



Session Recording service

Contents

Session Recording service	3
What's new	5
Third party notices	17
Known issues	18
Get started	19
Plan your deployment	19
Connect existing Session Recording servers to the cloud	22
Install Session Recording servers from within the cloud	30
Deploy Session Recording resources to a cloud subscription	44
Schedule cloud client upgrades	112
Configure	116
Site and server settings	117
Configure policies	123
Configure session recording policies	124
Configure event detection policies	132
Configure event response policies	135
Playback permissions	151
Administrator permissions	158
Configure preferences	161
View recordings	162
Search for recordings	162
Place access restrictions on recordings	164
Open and play recordings	167

Share recordings as links	170
Specify players for a site	178
Highlight idle periods	181
Use events and comments	182
View graphical event statistics	184
View performance data points	188
Manage recordings	189
Manage selected recordings	190
Manage recordings on schedule	192
Administrator logging	194
Management dashboard	198
Activity feed	207
Notifications	210
Customer data management	215
Best practices	216
Integrate with Citrix HDX plus for Windows 365 in a Session Recording deployment	217
Troubleshoot	238
Server troubleshooting from the cloud	238
Servers not seen in the cloud	241

Session Recording service

February 23, 2024

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.

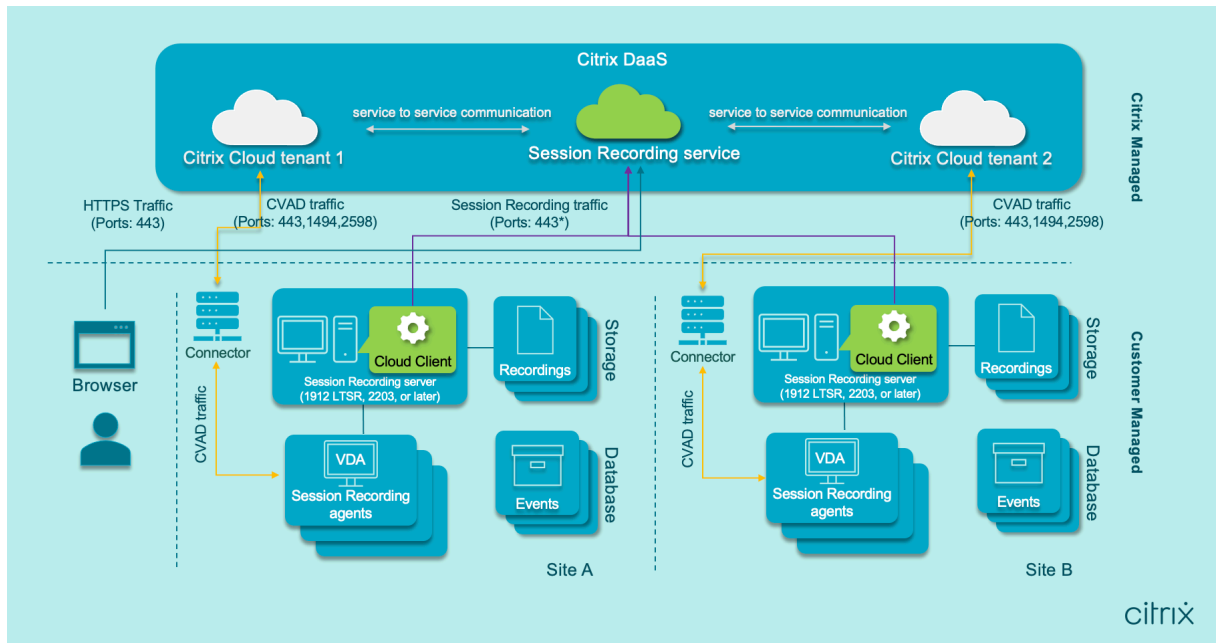
Overview

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.

The Session Recording service is a management platform that provides comprehensive automation, faster troubleshooting, and informative insights. 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.

Session Recording service



Note:

With versions 7.40.13020.11 and later of the cloud client, you need to only open a single port (TCP port 443) for communication. With a cloud client earlier than version 7.40.13020.11, allow the outbound ports 80, 443, 8088, and 9090–9094 for session recording traffic. For more information, see [Ports](#).

Video about the Session Recording service:



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
- Install Session Recording servers from within the cloud
- Query and play recordings from the connected Session Recording servers
- Configure settings on the connected Session Recording servers
- Configure session recording, event detection, and event response policies for a specific site
- Configure playback permissions
- Place and remove access restrictions on recordings
- Archive and delete recordings automatically on a regular schedule
- View event visualization reports and leave comments about recordings
- View data points related to each recorded session
- Gain insights into your system through the Session Recording management dashboard

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](#).

What's new

April 26, 2024

A goal of Citrix is to deliver new features and product updates to Session Recording service customers when they're 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.

April 2024

Azure Resource Manager template (ARM template) support for simplified deployment in Azure

You can now create an Azure Resource Manager template (ARM template) to deploy Session Recording resources in Azure. The ARM template is a JavaScript Object Notation (JSON) file that contains how and which resources you want to deploy. For more information, see [Create and deploy a site through an ARM template](#).

Pure Azure Active Directory (Azure AD) deployment can now be achieved through simplified deployment

Simplified deployment refers to creating and deploying a site through a host connection or an ARM template. While doing simplified deployment, you now have an option to join the Session Recording servers you are about to deploy to an Azure AD domain where your VDAs reside. For more information, see [Deploy Session Recording resources to a cloud subscription](#).

Community-driven event trigger templates

To help you quickly find a template that fits your business need, Cloud Software Group has created a community for all full admins of the Session Recording service to contribute towards it. You can contribute to the community by publishing templates of your organization for other customers to access for free. Cloud Software Group has also built a resource library to accommodate all event trigger templates, both from your organization and from the other community members including Cloud Software Group itself.

Note:

See the [End User Agreement](#) before submitting a template.

For more information, see [Create a custom event response policy](#).

Recording success rates visualized on the cloud

You can now see a new widget showing the recording success rates for the current site on the upper right corner of the Session Recording [management dashboard](#). You can see both the latest recording success rate and the recording success rates for the past 12 hours.

To facilitate identifying issues, recording success rates below 100% are displayed as an orange dot in comparison to 100% success rates that are displayed as a green dot. You can hover over an orange dot and click the link in the hint to jump to the corresponding event logged on the [Activity Feed](#) page where you can:

- view the event details including those sessions which failed to record.
- subscribe to [Email notifications](#) to get notified when a recording success rate is below 100%.

Note:

This feature is available with the cloud client versions 7.42.15010.4 and later. To use this feature, make sure that only one site has available servers and this feature is enabled on the dashboard settings page of that site.

For more information, see [Management dashboard](#).

Fixes

- Attempts to add or modify a policy might fail if the length of users or user groups specified as the applicable scope exceeds 16 characters. [SRT-12247]
- Attempts to [install a Session Recording server from within the cloud](#) might fail. The issue occurs when you connect the Session Recording server to a cloud database but the database password you provide contains a double quote (“). [SRT-12119]

March 2024**Azure Active Directory (AD) support (preview)**

You can now install the Session Recording server and agent on an Azure AD joined machine and enable Azure AD support for them. Later when you configure various policies and playback permissions from the cloud, you can specify Azure AD users and groups who launch sessions from Azure AD joined machines.

For information about installing Session Recording, see [Install, upgrade, and uninstall](#).

For information about configuring policies and playback permissions from the cloud, see [Configure session recording policies](#) and [Playback permissions](#).

Note:

Azure AD support is available with Session Recording version 2402 and later.

January 2024**Storage consumption forecast**

A storage consumption forecast for the next 7 days can be generated based on sufficient historical consumption data of approximately one month. This feature allows you to predict resource usage

and take precautions in advance. For more information, see the [Management dashboard](#) article.

Support for sharing recordings as restricted and unrestricted links from the cloud player

You can now share recordings as restricted and unrestricted links from the cloud player. Other users can use the links to access the shared recordings directly, which obliterates the need to search among many recordings. If you share a recording as a restricted link, only users who already have [playback permission](#) can view the recording using the link. If you share a recording as an unrestricted link, anyone in your AD domain can view the recording using the link.

For unrestricted recording sharing, you can further:

- Specify whether to issue email notifications to specific recipients when an unrestricted recording link is generated. For more information, see [Notifications](#).
- View the events related to unrestricted recording sharing on the Events tab of the [activity feed](#).

To share recordings as links and manage unrestricted links, you must have full access to the Session Recording service. It means that you must be a Citrix Cloud administrator assigned any of the following permissions:

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

For more information, see [Share recordings as links](#) and [Types of Session Recording administrators](#).

October 2023

Simplified Session Recording deployment to Microsoft Azure is now generally available

You can create a site to deploy the Session Recording resources to your Azure subscription from within the Session Recording service. The feature is now generally available and enhanced to let you:

- Add resources including servers and storage to an existing site deployed on Azure.
- Change the IP addresses that are allowed to access the load balancer.

For more information, see [Deploy Session Recording resources to a cloud subscription](#).

Introduction of event trigger templates

By event triggers in event response policies, you can specify actions in response to different events including session starts and the events detected in recorded sessions. Starting with this release, you'

re provided with event trigger templates for direct use or customization. For more information, see [Configure event response policies](#).

Support for single-port communication

With versions 7.40.13020.11 and later of the cloud client, you need to only open a single port (TCP port 443) for communication.

Fixes

- Host connections can't be created successfully until you've onboarded at least one Session Recording server to the Session Recording service. [SRT-11065]
- Viewing the Session Recording management dashboard causes high CPU utilization on the database machine. [SRT-11190]
- Custom policies aren't available for a site containing the Session Recording server 1912. [SRT-11334]

September 2023

Administrative access to the Session Recording service is enabled for Azure Active Directory (AD) users and groups

For more information, see [Add administrators from Azure AD](#).

Audio recording for non-optimized HDX audio (preview)

You can now enable audio recording for non-optimized HDX audio when configuring session recording policies. The audio that is handled on the VDA and delivered to/from the client where the Citrix Workspace app is installed is referred to as non-optimized HDX audio. Unlike non-optimized HDX audio, optimized HDX audio has its processing offloaded to the client, as seen in the Browser Content Redirection (BCR) and Optimization for Microsoft Teams scenarios.

For information about enabling audio recording, see [Configure session recording policies](#).

Note:

This feature is available with Session Recording version 2308 and later.

Lossy screen recording

Lossy screen recording lets you adjust compression options to reduce the size of recording files and to accelerate navigating recorded sessions during playback.

You can enable lossy screen recording in any of the following ways:

- Activate a system-defined session recording policy that has lossy screen recording enabled.
- Create and activate a custom session recording policy, and make sure to select **Enable lossy screen recording** when creating the custom policy.
- Select **Enable lossy screen recording** when configuring an event response policy. When a monitored event is detected later, lossy screen recording is triggered.

After you enable lossy screen recording, you can adjust compression options through the **Lossy Screen** tab of Session Recording Agent Properties.

For more information, see:

- [Configure session recording policies](#)
- [Configure event response policies](#)
- [Enable or disable lossy screen recording](#)

Note:

This feature is available with Session Recording version 2308 and later.

Fast seeking through ICA screen recording

You can now enable fast seeking through ICA screen recording by configuring how often an I-Frame is generated. This feature significantly improves the playback seeking experience.

For more information, see [Configure preferences](#) and [Enable fast seeking](#).

Note:

This feature is available with Session Recording version 2308 and later.

Fixes

- Session recording and event response policies configured from the cloud don't take effect. This issue occurs when you use Session Recording server 2305 or earlier. [SRT-10813]

July 2023

Simplified Session Recording deployment to Microsoft Azure (preview)

You can now deploy the following Session Recording resources to your Azure subscription from within the Session Recording service: the Session Recording servers, databases, storage, and load balancer. You can also obtain recommended VM and storage configurations, predict costs, and view the actual costs for using Azure from within the Session Recording service.

For more information, see [Deploy Session Recording resources to a cloud subscription \(preview\)](#).

Remove Session Recording servers from the cloud

You can now remove servers with the **Offline**, **Uninstalled**, and **Installation Failed** states from the cloud to display only the desired Session Recording servers.

For more information, see [Server removals](#).

Troubleshoot Session Recording servers from the cloud

You can perform a few troubleshooting actions from the cloud for the Session Recording servers connected to the Session Recording service.

For more information, see [Server troubleshooting from the cloud](#).

Specify players for a site

You can now specify either the cloud player, on-premises players, or both to play the recordings of a site. By default, both the cloud player and on-premises players are selected.

This feature is available with Session Recording server 2308 and later.

For more information, see [Specify players for a site](#).

Fixes

- Attempts to send storage consumption and session statistics to the Session Recording management dashboard always fail for Session Recording servers with a French operating system. [SRT-10219]

April 2023

A daemon introduced for the cloud client

This release introduces a daemon to keep the Session Recording cloud client running and to automatically repair it when it runs abnormally. The daemon is available in cloud client versions 7.38.10030.16 and later.

Activity feed

As a supplement to the [Session Recording management dashboard](#), the Session Recording service introduces an activity feed to improve data visibility and data visualization.

The activity feed gives you information about the events and tasks that happened in the past.

For more information, see the [Activity feed](#) article.

Email notifications

To get notified about specific events and tasks through email, you can now subscribe to email notifications.

You can subscribe to be notified about:

- **Resource usage alerts:** When resource usage thresholds are exceeded
- **Server status changes:** When the status of a Session Recording server changes
- **Storage maintenance results:** A digest of the results of automated tasks for archiving and deleting recordings

For more information, see [Email notifications](#).

Fixes

- Automated tasks for archiving and deleting recordings are terminated if the target sessions are still live. [SRT-9832]
- If you edit more than one rule of a policy in the Session Recording service, your edits might not take effect and a “**Policy adding failed**” error is logged in your web browser console. [SRT-9754]
- Attempts to edit policy rules that have a Japanese name fail. [SRT-9675]

February 2023

Support for scheduling cloud client upgrades

Previously, the Session Recording cloud client was automatically upgraded each time a new release was issued. Starting with this release, you can upgrade the Session Recording cloud client immediately or schedule automatic upgrades. For more information, see [Schedule cloud client upgrades](#).

Cloud client enhancement

We've enhanced the Session Recording cloud client in version 7.37.9010.3. This version of the cloud client handles REST API requests and file streaming requests directly, which brings the following benefits and changes:

- Previously, to make a Session Recording server work properly in the cloud, you must install an SSL certificate on it and add a certificate binding in IIS. Versions 7.37.9010.3 and later of the cloud client don't depend on the local certificates on Session Recording servers and don't support the **CUSTOMDOMAIN** parameter.

For more information, see [Connect existing Session Recording servers to the cloud](#) or [Install Session Recording servers from within the cloud](#).

- Versions 7.37.9010.3 and later of the cloud client obliterate the need to configure the web streaming service in IIS if you want to use the cloud player only.
- We've removed the web configuration file (**Web.config**) from **<Session Recording server installation path>/WebSocketServer**, and use the registry instead for setting the transport packet size. You can locate the registry key at **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SessionRecording**. For more information, see [Increase the transport packet size](#).
- The cloud client enhancement increases playback speed and creates a greater playback experience.

December 2022

Server installation from within the cloud

Previously, you could connect only existing Session Recording servers to the Session Recording service. For more information, see [Connect existing Session Recording servers to the cloud](#).

Starting with this release, you can connect any machine to the Session Recording service and then install the Session Recording server component on it from within the cloud. After installation completes successfully, the machine becomes a Session Recording server that is connected to the Session Recording service. To do so:

1. Prepare a machine and install the Session Recording cloud client on it.
The machine is automatically connected to the Session Recording service, appearing in the **Unallocated servers** list on the **Server Management** page.
2. Verify that the machine is in the **Ready to install** status, and then click the installation icon. The installation wizard appears.
3. Follow the wizard to install the Session Recording server component on the machine.

This new feature obliterates the need to download the Citrix Virtual Apps and Desktops installer or the SessionRecordingAdministrationx64.msi file. It also performs domain joining and certificate binding checks to prevent issues that might keep Session Recording servers from functioning after being connected.

For more information, see [Install Session Recording servers from within the cloud](#).

Improved experience in server onboarding

To connect a Session Recording server to the cloud, you must install the cloud client on it. Previously, you had to manually enter a command to do that.

This release introduces a **Generate command** wizard where you can generate a command by providing the necessary information. The wizard also provides important reminders such as for certificate binding. To open the wizard, click **Generate command** on the **Server connection guide** page or click **Continue configuration** on the Session Recording service **Welcome** page and then click **Generate command**.

For more information, see [Connect existing Session Recording servers to the cloud](#) and [Install Session Recording servers from within the cloud](#).

Playback justification logging

This release introduces playback justification logging and creates a **Playback Logging** page to aggregate all playback logs. With playback justification logging enabled, each time a user plays a recording, a dialog box appears, asking the user to enter a justification for playback. For more information, see [Playback logging](#).

November 2022

Session Recording management dashboard

The Session Recording service introduces a comprehensive management dashboard that helps you gain insights into your system. The dashboard lets you monitor various aspects of your system, including:

- Server status
- Storage consumption
- Session statistics
- Client device information

For more information, see the [Session Recording management dashboard](#).

Trace collection from cloud clients

Citrix collects traces from the cloud clients installed on on-premises Session Recording servers and uses the traces for troubleshooting.

September 2022

Support for automatically archiving and deleting recordings on a regular basis

In addition to archiving and deleting recordings manually, you can now schedule site-level tasks to automatically archive and delete recordings **on a regular basis**. For more information, see [Manage recordings](#).

Recording access control

You can now restrict access to selected recordings from within the Session Recording service. In addition to [playback permissions](#), this feature provides more granular access control.

Citrix Cloud administrators assigned any of the following access permissions are allowed to place access restrictions on recordings:

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

Restricted recordings aren't accessible to Session Recording read-only administrators, that is, Citrix Cloud administrators assigned **only** the **Session Recording-ReadOnlyAdmin, All** role. Session Recording read-only administrators do not have permission to access the **Restricted** page or remove access restrictions on the page. For more information, see [Place access restrictions on recordings](#).

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 [Manage recordings](#).

June 2022

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

In addition to the US and EU regions, the Session Recording service is now also 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 existing Session Recording servers to the cloud](#), [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 existing Session Recording servers to the cloud](#).

Support for configuring additional event response actions from the cloud

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

In addition to the US region, the Session Recording service is now also 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

July 18, 2023

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

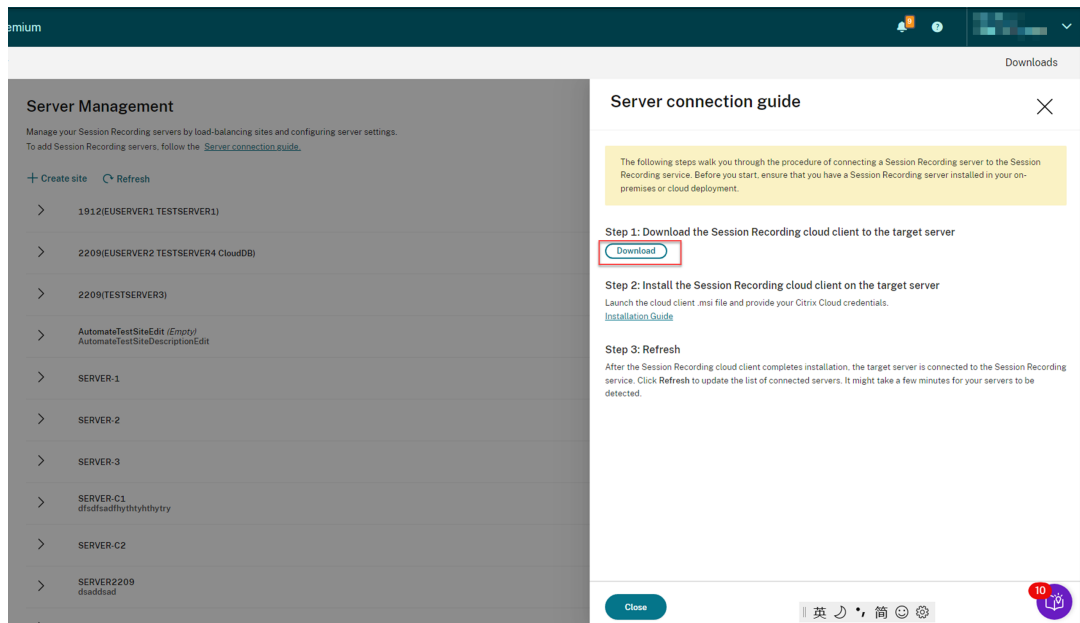
[The Session Recording service third party notices](#)

Known issues

April 26, 2024

- A Session Recording server might persist in maintenance status. The issue occurs when the Session Recording cloud client that you installed on the Session Recording server didn't update with the new release. As a workaround, complete the following steps:

1. Remove the cloud client package (`SRCloudClientService.msi`) from the Session Recording server.
2. Download a new cloud client package to the Session Recording server. To download the package, navigate to **Configuration > Server Management > Server connection guide** and then click **Download**.



3. Install the Session Recording cloud client by using a command similar to the following:

```
1 msixexec /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 (;)>" /l*v "<log path>" /qn+
2 <!--NeedCopy-->
```

Note:

Versions 7.37.9010.3 and later of the cloud client don't depend on the local certificates on Session Recording servers and don't support the **CUSTOMDOMAIN** parameter.

For information on the command variables, see [Connect existing Session Recording servers to the cloud](#).

Get started

June 20, 2023

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 existing Session Recording servers to the clouds](#)
- [Install Session Recording servers from within the cloud](#)
- [Schedule cloud client upgrades](#)

Plan your deployment

May 24, 2024

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 the Session Recording cloud client)

The cloud player requires access to the following address over WebSocket:

- **wss://*.apps.cloud.com** (provides access to play back recorded session files)

Ports

With versions 7.40.13020.11 and later of the cloud client, you need to only open a single port (TCP port 443) for communication:

Source	Destination	Type	Port	Details
Session Recording cloud client on each Session Recording server	Citrix Cloud and Microsoft Azure	TCP (HTTPS, Websocket)	443	Communication with Citrix Cloud and Microsoft Azure.

Cloud clients earlier than version 7.40.13020.11 require you to open more ports:

Source	Destination	Type	Port	Details
Session Recording cloud client on each Session Recording server	Citrix Cloud and Microsoft Azure	TCP (HTTPS)	80, 443	Communication with Citrix Cloud and Microsoft Azure.
Session Recording cloud client on each Session Recording server	Session Recording service	TCP (Websocket)	8088, 9090–9094	WebSocket connection between the Session Recording cloud client and the Session Recording service

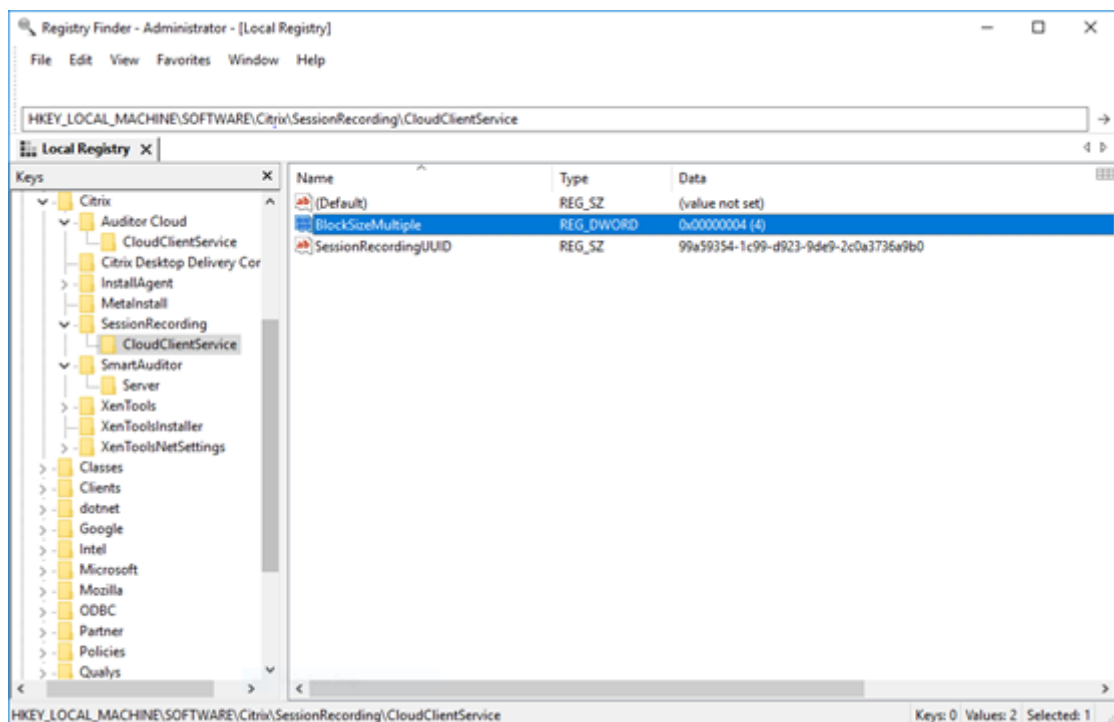
Proxy

You can set up a proxy when installing the Session Recording cloud client. For more information, see [Connect existing Session Recording servers to the cloud](#).

Increase the transport packet size

1. On the Session Recording server where you installed the cloud client, browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SessionRecording\CloudClientService**
2. Edit the **BlockSizeMultiple** value.

The default value is 4 (16 KB). We recommend you set the value to 8 (32 KB).



Install certificates in IIS

Note:

If you're using version 7.37.9010.3 or later of the cloud client and want to use the cloud player only, you can skip this step.

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.

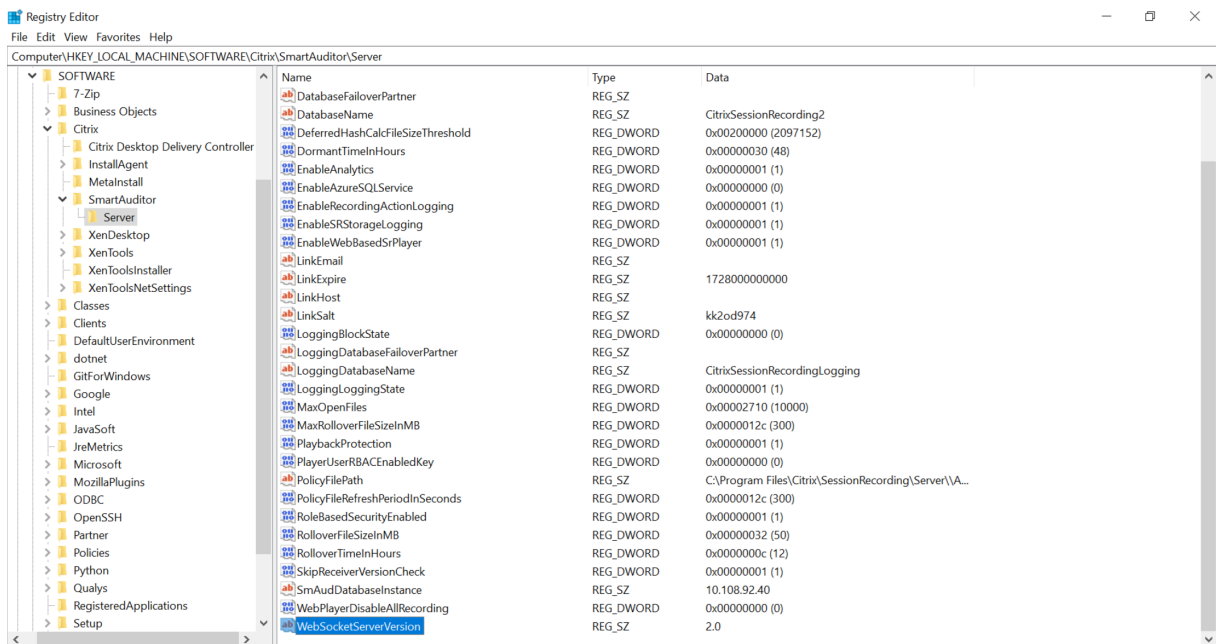
For more information, see step 1 of [HTTPS configuration](#).

Switch to web streaming service version 2.0

Note:

If you're using version 7.37.9010.3 or later of the cloud client and want to use the cloud player only, you can skip this step.

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 (version 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 existing Session Recording servers to the cloud

April 26, 2024

You can connect Session Recording servers in a 1912 LTSR, 2203, or later deployment to the Session Recording service.

Before proceeding to the following steps on each server you want to connect, watch the video about connecting Session Recording servers:



Note:

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

Steps

To connect an existing Session Recording server to the Session Recording service, complete the following steps on the server:

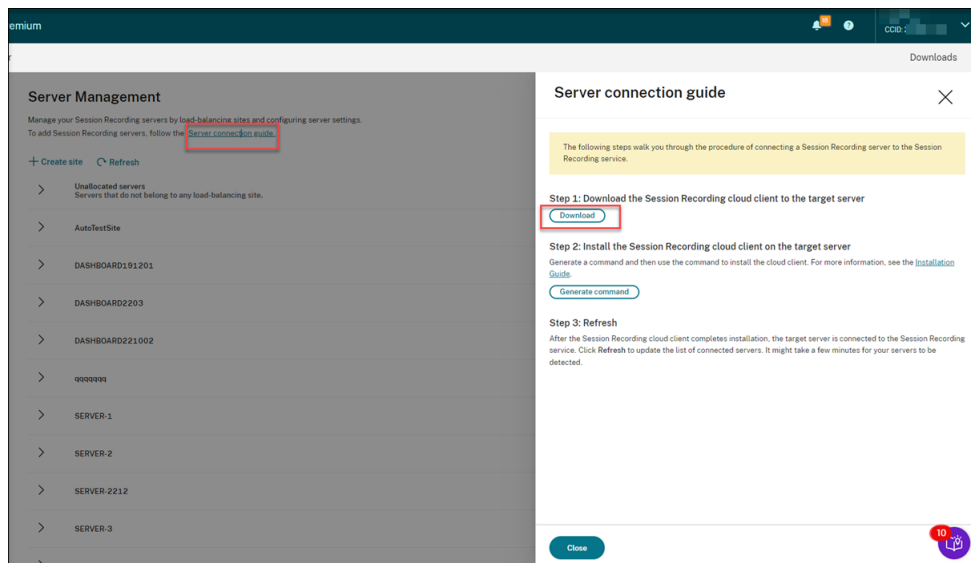
1. Allow the outbound ports based on the version of your cloud client.
 - If you are using version 7.40.13020.11 or later of the cloud client, allow the outbound port 443 only.
 - If you are using a cloud client earlier than version 7.40.13020.11, allow the outbound ports 80, 443, 8088, and 9090–9094.
2. Download and install the Session Recording cloud client. After the Session Recording cloud client completes installation, the target server is connected to the Session Recording service.

Note:

A daemon maintaining the cloud client's running state is available for versions 7.38.10030.16 and later of the cloud client. The daemon automatically fixes the cloud

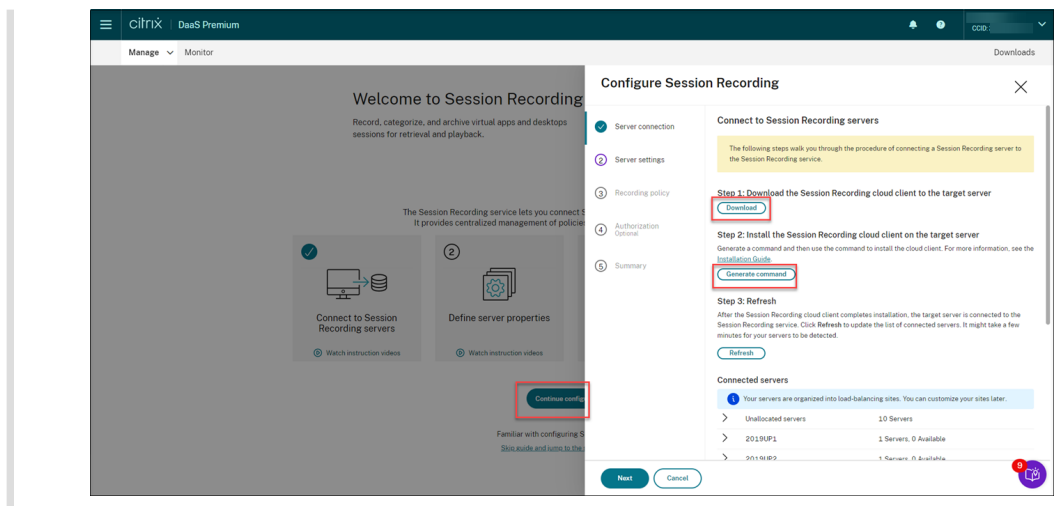
client when it runs abnormally.

- a) Sign in to Citrix Cloud.
- b) In the upper left menu, select **My Services > DaaS**.
- c) From **Manage**, select **Session Recording**.
- d) Select **Configuration > Server Management** from the left navigation of the Session Recording service.
- e) Click **Download** on the **Server connection guide** page.

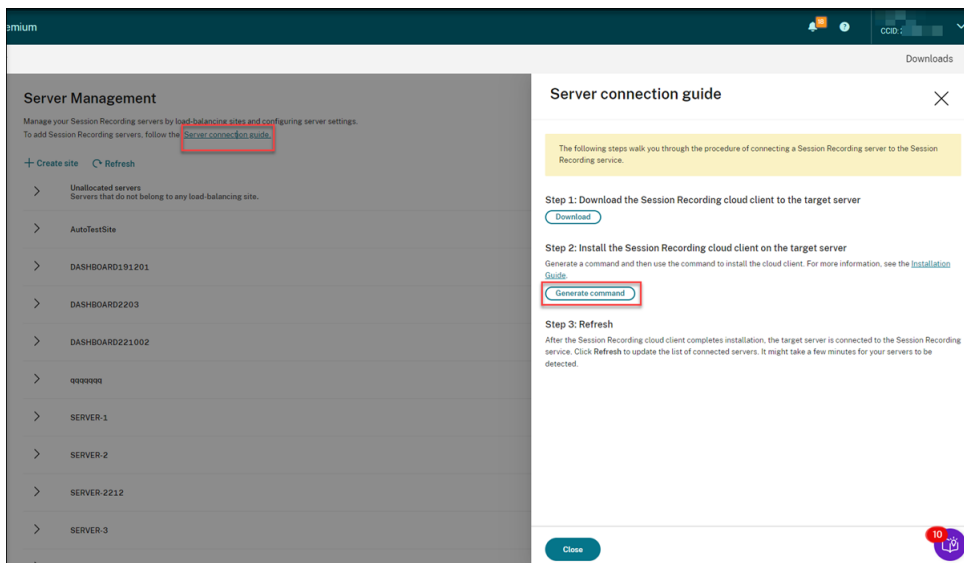


Tip:

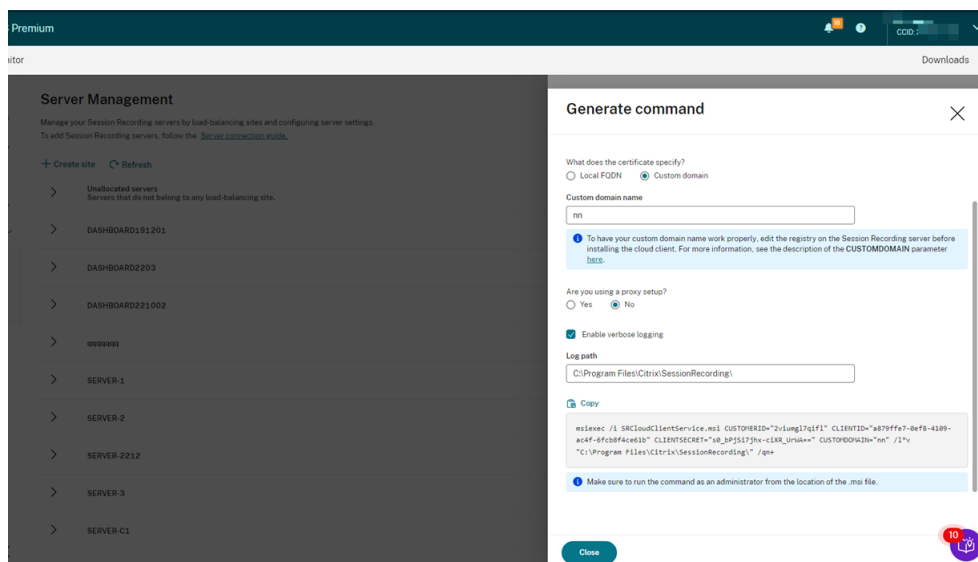
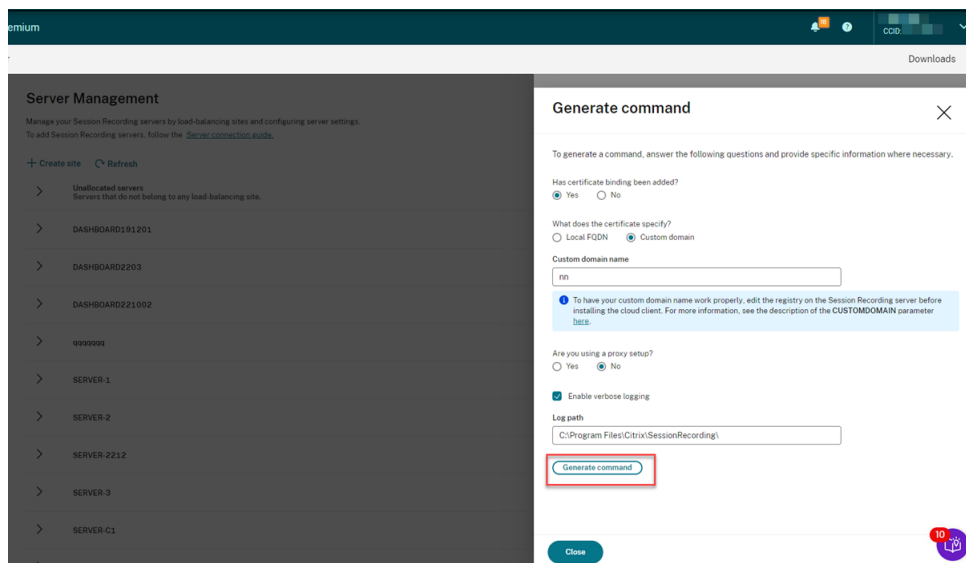
- The **Generate command** button for cloud client installation is unavailable for the administrators that are added through Azure AD groups.
- You can also access the **Download** and **Generate command** buttons by clicking **Continue configuration** on the Session Recording service **welcome** page:



- f) Install the cloud client on the Session Recording server. To do that, run a command as an administrator from the location of the cloud client .msi file that you downloaded earlier. You can enter a command manually or generate a command by clicking **Generate command** on the **Server connection guide** page.



Answer questions and provide information where necessary on the **Generate command** page. After that, click the **Generate command** button.



If you modify the answers or provide different information after clicking the **Generate command** button, the generated command automatically updates accordingly. The **Generate command** button is available again after you sign out and sign back in to Citrix Cloud.

The command is similar to the following:

```

1 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 (;)>" /l*xv "<log path>" /qn+
2 <!--NeedCopy-->
    
```

Where:

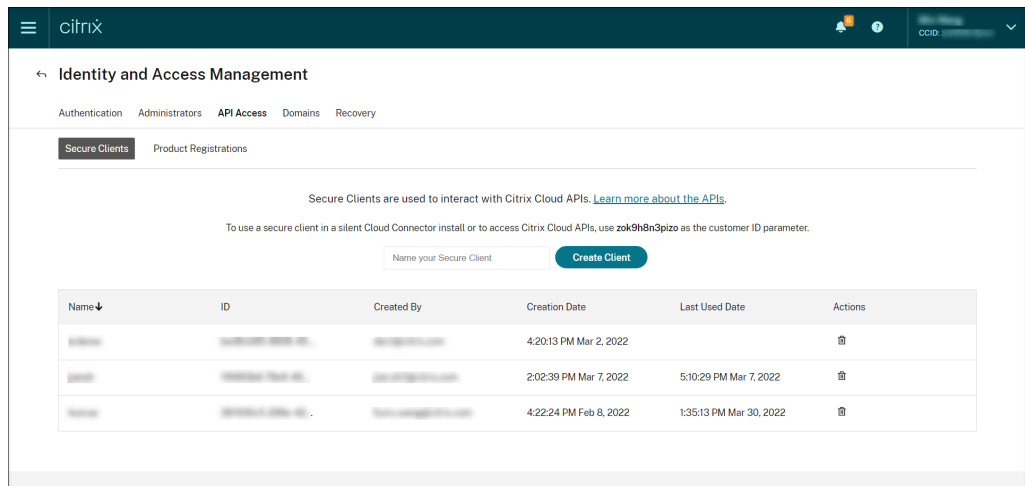
- **SRCloudClientService.msi** installs the Session Recording cloud client that enables interaction with Citrix Cloud. Download or copy the .msi file to each Session Recording server you want to connect.

Note:

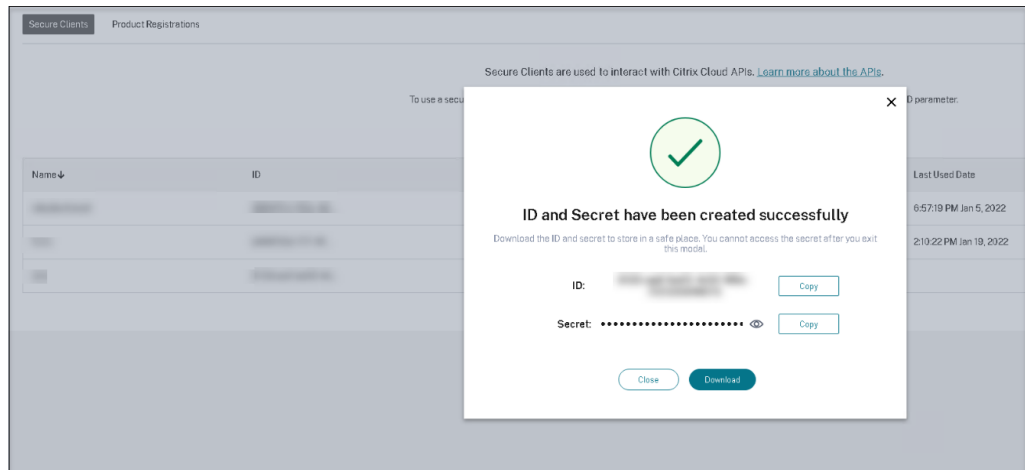
The status of a Session Recording server might not change to **Offline** after you stop the cloud client service (CitrixSsRecCloudClientService) on it. For more information, see [Configure Session Recording servers](#).

Citrix collects traces from the cloud clients installed on on-premises Session Recording servers and uses the traces for troubleshooting.

- **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:



- **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.



- **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.

Note:

Versions 7.37.9010.3 and later of the cloud client don't depend on the local certificates on Session Recording servers and don't support the **CUSTOMDOMAIN** parameter.

- To have the custom domain name work properly, use either of the following methods before installing the Session Recording cloud client:

(Recommended) Method 1:

- i. On the machine where you installed the Session Recording server, open Registry Editor.
- ii. Locate the following registry key:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0`
- iii. Right-click **MSV1_0** and create a multi-string value.
- iv. 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.

- v. Exit Registry Editor.

- vi. Restart the machine.

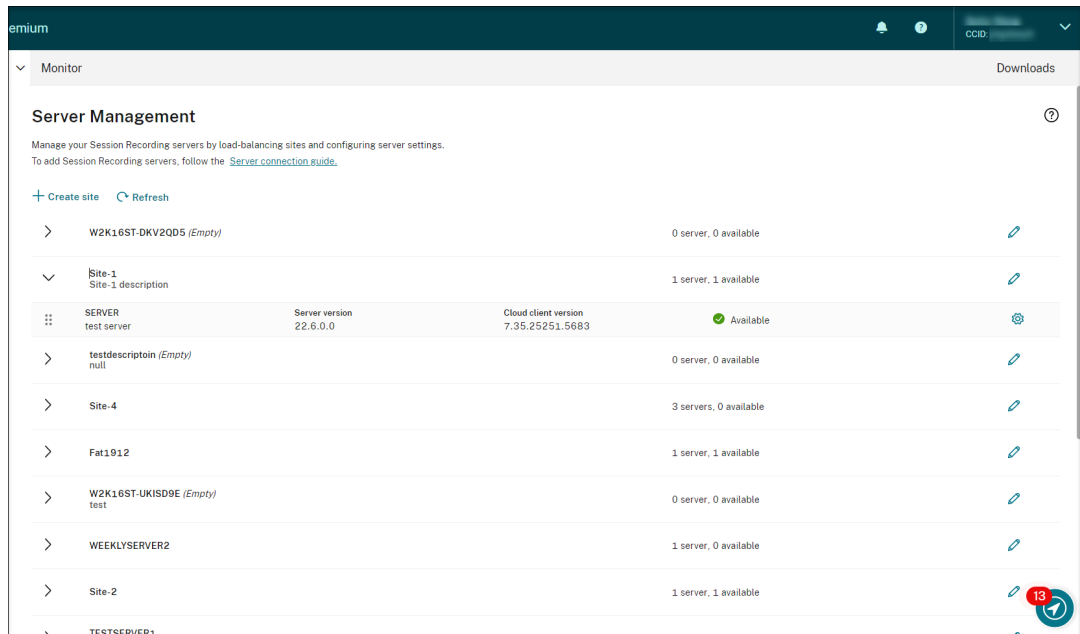
Method 2:

Note:

This method reduces security because it disables the authentication loopback check.

- i. On the machine where you installed the Session Recording server, open Registry Editor.
 - ii. Locate the following registry key:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`
 - iii. Right-click **Lsa** and create a DWORD value.
 - iv. Set the value name to **DisableLoopbackCheck** and the value data to 1.
 - v. Exit Registry Editor.
 - vi. Restart the machine.
- **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 the 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/95rc2MBacUpwBGI/v2/proxy.pac>. If you leave the parameter unspecified, proxy auto-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.



Server management

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](#).

Install Session Recording servers from within the cloud

April 26, 2024

You can [connect existing Session Recording servers to the cloud](#). You can also install Session Recording servers directly from within the cloud.

This feature obliterates the need to download the Citrix Virtual Apps and Desktops installer or the SessionRecordingAdministrationx64.msi file. It also checks domain joining to prevent issues that might keep Session Recording servers from functioning after being connected.

This article walks you through the process of installing a Session Recording server from within the cloud and provides guidance for post-installation actions.

Note:

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

Installation steps

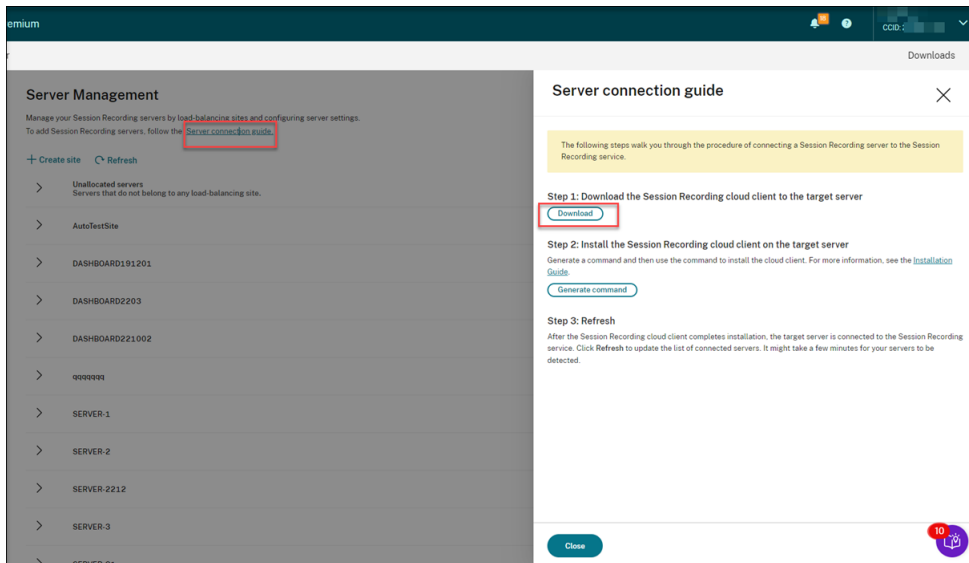
To install a Session Recording server from within the cloud, connect a machine to the Session Recording service and then install the Session Recording server on it from within the cloud. To do so:

1. Prepare a machine.
2. Allow the outbound ports based on the version of your cloud client.
 - If you are using version 7.40.13020.11 or later of the cloud client, allow the outbound port 443 only.
 - If you are using a cloud client earlier than version 7.40.13020.11, allow the outbound ports 80, 443, 8088, and 9090–9094.
3. Download and install the Session Recording cloud client on the machine.

Note:

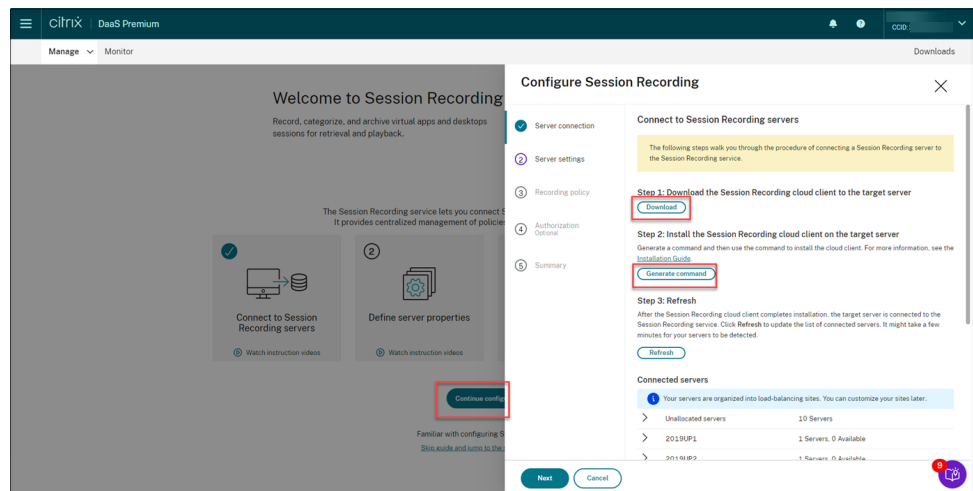
A daemon maintaining the cloud client's running state is available for versions 7.38.10030.16 and later of the cloud client. The daemon automatically fixes the cloud client when it runs abnormally.

- a) Sign in to Citrix Cloud.
- b) In the upper left menu, select **My Services > DaaS**.
- c) From **Manage**, select **Session Recording**.
- d) Select **Configuration > Server Management** from the left navigation of the Session Recording service.
- e) Click **Download** on the **Server connection guide** page.



Tip:

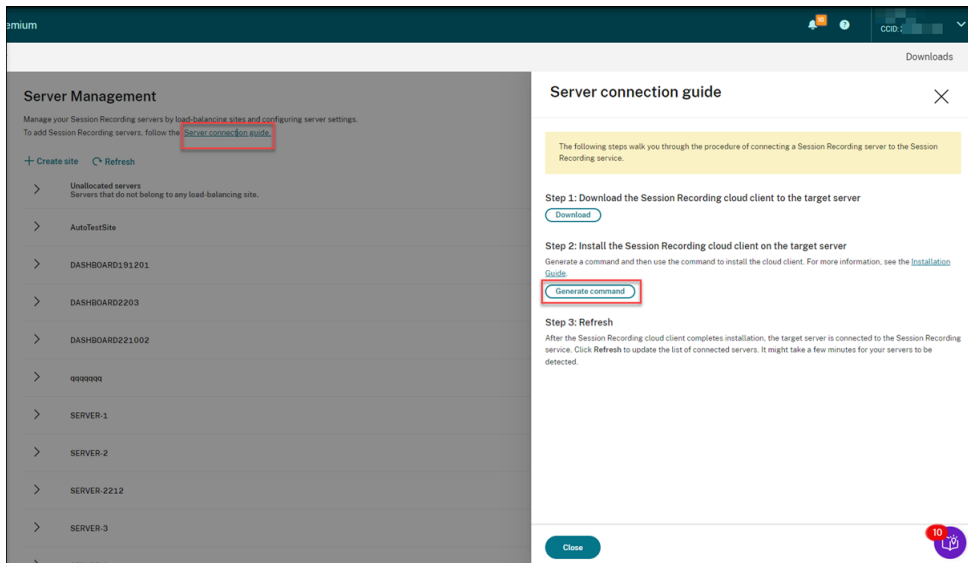
- The **Generate command** button for cloud client installation is unavailable for the administrators that are added through Azure AD groups.
- You can also access the **Download** and **Generate command** buttons by clicking **Continue configuration** on the Session Recording service **welcome** page:



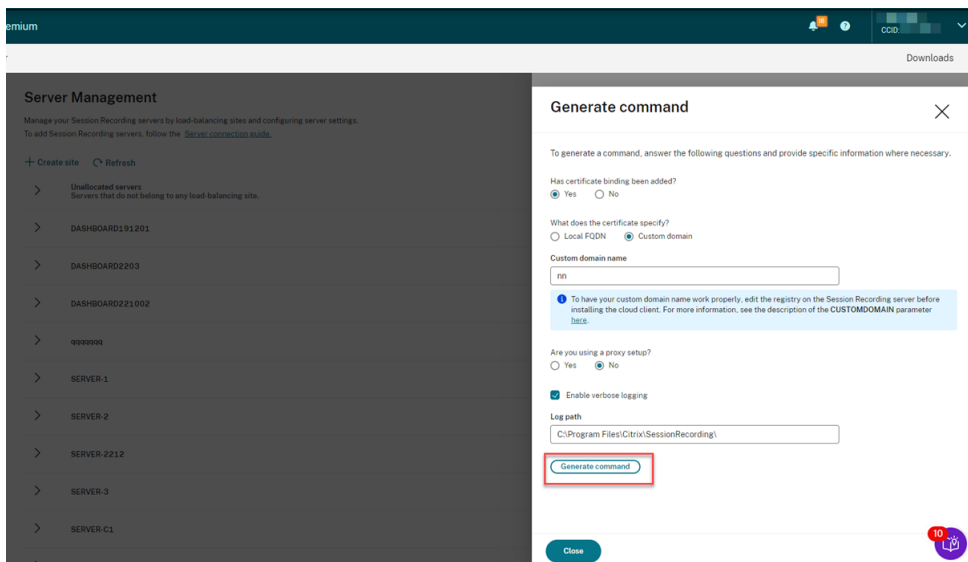
- f) Install the cloud client on the machine. To do that, run a command as an administrator from the location of the cloud client .msi file that you downloaded earlier.

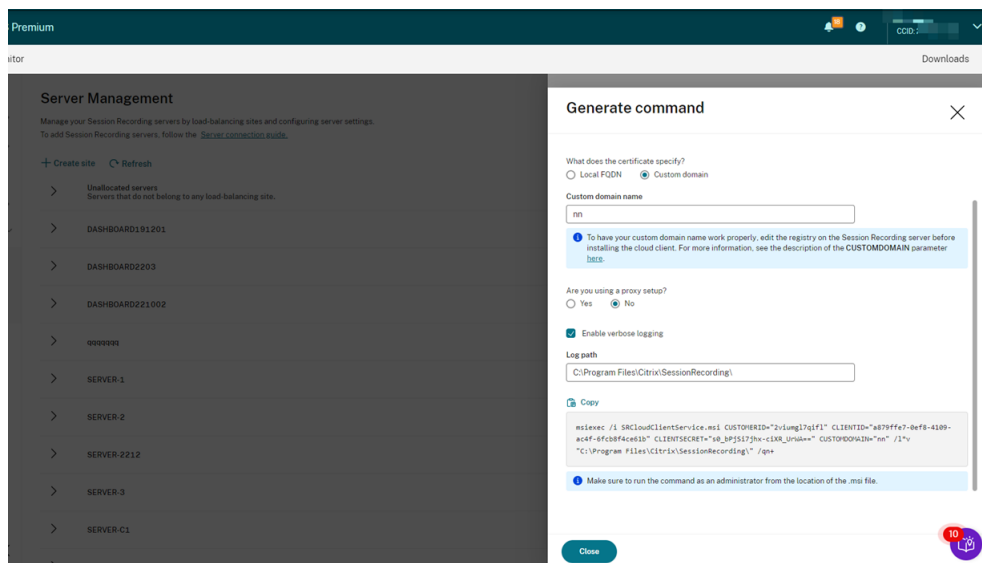
You can enter a command manually or generate a command by clicking **Generate command** on the **Server connection guide** page.

Session Recording service



Answer questions and provide information where necessary on the **Generate command** page. After that, click the **Generate command** button.





If you modify the answers or provide different information after clicking the **Generate command** button, the generated command automatically updates accordingly. The **Generate command** button is available again after you sign out and sign back in to Citrix Cloud.

Note:

Versions 7.37.9010.3 and later of the cloud client don't depend on the local certificates on Session Recording servers and don't support the **CUSTOMDOMAIN** parameter.

To have a custom domain name work properly, use either of the following methods **before installing the Session Recording cloud client**:

(Recommended) Method 1:

- i. On the machine, open Registry Editor.
- ii. Locate the following registry key:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0`
- iii. Right-click **MSV1_0** and create a multi-string value.
- iv. 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.

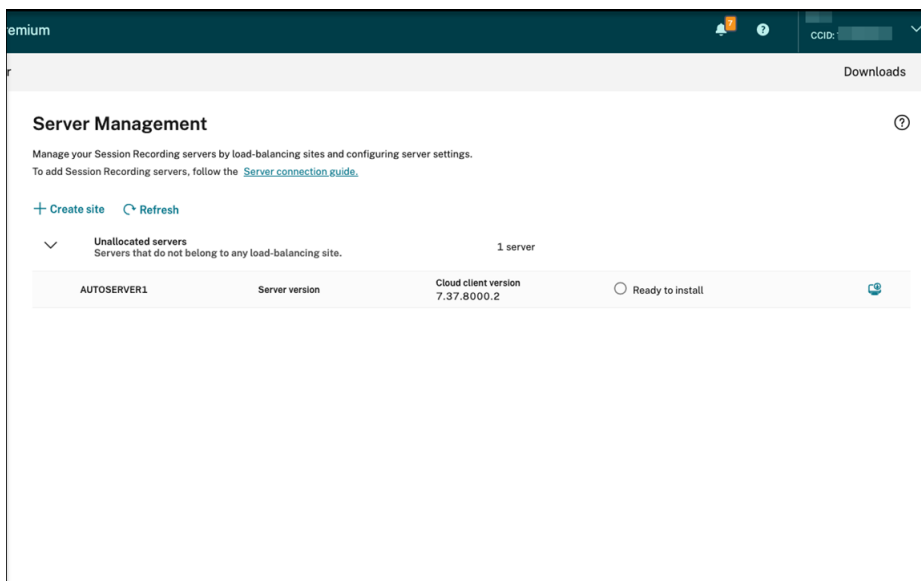
- v. Exit Registry Editor.
- vi. Restart the machine.

Method 2:

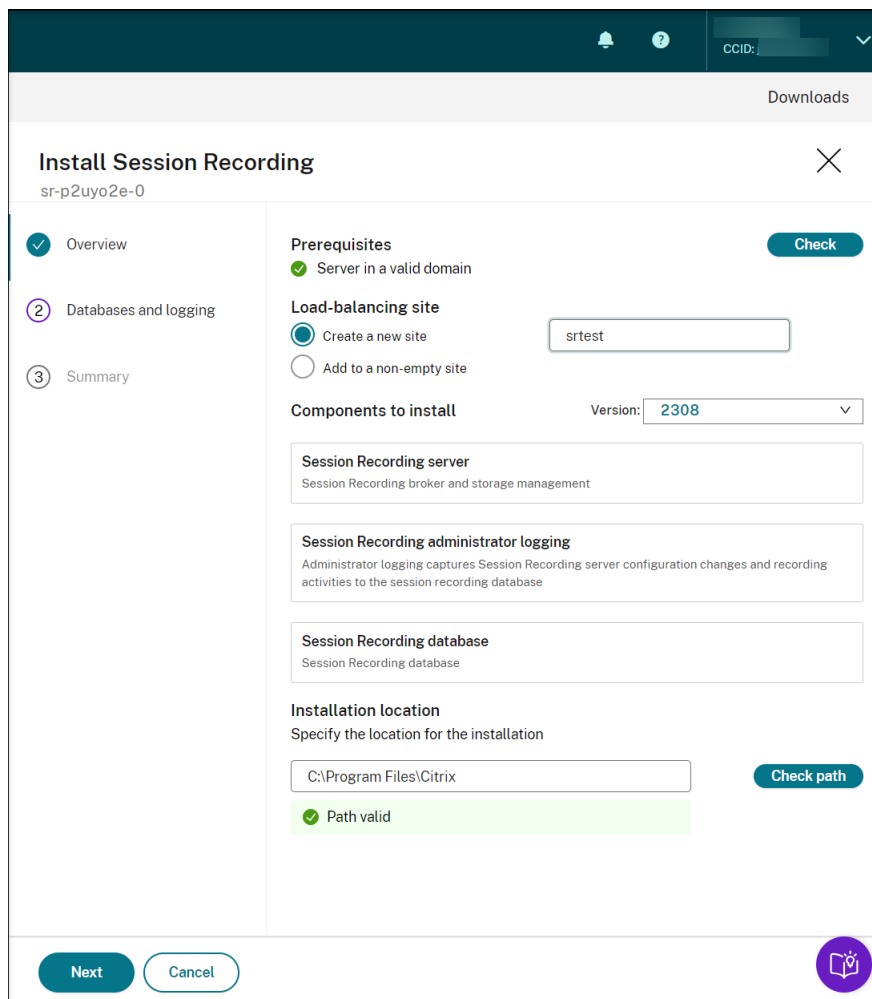
Note:

This method lowers security thresholds because it disables the authentication loop-back check.

- i. On the machine, open Registry Editor.
 - ii. Locate the following registry key:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`
 - iii. Right-click **Lsa** and create a DWORD value.
 - iv. Set the value name to **DisableLoopbackCheck** and the value data to 1.
 - v. Exit Registry Editor.
 - vi. Restart the machine.
4. Verify that the status of the machine shows **Ready to install**, and then click the installation icon.



5. Follow the wizard to install the Session Recording server component on the machine.



- a) On the **Overview** page, complete the following steps:
 - i. Run a check to verify that the machine is in a valid domain.
 The prerequisite check is to prevent issues that might keep Session Recording servers from functioning after being connected.
 - ii. Create a site for the machine or add the machine to an existing non-empty site.
 - iii. Choose a server version to install.
 - iv. Specify an installation path and verify that the path is valid.
 - v. Click **Next** to proceed to the **Databases** page.
- b) On the **Databases** page, choose whether to use a cloud database, fill the fields accordingly, and then click **Test connection** to test the connectivity to the Session Recording database and the administrator logging database.

Downloads

Install Session Recording

CNENG5REQMKF8PX

- Overview
- 2 Databases and logging**
- 3 Summary

Databases

We will create 2 SQL databases for recording and logging data, respectively. Specify the instance name and customize the database names as needed.

Use cloud database

Instance name

Session Recording database name

Administrator logging database name

[Test connection](#)

Administrator logging options

- Enable administrator logging**
Enable or disable the administrator logging service.
- Enable mandatory blocking**
Lets you allow or block changes to policies and server properties if logging fails.

[Next](#) [Back](#)

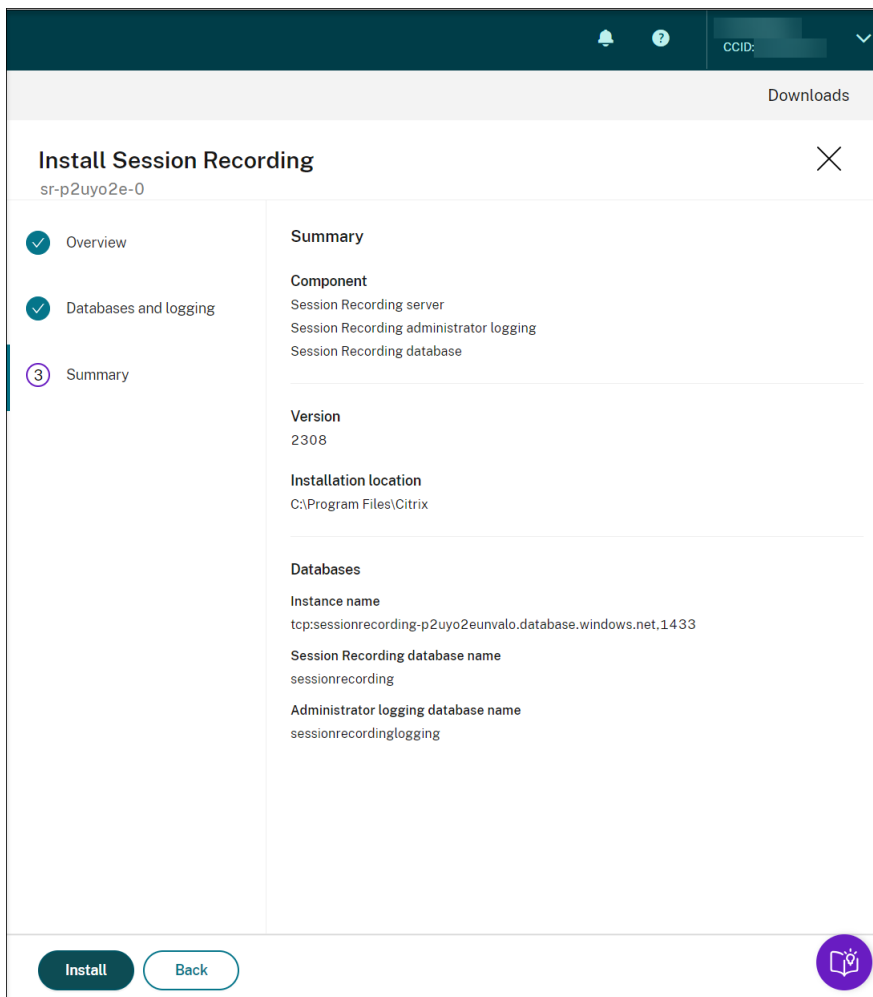
Tip:

- If you allocated the machine to an existing non-empty site earlier, the fields on the **Databases** page are automatically filled.
- You can deploy the Session Recording database on the following cloud SQL database services:
 - Azure SQL Database
 - Azure SQL Managed Instance
 - SQL Server on Azure Virtual Machines (VMs)
 - AWS RDS
 - Google Cloud SQL Server

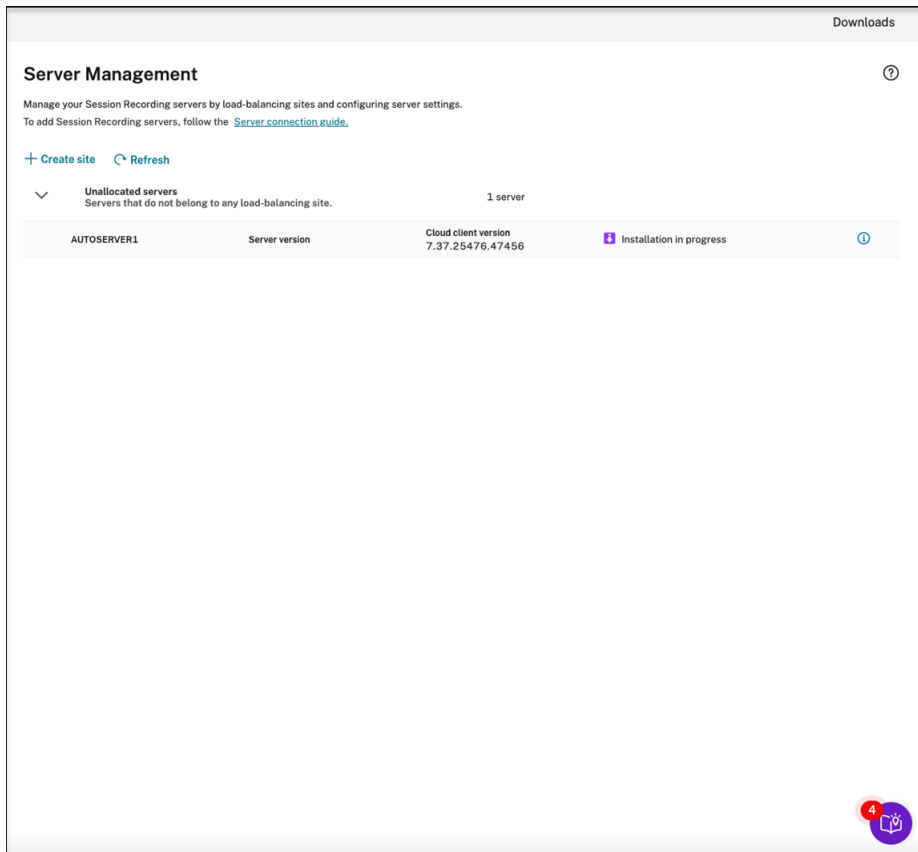
- **Instance name:** If the database instance isn't a named instance, you can use only the computer name of the SQL Server. If you have named the instance during the instance setup, use computer-name\instance-name as the database instance name. To determine the server instance name that you are using, run **select @@servername** on the SQL Server. The return value is the exact database instance name. If your SQL server is configured to be listening on a custom port other than the default port 1433, set the custom listener port by appending a comma to the instance name. For example, type **DXSBC-SRD-1,2433** in the **Instance name** text box, where 2433, following the comma, denotes the custom listener port.
- **Session Recording database name:** Type a custom database name. The machine must have the **sysadmin** role permission of the database. Otherwise, ask the database administrator to assign the permission. Click **Test connection** to test the connectivity to the SQL Server instance and the validity of the database name.

- **Administrator logging database name:** The administrator logging database name must be different from the Session Recording database name. After typing the administrator logging database name, click **Test connection** to test the connectivity to the administrator logging database.
- **Enable administration logging:** By default, the administration logging feature is enabled. You can disable it by clearing the check box.
- **Enable mandatory blocking:** By default, mandatory blocking is enabled. The normal features might be blocked if logging fails. You can disable mandatory blocking by clearing the check box.

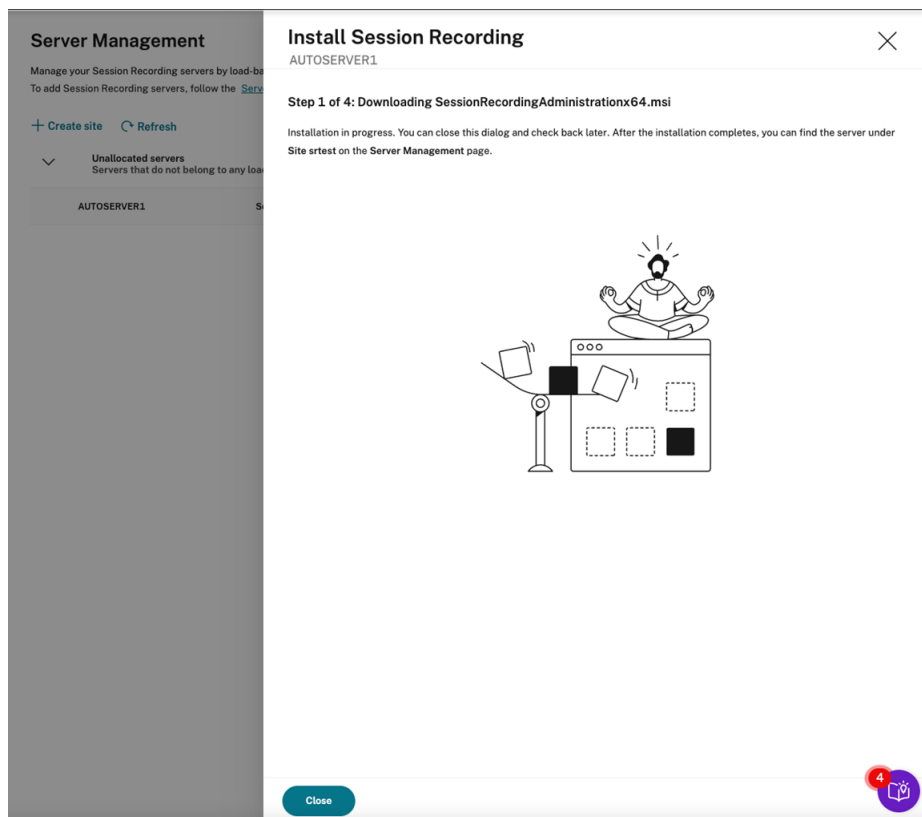
c) On the **Summary** page, verify your settings and click **Install**.



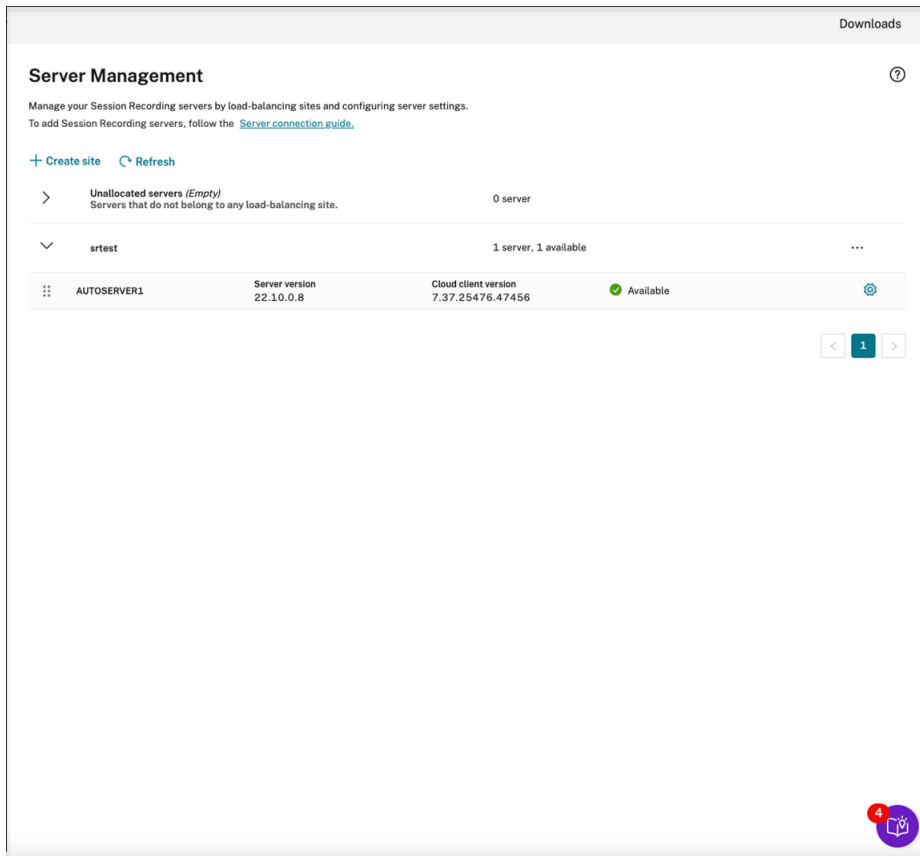
d) Check the installation progress by clicking the icon next to **Installation in progress**.



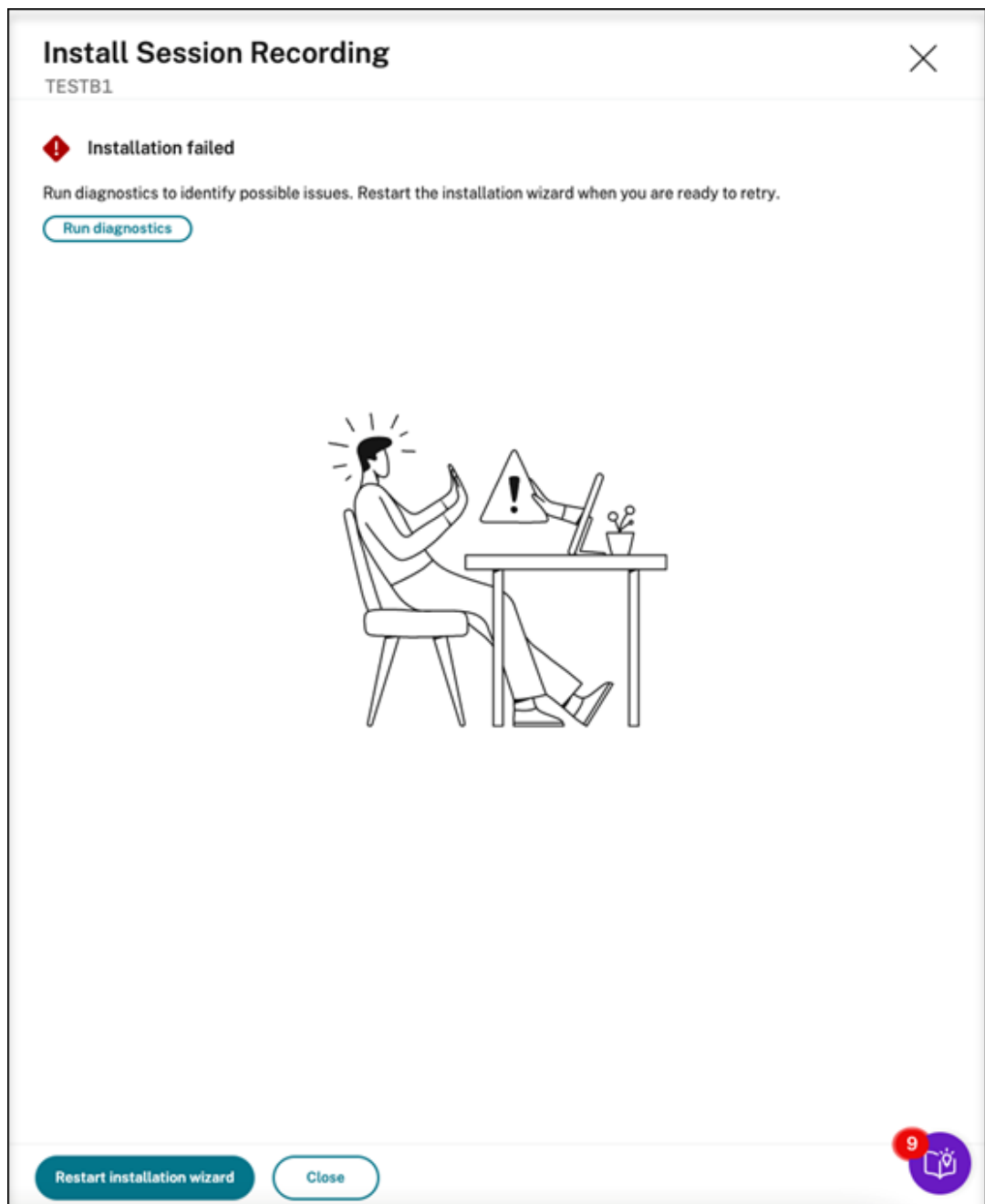
For example, the installation has progressed to the first step.



After installation completes successfully, the machine becomes a Session Recording server that is connected to the Session Recording service. You can find the server under the site that you created or specified. Refresh the **Server Management** page to view all connected servers.



If the installation fails, click the icon next to **Installation failed** and run diagnostics to identify possible issues. Fix the issues if any, restart the machine, and then restart the installation wizard.



Post-installation actions

After installing a Session Recording server from within the cloud, perform the following operations:

- Connect the newly installed Session Recording server to the target Session Recording agent. Go to the target VDA or VDI machine and open **Session Recording Agent Properties**. Type the computer name of the machine where you installed the Session Recording server. Type the protocol and port information for the connection to the Session Recording server.

- Configure [server settings](#), [policies](#), and [playback permissions](#) based on your needs.
- Launch sessions to verify that sessions are recording.
- View [administrator logging data](#).
- Go to the Session Recording management dashboard to gain insights into your deployment. For fresh installations, data is not immediately available on the dashboard.

Deploy Session Recording resources to a cloud subscription

June 21, 2024

This article provides information on deploying Session Recording resources to an Azure subscription.

You can deploy the following Session Recording resources to an Azure subscription from within the Session Recording service:

- Session Recording servers
- Databases
- Storage
- Load balancer

There are two ways of deploying Session Recording resources to an Azure subscription:

- **Use a host connection** that connects to the Azure subscription. Creating a host connection requires you to provide your subscription information. For more information, see [Create and deploy a site through a host connection](#) later in this article.
- **If you do not want to provide your subscription information, create an Azure Resource Manager template (ARM template)** that contains how and which resources you want to deploy. For more information, see [Create and deploy a site through an ARM template](#) later in this article.

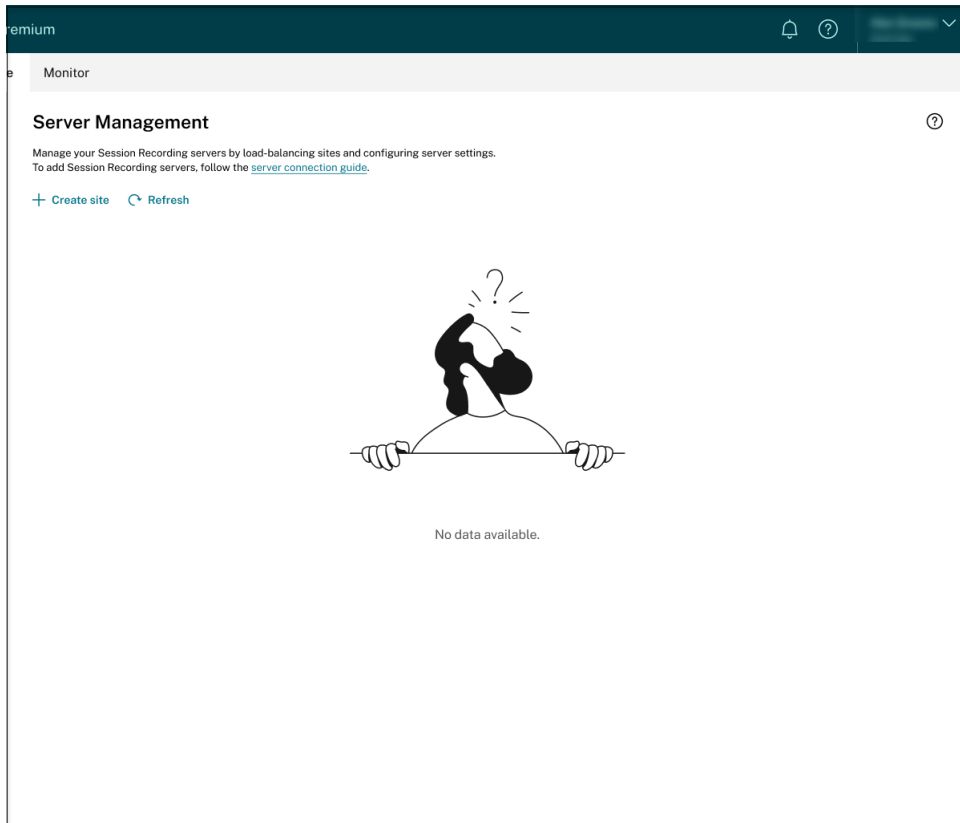
Create and deploy a site through a host connection

This section guides you through the procedure of creating and deploying a site through a host connection and the following operations that can be performed on a site deployed this way:

- Add resources to an existing site deployed on Azure
- Change the IP addresses that are allowed to access the load balancer
- View actual costs for using Azure

Create and deploy a site through a host connection

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



2. On the **Server Management** page, click **Create site**. The **Create Site** page appears.

Create site [Close]

1 Site information

What would you like to do?

- Create an empty site**
Create a site and add servers later.
- Create and deploy a site through a host connection**
Deploy Session Recording resources using a host connection that connects to your specific cloud subscription. [Learn more](#)
- Create and deploy a site through an ARM template**
Create an Azure Resource Manager template (ARM template) to deploy Session Recording resources in Azure. [Learn more](#)

Site name
Name this site

Description (optional)
Enter description

Save Cancel [Help 8]

3. Select **Create and deploy a site through a host connection**. The main steps are listed in the left navigation.

4. Enter a site name and description, select a host connection that connects to your Azure subscription, and specify a region.

- If you don't have a host connection in place, add one by referring to [Add a host connection](#) later in this article.
- Azure Government regions aren't supported.

5. After completing the site information, click **Next** to continue.

6. (Optional) To get recommendations for VM and storage configurations, provide information about your recording needs.

You can skip this step by clicking **I'm good, skip this step** or by clicking **Next** with nothing selected.

Create site

- Site information
- About your deployment**
Optional
- Network
- Virtual machines
- Domain and certificate
- Storage
- Databases
- Load balancer
- Tags
Optional
- Secure client
- Summary

Tell us about your recording needs, so we can provide some recommendations for your VM and storage configurations.
[I'm good, skip this step.](#)

The following information helps determine the recommended number of Session Recording servers.

How many concurrent sessions do you have at most?

4,000-6,000

Recommended number of servers: 3 [reset](#)

The following information helps determine the recommended storage capacity.

How much visual movement do your sessions typically have?

Some, the display changes but not drastically

How many sessions do you need to record per day?

5,000-10,000

For how long do you need to retain each recording file?

15-30 days

Recommended storage capacity: 30 TiB [reset](#)

[Next](#) [Cancel](#)

When you select an option from the drop-down list, a recommendation is presented according to your selection. A **reset** button is available next to the recommendation. It lets you clear your selections and the corresponding recommendation in that section.

- Specify the virtual network and subnet for your Session Recording servers to join. If your VDAs reside in a different virtual network from the Session Recording servers or in an on-premises network, establish connectivity to ensure the Session Recording servers can communicate with your VDAs.

Create site [Close]

- ✓ Site information
- ✓ About your deployment
Optional
- 3 Network**
- 4 Virtual machines
- 5 Domain and certificate
- 6 Storage
- 7 Databases
- 8 Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

Specify the virtual network and subnet for your Session Recording servers to join.

Virtual network
[Dropdown menu]
Select a virtual network that your VDAs can connect to.

Subnet
[Dropdown menu]
Select a subnet that your VDAs can connect to.

Next Cancel [Help icon with 8]

8. Create virtual machines (VMs) as your Session Recording servers.

Create site [X]

- Site information
- About your deployment Optional
- Network
- 4 Virtual machines**
- 5 Domain and certificate
- 6 Storage
- 7 Databases
- 8 Load balancer
- 9 Tags Optional
- 10 Secure client
- 11 Summary

Create virtual machines as your Session Recording servers.

Session Recording server version to install: 2311

Image
Windows Server 2022 Datacenter: Azure Edition - x64 Gen2

Size
Standard_D4s_v3-4vcpus, 16 GiB memory

Number of VMs
3 Recommended for you: 3

Estimated cost (per month)
\$812.16

Create an administrator account for the virtual machines.

Administrator account username
Set username

Password
Set password

Confirm password
Confirm password

Next Cancel [8]

Note:

- The **Number of VMs** field is prefilled with the recommended number if there's one. Change the number as needed.
- Estimated costs are based on standard pricing and don't take discounts into consideration. You can expect lower actual costs than estimated.

9. Join the Session Recording servers to the same domain with your VDAs and specify a certificate for the Session Recording servers.

- If your VDAs connect to an Active Directory domain, select the **Join servers to an Active Directory domain** check box and enter the relevant information. By selecting the **Join servers to an Active Directory domain** check box, you are configuring the deployment for a hybrid scenario, integrating on-premises Active Directory with Azure AD.
- If your VDAs connect to an Azure Active Directory (Azure AD) domain, clear the **Join servers to an Active Directory domain** check box. After you complete creating the current site, make sure to manually join the Session Recording servers to the same Azure AD domain. Notice that pure Azure AD deployment is available only for Session Recording 2402 and later.

Create site ✕

- ✓ Site information
- ✓ About your deployment
Optional
- ✓ Network
- ✓ Virtual machines
- 5** Domain and certificate
- 6 Storage
- 7 Databases
- 8 Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

Join servers to an Active Directory domain

i This should be the domain where your VDAs reside.

Domain name

Domain controller IP address

Username


Specify a domain user with sufficient rights to join machines to the domain.

Password

Specify a certificate for the virtual machines to use. Only .pfx files are supported.

Certificate

Certificate password



Create site

- Site information
- About your deployment
Optional
- Network
- Virtual machines
- 5 Domain and certificate**
- 6 Storage
- 7 Databases
- 8 Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

Join servers to an Active Directory domain

Supported only on Session Recording server version 2402 or later. Please select a compatible version in the previous step. [Go back](#)

Specify a certificate for the virtual machines to use. Only .pfx files are supported.

Certificate

[Browse](#)

Certificate password

Enter password

[Next](#) [Cancel](#)

Note:

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

10. Configure an Azure storage account and file shares to store your recording files. For pricing information, see [Azure Files pricing](#).

Create site

- Site information
- About your deployment
Optional
- Network
- Virtual machines
- Domain and certificate
- Storage**
- Databases
- Load balancer
- Tags
Optional
- Secure client
- Summary

Configure a storage account and file shares to store your recording files. For pricing information, see [Azure File Pricing](#).

i A separate storage account will be created for your archived recordings, which does not generate any cost if not used.

Storage account

Performance

Standard: Recommended for most scenarios (general-purpose v2 account).
 Premium: Recommended for scenarios that requires low latency.

Redundancy

Locally-redundant storage (LRS)

File shares

Tier

Transaction optimized

Maximum capacity

5 TiB

Number of file shares

6 **i** Recommended for you: 6

Estimated cost (per month)

\$1843.2 (max.)
\$0.06 per used GiB, actual cost depends on your usage.

Next **Cancel**

11. Create two SQL databases in Azure. One is used as the Session recording database (named **sessionrecording**) and the other as the administrator logging database (named **sessionrecordinglogging**).

Create site

Create 2 SQL databases for recording and logging data, respectively.

- Site information
- About your deployment
Optional
- Network
- Virtual machines
- Domain and certificate
- Storage
- 7 Databases**
- 8 Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

Compute + storage

Service tier
General Purpose

Compute tier
Provisioned

Hardware configuration
Standard-series (Gen5)
Up to 128 vCores, up to 625 GiB memory

vCores
2

Data max size (GiB)
32

Estimated cost (per month)
\$441.3

Database administrator

Username
dbadmin1

Password
.....

Confirm password
.....

Next **Cancel**

12. Create a load balancer to distribute workload among the Session Recording servers. Enter the IP addresses or ranges of your VDAs and separate them by a comma (,) in the **Restrict access of the load balancer to only the following addresses** field. For pricing information, see [Load Balancer pricing](#).

Create site ✕

- ✓ Site information
- ✓ About your deployment
Optional
- ✓ Network
- ✓ Virtual machines
- ✓ Domain and certificate
- ✓ Storage
- ✓ Databases
- 8** Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

Create a load balancer to distribute workload among the servers. For pricing information, see [Load Balancer Pricing](#).

Azure load balancer

SKU
Standard

Type
Public

Tier
Regional

Estimated cost (per month)
\$189.6

Access

Restrict access of the load balancer to only the following addresses ?

Next **Cancel** 8


13. (Optional) Apply tags to the Azure resources to be created.

Create site ✕

- ✓ Site information
- ✓ About your deployment
Optional
- ✓ Network
- ✓ Virtual machines
- ✓ Domain and certificate
- ✓ Storage
- ✓ Databases
- ✓ Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

You can apply tags to the Azure resources that will be created.
If no tags are needed, simply click **Next** to continue.

Name	Value
+ Add	

Next **Cancel** 

14. Create a secure client to onboard the Session Recording servers to the Session Recording service.

Click **Create client** to let Citrix create a secure client on your behalf. Alternatively, you can create a secure client through the **Identity and Access Management > API Access** tab of the Citrix Cloud console and then fill in the information below.

Create site ✕

- ✓ Site information
- ✓ About your deployment
Optional
- ✓ Network
- ✓ Virtual machines
- ✓ Domain and certificate
- ✓ Storage
- ✓ Databases
- ✓ Load balancer
- ✓ Tags
Optional
- 10 Secure client
- 11 Summary

Create a secure client to onboard the Session Recording servers to the Session Recording service.


Click Create client and we will create a secure client on your behalf. Alternatively, you can create a secure client through the [Identity and Access Management > API Access](#) tab of the Citrix Cloud console and then fill in the information below.

[Create client](#)

ID

Secret

[Next](#) [Cancel](#)



15. View the summary about the site to be created. Click the pencil icon to edit your settings if needed or click the button to start deployment.

The screenshot shows the 'Create site' wizard in Azure. The left sidebar lists the steps: Site information, About your deployment (Optional), Network, Virtual machines, Domain and certificate, Storage, Databases, Load balancer, Tags (Optional), Secure client, and Summary (11). The main area displays a summary of resources to be created for the 'US East' region. The resources include:

- Virtual machine (3):** Image: Windows Server 2022 Datacenter: Azure Edition-x64 Gen2, Size: Standard_D4s_v3-4vcpus, 16 GiB memory.
- Storage account:** Performance: Standard, Redundancy: LRS.
- Storage account (for archive):** Performance: Standard, Redundancy: LRS.
- File shares (6):** Maximum capacity: 5 TiB.
- File Share:** Maximum capacity: 5 TiB.
- Databases (2):** Service tier: General Purpose, vCores: 2, Data max size: 32 GiB.
- Load balancer:** SKU: Standard, Type: Regional, Tier: Tier.

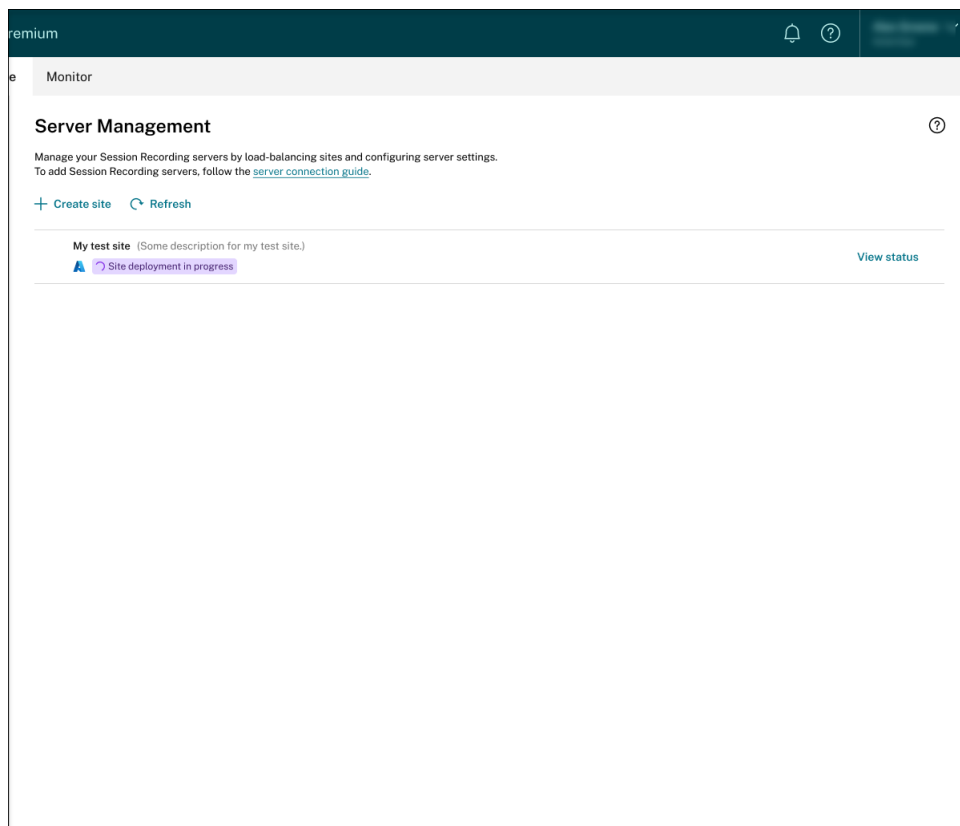
The estimated cost (per month) is \$3286.26. A table breaks down the costs:

Resource	Cost	Resource	Cost
Virtual machines	\$812.16	Databases	\$441.30
Storage	\$1843.20	Azure load balancer	\$189.60

At the bottom, there are 'Start deployment' and 'Cancel' buttons, and a notification icon with the number 8.

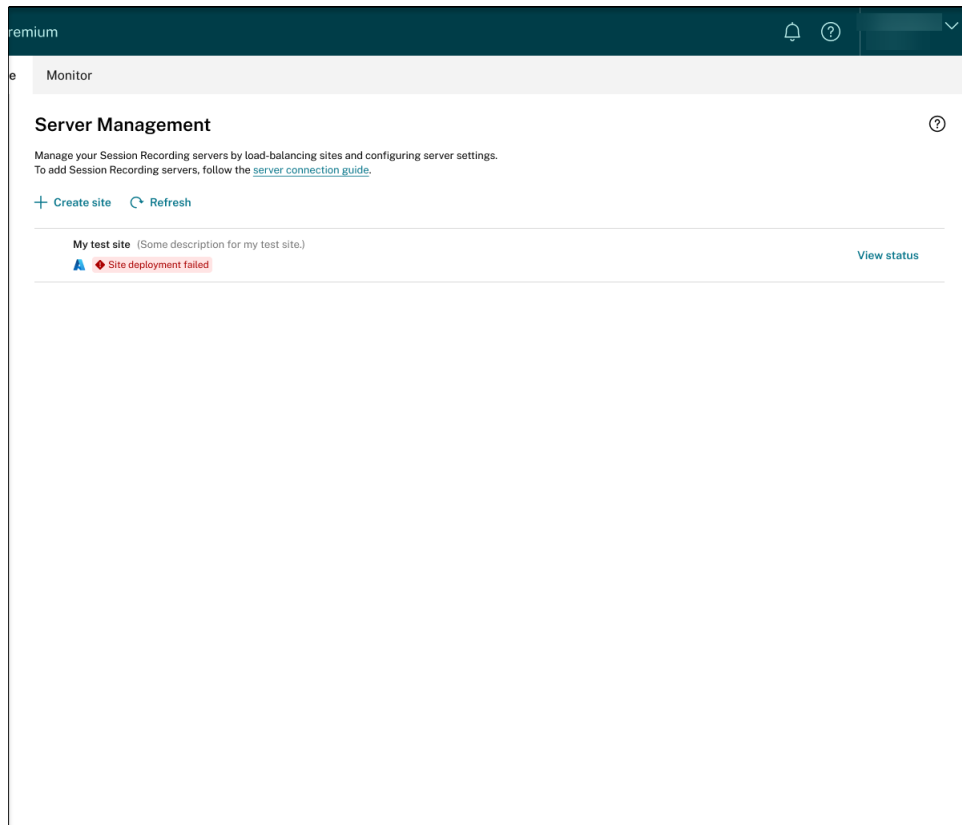
The following are examples of the deployment process:

Deployment in progress:




While a site deployment is in progress, you can click **View status** to view the progress.


Deployment failed:



If errors occur during the deployment process, click **View status** to view the error details. For an example of the error details:


Create site ✕

 Error



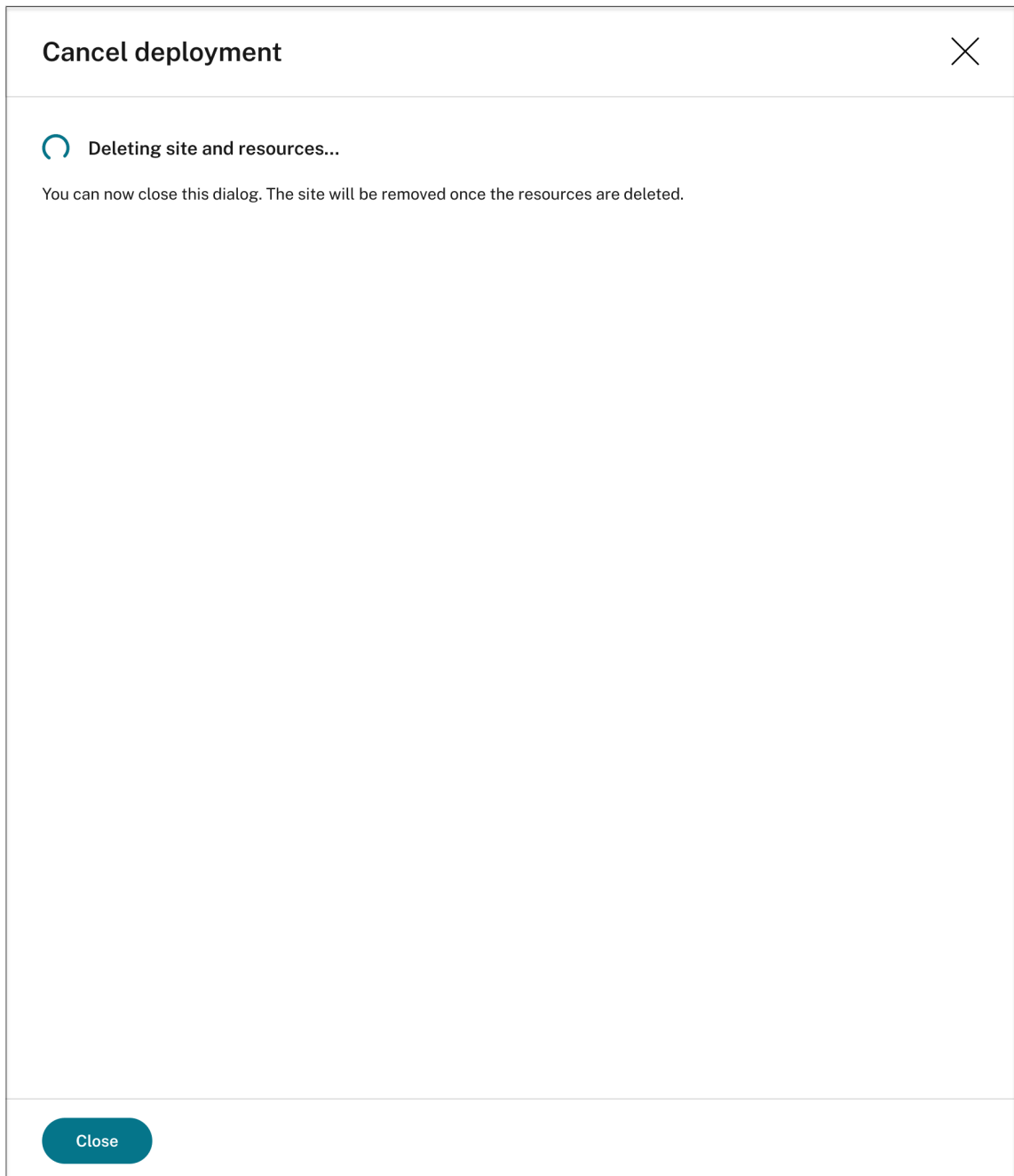
Go back to adjust your input as needed and then try again. When you retry, we will delete the resources that have been created and start afresh.

Don't want to create this site anymore? You can [cancel the deployment](#) and we will delete any resources already created.



[Back to configuration](#) [Close](#)

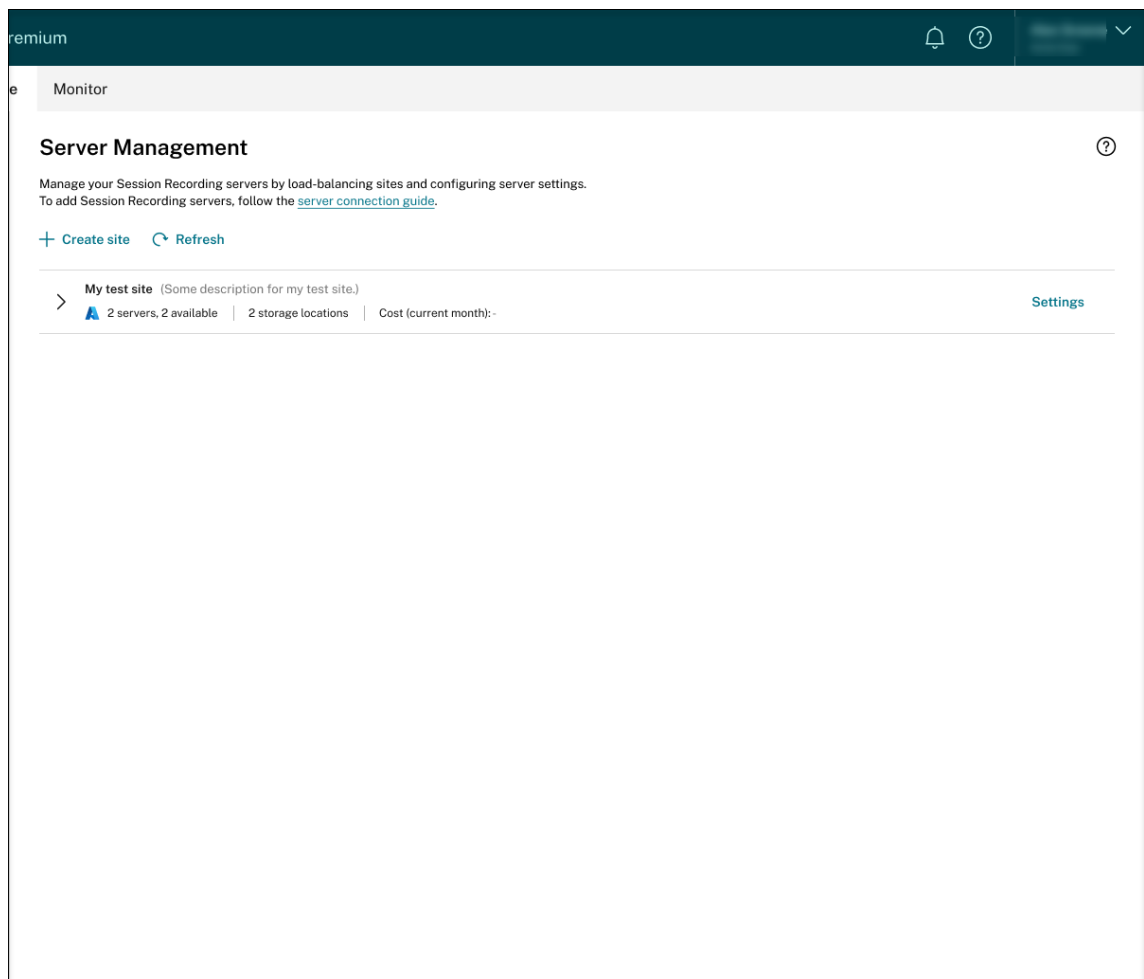
You can click **Back to configuration** or **cancel the deployment**. If you click **Back to configuration**, you're taken back to the **Create Site** page where you can alter your configurations and try again. If you're sure to cancel the deployment, follow the wizard to remove the site and the Azure resources created for the site. For example:



Deployment success:

When a site deployment is complete, you can expand the site and view and manage the resources created under it. The **View status** button changes to **Settings**. An Azure icon is available to represent sites deployed on Azure.

For information about site settings, see [Site and server settings](#).



Add resources to an existing site deployed on Azure

For an existing site that you have deployed on Azure **through a host connection**, you can add resources including servers and storage to it. To do so, complete the following steps:

1. Select **Configuration > Server Management** from the left navigation of the Session Recording service.
2. On the **Server Management** page, locate and unfold the target site. An Azure icon is available to represent sites deployed on Azure.
3. Click **Add resources**.

premium

Monitor

Server Management

Manage your Session Recording servers by load-balancing sites and configuring server settings. To add Session Recording servers, follow the [server connection guide](#).

+ Create site Refresh

My test site (Some description for my test site.) [Settings](#)

2 servers, 2 available | 2 storage locations | Cost (current month): [\\$746.47](#) **Add resources**

Servers

Server name	Server version	Cloud client version	Status	Actions
rsrserver1 Server description goes here.	23.05.0.1	7.39.16000.1	Available	Info Settings
rsrserver2 Server description goes here.	23.05.0.1	7.39.16000.1	Available	Info Settings

Storage locations [Storage maintenance](#)

Storage location	Maximum capacity
\\test.file.core.windows.net\recordings1	5 TiB
\\test.file.core.windows.net\recordings2	5 TiB

Databases

Database name	Pricing tier
sr-recording	General Purpose: Serverless, Gen5, 1 vCore
sr-logging	General Purpose: Serverless, Gen5, 1 vCore

Load balancer

Load balancer name	Actions
sr-load-balancer	Settings

Site 1 (This is the description for Site 1.) [Settings](#)

3 servers, 1 available

Site 2 (This is the description for Site 2.) [Settings](#)

1 server, 1 available

4. On the **Add resources** page, click **Add server** and **Add storage** as needed.

Add resources

My test site ✕

+ Add server

+ Add storage

Start deployment Cancel

- To add servers, click **Add server** and then complete the following steps:

Add resources

My test site

Server Estimated cost (per month): \$83.51 ⊖ 1 ⊕

Image
Windows Server 2019 Datacenter - x64 Gen2

Size
Standard_D4as_v4 - 4vcpus, 16 GiB memory

Domain
test.net (10.10.10.10) [Edit credentials](#)

Secure client ● [Create client](#)

Session Recording server version to install
23.05.0.1 ?

+ Add storage

[Start deployment](#) [Cancel](#)

- Specify the number of servers to add.
 - Click **Provide credentials** to join the new servers to the same domain as the existing servers.
 - Click **Create client** to onboard the new servers to the Session Recording service.
 - Click **Start deployment**.
- To add storage for storing recording files, click **Add storage** and then complete the following steps accordingly:
 - If your site was created with a standard storage account, you're prompted to specify the number of file shares to add. For example:

Add resources

My test site

+ Add server

File shares Estimated cost (per month): \$307.20 (max.) ? ⊖ 1 ⊕

Tier	Maximum capacity
Transaction optimized	5 TiB

Start deploymentCancel

b) If your site was created with a premium storage account, you can specify the number of file shares to add and customize the capacity of each file share. For example:

Add resources

My test site

+ Add server

File shares Estimated cost (per month): \$819.20 ? ⊖ 1 ⊕

Provisioned capacity (GiB)

5120 ⬆️ ⬇️ ⬆️

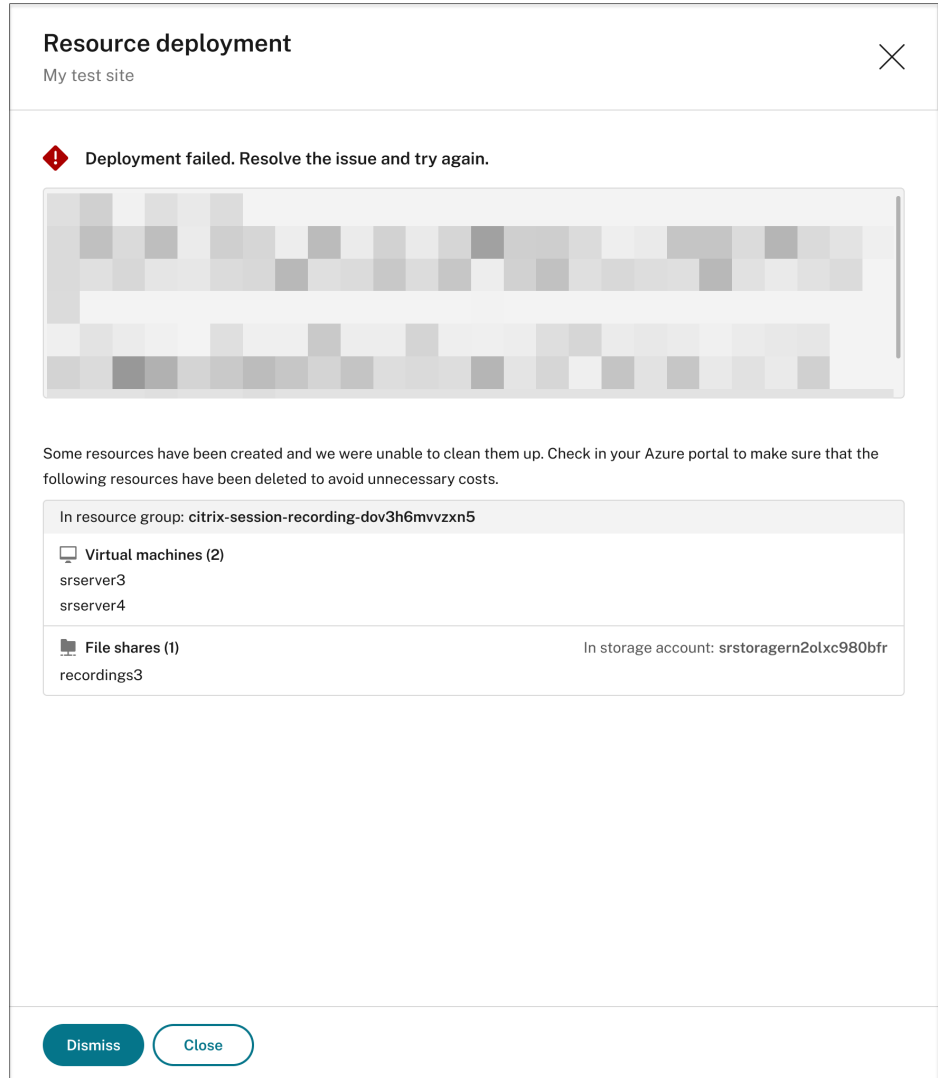
Start deploymentCancel

c) Click **Start deployment**.

Note:

- The **Start deployment** button is available when either of the following conditions is met:
 - * At least one server has been specified and the domain and secure client have been configured.
 - * At least one file share has been specified.
- When resource deployment is in progress, the **Settings** button for the load balancer is disabled.

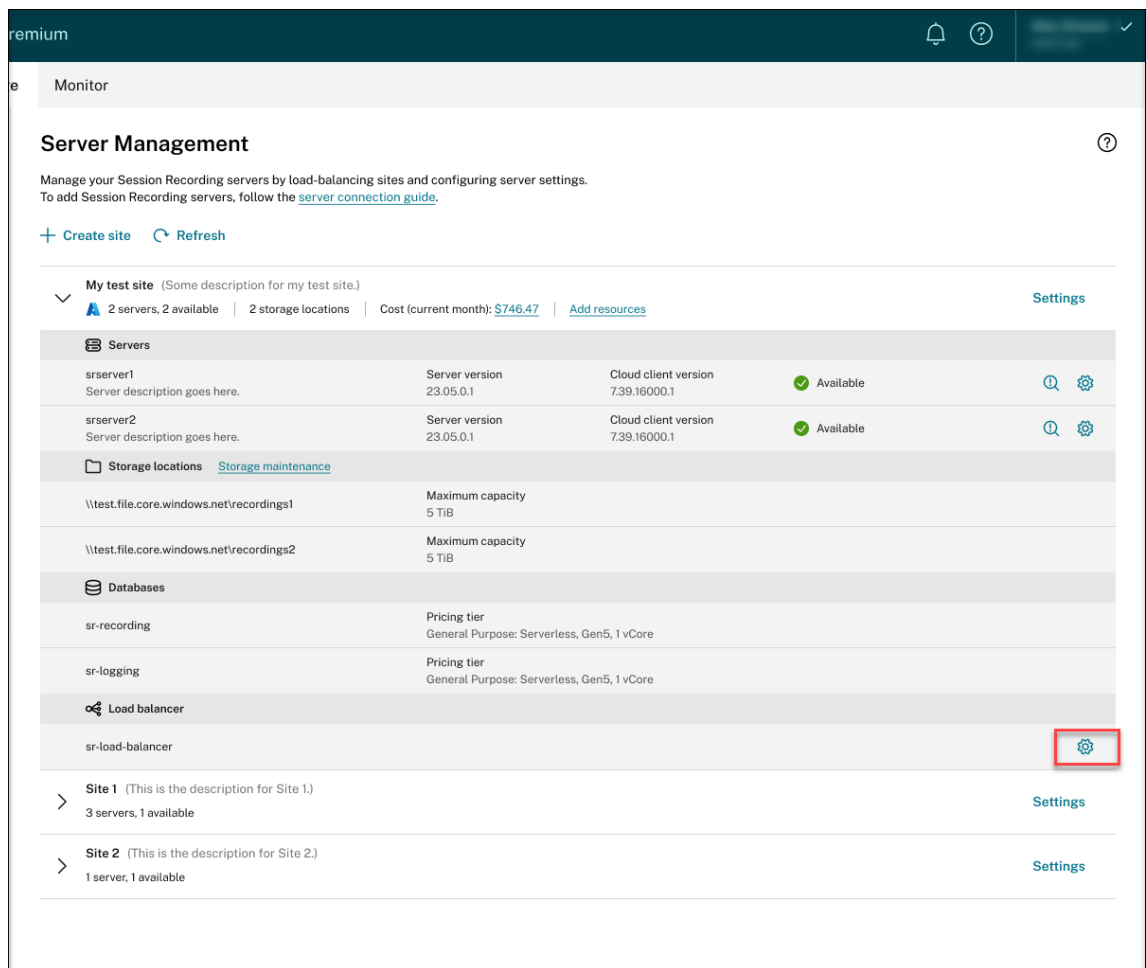
- The deployment of added resources can fail and the Session Recording service might not be able to remove these resources from your subscription. In this case, a prompt similar to the following is provided for you to take action:



Change the IP addresses that are allowed to access the load balancer

For an existing site that you have deployed on Azure **through a host connection**, you can change the IP addresses that are allowed to access the load balancer. To do so, complete the following steps:

1. Select **Configuration > Server Management** from the left navigation of the Session Recording service.
2. On the **Server Management** page, locate and unfold the target site. An Azure icon is available to represent sites deployed on Azure.
3. Click the **Settings** button in the **Load balancer** section.



- On the **Load balancer** settings page, enter the new IP addresses or ranges of your VDAs and separate them by a comma (,) in the **Restrict access of the load balancer to only the following addresses** field.

Load balancer settings ✕

Access

Restrict access of the load balancer to only the following addresses ?

Save **Cancel**

5. Click **Save**.

View actual costs for using Azure

For an existing site that you have deployed on Azure **through a host connection**, click the cost amount to view the cost details. For example:

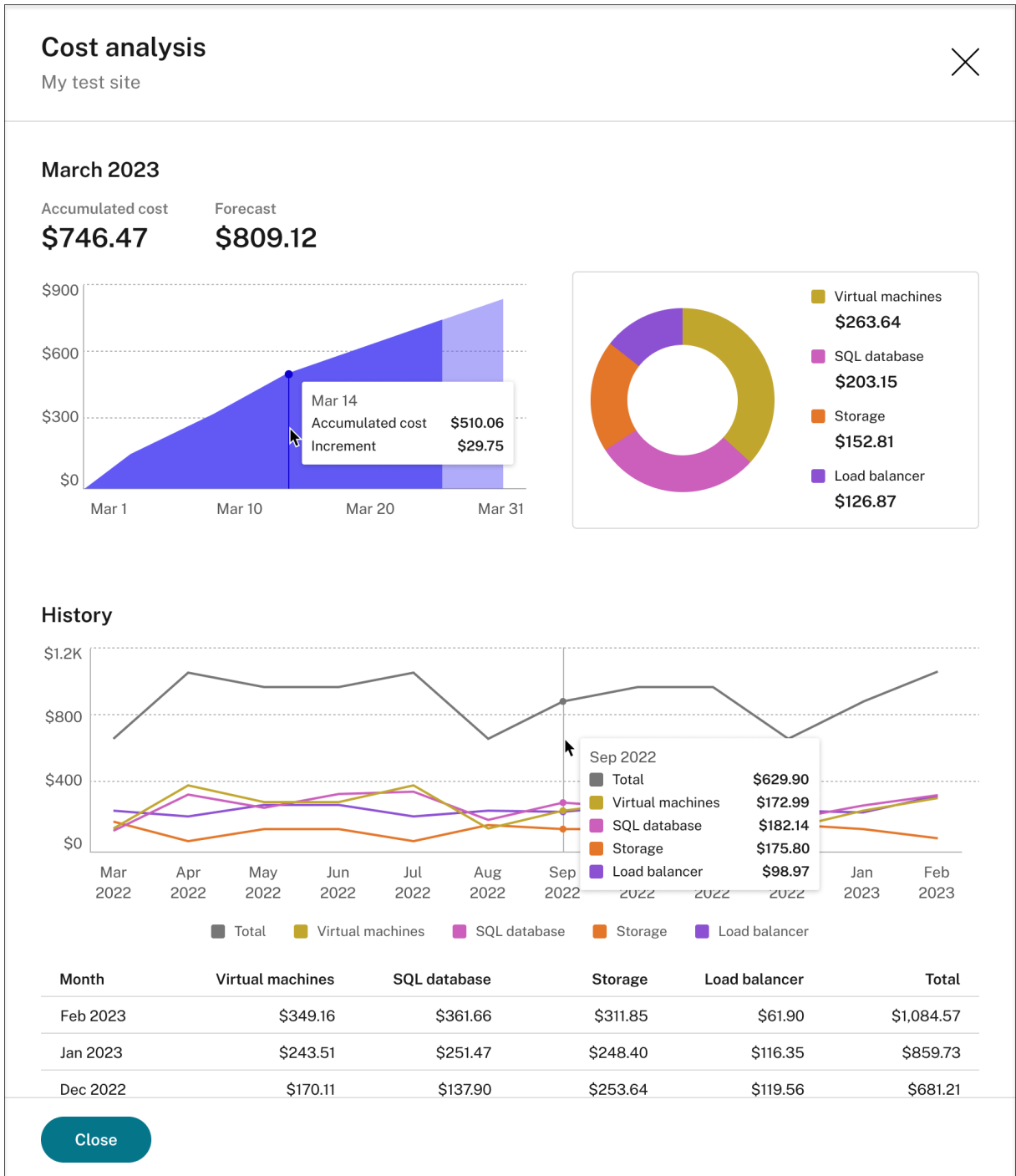
The screenshot shows the Azure portal interface for Session Recording. The main heading is "Server Management" with a subtitle "Manage your Session Recording servers by load-balancing sites and configuring server settings." Below this, there are buttons for "Create site" and "Refresh". A site named "My test site" is expanded, showing "2 servers, 2 available" and "2 storage locations". A red box highlights the "Cost (current month): \$746.47" link. Below this, there are sections for "Servers", "Storage locations", "Databases", and "Load balancer".

Servers			
sr-server-01	Server version 22.12.0.0	Cloud client version 7.36.25412.54733	Available
sr-server-02	Server version 22.12.0.0	Cloud client version 7.35.25358.46145	Available

Storage locations	
\\test.file.core.windows.net\share1	Maximum capacity 5 TiB
\\test.file.core.windows.net\share2	Maximum capacity 5 TiB

Databases	
sr-recording	Pricing tier General Purpose: Serverless, Gen5, 1 vCore
sr-logging	Pricing tier General Purpose: Serverless, Gen5, 1 vCore

Load balancer	
sr-load-balancer	



Tips for viewing the actual costs:

- When you hover on the area graph for the current month, a reference line for the date and data from that day appears as an overlay.
- The history costs of different resources are represented by line graphs. **Line graphs are available when there are at least two months of data.** When you hover on the line graphs, a reference line and cost breakdown from the month appears as an overlay. To view the line graph of

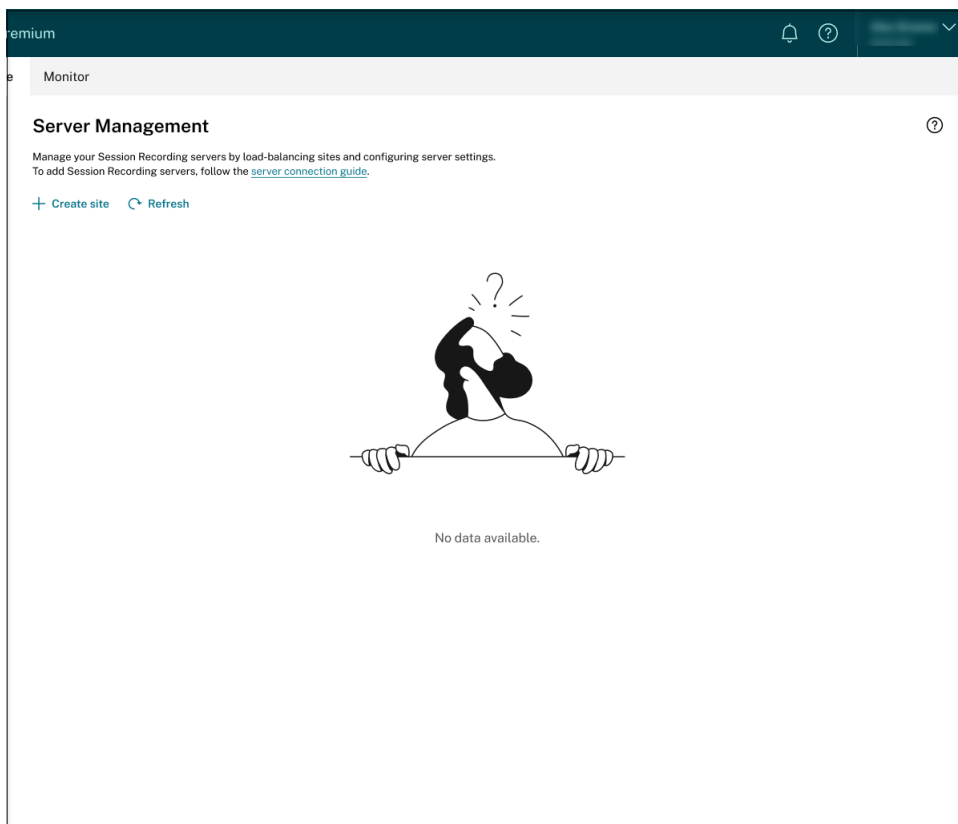
only a specific resource, hover on the resource.

Add a host connection

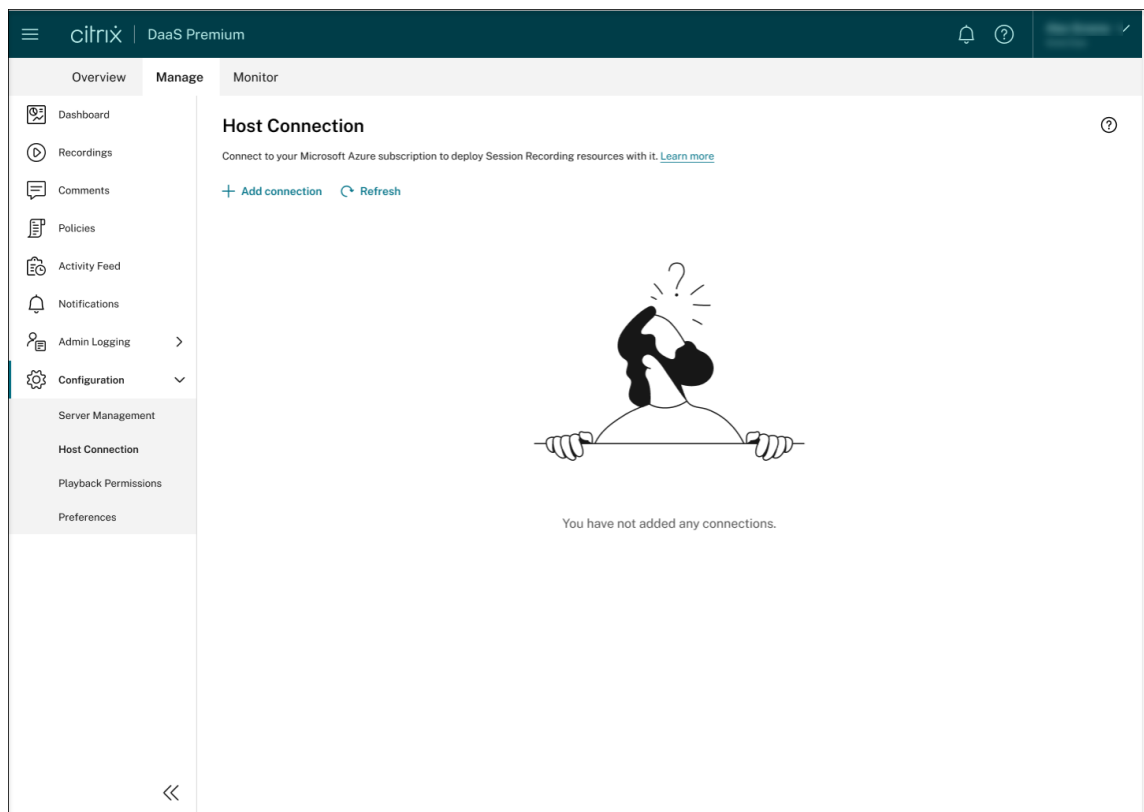
To add a host connection, complete the following steps:

1. Click **Add connection** on the **Create site** page with **Create and deploy a site through a host connection** selected. Or, click **Add connection** on the **Host Connection** page.

To access the **Create site** page, select **Configuration > Server Management** from the left navigation of the Session Recording service, and then click **Create site**.



To access the **Host Connection** page, select **Configuration > Host Connection** from the left navigation of the Session Recording service:



2. On the **Add connection** page, give the new host connection a name and a description (optional). Enter your Azure subscription ID and the following required information about your application registration:
 - Application (client) ID
 - Service principal object ID (ID of the service principal object associated with the application)
 - Directory (tenant) ID
 - Client secret
 - Secret expiration date

Add connection ✕

Name

Description (optional)

Complete the following fields to add a connection. You can obtain the information from your Azure portal.

Subscription ID


Use the subscription with which your VDAs are deployed.

Application (client) ID

Service principal object ID [?]

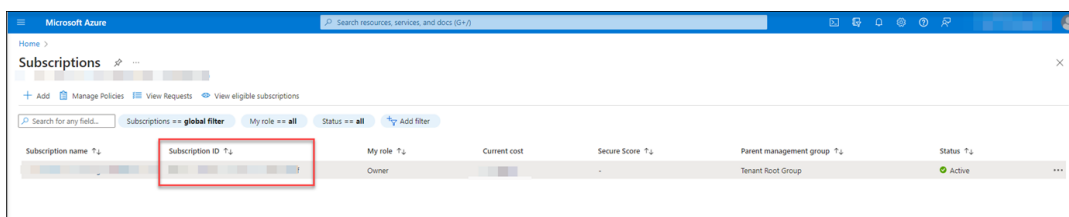
Directory (tenant) ID

Client secret

Secret expiration date


To find your Azure subscription ID, do the following:

- a) Sign in to the Azure portal.
- b) Under the **Azure services** section, select **Subscriptions**.
- c) Find your subscription in the list and copy the **Subscription ID** shown in the second column.



To obtain the required information about your application registration, do the following:

- a) (Skip this step if you already have an application registered.) Register an application with your Azure AD tenant. An application must be registered to delegate identity and access management functions to Azure AD.

There are two methods for registering an application.

Method 1:

- i. Copy the following Citrix-provided script and name it, for example, **AppRegistration.ps1**:

```

1 <#
2 .SYNOPSIS
3     Copyright (c) Citrix Systems, Inc. All Rights Reserved.
4 .DESCRIPTION
5     Create Azure app registrations and give proper
6     permissions for Citrix Session Recording service
7     deployment
8 .Parameter azureTenantID
9 .Parameter azureSubscriptionID
10 .Parameter appName
11 .Parameter role
12 #>
13 [CmdletBinding()]
14 Param(
15     [Parameter(Mandatory = $true)] [String] $tenantId,
16     [Parameter(Mandatory = $true)] [String] $subscriptionId,
17     [Parameter(Mandatory = $true)] [String] $appName,
18     [Parameter(Mandatory = $true)] [String] $role
19 )
20 if ($role -ne "Citrix Session Recording service" -and $role
21     -ne "Citrix Session Recording Deployment" -and $role -
22     ne "Contributor") {
23     throw [System.Exception] "Invalid role '$role', only
24     support 'Citrix Session Recording service', 'Citrix
25     Session Recording Deployment', and 'Contributor'."
26 }

```

```
26 try {
27
28     Get-InstalledModule -Name "Az.Accounts" -ErrorAction
        Stop
29 }
30
31 catch {
32
33     Install-Module -Name "Az.Accounts" -Scope CurrentUser -
        Repository PSGallery -SkipPublisherCheck -Force
34 }
35
36 try {
37
38     Get-InstalledModule -Name "Az.Resources" -ErrorAction
        Stop
39 }
40
41 catch {
42
43     Install-Module -Name "Az.Resources" -Scope CurrentUser
        -Repository PSGallery -SkipPublisherCheck -Force
44 }
45
46
47 Connect-AzAccount -TenantId $tenantId -Subscription
    $subscriptionId
48
49 try {
50
51
52     $azureAdApplication = Get-AzADApplication -DisplayName
        $appName
53     if ($null -eq $azureAdApplication) {
54
55         Write-Host "Create a new app registration for
            Citrix Session Recording" -ForegroundColor Green
56         $azureAdApplication = New-AzADApplication -
            DisplayName $appName -AvailableToOtherTenants
            $false
57     }
58
59     else {
60
61         Write-Host "App registration '$appName' already
            exists." -ForegroundColor Yellow
62     }
63
64
65     $azureAdApplicationServicePrincipal = Get-
        AzADServicePrincipal -DisplayName $appName
66     if($null -eq $azureAdApplicationServicePrincipal) {
67
```

```
68     $azureAdApplicationServicePrincipal = New-
        AzADServicePrincipal -AppId $azureAdApplication.
        AppId
69     Write-Host "Create a service principal for app
        registration '$appName'" -ForegroundColor Green
70     }
71     else{
72
73         Write-Host "Service principal already exists for
        app registration '$appName'" -ForegroundColor
        Yellow
74     }
75
76
77     if ($role -eq "Citrix Session Recording service" -or
        $role -eq "Citrix Session Recording Deployment") {
78
79         $rootPath = Get-Location
80         $customRolePath = $(Join-Path -Path $rootPath -
            ChildPath "sessionrecording.json") | Resolve-
            Path
81         $customRoleJson = Get-Content $customRolePath |
            ConvertFrom-Json
82         $customRoleJson.AssignableScopes[0] = "/"
            subscriptions/" + $subscriptionId
83         $tmpCustomRolePath = Join-Path -Path $rootPath -
            ChildPath "sessionrecording_tmp.json"
84
85         $roleDef = Get-AzRoleDefinition -Name $role
86         if ($null -eq $roleDef) {
87
88             try {
89
90                 $customRoleJson | ConvertTo-Json -depth 32
                    | Set-Content $tmpCustomRolePath
91                 Write-Host "Create a custom role '$role'" -
                    ForegroundColor Green
92                 New-AzRoleDefinition -InputFile
                    $tmpCustomRolePath
93             }
94
95             catch {
96
97                 Write-Host "Failed to create custom role,
                    error: $_" -ForegroundColor Red
98                 throw $_.Exception
99             }
100
101         }
102
103     else {
104
105         try {
```



```
106
107     $customRoleJson | Add-Member -MemberType
        NoteProperty -Name 'id' -Value $(
        $roleDef.Id)
108     $customRoleJson | ConvertTo-Json -depth 32
        | Set-Content $tmpCustomRolePath
109     Write-Host "Update the custom role '$role'
        " -ForegroundColor Green
110     Set-AzRoleDefinition -InputFile
        $tmpCustomRolePath
111     }
112
113     catch {
114
115         Write-Host "Failed to update custom role,
        error: $_" -ForegroundColor Red
116         throw $_.Exception
117     }
118
119     }
120
121     }
122
123
124     $roleAssignment = Get-AzRoleAssignment -
        RoleDefinitionName $role -ObjectId $(
        $azureAdApplicationServicePrincipal.Id)
125     if ($null -eq $roleAssignment) {
126
127         Write-Host "Assign role '$role' to app '$appName'"
        -ForegroundColor Green
128         New-AzRoleAssignment -RoleDefinitionName $role -
        ApplicationId $azureAdApplication.AppId
129     }
130
131     else {
132
133         Write-Host "Role '$role' already assigned to app '
        $appName'" -ForegroundColor Yellow
134     }
135
136
137     Write-Host "Tenant ID:                $tenantId" -
        ForegroundColor Green
138     Write-Host "Subscription ID:
        $subscriptionId" -ForegroundColor Green
139     Write-Host "Application ID:                $(
        $azureAdApplication.AppId)" -ForegroundColor Green
140     Write-Host "Service principal object ID: $(
        $azureAdApplicationServicePrincipal.Id)" -
        ForegroundColor Green
141 }
142
```

```
143 catch {
144
145     Write-Host "Failed to assign role assignment to this
        app, error: $_" -ForegroundColor Red
146     Write-Host "Please make sure the current azure admin
        has permission to assign roles" -ForegroundColor Red
147 }
148
149 <!--NeedCopy-->
```

- ii. Copy the following custom role file and name it **sessionrecording.json**. This custom role file helps to assign least permissions for the application to be registered.

```
1 {
2
3     "Name": "Citrix Session Recording service",
4     "Description": "Custom role for session recording
        service",
5     "AssignableScopes": [
6         "/subscriptions/*"
7     ],
8     "Actions": [
9         "Microsoft.Authorization/roleAssignments/write",
10        "Microsoft.Authorization/roleDefinitions/delete",
11        "Microsoft.Authorization/roleDefinitions/write",
12        "Microsoft.Compute/availabilitySets/write",
13        "Microsoft.Compute/virtualMachines/delete",
14        "Microsoft.Compute/virtualMachines/extensions/read"
15        ,
16        "Microsoft.Compute/virtualMachines/extensions/write"
17        ,
18        "Microsoft.Compute/virtualMachines/read",
19        "Microsoft.Compute/virtualMachines/runCommands/read"
20        ,
21        "Microsoft.Compute/virtualMachines/runCommands/
22        write",
23        "Microsoft.Compute/virtualMachines/write",
24        "Microsoft.CostManagement/forecast/read",
25        "Microsoft.CostManagement/query/read",
26        "Microsoft.KeyVault/locations/deletedVaults/purge/
27        action",
28        "Microsoft.KeyVault/vaults/read",
29        "Microsoft.KeyVault/vaults/write",
30        "Microsoft.ManagedIdentity/userAssignedIdentities/
        assign/action",
        "Microsoft.ManagedIdentity/userAssignedIdentities/
        read",
        "Microsoft.ManagedIdentity/userAssignedIdentities/
        write",
        "Microsoft.Network/loadBalancers/
        backendAddressPools/join/action",
        "Microsoft.Network/loadBalancers/write",
        "Microsoft.Network/networkInterfaces/join/action",
```

```
31     "Microsoft.Network/networkInterfaces/read",
32     "Microsoft.Network/networkInterfaces/write",
33     "Microsoft.Network/networkSecurityGroups/delete",
34     "Microsoft.Network/networkSecurityGroups/join/
35         action",
36     "Microsoft.Network/networkSecurityGroups/read",
37     "Microsoft.Network/networkSecurityGroups/
38         securityRules/read",
39     "Microsoft.Network/networkSecurityGroups/
40         securityRules/write",
41     "Microsoft.Network/networkSecurityGroups/write",
42     "Microsoft.Network/publicIPAddresses/join/action",
43     "Microsoft.Network/publicIPAddresses/read",
44     "Microsoft.Network/publicIPAddresses/write",
45     "Microsoft.Network/virtualNetworks/read",
46     "Microsoft.Network/virtualNetworks/subnets/join/
47         action",
48     "Microsoft.Network/virtualNetworks/subnets/read",
49     "Microsoft.Resources/deployments/operationstatuses/
50         read",
51     "Microsoft.Resources/deployments/read",
52     "Microsoft.Resources/deployments/write",
53     "Microsoft.Resources/subscriptions/resourceGroups/
54         delete",
55     "Microsoft.Resources/subscriptions/resourceGroups/
56         read",
57     "Microsoft.Resources/subscriptions/resourceGroups/
58         write",
59     "Microsoft.Sql/servers/auditingSettings/write",
60     "Microsoft.Sql/servers/databases/write",
61     "Microsoft.Sql/servers/firewallRules/write",
62     "Microsoft.Sql/servers/read",
63     "Microsoft.Sql/servers/write",
64     "Microsoft.Storage/storageAccounts/fileServices/
65         shares/delete",
66     "Microsoft.Storage/storageAccounts/fileServices/
67         shares/write",
68     "Microsoft.Storage/storageAccounts/listkeys/action"
69     ,
70     "Microsoft.Storage/storageAccounts/read",
71     "Microsoft.Storage/storageAccounts/write"
72 ],
73 "NotActions": [
74 ],
75 "DataActions": [
76 ],
77 "NotDataActions": [
78 ]
79 }
```

```
73 <!--NeedCopy-->
```

- iii. Put **AppRegistration.ps1** and **sessionrecording.json** in the same folder.
- iv. Run either of the following commands as needed.

To create an application and assign it least permissions with the preceding custom role file (**sessionrecording.json**), run:

```
1 .\AppRegistration.ps1 -tenantId <tenant ID> -subscriptionId
  <subscription ID> -appName <application name> -role "
  Citrix Session Recording service"
2 <!--NeedCopy-->
```

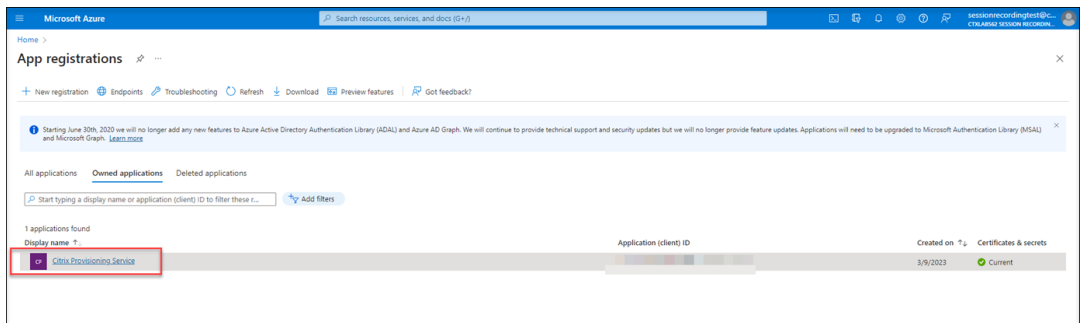
To create an application and assign it the Azure built-in **Contributor** role, run:

```
1 .\AppRegistration.ps1 -tenantId <tenant ID> -subscriptionId
  <subscription ID> -appName <application name> -role "
  Contributor"
2 <!--NeedCopy-->
```

Method 2:

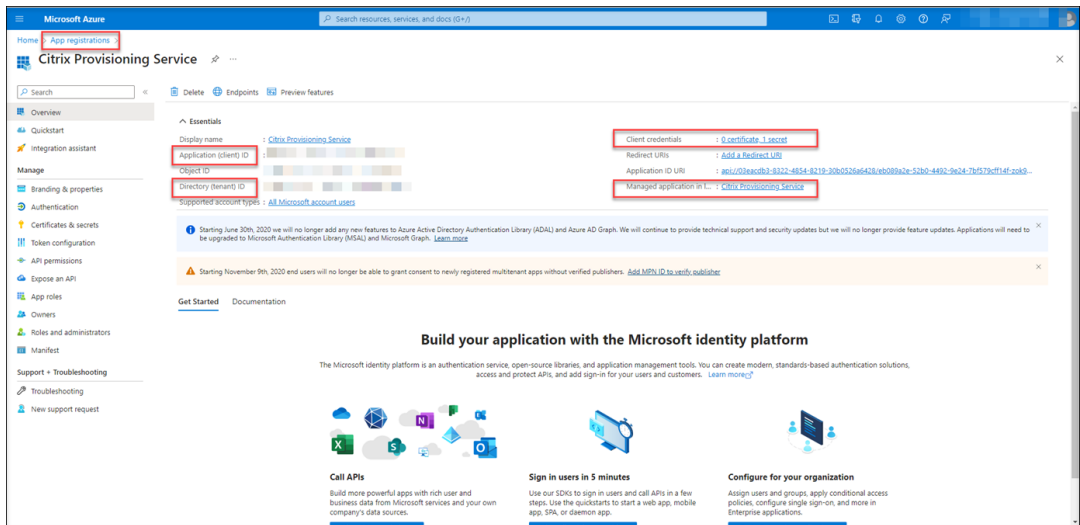
Go to the Azure portal and register an application by yourself. Grant proper permissions to the application. For the least permissions that are required, see the **sessionrecording.json** file in **Method 1**.

- b) Click the display name of your application.

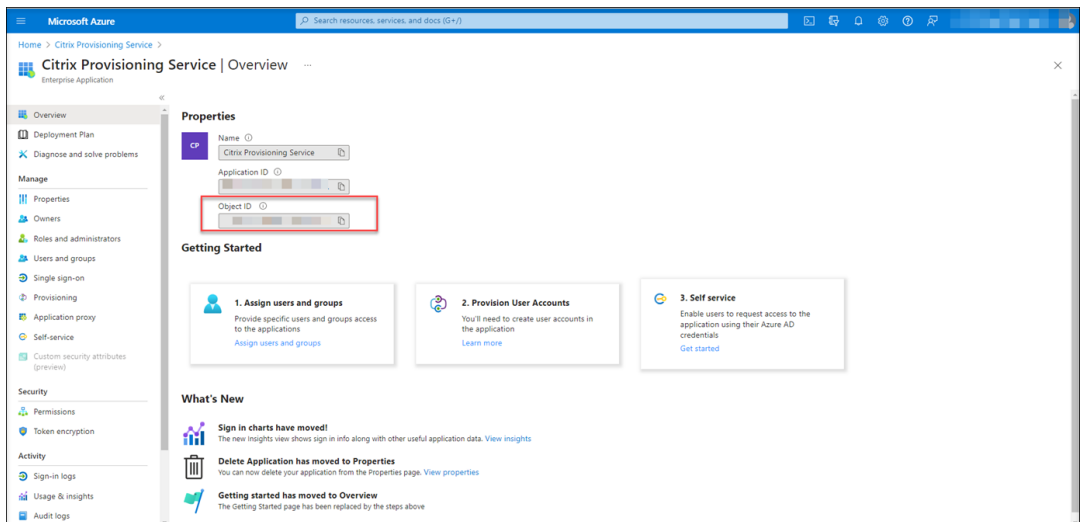


- c) On the overview page, find the application (client) ID and directory (tenant) ID. Click the link next to **Managed application in local directory** to find the ID of the service principal object associated with the application. Click the link next to **Client credentials** to find the client secret ID and its expiration date.

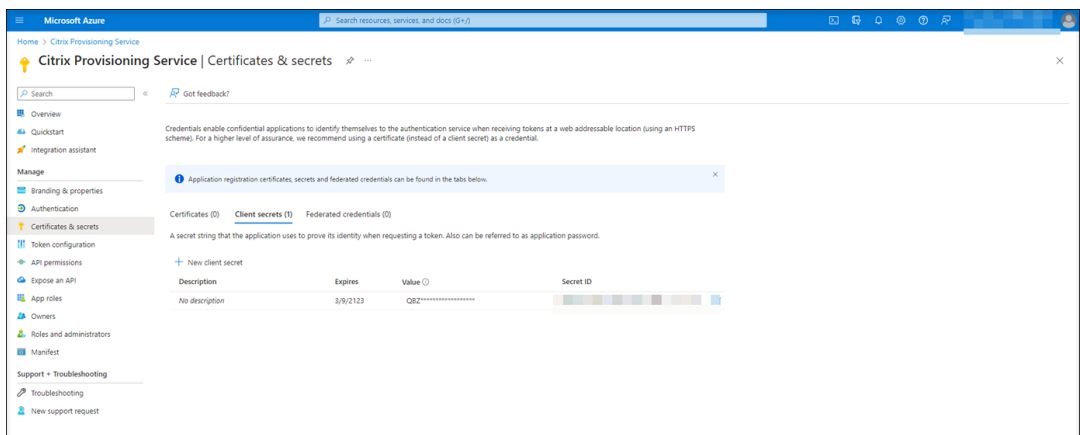
Session Recording service



For example, the ID of the service principal object associated with the application:



For example, the client secret ID and its expiration date:



3. Click **Save** to test whether the host connection you specify is available.

If the host connection you specify is available, you're taken back to the **Host Connection** page and prompted that the host connection is added successfully.

The Session Recording service reminds you of expired and expiring client secrets using error and warning icons, respectively. You can click the corresponding host connection and click **Change secret** on the **Connection details** page to update the client secret and its expiration date.

The screenshot shows the 'Host Connection' page in the Session Recording service. A table lists several connections, with 'BDTestTurnKey' highlighted. A red box highlights the warning icon (a triangle with an exclamation mark) next to its expiration date, '7/22/2023'. To the right, the 'Connection details' panel is open, showing the 'BDTestTurnKey' details. A red box highlights the 'Change secret' button at the bottom of the details panel, which is also accompanied by a warning icon and the text 'The secret is expiring in 6 days.'

Name	Description	Secret expiration date
AJJ-TEST	test	8/30/2023
APIAutoTestTurnkey	APIAutoTestTurnkeyDescription	8/25/2023
APIAutoTestTurnkey	APIAutoTestTurnkeyDescription	8/30/2023
BDTestTurnKey	testing0628	7/22/2023
Curry Bi		7/8/2023
Hui	ss	7/13/2023
Huijn-TEST	Huijn test	8/28/2023
UIAutoTest202306261702	UIAutoTestDescription	8/25/2023
UIAutoTest202306261721	UIAutoTestDescription	8/25/2023
UIAutoTest202306261733	UIAutoTestDescription	8/25/2023

Connection details

Name: BDTestTurnKey

Description: testing0628

Subscription ID: eb0889a2e-52b0-449d-9e24-7bf579cff14f

Application (client) ID: 79a82451-c782-4734-832c-48e594a5ce0e

Service principal object ID: da94d8ae-55e8-4d9d-9213-88d9def63c33

Directory (tenant) ID: 03eacdb3-8322-4854-8219-30b0526a6428

Secret expiration date: 7/22/2023

The secret is expiring in 6 days.

Change secret

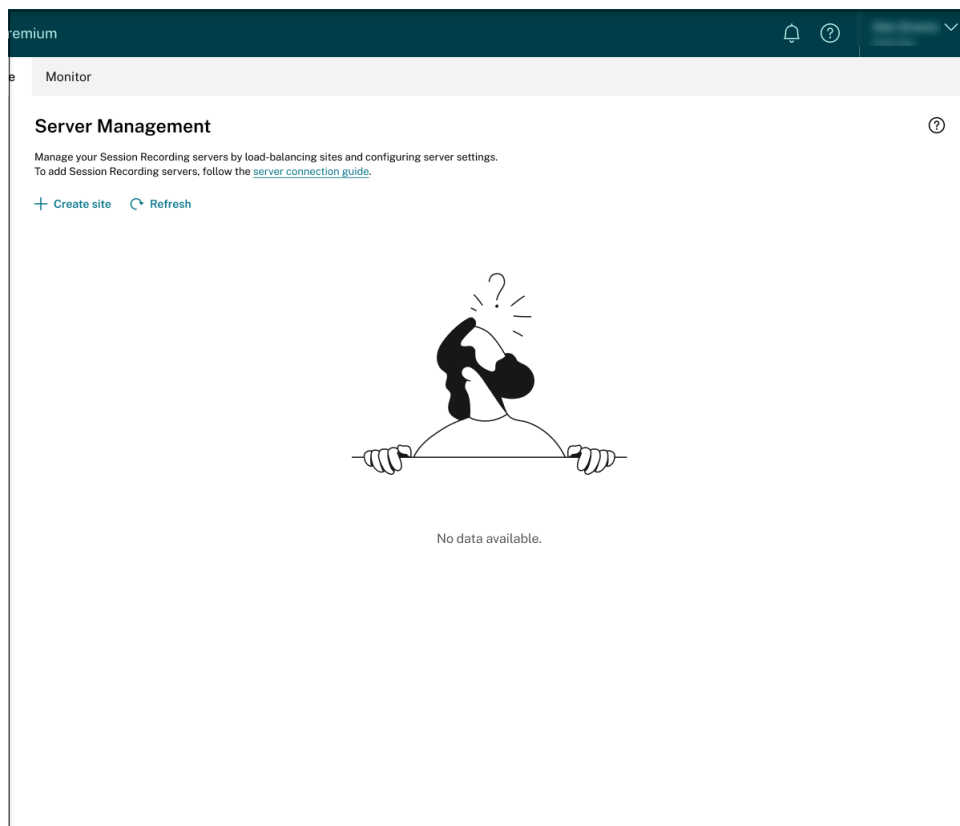
Create and deploy a site through an ARM template

You can create an Azure Resource Manager template (ARM template) to deploy Session Recording resources in Azure. The following are the main steps to achieve this goal:

1. Create an ARM template in the Session Recording service. The ARM template is a JavaScript Object Notation (JSON) file that contains how and which resources you want to deploy.
2. Download and unzip the ARM template. Run the deployment script in the unzipped template folder to start deploying the resources specified in the template to Azure.
3. Check the deployment progress in Azure. After the deployment is complete, set up Session Recording to get it up and running. To set up Session Recording, you need to specify the version of the Session Recording server to install and upload the **resourceInfo.json** file.

The specific steps are as follows:

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



2. On the **Server Management** page, click **Create site**. The **Create Site** page appears.

Create site [Close]

1 Site information

What would you like to do?

- Create an empty site**
Create a site and add servers later.
- Create and deploy a site through a host connection**
Deploy Session Recording resources using a host connection that connects to your specific cloud subscription. [Learn more](#)
- Create and deploy a site through an ARM template**
Create an Azure Resource Manager template (ARM template) to deploy Session Recording resources in Azure. [Learn more](#)

Site name
Name this site

Description (optional)
Enter description

Save Cancel [Help 8]

3. Select **Create and deploy a site through an ARM template**. The main steps are listed in the left navigation.

Downloads

Create site

- 1 Site information
- 2 About your deployment
Optional
- 3 Network
- 4 Virtual machines
- 5 Domain and certificate
- 6 Storage
- 7 Databases
- 8 Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

What would you like to do?

- Create an empty site**
Create a site and add servers later.
- Create and deploy a site through a host connection**
Deploy Session Recording resources using a host connection that connects to your specific cloud subscription. [Learn more](#)
- Create and deploy a site through an ARM template**
Create an Azure Resource Manager template (ARM template) to deploy Session Recording resources in Azure. [Learn more](#)

Site name

Description (optional)

Region

All your resources will be created in this region.

Next **Cancel**

4. Enter a site name and description, and then click **Next**.
5. (Optional) To get recommendations for VM and storage configurations, provide information about your recording needs.

You can skip this step by clicking **I'm good, skip this step** or by clicking **Next** with nothing selected.

Create site ✕

1 Site information

2 About your deployment Optional

3 Network

4 Virtual machines

5 Domain and certificate

6 Storage

7 Databases

8 Load balancer

9 Tags Optional

10 Secure client

11 Summary

Tell us about your recording needs, so we can provide some recommendations for your VM and storage configurations.

[I'm good, skip this step.](#)

The following information helps determine the recommended number of Session Recording servers.

How many concurrent sessions do you have at most?

4,000-6,000

Recommended number of servers: 3 [reset](#)

The following information helps determine the recommended storage capacity.

How much visual movement do your sessions typically have?

Some, the display changes but not drastically

How many sessions do you need to record per day?

5,000-10,000

For how long do you need to retain each recording file?

15-30 days

Recommended storage capacity: 30 TiB [reset](#)

[Next](#) [Cancel](#) 8

When you select an option from the drop-down list, a recommendation is presented according to your selection. A **reset** button is available next to the recommendation. It lets you clear your selections and the corresponding recommendation in that section.

6. Go to the Azure portal and create a new virtual network in the region you selected and set up virtual network peering between the new virtual network and the one that your VDAs are connected to. Then, add a subnet in the new virtual network. Find and enter the subnet ID below.

The screenshot shows the 'Create site' wizard in the Azure portal. The wizard is titled 'Create site' and has a close button (X) in the top right corner. On the left side, there is a vertical list of steps: 1. Site information (checked), 2. About your deployment (Optional, checked), 3. Network (selected), 4. Virtual machines, 5. Domain and certificate, 6. Storage, 7. Databases, 8. Load balancer, 9. Tags (Optional), 10. Secure client, and 11. Summary. The main content area is for the 'Network' step. It contains the following text: 'Before you continue, head over to Azure and create a new virtual network in the region you selected and set up virtual network peering between the new virtual network and the one that your VDAs are connected to. Then, add a subnet in the new virtual network and enter the subnet ID below. This will be the subnet for your Session Recording resources to connect to.' Below this text is a link: '[How to find the subnet ID?](#)'. There is a 'Subnet ID' label followed by a text input field containing the placeholder text 'Enter Subnet ID'. Below the input field is a checkbox labeled 'Create private endpoints for storage and databases'. A blue information box with an 'i' icon contains the text: 'Use this option if you need to keep the connections between resources within the private network.' At the bottom of the wizard, there are two buttons: 'Next' (dark blue) and 'Cancel' (light blue). In the bottom right corner, there is a purple circular icon with a white book symbol and a red 'B' notification badge.

To keep the connections between resources within the private network, select the **Create private endpoints for storage and databases** check box.

After you select the **Create private endpoints for storage and databases** check box, decide on whether to enter another subnet ID by taking the following into consideration:

- If you do not plan to join your Session Recording servers to an Active Directory domain, the subnet is not needed and thus leave the subnet ID field empty.
- If you leave the subnet ID field empty, you are joining your Session Recording servers to an Azure Active Directory domain.

Create site [X]

- Site information
- About your deployment (Optional)
- 3 Network**
- 4 Virtual machines
- 5 Domain and certificate
- 6 Storage
- 7 Databases
- 8 Load balancer
- 9 Tags (Optional)
- 10 Secure client
- 11 Summary

Before you continue, head over to Azure and create a new virtual network in the region you selected and set up virtual network peering between the new virtual network and the one that your VDAs are connected to. Then, add a subnet in the new virtual network and enter the subnet ID below. This will be the subnet for your Session Recording resources to connect to.

[How to find the subnet ID?](#)

Subnet ID
Enter Subnet ID

Create private endpoints for storage and databases

Using private endpoints requires a DNS private resolver, which needs a dedicated subnet. In the same virtual network you created, add another subnet and enter its ID below.

Note: If you do not plan to join your Session Recording servers to an Active Directory domain, the subnet is not needed.

Subnet ID
Enter Subnet ID

Estimated cost (per month)
\$182.5

Next Cancel [8]

7. (Skip this step if you already have an application registered.) Register an application with your Azure AD tenant. An application must be registered to delegate identity and access management functions to Azure AD.

There are two methods for registering an application.

Method 1:

- a) Copy the following Citrix-provided script and name it, for example, **AppRegistration.ps1**:

```

1 <#
2 .SYNOPSIS
3     Copyright (c) Citrix Systems, Inc. All Rights Reserved.
4 .DESCRIPTION
5     Create Azure app registrations and give proper permissions
6     for Citrix Session Recording service deployment
7 .Parameter azureTenantID
8 .Parameter azureSubscriptionID
9 .Parameter appName
10 .Parameter role
11 #>
12 [CmdletBinding()]
13 Param(
14     [Parameter(Mandatory = $true)] [String] $tenantId,
```

```
15     [Parameter(Mandatory = $true)] [String] $subscriptionId,
16     [Parameter(Mandatory = $true)] [String] $appName,
17     [Parameter(Mandatory = $true)] [String] $role
18 )
19
20 if ($role -ne "Citrix Session Recording service" -and $role -
    ne "Citrix Session Recording Deployment" -and $role -ne "
    Contributor") {
21
22     throw [System.Exception] "Invalid role '$role', only
        support 'Citrix Session Recording service', 'Citrix
        Session Recording Deployment', and 'Contributor'."
23 }
24
25
26 try {
27
28     Get-InstalledModule -Name "Az.Accounts" -ErrorAction Stop
29 }
30
31 catch {
32
33     Install-Module -Name "Az.Accounts" -Scope CurrentUser -
        Repository PSGallery -SkipPublisherCheck -Force
34 }
35
36 try {
37
38     Get-InstalledModule -Name "Az.Resources" -ErrorAction Stop
39 }
40
41 catch {
42
43     Install-Module -Name "Az.Resources" -Scope CurrentUser -
        Repository PSGallery -SkipPublisherCheck -Force
44 }
45
46
47 Connect-AzAccount -TenantId $tenantId -Subscription
    $subscriptionId
48
49 try {
50
51
52     $azureAdApplication = Get-AzADApplication -DisplayName
        $appName
53     if ($null -eq $azureAdApplication) {
54
55         Write-Host "Create a new app registration for Citrix
            Session Recording" -ForegroundColor Green
56         $azureAdApplication = New-AzADApplication -DisplayName
            $appName -AvailableToOtherTenants $false
57     }
```

```
58
59     else {
60
61         Write-Host "App registration '$appName' already exists
62             ." -ForegroundColor Yellow
63     }
64
65     $azureAdApplicationServicePrincipal = Get-
66         AzADServicePrincipal -DisplayName $appName
67     if($null -eq $azureAdApplicationServicePrincipal) {
68
69         $azureAdApplicationServicePrincipal = New-
70             AzADServicePrincipal -AppId $azureAdApplication.
71             AppId
72         Write-Host "Create a service principal for app
73             registration '$appName'" -ForegroundColor Green
74     }
75     else{
76
77         Write-Host "Service principal already exists for app
78             registration '$appName'" -ForegroundColor Yellow
79     }
80
81     if ($role -eq "Citrix Session Recording service" -or $role
82         -eq "Citrix Session Recording Deployment") {
83
84         $rootPath = Get-Location
85         $customRolePath = $(Join-Path -Path $rootPath -
86             ChildPath "sessionrecordingdeployment.json") |
87             Resolve-Path
88         $customRoleJson = Get-Content $customRolePath |
89             ConvertFrom-Json
90         $customRoleJson.AssignableScopes[0] = "/subscriptions/
91             " + $subscriptionId
92         $tmpCustomRolePath = Join-Path -Path $rootPath -
93             ChildPath "sessionrecording_tmp.json"
94
95         $roleDef = Get-AzRoleDefinition -Name $role
96         if ($null -eq $roleDef) {
97
98             try {
99
100                 $customRoleJson | ConvertTo-Json -depth 32 |
101                     Set-Content $tmpCustomRolePath
102                 Write-Host "Create a custom role '$role'" -
103                     ForegroundColor Green
104                 New-AzRoleDefinition -InputFile
105                     $tmpCustomRolePath
106             }
107
108             catch {
```

```
96
97     Write-Host "Failed to create custom role,
98         error: $_" -ForegroundColor Red
99     throw $_.Exception
100 }
101 }
102
103 else {
104
105     try {
106
107         $customRoleJson | Add-Member -MemberType
108             NoteProperty -Name 'id' -Value $($roleDef.
109                 Id)
110         $customRoleJson | ConvertTo-Json -depth 32 |
111             Set-Content $tmpCustomRolePath
112         Write-Host "Update the custom role '$role'" -
113             ForegroundColor Green
114         Set-AzRoleDefinition -InputFile
115             $tmpCustomRolePath
116     }
117
118     catch {
119
120         Write-Host "Failed to update custom role,
121             error: $_" -ForegroundColor Red
122         throw $_.Exception
123     }
124 }
125
126 $roleAssignment = Get-AzRoleAssignment -RoleDefinitionName
127     $role -ObjectId $($azureAdApplicationServicePrincipal.
128         Id)
129 if ($null -eq $roleAssignment) {
130
131     Write-Host "Assign role '$role' to app '$appName'" -
132         ForegroundColor Green
133     New-AzRoleAssignment -RoleDefinitionName $role -
134         ApplicationId $azureAdApplication.AppId
135 }
136
137 else {
138
139     Write-Host "Role '$role' already assigned to app '
140         $appName'" -ForegroundColor Yellow
141 }
142 }
```

```
137 Write-Host "Tenant ID:                $tenantId" -
    ForegroundColor Green
138 Write-Host "Subscription ID:          $subscriptionId"
    -ForegroundColor Green
139 Write-Host "Application ID:            $(
    $azureAdApplication.AppId)" -ForegroundColor Green
140 Write-Host "Service principal object ID: $(
    $azureAdApplicationServicePrincipal.Id)" -
    ForegroundColor Green
141 }
142
143 catch {
144
145     Write-Host "Failed to assign role assignment to this app,
    error: $_" -ForegroundColor Red
146     Write-Host "Please make sure the current azure admin has
    permission to assign roles" -ForegroundColor Red
147 }
148
149 <!--NeedCopy-->
```

- b) Copy the following custom role file and name it **sessionrecordingdeployment.json**. This custom role file helps to assign least permissions for the application to be registered.

```
1 {
2
3     "name": "Citrix Session Recording Deployment",
4     "description": "This role has permissions which allow
    users to deploy Session Recording resources using an
    Azure Resource Manager template (ARM template). ",
5     "assignableScopes": [
6         "/subscriptions/*"
7     ],
8     "actions": [
9         "Microsoft.Compute/availabilitySets/write",
10        "Microsoft.Compute/virtualMachines/extensions/read",
11        "Microsoft.Compute/virtualMachines/extensions/write",
12        "Microsoft.Compute/virtualMachines/read",
13        "Microsoft.Compute/virtualMachines/runCommands/read",
14        "Microsoft.Compute/virtualMachines/runCommands/write",
15        "Microsoft.Compute/virtualMachines/write",
16        "Microsoft.ContainerInstance/containerGroups/read",
17        "Microsoft.ContainerInstance/containerGroups/write",
18        "Microsoft.KeyVault/vaults/
    PrivateEndpointConnectionsApproval/action",
19        "Microsoft.KeyVault/vaults/read",
20        "Microsoft.KeyVault/vaults/secrets/read",
21        "Microsoft.KeyVault/vaults/secrets/write",
22        "Microsoft.KeyVault/vaults/write",
23        "Microsoft.ManagedIdentity/userAssignedIdentities/assign
    /action",
24        "Microsoft.ManagedIdentity/userAssignedIdentities/read",
25        "Microsoft.ManagedIdentity/userAssignedIdentities/write"
```



```
26     ,
27     "Microsoft.Network/dnsForwardingRulesets/forwardingRules
28     /read",
29     "Microsoft.Network/dnsForwardingRulesets/forwardingRules
30     /write",
31     "Microsoft.Network/dnsForwardingRulesets/read",
32     "Microsoft.Network/dnsForwardingRulesets/
33     virtualNetworkLinks/read",
34     "Microsoft.Network/dnsForwardingRulesets/
35     virtualNetworkLinks/write",
36     "Microsoft.Network/dnsForwardingRulesets/write",
37     "Microsoft.Network/dnsResolvers/outboundEndpoints/join/
38     action",
39     "Microsoft.Network/dnsResolvers/outboundEndpoints/read",
40     "Microsoft.Network/dnsResolvers/outboundEndpoints/write"
41     ,
42     "Microsoft.Network/dnsResolvers/read",
43     "Microsoft.Network/dnsResolvers/write",
44     "Microsoft.Network/loadBalancers/backendAddressPools/
45     join/action",
46     "Microsoft.Network/loadBalancers/write",
47     "Microsoft.Network/networkInterfaces/join/action",
48     "Microsoft.Network/networkInterfaces/read",
49     "Microsoft.Network/networkInterfaces/write",
50     "Microsoft.Network/networkSecurityGroups/join/action",
51     "Microsoft.Network/networkSecurityGroups/read",
52     "Microsoft.Network/networkSecurityGroups/securityRules/
53     read",
54     "Microsoft.Network/networkSecurityGroups/securityRules/
55     write",
56     "Microsoft.Network/networkSecurityGroups/write",
57     "Microsoft.Network/privateDnsZones/join/action",
58     "Microsoft.Network/privateDnsZones/read",
59     "Microsoft.Network/privateDnsZones/virtualNetworkLinks/
60     read",
61     "Microsoft.Network/privateDnsZones/virtualNetworkLinks/
62     write",
63     "Microsoft.Network/privateDnsZones/write",
64     "Microsoft.Network/privateEndpoints/privateDnsZoneGroups
65     /read",
66     "Microsoft.Network/privateEndpoints/privateDnsZoneGroups
67     /write",
68     "Microsoft.Network/privateEndpoints/read",
69     "Microsoft.Network/privateEndpoints/write",
70     "Microsoft.Network/publicIPAddresses/join/action",
71     "Microsoft.Network/publicIPAddresses/read",
72     "Microsoft.Network/publicIPAddresses/write",
73     "Microsoft.Network/virtualNetworks/join/action",
74     "Microsoft.Network/virtualNetworks/read",
75     "Microsoft.Network/virtualNetworks/subnets/join/action",
76     "Microsoft.Network/virtualNetworks/subnets/read",
77     "Microsoft.Resources/deploymentScripts/read",
78     "Microsoft.Resources/deploymentScripts/write",
```

```
65     "Microsoft.Resources/deployments/operationstatuses/read"
66     ,
67     "Microsoft.Resources/deployments/read",
68     "Microsoft.Resources/deployments/validate/action",
69     "Microsoft.Resources/deployments/write",
70     "Microsoft.Resources/subscriptions/resourceGroups/read",
71     "Microsoft.Resources/subscriptions/resourceGroups/write"
72     ,
73     "Microsoft.Resources/templateSpecs/read",
74     "Microsoft.Resources/templateSpecs/versions/read",
75     "Microsoft.Resources/templateSpecs/versions/write",
76     "Microsoft.Resources/templateSpecs/write",
77     "Microsoft.Sql/servers/auditingSettings/write",
78     "Microsoft.Sql/servers/databases/write",
79     "Microsoft.Sql/servers/firewallRules/write",
80     "Microsoft.Sql/servers/
81     privateEndpointConnectionsApproval/action",
82     "Microsoft.Sql/servers/read",
83     "Microsoft.Sql/servers/write",
84     "Microsoft.Storage/storageAccounts/
85     PrivateEndpointConnectionsApproval/action",
86     "Microsoft.Storage/storageAccounts/blobServices/
87     containers/read",
88     "Microsoft.Storage/storageAccounts/blobServices/
89     containers/write",
90     "Microsoft.Storage/storageAccounts/fileServices/shares/
91     write",
92     "Microsoft.Storage/storageAccounts/listkeys/action",
93     "Microsoft.Storage/storageAccounts/read",
94     "Microsoft.Storage/storageAccounts/write"
95 ],
96 "notActions": [],
97 "dataActions": [],
98 "notDataActions": []
99 }
100 <!--NeedCopy-->
```

- c) Put **AppRegistration.ps1** and **sessionrecordingdeployment.json** in the same folder.
- d) Run either of the following commands as needed.

To create an application and assign it least permissions with the preceding custom role file (**sessionrecordingdeployment.json**), run:

```
1 .\AppRegistration.ps1 -tenantId <tenant ID> -subscriptionId <
2 subscription ID> -appName <application name> -role "Citrix
3 Session Recording Deployment"
4 <!--NeedCopy-->
```

To create an application and assign it the Azure built-in **Contributor** role, run:

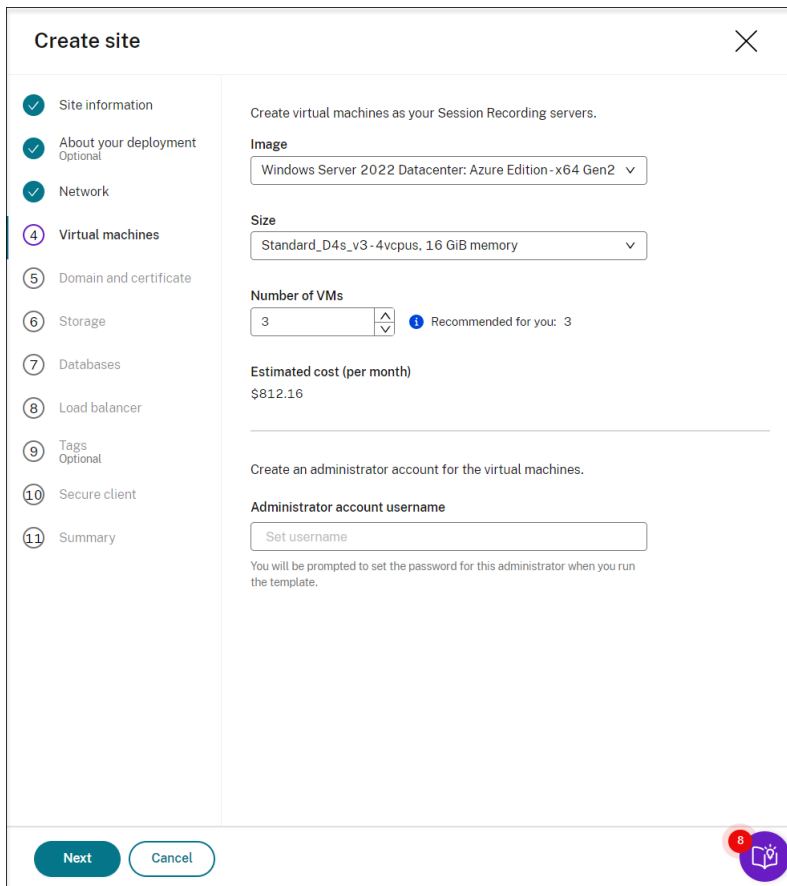
```
1 .\AppRegistration.ps1 -tenantId <tenant ID> -subscriptionId <
```

```
subscription ID> -appName <application name> -role "
Contributor"
2 <!--NeedCopy-->
```

Method 2:

Go to the Azure portal and register an application by yourself. Grant proper permissions to the application. For the least permissions that are required, see the **sessionrecordingdeployment.json** file in **Method 1**.

- Specify configurations for your Session Recording servers to be installed later.



Note:

- The **Number of VMs** field is prefilled with the recommended number if there's one. Change the number as needed.
- Estimated costs are based on standard pricing and don't take discounts into consideration. You can expect lower actual costs than estimated.

- Join the Session Recording servers to the same domain with your VDAs and specify a certificate for the Session Recording servers.

- If your VDAs connect to an Active Directory domain, select the **Join servers to an Active Directory domain** check box and enter the relevant information.
- If your VDAs connect to an Azure Active Directory (Azure AD) domain, clear the **Join servers to an Active Directory domain** check box. After you complete creating the current site, make sure to manually join the Session Recording servers to the same Azure AD domain. Notice that pure Azure AD deployment is available only for Session Recording 2402 and later.

Create site [Close]

Progress: 1 Site information, 2 About your deployment (Optional), 3 Network, 4 Virtual machines, **5 Domain and certificate**, 6 Storage, 7 Databases, 8 Load balancer, 9 Tags (Optional), 10 Secure client, 11 Summary

Join servers to an Active Directory domain
This should be the domain where your VDAs reside.

Domain name
Enter domain name

Domain controller IP address
Enter IP address

Username
Enter domain\username
Specify a domain user with sufficient rights to join machines to the domain.

Password
Enter password

Specify a certificate for the virtual machines to use. Only .pfx files are supported.

Certificate
Browse

Certificate password
Enter password

Next Cancel [Help 8]

Create site ✕

- ✓ Site information
- ✓ About your deployment
Optional
- ✓ Network
- ✓ Virtual machines
- 5** Domain and certificate
- 6 Storage
- 7 Databases
- 8 Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

Join servers to an Active Directory domain


✖ Supported only on Session Recording server version 2402 or later. Please select a compatible version in the previous step. [Go back](#)

Specify a certificate for the virtual machines to use. Only .pfx files are supported.

Certificate
[Browse](#)

Certificate password
Enter password

[Next](#) [Cancel](#)



10. Configure an Azure storage account and file shares to store your recording files. For pricing information, see [Azure Files pricing](#).

Create site

- Site information
- About your deployment
Optional
- Network
- Virtual machines
- Domain and certificate
- Storage**
- Databases
- Load balancer
- Tags
Optional
- Secure client
- Summary

Configure a storage account and file shares to store your recording files. For pricing information, see [Azure File Pricing](#).

i A separate storage account will be created for your archived recordings, which does not generate any cost if not used.

Storage account

Performance

Standard: Recommended for most scenarios (general-purpose v2 account).
 Premium: Recommended for scenarios that requires low latency.

Redundancy

Locally-redundant storage (LRS)

File shares

Tier

Transaction optimized

Maximum capacity

5 TiB

Number of file shares

6 **i** Recommended for you: 6

Estimated cost (per month)

\$1843.2 (max.)
\$0.06 per used GiB, actual cost depends on your usage.

Next **Cancel**

11. Create two SQL databases in Azure. One is used as the Session recording database (named **sessionrecording**) and the other as the administrator logging database (named **sessionrecordinglogging**).

Create site

- Site information
- About your deployment
Optional
- Network
- Virtual machines
- Domain and certificate
- Storage
- Databases**
- Load balancer
- Tags
Optional
- Secure client
- Summary

Create 2 SQL databases for recording and logging data, respectively.

Compute + storage

Service tier
General Purpose

Compute tier
Provisioned

Hardware configuration
Standard-series (Gen5)
Up to 128 vCores, up to 625 GiB memory

vCores


Data max size (GiB)

Estimated cost (per month)
\$441.3

Database administrator

Username

You will be prompted to set the password for this administrator when you run the template.



12. Create a load balancer to distribute workload among the Session Recording servers. Enter the IP addresses or ranges of your VDAs and separate them by a comma (,) in the **Restrict access of the load balancer to only the following addresses** field. For pricing information, see [Load Balancer pricing](#).

Create site ✕

- ✓ Site information
- ✓ About your deployment
Optional
- ✓ Network
- ✓ Virtual machines
- ✓ Domain and certificate
- ✓ Storage
- ✓ Databases
- ✓ Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

Create a load balancer to distribute workload among the servers. For pricing information, see [Load Balancer Pricing](#).

Azure load balancer

SKU
Standard

Type

Public

Internal


You need to assign an IP address to the internal load balancer. Enter an unoccupied IP address in the subnet that you created for your Session Recording resources in the **Network** step.

Tier
Regional

Estimated cost (per month)
\$189.6

Access

Restrict access of the load balancer to only the following addresses ?

Next **Cancel** 


13. (Optional) Apply tags to the Azure resources to be created.

Create site ✕

- ✓ Site information
- ✓ About your deployment
Optional
- ✓ Network
- ✓ Virtual machines
- ✓ Domain and certificate
- ✓ Storage
- ✓ Databases
- ✓ Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

You can apply tags to the Azure resources that will be created.
If no tags are needed, simply click **Next** to continue.

Name	Value
+ Add	

Next **Cancel** 

14. Create a secure client to onboard the Session Recording servers to the Session Recording service.

Click **Create client** to let Citrix create a secure client on your behalf. Alternatively, you can create a secure client through the **Identity and Access Management > API Access** tab of the Citrix Cloud console and then fill in the information below.

Create site

- Site information
- About your deployment
Optional
- Network
- Virtual machines
- Domain and certificate
- Storage
- Databases
- Load balancer
- Tags
Optional
- Secure client
- Summary

Create a secure client to onboard the Session Recording servers to the Session Recording service.

Click Create client and we will create a secure client on your behalf. Alternatively, you can create a secure client through the [Identity and Access Management > API Access](#) tab of the Citrix Cloud console and then fill in the information below.

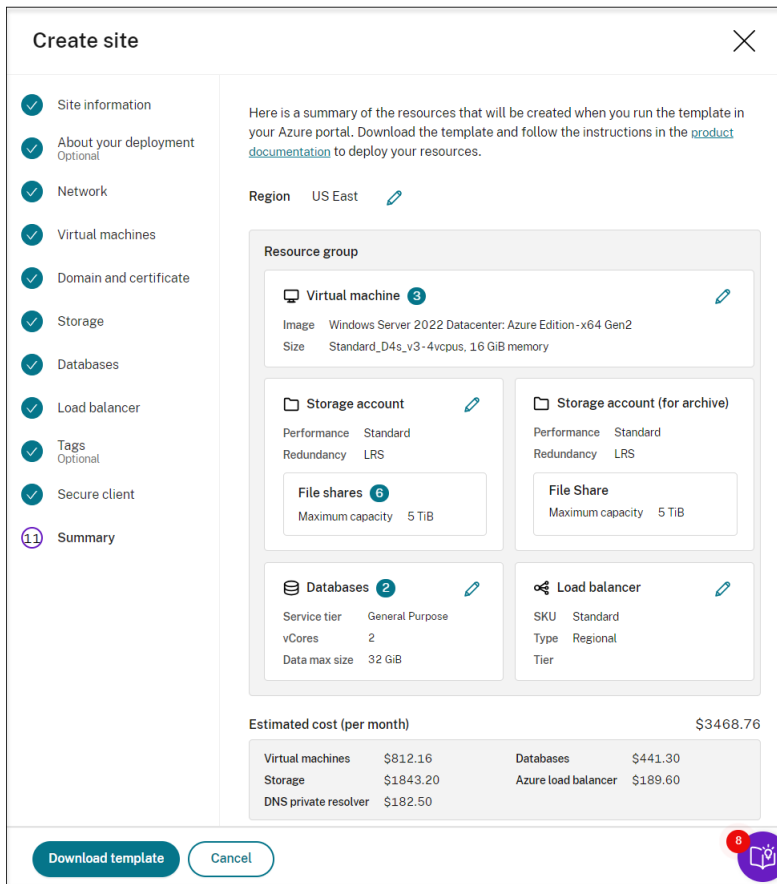
[Create client](#)

ID
6b63afdf-d048-49e1-b27d-781bfea97a2

Secret
.....

[Next](#) [Cancel](#)

- View the summary about the resources to be created and click the pencil icon to edit your settings if needed. After that, click **Download template**. An AEM template that contains how and which resources you want to deploy is then downloaded to the **Downloads** folder on your machine. You can also see the newly created site on the **Server Management** page.



- Go to the **Downloads** folder and unzip the ARM template. Open the unzipped file folder, type PowerShell in the address bar, and hit **Enter**. Wait till a PowerShell window is opened at that folder.
- Run the JavaScript Object Notation (JSON) script named **DeploySessionRecording.ps1**. Provide values for the parameters prompted. The actual parameters vary depending on the settings you specified when creating the template. For example:

```
PS D:\Downloads\Edge Downloads\471a0ec3-f680-4d33-a655-047480922194> .\DeploySessionRecording.ps1
cmdlet DeploySessionRecording.ps1 at command pipeline position 1
Supply values for the following parameters:
TenantId: |
```

```
PS D:\Downloads\Edge Downloads\471a0ec3-f680-4d33-a655-047480922194> .\DeploySessionRecording.ps1

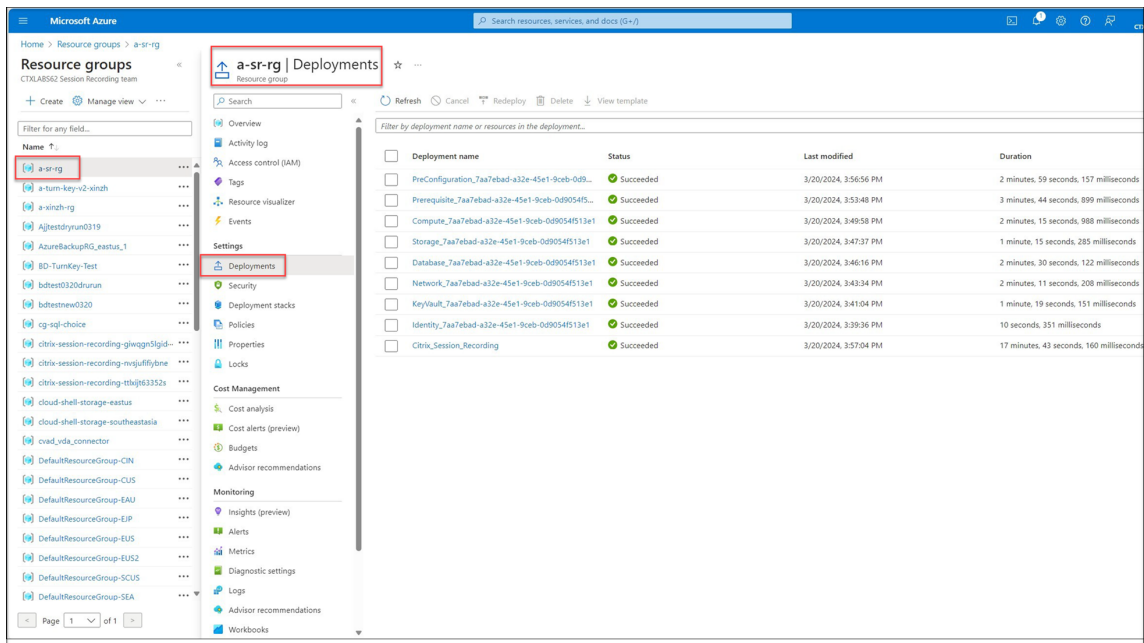
cmdlet DeploySessionRecording.ps1 at command pipeline position 1
Supply values for the following parameters:
TenantId: 03eacdb3-8322-4854-8219-30b0526a6428
AzureClientId: 59e6df48-2aeb-487b-95b8-b95c64b8c897
AzureClientSecret: *****
SubscriptionId: eb089a2e-52b0-4492-9e24-7bf579cff14f
ResourceGroupName: a-xinzhang-rg-1
DomainPassword: *****
VmAdminPassword: *****
SqlAdminPassword: *****
WARNING: The provided service principal secret will be included in the 'AzureRmContext.json' file found in the user
profile ( C:\Users\xinzh\Azure ). Please ensure that this directory has appropriate protections.

Account                               SubscriptionName                       TenantId                               Env
-----                               -
59e6df48-2aeb-487b-95b8-b95c64b8c897 cvad-session-recording-tie.liu@citrix.com 03eacdb3-8322-4854-8219-30b0526a6428 Azu

ResourceGroupName : a-xinzhang-rg-1
Location           : eastus
ProvisioningState  : Succeeded
Tags               : {admin}
TagsTable          :
                  Name Value
                  ====
                  admin xinzh

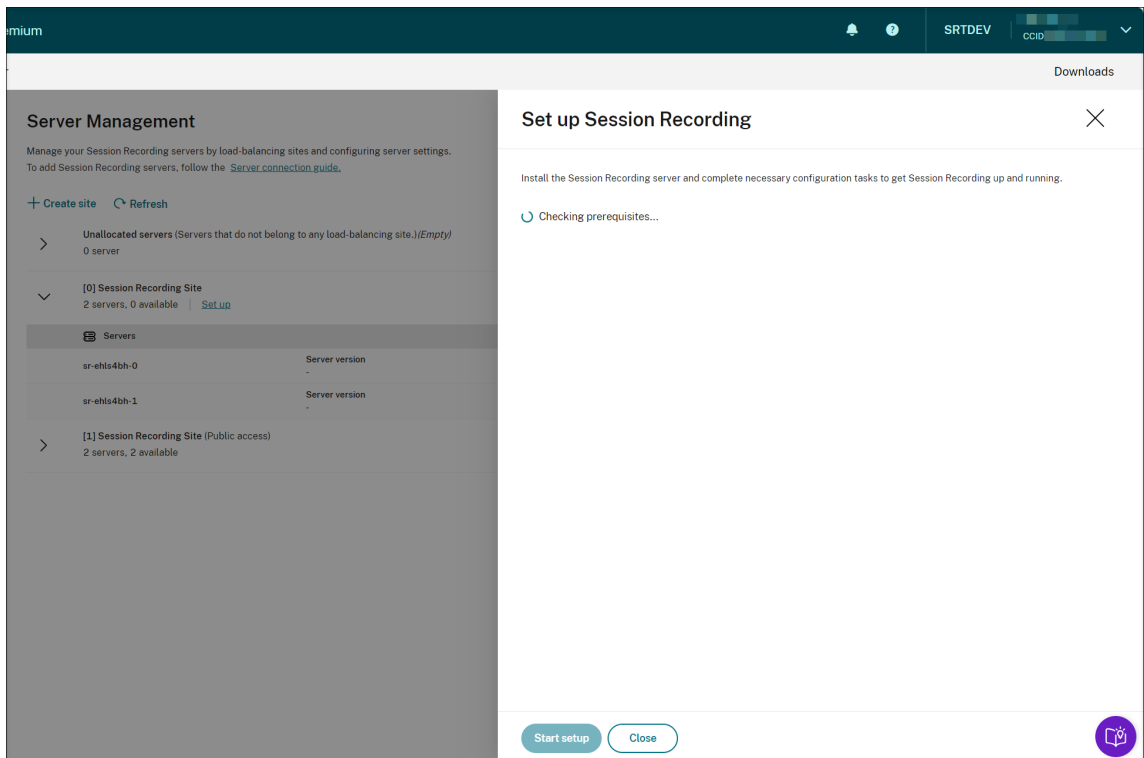
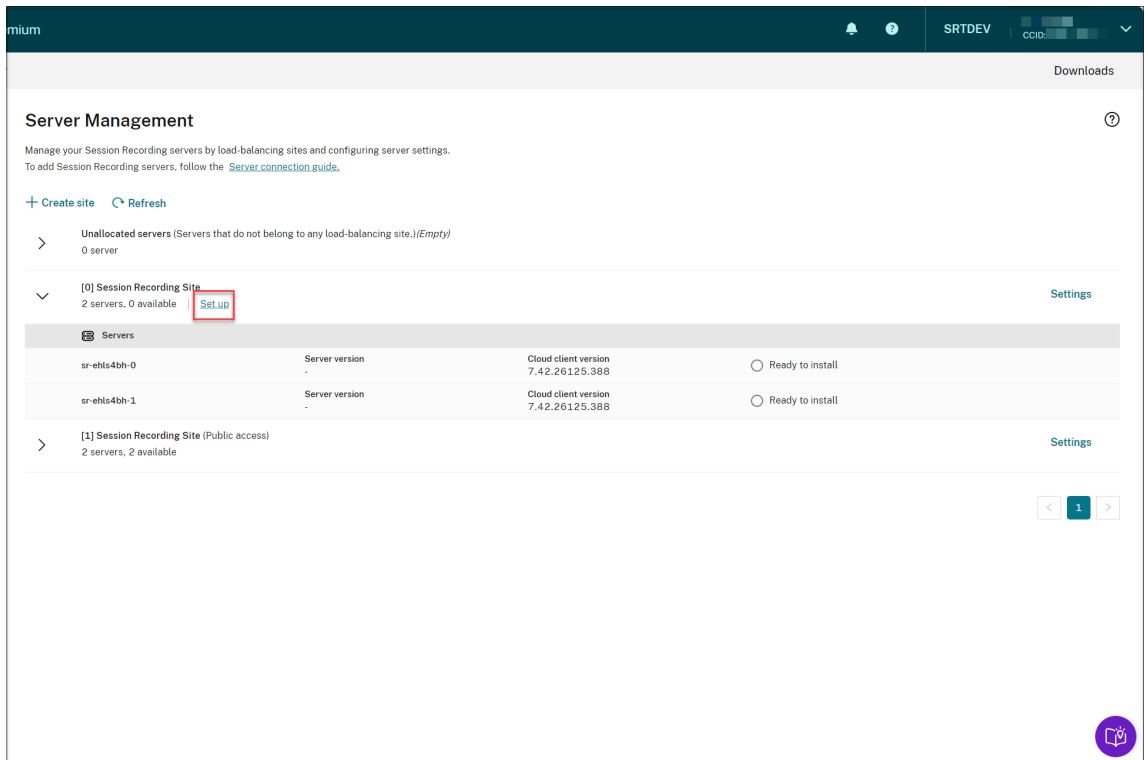
ResourceId         : /subscriptions/eb089a2e-52b0-4492-9e24-7bf579cff14f/resourceGroups/a-xinzhang-rg-1
ManagedBy        :
```

- Go to the Azure portal, locate the resource group that contains your deployment, and then check the deployment progress. Wait until the entire deployment shows **Succeeded**.



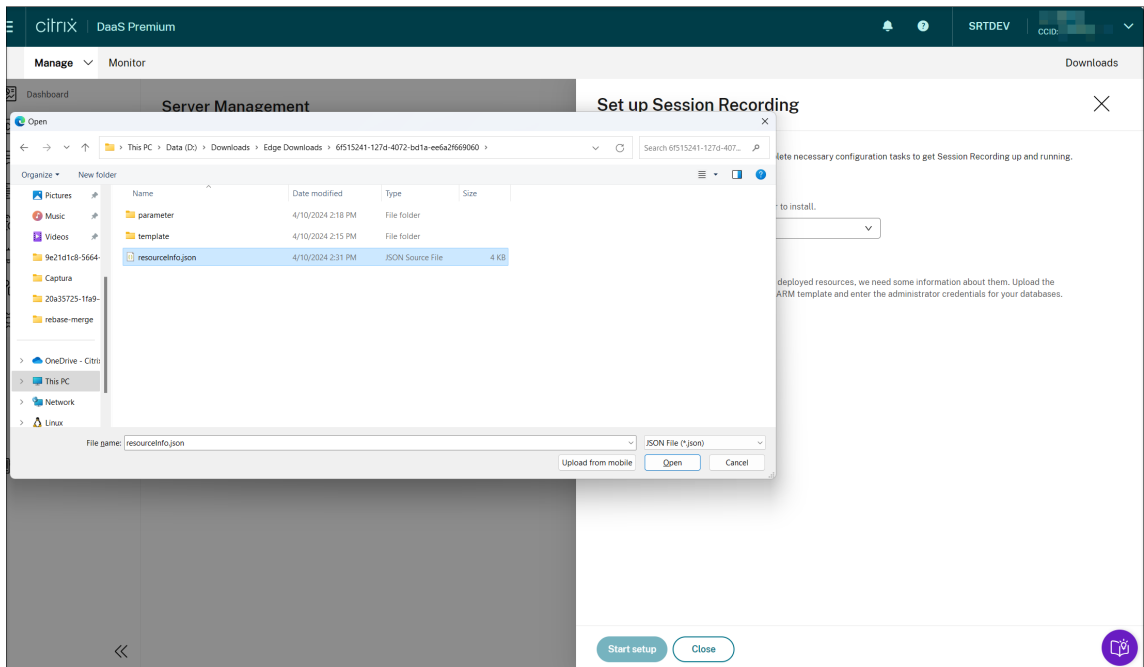
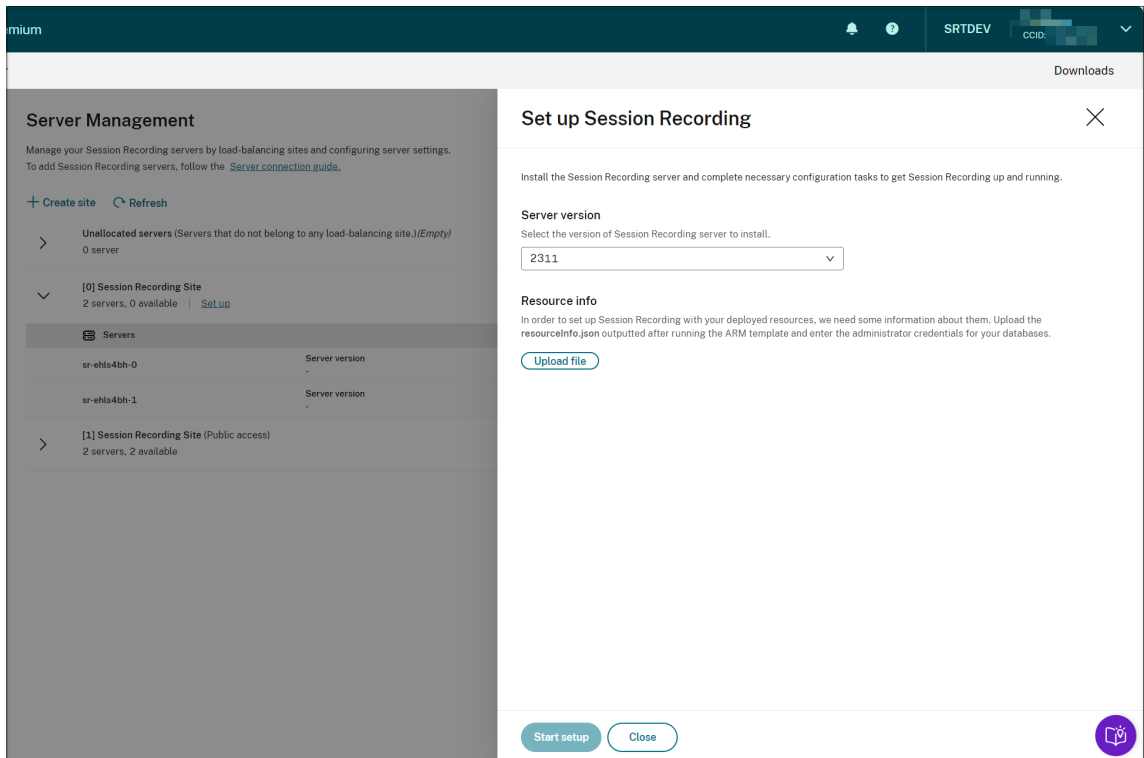
- Return to the **Server Management** page of the Session Recording service. Find the newly created site, and you will see a **Set up** button available. Click **Set up** to set up Session Recording to get it up and running.

Session Recording service



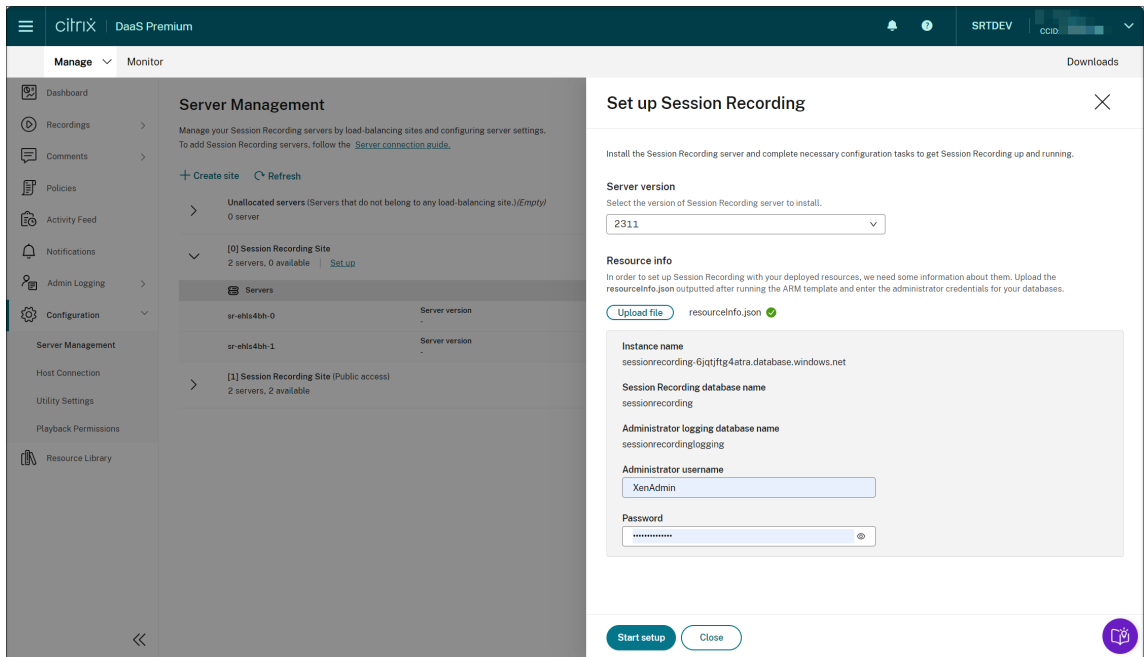
To set up Session Recording, you need to specify the version of the Session Recording server to install and upload the **resourceInfo.json** file.

Session Recording service

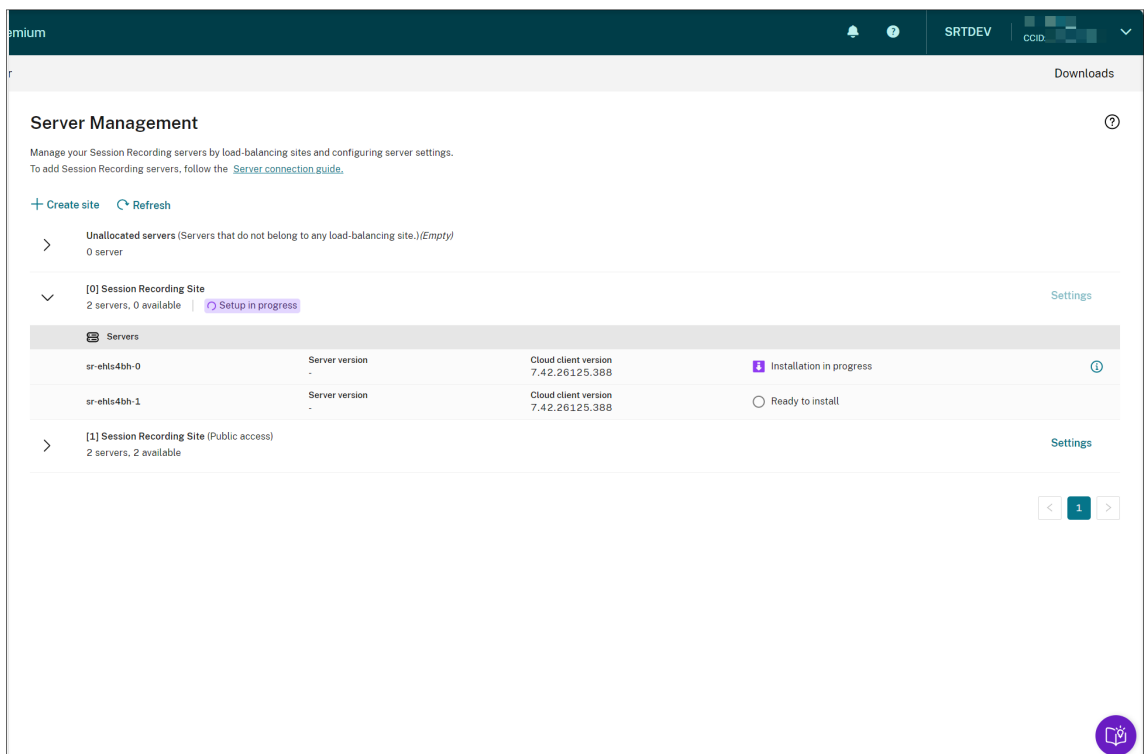


Enter the credentials for your databases.

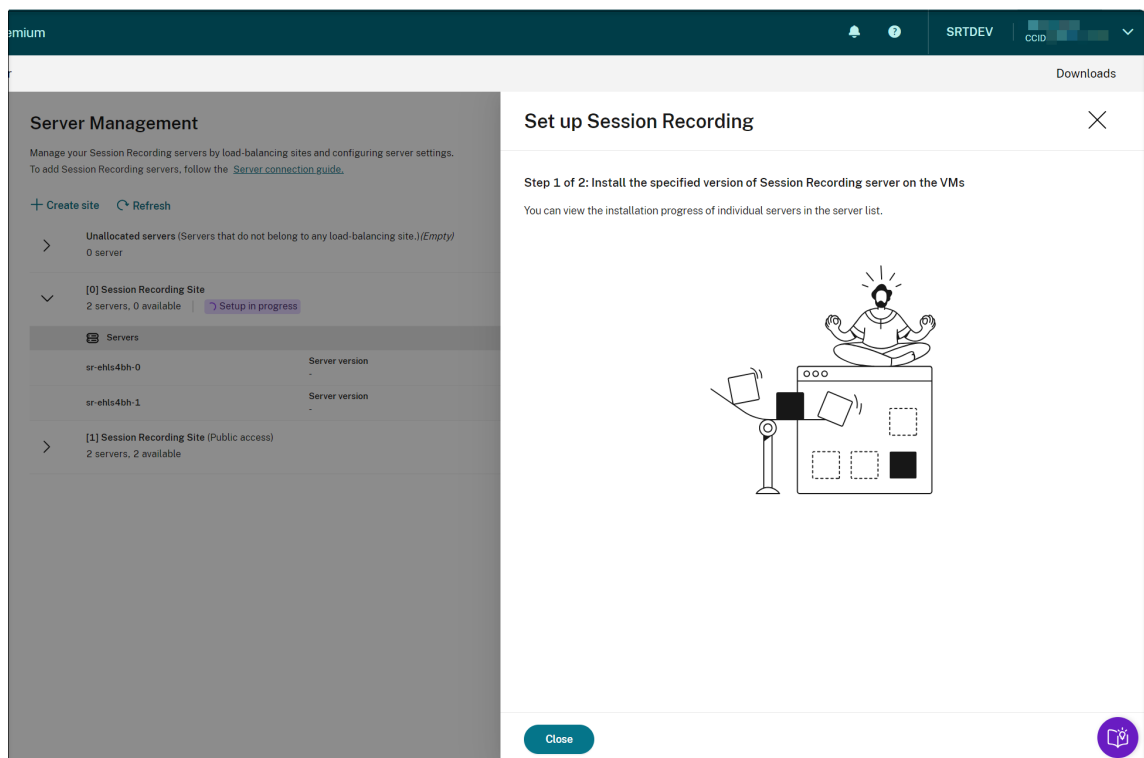
Session Recording service



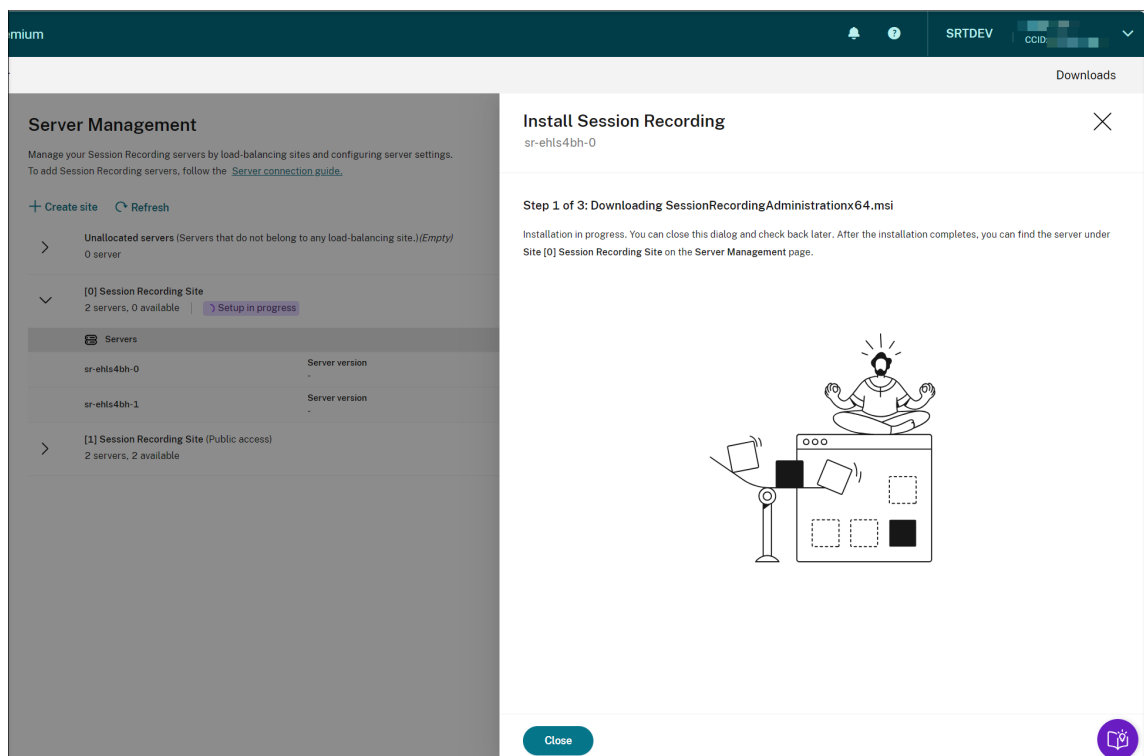
Click **Start startup**. You can then check the setup progress on the **Server Management** page.



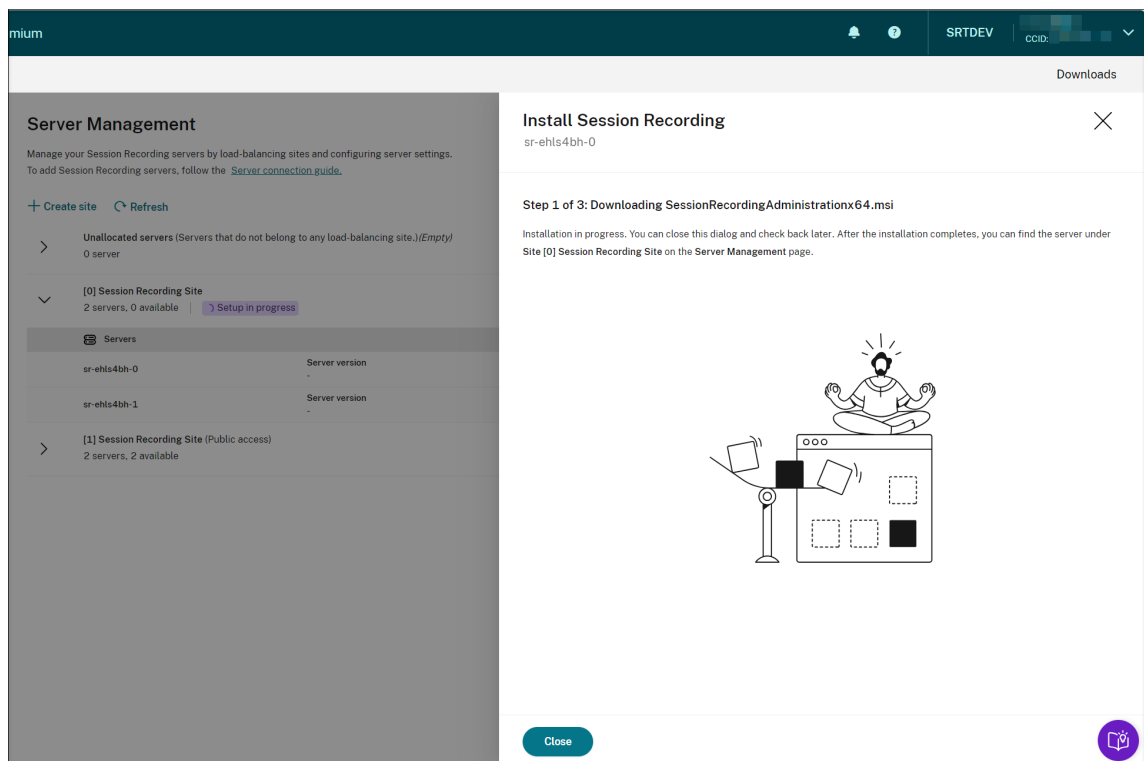
Session Recording service



You can view the installation progress of individual servers in the server list.



When all the Session Recording servers show available in the list, your site creation is complete and the specified resources are deployed to Azure.



Schedule cloud client upgrades

April 26, 2024

You install the Session Recording cloud client on each Session Recording server that you want to connect to the cloud. Citrix checks for upgrades for the Session Recording cloud client automatically. You can upgrade the cloud client immediately or specify a time to upgrade the cloud client automatically.

Upgrade the cloud client immediately or automatically

To upgrade the cloud client immediately or automatically, choose either of the following methods:

Method 1: Click Cloud client version in the row of the target Session Recording server

1. Locate the target Session Recording server by selecting **Configuration > Server Management** from the left navigation of the Session Recording service.
2. Ensure that the Session Recording server is in **Available** status.

3. Click **Cloud client version** in the row of the Session Recording server.

Cloud client version is not clickable if the server is not in **Available** status.

Server ID	Server version	Cloud client version	Status	Actions
SR1912	19.12.6000.24093	7.37.25542.42517	Available	Settings
SR2203	22.3.2000.36	7.37.25542.42517	Offline	Settings
SRS-7	Site description justo eget magna fermentum iaculis.		1 server, 1 available	Settings
STANDALONE2209	22.9.0.1	7.37.25542.42517	Available	Settings
W2K19ST-SRGXDEV			1 server, 1 available	Settings
W2K19ST-74G7G16			1 server, 1 available	Settings
W2K19ST-DRV9J12			1 server, 0 available	Settings
W2K19ST-GA37VLG			1 server, 1 available	Settings
W2K19ST-VMODNLK			1 server, 0 available	Settings
WEEKLYSERVER2			4 servers, 1 available	Settings

4. Click **Upgrade now** or **Configure automatic upgrade**.

Cloud client version

Current version 7.37.25459.8745

Latest version 7.37.25542.42517

i Upgrade available.

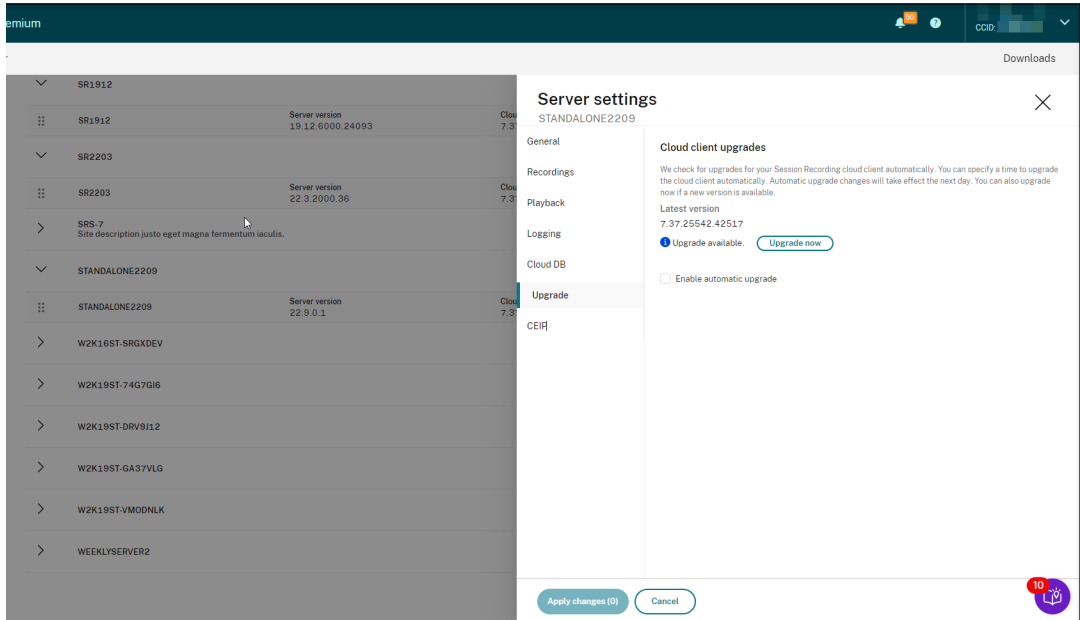
Upgrade now
Configure automatic upgrade

- Click **Upgrade now**.

Upgrade now is not available if the version of your cloud client is already up to date. After clicking **Upgrade now**, you are not prompted to confirm the upgrade.

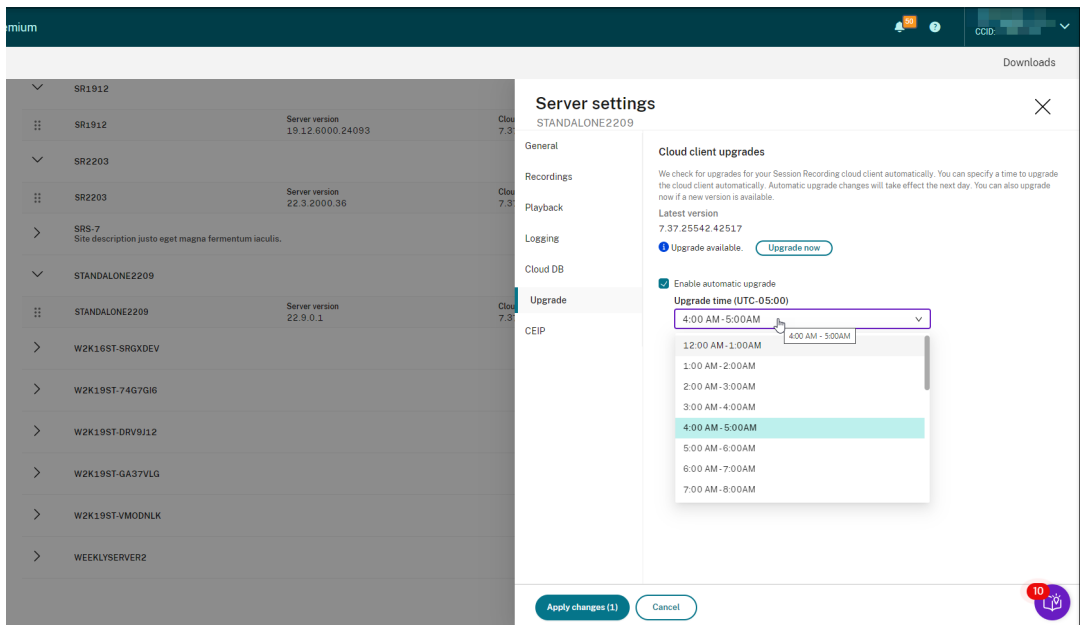
- Click **Configure automatic upgrade**.

After clicking **Configure automatic upgrade**, you are taken to the **Cloud client upgrades** page where you can specify a time to upgrade the cloud client automatically.



By default, automatic upgrade is enabled and occurs from 2:00 AM through 3:00 AM every day. You can clear the **Enable automatic upgrade** check box to allow only manual upgrades.

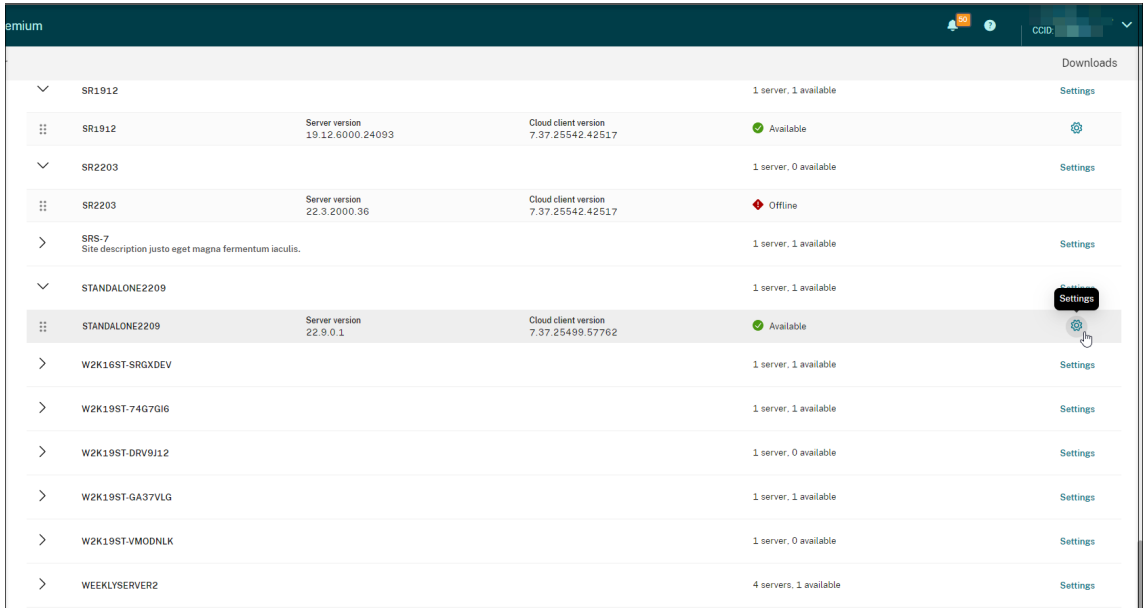
If you select the **Enable automatic upgrade** check box, you can specify a custom time slot that suits your needs. The time shown here is the time on the Session Recording server.



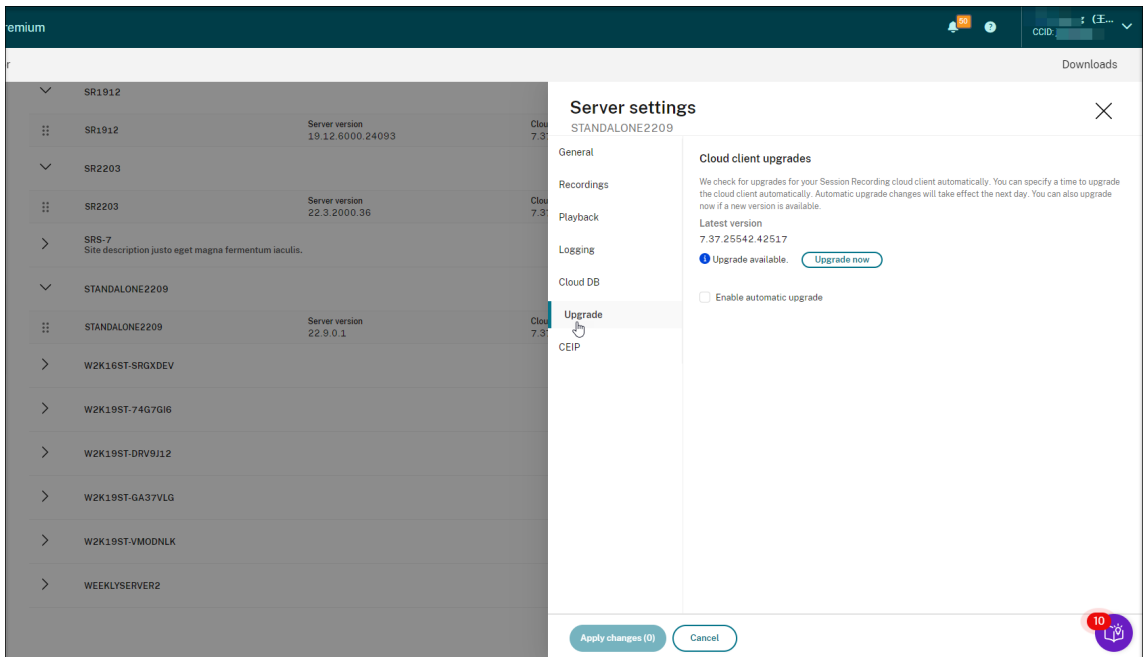
Your automatic upgrade settings take effect the next day.

Method 2: Click the settings icon in the row of the target Session Recording server

1. Locate your target Session Recording server by selecting **Configuration > Server Management** from the left navigation of the Session Recording service.
2. Ensure that the Session Recording server is in **Available** status.
3. Click the settings icon in the row of the Session Recording server. The **Server settings** window appears.



4. Click **Upgrade** in the left navigation.

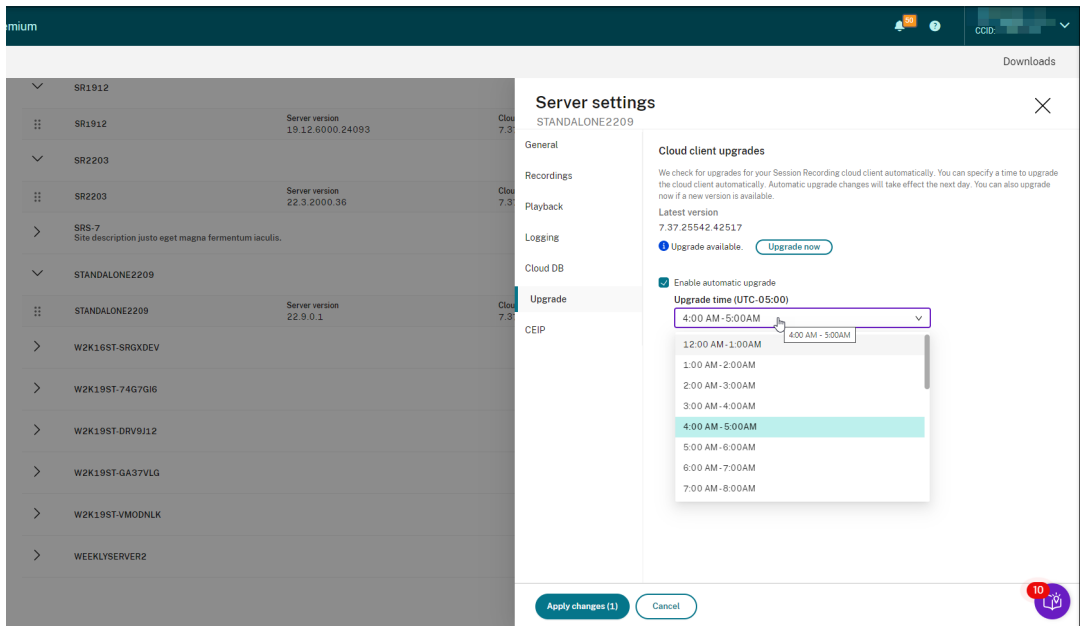


5. Click **Upgrade now** or set **Enable automatic upgrade**.

- Click **Upgrade now**.

Upgrade now is not available if the version of your cloud client is already up to date. After clicking **Upgrade now**, you are prompted to confirm the upgrade.

- Set **Enable automatic upgrade**.



Note:

Ensure that the time you set for automatic cloud client upgrades is earlier than the time you set for [automatic archiving and deletion of recordings](#). Otherwise, automatic archiving and deletion might fail.

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](#)

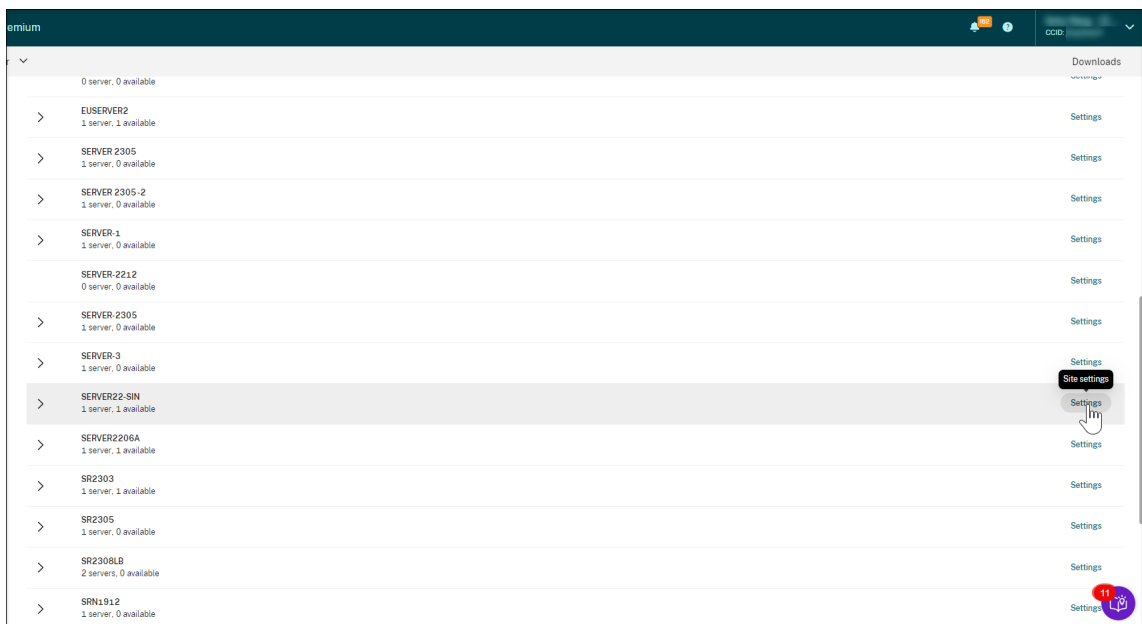
- [Configure playback permissions](#)
- [Configure utilities](#)

Site and server settings

July 17, 2023

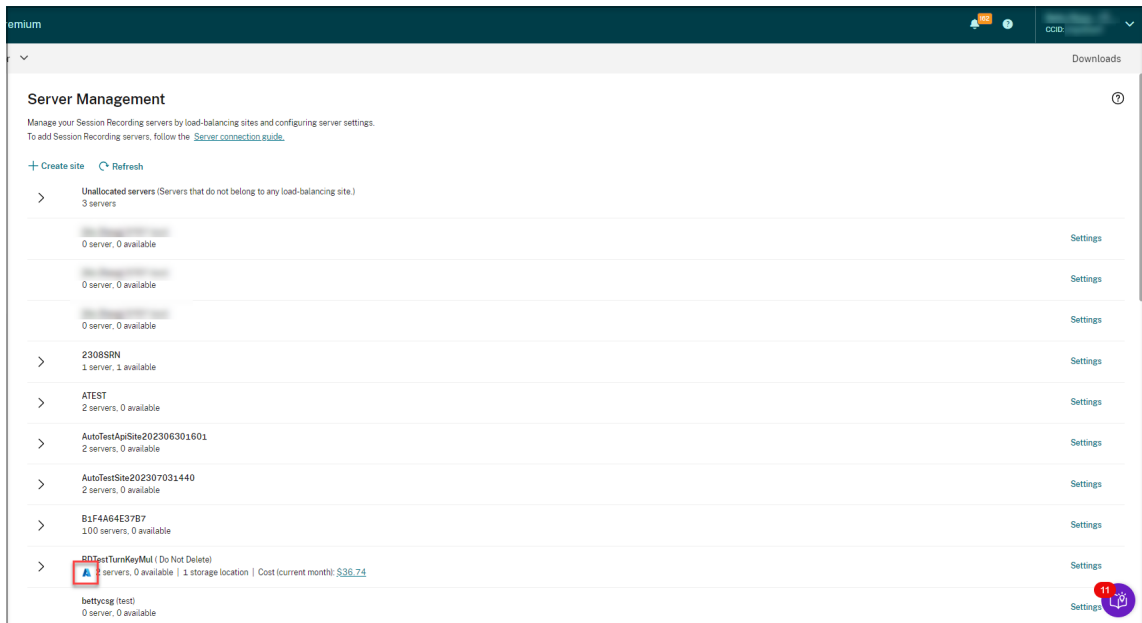
Site settings

1. Select **Configuration > Server Management** from the left navigation of the Session Recording service.
2. Click **Settings** for the target site.

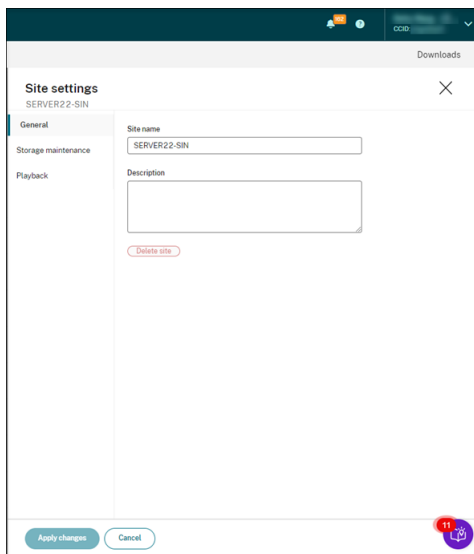


An Azure icon is available to represent sites deployed on Azure.

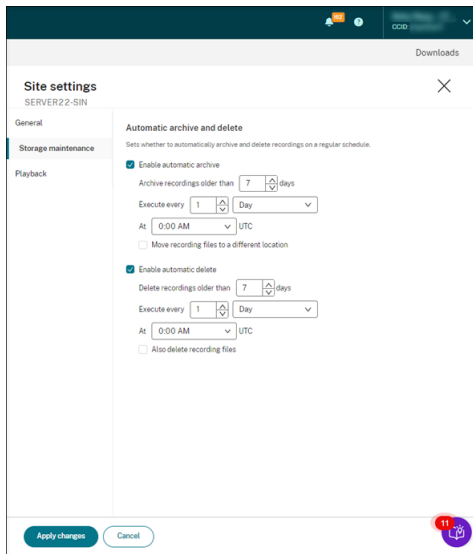
Session Recording service



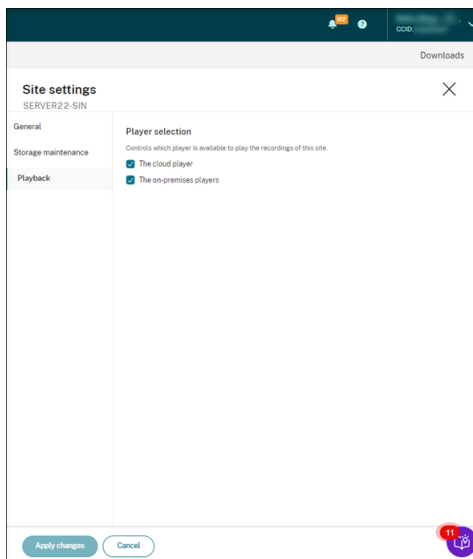
3. Rename the site and give it a new description as needed.



4. Schedule site-level tasks to automatically archive and delete recordings. For more information, see [Manage recordings on schedule](#).



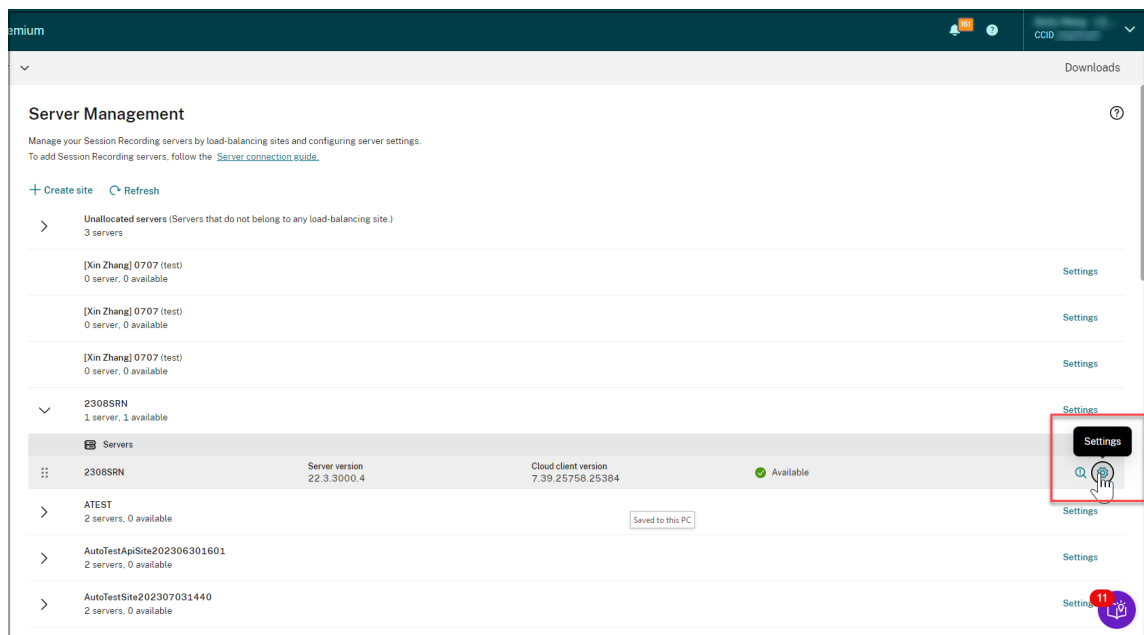
5. Specify either the cloud player, on-premises players, or both to play the recordings of a site. By default, both the cloud player and on-premises players are selected. The on-premises players include the Session Recording player (Windows) and the Session Recording web player. For more information, see [Specify players for a site](#).



Server settings

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 next to it. The **Settings** icon is present only for servers in **Available** state.

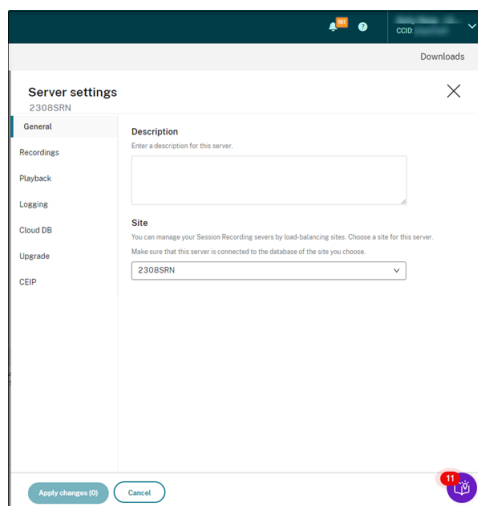
Session Recording service



Note:

The status of a Session Recording server might not change to **Offline** after you stop the cloud client service (CitrixSsRecCloudClientService) on it.

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:

Server setting	Description
File storage location	Specifies where to store recorded session files. You can specify multiple locations to store files in a load-balanced manner.
Certificate	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.
File rollover	Lets you specify two thresholds for a rollover: file size and recording duration.
Notification	Customizes messages sent to end users to notify them that their sessions are being recorded.
Restore location for archived files	Specifies a location to temporarily store archived session recordings and make them available for playback.
Live session playback	Sets whether you allow users to play ongoing sessions that are being recorded.
Recording file encryption	Sets whether to encrypt recording files before downloading to the player. Encryption prevents files from being copied and viewed by users other than the user who originally downloaded them. This setting applies only to the Session Recording player.
Citrix Workspace app version check	Sets whether you allow users to skip the Citrix Workspace app version check that occurs before the Session Recording player plays back a recording. This setting applies only to the Session Recording player.

Server setting	Description
Hiding content on the web player home page	Sets whether to prevent the web player home page from displaying any content. Recordings can be accessed only by way of their URLs. This setting applies only to the on-premises web player.
Administrator logging	Sets whether to enable the administrator logging service.
Mandatory blocking	Sets whether to block changes to policies and server settings if administrator logging fails.
Cloud SQL support	Lets you enable or disable cloud SQL.
Cloud client upgrades	Lets you specify a time to upgrade the cloud client automatically. Automatic upgrade changes take effect the next day. You can also upgrade immediately if a new version is available.
CEIP	Sets whether to join the Citrix Customer Experience Improvement Program (CEIP).

Server removals

The Session Recording service is a cloud platform that provides a unified entry point to manage and observe the Session Recording servers across your organization. You can remove servers with the **Offline**, **Uninstalled**, and **Installation Failed** states from the cloud to display only the desired Session Recording servers.

Note:

Removing a session recording server does not delete it and only hides it from the cloud user interface.

Session Recording service

W2K19ST-VMODNLK 2 servers, 1 available				Settings
Servers				
W2K19ST-S2N3DM7	Server version 22.10.0.8	Cloud client version 7.39.25738.41023	Available	
W2K19ST-VMODNLK	Server version 22.9.0.2	Cloud client version 7.39.25771.65403	Offline	
W2K22ST-TB81E13 1 server, 0 available				Settings
Servers				
W2K22ST-TB81E13	Server version 23.5.0.0	Cloud client version 7.39.25726.60926	Offline	
WEEKLYSERVER2 4 servers, 1 available				Settings
Servers				
SR-Server	Server version 22.3.1000.5	Cloud client version 7.36.25431.20278	Uninstalled	
SR-Server2 1213	Server version 22.3.1000.5	Cloud client version 7.36.25410.34348	Upgrading	
W2K19ST-GBVQ3PL	Server version 22.10.0.8	Cloud client version 7.36.25431.20278	Offline	
WEEKLYSERVER2	Server version 22.12.0.844	Cloud client version 7.36.7020.11	Available	

- **Offline:** Session Recording servers with this state are disconnected from the Session Recording service.
- **Uninstalled:** Session Recording servers with this state are those servers that had the cloud client installed and then uninstalled.
- **Installation failed:** Session Recording servers with this state are those servers that you failed to install from within the cloud. For more information, see [Install Session Recording servers from within the cloud](#).

Configure policies

November 3, 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.

For more information, see:

- [Configure session recording policies](#)
- [Configure event detection policies](#)
- [Configure event response policies](#)

Video about configuring policies:



Configure session recording policies

May 9, 2024

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

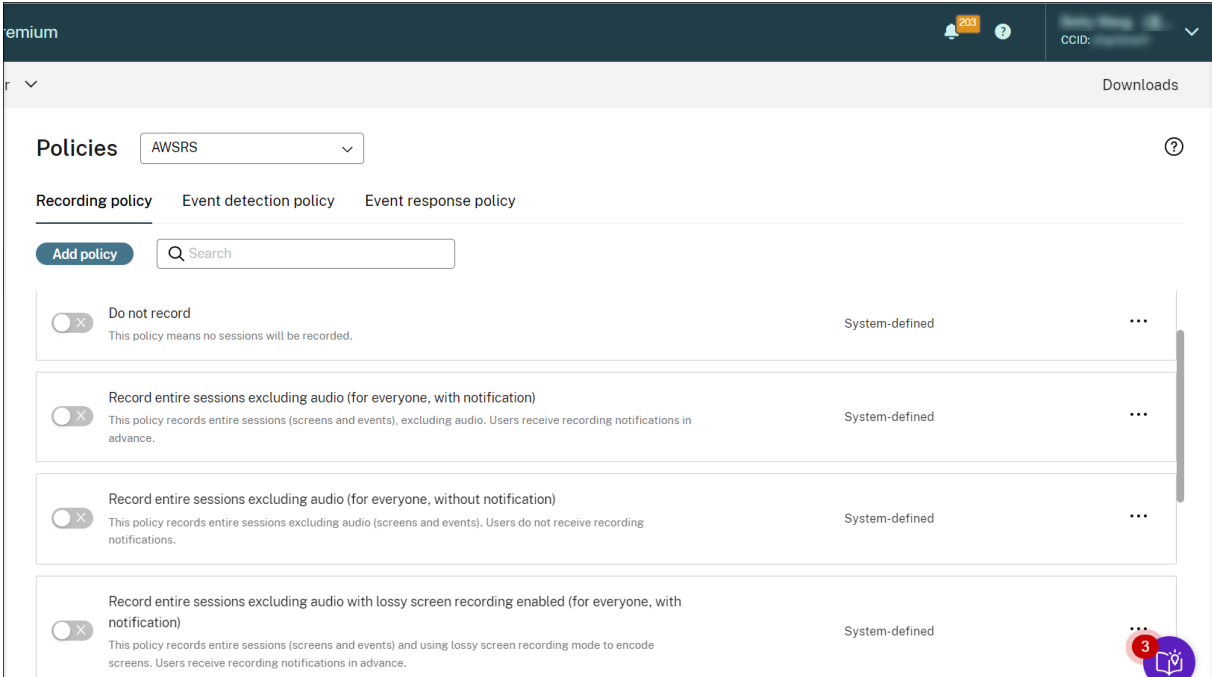
The active recording policy determines which sessions are recorded. Only one recording policy is active at a time.

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:



The screenshot shows the 'Policies' section of the Session Recording service interface. The account name 'AWSRS' is selected in a dropdown menu. Below the menu, there are tabs for 'Recording policy', 'Event detection policy', and 'Event response policy'. An 'Add policy' button and a search bar are visible. A list of four system-defined policies is shown, each with a toggle switch and a description:

- Do not record**: This policy means no sessions will be recorded.
- Record entire sessions excluding audio (for everyone, with notification)**: This policy records entire sessions (screens and events), excluding audio. Users receive recording notifications in advance.
- Record entire sessions excluding audio (for everyone, without notification)**: This policy records entire sessions excluding audio (screens and events). Users do not receive recording notifications.
- Record entire sessions excluding audio with lossy screen recording enabled (for everyone, with notification)**: This policy records entire sessions (screens and events) and using lossy screen recording mode to encode screens. Users receive recording notifications in advance.

Note:

Both lossy screen recording and audio recording for non-optimized HDX audio are available with Session Recording version 2308 and later.

- **Do not record.** The default policy. If you do not specify another policy, no sessions are recorded.
- **Record entire sessions excluding audio (for everyone, with notification).** This policy records entire sessions (including screens and events but excluding audio). Users receive recording notifications in advance.
- **Record entire sessions excluding audio (for everyone, without notification).** This policy records entire sessions (including screens and events but excluding audio). Users do not receive recording notifications.
- **Record entire sessions excluding audio with lossy screen recording enabled (for everyone, with notification).** This policy records entire sessions (including screens and events but excluding audio). Lossy screen recording is enabled to reduce the size of recording files. Users receive recording notifications in advance.
- **Record entire sessions excluding audio with lossy screen recording enabled (for everyone, without notification).** This policy records entire sessions (including screens and events but excluding audio). Lossy screen recording is enabled to reduce the size of recording files. Users do not receive recording notifications.
- **Record entire sessions including audio (for everyone, with notification).** This policy records entire sessions (including screens, events, and audio). Users receive recording notifications in advance. You can enable audio recording for non-optimized HDX audio. Non-optimized HDX audio refers to the audio that is processed on the VDA and transmitted to/from the

client where Citrix Workspace app is installed. In contrast to non-optimized HDX audio is optimized HDX audio whose processing is offloaded to the client, such as in the Browser Content Redirection (BCR) and Optimization for Microsoft Teams scenarios.

- **Record entire sessions including audio (for everyone, without notification).** This policy records entire sessions (including screens, events, and audio). Users do not receive recording notifications.
- **Record only events (for everyone, with notification).** This policy records only events that your event detection policy specifies. It does not record screens or audio. 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 or audio. Users do not receive recording notifications.

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

Create a custom recording policy

Considerations

You can record sessions of specific 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.

You can also specify smart access tags to use as scopes for a custom recording policy to apply to. This feature is available with Session Recording 2402 and later. It lets you apply policies based on the user access context including:

- The user's location
- IP address range
- Delivery group
- Device type
- Installed applications

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:

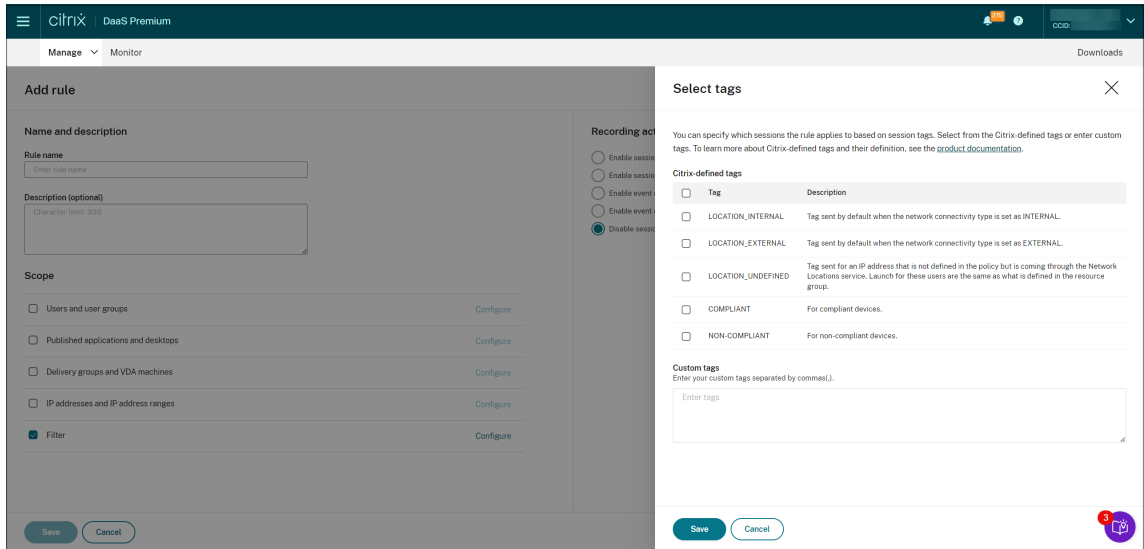
- **Enable session recording with notification.** This option records entire sessions (screens and events). Users receive recording notifications in advance. You can further select to enable audio recording or lossy screen recording.
- **Enable session recording without notification.** This option records entire sessions (screens and events). Users do not receive recording notifications. You can further select to enable audio recording or lossy screen recording.
- **Enable event only session recording with notification.** Recording only specific events helps to free up storage space. This option records throughout sessions only events that your event detection policy specifies. It does not record screens. Users receive recording notifications in advance.
- **Enable event only session recording without notification.** Recording only specific events helps to free up storage space. This option records throughout sessions only events that your event detection policy specifies. It does not record screens. Users do not receive recording notifications.
- **Disable session recording.** This option means that no sessions are recorded.

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.

- **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

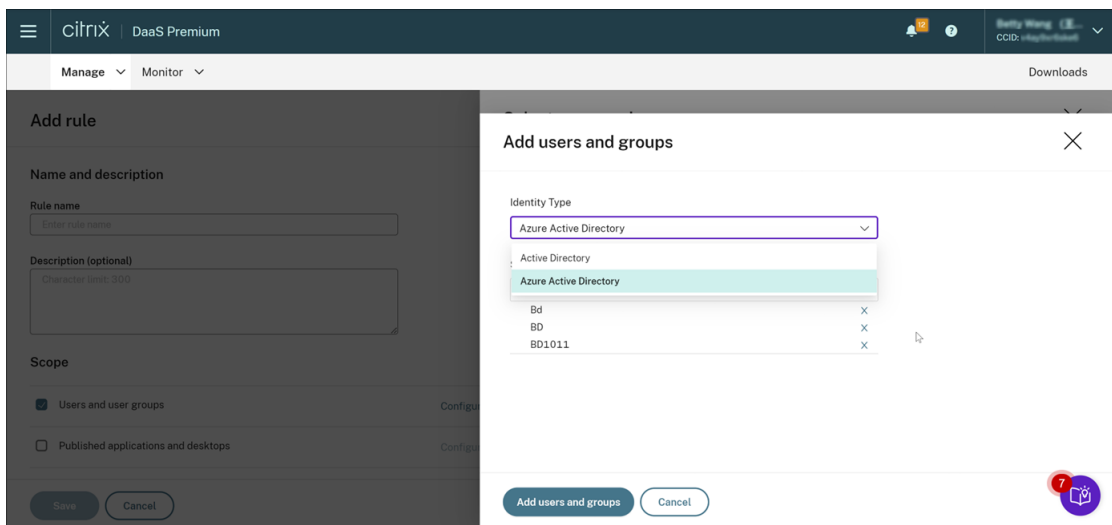
which the action of the rule applies.

- **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.
- **Filter.** Creates a list of smart access tags to which the action of the rule applies. You can configure contextual access (smart access) using smart access policies on Citrix NetScaler, [Citrix Device Posture service](#), and [Adaptive access based on the user's network location](#).



Contextual access (smart access) is available with Session Recording 2402 and later.

- **Users and user groups.** Creates a list of users and user groups to which the action of the rule applies. Both Azure Active Directory (Azure AD) and Active Directory identity types are supported. For an example user group scenario, see [Use user groups](#) and [white list users](#).



Note:

Azure AD support is a preview feature. It is available with Session Recording version 2402 and later.

Preview features might not be fully localized and are recommended for use in non-production environments. Citrix Technical Support doesn't support issues found with preview features.

To fully enable Azure AD identity support for configuring various policies and [playback permissions](#) from the cloud, complete the following steps and then restart the VDA:

- Use the Citrix Virtual Apps and Desktops installer to install the Session Recording agent on an Azure AD joined machine. Select **Enable Azure AD support** during the installation.

For a Session Recording agent that you've installed otherwise, set the following registry values under **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent** to enable Azure AD support:

- * Set **CommunicationProtocolToggle** to **1** (**0** means .net remoting. **1** means **Web-socket**).
 - * Set **AuthType** to **1** (**0** means Active Directory. **1** means Citrix Cloud authentication).
 - * Set **SmAudIdpEnabled** to **1** (**0** means disabled. **1** means enabled)
- Use the MSI package to install the Session Recording server on an Azure AD joined machine as well. Select **Enable Azure AD support** during the MSI installation.
 - [Connect Citrix Cloud to Azure AD](#).
 - Go to the home page for the Full Configuration interface and enable the **SessionRecordingSupportAAD** and **Send User Identity Info In Prepare Session** toggles under the **Preview features** section. To access the home page for the Full Configuration interface, complete the following steps:
 1. Sign in to [Citrix Cloud](#).
 2. In the upper left menu, select **My Services > DaaS**. By default, the home page for the Full Configuration interface appears.

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 **Disable session recording** action have the highest priority.
- Rules with the **Enable session recording with notification** action have the second-to-highest priority.

- Rules with the **Enable session recording 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 lowest priority.

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 **Disable session recording**. You cannot modify or delete the fallback rule.

Steps

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.
3. From **Manage**, select **Session Recording**.
4. Select **Policies** from the left navigation of the Session Recording service page.
5. Select a target site. The **Recording policy** tab is displayed by default.
6. Click **Add policy**.
7. Enter a name and description for the new policy, and then click **Add rule**.
8. Enter a name and description for the rule. Specify a recording action and choose at least one of the following items to create the rule scope.

For each rule, specify a recording action:

- **Enable session recording with notification**
- **Enable session recording without notification**
- **Enable event only session recording with notification**
- **Enable event only session recording without notification**
- **Disable session recording**

For each rule, choose at least one of the following items to create the rule scope.

- **Published applications and desktops**
- **Users and user groups**
- **Delivery groups and VDA machines**
- **IP addresses and IP address ranges**
- **Filter**

9. After the new policy is created, find it on the **Recording policy** tab and turn the toggle on to activate the policy.

Use user groups

Session Recording allows you to use user groups when creating policies. Using user 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 called **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 called **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:

If the previous recording policy was	And the new recording policy is	After a rollover, the recording policy will be
Do not record	Any other policy	No change. The new policy takes effect only when the user logs on to a new session.
Record without notification	Do not record	The recording stops.
Record without notification	Record with notification	The recording continues and a notification message appears.

If the previous recording policy was	And the new recording policy is	After a rollover, the recording policy will be
Record with notification	Do not record	The recording stops.
Record with notification	Record without notification	The recording continues. No message appears the next time a user logs on.

Video about configuring policies



Configure event detection policies

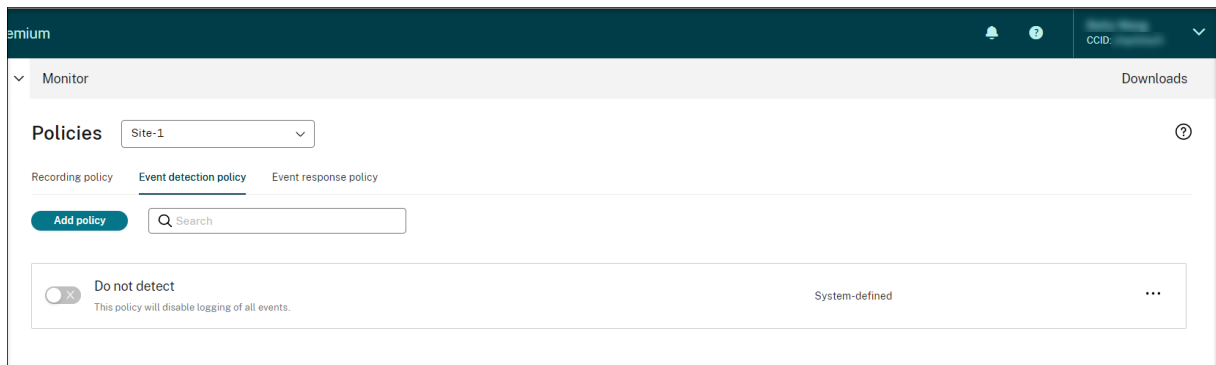
June 24, 2024

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

Note:

An event detection policy applies to all Session Recording servers of a specific 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:

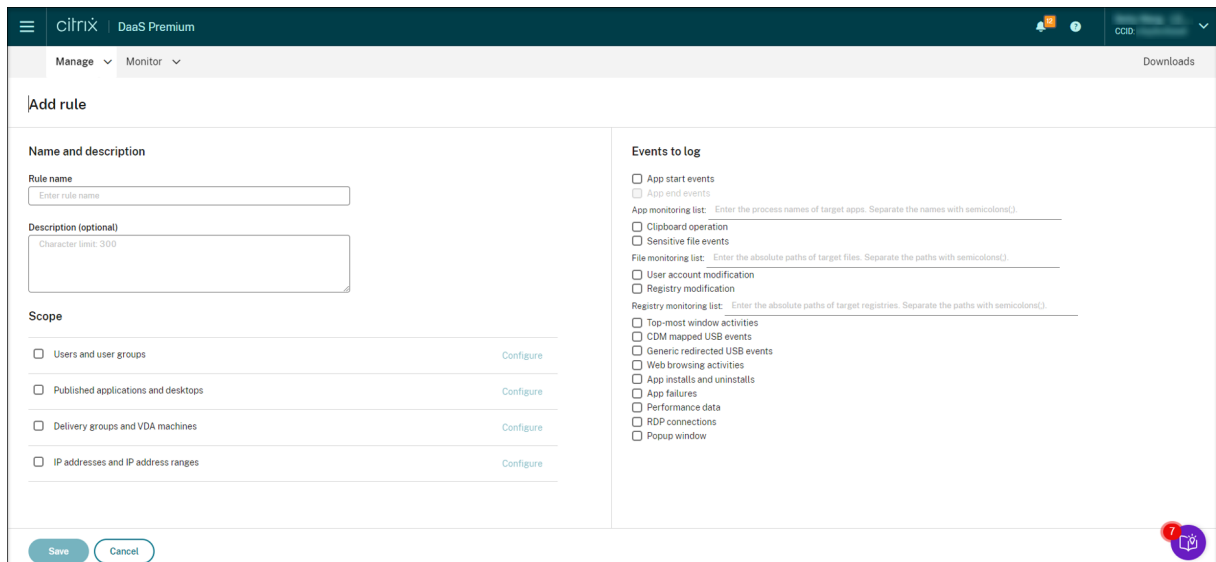
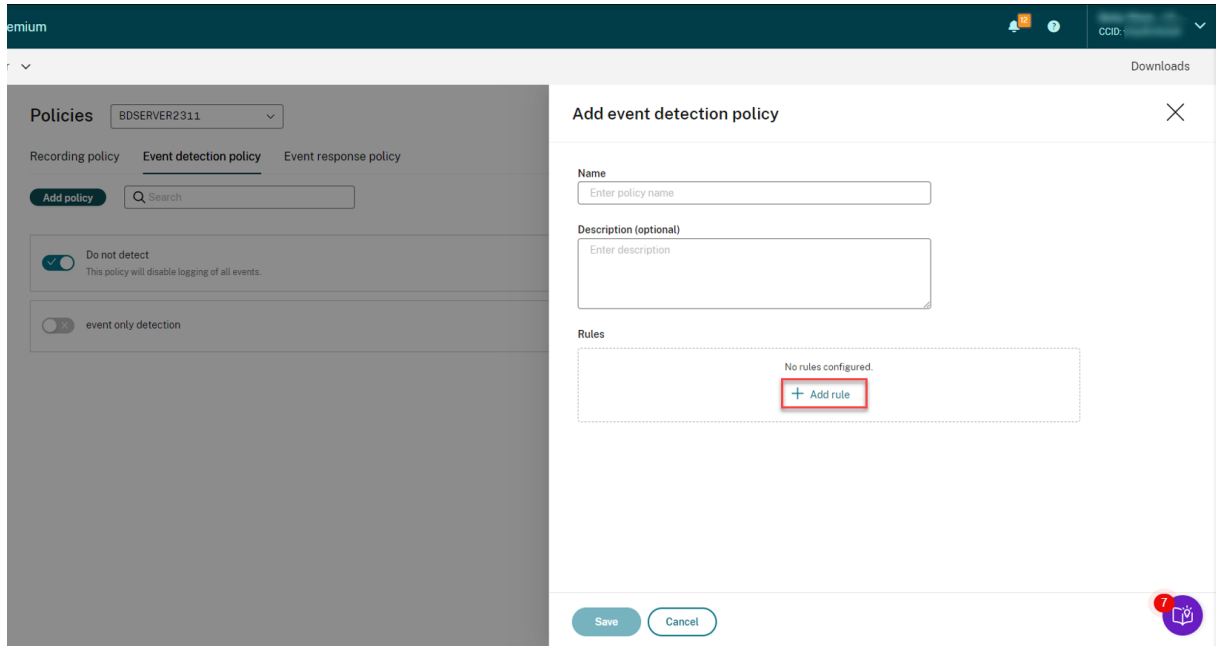
- Insertion of USB mass storage devices
- Application starts and ends
- App failures
- App installs and uninstalls
- File renaming, creation, deletion, and moving operations within sessions
- File transfers between session hosts (VDAs) and client devices (including mapped client drives and generic redirected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

Session Recording service

- Performance data (data points related to the recorded session)
- Popup window events

For more information about the various events, see [the counterpart of the on-premises Session Recording documentation](#).

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



Similar to creating a custom recording policy, you can choose one or more rule criteria. For more information, see the instructions in the [Create a custom recording policy](#) section.

Video about configuring policies



Configure event response policies

April 25, 2024

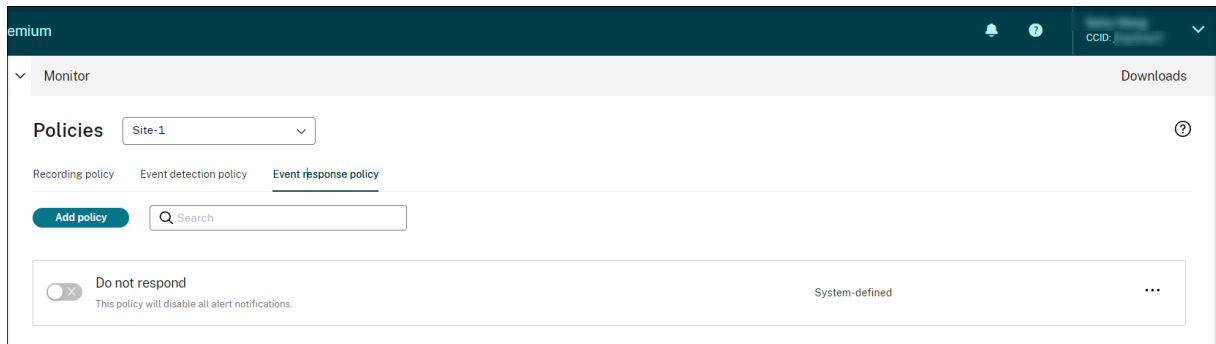
Event response policies let you configure event-triggered actions so that you can:

- Send an email alert when a session start event is detected.
- Take action (any combination of the following actions) when events are detected in recorded sessions:
 - Send email alerts
 - Start screen recording immediately (with or without lossy screen recording enabled)
 - 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's 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. On the **Add event response policy** page, enter a name and description for your new policy.

Add event response policy [Close]

Name
Enter policy name

Description (optional)
Enter description

Rules
No rules configured.
[+ Add rule](#)

Save Cancel [Notification]

3. Click **Add Rule**.
4. Enter the rule name and description.

Add rule

Name and description
Rule name: Enter rule name
Description (optional): Character limit: 300

Events and responses
Event triggers
Configure event triggers to trigger actions when certain events are detected.
[Configure](#)

Scope

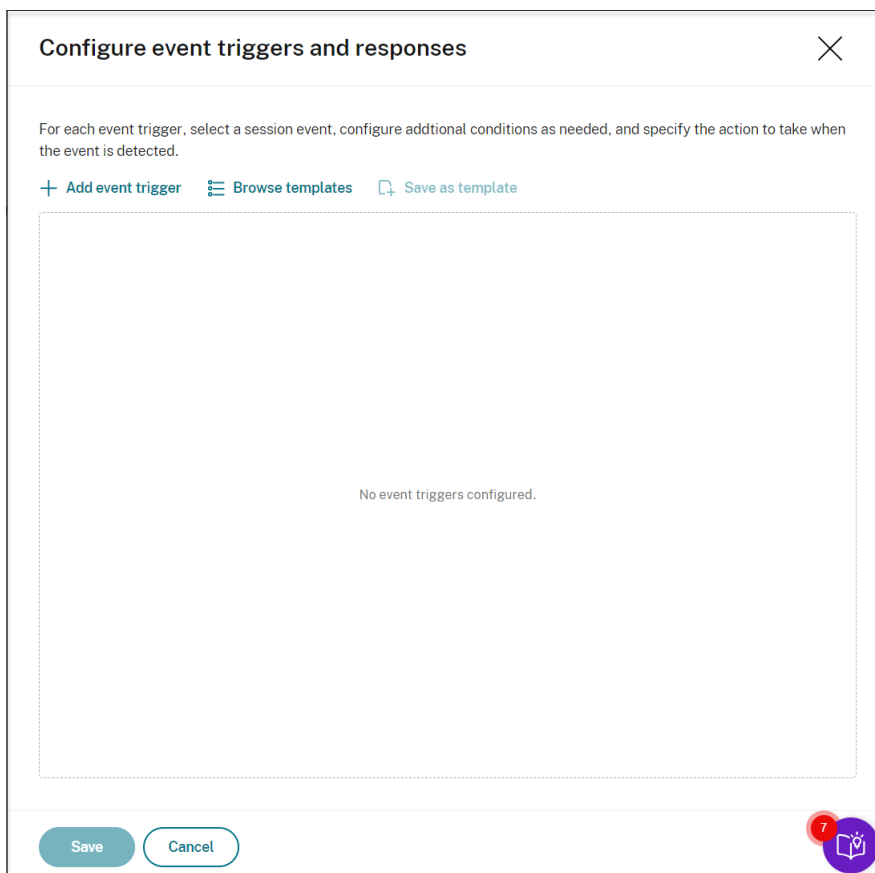
- Users and user groups [Configure](#)
- Published applications and desktops [Configure](#)
- Delivery groups and VDA machines [Configure](#)
- IP addresses and IP address ranges [Configure](#)
- Filter [Configure](#)

Save Cancel [Notification]

5. In the **Event triggers** section, click **Configure** to configure event-triggered actions so that you can:
 - Send an email alert when a session start event is detected.

- Take action (any combination of the following actions) when events are detected in recorded sessions
 - Send email alert
 - Start screen recording immediately (with or without lossy screen recording enabled)
 - Lock session
 - Log off session
 - Disconnect session

Click **Add event triggers** to create event triggers from scratch. Or, click **Browse templates** to select existing event trigger templates to use directly or customize.



Each time you click **Add event triggers**, a new event trigger is created in the pane below. You can also click the **Duplicate** button to make duplicates of an existing event trigger.

Configure event triggers and responses

For each event trigger, select a session event, configure additional conditions as needed, and specify the action to take when the event is detected.

[+ Add event trigger](#) [Browse templates](#) [Save as template](#)

If event type is

Then Send email alert and

Description:

If event type is

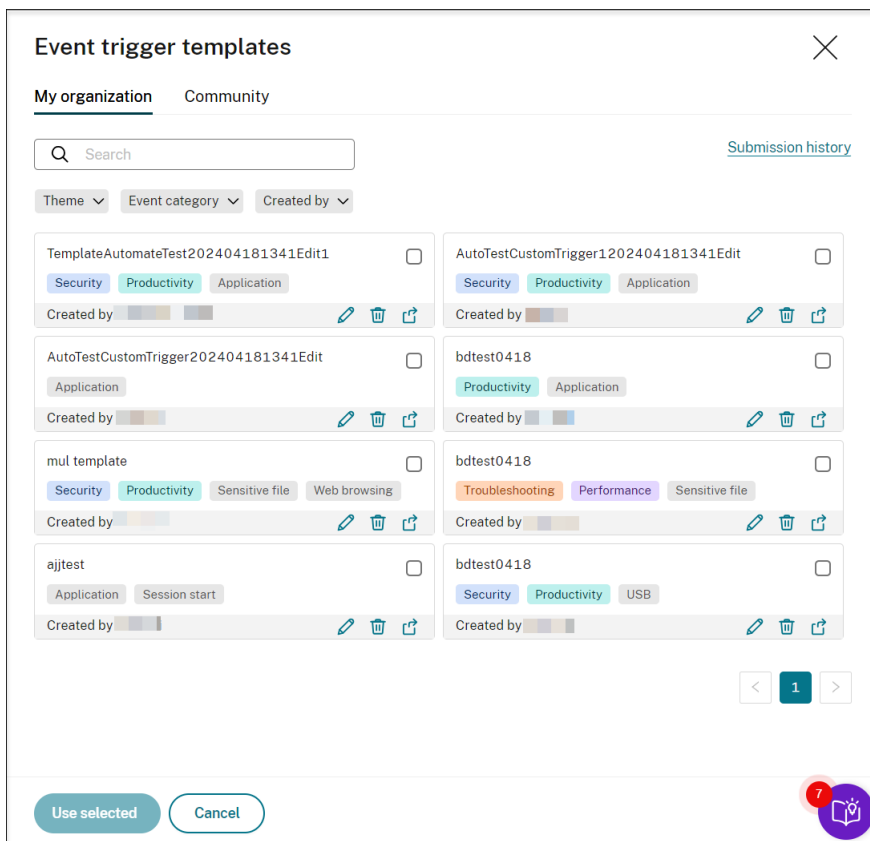
Then Send email alert and

Description:

- None
- Start screen recording**
- Log off session
- Disconnect session
- Lock session

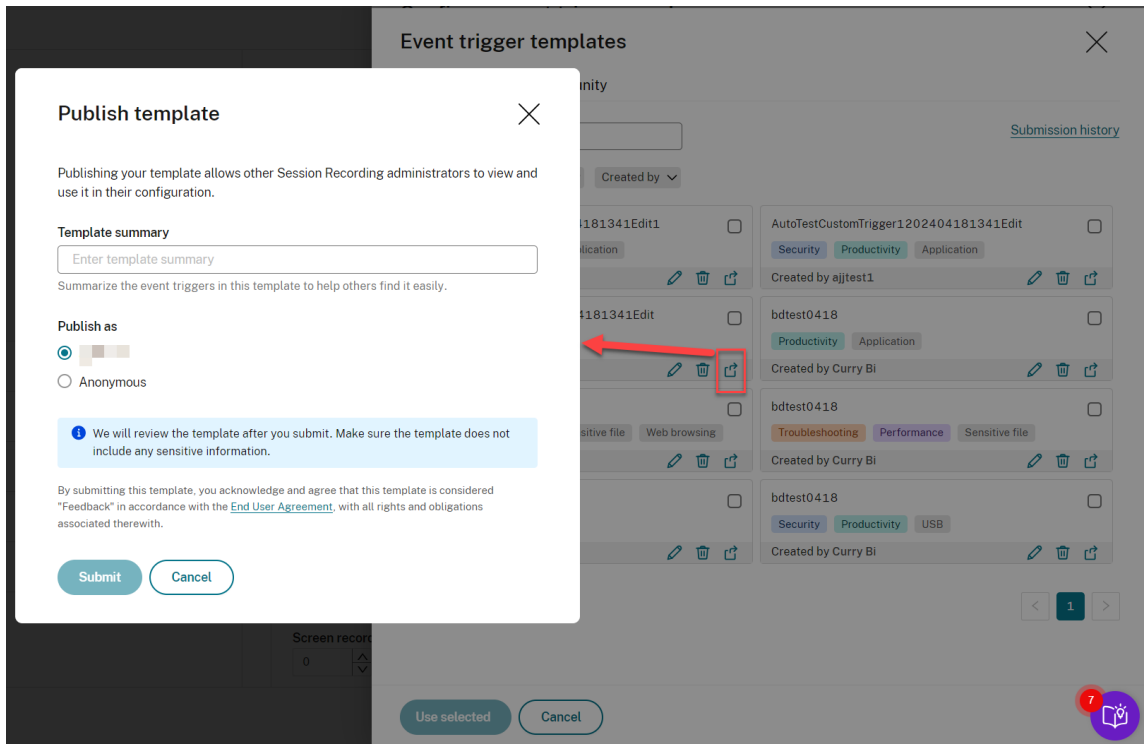
When you finish creating at least one event trigger, click **Save as template** to save your event triggers as a template. You can then find the new template on the **My organization** tab of the **Event trigger templates** page.

To access the **Event trigger templates** page, click **Browse Template** or click **Resource Library** from the left navigation pane of the Session Recording service page.



The **Event trigger templates** page accommodates all event trigger templates, both from your organization and from the other community members including Cloud Software Group itself.

On the **My organization** tab of the **Event trigger templates** page, you can publish your templates to the community for the other customers to access for free.



Note:

See the [End User Agreement](#) before submitting a template.

On the **My organization** or **Community** tab of the **Event trigger templates** page, you can search for target event trigger templates by keyword, theme, event category, and contributor. You can also bookmark or give likes to the templates of your interest.

You can select multiple event trigger templates at a time. The templates you select appear on the **Add event triggers** page where you can customize as needed.

Click **Save** to save your settings. You are taken back to the **Events and responses** page where the event triggers you specify are listed. Click **Configure** to further adjust your event triggers. If you select the **Send email alert** or **Start screen recording** action for any of your event triggers, follow the GUI to configure email settings and recording options.

Events and responses

Event triggers (6) Configure

Configure event triggers to trigger actions when certain events are detected.

Event type	Email alert	Action
Client drive mapping	✔ Yes	Lock session
File deletion	✔ Yes	Start screen recording
App start	⊘ No	None
App end	✔ Yes	Start screen recording
App start	⊘ No	Start screen recording
Client drive mapping	⊘ No	Start screen recording

i For your event triggers to work as expected, ensure that the relevant event types are logged by your active event detection policy.

Email settings

Applicable if you enabled **send email alert** in your event triggers.
To configure the email sender and content, go to **site settings** in **Configuration > Server Management**.

Recipients

Enter email addresses separated by semicolons (;)

Recording options

Applicable to the **start screen recording** action.

Screen recording time span after an event is detected (min) ?

0

^
v

Screen recording time span before an event is detected (sec) ?

0

^
v

Enable lossy screen recording

Session operation options

Applicable to the **log off session**, **disconnect session**, and **lock session** actions.

Delay before session operations begin (sec) ?

0

^
v

Note:

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

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, set the relevant parameters as illustrated later in this article. After that, dynamic screen recording automatically starts when certain events occur during an event-only recording.

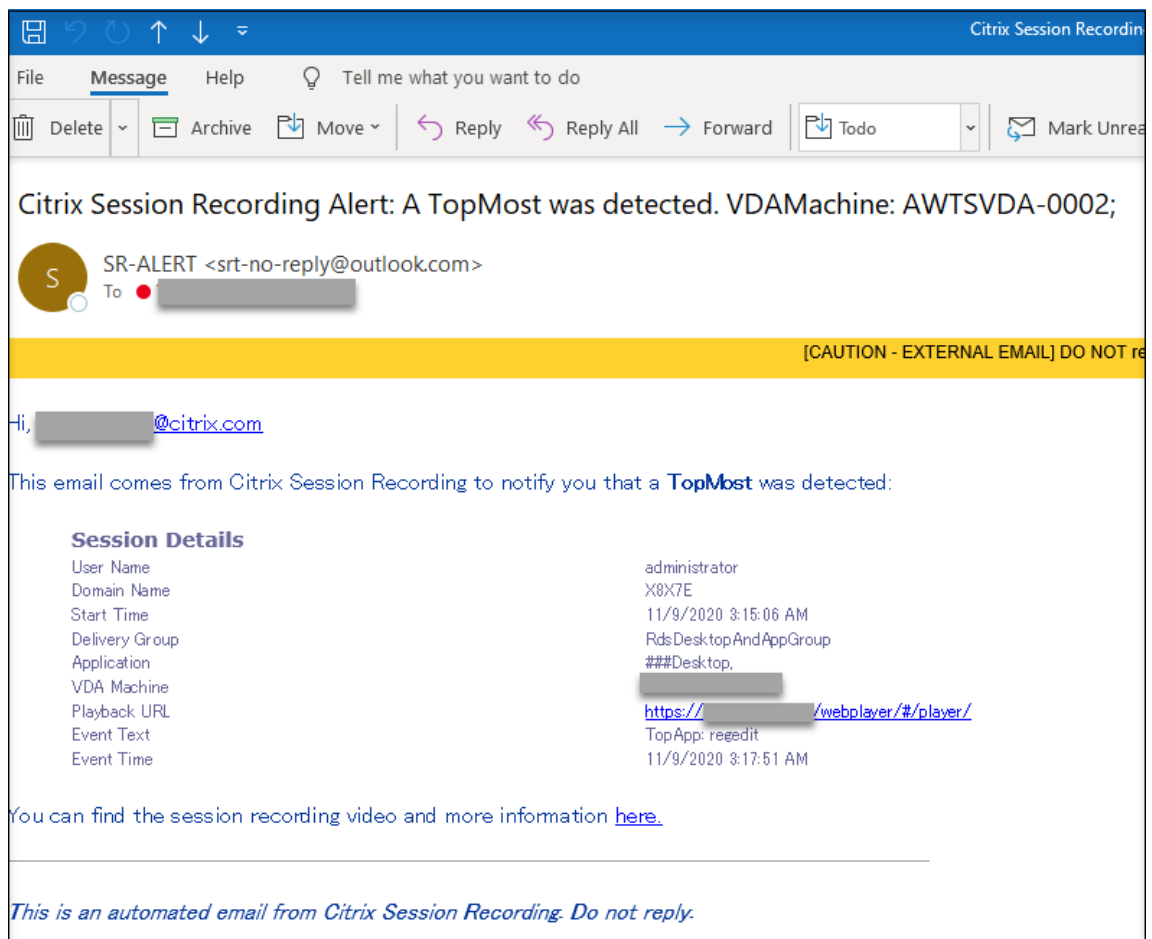
For a complete list of supported event types, see the following table.

Event type	Dimension	Option
App Start	App name	Includes, Equals, Matches
	Full command line	Includes, Equals, Matches
App End	App name	Includes, Equals, Matches
Top Most	App name	Includes, Equals, Matches
	Windows title	Includes, Equals, Matches
Web Browsing	URL	Includes, Equals, Matches
	Tab title	Includes, Equals, Matches
	Browser name	Includes, Equals, Matches
File Create	Path	Includes, Equals, Matches
	File size (MB)	Greater than, Between, Smaller than
File Rename	Path	Includes, Equals, Matches
	Name	Includes, Equals, Matches
File Move	Source path	Includes, Equals, Matches
	Destination path	Includes, Equals, Matches
	File size (MB)	Greater than, Between, Smaller than
File Delete	Path	Includes, Equals, Matches
	File size (MB)	Greater than, Between, Smaller than
CDM USB	Drive letter	Equals

Event type	Dimension	Option
Generic USB	Device name	Includes, Equals, Matches
	idle duration (Hrs)	Greater than
File Transfer	File source	Equals (“host” or “client”)
	File size (MB)	Greater than
	File name	Includes, Equals, Matches
Registry Create	Key name	Includes, Equals, Matches
	Key name	Includes, Equals, Matches
Registry Delete	Key name	Includes, Equals, Matches
	Key name	Includes, Equals, Matches
Registry Set Value	Key name	Includes, Equals, Matches
	Value name	Includes, Equals, Matches
Registry Delete Value	Key name	Includes, Equals, Matches
	Value name	Includes, Equals, Matches
Registry Rename	Key name	Includes, Equals, Matches
	Key name	Includes, Equals, Matches
User Account Modification	User name	Includes, Equals, Matches
	User name	Includes, Equals, Matches
Unexpected App Exit	App name	Includes, Equals, Matches
	App name	Includes, Equals, Matches
App Not Responding	App name	Includes, Equals, Matches
	App name	Includes, Equals, Matches
New App Installed	App name	Includes, Equals, Matches
	App name	Includes, Equals, Matches
App Uninstalled	App name	Includes, Equals, Matches
	App name	Includes, Equals, Matches

Event type	Dimension	Option
RDP Connection	App name	Includes, Equals, Matches
	IP address	Includes, Equals, Matches
Popup Window	Process name	Includes, Matches
	Window content	Includes, Equals, Matches
Performance Data	CPU usage (%)	Greater than
	Memory usage (%)	Greater than
	Net send (MB)	Greater than
	Net receive (MB)	Greater than
	RTT (ms)	Greater than
Clipboard Operation	Data type	Equals (Text, File, Bitmap)
	Process name	Includes, Equals, Matches
	Content	Includes, Equals, Matches

6. (Optional) Email settings are available after you choose **Send email alert** in your event triggers. For an example email alert, see the following screen capture:



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.

To send email alerts in response to detected events, complete the following settings:

- a) In the **Recipients** section of the **Events and responses** page, enter email addresses for the target recipients.
- b) On the **Email alerts** page of your **Site settings**, specify the email sender and content.

Site settings
SRN2203

General

Storage maintenance

Email alerts

SMTP server
bd

Port
25 Enable SSL

Display name
d

Email address
[redacted]@citrix.com

Password
[redacted]

Email subject	Email body
<input checked="" type="checkbox"/> User name	<input type="checkbox"/> User name
<input checked="" type="checkbox"/> Domain name	<input checked="" type="checkbox"/> Domain name
<input type="checkbox"/> Start Time	<input checked="" type="checkbox"/> Start Time
<input type="checkbox"/> Delivery group	<input type="checkbox"/> Delivery group
<input type="checkbox"/> Application	<input type="checkbox"/> Application
<input type="checkbox"/> VDA machine	<input type="checkbox"/> VDA machine
	<input type="checkbox"/> Recording URL

Apply changes Cancel

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 that 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 called **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's a limit for sending emails within a given period. For example, when the daily limit is reached, you can't 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.

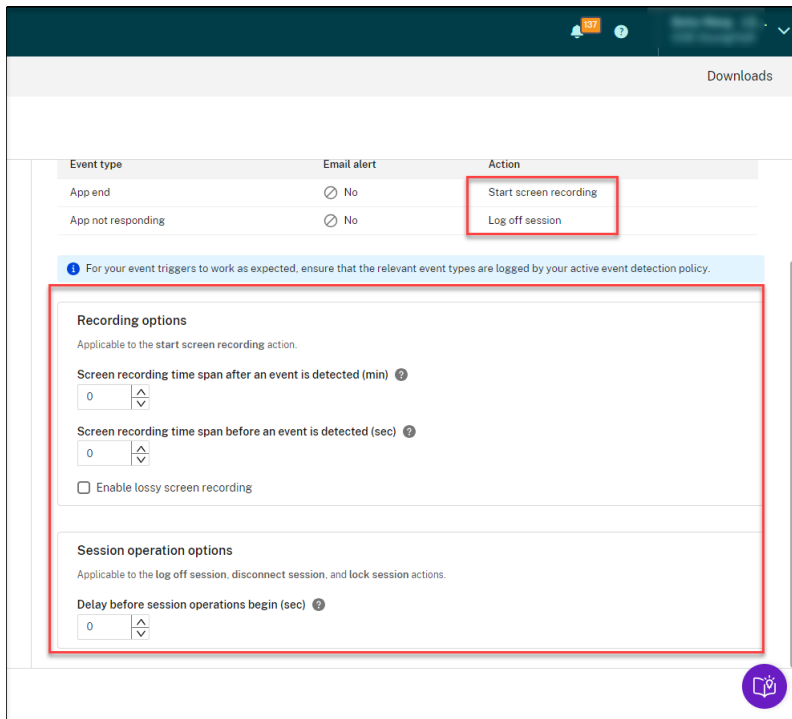
7. (Optional) To start screen recording immediately when certain events occur during an event-only recording, set the following options for dynamic screen recording in the **Recording options** section:

- **Screen recording time span after an event is detected (min):** You can configure the time duration (minutes) that 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 before an event is detected (sec):** You can configure the time duration (seconds) of the screen recording you want to keep before events are detected. 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.
- **Enable lossy screen recording:** You can specify whether to enable lossy screen recording when a session event is detected. Lossy screen recording lets you adjust compression options to reduce the size of recording files and to accelerate navigating recorded sessions during playback. This feature is available with Session Recording 2308 and later. For more information, see [Enable or disable lossy screen recording](#).

8. (Optional) Specify delay before session operations begin (sec). If you specify any of the following actions in response to logged events in recorded sessions, you can notify users of the actions in advance:

- Lock session
- Log off session
- Disconnect session

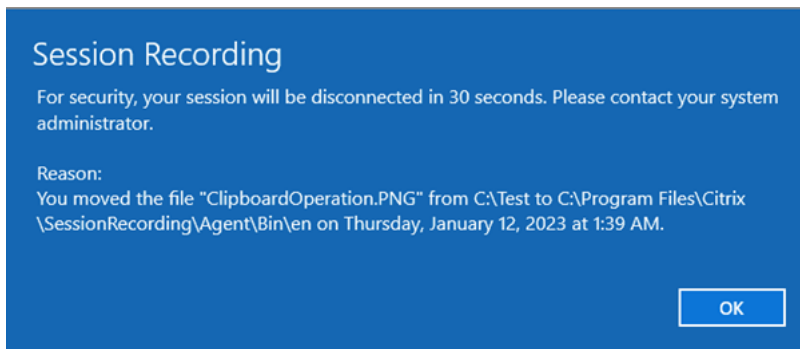
For example:



Note:

If you set the value to 0, it means that users aren't notified when you lock, log off, or disconnect them from their virtual sessions. To notify users, set an appropriate value.

For an example notice, see the following screen capture:

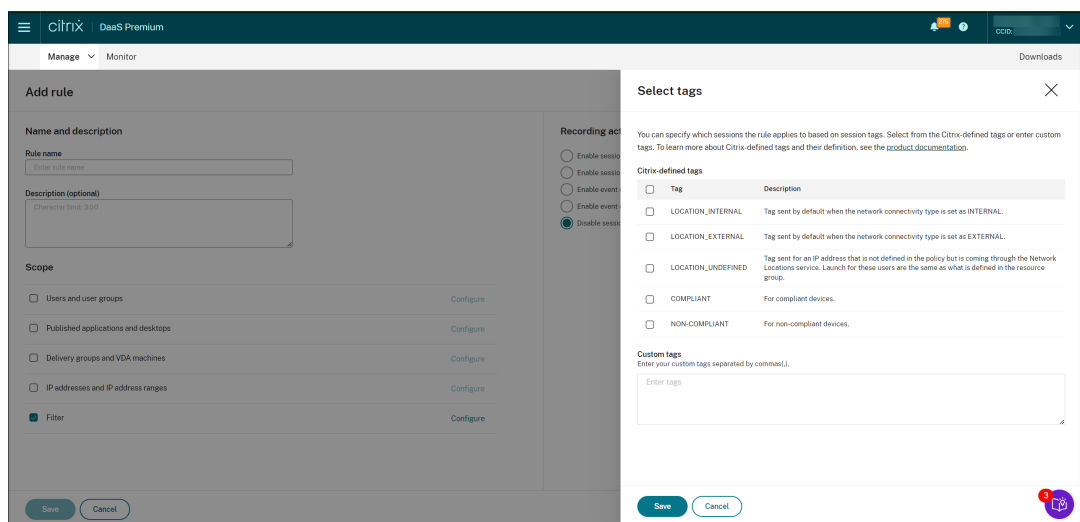


9. Select and edit the rule scope.

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. Both Azure Active Directory (Azure AD) and Active Directory identity types are supported. For more information, see the instructions in the [Create a custom recording policy](#) section.

- **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.
- **Filter.** Creates a list of smart access tags to which the rule applies. You can configure contextual access (smart access) using smart access policies on Citrix NetScaler, [Citrix Device Posture service](#), and [Adaptive access based on the user's network location](#).



Contextual access (smart access) is available with Session Recording 2402 and later.

It lets you apply policies based on the user access context including:

- The user's location
- IP address range
- Delivery group
- Device type
- Installed applications

Note:

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

10. Follow the wizard to complete the configuration.
11. Activate the new event response policy.

Video about configuring policies



Playback permissions

February 19, 2024

Session Recording administrators and their playback permissions

Session Recording administrators are Citrix Cloud administrators assigned a permission to access the Session Recording service. For an overview of Session Recording administrators and their playback permissions, see the following table:

Type of Session Recording administrator	Playback permission	Remarks
Citrix Cloud administrator assigned full access	Can play all recordings	Shows as a full admin on the Playback Permissions page of the Session Recording service
Citrix Cloud administrator assigned the Cloud Administrator, All role	Can play all recordings	Shows as a full admin on the Playback Permissions page of the Session Recording service

Type of Session Recording administrator	Playback permission	Remarks
Citrix Cloud administrator assigned the Session Recording-FullAdmin, All role	Can play all recordings	Shows as a full admin on the Playback Permissions page of the Session Recording service
Citrix Cloud administrator assigned the Session Recording-PrivilegedPlayerAdmin, All role	Can play all recordings	Shows as a privileged player on the Playback Permissions page of the Session Recording service
Citrix Cloud administrator assigned only the Session Recording-ReadOnlyAdmin, All role	Can play all recordings except restricted 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.	Shows as a full admin on the Playback Permissions page of the Session Recording service by default, or shows as a read-only admin on the Playback Permissions page of the Session Recording service when you specify the scope.

- For information about restricted recordings, see [Place access restrictions on recordings](#).
- Citrix Cloud administrators assigned only the **Session Recording-ReadOnlyAdmin, All** role are called Session Recording read-only administrators later in this article. For more information, see [Types of Session Recording administrators](#). You can limit playback permissions so that Session Recording read-only administrators can play only specific recordings from a target site.

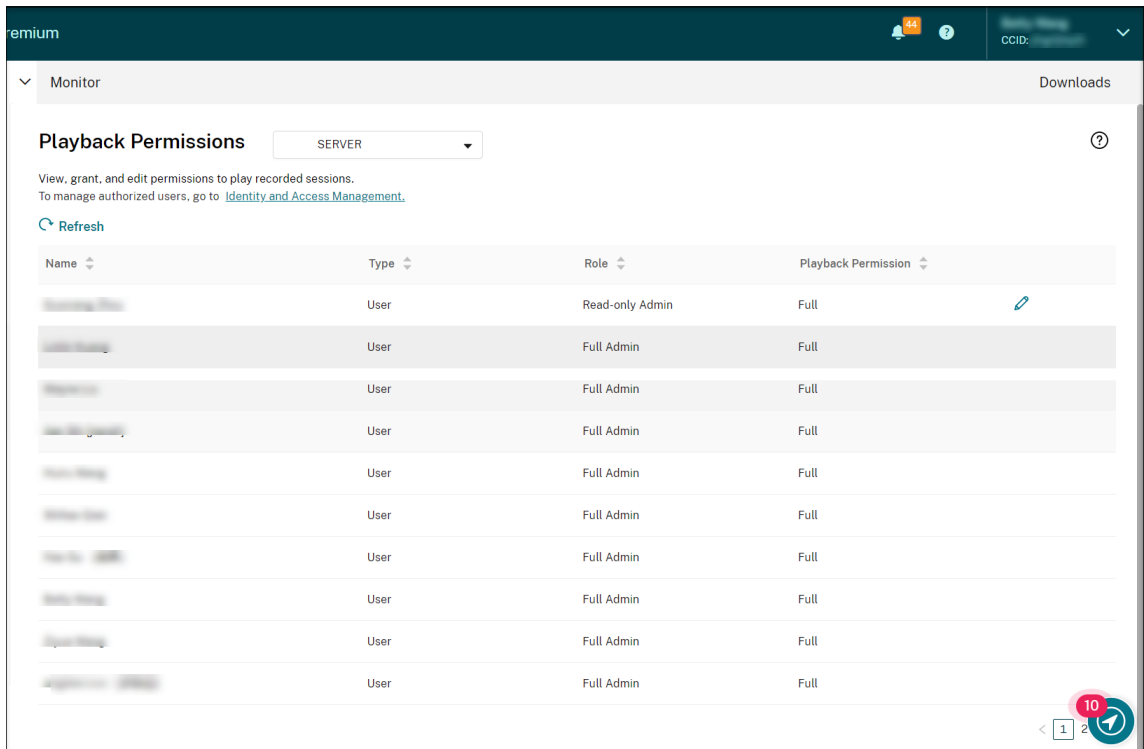
Limit the playback permission of a Session Recording read-only administrator

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

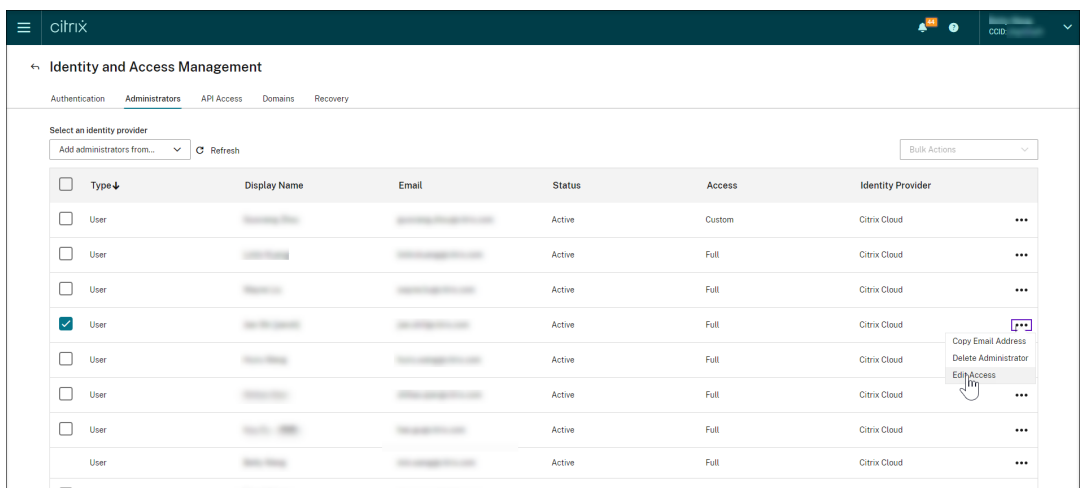
1. Select **Configuration > Playback Permissions** from the left navigation of the Session Recording service.

Note:

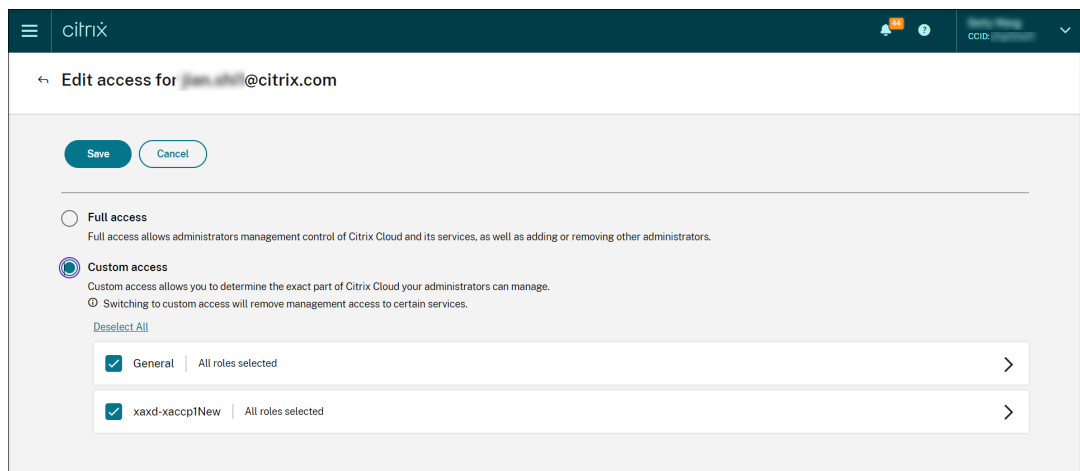
- The **Playback Permissions** menu in the left navigation of the Session Recording service is invisible for the administrators that are added through Azure AD groups. It is also invisible for Session Recording read-only administrators.
- All Session Recording administrators are listed on the **Playback Permissions** page.



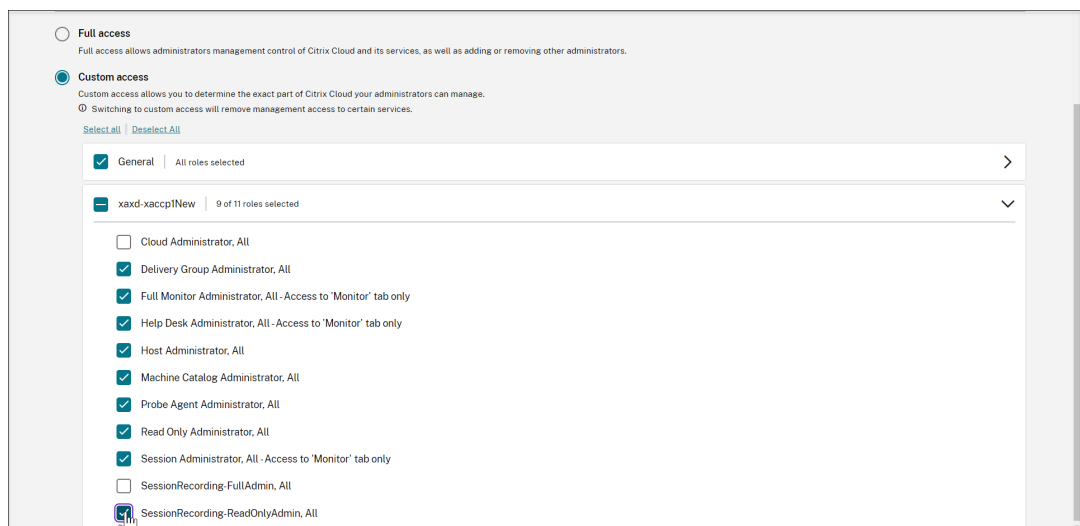
2. Select a target site.
3. Target an administrator on the **Playback Permissions** page. To make the administrator a Session Recording read-only administrator, complete the following steps:
 - a) Go to the **Identity and Access Management > Administrators** tab of the Citrix Cloud console.
 - b) Locate the target administrator, click the ellipsis button, and select **Edit** access.



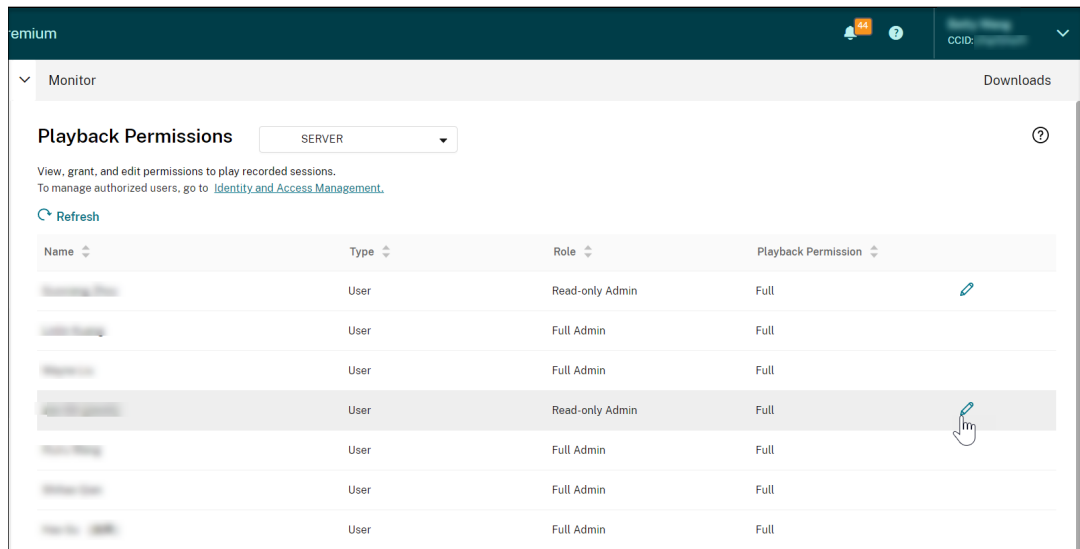
- c) Select **Custom access**.



- d) Click the angle bracket to expand all roles.
- e) Clear the check marks next to **Cloud Administrator, All**, **Session Recording-FullAdmin, All**, and **Session Recording-PrivilegedPlayerAdmin, All**. Select the check mark next to **Session Recording-ReadOnlyAdmin, All**.



- f) Click **Save**.
- g) 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.

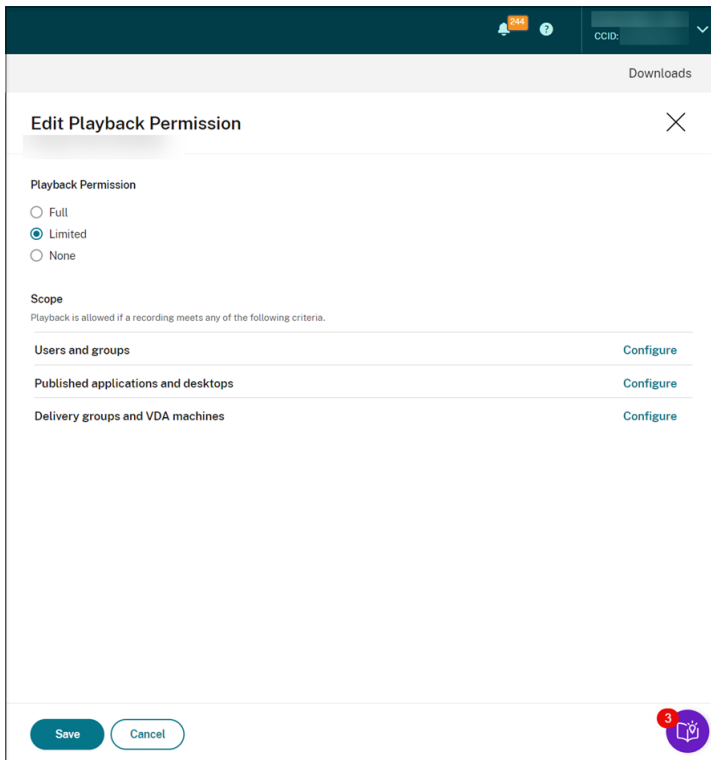


4. Click the **Edit** icon in the row of the Session Recording read-only administrator.

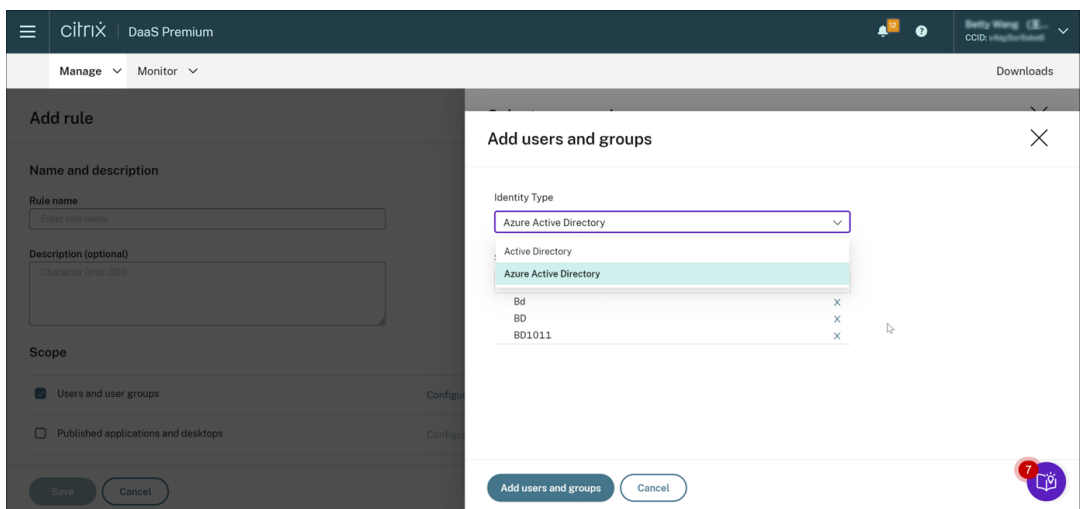
Tip:

A Session Recording read-only 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.

5. To limit the recordings that the Session Recording read-only administrator can play, choose **Limited** on the **Edit Playback Permission** page. The **Scope** section appears on the **Edit Playback Permission** page.



6. Click **Configure** to specify the scope of recordings that the Session Recording read-only administrator can play. Playback is allowed if a recording meets any of the following criteria.
- **Users and user groups.** Sets that the Session Recording read-only administrator can replay only the sessions that are opened by specific users and user groups. Both Azure Active Directory (Azure AD) and Active Directory identity types are supported.



Note:

- The Azure AD identity support for configuring playback permissions is avail-

able with Session Recording server 2402 and later. It is a preview feature. Preview features might not be fully localized and are recommended for use in non-production environments. Citrix Technical Support doesn't support issues found with preview features.

- The corresponding identity type is displayed only when the site is connected to AD or Azure AD through Citrix Cloud's Identity and Access Management (IAM). You can check it on the **Authentication** tab of Citrix Cloud's IAM.

- **Published applications and desktops.** Sets that the Session Recording read-only administrator can replay only specific application and desktop sessions.
- **Delivery groups and VDA machines.** Sets that the Session Recording read-only administrator can replay only the sessions of specific delivery groups and VDAs.

Your settings might not show on the **Playback Permissions** page. The issue occurs after you upgrade to Session Recording 2204 or the initial release of Session Recording 2203 LTSR. As a workaround, run the following script in SQL Server Management Studio (SSMS) that corresponds to your Session Recording database:

```
1 ALTER procedure [dbo].[EnumPlayerUserDeliveryGroupPoliciesOnCloud]
2 as
3 begin
4 set nocount on
5
6 select 3 as RoleType,
7 a.ID as RoleAccountID,
8 h.principleName as PrincipleName,
9 a.IsEnabled as IsEnabled,
10 e.name as PolicyType,
11 d.DeliveryGroupID as AccountMemberAccountID,
12 g.Name as AccountMemberName
13
14 from PlayerUserCloudAccountRoleConfigure a,
15 PlayerUserPolicyConfigSetMember b,
16 PlayerUserPolicyDeliveryGroupSetMember d,
17 PlayerUserPolicyType e,
18 DeliveryGroup g,
19 PlayerUserCloudAccount h
20 where e.id=5
21 and b.PlayerUserPolicyTypeID = e.ID
22 and a.PlayerUserPolicyConfigSetID = b.PlayerUserPolicyConfigSetID
23 and b.PolicySetID = d.PlayerUserPolicyDeliveryGroupSetID
24 and g.ID=d.DeliveryGroupID
25 and h.ID=a.CloudAccountID
26
27 end
28 <!--NeedCopy-->
```

[SRT-8028]

Administrator permissions

March 27, 2024

Assign administrative permissions

To assign permissions to administrators, go to the **Administrators** tab on the **Identity and Access Management** page of Citrix Cloud.

Video about assigning permissions to administrators:



Types of Session Recording cloud administrators

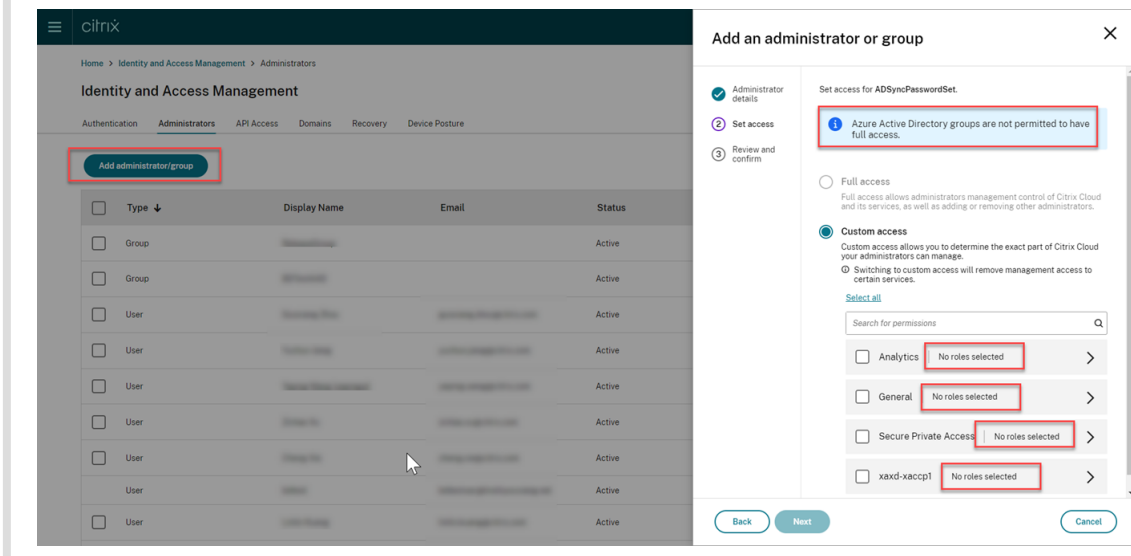
For the Session Recording service specifically, there are three types of cloud administrators, which are achieved by assigning different roles:

Type of Session Recording cloud administrator	Description
Full admin	Refers to a Citrix Cloud administrator assigned Full access , the Cloud Administrator, All role, or the Session Recording-FullAdmin, All role.

Type of Session Recording cloud administrator	Description
Privileged player admin	Refers to a Citrix Cloud administrator assigned only the Session Recording-PrivilegedPlayerAdmin, All role, or assigned the Session Recording-PrivilegedPlayerAdmin, All and the Session Recording-ReadOnlyAdmin, All roles.
Read-only admin	Refers to a Citrix Cloud administrator assigned only the Session Recording-ReadOnlyAdmin, All role.

Note:

The administrators that you add through Azure AD groups don't have any permissions initially. To assign them permissions, specify custom access that aligns with the administrators' roles in your organization.



Add administrators from Azure AD

Administrative access to the Session Recording service is enabled for Azure Active Directory (AD) users and groups.

A general workflow to use the feature is as follows:

1. Connect your Citrix Cloud account to your Azure AD. For more information, see [Connect Citrix Cloud to Azure AD](#).

2. Add administrators to Citrix Cloud from Azure AD.

Citrix Cloud supports adding administrators either individually or as Azure AD groups.

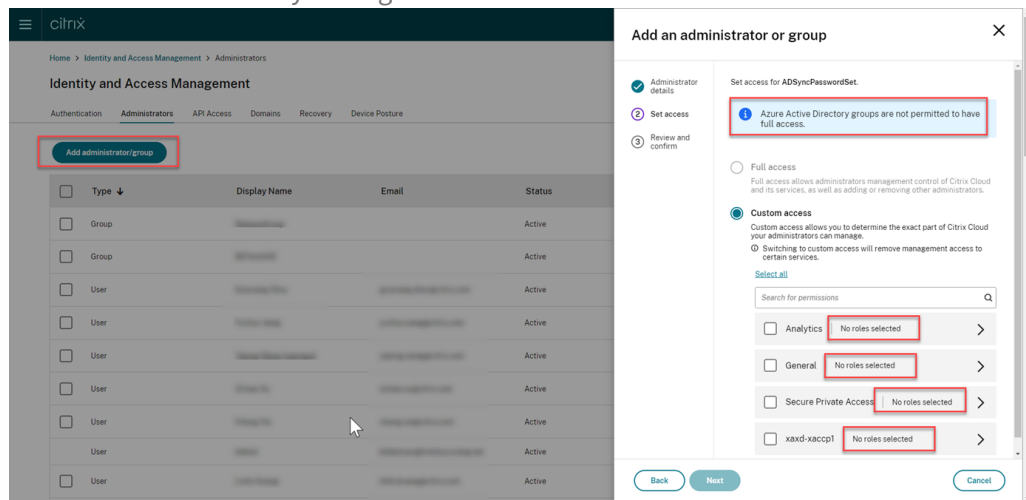
- To add individual administrators from Azure AD, see [Add new administrators](#). When you add an administrator, Citrix sends them an invitation email. Before the administrator can sign in, they must accept the invitation.
- To add Azure AD administrator groups to Citrix Cloud, see [Add an administrator group to Citrix Cloud](#). Administrators that you add through Azure AD groups don't receive invitations and can sign in to Citrix Cloud immediately after you add them.

3. Specify permissions for the administrators that you add.

For Session Recording specifically, there are three types of administrators, which are achieved by assigning different roles. For more information, see [Types of Session Recording administrators](#).

Note:

- The administrators that you add through Azure AD groups don't have any permissions initially. To assign them permissions, specify custom access that aligns with the administrators' roles in your organization.



- The **Playback Permissions** menu in the left navigation of the Session Recording service is invisible for the administrators that are added through Azure AD groups.
- The **Generate command** button for cloud client installation is unavailable for the administrators that are added through Azure AD groups.

Permissions of Session Recording administrators

For the permissions of Session Recording administrators, see the following table:

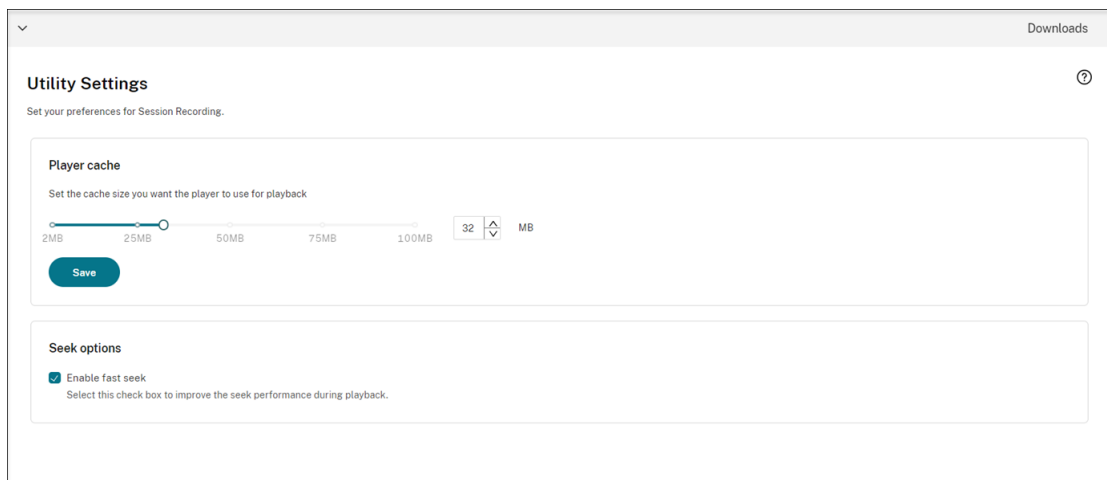
	Full admin	Privileged player admin	Read-only admin
Access the Dashboard page	Enabled	Disabled	Disabled
Configure server settings	Enabled	Disabled	Disabled
Configure policies	Enabled	Disabled	Disabled
Place access restrictions on recordings	Enabled	Enabled	Enabled
Remove access restrictions on recordings	Enabled	Enabled	Disabled
Archive and delete recordings manually	Enabled	Enabled	Disabled
Archive and delete recordings automatically	Enabled	Disabled	Disabled
Configure playback permissions	Enabled	Disabled	Disabled

For information on configuring permissions for Session Recording read-only administrators, see [Configure playback permissions](#).

Configure preferences

September 6, 2023

To configure your preferences for Session Recording, select **Configuration > Utility Settings** from the left navigation.



You can configure the following preferences for Session Recording:

- **Player cache.** Drag the slider to set the cache size you want the player to use for playback.
- **Fast seek.** You can enable fast seeking through ICA screen recording by configuring how often an I-Frame is generated. This feature significantly improves the playback seeking experience and is available with Session Recording 2308 and later.

View recordings

June 11, 2024

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.

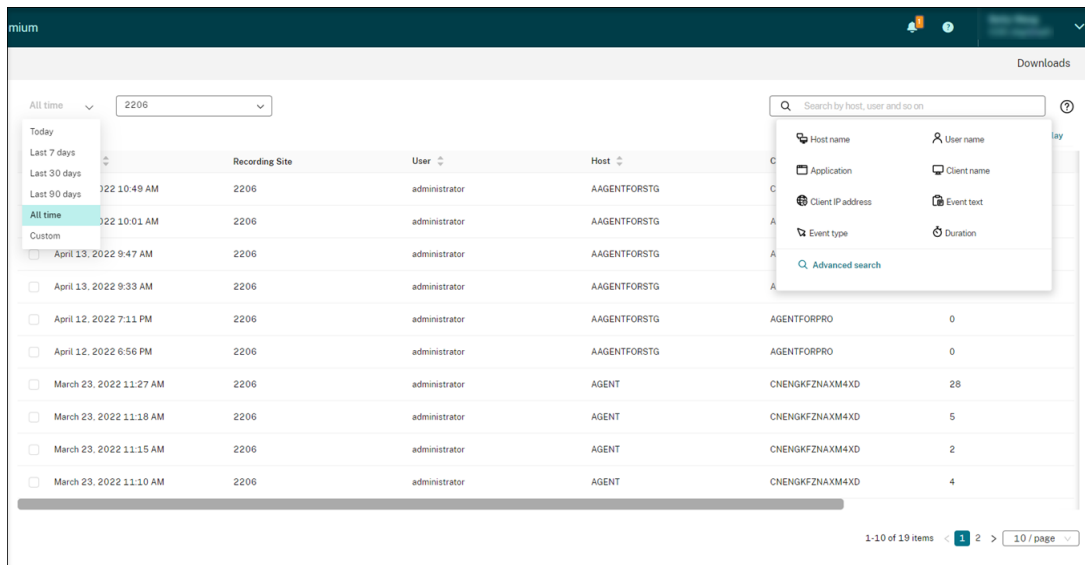
Search for recordings

September 12, 2022

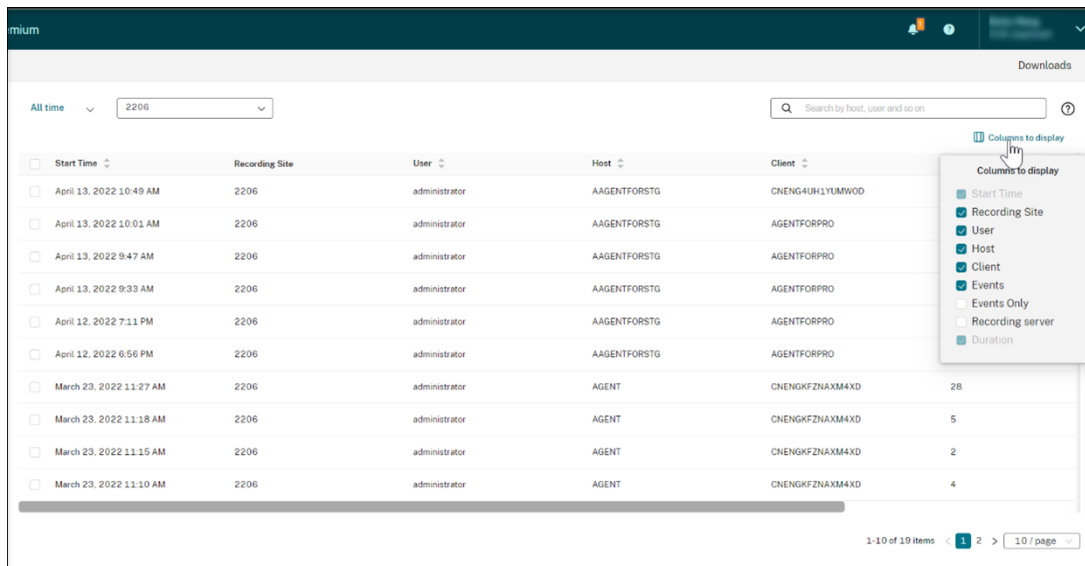
Search for recordings

On each subpage of **Recordings**, 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.
- Filters include **Host name**, **Client name**, **User name**, **Application**, **Client IP address**, **Event text**, **Event type**, and **duration**.
- Advanced search criteria.

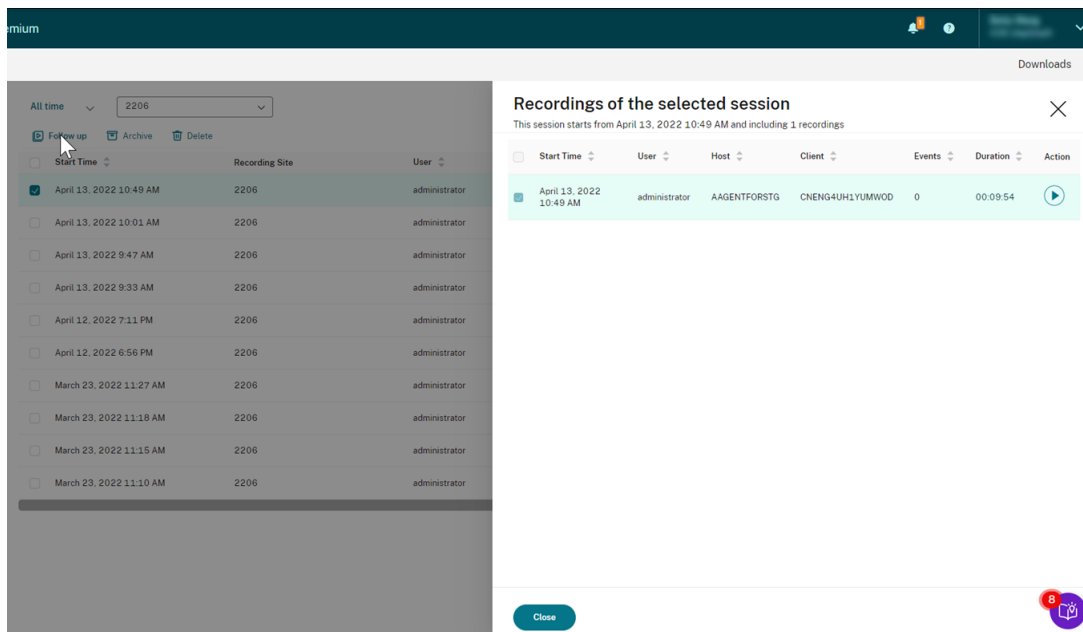


You can also specify **Columns to display**.



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.



Place access restrictions on recordings

November 17, 2022

Overview

You can restrict access to selected recordings from within the Session Recording service. In addition to [playback permissions](#), this feature provides more granular access control.

Citrix Cloud administrators assigned any of the following access permissions are allowed to place access restrictions on recordings:

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

Restricted recordings are not accessible to Session Recording read-only administrators, that is, Citrix Cloud administrators assigned **only** the **Session Recording-ReadOnlyAdmin, All** role. Session

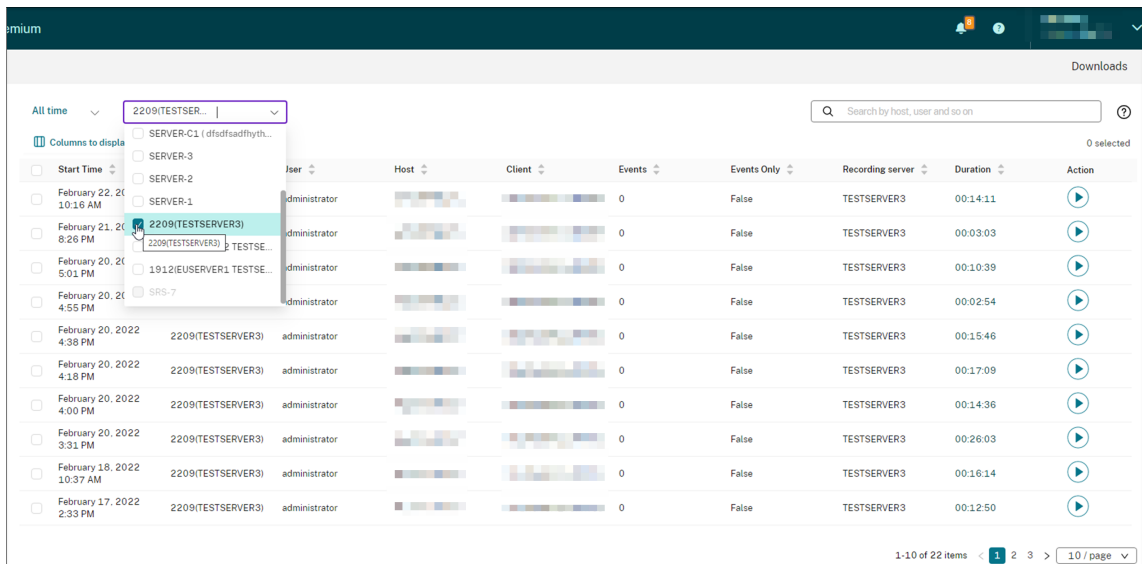
Recording read-only administrators do not have permission to access the **Restricted** page or remove access restrictions on the page.

Note:

- This feature requires Session Recording server 2209 or later.
- Placing access restrictions on live recordings is not supported.

Place and remove access restrictions on target recordings

1. Select **Recordings > All Recordings** from the left navigation of the Session Recording service.
2. Select a site consisting of Session Recording server 2209 or later.



3. On the **All Recordings** page, select one or more target recordings.

Note:

We recommend you select no more than 40 recordings at a time. Otherwise, access restrictions can fail.

4. Click **Place access restrictions**.

Session Recording service

Downloads

All time 2209(TESTSER... Search by host, user and so on

Columns to display Follow up Place access restrictions Archive Delete 2 selected

<input type="checkbox"/>	Start Time	Recording Site	User	Host	Client	Events	Events Only	Recording server	Duration	Action
<input checked="" type="checkbox"/>	February 22, 2022 10:16 AM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:14:11	
<input checked="" type="checkbox"/>	February 21, 2022 8:26 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:03:03	
<input type="checkbox"/>	February 20, 2022 5:01 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:10:39	
<input type="checkbox"/>	February 20, 2022 4:55 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:02:54	
<input type="checkbox"/>	February 20, 2022 4:38 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:15:46	
<input type="checkbox"/>	February 20, 2022 4:18 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:17:09	
<input type="checkbox"/>	February 20, 2022 4:00 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:14:36	
<input type="checkbox"/>	February 20, 2022 3:31 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:26:03	
<input type="checkbox"/>	February 18, 2022 10:37 AM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:16:14	
<input type="checkbox"/>	February 17, 2022 2:33 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:12:50	

1-10 of 22 items 1 2 3 10 / page

5. Read the prompt and then click **Confirm**.

Downloads

All time 2209(TESTSER... Search by host, user and so on

Columns to display Follow up Place access restrictions Archive Delete 1 selected

Place access restrictions

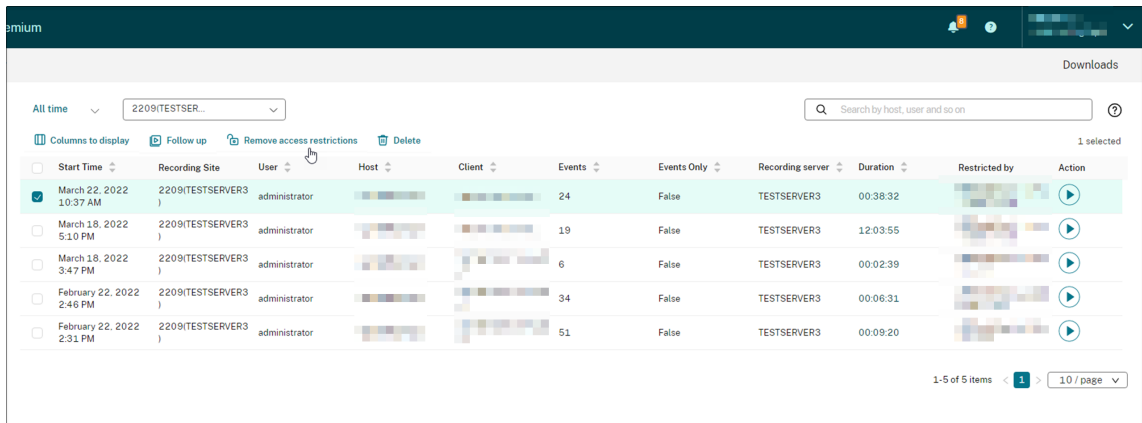
Are you sure you want to restrict access to the selected recordings?
Restricted recordings are accessible only to privileged players.
Note: A single recorded session can produce more than one recording. If you select any recording of a session, the access restrictions apply to all other recordings of the same session.

Confirm **Cancel**

<input type="checkbox"/>	Start Time	Recording Site	User	Host	Client	Events	Events Only	Recording server	Duration	Action
<input checked="" type="checkbox"/>	February 22, 2022 10:16 AM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:14:11	
<input type="checkbox"/>	February 21, 2022 8:26 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:03:03	
<input type="checkbox"/>	February 20, 2022 5:01 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:10:39	
<input type="checkbox"/>	February 20, 2022 4:55 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:02:54	
<input type="checkbox"/>	February 20, 2022 4:38 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:15:46	
<input type="checkbox"/>	February 20, 2022 4:18 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:17:09	
<input type="checkbox"/>	February 20, 2022 4:00 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:14:36	
<input type="checkbox"/>	February 20, 2022 3:31 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:26:03	
<input type="checkbox"/>	February 18, 2022 10:37 AM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:16:14	
<input type="checkbox"/>	February 17, 2022 2:33 PM	2209(TESTSERVER3)	administrator			0	False	TESTSERVER3	00:12:50	

1-10 of 22 items 1 2 3 10 / page

6. Verify that the selected recordings on which you placed access restrictions are moved from the **All Recordings** page to the **Restricted** page.
7. On the **Restricted** page, remove access restrictions as needed. With access restrictions removed, recordings are moved back to the **All Recordings** page.



The screenshot shows the Citrix DaaS Premium interface with a table of recordings. The table has columns for Start Time, Recording Site, User, Host, Client, Events, Events Only, Recording server, Duration, Restricted by, and Action. The first row is selected, showing a recording from March 22, 2022, at 10:37 AM, with a duration of 00:38:32. The Action column contains a play button icon.

Start Time	Recording Site	User	Host	Client	Events	Events Only	Recording server	Duration	Restricted by	Action
March 22, 2022 10:37 AM	2209(TESTSERVER3)	administrator	[blurred]	[blurred]	24	False	TESTSERVER3	00:38:32	[blurred]	[play button]
March 18, 2022 5:10 PM	2209(TESTSERVER3)	administrator	[blurred]	[blurred]	19	False	TESTSERVER3	12:03:55	[blurred]	[play button]
March 18, 2022 3:47 PM	2209(TESTSERVER3)	administrator	[blurred]	[blurred]	6	False	TESTSERVER3	00:02:39	[blurred]	[play button]
February 22, 2022 2:46 PM	2209(TESTSERVER3)	administrator	[blurred]	[blurred]	34	False	TESTSERVER3	00:06:31	[blurred]	[play button]
February 22, 2022 2:31 PM	2209(TESTSERVER3)	administrator	[blurred]	[blurred]	51	False	TESTSERVER3	00:09:20	[blurred]	[play button]

Open and play recordings

January 30, 2024

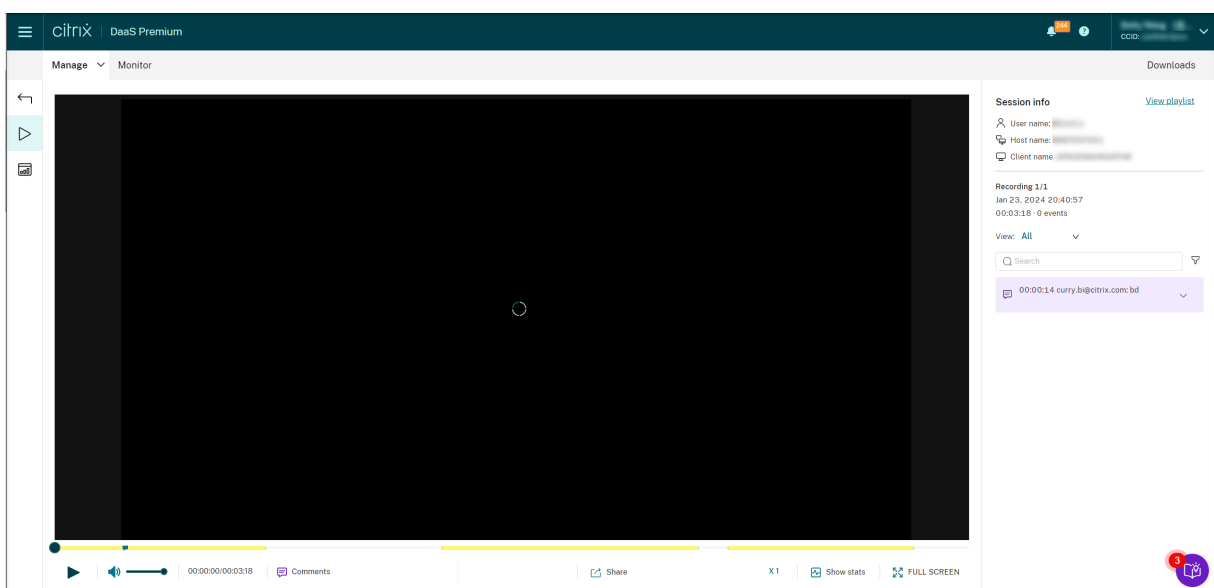
Open and play recordings

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 a GPU for a better playback experience on it.

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



The screenshot shows the Citrix DaaS Premium playback interface. The main area is a large black video player with a play button on the left. Below the player is a progress bar and a volume control. On the right side, there is a 'Session info' panel with fields for User name, Host name, and Client name. Below that, it shows 'Recording 1/1' with a timestamp of 'Jan 23, 2024 20:40:57' and '00:03:18 - 0 events'. There is a search bar and a dropdown menu showing '00:00:14 curry.bi@citrix.com.bd'. At the bottom right, there is a 'FULL SCREEN' button and a notification icon.

Tip:

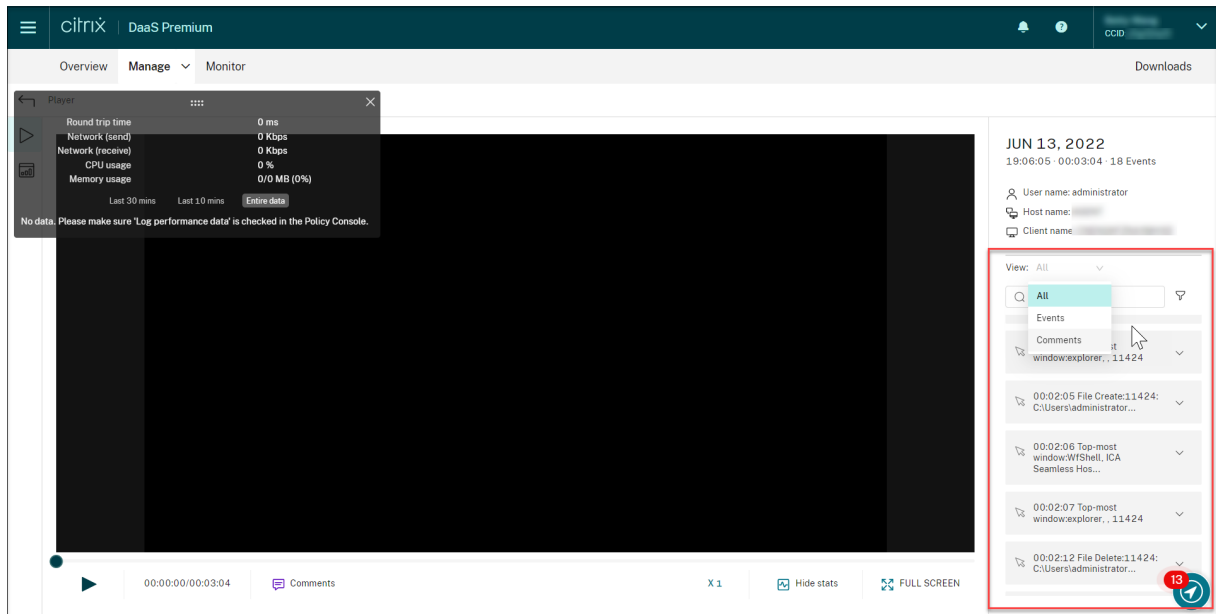
- Clicking the session progress time lets you switch to the absolute date and time the session was recorded.
- For an event-only recording, the play icon in the upper left corner is unavailable.

Player controls

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

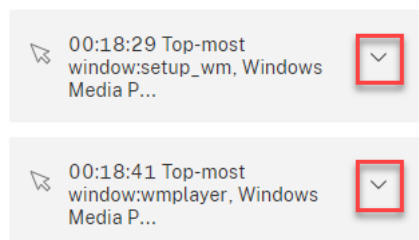
Player Control	Description
Play button	Plays the selected recording file.
Mute/unmute button	Determines whether to remove audio during playback.
Progress bar	You can drag the progress bar during playback. Idle periods of recorded sessions are highlighted during playback.
Current position of recording playback	Indicates the current position of the recording playback and the total recording duration. The time format is HH:MM:SS.
Comments	Lets you click and leave a comment about the recording being played.
Share	Lets you share the recording as restricted and unrestricted links.
Show stats	Shows the overlay that features data points related to the recorded session.
Hide stats	Hides the session data overlay.
Playback speed	Indicates the current speed of playback. Click the icon to switch between options including X0.5, X1, X2, and X4.
Full screen	Displays the playback in full screen.
Exit full screen button	Displays the playback within the webpage.

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.
- 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 display 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.

Share recordings as links

January 30, 2024

Overview

You can share recordings as restricted and unrestricted links from the cloud player. Other users can use the links to access the shared recordings directly, which obliterates the need to search among many recordings. If you share a recording as a restricted link, only users who already have [playback permission](#) can view the recording using the link. If you share a recording as an unrestricted link, anyone in your AD domain can view the recording using the link.

For unrestricted recording sharing, you can further:

- Specify whether to issue email notifications to specific recipients when an unrestricted recording link is generated. For more information, see [Notifications](#).
- View the events related to unrestricted recording sharing on the **Events** tab of the [activity feed](#).

To facilitate managing unrestricted links, the Session Recording service lets you:

- Set a validity period for each of the links.
- (Optional) Enter a justification when generating the links.
- Get an overview of which recordings have been shared as unrestricted links.
- View all unrestricted links of a specific recording.
- Know which users have accessed an unrestricted link.
- Revoke unrestricted links that haven't expired.
- Clear invalid links that have expired or revoked.

To share recordings as links and manage unrestricted links, you **must** have full access to the Session Recording service. It means that you must be a Citrix Cloud administrator assigned any of the following permissions:

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

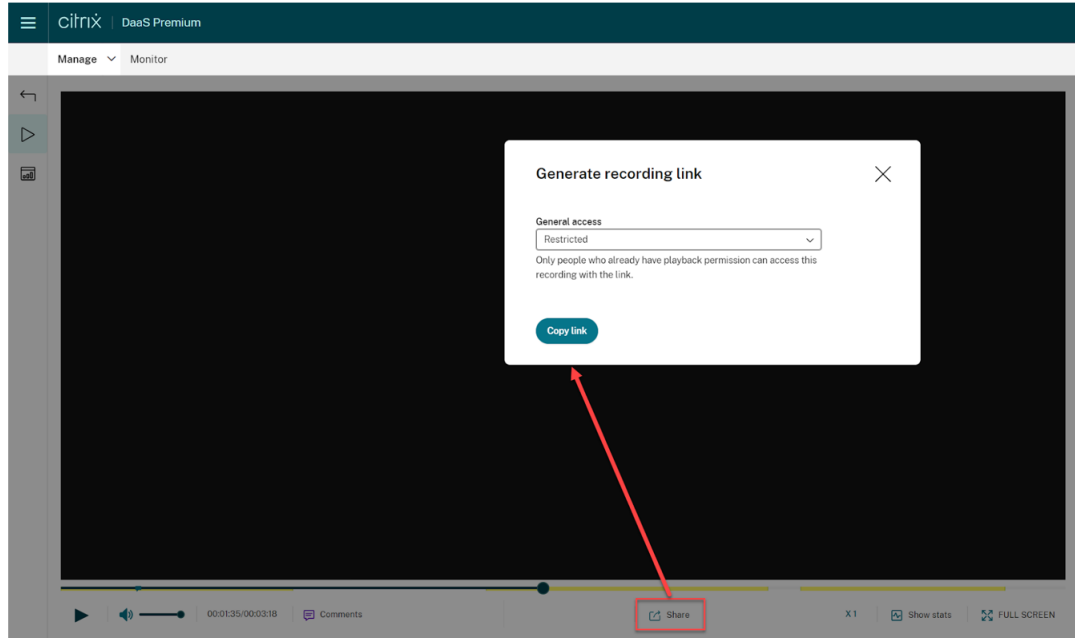
Note:

- To view a recording using an unrestricted link, users must enter a justification.

Share recordings as restricted links

To share recordings as restricted links, complete the following steps:

1. In the cloud player, open and play the recording that you want to share.
2. Click **Share** on the playback page of the recording. The **Generate recording link** dialog appears.



3. Select **Restricted** from the **General access** drop-down.
4. Click **Copy link**.

After you click **Copy link**, either of the following messages appears, indicating a successful or failed operation respectively:

- **The URL to the shared recording has been copied to the clipboard**
- **Sharing the recording URL failed**

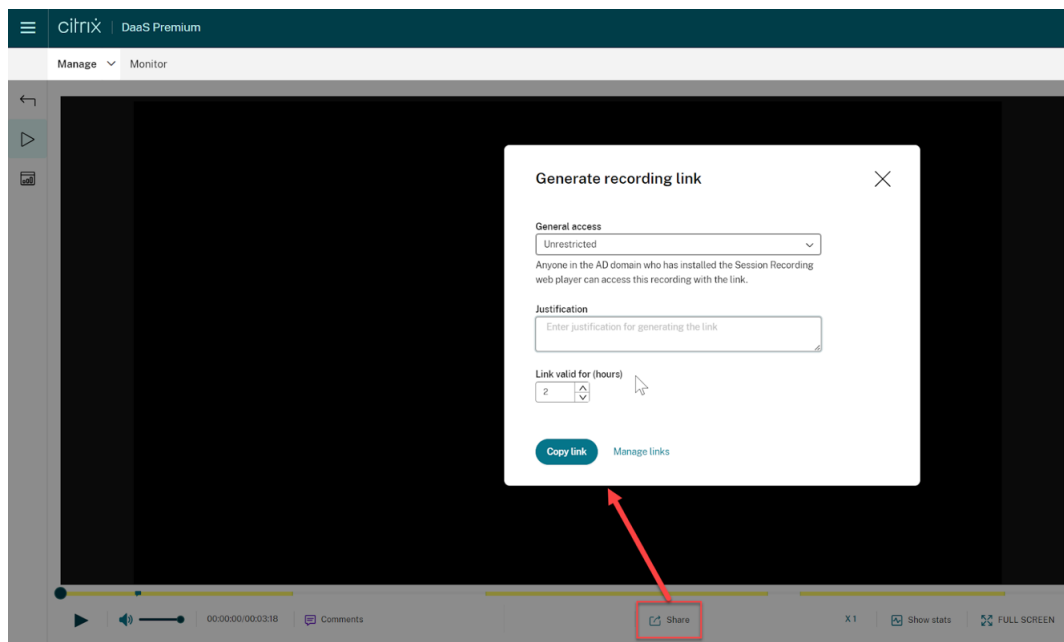
5. Share the generated URL link with users who already have playback permission.

Pasting the link in the address bar lets you jump to the location where the link was copied.

Share recordings as unrestricted links

To share recordings as unrestricted links, complete the following steps:

1. In the cloud player, open and play the recording that you want to share.
2. Click **Share** on the playback page of the recording. The **Generate recording link** dialog appears.
3. Select **Unrestricted** from the **General access** drop-down.



4. (Optional) Enter your justification for sharing the recording.
5. Set an expiration period for the link to be generated.
6. Click **Copy link**.

After you click **Copy link**, either of the following messages appears, indicating a successful or failed operation respectively:

- **The URL to the shared recording has been copied to the clipboard**
- **Sharing the recording URL failed**

7. Share the generated URL link with anyone in your AD domain.

Pasting the link in the address bar lets you jump to the location where the URL link was copied.

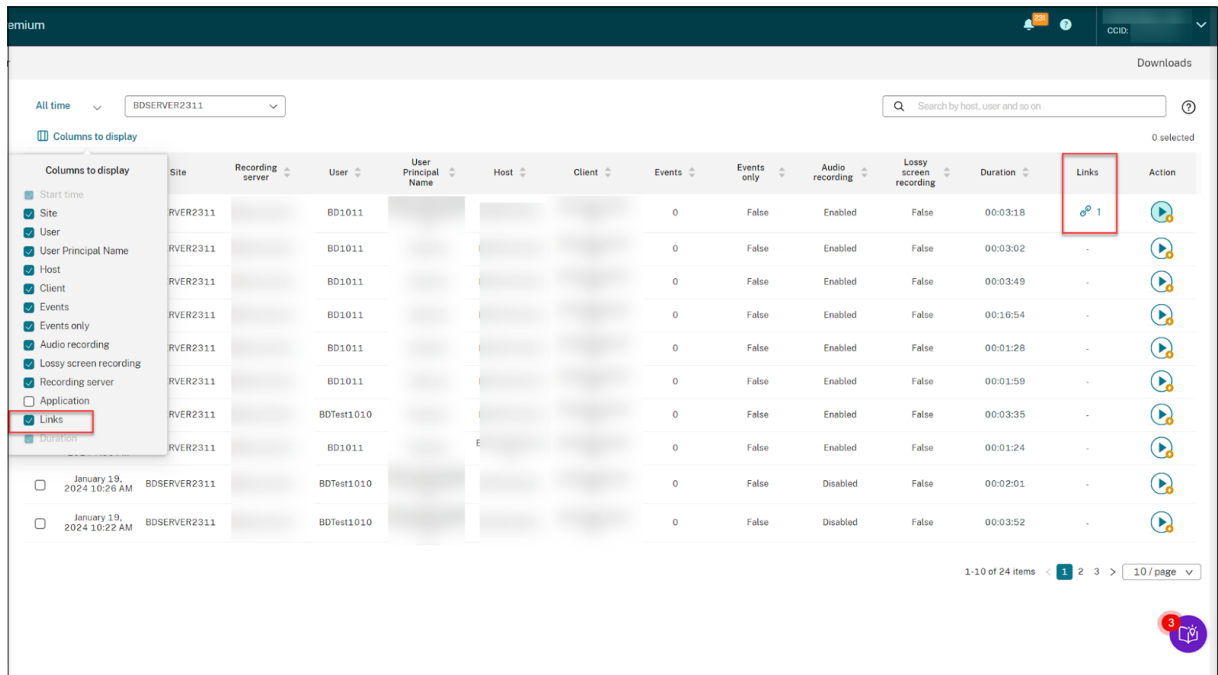
Note:

- To view a recording using an unrestricted link, users must enter a justification.
- The actions of generating unrestricted links are logged on the **Events** tab of the [activity feed](#).
- For unrestricted recording sharing, you can specify whether to issue email notifications to specific recipients when an unrestricted recording link is generated. For more information, see [Notifications](#).

Manage unrestricted links

View which recordings have been shared as unrestricted links

To get an overview of which recordings have been shared as unrestricted links, check the **Links** column on the **All Recordings** page. If the **Links** column doesn't show up, click **Columns to display** and then select **Links**.



After you click the link icon corresponding to a recording, the details about unrestricted links generated for the current recording appear, for example:

The screenshot shows a dialog box titled "Manage unrestricted links" with a close button (X) in the top right corner. Below the title, there is a brief instruction: "View and manage unrestricted links generated for this recording. Expand each row to view details." Below this instruction are two action buttons: "Refresh" (with a circular arrow icon) and "Clear invalid links" (with a trash can icon). The main content is a table with the following columns: "Generated at (UTC+08:00)", "Generated by", "Justification", and "Status". The table contains three rows of data:

Generated at (UTC+08:00)	Generated by	Justification	Status
Jan 24, 2024 5:39:31 PM	[redacted]@citrix.com	test	Expired
Jan 25, 2024 2:45:45 PM	[redacted]@citrix.com	a	Revoked
Jan 24, 2024 5:30:54 PM	[redacted]@citrix.com		Expired

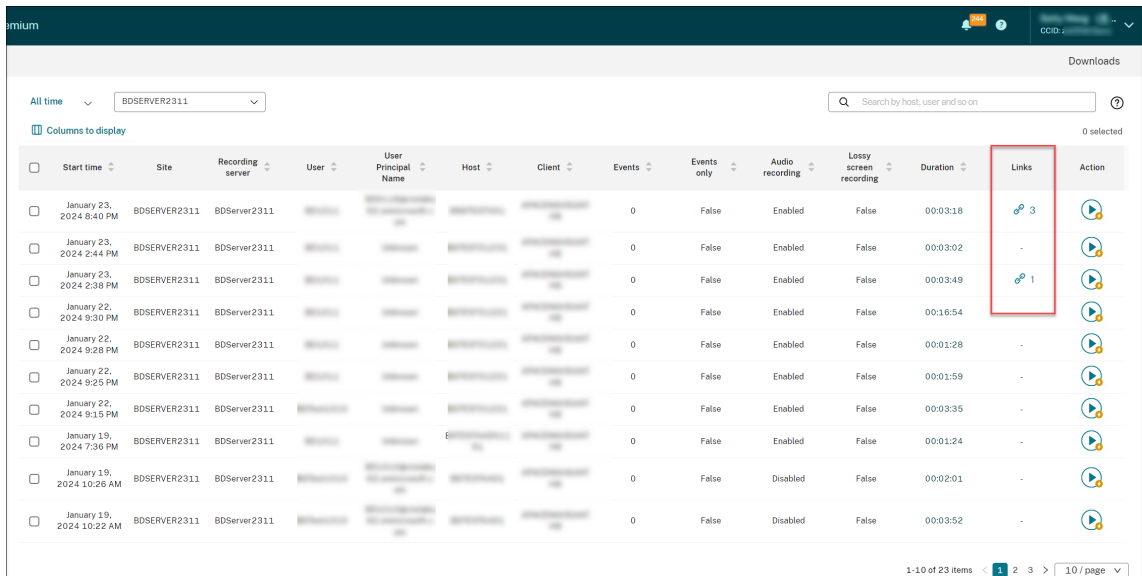
At the bottom left of the dialog is a "Done" button. At the bottom right is a purple circular icon with a white document symbol and a red notification badge with the number "3".

View and manage unrestricted links of a specific recording

1. Open the **Manage unrestricted links** page.

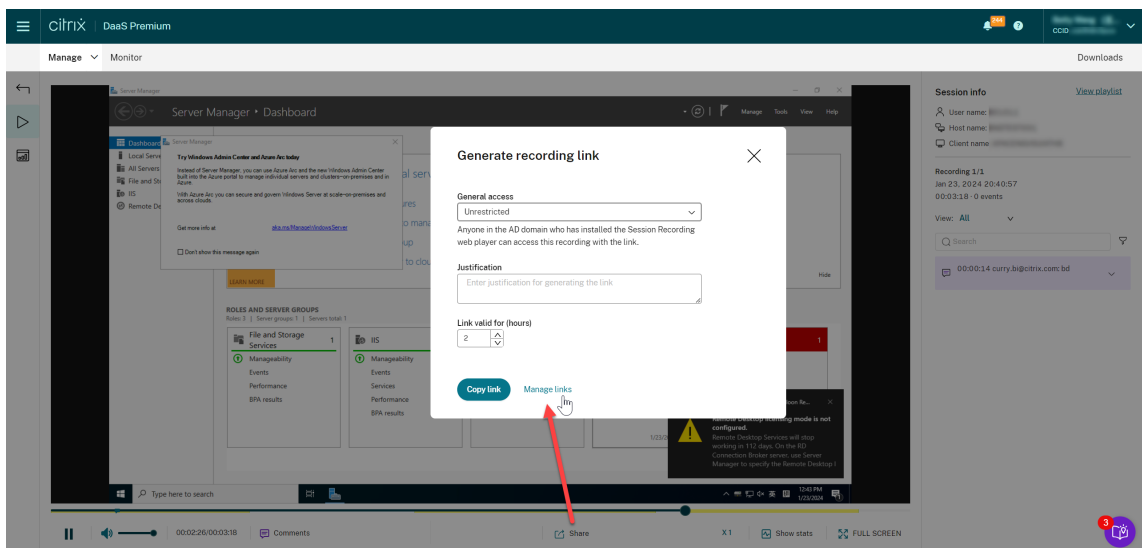
Method 1: On the **All Recordings** page, click the link icon in the **Links** column next to a specific recording.

Session Recording service

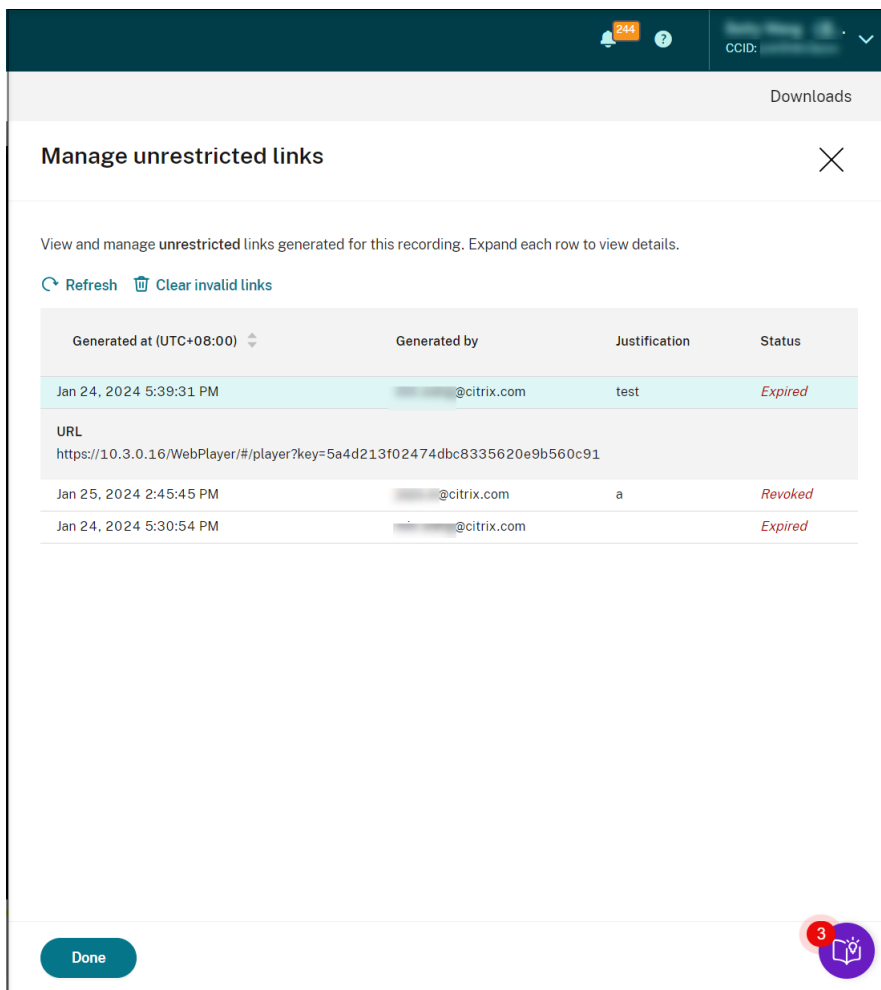


	Start time	Site	Recording server	User	User Principal Name	Host	Client	Events	Events only	Audio recording	Lossy screen recording	Duration	Links	Action
<input type="checkbox"/>	January 23, 2024 8:40 PM	BDSERVER2311	BDServer2311					0	False	Enabled	False	00:03:18	3	
<input type="checkbox"/>	January 23, 2024 2:44 PM	BDSERVER2311	BDServer2311					0	False	Enabled	False	00:03:02	-	
<input type="checkbox"/>	January 23, 2024 2:38 PM	BDSERVER2311	BDServer2311					0	False	Enabled	False	00:03:49	1	
<input type="checkbox"/>	January 22, 2024 9:30 PM	BDSERVER2311	BDServer2311					0	False	Enabled	False	00:16:54	-	
<input type="checkbox"/>	January 22, 2024 9:28 PM	BDSERVER2311	BDServer2311					0	False	Enabled	False	00:01:28	-	
<input type="checkbox"/>	January 22, 2024 9:25 PM	BDSERVER2311	BDServer2311					0	False	Enabled	False	00:01:59	-	
<input type="checkbox"/>	January 22, 2024 9:15 PM	BDSERVER2311	BDServer2311					0	False	Enabled	False	00:03:35	-	
<input type="checkbox"/>	January 19, 2024 7:36 PM	BDSERVER2311	BDServer2311					0	False	Enabled	False	00:01:24	-	
<input type="checkbox"/>	January 19, 2024 10:26 AM	BDSERVER2311	BDServer2311					0	False	Disabled	False	00:02:01	-	
<input type="checkbox"/>	January 19, 2024 10:22 AM	BDSERVER2311	BDServer2311					0	False	Disabled	False	00:03:52	-	

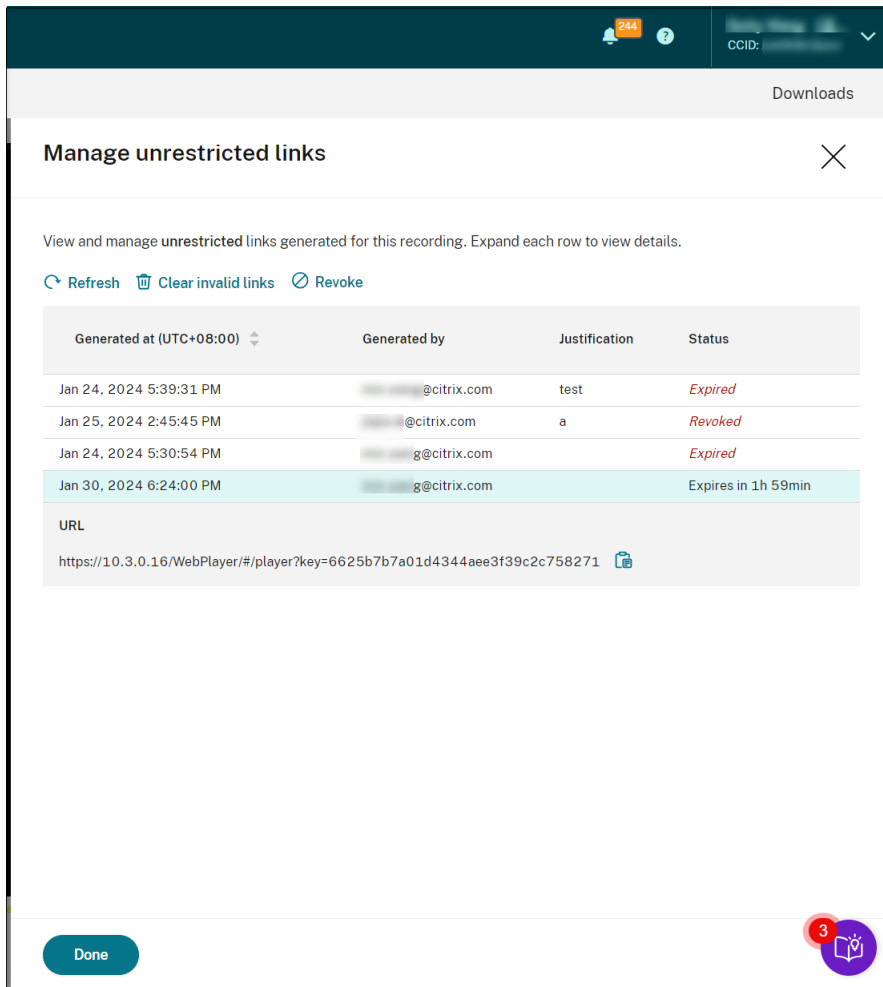
Method 2: Click **Manage Links** in the **Generate recording link** dialog.



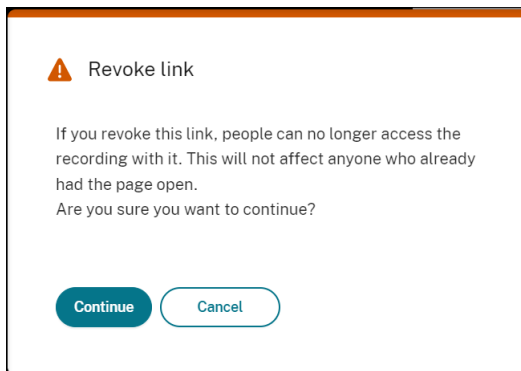
2. On the **Manage unrestricted links** page, expand each row to view details about the unrestricted links that are generated for the specific recording.



3. (Optional) To revoke a link, select it and then click **Revoke** that appears.



After you click **Revoke**, you are prompted to confirm the action.



4. (Optional) To remove the links that have expired or revoked, click **Clear invalid links**.

Specify players for a site

July 17, 2023

Overview

You can now specify either the cloud player, on-premises players, or both to play the recordings of a site. By default, both the cloud player and on-premises players are selected.

Note:

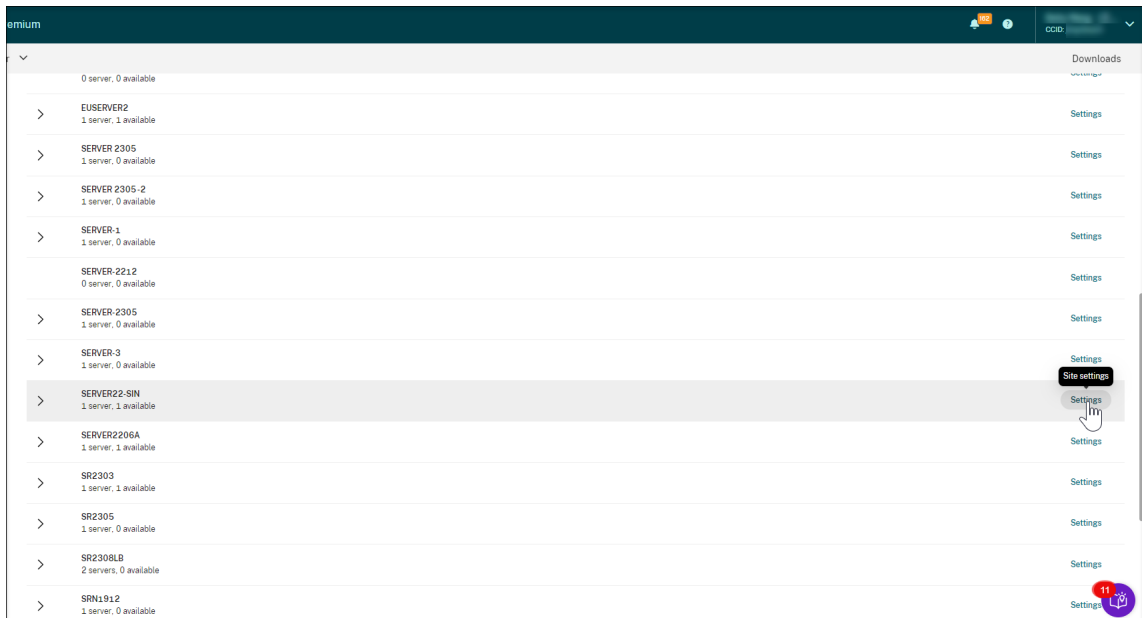
This feature is available for Session Recording server 2308 and later only.

The on-premises players include the Session Recording player (Windows) and the Session Recording web player.

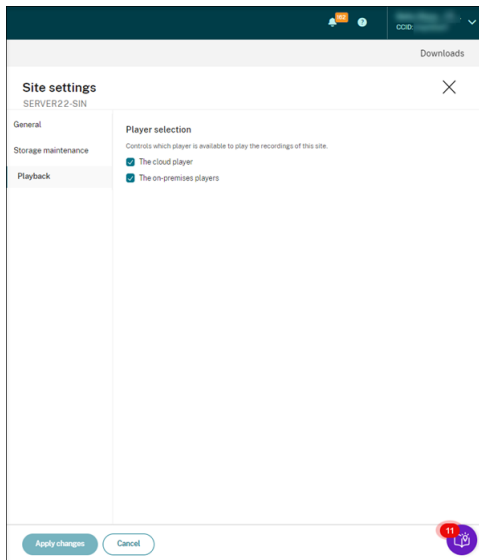
Configuration

To specify players available to play the recordings of a site, complete the following steps:

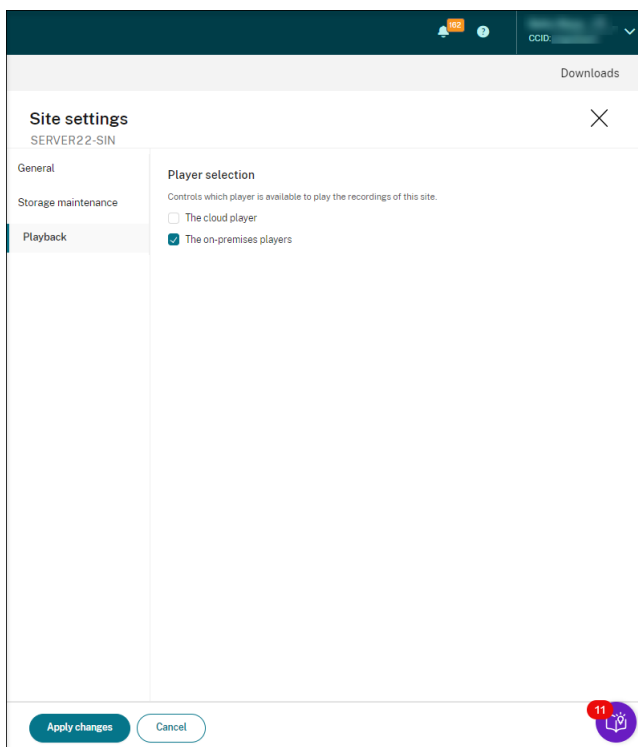
1. Select **Configuration > Server Management** from the left navigation of the Session Recording service.
2. Click **Settings** for the target site. The **Site settings** page appears.



3. On the **Site settings** page, select the **Playback** menu. The player selection page appears. By default, both options are selected.



4. Select at least one option as needed and then click **Apply changes**. For example, select only the on-premises players:



What if a player is disabled (not selected)

- If the cloud player is disabled for recording playback of a site, the play button for recordings from the site is unavailable with a tooltip on hover.

Session Recording service

The screenshot shows the emium Session Recording interface. At the top, there's a search bar and a dropdown menu set to 'SERVER22-SIN'. Below the search bar, there's a table with columns: Start Time, Recording Site, User, Host, Client, Events, Duration, and Action. The table contains 10 rows of recording data. A tooltip message is visible over one of the rows, stating 'Recordings from this site can't be played from the cloud.'

Start Time	Recording Site	User	Host	Client	Events	Duration	Action
July 14, 2023 11:24 AM	SERVER22-SIN	administrator	WIN10EN-4PVEICQ	NKGWYUCHUNJ01	0	00:00:59	▶
July 14, 2023 11:14 AM	SERVER22-SIN	administrator	WIN10EN-4PVEICQ	NKGWYUCHUNJ01	0	00:00:45	▶
July 14, 2023 11:09 AM	SERVER22-SIN	administrator	WIN10EN-4PVEICQ	NKGWYUCHUNJ01	0	00:00:41	▶
July 14, 2023 11:03 AM	SERVER22-SIN	administrator	WIN10EN-4PVEICQ	NKGWYUCHUNJ01	0	00:01:04	▶
July 14, 2023 10:48 AM	SERVER22-SIN	administrator	WIN10EN-4PVEICQ	NKGWYUCHUNJ01	0	00:02:20	▶
July 14, 2023 10:40 AM	SERVER22-SIN	administrator	WIN10EN-4PVEICQ	NKGWYUCHUNJ01	0	00:05:44	▶
July 14, 2023 10:30 AM	SERVER22-SIN	administrator	WIN10EN-4PVEICQ	NKGWYUCHUNJ01	0	00:23:54	▶
July 14, 2023 9:45 AM	SERVER22-SIN	administrator	WIN10EN-4PVEICQ	NKGWYUCHUNJ01	0	00:11:08	▶
July 14, 2023 9:22 AM	SERVER22-SIN	administrator	AWTSVDA-0001	NKGWYUCHUNJ01	4	00:18:28	▶

- If the on-premises players are disabled for recording playback of a site, you are prompted when selecting recordings the site. The prompt message reads “Recording playback has been disabled for this server in the current player.” For an example of the prompt message in the on-premises Session Recording web player:

The screenshot shows the Citrix Session Recording interface. At the top, there's a search bar and a dropdown menu. Below the search bar, there's a message: 'Recording playback has been disabled for this server in the current player.' Below the message, there's a table with columns: Start Time, User, Host, Client, Events, Events Only, Audio Recording, Recording Server, and Duration. The table contains 13 rows of recording data.

Start Time	User	Host	Client	Events	Events Only	Audio Recording	Recording Server	Duration
Jul 10, 2023 11:07:18 AM	administrator	SR2308VDA	APACENGVSUIATH8	0	False	Enabled	NewTest	00:03:27
Jul 10, 2023 10:47:11 AM	administrator	SR2308VDA	APACENGVSUIATH8	0	False	Enabled	NewTest	00:03:23
Jul 10, 2023 10:45:15 AM	administrator	SR2308VDA	APACENGVSUIATH8	0	False	Enabled	NewTest	00:01:37
Jul 10, 2023 10:32:41 AM	administrator	SR2308VDA	APACENGVSUIATH8	0	False	Enabled	NewTest	00:07:59
Jul 10, 2023 10:23:15 AM	administrator	SR2308VDA	APACENGVSUIATH8	0	False	Enabled	NewTest	00:01:18
Jul 10, 2023 10:13:52 AM	administrator	SR2308VDA	APACENGVSUIATH8	0	False	Enabled	NewTest	00:02:59
Jul 7, 2023 6:31:45 PM	administrator	SR2308VDA	APACENGVSUIATH8	0	False	Disabled	NewTest	00:09:27
Jul 7, 2023 6:17:55 PM	administrator	SR2308VDA	APACENGVSUIATH8	0	False	Disabled	NewTest	00:09:38
Jul 7, 2023 4:26:46 PM	administrator	SR2308VDA	APACENGVSUIATH8	0	True	Disabled	NewTest	00:02:10
Jul 7, 2023 4:01:46 PM	administrator	SR2308VDA	APACENGVSUIATH8	0	True	Disabled	NewTest	00:03:10
Jul 6, 2023 8:14:34 PM	administrator	SR2308VDA	APACENGVSUIATH8	0	True	Disabled	NewTest	00:04:00
Jul 6, 2023 8:12:04 PM	administrator	SR2308VDA	APACENGVSUIATH8	8	True	Disabled	NewTest	00:01:54
Jul 6, 2023 8:08:00 PM	administrator	SR2308VDA	APACENGVSUIATH8	31	True	Disabled	NewTest	00:02:32

Meanwhile, if any recording of the site was shared as a link earlier, the **Playback unavailable** message appears when the viewer opens the link to access the 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`.

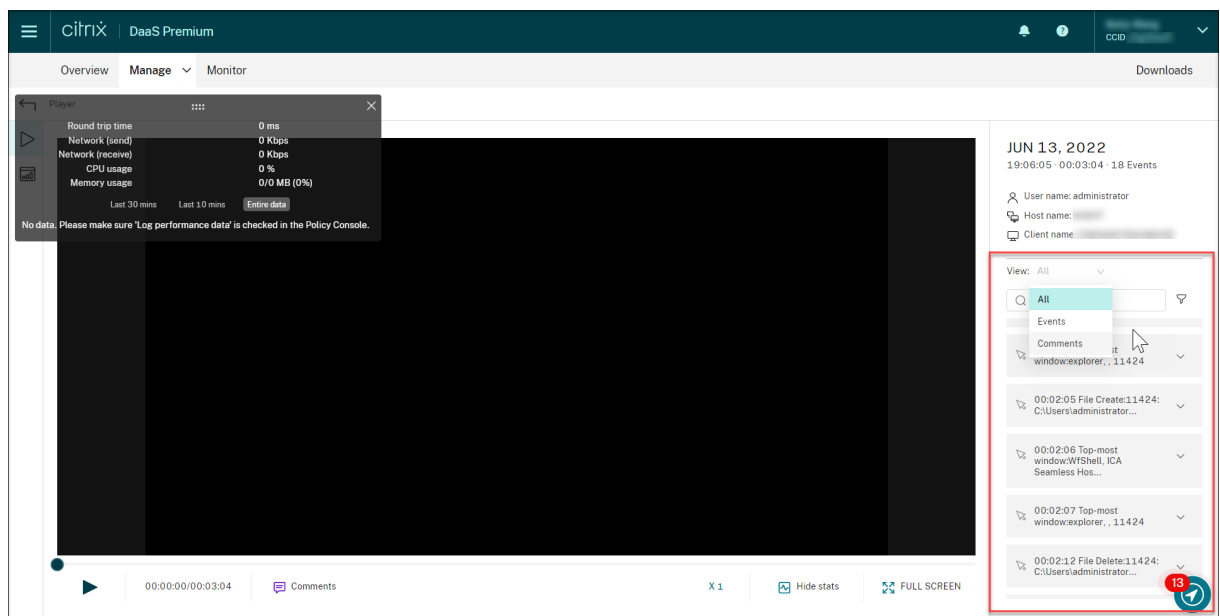
Registry key	Default value	Description
<code>DisableIdleEvent</code>	0	To disable the idle event feature, set the value to 1 . To enable the idle event feature, set the value to 0 .
<code>IdleEventThrottle</code>	30 seconds	If there is no user activity (including graphics changes and keyboard/mouse inputs) 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.
<code>IdleEventActiveThrottle</code>	2 seconds	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.
<code>IdleEventActivePktNumThrottle</code>	3 packets	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.

Registry key	Default value	Description
IdleEventActivePktSizeThrottle	300 bytes	Graphics packets smaller than the key value are ignored and the relevant time duration is regarded as idle.

Use events and comments

June 13, 2022

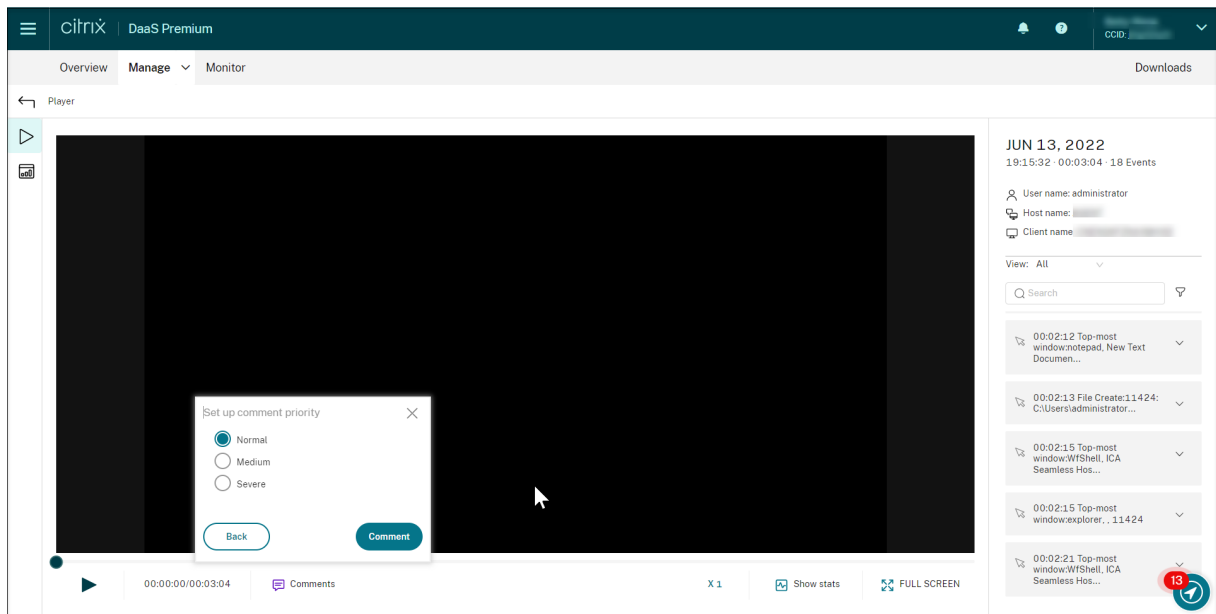
In the right pane of the playback page, the **Events** and **Comments** filters are available. You can use events and comments to help you navigate through recorded sessions in the web player.



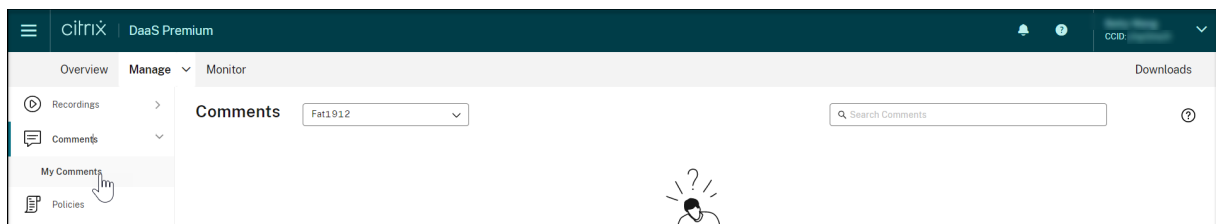
Comment on recordings

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 web-page, expand the comment, and then click **Delete**.

Session Recording service




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.

 Add Roles and Features Wizard

Select server roles

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- Hyper-V
- MultiPoint Services
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS) (27 of 43 installed)
 - Web Server (21 of 34 installed)
 - Common HTTP Features (5 of 6 installed)
 - Default Document (Installed)
 - Directory Browsing (Installed)
 - HTTP Errors (Installed)
 - Static Content (Installed)
 - HTTP Redirection (Installed)
 - WebDAV Publishing
 - Health and Diagnostics (4 of 6 installed)
 - Performance (Installed)
 - Security (3 of 9 installed)

< Previous Next >

View graphical event statistics

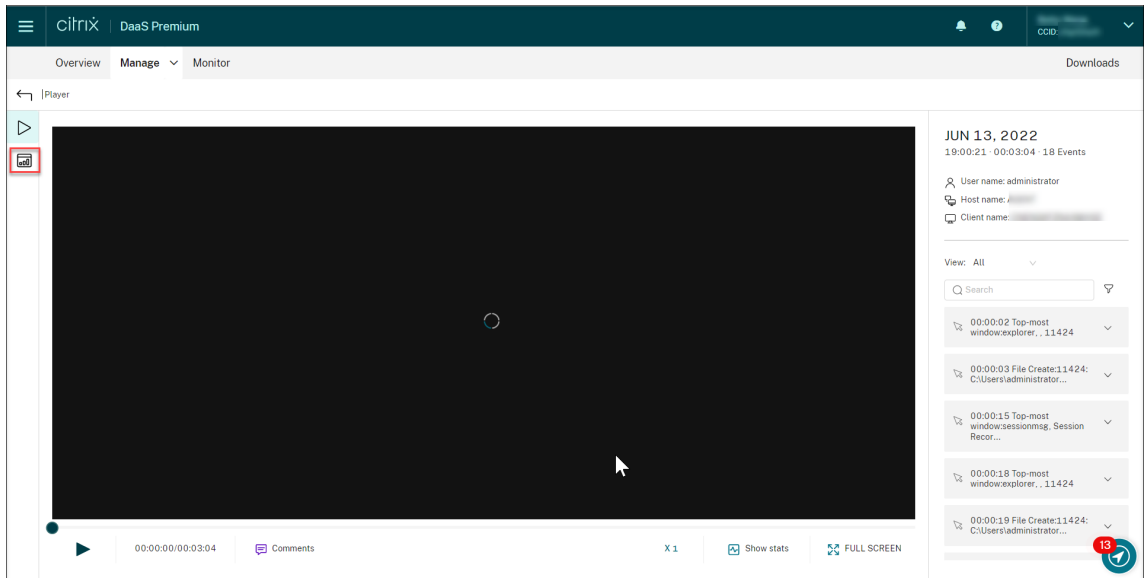
November 11, 2022

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.

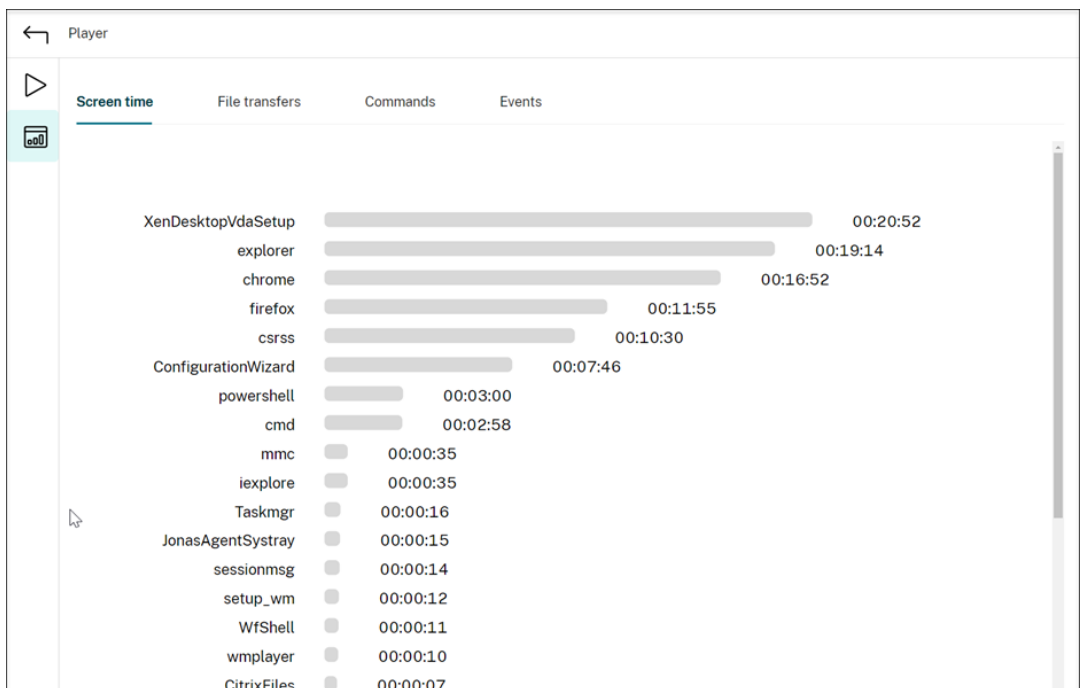
2. In the upper left corner of the playback page, click the statistics icon.



3. Switch between the **Screen time**, **File transfers**, **Commands**, and **Events** tabs to view statistics from different perspectives.

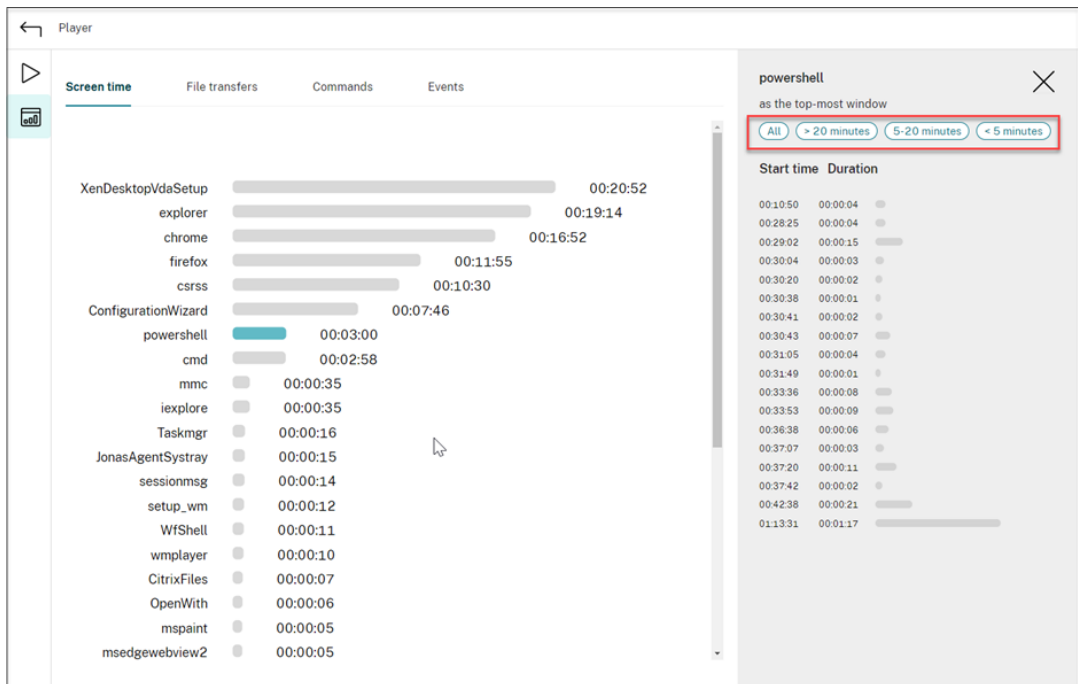
- **Screen time**

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



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** option. For example:

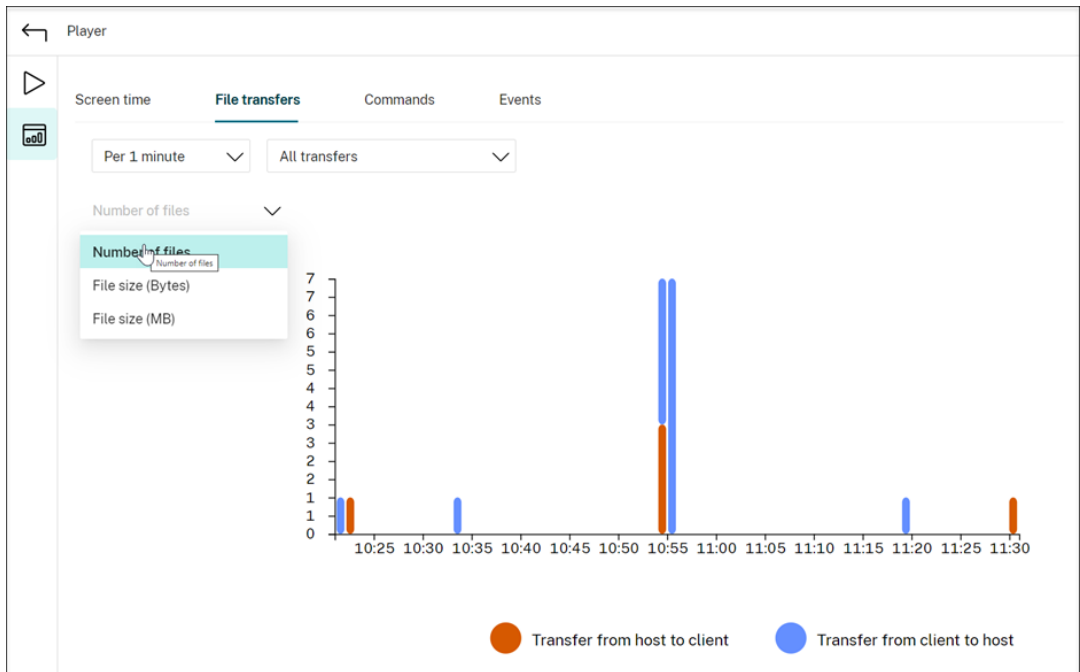


- **File transfers**

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:

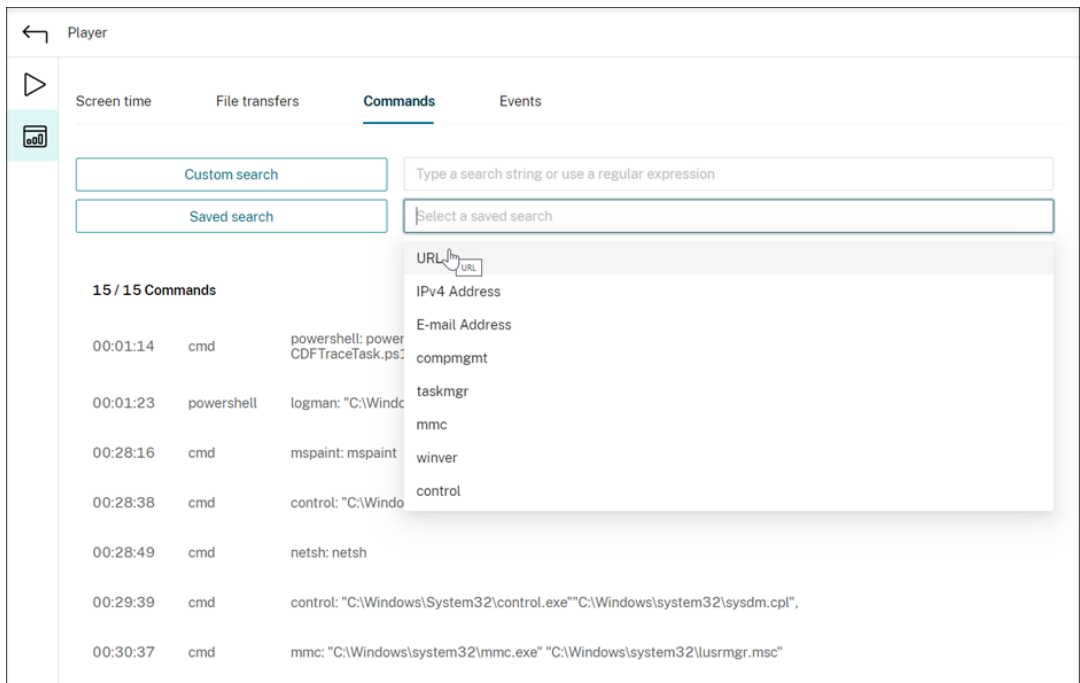
- Time granularity: **Per 1 minute, Per 10 minutes, Per hour**
- File transfer destination: **All transfers, Transfer from host to client, Transfer from client to host**
- Number or size (Bytes or MB) of transferred files

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



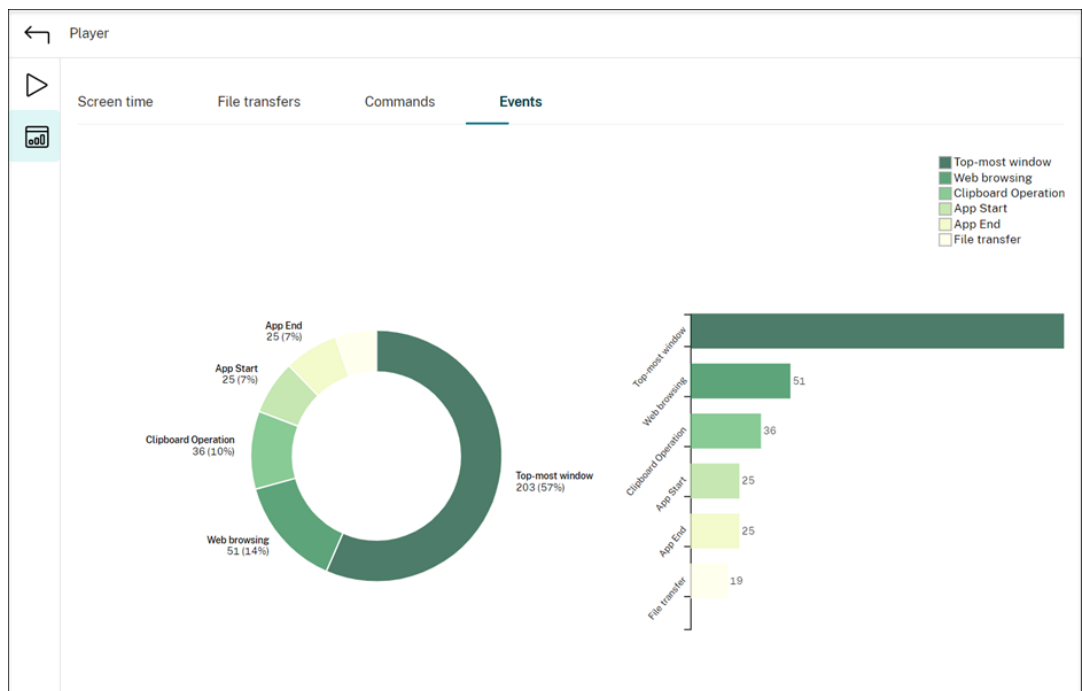
- **Commands**

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.

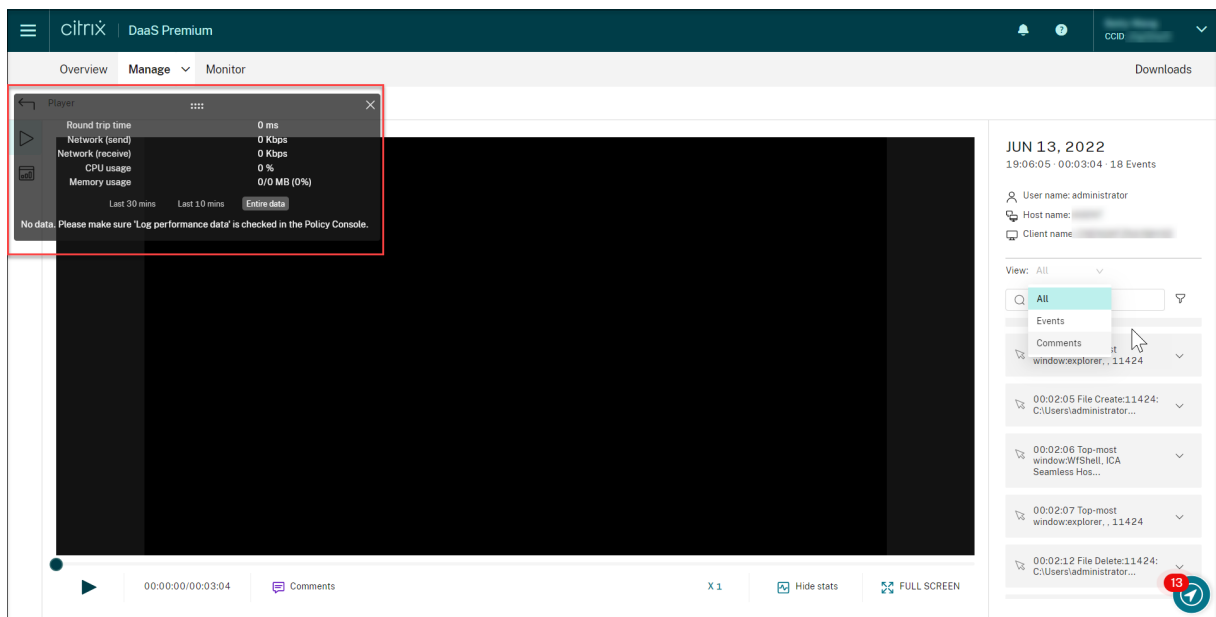


View performance data points

April 26, 2024

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



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](#).

Manage recordings

November 17, 2022

This section provides instructions for you to:

- [Manage selected recordings](#)

- [Archive recordings manually](#)
- [Delete recordings manually](#)
- [Manage recordings on schedule](#)
 - [Archive and delete recordings on schedule](#)

Manage selected recordings

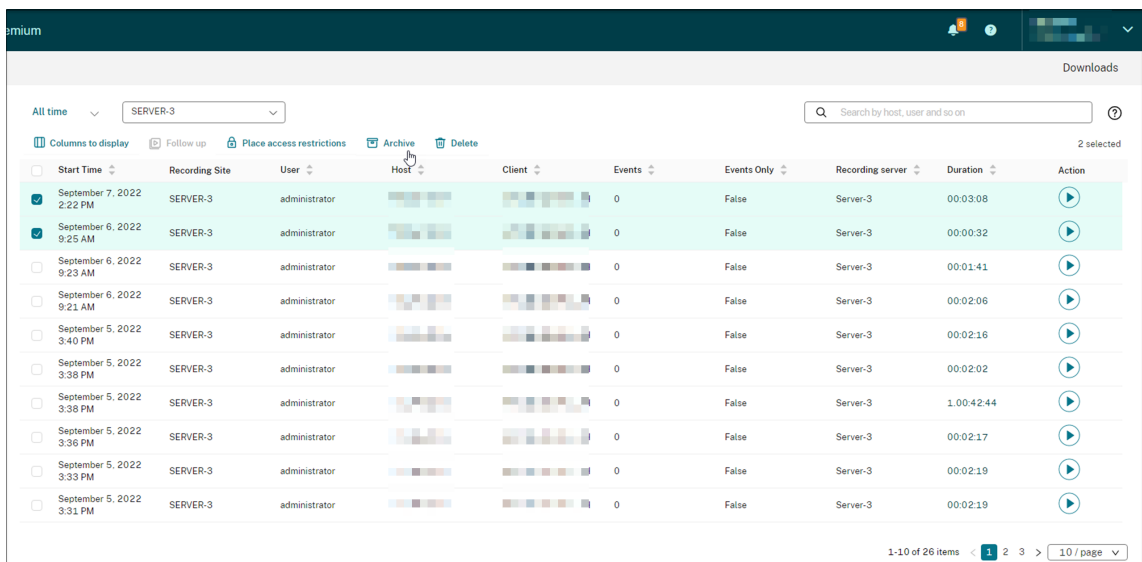
November 11, 2022

You can select target recordings to archive and delete manually.

Archive recordings manually

To archive recordings manually:

1. Select **Recordings > All Recordings** from the left navigation of the Session Recording service.
2. Select one or more target recordings.
3. Click **Archive**.



The screenshot shows the Citrix Cloud interface for managing recordings. At the top, there are filters for 'All time' and 'SERVER-3'. Below the filters, there are icons for 'Columns to display', 'Follow up', 'Place access restrictions', 'Archive', and 'Delete'. The 'Archive' icon is highlighted with a mouse cursor. Below the icons is a table of recordings. The table has columns for 'Start Time', 'Recording Site', 'User', 'Host', 'Client', 'Events', 'Events Only', 'Recording server', 'Duration', and 'Action'. Two recordings are selected, indicated by checkmarks in the first column. The 'Action' column contains play icons for each recording. At the bottom right of the table, it says '1-10 of 26 items' and '10 / page'.

<input type="checkbox"/>	Start Time	Recording Site	User	Host	Client	Events	Events Only	Recording server	Duration	Action
<input checked="" type="checkbox"/>	September 7, 2022 2:22 PM	SERVER-3	administrator	[blurred]	[blurred]	0	False	Server-3	00:03:08	[play icon]
<input checked="" type="checkbox"/>	September 6, 2022 9:25 AM	SERVER-3	administrator	[blurred]	[blurred]	0	False	Server-3	00:00:32	[play icon]
<input type="checkbox"/>	September 6, 2022 9:23 AM	SERVER-3	administrator	[blurred]	[blurred]	0	False	Server-3	00:01:41	[play icon]
<input type="checkbox"/>	September 6, 2022 9:21 AM	SERVER-3	administrator	[blurred]	[blurred]	0	False	Server-3	00:02:06	[play icon]
<input type="checkbox"/>	September 5, 2022 3:40 PM	SERVER-3	administrator	[blurred]	[blurred]	0	False	Server-3	00:02:16	[play icon]
<input type="checkbox"/>	September 5, 2022 3:38 PM	SERVER-3	administrator	[blurred]	[blurred]	0	False	Server-3	00:02:02	[play icon]
<input type="checkbox"/>	September 5, 2022 3:38 PM	SERVER-3	administrator	[blurred]	[blurred]	0	False	Server-3	1.00:42:44	[play icon]
<input type="checkbox"/>	September 5, 2022 3:36 PM	SERVER-3	administrator	[blurred]	[blurred]	0	False	Server-3	00:02:17	[play icon]
<input type="checkbox"/>	September 5, 2022 3:33 PM	SERVER-3	administrator	[blurred]	[blurred]	0	False	Server-3	00:02:19	[play icon]
<input type="checkbox"/>	September 5, 2022 3:31 PM	SERVER-3	administrator	[blurred]	[blurred]	0	False	Server-3	00:02:19	[play icon]

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
- The **Session Recording-PrivilegedPlayerAdmin, 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.

If you select any recording of a session, all other recordings of the same session are archived as well.

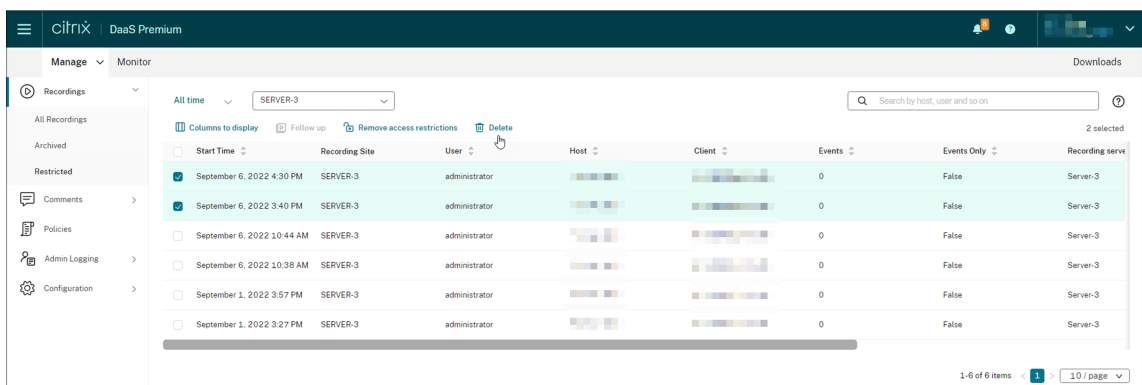
You can select one or more recordings to archive at a time. When archiving recordings, you can choose to move the recording files to a different location from the one where they were originally stored.

- If you move the recording 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.

Delete recordings manually

To delete recordings manually:

1. Select **Recordings** from the left navigation of the Session Recording service.
2. Find one or more target recordings on any of the **All Recordings**, **Archived**, or **Restricted** pages.
3. Click **Delete**.



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
- The **Session Recording-PrivilegedPlayerAdmin, All** role

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

If you select any recording of a session, all other recordings of the same session are deleted as well.

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.

Manage recordings on schedule

April 28, 2023

You can schedule site-level tasks to automatically archive and delete recordings **on a regular basis**.

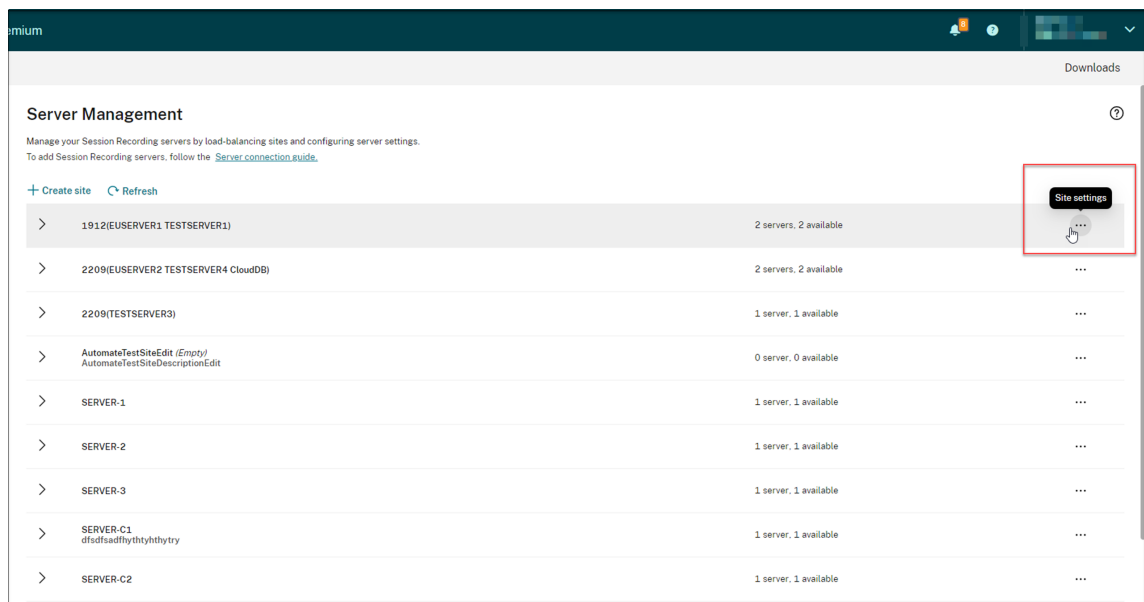
Note:

Only Citrix Cloud administrators of the following roles can schedule the tasks:

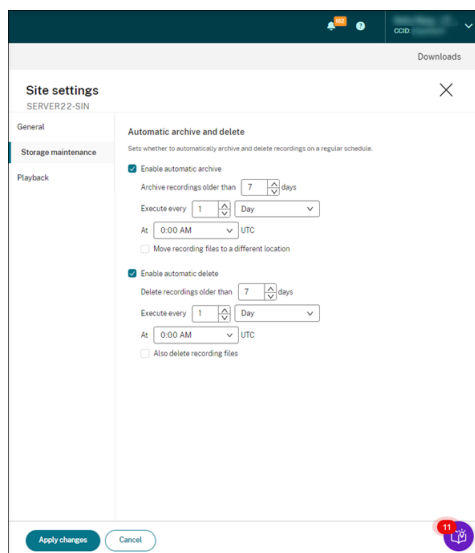
- Full access
- The **Cloud Administrator, All** role
- The **Session Recording-FullAdmin, All** role

Archive and delete recordings on schedule

1. Select **Configuration > Server Management** from the left navigation of the Session Recording service.
2. Click the ellipsis (...) next to a target site.



3. On the **Site settings** page, select **Storage maintenance**.



4. Schedule tasks as needed and then click **Apply changes**.

Note:

The time you set for automatic archiving and deletion must be later than the time you set for [automatic cloud client upgrades](#). Otherwise, automatic archiving and deletion might fail.

Administrator logging

April 27, 2023

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

Note:

If you install SQL Server on the same machine with the Session Recording server, the administrator logging data might not be available and a “**No data available**” message is displayed. To ensure that you can view the administrator logging data, add the **NT AUTHORITY\SYSTEM** user to your Session Recording databases and assign it the **db_owner** permission.

Configuration Logging SERVER2209

Log of administrator activities.

All time Category Action Action taken by

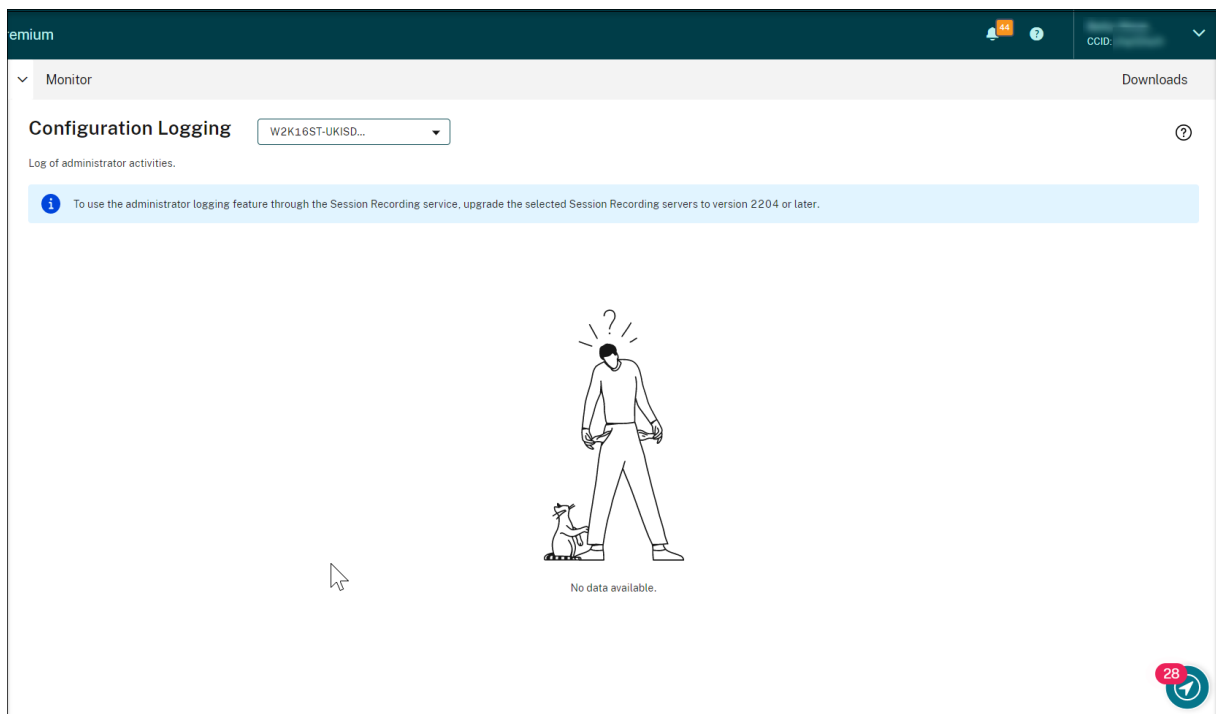
ID	Name	Logging time	Category	Action	Action taken by	Authorized
409	SERVER2209	12/6/2022 2:29:00 PM	Policy change	Save policy document	SRCloudUser/curry.bi@ctrix.com	True
408	SERVER2209	12/6/2022 2:29:00 PM	Policy change	Save policy document	SRCloudUser/curry.bi@ctrix.com	True
407	SERVER2209	12/6/2022 2:28:00 PM	Policy change	Set active policy document	SRCloudUser/curry.bi@ctrix.com	True
406	SERVER2209	12/6/2022 2:27:00 PM	Policy change	Save policy document	SRCloudUser/curry.bi@ctrix.com	True
405	SERVER2209	12/6/2022 2:27:00 PM	Policy change	Save policy document	SRCloudUser/curry.bi@ctrix.com	True
404	SERVER2209	12/6/2022 2:26:00 PM	Policy change	Save policy document	SRCloudUser/curry.bi@ctrix.com	True
403	SERVER2209	12/6/2022 2:26:00 PM	Policy change	Save policy document	SRCloudUser/curry.bi@ctrix.com	True
402	SERVER2209	12/6/2022 2:26:00 PM	Policy change	Save policy document	SRCloudUser/curry.bi@ctrix.com	True
401	SERVER2209	12/6/2022 2:26:00 PM	Policy change	New policy document	SRCloudUser/curry.bi@ctrix.com	True
400	SERVER2209	12/1/2022 5:41:00 PM	Policy change	Save policy document	SRCloudUser/huix.wang@ctrix.com	True

1-10 of 80

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 site that contains a Session Recording server earlier than version 2204, the following banner appears, and no data is available.

Session Recording service

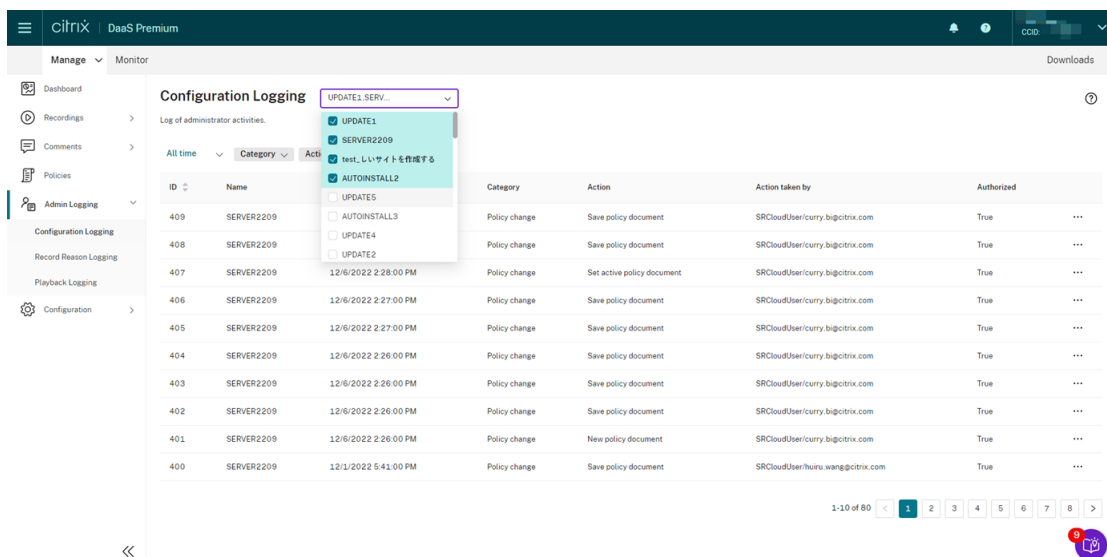


Logging data overview

Administrator logging data consists of:

- Configuration logging
- Recording reason logging
- Playback logging

You can select more than one Session Recording site to view logs.



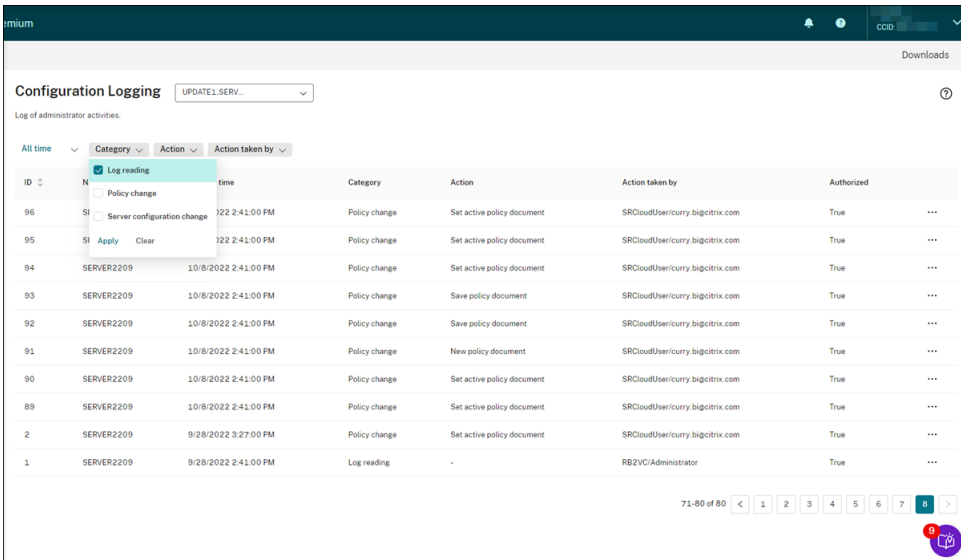
Click the three dots (ellipsis) to view details about each log.

Configuration logging

This part logs the following administrator activities:

- **Policy change** - Changes to policies on the Session Recording policy console or Citrix Director
- **Server configuration change** - Changes in Session Recording Server Properties
- **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.



The screenshot shows the 'Configuration Logging' interface. At the top, there is a search filter set to 'UPDATE1.SERV...'. Below the search bar, there are filter options for 'All time', 'Category', 'Action', and 'Action taken by'. A dropdown menu is open over the 'Action' filter, showing options for 'Log reading', 'Policy change', and 'Server configuration change'. The main table displays a list of logs with columns for ID, time, Category, Action, Action taken by, and Authorized. The table contains 10 rows of data, with the first row (ID 96) highlighted. At the bottom of the table, there is a pagination control showing '71-80 of 80' and a search icon.

ID	time	Category	Action	Action taken by	Authorized
96	10/8/2022 2:41:00 PM	Policy change	Set active policy document	SRCloudUser\curry.bigcitrix.com	True
95	10/8/2022 2:41:00 PM	Policy change	Set active policy document	SRCloudUser\curry.bigcitrix.com	True
94	10/8/2022 2:41:00 PM	Policy change	Set active policy document	SRCloudUser\curry.bigcitrix.com	True
93	10/8/2022 2:41:00 PM	Policy change	Save policy document	SRCloudUser\curry.bigcitrix.com	True
92	10/8/2022 2:41:00 PM	Policy change	Save policy document	SRCloudUser\curry.bigcitrix.com	True
91	10/8/2022 2:41:00 PM	Policy change	New policy document	SRCloudUser\curry.bigcitrix.com	True
90	10/8/2022 2:41:00 PM	Policy change	Set active policy document	SRCloudUser\curry.bigcitrix.com	True
89	10/8/2022 2:41:00 PM	Policy change	Set active policy document	SRCloudUser\curry.bigcitrix.com	True
2	9/28/2022 3:27:00 PM	Policy change	Set active policy document	SRCloudUser\curry.bigcitrix.com	True
1	9/28/2022 2:41:00 PM	Log reading	-	RB2VC\Administrator	True

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

1. Select **Configuration > Server Management** from the left navigation of the Session Recording service.
2. Find your Session Recording servers.
3. Click the gear icon corresponding to each Session Recording server.
4. 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 enabling 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.

The screenshot shows the 'Record Reason Logging' interface. It features a table with the following columns: ID, Logging time, Applicable policy, Recorded user, and Authorized. The table contains 10 rows of log entries. A dropdown menu is open over the 'Applicable policy' column, showing options for 'Event detection reason' and 'Recording reason'. The table also includes a search bar, filters for 'All time', 'Applicable policy', and 'Recorded user', and a pagination control at the bottom right showing '1-10 of 50'.

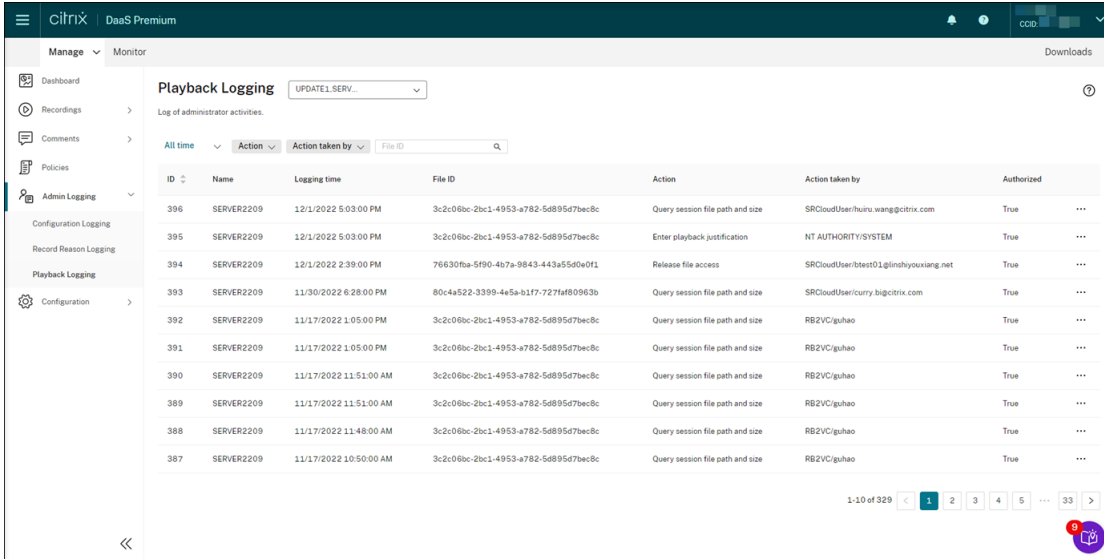
ID	Logging time	Applicable policy	Recorded user	Authorized
50	11/28/2022 2:53:00 PM	Event detection reason	RB2VC\Administrator	True
49	11/28/2022 2:53:00 PM	Recording reason	RB2VC\Administrator	True
48	11/24/2022 9:47:00 AM	Event detection reason	RB2VC\Administrator	True
47	11/24/2022 9:47:00 AM	Recording reason	RB2VC\Administrator	True
46	11/9/2022 12:18:00 PM	Event detection reason	RB2VC\Administrator	True
45	11/9/2022 12:18:00 PM	Recording reason	RB2VC\Administrator	True
44	11/2/2022 2:15:00 PM	Recording reason	RB2VC\Administrator	True
43	11/1/2022 10:58:00 AM	Recording reason	RB2VC\User0	True
42	11/1/2022 10:57:00 AM	Recording reason	RB2VC\User0	True
41	11/1/2022 10:55:00 AM	Recording reason	RB2VC\User0	True

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 enabling the recording reason logging, see [Disable or enable the recording reason logging](#).

Playback logging

This part logs playback-related actions. Click the three dots (ellipsis) to view details about each log.



The screenshot displays the Citrix DaaS Premium interface for Playback Logging. The left sidebar shows navigation options: Dashboard, Recordings, Comments, Policies, Admin Logging (selected), Configuration Logging, Record Reason Logging, Playback Logging, and Configuration. The main area is titled 'Playback Logging' and shows a log of administrator activities. A table lists 10 entries with columns for ID, Name, Logging time, File ID, Action, Action taken by, and Authorized. The actions include 'Query session file path and size' and 'Enter playback justification'. The bottom of the table shows pagination: 1-10 of 329, with page 1 selected.

ID	Name	Logging time	File ID	Action	Action taken by	Authorized
396	SERVER2209	12/1/2022 5:03:00 PM	3c2c06bc-2bc1-4953-a782-5d895d7bec8c	Query session file path and size	SRCloudUser/huiru.wang@citrix.com	True
395	SERVER2209	12/1/2022 5:03:00 PM	3c2c06bc-2bc1-4953-a782-5d895d7bec8c	Enter playback justification	NT AUTHORITY\SYSTEM	True
394	SERVER2209	12/1/2022 2:39:00 PM	76630ba-5f90-4b7a-9843-443a55d0e0f1	Release file access	SRCloudUser/btest01@linshiyouxiang.net	True
393	SERVER2209	11/30/2022 6:28:00 PM	80c44522-3399-445a-b1f7-727faf80963b	Query session file path and size	SRCloudUser/curry.big@citrix.com	True
392	SERVER2209	11/17/2022 1:05:00 PM	3c2c06bc-2bc1-4953-a782-5d895d7bec8c	Query session file path and size	RB2VC\guhao	True
391	SERVER2209	11/17/2022 1:05:00 PM	3c2c06bc-2bc1-4953-a782-5d895d7bec8c	Query session file path and size	RB2VC\guhao	True
390	SERVER2209	11/17/2022 11:51:00 AM	3c2c06bc-2bc1-4953-a782-5d895d7bec8c	Query session file path and size	RB2VC\guhao	True
389	SERVER2209	11/17/2022 11:51:00 AM	3c2c06bc-2bc1-4953-a782-5d895d7bec8c	Query session file path and size	RB2VC\guhao	True
388	SERVER2209	11/17/2022 11:48:00 AM	3c2c06bc-2bc1-4953-a782-5d895d7bec8c	Query session file path and size	RB2VC\guhao	True
387	SERVER2209	11/17/2022 10:50:00 AM	3c2c06bc-2bc1-4953-a782-5d895d7bec8c	Query session file path and size	RB2VC\guhao	True

To log playback justifications, enable both administrator logging and playback justification logging on your Session Recording servers. If administrator logging is disabled, enabling playback justification logging does not take effect.

Note:

Playback justification logging is available for Session Recording server 2212 and later only. If you select a site that contains a Session Recording server earlier than version 2212, the playback justification logging enabler isn't available for any server in the site.

Management dashboard

April 25, 2024

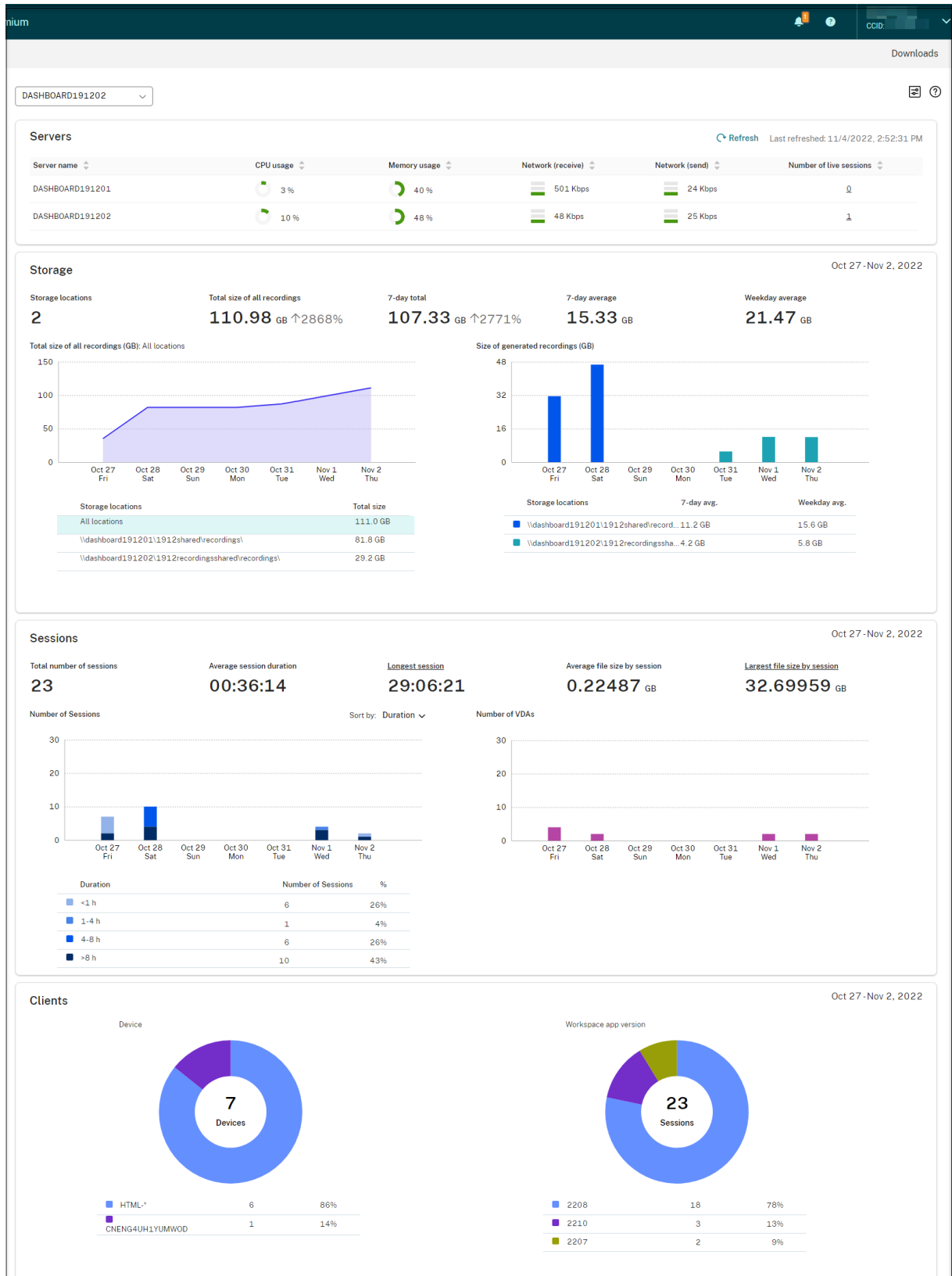
Overview

The Session Recording management dashboard helps you gain insights into your system. It lets you monitor various aspects of your system, including:

- Server status
- Recording success rate
- Storage consumption
- Session statistics
- Client device information

Session Recording service

For a sample dashboard, see the following screen capture:

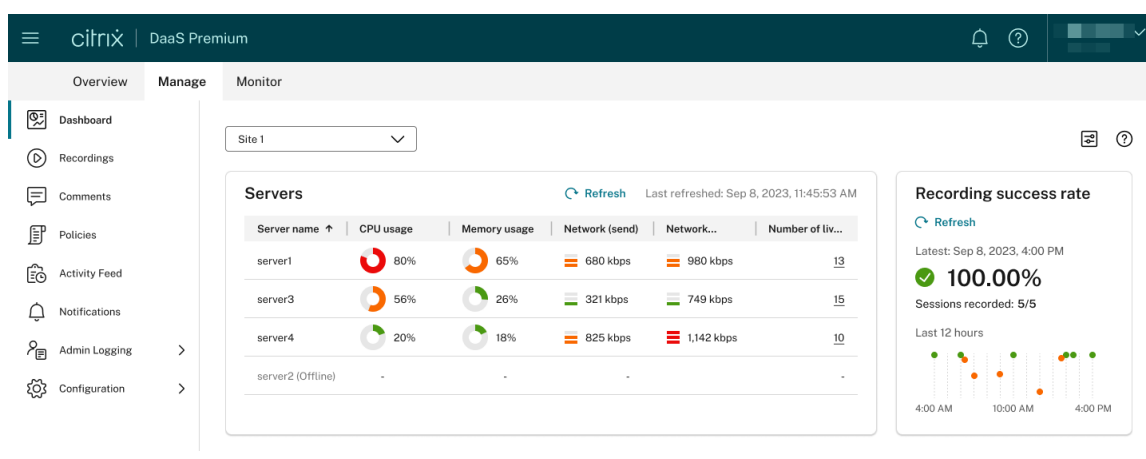


Note:

The recording success rate widget can be shown next to the **Servers** section if the following conditions are met:

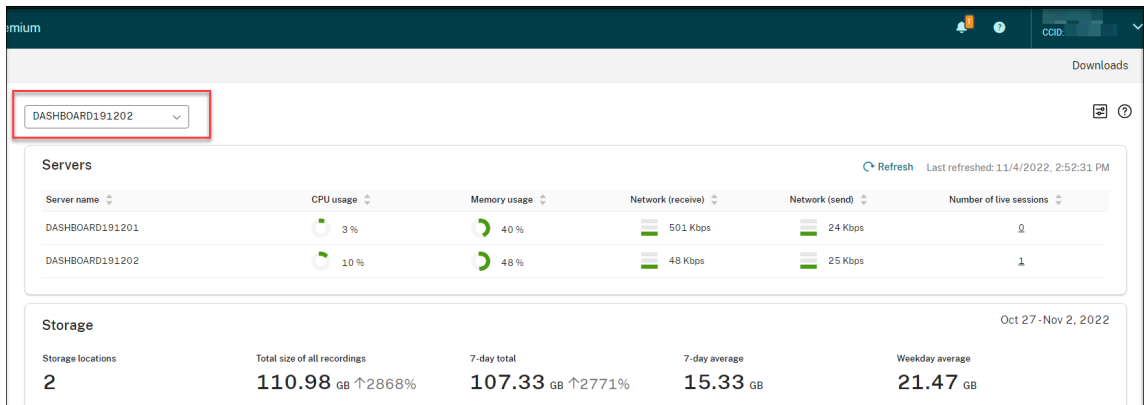
- You are using the cloud client version 7.42.15010.4 or later.
- You have only one site that has available servers and you have turned on the feature toggle on the dashboard settings page of that site.

For example:

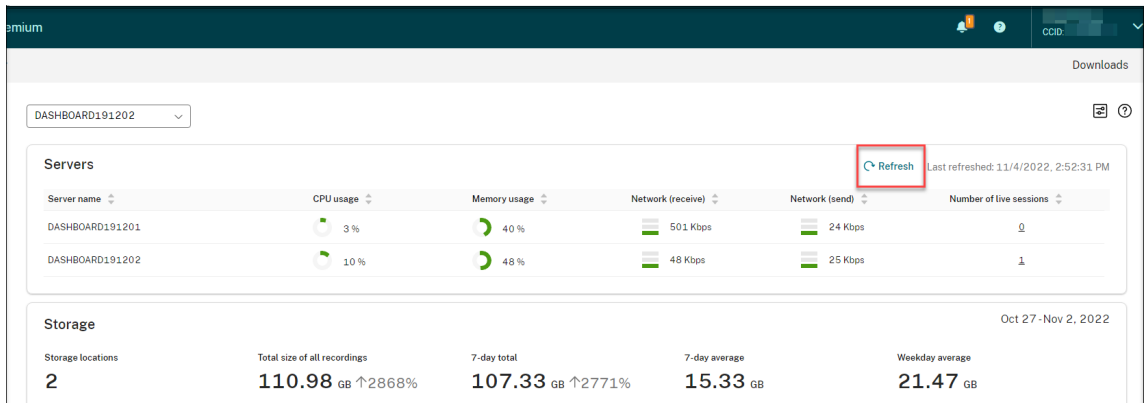


Tips for using the dashboard

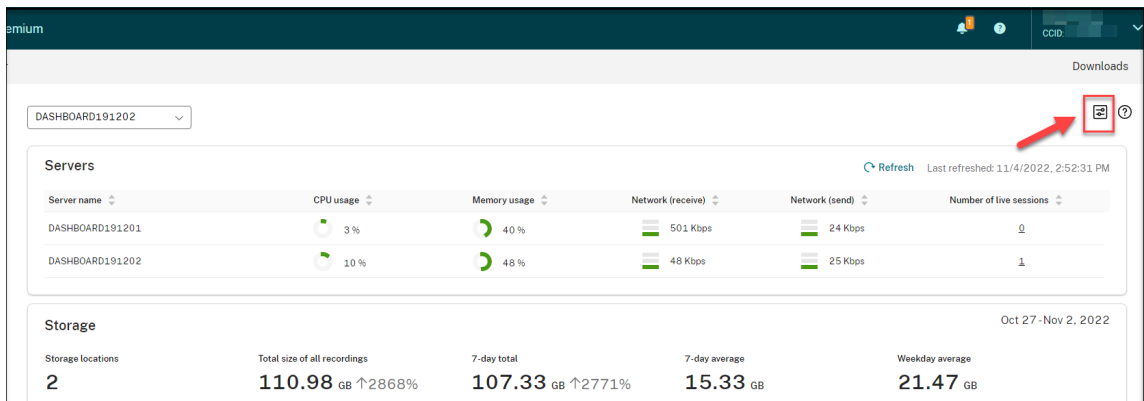
- The dashboard is the new home page for the Session Recording service console. It is available only for Citrix Cloud administrators assigned any of the following roles:
 - Full access
 - **Cloud Administrator, All** role
 - **Session Recording-FullAdmin, All** role
- The dashboard presents data relevant to the site that you select from the drop-down menu in the upper-left corner.



- The **Servers** section refreshes data automatically every 120 seconds. Immediate data refreshes occur when you open the dashboard page, select a site, or click **Refresh**. The next data refresh does not start until the previous refresh completes. Thus, if you click **Refresh** during a data refresh, a popup window appears asking you to try again later.



- The **Storage**, **Sessions**, and **Clients** sections refresh data automatically at a specific time every day. When you select a site or click **Refresh** on the dashboard page, data is refreshed immediately.
- Select a site from the drop down list and click on the icon to display and configure the dashboard settings.



Dashboard settings ✕

Servers

CPU usage

Warning threshold (%) Critical threshold (%)

65 90

Memory usage

Warning threshold (%) Critical threshold (%)

75 90

Network (send)

Warning threshold (kbps) Critical threshold (kbps)

10000 50000

Network (receive)

Warning threshold (kbps) Critical threshold (kbps)

10000 50000

Recording success rate

Collect and show recording success rate

Storage

Storage location	Warning threshold	
\\servername\sharename\directory	Not configured	
\\servername\sharename\directory1	Not configured	
\\servername\sharename\directory2	Not configured	
\\servername\sharename\directory3	Not configured	
\\servername\sharename\directory4	Not configured	

Enable storage consumption forecast

Apply
Cancel

Dashboard settings allow you to:

- Set warning and critical thresholds for:
 - * CPU usage
 - * Memory usage
 - * Network (send)
 - * Network (receive)
- Enable the feature to collect and show recording success rates.
- Allocate space in a location for recording storage and set warning thresholds for the space

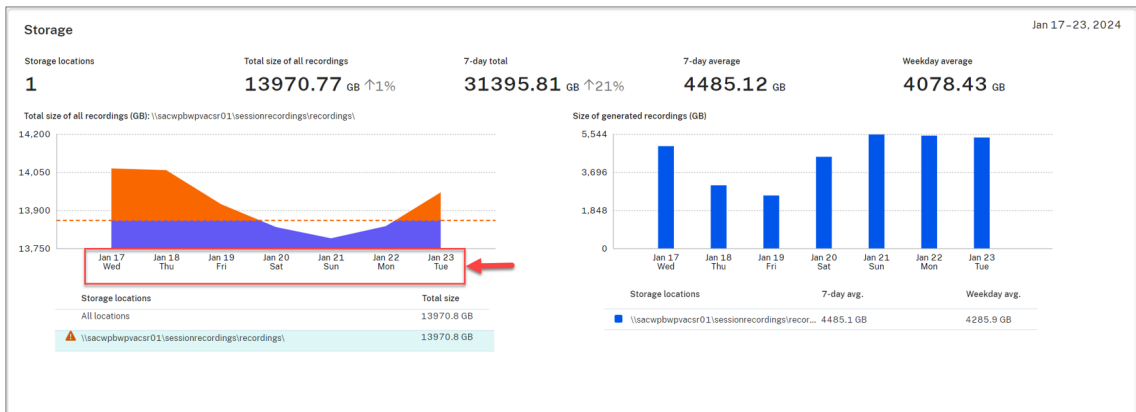
usage. When a warning or critical threshold is reached, the entry is displayed with an orange or red icon.

The storage usage for recorded sessions is influenced by factors such as the chosen image mode and the on-screen activities throughout the sessions. For instance, viewing videos during a virtual session can result in larger recording files.



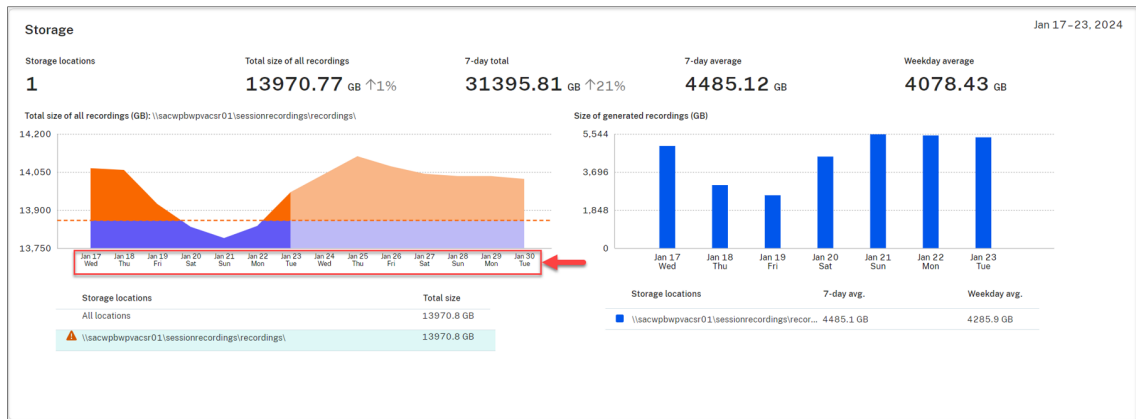
- Enable storage consumption forecast. Storage consumption forecast allows you to predict resource usage and take precautions in advance. After you enable the feature, a storage consumption forecast for the next 7 days can be generated based on sufficient historical consumption data of approximately one month. You can view the forecast on the **Total size of all recordings** chart of the **Storage** section.

When the storage consumption forecast is not enabled, the **Total size of all recordings** chart shows only the actual consumption data over the past 7 days. For example:



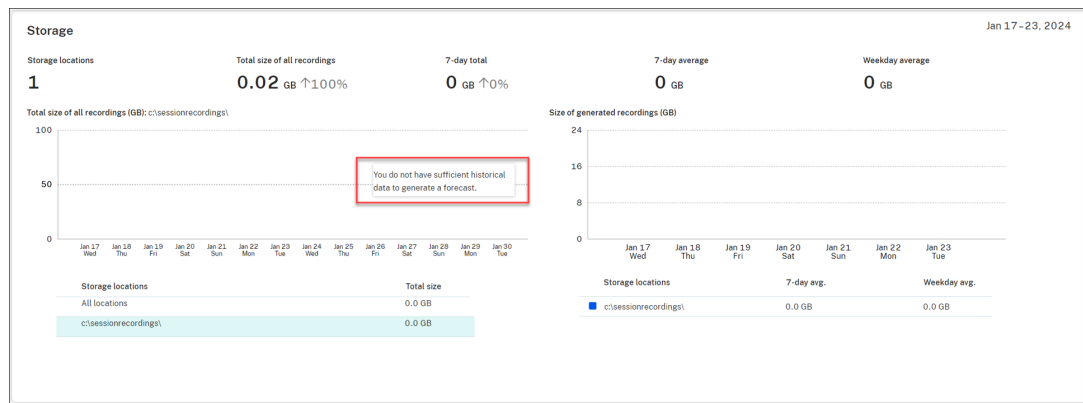
When the storage consumption forecast is enabled, the **Total size of all recordings** chart shows not only the actual consumption data over the past 7 days but also a consumption forecast for the next 7 days. For example:

Session Recording service

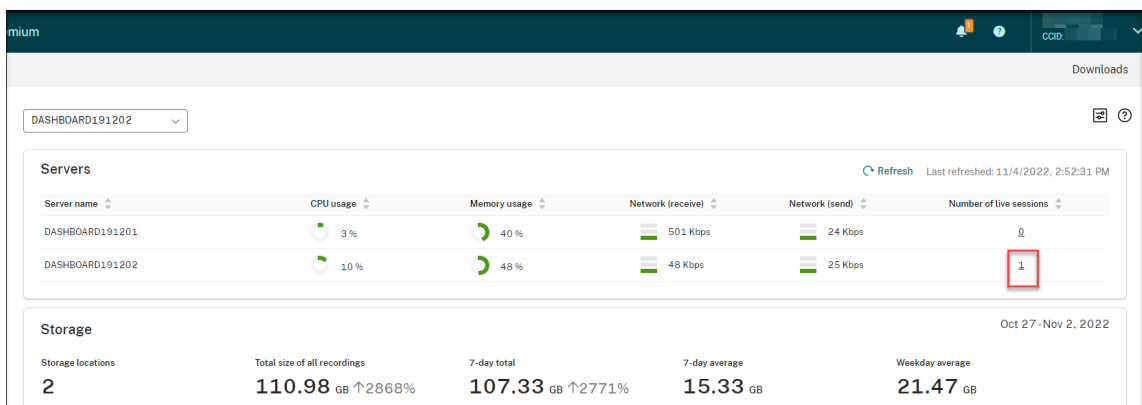


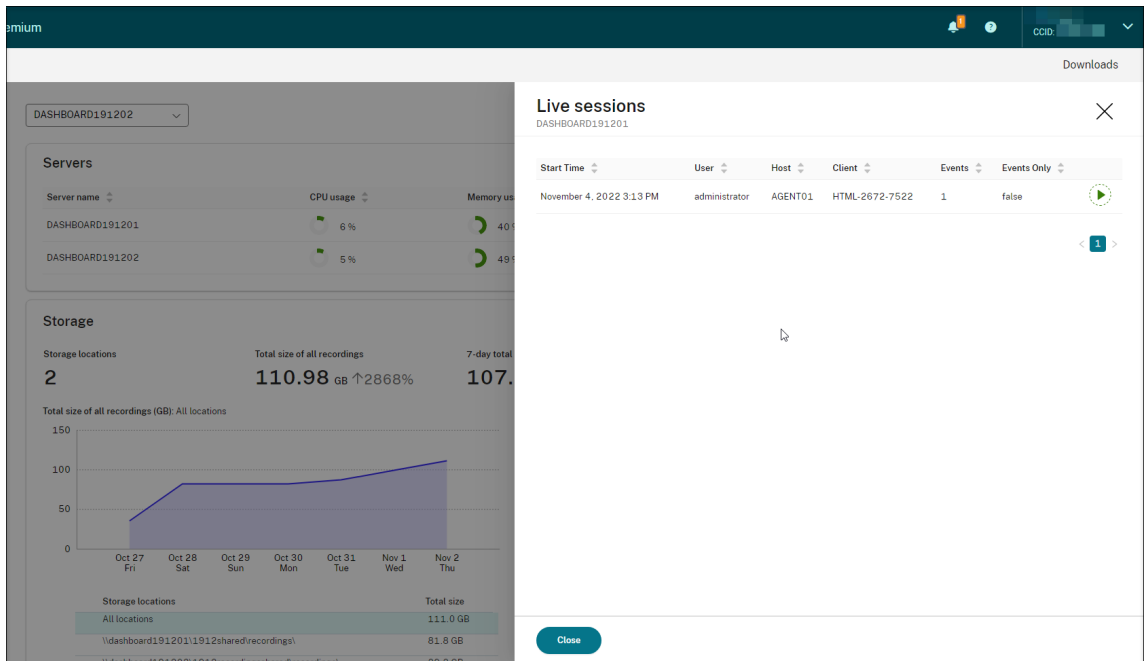
Note:

The consumption forecast requires sufficient historical data of approximately one month. For example, see the following prompt:



- In the **Servers** section, you can open and play live sessions by clicking on the number of live sessions. For example:





- In the **Recording success rate** section, you can see a widget showing the recording success rates for the current site. The recording success rate is calculated as follows:

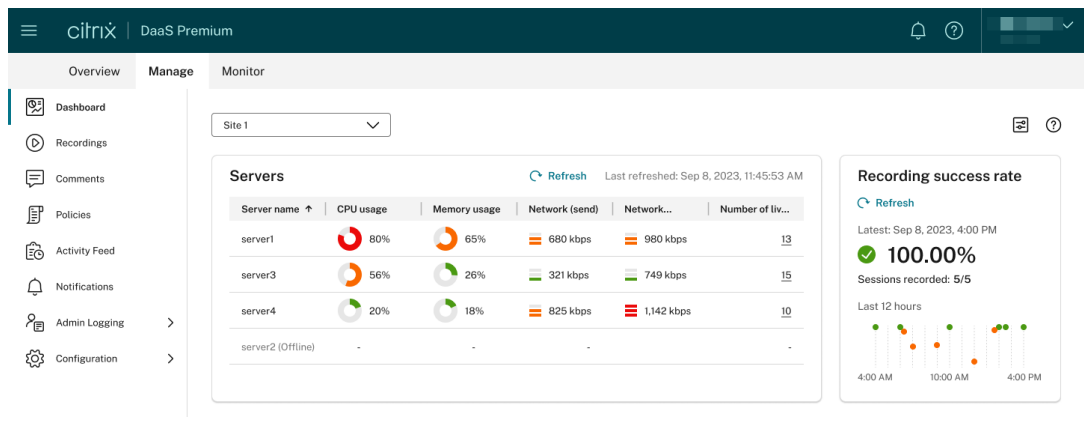
Recording success rate = the number of successfully recorded sessions / the total number of sessions matching the currently active recording policy

Note:

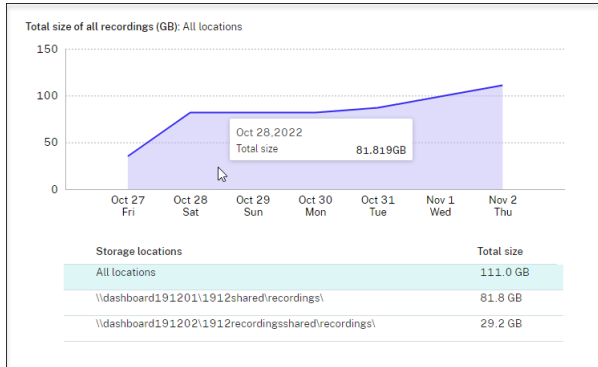
The recording success rate widget can be shown next to the **Servers** section if the following conditions are met:

- You are using the cloud client version 7.42.15010.4 or later.
- You have only one site that has available servers and you have turned on the feature toggle on the dashboard settings page of that site.

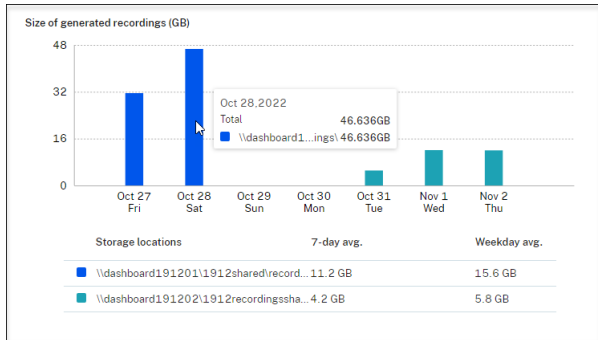
For example:



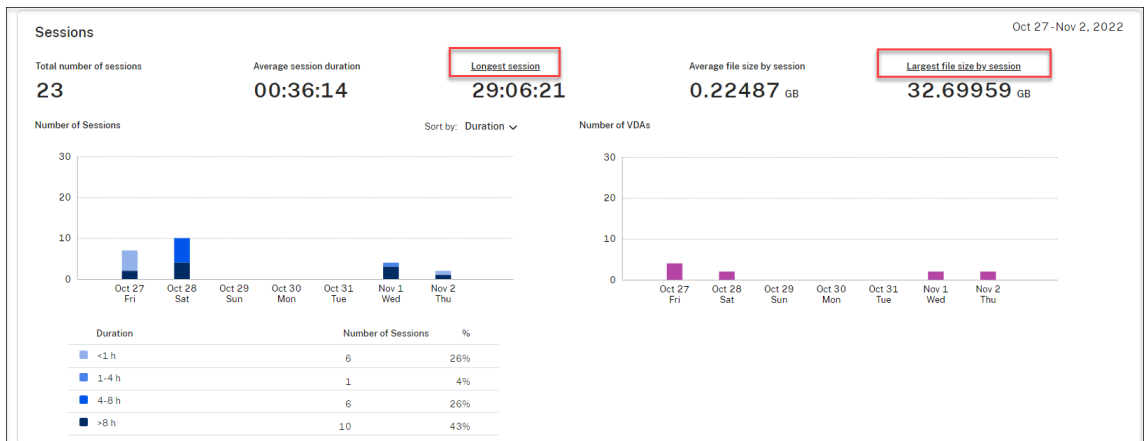
- In the **Total size of all recordings (GB)** section, you can switch between storage locations to view relevant data. You can also hover over the chart to view the total size of all recordings on a specific day.

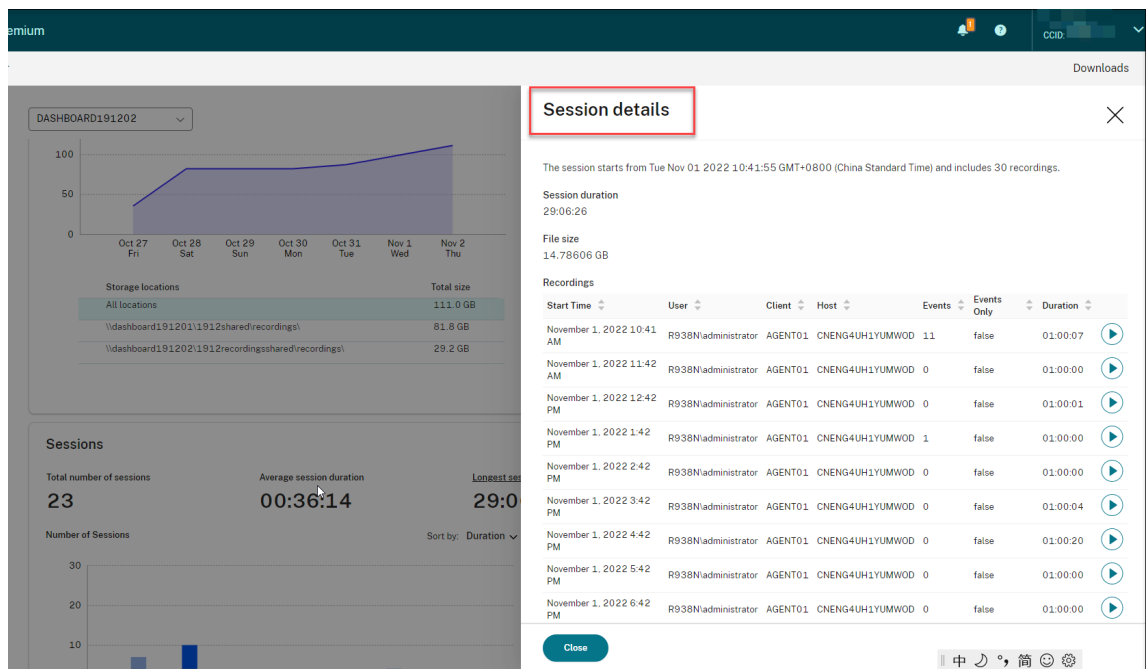


- In the **Size of generated recordings (GB)** section, you can hover over the bar chart corresponding to a day to view the size of newly generated recordings on that day.

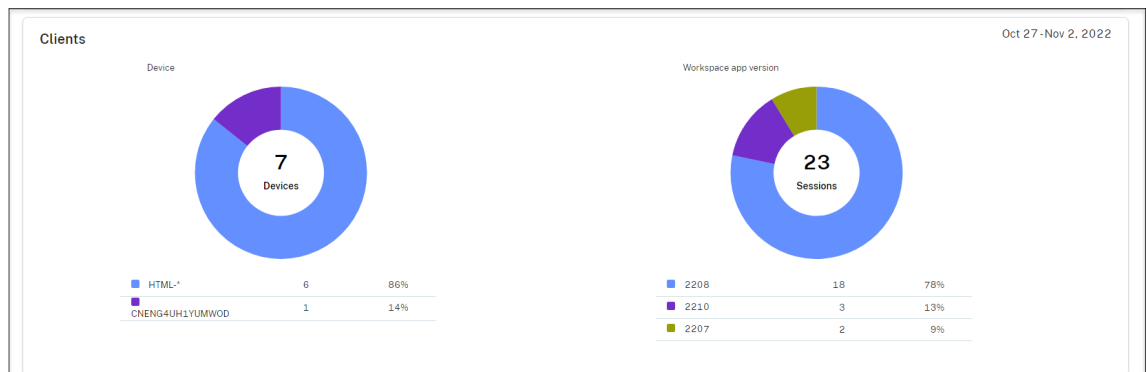


- In the **Sessions** section, you can click **Longest session** and **Largest file size by session** to view session details.





- The **Clients** section shows the percentage of client devices that have different machine name prefixes and the percentage of sessions that run on different versions of Citrix Workspace app.



Activity feed

April 26, 2024

Overview

As a supplement to the [Session Recording management dashboard](#), the Session Recording service introduces an activity feed to improve data visibility and data visualization.

The activity feed gives you information about events and tasks that happened in the past.

Events that the activity feed can show

- CPU usage exceeds threshold
- Memory usage exceeds threshold
- Network (send) usage exceeds threshold
- Network (receive) usage exceeds threshold
- Recording success rate alert
- Storage usage exceeds threshold
- Server status change
- Unrestricted playback link sharing

Note:

The thresholds and the toggle for recording success rate alerts are configurable through the Session Recording management dashboard. For more information, see dashboard settings in the [Tips for using the dashboard](#) section.

Tasks that the activity feed can show

- Automatic archive
- Automatic delete
- Manual archive
- Manual delete
- Statistics

Note:

- You can select target recordings to archive and delete manually. You can also schedule site-level tasks to automatically archive and delete recordings. For more information, see [Manage selected recordings](#) and [Manage recordings on schedule](#).
- Statistics refer to the daily tasks initiated by the system to collect data on storage consumption, sessions, and client devices. The three types of data are displayed in the corresponding sections of the Session Recording management dashboard.

View the activity feed

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.
3. From **Manage**, select **Session Recording**.
4. From the left navigation of the Session Recording service, select **Activity Feed**.

5. Switch between the **Events** and **Tasks** tabs to view the information about events and tasks that happened in the past.

Activity Feed –the **Events** tab

The screenshot shows the 'Events' tab of the Activity Feed. The table lists various events such as 'Server status change' and 'Memory usage exceeds threshold'. The right sidebar shows the details for a selected event, including its time, site, server, and severity.

Time (UTC+08:00)	Event	Site	Server	Severity
January 30, 2024 6:33 PM	Server status change			Info
January 30, 2024 6:33 PM	Server status change			Info
January 30, 2024 6:33 PM	Server status change			Info
January 30, 2024 6:33 PM	Server status change			Info
January 30, 2024 6:33 PM	Server status change			Info
January 30, 2024 6:33 PM	Server status change			Info
January 30, 2024 6:33 PM	Server status change			Info
January 30, 2024 6:33 PM	Server status change			Info
January 30, 2024 6:33 PM	Server status change			Info
January 30, 2024 6:33 PM	Server status change			Info
January 30, 2024 6:33 PM	Server status change			Info
January 30, 2024 6:24 PM	Unrestricted playback link sharing			Info
January 30, 2024 3:34 PM	Memory usage exceeds threshold			Warning
January 30, 2024 3:33 PM	Memory usage exceeds threshold			Warning
January 30, 2024 3:03 PM	Memory usage exceeds threshold			Warning
January 30, 2024 3:03 PM	Memory usage exceeds threshold			Warning

Activity Feed –the **Tasks** tab

The screenshot shows the 'Tasks' tab of the Activity Feed. The table lists various tasks such as 'Manual archive', 'Statistics', and 'Manual delete'. The right sidebar shows the details for a selected task, including its start and end times, status, and a description.

Task	Initiated by	Site	Server	Start Time (UTC+08:00)	End Time (UTC+08:00)	Status
Manual archive	@citrix.com			January 30, 2024 2:11 PM	January 30, 2024 2:11 PM	Completed
Manual archive	@citrix.com			January 30, 2024 1:53 PM	January 30, 2024 1:53 PM	Completed
Statistics	System			January 30, 2024 12:10 PM	January 30, 2024 12:12 PM	Completed
Statistics	System			January 30, 2024 12:10 PM	January 30, 2024 12:12 PM	Completed
Statistics	System			January 30, 2024 12:10 PM	January 30, 2024 12:13 PM	Completed
Statistics	System			January 30, 2024 12:10 PM	January 30, 2024 12:13 PM	Completed
Manual delete	@citrix.com			January 30, 2024 10:30 AM	January 30, 2024 10:30 AM	Completed
Manual delete	@citrix.com			January 30, 2024 10:22 AM	January 30, 2024 10:22 AM	Completed
Manual archive	@citrix.com			January 30, 2024 10:16 AM	January 30, 2024 10:16 AM	Completed
Manual delete	@citrix.com			January 30, 2024 10:14 AM	January 30, 2024 10:15 AM	Failed
Statistics	System			January 29, 2024 12:10 PM	January 29, 2024 12:12 PM	Completed
Statistics	System			January 29, 2024 12:10 PM	January 29, 2024 12:12 PM	Completed
Statistics	System			January 28, 2024 12:10 PM	January 28, 2024 12:12 PM	Completed
Statistics	System			January 28, 2024 12:10 PM	January 28, 2024 12:12 PM	Completed

Note the following tips when viewing the activity feed:

Task	Action
To filter and view specific events or tasks	Select the corresponding filters on the Events or Tasks tab. For example, select the Last 7 days filter to show only events or tasks that happened within the past 7 days.
To update the list of events or tasks immediately	Click Refresh on the Events or Tasks tab.
To copy details about the entire events or tasks	Click Export on the Events or Tasks tab.
To dismiss the entire events or tasks	Click Dismiss all on the Events or Tasks tab. When you click Dismiss all , you are prompted to confirm the action.
To view the details of an individual event or task	Click the event or the task in the list. Events of the same type, site, server and severity are combined into one record and you can expand to display all events.
To copy the details of an individual event or task	Click Copy on the Event Details or Task Details page.
To dismiss an individual event or task	Click Dismiss on the Event Details or Task Details page. You are not prompted for confirmation when clicking Dismiss .

Notifications

April 26, 2024

Email notifications

Overview

To get notified about specific events and tasks through email, subscribe to email notifications.

You can subscribe to be notified about:

- **Resource usage alerts:** When resource usage thresholds are exceeded

Resource usage refers to:

- CPU usage

- Memory usage
- Network (send) usage
- Network (receive) usage
- Storage usage

Resource usage thresholds are configurable through the Session Recording management dashboard. For more information, see dashboard settings in the [Tips for using the dashboard](#) section.

- **Server status changes:** When the status of a Session Recording server changes

The status of a server can change to:

- Offline
- Discovered
- Available
- Deleted
- Uninstalled
- Upgrading
- Ready to install
- Installation in progress

- **Recording success rate alerts:** When a recording success rate is below 100%. To ensure that you can receive email notifications on recording success rates, enable the feature on the dashboard settings page of your site. For more information, see [Management dashboard](#).

- **Storage maintenance results:** A digest of the results of automated tasks for archiving and deleting recordings

For information on scheduling storage maintenance tasks, see [Manage recordings on schedule](#).

- **Unrestricted playback link sharing:** When an unrestricted playback link is shared

For more information, see [Share recordings as links](#).

Subscribe to email notifications

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.
3. From **Manage**, select **Session Recording**.
4. From the left navigation of the Session Recording service, select **Notifications**.

Tip:

You are entitled to 500 email notifications from the Session Recording service every month. After the monthly quota is used up, the Session Recording service stops sending email notifications until the UTC first day of a new month.

5. Set the default recipients that you can apply to all subscribed categories.

Notifications
Email

Quota usage
You're entitled to 500 email notifications from the Session Recording service per month. View your email quota usage below.

426/500

85% used

Resource usage alerts	22
Server status changes	388
Storage maintenance results	10
Recording success rate alerts	3
Unrestricted playback link sharing	3

Subscription
Send email notifications based on your subscriptions below.

Default recipients (0) [Manage recipients](#)

Subscribe to

- Resource usage alerts
Send a notification when resource usage exceeds the threshold.
- Server status changes
Send a notification when the status of a server changes.
- Recording success rate alerts
Send a notification when recording success rate is below 100%
- Storage maintenance results
Send a summary of the results of automated tasks for archiving and deleting recordings.
- Unrestricted playback link sharing
Send a notification when an unrestricted playback link is shared.

Notifications
Email

Quota usage
You're entitled to 500 email notifications from the Session Recording service per month. View your email quota usage below.

85% used

Resource usage alerts	22
Server status changes	388
Storage maintenance results	10
Recording success rate alerts	3
Unrestricted playback link sharing	3

Subscription
Send email notifications based on your subscriptions below.

Default recipients (0) [Manage recipients](#)

Subscribe to

- Resource usage alerts
Send a notification when resource usage exceeds the threshold.
- Server status changes
Send a notification when the status of a server changes.
- Recording success rate alerts

Manage default recipients

✕

Emails are sent to the default recipients if no recipient is specified for a subscribed category.

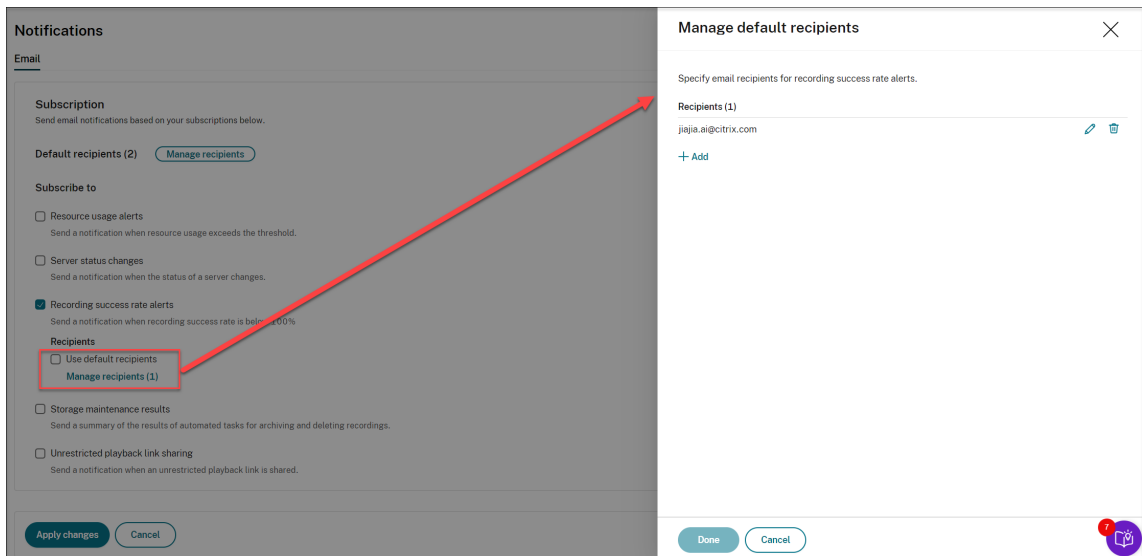
Recipients (0)

+ Add

Done Cancel

Emails are sent to the default recipients if no recipient is specified for a subscribed category.

To specify recipients for a subscribed category, clear the **Use default recipients** check box and then click **Manage recipients** to add recipients.



6. Subscribe to any of the following categories by selecting the check boxes next to them:

- **Resource usage alerts**
- **Server status changes**
- **Recording success rate alerts**
- **Storage maintenance results**
- **Unrestricted playback link sharing**

Tips:

- When you select **Resource usage alerts**, specify the alert types and severities. To optimize your quota usage, warning alerts are withheld after you exceed 50% of your quota until the end of the month.

Notifications

Email

Quota usage
You're entitled to 500 email notifications from the Session Recording service per month. View your email quota usage below. March 2023

338/500

68% used

Resource usage alerts	188
Server status changes	136
Storage maintenance results	14

Subscription

Resource usage alerts
Send a notification when resource usage exceeds the threshold.

Alert type: All selected

- CPU usage
- Memory usage
- Network (send) usage
- Network (receive) usage
- Storage usage

Use default recipients

Server status changes
Send a notification when the status of a server changes.

Send email when a server's status changes to: All selected

Recipients: Use default recipients

Storage maintenance results
Send a summary of the results of automated tasks for archiving and deleting recordings.

Recipients: Use default recipients

Notifications

Email

Subscription
Send email notifications based on your subscriptions below.

Default recipients (7) [Manage recipients](#)

Subscribe to

Resource usage alerts
Send a notification when resource usage exceeds the threshold.

Alert type: All selected

Severity

- Critical
- Warning

To optimize your quota usage, warning alerts are withheld after you exceed 50% of your quota until the end of the month. X

Recipients: Use default recipients
Manage recipients (1)

Server status changes
Send a notification when the status of a server changes.

[Apply changes](#) [Cancel](#)

- For the available server statuses, see the following screen capture:

Session Recording service

Notifications

Email

Quota usage
You're entitled to 500 email notifications from the Session Recording service per month. View your email quota usage below. March 2023

68% used

338/500

Resource usage alerts	188
Server status changes	136
Storage maintenance results	14

Subscription
Send email notifications based on your subscriptions below.

Default recipients (6) [Manage recipients](#)

Subscribe to

Resource usage alerts
Send a notification when resource usage exceeds the threshold.

Alert type: All selected

Severity: Offline, Discovered, Available, Deleted, Uninstalled, Upgrading, Ready to install, Installation in progress

Storage maintenance results
Send a summary of the results of automated tasks for archiving and deleting recordings.

Recipients: Use default recipients

- Emails are sent separately for each subscribed category. For example, an email notification about resource usage is similar to the following:

Session Recording resource usage alert External Inbox

sessionrecording-xac-no-reply@apps.cloud.com to me

8:00 AM (6 hours ago)

citrix

Session Recording - Memory usage alert (Critical)

Customer name: [redacted]
Organization ID: [redacted]

Memory usage has exceeded Critical threshold.

Site: [redacted]
Critical threshold: 75%
Time (UTC-05:00): 2023-03-28T19:41:51.514996

Server: [redacted]

Memory usage: 76%

To change your email notification settings, go to Configuration > Notification Settings in the Session Recording service.

This is an automated email from the Session Recording service. Do not reply.

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.

Best practices

June 19, 2024

You can consult the following best practices documentation for deploying Session Recording and configuring load balancing:

- [Configure load balancing in an existing deployment](#)
- [Deploy and load-balance Session Recording in Azure](#)

Integrate with Citrix HDX plus for Windows 365 in a Session Recording deployment

June 20, 2024

This article walks you through the procedures of creating a Session Recording site through a host connection and then integrating the Session Recording service with Citrix HDX plus for Windows 365.

Requirements for using this solution

To successfully implement the solution, the following requirements must be fulfilled:

Citrix requirements

- Citrix Cloud tenant with [Citrix HDX Plus for Windows 365](#) entitlement
- Citrix Cloud administrator account with full administrator rights.
- The deployed environment must have access to:
 - 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 the Session Recording cloud client)

Microsoft requirements

- Azure administrator account:
 - Azure AD Global administrator

Supported Configurations

The Session Recording service supports Windows 365 deployments with Entra joined, and Entra hybrid joined Cloud PCs.

Step 1: Add a host connection to your Azure subscription

For a step-by-step guide, see [Add a host connection](#).

Step 2: Create and deploy a Session Recording site through the host connection

You can create a site to deploy the following Session Recording resources to your Azure subscription from within the Session Recording service:

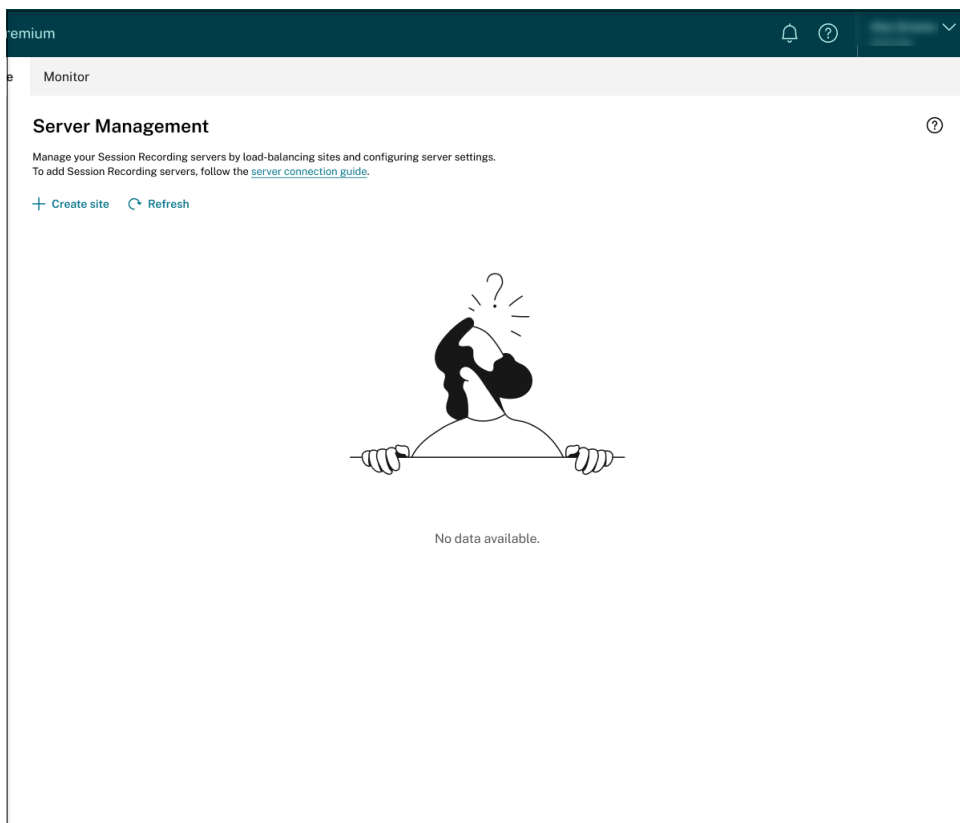
- Session Recording servers
- Databases
- Storage
- Load balancer

You can also get recommended VM and storage configurations, predict costs, and view the actual monthly costs for using Azure from within the Session Recording service.

For an existing site deployed on Azure, you can add resources including servers and storage to it and change the IP addresses that are allowed to access the load balancer.

This article guides you through the following procedures:

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



2. On the **Server Management** page, click **Create site**. The **Create Site** page appears.

Create site [Close]

1 Site information

What would you like to do?

- Create an empty site**
Create a site and add servers later.
- Create and deploy a site through a host connection**
Deploy Session Recording resources using a host connection that connects to your specific cloud subscription. [Learn more](#)
- Create and deploy a site through an ARM template**
Create an Azure Resource Manager template (ARM template) to deploy Session Recording resources in Azure. [Learn more](#)

Site name
Name this site

Description (optional)
Enter description

Save Cancel [Help 8]

3. Select **Create and deploy a site through a host connection**. The main steps are listed in the left navigation.

4. Enter a site name and description, select the host connection that you added in Step 1, and specify a region. Azure Government regions aren't supported.
5. After completing the site information, click **Next** to continue.
6. (Optional) To get recommendations for VM and storage configurations, provide information about your recording needs.

You can skip this step by clicking **I'm good, skip this step** or by clicking **Next** with nothing selected.

Create site ✕

1 Site information

2 About your deployment
Optional

3 Network

4 Virtual machines

5 Domain and certificate

6 Storage

7 Databases

8 Load balancer

9 Tags
Optional

10 Secure client

11 Summary

Tell us about your recording needs, so we can provide some recommendations for your VM and storage configurations.

[I'm good, skip this step.](#)

The following information helps determine the recommended number of Session Recording servers.

How many concurrent sessions do you have at most?

4,000-6,000

Recommended number of servers: 3 [reset](#)

The following information helps determine the recommended storage capacity.

How much visual movement do your sessions typically have?

Some, the display changes but not drastically

How many sessions do you need to record per day?

5,000-10,000

For how long do you need to retain each recording file?

15-30 days

Recommended storage capacity: 30 TiB [reset](#)

[Next](#) [Cancel](#) 8

When you select an option from the drop-down list, a recommendation is presented according to your selection. A **reset** button is available next to the recommendation. It lets you clear your selections and the corresponding recommendation in that section.

7. Specify the virtual network and subnet for your Session Recording servers to join. If your VDAs reside in a different virtual network from the Session Recording servers or in an on-premises network, establish connectivity to ensure the Session Recording servers can communicate with your VDAs.

Create site ✕

- ✓ Site information
- ✓ About your deployment
Optional
- 3 Network**
- 4 Virtual machines
- 5 Domain and certificate
- 6 Storage
- 7 Databases
- 8 Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary


Specify the virtual network and subnet for your Session Recording servers to join.

Virtual network

Select a virtual network that your VDAs can connect to.

Subnet

Select a subnet that your VDAs can connect to.

Next **Cancel** 

8. Create virtual machines (VMs) as your Session Recording servers.

Note:

- The **Number of VMs** field is prefilled with the recommended number if there’s one. Change the number as needed.
- Estimated costs are based on standard pricing and don’t take discounts into consideration. You can expect lower actual costs than estimated.

9. Join the Session Recording servers to the same domain with your VDAs and specify a certificate for the Session Recording servers.

- If your VDAs connect to an Active Directory domain, select the **Join servers to an Active Directory domain** check box and enter the relevant information. By selecting the **Join servers to an Active Directory domain** check box, you are configuring the deployment for a hybrid scenario, integrating on-premises Active Directory with Azure AD.
- If your VDAs connect to an Azure Active Directory (Azure AD) domain, clear the **Join servers to an Active Directory domain** check box. After you complete creating the current site, make sure to manually join the Session Recording servers to the same Azure AD domain. Notice that pure Azure AD deployment is available only for Session Recording 2402 and later.

Create site ✕

- ✓ Site information
- ✓ About your deployment
Optional
- ✓ Network
- ✓ Virtual machines
- 5 Domain and certificate**
- 6 Storage
- 7 Databases
- 8 Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

Join servers to an Active Directory domain

i This should be the domain where your VDAs reside.

Domain name

Domain controller IP address

Username


Specify a domain user with sufficient rights to join machines to the domain.

Password

Specify a certificate for the virtual machines to use. Only .pfx files are supported.

Certificate

Certificate password



Create site

- Site information
- About your deployment
Optional
- Network
- Virtual machines
- 5 Domain and certificate**
- 6 Storage
- 7 Databases
- 8 Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

Join servers to an Active Directory domain

Supported only on Session Recording server version 2402 or later. Please select a compatible version in the previous step. [Go back](#)

Specify a certificate for the virtual machines to use. Only .pfx files are supported.

Certificate

[Browse](#)

Certificate password

Enter password

[Next](#) [Cancel](#)

Note:

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

10. Configure an Azure storage account and file shares to store your recording files. For pricing information, see [Azure Files pricing](#).

Create site

- Site information
- About your deployment
Optional
- Network
- Virtual machines
- Domain and certificate
- Storage**
- Databases
- Load balancer
- Tags
Optional
- Secure client
- Summary

Configure a storage account and file shares to store your recording files. For pricing information, see [Azure File Pricing](#).

i A separate storage account will be created for your archived recordings, which does not generate any cost if not used.

Storage account

Performance

Standard: Recommended for most scenarios (general-purpose v2 account).
 Premium: Recommended for scenarios that requires low latency.

Redundancy

Locally-redundant storage (LRS)

File shares

Tier

Transaction optimized

Maximum capacity

5 TiB

Number of file shares

6 **i** Recommended for you: 6

Estimated cost (per month)

\$1843.2 (max.)
\$0.06 per used GiB, actual cost depends on your usage.

Next **Cancel**

11. Create two SQL databases in Azure. One is used as the Session recording database (named **sessionrecording**) and the other as the administrator logging database (named **sessionrecordinglogging**).

Create site

Create 2 SQL databases for recording and logging data, respectively.

- Site information
- About your deployment
Optional
- Network
- Virtual machines
- Domain and certificate
- Storage
- 7 Databases**
- 8 Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

Compute + storage

Service tier
General Purpose

Compute tier
Provisioned

Hardware configuration
Standard-series (Gen5)
Up to 128 vCores, up to 625 GiB memory

vCores
2

Data max size (GiB)
32

Estimated cost (per month)
\$441.3

Database administrator

Username
dbadmin1

Password
.....

Confirm password
.....

Next Cancel

12. Create a load balancer to distribute workload among the Session Recording servers. Enter the IP addresses or ranges of your VDAs and separate them by a comma (,) in the **Restrict access of the load balancer to only the following addresses** field. For pricing information, see [Load Balancer pricing](#).

Create site ✕

- ✓ Site information
- ✓ About your deployment
Optional
- ✓ Network
- ✓ Virtual machines
- ✓ Domain and certificate
- ✓ Storage
- ✓ Databases
- 8** Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

Create a load balancer to distribute workload among the servers. For pricing information, see [Load Balancer Pricing](#).

Azure load balancer

SKU
Standard

Type
Public

Tier
Regional

Estimated cost (per month)
\$189.6

Access

Restrict access of the load balancer to only the following addresses ?

Next **Cancel** 8


13. (Optional) Apply tags to the Azure resources to be created.

Create site ✕

- ✓ Site information
- ✓ About your deployment
Optional
- ✓ Network
- ✓ Virtual machines
- ✓ Domain and certificate
- ✓ Storage
- ✓ Databases
- ✓ Load balancer
- 9 Tags
Optional
- 10 Secure client
- 11 Summary

You can apply tags to the Azure resources that will be created.
If no tags are needed, simply click **Next** to continue.

Name	Value
+ Add	

Next **Cancel** 

14. Create a secure client to onboard the Session Recording servers to the Session Recording service.

Click **Create client** to let Citrix create a secure client on your behalf. Alternatively, you can create a secure client through the **Identity and Access Management > API Access** tab of the Citrix Cloud console and then fill in the information below.

Create site ✕

- ✓ Site information
- ✓ About your deployment
Optional
- ✓ Network
- ✓ Virtual machines
- ✓ Domain and certificate
- ✓ Storage
- ✓ Databases
- ✓ Load balancer
- ✓ Tags
Optional
- 10 Secure client
- 11 Summary

Create a secure client to onboard the Session Recording servers to the Session Recording service.


Click Create client and we will create a secure client on your behalf. Alternatively, you can create a secure client through the [Identity and Access Management > API Access](#) tab of the Citrix Cloud console and then fill in the information below.

[Create client](#)

ID

Secret

[Next](#) [Cancel](#)



15. View the summary about the site to be created. Click the pencil icon to edit your settings if needed or click the button to start deployment.

The screenshot shows the 'Create site' wizard in Azure. The left sidebar lists the steps: Site information, About your deployment (Optional), Network, Virtual machines, Domain and certificate, Storage, Databases, Load balancer, Tags (Optional), Secure client, and Summary (11). The main area displays a summary of resources to be created for the 'US East' region. The resources include:

- Virtual machine (3):** Image: Windows Server 2022 Datacenter: Azure Edition -x64 Gen2, Size: Standard_D4s_v3-4vcpus, 16 GiB memory.
- Storage account:** Performance: Standard, Redundancy: LRS.
- Storage account (for archive):** Performance: Standard, Redundancy: LRS.
- File shares (6):** Maximum capacity: 5 TiB.
- File Share:** Maximum capacity: 5 TiB.
- Databases (2):** Service tier: General Purpose, vCores: 2, Data max size: 32 GiB.
- Load balancer:** SKU: Standard, Type: Regional, Tier: Tier.

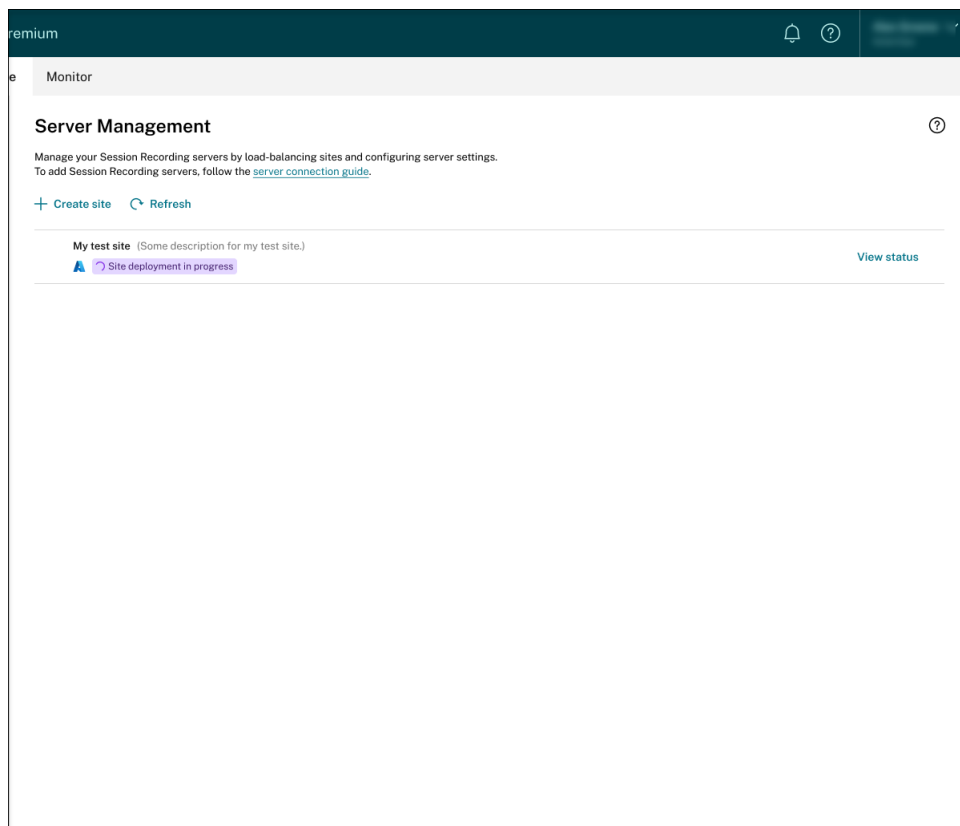
Estimated cost (per month): \$3286.26

Virtual machines	\$812.16	Databases	\$441.30
Storage	\$1843.20	Azure load balancer	\$189.60

At the bottom, there are 'Start deployment' and 'Cancel' buttons, and a notification icon with the number 8.

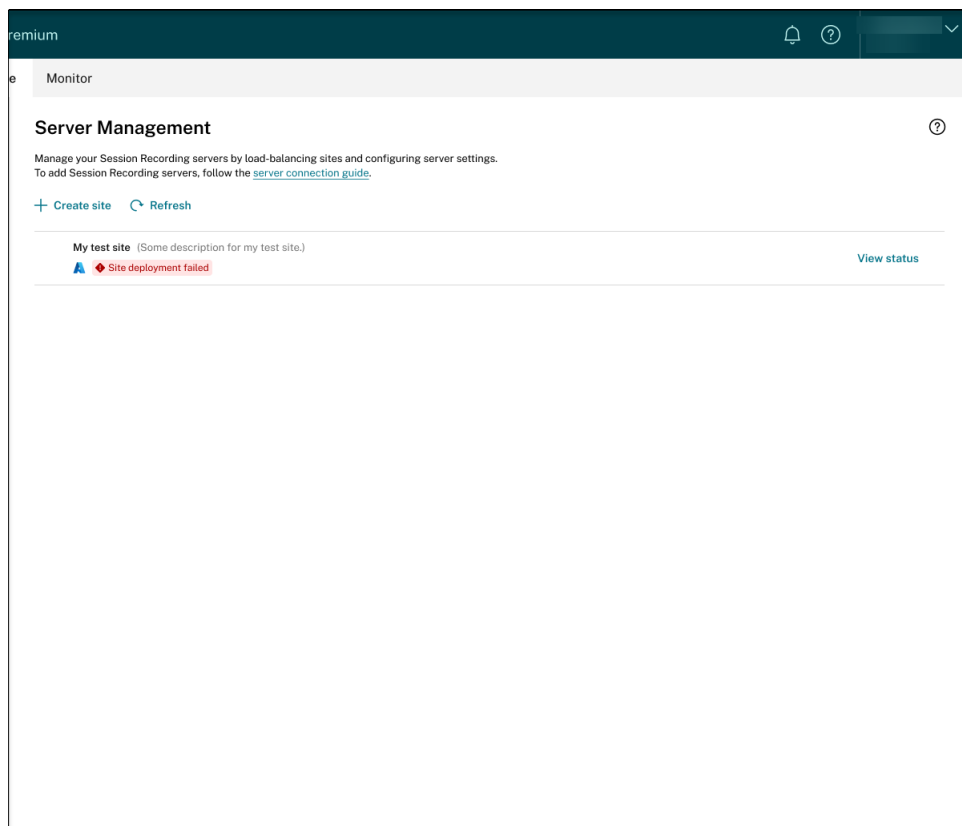
The following are examples of the deployment process:

Deployment in progress:




While a site deployment is in progress, you can click **View status** to view the progress.


Deployment failed:



If errors occur during the deployment process, click **View status** to view the error details. For an example of the error details:


Create site ✕

 Error



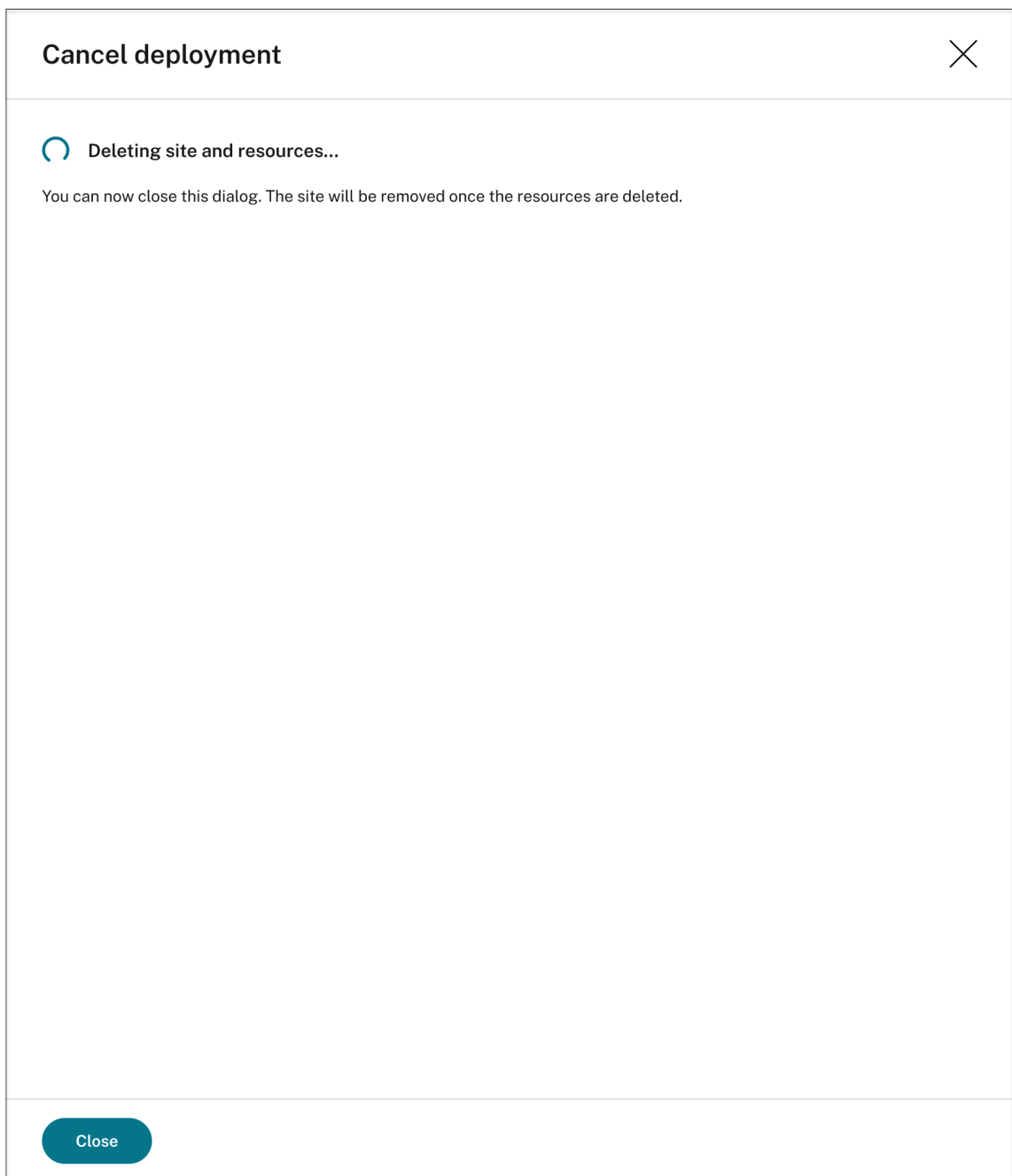
Go back to adjust your input as needed and then try again. When you retry, we will delete the resources that have been created and start afresh.

Don't want to create this site anymore? You can [cancel the deployment](#) and we will delete any resources already created.



[Back to configuration](#) [Close](#)

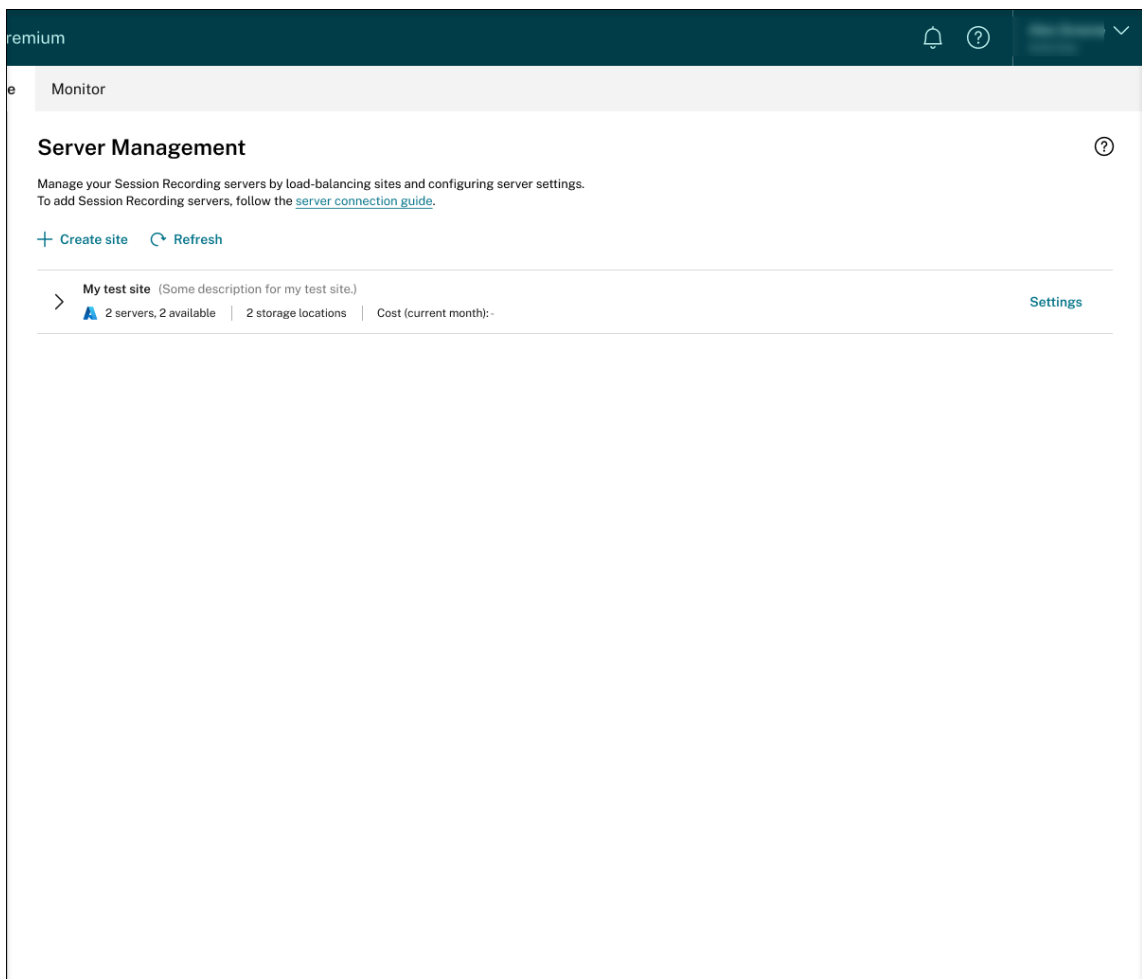
You can click **Back to configuration** or **cancel the deployment**. If you click **Back to configuration**, you're taken back to the **Create Site** page where you can alter your configurations and try again. If you're sure to cancel the deployment, follow the wizard to remove the site and the Azure resources created for the site. For example:



Deployment success:

When a site deployment is complete, you can expand the site and view and manage the resources created under it. The **View status** button changes to **Settings**. An Azure icon is available to represent sites deployed on Azure.

For information about site settings, see [Site and server settings](#).

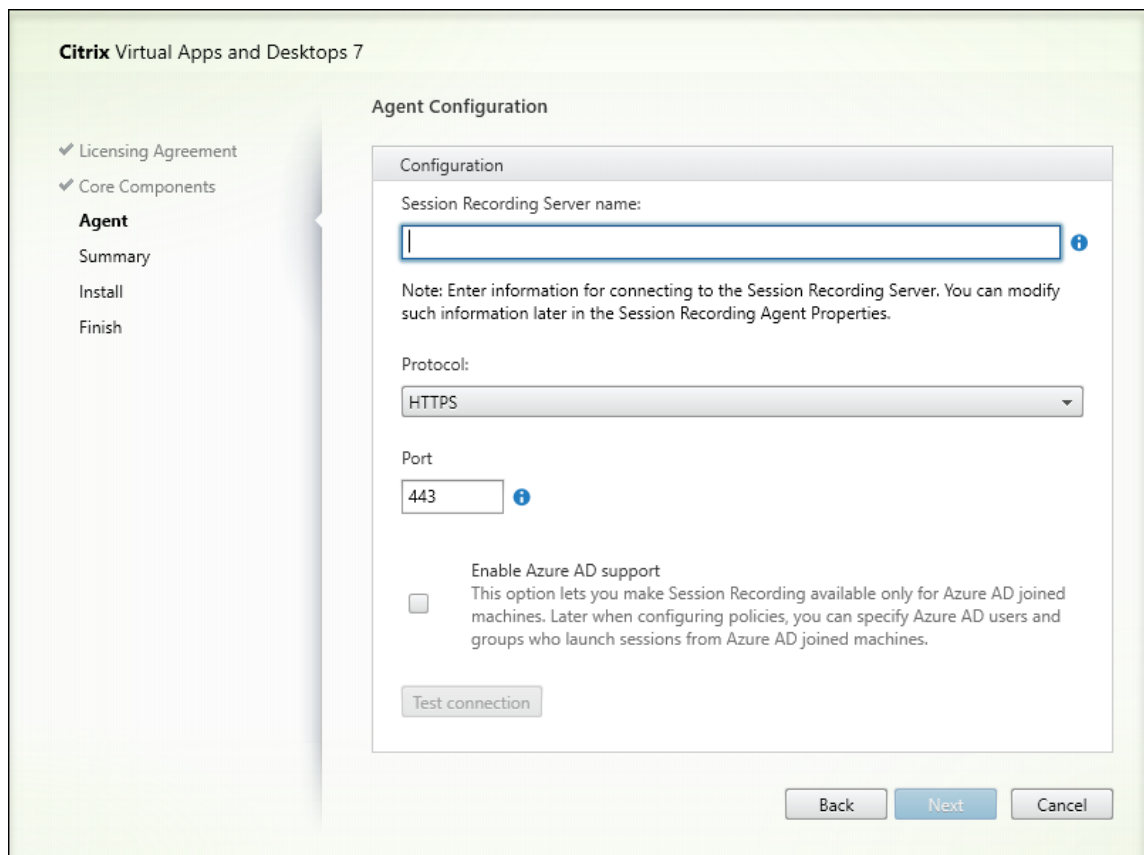


Keep a record of the storage location and the DNS name listed in the load balancer section. The DNS name will serve as the Session Recording server name that you need to fill in later for communicating with the VDAs.

Step 3: Install and configure the Session Recording agent on Windows 365 cloud PCs

On the target Windows 365 cloud PCs, install the Session Recording agent. During the agent installation, make sure that you complete the following steps on the **Agent configuration** page:

- Enter the DNS name you previously recorded in the **Session Recording Server name** text box.
- If you are installing the Session Recording agent on an Azure AD joined machine, select **Enable Azure AD support**. Otherwise, clear the check box. By clearing the check box, you are configuring the deployment for a hybrid scenario, integrating on-premises Active Directory with Azure AD.



Step 4: Configure policies

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.

For more information, see:

- [Configure session recording policies](#)
- [Configure event detection policies](#)
- [Configure event response policies](#)

Step 5: Replay recorded sessions

To replay recorded sessions, go to the **All Recordings** and **Archived** pages. Each recording has a play button on the right side. You can play live and completed recordings. For more information, see the [View recordings](#) chapter.

Troubleshoot

February 22, 2024

The troubleshooting information contains solutions to issues that might occur when you use the Session Recording service, for example:

- [Server troubleshooting from the cloud](#)
- [Servers not seen in the cloud](#)

Server troubleshooting from the cloud

July 13, 2023

When a Session Recording server does not work as expected even though it shows **Available** on the cloud, you can perform a few troubleshooting actions from the cloud:

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 **Troubleshooting** icon next to it. The **Troubleshooting** page appears.

Tip:

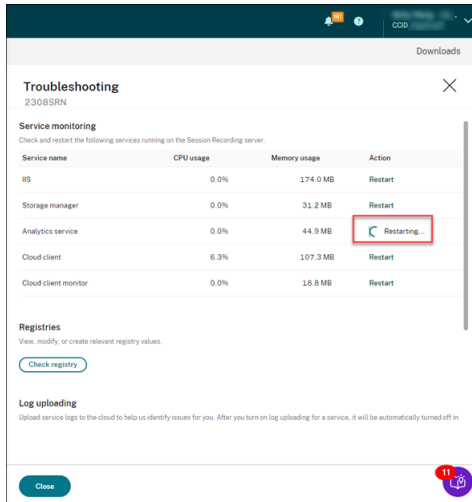
The **Troubleshooting** icon is present only for servers in **Available** state.

Site	Server ID	Server version	Cloud client version	Status	Actions
2308SRN 1 server, 1 available	2308SRN	22.3.3090.4	7.39.25758.25384	Available	Troubleshooting, Settings
	Servers				
ATEST 2 servers, 0 available	79880BF6891	22.6.0.760	7.39.25732.44993	Offline	Settings
	AUTOSERVER3	23.3.0.17	7.39.25754.46001	Uninstalled	Settings
	Servers				
AutoTestApiSite202306301601 2 servers, 0 available	AUTOSERVER1	22.10.0.8	7.39.25758.25384	Offline	Settings
	AUTOSERVER2	22.10.0.8	7.39.25758.25384	Uninstalled	Settings
	Servers				

3. Perform the following troubleshooting actions on the target server as needed :
 - a) In the **Service monitoring** section, check and restart the following services running on the Session Recording server:

- The IIS,
- The Citrix Session Recording Analytics Service (CitrixSsRecAnalyticsService),
- The Citrix Session Recording Storage Manager Service (CitrixSsRecStorageManager),
and
- The Citrix Session Recording Cloud Client Monitor Service (CitrixSsRecCloudClient-MonitorService).

For example:

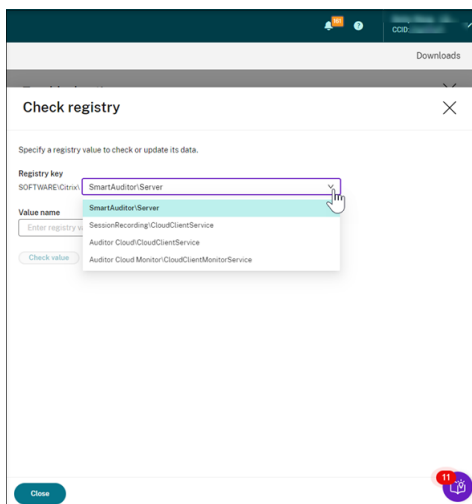


If you restart a service successfully, the **Restarted** status initially appears and then the **Restart** button is displayed.

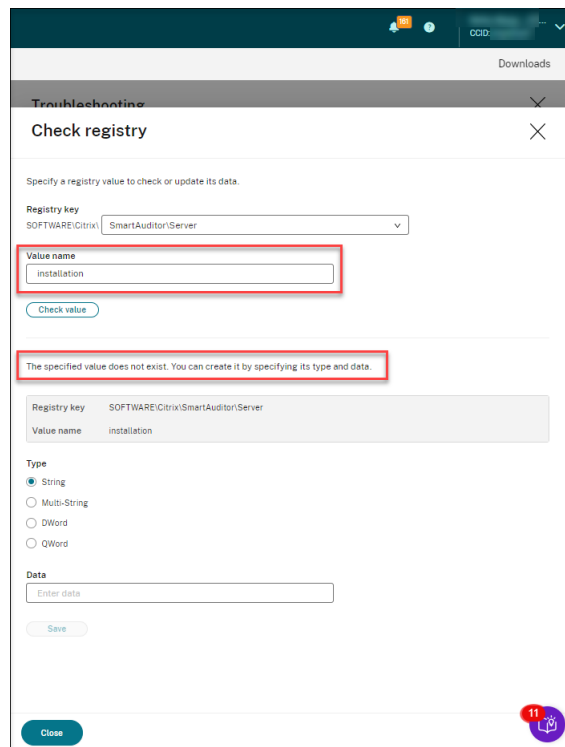
If your attempt to restart a service is unsuccessful, the **Failed** status initially appears and then the **Restart** button is displayed.

- b) In the **Registries** section, click **Check Registry** to view, modify, and create relevant registry values.

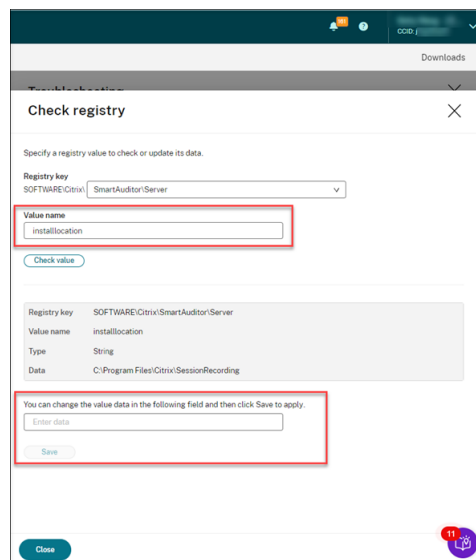
Select a registry key from the drop-down list.



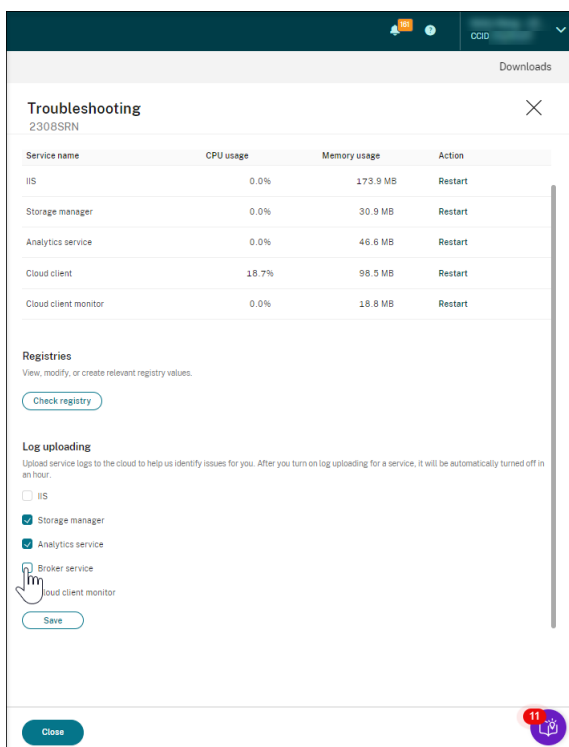
Enter a registry value to check whether it exists. If a registry value you enter does not exist, you can create it as needed by following the instructions.



If a registry value you enter exists, you can view its information and modify its value data as needed.



- c) In the **Log uploading** section, select services of your choice to upload logs about them to the cloud. The logs help Citrix identify issues for you. Click Save after making your selections.



Servers not seen in the cloud

February 22, 2024

A Session Recording server you connected might not show in the cloud.

Possible cause: Outbound traffic is denied for the Session Recording server to reach the Session Recording service through port 443 or ports 80, 443, 8088, and 9090–9094 depending on the version of your cloud client.

With versions 7.40.13020.11 and later of the cloud client, you need to only open a single port (TCP port 443) for communication. Cloud clients earlier than version 7.40.13020.11 require you to open more ports. For more information, see [Ports](#).

If you are using version 7.40.13020.11 or later of the cloud client, complete the following steps to address the issue:

1. Check whether port 443 is open by running the following script on the Session Recording server:

```
1 # Copyright (c) Citrix Systems, Inc. All rights reserved.
2
3 <#
4     .SYNOPSIS
5     This script is used to check whether or not port 443 is open.
```

```
6     Note: Execute this script from the machine where you installed
      the cloud client.
7 #>
8
9 $SR_CLOUD_DOMAIN = "srs.apps.cloud.com"
10 function Check-PortStatus {
11
12
13
14     $cstResult = tnc $SR_CLOUD_DOMAIN -port 443
15     if($cstResult.TcpTestSucceeded -ne $True) {
16
17         Write-Host "Error : $SR_CLOUD_DOMAIN : $_ is unreachable"
18         -ForegroundColor Red
19     }
20     else {
21
22         Write-Host "$SR_CLOUD_DOMAIN : 443 is open" -
23         ForegroundColor Green
24     }
25 }
26
27
28 Check-PortStatus
29 <!--NeedCopy-->
```

The output of the port checking script can be **srs.apps.cloud.com <port number> is unreachable** or **srs.apps.cloud.com <port number> is open**.

2. Allow outbound traffic on port 443 for the Session Recording server to reach the Session Recording service.
3. Reinstall the cloud client on the Session Recording server.

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.

If you are using a cloud client earlier than version 7.40.13020.11, complete the following steps to address the issue:

1. Check whether ports 8088, 443, 9090, 9091, 9092, 9093, and 9094 are open by running the following script on the Session Recording server:

```
1 # Copyright (c) Citrix Systems, Inc. All rights reserved.
2
3 <#
4 .SYNOPSIS
5 This script is used to check whether or not ports
   8088,443,9090,9091,9092,9093,and 9094 are open.
```

```

6     Note: Execute this script from the machine where you installed
      the cloud client.
7 #>
8
9 $SR_CLOUD_DOMAIN = "sessionrecording.apps.cloud.com"
10 function Check-PortStatus {
11
12     (8088,443,9090,9091,9092,9093,9094) | ForEach-Object {
13
14         $tResult = tnc $SR_CLOUD_DOMAIN -port $_
15         if($tResult.TcpTestSucceeded -ne $True) {
16
17             Write-Host "Error : $SR_CLOUD_DOMAIN : $_ is
18                 unreachable" -ForegroundColor Red
19         }
20         else {
21
22             Write-Host "$SR_CLOUD_DOMAIN : $_ is open" -
23                 ForegroundColor Green
24         }
25     }
26 }
27 }
28
29
30 Check-PortStatus
31 <!--NeedCopy-->

```

The output of the port checking script can be **sessionrecording.apps.cloud.com <port number> is unreachable** or **sessionrecording.apps.cloud.com <port number> is open**.

2. Allow outbound traffic on ports 80, 443, 8088, and 9090–9094 for the Session Recording server to reach the Session Recording service.
3. Reinstall the cloud client on the Session Recording server.

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.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).