Session Recording service

Note:

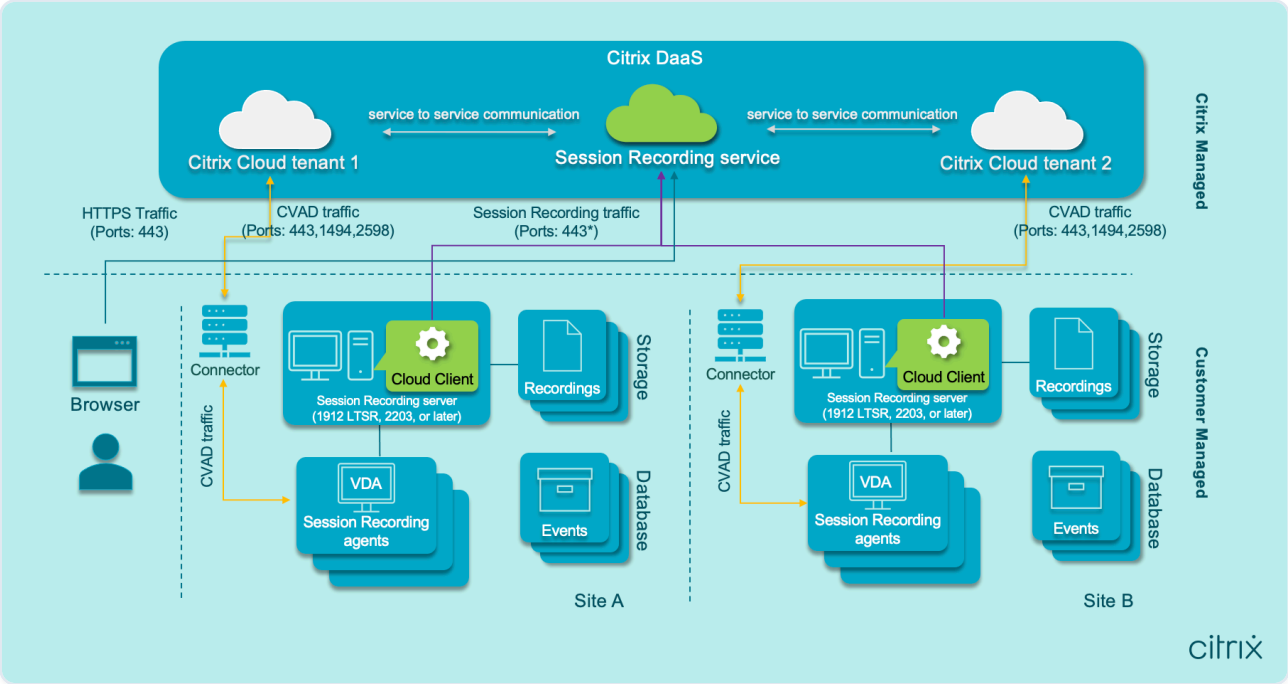
- The Session Recording service is available for provisioning in the Asia Pacific South (APS), EU, Japan, and US regions of Citrix Cloud. For more information, see Citrix Cloud Geographical Considerations.
- For information about the Session Recording service customer data storage, retention, and control, 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.



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:

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

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.

October 2026

Deep inspection in AI-powered insights

Session Recording now supports deep inspection in the security analysis of AI-powered insights. Administrators define behavior indicators — end-user activities such as unauthorized access or unusual file transfers — in a security prompt template, and the AI investigates each recording for those behaviors.

Key capabilities include:

- **Custom behavior indicators**: Describe the behaviors to detect in plain language, and the AI generates detection guides that you can review and refine.
- **Incident reporting**: Matches appear as incidents in the Deep inspection results section of the security analysis report, each with a clickable timestamp for playback.
- **Confidence tagging**: Incidents that are difficult to distinguish from normal activity are tagged Low confidence for manual review.

Deep inspection requires an AI model that supports reasoning.

For more information, see AI-powered insights for session recording.

August 2026

Session event data export as JSON

When administrators export a recording using the Session Recording Export console, Session Recording now generates a sidecar JSON file alongside the exported MP4, containing all detected session events.

For more information, see Session Recording file export.

Idle period detection in event detection policies

Session Recording now supports idle period detection as a configurable event type in event detection policies. Administrators can enable idle period detection directly in a policy to log periods of user inactivity within recorded sessions.

For more information, see Configure event detection policies.

April 2026

Playback scaling support in the web player

The Session Recording web player now supports playback scaling. This feature ensures that you can clearly view all session recordings directly in the web player, regardless of resolution differences between the recording source and your playback device.

Key capabilities include:

- Fit to Window: Scales the recorded session to fit your current browser window. This provides a complete overview of the session, allowing reviewers to quickly understand the overall operational context. High-quality resolution is provided by default.
- Original Size: Displays the recording at its native resolution. This mode is intended for detailed forensic analysis that requires the highest level of clarity and pixel-perfect detail.

For more information, see Open and play recordings.

March 2026

AI-powered insights for session recording

This new feature uses AI to analyze session recordings and provide actionable insights without manually reviewing hours of video.

Key capabilities:

- Insights dashboard for session activities
- Detailed reports for security and productivity analysis
- Customizable prompt templates for tailoring analysis to your business needs

For configuration details, see AI-powered insights for session recording.

December 2025

Session recording for endpoint devices (preview)

The Session Recording service can now configure to capture user actions on endpoint devices when accessing Citrix-delivered web apps, virtual apps and desktops. This capability, currently in preview, helps you monitor user actions on the endpoint itself.

For more information, refer to endpoint recording policies and Site settings.

September 2025

Enhanced visibility for session recording agents and servers

Session Recording service now provides enhanced visibility into your Session Recording agents and servers. Key updates include a comprehensive agent status overview on the dashboard, detailed agent information within site management, and the introduction of server geolocation. For more information, see the articles under Site and server settings and Management dashboard.

Session recording file export

Authorized administrators can now securely export session recordings to MP4 format. This feature is designed for critical use cases like digital evidence and compliance audits. Key capabilities include:

- Role-based access control to ensure only authorized users can export.

- Mandatory justifications for every export action.
- A complete audit trail for all export activities in the Playback Logging.

For more information, see Session recording file export.

June 2025

Interactive Demo Mode for exploring Session Recording

The Interactive Demo Mode for Session Recording allows administrators to explore and understand the functionalities of the session recording service without impacting real user data or requiring initial server setup. This feature provides a hands-on management experience using pre-generated or synthetic data, offering a risk-free environment to learn the service.

The Interactive Demo Mode offers a risk-free environment for administrators to:

- Navigate the management interface and become familiar with its layout.
- Observe how data is presented and how different features operate using sample data.
- Evaluate the service's suitability for their organization's needs before onboarding actual session recording servers.

For more information, see Interactive Demo Mode for exploring Session Recording

Enhanced Recording Playback Insights

The Session Recording service now offers enhanced insights into recording playback activity. This includes a new "Recording playback" statistical section on the management console's Dashboard, as well as the ability to view detailed playback history for individual recordings within the player.

These new capabilities help administrators better understand how session recordings are being utilized. Key benefits include:

- Quickly identify frequently accessed or critical recordings through the "Most played recordings" view.
- Understand the primary consumers of recordings via the "Top viewers" data.
- Audit playback activity for specific recordings directly within the player through a detailed history.

For more information, see the articles under Tips for using the dashboard and the Open and play recordings.

March 2025

Agent installation prompt on the welcome page

The Session Recording agent is essential for recording sessions and capturing detailed user activity. We've updated the Session Recording service welcome page to include a required agent installation prompt. Find it within the service or learn more here: Get-started guide

Support for multiple Azure AD identity provider instances

The Session Recording service now supports multiple Azure AD identity provider instances. When configuring policies and playback permissions, selecting Azure AD as the identity provider allows you to choose an instance from the drop-down list. For more information, see the articles under Configure policies and the Playback permissions.

Site-level user activity reporting to the cloud

Based on event detection in recorded sessions, Session Recording now empowers you to identify incidents from events. It also displays the event and incident data in the cloud for aggregation and analysis, providing a comprehensive view of user activity across an entire site.

This site-level reporting feature enables you to:

- Quickly filter incidents from events by category.
- Identify abnormal activity with greater efficiency.
- Gain a broader understanding of user activity patterns across your site.

> **Note:**

> The availability of the event data in the cloud is solely determined by the active event detection policy, and is independent of settings or Session Recording server versions. Therefore, if the active policy dictates event data, it will always be displayed in the cloud.

> The availability of the incident data in the cloud is governed by three factors: the active event detection policy, site-specific event data analysis settings, and incident library settings that identify incidents from events. Separately, Session Recording 2503 or later is required for incident identification and display in the cloud.

Incidents, like event data, are tagged within recordings, which simplifies searching and review during playback.

For more information, see Site-level user activity reporting.

November 2024

Session Recording service now available in the Japan region of Citrix Cloud™

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

Diagnostic logging

A new diagnostic logging view is now available in the cloud, providing enhanced visibility into issues detected on the VDAs.

Diagnostic logging is available and enabled by default with Session Recording version 2411 and later. For more information, see Diagnostic logging.

Capturing printing activities in recorded sessions is now generally available

You can capture printing activities that occur during recorded sessions, tagging them as events for easy search and playback. This feature, which captures the full path of printed files for enhanced context, was previewed in Session Recording 2407 and is now generally available in both the cloud and on-premises releases, starting with Session Recording version 2411. For more information, see Configure event detection policies.

Unified platform experience with Citrix DaaS™

We have redesigned the Session Recording service navigation pane to offer a unified platform experience with Citrix DaaS.

Tip:

To access the Session Recording service, scroll down in the DaaS navigation pane and locate **Session Recording** which is at the same level as the **Manage** menu. You can hover

> over and pin the **Session Recording** menu to the top **PINNED** section of the navigation pane for quick access.

Fixes

Automatic upgrades of the cloud client might fail if PROXYMODE was set to 2 for automatic proxy setup during the previous installation. This release resolves the issue, allowing successful automatic upgrades from this version onward. If your cloud client is not upgraded to the latest version, follow these steps to upgrade it manually:

1. Download the latest installer for the Session Recording cloud client by following the relevant step in Connect existing Session Recording servers to the cloud.
2. Run the following command to upgrade the Session Recording cloud client manually.

```
msiexec /i SRCloudClientServices.msi /l*v "C:
\tmp\srcloudclientupgrade.log" /qn+
```

July 2024

Deployment to Microsoft Azure is further simplified and enhanced

When creating and deploying a site through a host connection, you now have the option to create private endpoints for storage and databases, and to create an Azure load balancer with the internal type.

For more information, see Deploy Session Recording resources to a cloud subscription.

Hide specific applications during screen recording

This feature requires that you select **Enable lossy screen recording**. It lets you hide specific applications with a layer mask during screen recording. The color for the layer mask is configurable, which can be Black, Gray, or White.

Explicit user consent before recording sessions

If the active recording policy records sessions with notifications, users receive recording notifications after typing credentials. This feature forces end users to explicitly consent to the session recording disclaimer before they can continue with their session. If end users accept the

disclaimer, their session continues with session recording enabled. If end users deny the disclaimer, their session is terminated.

To enable this feature, configure Session Recording Server settings. For more information, see Site and server settings.

Capture printing activities in recorded sessions (preview)

We have extended the scope of event detection to monitor printing activities that occur during recorded sessions and tag the printing activities as events in recordings for later search and playback.

To use this feature, make sure that:

- You have configured and activated a session recording policy that specifies sessions to record. For more information, see Configure session recording policies.
- You have created an event detection policy and selected the **Printing** option when specifying events to log. For more information, see Configure event detection policies.

> **Note:**
>
> This is a preview feature. It is available with Session Recording version 2407 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.

Fixes

Error 8632 might be raised when you archive or delete recordings.

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.
- 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 (").

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.
- Viewing the Session Recording management dashboard causes high CPU utilization on the database machine.
- Custom policies aren't available for a site containing the Session Recording server 1912.

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.

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.

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.
- 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.
- Attempts to edit policy rules that have a Japanese name fail.

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\CloudClientService\BlockSizeMultipl
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

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

- 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:

  a. Remove the cloud client package (`SRCloudClientService.msi`) from the Session Recording server.

  b. 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**.

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

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

  > **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.

- Accounts created in 2025 may be unable to use the **Generate Command** button. If the automatic generation fails, assemble the installation command manually by applying your client ID and secrets from secure client or service principal.

Get started

This section provides instructions for you to:

- Plan your deployment
- Get-started guide
- Connect existing Session Recording servers to the cloud
- Install Session Recording servers from within the cloud
- Deploy Session Recording resources to a cloud subscriptions
- Schedule cloud client upgrades

Plan your deployment

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)

FULL URL ADDRESSES
srs.apps.cloud.com
srs-eu.apps.cloud.com
srs-ap-s.apps.cloud.com

SESSION RECORDING SERVICE
FULL URL ADDRESSES
srs-a.apps.cloud.com
srs-b.apps.cloud.com
srs-eu-a.apps.cloud.com
srs-eu-b.apps.cloud.com
srs-ap-s-a.pps.cloud.com
srs-ap-s-b.apps.cloud.com
trust.citrixworkspacesapi.net
trust-us.citrixworkspacesapi.net
trust-eu.citrixworkspacesapi.net
core.citrixworkspacesapi.net
produssrcloudclient.blob.core.windows.net

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:

SESSION RECORDING SERVICE

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

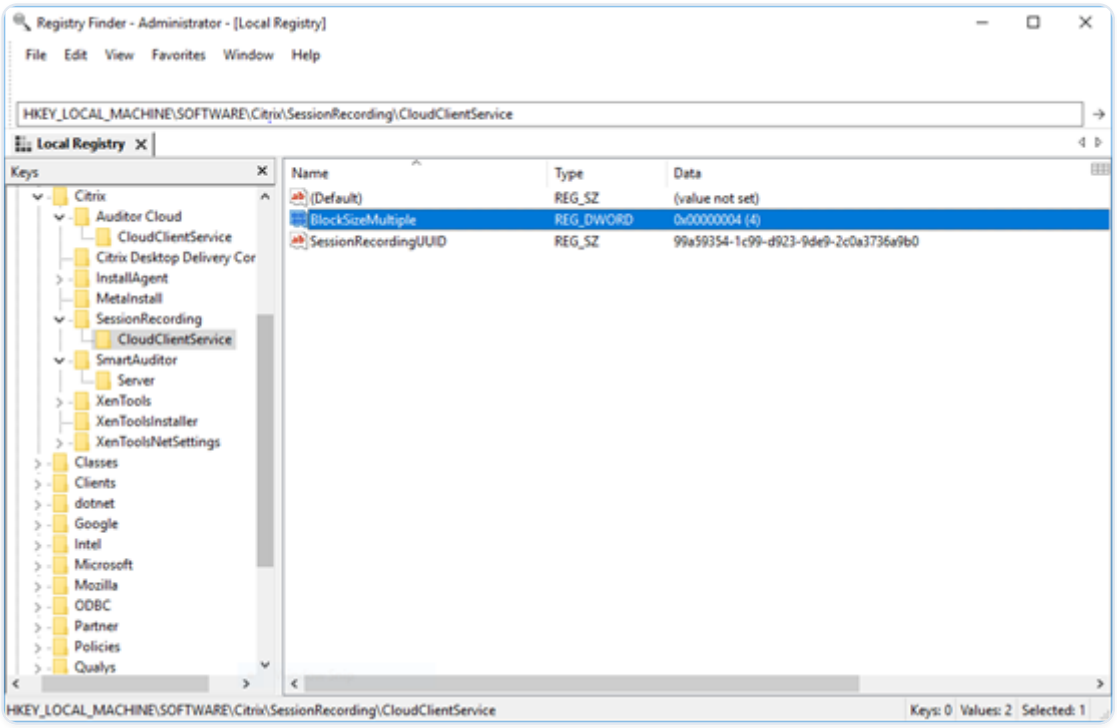
Proxy

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\BlockSizeMultipl**
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:

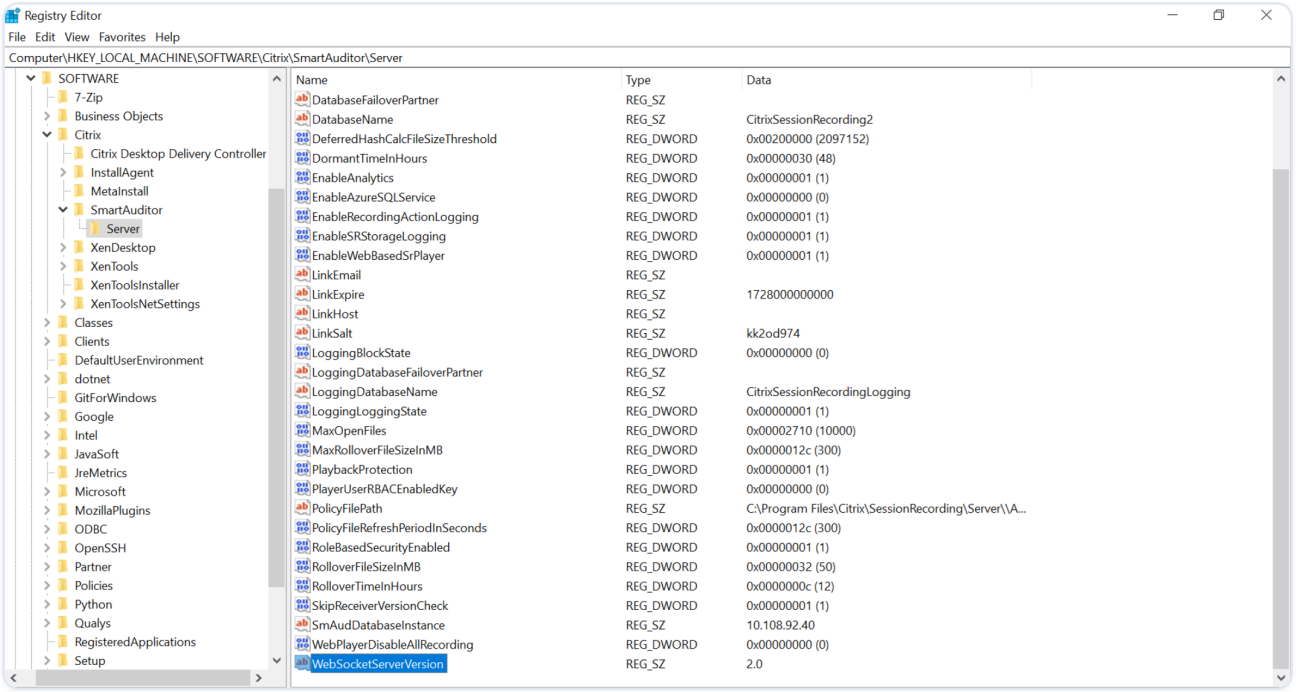
- The Session Recording servers can connect to Citrix Cloud properly.
- You can use HTTPS to access the player.

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`.



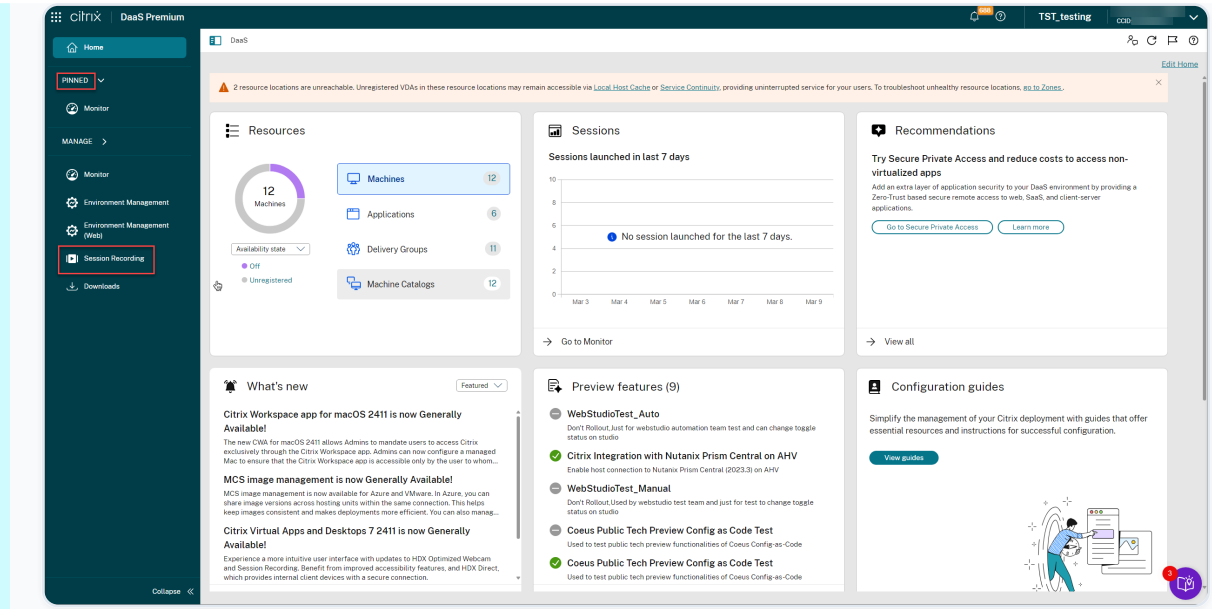
An upgrade installation from an earlier version to Session Recording 2103 and later connects your web browser to the Python-based web streaming service (version 1.0). To connect to the web streaming service hosted in IIS, run the `<Session Recording Server installation path>\Bin\SsRecUtils.exe -enablestreamingservice` command.

Get-started guide

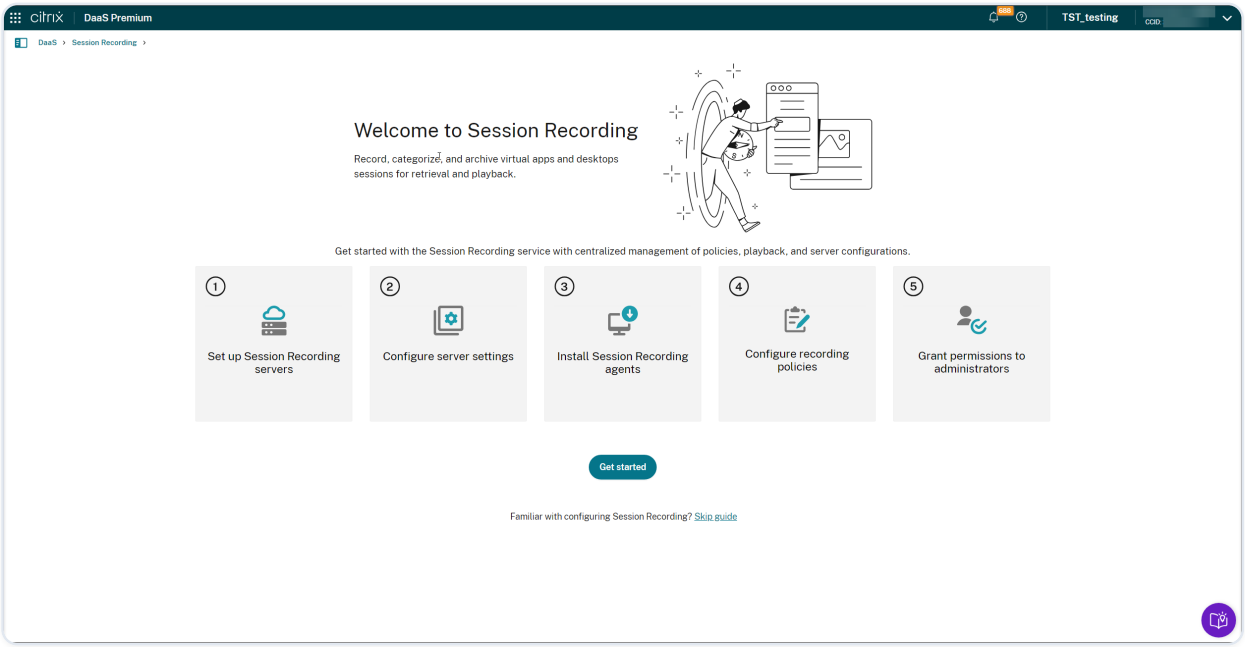
The get-started guide outlines the necessary procedures for new and experienced administrators to deploy and use the Session Recording service.

1. Access the Session Recording service hosted in Citrix DaaS.

> **Tip:**
>
> To access the Session Recording service, scroll down in the DaaS navigation pane and locate **Session Recording** which is at the same level as the **Manage** menu. You can hover over and pin the **Session Recording** menu to the top **PINNED** section of the navigation pane for quick access.

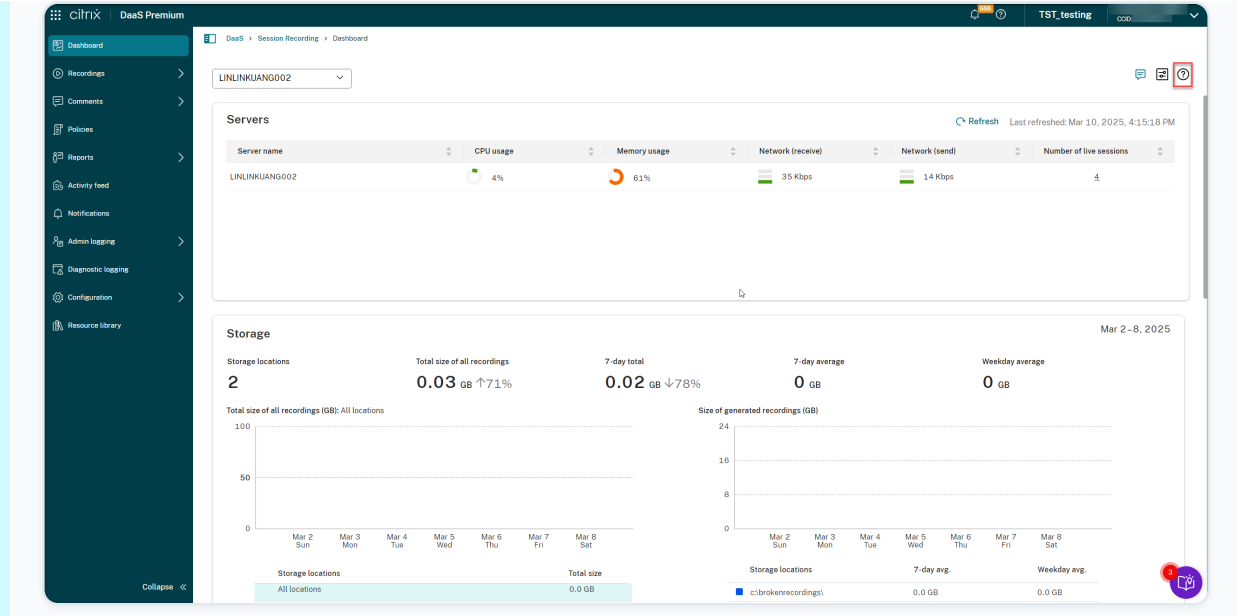


The Session Recording service displays its welcome page.

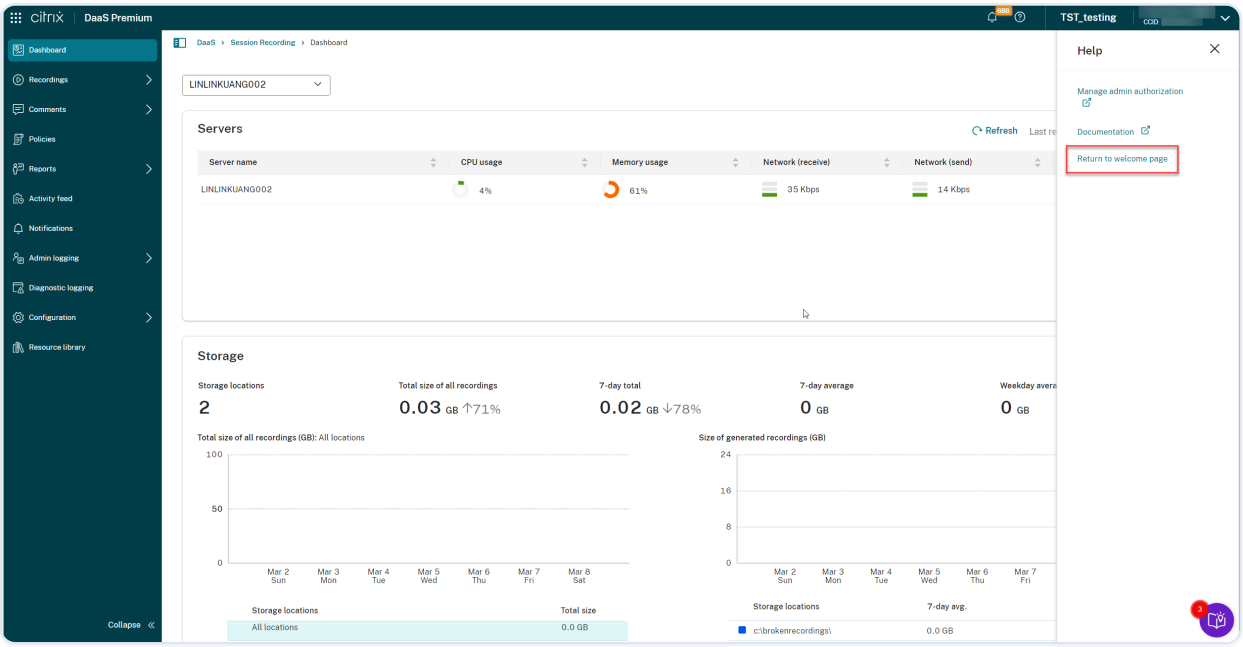


Tip:

You can also access the welcome page by clicking the question mark icon (?) in the upper right corner of any Session Recording service page. For example, see the following screen capture:

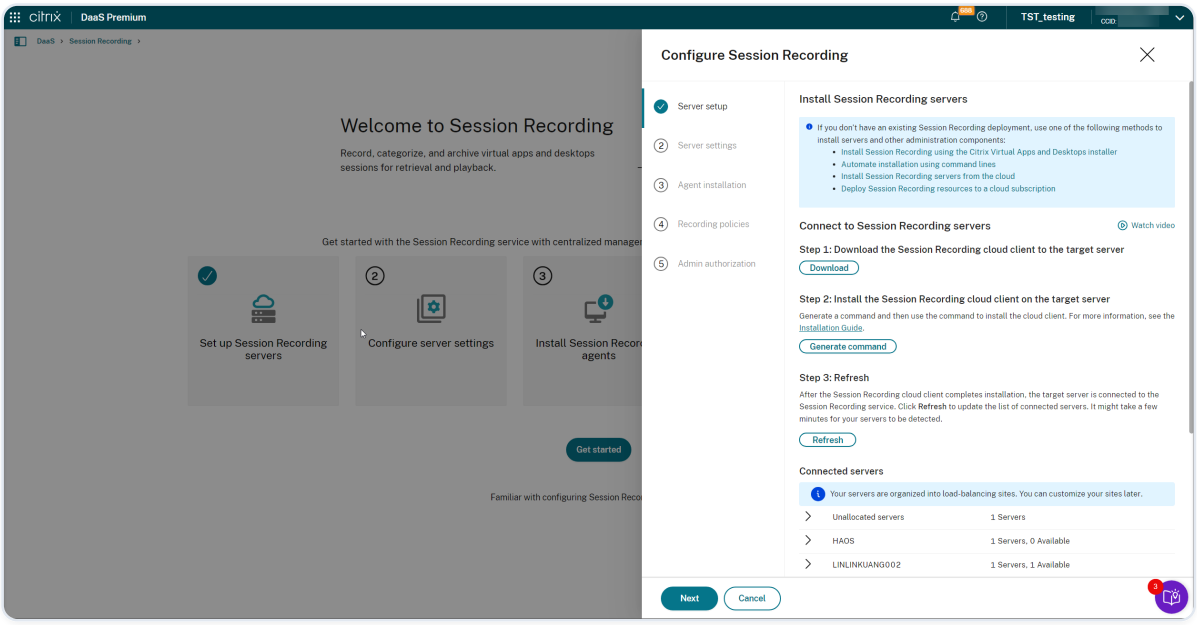


Clicking the question mark icon (?) makes the **Return to welcome page** option available.

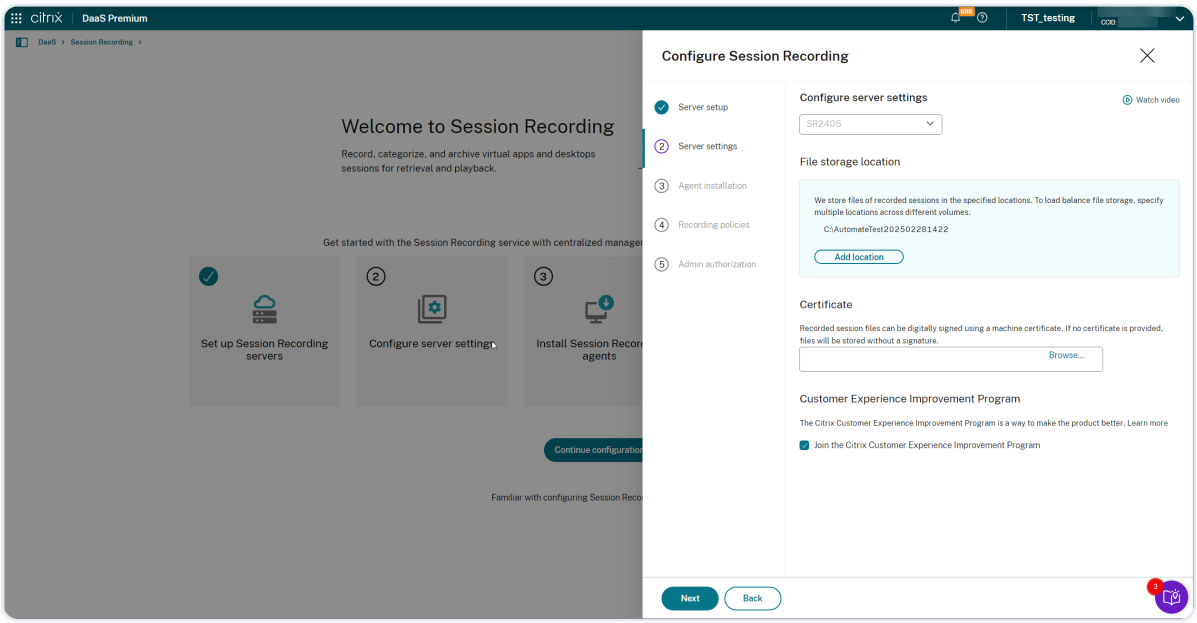


2. On the welcome page, review the Session Recording service's deployment and usage procedures. If you've already installed the Session Recording server and agent and are familiar with the configuration, click **Skip guide** to go directly to the service pages for setup. Otherwise, click **Get started** to begin deployment.
3. (Optional) Follow the wizard to complete the getting started procedures.

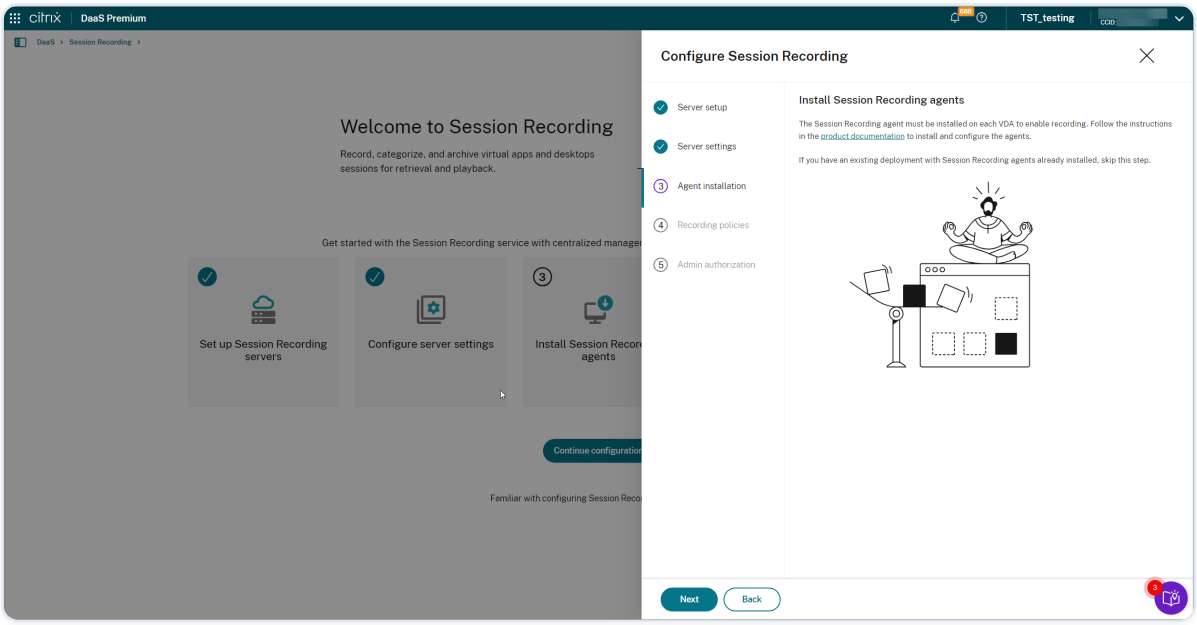
    a. **Server setup**: This page guides you through installing the Session Recording server and connecting it to the cloud by downloading and installing the cloud client on it.



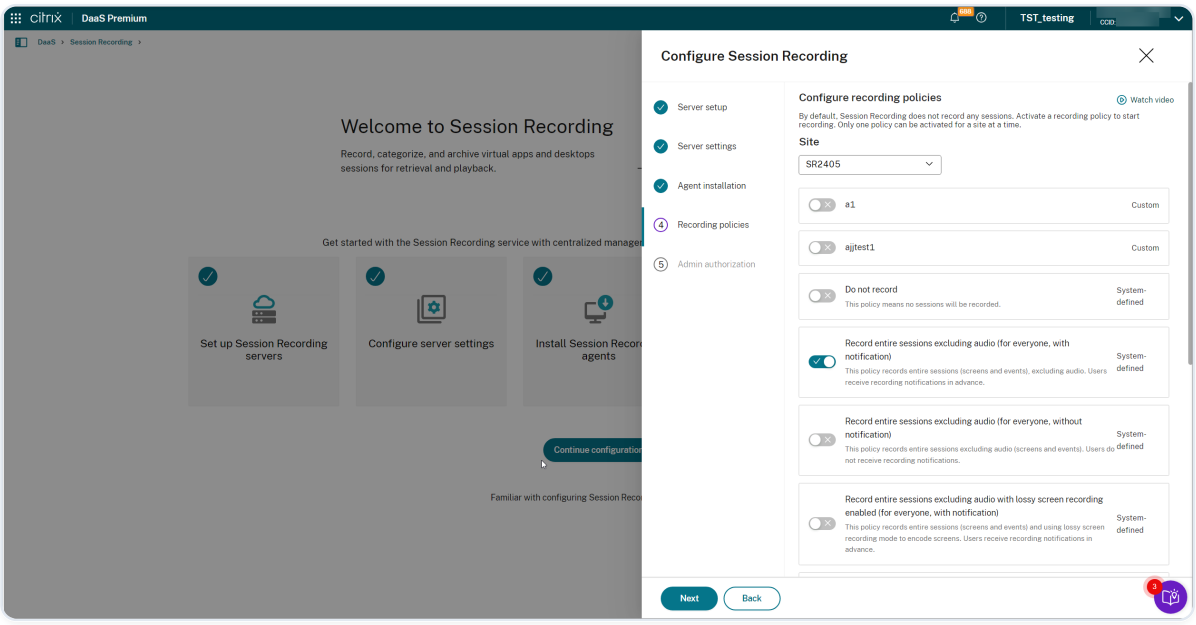
b. **Server settings**: This page displays essential server settings for using the service. More settings can be configured later, as detailed in Server settings.



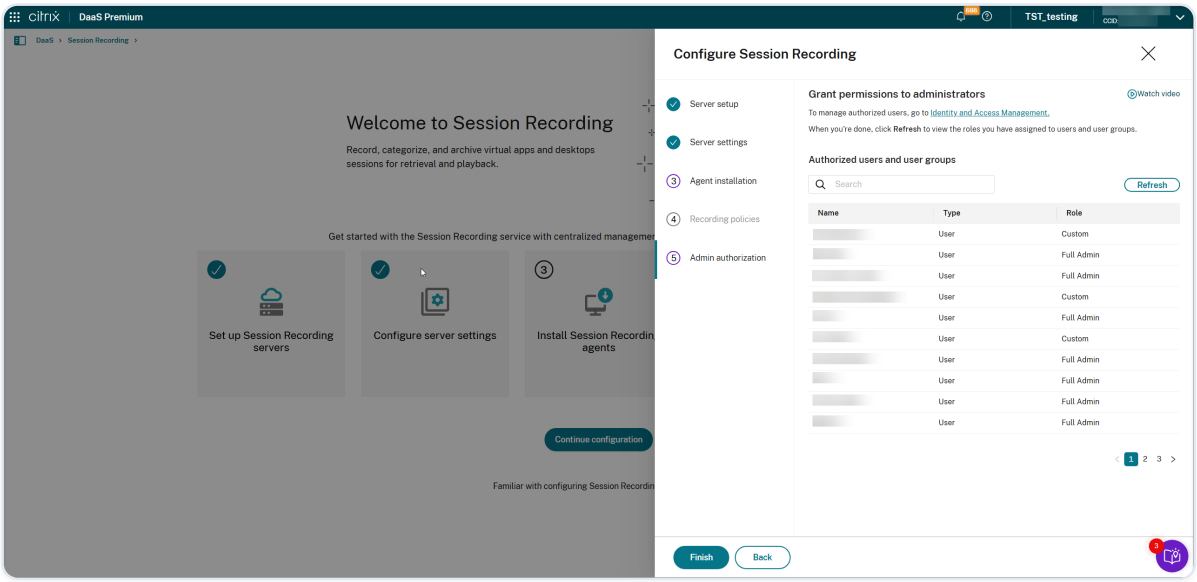
c. **Agent installation**: This agent installation prompt reminds you that the Session Recording agent, which is essential for recording sessions and capturing detailed user activity, must be installed. Install it on each target VDA to record hosted sessions.



d. **Recording policies**: Activate a recording policy to enable session recording on a specific site. The policy you activate applies to all Session Recording servers of the site. For policy configuration details, see the Configure policies chapter.



e. **Admin authorization**: This page reminds you to assign permissions to administrators. For more information, see Administrator permissions.



Connect existing Session Recording servers to the cloud

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.

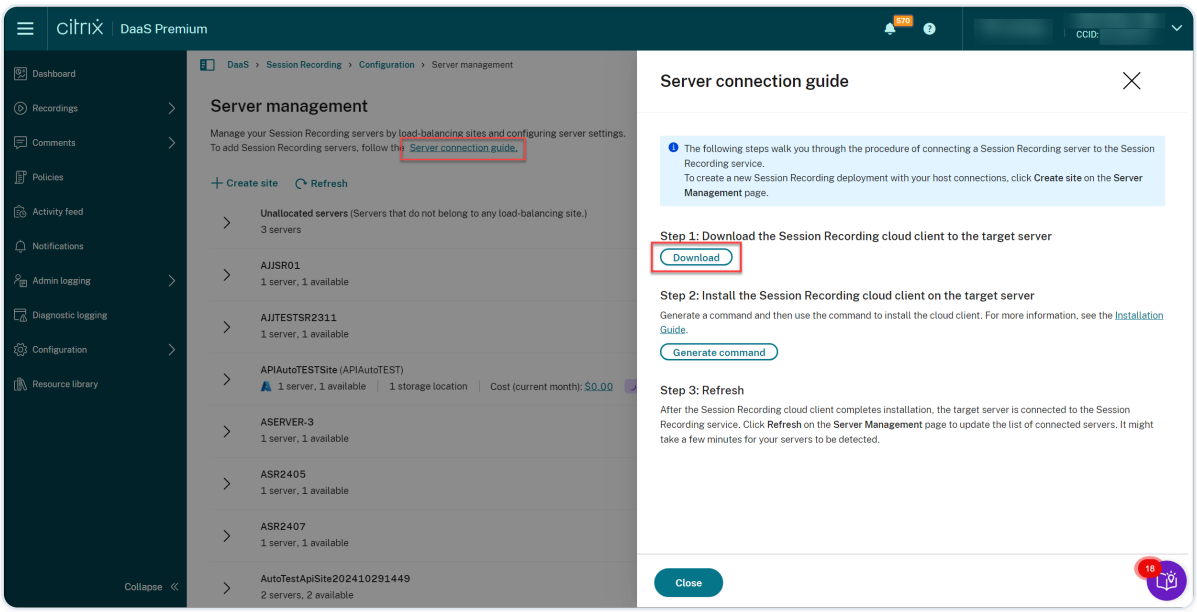
   a. Sign in to Citrix Cloud.

   b. In the upper left menu, select **My Services > DaaS**.

   c. In the DaaS tile, scroll down in the left navigation pane and select **Session Recording**. You can hover over and pin the **Session Recording** menu to the top **PINNED** section of the navigation pane for quick access. You can reorder pinned menus by dragging them to the desired places.

   d. In the Session Recording service view, select **Configuration > Server Management** from the left navigation.

   e. Click **Download** on the **Server connection guide** page.

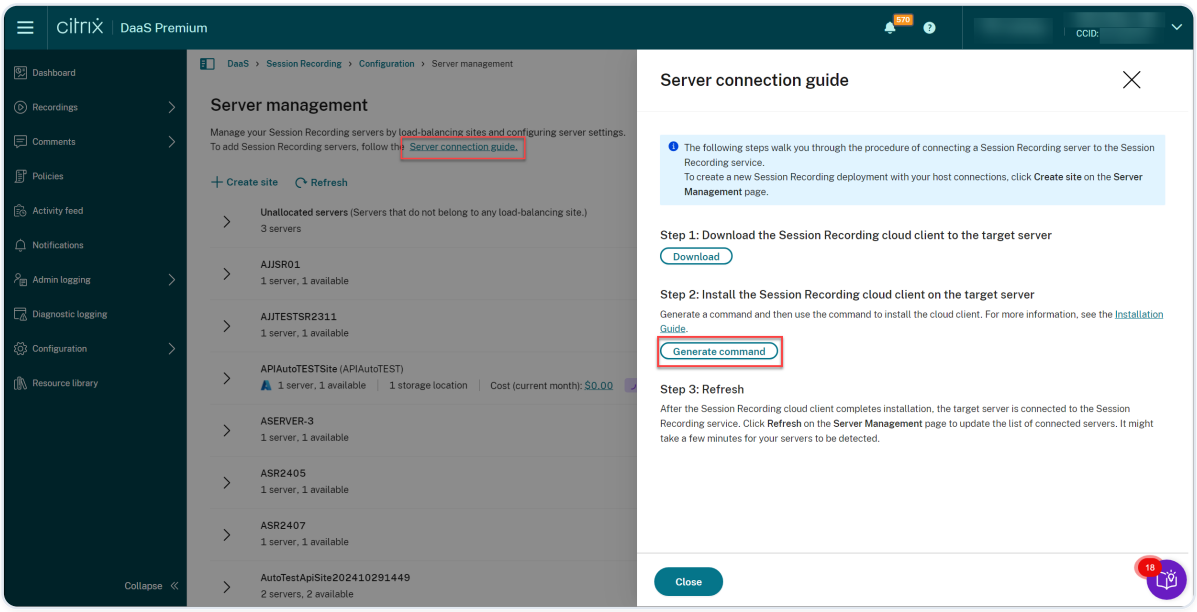


> **Tip:**

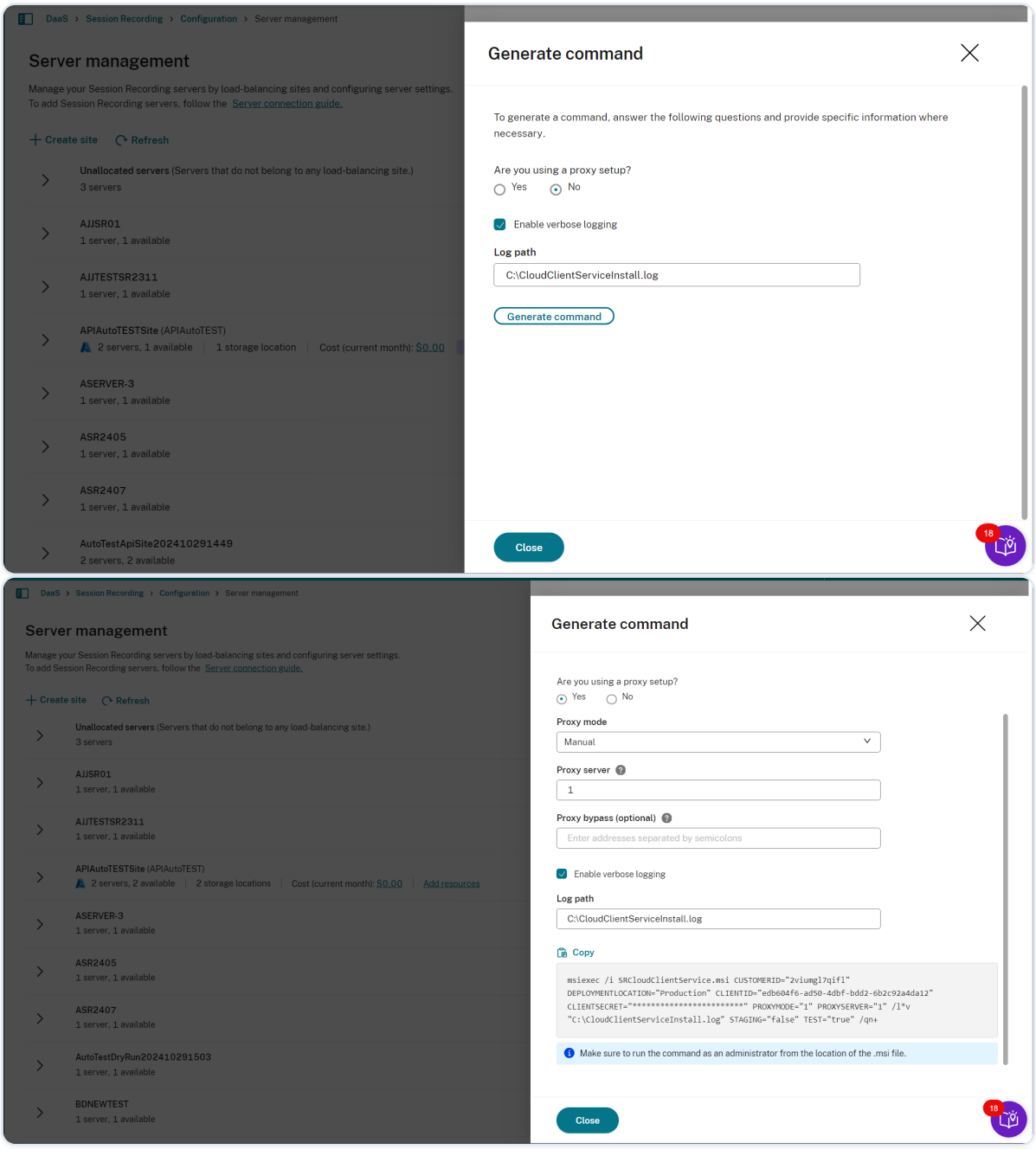
- The **Generate command** button for cloud client installation is unavailable for the administrators that are added through Azure AD groups.
- You can also access the **Download** and **Generate command** buttons by clicking **Continue configuration** on the Session Recording service **welcome** page:

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:

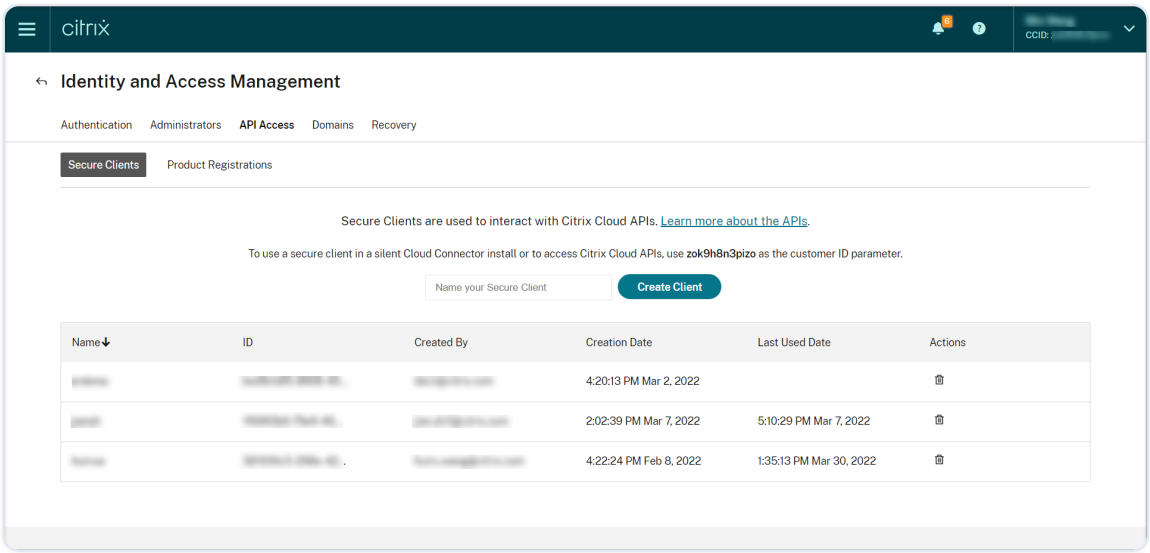
```
msiexec /i SRCloudClientService.msi CUSTOMERID="2viumgl7qifl"
DEPLOYMENTLOCATION="Production" CLIENTID="edb604f6-ad50-4dbf-
bdd2-6b2c92a4da12" CLIENTSECRET="yPj5zU_BVuo3Od2eZTHaCw=="
PROXYMODE="1" PROXYSERVER="1" /l*v "C:
\CloudClientServiceInstall.log" STAGING="false" TEST="true" /qn+
```

Where:

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

  > **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:



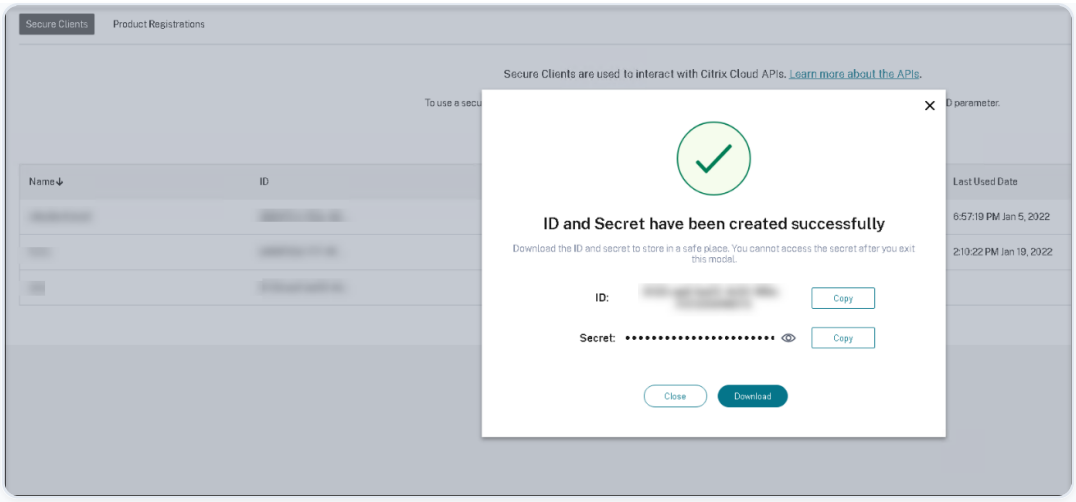
- **CLIENTID** is a ***required*** parameter. The secure client ID is a Universally Unique Identifier (UUID) automatically generated when you create the secure client. Secure clients are used to interact with Citrix Cloud APIs.
- **CLIENTSECRET** is a ***required*** parameter. The secure client secret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

Note:

You need the secure client ID and secure client secret of the secure principal that will be used to install the Session Recording Cloud Client.

To obtain these values, you must first create a secure principal in Citrix Cloud.

Ensure that the secure principal is created with Full Access permissions.



- **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>`.
- **/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

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.

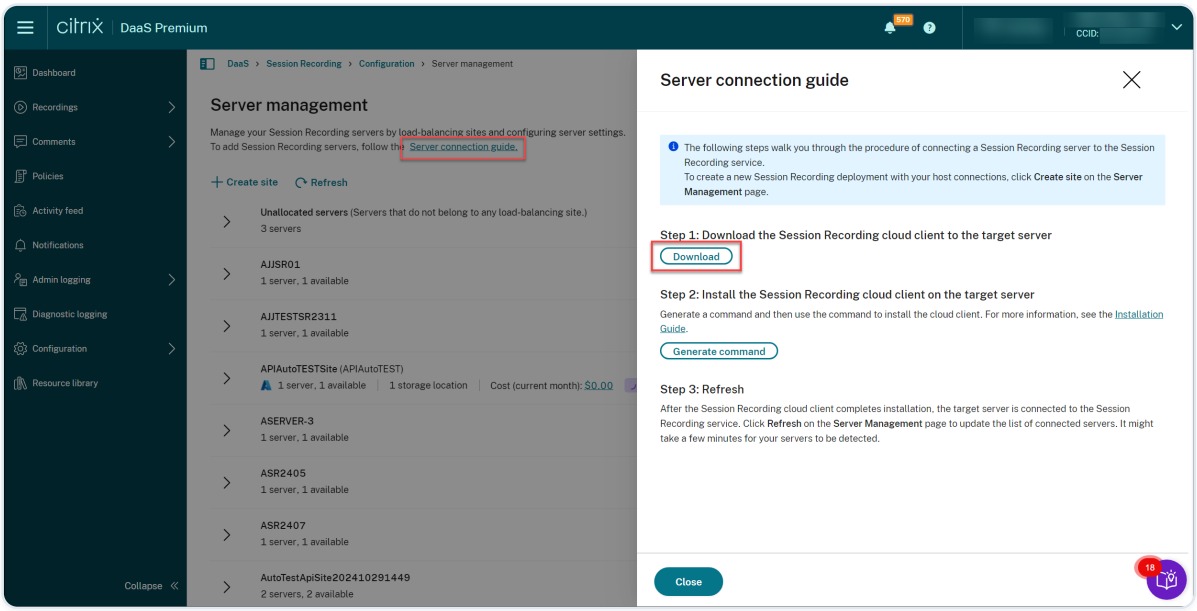
Installation steps

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. In the DaaS tile, scroll down in the left navigation pane and select **Session Recording**. You can hover over and pin the **Session Recording** menu to the top **PINNED** section of the navigation pane for quick access. You can reorder pinned menus by dragging them to the desired places.
    d. In the Session Recording service view, select **Configuration > Server Management** from the left navigation.
    e. Click **Download** on the **Server connection guide** page.

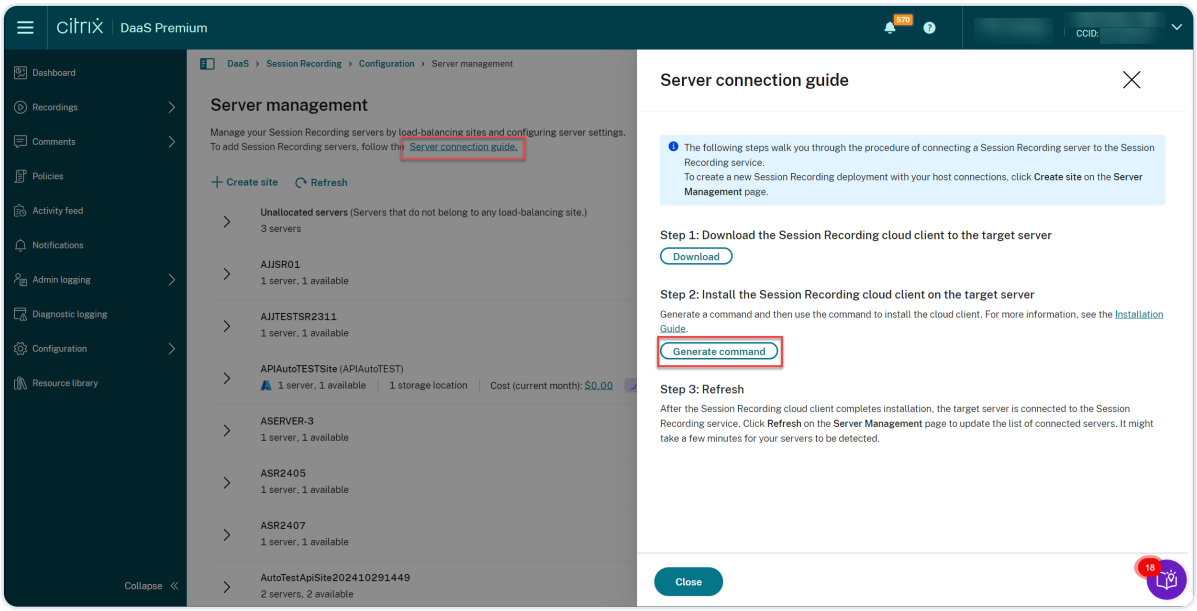


Tip:

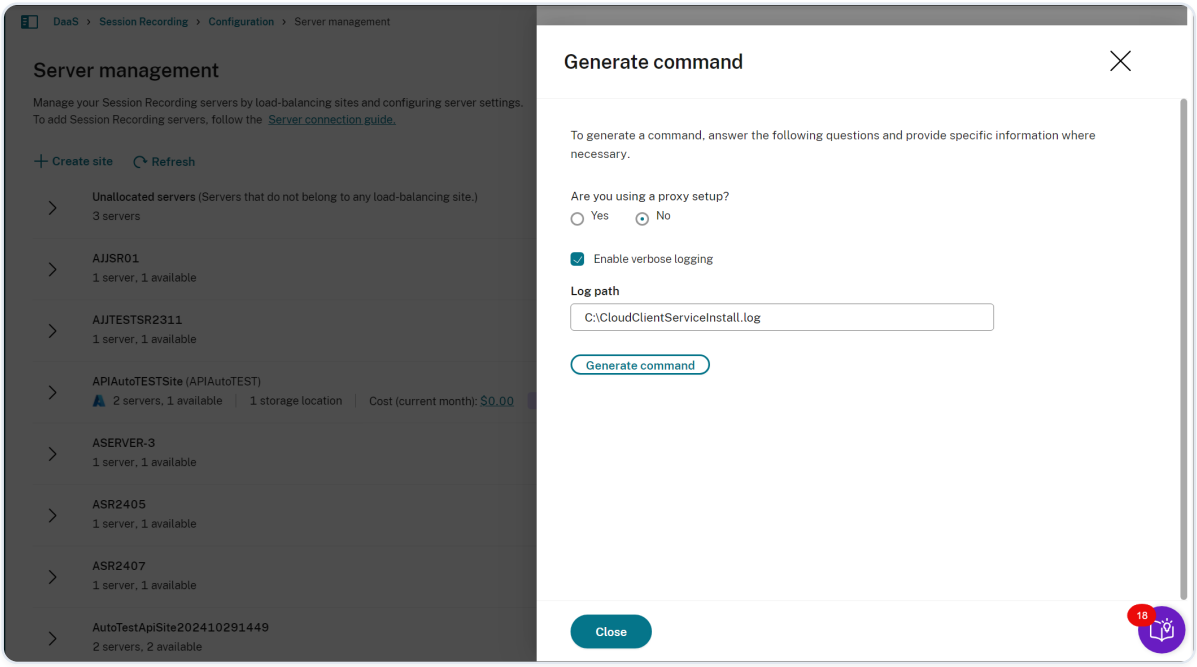
- The **Generate command** button for cloud client installation is unavailable for the administrators that are added through Azure AD groups.
- You can also access the **Download** and **Generate command** buttons by clicking **Continue configuration** on the Session Recording service **welcome** page:

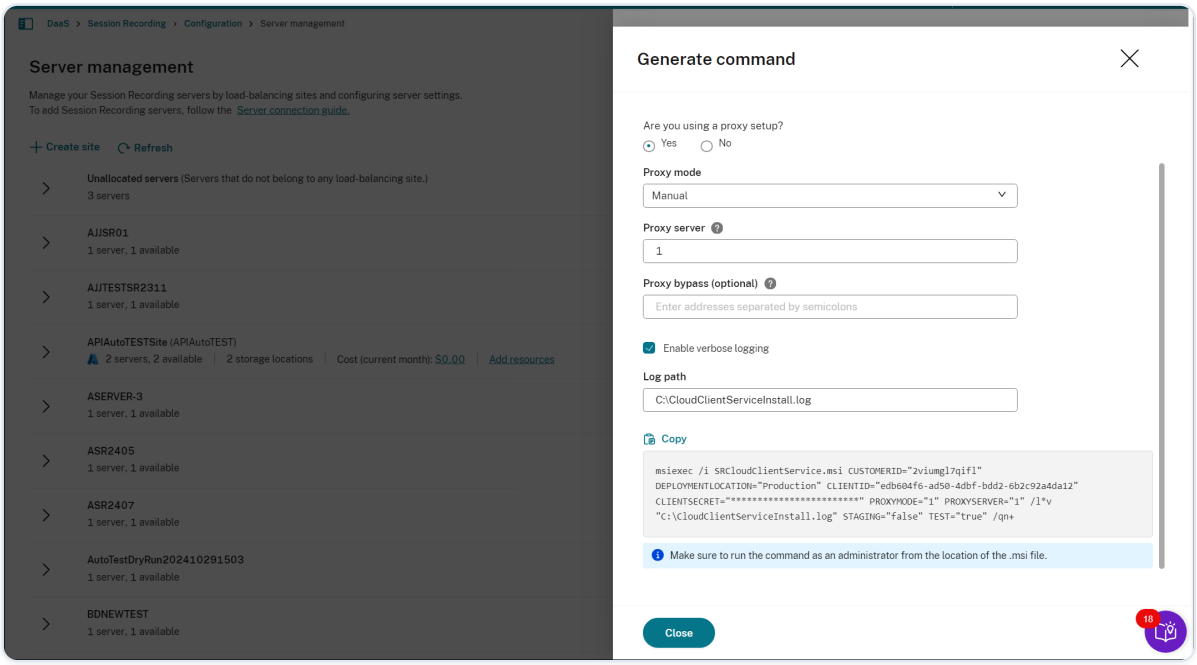
f. Install the cloud client on the machine. To do that, run a command as an administrator from the location of the cloud client .msi file that you downloaded earlier.

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



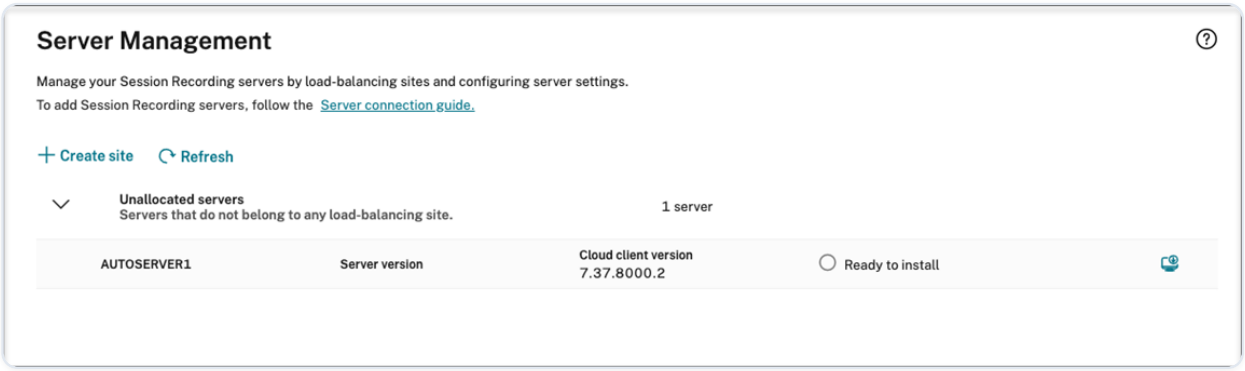
Answer questions and provide information where necessary on the **Generate command** page. After that, click the **Generate command** button.



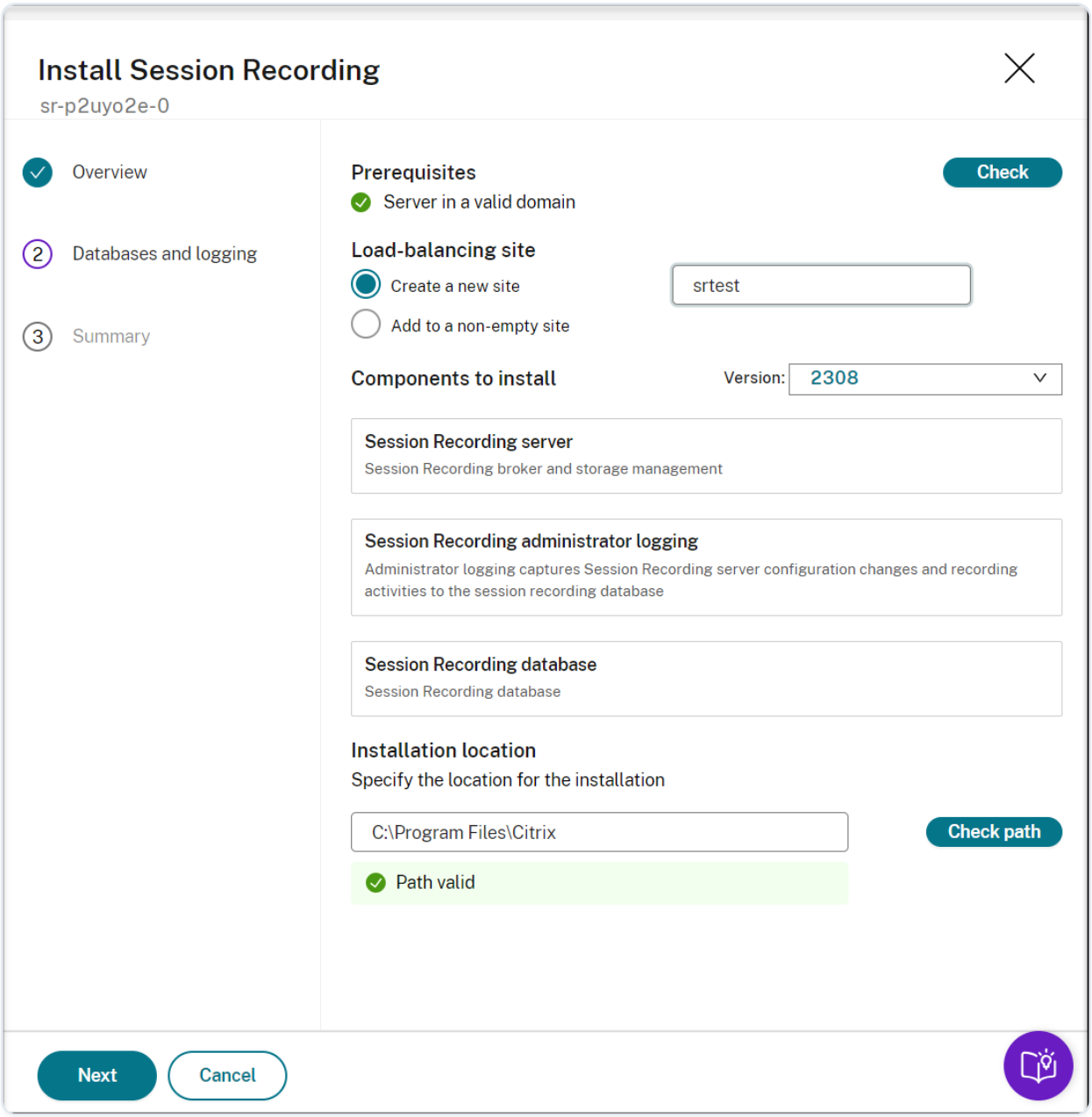


If you modify the answers or provide different information after clicking the **Generate command** button, the generated command automatically updates accordingly. The **Generate command** button is available again after you sign out and sign back in to Citrix Cloud.

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.

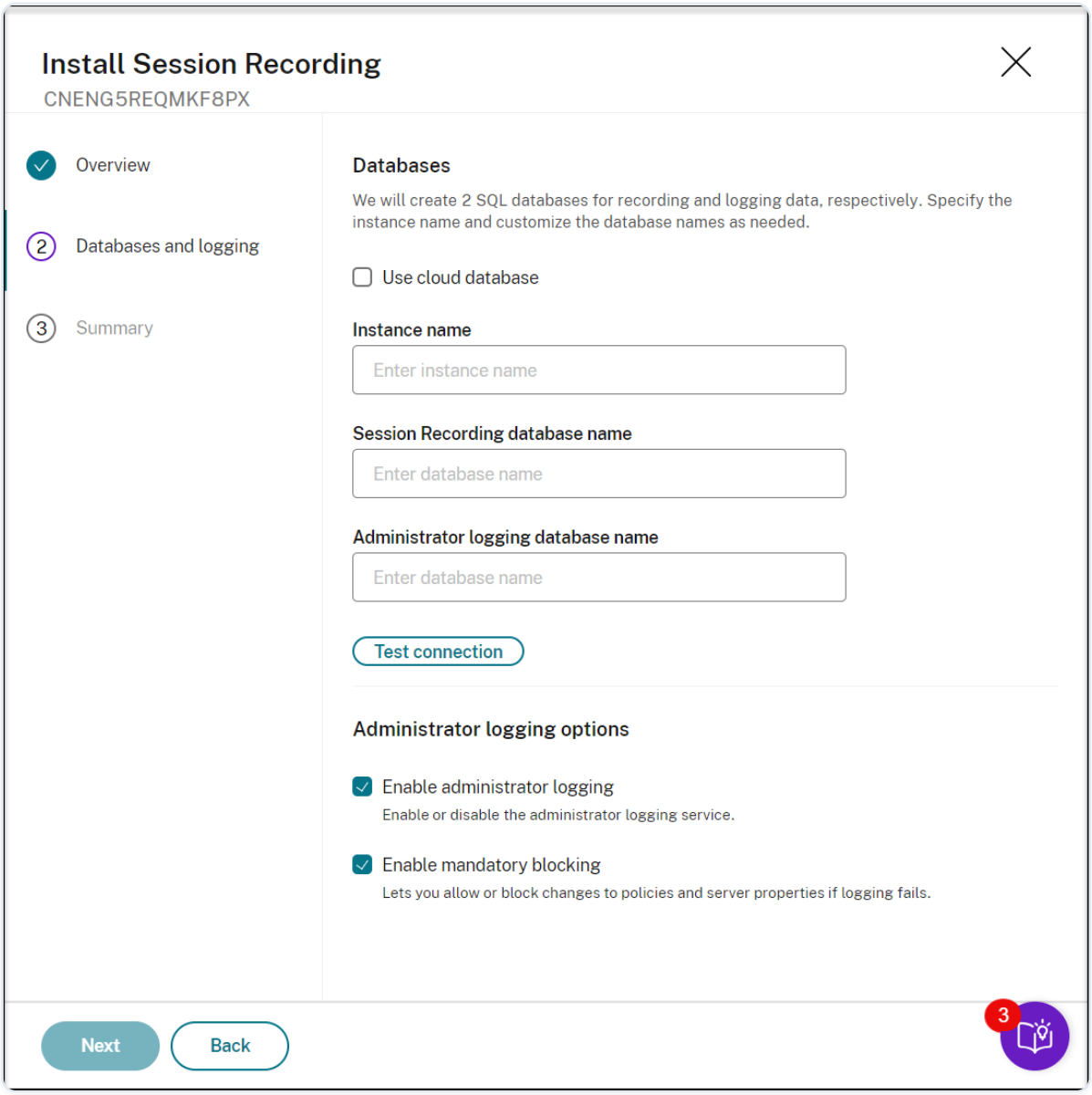
   ii. Create a site for the machine or add the machine to an existing non-empty site.

   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.

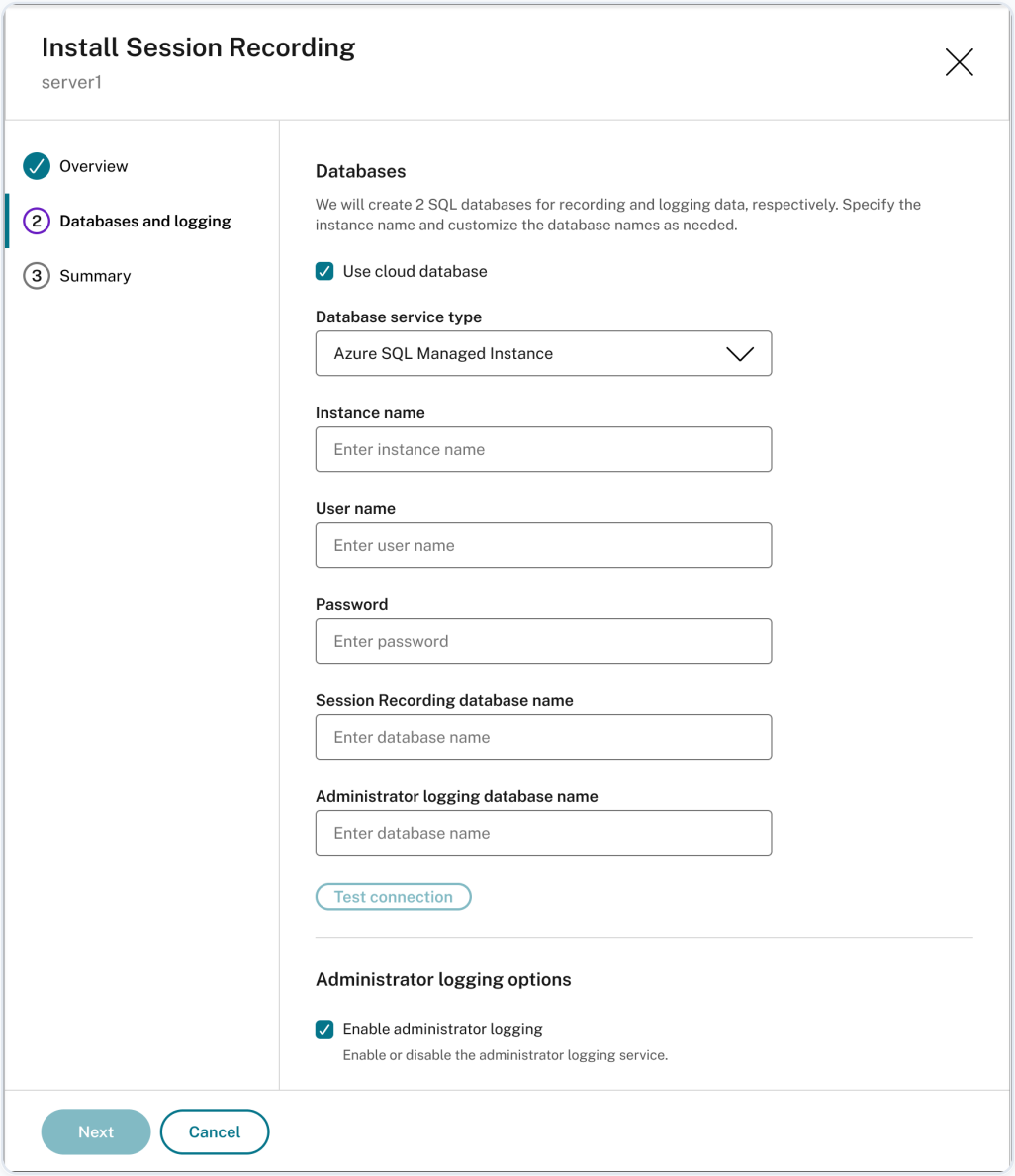
b. On the **Databases** page, choose whether to use a cloud database, fill the fields accordingly, and then click **Test connection** to test the connectivity to the Session Recording database and the administrator logging database.



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. If the Session Recording server and the database instance are installed on different machines, grant the **sysadmin** role permission on the database to the machine where the Session Recording server is installed. If both the Session Recording server and the database instance are installed on the same machine, grant the **sysadmin** role permission on the database to the machine where the Session Recording server is installed and to the NT AUTHORITY\NETWORK SERVICE and NT AUTHORITY\SYSTEM accounts. 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.

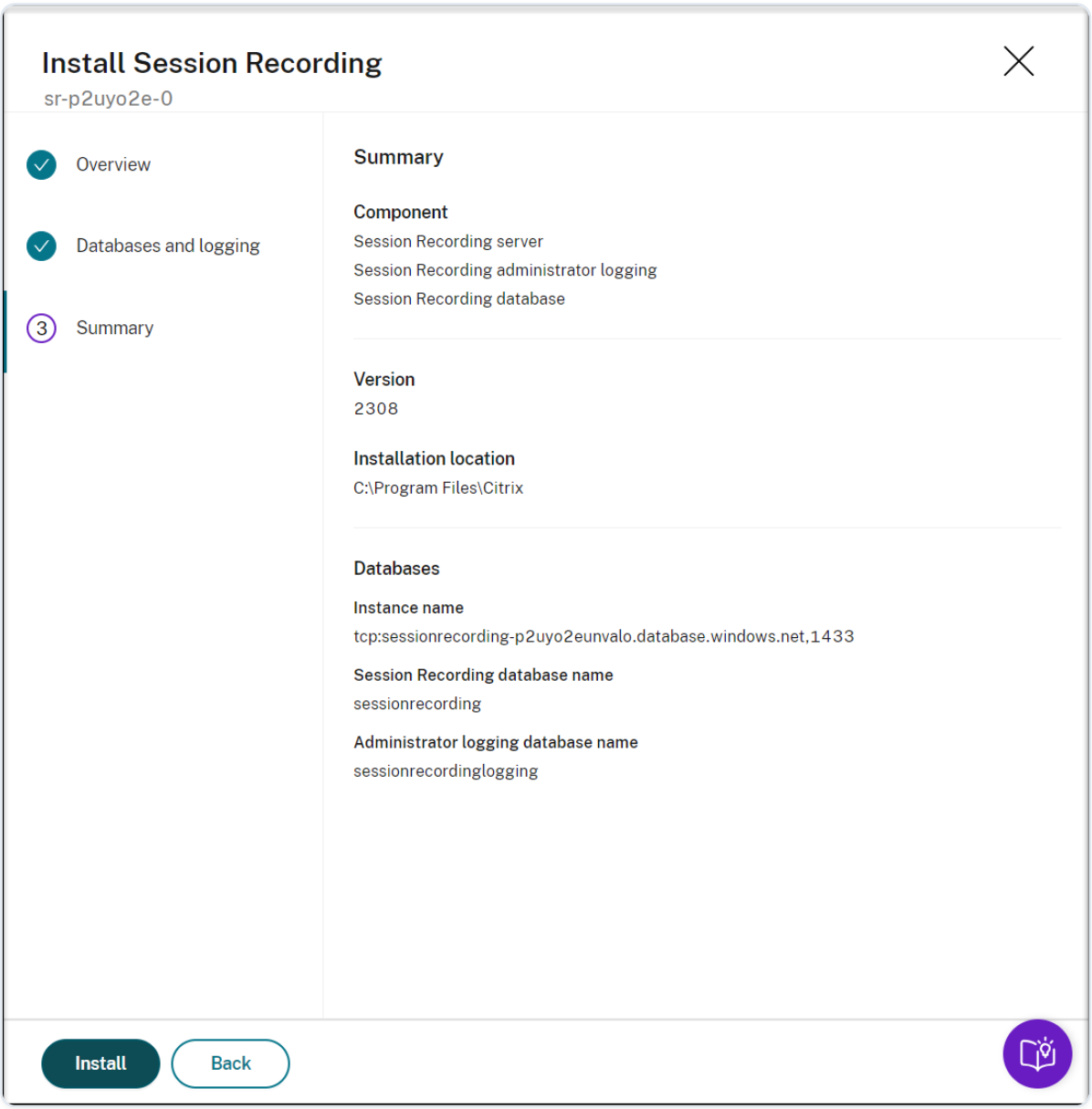
Session Recording now supports different types of sql authentication, please refer to the following table for details:

SUPPORTED SQL AUTHENTICATION METHOD	SUPPORTED SQL SERVER TYPE
SQL Server Authentication	- On-Premises SQL Server
	- Azure SQL Database
	- Azure SQL Managed Instance
	- SQL Server on Azure VMs
	- AWS RDS
	- Google Cloud SQL Server

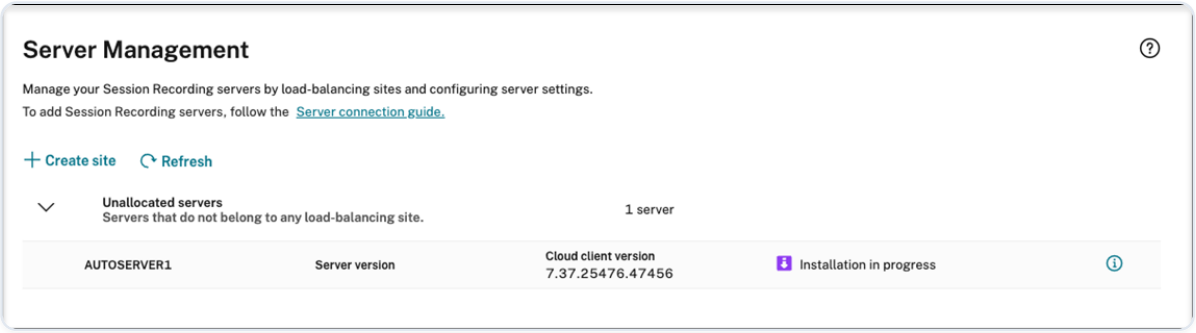
SUPPORTED SQL AUTHENTICATION METHOD	SUPPORTED SQL SERVER TYPE
Microsoft Entra ID Password Authentication with Cloud Managed Entra id account	- Azure SQL Database
	- Azure SQL Managed Instance
Microsoft Entra ID Service Principal Authentication with Cloud Managed Entra id account	Azure SQL Managed Instance
Azure managed identity	- Azure SQL Database
	- Azure SQL Managed Instance

> **Note:**
>
> Need to install OLE DB Driver and ODBC Driver on the same machine as the cloud client.

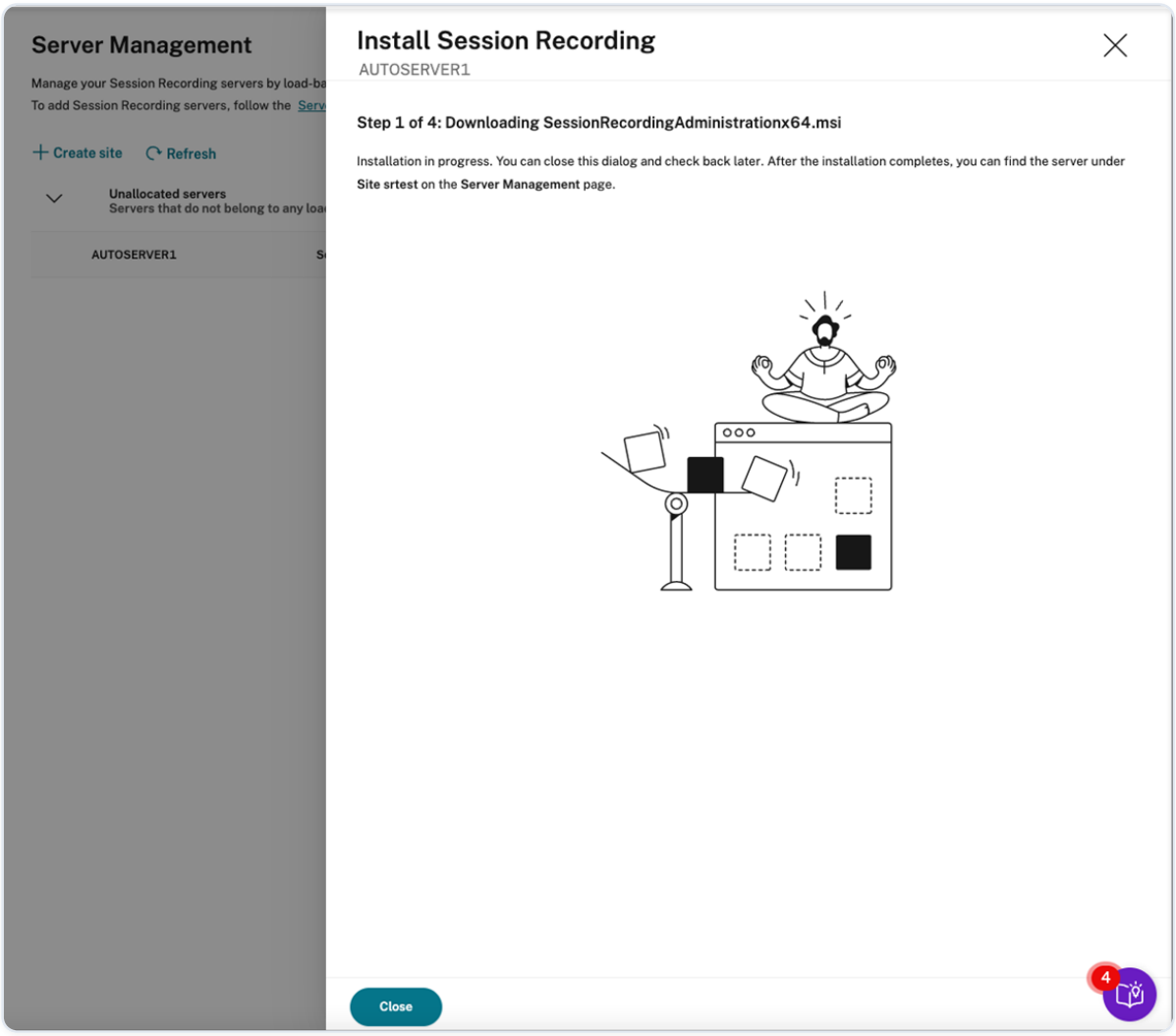
c. On the **Summary** page, verify your settings and click **Install**.



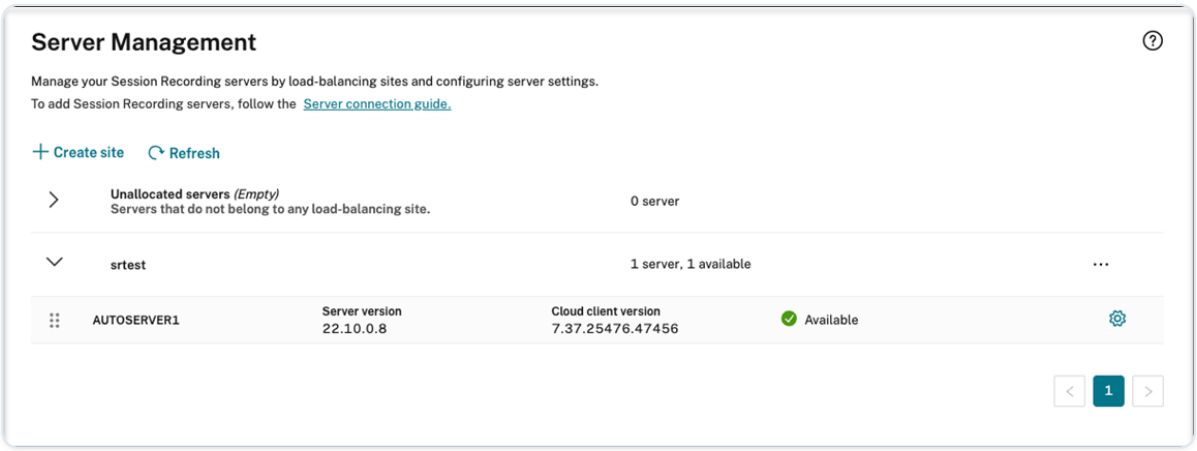
d. Check the installation progress by clicking the icon next to **Installation in progress**.



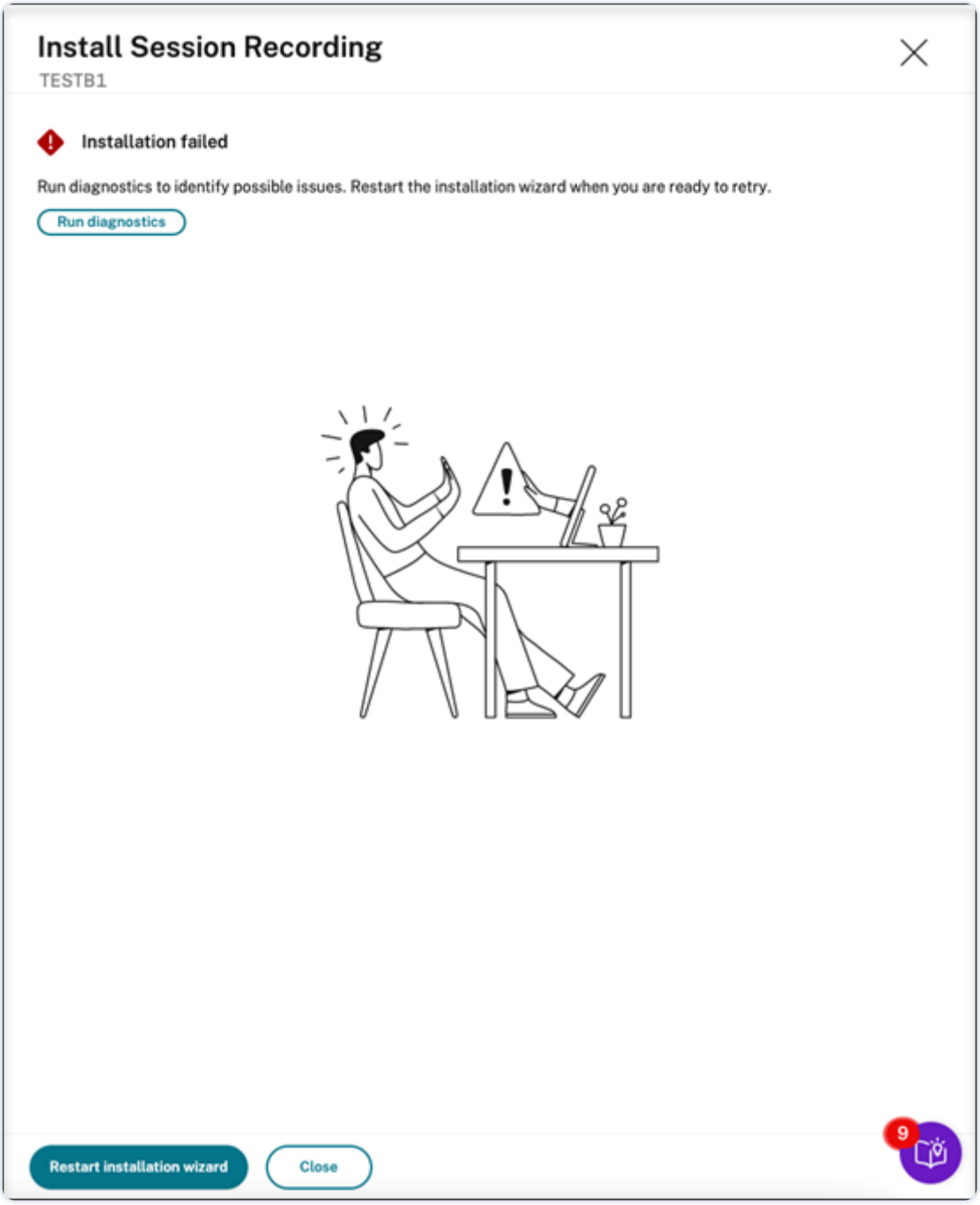
For example, the installation has progressed to the first step.



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

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:

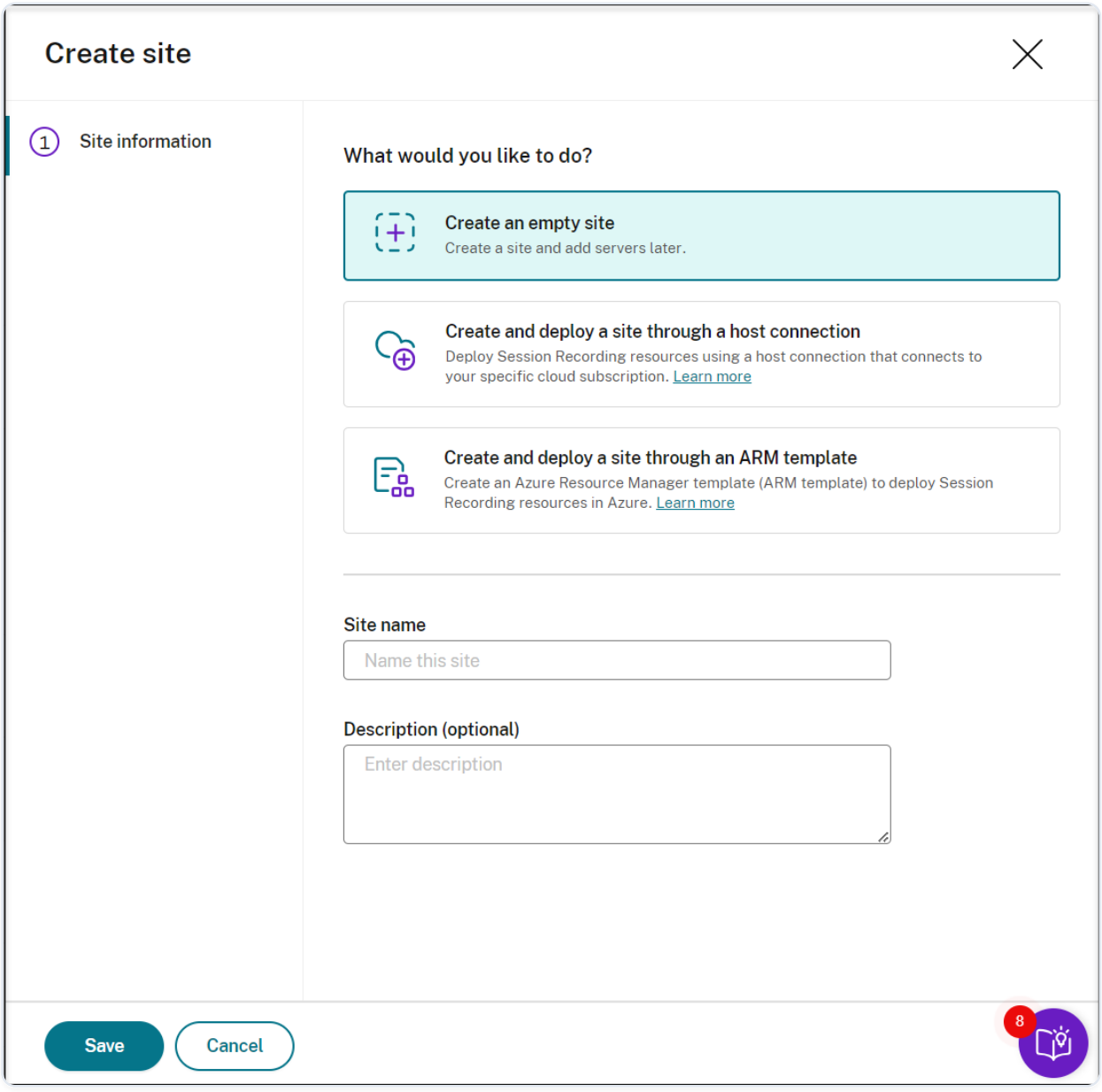
- Add resources to an existing site deployed on Azure
- Change the IP addresses that are allowed to access the load balancer
- View actual costs for using Azure

Create and deploy a site through a host connection

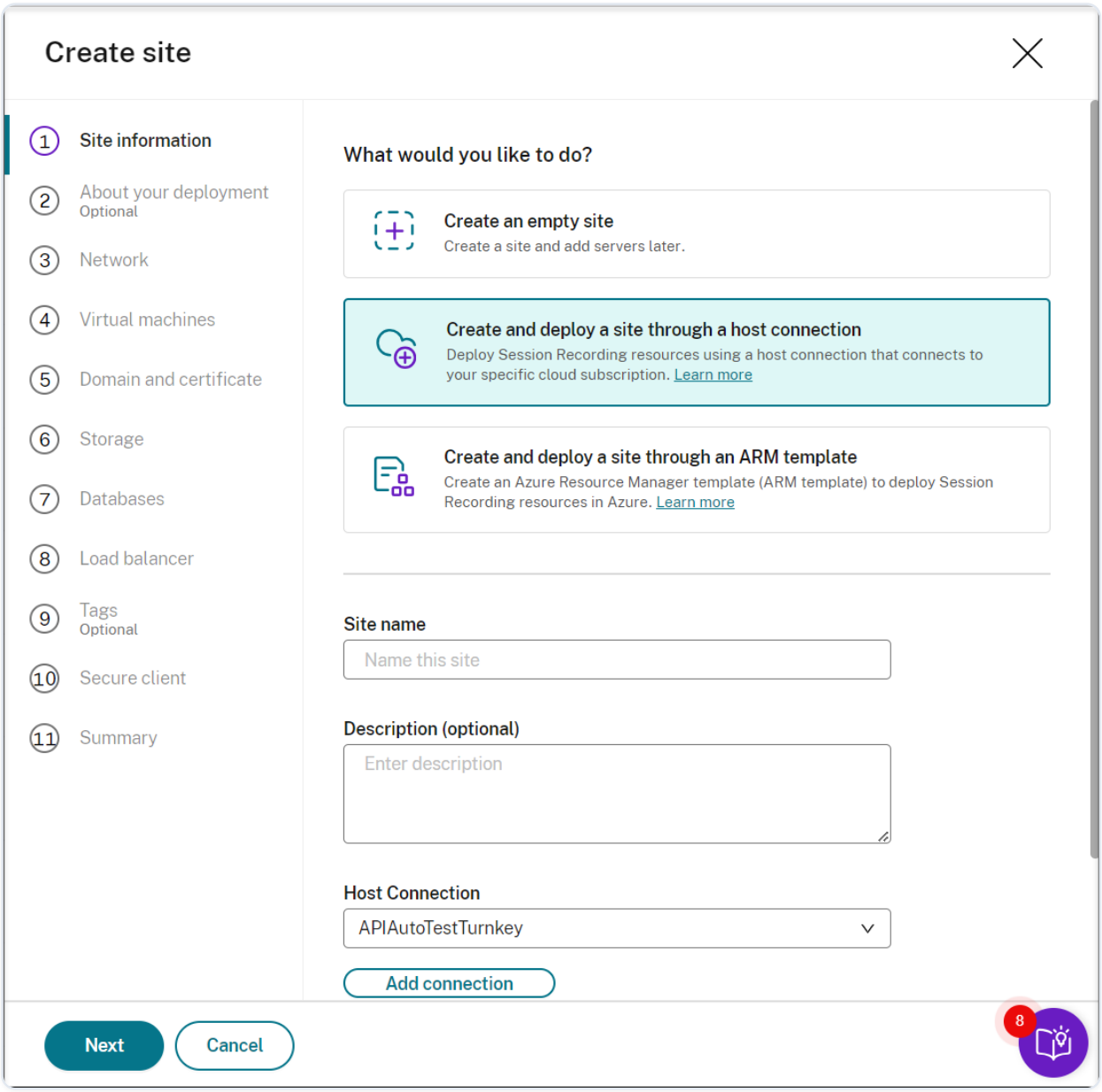
1. Select **Configuration > Server Management** from the left navigation of the Session Recording service.



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



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

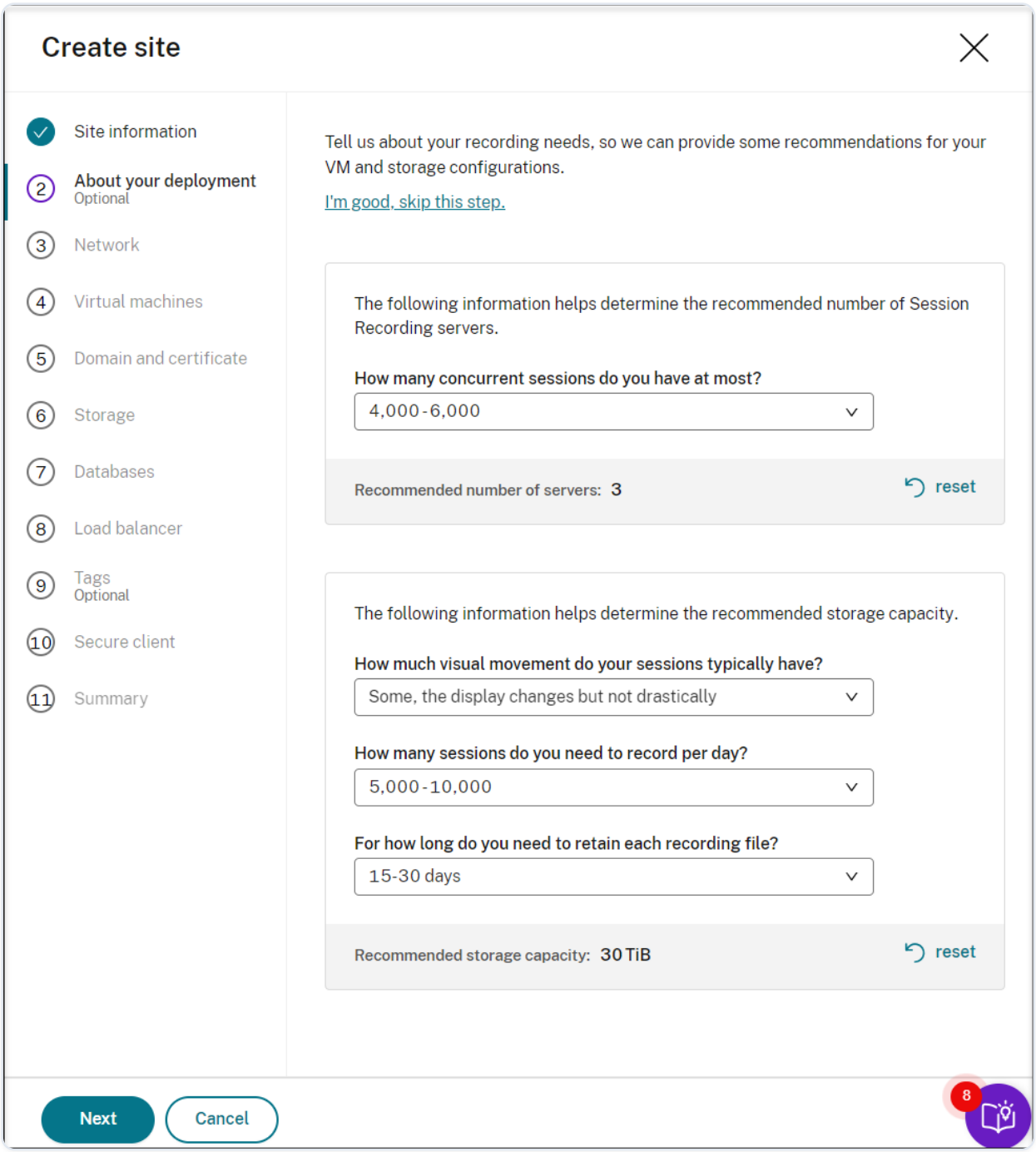


4. Enter a site name and description, select a host connection that connects to your Azure subscription, and specify a region.

   - 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.

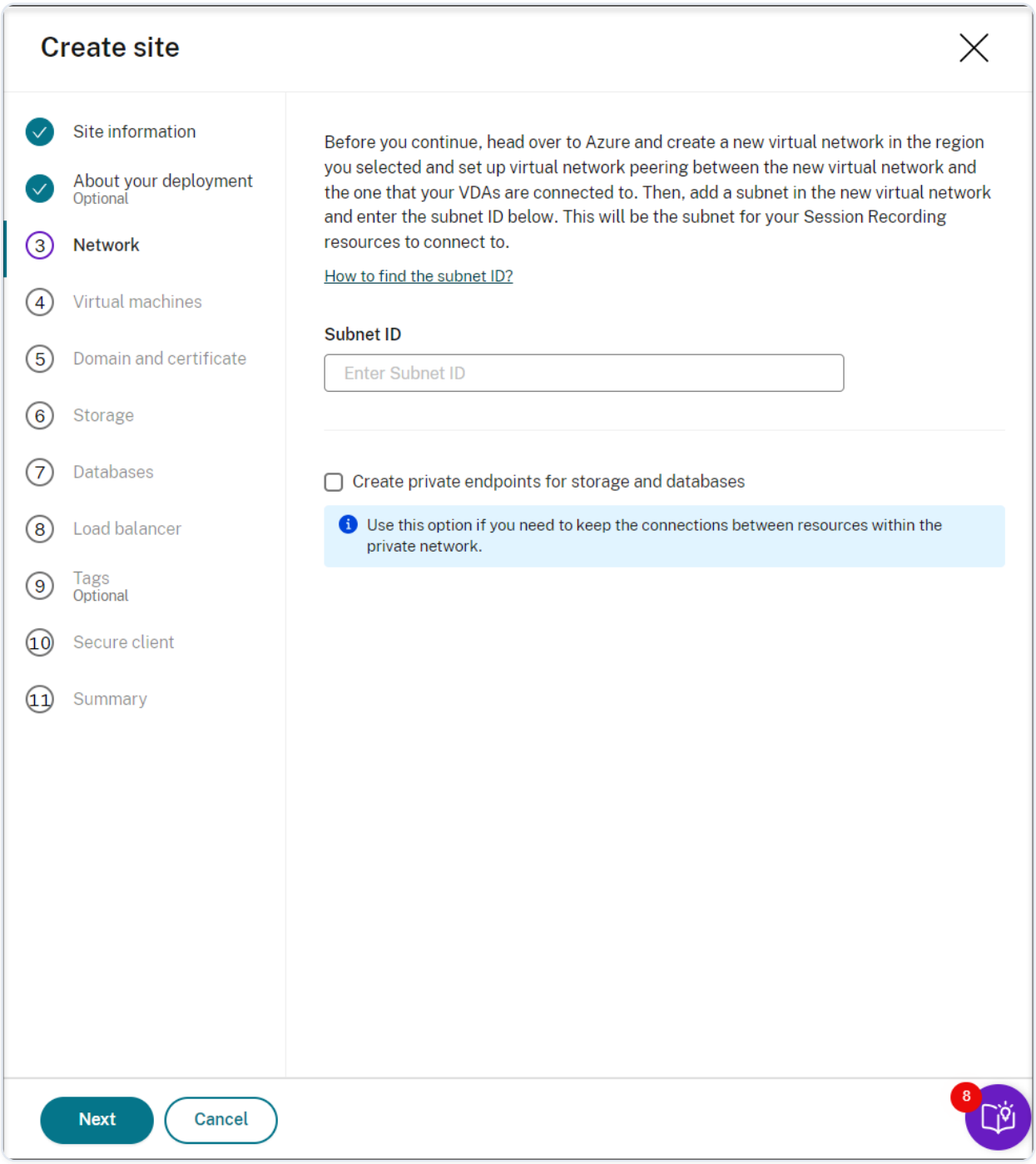
5. After completing the site information, click **Next** to continue.
6. (Optional) To get recommendations for VM and storage configurations, provide information about your recording needs.

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



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.

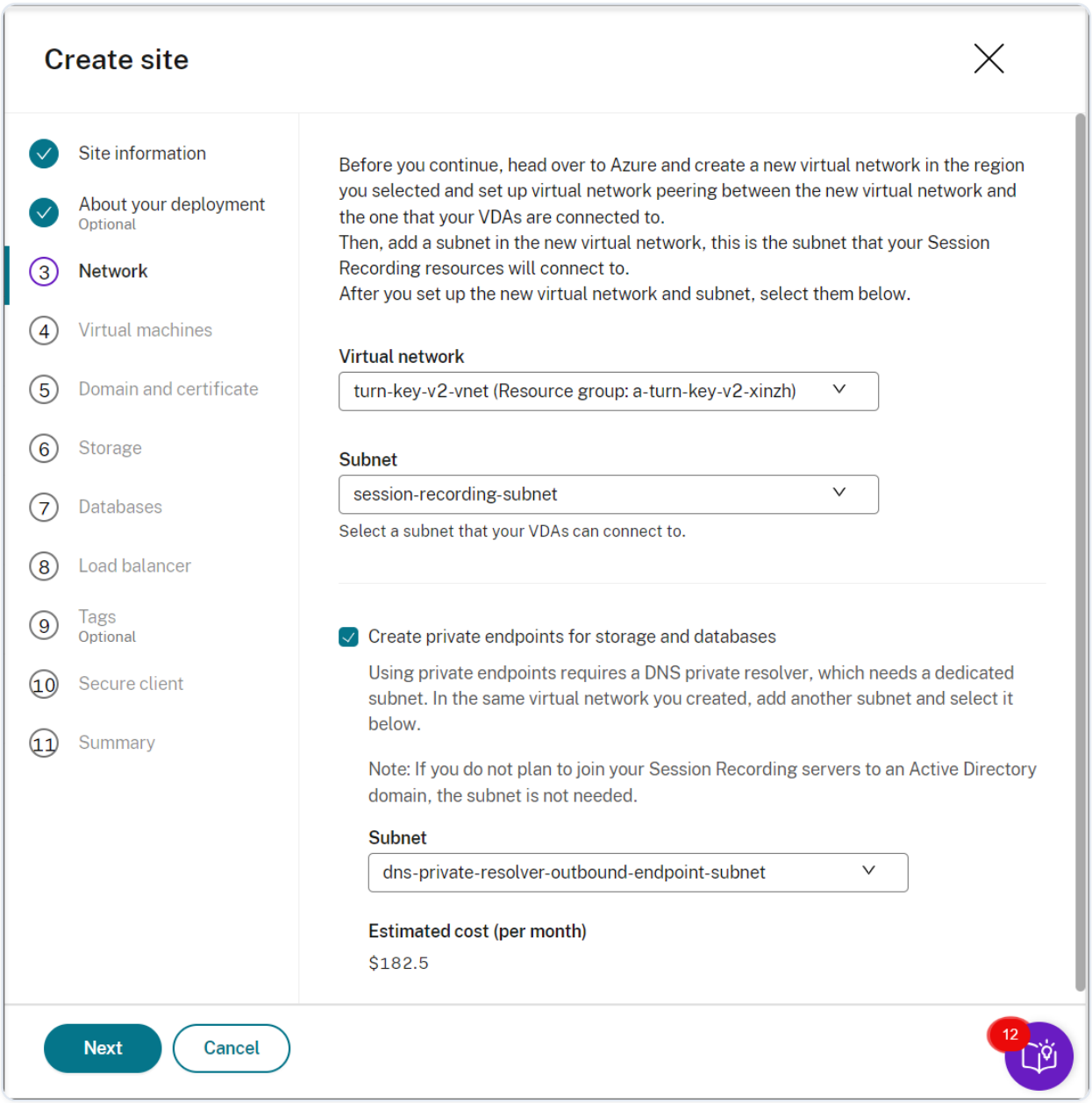
7. Go to the Azure portal and create a new virtual network in the region you selected and set up virtual network peering between the new virtual network and the one that your VDAs are connected to. Then, add a subnet in the new virtual network. Find and enter the subnet ID below.



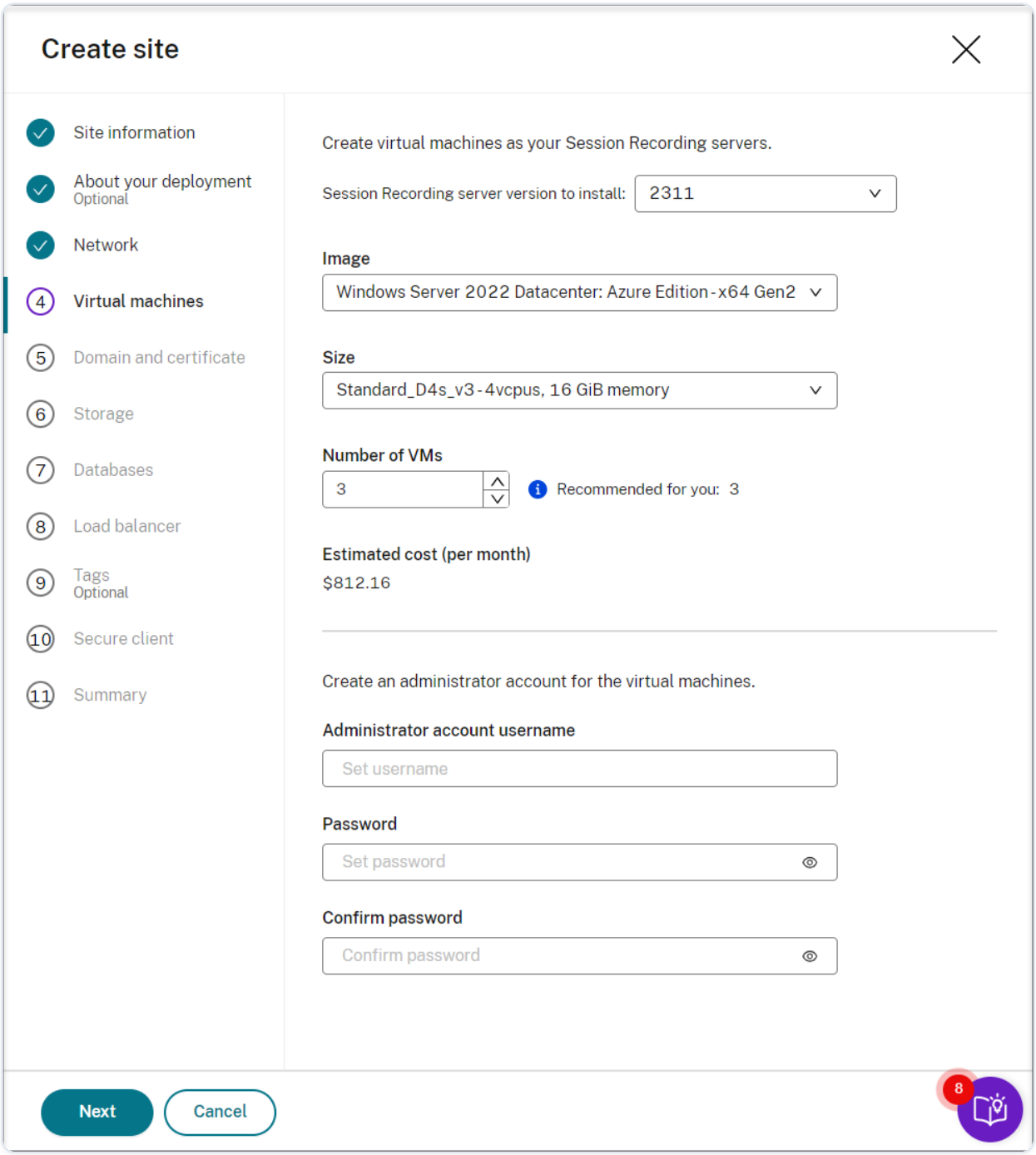
To keep the connections between resources within the private network, select the **Create private endpoints for storage and databases** check box.

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.



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

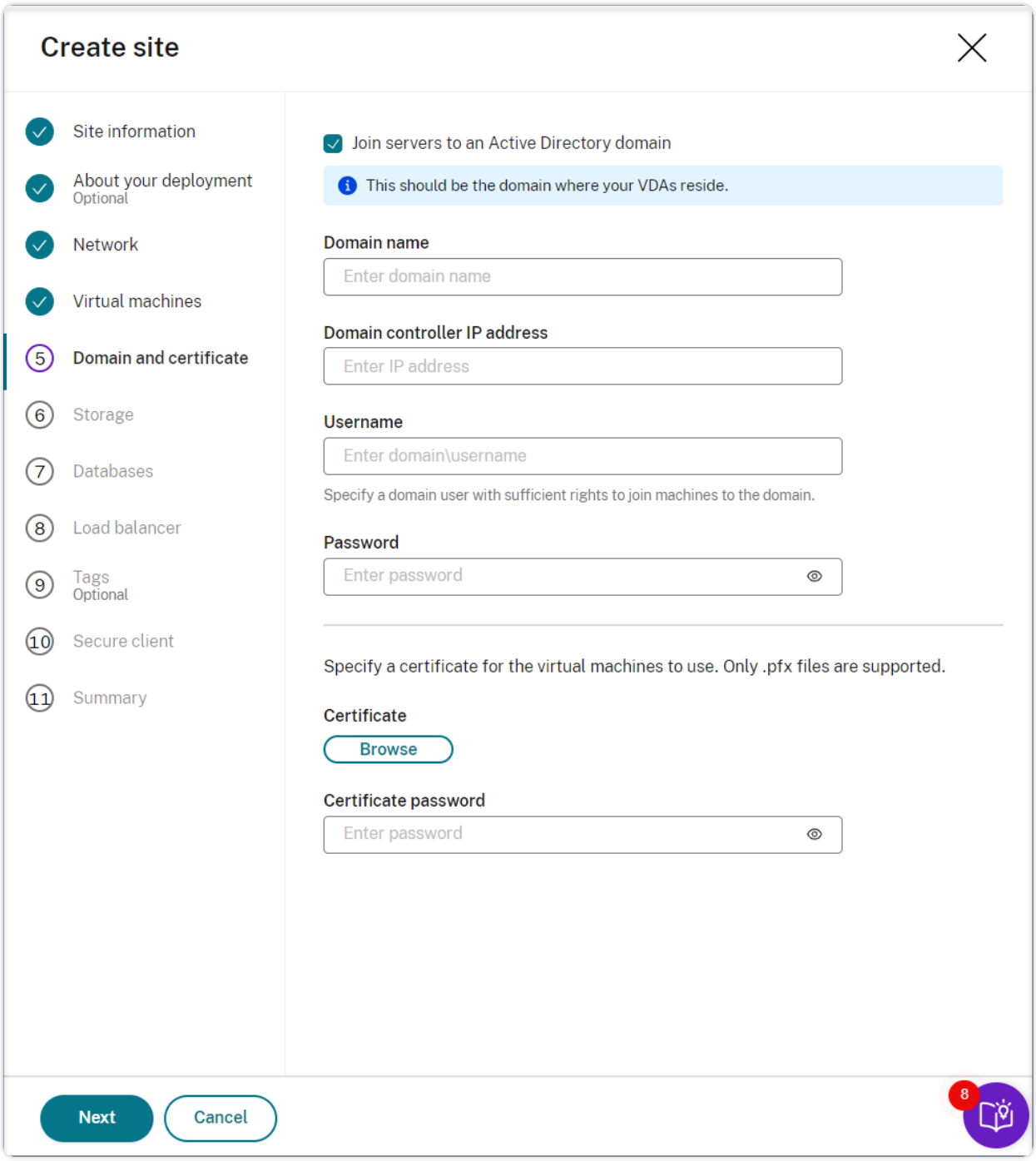


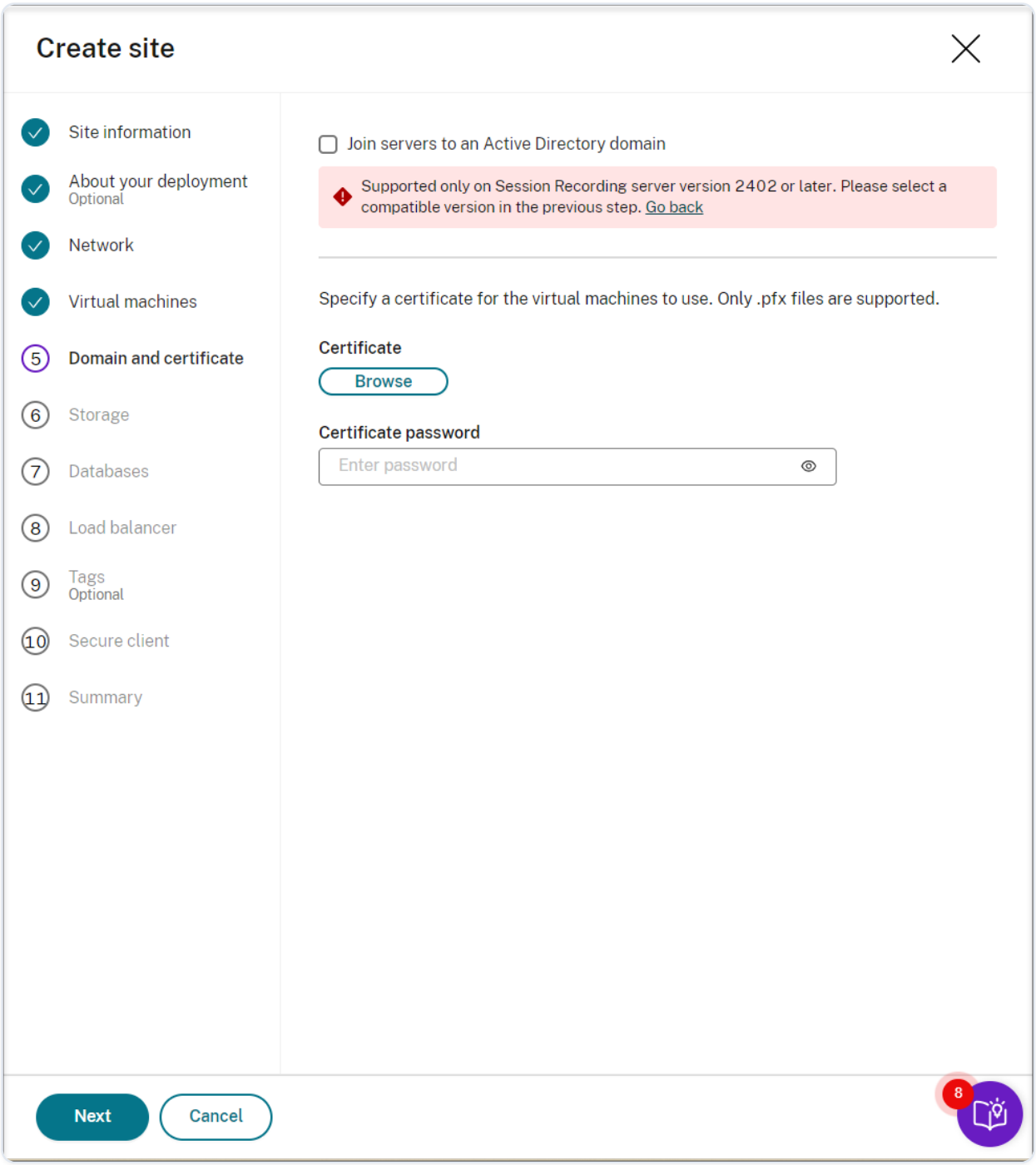
Note:

- 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.

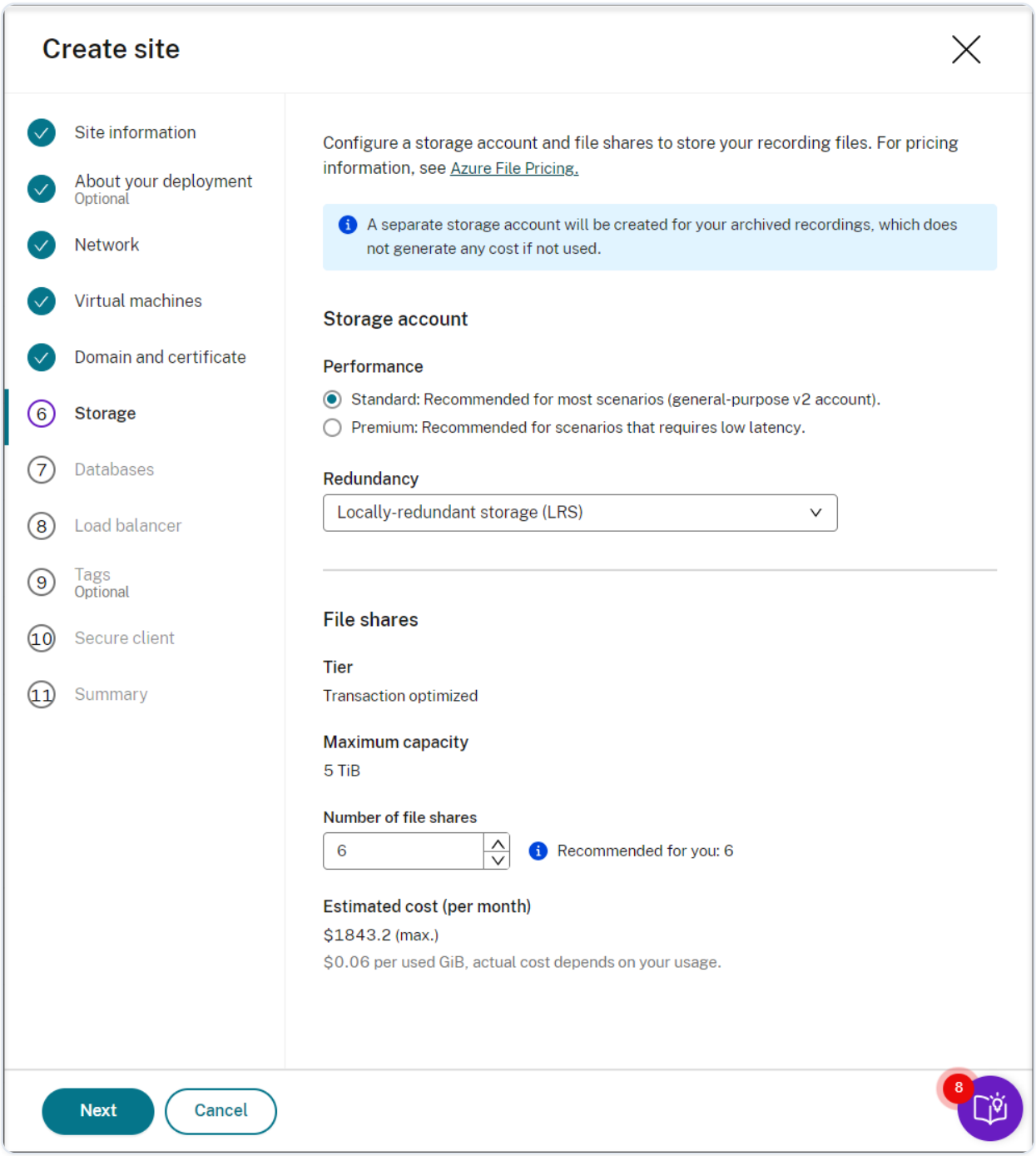

Create site
Site information
About your deployment
Optional
Network
Virtual machines
5
Domain and certificate
6
Storage
7
Databases
8
Load balancer
9
Tags
Optional
10
Secure client
11
Summary
Join servers to an Active Directory domain
This should be the domain where your VDAs reside.
Domain name
Enter 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
8



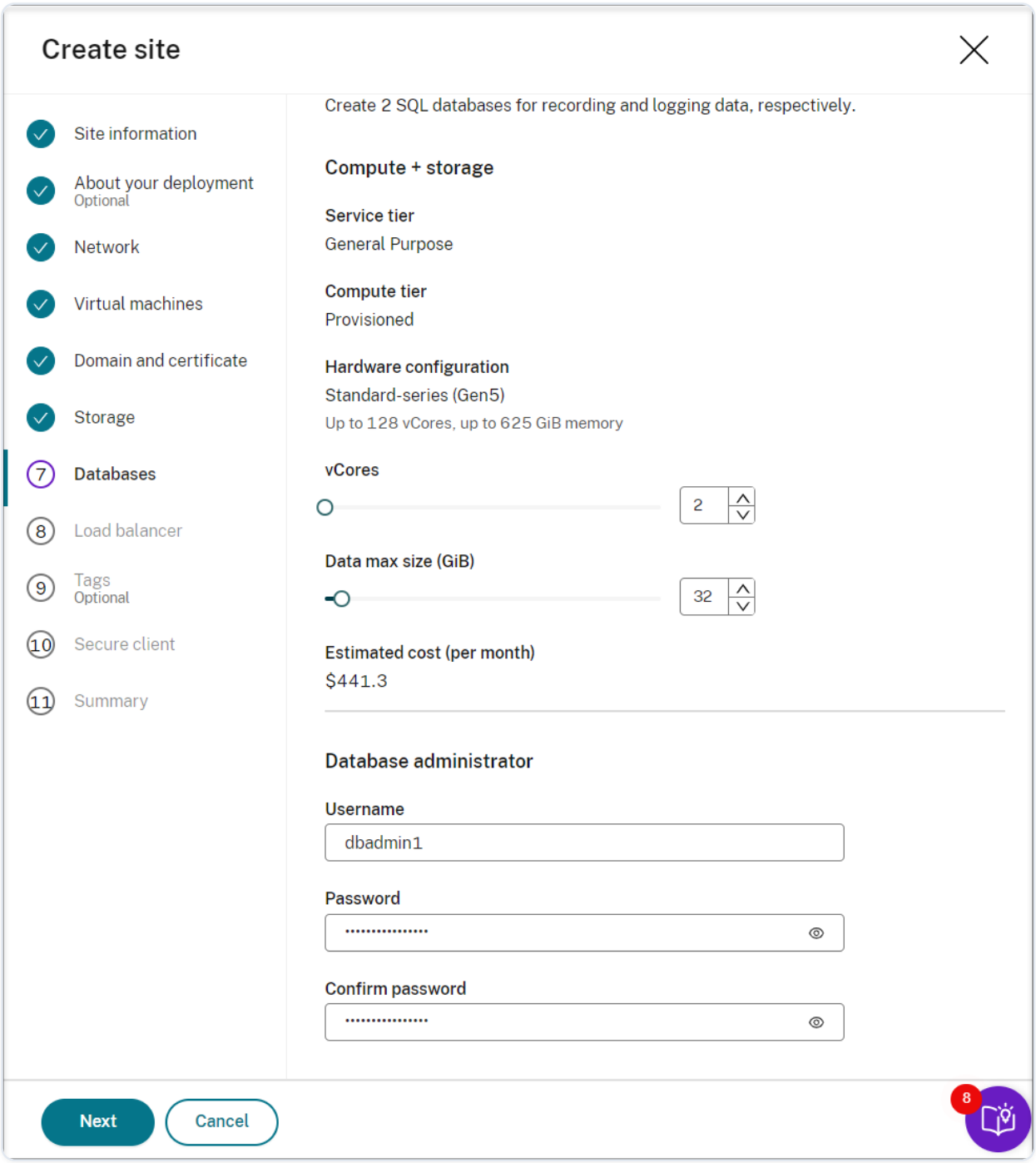
Note:

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.



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**).

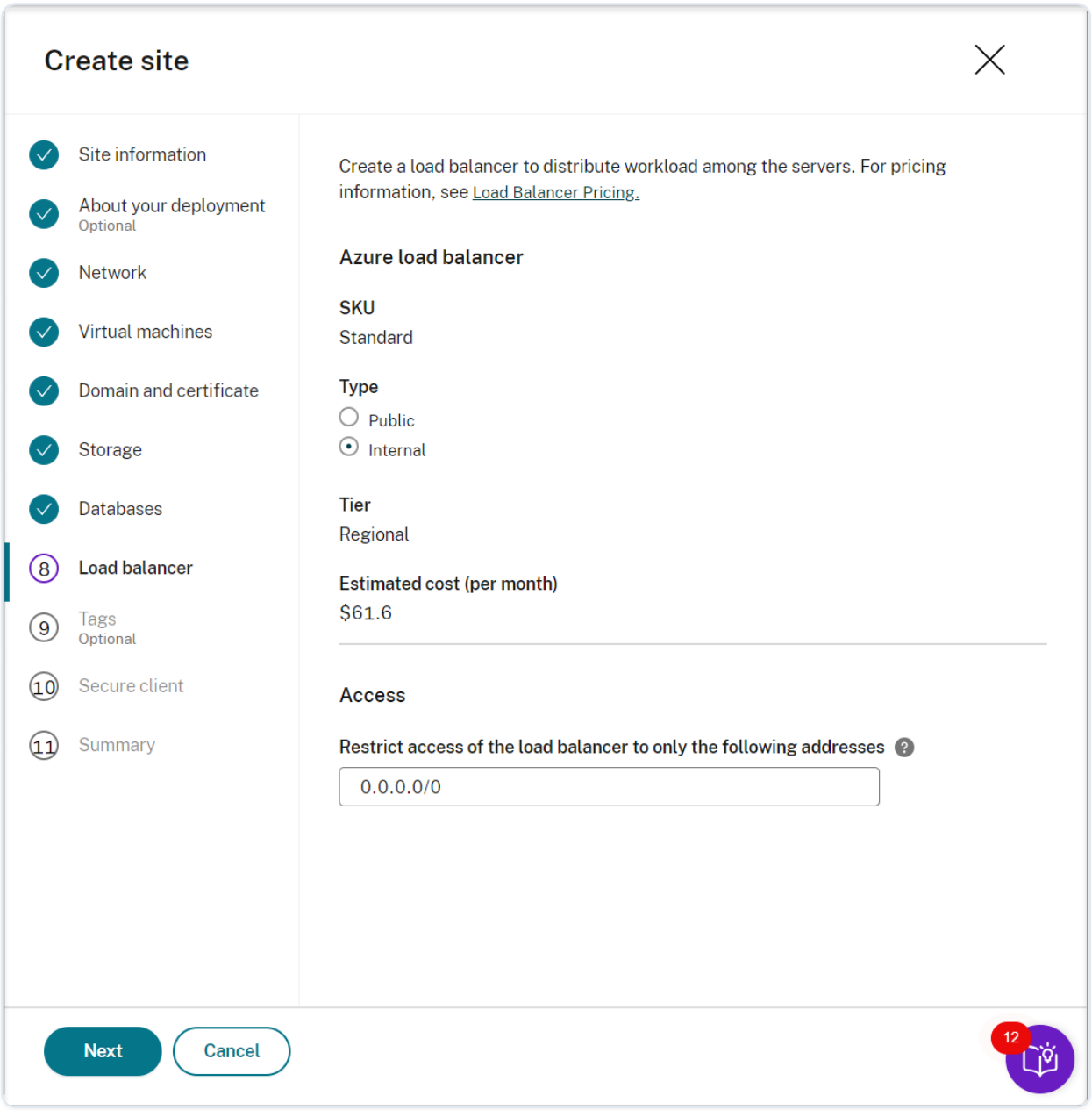


Note:

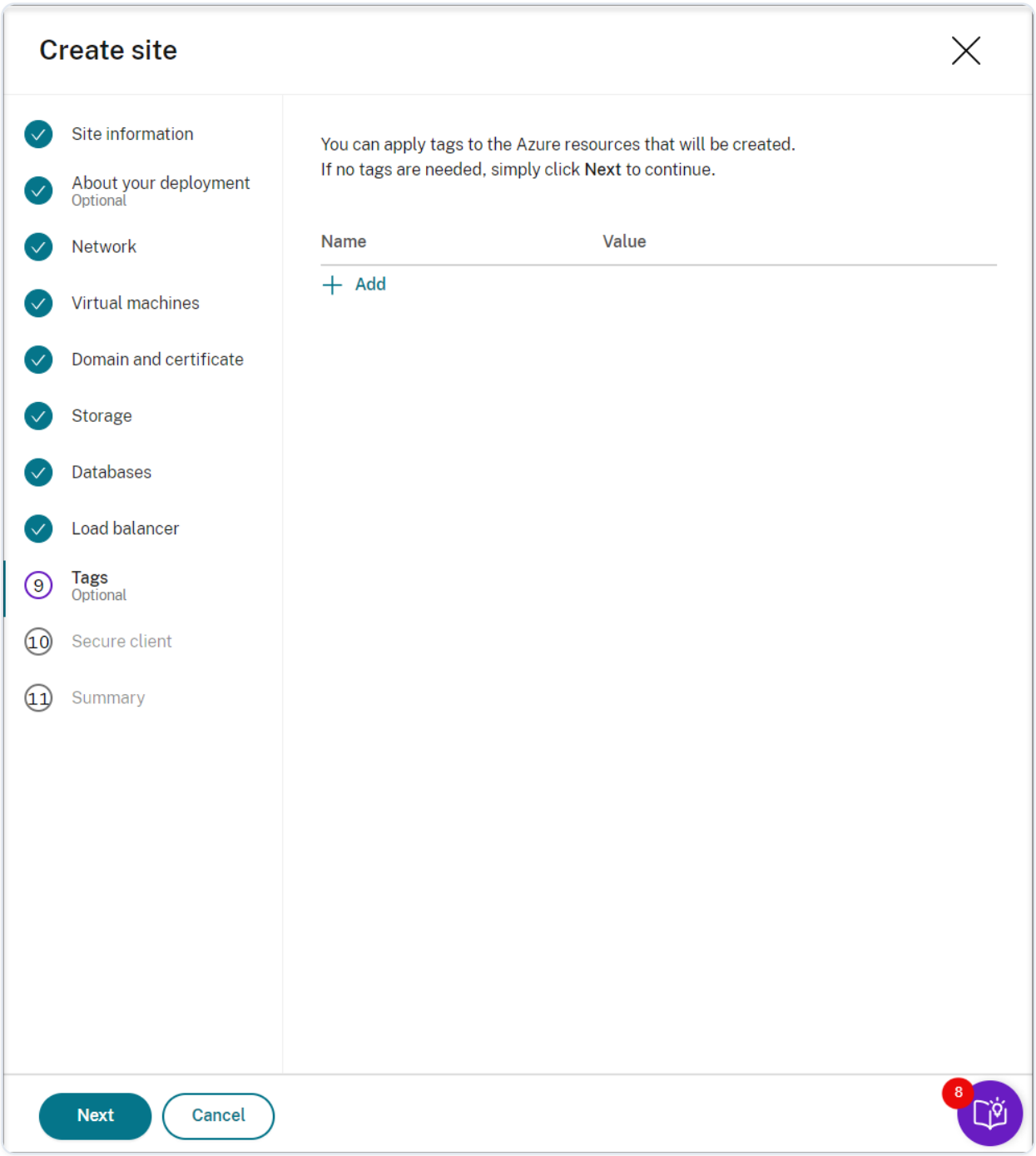
When adding resources, specifically Session Recording servers, to an existing site deployed through a host connection, you are required to provide the database administrator password set during the site creation.

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.

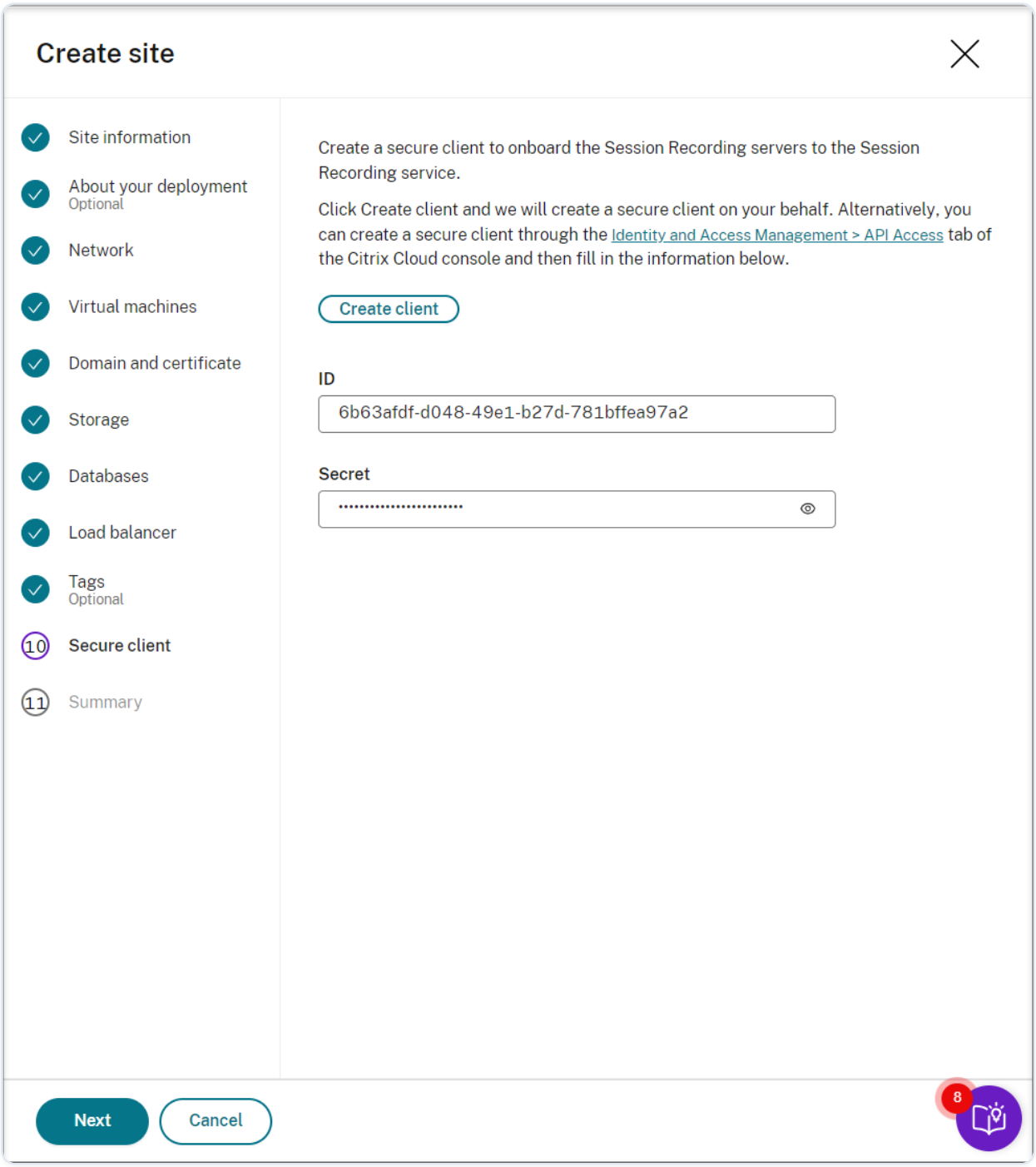


13. (Optional) Apply tags to the Azure resources to be created.

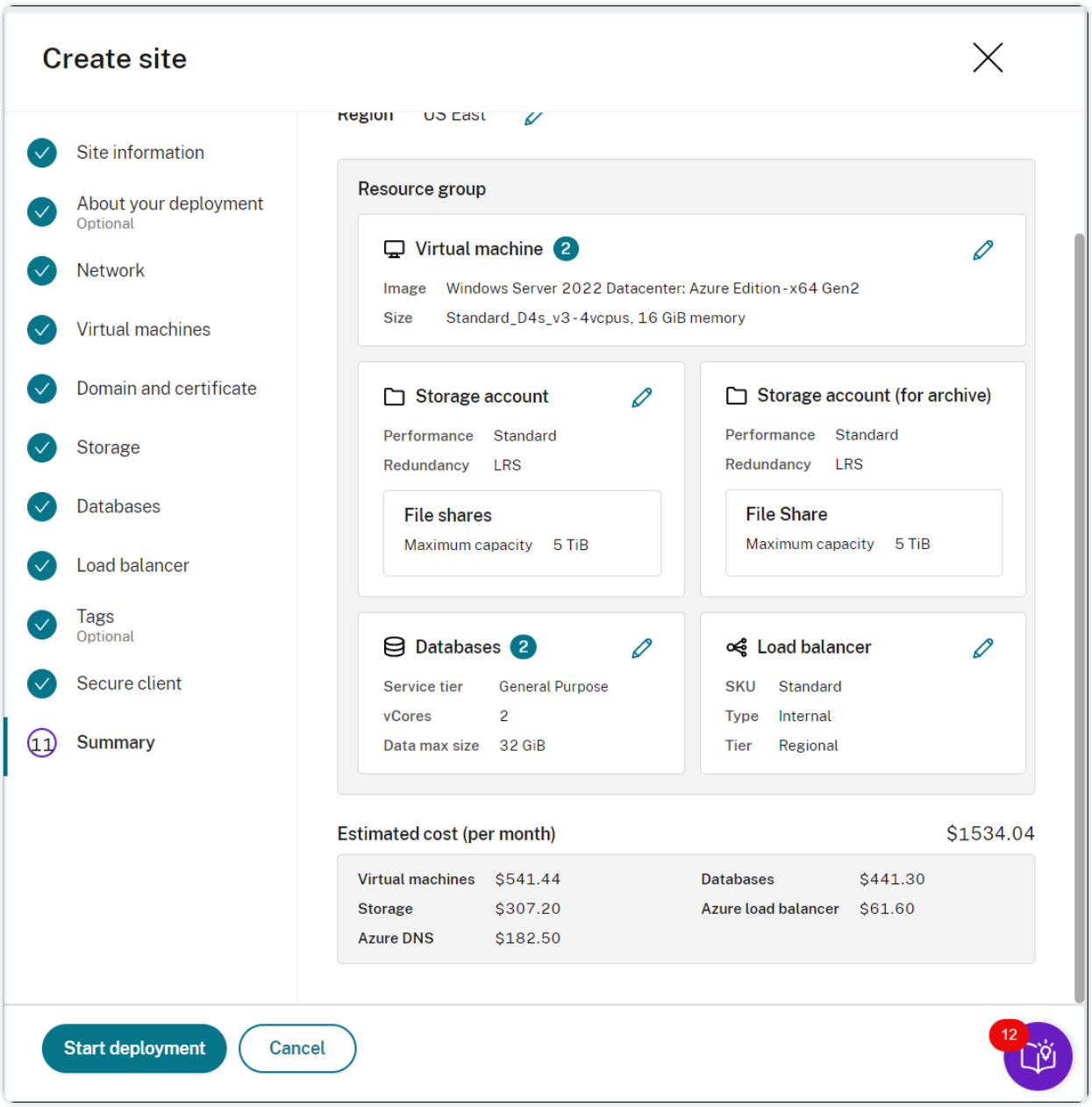


14. Create a secure client to onboard the Session Recording servers to the Session Recording service.

    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.

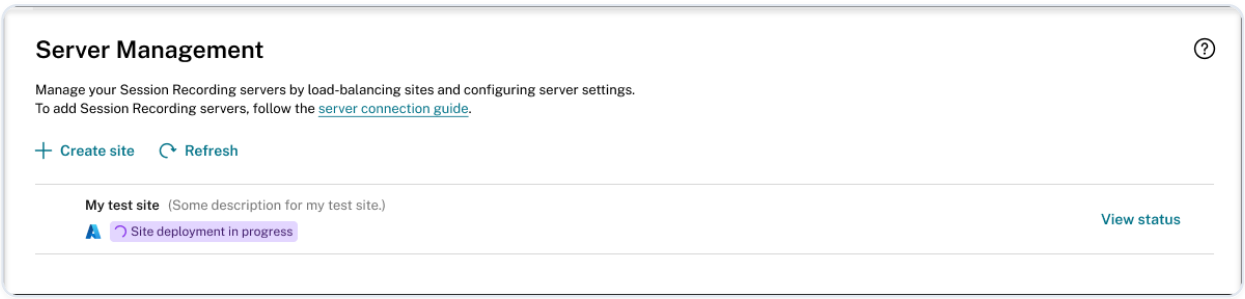


15. View the summary about the site to be created. Click the pencil icon to edit your settings if needed or click the button to start deployment.



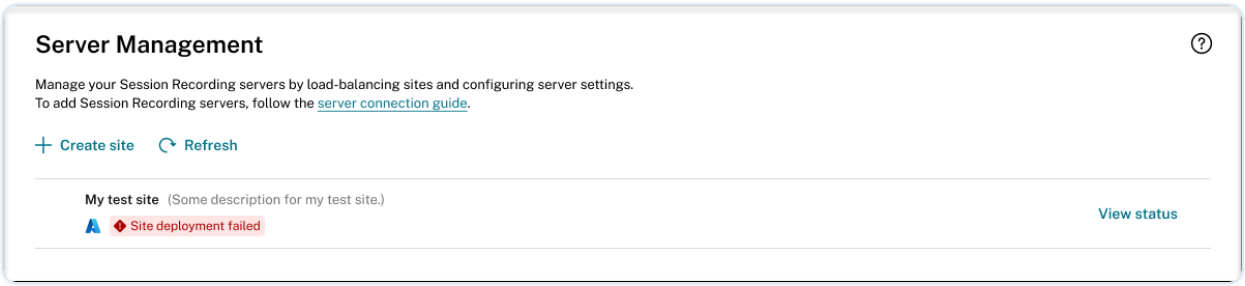
The following are examples of the deployment process:

Deployment in progress:

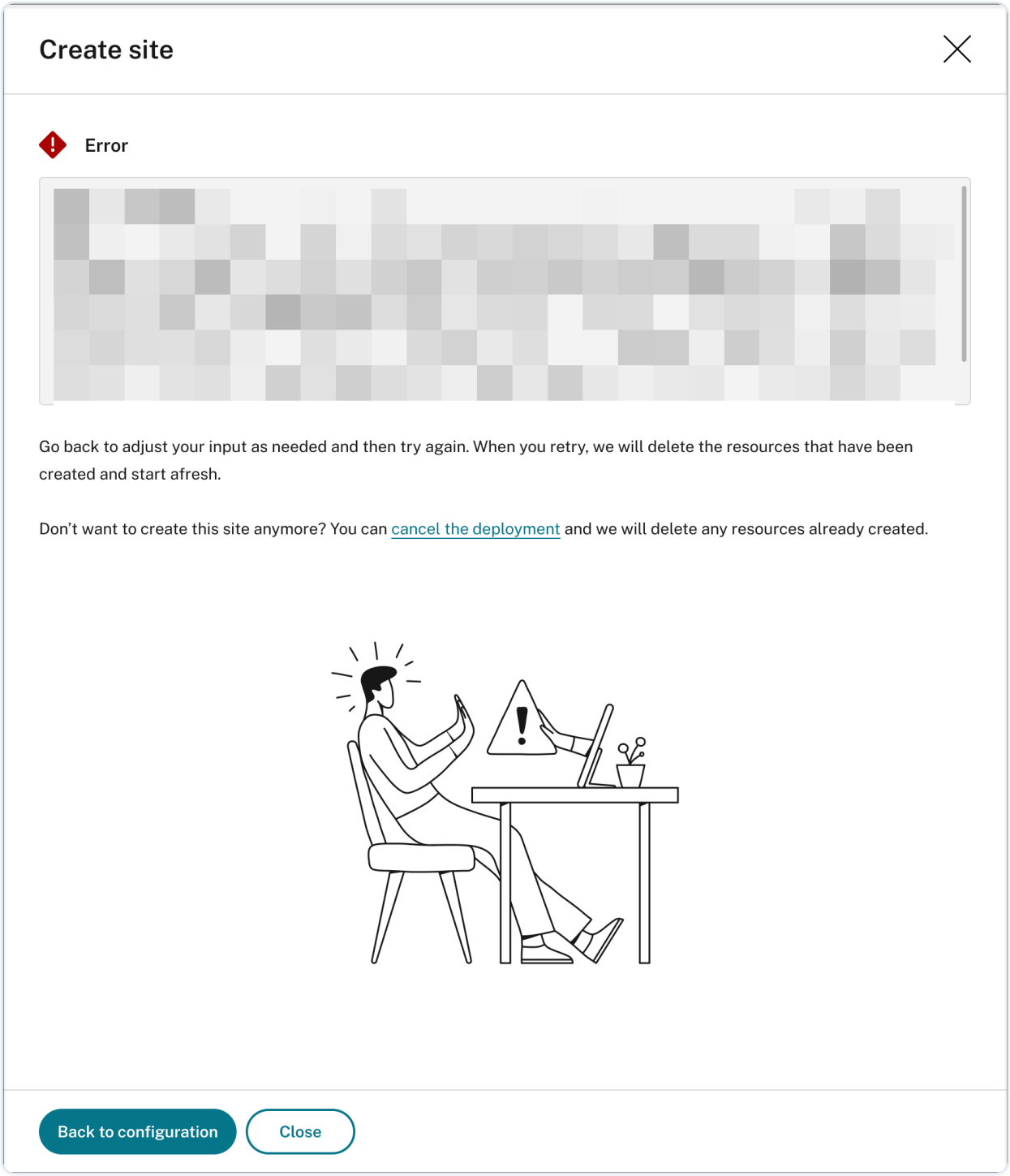


While a site deployment is in progress, you can click **View status** to view the progress.

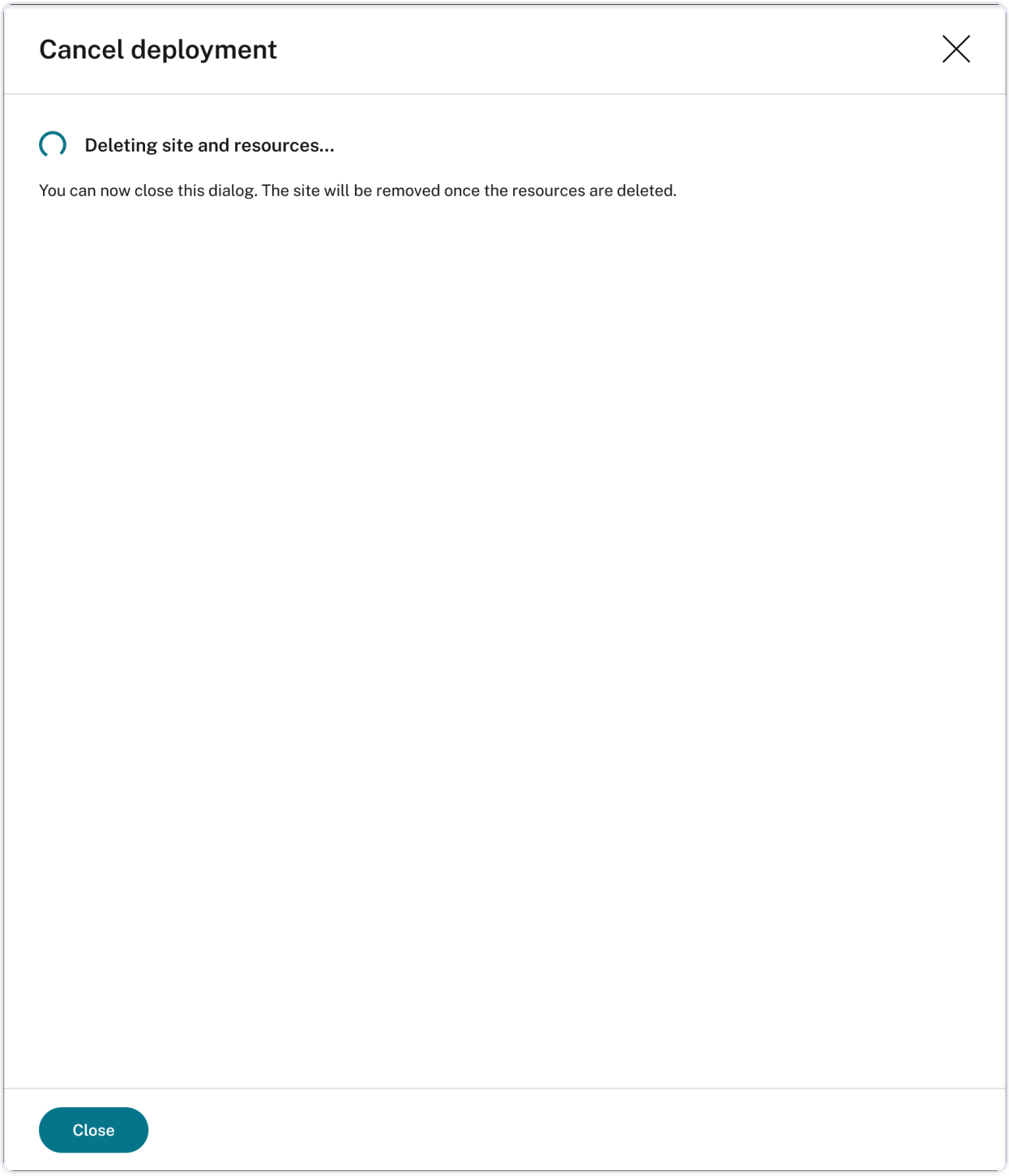
Deployment failed:



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



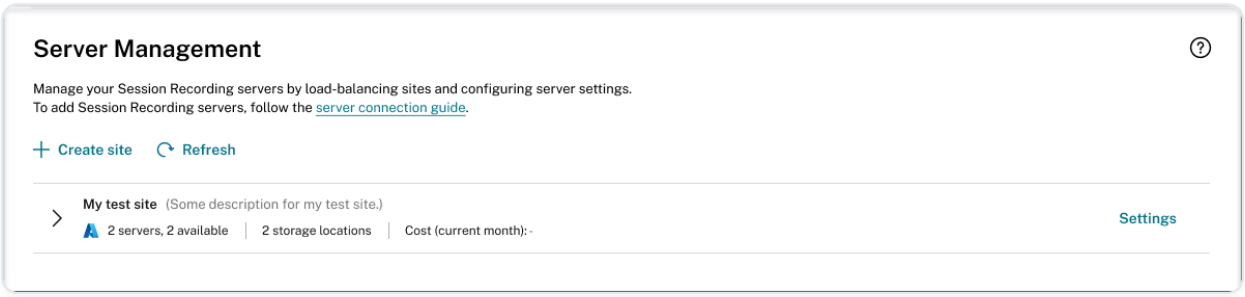
You can click **Back to configuration** or **cancel the deployment**. If you click **Back to configuration**, you're taken back to the **Create Site** page where you can alter your configurations and try again. If you're sure to cancel the deployment, follow the wizard to remove the site and the Azure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

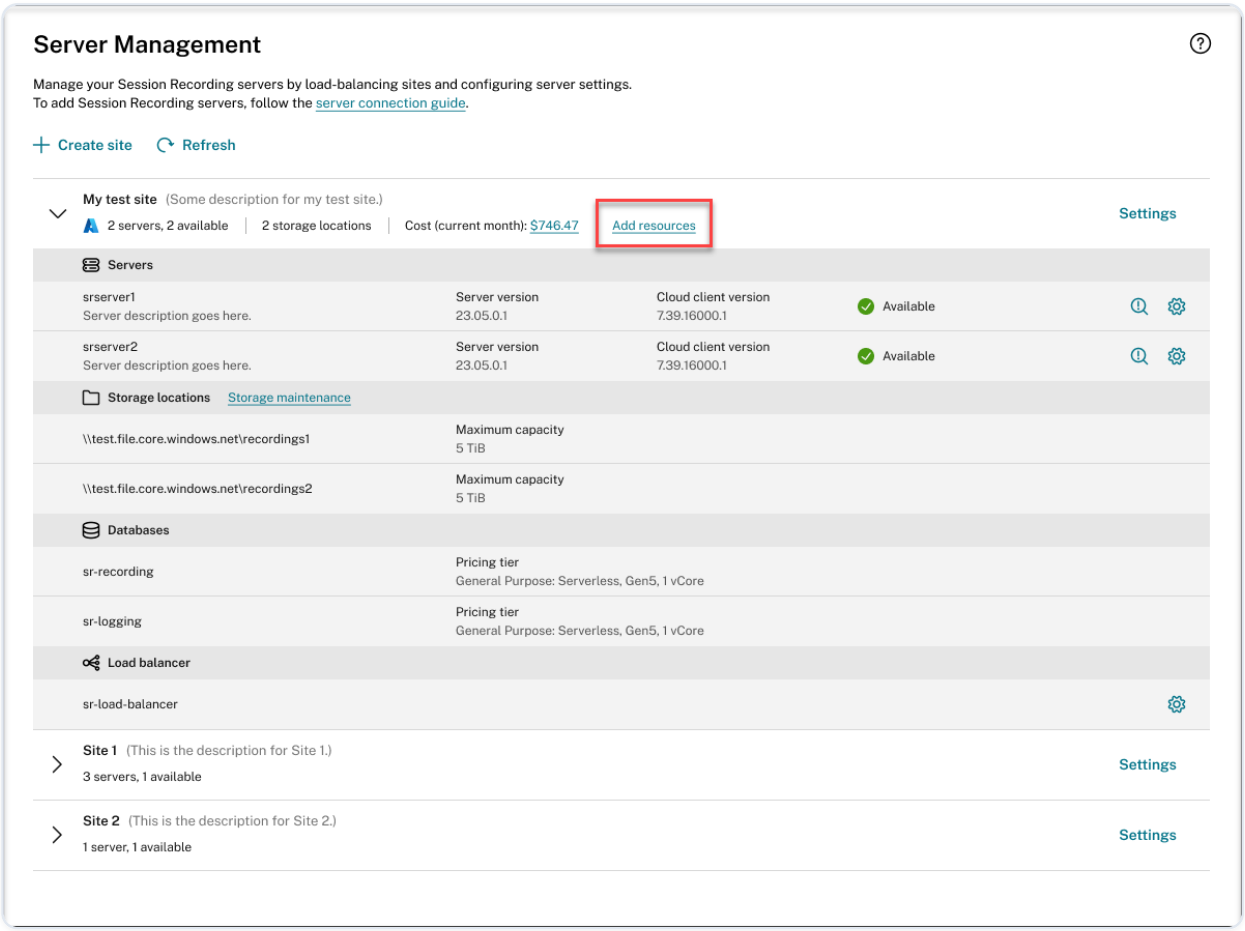
available to represent sites deployed on Azure. For information about site settings, see Site and server settings.



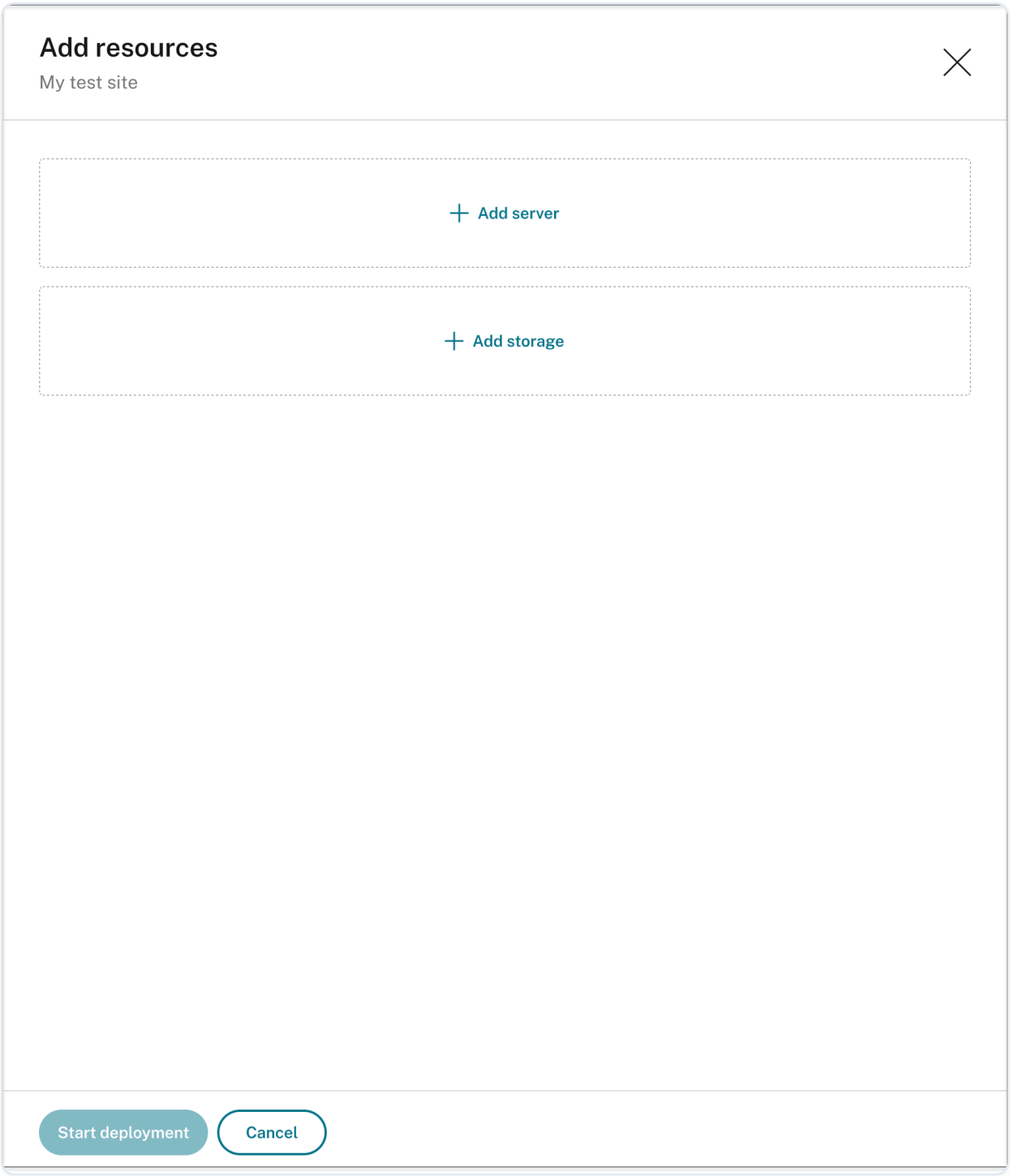
Add resources to an existing site deployed on Azure

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:

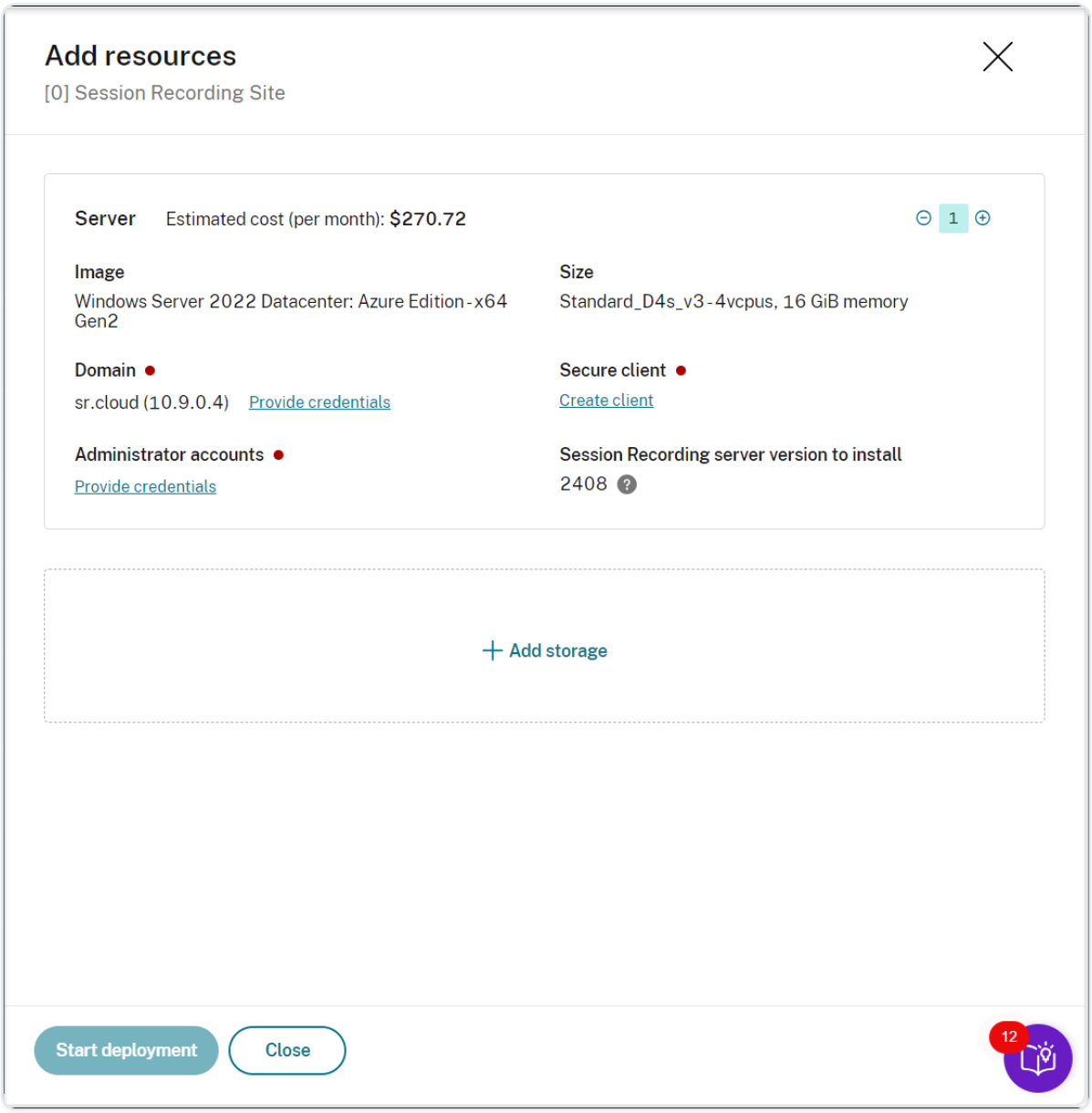
1. Select **Configuration > Server Management** from the left navigation of the Session Recording service.
2. On the **Server Management** page, locate and unfold the target site. An Azure icon is available to represent sites deployed on Azure.
3. Click **Add resources**.



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



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



a. Specify the number of servers to add.

b. Click **Provide credentials** in the **Domain** section to join the new servers to the same domain as the existing servers.

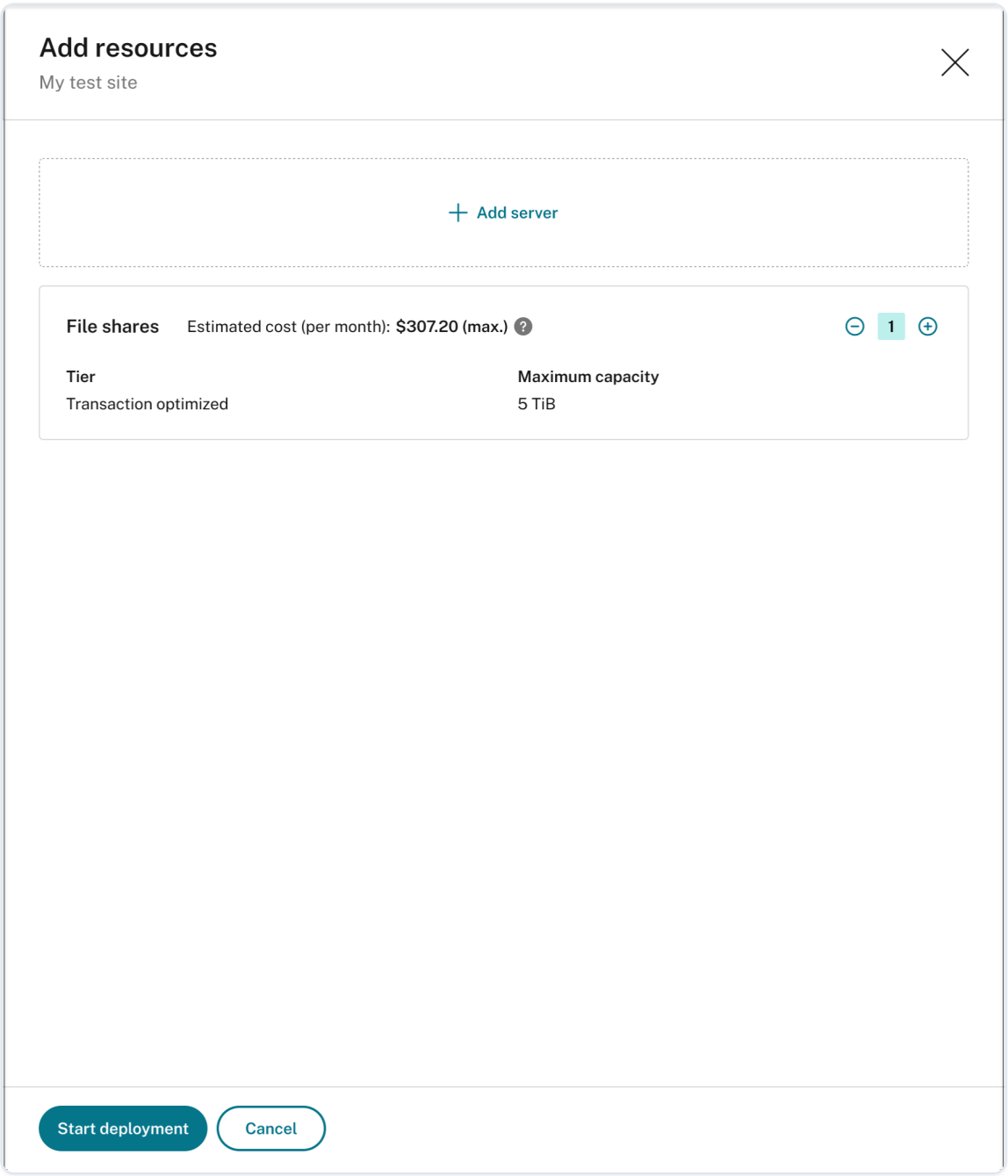
c. Click **Provide credentials** in the **Administrator accounts** section to provide the database administrator password set during the site creation. Additionally, you need to set a password for the administrator account on the server machine(s) being added. We recommend using the same password as the one set during site creation.

d. Click **Create client** to onboard the new servers to the Session Recording service.

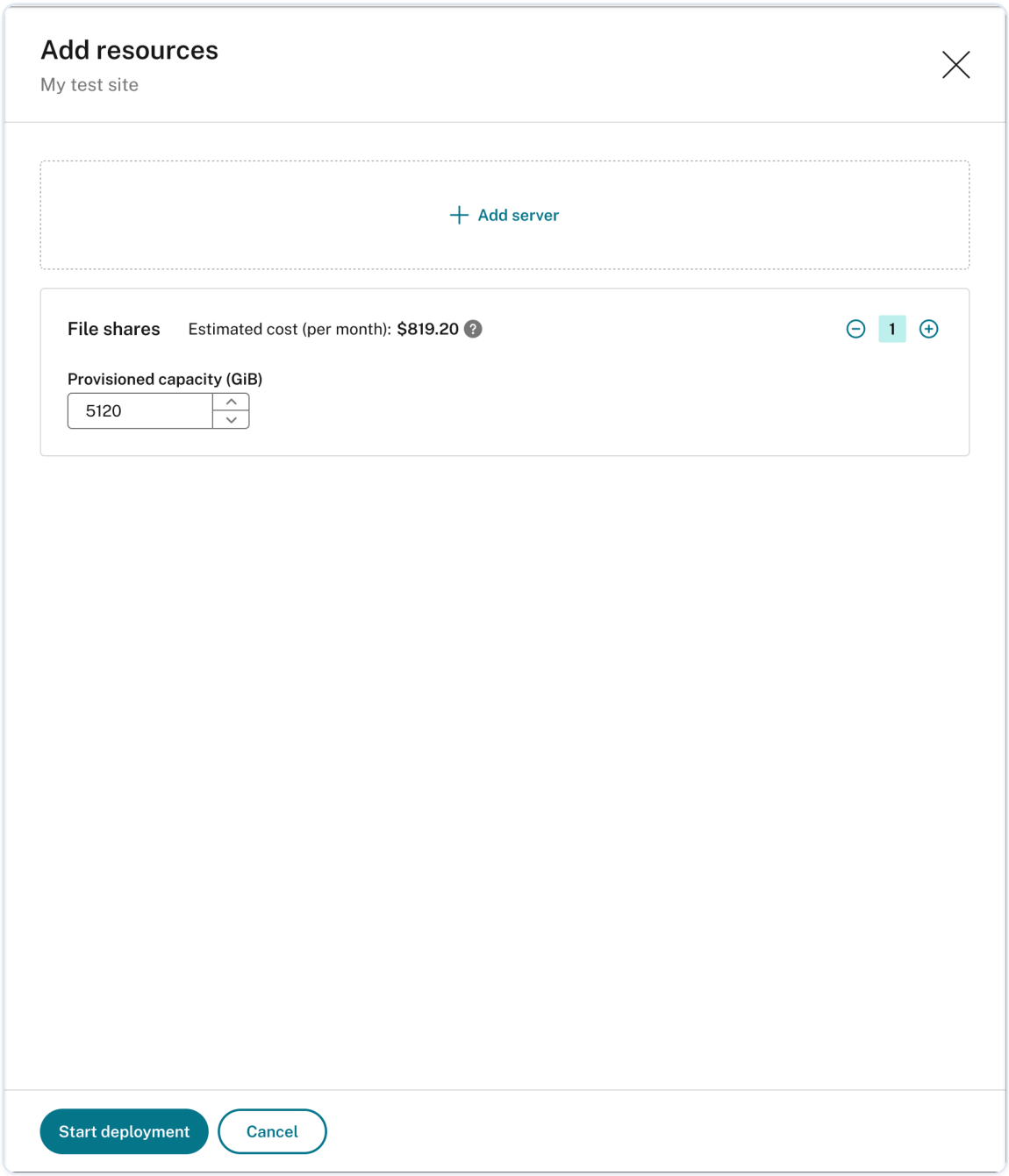
e. Click **Start deployment**.

- To add storage for storing recording files, click **Add storage** and then complete the following steps accordingly:

a. If your site was created with a standard storage account, you're prompted to specify the number of file shares to add. For example:



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:

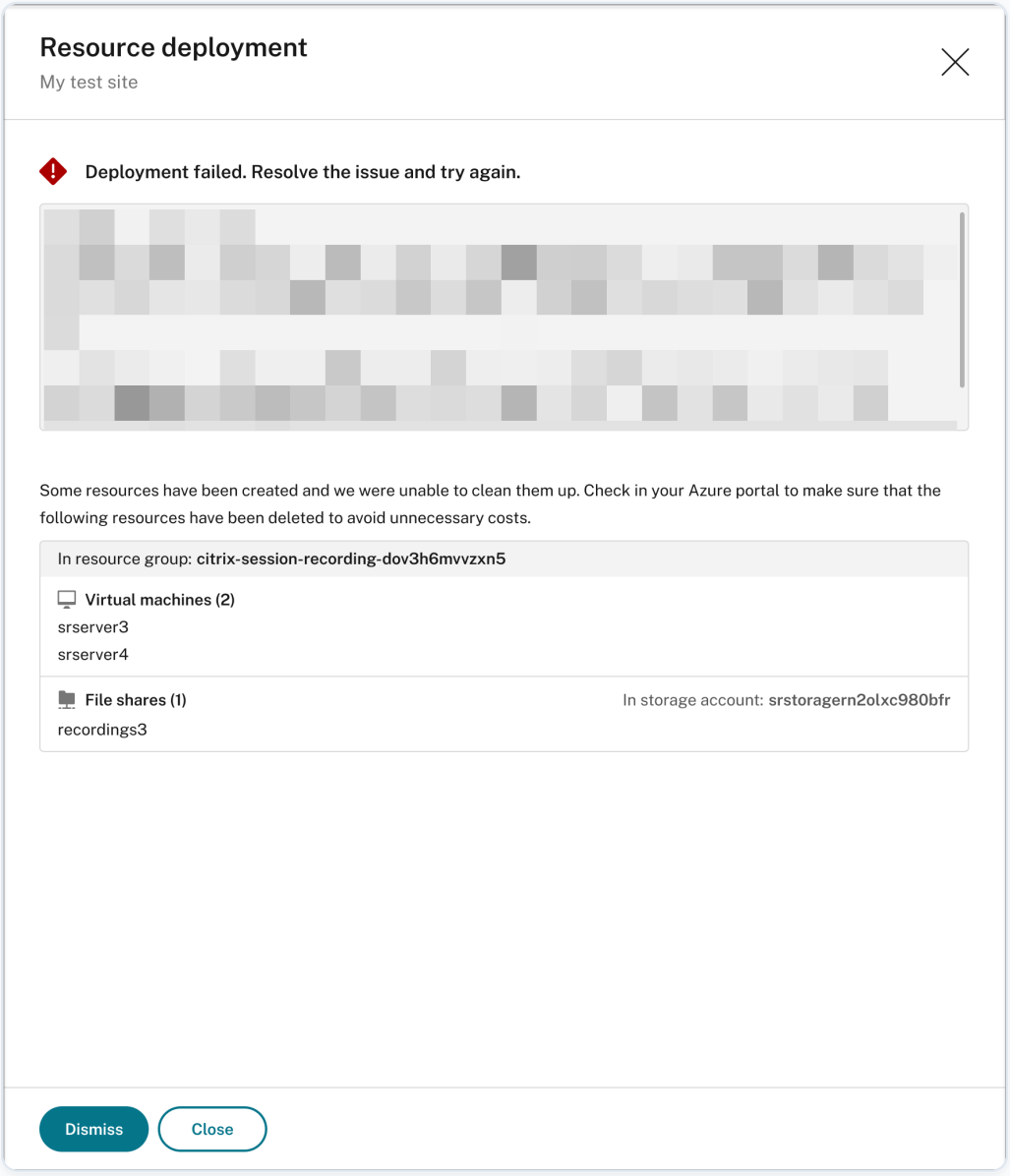


c. Click **Start deployment**.

> **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.

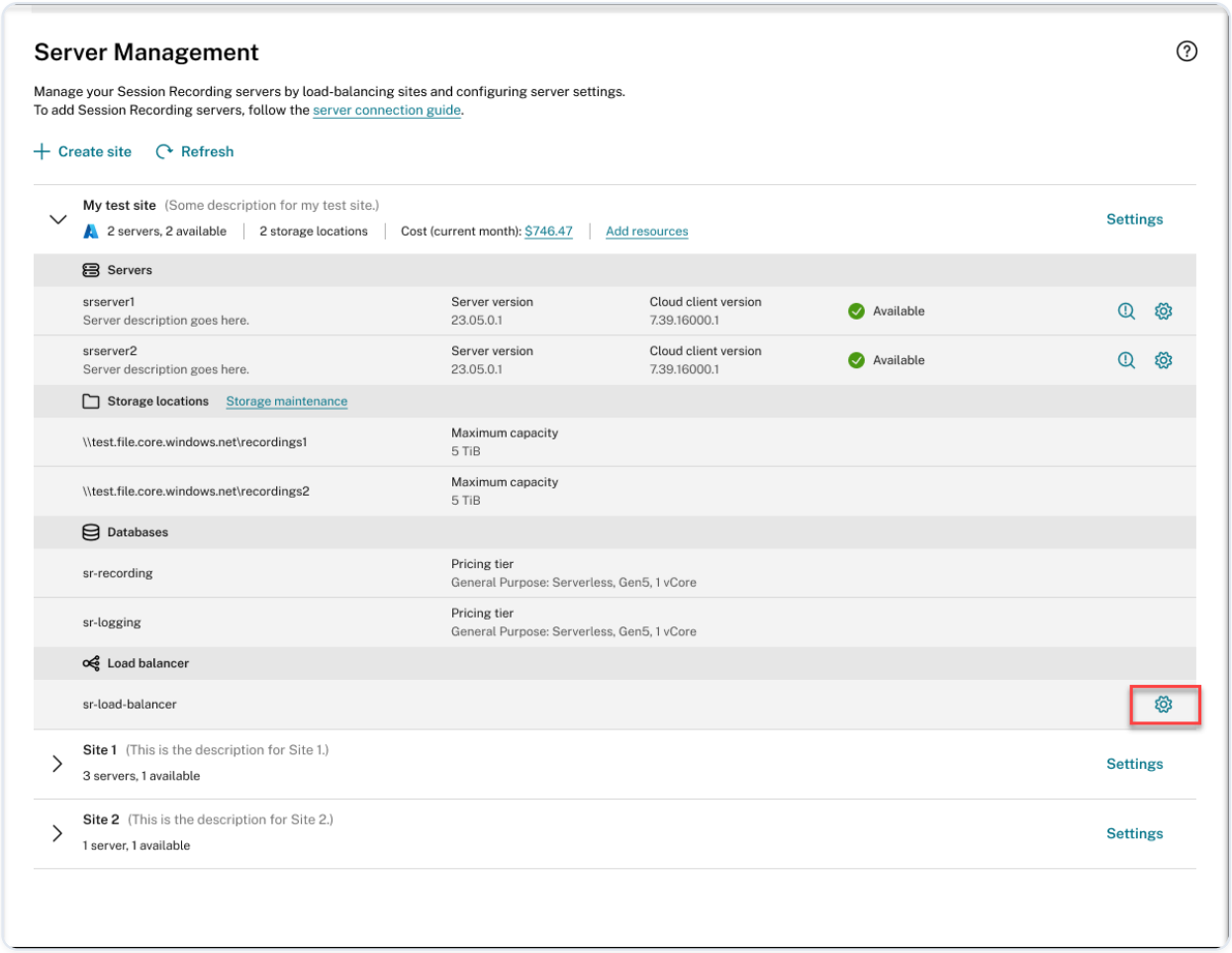
- When resource deployment is in progress, the **Settings** button for the load balancer is disabled.
- The deployment of added resources can fail and the Session Recording service might not be able to remove these resources from your subscription. In this case, a prompt similar to the following is provided for you to take action:



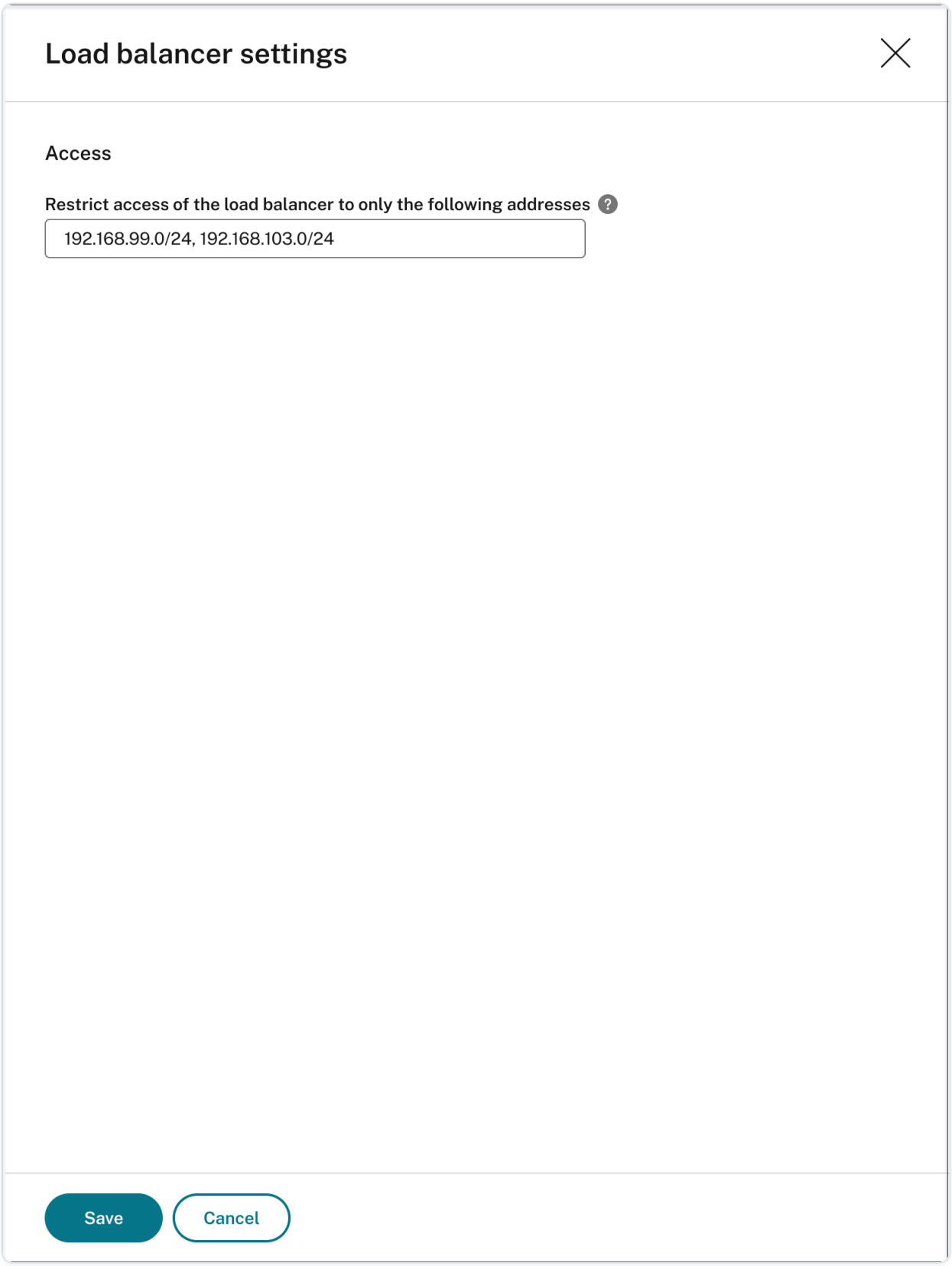
Change the IP addresses that are allowed to access the load balancer

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.



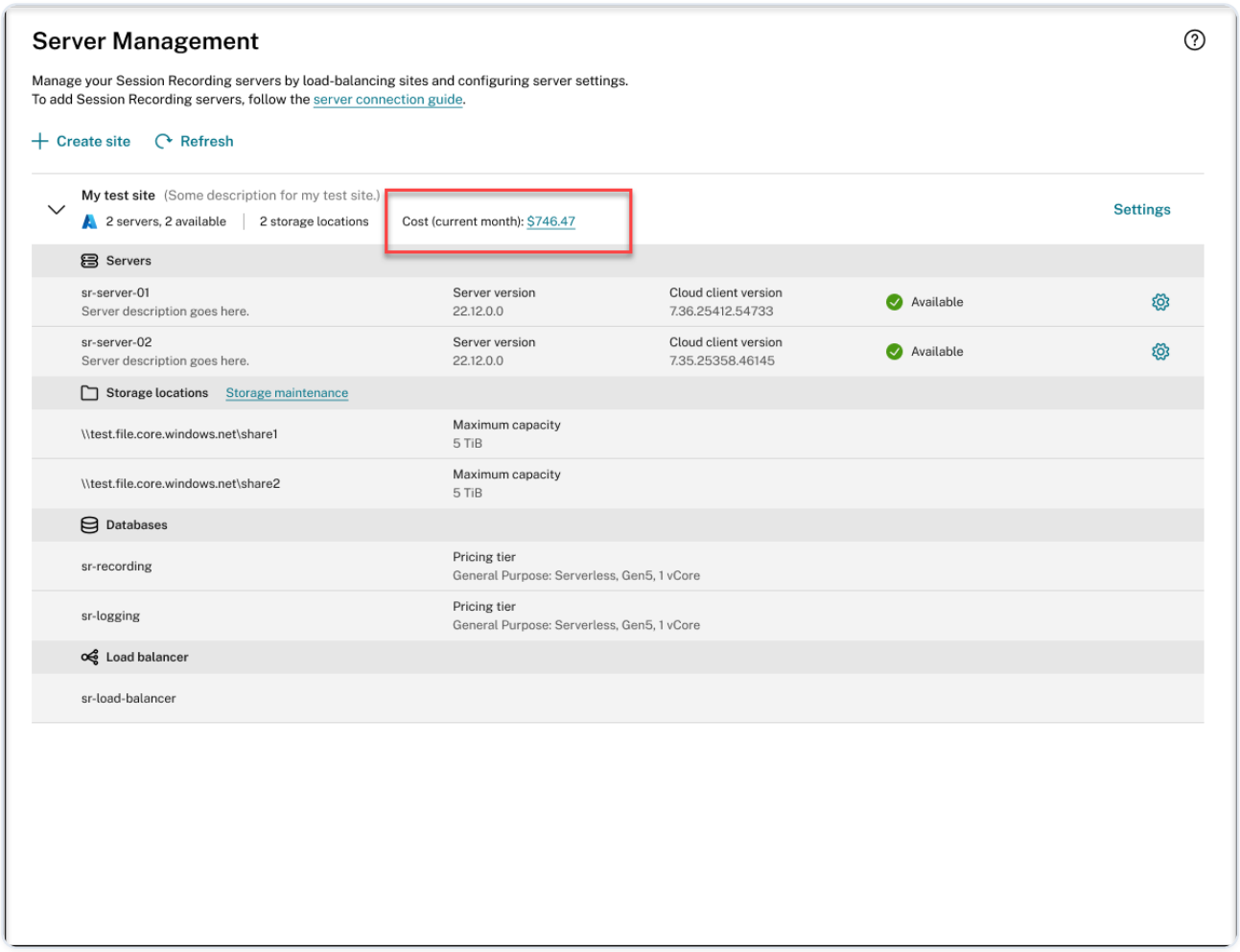
4. On the **Load balancer** settings page, enter the new IP addresses or ranges of your VDAs and separate them by a comma (,) in the **Restrict access of the load balancer to only the following addresses** field.

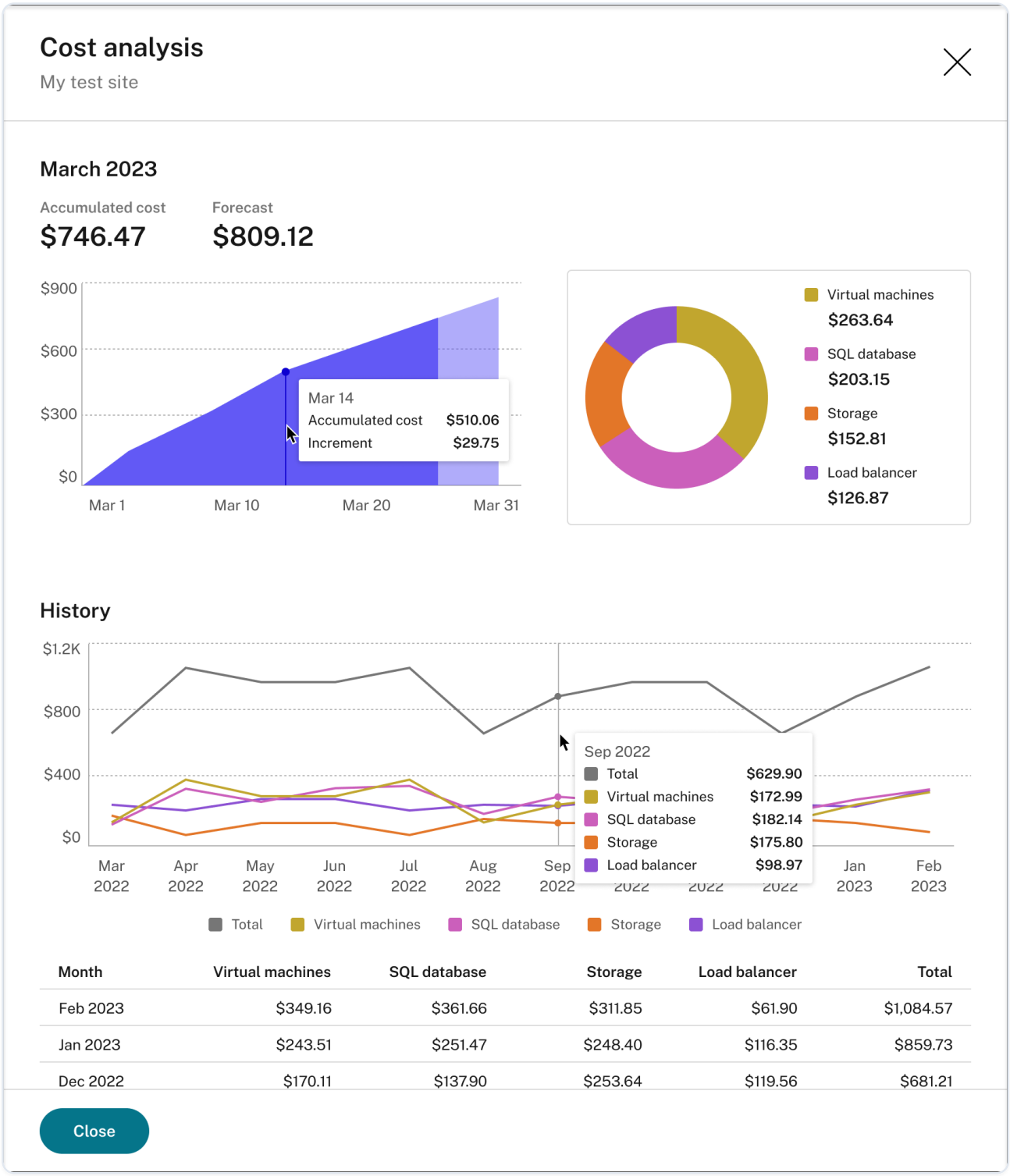


5. Click **Save**.

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:


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.)
2 servers, 2 available
2 storage locations
Cost (current month): $746.47
Settings
Servers
sr-server-01
Server description goes here.
Server version
22.12.0.0
Cloud client version
7.36.25412.54733
Available
sr-server-02
Server description goes here.
Server version
22.12.0.0
Cloud client version
7.35.25358.46145
Available
Storage locations
Storage maintenance
\\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



Month	Virtual machines	SQL database	Storage	Load balancer	Total
Feb 2023	$349.16	$361.66	$311.85	$61.90	$1,084.57
Jan 2023	$243.51	$251.47	$248.40	$116.35	$859.73
Dec 2022	$170.11	$137.90	$253.64	$119.56	$681.21

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

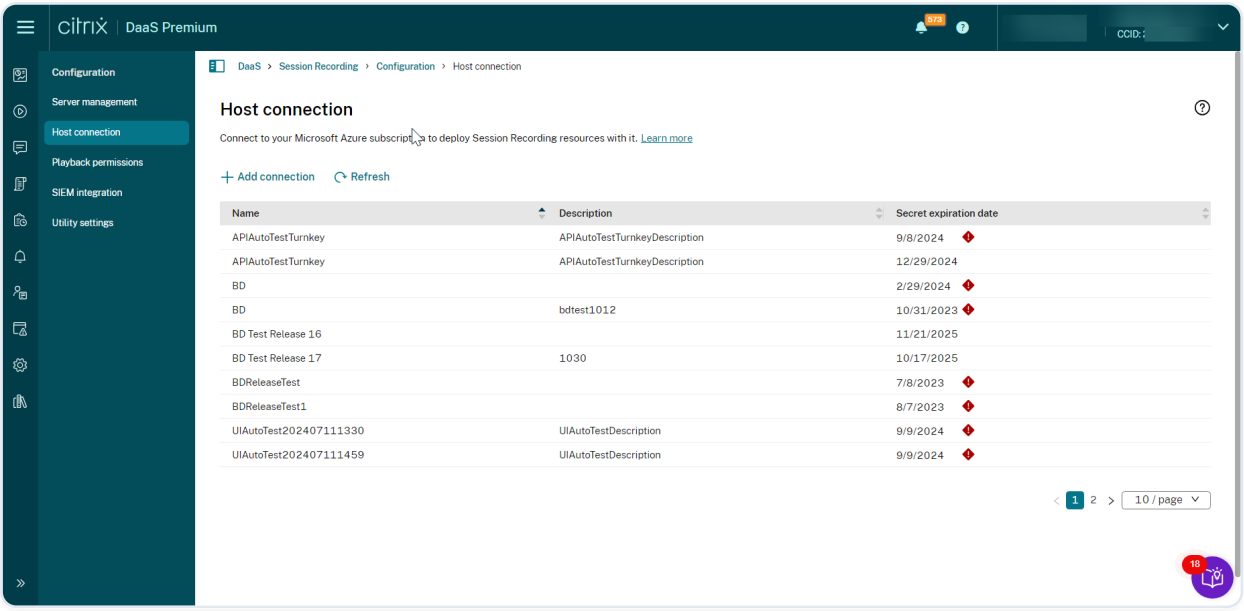
To add a host connection, complete the following steps:

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**.

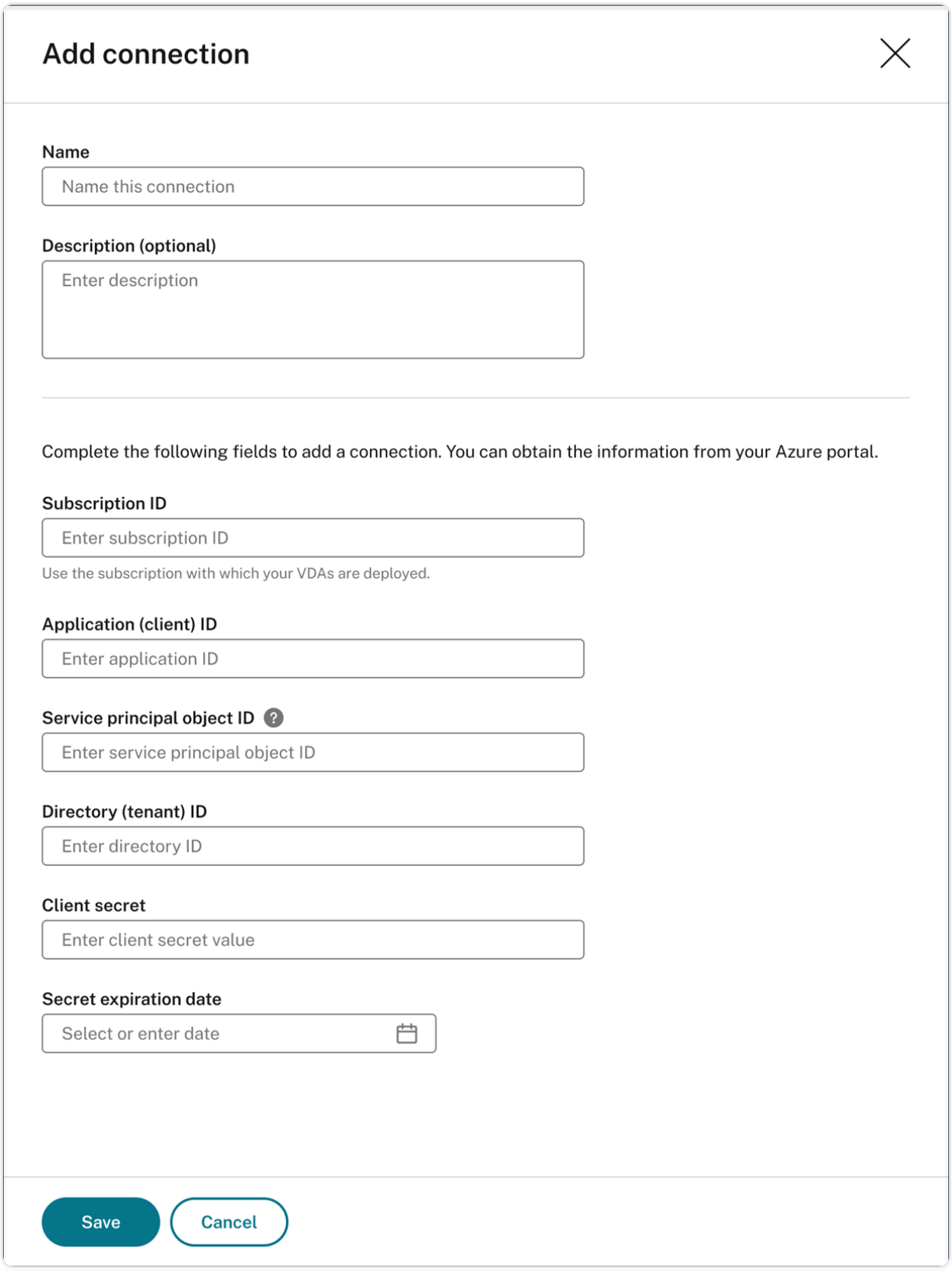


   To access the **Host Connection** page, select **Configuration > Host Connection** from the left navigation of the Session Recording service:



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

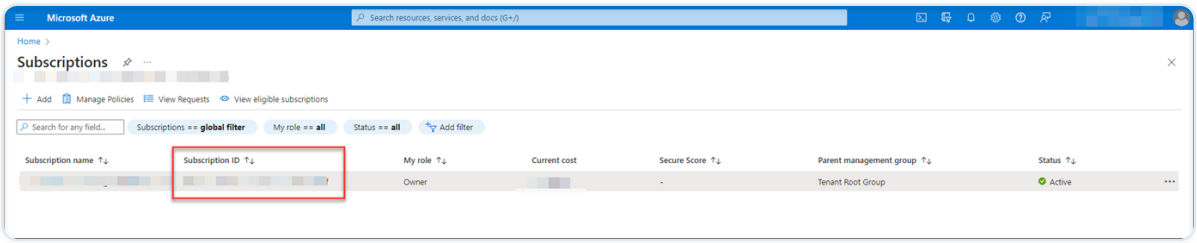


To find your Azure subscription ID, do the following:

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**:

```
<#

.SYNOPSIS

    Copyright (c) Citrix Systems, Inc. All Rights Reserved.

.DESCRIPTION

    Create Azure app registrations and give proper permissions
for Citrix Session Recording service deployment

.Parameter azureTenantID

.Parameter azureSubscriptionID

.Parameter appName

.Parameter role

#>
```

```
[CmdletBinding()]

Param(

    [Parameter(Mandatory = $true)] [String] $tenantId,

    [Parameter(Mandatory = $true)] [String] $subscriptionId,

    [Parameter(Mandatory = $true)] [String] $appName,

    [Parameter(Mandatory = $true)] [String] $role

)



if ($role -ne "Citrix Session Recording service" -and $role -ne
"Citrix Session Recording Deployment" -and $role -ne
"Contributor") {

    throw [System.Exception] "Invalid role '$role', only support
'Citrix Session Recording service', 'Citrix Session Recording
Deployment', and 'Contributor'."

}



try {

    Get-InstalledModule -Name "Az.Accounts" -ErrorAction Stop

}

catch {

    Install-Module -Name "Az.Accounts" -Scope CurrentUser
-Repository PSGallery -SkipPublisherCheck -Force

}

try {
```

```
    Get-InstalledModule -Name "Az.Resources" -ErrorAction Stop

}

catch {

    Install-Module -Name "Az.Resources" -Scope CurrentUser
-Repository PSGallery -SkipPublisherCheck -Force

}



Connect-AzAccount -TenantId $tenantId -Subscription
$subscriptionId



try {



    $azureAdApplication = Get-AzADApplication -DisplayName
$appName

    if ($null -eq $azureAdApplication) {

        Write-Host "Create a new app registration for Citrix
Session Recording" -ForegroundColor Green

        $azureAdApplication = New-AzADApplication -DisplayName
$appName -AvailableToOtherTenants $false

    }

    else {

        Write-Host "App registration '$appName' already exists."
-ForegroundColor Yellow

    }
```

```
    $azureAdApplicationServicePrincipal = Get-
AzADServicePrincipal -DisplayName $appName

    if($null -eq $azureAdApplicationServicePrincipal) {

        $azureAdApplicationServicePrincipal = New-
AzADServicePrincipal -AppId $azureAdApplication.AppId

        Write-Host "Create a service principal for app
registration '$appName'" -ForegroundColor Green

    }else{

        Write-Host "Service principal already exists for app
registration '$appName'" -ForegroundColor Yellow

    }



    if ($role -eq "Citrix Session Recording service" -or $role
-eq "Citrix Session Recording Deployment") {

        $rootPath = Get-Location

        $customRolePath = $(Join-Path -Path $rootPath -ChildPath
"sessionrecording.json") | Resolve-Path

        $customRoleJson = Get-Content $customRolePath |
ConvertFrom-Json

        $customRoleJson.AssignableScopes[0] = "/subscriptions/" +
$subscriptionId

        $tmpCustomRolePath = Join-Path -Path $rootPath -ChildPath
"sessionrecording_tmp.json"



        $roleDef = Get-AzRoleDefinition -Name $role

        if ($null -eq $roleDef) {
```

```
            try {

                $customRoleJson | ConvertTo-Json -depth 32 | Set-
Content $tmpCustomRolePath

                Write-Host "Create a custom role '$role'"
-ForegroundColor Green

                New-AzRoleDefinition -InputFile
$tmpCustomRolePath

            }

            catch {

                Write-Host "Failed to create custom role, error:
$_" -ForegroundColor Red

                throw $_.Exception

            }

        }

        else {

            try {

                $customRoleJson | Add-Member -MemberType
NoteProperty -Name 'id' -Value $($roleDef.Id)

                $customRoleJson | ConvertTo-Json -depth 32 | Set-
Content $tmpCustomRolePath

                Write-Host "Upadate the custom role '$role'"
-ForegroundColor Green

                Set-AzRoleDefinition -InputFile
$tmpCustomRolePath

            }

            catch {
```

```
                Write-Host "Failed to update custom role, error:
$_" -ForegroundColor Red

                throw $_.Exception

            }

        }

    }



    $roleAssignment = Get-AzRoleAssignment -RoleDefinitionName
$role -ObjectId $($azureAdApplicationServicePrincipal.Id)

    if ($null -eq $roleAssignment) {

        Write-Host "Assign role '$role' to app '$appName'"
-ForegroundColor Green

        New-AzRoleAssignment -RoleDefinitionName $role
-ApplicationId $azureAdApplication.AppId

    }

    else {

        Write-Host "Role '$role' already assigned to app
'$appName'" -ForegroundColor Yellow

    }



    Write-Host "Tenant ID:                    $tenantId"
-ForegroundColor Green

    Write-Host "Subscription ID:              $subscriptionId"
-ForegroundColor Green

    Write-Host "Application ID:               $
($azureAdApplication.AppId)" -ForegroundColor Green
```

```
    Write-Host "Service principal object ID: $
($azureAdApplicationServicePrincipal.Id)" -ForegroundColor Green

}

catch {

    Write-Host "Failed to assign role assignment to this app,
error: $_" -ForegroundColor Red

    Write-Host "Please make sure the current azure admin has
permission to assign roles" -ForegroundColor Red

}
```

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.

```
{

    "name": "Citrix Session Recording service",

    "description": "This role has permissions which allow Citrix
Session Recording service to deploy Session Recording resources
using a host connection.",

    "assignableScopes": [

        "/subscriptions/*"

    ],

    "actions": [

        "Microsoft.Compute/availabilitySets/write",

        "Microsoft.Compute/virtualMachines/delete",

        "Microsoft.Compute/virtualMachines/extensions/read",

        "Microsoft.Compute/virtualMachines/extensions/write",
```

```
        "Microsoft.Compute/virtualMachines/read",
        "Microsoft.Compute/virtualMachines/runCommands/read",
        "Microsoft.Compute/virtualMachines/runCommands/write",
        "Microsoft.Compute/virtualMachines/write",
        "Microsoft.CostManagement/forecast/read",
        "Microsoft.CostManagement/query/read",
        "Microsoft.KeyVault/locations/deletedVaults/purge/
action",
        "Microsoft.KeyVault/vaults/
PrivateEndpointConnectionsApproval/action",
        "Microsoft.KeyVault/vaults/read",
        "Microsoft.KeyVault/vaults/secrets/read",
        "Microsoft.KeyVault/vaults/secrets/write",
        "Microsoft.KeyVault/vaults/write",
        "Microsoft.ManagedIdentity/userAssignedIdentities/assign/
action",
        "Microsoft.ManagedIdentity/userAssignedIdentities/read",
        "Microsoft.ManagedIdentity/userAssignedIdentities/write",
        "Microsoft.Network/dnsForwardingRulesets/forwardingRules/
read",
        "Microsoft.Network/dnsForwardingRulesets/forwardingRules/
write",
        "Microsoft.Network/dnsForwardingRulesets/read",
        "Microsoft.Network/dnsForwardingRulesets/
virtualNetworkLinks/read",
```

```
        "Microsoft.Network/dnsForwardingRulesets/
virtualNetworkLinks/write",

        "Microsoft.Network/dnsForwardingRulesets/write",

        "Microsoft.Network/dnsResolvers/outboundEndpoints/join/
action",

        "Microsoft.Network/dnsResolvers/outboundEndpoints/read",

        "Microsoft.Network/dnsResolvers/outboundEndpoints/write",

        "Microsoft.Network/dnsResolvers/read",

        "Microsoft.Network/dnsResolvers/write",

        "Microsoft.Network/loadBalancers/backendAddressPools/
join/action",

        "Microsoft.Network/loadBalancers/read",

        "Microsoft.Network/loadBalancers/write",

        "Microsoft.Network/networkInterfaces/join/action",

        "Microsoft.Network/networkInterfaces/read",

        "Microsoft.Network/networkInterfaces/write",

        "Microsoft.Network/networkSecurityGroups/delete",

        "Microsoft.Network/networkSecurityGroups/join/action",

        "Microsoft.Network/networkSecurityGroups/read",

        "Microsoft.Network/networkSecurityGroups/securityRules/
read",

        "Microsoft.Network/networkSecurityGroups/securityRules/
write",

        "Microsoft.Network/networkSecurityGroups/write",
```

```
        "Microsoft.Network/privateDnsZones/join/action",
        "Microsoft.Network/privateDnsZones/read",
        "Microsoft.Network/privateDnsZones/virtualNetworkLinks/
read",
        "Microsoft.Network/privateDnsZones/virtualNetworkLinks/
write",
        "Microsoft.Network/privateDnsZones/write",
        "Microsoft.Network/privateEndpoints/privateDnsZoneGroups/
read",
        "Microsoft.Network/privateEndpoints/privateDnsZoneGroups/
write",
        "Microsoft.Network/privateEndpoints/read",
        "Microsoft.Network/privateEndpoints/write",
        "Microsoft.Network/publicIPAddresses/join/action",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/virtualNetworks/join/action",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Network/virtualNetworks/subnets/read",
        "Microsoft.Resources/deployments/operationstatuses/read",
        "Microsoft.Resources/deployments/read",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/subscriptions/resourceGroups/
```

```
delete",
        "Microsoft.Resources/subscriptions/resourceGroups/read",
        "Microsoft.Resources/subscriptions/resourceGroups/write",
        "Microsoft.Sql/servers/auditingSettings/write",
        "Microsoft.Sql/servers/databases/write",
        "Microsoft.Sql/servers/firewallRules/write",
        "Microsoft.Sql/servers/
privateEndpointConnectionsApproval/action",
        "Microsoft.Sql/servers/read",
        "Microsoft.Sql/servers/write",
        "Microsoft.Storage/storageAccounts/
PrivateEndpointConnectionsApproval/action",
        "Microsoft.Storage/storageAccounts/fileServices/shares/
delete",
        "Microsoft.Storage/storageAccounts/fileServices/shares/
read",
        "Microsoft.Storage/storageAccounts/fileServices/shares/
write",
        "Microsoft.Storage/storageAccounts/listkeys/action",
        "Microsoft.Storage/storageAccounts/read",
        "Microsoft.Storage/storageAccounts/write"
    ],
    "NotActions": [],
    "DataActions": [],
    "NotDataActions": []
```

```
}
```

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:

```
```

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

```
```

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

```
```

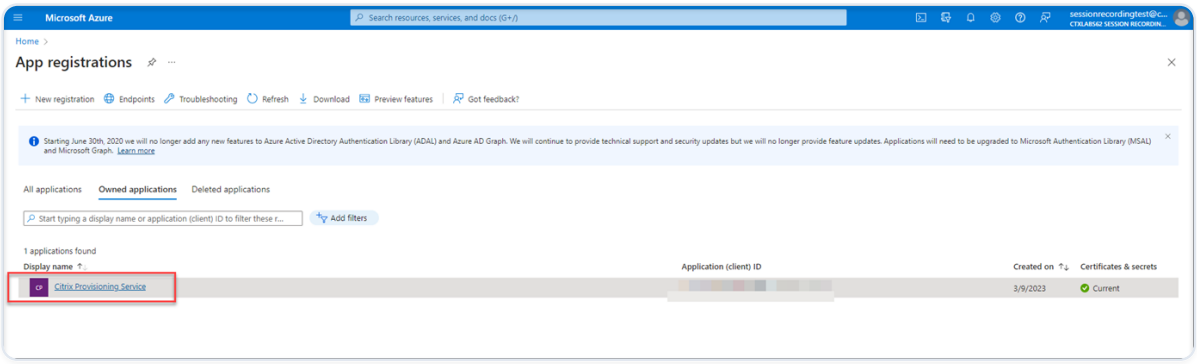
.\AppRegistration.ps1 -tenantId <tenant ID> -subscriptionId
<subscription ID> -appName <application name> -role "Contributor"

```
```

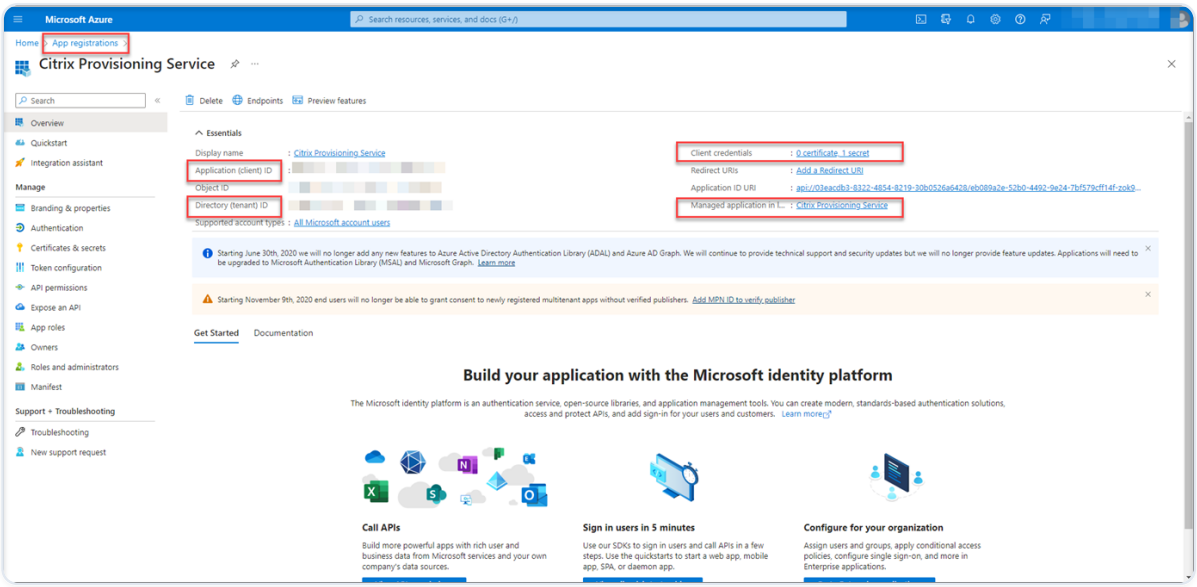
Method 2:

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**.

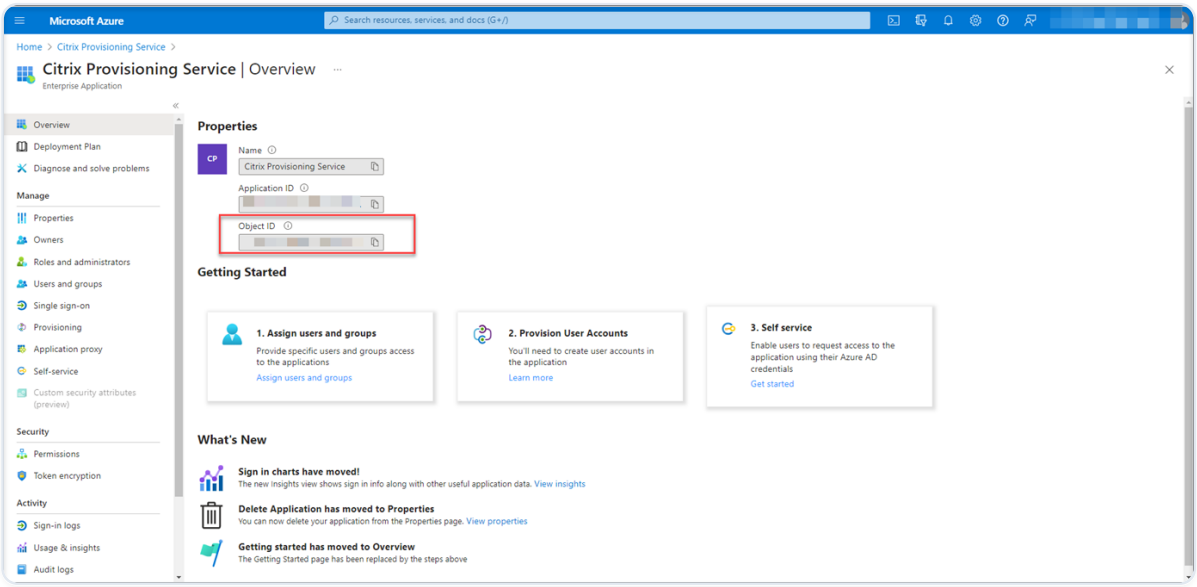
b. Click the display name of your application.



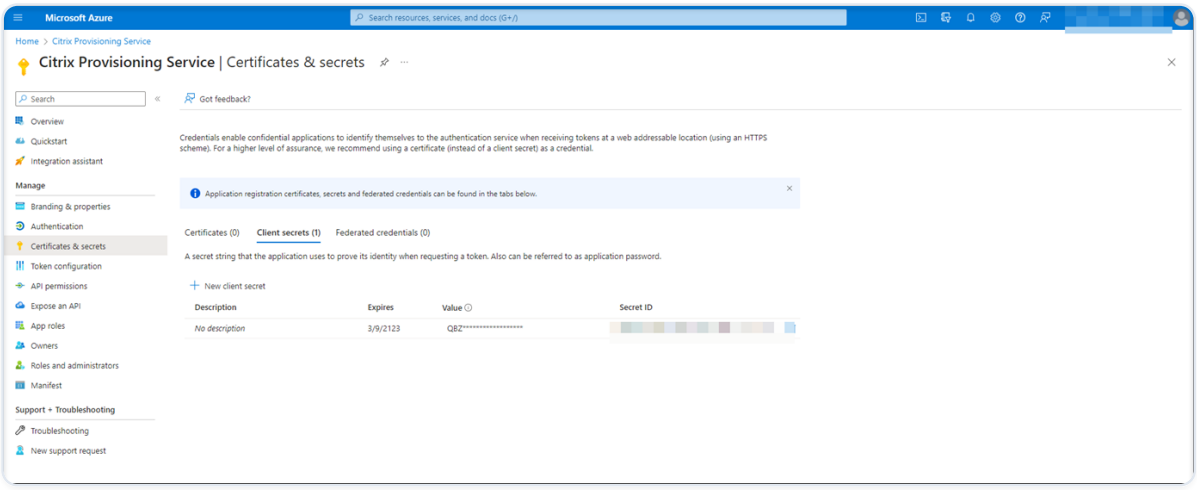
c. On the overview page, find the application (client) ID and directory (tenant) ID. Click the link next to **Managed application in local directory** to find the ID of the service principal object associated with the application. Click the link next to **Client credentials** to find the client secret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



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



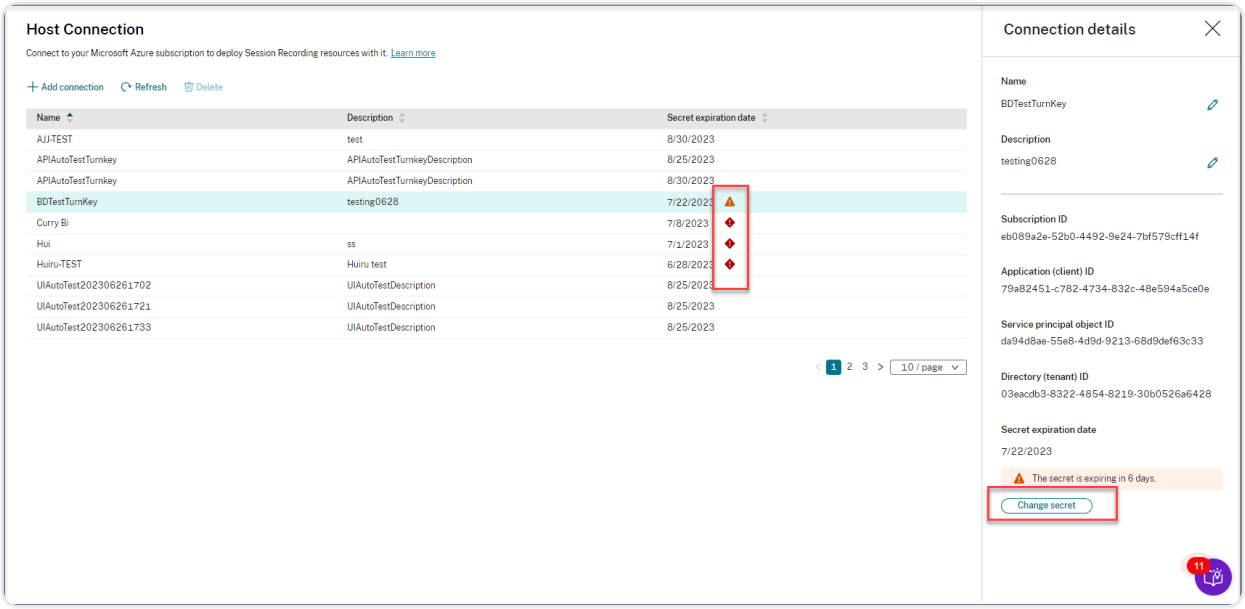
For example, the client secret ID and its expiration date:



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.



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.

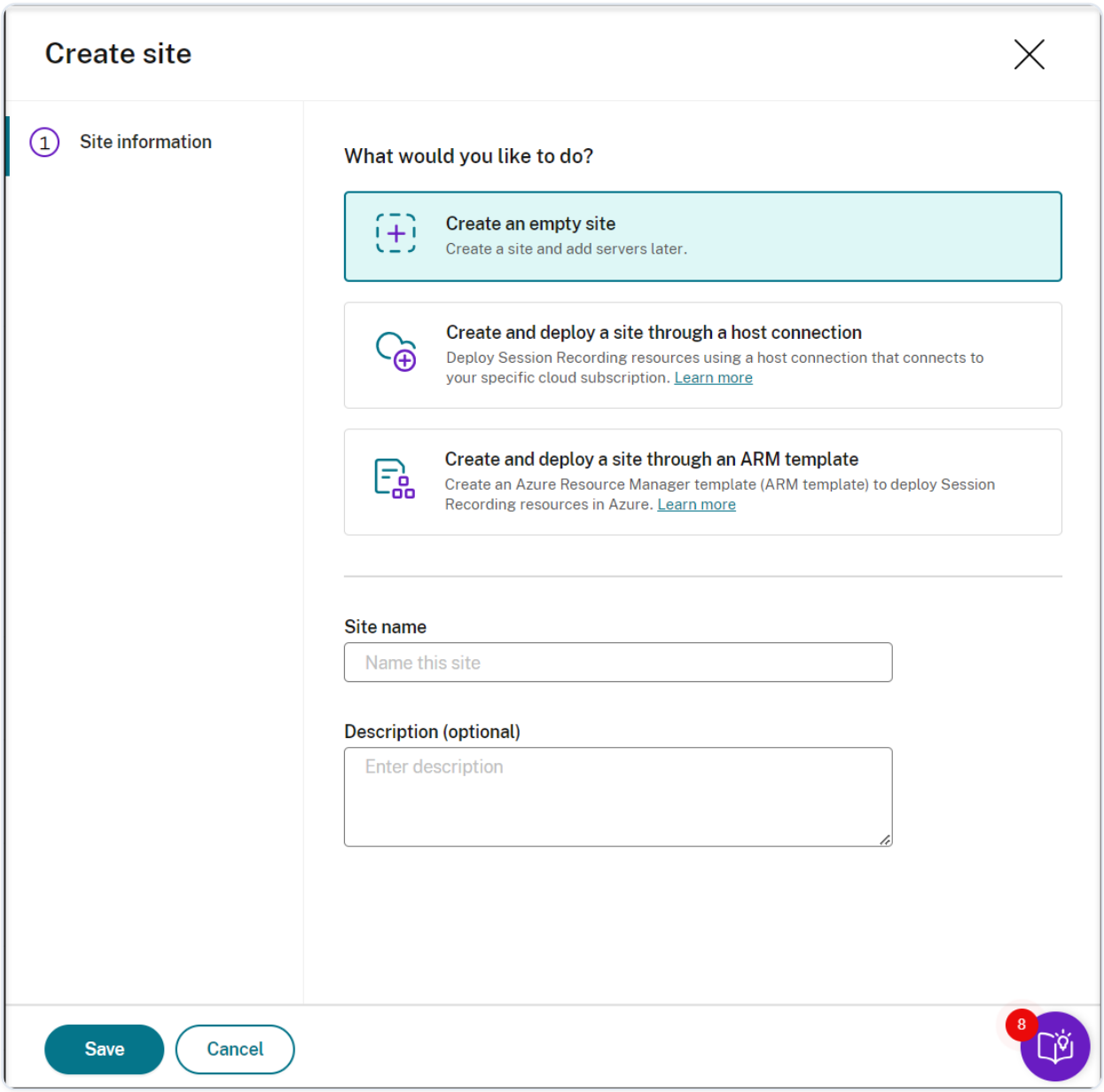
2. Download and unzip the ARM template. Run the deployment script in the unzipped template folder to start deploying the recourses specified in the template to Azure.
3. Check the deployment progress in Azure. After the deployment is complete, set up Session Recording to get it up and running. To set 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:

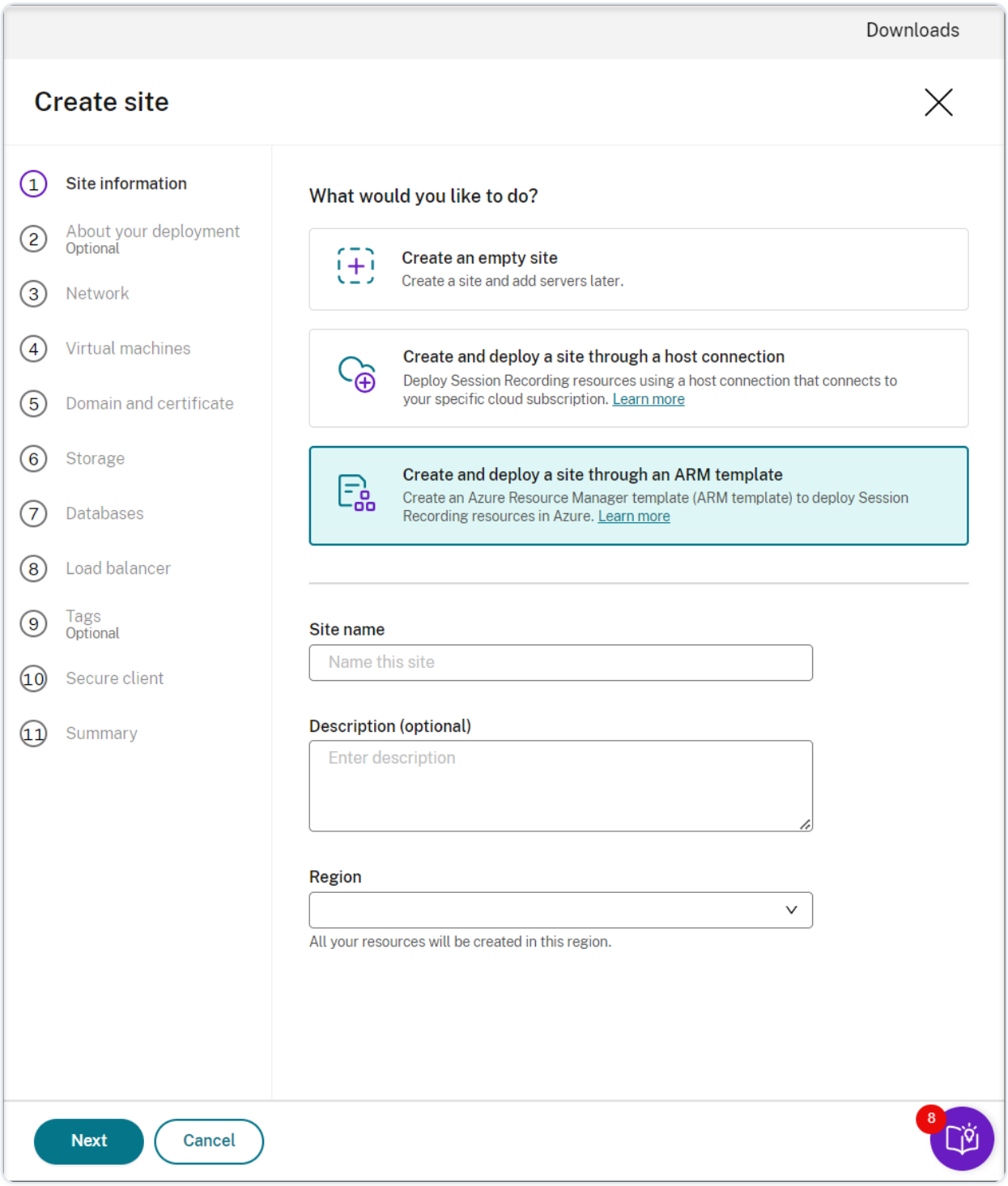
1. Select **Configuration > Server Management** from the left navigation of the Session Recording service.



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

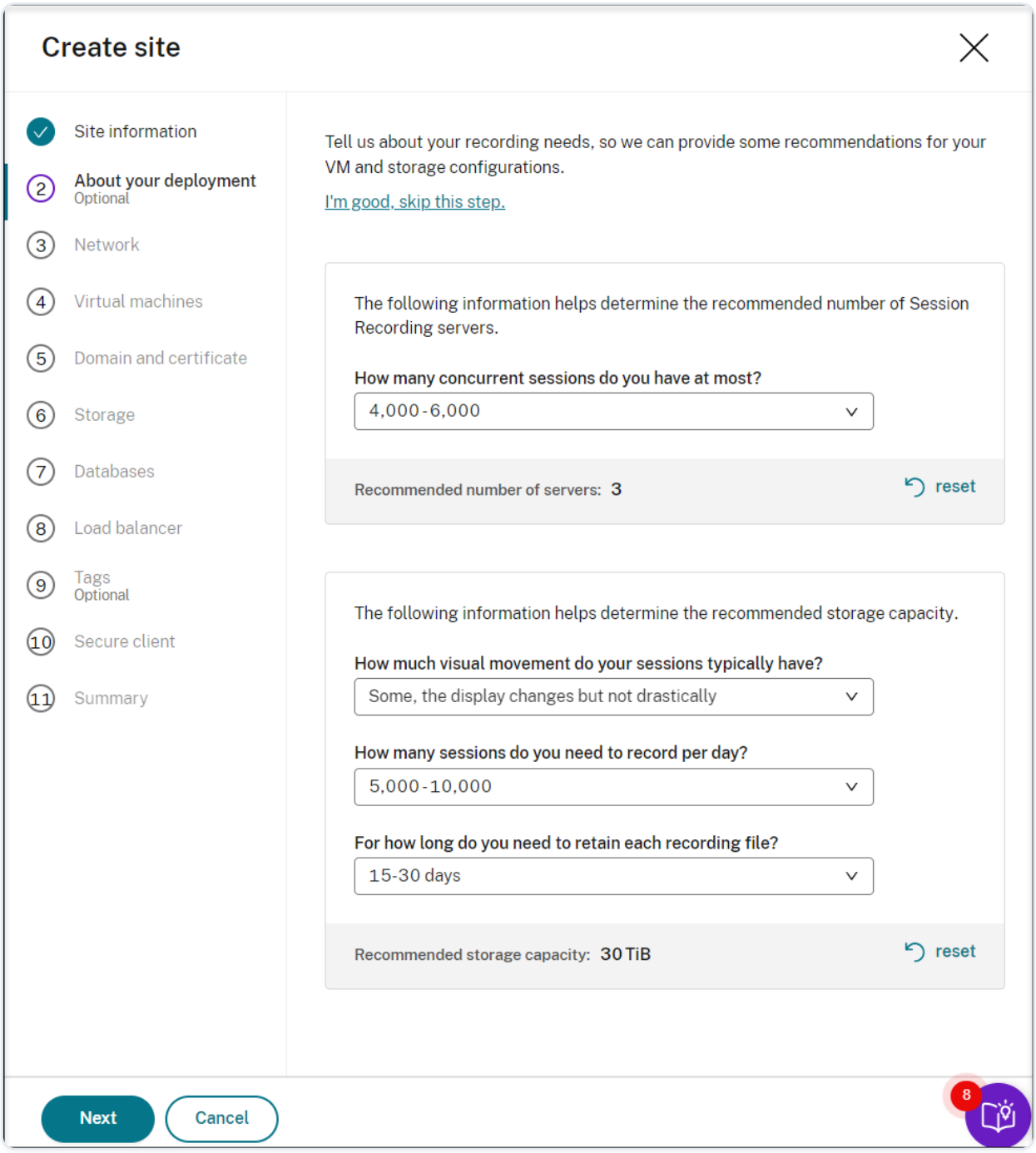


3. Select **Create and deploy a site through an ARM template**. The main steps are listed in the left navigation.



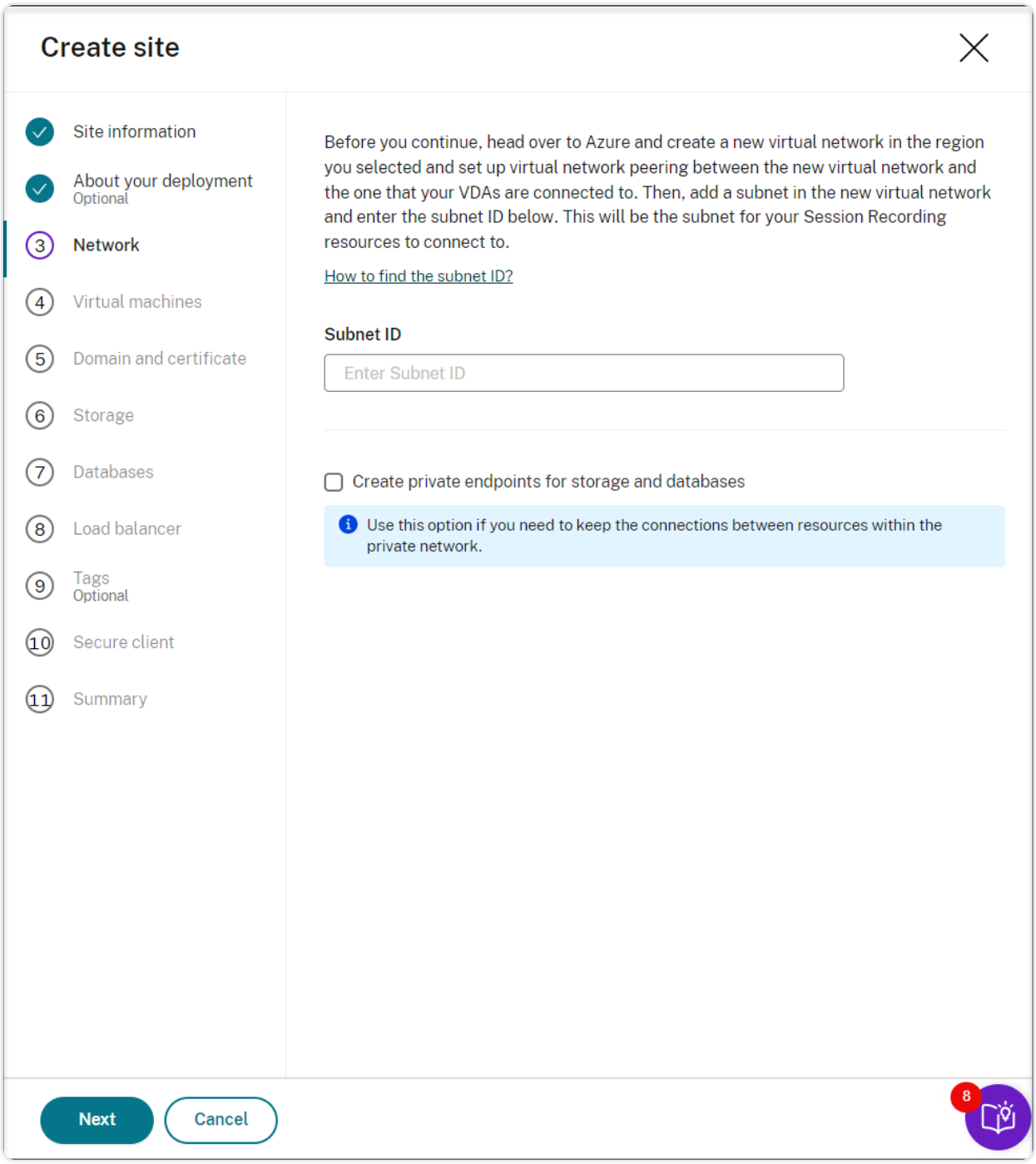
4. Enter a site name and description, and then click **Next**.
5. (Optional) To get recommendations for VM and storage configurations, provide information about your recording needs.

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



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.

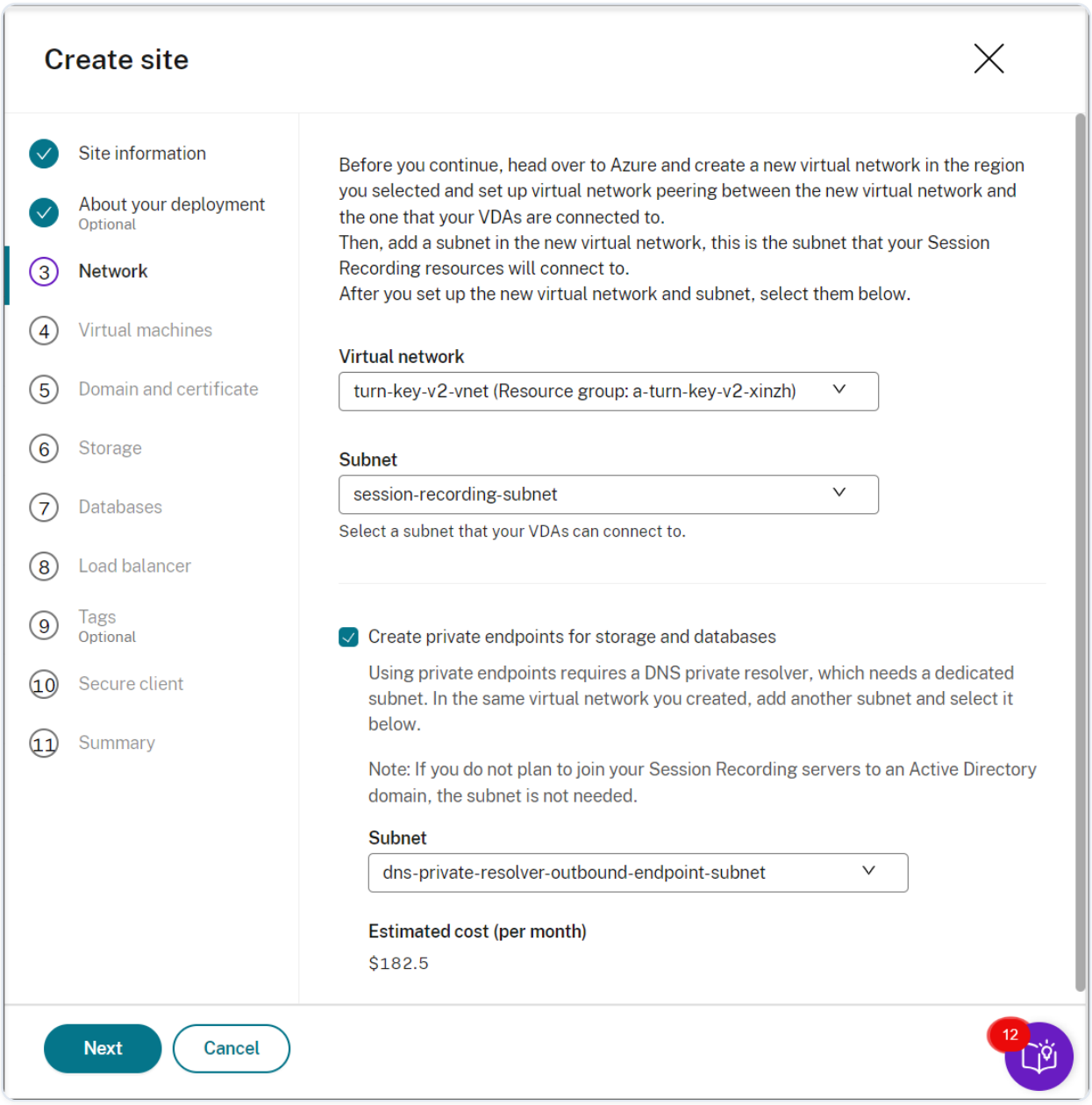
6. Go to the Azure portal and create a new virtual network in the region you selected and set up virtual network peering between the new virtual network and the one that your VDAs are connected to. Then, add a subnet in the new virtual network. Find and enter the subnet ID below.



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.



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**:

```
<#

.SYNOPSIS

    Copyright (c) Citrix Systems, Inc. All Rights Reserved.
```

```
.DESCRIPTION

    Create Azure app registrations and give proper permissions for
Citrix Session Recording service deployment

.Parameter azureTenantID

.Parameter azureSubscriptionID

.Parameter appName

.Parameter role

#>



[CmdletBinding()]

Param(

    [Parameter(Mandatory = $true)] [String] $tenantId,

    [Parameter(Mandatory = $true)] [String] $subscriptionId,

    [Parameter(Mandatory = $true)] [String] $appName,

    [Parameter(Mandatory = $true)] [String] $role

)



if ($role -ne "Citrix Session Recording service" -and $role -ne
"Citrix Session Recording Deployment" -and $role -ne "Contributor")
{

    throw [System.Exception] "Invalid role '$role', only support
'Citrix Session Recording service', 'Citrix Session Recording
Deployment', and 'Contributor'."

}
```

```
try {
    Get-InstalledModule -Name "Az.Accounts" -ErrorAction Stop
}
catch {
    Install-Module -Name "Az.Accounts" -Scope CurrentUser
-Repository PSGallery -SkipPublisherCheck -Force
}
try {
    Get-InstalledModule -Name "Az.Resources" -ErrorAction Stop
}
catch {
   Install-Module -Name "Az.Resources" -Scope CurrentUser
-Repository PSGallery -SkipPublisherCheck -Force
}

Connect-AzAccount -TenantId $tenantId -Subscription $subscriptionId

try {

    $azureAdApplication = Get-AzADApplication -DisplayName $appName
    if ($null -eq $azureAdApplication) {
        Write-Host "Create a new app registration for Citrix Session
Recording" -ForegroundColor Green
```

```
        $azureAdApplication = New-AzADApplication -DisplayName
$appName -AvailableToOtherTenants $false

    }

    else {

        Write-Host "App registration '$appName' already exists."
-ForegroundColor Yellow

    }



    $azureAdApplicationServicePrincipal = Get-AzADServicePrincipal
-DisplayName $appName

    if($null -eq $azureAdApplicationServicePrincipal) {

        $azureAdApplicationServicePrincipal = New-
AzADServicePrincipal -AppId $azureAdApplication.AppId

        Write-Host "Create a service principal for app registration
'$appName'" -ForegroundColor Green

    }else{

        Write-Host "Service principal already exists for app
registration '$appName'" -ForegroundColor Yellow

    }



    if ($role -eq "Citrix Session Recording service" -or $role -eq
"Citrix Session Recording Deployment") {

        $rootPath = Get-Location

        $customRolePath = $(Join-Path -Path $rootPath -ChildPath
"sessionrecordingdeployment.json") | Resolve-Path

        $customRoleJson = Get-Content $customRolePath | ConvertFrom-
```

```
Json

        $customRoleJson.AssignableScopes[0] = "/subscriptions/" +
$subscriptionId

        $tmpCustomRolePath = Join-Path -Path $rootPath -ChildPath
"sessionrecording_tmp.json"



        $roleDef = Get-AzRoleDefinition -Name $role

        if ($null -eq $roleDef) {

            try {

                $customRoleJson | ConvertTo-Json -depth 32 | Set-
Content $tmpCustomRolePath

                Write-Host "Create a custom role '$role'"
-ForegroundColor Green

                New-AzRoleDefinition -InputFile $tmpCustomRolePath

            }

            catch {

                Write-Host "Failed to create custom role, error: $_"
-ForegroundColor Red

                throw $_.Exception

            }

        }

        else {

            try {

                $customRoleJson | Add-Member -MemberType
NoteProperty -Name 'id' -Value $($roleDef.Id)
```

```
                $customRoleJson | ConvertTo-Json -depth 32 | Set-
Content $tmpCustomRolePath

                Write-Host "Upadate the custom role '$role'"
-ForegroundColor Green

                Set-AzRoleDefinition -InputFile $tmpCustomRolePath

            }

            catch {

                Write-Host "Failed to update custom role, error: $_"
-ForegroundColor Red

                throw $_.Exception

            }

        }

    }



    $roleAssignment = Get-AzRoleAssignment -RoleDefinitionName $role
-ObjectId $($azureAdApplicationServicePrincipal.Id)

    if ($null -eq $roleAssignment) {

        Write-Host "Assign role '$role' to app '$appName'"
-ForegroundColor Green

        New-AzRoleAssignment -RoleDefinitionName $role
-ApplicationId $azureAdApplication.AppId

    }

    else {

        Write-Host "Role '$role' already assigned to app '$appName'"
-ForegroundColor Yellow
```

```
    }



    Write-Host "Tenant ID:                    $tenantId"
-ForegroundColor Green

    Write-Host "Subscription ID:              $subscriptionId"
-ForegroundColor Green

    Write-Host "Application ID:               $
($azureAdApplication.AppId)" -ForegroundColor Green

    Write-Host "Service principal object ID: $
($azureAdApplicationServicePrincipal.Id)" -ForegroundColor Green

}

catch {

    Write-Host "Failed to assign role assignment to this app, error:
$_" -ForegroundColor Red

    Write-Host "Please make sure the current azure admin has
permission to assign roles" -ForegroundColor Red

}
```

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.

```
{

    "name": "Citrix Session Recording Deployment",

    "description": "This role has permissions which allow users to
deploy Session Recording resources using an Azure Resource Manager
template (ARM template). ",

    "assignableScopes": [

      "/subscriptions/*"
```

```
    ],
    "actions": [
      "Microsoft.Compute/availabilitySets/write",
      "Microsoft.Compute/virtualMachines/extensions/read",
      "Microsoft.Compute/virtualMachines/extensions/write",
      "Microsoft.Compute/virtualMachines/read",
      "Microsoft.Compute/virtualMachines/runCommands/read",
      "Microsoft.Compute/virtualMachines/runCommands/write",
      "Microsoft.Compute/virtualMachines/write",
      "Microsoft.ContainerInstance/containerGroups/read",
      "Microsoft.ContainerInstance/containerGroups/write",
      "Microsoft.KeyVault/vaults/PrivateEndpointConnectionsApproval/
action",
      "Microsoft.KeyVault/vaults/read",
      "Microsoft.KeyVault/vaults/secrets/read",
      "Microsoft.KeyVault/vaults/secrets/write",
      "Microsoft.KeyVault/vaults/write",
      "Microsoft.ManagedIdentity/userAssignedIdentities/assign/
action",
      "Microsoft.ManagedIdentity/userAssignedIdentities/read",
      "Microsoft.ManagedIdentity/userAssignedIdentities/write",
      "Microsoft.Network/dnsForwardingRulesets/forwardingRules/
read",
```

```
      "Microsoft.Network/dnsForwardingRulesets/forwardingRules/
write",

      "Microsoft.Network/dnsForwardingRulesets/read",

      "Microsoft.Network/dnsForwardingRulesets/virtualNetworkLinks/
read",

      "Microsoft.Network/dnsForwardingRulesets/virtualNetworkLinks/
write",

      "Microsoft.Network/dnsForwardingRulesets/write",

      "Microsoft.Network/dnsResolvers/outboundEndpoints/join/
action",

      "Microsoft.Network/dnsResolvers/outboundEndpoints/read",

      "Microsoft.Network/dnsResolvers/outboundEndpoints/write",

      "Microsoft.Network/dnsResolvers/read",

      "Microsoft.Network/dnsResolvers/write",

      "Microsoft.Network/loadBalancers/backendAddressPools/join/
action",

      "Microsoft.Network/loadBalancers/write",

      "Microsoft.Network/networkInterfaces/join/action",

      "Microsoft.Network/networkInterfaces/read",

      "Microsoft.Network/networkInterfaces/write",

      "Microsoft.Network/networkSecurityGroups/join/action",

      "Microsoft.Network/networkSecurityGroups/read",

      "Microsoft.Network/networkSecurityGroups/securityRules/read",

      "Microsoft.Network/networkSecurityGroups/securityRules/write",
```

```
      "Microsoft.Network/networkSecurityGroups/write",
      "Microsoft.Network/privateDnsZones/join/action",
      "Microsoft.Network/privateDnsZones/read",
      "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
      "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
      "Microsoft.Network/privateDnsZones/write",
      "Microsoft.Network/privateEndpoints/privateDnsZoneGroups/
read",
      "Microsoft.Network/privateEndpoints/privateDnsZoneGroups/
write",
      "Microsoft.Network/privateEndpoints/read",
      "Microsoft.Network/privateEndpoints/write",
      "Microsoft.Network/publicIPAddresses/join/action",
      "Microsoft.Network/publicIPAddresses/read",
      "Microsoft.Network/publicIPAddresses/write",
      "Microsoft.Network/virtualNetworks/join/action",
      "Microsoft.Network/virtualNetworks/read",
      "Microsoft.Network/virtualNetworks/subnets/join/action",
      "Microsoft.Network/virtualNetworks/subnets/read",
      "Microsoft.Resources/deploymentScripts/read",
      "Microsoft.Resources/deploymentScripts/write",
      "Microsoft.Resources/deployments/operationstatuses/read",
      "Microsoft.Resources/deployments/read",
```

```
      "Microsoft.Resources/deployments/validate/action",
      "Microsoft.Resources/deployments/write",
      "Microsoft.Resources/subscriptions/resourceGroups/read",
      "Microsoft.Resources/subscriptions/resourceGroups/write",
      "Microsoft.Resources/templateSpecs/read",
      "Microsoft.Resources/templateSpecs/versions/read",
      "Microsoft.Resources/templateSpecs/versions/write",
      "Microsoft.Resources/templateSpecs/write",
      "Microsoft.Sql/servers/auditingSettings/write",
      "Microsoft.Sql/servers/databases/write",
      "Microsoft.Sql/servers/firewallRules/write",
      "Microsoft.Sql/servers/privateEndpointConnectionsApproval/
action",
      "Microsoft.Sql/servers/read",
      "Microsoft.Sql/servers/write",
      "Microsoft.Storage/storageAccounts/
PrivateEndpointConnectionsApproval/action",
      "Microsoft.Storage/storageAccounts/blobServices/containers/
read",
      "Microsoft.Storage/storageAccounts/blobServices/containers/
write",
      "Microsoft.Storage/storageAccounts/fileServices/shares/write",
      "Microsoft.Storage/storageAccounts/listkeys/action",
      "Microsoft.Storage/storageAccounts/read",
```

```
      "Microsoft.Storage/storageAccounts/write"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
```

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:

```
.\AppRegistration.ps1 -tenantId <tenant ID> -subscriptionId
<subscription ID> -appName <application name> -role "Citrix Session
Recording Deployment"
```

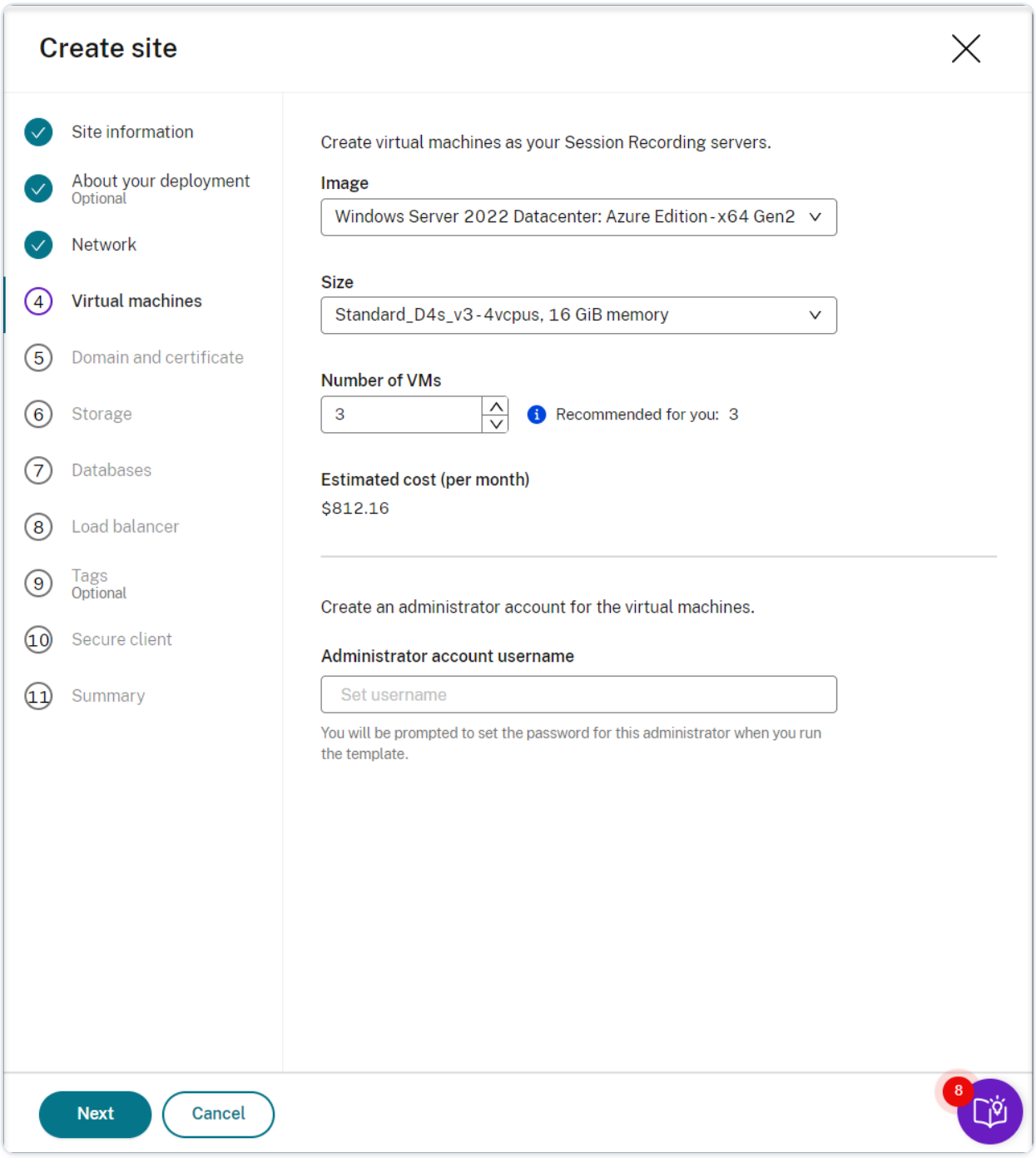
   To create an application and assign it the Azure built-in **Contributor** role, run:

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

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**.

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

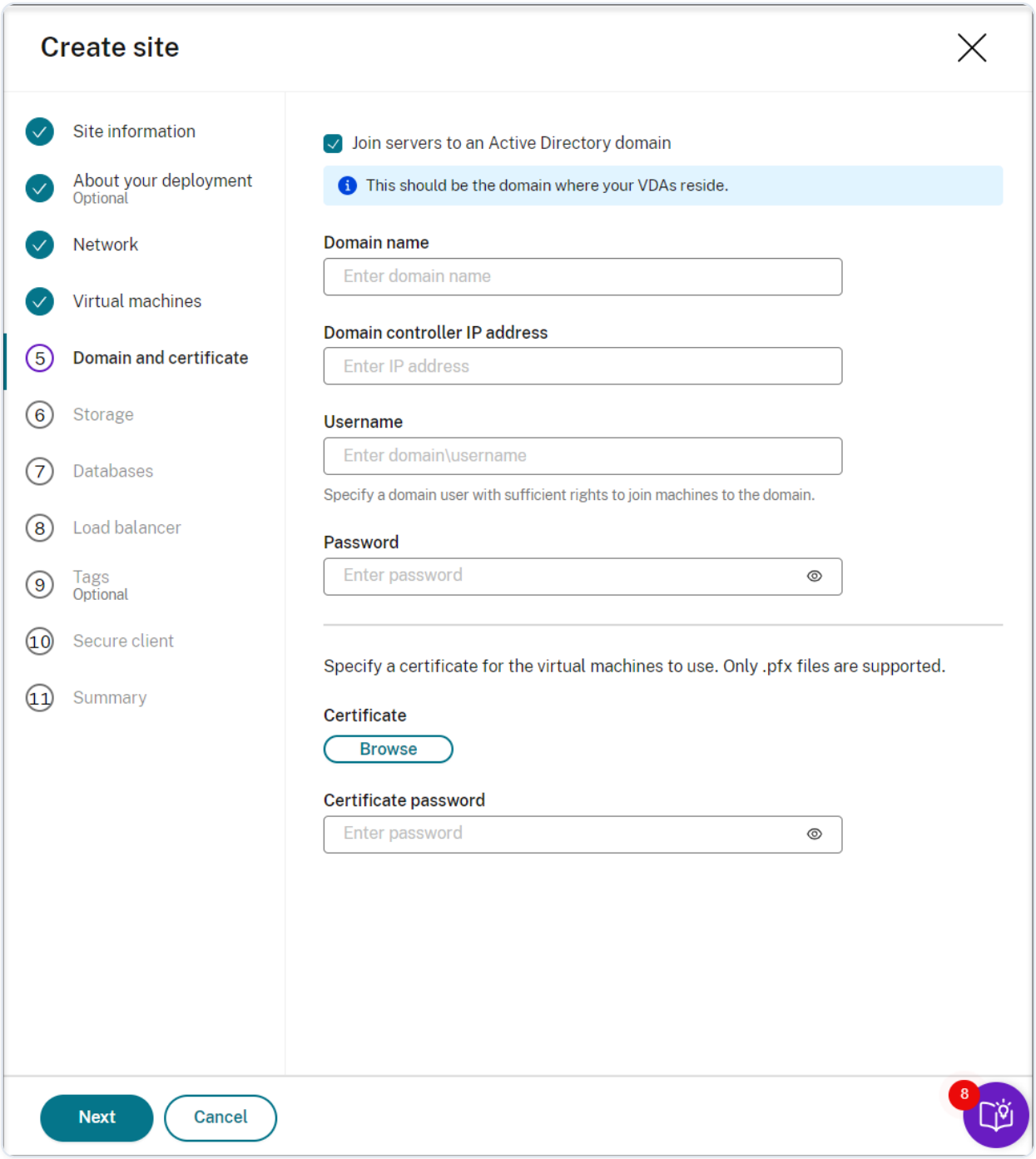


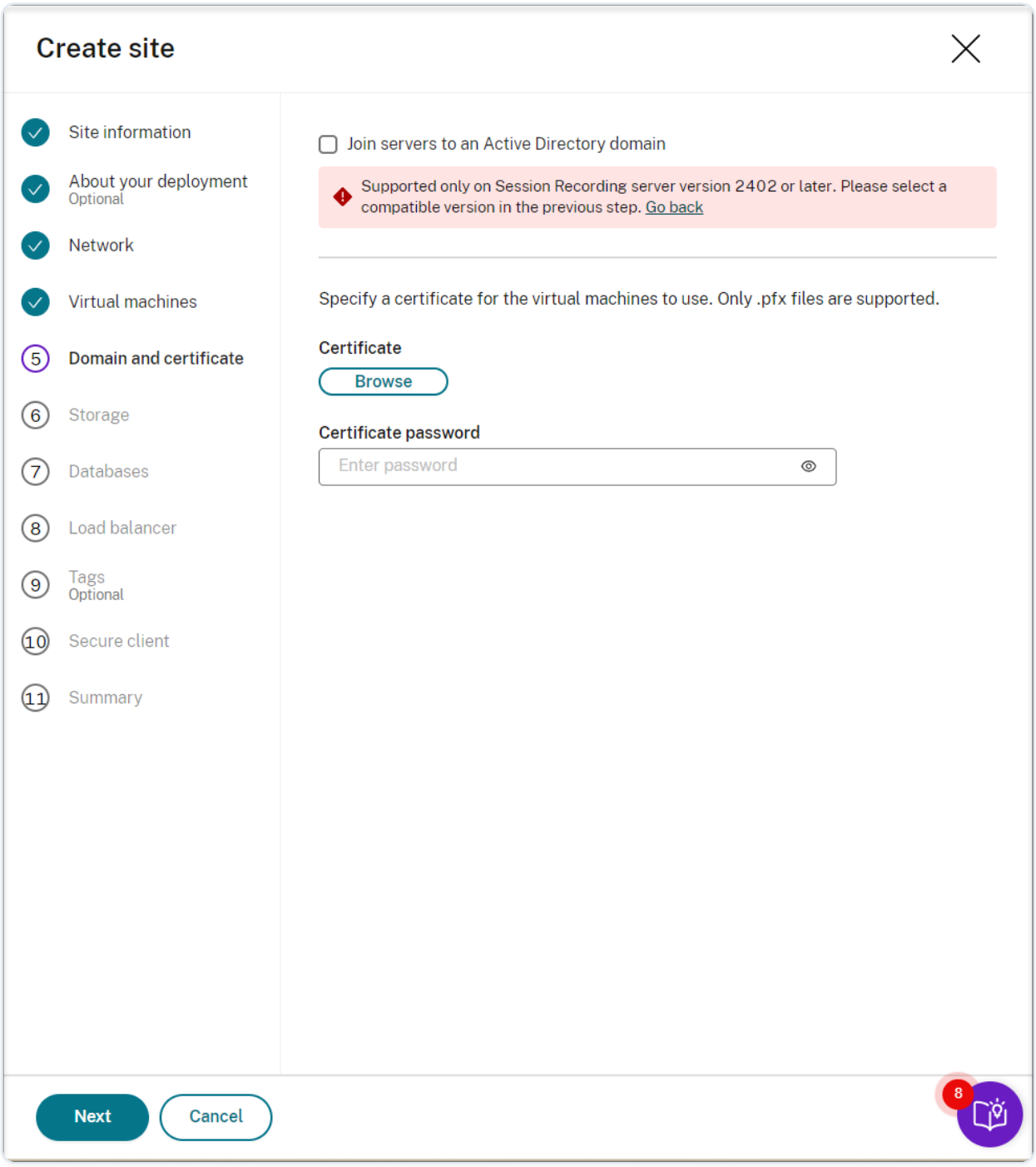
Note:

- 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.

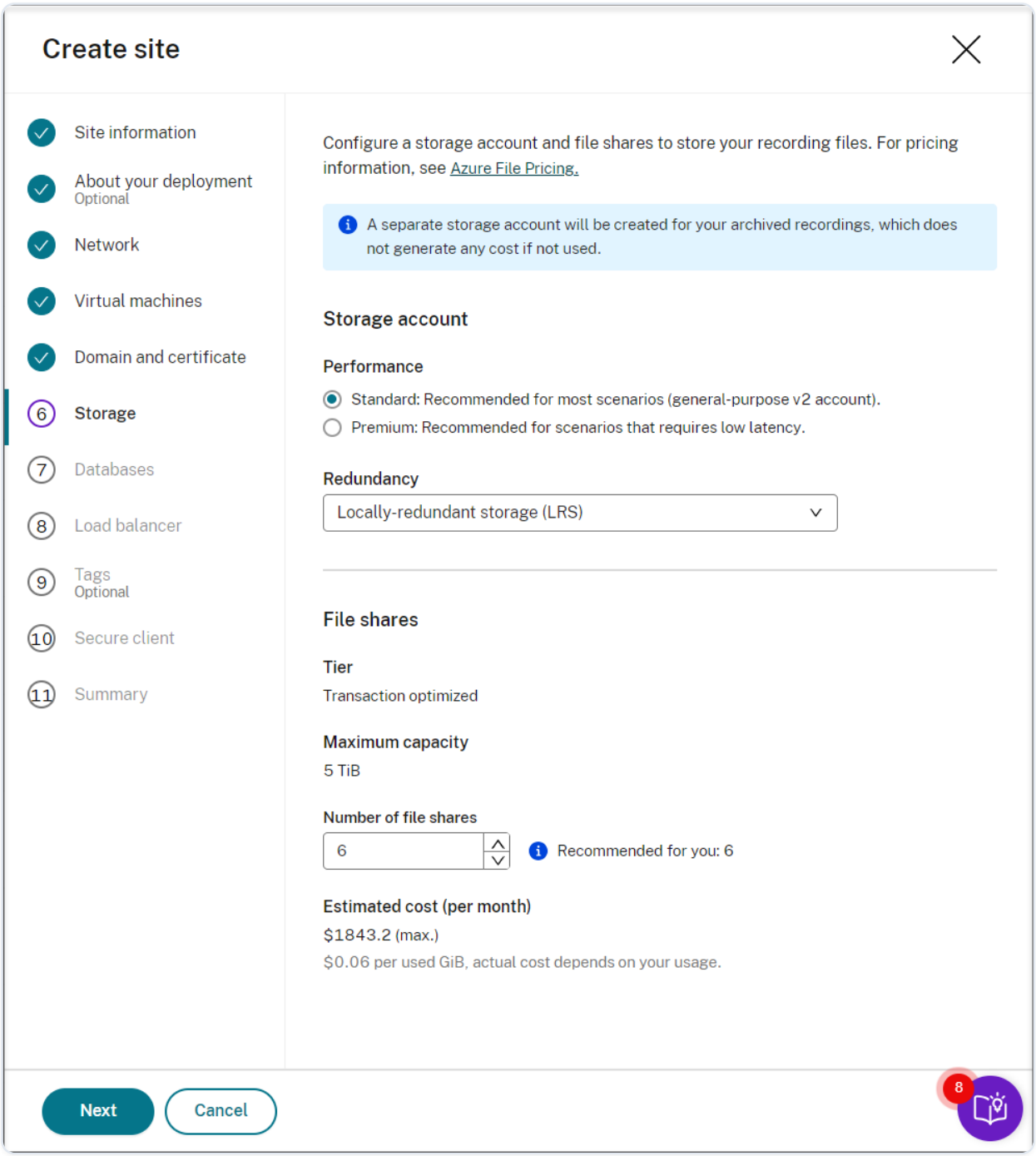
9. Join the Session Recording servers to the same domain with your VDAs and specify a certificate for the Session Recording servers.

   - 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.
   - 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.

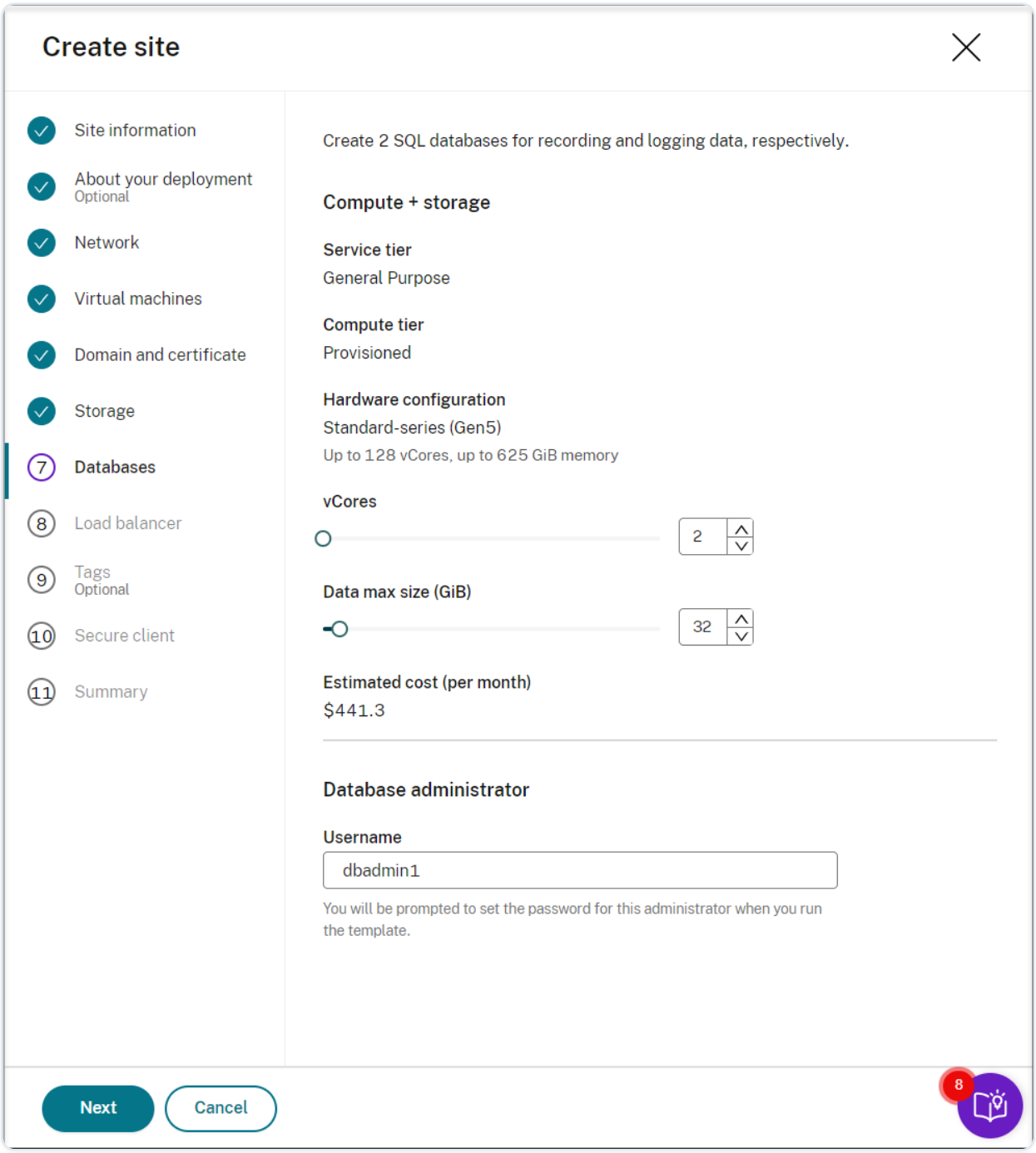




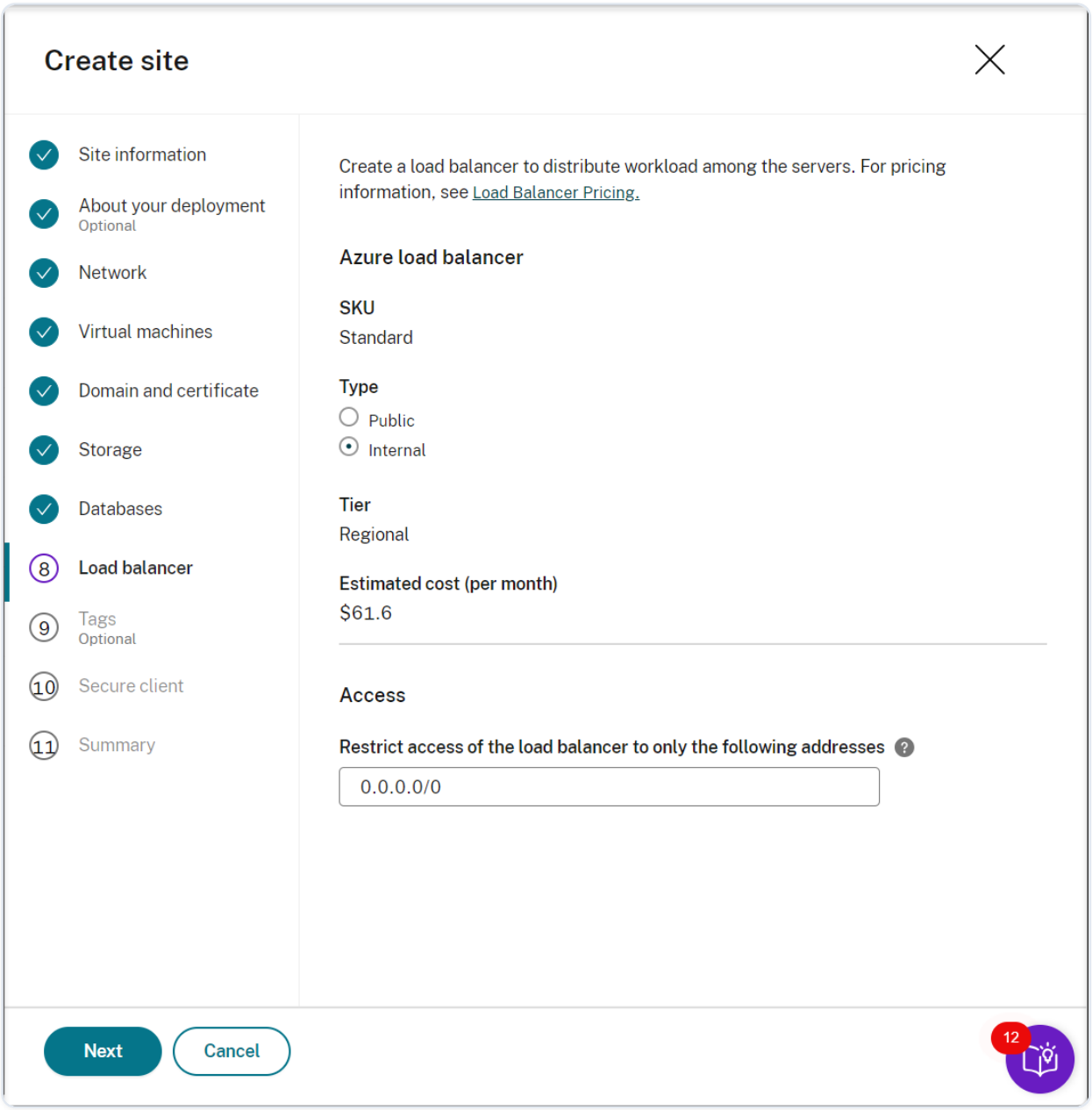
10. Configure an Azure storage account and file shares to store your recording files. For pricing information, see Azure Files pricing.



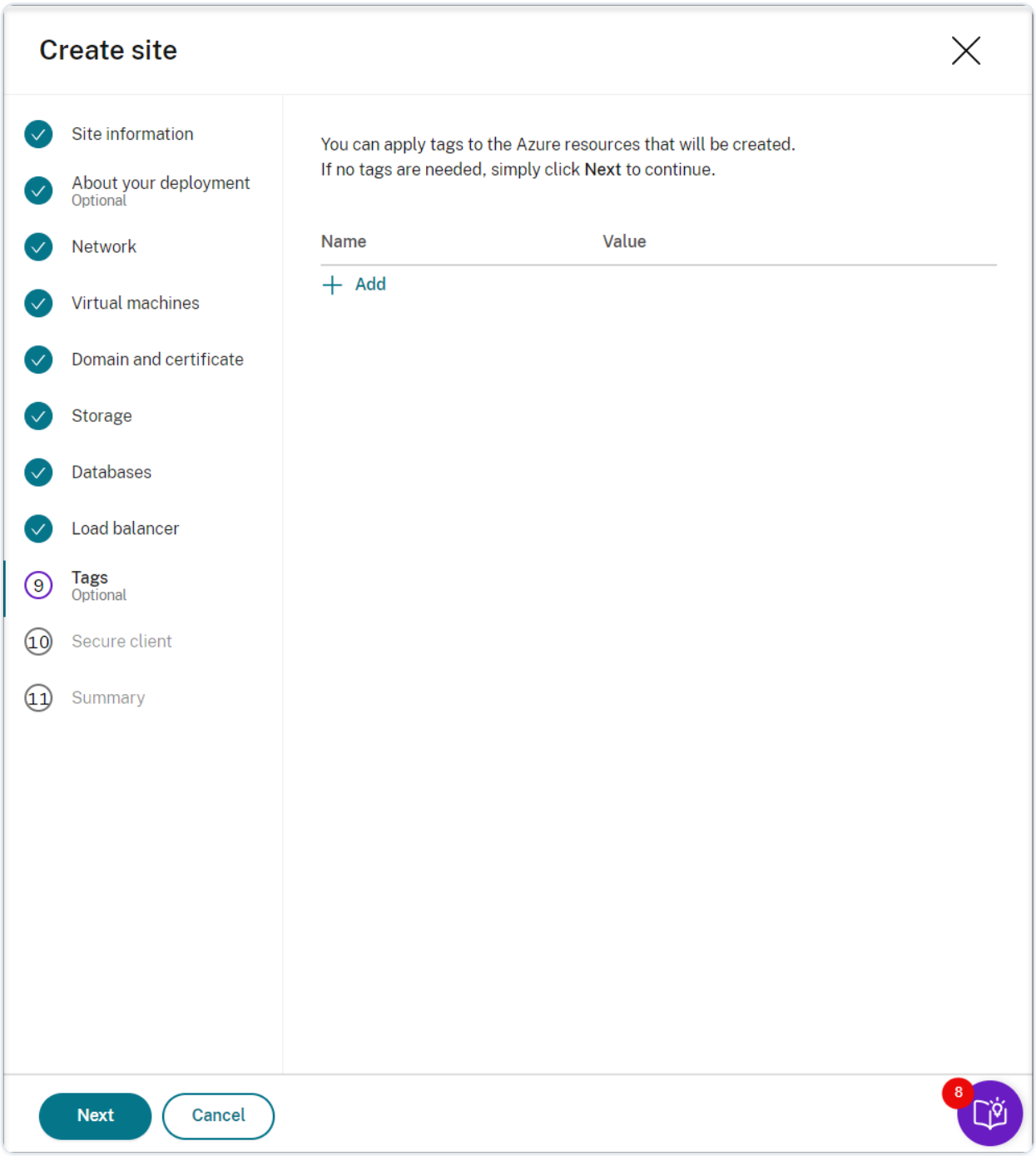
11. Create two SQL databases in Azure. One is used as the Session recording database (named **sessionrecording**) and the other as the administrator logging database (named **sessionrecordinglogging**).



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.

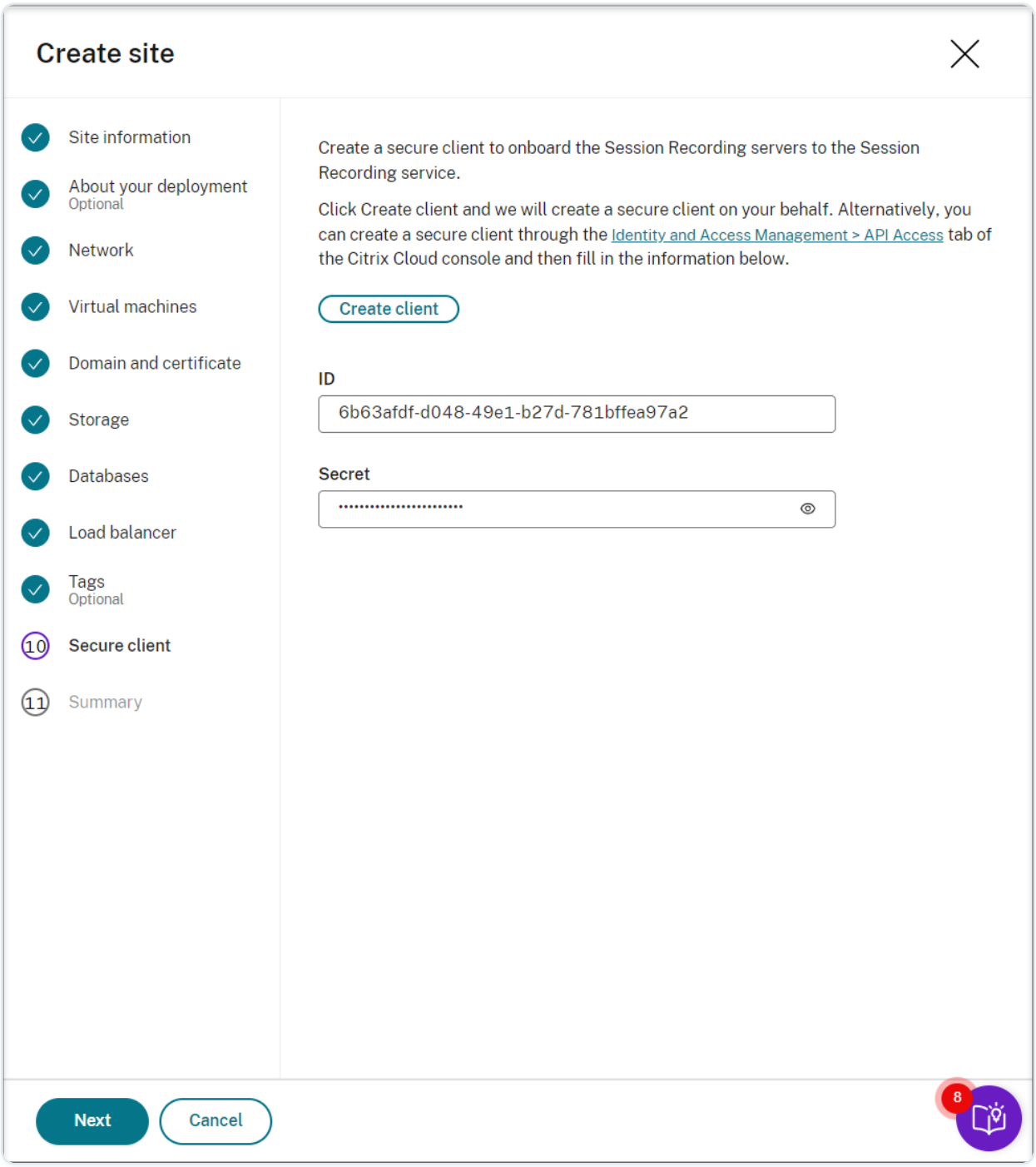


13. (Optional) Apply tags to the Azure resources to be created.

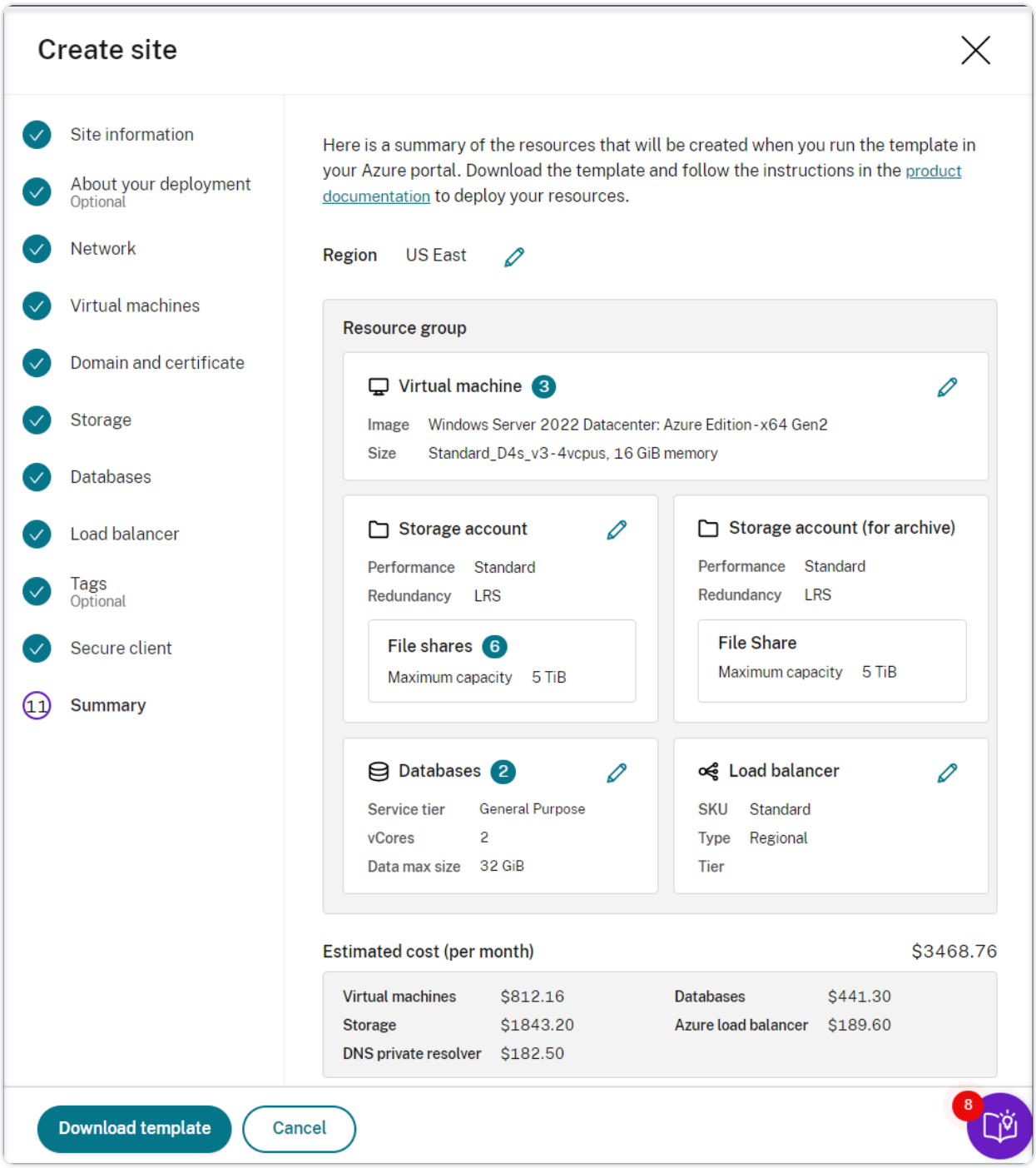


14. Create a secure client to onboard the Session Recording servers to the Session Recording service.

    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.



15. 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.



16. 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.
17. 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-a655-0474809221 94> .\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

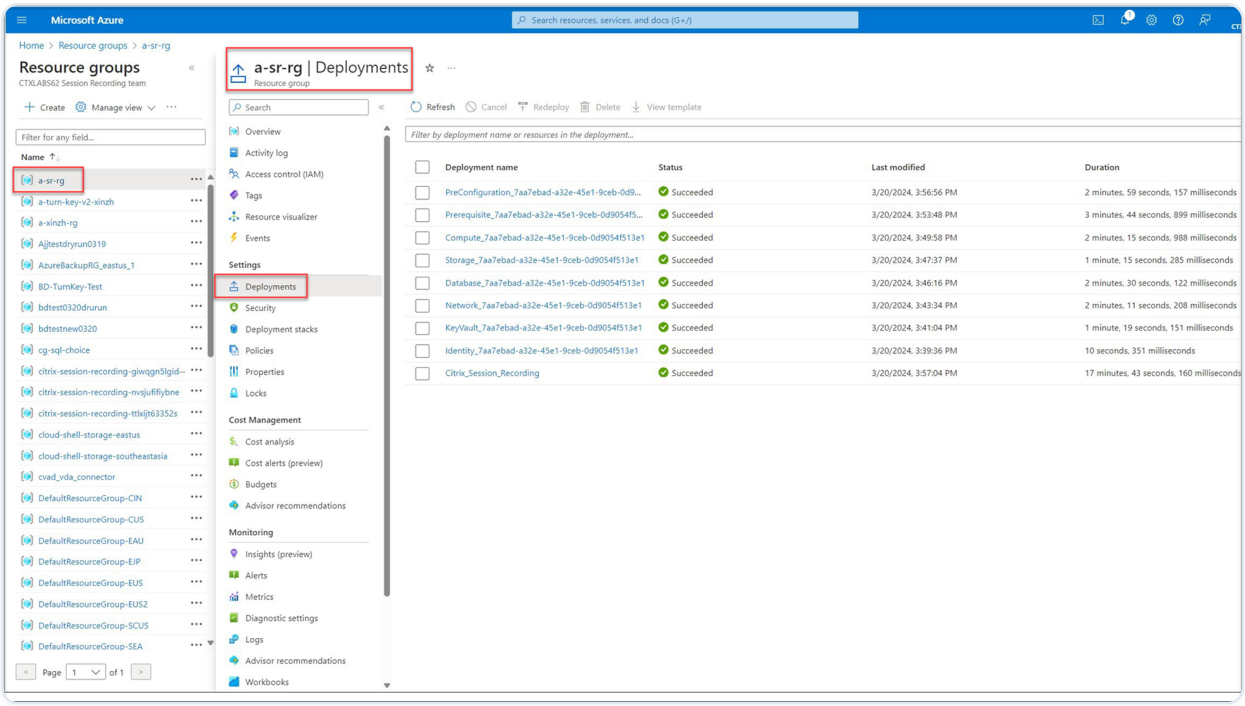
cmdlet DeploySessionRecording.ps1 at command pipeline position 1
Supply values for the following parameters:
TenantId: 03eacdb3-8322-4854-8219-30b0526a6428
AzureClientId: 59e6df48-2aeb-487b-95b8-b95c64b8c897
AzureClientSecret: ************************************
SubscriptionId: eb089a2e-52b0-4492-9e24-7bf579cff14f
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
                                                                                                             iro
                                                                                                             nme
                                                                                                             nt
-------                             ----------------                    --------                             ---
59e6df48-2aeb-487b-95b8-b95c64b8c897 cvad-session-recording-tie.liu@citrix.com 03eacdb3-8322-4854-8219-30b0526a6428 Azu

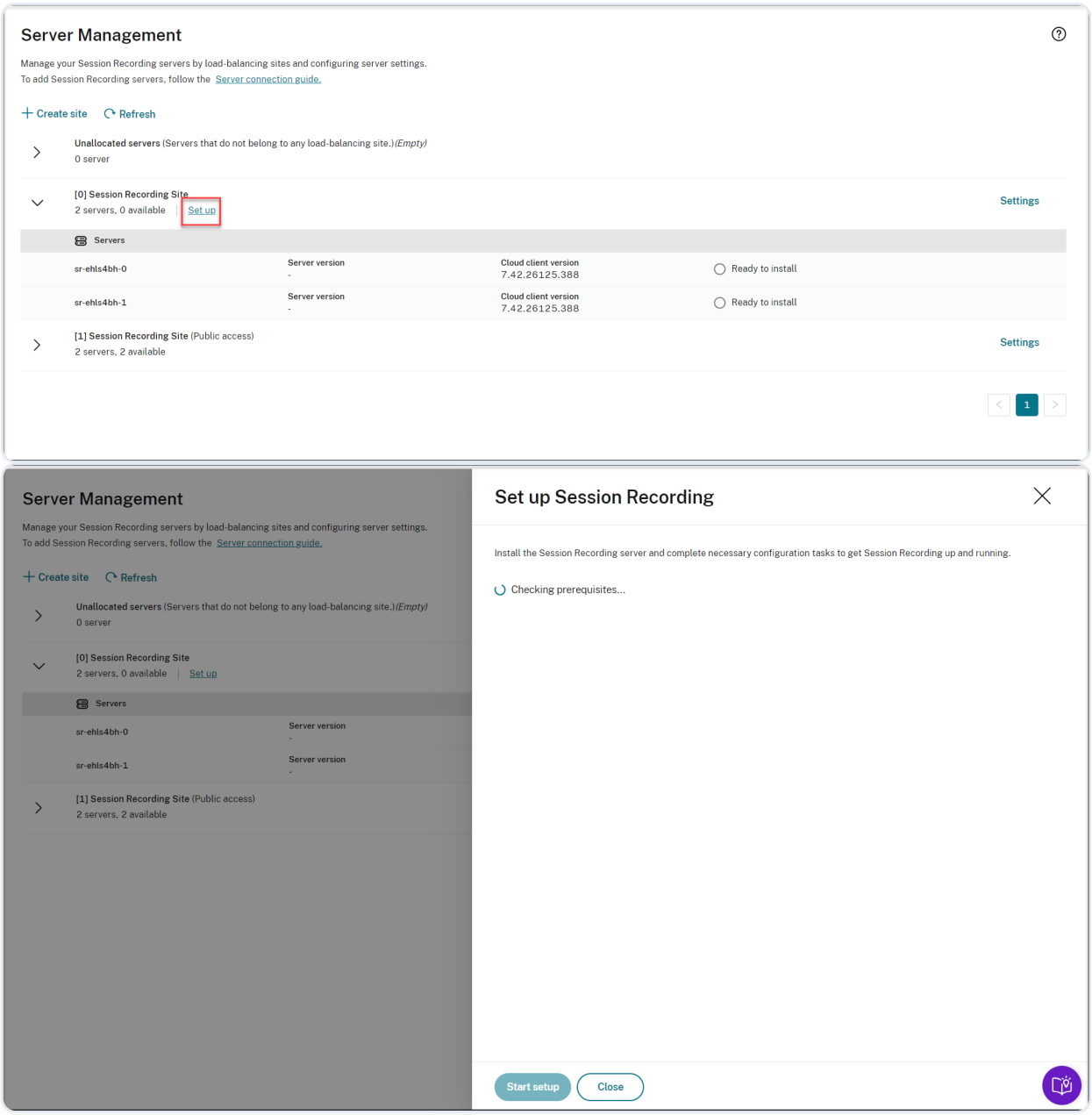
ResourceGroupName : a-xinzhang-rg-1
Location          : eastus
ProvisioningState : Succeeded
Tags              : {admin}
TagsTable         :
                    Name   Value
                    =====  =====
                    admin  xinzh

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

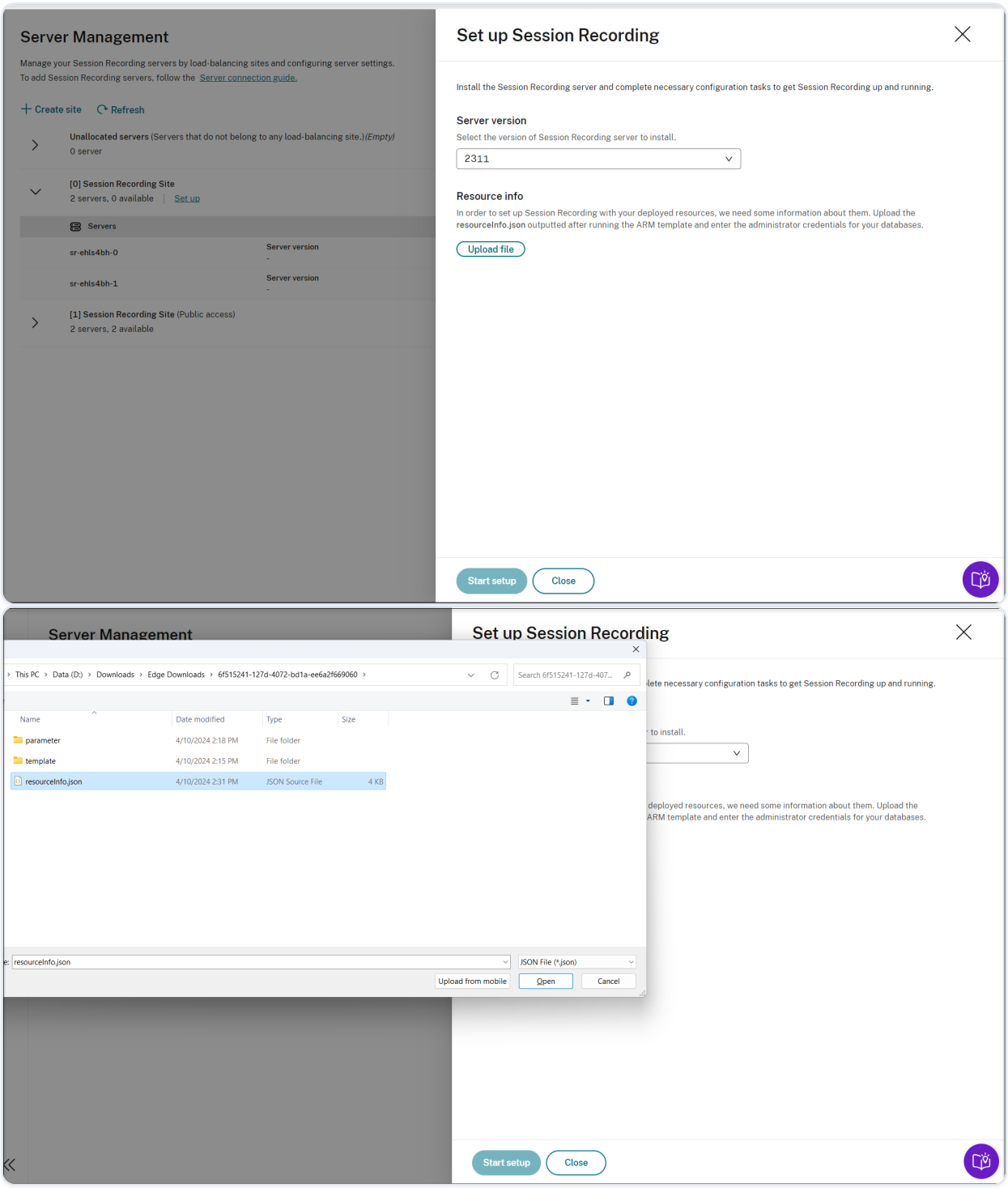
18. Go to the Azure portal, locate the resource group that contains your deployment, and then check the deployment progress. Wait until the entire deployment shows **Succeeded**.



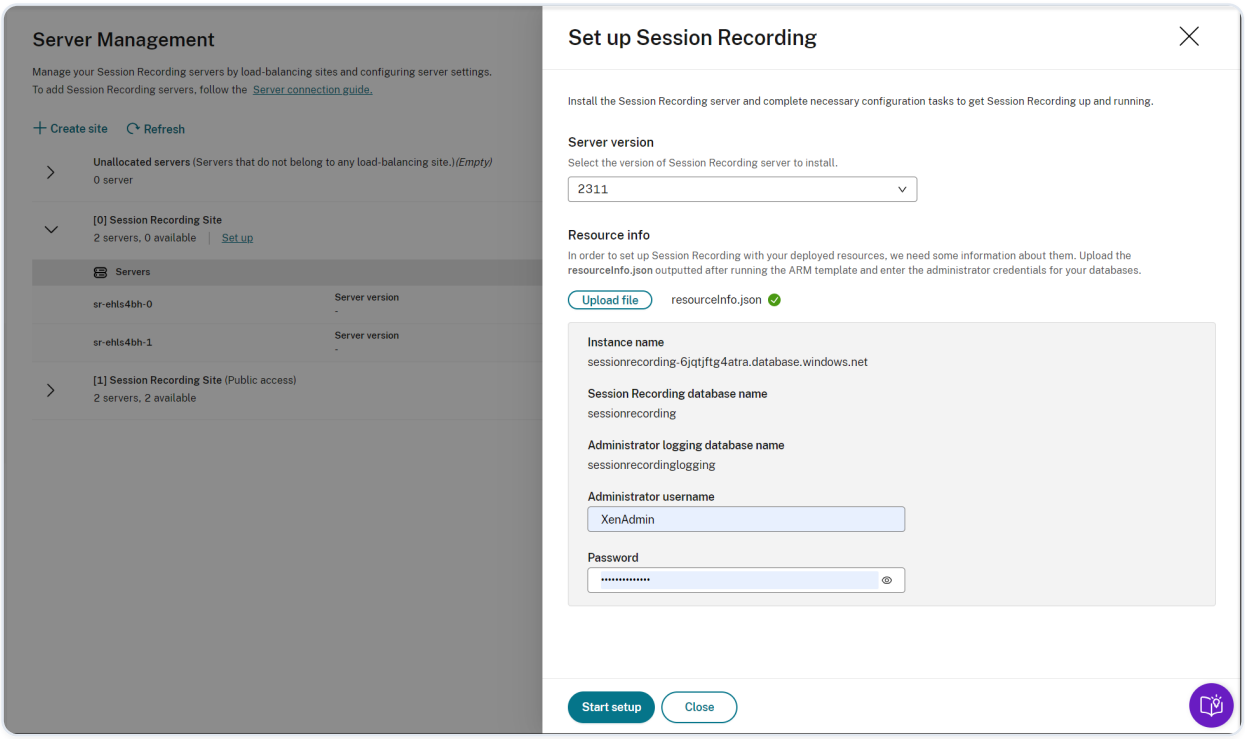
19. Return to the **Server Management** page of the Session Recording service. Find the newly created site, and you will see a **Set up** button available. Click **Set up** to set up Session Recording to get it up and running.



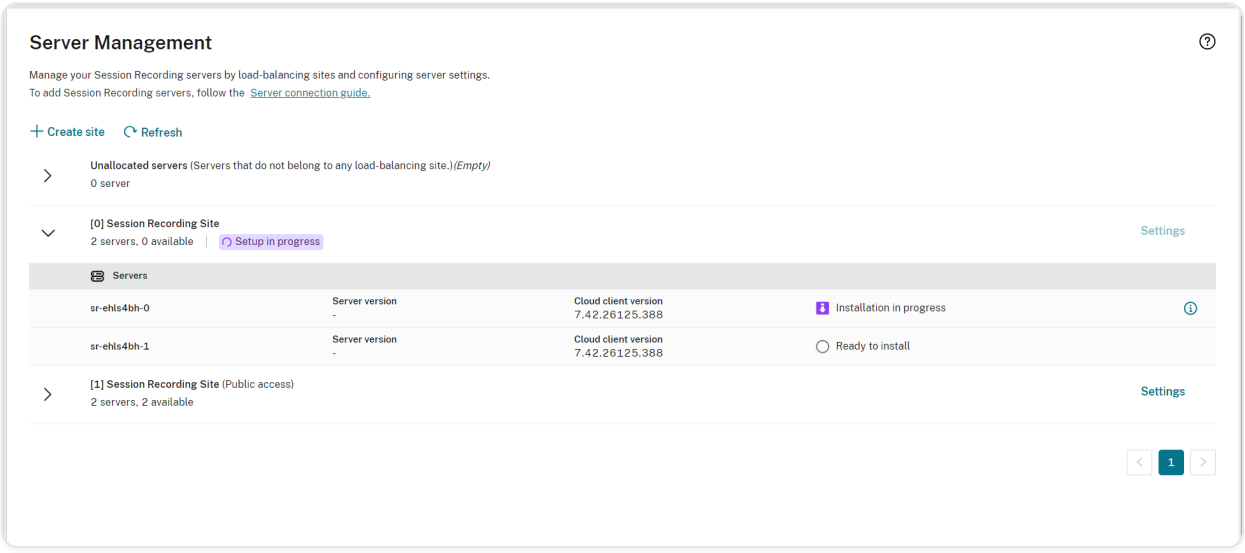
To set up Session Recording, you need to specify the version of the Session Recording server to install and upload the **resourceInfo.json** file.

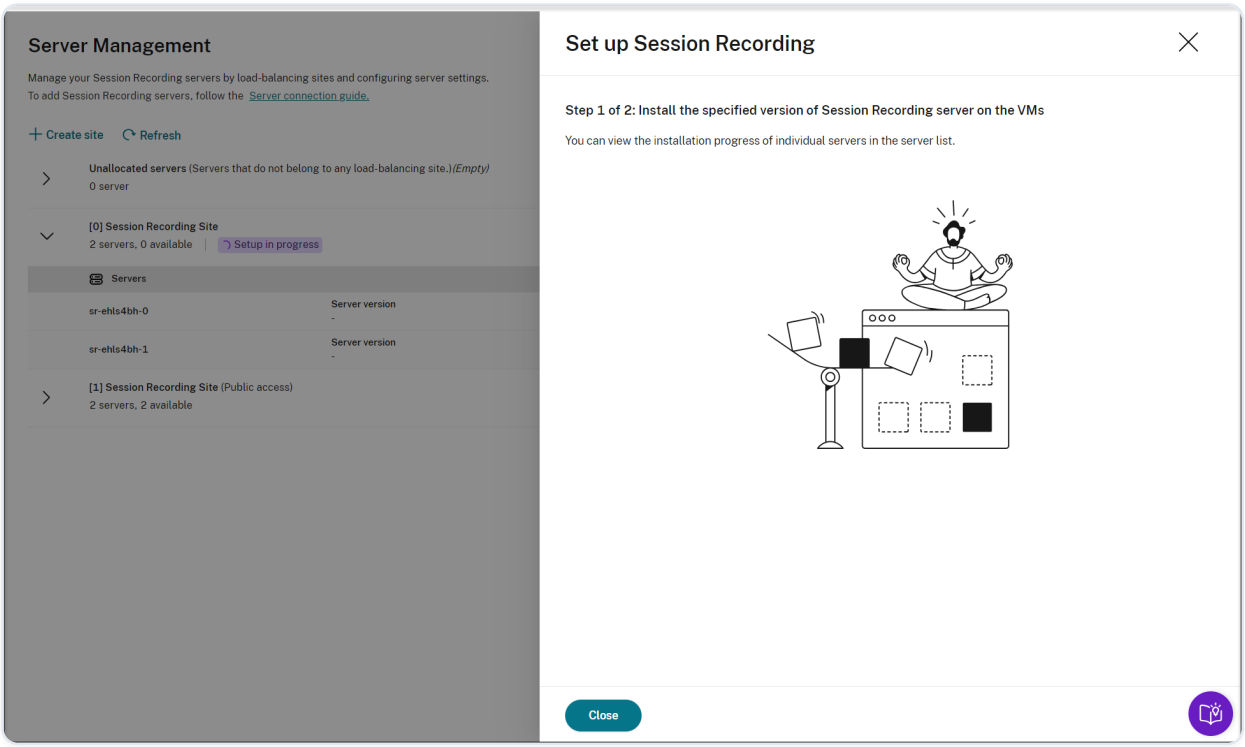


Enter the credentials for your databases.

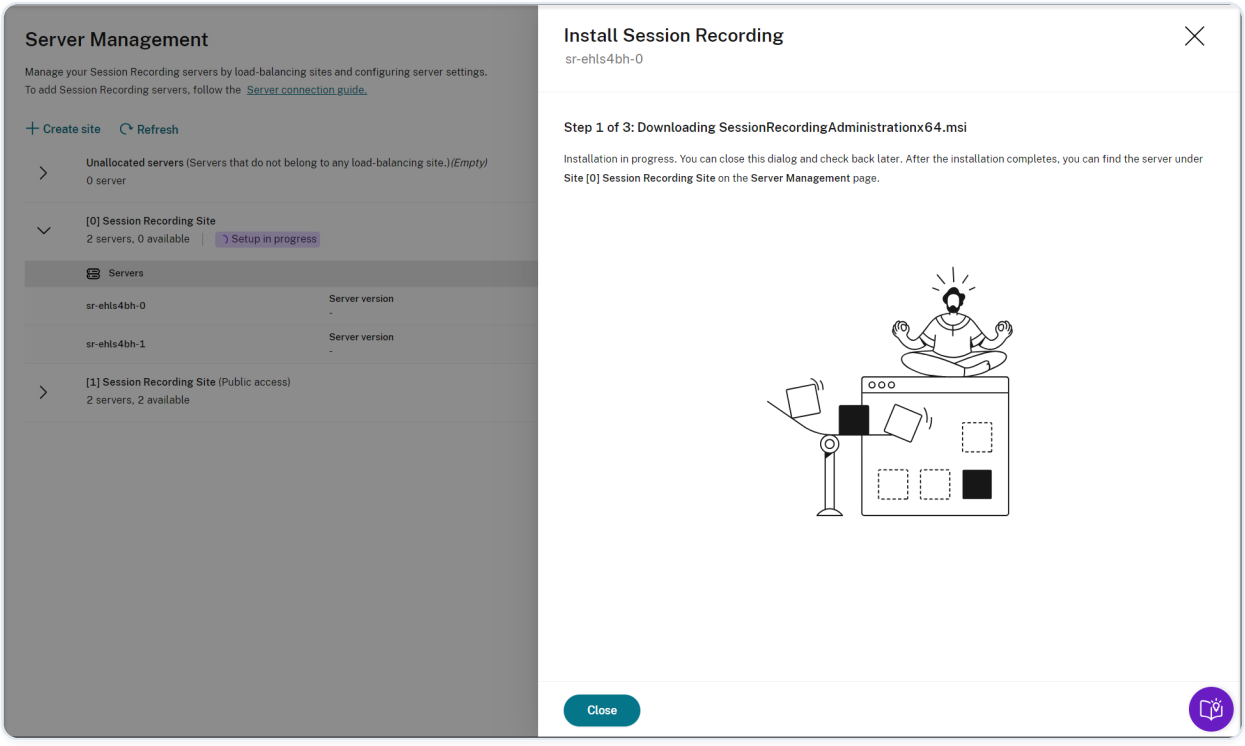


Click **Start startup**. You can then check the setup progress on the **Server Management** page.

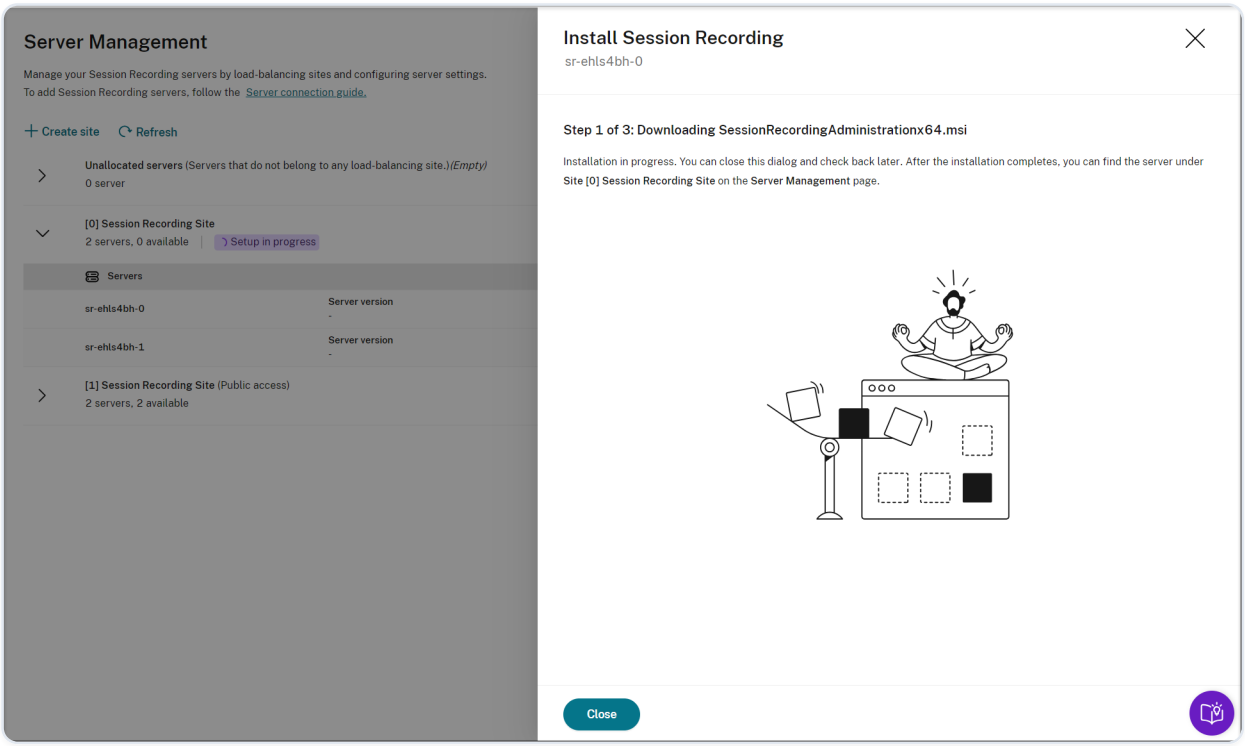




You can view the installation progress of individual servers in the server list.



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

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.

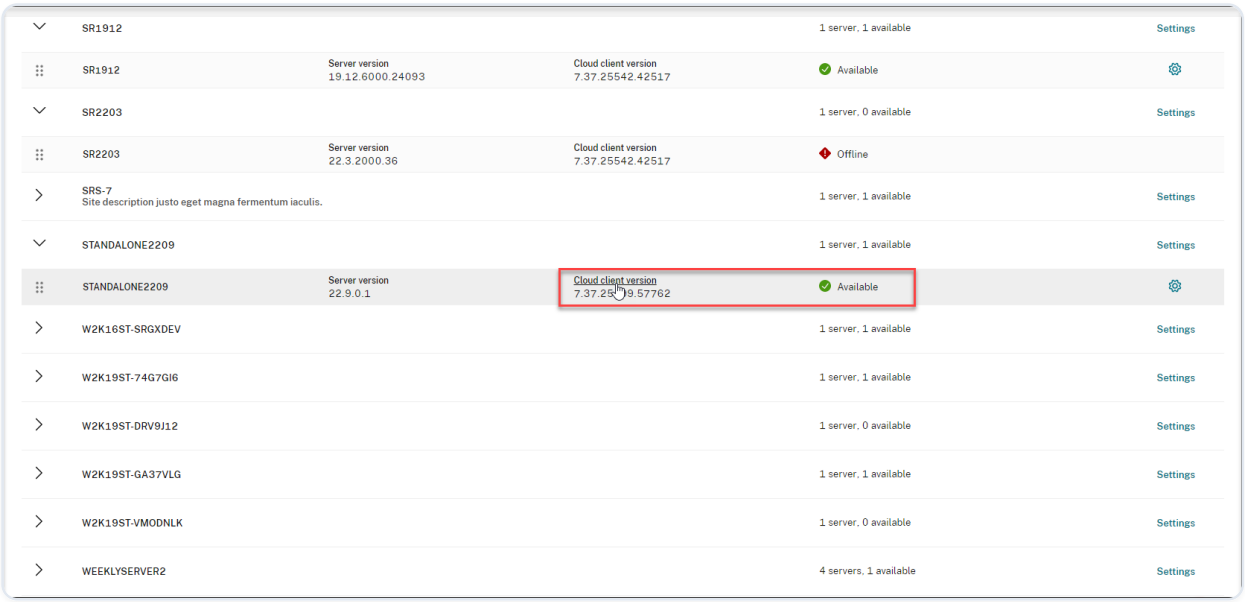
Upgrade the cloud client immediately or automatically

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

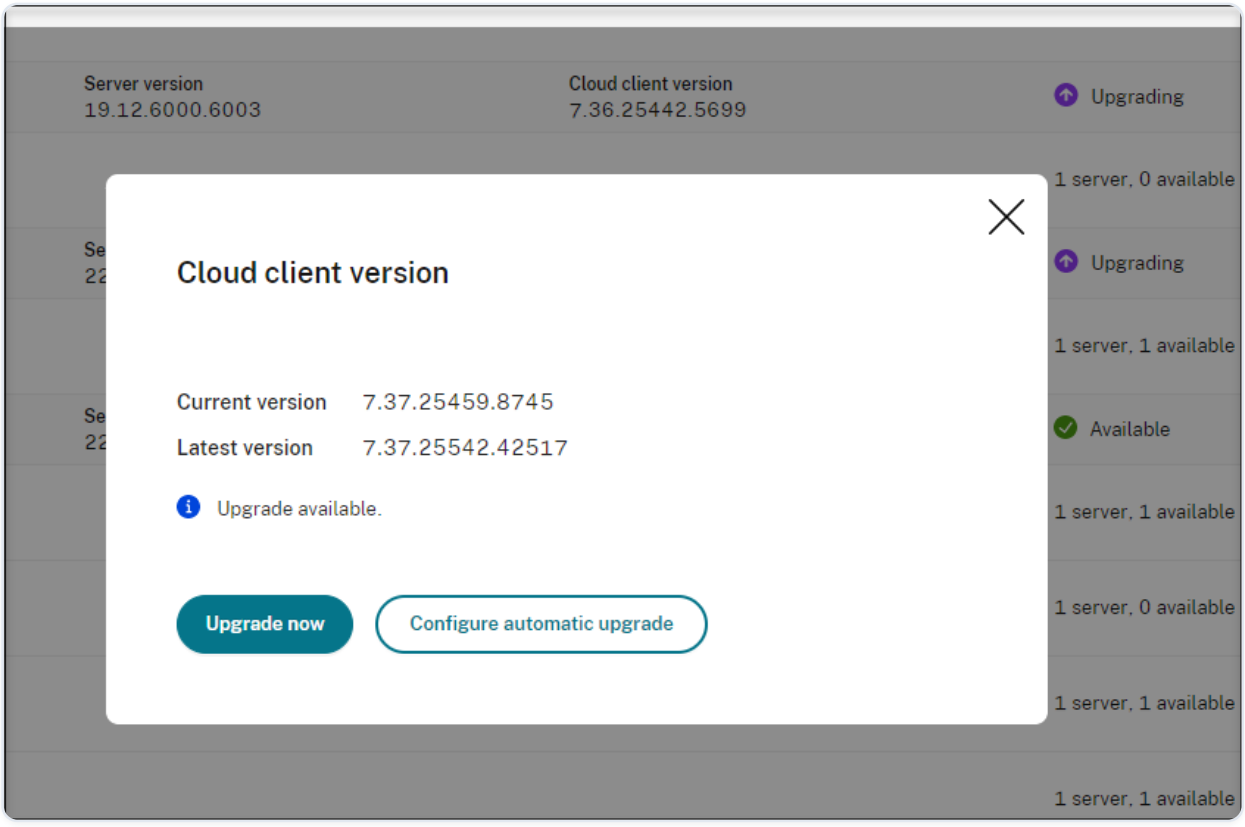
Method 1: Click Cloud client version in the row of the target Session Recording server

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.



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

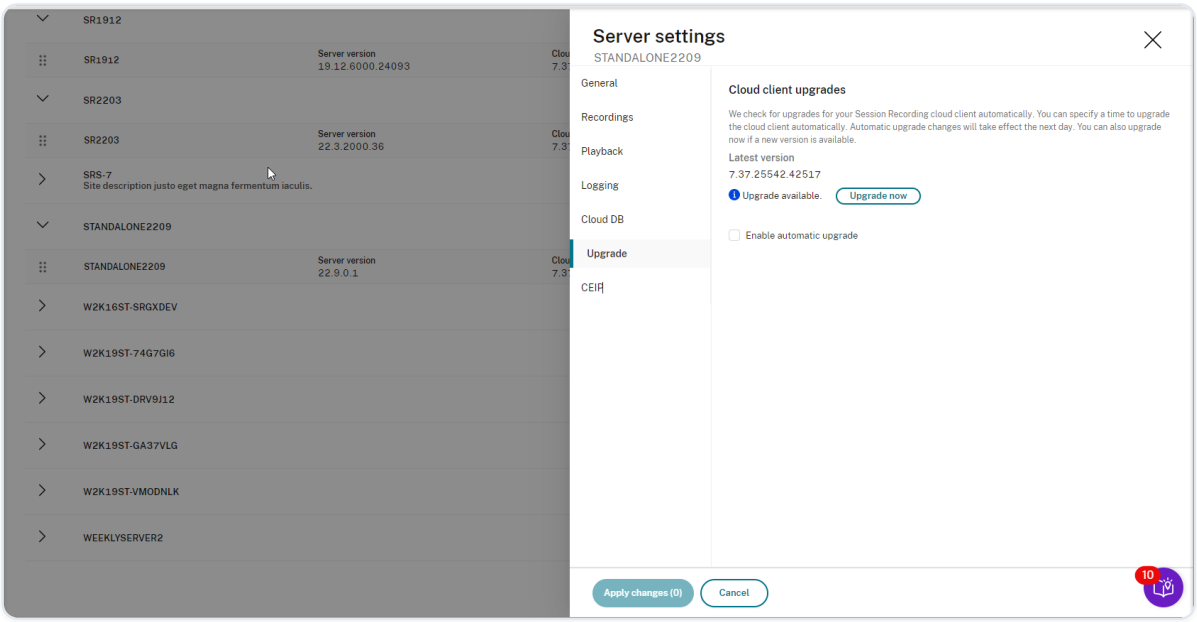


- Click **Upgrade now**.

  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.

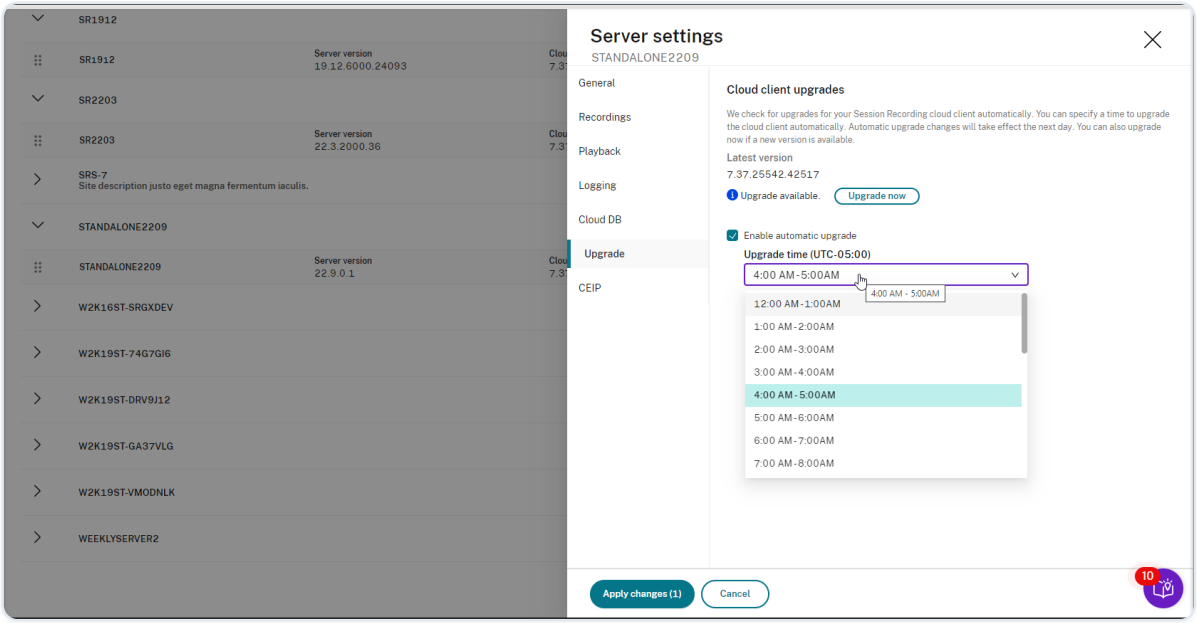
- Click **Configure automatic upgrade**.

  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.

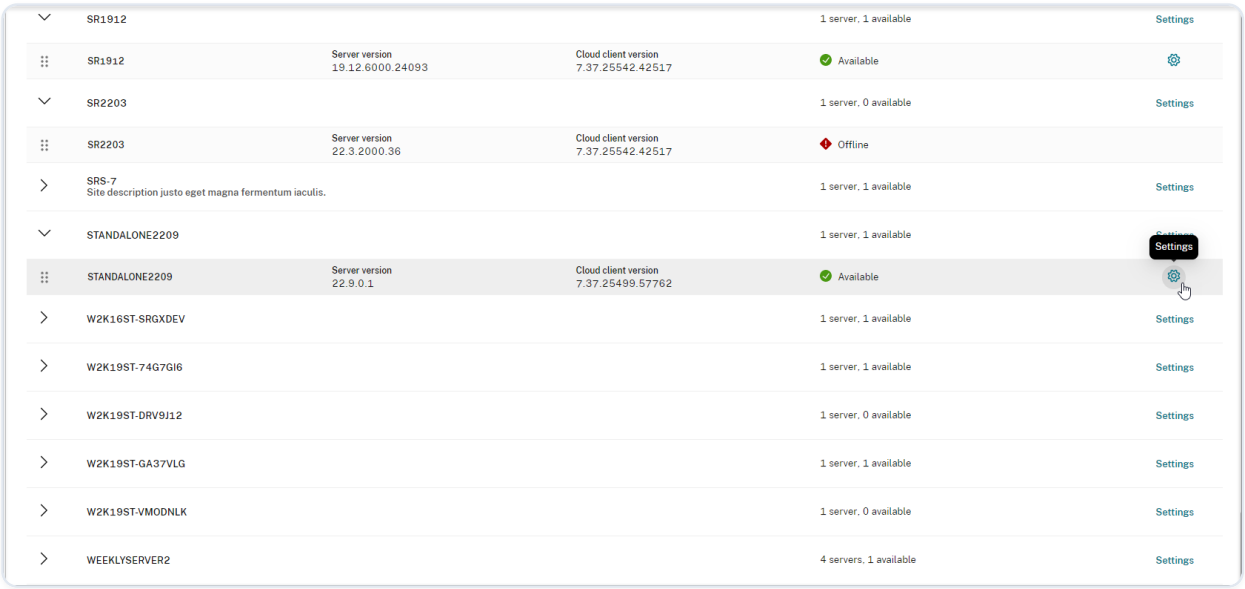


Your automatic upgrade settings take effect the next day.

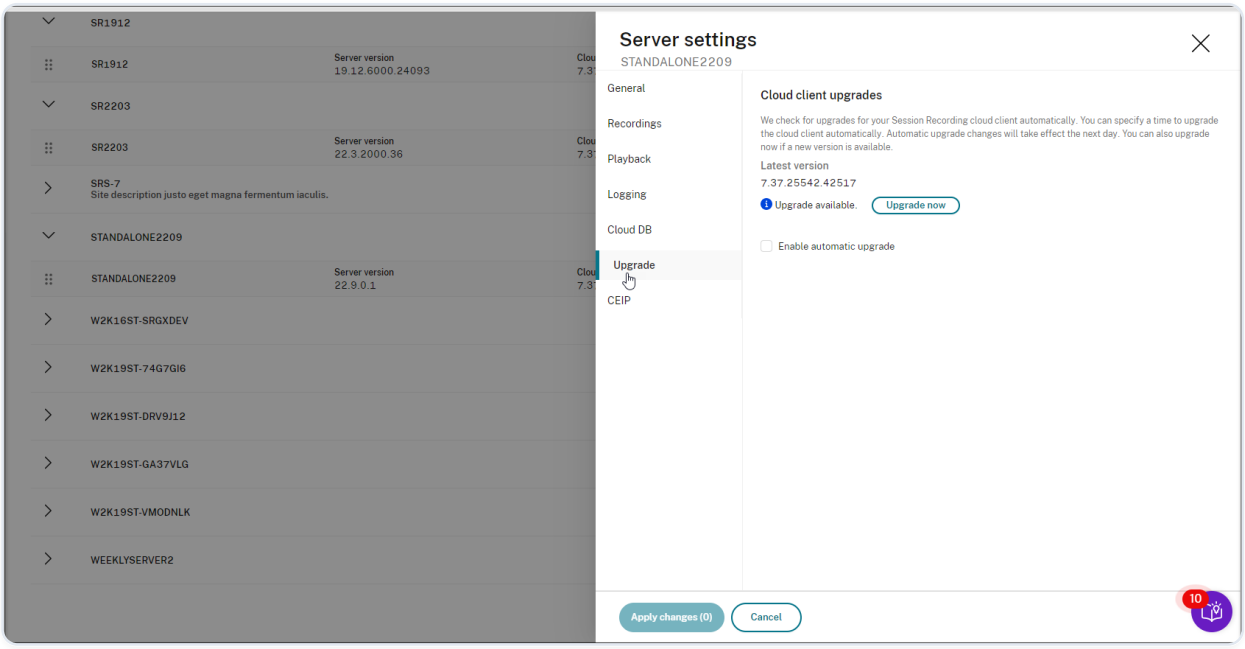
Method 2: Click the settings icon in the row of the target Session Recording server

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.

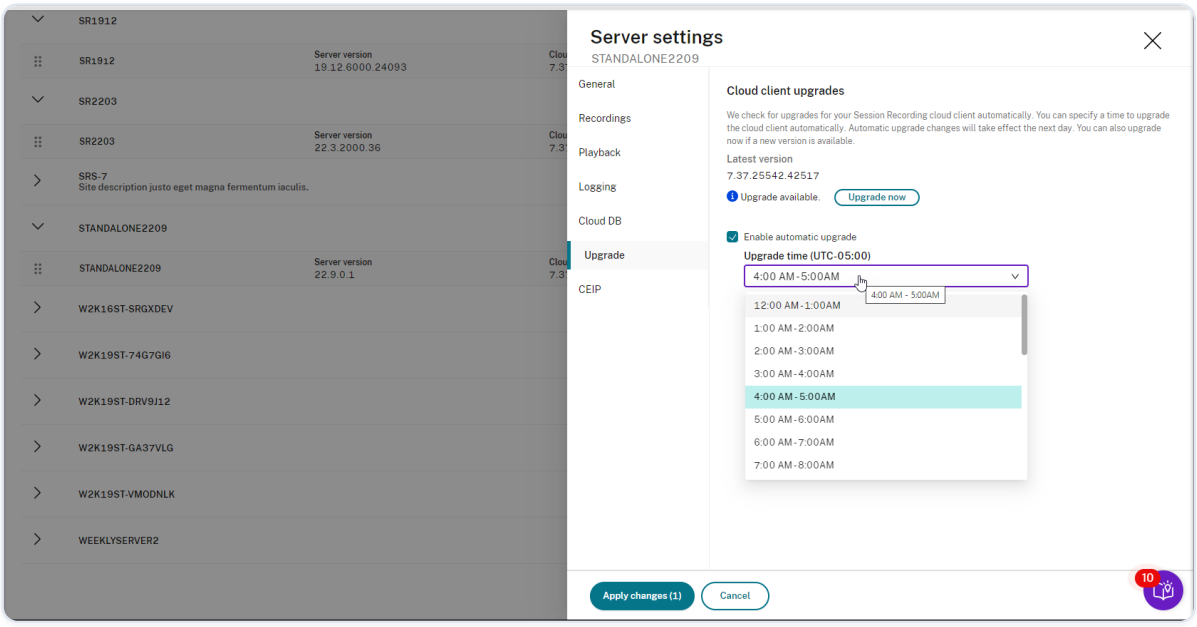


5. Click **Upgrade now** or set **Enable automatic upgrade**.

   - 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.

Interactive Demo Mode for exploring Session Recording

The Interactive Demo Mode for Session Recording allows the administrators to explore and understand the functionalities of the session recording service without impacting real user data or requiring initial server setup. It provides a hands-on management experience using pre-generated or synthetic data.

The Interactive Demo Mode offers a risk-free environment for administrators to:

- Navigate the management interface and become familiar with its layout.
- Observe how data is presented and how different features operate using sample data.
- Evaluate the service's suitability for their organization's needs before onboarding actual session recording servers.

Use cases

- **New Administrator Onboarding:** A new Citrix Cloud™ administrator can use the interactive demo mode to quickly learn how to manage and use the session recording service.

- **Pre-Deployment Evaluation:** An IT manager considering implementing session recording can explore its features in the demo mode to make an informed decision.
- **Training and Demonstration:** Internal IT teams can use the interactive demo mode to train other staff members on the session recording service's capabilities.

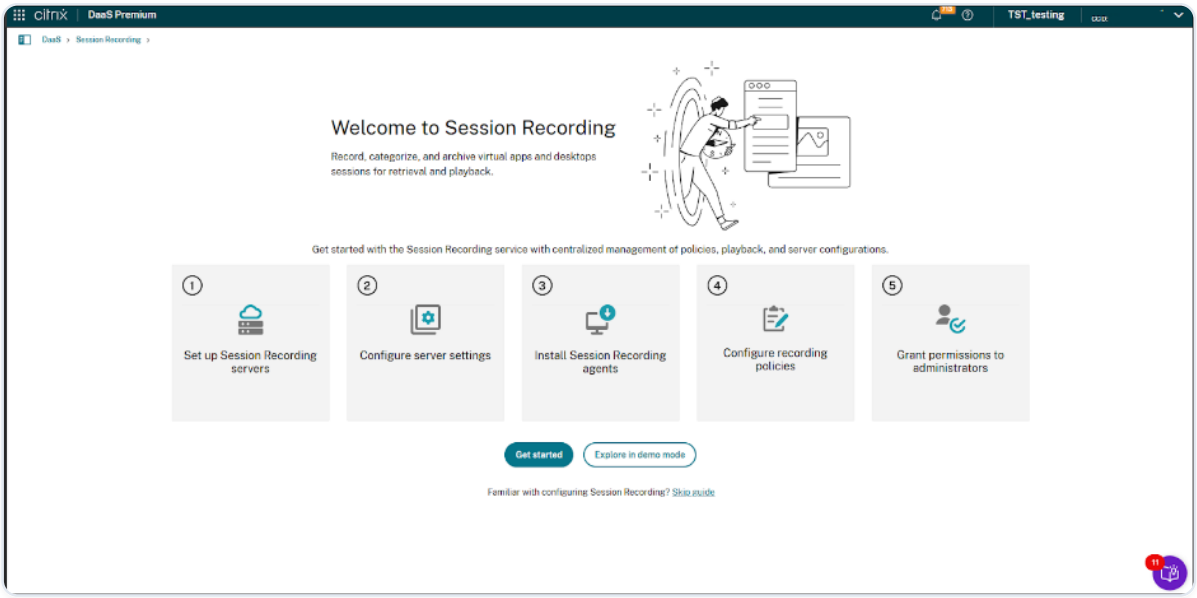
Required permissions

Access to the Interactive Demo Mode is available for Citrix Cloud administrators assigned any of the following roles:

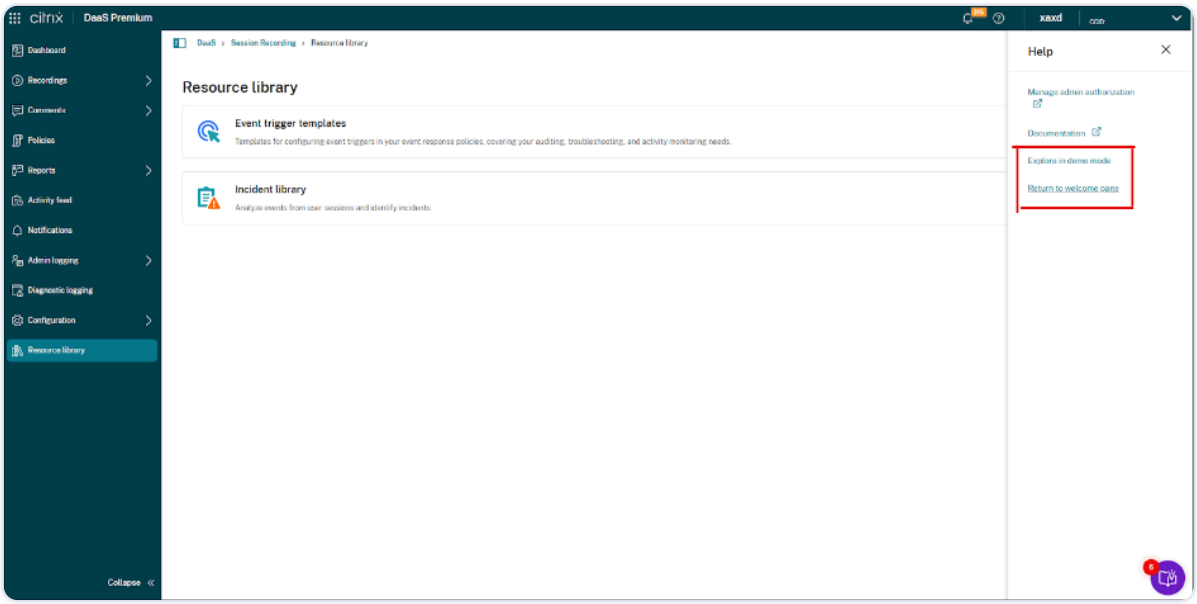
- Full access
- Cloud Administrator role
- Session Recording-FullAdmin role

How to enable the Interactive Demo Mode

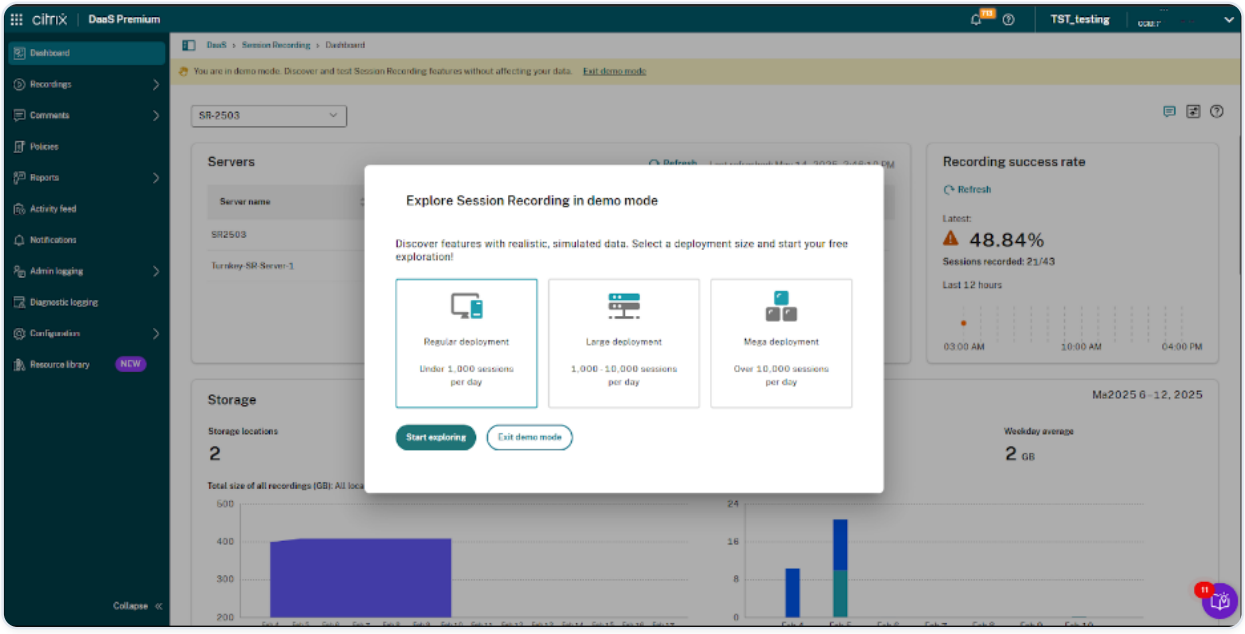
1. Navigate to the Session Recording welcome page within Citrix Cloud.
2. Select the option to explore in demo mode on the welcome page or in the help panel.
    - On the welcome page, click the "Explore in demo mode" button.



    - Alternatively, find the "Explore in demo mode" link in the help panel.



3. Once you initiate the demo mode, you are prompted to choose a deployment size (for example: Regular deployment, Large deployment, Mega deployment) which influences the amount and type of simulated data presented. Select the option that best reflects your anticipated usage.
4. Click the "**Start exploring**" button to enter the simulated environment.



How to use the Interactive Demo Mode

Once you enable the Interactive Demo Mode, navigate normally through the different sections of the Session Recording service interface. The corresponding simulated data (for example: server lists, storage information, recording success rates) is displayed. You can interact with the interface elements to understand their function without making any actual changes to a live environment.

How to disable the Interactive Demo Mode

- Click the "**Exit demo mode**" button, typically found in a banner at the top of the page.
- Alternatively, the demo mode is disabled when you return to the welcome page.
- You can proceed to the standard service pages by clicking "**Get started**" or "**Skip guide**" on the welcome page to configure and use the service with your actual session recording servers.

Configure

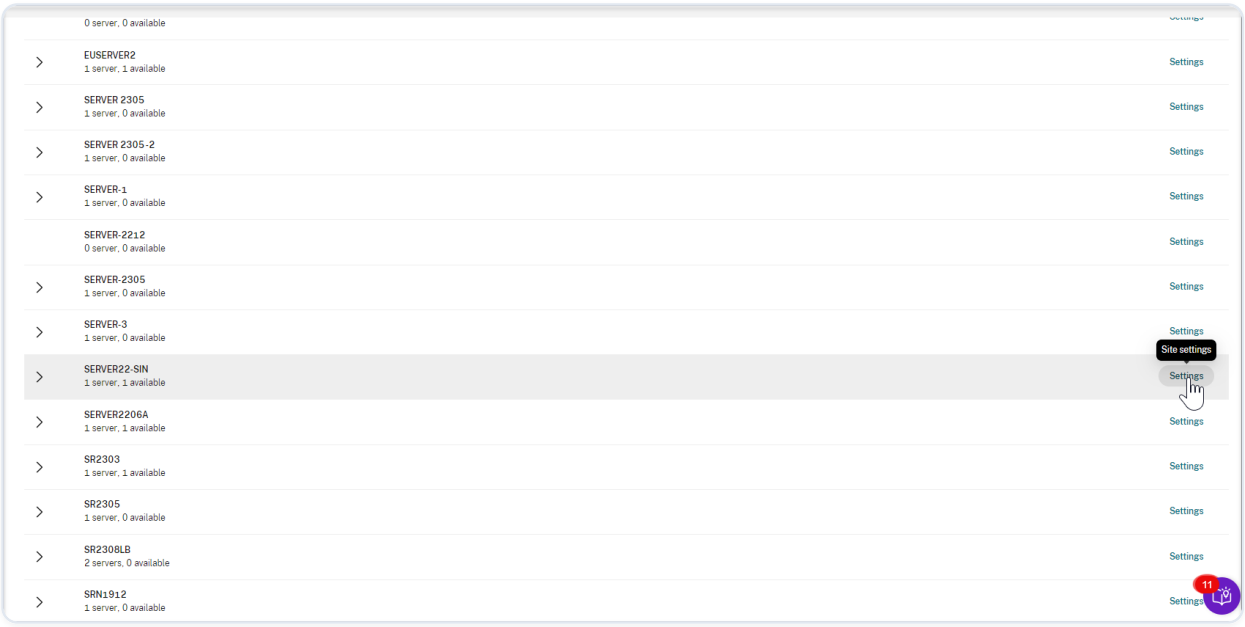
This section provides instructions for you to:

- Site and server settings
- Configure policies
  - Configure session recording policies
  - Configure event detection policies
  - Configure event response policies
  - Configure endpoint recording policies
- Playback permissions
- Administrator permissions
- Configure preferences

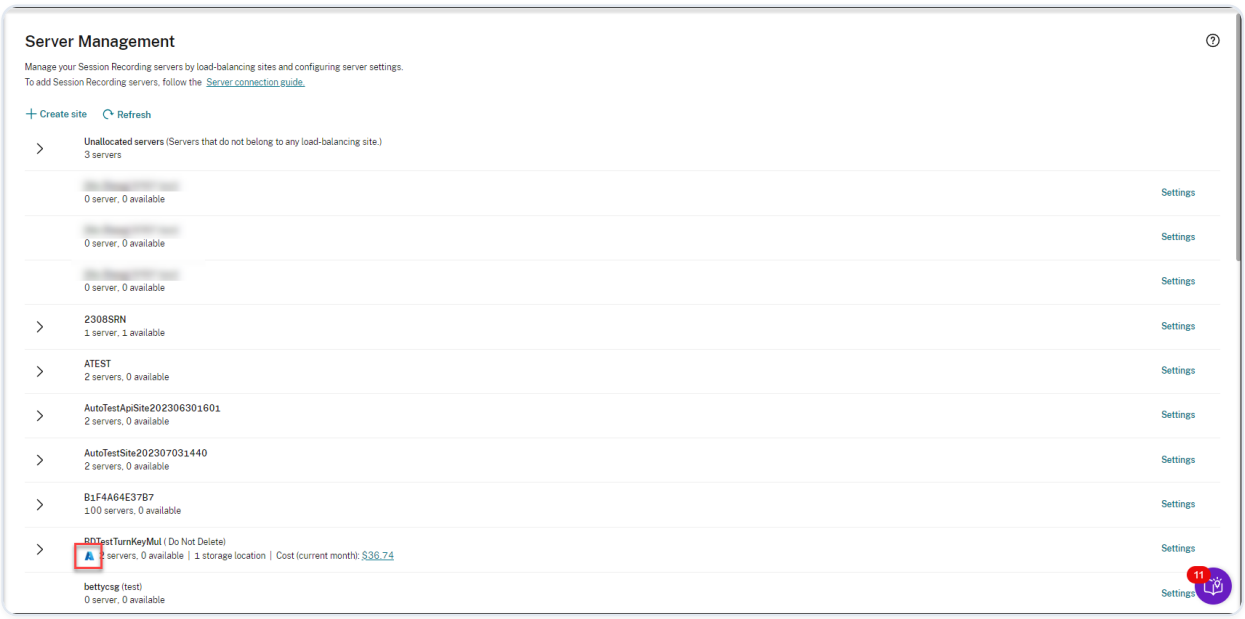
Site and server settings

Site settings

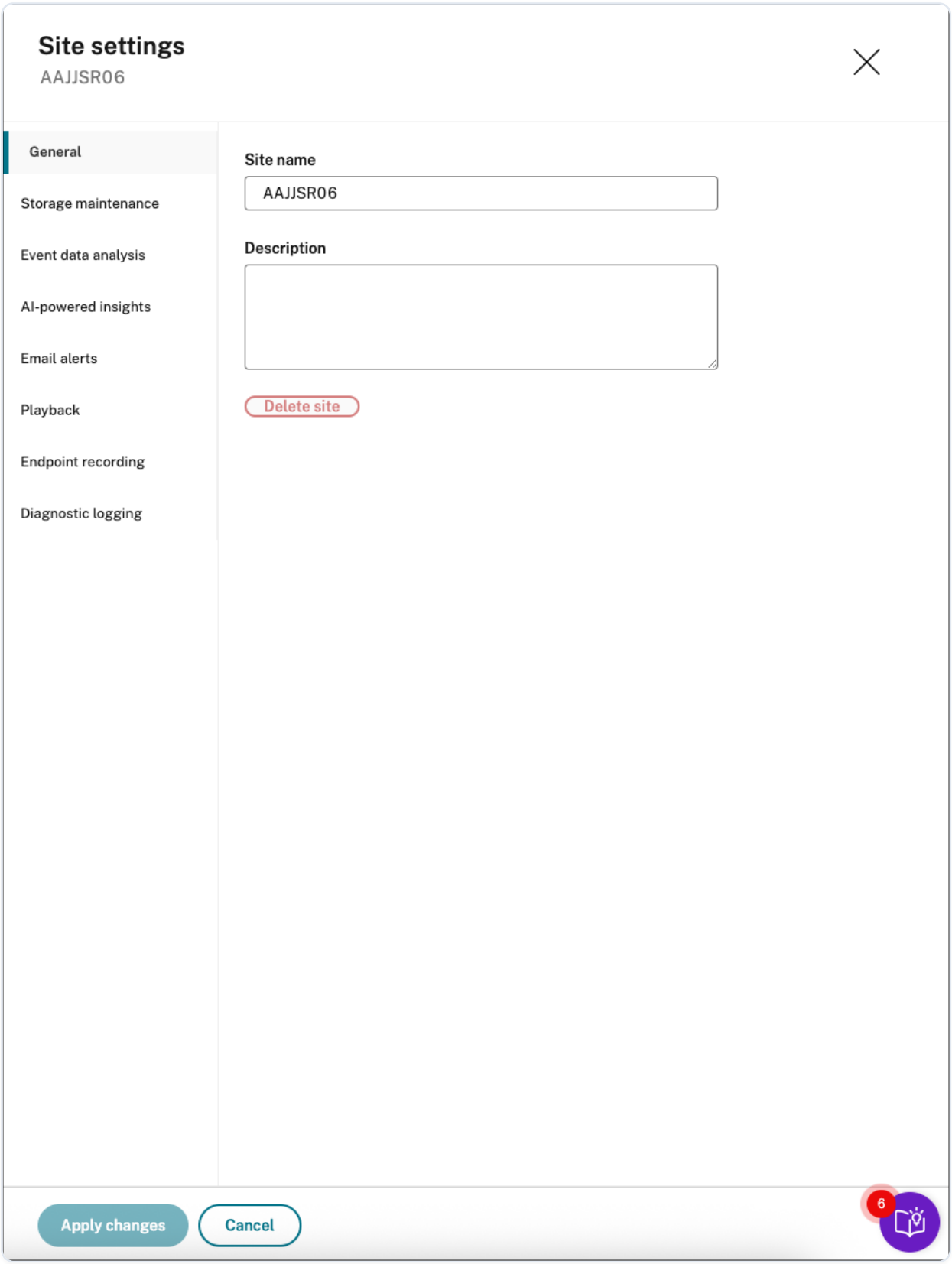
1. Select **Configuration > Site Management** from the left navigation of the Session Recording service.
2. Click **Settings** for the target site.



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



3. (Optional) On the **General** page, rename the site and give it a new description.



4. (Optional) On the **Storage maintenance** page, schedule site-level tasks to automatically archive and delete recordings. For more information, see Manage recordings on schedule.
5. (Optional) On the **Event data analysis** page, specify which events need to be forwarded to a third-party Security Information and Event Management (SIEM) system. For more information,

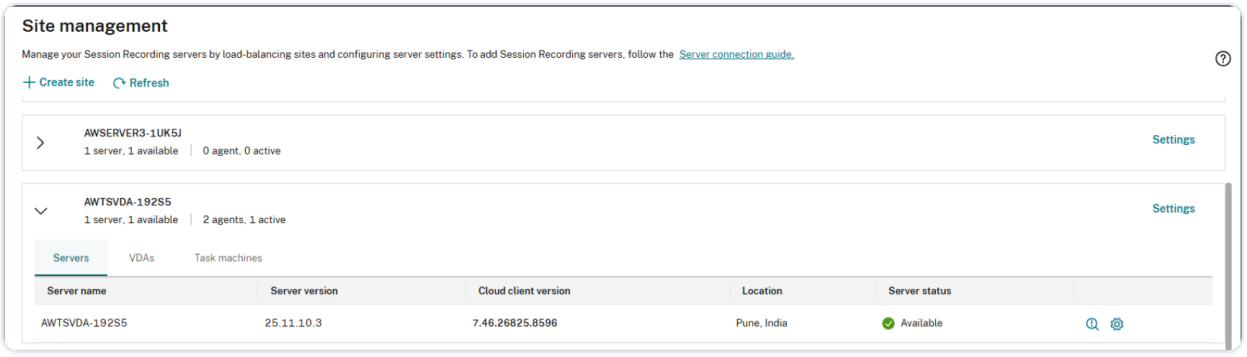
see Third-party SIEM integration. Additionally, you can enable the presentation of incident data in the cloud, for more information, see Configure site-level user activity reporting.

6. (Optional) On the **AI-powered insights** page, specify the parameters of your AI model. For more information, see AI-powered insighs for session recording.
7. (Optional) On the **Email alerts** page, specify the email sender and content to send email alerts in response to detected events. For more information, see Create a custom event response policy.
8. (Optional) On the **Playback** page, 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.
9. (Optional) On the **Endpoint recording** page, specify which site's policy can be in effect globally. For more information, see Select the global configuration site.
10. (Optional) On the **Diagnostic logging** page, specify the retention period for diagnostic logs. For more information, see Diagnostic logging.

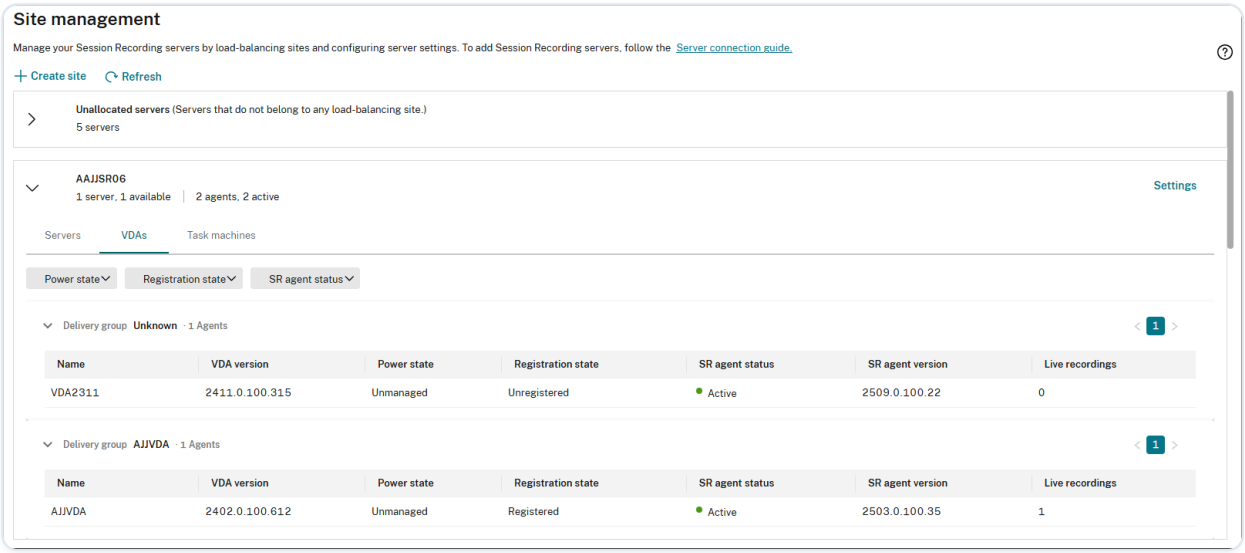
Server settings

1. Select **Configuration > Site Management** from the left navigation of the Session Recording service. You can manage the settings for your sites and the servers within them. This page is organized into three tabs: **Servers, VDAs and Media Servers**.

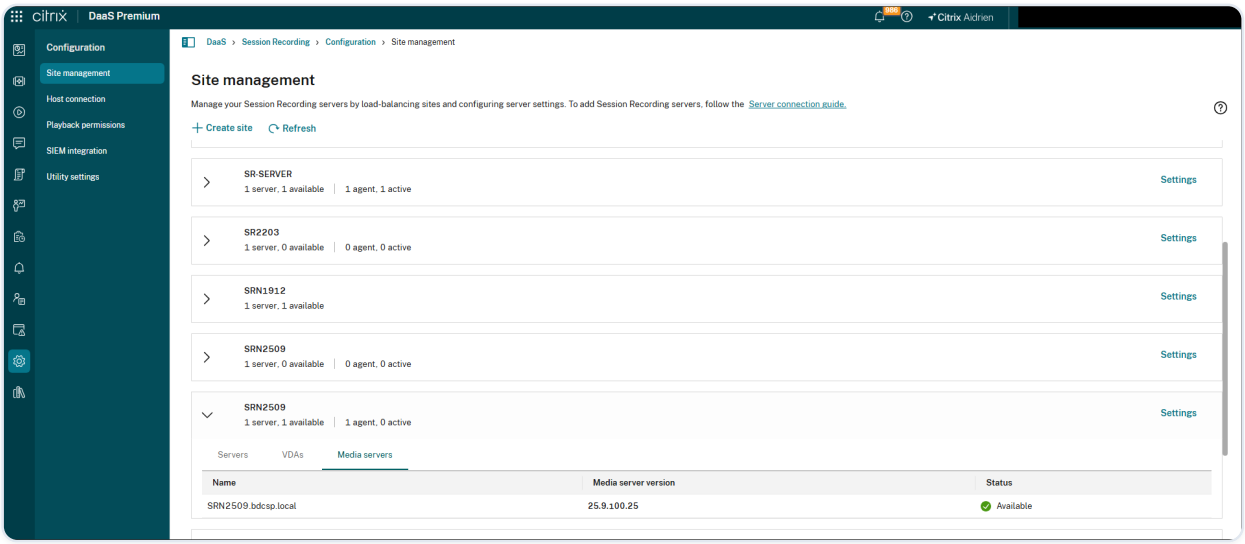
   The Servers tab displays a list of the Session Recording servers associated with the selected site.



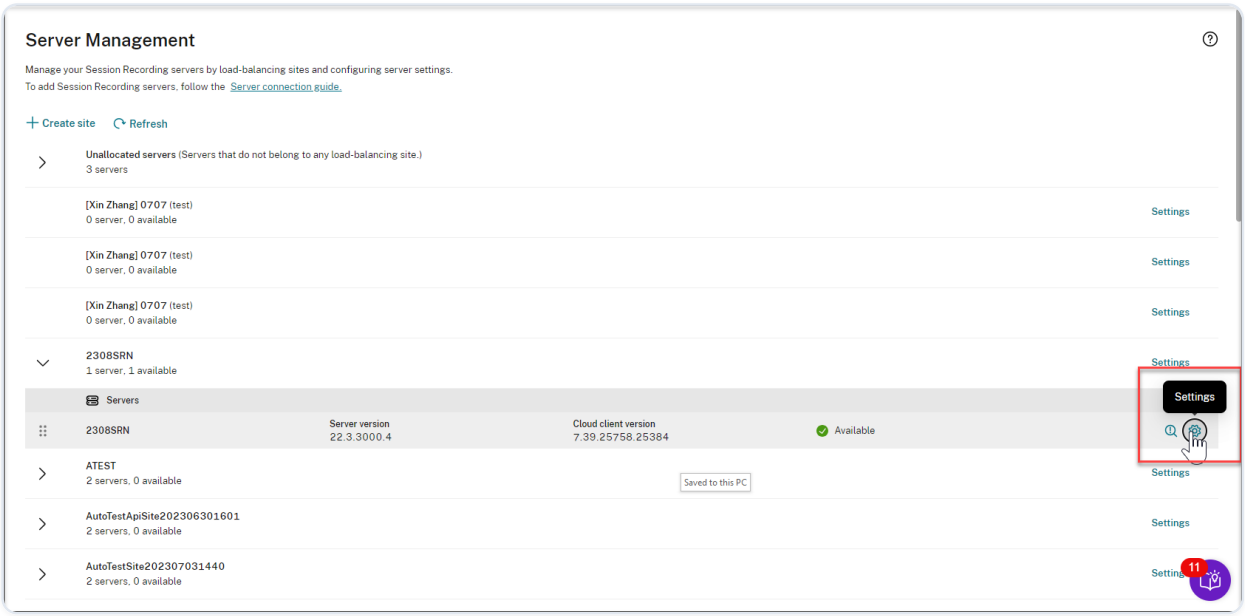
   The VDAs tab provides detailed information about the Session Recording agents running on the VDAs connected to the site. You can use the filters to quickly find specific VDAs.



The **Media servers** tab provides detailed information about the version and running status of the media servers:



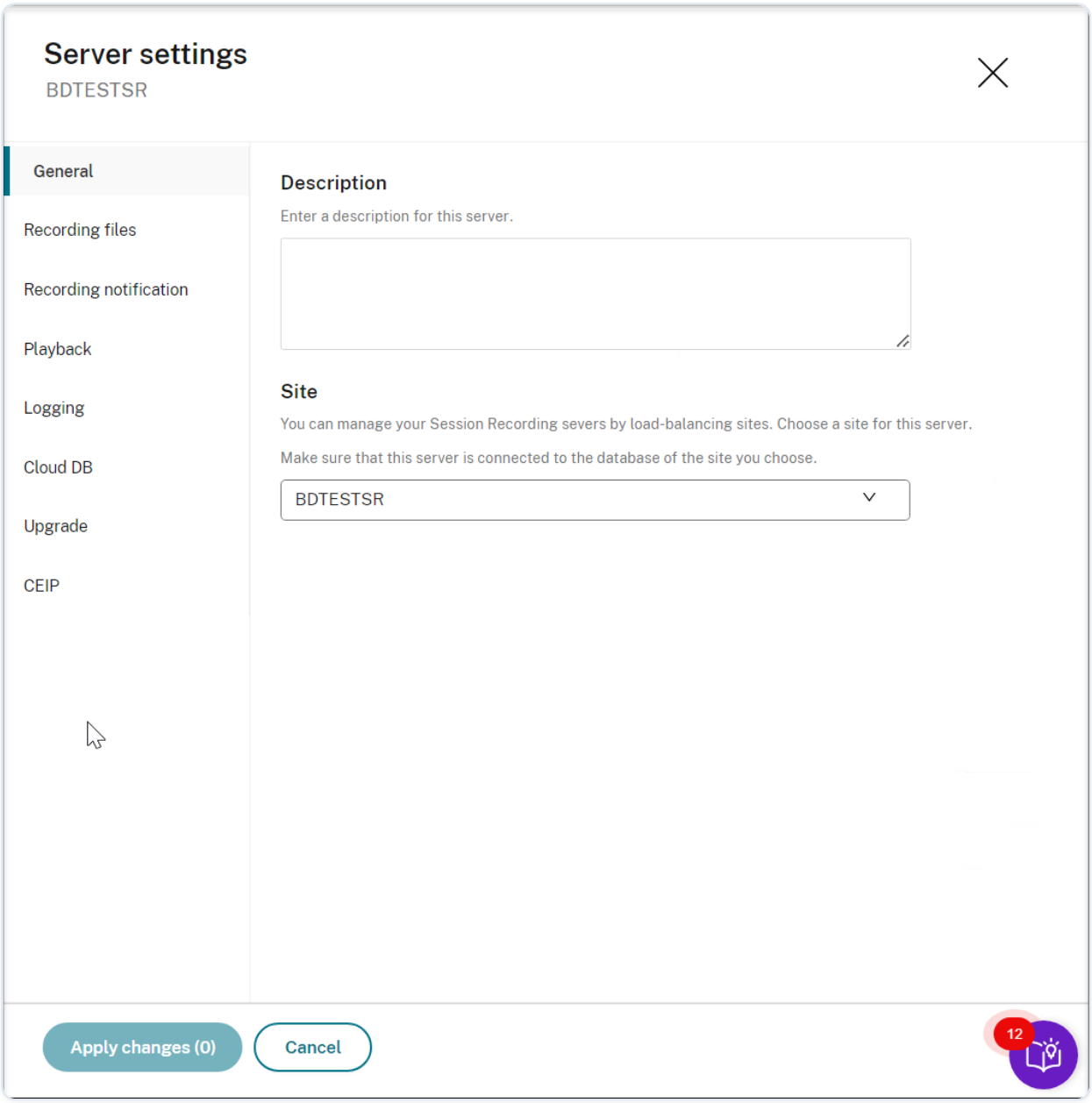
2. Expand a site to locate the target Session Recording server and then click the **Settings** icon next to it. The **Settings** icon is present only for servers in **Available** state.



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 **Recording files** and other pages, configure the server settings listed in the following table:

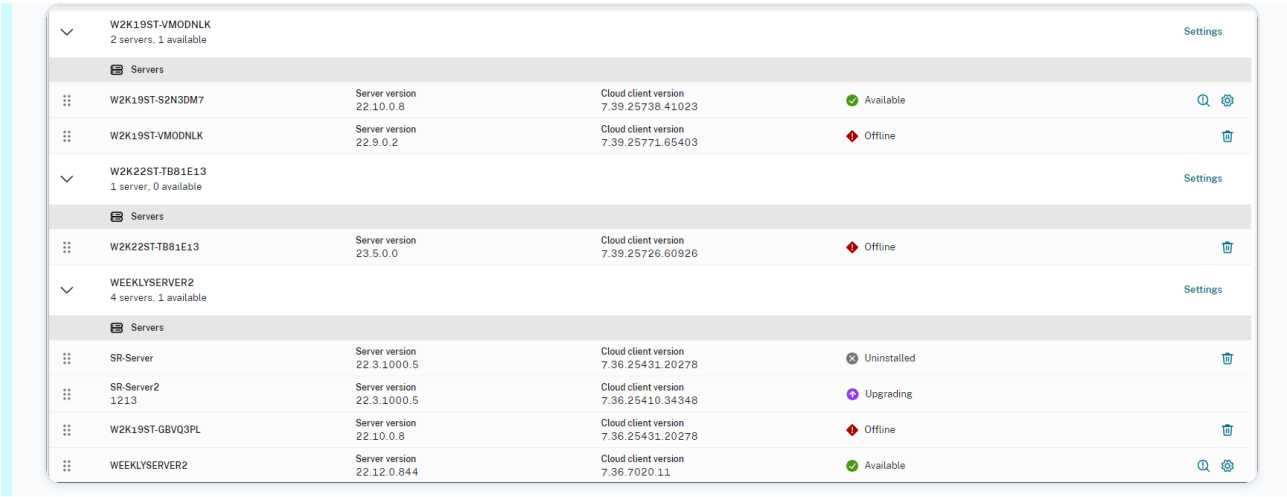
   |Server setting|Description| |--|--| |File storage location|Specifies where to store recorded session files. You can specify multiple locations to store files in a load-balanced manner.| |Certificate|Lets you select a machine certificate to sign recordings. If no certificate is provided, HTTP is used 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.| |Restore location for archived files|Specifies a location to temporarily store archived session recordings and make them available for playback.| |Recording notification|Customizes messages sent to end users to

notify them that their sessions are being recorded. You can select **Allow end user to deny recording of their session** to enable the feature that forces end users to explicitly consent to the session recording disclaimer before they can continue with their session. If end users accept the disclaimer, their session continues with session recording enabled. If end users deny the disclaimer, their session is terminated. When **Allow end user to deny recording of their session** is not enabled, the default notification message is **Your activity with the desktop or program(s) you recently started is being recorded**. If you object to this condition, close the desktop or program(s). Users can click **OK** to dismiss the window and continue their sessions.| |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.| | 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.



- **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

Session Recording policies let you control your recording environment. You can:

- Specify which VDA sessions are recorded.
- Specify which events are logged within recorded VDA sessions.
- Specify which actions to trigger automatically in response to detected events in recorded VDA sessions.
- Specify which endpoint sessions are recorded.

For more information, see:

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

Video about configuring policies:

Configure session recording policies

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.

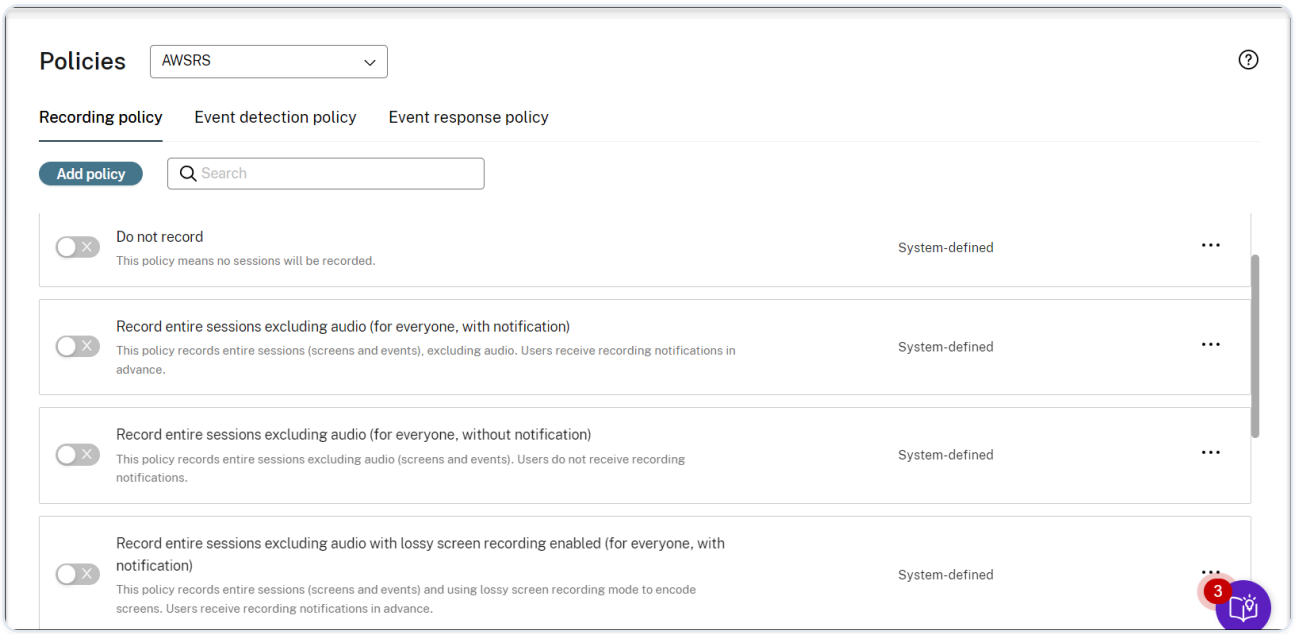
The active recording policy determines which sessions are recorded. Only one recording policy is active at a time.

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:



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

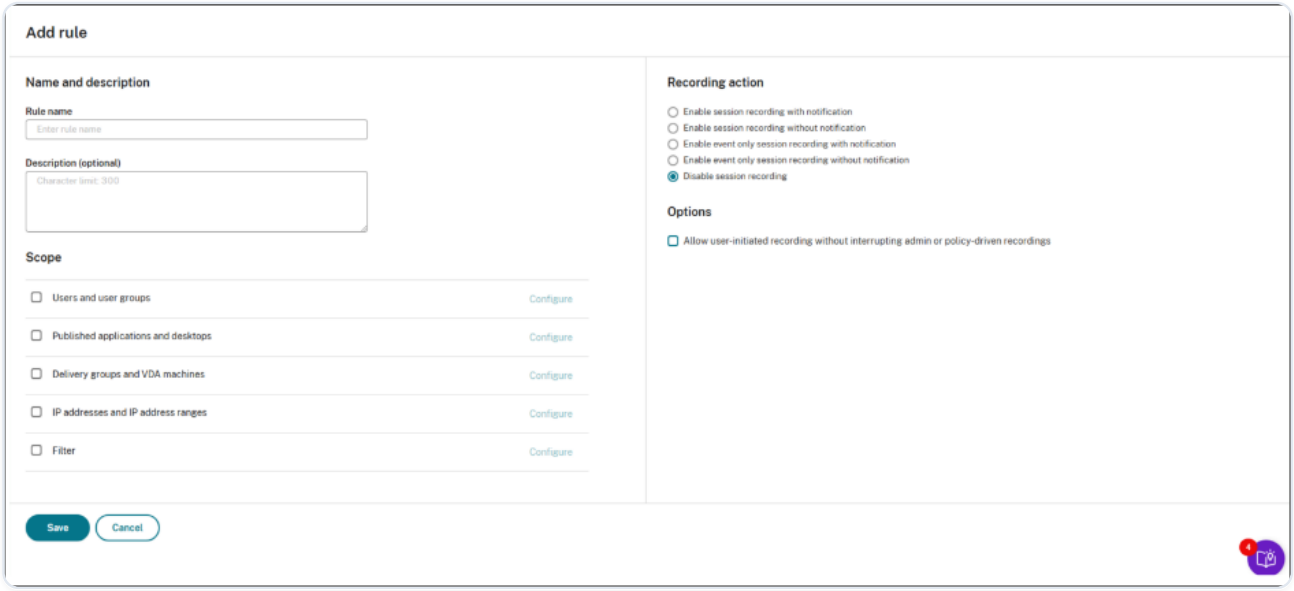
You can record sessions of specific users or groups, published applications or desktops, delivery groups or VDA machines, and Citrix Workspace™ app client IP addresses. To obtain the lists of published applications or desktops and delivery groups or VDA machines, you must have the **read** permission 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.

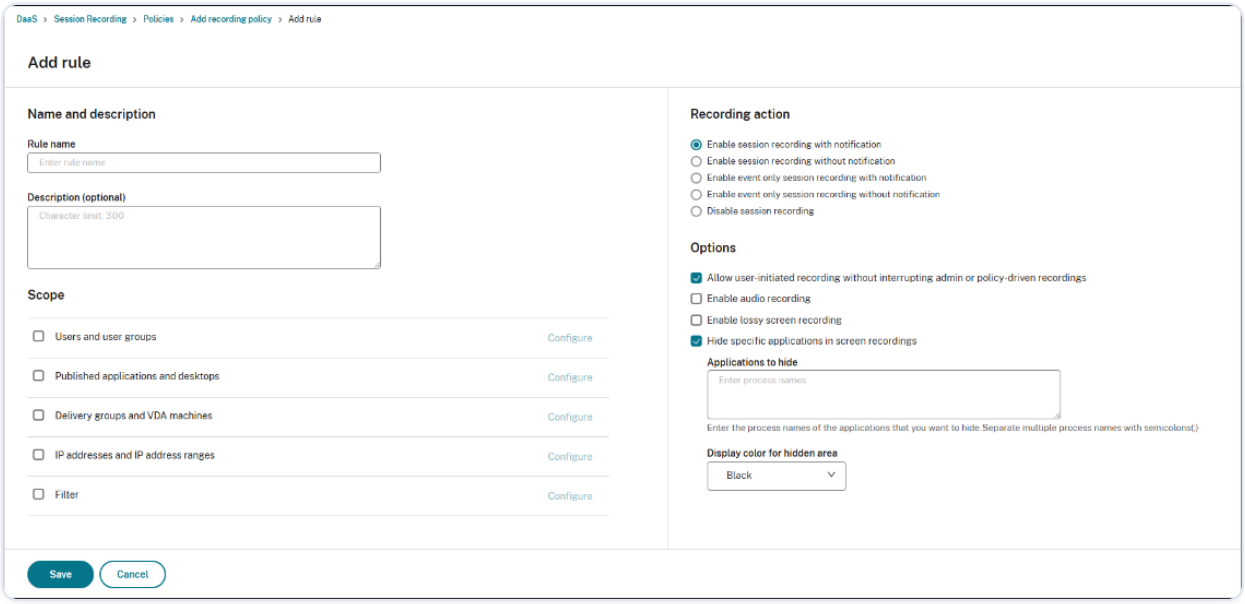
For each rule, choose one recording action:



- **Enable session recording with notification**. This option records entire sessions (screens and events). Users receive recording notifications in advance. With this option selected, you can

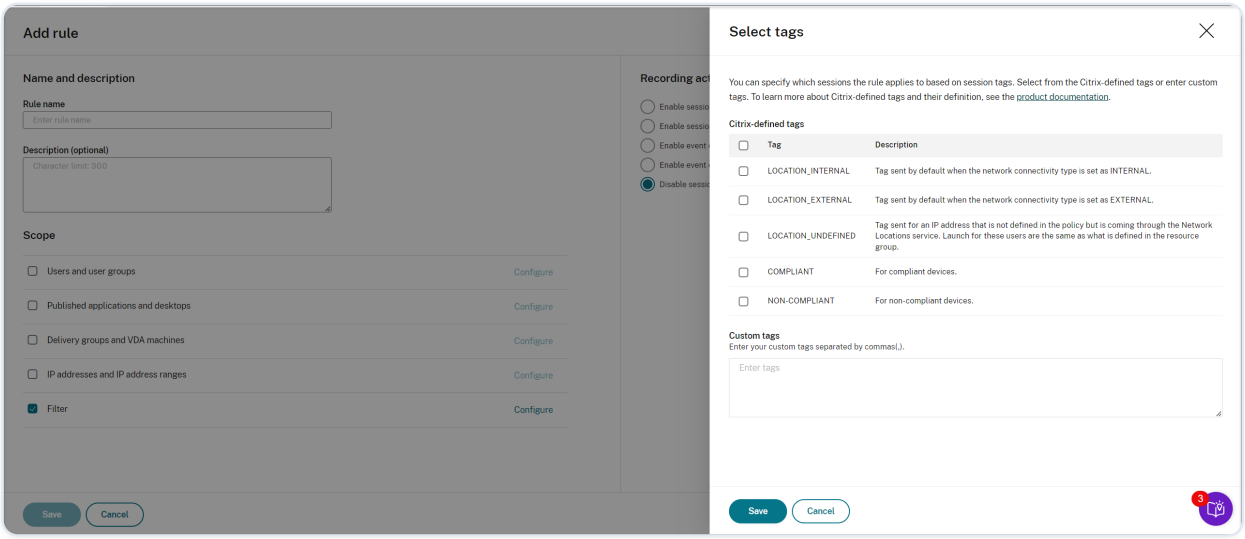
further select to enable audio recording or lossy screen recording. Additionally, you can choose to hide specific applications in screen recordings.

- **Enable session recording without notification**. This option records entire sessions (screens and events). Users do not receive recording notifications. With this option selected, you can further select to enable audio recording or lossy screen recording. Additionally, you can choose to hide specific applications in screen recordings.
- **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.
- **Allow user-initiated recording without interrupting admin or policy-driven recordings**. This feature lets end users start and stop recordings on demand. Administrator initiated and policy-driven recordings take precedence and are not interrupted by end user triggered recordings.
- **Hide specific applications in screen recording**. This feature requires that you select **Enable lossy screen recording**. It lets you hide specific applications with a layer mask during screen recording. The color for the layer mask is configurable, which can be Black, Gray, or White.



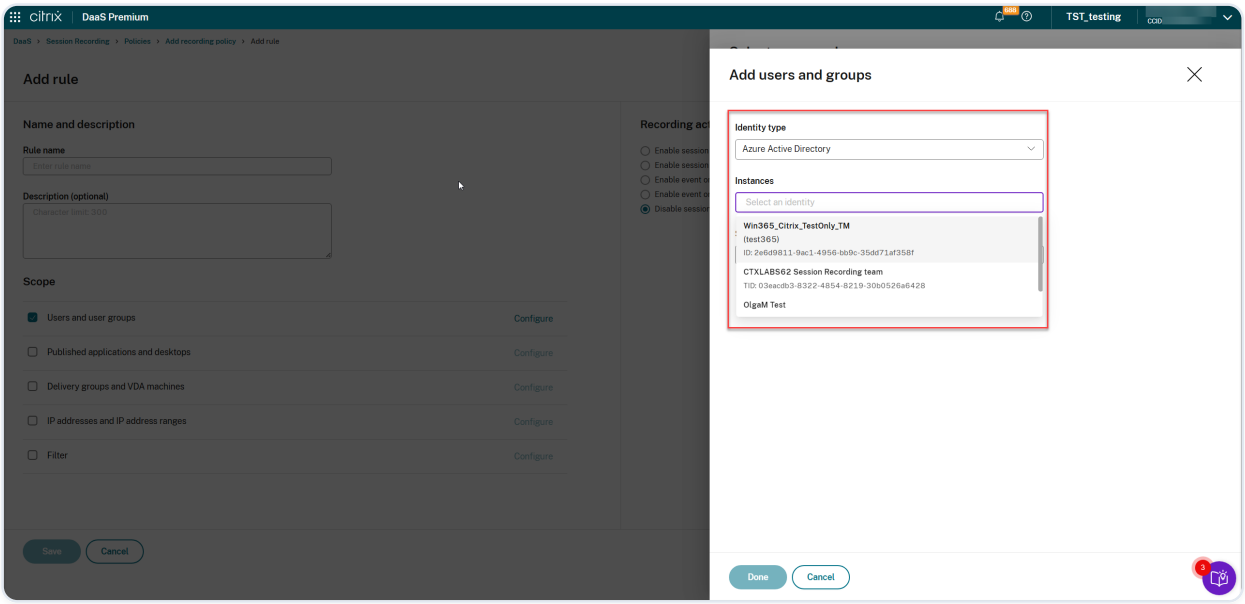
For each rule, choose at least one of the following items to create the rule scope. When a rule applies, both the "AND" and the "OR" logical operators are used to compute the final action. Generally speaking, the "OR" operator is used *within* a rule item, and the "AND" operator is used *between* separate 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. Selecting Azure AD as the identity provider allows you to choose an instance from the drop-down list. The available instances depend on your settings on the Citrix Cloud **Identity and Access Management > Authentication** tab. 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 **CommunicationProtocalToggle** to **1** (**0** means .net remoting. **1** means **Websocket**).
  - 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.

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. In the DaaS tile, scroll down in the left navigation pane and select **Session Recording**.
4. In the Session Recording service view, select **Policies** from the left navigation.
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.
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

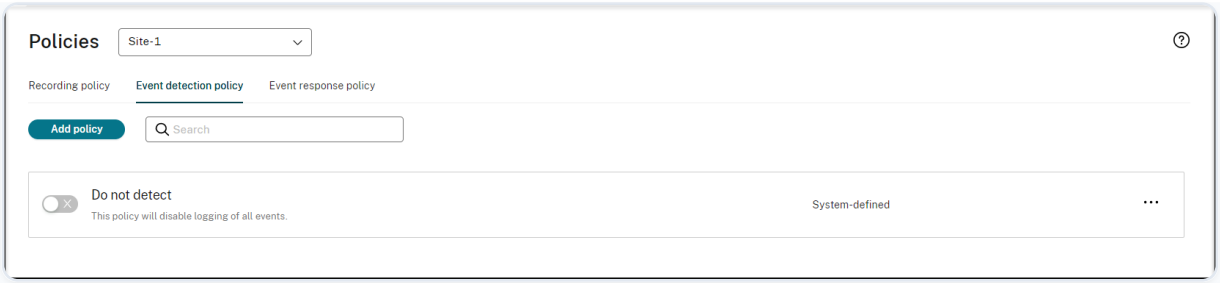


Configure event detection policies

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

- Printing activities
- Idle periods

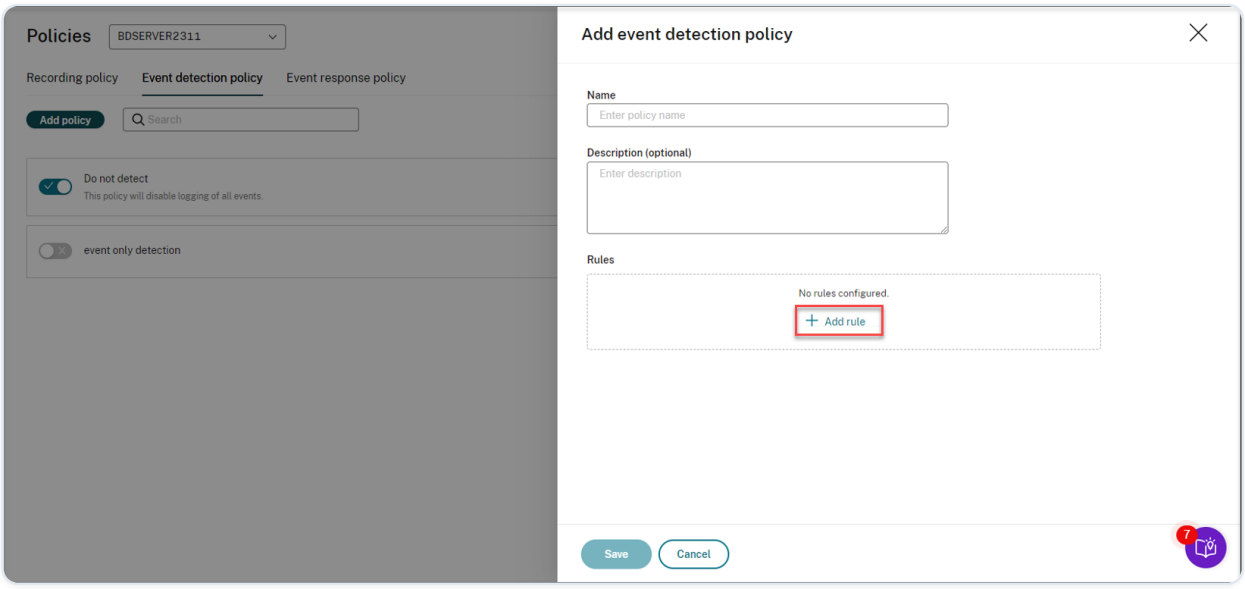
For more information about the various events, see the counterpart of the on-premises Session Recording documentation.

Create a custom event detection policy

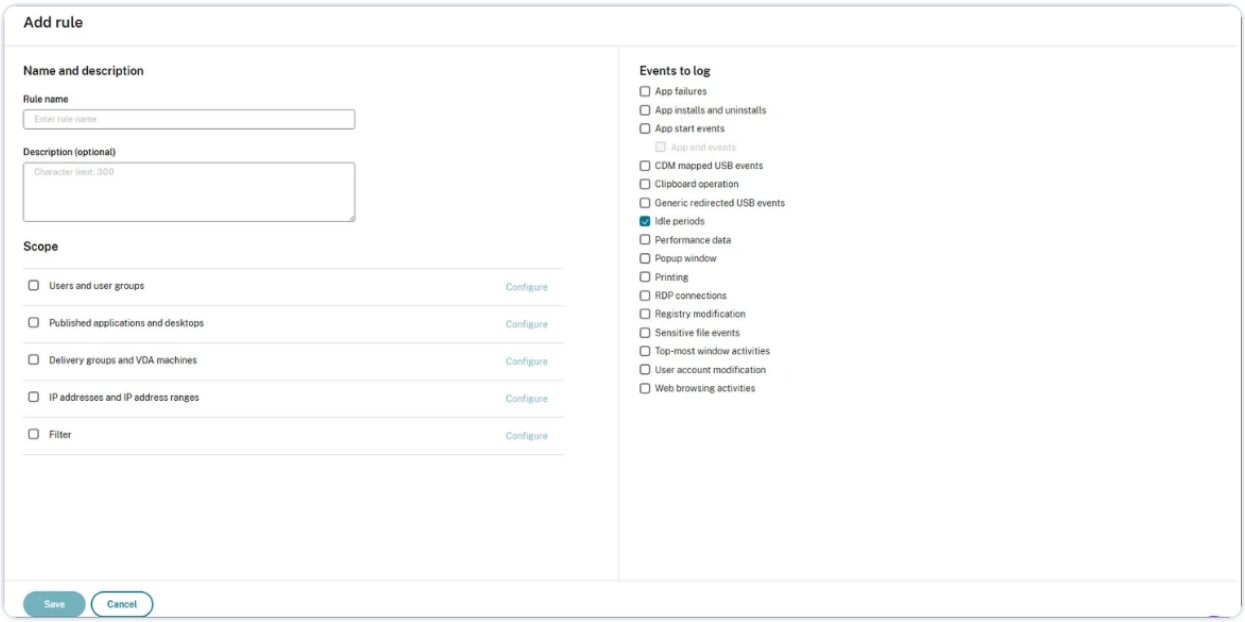
You can define which events to monitor by creating a custom event detection policy. Each policy can include one or more rules. For each rule, you specify the events to monitor and determine which sessions the rule applies to using the rule scope settings.

Steps

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.
3. In the DaaS tile, scroll down in the left navigation pane and select **Session Recording**.
4. In the Session Recording service view, select **Policies** from the left navigation.
5. Select a target site. The **Recording policy** tab is displayed by default.
6. Select **Event detection policy**.
7. Click **Add policy**.
8. Enter a name and description for the new policy, and then click **Add rule**.



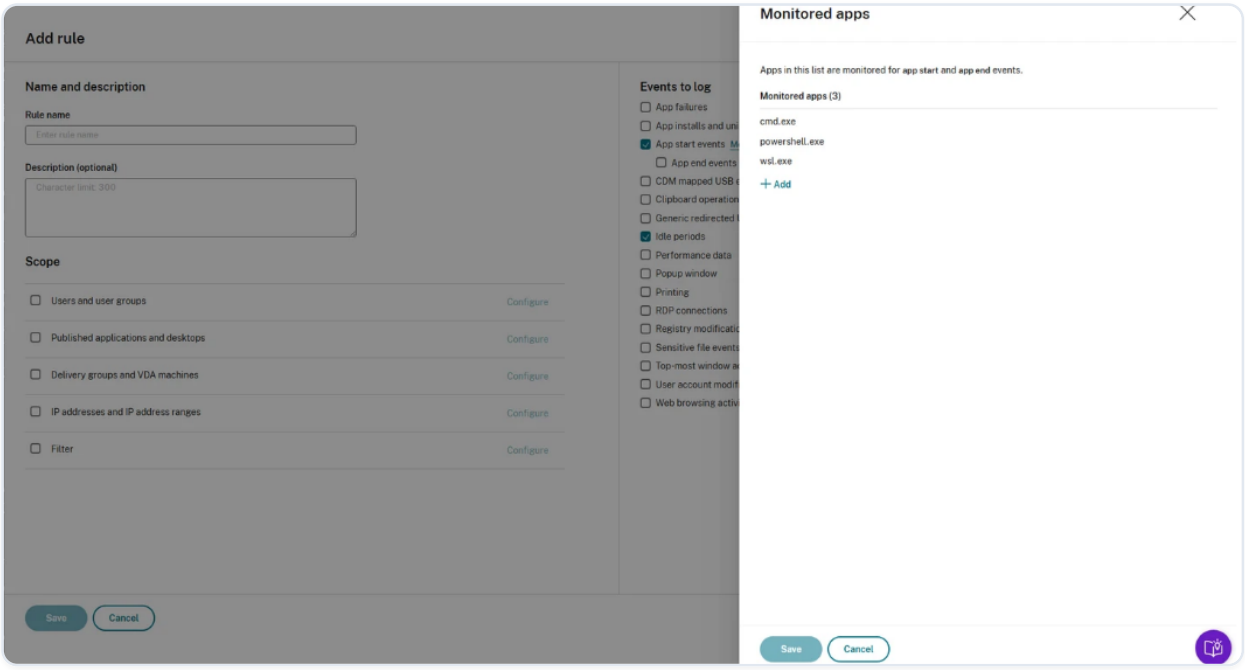
9. Enter a name and description for the rule.



10. Choose at least one of the following items to create the rule scope. For more information about the rule scope settings, see Create a custom event response policy.

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

11. Specify one or more target events to monitor by selecting the check box next to each event type. For exmaple, after you select **App start events**, you can click **Monitored apps** to specify target applications to monitor and to avoid an excessive number of events from flooding the recordings.



12. (Optional) Add more rules as needed. Each policy can include one or more rules.

Video about configuring policies

Configure event response policies

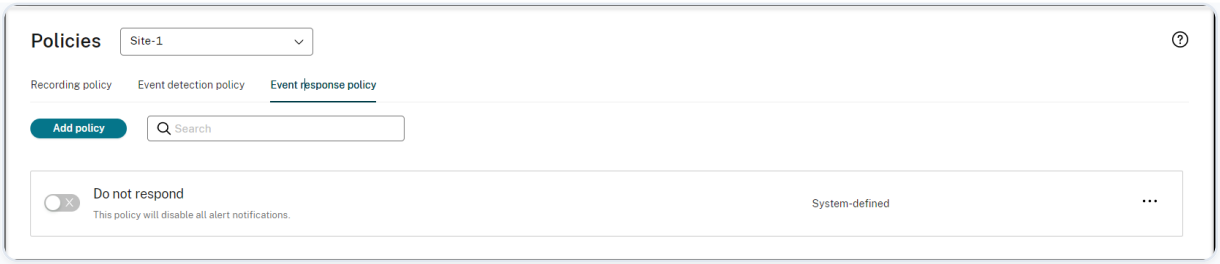
Event response policies let you configure event-triggered actions so that you can:

- 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.



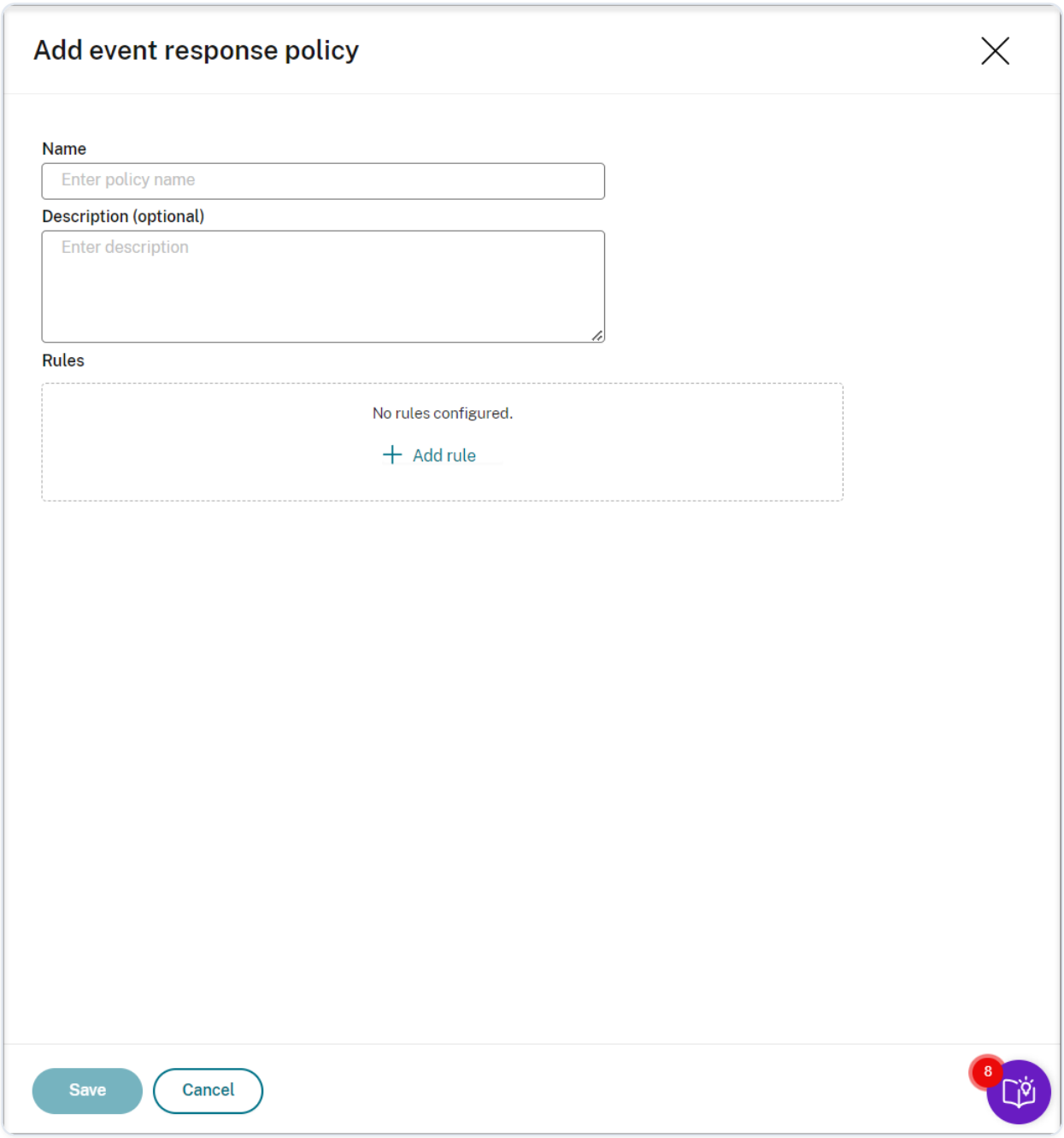
System-defined event response policy

Session Recording provides one system-defined event response policy:

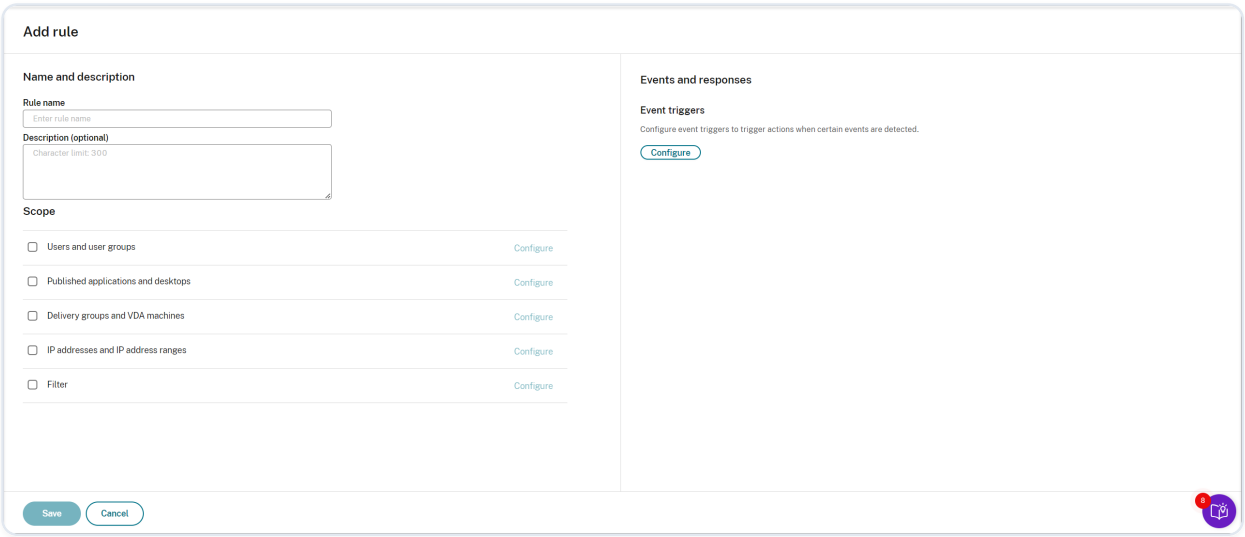
- **Do not respond**. By default, no action is taken in response to logged events in your recordings.

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.



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

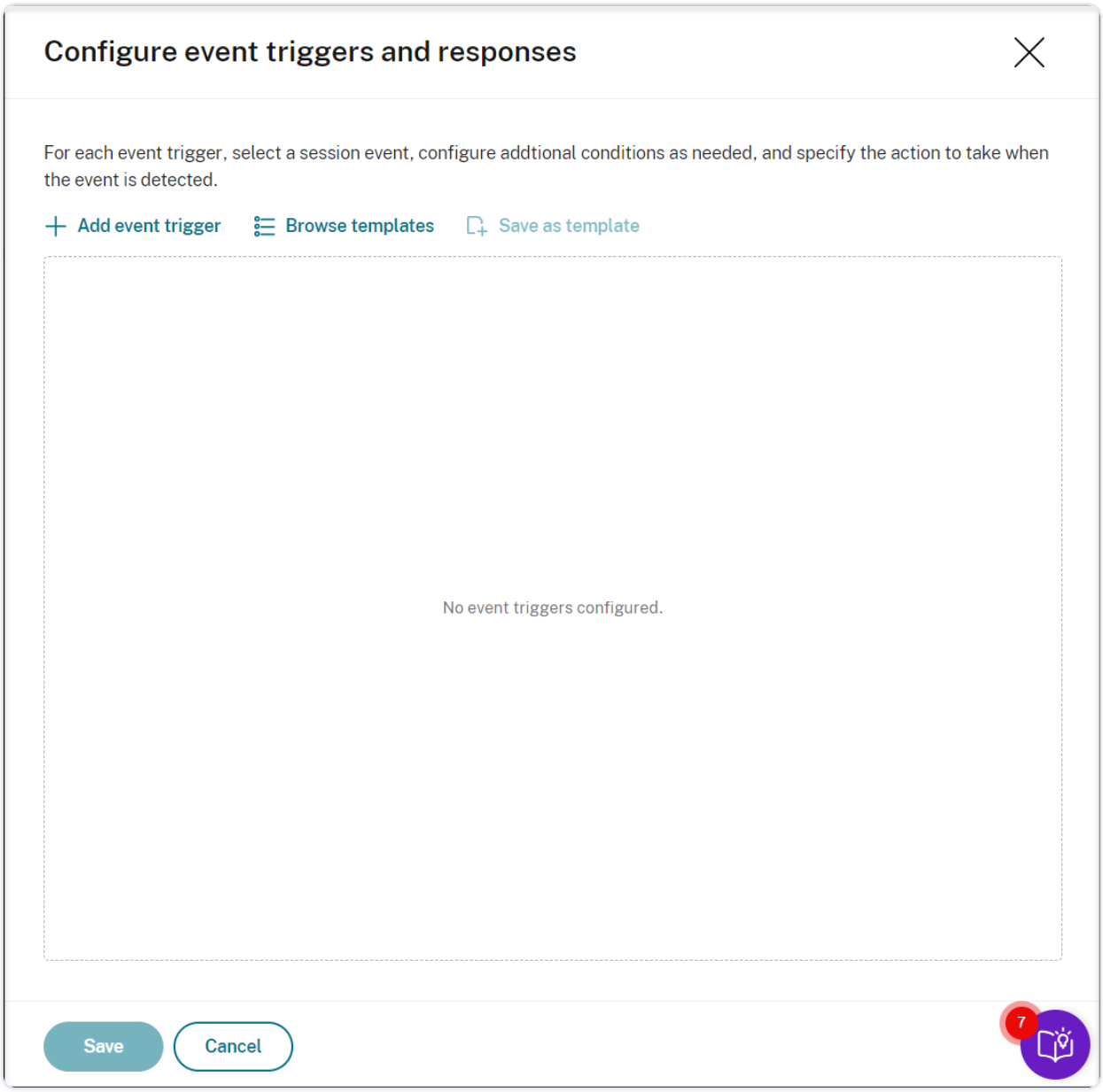


5. In the **Event triggers** section, click **Configure** to configure event-triggered actions so that you can:

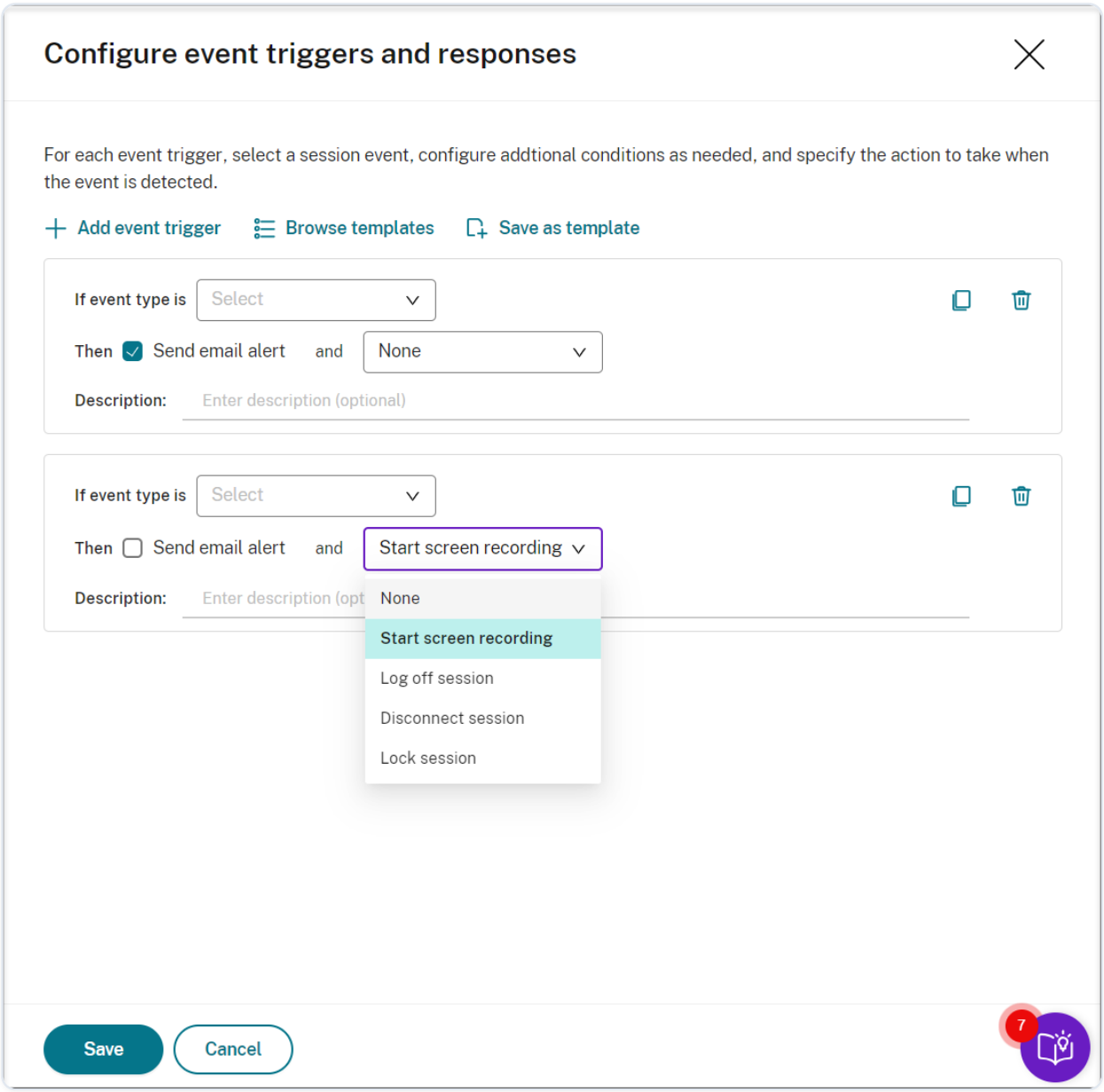
   - Send an email alert when a session start event is detected.
   - Take action (any combination of the following actions) when events are detected in recorded sessions

     - 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.

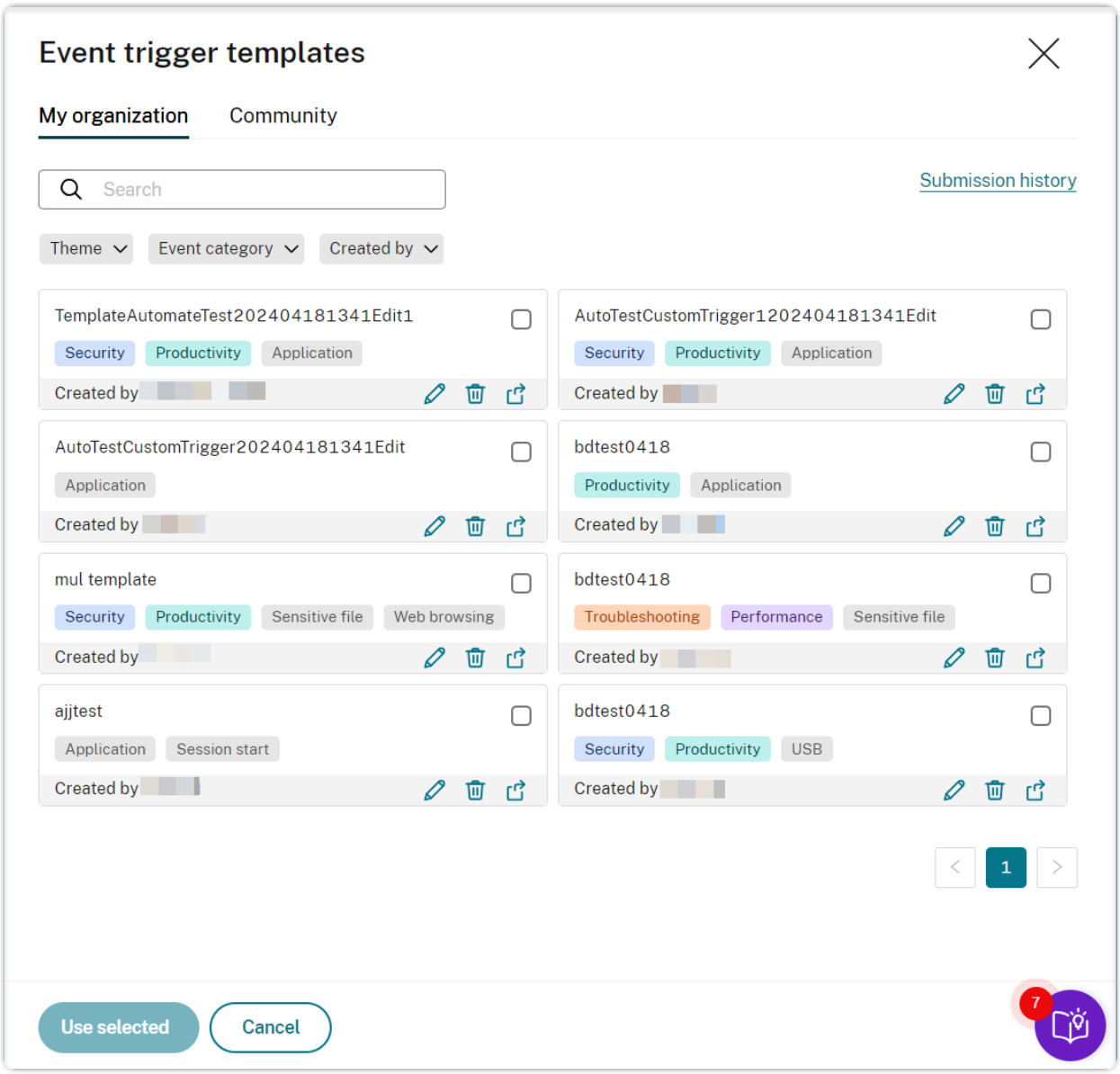


Each time you click **Add event triggers**, a new event trigger is created in the pane below. You can also click the **Duplicate** button to make duplicates of an existing event trigger.



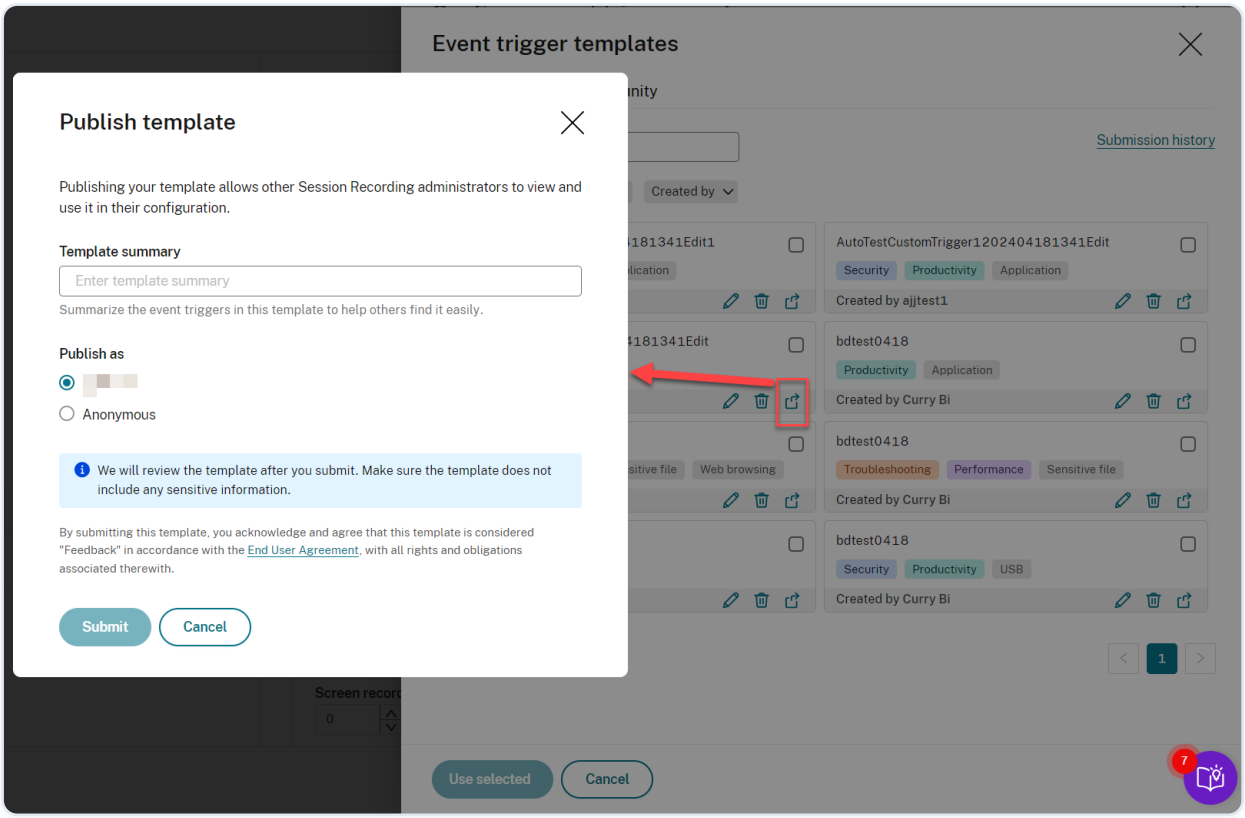
When you finish creating at least one event trigger, click **Save as template** to save your event triggers as a template. You can then find the new template on the **My organization** tab of the **Event trigger templates** page.

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.



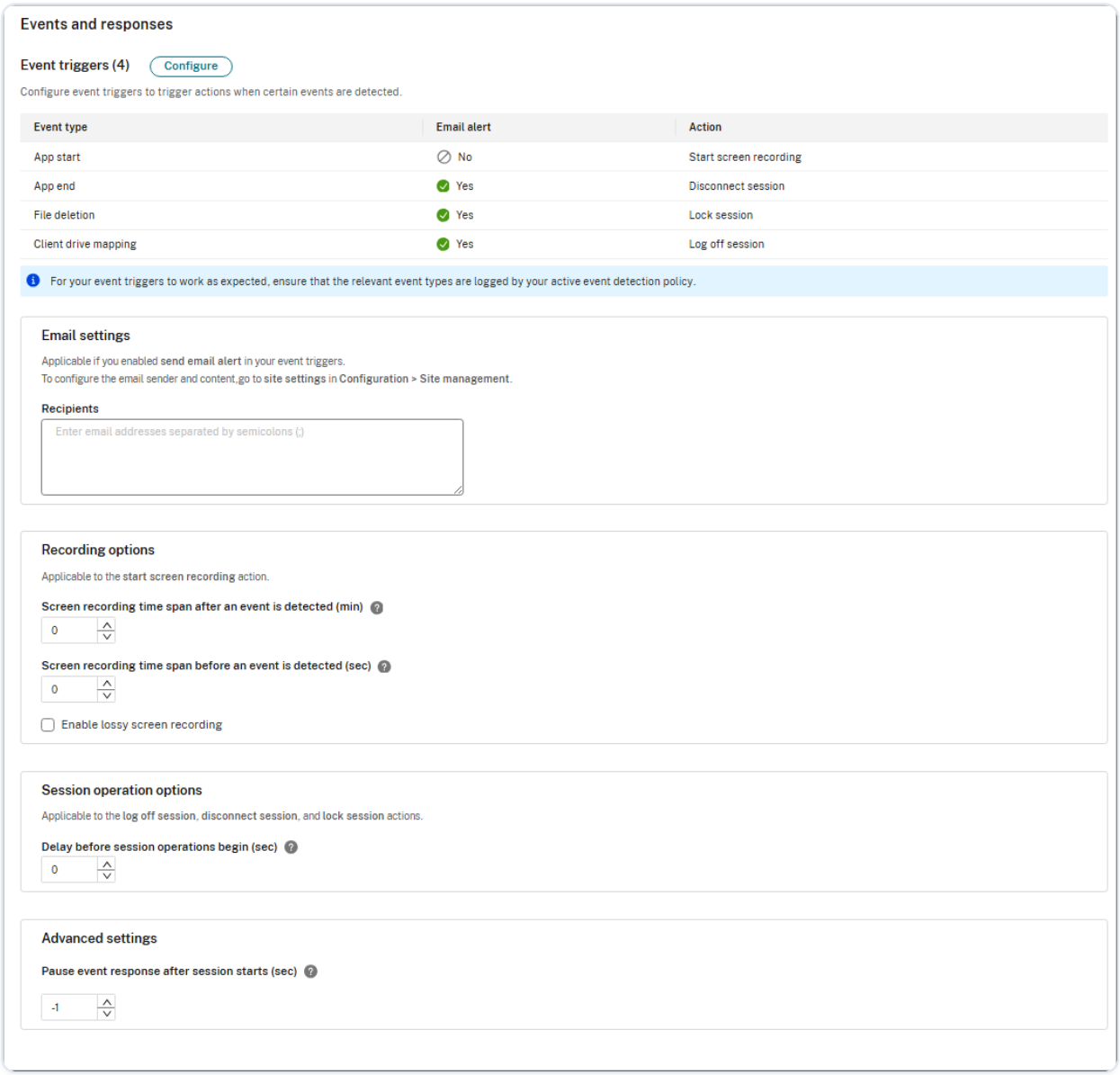
Note:

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.



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.

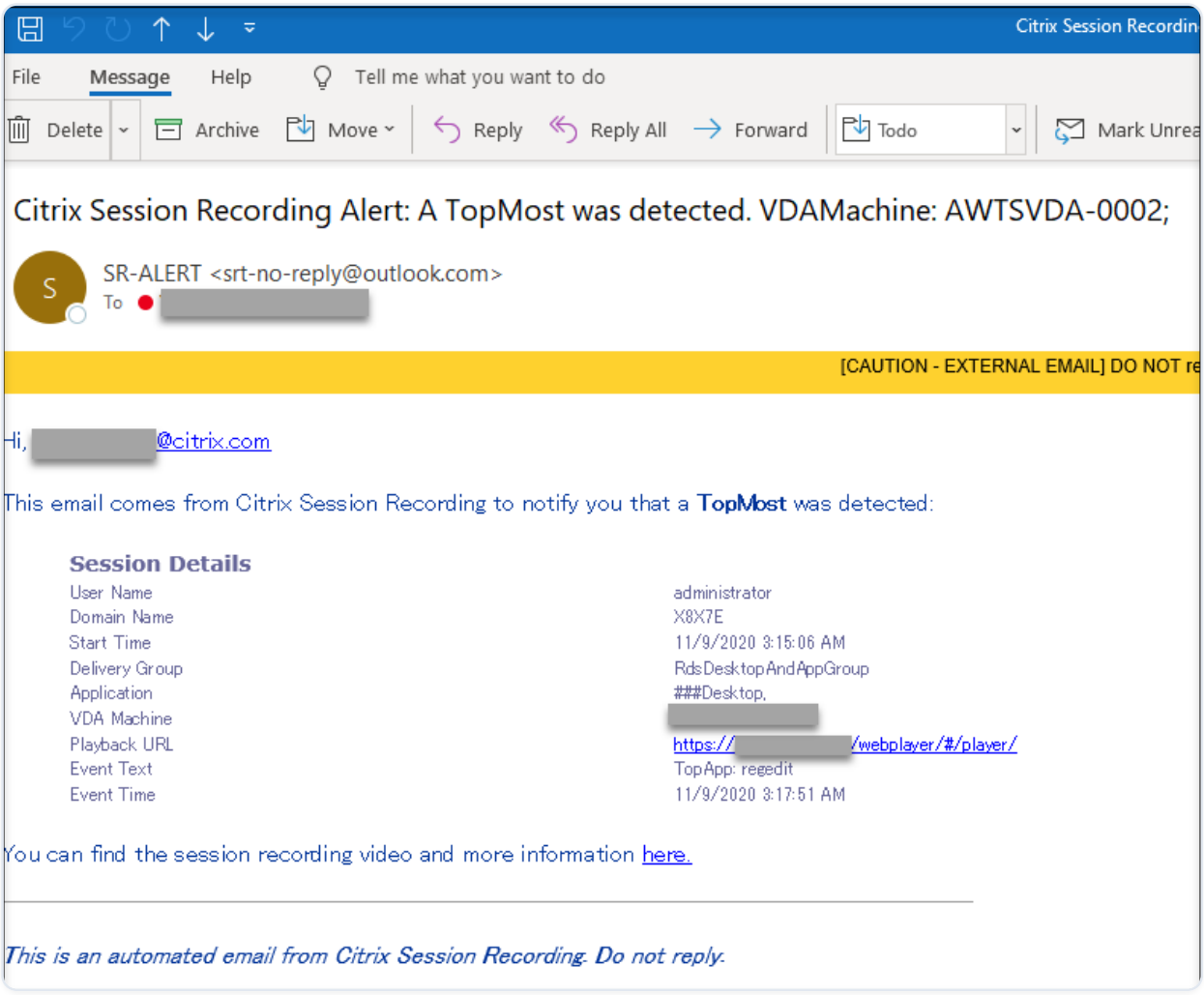
EVENT TYPE	DIMENSION	OPTION
App Start		
	App name	Includes, Equals, Matches
	Full command line	Includes, Equals, Matches
App End		
	App name	Includes, Equals, Matches
Top Most		
	App name	Includes, Equals, Matches
	Windows title	Includes, Equals, Matches
Web Browsing		
	URL	Includes, Equals, Matches
	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

EVENT TYPE	DIMENSION	OPTION
	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
Generic USB		
	Device name	Includes, Equals, Matches
Idle		
	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
Registry Delete		
	Key name	Includes, Equals, Matches
Registry Set Value		
	Key name	Includes, Equals, Matches

EVENT TYPE	DIMENSION	OPTION
	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
User Account Modification		
	User name	Includes, Equals, Matches
Unexpected App Exit		
	App name	Includes, Equals, Matches
App Not Responding		
	App name	Includes, Equals, Matches
New App Installed		
	App name	Includes, Equals, Matches
App Uninstalled		
	App name	Includes, Equals, Matches
RDP Connection		
	IP address	Includes, Equals, Matches
Popup Window		
	Process name	Includes, Matches
	Window content	Includes, Equals, Matches

EVENT TYPE	DIMENSION	OPTION
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:



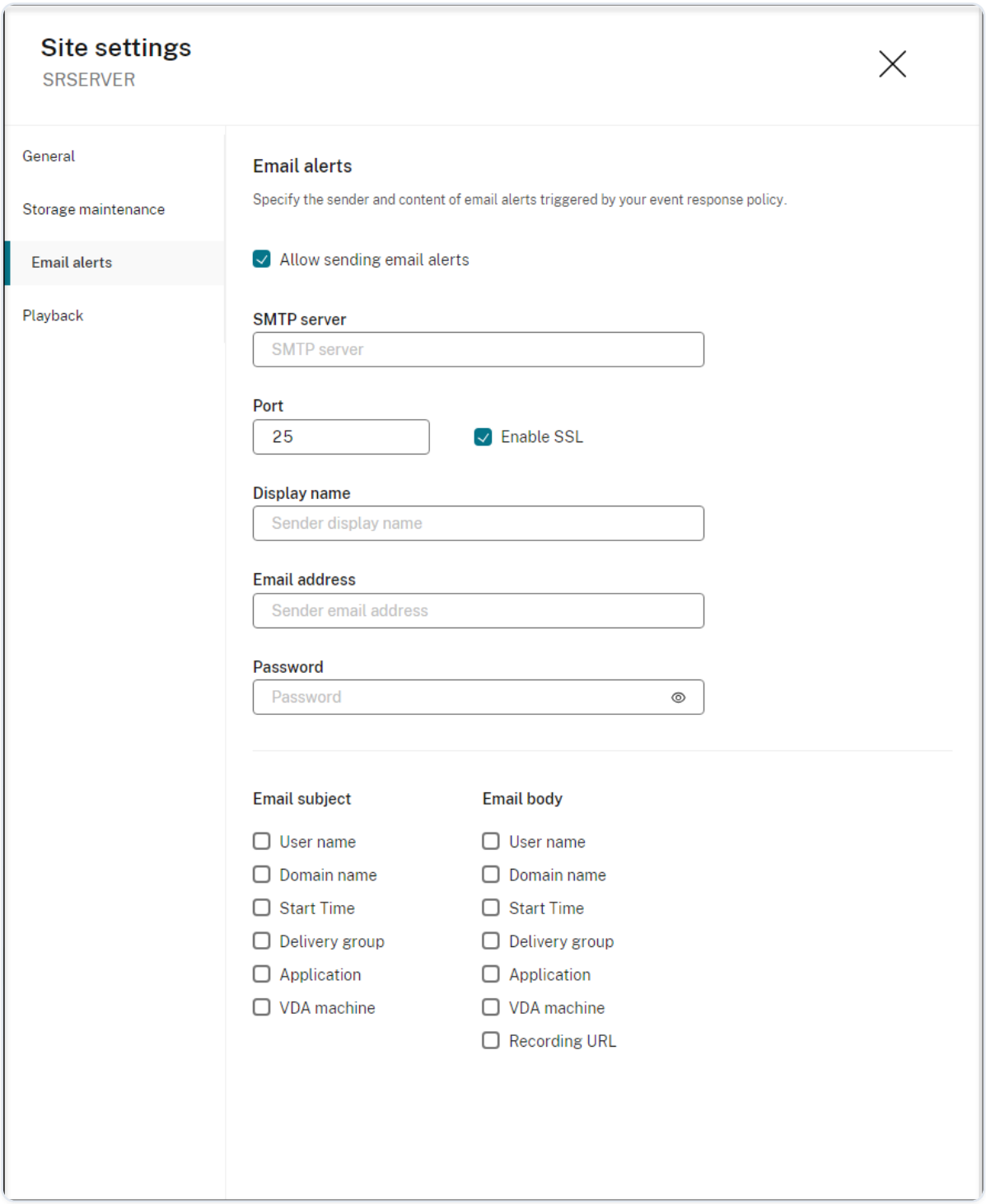
Tip:

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.



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.

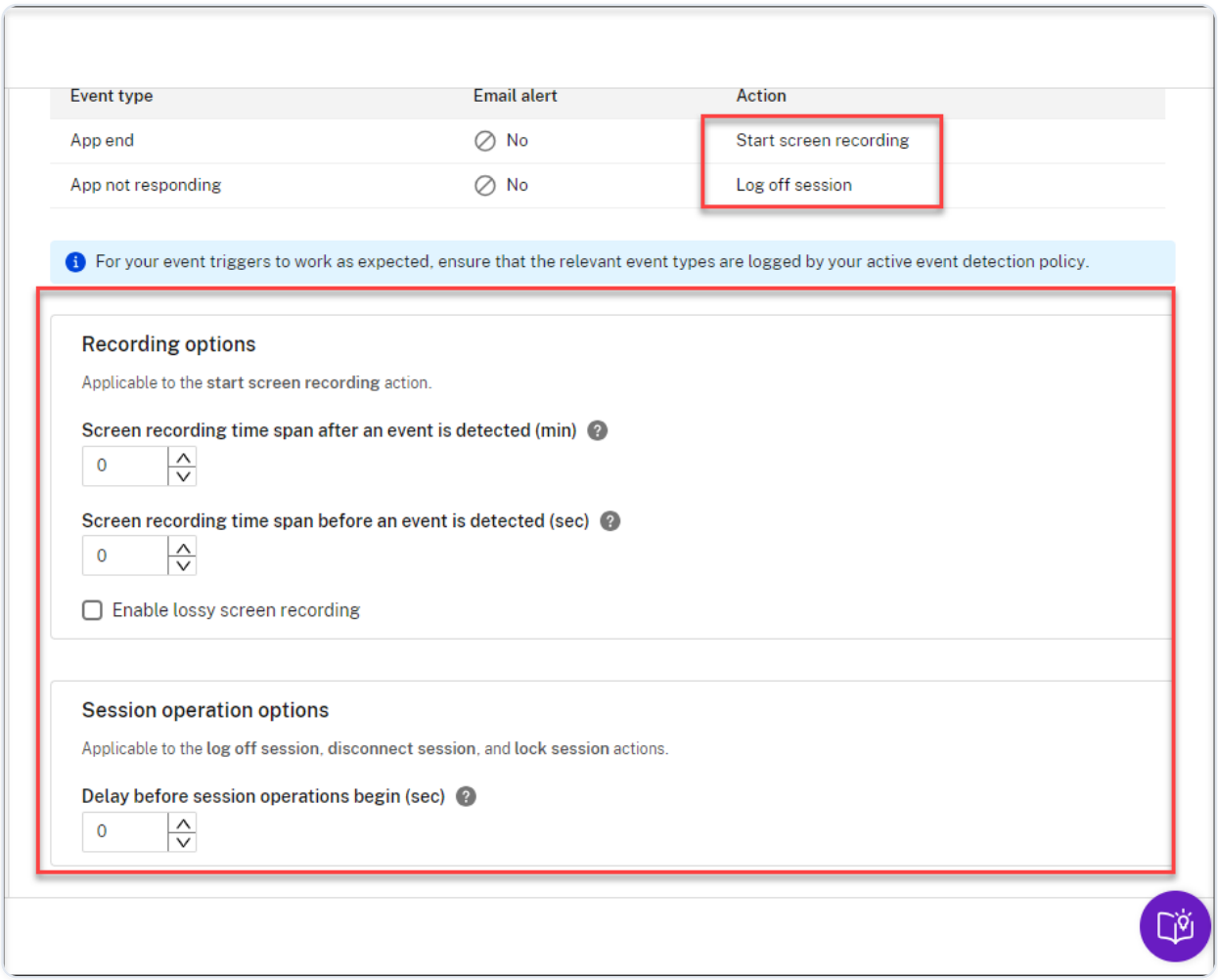
7. (Optional) To start screen recording immediately when certain events occur during an event-only recording, set the following options for dynamic screen recording in the **Recording options** section:

   - **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

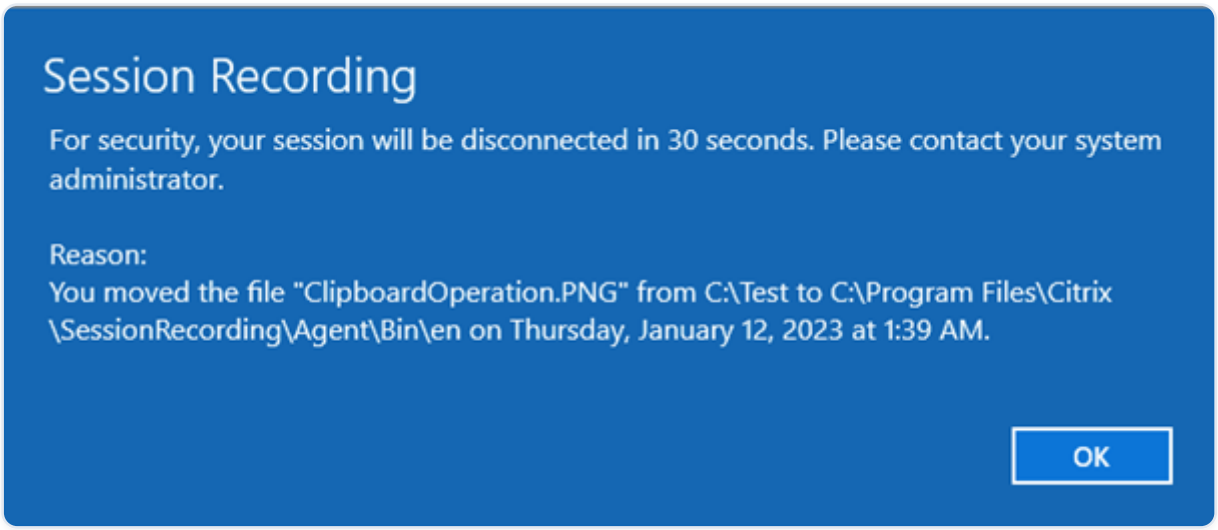
   For example:



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. (Optional) Specify pause event response after session start (sec) . Specify how many seconds (up to 300) you want to pause event response after a session starts.

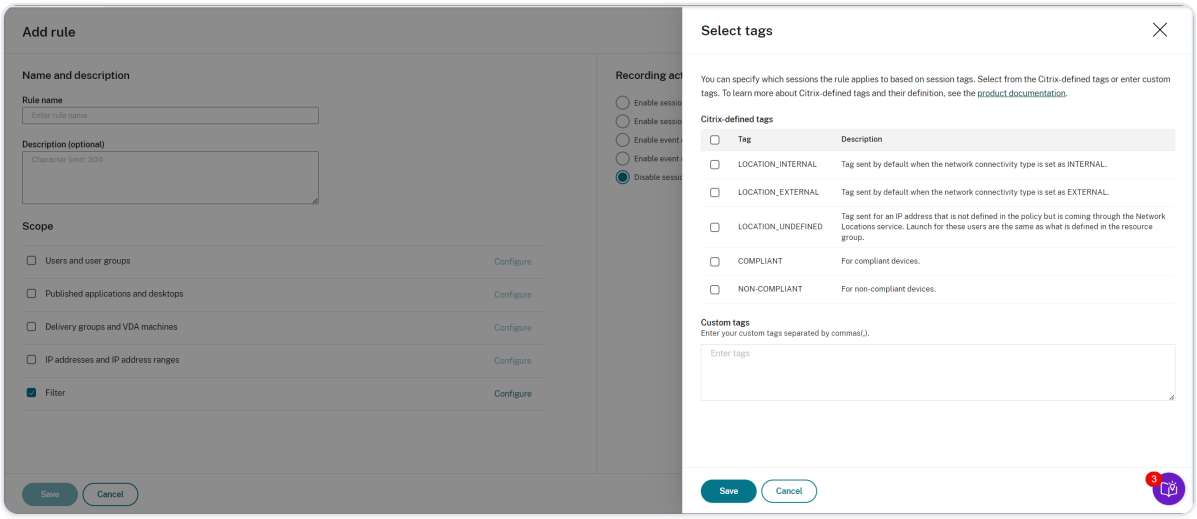
   > **Note:**
   >
   > By default, the value is set to -1, it means that the event response will not be paused.

10. 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. Selecting Azure AD as the identity provider allows you to choose an instance from the drop-down list. The available instances depend on your settings on the Citrix Cloud™ **Identity and Access Management > Authentication** tab. 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.

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

Video about configuring policies

Configure endpoint recording policies

You can define policies to capture user actions on endpoint devices when accessing Citrix-delivered web apps, virtual apps and desktops.

Prerequisites

Before you begin, ensure you have met the following requirements:

- Citrix Session Recording server version 2511 or later
- Citrix Workspace App version 2511 or later
- Proper integration with Citrix Gateway and StoreFront, see Site settings

> **Note:**
>
> Endpoint recording is triggered only when the ICA session is launched through Citrix Workspace app (CWA). Sessions launched by any other means are not recorded.

Configure endpoint recording policies

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

> **Note:**
>
> After you create or activate an endpoint recording policy, the policy applies to all Session Recording servers of the selected site. You can create and activate separate endpoint recording policies for different sites, but only one site's active policy can be in effect globally.

System-defined endpoint recording policies

Session Recording provides the following system-defined endpoint recording policies:



- **Do not record endpoint sessions**. The default policy. If you do not specify another policy, no sessions are recorded.

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

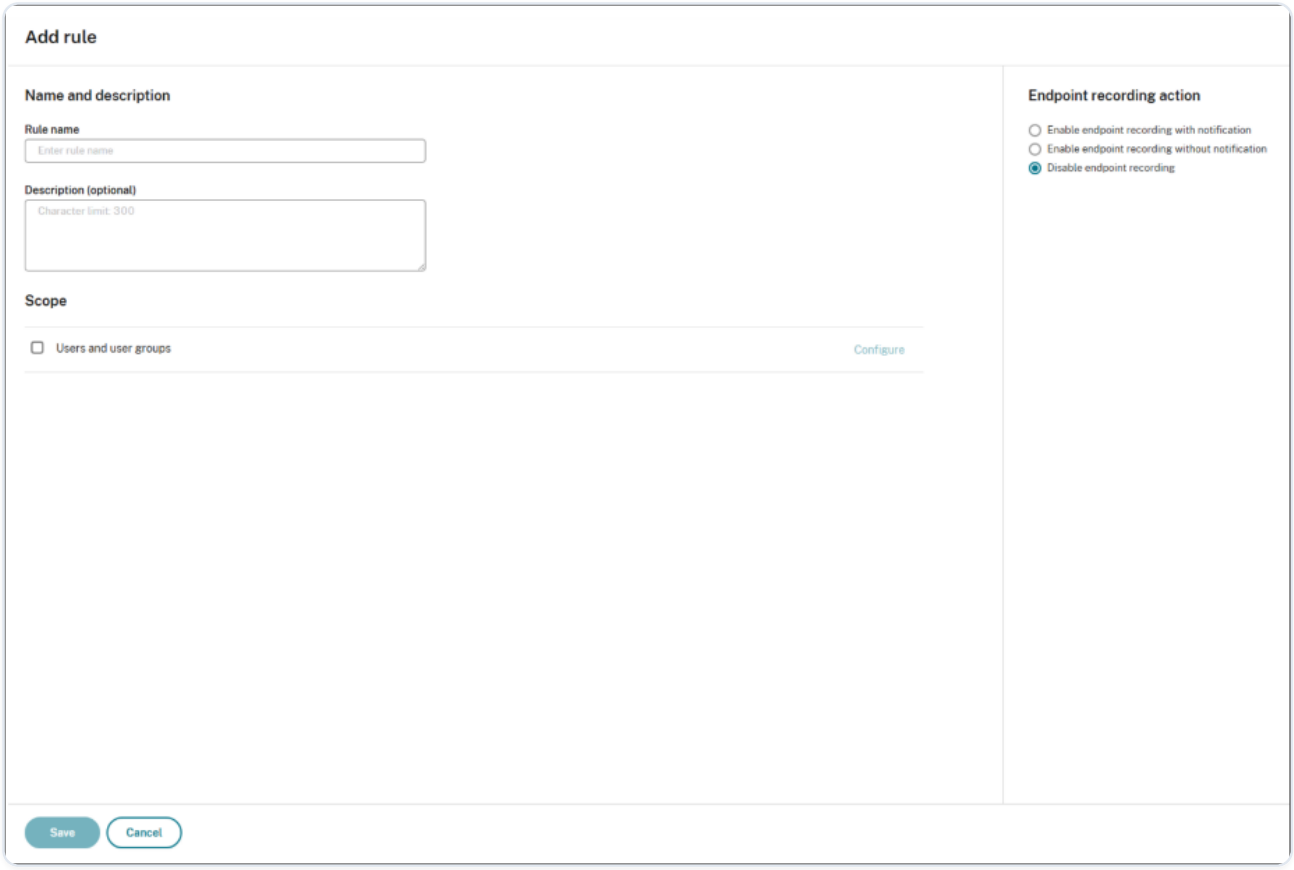
Create a customer endpoint recording policy

Considerations

You can record endpoint sessions of specific users or groups.

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

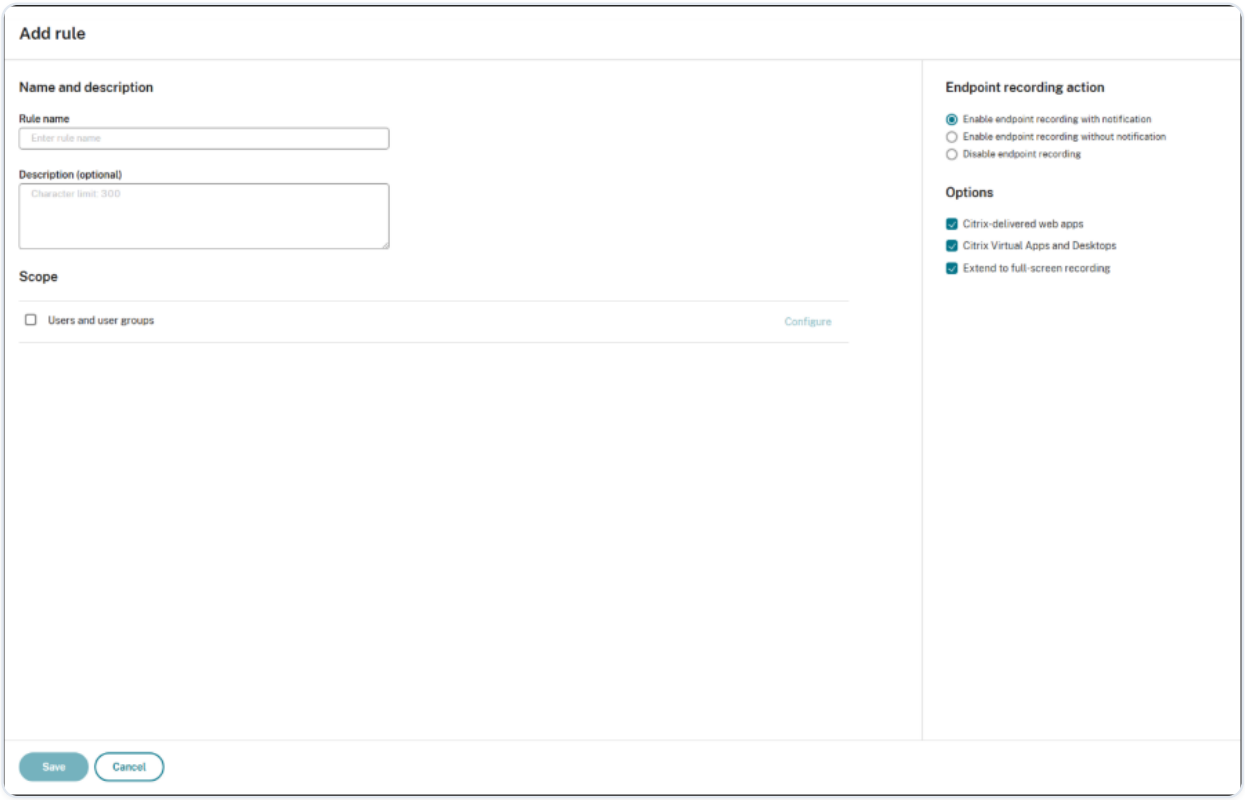
For each rule, choose one endpoint recording action:



- **Enable endpoint recording with notification**. This option records user actions on endpoint devices. Users receive recording notifications in advance. With this option selected, you can further select to enable recording for Citrix-delivered web apps or Citrix Virtual Apps and Desktops. Additionally, you can choose to extend to full-screen record in endpoint recording.
- **Enable endpoint recording without notification**. This option records user actions on endpoint. Users do not receive recording notifications. With this option selected, you can further

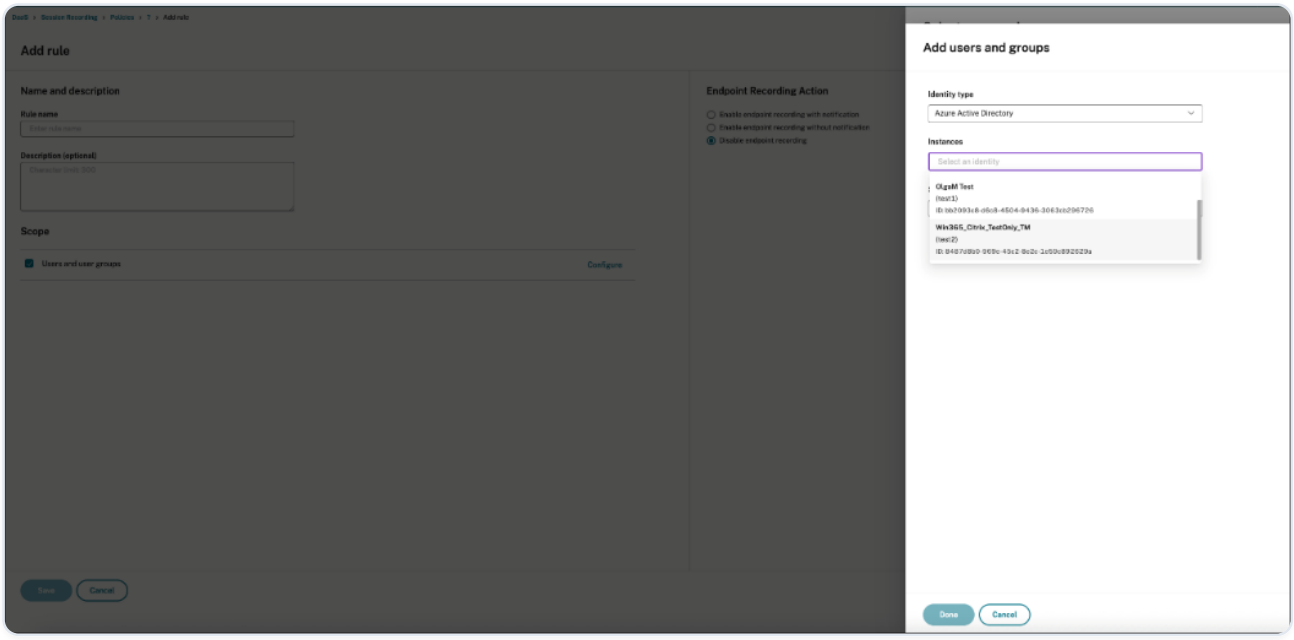
select to enable recording for Citrix-delivered web apps or Citrix Virtual Apps and Desktops. Additionally, you can choose to extend to full-screen record in endpoint recording.

- **Disable endpoint recording**. This option means that no user actions on endpoint devices are recorded.
- **Citrix-delivered web apps**. This option lets you record user actions on endpoint devices accessing these apps.
- **Citrix Virtual Apps and Desktops**. This option lets record user actions on endpoint devices accessing these apps.
- **Extend to full-screen recording**. This option lets you record the entire screen space, including any extended displays.



For each rule, choose the following items to create the rule scope.

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. Selecting Azure AD as the identity provider allows you to choose an instance from the drop-down list. The available instances depend on your settings on the Citrix Cloud **Identity and Access Management > Authentication** tab.



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 nonproduction environments. Citrix Technical Support doesn't support issues found with preview features.

When you create more than one rule in an endpoint 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 endpoint recording action** have the highest priority.
- Rules with the **Enable endpoint recording with notification** action have the second-to-highest priority.
- Rules with the **Enable endpoint recording without notification** action have the lowest priority.

Some sessions might not meet any rule criteria in an endpoint recording policy. For these sessions, the action of the policy fallback rule applies. The action of the fallback rule is always **Disable endpoint recording**. You can't modify or delete the fallback rule.

STEPS

1. Sign in to **Citrix Cloud**.
2. In the upper left menu, select **My Services > DaaS**.
3. In the DaaS tile, scroll down in the left navigation pane and select **Session Recording**.
4. In the Session Recording service view, select **Policies** from the left navigation.
5. Select a target site. Choose the **Endpoint recording policy**.
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 endpoint recording action and choose at least one of the following items to create the rule scope.

   For each rule, specify a recording action:

   - Enable endpoint recording with notification.
   - Enable endpoint recording without notification.
   - Disable endpoint recording.

   For each rule, choose the following items to create the rule scope:

   - Users and user groups.
9. After the new policy is created, find it on the Endpoint recording policy tab and turn the toggle on to activate the policy.

Select the global configuration site

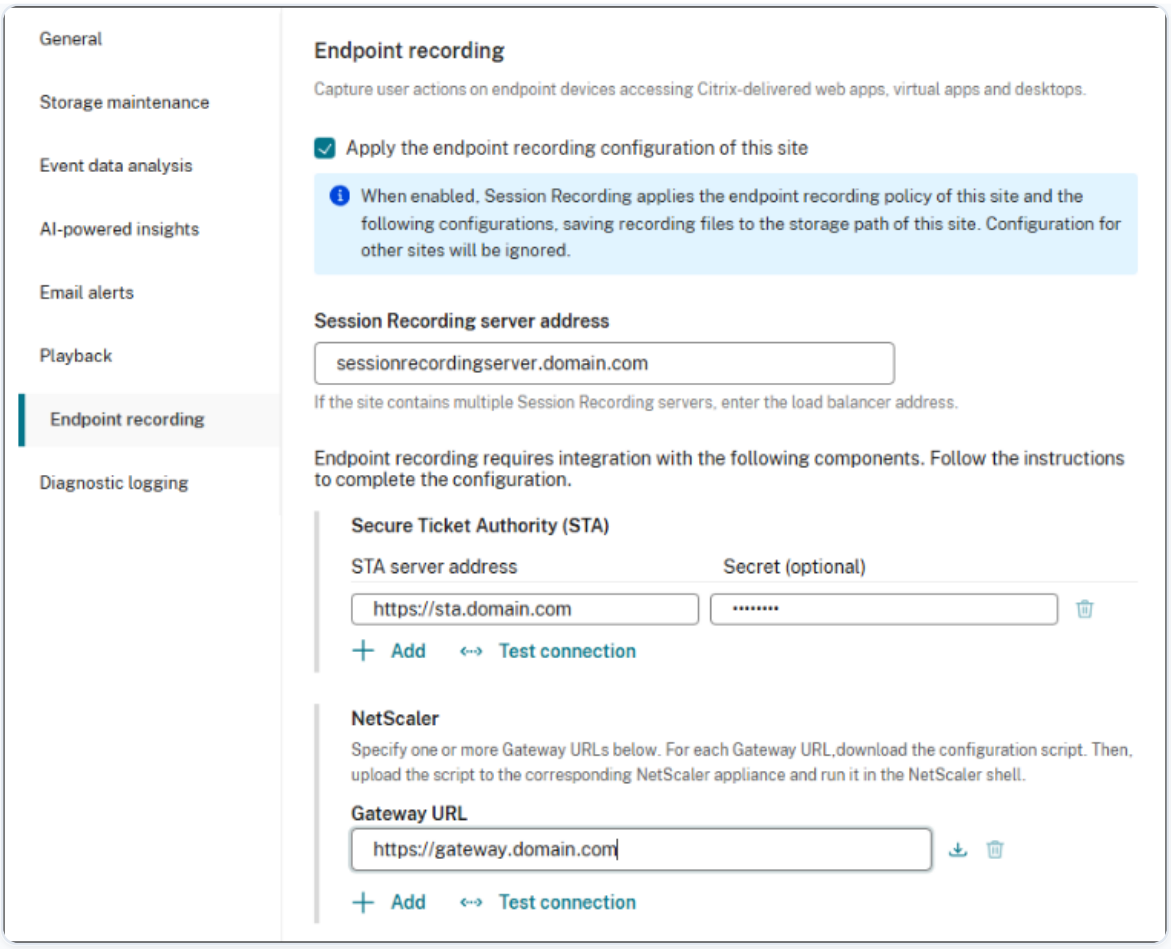
Although you can have different active policies on different sites, only one site's configuration and active policy can be in effect globally at any time.

STEPS

1. Select **Configuration > Site Management** from the left navigation of the Session Recording service.
2. Click **Settings** for the target site.
3. On the **Endpoint recording** page, enable the checkbox of **Apply the endpoint recording configuration of this site**.

   > **Note:**

- By checking this box, you are making this site the single source for all endpoint recording.
- The active policy and configuration you set for this site will now be applied globally. Recording files will be saved to this site's storage path.
- All endpoint recording policies and configurations on all other sites will be ignored.



4. Complete the other configuration fields.

   - **Session Recording server address**: e.g., `https://SRServer.domain.com`
   - **STA server address**: e.g., `https://sta.domain.com`
   - **Gateway URL**: e.g., `https://gateway.domain.com`
   - **(Optional) StoreFront server address**: e.g., `https://storefront.domain.com/citrix/store`
     - Required for On-premised StoreFront.
     - Leave this blank if you are using Citrix Cloud StoreFront.

> **Note:**
>
> By default, the Cloud StoreFront integration is disabled. You must set the following registry key to enable the Citrix Workspace app to communicate with the Cloud StoreFront service.
>
> - For 64-bit Citrix Workspace App

```
Location: HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle

Name: EnableCwaToSraCloudstore

Type: String

Value: true
```

> - For 32-bit Citrix Workspace App

```
Location: HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle

Name: EnableCwaToSraCloudstore

Type: String

Value: true
```

Integrate the Session Recording server with StoreFront

> **Note:**
>
> This step can be skipped if you are using Citrix Cloud Workspace (cloud-hosted StoreFront).
>
> Perform the following steps to configure StoreFront manually.

1. Download the script from the Session Recording Web Console (Configuration> Site Settings-> Endpoint recording-> StoreFront areas.
2. Click the download icon corresponding to the StoreFront entry for which the configuration changes must be made. The downloaded zip file contains a configuration script, a README file, and a configuration cleanup script. The cleanup script can be used in case integration between StoreFront and Session Recording Server is to be removed.

   The download button will be enabled when the Session Recording Server address and Storefront address are both not empty.
3. Run the script as an admin on a PowerShell 64-bit instance by using the command. / ConfigureStorefront.ps1.

   - No other parameters are required.
   - The PowerShell script execution policy must be set to Unrestricted or Bypass to run the StoreFront script.
   - The script also propagates the configuration to other StoreFront servers if StoreFront is configured as a cluster.

Integrate the Session Recording server with Secure Ticket Authority

> **Note:**
>
> This step can be skipped if using On-prem StoreFront.

1. STA is an XML web service that exchanges XenApp® server information for randomly generated tickets. It is used to control access for a Citrix Secure Gateway server.
2. Use your Citrix account credentials to access the Citrix Virtual Apps and Desktops™ download page and download the product ISO file. Unzip the ISO file or burn a DVD of it.
3. Use a local administrator account to log on to the machine in your trusted network and that is accessible by the Session Recording Server. Insert the DVD in the drive or mount the ISO file. The installer can be found in `x64/Citrix Desktop Delivery Controller/Sta_Service_x64.msi`.
4. Install the secure ticket authority server. On a trusted machine, mount the CVAD product ISO and install the STA service from `x64/Citrix Desktop Delivery Controller/Sta_Service_x64.msi`.
5. Configure Secure Ticket Authority service.

a. This step is mandatory if sta service is installed in the same machine with session recording server.

   i. Update new ports for STA service: navigate to `"C:\Program Files\Citrix\StaService\Service"`

   ii. `run.\StaService.exe -StoreFrontPort 8980 -StoreFrontTlsPort 8443`

b. Update Certificate Binding for New HTTPS Port.

c. Restart Citrix Secure Ticketing Authority Service in Windows Services Management.

Integrate the Session Recording server with NetScaler

> **Note:**
>
> This step can be skipped if the endpoint devices and the Session Recording server are in the same internal network (intranet). Otherwise, NetScaler configuration is required.

1. On the Session Recording server, download the generated NetScaler configuration script from the Session Recording Web Console Configuration> Site Settings-> Endpoint recording-> Gateway areas.
2. Upload the script to the NetScaler appliance. You can use tools such as **WinSCP** or a **scp** command similar to the following:

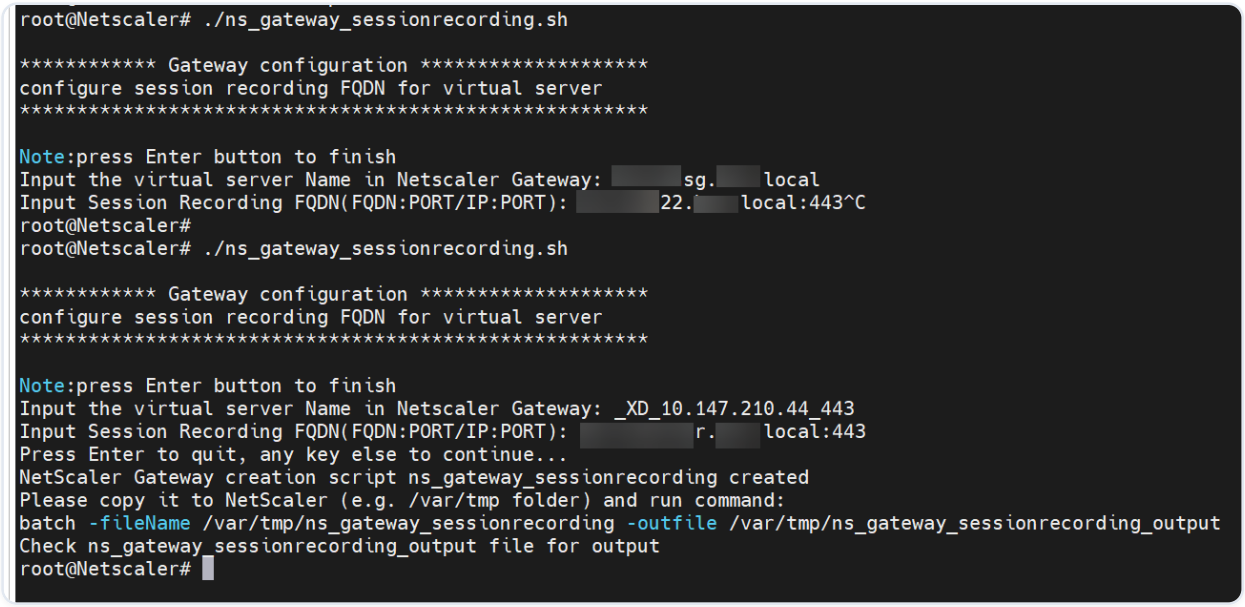
   ```
   scp ns_gateway_sessionrecording.sh root@NetScaler:/var/tmp
   ```

   (Replace **NetScaler** with the actual host name or IP address.)

   Ensure that the script is saved with LF (Line Feed) line endings. FreeBSD (which NetScaler OS is based on) does not support CRLF (Carriage Return Line Feed) line endings. If you encounter the error **-bash: /var/tmp/ns_gateway_sessionrecording.sh: /bin/sh\^M: bad interpreter: No such file or directory**, it indicates incorrect line endings. Convert the script using a text editor such as Notepad++ and ensure that it's saved with LF line endings.
3. Connect to the NetScaler appliance through SSH and switch to the NetScaler shell by typing **shell** in the NetScaler CLI.
4. Make the uploaded script executable using the **chmod** command:

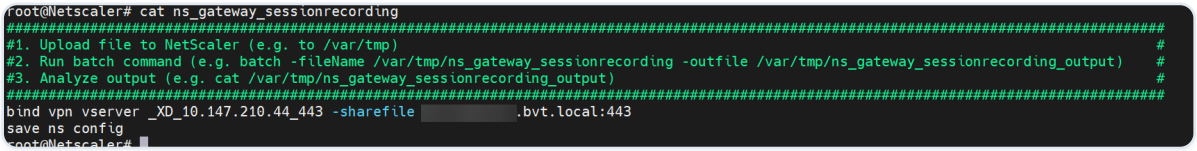
```
Chmod +x  /var/tmp/ns_gateway_sessionrecording.sh
```

5. Run the uploaded script in the NetScaler shell.



6. Provide the required parameters. The script prompts you for the following:

   - The name of the virtual server in NetScaler Gateway, which can be found in the NetScaler console.
   - The Fully Qualified Domain Name (FQDN) of the Session Recording server (or load balancer if applicable).
   - The script generates a new file, **/var/tmp/ns_gateway_sessionrecording**, containing multiple NetScaler commands. You can review the input parameters using the **cat /var/tmp/ns_gateway_sessionrecording** command.



7. Return to the NetScaler CLI and run the generated commands using a **batch** command similar to the following:

```
batch -fileName /var/tmp/ns_gateway_sessionrecording -outfile /var/tmp/
ns_gateway_sessionrecording_output
```

   NetScaler executes the commands sequentially. If a command fails, it proceeds to the next.

8. Ensure that all commands were successfully completed.

```
> batch -fileName /var/temp/ns_gateway_sessionrecording -outfile /var/temp/ns_gateway_sessionrecording_output
 Done
>
```

9. Add Secure Ticket Authority(STA) server address in NetScaler. For more information, see Configure NetScaler Gateway to handle the STA and ICA traffic

> **Note:**
>
> If you are using Citrix Workspace app for Windows version 2503, ensure that ICA® Proxy mode is set to OFF on the Citrix NetScaler Gateway to enable endpoint recording functionality.
>
> For detailed configuration steps, refer to the NetScaler command reference guide.

> **Note:**
>
> For more detailed information on configuration steps, refer to session recording for endpoint devices.

Playback permissions

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

SESSION RECORDING SERVICE		
TYPE OF SESSION RECORDING ADMINISTRATOR	**PLAYBACK PERMISSION**	**REMARKS**
Citrix Cloud administrator assigned the **Cloud Administrator** 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-FullAdmin** 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** 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** 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.

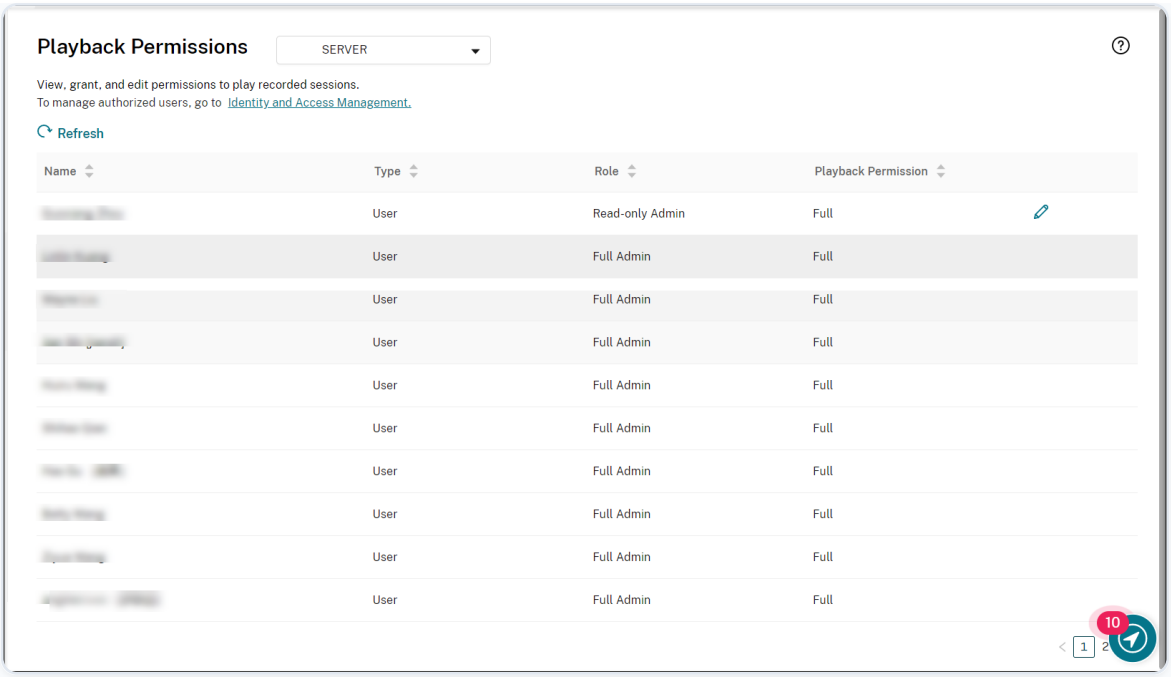
Limit the playback permission of a Session Recording read-only administrator

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:

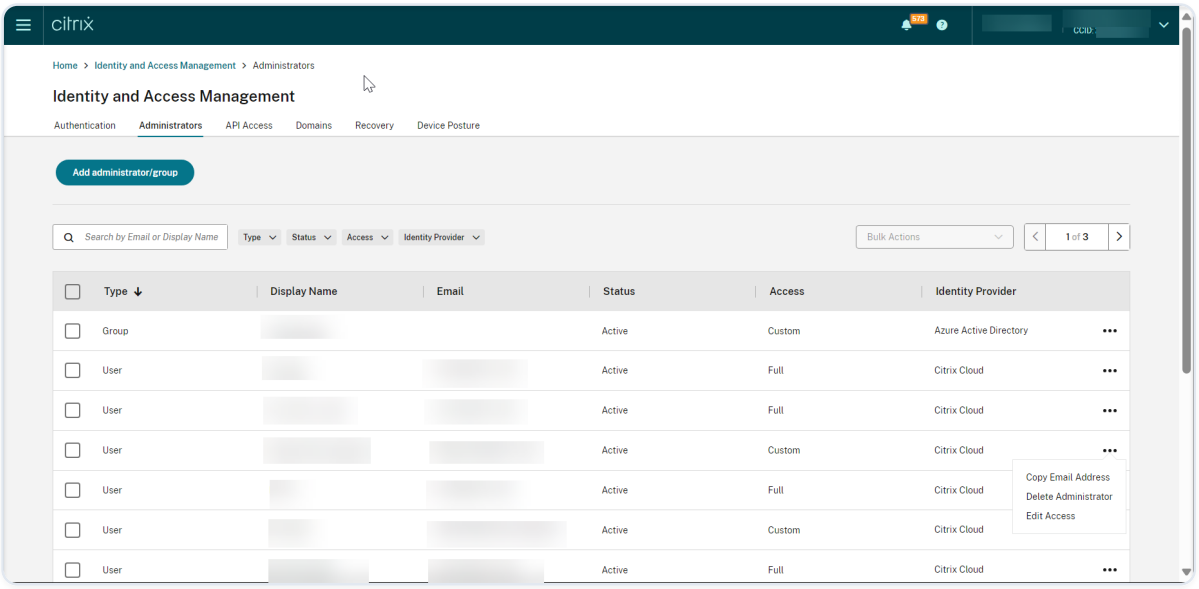
   - The **Playback Permissions** menu in the left navigation of the Session Recording service is invisible for the administrators that are added through Azure AD groups. It is also invisible for Session Recording read-only administrators.
   - All Session Recording administrators are listed on the **Playback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

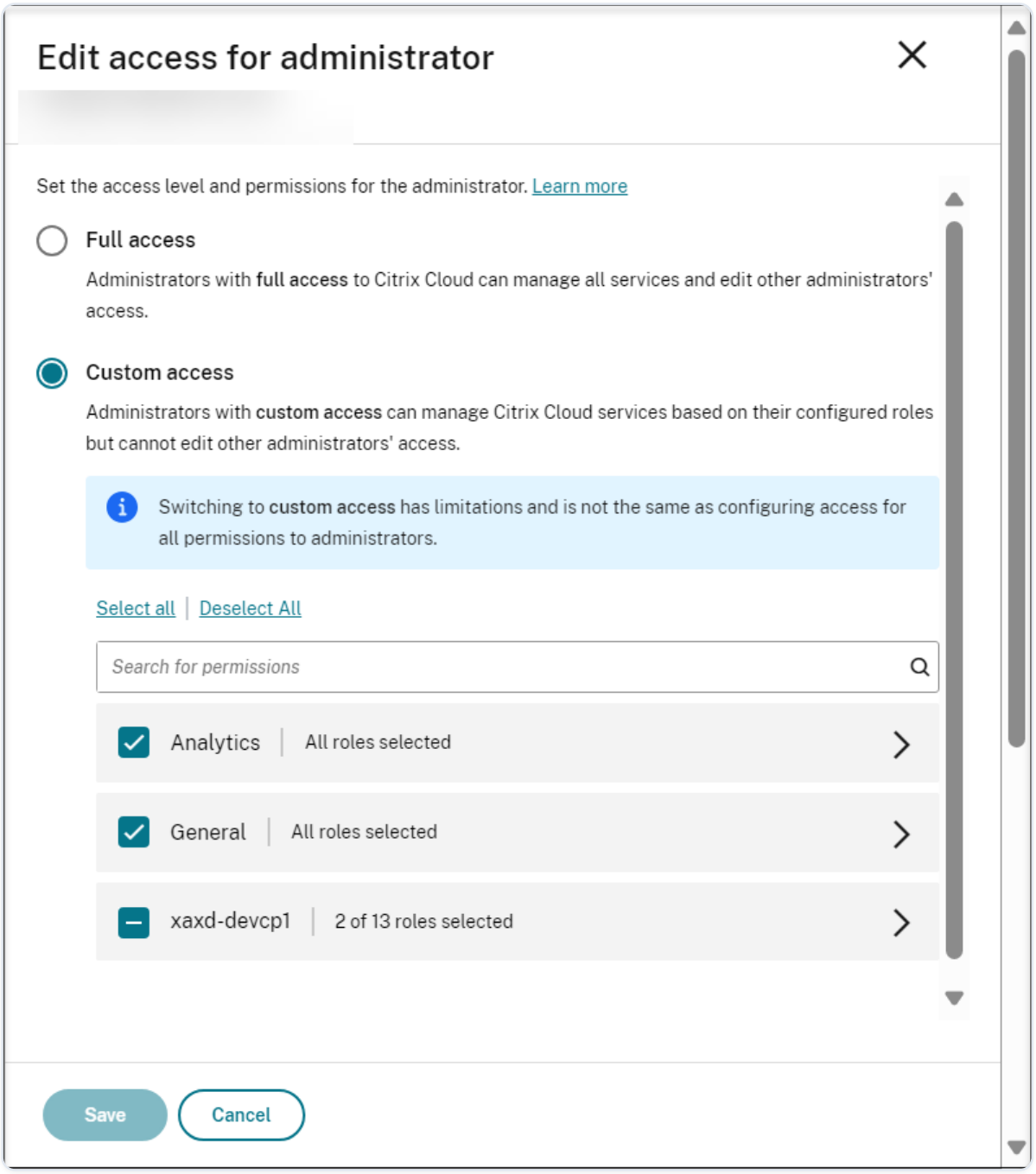
2. Select a target site.
3. Target an administrator on the **Playback Permissions** page. To make the administrator a Session Recording read-only administrator, complete the following steps:

   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**.

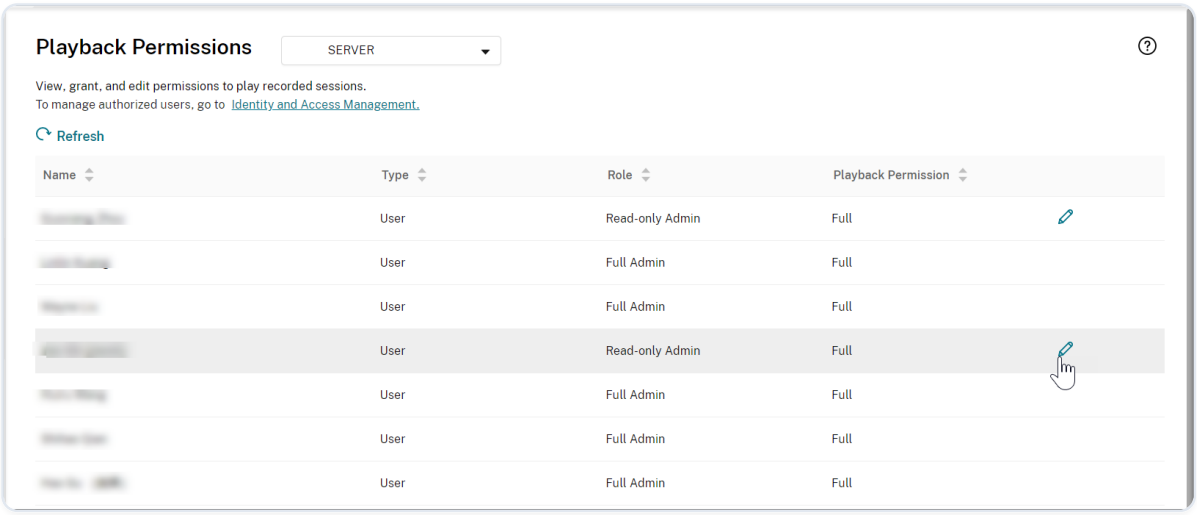


d. Click the angle bracket to expand all roles.

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

f. Click **Save**.

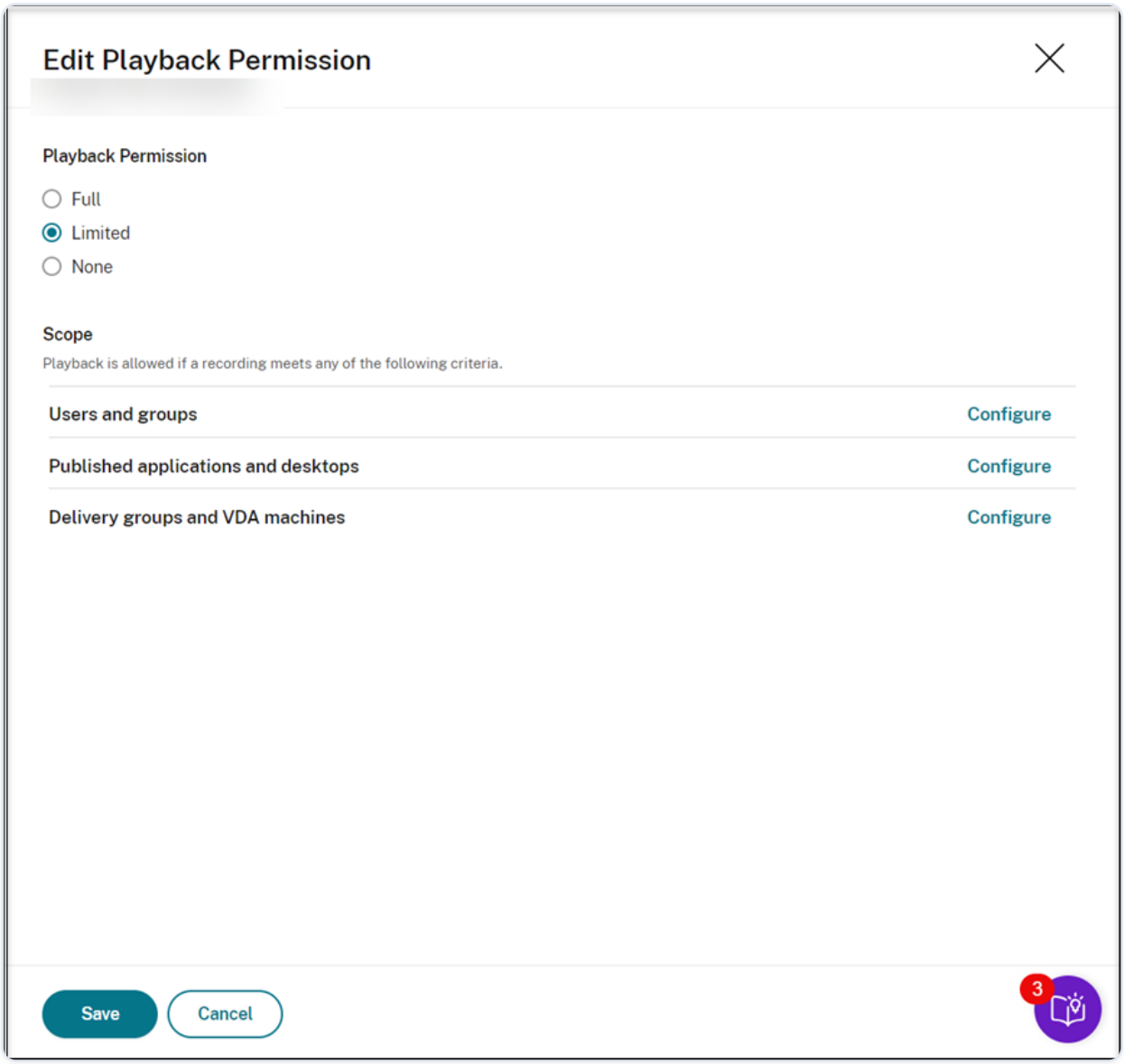
g. Return to and refresh the **Playback Permissions** page of the Session Recording service. The Citrix Cloud administrator you edited shows as a Session Recording read-only administrator.



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

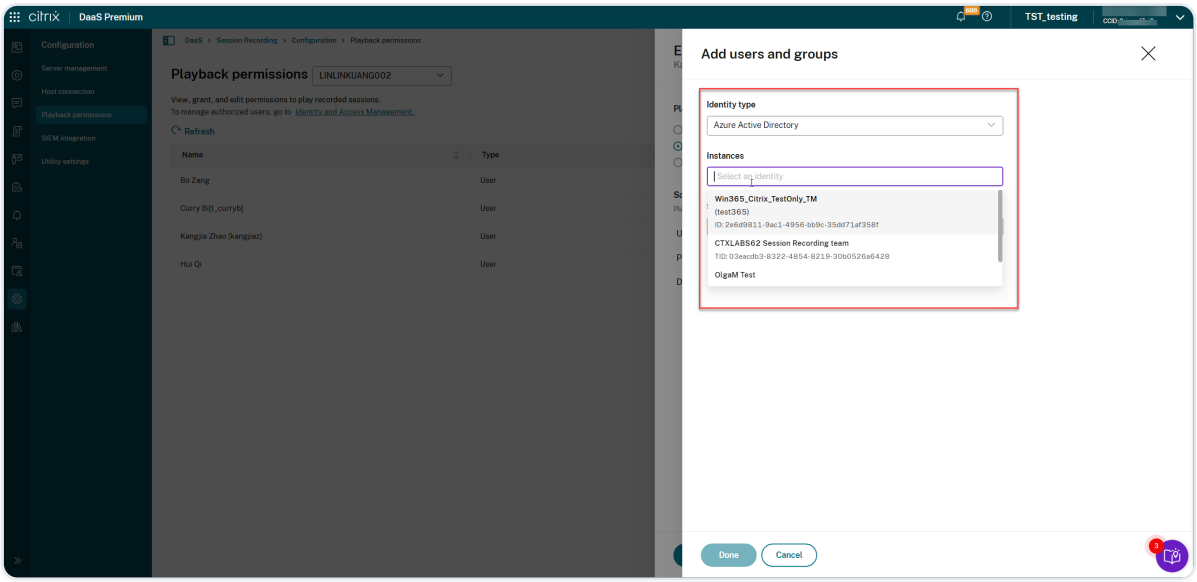
> **Tip:**
>
> A Session Recording read-only administrator can have **full** permission to play all recordings, **limited** permission to play only specific recordings, or **no** permission to play any recordings. Unless otherwise specified, a Session Recording read-only administrator has full permission 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. Selecting Azure AD as the identity provider allows you to choose an instance from the drop-down list. The available instances depend on your settings on the Citrix Cloud **Identity and Access Management > Authentication** tab.



Note:

- The Azure AD identity support for configuring playback permissions is available 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:

```
ALTER procedure [dbo].[EnumPlayerUserDeliveryGroupPoliciesOnCloud]

as
```

```
begin

set nocount on



select 3 as RoleType,

a.ID as RoleAccountID,

h.principleName as PrincipleName,

a.IsEnabled as IsEnabled,

e.name as PolicyType,

d.DeliveryGroupID as AccountMemberAccountID,

g.Name as AccountMemberName



from PlayerUserCloudAccountRoleConfigure a,

PlayerUserPolicyConfigSetMember b,

PlayerUserPolicyDeliveryGroupSetMember d,

PlayerUserPolicyType e,

DeliveryGroup g,

PlayerUserCloudAccount h

where e.id=5

and b.PlayerUserPolicyTypeID = e.ID

and a.PlayerUserPolicyConfigSetID = b.PlayerUserPolicyConfigSetID

and b.PolicySetID = d.PlayerUserPolicyDeliveryGroupSetID

and g.ID=d.DeliveryGroupID
```

```
and h.ID=a.CloudAccountID



end
```

Administrator permissions

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:



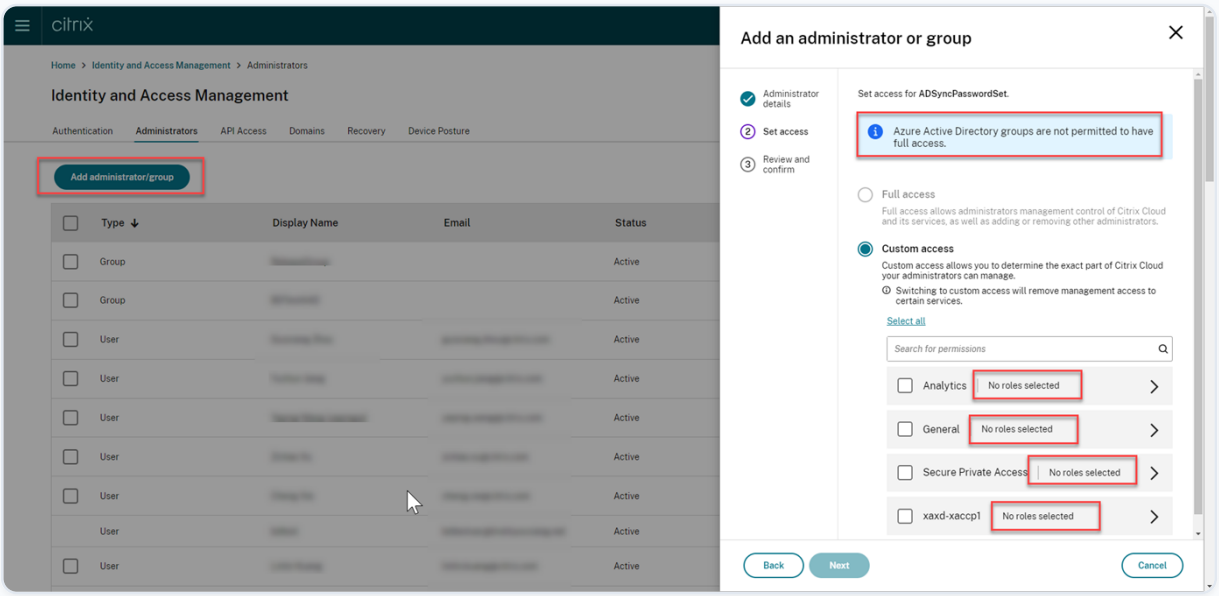
Types of Session Recording cloud administrators

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** role, or the **Session Recording-FullAdmin** role.
Privileged player admin	Refers to a Citrix Cloud administrator assigned **only** the **Session Recording-PrivilegedPlayerAdmin** role, or assigned the **Session Recording-PrivilegedPlayerAdmin** and the **Session Recording-ReadOnlyAdmin** roles.
Read-only admin	Refers to a Citrix Cloud administrator assigned **only** the **Session Recording-ReadOnlyAdmin** 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.

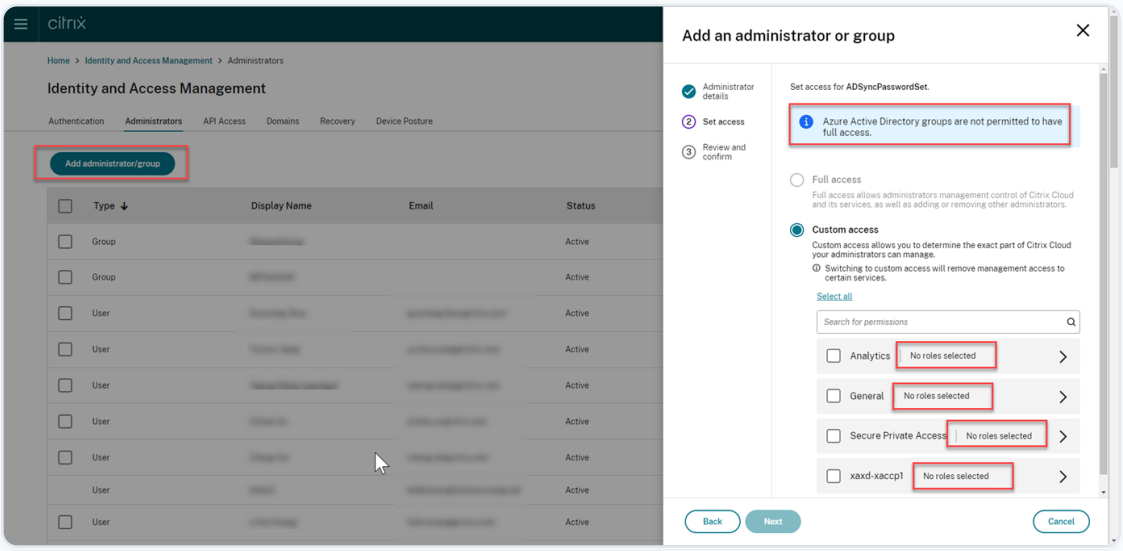
   Citrix Cloud supports adding administrators either individually or as Azure AD groups.

   - 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:

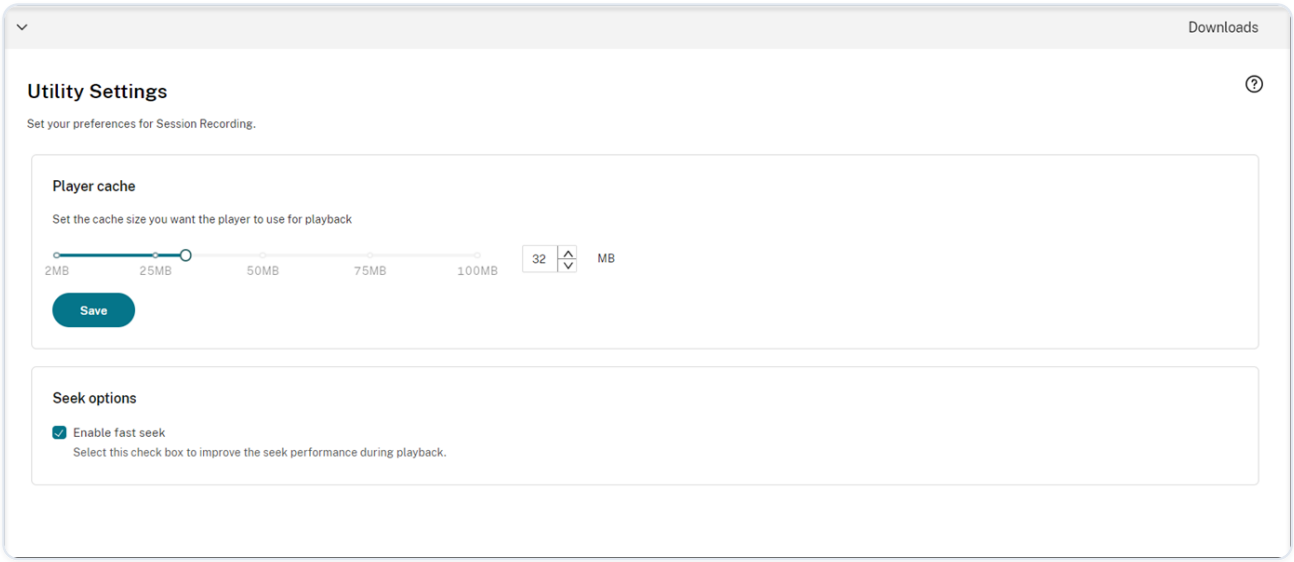
	FULL ADMIN	PRIVILEGED PLAYER ADMIN	READ-ONLY ADMIN
Access the **Dashboard** page	Enabled	Disabled	Disabled
Configure server settings	Enabled	Disabled	Disabled

SESSION RECORDING SERVICE			
	FULL ADMIN	PRIVILEGED PLAYER ADMIN	READ-ONLY ADMIN
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

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

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.

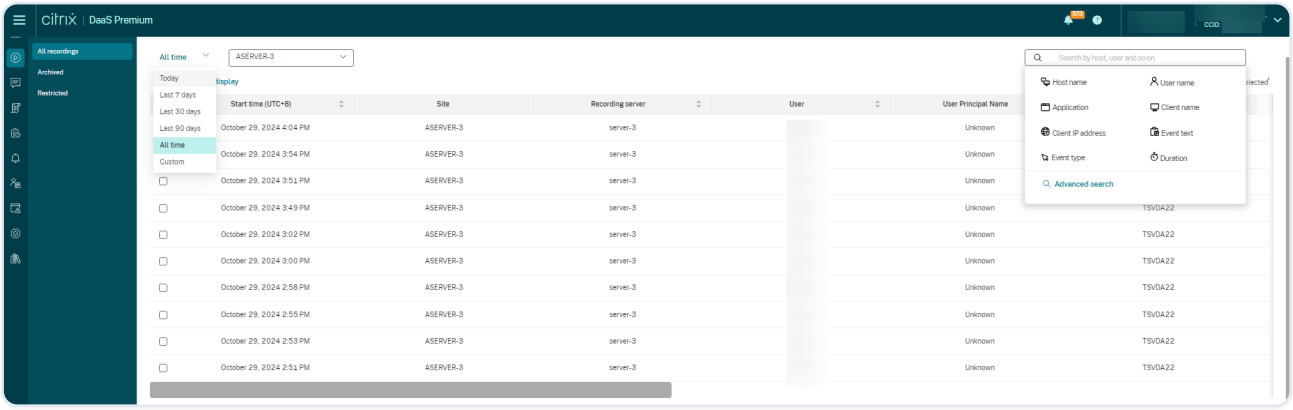
> **Note:**
>
> Grant users the right to access the recorded sessions of VDAs.

Search for recordings

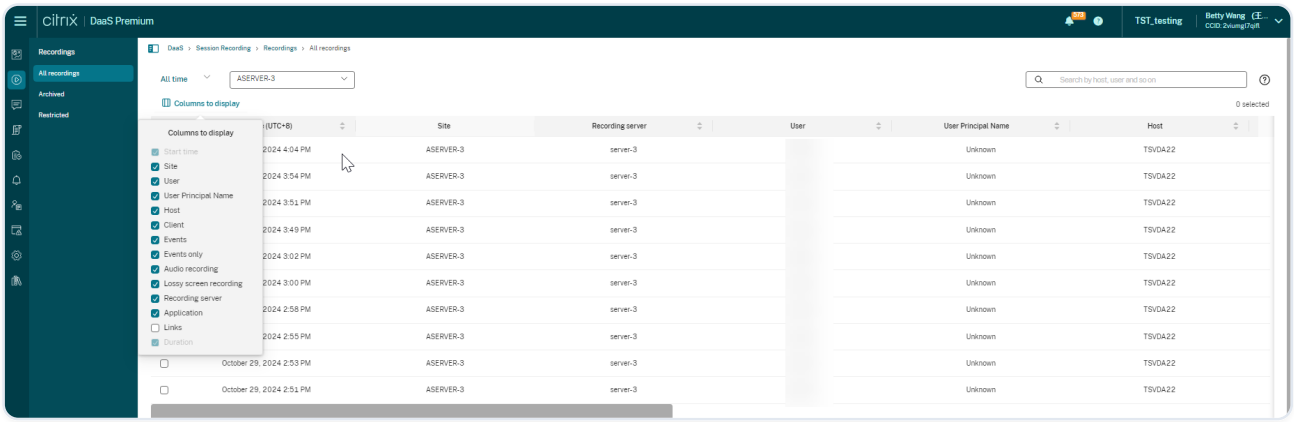
Search for recordings

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.

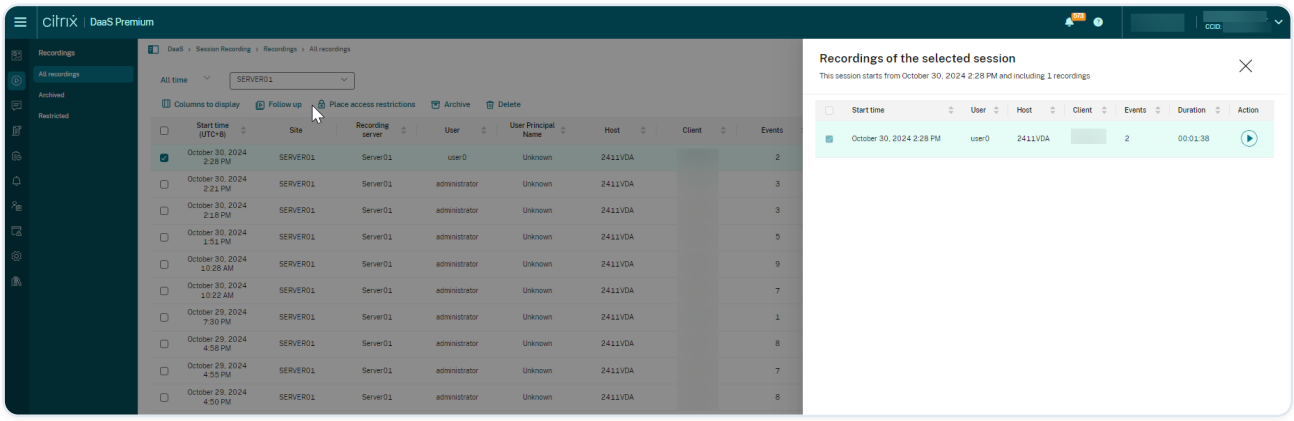


You can also specify **Columns to display**.



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

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** role
- **Session Recording-FullAdmin** role
- **Session Recording-PrivilegedPlayerAdmin** role
- **Session Recording-ReadOnlyAdmin** role

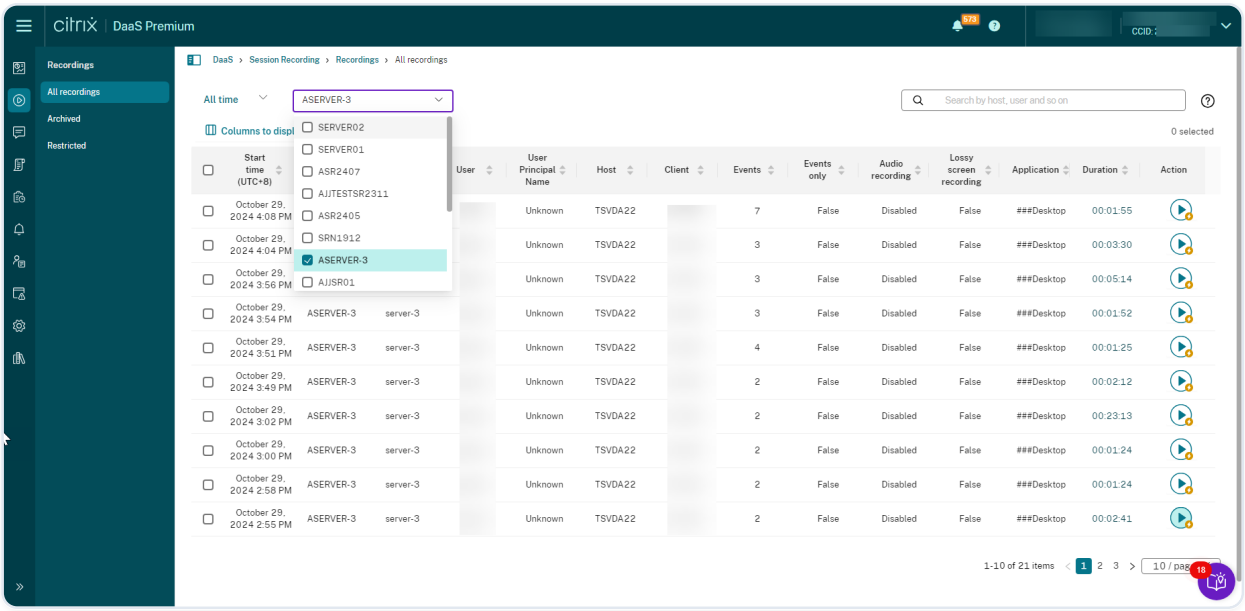
Restricted recordings are not accessible to Session Recording read-only administrators, that is, Citrix Cloud administrators assigned **only** the **Session Recording-ReadOnlyAdmin** role. Session Recording read-only administrators do not have permission to access the **Restricted** page or remove access 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.

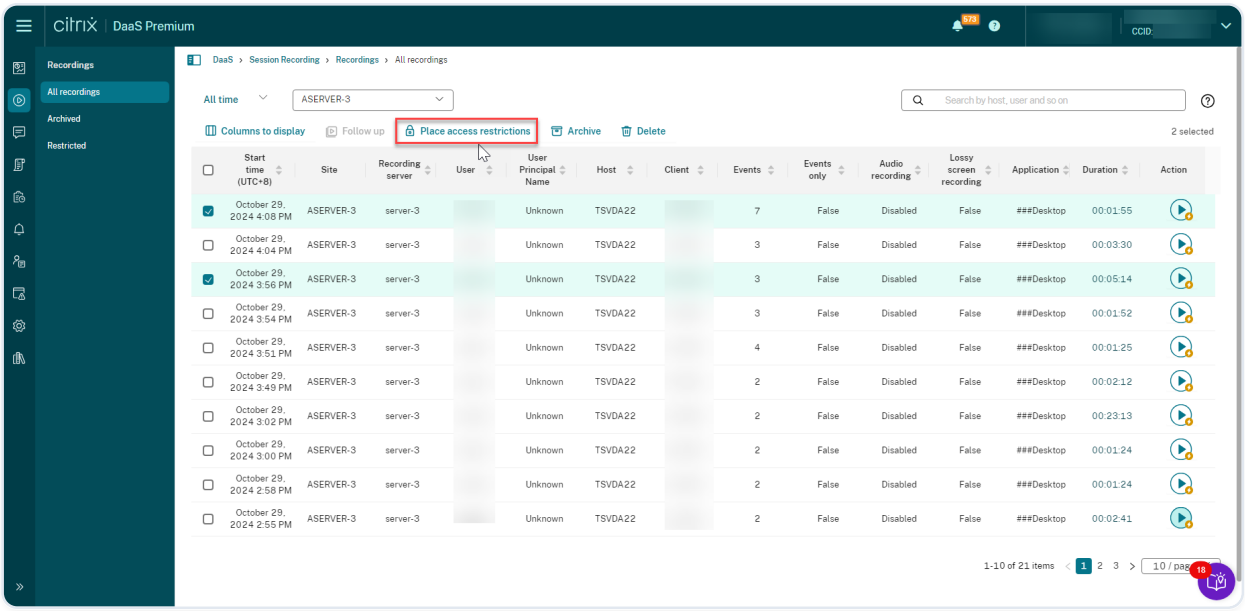


3. On the **All Recordings** page, select one or more target recordings.

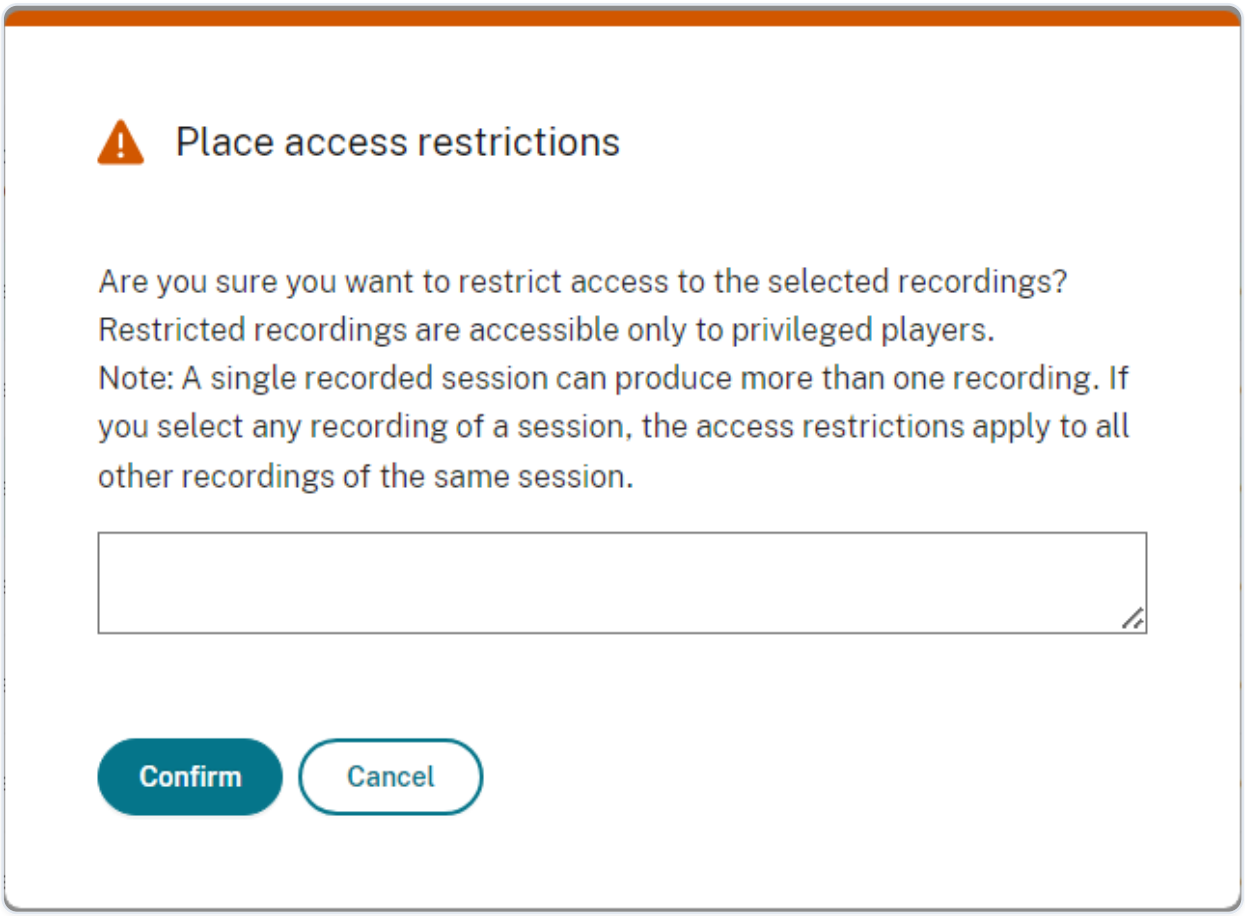
Note:

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

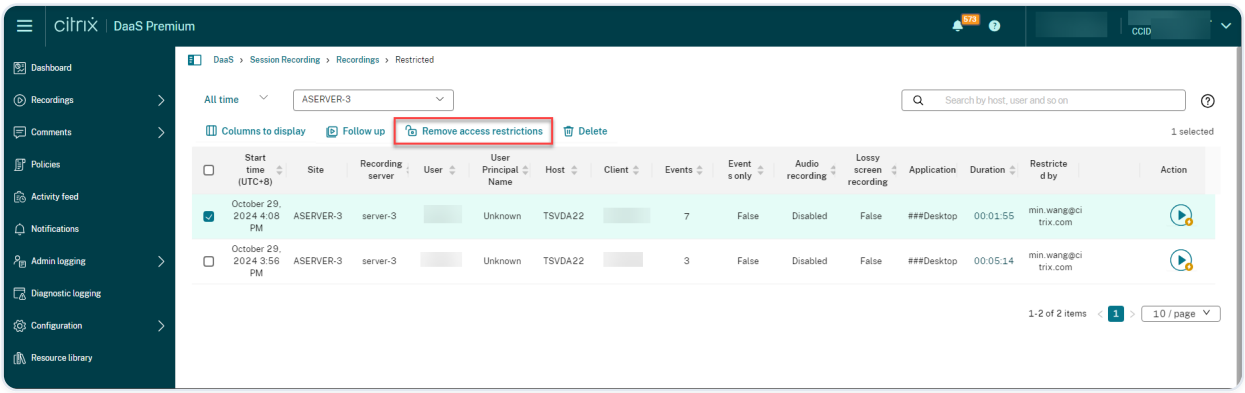
4. Click **Place access restrictions**.



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



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.



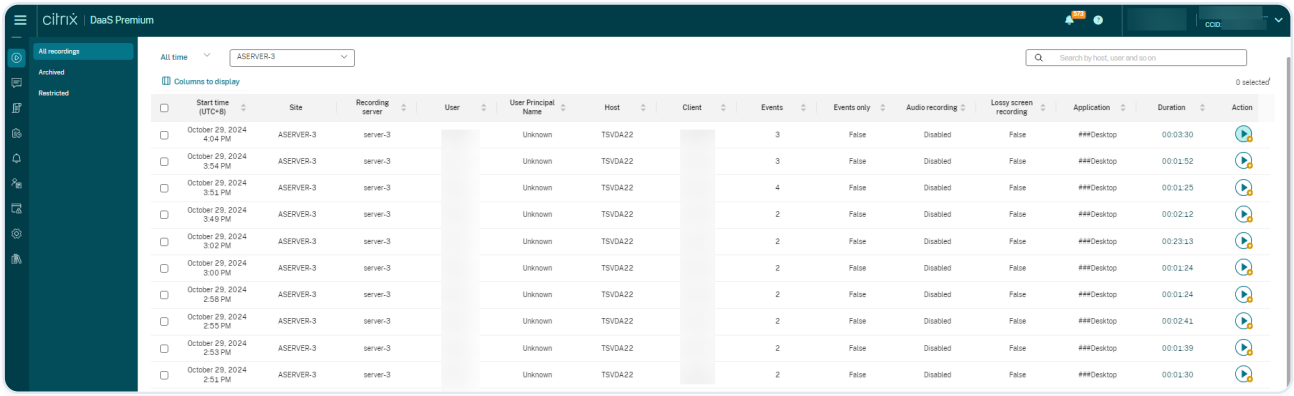
Open and play recordings

Open and play recordings

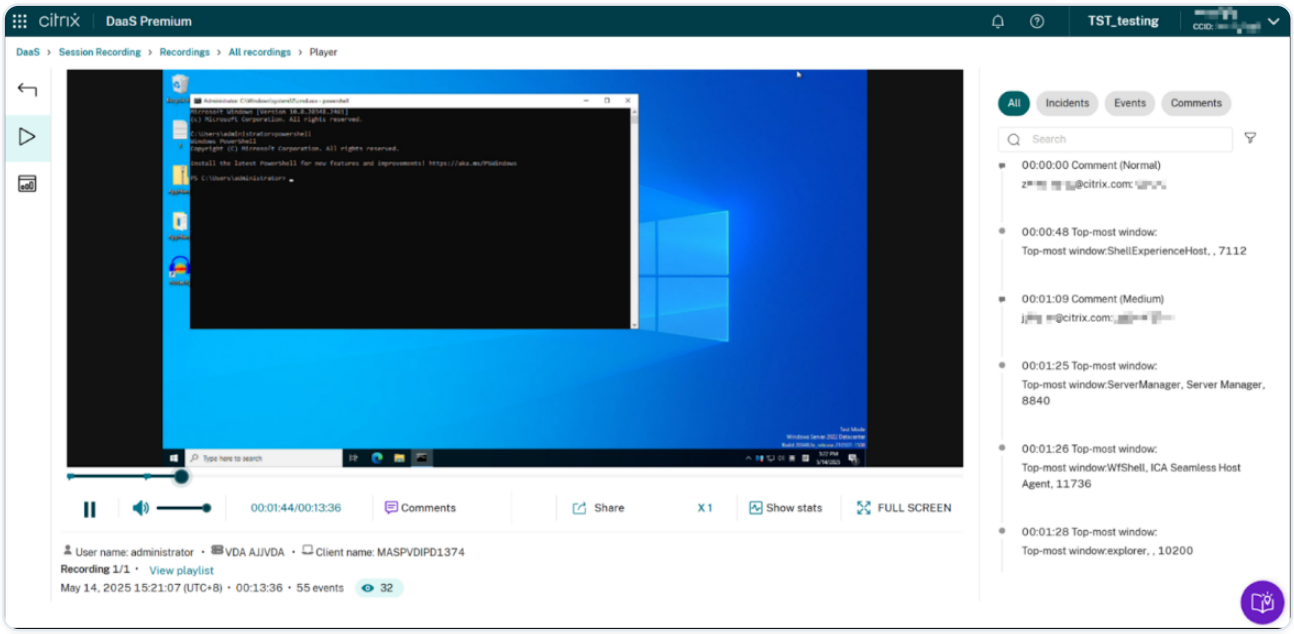
Tip:

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

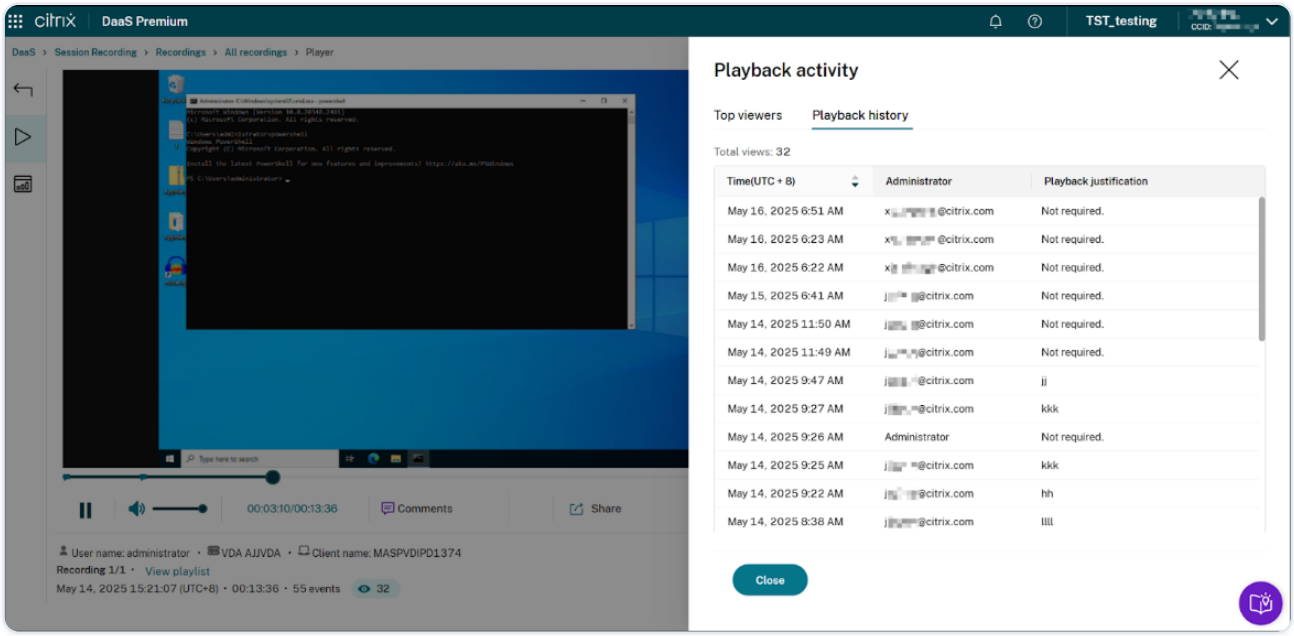
You can play live and completed recordings. Click the play button. Playback starts after memory caching.



The playback page provides comprehensive controls and information. For an example, see the following screen capture. Notice at the bottom of the player, next to the recording date and time, a count indicates how many times the recording has been played.



Clicking this playback count opens the Playback activity panel. This panel has two tabs: Top viewers, which displays a list of users who have played this recording most frequently, and Playback history, which shows a detailed log of each time the recording was played, including the viewer, timestamp, and any justification provided (if applicable).



Tip:

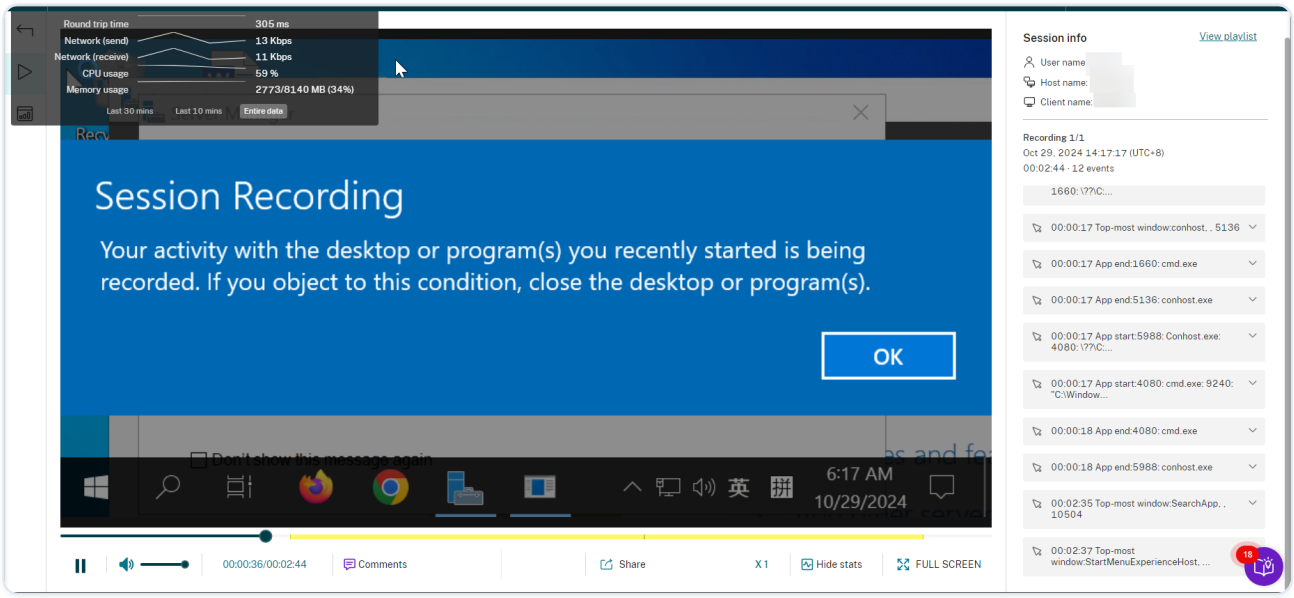
- Clicking the session progress time lets you switch to the absolute date and time the session was recorded.
- For an event-only recording, the play icon in the upper left corner is unavailable.

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.
Magnify	Zoom in on the current playback area.

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, **Oct 29, 2024** and **14:17:17**.
- The duration of the recording in playback. In this example, **00:02:44**.
- The number of events in the recording. In this example, **12 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.
- 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

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.

> **Note:**

- Sharing recordings as restricted links requires Session Recording 2203 or later.
- Sharing recordings as unrestricted links requires Session Recording 2305 or later.

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** role
- **Session Recording-FullAdmin** role

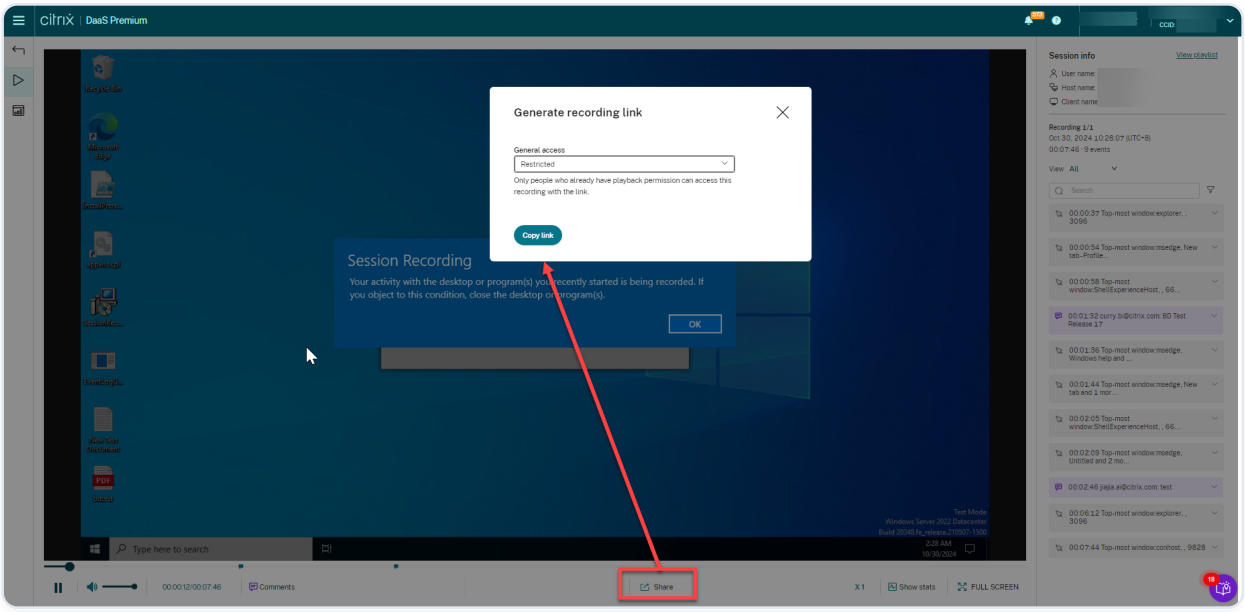
Note:

- 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 list.
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**

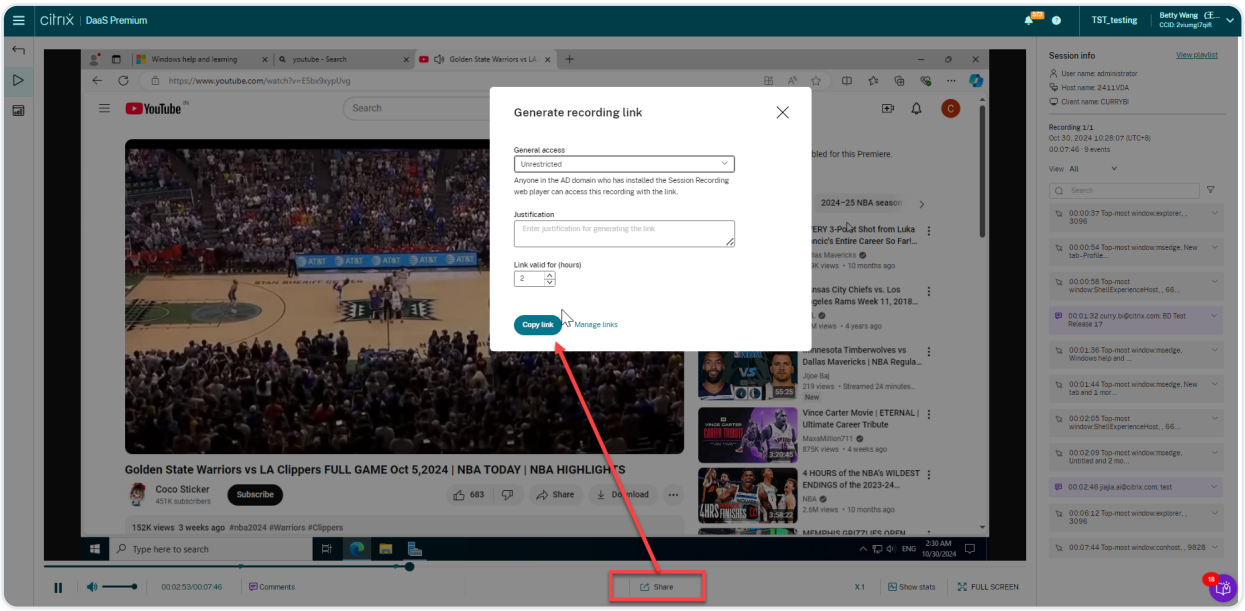
5. Share the generated URL link with users who already have playback permission.

   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 list.



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.

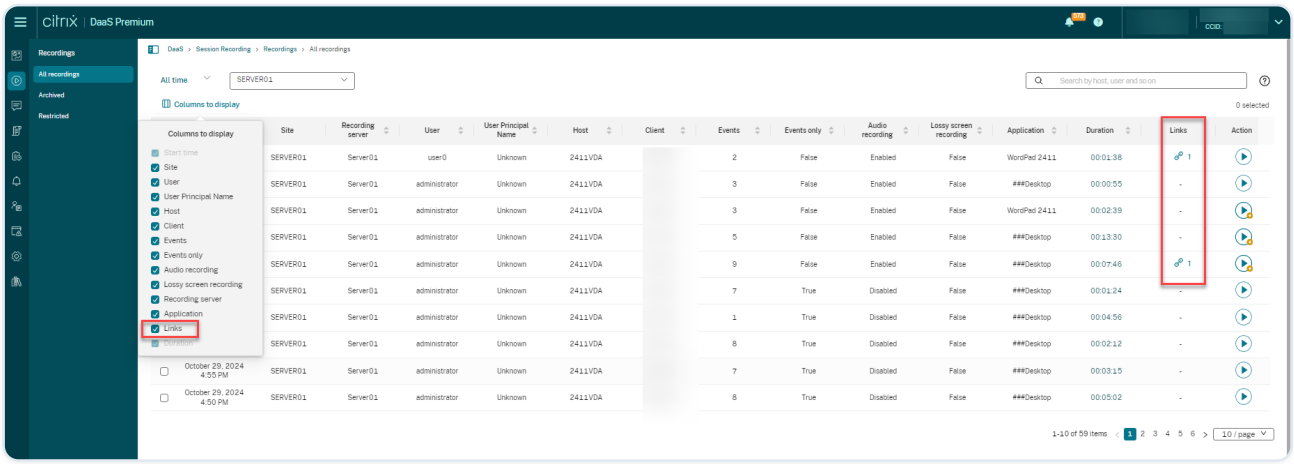
   Pasting the link in the address bar lets you jump to the location where the URL link was copied.

> **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.

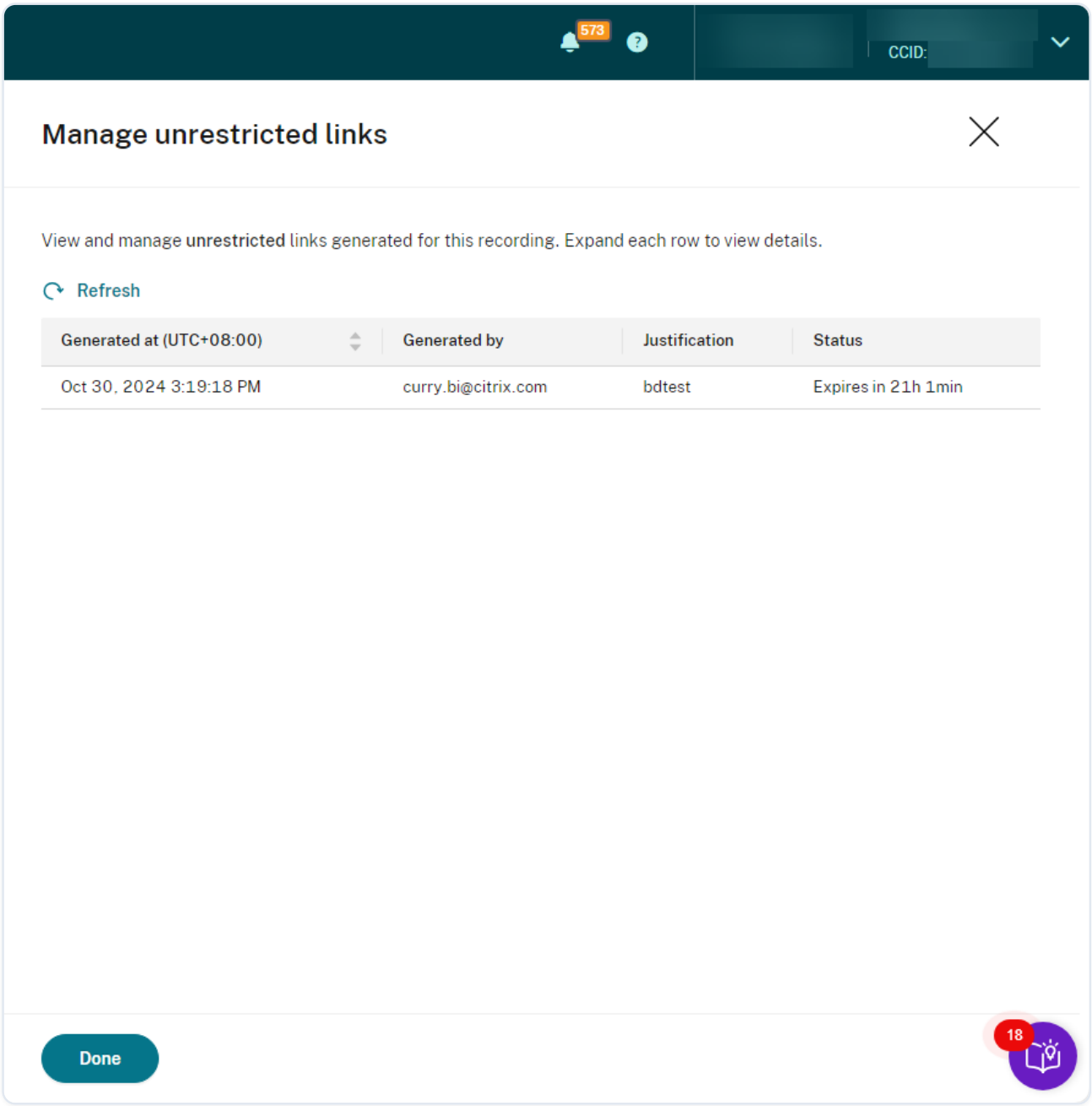
Manage unrestricted links

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**.



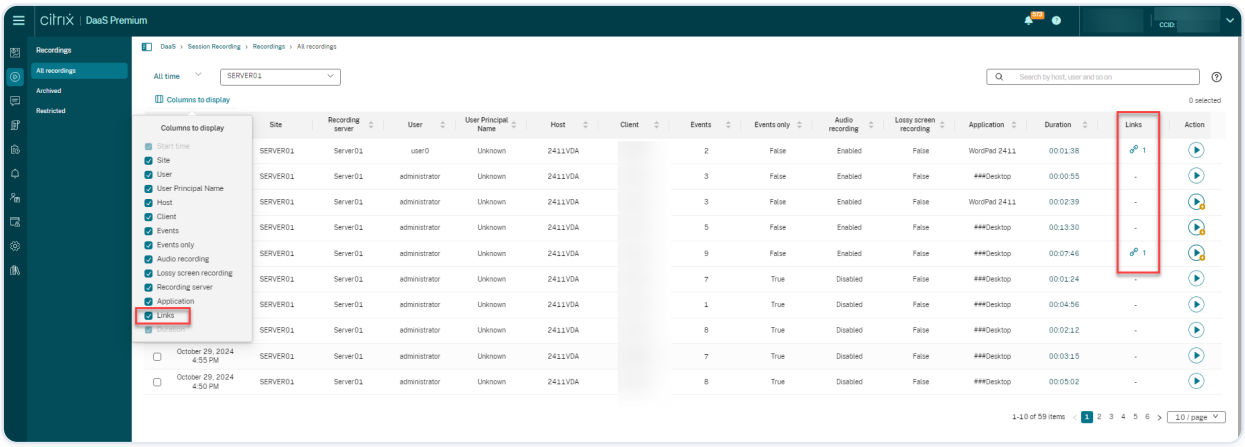
After you click the link icon corresponding to a recording, the details about unrestricted links generated for the current recording appear, for example:



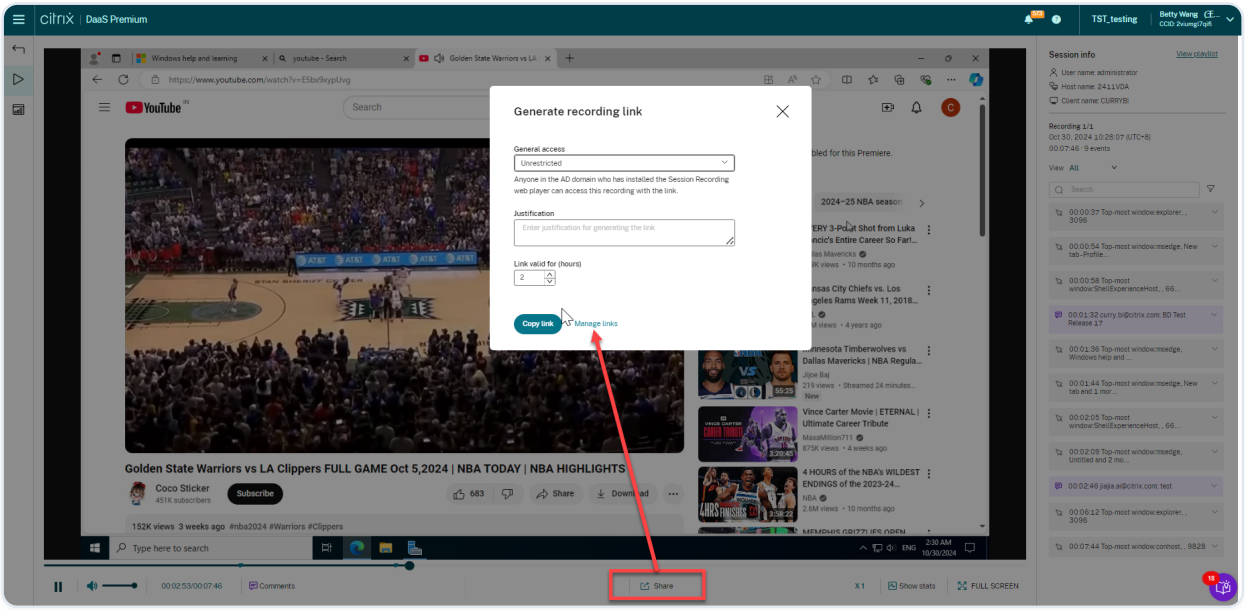
View and manage unrestricted links of a specific recording

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

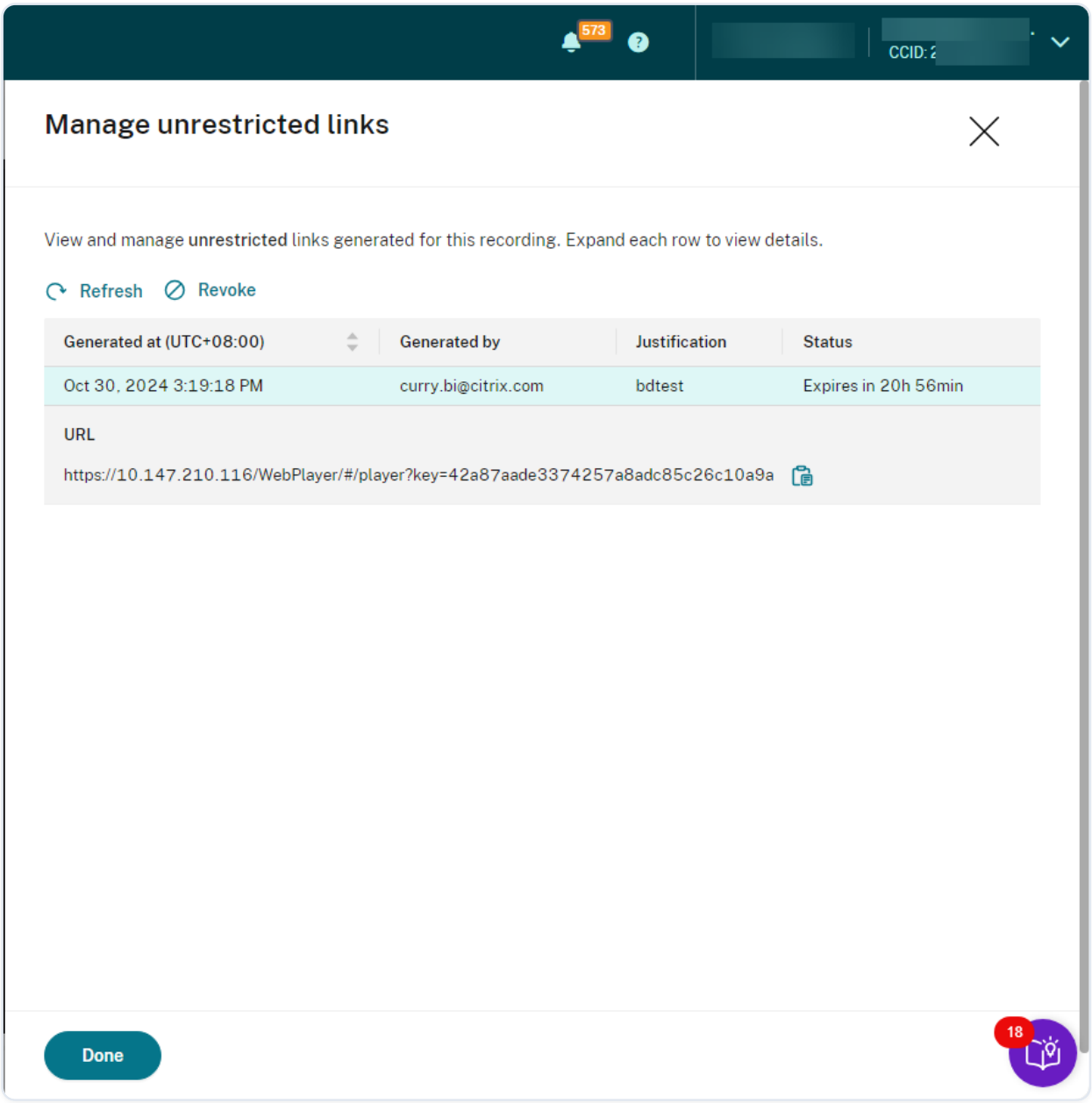
   Method 1: On the **All Recordings** page, click the link icon in the **Links** column next to a specific recording.



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

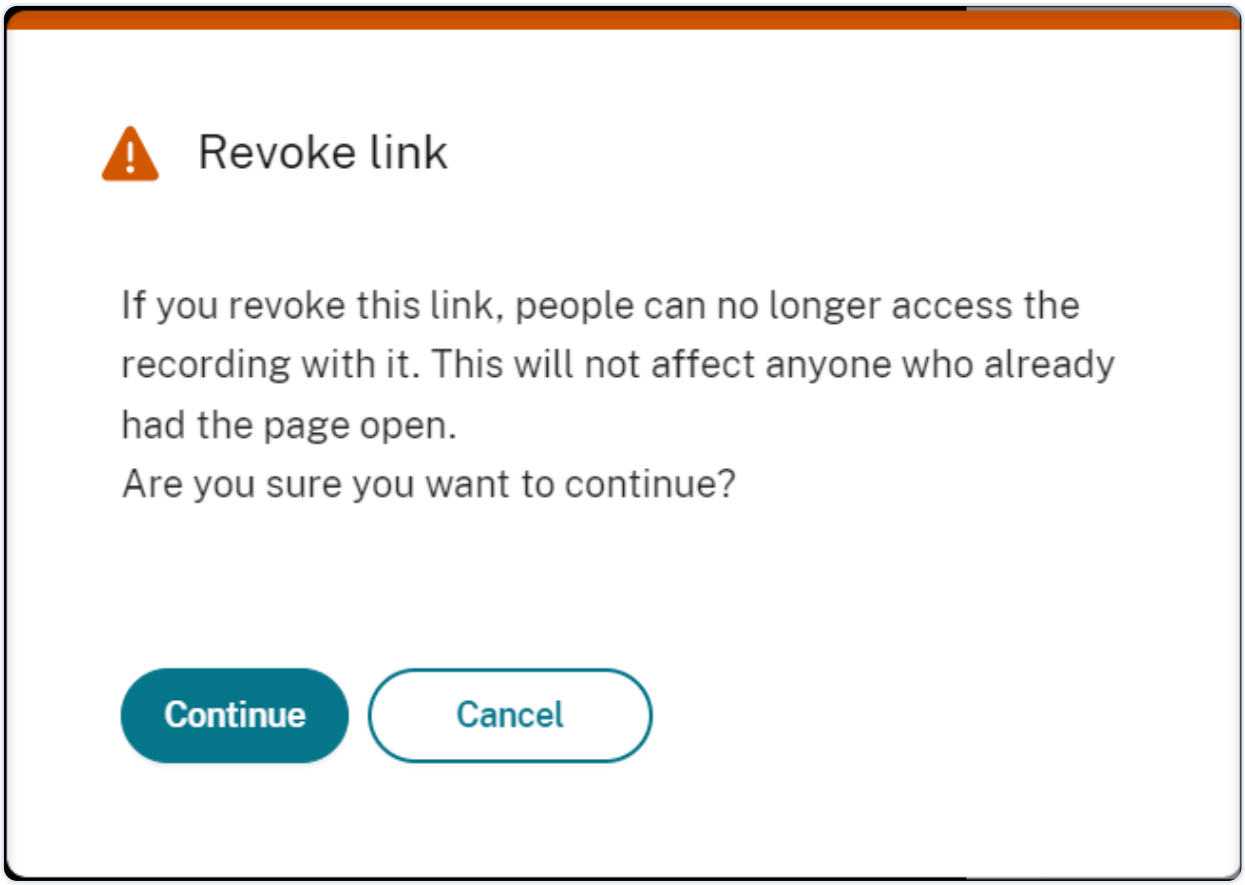


2. On the **Manage unrestricted links** page, expand each row to view details about the unrestricted links that are generated for the specific recording.



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

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.

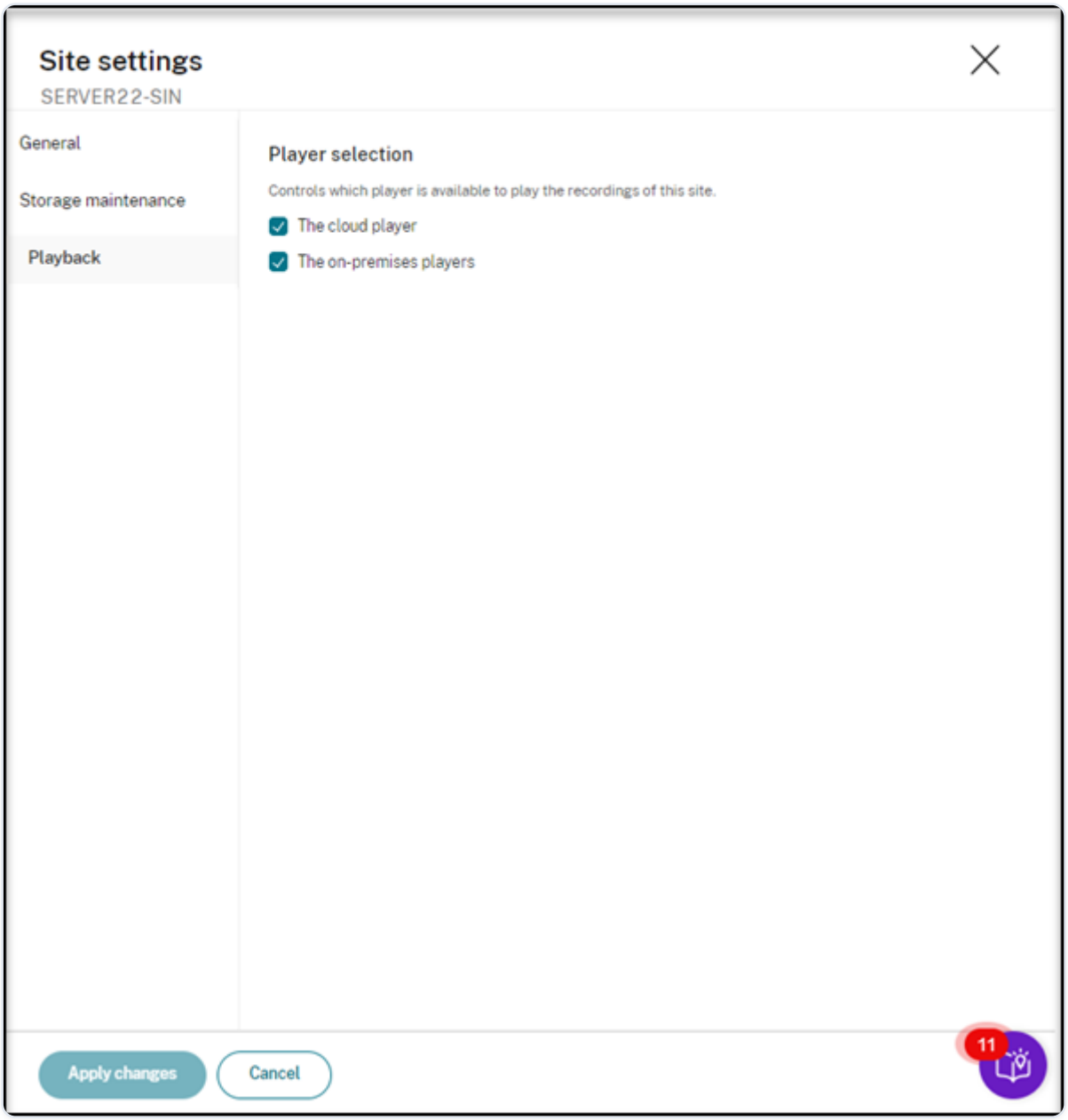
Configuration

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.



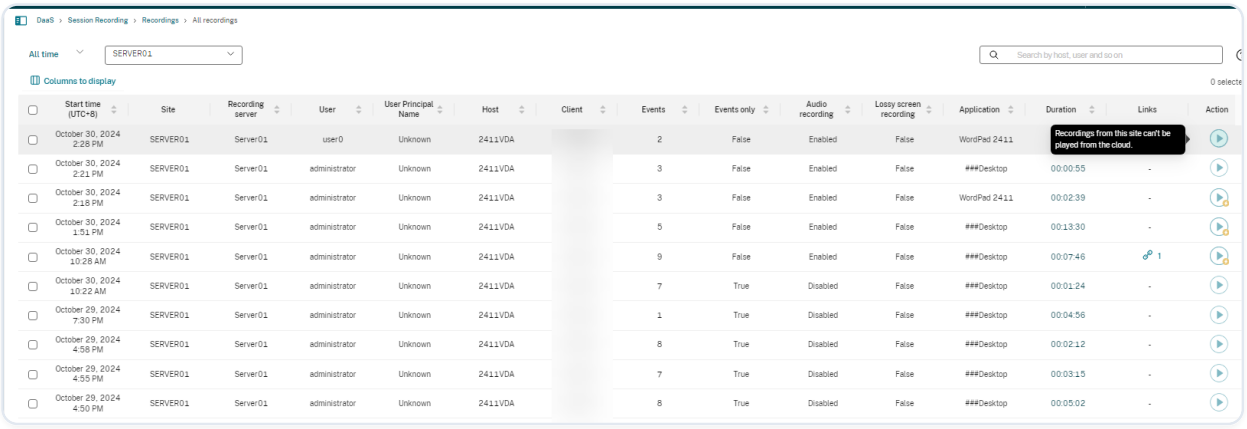
3. On the **Site settings** page, select the **Playback** menu. The player selection page appears. By default, both options are selected.



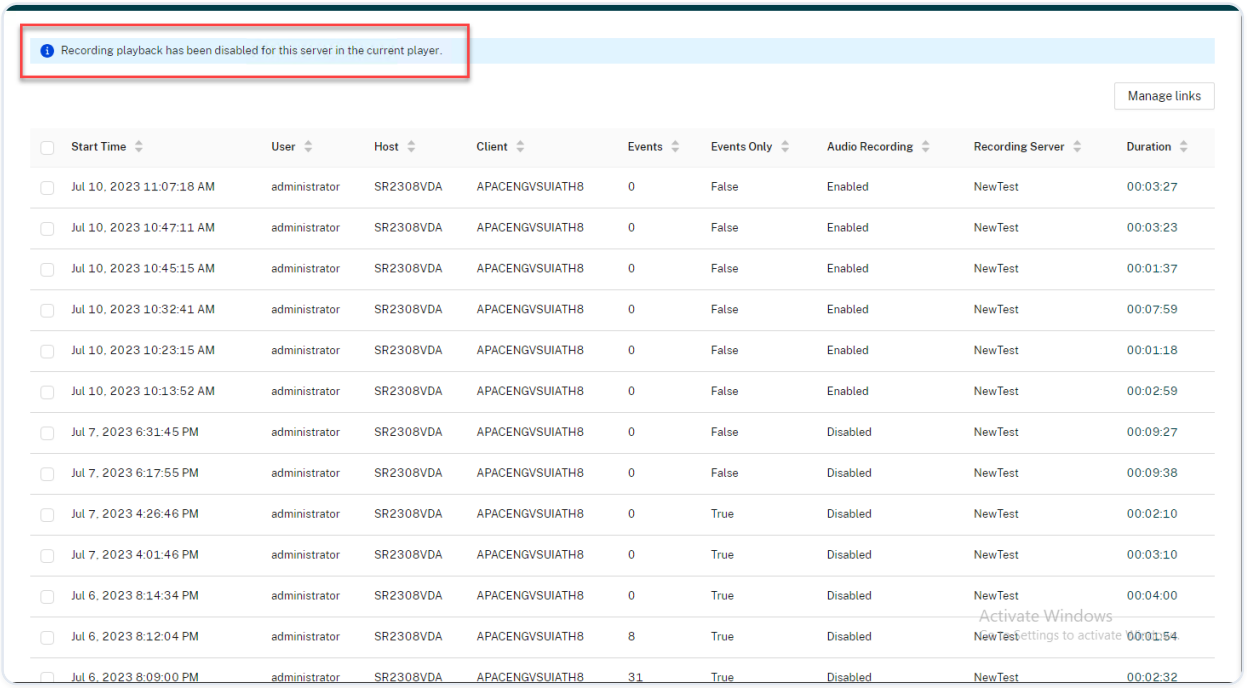
4. Select at least one option as needed and then click **Apply changes**.

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.



- If the on-premises players are disabled for recording playback of a site, you are prompted when selecting recordings from 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:



  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

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

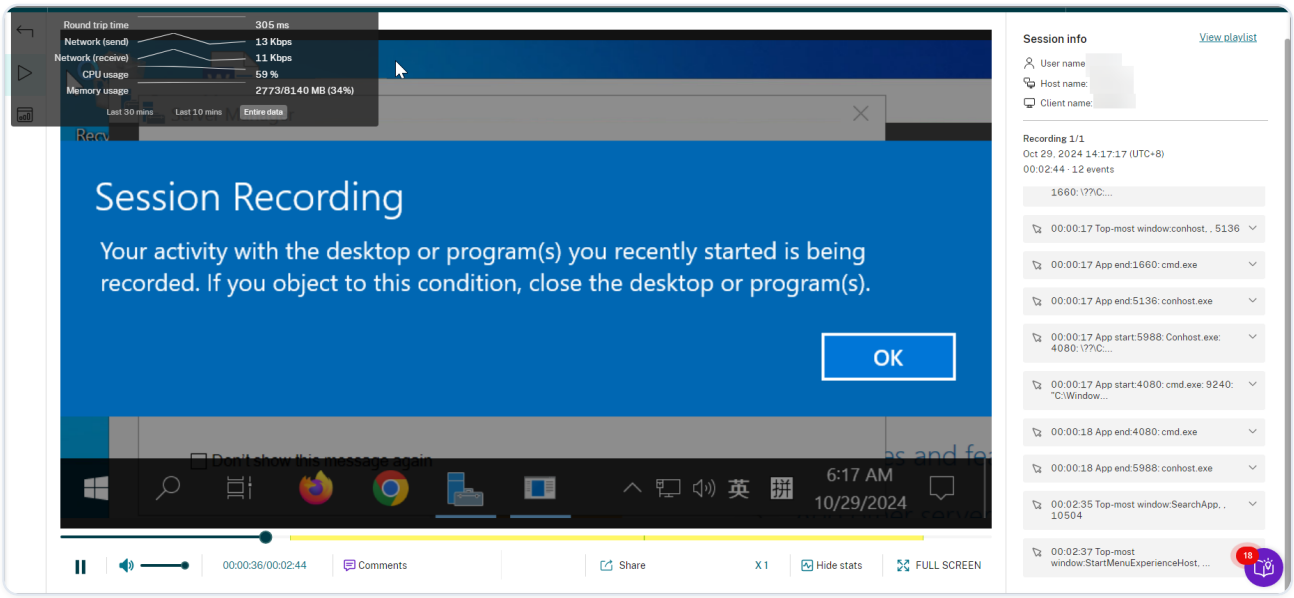
To customize the idle event feature, set the following registry keys at `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SessionEvents`.

SESSION RECORDING SERVICE

REGISTRY KEY	DEFAULT VALUE	DESCRIPTION
DisableIdleEvent	0	To disable the idle event feature, set the value to **1**. To enable the idle event feature, set the value to **0**.
IdleEventThrottle	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.
IdleEventActiveThrottle	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.
IdleEventActivePktNumThrottle	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.
IdleEventActivePktSizeThrottle	300 bytes	Graphics packets smaller than the key value are ignored and the relevant time duration is regarded as idle.

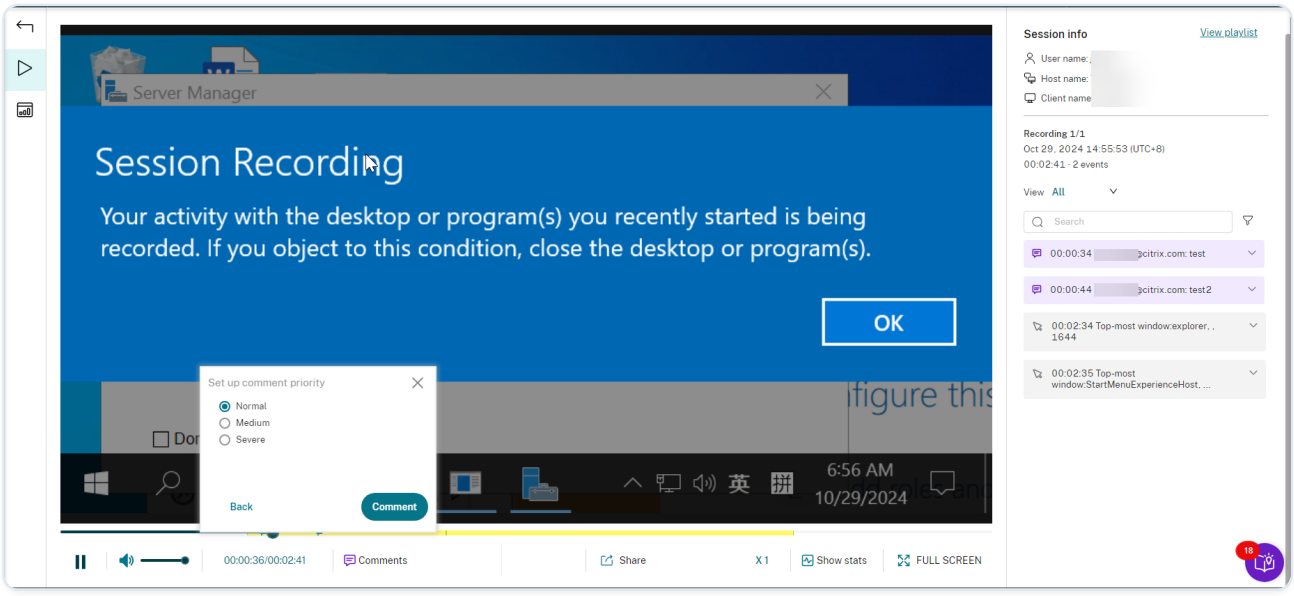
Use events and comments

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.

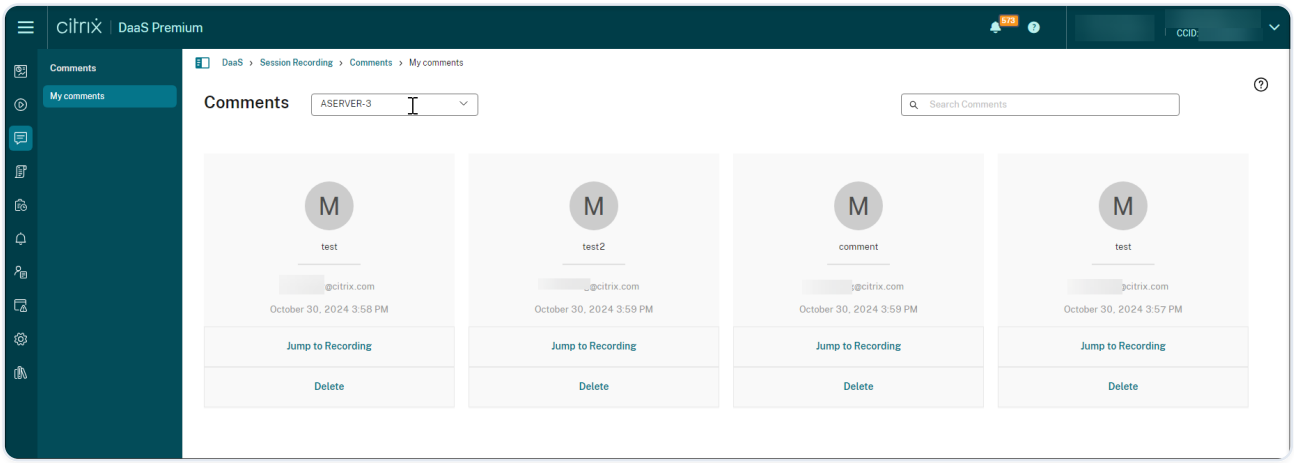


Comment on recordings

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.

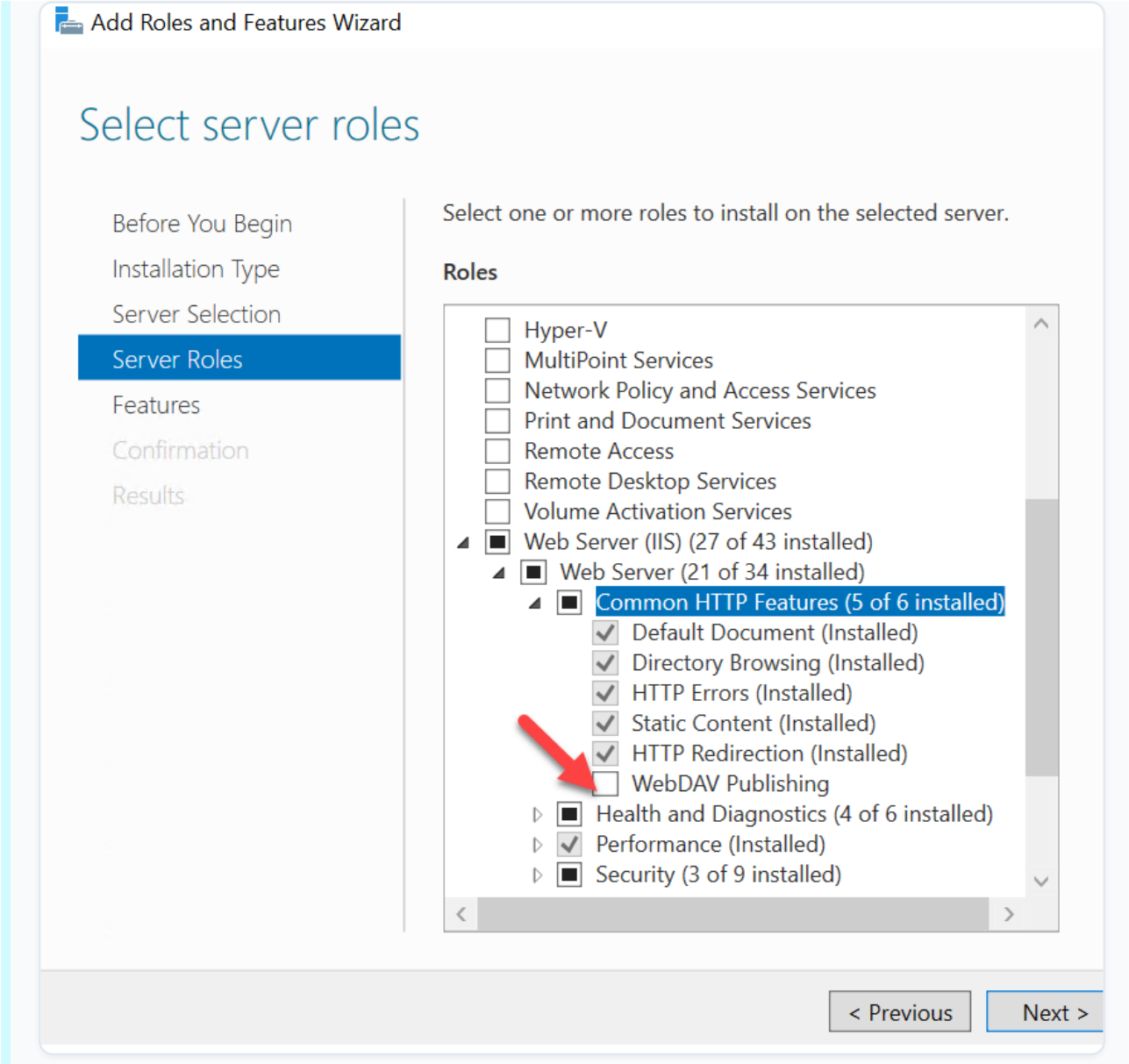


Clicking a comment lets you jump to the location where the comment was given. You can view all your comments on the **My comments** page.



Note:

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

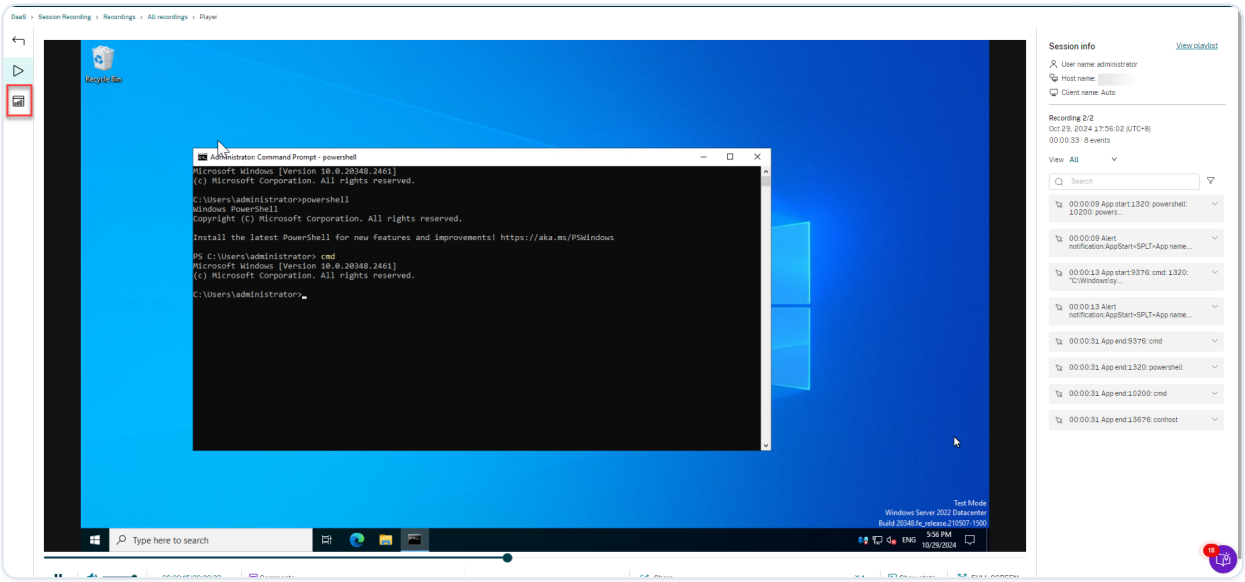


View graphical event statistics

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:

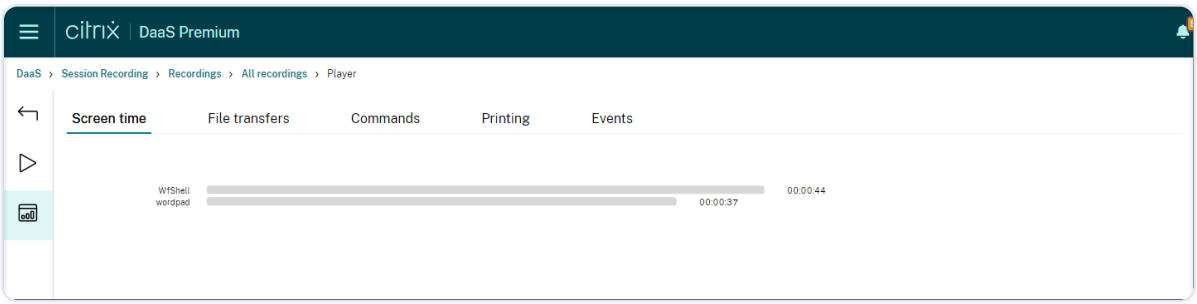
1. Open and play a recording.
2. In the upper left corner of the playback page, click the statistics icon.



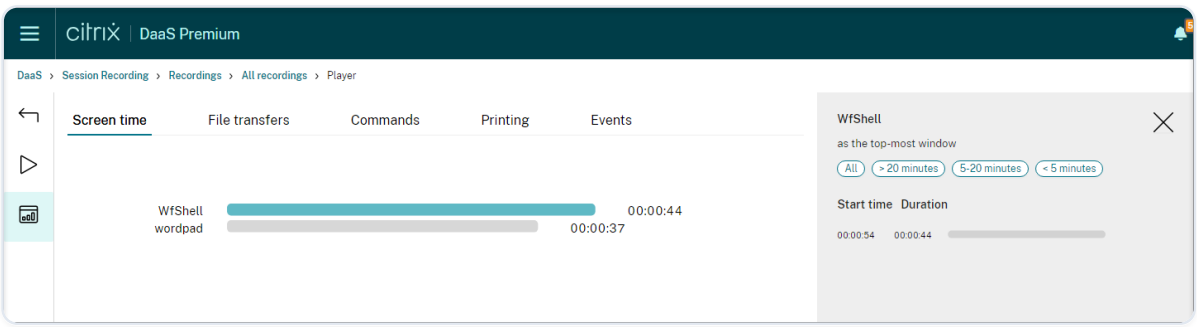
3. Switch between the **Screen time**, **File transfers**, **Commands**, **Printing**, and **Events** tabs to view statistics from different perspectives.

   - **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:

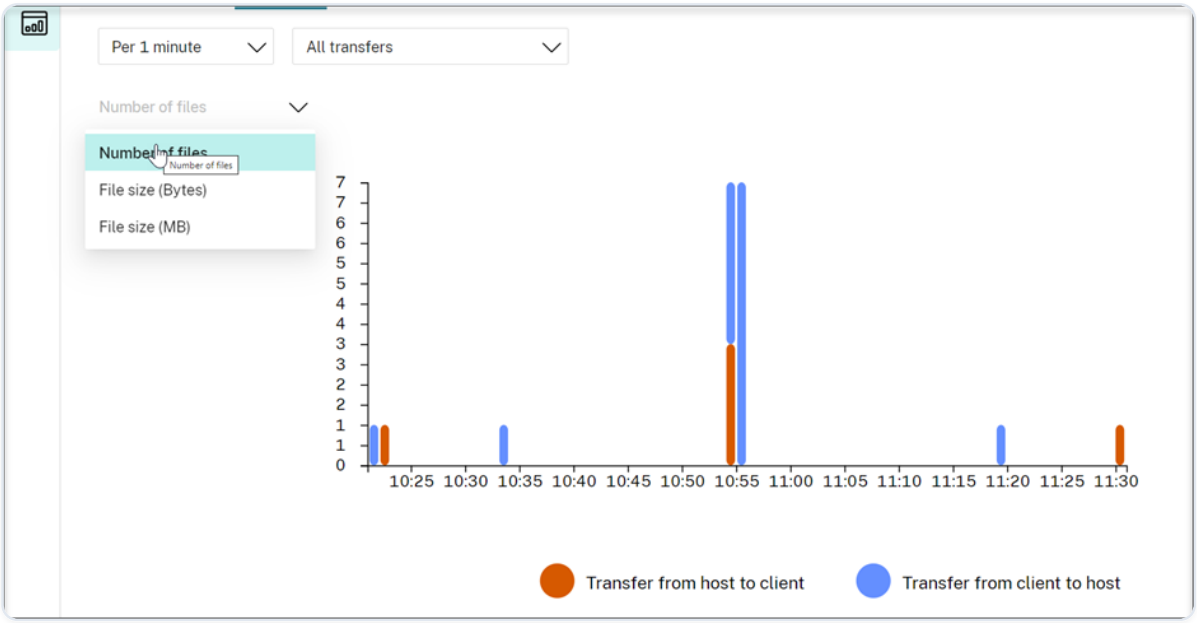


   - **File transfers**

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:

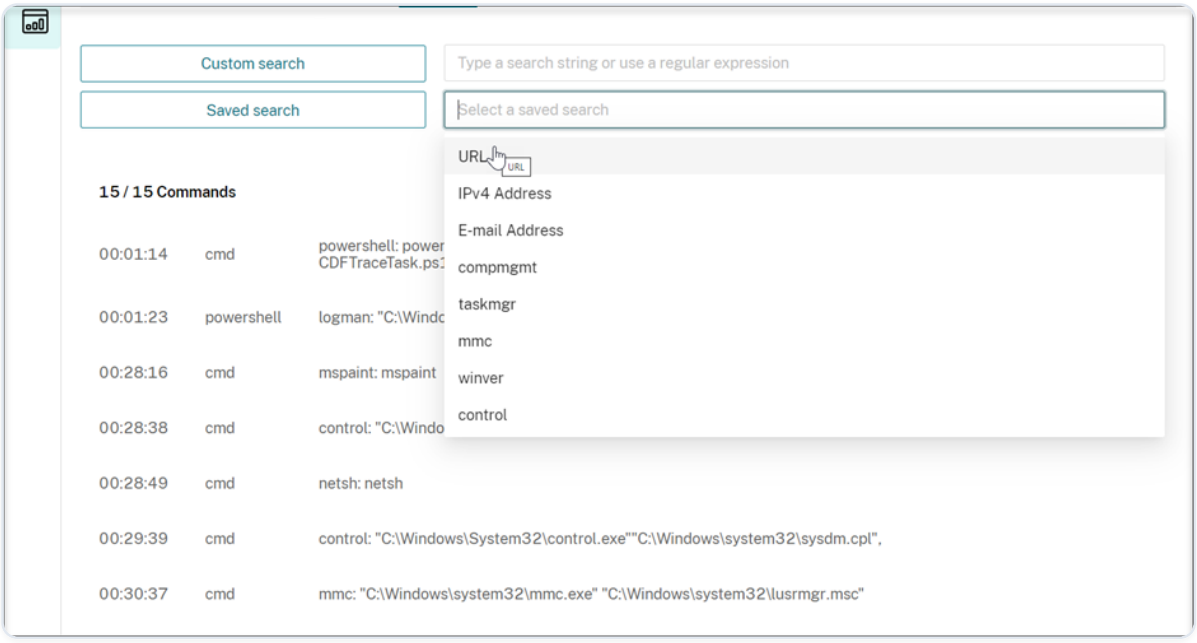
- Time granularity: **Per 1 minute**, **Per 10 minutes**, **Per hour**
- File transfer destination: **All transfers**, **Transfer from host to client**, **Transfer from client to host**
- Number or size (Bytes or MB) of transferred files

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



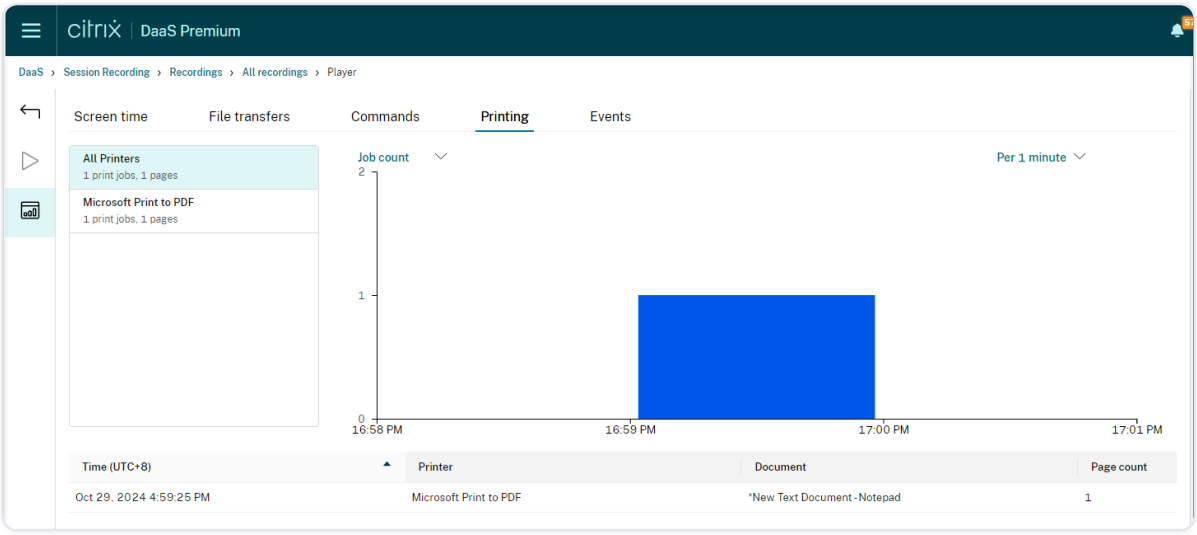
- **Commands**

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.



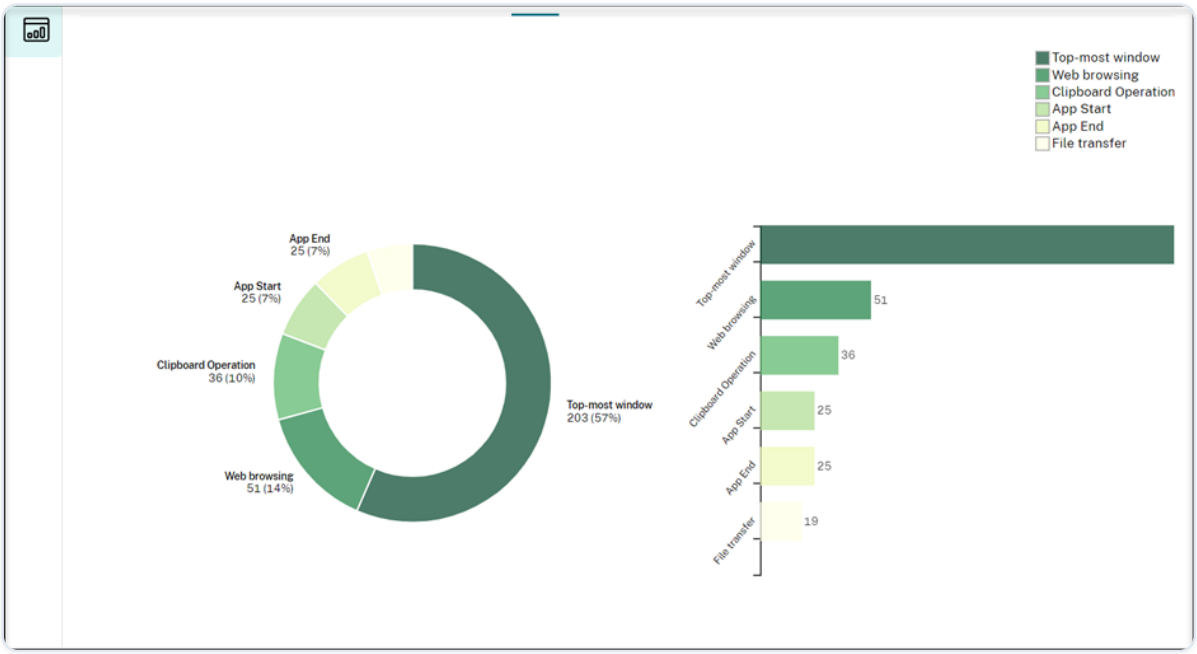
- **Printing**

  The **Printing** tab provides graphical statistics of printing activities in the recorded session.



- **Events**

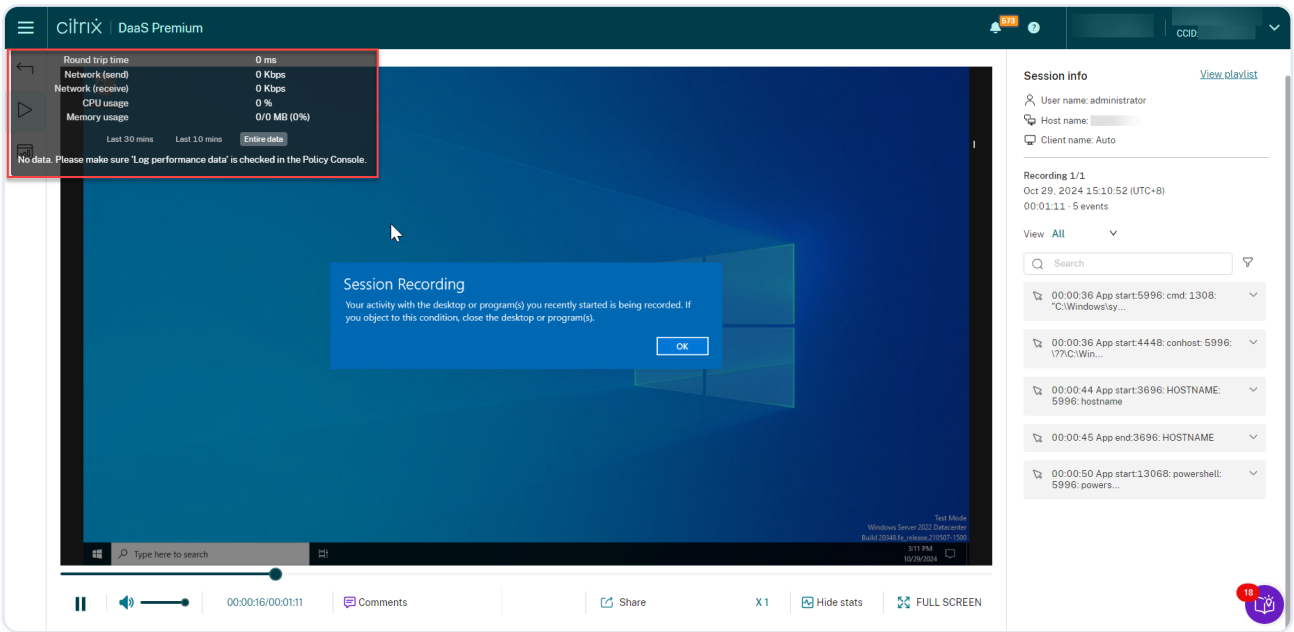
  The **Events** tab shows the proportions and numbers of all types of events in the recorded session.



View performance data points

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

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
- Session recording media task service
- Session recording file export

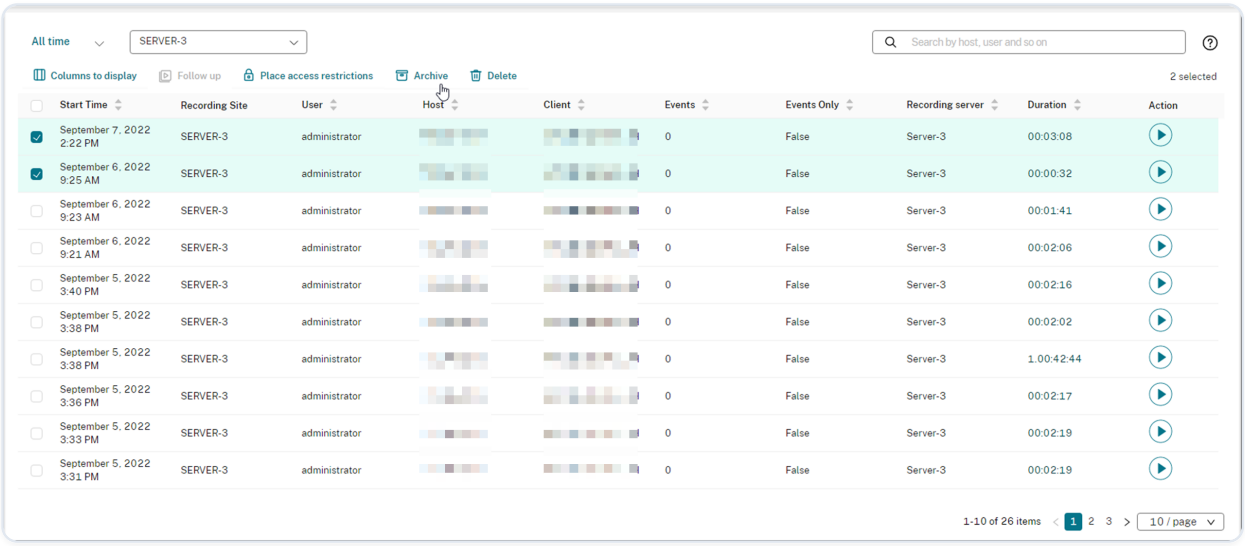
Manage selected recordings

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**.



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.

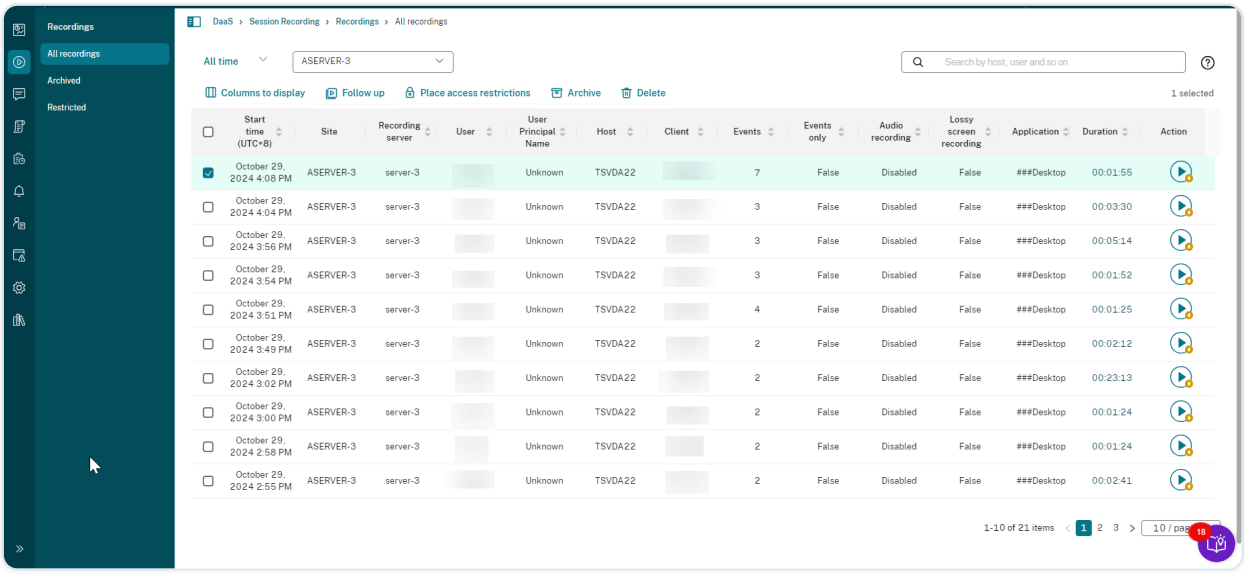
- If you move the recording files to a different location on the same Session Recording server, grant permissions for the System and Network Service accounts to read and write the archived recordings.

- 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.

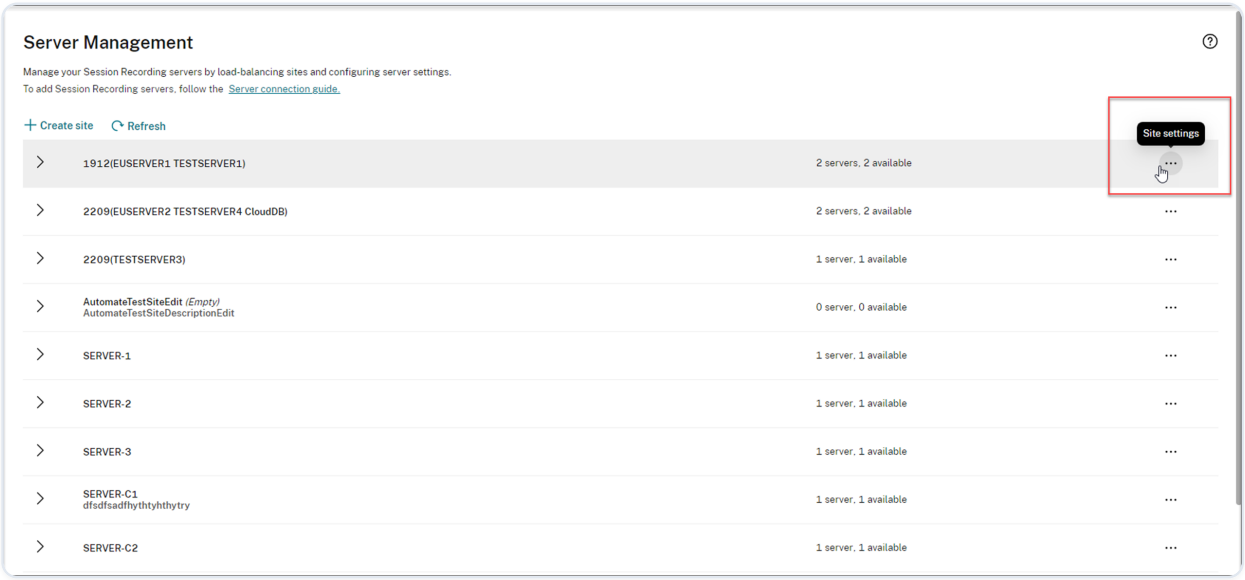
Manage recordings on schedule

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

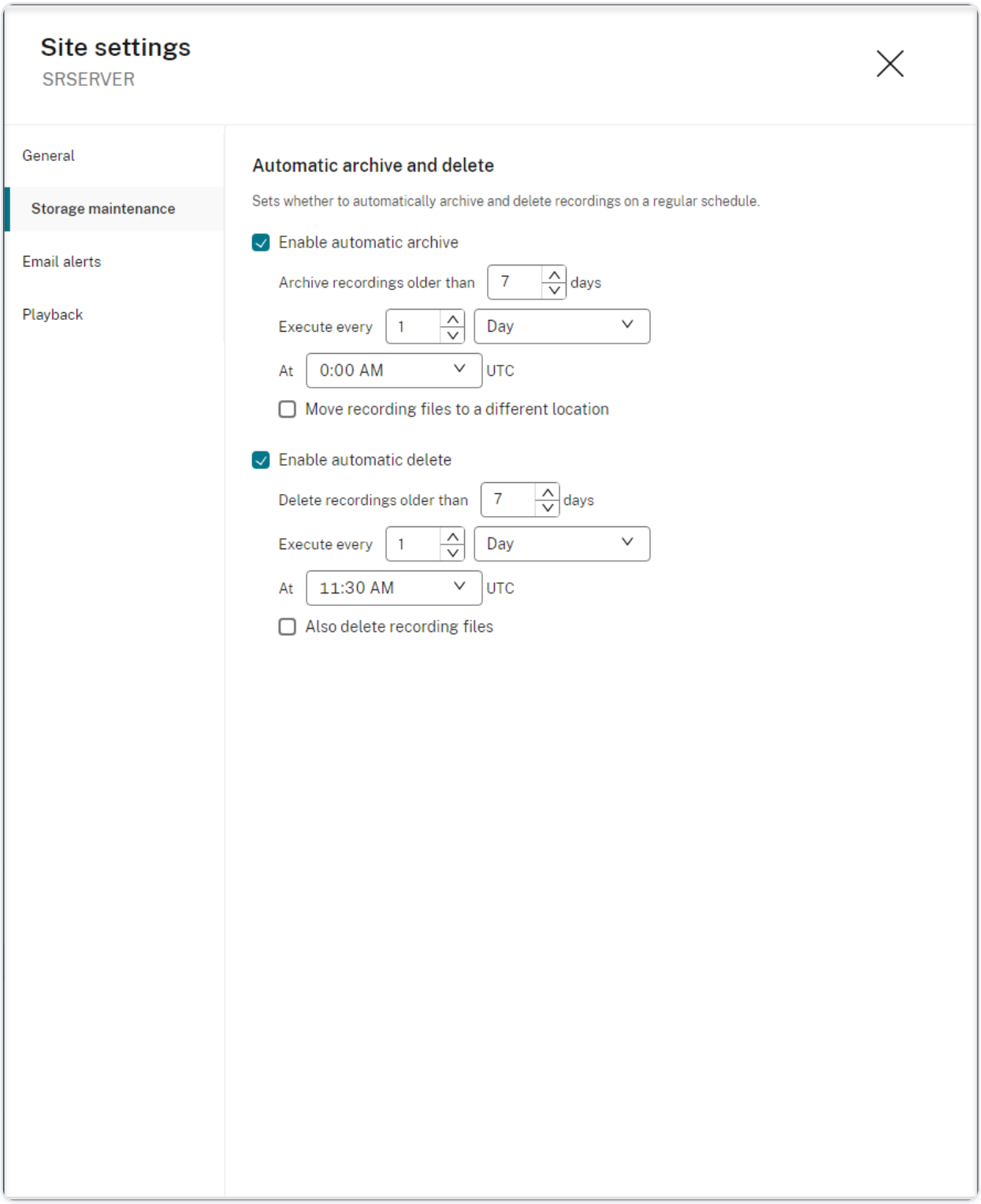
> **Note:**
>
> Only Citrix Cloud™ administrators of the following roles can schedule the tasks:
>
> - Full access
> - The **Cloud Administrator, All** role
> - The **Session Recording-FullAdmin, All** role

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.

Session recording media task service

The Session Recording Media Task Service handles backend operations such as exporting session recordings and performing AI-based analysis tasks. It can be installed either on the Session Recording Server itself or on a separate high-performance server within the same domain.

Prerequisites

For optimal performance, the server hosting the media task service should have:

- 8-core CPU
- 16 GB RAM

Installation and configuration

Follow the steps below to install and configure the Task.

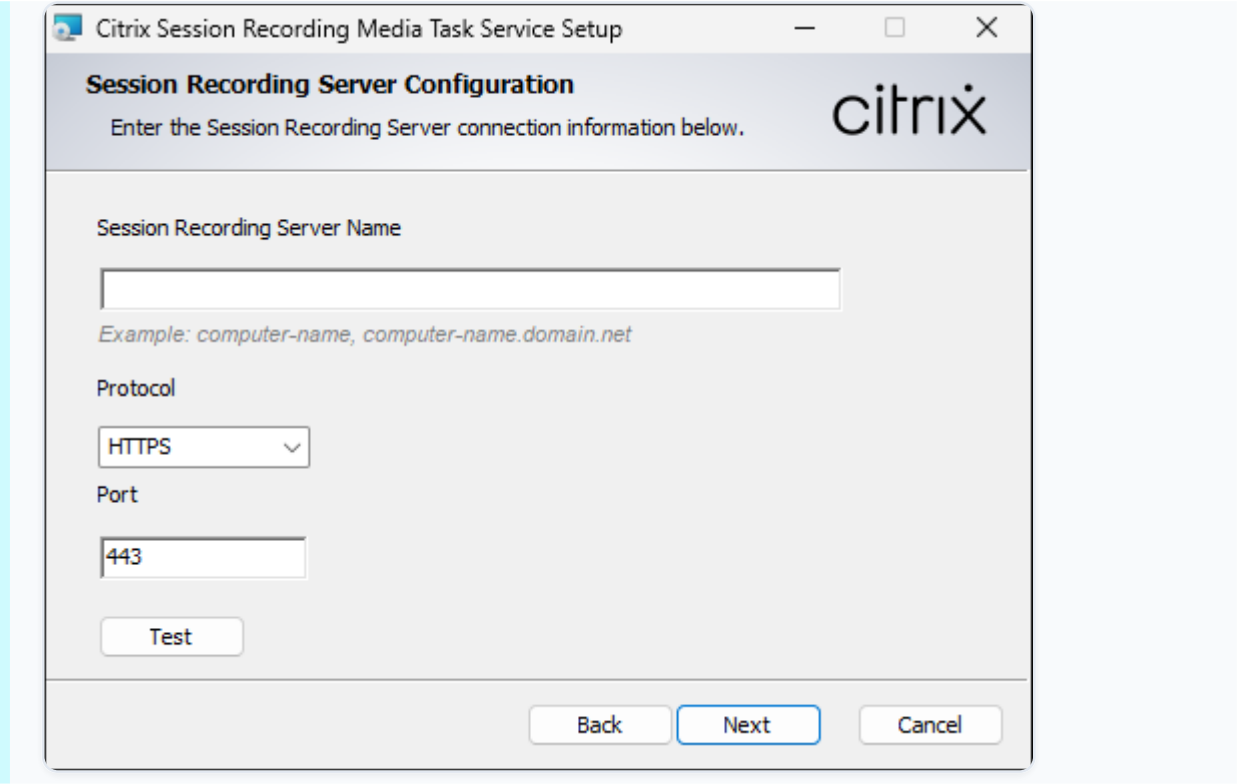
Step 1: Install the Session Recording media task service

1. Run the installer `SessionRecordingTaskClient.msi` which is included in the Session Recording installer package.
2. On the Session Recording Server Configuration screen, enter the name of your Session Recording Server or for load-balanced environments, the load balancer address. Specify the protocol (HTTPS/HTTP) and port (443/80), then click the Test button to verify the connection.

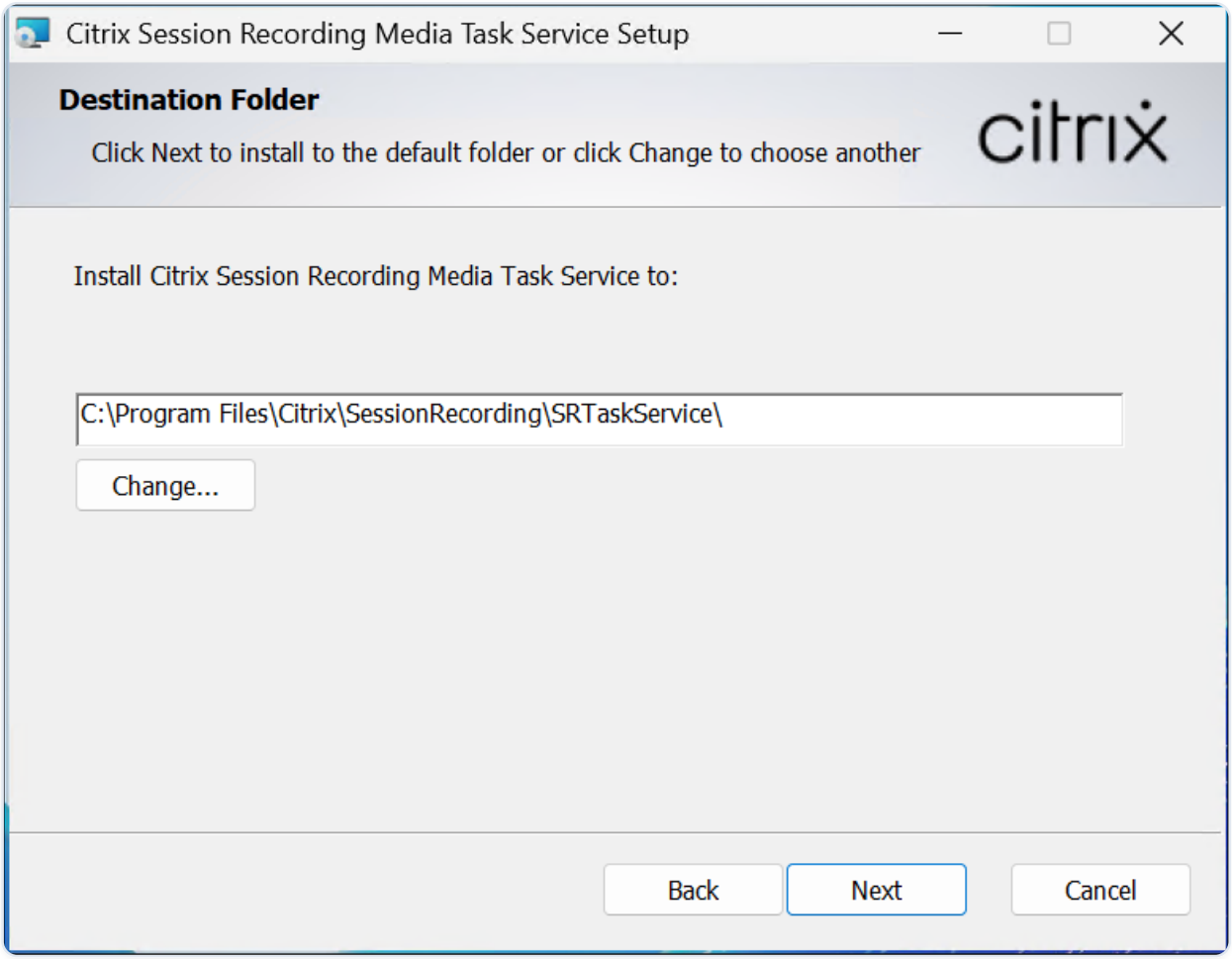
> **Note:**

> When deploying in a load-balanced environment, enable session persistence on your load balancer and select SOURCEIP (or equivalent) as the persistence type.

> - For Citrix NetScaler/ADC, see Persistence settings.
> - For Azure Load Balancer, see Session Persistence.

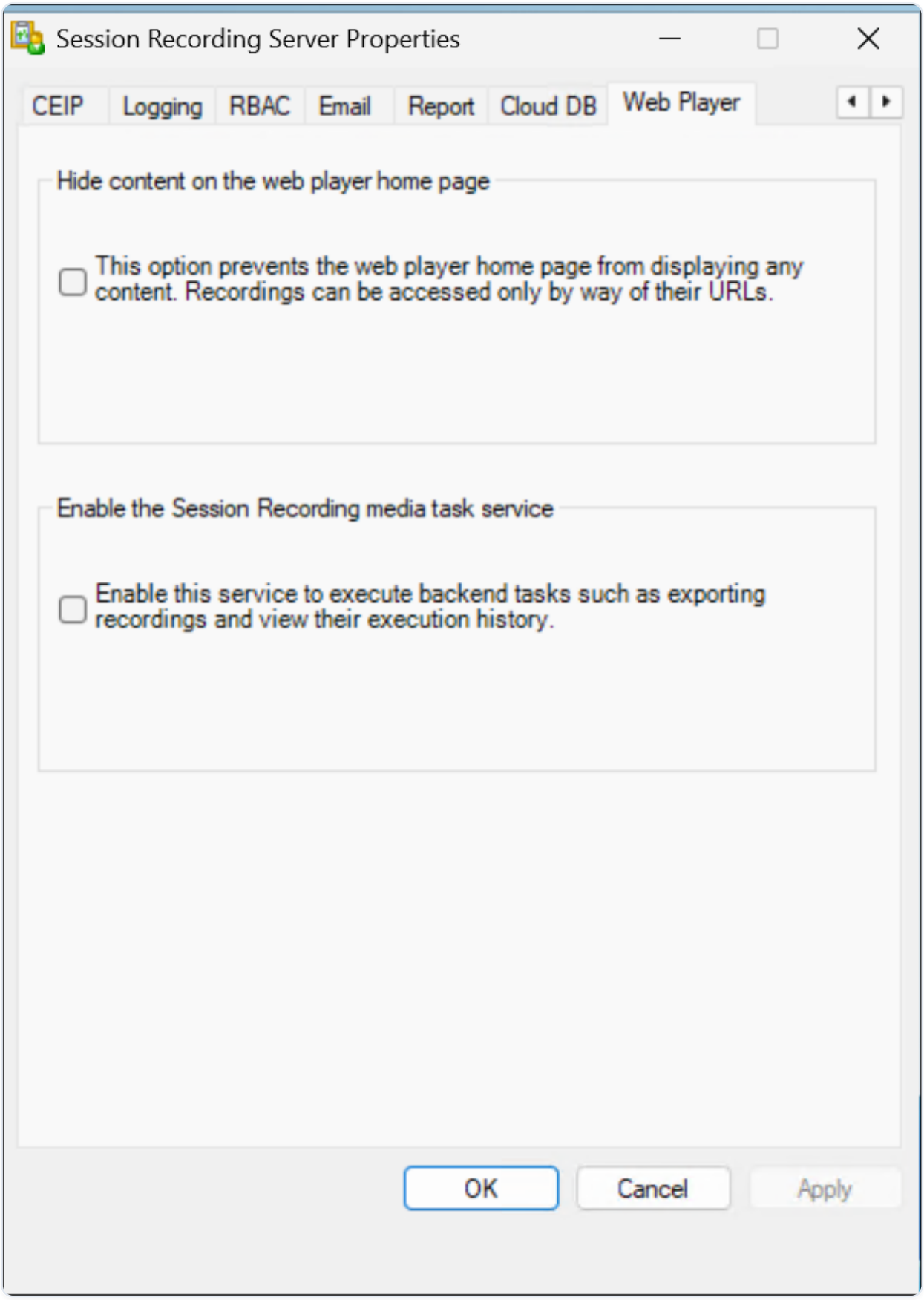


3. On the **Destination Folder** screen, confirm or change the installation path, and then complete the installation.



Step 2: Enable the media task service on the server

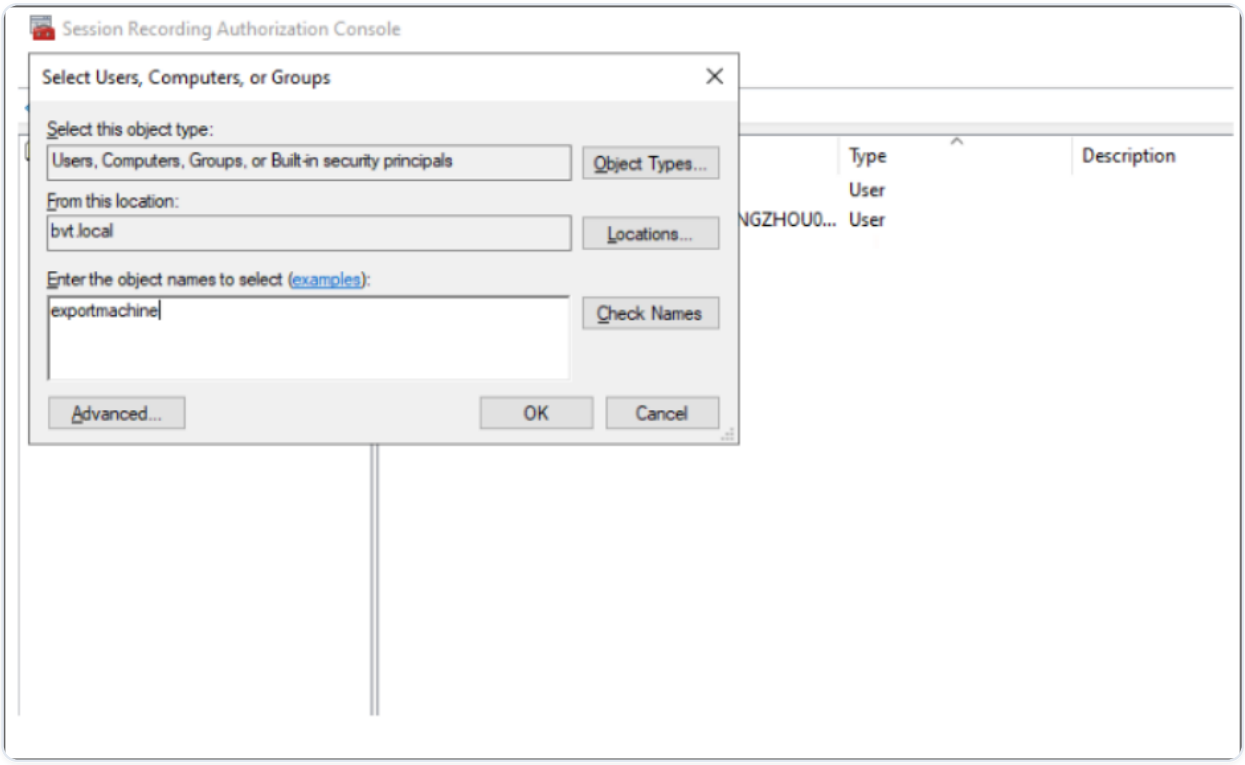
1. On the Session Recording Server, open **Session Recording Server Properties**.
2. Switch to the **Web Player** tab.
3. Check the **Enable the Session Recording media task service** checkbox.
4. Click **Apply**. This action allows the service to perform backend tasks, such as exporting recordings.



Step 3: Assign permissions for the media task service

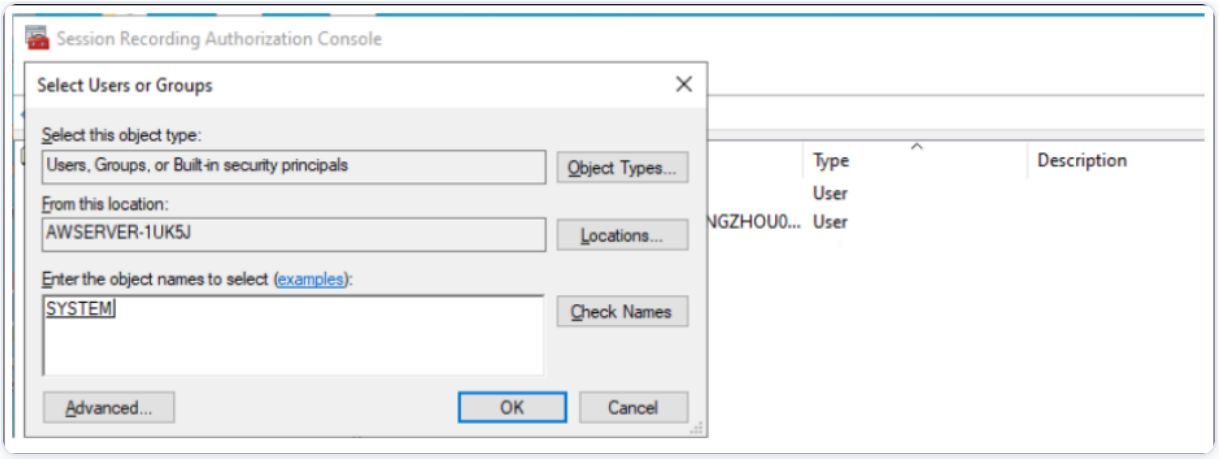
1. On the Session Recording Server, open the **Session Recording Authorization Console**.

2. From the menu bar, select **Player > Assign Users and Groups**.
3. Add the Fully Qualified Domain Name (FQDN) of the computer where the **Session Recording Media Task Service** is installed.



Important:

If the Media Task Service is installed on the same machine as the Session Recording Server, you must also add the SYSTEM account to the Player role.



Step 4 (Optional): Configure a custom export directory

Users can configure a custom path for exporting recordings by changing the registry key value for: at `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SRTaskService\SROutputDir`.

Session recording file export

The session recording file export feature provides a secure and verifiable method for exporting session recordings to meet critical needs such as digital evidence, fraud investigations, and regulatory compliance. It allows authorized administrators to export selected session recordings into a universal MP4 format, along with a sidecar JSON file containing all detected session events.

Key capabilities of this feature include:

- **Role-Based Access Control:** Ensures that only authorized users can perform export operations.
- **Mandatory Justification:** Requires a reason for each export, enhancing the traceability of operations.
- **Comprehensive Activity Logging:** All export activities are recorded in detail for auditing purposes.

Prerequisites

Before you begin the configuration, please ensure your environment meets all of the following requirements:

- The Session Recording Agent, Session Recording Server, and Session Recording Web Player are all installed or have been upgraded to version **2511 or later**.
- Session recording media task service version 2511 or later is installed. Refer to the official setup guide.

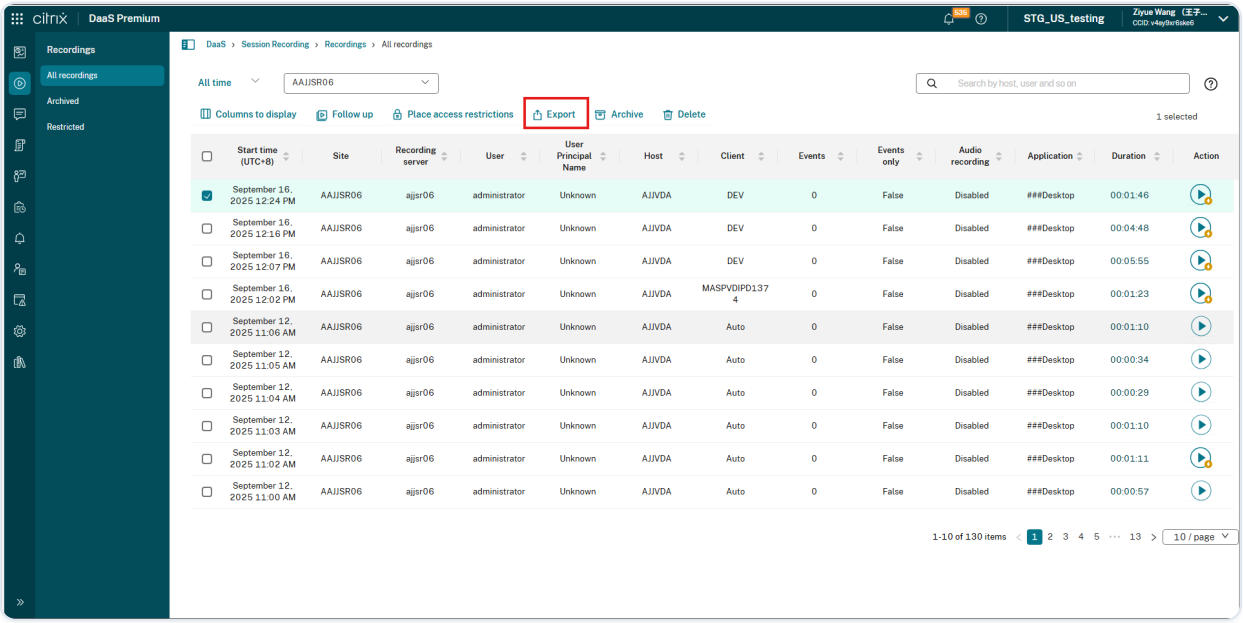
How to use recording file export

How to export Session Recording files

> **Note:**

> Only administrators who have been assigned as full admin can perform export operations. You can refer to Playback permissions for more details.

1. Select **All Recordings** from the left navigation of the Session Recording service.
2. Select one or more recordings that you need to export.
3. Click the **Export** button located above the list.



4. Check the export files under the following folder on the machine running media task service:

   `%ProgramData%\Citrix\SessionRecording\SRTask\Cache`.

   The folder contains the exported MP4 file and, if events were detected during the session, a sidecar JSON file of the same name containing the event data.

> **Note:**
>
> The sidecar JSON file is generated only when the Session Recording media task service is version 2607 or later.

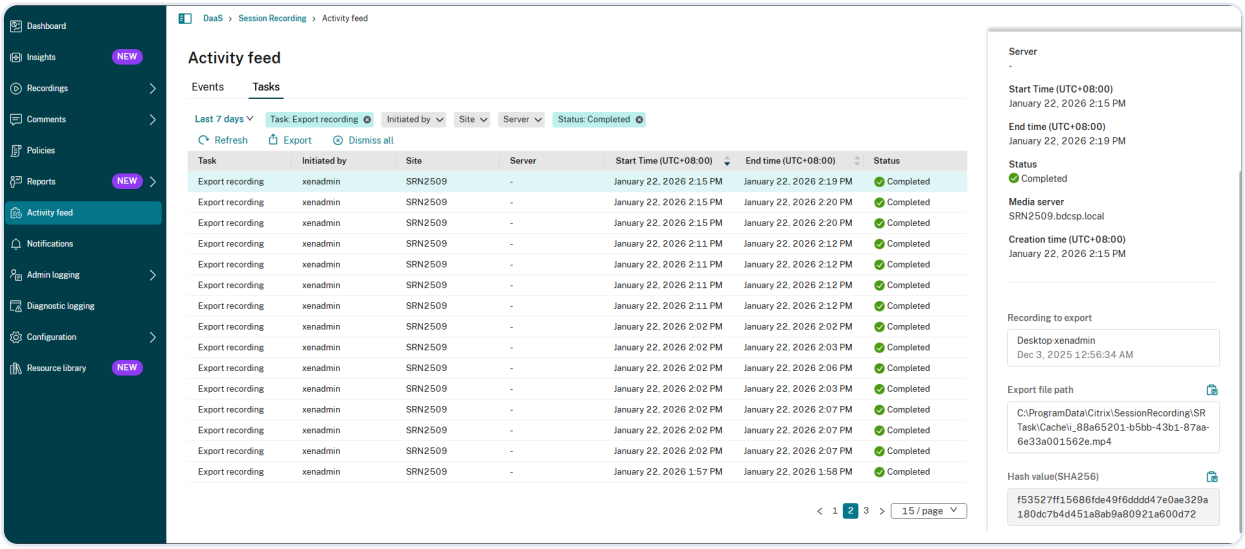
How to monitor export tasks and audit logs

- To view export status:

  a. In the Session Recording service view, select **Activity Feed** from the left navigation.

  b. Switch to **Tasks** tabs to view the information about tasks that happened in the past.

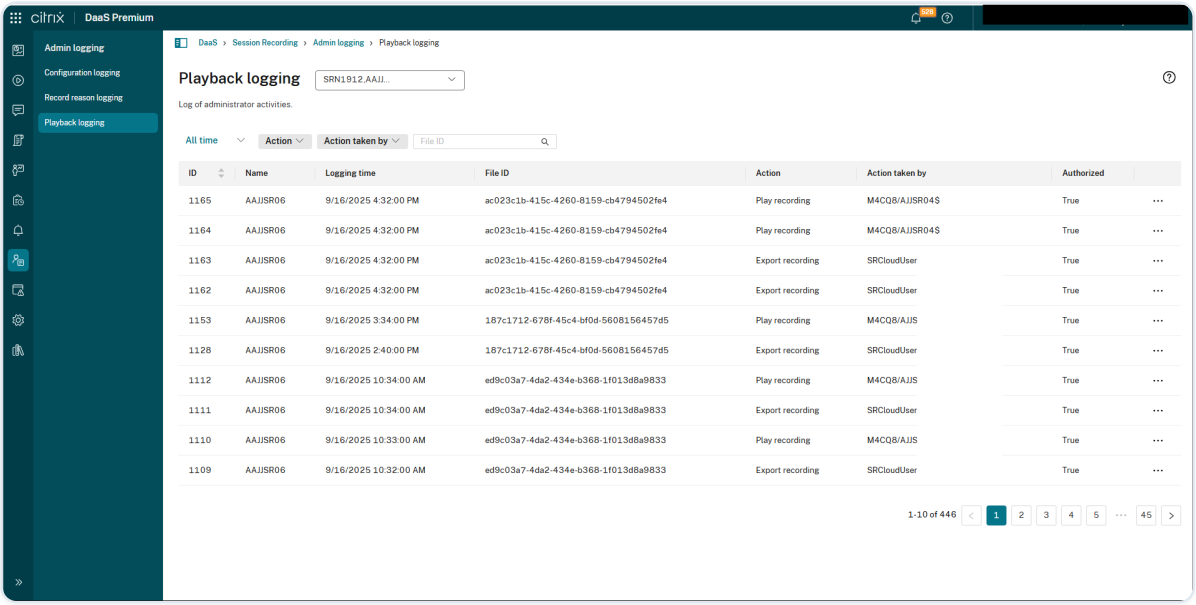
c. This page displays the real-time status of all export tasks, including "In Progress," "Completed," "Pending," or "Failed."



- To audit export activities:

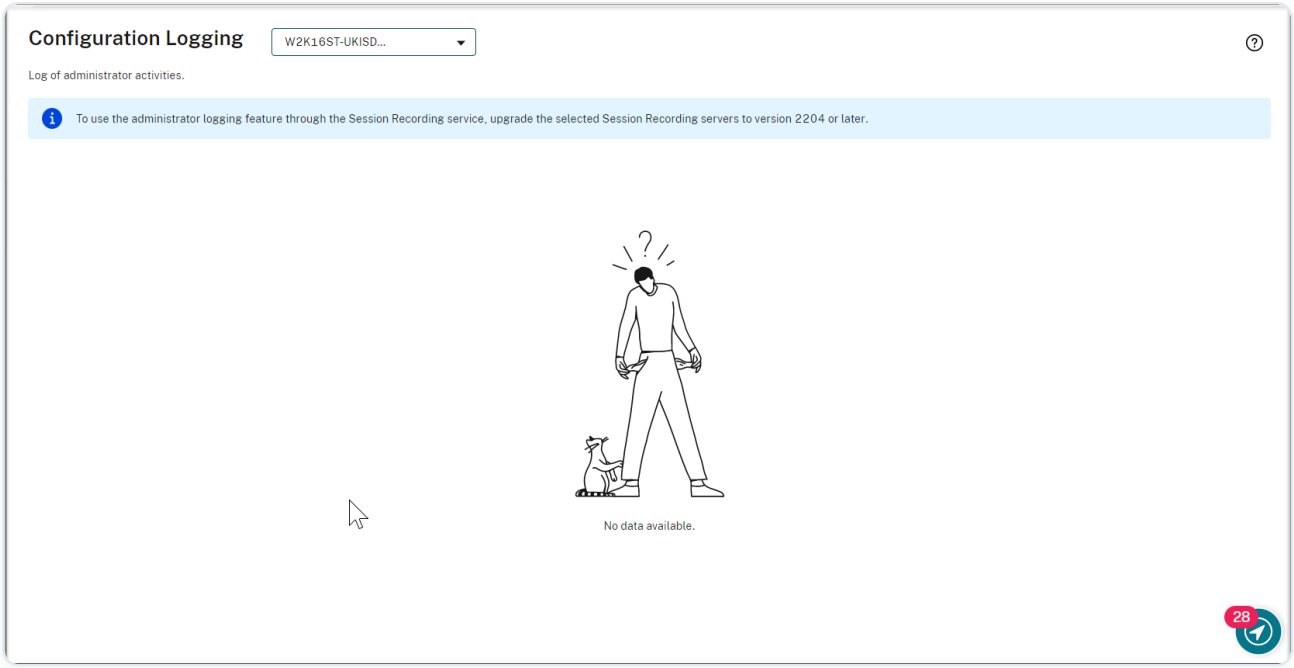
a. Navigate to **Admin Logging -> Playback Logging**.

b. Here you can view the export records for all recordings *(Action will be Export recording)*, along with details such as the user who performed the action and the timestamp.



Administrator logging

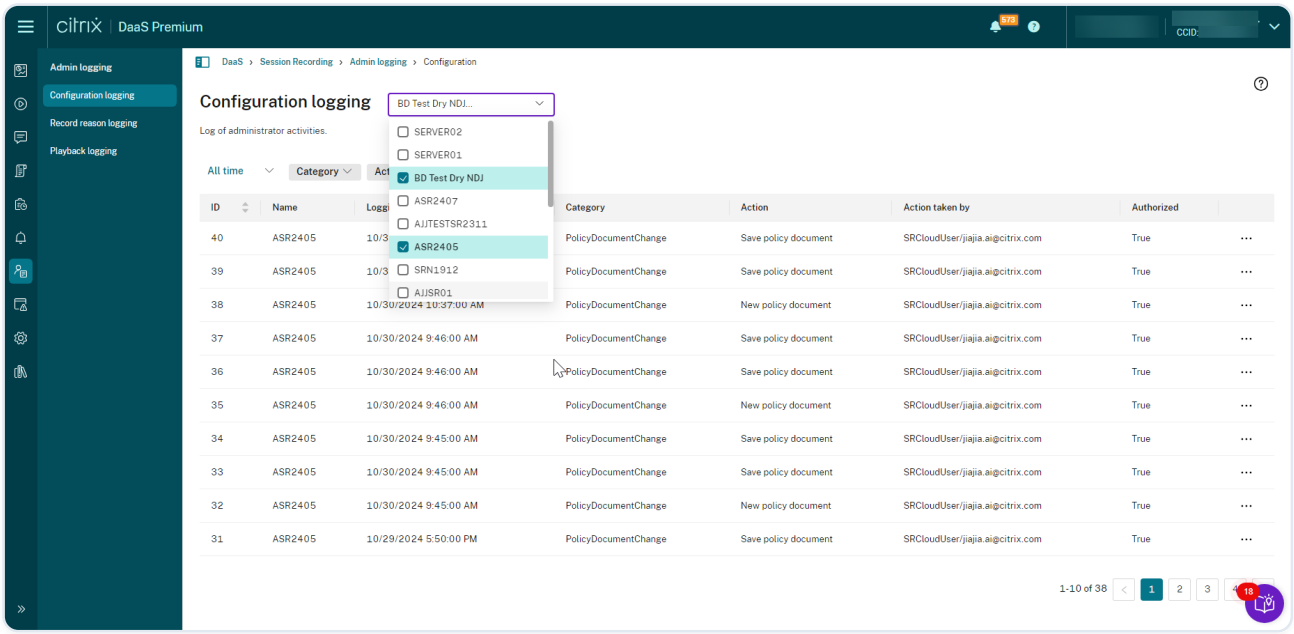
Using Session Recording server 2204 or later, you can query administrator logging data through the Session Recording service. If you select a site that contains a Session Recording server earlier than version 2204, the following banner appears, and no data is available.



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.

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



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

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

Logging data overview

Administrator logging data consists of:

- Configuration logging
- Recording reason logging
- Playback logging

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.

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**

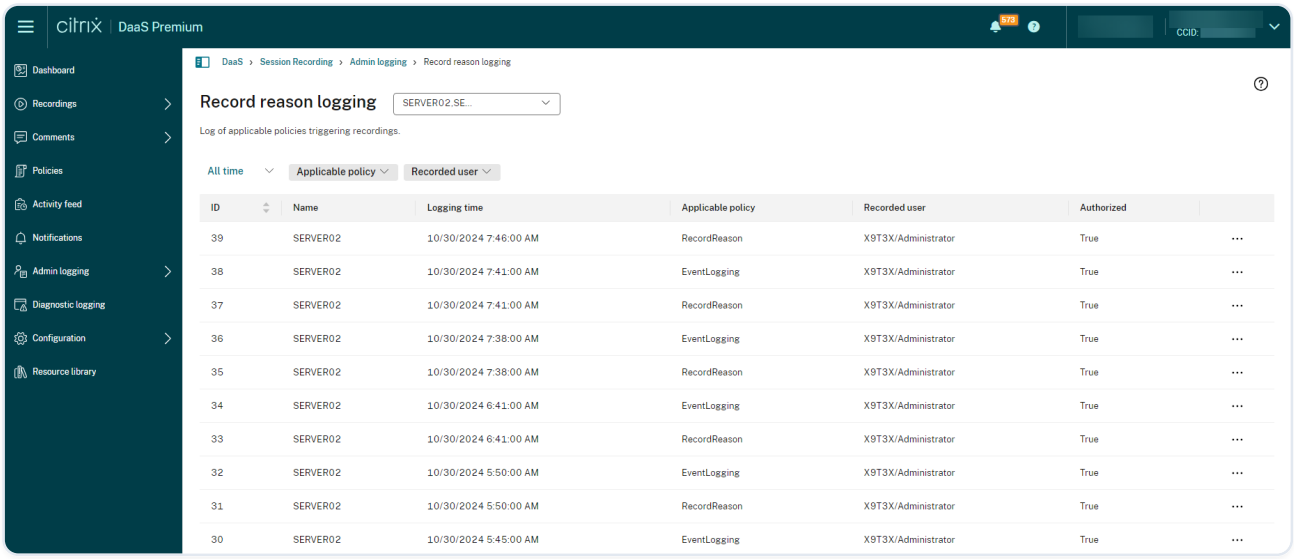
   The mandatory blocking setting does not impact the recording of sessions.

> **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.

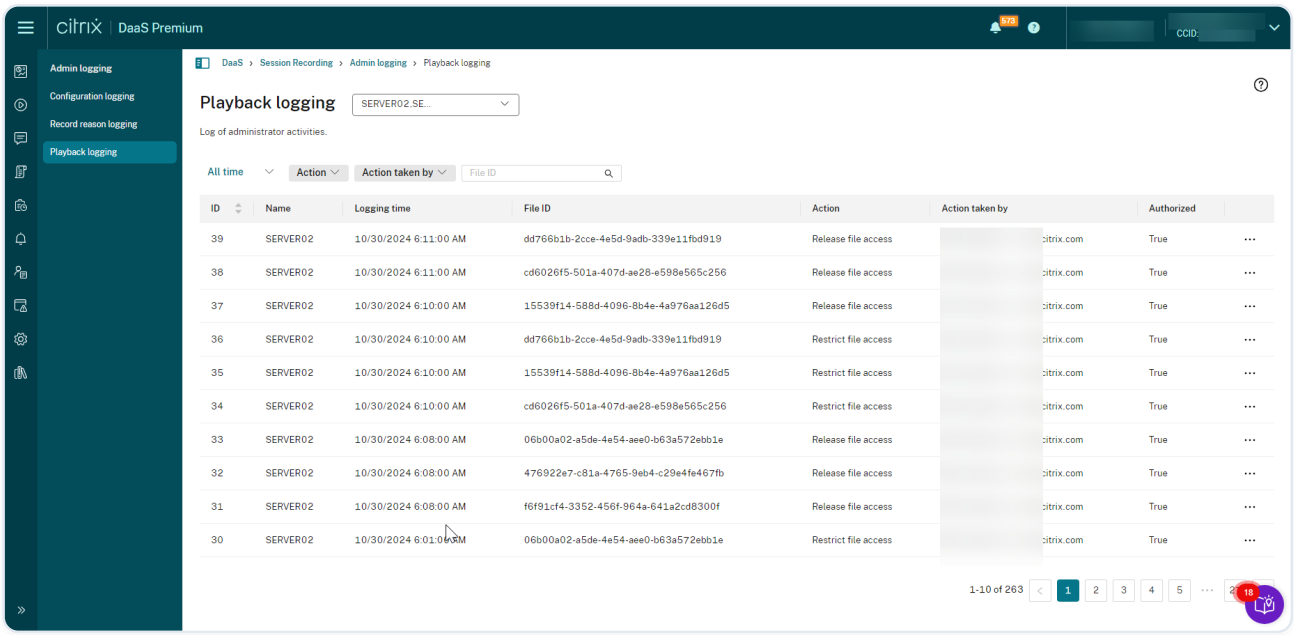


To enable the feature, enable both administrator logging and recording reason logging on your Session Recording servers. If **Enable administrator logging** is not selected, enabling recording reason logging does not take effect.

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.



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.

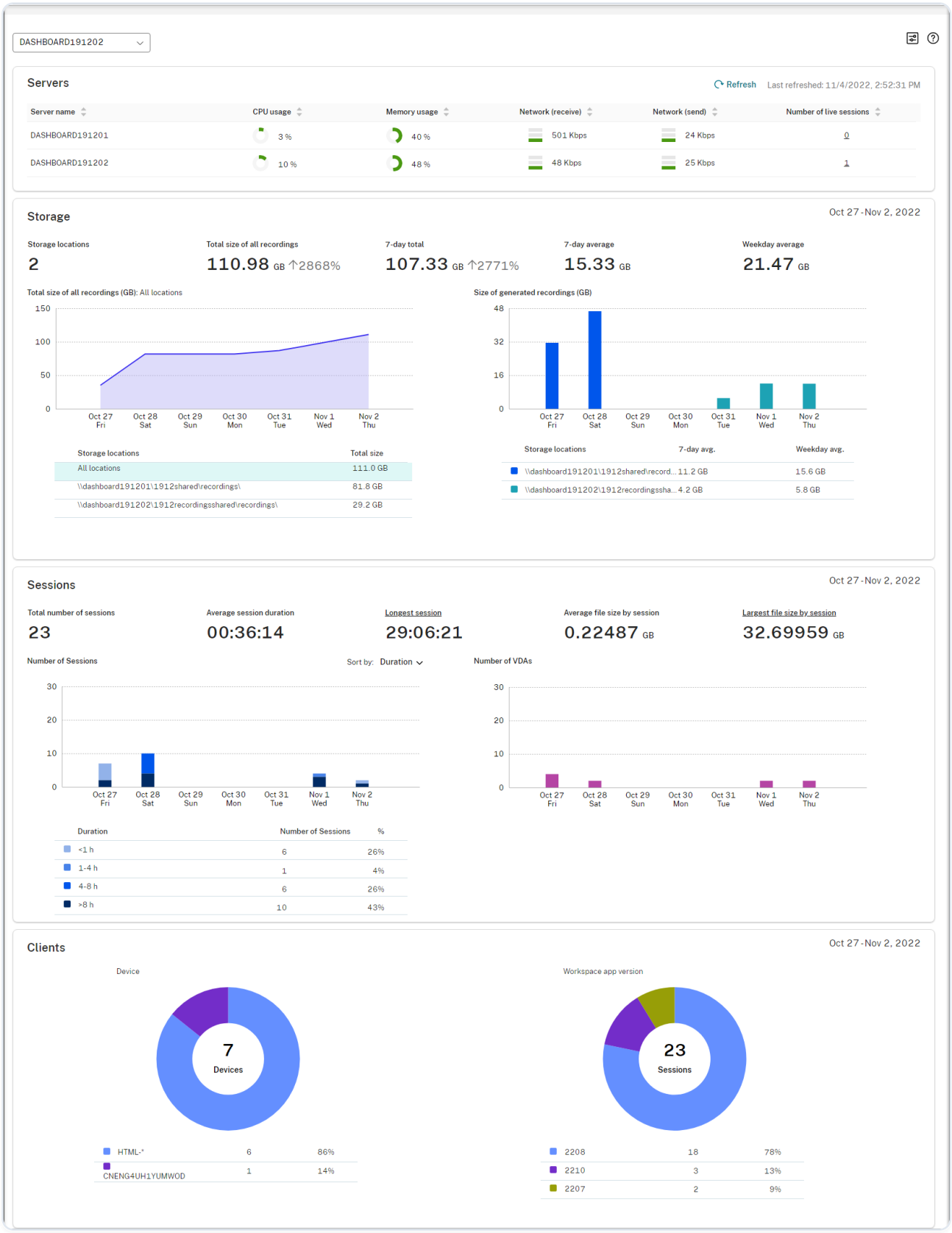
Management dashboard

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
- Agent Status

For a sample dashboard, see the following screen capture:


DASHBOARD191202
Servers
Refresh
Last refreshed: 11/4/2022, 2:52:31 PM
Server name
CPU usage
Memory usage
Network (receive)
Network (send)
Number of live sessions
DASHBOARD191201
3 %
40 %
501 Kbps
24 Kbps
0
DASHBOARD191202
10 %
48 %
48 Kbps
25 Kbps
1
Storage
Oct 27 - Nov 2, 2022
Storage locations
2
Total size of all recordings
110.98 GB ↑2868%
7-day total
107.33 GB ↑2771%
7-day average
15.33 GB
Weekday average
21.47 GB
Total size of all recordings (GB): All locations
150
100
50
0
Oct 27 Fri
Oct 28 Sat
Oct 29 Sun
Oct 30 Mon
Oct 31 Tue
Nov 1 Wed
Nov 2 Thu
Storage locations
Total size
All locations
111.0 GB
\\dashboard191201\1912shared\recordings\
81.8 GB
\\dashboard191202\1912recordingsshared\recordings\
29.2 GB
Size of generated recordings (GB)
48
32
16
0
Oct 27 Fri
Oct 28 Sat
Oct 29 Sun
Oct 30 Mon
Oct 31 Tue
Nov 1 Wed
Nov 2 Thu
Storage locations
7-day avg.
Weekday avg.
\\dashboard191201\1912shared\record...
11.2 GB
15.6 GB
\\dashboard191202\1912recordingssha...
4.2 GB
5.8 GB
Sessions
Oct 27 - Nov 2, 2022
Total number of sessions
23
Average session duration
00:36:14
Longest session
29:06:21
Average file size by session
0.22487 GB
Largest file size by session
32.69959 GB
Number of Sessions
Sort by: Duration
30
20
10
0
Oct 27 Fri
Oct 28 Sat
Oct 29 Sun
Oct 30 Mon
Oct 31 Tue
Nov 1 Wed
Nov 2 Thu
Duration
Number of Sessions
%
<1 h
6
26%
1-4 h
1
4%
4-8 h
6
26%
>8 h
10
43%
Number of VDAs
30
20
10
0
Oct 27 Fri
Oct 28 Sat
Oct 29 Sun
Oct 30 Mon
Oct 31 Tue
Nov 1 Wed
Nov 2 Thu
Clients
Oct 27 - Nov 2, 2022
Device
7
Devices
HTML-*
6
86%
CNENG4UH1YUMWOD
1
14%
Workspace app version
23
Sessions
2208
18
78%
2210
3
13%
2207
2
9%

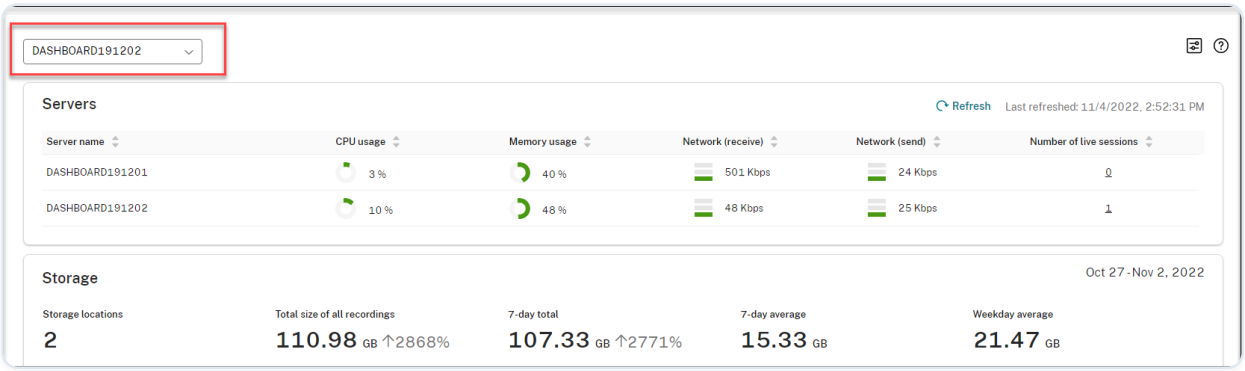
Note:

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

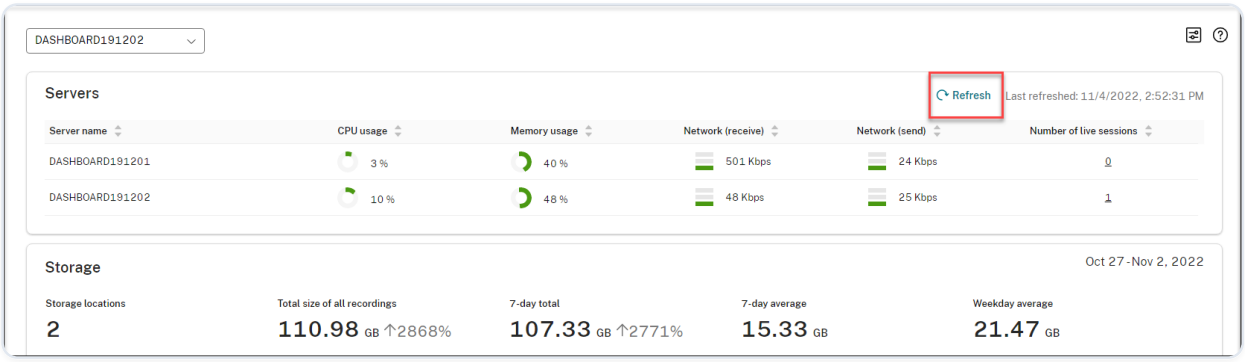
- You are using the cloud client version 7.42.15010.4 or later.
- You have only one site that has available servers and you have turned on the feature toggle on the dashboard settings page of that site.

Tips for using the dashboard

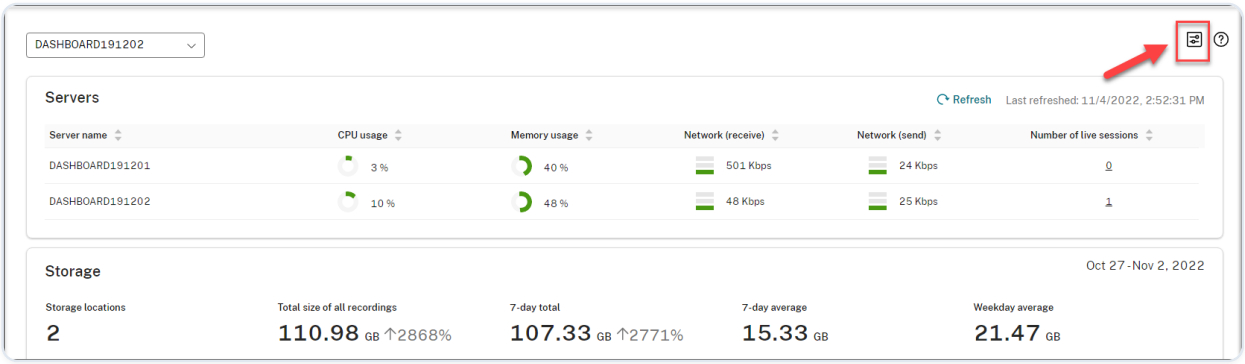
- The dashboard is the new home page for the Session Recording service console. It is available only for Citrix Cloud™ administrators assigned any of the following roles:
  - Full access
  - **Cloud Administrator** role
  - **Session Recording-FullAdmin** role
- The dashboard presents data relevant to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

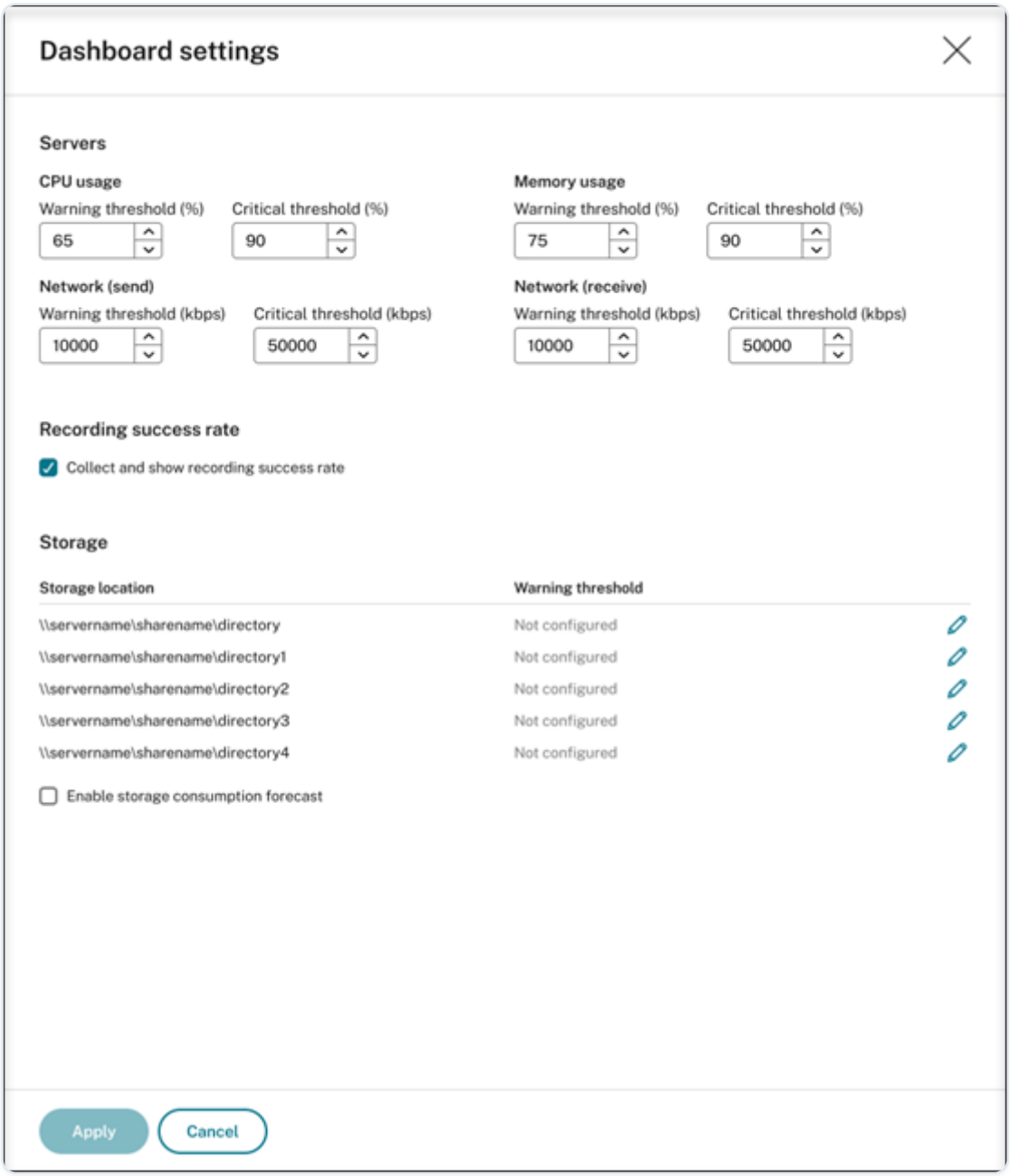


- The **Servers** section refreshes data automatically every 120 seconds. Immediate data refreshes occur when you open the dashboard page, select a site, or click **Refresh**. The next data refresh does not start until the previous refresh completes. Thus, if you click **Refresh** during a data refresh,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

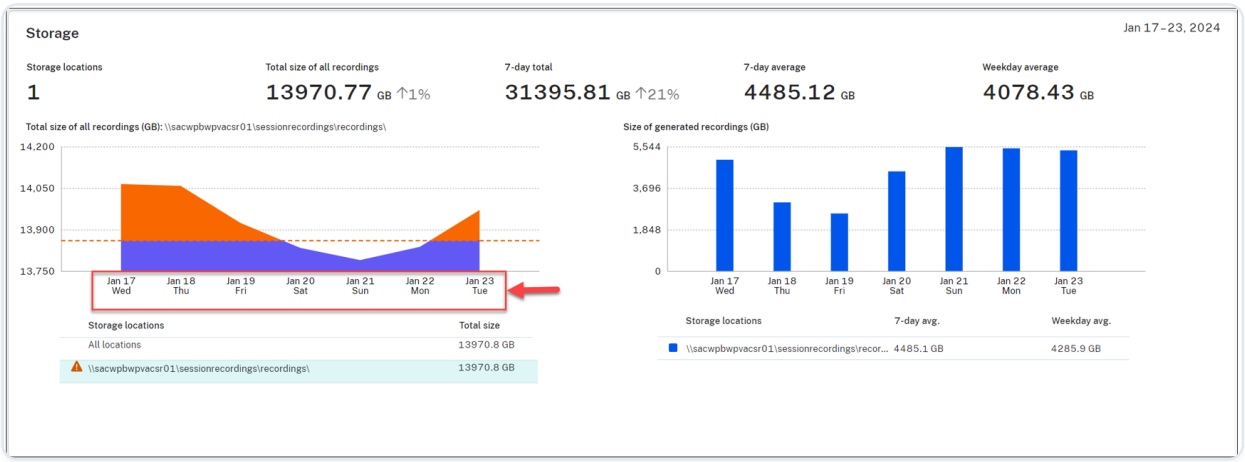
- Allocate space in a location for recording storage and set warning thresholds for the space usage. When a warning or critical threshold is reached, the entry is displayed with an orange or red icon.

  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.

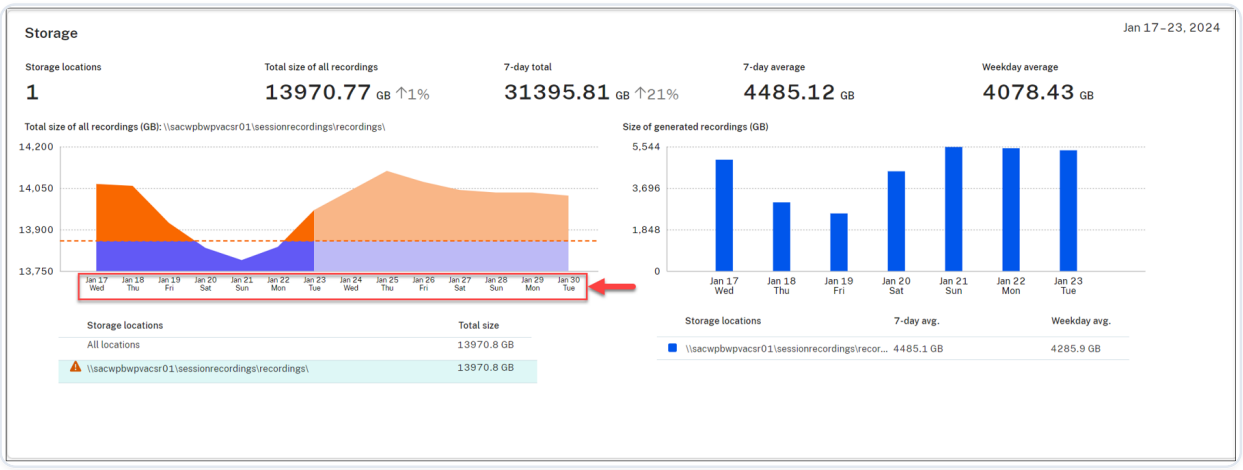


- Enable storage consumption forecast. Storage consumption forecast allows you to predict resource usage and take precautions in advance. After you enable the feature, a storage consumption forecast for the next 7 days can be generated based on sufficient historical consumption data of approximately 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:

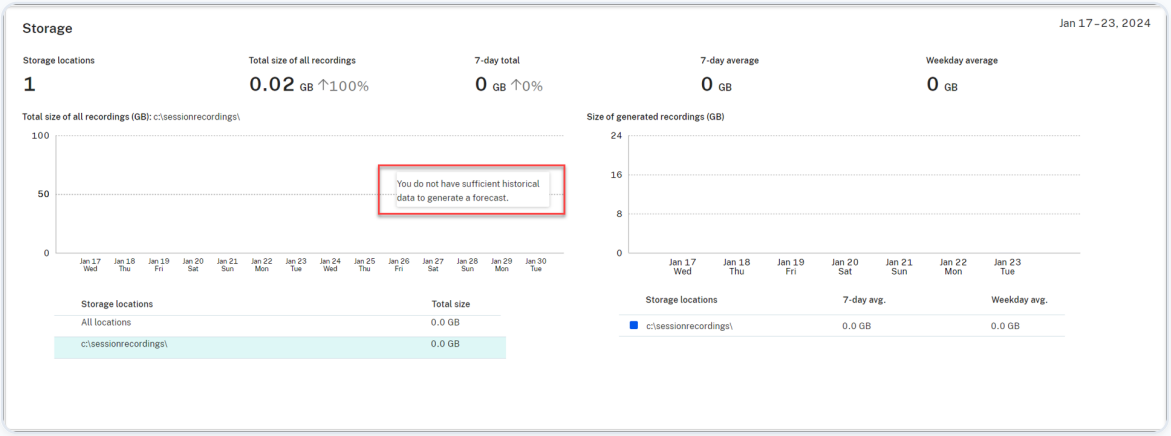


When the storage consumption forecast is enabled, the **Total size of all recordings** chart shows not only the actual consumption data over the past 7 days but also a consumption forecast for the next 7 days. For example:

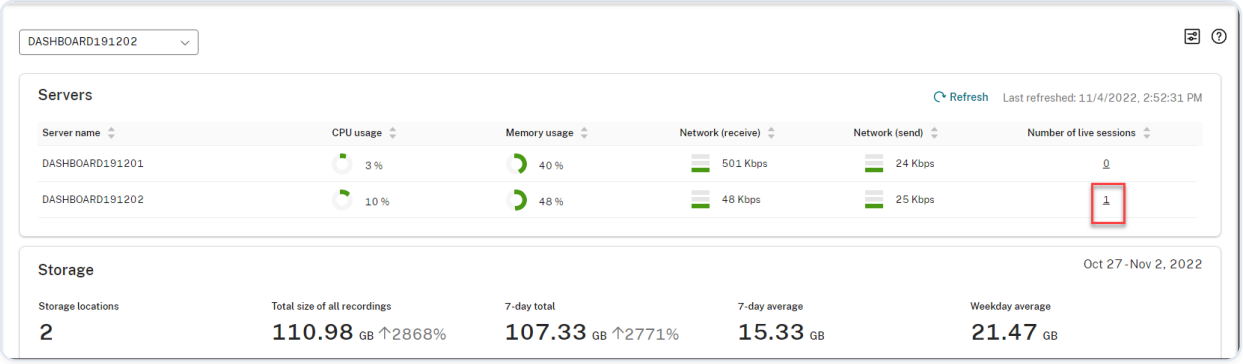


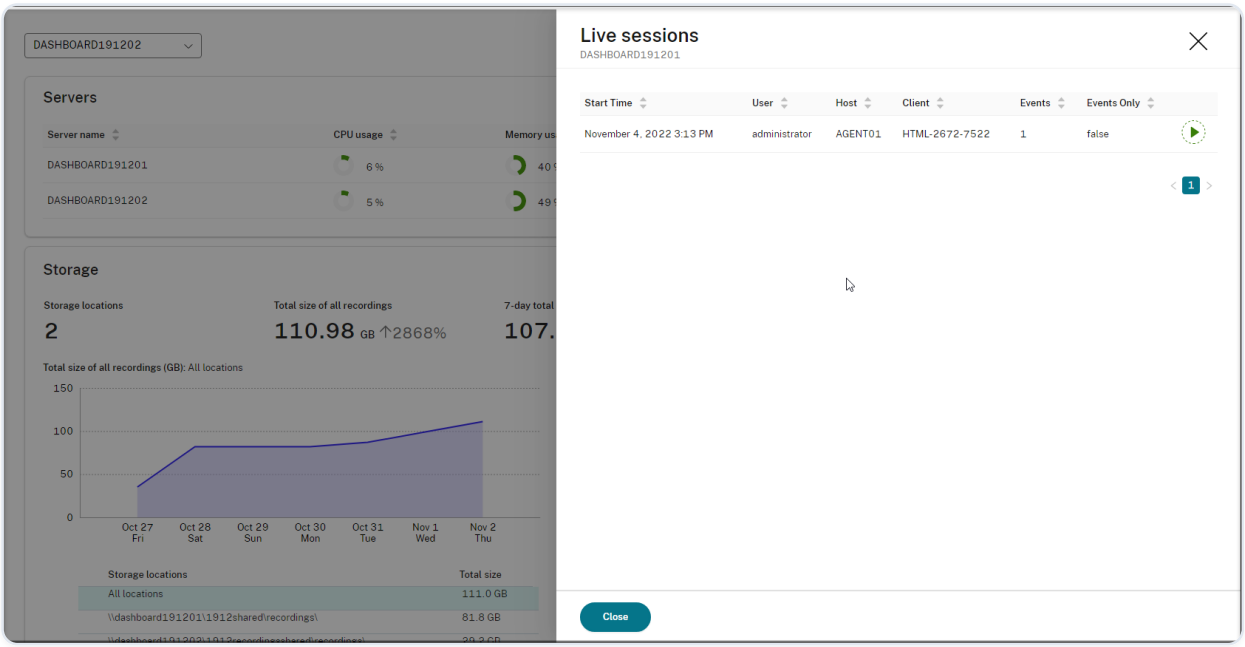
Note:

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:

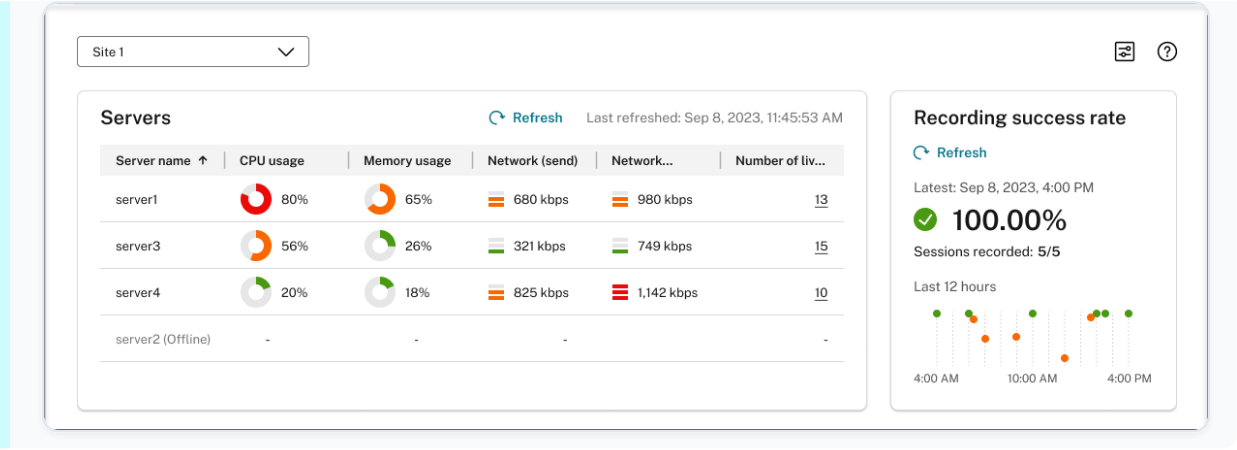




- In the **Recording success rate** section, you can see a widget showing the recording success rates for the current site. The recording success rate is calculated as follows:

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

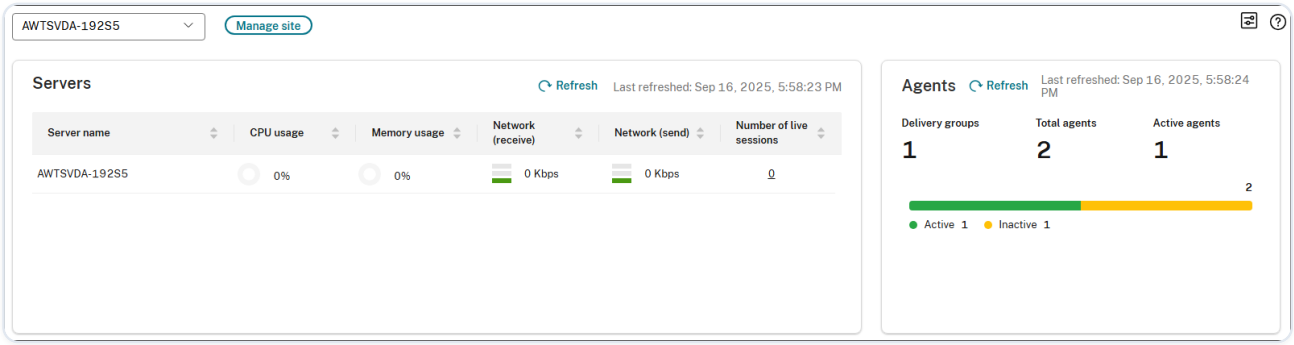
> **Note:**
>
> The recording success rate widget can be shown next to the **Servers** section if the following conditions are met:
>
> - You are using the cloud client version 7.42.15010.4 or later.
> - You have only one site that has available servers and you have turned on the feature toggle on the dashboard settings page of that site.
>
> For example:



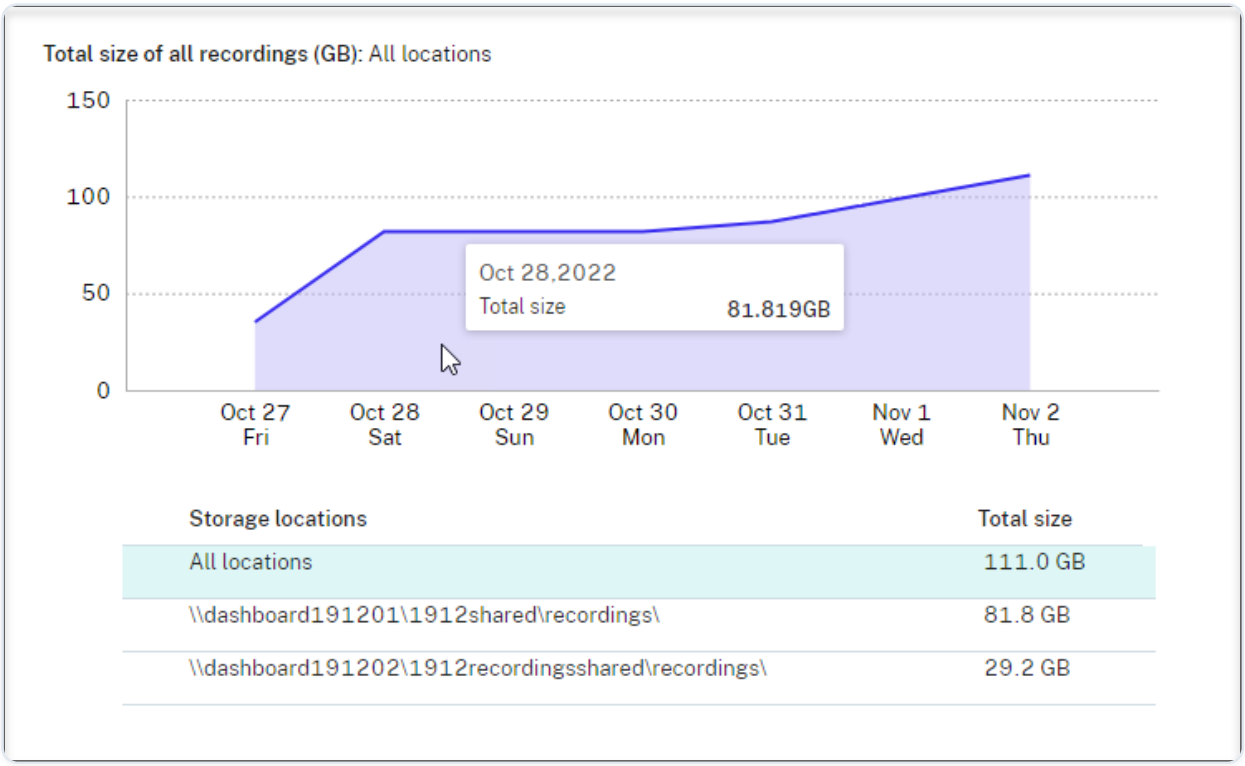
- The **Agent** section provides a quick summary of the status of all your Session Recording agents if the Session Recording Server/Agent are upgraded to 2503. It displays:
  - **Total agents:** The total number of Session Recording agents connected to the service.
  - **Active agents:** The number of agents that are currently online and sending heartbeats to the service.
  - **Inactive agents:** The number of agents that are currently offline or have not sent a heartbeat within a specified time.

This overview helps you quickly identify any potential issues with agent connectivity and ensure that your recording environment is healthy. For more detailed information about individual agents, including their VDA status, you can navigate to Configuration > Site management.

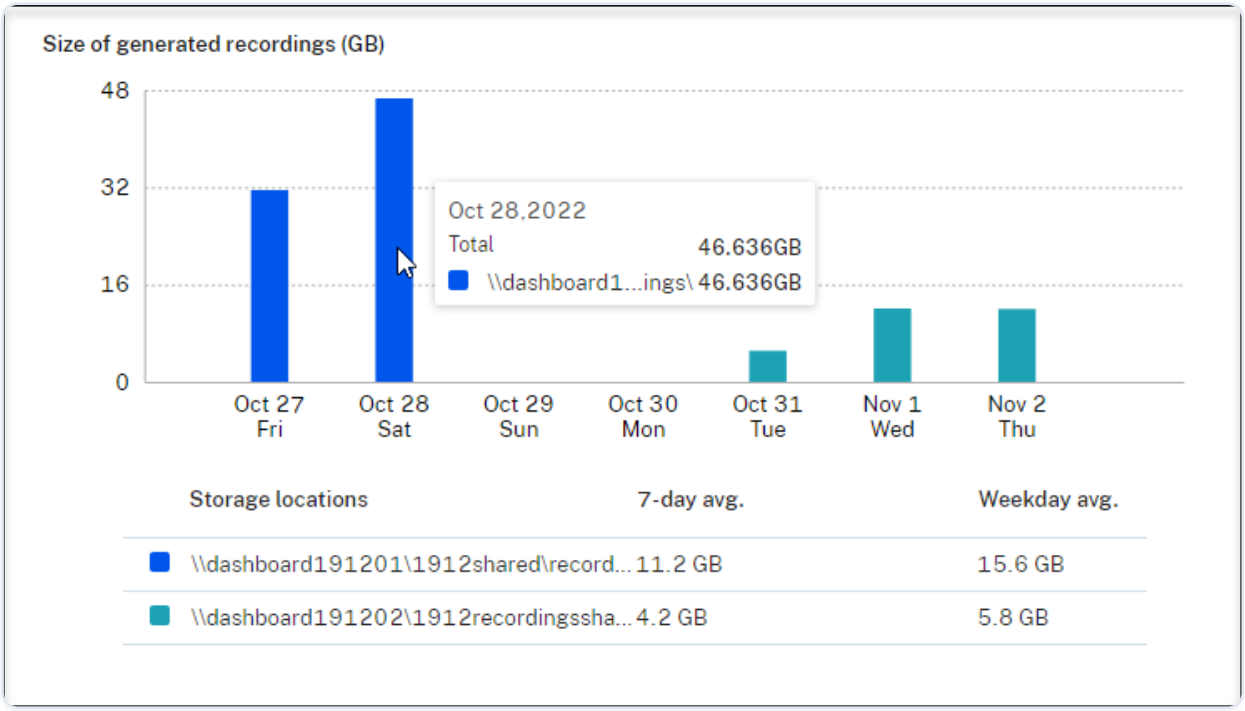
For Example:



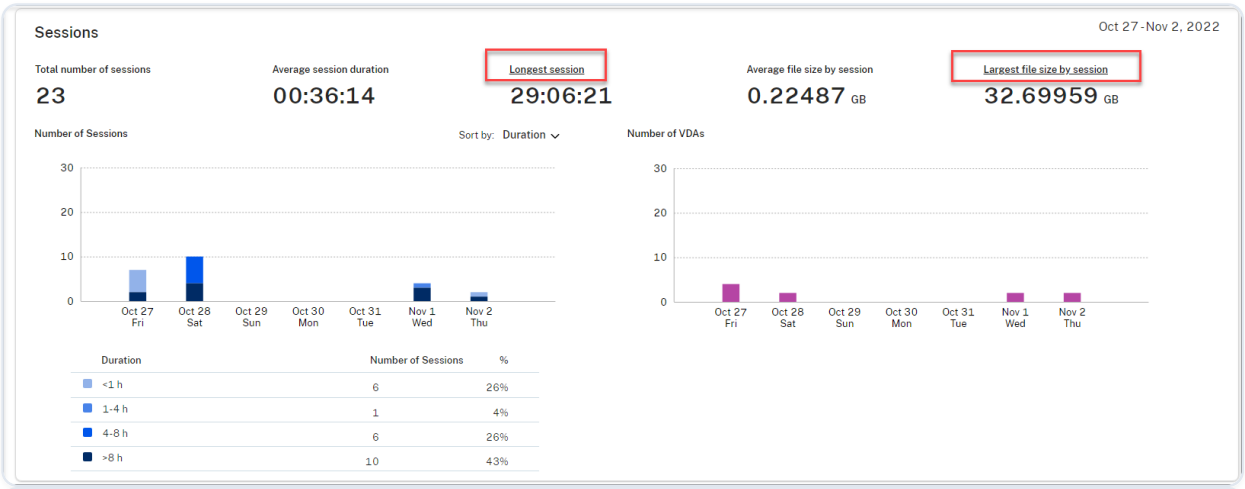
- In the **Total size of all recordings (GB)** section, you can switch between storage locations to view relevant data. You can also hover over the chart to view the total size of all recordings on a specific day.

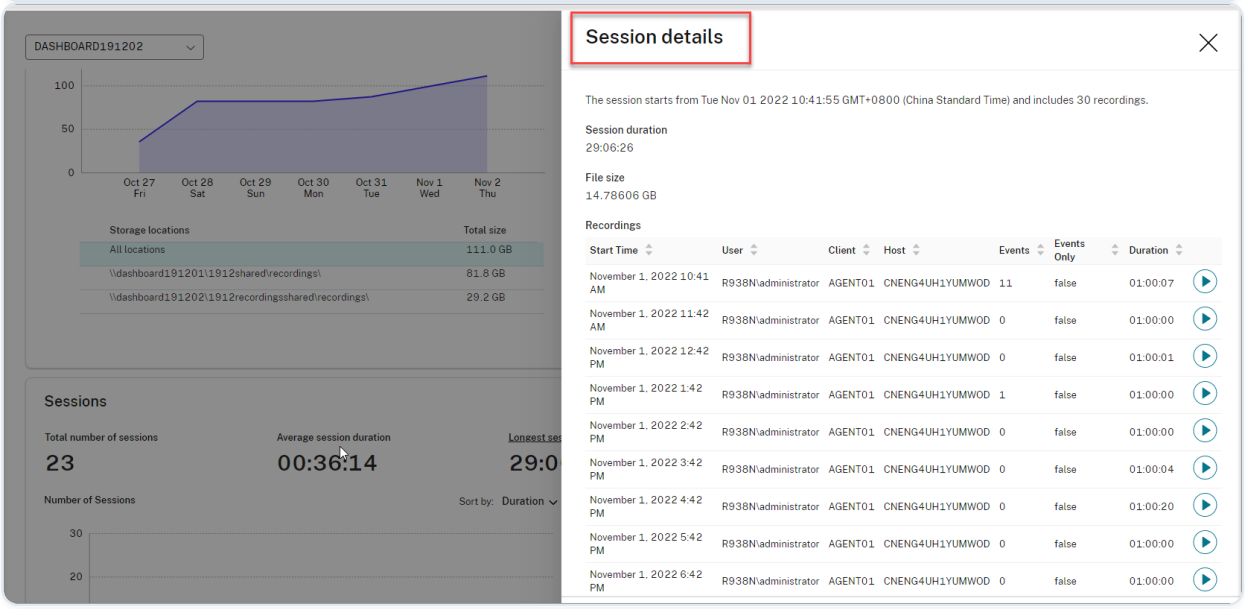


- In the **Size of generated recordings (GB)** section, you can hover over the bar chart corresponding to a day to view the size of newly generated recordings on that day.

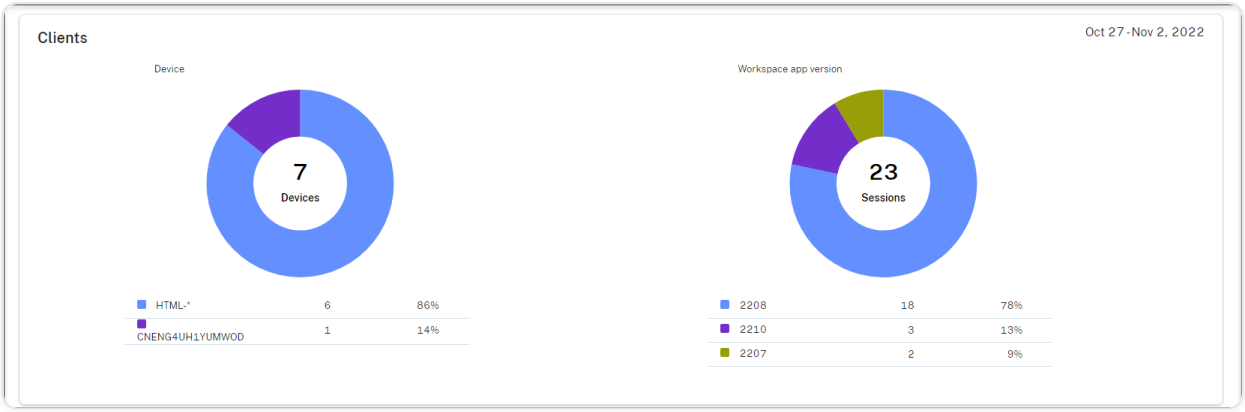


- In the **Sessions** section, you can click **Longest session** and **Largest file size by session** to view session details.

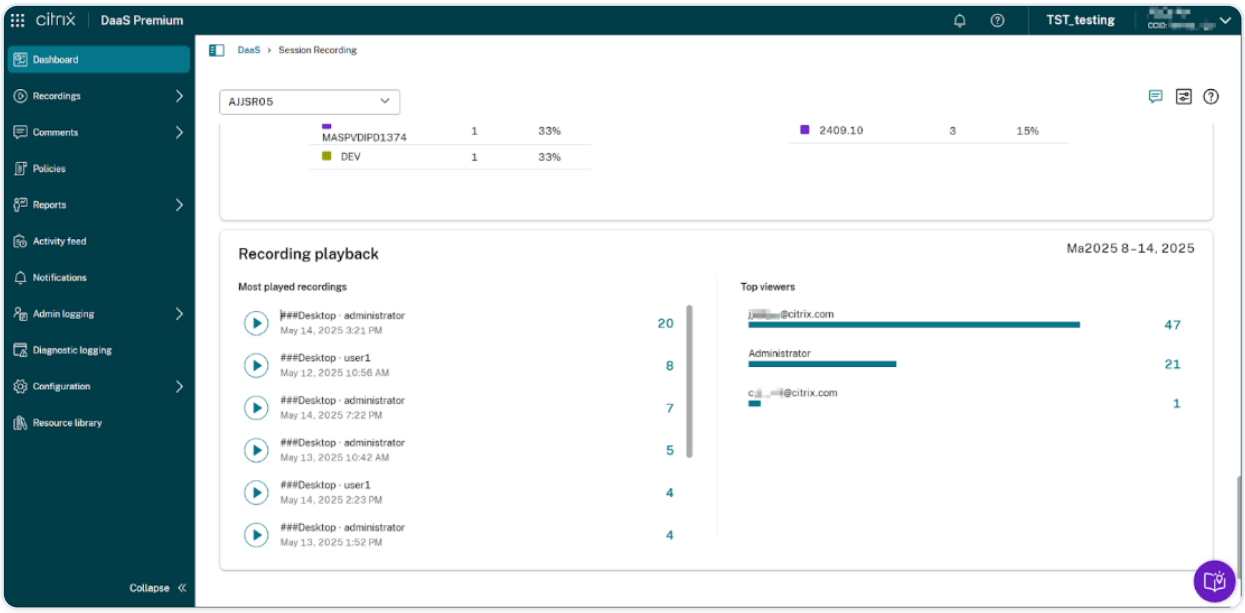




- The **Clients** section shows the percentage of client devices that have different machine name prefixes and the percentage of sessions that run on different versions of Citrix Workspace™ app.

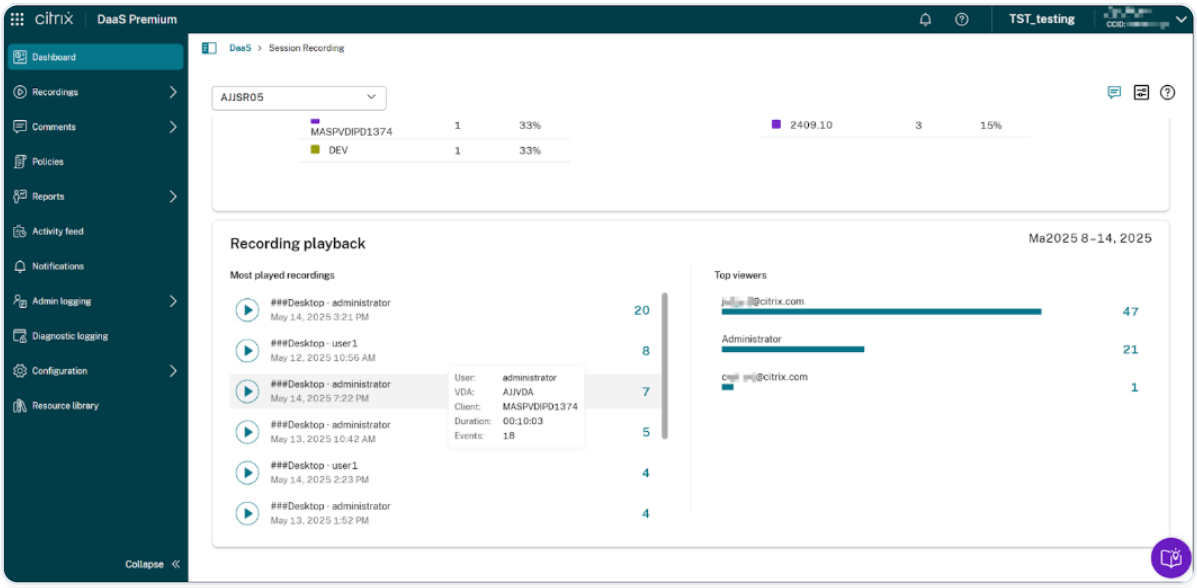


- The Recording playback section provides statistics for recording playback. It displays two views: the most played recordings and the top viewers.

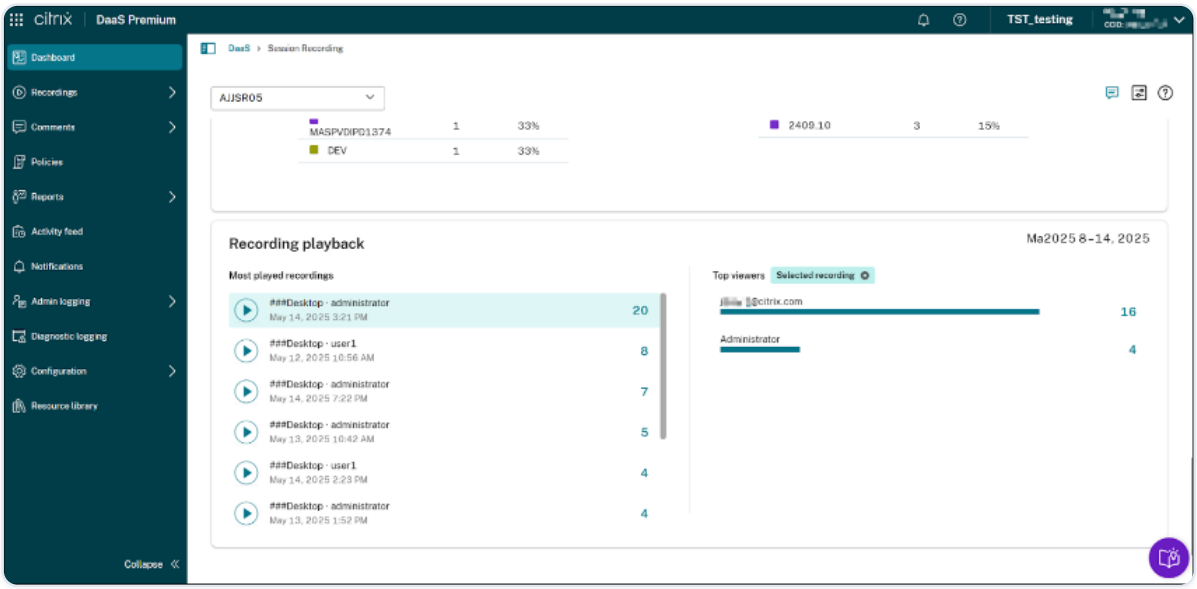


In this section:

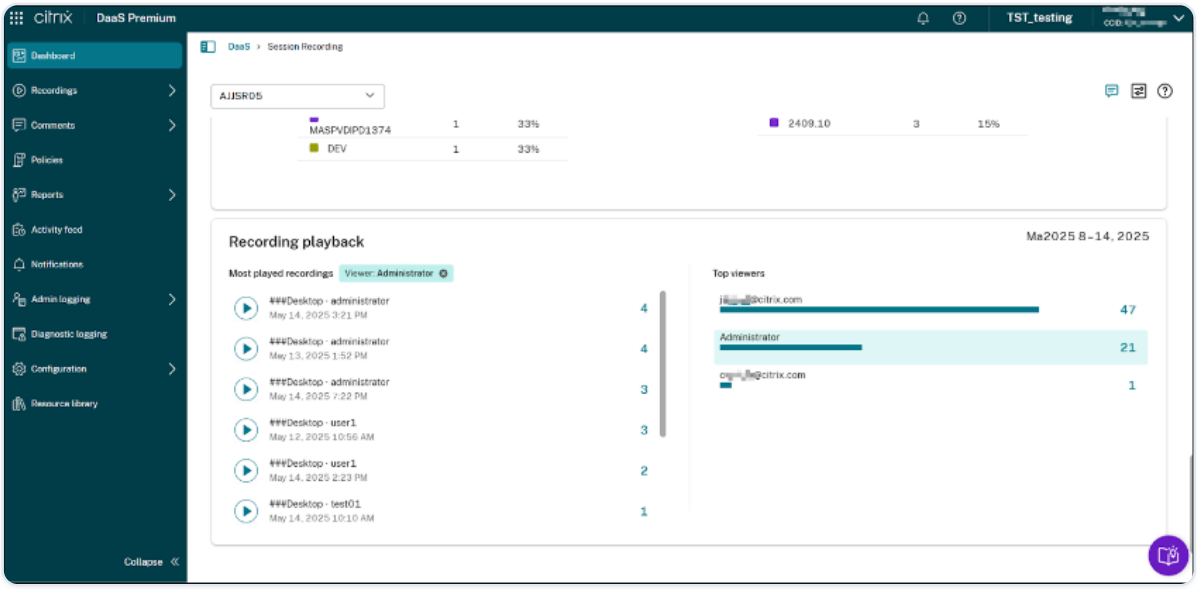
- When you hover the mouse over a recording item in the "Most played recordings" view (left side), detailed information about that recording is displayed.



- If you click on a recording item in the "Most played recordings" view, the "Top viewers" view (right side) shows the top 10 users who have played that specific recording.



- Conversely, if you click on a viewer item in the "Top viewers" view, the "Most played recordings" view will update to show the top 10 recordings played by that specific viewer.



AI-powered insights for session recording

Overview

The AI-powered insights feature enhances the value of session recordings by leveraging Multimodal Large Language Models. This capability enables automated analysis of session recordings, providing actionable summaries, key highlights, and statistical insights to support both security auditing and productivity monitoring.

Prerequisites

To enable and use AI-powered insights, ensure the following requirements are met:

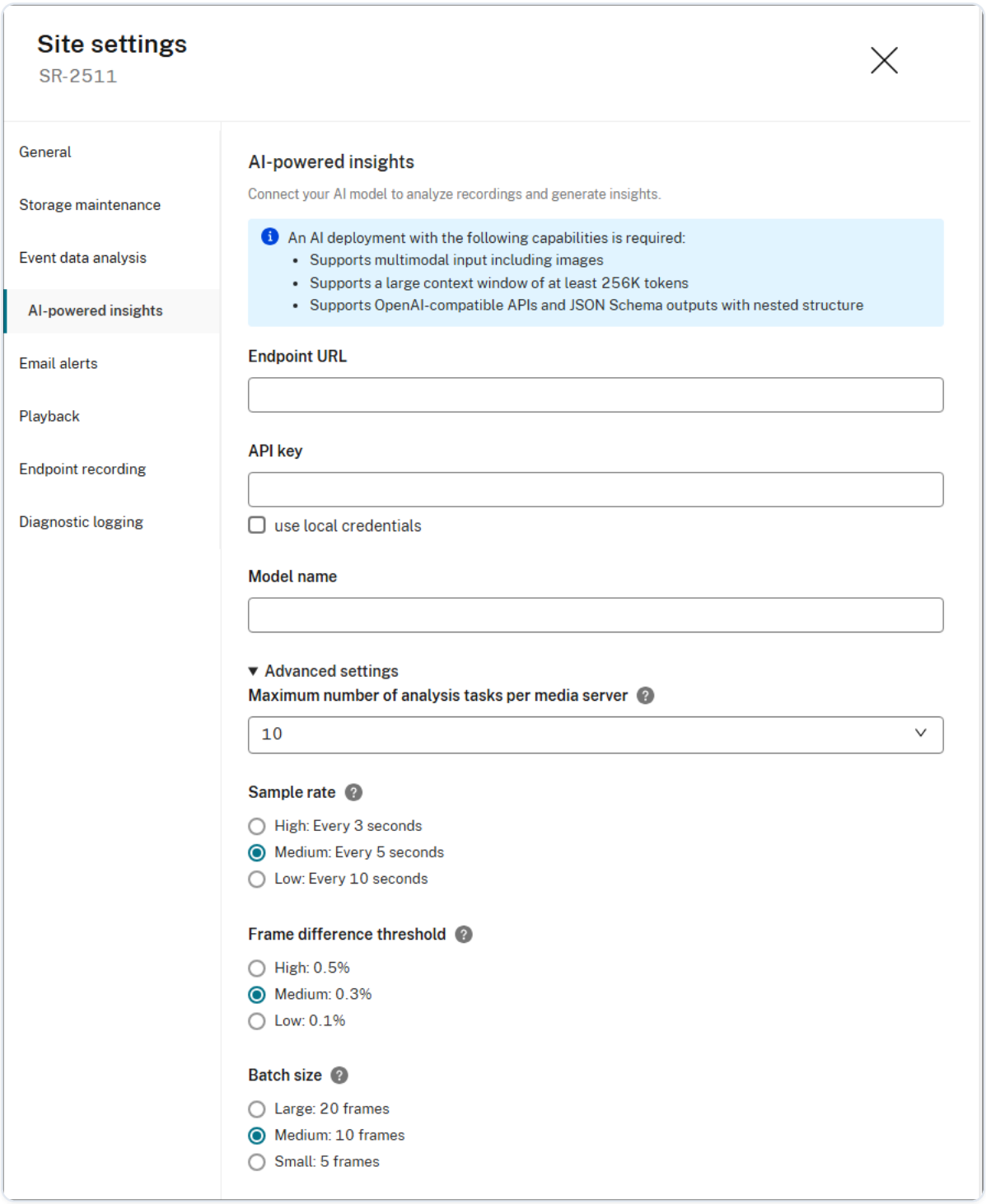
- Citrix Session recording server version 2511 or later is installed.
- Session recording media task service version 2511 or later is installed. Refer to the official setup guide.
- Session recording is properly configured and operational.
- Access to an OpenAI-compatible API endpoint (e.g., Azure OpenAI) is available for AI analysis.

Get Started

Follow below steps to configure and use AI-powered insights:

Configure AI-Powered Insights in Site Settings

1. Open the **Session Recording Console** and navigate to **Site management**.
2. Select the target site to configure.
3. In the **Site Settings** panel, locate the **AI-powered insights** section.
4. Provide the following parameters:
    - **Endpoint URL**: The API endpoint of your AI model (e.g., https://example.azure.com/openai/v1/).
    - **API Key**: The authentication key for your AI service.



Note:

If you want to use Google Gemini series model from Vertex AI, refer to the following guidance:

- The endpoint URL, e.g., “https://aiplatform.googleapis.com”.

- Model name, e.g., “gemini-2.5-flash”.
- Check the “use local credentials” checkbox and leave the API key as empty.
- Go to the machine where you installed the Session Recording media task service and modify the registry:
  - Change the value of HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SRTaskService\SRAIModelAPIT to 3.
  - Add a string value HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SRTaskService\SRAIModelProje set the value to your project id in Vertex AI.
  - Add a string value HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SRTaskService\SRAIModelLocat set the value to your Vertex AI region. E.g., “global” for Global endpoint, other regions e.g. “us-east5” (refer to https://docs.cloud.google.com/vertex-ai/generative-ai/docs/learn/locations#google_model_endpoint_locations)
  - Add an environment variable GOOGLE_APPLICATION_CREDENTIALS at System level, set its value to the path of your Vertex AI private key file.

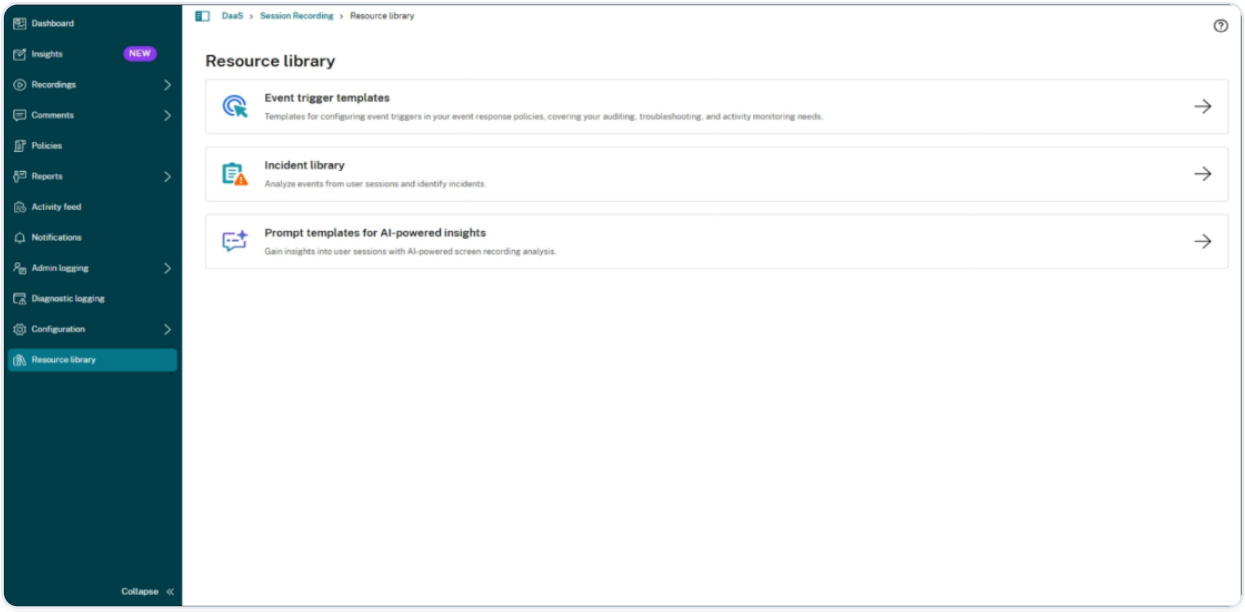
5. (Optional) Configure Advanced Settings:
   - **Maximum number of analysis tasks per media server**: Defines how many AI analysis tasks can run simultaneously on a single media server (e.g., set to `2`).
   - **Sample rate**: Determines how frequently video frames are analyzed.
   - **Frame difference threshold**: Sets the percentage of pixel changes required to consider a frame as "changed."
   - **Batch size**: The number of frames sent to the AI model per batch.
6. Click **Apply changes** to save the configuration.

Note:

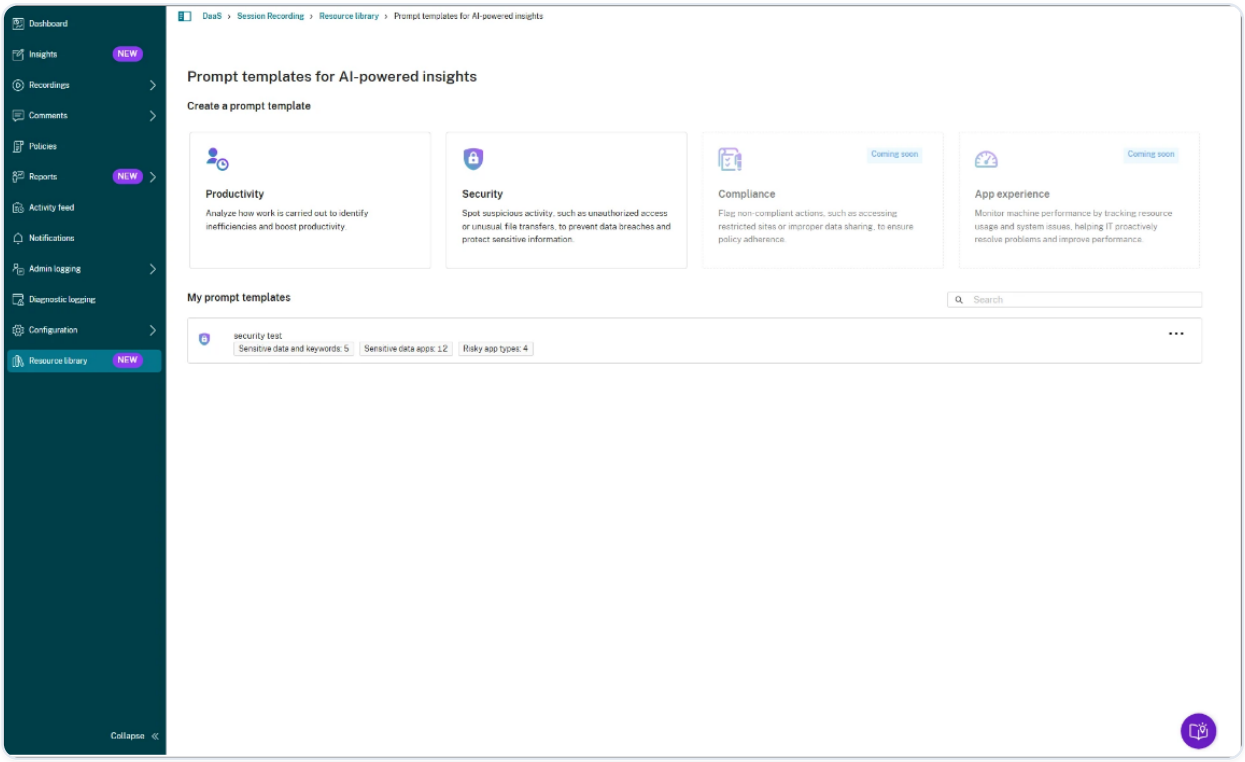
Session Recording will not collect your data that is sent to AI models.

Configure Prompt Templates

1. Go to the **Resource library**.



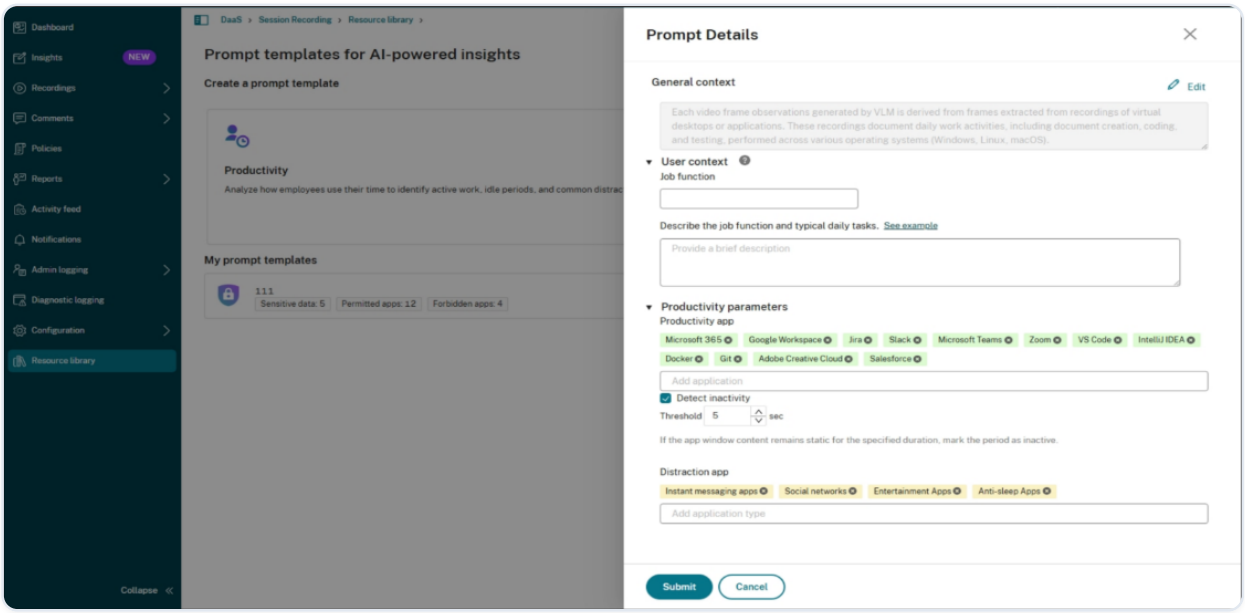
2. Under **Prompt templates for AI-powered insights**, define or customize prompt templates to guide AI analysis.
3. Templates can be tailored for different goals (e.g., Productivity, Security).



Productivity Prompt Template

When creating or editing a productivity prompt template, configure:

- **General context:** Explains the overall purpose of the template.
- User context
  - **Job function:** Enter the user's role (e.g., Accountant, Software Engineer).
  - **Describe the role and typical daily tasks:** Provide a short description of the responsibilities (e.g., Responsible for financial reconciliation, preparing reports, and reviewing compliance with accounting standards).
- Productivity parameters
  - **Productivity apps:** List applications considered productive for this role.
  - **Detect inactivity:** Enable and set a threshold (in seconds).
  - **Distraction Apps:** Define app types considered non-productive (e.g., Instant messaging apps , Social networks).

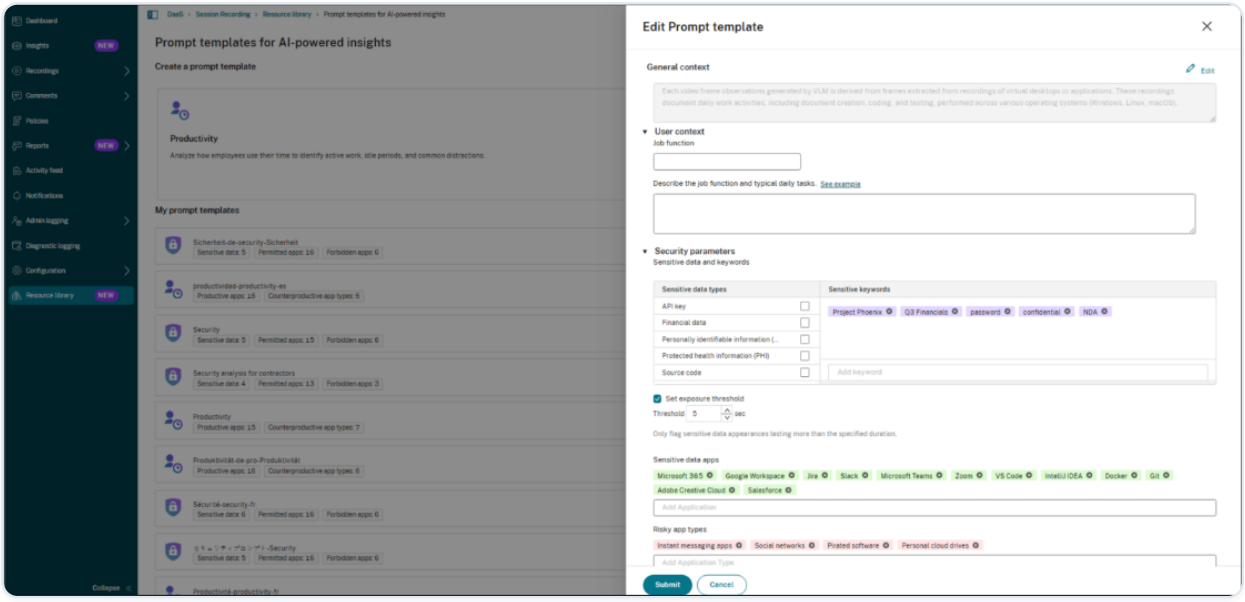


Security prompt template

When creating or editing a security prompt template, configure:

- **General context:** Explains the overall purpose of the template.
- User context
  - **Job function:** Enter the user's role.
  - **Describe the role and typical daily tasks:** Provide a short description of the responsibilities.
- Security parameters

- **Sensitive datatypes:** Categories beyond keywords (e.g., Source code, Financial data).
- **Sensitive Keywords:** Define keywords indicating sensitive data (e.g., **password**, **credit card**).
- **Set exposure threshold:** Minimum duration (in seconds) sensitive data must remain visible on screen before being flagged.
- **Sensitive data apps:** Apps where sensitive data is likely to appear (e.g., Microsoft Excel, Dynamics 365).
- **Risky app types:** High-risk categories (e.g., Social networks, Personal cloud drives).



Security Templates and Sensitive Data Definitions

Session Recording utilizes pre-defined security templates to identify sensitive information within recorded sessions. The AI model analyzes screen content based on the following standard categories.

Pre-defined Sensitive Data Categories

The system detects five primary categories of sensitive data by default:

1. **PII (Personally Identifiable Information)**

   Detects personal data points that can identify an individual, including:

   - **Identity & Demographics**: Name, ID Number, Social Security Number (SSN), Passport Number, Driver's License Number, Vehicle Class, Gender, Religion, Race, Nationality.
   - **Contact Information**: Phone Number, Email Address, Home Address, Zip Code.
   - **Dates**: Date of Birth, Date of Issue, Date of Expiry.

- **Employment**: Job Title, Company, Business Contact Information.

2. **Financial Information**

   Detects banking and payment-related data, including:

   - **Card Data**: Card Number, Cardholder Name, Expiry Date, CVV Code.
   - **Account Details**: Account Number, Tax ID, Payee Information.
   - **Transaction Details:** Transaction Records, Amounts, Financial Amounts, Payment Date, Invoice Number.
   - **Document Context**: Document Title, Signature Area, Company Information.

3. **PHI (Protected Health Information)**

   Detects medical and health-related records, including:

   - **Patient Identity**: Patient Name, Medical Record Number, Insured Person's Name, Insurance Policy Number.
   - **Medical Details**: Diagnosis Results, Medication Name, Dosage Information.
   - **Documentation**: Document Title, Doctor's Signature.

4. **Source Code**

   Detects programming code snippets, scripts, and syntax typical of software development.

5. **API Keys**

   Detects strings and patterns resembling Application Programming Interface authentication keys and tokens.

6. **IP (Internet Protocol address)**

   Detects strings and patterns resembling IPs in both IPv4 and IPv6 formats, The specific IP string will be shown in the reports.

> **Note on AI Contextual Analysis:**

> In addition to keyword matching, the AI model leverages contextual information to improve judgment accuracy. This helps distinguish between sensitive data and non-sensitive text that may share similar formats.

Customizing Definitions

If your organization requires specific adjustments to these definitions (e.g., specific internal terminology or excluding certain fields), you can provide custom detection rules in an additional context field.

Deep inspection

Deep inspection extends the security analysis with AI-investigated behavior indicators, in addition to the keyword and pattern-based sensitive data detection described above.

- **Custom behavior indicators**: Describe the behaviors to detect in plain language, and the AI generates detection guides that you can review and refine.
- **Incident reporting**: Matches appear as incidents in the Deep inspection results section of the security analysis report, each with a clickable timestamp for playback.
- **Confidence tagging**: Incidents that are difficult to distinguish from normal activity are tagged Low confidence for manual review.

Deep inspection requires an AI model that supports reasoning.

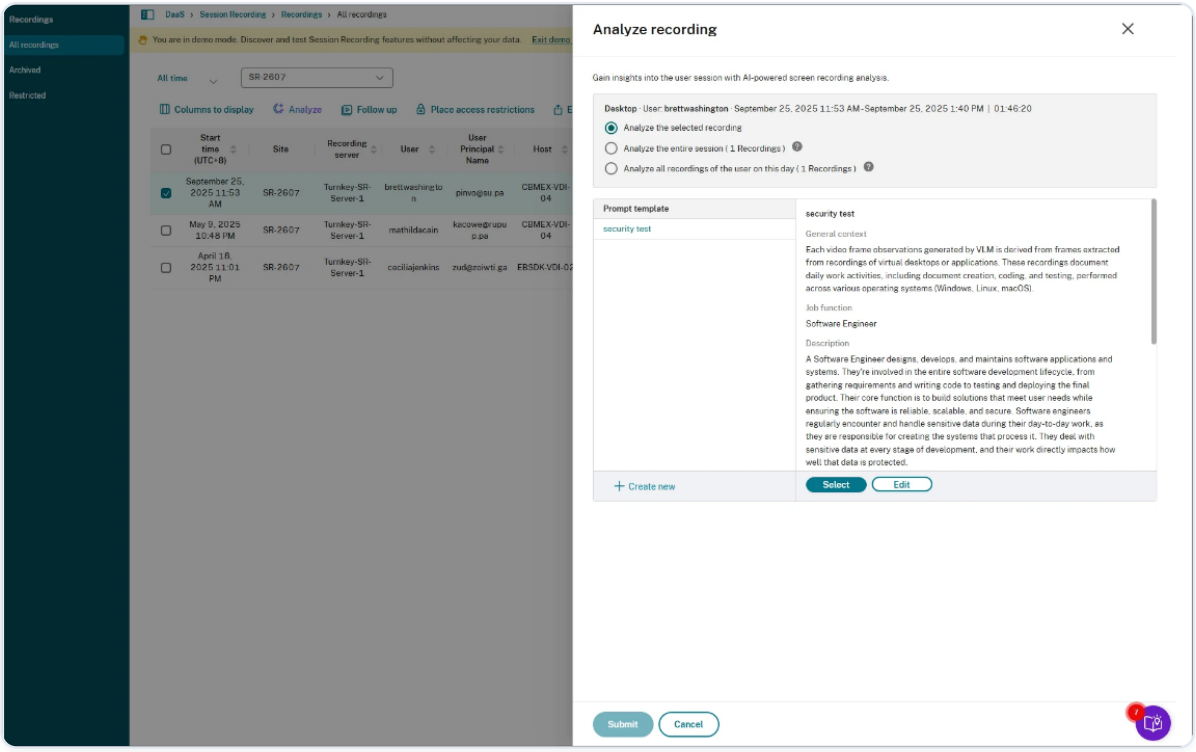
Select Recordings for Analysis

1. Navigate to **Recordings** in the **Session Recording Console**.
2. Use filters or search to locate the session(s) for analysis.
3. Select one or more video recordings, then click **Analyze**.
4. In the dialog:
    - Select a prompt template from the **Resource Library** or **Create new**.
    - Choose the analysis scope based on the session type:
        - **Analyze the selected recording** – analyzes only the selected recording file.
        - **Analyze the entire session** — for rollover sessions (sessions that span multiple recording files).
        - **Analyze all recordings of the user on this day** — for a daily insight summary covering all recordings of the selected user on that day.

> **Note:**

> The Analyze the entire session and Analyze all recordings of the user on this day options require Session Recording media task service version 2603 or later.

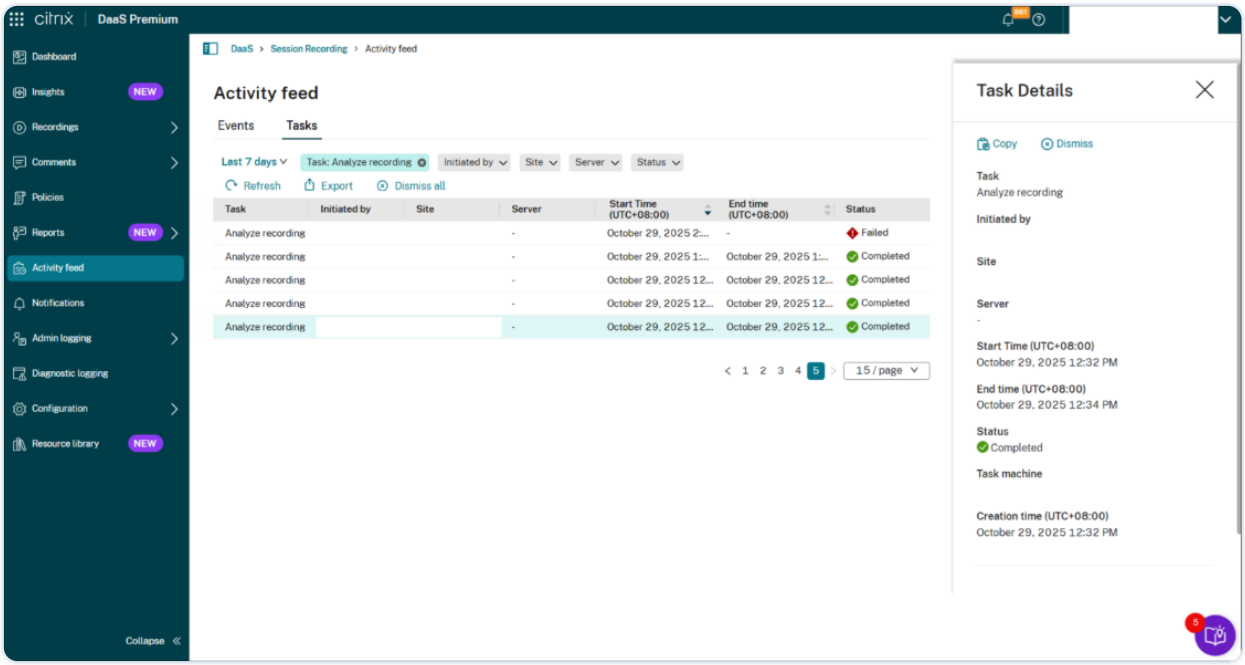
- (Optional) Provide additional context before submitting.



- Click **Submit** to start the analysis task.

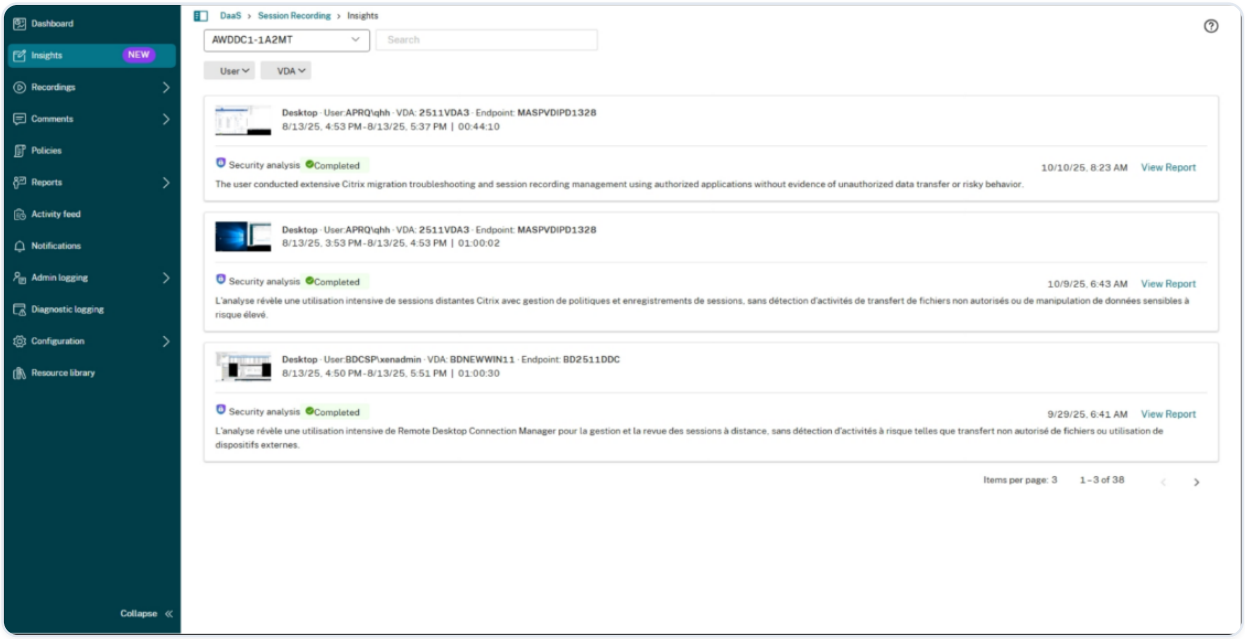
Monitor Task Progress

1. Go to **Activity feed > Tasks** to track analysis status (Pending, In Progress, Completed, Failed).
2. Each task includes recording file details.



Review AI-Powered Insights

1. Navigate to the **Insights** page to view completed analyses.
2. Use filters (Site, User, VDA) and search bar for quick access.
3. Each session card displays:
    - AI-generated summary.
    - Analysis type and status.
    - A **View Report** link for detailed insights.

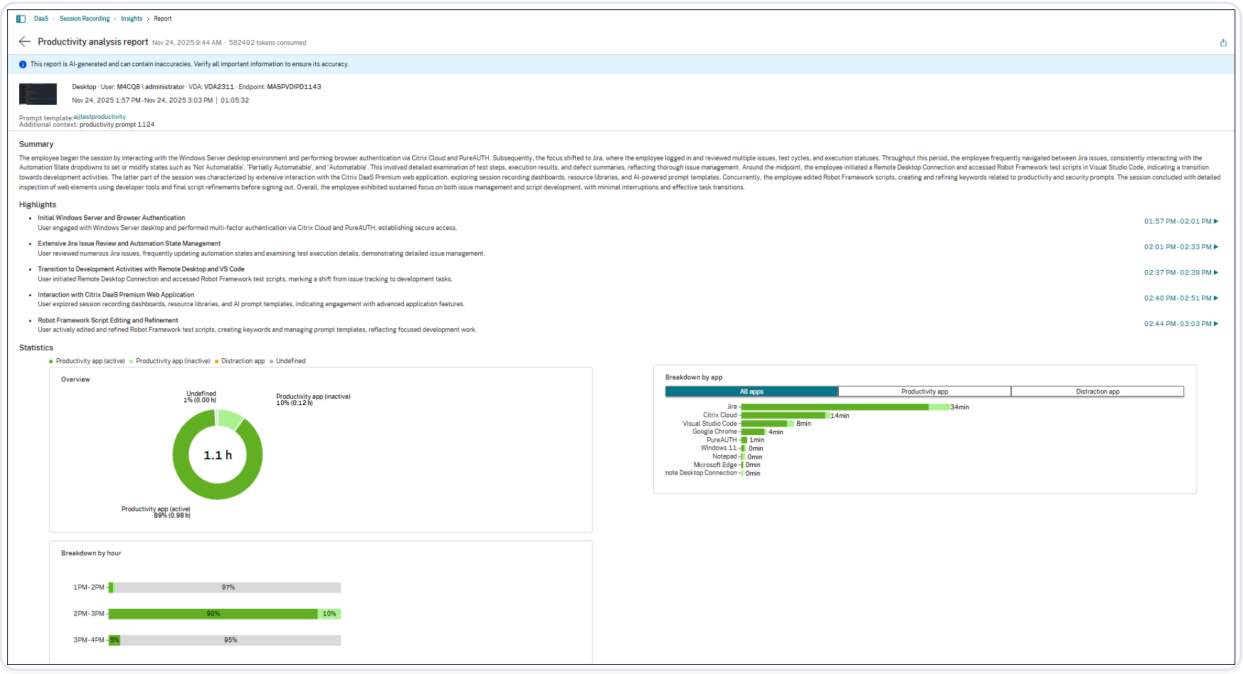


Detailed Reports

Productivity Analysis Report

Includes:

- **Summary**: Proportion of time spent on productive vs. non-productive activities.
- **Highlights**: Key time blocks, with clickable timestamps.
- **Statistics**:
  - **Overview Chart**: Breakdown of active work, idle time, and distractions.
    - **Breakdown by App**: Time spent in productivity app vs. distraction app.
    - **Hourly Pattern**: Shows productivity trends throughout the day.

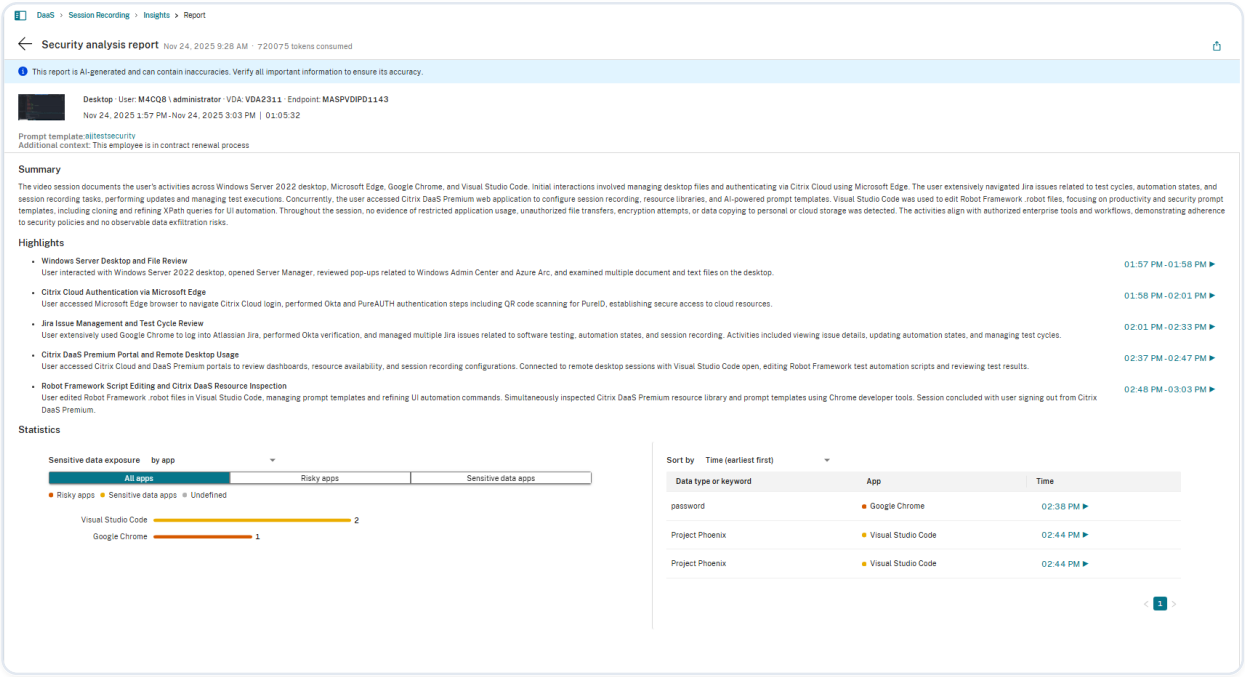


Security Analysis Report

Includes:

- **Summary**: Overview of session's security posture, highlighting risky behaviors and sensitive data exposure.
- **Highlights**: Key security events with clickable timestamps.
- **Statistics**:
  - **Sensitive Data Exposure**:

    - **by data types or keyword:** Shows which sensitive terms appeared most often.
    - **by app:** Highlights apps where sensitive data appeared.
- **Timeline View**: Lists sensitive keywords with timestamps and associated apps.



Limitations

- **Virtual App Support**: Insights may be limited for virtual application sessions.
- **Short Sessions**:
    - Sessions shorter than 15 minutes generate only a basic summary.
    - Sessions shorter than 30 minutes omit statistical charts.

Legal and Privacy Disclaimer

The AI Insights in Session Recording feature (“AI Insights”) is provided “As-Is”, with no warranties or representations, whether express or implied. Its provided prompt templates as well as the outputs, reports and/or information that may be generated from utilizing this feature are not intended to provide legal, security, regulatory and/or technical advice.

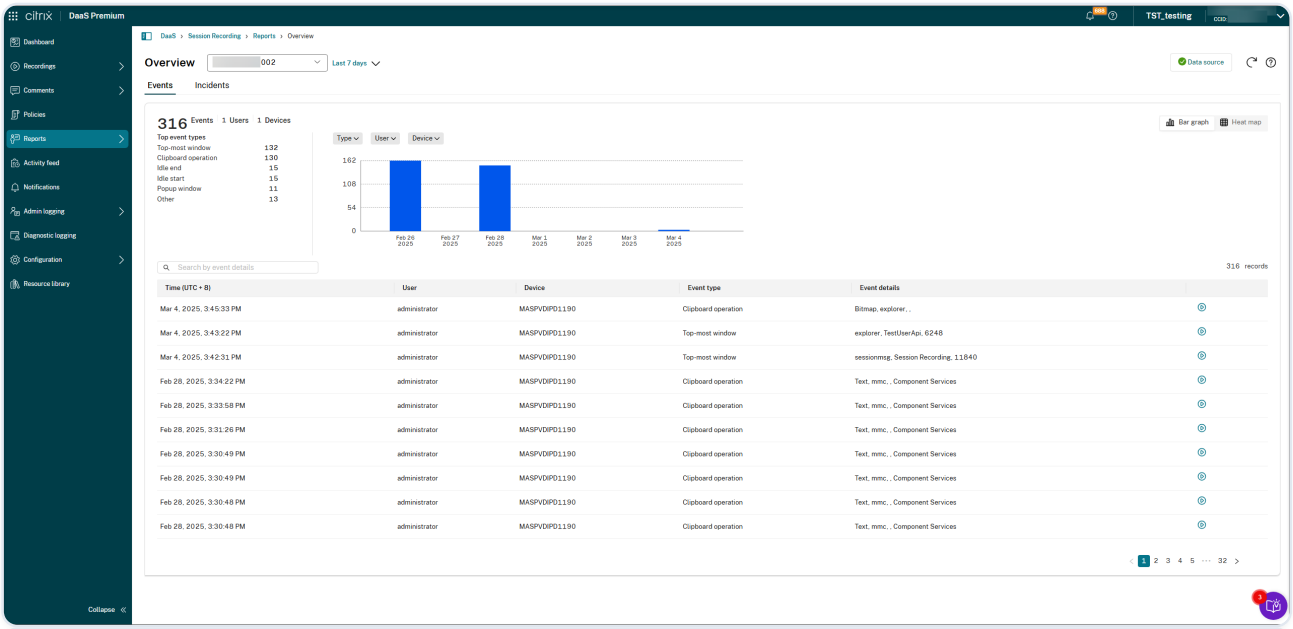
Customer is solely responsible for the legal and regulatory compliance of processing any personal data or sensitive information including but not limited to balancing your internal data classification obligations, global data and/or AI regulatory compliance as well as industry related compliance obligations.

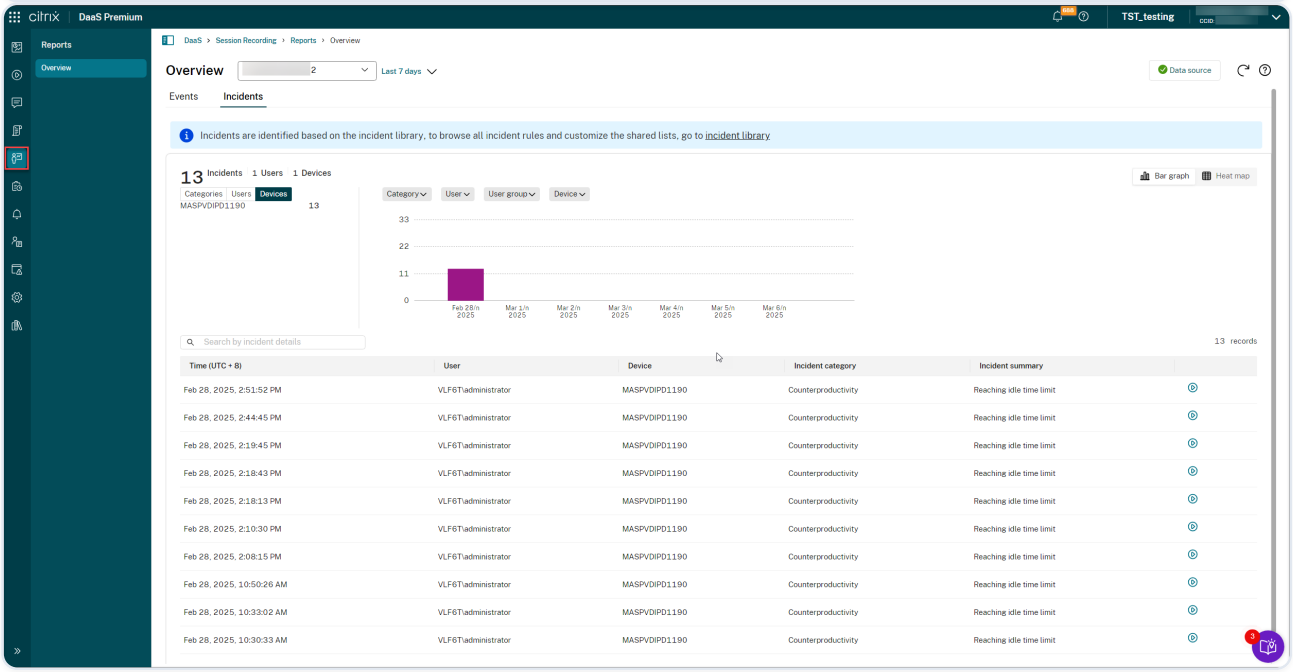
Customers acknowledges and understands that utilizing AI Insights involves transmitting all VDA session data to their configured AI model endpoint. This data may include Personal Data or sensitive and/or confidential information captured during VDA session recordings. All VDA session data generated, as well as the AI Insights output, is considered Customer Content.

Site-level user activity reporting

Based on event detection in recorded sessions, Session Recording empowers you to identify incidents from events. It also displays the event and incident data in the cloud for aggregation and analysis, providing a comprehensive view of user activity across an entire site.

The following screen captures illustrate a site-specific overview of events and incidents.





This site-level reporting feature enables you to:

- Quickly filter incidents from events by category.
- Identify abnormal activity with greater efficiency.
- Gain a broader understanding of user activity patterns across your site.

Prerequisites

- The availability of the event data in the cloud is solely determined by the active event detection policy, and is independent of settings or Session Recording server versions. Therefore, if the active policy dictates event data, it will always be displayed in the cloud.
- The availability of the incident data in the cloud is governed by three factors: the active event detection policy, site-specific event data analysis settings, and incident library settings that identify incidents from events. Separately, Session Recording 2503 or later is required for incident identification and display in the cloud.

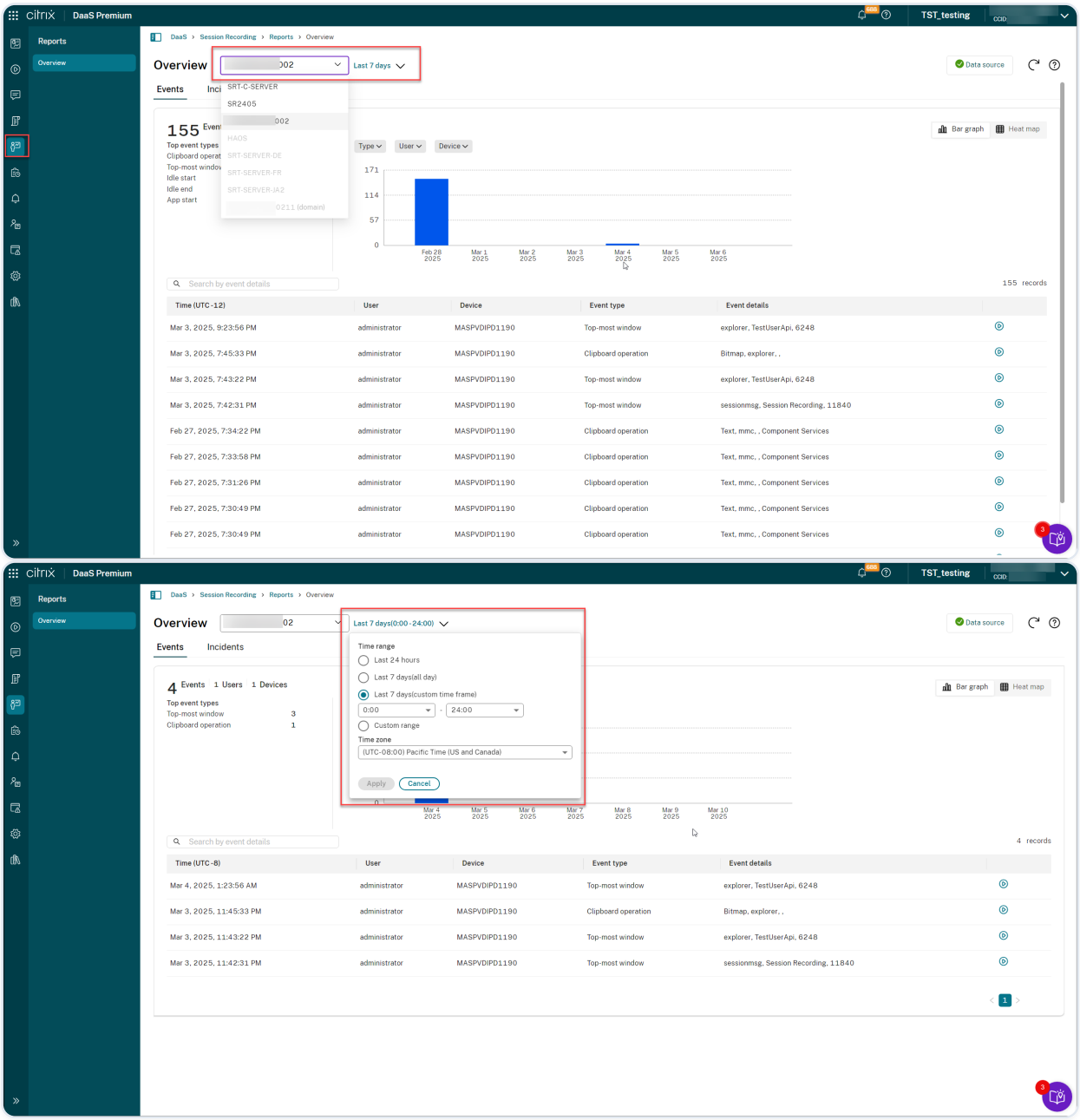
For information about the event detection policy settings, see Configure event detection policies.

For information about the event data analysis and incident library settings, see Configure site-level user activity reporting later in this article.

View site-specific user activity reports

Site-level user activity reporting delivers a comprehensive perspective of events and incidents across an entire site, enabling enhanced monitoring and analysis. To view site-specific user activity reports, proceed with the following steps:

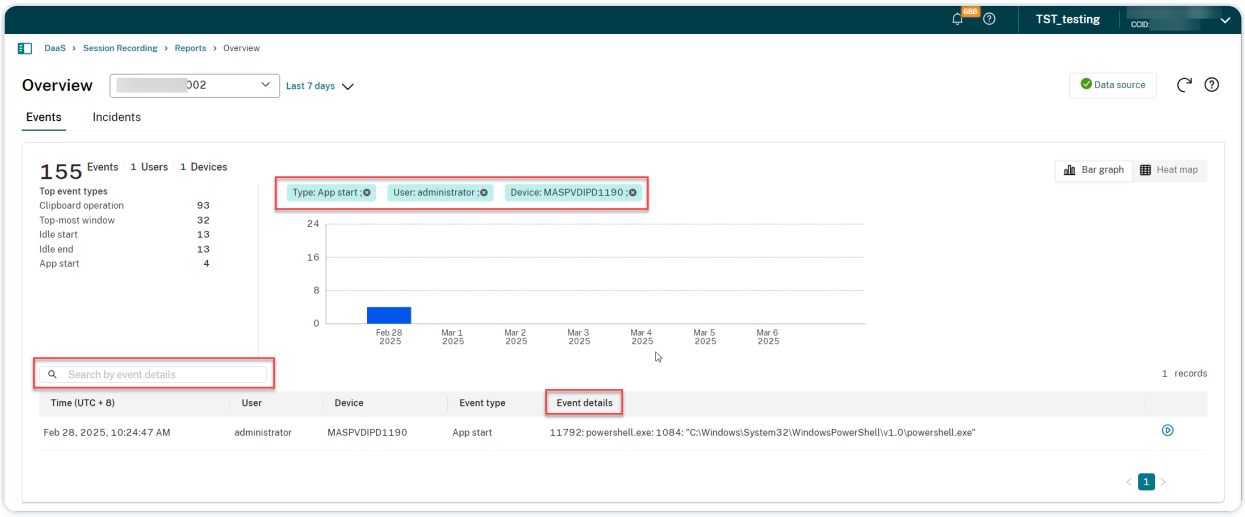
1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.
3. In the DaaS tile, scroll down in the left navigation pane and select **Session Recording**.
4. In the Session Recording service view, select **Reports** from the left navigation.
5. Select a target site and specify the time range and time zone.



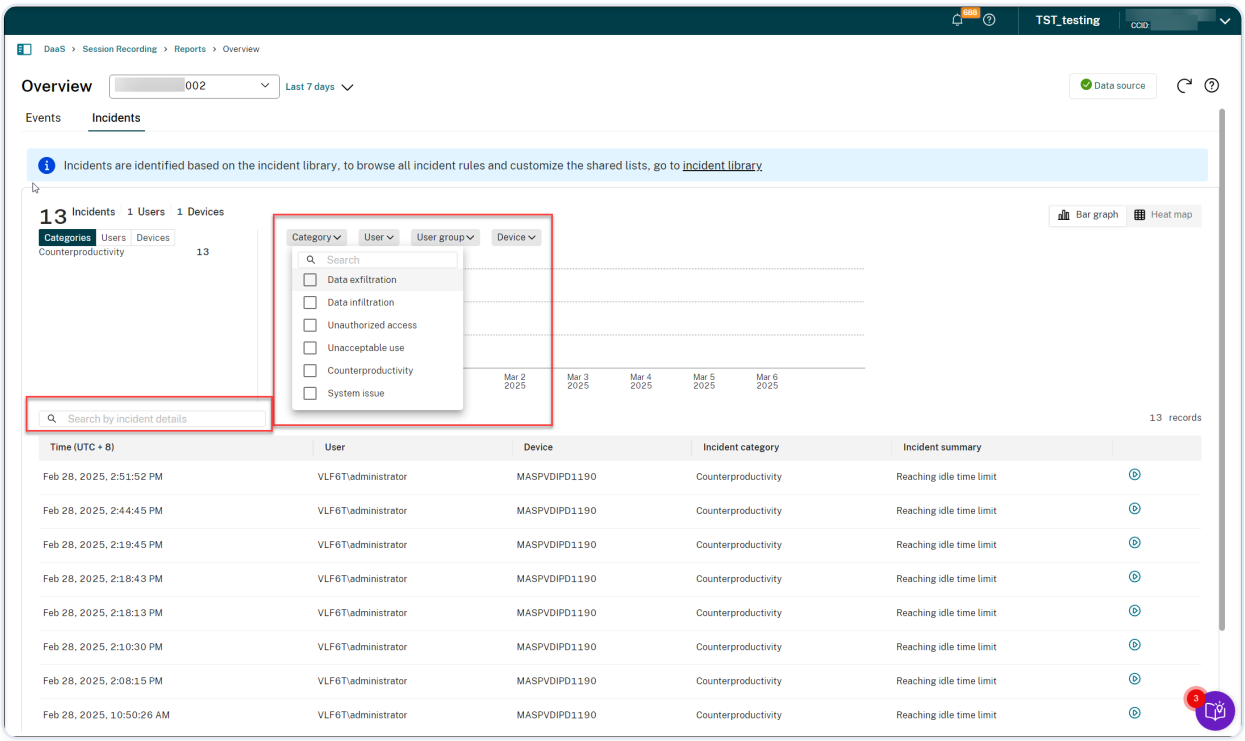
6. Use the **Events** and **Incidents** tabs to review detected events within recorded sessions and incidents identified from those events.

   You can filter events and incidents for detailed analysis.

   To find specific events on the **Events** tab, you can filter by event type, session user, and client device. You can also use the search box to find events by keyword. Filters are combined using 'AND'.

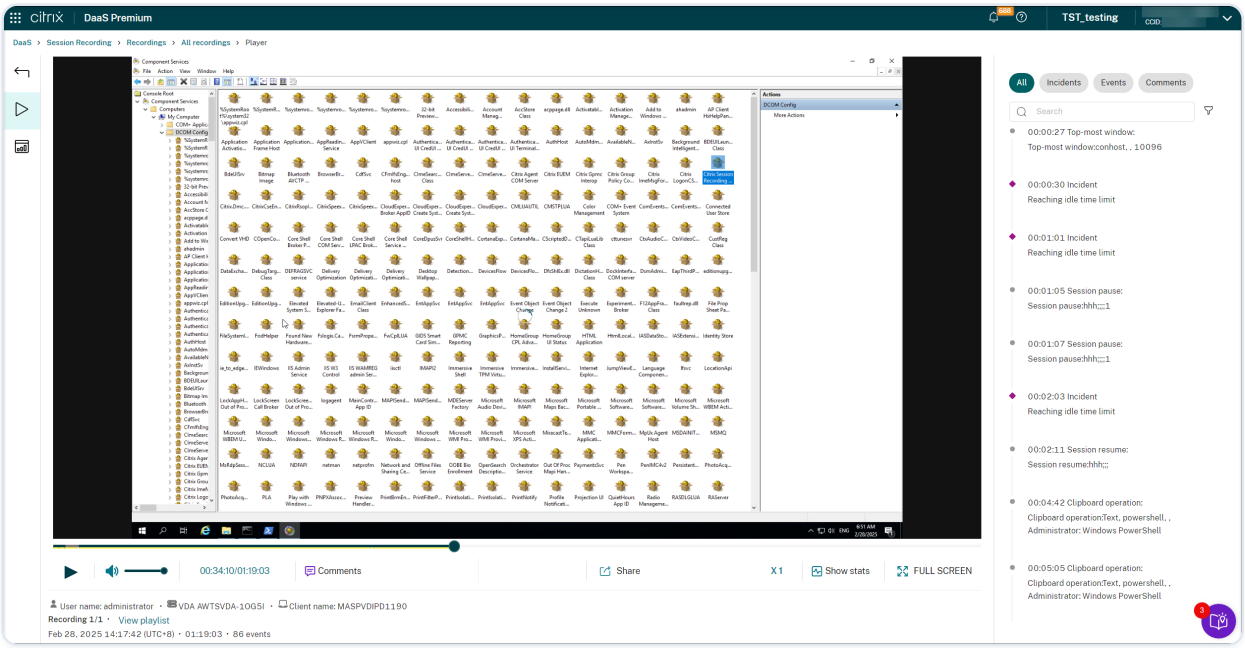


To find specific incidents on the **Incidents** tab, you can filter by category, session user, user group, and client device. You can also use the search box to find events by keyword. Filters are combined using 'AND'.



Both events and incidents are tagged within recordings, allowing for easy search and playback review. Clicking the play button takes you to the recording playback page, where you can view the events, incidents, and comments for the recorded session.

For example, see the following screen capture:



Configure site-level user activity reporting

To enable the presentation of event and incident data in the cloud for enhanced user activity monitoring and analysis, follow the configuration steps outlined below.

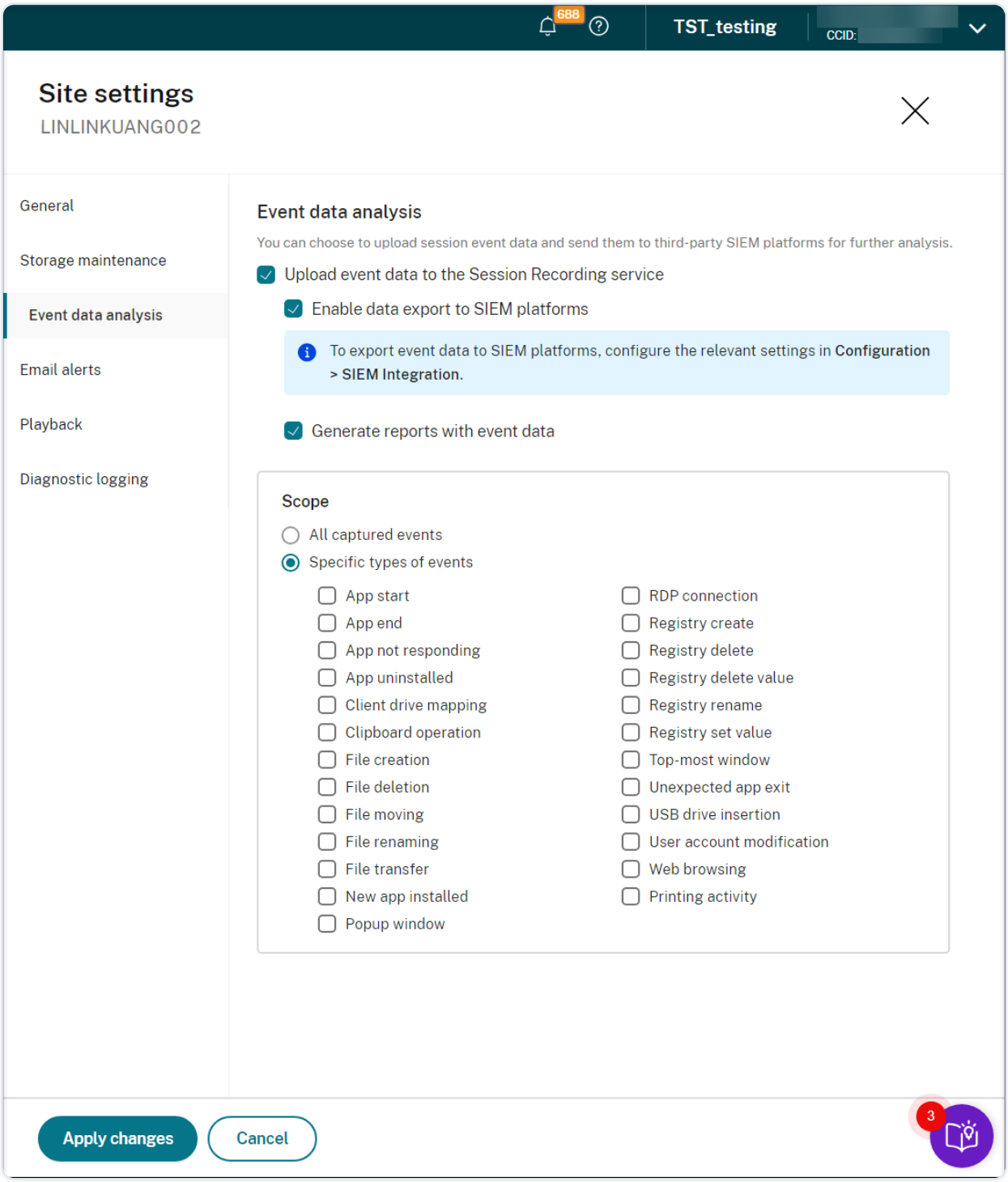
Step 1: Enable the presentation of event data in the cloud

Configure and activate an event detection policy. Verify that the policy includes all event types necessary for comprehensive data capture. Event data captured by the policy will be displayed in the cloud for user activity monitoring and analysis. To also enable cloud presentation of incident data, continue with Step 2 below.

For information about the event detection policy settings, see Configure event detection policies.

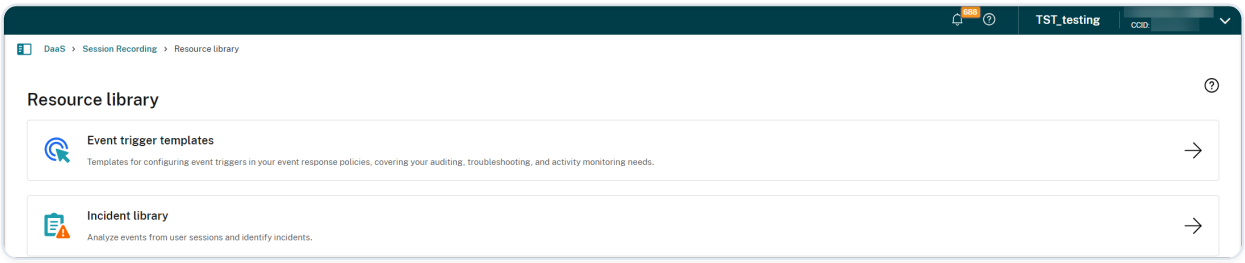
Step 2: Enable the presentation of incident data in the cloud

1. Select **Configuration > Server Management** from the left navigation of the Session Recording service.
2. Click **Settings** for the target site.
3. On the **Event data analysis** page, select **Upload event data to the Session Recording service** and **Generate reports with event data**. Specify whether to upload all captured events or select specific types of events.

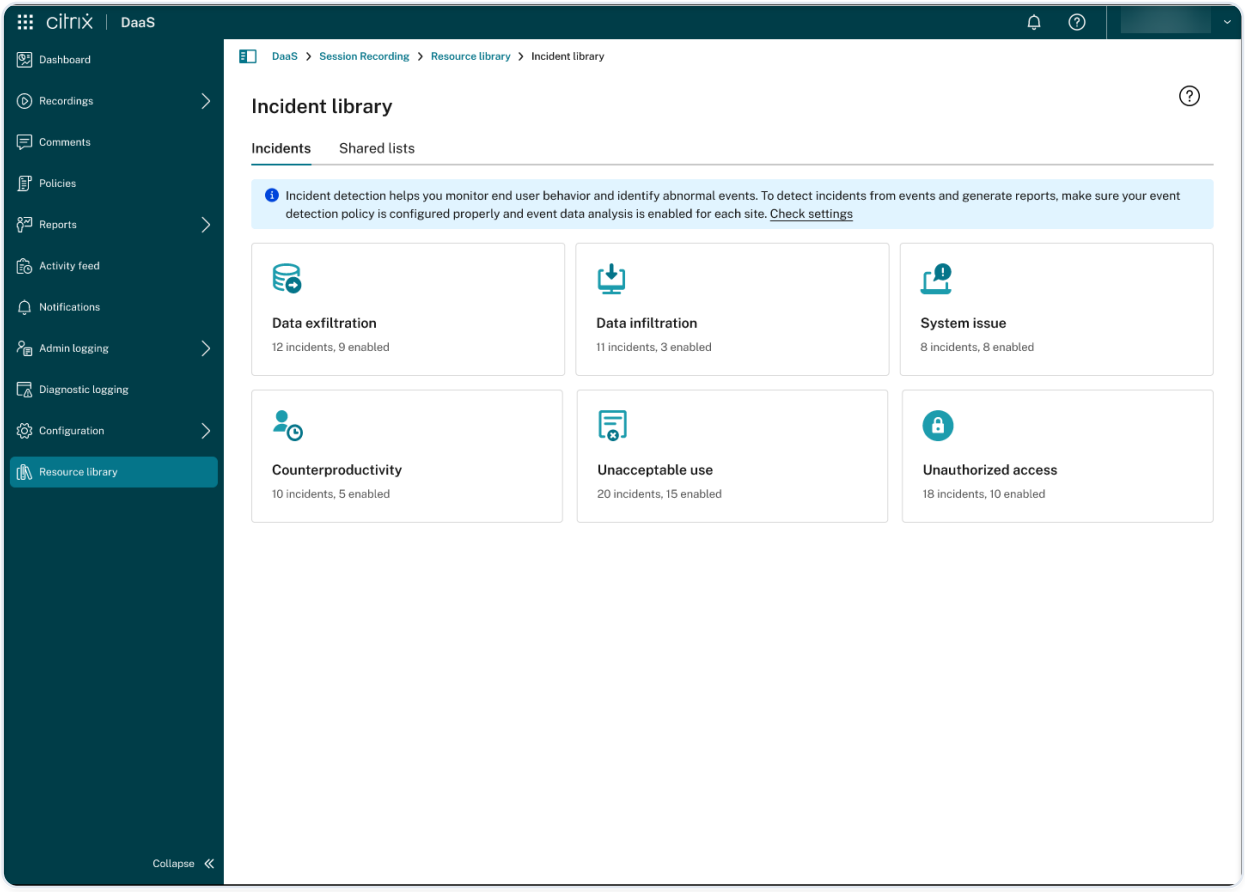


4. Access the incident library settings and configure the incident identification rules to analyze the uploaded event data and identify incidents from them.

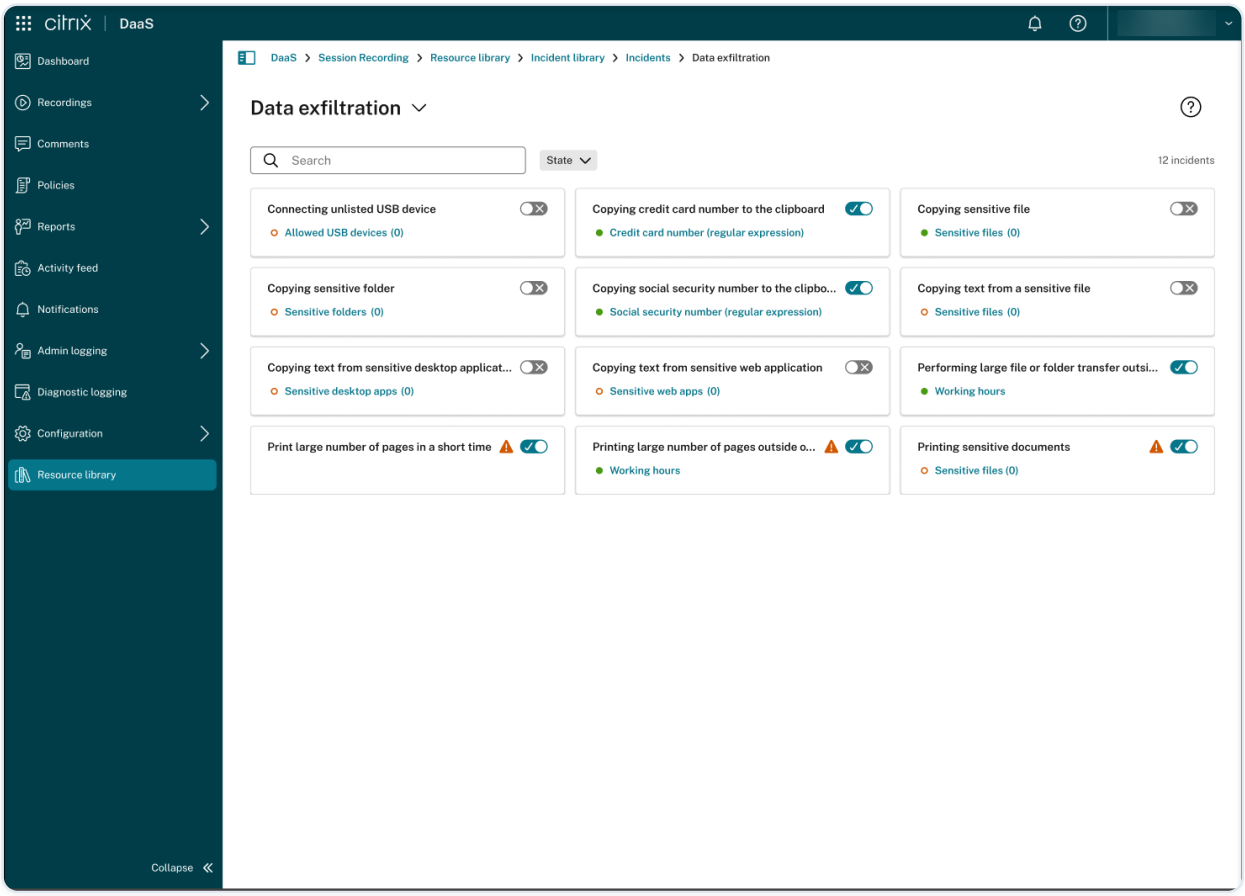
   To access the incident library settings, click **Resource Library** from the left navigation pane of the Session Recording service page and then click **Incident library**.



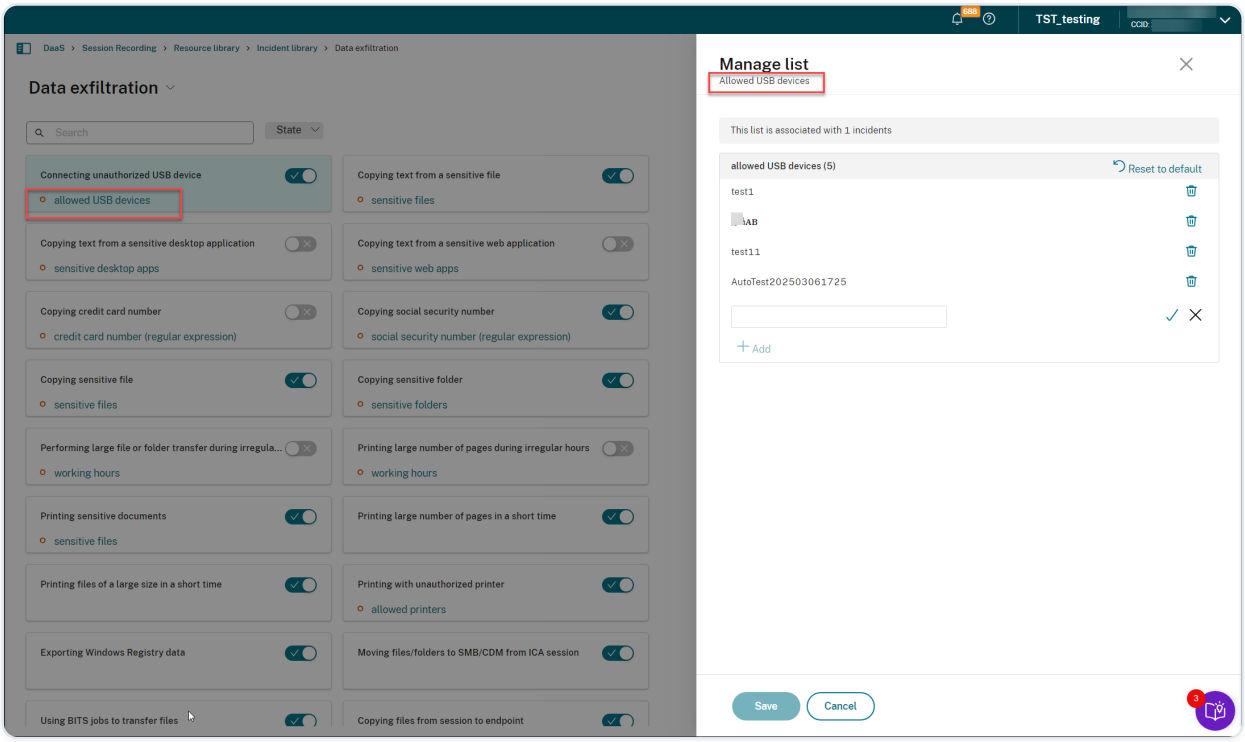
The **Incident library** page contains two tabs, **Incidents** and **Shared lists**.



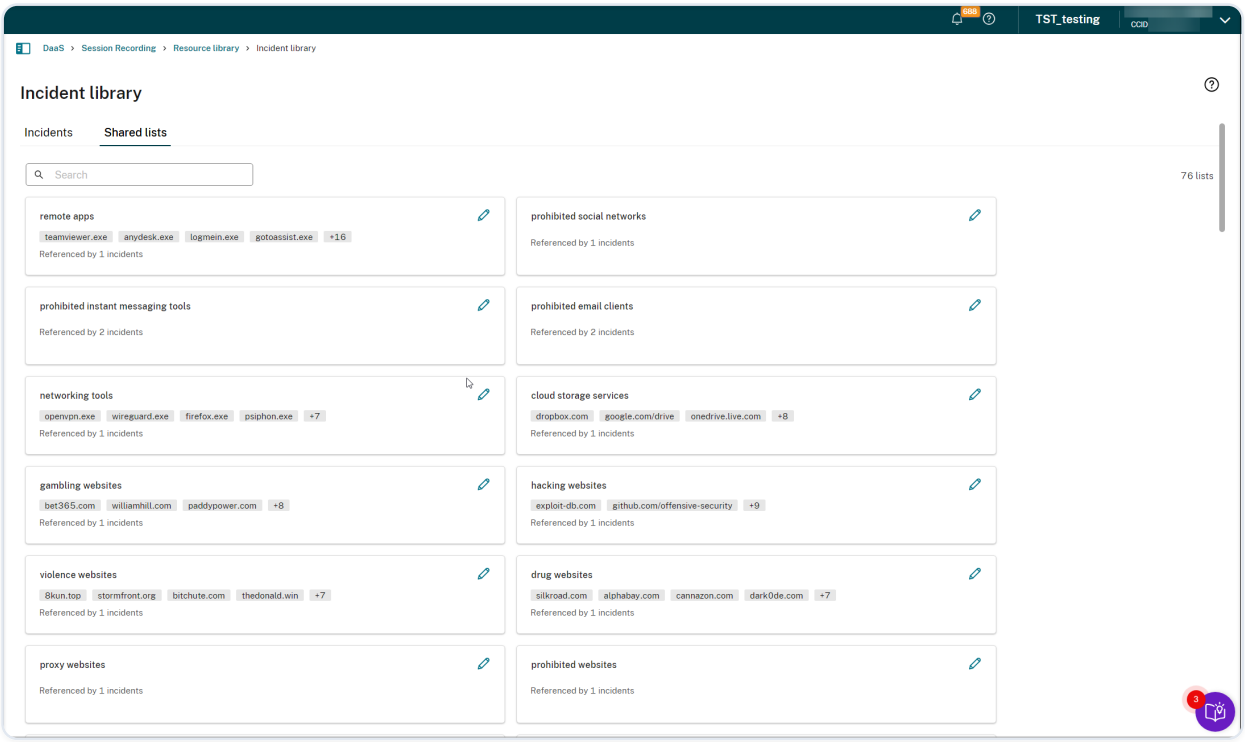
The **Incidents** tab displays categories of incidents that can be reported, each containing pre-defined incidents related to that category. For example, to view all pre-defined incidents related to the data exfiltration category that can be reported, click **Data exfiltration**.



To enable or disable reporting for a pre-defined incident related to a category, toggle the switch next to it. Some of the pre-defined incidents have a filter to define identification criteria. For example, the **allowed USB devices** filter lets you define an allow list. When a USB device not on this list is connected during a recorded session, an incident is triggered.



You can find a collection of these filters on the **Shared lists** tab.


TST_testing
DaaS › Session Recording › Resource library › Incident library
Incident library
Incidents
Shared lists
Search
76 lists
remote apps
teamviewer.exe anydesk.exe logmein.exe gotoassist.exe +16
Referenced by 1 incidents
prohibited social networks
Referenced by 1 incidents
prohibited instant messaging tools
Referenced by 2 incidents
prohibited email clients
Referenced by 2 incidents
networking tools
openvpn.exe wireguard.exe firefox.exe psiphon.exe +7
Referenced by 1 incidents
cloud storage services
dropbox.com google.com/drive onedrive.live.com +8
Referenced by 1 incidents
gambling websites
bet365.com williamhill.com paddypower.com +8
Referenced by 1 incidents
hacking websites
exploit-db.com github.com/offensive-security +9
Referenced by 1 incidents
violence websites
8kun.top stormfront.org bitchute.com thedonald.win +7
Referenced by 1 incidents
drug websites
silkroad.com alphabay.com cannazon.com dark0de.com +7
Referenced by 1 incidents
proxy websites
Referenced by 1 incidents
prohibited websites
Referenced by 1 incidents

Activity feed

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
- Registry modification

> **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
- Export recording
- Analyze recording

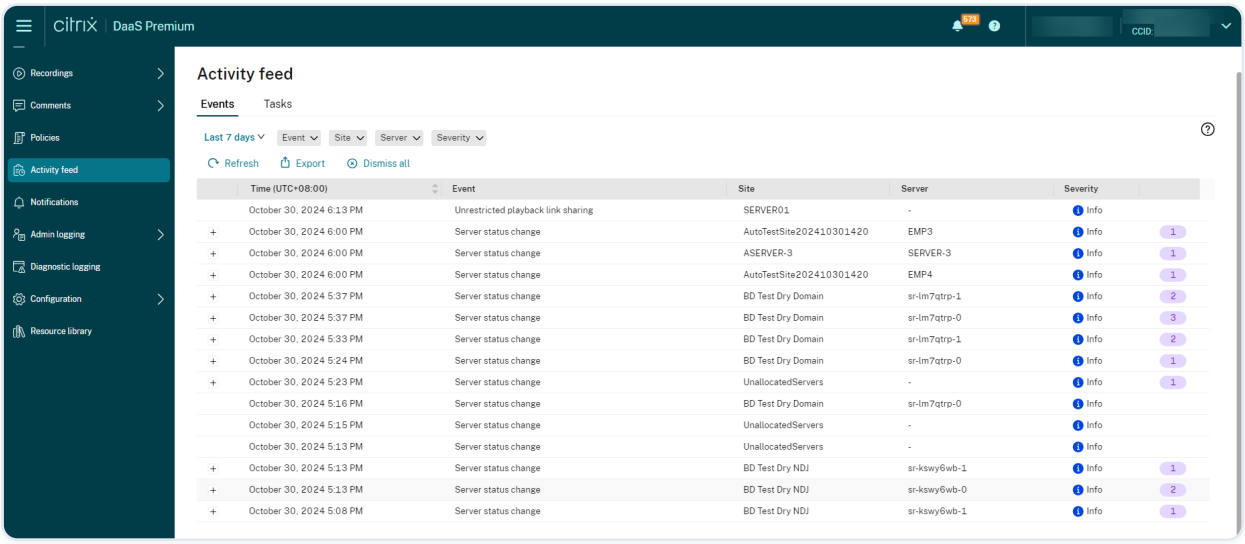
Note:

- 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.

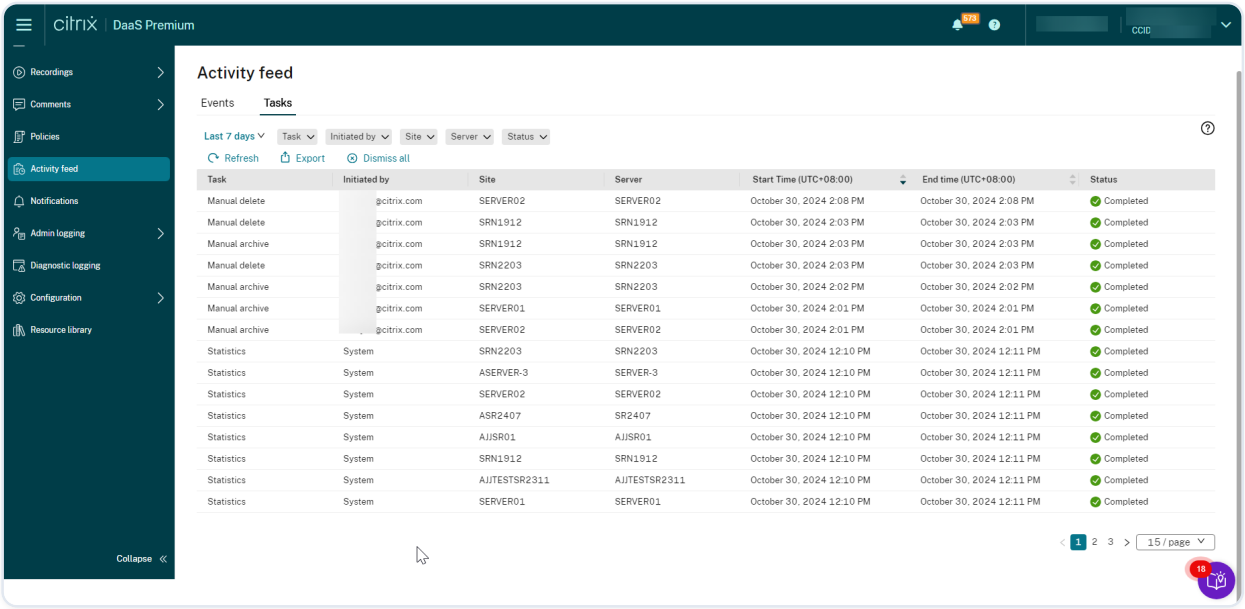
View the activity feed

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.
3. In the DaaS tile, scroll down in the left navigation pane and select **Session Recording**.
4. In the Session Recording service view, select **Activity Feed** from the left navigation.
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



Activity Feed – the **Tasks** tab



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.

TASK	ACTION
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 dismissan individual event or task	Click **Dismiss** on the **Event Details** or **Task Details** page. You are not prompted for confirmation when clicking **Dismiss**.

Notifications

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

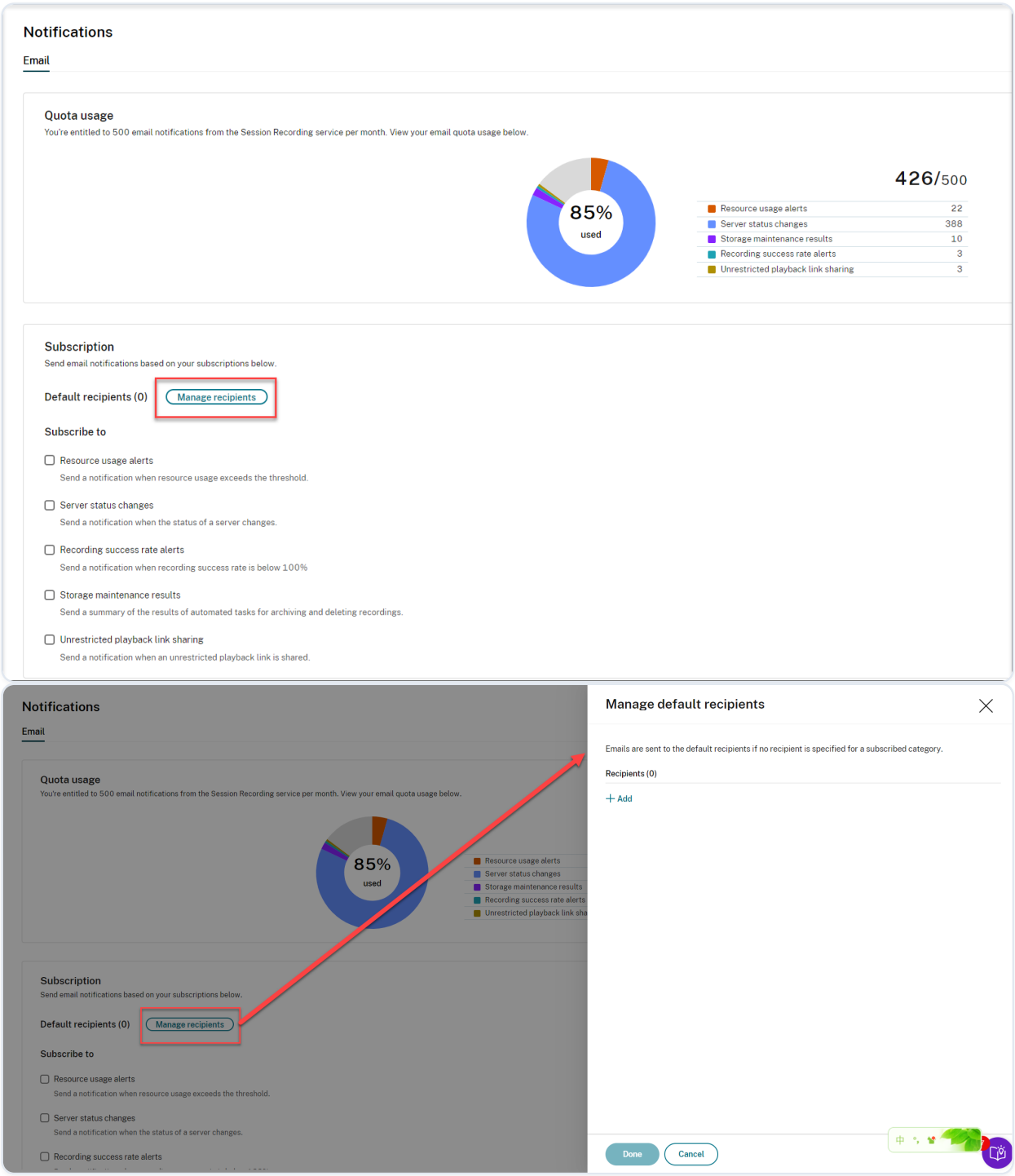
  For more information, see Share recordings as links.

Subscribe to email notifications

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

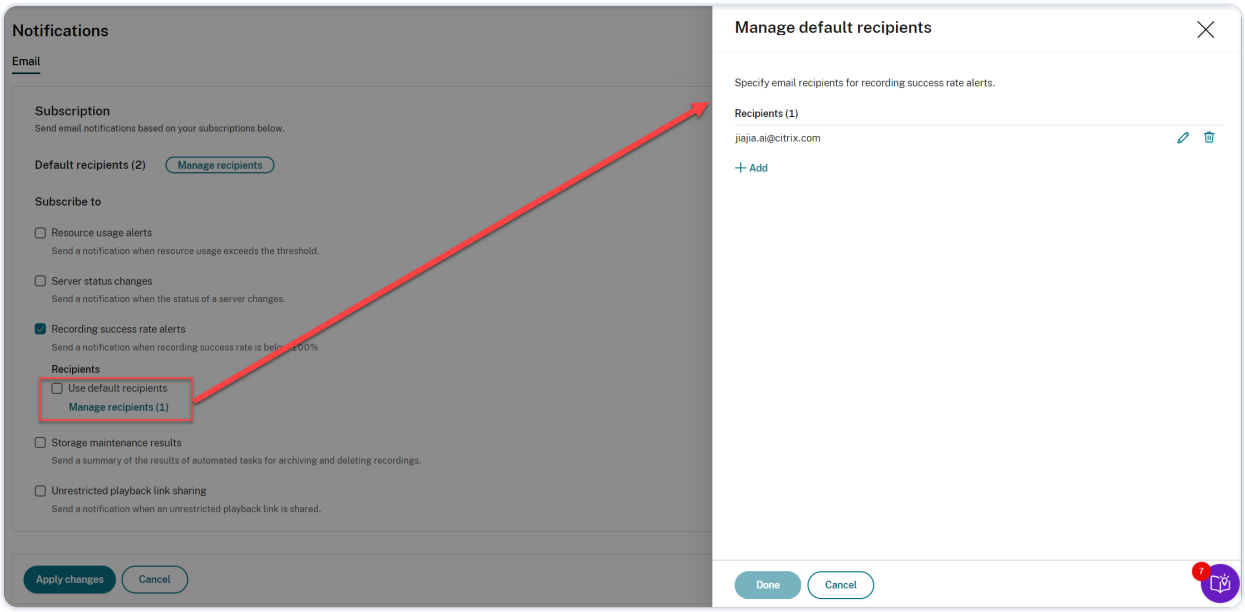
   > **Tip:**
   >
   > You are entitled to 500 email notifications from the Session Recording service every month. After the monthly quota is used up, the Session Recording service stops sending email notifications until the UTC first day of a new month.

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



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.

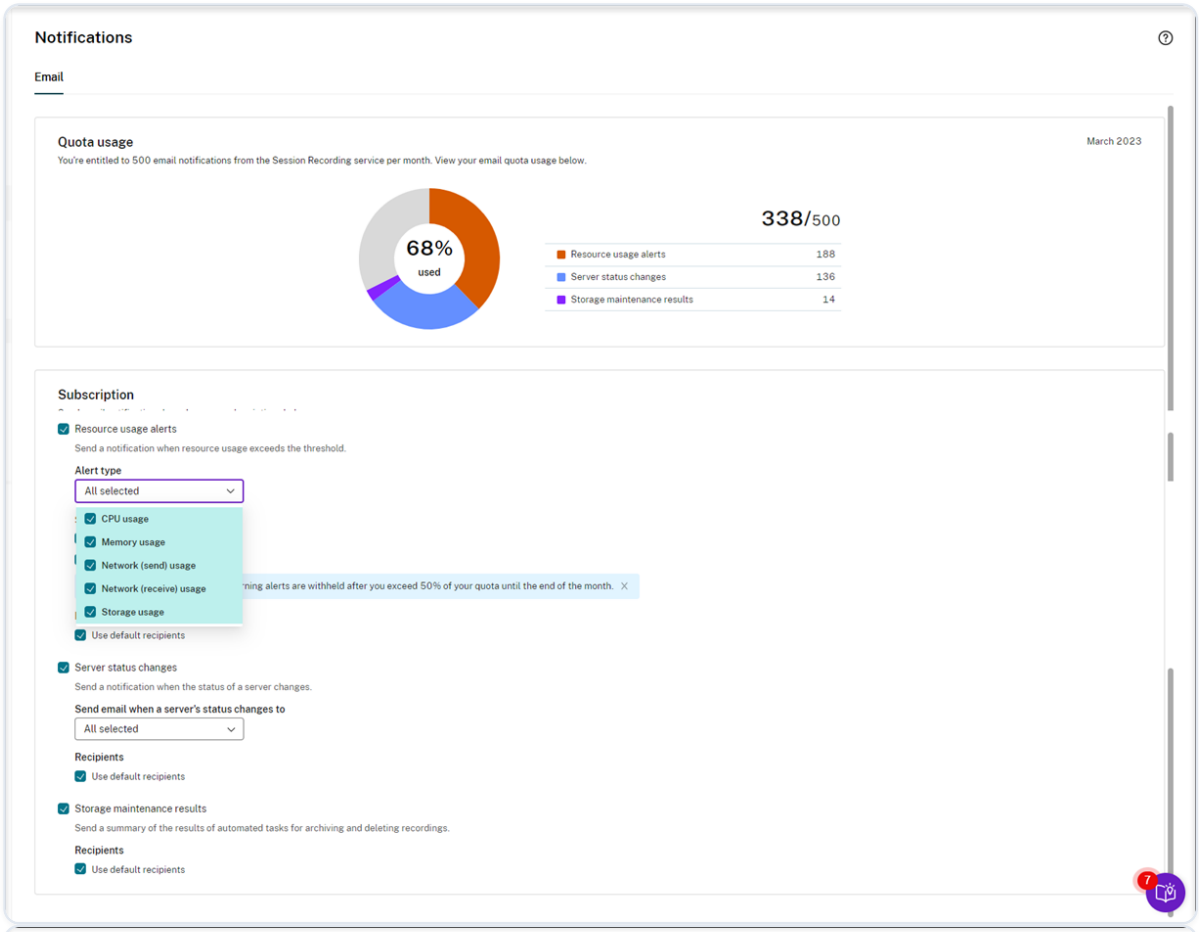


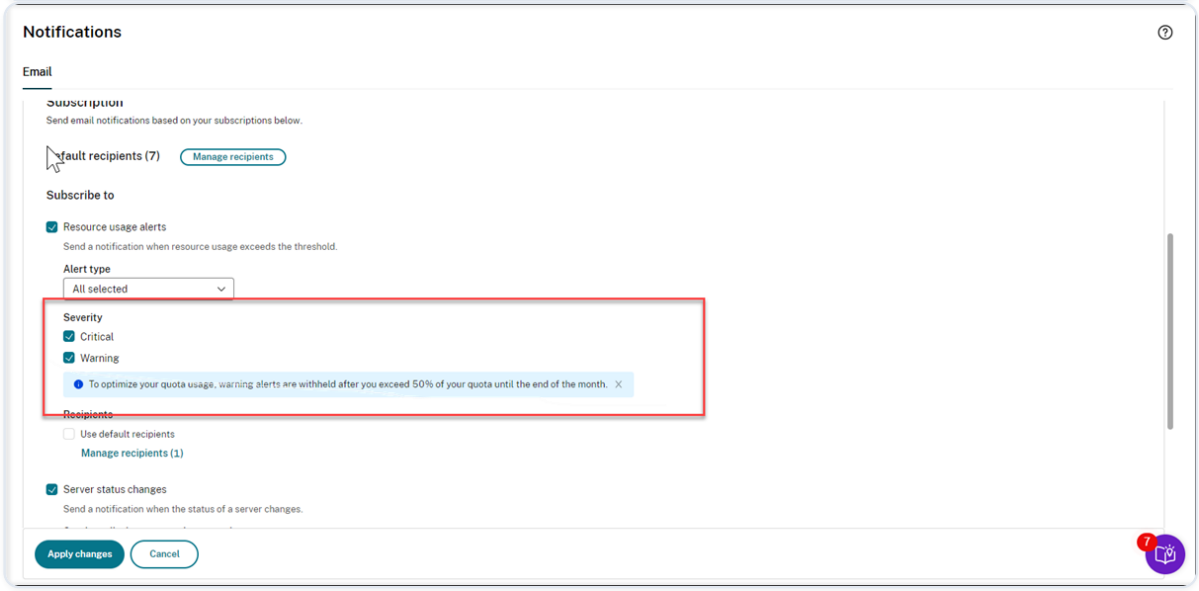
6. Subscribe to any of the following categories by selecting the check boxes next to them:

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

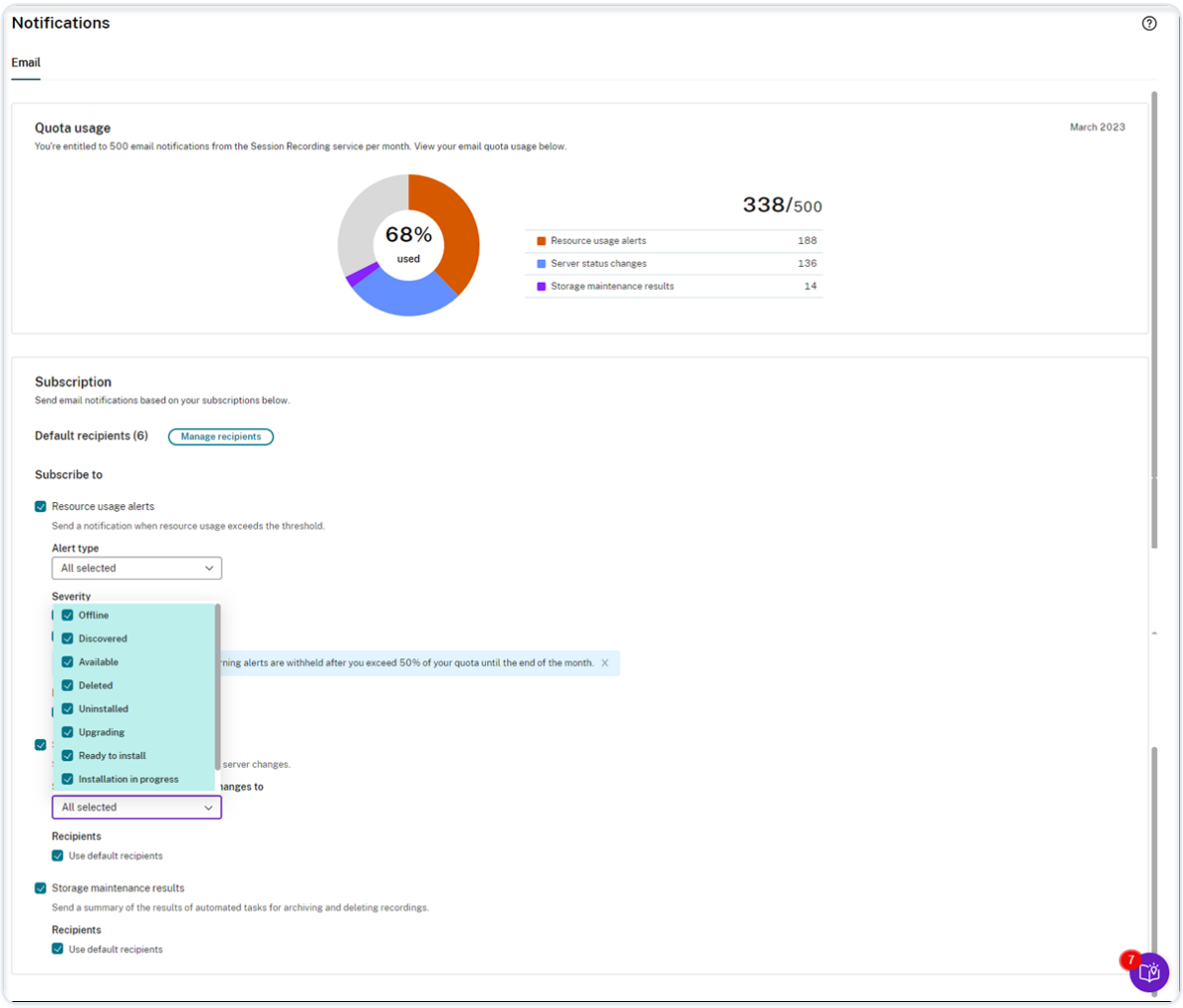
   Tips:

   - 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.

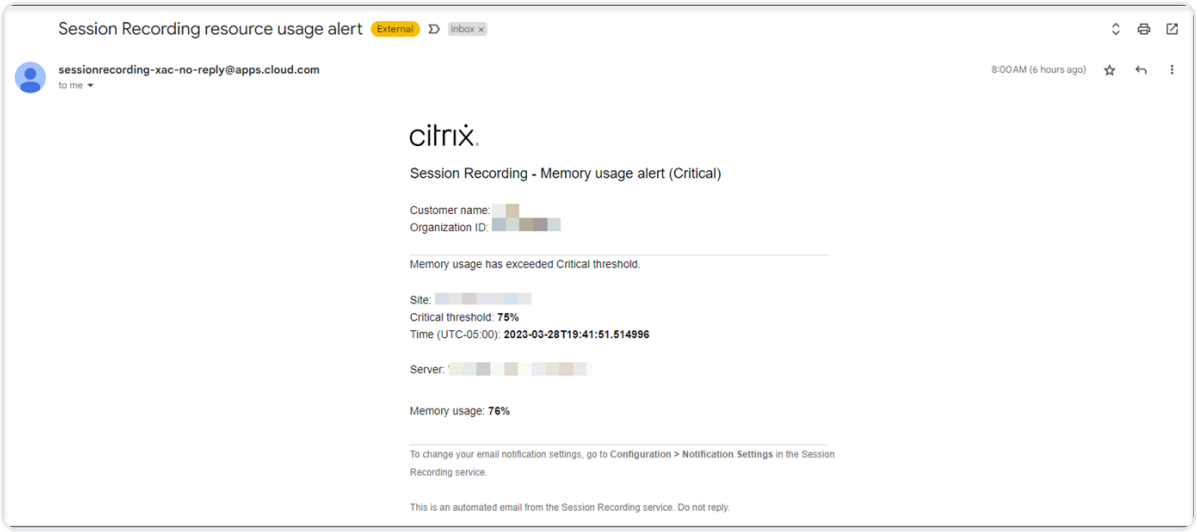




- For the available server statuses, see the following screen capture:



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



Customer data management

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.

Third-party SIEM integration

Overview

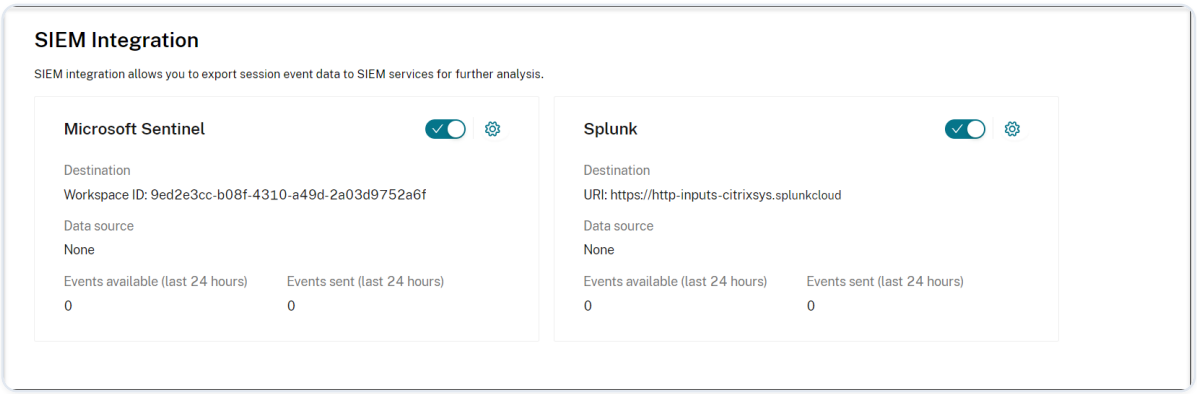
Session Recording provides the capability to capture various events in recorded sessions. You can upload a selected set of the event data to the Session Recording service and forward it to a third-party Security Information and Event Management (SIEM) system for further analysis. Currently, the Session Recording service supports integration with Splunk (both Splunk Cloud and Splunk Enterprise) and Microsoft Sentinel.

Integrating with a third-party SIEM platform enhances your organization's security posture by leveraging advanced analytics and correlation capabilities to detect and respond to potential threats more effectively.

Configuration

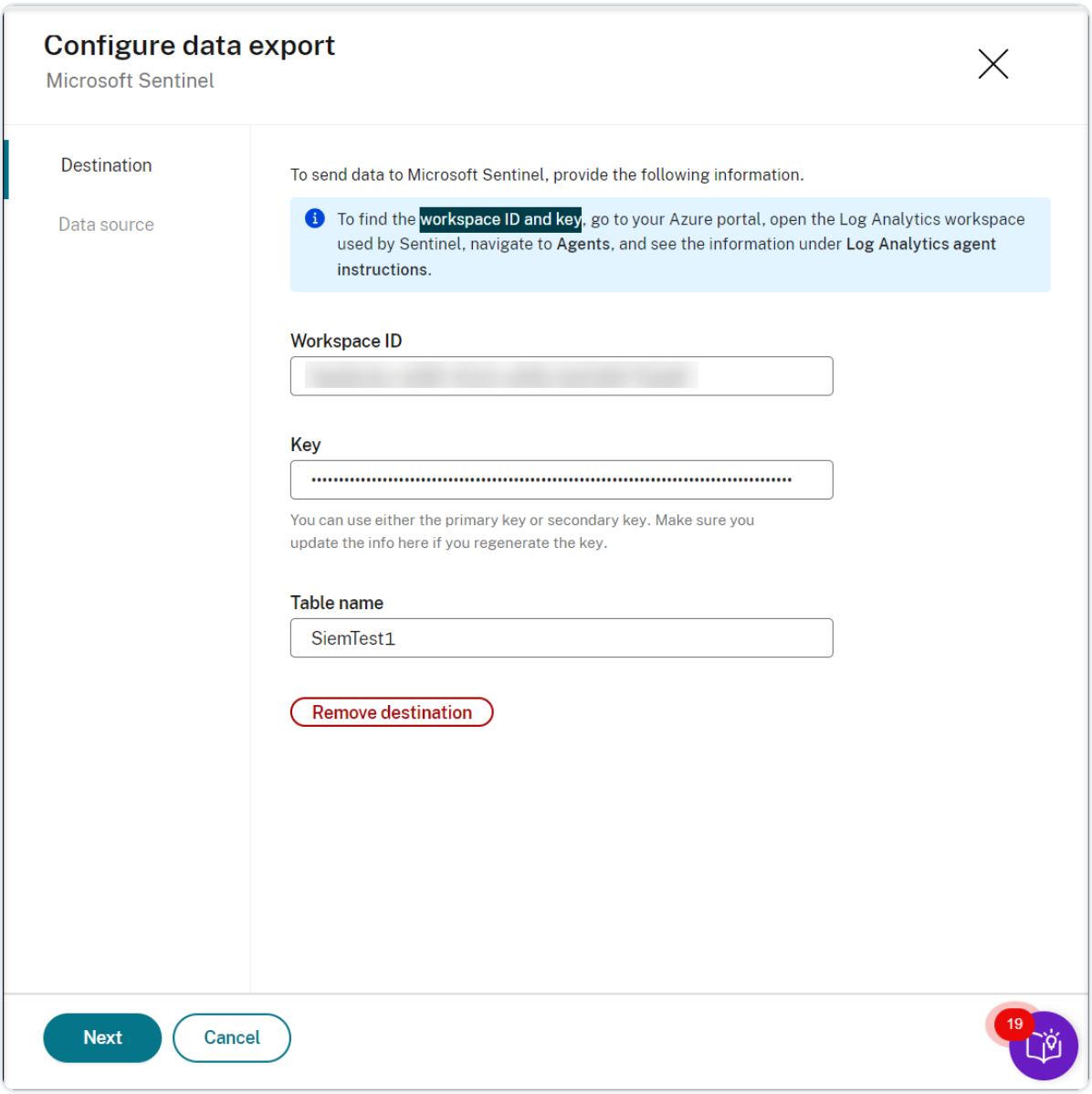
1. Enable SIEM integration.

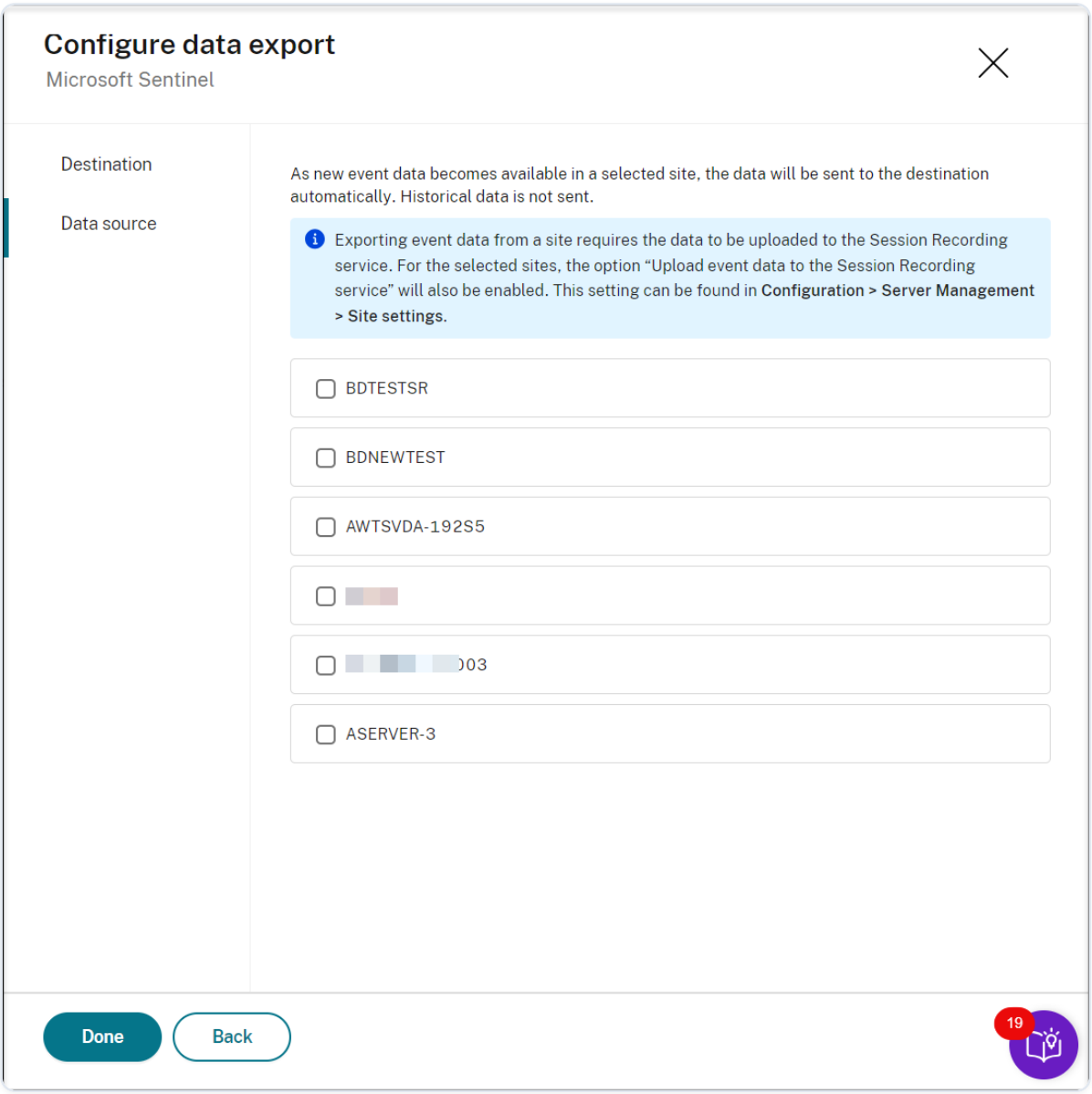
    a. Select **Configuration > SIEM Integration** from the left navigation of the Session Recording service.



    b. Enable Microsoft Sentinel, Splunk, or both as needed. Then, click the **Configure** icon next to the toggle to configure the destination and data source.

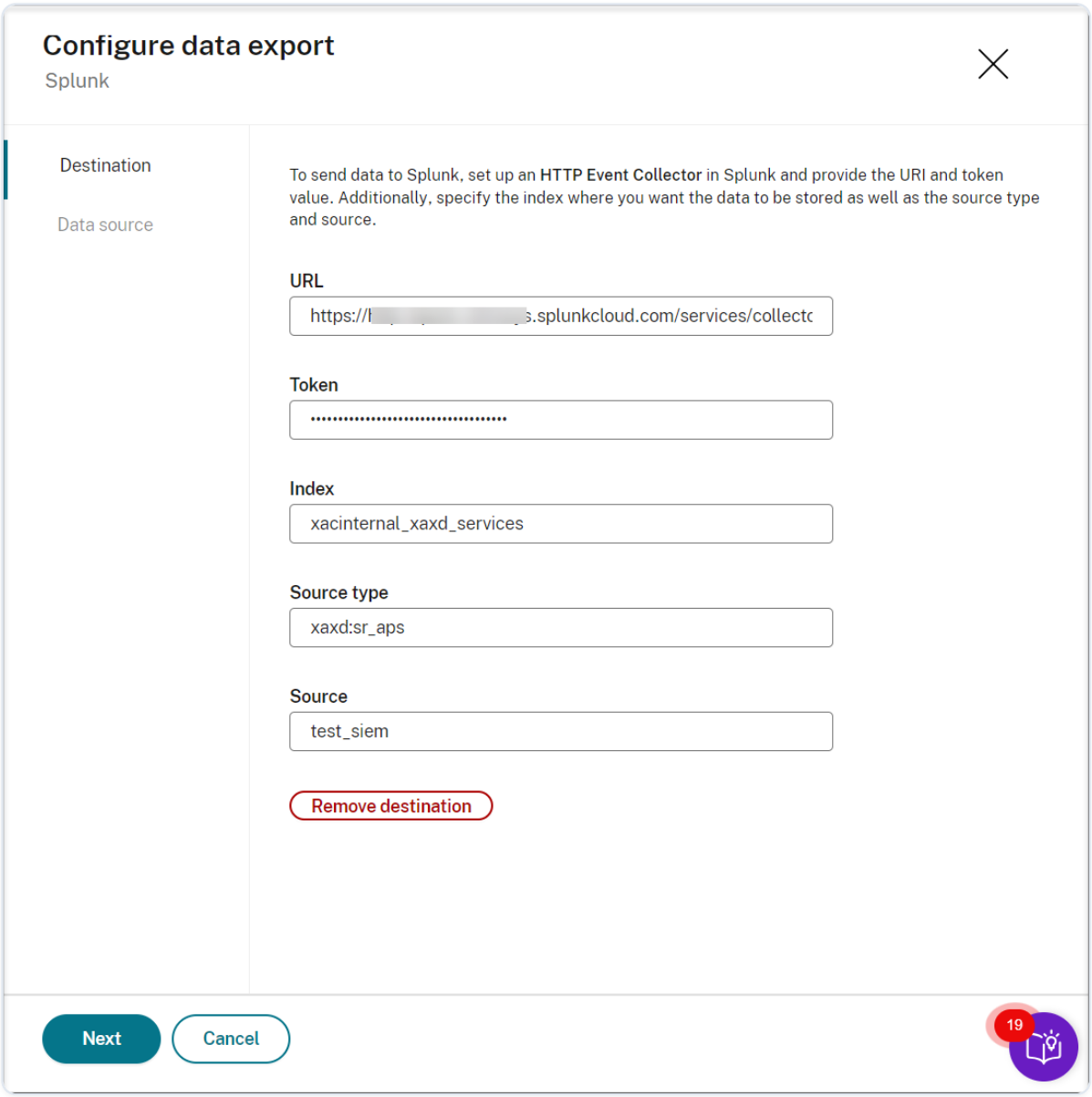
        To send data to Microsoft Sentinel, provide the workspace ID and key for the Microsoft Sentinel destination and select the target sites as the source of data to be sent. Only sites containing Session recording version 2411 and later are supported for SIEM integration.

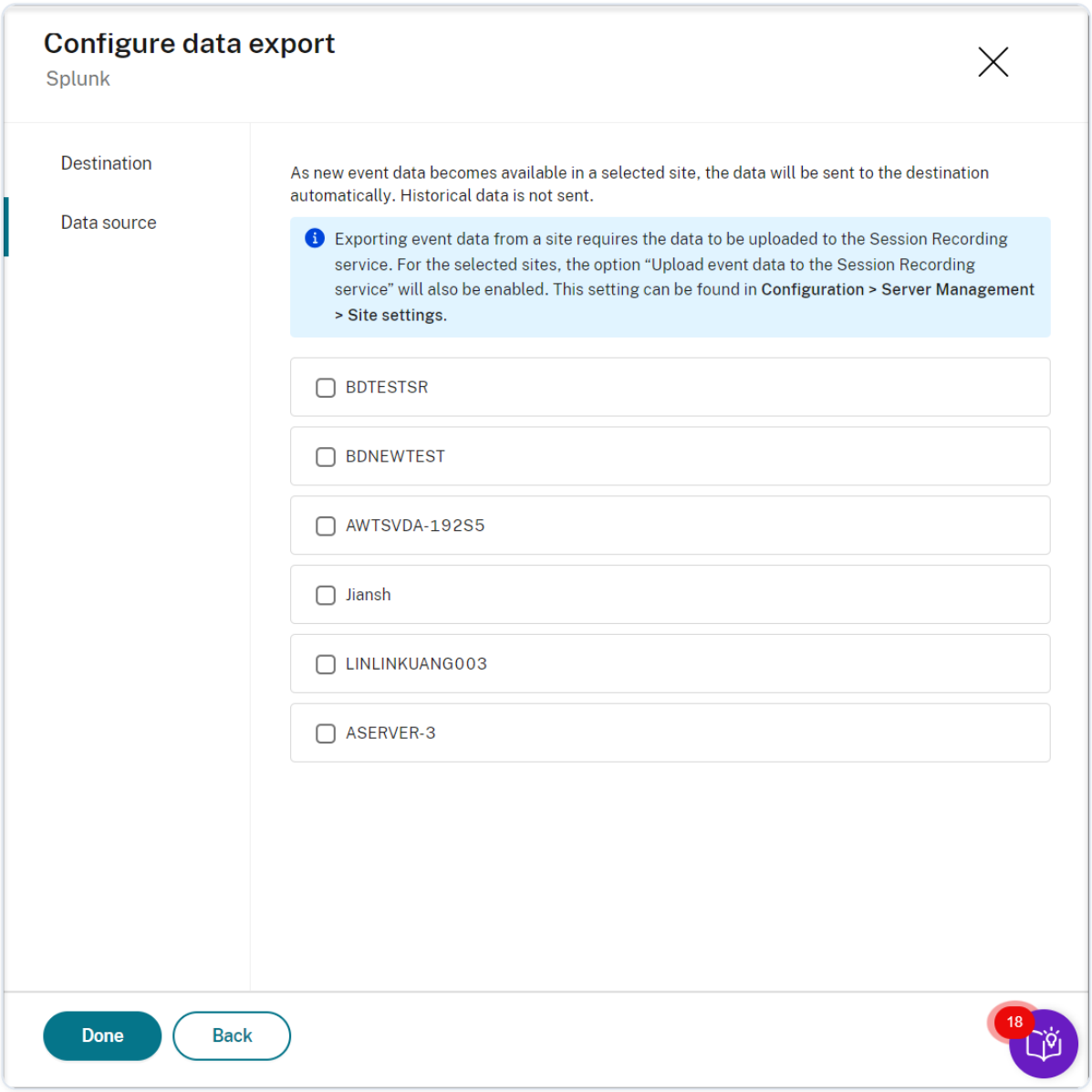

Configure data export
Microsoft Sentinel
Destination
Data source
To send data to Microsoft Sentinel, provide the following information.
To find the workspace ID and key, go to your Azure portal, open the Log Analytics workspace used by Sentinel, navigate to Agents, and see the information under Log Analytics agent instructions.
Workspace ID
Key
You can use either the primary key or secondary key. Make sure you update the info here if you regenerate the key.
Table name
SiemTest1
Remove destination
Next
Cancel
19



To send data to Splunk, set up an HTTP Event Collector in Splunk. For instructions, see the Splunk documentation: Set up and use HTTP Event Collector in Splunk Web. The Session Recording service supports both Splunk Cloud and Splunk Enterprise. If you are using Splunk Enterprise, ensure that inbound connectivity from the Session Recording service (currently hosted on Microsoft Azure) to your Splunk Enterprise is configured.

Provide the URL, token value, and specify the index where you want the data to be stored in addition to the source type and source. Then, similar to Microsoft Sentinel, select the target sites as the source of data to be sent. Only sites containing Session recording version 2411 and later are supported for SIEM integration.

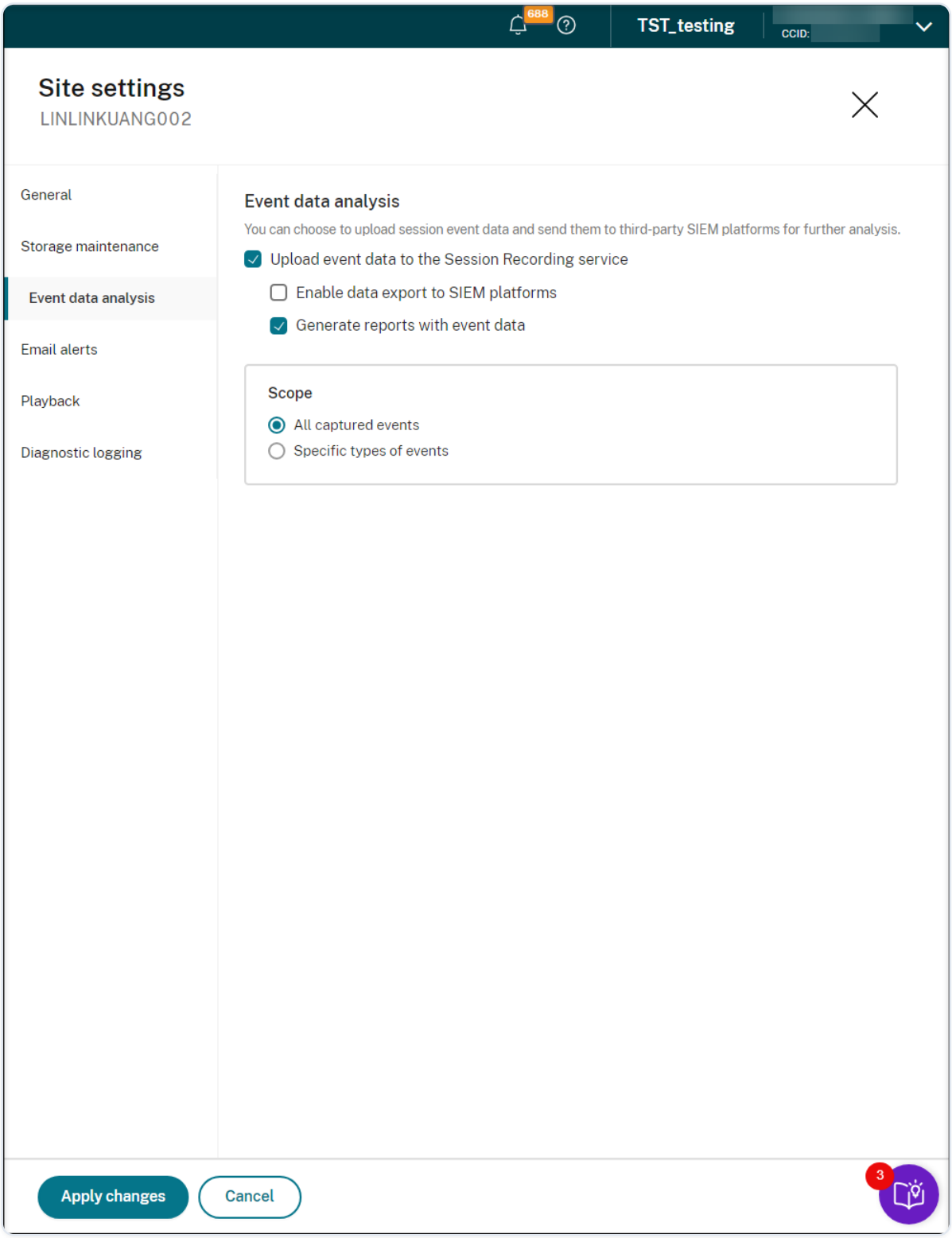

Configure data export
Splunk
Destination
Data source
To send data to Splunk, set up an HTTP Event Collector in Splunk and provide the URI and token value. Additionally, specify the index where you want the data to be stored as well as the source type and source.
URL
https://[redacted].splunkcloud.com/services/collectc
Token
Index
xacinternal_xaxd_services
Source type
xaxd:sr_aps
Source
test_siem
Remove destination
Next
Cancel
19



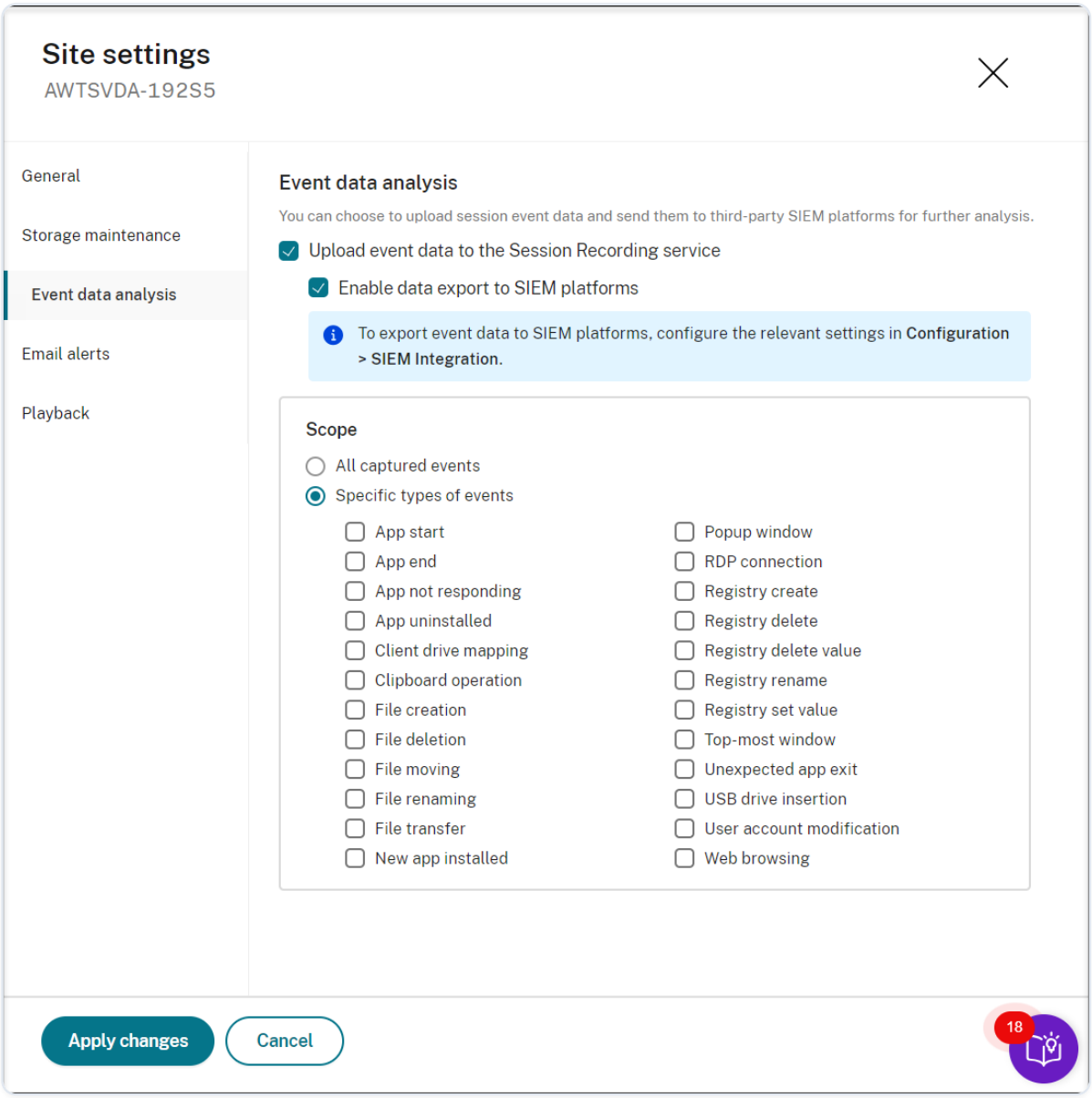
2. Specify events to forward.

   You must specify the types of events to be uploaded to the Session Recording service and forwarded to the SIEM platforms you specified earlier. To do so, complete the following steps:

   a. Go to **Site settings** for each of the sites that you selected earlier as the data source. For example:



b. Select **Upload event data to the Session Recording service** and then select **Enable data export to SIEM platforms**. In the **Scope** section, specify the types of events to forward. For example:



3. Test the integration.

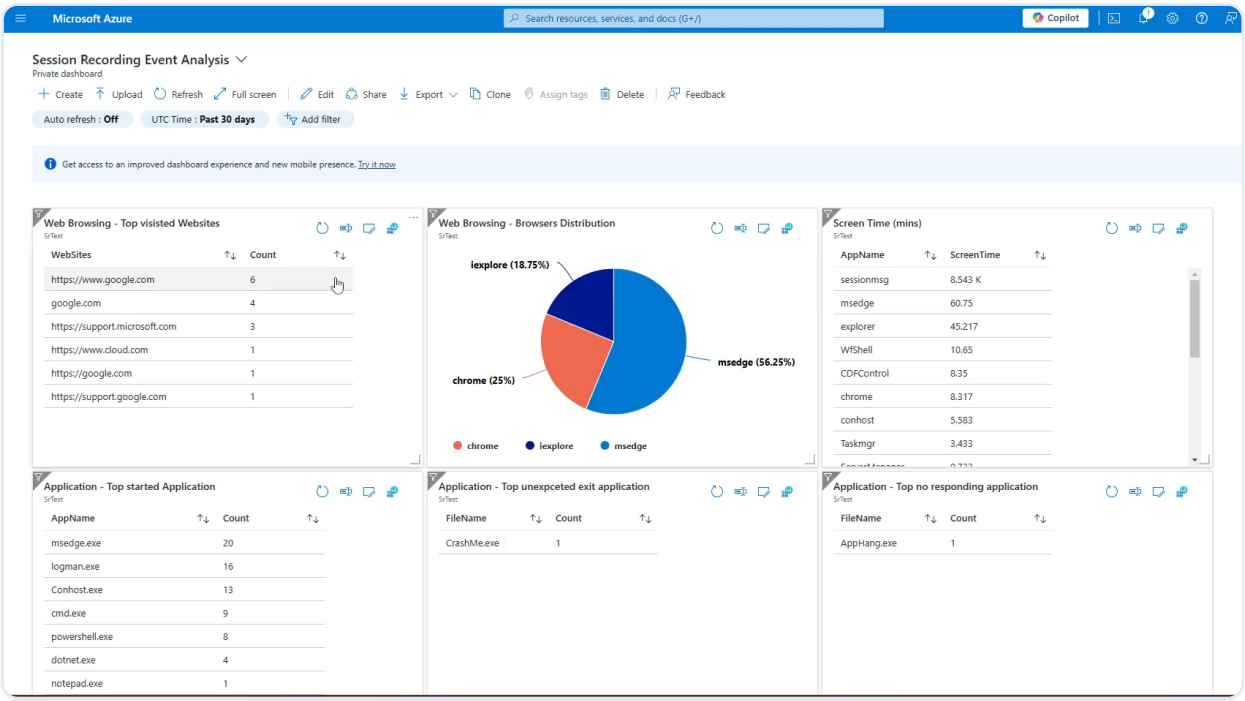
   After configuring the integration, test it to ensure that events are being forwarded correctly to the SIEM platforms specified.

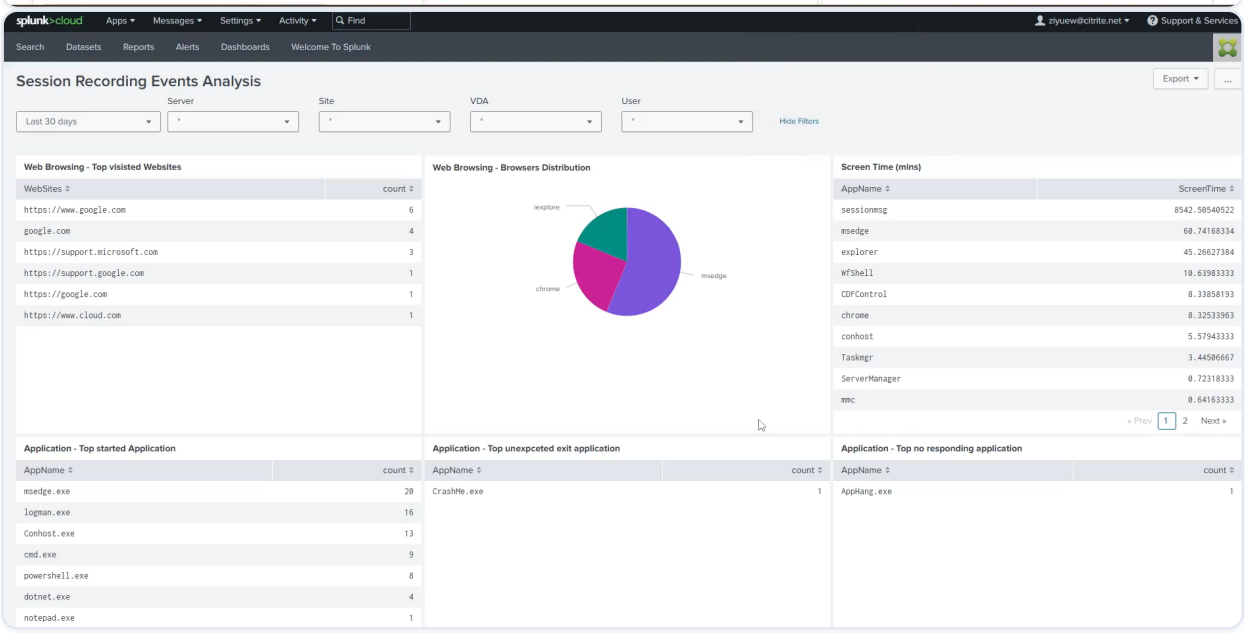
4. Monitor and adjust.

   Continuously monitor the integration to ensure it is functioning as expected. Adjust the configuration as needed to fine-tune the event forwarding and improve the accuracy of the alerts.

5. Visualize event data.

   You can visualize event data in Microsoft Sentinel and Splunk. The following are example views:





To visualize event data in Microsoft Sentinel, contact Citrix Technical Support.

To quickly import and visualize event data in Splunk, use the following dashboard template by customizing the search queries and visualizations to match your data:

```
<form version="1.1" theme="light">

 <label>Session Recording Events Analysis</label>

 <fieldset submitButton="false">

  <input type="time" token="time_field">
```

```
    <label></label>
    <default>
     <earliest>-24h@h</earliest>
     <latest>now</latest>
   </default>
  </input>
  <input type="dropdown" token="Server">
   <label>Server</label>
   <default>*</default>
   <initialValue>*</initialValue>
   <fieldForValue>Server</fieldForValue>
   <search>
    <query>index={{index}} sourcetype={{source_type}} source={{source}}
| table dvc
| rename dvc as Server
| dedup Server
| sort Server</query>
      <earliest>$time_field.earliest$</earliest>
      <latest>$time_field.latest$</latest>
    </search>
   </input>
   <input type="dropdown" token="Site">
```

```
    <label>Site</label>
    <default>*</default>
    <initialValue>*</initialValue>
    <fieldForValue>Site</fieldForValue>
    <search>
     <query>index="{{}}" sourcetype={{source_type}} source={{source}}
| table tenant.srSiteId
| rename tenant.srSiteId  as Site
| dedup Site
| sort Site</query>
     <earliest>$time_field.earliest$</earliest>
     <latest>$time_field.latest$</latest>
    </search>
   </input>
   <input type="dropdown" token="VDA">
    <label>VDA</label>
    <default>*</default>
    <initialValue>*</initialValue>
    <fieldForValue>VDA</fieldForValue>
    <search>
     <query>index={{index}} sourcetype={{source_type}}
source={{source}}
```

```
| table payload.deviceId

| rename payload.deviceId as VDA

| dedup VDA

| sort VDA</query>

     <earliest>$time_field.earliest$</earliest>

     <latest>$time_field.latest$</latest>

    </search>

   </input>

   <input type="dropdown" token="User">

    <label>User</label>

    <default>*</default>

    <initialValue>*</initialValue>

    <fieldForValue>User</fieldForValue>

    <search>

     <query>index={{index}} sourcetype={{source_type}}
source={{source}}

| table payload.user

| rename payload.user as User

| dedup User

| sort User</query>

    <earliest>$time_field.earliest$</earliest>

    <latest>$time_field.latest$</latest>
```

```
  </search>

 </input>

</fieldset>

<row>

 <panel>

  <table>

    <title>Web Browsing - Top visisted Websites</title>

    <search>

     <query>index={{index}} sourcetype={{source_type}}
source={{source}}

| search type=Citrix.EventMonitor.WebBrowsing

| spath payload.ExtEventData1

| stats count by payload.ExtEventData1

| sort count desc

| rename payload.ExtEventData1 as WebSites</query>

      <earliest>$time_field.earliest$</earliest>

      <latest>$time_field.latest$</latest>

      <sampleRatio>1</sampleRatio>

     </search>

     <option name="dataOverlayMode">none</option>

     <option name="drilldown">none</option>

     <option name="percentagesRow">false</option>
```

```
      <option name="rowNumbers">false</option>

      <option name="totalsRow">false</option>

      <option name="wrap">true</option>

      <format type="color" field="FunctionFailed">

       <colorPalette type="list">[#118832,#D41F1F]</colorPalette>

       <scale type="threshold">1</scale>

      </format>

     </table>

    </panel>

    <panel>

     <chart>

      <title>Web Browsing - Browsers Distribution</title>

      <search>

       <query>index={{index}} sourcetype={{source_type}}
source={{source}}

| search type=Citrix.EventMonitor.WebBrowsing

| spath payload.ExtEventData3

| stats count by payload.ExtEventData3|sort count desc</query>

        <earliest>$time_field.earliest$</earliest>

        <latest>$time_field.latest$</latest>

        <sampleRatio>1</sampleRatio>

       </search>
```

```
      <option name="charting.chart">pie</option>
      <option name="charting.drilldown">none</option>
      <option name="refresh.display">progressbar</option>
     </chart>
   </panel>
   <panel>
    <table>
     <title>Screen Time (mins)</title>
     <search>
       <query>index={{index}} sourcetype={{source_type}}
source={{source}}
| spath "payload.type"
| search "payload.type"="Citrix.EventMonitor.TopMost"
| rename payload.ExtEventData1 as AppName, payload.deviceId as DeviceId
| eval time=strptime(st, "%Y-%m-%dT%H:%M:%S.%7N")
| sort DeviceId time
| streamstats current=f window=1 last(time) as last_time by DeviceId
| eval time_diff = if(isnull(last_time), null(), time - last_time)
| table time, DeviceId, AppName, time_diff |eval time_diff = time_diff/
60
| stats sum(time_diff) by AppName |sort by sum(time_diff) desc |rename
sum(time_diff) as ScreenTime</query>
       <earliest>$time_field.earliest$</earliest>
```

```
      <latest>$time_field.latest$</latest>
      <sampleRatio>1</sampleRatio>
    </search>
    <option name="dataOverlayMode">none</option>
    <option name="drilldown">none</option>
    <option name="percentagesRow">false</option>
    <option name="refresh.display">progressbar</option>
    <option name="rowNumbers">false</option>
    <option name="totalsRow">false</option>
    <option name="wrap">true</option>
    <format type="color" field="FunctionFailed">
     <colorPalette type="list">[#118832,#D41F1F]</colorPalette>
     <scale type="threshold">1</scale>
    </format>
   </table>
  </panel>
 </row>
 <row>
  <panel>
   <table>
    <title>Application - Top started Application</title>
    <search>
```

```
       <query>index={{index}} sourcetype={{source_type}}
source={{source}}

| search type=Citrix.EventMonitor.AppStart

| spath payload.ExtEventData2

| stats count by payload.ExtEventData2

| sort count desc

| rename payload.ExtEventData2 as AppName</query>

      <earliest>$time_field.earliest$</earliest>

      <latest>$time_field.latest$</latest>

      <sampleRatio>1</sampleRatio>

     </search>

     <option name="dataOverlayMode">none</option>

     <option name="drilldown">none</option>

     <option name="percentagesRow">false</option>

     <option name="rowNumbers">false</option>

     <option name="totalsRow">false</option>

     <option name="wrap">true</option>

     <format type="color" field="FunctionFailed">

      <colorPalette type="list">[#118832,#D41F1F]</colorPalette>

      <scale type="threshold">1</scale>

     </format>

    </table>
```

```
   </panel>

   <panel>

    <table>

     <title>Application - Top unexpceted exit application</title>

     <search>

      <query>index={{index}} sourcetype={{source_type}}
source={{source}}

| search type=Citrix.EventMonitor.UnexpectedAppExit

| spath payload.ExtEventData2

| stats count by payload.ExtEventData2

| sort count desc

| rename payload.ExtEventData2 as AppPath

| eval AppNameSplit = split(AppPath, "\\")

| eval AppName = mvindex(AppNameSplit, -1)

| table AppName|stats count by AppName</query>

       <earliest>$time_field.earliest$</earliest>

       <latest>$time_field.latest$</latest>

       <sampleRatio>1</sampleRatio>

      </search>

      <option name="dataOverlayMode">none</option>

      <option name="drilldown">none</option>

      <option name="percentagesRow">false</option>
```

```
      <option name="refresh.display">progressbar</option>
      <option name="rowNumbers">false</option>
      <option name="totalsRow">false</option>
      <option name="wrap">true</option>
      <format type="color" field="FunctionFailed">
       <colorPalette type="list">[#118832,#D41F1F]</colorPalette>
       <scale type="threshold">1</scale>
      </format>
     </table>
    </panel>
    <panel>
     <table>
     <title>Application - Top no responding application</title>
     <search>
      <query>index={{index}} sourcetype={{source_type}}
source={{source}}
| search type=Citrix.EventMonitor.AppNotResponding
| spath payload.ExtEventData2
| stats count by payload.ExtEventData2
| sort count desc
| rename payload.ExtEventData2 as AppPath
| eval AppNameSplit = split(AppPath, "\\")
```

```
| eval AppName = mvindex(AppNameSplit, -1)
| table AppName|stats count by AppName</query>
       <earliest>$time_field.earliest$</earliest>
       <latest>$time_field.latest$</latest>
       <sampleRatio>1</sampleRatio>
      </search>
      <option name="dataOverlayMode">none</option>
      <option name="drilldown">none</option>
      <option name="percentagesRow">false</option>
      <option name="refresh.display">progressbar</option>
      <option name="rowNumbers">false</option>
      <option name="totalsRow">false</option>
      <option name="wrap">true</option>
      <format type="color" field="FunctionFailed">
       <colorPalette type="list">[#118832,#D41F1F]</colorPalette>
       <scale type="threshold">1</scale>
      </format>
     </table>
    </panel>
   </row>
   <row>
    <panel>
```

```
     <table>
      <title>File Transfer - Top transfered in file count</title>
      <search>
       <query>index={{index}} sourcetype={{source_type}}
source={{source}}type="Citrix.EventMonitor.FileTransfer"
| spath payload.ExtEventData3
| search payload.ExtEventData3 = "Host:*"
| rename payload.ExtEventData3 as filePath
| eval fileSplit = split(filePath, "\\")
| eval FileName = mvindex(fileSplit, -1)
| table FileName
| stats count by FileName
| sort bv count desc</query>
       <earliest>$time_field.earliest$</earliest>
       <latest>$time_field.latest$</latest>
       <sampleRatio>1</sampleRatio>
      </search>
      <option name="dataOverlayMode">none</option>
      <option name="drilldown">none</option>
      <option name="percentagesRow">false</option>
      <option name="rowNumbers">false</option>
      <option name="totalsRow">false</option>
```

```
      <option name="wrap">true</option>

      <format type="color" field="FunctionFailed">

       <colorPalette type="list">[#118832,#D41F1F]</colorPalette>

       <scale type="threshold">1</scale>

      </format>

     </table>

    </panel>

    <panel>

     <table>

      <title>File Transfer - Top transfered in file size by user</
title>

      <search>

       <query>index={{index}} sourcetype={{source_type}}
source={{source}}type="Citrix.EventMonitor.FileTransfer"

| spath payload.ExtEventData3

| search payload.ExtEventData3 = "Host:*"

| rename payload.ExtEventData4 as filesize

| eval filesize_mb =

   case(

   like(filesize, "% B"), tonumber(replace(filesize, " B", "")) /
1024 /1024,

   like(filesize, "% KB"), tonumber(replace(filesize, " KB", "")) /
1024,

   like(filesize, "% MB"), tonumber(replace(filesize, " MB", "")),
```

```
   like(filesize, "% GB"), tonumber(replace(filesize, " GB", "")) *
1024,

   like(filesize, "% TB"), tonumber(replace(filesize, " TB", "")) *
1024 * 1024

   )

| table payload.user, filesize_mb

| stats sum by payload.user |rename sum(filesize_mb) as FileSize(MB),
payload.user as User</query>

        <earliest>$time_field.earliest$</earliest>

        <latest>$time_field.latest$</latest>

        <sampleRatio>1</sampleRatio>

      </search>

      <option name="dataOverlayMode">none</option>

      <option name="drilldown">none</option>

      <option name="percentagesRow">false</option>

      <option name="refresh.display">progressbar</option>

      <option name="rowNumbers">false</option>

      <option name="totalsRow">false</option>

      <option name="wrap">true</option>

      <format type="color" field="FunctionFailed">

        <colorPalette type="list">[#118832,#D41F1F]</colorPalette>

        <scale type="threshold">1</scale>

      </format>
```

```
      </table>

     </panel>

     <panel>

      <table>

       <title>File Transfer - Top transfered out file count by user</
title>

       <search>

        <query>index={{index}} sourcetype={{source_type}}
source={{source}}type="Citrix.EventMonitor.FileTransfer"

| spath payload.ExtEventData2

| search payload.ExtEventData2 = "Host:*"

| table payload.user, payload.ExtEventData2

| stats count by payload.user

| rename payload.user as User</query>

      <earliest>$time_field.earliest$</earliest>

      <latest>$time_field.latest$</latest>

      <sampleRatio>1</sampleRatio>

     </search>

     <option name="dataOverlayMode">none</option>

     <option name="drilldown">none</option>

     <option name="percentagesRow">false</option>

     <option name="rowNumbers">false</option>

     <option name="totalsRow">false</option>
```

```
     <option name="wrap">true</option>
     <format type="color" field="FunctionFailed">
      <colorPalette type="list">[#118832,#D41F1F]</colorPalette>
      <scale type="threshold">1</scale>
     </format>
    </table>
   </panel>
  </row>
 </form>
```

Best practices

You can consult the following best practices documentation for deploying Session Recording:

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

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

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.

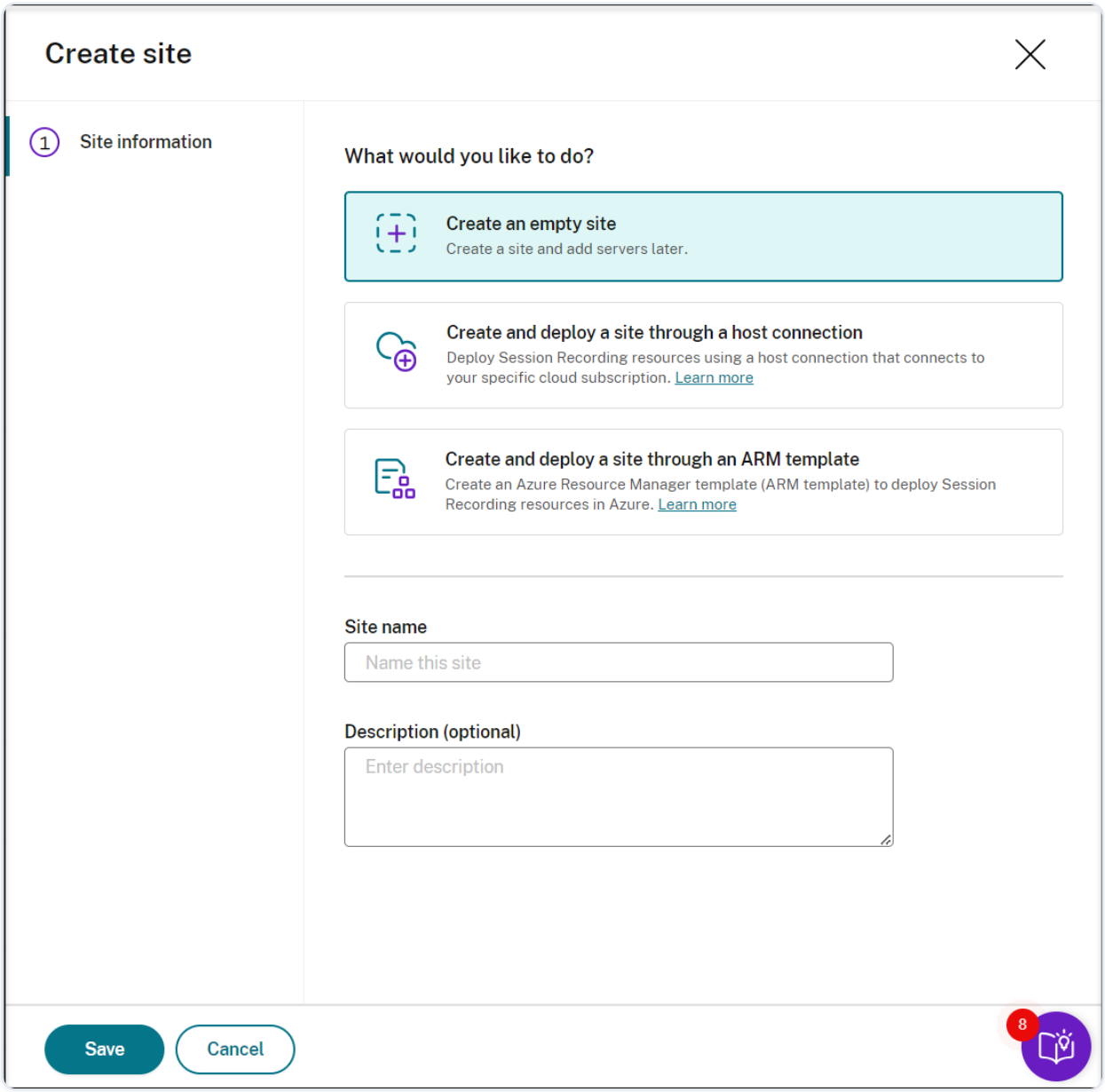
For an existing site deployed on Azure, you can add resources including servers and storage to it and change the IP addresses that are allowed to access the load balancer.

This article guides you through the following procedures:

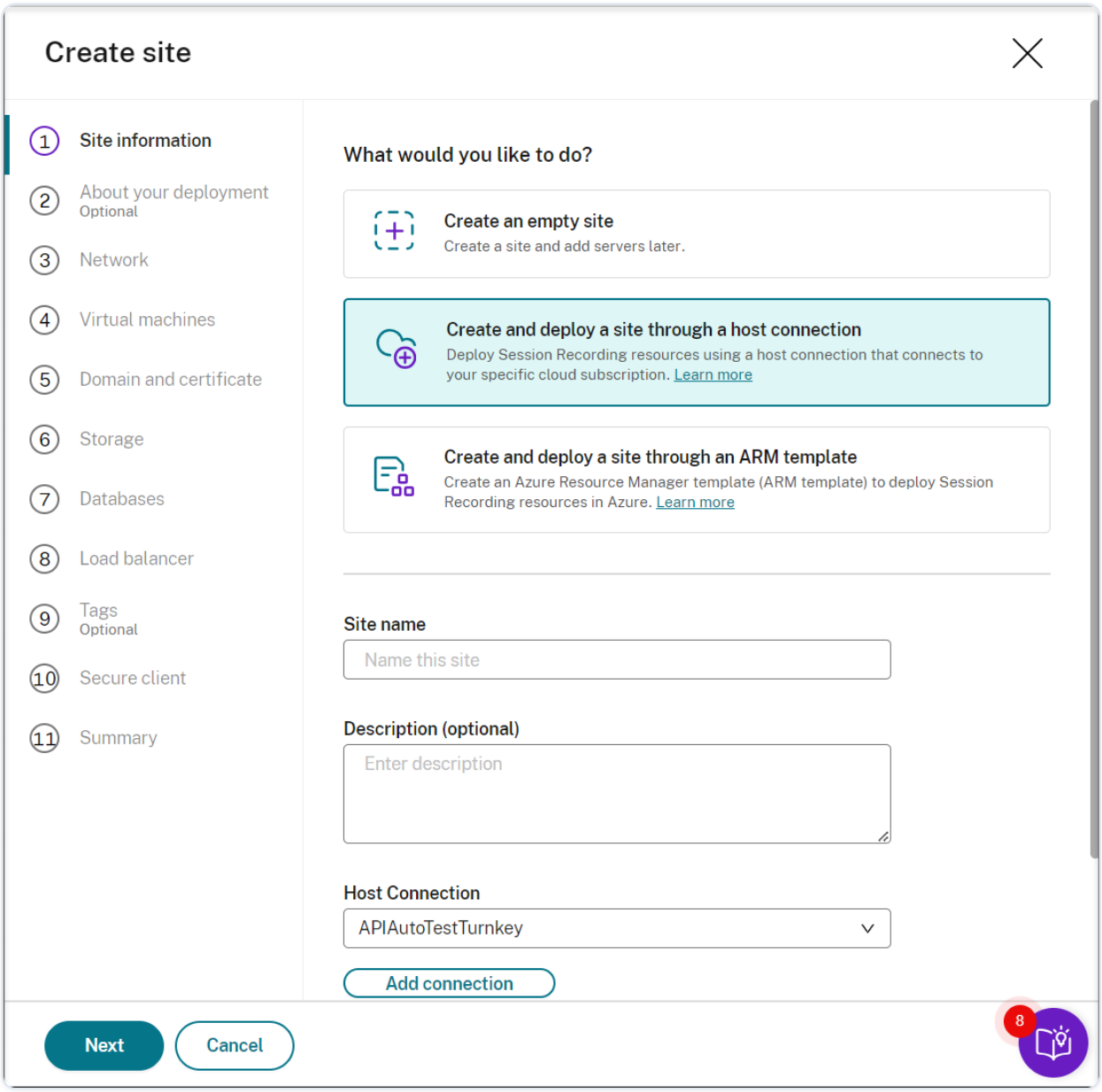
1. Select **Configuration > Server Management** from the left navigation of the Session Recording service.



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

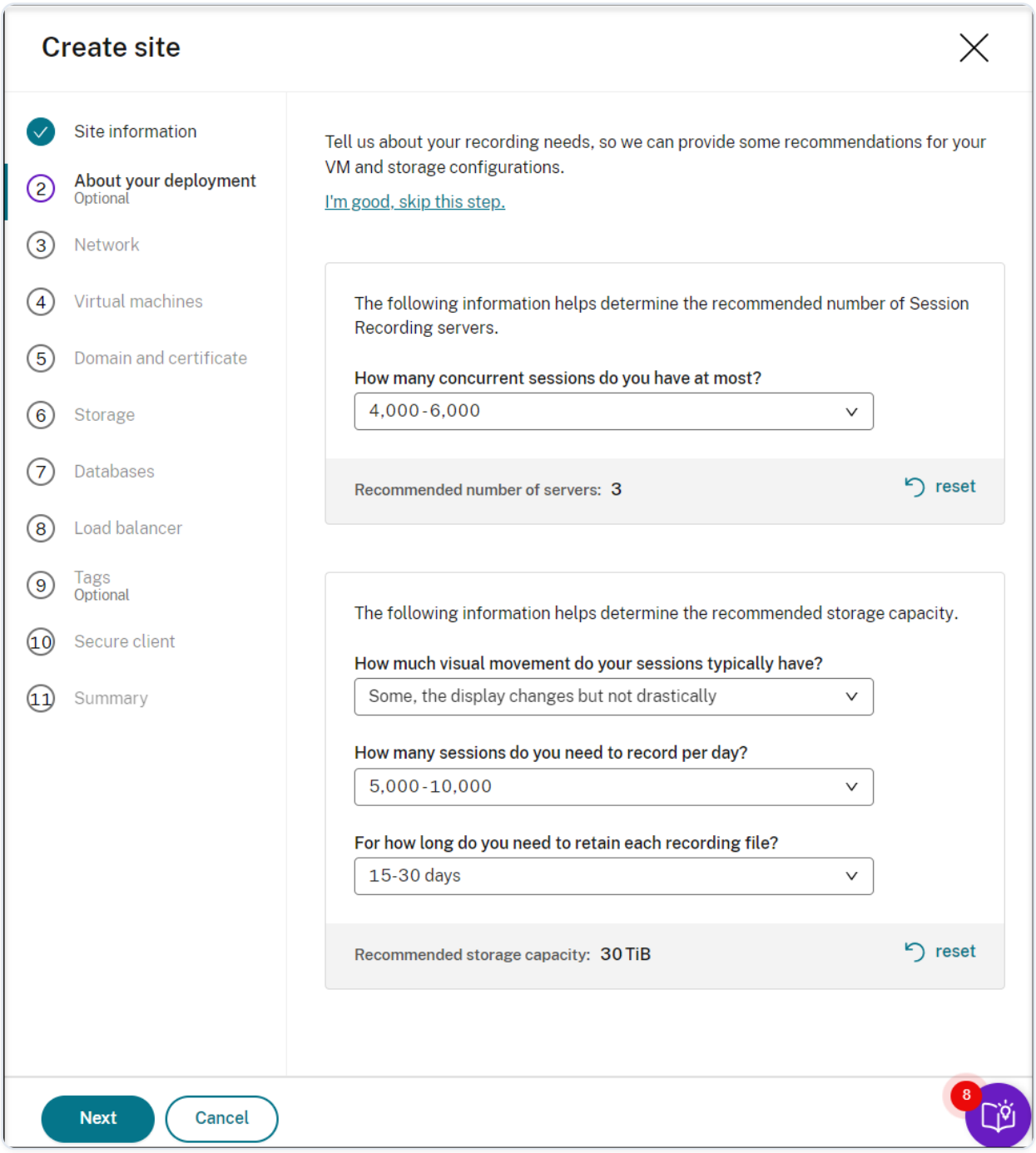


3. Select **Create and deploy a site through a host connection**. The main steps are listed in the left navigation.



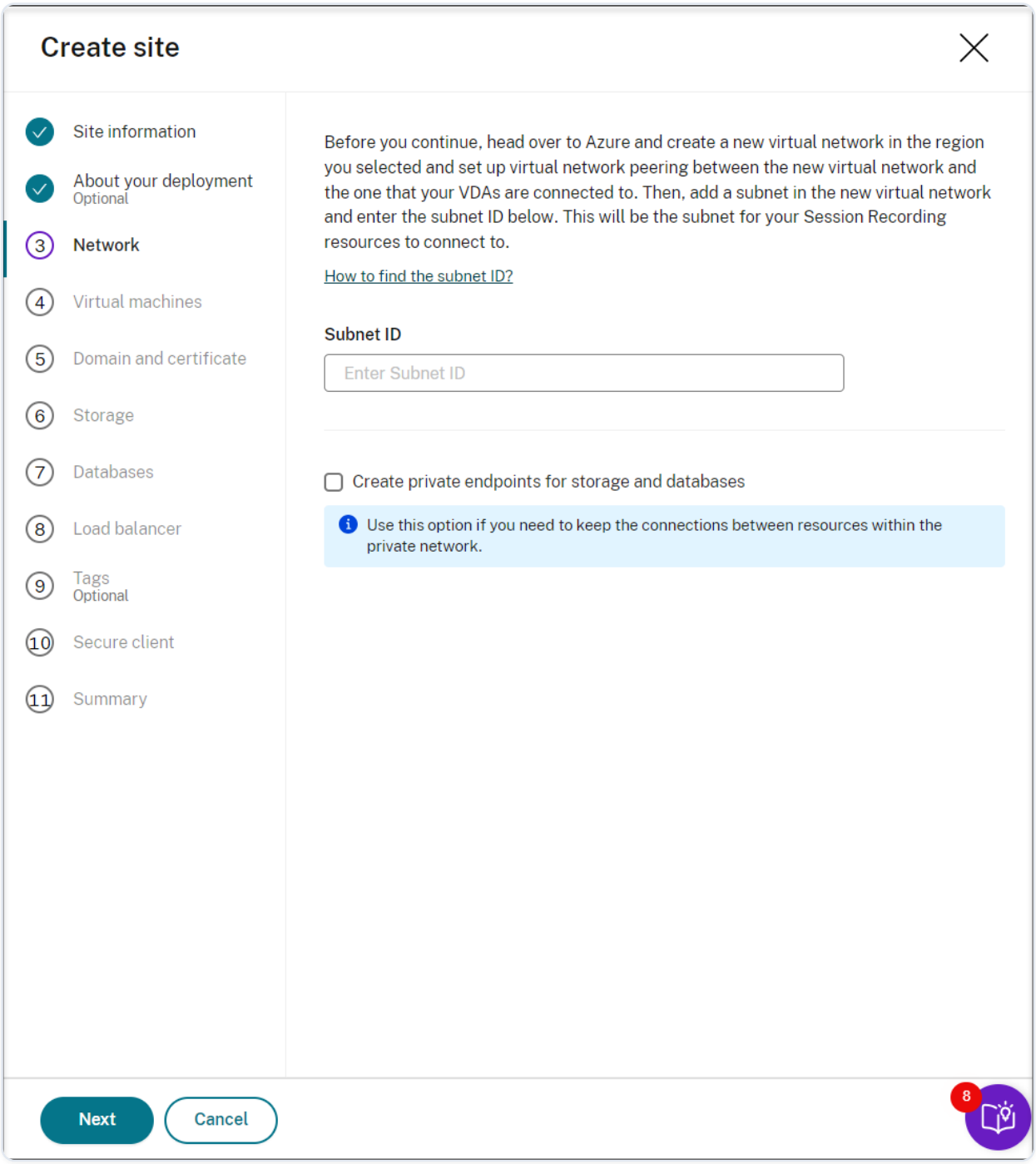
4. Enter a site name and description, select the host connection that you added in Step 1, and specify a region. Azure Government regions aren't supported.
5. After completing the site information, click **Next** to continue.
6. (Optional) To get recommendations for VM and storage configurations, provide 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.



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.

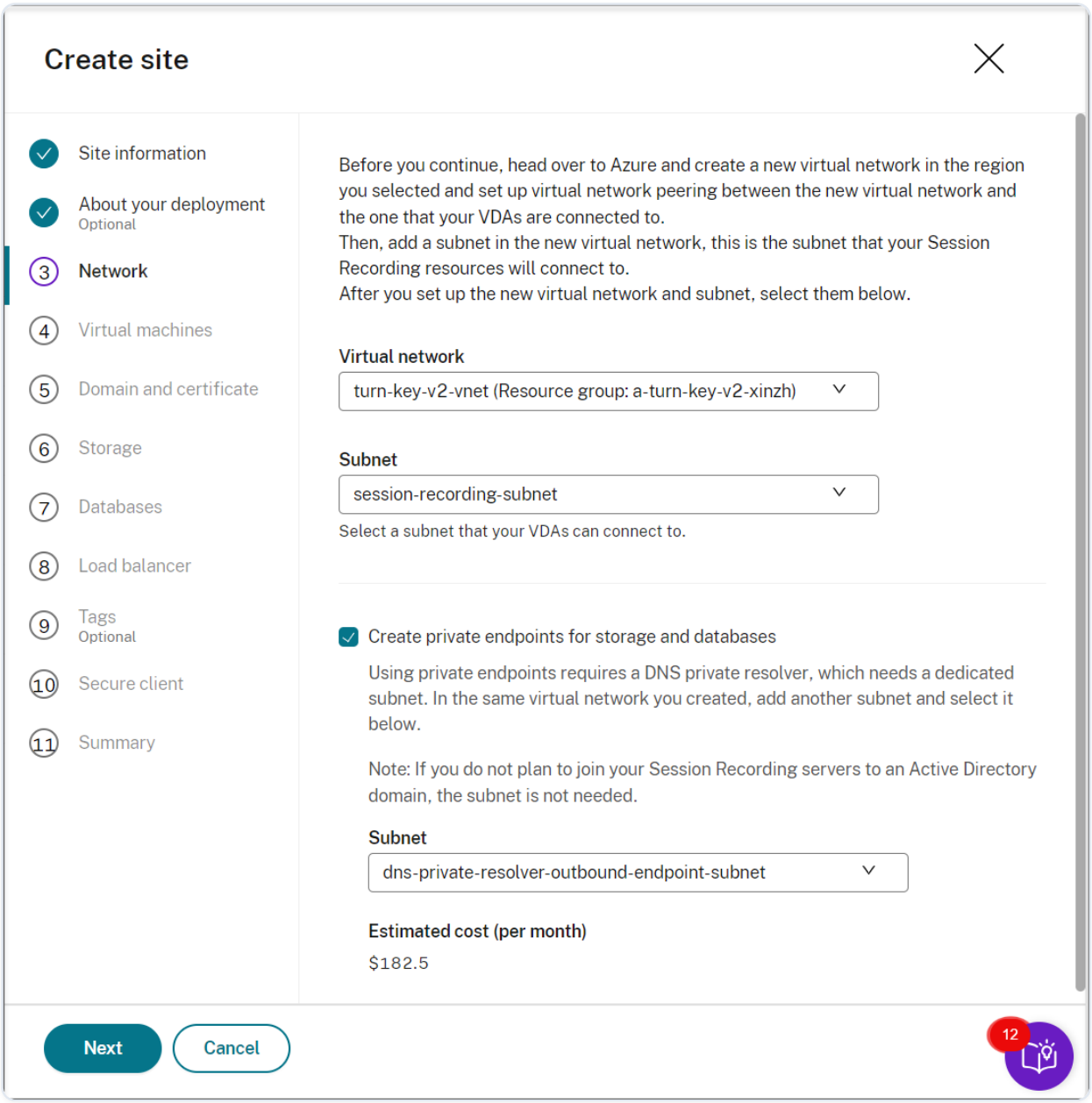
7. Go to the Azure portal and create a new virtual network in the region you selected and set up virtual network peering between the new virtual network and the one that your VDAs are connected to. Then, add a subnet in the new virtual network. Find and enter the subnet ID below.



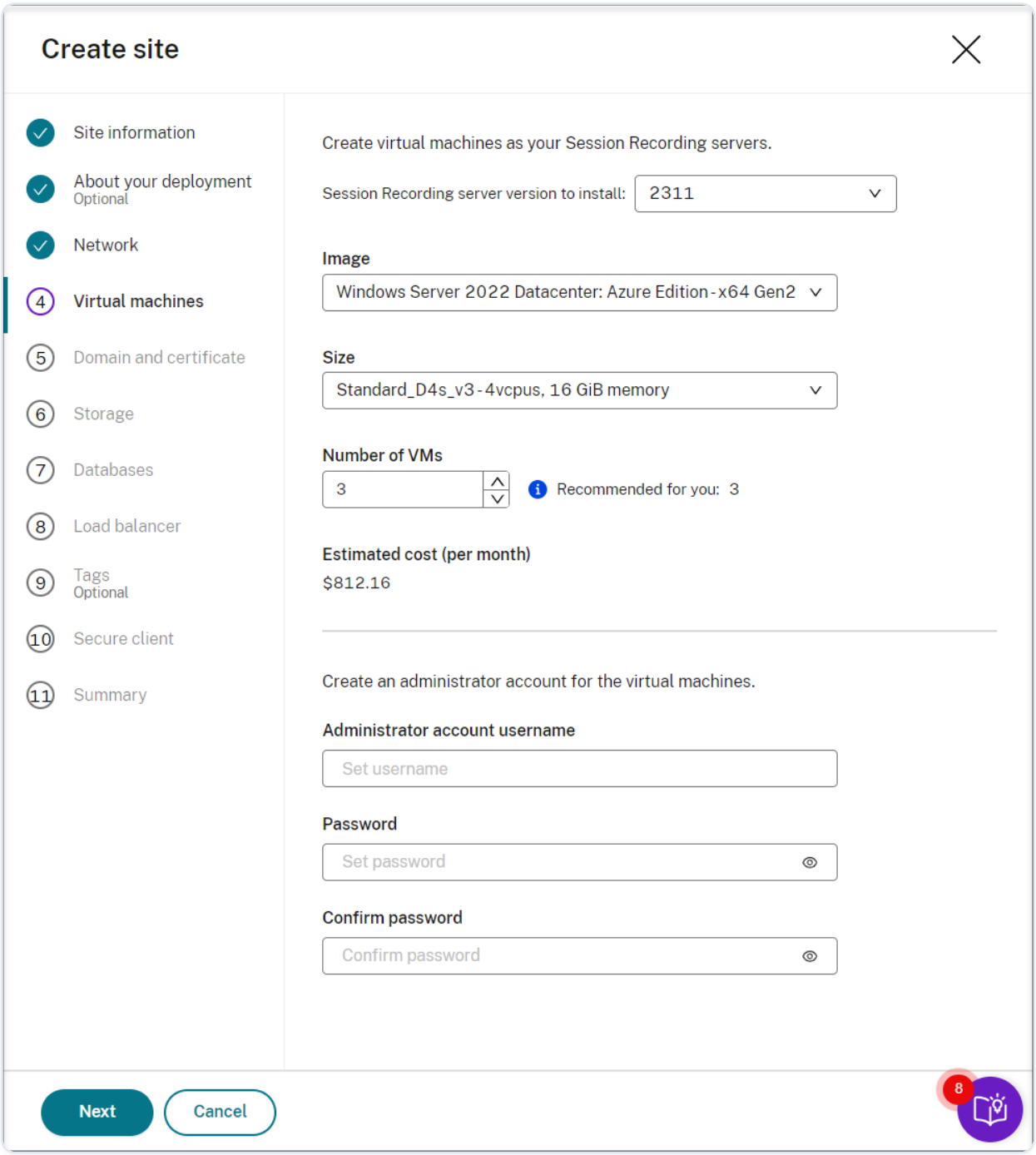
To keep the connections between resources within the private network, select the **Create private endpoints for storage and databases** check box.

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.



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

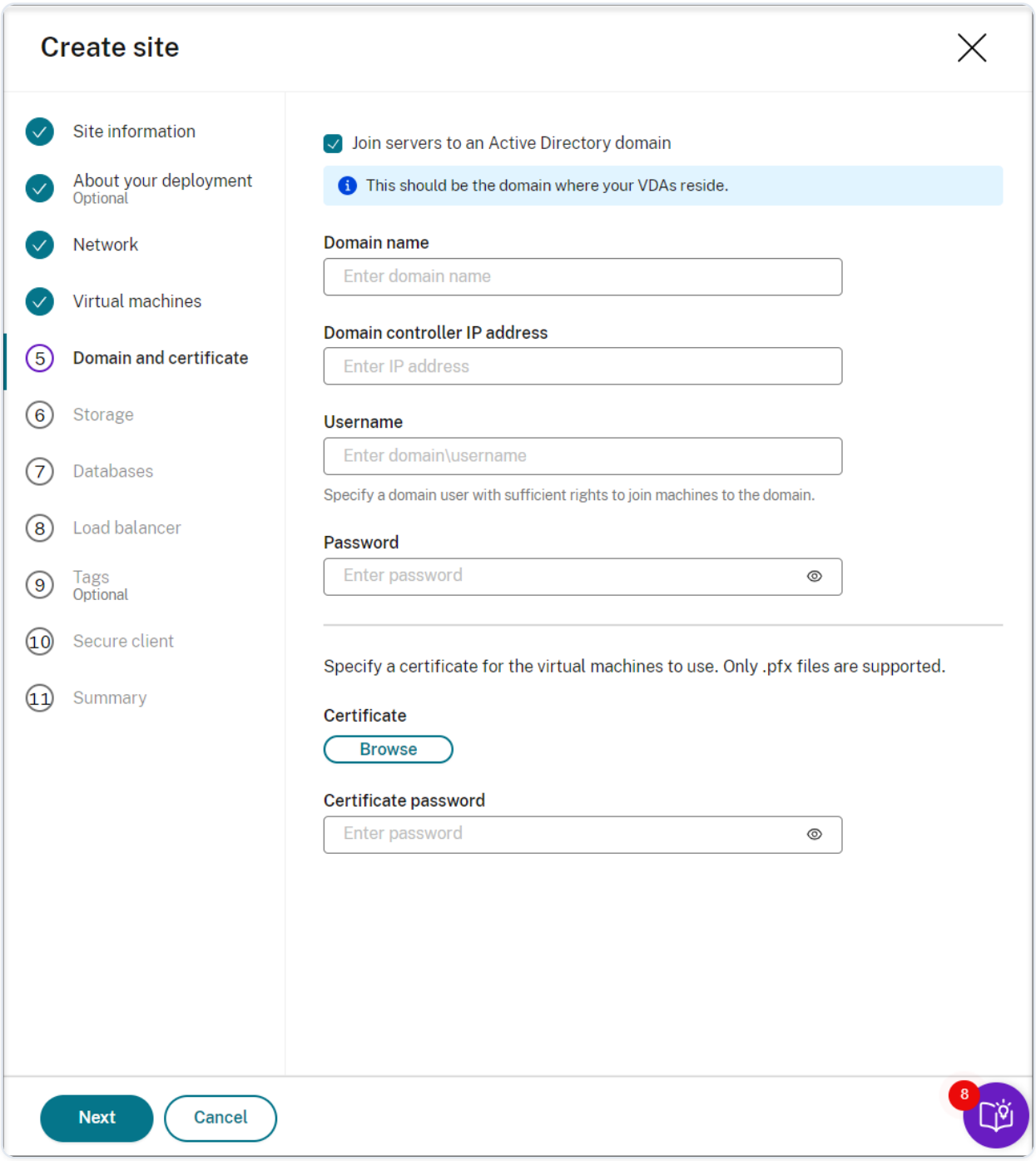


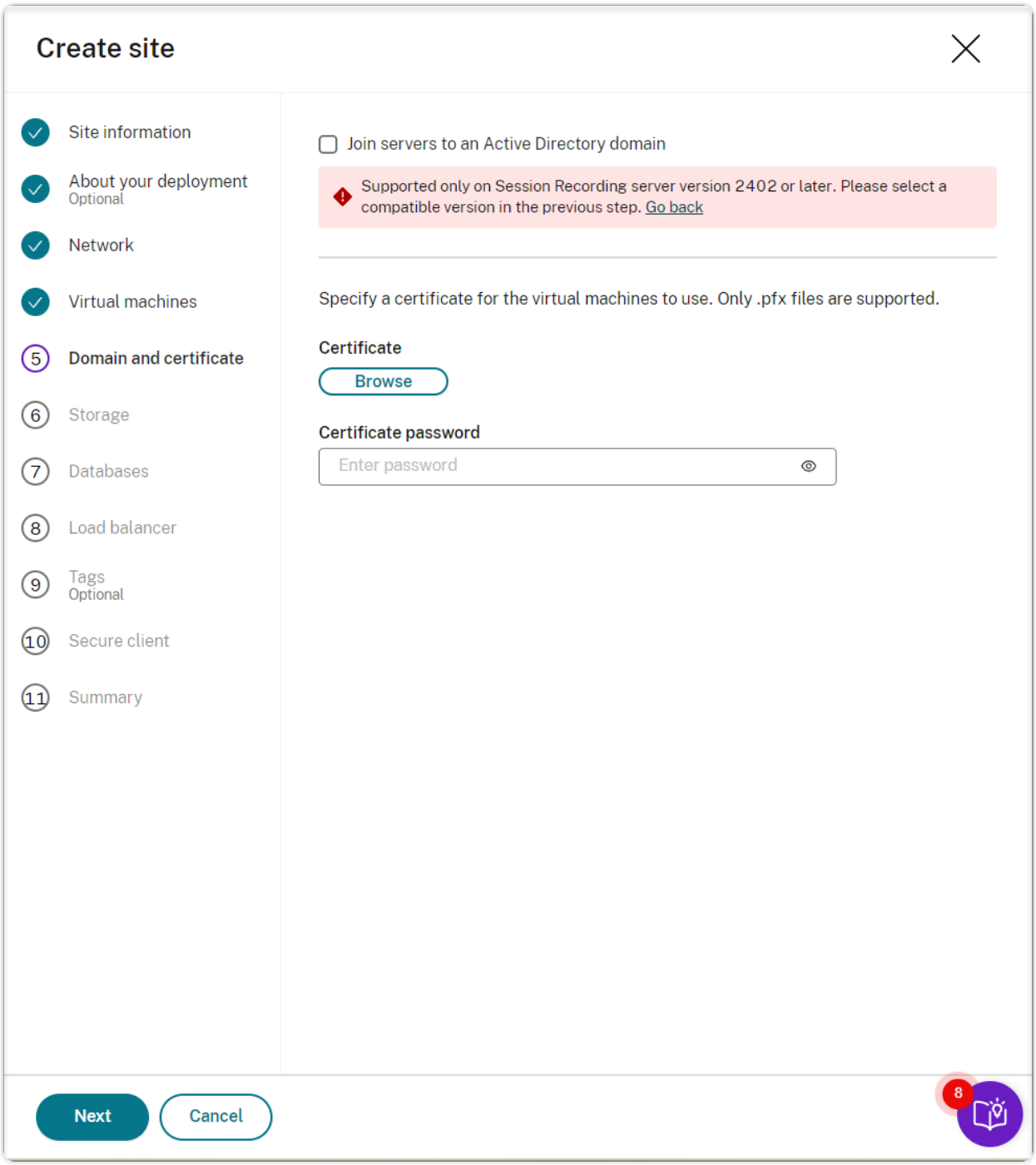
Note:

- 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.

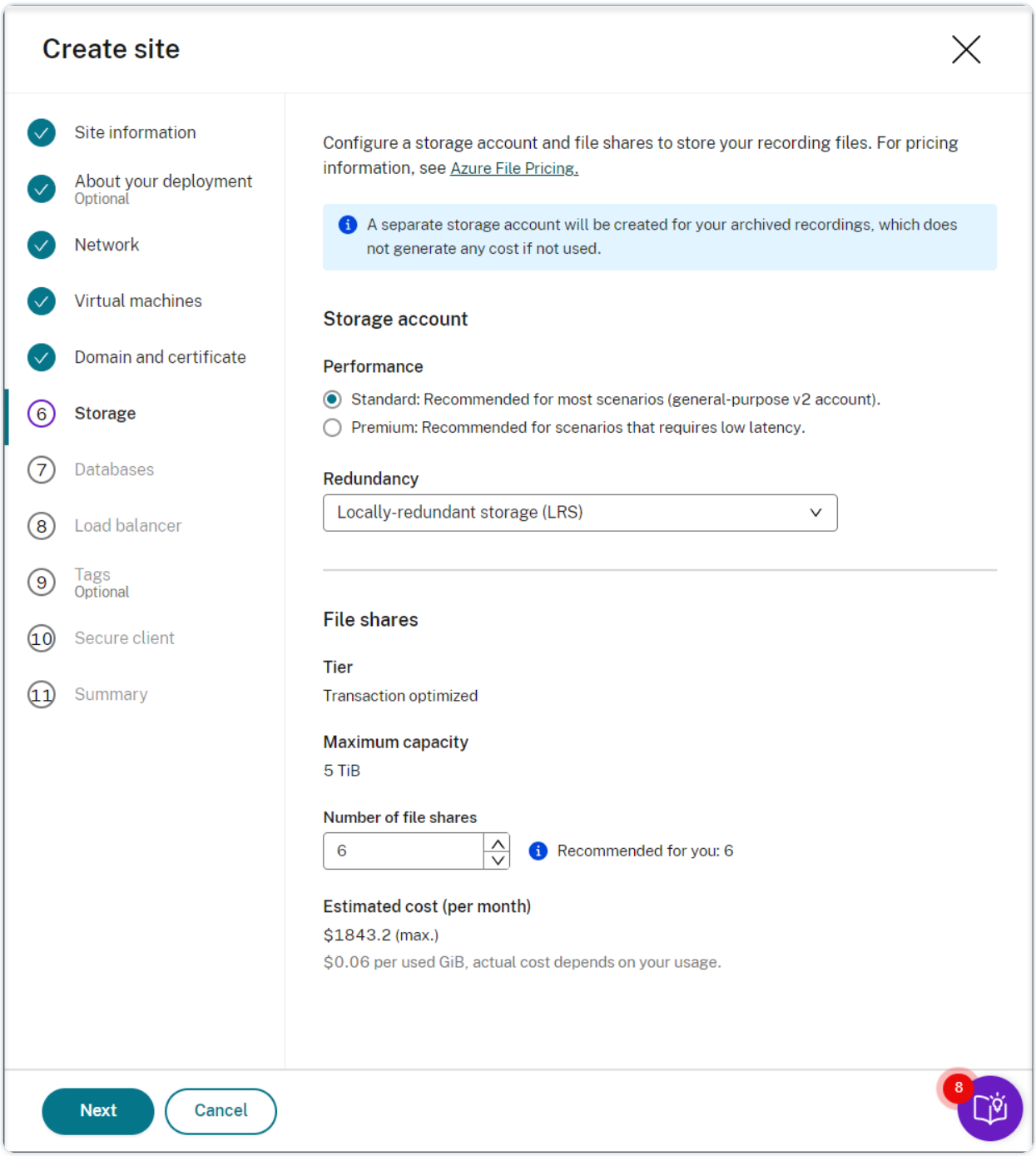

Create site
Site information
About your deployment
Optional
Network
Virtual machines
5
Domain and certificate
6
Storage
7
Databases
8
Load balancer
9
Tags
Optional
10
Secure client
11
Summary
Join servers to an Active Directory domain
This should be the domain where your VDAs reside.
Domain name
Enter 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
8



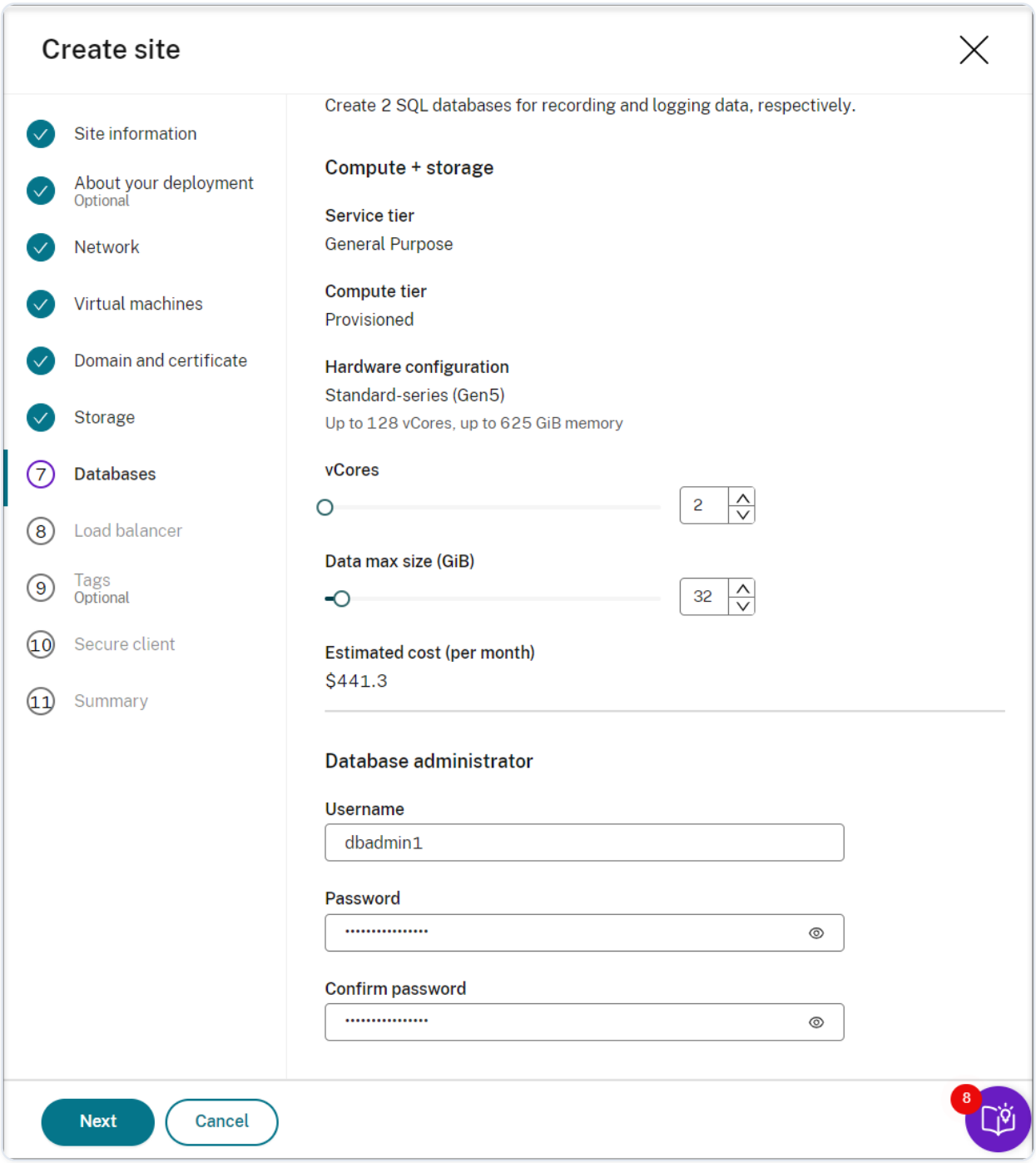
Note:

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.

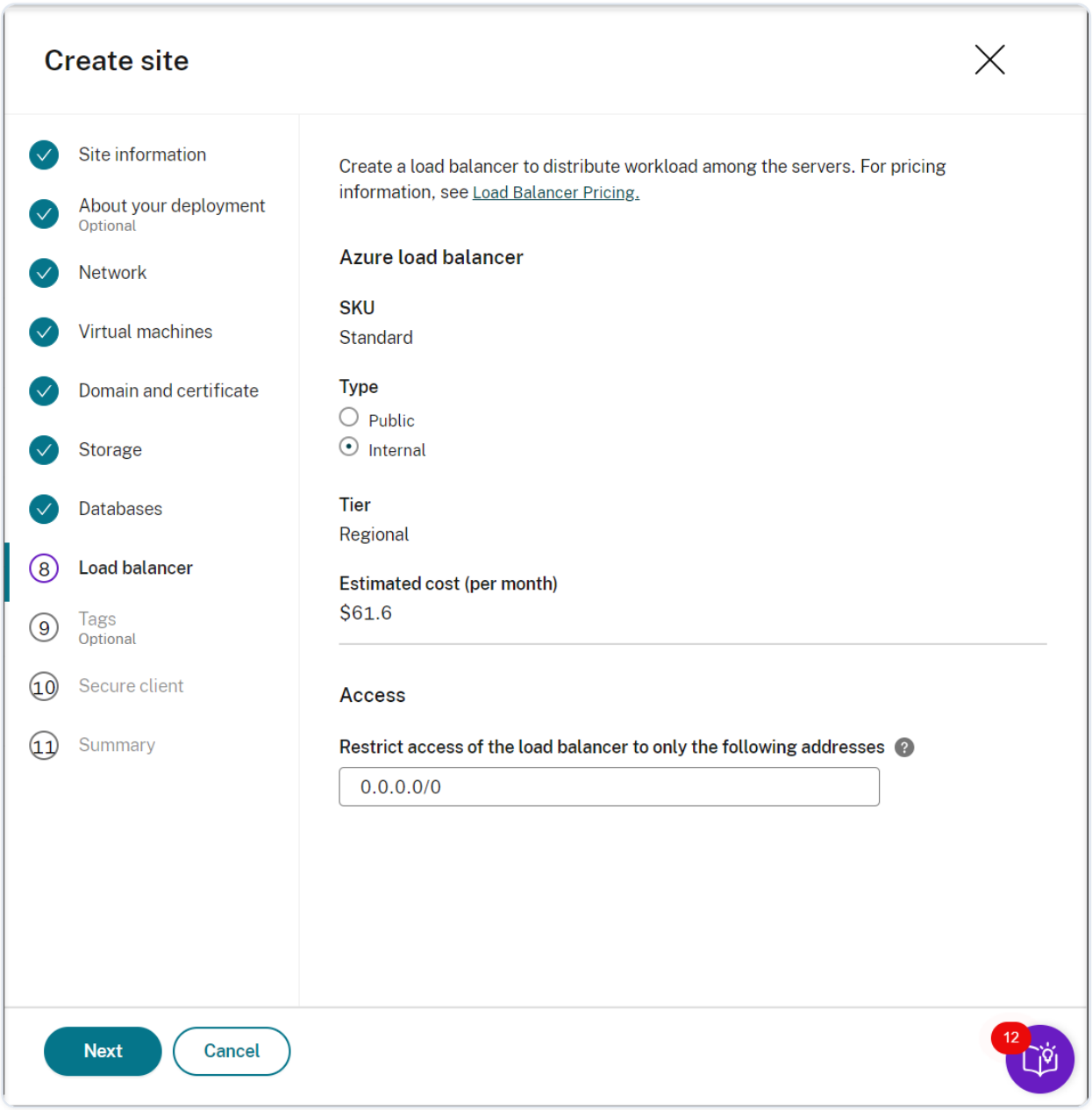
10. Configure an Azure storage account and file shares to store your recording files. For pricing information, see Azure Files pricing.



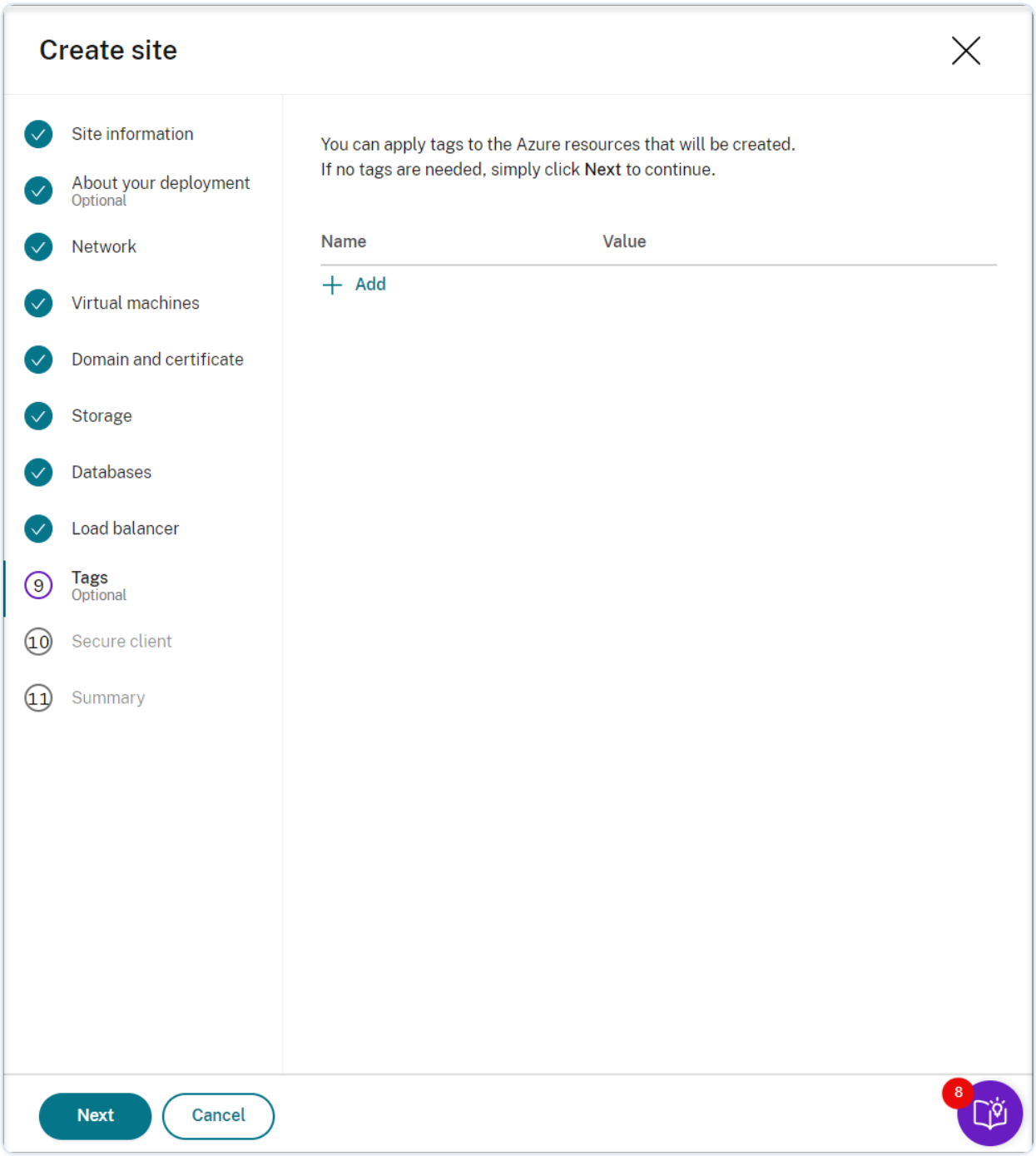
11. Create two SQL databases in Azure. One is used as the Session recording database (named **sessionrecording**) and the other as the administrator logging database (named **sessionrecordinglogging**).



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.

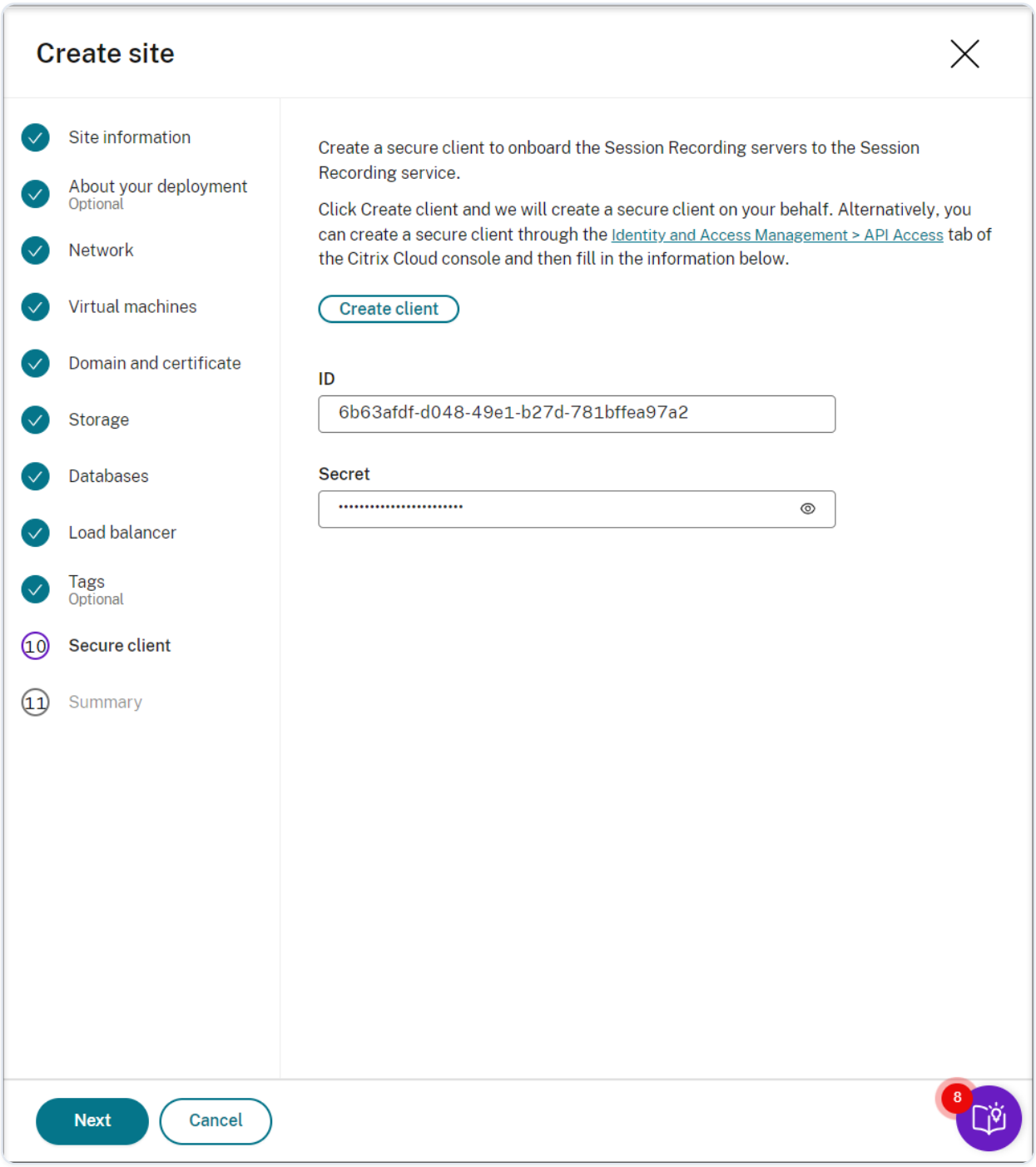


13. (Optional) Apply tags to the Azure resources to be created.

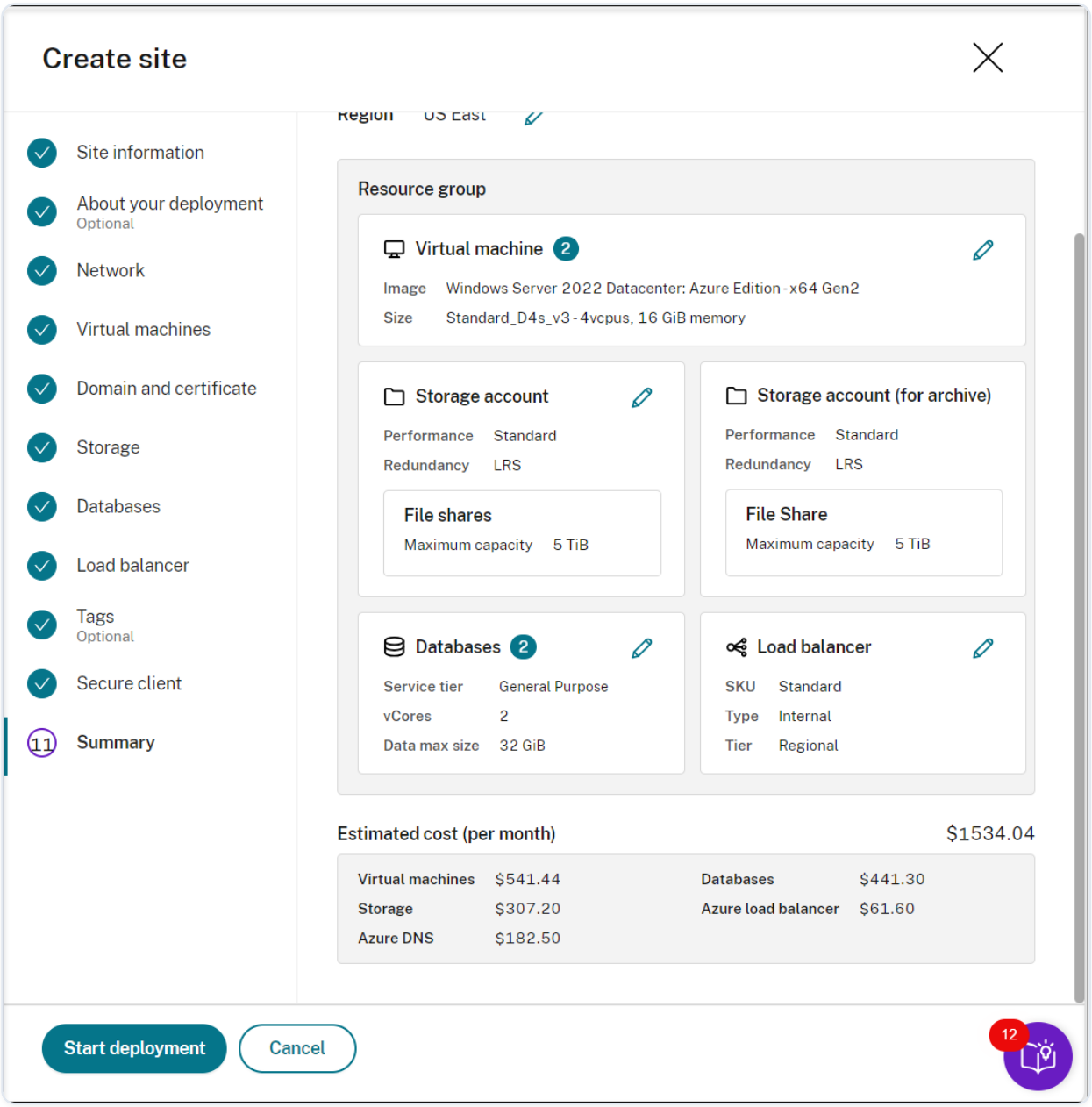


14. Create a secure client to onboard the Session Recording servers to the Session Recording service.

    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.

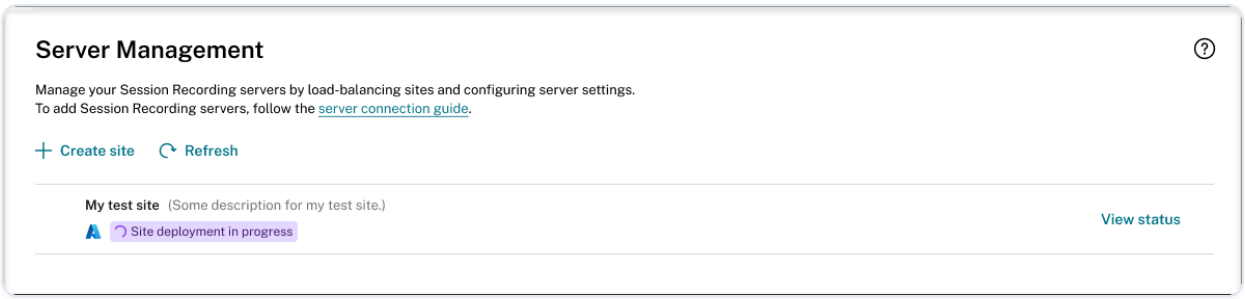


15. View the summary about the site to be created. Click the pencil icon to edit your settings if needed or click the button to start deployment.



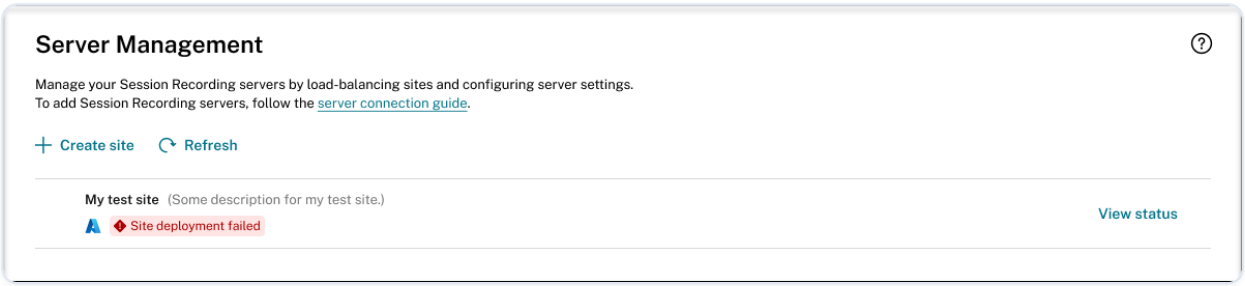
The following are examples of the deployment process:

Deployment in progress:

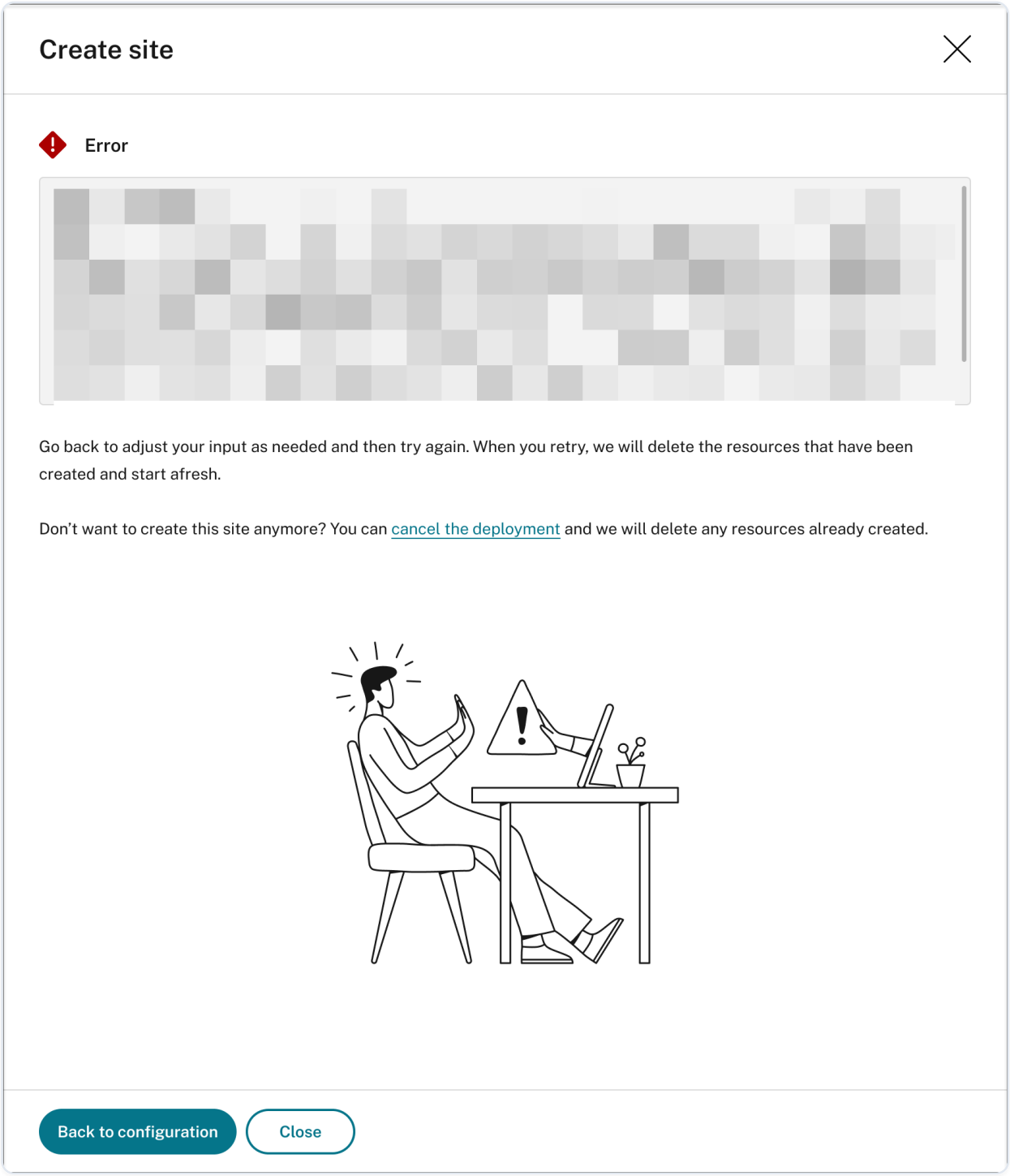


While a site deployment is in progress, you can click **View status** to view the progress.

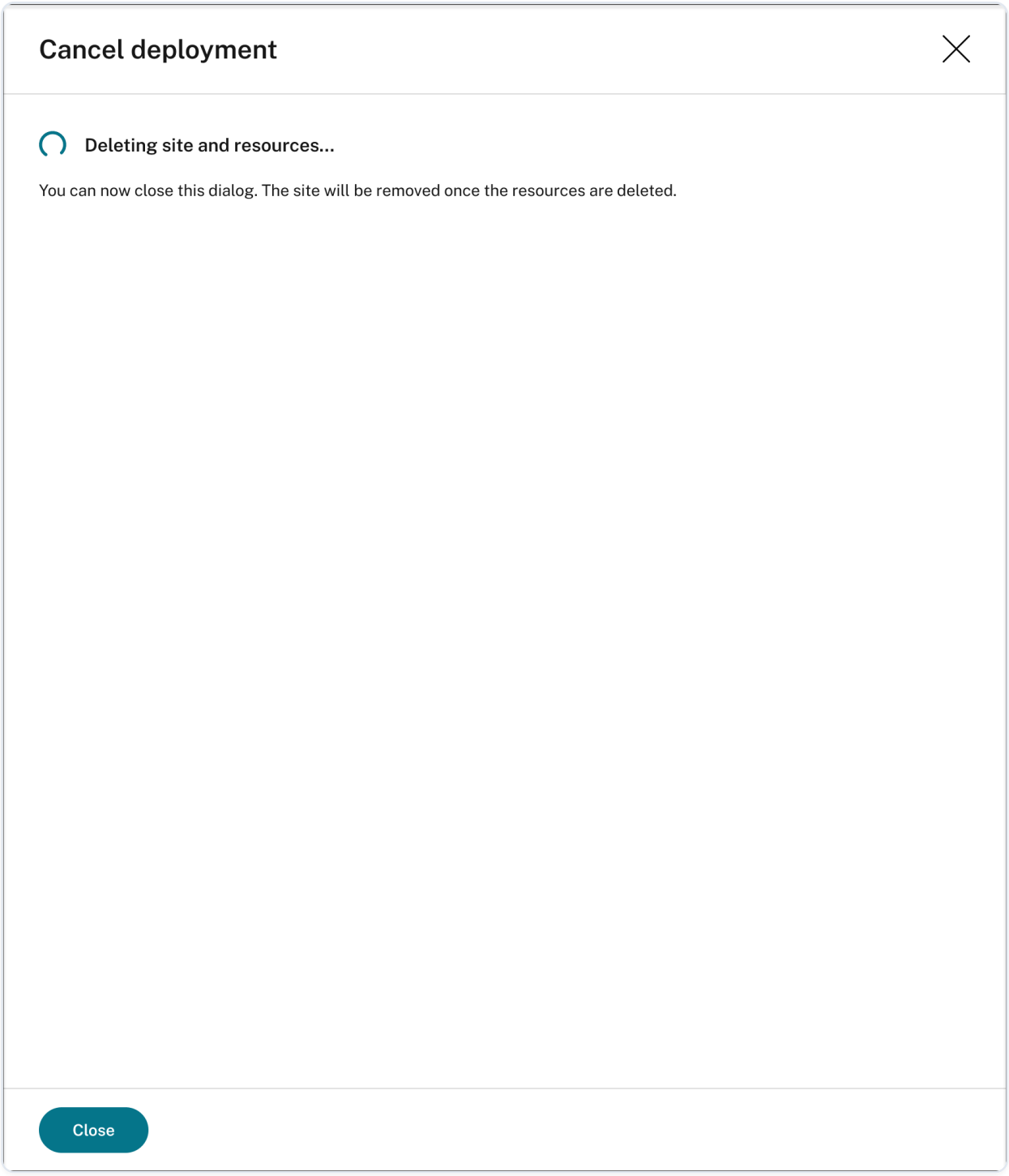
Deployment failed:



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



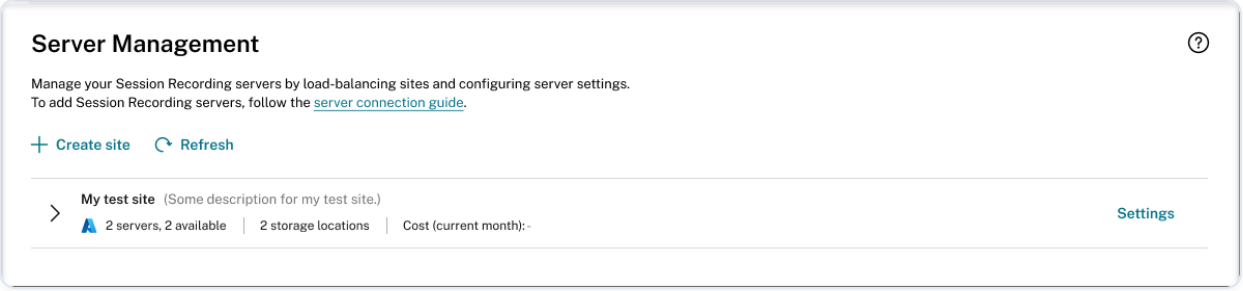
You can click **Back to configuration** or **cancel the deployment**. If you click **Back to configuration**, you're taken back to the **Create Site** page where you can alter your configurations and try again. If you're sure to cancel the deployment, follow the wizard to remove the site and the Azure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

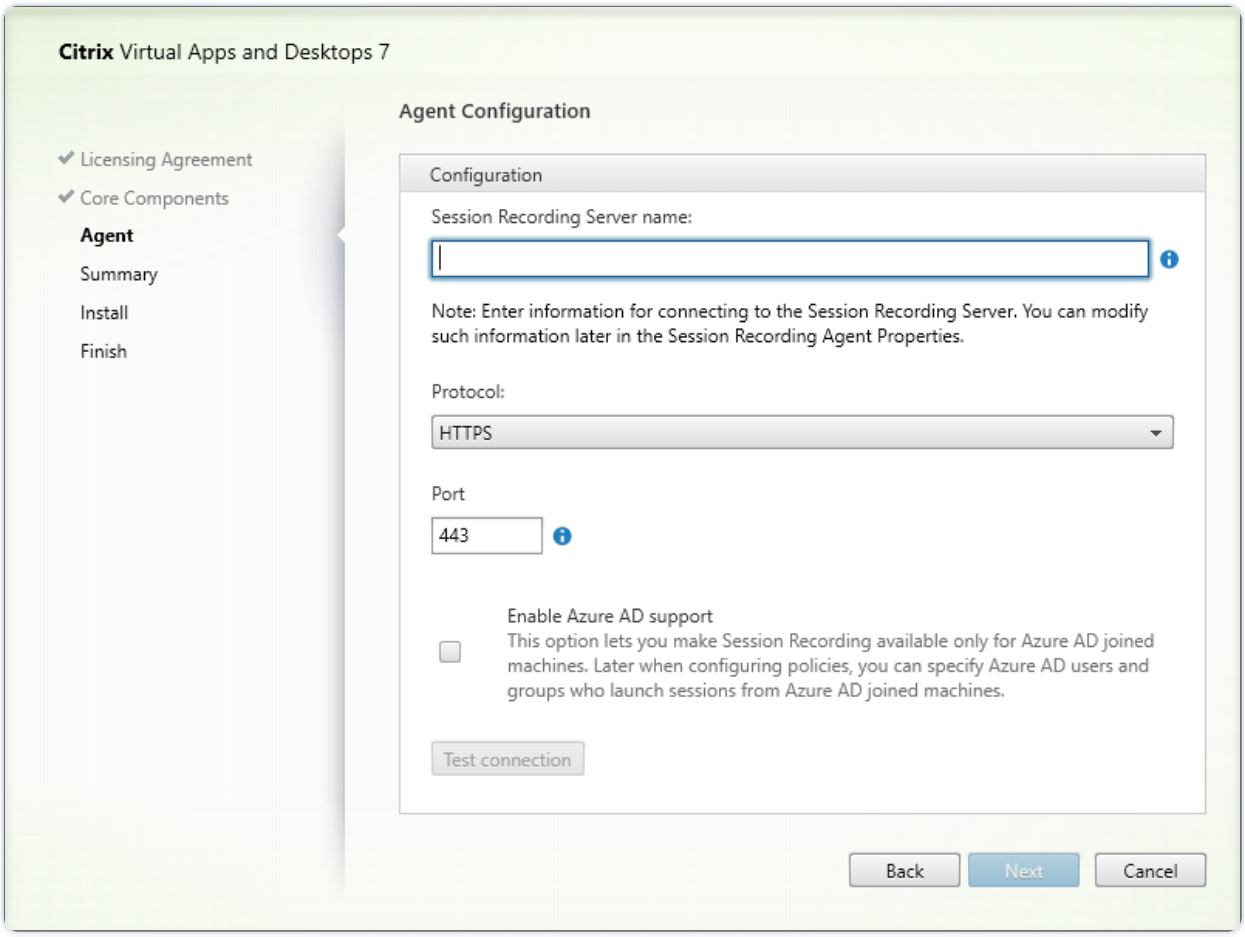


Keep a record of the storage location and the DNS name listed in the load balancer section. The DNS name will serve as the Session Recording server name that you need to fill in later for communicating with the VDAs.

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

The troubleshooting information contains solutions to issues that might occur when you use the Session Recording service, for example:

- Diagnostic logging
- Server troubleshooting from the cloud
- Servers not seen in the cloud

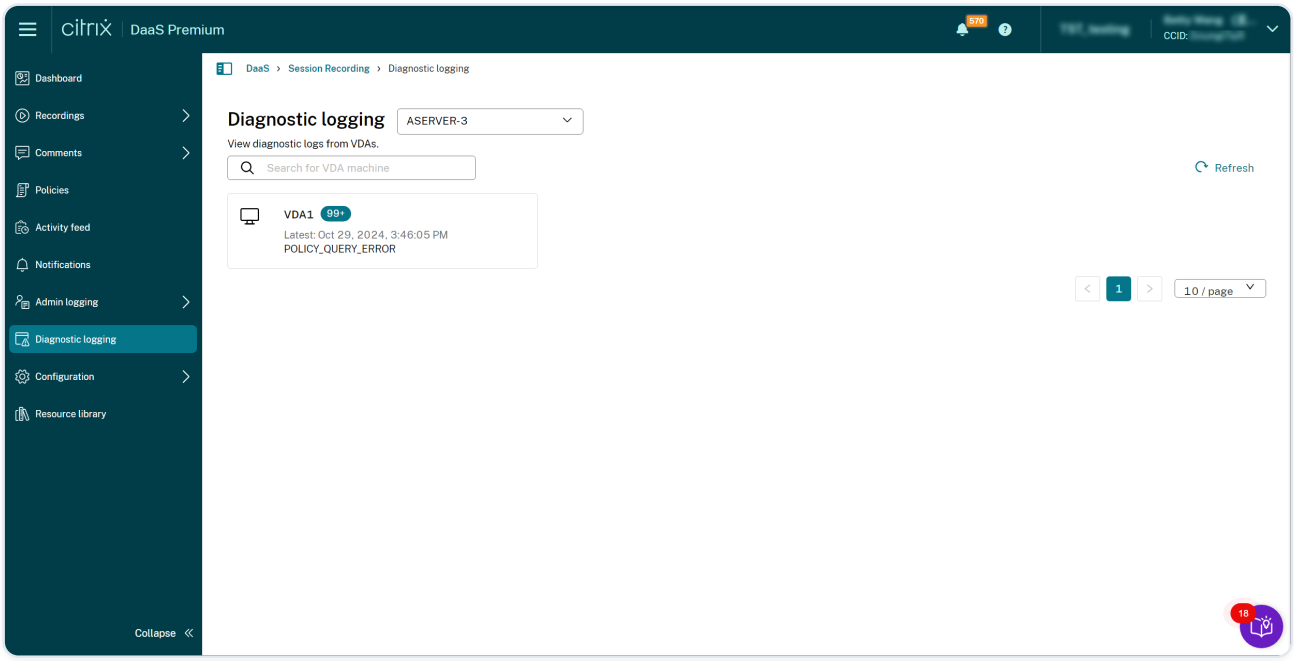
Diagnostic logging

Overview

Issues detected on the VDAs (such as message queue quota exceedance) can be sent to the Session Recording service as diagnostic logs for display.

> **Note:**
>
> Diagnostic logging is available and enabled by default with Session Recording 2411 and later.

> For an example diagnostic logging view, see the following screen capture:



Message queue quota exceedance

In any of the scenarios outlined below, there's a chance of exceeding the maximum size of the Microsoft Message Queuing (MSMQ) directory on a VDA, resulting in packet drops or pushback.

- On the VDA side, the incoming rate of Message Queuing messages exceeds the outgoing rate.
- The network connection between the VDA and the Session Recording server is poor and thus messages are stuck in the queue on the VDA side.
- The queue quota on the Session Recording server side is used up and messages are stuck in the queue on the VDA side.

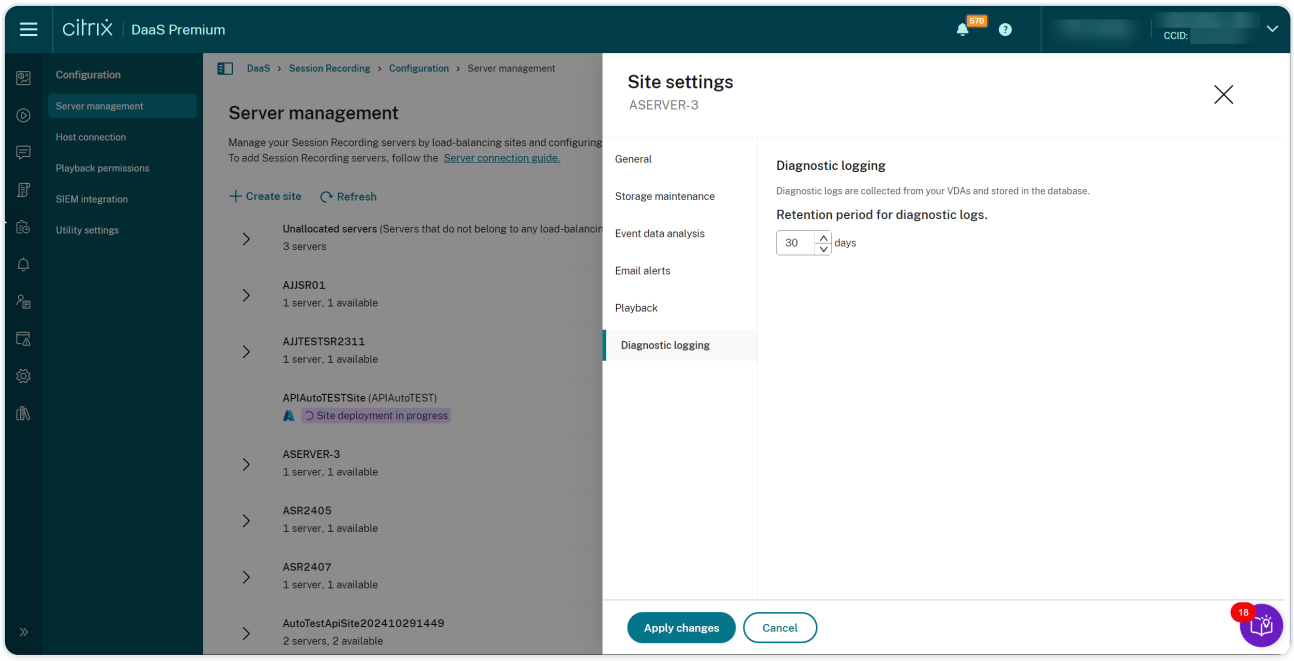
Configuration

Diagnostic logging is enabled by default. You can disable and re-enable the feature by using the following registry value on the target VDA:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent\DiagnosticLoggingEnabled

Value data: 1 = enabled, 0 = disabled

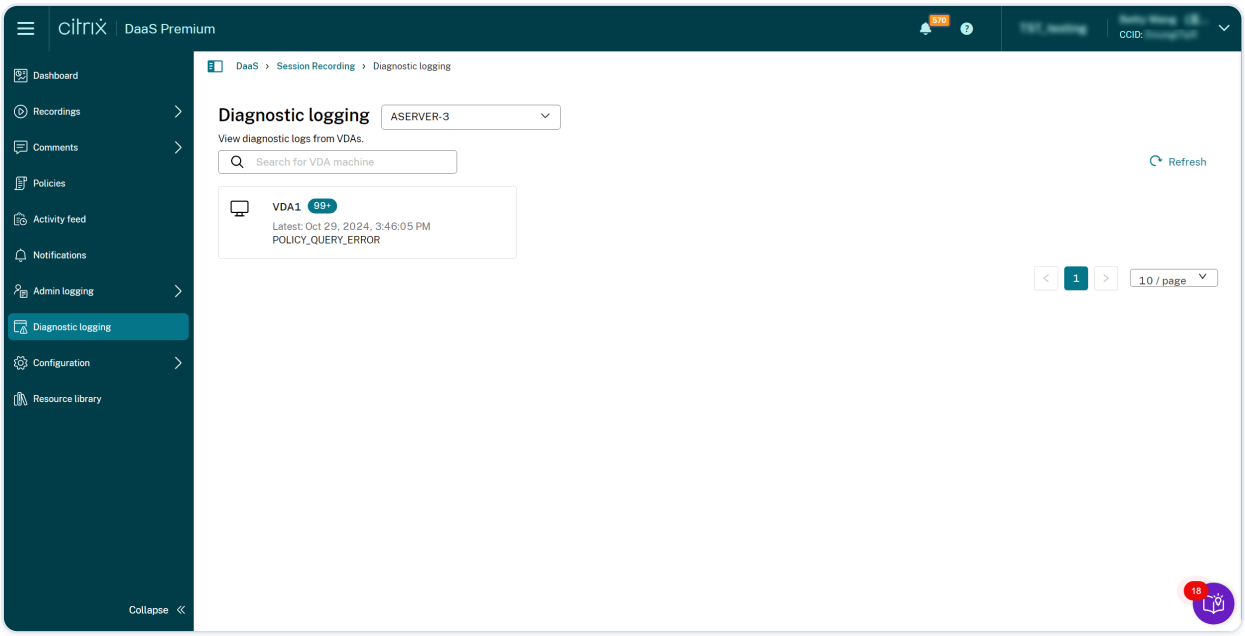
You can also set how long these logs can be retained on the Session Recording database. To do so, go to the site settings for the target site and configure the retention period for diagnostic logs. The default value is 30 days.



View diagnostic logging

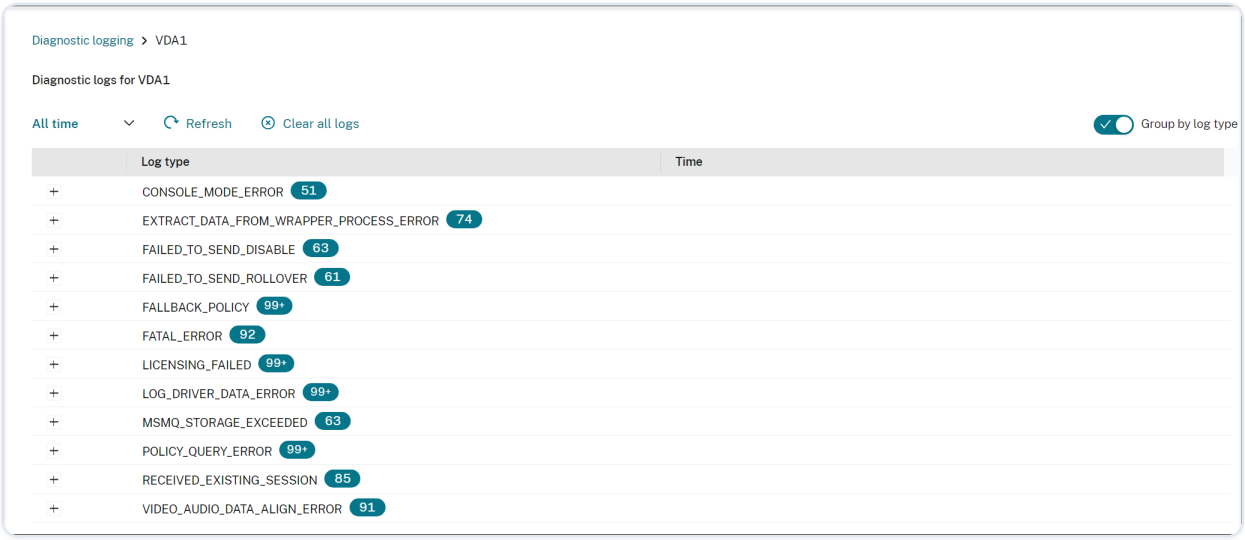
1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.
3. In the DaaS tile, scroll down in the left navigation pane and select **Session Recording**. You can hover over and pin the **Session Recording** menu to the top **PINNED** section of the navigation pane for quick access. You can reorder pinned menus by dragging them to the desired places.
4. In the Session Recording service view, select **Diagnostic logging** from the left navigation.

   All VDAs with diagnostic logs are presented and sorted by their total log counts. You can also view the time the latest log is generated on each VDA and click **Refresh** to check for more incoming logs.



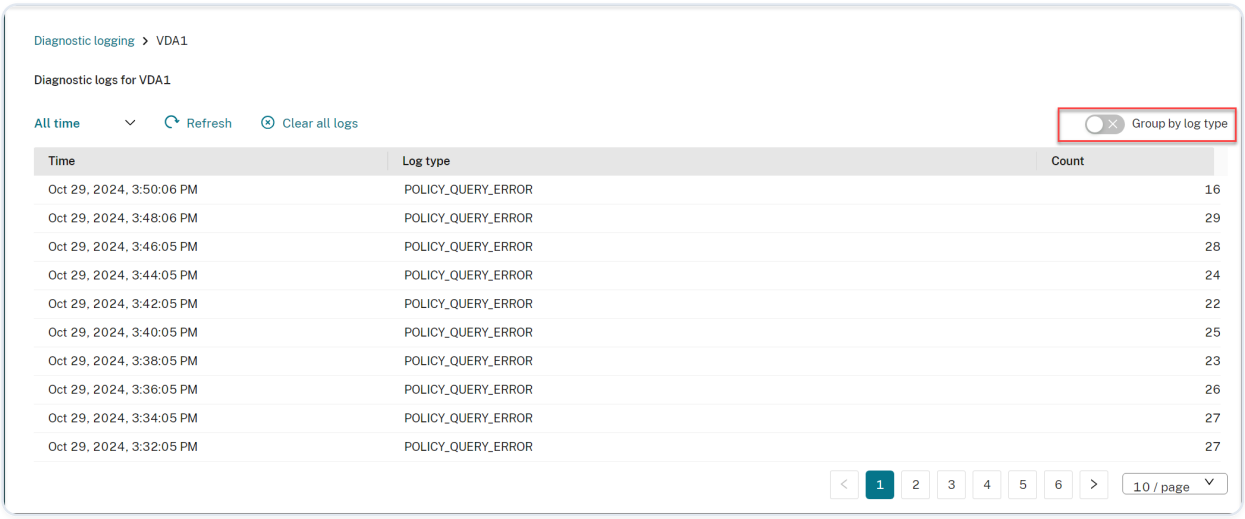
5. Click a target VDA to view its diagnostic logs.

   By default, logs are grouped by type. For example:

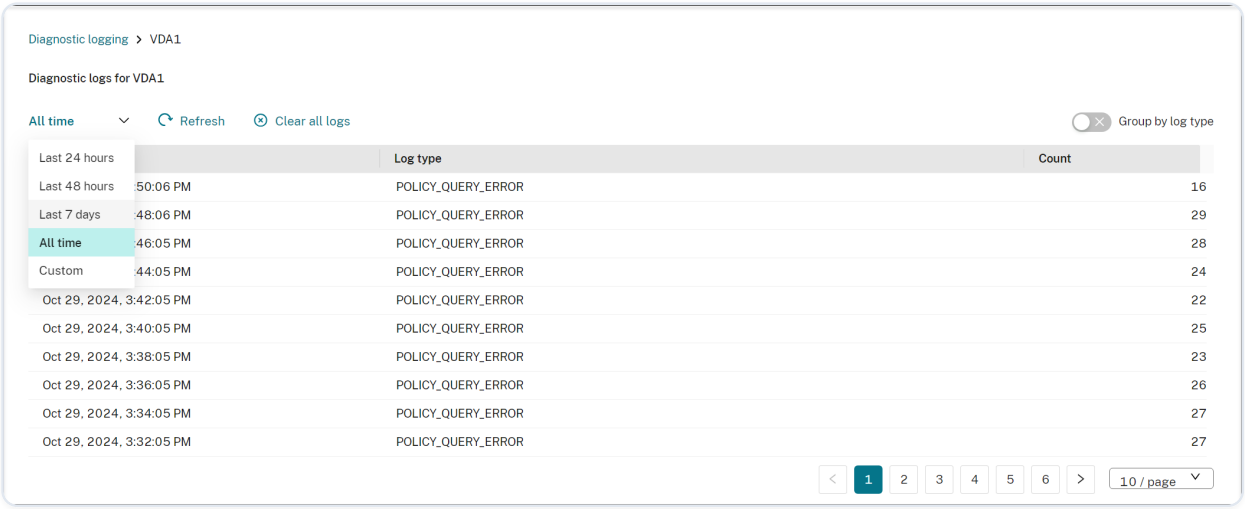


   You can disable log grouping by type and list all logs in chronological order instead.

   For example:



6. Use the time filter to select and view logs generated during the specified time frame.



7. To check for any incoming logs, click **Clear all logs** to hide the currently displayed logs, and then click **Refresh**.

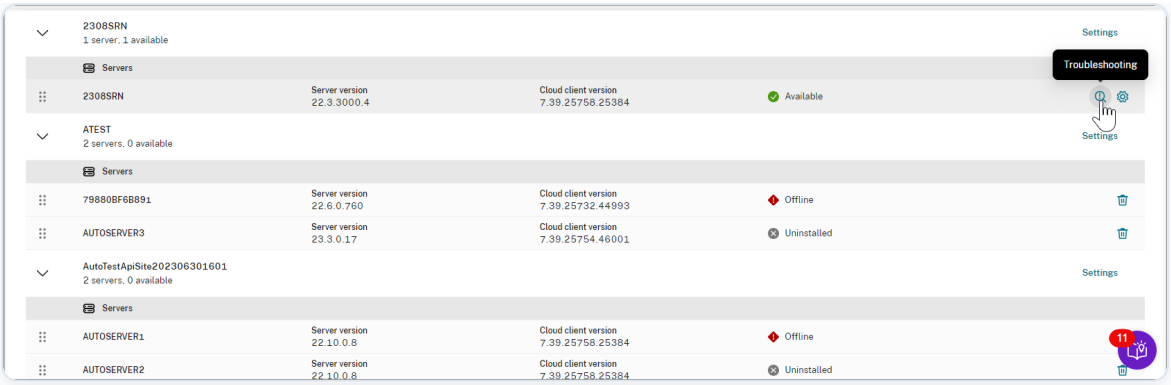
Server troubleshooting from the cloud

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.

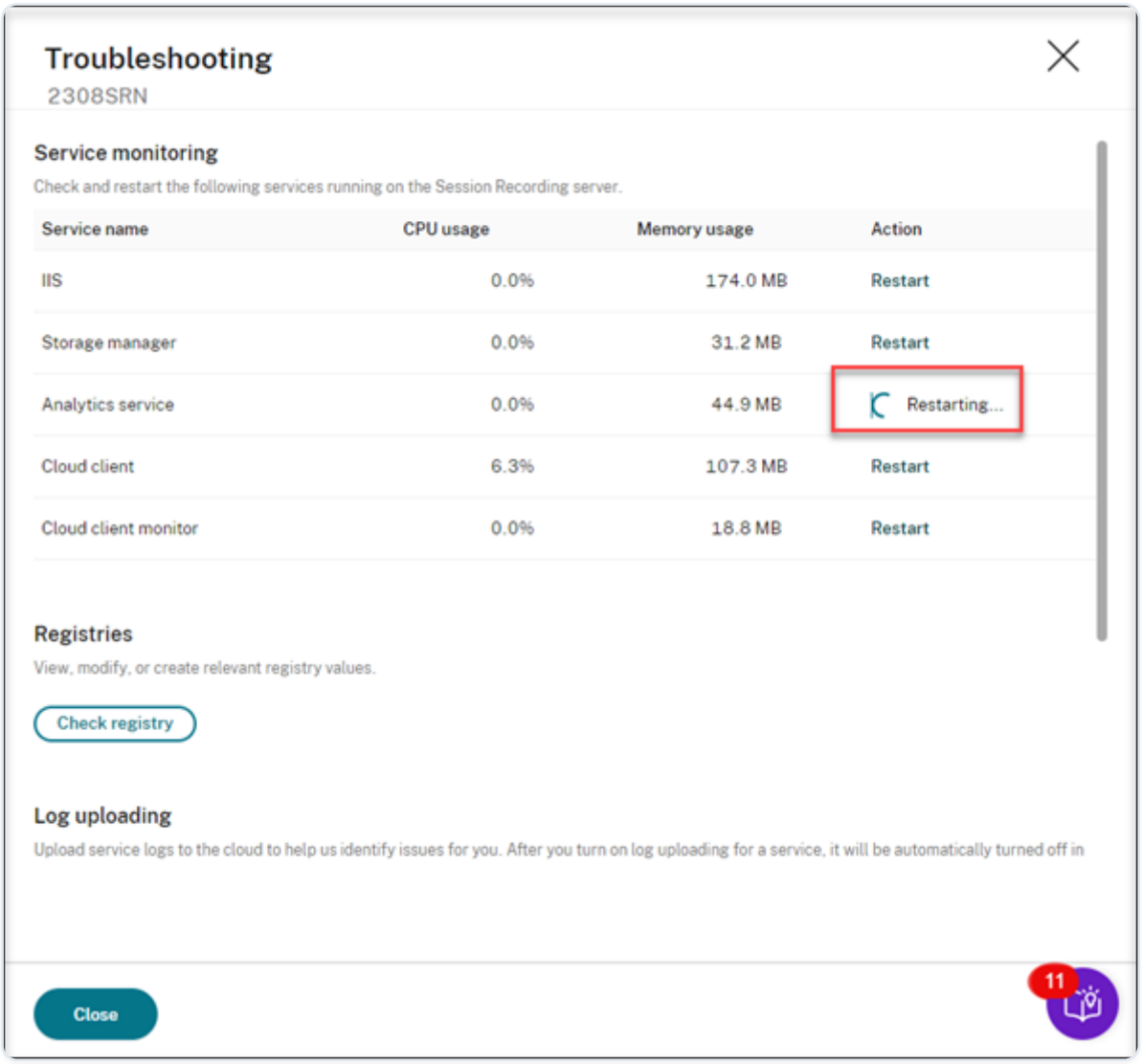


3. Perform the following troubleshooting actions on the target server as needed :

   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 (CitrixSsRecCloudClientMonitorService).

      For example:

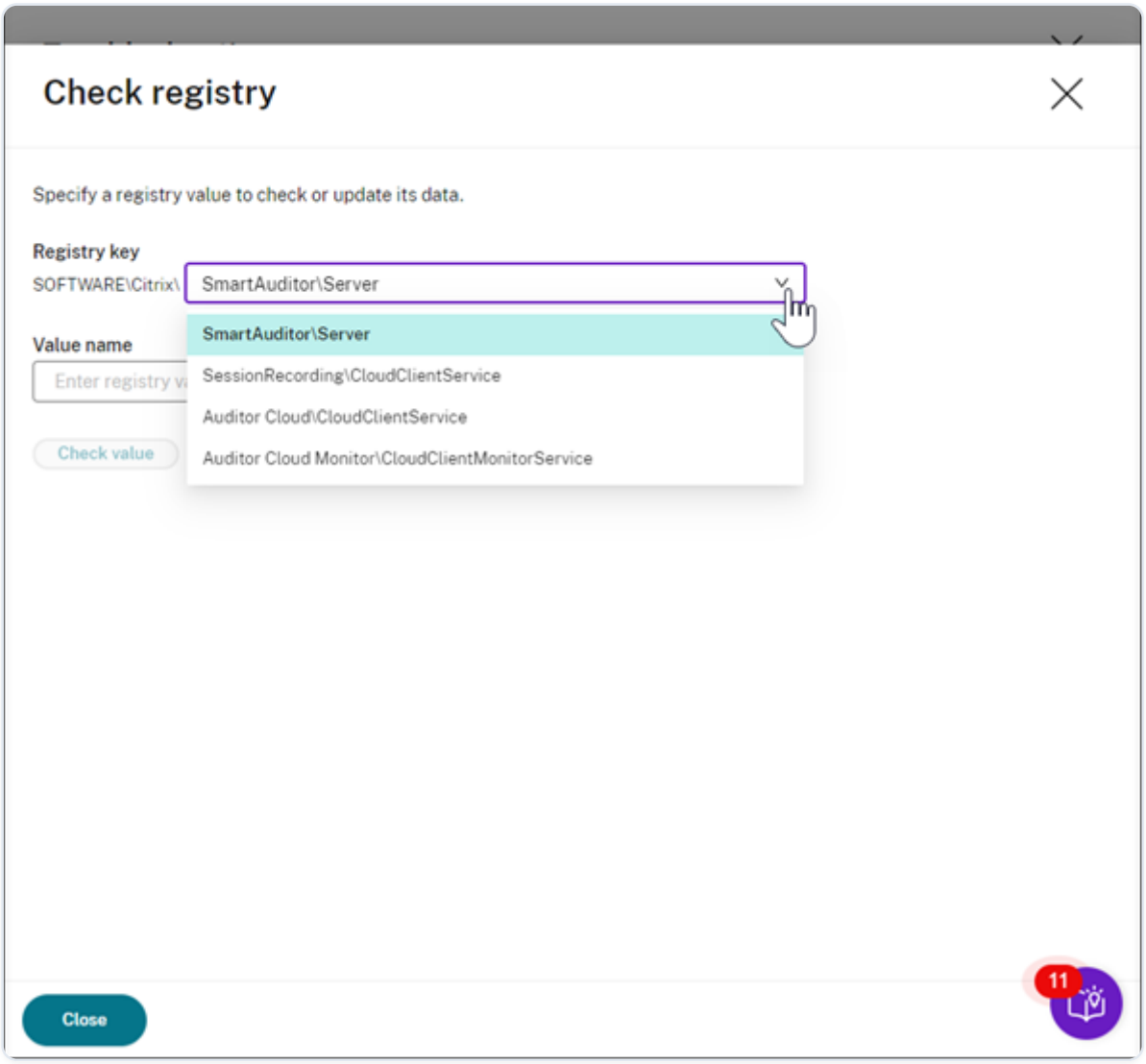


If you restart a service successfully, the **Restarted** status initially appears and then the **Restart** button is displayed.

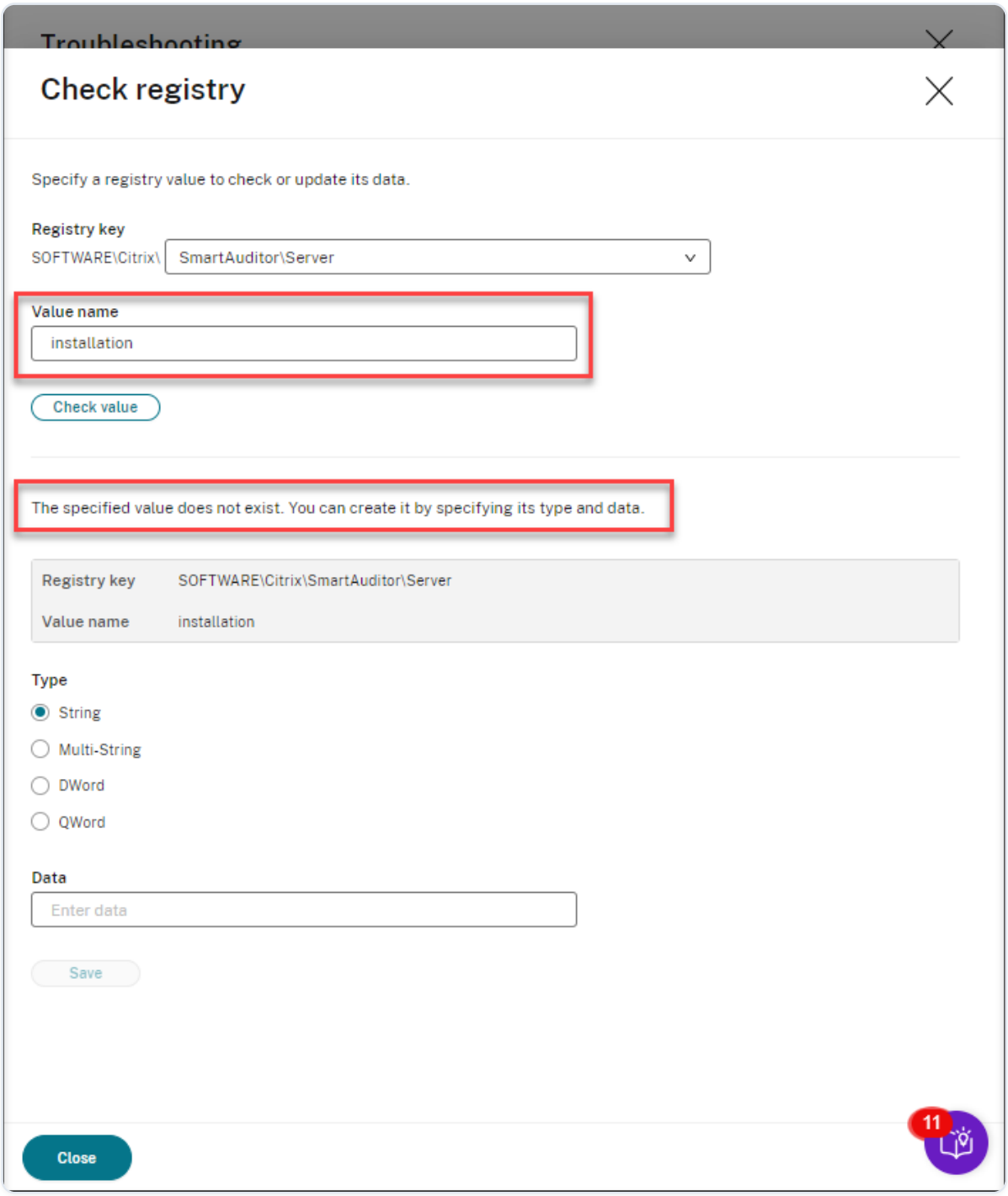
If your attempt to restart a service is unsuccessful, the **Failed** status initially appears and then the **Restart** button is displayed.

b. In the **Registries** section, click **Check Registry** to view, modify, and create relevant registry values.

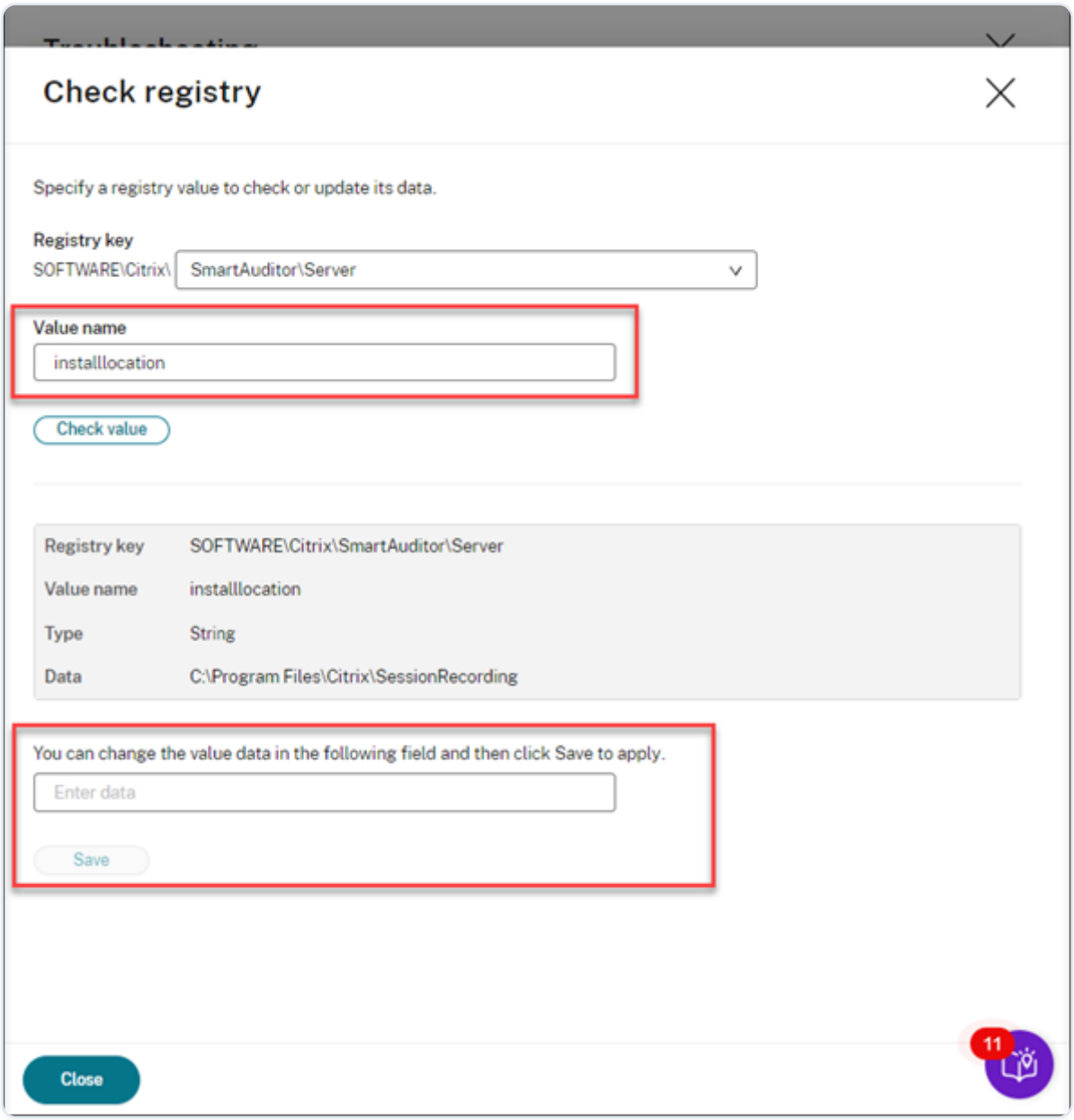
   Select a registry key from the drop-down list.



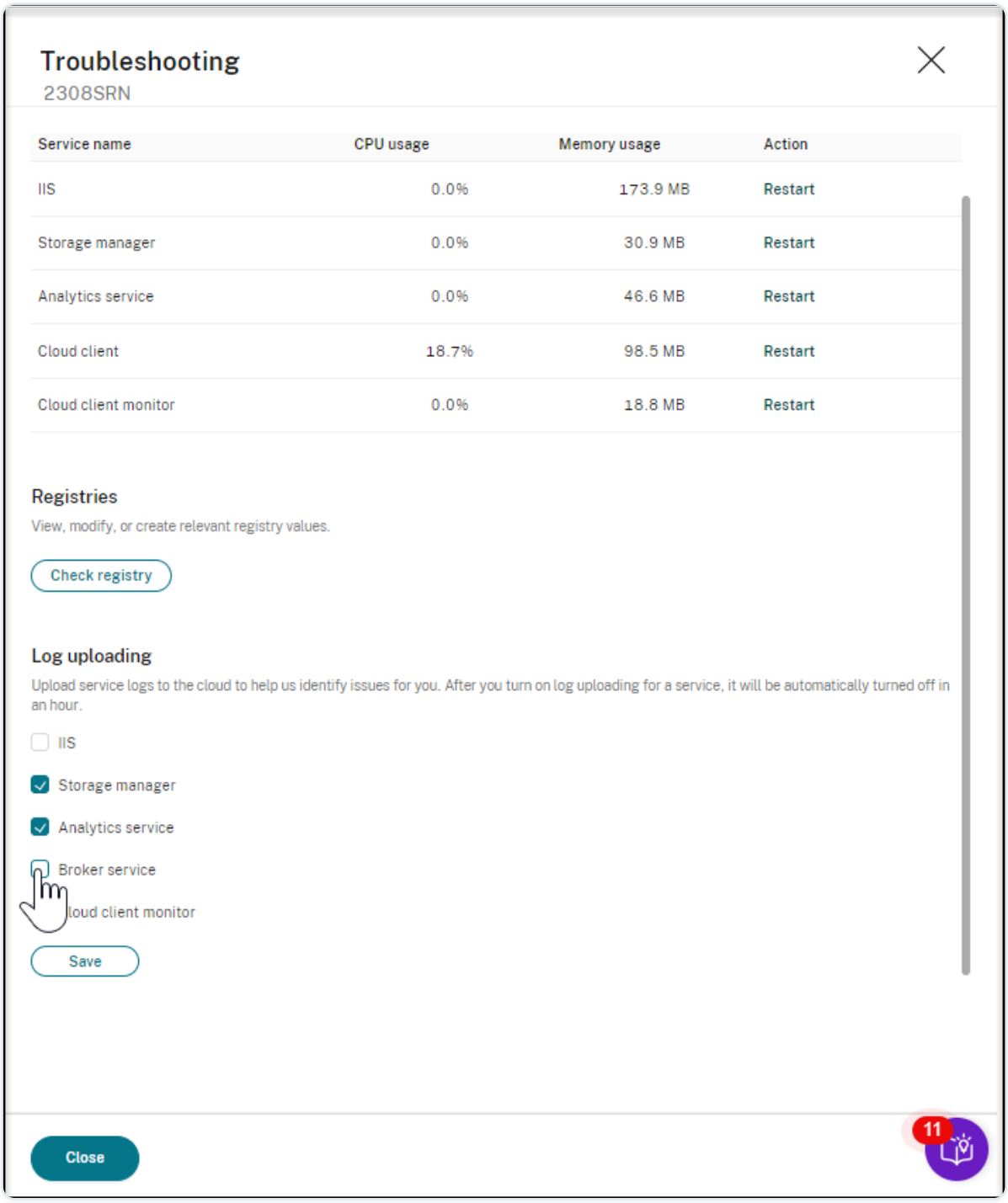
Enter a registry value to check whether it exists. If a registry value you enter does not exist, you can create it as needed by following the instructions.



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

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:

```
# Copyright (c) Citrix Systems, Inc.  All rights reserved.



<#

    .SYNOPSIS

    This script is used to check whether or not port 443 is open.

    Note: Execute this script from the machine where you installed the
cloud client.

#>



$SR_CLOUD_DOMAIN = "srs.apps.cloud.com"

function Check-PortStatus {







    $ctResult = tnc  $SR_CLOUD_DOMAIN  -port 443

    if($ctResult.TcpTestSucceeded -ne $True) {

        Write-Host "Error : $SR_CLOUD_DOMAIN : $_ is unreachable"
-ForegroundColor Red

    }
```

```
    else {

        Write-Host "$SR_CLOUD_DOMAIN : 443 is open" -ForegroundColor
Green

    }

}



Check-PortStatus
```

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:

```
# Copyright (c) Citrix Systems, Inc.  All rights reserved.



<#

    .SYNOPSIS

    This script is used to check whether or not ports
8088,443,9090,9091,9092,9093,and 9094 are open.

    Note: Execute this script from the machine where you installed the
```

```
cloud client.

#>



$SR_CLOUD_DOMAIN = "sessionrecording.apps.cloud.com"

function Check-PortStatus {

       (8088,443,9090,9091,9092,9093,9094) | ForEach-Object {

           $ctResult = tnc  $SR_CLOUD_DOMAIN  -port $_

           if($ctResult.TcpTestSucceeded -ne $True) {

            Write-Host "Error : $SR_CLOUD_DOMAIN : $_ is unreachable"
-ForegroundColor Red

           }

           else {

            Write-Host "$SR_CLOUD_DOMAIN : $_ is open" -ForegroundColor
Green

           }

       }

}



Check-PortStatus
```

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.

Session Recording service document history

The following table describes important changes to the Session Recording service product documentation. To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	DESCRIPTION
11 Mar 2025	Release	For a summary of new features, see What's new.
15 Nov 2024	Release	For a summary of new features, see What's new.
26 Jul 2024	Release	For a summary of new features, see What's new.
19 Jun 2024	Added an article	See Integrate with Citrix HDX plus for Windows 365 in a Session Recording deployment.
26 Apr 2024	Release	For a summary of new features, see What's new.
12 Mar 2024	Added a known issue	See Known issues.
30 Jan 2024	Release	For a summary of new features, see What's new.
31 Oct 2023	Release	For a summary of new features, see What's new.
06 Sep 2023	Release	For a summary of new features, see What's new.
20 Jul 2023	Release	For a summary of new features, see What's new.

SESSION RECORDING SERVICE

DATE	CHANGE	DESCRIPTION
28 Apr 2023	Release	For a summary of new features, see What's new.
16 Feb 2023	Release	For a summary of new features, see What's new.
11 Dec 2022	Release	For a summary of new features, see What's new.
09 Nov 2022	Added an article	See Administrator role management.
08 Nov 2022	Release	For a summary of new features, see What's new.
20 Sep 2022	Release	For a summary of new features, see What's new.
28 Jul 2022	Release	For a summary of new features, see What's new.
16 Jun 2022	Release	For a summary of new features, see What's new.
26 Apr 2022	Release	For a summary of new features, see What's new.
01 Apr 2022	Release	Initial release of the Session Recording service