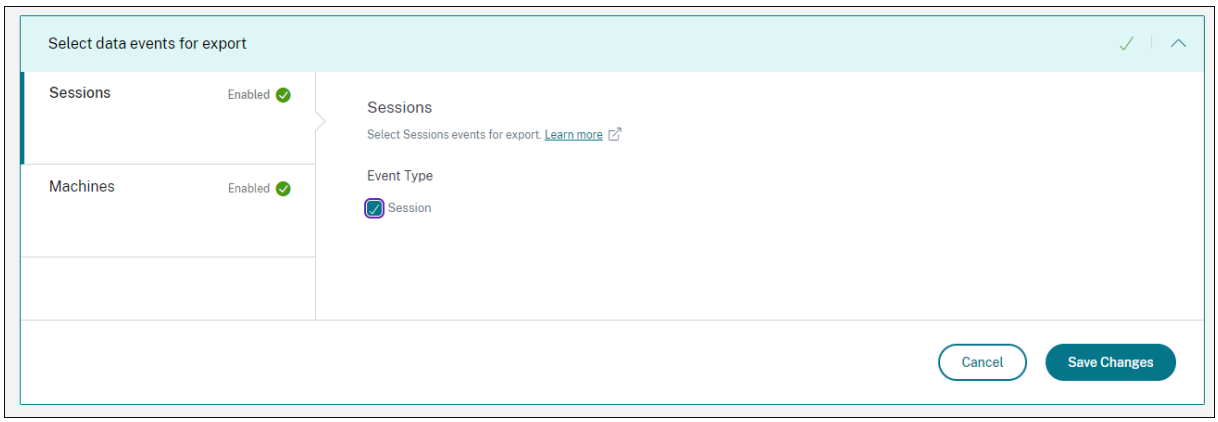
Select data events for Export

This section lists data that is exported to the Observability platform. You can select the events you want to export from the Sessions and Machines data sources. The changes made to this selection takes up to two hours to be available in the exported data.

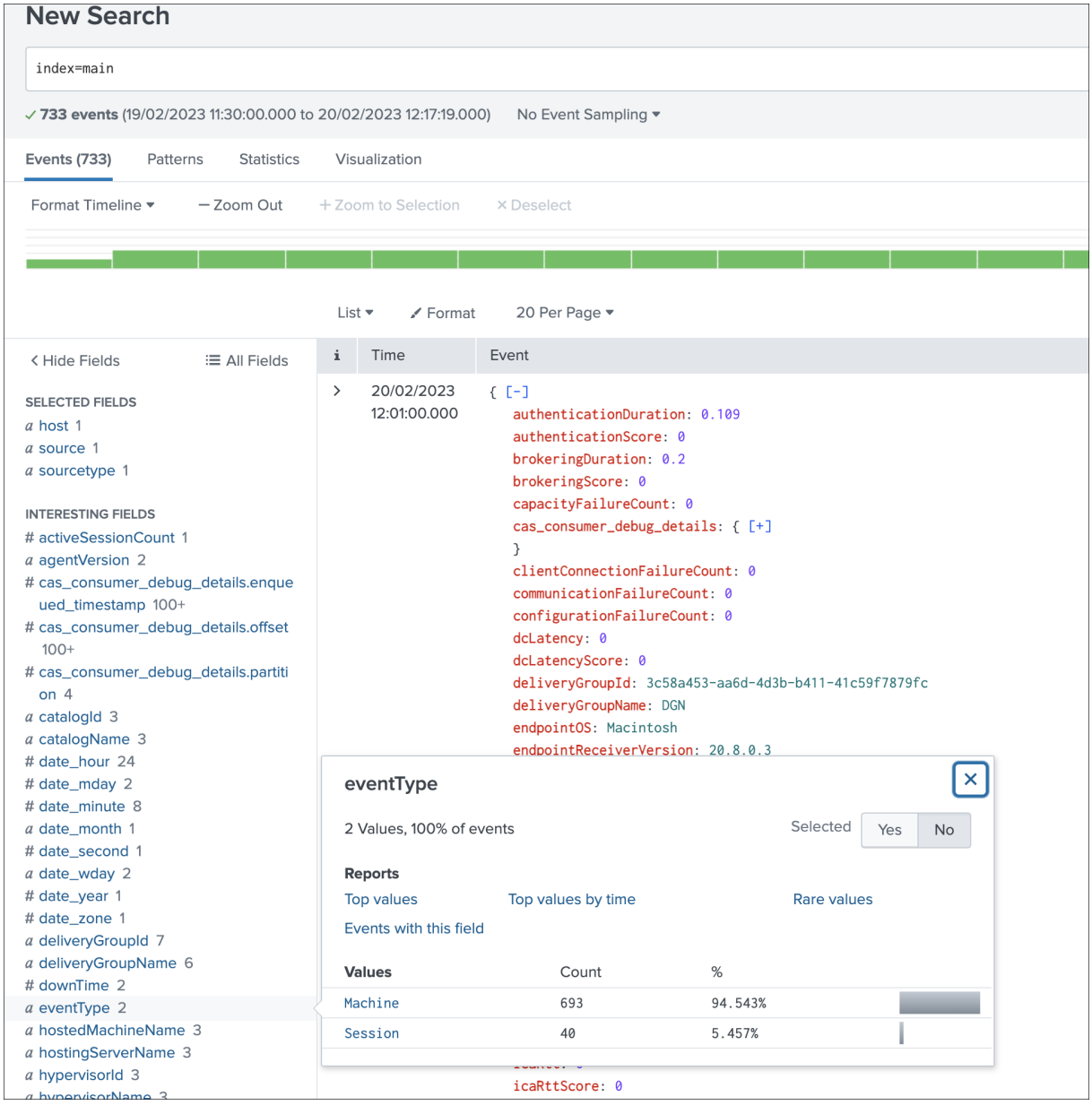
How to consume events in Splunk

After you configure the add-on, Splunk starts retrieving performance data and events from Citrix Analytics for Performance. You can start searching your organization's events on the Splunk search head based on the configured data input.

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

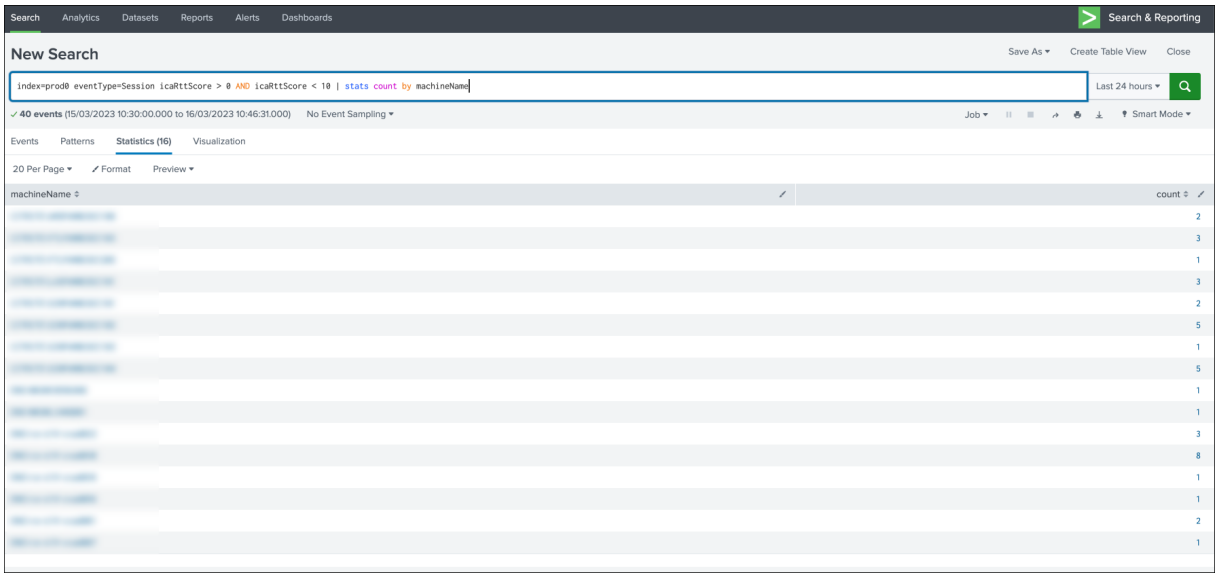


The search results are displayed in the following format:

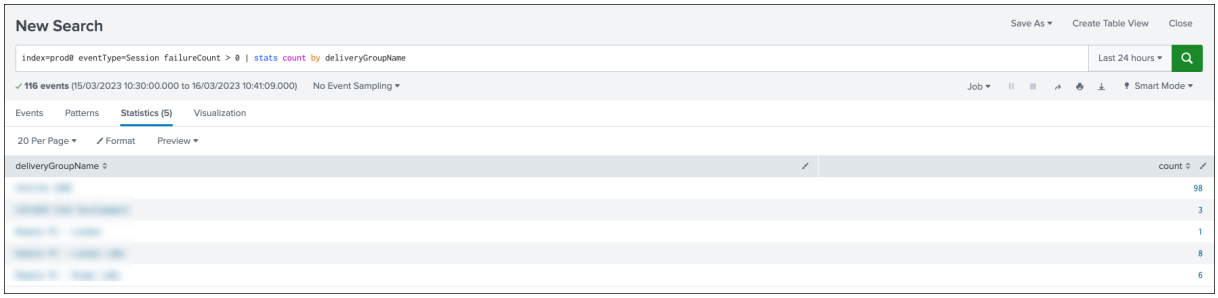


© 1997–2026 Citrix Systems, Inc. All rights reserved.

A sample displaying the list of machines running sessions with poor session responsiveness:



A sample displaying the failed sessions:



For more information about the data format, see Data Structure of the Machines Events and Data Structure of the Sessions Events.

For more information about Splunk integration, refer to the following links:

- Citrix Analytics Integration with Splunk
- The Citrix Analytics add-on for Splunk, now in Splunkbase

Troubleshoot Citrix Analytics Add-on for Splunk

If you don't see any data in your Splunk dashboards or encountered issues while configuring Citrix Analytics Add-on for Splunk, perform the debugging steps to fix the issue. For more information, see Configuration issues with Citrix Analytics add-on for Splunk.

> **Note**

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

> Contact CAS-PM-Ext@cloud.com to request assistance for the Splunk integration, exporting data to Splunk, or to provide feedback.

Elasticsearch integration

September 1, 2025

> **Note:**
>
> Contact CAS-PM-Ext@cloud.com to request assistance for the Elasticsearch integration, exporting data to Elasticsearch, or provide feedback.

You can integrate Citrix Analytics for Performance™ with Elasticsearch by using the Logstash engine. This integration enables you to export and correlate the users'data from your Citrix IT environment to Elasticsearch and get deeper insights into your organization's security posture.

For more information about the benefits of the integration and the type of processed data that is sent to your Observability platform, see Data Export.

Prerequisites

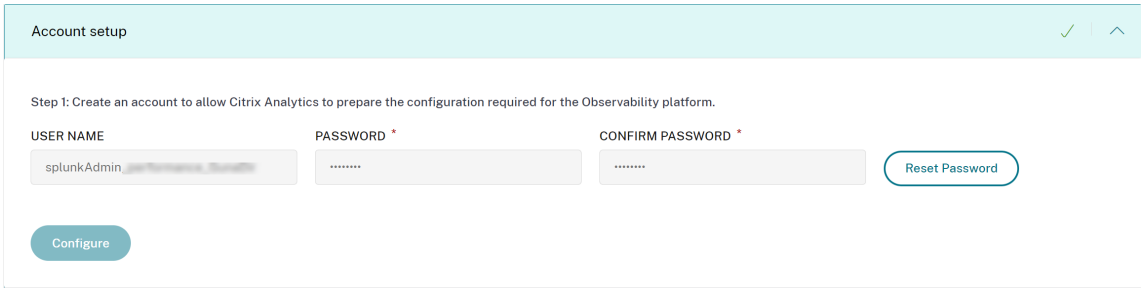
- Turn on data processing for at least one data source. It helps Citrix Analytics for Performance to begin the Elasticsearch integration process.
- Ensure that the following endpoint is in the allow list in your network.

Endpoint	United States region	European Union region	Asia Pacific South region
Kafka brokers	casnb-0.citrix.com:9094 casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-0.citrix.com:9094 casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-0.citrix.com:9094 casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

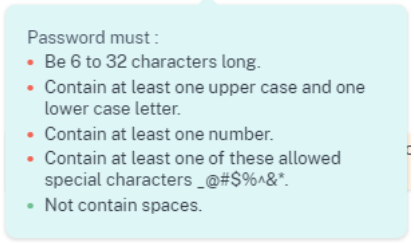
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Integrate with Elasticsearch

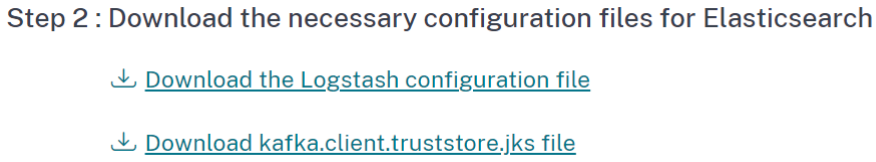
1. Go to **Settings** > **Data Exports**.
2. On the **Account set up** section, create an account by specifying the user name and a password. This account is used to prepare a configuration file, which is required for integration.



3. Ensure that the password meets the following conditions:



4. Click **Configure** to generate the Logstash configuration file.

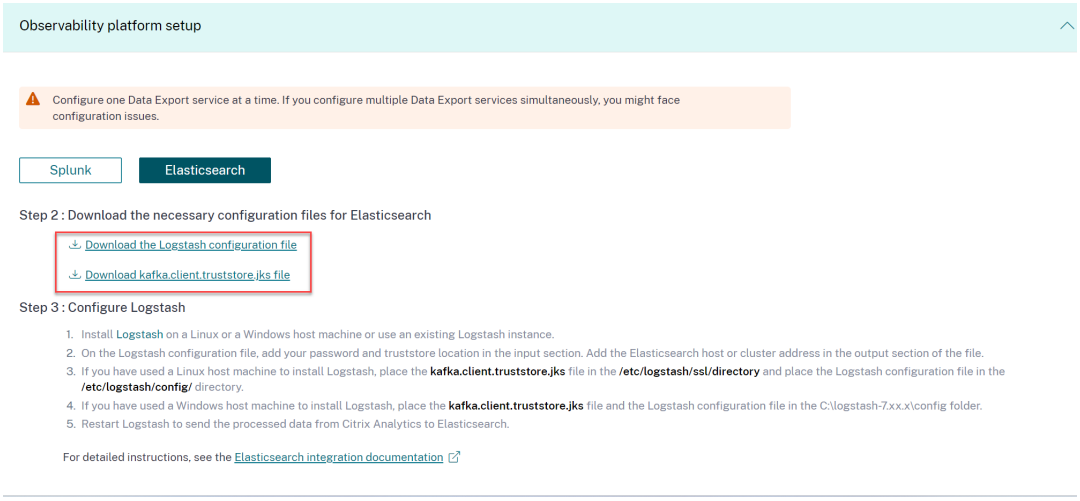


5. Select the **Elastic Search** tab from the Observability Platform section to download the configuration files:

   - **Logstash config file**: Contains the configuration data (input, filter, and output sections) for sending events from Citrix Analytics for Performance to Elasticsearch using the Logstash data collection engine. For information on the Logstash config file structure, see the Logstash documentation.
   - **JKS file**: Includes the certificates required for SSL connection.

     > **Note**
     >
     > These files contain sensitive information. Keep them in a safe and secure location.

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



6. Configure Logstash:

   a) On your Linux or Windows host machine, install Logstash. You can also use your existing Logstash instance.

   b) On the host machine where you have installed Logstash, place the following files in the specified directory:

Host machine type	File name	Directory path
Linux	CAS_Elasticsearch_LogStash_Config.conf	For Debian and RPM packages: `/etc/logstash/conf.d/` For .zip and .tar.gz archives: `{ extract.path } /config`
	kafka.client.truststore.jks	For Debian and RPM packages: `/etc/logstash/ssl/` For .zip and .tar.gz archives: `{ extract.path } /ssl`
Windows	CAS_Elasticsearch_LogStash_Config.conf	`C:\logstash-7.xx.x\config`
	kafka.client.truststore.jks	

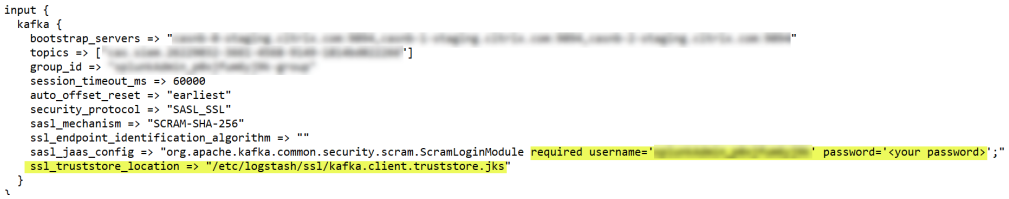
   For information on the default directory structure of Logstash installation packages, see the Logstash documentation.

   c) Open the Logstash config file and do the following:

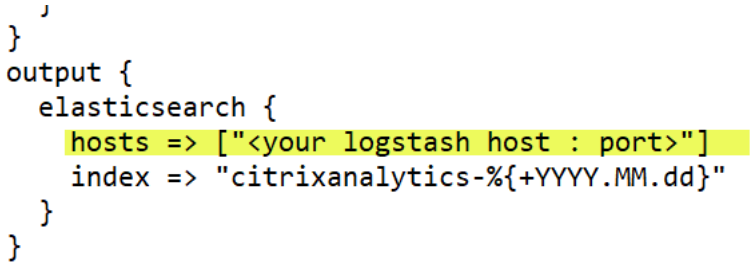
      i. In the input section of the file, enter the following information:

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

- **Password**: The password of the account that you've created in Citrix Analytics for Performance to prepare the configuration file.
- **SSL truststore location**: The location of your SSL client certificate. This is the location of the kafka.client.truststore.jks file in your host machine.



ii. In the output section of the file, enter the address of your host machine or the cluster where Elasticsearch is running.



d) Restart your host machine to send processed data from Citrix Analytics for Performance to Elasticsearch.

After configuration is complete, verify that you can view the Citrix Analytics data in your Elasticsearch.

Logstash configuration

A sample Logstash configuration can be downloaded from the Citrix Analytics for Performance page.

The following is a small variation of the Logstash pipeline definition that can support the provided sample Kibana dashboards:

```
filter {

  json {

    source => "message"
    remove_field => ["message"]
   }

  date {

```

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

```
    match => [ "timestamp", "ISO8601", "yyyy-MM-dd HH:mm:ss" ]
    target => "@timestamp"
   }

 }


filter {

  mutate {

    copy => ["eventType", "[@metadata][eventTypeIndex]"]
   }

 }


filter {

  mutate {

    lowercase => ["[@metadata][eventTypeIndex]"]
   }

 }


output {

  elasticsearch {

    hosts => ["<your logstash host : port>"]
    index => "citrixanalytics-%{
 [@metadata][eventTypeIndex] }
 -%{
 +YYYY.MM.dd }
 "
   }

 }
```

Based on the previous configuration, Logstash uses the `eventType` field to separate Session and Machine events to separate indexes.

You can replace the “filter”and “output”sections of the default configuration file downloaded from the Citrix Analytics page with the preceding content and restart the Logstash service.

Kibana dashboard samples

You can import the sample Kibana dashboard provided by Citrix which includes:

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

- Metrics
- Time charts
- Other useful visualizations of session and infrastructure telemetry.

You can download the dashboard definitions (JSON files) from the Citrix Analytics downloads page.

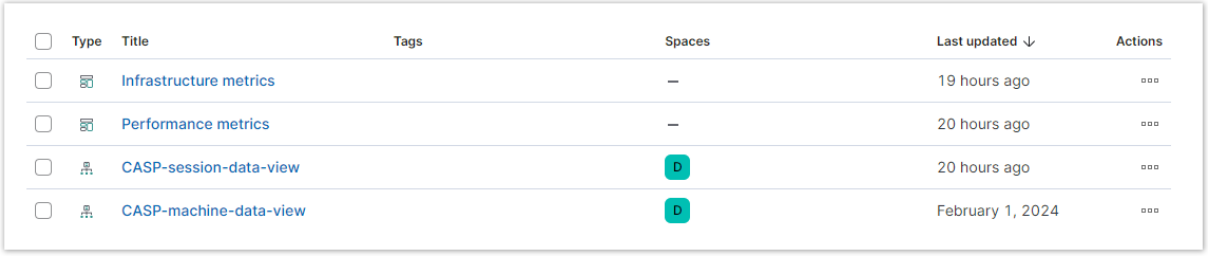
You can import the dashboard files into your Kibana instance, either to a Elasticsearch cloud or enterprise account.

Before importing the dashboard, make sure you have properly configured your Logstash, Elasticsearch, and Kibana instances and are able to view `citrixanalytics` indexes in the Kibana Index Management page.

To import the dashboards and referenced data views, perform the following steps:

1. Navigate to **Management** > **Saved Object**.
2. Click **Import** and select the provided `ndjson` file included in the given compressed file.
3. You can optionally select **Create new objects with random IDs**.
4. Click **Import**.

After you complete the preceding steps, you can view the four new saved objects as displayed in the following image:

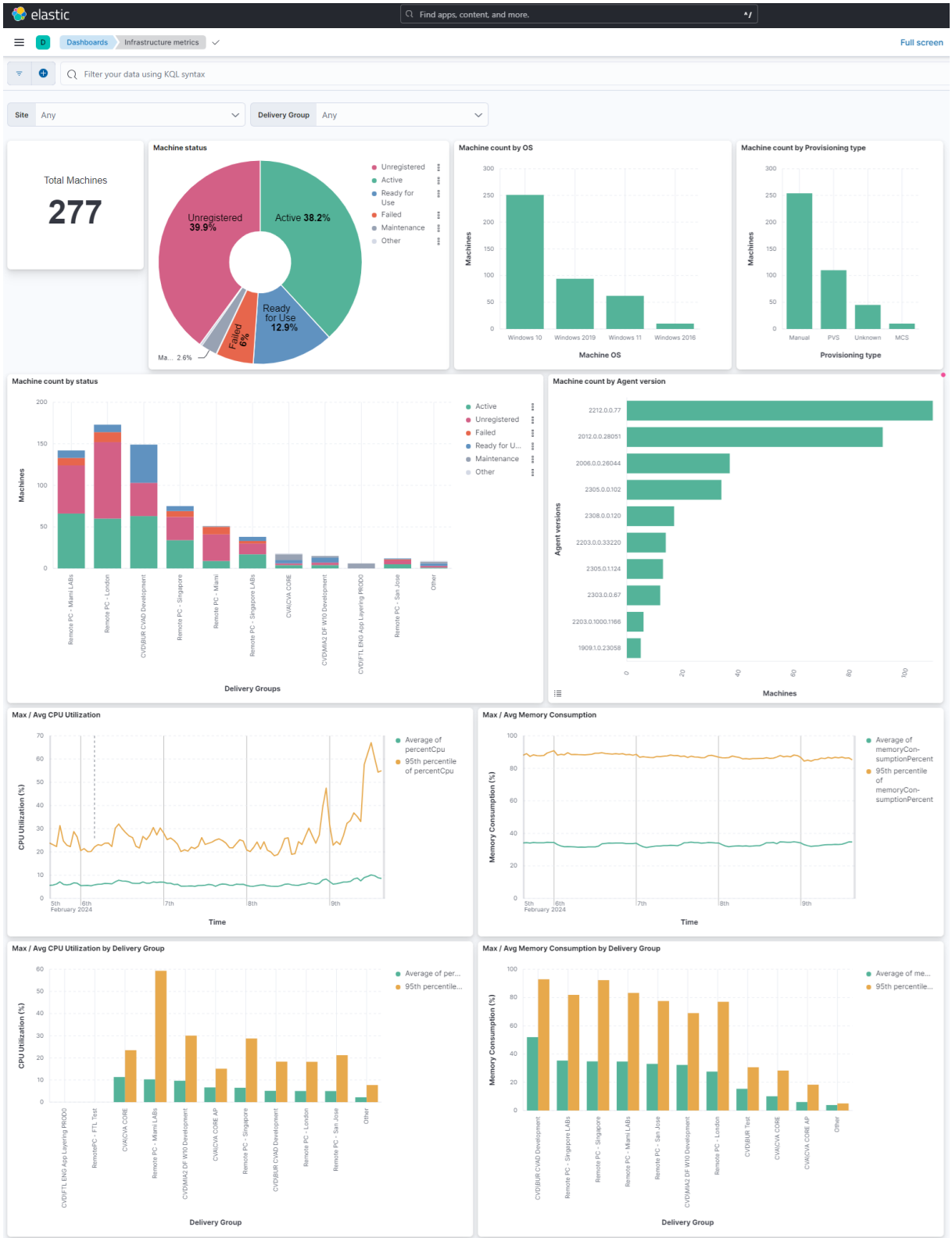


The data views are referenced by the dashboard visualizations and are referencing the indexes defined in the preceding Logstash configuration. You must be able to open the dashboards. The following are sample dashboards:

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



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



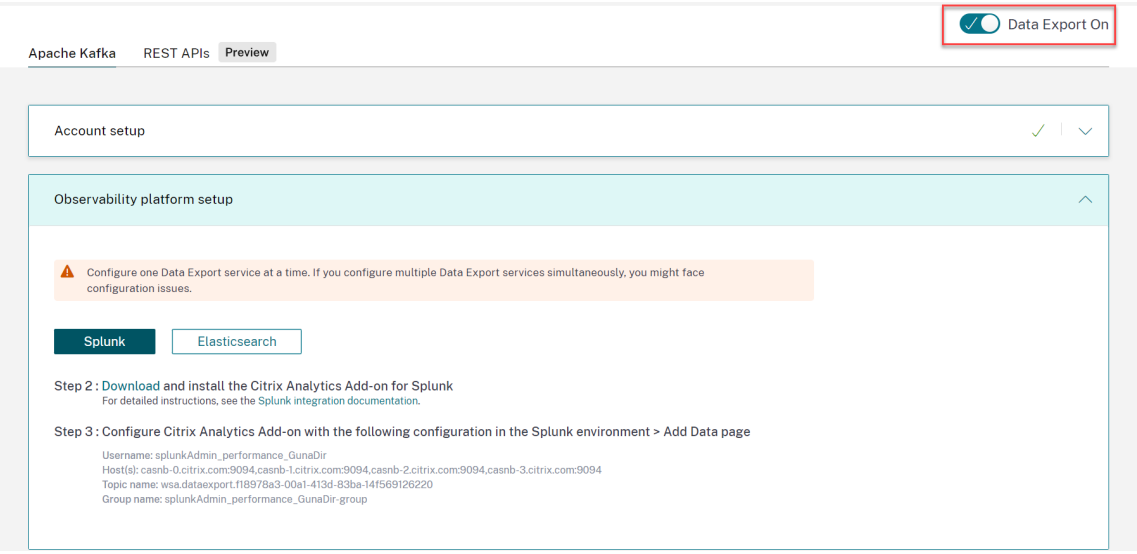
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Turn on or off data transmission

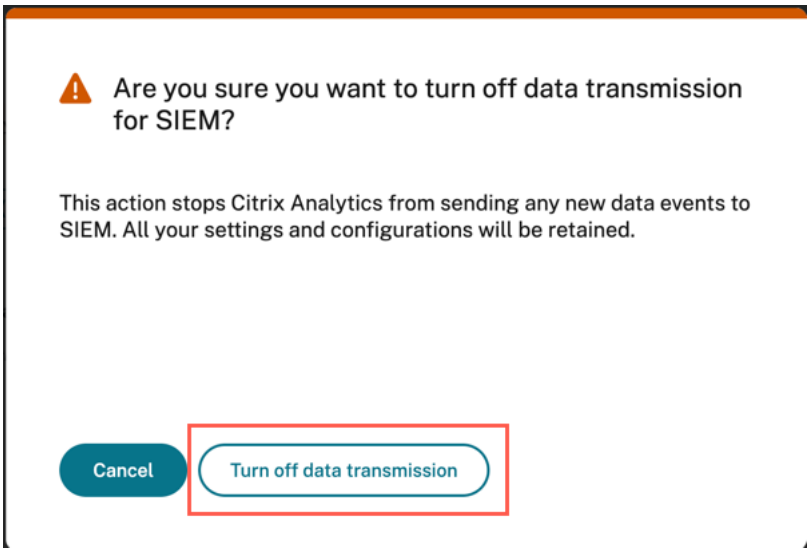
After Citrix Analytics for Performance prepares the configuration file, data transmission is turned on for Elasticsearch.

To stop transmitting data from Citrix Analytics for Performance:

1. Go to **Settings** > **Data Exports**.
2. Turn off the toggle button to disable the data transmission. By default, the **data transmission** is always enabled.



3. A warning window appears for your confirmation. Click **Turn off data transmission** to stop the transmission activity.



To enable data transmission again, turn on the toggle button.

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

Grafana integration

September 1, 2025

> **Note:**
>
> Contact CAS-PM-Ext@cloud.com to request assistance for the Grafana integration, exporting data to Grafana, or provide feedback.

You can integrate Citrix Analytics for Performance™ with Grafana by using the `Promtail` agent. This integration enables you to export and correlate the session and infrastructure data from your Citrix IT environment to Grafana. Also, get deeper insights into your organization's security posture.

For more information about the following, see Data Export:

- Benefits of the integration
- The type of processed data that is sent to your Observability platform

Prerequisites

- Turn on data processing for at least one data source. It helps Citrix Analytics for Performance to begin the Grafana integration process.
- Ensure that the following endpoint is in the allow list in your network.

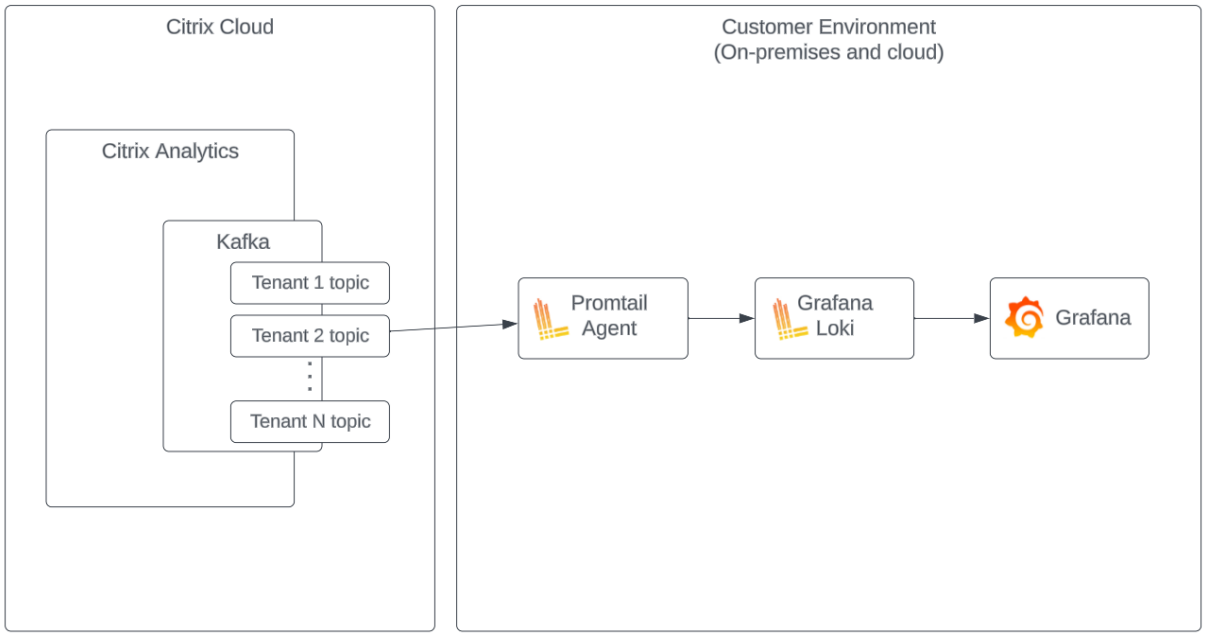
Endpoint	United States region	European Union region	Asia Pacific South region

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

Integrate with Grafana

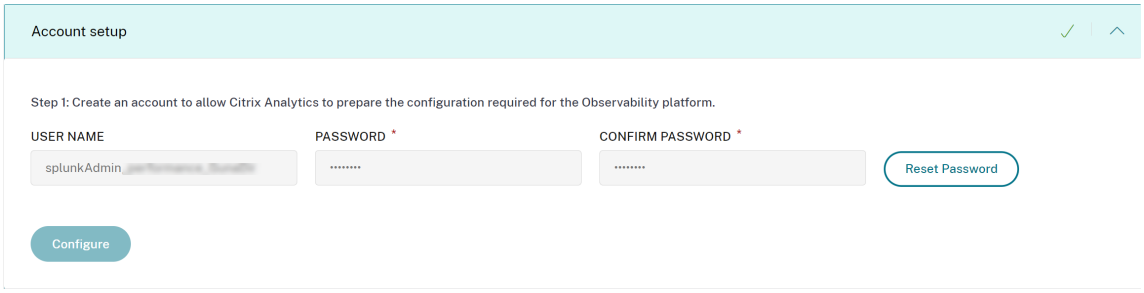
The following architecture diagram explains how data flows from Citrix Analytics for Performance to the Grafana observability platform:

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

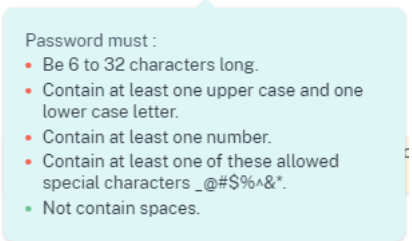


Setup Data Export account

1. Go to **Settings** > **Data Exports**.
2. On the **Account set up** section, create an account by specifying the user name and a password. This account is used in the `Promtail` configuration file, which is required for the integration.



3. Ensure that the password meets the following conditions:



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

Promtail configuration

The Promtail is an agent which ships the contents of local logs to a private Grafana Loki instance or Grafana Cloud. You can install the Promtail Agent using Docker, Helm, apt, or even manually.

Promtail is configured in a YAML file, usually referred to as config.yaml. This YAML file contains information on the Promtail server, where positions are stored, and how to scrape logs from files.

The following is a sample Promtail scrape configuration for consuming records from the Citrix Analytics for Performance:

```
scrape_configs:
- job_name: kafka
  kafka:
    brokers:
      - [Citrix Analytics Kafka broker1]
      - [Citrix Analytics Kafka broker2]
      ...
    topics:
      - [Citrix Analytics for Performance Kafka topic]
    group_id: [Citrix Analytics Kafka group ID]
    authentication:
      type: sasl
      sasl_config:
        mechanism: SCRAM-SHA-256
        user: [Citrix Analytics Kafka account username]
        password: [Citrix Analytics Kafka account password]
        ca_file: [Path to the Citrix Analytics certificate file (.pem)]
        use_tls: true
        insecure_skip_verify: true
    labels:
      job: kafka_casp
  relabel_configs:
      - action: replace
        source_labels:
          - __meta_kafka_topic
        target_label: topic
  pipeline_stages:
  - match:
      selector: '{
 job = "kafka_casp" }
  |= "sessionKey"'
      stages:
      - json:
          expressions:
            eventType: eventType
            siteName: siteName
            deliveryGroupName: deliveryGroupName
            protocol: protocol
            timestamp: timestamp
      - timestamp:
```

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

```
41            source: timestamp
42            format: 2006-01-02T15:04:05Z
43        - labels:
44            eventType:
45            siteName:
46            deliveryGroupName:
47            protocol:
48    - match:
49        selector: '{
50   job = "kafka_casp" }
51    != "sessionKey"'
52        stages:
53        - json:
54            expressions:
55              eventType: eventType
56              siteName: siteName
57              deliveryGroupName: deliveryGroupName
58              machineName: machineName
59              timestamp: timestamp
60        - timestamp:
61            source: timestamp
62            format: 2006-01-02 15:04:05
63        - labels:
64            eventType:
65            siteName:
66            deliveryGroupName:
67            machineName:
```

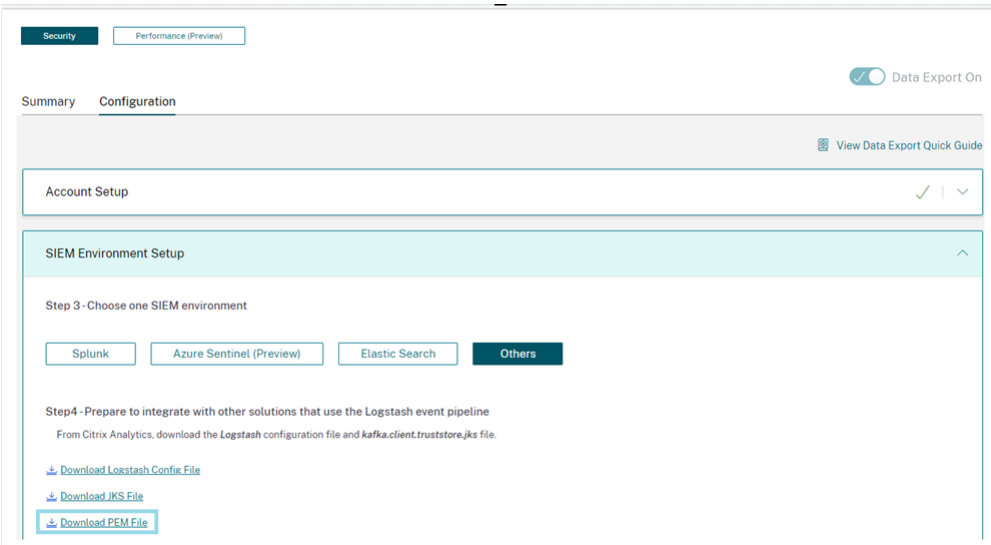
Based on the preceding configuration, `Promtail` connects to the Citrix Analytics brokers and consumes the Citrix Analytics for Performance records. TThe consumed Kafka topic includes Session and Machine records.

The `Promtail` separates the Session and Machine details using the `eventType` label, but also adds labels like the `siteName` and the `deliveryGroupName`. The event **timestamp** field is parsed and overrides the final time value of the logs stored in `Loki`.

You can download the certificate file referenced in the preceding configuration using the following steps:

1. Go to **Citrix Analytics** > **Settings** > **Data Exports** > **Security**.
2. Click the **SIEM Environment Setup** pane and select the *Others* option.
3. Download the PEM file and store it in the system that hosts the `Promtail` agent.

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



Grafana dashboard sample

You can import the sample Grafana dashboard provided by Citrix which includes:

- Metrics
- Time charts
- Other useful visualizations of session and infrastructure telemetry.

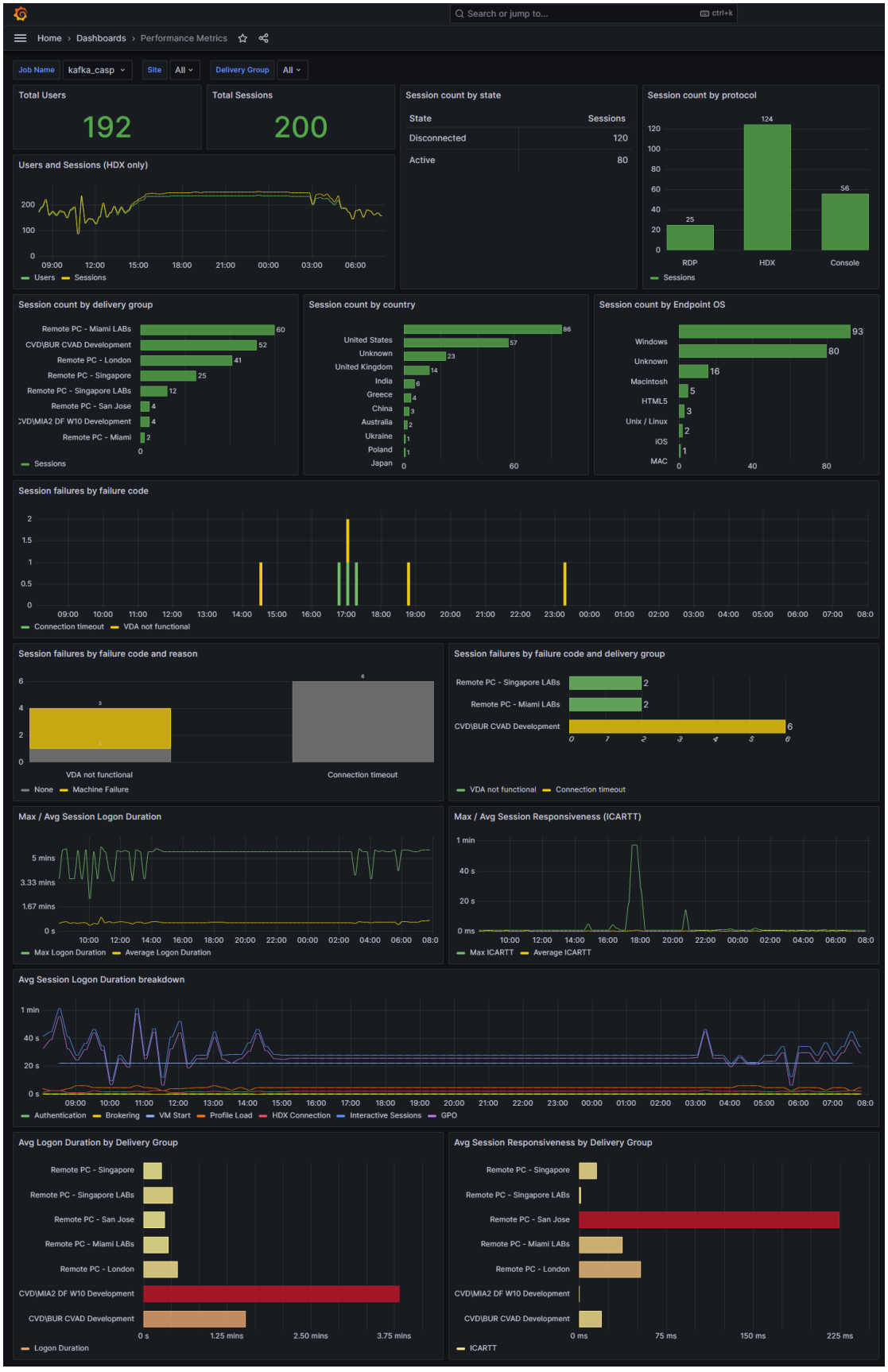
You can download the dashboard definitions (JSON files) from the Citrix Analytics downloads page.

You can import the dashboard files into your Grafana instance, either to a Grafana cloud or to an enterprise account.

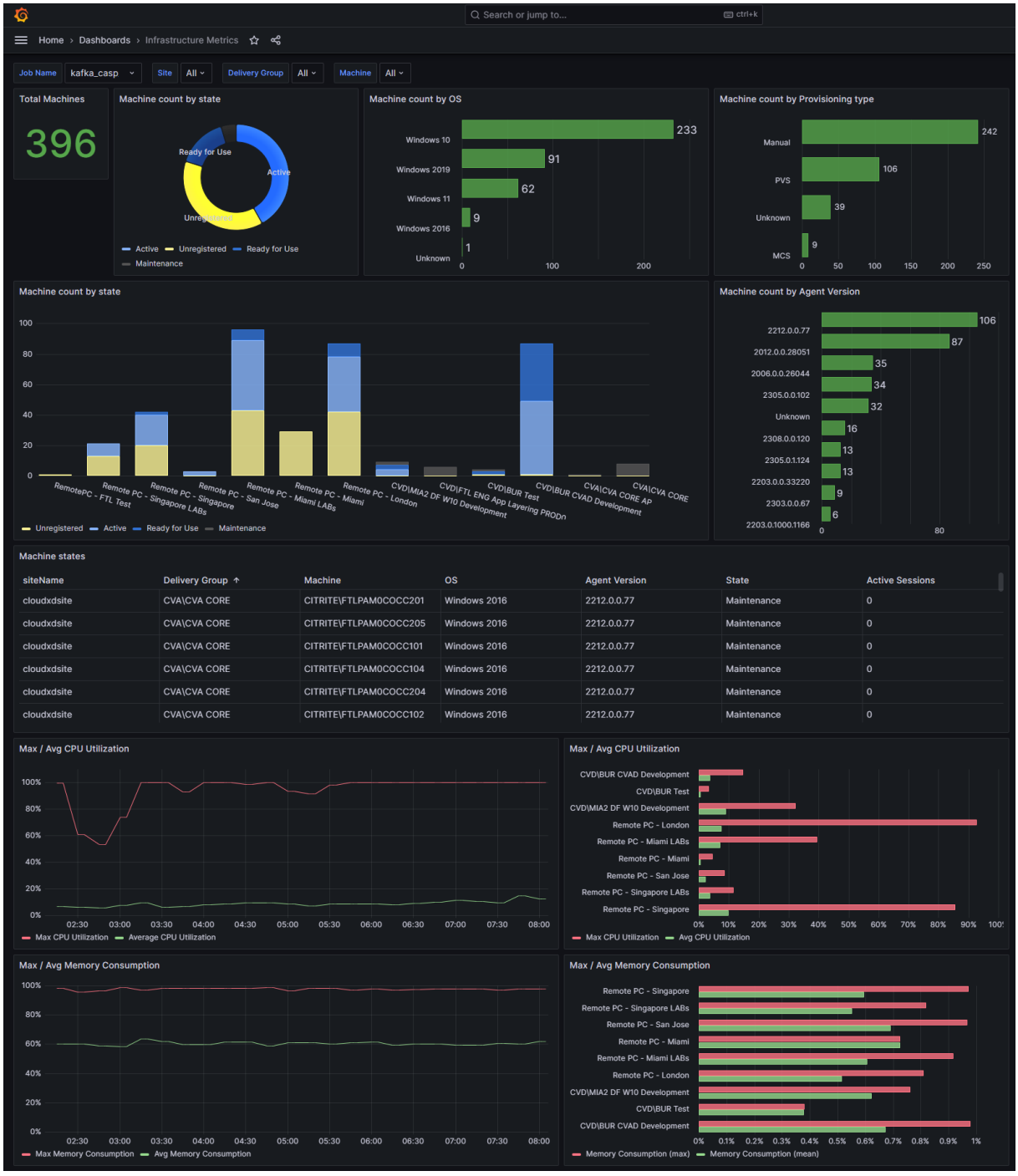
Before importing the dashboard, make sure that you have properly configured your `Loki` data source in Grafana. During the dashboard importing, you're prompted to select the `Loki` data source. After the dashboard is imported, you can view the dashboards on Grafana.

Following are the sample dashboards:

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



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



Data Structure of the Sessions Events

September 11, 2025

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

Sessions Dimensions Data Source

Session Meta Data	Type	Nullable	Description	Values
sessionKey	GUID	No	Identifier for a virtual app or desktop session.	
userId	String	No	User AD identifier for a virtual app or desktop session.	
userName	String	No	Name of the user who has launched a virtual app or desktop session.	
deliveryGroupId	GUID	No	Delivery Group Identifier	
deliveryGroupName	String	No	Delivery Group Name	
siteId	GUID	No	Citrix Virtual Apps and Desktops™ Site Identifier	
siteName	String	No	Citrix Virtual Apps and Desktops Site Name	
machineId	GUID	No	Machine Identifier of the machine on which the session is launched.	
machineSid	GUID	No	Machine AD Identifier of the machine on which the session is launched.	
machineName	String	No	The name of the machine on which the session is launched.	

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

Session Meta Data	Type	Nullable	Description	Values
sessionLaunchStatus	String	No	Launch status of the session	0 (Successful Launch), 1(Session Failed), 2(User Terminated)
sessionStartTime	Timestamp	No	Time when the session was launched	The value format is “yyyy-MM-ddTHH:mm:ss”
protocol	String	Yes	The protocol used to launch the session	HDX™, RDP, Console
sessionType	Integer	Yes	Session Type	The value mapping is: 0: Desktop, 1: Application
sessionEndTime	Timestamp	Yes	Time when the session ended	The value format is “yyyy-MM-ddTHH:mm:ss
stateChangedTime	Timestamp	Yes	The time at which the session state changed	The value format is “yyyy-MM-ddTHH:mm:ss
sessionState	String	No	Session life cycle state	The value mapping is: 0: Unknown, 1: Connected, 2: Disconnected, 3: Terminated, 4: PreparingSession, 5: Active, 6: Reconnecting, 7: NonBrokeredSession, 8: Other, and 9: Pending
sessionLaunchType	String	No	Session Launch type	ICA®, ConnectionLease

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

Session Meta Data	Type	Nullable	Description	Values
endpointOS	String	Yes	Citrix Workspace™ app - OS Type	The possible values include, for example: Windows, Unix or Linux, HTML5, Macintosh, ThinOS, iOS, Chrome, and Android. However, the OS type can include more options.
endpointReceiverVersion	String	No	Citrix Workspace app Version	
endpointLocationContinent	String	No	Continent from which the session was launched.	
endpointLocationCountry	String	No	The country from which the session was launched.	
endpointLocationCity	String	No	The city from which the session was launched.	
endpointLocationLatitude	String	No	The latitude from which the session was launched.	
endpointLocationLongitude	String	No	The longitude from which the session was launched.	
endpointLocationTimezone	String	No	Timezone of the place where the session was launched.	
isp	String	Yes	ISP using which the session was launched.	

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

Session Meta Data	Type	Nullable	Description	Values
gatewayFQDN	String	Yes	Gateway FQDN through which the session was launched.	
vdaIP	String	Yes	IP of VDA on which the session was launched.	
connectionType	String	Yes	Type of connection established from the Citrix Workspace app	Internal, External
connectionViaAG	String	Yes		
networkInterfaceType	String	No	Network Interface Type of the endpoint device	Wi-Fi, Ethernet, and so on
failureReason	Integer	No	Failure Category in which error has occurred	0 - “None” 1 - “Client Connection Failure” 2 - “Machine Failure” 3 - “No Capacity Available” 4 - “No Licenses Available” 5 - “Configuration” 6 - “Communication Failure” 100 - “Blackhole VDA” 101 - “Zombie Session” 0 - “Unknown error”
failureCode	Integer	No	Specifies type of failure	

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

Session Meta Data	Type	Nullable	Description	Values
				1 - “No failure” 2 - “Session preparation failed” 3 - “Registration timeout” 4 - “Connection timeout” 5 - “License unavailable” 6 - “Ticketing failed” 7 - “Unknown failure” 8 - “General failure” 9 - “Resource in maintenance mode” 10 - “Application disabled” 11 - “Required feature not licensed” 12 - “VDA unavailable” 13 - “VDA is already in use” 14 - “Requested protocol not allowed” 15 - “Resource unavailable” 16 - “Active session reconnect disabled”

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

Session Meta Data	Type	Nullable	Description	Values
				17 - “Cannot find a session to reconnect” 18 - “VDA power-up failed” 19 - “Session refused” 20 - “Set configuration failed” 21 - “Total concurrent usage limit of app reached” 22 - “Per user usage limit of app reached” 23 - “VDA not contactable” 24 - “Per machine usage limit reached” 25 - “Per entitlement usage limit leached” 51 - “Endpoint to Machine Communication error” 52 - “Gateway to Machine Communication error” 100 - “VDA unavailable” 101 - “VDA not functional”

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

Session Meta Data	Type	Nullable	Description	Values
failureReasonString	String	Yes	FailureReasonString mapped to the string value of failureReason.	
failureCodeString	String	Yes	FailureCodeString mapped to the string value of failureCode.	
sessionScore	Integer	No	Session Experience score based on the performance factors	-1–100
userScore	Integer	No	User experience score calculated based on session experience and failure rate.	0 -100
icaRtt	Integer	No	Session Responsiveness (in milliseconds) which defines the average round-trip time of the ICA session in the interval of the last 15 minutes.	>= 0
icaRttScore	Integer	No	IcaRtt (Session Responsiveness) score is calculated based on the current IcaRtt value and deviation from the baseline threshold of that metric.	0–100

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

Session Meta Data	Type	Nullable	Description	Values
reconnects	Integer	No	The number of auto-reconnects that happened in the interval of the last 15 minutes.	`>= 0`
reconnectScore	Integer	No	reconnectScore(Session Resiliency) score is calculated based on the current number of auto-reconnects and deviation from the baseline threshold of that metric.	0–100
logonDuration	Decimal	No	Total log on duration for this session (total initialization time of the session) in seconds.	
brokeringDuration	Decimal	Yes	Total time taken by the Broker in initializing the session in seconds.	
vmStartDuration	Decimal	Yes	Total time taken in starting the VM during the logon process in seconds.	

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

Session Meta Data	Type	Nullable	Description	Values
hdxConnectionDuration	Decimal	Yes	Total time taken by HDX connection during the logon process in seconds.	
authenticationDuration	Decimal	Yes	Total time taken in authentication during the logon process in seconds.	
gpoDuration	Decimal	Yes	Total time taken in GPO processing during the logon process in seconds.	
logonScriptsDuration	Decimal	Yes	Total time taken in logon script processing during the logon process in seconds.	
profileLoadDuration	Decimal	Yes	Total time taken in profile load during the logon process in seconds.	
interactiveSessionsDuration	Decimal	Yes	Total time taken in initializing an interactive session including shell initialization time in seconds.	

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

Session Meta Data	Type	Nullable	Description	Values
logonDurationScore	Integer	No	The logonDuration score is calculated based on the current logonDuration value and deviation from the baseline threshold of that metric.	0–100
gpoScore	Integer	No	The GPO score is calculated based on the current GPO value and deviation from the baseline threshold of that metric.	0–100
profileLoadScore	Integer	No	profileLoad score is calculated based on the current profile-LoadDuration value and deviation from the baseline threshold of that metric.	0–100

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

Session Meta Data	Type	Nullable	Description	Values
interactiveSessionScore	Integer	No	The interactiveSession score is calculated based on the current interactiveSessionDuration value and deviation from the baseline threshold of that metric.	0–100
brokeringScore	Integer	No	Brokering score is calculated based on the current brokeringDuration value and deviation from the baseline threshold of that metric.	0–100
vmStartScore	Integer	No	The vmStart score is calculated based on the current vmStartDuration value and deviation from the baseline threshold of that metric.	0–100

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

Session Meta Data	Type	Nullable	Description	Values
hdxConnectionScore	Integer	No	The hdxConnection score is calculated based on the current hdxConnection-Duration value and deviation from the baseline threshold of that metric.	0–100
authenticationScore	Integer	No	authentication score is calculated based on the current authentication-Duration value and deviation from the baseline threshold of that metric.	0–100
logonScriptsScore	Integer	No	logonScripts score is calculated based on the current logonScriptsDura-tion value and deviation from the baseline threshold of that metric.	0–100
profileSize	Integer	Yes	Total profile size of a user.	> 0
totalFileCount	Integer	Yes	Total files in that profile.	> 0

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

Session Meta Data	Type	Nullable	Description	Values
largeFileCount	Integer	Yes	Total number of large files in that profile.	> 0
failureScore	Integer	No	Calculated based on the number of failures against the number of session launches in the interval of the last 15 minutes.	0–100
failureCount	Integer	No	Total failures that occurred in the interval of the last 15 minutes.	>= 0
launchAttempts	Integer	No	Total launches attempted in the interval of the last 15 minutes.	>=0
machineFailureCount	Integer	No	Total count of machine failures.	>=0
clientConnectionFailureCount	Integer	No	Total count of client connection failures.	>=0
capacityFailureCount	Integer	No	Total count of capacity failures.	>=0
configurationFailureCount	Integer	No	Total count of configuration failures.	No
licenseFailureCount	Integer	No	Total count of license failures.	>=0
communicationFailureCount	Integer	No	Total count of communication failures.	>=0

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

Session Meta Data	Type	Nullable	Description	Values
inputBandwidthAvailable	Integer	Yes	Average Input Bandwidth Consumed by ICA Session in the last 15 minutes.	>=0
inputBandwidthConsumed	Integer	Yes	Average Input Bandwidth Consumed by ICA Session in the last 15 minutes.	>=0
outputBandwidthAvailable	Integer	Yes	Average Output Bandwidth Available in the last 15 minutes.	>=0
outputBandwidthUsed	Integer	Yes	Average Output Bandwidth Used in the last 15 minutes.	>=0
networkLatency	Integer	Yes	Average Network latency of the ICA Session in the last 15 minutes.	>=0
endpointLinkSpeed	Integer	Yes	Link speed of the endpoint device network interface like Wi-Fi, Ethernet	>=0
endpointSignalStrength	Integer	Yes	Signal Strength of the endpoint device.	>=0
avgEndpointThroughputBytesReceived	Integer	Yes	Total bytes received on the network interface.	>=0
avgEndpointThroughputBytesSent	Integer	Yes	Total bytes sent on the network interface.	>=0

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

Session Meta Data	Type	Nullable	Description	Values
wanLatency	Integer	Yes	This subfactor is the latency measured from the virtual machine to the Gateway. A high WAN Latency indicates sluggishness in the endpoint machine network. WAN latency increases when the user is geographically farther from the Gateway.	`>=0`
dcLatency	Integer	Yes	This subfactor is the latency measured from the Citrix Gateway to the server (VDA). A high Data Center Latency indicates delays because of a slow server network. This metric is available only when an on-premises gateway is onboarded to CAS.	`>=0`

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

Session Meta Data	Type	Nullable	Description	Values
hostDelay	Integer	Yes	This subfactor measures the Server OS induced delay. A high ICA RTT with low Data Center and WAN latencies, and a high Host Latency indicates an application error on the host server.	>=0
wanLatencyScore	Integer	No	WAN Latency Score is calculated based on wanLatency value and deviation from the baseline threshold value of the same metric.	0–100
dcLatencyScore	Integer	No	The DC Latency Score is calculated based on dcLatency value and deviation from the baseline threshold value of the same metric.	0–100

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

Session Meta Data	Type	Nullable	Description	Values
hostDelayScore	Integer	No	Host Delay Score is calculated based on the host delay value and deviation from the baseline threshold value of the same metric.	0–100

Data Structure of the Machines Events

September 11, 2025

Machine Dimensions data source

Machine Meta Data	Type	Nullable	Description	Value
machineId	GUID	Yes	Machine identifier.	
machineSid	GUID	No	Machine AD identifier.	
machineName	String	No	User defined machine name.	
machineIP	String	Yes	IP Address of the machine.	
operatingSystem	String	No	Operating system of the machine.	
deliveryGroupId	GUID	No	Delivery group identifier.	
deliveryGroupName	String	No	Delivery group name.	

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

Machine Meta Data	Type	Nullable	Description	Value
siteId	GUID	No	Citrix Virtual Apps and Desktops™ Site Identifier.	
siteName	String	No	Citrix Virtual Apps and Desktops Site Name	
machineProvisioningType	Integer	No	Describes how the machine was provisioned	0: Unknown, 1: MCS - Machine provisioned by Machine Creation Services™ (machine must be a VM), 2: PVS - Machine provisioned by Provisioning Services (might be physical, blade, VM), 3: Manual - No automated provisioning
hypervisorName	String	No	Name of hypervisor	
hypervisorId	GUID	No	Unique identifier of Hypervisor	
catalogName	String	No	Name of Catalog Broker name	
catalogId	GUID	No	Unique identifier for the Catalog	
agentVersion	String	No	VDA version installed on the machine	
hostedMachineName	String	Yes		
hostingServerName	String	Yes		

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

Machine Meta Data	Type	Nullable	Description	Value
sessionSupport	String	No	Specifies the session support of the machines in the catalog	1: Single-session, 2: Multi-session
status	Integer	No	Last known status of the machine in the last 15 minutes	1: Unregistered, 2: Registered, 3: Under Maintenance, 4: Failed, 5: Powered off
statusChangeTime	Timestamp	No	Time when machine status has changed in the last 15 minutes	The value format is "yyyy-MM-ddTHH:mm:ss.SSSZ"
machineActualStatus	Integer	No	Calculated machine status using multiple state transitions that happened in the last 15 minutes. If the machine went from registered to unregistered state, machineActualStatus is unregistered	1: Unregistered, 2: Registered, 3: Failed
machineFailureReason	String	Yes	Failure reason why machine went into failed state	Fault unknown No fault (healthy machine) The last power-on operation for the machine failed

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

Machine Meta Data	Type	Nullable	Description	Value
				The machine does not seem to have booted following power on (VM tools did not transition to running) The machine has failed to register within the expected period, or its registration has been rejected The machine is reporting itself at maximum capacity
machineFailureType	String	Yes		Values can be any of: “Unknown”, “None”, “FailedToStart”, “StuckOnBoot”, “Unregistered”, “MaxCapacity
machinePowerState	Integer	No	Represents machine power state	0: Unknown 1: Unavailable 2: Off 3: On 4: Suspended 5: TurningOn 6: TurningOff 7: Suspending 8: Resuming 9: Unmanaged

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

Machine Meta Data	Type	Nullable	Description	Value
				10: NotSupported
unregisteredStartTime	Timestamp	Yes	Time when the machine went into the unregistered state	The value format is “yyyy-MM-ddTHH:mm:ss”
unregisteredEndTime	Timestamp	Yes	Time when the machine came out from the unregistered state	The value format is “yyyy-MM-ddTHH:mm:ss”
isMaintenanceMode	Boolean	Yes	A boolean flag specifies if the machine is in Maintenance mode or not	0: true, 1: false
isUnregistered	Boolean	Yes	A boolean flag specifies if the machine is in an unregistered state or not	0: true, 1: false
machineFailureTime	Timestamp	Yes	Time when a machine went into a failed state	Any date-time value
cpuSpikesCount	Integer	Yes	Represents the number of times CPU utilization crossed the CPU threshold of 80% and sustained for 5 minutes or more in an interval of the last 15 minutes.	
usedMemory	Decimal	No	Used memory (bytes)	

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

Machine Meta Data	Type	Nullable	Description	Value
totalMemory	Integer	No	Total available memory (bytes)	
percentCpu	Integer	No	Average percentage CPU used on a machine	
ramSpikeCount	Integer	Yes	Represents the number of times memory consumption crossed the memory threshold of 80%. Also, sustained for 5 minutes or more in the interval of the last 15 minutes.	
sessionCount	Integer	Yes	Total number of sessions (successful + failed) launched on the machine in the last 15 minutes.	
downTime	Integer	Yes	The total downtime of the machine calculated in seconds.	
consecutiveMachineFailures	Integer	Yes	Consecutive failures on a machine known in an interval of the last 15 minutes.	

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

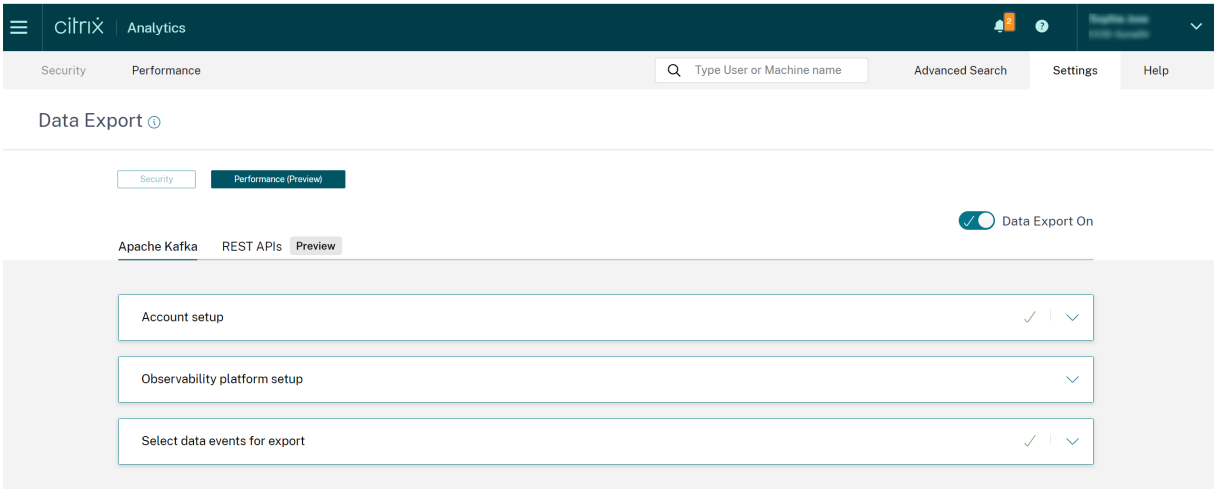
Machine Meta Data	Type	Nullable	Description	Value
activeSessionCount	Integer	Yes	The number of active sessions in an interval of the last 15 minutes.	
successfulSessionCount	Integer	No	The number of successful sessions launched in an interval of the last 15 minutes.	
machineFailureOccurred	Integer	Yes	Session Failures that occurred on the machine in an interval of the last 15 minutes.	
unRegistrationCount	Integer	No	The number of times the machine went into the registered State in an interval of the last 15 minutes.	

Data export via REST APIs (Preview)

September 1, 2025

Citrix Analytics for Performance™ is now integrated with the Power BI observability. You can use the **Data Export** feature to export performance data and events from Citrix Analytics for Performance to Power BI using the REST APIs.

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



For more information, see the following articles:

- Citrix Analytics ODATA API
- Data export to Power BI with incremental refresh for Citrix Performance Analytics

Citrix Analytics ODATA API

September 11, 2025

Overview

CAS ODATA v4 REST API helps you to easily fetch the aggregated data. Currently, we are supporting user to fetch session data from CAS performance data source.

This article provides a guidance about how to use the APIs.

API specifications

Authentication

The implementation uses Citrix Cloud™ bearer token to authenticate.

References:

Citrix Cloud client ID and Citrix Cloud client secret

The following is sample request to get the token.

Request sample:

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

```
    POST https://api.cloud.com/cctrustoauth2/{
customerid }
/tokens/clients
    Accept: application/json
    Content-Type: application/x-www-form-urlencoded
    Body: grant_type=client_credentials&client_id={
client_id }
&client_secret={
client_secret }
```

Response sample:

```
HTTP/1.1 200 OK
Content-Type: application/json
...
{

"token_type": "bearer",
"access_token": "ey1..",
"expires_in": "3600"
 }
```

> **Note:**
>
> The expiration period of the bearer token is 1 hour. Regenerate it if you need to do the query after one hour.

Endpoints

Global: `https://api.cloud.com/casodata`

Sample:

`https://api.cloud.com/casodata/sessions?year=2023&month=04&day=14` will fetch the aggregated sessions data for date 2023/04/14 (UTC).

Service path

This section includes information on service path and entity names such as sessions, machines, and users. For example, see the following sample service path:

```
/sessions?year=2023&month=04&day=14
```

The parameters year, month, and day are mandatory and added in UTC format.

The data of a specified hour is also supported, the path is as follows:

```
/sessions?year=2023&month=04&day=14&hour=10 (Fetch the data of
    2023/04/14 10:00)
```

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

HTTP headers

Key	Sample	Value	Mandatory
Authorization	CwsAuth bearer=		Yes
Citrix-CustomerId			Yes
Content-Type	application/json		Yes
Citrix-TransactionId			No
Accept-Encoding	gzip		No

System operators

CAS ODATA API supports the following basic odata system options:

System option	Sample
$select	https:///casodata/sessions?year=2023&month=04&day=14&$
$orderby	https:///casodata/sessions?year=2023&month=04&day=14&$ desc
$top	https:///casodata/sessions?year=2023&month=04&day=14&$
$top&$skip	https:///casodata/sessions?year=2023&month=04&day=14&$
$count	https:///casodata/sessions?year=2023&month=04&day=14&$
$filters	https:///casodata/sessions?year=2023&month=04&day=14&$ ne 20

> **Note:**
>
> Don't add any space in the value of $select option.

$filter operators and functions CAS ODATA API supports the following odata logical operators and string functions for $filter option:

Category	Operators	Samples
Logical operators	eq/ne/gt/lt/le/ge	https:///casodata/sessions?year=2023&mon ge 20

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

Category	Operators	Samples
	not	https:///casodata/sessions?year=2023&mon eq null)
	and/or	https:///casodata/sessions?year=2023&mon eq ‘5’and (sessionScore le 20 or logonDuration gt 19.914)
	in	https:///casodata/sessions?year=2023&mon in (‘5’,’3’)
	not in	https:///casodata/sessions?year=2023&mon (sessionState in (‘5’,’3’))
String functions	contains	https:///casodata/sessions?year=2023&mon PRD’)
	startswith	https:///casodata/sessions?year=2023&mon endswith(deliveryGroupName,’ CVAD Development’)
	endswith	https:///casodata/sessions?year=2023&mon 09c3268e’)

Entities and data attributes

The following three CAS performance entities are supported:

- Users
- Sessions
- Machines

Sample use cases

Get the metadata and pick some columns from them to do the query

1. Requesting the metadata

   Request sample:

```
curl --location 'https://api.cloud.com/casodata/$metadata' \
--header 'Authorization: CwsAuth bearer=eyJhbGciOiJSUzI1NiIsInR5
    .....' \
--header 'Citrix-CustomerId: qt64gkrzji7h' \
--header 'Content-Type: application/json'
```

   Response sample:

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

```
<?xml version="1.0" encoding="UTF-8"?>
<edmx:Edmx Version="4.0" xmlns:edmx="http://docs.oasis-open.org/odata/ns/edmx">
<edmx:DataServices>
<Schema xmlns="http://docs.oasis-open.org/odata/ns/edm" Namespace="cas.odata.v1">
<EntityType Name="session">
<Property Name="timestamp" Type="Edm.String"></Property>
<Property Name="sessionKey" Type="Edm.String"></Property>
<Property Name="sessionScore" Type="Edm.Double"></Property>
<Property Name="sessionState" Type="Edm.String"></Property>
...
<Property Name="sessionLaunchStatus" Type="Edm.Int32"></Property>
<Property Name="sessionLaunchStatusCustom" Type="Edm.String"></Property>
</EntityType>
<EntityContainer Name="Container">
<EntitySet Name="sessions" EntityType="cas.odata.v1.session" IncludeInServiceDocument="false"></EntitySet>
</EntityContainer>
</Schema>
</edmx:DataServices>
</edmx:Edmx>
```

2. Pick columns `sessionKey`, `sessionScore`, and `sessionState` to do the query

Request sample:

```
curl --location 'https://api.cloud.com/casodata/sessions?year=2023&month=04&day=14&%24select=sessionKey%2CsessionScore%2CsessionState' \
--header 'Authorization: CwsAuth bearer=eyJhbGciOiJSUzI1NiIsInR5.....' \
--header 'Citrix-CustomerId: qt64gkrzji7h' \
--header 'Content-Type: application/json'
```

Response sample:

```
{

"@odata.context": "$metadata#sessions(sessionKey,sessionScore,sessionState)/$entity",
"value": [
{

"sessionKey": "009e7f0f-5707-4083-934f-24d8ad5e91f8",
"sessionScore": -1.0,
"sessionState": "2"
 }
 ,
...
{

```

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

```
"sessionKey": "ff0504e3-0867-414a-b0b2-beb73f06fdad",
"sessionScore": 0.0,
"sessionState": "5"
 }

]
 }
```


Fetch all the data of a specified day with pagination

The default limitation of the query is 1000 rows.

User is able to set the value of `$top` option to limit the result rows in the query. In this scenario, the next page link is provided at the bottom of query response.

Request sample:

```
curl --location 'https://api.cloud.com/casodata/sessions?year=2023&
   month=04&day=14&%24top=100' \
--header 'Authorization: CwsAuth bearer=eyJhbGciOiJSUzI1NiIsInR5.....'
   \
--header 'Citrix-CustomerId: qt64gkrzji7h' \
--header 'Content-Type: application/json'
```

Response sample:


```
{

"@odata.context": "$metadata#sessions/$entity",
"value": [
{

"timestamp": "2023-03-28T00:00:00.000Z",
"sessionKey": "009e7f0f-5707-4083-934f-24d8ad5e91f8",
"sessionScore": 79.0,
"sessionState": "2",
"sessionType": "0",
"userName": "81
   d0260b529c11fbb05c8dfabb3d312182e6af9deecfc6c036768df2ed3c3a39",
"sessionStartTime": "2023-03-28T17:38:38.000Z",
"machineName": "253
   f6a031c9b65cbb7bcc3f137b9878fe0effef010757aec54420776a0d2dd71",
"deliveryGroupName": "CVD\\BUR CVAD Development",
"logonDuration": 18.69,
"brokeringDuration": 0.0,
"vmStartDuration": 0.0,
"hdxConnectionDuration": 0.0,
"authenticationDuration": 0.0,
"gpoDuration": 0.0,
"logonScriptsDuration": 0.0,
```


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

```
"profileLoadDuration": 0.0,
"interactiveSessionsDuration": 0.0,
"siteName": "cloudxdsite",
"icaRtt": 125.38,
"reconnects": 0.0,
"wanLatency": 0,
"hostDelay": 0,
"dcLatency": 0,
"endpointLocationCity": null,
"endpointReceiverVersion": "21.6.0.47",
"endpointOS": "Windows",
"endpointLocationCountry": null,
"endpointLinkSpeed": -1.0,
"endpointName": "64368231
   b5d925e40d67449640ca110e9658f63eef37d2579b09b975cc7f7e88",
"endpointIP": "850
   a4b2abc159a2f7d44dac564bda06afad0c558a070a2681f5cc0e1aa81991c",
"vdaIP": null,
"gatewayFQDN": null,
"connectionType": "External",
"connectorName": null,
"connectorGatewayLatency": 0.0,
"networkInterfaceType": null,
"isp": null,
"sessionLaunchType": "ICA",
"throughputBytesReceived": -1.0,
"throughputBytesSent": -1.0,
"inputBandwidthConsumed": -1.0,
"outputBandwidthAvailable": -1.0,
"outputBandwidthUsed": -1.0,
"networkLatency": -1.0,
"outputBandwidthUtilization": -1.0,
"siteId": "090e20c8-c852-4a92-9b3f-dfb8d8b2ab61",
"sessionLaunchStatus": 0,
"sessionLaunchStatusCustom": "Succeeded"
 }
 ,
...
{

"timestamp": "2023-04-14T00:00:00.000Z",
"sessionKey": "ff0504e3-0867-414a-b0b2-beb73f06fdad",
"sessionScore": 0.0,
"sessionState": "5",
"sessionType": "0",
"userName": "
   aed8a56c38d5d2824d8699a48cdd1b19eb3b16f135c8d61bf2cd6acd465aa998",
"sessionStartTime": "2023-03-09T21:39:51.000Z",
"machineName": "5603
   b4dcad97424b6329caccc9cc6ad949b764bbc0015bc6e2a2b4938e4be954",
"deliveryGroupName": "Remote PC - Miami LABs",
"logonDuration": 0.0,
"brokeringDuration": 0.0,
```


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

```
"vmStartDuration": 0.0,
"hdxConnectionDuration": 0.0,
"authenticationDuration": 0.0,
"gpoDuration": 0.0,
"logonScriptsDuration": 0.0,
"profileLoadDuration": 0.0,
"interactiveSessionsDuration": 0.0,
"siteName": "cloudxdsite",
"icaRtt": 0.0,
"reconnects": 0.0,
"wanLatency": 0,
"hostDelay": 0,
"dcLatency": 0,
"endpointLocationCity": null,
"endpointReceiverVersion": null,
"endpointOS": "Windows 10",
"endpointLocationCountry": null,
"endpointLinkSpeed": -1.0,
"endpointName": "Precision 5550",
"endpointIP": "
   e74dbbbd20d20f971c0254c6680aad800ad3932c4740544b39a42bb422424272",
"vdaIP": null,
"gatewayFQDN": null,
"connectionType": "External",
"connectorName": null,
"connectorGatewayLatency": 0.0,
"networkInterfaceType": null,
"isp": null,
"sessionLaunchType": "ICA",
"throughputBytesReceived": -1.0,
"throughputBytesSent": -1.0,
"inputBandwidthConsumed": -1.0,
"outputBandwidthAvailable": -1.0,
"outputBandwidthUsed": -1.0,
"networkLatency": -1.0,
"outputBandwidthUtilization": -1.0,
"siteId": "090e20c8-c852-4a92-9b3f-dfb8d8b2ab61",
"sessionLaunchStatus": 0,
"sessionLaunchStatusCustom": "Succeeded"
 }

],
"@odata.nextLink": "https://api.cloud.com/casodata/sessions?year=2023&
   month=04&day=14&%
24skip=100&%24top=100"
 }
```


Get all the data of a certain session (filter the data with sessionkey)

Request sample:

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

```
curl --location 'https://api.cloud.com/casodata/sessions?year=2023&
   month=04&day=14&%24filter=sessionKey%20eq%20%
27009e7f0f-5707-4083-934f-24d8ad5e91f8%27' \
--header 'Authorization: CwsAuth bearer=eyJhbGciOiJSUzI1NiIsInR5.....'
   \
--header 'Citrix-CustomerId: qt64gkrzji7h' \
--header 'Content-Type: application/json'
```

Response sample:


```
{

"@odata.context": "$metadata#sessions/$entity",
"value": [
{

"timestamp": "2023-04-14T00:00:00.000Z",
"sessionKey": "009e7f0f-5707-4083-934f-24d8ad5e91f8",
"sessionScore": -1.0,
"sessionState": "2",
"sessionType": "0",
"userName": "81
   d0260b529c11fbb05c8dfabb3d312182e6af9deecfc6c036768df2ed3c3a39",
"sessionStartTime": "2023-04-05T17:32:45.000Z",
"machineName": "253
   f6a031c9b65cbb7bcc3f137b9878fe0effef010757aec54420776a0d2dd71",
"deliveryGroupName": "CVD\\BUR CVAD Development",
"logonDuration": 21.2,
"brokeringDuration": 0.0,
"vmStartDuration": 0.0,
"hdxConnectionDuration": 0.0,
"authenticationDuration": 0.0,
"gpoDuration": 0.0,
"logonScriptsDuration": 0.0,
"profileLoadDuration": 0.0,
"interactiveSessionsDuration": 0.0,
"siteName": "cloudxdsite",
"icaRtt": 0.0,
"reconnects": 0.0,
"wanLatency": 0,
"hostDelay": 0,
"dcLatency": 0,
"endpointLocationCity": null,
"endpointReceiverVersion": "21.6.0.47",
"endpointOS": "Windows",
"endpointLocationCountry": null,
"endpointLinkSpeed": -1.0,
"endpointName": "64368231
   b5d925e40d67449640ca110e9658f63eef37d2579b09b975cc7f7e88",
"endpointIP": "8
   dbacd9197f4d3dc068fd44b4837828f8e10a19358b14e96d439cfc82042b70f",
"vdaIP": null,
"gatewayFQDN": null,
```


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

```
"connectionType": "External",
"connectorName": null,
"connectorGatewayLatency": 0.0,
"networkInterfaceType": null,
"isp": null,
"sessionLaunchType": "ICA",
"throughputBytesReceived": -1.0,
"throughputBytesSent": -1.0,
"inputBandwidthConsumed": -1.0,
"outputBandwidthAvailable": -1.0,
"outputBandwidthUsed": -1.0,
"networkLatency": -1.0,
"outputBandwidthUtilization": -1.0,
"siteId": "090e20c8-c852-4a92-9b3f-dfb8d8b2ab61",
"sessionLaunchStatus": 0,
"sessionLaunchStatusCustom": "Succeeded"
 }

]
 }
```


Count all the active sessions of a certain day

Request sample:

```
curl --location 'https://api.cloud.com/casodata/sessions?year=2023&
   month=04&day=14&%24count=true&%24filter=sessionState%
20eq%20%275%27' \
--header 'Authorization: CwsAuth bearer=eyJhbGciOiJSUzI1NiIsInR5.....'
   \
--header 'Citrix-CustomerId: qt64gkrzji7h' \
--header 'Content-Type: application/json'
```

Response sample:

207

Data source

The CAS self service search dashboard visulize and display the data to the customer admins and enable search functionality. The ODATA API uses the same data source and provide more flexibilities to customer admins to fetch and filter the data. For more information, see Tabular data.

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

Data Structure of the users events

September 1, 2025

Field	Type	Nullable	Description	Value
Timestamp	String	No	Time when an API is called.	
UserExperience	Double	No	The score of the user experience which is calculated based on user score.	0–100
UserName	String	No	Name of the user who has launched a virtual app or desktop session.	
TotalSessions	Integer	No	Total sessions of a user.	>=0
ExcellentSessions	Integer	No	Number of sessions with session score >= 70.	>=0
FairSessions	Integer	No	Number of sessions with session score >= 40 and session score < 70.	>=0
PoorSessions	Integer	No	Number of sessions with session score >= 1 and session score < 40.	>=0

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

Field	Type	Nullable	Description	Value
SessionLogonDuration	Double	No	Total log-on duration for this user (total initialization time of the user) in seconds.	`>0`
SessionResponsiveness	Double	No	Average round-trip time of ICA® session for this user in the last 15-minutes interval.	`>=0`
`WANLatency`	Double	Yes	This subfactor is the latency measured from the virtual machine to the Gateway. A high WAN Latency indicates sluggishness in the endpoint machine network. WAN latency increases when the user is geographically farther from the Gateway.	`>=0`

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

Field	Type	Nullable	Description	Value
HostDelay	Double	Yes	This subfactor measures the Server OS induced delay. A high ICA RTT with low Data Center and WAN latencies, and a high Host Latency indicates an application error on the host server.	>=0
DataCenterLatency	Double	Yes	This subfactor is the latency measured from the Citrix Gateway to the server (VDA). A high Data Center Latency indicates delays due to a slow server network. This metric is available only when an on-premises gateway is onboarded to CAS.	>=0
Brokering	Double	Yes	Average time taken by a Broker in initializing the session in seconds.	

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

Field	Type	Nullable	Description	Value
VMStart	Double	Yes	Average time taken in starting the VM during the logon process in seconds.	
HDXConnection	Double	Yes	Average time taken by HDX™ connection during the logon process in seconds.	
Authentication	Double	Yes	Average time taken in authentication during the logon process in seconds.	
GPOs	Double	Yes	Average time taken in GPO processing during the logon process in seconds.	
LogonScripts	Double	Yes	Average time taken in logon script processing during the logon process in seconds.	
ProfileLoad	Double	Yes	Average time taken in profile load during the logon process in seconds.	

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

Field	Type	Nullable	Description	Value
InteractiveSession	Double	Yes	Average time taken in initializing interactive session including shell initialization time in seconds.	
FailureCount	Integer	No	Total failures that occurred in the last 15 minutes.	`>=0`
LaunchAttemptsCount	Integer	No	Total launches attempted in the last 15 minutes.	`>=0`
SessionResiliency	Double	No	The number of auto-reconnects that happened in the last 15 minutes.	
EndpointCity	String	Yes	The city from which the session was launched.	
EndpointCountry	String	Yes	The country from which the session was launched.	
AverageProfileSize	Double	Yes	Average profile size of a user.	
ProfileSize	Double	Yes	Latest profile size of a user.	

Data Structure of the Sessions Events

September 1, 2025

Sessions Dimensions Data Source

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

Field	Type	Nullable	Description	Values
Timestamp	String	No	Time when an API is called.	
SessionKey	String	No	Identifier for a virtual app or desktop session.	
SessionExperience	Double	No	The score of the session experience which is calculated based on the session score.	
SessionStat	String	No	Session life cycle stat.	The value mapping is: 0: Unknown, 1: Connected, 2: Disconnected, 3: Terminated, 4: PreparingSession, 5: Active, 6: Reconnecting, 7: NonBrokeredSession, 8: Other, and 9: Pending
SessionType	String	No	Session Type	The value mapping is: 0: Desktop, 1: Application
UserName	String	No	Name of the user who has launched a virtual app or desktop session.	
SessionStartTime	String	No	Time when the session was launched.	The value format is “yyyy-MM-ddTHH:mm:ss”

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

Field	Type	Nullable	Description	Values
MachineName	String	No	The name of the machine on which the session is launched.	>=0
DeliveryGroupName	String	No	Name of the Delivery Group.	>=0
SessionLogonDuration	Double	No	Average log on duration for this session (total initialization time of the session) in seconds.	>=0
Brokering	Double	Yes	Average time taken by a Broker in initializing the session in seconds.	>=0
VMStart	Double	Yes	Average time taken in starting the VM during the logon process in seconds.	>=0
HDXConnection	Double	Yes	Average time taken by HDX™ connection during the logon process in seconds.	>=0
Authentication	Double	Yes	Average time taken in authentication during the logon process in seconds.	>=0

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

Field	Type	Nullable	Description	Values
GPOs	Double	Yes	Average time taken in GPO processing during the logon process in seconds.	
LogonScripts	Double	Yes	Average time taken in logon script processing during the logon process in seconds.	>=0
ProfileLoad	Double	Yes	Average time taken in profile load during the logon process in seconds.	>=0
InteractiveSessions	Double	Yes	Average time taken in initializing interactive session including shell initialization time in seconds.	>=0
SiteName	String	No	Citrix Virtual Apps and Desktops™ Site Name	
SessionResponsiveness	Double	No	Average round-trip time of ICA® session in the last 15-minutes interval.	>=0
SessionResiliency	Double	No	Total number of auto-reconnects.	

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

Field	Type	Nullable	Description	Values
WANLatency	Double	Yes	This subfactor is the average latency measured from the virtual machine to the Gateway. A high WAN Latency indicates sluggishness in the endpoint machine network. WAN latency increases when the user is geographically farther from the Gateway.	
HostDelay	Double	Yes	This subfactor measures the average Server OS induced delay. A high ICA RTT with low Data Center and WAN latencies, and a high Host Latency indicates an app error on the host server.	

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

Field	Type	Nullable	Description	Values
DataCenterLatency	Double	Yes	This subfactor is the average latency measured from the Citrix Gateway to the server (VDA). A high Data Center Latency indicates delays because of a slow server network. This metric is available only when an on-premises gateway is onboarded to CAS.	
EndpointCity	String	Yes	The city from which the session was launched.	
WorkspaceAppVersion	String	No	Citrix Workspace™ app version	
EndpointOS	String	Yes	Citrix Workspace app - OS Type	The possible values include, for example: Windows, Unix or Linux, HTML5, Macintosh, ThinOS, iOS, Chrome, and Android. However, the OS type can include more options.

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

Field	Type	Nullable	Description	Values
EndpointCountry	String	Yes	The country from which the session was launched.	
EndpointLinkSpeed	Double	Yes	Average Link speed of the endpoint device network interface like Wi-Fi, Ethernet	>=0
EndpointName	String	Yes	Name of Client where the session was launched.	
EndpointIP	String	Yes	IP of Client where the session was launched.	
MachineAddress	String	Yes	IP of VDA where the session was launched	
Gateway	String	Yes	Gateway FQDN through which the session was launched.	
ConnectionType	String	Yes	Type of connection established from the Citrix Workspace app.	Internal, External
Connector	String	Yes	Connector name of Gateway FQDN.	
GatewayConnectorLatency	Double	Yes	Average Gateway connector latency.	
NetworkInterfaceType	String	No	Network Interface Type of the endpoint device.	Wi-Fi, Ethernet, and so on

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

Field	Type	Nullable	Description	Values
ISP	String	Yes	ISP using which the session was launched	
LaunchType	String	No	Session Launch type	ICA, ConnectionLease
EndpointThroughputOutgoing	Double	Yes	Total bytes sent on the network interface.	
EndpointThroughputIncoming	Double	Yes	Total bytes received on the network interface.	>=0
InputBandwidthConsumed	Double	Yes	Average Input Bandwidth Consumed by ICA Session in the last 15 minutes.	>=0
OutputBandwidthAvailable	Double	Yes	Average Input Bandwidth Consumed by ICA Session in the last 15 minutes.	>=0
OutputBandwidthUsed	Double	Yes	Average Output Bandwidth Used in the last 15 minutes.	>=0
NetworkLatency	Double	Yes	Average Network latency of the ICA Session in the last 15 minutes.	>=0
OutputBandwidthUtilization	Double	Yes	Average Output Bandwidth Utilization percentage in the last 15 minutes.	>=0

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

Field	Type	Nullable	Description	Values
LaunchStatus	Integer	No	Launch status of the session.	0 (Successful Launch), 1(Session Failed), 2(User Terminated)

Data Structure of the Machines Events

September 11, 2025

Machine Meta Data	Type	Nullable	Description	Value
Timestamp	String	No	Time when an API is called.	
SiteId	String	No	Citrix Virtual Apps and Desktops™ Site identifier.	
SiteName	String	No	Citrix Virtual Apps and Desktops Site name.	
MachineName	String	No	User defined machine name	
DeliveryGroupName	String	No	Delivery group name	
MachineOS	String	No	Operating system	
LatestConsecutiveFailures	Integer	Yes	Consecutive failures on a machine known in the interval of the last 15 minutes.	

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

Machine Meta Data	Type	Nullable	Description	Value
Status	String	No	Last known status of the machine in the interval of the last 15 minutes.	1: Unregistered, 2: Registered, 3: Under Maintenance, 4: Failed, 5: Powered off
UnRegistrationCount	Integer	No	The number of times the machine went into registered State in the interval of the last 15 minutes.	>=0
SustainedCpuSpikes	Integer	Yes	Represents the number of times CPU utilization crossed the CPU threshold of 80%. Also, sustained for 5 minutes or more in the interval of the last 15 minutes.	>=0
SustainedMemorySpikes	Integer	Yes	Represents the number of times memory consumption crossed the memory threshold of 80%. Also, sustained for 5 minutes or more in the interval of the last 15 minutes.	>=0

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

Machine Meta Data	Type	Nullable	Description	Value
PeakConcurrentSessions	Integer	Yes	The total number of sessions (successful and failed) launched on the machine in the interval of the last 15 minutes.	>=0
SessionFailureRate	Double	Yes	Session failure rate on machine.	0–100
LoadIndicator	Double	No	Number of machines with machine score > 0.	>=0
DownTime	Double	Yes	Total downtime of the machine calculated in seconds.	
AvgMemoryConsumption	Double	No	Average used memory percentage on a machine.	0–100
PeakMemoryConsumption	Double	No	Total available memory percentage on a machine.	0–100
AvgCPU	Double	No	Average percentage of CPU used on a machine.	0–100
PeakCPU	Double	No	Maximum percentage of CPU used on a machine.	0–100
MachineOSType	String	No	Specifies the session support of the machines in the catalog.	1: Single-session, 2: Multi-session

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

Machine Meta Data	Type	Nullable	Description	Value
LowLoadInstances	Integer	No	Number of machines with machine score < 41.	>=0
MediumLoadInstances	Integer	No	Number of machines with machine score >= 40 and machine score < 70	>=0
HighLoadInstances	Integer	No	Number of machines with machine score >=70.	>=0
AggregatedStatus	String	No	Status description Failed, Unregistered, Maintenance, Active, Ready for use.	
ReadyForUseInstance	Integer	No	Number of machines with ‘Ready for use’ status.	>=0
ActiveInstance	Integer	No	Number of machines with ‘Active’status.	>=0
UnregisteredInstance	Integer	No	Number of machines with ‘Unregistered’ status.	>=0
FailedInstance	Integer	No	Number of machines with ‘Failed’status.	>=0

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

MaintenanceInstance	Integer	No	Number of machines with 'Maintenance' status.	>=0

Power BI integration for Citrix Performance Analytics

September 1, 2025

The Citrix Analytics Service platform ODATA API currently supports the Performance Analytics data export capability.

This document describes the necessary steps required to integrate the CAS ODATA API with Power BI, which also supports:

1. Incremental data refresh (this support is critical for a large data set)
2. Scheduled data refresh (automatically pull and export the data to Power BI workspace)

Prerequisites

The following items are required to connect the CAS ODATA feed:

1. Citrix Cloud™ customer ID (CCID)
2. Global CAS ODATA API endpoint: `https://api.cloud.com/casodata`
3. Citrix Cloud API client.

The CAS ODATA API uses the Citrix Cloud bearer token for authentication. A Citrix Cloud API client is required to get the bearer token. For information on how to to create a Citrix Cloud API client and save the client ID and secret, see the Get started with Citrix Cloud APIs documentation.

> **Note:**
>
> The admin who creates the API client needs to have the "Read-only"access or the "Full admin access"to the Citrix Cloud Analytics service.

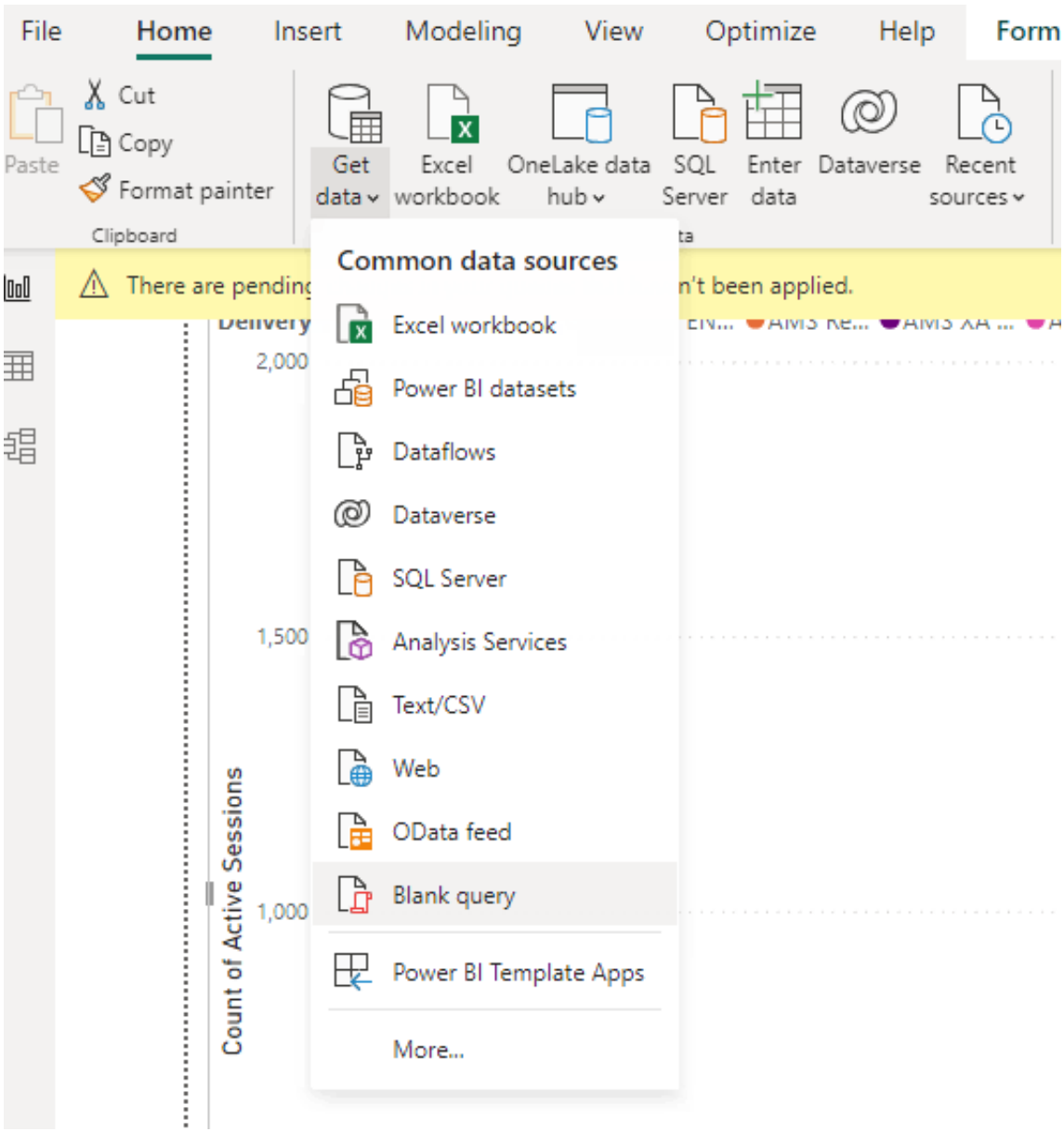
Connect CAS ODATA feed with Power BI

Perform the following steps to connect the CAS ODATA feed with Power BI:

1. Open Power BI desktop.

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

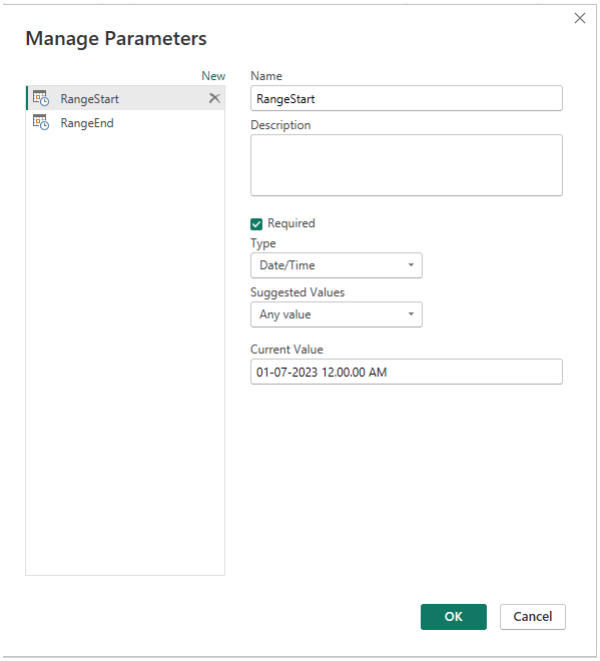
2. Select **Home** -> **Get Data** -> **Blank Query**. The **Power Query Editor** page appears.



3. On the **Power Query Editor** screen, select **Manage Parameters** and add the following two parameters to support incremental refresh:

   - RangeStart: the refresh start date (must use the "Date/Time"type)
   - RangeEnd: the refresh end date (must use "Date/Time"type)

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



For more information, see the Microsoft documentation.

4. On the **Power Query Editor** screen, select **Advanced Editor**, enter the following query to interact with Citrix Cloud to get the bearer token and to interact with the CAS ODATA feed to get the data required.

> **Note:**
>
> Use the bearer token retrieved in the previous step for authentication.

```
let
customerId = "placeholder_customerId",
// get citrix cloud API credential (bearer token)
tokenUrl = "placeholder_tokenUrl",
headers = [
#"customerid" = customerId,
#"Content-Type" = "application/x-www-form-urlencoded",
#"Accept" = "*/*"
],
postData = [
grant_type = "client_credentials",
client_id = "placeholder_ApiClientId",
client_secret = "placeholder_ApiSecretKey"
],
response = Json.Document(Web.Contents(tokenUrl, [Headers =
   headers, Content = Text.ToBinary(Uri.
BuildQueryString(postData))])),
// get the CC bearer toekn from the response
token = "CwsAuth bearer=" & response[access_token],
reportDate = DateTime.AddZone(RangeStart, 0),
reportDateYear = Number.ToText(Date.Year(reportDate)),
```

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

```
    reportDateMonth = Number.ToText(Date.Month(reportDate)),
    reportDateDay = Number.ToText(Date.Day(reportDate)),
    // CAS ODATA API endpoint and ODATA query. Sample below will
       retrieve active sessions (non-terminated)
    // apiURL = "https://api.cloud.com/casodata/sessions?$filter=
       SessionState ne '3'",
    apiURL = "placeholder_OdataApiUrl",
    // have to separate api queries below to make PowerBI happy
    apiQuery = [
    #"year" = reportDateYear,
    #"month" = reportDateMonth,
    #"day" = reportDateDay
    ],
    apiHeaders = [
    #"Authorization" = token,
    #"Citrix-CustomerId" = customerId
    ],
    Source = OData.Feed(apiURL, null, [Query=apiQuery, Headers=
       apiHeaders]),
    #"Filtered Rows" = Table.SelectRows(Source, each [Timestamp]
       >= DateTime.AddZone(RangeStart, 0) and [Timestamp] <=
       DateTime.AddZone(RangeEnd, 0))
    in
    #"Filtered Rows"
```

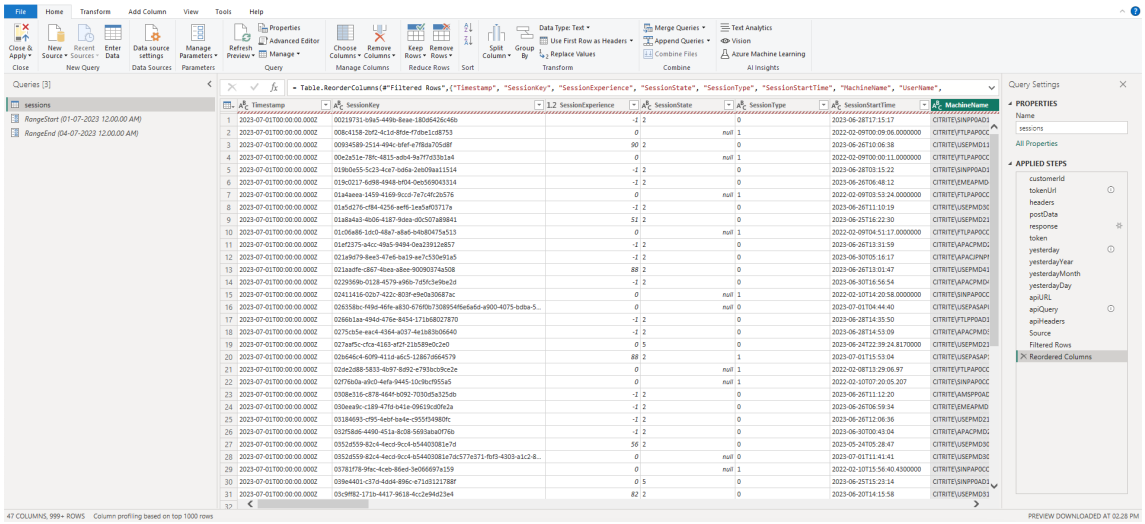
5. Replace the following placeholders based on your site:

   - Placeholder_customerId: customer ID
   - placeholder_tokenUrl: regional specific CC auth URL

     `https://api.cloud.com/cctrustoauth2/root/tokens/clients`
   - placeholder_ApiClientId: API client ID
   - placeholder_ApiSecretKey: API client secret key
   - placeholder_OdataApiUrl: API URL for CAS ODATA with optional ODATA query (for example: `"https://api.cloud.com/casodata/sessions?$filter=SessionState ne '3'"`)

6. Once completed, click **Done**. The request for data source access credentials appears.
7. Select **Anonymous** and then click **Apply**. The data is refreshed as follows:

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

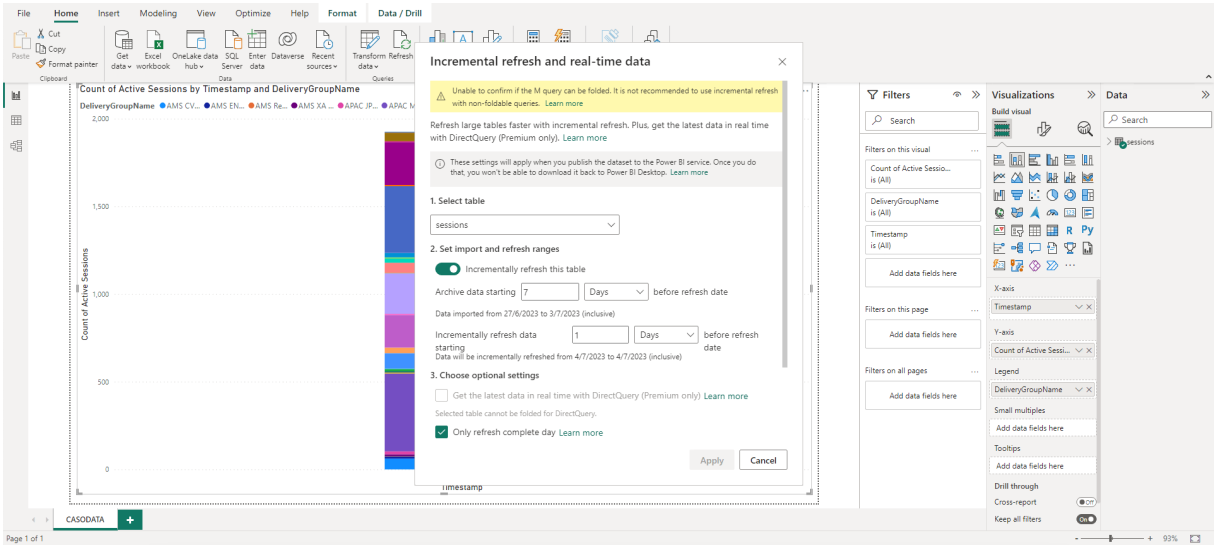


Configure PowerBI to support incremental refresh

When the Power Query can pull data, you need to configure incremental refresh for the data source.

Right-click the data source and select **Incremental refresh** to configure the policy to enable incremental refresh:

> **Note:**
>
> Power BI premium or pro license is required to support incremental refresh.



> **Important:**
>
> - When the incremental refresh is enabled, the first refresh triggers the ODATA API calls to get all the historical data. As the ODATA API aggregates the data in a daily manner, it's impor-

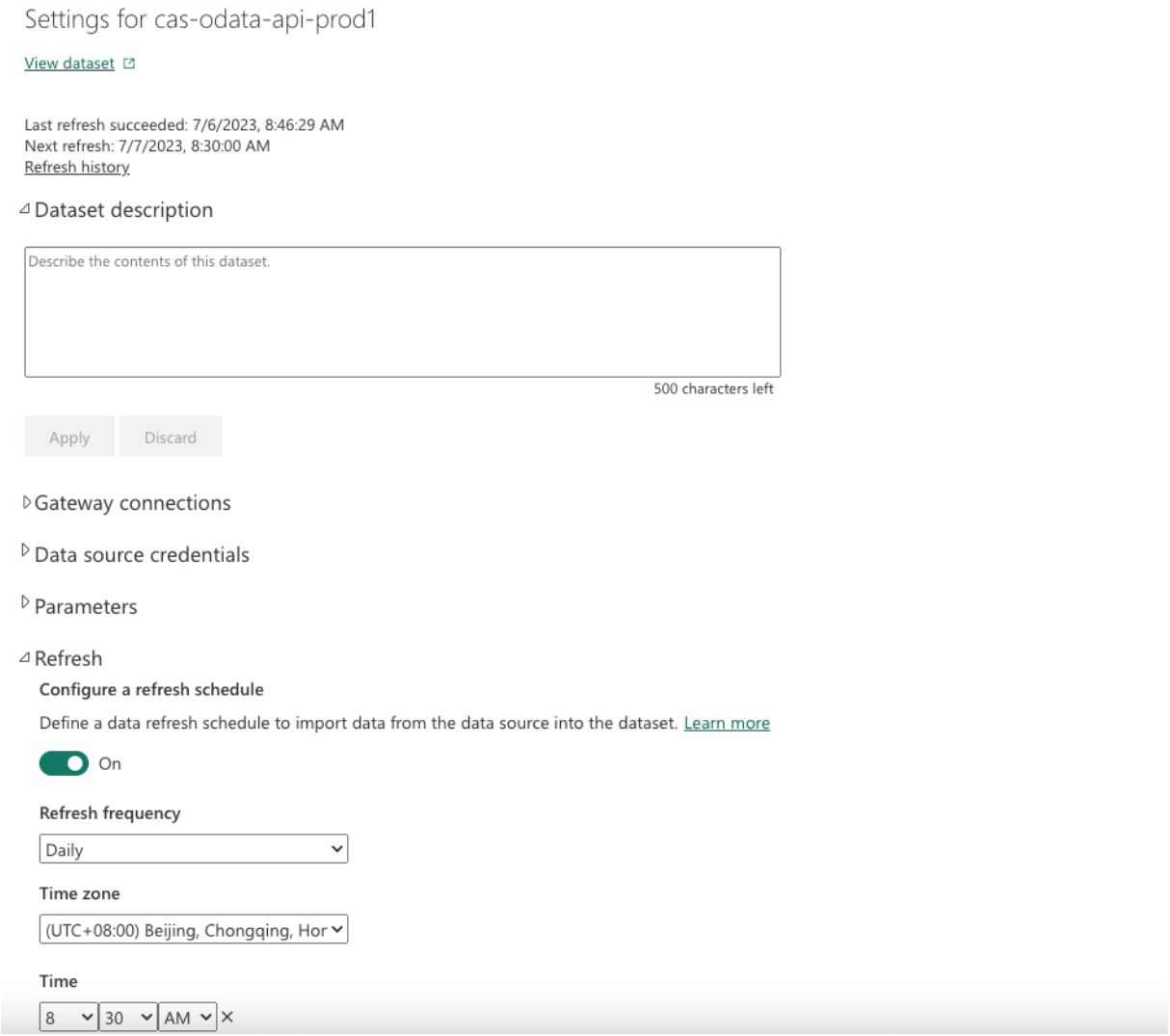
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> tant to use number of “days”for archived data.
> - Consider a reasonable number of days to keep the data to save your PowerBI workspace disk space (for example “7”days).

Publish to Power BI cloud and enable scheduled refresh

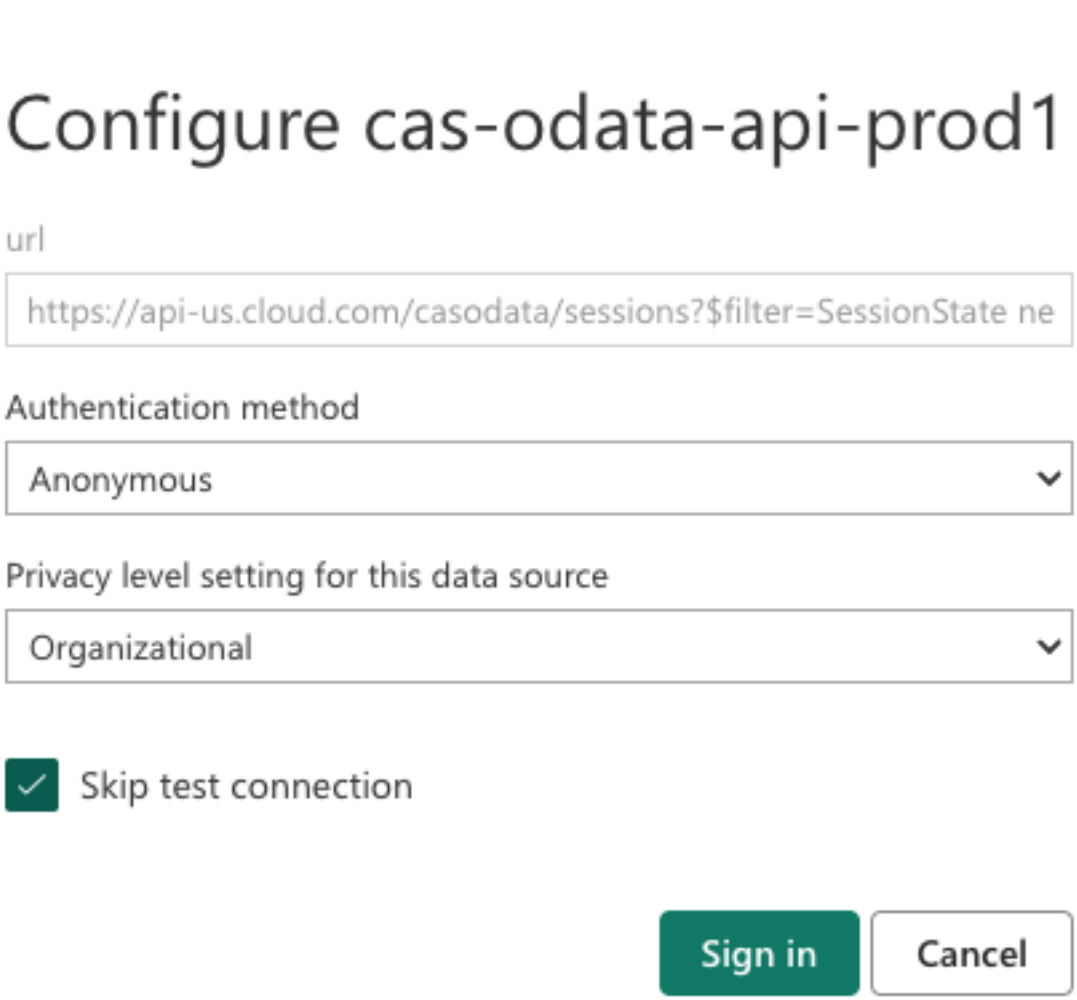
Once the preceding changes are completed, select Power BI desktop **Home** -> **File** -> **Publish to Power BI**. The dataset and reports are published to the Power BI cloud workspace.

Enable the scheduled refresh by clicking **Settings** in the dataset:



Configure anonymous access for the data sources in the **Data source credentials** section and select **Skip connection test**, and then click **Sign in** as follows:

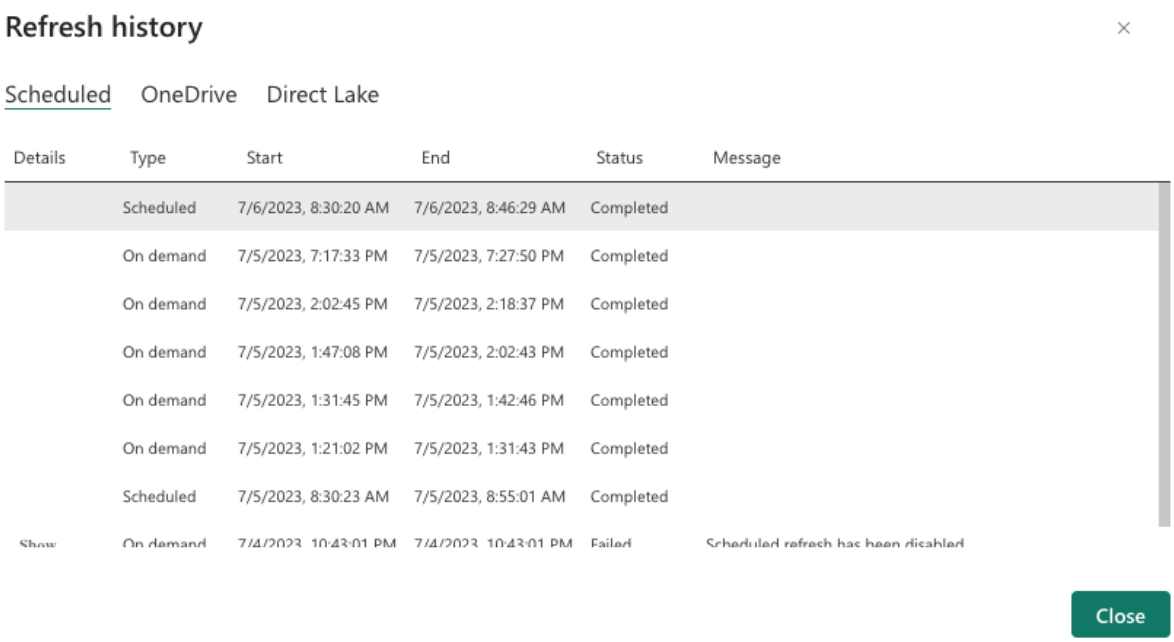
© 1997–2026 Citrix Systems, Inc. All rights reserved.



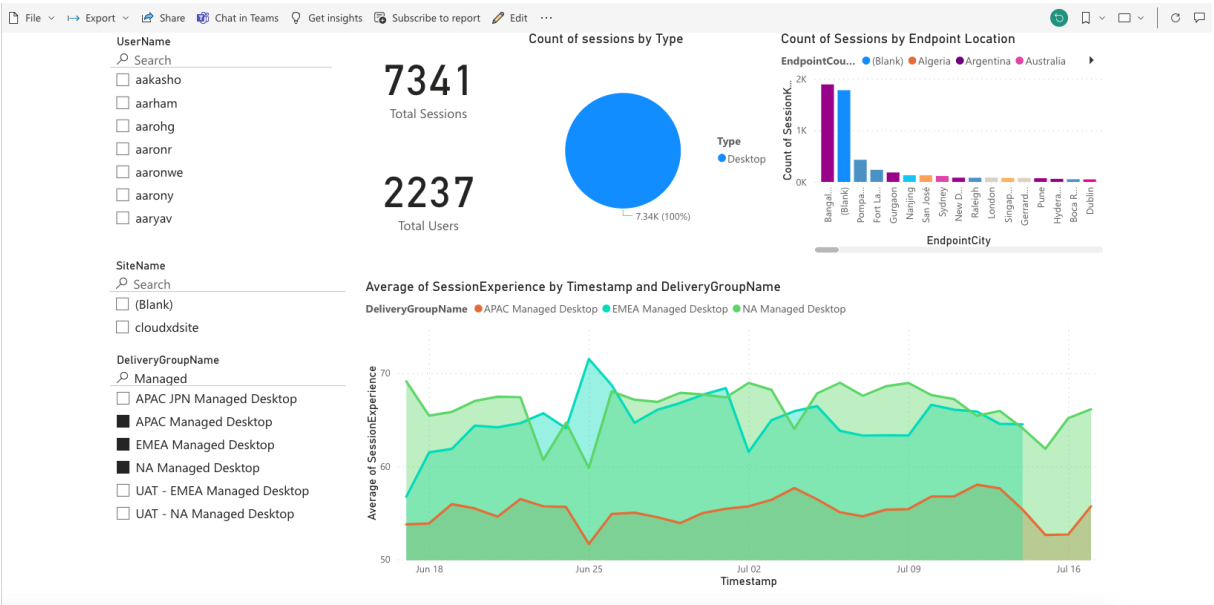
The first dataset refresh pulls the historical data, which might take a longer time. And the later incremental refresh pulls only the latest day's data. This refresh is done as configured in the incremental refresh policy in the previous section.

The refresh history looks as follows:

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



Once the refresh is completed, you are able to continuously pull the data to Power BI automatically.



Limits

September 1, 2025

The values in this article are the tested and recommended limits for the Citrix Analytics for Performance™ service instance per customer. These values are intended to help evaluate the product for

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

sizing and scalability. If you have requirements that these limits do not address, contact your Citrix representative for assistance.

Configuration Limits

Resource	Limit
Delivery Groups	1,000
Machines/VDAs	100,000
Machines on Process Utilization Group Policy	10,000
Number of on-premises CVAD Sites	20

Usage Limits

Resource (across all CVAD Sites)	Limit
Concurrent administrators	8
Concurrent end users	100,000
Concurrent session launches	100,000

Manage Administrator Roles for Performance Analytics

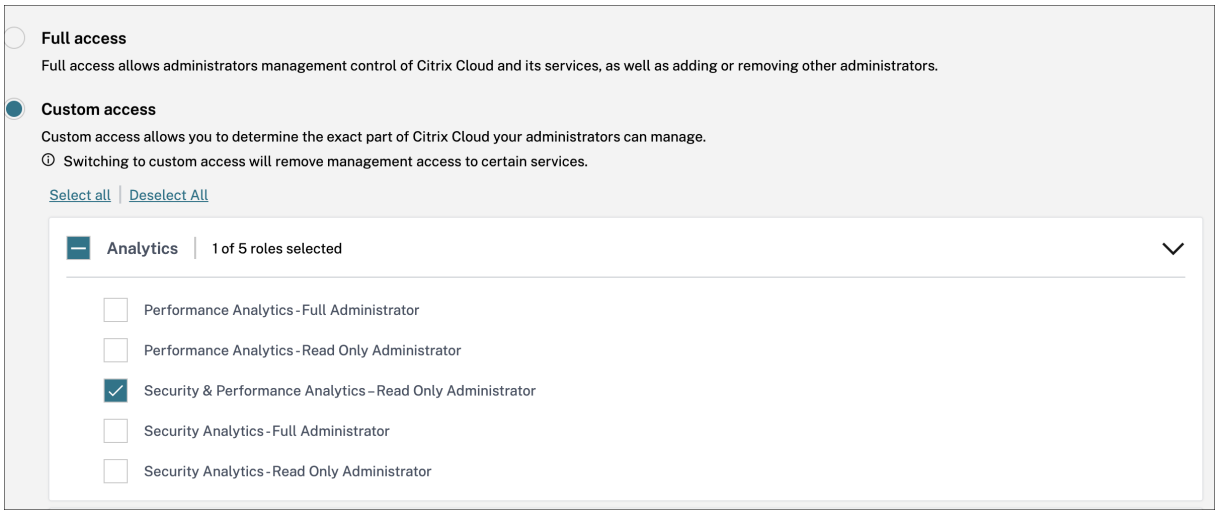
September 1, 2025

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

As a Citrix Cloud administrator with full access permissions, you can invite other users or Azure Active Directory groups to manage the Performance Analytics offering. The users and groups must be configured as administrators on Citrix Cloud using Identity and Access Management > Administrators. For more information, see Identity and access management.
You can assign them one of the following custom roles:

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

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



Notes:

- If an administrator is configured as a user and also belongs to a group, their permission as a user takes precedence over the group permissions.
- If a user is a member of more than one group, their permission is a sum of the permissions the user has in each group.
- Administrators belonging to groups are not identified with email ids. Hence, they would not receive any Alert Notifications.

Permissions for the custom roles

The administrators with the **Performance Analytics- Full Administrator** role can access all the features and functionalities of the Performance Analytics offering.

The administrators with the **Performance Analytics- Read Only Administrator** role can access and use the User Experience and Infrastructure Dashboards like the Full Administrators. However, Machine Actions in the Machine Statistics page are disabled for read-only users. Administrators with read-only access will not receive alert notifications from Citrix Analytics.

For more information on the actions allowed in the Self-service view, see the Self-Service article.

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

User Experience Analytics

September 1, 2025

What is User Experience Analytics?

The User Experience Analytics gives actionable insights into the user and session performance parameters of your environment.

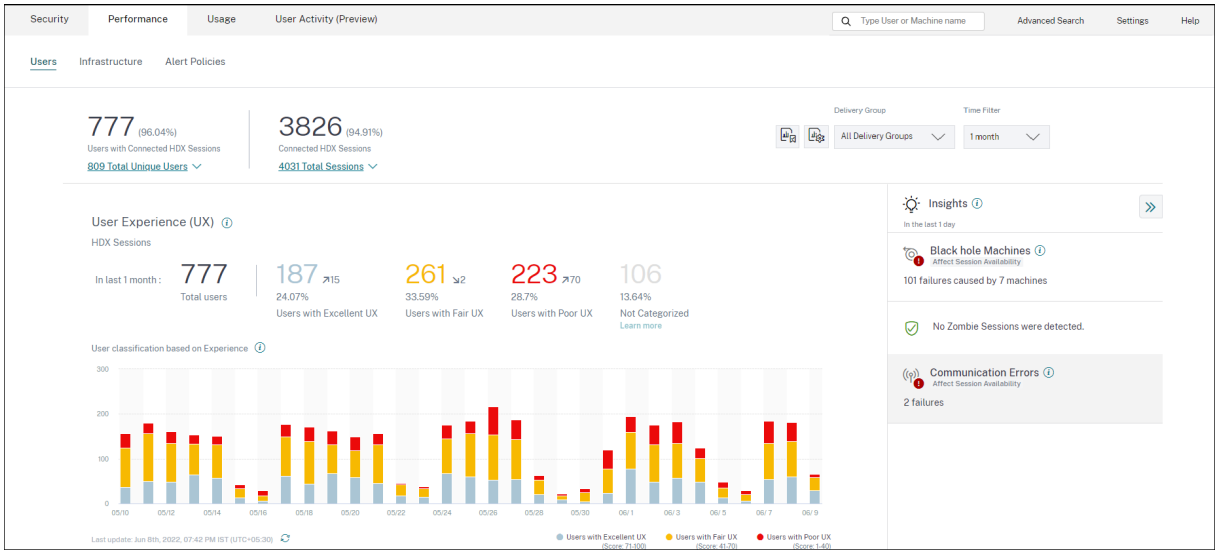
- User Experience Analytics provides a comprehensive analytical solution for all the Sites across an organization in a single consolidated dashboard.
- User Experience Analytics analyzes user sessions based on important parameters that define its performance - Session Logon Duration, Session Responsiveness, Session Availability, and Session Resiliency.
- The performance metrics are baselined using dynamic thresholds. The thresholds help measure the Session Experience score and categorize sessions into Excellent, Fair, or Poor categories.
- The User Experience (UX) score is calculated with the individual Session Experience scores. The UX score quantifies the complete user experience in the Sites and allows for users to be segregated as having an Excellent, Fair, or Poor experience.
- The drilldown view further provides an overview of the user performance across factors and subfactors, providing specific actionable insights for users facing suboptimal experience.

How to access the User Experience dashboard

To view the User Experience dashboard:

1. Log on to Citrix Cloud™ and select the Cloud Customer.
2. On the Analytics Service tile, click **Manage**.
3. On the Analytics overview page, click **Manage** under the **Performance** offering.
4. Click the **Users** tab.

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



How to use the User Experience dashboard

Site selection is available if multiple Sites are present in the environment. Use the Time Filter to select the required duration, and select the required Delivery Groups. The dashboard gives an overview of the user and session experience. You get,

- User classification of users running HDX™ sessions based on User Experience.
- Trend of user classification for the selected duration.
- Trend of user sessions and session failures for the selected duration.
- Session classification based on Session Responsiveness and Session Logon Duration factors.

The following section describes the various elements on the User Experience dashboard.

User Experience score

The UX score is a comprehensive end user experience index calculated based on the performance factors that affect a user session. Metrics that are measured through the session life cycle from its launch attempt to its end, contribute to the calculation of the UX Score.

- **Session Logon Duration** represents the session launch experience.
- **Session Responsiveness** represents the in-session responsiveness or session latency.
- **Session Availability** represents the success rate of establishing a session connection when attempted by the user.
- **Session Resiliency** indicates how the Workspace app recovers from network failures when the user is connected over a sluggish network. It measures the reconnection rate.

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

For more information about the UX score calculation and threshold calibration for user classification, see the UX score article.

Granularity of data collection is based on the selected time period. All data on the dashboard and the drilldown screens is obtained and refreshed from the database as per the data collection granularity. Click the refresh icon to update the data immediately.

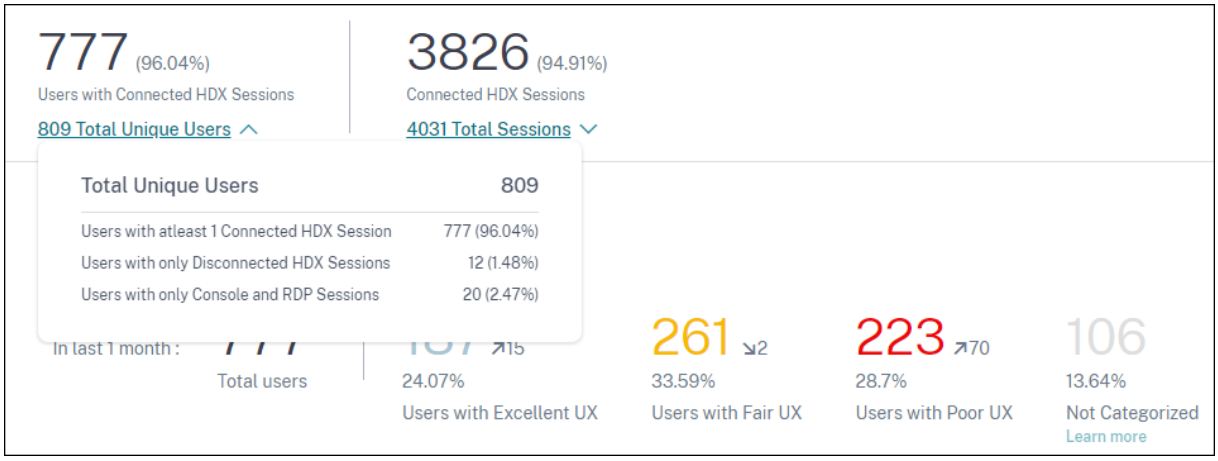
Breakup of Users and Sessions

The dashboard now shows the breakup of users and sessions in the virtual apps and desktops environment based on the session protocol and the connection status.

The dashboard provides performance metrics for only connected HDX sessions. Sessions that have been disconnected throughout during the selected period indicates that the user was not active for the entire selected period. Hence, Session and User Experience scores are not applicable for disconnected sessions.

The following metrics are available in the breakup:

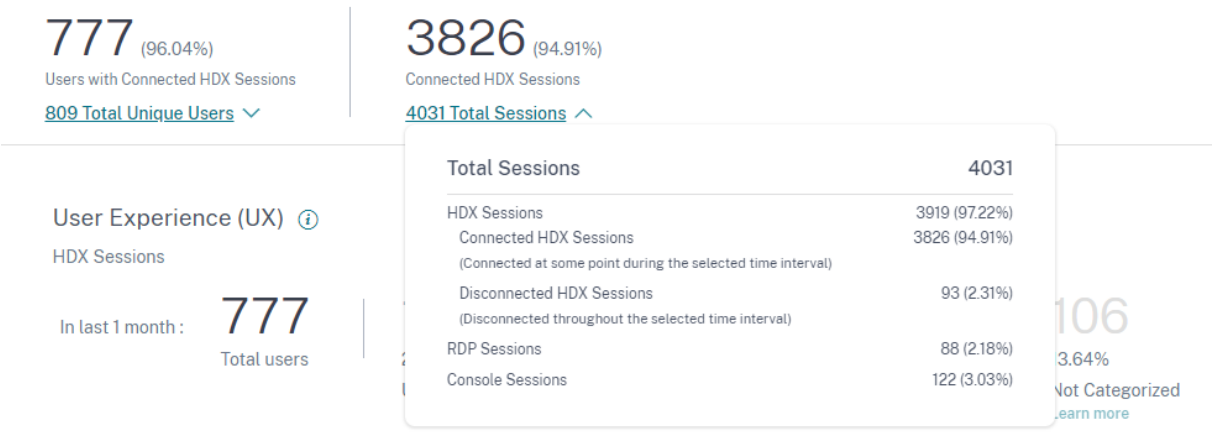
- Number and percentage of users with connected HDX sessions
- Number and percentage of connected HDX sessions
- Total number of unique users with breakup
- Total number of sessions with breakup



Based on the session protocols and connection status, the total unique users are classified as:

- Users with at least one Connected HDX Session: These users have had at least one HDX session in connected state at some point during the time interval.
- Users with only Disconnected HDX Sessions: All the sessions of these users have been disconnected throughout the time interval.
- Users with only Console and RDP Sessions

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



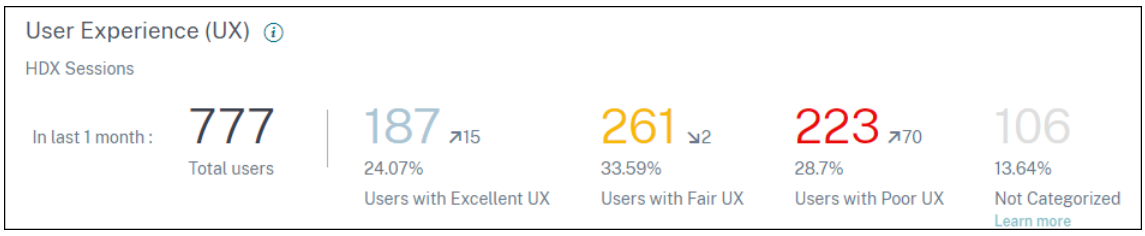
Based on the session protocols and connection status, the total sessions are also categorized similarly as follows:

- HDX Sessions
  - HDX Connected Sessions: Sessions that were in connected state at some point during the time interval.
  - HDX Disconnected Sessions: Sessions that were in disconnected state throughout the time interval.
- RDP Sessions
- Console Sessions

User Classification by Experience

To view the classification of users based on the UX score:

1. On the **Users** tab, select the time period for which you want to view the User Experience. The last 2 hours (2H) time period is selected by default.
2. Select the Site and Delivery Groups. If you select **All Sites**, metrics consolidated across all the Sites are displayed.



3. The total number of active users in one or more selected Sites and Delivery Groups for the selected time duration is displayed.

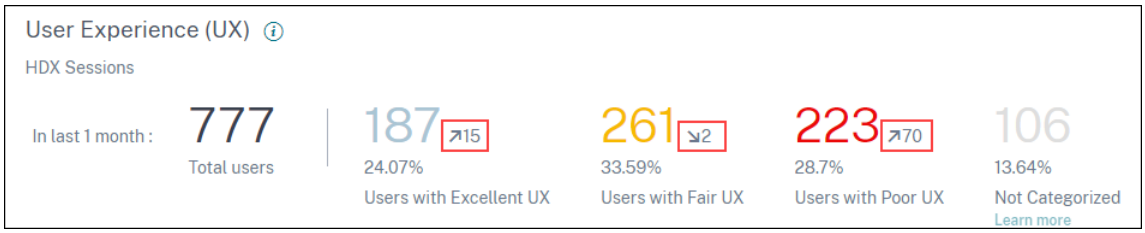
© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Users distribution across each of the Excellent, Fair, and Poor categories based on their UX Scores is displayed in numbers and percentages. The User Experience score thresholds for classification of users are calculated using statistical methods.

    - **Users with Excellent UX**: Represents users with a UX score of 71-100. Users with Excellent UX had a consistently good experience across all factors.
    - **Users with Fair UX**: Represents users with a UX score of 41-70. These users had a degraded experience for a limited period across certain factors.
    - **Users with Poor UX**: Represents users with a UX score 1–40. These users had a prolonged degradation across several indicators.
    - **User Not Categorized**: For information about users that are **Not Categorized**, see the Not Categorized Metrics article.

User Classification Trend

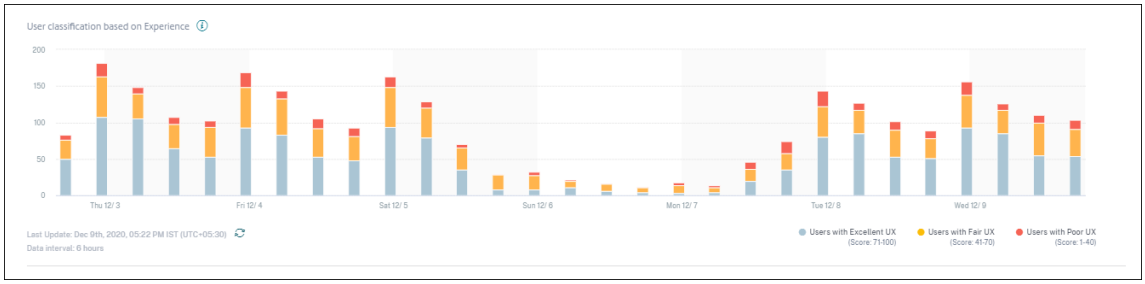
1. The up/down arrows indicate the trend in the number of users. It shows an increment or decrement of the number of users in each category as compared to the previous time period. For example, in the following scenario,



    - In the last 1 month, the Site had logons by a total of 777 users.
    - Of these, 187 users had an excellent user experience in the last month. This count is 15 users more than the number of users who had an excellent user experience in the previous month. So, the previous month had 172 users with an excellent user experience.
    - 261 users had a fair user experience in the last month. This count is 2 users lesser those who had a fair experience in the previous month.
    - 223 users had a poor user experience in the last month. 153 users had a poor experience in the previous month.

2. Click the categorized user numbers to further drill down into the factors affecting those users. For more information, see the Factor Drilldown article.
3. The **User classification based on Experience** trend displays the distribution of users across the categories during the selected time period. The length of a color on the bar indicates the number of users in an experience category.

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

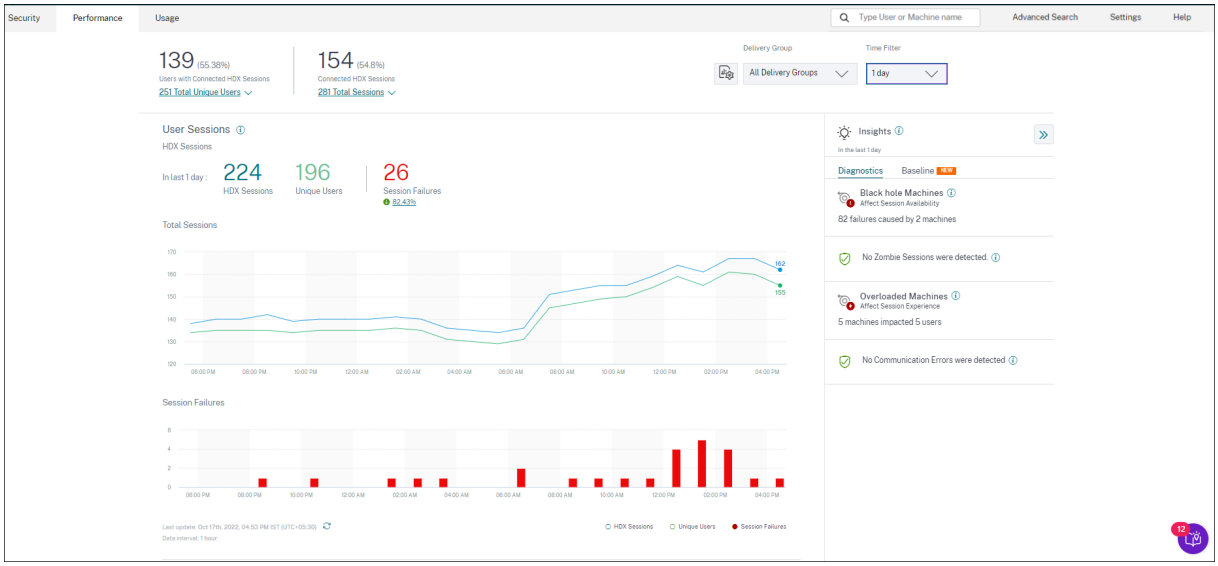


4. Hovering over the chart displays a tooltip containing the user classification for the specific data interval. Click the Excellent, Fair, or Poor region on the bars to see the drilldown displaying the classification of the specific set of users for the data interval represented by the bar.

User Sessions

A user session is created when an app or a desktop is launched from the Workspace app. The user interacts with the app or desktop through the user session. The experience the user has in each session adds up to the overall experience of the user in the Apps and Desktops environment.

The **User Sessions** section of the User Experience dashboard displays important session metrics of HDX sessions for the chosen time period, Site, and Delivery Groups.



You can view the following user session data:

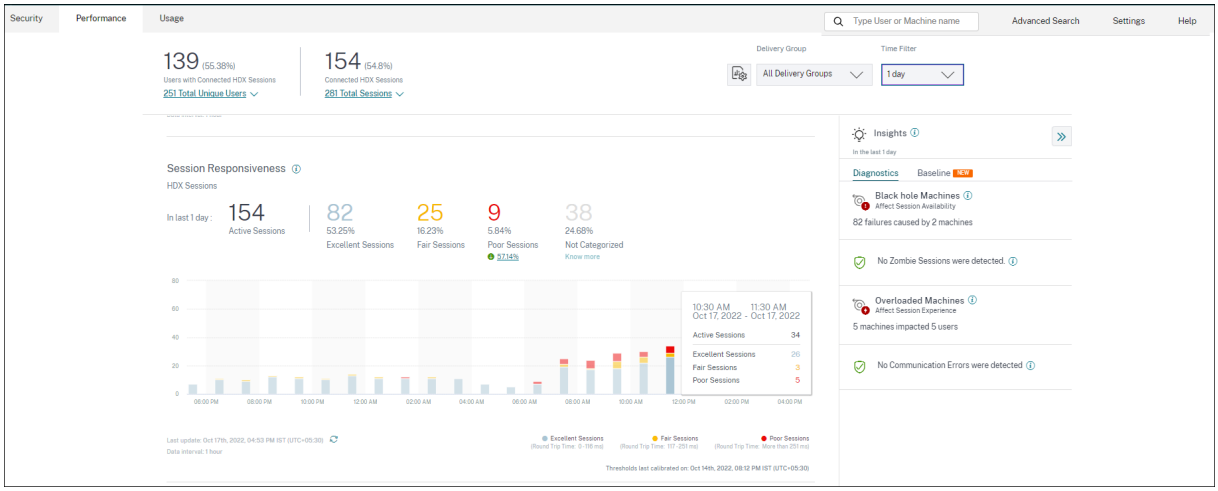
- **Total Sessions:** Total number of user sessions over the chosen time period. A single user can establish multiple user sessions. The number includes all sessions launched or active during the chosen period.
- **Total Unique Users:** Number of unique users who either launched a session or have an active session during the chosen period.

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

- **Session Failures:** Number of user sessions that failed to launch during this time period. Clicking the failure count opens the Sessions based self-Service search. Hover over the graphs to view detailed information for a specific collection interval. The charts help identify the pattern in the failures versus the total number of sessions connected. The unique users trend helps analyze the license usage in the Site and selected Delivery Groups. Deviation from the baseline is also displayed, clicking the deviation displays the respective Baseline Insight. For more information about Insights, see the Insights article.
- **Failure Insights:** Insights into the causes for session failure, drill down to specific users, sessions, or machines that the failures are associated with. Also available is a set of recommended steps to mitigate the failures. For more information, see the Insights article.

Session Responsiveness

Session Responsiveness represents the ICA® Round Trip Time (ICA RTT). ICA RTT is used to quantify the response time. It is the amount of time it takes for user input to reach the server and the response to appear on the endpoint machine. It measures the in-session experience and quantifies the lag experienced while interacting with a virtual app or desktop.



The Session Responsiveness section has the following information:

Active sessions: Active sessions are user sessions currently in operation and connected to Apps and Desktops.

Session classification: Sessions are categorized as Excellent, Fair, or Poor based on their ICA RTT measurements over the selected time period. Click the classification numbers to view the Sessions based self-Service search for the selected set of sessions.

The thresholds for categorization are calculated for the current customer and are recalibrated dynamically. For more information, see the Dynamic thresholding documentation.

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

Deviation from the baseline is also displayed, clicking the deviation displays the respective Baseline Insight. For more information about Insights, see the Insights article.

For information about sessions that are **Not Categorized**, see the Not Categorized Metrics article.

Session classification trend

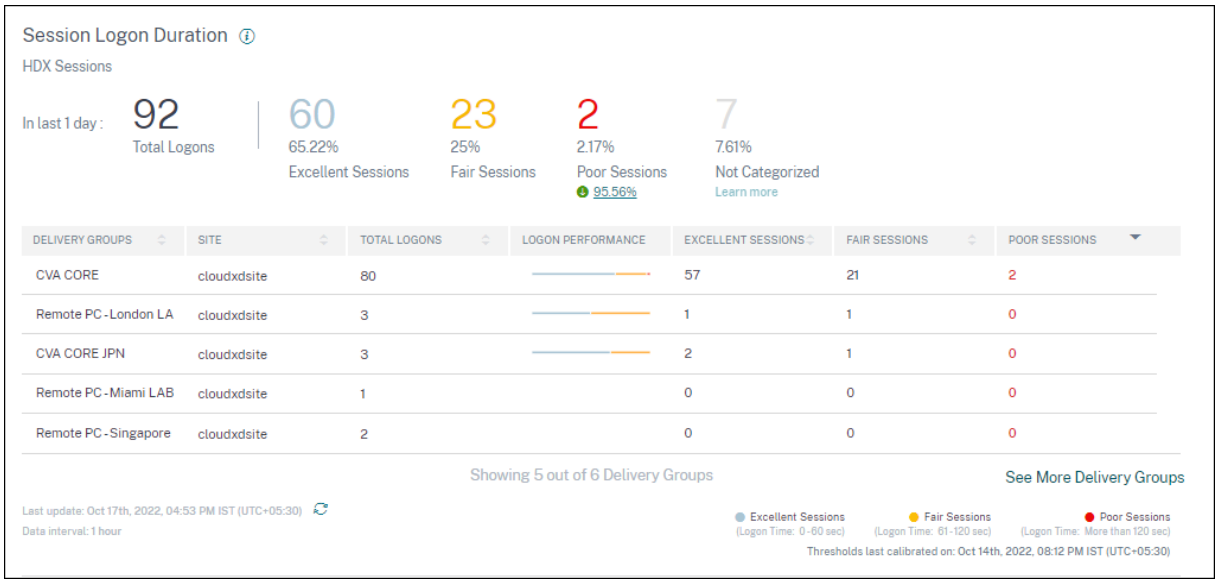
Session classification is plotted for the selected Site and Delivery Groups across the selected time duration. The legend displays the current thresholds used to plot the chart and the last updated time for the thresholds.

The session classification trend based on Session Responsiveness helps identify sessions facing network issues.

Session Logon Duration

The period from when a user clicks an application or a desktop in the Citrix Workspace™ app to the instant the app or desktop is available for use is called the logon duration. The logon duration includes the time taken for various processes in the complex launch sequence. Total logon time includes phases such as Brokering, VM Start, HDX Connection, Authentication, Profile Load, Logon Script, GPO, and Shell Launch.

Breaking down the Session Logon Duration data to individual phases helps troubleshoot and identify a specific phase causing a longer logon duration.



This section has the following information:

Total logons: The total number of logons to virtual apps or desktops in the selected duration, Site, and Delivery Groups.

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

Session classification: Sessions are categorized as Excellent, Fair, or Poor based on their Session Logon Duration measurements over the selected time period. Click the classification numbers to view the Sessions based self-Service search for the selected set of sessions.
The thresholds for categorization are calculated specifically for the current customer and are recalibrated dynamically. For more information, see the Dynamic thresholding documentation. The legend displays the current thresholds used to plot the chart and the last updated time for the thresholds. Deviation from the baseline is also displayed, clicking the deviation displays the respective Baseline Insight. For more information about Insights, see the Insights article.

Sessions Not Categorized for Logon Duration

Sessions might be **Not Categorized** for Logon Duration if the subfactors are not configured to be measured as described in Session Logon Duration subfactors.

Session Logon Duration sorted by Delivery Groups

Session Logon Duration data is displayed in tabular format with the following information:

- Delivery group and the corresponding Site.
- Session distribution chart based on performance indicators- Excellent, Fair, or Poor.
- Total number of sessions.
- Number of Excellent, Fair, and Poor sessions.

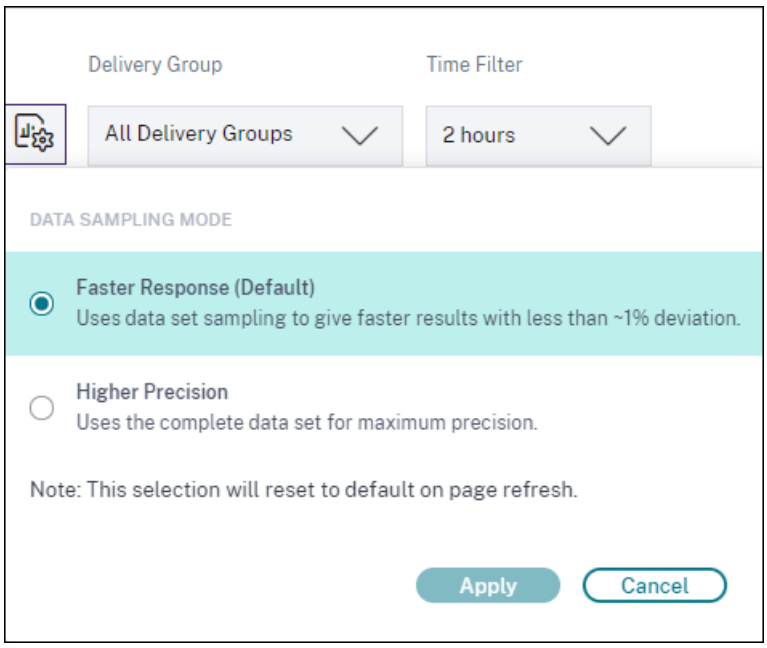
By default, the table data is sorted based on the **Poor Sessions** column. You can choose to sort it based on any of the other columns. The first five Delivery Groups based on the sort criteria are displayed. Click **See More Delivery Groups** to see more data.

This table helps identify the Delivery Groups with the maximum number of poor sessions. You can troubleshoot further to identify policies causing higher logon duration on the specific Delivery Group.

Approximation Mode

Data Sampling mode is available on the User Experience Dashboard in Citrix Analytics for Performance™ to help load the dashboard metrics faster. This mode is available on tenants with more than 25K active unique users in the past 30 days.

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



Data Sampling modes available are:

- **Faster Response Mode:** This mode uses data set sampling to arrive at performance metrics for all time periods. This helps load the metrics on the User Experience Dashboard faster especially in tenants with large number of users. The metrics deviate by approximately one percent from the numbers that are available in the Higher Precision mode.
  Faster Response is the default sampling mode. The dashboard gets reset to this mode upon page refresh for large tenants.
- **Higher Precision Mode:** This mode uses the complete data set to arrive at the performance metrics. Choosing this mode might result in slower loading of the dashboard. You can choose this mode to see more accurate metrics for the exact period chosen.
  Data Sampling Mode feature is applicable on the User Experience Dashboard only. The Intermediate drilldown and the Self-service pages continue to operate in Faster Response mode.

Data Availability

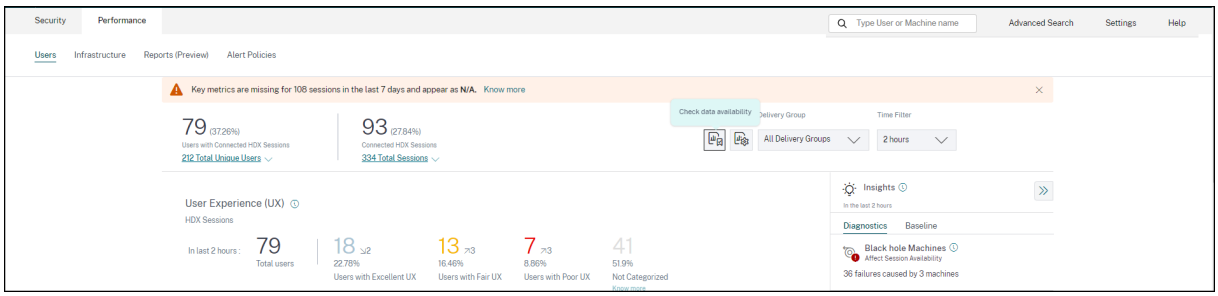
Accuracy of Performance Analytics depends on the data collected from various site infrastructure like the endpoints, machines, Gateway, and Delivery Controller. A good availability of the required metrics ensures that the data and insights provided by Performance Analytics closely represents the actual performance of the site.

The **Data Availability** feature helps identify sessions that do not have the data required to monitor the performance of your endpoints. Endpoint metrics like Endpoint Link Speed, Location, Throughput, ISP, Network Interface type, OS and Endpoint receiver version that are critical to analyze issues specific to endpoints.

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

Endpoint metrics require that the StoreFront™ be onboarded correctly, and the Citrix Workspace App versions installed on the endpoints are correct. The number of sessions across all the onboarded sites which don't have endpoint metrics during the past seven days is displayed when you open Citrix Analytics for Performance. If you are using Citrix Workspace, the service is automatically discovered and does not require onboarding.

Click **Know more**. A modal box containing the reasons in detail and the actions that you could take to solve the issues, is displayed. You can also click the Data Availability icon to view the modal.



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

- One of the key reasons for missing endpoint telemetry is StoreFront onboarding. StoreFront must be onboarded correctly; data processing must be switched on and appropriate URLs must be whitelisted. **Review StoreFront Data Sources** takes you to the Data Sources page that leads you through the StoreFront onboarding process required for the Workspace App Data Collection. Click **Sessions missing endpoint data** to open the Sessions self-service view with the list of sessions whose endpoint metrics are missing because of incorrect or non-existent StoreFront Onboarding. If you are using Citrix Workspace, the service is automatically discovered and does not require onboarding.
- Endpoint telemetry is not available for sessions launched from endpoints that run unsupported OS platforms or incompatible Citrix Workspace app versions. Clicking **Sessions missing endpoint data** opens the Sessions self-service view with the list of the sessions missing endpoint telemetry due to a specific listed reason. For more information, see the Version matrix that lists for each feature, the OS versions and the required Workspace app version on which it is supported.

User Experience Score

September 1, 2025

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

What does the User Experience represent?

The User Experience is a comprehensive measurement of the quality of the session established by the user while using Apps and Desktops. The User Experience (UX) score indicates the quality of user experience. UX score is calculated using performance factors that define the quality of a user session. The factor metrics are analyzed and processed using statistical methods over a time period to arrive at a score out of 100. This score is a quantitative reflection of the actual experience a user has while using Apps and Desktops.

The performance factor metrics represent the experience of a session through its life cycle from session launch to the session end.

- **Session Logon Duration** factor represents the session launch experience.
- **Session Responsiveness** factor represents the in-session responsiveness or sluggishness.
- **Session Availability** represents the success rate of establishing a session connection when attempted by the user.
- **Session Resilience** measures the reconnection rate when the user is connected over a sluggish network.

The performance factors are further divided into subfactors/types. For example, Session Logon Duration is calculated using individual phases that occur during logon, such as the GPOs, Interactive session, and Profile load.
The factor and subfactor thresholds are calibrated to classify users and sessions as Excellent, Fair, or Poor.

UX scores are benchmarked into the following categories:

- **Excellent**: UX score of 71-100
- **Fair**: UX score of 41-70
- **Poor**: UX score of 1-40

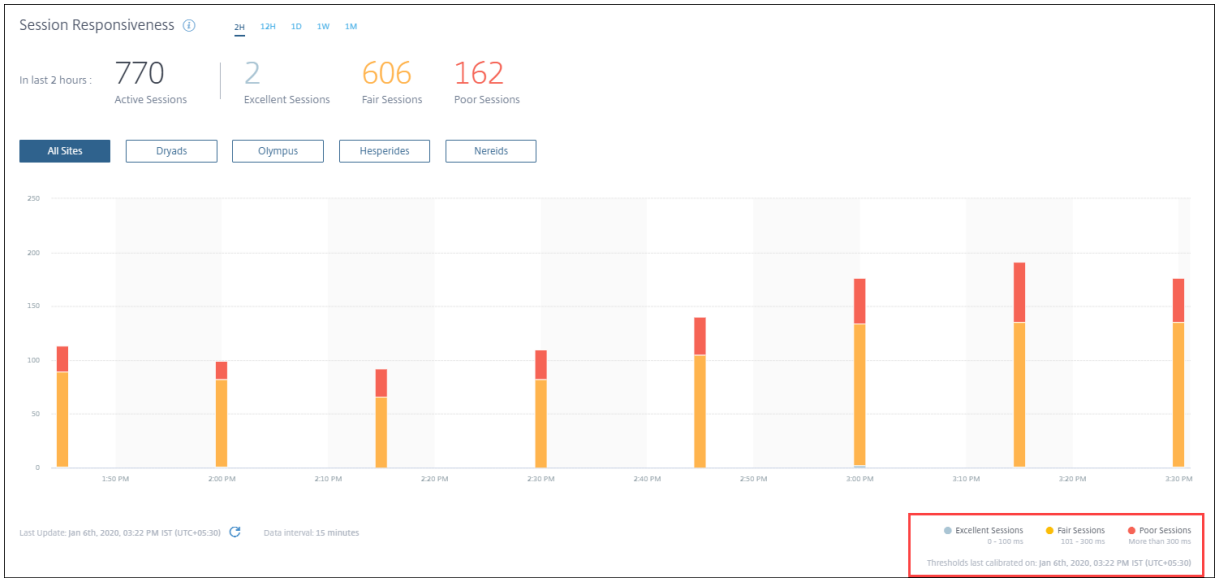
How are dynamic thresholds calculated

The concept of dynamic thresholds is used to benchmark the Session Logon Duration and the Session Responsiveness factors and their subfactors individually for every customer. Statistical techniques are used to periodically calculate thresholds that classify users as Excellent, Fair, or Poor.

- Calculation of thresholds for factors and subfactors is done on a per customer basis. This method of calculation ensures that the specific configuration and range of accepted behavior for every customer is accommodated for.
- Thresholds are calculated for each customer based on metrics collected during the past 30 days.

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

- Thresholds are recalibrated every seven days to reflect any changes in the environment, such as, reconfiguration of machines or a network upgrade. The recalibrated thresholds represent the resulting changes in factor measurements.



In this example, the chart legend indicates the dynamic thresholds of Session Responsiveness as:

- Excellent session - 0–100 ms
- Fair session - 101–300 ms
- Poor session - greater than 300 ms

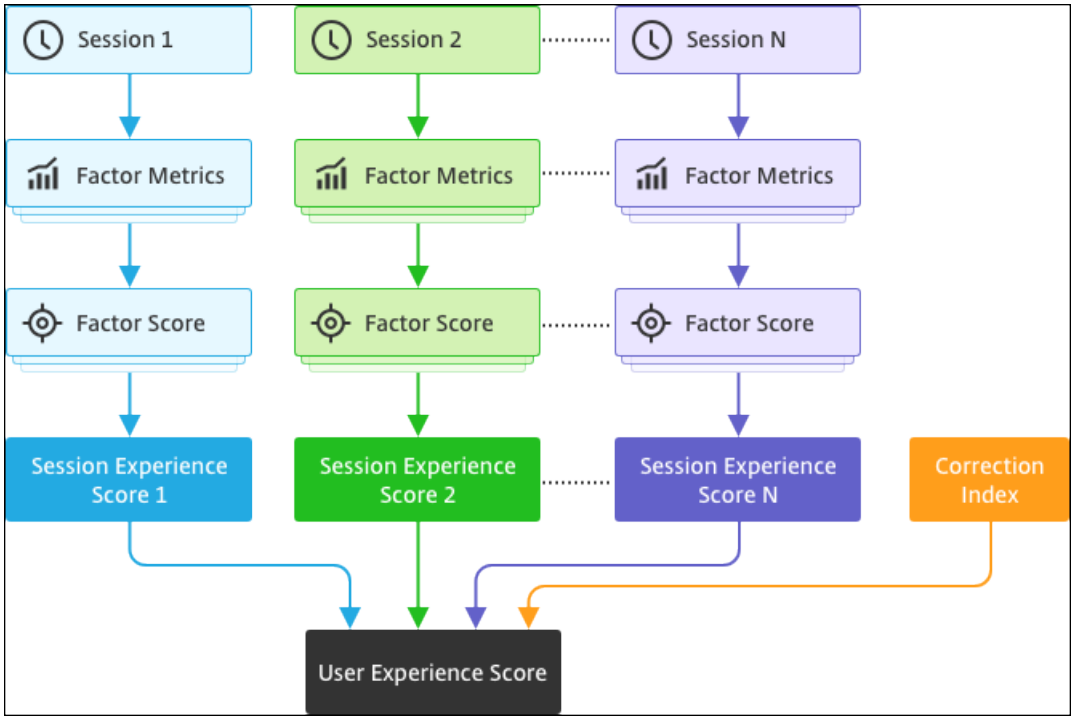
Time stamp of the last thresholds update is displayed below the chart legend. The chart is replotted based on the latest thresholds.

Dynamic thresholds ensure that the classification of session and users reflects the environment that is being analyzed precisely. Users with poor experience in any customer environment are highlighted accurately for further troubleshooting.

How is the UX score calculated

The User Experience score is calculated from the contributing factor scores using the bottom up approach.

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



1. **Benchmark factors**:

   For each session, Session Logon Duration and Session Responsiveness factors and their subfactors are calibrated dynamically once every seven days. Based on these thresholds, sessions are classified as Excellent, Fair, or Poor.
   The measurements are used to arrive at factor scores (out of 100) for each session.

2. **Relative weights of factors**:

   The severity by which the factors impact the user experience might differ. For example, the impact of Session Resiliency on the session experience is more than the impact of Session Logon Duration. So, a relative weight is applied on each factor.

3. **Session Experience score**:

   The session experience score is calculated as the weighted average of various factor scores applicable for the selected duration.

   Next, the session experience scores of individual sessions applicable to the user are collated.

4. **Correction factor**:

   The Session Availability factor indicates the success rate of getting a session connection when attempted. The impact of this factor is at the user level and not at the session level. Hence, the Session Availability score is applied as a correction factor to the sum of the individual session scores to arrive at the User Experience (UX) score.

The UX score gives you actionable insights about the user experience. Drilling down further into met-

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

rics of users with a poor user experience score helps identify a particular factor or subfactor that is causing the poor experience.

User Experience (UX) Factors

September 1, 2025

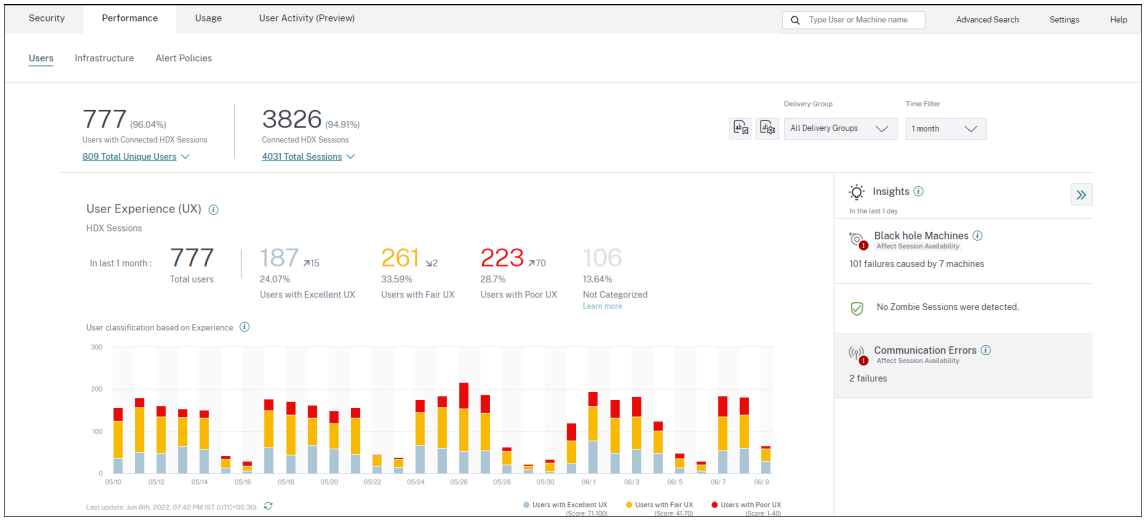
The UX Factors page provides an insight into the factor and subfactor level experience of the set of users you select on the UX dashboard.

Click any of the Excellent, Fair, or Poor UX category on the UX dashboard to open the UX Factors page. It quantifies the effect of factor and subfactor metrics on the user experience. This page classifies the selected set of users based on their experience concerning the factors - Session Availability, Session Responsiveness, Session Resiliency, and Session Logon Duration. Further, the selected users are also classified based on their experience concerning the subfactors within these factors. This drilldown enables you to identify the actual subfactor responsible for the poor experience of users in your environment.

How to use the User Experience (UX) Factors page?

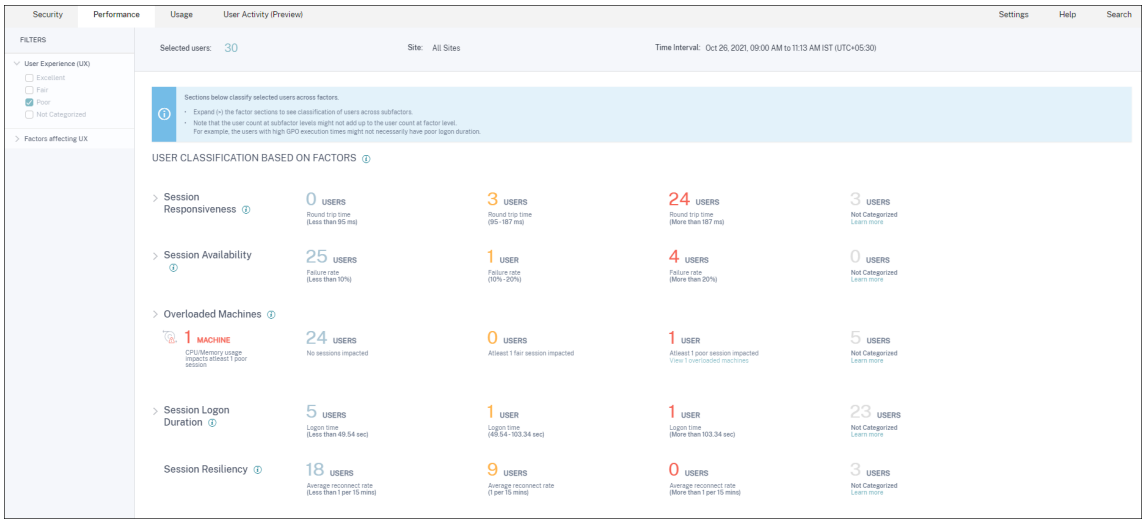
To drill deeper into the factor metrics affecting the user experience, click the number in any of the Excellent, Fair, or Poor category on the UX dashboard.

1. Consider the scenario, where the environment has 21 users having an excellent experience, 39 having a fair experience and 30 users having a poor experience during the last two hours. To understand the reason for the 30 users facing a poor user experience, click the number 30 from the User Experience dashboard.

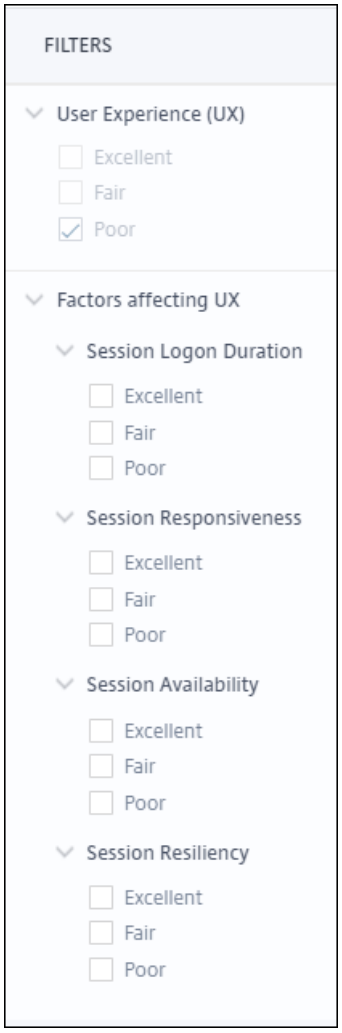


© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. The User Experience (UX) factors screen shows a drilldown of the factors affecting the poor experience of users in all the Sites during the last two hours.



3. The left panel displays the selection filters for the User Experience and the factors.



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

Click the **Selected users** number to access the self-Service Search page for the specific set of users.

4. The sections on the UX factors page classify the selected set of users further based on the factors Session Availability, Session Responsiveness, Session Resiliency, Session Logon Duration, and Overloaded Machines. Expand (click >) each factor section to see the user classification based on experience across the respective subfactors. The factors are sorted based on the number of users with poor factor experience.
5. The overall user experience classification might not match with the user count at the factor level. And, a poor experience across one or more factors might not necessarily mean an overall poor user experience.
6. Similarly, the user count at individual subfactor levels might not add up to the user count at the factor level. For example a user with high GPOs might not necessarily have a poor logon experience as the user's experience with other subfactors might have been excellent.
7. The classification of users at factor and subfactor levels helps identify and troubleshoot the precise cause of poor overall user experience.
8. For information about users that are **Not Categorized**, see the Not Categorized Metrics article.

Session Logon Duration

Session Logon Duration is the time taken to launch a session. It is measured as the period from the time the user connects from the Citrix Workspace app to the time when the app or desktop is ready to use. This section classifies users based on the session logon duration readings. The logon duration thresholds for classification of the experience as Excellent, Fair, or Poor are calculated dynamically. For more information on the Dynamic thresholds for Session Logon Duration, see the Dynamic Thresholds section.



Clicking the classified user count numbers lead to the **Self-Service** screen displaying the actual performance factor measurements for the selected set of users.

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

Session Logon Duration is broken down into subfactors that represent individual phases in the complex launch sequence. Each row in the Session Logon Duration drilldown table represents the user categorization for the individual phases occurring during session launch. This helps troubleshoot and identify specific user logon issues.



The user counts for Excellent, Fair, and Poor category related to each subfactor experience are displayed. Use this information to analyze specific subfactor phases that might be contributing to longer logon duration.

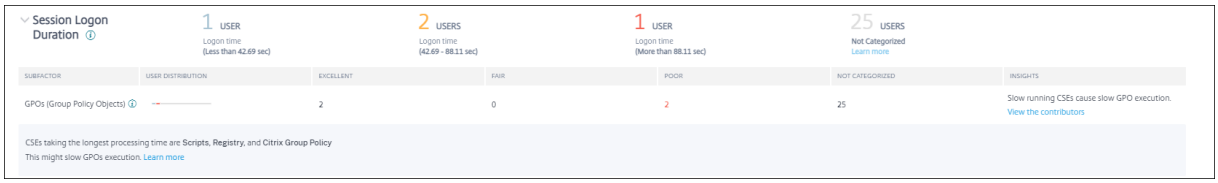
For example, if GPOs show the highest number of users facing poor experiences, review the GPO policies applicable for these users to help improve logon duration experience.

The last **Not Categorized** column displays the number of users for whom specific subfactor measurements are not available for the selected time period. Specific reasons are elaborated with individual subfactor descriptions.

GPOs

GPOs is the time taken to apply group policy objects during logon. GPOs' measurement is available only if the Group Policy settings are configured and enabled on the virtual machines.

GPOs Insights displays client-side extensions in the environment taking the longest processing time during the selected time period. To see the insights, click the **View the contributors** link in the **Insights** column of GPOs in the Session Logon Duration subfactor table. GPO Insights are based on the analysis of user sessions having poor experience in GPO execution.



A client-side extension (CSE) is a dynamic-link library (DLL) that implements the Group Policy on the client machine. CSEs with long processing time increase GPO execution times and optimizing CSE

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

processing improve the overall session logon experience of the user.

Average CSE execution time depends on the number and type of policies applied with it. Use the following pointers to improve the processing time of CSEs.

- **Folder Redirection:** CSE execution time depends on the number of folders redirected and the contents of each folder. The system can have a wait configured that gets applied after every folder redirection. Optimize the number of folders, to achieve lower CSE execution time.
- **Drive Mapping:** Logon scripts can try to map drives to non-existent target servers resulting in a higher execution time. Make sure the server addresses are correct and available.

Review and tune policies associated with CSEs taking the longest processing time as indicated in the GPO insights. Further, consider deleting the ones that are not required.

Profile Load

Profile load is one of the most critical phases of logon duration. It is the time it takes to load a user's profile, which includes the registry hive (NTUser.dat) and the user files. Optimizing the profile load time can help improve the overall logon duration experience.

Profile load measurement is available only if profile settings are configured for the user on the virtual machine.

The **Insights** column in the Profile Load displays insights into profile size being the contributing factor to long profile load times. It identifies users who are likely to be affected by a large profile size.



Click the **View the correlation** link to see the average profile size of users. The average profile size is calculated using the profile sizes of users who have had excellent and fair profile load experience during the last 30 days. This profile size is identified as optimum. Users having a profile size larger than the average are likely to have poor profile load times.

Click **View analysis** to see the list of users whose profile size is larger than the average. This view shows the last known and average profile size for each user. Use facets to further filter this data to view users with both large profile size and poor logon duration experience.

Expand the user details to view specific performance metrics to further troubleshoot the reason for poor experience.

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

Use these insights to recommend users to reduce large files in their profile.

Insights are not displayed if the profile size measurements or the average profile size are not available.

- Profile size measurement requires Citrix Profile Management to be installed on the machines.
- Profile size measurement is supported on machine versions 1912 and later.
- Profile size measurements of users with fair and excellent profile load experience over the past 30 days are used to calculate the average profile size. The insights are not derived if no data points are available for this duration.
- Profile load insights are derived in cases where profile size is the cause for slow profile load. The presence of several profile files in the profile might also result in slow profile load.

Interactive Session

The time taken to "hand off"keyboard and mouse control to the user after the user profile has been loaded. It is normally the longest duration of all the phases of the logon process.

Brokering

The time taken to decide which desktop to assign to the user.

VM Start

If the session required a machine start, it is the time taken to start the virtual machine. This measurement is not available for non-power managed machines.

HDX™ connection

The time taken to complete the steps required in setting up the HDX connection from the endpoint to the virtual machine.

Authentication

The time taken to complete authentication to the remote session.

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

Logon scripts

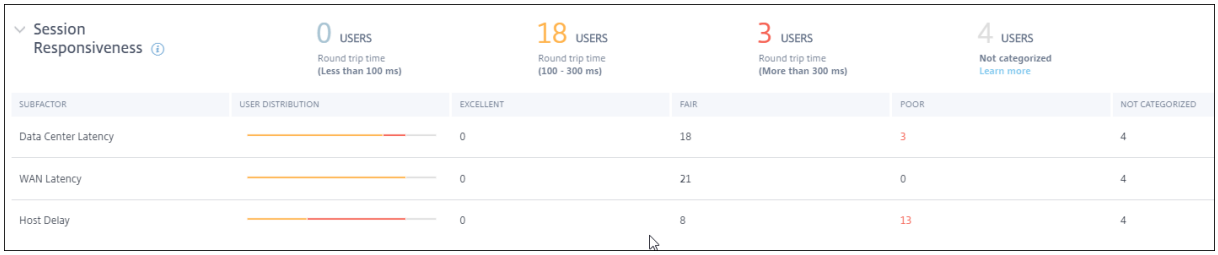
It is the time taken for the logon scripts to run. This measurement is available only if logon scripts are configured for the session.

Session Responsiveness

Once a session is established, the Session Responsiveness factor measures the screen lag that a user experiences while interacting with an app or desktop. Session Responsiveness is measured using the ICA® Round Trip Time (ICA RTT) that represents the time elapsed from when the user pushes down a key until the graphical response is displayed back.

ICA RTT is measured as the sum of traffic delays in the server and endpoint machine networks, and the time taken to launch an application. ICA RTT is an important metric that gives an overview of the actual user experience.

The Session Responsiveness thresholds for classification of the experience as Excellent, Fair, or Poor are calculated dynamically. For more information on the Dynamic thresholds for Session Responsiveness, see the Dynamic Thresholds section.



The Session Responsiveness Drilldown represents the classification of users based on the ICA RTT readings of the sessions. Clicking these numbers drills down to the metrics for that category. The users with excellent Session Responsiveness had highly reactive sessions while the users with poor Session Responsiveness faced lag in their sessions.

> **Note:**
>
> While the ICA RTT readings are obtained from the Apps and Desktops, the subfactor measurements are obtained from the on-premises Citrix Gateway. Hence, the subfactor values are available only when the user is connecting to an app or a desktop via a configured on-premises Citrix Gateway. For steps to configure Citrix Gateway with Citrix Analytics for Performance, see Gateway data source. In addition, you must configure L7 latency thresholding. For more information, see L7 Latency Thresholding.
>
> Further, these measurements are available for sessions,
>
> - launched from machines enabled for NSAP

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

> - new CGP (Common Gateway Protocol) sessions, and not reconnected sessions.
>
> These measurements are not available when the user is connected via Citrix Gateway Service.

The rows in the Session Responsiveness drilldown table represent the user categorization in the subfactor measurements. For each subfactor, the number of users in each category is displayed in the Excellent, Fair, and Poor columns. This information helps analyze the specific subfactor that is contributing to poor user experience.

For example, the highest number of Poor Users recorded for Data Center Latency indicates an issue with the server-side network.

The last **Not Categorized** column displays the number of users for whom the specific subfactor measurement was not available during the selected time period.

The following subfactors contribute to the Session Responsiveness. However, the total ICA RTT is not a sum of the subfactor metrics, as the subfactors of ICA RTT that occur until Layer 4 only are measurable.

- **Data Center Latency:** This subfactor is the latency measured from the Citrix Gateway to the server. A high Data Center Latency indicates delays due to a slow server network.
- **WAN Latency:** This subfactor is the latency measured from the virtual machine to the Gateway. A high WAN Latency indicates sluggishness in the endpoint machine network. WAN latency increases when the user is geographically farther from the Gateway.
- **Host Latency:** This subfactor measures the Server OS induced delay. A high ICA RTT with low Data Center and WAN latencies, and a high Host Latency indicates an application error on the host server.

A high number of users facing poor experience in any of the subfactors helps understand where the issue lies. You can further troubleshoot the issue using Layer 4 delay measurements. None of these latency metrics account for packet loss, out of order packets, duplicate acknowledgments, or retransmissions. Latency might increase in these cases.

For more information on the calculation of ICA RTT, see How ICA RTT is calculated on NetScaler Insight. For more information about onboarding Citrix Gateway, see Gateway data source.

Session Availability

Session Availability is calculated based on the failure rate. It is the rate of failed session connections with respect to the total number of attempted session connections.

The Session Availability experience is categorized based on the session failure rate as follows:

Excellent: Failure rate is less than 10%. An excellent Session Availability factor indicates the users being able to successfully connect to and use the app or desktop.

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

Fair: Failure rate is 10–20%.

Poor: Failure rate is more than 20%. Many users with poor Session Availability experience indicate inability to connect and use sessions.

Since failure to launch sessions disrupts user productivity, it is an important factor in quantifying the overall user experience.



The rows in the Session Reliability drilldown table display the failure types categorized with the number of users and the number of failures in each category. Use the listed Failure types to further troubleshoot the failures.

For more information about the possible reasons within an identified failure type, see the Citrix Director failure reasons and troubleshooting.
document.

Session Resiliency

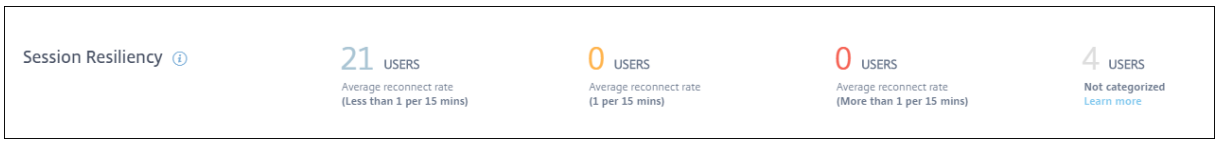
Session Resiliency indicates the number of times the Citrix Workspace™ app auto reconnected to recover from network disruptions. Auto reconnect keeps sessions active when network connectivity is interrupted. Users continue to see the application they are using until network connectivity resumes. An excellent Session Resiliency factor indicates a smooth user experience and lesser number of reconnects due to network disruptions.

Auto reconnect is enabled when the Session Reliability or the Auto Client Reconnect policies are in effect. When there is a network interruption on the endpoint, the following Auto reconnect policies come into effect:

- Session Reliability policy comes into effect (by default in 3 minutes) where the Citrix Workspace app tries to connect to the machine.
- Auto Client Reconnect policy comes into effect between 3 and 5 minutes where the endpoint tries to connect to the machine.

For each user, the number of auto reconnects are measured during every 15 min interval across the selected time period. Based on the number of auto reconnects in most of the 15 min intervals, the experience is classified as Excellent, Fair, or Poor.

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



The Session Resiliency experience is categorized based on the reconnect rate as follows:

Excellent: In most of the 15 min intervals in the chosen time period, there were no reconnects.

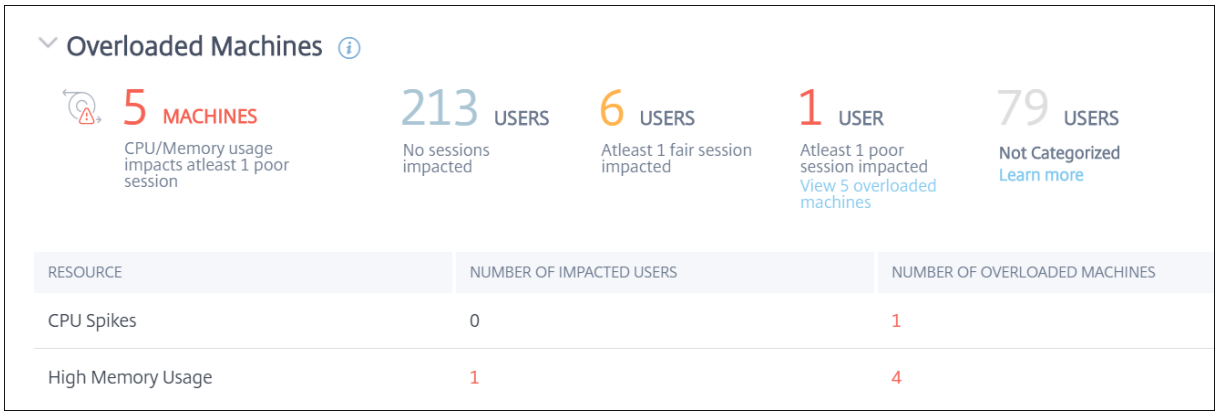
Fair: In most of the 15 min intervals in the chosen time period, there was one reconnect.

Poor: In most of the 15 min intervals in the chosen time period, there were more than 1 reconnects.

Overloaded Machines

Overloaded resources can cause high latency, high logon duration, and failures resulting in poor user experience. The **Overloaded Machines** factor gives visibility on overloaded resources causing poor experience.

Machines that have experienced sustained CPU spikes, or high memory usage, or both, that have lasted for 5 minutes or more, resulting in a poor user experience in the selected duration are considered to be overloaded.



> **Note:**
>
> The Overloaded Machines factor section is available only for the 2 hours, 12 hours and 1 day ranges. The feature is disabled for 1 week and 1 month time periods for optimization.

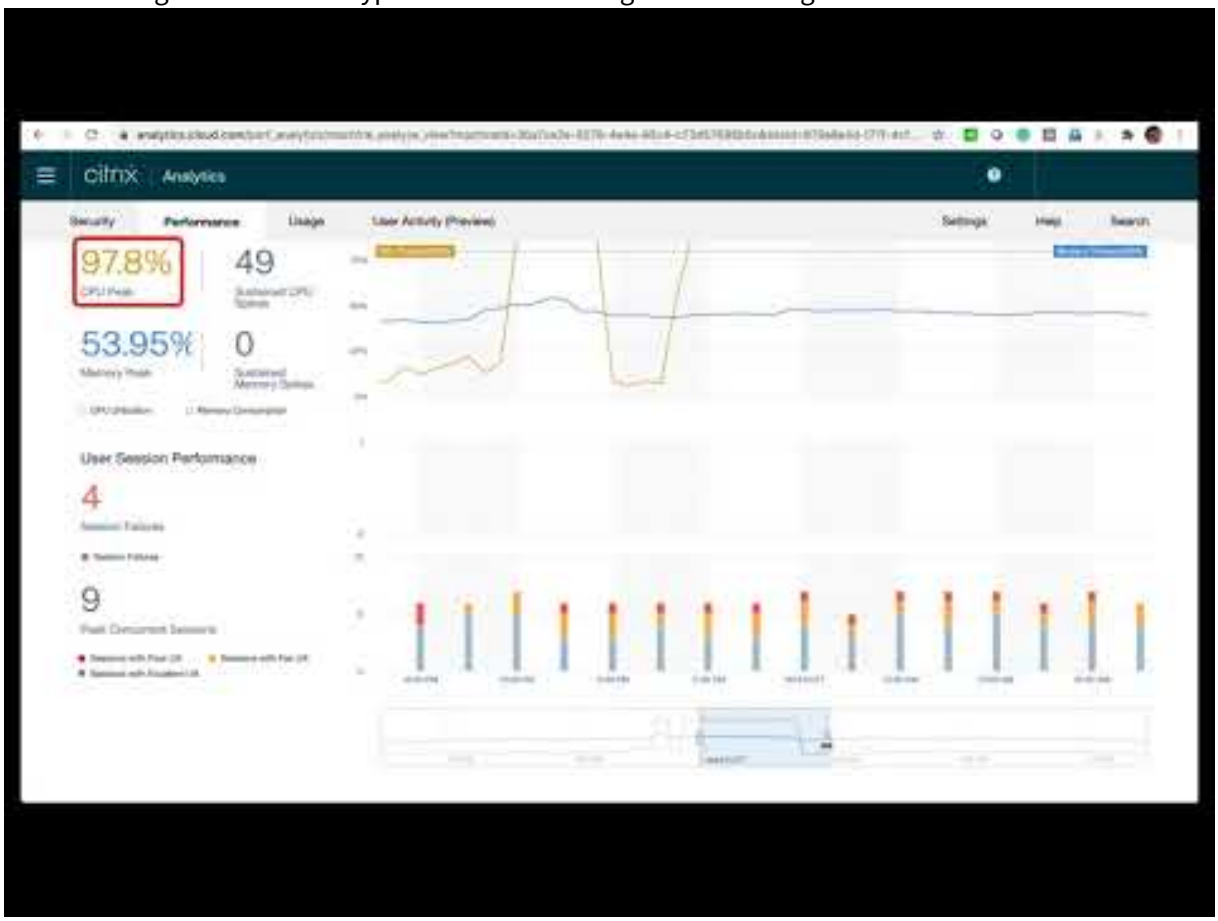
The **Overloaded Machines** section has the following data:

- The number of machines in which CPU or memory usage has impacted at least one poor session independent of the user experience.
- The number of users affected due to the impact of overloaded CPU or memory on the session experience.
    - Excellent –users with no sessions impacted by overloaded machines.

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

  - Fair –users with at least one fair session impacted by overloaded machines.
  - Poor –users with at least one poor session impacted by overloaded machines.
  - Not categorized –users whose session experience cannot be correlated with resource overload.
- Breakup of:
  - the number of machines affecting users with poor experience due to overloaded resource.
  - the number of users with poor experience impacted by CPU Spikes and High memory usage.
- Clicking the number of overloaded users leads to the Users self-service view filtered to show users whose sessions are affected by the overloaded resources.
- Clicking the number of overloaded machines leads to the Machines self-service view filtered to show the chosen set of overloaded machines - based on classification, or based on the overloaded resource, CPU, or machine.

The following video shows a typical troubleshooting scenario using the Overloaded Machines factor.



The Machines, Users, and Sessions self-service views are enhanced with the Overloaded Machines facet. The Machines self-service view additionally has the Overloaded CPU/Memory facet to help

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

troubleshoot overload issues in machines. For more information, see Overloaded Machines in the Self-service article.

Further drilldown from the Machines self-service view to see specific machine statistics to troubleshoot the resource overload issues.

Infrastructure Analytics

September 1, 2025

What is Infrastructure Analytics?

The Infrastructure analytics from Citrix Analytics for Performance™ provides insights into the status of key components in your Apps and Desktops sites.

- You can view the health and status of multiple machines on a single dashboard.
- You can view the analytics of machines in a single site or get a cohesive view across all sites.
- You can view the analytics across selected single or multi-session OS Delivery Groups.
- You can view machine usage trends over a period based on its availability and performance.

This data enables you to take better-informed decisions about capacity management, perform analysis and risk assessment of your Sites. Thus, you can proactively take necessary actions to minimize critical failures and optimize the usage and performance of your Sites.

Machine Availability provides information about single and multi-session OS machines. You can view the current availability of machines across your environment. You can see the distribution of machines in available and unavailable states across the selected sites and Delivery Groups.
The Aggregate State of machines is also plotted alongside Session Availability across the chosen time interval.

Machine Performance provides information about the performance of multi-session OS machines only.

You can use the custom time selection filter to view the machine availability and machine performance of machines for a specific time period.

How to access the Infrastructure dashboard

To view the Infrastructure dashboard:

1. Log on to Citrix Cloud™ and select your Cloud Customer.

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

2. On the Citrix Analytics service tile, click **Manage**.
3. Citrix Analytics service opens, click the **Performance** tab.
4. Click the **Infrastructure** tab.

How to use the Infrastructure dashboard

The Infrastructure dashboard provides the detailed status of the machines deployed across the sites.

As an administrator, if you manage and monitor few sites for your organization, you can use the Infrastructure dashboard to get insights into the availability and performance of machines across the Delivery Groups in all the sites. This information helps take infrastructure decisions proactively to improve the user experience while also keeping track of optimum usage and infrastructure cost reduction.

Current Machine Availability

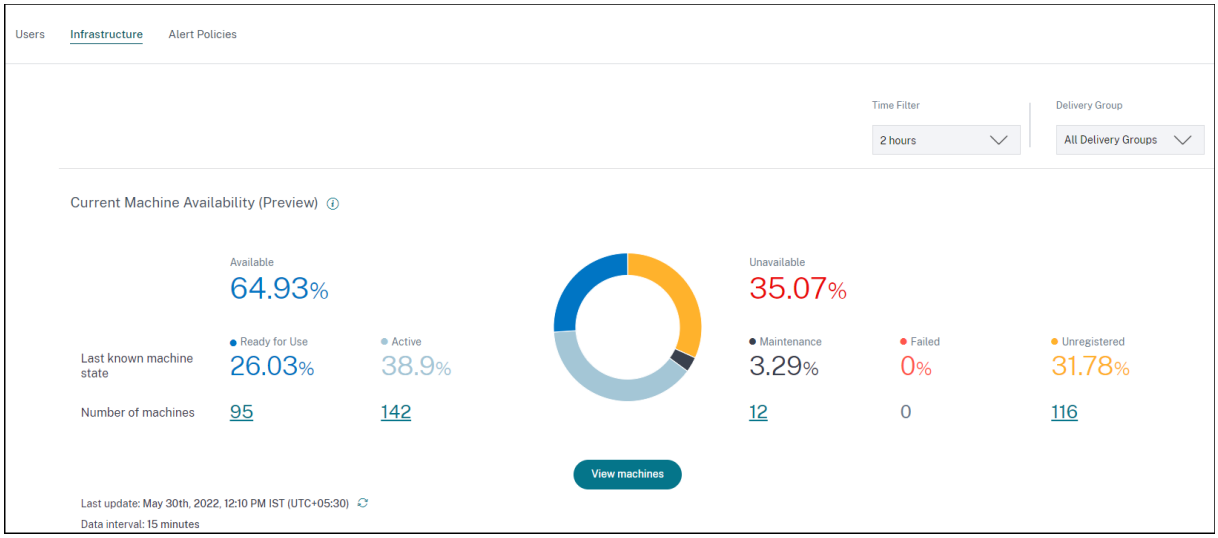
> **Note:**
>
> **Current Machine Availability** is under Preview.

The Current Machine Availability panel provides the availability of machines in the last 15 minutes. A breakup of machine count is displayed per state under the Available and Unavailable Category.

Note that machine availability does not ensure service availability as the service is also dependent on other factors. This information helps determine the availability of provisioned machines to serve sessions.

The machine count and percentage in each last known machine state is displayed. The machine count does not include machines which are in a catalog but are not yet assigned to a delivery group. Clicking the machine count opens the Machines self-service page. This view lists the machines in the specific state with further details for each machine during the last 15 minutes.

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



Available Machines: You can view the percentage of machines that were available in the last 15 minutes in the selected sites and Delivery Groups. Available Machines are in the following states:

- Ready for use (single and multi-session machines): These machines have no active sessions. The machines are in healthy state.
- Active (single and multi-session): In this state, the machine has at least one active session. New sessions cannot be launched on single-session OS machines in the active state. On multi-session OS machines, new sessions can be launched depending on the machine capacity. Active machines number also includes the machines on which all sessions have been disconnected.

Unavailable Machines: You can view the percentage of machines that were unavailable in the last 15 minutes in the selected sites and Delivery Groups. You can use this information to optimize machine utilization across your environment. Unavailable Machines are in the following states:

- Unregistered: Machine is not registered with the Broker Service.
- Failed: Machine failed to start.
- Maintenance: Machine is in maintenance mode, no new connections are allowed. These are the machines which were registered in healthy state and are now in maintenance. Machines that weren't registered are counted as an Unregistered machines.

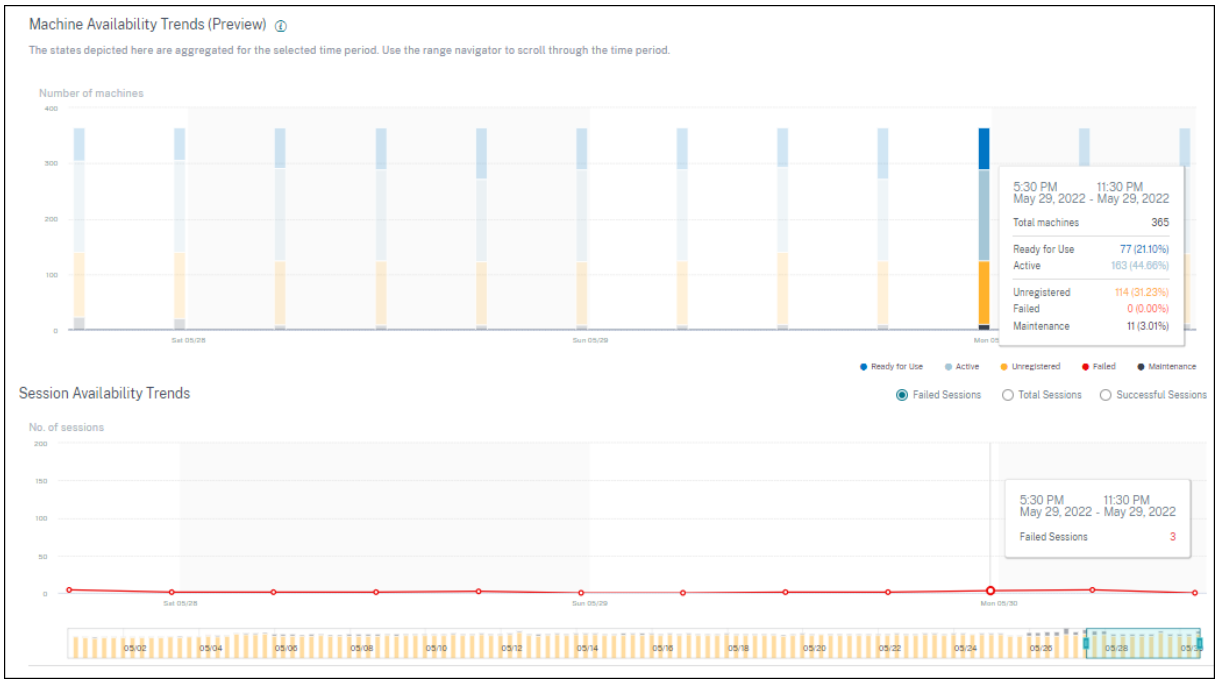
View Machines takes you to the Machines self-service page showing all the machines in the environment. For more information, see the Self-Service search for Machines.

Machine Availability and Session Availability Trends

> **Note:**
>
> **Machine Availability Trends** is under Preview.

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

The Machine Availability trend shows the Aggregate State of machines plotted across the selected period. The machine state is aggregated to consider the least favorable state from among Ready for use, Active, Maintenance, Unregistered and Failed in that order.



You can drill down from a specific section on the graph to view the details of the machines in a specific state in the Machine self-service view. On the Session Availability trend, you can choose from among Successful, Failed, and Total sessions to be plotted for the selected period.
Trends for one-month and one-week periods are plotted with a 6-hour granularity. You can zoom into the one-month Machine and Sessions Availability trends using the time navigator in a range of 3-7 days.

The time navigator also reflects the machine availability trends. This helps you identify time periods with a large number of unavailable machines, so you can easily navigate and zoom into the required period in the Machine availability trend.
You can use the synchronized tool tips on the Machines and Sessions Availability trends to understand the correlation between unavailable machines and failed sessions.

Troubleshooting Machines Unregistered and failed machines can become unusable for the following reasons:

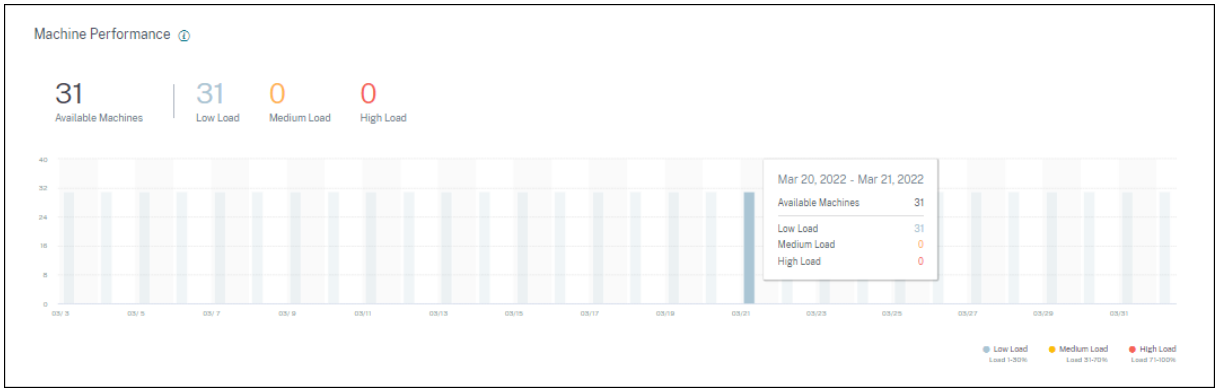
- The machine fails to communicate with the Delivery Controller.
- Broker Service experiences issues while creating a session prepare request.
- Network issues that resulted in the machine not accepting the session prepare request.
- A timeout occurs when the machine is attempting to register with the Delivery Controller.

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

- The machine might not be powered on for session launch.
- Delivery Controller sends a request to the machine to prepare for a connection from an end user but the machine actively refuses the request.
- Delivery Controller does not send the required configuration data, such as policy settings and session information to the machine during session launch.
- The machine is removed from the Delivery Group.
- The machine is not registered.
- Machine is in unavailable power state.
- The machine is experiencing internal issues.
- The machine fails to connect and register with the Cloud Connector or Delivery Controller.
- The machine is powered off or shut down.

Machine Performance

The **Machine Performance** panel shows the distribution of machines based on the load.



This information is available only for multi-session OS machines. You can view the number of machines in usable state categorized based on the load evaluator index such as high, medium, and low for the chosen selected time period, Site, and Delivery Groups.

The graph displays machines plotted based on the categorization as high, medium, and low load over the selected duration. Hover over the bar graph to view the detailed status of the usable machines at a given time. You can monitor the load distribution trends across the machines over a time period.

The load evaluator index for a machine is the maximum value of the individual indexes that are enabled such as session count, CPU plus five percent of the average of the other enabled indexes. Based on the load evaluator index, you can configure load management between servers delivering Windows Server OS machines. For more information, see Load management policy settings.

Machine load is categorized as follows:

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

- High load: Load more than 70%
- Medium load: Load between 30% to 70%
- Low load: Load less than 30%

For information about how the load evaluator index is calculated, see Knowledge Center article CTX202150.

Connector Statistics

September 1, 2025

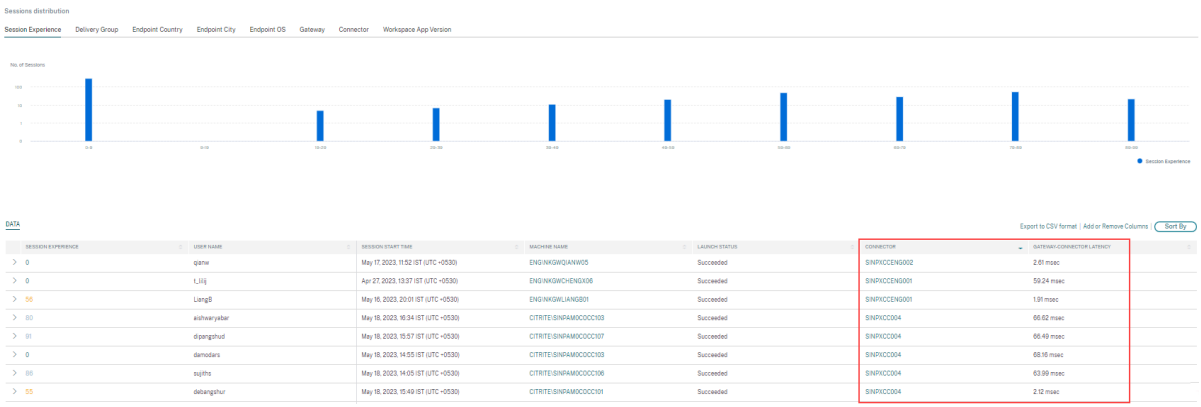
The Connector statistics page provides a comprehensive view of the resource consumption on the selected connector during the last 24 hours. This information helps administrators correlate high CPU, memory, or bandwidth usage occurrences on the connector with session failures and experience across the sessions.

The page displays the synthetic latency calculated from the connector to the Gateway PoPs in your virtual apps and desktops environment. This information helps you choose and configure the closest Gateway PoP to achieve the optimum session experience.

> **Note:**
>
> Connector Statistics are not available for sessions connected using the Rendezvous protocol. This is because the Rendezvous protocol allows machines to bypass the Citrix Cloud Connectors to connect directly and securely with the Citrix Cloud control plane. For more information, see Rendezvous protocol.

Accessing the Connector statistics page

Click the connector name link from the Self-service view for Sessions.

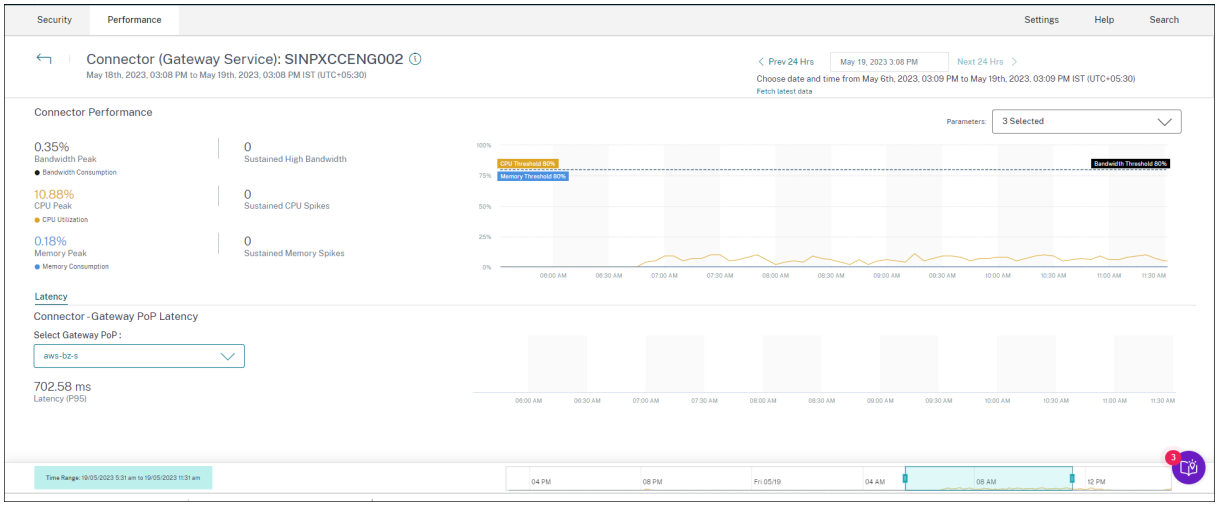


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using the Connector statistics page

The Connector Statistics page displays usage statistics of connector resources-bandwidth, CPU, and memory in a single view. This helps corelate the usage pattern of connector resources with high latency and poor session performance occurrences.

The latency values from Connector to Gateway PoPs help you choose and configure the closest Gateway PoP to achieve the optimum session experience.



The Connector Statistics page displays data for the last 24 hours, by default. However, data is available for the last 14 days. To choose a different 24 hour period, use the calendar. Data is displayed for the last 24 hours from the time you choose.

Connector Performance

Key parameters that define the connector resource usage are displayed. You can choose the parameters to be displayed from CPU, Bandwidth, and Memory.

- **Bandwidth Peak** represents the maximum bandwidth consumption in the connector in the last 24 hrs.
- **Sustained High Bandwidth** represents the number of times Bandwidth consumption crossed the Bandwidth threshold of 80% and sustained for 5 minutes or more.
- **CPU Peak** represents the maximum CPU utilization in the connector in the last 24 hrs.
- **Sustained CPU Spikes** represents the number of times CPU utilization crossed the CPU threshold of 80% and sustained for 5 minutes or more.
- **Memory Peak** represents the maximum memory consumption in the last 24 hrs.
- **Sustained Memory Spikes** represents the number of times memory consumption crossed the memory threshold of 80% and sustained for 5 minutes or more.

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

The peak percentage of each metric consumed in the connector is plotted over the 24 hour period available at a 5 minute granularity. This Connector Performance trend helps admins correlate issues of session failures and poor latency due to high resource consumption on the connector.

Connector Performance trends are plotted for a default 4-hour window. To view data corresponding to any other window in the 24-hour range, move the time navigation bars and choose a different time range. You can zoom in or out in a 6 hour window, to view the events corresponding to the selected time range.

Latency

Connector - Gateway PoP Latency represents the average value of synthetic latency calculated for the selected Gateway PoP in your virtual apps and desktops environment.

Typical use case

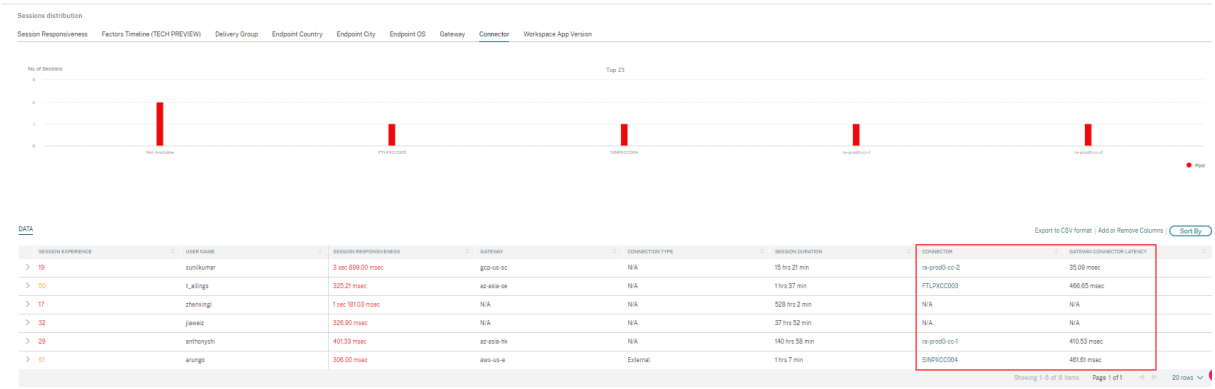
Connector Statistics view can be used to find out if high resource consumption on connectors is leading to sessions failures and high latency.

Click the sessions with poor Session Responsiveness on the User Experience dashboard.



The Sessions self-service view is displayed with the details of the sessions having poor session responsiveness.

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



You can use the **Connector** pivot to see the distribution of sessions with poor responsiveness across the various connectors. Click the **Add or Remove Columns** link to add the **Connector** and **Gateway-Connector** columns to your view. Click the connector link to open the **Connector Statistics view**.



This view helps identify instances of high resource consumption on the connector and understand if they might cause poor responsiveness.

The Connector - Gateway PoP Latency value in the Latency tab shows average value of synthetic latency calculated for selected Gateway PoPs in your virtual apps and desktops environment. This information helps you choose and configure the closest Gateway PoP to achieve the optimum session experience.

Session Details

September 1, 2025

The Session Details page provides a holistic view of the performance metrics of the selected session. Comprehensive session details and factors affecting the session performance are displayed for the session duration. This view gives visibility into session factors like ICARTT, Session Reconnects, bandwidth metrics, network latency, and endpoint network metrics. These factors are plotted along with

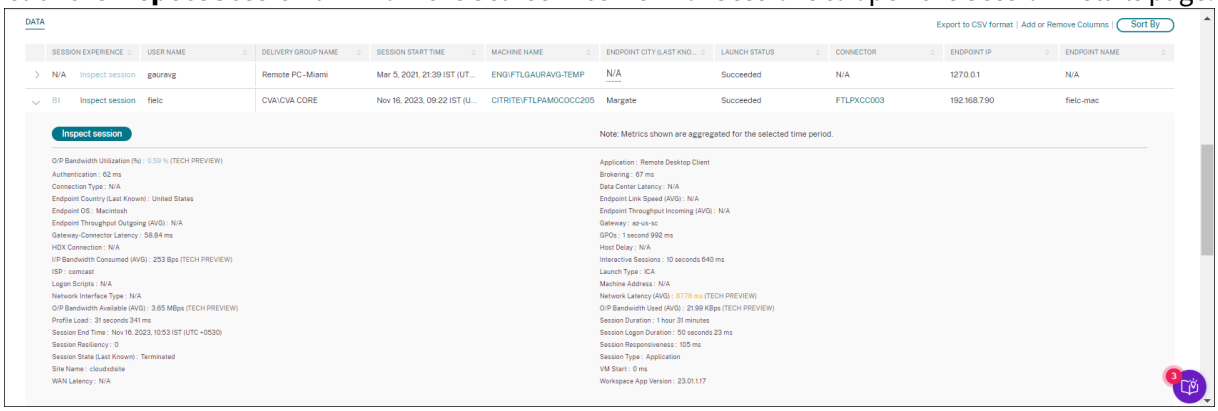
© 1997–2026 Citrix Systems, Inc. All rights reserved.

the Session Score for the selected period. The Session Details view helps correlate the impact of available bandwidth and network latency on ICARTT and Session Score.

> **Notes:**
>
> - You need endpoints running Citrix Workspace™ app for Windows version 7 2108 or later to view Endpoint Network metrics.
> - You need machines running Citrix Virtual Apps and Desktops™ 7 2112 or later on Citrix DaaS to view the bandwidth and network latency metrics.
> - You must have the **VDA data collection for Analytics** policy 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 Analytics.

Accessing the Session Details page

Click the **Inspect Session** link from the Self-service view for Sessions to open the Session Details page.



Using the Session Details page

The Session Details page displays statistics of the session like the ICARTT, Session Reconnects, Network Latency, Bandwidth, and Endpoint Network metrics on a single view. This information helps correlate the session performance with these factors.

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



The Session Statistics page displays data for up to 72 hours of the session duration.

Session Score and the other session performance and factors metric charts take into account the disconnected duration of the session. This consideration enables the overall Session Score and associated metrics to be an accurate representation of the session performance. The duration for which the session is disconnected is represented in the all charts and tooltips.

Session attributes

Key session attributes are displayed as follows:

- User name
- Session status
- Session Duration
- Logon Duration
- Delivery Group
- Site
- The machine on which the session was launched. Click the machine name link to see the corresponding Machine Statistics page.
- ISP
- Endpoint Link Speed (Avg)
- Endpoint Location

Session Performance

The key parameters that define the session performance displayed here are as follows:

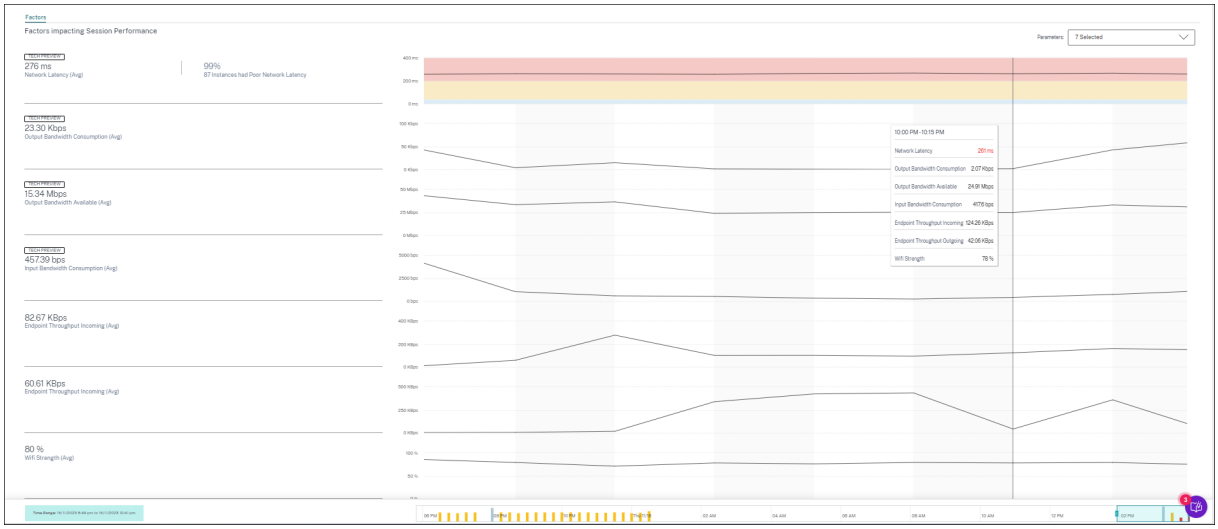
- The average Session Score, ICARTT measurement, and Session Reconnects measurement

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

- The percentage values of session duration during which Poor Session Score, High ICARTT, and High Reconnect Rate was experienced
- The number of instances (of 15 min duration) during which Poor Session Score, High ICARTT, and High Reconnect Rate was experienced
- The average values of Session Score, ICARTT, and Session Reconnects plotted over the session duration at a 5 min granularity.
  The graphs are color-coded to indicate the performance of individual factors. You can choose the parameters to be displayed from Session Score, ICARTT, and Session Reconnects.

Factors (Preview)

This section displays measurements of bandwidth, network latency, and endpoint throughput factors that impact the session performance. Average values of Network Latency, Output Bandwidth Consumption, Output Bandwidth Available, Input Bandwidth Consumption, WiFi Signal Strength, Endpoint Throughput Incoming, and Endpoint Throughput Outgoing are listed. The metrics are available out-of-box and do not require any specific configuration.



The metrics are plotted over the session duration with 15-minute granularity. You can choose the parameters you want to see in this section. These graphs are color-coded to indicate if the factors were excellent, fair, or poor.

All the trends are plotted for a default 4-hour window. To view data corresponding to any other window during the session duration, move the time navigation bars and choose a different time range. You can zoom in or out in a 6-hour window, to view the events corresponding to the selected time range.

The bandwidth, network latency, and endpoint throughput metrics and trends help analyze the session performance with respect to the individual parameter performance. It helps identify a specific factor that might be affecting the session performance.

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

Typical use case

Session Details view can be used to triage a specific factor that might be causing poor session performance. All the details pertaining to a launched session in the selected duration are available on the details view.

1. You can start from the Poor Sessions number in the Session Responsiveness section of the User Experience dashboard.
2. The Sessions self-service view is displayed with the details of the sessions having poor session responsiveness.
3. Choose Session Responsiveness as the factor to view the sessions. Choose Factors Timeline as the pivot. The graph shows the distribution of sessions based on the Output Bandwidth Usage, Network Latency, and ICARTT.
4. On the tabular view, expand the selected session row to see all the metrics related to the session. The bandwidth, latency, and endpoint throughput metrics are listed here.
5. Click the session score to open the Session Details view. Analyze the view over the required interval to identify the factor causing poor session experience.
6. Use the graphs to identify the factors that might be causing poor session experience.
7. You can compare the overall throughput consumption with the endpoint link speed and the bandwidth consumption to spot if a user was probably running a bandwidth-intensive application outside the HDX™ channel resulting in poor session experience.
8. You can identify if a drop in the WiFi signal strength led to a poor session experience.

Machine Statistics

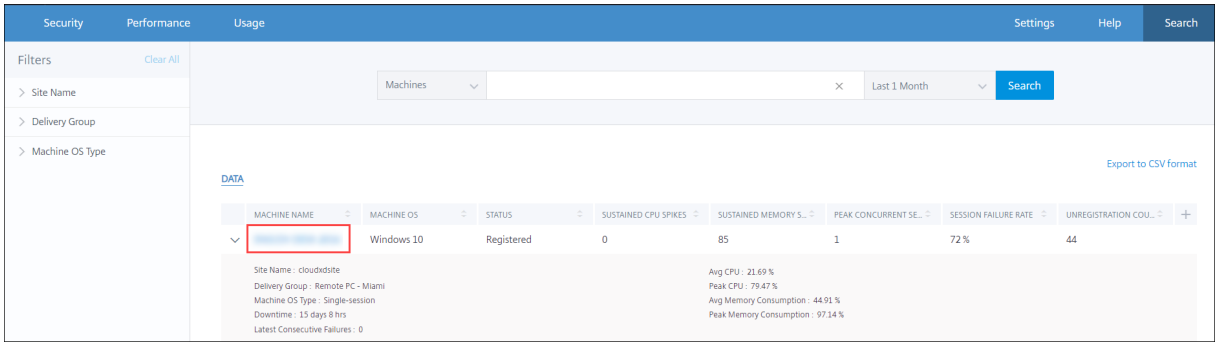
September 11, 2025

The Machine statistics page provides a comprehensive view of resource consumption and session experience on the selected machine during the last 24 hours. This information helps administrators correlate high CPU or memory usage occurrences with session failures and experience across the machines in their Apps and Desktops environment. Administrators can view the processes contributing to high resource consumption and get a timeline view of the machine states. This feature helps slice and dice important parameters concerning the machines in the environment and spot inefficiencies easily.

Accessing the Machine statistics page

Click the machine name link from the Self-service view for Machines.

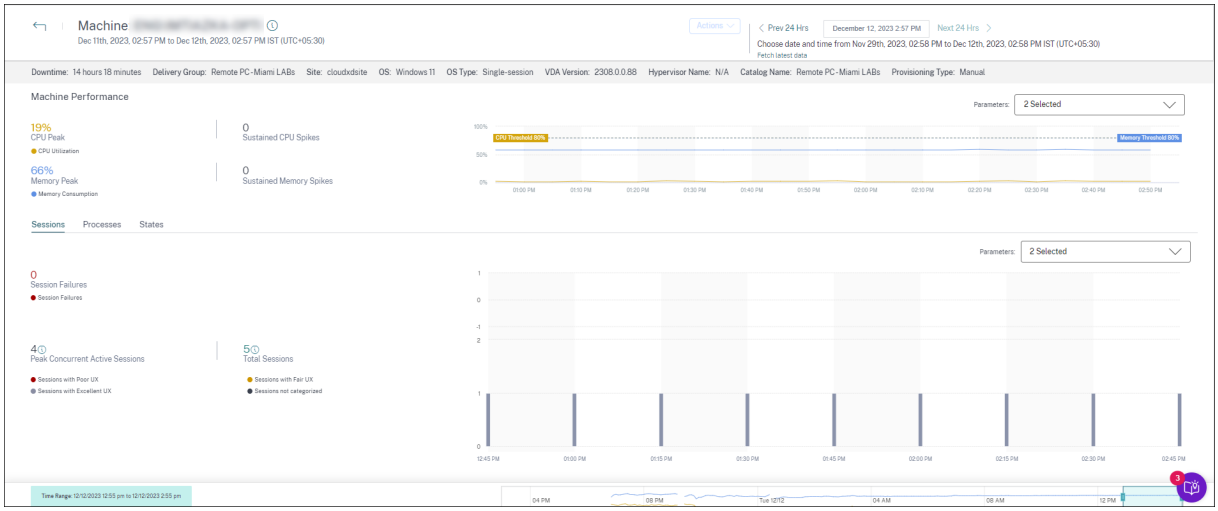
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Using the Machine statistics page

The Machine Statistics page displays the machine and session performance statistics in the same view. This view helps analyze machine resources, their usage pattern, and understand if machine resources might have been the bottleneck for poor performance.

The Machine Statistics page displays data for the last 24 hours, by default. However, data is available for the last 14 days. To choose a different 24 hour period, use the calendar. Data is displayed for the last 24 hours from the time that you choose.



Machine attributes

Key machine attributes are displayed.

- Delivery Group, Site, OS type, OS, VDA version, Hypervisor, Catalog, and Provisioning type of the machine are displayed.
- Downtime shows the period in seconds during which the machine was in `Unregistered`, `Failed`, or `Powered off` state in the last 24 hours.

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

Machine Performance statistics

Key metrics that define the machine performance are displayed.

- **CPU Peak** represents the maximum CPU utilization in the machine in the last 24 hrs.
- **Sustained CPU Spikes** represents the number of times CPU utilization crossed the CPU threshold of 80% and sustained for 5 minutes or more.
- **Memory Peak** represents the maximum memory consumption in the last 24 hrs.
- **Sustained Memory Spikes** represents the number of times memory consumption crossed the memory threshold of 80% and sustained for 5 minutes or more.
- The **Machine Performance trend** for a default 4 hour window in the last 24 hours shows CPU utilization and memory consumption plotted at 5 min granularity.

Session Performance Statistics

Key session performance related metrics are displayed.

- **Session Failures** that occurred on the machine over the last 24 hours.
- **Session Failure trend** displays the session failures count plotted for a default 4 hour window in the last 24 hours.
- **Peak Concurrent Active Sessions** represents the maximum number of concurrent sessions that were established on the machine over the past 24 hours.
- **Total Sessions** represents the total number of sessions that were active during the selected time period on the machine. Clicking the Total Sessions number opens the Sessions self-service view with the corresponding set of sessions displayed. You can further drilldown and inspect the session metrics from the Session Details view.
- The **User Session Performance trend** shows the classification of sessions based on session experience as Excellent, Fair, or Poor, plotted for a default 4-hour window in the last 24 hours.

You can click the **Session Failure number**, the bars in the chart displaying the session failures, and the categorized session counts to view the sessions in the Sessions self-service view.

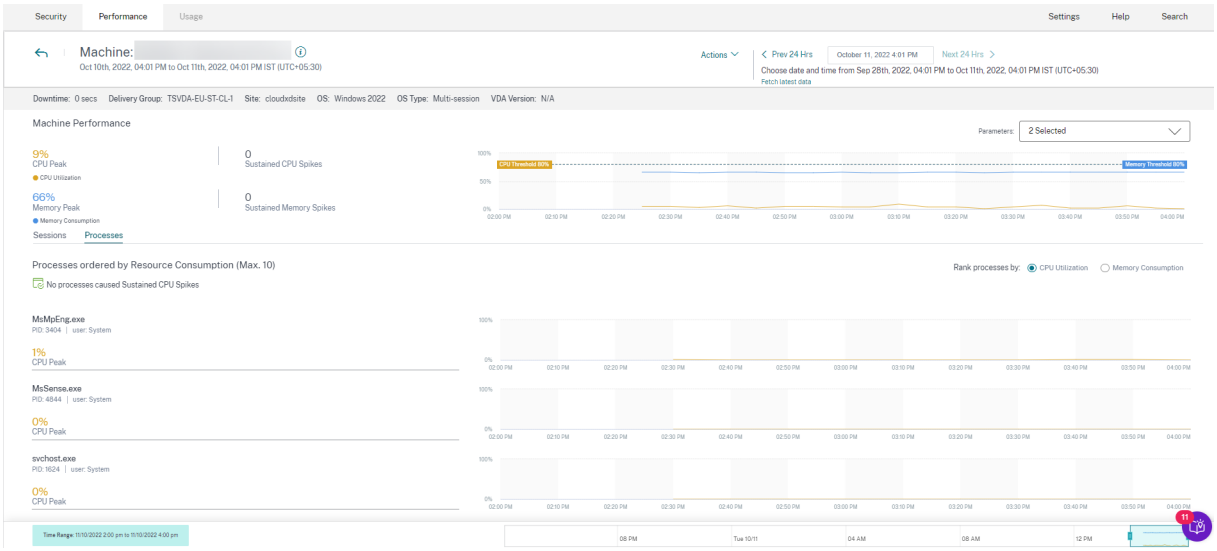
Machine Statistics a comprehensive view displaying all machine-related metrics required to triage and fix issues related to the machine and the sessions running on the machine.

Top resource consuming processes

Click the **Processes** tab to gain visibility into the high resource consuming processes running on the machine in the selected time period. You must enable the Process Monitoring policy from Citrix Studio to see this information. This feature is available multi-session and single-session OS machines on cloud and on-premises sites.

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

You can choose to view the processes ranked as per **CPU Utilization** or **Memory Consumption**.

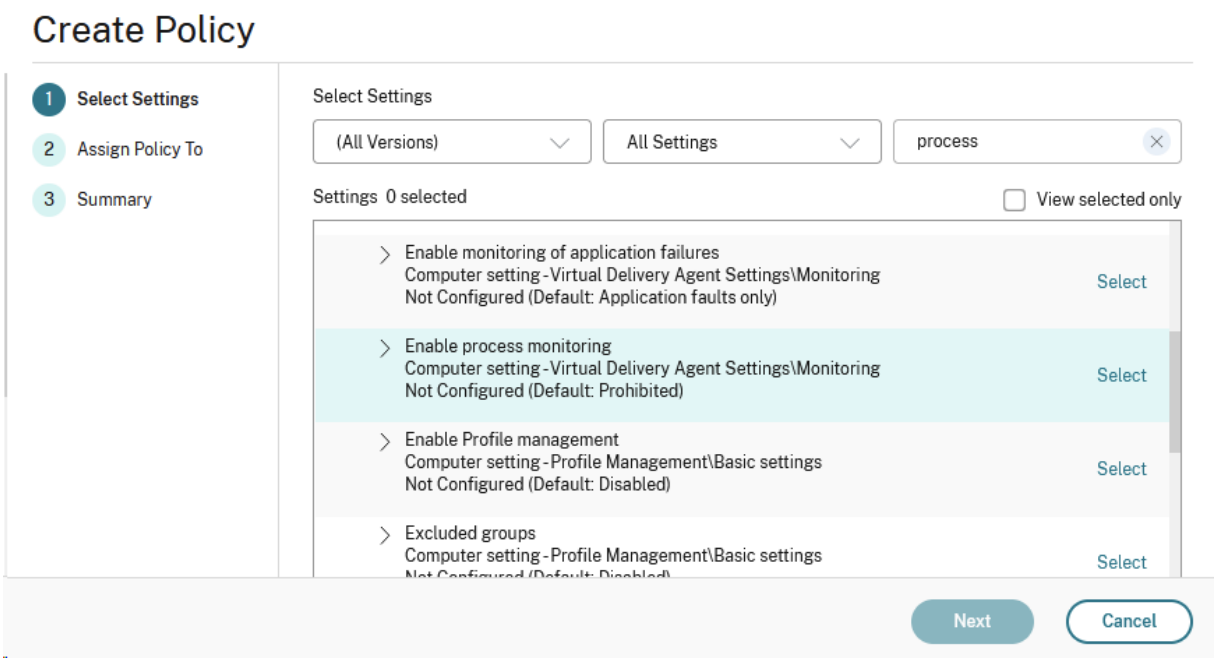


Up to 10 **Most Resource Consuming Processes** are displayed with percentage CPU or Memory Peak as selected. These are processes that caused sustained CPU or Memory spikes coinciding with high resource consumption on the corresponding machine. The top resource consuming processes are displayed even if there are no memory or CPU spikes during the selected time period.

The charts plot CPU Utilization or Memory Consumption by the process across the selected time period. This helps correlate resource consumption by the processes with session failures on the machine.

Process visibility is available for multi-session OS machines and single-session OS machines on cloud and on-premises sites. This feature requires that you enable the **Process Monitoring policy** from Citrix Studio. This policy is disabled by default. You must enable it explicitly to view the processes running on the machine in Performance Analytics.

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



For more information, see Monitoring policy settings

Note:

- In the case of on-premises sites, machines running **Citrix Virtual Apps and Desktops™ Version 2203** and later are supported.
- It is recommended that you enable process data to Citrix Analytics for Performance only and you enable process data to Director only if needed. For more information about the approximate storage consumption if you choose to enable process data flow to Director, see Process Data.

Use the following PowerShell cmdlet to control the flow of process data.

- To enable process data flow only to Citrix Analytics for Performance™ and not to Director (recommended)

```
Set-MonitorConfiguration SendProcessDataToCASAndSkipDatabase $true
```

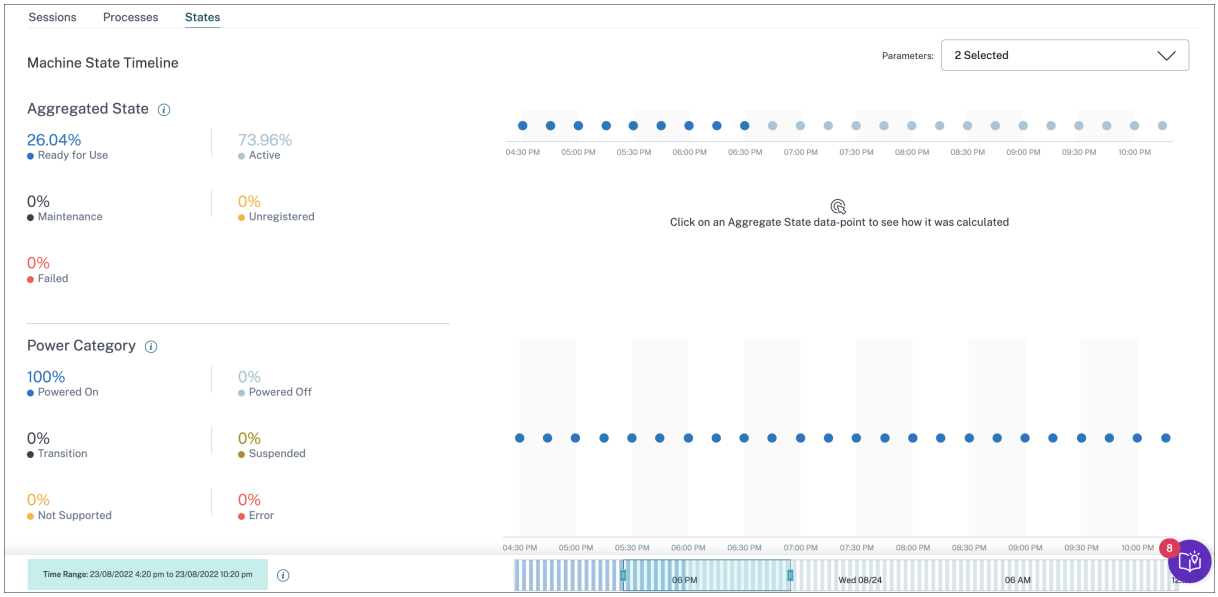
- To enable process data flow to both Citrix Analytics for Performance and Director.

```
Set-MonitorConfiguration -SendProcessDataToCASAndDatabase $true
```

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

Machine State Visibility

The Machine Statistics page now includes information on Machine States. The **States** tab shows the timeline of Machine Aggregated State and Machine Power Category for the last 24 hours. The plotting is done at 15 min intervals. This feature helps slice and dice important parameters concerning the machines in the environment and spot inefficiencies easily.



Click an Aggregated State data point to see how it was calculated. A breakdown of the actual values of Machine State and Maintenance Mode that resulted in the plotted Aggregated State is displayed. This helps comprehend the machine's state changes over time. Failure Type and Deregistration Reason help debug machine issues.
Hover over the Power Category data point to see the actual Power State that the machine has been in.

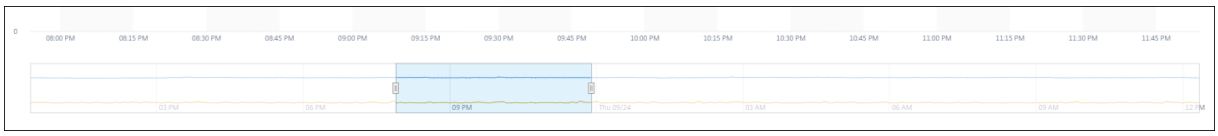
Time navigation bar

The Time navigation bar has the following charts plotted for a default 4-hour window:

- The Machine and User Session Performance trends are plotted when you are in the Sessions or Processes tab
- The Machine Aggregated State trend is plotted when you are in the States tab.

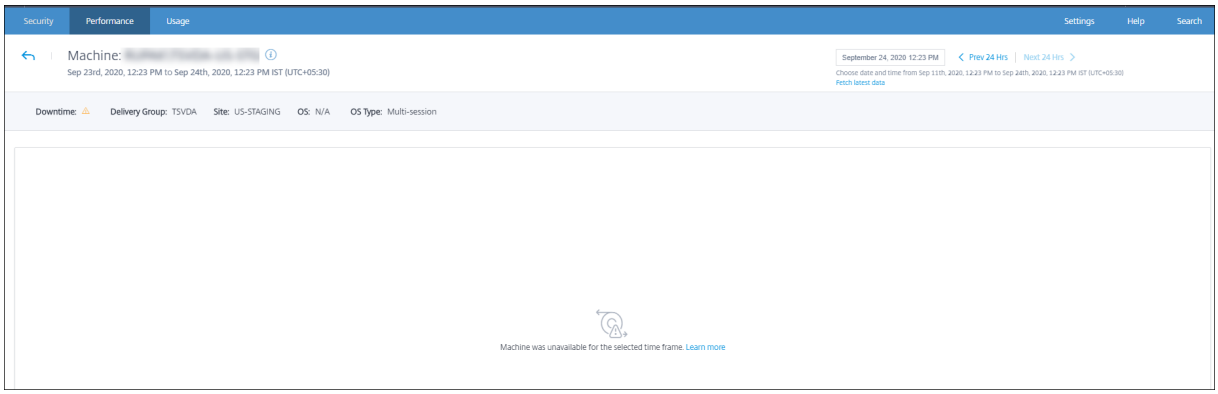
This helps get an overview of the trend and then zoom in to the interested time range. To view data corresponding to any other window in the 24-hour range, move the time navigation bars and choose a different time range. You can zoom in or out in a 2–8 hour window, to view the events corresponding to the selected time range.

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



Usage Notes

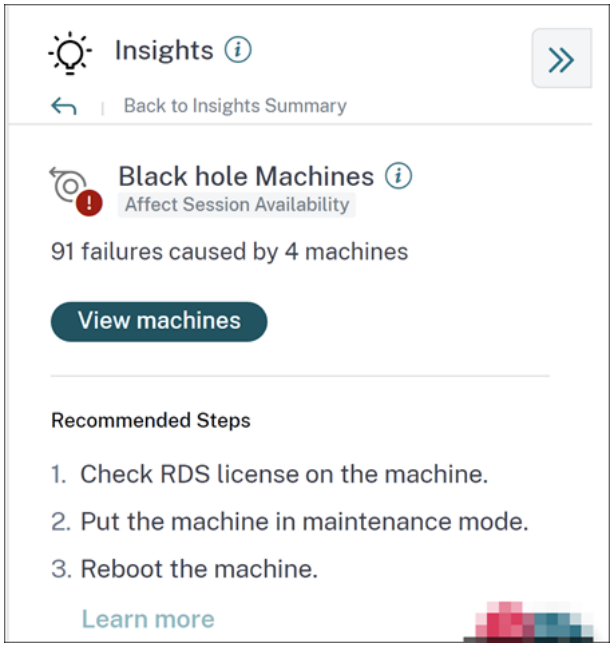
- Machine downtime might cause disrupted plotting of the Machine Performance trend.
- If machines in your on-premises Virtual Apps and Desktops environment were added to the machine catalog before the site was onboarded to Performance Analytics, the OS information of the machine might not be available in the Machine Statistics view. As a workaround, add the machines to the machine catalog after the onboarding the site.
- Statistics of machines in your on-premises Virtual Apps and Desktops environment are available (up to) 24 hours after the onboarding to Performance Analytics has been initiated.
- The Machine Performance trend is not available for the duration when the machine was in `Unregistered`, `Failed`, `Powered off` status, or if it was deleted from the Delivery Group. Statistics are available only for the period when the machine was available.
- To determine why a machine was not in the `Active` or the `Ready for Use` state, click the dotted chart of the Machine Aggregated State trend in the State tab.



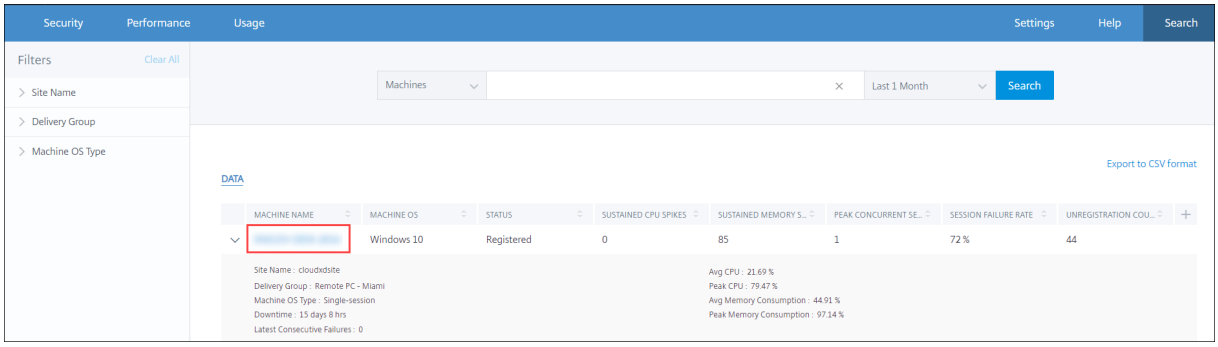
Typical use case for Machine Statistics view

The Machine statistics view provides information to troubleshoot a machine comprehensively.
Let us understand the usage of this view with a typical use case starting from the User Experience Dashboard.
The **Failure insights** panel on the User Experience Dashboard, provides a list of black hole machines that resulted in three or more consecutive session failures.

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

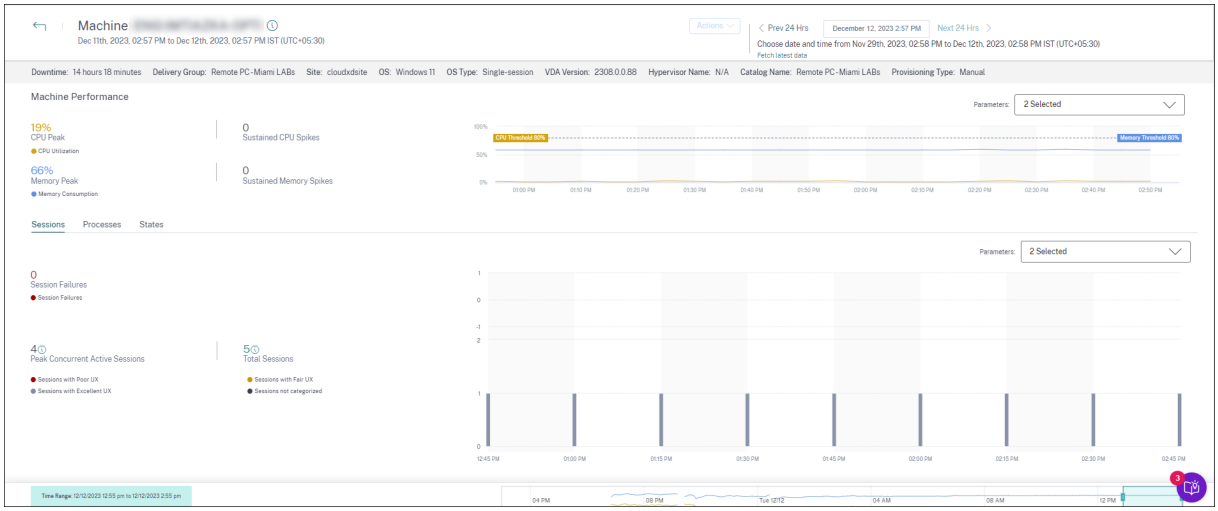


Clicking the black hole machines link leads you to the Machines based self-service view. This view lists all the metrics related to the black hole machines such as the downtime, peak CPU, and peak memory.

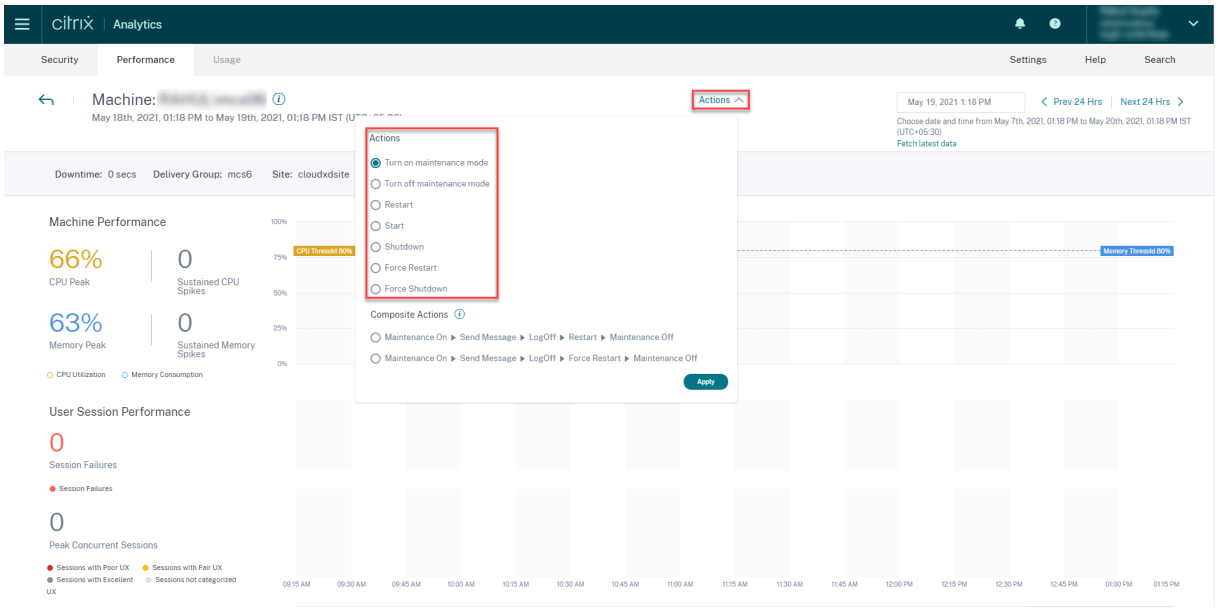


Click a machine name in the self-service view for Machines to display the Machine statistics page. This page displays the machine, session performance, and process resource parameters plotted for the same time range. You can use this information to compare resource usage at the time of session failures and get insights on the possibility of resource crunch being a cause for failures.

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



Machine Actions and Composite Actions



Machine Actions

Machine Actions are available on power managed machines in your Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) sites on cloud. Admins with Full Administrator access can perform the following actions on the machines:

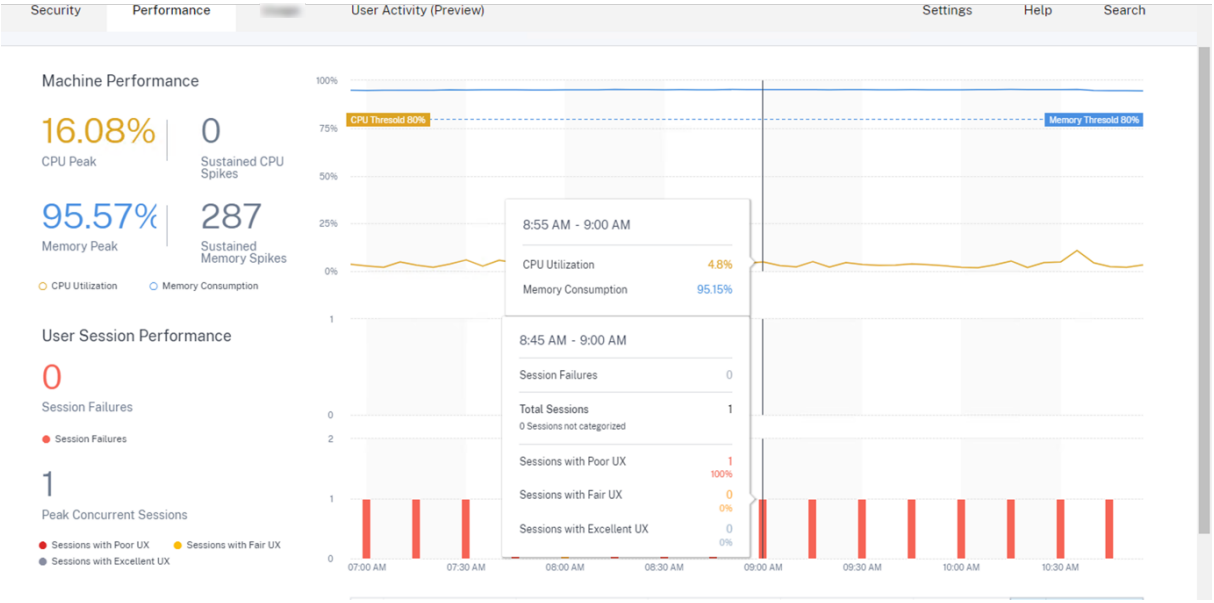
- Turn on maintenance mode
- Turn off maintenance mode
- Restart machine
- Start machine

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

- Shutdown machine
- Force restart machine
- Force shut down machine

> **Note:**
>
> The **Machine Actions** option is visible for all machines. However, it works only on MCS or power-managed machines.
> The **Machine Actions** are disabled for machines hosted on on-premises sites.

Typical use case for Machine Actions Machine actions help resolve poor user experience.
If a machine is impacted due to high memory usage, you can understand the exact nature of the issue in the Machines self-service view.
The Machines self-service view displays the OS, the number of memory spikes, and CPU spikes over a period. You can click individual machines to see the correlation between the resources and the session experience in the Machine Statistics page. A sample screenshot is given here.



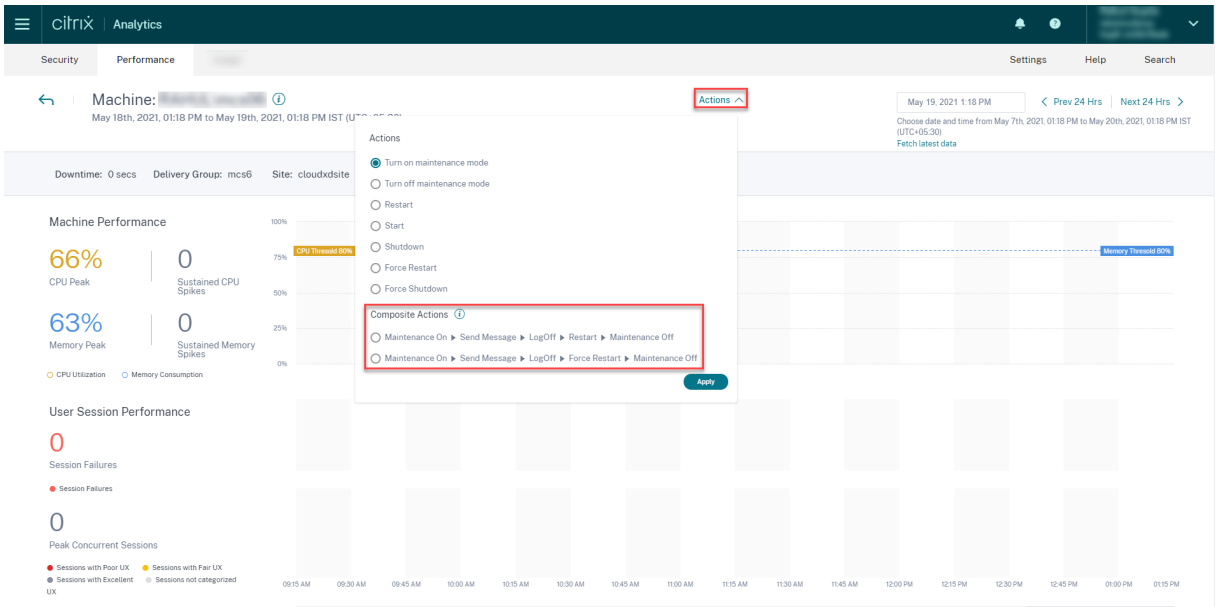
As a full administrator, you can put the machine in maintenance so that no more connections or sessions are allowed on this machine. You can then restart the machine or perform other troubleshooting procedures to free up the memory.

You can perform all these actions from within the Machine Statistics view instead of navigating to Web Studio or Citrix Director.

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

Composite Actions

Composite Actions help perform a sequence of machine actions in a single click from the Machine Statistics view.



You can use one of the following two sequences of **Composite Actions**.

- Maintenance On > Send Message > Logoff > Restart > > Maintenance Off**

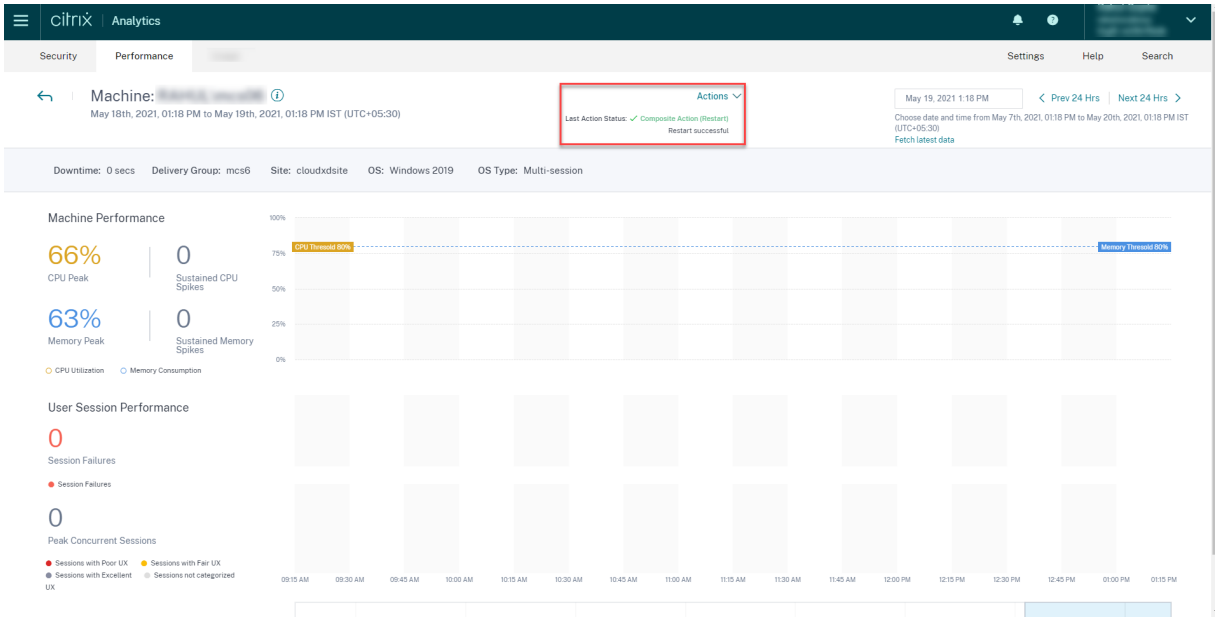
    1. Move the machine to Maintenance On mode.
    2. Send restart warning messages to all users logged into the machine.
    3. Wait for a timeout of 30 minutes or wait for all users to log off.
    4. Restart the machine.
    5. Move the machine to Maintenance Off mode.

- Maintenance On > Send Message > Logoff > Force Restart » Maintenance Off

    1. Move the machine to Maintenance On mode.
    2. Send restart warning messages to all users logged into the machine.
    3. Wait for a timeout of 30 minutes or wait for all users to log off.
    4. Force restart the machine.
    5. Move the machine to Maintenance Off mode.

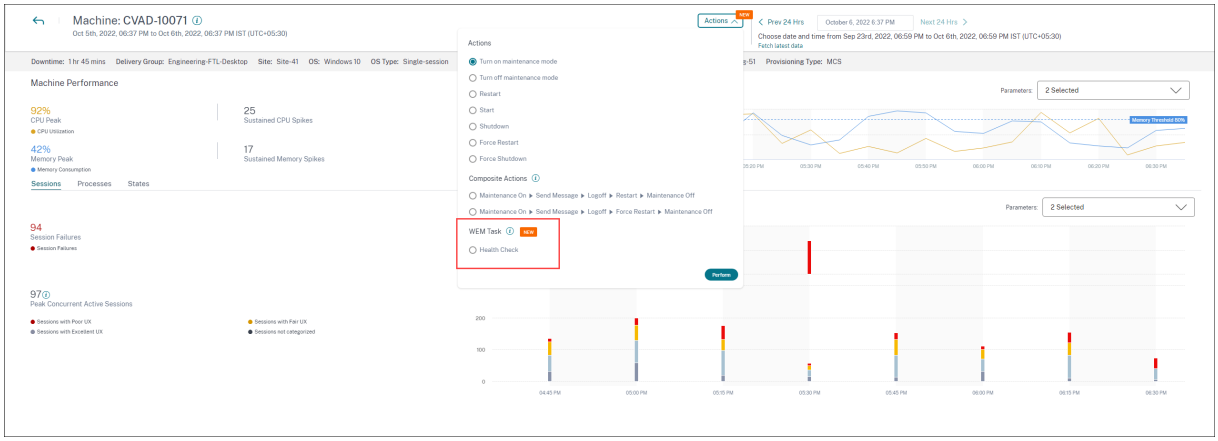
The overall status of the action and that of the individual steps are displayed under the **Actions** link.

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



WEM Tasks Health Check

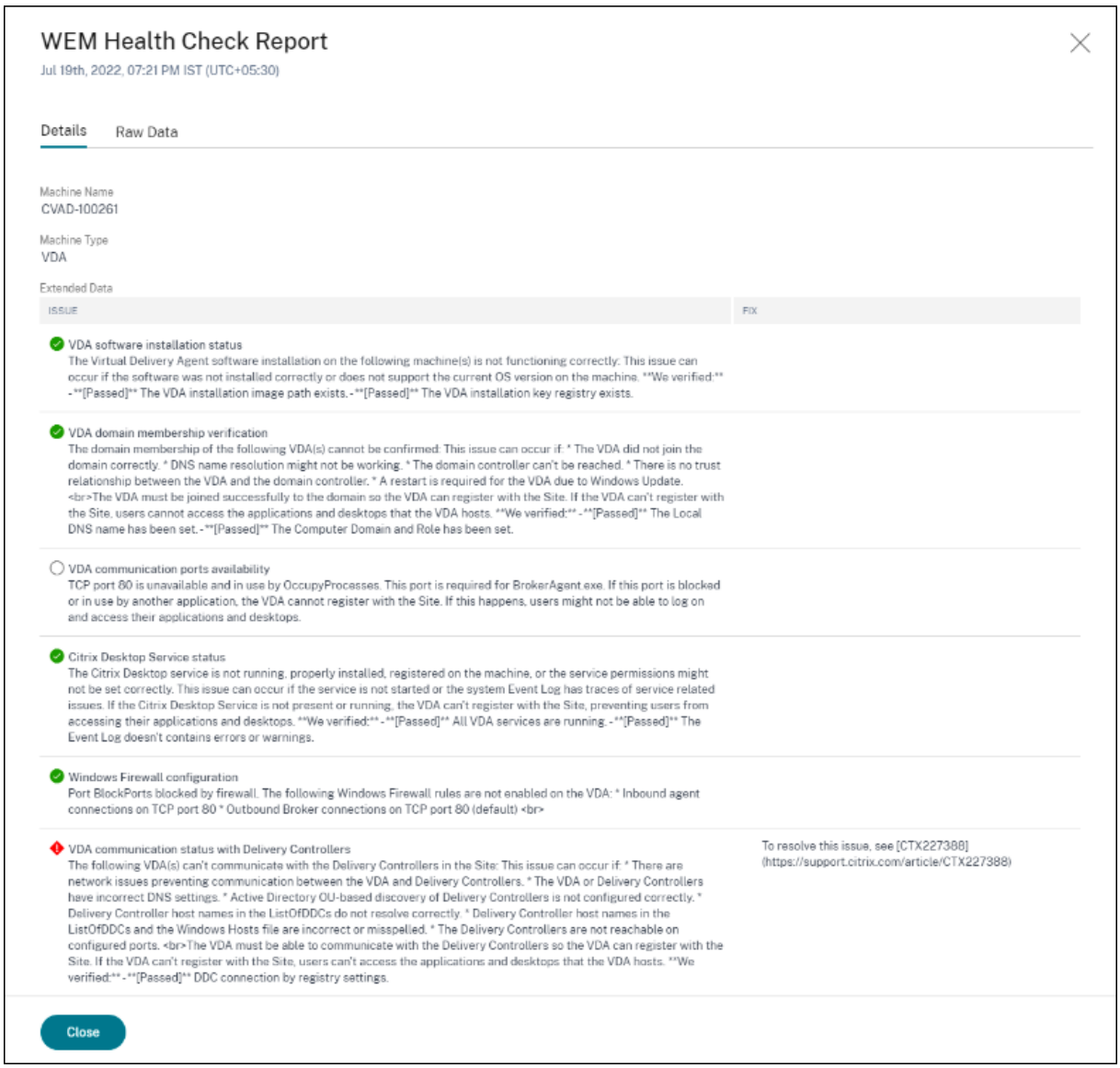
You can perform WEM Health Checks on machines from Performance Analytics. Workspace Environment Management™ (WEM) is a user environment management tool that helps optimize desktops for the best possible user experience.



Select the **WEM Task** -> **Health Check** action. This action runs the WEM Cloud Health Check script to get information on the availability of machines. This feature helps root cause common machine issues with the machine configuration, connectivity or policies easily within Performance Analytics.

The overall status of the WEM Cloud Health Check action is displayed. A link to a report is displayed once the script runs successfully. Clicking this link opens a detailed report containing the results of the WEM Cloud Health Check and possible actions that can be performed to fix them is also provided on Performance Analytics.

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



> **Note:**
>
> WEM Tasks are enabled for Cloud admins with full access and valid entitlement to WEM.
>
> For more information regarding the WEM Task Health Check, see Scripted Tasks article in the Workspace Environment Management documentation.

N/A or Not Categorized Metrics

September 11, 2025

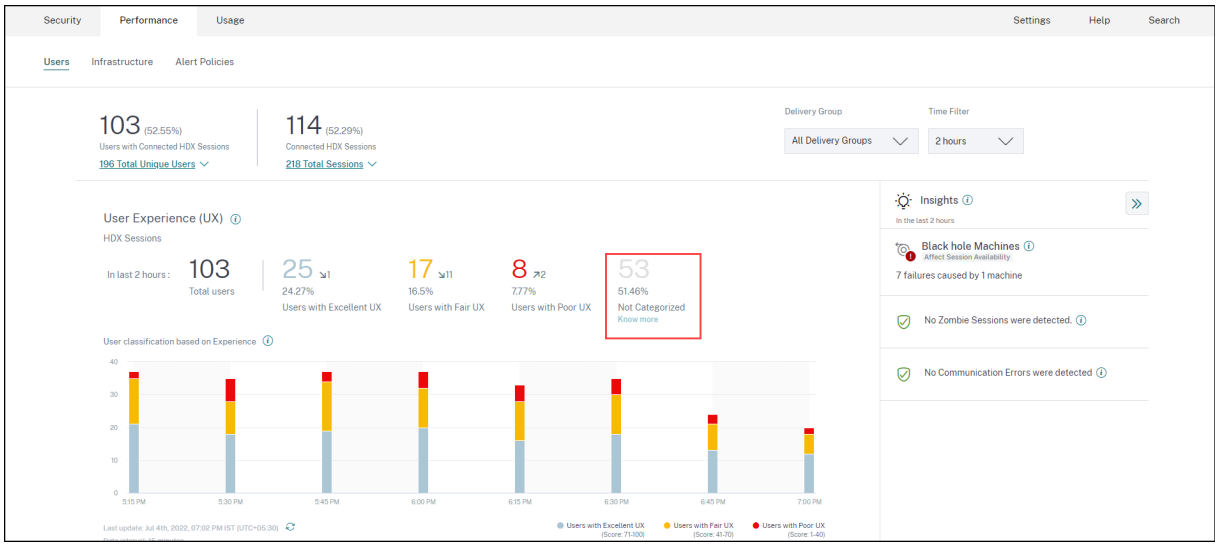
The User Experience Dashboard and the UX Factors pages can have users and sessions not categorized

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

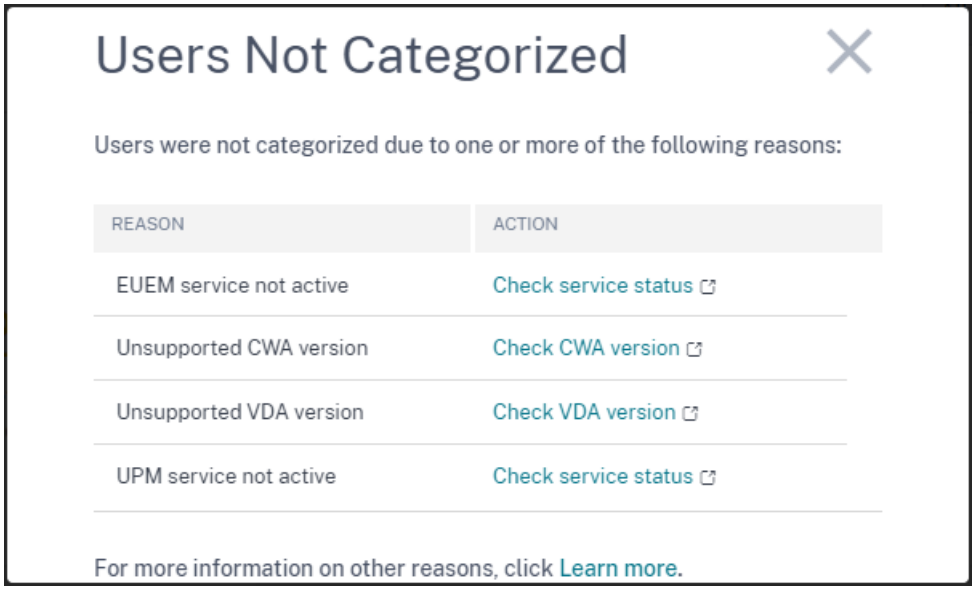
in excellent, fair, or poor categories with respect to a particular factor or subfactor.
In addition, the UX Factors and the self-service can have metrics with N/A value indicating that the measurement was either not available, or the metric is not applicable in the particular workflow.

This might happen due to instrumentation issues with the product or due to network connectivity issues. In addition, the values might not be categorized due to specific configuration issues or dependencies.

Reasons for Users and Sessions Not Categorized



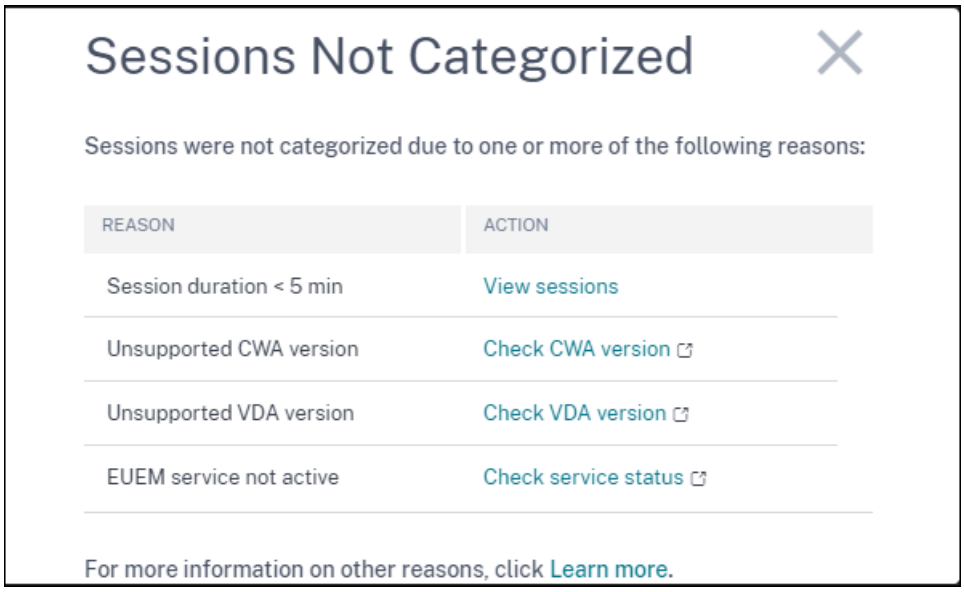
Click the **Know more** link below the Not Categorized classification in the User Experience and Session Responsiveness trends to view the primary reasons for certain users and sessions being not categorized.



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

- **EUEM service not active:** Citrix EUEM service must be installed and running for the UX score to be available and the user classification to take place. The **Check service status** link for EUEM service not active leads to the Citrix EUEM and Citrix Profile Management Services Check section in this document. It contains PowerShell code that you can run to identify the machines in your apps and desktops environment that don't have the Citrix EUEM service running.
- **UPM service not active:** Citrix Profile Management service must be installed and running for the UX score to be available and the user classification to take place. The **Check service status** link for UPM service not active leads to the Citrix EUEM and Citrix Profile Management Services Check section in this document. It contains PowerShell code that you can run to identify the machines in your apps and desktops environment that don't have the Citrix Performance Management service running.
- **Unsupported CWA version: Check CWA version** link leads to Citrix Workspace app Version Matrix that lists the minimum required Citrix Workspace app version for Citrix Analytics for Performance features.
- **Unsupported VDA version: Check VDA version** link leads to Citrix VDA Version Matrix that lists the minimum required Citrix Virtual Apps and Desktops to be running on the machines for Citrix Analytics for Performance features.

Clicking the **Know more** link under the Not Categorized classification of sessions in the Session Responsiveness trend provides reasons as follows:



One of the main reasons for sessions being not categorized is that short sessions with duration of less than 5 minutes do not send performance metrics like ICARTT that is the basis for categorization. Click the View sessions link to open the Sessions self-service view listing sessions with a duration of under 5 minutes.

The other reasons for sessions being not categorized are Unsupported CWA version, Unsupported VDA

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

version and EUEM service not active.

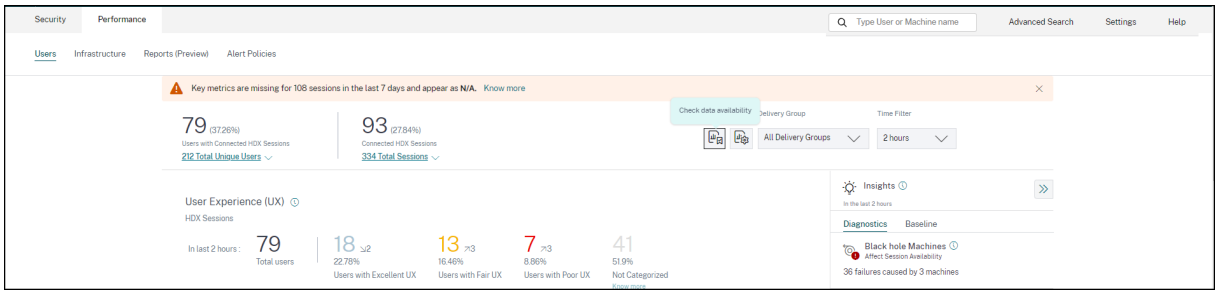
> **Note:**
>
> - All the metrics for a failed session are displayed as N/A.
> - All sessions launched via a Connection lease are **Not Categorized** as the ICA® RTT and logon duration metrics are not available.

Described below are the reasons for the specific metrics on the Performance Analytics dashboard and drilldowns being N/A or Not Categorized.

Reasons for endpoint metrics displaying N/A values

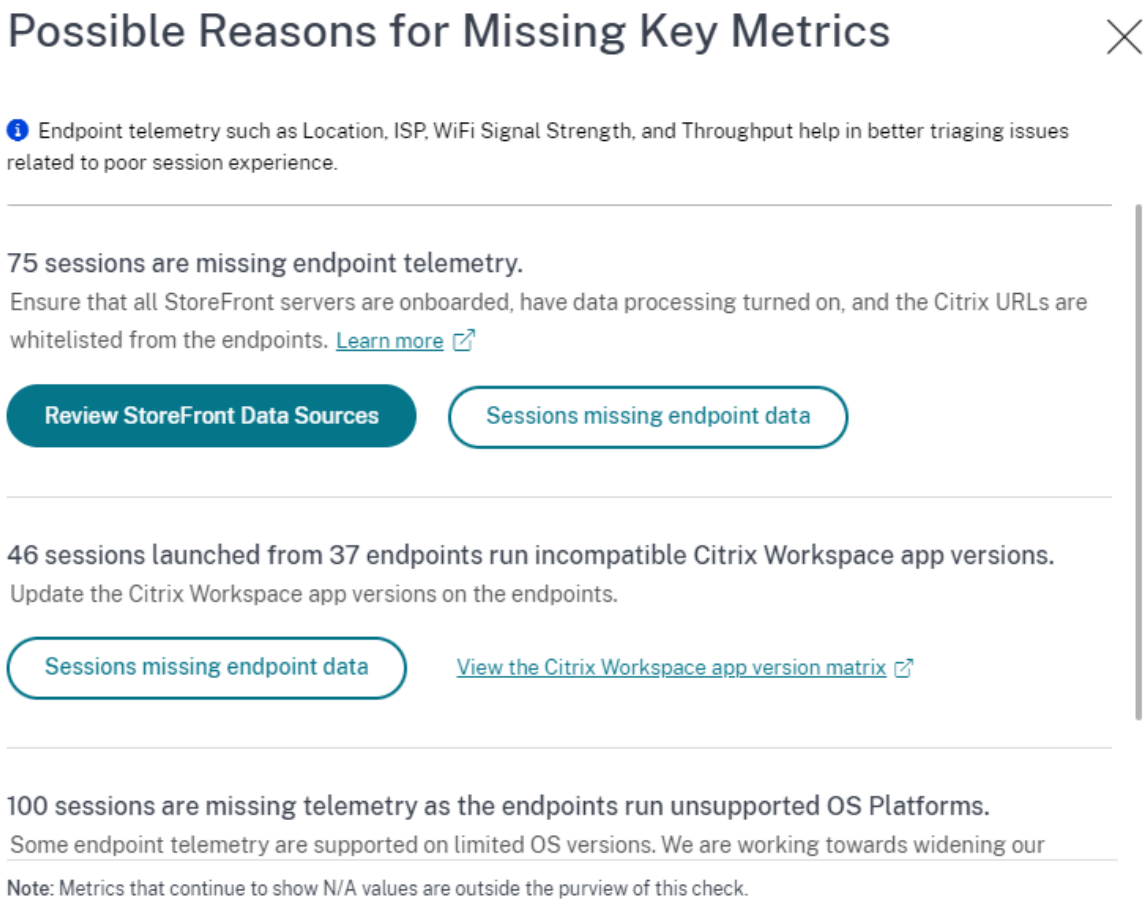
Data availability is important to optimally analyze your Citrix Virtual Apps and Desktops™ environments. Endpoint metrics like Location, ISP, WiFi Strength and Throughput are important indicators that help triage poor session experience. Endpoint metric values might be missing if the appropriate prerequisites are not met.

The User Experience dashboard contains a banner displaying the number of sessions that have missing endpoint metrics during the last 7 days.



Click **Know more**. A modal box containing the reasons in detail and the actions that you could take to solve the issues, is displayed. You can also click the Data Availability icon to view the modal.

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



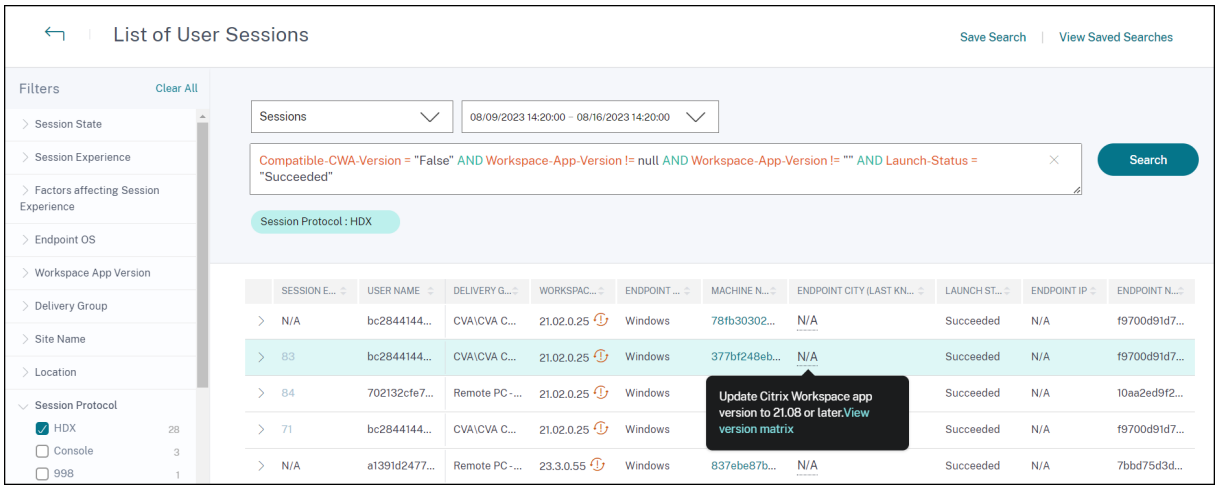
- One of the key reasons for missing endpoint telemetry is StoreFront™ onboarding. StoreFront must be onboarded correctly; data processing must be switched on and appropriate URLs must be whitelisted. **Review StoreFront Data Sources** takes you to the Data Sources page that leads you through the StoreFront onboarding process required for the Workspace App Data Collection. Citrix Workspace™ does not require onboarding. Click **Sessions missing endpoint data** to open the Sessions self-service view with the list of sessions whose endpoint metrics are missing because of incorrect or non-existent StoreFront Onboarding.
- Endpoint telemetry is not available for sessions launched from endpoints that run unsupported OS platforms or incompatible Citrix Workspace app versions. Clicking **Sessions missing endpoint data** opens the Sessions self-service view with the list of the sessions missing endpoint telemetry due to a specific listed reason. For more information, see the Version matrix that lists for each feature the OS versions and the required Workspace app version on which it is supported.

Tool tips elaborating the reason for N/A values are now in available in the Sessions self-service view for the following endpoint related metrics:

- Workspace App Version

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

- Endpoint Country (Last known)
- Endpoint City (Last known)
- Endpoint Link Speed (P95)
- Endpoint Throughput Incoming (P95)
- Endpoint Throughput Outgoing (P95)
- ISP (Internet Service Provider)



Tooltips are displayed on the N/A values of these metrics with the reason as incorrect StoreFront onboarding, or sessions launched from endpoints that run unsupported OS platforms or incompatible Citrix Workspace app versions. For more information about the metrics available in the Sessions self-service view, see Self-service view for sessions.

Users, User Experience Score, Session Score Not Categorized

Users, User Experience Score, Session Score might not be categorized when either the Session Responsiveness or the Session Logon Duration factor measurements be unavailable for the selected time period.

ICA RTT N/A and Session Responsiveness Not Categorized

ICA RTT being N/A leads to sessions not categorized for Session Responsiveness. This can happen due to the following reasons:

- Endpoint OS is running either HTML5 or iOS.
- Session is in Failed, Disconnected state.
- Session is reconnected.
- Session is not running on HDX™ protocol.
- Citrix Profile Management is not running.

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

- End User Experience Monitoring (EUEM) service is not running, and the corresponding policies are not configured on the machines.
- Session is not connected through Citrix Gateway version 12.1 or later, and configured with Citrix Analytics for Performance. For more information, see Gateway data source.
- Session is launched from machines that are not enabled for NSAP.
- Session is not a new CGP (Common Gateway Protocol) session.

Logon Duration Not Categorized

- Session is not running on HDX protocol.
- Logon Duration requires Citrix Profile Management to be running on the machines. Citrix Profile Management calculates the Logon Duration based on machine events and forwards the same to the Monitor Service. If a Remote PC Access deployment exists and a machine upgrade is not required, you can deploy the Profile Management components separately - Citrix Profile Management and Citrix Profile Management WMI plug-in. For more information, see the blog, Monitor, and troubleshoot Remote PC Access machines.

GPO N/A

Group Policy settings are not configured or enabled on the virtual machines.

Profile Load N/A

- Citrix Profile Management is not running on the machines.
- Machine is not running Citrix Virtual Apps and Desktops version 1912 or later.

VM start N/A

This measurement is available only when the power managed machine is started during session launch.

Logon Scripts N/A

Logon scripts are not configured for the session.

Overloaded Machines Not Categorized

- Machine not registered
- Users whose poor session experience is not due to resource overload.

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

Location and ISP N/A

- Endpoint is running on an older version of Citrix Workspace app. For information on the minimum required Citrix Workspace app versions for Citrix Analytics for Performance features, see Citrix Workspace app version matrix.
- Session state is **Failed**.
- Communication time-out occurred with the URL, `https://locus.analytics.cloud.com/api/locateip`.
- IP might not be resolved.
- The SendPublicIPAddress registry entry in the endpoint machine is set to disable the IP address transmission.
- The StoreFront server of your on-premises Site deployment is not configured with Citrix Analytics. For more information, see Onboard Virtual Apps and Desktops sites using StoreFront.

Workspace App Version or Endpoint OS N/A

- Endpoints are not running Citrix Workspace app for Windows version 1912 or later.
- Session is not running on HDX protocol.
- Session has failed.

Connection Type N/A

Endpoints are not running Citrix Workspace app for Windows version 20.12.0 or later.

Network Interface Type N/A

Endpoints are not running Citrix Workspace app for Windows version 2105 or later.

Bandwidth and Network Latency Metrics N/A

Machine is not running Citrix Virtual Apps and Desktops 7 2112 or later.

The **VDA data collection for Analytics** policy is not set to **Allowed** on machines. This is required 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 Analytics.

Endpoint Network Metrics N/A

Endpoints are not running Citrix Workspace app for Windows version 2108 or later.

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

Gateway Service and Connector N/A

Gateway Service and Connector metrics are supported only for Gateway Service (Non-rendezvous) and Rendezvous 1.

Machines Not Categorized based on Load

Machines might be not categorized in the following cases:

- The machine is in shutdown, unregistered, or failed state.
- Resource data is not available for the machine. Ensure that the Resource Monitoring policy is enabled on the machine. For more information, see Enable Resource Monitoring.

Citrix EUEM and Citrix Profile Management Services Check

Run the following PowerShell script to identify the machines in your Apps and Desktops environment that don't have the Citrix EUEM and Citrix Profile Management services running. To run the Service Check script, do the following steps:

1. Start an RDP session to Cloud Connector for a cloud environment or Delivery Controller™ for an on-premises environment.
2. Run the following Service Check PowerShell Script. If you run this script on Cloud Connector, the script displays a popup window to log in and select the customer.

The script produces two output files in the same folder as the script itself.

- upmnotrunning.txt specifies the list of machines on which Citrix Profile Management is not running.
- EUEMnotrunning.txt specifies the list of machines on which the EUEM service is not running.

```
add-pssnapin citrix*

#for more filter : https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/
$dgList = @('All') #Add the delivery group names here

#Get list of machine in that environment
if($dgList[0] -eq 'All')
{

  $machineList = Get-BrokerMachine
 }

else
{
```

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

```
15
16     for($i=0; $i -lt $dgList.Length; $i++)
17     {
18
19        $machineList += Get-BrokerMachine -DeliveryGroupName $dgList[$i]
20      }
21
22  }
23
24
25
26 $upmNotRunning = [System.Collections.ArrayList] @()
27 $euemNotRunning = [System.Collections.ArrayList] @()
28
29 #Check for UPM and EUEM service status in machine
30 for($i=0; $i -lt $machineList.Length; $i++)
31 {
32
33     Write-Host("Machine Name : " + $machineList[$i].DNSName)
34
35     #UPM Service check
36
37         $upm = Get-Service ctxProfile -ComputerName $machineList[$i].
               DNSName -ErrorVariable getServiceErrorUpm -ErrorAction
               SilentlyContinue
38
39         if ($getServiceErrorUpm.Count -gt 0 -and ($getServiceErrorUpm |
               foreach {
40  $_.FullyQualifiedErrorId -like "*NoServiceFoundForGivenName*" }
41  ))
42         {
43
44              Write-Warning "There is no service named UPM in
                    $machineList[$i].DNSName"
45              $upmNotRunning.Add($machineList[$i].DNSName)
46          }
47
48         elseif ($getServiceErrorUpm.Count -gt 0)
49         {
50
51             Write-Warning("Exception on $machineList[$i].DNSName :
                   $getServiceErrorUpm")
52          }
53
54         else
55         {
56
57             if ( -Not('Running' -eq $upm.Status))
58             {
59
60                 Write-Host("UPM service not running on $machineList[$i
                       ].DNSName")
61                 $upmNotRunning.Add($machineList[$i].DNSName)
```

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

```
62                }
63
64             }
65
66
67
68        #EUEM Service check
69            $euem = Get-Service 'Citrix EUEM' -ComputerName $machineList[$i
                  ].DNSName -ErrorVariable getServiceErrorEuem -ErrorAction
                  SilentlyContinue
70
71            if ($getServiceErrorEuem.count -gt 0 -and ($getServiceErrorEuem
                   | foreach {
72    $_.FullyQualifiedErrorId -like "*NoServiceFoundForGivenName*" }
73    ))
74            {
75
76                 Write-Warning "There is no service named Citrix EUEM in
                       $machineList[$i].DNSName"
77                 $euemNotRunning.Add($machineList[$i].DNSName)
78             }
79
80            elseif ($getServiceErrorEuem -gt 0)
81            {
82
83                 Write-Warning("Exception on $machineList[$i].DNSName :
                       $getServiceErrorEuem")
84             }
85
86            else
87            {
88
89                if (-Not('Running' -eq $euem.Status))
90                {
91
92                     Write-Host("EUEM service not running on $machineList[
                           $i].DNSName")
93                    $euemNotRunning.Add($machineList[$i].DNSName)
94                 }
95
96             }
97
98
99    }
100
101
102   # Add the list of machines not having UPM or EUEM services running to a
          file
103   Out-File -FilePath .\UpmNotRunning.txt -InputObject $upmNotRunning -
          Encoding ASCII -Width 100
104   Out-File -FilePath .\EuemNotRunning.txt -InputObject $euemNotRunning -
          Encoding ASCII -Width 100
```

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

Self-service search

September 1, 2025

What is self-service search?

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

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

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

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

How to access self-service search

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

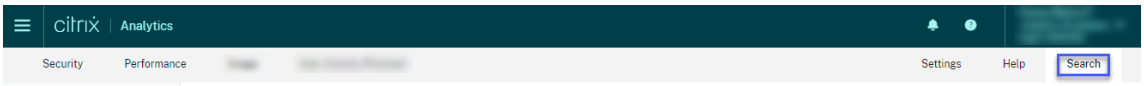
- **Top bar**: Click **Search** from the top bar to view all user events for the selected data source.
- **Risk timeline on a user profile page**: Click **Event Search** to view the events for the respective user.

Self-service search from the top bar

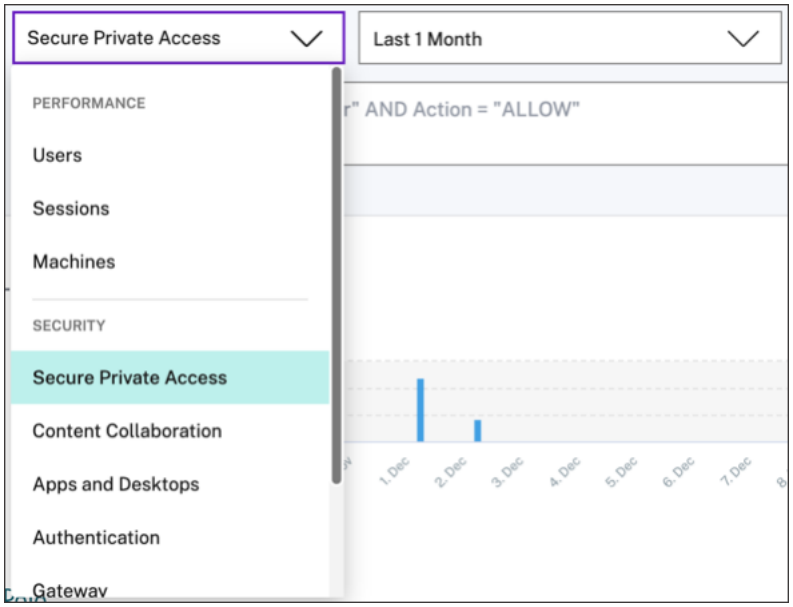
Use this option to go to the self-service search page from any place in the user interface.

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

1. Click **Search** to view the self-service page.



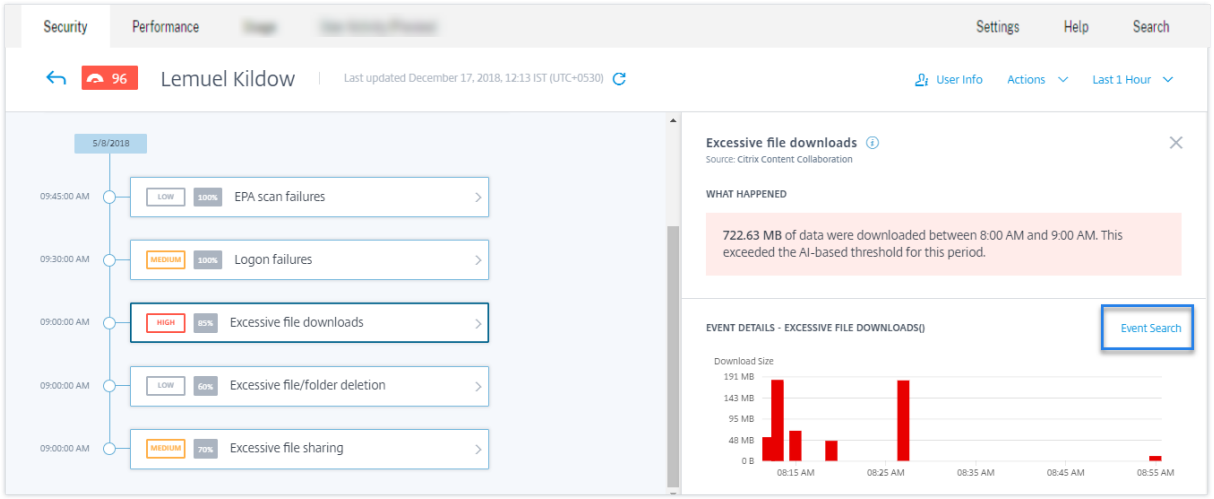
2. Select the data source and the time period to view the corresponding events.



Self-service search from user's risk timeline

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

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



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

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

How to use self-service search

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

- Facets to filter your events.
- Search box to enter your query and filter events.
- Time selector to select the time period.
- Timeline details to view the event graphs.
- Event data to view the events.
- Export to CSV format to download your search events as a CSV file.
- Export visual summary to download the visual summary report of your search query.
- Multicolumn sorting to sort the events by multiple columns.

Use facets to filter events

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

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

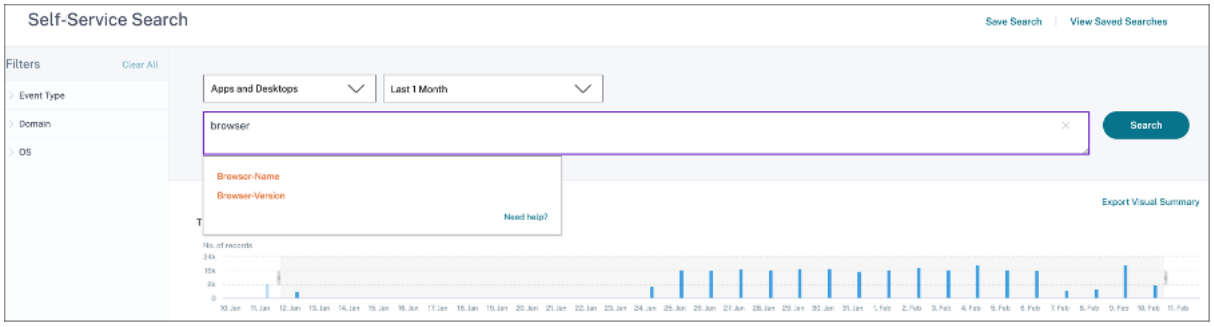
For more information on the facets corresponding to each data source, see the self-service search article for the data source mentioned earlier in this article.

Use search query in the search box to filter events

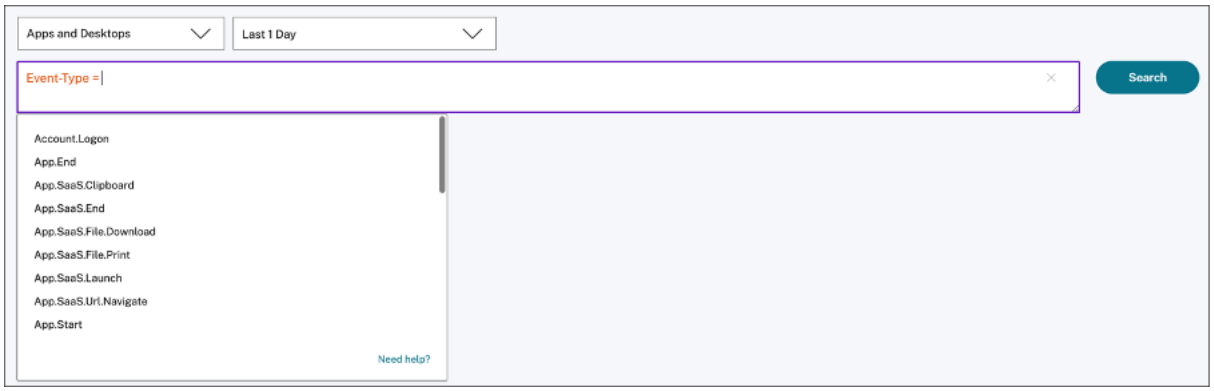
When you place your cursor in the search box, the search box displays a list of dimensions based on the user events. These dimensions vary according to the data source. Use the dimensions and the valid operators to define your search criteria and search for the required events.

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

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



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



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

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

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

Operator	Description	Example	Output
AND	Search events where the specified conditions are true.	User-Name : John AND Data Volume > 100	Displays events of user John where data volume is greater than 100 GB.
! ~	Checks events for the matching pattern that you specify. This NOT LIKE operator returns the events that do not contain the matching pattern anywhere in the event string.	User-Name !~ John	Displays events for the users except John, John Smith, or any such users that contain the matching name “John”.
! =	Checks events for the exact string that you specify. This NOT EQUAL operator returns the events that do not contain the exact string anywhere in the event string.	Country != USA	Displays events for the countries except USA.
*	Search events that match the specified strings. Currently, the * operator is supported only with the following operators :, =, and !=. The search results are case-sensitive.	User-Name = John*	Displays events for all user names that begin with John.
		User-Name = *John*	Displays events for all user names that contain John.
		User-Name = *Smith	Displays events for all user names that end with Smith.
		User-Name : John*	Displays events for all user names that begin with John.

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

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

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

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

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

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

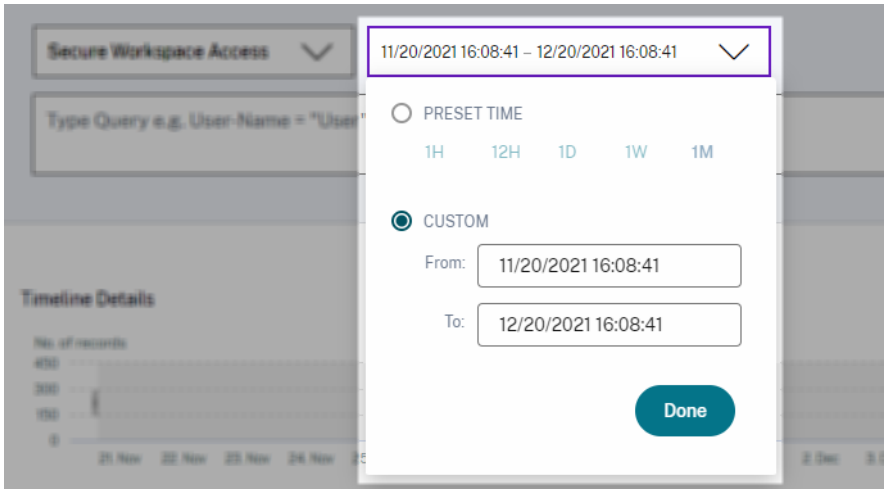
> **Note**
>
> For the **NOT EQUAL** operator, while entering the values for the dimensions in your query, use the exact values available on the self-service search page for a data source. The dimension values are case-sensitive.

For more information on how to specify your search query for the data source, see the self-service search article for the data source mentioned earlier in this article.

Select time to view event

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

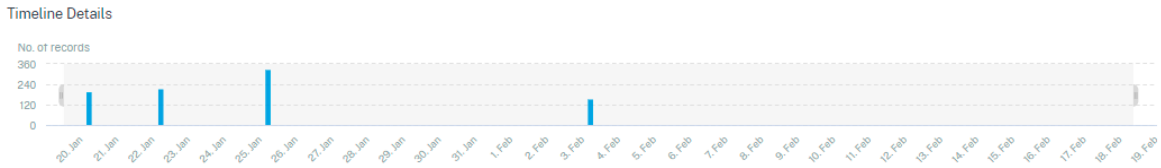
© 1997–2026 Citrix Systems, Inc. All rights reserved.



View the timeline details

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

The figure shows timeline details for access data.

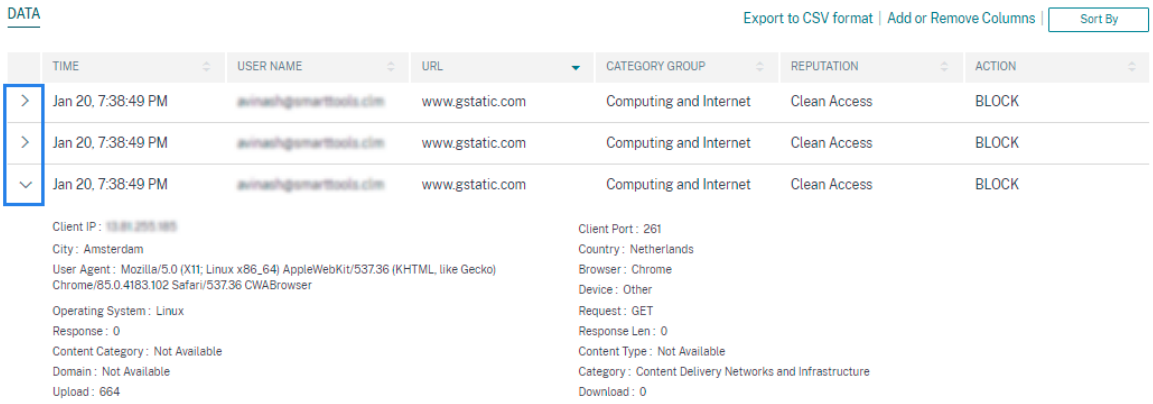


View the event

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

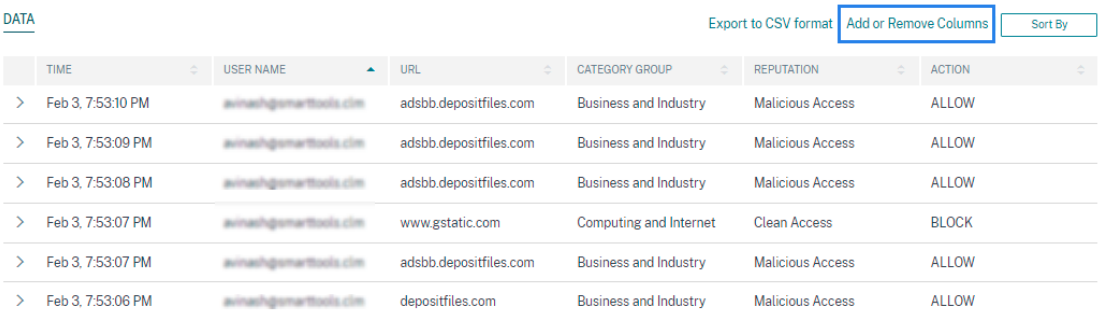
The figure shows the details about the user's access data.

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



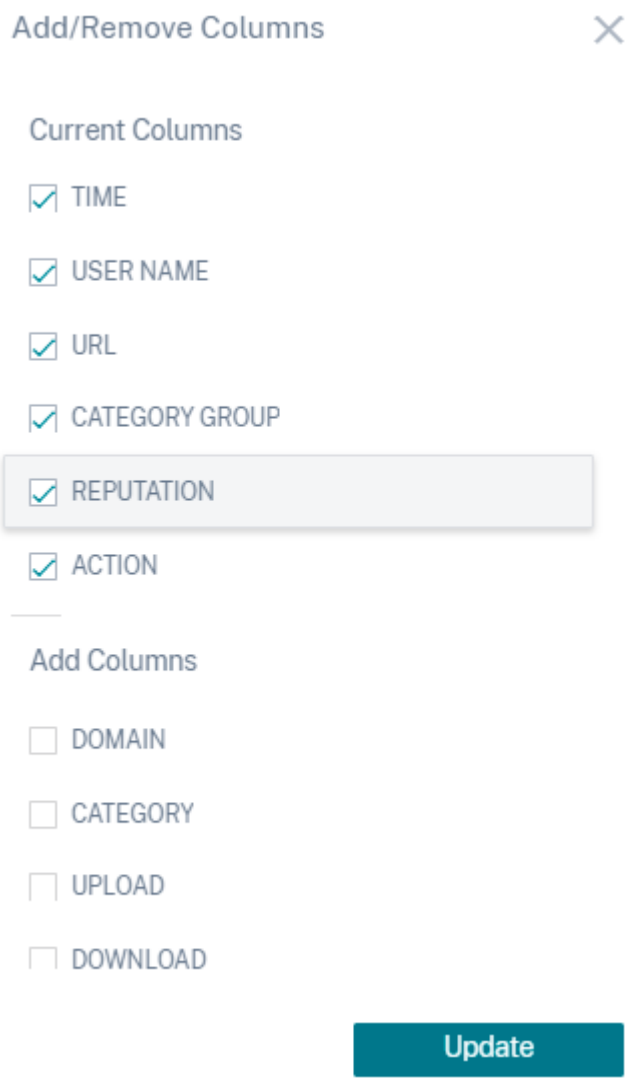
Add or remove columns You can either add or remove columns from the event table to display or hide the corresponding data points. Do the following:

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



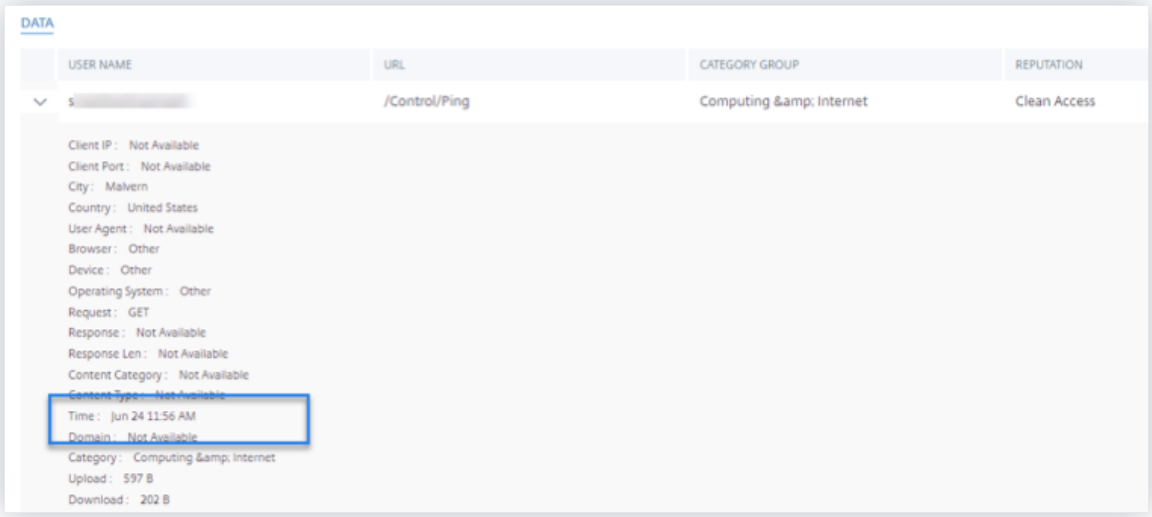
2. Select or deselect the data elements from the list and then click **Update**.

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



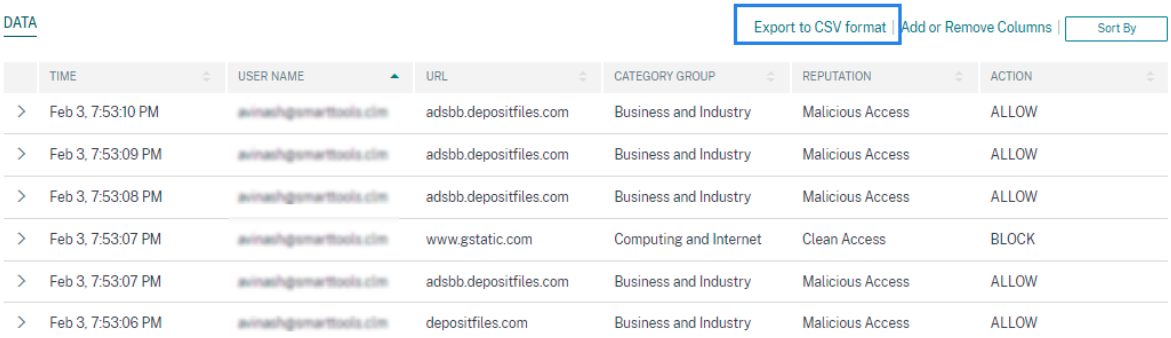
If you deselect a data point from the list, the corresponding column is removed from the event table. However, you can view that data point by expanding the event row for a user. For example, when you deselect the **TIME** data point from the list, the **TIME** column is removed from the event table.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

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



Export the events to a CSV file

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



Export visual summary

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

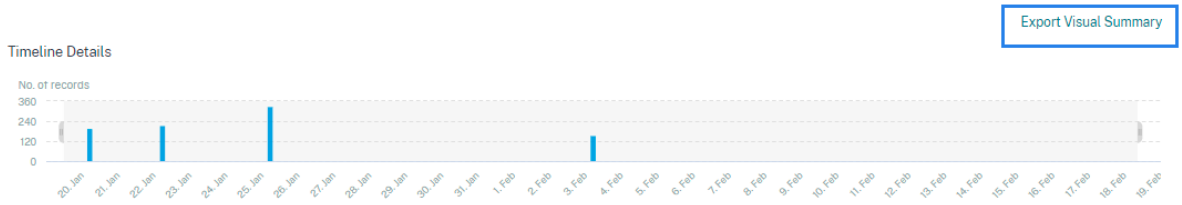
Click **Export Visual Summary** to download the visual summary report as a PDF. The report contains the following information:

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

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

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

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

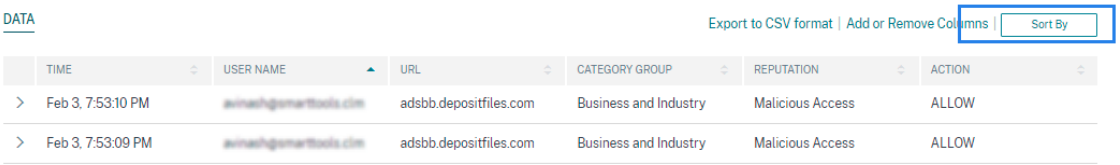


Multi-column sorting

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

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

1. Click **Sort By**.



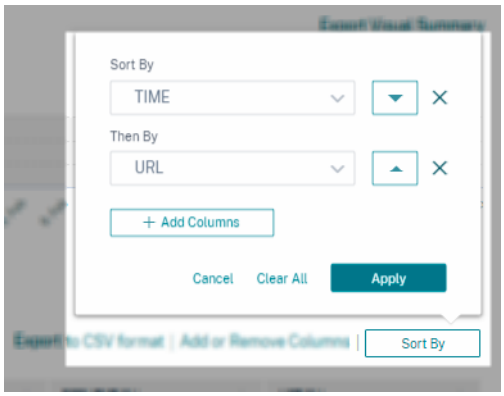
2. Select a column from the **Sort By** list.
3. Select the sorting order- ascending (up arrow) or descending (down arrow) to sort the events in the column.
4. Click **+ Add Columns**.
5. Select another column from the **Then By** list.
6. Select the sorting order- ascending (up arrow) or descending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

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

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

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

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



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

How to save the self-service search

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

- Applied search filters
- Selected data source and duration

Do the following to save a self-service query:

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

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

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

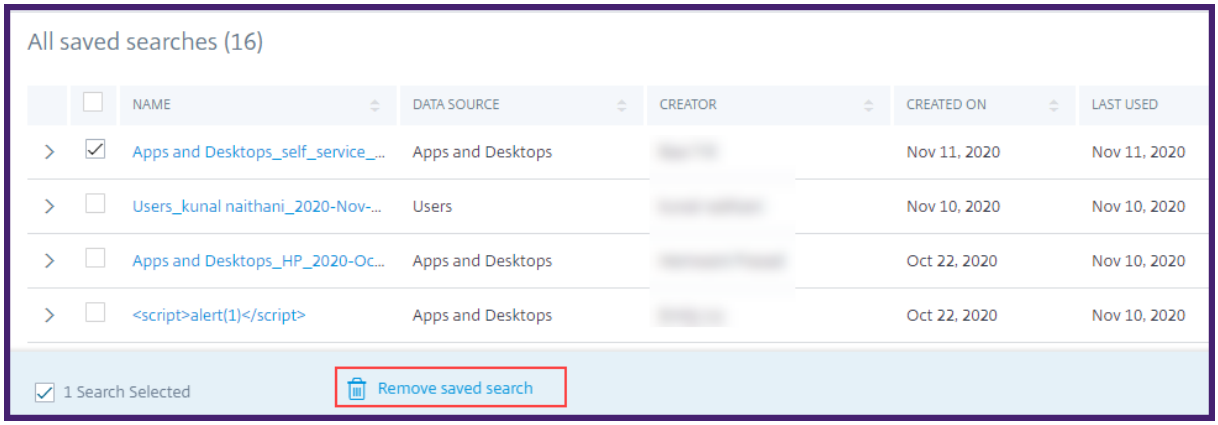
6. Enable the **Schedule email report** button if you want to send a copy of the search query report to yourself and other users at a regular interval. For more information, see Schedule an email for a search query.
7. Click **Save**.

To view the saved searches:

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

To remove a saved search:

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



To modify a saved search:

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

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

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

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

Schedule an email for a search query

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

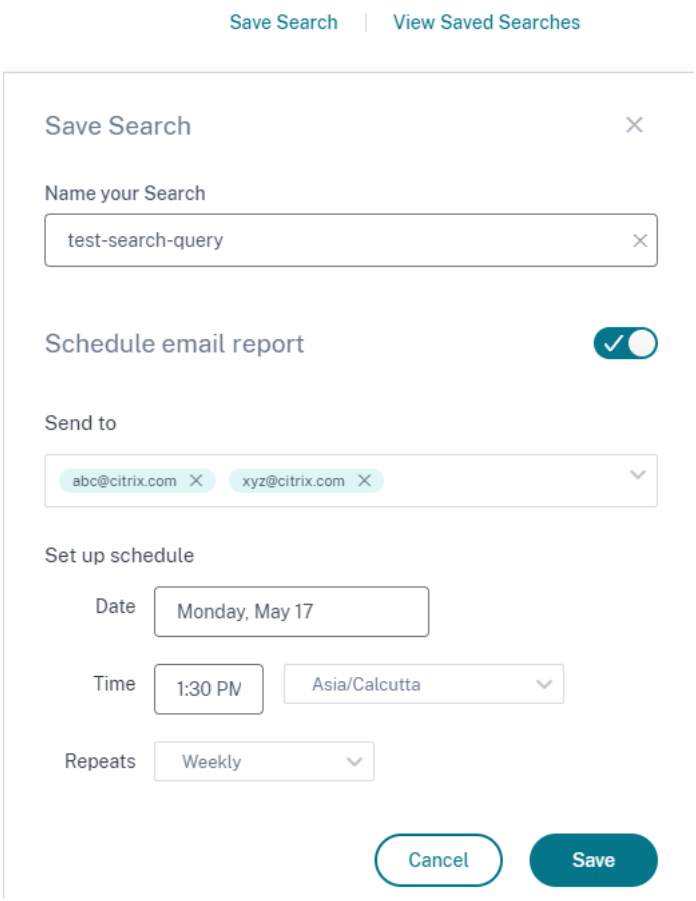
This option is available only if your search query report contains data in visual formats such as bar charts, timeline details. Otherwise, you cannot schedule an email delivery. For example, you can schedule an email for the data sources such as Apps and Desktops, Sessions, where you see data as timeline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

Schedule an email while saving a search query

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

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

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



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

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

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

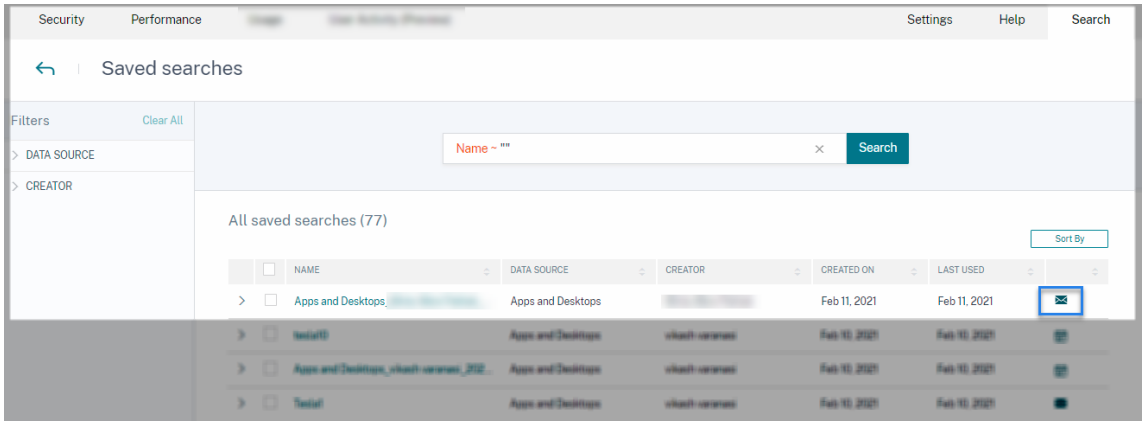
Schedule an email for an already saved search query

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

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

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

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



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

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

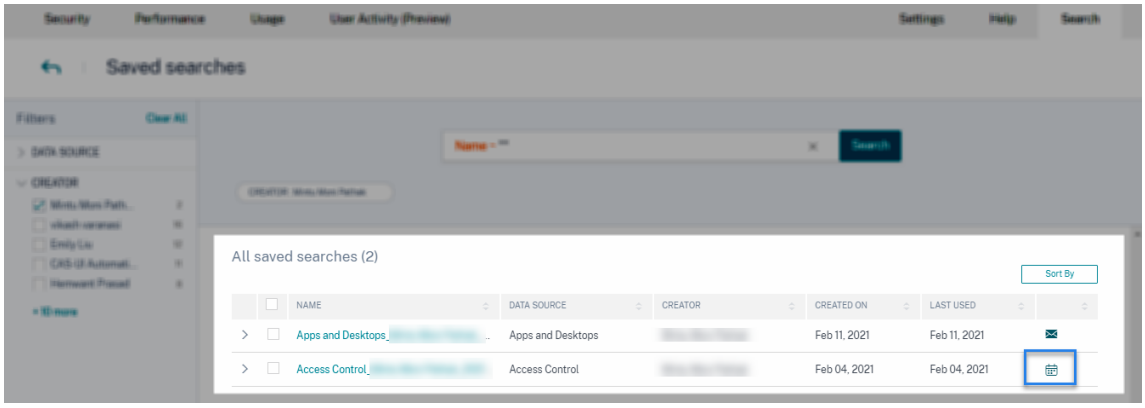
5. Set the date and time for the email delivery.
6. Select the delivery frequency- daily, weekly, or monthly.
7. Click **Save**.

Stop an email delivery schedule for a search query

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

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

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



3. Disable the **Schedule email report** button.
4. Click **Save**.

Email content

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

The search query report contains the following information:

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

Permissions for full access and read-only access administrators

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

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

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

Self-Service Search for Performance

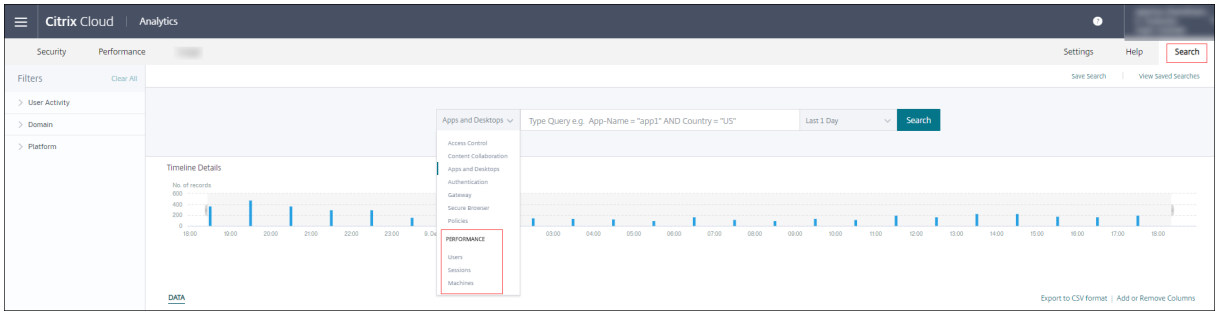
September 11, 2025

Self-service search provides insights into key performance indicators associated with users, sessions, and machines collected by Citrix Analytics for Performance. Performance metrics such as session responsiveness, logon duration, session launch attempts, session failure count are displayed for users, machines, or sessions sorted and filtered based on your selection.

You can reach the self-service page from the main **Search** menu of the Citrix Analytics.

> **Note:**
>
> For more information on the self-service functionalities, like the usage of self-service search, scheduling an email for a search query and more, see Self-service search.

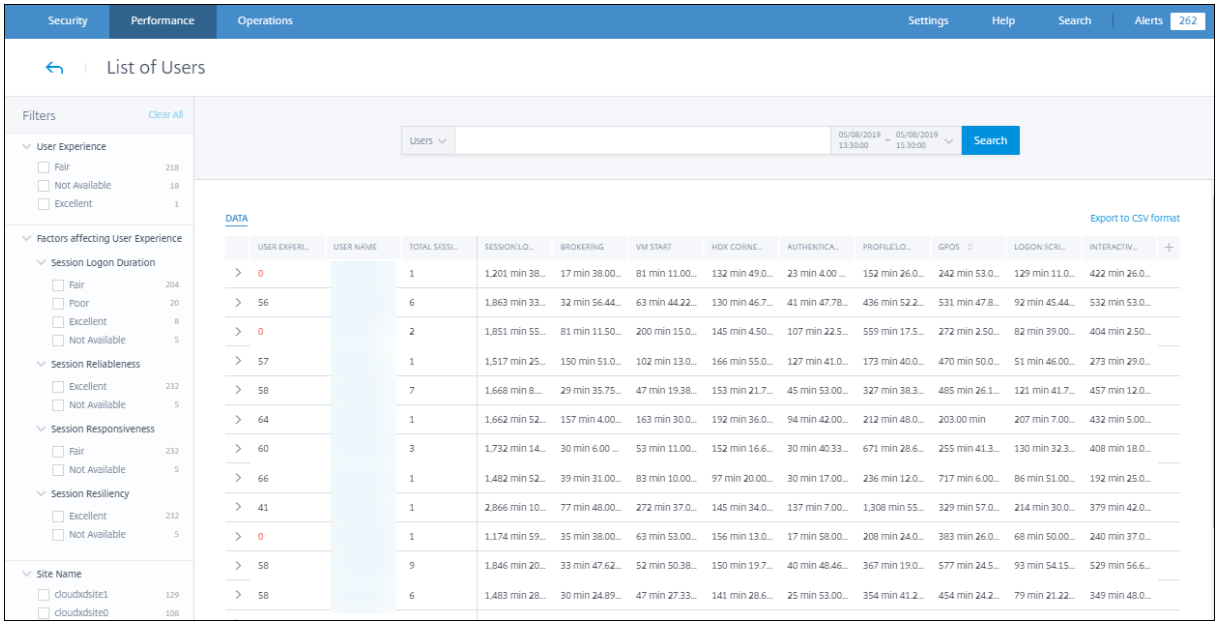
To view the Performance related events on the self-service page, select **Users**, **Sessions**, or **Machines** under **Performance** from the list in the search bar, select the time period, and then click **Search**.



Specific Users, Sessions, and Machines based self-service pages are also displayed upon clicking the users, sessions, or machines numbers respectively on the User experience dashboard and User Experience (UX) Factors pages.

You can use the search bar to enter your query to filter the results. You can also narrow down your search using the facets on the left hand pane. The set of users, sessions, or machines displayed is based on the selection criteria.

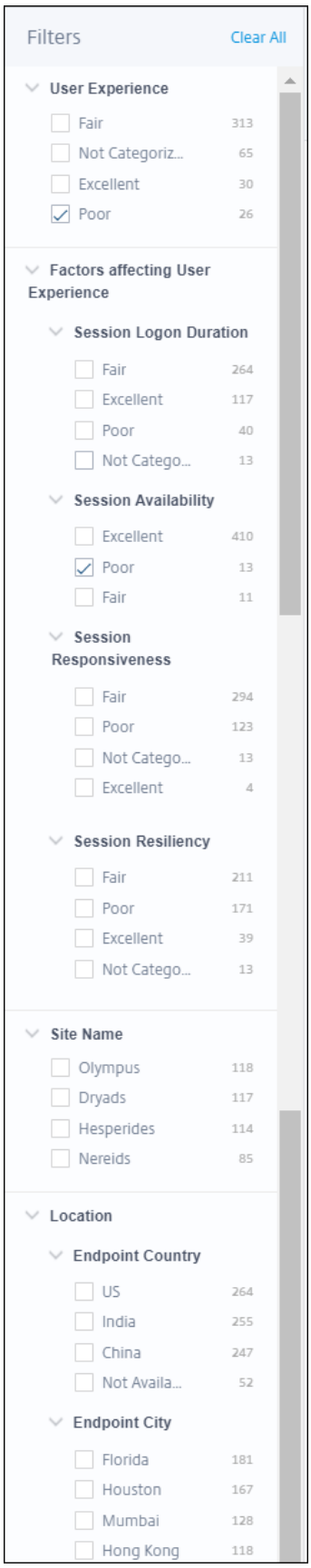
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Select facets to filter events

Use the facets on the left-hand side pane to filter the data. Some of the facets associated with the Citrix Analytics for Performance are as follows:

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



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

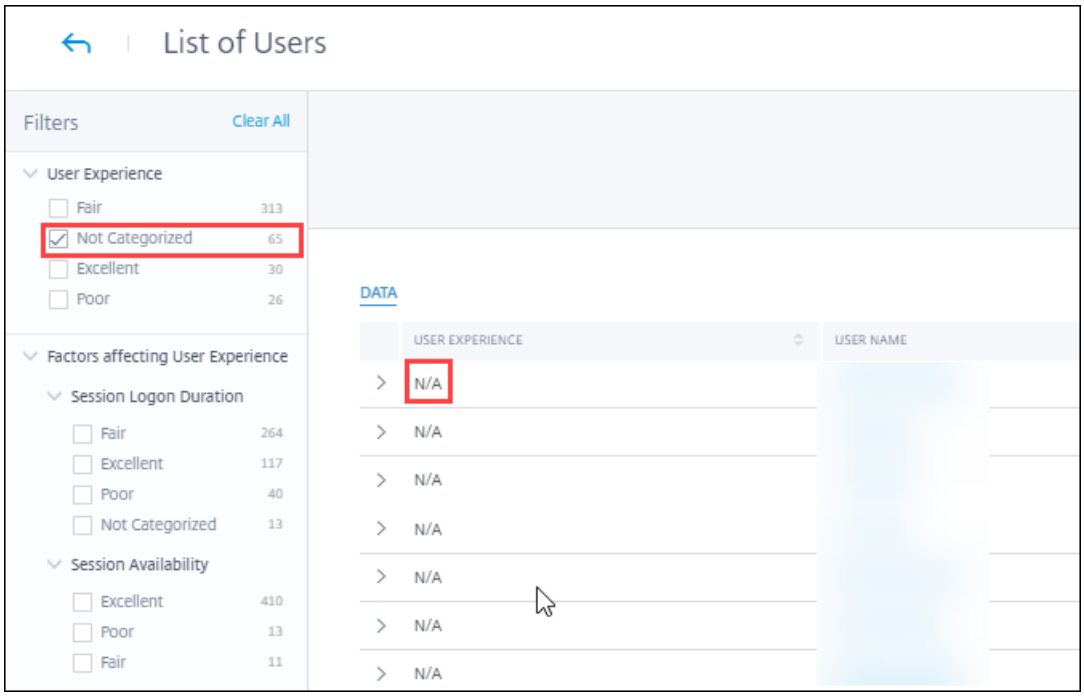
Session State

In the Sessions self-service view, you can select sessions based on the state of the session from among the following values:

- Unknown
- Connected
- Disconnected
- Terminated
- PreparingSession
- Active
- Reconnecting
- NonBrokeredSession
- Other
- Pending

User Experience

Search users based on the user experience being Excellent, Fair, or Poor. The User Experience score can be "Not Categorized"if either the Session Responsiveness or the Session Logon Duration factor measurements be unavailable for the selected time period. The User Experience Score and the Session Experience Score are displayed as N/A in the self-service search results in these cases.



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

Session Experience

Search sessions based on the session experience being Excellent, Fair, or Poor. The Session Experience score can be ‘‘Not Categorized’’if either the Session Responsiveness or the Session Logon Duration factor measurements are unavailable for the selected time period. The Session Experience Score is displayed as N/A in the self-service search results in these cases.

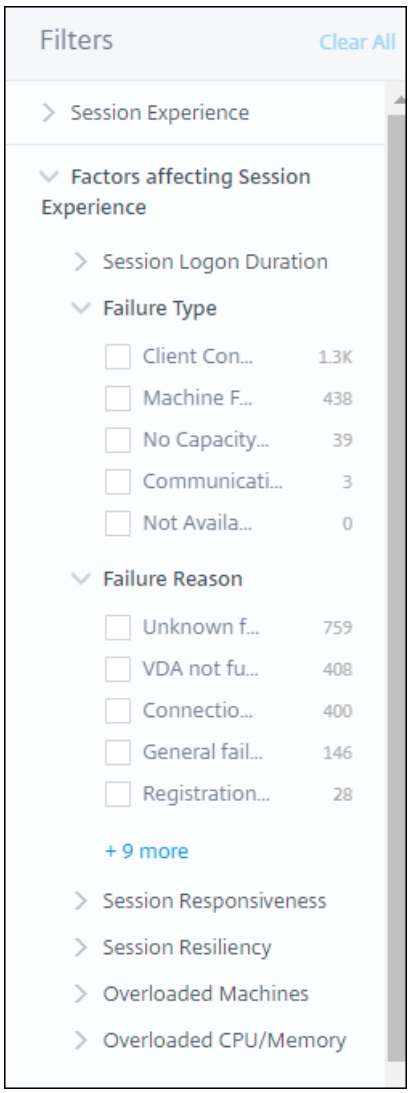
Factors affecting User Experience

Search users, sessions, and machines based on the individual factors affecting the user experience, such as Session Logon Duration, Session Responsiveness, Session Availability, or Session Resiliency.

Failure Type and Reason

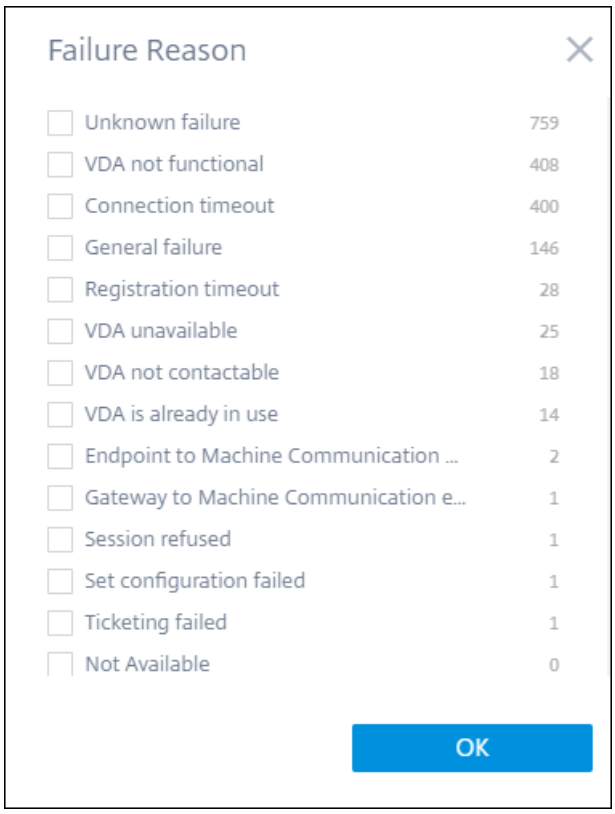
In the Sessions self-service view, Failure Type and Failure Reason facets represents the Session Availability performance factors.

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



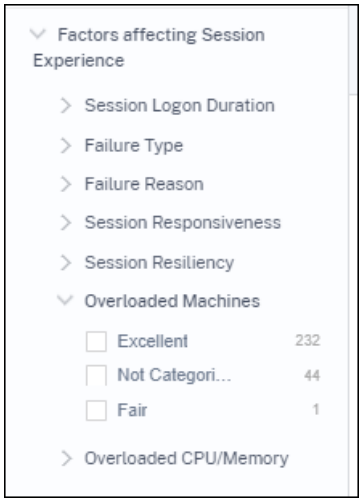
Failure Type provides filtering based on the type of session failures, such as Machine Failure, Client Connection Failure, Communication Failure. Failure Reason provides filtering based on the reason for session failure, such as a machine not functional, or a registration timeout.

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



Overloaded Machines and CPU/Memory

The Overload facets help filter machines, users, and sessions based on the load on the CPU and memory resources.



Overloaded Machines provides filtering based on how overloaded the machine resources are. Overloaded CPU/Memory provides filtering based on whether CPU or memory caused the overload.

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

Endpoint OS

Search sessions based on the operating system running on the endpoint machine from which the session has been launched. This parameter helps identify issues that can be common among all endpoints running the same OS. The OS information is displayed as N/A for endpoints running **Citrix Workspace app for Windows version 1912 and earlier**.

Workspace App Version

Search sessions based on the Workspace App Version on the endpoint machine from which the session has been launched. This parameter helps identify issues specific to a particular Workspace App Version. The Workspace App Version information is displayed as N/A for endpoints running **Citrix Workspace app for Windows version 1912 and earlier**.

Delivery Group

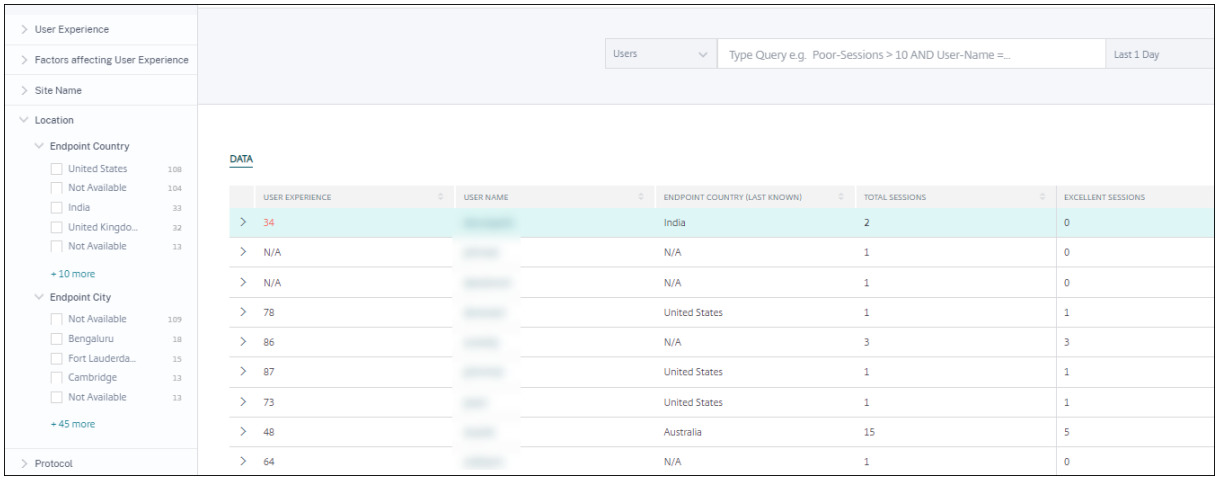
Filter users, sessions, and machines based on the Delivery Group the machines belong to.

Site Name

Filter users, sessions, and machines based on Site.

Location

You can now search users and sessions based on the location of the Endpoint Country or City. The Location facet helps isolating latency-related issues to a specific location.



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

The location information is extracted from the public IP address securely transmitted by the endpoint machine to Citrix Analytics. If your organization uses an on-premises StoreFront deployment, you can configure your StoreFront servers to enable Citrix Workspace app to send events to Citrix Analytics. Follow the steps as described in Onboard Virtual Apps and Desktops Sites using StoreFront.

You can disable the transmission of the IP address from the Citrix Workspace app on the endpoint machine by setting the **SendPublicIPAddress** registry entry to `false`. For more information, see Enhancement to Citrix Analytics Service in the Citrix Workspace app for Windows documentation.

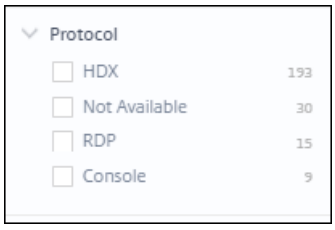
> **Note:**
>
> In the case of a closed customer environment where the endpoints are operating within an intranet, ensure that the URL `https://locus.analytics.cloud.com/api/locateip` is accessible to the endpoints.

Location of an endpoint can be `Not Available` or `N/A` for the following reasons:

- The session failed to launch.
- Communication time-out occurred with the URL, `https://locus.analytics.cloud.com/api/locateip`.
- The **SendPublicIPAddress** registry entry in the endpoint machine is set to disable the IP address transmission.
- The StoreFront™ server of your on-premises Site deployment is not configured with Citrix Analytics.
- The Citrix Workspace App for Windows version is earlier than 1912. See the Citrix Workspace app versions supported for other OS in the Citrix Workspace app Version Matrix article

Session Protocol

The Protocol facet helps you filter users and sessions based on the protocol of the session - HDX™, Console, or RDP.



This facet lists only the current protocols of sessions and not all supported session protocols.

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

Connection Type

Use the Connection Type facet to filter sessions based on whether the endpoints are directly connected to the machines or through a gateway. The Connection Type facet has the following elements,

- internal –for direct connections without Gateway
- external –for connections through Gateway

The Connection details are available for Endpoints running Citrix Workspace app version 20.12.0 or later for Windows. For all other endpoints, the Connection type is displayed as N/A.

This facet helps identify and troubleshoot issues related to the gateway easily.

Machine OS Type

This facet is available on the Machines based self-service view. It helps narrow down your search to a specific Machine OS type.

Launch Type

This facet shows the classification of sessions as ICA® based or Connection leased on the Sessions Self-service view. It helps find the number of sessions that were launched via Connection Lease.

Aggregated State

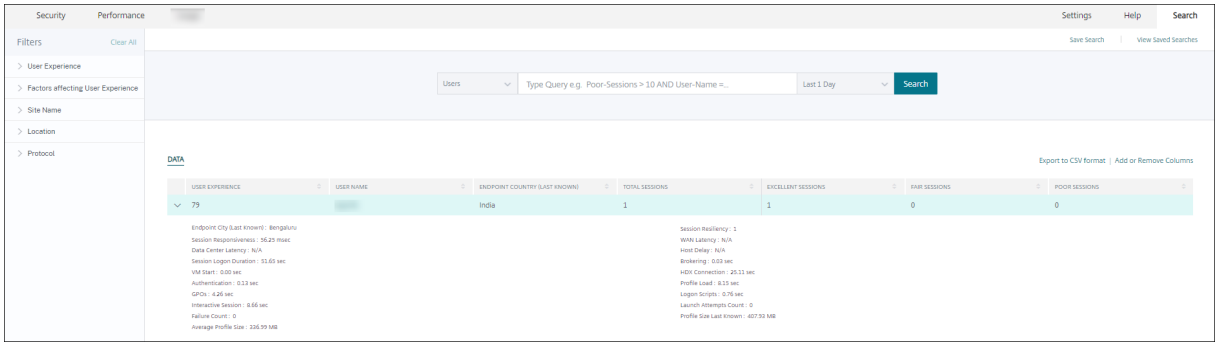
This facet is available on the Machines based self-service view to help narrow down your search based on the Aggregated State of the machine. Aggregated state represents the least favorable state the machine has been in, from among Ready for use, Active, Maintenance, Unregistered and Failed in that order.

Load

The Load facet is available on the Machines based self-service view to help narrow down your search based on the load on the machine. You can select machines with High, Medium, or Low load. The machines might not be categorized if they are in shutdown, unregistered or failed state or if the resource data is not available for the machine.

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

Self-service search for Users



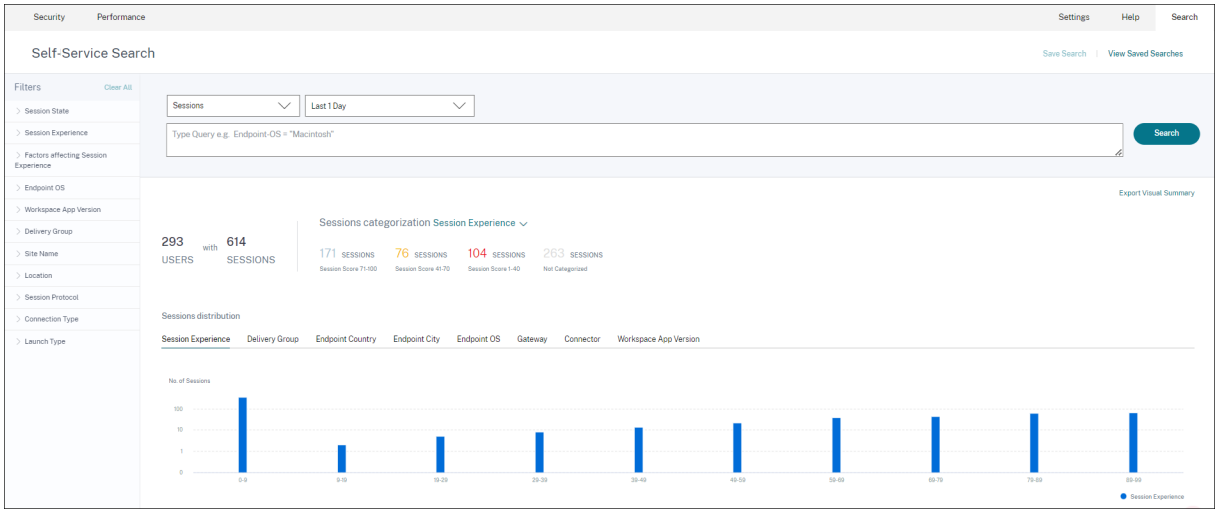
The Users based self-service page is available on clicking the user classification numbers on the User experience dashboard and drilldown pages. You can also access the Users based self-service view from the **Search** menu in your Citrix Analytics. In the list of services in the **Search** tab, select **Users** under the **Performance** section.

This view provides the important performance metrics related to users, such as,

- **Total Sessions:** Number of sessions successfully launched by the user.
- **Launch attempts count:** Number of times the user attempted to launch a session.
- **Failure count:** Number of sessions that failed to establish.
- **User Experience:** Overall user experience score calculated across all the sessions launched by the user.
- **Classification of sessions**: User sessions classified as excellent, fair, and poor.
- **Factors and sub-factors metrics** Key performance indicators that affect the user experience.
- **Endpoint Country (last known) and Endpoint Country (last known):** Last known location.
- **Profile Load:** The time taken to load the user's profile.
- **Profile Size (last known):** The last measured value of profile size.
- **Average Profile Size:** Average profile size for the selected duration.

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

Self-service search for Sessions



The Sessions-based self-service is available on clicking the session classification numbers on the dashboard. You can also access the Sessions-based self-service view from the **Search** menu in your Citrix Analytics. In the list of services in the **Search** tab, select **Sessions** under the **Performance** section.

Visual Summary on Sessions self-service view

Visual Summary presents raw data in the Sessions self-service tables as charts to improve visibility into the session performance.

The Visual Summary chart displays session categorization based on chosen criteria. In addition, you can choose to view the session distribution pivoted on a specific parameter. This helps identify session performance issues related to the pivots.

Use the visualization to identify patterns in data and troubleshoot specific session performance issues.

Factors Timeline(Preview) Factors Timeline pivot is added in the **Session Distribution** section of the Sessions self-service view under the **Session Responsiveness category**. You can use this pivot to analyze sessions based on Poor Output Bandwidth Usage, Poor Network Latency, and Poor ICARTT.

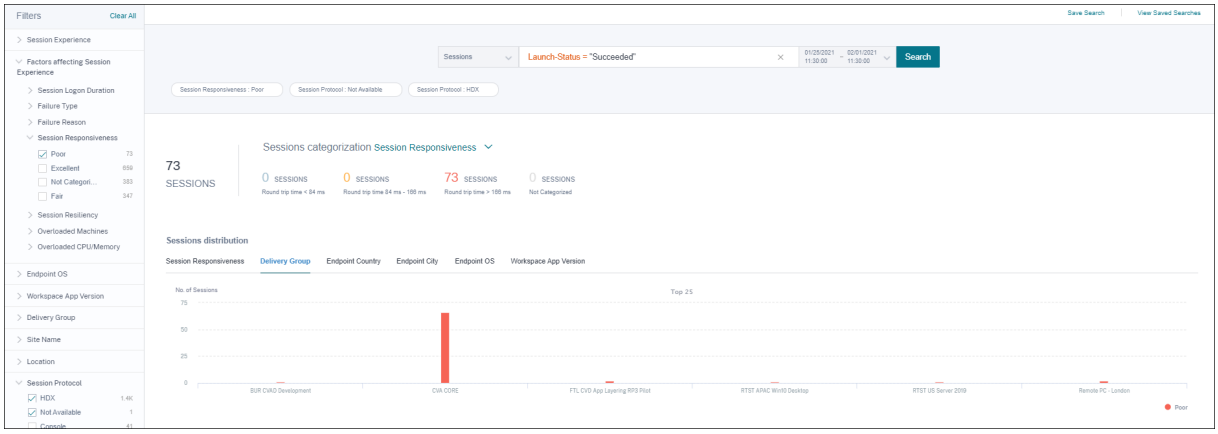
Use case - Access Visual Summary starting from the Dashboard You can use the Visual Summary chart to troubleshoot sessions having poor Session Logon Duration or Session Responsiveness experience displayed on the User Experience dashboard.

Click the poor sessions number in the Session Responsiveness chart to view the Visual Summary chart on the Sessions self-service view. A Visual Summary chart displays sessions categorized by Session

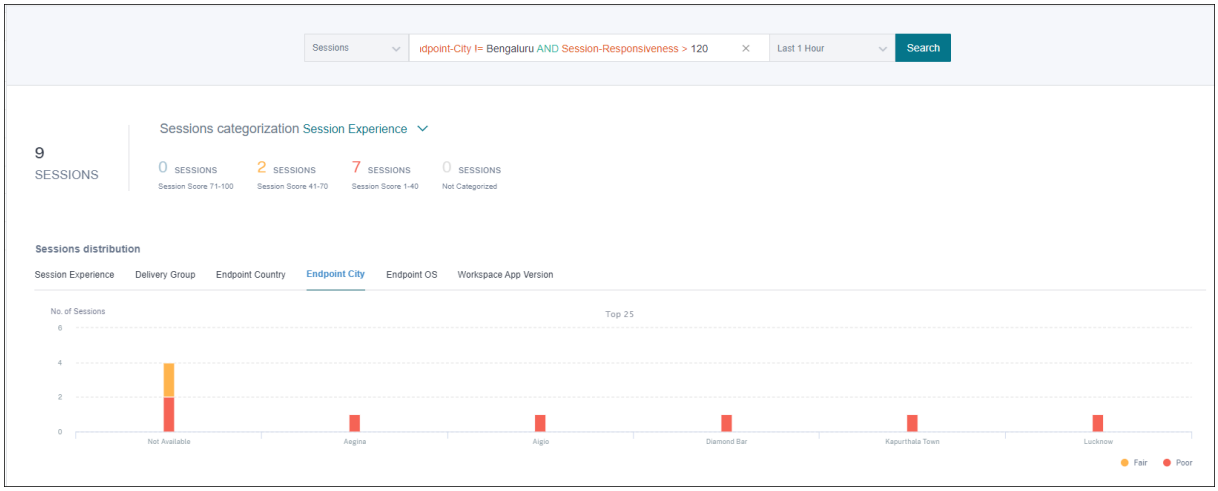
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Responsiveness over the selected duration. This helps identify specific time intervals where the ICA RTT has been high.

Further, choose the pivot from among Delivery Group, Endpoint Country, Endpoint City, Endpoint OS, Connector, Gateway, and Workspace version to plot the session distribution. For example, selecting the Delivery Group pivot results in sessions plotted based on Delivery Groups. Use the chart to identify if sessions of a specific Delivery Group have high ICA RTT. Performance of sessions from Delivery Groups delivering business critical applications can be monitored easily using Visual Summary.



Use case - Access Visual Summary using the Search menu You can visualize the result of your custom search query on the Sessions self-service view. In the **Search** tab, select **Sessions** under the **Performance** section. Enter your search query and click **Search**. To further customize the visualization of the results, choose the session categorization and distribution criteria.



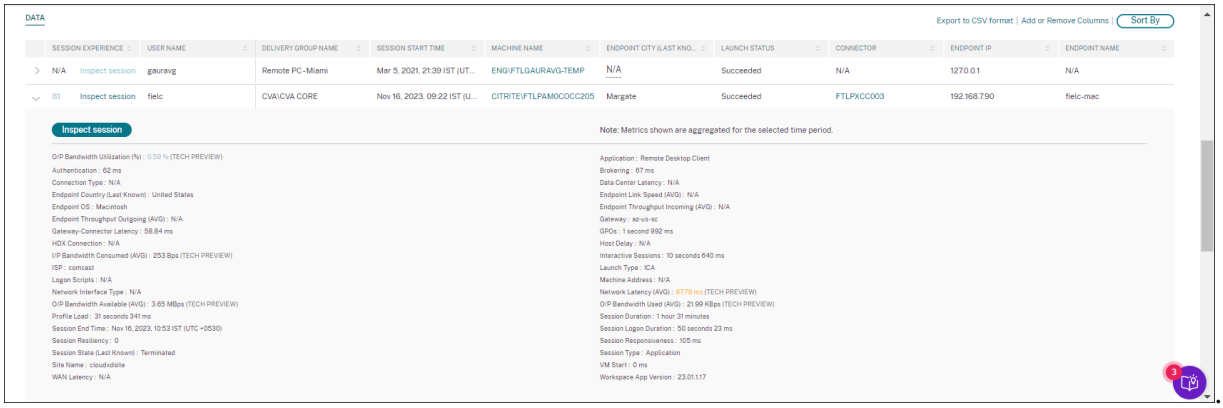
The preceding example shows a query returning sessions with poor Session Responsiveness and not located in `Bengaluru`. Further pivoting on the Endpoint City gives visibility into other locations from where sessions have high ICA RTT.

This feature is especially useful in reporting, you can also save and reuse the query.

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

Tabular data

This Sessions self-service view provides important performance metrics related to sessions in tabular format. Expanding a row displays session metrics that are relevant for the session state. If the session was in a disconnected state during the selected time interval, session metrics related to responsiveness and bandwidth, that are not applicable for disconnected sessions are not displayed. For a failed session, the failure reason and type are displayed to help triage the reason for the session failure. Any columns added to the table that are not relevant for the session state is displayed as "–".



- **Session Experience:** Session Experience score based on the performance factors.
- **Session specific metrics:** Metrics such as the session start time and launch status.
- **Data Center Latency:** This ICARTT subfactor is the latency measured from the Citrix Gateway to the server. A high Data Center Latency indicates delays due to a slow server network.
- **WAN Latency:** This ICARTT subfactor is the latency measured from the virtual machine to the Gateway. A high WAN Latency indicates sluggishness in the endpoint machine network. WAN latency increases when the user is geographically farther from the Gateway.
- **Host Latency:** This ICARTT subfactor measures the Server OS induced delay. A high ICA RTT with low Data Center and WAN latencies, and a high Host Latency indicates an application error on the host server.

  > Note:
  >
  > To get the ICARTT subfactor metrics, configure L7 latency thresholding. For more information, see L7 Latency Thresholding.

- **Endpoint City (last known)** and **Endpoint Country (last known):** Last known location.
- **Workspace App version and Endpoint OS**
- **Average Profile Size:** Average profile size for the selected duration.
- **Connection Type:** `internal` for direct connections from machine to endpoint, `external` for connections through gateway.

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

- **Gateway address:** Gateway address for external connections.
- **Machine FQDN:** Machine address with port id for internal connections.
- **Launch Status:** Displays the launch status of the session as `Succeeded`, `Failed`, or `User Terminated` - in case the user voluntarily closed the session.
  Launch Status is supported with endpoints running:

  - Citrix Workspace app 20.9.0 or later for Android
  - Citrix Workspace app 20.8.0 or later for iOS
  - Citrix Workspace app 20.8.0 or later for Windows

  Launch Status is not available with endpoints running Workspace on the web.
- **Network Interface Type** Displays the network interface type of the client. Possible values for Network Interface Type are:

  - Ethernet
  - Wi-Fi
  - TokenRing
  - FDDI
  - PPP
  - Loopback
  - Slip
  - Other
  - UnknownType

  The value of this field is N/A for endpoints running Citrix Workspace app Windows version earlier than 2105.
- **Bandwidth and Latency metrics (Preview)** Displays the following values:

  - Average values of the bandwidth metrics - Input Bandwidth Consumed, Output Bandwidth Available, Output Bandwidth Used,
  - Percentage value of Output Bandwidth Utilization, and
  - Average value of the Network Latency

  These metrics are available out-of-the-box for Citrix DaaS (formerly the Citrix Virtual Apps and Desktops™ service).

  - You need machines running Citrix Virtual Apps and Desktops 7 2112 or later.
  - The **VDA data collection for Analytics** policy must be set to **Allowed** on machines to enable the Monitoring service to collect machine related performance metrics. For more information, see Policy for collecting data for Analytics.
- **Session Duration** Displays the length of the session.

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

- **ISP** Displays the Internet Service provider serving on the endpoint. This metric is available if the endpoint is running Citrix Workspace app for Windows versions 1912 and later. For more details regarding the availability of this feature with Citrix Workspace app for other OS, see the Workspace app matrix.
- **Connector** Displays the name of the connector. This column helps identify connectors through which sessions with poor responsiveness are routed. Connector is an optional column that can be added to the Sessions self-service view by clicking Add or Remove columns.

  Clicking the Connector name link opens the Connector Statistics view. For more information, see the Connector Statistics article.
- **Gateway** Displays the name of the Gateway for on-premises and the Gateway Point of Presence for Cloud customers. This information helps identify the gateways through which sessions with poor responsiveness are routed. It also helps identify the distribution of sessions routed from a user location through different Gateway PoPs. Gateway is an optional column that can be added to the Sessions self-service view by clicking **Add or Remove columns**.

  The value of the **Connector** might be N/A for any of the following reasons:

  - There was a delay in receiving Connector events.
  - Cloud Connector version is earlier than 16.0.0.7.

  Also, ensure that the data processing via your Cloud Connectors is on. To do this, you can check the **Data processing on** state on the Cloud Connectors tile from the **Performance** tab in **Citrix Analytics** > **Data Sources**.
- **Gateway-Connector Latency** Displays the latency value from the Connector to the Gateway Point of Presence that was used to establish the session. Gateway-Connector Latency is an optional column that can be added to the Sessions self-service view by clicking **Add or Remove columns**.
- **Launch Type** Displays if sessions are ICA based or Connection leased. This information helps find the number of sessions that were launched via Connection Lease. You can use the failure reason to troubleshoot Connection leased sessions that have failed to launch.
- **Endpoint Link Speed (Avg)** Link speed helps identify if the poor session experience was due to low speed.
- **Endpoint Throughput Incoming (Avg)** Displays the total bytes received.
- **Endpoint Throughput Outgoing (Avg)** Displays the total bytes sent.

> **Note:**
>
> The Endpoint metrics require that the StoreFront server of your on-premises Site deployment is configured with Citrix Analytics. For more information, see Onboard Virtual Apps

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

> and Desktops sites using StoreFront.

- **Endpoint IP** Displays the IP address of the endpoint.
- **Endpoint Name** Displays the IP name of the endpoint.
- **Failure Type** –Indicates the kind of failure from among the following values:
  - Client Connection Failure
  - Machine Failure
  - No Capacity Available
  - No Licenses Available
  - Configuration
  - Communication Failure
  - Unknown error
- **Failure Reasons** –Indicates the exact reason for the failure. You can resolve the failure using the corresponding recommended steps in Citrix Director failure reasons and troubleshooting. The failure columns are especially helpful when you navigate from the failed session count on the dashboard to a filtered set of failed sessions in Sessions self-service view.
- **Session Type** –Indicates if the session is an application or a desktop session.
- **Session State** –Indicates the state of the session from among the following values:
  - Unknown
  - Connected
  - Disconnected
  - Terminated
  - PreparingSession
  - Active
  - Reconnecting
  - NonBrokeredSession
  - Other
  - Pending
- **Session End Time** –Indicates the time at which the session ended.

Click the **Inspect Session** link from the Self-service view for Sessions to open the Session Details view for the session.

Tabular data on the Session-based self-service view is **color coded** to indicate the excellent, fair, or poor category the metrics belong to. This categorization is based on the individual threshold levels of the metrics. The thresholds are calculated dynamically, for more information, see How are Dynamic Thresholds calculated?.

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

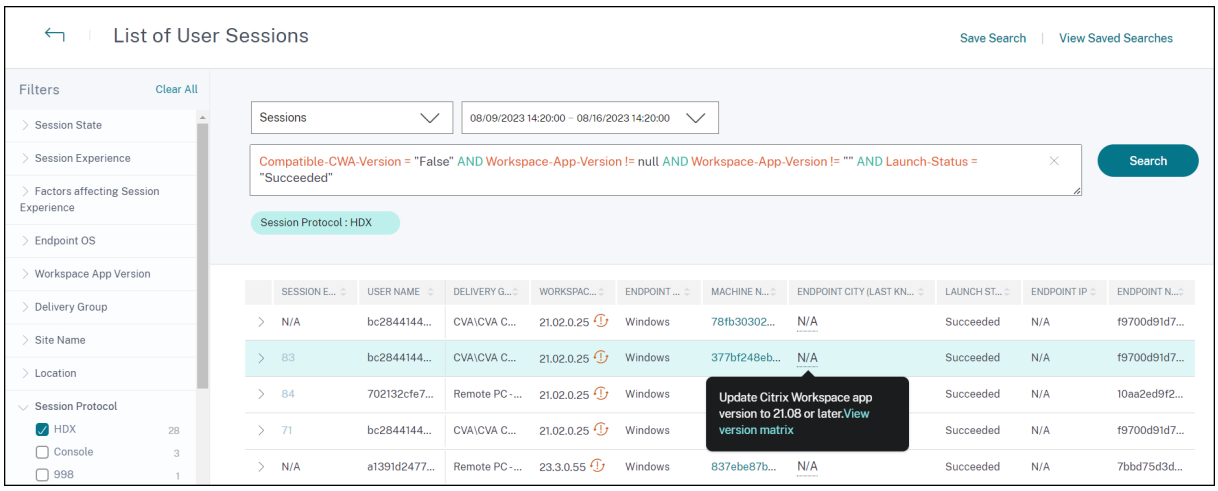
SESSION EXPERIENCE	USER NAME	DELIVERY GROUP NAME	SESSION START TIME	MACHINE NAME	ENDPOINT CITY (LAST KNOWN)	LAUNCH STATUS
0		CVA CORE	May 27, 2021, 17:54 IST (UTC +...		N/A	Failed
0		CVA CORE	Jun 18, 2021, 13:02 IST (UTC +...		N/A	Failed
0		RemotePC - FTL Test	Jun 1, 2021, 20:51 IST (UTC +0...		N/A	Failed
0		CVA CORE	Jun 10, 2021, 15:41 IST (UTC +0...		N/A	Failed
0		Remote PC - London	Jun 1, 2021, 18:29 IST (UTC +0...		N/A	Failed
0		Remote PC - London	Jun 7, 2021, 15:08 IST (UTC +0...		N/A	Failed
0		CVA CORE	Jun 7, 2021, 07:12 IST (UTC +0...		N/A	Failed
0		CVA CORE	Jun 16, 2021, 16:46 IST (UTC +...		N/A	Failed
42		CVA CORE	Jun 19, 2021, 00:21 IST (UTC +...		North Grafton	Succeeded
82		CVA CORE	Jun 4, 2021, 04:47 IST (UTC +0...		Fremont	Succeeded
N/A		CVA CORE	Jun 19, 2021, 22:57 IST (UTC +...		Kharanitar	Succeeded
27		CVA CORE	Jun 2, 2021, 21:29 IST (UTC +0...		Bengaluru	Succeeded
68		CVA CORE	Jun 7, 2021, 19:36 IST (UTC +0...		Pompano Beach	Succeeded

Similar color coding is applied to the metrics available on expanding the rows on the Session-based self-service view.

Color coding visually aids in focusing on and identifying factors that are contributing to poor performance. It also gives an overview of the performance across various factors for the sessions that have been filtered to be seen in the current view.

Tool tips elaborating the reason for N/A values are now in available in the Sessions self-service view for the following endpoint-related metrics:

- Workspace App Version
- Endpoint Country (Last known)
- Endpoint City (Last known)
- Endpoint Link Speed (P95)
- Endpoint Throughput Incoming (P95)
- Endpoint Throughput Outgoing (P95)
- ISP (Internet Service Provider)

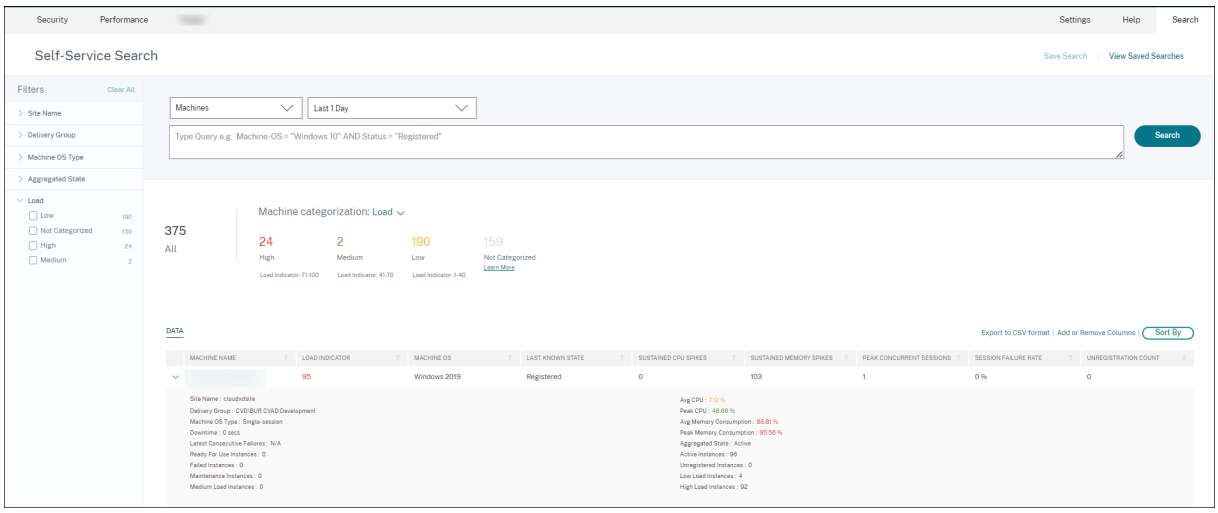


Tooltips are displayed on the N/A values of these metrics with the reasons as incorrect StoreFront

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

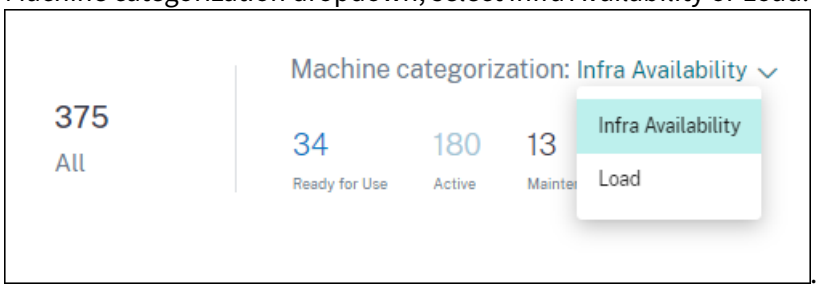
onboarding, or sessions launched from endpoints that run unsupported OS platforms or incompatible Citrix Workspace app versions.

Self-service search for Machines



You can access the Machines based self-service view from the **Search** menu in your Citrix Analytics. In the list of services on the **Search** tab, under the **Performance** section, select **Machines**. The Machines based self-service view is also available when you drill down from black hole machines. To access the view, on the User experience dashboard, in the **Failure Insights** section, click the **Black hole machines** number.

The Machines self-service view provides machine categorization based on availability and load. In the Machine categorization dropdown, select Infra Availability or Load.



Machines are categorized as follows based on availability:

- Ready for Use - Machines in a healthy state with no active sessions.
- Active –Machines with at least one active session.
- Maintenance –Machines in Maintenance mode, no connections are accepted.
- Unregistered - Machines not registered with the Broker Service.

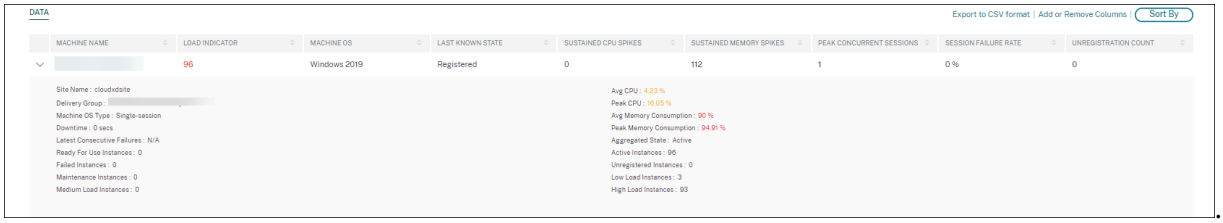
Machines are categorized based load using the Load Indicator of the machines. The load indicator for a machine is calculated based on the resource utilization, the overall user experience on the machine

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

and the number of sessions hosted in the case of multi-session OS machines. The value is aggregated over the selected time period. This helps identify machines that are underutilized or overloaded. This enables proactive action to ensure optimal usage of the infrastructure and improve the overall machine performance. Machines are categorized as follows based on load:

- High(red) - Machines with Load Indicator in the range 71-100
- Medium(green) –Machines with Load Indicator in the range 41-70
- Low(amber) –Machines with Load Indicator in the range 1-40.
- Not Categorized - The machines might not be categorized if they are in shutdown, unregistered or failed state or if resource data is not available for the machine.

The Machines self-service view provides the important performance metrics related to machines.



- **Status**: Last known machine state - `Registered`, `Unregistered`, `Powered off`, or`Failed`.
- **Sustained CPU Spikes**: Number of CPU spikes in the selected time period. Each CPU spike refers to sustained CPU utilization above the threshold of 80% for 5 min or more.
- **Sustained Memory Spikes:** Number of memory spikes in the selected time period. Each memory spike refers to sustained memory consumption above the threshold of 80% for 5 min or more.
- **Peak Concurrent Sessions:** Number of sessions running concurrently on the machine.
- **Unregistration Count:** Number of times the machine transitioned into an unregistered state during the selected period.
- **<`Aggregated State`/> Instances:** Aggregated state represents the least favorable state the machine has been in, from among the Ready for use, Active, Maintenance, Unregistered and Failed machine states in that order. <`Aggregated State`> Instances represent the number of instances (15 min intervals) the machine was in a specific Aggregated state during the selected period. The column names are available as Ready for use Instances, Active Instances, Maintenance Instances, Unregistered Instances, and Failed Instances.
- **Latest Consecutive Failures:** Number of consecutive session failures in the last 5 min.
- **Downtime:** Period in seconds during which the machine was in `Unregistered`, `Failed`, or `Powered off` state during the selected interval.
- **Avg CPU:** Average CPU utilization in the selected time period.
- **Peak CPU:** Maximum CPU utilization recorded in the selected time period.
- **Avg Memory Consumption:** Average memory consumption in the selected time period.

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

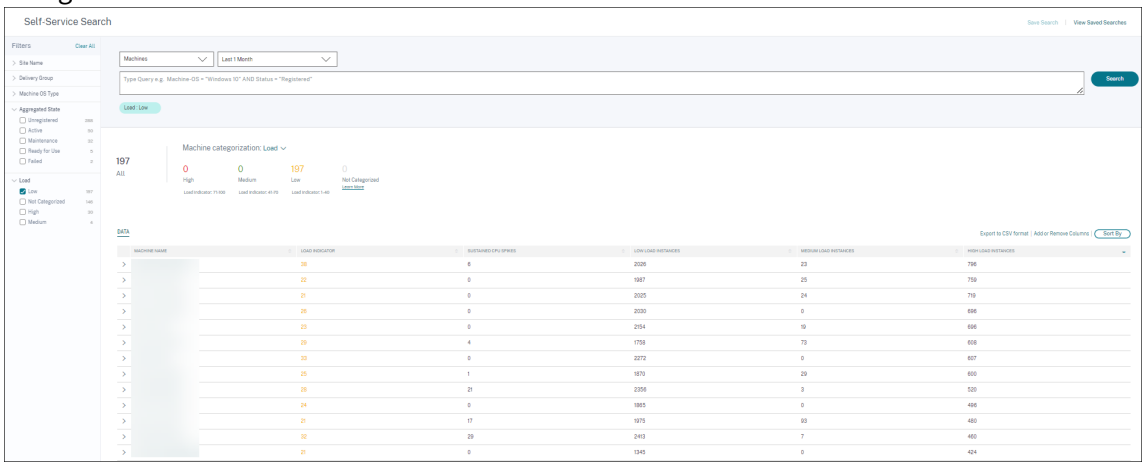
- **Peak Memory Consumption:** Maximum memory consumption recorded in the selected time period.
- **Load Indicator:** Load Indicator is a score indicating the load on the machine. It is calculated based on the resource utilization, the overall user experience on the machine and the number of sessions hosted in the case of multi-session OS machines. The value is aggregated over the selected time period.
- **High, Medium and Low Load Instances:** Number of instances during the selected period when the machine was in High Load (Load Indicator: 71-100), Medium Load (Load Indicator: 41-70) and Low Load (Load Indicator: 1-40). These metrics help quantify and evaluate the load on the specific machine.

This view helps admins identify specific machines contributing to poor user experience and correlate the machine resource parameters with the performance factor metrics.
Clicking the machine name on the Machines based self-service view opens the Machine Statistics view. For more information, see the Machine Statistics article.

> **Note:**
>
> The values of the metrics, Avg CPU, and Avg memory consumption is calculated only in the duration when the machine was overloaded.

Use case - Optimize Machine Usage using Machine Load metrics

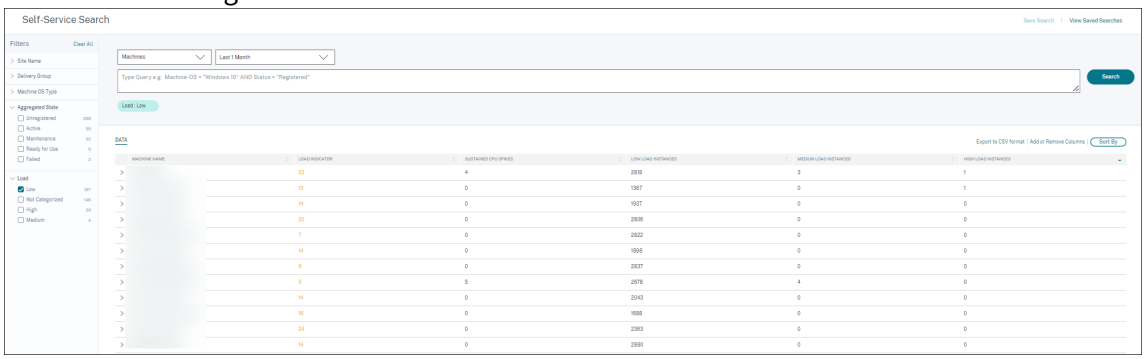
1. Go to Machines self-service view. Choose a suitable time period.
2. Expand the **Load** facet and select the **Low** category. Machines with aggregated low load for the selected time period are displayed.
3. Now, add the High, Medium, and Low Load Instances columns to the view.
4. Sort the view on High Load Instances. The screenshot below shows the first page of the sorted view with machines that have aggregated low load during the past one week but a high number of high load instances.



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

This indicates that though the overall load on these machines is low, the machines are well used. Click the machine name to see the Machine Statistics page. Analyze the usage pattern during the day to understand if more machines need to be onboarded onto the environment.

5. Scrolling to the last few machines in this list shows machines with low aggregate load and the least number of high load instances.

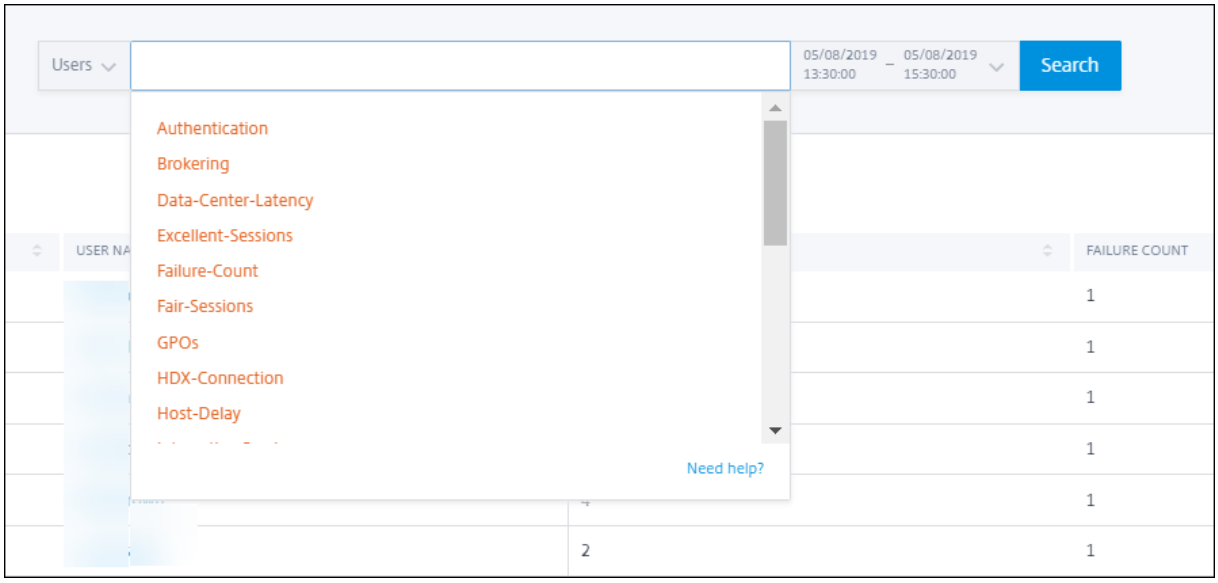


Click the machine name to see the Machine Statistics page and analyze the usage pattern. Also, the name of the Catalog the machine belongs to, is available here. This helps identify the least used machines that could possibly be shut down or switched on during specific periods during the day to reduce cost.

Using the Load facet to identify the aggregated load on the machines, and the instances columns to identify the machine load pattern during the time period helps optimize the infrastructure as per usage.

Specify search query to filter events

When you place your cursor in the search box, you get the list of search suggestions relevant for the Citrix Analytics for Performance. Use the search suggestions to specify your query and filter the events.

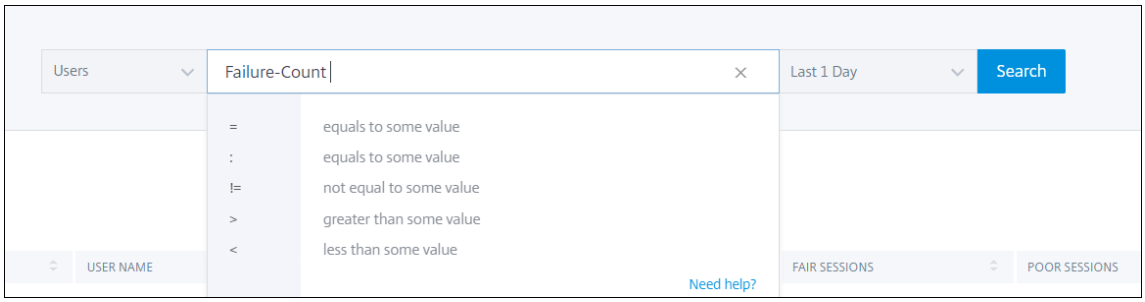


© 1997–2026 Citrix Systems, Inc. All rights reserved.

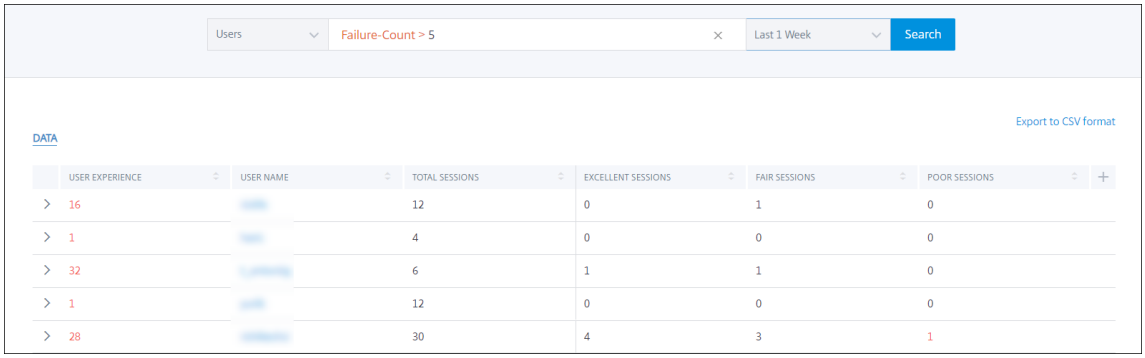
You can also use operators in your search queries to narrow the focus of your search. For more information on the valid operators, see Use search query in the search box to filter events.

For example, you want to search events for users with Failure-count more than 5 in the past week. Specify the following query.

1. Click the search bar and select the **Failure-count** field.
2. Click **Failure-count**, select the > sign, and then specify the value "5".



3. Click the time period drop-down list and select **Last 1 week**



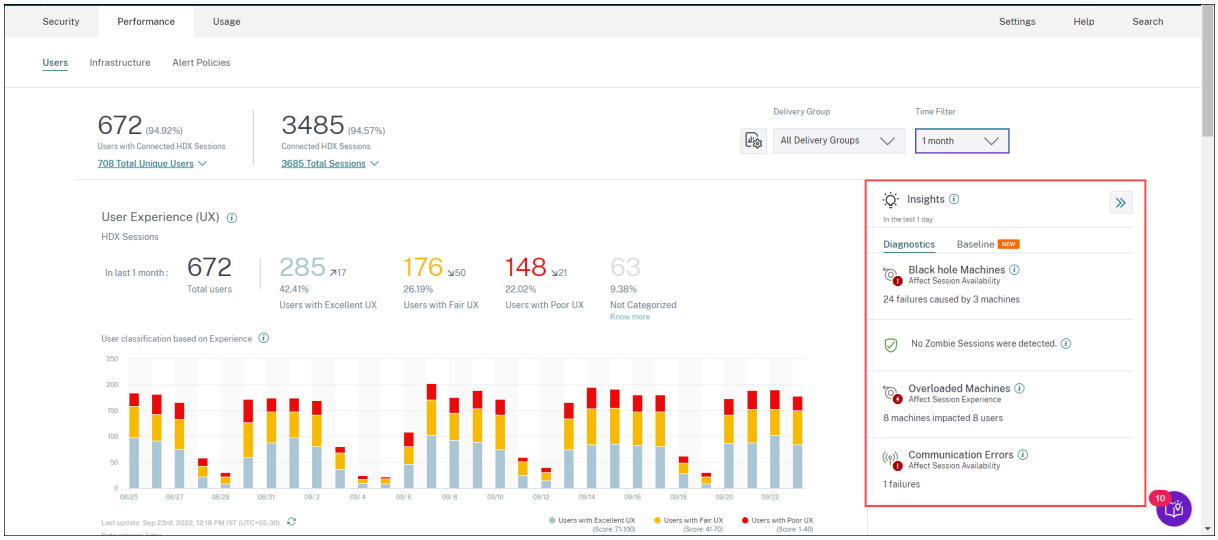
4. Click **Search** to view the events based on your search query.

Insights

September 1, 2025

The **Insights** panel provides information on the root causes for session failures in your environment. Drilling deeper into specific metrics with these insights helps troubleshoot and resolve session failures faster. Failure Insights specifically help administrators to improve the session availability, which is an important factor that determines user experience.
These insights are designed to aid in proactive monitoring of the user experience. Hence, Insights are displayed for a maximum duration of the 1 day even if a 1 month or 1 week time period is selected on the dashboard.

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

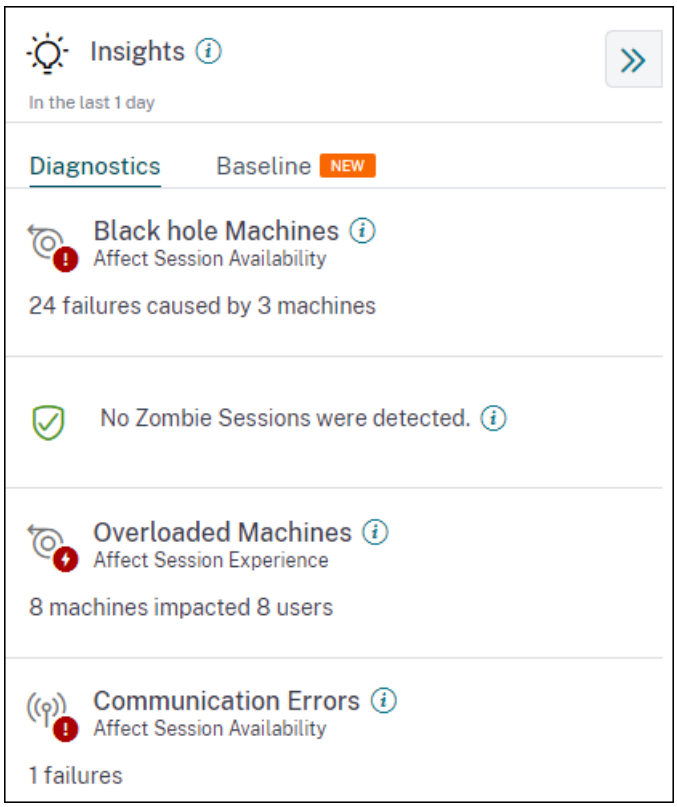


Clicking the insight from the summary pane displays the insight pane with details about the insight and options to drilldown to the Self-service views.

Insights are displayed in two categories:

- **Diagnostic Insights:** The Diagnostic subpane shows crucial insights about failures that have occurred on the site. The Blackhole Machines, Zombie Sessions, Overloaded Machines, and Communication Error Diagnostic Insights are available in this subpane.
  Each insight upon expansion displays a link to the failed sessions or the machines hosting them. This leads to the self-service view containing the failed machines or sessions. Further drill-down is possible from here when you click a specific machine, session, or connector and see the time-line details and the detailed metrics.

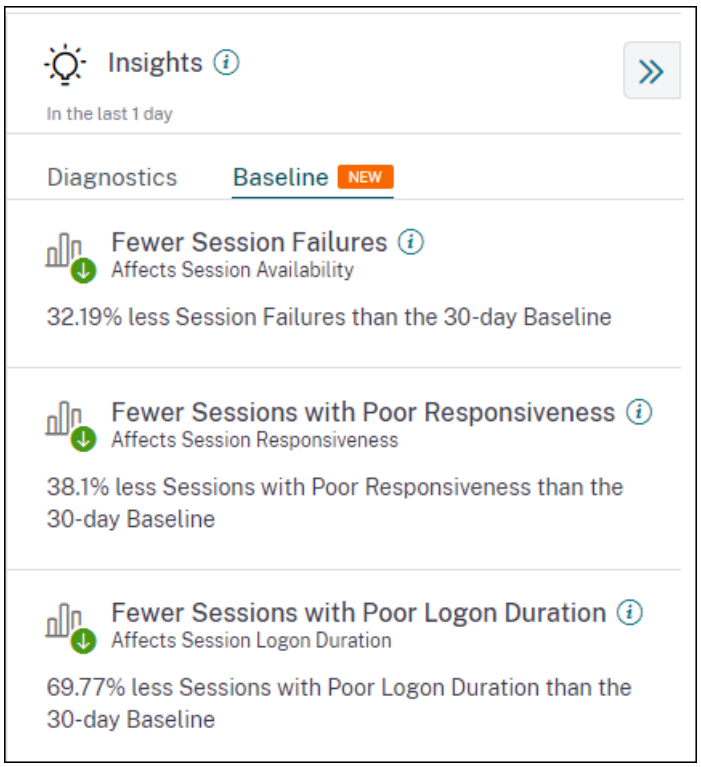
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Top failure patterns detected with respect to the site, Delivery Group, single or multi-OS session machines is displayed. These patterns are aimed to help you spot if there is a specific cohort of users experiencing the issue. In cases where the system is unable to highlight any pattern due to a distributed cohort, it is recommended to drill down to self-analyze. Also, actions that are recommended to be taken to troubleshoot and resolve the issues are shown.

- **Baseline Insights:** The Baseline Insights provide the deviation of key performance metrics from the historical baseline. These insights show if key metrics are improving or deteriorating in a glance. They help spot incident indicators quickly and take proactive steps to improve the performance of your environment.

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



Baseline Insights for Poor Session Failures, Session Responsiveness, and Session Logon Duration are available on the **Baseline** subpane. The panes show if you have fewer or more sessions with Session Failures, Poor Session Responsiveness, and Poor Session Logon Duration.

The baseline is based on the P80 value of the metric over the last 30 days measured during the same time interval as the one for which the insight is being derived. The P80 value is used to ensure that outlier conditions like outages do not inflate the baseline.

For example, if the current time stamp is Sep 23, 2022, 02:35 PM, and you choose to see the Session Failure Baseline Insights for the last 2 hours. The baseline is calculated as the P80 value of Session Failures during the interval 012:35 p.m. - 02:35 p.m. over the last 30 days.

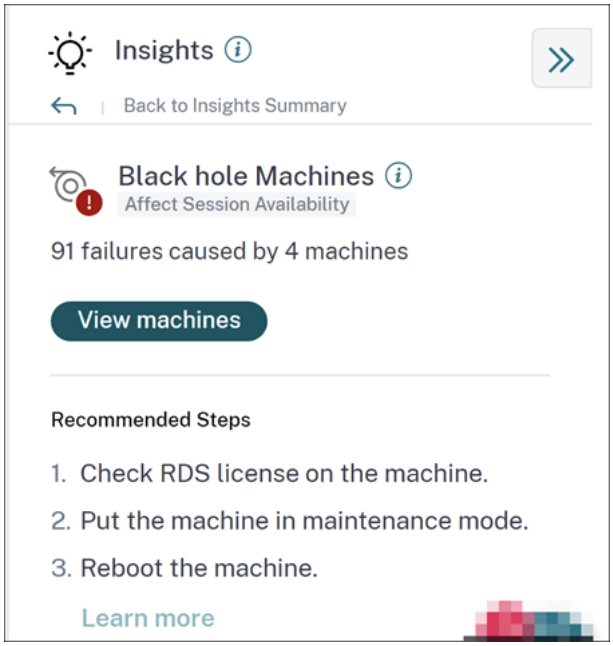
> **Note:**
>
> - Baseline Insights are available seven days after a new customer is onboarded.
> - Updating alert parameters also alters the calculation of the corresponding insight on the UX dashboard. For more information, see Alerts.

Diagnostic Insights: Black hole machines

Some machines in your environment though registered and appearing healthy might not service sessions brokered to them, resulting in failures. Machines that have failed to service four or more consecutive session requests are termed as Black hole machines. The reasons for these failures are related to various factors that might affect the machine, such as insufficient RDS licenses, intermittent net-

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

working issues, or instantaneous load on the machine. These failures do not include failures due to capacity or license availability. The presence of black hole machines in the environment increases session failures resulting in poor session availability.
The Black hole machines insights show the number of black hole machines identified in your environment during the selected time period.



Clicking **View machines** opens the Machines based self-service view that is filtered to show all the black hole machines in your environment during the selected time period. Here, you can analyze the individual performance metrics of the machine to identify and understand possible reasons for the machine not accepting session requests. For more information about the performance indicators available on the Machines based self-service view, see Self-service search for Machines.
Further, clicking the machine name opens the Machine Statistics view that helps correlate the resource performance parameters of the machine with the session performance parameters during the same time period. For more information see the Machine Statistics view article.

Recommended Steps to help reduce the number of black holes are provided,

- to check the RDS license status,
- to put the machine in maintenance mode, or
- to reboot the machine.

The **Patterns Detected** section shows the top three patterns noticed in black hole machines with respect to the following criteria:

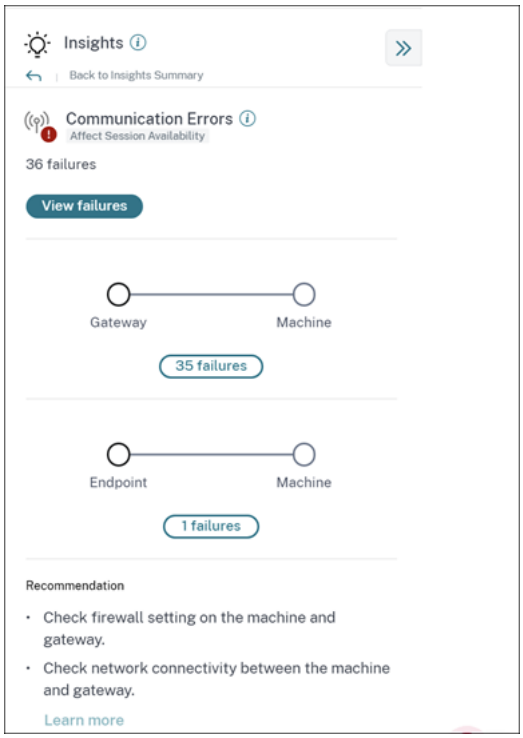
- Number of black hole machines in each Delivery Group
- Number of black hole machines running single-session or multi-session OS

For more information about Black Hole Machine Alerts, see the Alerts article.

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

Diagnostic Insights: Communication Errors

The Communication Errors subpane lists the number of session failures due to communication errors between the endpoint (where the user launches the session) and the machine. These errors can occur due to incorrect firewall configurations or other errors on the network path.



The two categories of communication errors are:

- Endpoint to machine—lists the sessions where communication errors have occurred between the endpoint and the machine.
- Gateway to machine—lists the sessions where communication errors have occurred between the gateway and the machine.

Additionally, the Communication Error subpane displays the following recommendations to resolve the errors.

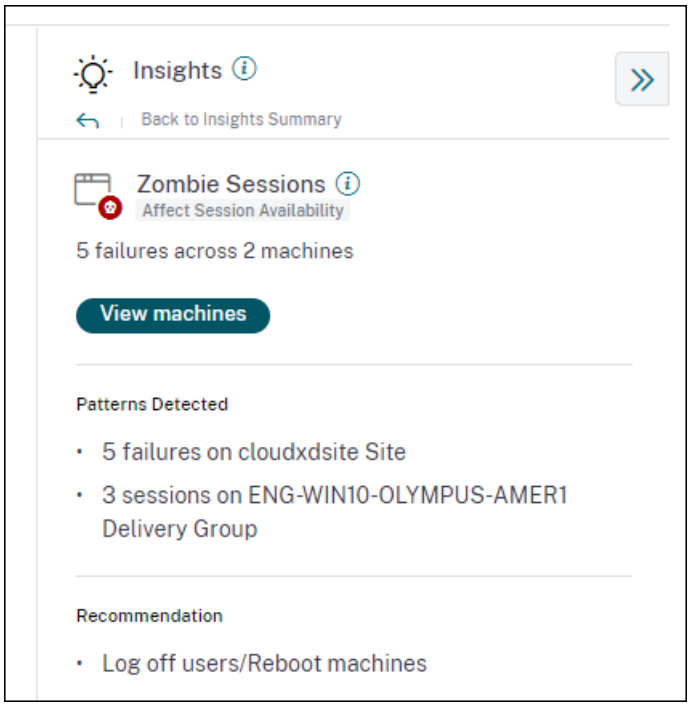
- Check the firewall settings on the machine and gateway.
- Check network connectivity between the machine and gateway.

Clicking the failure number opens the sessions based self-service view that is filtered to show all the sessions that have failed due to communication errors in your environment during the selected time period. This view helps analyze the individual sessions that have failed and get a possible root cause. For more information about the indicators available on the sessions based self-service view, see Self-service search for sessions.

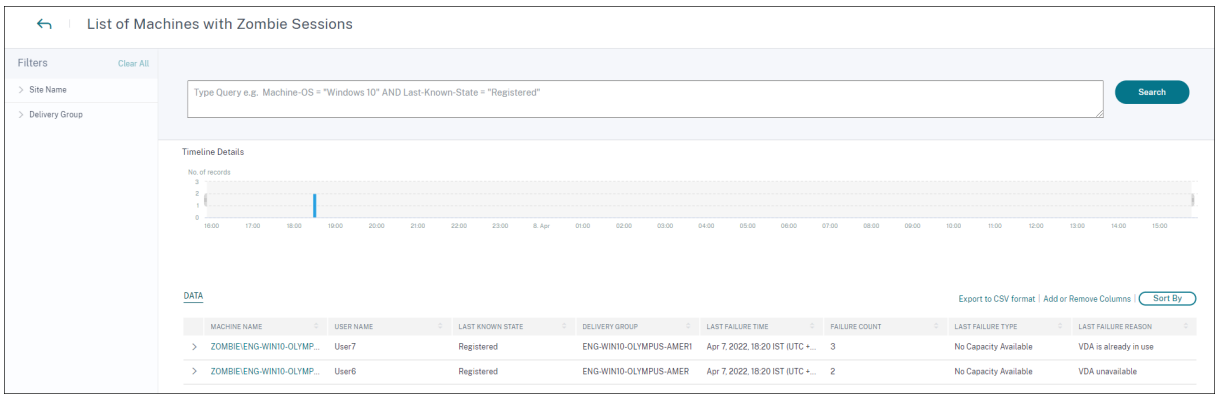
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Diagnostic Insights: Zombie sessions

The Zombie Sessions subpane shows information on session failures that have occurred due to zombie sessions in the environment. A zombie session is an abandoned session on a single-session OS machine resulting in new session launches on the machine to fail. Attempts to launch sessions on this machine fails with an **Unavailable Capacity** error. All future session launch attempts fail until the abandoned session is terminated. Zombie Sessions insights aim to help in spotting these machines with abandoned sessions and to proactively mitigate these failures.



Click **View machines** to go to the Self-service view filtered with the list of machines containing Zombie Sessions.



Here, **Failure Count** represents the number of session failures that have occurred in the selected interval. The **Last Failure Type and Reason** help root cause reasons for machines containing zombie sessions.

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

A Zombie session alert mail is generated when a new machine with a zombie session is detected in the environment in a 15 mins interval. For more information, see the [Alert for Machines with Zombie Sessions] Self-service search for sessions article.

Recommended actions for Zombie Sessions

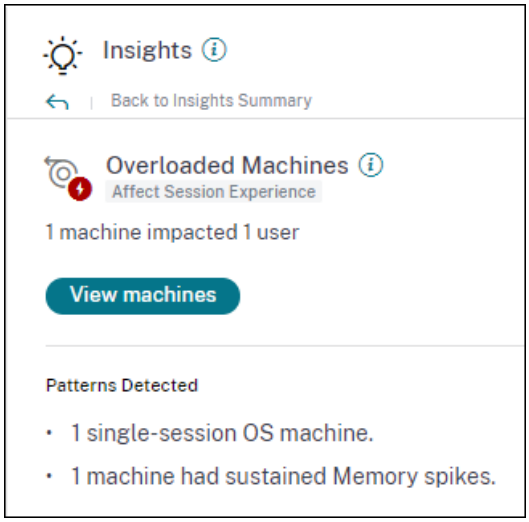
You can either log the users off or reboot the machines containing Zombie sessions.

- You can log the users out of the zombie sessions using Monitor for Citrix DaaS sites. For more information, see the Site Analytics article.
- You can reboot the machines containing zombie sessions from Performance Analytics, see the Machine actions article.

Diagnostic Insights: Overloaded Machines

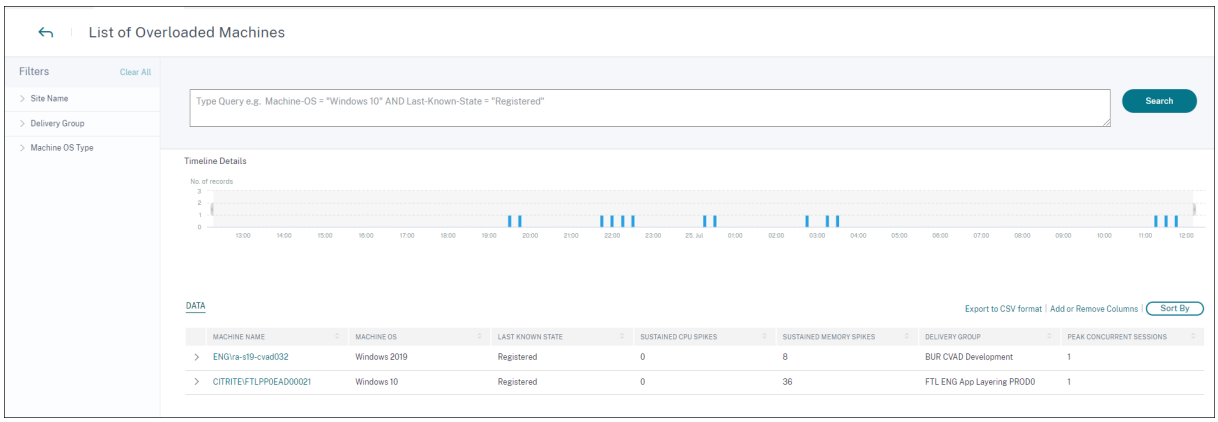
Overloaded Machines Insight gives visibility into overloaded resources causing poor experience. Machines that have experienced sustained CPU spikes, or high memory usage, or both, that have lasted for 5 minutes or more, resulting in a poor user experience in the selected duration are considered to be overloaded. There might be other machines in the environment with high resource usage but not impacting the User Experience. These machines are not categorized as overloaded machines.

The Overloaded Machines Insight shows the number of overloaded machines and the number of users affected in the selected duration.



Click **View Machines** to see the overloaded machines listed on the Machines self-service page for Overloaded Machines. Overloaded machines are listed with the number of Sustained Memory and CPU Spikes that have occurred on these machines during the selected interval.

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



The timeline graph shows the number of machines that have been overloaded over the selected time interval plotted at a 15-minute interval.
You can further click a specific machine to see the Machine Statistics view.

The **Patterns Detected** section shows the top three patterns noticed in overloaded machines with respect to the following criteria:

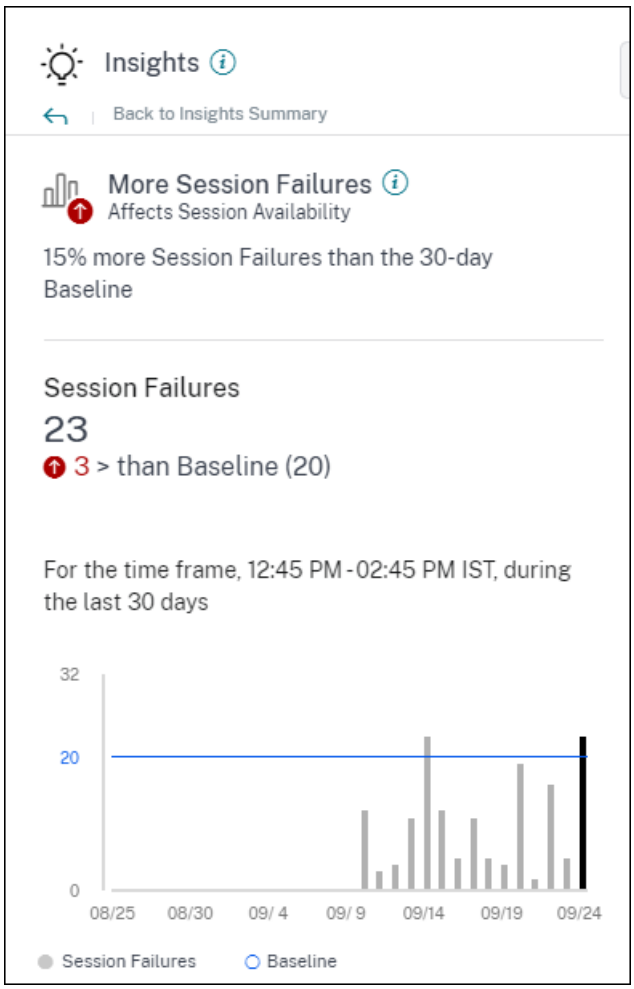
- Number of overloaded machines in each Delivery Group
- Number of overloaded machines running single-session or multi-session OS
- Number of overloaded machines with Sustained Memory or CPU spikes

For more information about Overloaded Machine Alerts, see the Alerts article.

Baseline Insights: Session Failures

This insight shows the deviation of the session failure count from the 30-day baseline value. The baseline value is calculated as the P80 value of the session failure count measured during the last 30 days for the same time frame.

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



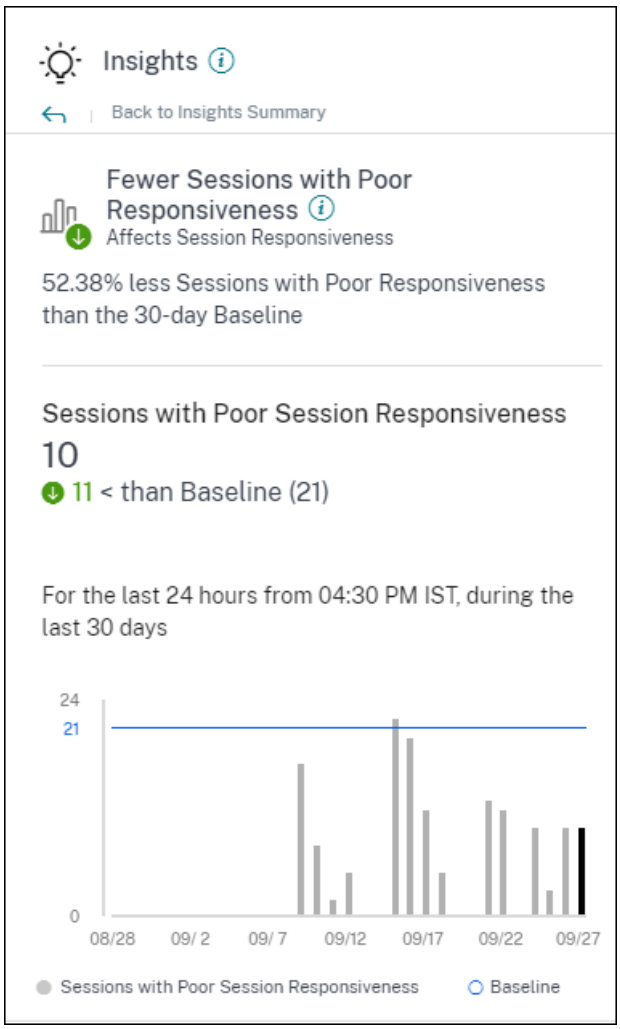
Session Failures Baseline insight on expansion shows the following:

- the percentage change in the current session failures count compared to the baseline value
- the current number of session failures
- increase or decrease in the number of session failures with respect to the baseline value
- a graph showing the baseline value and session failure count plotted over the last 30 days

Baseline Insights: Session Responsiveness

This insight shows the deviation of the number of sessions with poor responsiveness from the 30-day baseline value. The baseline value is calculated as the P80 value of the number of sessions with poor responsiveness measured during the last 30 days for the same time frame.

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



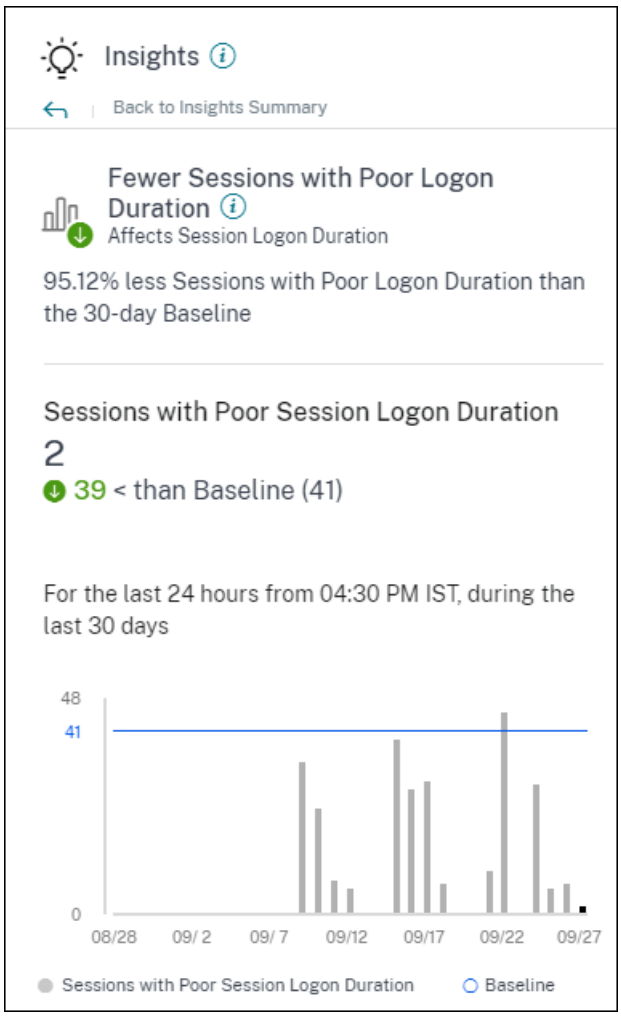
Session Responsiveness Baseline insight on expansion shows the following:

- the percentage change in the current number of sessions with poor responsiveness value as compared with the baseline value.
- the current number of sessions with poor responsiveness.
- increase or decrease in the number of sessions with poor responsiveness with respect to the baseline value
- a graph showing the baseline value and number of sessions with poor responsiveness plotted over the last 30 days

Baseline Insights: Session Logon Duration

The **Sessions with Poor Logon Duration** Baseline Insight shows the deviation of the number of sessions with poor logon duration from the 30-day baseline value. The baseline value is calculated as the P80 value of the number of sessions with poor logon duration measured during the last 30 days for the same time frame.

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



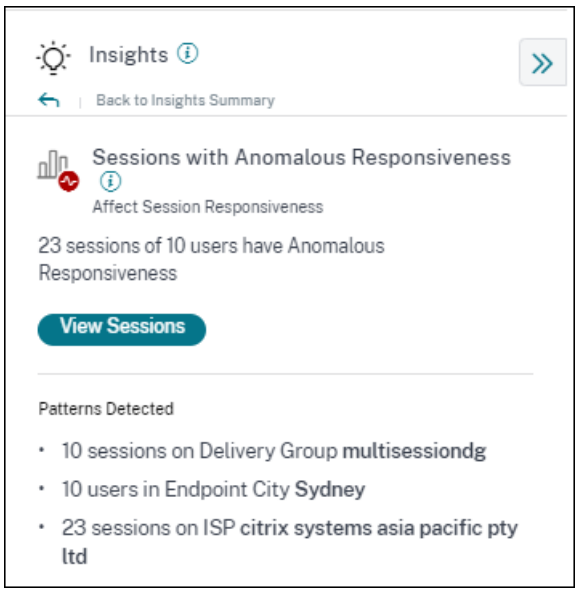
Session Logon Duration Baseline insight on expansion shows the following:

- the percentage change in the current number of sessions with poor logon duration as compared with the baseline value
- the current number of sessions with poor logon duration
- increase or decrease in the number of sessions with poor logon duration with respect to the baseline value
- a graph showing the baseline value and number of sessions with poor logon duration plotted over the last 30 days

Baseline Insights: Sessions with Anomalous Responsiveness

This insight shows the number of sessions and users whose responsiveness is higher than the 30-day user-specific baseline value for responsiveness. The baseline value is calculated using the P95 ICARTT values measured over the last 30 days for the same time frame.

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



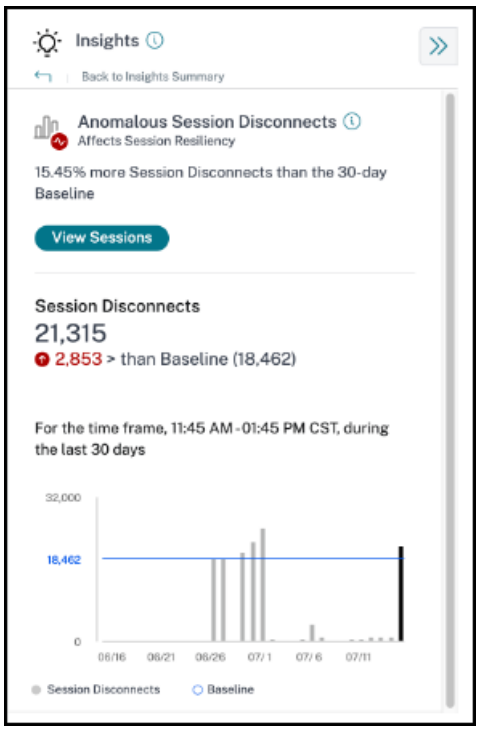
This insight on expansion shows the following data:

- **View Sessions** link takes you to the Self-Service view listing the sessions with anomalous responsiveness during the selected time frame.
- Top patterns detected with respect to Delivery Group, Endpoint City and ISP are displayed to help you spot if there is a specific cohort of users experiencing the issue.

Baseline Insights: Anomalous Session Disconnects

The **Anomalous Session Disconnects** Baseline Insight shows the deviation of the number of session disconnects from the 30-day baseline value. The baseline value is calculated as the P80 value of the number of session disconnects measured during the last 30 days for the same time frame.

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



Session Disconnects Baseline insight on expansion shows the following:

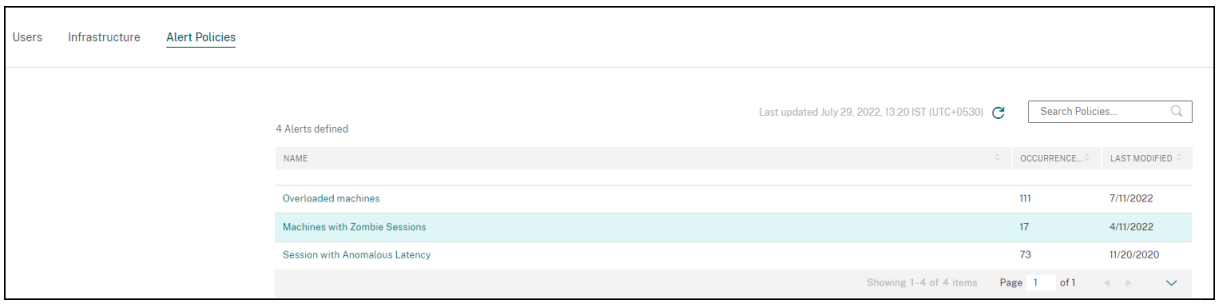
- the percentage change in the current number of session disconnects as compared with the baseline value
- the current number of session disconnects
- increase or decrease in the number of session disconnects with respect to the baseline value
- a graph showing the baseline value and number of session disconnects plotted over the last 30 days

Alerts

September 1, 2025

Performance Analytics generates alerts to help administrators to monitor the environment proactively. The alerts are generated when factors affecting the user experience get deteriorated.

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



The available policies are listed in the **Alert Policies** tab. The alerts are enabled by default, and can be disabled using the **Status** toggle. Alert email notifications for stakeholders can be enabled for recipients who don't have administrator access to your Citrix Cloud account. Click the alert name to edit the mail recipients list. For more information, see the Email distribution list article.

You must enable receiving email notifications for all recipients from the **Account Settings** menu in Citrix Cloud to receive the alert mails. For more information, see the Notifications article.

Webhook Support for Alert Notifications

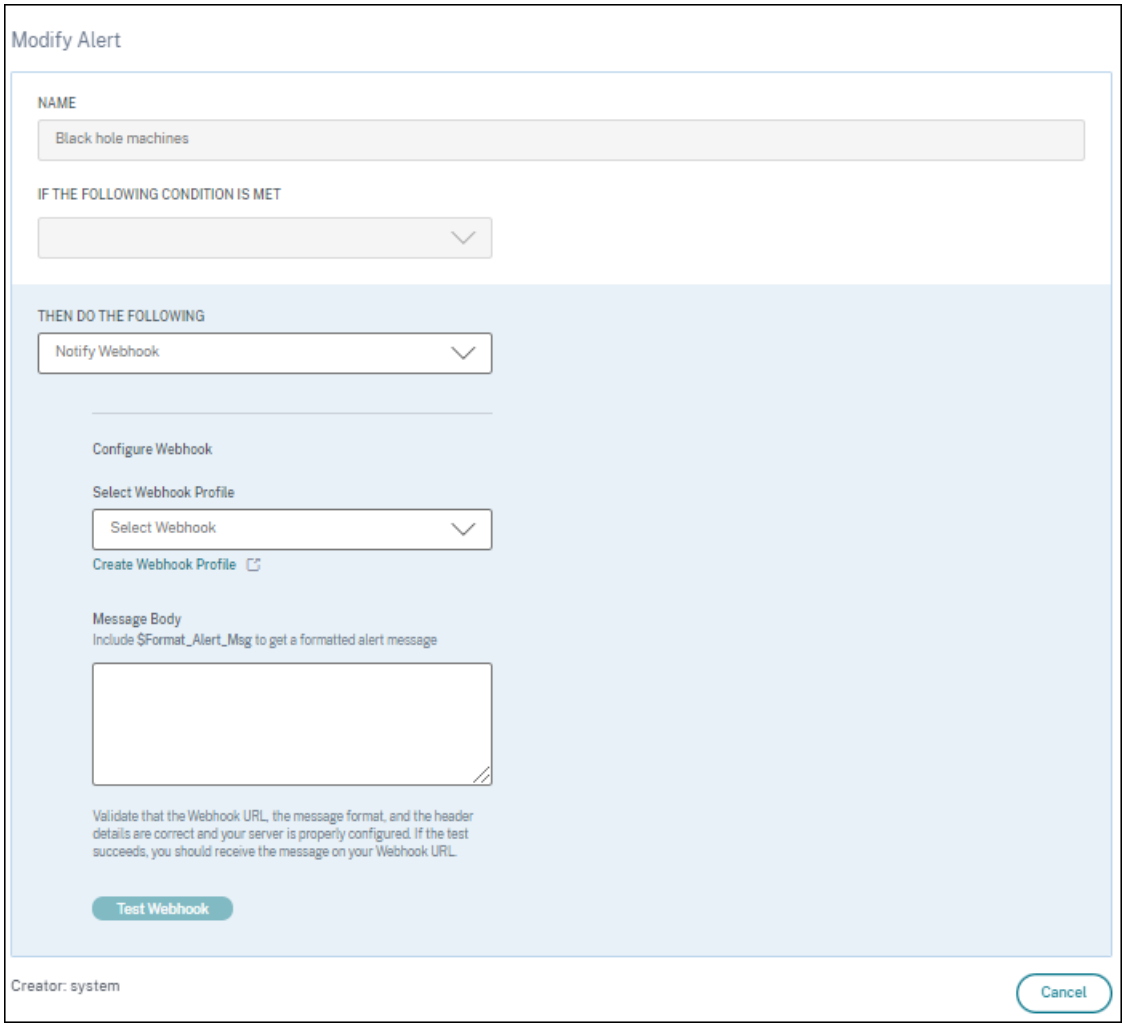
You can publish alert notifications from Performance Analytics to a preferred Webhook listener such as Slack, JIRA. This helps enterprise customers automate the flow from incident detection to closure, and hence easily drive workflows in response to Performance Analytics Alert notifications.

For information about creating a webhook profile, see Create a Webhook Profile.

To configure a webhook-based alert notification:

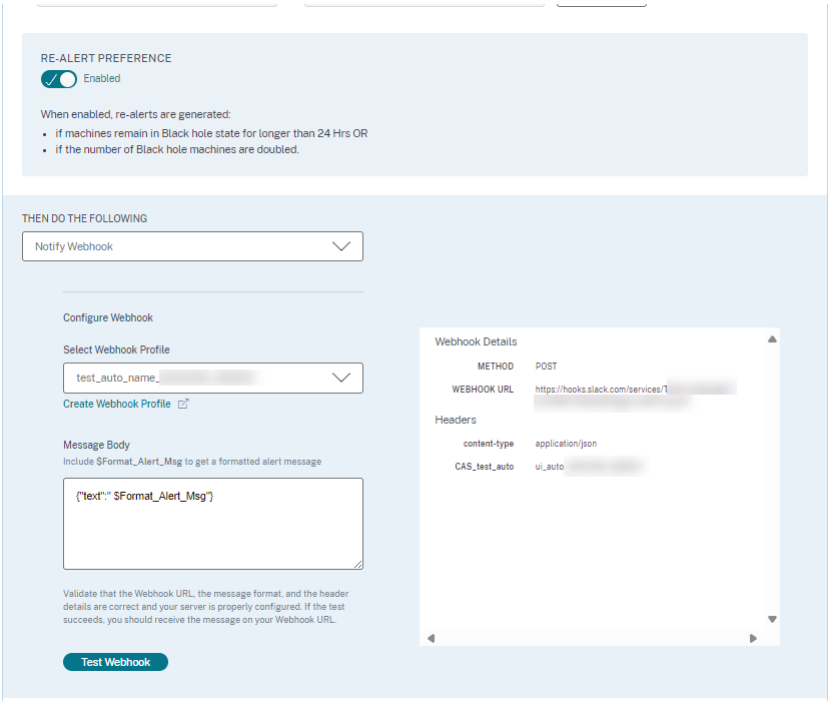
1. Go to the **Alert Policies** tab.

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



2. Click the policy that you want to configure with a webhook.
3. **Modify Alert** page opens. In the **Then do the following** drop-down list, select **Notify webhook or Email** or **Notify webhook** as required.
4. If you have the webhook profile already created, choose the correct webhook from the **Select Webhook Profile** drop-down list.
5. In the **Message Body** text box, include the `$Format_Alert_Msg` string to get a regular alert message with a templated string stored in the back-end. For example to send alert message to Slack, you can use this format: `{ "text":"$Format_Alert_Msg"}`.

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



CSV attachments in alert mailers

Black hole Machines, Overloaded Machine and Zombie Session alerts emails have CSV attachments containing information about the affected machines and sessions.
The attachment has the following data:

- Machine Name
- Site ID
- Catalog Name
- Delivery Group Name
- Failure count (Number of failed machines or sessions as applicable).

The CSV attachments in alert mailers help identify faulting machines and sessions without having to log on to Citrix Analytics for Performance. This helps establish automation pipelines to create and forward tickets to stakeholders responsible for speedy resolution of issues.

Exclude delivery groups from receiving alerts

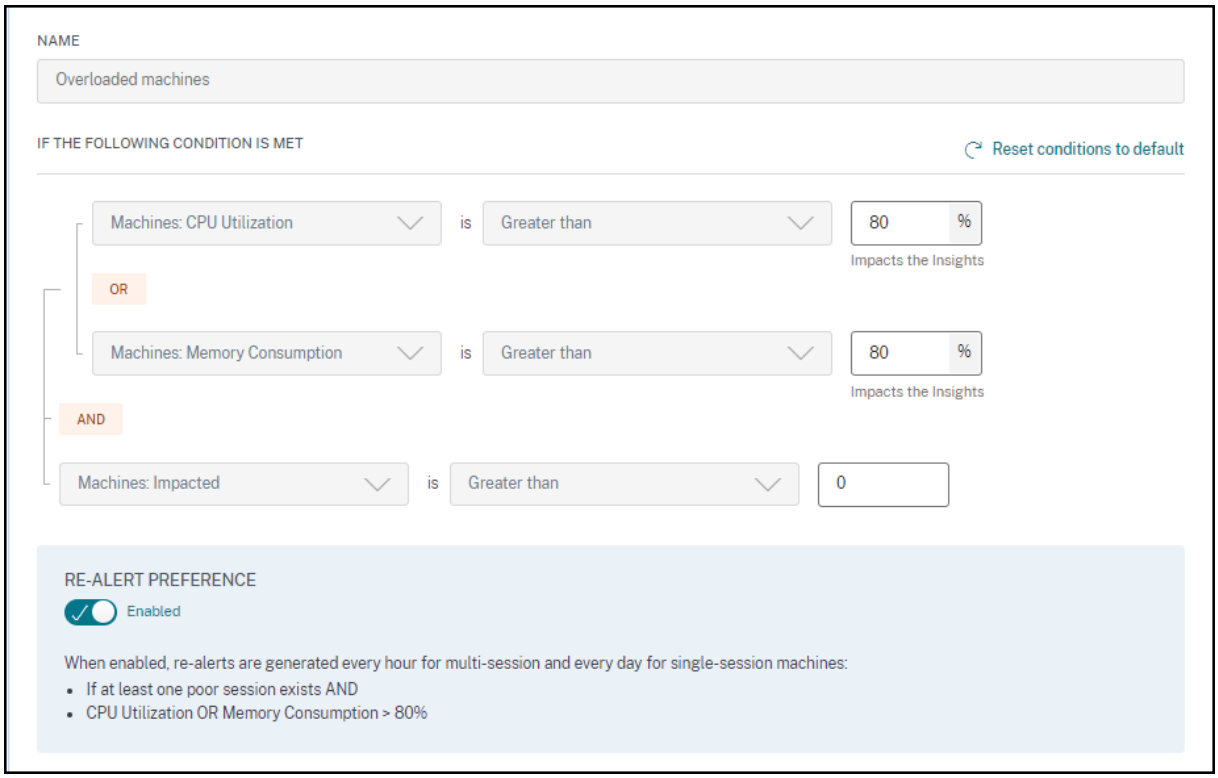
You can now specify delivery groups to be excluded from receiving alert notifications. You can remove unused delivery groups or those created for testing purposes from the alerting process. Excluding delivery groups helps reduce alert fatigue and improve the relevance of alerts.

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

Customize Alert Parameters

Alert policies are pre-built with default parameter values. You can modify the alert parameters to make them more relevant to your environment.

Click the alert policy name to open the **Modify Alert** window. Modify the values of the listed parameters to suit your environment. Subsequent alert notifications are generated based on the custom conditions.



> **Note:**
> Updating the alert parameters also alters the calculation of the corresponding insight on the UX dashboard.

In alerts where re-alerting is supported, you can also control the re-alerting preference. Alert notifications are resent if the re-alert preference is set to **Enabled** and the conditions as specified in the re-alert preference persist.

Customized alerts are more relevant to your environment, they help identify anomalies easily, and are more dependable for proactive monitoring.

Alert for Machines with Zombie Sessions

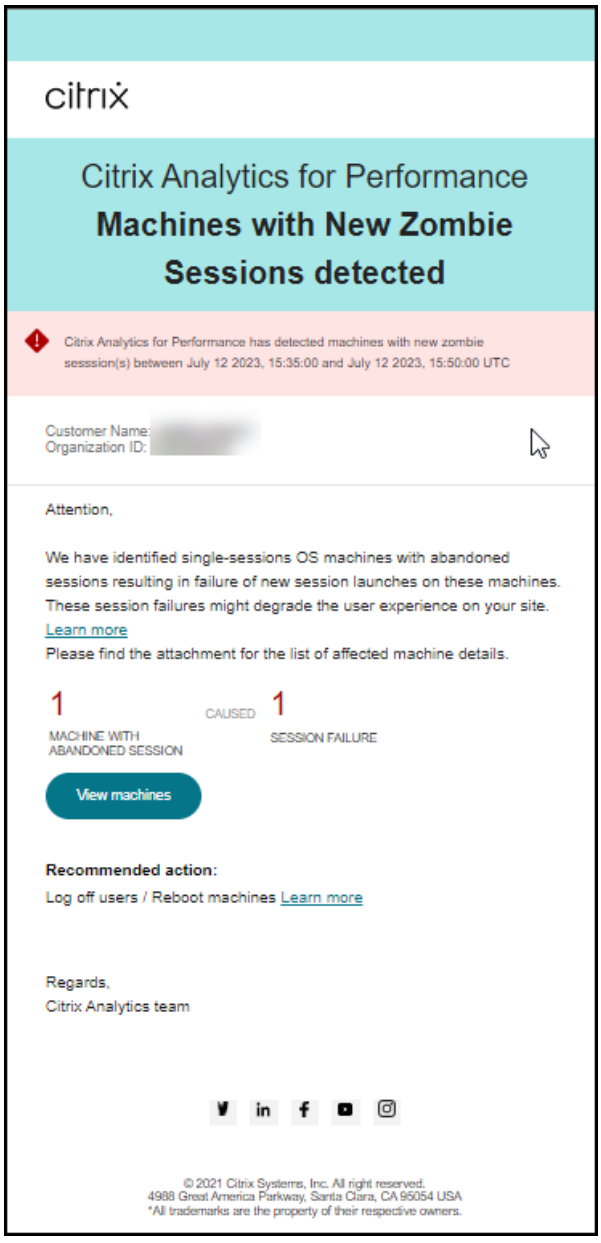
The **Machines with Zombie Sessions** alert mail is generated when a new machine with a zombie session is detected in the environment in a 15 mins interval.

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

You can customize the alert conditions for the Machines with Zombie Sessions alert.



An email alert containing details of the number of machines with zombie sessions and session failures that have resulted due to zombie sessions is sent to the administrators. The numbers in the mailer are for the last 15 min interval.



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

Click **View machines** in the mailer to see single-session machines with abandoned sessions on the Self-service view for Machines with Zombie Sessions. The view reflects the 15 min interval as per the mailer, use the time navigator to choose a larger time window.

Re-alerting on the same machine is done only if the same-abandoned session persists on the same machine for over 24 hours from the initial detection. The re-alerting preference for this alert cannot be set to disabled.

Alert for Sessions with Anomalous Latency

Anomalous Latency is the primary cause for poor session experience. The Anomalous Latency alerts help administrators when there is a significant deviation in the session latency values. The proactive alerting helps administrators identify specific users whose sessions have poor responsiveness.

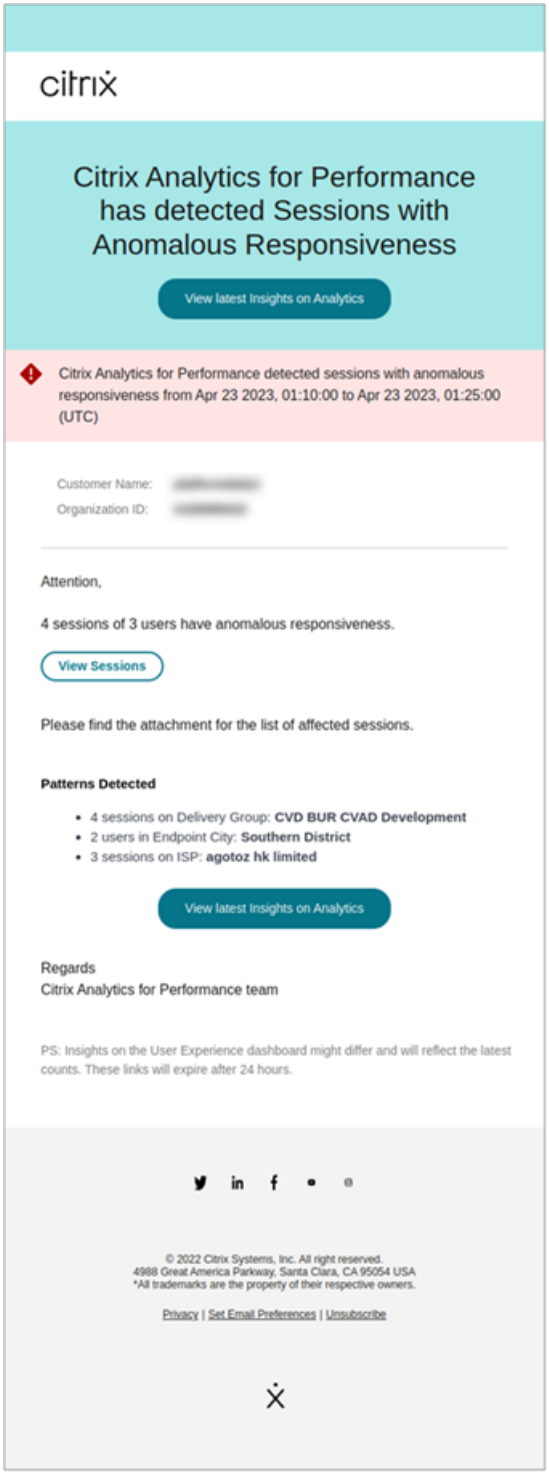
You can customize the alert conditions for the Sessions with Anomalous Latency alert.



Updating the parameters alters the calculation of the Baseline Insight for Sessions with Anomalous Responsiveness.

This alert shows the number of sessions and users whose session latency readings deviate from the user's 30-day baseline value. The user-specific baseline is calculated using the P95 ICARTT values measured over the last 30 days.

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



The alert mail shows the number of sessions and users facing anomalous responsiveness in the mentioned time period. Click **View Sessions** to see the sessions with anomalous responsiveness listed in the Sessions self-service page.

The **Patterns Detected** section shows the top three patterns noticed in sessions with anomalous responsiveness based on the following criteria:

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

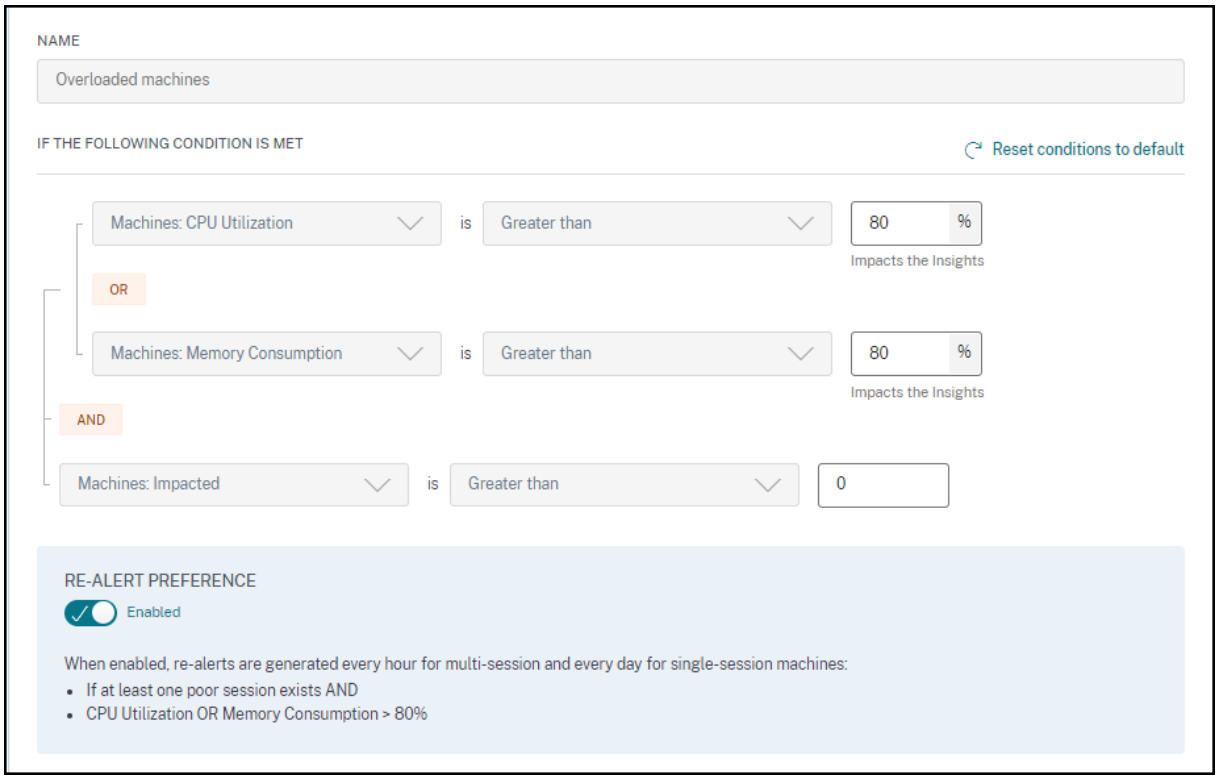
- Number of sessions with anomalous responsiveness in each Delivery Group
- Number of users with anomalous responsiveness in each Endpoint City
- Number of sessions with anomalous responsiveness in each ISP

The **View latest insights on Analytics** link leads to the User Experience dashboard showing the latest statistics in the **Insights** panel. Analyze the Location, ICARTT, ISP, Bandwidth, and Latency metrics for a specific session to root cause the issue. For more information about the indicators available in the Sessions based Self-service view, see Self-service search for sessions.

Alert for Overloaded Machines

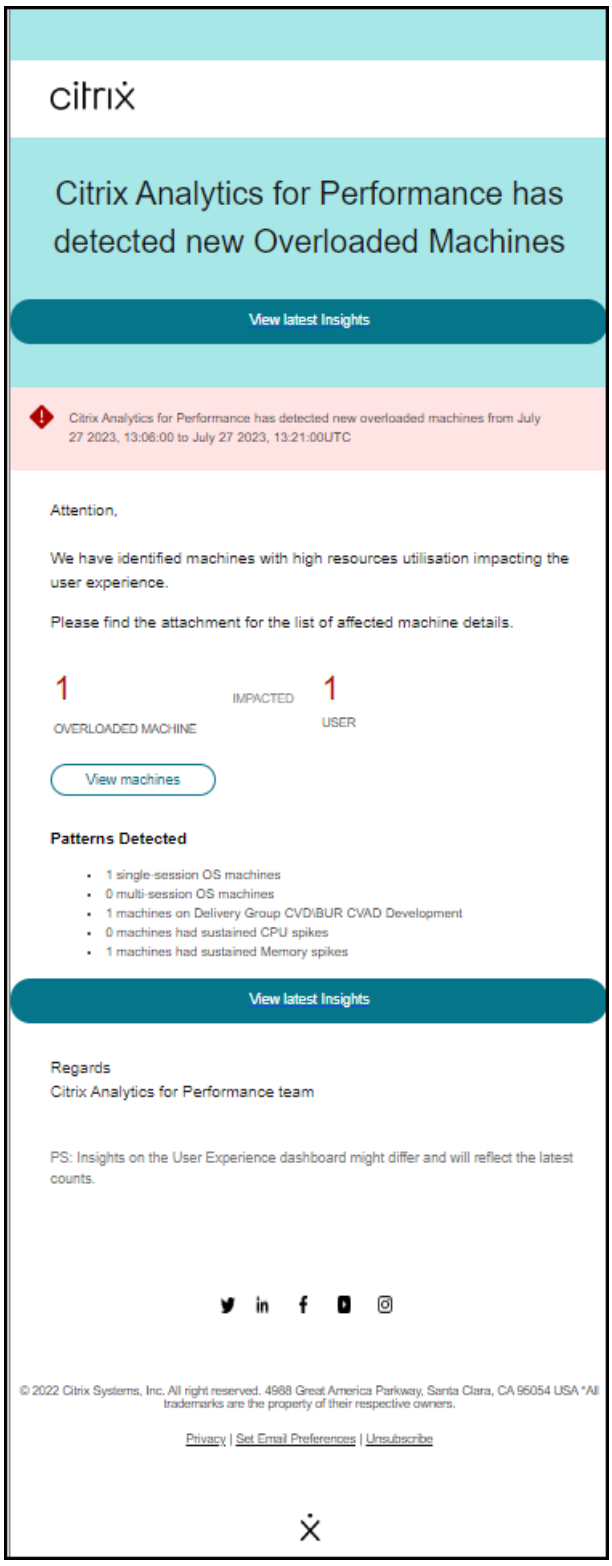
Machines that have experienced sustained CPU spikes, or high memory usage, or both, that have lasted for 5 minutes or more, resulting in a poor user experience during the selected interval are considered to be overloaded.

You can customize the alert conditions and the re-alert preference for the Overloaded Machines alert.



An Overloaded Machines alert mail is sent to administrators when an overloaded machine is detected in the environment in a 15-minute interval.

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



If the machine remains in an overloaded condition, re-alert mails are generated,

- in the case of a single-session machine, once in 24 hours,
- in the case of multi-session machines, up to three times on the first day if the machine has a

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

new session with poor Session Score and once after 24 hours.

The alert mail shows the number of overloaded machines causing poor user experience and the number of users affected during the selected duration.

Click **View Machines** to see the overloaded machines listed in the Machines self-service page for Overloaded Machines.

The **Patterns Detected** section shows the top three patterns noticed in overloaded machines with respect to the following criteria:

- Number of overloaded machines in each Delivery Group
- Number of overloaded machines running single-session or multi-session OS
- Number of overloaded machines with Sustained Memory or CPU spikes

The **View latest insights** link leads to the User Experience dashboard showing the latest statistics in the **Insights** panel.

Updating the parameters alters the calculation of the Diagnostic Insight for Overloaded Machines.

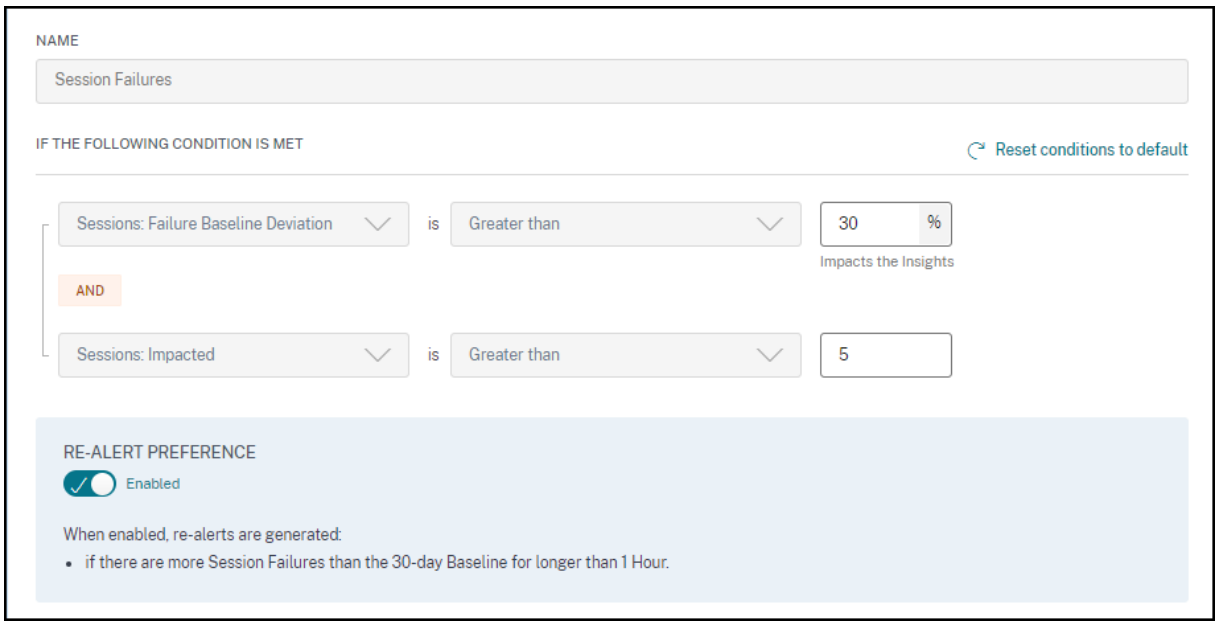
For more information, see the Insights article.

Alert for Black Hole Machines

Citrix Analytics for Performance scans for black hole machines every 15 minutes and sends out an alert to enable administrators to proactively mitigate session failures faced by users due to black hole machines. Machines that have failed to service four or more consecutive session requests are termed as Black hole machines. With black hole failure alerting, administrators need not be logged into Performance Analytics to know the session failures that occurred due to black hole machines.

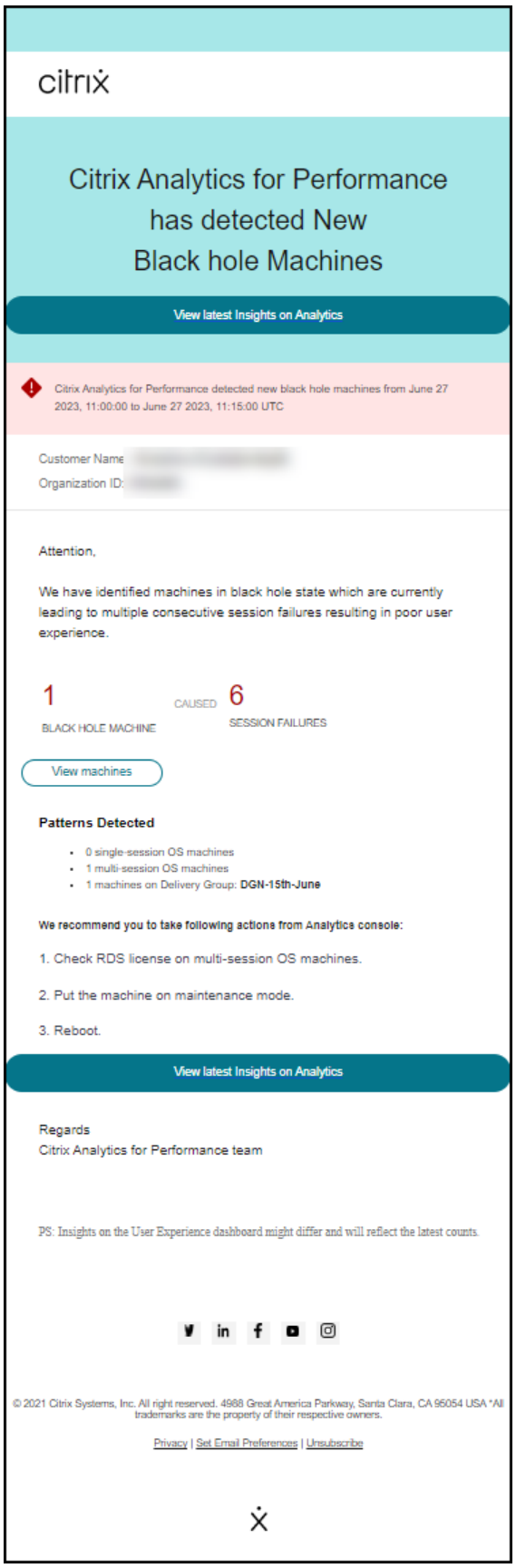
You can customize alert conditions and the re-alert preference for the Black Hole Machines alert.

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



Details of the machines and the session failures caused by them are sent in the alert mails to administrators. The **Black Hole Machines** alert policy must be enabled to receive these mails.

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



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

Clicking the View machines link takes you to the Machines self-service view displaying the list of black hole machines during the 15 min interval. In addition, the timeline view shows black hole machines identified over the last 24 hours.
Administrators are re-alerted if the number of session failures due to the same black hole machine is doubled within 24 hours and the re-alerting preference is set to **Enabled**.

The **View latest insights** link leads to the User Experience dashboard showing the latest statistics in the **Insights** panel.

The **Patterns Detected** section shows the top three patterns noticed in black hole machines with respect to the following criteria:

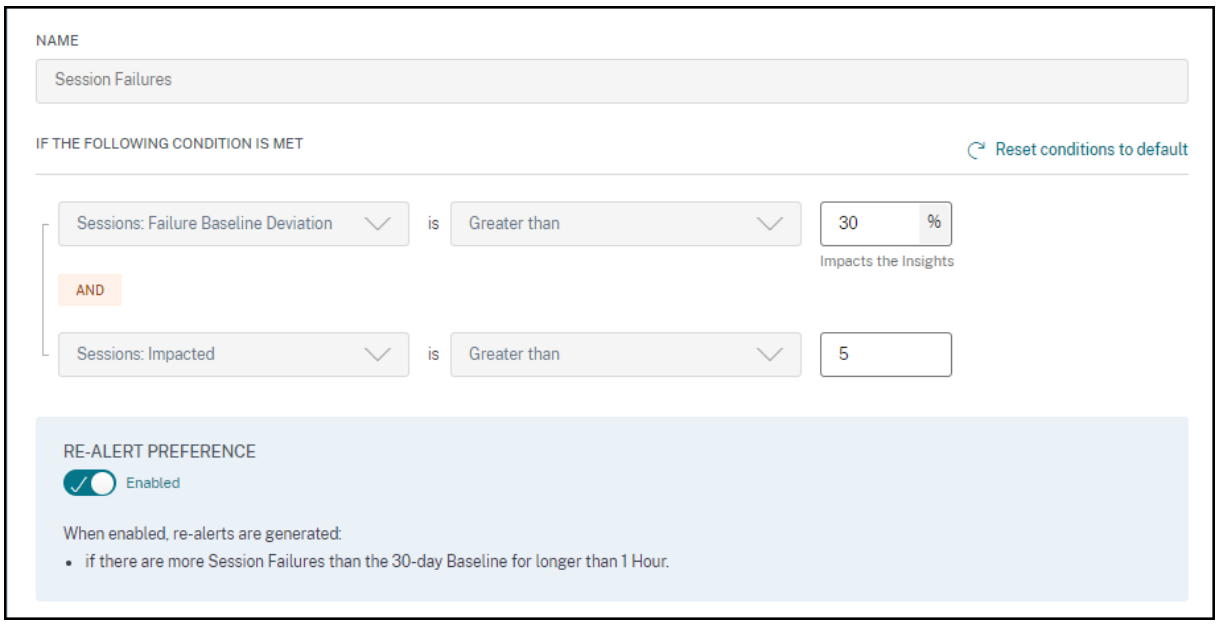
- Number of black hole machines in each Delivery Group
- Number of black hole machines running single-session or multi-session OS

Updating the parameters alters the calculation of the Diagnostic Insight for Black Hole Machines. For more information, see the Insights article.

Alert for Session Failures

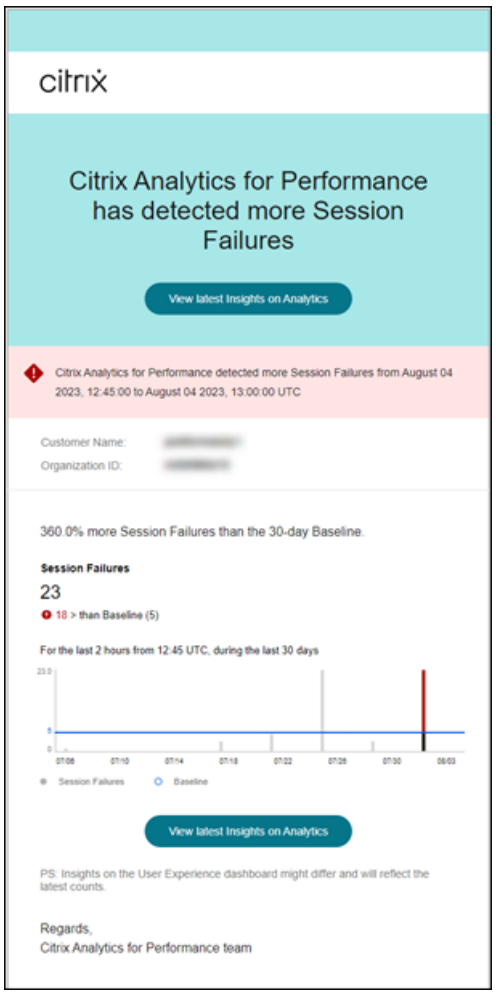
The **Session Failures** alert is generated when the number of sessions that have failed to launch has exceeded by 30% or more from the 30-day baseline value and more than 5% of the total number of sessions have failed. The baseline value is calculated as the P80 value of the session failure count measured during the last 30 days for the same time frame.

You can customize alert conditions and the re-alert preference for the Session Failures alert.



Session Failures alert notification is mailed to all configured administrators.

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



The Session Failures alert mail displays the following information:

- the percentage change in the current session failure count compared to the baseline value
- the current number of session failures
- increase in the number of session failures with respect to the baseline value
- a graph showing the baseline value and session failure count plotted over the last 30 days.

The **View latest insights** link leads to the User Experience dashboard showing the latest statistics in the **Baseline Insights** panel.

Updating the parameters alters the calculation of the Baseline Insight for Session Failures. For more information, see the Insights article.

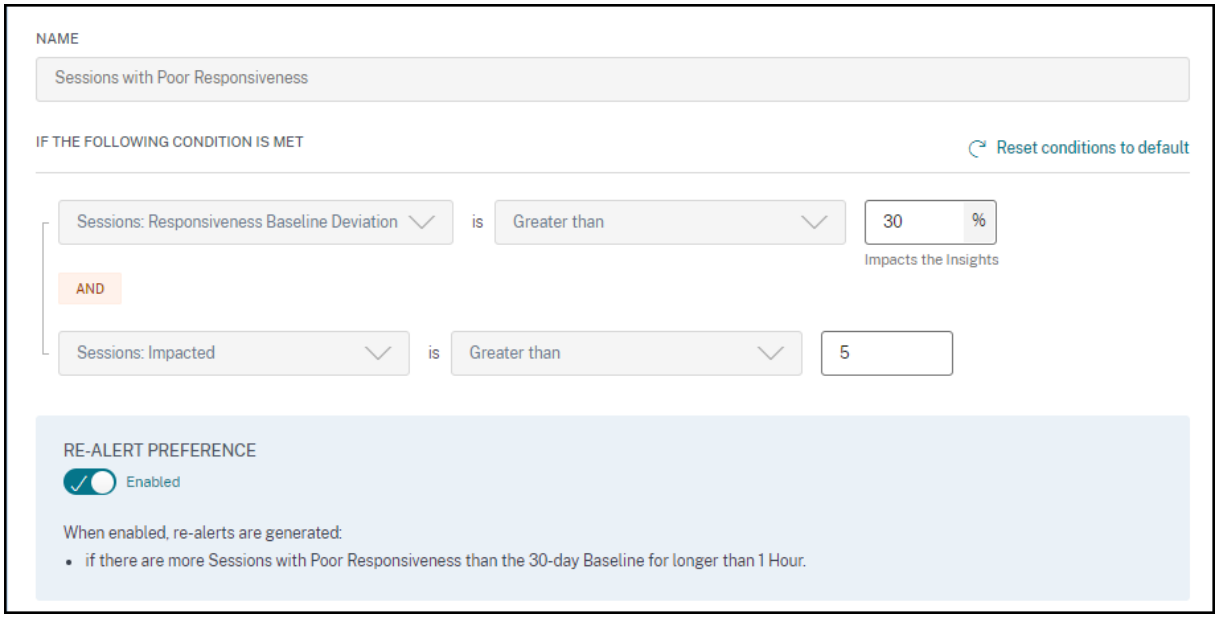
Alert for Sessions with Poor Responsiveness

The **Sessions with Poor Responsiveness** alert is generated when the number of sessions with poor responsiveness has increased 30% or more from the 30-day baseline value and this increase impacts

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

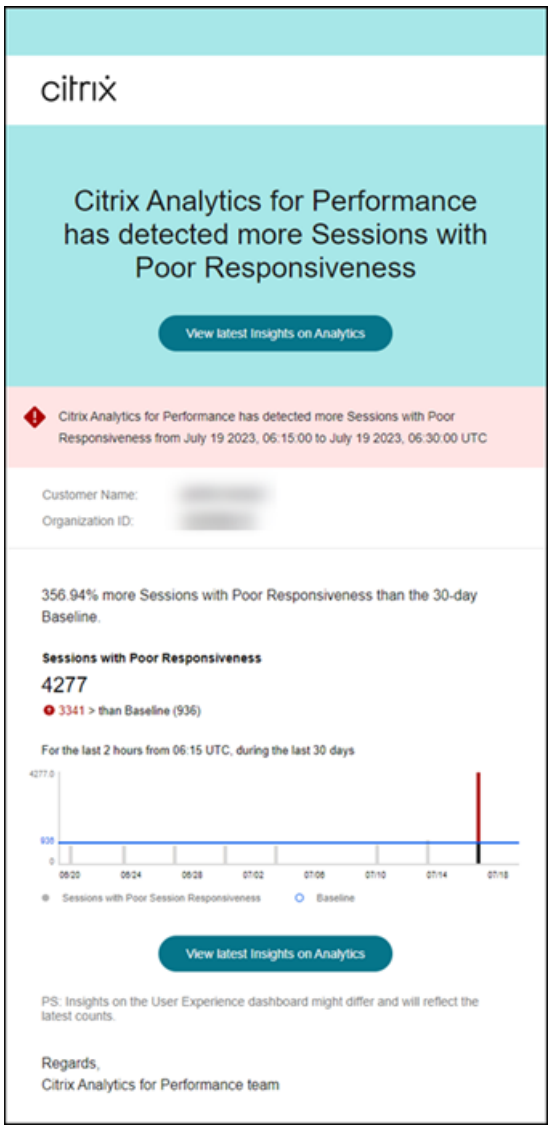
more than 5% of the sessions. The baseline value is calculated as the P80 value of the number of sessions with poor responsiveness measured during the last 30 days for the same time frame.

You can customize alert conditions and the re-alert preference for the Sessions with Poor Responsiveness alert.



Sessions with Poor Responsiveness alert notification is mailed to the configured administrators.

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



The alert mail contains the following information:

- the percentage change in the current number of sessions with poor responsiveness value compared to the baseline value
- the current number of sessions with poor responsiveness
- the increase or decrease in the sessions with poor responsiveness with respect to the baseline value
- a graph showing the baseline value and the number of sessions with poor responsiveness trend over the last 30 days.

The **View latest insights** link leads to the User Experience dashboard showing the latest statistics in the **Insights** panel.

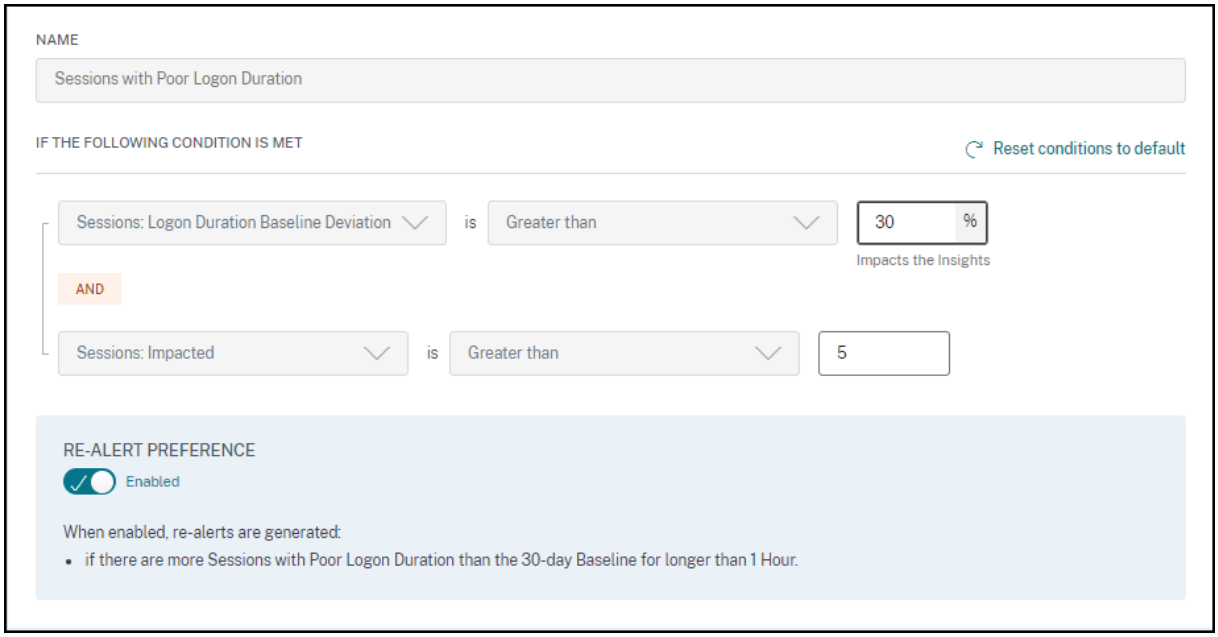
Updating the parameters alters the calculation of the Baseline Insight for Sessions with Poor Responsiveness. For more information, see the Insights article.

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

Alert for Sessions with Poor Logon Duration

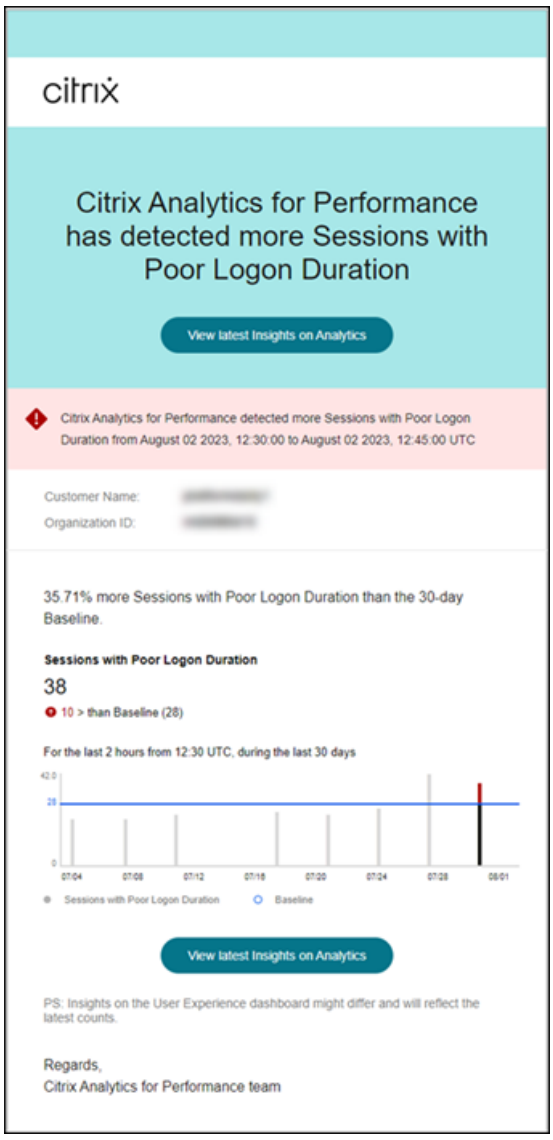
The **Sessions with Poor Logon Duration** alert is generated when the number of sessions with poor logon duration has increased 30% or more from the 30-day baseline value and this increase impacts more than 5% of the sessions. The baseline value is calculated as the P80 value of the number of sessions with poor logon duration measured during the last 30 days for the same time frame.

You can customize alert conditions and the re-alert preference for the Sessions with Poor Logon Duration alert.



Sessions with Poor Logon Duration alert notification is mailed to the configured administrators.

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



The Sessions with Poor Logon Duration alert mail shows the following information:

- the percentage change in the current number of sessions with poor logon duration value compared to the baseline value
- the current number of sessions with poor logon duration
- increase or decrease in the sessions with poor logon duration with respect to the baseline value
- a graph showing the baseline value and the number of sessions with poor logon duration plotted over the last 30 days

The **View latest insights** link leads to the User Experience dashboard showing the latest statistics in the **Baseline Insights** panel.

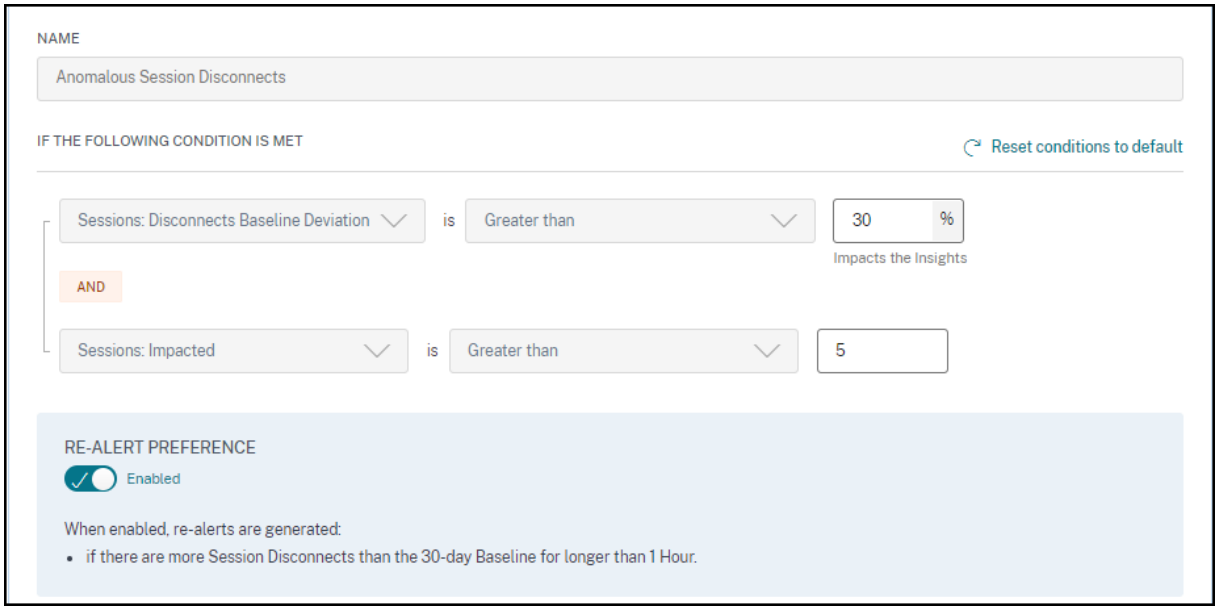
For more information, see the Insights article.

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

Alert for Anomalous Session Disconnects

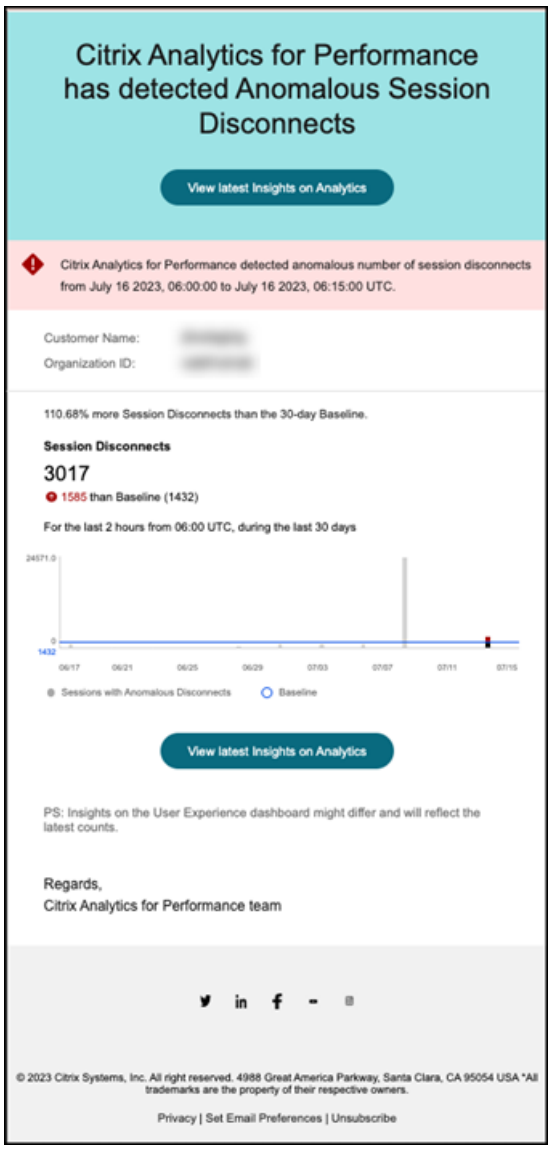
The **Anomalous Session Disconnects** alert is generated when the session disconnects count has increased 30% or more from the 30-day baseline value and this increase impacts more than 5% of the sessions. The baseline value is calculated as the P80 value of the number of sessions disconnects measured during the last 30 days for the same time frame.

You can customize alert conditions and the re-alert preference for the Anomalous Session Disconnects alert.



Sessions with Poor Logon Duration alert notification is mailed to the configured administrators.

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



The Anomalous Sessions Disconnects alert mail shows the following information:

- the percentage change in the current session disconnects count as compared to the baseline value
- the current number of session disconnects
- increase in session disconnects with respect to the baseline value
- a graph showing the baseline value and the number of session disconnects plotted over the last 30 days.

The **View latest insights** link leads to the User Experience dashboard showing the latest statistics in the **Baseline Insights** panel.

Updating the parameters alters the calculation of the Baseline Insight for Anomalous Session Disconnects. For more information, see the Insights article.

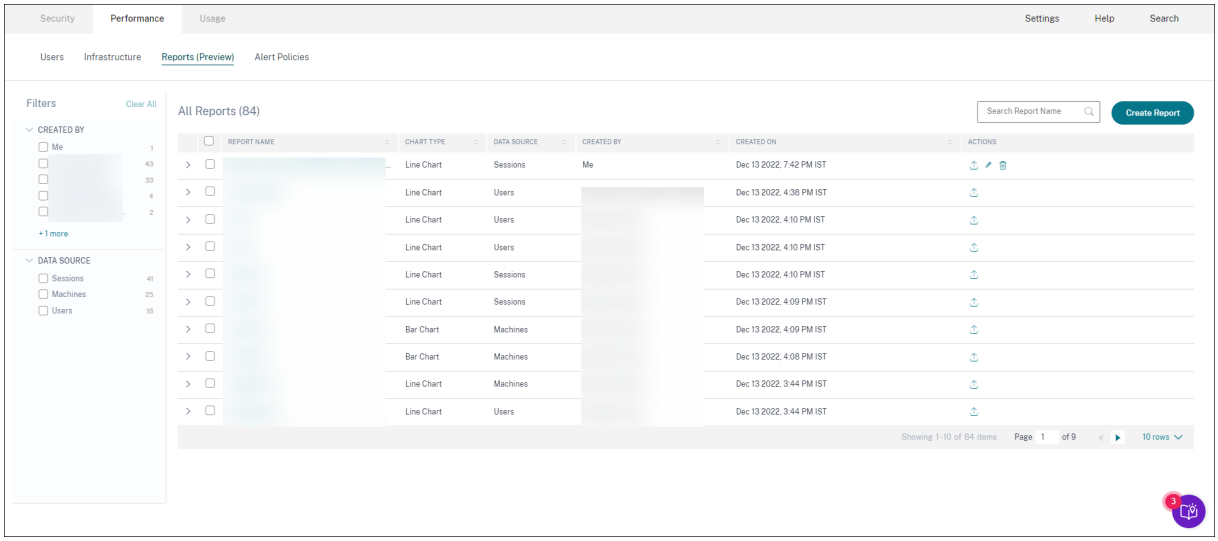
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Custom Reports (Preview)

September 1, 2025

You can create and schedule custom reports using the performance metrics in Citrix Analytics for Performance. Custom reports help you to extract information of specific interest and organize the data graphically. It helps to create executive reports in a regular cadence and analyze the performance of your environment over time.

Click **Reports** in Performance Analytics to see the list of existing reports in the current tenant. Expand the report row to see a preview of the report.



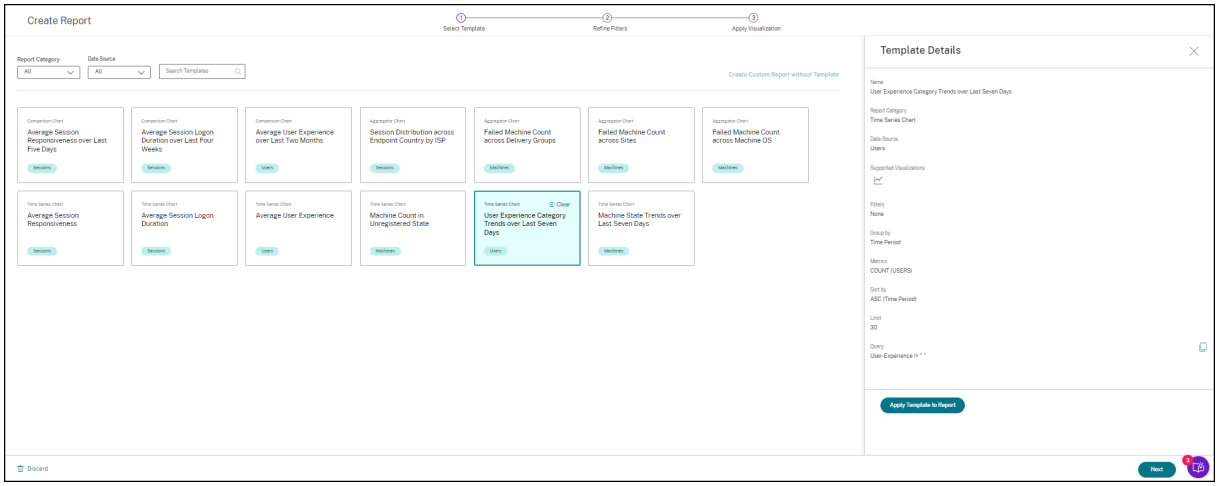
You can perform the following actions on reports using this view:

- Click **Create Report** to create a custom report.
- Expand a row to see the preview of an existing custom report.
- Click the report name to see the report of an existing custom report.
- Click the export icon to export an existing custom report in CSV format, PDF format or both.
- Click the edit icon to edit the reports you have created.
- Click the delete icon to delete the reports you have created.

How to create a custom report

To create a custom report, click **Create Reports**. On the **Create Report** page, you can choose to create a custom report with or without templates.

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



To create a custom report with template, do the following:

1. Select a template. Choose the **Report Category** from among the following:

    - Time Series Chart: This chart helps analyze a selected metric across a period, like the Average Session Responsiveness.
    - Aggregator Chart: This chart plots aggregated values of a selected metric grouped by a characteristic (like region) over a period, such as the Session Distribution across Endpoint Country by ISP. It helps understand the session activity across different geographies and ISPs.
    - Comparison Chart: This chart plots the average metric value compared over a set of time periods like Average Session Responsiveness over Last Five Days. It helps understand the performance of a given metric across different time periods.

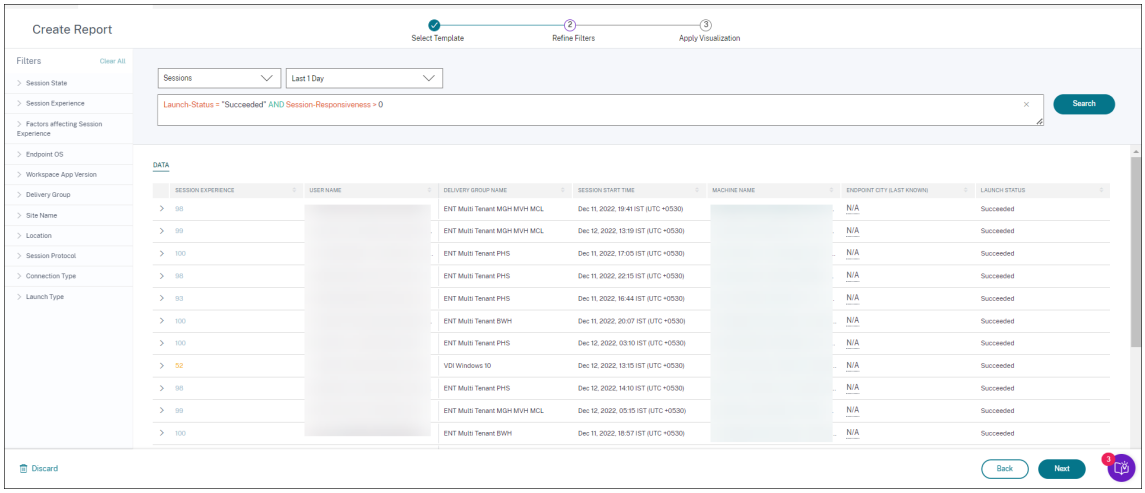
2. Choose a **Data Source** from among Users, Sessions, or Machines, and select one of the predefined templates for the chart.

    - Templates based on the Users Data source:
        - Average User Experience over Last Two Months
        - Average User Experience
        - User Experience Category Trends over Last Seven Days
    - Templates based on the Sessions Data source:
        - Average Session Responsiveness over Last Five Days
        - Average Session Logon Duration over Last Four Weeks
        - Session Distribution across Endpoint Country by ISP
        - Average Session Responsiveness
        - Average Session Logon Duration
    - Templates based on the Machines Data source:
        - Machine Count in Unregistered State

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

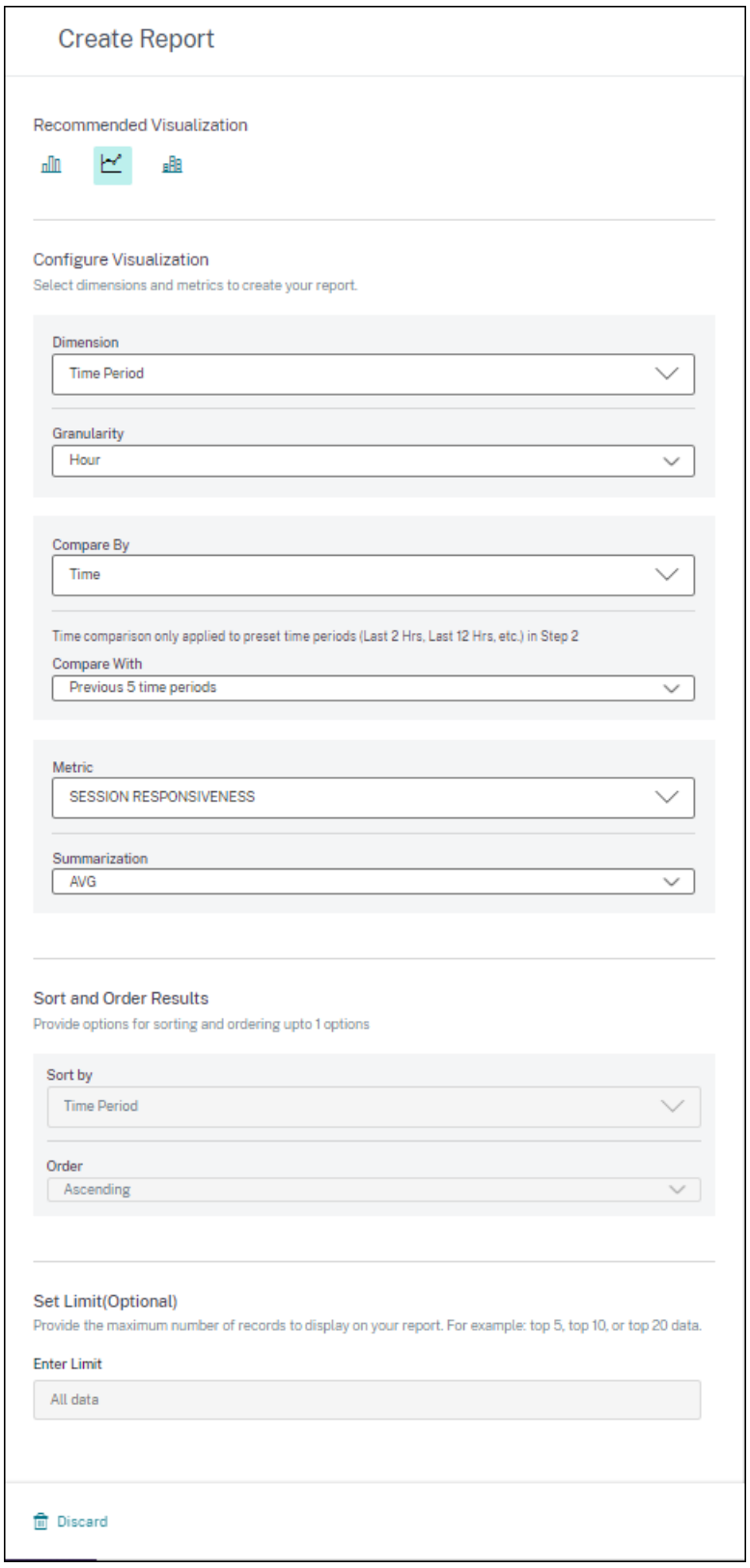
- Failed Machine Count across Delivery Groups
- Failed Machine Count across Sites
- Failed Machine Count across Machine OS
- Machine State Trends over Last Seven Days

3. Once you click a template, the template details are listed on the right. Click **Apply Template to Report** to enable the report to use the selected template.
4. Refine Filters. On the **Refine Filters** page, the predefined filters as per the selected template are shown. Make the required changes and then click **Next**.



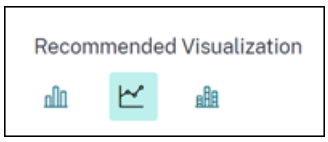
5. Apply Visualization. Choose the parameters that make up the chart.

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



Select one of the available visualizations for displaying the report.

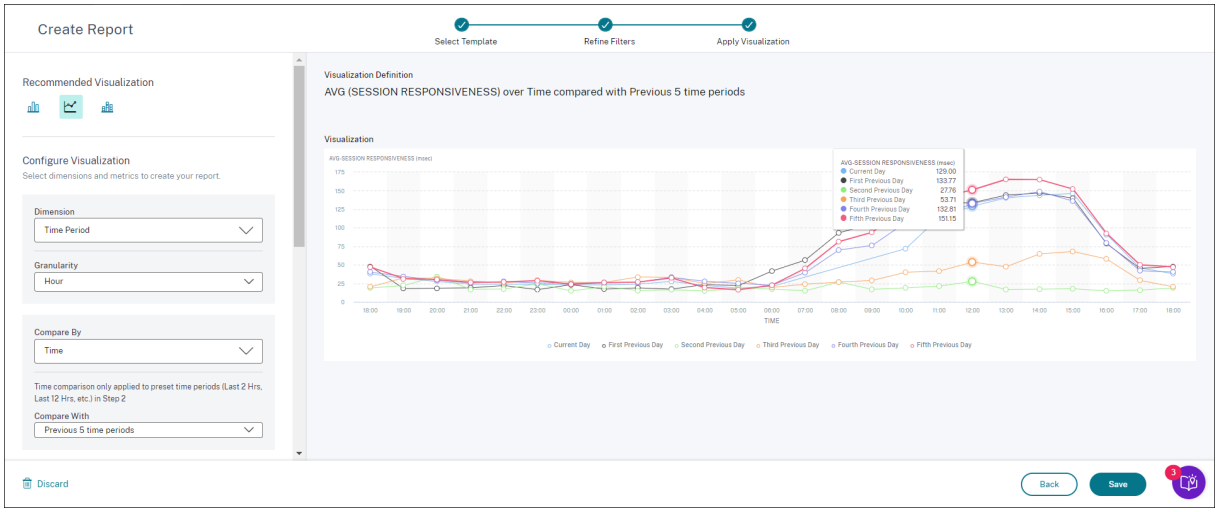
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Bar Chart: Presents data with vertical rectangular bars with height proportional to the values. Used for comparing events.
- Line chart: Presents data with dots connected by straight line segments. Used to visualize data trends over a time period.
- Stacked Column Chart: Presents data in the form of bars stacked one over the other. Used to visualize more than one data over the same time period.

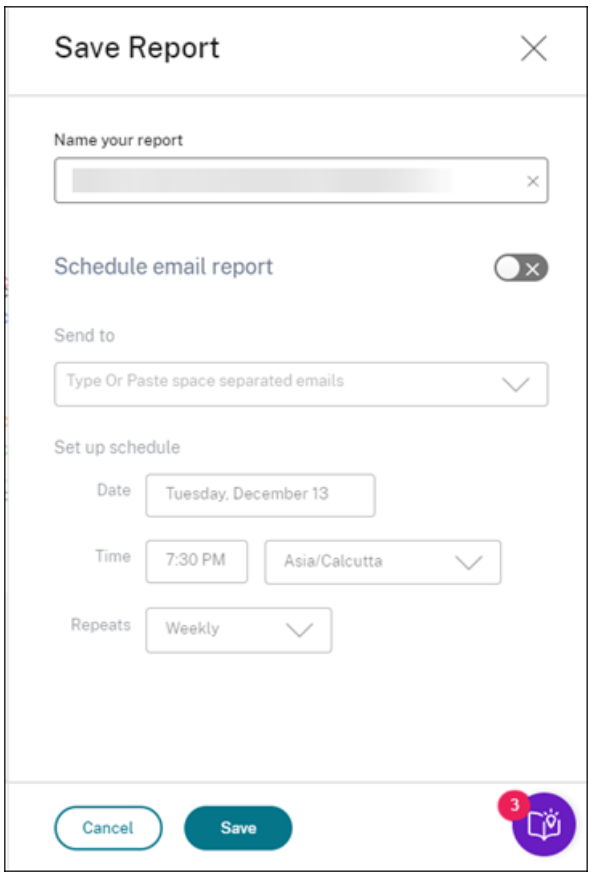
6. Now configure the visualization with the following parameters:

   - Dimension for the x-axis,
   - Plotting granularity,
   - Metrics to be plotted in the y-axis,
   - Summarization or aggregation, such as average or count, to be applied to the metric,
   - Options for sorting and ordering
   - An optional limit for the maximum number of records to be displayed on the report.



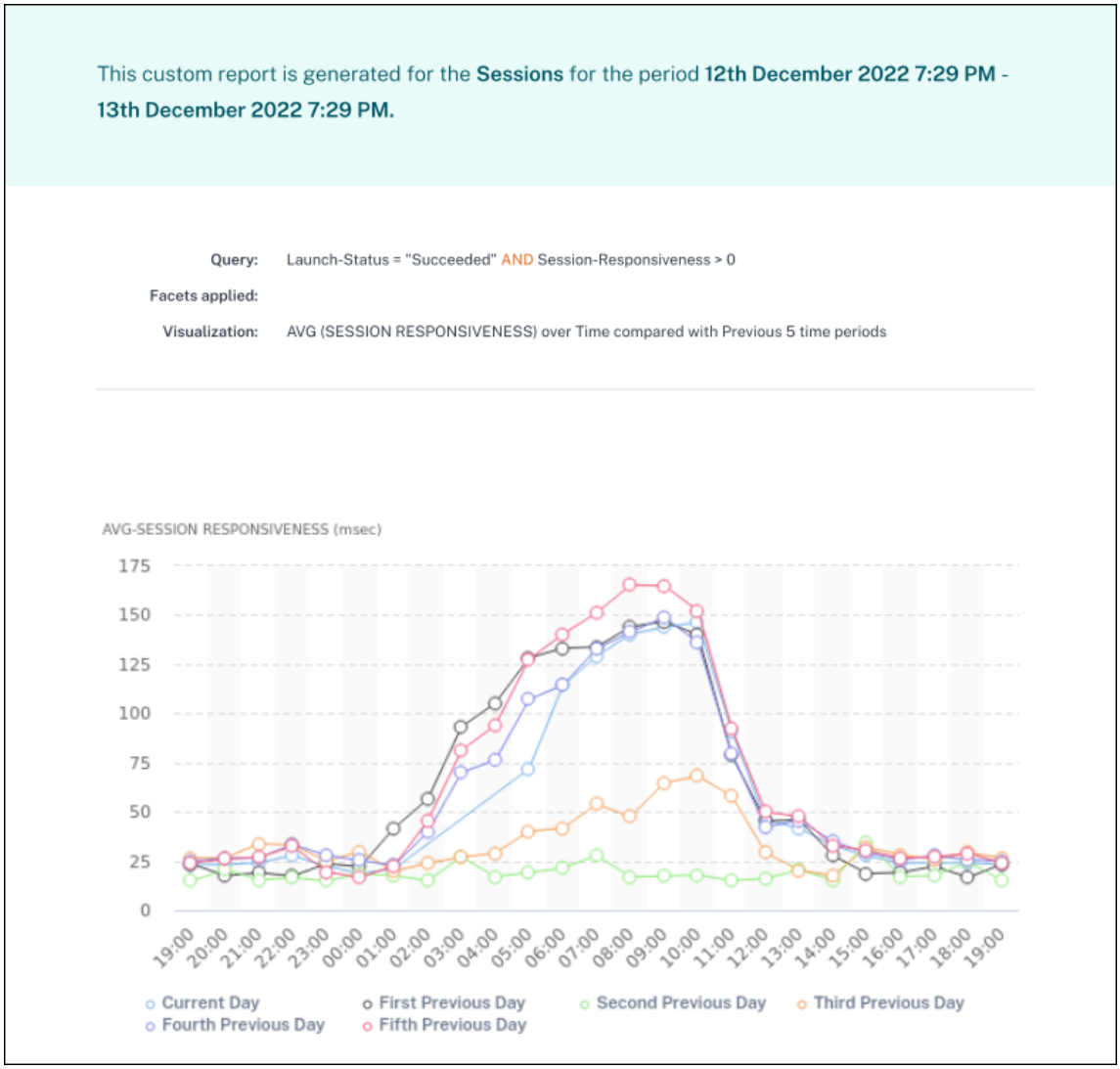
1. To save the report, click **Save**. Specify a title for your report.
2. You can schedule to email the report to the specified email ids and distribution lists on a specific date and time. Further, you can choose to repeat this daily, weekly, or monthly.

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



3. After you have created and saved a report, you can view the report on the **Reports** page. You can also modify or delete a saved report.
4. Click the export icon to download the report in CSV format, PDF format or both formats.

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



You can also create a custom report without a predefined template. Click the **Create Custom Report without Template** link. Follow the steps to define the filters, apply visualization, save, and schedule the report.

Citrix Analytics offerings

September 11, 2025

Citrix Analytics for Security™

Collates and provides visibility into user and application behavior, collected from customers' connected data sources, such as Secure Private Access, Citrix Virtual Apps and Desktops™, Citrix DaaS

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

Site, or NetScaler Gateway. You can track every aspect of the behavior, and by leveraging advanced Machine Learning algorithms, you can distinguish between normal behavior and a malicious attacker. Thus, enabling you to proactively identify and manage internal and external threats.

Learn more: Citrix Analytics for Security

Citrix Analytics for Performance™

Provides holistic end-to-end visibility across hybrid deployments of Citrix Virtual Apps and Desktops and Citrix DaaS sites. Performance is indicated by the User Experience Score which quantifies historical factors and metrics that define the experience a user has while using a Citrix-provided published application, published desktop, or Remote PC.

Learn more: Citrix Analytics for Performance

Citrix Analytics - Usage (End of Life)

> **Note**
>
> **Attention**: Citrix Usage Analytics has reached its end of life and is no longer available to users.

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.