Citrix Analytics for Performance
## Contents

**What's new** 3

**Known Issues** 34

**Data Sources** 34

**Data Governance** 41

**Limits** 79

**Citrix Analytics offerings** 80

**Configuring on-premises Citrix Virtual Apps and Desktops Sites with Citrix Analytics for Performance** 81

**Manage Administrator Roles for Performance Analytics** 86

**Self-service search** 87

**User Experience Analytics** 105

**User Experience** 114

**User Experience (UX) Factors** 118

**Self-Service Search for Performance** 128

**Connector Statistics** 145

**Session Details** 148

**Machine Statistics** 151

**N/A or Not Categorized Metrics** 160

**Infrastructure Analytics** 168

**Insights** 173

**Alerts** 178
What’s new

August 19, 2022

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 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.

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 be logged 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.
Citrix Analytics for Performance has detected New Blackhole Machines

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 realert mail is sent if the same machine remains in the overloaded condition after 24 hours. The administrators are realerted 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.
For more information, see Overloaded Machine Alerts.

July 18, 2022

Machine States ROLLING OUT

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 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 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 being not categorized. This feature provides the clarity required to quickly discover and fix any configuration issues.

For more information, see the Not Categorized article.
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.

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.

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 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.

**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.
A Zombie session alert mail is generated when a new machine with 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. Realerting 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.
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 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 in 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
Citrix Analytics for Performance

- 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 in 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 in 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 in the Sessions Self-service view.

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 Connection lease to maintain service continuity.

Connection leased sessions are displayed under the Not Categorized classification in the User Experience Dashboard. ICA RTT and logon duration metrics are not available for Connection leased sessions.
You can see the classification of sessions as ICA based or Connection leased using the Launch Type facet in the Sessions Self-service view.

The optional column, Launch Type in 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 in 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 in the Visual summary help triage poor sessions that might all be routed through a single Gateway PoP or Connector.
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
percentages of each metric consumed in the connector along with the number of instances when the metric crossed the threshold values 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 in 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 in the Session Self-service view, see the Sessions self-service article.

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 session 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. 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.

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 in the tabular view when you expand the selected session row in 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.
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. 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 in the Sessions Self-service view, see the Sessions self-service article.

**Session Duration in Sessions Self-Service View**

Session Duration is now available in the Sessions self-service view. Use Add or Remove Columns to add Session Duration. 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 in the Sessions Self-service view, see the Sessions self-service article.
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
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.

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 in 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.

For more information, see Process visibility.
June 10, 2021

Color coding in Session-based self-service view

Tabular data in 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.

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:

- 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 in Sessions self-service view**

Visual Summary of data is available in the Sessions self-service view. Visual Summary presents 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.

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 resource.
  – 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.
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 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 is 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 is available in the Users, and Sessions based self-service views. Use the Protocol facet to filter the results based on the session protocol.

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 in 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 in 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 columns in 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.

- 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 in 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.

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 in 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**.

**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, in the **Machines self-service view**, click the machine name link.

Key data points available on this page are:
Citrix Analytics for Performance

- 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 in 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 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 sub factor 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.

April 23, 2020

Location and Endpoint based Self-Service Search

Now, you can search events based on the Endpoint Country or City in 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.
Citrix Analytics for Performance

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

August 19, 2022

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.

The Protocol facet in the Sessions and Users based self-service views lists only the current protocols of user sessions and not all supported session protocols. [WSA-6558]

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 Sources

August 19, 2022

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.

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Required Service Subscriptions</th>
<th>Product Component and version</th>
<th>Onboarding</th>
<th>Value-add</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)</td>
<td>Citrix Cloud license, Citrix DaaS subscription</td>
<td>See Citrix Workspace app version matrix</td>
<td>Automatically detected. Ensure accessibility to the https://<em>.cloud.com/ and https://</em>.windows.net/ URLs from all endpoints (or proxies, if they are configured)</td>
<td>Performance analytics features</td>
</tr>
<tr>
<td>Citrix Virtual Apps and Desktops on-premises</td>
<td>Citrix Workspace service, Citrix Virtual Apps and Desktops</td>
<td>See Citrix Workspace app version matrix and Citrix VDA/Machine version matrix</td>
<td>Onboard from Director through a 3-step process</td>
<td>Performance analytics features</td>
</tr>
</tbody>
</table>

End User Experience Monitoring (EUEM) service installed and running

Logon Duration, UX Score

Session Responsiveness, UX Score
### Citrix Analytics for Performance

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Required Service Subscriptions</th>
<th>Product Component and version</th>
<th>Onboarding</th>
<th>Value-add</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Gateway On-premises</td>
<td>Application Delivery Management agent</td>
<td>Citrix Gateway 12.1.x.x and later</td>
<td>Gateway data source</td>
<td>Session Responsiveness (Latency) breakdown</td>
</tr>
<tr>
<td>Citrix Profile Management installed and running</td>
<td></td>
<td></td>
<td>Logon Duration, UX Score</td>
<td></td>
</tr>
<tr>
<td>StoreFront 1906 and later (for StoreFront users)</td>
<td></td>
<td>Onboard Virtual Apps and Desktops sites using StoreFront</td>
<td></td>
<td>Endpoint Location, Failure Insights: Communication error, Failed Sessions: Endpoint OS, Workspace app Version, User Terminated Launch status</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>User Ex-</th>
<th>UI Parameter</th>
<th>Windows</th>
<th>Linux</th>
<th>Android</th>
<th>iOS</th>
<th>MAC</th>
<th>HTML5</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Experience Score</td>
<td>User Ex-</td>
<td></td>
<td>1906</td>
<td>2104</td>
<td>2010.5</td>
<td>21.9</td>
<td>21.6.0</td>
<td>21.1</td>
</tr>
<tr>
<td></td>
<td>perience</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dashboard</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Citrix Analytics for Performance

<table>
<thead>
<tr>
<th>Feature</th>
<th>UI Parameter</th>
<th>Windows</th>
<th>Linux</th>
<th>Android</th>
<th>iOS</th>
<th>MAC</th>
<th>HTML5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Location, ISP</td>
<td>Sessions self-service view &gt; Endpoint</td>
<td>1912</td>
<td>2104</td>
<td>20.3.0</td>
<td>20.4.0</td>
<td>20.05.06</td>
<td>2004</td>
</tr>
<tr>
<td>(ensure that the URL</td>
<td>City, Endpoint</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>https://locus.analytics.cloud.com/api/locateip</code> is accessible to the endpoints)</td>
<td>Country</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Network Metrics</strong></td>
<td>Sessions self-service view &gt; Network Interface Type</td>
<td>2105</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Gateway information</strong></td>
<td>Sessions self-service view &gt; Connection Type, Machine FQDN, Gateway Address</td>
<td>2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 1999–2022 Citrix Systems, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Feature</th>
<th>UI Parameter</th>
<th>Windows</th>
<th>Linux</th>
<th>Android</th>
<th>iOS</th>
<th>MAC</th>
<th>HTML5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Launch Status</td>
<td>Sessions self-service view &gt; Launch Status</td>
<td>20.8.0</td>
<td>2101</td>
<td>20.9.0</td>
<td>20.8.0</td>
<td>2101</td>
<td>Not supported</td>
</tr>
<tr>
<td>Communication Error Insights</td>
<td>Dashboard &gt; Failure Insights &gt; Communication Errors</td>
<td>2103</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
</tbody>
</table>
### Citrix Analytics for Performance

<table>
<thead>
<tr>
<th>Feature</th>
<th>UI Parameter</th>
<th>Windows</th>
<th>Linux</th>
<th>Android</th>
<th>iOS</th>
<th>MAC</th>
<th>HTML5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Network Statistics</td>
<td>Sessions self-service view &gt; Endpoint Link Speed (P95), Endpoint Throughput Incoming (P95), Endpoint Throughput Outgoing (P95) and Sessions Details page &gt; WiFi Signal Strength, Endpoint Throughput Incoming and Endpoint Throughput Outgoing</td>
<td>2108</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
</tbody>
</table>

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Citrix Analytics for Performance

**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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>UI Parameter</th>
<th>Citrix VDA version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Analytics for Performance</td>
<td>—</td>
<td>Citrix Virtual Apps and Desktops 7.15 LTSR</td>
</tr>
<tr>
<td>Bandwidth and Network Latency Metrics</td>
<td>Bandwidth and Network Latency metrics in the Sessions self-service and Session Details views</td>
<td>Citrix Virtual Apps and Desktops 7 2112</td>
</tr>
</tbody>
</table>

**Data Governance**

August 19, 2022

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 Content Collaboration
- Citrix Endpoint Management
- Citrix Gateway (on-premises)
- Citrix Identity provider
- Citrix Secure Browser
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)
- Citrix Microapps 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.

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

**Data control**

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

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

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

Data retention

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

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

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

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

Data export

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

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

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

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

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

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

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

Currently, you can integrate with the following SIEM services:

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

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

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

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

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

Citrix Services Security Exhibit

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

Definitions

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

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

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

Data collection agreement

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

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

Appendix: logs collected

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

Citrix Analytics for Security logs

- General logs
- Citrix Content Collaboration logs
Citrix Analytics for Performance

- Citrix Endpoint Management service logs
- Citrix Secure Private Access logs
- Citrix Virtual Apps and Desktops and Citrix DaaS logs
- Citrix ADC logs
- Citrix DaaS Standard for Azure logs
- Citrix Microapps service logs
- Citrix Identity provider logs
- Citrix Gateway logs
- Citrix Secure Browser logs
- Microsoft Graph Security logs
- Microsoft Active Directory logs

General logs

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

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

Citrix Content Collaboration logs

The Citrix Content Collaboration logs contain the following data points:

- Account Id
• Account Info: API Control Plane, App Control Plane, Subdomain
• Add On Name
• Additional Bandwidth
• Additional Bandwidth Rate
• Additional Disk Space
• Additional Disk Space Rate
• Additional User Rate
• Additional Users
• Address1
• Address2
• Advanced Custom Branding Folder Name
• Alias Id
• App Code
• Associated Folder Template Id
• Bandwidth Max
• Base Bandwidth
• Base Billing Rate
• Base Disk Space
• Base Users
• Billing Contact Id
• Billing Cycle
• Billing Rate
• Billing Type
• Branding Styles
• Bytes Downloaded
• Bytes Total
• Cc Sender
• City
• Client Information: City, Client IP, Control Plane, Country, OAuth Client Id, Operating System, Tool Display Name, Tool Name, Tool Version
• Client Name
• Company
• Company Name
• Component Name
• Connector Type
• Contacts: Op Name, Values, Contact Id, Email
• Context: Resource Id, Resource Type
• Copied File Id
• Country
• Created By
• Creation Date
• Creator Id
• Default Zone Id
• Deleted Permanently
• Description
• Destination: File Path, Parent Id, Path, Zone Id
• Disk Space Limit
• Disk Space Max
• DLP Status
• Download By Service
• Download Id
• Email Addresses: Op Name, Values
• Encryption Rate
• End Time
• Entity Id
• Event Id
• Event Time
• Event User Email
• Event User Id
• Events: Operation Name, Resource Type

• Expiration Date

• Fields: Account Id, Account Information Type, API Control Plane, App Control Plane, Subdomain, Approval Context Type, Approval Id, Approval Step Id, Approval Step Status, Is Linked to Approval Step, Bytes Downloaded, Client Information Type, City, Client IP, Control Plane, Country, OAuth Client ID, Operating System, Tool Display Name, Tool Name, Tool Version, Completed Step Id, Connector Type, Created By Type, Created By Email Address, Created By First Name, Created By Id, Created By Last Name, Due, End Time Event User Id, File Extension, File Id, File Name, File Path, File Size, Form Id, Last Ping Back, Name, Next Step Id, Participant Type, Participant Role, Participant Status, Participant User Id, Recipient Type, Recipient Op Name, Recipient Email Address, Recipient First Name, Recipient Id, Recipient Last Name, Role Type, Role Initiators Type, Role Initiators Op Name, Role Initiators Email Address, Role Initiators First Name, Role Initiators Id, Role Initiators Last Name, Role Instance Manager Type, Role Instance Manager Op Name, Role Instance Manager Email Address, Role Instance Manager First Name, Role Instance Manager Id, Role Instance Manager Last Name, Role Template Manager Type, Role Template Manager Op Name, Role Template Manager Email Address, Role Template Manager First Name, Role Template Manager Id, Role Template Manager Last Name, Role View Report Type, Role View Report Op Name, Role View Report Email Address, Role View Report First Name, Role View Report Id, Role View Report Last Name, Routing Key Type, Routing Key Account Id, Routing Key Component Name, Routing Key File Extension, Routing Key File Id, Routing Key File Name, Routing Key Form Id, Routing Key Operation Name, Routing Key Product Name, Routing Key Resource Type, Routing Key Storage Center Id, Routing Key Submission Id, Routing Key Template Id, Routing Key Workflow Id, Routing Key Zone Id, Routing Key Zone Version, Server Name, Start Time, State, Step Data Type, Step Data File Id, Step Data Status, Step Data Step Type, Steps Completed, Steps Remaining, Steps Type, Steps Approvers Type, Steps Approvers Email Address, Steps Approvers First Name, Steps Approvers Id, Steps Approvers Last Name, Steps Days To Complete, Steps Sequential, Steps Step Id, Steps To Type, Steps To Email Address, Steps To First Name, Steps To Id, Steps To Last Name, Steps Viewers Type, Steps Viewers Email Address, Steps Viewers First Name, Steps Viewers Id, Steps Viewers Last Name, Steps Viewers Name, Storage Center Id, Stream Id, Submission Id, Templated Id, Trigger Type, Trigger Folder Ids, Trigger Form Id, User Id, Workflow Type, Workflow Id, Workflow Initiator Type, Workflow Initiator User Id, Workflow Name, Workflow Template Id, Workflow Trigger Resource Id, Workflow Trigger Type, Workflow Initiator Info User Id, Workflow Status, Workflow Type, Zone Id, Zone Services, Zone Version

• File Extension

• File Id

• File Name

• File Path
• File Size
• File Size Bytes
• First Name
• Folder Id
• Folder Name
• Grant Types
• Group Id
• Has Encryption
• Has Multiple Versions
• Has Power Tools
• Hash
• Integration OAuth Client Id
• Integration Provider Type
• IRM Classification Id
• Is Confirmed
• Is Disabled
• Is Employee
• Is Free Trial
• Is Shared
• Is Template Owned
• Is View Only
• Item Extension
• Item Extensions
• Last Any Login
• Last Name
• Lock Id
• Lock Type
• Logo URL
• Max Downloads
• Method
• Name
• New Stream Id
• Number Of Licenses
• Number Of Paid Licenses
• OAuth Client Id
• Old Stream Id
• Operation Name
• Owner Id
• Parent Id
• Path
• Phone
• Plan Name
• Plan Track
• Power Tools Rate
• Price Per License
• Primary Email
• Primary Subdomain
• Product Code
• Product Name
• Recipient Id
• Recipient Ids
• Redirect URIs
• Required Login
• Required User Info
• Resource Type
• Root Item Id

• Routing Key: Account Id, Add On Name, App Code, Component Name, Connector Type, Entity Id, File Id, Folder Id, Group Id, Integration Provider Type, OAuth Client Id, Operation Name, Parent Id, Product Name, Resource Type, Share Id, Stream Id, User Id, Version, Zone Id
Citrix Analytics for Performance

- Scope
- Semantic Path
- Server Name
- Share Id
- Share Info: Alias Id, Creator Id, Share Id, Share Sub Type Id
- Share Sub Type Id
- Share Type
- Single Version
- Start Time
- State
- Storage Center Name
- Stream Id
- Subdomains: Op Name, Values
- Subscribed Resource Id
- Subscribed Resource Type
- Tax Area Code
- Title
- Update Date
- Upload Id
- URL Path
- Use Advanced Custom Branding
- User Email
- User Id
- User Max
- User Roles: Op Name, Values
- Version
- Webhook Subscription Id
- Webhook URL
- Zip
- Zone Id
Citrix Endpoint Management service logs

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

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

Citrix Secure Private Access logs

- AAA User Name
- Auth Policy Action Name
- Authentication Session ID
- Request URL
- URL Category Policy Name
- VPN Session ID
• Vserver IP
• AAA User Email ID
• Actual Template Code
• App FQDN
• App Name
• App Name Vserver LS
• Application Flags
• Authentication Type
• Authentication Stage
• Authentication Status Code
• Back-end Server Dst IPv4 Address
• Back-end Server IPv4 Address
• Back-end Server IPv6 Address
• Category Domain Name
• Category Domain Source
• Client IP
• Client MSS
• Client Fast Retx Count
• Client TCP Jitter
• Client TCP Packets Retransmitted
• Client TCP RTO Count
• Client TCP Zero Window Count
• Clt Flow Flags Rx
• Clt Flow Flags Tx
• Clt TCP Flags Rx
• Clt TCP Flags Tx
• Connection Chain Hop Count
• Connection Chain ID
• Egress Interface
• Exporting Process ID
• Flow Flags Rx
• Flow Flags Tx
• HTTP Content Type
• HTTP Domain Name
• HTTP Req Authorization
• HTTP Req Cookie
• HTTP Req Forw FB
• HTTP Req Forw LB
• HTTP Req Host
• HTTP Req Method
• HTTP Req Rcv FB
• HTTP Req Rcv LB
• HTTP Req Referer
• HTTP Req URL
• HTTP Req XForwarded For
• HTTP Res Forw FB
• HTTP Res Forw LB
• HTTP Res Location
• HTTP Res Rcv FB
• HTTP Res Rcv LB
• HTTP Res Set Cookie
• HTTP Rsp Len
• HTTP Rsp Status
• HTTP Transaction End Time
• HTTP Transaction ID
• IC Cont Grp Name
• IC Flags
• IC No Store Flags
• IC Policy Name
• Ingress Interface Client
• NetScaler Gateway Service App ID
• NetScaler Gateway Service App Name
• NetScaler Gateway Service App Type
• NetScaler Partition ID
• Observation Domain ID
• Observation Point ID
• Origin Res Status
• Origin Rsp Len
• Protocol Identifier
• Rate Limit Identifier Name
• Record Type
• Responder Action Type
• Response Media Type
• Srv Flow Flags Rx
• Srv Flow Flags Tx
• Srvr Fast Retx Count
• Srvr TCP Jitter
• Srvr TCP Packets Retransmitted
• Srvr TCP Rto Count
• Srvr TCP Zero Window Count
• SSL Cipher Value BE
• SSL Cipher Value FE
• SSL Client Cert Size BE
• SSL Client Cert Size FE
• SSL Clnt Cert Sig Hash BE
• SSL Clnt Cert Sig Hash FE
• SSL Err App Name

© 1999–2022 Citrix Systems, Inc. All rights reserved.
• SSL Err Flag
• SSL Flags BE
• SSL Flags FE
• SSL Handshake Error Msg
• SSL Server Cert Size BE
• SSL Server Cert Size FE
• SSL Session ID BE
• SSL Session ID FE
• SSL Sig Hash Alg BE
• SSL Sig Hash Alg FE
• SSL Srvr Cert Sig Hash BE
• SSL Srvr Cert Sig Hash FE
• SSL iDomain Category
• SSL iDomain Category Group
• SSL iDomain Name
• SSL iDomain Reputation
• SSL iExecuted Action
• SSL iPolicy Action
• SSL iReason For Action
• SSL iURL Set Matched
• SSL iURL Set Private
• Subscriber Identifier
• Svr Tcp Flags Rx
• Svr Tcp Flags Tx
• Tenant Name
• Tracing Req Parent Span ID
• Tracing Req Span ID
• Tracing Trace ID
• Trans Clt Dst IPv4 Address
• Trans Clt Dst IPv6 Address
• Trans Clt Dst Port
• Trans Clt Flow End Usec Rx
• Trans Clt Flow End Usec Tx
• Trans Clt Flow Start Usec Rx
• Trans Clt Flow Start Usec Tx
• Trans Clt IPv4 Address
• Trans Clt IPv6 Address
• Trans Clt Packet Tot Cnt Rx
• Trans Clt Packet Tot Cnt Tx
• Trans Clt RTT
• Trans Clt Src Port
• Trans Clt Tot Rx Oct Cnt
• Trans Clt Tot Tx Oct Cnt
• Trans Info
• Trans Srv Dst Port
• Trans Srv Packet Tot Cnt Rx
• Trans Srv Packet Tot Cnt Tx
• Trans Srv Src Port
• Trans Svr Flow End Usec Rx
• Trans Svr Flow End Usec Tx
• Trans Svr Flow Start Usec Rx
• Trans Svr Flow Start Usec Tx
• Trans Svr RTT
• Trans Svr Tot Rx Oct Cnt
• Trans Svr Tot Tx Oct Cnt
• Transaction ID
• URL Category
• URL Category Group
Citrix Analytics for Performance

• 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
• 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
Citrix Analytics for Performance

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

Citrix ADC logs

The Citrix ADC logs contain the following data points:

- Container
- Files
- Format
- Type

Citrix DaaS Standard for Azure logs

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

- App Name
- Browser
- Details: Format Size, Format Type, Initiator, Result
- Device Id
- Device Type
- File Name
- File Path
- File Size
- Jail Broken
Citrix Analytics for Performance

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

Note

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

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

Microapps service logs

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

- Data Integration Provider API Call Average Duration
- Data Integration Provider API Call Peak Rate
- Data Integration Provider API Call Rate
- Data Integration Provider API Calls Total
- Data Integration Provider API Call Duration
- Data Integration Provider API Call Result

Citrix Identity provider logs

- User Login:
  - Authentication Domains: Name, Product, IdP Type, IdP Display Name
    - IdP Properties: App, Auth Type, Customer Id, Client Id, Directory, Issuer, Logo, Resources, TID
    - Extensions:
      - Workspace: Background Color, Header Logo, Logon Logo, Link Color, Text Color, StoreFront Domains
      - ShareFile: Customer Id, Customer Geo
      - Long Lived Token: Enabled, Expiry Type, Absolute Expiry Seconds, Sliding Expiry Seconds
  - Authentication Result: User Name, Error Message
  - Sign-in Message: Client Id, Client Name
  - User Claim: AMR, Access Token Hash, Aud, Auth Time, CIP Cred, Auth Alias, Auth Domains, Groups, Product, System Aliases, Email, Email Verified, Exp, Family Name, Given Name, IAT, IdP, ISS, Locale, Name, NBF, SID, Sub
    - 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

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Citrix Gateway logs

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

  - ICA Event: Record Type, Actual Template Code, Source IPv4 Address Rx, Destination IPv4 Address Rx, ICA Session Guid, MSI Client Cookie, Connection Chain ID, ICA Client Version, ICA Client Host Name, ICA User Name, ICA Domain Name, Logon Ticket Setup, Server Name, Server Version, Flow Id Rx, ICA Flags, Observation Point Id, Exporting Process Id, Observation Domain Id, Connection Id, ICA Device Serial Number, ICA Session Setup Time, ICA Client IP, NS ICA Session Status Setup, Source Transport Port Rx, Destination Transport Port Rx, ICA Client Launcher, ICA Client Type, ICA Connection Priority Setup, NS ICA Session Server Port, NS ICA Session Server IP Address, IPv4, Protocol Identifier, Connection Chain Hop Count, Access Type

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


- **AppFlow**: Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, Transaction Id, Appfw Violation Occurred Time, App Name App Id, Appfw Violation Severity, Appfw Violation Type, Appfw Violation Location, Appfw Violation Threat Index, Appfw NS Longitude, Appfw NS Latitude, Source IPv4 Address Rx, Appfw Http Method, Appfw App Threat Index, Appfw Block Flags, Appfw Transform Flags, Appfw Violation Profile Name, Appfw Session Id, Appfw Req Url, Appfw Geo Location, Appfw Violation Type Name 1, Appfw Violation Name Value 1, Appfw Sig Category 1, Appfw Violation Type Name 2, Appfw Violation Name Value 2, Appfw Sig Category 2, Appfw Violation Type Name 3, Appfw Violation Name Value 3, Appfw Sig Category 3, Appfw Violation Type Name 4, Appfw Violation Name Value 4, Appfw Sig Category 4, Appfw Violation Type Name 5, Appfw Violation Name Value 5, Appfw Sig Category 5, Appfw X Forwarded For, Appfw App Name Ls, App Flow 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, SNP 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, HttpReq Cookie, HttpReq 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,
<table>
<thead>
<tr>
<th>Metric events:</th>
</tr>
</thead>
</table>

- **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,
Citrix Analytics for Performance

- 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 SvcCfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Service Group: RATE Si Tot Request Bytes, RATE Si Tot Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot 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 Ttlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb, Si Tot 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 SvcCfg, 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 Tc Count, RATE Tcp Err Rst, RATE Tcp Tot Client Open, RATE Tcp Tot Server Open, RATE Tcp Tot Rx Bytes, RATE Tcp Tot Rx Pkts, RATE Tcp Tot Syn, RATE Tcp Tot Tx Bytes, RATE Tcp Tot Tx Pkts, RATE Udp Tot Rx Bytes, RATE Udp Tot Rx Pkts, RATE Udp Tot Tx Bytes, RATE Udp Tot Tx Pkts, ALL Nic Tot Rx Mbits, ALL Nic Tot Rx Mbits, Cpu Use, Dns Tot Queries, Dns Tot Neg Nxdmn Entries, Http Tot Gets, Http Tot Others, Http Tot Posts, Http Tot Requests, Http Tot Requests 1.0, Http Tot Requests 1.1, Http Tot Responses, Http Tot Rx Request Bytes, Http 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
Citrix Analytics for Performance

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

- **Memory Pool:** Bind Entity Name, Entity Name, Mon Service Binding, NetScalerId, 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 Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rvd, Si Tot Pkt Sent, Si Ttlb Frustrating Transactions, Si Ttlb 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

---

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect

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

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

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

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

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

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

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

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

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

Microsoft Graph Security logs

• Tenant Id
• User Id
• Indicator Id
• Indicator UUID
• Event Time
• Create Time
• Category of alert
Citrix Analytics for Performance

- Logon Location
- Logon IP
- Logon Type
- User Account Type
- Vendor Information
- Vendor Provider Information
- Vulnerability States
- Vulnerability Severity

**Microsoft Active Directory logs**

- Tenant Id
- Collect Time
- Type
- Directory Context
- Groups
- Identity
- User Type
- Account Name
- Bad Password Count
- City
- Common Name
- Company
- Country
- Days Until Password Expiry
- Department
- Description
- Display Name
- Distinguished Name
- Email
• Fax Number
• First Name
• Group Category
• Group Scope
• Home Phone
• Initials
• IP Phone
• Is Account Enabled
• Is Account Locked
• Is Security Group
• Last Name
• Manager
• Member of
• Mobile Phone
• Pager
• Password Never Expires
• Physical Delivery Office Name
• Post Office Box
• Postal Code
• Primary Group Id
• State
• Street Address
• Title
• User Account Control
• User Group List
• User Principal Name
• Work Phone
Citrix Analytics for Performance logs

- actionid
- actionreason
- actiontype
- adminfolder
- agentversion
- allocationtype
- applicationid
- applicationname
- applicationpath
- applicationtype
- applicationversion
- associateduserfullnames
- associatedusername
- associatedusernames
- associateduserupns
- authenticationduration
- autoreconnectcount
- autoreconnecttype
- AvgEndpointThroughputBytesReceived
- AvgEndpointThroughputBytesSent
- blobcontainer
- blobendpoint
- blobpath
- brokerapplicationchanged
- brokerapplicationcreated
- brokerapplicationdeleted
- brokeringdate
- brokeringduration
• brokerloadindex
• brokerregistrationstarted
• browsername
• catalogchangeevent
• catalogcreatedevent
• catalogdeletedevent
• catalogid
• catalogname
• catalogsync
• clientaddress
• clientname
• clientplatform
• clientsessionvalidatedate
• clientversion
• collecteddate
• connectedviahostname
• connectedviaipaddress
• connectionid
• connectioninfo
• connectionstate
• connectiontype
• controllerdnsname
• cpu
• cpuindex
• createddate
• currentloadindexid
• currentpowerstate
• currentregistrationstate
• currentsessioncount
- datetime
- deliverygroupadded
- deliverygroupchanged
- deliverygroupdeleted
- deliverygroupid
- deliverygroupmaintenancemodechanged
- deliverygroupname
- deliverygroupsync
- deliverytype
- deregistrationreason
- desktopgroupdeletedevent
- desktopgroupid
- desktopgroupname
- desktopkind
- disconnectcode
- disconnectreason
- disk
- diskindex
- dnsname
- domainname
- effectiveloadindex
- enddate
- errormessage
- establishmentdate
- eventreporteddate
- eventtime
- exitcode
- failurecategory
- failurecode
- failedata
- failedate
- failurereason
- failuretype
- faultstate
- functionallevel
- gpoenddate
- gpostartdate
- hdxenddate
- hdxstartdate
- host
- hostedmachineid
- hostedmachinename
- hostingservername
- hypervisorconnectionchangedevent
- hypervisorconnectioncreatedevent
- hypervisorid
- hypervisormame
- hypervisorsync
- icartt
- icarttms
- id
- idletime
- inputbandwidthavailable
- inputbandwidthused
- instancecount
- interactiveenddate
- interactivestartdate
- ipaddress
- isassigned
- isinmaintenancemode
- ismachinephysical
- ispendingupdate
- ispreparing
- isremotepc
- issecureica
- lastderegisteredcode
- launchedviahostname
- launchedviaipaddress
- lifecyclestate
- LinkSpeed
- logonduration
- logonenddate
- logonscriptsenddate
- logonscriptsstartdate
- logonstartdate
- long
- machineaddedtodesktopgroupevent
- machineassignedchanged
- machinecatalogchangedevent
- machinecreatedevent
- machinedeletedevent
- machinederegistrationevent
- machinednsname
- machinefaultstatechangeevent
- machinehardregistrationevent
- machineid
- machinemaintenancemodechangeevent
• machinename
• machinepvdstatechanged
• machinerole
• machinesid
• machineupdatedevent
• machineregistrationendedevent
• machineremovedfromdesktopgroupevent
• machinesid
• memory
• memoryindex
• modifieddate
• NGSConnector.ICACo
• profileloadstartdate
• protocol
• provisioningschemeid
• provisioningtype
• publishedname
• registrationstate
• serversessionvalidatedate
• sessioncount
• sessionend
• sessionfailure
• sessionid
• sessionidlesince
• sessionindex
• sessionkey
• sessionstart
• sessionstate
• sessionsupport
• sessiontermination
• sessiontype
• sid
• SignalStrength
• siteid
• sitename
• startdate
• totalmemory
• triggerinterval
• triggerlevel
• triggerperiod
• triggervalue
Citrix Analytics for Performance

- usedmemory
- userid
- userinputdelay
- username
- usersid
- vdialogonduration
- vdaprocessdata
- vdaresourcedata
- version
- vmstartenddate
- vmstartstartdate
- windowsconnectionsetting
- xd.SessionStart

Limits

August 6, 2021

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

Configuration Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery Groups</td>
<td>1,000</td>
</tr>
<tr>
<td>Machines/VDAs</td>
<td>60,000</td>
</tr>
<tr>
<td>Machines on Process Utilization Group Policy</td>
<td>10,000</td>
</tr>
<tr>
<td>Number of on-premises CVAD Sites</td>
<td>20</td>
</tr>
</tbody>
</table>
Usage Limits

<table>
<thead>
<tr>
<th>Resource (across all CVAD Sites)</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concurrent administrators</td>
<td>2</td>
</tr>
<tr>
<td>Concurrent end users</td>
<td>100,000</td>
</tr>
<tr>
<td>Concurrent session launches</td>
<td>100,000</td>
</tr>
</tbody>
</table>

Citrix Analytics offerings

June 2, 2020

Citrix Analytics for Security

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

Learn more: Citrix Analytics for Security

Citrix Analytics for Performance

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

Learn more: Citrix Analytics for Performance

Citrix Analytics - Usage

Delivers consolidated basic usage information to all Citrix customers on supported Citrix products. You can view a timeline summary of active users with granular drill-downs, basic product usage, and core insights in easy-to-understand summary views.

Note

Citrix Analytics - Usage is included with the Citrix Analytics - Fundamentals package.

Learn more: Citrix Analytics - Usage.
Configuring on-premises Citrix Virtual Apps and Desktops Sites with Citrix Analytics for Performance

May 23, 2022

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.

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 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 following URLs:
  - Citrix Key Registration: https://*.citrixnetworkapi.net/
  - Citrix Cloud: https://*.citrixworkspacesapi.net/
  - Citrix Analytics: https://*.cloud.com/
  - Microsoft Azure: https://*.windows.net/

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:

```xml
<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.
The **defaultproxy** field in the config file controls the outbound access of Director and Monitor Service. Configuration and communication with Performance Analytics requires the **default-proxy** 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.

- Ensure accessibility to the following URLs from all endpoints (or proxies, if they are configured):
  - 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](microsoft.com/en-us/dotnet/framework/network-programming/proxy-configuration).

**Configuration steps**

After you have verified the prerequisites, do the following:

1. Log on to Director as a full administrator and select the Site which you want to configure with Performance Analytics.

2. Click the **Analytics** tab. The **Configuration** page is displayed.

3. Review the steps, select the terms of service, and then click **Get Started**.

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

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

7. Click **Copy Code** to copy the code and then click **Register on Citrix Cloud**.

8. You are redirected to the Registration URL in Citrix Cloud. Log in with your Citrix Cloud credentials and select your customer.

9. Paste the copied registration code in the Product Registrations page in Citrix Cloud. Click **Continue** to register. Review the registration details and click **Register**.
In case the registration input is not displayed, follow the steps described in Register a product.

10. Your on-premises Site registers with Citrix Cloud. Now, from Director, click Go to Analytics in the Analytics tab.

11. Citrix Analytics for Performance is opened on a new tab in your browser.
If your Citrix Cloud session has expired, you might be redirected to the Citrix.com or My Citrix account logon page.

12. 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.

13. 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.

Manage Administrator Roles for Performance Analytics

April 20, 2022
As a Citrix Cloud administrator with full access permissions, you can invite other administrators to manage the Performance Analytics offering and assign them one of the following custom 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.

**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 is 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.

**Self-service search**

July 7, 2022

**What is self-service search?**

The self-service search feature enables you to find and filter user events received from your data sources. You can explore the underlying user events and its attributes. These events help you to iden-
Citrix Analytics for Performance

tify 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
- Content Collaboration
- Gateway
- Secure Browser
- Secure Private Access
- Apps and Desktops
- Performance Users, Machines, and Sessions

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

How to access self-service search

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

- **Top bar**: Click Search from the top bar to view all user events for the selected data source.

- **Risk timeline on a user profile page**: Click Event Search to view the events for the respective user.

Self-service search from the top bar

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

1. Click Search to view the self-service page.

2. Select the data source and the time period to view the corresponding events.
Self-service search from user’s risk timeline

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

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

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

How to use self-service search

Use the following 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.

When you select a dimension and a valid operator, the values of the dimension are shown automatically. The list of values suggested for a dimension is either predefined (known values) in the data base or based on the historical events.

For example, the value of the Event-Type dimension is auto suggested. Whereas you need to manually enter the value of your Gateway-FQDN.

For example, the values of the dimensions Browser, IP-Address, City, and Country are suggested based on the users’ historical events. Whereas the values suggested for the dimension Clipboard-Operations are predefined such as copy, cut, or paste.

You can choose a value from the suggested values or enter a new value depending on your requirements.

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.
**Supported operators in search query**

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

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>:</td>
<td>Assign a value to a search dimension.</td>
<td>User-Name : John</td>
<td>Displays events for the user John.</td>
</tr>
<tr>
<td>=</td>
<td>Assign a value to a search dimension.</td>
<td>User-Name = John</td>
<td>Displays events for the user John.</td>
</tr>
<tr>
<td>~</td>
<td>Search events with similar values.</td>
<td>User-Name ~ test</td>
<td>Displays events having similar user names.</td>
</tr>
<tr>
<td>III III</td>
<td>Enclose values separated by spaces.</td>
<td>User-Name = “John Smith”</td>
<td>Displays events for the user John Smith.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Search for relational value.</td>
<td>Data Volume &gt; 100</td>
<td>Displays events where data volume is greater than 100 GB.</td>
</tr>
<tr>
<td>AND</td>
<td>Search events where the specified conditions are true.</td>
<td>User-Name : John AND Data Volume &gt; 100</td>
<td>Displays events of user John where data volume is greater than 100 GB.</td>
</tr>
<tr>
<td>! ~</td>
<td>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.</td>
<td>User-Name !~ John</td>
<td>Displays events for the users except John, John Smith, or any such users that contain the matching name “John”.</td>
</tr>
<tr>
<td>Operator</td>
<td>Description</td>
<td>Example</td>
<td>Output</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>!=</td>
<td>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.</td>
<td>Country != USA</td>
<td>Displays events for the countries except USA.</td>
</tr>
<tr>
<td>*</td>
<td>Search events that match the specified strings. Currently, the * operator is supported only with the following operators :, =, and !=. The search results are case-sensitive.</td>
<td>User-Name = John*</td>
<td>Displays events for all user names that begin with John.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User-Name = <em>John</em></td>
<td>Displays events for all user names that contain John.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User-Name = *Smith</td>
<td>Displays events for all user names that end with Smith.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User-Name : John*</td>
<td>Displays events for all user names that begin with John.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User-Name : <em>John</em></td>
<td>Displays events for all user names that contain John.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User-Name : *Smith</td>
<td>Displays events for all user names that end with Smith.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User-Name != John*</td>
<td>Displays events for all user names that do not begin with John.</td>
</tr>
</tbody>
</table>
### Operator Description Example Output

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>IN</code></td>
<td>Assign multiple values to a search dimension to get the events related to one or more values. <strong>Note:</strong> Currently, you can use this operator with the following dimensions of Apps and Desktops- <strong>Device ID, Domain, Event-Type, and User-Name.</strong> This operator is applicable only for the string values.</td>
<td>User-Name IN (John, Kevin)</td>
<td>Find all events related to John or Kevin.</td>
</tr>
<tr>
<td><code>NOT IN</code></td>
<td>Assign multiple values to a search dimension and find the events that do not contain the specified values. <strong>Note:</strong> Currently, you can use this operator with the following dimensions of Apps and Desktops- <strong>Device ID, Domain, Event-Type, and User-Name.</strong> This operator is applicable only for the string values.</td>
<td>User-Name NOT IN (John, Kevin)</td>
<td>Find the events for all users except John and Kevin.</td>
</tr>
<tr>
<td>Operator</td>
<td>Description</td>
<td>Example</td>
<td>Output</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>IS EMPTY</td>
<td>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.</td>
<td>Country IS EMPTY</td>
<td>Find events where the country name is not available or empty (not specified).</td>
</tr>
<tr>
<td>IS NOT EMPTY</td>
<td>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.</td>
<td>Country IS NOT EMPTY</td>
<td>Find events where the country name is available or specified.</td>
</tr>
</tbody>
</table>

**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
Citrix Analytics for Performance

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.

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.
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**.
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.
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.

Export visual summary

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

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

- The search query that you have specified for the events for the selected time period.
- The facets (filters) that you have applied on the events for the selected time period.
- The visual summary such as the timeline charts, bar charts, or graphs of the search events for the selected time period.
For a data source, you can download the visual summary report only if the data is displayed in visual formats such as bar charts, timeline details. Otherwise, this option is not available. For example, you can download the visual summary report of the data sources such as Apps and Desktops, Sessions, where you see data as timeline details and bar charts. For the data sources such as Users and Machines, you see data only in tabular format. Therefore, you cannot download any visual summary report.

**Multi-column sorting**

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

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

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

**Note**

You can add up to six columns to perform the sorting.

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

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

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

**How to save the self-service search**

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

- Applied search filters
- Selected data source and duration

Do the following to save a self-service query:

1. Select the required data source and duration.
2. Type a query in the search bar.
3. Apply the required filters.
4. Click **Save Search**.
5. Specify the name to save the custom query.
   
   **Note**
   
   Ensure that the query name is unique. Otherwise, the query does not save.

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

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

To remove a saved search:

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

To modify a saved search:

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

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

Note

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

Schedule an email for a search query

You can send a copy of the search query report to yourself and other users on regular intervals by setting up an email delivery schedule.
This option is available only if your search query report contains data in visual formats such as bar charts, timeline details. Otherwise, you cannot schedule an email delivery. For example, you can schedule an email for the data sources such as Apps and Desktops, Sessions, where you see data as timeline details and bar charts. For the data sources such as Users and Machines, you see data only in tabular format. Therefore, you cannot schedule an email.

**Schedule an email while saving a search query**

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

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

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

   **Note**
   
   Email groups are not supported.

3. Set the date and time for the email delivery.

4. Select the delivery frequency- daily, weekly, or monthly.

5. Click **Save**.
Schedule an email for an already saved search query

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

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

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

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.
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](#).
User Experience Analytics

August 11, 2022

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 sub factors, 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.
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 in 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.

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 atleast one Connected HDX Session: These users have had atleast 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
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.
  - HDXDisconnected 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.

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,

   ![User Experience (UX) Table](image)

   - 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.
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.
• **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.

• **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.

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.

**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
Citrix Analytics for Performance

displays the current thresholds used to plot the chart and the last updated time for the thresholds.

**Sessions Not Categorized for Logon Duration**

Sessions might be **Not Categorized** for Logon Duration if the sub factors are not configured to be measured as described in Session Logon Duration sub factors.

**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.
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 Higher Precision mode.

**User Experience**

March 30, 2022

**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.
Citrix Analytics for Performance

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 sub factors/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 sub factor 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 sub factors 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 sub factors 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.
- 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.
1. **Benchmark factors:**

   For each session, Session Logon Duration and Session Responsiveness factors and their sub factors 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 metrics of users with a poor user experience score helps identify a particular factor or sub factor that is
causing the poor experience.

User Experience (UX) Factors

April 5, 2022

The UX Factors page provides an insight into the factor and sub factor level experience of the set of users you select in the UX dashboard.

Click any of the Excellent, Fair, or Poor UX category in the UX dashboard to open the UX Factors page. It quantifies the effect of factor and sub factor 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 sub factors within these factors. This drilldown enables you to identify the actual sub factor 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 in 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.

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.

Click the **Selected users** number to access the self-Service Search page for the specific set of users.
4. The sections in 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 sub factors. 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 sub factor 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 sub factors might have been excellent.

7. The classification of users at factor and sub factor 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 Sub factors

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.

<table>
<thead>
<tr>
<th>Session Logon Duration</th>
<th>8 Users</th>
<th>12 Users</th>
<th>1 Users</th>
<th>4 Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPOs</td>
<td>Excellent</td>
<td>Poor</td>
<td>Not Categorized</td>
<td>Not Categorized</td>
</tr>
<tr>
<td>Profile Load</td>
<td>0</td>
<td>7</td>
<td>14</td>
<td>4</td>
</tr>
<tr>
<td>Interactive Session</td>
<td>2</td>
<td>17</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Booting</td>
<td>10</td>
<td>11</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>UI Start</td>
<td>3</td>
<td>8</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Initiation Connection</td>
<td>17</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>4</td>
<td>17</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Logs/Scripts</td>
<td>1</td>
<td>11</td>
<td>9</td>
<td>4</td>
</tr>
</tbody>
</table>

Clicking the classified user count numbers lead to the Self-Service screen displaying the actual performance factor measurements for the selected set of users.

Session Logon Duration is broken down into sub factors 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.

<table>
<thead>
<tr>
<th>Session Logon Duration</th>
<th>6 USERS</th>
<th>12 USERS</th>
<th>1 USERS</th>
<th>4 USERS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EXCELLENT</td>
<td>FAIR</td>
<td>POOR</td>
<td>NOT CATEGORIZED</td>
</tr>
<tr>
<td>GPOs</td>
<td>7</td>
<td>10</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Profile Load</td>
<td>0</td>
<td>7</td>
<td>14</td>
<td>4</td>
</tr>
<tr>
<td>Interactive Session</td>
<td>2</td>
<td>17</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Breaking</td>
<td>0</td>
<td>10</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>Start</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>Domain Connection</td>
<td>2</td>
<td>17</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Authentication</td>
<td>0</td>
<td>4</td>
<td>17</td>
<td>4</td>
</tr>
<tr>
<td>Login Length</td>
<td>1</td>
<td>11</td>
<td>9</td>
<td>4</td>
</tr>
<tr>
<td>Not Categorized</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The user counts for Excellent, Fair, and Poor category related to each sub factor experience are displayed. Use this information to analyze specific sub factor 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 sub factor measurements are not available for the selected time period. Specific reasons are elaborated with individual sub factor 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 sub factor 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 processing improve the overall session logon experience of the user.
Citrix Analytics for Performance

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.

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.

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 sub factors

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 sub factor measurements are obtained from the Citrix Gateway. Hence, the sub factor values are available only when the user is connecting to an app or a desktop via a configured Citrix Gateway. For steps to configure Citrix Gateway with Citrix Analytics for Performance, see Gateway data source.

Further, these measurements are available for sessions,

- launched from machines enabled for NSAP
- new CGP (Common Gateway Protocol) sessions, and not reconnected sessions.

The rows in the Session Responsiveness drilldown table represent the user categorization in the sub factor measurements. For each sub factor, the number of users in each category is displayed in the Excellent, Fair, and Poor columns. This information helps analyze the specific sub factor 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 sub factor measurement was not available during the selected time period.

The following sub factors contribute to the Session Responsiveness. However, the total ICA RTT is not a sum of the sub factor metrics, as the sub factors of ICA RTT that occur until Layer 4 only are measurable.

- **Data Center Latency**: This sub factor 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 sub factor 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 sub factor 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 sub factors 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.

- **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 Failure Reasons 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.

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.
Citrix Analytics for Performance

**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.

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.
  - 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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.
• 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 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.

**Self-Service Search for Performance**

August 19, 2022
Self-service search gives 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 in 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 in the left hand pane. The set of users, sessions, or machines displayed is based on the selection criteria.
Select facets to filter events

Use the facets in the left-hand side pane to filter the data. Some of the facets associated with the Citrix Analytics for Performance are as follows:
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.

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.
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 machine not functional, or a registration timeout.
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.
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.

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
Citrix Analytics for Performance

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.
- 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.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDX</td>
<td>153</td>
</tr>
<tr>
<td>Not Available</td>
<td>10</td>
</tr>
<tr>
<td>RDP</td>
<td>15</td>
</tr>
<tr>
<td>Console</td>
<td>9</td>
</tr>
</tbody>
</table>

This facet lists only the current protocols of sessions and not all supported session protocols.

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Citrix Analytics for Performance

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 in 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 in the Sessions Self-service view. It helps find the number of sessions that were launched via Connection Lease.

Aggregated State

This facet is available in 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.

Self-service search for Users

The Users based self-service page is available on clicking the user classification numbers in 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.
Citrix Analytics for Performance

- **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.

**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 in 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 in the Sessions self-service view. Visual Summary chart displays sessions categorized by Session 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.

![Visual Summary Chart](image)

**Use case - Access Visual Summary using the Search menu**

You can visualize the result of your custom search query in 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.

**Tabular data**

This Sessions self-service view provides important performance metrics related to sessions in tabular format, such as,

- **Session Experience**: Session Experience score based on the performance factors.
- **Session specific metrics**: Metrics such as the session start time and launch status.
- **Session specific factors and sub factors measurement**: Key performance indicators that affect the session experience.
- **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.
- **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 Analytics for Performance

- 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 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:
  - 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

These metrics are available out-of-the-box for Citrix DaaS (formerly Citrix Virtual Apps and Desktops service).

- You need machines running Citrix Virtual Apps and Desktops 7 2112 or later.
- The **VDA data collection for Performance Analytics** policy must be set to **Allowed** on machines to enable the Monitoring service to collect machine related performance metrics. For more information, see **Policy for collecting data for Performance Analytics**.

- **Session Duration** Displays the length of the session.

- **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 several 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.

- **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 (P95)** Link speed helps identify if the poor session experience was due to low speed.

- **Endpoint Throughput Incoming (P95)** Displays the total bytes received.

- **Endpoint Throughput Outgoing (P95)** Displays the total bytes sent.

Tabular data in 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?

![Color Coded Table](image)

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.

### 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.

This view provides the important performance metrics related to machines, such as,

- **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 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 represents 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.
Citrix Analytics for Performance

- **Peak CPU**: Maximum CPU utilization recorded in the selected time period.
- **Avg Memory Consumption**: Average memory consumption in the selected time period.
- **Peak Memory Consumption**: Maximum memory consumption recorded in the selected time period.

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 in 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.

**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.

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”. 

© 1999–2022 Citrix Systems, Inc. All rights reserved.
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.

**Connector Statistics**

March 2, 2022

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.

**Accessing the Connector statistics page**

Click the connector name link from the Self-service view for Sessions.
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 correlate the usage pattern of connector resources with high latency and poor session performance occurrences.

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.

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.

**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 in the User Experience dashboard.

The Sessions self-service view is displayed with the details of the sessions having poor session responsiveness.
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** column 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.

**Session Details**

April 27, 2022

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 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.
Citrix Analytics for Performance

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.

Accessing the Session Details page

Click the session score link from the Self-service view for Sessions.

<table>
<thead>
<tr>
<th>Session Experience</th>
<th>User Name</th>
<th>Delivery Group Name</th>
<th>Session Start Time</th>
<th>Machine Name</th>
<th>Endpoint CE (Last Hours)</th>
<th>Launch Status</th>
<th>Session Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Citrix Core</td>
<td>Dec 15, 2021, 04:48:07 UTC</td>
<td>N/A</td>
<td></td>
<td>Succeeded</td>
<td>4 hrs 59 mins</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Citrix Core</td>
<td>Dec 14, 2021, 2:07:07 UTC</td>
<td>N/A</td>
<td></td>
<td>Succeeded</td>
<td>3 mins</td>
</tr>
</tbody>
</table>

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 in a single view. This information helps correlate the session performance with these factors.

The Session Statistics page displays data for up to 72 hours of the session duration.

Session attributes

Key session attributes are displayed - user name, session status, total session duration, logon duration of the session, Delivery Group and Site the session belongs to, and the machine on which the session was launched. Click the machine name link to see the corresponding Machine Statistics page.
Citrix Analytics for Performance

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
- 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. P95 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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.
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.

**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 is available in 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. In 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 factor 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**

July 22, 2022

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.

<table>
<thead>
<tr>
<th>Security</th>
<th>Performance</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Delivery Group</td>
<td>Machine OS Type</td>
</tr>
<tr>
<td>Site Name</td>
<td>Delivery Group</td>
<td>Machine OS Type</td>
</tr>
<tr>
<td>Delivery Group</td>
<td>Machine Type</td>
<td>Single-session</td>
</tr>
<tr>
<td>Machine OS Type</td>
<td>Last 24 hours</td>
<td>Last 1 month</td>
</tr>
</tbody>
</table>

**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** and **Site** the machine belongs to,
- **OS type, OS** of the machine,
• **Downtime** represents the period in seconds during which the machine was in **Unregistered**, **Failed**, or **Powered off** state in the last 24 hours.

**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 Sessions** represents the maximum number of concurrent sessions that were established on the machine over the past 24 hours.
- 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.

**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 only for multi-session OS machines on cloud sites.

You can choose to view the processes ranked as per **CPU Utilization** or **Memory Consumption**.
Top three **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 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 currently available for multi-session OS machines. This feature requires that you enable the **Process Monitoring policy** from Citrix Studio.

For more information, see **Monitoring policy settings**
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 the machine has been in.

Time navigation bar

Machine and User Session 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 2–8 hour window, to view the events corresponding to the selected time range.

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.

**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.
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.
Machine Actions and Composite 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
- 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.

**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 composite action and that of the individual steps are displayed under the Actions link.

The User Experience Dashboard and the UX Factors pages can have users and sessions not categorized in excellent, fair, or poor categories with respect to a particular factor or sub factor. 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.
Citrix Analytics for Performance

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.

Users Not Categorized

Users were not categorized due to one or more of the following reasons:

<table>
<thead>
<tr>
<th>REASON</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>EUEM service not active</td>
<td>Check service status</td>
</tr>
<tr>
<td>Unsupported CWA version</td>
<td>Check CWA version</td>
</tr>
<tr>
<td>Unsupported VDA version</td>
<td>Check VDA version</td>
</tr>
<tr>
<td>UPM service not active</td>
<td>Check service status</td>
</tr>
</tbody>
</table>

For more information on other reasons, click **Learn more**.

- **EUEM service not active**: Citrix EUEM service needs to 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 you can run to identify the machines in your apps and desktops environment that don’t have the Citrix EUEM service running.
Citrix Analytics for Performance

- **UPM service not active:** Citrix Profile Management service needs to 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 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:

<table>
<thead>
<tr>
<th>Reason</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session duration &lt; 5 min</td>
<td>View sessions</td>
</tr>
<tr>
<td>Unsupported CWA version</td>
<td>Check CWA version</td>
</tr>
<tr>
<td>Unsupported VDA version</td>
<td>Check VDA version</td>
</tr>
<tr>
<td>EUEM service not active</td>
<td>Check service status</td>
</tr>
</tbody>
</table>

For more information on other reasons, click Learn more.

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 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.

**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.
- 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.

Location and ISP N/A

- Endpoint is not running Citrix Workspace app for Windows version 1912 or later.
- Session state is Failed.
- 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.

**Endpoint Network Metrics N/A**

Endpoints are not running Citrix Workspace app for Windows version 2108 or later.

**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.

```powershell
1 add-pssnapin citrix*
2
4 $dgList = @('All') #Add the delivery group names here
5 #Get list of machine in that environment
6 if($dgList[0] -eq 'All')
7 {
8     $machineList = Get-BrokerMachine
9 } else
10
11
12
13 ©1999–2022 Citrix Systems, Inc. All rights reserved.
165```
```powershell
{  
    for($i=0; $i -lt $dgList.Length; $i++)  
    {  
        $machineList += Get-BrokerMachine -DeliveryGroupName $dgList[$i]  
    }  
}  

$upmNotRunning = [System.Collections.ArrayList] @()  
$euemNotRunning = [System.Collections.ArrayList] @()  
# Check for UPM and EUEM service status in machine  
for($i=0; $i -lt $machineList.Length; $i++)  
{  
    Write-Host("Machine Name : " + $machineList[$i].DNSName)  
    # UPM Service check  
    $upm = Get-Service ctxProfile -ComputerName $machineList[$i].DNSName -ErrorVariable getServiceErrorUpm -ErrorAction SilentlyContinue  
    if ($getServiceErrorUpm.Count -gt 0 -and ($getServiceErrorUpm | foreach {$_.FullyQualifiedErrorId -like "*NoServiceFoundForGivenName*"}))  
    {  
        Write-Warning "There is no service named UPM in $machineList[$i].DNSName"  
        $upmNotRunning.Add($machineList[$i].DNSName)  
    }  
    elseif ($getServiceErrorUpm.Count -gt 0)  
    {  
        Write-Warning("Exception on $machineList[$i].DNSName : $getServiceErrorUpm")  
    }  
}  
```
else
{
    if (-Not('Running' -eq $upm.Status))
    {
        Write-Host("UPM service not running on $machineList[$i].DNSName")
        $upmNotRunning.Add($machineList[$i].DNSName)
    }
}

#EUEM Service check
$euem = Get-Service 'Citrix EUEM' -ComputerName $machineList[$i].DNSName -ErrorVariable getServiceErrorEuem -ErrorAction SilentlyContinue

if ($getServiceErrorEuem.count -gt 0 -and ($getServiceErrorEuem | foreach {
$_ .FullyQualifiedErrorId -like "*NoServiceFoundForGivenName*" })
)
{
    Write-Warning "There is no service named Citrix EUEM in $machineList[$i].DNSName"
    $euemNotRunning.Add($machineList[$i].DNSName)
}
elseif ($getServiceErrorEuem -gt 0)
{
    Write-Warning("Exception on $machineList[$i].DNSName : $getServiceErrorEuem")
}
else
{
    if (-Not('Running' -eq $euem.Status))
    {
        Write-Host("EUEM service not running on $machineList[}
Infrastructure Analytics

August 19, 2022

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.
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. 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.
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.

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.

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.

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.
- 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:

- 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.

**Insights**

August 5, 2022

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 diagnostic 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.

Each insights sub pane shows crucial insights about failures that have occurred on the site. A link to the failed sessions or the machines hosting them, 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 or session and see the timeline details and the detailed metrics.

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

**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 in the sessions based self-service view, see Self-service search for sessions.
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 fail 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, thus enabling 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.
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.

**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 in 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.
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.

**Alerts**

**August 22, 2022**

Performance Analytics generates alerts to help administrators to monitor the environment proactively. The alerts are generated when factors affecting the user experience get deteriorated.

The available policies are listed in the **Alert Policies** tab. The alerts are enabled by default, and can be disabled using the **Status** toggle. By default, alert mails are sent to all full administrators in the customer. Click the alert name to edit the mail recipients list.
You must enable receiving email notifications from the **Account Settings** menu in Citrix Cloud to receive the alert mails. For more information, see the **Notifications article**.

### Alert for Machines with Zombie Sessions

A Zombie session alert mail is generated when a new machine with a zombie session is detected in the environment in a 15 min interval.

An email alert containing details of the number of machines with zombie sessions and sessions 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.

![Citrix Analytics for Performance Machines with New Zombie Sessions detected](image)

We have identified single-session U3 machines with abandoned sessions resulting in failure of new session launches on these machines. These session failures might degrade the user experience on your site. [Learn more](#).

<table>
<thead>
<tr>
<th>Zombie Sessions</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machines with abandoned sessions</td>
<td>12</td>
</tr>
<tr>
<td>Machines with session failures</td>
<td>46</td>
</tr>
</tbody>
</table>

**Recommended actions:**
- Log off users / Reboot machines [Learn more](#)

Click **View machines** in the mailer to see single-session machines with abandoned sessions in 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.

Realerting 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.
**Alert for Sessions with Anomalous Latency**

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.

A machine learning model is used to determine the baseline latency value for all Delivery Group-Location pairs in a specific customer. The baseline latency value is calibrated every day based on the data 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. The amount of deviation quantifies the impact of the poor latency on the session experience for these users.

The next alert is generated when the ICARTT measurements are higher than the last known value.

This feature requires you to 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*.

The mail contains the following details for a specific customer, Delivery Group, and Location,

- Latency, the ICARTT value measured in the specified period
- Delivery Group of the virtual machine
- Location of the endpoint
- Median Latency and its variation from the baseline.
- Number of sessions affected by poor responsiveness
- Percentage variation of measured latency from the baseline value.
Click View Issue Details to go to the Sessions self-service view with the list of sessions that were affected by poor responsiveness. Analyze the fields showing such as 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. An Overloaded Machines alert mail is sent to administrators when an overloaded machine is detected in the environment in a 15 minutes interval.
If the machine continues to be in overloaded condition, realert 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 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
Citrix Analytics for Performance

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.

For more information about Overloaded Machine Insights, 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. 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.

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 realerted if the number of session failures due to the same black hole machine is doubled within 24 hours.

The View latest insights link leads to the User Experience dashboard showing the latest statistics in the Insights panel.

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