Session Recording service
Contents

Session Recording service (preview) 3
What's new 5
Third party notices 6
Get started 7
Plan your deployment 7
Connect Session Recording servers 10
Configure 14
Configure Session Recording servers 15
Configure policies 16
Configure session recording policies 17
Configure event detection policies 21
Configure event response policies 23
Configure playback permissions 32
Configure utilities 37
View recordings 38
Search for, archive, and delete recordings 38
Open and play recordings 42
Highlight idle periods 44
Use events and comments 45
View graphical event statistics for each recording 48
View data points related to each recorded session 52
Query administrator logging data 53
Customer data management 58
Session Recording service

Session Recording service (preview)

July 26, 2022

Note:

• The Session Recording service is available for provisioning in the Asia Pacific South (APS), EU, and US regions of Citrix Cloud. For more information, see Citrix Cloud Geographical Considerations.
• For information about the Session Recording service customer data storage, retention, and control, see Customer data management.
• The Session Recording service doesn’t send data to Citrix Analytics for Security (CAS). On-premises Session Recording servers can send data to CAS. For more information, see Connect to Session Recording deployment in the Citrix Analytics for Security documentation.

Overview

Session Recording is a key differentiator for security in Citrix DaaS (formerly the Citrix Virtual Apps and Desktops service). A common challenge that prevents you from benefiting from Session Recording is the solution’s deployment and management complexity.

The introduction of the Session Recording service provides an advanced administration experience and simplifies deployment. It supports centralized management of server settings, policies, and playback. It facilitates administrative tasks by providing a unified entry point to manage and observe the Session Recording servers across your organization.

The following diagram illustrates how the Session Recording service works.
Service features and functionality

You can use the Session Recording service to perform the following actions:

- Connect both on-premises and cloud-deployed Session Recording servers to the Session Recording service.
- Configure settings on the connected Session Recording servers.
- Configure session recording, event detection, and event response policies for a specific site.
- Configure role-based access control for recordings.
- Query and play recordings from the connected Session Recording servers.
- View event visualization reports and leave comments about recordings.

Prerequisites

Prerequisites for using the Session Recording service:

- You have subscribed to Citrix DaaS.
- You have a Session Recording 1912 LTSR, 2203, or later deployment in place.

For information on how to install the Session Recording components, see the installation article.
Session Recording service

What’s new

July 28, 2022

A goal of Citrix is to deliver new features and product updates to Session Recording service customers when they are available. New releases provide more value, so there's no reason to delay updates. Updates are rolled out to the service release approximately every six weeks.

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

July 2022

Support for 1912 LTSR

Previously, using the Session Recording service required a Session Recording 2203 or later deployment. Starting with this release, you can connect Session Recording servers in a 1912 LTSR deployment to the Session Recording service.

Support for archiving and deleting recordings

You can now archive and delete recordings using the Session Recording service. When archiving recordings, you can choose to move the recording files to a different location from the one where they were originally stored. When deleting recordings, you can choose to also delete the recording files along with the database records.

For information about the archiving and deletion operations, see Search for, archive, and delete recordings.

June 2022

Session Recording service available in the Asia Pacific South (APS) region of Citrix Cloud

The Session Recording service is now available for provisioning in the Asia Pacific South (APS) region of Citrix Cloud.

Load-balancing Session Recording servers across sites

You can now manage Session Recording servers by load-balancing them across multiple sites. You can also create or activate a policy for all Session Recording servers in a site at a time. For more information, see Connect Session Recording servers, Configure Session Recording servers, and Configure session recording policies.
Custom domain name support for HTTPS requests

In addition to the default FQDN, a Session Recording server can now use, for HTTPS requests, a custom domain name with an SSL certificate binding. For more information, see Connect Session Recording servers.

Support for configuring additional event response actions from the cloud

In addition to email alerts and dynamic screen recording, you can now configure, from the cloud, the following actions in response to logged events in recorded sessions:

- Lock session
- Log off session
- Disconnect session

This feature is available for Session Recording 2206 and later. For more information, see Configure event response policies.

April 2022

Session Recording service available in the EU region of Citrix Cloud

The Session Recording service is now available for provisioning in the EU region of Citrix Cloud.

Administrator logging data available in the Session Recording service

The Session Recording service presents administrator logging data for Session Recording server 2204 and later. The data contains logs of administrator activities and of applicable policies triggering recordings. For more information, see Query administrator logging data.

Support for configuring playback permissions

By default, all Citrix Cloud administrators with the Session Recording role have permission to play all recordings. You can now limit playback permissions so that Session Recording read-only administrators can play only specific recordings on a target Session Recording server. For more information, see Configure playback permissions.

Third party notices

March 30, 2022
The Session Recording service might include third-party software licensed under the terms defined in the following document:

The Session Recording service Third Party Notices

Get started

June 15, 2022

This section provides instructions for you to:

- Plan your deployment
  - Connectivity requirements
  - Increase the transport packet size
  - Install certificates in IIS
  - Switch to web streaming service version 2.0
- Connect Session Recording servers

Plan your deployment

June 14, 2022

Connectivity requirements

Session Recording cloud client

The Session Recording cloud client requires access to the following addresses:

- https://*.citrixworkspacesapi.net (provides access to Citrix Cloud APIs that the services use)
- https://*.cloud.com (provides access to the Citrix Cloud sign-in interface)
- https://*.blob.core.windows.net (provides access to Azure Blob Storage, which stores updates for Citrix Cloud Connector)
- https://*.servicebus.windows.net (provides access to Azure Service Bus, which is used for logging and for the Active Directory agent)

Ports
Session Recording service

<table>
<thead>
<tr>
<th>Usage</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>For video playback</td>
<td>Open port 9191 on end users' devices and networks</td>
</tr>
<tr>
<td>For communication with the cloud</td>
<td>Allow outbound ports 8088 and 9090–9094 on each Session Recording server</td>
</tr>
</tbody>
</table>

**Proxy**

You can set up a proxy when installing the Session Recording cloud client. For more information, see Connect Session Recording servers.

**Increase the transport packet size**

1. Locate the Web configuration file under `<Session Recording installation path>/WebSocketServer`.
2. Open the Web configuration file.
3. Edit the BlockSizeMultiple value.

   The default value is 1 (4 KB). We recommend you set the value to 8 (32 KB).
Install certificates in IIS

Add an SSL binding in IIS so that:

- The Session Recording servers can connect to Citrix Cloud properly.
- You can use HTTPS to access the player.

For more information, see step 1 of HTTPS configuration.

Switch to web streaming service version 2.0

A fresh installation of Session Recording 2103 and later connects your web browser to the web streaming service hosted in IIS when you access the player. The web streaming service hosted in IIS is versioned 2.0, as indicated by WebsocketServerVersion under HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.
An upgrade installation from an earlier version to Session Recording 2103 and later connects your web browser to the Python-based web streaming service, which is versioned 1.0. To connect to the web streaming service hosted in IIS, run the `<Session Recording Server installation path>\Bin\SsRecUtils.exe -enablestreamingservice` command.

**Connect Session Recording servers**

**July 27, 2022**

The welcome page highlights four main steps for setting up the Session Recording service. The first and most important step is connecting your Session Recording servers to the Session Recording service. You can connect Session Recording servers in a 1912 LTSR, 2203, or later deployment to the Session Recording service.
On each server you want to connect, complete the following steps:

1. Allow outbound ports 8088 and 9090–9094.
2. Install the Session Recording cloud client by using a command similar to the following:

```
msiexec /i SRCloudClientService.msi CUSTOMERID="<Citrix Cloud customer ID>" CLIENTID="<secure client ID>" CLIENTSECRET="<secure client secret>" CUSTOMDOMAIN="<a custom domain name of the Session Recording server>" PROXYMODE="<set the value to 1 or 2>" PROXYSERVER="<http://proxy.example.com:proxy_port_number>" PROXYSCRIPT="<script address>" PROXYBYPASS="<entries separated by semicolons (;)>" /lv "<log path>" /qn+
```

Where:

- **SRCloudClientService.msi** installs the Session Recording cloud client that enables interaction with Citrix Cloud. Download or copy the .msi file to each Session Recording server you want to connect. To download SRCloudClientService.msi, perform the following steps:
  a) Access the Session Recording service from within the Manage tab of Citrix DaaS (formerly the Citrix Virtual Apps and Desktops service).
  b) Select **Configuration > Server Management**.
  c) On the Server Management page, click the **Server connection guide** hyperlink. The **Server connection guide** page appears.
  d) Download **SRCloudClientService.msi**.
Session Recording service

Note:
The status of a Session Recording server might not change to **Offline** after you stop the cloud client service (CitrixSsRecCloudClientService) on it. For more information, see [Configure Session Recording servers](#).

- **CUSTOMERID** is a *required* parameter. You can find the Citrix Cloud customer ID in the upper right corner of the Citrix Cloud console. You can also find it on the Secure Clients tab (Identity and Access Management > API Access > Secure Clients). For example, see the following screen capture:

![](image1)

- **CLIENTID** is a *required* parameter. The secure client ID is a Universally Unique Identifier (UUID) automatically generated when you create the secure client. Secure clients are used to interact with Citrix Cloud APIs.

- **CLIENTSECRET** is a *required* parameter. The secure client secret shows only once — at the client creation time. After the secure client is created, click **Download** to save both the secure client ID and the secure client secret in a file.

![](image2)
Session Recording service

- **CUSTOMDOMAIN** is an optional parameter. It specifies a custom domain name with an SSL certificate binding that the Session Recording server uses for HTTPS requests. If it is not specified, the FQDN is used by default. To have the custom domain name work properly, complete the following steps on the Session Recording server before installing the Session Recording cloud client:
  a) Open Registry Editor.
  b) Locate the following registry key:
     
     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0`
  c) Right-click **MSV1_0** and create a multi-string value.
  d) Set the value name to **BackConnectionHostNames** and the value data to include your custom domain name.

  **Note:**
  Type your custom domain name on a separate line.
  If the **BackConnectionHostNames** registry value exists as a REG_DWORD type, delete it and recreate a multi-string value.
  e) Restart the machine where you installed the Session Recording server.

- **PROXYMODE** is an optional parameter. Set the value to 1 or 2 to enable a manual or automatic proxy setup for the Session Recording service, respectively. If you leave the parameter unspecified, the default value is 0, which means proxy is disabled.

- **PROXYSERVER** is an optional parameter. However, if you set **PROXYMODE** to 1, this parameter is required. It specifies the proxy server name or IP address and the proxy port number. For example, `http://proxy.example.com:proxy_port_number`.

- **PROXYSCRIPT** is an optional parameter. It specifies the proxy script address, for example, `https://node-cluster143516-swg.ibosscloud.com/95rc2MBacUpwBGIv2/proxy.pac`. If you leave the parameter unspecified, automatic proxy detection takes effect.

- **PROXYBYPASS** is an optional parameter. Use the proxy server except for addresses that start with the entries you specify, separated by semicolons (;).

- **/l*v** is an optional parameter. It specifies verbose logging.

- **/qn** is a required parameter. It specifies a silent install with a user prompt at the end.

After the Session Recording cloud client completes installation, the target server is connected to the Session Recording service. Click **Refresh** on the **Server Management** page to update the list of connected servers. It might take a few minutes for your servers to be detected.
You can manage Session Recording servers by load-balancing them across multiple sites. A site can contain multiple Session Recording servers that connect to the same Session Recording database.

After you connect a Session Recording server to the Session Recording service, the server is automatically grouped to the site connected to the same Session Recording database. If no such site is available, the server becomes a site itself and the site name is the name of the server.

You can perform the following actions for server management:

- Create and edit sites with custom names and descriptions.
- Expand sites to access Session Recording servers in them.
- Drag and drop Session Recording servers to different sites. You can also change a server's site by clicking the **Settings** icon of the server. The **Settings** icon is present only for available servers.
- Configure server settings. For more information, [Configure Session Recording servers](#).

### Configure

**June 15, 2022**

This section provides instructions for you to:

- Configure Session Recording servers
- Configure policies
  - Configure session recording policies
  - Configure event detection policies
  - Configure event response policies
- Configure playback permissions

© 1999–2022 Citrix Systems, Inc. All rights reserved.
To configure settings on a Session Recording server through the Session Recording service, complete the following steps:

1. Select **Configuration > Server Management** from the left navigation of the Session Recording service.

2. Expand a site to locate the target Session Recording server and then click the **Settings** icon. The **Settings** icon is present only for available servers.

3. On the **General** page, enter a description for the Session Recording server and move the server to a different site. You can also drag and drop the Session Recording server to a different site.

4. On the **Recordings** and other pages, configure the server settings listed in the following table:

   Note:
   The status of a Session Recording server might not change to **Offline** after you stop the cloud client service (CitrixSsRecCloudClientService) on it.
<table>
<thead>
<tr>
<th>Server setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File storage location</td>
<td>Specifies where to store recorded session files. You can specify multiple locations to store files in a load-balanced manner.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Lets you select a machine certificate to sign recordings. If no certificate is provided, HTTP is used as the communication protocol. In this case, ensure that: (1) Secure Sockets Layer (SSL) is disabled in Microsoft Internet Information Services (IIS) on each Session Recording server. (2) HTTP is selected as the connection protocol on the Session Recording Agent. For more information, see Use HTTP as the communication protocol.</td>
</tr>
<tr>
<td>File rollover</td>
<td>Lets you specify two thresholds for a rollover: file size and recording duration.</td>
</tr>
<tr>
<td>Notification</td>
<td>Customizes messages sent to end users to notify them that their sessions are being recorded.</td>
</tr>
<tr>
<td>Live session playback</td>
<td>Sets whether you allow users to play ongoing sessions that are being recorded.</td>
</tr>
<tr>
<td>Administrator logging</td>
<td>Sets whether to enable the administrator logging service.</td>
</tr>
<tr>
<td>Mandatory blocking</td>
<td>Sets whether to block changes to policies and server settings if administrator logging fails.</td>
</tr>
<tr>
<td>CEIP</td>
<td>Sets whether to join the Citrix Customer Experience Improvement Program (CEIP).</td>
</tr>
</tbody>
</table>

**Configure policies**

June 16, 2022

The Session Recording service lets you view and configure session recording, event detection, and event response policies for a specific site. Each policy you create or activate applies to all Session Recording servers of a site.
Session Recording service

For more information, see:

- Configure session recording policies
- Configure event detection policies
- Configure event response policies

Configure session recording policies

June 14, 2022

You can activate system-defined recording policies or create and activate your own custom recording policies. System-defined recording policies apply a single rule to entire sessions. Custom recording policies specify which sessions are recorded.

The active recording policy determines which sessions are recorded. Only one recording policy is active at a time.

Note:

After you create or activate a recording policy, the policy applies to all Session Recording servers of the selected site. You can create and activate separate recording policies for different sites.

System-defined recording policies

Session Recording provides the following system-defined recording policies:

- **Do not record.** The default policy. If you do not specify another policy, no sessions are recorded.
• **Record only events (for everyone, with notification).** This policy records only events that your event detection policy specifies. It does not record screens. Users receive recording notifications in advance.

• **Record only events (for everyone, without notification).** This policy records only events that your event detection policy specifies. It does not record screens. Users do not receive recording notifications.

• **Record entire sessions (for everyone, with notification).** This policy records entire sessions (screens and events). Users receive recording notifications in advance.

• **Record entire sessions (for everyone, without notification).** This policy records entire sessions (screens and events). Users do not receive recording notifications.

You can’t modify or delete the system-defined recording policies.

### Create a custom recording policy

You can record sessions of specified users or groups, published applications or desktops, delivery groups or VDA machines, and Citrix Workspace app client IP addresses. To obtain the lists of published applications or desktops and delivery groups or VDA machines, you must have the read permission as a site administrator. Configure the administrator read permission on the Delivery Controller of the site.

For each rule you create, you specify a recording action and a rule scope. The recording action applies to sessions that fall into the rule scope.

For each rule, choose one recording action:

• **Enable session recording with notification.** Records entire sessions (screens and events). Users receive recording notifications in advance.

• **Enable session recording without notification.** Records entire sessions (screens and events). Users do not receive recording notifications.

• **Enable event only session recording with notification.** Records throughout sessions only events that your event detection policy specifies. Does not record screens. Users receive recording notifications in advance.

• **Enable event only session recording without notification.** Records throughout sessions only events that your event detection policy specifies. Does not record screens. Users do not receive recording notifications.

• **Disable session recording.** Does not record sessions of the specified scope.
For each rule, choose at least one of the following items to create the rule scope. When a rule applies, both the “AND” and the “OR” logical operators are used to compute the final action. Generally speaking, the “OR” operator is used within a rule item, and the “AND” operator is used between separate rule items. If the result is true, the Session Recording policy engine takes the rule’s action. Otherwise, it goes to the next rule and repeats the process.

- **Users and user groups.** Creates a list of users and user groups to which the action of the rule applies. Session Recording allows you to use Active Directory groups and white list users.

- **Published applications and desktops.** Creates a list of published applications and desktops to which the action of the rule applies. Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) sites are selected by default. Citrix Virtual Apps and Desktops sites are not supported.

- **Delivery groups and VDA machines.** Creates a list of delivery groups and VDA machines to which the action of the rule applies.

- **IP addresses and IP address ranges.** Creates a list of IP addresses and ranges of IP addresses to which the action of the rule applies. The IP addresses mentioned here are the IP addresses of the Citrix Workspace apps.

When you create more than one rule in a recording policy, some sessions might match the criteria for more than one rule. In these cases, the rule with the highest priority is applied to the sessions.

The recording action of a rule determines its priority:

- Rules with the **Do not record** action have the highest priority.
- Rules with the **Record with notification** action have the second-to-highest priority.
- Rules with the **Record without notification** action have the second-to-lowest priority.
- Rules with the **Enable event only session recording with notification** action have the medium priority.
- Rules with the **Enable event only session recording without notification** action have the low-
Some sessions might not meet any rule in a recording policy. For these sessions, the action of the policy fallback rule applies. The action of the fallback rule is always Do not record. You cannot modify or delete the fallback rule.

Use Active Directory groups

Session Recording allows you to use Active Directory groups when creating policies. Using Active Directory groups instead of individual users simplifies the creation and management of rules and policies. For example, if users in your company’s finance department are contained in an Active Directory group named Finance, you can create a rule that applies to all the group members by selecting the Finance group in the Rules wizard.

White list users

You can create Session Recording policies ensuring that the sessions of some users in your organization are never recorded. This case is called white listing these users. White listing is useful for users who handle privacy-related information or when your organization does not want to record the sessions of a certain class of employees.

For example, if all managers in your company are members of an Active Directory group named Executive, you can ensure that sessions of these users are never recorded by creating a rule that disables session recording for the Executive group. While the policy containing this rule is active, no sessions of members of the Executive group are recorded. The sessions of other members of your organization are sessions recorded based on other rules in the active policy.

Understand rollover behavior

When you activate a policy, the previously active policy remains in effect until the session being recorded ends or the session recording file rolls over. Files roll over when they have reached the maximum size. For more information about the maximum file size for recordings, see Specify file size for recordings.

The following table details what happens when you apply a new recording policy while a session is being recorded and a rollover occurs:
Session Recording service

<table>
<thead>
<tr>
<th>If the previous recording policy was:</th>
<th>And the new recording policy is:</th>
<th>After a rollover, the recording policy will be:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not record</td>
<td>Any other policy</td>
<td>No change. The new policy takes effect only when the user logs on to a new session.</td>
</tr>
<tr>
<td>Record without notification</td>
<td>Do not record</td>
<td>Recording stops.</td>
</tr>
<tr>
<td>Record without notification</td>
<td>Record with notification</td>
<td>Recording continues and a notification message appears.</td>
</tr>
<tr>
<td>Record with notification</td>
<td>Do not record</td>
<td>Recording stops.</td>
</tr>
<tr>
<td>Record with notification</td>
<td>Record without notification</td>
<td>Recording continues. No message appears the next time a user logs on.</td>
</tr>
</tbody>
</table>

Configure event detection policies

June 14, 2022

You can configure event detection policies through the Session Recording service to log target events in recorded sessions. The system-defined event detection policy is **Do not detect**. It's inactive by default. When it's active, no events are logged.

**Note:**

After you create or activate an event detection policy, the policy applies to all Session Recording servers of the selected site. You can create and activate separate event detection policies for different sites.
**Events that can be detected**

Session Recording detects target events and tags those events in recordings for later search and playback. You can search for events of interest from large amounts of recordings and locate those events during playback.

**System-defined events**

Session Recording can detect and log the following system-defined events that occur during recorded sessions:

- Insertion of USB mass storage devices
- Application starts and ends
- App failures
- App installs and uninstalls
- File renaming, creation, deletion, and moving operations within sessions
- File transfers between session hosts (VDAs) and client devices (including mapped client drives and generic redirected mass storage devices)
- Web browsing activities
- Topmost window events
- Clipboard activities
- Windows registry modifications
- User account modifications
- RDP connections
- Performance data (data points related to the recorded session)
- Popup window events

When you create a custom event detection policy, you can add rules to select target events to monitor.
Configure event response policies

June 14, 2022

This policy setting lets you take the following actions in response to logged events in recorded sessions:

- Send email alerts
- Start screen recording immediately
Session Recording service

- Lock session
- Log off session
- Disconnect session

The only system-defined event response policy is **Do not respond**. You can create custom event response policies as needed. Only one event response policy can be active at a time. By default, there is no active event response policy.

**Note:**
After you create or activate an event response policy, the policy applies to all Session Recording servers of the selected site. You can create and activate separate event response policies for different sites.

**System-defined event response policy**

Session Recording provides one system-defined event response policy:

- **Do not respond**. By default, no action is taken in response to logged events in your recordings.

**Create a custom event response policy**

1. Click **Add policy**.
2. Name and describe your new policy.
3. Click **Add Rule**.
4. Name and describe your new rule.

5. Select **Email alert when a session start is detected** or **Trigger response actions when a session event is detected** based on your needs.

6. (Optional) Set email recipients and the email sender properties.

   For an example email alert, see the following screen capture:
Session Recording service

Tip:

Clicking the playback URL opens the playback page of the recorded session in the on-premises web player. Clicking here opens the All recordings page in the on-premises web player.

a) Type email addresses for the alert recipients in the Rules wizard.

b) Configure outgoing email settings in the Session Recording Server Properties.
Session Recording service

**Note:**

If you select more than two options in the **Email title** section, a warning dialog appears, saying that the email subject might be too long. After you select **Allow sending email notifications** and click **Apply**, Session Recording sends an email to verify your email settings. If any setting is incorrect, for example, an incorrect password or port, Session Recording returns an error message with the error details.

![Validation Error]

Your email settings need about five minutes to take effect. To have your email settings take effect immediately or fix the issue that emails are not sent according to the settings, restart the Storage Manager (**CitrixSsRecStorageManager**) service. Also, restart the Storage Manager service if you upgrade to the current release from Version 2006 and earlier.

c) **Edit registry for accessing the on-premises web player.**

To make the playback URLs in your alert emails work as expected, browse to the registry key at `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server` and do the following:

- Set the value data of **LinkHost** to the URL of the domain you use to access the on-premises web player. For example, to access an on-premises web player at `https://example.com/webplayer/##/player/`, set the value data of **LinkHost** to `https://example.com`.

- Add a value, **EmailThreshold**, and set its value data to a number in the range of 1 through 100. The value data determines the maximum number of alert emails that an email sending account sends within a second. This setting helps slow down the number of emails that are being sent and thus reduces the CPU usage. If you leave the value data unspecified or set it to a number out of range, the value data falls back to 25.
Note:

- Your email server might treat an email sending account as a spam bot and thus prevent it from sending emails. Before an account is allowed to send emails, an email client such as Outlook might request you to verify that the account is used by a human user.

- There is a limit for sending emails within a given period. For example, when the daily limit is reached, you cannot send emails until the start of the next day. In this case, ensure that the limit is more than the number of sessions being recorded within the period.

7. (Optional) Click **Configure event triggers and responses** to specify logged events that can trigger the following response actions:

- Send email alerts
- Start screen recording immediately
- Lock session
- Log off session
- Disconnect session

Note:

You must select the event types that the active event detection policy logs.

You can set up to seven event triggers for each policy rule. You can define your event triggers on the **Description** row or leave the row empty. Your defined description of an event trigger is provided in the alert emails if you have **Send email** selected and events of the type are logged. If you have **Start screen recording** selected, dynamic screen recording automatically starts when certain events occur during an event-only recording. Set the time spans for dynamic screen
Session Recording service

recording:

- **Screen recording time span (minutes) after a session event is detected**: You can configure how many minutes you want to record the screen after events are detected. If you leave the value unspecified, screen recording continues until the recorded sessions end.

- **Screen recording time span (seconds) before we detect an event (available only for virtual desktop sessions)**: You can configure how many seconds of the screen recording you want to keep before events are detected. This feature is available only for virtual desktop sessions. The value ranges from 1 to 120. Setting the value to any of 1 through 10 makes the value 10 effective. If you leave the value unspecified, the feature does not take effect. The actual length of the screen recording that Session Recording keeps might be a little longer than your configuration.

For a complete list of supported event types, see the following table.

<table>
<thead>
<tr>
<th>Event type</th>
<th>Dimension</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Start</td>
<td>App name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td></td>
<td>Full command line</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>App End</td>
<td>App name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>Top Most</td>
<td>App name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td></td>
<td>Windows title</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>Web Browsing</td>
<td>URL</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td></td>
<td>Tab title</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td></td>
<td>Browser name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>File Create</td>
<td>Path</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td></td>
<td>File size (MB)</td>
<td>Greater than/Between/Smaller than</td>
</tr>
<tr>
<td>File Rename</td>
<td>Path</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>Event type</td>
<td>Dimension</td>
<td>Option</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>File Move</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source path</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td></td>
<td>Destination path</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td></td>
<td>File size (MB)</td>
<td>Greater than/Between/Smaller than</td>
</tr>
<tr>
<td>File Delete</td>
<td>Path</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td></td>
<td>File size (MB)</td>
<td>Greater than/Between/Smaller than</td>
</tr>
<tr>
<td>CDM USB</td>
<td>Drive letter</td>
<td>Equals</td>
</tr>
<tr>
<td>Generic USB</td>
<td>Device name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>Idle</td>
<td>idle duration (Hrs)</td>
<td>Greater than</td>
</tr>
<tr>
<td>File Transfer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>File source</td>
<td>Equals (&quot;host&quot; or &quot;client&quot;)</td>
</tr>
<tr>
<td></td>
<td>File size (MB)</td>
<td>Greater than</td>
</tr>
<tr>
<td></td>
<td>File name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>Registry Create</td>
<td>Key name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>Registry Delete</td>
<td>Key name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>Registry Set Value</td>
<td>Key name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td></td>
<td>Value name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>Registry Delete Value</td>
<td>Key name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td></td>
<td>Value name</td>
<td>Includes/Equals/Matches</td>
</tr>
</tbody>
</table>
## Session Recording service

<table>
<thead>
<tr>
<th>Event type</th>
<th>Dimension</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry Rename</td>
<td>Key name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>User Account Modification</td>
<td>User name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>Unexpected App Exit</td>
<td>App name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>App Not Responding</td>
<td>App name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>New App Installed</td>
<td>App name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>App Uninstalled</td>
<td>App name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>RDP Connection</td>
<td>IP address</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>Popup Window</td>
<td>Process name</td>
<td>Includes/Matches</td>
</tr>
<tr>
<td></td>
<td>Window content</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td>Performance Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CPU usage (%)</td>
<td>Greater than</td>
</tr>
<tr>
<td></td>
<td>Memory usage (%)</td>
<td>Greater than</td>
</tr>
<tr>
<td></td>
<td>Net send (MB)</td>
<td>Greater than</td>
</tr>
<tr>
<td></td>
<td>Net receive (MB)</td>
<td>Greater than</td>
</tr>
<tr>
<td></td>
<td>RTT (ms)</td>
<td>Greater than</td>
</tr>
<tr>
<td>Clipboard Operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data type</td>
<td>Equals (Text/File/Bitmap)</td>
</tr>
<tr>
<td></td>
<td>Process name</td>
<td>Includes/Equals/Matches</td>
</tr>
<tr>
<td></td>
<td>Content</td>
<td>Includes/Equals/Matches</td>
</tr>
</tbody>
</table>

8. Select and edit the rule scope.
In a way similar to when you create a custom recording policy, you can choose at least one of the following items to create the rule scope:

- **Users and user groups.** Creates a list of users and groups to which the responses of the rule apply.
- **Published applications and desktops.** Creates a list of published applications and desktops to which the responses of the rule apply.
- **Delivery groups and VDA machines.** Creates a list of delivery groups and VDA machines to which the responses of the rule apply.
- **IP addresses and IP address ranges.** Creates a list of IP addresses and ranges of IP addresses to which the responses of the rule apply. The IP addresses mentioned here are the IP addresses of the Citrix Workspace apps.

**Note:**
When a session or an event meets more than one rule in a single event response policy, the oldest rule takes effect.

9. Follow the wizard to complete the configuration.

10. Activate the new event response policy.

### Configure playback permissions

**June 10, 2022**

**Note:**
For video playback, make sure port 9191 is open on your end users’ devices and networks.

By default, all Citrix Cloud administrators with the Session Recording role have permission to play all recordings. You can limit playback permissions so that Session Recording read-only administrators can play only specific recordings on a target Session Recording server.

For an overview of the Citrix Cloud administrators and their playback permissions, see the following table:

<table>
<thead>
<tr>
<th>Citrix Cloud administrator</th>
<th>Playback permission</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>With full access</td>
<td>Can play all recordings</td>
<td>Shows as a full admin on the Playback Permissions page of the Session Recording service</td>
</tr>
</tbody>
</table>

© 1999–2022 Citrix Systems, Inc. All rights reserved.
### Session Recording service

<table>
<thead>
<tr>
<th>Citrix Cloud administrator</th>
<th>Playback permission</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>With the <strong>Cloud Administrator, All</strong> role</td>
<td>Can play all recordings</td>
<td>Shows as a full admin on the <strong>Playback Permissions</strong> page of the Session Recording service</td>
</tr>
<tr>
<td>With the <strong>Session Recording-FullAdmin, All</strong> role</td>
<td>Can play all recordings</td>
<td>Shows as a full admin on the <strong>Playback Permissions</strong> page of the Session Recording service</td>
</tr>
<tr>
<td>With the <strong>Session Recording-ReadOnlyAdmin, All</strong> role</td>
<td>Can play all recordings by default, or can play only recordings that originate from users and groups, published applications and desktops, and delivery groups and VDAs you specify.</td>
<td>Shows as a full admin on the <strong>Playback Permissions</strong> page of the Session Recording service by default, or shows as a read-only admin on the <strong>Playback Permissions</strong> page of the Session Recording service when you specify the scope.</td>
</tr>
</tbody>
</table>

To limit the playback permission of a Session Recording read-only administrator, complete the following steps:

1. Select a target Session Recording server.
2. Select **Configuration > Playback Permissions** from the left navigation of the Session Recording service.

All Citrix Cloud administrators who have the role of Session Recording are listed on the **Playback Permissions** page of the Session Recording service.

The **Playback Permissions** page is not visible to Session Recording read-only administrators.
3. Target an administrator on the **Playback Permissions** page.

4. Go to the **Identity and Access Management > Administrators** tab of the Citrix Cloud console.

5. Locate the target administrator, click the ellipsis button, and select **Edit** access.

6. Select **Custom access**.
7. Click the angle bracket to expand all roles.

8. Clear the check marks next to **Cloud Administrator, All** and **Session Recording-FullAdmin, All**. Select the check mark next to **Session Recording-ReadOnlyAdmin, All**.

9. Click **Save**.

10. Return to and refresh the **Playback Permissions** page of the Session Recording service. The Citrix Cloud administrator you edited shows as a Session Recording read-only administrator.
Tip:
An administrator can have full permission to play all recordings, limited permission to play only specific recordings, or no permission to play any recordings.

Unless otherwise specified, a Session Recording read-only administrator has full permission to play all recordings.

11. Click the **Edit** icon in the row of the administrator.

12. On the **Edit Playback Permission** page, specify the scope of recordings that the administrator can play.

Note:
Playback permissions that you set might not show on the **Playback Permissions** page. The issue occurs after upgrading to Session Recording 2204. As a workaround, run the following script in
Session Recording service

SQL Server Management Studio (SSMS) that corresponds to your Session Recording database:

```sql
ALTER procedure [dbo].[EnumPlayerUserDeliveryGroupPoliciesOnCloud]
as
begin
set nocount on
select 3 as RoleType,
a.ID as RoleAccountID,
h.principleName as PrincipleName,
a.IsEnabled as IsEnabled,
e.name as PolicyType,
d.DeliveryGroupID as AccountMemberAccountID,
g.Name as AccountMemberName
from PlayerUserCloudAccountRoleConfigure a,
PlayerUserPolicyConfigSetMember b,
PlayerUserPolicyDeliveryGroupSetMember d,
PlayerUserPolicyType e,
DeliveryGroup g,
PlayerUserCloudAccount h
where e.id=5
and b.PlayerUserPolicyTypeID = e.ID
and a.PlayerUserPolicyConfigSetID = b.
    PlayerUserPolicyConfigSetID
and b.PolicySetID = d.PlayerUserPolicyDeliveryGroupSetID
and g.ID=d.DeliveryGroupID
and h.ID=a.CloudAccountID
end
```

Configure utilities

June 14, 2022

You can set your preferences for Session Recording. Currently, you can set the cache size you want the player to use for playback.
Session Recording service

To set the cache size, select **Configuration > Utility Settings** from the left navigation and then drag the slider.

![](image)

**View recordings**

**June 20, 2022**

If sessions are recorded with the live playback feature enabled, you can view sessions that are in progress, with a delay of 1-2 seconds.

Sessions that have a longer duration or larger file size than the limits configured appear in more than one session file.

**Note:**

Grant users the right to access the recorded sessions of VDAs.

**Search for, archive, and delete recordings**

**July 26, 2022**

**Search for recordings**

On the **All Recordings** and **Archived** pages, you can search for recordings by specifying:

- A specific time period. The options include **Today, Last 7 days, Last 30 days, Last 90 days, All time**, and **Custom**.
- One or more sites.
Session Recording service

- Filters include Host name, Client name, User name, Application, Client IP address, Event text, Event type, and duration.
- Advanced search criteria.

You can also specify Columns to display.

Show all recordings of a session

You can select a recording and click the Follow up button to show all recordings of the recorded session.
Archive recordings

**Note:**

Only Citrix Cloud administrators of the following roles can archive recordings:

- Full access
- The Cloud Administrator, All role
- The Session Recording-FullAdmin, All role

If archiving a recording does not complete successfully, the recording is not available for playback or deletion for the first 24 hours following the archiving operation.

A single session can produce multiple recordings. Only recordings of sessions recorded in their entirety can be archived.

You can select one or more recordings to archive at a time. When archiving recordings, you can choose to move the recording files to a different location from the one where they were originally stored.

- If you move the recordings files to a different location on the same Session Recording server, grant permissions for the System and Network Service accounts to read and write the archived recordings.
- If you move the recording files to a UNC path, grant permissions for all computer accounts in your site to read and write the archived recordings.
**Session Recording service**

Delete recordings

*Note:*

Only Citrix Cloud administrators of the following roles can delete recordings:

- Full access
- The **Cloud Administrator, All** role
- The **Session Recording-FullAdmin, All** role

A single session can produce multiple recordings. Only recordings of sessions recorded in their entirety can be deleted.

You can select one or more recordings to delete at a time. When deleting recordings, you can choose to also delete the recording files along with the database records.
Session Recording service

Open and play recordings

July 25, 2022

You can play live and completed recordings. On the All Recordings and Archived pages, each recording has a play button on the right side, next to the Duration item.

Tip:
Use a machine with GPU for better playback experience on it.

Click the play button. The playback page appears. Playback starts after memory caching.

Tip:
- Clicking the session progress time lets you switch to the absolute date and time the session was recorded.
- For an event-only recording, the play icon in the upper left corner is unavailable.

For a description of the player controls, see the following table:

<table>
<thead>
<tr>
<th>Player Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Play button</td>
<td>Plays the selected recording file.</td>
</tr>
<tr>
<td>Progress bar</td>
<td>You can drag the progress bar during playback. Idle periods of recorded sessions are highlighted during playback.</td>
</tr>
</tbody>
</table>
Session Recording service

<table>
<thead>
<tr>
<th>Player Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current position of recording playback</td>
<td>Indicates the current position of the recording playback and the total recording duration. The time format is HH:MM:SS.</td>
</tr>
<tr>
<td>Comments</td>
<td>Lets you click and leave a comment about the recording being played.</td>
</tr>
<tr>
<td>Show stats</td>
<td>Shows the overlay that features data points related to the recorded session.</td>
</tr>
<tr>
<td>Hide stats</td>
<td>Hides the session data overlay.</td>
</tr>
<tr>
<td>Playback speed</td>
<td>Indicates the current speed of playback. Click the icon to switch between options including X0.5, X1, X2, and X4.</td>
</tr>
<tr>
<td>Full screen</td>
<td>Displays the playback in full screen.</td>
</tr>
<tr>
<td>Exit full screen button</td>
<td>Displays the playback within the webpage.</td>
</tr>
</tbody>
</table>

In the right pane of the playback page, the **Events** and **Comments** filters, quick search box, and some recording data are available:

- The date and time on the player machine. In this example, **JUN 13, 2022 and 19:11:02**.
- The duration of the recording in playback. In this example, **00:03:04**.
- The number of events in the recording. In this example, **18 EVENTS**.
- The name of the user whose session was recorded.
Session Recording service

- The host name of the VDA where the recorded session was hosted.
- The name of the client device where the session was running.
- Options for sorting search results: Select **All**, **Events**, or **Comments** to sort search results.
- Event filters. You can select more than one filter to search for events in the current recording.

Click the icon to expand displays of events. For example:

- Event list. Clicking an event on the list takes you to the position of the event in the recording.
- Quick search box. The **search events** quick search box helps to quickly narrow down a list of events in the current recording.

**Highlight idle periods**

June 13, 2022

Session Recording can record idle events and highlight idle periods in the player.

To customize the idle event feature, set the following registry keys at `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SessionEvents`.

<table>
<thead>
<tr>
<th>Registry key</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisableIdleEvent</td>
<td>0</td>
<td>To disable the idle event feature, set the value to 1. To enable the idle event feature, set the value to 0.</td>
</tr>
</tbody>
</table>
### Session Recording service

<table>
<thead>
<tr>
<th>Registry key</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdleEventThrottle</td>
<td>30 seconds</td>
<td>If there is no user activity (including graphics changes and keyboard/mouse inputs) longer than the time threshold set by the registry key, an idle event is recorded. The idle period is highlighted when the recorded session plays back on the Session Recording web player.</td>
</tr>
<tr>
<td>IdleEventActiveThrottle</td>
<td>2 seconds</td>
<td>Only a specified number of graphics changes within a specified amount of time qualify as user activities. By default, at least three packets within 2 seconds can qualify as user activities.</td>
</tr>
<tr>
<td>IdleEventActivePktNumThrottle</td>
<td>3 packets</td>
<td>Only a specified number of graphics changes within a specified amount of time qualify as user activities. By default, at least three packets within 2 seconds can qualify as user activities.</td>
</tr>
<tr>
<td>IdleEventActivePktSizeThrottle</td>
<td>300 bytes</td>
<td>Graphics packets smaller than the key value are ignored and the relevant time duration is regarded as idle.</td>
</tr>
</tbody>
</table>

### Use events and comments

June 13, 2022

In the right pane of the playback page, the **Events** and **Comments** filters are available. You can use events and comments to help you navigate through recorded sessions in the web player.
Comment on recordings

When a recorded session is being played, you can click the Comments player control to leave comments and set comment severities. Severities include Normal, Medium, and Severe. Severe and Medium comments are indicated with red and orange dots, respectively. During session playback, you can view all comments about a recording. To delete a comment that you left, refresh your webpage, expand the comment, and then click Delete.

Clicking a comment lets you jump to the location where the comment was given. You can view all your comments on the My comments page.
**Not**

To make the comment feature work as expected, clear the **WebDAV Publishing** check box in the **Add Roles and Features** wizard of Server Manager on the Session Recording Server.
View graphical event statistics for each recording

June 13, 2022

Event data visualization is available for each recording. It provides graphical event statistics for you to quickly comprehend the events inserted in recordings.

To view graphical event statistics, complete the following steps:

1. Open and play a recording.
2. In the upper left corner of the playback page, click the statistics icon.
3. Switch between the **Screen time**, **File transfers**, **Commands**, and **Events** tabs to view statistics from different perspectives.

- **Screen time**
  
  The **Screen time** tab lets you know the cumulative time an application window is in focus (active window).

  ![Screen time screenshot]

  There is a horizontal time bar next to each application. Click the bar to view the start time and duration each time an application becomes and stays in focus, respectively. You can narrow down your search range by specifying a duration range other than the default **All**.
Session Recordingservice

For example:

- File transfers

The File transfers tab provides graphical statistics about bidirectional file transfers between the VDA hosting the recorded session and the client device where the session runs. You can customize the visualization by using the following settings:

  - Time granularity: Per 1 minute, Per 10 minutes, Per hour
  - File transfer destination: All transfers, Transfer from host to client, Transfer from client to host
  - Number or size (Bytes or MB) of transferred files

The X axis represents the absolute time in the 24-hour system.
Session Recording service

• Commands

The **Commands** tab shows CMD and PowerShell commands that are run during the recorded session. You can customize the data display by typing your custom search in **Custom search** or selecting a saved search from **Saved search**. The “OR” logical operator is used to compute the final action.

• Events
The **Events** tab shows the proportions and numbers of all types of events in the recorded session.

### View data points related to each recorded session

**June 13, 2022**

During playback, you can click the **Show stats** control to view, on an overlay, the following data points related to the recorded session:

- Round trip time
- Network (send)
- Network (receive)
- CPU usage
- Memory usage
Session Recording service

Note:

- Session Recording collects round trip time every 15 seconds and the rest of the data points every second.
- Theoretically, Session Recording refreshes data on round trip times every five seconds. However, round trip time data actually refreshes every 15 seconds because of the collection cycle.
- Session recording refreshes the rest of the data points every 5 seconds and presents their average values on the overlay.

The overlay is semitransparent. You can relocate and hide it.

- To relocate the overlay, hover your mouse over the eight dots and then do a drag and drop.
- To hide the overlay, click **Hide stats**.

You can enable the overlay by selecting **Log performance data** when creating your event detection policy. For more information, see Configure event detection policies.

Query administrator logging data

May 26, 2022

Using Session Recording server 2204 or later, you can query administrator logging data through the Session Recording service.
Note:

An administrator with **Full** access can view administrator logging. To grant the **Full** access permission, go to **Identity and Access Management** in Citrix Cloud.

If you select a Session Recording server earlier than version 2204, the following banner appears, and no data is available.

Logging data overview

Administrator logging data consists of two parts - configuration logging and recording reason logging. You can select more than one Session Recording server to view logs.
Hover over the three dots (ellipsis) to view details about each log.

---

**Configuration logging**

This part logs the following administrator activities:

- **Policy document change** - Changes to policies on the Session Recording policy console or Citrix Director
- **Server configuration change** - Changes in Session Recording Server Properties
- **Recording file playback** - Playback of recorded sessions
• **Log reading** - Unauthorized attempts to access the administrator logging data

You can use the **Logging time, Category, Action**, and **Action taken by** filters to narrow your search. The “AND” operator is used between the filters to compute the search action.

When more than one filter is applied, the **Clear all** button becomes available. You can click the button to clear all filters.

To log administrator activities, complete the following steps to enable administrator logging on your Session Recording servers.

1. Select **Configuration > Server Settings** from the left navigation of the Session Recording service.
Session Recording service

2. Click the host name of your target Session Recording server on the list.

3. On the **Server Settings** page, select **Logging** from the left navigation and then select **Enable administrator logging**.

   If you select **Enable mandatory blocking**, the following activities are blocked if logging fails. A system event is also logged with an Event ID 6001:
   - Changes to recording policies on the Session Recording Policy Console or Citrix Director
   - Changes in Session Recording Server Properties

   The mandatory blocking setting does not impact the recording of sessions.

   **Tip:**
   You can enable administrator logging both through the Session Recording service and through Session Recording Server Properties. For information on how to enable administrator logging through Session Recording Server Properties, see [Disable or enable administrator logging](#).

   You can also **configure an administrator logging service account** to enhance security.

**Recording reason logging**

This part logs which policies have triggered recordings.

To enable the feature, enable both administrator logging and recording reason logging on your Session Recording servers. If **Enable administrator logging** is not selected, enabling recording reason logging does not take effect.

For information on how to enable the recording reason logging, see [Disable or enable the recording reason logging](#).
Customer data management

April 1, 2022

Data collection

The Session Recording service collects three types of customer data to Citrix Cloud:

- Logs collected from the Session Recording service console and from the Session Recording infrastructure services
- The Session Recording service configurations and policies defined by administrators
- Statistics associated with Session Recording servers

Data control and storage

Log files. All log files are sent to Splunk.

Session Recording service configurations and policies. All the configurations and policies you configure are saved and stored in the SQL Server database of your on-premises deployment.

Statistics associated with Session Recording servers. All statistics associated with Session Recording servers are saved and stored in the back-end Azure database. They are not accessible to customers.

Data retention

The customer data associated with the Session Recording service is retained by Citrix. Retention periods differ for different types of data:

- Log files are retained for 90 days by default and deleted thereafter. Retaining those log files for a custom time period is not supported.
- Statistics associated with Session Recording servers are retained for 90 days by default and deleted thereafter.