Session Recording 2305

> **Important:**
>
> The product lifecycle strategy for Current Releases (CR) and Long Term Service Releases (LTSR) is described in Lifecycle Milestones.

Session Recording records, catalogs, and archives sessions for retrieval and playback.

Session Recording provides flexible policies to trigger recordings of application and desktop sessions automatically. Session Recording also supports dynamic session recording. Session Recording enables IT personnel to monitor and examine user activity, and so supports internal controls for regulatory compliance and security monitoring. Similarly, Session Recording also aids in technical support by speeding problem identification and time-to-resolution.

Benefits

Enhanced security through logging and monitoring. Session Recording allows organizations to record on-screen user activity for applications that deal with sensitive information, monitoring and preventing the leakage of sensitive information from virtual sessions. Prevention of sensitive information leakage is especially critical in regulated industries such as healthcare and finance.

Powerful activity monitoring. Session Recording captures and archives screen updates, including mouse activity and visible output of keystrokes to provide a record of activity for specific users, applications, and servers.

Session Recording isn't designed for the evidence collection for legal proceedings. However, organizations can use Session Recording together with other techniques for evidence collection, such as conventional video records combined with traditional text-based eDiscovery tools.

Faster problem resolution. When users call with a problem that is difficult to reproduce, help desk support staff can enable recording of user sessions. If the issue recurs, Session Recording provides a time-stamped visual record of the error, which can then be used for faster troubleshooting.

What's new

What's new in 2305

This release includes the following new features and addresses issues to improve the user experience:

Support for Azure SQL Database

You can now install the Session Recording database on Azure SQL Database.

For more information, see Install the Session Recording database on Azure SQL Database. For a complete list of the operating systems and database services that you can install the Session Recording database on, see System requirements.

Support for sharing recordings as unrestricted links

In the Session Recording web player, you can now share recordings as unrestricted links so that anyone in your AD domain can access the recordings using the links.

To facilitate managing unrestricted links, Session Recording 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.

For more information, see Share recordings as links.

Configure Session Recording timespan for blocking sensitive information disclosure

Session Recording allows you to bypass specified periods when recording the screen to prevent sensitive information from being disclosed. The sensitive information blocking capability is enabled by using the **Session-Pause** and **Session-Resume** cmdlets. This release enhances the feature by allowing you to configure the amount of time of the screen recording you want to skip before sensitive information is detected. The default value is 1 second. For more information, see Sensitive information blocking.

Advanced filters available for ICLDB ARCHIVE and ICLDB REMOVE commands

When using the ICLDB ARCHIVE and ICLDB REMOVE commands to archive and remove session recording files, you can now set advanced filters by appending the RULES parameter. For more information, see Manage recordings.

Support for email alerts in your preferred language

You can now send email alerts even if the operating system language of your Session Recording server is not one of the following languages that Session Recording supports:

- English
- French
- German
- Spanish
- Japanese
- Simplified Chinese

If the operating system language of your Session Recording server is not one of the supported languages, email alerts are sent in English by default. You can customize a language to send email alerts in. To do so, find the email template called `template.en.html` under `<Session Recording server installation path>\Bin\templates` and then change the plain text in the template to your preferred language. For more information, see Configure event response policies.

What's new in earlier releases

For new features included in the releases that shipped after the 1912 LTSR through the 2303 CR, see What's new history.

Fixed issues

Compared with: Session Recording 2303

Session Recording 2305 adds the following fixes:

- Session Recording might not work when the HTTP or HTTPS protocol is the only one enabled.
- If you leave the delivery group query empty in the Session Recording Policy Console for non-English language versions, the query result might also be empty.
- Recording playback in the Session Recording player might freeze after two minutes, but mouse movements captured in a recording replay normally. The issue occurs when you use Session Recording 2212 or 2303.

Known issues

The following issues have been identified in this release:

- Upgrading the Session Recording server fails when "Require SSL" is enabled in IIS for the SessionRecordingBroker application and only TLS 1.2 is enabled for the server-side protocol on the SR server.

  To work around this issue, complete the following steps:

  a. **Temporarily Disable SSL**: On the Session Recording server, open IIS Manager. For the **SessionRecordingBroker** application, go to **SSL Settings** and uncheck **"Require SSL"**.

  b. **Run Upgrade**: Execute the upgrade installer for the Session Recording server.

  c. **Re-enable SSL**: After the upgrade completes, go back to the **SSL Settings** in IIS and re-check **"Require SSL"** for the **SessionRecordingBroker** application.

- If you are using Citrix Web App Firewall (WAF) signatures to mitigate in part the CVE-2021-44228 vulnerability, Session Recording might not work as expected. To resolve the issue, exclude the IP addresses of your Session Recording servers from the **mitigate_cve_2021_44228** policy on the NetScaler side.
- When you upgrade Session Recording to the latest version, your image resolution scaling settings for lossy video codec are lost and the default value 1.0 is restored.
- A domain user with local administrator privileges on the Session Recording policy console can add local and domain users to which the action of a policy rule applies. However, a local user with local administrator privileges can add only local users but not domain users.

- The web player might not work properly if you upgrade it from Version 2009 or earlier. To work around the issue, clear your browser cache.
- Rules of custom policies might be lost after you update Session Recording from the version included in XenApp and XenDesktop 7.6 LTSR to the latest version. As a workaround, update the software to the version included in the latest CU of XenApp and XenDesktop 7.15 LTSR and then update it to the latest release.
- When Machine Creation Services™ (MCS) or Citrix Provisioning (PVS) creates multiple VDAs with Microsoft Message Queuing (MSMQ) installed, those VDAs can have the same `QMId`. This condition might cause various issues, for example:
  - Sessions might not be recorded even if the recording agreement is accepted.
  - The Session Recording server might not be able to receive session-logoff signals and therefore, sessions might always be in a live state.

  For information about a workaround, see Install, upgrade, and uninstall.

Third party notices

Session Recording Version 2305 (PDF Download)

This release of Session Recording can include third party software licensed under the terms defined in this document.

What's new history

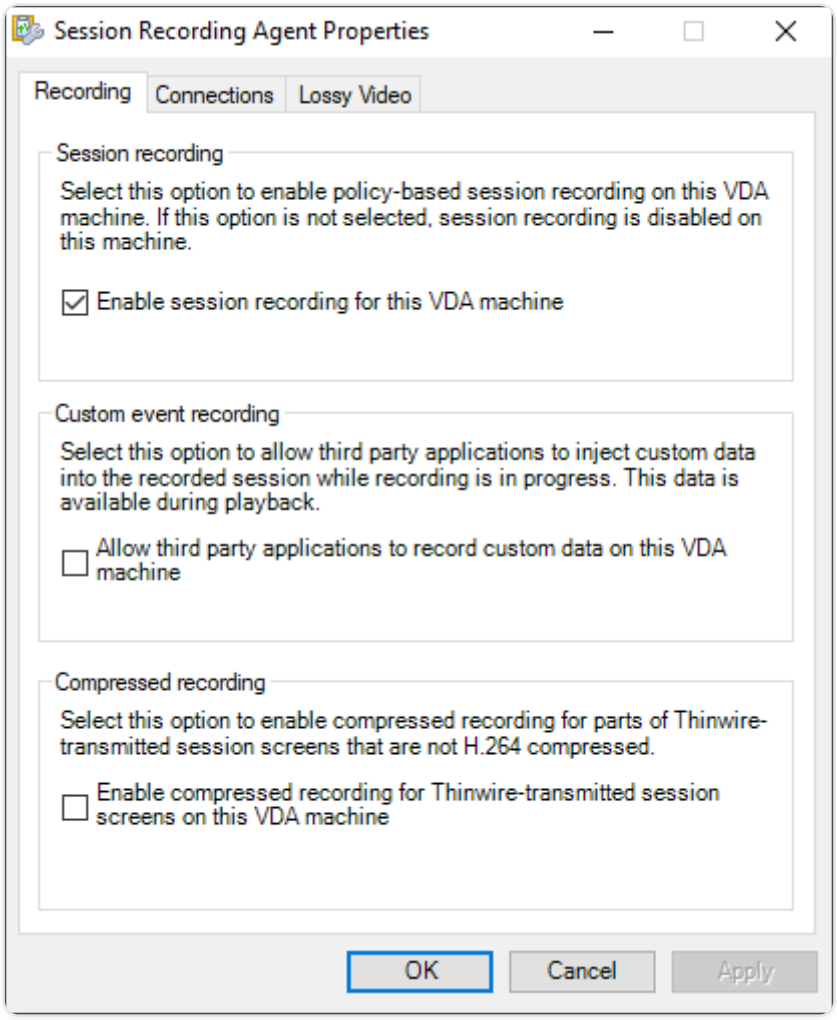
This article provides information about new features included in the releases that shipped after the 1912 LTSR through the 2303 CR.

What's new in 2303

This release includes the following new features and addresses issues to improve the user experience:

Compressed recording

You can enable compressed recording for parts of Thinwire-transmitted session screens that are not H.264 compressed. This feature reduces recording file size significantly. To enable this feature, go to the **Recording** tab of **Session Recording Agent Properties** and select the check box in the **Compressed recording** section.



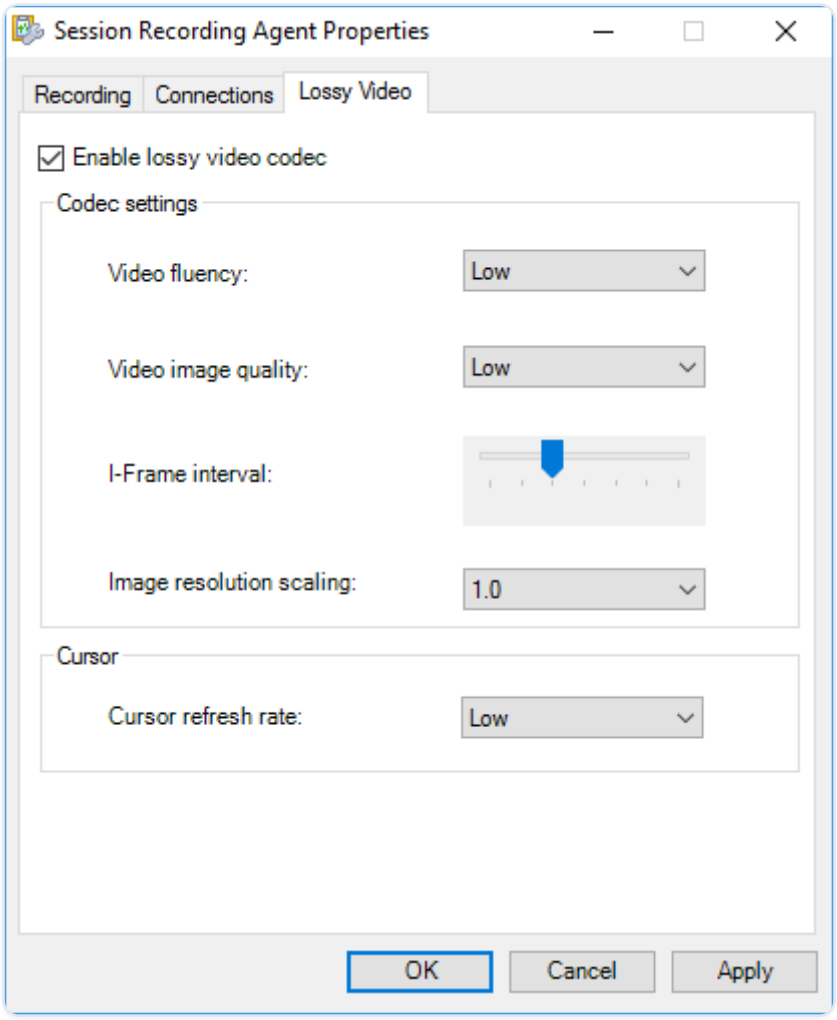
Note:

- This feature is disabled by default.
- The minimum version required for the VDA is 2303.

For more information, see Enable or disable recording.

Image resolution scaling for lossy video codec

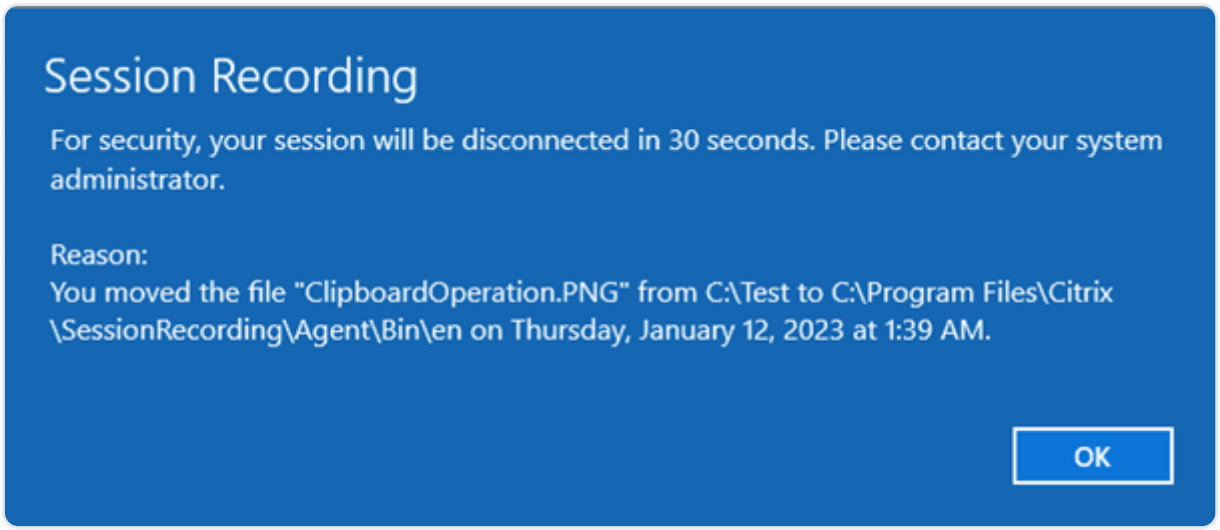
Lossy video codec lets you adjust compression options to reduce the size of recording files and to accelerate navigation through recorded sessions during playback. This release adds a compression option, image resolution scaling, to the lossy video codec feature. Image resolution scaling lets you downscale the resolution of recorded screens.



For more information, see Enable or disable lossy video codec.

Enhanced notification for event response actions

Starting with Session Recording 2206, you can disconnect, log off, or lock users from their virtual sessions when a specific event is detected. You can also notify users of the actions by setting the time interval between a notice and its execution. This release enhances the notification feature by giving users a clearer understanding of the reason behind the actions. For an example notice, see the following screen capture:



For more information, see Create a custom event response policy.

Google Analytics disabled for EU customers by default

Google Analytics is now disabled for EU customers by default. For more information, see CEIP and Google Analytics.

More optional parameters for ICLDB commands

This release introduces the RELOCATE parameter to the IMPORT command and the FILTER parameter to the ARCHIVE and REMOVE commands of the ICLDB utility.

- **The RELOCATE parameter for ICLDB IMPORT**

  You can move session recording files to different storage paths for load balancing or other purposes. To ensure that the files can still be played, you must update their new paths to the Session Recording database. To do so, use the ICLDB IMPORT command. To accelerate the import process, append the RELOCATE parameter to the ICLDB IMPORT command.

  Without the RELOCATE parameter, the ICLDB IMPORT command parses session recording files in their entirety, which takes time. With the RELOCATE parameter, the ICLDB IMPORT command simply locates the database records of session recording files and updates their file paths directly.

- **The FILTER parameter for ICLDB ARCHIVE and ICLDB REMOVE**

  Previously, only the RETENTION parameter was available for the ICLDB ARCHIVE and ICLDB REMOVE commands to specify target session recording files to manipulate. Starting with this release, you can add the FILTER parameter to manipulate session recording files that meet both RETENTION and FILTER. The FILTER parameter lets you filter file paths by using the `*` and `?` wildcards.

For more information about the ICLDB utility, see Manage recordings.

What's new in 2212

This release includes the following new features and addresses issues to improve the user experience:

Lossy video codec

Lossy video codec lets you adjust compression options to reduce the size of recording files and to accelerate navigating recorded sessions during playback. Lossy video codec is suitable for use when:

- the size of recording files per time unit is too large, or
- there is a lag while you fast forward or rewind during playback.

For more information, see Enable or disable lossy video codec.

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.

What's new in 2210

This release includes the following new feature and addresses an issue to improve the user experience:

Support for installation in session 0

This release introduces the **AllowSession0Install** argument for you to automate installation of the Session Recording administration components in session 0. For more information, see Automate installation.

What's new in 2209

This release includes the following new feature and addresses an issue to improve the user experience:

Recording access control

You can now place access restrictions on target recordings in addition to role-based access control through recording viewing policies. Restricted recordings are accessible only to users and user groups that are assigned the **PrivilegedPlayer** role through the Session Recording Authorization Console. For more information, see Place access restrictions on recordings in the web player and Place access restrictions on recordings in the Session Recording player.

What's new in 2207

This release includes the following new feature and addresses an issue to improve the user experience:

Improved performance of the web player

We have optimized the graphics engine to improve the performance of the web player. If you encounter compatibility or other issues with the optimized engine, you can disable it through the **Configuration > Preferences** menu on the web player page. For more information, see Configure preferences.

What's new in 2206

This release includes the following new features and enhancements:

Regular session recording storage reports

You can now schedule reports through Session Recording Server Properties to receive emailed session recording storage reports on a daily or weekly basis. A session recording storage report provides weekly statistics on screen recordings. For more information, see Session recording storage reports.

Support for additional event response actions

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

- Lock session
- Log off session
- Disconnect session

For more information, see Configure event response policies.

What's new in 2204

This release addresses issues to improve the user experience.

What's new in 2203 LTSR (initial release)

This release includes the following new features and enhancements:

Monitoring popup window events

When users open or close a confidential file or access a folder, a popup window might appear, showing a prompt or asking for a password. Session Recording can now monitor such popup window events while recording sessions. Popup windows in web browsers are not monitored. For more information, see Configure event detection policies.

Responses configurable for more event types

You can now specify how to respond when the following session events are detected:

- File transfers between session hosts (VDAs) and client devices
- Windows registry modifications
- User account modifications
- App failures
- App installs and uninstalls
- RDP connections
- Clipboard activities
- Popup window events
- Performance data (data points related to the recorded session)

For more information, see Configure event response policies.

Configurable time span for screen recording before a session event is detected

When you specify events to trigger dynamic screen recording, you can configure the amount of time of the screen recording you want to keep before events are detected. The actual length of the screen recording that Session Recording keeps might be a little longer than your configuration.

This feature is available only for virtual desktop sessions. For more information, see Configure event response policies.

What's new in 2201

This release addresses issues to improve the user experience.

What's new in 2112

This release includes the following new features and addresses an issue to improve the user experience:

Integration with Citrix Analytics for Security™

You can now configure Session Recording servers to send user events to Citrix Analytics for Security, which processes those user events to provide actionable insights into user behaviors.

For more information, see Integrate with Citrix Analytics for Security.

Extended scope of event detection

We have extended the scope of event detection to monitor the following events while recording sessions:

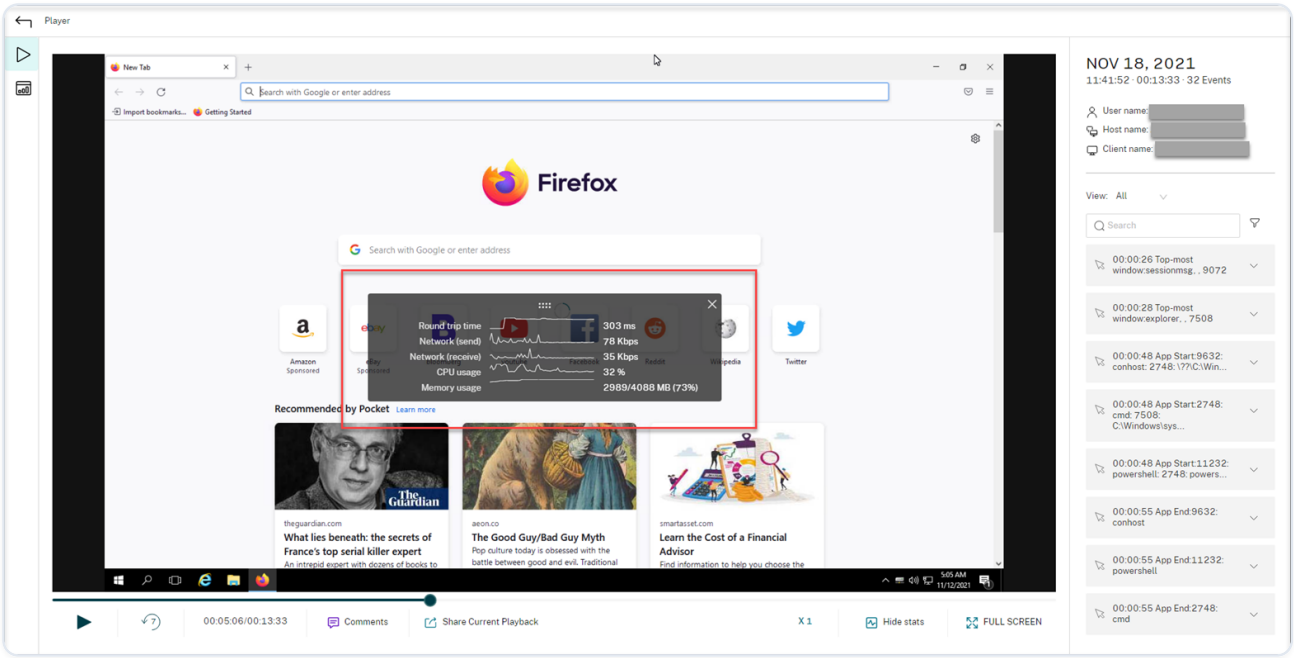
- App failures: including unexpected app exits and unresponsive apps.
- User account modifications: including account creation, enablement, disablement, deletion, name changes, and password modification attempts.
- RDP connections: RDP connections initiated from the VDA hosting the recorded session.
- App installs and uninstalls

For more information, see Create a custom event detection policy.

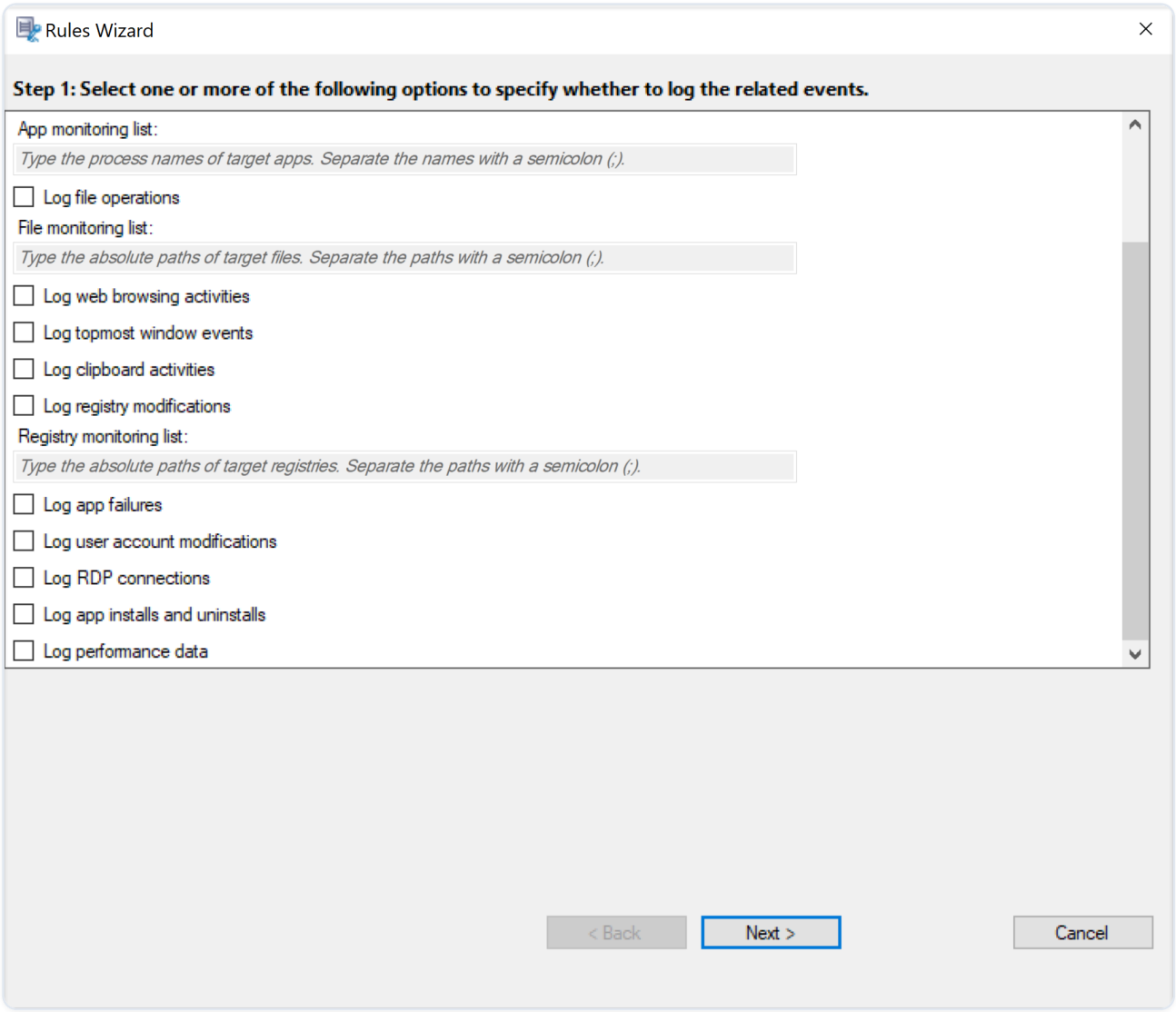
Session data overlay

This release introduces a screen overlay during session playback in the web player. It is a semi-transparent overlay that you can relocate and hide. The overlay features the following data points related to the recorded session:

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



To enable the feature, select **Log performance data** when creating your event detection policy. For more information, see Create a custom event detection policy and Session Recording web player.



What's new in 2110

This release addresses issues to improve the user experience.

> **Note:**
>
> Starting with 2110, before installing the Session Recording Administration components on Windows Server 2016 where TLS 1.0 is disabled, complete the following steps:
>
> 1. Install Microsoft OLE DB Driver for SQL Server.
> 2. Under the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319` registry key, add the `SchUseStrongCrypto` DWORD (32-bit) value and set the value data to 1.

3. Reboot.

What's new in 2109

The 2109 release includes the following new feature and addresses issues to improve the user experience:

Windows 11 support

The Citrix components, features, and technologies in this release that support the Windows 10 OS now also support Windows 11, unless otherwise noted. For more information, see Windows 11 support.

Support for event data visualization

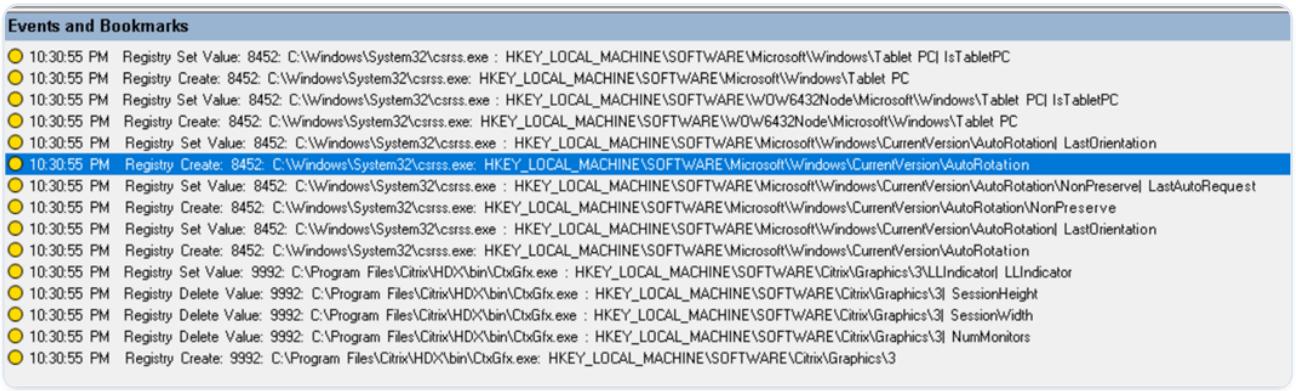
Event data visualization is now available in the web player for each recording. It provides graphical event statistics that help you quickly comprehend large numbers of events inserted in recordings, allowing you to easily see and communicate event trends. For more information, see View graphical event statistics in the Session Recording web player article.

Monitor registry modifications

We have extended the scope of event detection to monitor the following registry modifications while recording sessions:

REGISTRY MODIFICATION	CORRESPONDING EVENT
Adding a key	Registry Create
Adding a value	Registry Set Value
Renaming a key	Registry Rename
Renaming a value	Registry Delete Value and Registry Set Value
Changing an existing value	Registry Set Value
Deleting a key	Registry Delete
Deleting a value	Registry Delete Value

For example:



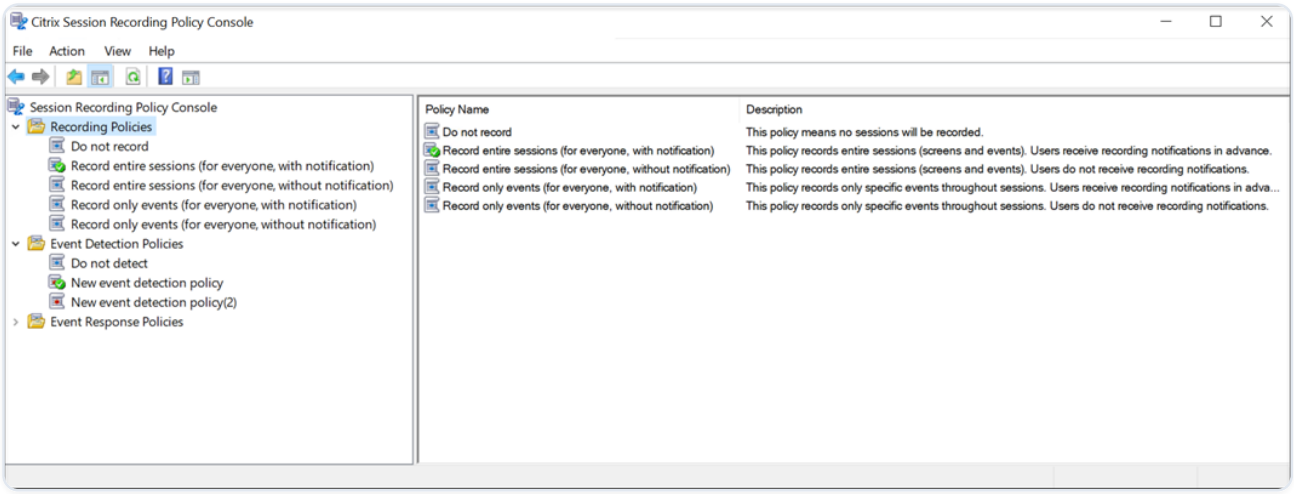
To enable this registry monitoring functionality, select the **Log registry modifications** option for your event detection policy. For more information, see Create a custom event detection policy and Log events.

Renamed policies

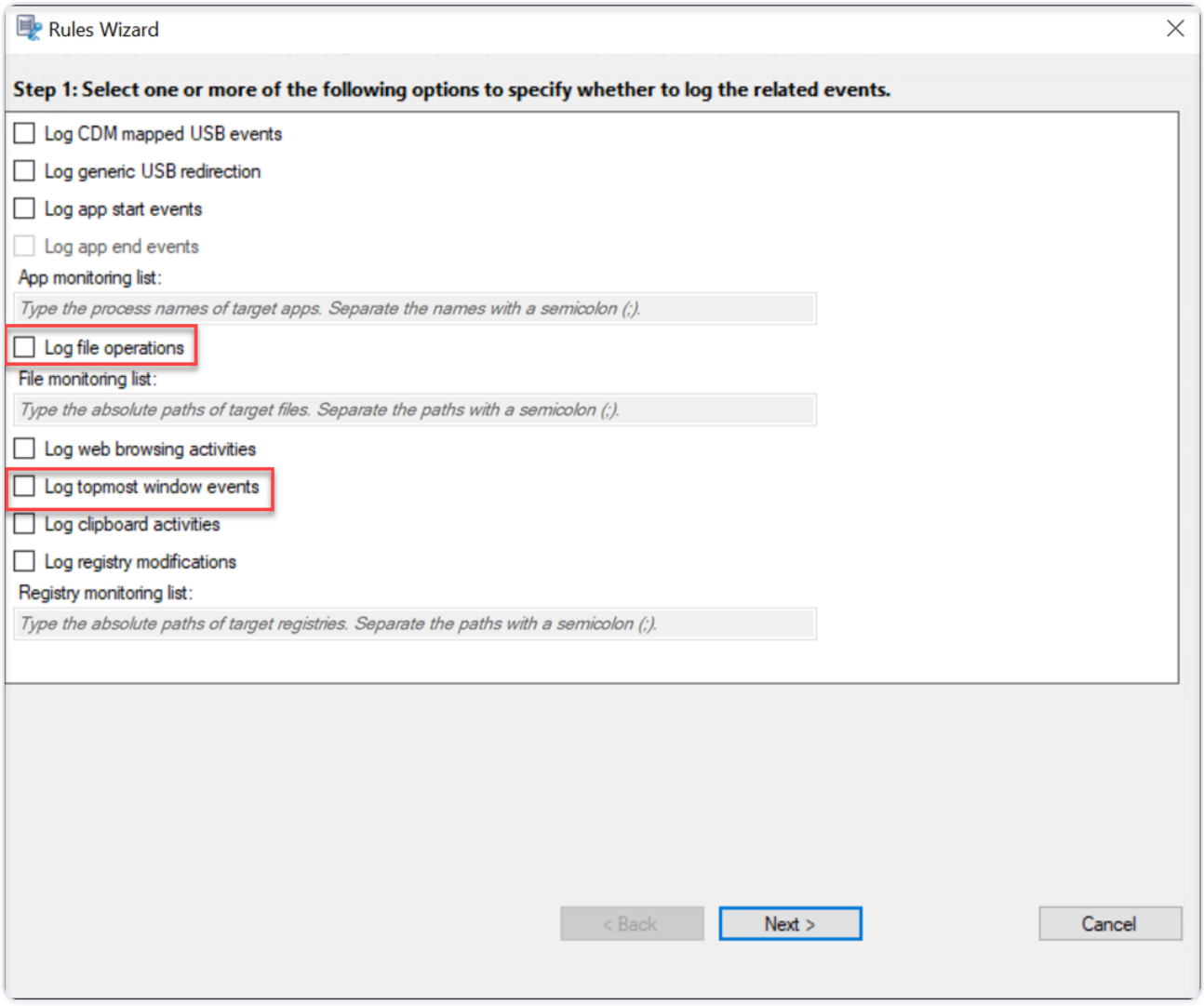
In the Session Recording Policy Console, we have renamed the following recording policies and options for event detection settings:

OLD NAME	NEW NAME
Record event only for everyone with notification	Record only events (for everyone, with notification)
Record event only for everyone without notification	Record only events (for everyone, without notification)
Record everyone with notification	Record entire sessions (for everyone, with notification)
Record everyone without notification	Record entire sessions (for everyone, without notification)
Log sensitive file events	Log file operations
Log top-most window activities	Log topmost window events

Renamed recording policies:



Renamed options for event detection settings:

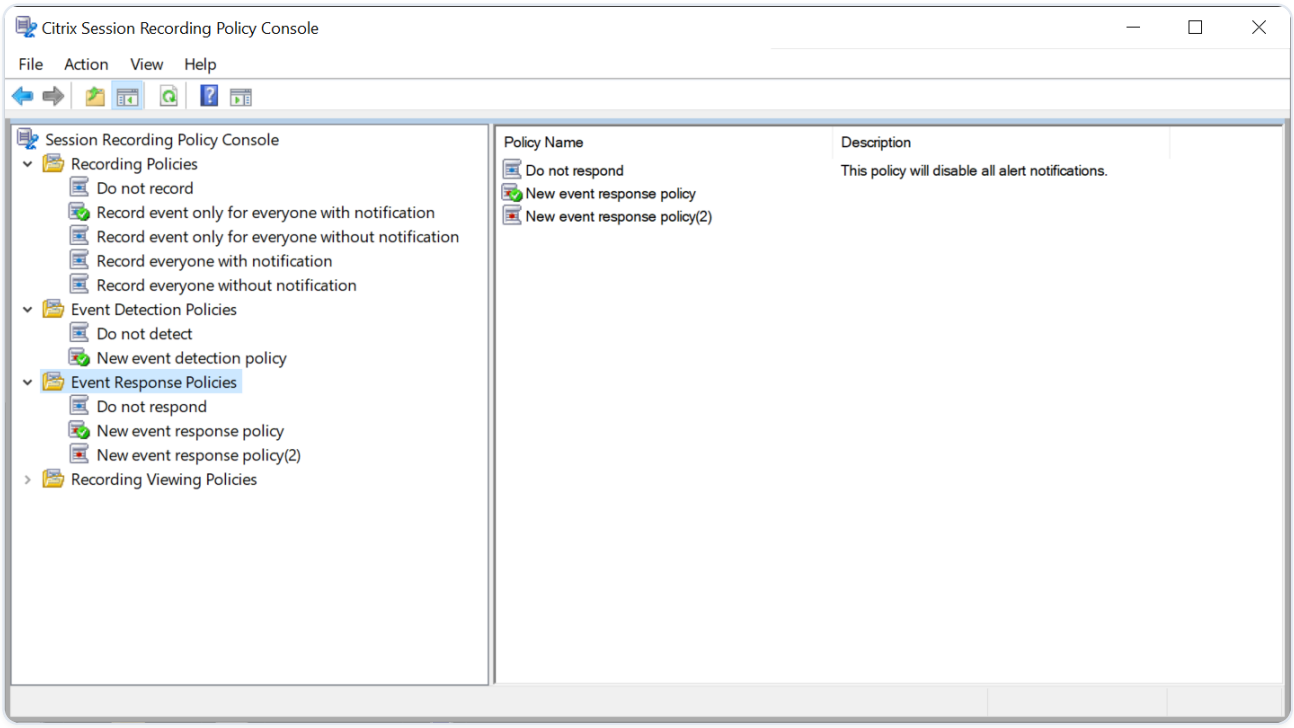


What's new in 2107

This release includes the following new feature and addresses issues to improve the user experience:

Event-triggered dynamic screen recording

The 2106 release introduced event-only recordings - the ability to record only specific events throughout a session - without capturing any screens. However, there are scenarios where you might want to automatically start recording screens when certain events occur during an event-only recording. As of this release, you can configure this recording behavior (event-triggered dynamic screen recording) using event response policies. For more information, see Event response policies.



> **Tip:**
>
> In this release, we renamed **Email Alert Policies** to **Event Response Policies** and **Event Logging Policies** to **Event Detection Policies**.

What's new in 2106

This release includes the following new features and enhancements:

Windows Server 2022 support

Components, features, and technologies that support Windows Server operating systems now also support Windows Server 2022, unless noted otherwise. For more information, see Windows Server 2022 support.

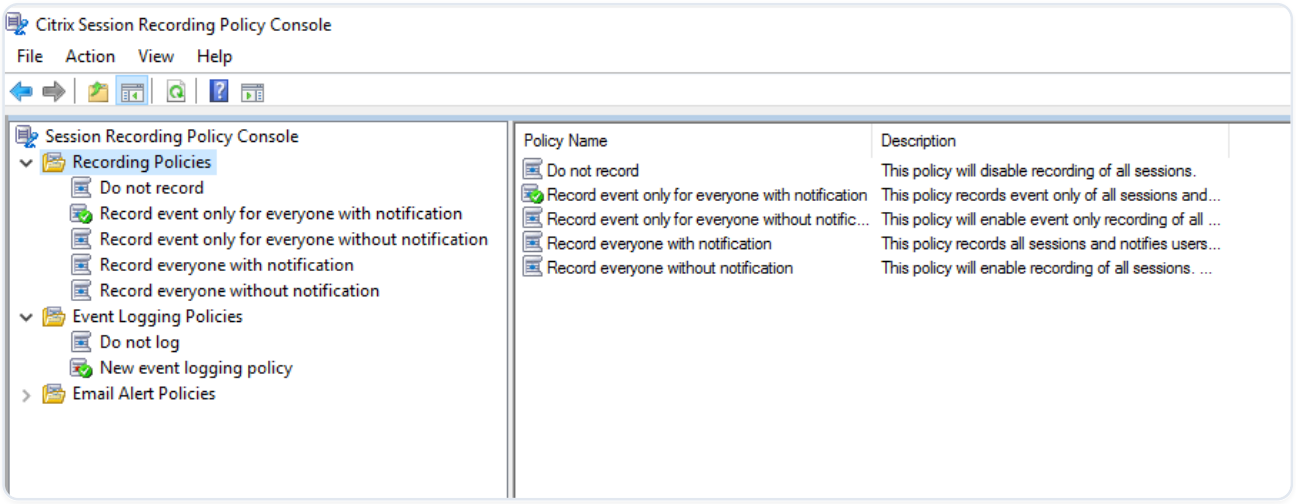
Monitor file transfers

We've extended the scope of event logging to monitor file transfers between session hosts (VDAs) and client devices (including mapped client drives and generic redirected mass storage devices). Selecting the **Log sensitive file events** option for an event logging policy triggers the logging of file transfers, no matter whether you specify the **File monitoring list**. This enhanced feature requires Windows VDA 2106 or later. For more information, see Configure policies.

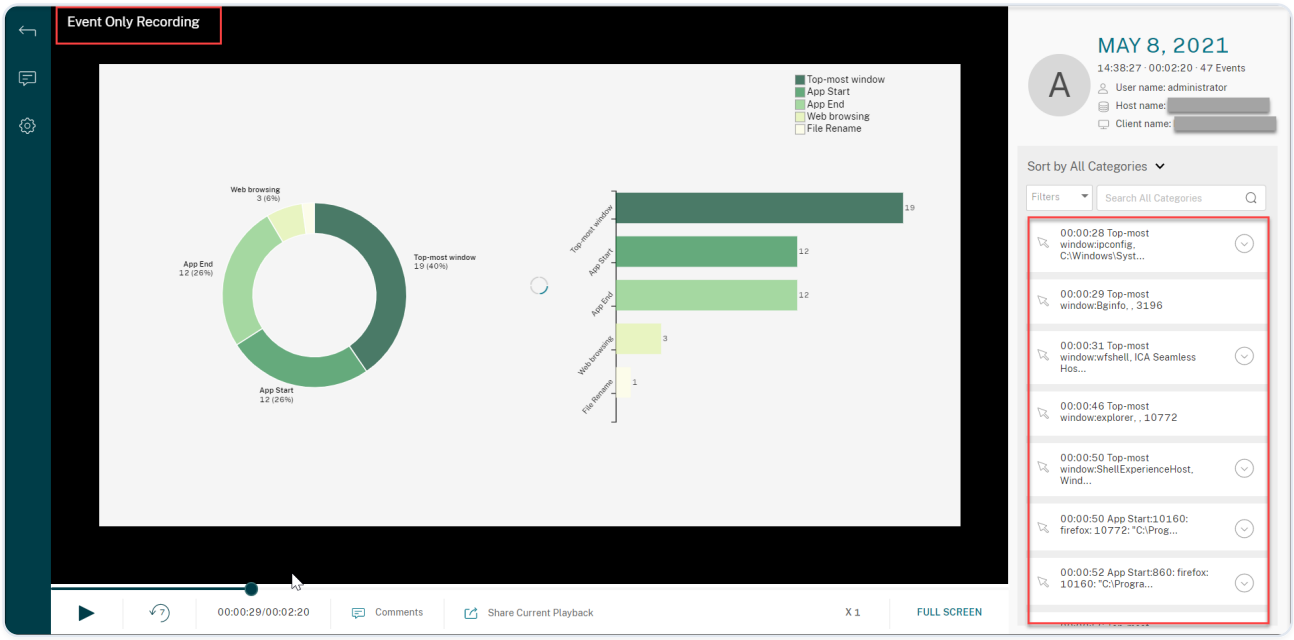
Record events only

In addition to recording screens, you can now record only specific events. This feature helps to free up storage space. To use this feature, activate either of the following new system-defined policies and then set an event logging policy to specify which events to record.

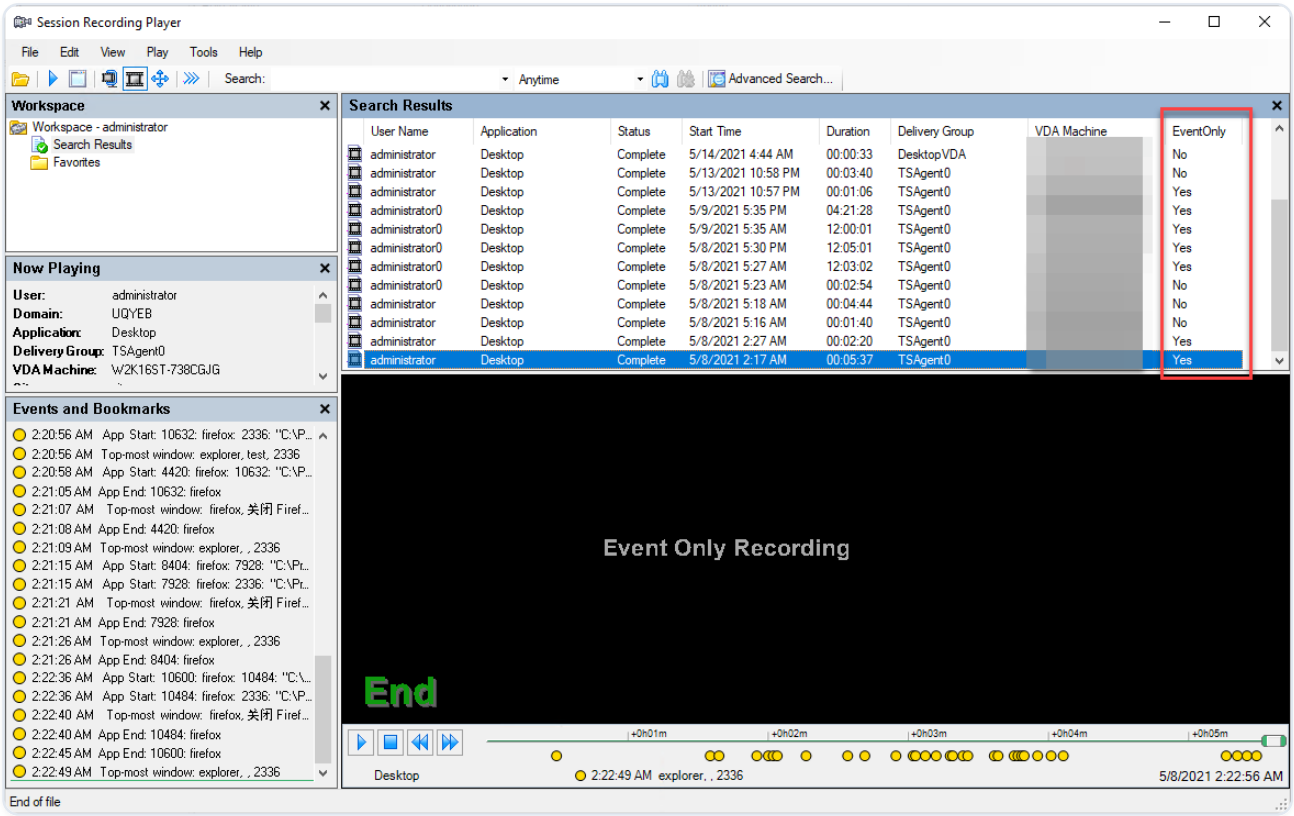
- Record event only for everyone with notification
- Record event only for everyone without notification



An event-only recording played in the web player contains an event statistics pie chart and histogram. The pie chart and histogram hold static throughout playback. You can navigate to a specific event from within the right pane.



The following screen capture shows an example of an event-only recording being played in the Session Recording Player. The **EventOnly** column indicates a screen recording or an event-only recording. All events are present in the **Events and Bookmarks** panel and show as yellow dots in the lower part of the Session Recording Player.



For more information, see Configure policies.

What's new in 2104

This release includes the following enhancement and addresses an issue to improve the user experience:

Enhancement to recording file creation and storage

Previously, recording files were created and visible in the recording storage folder for all sessions when they were launched. The files were then deleted if policies were set not to record the launched sessions. As of this release, recording files are created only for recorded sessions.

What's new in 2103

This release includes the following new features and enhancements:

Support for deploying the Database on AWS RDS

You can now deploy the Session Recording Database on AWS RDS by using the SessionRecordingAdministrationx64.msi package under **\layout\image-full\x64\Session Recording** on the Citrix Virtual Apps and Desktops ISO. For more information, see Deploy the Session Recording Database on cloud SQL database services.

Support for Azure Files and load balancing in Azure

You can now store recording files in Azure file shares that you can mount to both cloud and on-premises deployments. You can also deploy all Session Recording components in Azure and configure load balancing to evenly distribute loads across Session Recording Servers. For more information, see Specify where recordings are stored and Deploy and load-balance Session Recording in Azure.

Citrix Virtual Apps and Desktops™ Remote PowerShell SDK support for dynamic session recording

We have added support for the Citrix Virtual Apps and Desktops Remote PowerShell SDK to facilitate dynamic session recording in a Citrix Virtual Apps and Desktops service environment. For more information, see Dynamic session recording.

Font and color redesigns for the web player website

We have implemented font and color redesigns on the web player website. For more information, see Session Recording web player.

Recording playback enhancements

As recordings grow in size, recording files can take longer to download and respond more slowly when you use the seek slider to navigate during playback. To enhance playback experience, we've decreased the recording file upper limit from 1 GB to 300 MB and achieved continuous playback by splitting a single recording into multiple files. You can also right-click or select a recording and then choose or click **Follow up** to show all recording files of the recorded session. For more information, see Specify file size for recordings, Launch the Session Recording Player, and Session Recording web player.

Hiding content on the web player home page

We have added an option in **Session Recording Server Properties**. It lets you prevent the web player home page from displaying any content. Recordings are accessible only by way of their URLs. For more information, see Session Recording web player.

Migrating the WebSocket server to IIS

This release migrates the WebSocket server to IIS. A fresh installation of the latest Current Release connects your web browser to the WebSocket server hosted in IIS when you access the web player website. An upgrade installation from an earlier version to the latest Current Release connects your web browser to the original Python-based WebSocket server. To connect to the WebSocket server hosted in IIS, run the **<Session Recording Server installation path\>\Bin\SsRecUtils.exe -enablestreamingservice** command. For more information, see Session Recording web player and Configure load balancing in an existing deployment.

> **Tip:**
>
> Starting from this release, the `ArchiveSample.ps1`, `SrServerConfigurationSync.ps1`, and `GenRandomQMID.ps1` scripts are available under **<Session Recording Server installation path\>\Scripts**.

System requirements

Session Recording includes the Session Recording Administration components, the Session Recording agent, and the Session Recording player. You can install the Session Recording Administration components (Session Recording database, Session Recording server, and Session Recording policy console) on a single server or on different servers. The following section details the requirements for each of the Session Recording components.

For information about using this Current Release (CR) in a Long Term Service Release (LTSR) environment and other FAQs, see Knowledge Center article.

Session Recording database

Supported operating systems:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Supported Microsoft SQL Server versions:

- Microsoft SQL Server 2019 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2017 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2016 SP2 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2016 SP1 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2014 SP2 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2012 SP3 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2008 R2 SP3 Enterprise, Express, and Standard editions

Supported Azure SQL database services:

- Azure SQL Managed Instance
- SQL Server on Azure Virtual Machines (VMs) (Use supported versions of Microsoft SQL Server that are listed earlier.)

- Azure SQL Database

Supported AWS RDS database services:

- SQL Server

Requirement: .NET Framework 4.7.2

> **Note:**

> Ledger databases are not supported. Password cannot contain quote marks (") and minimum of 8 characters.

Session Recording server

Supported operating systems:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Other requirements:

- Internet Information Services (IIS) 10, 8.5, 8.0, or 7.5
- .NET Framework Version 4.7.2
- If the Session Recording server uses HTTPS as its communications protocol, add a valid certificate. Session Recording uses HTTPS by default, which Citrix® recommends.
- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled and MSMQ HTTP support enabled.
- For Administrator Logging: Latest version of Chrome, Firefox, or Internet Explorer 11

Session Recording policy console

Supported operating systems:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Requirement: .NET Framework 4.7.2

Session Recording agent

Install the Session Recording agent on every Windows Virtual Delivery Agent (VDA) on which you want to record sessions.

Supported operating systems:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 11
- Windows 10, minimum version 1607
- Windows 10 Enterprise for Virtual Desktops

Requirements:

- Citrix Virtual Apps and Desktops™ 7 2203 with Premium license
- Citrix Virtual Apps™ and Desktops 7 1912 LTSR CU4 or later with Platinum license
- XenApp and XenDesktop 7.15 LTSR CU8 with Platinum license
- .NET Framework 4.7.2
- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled and MSMQ HTTP support enabled

> **Note:**
>
> Session Recording currently supports Citrix DaaS™ (formerly Citrix Virtual Apps and Desktops service) Advanced, Advanced Plus, Premium, and Premium Plus editions.

Session Recording player

Supported operating systems:

- Windows Server 2022
- Windows Server 2019

- Windows Server 2016
- Windows 11
- 64-bit Windows 10, minimum version 1607

Requirement: .NET Framework 4.7.2

> **Note:**

> On 32-bit Windows 10, you can install the player only by using the SessionRecordingPlayer.msi file. You can find the msi file on the Citrix Virtual Apps and Desktops ISO under **\x86\Session Recording**.

> For optimal results, install the Session Recording player on a workstation with:

- Screen resolution of 1024 x 768
- Color depth of at least 32-bit
- 2 GB RAM minimum; more RAM and CPU/GPU resources can improve performance when playing graphics-intensive recordings, especially when recordings contain many animations

The seek response time depends on the size of the recording and your machine's hardware specifications.

Get started

Session Recording consists of five components:

Session Recording components

Session Recording consists of the following components:

- **Session Recording Administration components**:
  - **Session Recording policy console.** A console used to configure policies such as session recording policies that specify which sessions to record. For more information, see Policies.
  - **Session Recording server.** A server that hosts:
    - The Broker. An IIS 6.0+ hosted Web application that serves the following purposes:
      - Handling search queries and file download requests from the Session Recording player and web player.
      - Handling policy administration requests from the Session Recording policy console.
      - Evaluating recording policies for each Citrix Virtual Apps and Desktops™ or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) session.
    - The Storage Manager. A Windows service that manages the recorded session files received from each Session Recording-enabled VDA.
    - **Administrator logging**. An optional subcomponent installed with the Session Recording server to log the administration activities. All the logging data is stored in a separate SQL Server database named **CitrixSessionRecordingLogging** by default. You can customize the database name.
  - **Session Recording database.** A component that manages the SQL Server database for storing recorded session data. When this component is installed, it creates a database named **CitrixSessionRecording** by default. You can customize the database name.
- **Session Recording agent.** A component installed on each VDA for multi-session OS or single-session OS to enable recording. It is responsible for recording session data.

- **Session Recording player / web player.** A user interface that users access from a workstation to play recorded session files.

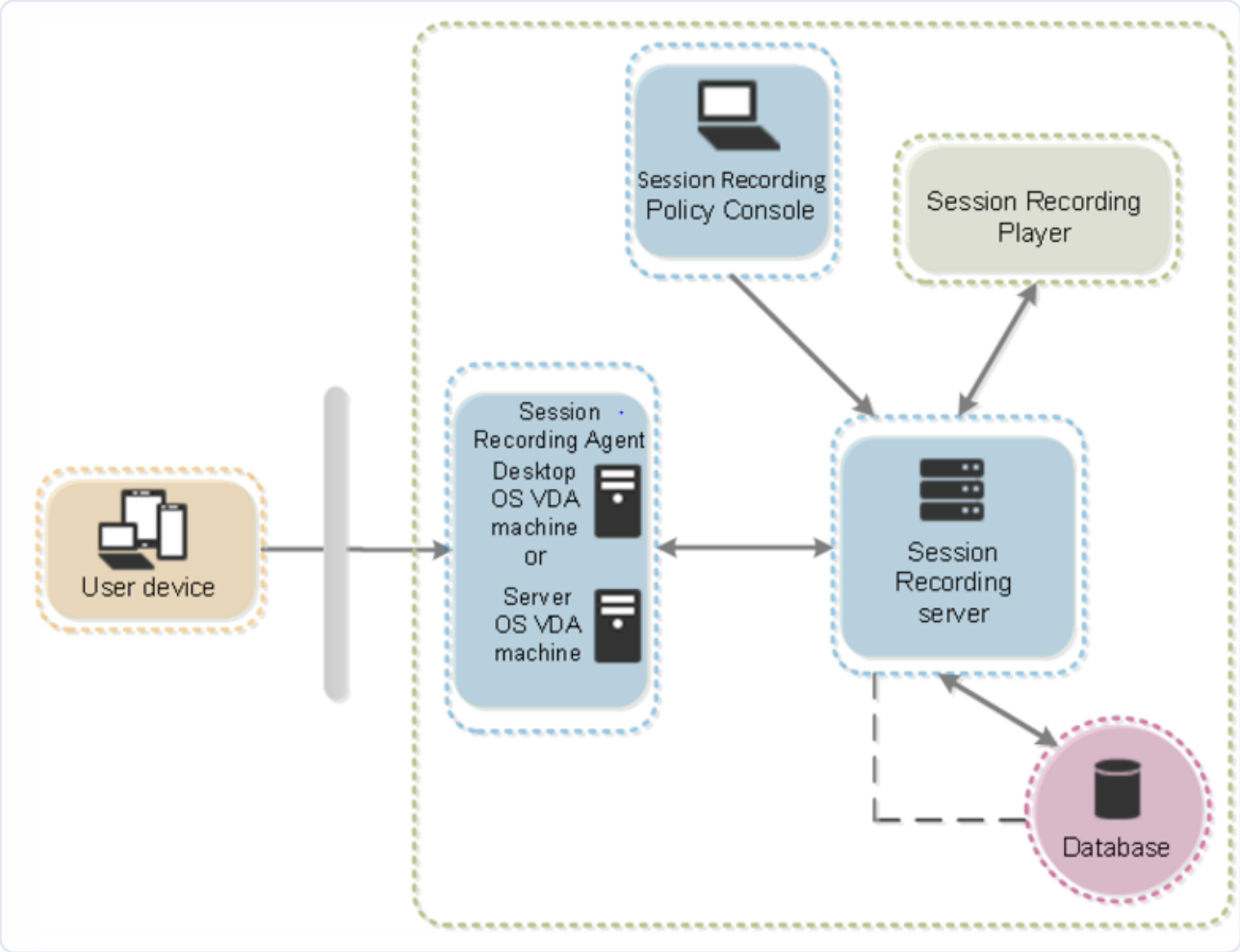
To install Session Recording or upgrade an existing installation, go to each machine where you are about to or have already installed the Session Recording components and then run the Citrix Virtual Apps™ and Desktops ISO.

> **Tip:**
>
> Go to the Citrix Virtual Apps and Desktops download page to download the appropriate version of Citrix Virtual Apps and Desktops.

> For more information about installing Session Recording, see Install, upgrade, and uninstall. You can also refer to the Citrix Tech Zone article POC Guide: Citrix Session Recording for information on how to quickly set up and configure Citrix Session Recording and Citrix Session Recording service.

Example deployment

The following diagram shows an example deployment:



- All the Session Recording components reside behind a security firewall.
- The Session Recording agent is installed on a VDA for multi-session OS or single-session OS.
- A second server hosts the Session Recording policy console, a third server acts as the Session Recording server, and a fourth server hosts the database.
- The Session Recording player is installed on a workstation. Installing the Session Recording server lets you install the Session Recording web player automatically.
- A client device outside the firewall communicates with the VDA where the Session Recording agent is installed.
- Inside the firewall, the Session Recording agent, policy console, player, and database all communicate with the Session Recording server.

Plan your deployment

Limitations and caveats

Session Recording doesn't support Desktop Composition Redirection (DCR) display mode. By default, Session Recording disables DCR in a session to be recorded. You can configure this behavior in **Session Recording Agent properties**.

When you browse URLs configured in the browser content redirection policy in Internet Explorer, graphics activities are not recorded.

Session Recording does not support the Framehawk display mode. Sessions in Framehawk display mode cannot be recorded and played back correctly. Sessions recorded in Framehawk display mode might not contain the sessions' activities.

Session Recording can't record the Lync webcam video when using the HDX™ RealTime Optimization Pack.

Depending upon your environment, you can deploy the Session Recording components in different scenarios.

A Session Recording deployment is not limited to a single site. Except the Session Recording agent, all components are independent of the server site. For example, you can configure multiple sites to use a single Session Recording server.

A single Session Recording server might experience a high performance demand. For example, you might have a large site with many agents and plan to record many sessions or many graphically intense applications such as AutoCAD. To alleviate performance issues, you can install multiple Session Recording servers and configure load balancing.

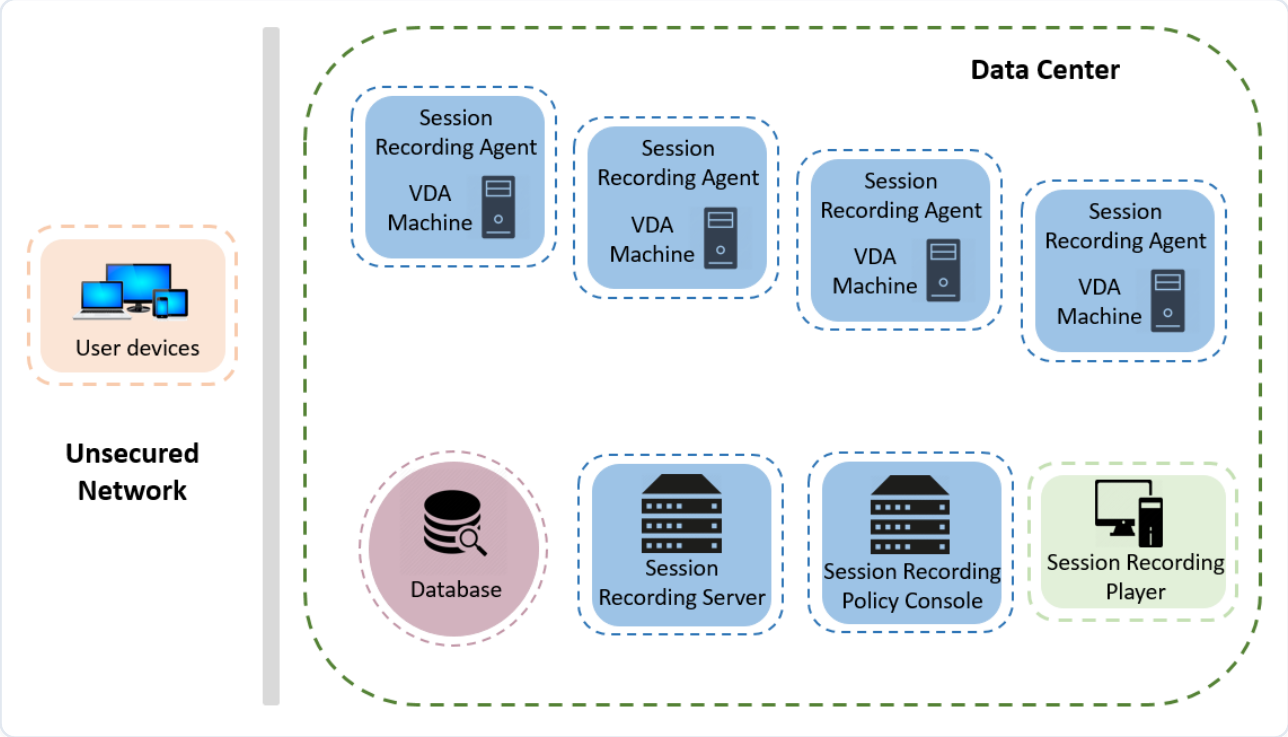
Ports

SOURCE	DESTINATION	TYPE	PORT	DETAILS
Virtual Delivery Agent	Session Recording server	TCP	80, 443	Communication between the Session Recording agent installed on Virtual Delivery Agent and the

SOURCE	DESTINATION	TYPE	PORT	DETAILS
				Session Recording server. Default installation uses HTTPS/SSL to secure communications. If SSL is not configured, use HTTP.
Session Recording policy console	Session Recording server	TCP	80, 443	Communication between the server where the Session Recording policy console is installed and the Session Recording server.
Session Recording player	Session Recording server	TCP	80, 443	Communication between the workstation where the Session Recording player is installed and the Session Recording server.
Session Recording server	Microsoft SQL Server	TCP	1433	Connection to the Session Recording database.

Suggested server site deployment

Use this type of deployment for recording sessions for one or more sites. The Session Recording agent is installed on each VDA in a site. The site resides in a data center behind a security firewall. The Session Recording Administration components (Session Recording database, Session Recording server, and Session Recording policy console) are installed on other servers and the Session Recording player is installed on a workstation, all behind the firewall. It is recommended to deploy the Session Recording server in a secure, intranet data center.



Important deployment notes

- To enable Session Recording components to communicate with each other, install them in the same domain or across trusted domains that have a transitive trust relationship. The system cannot be installed on a workgroup or across domains that have an external trust relationship.
- Considering its intense graphical nature and memory usage when playing back large recordings, we do not recommend installing the Session Recording Player as a published application.
- The Session Recording installation is configured for TLS/HTTPS communication. Install a certificate on the Session Recording server. Make sure the root certificate authority (CA) is trusted on the Session Recording components.
- For the Session Recording server on a standalone server running SQL Server, enable the TCP/IP protocol and run the SQL Server Browser service. These settings are disabled by default, but they must be enabled for the Session Recording server to communicate with the database.

For more information, see the Microsoft articles Enable TCP/IP Network Protocol for SQL Server and SQL Server Browser service.

- Consider the effects of session sharing when planning your Session Recording deployment. Session sharing for published applications can conflict with Session Recording policy rules for published applications. Session Recording matches the active policy with the first published application that a user opens. After the user opens the first application, any subsequent applications opened during the same session continue to follow the policy that is in force for the first application. For example, if a policy states to record only Microsoft Outlook, the recording commences when the user opens Outlook. If the user opens a published Microsoft Word second while Outlook is running, Word also is recorded. Conversely, if the active policy doesn't specify to record Word and the user launches Word before Outlook, Outlook is not recorded.
- Though you can install the Session Recording server on a Delivery Controller™, we don't recommend it because of performance issues.
- You can install the Session Recording Policy Console on a Delivery Controller.
- You can install both the Session Recording server and the Session Recording Policy Console on the same system.
- Ensure that the NetBIOS name of the Session Recording server does not exceed the limit of 15 characters. Microsoft has a 15-character limit on the host name length.
- PowerShell 5.1 or later is required for custom event logging. Upgrade PowerShell if you install the Session Recording agent on Windows Server 2012 R2 that has PowerShell 4.0 installed. Failure to comply can cause failed API calls.
- For step-by-step instructions on deploying and configuring the Citrix Session Recording and Citrix Session Recording service, see this Citrix Tech Zone article: POC Guide: Citrix Session Recording.

Security recommendations

Session Recording is deployed within a secure network and accessed by administrators, and as such, is secure. Out-of-the-box deployment is simple and security features such as digital signing and encryption can be configured optionally.

Communication between Session Recording components is achieved through Internet Information Services (IIS) and Microsoft Message Queuing (MSMQ). IIS provides the web services communication link between Session Recording components. MSMQ provides a reliable data transport mechanism to send recorded session data from the Session Recording agent to the Session Recording server.

Warning:

Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix® cannot guarantee that problems resulting from the incorrect use of **Registry Editor** can be solved. Use **Registry Editor** at your own risk. Be sure to back up the registry before you edit it.

Consider these security recommendations when planning your deployment:

- Configure Microsoft Internet Information Services (IIS).

  You can configure Session Recording with a restricted IIS configuration. On each Session Recording server, open the IIS Manager and set the following recycling limits for each IIS application pool:

  - **Virtual Memory Limit**: Set the value to 4,294,967,295.
  - **Private Memory Limit**: Set the value to the physical memory of the Session Recording server. For example, if the physical memory is 4 GB, set the value to 4,194,304.
  - **Request Limit**: We recommend you leave this setting unspecified. Or you can set the value to 4,000,000,000.

  Tip:

  To access the preceding settings, highlight each application pool, select **Advanced Settings** in the **Actions** pane, and then scroll down to the **Recycling** section in the **Advanced Settings** dialog box.

- Ensure that you properly isolate the different administrator roles in the corporate network, in the Session Recording system, or on individual machines. By not doing so, security threats that can impact the system functionality or abuse the system might occur. We recommend that you assign different administrator roles to different persons or accounts. Do not allow general session users to have administrator privileges to the VDA system.

  - Do not grant VDA local administrator role to any users of published apps or desktops. If the local administrator role is a requirement, protect the Session Recording agent components by using Windows mechanisms or third-party solutions.

  - Separately assign the Session Recording database administrator and Session Recording policy administrator.
  - Do not assign VDA administrator privileges to general session users, especially when using Remote PC Access.
  - The Session Recording server's local administration account must be strictly protected.
  - Control access to machines where the Session Recording player is installed. If a user is not authorized for the Player role, do not grant that user the local administrator role for any player machine. Disable anonymous access.
  - We recommend using a physical machine as a storage server for Session Recording.

- Session Recording records session graphics activities without regard to the sensitivity of the data. Under certain circumstances, sensitive data (including but not limited to user credentials, privacy information, and third-party screens) might be recorded unintentionally. Take the following measures to prevent risks:

  - Disable core memory dump for VDAs unless for specific troubleshooting cases. To disable core memory dump:

    a. Right-click **My Computer**, and then select **Properties**.

    b. Click the **Advanced** tab, and then under **Startup and Recovery**, click **Settings**.

    c. Under **Write Debugging Information**, select **(none)**.

    See the Microsoft article at `<https://support.microsoft.com/en-us/kb/307973>`.

  - Session owners notify attendees that online meetings and remote assistance software might be recorded if a desktop session is being recorded.
  - Ensure that logon credentials or security information does not appear in all local and Web applications published or used inside the corporation. Otherwise, they are recorded by Session Recording.
  - Close any application that might expose sensitive information before switching to a remote ICA® session.
  - We recommend only automatic authentication methods (for example, single sign-on, smartcard) for accessing published desktops or Software as a Service (SaaS) applications.

- Session Recording relies on certain hardware and hardware infrastructure (for example, corporate network devices, operation system) to function properly and to meet security needs.

Take measures at the infrastructure levels to prevent damage or abuse to those infrastructures and make the Session Recording function secure and reliable.

- Properly protect and keep network infrastructure supporting Session Recording available.
- We recommend using a third-party security solution or Windows mechanism to protect Session Recording components. Session Recording components include:
  - On the Session Recording server
    - Processes: SsRecStoragemanager.exe and SsRecAnalyticsService.exe
    - Services: CitrixSsRecStorageManager and CitrixSsRecAnalyticsService
    - All files in the Session Recording server installation folder
    - Registry values within HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\ \SmartAuditor\\Server
  - On the Session Recording agent
    - Process: SsRecAgent.exe
    - Service: CitrixSmAudAgent
    - All files in the Session Recording agent installation folder
    - Registry values under `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent`

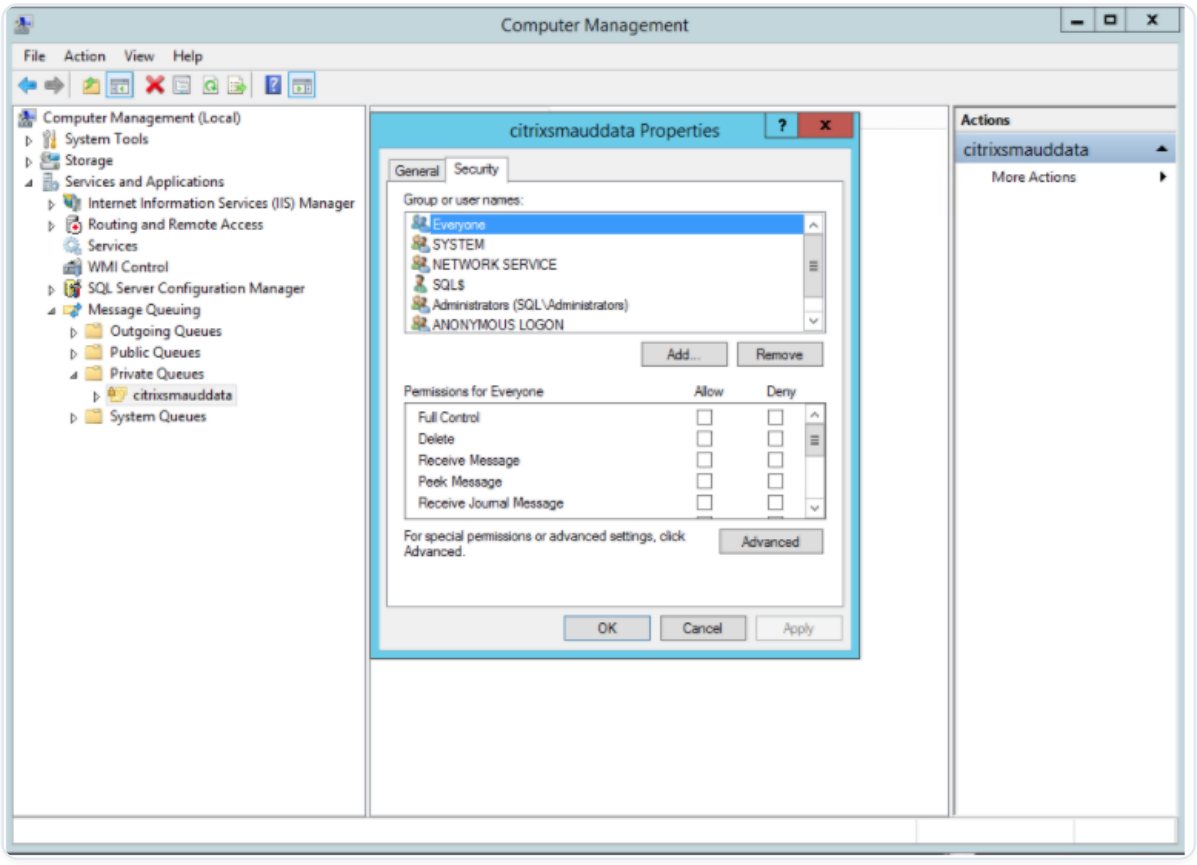
- As a security best practice, Citrix recommends using HTTPS on IIS.
- Set the access control list (ACL) for Message Queuing (MSMQ) on the Session Recording server to restrict VDA or VDI machines that can send MSMQ data to the Session Recording server and prevent unauthorized machines from sending data to the Session Recording server.

a. Install server feature **Directory Service Integration** on each Session Recording server and VDA or VDI machine where Session Recording is enabled. Then restart the **Message Queuing** service.

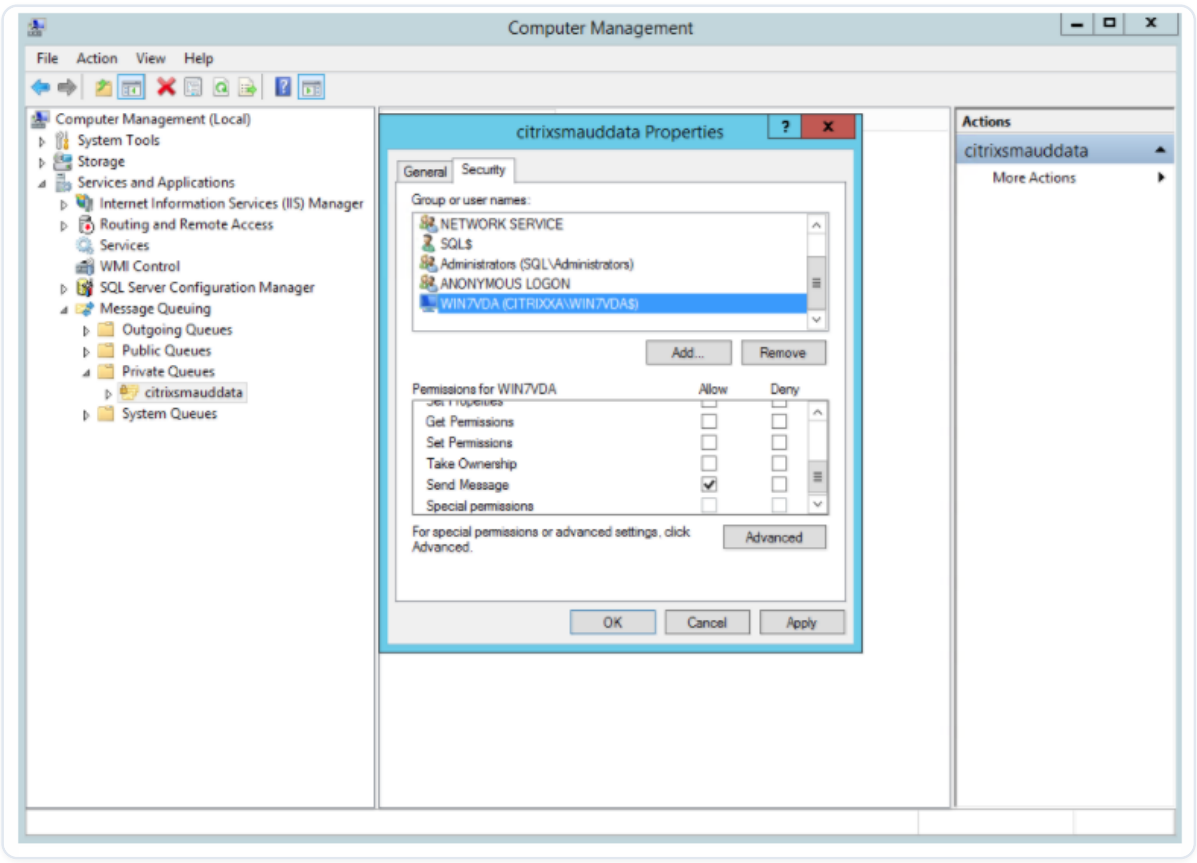
b. From the Windows **Start** menu on each Session Recording server, open **Administrative Tools** \> **Computer Management**.

c. Open **Services and Applications** \> **Message Queuing** \> **Private Queues**.

d. Click the private queue **citrixsmauddata** to open the **Properties** page and select the **Security** tab.



e. Add the computers or security groups of the VDAs that send MSMQ data to this server and grant them the **Send Message** permission.



- Properly protect the event log for the Session Record server and Session Recording agents. We recommend using a Windows or third-party remote logging solution to protect the event log or redirect the event log to the remote server.
- Ensure that servers running the Session Recording components are physically secure. If possible, lock these computers in a secure room to which only authorized personnel can gain direct access.
- Isolate servers running the Session Recording components on a separate subnet or domain.
- Protect the recorded session data from users accessing other servers by installing a firewall between the Session Recording server and other servers.
- Keep the Session Recording Administration Server and SQL database up-to-date with the latest security updates from Microsoft.
- Restrict non-administrators from logging on to the administration machine.
- Strictly limit who is authorized to make recording policy changes and view recorded sessions.
- Install digital certificates, use the Session Recording file signing feature, and set up TLS communications in IIS.
- Set up MSMQ to use HTTPS as its transport. The way is to set the MSMQ protocol listed in **Session Recording Agent Properties** to HTTPS. For more information, see Troubleshoot MSMQ.
- Use TLS 1.1 or TLS 1.2 (recommended) and disable SSLv2, SSLv3, TLS 1.0 on the Session Recording server and Session Recording Database.
- Disable RC4 cipher suites for TLS on the Session Recording server and Session Recording database:

  a. Using the Microsoft Group Policy Editor, navigate to **Computer Configuration > Administrative Templates > Network > SSL Configuration Settings**.

  b. Set the **SSL Cipher Suite Order** policy to **Enabled**. By default, this policy is set to **Not Configured**.

  c. Remove any RC4 cipher suites.

- Use playback protection. Playback protection is a Session Recording feature that encrypts recorded files before they are downloaded to the Session Recording player. By default, this option is enabled and is in **Session Recording Server Properties**.
- Follow NSIT guidance for cryptographic key lengths and cryptographic algorithms.
- Configure TLS 1.2 support for Session Recording.

We recommend using TLS 1.2 as the communication protocol to ensure the end-to-end security of the Session Recording components.

To configure TLS 1.2 support of Session Recording:

a. Log on to the machine hosting the Session Recording server. Install the proper SQL Server client component and driver, and set strong cryptography for `.NET Framework` (version 4 or later).

   a. Install the Microsoft ODBC Driver 11 (or a later version) for SQL Server.

   b. Apply the latest hotfix rollup of `.NET Framework`.

   c. Install `ADO.NET - SqlClient` based on your version of .NET Framework. For more information, see `<https://support.microsoft.com/en-us/kb/3135244>`.

   d. Add a DWORD value SchUseStrongCrypto = 1 under HKEY_LOCAL_MACHINE\ \SOFTWARE\\Microsoft\\.NetFramework\\v4.0.30319 and HKEY_LOCAL_MACHINE\ \SOFTWARE\\Wow6432Node\\Microsoft\\.NetFramework\\v4.0.30319.

   e. Restart the machine.

b. Log on to the machine hosting the Session Recording policy console. Apply the latest hotfix rollup of .NET Framework, and set strong cryptography for .NET Framework (version 4 or later). The method for setting strong cryptography is the same as substeps 1–4 and 1–5. You can omit these steps if you choose to install the Session Recording policy console on the same computer as the Session Recording server.

To configure the TLS 1.2 support for SQL Server with versions earlier than 2016, see `<https://support.microsoft.com/en-us/kb/3135244>`. To use TLS 1.2, configure HTTPS as the communication protocol for the Session Recording components.

Scalability considerations

Session Recording is a highly scalable system that handles thousands or tens of thousands of sessions. Installing and running Session Recording requires few extra resources beyond what is necessary to run Citrix Virtual Apps and Desktops™ or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). However, we still recommend you consider the performance of your system if you plan to record many sessions. Or, the sessions you plan to record might result in large session files (for example, graphically intense applications).

This article explains how Session Recording achieves high scalability and how you can get the most out of your recording system at a lowest cost.

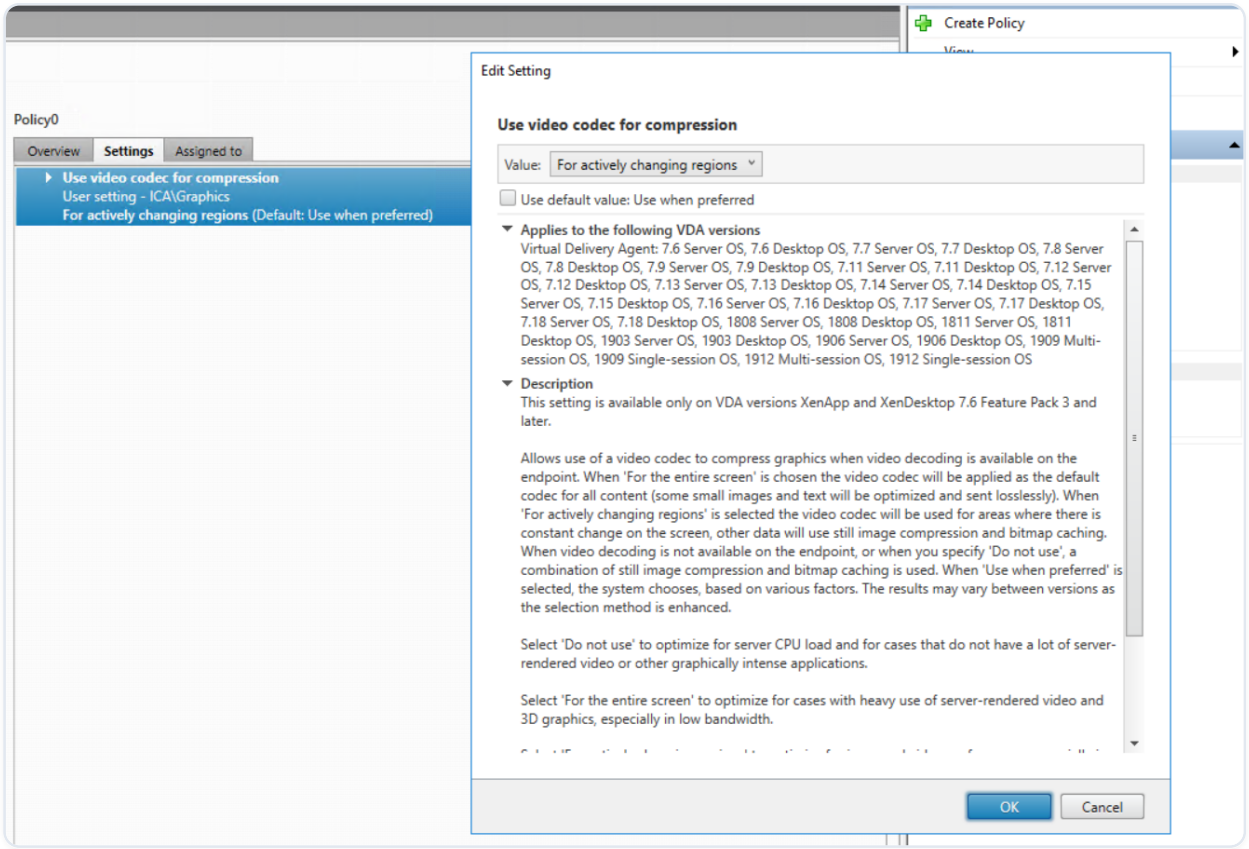
Why Session Recording scales well

There are two major reasons that Session Recording scales well compared with competitive products:

- Small file size

  A recorded session file made with Session Recording is highly compact. It is many orders of magnitude smaller than an equivalent video recording made with solutions that screen-scrape. The network bandwidth, disk space, and disk IOPS required to transport/store a recorded session file is typically at least 10 times less than an equivalent video file.

  The small size of recorded session files means faster and smoother rendering of video frames. Recordings are also lossless and have no pixelation that is common in most compact video formats. Text in recordings is easy to read during playback as it is in the original sessions. To maintain small file sizes, Session Recording does not record key frames within the files. Session Recording can drop H.264 packages while recording sessions that have videos running and thus reduce the recording file sizes. This feature is incompatible with the Compressed recording feature. To use this feature, set `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent\DropH264Enabled` to `1` on the Session Recording agent and set the value of **Use video codec for compression** to **For actively changing regions**.



- Low processing required to generate files

  A recorded session file contains the ICA® protocol data for a session that is extracted virtually in its native format. The file captures the ICA protocol data stream that is used to communicate with Citrix Workspace™ app. There is no need to run expensive transcoding or encoding software components to change the format of data in real time. The low amount of processing is also important for VDA scalability. It ensures the end-user experience is maintained when many sessions are recorded from the same VDA.

  Moreover, only those ICA virtual channels that can be played back are recorded, which results in a further optimization. For example, the printer and client drive mapping channels aren't recorded. The channels can generate high volumes of data without any benefit in video playback.

Estimate data input and processing rates

The Session Recording server is the central collection point for recorded session files. Each machine that is running a multi-session OS VDA with Session Recording enabled sends recorded session data to the Session Recording server. Session Recording can handle high volumes of data and can tolerate bursts and faults. But there are physical limits on how much data any one server can handle.

Consider how much data you send to each Session Recording server. Estimate how quickly the servers can process and store the data. The rate at which your system can store incoming data must be higher than the data input rate.

To estimate your data input rate, do the following calculation:

1. Multiply the number of recorded sessions by the average session size.
2. Divide the product by the time for which you are recording sessions.

For example, you might record 5,000 Microsoft Outlook sessions of 20 MB each over an 8-hour work day. In this case, the data input rate is approximately 28 Mbps (5,000 sessions multiplied by 20 MB, divided by 8 hours, divided by 3,600 seconds per hour, and multiplied by 8 for conversion to Mbps). A typical Session Recording server connected to a 100 Mbps LAN with sufficient disk space to store the recorded data can process data at around 5.0 Mbps. This rate is the processing rate based on the physical limits imposed by disk and network IOPS. In the example, the processing rate (5.0 Mbps) is lower than the input rate (28 Mbps), so recording the 5,000 Outlook sessions is impossible.

The amount of data per session varies greatly depending on what is being recorded. Other factors such as screen resolution, color depth, and graphics mode also have impacts. A session where CAD is running likely generates a much larger recording than a session where the user sends and receives emails in Outlook. Therefore, recording the same number of CAD sessions can generate a high input rate and require the use of more Session Recording servers.

Bursts and faults

The previous example assumes a simple uniform throughput of data but doesn't explain how the system deals with short periods of higher activity, known as bursts. A burst might occur when all users log on at the same time in the morning, known as the 9 o'clock rush. It can also occur when they receive the same email in their Outlook inbox at once. The 5.0 Mbps processing rate of the Session Recording server is highly inadequate at dealing with this sudden demand.

The Session Recording agent running on each VDA uses Microsoft Message Queuing (MSMQ) to send recorded data to the Storage Manager running on the central Session Recording server. The data is sent in a store-and-forward manner similar to how an email is delivered between the sender, mail server, and receiver. If the Session Recording server or network can't handle a high rate of data in bursts, the recorded data is temporarily stored. The data message might be temporarily stored in the outgoing queue on the VDA if the network is congested. The other case is that the data has traversed the network but the Storage Manager is busy processing other messages. In this case, the data message is stored on the Session Recording server's receiving queue.

MSMQ also serves as a fault tolerance mechanism. If the Session Recording server goes down or the link is broken, recorded data stays in the outgoing queue on each VDA. When the fault is rectified, all queued data is sent together. MSMQ also allows you to take a server offline for upgrade or maintenance without interrupting session recording and losing data.

The main limitation of MSMQ is that disk space for the temporary storage of data messages is finite. This limitation limits how long a burst, fault, or maintenance event can last before data is eventually lost. The overall system can continue after data loss, but in this situation, individual recordings have chunks of data missing. A file with missing data is still playable but only up to the point where data was first lost. Note the following:

- Adding more disk space to each server, especially the Session Recording server, and making it available to MSMQ can increase the tolerance to bursts and faults.
- It is important to configure the Message Life setting for each Session Recording agent to an appropriate level (on the **Connections** tab in Session Recording agent Properties). The default value is 7,200 seconds (two hours). It means that each recorded data message has two hours

to reach the Storage Manager before the Storage Manager discards it and damages the recording file. With more disk space available (or fewer sessions to record), you can choose to increase this value. The maximum value is 365 days.

The other limitation with MSMQ is that when data backlogs, there is extra disk IOPS in the queue to read and write data messages. Normally, the Storage Manager receives and processes data from the network directly, without data messages ever being written to disk. Storing the data involves a single write operation to disk that appends the recorded session file. When data is backlogged, the disk IOPS is tripled: each message must be written to disk, read from disk, and written to file. As the Storage Manager is heavily IOPS bound, the processing rate of the Session Recording server drops until the backlog of messages is cleared. To mitigate the effects of this extra IOPS, adopt the following recommendations:

- Make sure that the disk on which MSMQ stores messages is different from the recording file storage folders. Even though IOPS bus traffic is tripled, the drop in the true processing rate is never as severe.
- Plan outages at off-peak times only. Depending on budget constraints, follow recognized approaches to building high availability servers. The approaches include the use of Uninterruptible Power Supply (UPS), dual NICs, redundant switches, and hot swappable memory and disks.

Design for spare capacity

The data rate of recorded session data is unlikely to be uniform, bursts and faults might occur, and the clearing of message backlogs is expensive in IOPS. For this reason, design each Session Recording server with plenty of spare capacity. Adding more servers or improving the specification of existing servers, as described in later sections, always gains you extra capacity. The general rule of thumb is to run each Session Recording server at a maximum of 50% of its total capacity. In the earlier example, if the server can process 5.0 Mbps, target the system to run only at 2.5 Mbps.

Backlogs and live playback

Live playback is when a reviewer opens a session recording for playback while the session is still active. During live playback, the responsible Session Recording agent switches to a streaming mode for that session. Recording data is sent immediately to the Storage Manager without internal buffering. Because the recording file is constantly updated, the player can continue to be fed with the latest data from the live session. However, data sent from the agent to the Storage Manager is through MSMQ, so the queuing rules described earlier apply. A problem can occur in this scenario. When MSMQ is backlogged, the new recorded data available for live playback is queued like all

other data messages. The reviewer can still play the file, but viewing the latest live recorded data is delayed. If live playback is an important feature for reviewers, ensure a low probability of backlog. You can design spare capacity and fault tolerance into your deployment.

System scalability

Session Recording never reduces session performance and never stops sessions in response to recorded data backlogs. Maintaining the end-user experience and single-server scalability is paramount in the design of the Session Recording system. If the recording system becomes irreversibly overloaded, recorded session data is discarded. Recording ICA sessions has a low impact on the performance and scalability of VDAs. The size of the impact depends on the platform, the memory available, and the graphical nature of the sessions being recorded. With the following configuration, you can expect a single-server scalability impact of between 1% and 5%. In other words, if a server can host 100 users without Session Recording installed, it can host 95–99 users after installation:

- 64-bit server with 8 GB RAM running a multi-session OS VDA
- All sessions running Office productivity applications, such as Outlook and Excel
- The use of applications is active and sustained
- All sessions are recorded as configured by the Session Recording policies

With fewer sessions recorded or session activity less sustained and more sporadic, the impact is less. Often times, the scalability impact is negligible and user density per server remains the same. As mentioned earlier, the low impact results from the simple processing requirements of the Session Recording components on each VDA. Recorded data is extracted from the ICA session stack and sent as-is to the Session Recording server through MSMQ. There is no expensive encoding of data.

There is a minor overhead of using Session Recording even when no sessions are recorded. If you are not going to record any sessions from a particular server, you can disable recording on that server. Removing Session Recording is one way. A less invasive approach is to clear the **Enable session recording for this VDA machine** check box on the **Session Recording** tab in **Session Recording Agent Properties**. If session recording is required in future, reselect this check box.

Measuring throughput

You can measure the throughput of recorded session data from the sending VDA to the receiving Session Recording server. A simple and effective approach is to observe the size of recording files and the rate at which disk space on the Session Recording server is being consumed. The volume

of data written to disk closely reflects the volume of network traffic being generated. The Windows Performance Monitor tool (perfmon.exe) has standard system counters that you can observe in addition to some counters provided by Session Recording. Counters can be used to measure throughput, and identify bottlenecks and system problems. The following table outlines some of the most useful performance counters.

PERFORMANCE OBJECT	COUNTER NAME	DESCRIPTION
Citrix Session Recording Agent	`Active Recording Count`	The number of sessions that are currently being recorded on a particular VDA.
Citrix Session Recording Agent	`Bytes read from the Session Recording Driver`	The number of bytes read from the kernel components responsible for acquiring session data. Useful for determining how much data a single VDA generates for all sessions recorded on that server.
Citrix Session Recording Storage Manager	`Active Recording Count`	Similar to the Citrix Session Recording agent counter except for the Session Recording server. Indicates the total number of sessions currently being recorded for all servers.
Citrix Session Recording Storage Manager	`Message bytes/sec`	The throughput of all recorded sessions. Can be used to determine the rate at which the Storage Manager is processing data. If MSMQ is backlogged with messages, the Storage Manager runs at full speed. This value can be used to indicate the maximum processing rate of the Storage Manager.

PERFORMANCE OBJECT	COUNTER NAME	DESCRIPTION
LogicalDisk	`Disk Write Bytes/sec`	Can be used to measure disk write-through performance, which is important in achieving high scalability for the Session Recording server. Performance of individual drives can also be observed.
MSMQ Queue	`Bytes in Queue`	Can be used to determine the amount of data backlogged in the CitrixSmAudData message queue. If this value increases over time, the rate of recorded data received from the network is greater than the rate at which the Storage Manager can process data. This counter is useful for observing the effect of data bursts and faults.
MSMQ Queue	`Message in Queue`	Similar to the Bytes in Queue counter but measures the number of messages.
Network Interface	`Bytes Total/sec`	Can be used to measure on both sides of the link to observe how much data is generated when sessions are recorded. When measured on the Session Recording server, this counter indicates the rate at which incoming data is received. Contrasts with the Citrix Session Recording Storage Manager `Message bytes/sec` counter that measures the processing rate of data. If the network rate is greater than

PERFORMANCE OBJECT	COUNTER NAME	DESCRIPTION
		this value, messages build in the message queue.
Processor	`% Processor Time`	Worth monitoring even though CPU is unlikely to be a bottleneck.

Session Recording server hardware

You can increase the capacity of your deployment by carefully selecting the Session Recording server hardware. You have two choices: scaling up (by increasing the capacity of each server) or scaling out (by adding more servers). In making either of the choices, your aim is to increase scalability at a lowest cost.

Scaling up

When examining a single Session Recording server, consider the following best practices to ensure optimal performance for available budgets. The system depends on IOPS that can ensure a high throughput of recorded data from the network onto the disk. So it is important to invest in appropriate network and disk hardware. For a high-performance Session Recording server, a dual CPU or dual core CPU is recommended but little is gained from any higher specification. 64-bit processor architecture is recommended but an x86 processor type is also suitable. 4 GB of RAM is recommended but again there is little benefit from adding more.

Scaling out

Even with the best scaling up practices, there are limits to performance and scalability that can be reached with a single Session Recording server when recording many sessions. It might be necessary to add extra servers to meet the load. You can install more Session Recording servers on different machines to have the Session Recording servers work as a load balancing pool. In this type of deployment, the Session Recording servers share the storage and the database. To distribute the load, point the Session Recording agents to the load balancer that is responsible for the workload distribution.

Network capacity

A 100 Mbps network link is suitable for connecting a Session Recording server. A Gb Ethernet connection might improve performance, but does not result in 10 times greater performance than a 100 Mbps link. In practice, the gain in throughput is less.

Ensure that network switches used by Session Recording are not shared with third-party applications that might compete for available network bandwidth. Ideally, network switches are dedicated for use with the Session Recording server. If network congestion proves to be the bottleneck, a network upgrade is a relatively inexpensive way to increase the scalability of the system.

Storage

Investment in disk and storage hardware is the single most important factor in server scalability. The faster that data can be written to disk, the higher the performance of the overall system. When selecting a storage solution, take more note of the write performance than the read performance.

Store data on a RAID or a SAN.

> **Note:**
>
> Storing data on a NAS, based on file-based protocols such as SMB and NFS, might have performance and security implications. Use the latest version of the protocol in place to avoid security implications and perform scale testing to ensure proper performance.

> For a local drive setup, aim for a disk controller with built-in cache memory. Caching allows the controller to use elevator sorting during write-back. It minimizes disk head movement and ensures that write operations are completed without waiting for the physical disk operation to complete. It can improve write performance significantly at a minimal extra cost. Caching does however raise the problem of data loss after a power failure. To ensure the integrity of data and the file system, consider a battery backup facility for the caching disk controller.

Consider using a suitable RAID storage solution. There are many RAID levels available depending on performance and redundancy requirements. The following table specifies each of the RAID levels and how applicable each standard is to Session Recording.

RAID LEVEL	TYPE	MINIMUM NUMBER OF DISKS	DESCRIPTION
RAID 0	Striped set without parity	2	Provides high performance but no redundancy. Loss of any disk destroys the array. RAID 0 is a

RAID LEVEL	TYPE	MINIMUM NUMBER OF DISKS	DESCRIPTION
			low cost solution for storing recorded session files where the impact of data loss is low. Easy to scale up performance by adding more disks.
RAID 1	Mirrored set without parity	2	No performance gain over one disk, making it a relatively expensive solution. Use this solution only if a high level of redundancy is required.
RAID 3	Striped set with dedicated parity	3	Provides high write performance with redundancy characteristics similar to RAID 5. RAID 3 is recommended for video production and live streaming applications. As Session Recording is this type of application, RAID 3 is most highly recommended but it is not common.
RAID 5	Striped set with distributed parity	3	Provides high read performance with redundancy but at the cost of slower write performance.

RAID LEVEL	TYPE	MINIMUM NUMBER OF DISKS	DESCRIPTION
			RAID 5 is the most common for general purpose usages. But due to the slow write performance, RAID 5 is not recommended for Session Recording. RAID 3 can be deployed at a similar cost but with better write performance.
RAID 10	Mirrored set and striped set	4	Provides performance characteristics of RAID 0 with redundancy benefits of RAID 1. An expensive solution that is not recommended for Session Recording.

RAID 0 and RAID 3 are the most recommended RAID levels. RAID 1 and RAID 5 are popular standards but are not recommended for Session Recording. RAID 10 does provide some performance benefits but is too expensive for the additional gain.

Decide on the type and specification of disk drives. IDE/ATA drives and external USB or Firewire drives are not suitable for use in Session Recording. The main choice is between SATA and SCSI. SATA drives provide reasonably high transfer rates at a reduced cost per MB compared with SCSI drives. However, SCSI drives provide better performance and are more common in server deployments. Server RAID solutions mostly support SCSI drives but some SATA RAID products are now available. When evaluating the specifications of disk drive products, consider the rotational speed of disk and other performance characteristics.

Because the recording of thousands of sessions per day can consume significant amounts of disk space, you must choose between overall capacity and performance. From the earlier example, recording 5,000 Outlook sessions over an 8-hour work day consumes about 100 GB of storage

space. To store 10 days' worth of recordings (that is, 50,000 recorded session files), you need 1,000 GB (1 TB). This pressure on disk space can be eased by shortening the retention period before archiving or deleting old recordings. If 1 TB of disk space is available, a seven-day retention period is reasonable, ensuring disk space usage remains around 700 GB, with 300 GB remaining as a buffer for busy days. In Session Recording, the archiving and deleting of files is supported with the ICLDB utility. It has a minimum retention period of two days. You can schedule a background task to run once a day at some off-peak time. For more information about the **ICLDB** commands and archiving, see Manage your database records.

The alternative to using local drive and controllers is to use a SAN storage solution based on block-level disk access. To the Session Recording server, the disk array appears as a local drive. SANs are more expensive to set up, but as the disk array is shared, SANs do have the advantage of simplified and centralized management. There are two main types of SAN: Fibre Channel and iSCSI. iSCSI is essentially SCSI over TCP/IP and is gaining popularity over Fibre Channel since the introduction of Gb Ethernet.

Database scalability

The volume of data sent to the Session Recording database is small because the database stores only metadata about the recorded sessions. The files of the recorded sessions themselves are written to a separate disk. Typically, each recorded session requires only about 1 KB of space in the database, unless the Session Recording Event API is used to insert searchable events to the session.

The Express Editions of Microsoft SQL Server 2019, Microsoft SQL Server 2017, Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012, and Microsoft SQL Server 2008 R2 impose a database size limitation of 10 GB. At 1 KB per recording session, the database can catalog about 4,000,000 sessions. Other editions of Microsoft SQL Server have no database size restrictions and are limited only by available disk space. As the number of sessions in the database increases, performance of the database and speed of searches diminishes only negligibly.

If you are not making customizations through the Session Recording Event API, each recorded session generates four database transactions: two when recording starts, one when the user logs on to the session being recorded, and one when recording ends. If you use the Session Recording Event API to customize sessions, each searchable event recorded generates one transaction. Because even the most basic database deployment can handle hundreds of transactions per second, the processing load on the database is unlikely to be stressed. The impact is light enough

that the Session Recording database can run on the same SQL Server as other databases, including the Citrix Virtual Apps and Desktops data store database.

If your Session Recording deployment requires many millions of recorded sessions to be cataloged in the database, follow Microsoft guidelines for SQL Server scalability.

Install, upgrade, and uninstall

> **Note:**
>
> To configure server high availability through load balancing, see Configure load balancing in an existing deployment and Deploy and load balance Session Recording in Azure.
>
> To learn more about how to quickly set up and configure Citrix Session Recording and Citrix Session Recording service, see the Citrix Tech Zone article POC Guide: Citrix Session Recording.
>
> This article contains the following sections:

Installation checklist

Install Session Recording using the Citrix Virtual Apps and Desktops installer

Automate installation

Install the Session Recording database on cloud SQL database services

Upgrade Session Recording

Uninstall Session Recording

Integrate with Citrix Analytics for Security

Installation checklist

Before you start the installation, complete this list:

✓	STEP
	Select the machines on which you want to install each Session Recording component. Ensure that each computer meets the

✓	STEP
	hardware and software requirements for the component or components to be installed on it.
	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.
	To use the TLS protocol for communication between the Session Recording components, install the correct certificates in your environment.
	Install any hotfixes required for the Session Recording components. The hotfixes are available from the Citrix Support.
	Configure Director to create and activate the Session Recording policies. For more information, see Configure Director to use the Session Recording Server.

Note:

- We recommend that you divide the published applications into separate Delivery Groups based on your recording policies. Session sharing for published applications can conflict with the active policy if the applications are in the same Delivery Group. Session Recording matches the active policy with the first published application that a user opens. Starting with the 7.18 release, you can use the dynamic session recording feature to start or stop recording sessions at any time during the sessions. This feature can help to mitigate the conflict issue with the active policy. For more information, see Dynamic session recording.
- If you are planning to use Machine Creation Services™ (MCS) or Provisioning Services, prepare a unique QMId. Failure to comply can cause recording data losses.
- SQL Server requires TCP/IP, running SQL Server Browser service, and enabled Windows Authentication.

- To use HTTPS, configure server certificates for TLS/HTTPS.
- Ensure that users under **Local Users and Groups > Groups > Users** have write permission to the `C:\windows\Temp` folder.

Install Session Recording using the Citrix Virtual Apps™ and Desktops installer

Note:

We recommend that you install the Session Recording Administration, Session Recording agent, and Session Recording player components on separate servers.

The Session Recording Administration components include the Session Recording database, Session Recording server, and Session Recording policy console. Installing all of them on a single server is fine for a proof of concept. However, we recommend that you install the Session Recording policy console on a separate server and install the Session Recording server, administrator logging, and Session Recording database components on another separate server.

Installing the Session Recording server lets you install the Session Recording web player automatically.

Install the Session Recording Administration components

Install the Session Recording agent

Install the Session Recording player

Install the Session Recording Administration components

Note:

Starting with 2110, before installing the Session Recording Administration components on Windows Server 2016 where TLS 1.0 is disabled, complete the following steps:

1. Install Microsoft OLE DB Driver for SQL Server.
2. Under the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319` registry key, add the `SchUseStrongCrypto` DWORD (32-bit) value and set the value data to 1.
3. Restart Windows Server 2016.

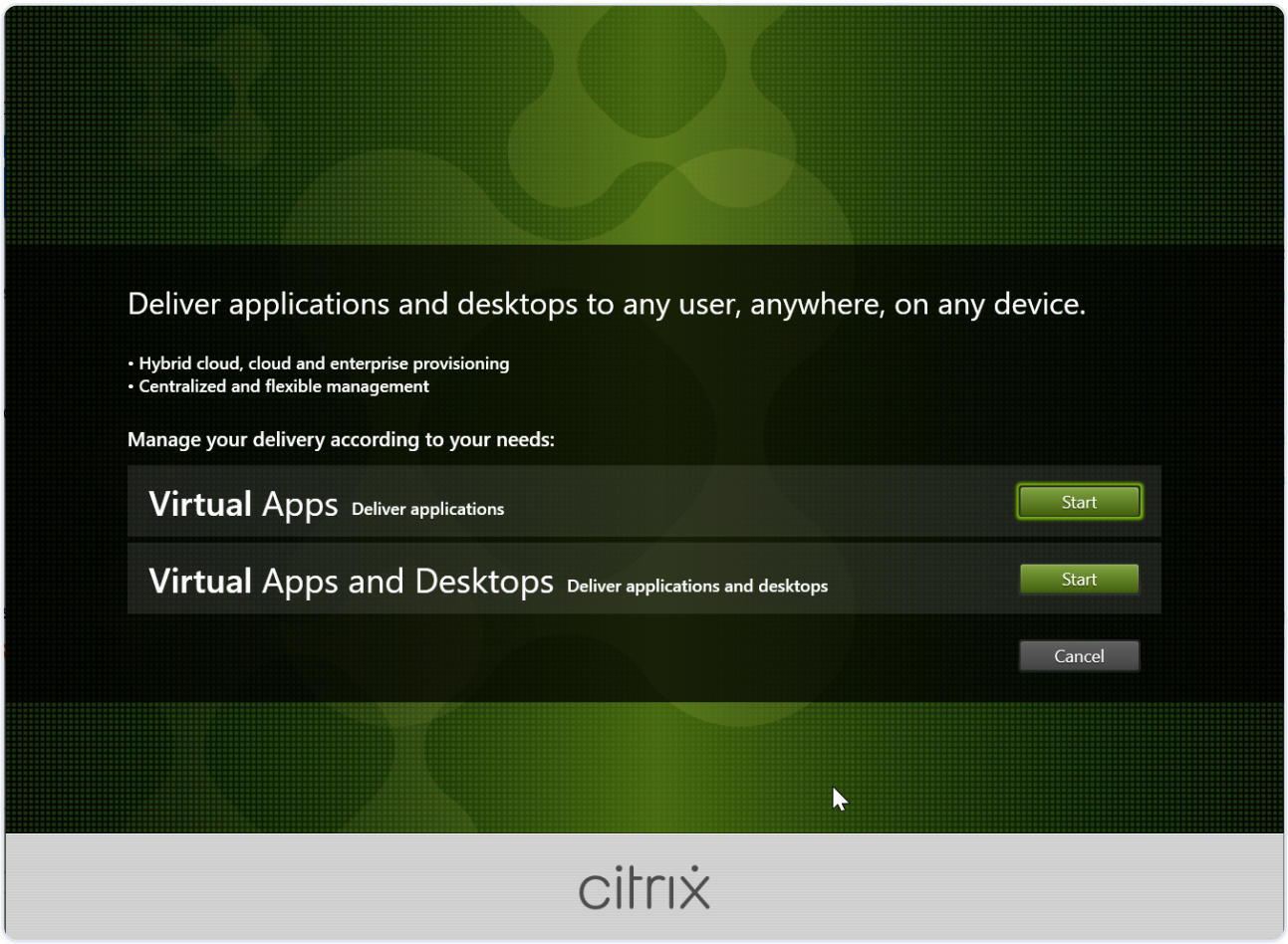
The Session Recording Administration components include the Session Recording database, Session Recording server, and Session Recording policy console. You can choose the component to install on a server.

Step 1: Download the product software and launch the wizard

1. 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.
2. Use a local administrator account to log on to the machine where you are installing the Session Recording Administration components. Insert the DVD in the drive or mount the ISO file. If the installer does not launch automatically, double-click the **AutoSelect** application or the mounted drive.

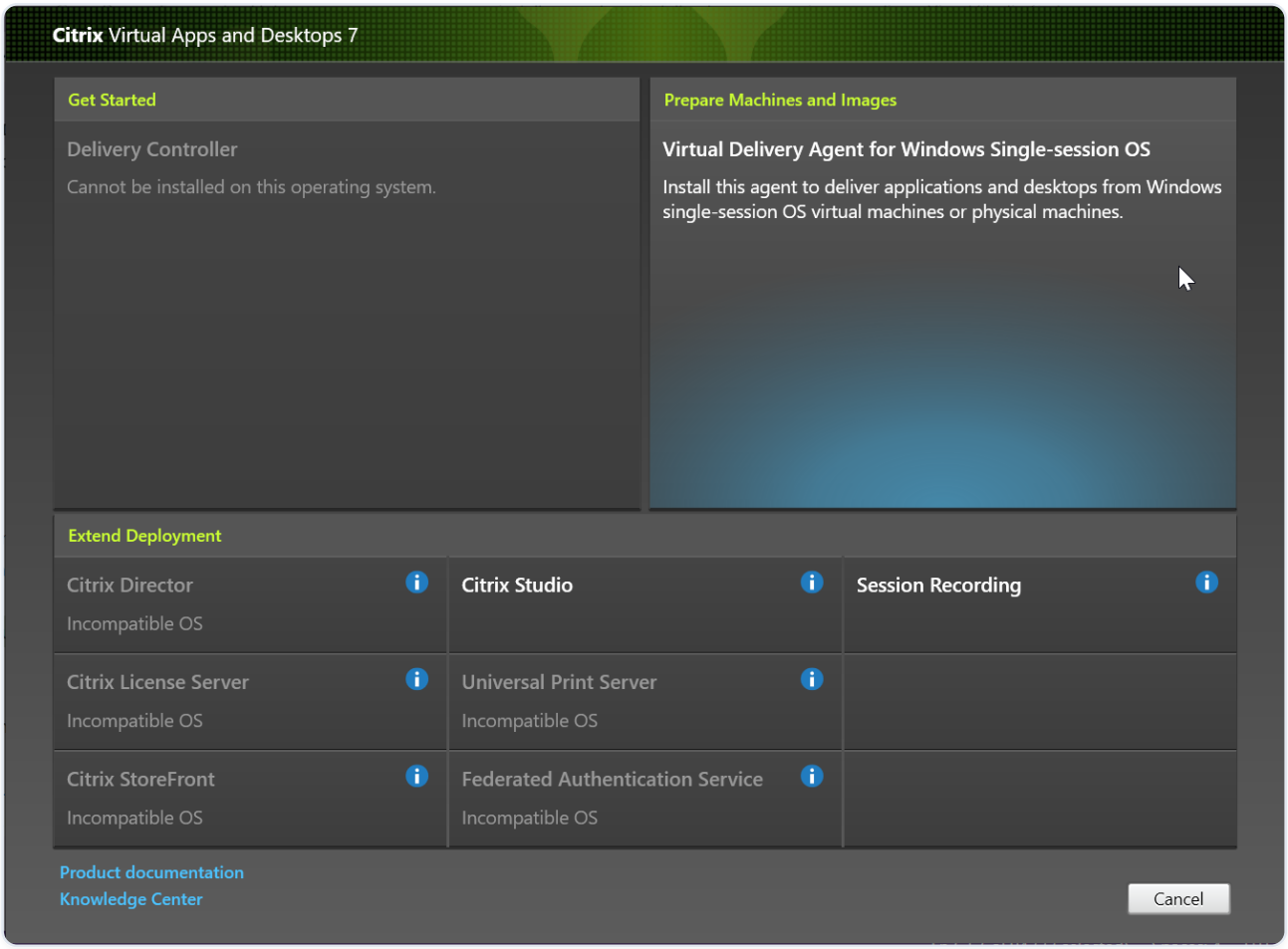
   The installation wizard launches.

Step 2: Choose which product to install



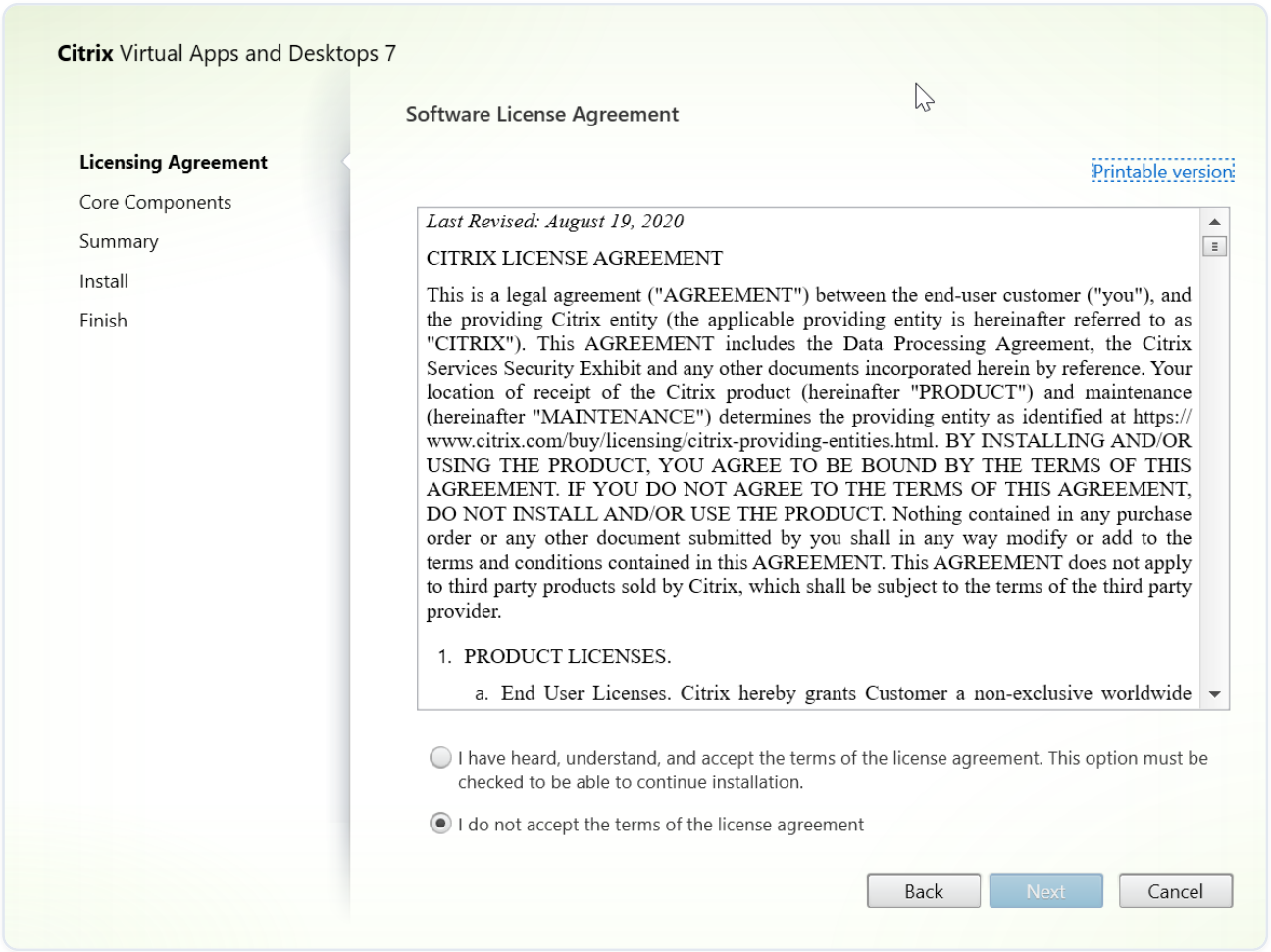
Click **Start** next to the product to install **Citrix Virtual Apps** or **Citrix Virtual Desktops™**.

Step 3: Select Session Recording



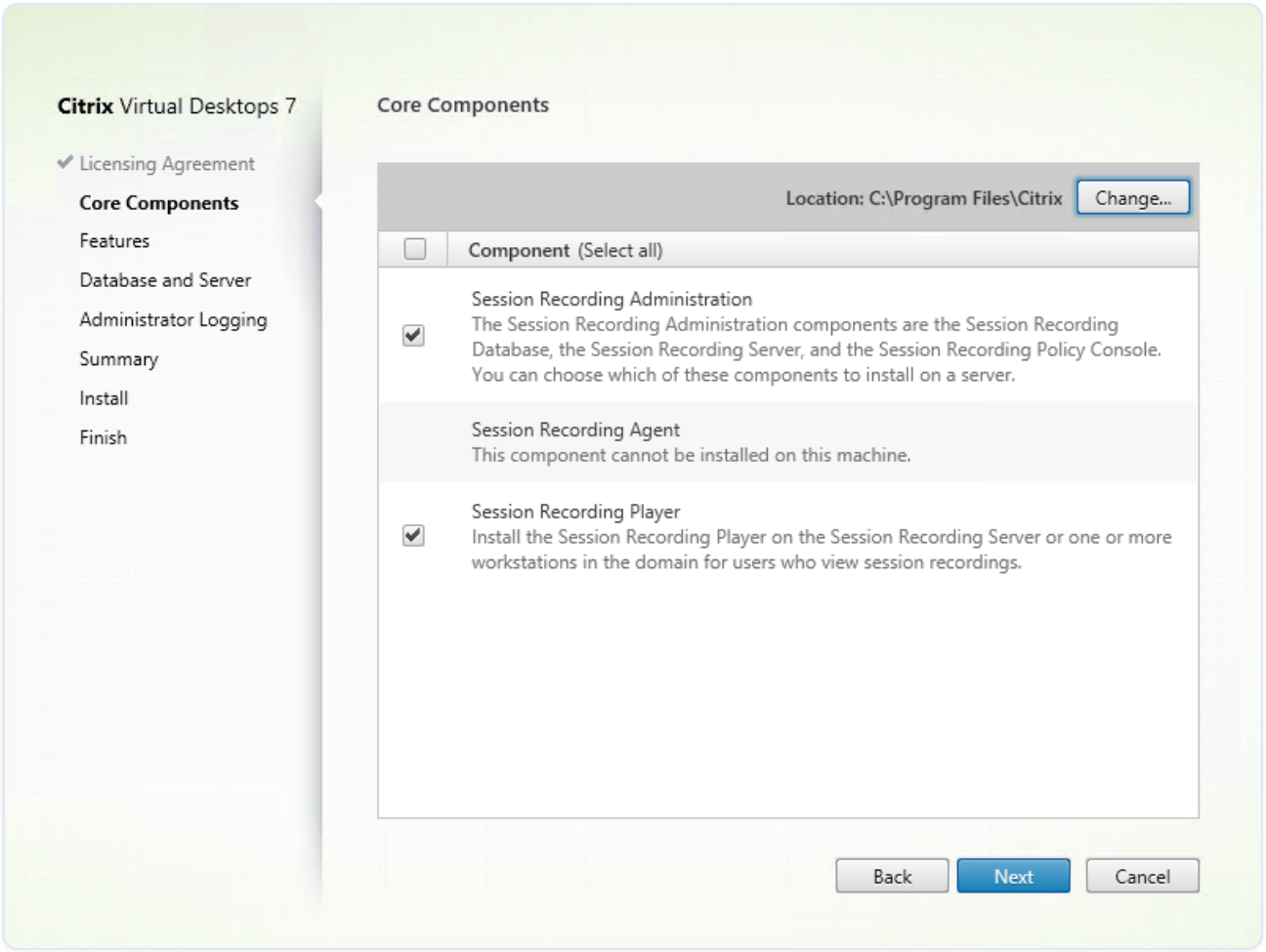
Select the **Session Recording** entry.

Step 4: Read and accept the license agreement



On the **Software License Agreement** page, read the license agreement, accept it, and then click **Next**.

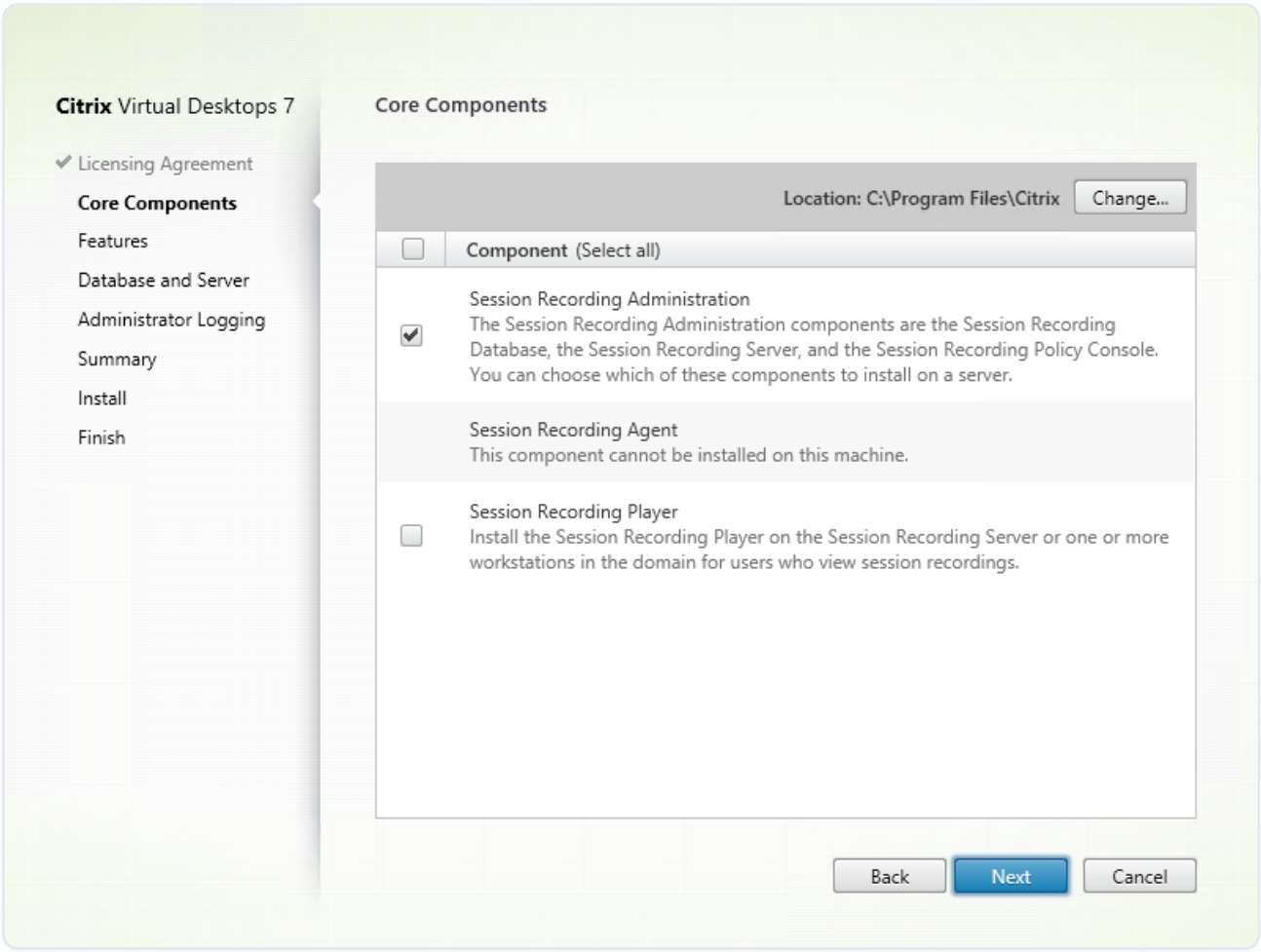
Step 5: Select the components to install and the installation location



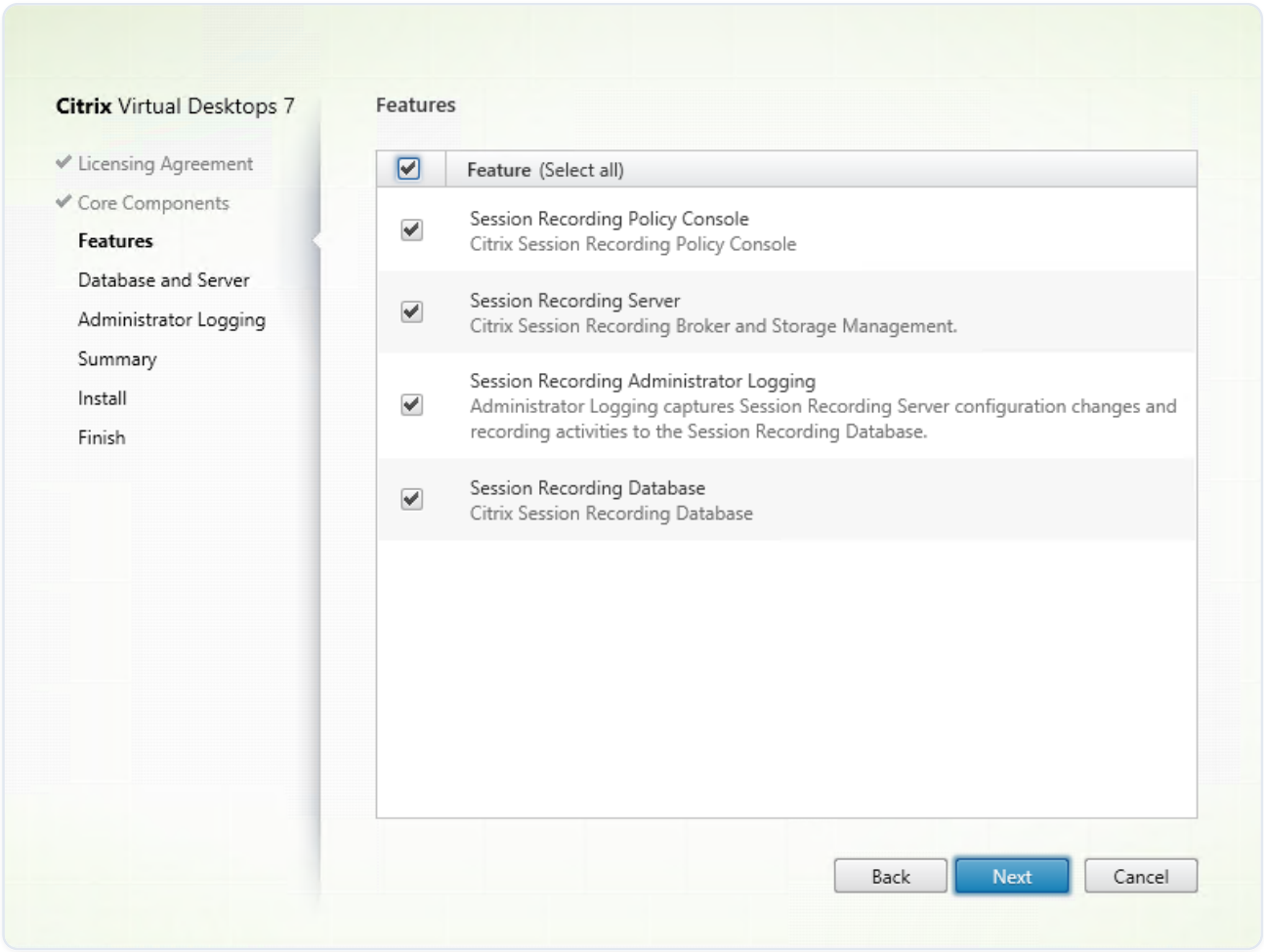
On the **Core Components** page:

- **Location**: By default, components are installed in C:\\Program Files\\Citrix. The default location works for most deployments. You can specify a custom installation location.
- **Component**: By default, all the check boxes next to the components that can be installed are selected. The installer knows whether it is running on a single-session OS or a multi-session OS. It allows the Session Recording Administration components to be installed on a multi-session OS only. It allows the Session Recording agent to be installed only on a machine that has a VDA installed. If you install the Session Recording agent on a machine that has no VDA installed in advance, the **Session Recording Agent** option is unavailable.

Select **Session Recording Administration** and click **Next**.


Citrix Virtual Desktops 7
Licensing Agreement
Core Components
Features
Database and Server
Administrator Logging
Summary
Install
Finish
Core Components
Location: C:\Program Files\Citrix
Change...
Component (Select all)
Session Recording Administration
The Session Recording Administration components are the Session Recording Database, the Session Recording Server, and the Session Recording Policy Console. You can choose which of these components to install on a server.
Session Recording Agent
This component cannot be installed on this machine.
Session Recording Player
Install the Session Recording Player on the Session Recording Server or one or more workstations in the domain for users who view session recordings.
Back
Next
Cancel

Step 6: Select the features to install



On the **Features** page:

- By default, all the check boxes next to the features that can be installed are selected. Installing all these features on a single server is fine for a proof of concept. For a large production environment, install the Session Recording policy console on a separate server. Install the Session Recording server, administrator logging, and database on another separate server.
- The Session Recording administrator logging is an optional subfeature of the Session Recording server. Select the Session Recording server before you can select the Session Recording administrator logging.
- If you select the Session Recording server, the Session Recording web player is installed too.
- To add features on the same server after you select and install features on it, you can only use the msi package. You cannot run the installer again.

Select the feature or features that you want to install and click **Next**.

Step 6.1: Install the Session Recording database

Note:

- The Session Recording database isn't an actual database. It is a component that creates and configures the required databases in the Microsoft SQL Server instance during installation. Session Recording supports three solutions for database high availability based on Microsoft SQL Server. For more information, see Database high availability.
- You can install 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

  On Azure SQL Database, installation of the Session Recording database can be done **only by** running a command similar to the following:

  ```
  msiexec /i "SessionRecordingAdministrationx64.msi"
  ADDLOCAL="SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
  DATABASEINSTANCE="DatabaseConnectionString "
  DATABASENAME="CitrixSessionRecording"
  LOGGINGDATABASENAME="CitrixSessionRecordingLogging"
  AZURESQLSERVICESUPPORT="1" CLOUDDBSUPPORT="1"
  AZUREUSERNAME="CloudSQLAdminName" AZUREPASSWORD="CloudSQLAdminPassword" /
  q /l*vx "c:\WithLogging.log"
  ```

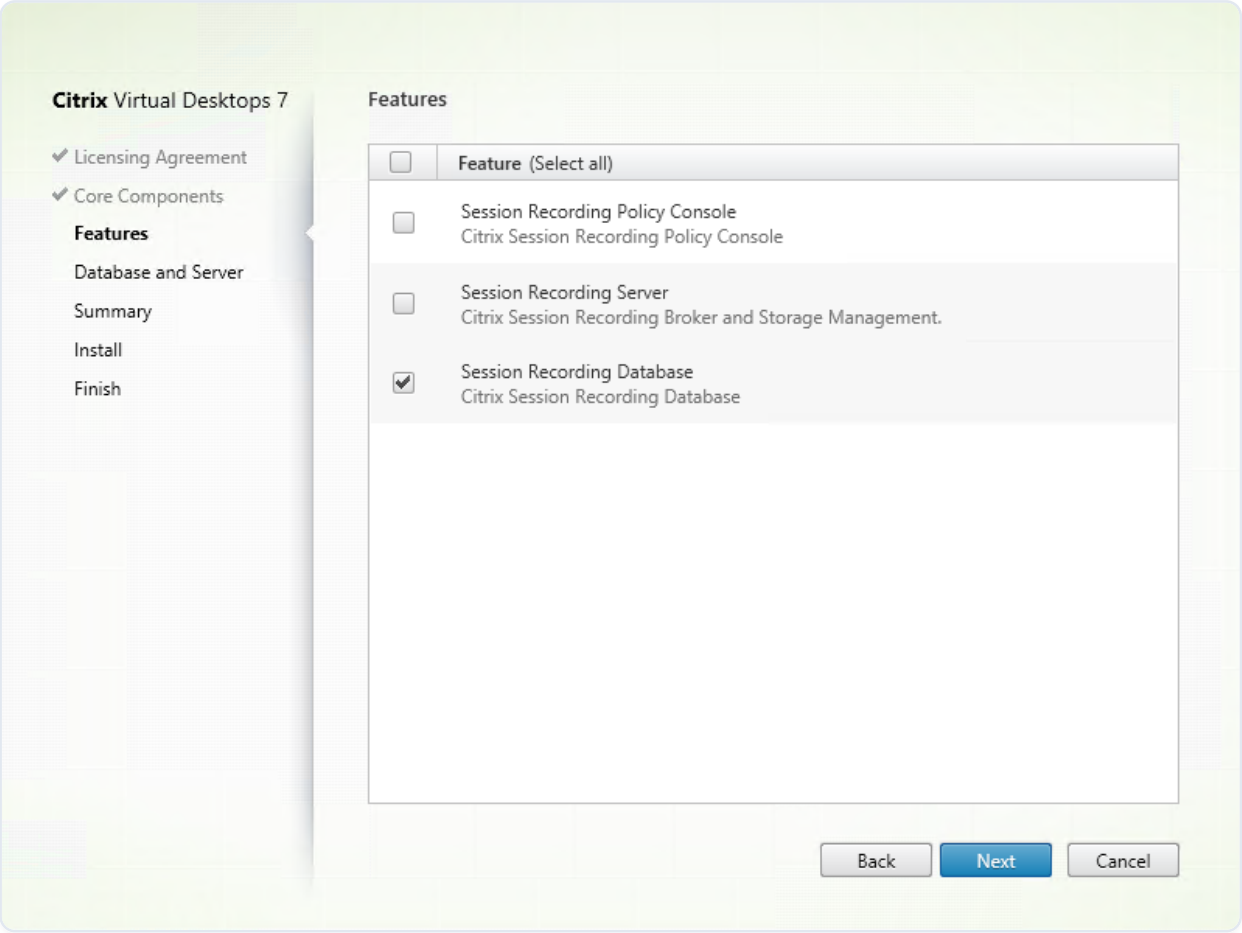
  On Azure SQL Managed Instance and on AWS RDS, installation of the Session Recording database can be done by running a command similar to the above or by double-clicking and running the SessionRecordingAdministrationx64.msi package. For more information, see Install the Session Recording database on Azure SQL Managed Instance or on AWS RDS.

  On SQL Server on Azure VMs, installation of the Session Recording database can be done by double-clicking and running the SessionRecordingAdministrationx64.msi package or by using the Citrix Virtual Apps and Desktops installer. For more information, see Install the Session Recording database on SQL Server on Azure VMs.

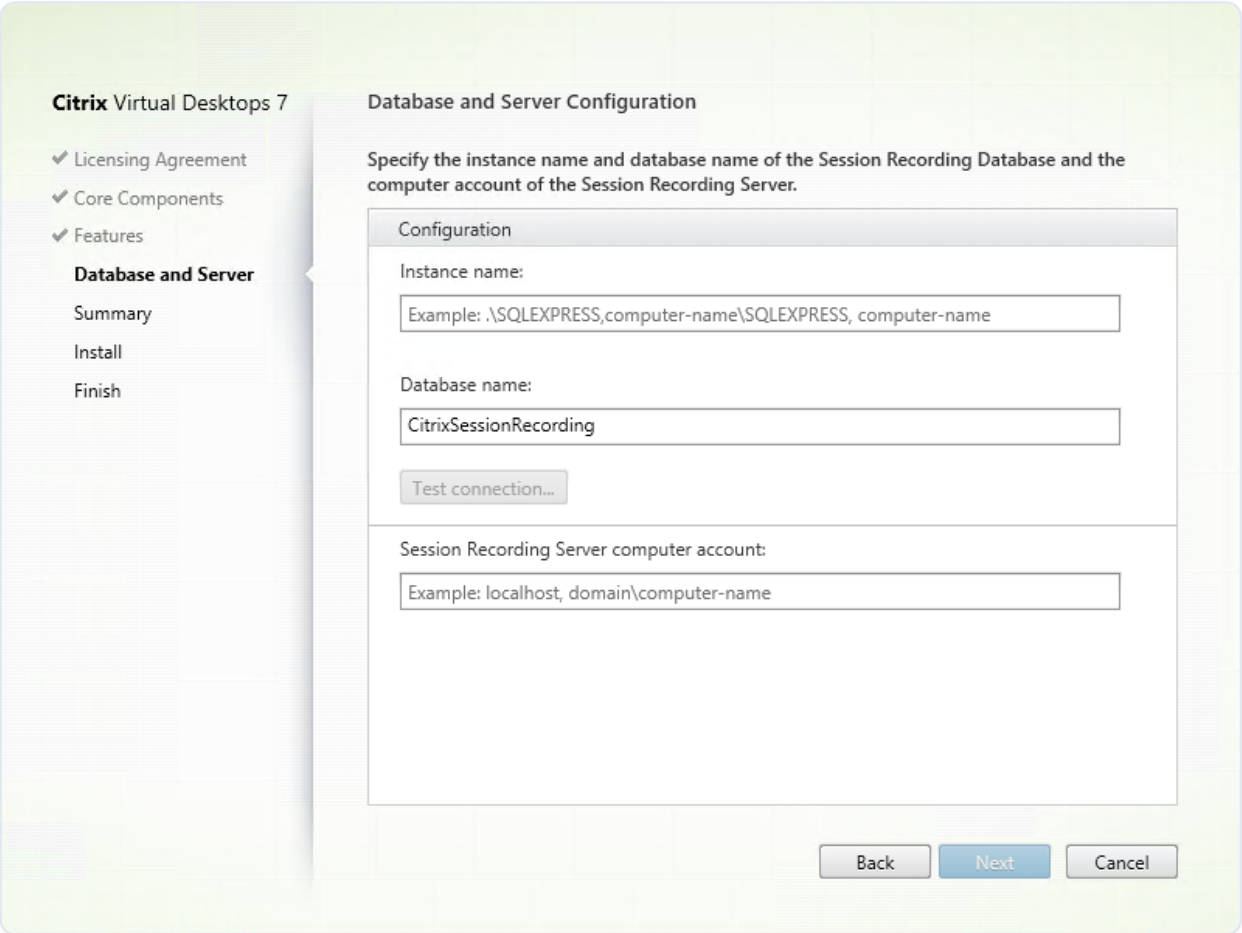
> There are typically three types of deployments for the Session Recording database and Microsoft SQL Server:

- Deployment 1: Install the Session Recording server and Session Recording database on the same machine and the Microsoft SQL Server on a remote machine. (**Recommended**)
- Deployment 2: Install the Session Recording server, Session Recording database, and Microsoft SQL Server on the same machine.
- Deployment 3: Install the Session Recording server on a machine and install both the Session Recording database and Microsoft SQL Server on another machine. (**Not recommended**)

1. On the **Features** page, select **Session Recording Database** and click **Next**.



2. On the **Database and Server Configuration** page, specify the instance name and database name of the Session Recording database and the computer account of the Session Recording server. Click **Next**.



On the **Database and Server Configuration** page:

- **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.
- **Database name**: Type a custom database name in the **Database name** text box or use the default database name preset in the text box. Click **Test connection** to test the connectivity to the SQL Server instance and the validity of the database name.

> **Important:**

> \>

> A custom database name must contain only A-Z, a-z, 0–9, and underscores, and cannot exceed 123 characters.

> You must have the **securityadmin** and **dbcreator** server role permissions of the database. If you do not have the permissions, you can:

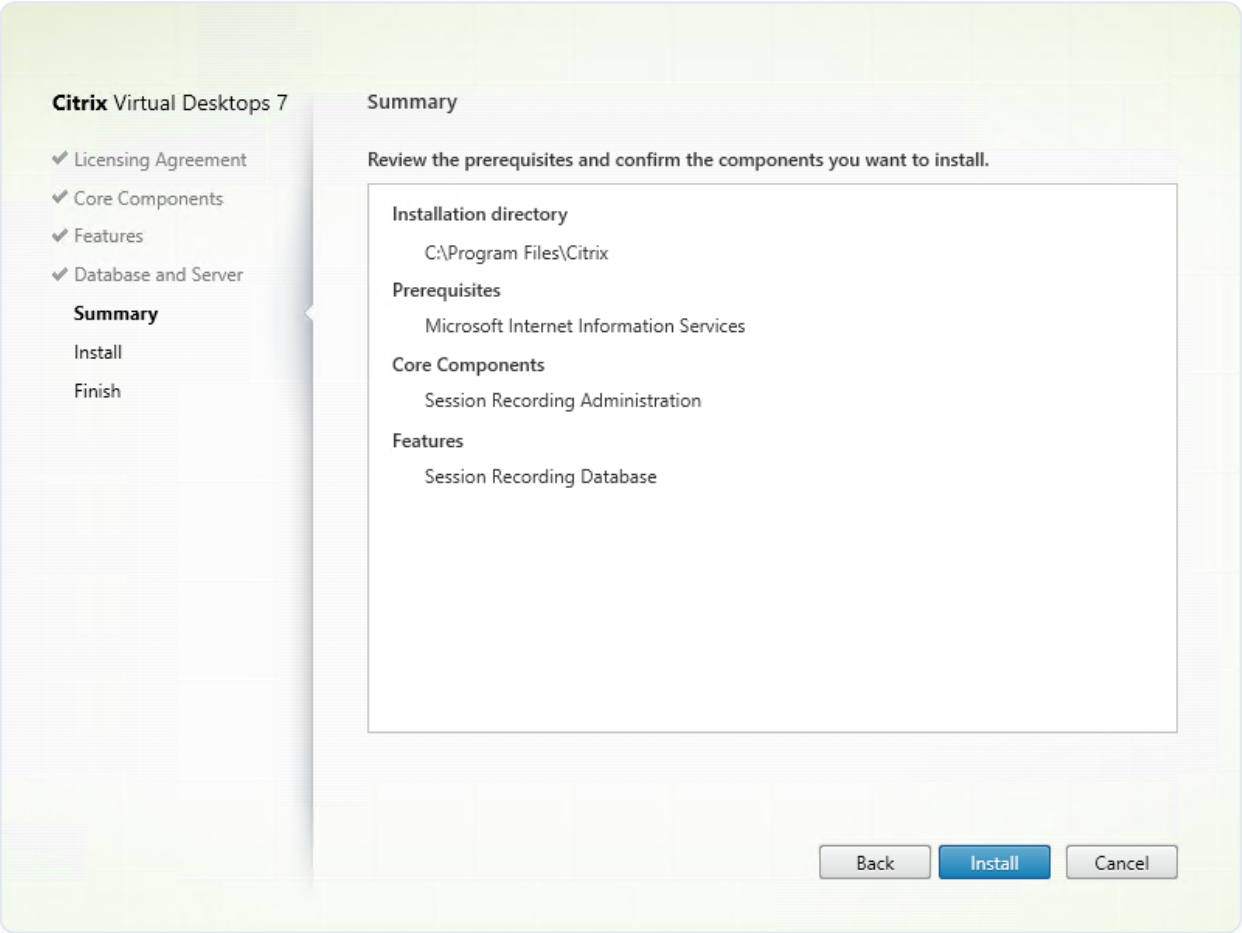
- Ask the database administrator to assign the permissions for the installation. After the installation completes, the **securityadmin** and **dbcreator** server role permissions are no longer necessary and can be safely removed.
- Or, use the SessionRecordingAdministrationx64.msi package under **\x64\Session Recording** on the Citrix Virtual Apps and Desktops ISO. During the msi installation, a dialog box prompts for the credentials of a database administrator with the **securityadmin** and **dbcreator** server role permissions. Type the correct credentials and then click **OK** to continue the installation.

  The installation creates the Session Recording database and adds the machine account of the Session Recording server as **db_owner**.

- **Session Recording Server computer account**:
  - **Deployments 1 and 2**: Type **localhost** in the **Session Recording Server computer account** text box.
  - **Deployment 3**: Type the name of the machine hosting the Session Recording server in the format of domain\\computer-name. The Session Recording server computer account is the user account for accessing the Session Recording database.

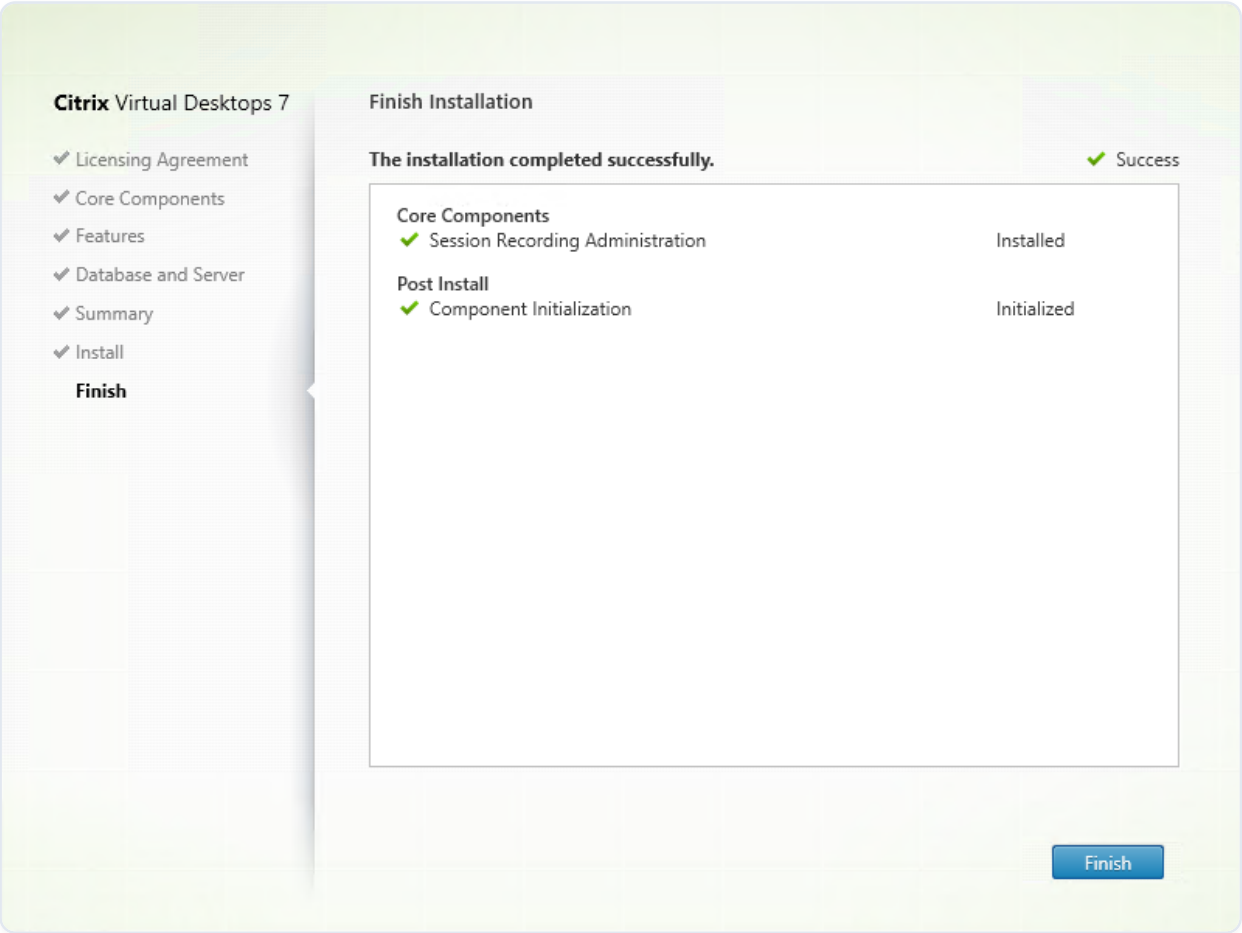
> **Note:**
>
> Attempts to install the Session Recording Administration components can fail with error code 1603 when a domain name is set in the **Session Recording Server computer account** text box. As a workaround, type **localhost** or NetBIOS domain name\\machine name in the **Session Recording Server computer account** text box. To get the NetBIOS domain name, go to the Session Recording server and run `$env:userdomain` in PowerShell or `echo %UserDomain%` in a command prompt.

3. Review the prerequisites and confirm the installation.



The **Summary** page shows your installation choices. You can click **Back** to return to the earlier wizard pages and make changes, or click **Install** to start the installation.

4. Complete the installation.



The **Finish Installation** page shows green check marks for all the prerequisites and components that have been installed and initialized successfully.

Click **Finish** to complete the installation of the Session Recording Database.

Step 6.2: Install the Session Recording server

The Session Recording server is a server that hosts:

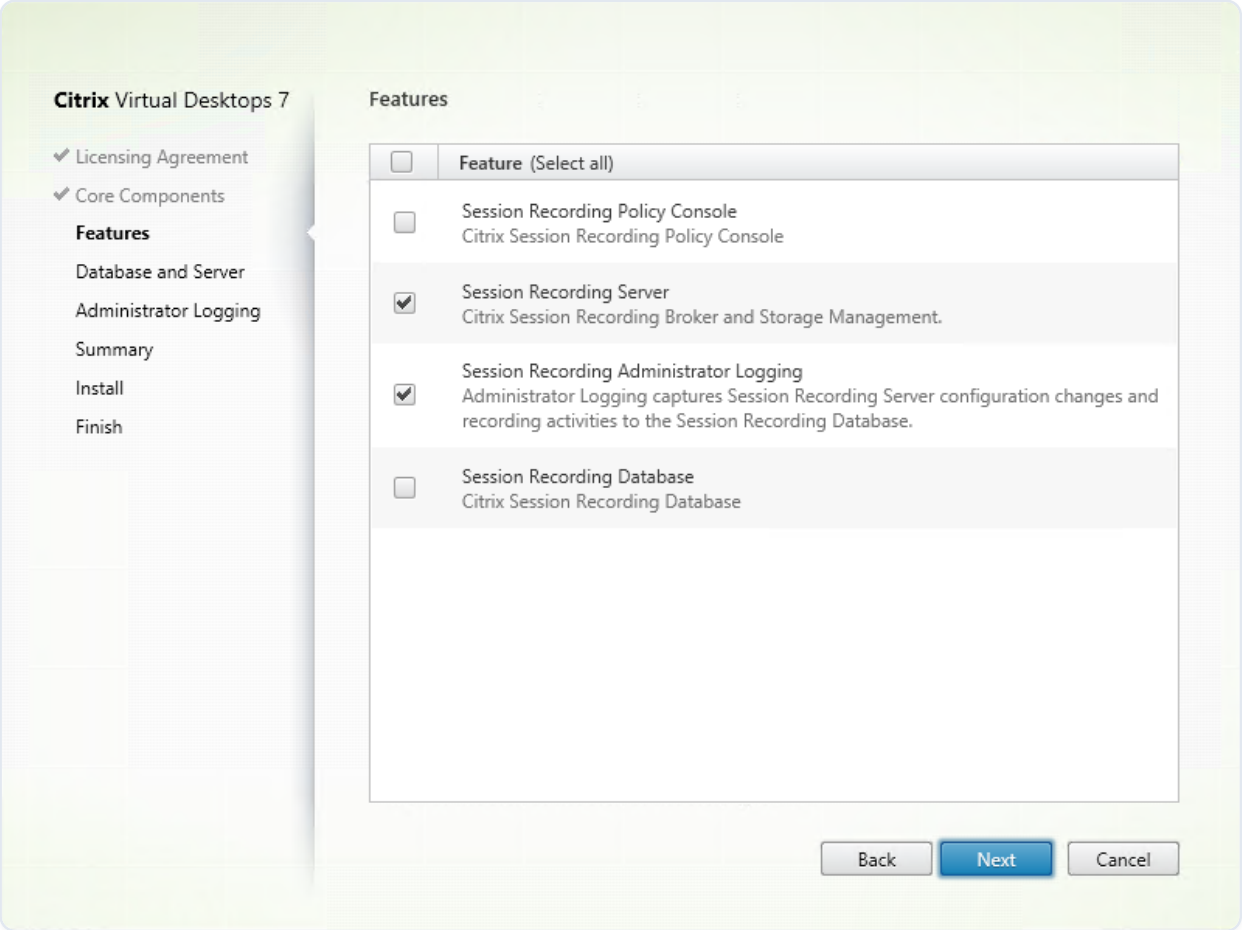
- The Broker. An IIS 6.0+ hosted Web application that serves the following purposes:
  - Handling search queries and file download requests from the Session Recording player and web player.
  - Handling policy administration requests from the Session Recording policy console.
  - Evaluating recording policies for each Citrix Virtual Apps and Desktops or Citrix DaaS™ (formerly Citrix Virtual Apps and Desktops service) session.
- The Storage Manager. A Windows service that manages the recorded session files received from each Session Recording-enabled VDA.
- Administrator Logging. An optional subcomponent installed with the Session Recording server to log the administration activities. All the logging data is stored in a separate SQL Server

database named **CitrixSessionRecordingLogging** by default. You can customize the database name.

Installing the Session Recording server lets you install the Session Recording web player automatically.

To install the Session Recording server, complete the following steps:

1. On the **Features** page, select **Session Recording Server** and **Session Recording Administrator Logging.** Click **Next**.

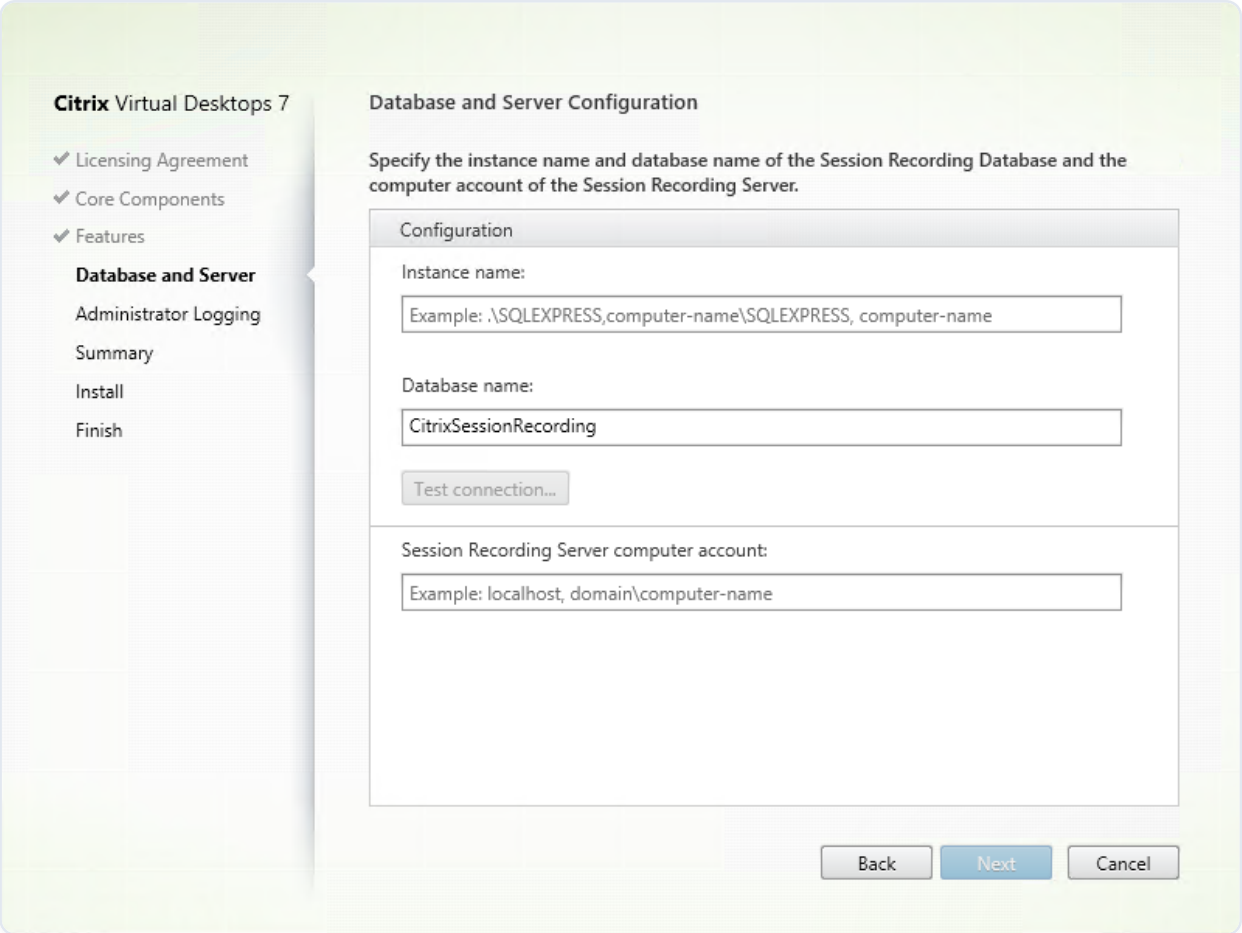


Note:

- The Session Recording administrator logging is an optional subfeature of the Session Recording server. Select the Session Recording server before you can select the Session Recording administrator logging.
- We recommend that you install the Session Recording administrator logging together with the Session Recording server at the same time. If you don't want the

> administrator logging feature to be enabled, you can disable it on a later page. However, if you choose not to install this feature at the beginning but want to add it later, you can only manually add it by using SessionRecordingAdministrationx64.msi.

2. On the **Database and Server Configuration** page, specify the configurations.



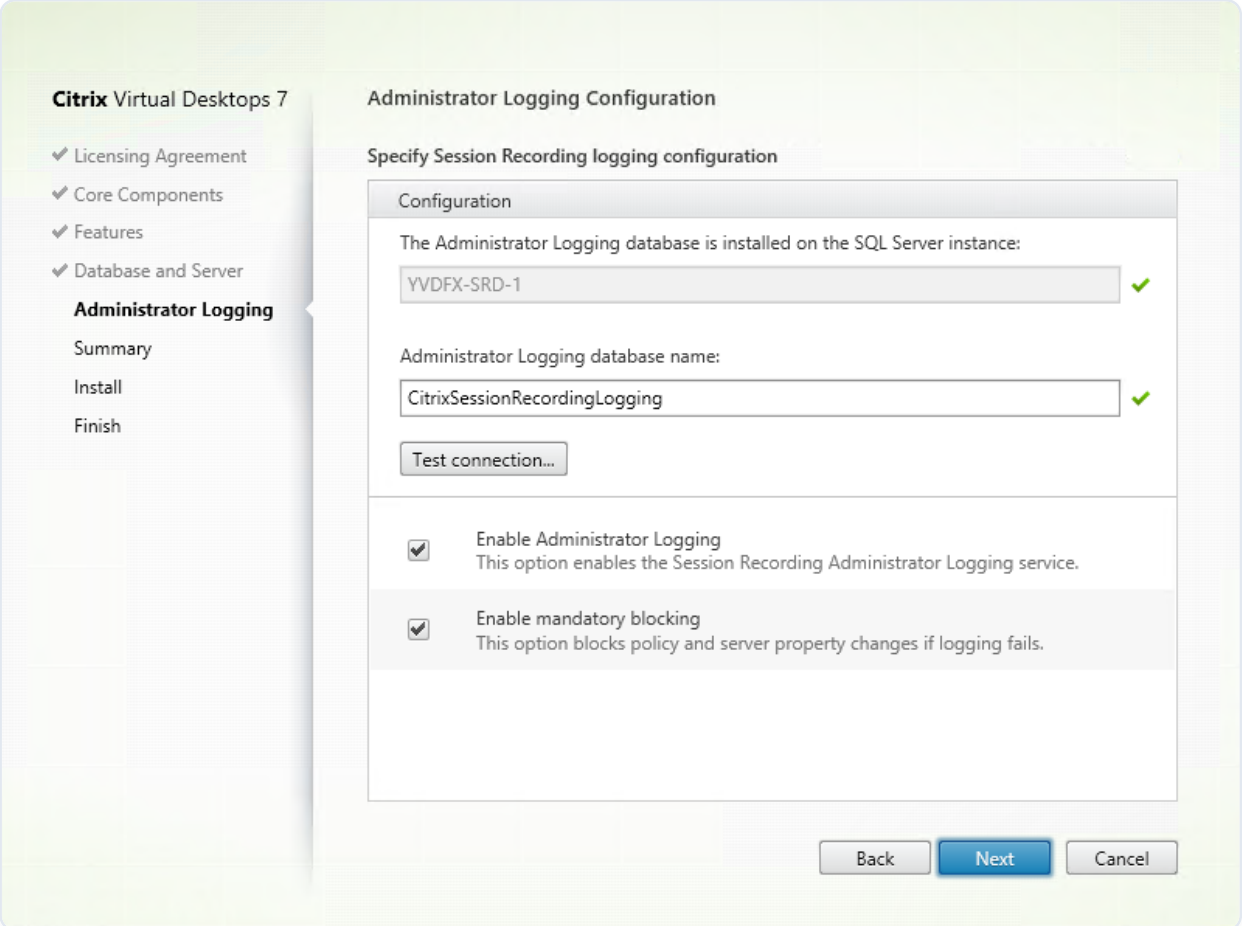
On the **Database and Server Configuration** page:

- **Instance name**: Type the name of your SQL Server in the **Instance name** text box. If you are using a named instance, type computer-name\\instance-name; otherwise, type computer-name only. 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. **Database name**: Type a custom database name in the **Database name** text box or use the default database name **CitrixSessionRecording** that is preset in the text box.
- You must have the **securityadmin** and **dbcreator** server role permissions of the database. If you do not have the permissions, you can:

- Ask the database administrator to assign the permissions for the installation. After the installation completes, the **securityadmin** and **dbcreator** server role permissions are no longer necessary and can be safely removed.
- Or, use the SessionRecordingAdministrationx64.msi package to install the Session Recording server. During the msi installation, a dialog box prompts for the credentials of a database administrator with the **securityadmin** and **dbcreator** server role permissions. Type the correct credentials and then click **OK** to continue the installation.

- After typing the correct instance name and database name, click **Test connection** to test the connectivity to the Session Recording database.
- Type the Session Recording server computer account, and then click **Next**.

3. On the **Administration Logging Configuration** page, specify configurations for the administration logging feature.



On the **Administration Logging Configuration** page:

- **The Administration Logging database is installed on the SQL Server instance**: This text box is not editable. The SQL Server instance name of the Administration Logging

database is automatically grabbed from the instance name that you typed on the **Database and Server Configuration** page.

- **Administrator Logging database name**: To install the Session Recording administrator logging feature, type a custom database name for the administrator logging database in this text box or use the default database name **CitrixSessionRecordingLogging** that is preset in the text box.

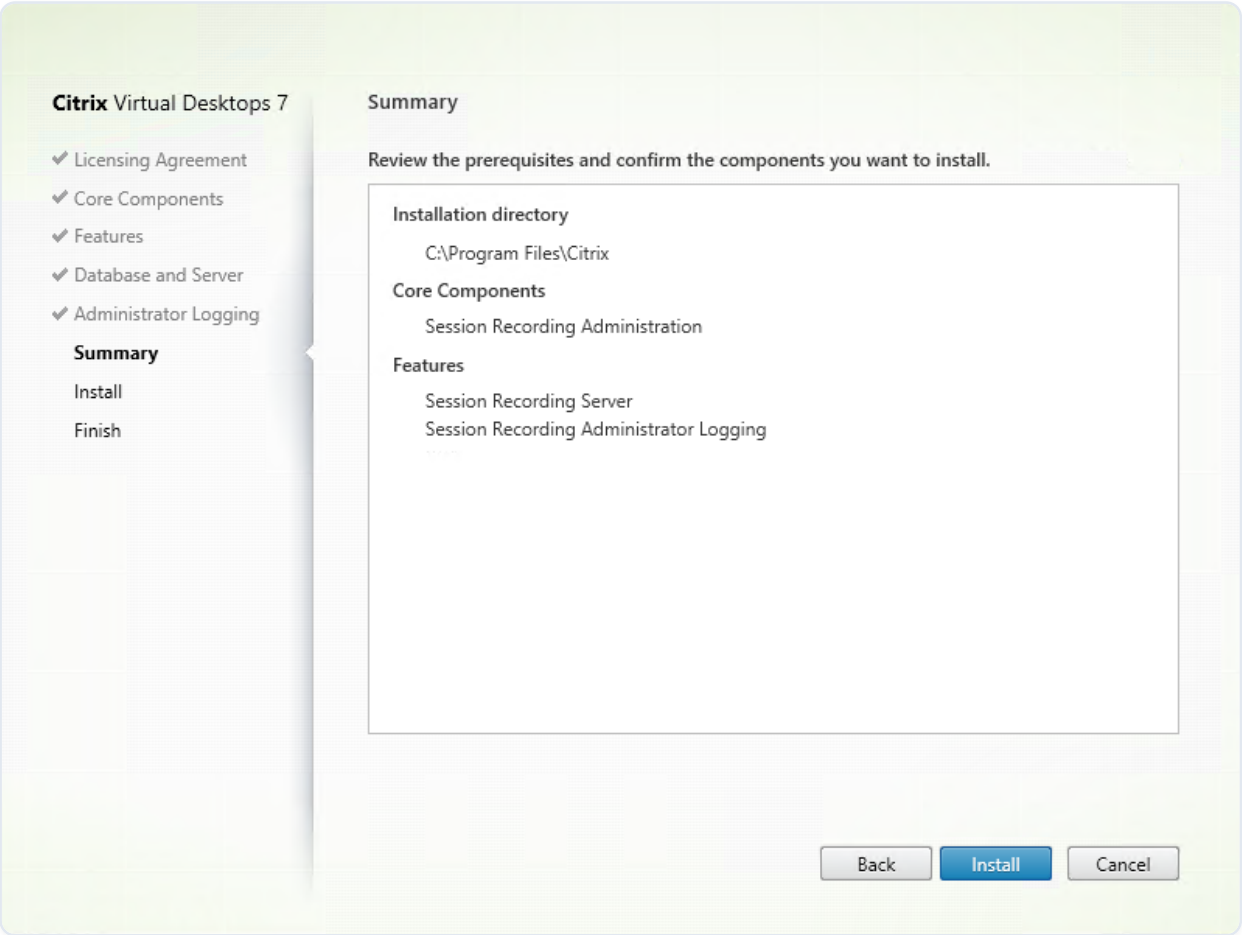
  \>**Note:**

  > The administrator logging database name must be different from the Session Recording database name that is set in the **Database name** text box on the previous **Database and Server Configuration** page.

- 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.

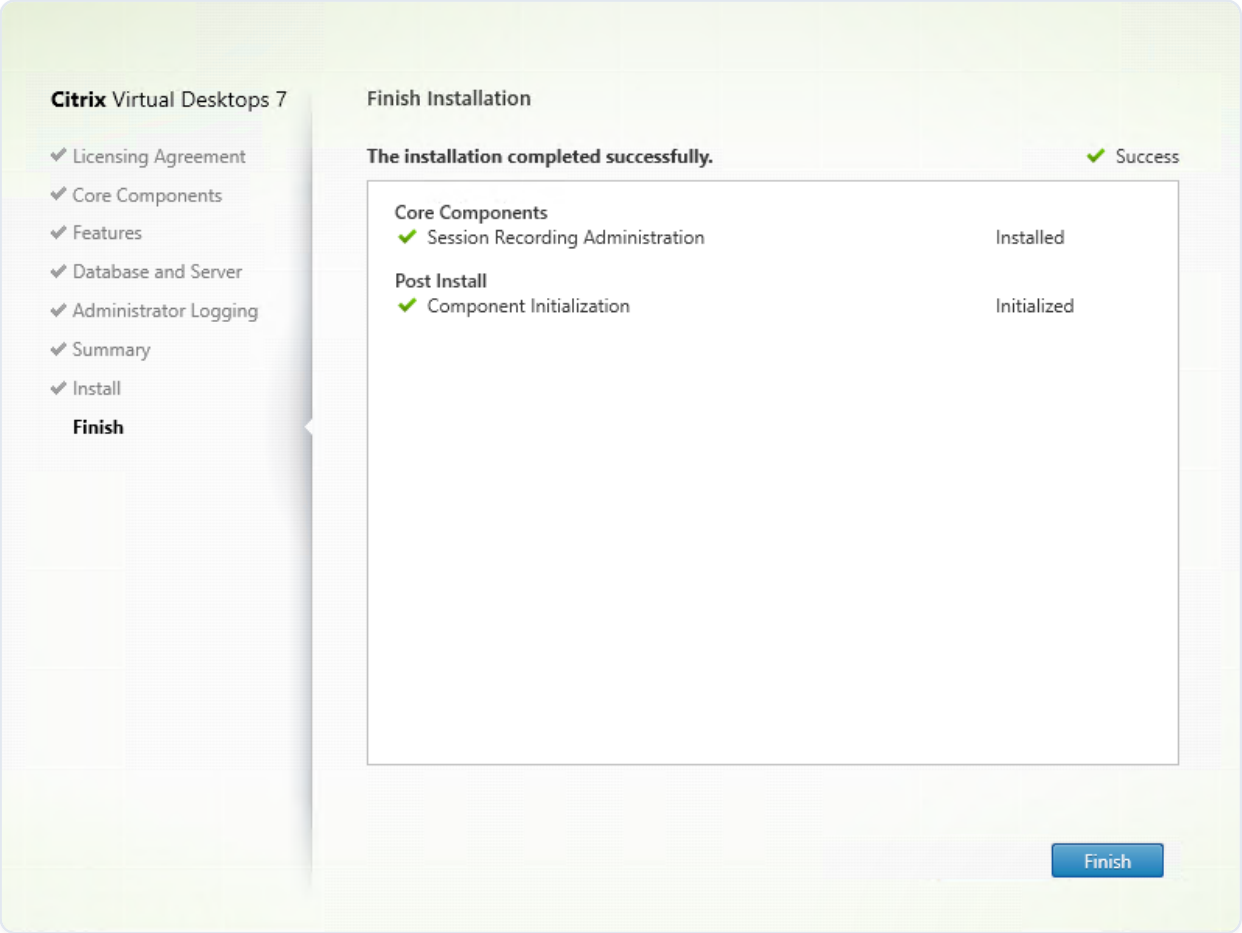
Click **Next** to continue the installation.

4. Review the prerequisites and confirm the installation.



The **Summary** page shows your installation choices. You can click **Back** to return to the earlier wizard pages and make changes, or click **Install** to start the installation.

5. Complete the installation.



The **Finish Installation** page shows green check marks for all the prerequisites and components that have been installed and initialized successfully.

Click **Finish** to complete the installation of the Session Recording server.

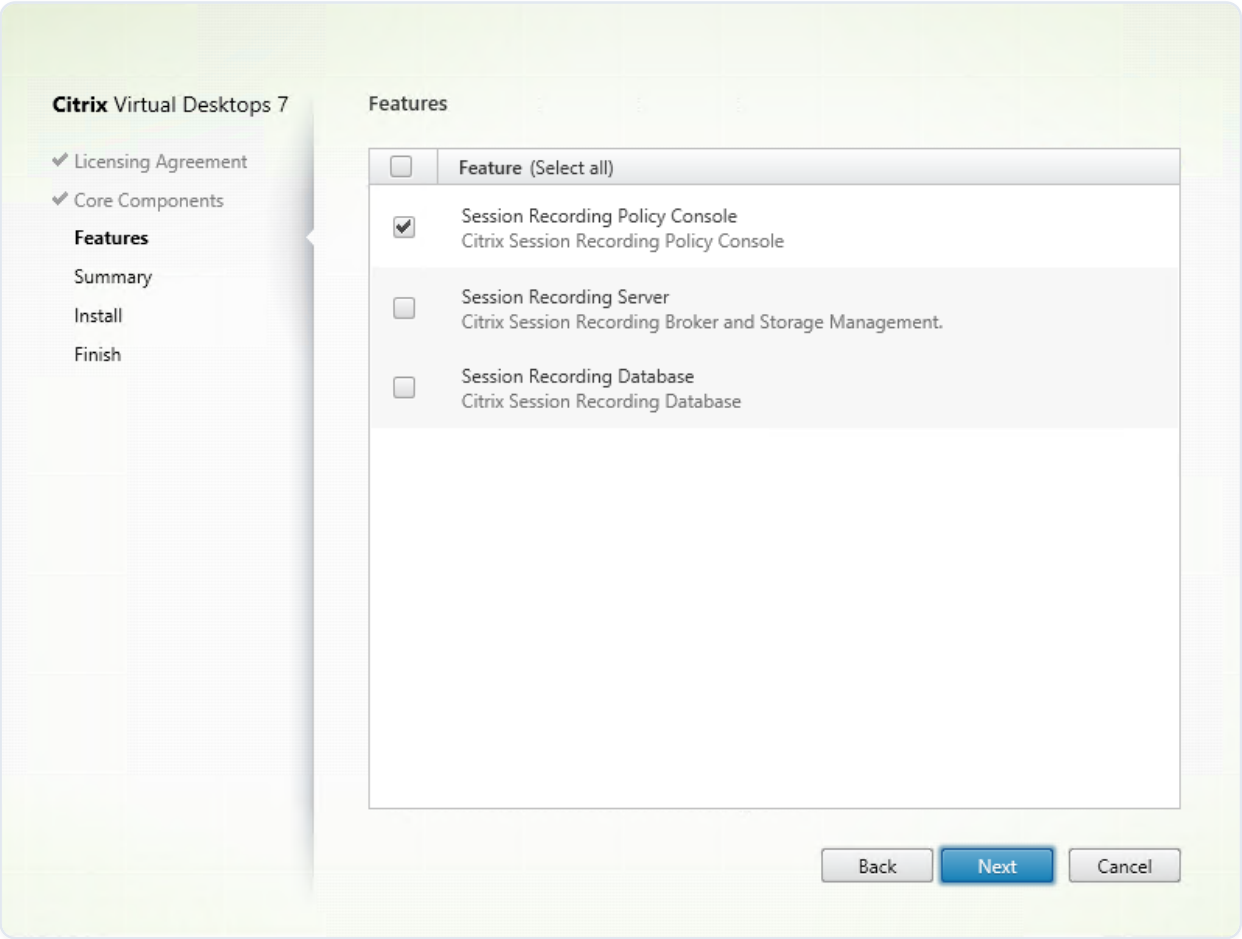
> **Note:**
>
> The Session Recording server default installation uses HTTPS/TLS to secure communications. If TLS is not configured in the default Internet Information Services (IIS) site of the Session Recording server, use HTTP. To do so, cancel the selection of SSL in the IIS Management Console by navigating to the Session Recording Broker site, opening the SSL settings, and clearing the **Require SSL** check box.

Step 6.3: Install the Session Recording policy console

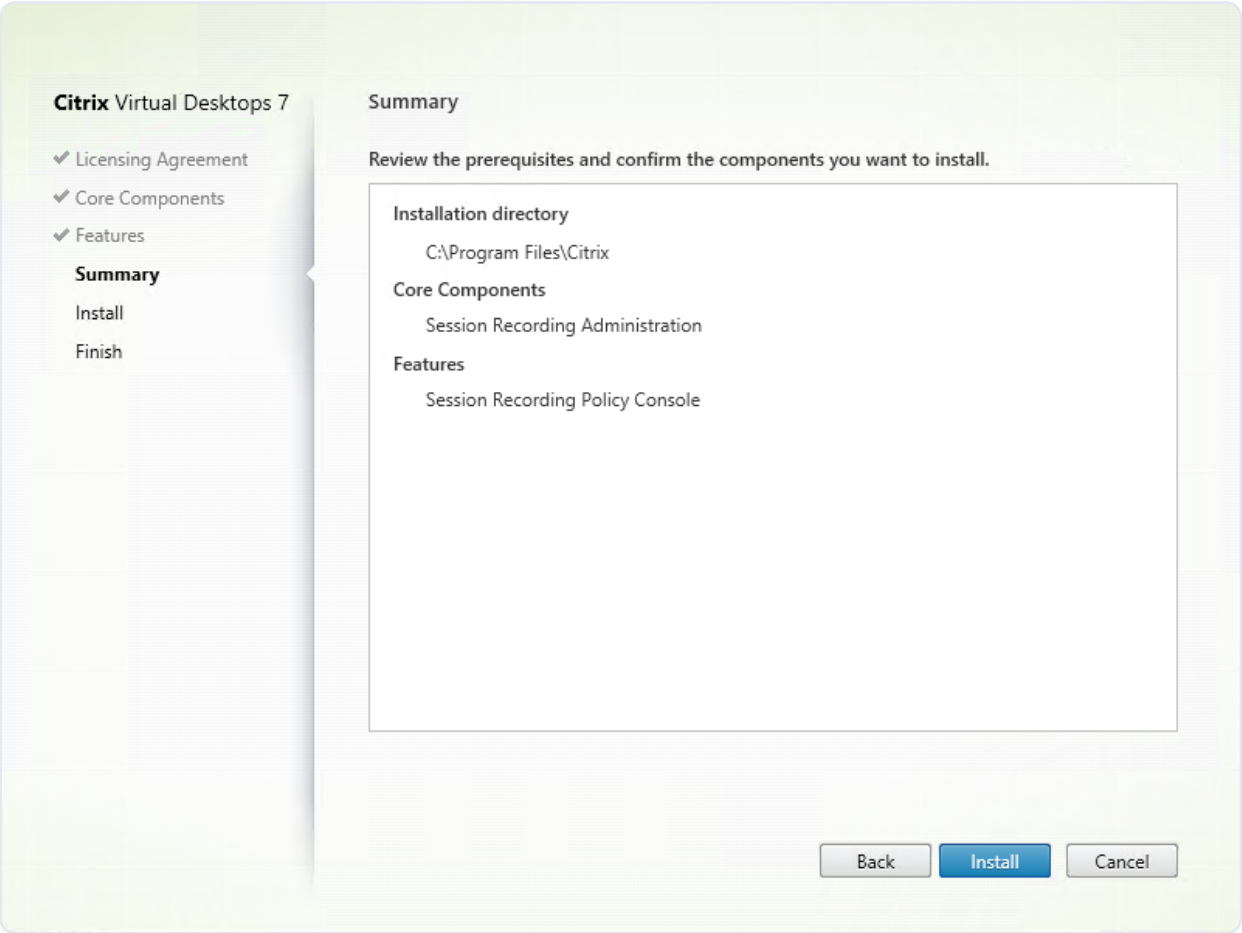
You can use the Session Recording policy console to configure policies.

To install the Session Recording policy console, complete the following steps:

1. On the **Features** page, select **Session Recording Policy Console** and click **Next**.

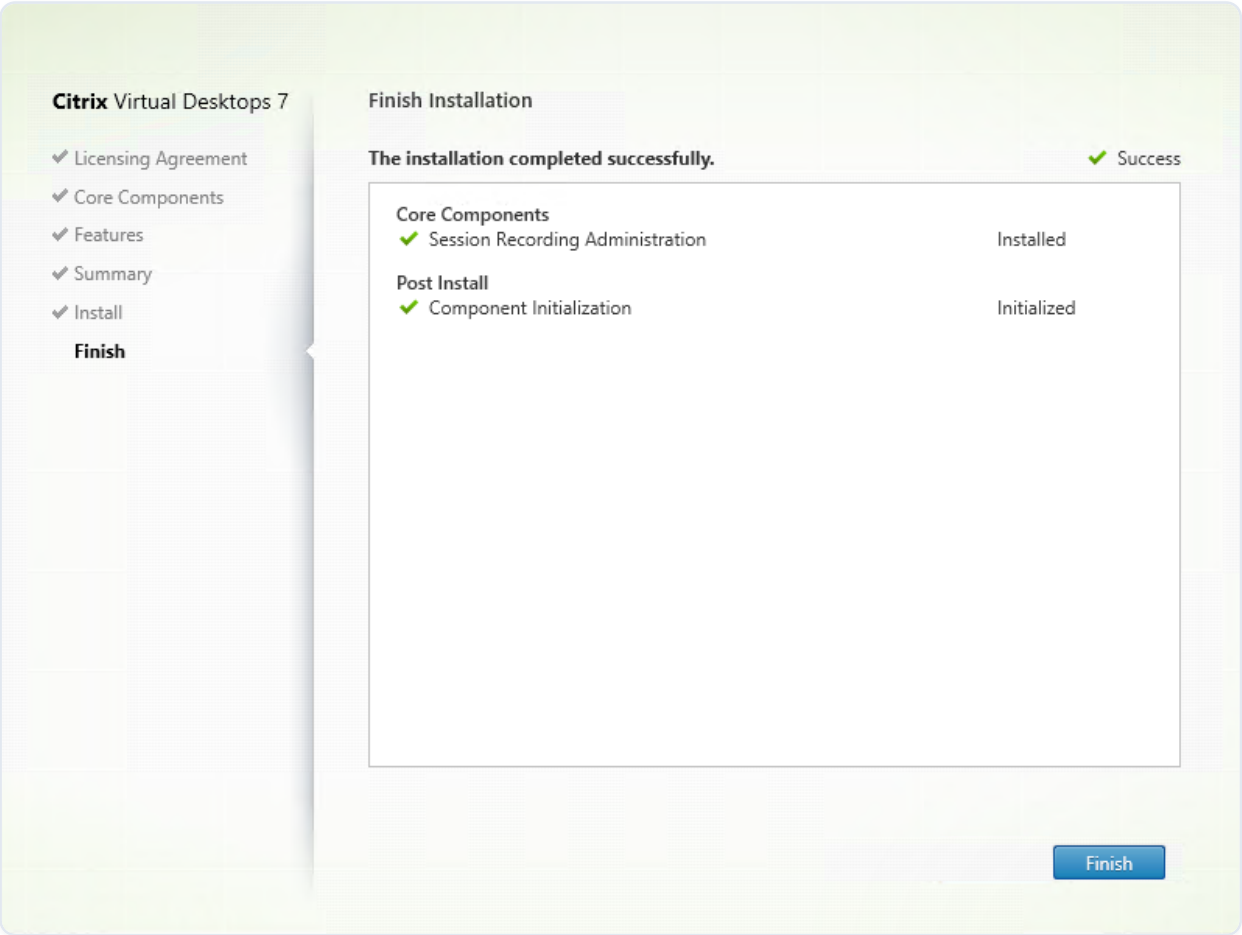


2. Review the prerequisites and confirm the installation.



The **Summary** page shows your installation choices. You can click **Back** to return to the earlier wizard pages and make changes, or click **Install** to start the installation.

3. Complete the installation.



The **Finish Installation** page shows green check marks for all the prerequisites and component that have been installed and initialized successfully.

Click **Finish** to complete your installation of the Session Recording policy console.

Step 7: Install Broker_PowerShellSnapIn_x64.msi

> **Important:**
>
> To use the Session Recording policy console, install the Broker PowerShell Snap-in (`Broker_PowerShellSnapIn_x64.msi`) manually. Locate the snap-in on the Citrix Virtual Apps and Desktops ISO (`\x64\Citrix Desktop Delivery Controller`) and follow the instructions for installing it. Failure to comply can cause an error.

Install the Session Recording agent

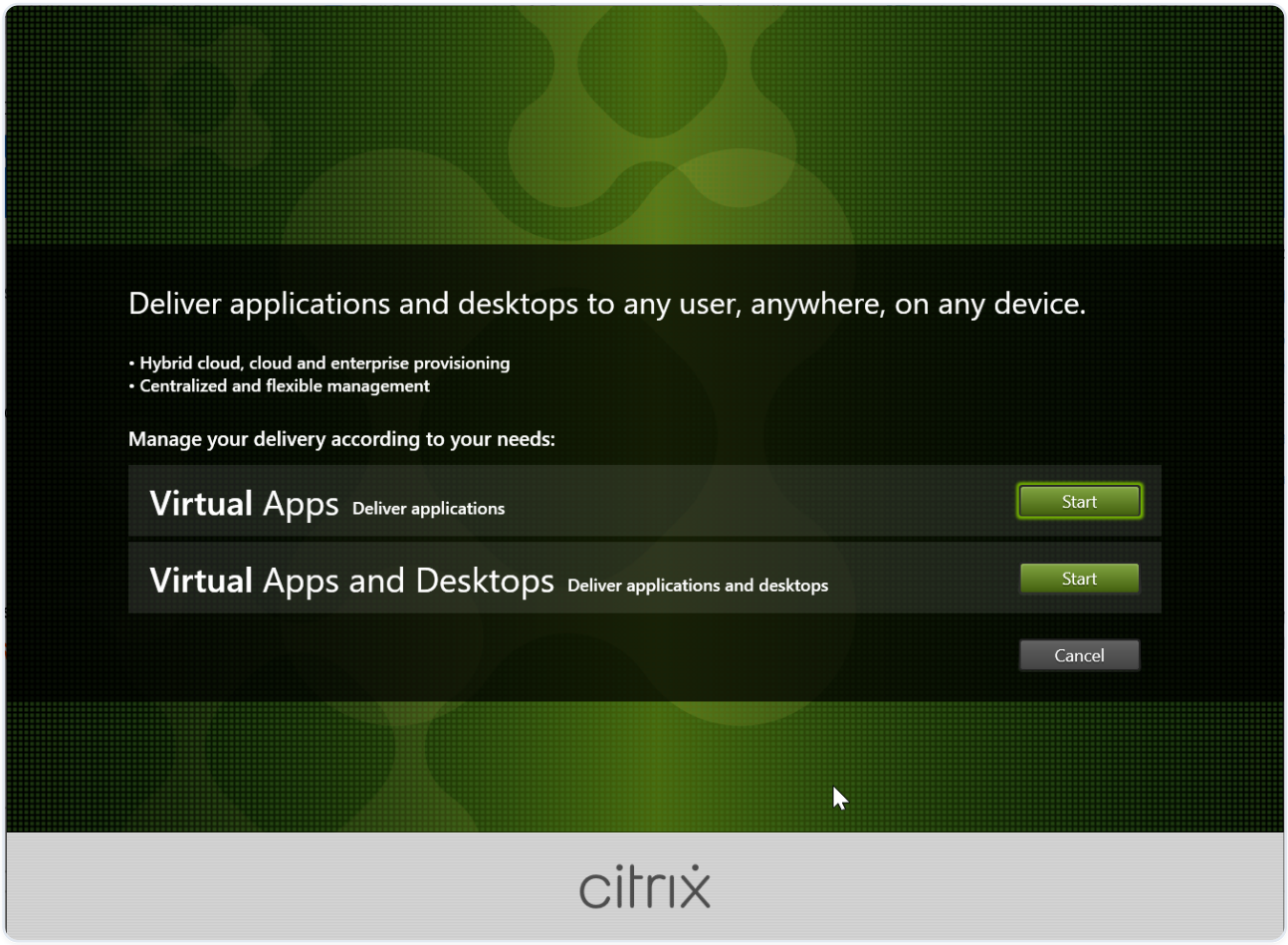
The Session Recording agent is a component installed on each VDA for multi-session OS or single-session OS to enable recording. It is responsible for recording session data.

Step 1: Download the product software and launch the wizard

Use a local administrator account to log on to the machine where you are installing the Session Recording agent. Insert the DVD in the drive or mount the ISO file. If the installer does not launch automatically, double-click the **AutoSelect** application or the mounted drive.

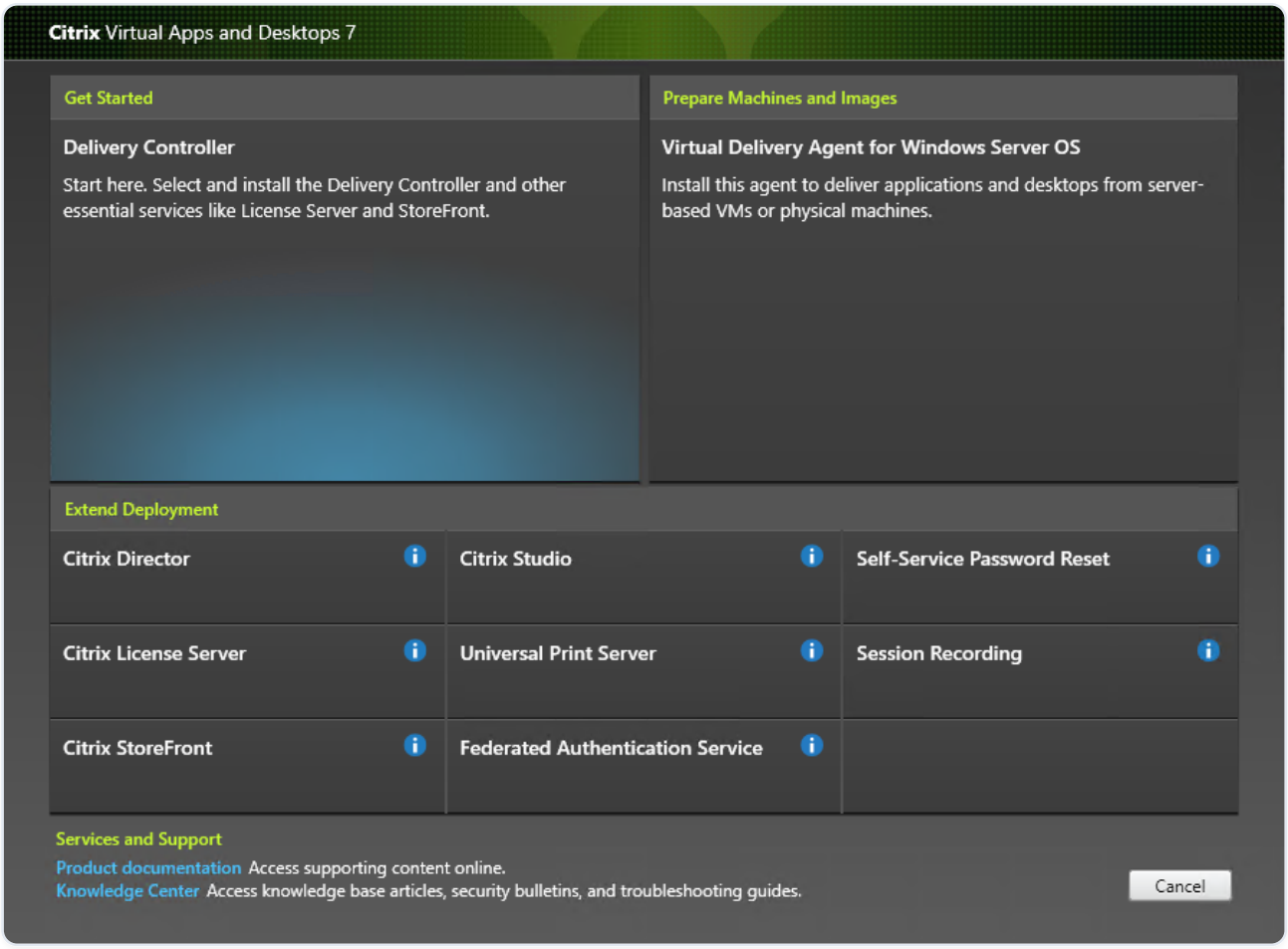
The installation wizard launches.

Step 2: Choose which product to install



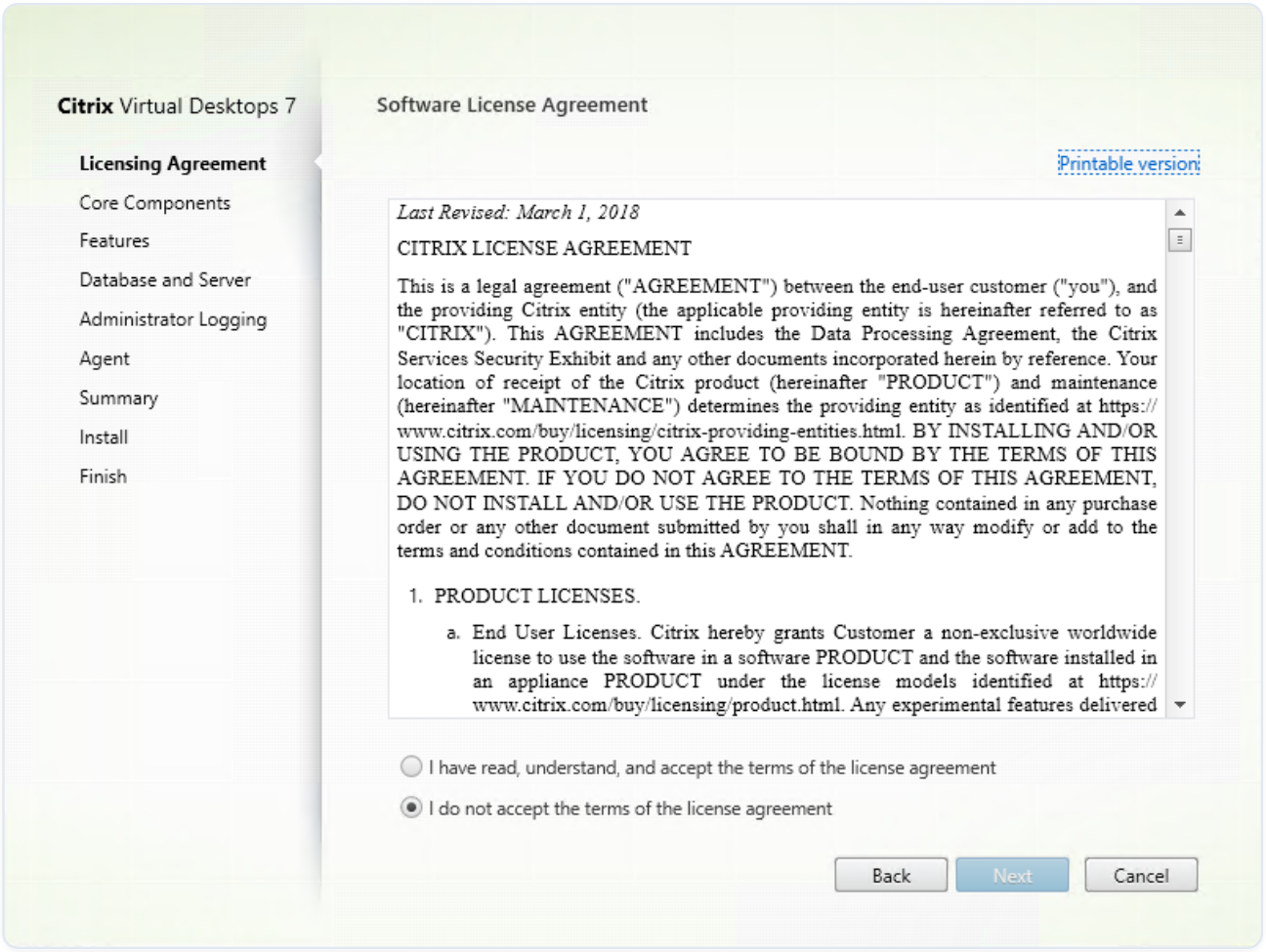
Click **Start** next to the product to install **Citrix Virtual Apps** or **Citrix Virtual Desktops**.

Step 3: Select Session Recording



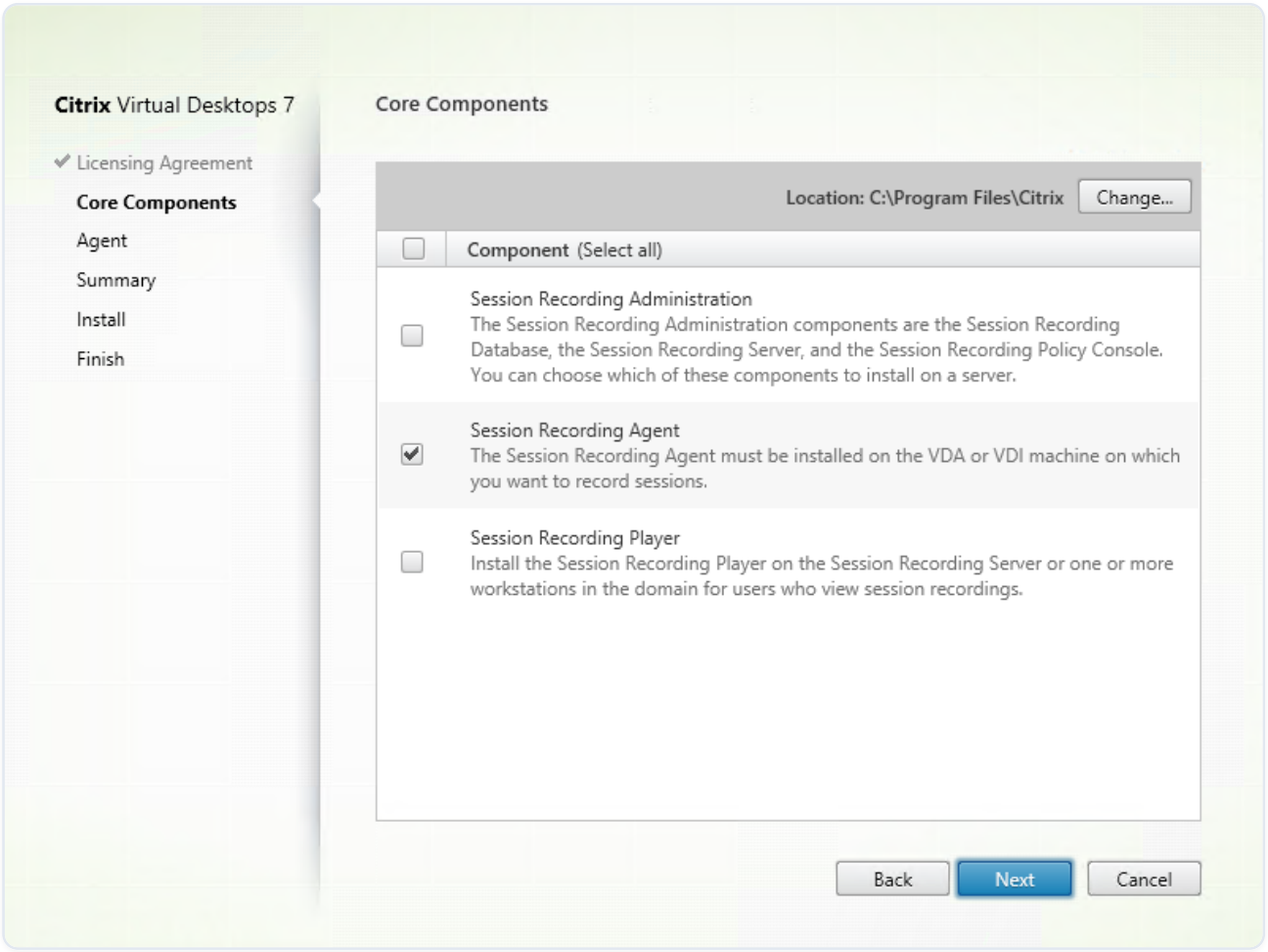
Select the **Session Recording** entry.

Step 4: Read and accept the license agreement



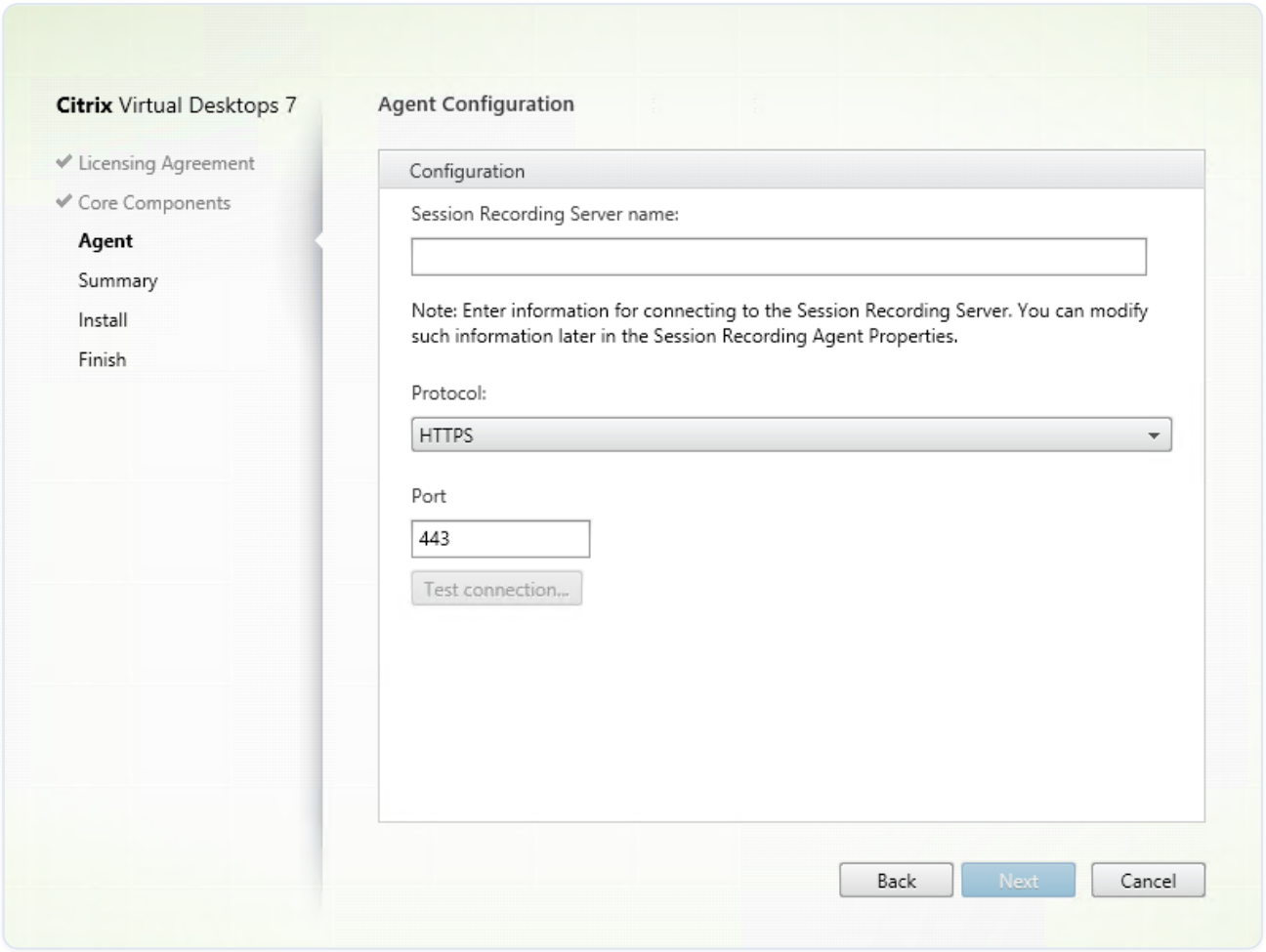
On the **Software License Agreement** page, read the license agreement, accept it, and then click **Next**

Step 5: Select the component to install and the installation location



Select **Session Recording Agent** and click **Next**.

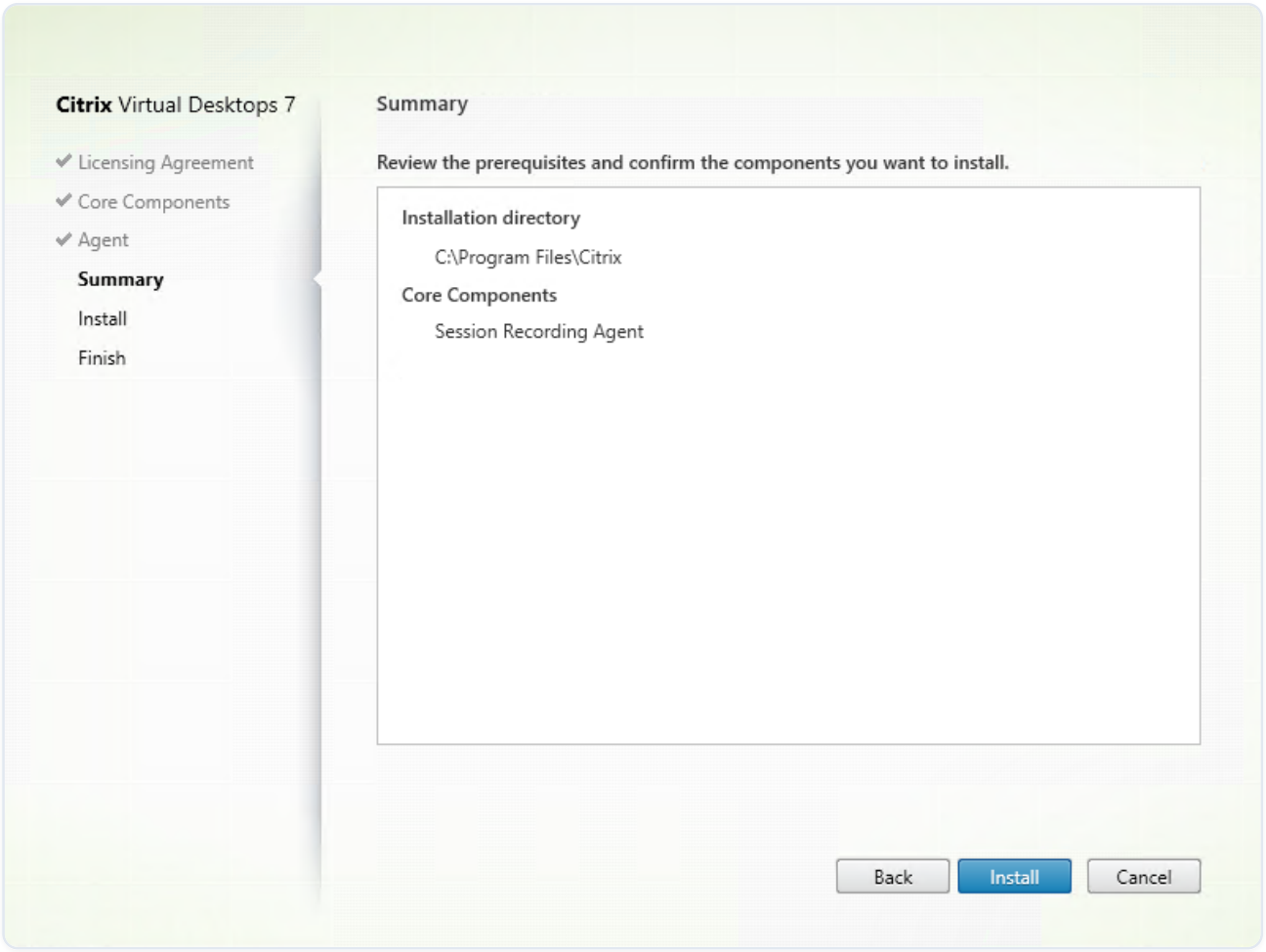
Step 6: Specify the agent configuration



On the **Agent Configuration** page: Type the computer name of the machine where you installed the Session Recording server and the protocol and port information for connecting to the Session Recording server. If you have not installed Session Recording yet, you can change such information later in **Session Recording Agent Properties**.

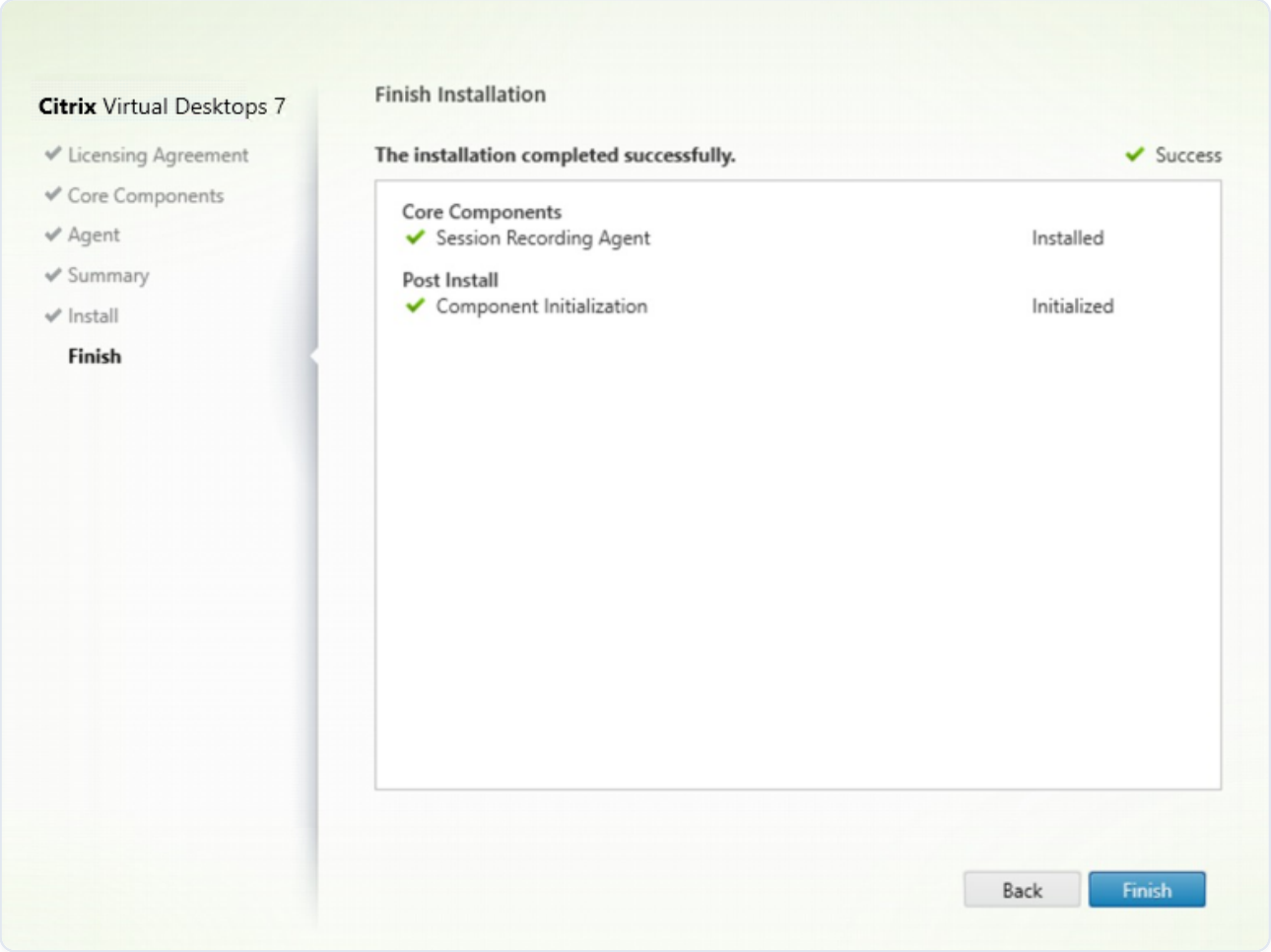
> **Note:**
>
> There is a limitation with the test connection function of the installer. It does not support the "HTTPS requires TLS 1.2" scenario. If you use the installer in this scenario, the test connection fails but you can ignore the failure and click **Next** to continue the installation. It does not affect normal functioning.

Step 7: Review the prerequisites and confirm the installation



The **Summary** page shows your installation choices. You can click **Back** to return to the earlier wizard pages and make changes, or click **Install** to start the installation.

Step 8: Complete the installation



The **Finish Installation** page shows green check marks for all the prerequisites and components that have been installed and initialized successfully.

Click **Finish** to complete the installation of the Session Recording Agent.

> **Note:**
>
> When Machine Creation Services (MCS) or Citrix Provisioning™ creates multiple VDAs with a master image and Microsoft Message Queuing (MSMQ) installed, the VDAs might have the same QMId. The same QMId might cause various issues, for example:
>
> - Sessions might not be recorded even if the recording agreement is accepted.
> - The Session Recording Server might not be able to receive session logoff signals and therefore, sessions might always be in Live status.

As a workaround, create a unique QMId for each VDA and it differs depending on the deployment methods.

No extra actions are required if single-session OS VDAs with the Session Recording agent installed are created with PVS 7.7 or later and MCS 7.9 or later in the static desktop mode that is, for example, configured to make all changes persistent with a separate Personal vDisk or the local disk of your VDA.

For multi-session OS VDAs created with MCS or PVS and single-session OS VDAs that are configured to discard all changes when a user logs off, use the **GenRandomQMID.ps1** script to change the QMId on system startup. Change the power management strategy to ensure that enough VDAs are running before user logon attempts.

To use the **GenRandomQMID.ps1** script, do the following:

1. Ensure that the execution policy is set to **RemoteSigned** or **Unrestricted** in PowerShell.

   Set-ExecutionPolicy RemoteSigned
2. Create a scheduled task, set the trigger as on system startup, and run with the SYSTEM account on the PVS or MCS master image machine.
3. Add the command as a startup task.

   `powershell .exe -file C:\\GenRandomQMID.ps1`

Summary of the GenRandomQMID.ps1 script:

1. Remove the current QMId from the registry.
2. Add `SysPrep = 1` to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters`.
3. Stop related services, including CitrixSmAudAgent and MSMQ.
4. To generate a random **QMId**, start the services that stopped previously.

Example GENRANDOMQMID.PS1:

```
# Remove old QMId from registry and set SysPrep flag for MSMQ



Remove-Itemproperty -Path
HKLM:Software\Microsoft\MSMQ\Parameters\MachineCache -Name QMId -Force



Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -Name
"SysPrep" -Type DWord -Value 1



# Get dependent services



$depServices = Get-Service -name MSMQ -dependentservices | Select
-Property Name



# Restart MSMQ to get a new QMId



Restart-Service -force MSMQ



# Start dependent services



if ($depServices -ne $null) {



    foreach ($depService in $depServices) {
```

```
        $startMode = Get-WmiObject win32_service -filter "NAME = '$
($depService.Name)'" | Select -Property StartMode



         if ($startMode.StartMode -eq "Auto") {



             Start-Service $depService.Name

         }

}



}
```

Install the Session Recording player

> **Tip:**

> Installing the Session Recording server lets you install the Session Recording web player automatically. This section describes how to install the Session Recording player.

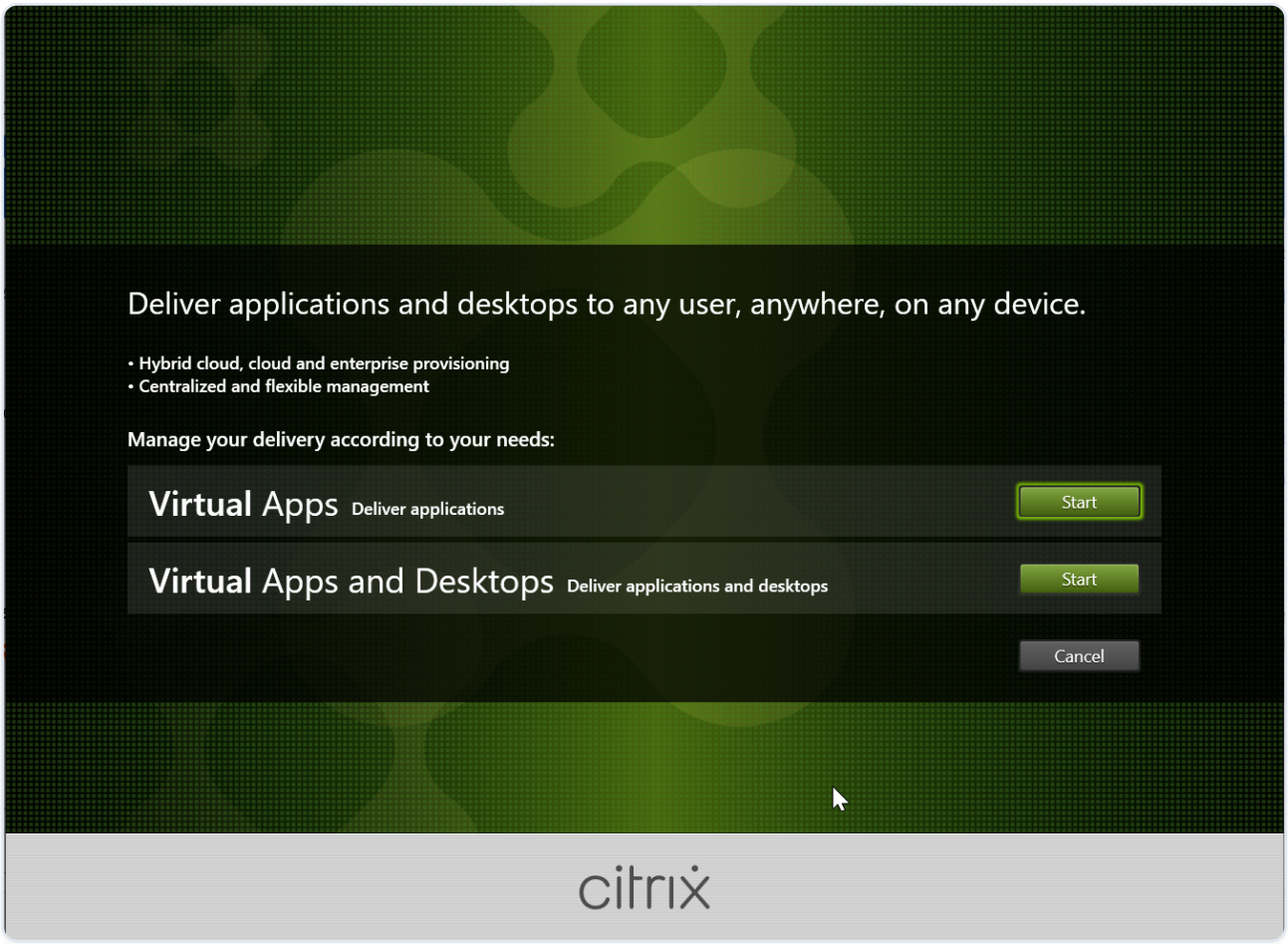
> The Session Recording player is a user interface that you access from a workstation to play recorded session files. Install the Session Recording player on the Session Recording server or on workstations in the domain.

Step 1: Download the product software and launch the wizard

Use a local administrator account to log on to the machine where you are installing the Session Recording player component. Insert the DVD in the drive or mount the ISO file. If the installer does not launch automatically, double-click the **AutoSelect** application or the mounted drive.

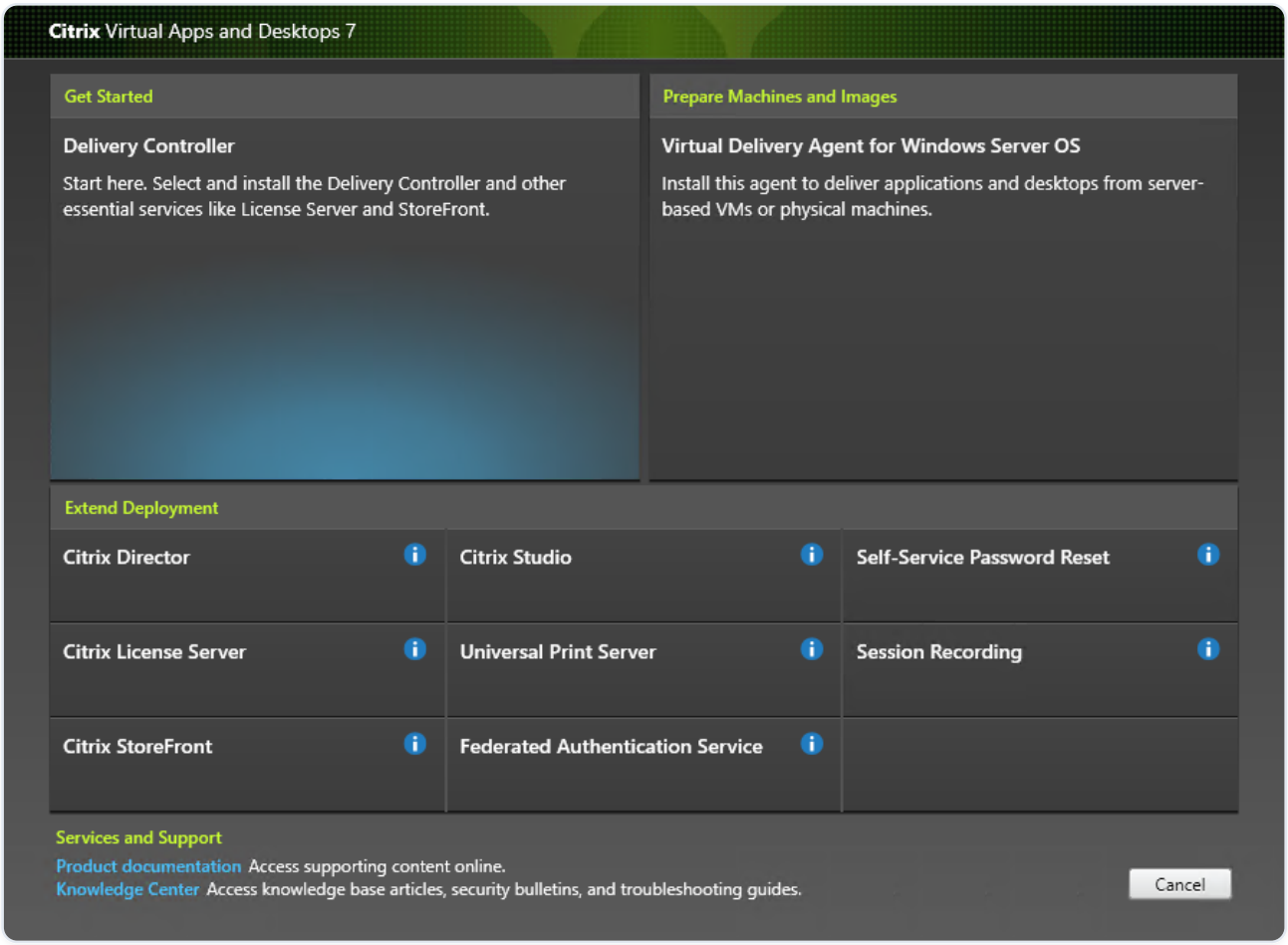
The installation wizard launches.

Step 2: Choose which product to install



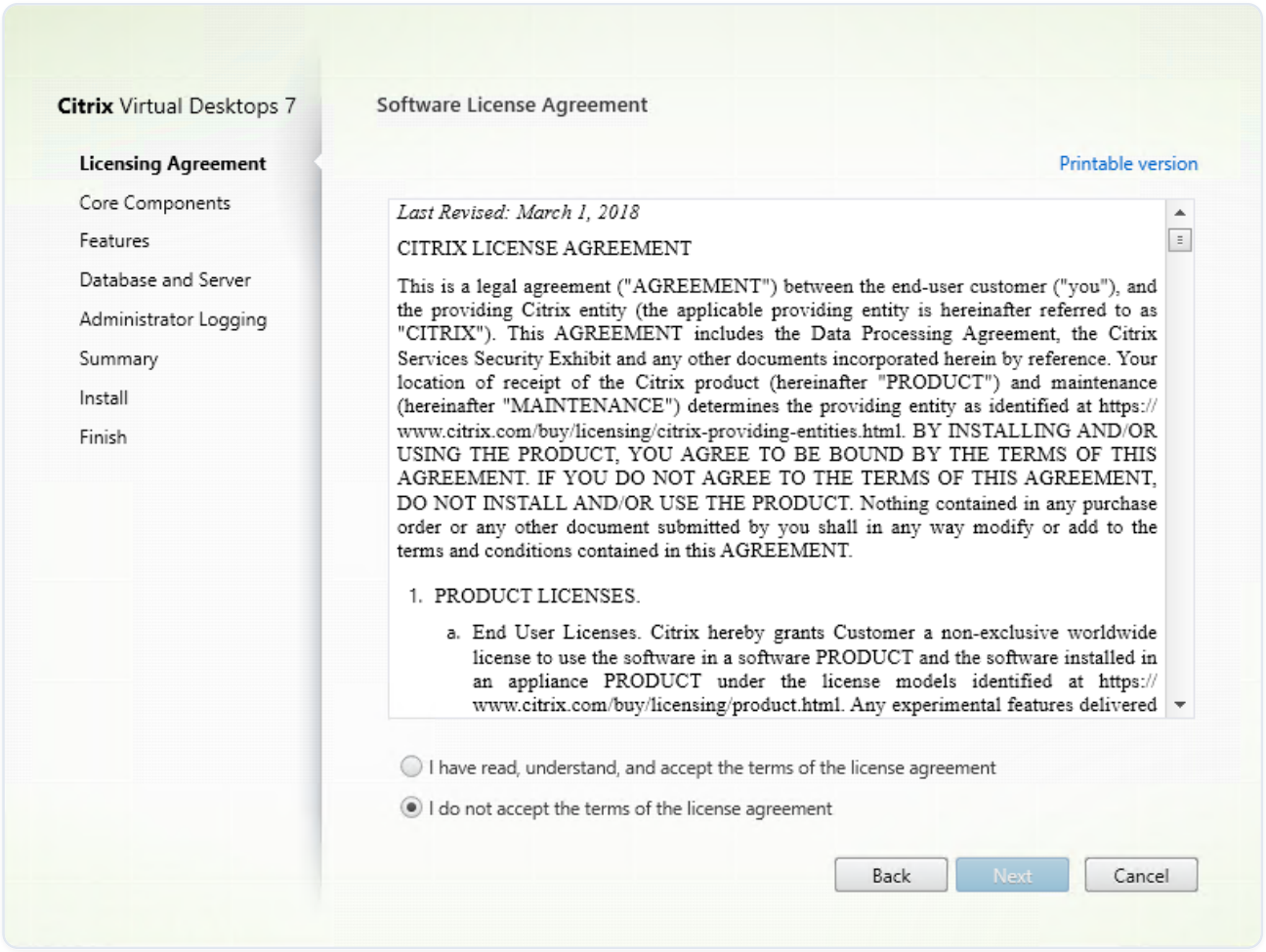
Click **Start** next to the product to install **Citrix Virtual Apps** or **Citrix Virtual Desktops**.

Step 3: Select Session Recording



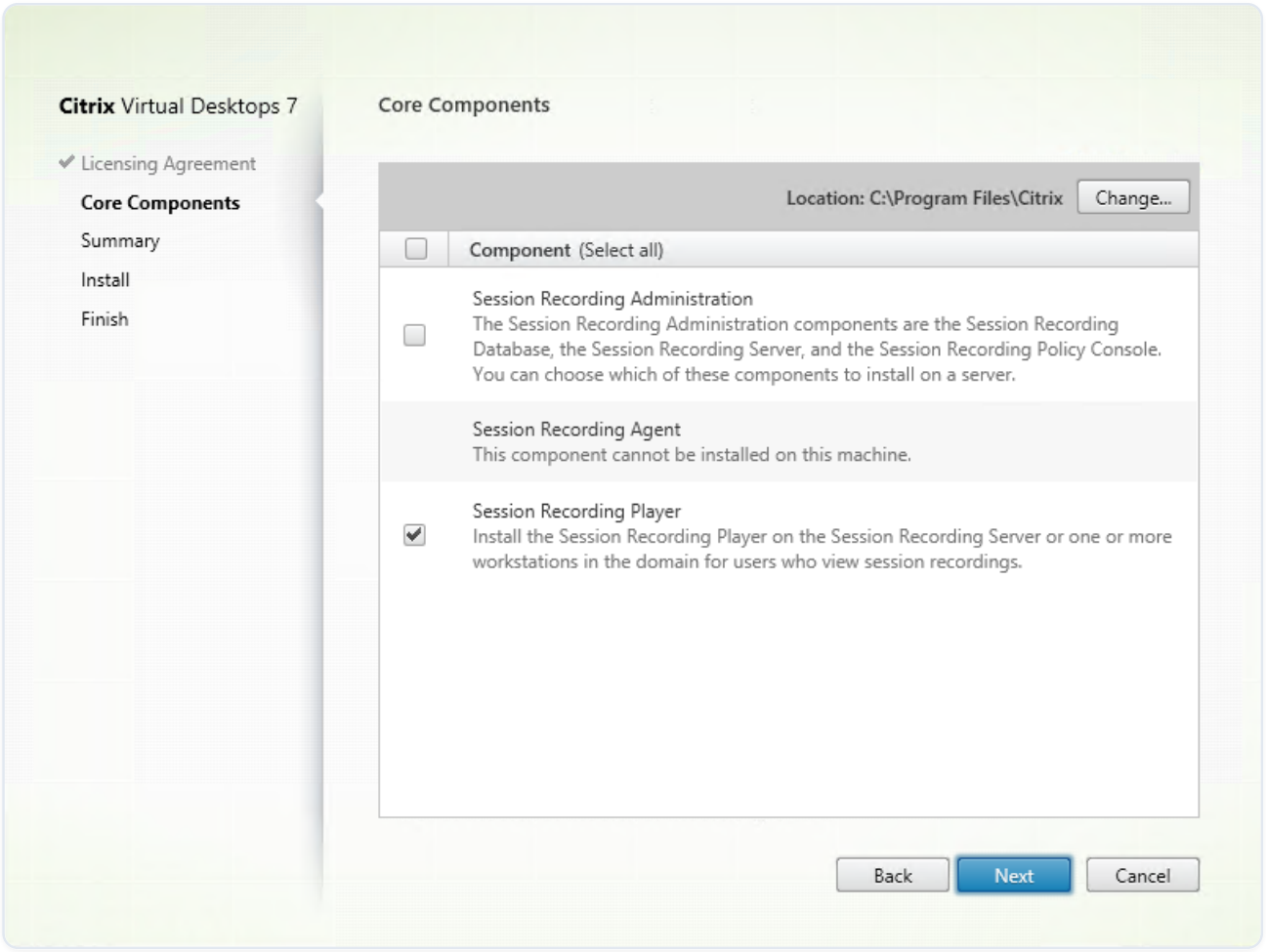
Select the **Session Recording** entry.

Step 4: Read and accept the license agreement



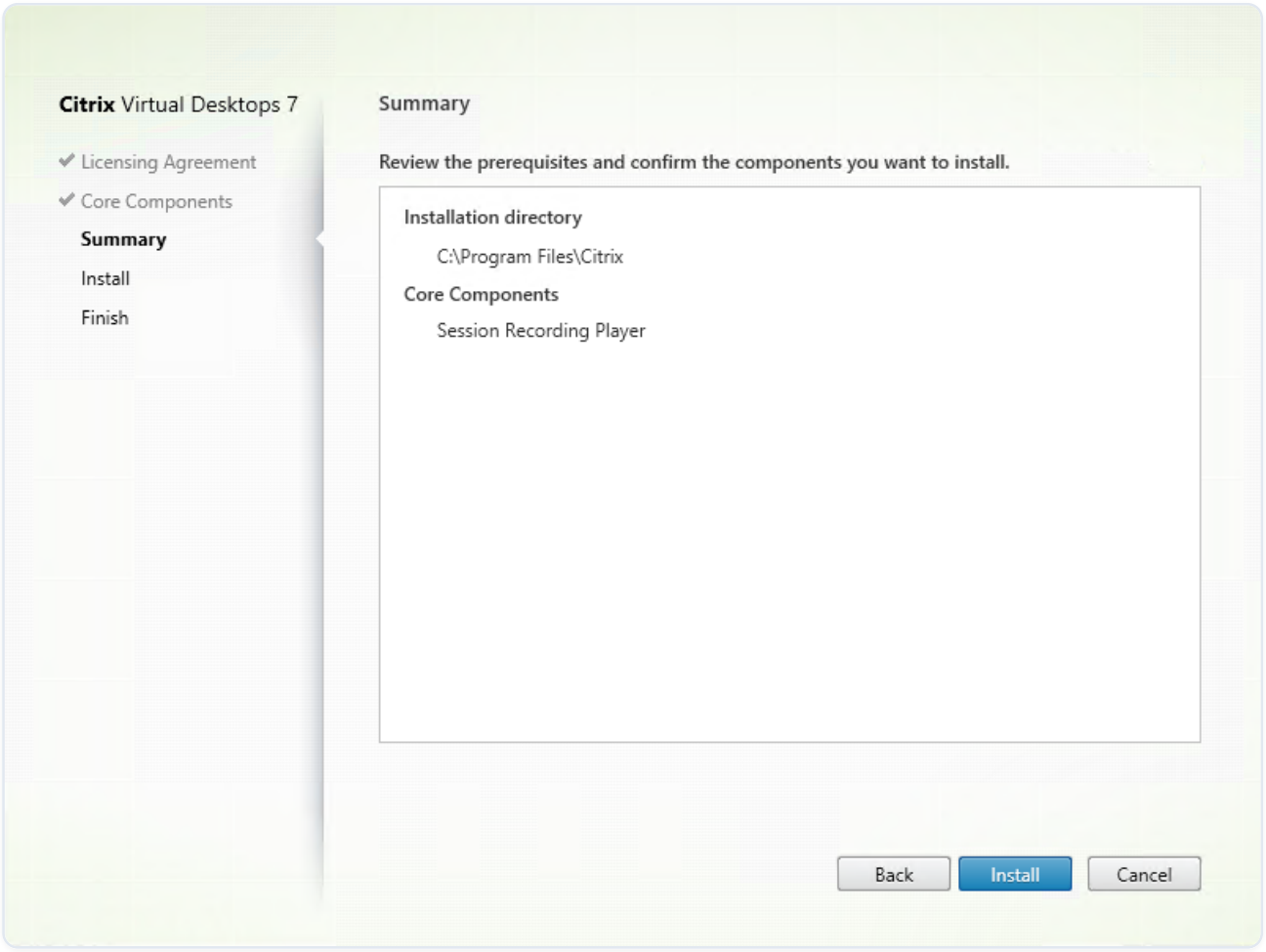
On the **Software License Agreement** page, read the license agreement, accept it, and then click **Next**.

Step 5: Select the component to install and the installation location



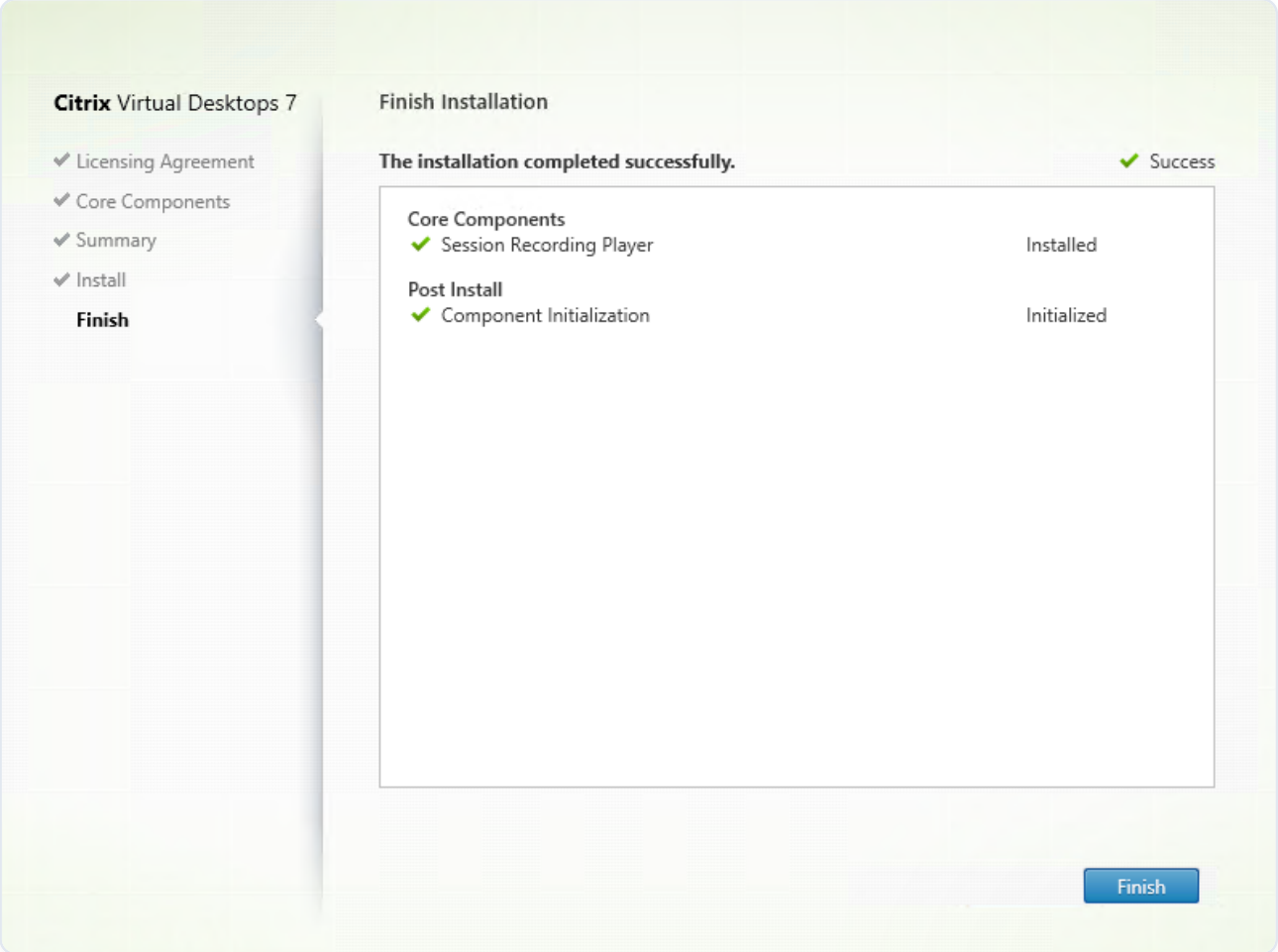
Select **Session Recording Player** and click **Next**.

Step 6: Review the prerequisites and confirm the installation



The **Summary** page shows your installation choices. You can click **Back** to return to the earlier wizard pages and make changes, or click **Install** to start the installation.

Step 7: Complete the installation



The **Finish Installation** page shows green check marks for all the prerequisites and components that have been installed and initialized successfully.

Click **Finish** to complete the installation of the Session Recording player.

Automate installation

Session Recording supports silent installation with options. Write a script that uses silent installation and run the relevant commands.

Automate installation of the Session Recording Administration components

Install the complete set of the Session Recording Administration components by using a single command

For example, either of the following commands installs the complete set of the Session Recording Administration components and creates a log file to capture the installation information.

```
msiexec /i "c:\SessionRecordingAdministrationx64.msi"
ADDLOCAL="SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
DATABASEINSTANCE="WNBIO-SRD-1" DATABASENAME="CitrixSessionRecording"
LOGGINGDATABASENAME="CitrixSessionRecordingLogging"
DATABASEUSER="localhost" /q /l*vx "yourinstallationlog"
```

```
msiexec /i "SessionRecordingAdministrationx64.msi"
ADDLOCAL="SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
DATABASEINSTANCE="CloudSQL" DATABASENAME="CitrixSessionRecording"
LOGGINGDATABASENAME="CitrixSessionRecordingLogging"
AZURESQLSERVICESUPPORT="1" AZUREUSERNAME="CloudSQLAdminName"
AZUREPASSWORD="CloudSQLAdminPassword" /q /l*vx "c:\WithLogging.log"
```

Note:

You can find the `SessionRecordingAdministrationx64.msi` file on the Citrix Virtual Apps and Desktops ISO under `\x64\Session Recording`.

Where:

- **ADDLOCAL** provides the features for you to select. You can select more than one option. SsRecServer is the Session Recording server. PolicyConsole is the Session Recording policy console. SsRecLogging is the Administrator Logging feature. StorageDatabase is the Session Recording database. Session Recording Administrator Logging is an optional subfeature of the Session Recording server. Select the Session Recording server before you can select Session Recording administrator logging.
- **DATABASEINSTANCE** is the instance name of the Session Recording database. For example, `.\SQLEXPRESS,computer-name\SQLEXPRESS,computer-name` or `tcp:srt-sql-support.public.ca7b16b60789.database.windows.net,3342` if you are using Azure SQL Managed Instance.
- **DATABASENAME** is the database name of the Session Recording database.
- **LOGGINGDATABASENAME** is the name of the administrator logging database.
- **AZURESQLSERVICESUPPORT** determines whether cloud SQL is supported. To use cloud SQL, set it to `1`.
- **DATABASEUSER** is the computer account of the Session Recording server.

- **AZUREUSERNAME** is the cloud SQL admin name.
- **AZUREPASSWORD** is the cloud SQL admin password.
- **/q** specifies quiet mode.
- **/l*v** specifies verbose logging.
- **yourinstallationlog** is the location of your installation log file.

Create a master image for deploying the Session Recording server

You might already have the Session Recording database and the administration logging database in place from an existing deployment. For such scenarios, you can now forego database checks when you are installing the Session Recording Administration components using SessionRecordingAdministrationx64.msi. You can create a master image for deploying the Session Recording server easily on many other machines. After deploying the Session Recording server on target machines using the master image, run a command on each machine to connect to the existing Session Recording database and administration logging database. This master image support facilitates deployment and minimizes the potential impact of human error. It applies only to fresh installations and consists of the following steps:

1. Start a command prompt and run a command similar to the following:

   ```
   msiexec /i "SessionRecordingAdministrationx64.msi"
   ADDLOCAL="SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
   DATABASEINSTANCE="sqlnotexists" DATABASENAME="CitrixSessionRecording2"
   LOGGINGDATABASENAME="CitrixSessionRecordingLogging2"
   DATABASEUSER="localhost" /q /l*vx "c:\WithLogging.log"
   IGNOREDBCHECK="True"
   ```

   This command installs the Session Recording Administration components without configuring and testing connectivity to the Session Recording database and the administration logging database.

   Set the **IGNOREDBCHECK** parameter to **True** and use random values for **DATABASEINSTANCE**, **DATABASENAME**, and **LOGGINGDATABASENAME**.
2. Create a master image on the machine that you are operating.
3. Deploy the master image to other machines for deploying the Session Recording server.
4. On each of the machines, run commands similar to the following:

```
.\SsRecUtils.exe -modifydbconnectionpara DATABASEINSTANCE DATABASENAME
LOGGINGDATABASENAME



iisreset /noforce
```

The commands connect the Session Recording server installed earlier to an existing Session Recording database and administration logging database.

You can find the `SsRecUtils.exe` file at `\Citrix\SessionRecording\Server\bin\`. Set the **DATABASEINSTANCE**, **DATABASENAME**, and **LOGGINGDATABASENAME** parameters as needed.

Retain databases when uninstalling the Session Recording Administration components

With **KEEPDB** set to **True**, the following command retains the Session Recording database and the administration logging database when uninstalling the Session Recording Administration components:

```
msiexec /x "SessionRecordingAdministrationx64.msi" KEEPDB="True"
```

Automate installation of the Session Recording player and web player

For example, the following commands install the Session Recording player and web player, respectively.

```
msiexec /i "c:\SessionRecordingPlayer.msi" /q /l*\vx "yourinstallationlog"
```

```
msiexec /i "c:\SessionRecordingWebPlayer.msi" /q /l*vx
"yourinstallationlog"
```

Note:

You can find `SessionRecordingPlayer.msi` on the Citrix Virtual Apps and Desktops ISO under `\x86\Session Recording`.

> You can find `SessionRecordingWebPlayer.msi` on the Citrix Virtual Apps and Desktops ISO under `\x64\Session Recording`.

> Where:

- **/q** specifies quiet mode.
- **/l*v** specifies verbose logging.
- **yourinstallationlog** is the location of your installation log file.

Automate installation of the Session Recording agent

For example, the following command installs the Session Recording Agent and creates a log file to capture the installation information.

For 64-bit systems:

```
msiexec /i SessionRecordingAgentx64.msi /q /l*vx yourinstallationlog
SESSIONRECORDINGSERVERNAME=yourservername

SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol
SESSIONRECORDINGBROKERPORT=yourbrokerport
```

> **Note:**

> You can find `SessionRecordingAgentx64.msi` on the Citrix Virtual Apps and Desktops ISO under `\x64\Session Recording`.

> **For 32-bit systems:**

```
msiexec /i SessionRecordingAgent.msi /q /l*vx yourinstallationlog
SESSIONRECORDINGSERVERNAME=yourservername

SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol
SESSIONRECORDINGBROKERPORT=yourbrokerport
```

> **Note:**

> You can find `SessionRecordingAgent.msi` on the Citrix Virtual Apps and Desktops ISO under `\x86\Session Recording`.

> Where:

- **yourservername** is the NetBIOS name or FQDN of the machine hosting the Session Recording server. If not specified, this value defaults to **localhost**.
- **yourbrokerprotocol** is the HTTP or HTTPS that the Session Recording agent uses to communicate with the Session Recording Broker. If not specified, this value defaults to HTTPS.
- **yourbrokerport** is the port number that the Session Recording agent uses to communicate with the Session Recording Broker. If not specified, this value defaults to zero, which directs the Session Recording Agent to use the default port number for your selected protocol: 80 for HTTP or 443 for HTTPS.
- **/q** specifies quiet mode.
- **/l*v** specifies verbose logging.
- **yourinstallationlog** is the location of your installation log file.

Upgrade Session Recording

You can upgrade certain deployments to later versions without having to first set up new machines or sites. You can upgrade from the version of Session Recording included in the latest CU of XenApp and XenDesktop 7.6 LTSR, and from any later version, to the latest release of Session Recording.

> **Note:**

> When you upgrade Session Recording Administration from 7.6 to 7.13 or later and choose **Modify** in Session Recording Administration to add the administrator logging service, the SQL Server instance name does not appear on the **Administrator Logging Configuration** page. The following error message appears when you click **Next**: **Database connection test failed. Please enter correct Database instance name.** As a workaround, add the read permission for localhost users to the following SmartAuditor Server registry folder: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`.

> You cannot upgrade from a Technical Preview version.

Requirements, preparation, and limitations

- Use the Session Recording installer's graphical or command line interface to upgrade the Session Recording components on the machine where you installed the components.
- Before any upgrade activity, back up the database named CitrixSessionRecording in the SQL Server instance. In this way, you can restore it if any issues are discovered after the database upgrade.
- In addition to being a domain user, you must be a local administrator on the machines where you are upgrading the Session Recording components.
- If the Session Recording server and Session Recording database aren't installed on the same server, you must have the database role permission to upgrade the Session Recording database. Otherwise, you can:
  - Ask the database administrator to assign the **securityadmin** and **dbcreator** server role permissions for the upgrade. After the upgrade completes, the **securityadmin** and **dbcreator** server role permissions are no longer necessary and can be safely removed.
  - Or, use the SessionRecordingAdministrationx64.msi package to upgrade. During the msi upgrade, a dialog box prompts for the credentials of a database administrator who has the **securityadmin** and **dbcreator** server role permissions. Type the correct credentials and then click **OK** to continue the upgrade.
- You can choose not to upgrade all Session Recording agents at the same time. Session Recording agent 7.6.0 (and later) is compatible with the latest (current) release of the Session Recording server. However, some new features and bug fixes might not take effect.
- Any sessions started during the upgrade of the Session Recording server are not recorded.
- The **Graphics Adjustment** option in Session Recording agent Properties is enabled by default after a fresh installation or upgrade to keep compatible with the Desktop Composition Redirection mode. You can disable this option manually after a fresh installation or upgrade.
- The administrator logging feature is not installed after you upgrade Session Recording from a previous release where the feature is unavailable. To add the feature, modify the installation after the upgrade.
- If there are live recording sessions when the upgrade process starts, there is little chance that the recording can be complete.
- Review the following upgrade sequence, so that you can plan and mitigate potential outages.

Upgrade sequence

To upgrade an existing installation, go to each machine where a Session Recording component is installed and then run the Citrix Virtual Apps and Desktops ISO.

> **Tip:**
>
> Go to the Citrix Virtual Apps and Desktops download page to download the appropriate version of Citrix Virtual Apps and Desktops.

> Upgrading an existing installation generally follows the following sequence:

1. Upgrade the Session Recording server component.

   If there are more than one Session Recording server, first upgrade the one where the Session Recording database component is installed. After that, upgrade the rest Session Recording servers.

   To do so, complete the following steps:

   a. Stop the Session Recording Storage Manager service manually on the Session Recording server.
   b. Through the Internet Information Services (IIS) Manager, ensure that the Session Recording Broker is running.
   c. Run the Citrix Virtual Apps and Desktops ISO and select the Session Recording entry to upgrade.

2. The Session Recording service is back online automatically when the upgrade of the Session Recording server is completed.
3. Upgrade the Session Recording agent (on the master image).
4. Upgrade the Session Recording policy console with or after the Session Recording server.
5. Upgrade the Session Recording player.

Install the Session Recording database on cloud SQL database services

This section describes how to install the Session Recording database on the following cloud SQL database services:

- Azure SQL Database
- Azure SQL Managed Instance
- AWS RDS
- SQL Server on Azure VMs

Install the Session Recording database on Azure SQL Database

1. Create an Azure SQL Database.
    a. Sign in to the Azure portal using your Azure account.
    b. From the portal menu, select **Create a resource**.
    c. In the portal search box, enter **SQL database**.
    d. From the list of search results, select **SQL databases**.
    e. Click **Create** to create an Azure SQL Database.
    f. In the **Create SQL Database** section, provide the following information:
        - **Subscription**: Select the Azure subscription that you want.
        - **Resource Group**: Select **Create new** or choose an existing resource group.
        - **Database Name**: A unique name is required.
        - **Server**: Select Create new, and fill out the **New Server** form with the following values:
            - **Server name**: Enter a unique name. Server names must be globally unique for all servers in Azure.
            - **Location**: Select a location from the drop-down list.
            - **Authentication method**: Select Use SQL authentication.
            - **Server admin login**: Enter a cloud SQL administrator name.
            - **Password**: Enter a cloud SQL administrator password that meets requirements and enter it again in the Confirm password field.
            - Select **OK**.

    After providing the preceding information, click **Review + Create**. Click the **Create** button to complete the Azure SQL Database.
2. Repeat Step 1 to create a different Azure SQL Database on the same **Server**.
3. Get the server connection string for the created Azure SQL Databases.

a. In the Azure portal, search for and click either of the Azure SQL Databases that you have created.

b. Click **Connection strings** from the left navigation.

c. Keep a record of the **Server** string that is to be used as the instance name of the Session Recording database and the Session Recording logging database later.

4. Run a command similar to the following to install the Session Recording database on the Azure SQL Database that you have created earlier.

> **Note:**
>
> On Azure SQL Database, installation of the Session Recording database can be done **only by** running a command similar to the following:

```
msiexec /i "SessionRecordingAdministrationx64.msi"
ADDLOCAL="SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
DATABASEINSTANCE="DatabaseConnectionString "
DATABASENAME="CitrixSessionRecording"
LOGGINGDATABASENAME="CitrixSessionRecordingLogging"
AZURESQLSERVICESUPPORT="1" CLOUDDBSUPPORT="1"
AZUREUSERNAME="CloudSQLAdminName" AZUREPASSWORD="CloudSQLAdminPassword" /
q /l*vx "c:\WithLogging.log"
```

Where:

- **ADDLOCAL** provides the features for you to select. You can select more than one option. SsRecServer is the Session Recording server. PolicyConsole is the Session Recording policy console. SsRecLogging is the Administrator Logging feature. StorageDatabase is the Session Recording database. Session Recording Administrator Logging is an optional subfeature of the Session Recording server. Select the Session Recording server before you can select Session Recording administrator logging.
- **DATABASEINSTANCE** is the instance name of the Session Recording database, which is specified by the Azure SQL Database connection string.
- **DATABASENAME** is the database name of the Session Recording database.
- **LOGGINGDATABASENAME** is the name of the administrator logging database.

- **AZURESQLSERVICESUPPORT** determines whether cloud SQL is supported. To use cloud SQL, set it to 1.
- **DATABASEUSER** is the computer account of the Session Recording server.
- **AZUREUSERNAME** is the cloud SQL admin name.
- **AZUREPASSWORD** is the cloud SQL admin password.
- **/q** specifies quiet mode.
- **/l*v** specifies verbose logging.
- **yourinstallationlog** is the location of your installation log file.

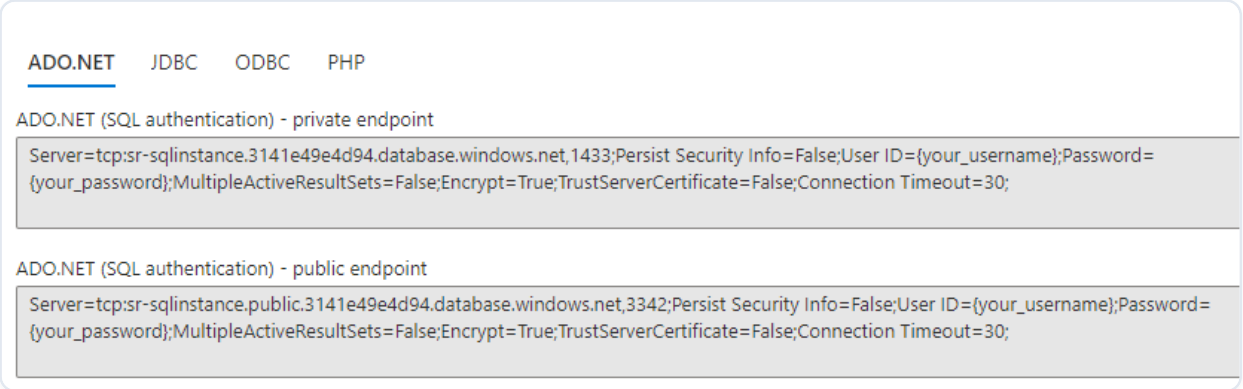
Install the Session Recording database on Azure SQL Managed Instance or on AWS RDS

Tip:

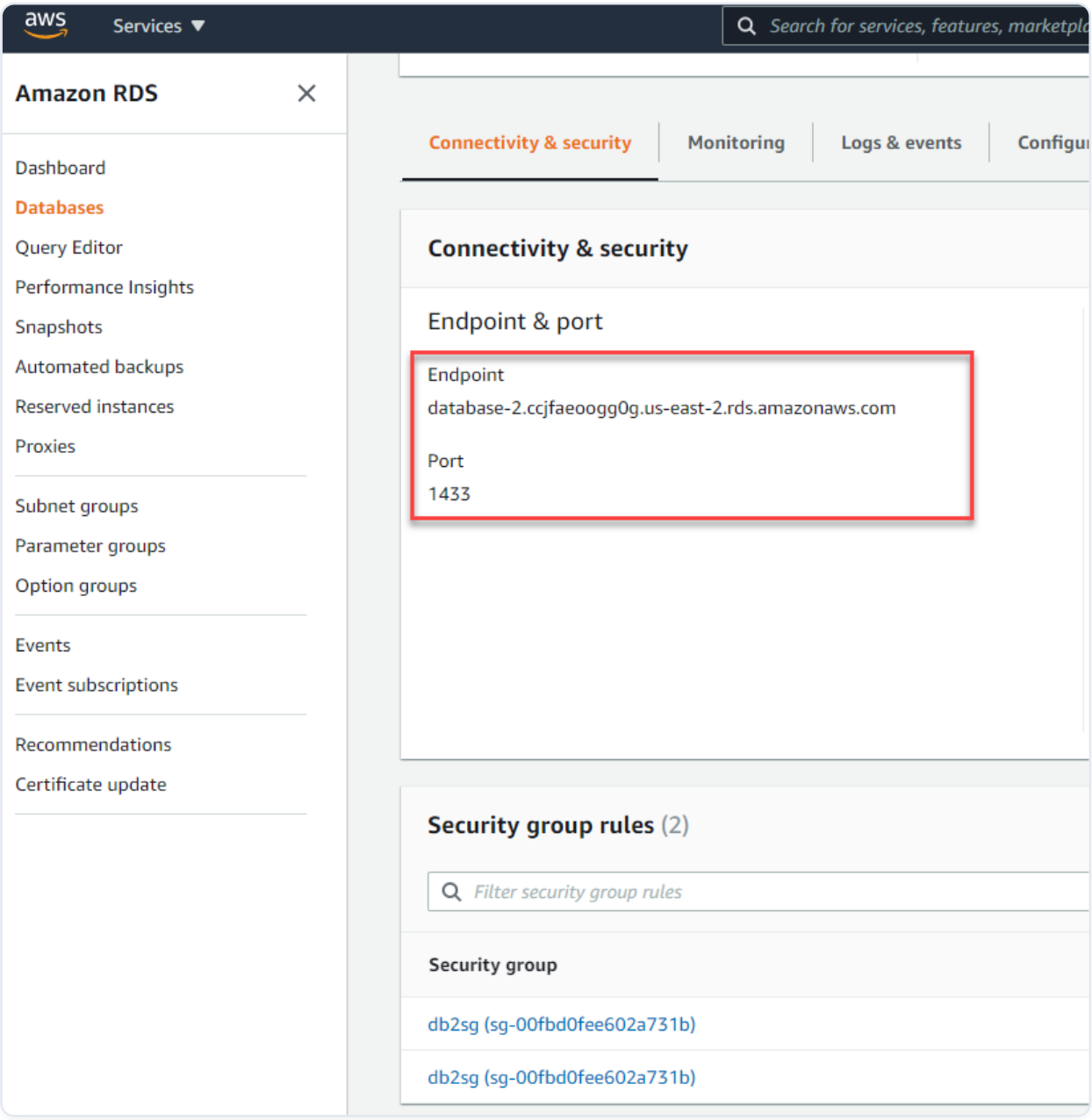
On Azure SQL Managed Instance and on AWS RDS, installation of the Session Recording database can be done by running a command similar to the following or by double-clicking and running the SessionRecordingAdministrationx64.msi package.

```
msiexec /i "SessionRecordingAdministrationx64.msi"
ADDLOCAL="SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
DATABASEINSTANCE="CloudSQL" DATABASENAME="CitrixSessionRecording"
LOGGINGDATABASENAME="CitrixSessionRecordingLogging"
AZURESQLSERVICESUPPORT="1" AZUREUSERNAME="CloudSQLAdminName"
AZUREPASSWORD="CloudSQLAdminPassword" /q /l*vx "c:\WithLogging.log"
```

1. Create an Azure SQL Managed instance or create a SQL Server instance through the Amazon RDS console.
2. (For Azure SQL only) Keep a record of the **Server** strings that appear in the properties panel. The strings are the instance name of the Session Recording database. For an example, see the following screen capture.

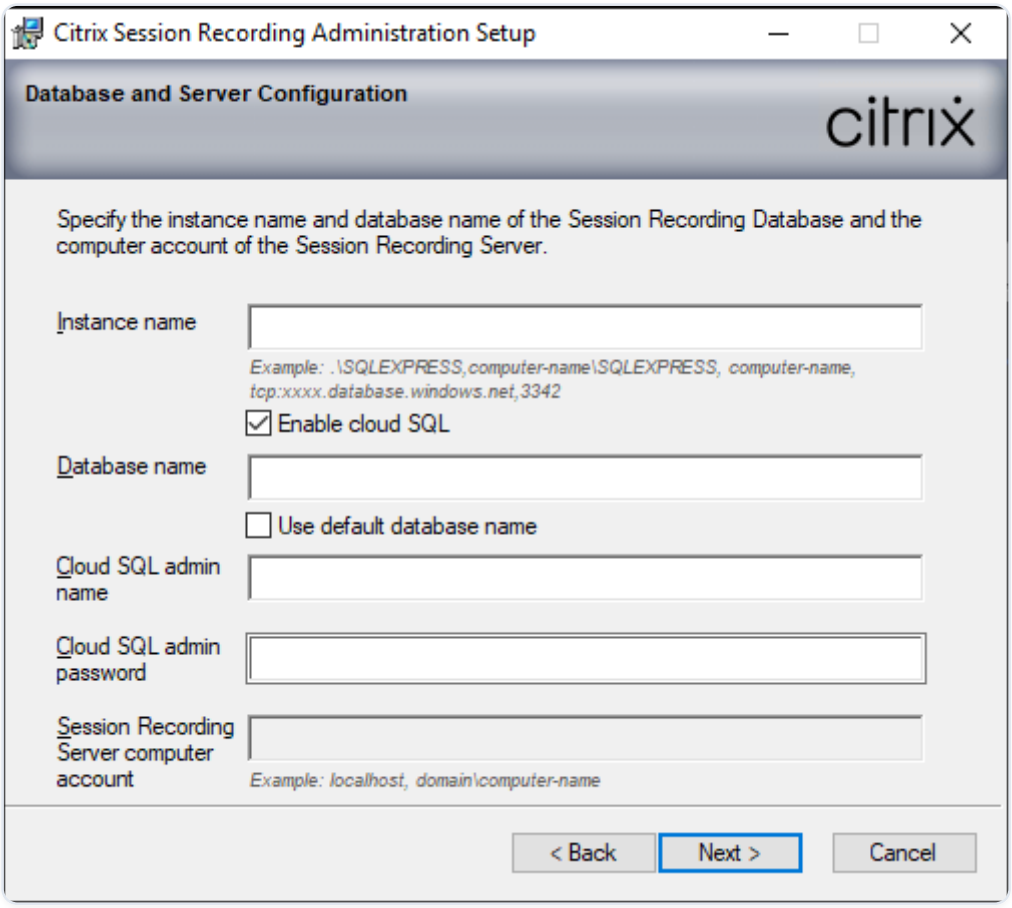


3. (For AWS RDS only) Keep a record of the **Endpoint** and **Port** information. We use it as the instance name of your database, in the format of **<Endpoint, Port>**.



4. Run SessionRecordingAdministrationx64.msi to install the Session Recording database.

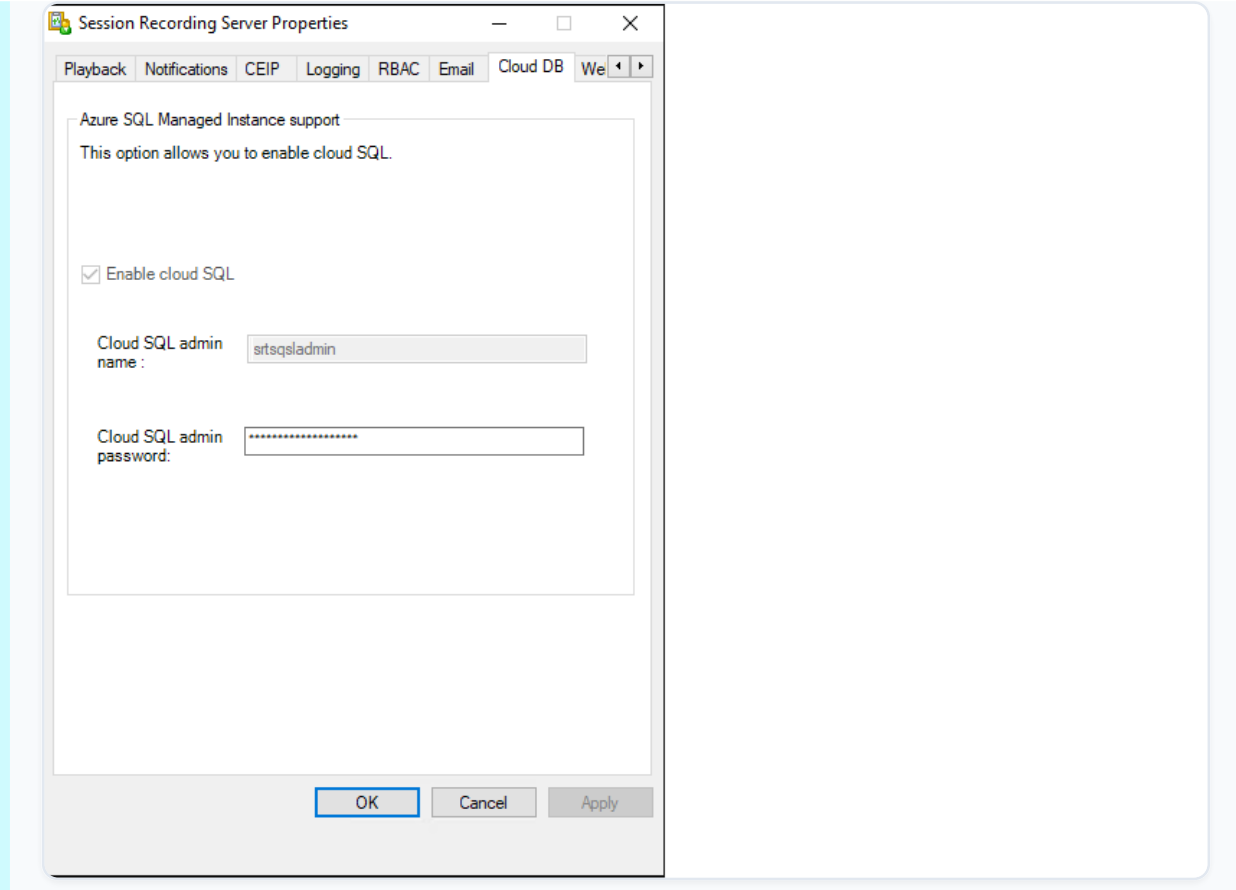
Select the **Enable cloud SQL** check box and fill in the cloud SQL admin name and password. Make other required configurations.



Note:

If you change the cloud SQL admin password, you must update the password in **Session Recording Server Properties**. When you open **Session Recording Server Properties**, an error message appears. Click **OK** to proceed, select the **Cloud DB** tab, and type the new cloud SQL admin password. Restart the Citrix Session Recording Analytics service, the Citrix Session Recording Storage Manager service, and the IIS service.

Azure AD authentication is not supported.



Migrate an on-premises database to cloud SQL Managed Instance

1. Migrate your on-premises database according to `<https://docs.microsoft.com/en-us/data-migration/>` or `<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-microsoft-sql-server-database-to-amazon-rds-for-sql-server.html>`.
2. To make Session Recording work properly after the migration, run SsRecUtils.exe on the Session Recording server.

   ```
   C:\Program Files\Citrix\SessionRecording\Server\bin\SsRecUtils.exe -modifyazuredbconnectionpara {Database Instance} {Session Recording Database Name} {Session Recording Logging Database Name} {AzureAdminName} {AzureAdminPassword} iisreset /noforce
   ```

3. On the Session Recording server, restart the Citrix Session Recording Analytics service, the Citrix Session Recording Storage Manager service, and the IIS service.

Migrate a production database from Azure SQL Managed Instance to an on-premises database

1. Migrate the database according to `<https://docs.microsoft.com/en-us/data-migration/>`.
2. To make Session Recording work properly after the migration, run SsRecUtils.exe on the Session Recording server.

   ```
   C:\Program Files\Citrix\SessionRecording\Server\bin\SsRecUtils.exe -modifydbconnectionpara {Database Instance} {Session Recording Database Name} {Session Recording Logging Database Name} iisreset /noforce
   ```

3. On the Session Recording server, restart the Citrix Session Recording Analytics service, the Citrix Session Recording Storage Manager service, and the IIS service.

Install the Session Recording database on SQL Server on Azure VMs

On SQL Server on Azure VMs, you can install the Session Recording database by double-clicking and running the SessionRecordingAdministrationx64.msi package or by using the Citrix Virtual Apps and Desktops installer.

1. Check out an Azure SQL VM.
2. Configure the VM and add it to the domain where you install the Session Recording components.
3. Use the VM's FQDN as the instance name during the installation of the Session Recording database. **Note:** If you are using SessionRecordingAdministrationx64.msi for the installation, clear the **Enable cloud SQL** check box.
4. Follow the installation user interface to complete installing the Session Recording database.

Uninstall Session Recording

To remove the Session Recording components from a server or workstation, use the uninstall or remove programs option available from the Windows Control Panel. To remove the Session Recording database, you must have the same **securityadmin** and **dbcreator** SQL Server role permissions as when you installed it.

For security reasons, the administrator logging database is not removed after the components are uninstalled.

Integrate with Citrix Analytics for Security™

You can configure Session Recording servers to send user events to Citrix Analytics for Security, which processes the user events to provide actionable insights into user behaviors.

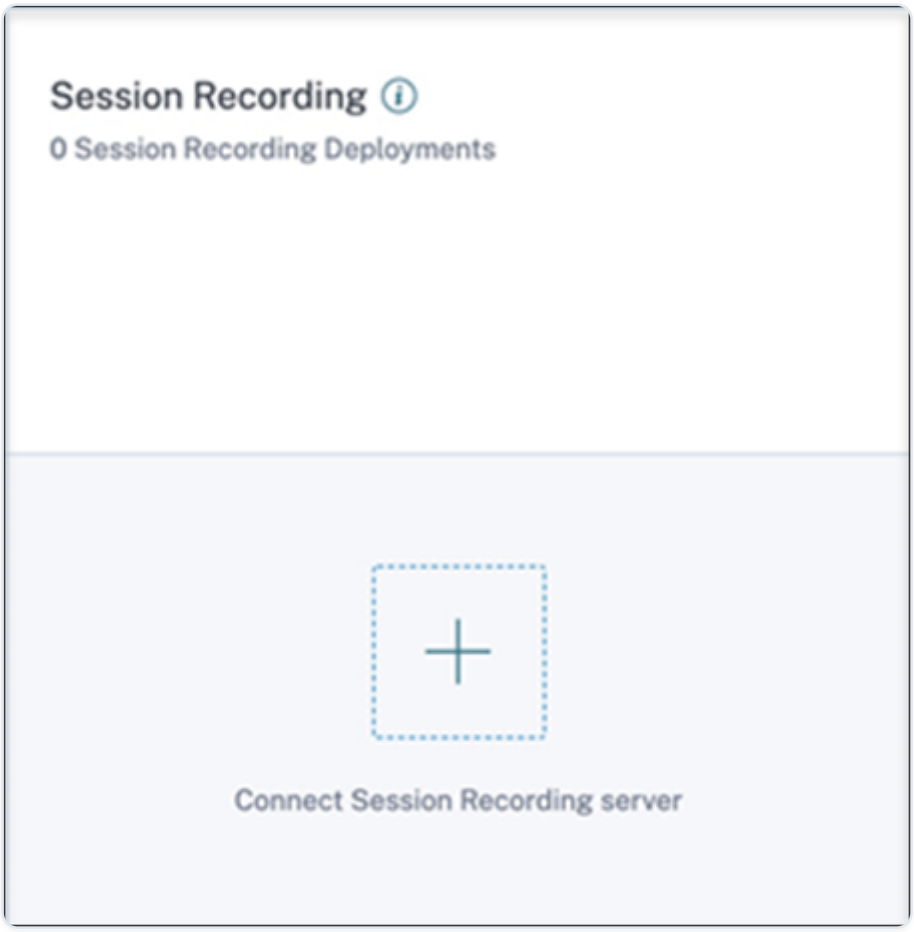
Prerequisites

Before you begin, ensure the following:

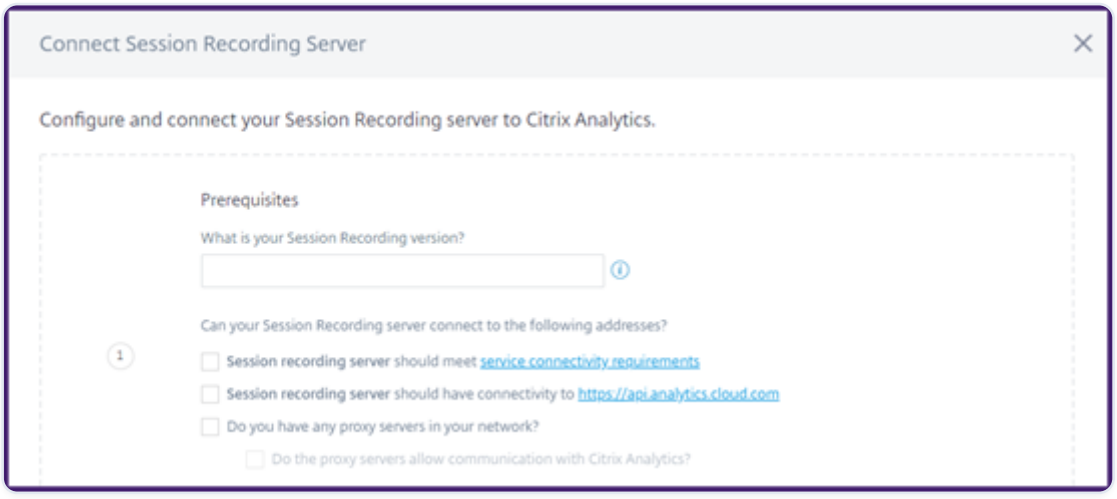
- The Session Recording server must be able to connect to the following addresses:
  - `<https://*.cloud.com>`
  - `<https://*.citrixdata.com>`
  - `<https://api.analytics.cloud.com>`
- The Session Recording deployment must have port 443 open for outbound internet connections. Any proxy servers on the network must allow this communication with Citrix Analytics for Security.
- If you are using Citrix Virtual Apps and Desktops 7 1912 LTSR, the supported Session Recording version is 2103 or later.

Connect your Session Recording server to Citrix Analytics for Security

1. Sign in to Citrix Cloud.
2. Find Citrix Analytics for Security and click **Manage**.
3. From the top bar, click **Settings > Data Sources**.
4. On the **Virtual Apps and Desktops- Session Recording** site card, click **Connect Session Recording server**.



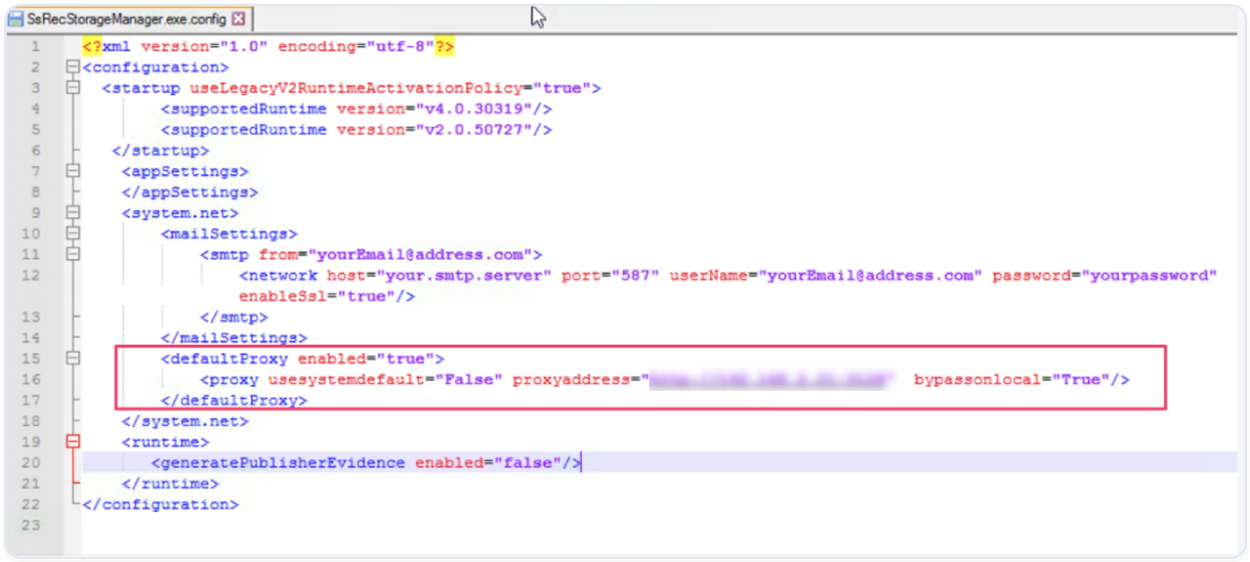
5. On the **Connect Session Recording Server** page, review the checklist, and select all the mandatory requirements. If you do not select a mandatory requirement, the **Download File** option is disabled.



6. If you have proxy servers in your network, enter the proxy address in the *SsRecStorageManager.exe.config* file in your Session Recording server.

   You can find the configuration file at `<Session Recording server installation path>\bin\SsRecStorageManager.exe.config`

For example: `C:\Program Files\Citrix\SessionRecording\Server\Bin\SsRecStorageManager.exe.config`



7. Click **Download File** to download the *SessionRecordingConfigurationFile.json* file.

> **Note:**
>
> The file contains sensitive information. Keep the file in a safe and secure location.

8. Copy the file to the Session Recording server that you want to connect to Citrix Analytics for Security.
9. If you have multiple Session Recording servers in your deployment, you must copy the file in each server that you want to connect and follow the steps to configure each server.
10. On the Session Recording server, run the following command to import the settings:

```
<Session Recording server installation path>\bin\SsRecUtils.exe
-Import_SRCasConfigurations <configuration file path>
```

For example:

```
C:\Program Files\Citrix\SessionRecording\Server\bin\SsRecUtils.exe
-Import_SRCasConfigurations C:
\Users\administrator\Downloads\SessionRecordingConfigurationFile.json
```

11. Restart the following services:

- Citrix Session Recording Analytics Service
- Citrix Session Recording Storage Manager

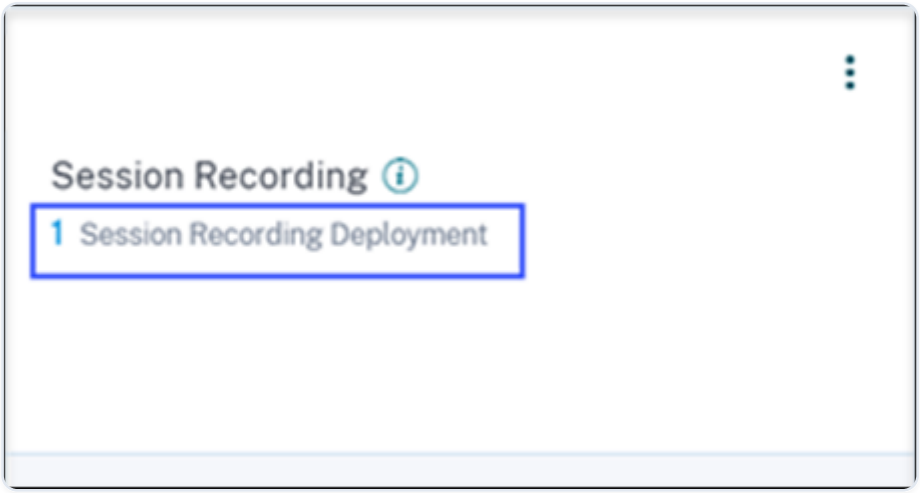
12. After configuration is successful, go to Citrix Analytics for Security to view the connected Session Recording server. Click **Turn On Data Processing** to allow Citrix Analytics for Security to process the data.

> **Note:**
>
> If you are using Session Recording server version 2103 or 2104, you must first launch a Virtual Apps and Desktops session to view the connected Session Recording server on Citrix Analytics for Security. Otherwise the connected Session Recording server fails to get displayed. This requirement is not applicable for Session Recording server version 2106 and later.

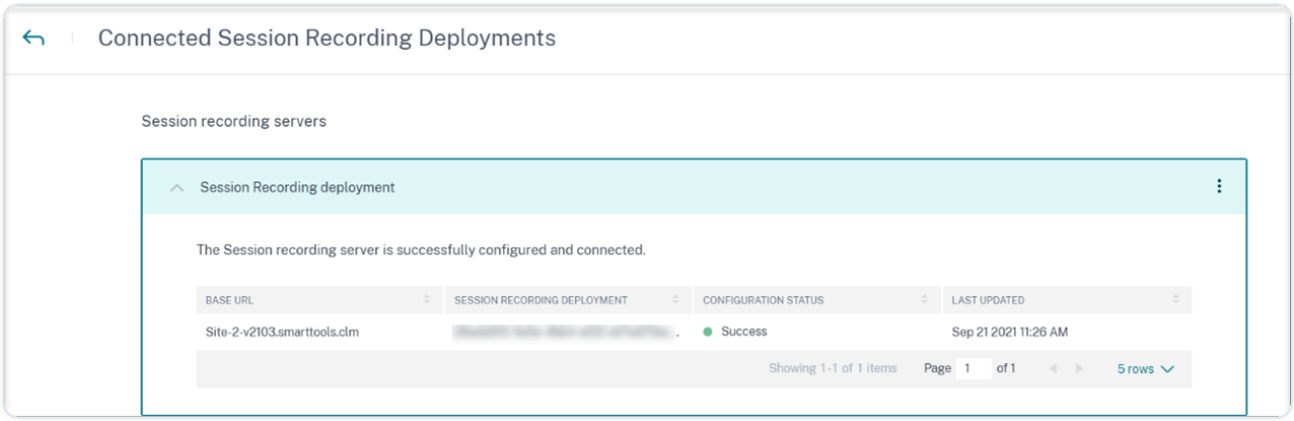
View the connected deployments

The server deployments appear on the Session Recording site card only if the configuration is successful. The site card shows the number of configured servers that have established connections with Citrix Analytics for Security.

If you don't see your Session Recording servers even after the configuration was successful, refer to the troubleshooting section at Configured Session Recording server fails to connect.



On the site card, click the number of deployments to view the connected server groups with Citrix Analytics for Security. For example, click **1 Session Recording Deployment** to view the connected server or server groups. Each Session Recording server is represented by a base URL and a ServerGroupID.



View received events

The site card displays the connected Session Recording deployments and the events received from these deployments for the last one hour, which is the default time selection. You can also select 1 week (1 W) and view the data. Click the number of received events to view the events on the self-service search page.

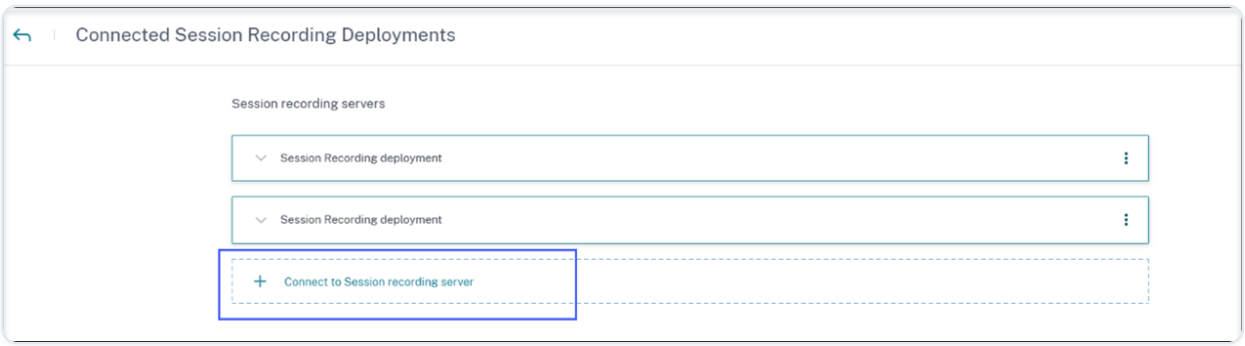
After you have enabled data processing, the site card might display the **No data received** status. This status appears for two reasons:

1. If you have turned on data processing for the first time, the events take some time to reach the event hub in Citrix Analytics. When Citrix Analytics receives the events, the status changes to **Data processing on**. If the status does not change after some time, refresh the Data Sources page.
2. Citrix Analytics has not received any events from the data source in the last one hour.

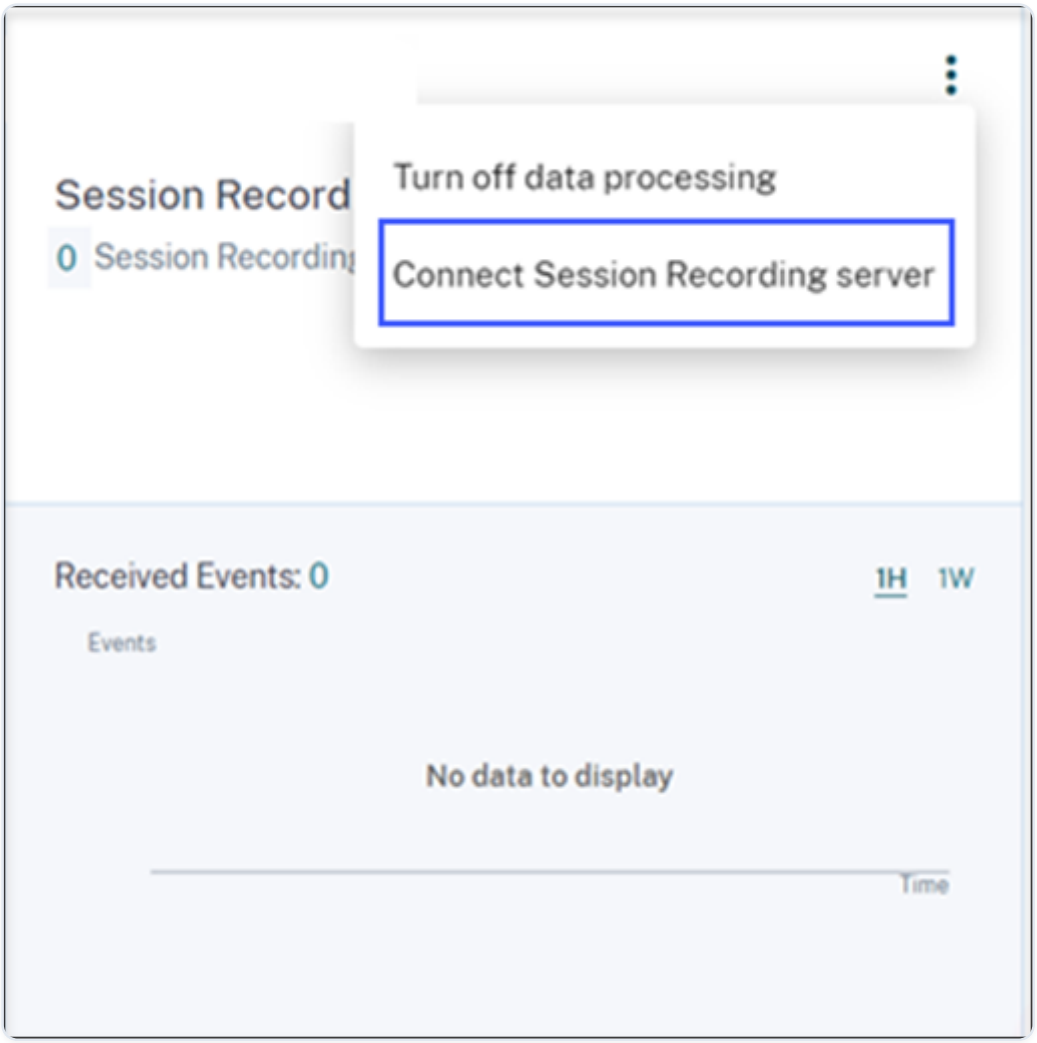
Add Session Recording servers

To add a Session Recording server, do one of the following:

- On the **Connected Session Recording Deployments** page, click **Connect to Session recording server**.



- On the **Virtual Apps and Desktops- Session Recording** site card, click the vertical ellipsis (⋮) and then select **Connect Session Recording server**.

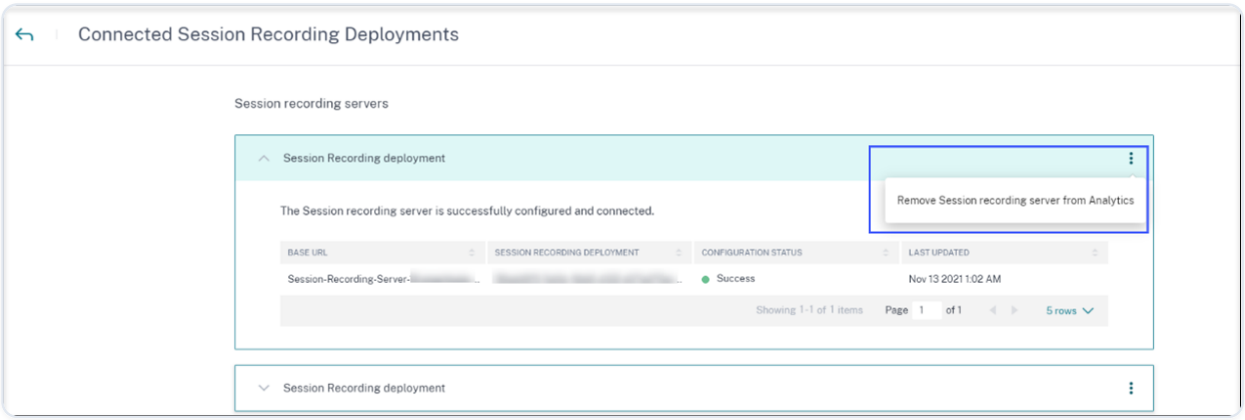


Follow the steps to download the configuration file and configure a Session Recording server.

Remove Session Recording servers

To remove a Session Recording server:

1. On Citrix Analytics for Security, go to the **Connected Session Recording Deployments** page and select the server deployment that you want to remove.
2. Click the vertical ellipses (⋮) and select **Remove Session Recording server from Analytics**.



3. On the Session Recording server that you have removed from Citrix Analytics, run the following command:

```
<Session Recording server installation path>\bin\SsRecUtils.exe
-Remove_SRCasConfigurations
```

For example:

```
C:\Program Files\Citrix\SessionRecording\Server\bin\SsRecUtils.exe
-Remove_SRCasConfigurations
```

Turn on or off data processing on the data source

You can stop the data processing at any time for a particular data source- Director and Workspace app. On the data source site card, click the vertical ellipsis (⋮) and then select **Turn off data processing**. Citrix Analytics stops processing data for that data source. You can also stop the data processing from the Virtual Apps and Desktops site card. This option applies to both data sources- Director and Workspace app. To enable data processing again, click **Turn On Data Processing**.

Configured Session Recording server fails to connect

Your Session Recording server fails to connect to Citrix Analytics after configuration. Therefore, you don't see the configured server on the **Session Recording** site card.

To troubleshoot this issue, do the following:

1. On your configured Session Recording server, run the following PowerShell command to check the Client Machine Identification (CMID):

```
Get-WmiObject -class SoftwareLicensingService | select Clientmachineid
```

2. If CMID is empty, add the following registry files in the specified paths:

REGISTRY NAME	REGISTRY PATH	KEY TYPE	VALUE
`AuditorUniqueID`	`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\`	String	Enter your UUID.
`EnableCASUseAuditorUniqueID`	`Computer/HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/SmartAuditor/Server/`	REG_DWORD	1

3. Restart the following services:

   - Citrix Session Recording Analytics Service
   - Citrix Session Recording Storage Manager

Dynamic session recording

Previously, session recording started strictly at the very beginning of sessions that met the recording policies and stopped strictly when those sessions ended.

Starting with the 7.18 release, Citrix introduces the dynamic session recording feature. With this feature, you can start or stop recording a specific session or sessions that a specific user launches, at any time during the sessions.

> **Note:**
>
> To make the feature work as expected, upgrade Session Recording, VDA, and Delivery Controller to Version 7.18 or later.

Enable or disable dynamic session recording

On the Session Recording agent, a registry value is added for enabling or disabling the feature. The registry value is set to **1** by default, which means that the feature is enabled by default.

To enable or disable the feature, complete the following steps:

1. After the Session Recording installation is complete, log on as an administrator to the machine where you installed the Session Recording agent.
2. Open the Registry Editor.
3. Browse to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor`.
4. Set the value of **DynamicControlAllowed** to **0** or use the default value, **1**.

   1: enable dynamic recording **0**: disable dynamic recording
5. Restart the Session Recording agent to make your setting take effect.

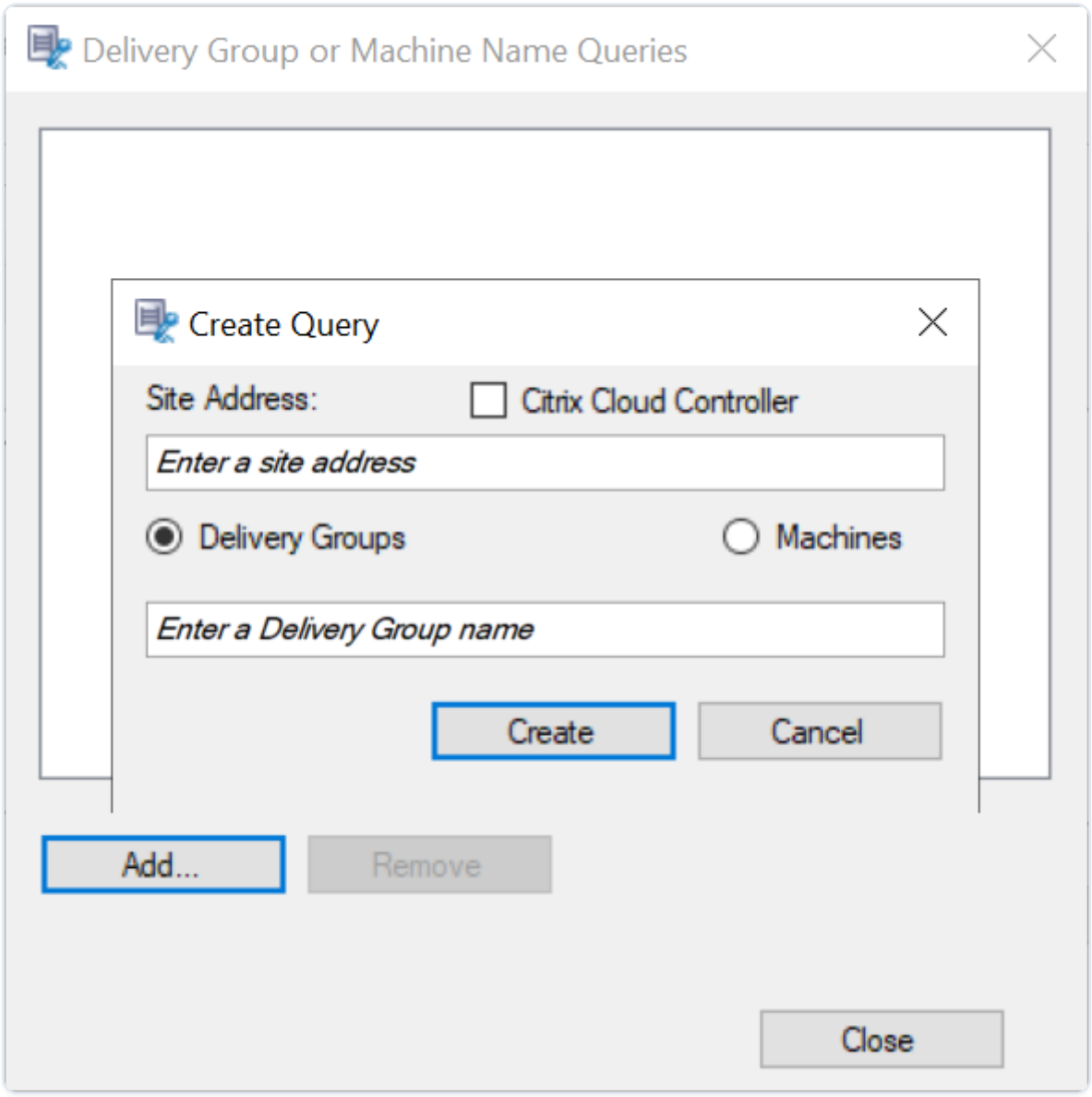
   If you are using MCS or PVS for deployment, change the setting on your master image and perform an update to make your change take effect.

> **Warning:**
>
> Incorrectly editing the registry can cause serious problems that might require you to reinstall your operating system. Citrix® cannot guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Dynamically start or stop recording by using PowerShell commands in the Citrix SDKs

You can use the dynamic session recording feature in both on-premises and Citrix Cloud environments. To use the feature in an on-premises environment, use the Citrix Virtual Apps and Desktops™ PowerShell SDK. To use the feature in a Citrix Cloud environment, use the Citrix DaaS Remote PowerShell SDK (formerly Citrix Virtual Apps and Desktops Remote PowerShell SDK).

To determine which SDK to install and use, be aware of the Delivery Controller™ that you specified when creating your recording policy. If you select the **Citrix Cloud Controller** check box to record sessions in a Citrix Cloud environment, you must validate your Citrix Cloud credentials.



Note:

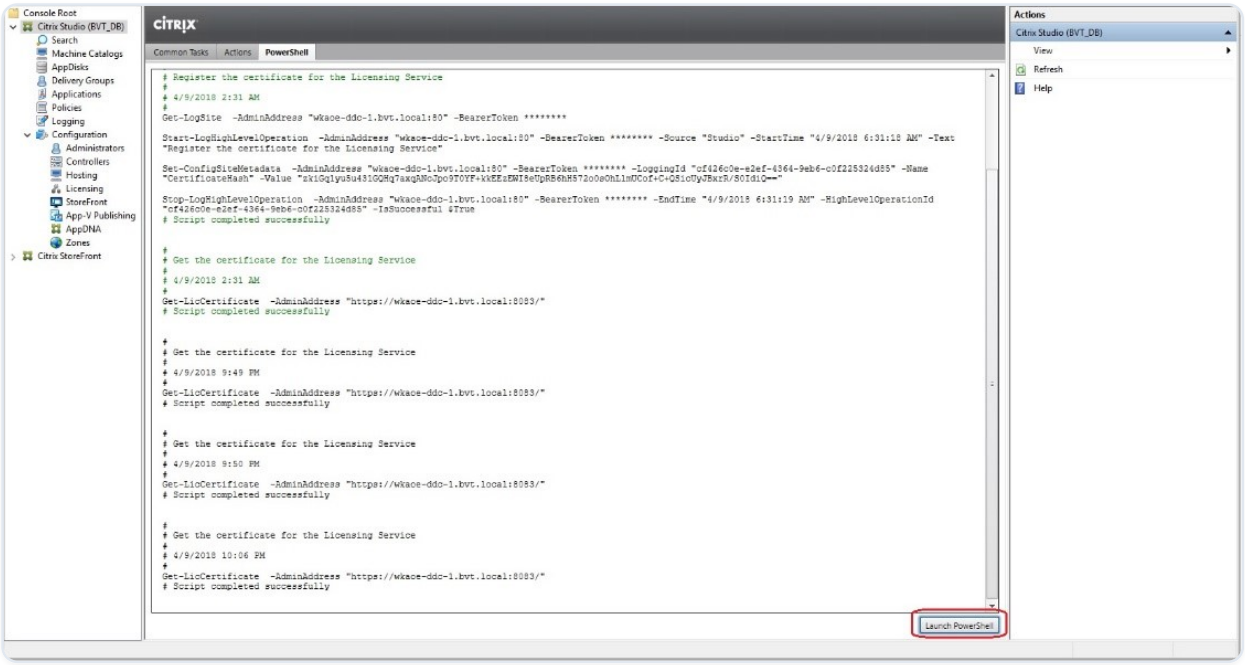
Do not install the Citrix DaaS Remote PowerShell SDK on a Citrix Cloud Connector™ machine. You can install the Remote PowerShell SDK on any domain-joined machine within the same resource location. We recommend that you do not run this SDK's cmdlets on Cloud Connectors. The SDK's operation does not involve the Cloud Connectors.

The following table lists three PowerShell commands that both Citrix SDKs provide for dynamic session recording.

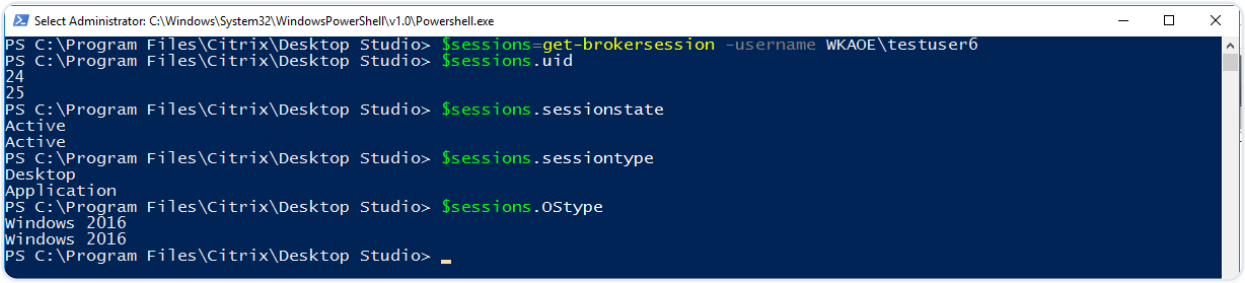
COMMAND	DESCRIPTION
Start-BrokerSessionRecording	Lets you start recording a specific active session, a list of active sessions, or sessions launched by a specific user. For more information, run `Get-Help Start-BrokerSessionRecording` to see the command online help.
Stop-BrokerSessionRecording	Lets you stop recording a specific active session, a list of active sessions, or sessions launched by a specific user. For more information, run `Get-Help Stop-BrokerSessionRecording` to see the command online help.
Get-BrokerSessionRecordingStatus	Lets you get the recording status of a specific active session. For more information, run `Get-Help Get-BrokerSessionRecordingStatus` to see the command online help.

For example, when a user reports an issue and needs timely support, you can use the feature to dynamically start recording the user's active sessions. You can play the live recording to proceed with the follow-up troubleshooting. You can do the following:

1. (For Citrix Virtual Apps™ and Desktops PowerShell SDK only) Launch PowerShell from the Citrix Studio console.



2. Use the `Get-BrokerSession` command to get all the active sessions of the target user.



3. Use the `Get-BrokerSessionRecordingStatus` command to get the recording status of the specified session.

```
PS C:\Program Files\Citrix\Desktop Studio> Get-BrokerSessionRecordingStatus -Session 24
SessionNotRecorded
PS C:\Program Files\Citrix\Desktop Studio> Get-BrokerSessionRecordingStatus -Session 25
SessionNotRecorded
PS C:\Program Files\Citrix\Desktop Studio>
```

> **Note:**
>
> The **-Session** parameter can accept only one session UID at a time.

4. Use the `Start-BrokerSessionRecording` command to start recording. By default, a notification message appears to inform users of the recording activity.

   The following table shows common ways of using the `Start-BrokerSessionRecording` command.

COMMAND	DESCRIPTION
`Start-BrokerSessionRecording -User DomainA \ UserA`	Starts recording all sessions of user UserA in the domain named DomainA and notifies UserA.
`Start-BrokerSessionRecording -User DomainA \ UserA -NotifyUser $false`	Starts recording all sessions of user UserA in the domain named DomainA and does not notify UserA.
`Start-BrokerSessionRecording -Sessions $SessionObject`	Starts recording all sessions in the object named $SessionObject and notifies the user. To get the object $SessionObject, run `$SessionObject=Get-BrokerSession –username UserA`. The name of an object is prefixed with a dollar sign $. For more information, see Step 2 and the command online help.
`Start-BrokerSessionRecording -Sessions uid1,uid2,…,uidn`	Starts recording the sessions `UID1`, `UID2`, … , and `UIDn`, and notifies the users.

5. Use the `Get-BrokerSessionRecordingStatus` command to get the recording status of each target session. The status is supposed to be **SessionBeingRecorded**.
6. Play back the **Live** or **Complete** recordings and proceed with the follow-up troubleshooting.

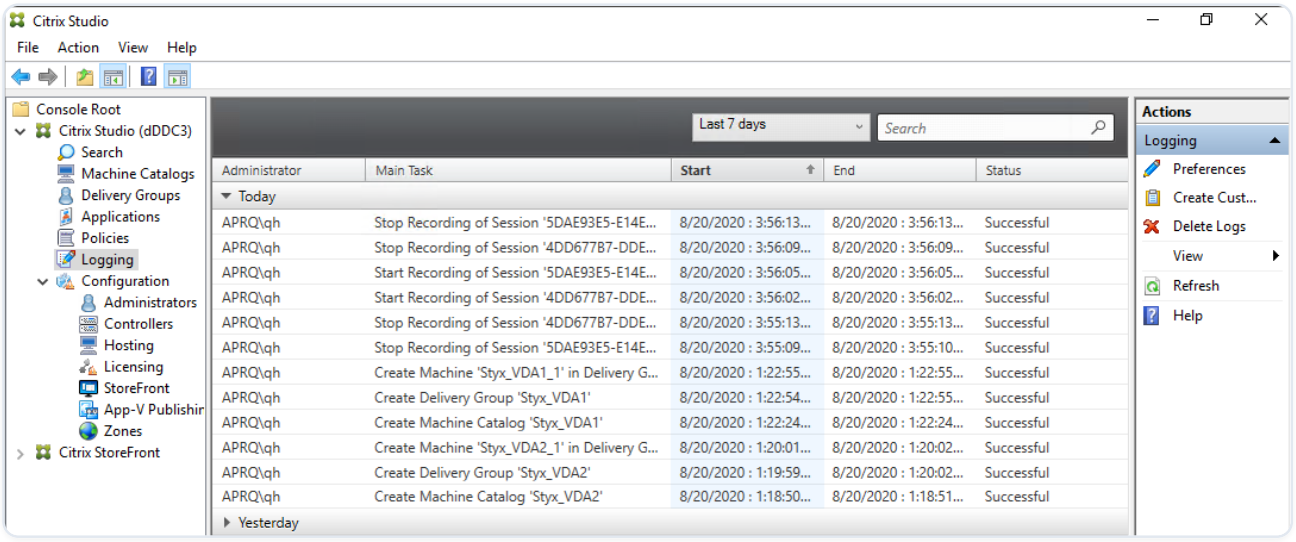
> **Note：**
>
> When you play a **Complete** recording ended by the `Stop-BrokerSessionRecording` command, the last section of the timeline on the player progress bar might show gray. And, the last section of the recorded session is idle. It is not obvious when the recorded session has constant activities.

7. Use the `Stop-BrokerSessionRecording` command to stop recording when the reported issue has been triaged or resolved.

   The following table shows common ways of using this command:

COMMAND	DESCRIPTION
`Stop-BrokerSessionRecording -User DomainA` \ UserA	Stops recording all sessions of user UserA in the domain named DomainA.
`Stop-BrokerSessionRecording -Sessions $SessionObject`	Stops recording all sessions in the $SessionObject.
`Stop-BrokerSessionRecording -Sessions uid1,uid2,…,uidn`	Stops recording the sessions `UID1`, `UID2`, … , and `UIDn`.

On the Citrix Studio **Logging** screen, you can view the resulting logs of the `Start-BrokerSessionRecording` and `Stop-BrokerSessionRecording` commands.



Configure

This section provides instructions for you to configure the following settings:

- Settings on the Session Recording agent
  - Enable or disable recording
  - Configure the connection to the Session Recording Server
  - Configure the communication protocol
- Settings on the Session Recording server
  - Authorize users
  - Customize notification messages
  - Specify where recordings are stored
  - Specify file size for recordings
  - Enable or disable digital signing
  - CEIP and Google Analytics
- Policies
  - Configure session recording policies
  - Configure recording viewing policies
  - Configure event detection policies
  - Configure event response policies
- High availability and load balancing
  - Load balance Session Recording servers
  - Configure database high availability

Configure settings on the Session Recording agent

This section guides you through the following settings:

- Enable or disable recording
- Configure the connection to the Session Recording Server
- Configure the communication protocol

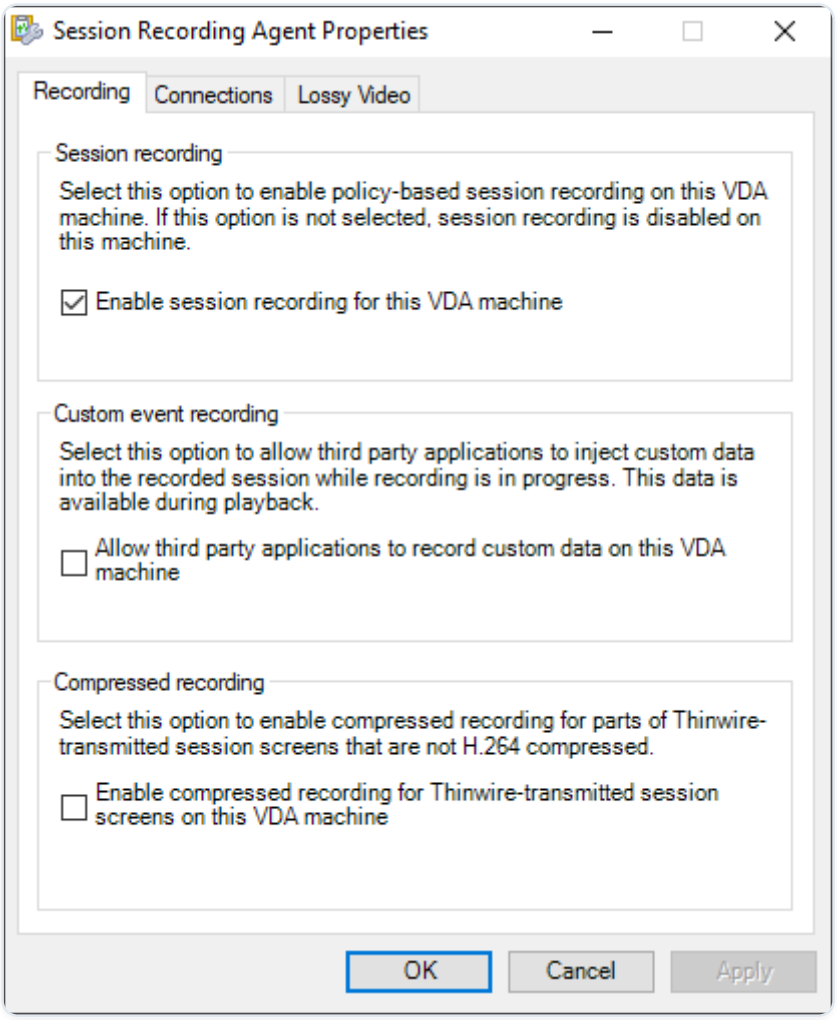
Enable or disable recording

You install the Session Recording agent on multi-session OS VDAs for which you want to record sessions. Within each agent is a setting that enables recording for the VDA on which it is installed. After recording is enabled, Session Recording evaluates the active recording policy that determines which sessions are recorded.

We recommend you disable session recording on VDAs that are not recorded. There is a small impact on performance, even if no recording takes place.

Enable or disable recording on a VDA

1. Log on to the server where the Session Recording agent is installed.
2. From the **Start** menu, choose **Session Recording Agent Properties**.
3. Under **Session Recording**, select or clear the **Enable session recording for this VDA machine** check box to specify whether sessions can be recorded for this VDA.



4. When prompted, restart the Session Recording agent service to accept the change.

> **Note:**
>
> When you install Session Recording, the active policy is **Do not record** (no sessions are recorded on any server). To begin recording, use the Session Recording policy console to activate a different policy.

Enable custom event recording

Session Recording allows you to use third-party applications to insert custom data, known as events, to recorded sessions. These events appear when the recorded session is played back. Events are part of the recorded session file and can't be modified after the session is recorded.

For example, an event might contain the following text: "User opened a browser." Each time a user opens a browser during a session being recorded, the text inserts to the recording at that point.

When a viewer plays back the recorded session, the viewer can locate and count the times that the user opened a browser by noting the number of markers.

To insert custom events to recordings on a server:

- Use **Session Recording Agent Properties** to enable a setting on each server where you want to insert custom events. Enable each server separately. You can't globally enable all servers in a site.
- Write applications built on the Event API that runs within each user's virtual session, to inject the data into the recording.

The Session Recording installation includes an event recording COM application (API) that allows you to insert text from third-party applications to a recording. You can use the API from many programming languages including Visual Basic, C++, or C#. For more information, see the Knowledge Center article CTX226844. The Session Recording Event API .dll is installed as part of the Session Recording installation. You can find it at `C:\rogram Files\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll`.

To enable custom event recording on a server, complete the following steps:

1. Log on to the server where the Session Recording agent is installed.
2. From the **Start** menu, choose **Session Recording Agent Properties**.
3. In **Session Recording Agent Properties**, click the **Recording** tab.
4. Under **Custom event recording**, select the **Allow third party applications to record custom data on this server** check box.

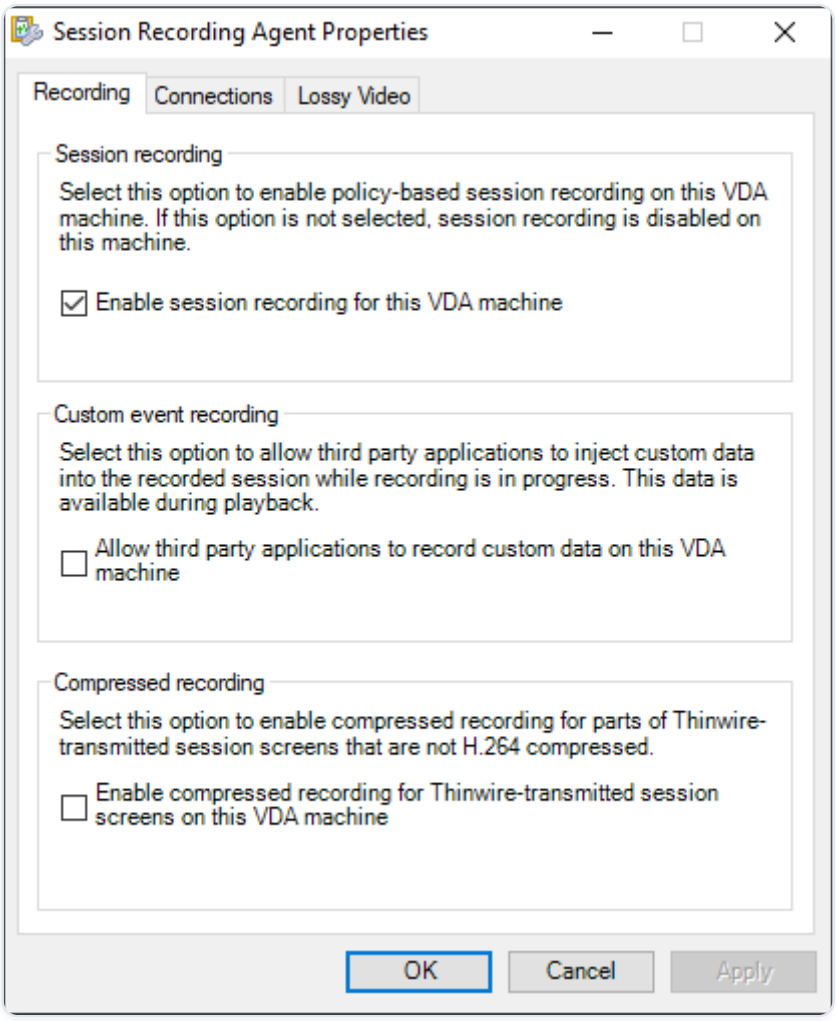
Enable compressed recording

You can enable compressed recording for parts of Thinwire-transmitted session screens that are not H.264 compressed. This feature reduces recording file size significantly.

> **Note:**
>
> - This feature is disabled by default.
> - This feature is incompatible with the H.264 package dropping feature.
> - The minimum version required for the VDA is 2303.

To enable compressed recording, complete the following steps:

1. Log on to the server where the Session Recording agent is installed.
2. From the **Start** menu, choose **Session Recording Agent Properties**.
3. In **Session Recording Agent Properties**, click the **Recording** tab.
4. Under **Compressed recording**, select the **Enable compressed recording for Thinwire-transmitted session screens on this VDA machine** check box.

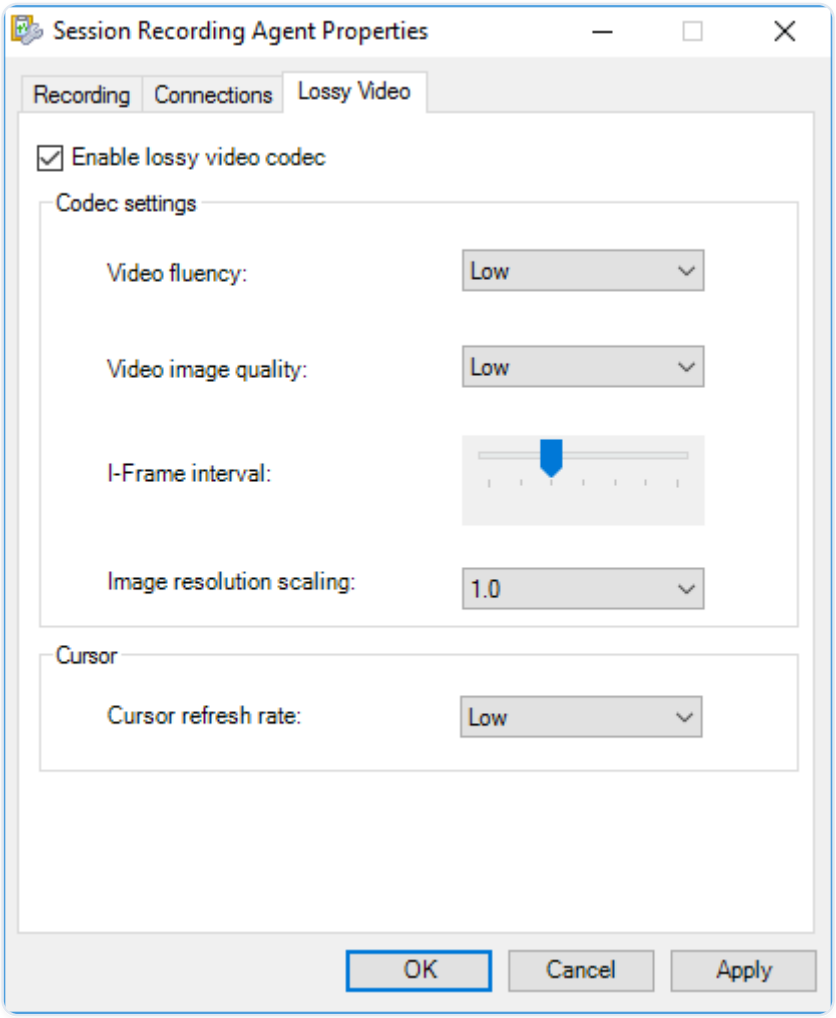


Enable or disable lossy video codec

Lossy video codec lets you adjust compression options to reduce the size of recording files and to accelerate navigating recorded sessions during playback. Lossy video codec is suitable for use when:

- the size of recording files per time unit is too large, or
- there is a lag while you fast forward or rewind during recording playback.

To enable the lossy video codec feature, open the **Lossy Video** tab of **Session Recording Agent Properties** and adjust the compression options to your needs. We recommend you use the default values unless there is a practical need to change the values.



For a description of compression options, see the following table:

COMPRESSION OPTION	DESCRIPTION	DEFAULT VALUE	REMARKS
Video fluency (FPS)	**Low**: 1, **Medium**: 10, **High**: 20	**Low**	N/A
Video image quality	**Low**: `minCrf:33` `maxCrf:45`, **Medium**: `minCrf:25` `maxCrf:37`, **High**: `minCrf:18` `maxCrf:30`	**Low**	N/A

COMPRESSION OPTION	DESCRIPTION	DEFAULT VALUE	REMARKS
I-Frame interval (seconds)	**60**, **120**, **300**, **600**, **1200**, **1800**, **3600**	**600**	The larger the I-Frame interval value, the smaller the storage space occupied by the compressed video. The smaller the I-Frame interval value, the better the seeking experience (fast forward and rewind).
Image resolution scaling	**1.0**, **0.9**, **0.8**, **0.7**, **0.6**, **0.5**, **0.4**	**1**	You can downscale the resolution of recorded screens to a percentage, for example, **0.9** means **90%**. If you don't want to change the resolution, use the default value, **1.0**.
Cursor refresh rate (times per second)	**Low**: 3, **Medium**: 5, **High**: 10	**Low**	N/A

You can also set image resolution scaling by editing Registry. To do so, complete the following steps:

> **Warning:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix® cannot guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. Browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent\SRGraphicsZoomFactor**.
2. Set a value data that suits your needs. For the optional values, see the preceding table.

Configure the connection to the Session Recording server

Configure the connection of the Session Recording player to the Session Recording server

Before a Session Recording player can play sessions, configure it to connect to the Session Recording server that stores the recorded sessions. Each player can be configured with the ability to connect to multiple Session Recording servers, but can connect to only one Session Recording server at a time. If a player is configured with the ability to connect to multiple Session Recording servers, users can change which Session Recording server the player connects to.

1. Log on to the workstation where the Session Recording player is installed.
2. Start the Session Recording player.
3. From the Session Recording player menu bar, choose **Tools > Options**.
4. On the **Connections** tab, click **Add**.
5. In the **Hostname** field, type the name or IP address of the machine hosting the Session Recording server and select the protocol. By default, Session Recording is configured to use HTTPS/SSL to secure communications. If SSL is not configured, select HTTP.
6. To configure the Session Recording player with the ability to connect to multiple Session Recording servers, repeat Steps 4 and 5 for each Session Recording server.
7. Ensure that you select the check box of the Session Recording server you want to connect to.

Configure the connection of the Session Recording agent to the Session Recording server

The connection is typically configured when the Session Recording agent is installed. To configure this connection after the Session Recording agent is installed, use **Session Recording Agent Properties**.

1. Log on to the server where the Session Recording agent is installed.
2. From the **Start** menu, choose **Session Recording Agent Properties**.
3. Click the **Connections** tab.
4. In the **Session Recording Server** field, type the FQDN of the Session Recording server.

> **Note:**
>
> To use Message Queuing over HTTPS (TCP is used by default), type an FQDN in the **Session Recording Server** field. Otherwise, session recording fails.

5. In the **Session Recording Storage Manager message queue** section, select the protocol that is used by the Session Recording Storage Manager to communicate and change the default port number if necessary.

> **Note:**
>
> To use Message Queuing over HTTP and HTTPS, install all the IIS recommended features.

6. In the **Message life** field, accept the default 7,200 seconds (two hours) or type a new value for the number of seconds each message is retained in the queue if there is a communication failure. After this time elapses, the message is deleted and the file is playable until the point where the data is lost.
7. In the **Session Recording Broker** section, select the communication protocol that the Session Recording Broker uses to communicate and change the default port number if necessary.
8. When prompted, restart the **Session Recording Agent Service** to accept the changes.

Change your communication protocol

For security reasons, Citrix® does not recommend using HTTP as a communication protocol. The Session Recording installation is configured to use HTTPS. To use HTTP instead of HTTPS, you must change several settings.

Use HTTP as the communication protocol

1. Log on to the machine hosting the Session Recording server and disable secure connections for Session Recording Broker in IIS.
2. Change the protocol setting from HTTPS to HTTP in **Session Recording Agent Properties** on each server where the Session Recording agent is installed:

    a. Log on to each server where the Session Recording agent is installed.

b. From the **Start** menu, choose **Session Recording Agent Properties**.

c. In **Session Recording Agent Properties**, choose the **Connections** tab.

d. In the **Session Recording Broker** area, select **HTTP** from the **Protocol** drop-down list and click **OK** to accept the change. If you are prompted to restart the service, click **Yes**.

3. Change the protocol setting from HTTPS to HTTP in the Session Recording Player settings:

a. Log on to each workstation where the Session Recording Player is installed.

b. From the **Start** menu, choose **Session Recording Player**.

c. From the **Session Recording Player** menu bar, choose **Tools** \> **Options** \> **Connections**, select the server, and choose **Modify**.

d. Select **HTTP** from the **Protocol** drop-down list and click **OK** twice to accept the change and exit the dialog box.

4. Change the protocol setting from HTTPS to HTTP in the Session Recording policy console:

a. Log on to the server where the Session Recording policy console is installed.

b. From the **Start** menu, choose **Session Recording Policy Console**.

c. Select **HTTP** from the **Protocol** drop-down list and click **OK** to connect. If the connection is successful, this setting is remembered the next time you start the Session Recording policy console.

Revert to HTTPS as the communication protocol

1. Log on to the machine hosting the Session Recording server and enable secure connections for the Session Recording Broker in IIS.
2. Change the protocol setting from HTTP to HTTPS in **Session Recording Agent Properties** on each server where the Session Recording agent is installed:

a. Log on to each server where the Session Recording agent is installed.

b. From the **Start** menu, choose **Session Recording Agent Properties**.

c. In **Session Recording Agent Properties**, choose the **Connections** tab.

d. In the **Session Recording Broker** area, select **HTTPS** from the **Protocol** drop-down list and click **OK** to accept the change. If you are prompted to restart the service, click **Yes**.

3. Change the protocol setting from HTTP to HTTPS in the Session Recording Player settings:

a. Log on to each workstation where the Session Recording Player is installed.

b. From the **Start** menu, choose **Session Recording Player**.

c. From the **Session Recording Player** menu bar, choose **Tools** \> **Options** \> **Connections**, select the server, and choose **Modify**.

d. Select **HTTPS** from the **Protocol** drop-down list and click **OK** twice to accept the change and exit the dialog box.

4. Change the protocol setting from HTTP to HTTPS in the Session Recording policy console:

a. Log on to the server where the Session Recording policy console is installed.

b. From the **Start** menu, choose **Session Recording Policy Console**.

c. Select **HTTPS** from the **Protocol** drop-down list and click **OK** to connect. If the connection is successful, this setting is remembered the next time you start the Session Recording policy console.

Configure settings on the Session Recording server

This section guides you through the following settings:

- Authorize users
- Customize notification messages
- Specify where recordings are stored
- Specify file size for recordings
- Enable or disable digital signing
- CEIP and Google Analytics

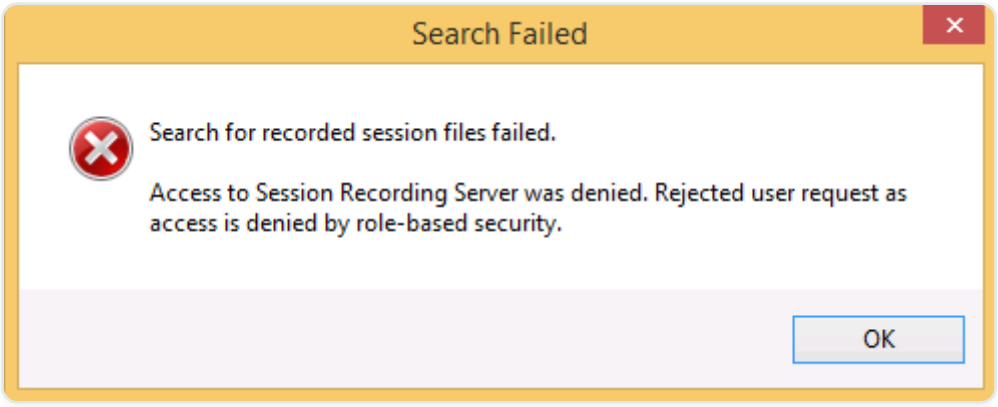
Authorize users

To grant users the rights, you assign users to roles using the Session Recording Authorization Console on the Session Recording server. Five roles are available:

> **Important:**

> For security reasons, grant users only the rights they need to perform specific functions, such as viewing recorded sessions.

- **PolicyAdministrator**. Grants the right to view, create, edit, delete, and enable recording policies. By default, administrators of the machine hosting the Session Recording server are members of this role.
- **PolicyQuery**. Allows the servers hosting the Session Recording agent to request recording policy evaluations. By default, authenticated users are members of this role.
- **LoggingWriter**. Grants the right to write the Administrator Logging logs. By default, local administrators and the Network Service group are members of this role. Changing the default **LoggingWriter** membership can cause log writing failure.
- **LoggingReader**. Grants the right to query the Administrator Logging logs. There is no default membership in this role.
- **PrivilegedPlayer**. Grants the right to place and remove access restrictions on recordings and the right to archive and delete recordings.
- **Player**. Grants the right to view recorded Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) sessions. There is no default membership in this role. When you install Session Recording, no user has the right to play recorded sessions. A user without the permission to play recorded sessions receives the following error message when trying to play a recorded session:



To assign users to a role, do the following:

1. Log on as an administrator to the machine hosting the Session Recording server.
2. Start the Session Recording Authorization Console.
3. Select the role to which you want to assign users.
4. From the menu bar, choose **Action > Assign Users and Groups**.
5. Add the users and groups.

Session Recording supports users and groups defined in the Active Directory.

Any changes made to the console take effect during the update that occurs once every minute. Also, starting with the 1906 release, you can use the Session Recording policy console to create recording viewing policies. For more information, see Recording viewing policies.

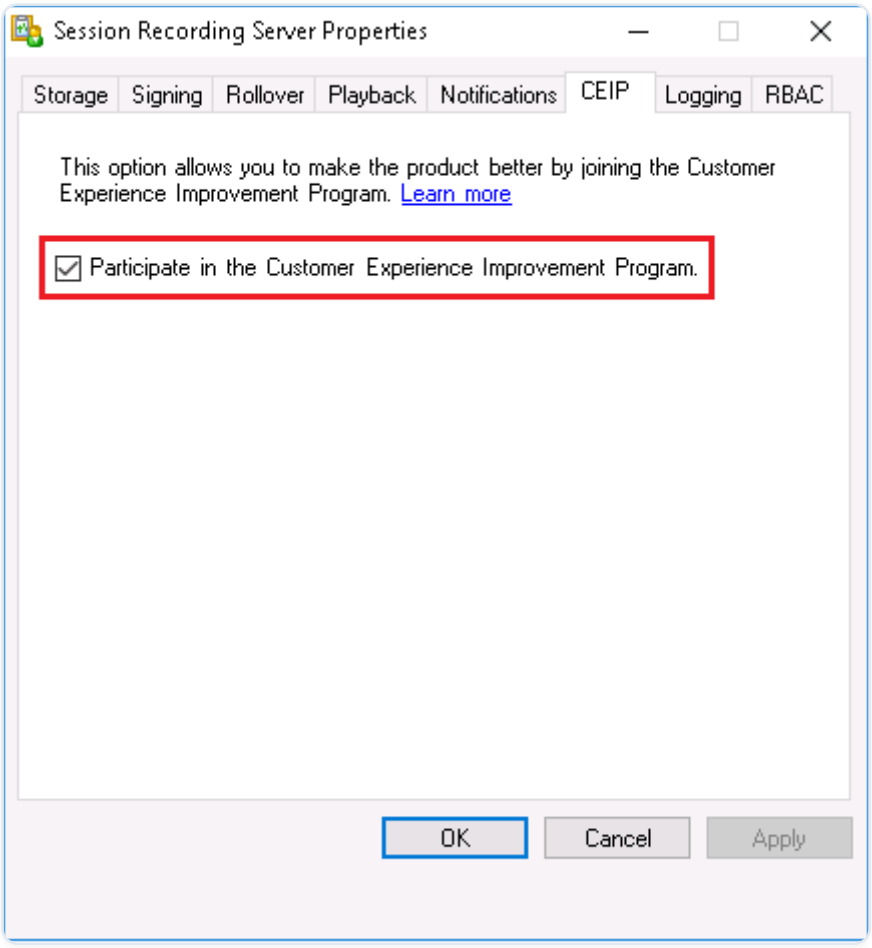
CEIP and Google Analytics

When you participate in the Citrix Customer Experience Improvement Program (CEIP), anonymous configuration and usage data is collected and sent to Citrix. The data helps improve the product quality and performance. In addition, a copy of the anonymous data can be sent to Google Analytics for fast and efficient analysis.

CEIP setting

By default, you automatically participate in CEIP when you install Session Recording. The first upload of data occurs approximately seven days after you install Session Recording. To unsubscribe from CEIP, do the following:

1. Log on to the machine hosting the Session Recording server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **CEIP** tab.
4. Clear the **Participate in the Customer Experience Improvement Program** check box.
5. Restart the **Citrix Session Recording Analytics Service** for the setting to take effect.



Google Analytics setting

When Google Analytics is enabled, the heartbeat data between Google Analytics and the Session Recording server is collected every 5 hours. User behavior data on the web player is also sent to Google Analytics. User behavior includes activities such as opening the web player and playing or searching recordings in it.

Google Analytics is enabled by default, except for EU customers. If the time zone or region you selected when installing Session Recording belong to the EU, you are considered an EU customer and Google Analytics is disabled for you by default.

Registry setting that enables or disables Google Analytics:

Location: HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\SmartAuditor\\Server\\

Name: CeipHeartBeatDisable

Value: 1 = disabled, 0 = enabled

To disable Google Analytics, complete the following steps:

1. Log on to the machine hosting the Session Recording server.

2. Open the **Registry Editor**.
3. Browse to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\`.
4. Locate or add the registry value **CeipHeartBeatDisable**.
5. Set the value data of **CeipHeartBeatDisable** to 1.
6. Restart the Citrix Session Recording Analytics Service for the setting to take effect.

To enable Google Analytics, complete the following steps:

1. Log on to the machine hosting the Session Recording server.
2. Open the Registry Editor.
3. Browse to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\`.
4. Remove the registry value **CeipHeartBeatDisable** or set its value data to 0.
5. Restart the Citrix Session Recording Analytics Service to make for the setting to take effect.

Data collected from the Session Recording server

The following table gives an example of the types of anonymous information collected. The data does not contain any details that identify you as a customer.

DATA POINT	KEY NAME	DESCRIPTION
Machine GUID	`machine_guid`	Identifying the machine where the data originates. With Google Analytics enabled, heartbeat data is sent to Google Analytics regardless of whether CEIP is enabled.
Operating System version	`OS_version`	Text string denoting the machine's operating system. With Google Analytics enabled, heartbeat data is sent to Google Analytics regardless of whether CEIP is enabled.
Session Recording server version	`SRS_version`	Text string denoting the installed version of the Session Recording server.

DATA POINT	KEY NAME	DESCRIPTION
		With Google Analytics enabled, heartbeat data is sent to Google Analytics regardless of whether CEIP is enabled.
Number of application recordings	`application-recording-number`	Integer denoting the number of application recording files. The data is sent when both Google Analytics and CEIP are enabled.
Number of recordings	`recording-number`	Integer denoting the number of both application and desktop recording files. The data is sent when both Google Analytics and CEIP are enabled.
Number of dynamic recordings	`dynamic-recording-number`	Integer denoting the number of dynamically recorded files. The data is sent when both Google Analytics and CEIP are enabled.
Number of agents hosting recorded sessions	`recorded-agent-number`	Integer denoting the number of VDAs hosting recorded sessions. The data is sent when both Google Analytics and CEIP are enabled.
Number of agents hosting recorded sessions containing logged events	`event-logging-enabled-agent-number`	Integer denoting the number of VDAs hosting recorded sessions that contain logged events. The data is sent when both Google Analytics and CEIP are enabled.
Number of recordings containing logged events	`event-logging-recording-number`	Integer denoting the number of recording files that contain logged events. The data is sent when both Google

DATA POINT	KEY NAME	DESCRIPTION
		Analytics and CEIP are enabled.
Administrator logging enablement	`admin-logging-status`	Digit indicating the enablement of administrator logging. "1" means enabled. "0" means disabled. The data is sent when both Google Analytics and CEIP are enabled.
Number of logged events	`collected-events-number`	Integer denoting the number of logged events. The data is sent when both Google Analytics and CEIP are enabled.
Number of custom policies	`customized-policies-number`	Integer denoting the number of custom session recording and event logging policies. The data is sent when both Google Analytics and CEIP are enabled.
Load balancing enablement	`load-balancing-status`	Digit indicating the enablement of load balancing. "1" means enabled. "0" means disabled. The data is sent when both Google Analytics and CEIP are enabled.
Recording viewing policy enablement	`rbac-status`	Digit indicating the enablement of recording viewing policies. "1" means enabled. "0" means disabled. The data is sent when both Google Analytics and CEIP are enabled.

Customize notification messages

If the active recording policy records sessions with notification, users receive recording notifications after typing credentials. 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.

The default notification message appears in the language of the operating system on the VDA.

You can create custom notifications in the languages you choose. However, you can have only one notification message for each language. Your users see notification messages in the languages of their preferred local settings.

Create a notification message

1. Log on to the machine hosting the Session Recording server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Notifications** tab.
4. Click **Add**.
5. Choose the language for the message and type the new message. You can create only one message for each language.

After accepting and activating, the new message appears in the language-specific notification message box.

Enable or disable digital signing

You can install certificates on machines where you installed the Session Recording server and the Session Recording player. Doing so can enhance the security of your deployment by assigning digital signatures to Session Recording.

By default, digital signing is disabled. After you select the certificate to sign the recordings, Session Recording grants the read permission to the Session Recording Storage Manager Service.

Enable digital signing

1. Log on to the machine hosting the Session Recording server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Signing** tab.

4. Browse to the certificate that enables secure communication among the machines where you installed the Session Recording components.

Disable digital signing

1. Log on to the machine hosting the Session Recording server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Signing** tab.
4. Click **Clear**.

Session recording storage reports

Overview

A session recording storage report provides weekly statistics on screen recordings of a single or multiple load-balanced Session Recording servers. It is emailed to you and contains digest charts similar to the following:

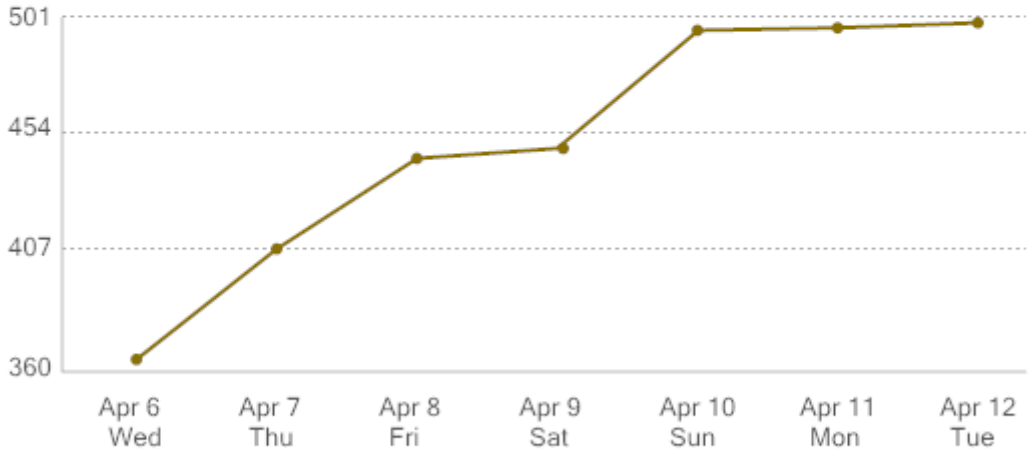
SERVER

Server time zone: (UTC-05:00) Eastern Time (US & Canada)

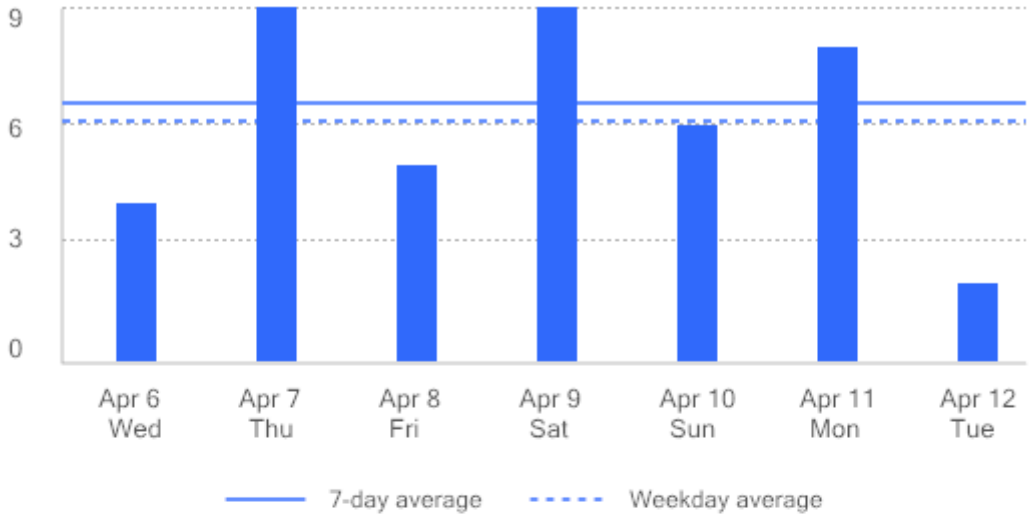
Total size of all recordings: 499.0 GB ▲ 4% over previous week

16.0 GB	1234
▼ -14%	▲ 170%
Storage used	Sessions recorded

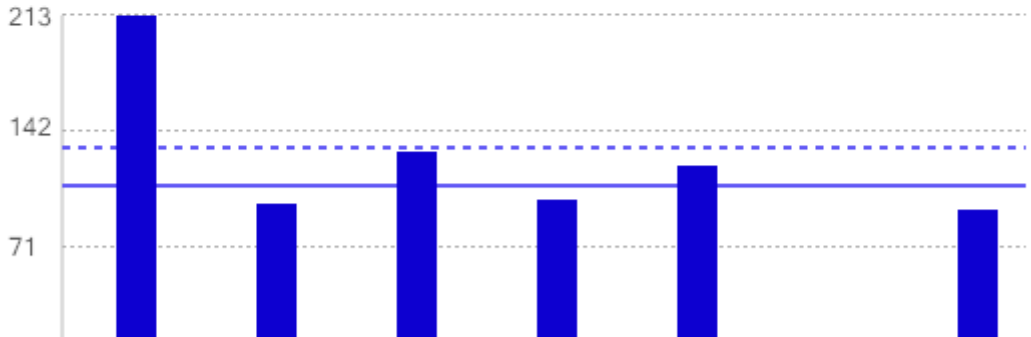
Total size of all recordings (GB)



Storage usage per day (GB)



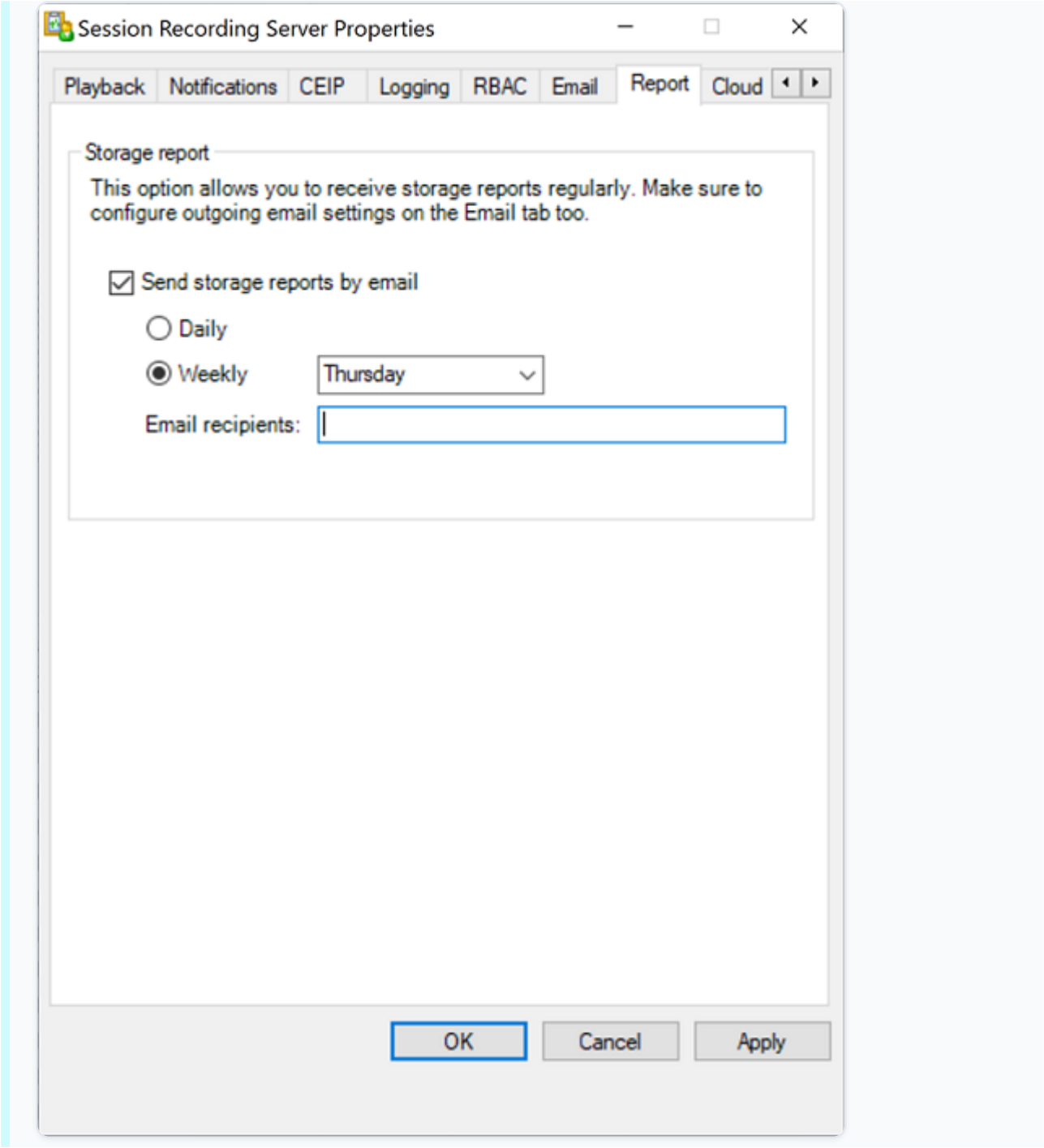
Number of sessions recorded per day



Configuration

To receive emailed session recording storage reports on a daily or weekly basis, schedule reports through Session Recording Server Properties. Make sure to configure outgoing email settings on the **Email** tab too.

> **Note:**
>
> If your Session Recording servers are configured in a load balancing manner, schedule reports on one of the servers. Otherwise, create a schedule on each of your Session Recording servers.



Specify file size for recordings

As recordings grow in size, recording files take longer to download and respond more slowly when you use the seek slider to navigate during playback. To control file size, specify a threshold limit for a file. When the recording reaches this limit, Session Recording closes the file and creates an extra file to continue recording. This action is called a rollover.

You can specify two thresholds for a rollover:

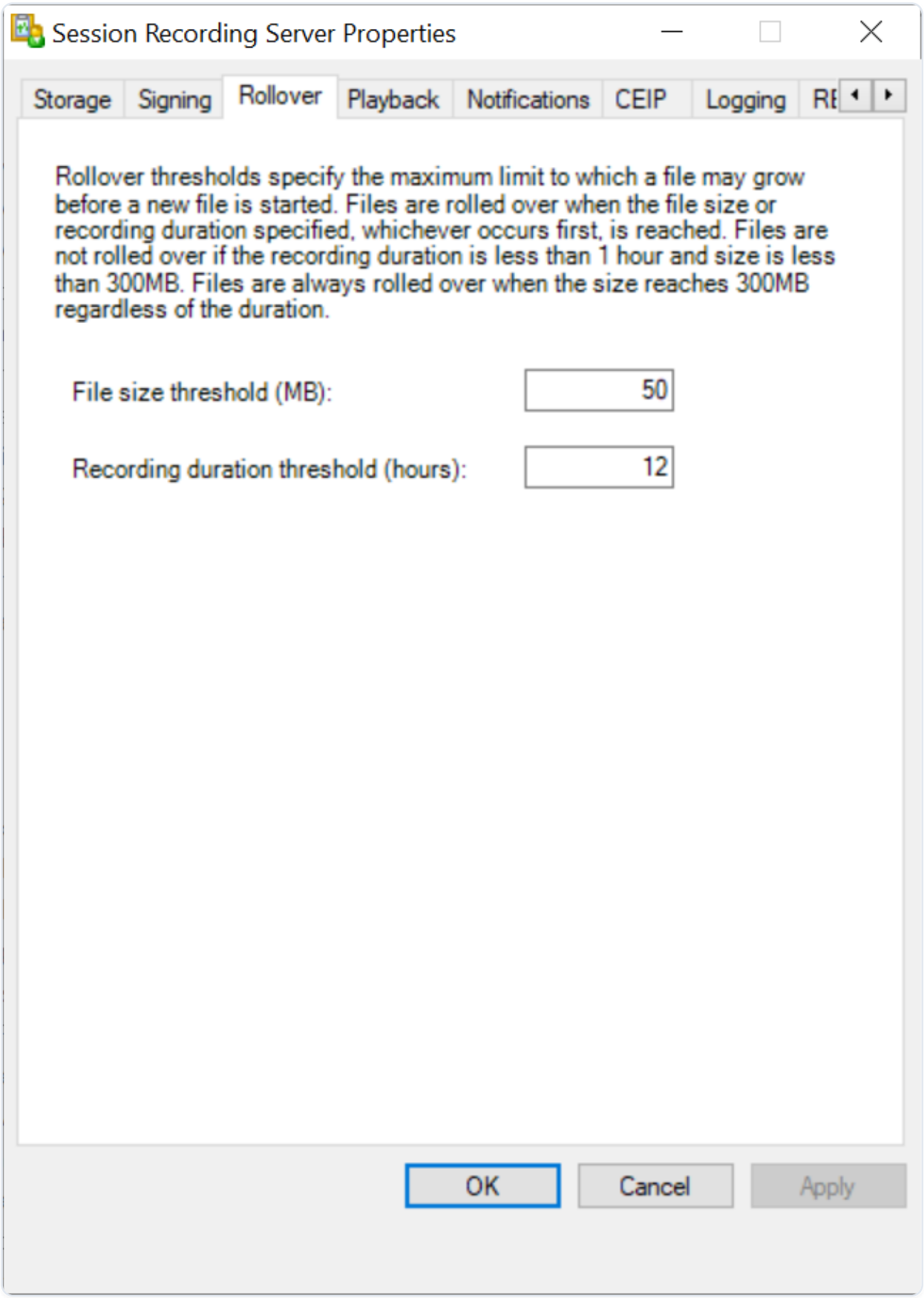
- **File size.** The current file closes when it reaches the size, and a new file opens. By default, the rollover occurs when the size exceeds 50 MB. Supported values: 10-300.
- **Duration.** When the duration is reached, the current file closes and a new file opens. By default, the rollover occurs when the session records for 12 hours. Supported values: 1-24.

Rollovers occur when the first of the two conditions above is met. For example, you specify 17 MB for the size and 6 hours for the duration. When your recording reaches 17 MB in 3 hours, Session Recording closes the file and opens a new one.

To prevent the creation of many small files, Session Recording doesn't roll over until at least one hour elapses regardless of the value specified for the file size. The exception to this rule is if the file size surpasses 300 MB.

Specify the maximum file size for recordings

1. Log on to the machine hosting the Session Recording server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Rollover** tab.



4. Type an integer between 10 and 300 to specify the maximum file size in MB.
5. Type an integer between 1 and 24 to specify the maximum recording duration in hours.

Specify where recordings are stored

Use **Session Recording Server Properties** to specify where recordings are stored and where archived recordings are restored for playback.

You can store recordings on a local drive, a SAN volume, and a location specified by a UNC network path. Starting from Version 2103, you can store recordings in Azure file shares. For more information, see Configure an Azure file share to store recordings later in this article.

Note:

- Storing data on a NAS, based on file-based protocols such as SMB and NFS, might have performance and security implications. Use the latest version of the protocol in place to avoid security implications and perform scale testing to ensure proper performance.
- To archive files or restore deleted files, use the ICLDB command.

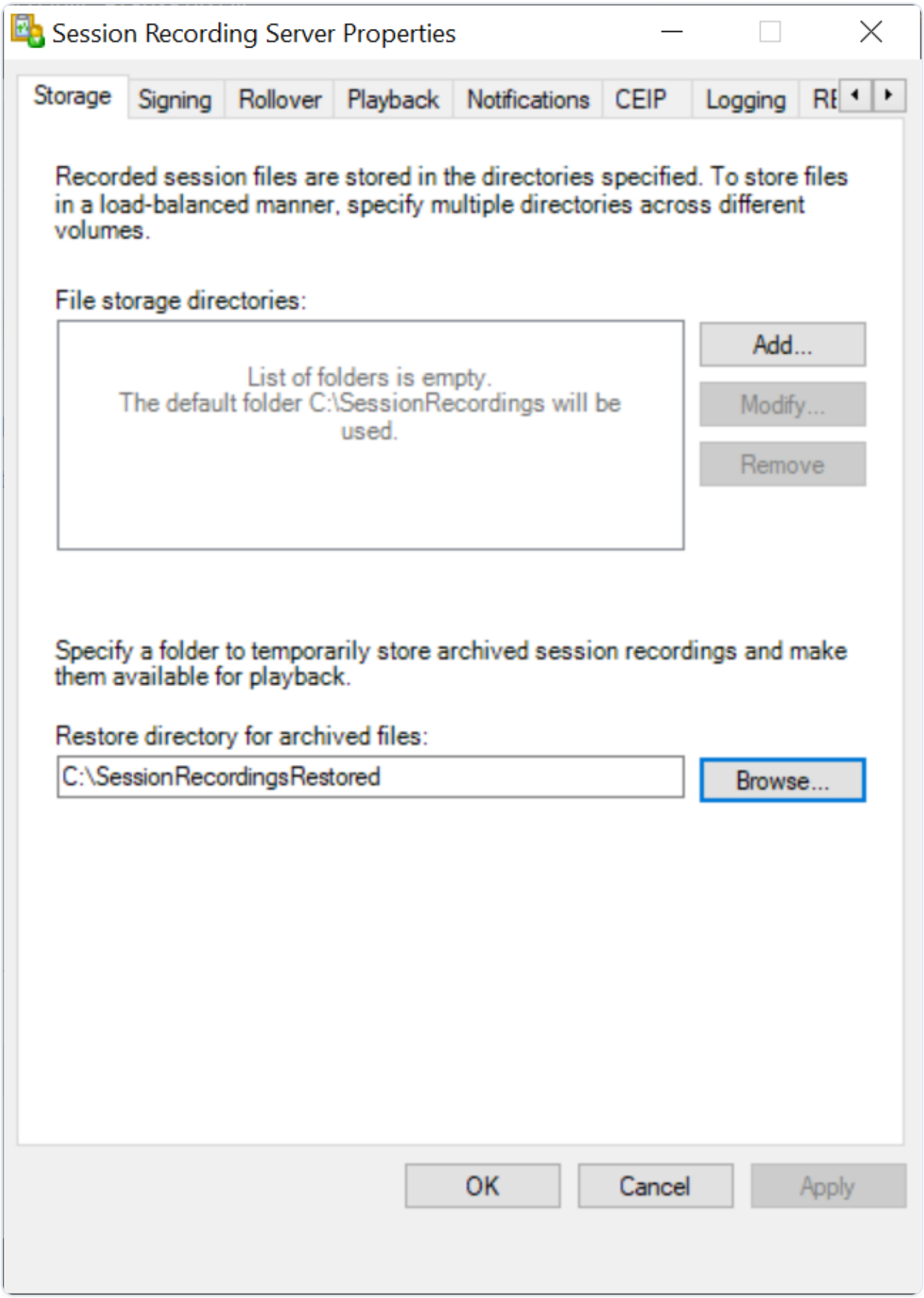
Specify one or more folders for storing recordings and a folder for restoring archived recordings

1. Log on to the machine hosting the Session Recording server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Storage** tab.
4. Use the **File storage directories** list to manage the folders where recordings are stored.

   After you select the folders, Session Recording grants its service with Full Control permission to these folders.

   By default, recordings are stored in the **<drive\>:\SessionRecordings** folder of the machine hosting the Session Recording server. You can change the folder where you store recordings, add extra folders to load-balance across multiple volumes, or make use of more space. Multiple folders in the list indicate that recordings are load-balanced across the folders. Load balancing cycles through the folders.
5. In the **Restore directory for archived files** field, type your folder for restoring archived recordings.

   By default, archived recordings are restored in the **<drive\>:\SessionRecordingsRestore** folder of the machine hosting the Session Recording server. You can change the folder.



Configure an Azure file share to store recordings

To create an Azure file share to store recordings, complete the following steps:

1. In the Azure portal, create a storage account and then create an Azure file share.

   For a quick start guide, see Create and manage Azure file shares with the Azure portal. The following table recommends configurations for your consideration.

RECORDING FILE SIZE MB/ HOUR	SESSION QUANTITY	FILE SHARE TYPE	FILE SHARE QUOTA (TB)	SESSION RECORDING SERVER QUANTITY	SESSION RECORDING SERVER SIZE
< 6.37	< 1,000	HDD Standard (StorageV2)	2	1	Standard D4as_v4
< 6.37	1,000–2,000	SSD Premium	3	1	Standard D4as_v4
< 6.37	2,000–3,000	SSD Premium	5	1	Standard D4as_v4
< 6.37	3,000–4,000	SSD Premium	6	1	Standard D4as_v4
Approx.10	< 1,000	HDD Standard (StorageV2)	3	1	Standard D4as_v4
Approx.10	1,000–2,500	SSD Premium	6	1	Standard D4as_v4
Approx.10	2,500–4,000	SSD Premium	10	2	Standard D4as_v4

   The file share quota is calculated based on eight hours per day, 23 working days per month, and a one-month retention period for each recording file.

2. Add the Azure file share credentials to the host where you installed the Session Recording server.

   a. Start a command prompt as an administrator and change the drive to the **<Session Recording Server installation path\>\Bin** folder.

By default, the Session Recording server is installed in `C:\Program Files\Citrix\SessionRecording\Server`.

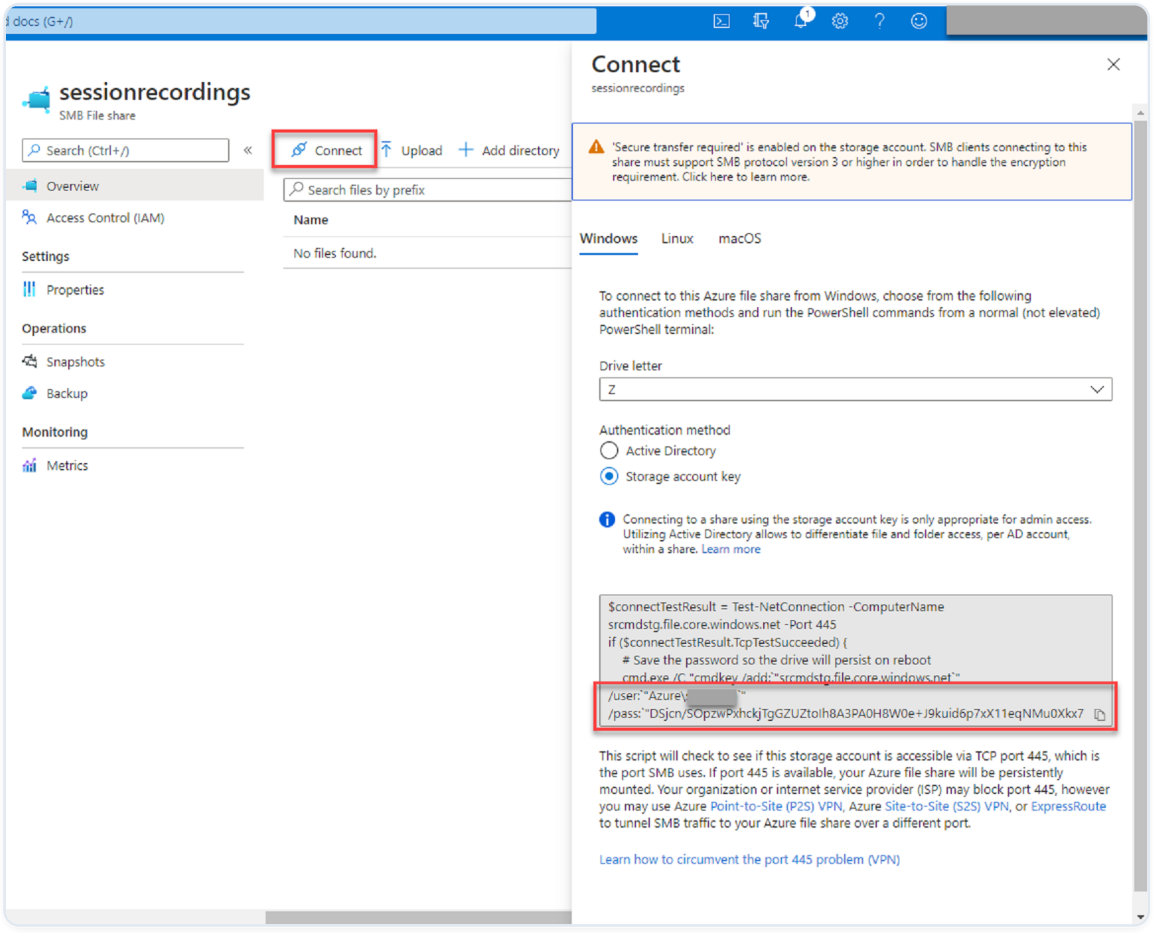
b. Run the **SsRecUtils.exe -AddAzureFiles <storageAccountName\> <fileShareName\> <accesskey\>** command.

Where,

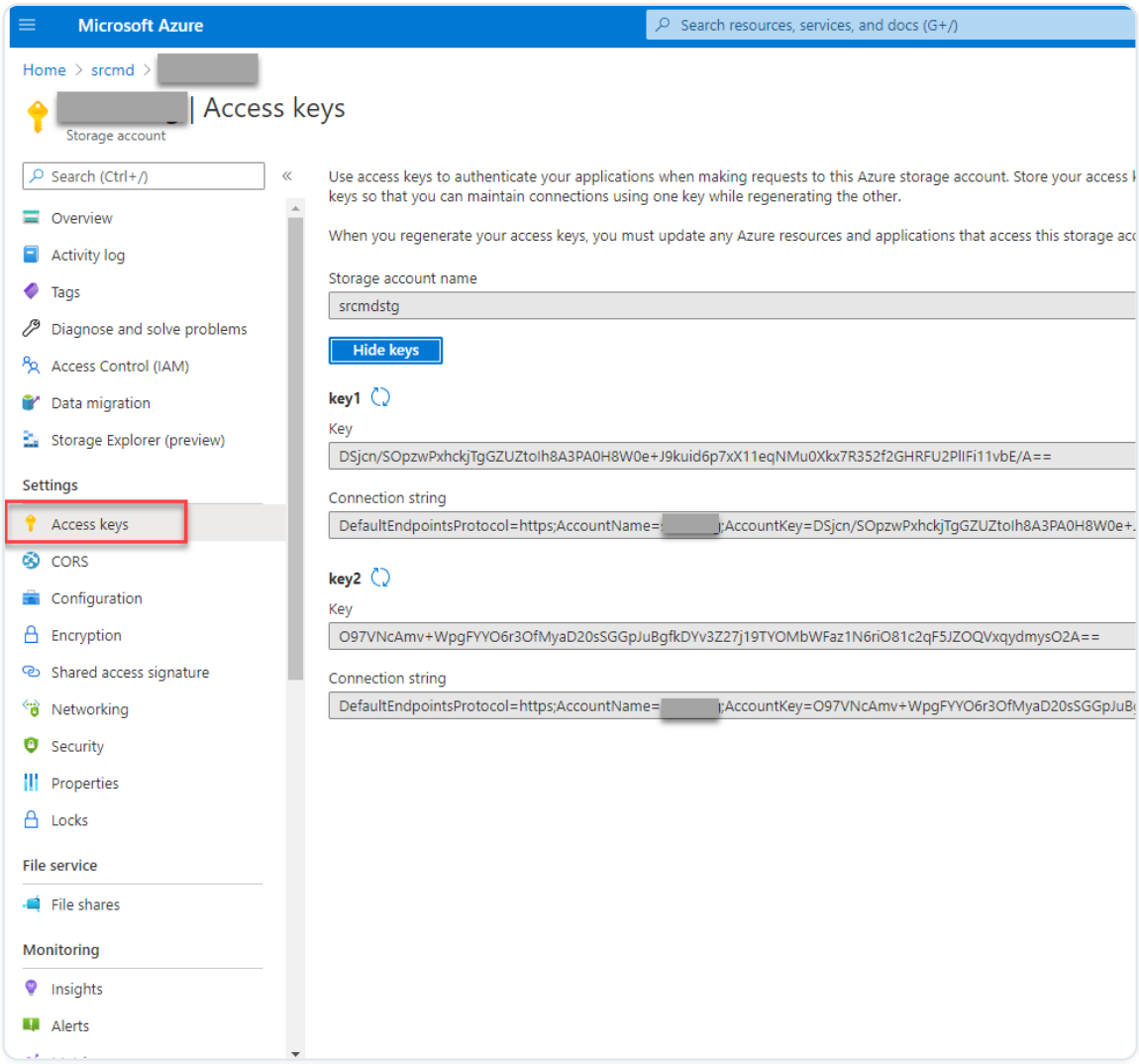
- **<storageaccountname\>** is the name of your storage account in Azure.
- **<filessharename\>** is the name of the file share contained within your storage account.
- **<accesskey\>** is your storage account key that can be used to access the file share.

There are two ways to obtain your storage account key:

- You can obtain your storage account key from the connection string that appears when you click the **Connect** icon in your file share page.



- You can also obtain your storage account key by clicking **Access keys** in the left navigation of your storage account page.



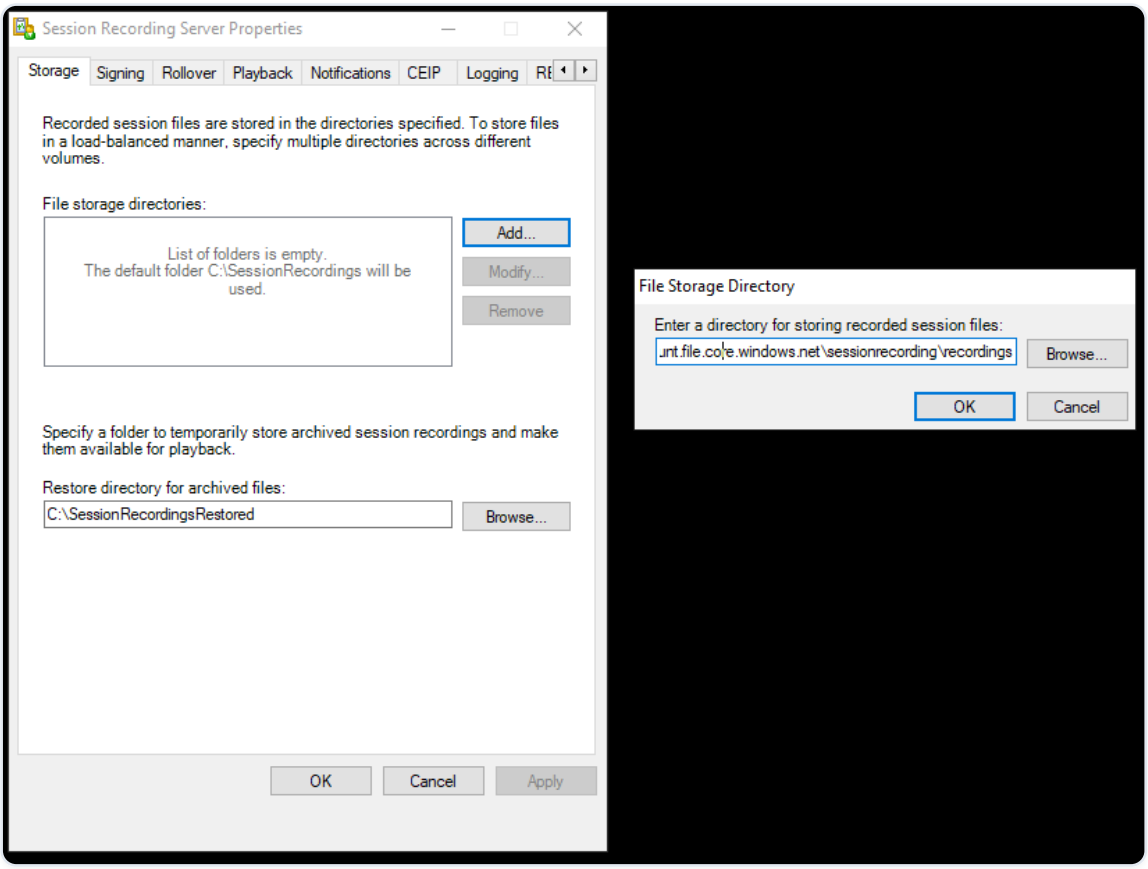
c. Mount the Azure file share to the host where you installed the Session Recording server.

   i. Open **Session Recording Server Properties**.

   ii. Click **Add** on the **Storage** tab.

   iii. Enter the UNC path in the format of **\\\\<storageaccountname\>.file.core.windows.net\\\<filessharename>\\<subfolder\>**.

   Specify a subfolder under the file share to store your recording files. The Session Recording server then automatically creates the subfolder for you.

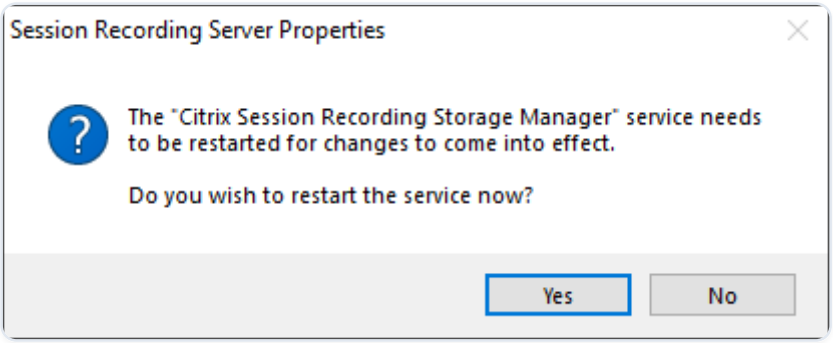


iv. Click **OK** in the **File Storage Directory** dialog box.

v. Click **Apply** in the **Session Recording Server Properties** window.

vi. Click **OK** after **Apply** becomes grayed out.

vii. Click **Yes** when you are prompted to restart the Session Recording Storage Manager service.



Policies

Use the Session Recording Policy Console to create recording policies, event detection policies, event response policies, and recording viewing policies. When creating the policies, you can specify Delivery Controllers from both the Citrix Cloud™ and on-premises environments.

> **Important:**
>
> To use the Session Recording Policy Console, you must have the Broker PowerShell Snap-in (Broker_PowerShellSnapIn_x64.msi) or the Citrix DaaS Remote PowerShell SDK (CitrixPoshSdk.exe) installed manually. Locate the Broker PowerShell snap-in on the Citrix Virtual Apps and Desktops ISO (`\x64\Citrix Desktop Delivery Controller`). Or, download the Citrix DaaS Remote PowerShell SDK from the Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) download page.

> **Tip:**
>
> You can edit the registry to prevent recording file losses in case that your Session Recording server might fail unexpectedly. Log on as an administrator to the machine where you installed the Session Recording Agent, open the Registry Editor, and add a DWORD value `DefaultRecordActionOnError` = `1` under `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent`.

Activate a policy

1. Log on as an administrator to the machine where you installed the Session Recording Policy Console.
2. Start the Session Recording Policy Console.
3. If the **Connect to Session Recording Server** window appears, ensure that the name of the Session Recording server, protocol, and port are correct. Click **OK**.
4. In the Session Recording Policy Console, expand the target policy type.
5. Select the policy to activate.
6. From the menu bar, choose **Activate Policy**.

Modify a policy

1. Log on as an administrator to the machine where you installed the Session Recording Policy Console.
2. Start the Session Recording Policy Console.
3. If the **Connect to Session Recording Server** window appears, ensure that the name of the Session Recording server, protocol, and port are correct. Click **OK**.

4. In the Session Recording Policy Console, expand the target policy type.
5. Select the policy that you want to modify. The rules for the policy appear in the right pane.
6. To add, modify, or delete a rule:
    - From the menu bar, choose **Add New Rule**. If the policy is active, a pop-up window appears requesting confirmation of the action. Use the **Rules** wizard to create a rule.
    - Select the rule that you want to modify, right-click, and choose **Properties**. Use the **Rules** wizard to modify the rule.
    - Select the rule that you want to delete, right-click, and choose **Delete Rule**.

Delete a policy

> **Note:**
>
> You cannot delete a system-defined policy or a policy that is active.

1. Log on as an administrator to the machine where you installed the Session Recording Policy Console.
2. Start the Session Recording Policy Console.
3. If the **Connect to Session Recording Server** window appears, ensure that the name of the Session Recording server, protocol, and port are correct. Click **OK**.
4. In the Session Recording Policy Console, expand the target policy type.
5. In the left pane, select the policy to delete. If the policy is active, you must activate another policy.
6. From the menu bar, choose **Delete Policy**.
7. Select **Yes** to confirm the action.

Configure session recording policies

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

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

System-defined recording policies

Session Recording provides the following system-defined recording policies:

- **Do not record**. The default policy. If you do not specify another policy, no sessions are recorded.
- **Record only events (for everyone, with notification)**. This policy records only events that your event detection policy specifies. It does not record screens. Users receive recording notifications in advance.
- **Record only events (for everyone, without notification)**. This policy records only events that your event detection policy specifies. It does not record screens. Users do not receive recording notifications.
- **Record entire sessions (for everyone, with notification)**. This policy records entire sessions (screens and events). Users receive recording notifications in advance.
- **Record entire sessions (for everyone, without notification)**. This policy records entire sessions (screens and events). Users do not receive recording notifications.

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

Create a custom recording policy

You can record sessions of specified users or groups, published applications or desktops, delivery groups or VDA machines, and Citrix Workspace™ app client IP addresses. A wizard within the Session Recording policy console helps you create rules. To obtain the lists of published applications or desktops and delivery groups or VDA machines, you must have the read permission as a site administrator. Configure the administrator read permission on the Delivery Controller™ of the site.

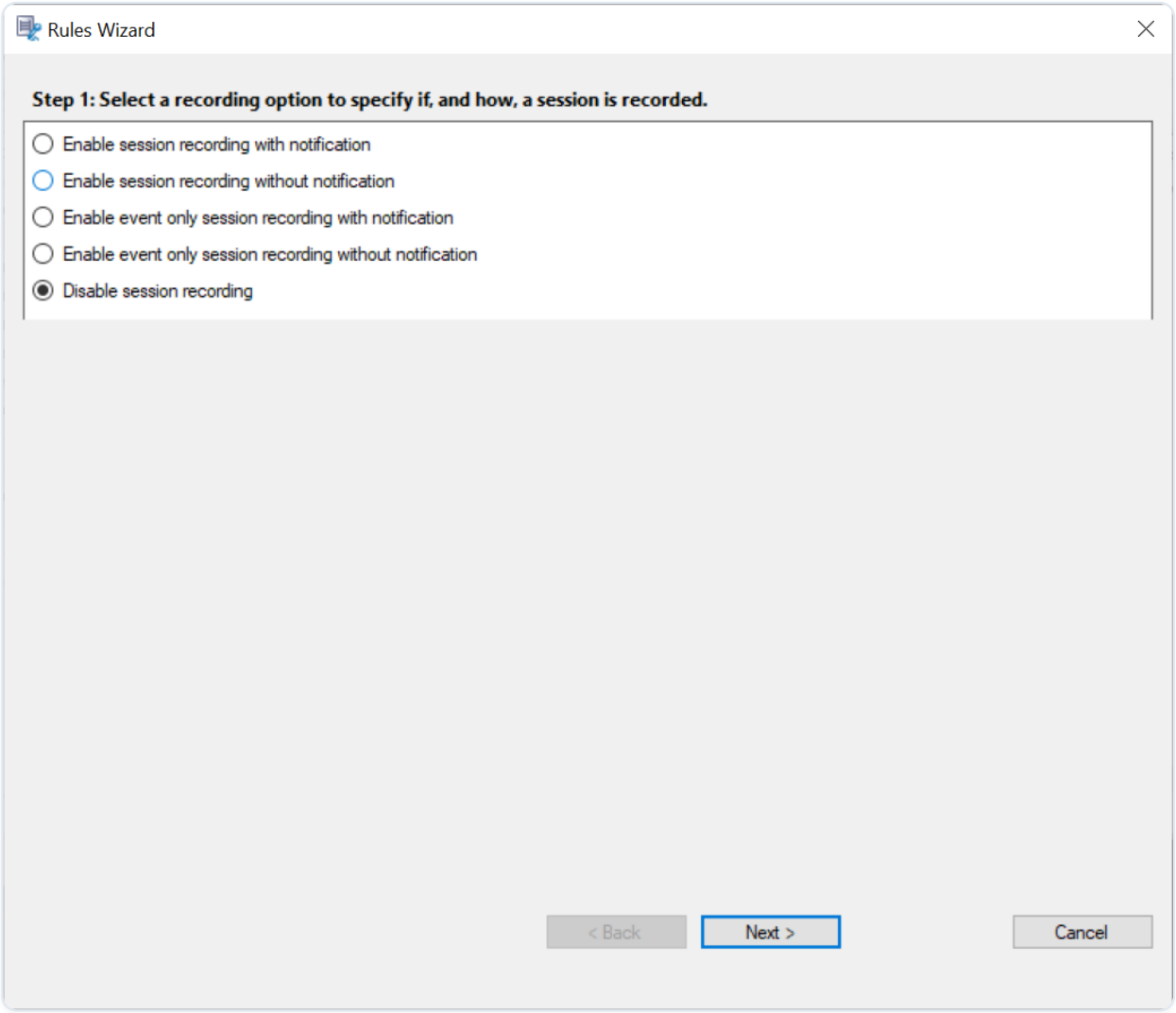
For each rule you create, you specify a recording action and rule criteria. The recording action applies to sessions that meet the rule criteria.

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.
- **Enable session recording without notification**. This option records entire sessions (screens and events). Users do not receive recording notifications.
- **Enable event only session recording with notification**. Recording only specific events helps to free up storage space. This option records throughout sessions only events that your event

detection policy specifies. It does not record screens. Users receive recording notifications in advance.

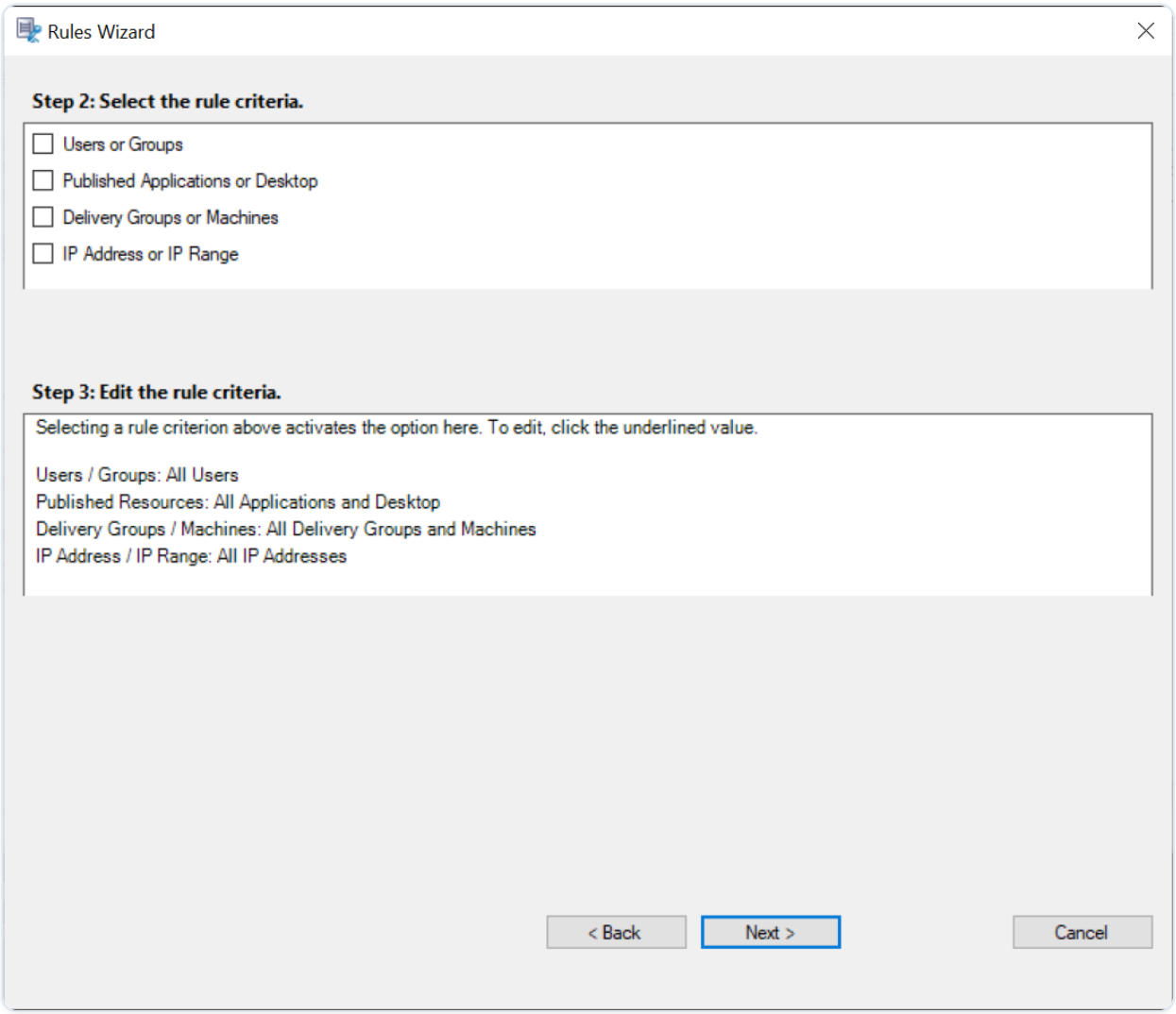
- **Enable event only session recording without notification**. Recording only specific events helps to free up storage space. This option records throughout sessions only events that your event detection policy specifies. It does not record screens. Users do not receive recording notifications.
- **Disable session recording**. This option means that no sessions are recorded.



For each rule, choose at least one of the following items to create the rule criteria:

- **Users or Groups**. Creates a list of users or groups to which the action of the rule applies. Session Recording allows you to use Active Directory groups and white list users.
- **Published Applications or Desktop**. Creates a list of published applications or desktops to which the action of the rule applies. In the **Rules** wizard, choose the Citrix Virtual Apps and Desktops™ or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) sites on which the applications or desktops are available.

- **Delivery Groups or Machines**. Creates a list of Delivery Groups or machines to which the action of the rule applies. In the **Rules** wizard, choose the location of the Delivery Groups or machines.
- **IP Address or IP Range**. Creates a list of IP addresses or ranges of IP addresses to which the action of the rule applies. On the **Select IP Address and IP Range** screen, add a valid IP address or IP range for which recording is enabled or disabled. The IP addresses mentioned here are the IP addresses of the Citrix Workspace apps.



Note:

The Session Recording policy console supports configuring multiple criteria within a single rule. 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 between items within a criterion, and the "AND" operator is used between separate criteria. 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.

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

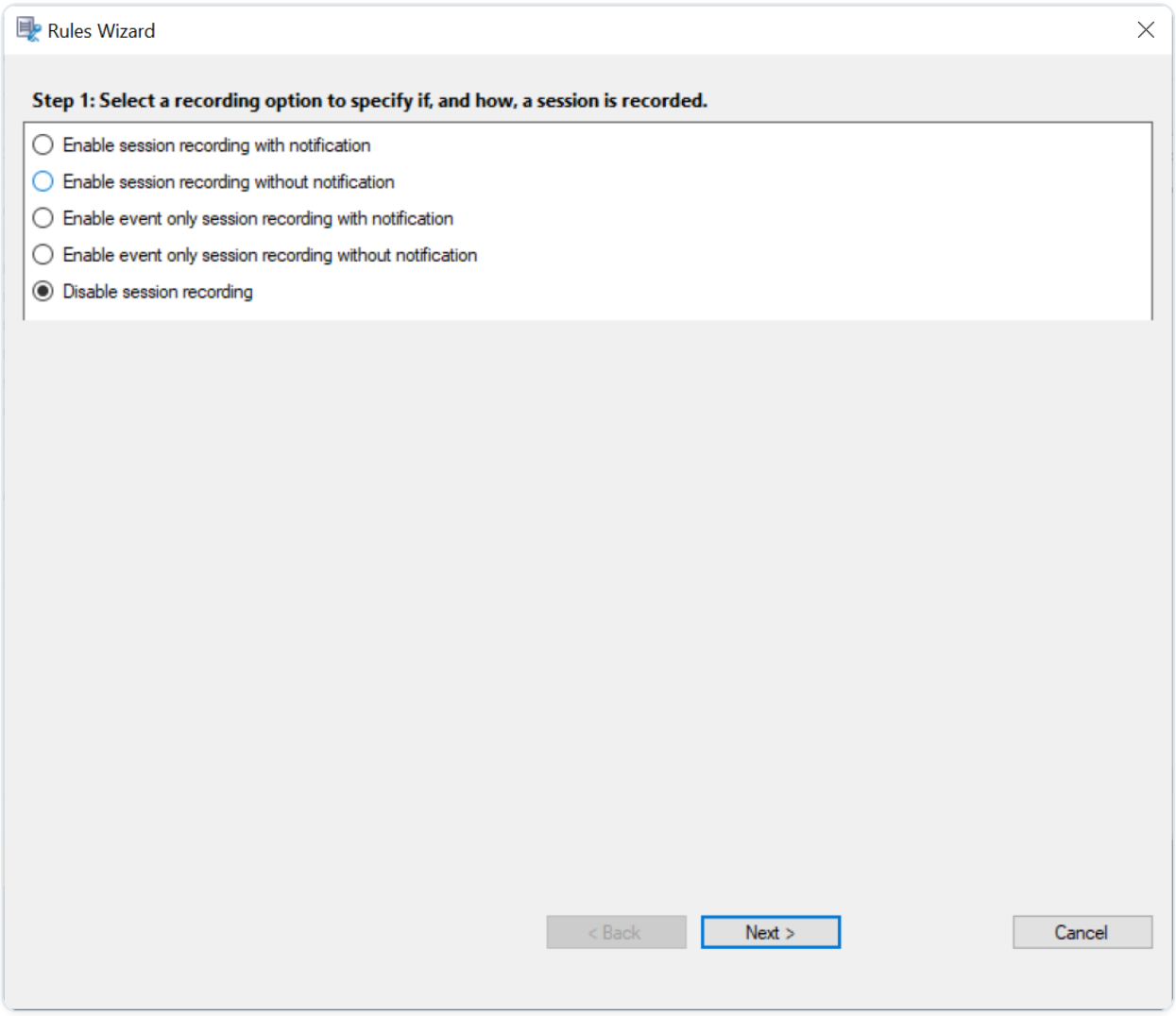
The recording action of a rule determines its priority:

- Rules with the **Do not record** action have the highest priority.
- Rules with the **Record with notification** action have the second-to-highest priority.
- Rules with the **Record without notification** action have the second-to-lowest priority.
- Rules with the **Enable event only session recording with notification** action have the medium priority.
- Rules with the **Enable event only session recording without notification** action have the lowest priority.

Some sessions might not meet any rule criteria in a recording policy. For these sessions, the action of the policy fallback rule applies. The action of the fallback rule is always **Do not record**. You cannot modify or delete the fallback rule.

To create a custom recording policy:

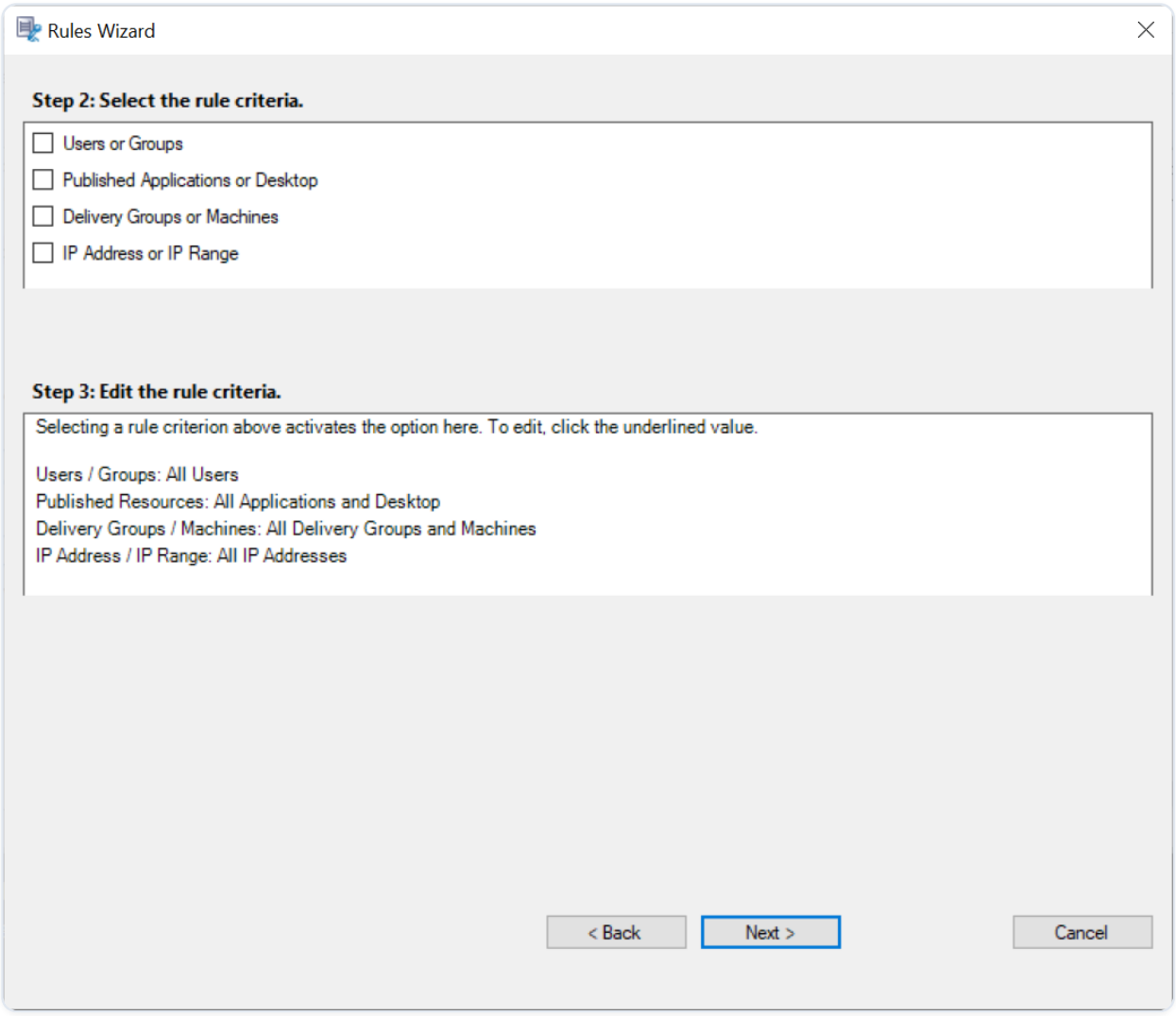
1. Log on as an authorized Policy Administrator to the server where the Session Recording policy console is installed.
2. Start the Session Recording policy console and select **Recording Policies** in the left pane. From the menu bar, choose **Add New Policy**.
3. Right-click the **New policy** and select **Add Rule**.
4. In the rules wizard, select a recording option and then click **Next**.



5. Select the rule criteria - You can choose one or more rule criteria:

   Users or Groups Published Applications or Desktop

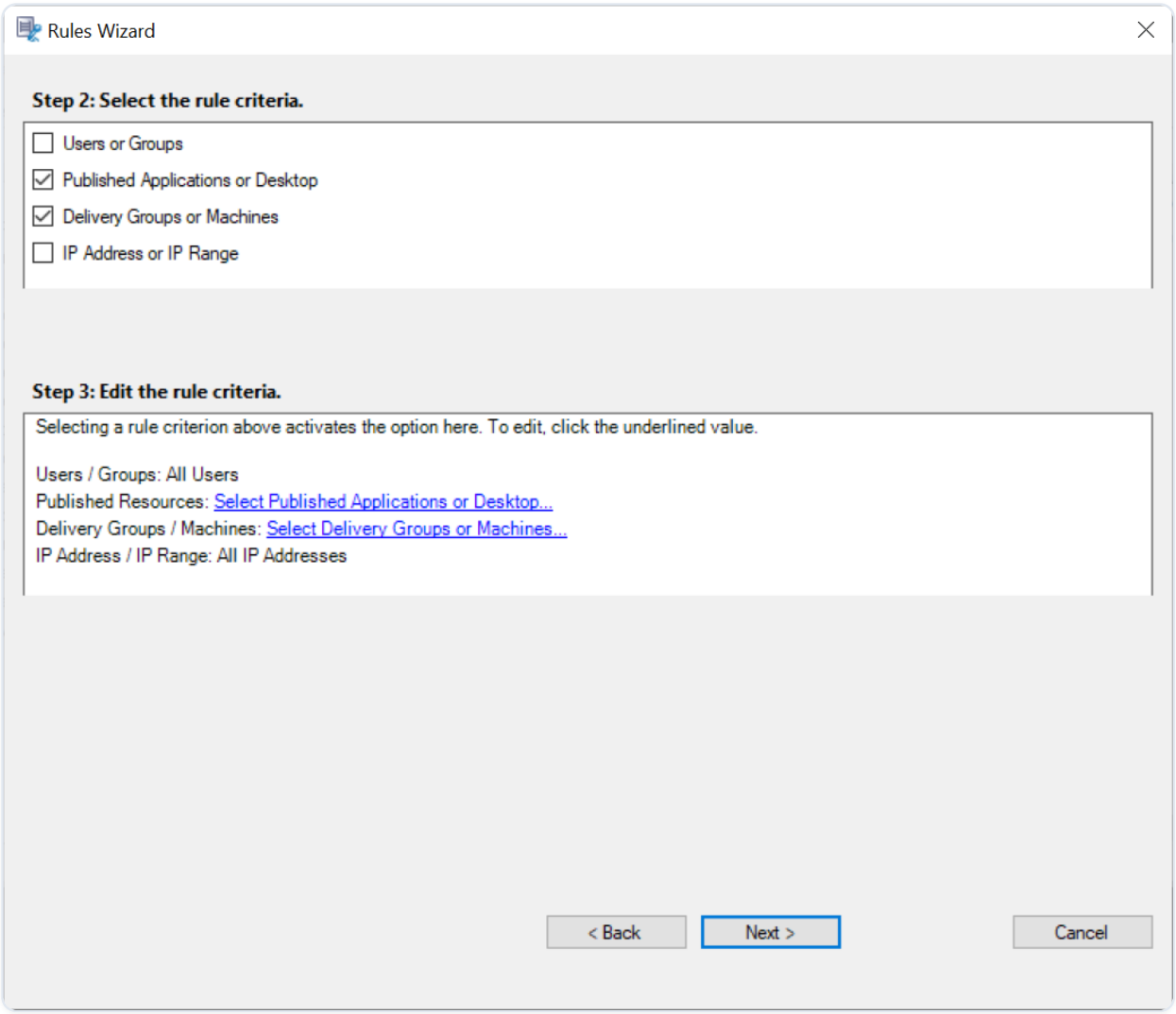
   Delivery Groups or Machines IP Address or IP Range



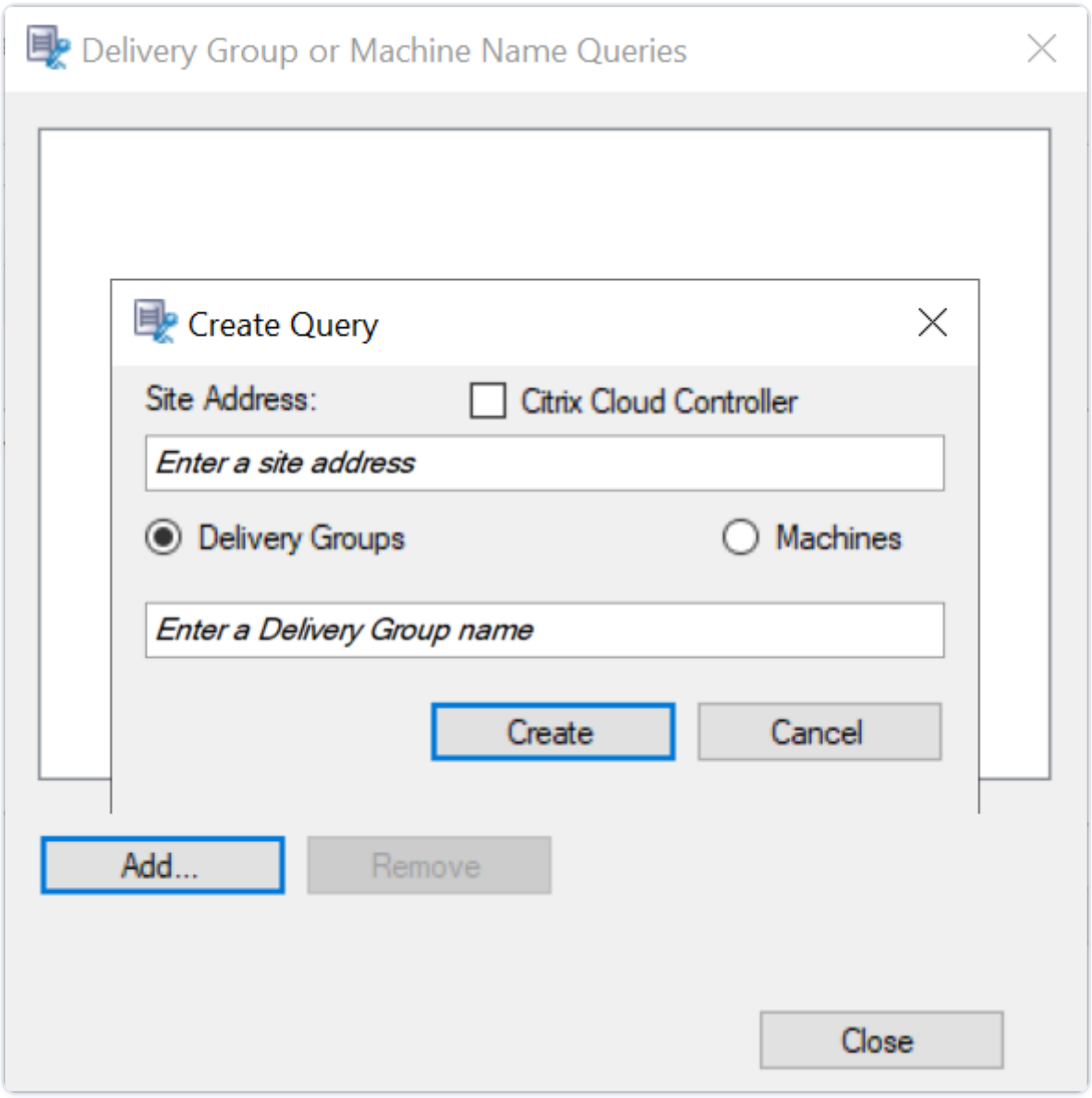
6. Edit the rule criteria - To edit, click the underlined values. The values are underlined based on the criteria that you chose in the previous step.

> **Note:**
>
> If you choose the **Published Applications or Desktop** underlined value, the **Site Address** is the IP address, a URL, or a machine name if the Controller is on a local network. The **Name of Application** list shows the display name.
>
> When choosing **Published Applications or Desktop** or **Delivery Groups or Machines**, specify the Delivery Controller for your Session Recording policy console to communicate with.

The Session Recording policy console is the only channel to communicate with Delivery Controllers from the Citrix Cloud™ and on-premises environments.



For example, when choosing **Delivery Groups or Machines**, click the corresponding hyperlink in Step 3 of the preceding screenshot and click **Add** to add queries to the Controller.



For a description of use cases that cover the on-premises and the Citrix Cloud Delivery Controllers, see the following table:

USE CASE	ACTION REQUIRED
On-Premises Delivery Controller	1. Install Broker_PowerShellSnapIn_x64.msi. 2. Clear the **Citrix Cloud Controller** check box.
Citrix Cloud Delivery Controller	1. Install the Citrix DaaS™ Remote PowerShell SDK. 2. Validate the Citrix Cloud account credentials. 3. Select the **Citrix Cloud Controller** check box.

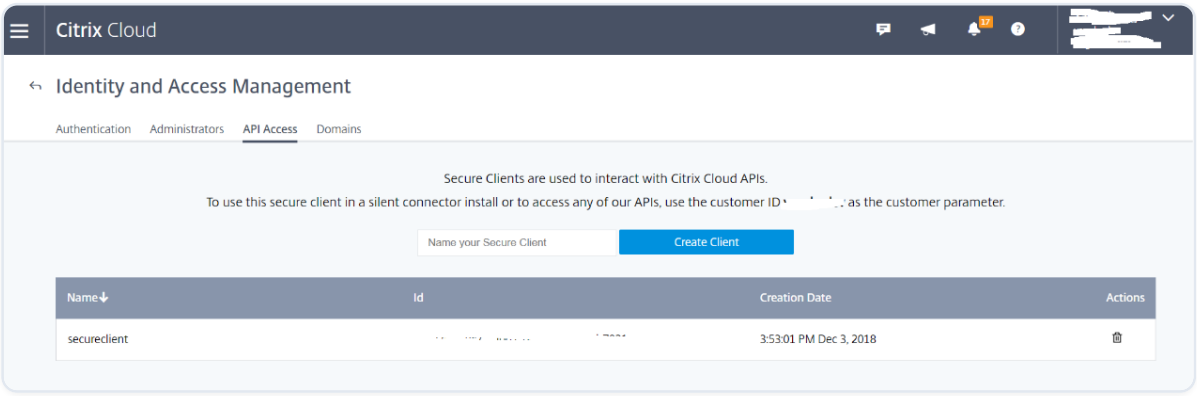
USE CASE	ACTION REQUIRED
Switch from an on-premises Delivery Controller to a Citrix Cloud Delivery Controller	1. Uninstall Broker_PowerShellSnapIn_x64.msi and restart the machine. 2. Install the Citrix DaaS Remote PowerShell SDK. 3. Validate the Citrix Cloud account credentials. 4. Select the **Citrix Cloud Controller** check box.
Switch from a Citrix Cloud Delivery Controller to an on-premises Delivery Controller	1. Uninstall the Citrix DaaS Remote PowerShell SDK and restart the machine. 2. Install Broker_PowerShellSnapIn_x64.msi. 3. Clear the **Citrix Cloud Controller** check box.

Validating the Citrix Cloud credentials

To query Delivery Controllers hosted in the Citrix Cloud, manually validate your Citrix Cloud credentials on the machine where the Session Recording policy console is installed. Failure to comply can cause an error and your Session Recording policy console might not work as expected.

To do the manual validation:

a. Log on to the Citrix Cloud console and locate **Identity and Access Management** > **API Access**. Create an API access Secure Client for obtaining an authentication profile that can bypass the Citrix Cloud authentication prompts. Download your Secure Client, rename, and save it in a safe location. The file name is defaulted to secureclient.csv.



b. Open a PowerShell session and run the following command to have the authentication profile (obtained in the preceding step) take effect.

```
asnp citrix.*

Set-XDCredentials -CustomerId "citrixdemo" -SecureClientFile "c:
\temp\secureclient.csv" -ProfileType CloudAPI –StoreAs "default"
```

Set **CustomerId** and **SecureClientFile** as required. The preceding command creates a default authentication profile for the customer `citrixdemo` to bypass authentication prompts in the current and all subsequent PowerShell sessions.

7. Follow the wizard to finish the configuration.

Note: Limitation regarding prelaunched application sessions:

- If the active policy tries to match an application name, it can't match applications that are opened in a prelaunched session. As a result, the prelaunched session can't be recorded.
- If the active policy records every application and session prelaunch is enabled, a recording notification appears when a user logs on to Citrix Workspace app for Windows. The prelaunched (empty) session and any applications to be launched in that session going forward are recorded.

As a workaround, publish applications in separate Delivery Groups according to their recording policies. Do not use an application name as a recording condition. This approach ensures that prelaunched sessions can be recorded. However, notifications still appear.

Use Active Directory groups

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

White list users

You can create Session Recording policies ensuring that the sessions of some users in your organization are never recorded. This case is called *white listing* these users. White listing is useful

for users who handle privacy-related information or when your organization does not want to record the sessions of a certain class of employees.

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

Configure Director to use the Session Recording server

You can use the Director console to create and activate the recording policies.

1. For an HTTPS connection, install the certificate to trust the Session Recording server in the Trusted Root Certificates of the Director server.
2. To configure the Director server to use the Session Recording server, run the `C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording` command.
3. Type the IP address or FQDN of the Session Recording server and the port number and connection type (HTTP/HTTPS) that the Session Recording agent uses to connect to the Session Recording Broker on the Director server.

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.

IF THE PREVIOUS RECORDING POLICY WAS	AND THE NEW RECORDING POLICY IS	AFTER A ROLLOVER, THE RECORDING POLICY WILL BE
Record without notification	Do not record	Recording stops.
Record without notification	Record with notification	Recording continues and a notification message appears.
Record with notification	Do not record	Recording stops.
Record with notification	Record without notification	Recording continues. No message appears the next time a user logs on.

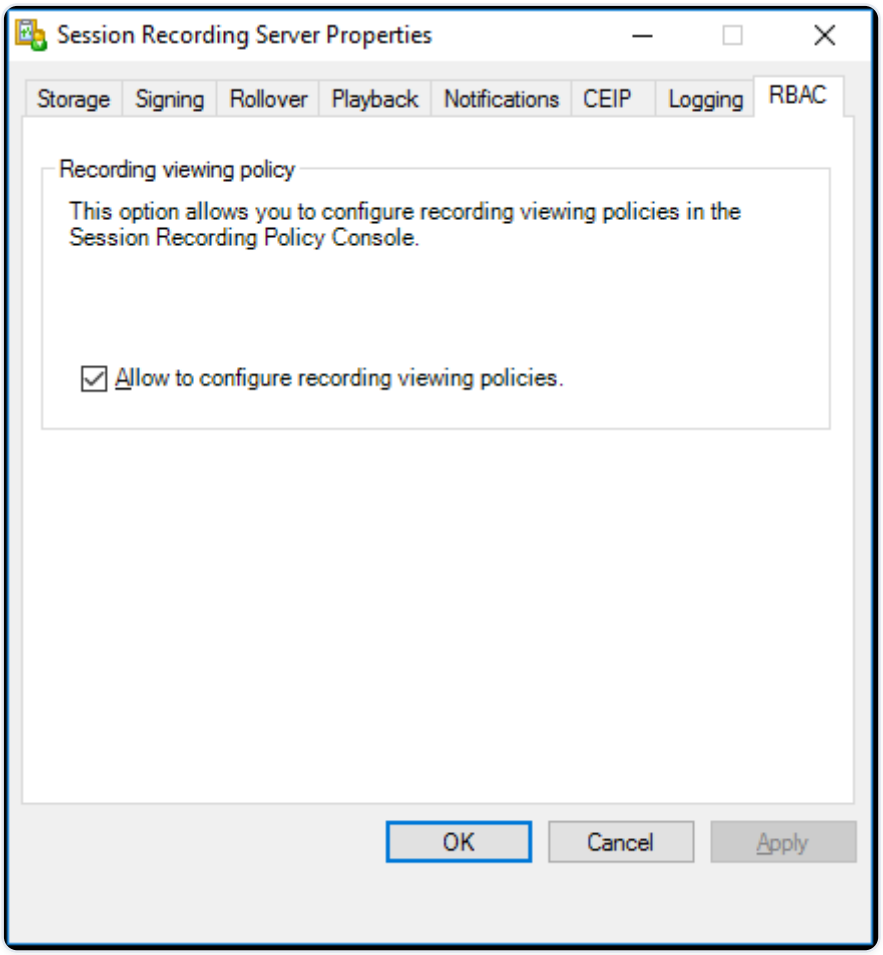
Configure recording viewing policies

Session Recording supports role-based access control. You can create recording viewing policies in the Session Recording policy console and add multiple rules to each policy. Each rule helps you select a user or user group as the recording viewer and set whose recordings are visible to the viewer.

Create a custom recording viewing policy

Before you can create recording viewing policies, enable the feature as follows:

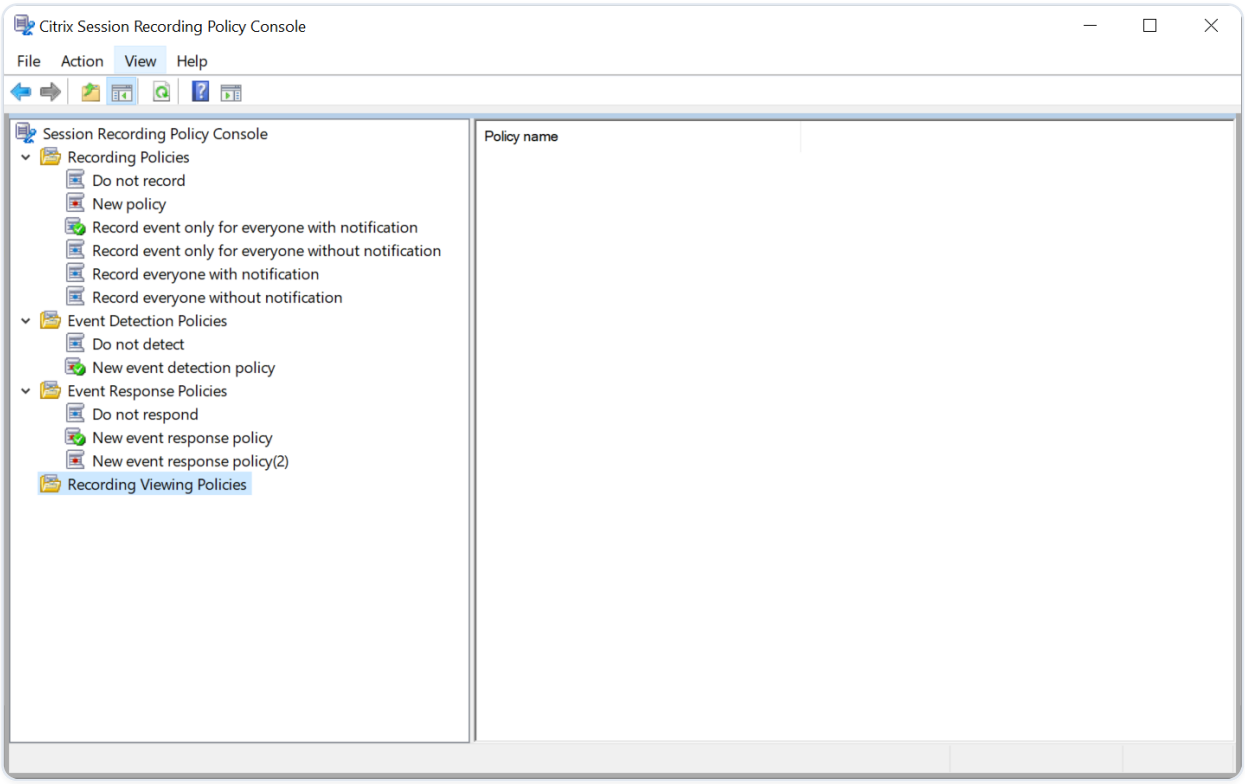
1. Log on to the machine hosting the Session Recording server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **RBAC** tab.
4. Select the **Allow to configure recording viewing policies** check box.



To create a custom recording viewing policy:

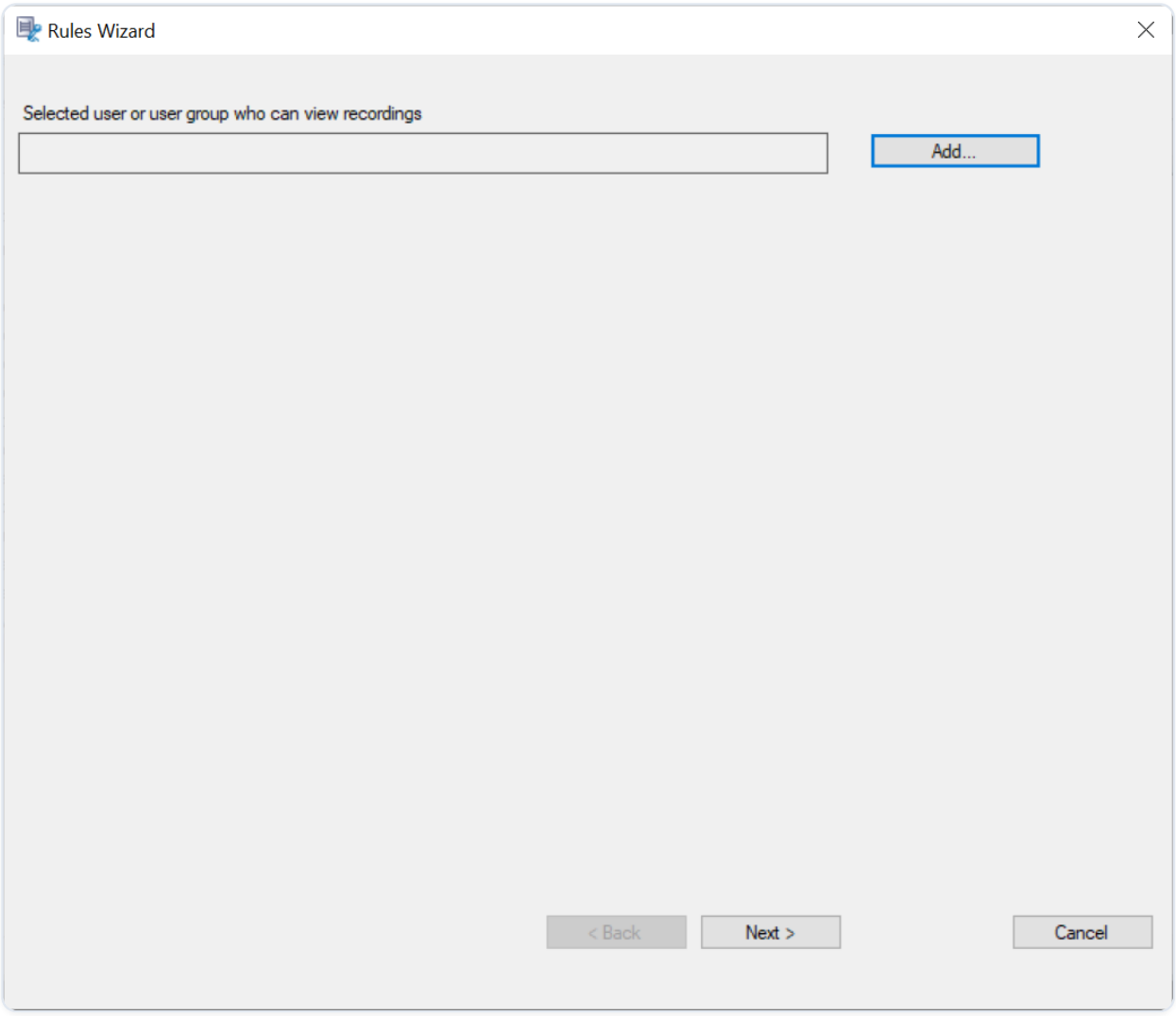
Note: Different from recording policies and event detection policies, a recording viewing policy (including all rules added within) is active immediately when it is created. You do not have to activate it.

1. Log on as an authorized Policy Administrator to the server where the Session Recording policy console is installed.
2. Start the Session Recording policy console. By default, there is no recording viewing policy.



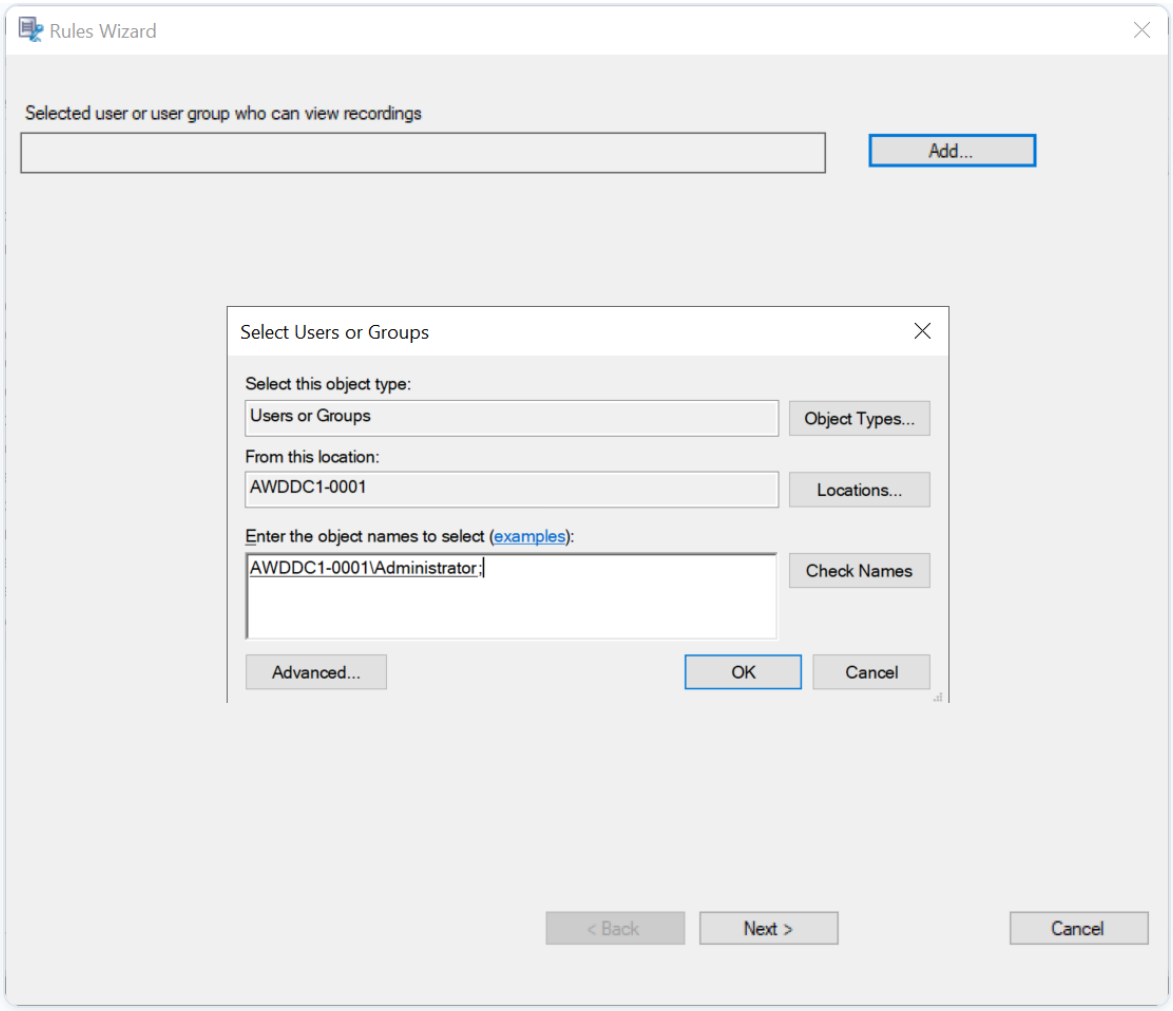
Note: To make **Recording Viewing Policies** available, enable the feature in **Session Recording Server Properties** first.

3. Select **Recording Viewing Policies** in the left pane. From the menu bar, choose **Add New Policy** to create a recording viewing policy.
4. (Optional) Right-click the new policy and rename it.
5. Right-click the new policy and select **Add rule**.



6. Click **Add**.
7. In the **Select Users or Groups** dialog, select a user or user group as the recording viewer.

> **Note:**
>
> A viewer must be assigned the Player role to view recorded sessions. For more information, see Authorize users.



Note:

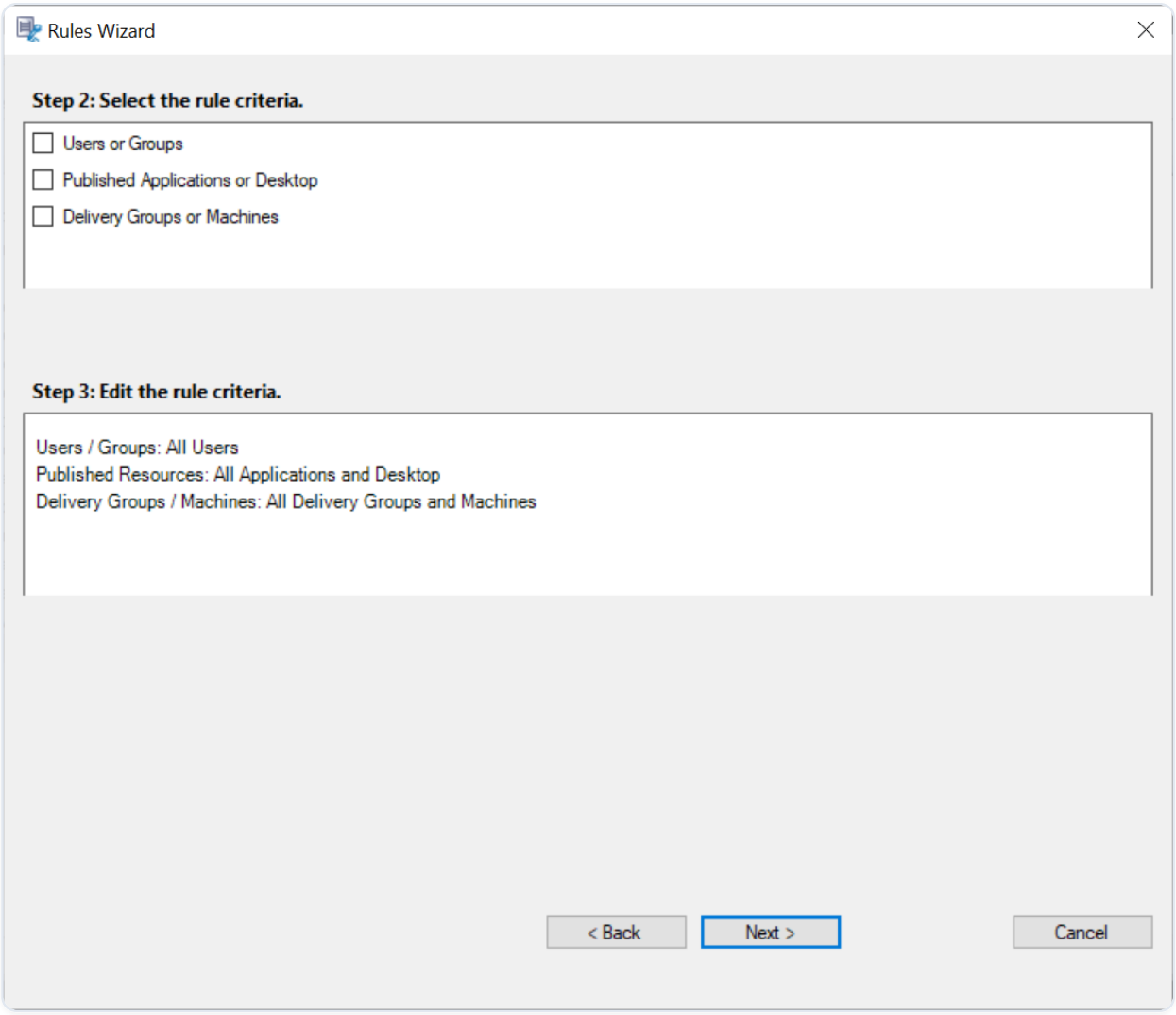
In each rule, you can select only one user or user group as the recording viewer. If you select multiple users or user groups, only your most recent selection takes effect and appears in the text box.

\>When you specify a recording viewer, ensure that you have assigned the viewer to the Player role. A user without the permission to play recorded sessions receives an error message when trying to play a recorded session. For more information, see Authorize users.

8. Click **OK** and then **Next**. The dialog for setting rule criteria appears.
9. Select and edit the rule criteria to specify whose recordings are visible to the viewer you specified earlier:

   - **Users or Groups**

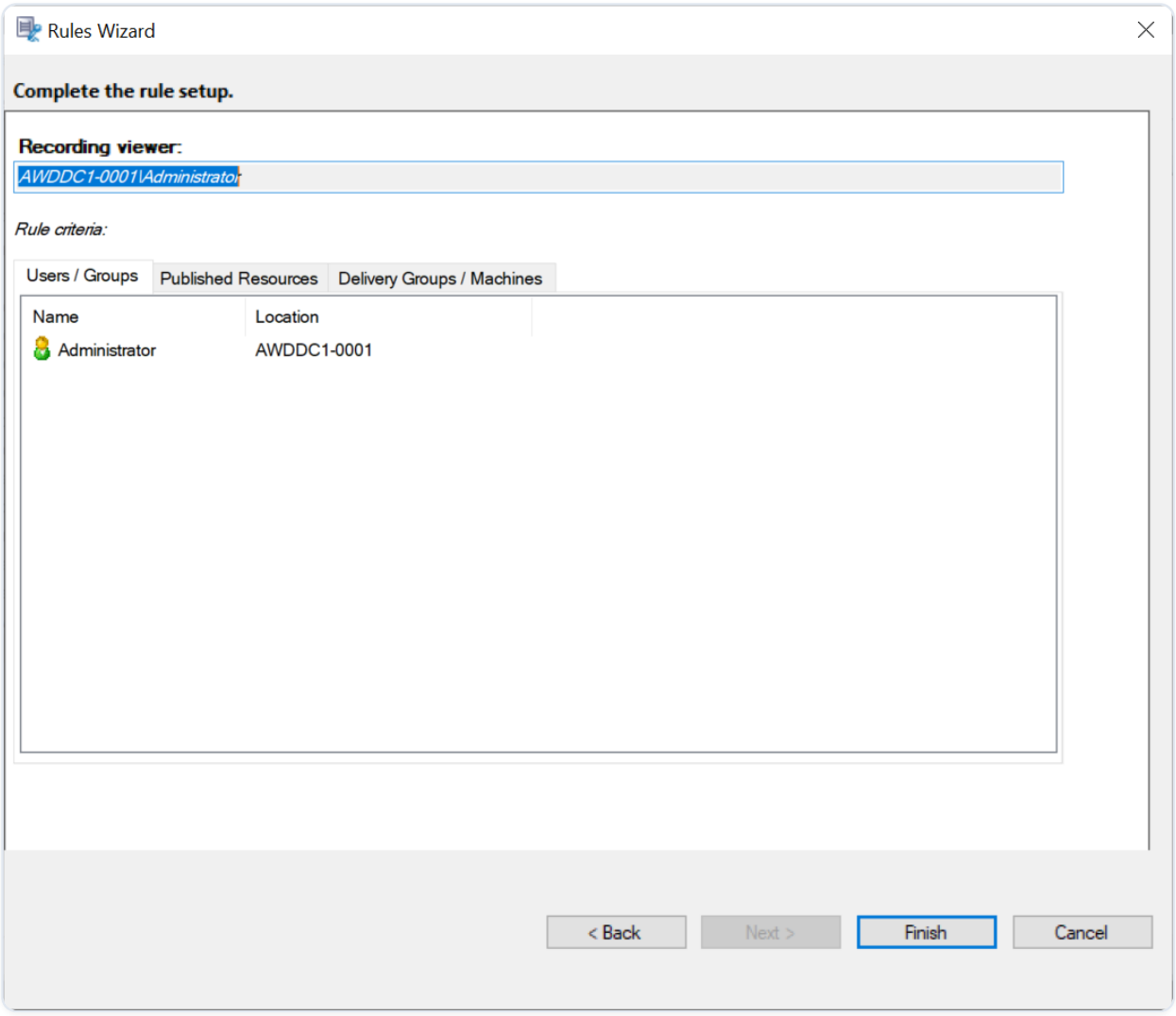
- **Published Applications or Desktop**
- **Delivery Groups or Machines**



> **Note:**
>
> The “OR” logical operator is used both between items within a rule criterion and between separate rule criteria.
>
> If you leave the rule criteria unspecified, the viewer specified earlier has no recordings to view.

10. Follow the wizard to complete the configuration.

    For example:



Configure event detection policies

Session Recording supports centralized configuration of event detection policies. You can create policies in the Session Recording policy console to log various events.

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

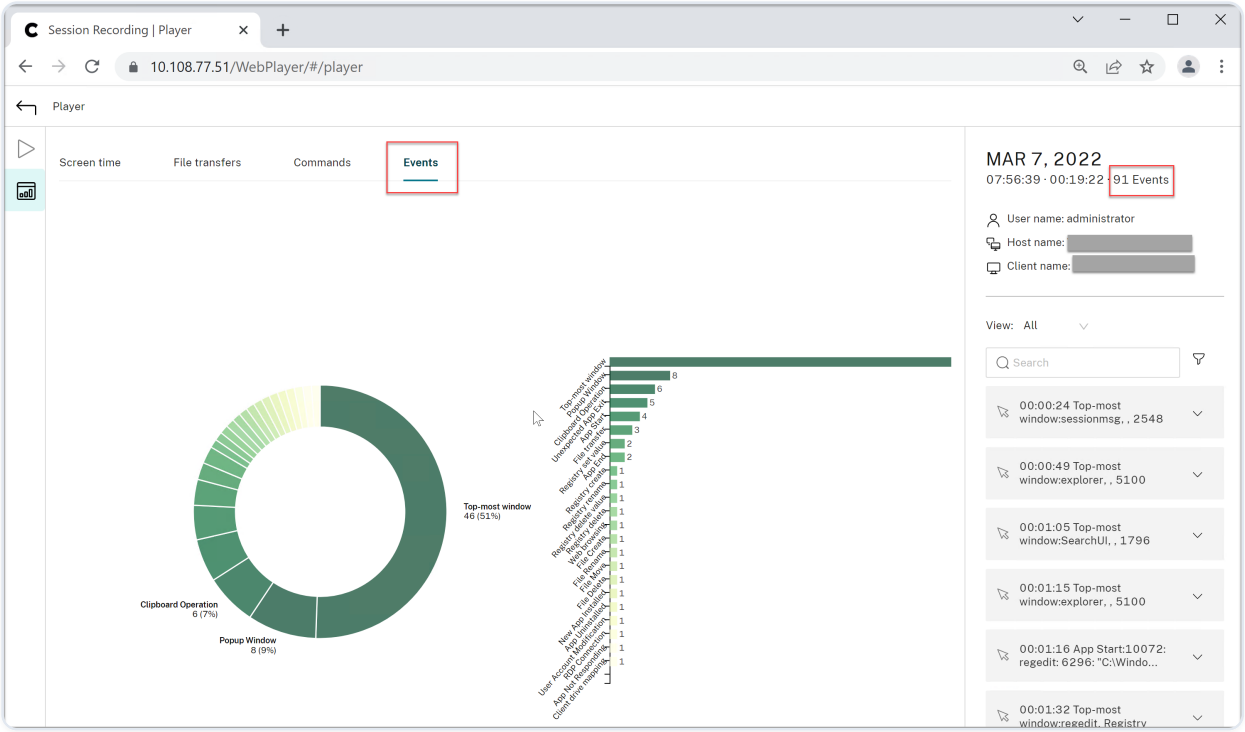
Session Recording can detect and log the following system-defined events that occur during recorded sessions:

- Insertion of USB mass storage devices
- Application starts and ends

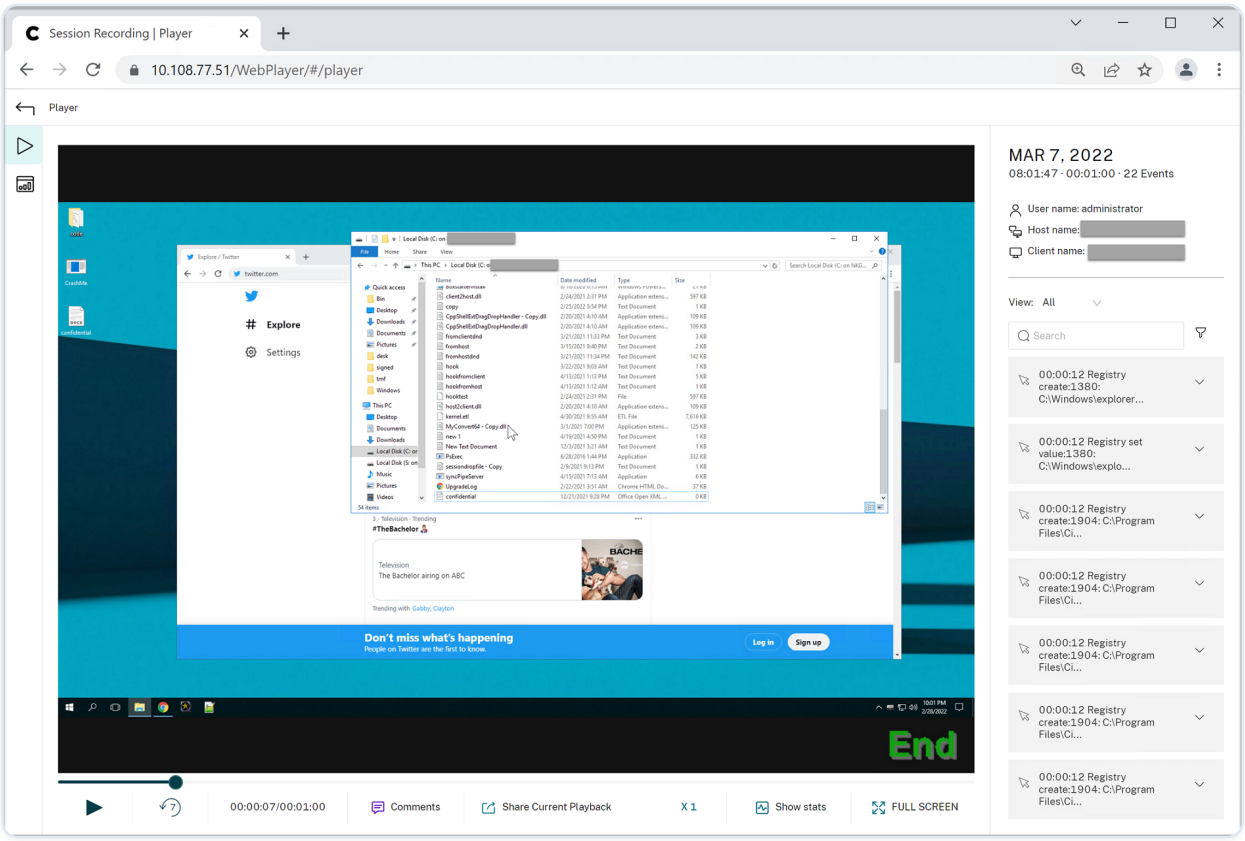
- App failures
- App installs and uninstalls
- File renaming, creation, deletion, and moving operations within sessions
- File transfers between session hosts (VDAs) and client devices (including mapped client drives and generic redirected mass storage devices)
- Web browsing activities
- Topmost window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

For example:

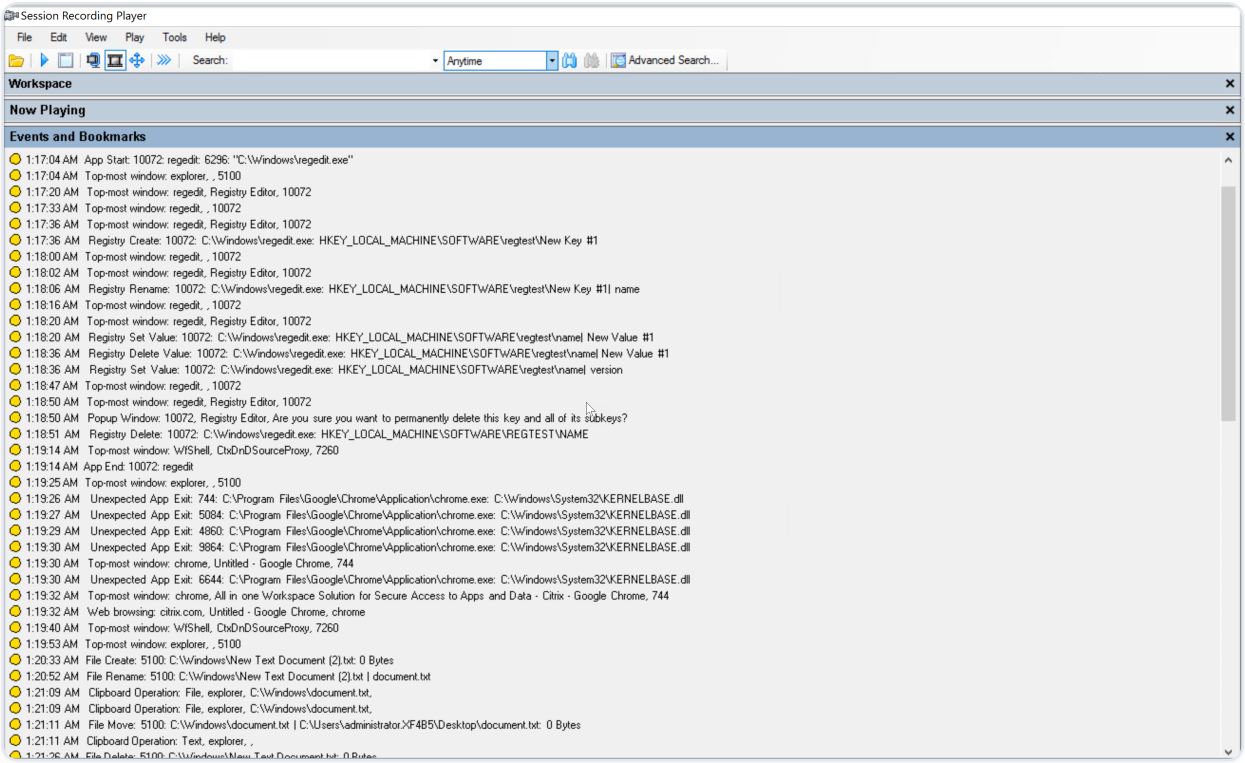
- Events in an event-only recording in the web player:



- Events in a screen recording in the web player:



- Events in the Session Recording player:



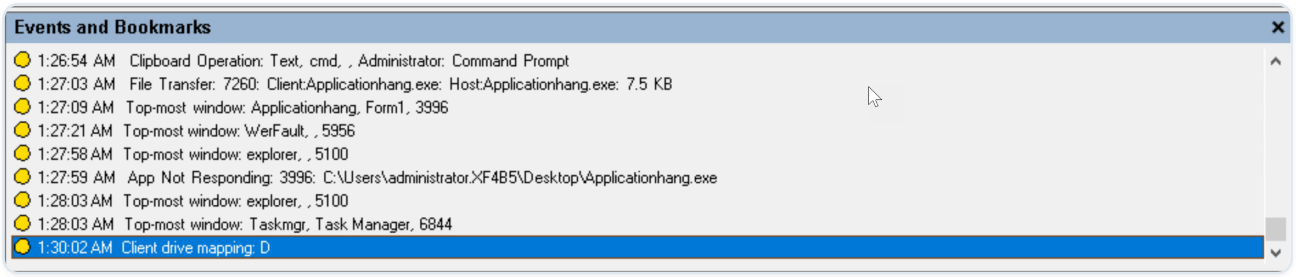
For more events in the Session Recording player, see the event descriptions later in this article.

Note:

> Applications built by PowerBuilder might exit unexpectedly when there are active policies detecting web browsing activities and topmost window events. To avoid the issue, use PowerBuilder 2019 R3 to build your applications.

INSERTION OF USB MASS STORAGE DEVICES

Session Recording can detect the insertion of a Client Drive Mapping (CDM) mapped or generic redirected USB mass storage device in a client where Citrix Workspace™ app for Windows or for Mac is installed. Session Recording tags these events in the recording.



> **Note:**

> To use an inserted USB mass storage device and detect the insertion events, set the **Client USB device redirection** policy to **Allowed** in Citrix Studio.

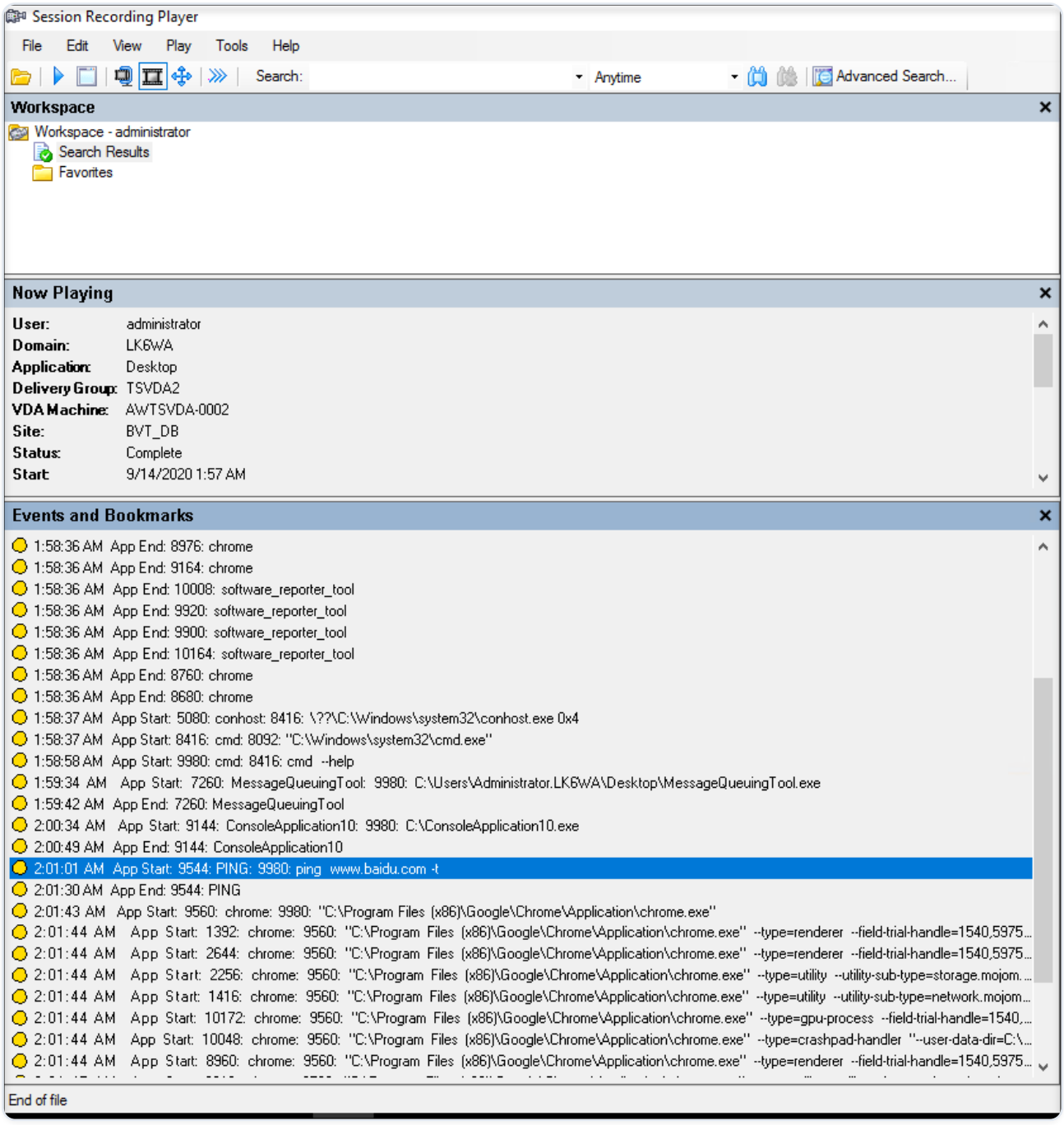
> Currently, only the insertion of USB mass storage devices (USB Class 08) can be detected.

APPLICATION STARTS AND ENDS

Session Recording supports detection of both application starts and ends. When you add a process to the **App monitoring list**, apps driven by the added process and its child processes are monitored. Child processes of a parent process that starts before Session Recording runs can also be captured.

Session Recording adds the process names, `cmd.exe`, `powershell.exe`, and `wsl.exe`, to the **App monitoring list** by default. If you select **Log app start events** and **Log app end events** for an event detection policy, the starts and ends of the Command Prompt, PowerShell, and Windows Subsystem for Linux (WSL) apps are logged no matter whether you manually add their process names to the **App monitoring list**. The default process names are not visible on the **App monitoring list**.

In addition, Session Recording provides a full command line for each app start event logged.



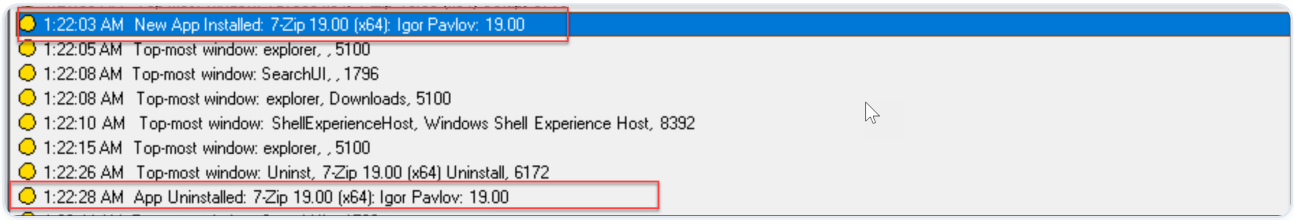
APPLICATION FAILURES

Session Recording detects app exits and unresponsive apps if you select **Log app failures** when creating your event detection policy. The **Log app failures rule** applies to all apps.



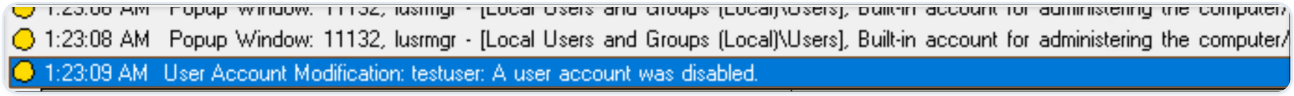
APP INSTALLS AND UNINSTALLS

The **Log app installs and uninstalls** rule applies to all apps.



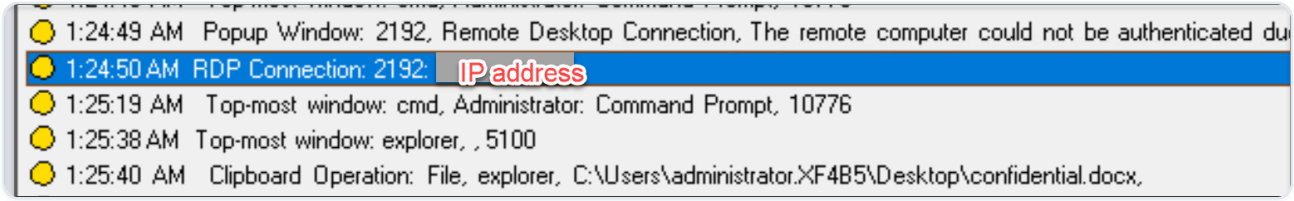
USER ACCOUNT MODIFICATIONS

Session Recording can detect account creation, enablement, disablement, deletion, name changes, and password modification attempts.



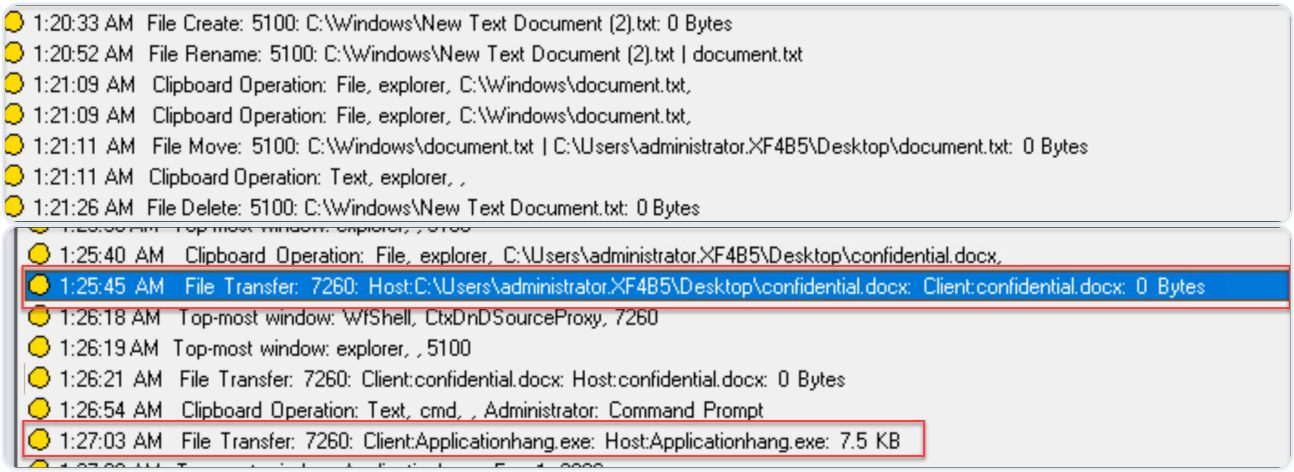
RDP CONNECTIONS

Session Recording can detect RDP connections initiated from the VDA hosting the recorded session.



FILE RENAMING, CREATION, DELETION, AND MOVING OPERATIONS WITHIN SESSIONS AND FILE TRANSFERS BETWEEN SESSION HOSTS (VDAS) AND CLIENT DEVICES

Session Recording can detect renaming, creation, deletion, and moving operations on target files and folders that you specify in the **File monitoring list**. Session Recording can also detect file transfers between session hosts (VDAs) and client devices (including mapped client drives and generic redirected mass storage devices). Selecting the **Log sensitive file events** option triggers the detection of file transfers, no matter whether you specify the **File monitoring list**.



Note:

> To enable file drag and drop and capture the drag and drop events, set the **Drag and Drop** policy to **Enabled** in Citrix Studio.

WEB BROWSING ACTIVITIES

Session Recording can detect user activities on supported browsers and tag the events in the recording. The browser name, URL, and page title are logged. For an example, see the following screen capture.



When you move your cursor away from a webpage that has focus, your browsing of this webpage is tagged without showing the browser name. This feature can be used to estimate how long a user stays on a webpage. For an example, see the following screen capture.



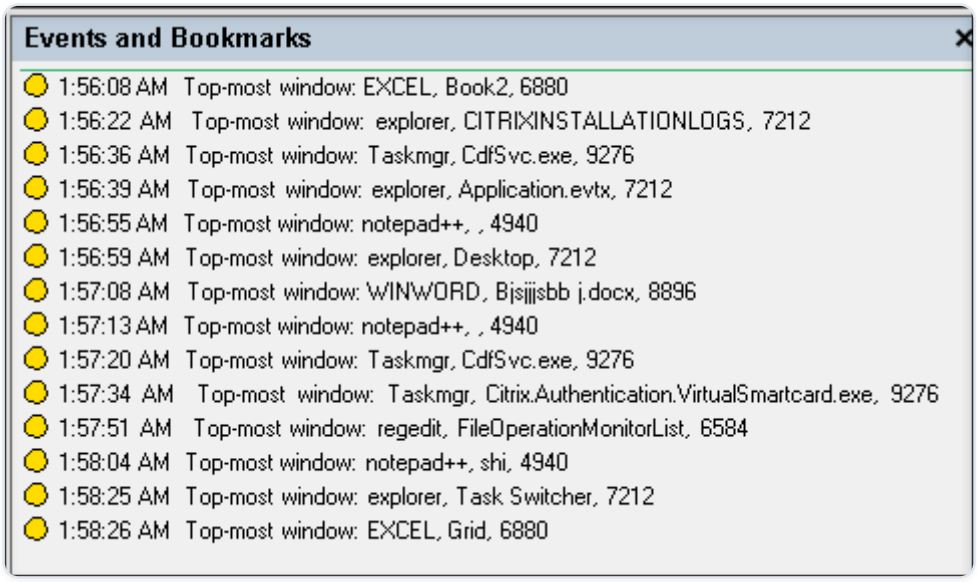
List of supported browsers:

- Google Chrome
- Microsoft Edge Chromium
- Mozilla Firefox

> **Note:**
>
> This feature requires Session Recording Version 1906 or later.

TOPMOST WINDOW EVENTS

Session Recording can detect the events when the window of an app is on top of all others. The process name, title, and process number are logged.

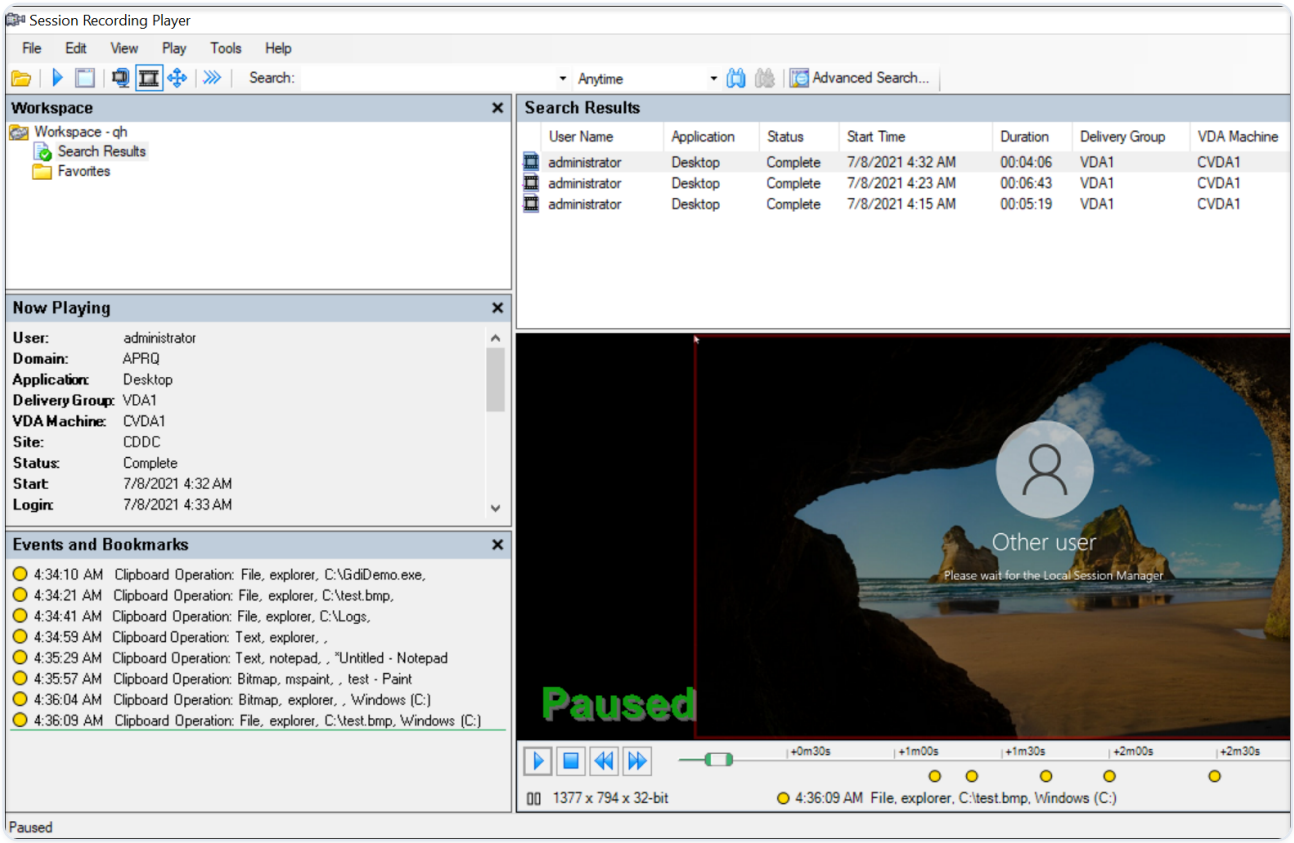


CLIPBOARD ACTIVITIES

Session Recording can detect copy operations of text, images, and files using the clipboard. The process name and file path are logged for a file copy. The process name and title are logged for a text copy. The process name is logged for an image copy.

Note: Content of copied text is not logged by default. To log text content, go to the Session Recording agent and set `HKEY_LOCAL_MACHINE\SOFTWARE

Citrix\SmartAuditor\Agent\CaptureClipboardContent `to` 1 `(the default value is` 0`).

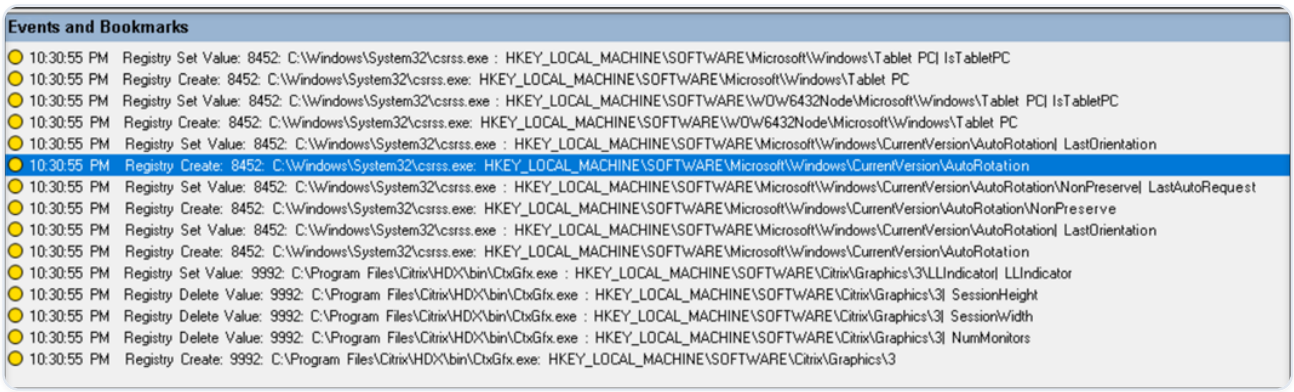


WINDOWS REGISTRY MODIFICATIONS

Starting with Version 2109, Session Recording can detect and log the following registry modifications while recording sessions:

REGISTRY MODIFICATION	CORRESPONDING EVENT
Adding a key	Registry Create
Adding a value	Registry Set Value
Renaming a key	Registry Rename
Renaming a value	Registry Delete Value and Registry Set Value
Changing an existing value	Registry Set Value
Deleting a key	Registry Delete
Deleting a value	Registry Delete Value

For example:



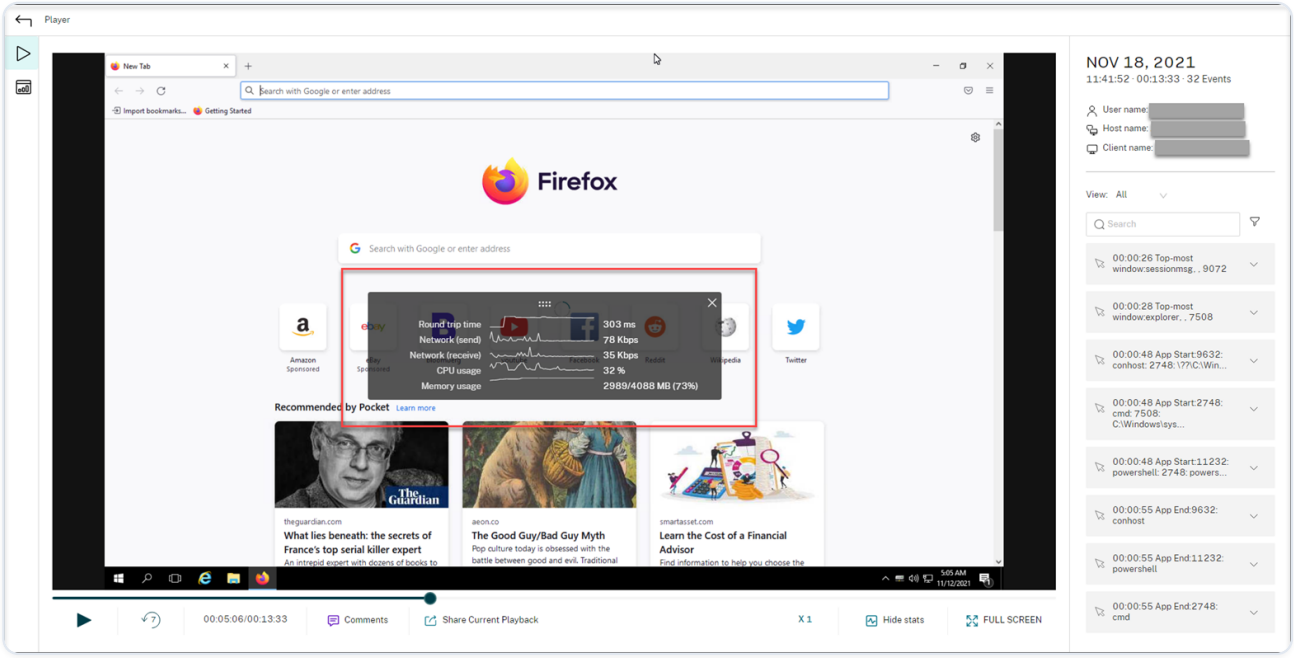
To enable this registry monitoring functionality, select the **Log registry modifications** option for your event detection policy.

PERFORMANCE DATA (DATA POINTS RELATED TO THE RECORDED SESSION)

When creating your event detection policy, select **Log performance data** to enable the session data overlay feature. The feature introduces a screen overlay during session playback in the web player. It is a semi-transparent overlay that you can relocate and hide. The overlay features the following data points related to the recorded session:

- Round trip time
- Network (send)

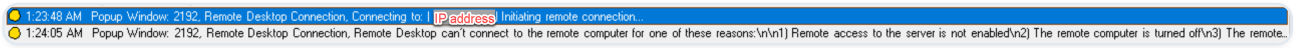
- Network (receive)
- CPU usage
- Memory usage



POPUP WINDOW EVENTS

When users open or close a confidential file or access a folder, a popup window might appear, showing a prompt or asking for a password. Session Recording can now monitor such popup window events while recording sessions. Popup windows in web browsers are not monitored.

Attributes of a popup window event are recorded, including the process name and content of the prompt.

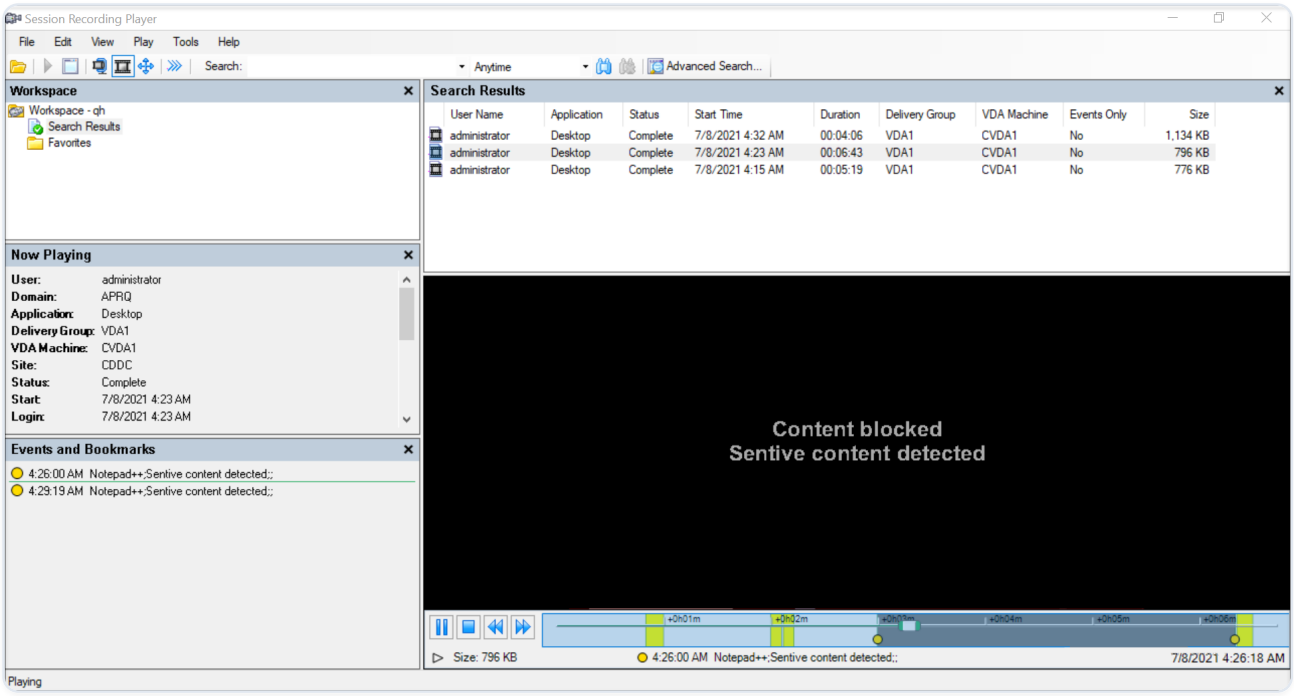


Custom events

The Session Recording agent provides the IUserApi COM interface that third-party applications can use to add application-specific event data into recorded sessions. Based on the event customization, Session Recording can block sensitive information and log the session pause and session resume events accordingly.

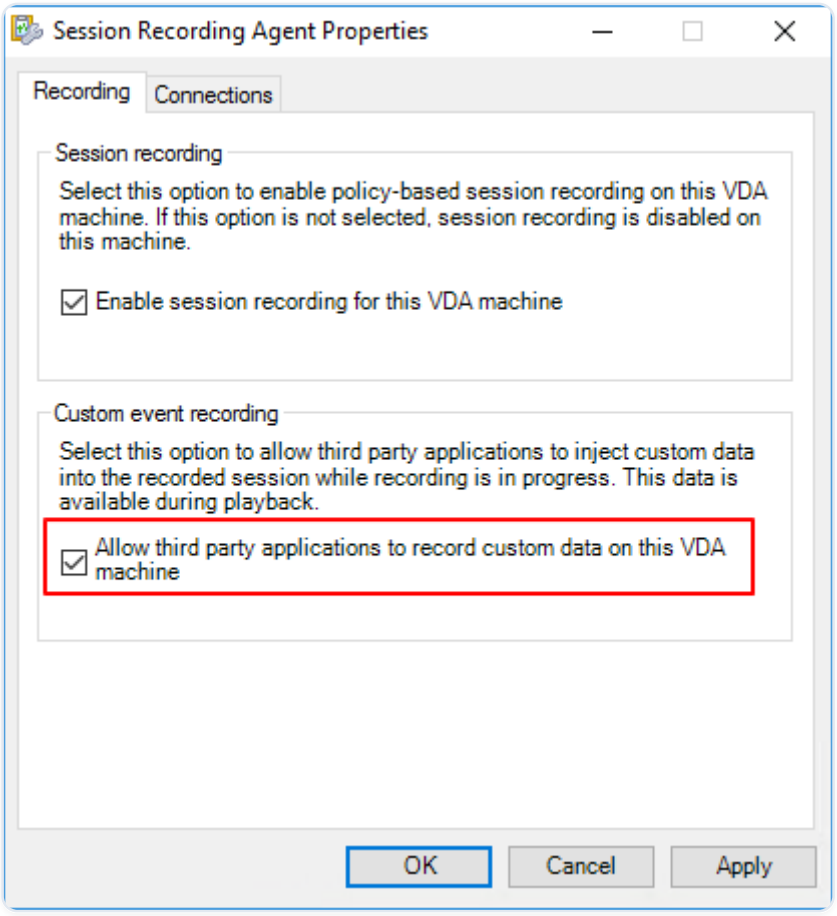
SENSITIVE INFORMATION BLOCKING

Session Recording lets you skip certain periods when recording the screen and blocks sensitive information in these periods during session playback. To use this feature, use Session Recording 2012 and later.



To use this feature, complete the following steps:

1. In **Session Recording Agent Properties**, select the **Allow third party applications to record custom data on this VDA machine** check box and click **Apply**.

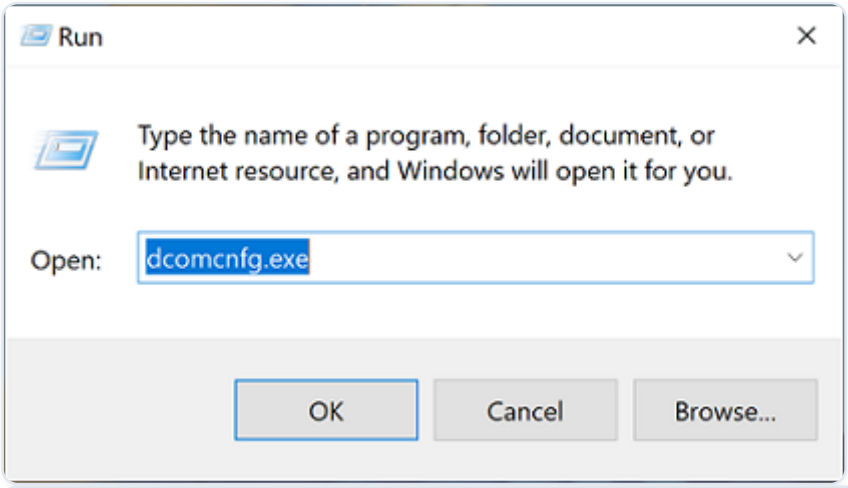


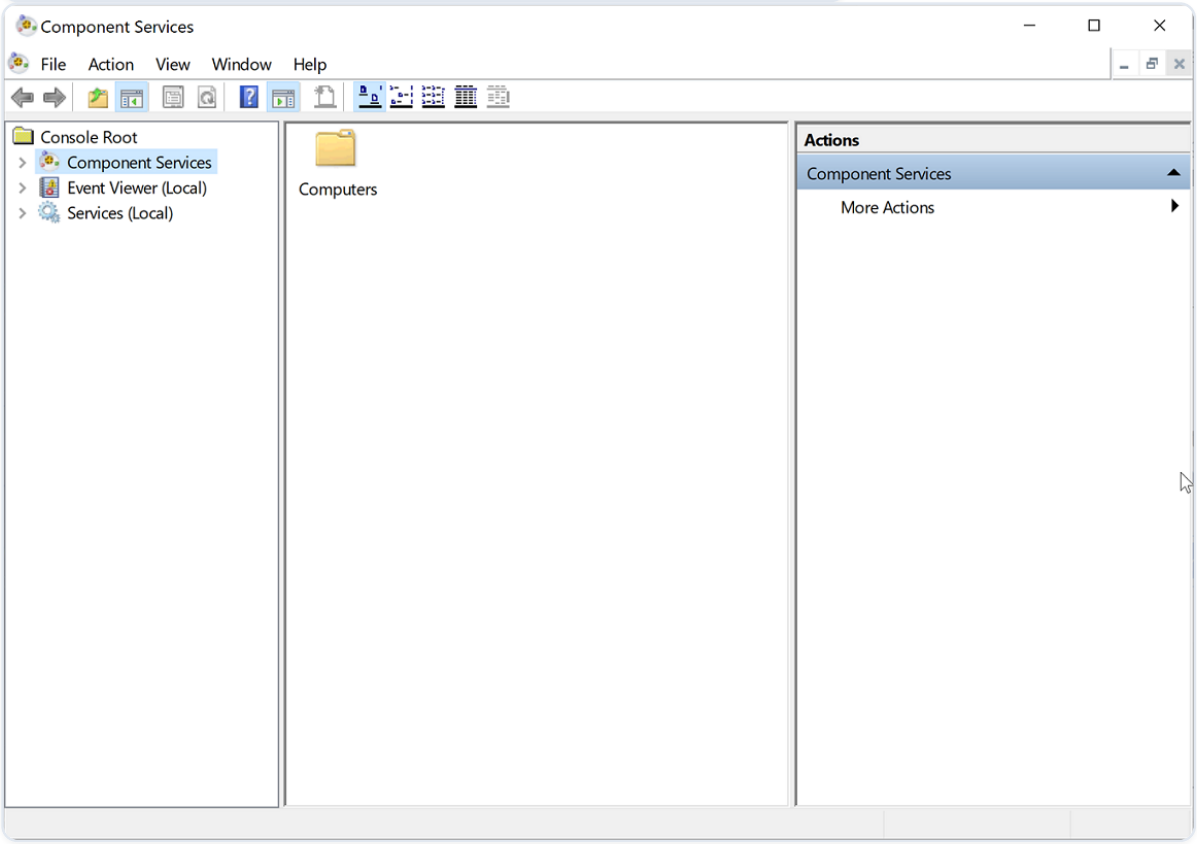
2. Grant users permission to invoke the Session Recording Event API (IUserApi COM interface).

Session Recording adds access control to the event API COM interface starting with version 7.15. Only authorized users are allowed to invoke the functionality to insert event metadata into a recording.

Logon users with local administrator privileges are granted with this permission by default. To grant other users this permission, use the Windows DCOM configuration tool:

a. On the Session Recording agent, run **comcnfg.exe** to open the Windows DCOM configuration tool.

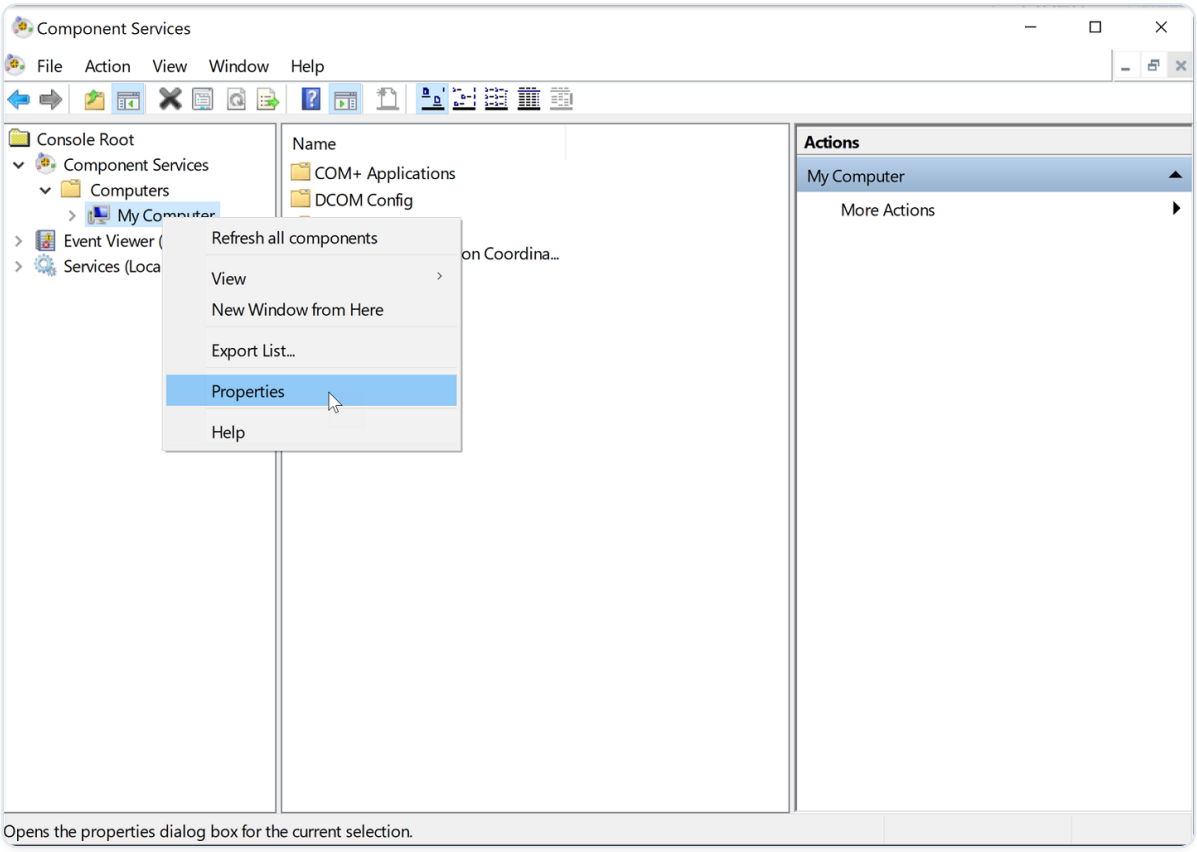




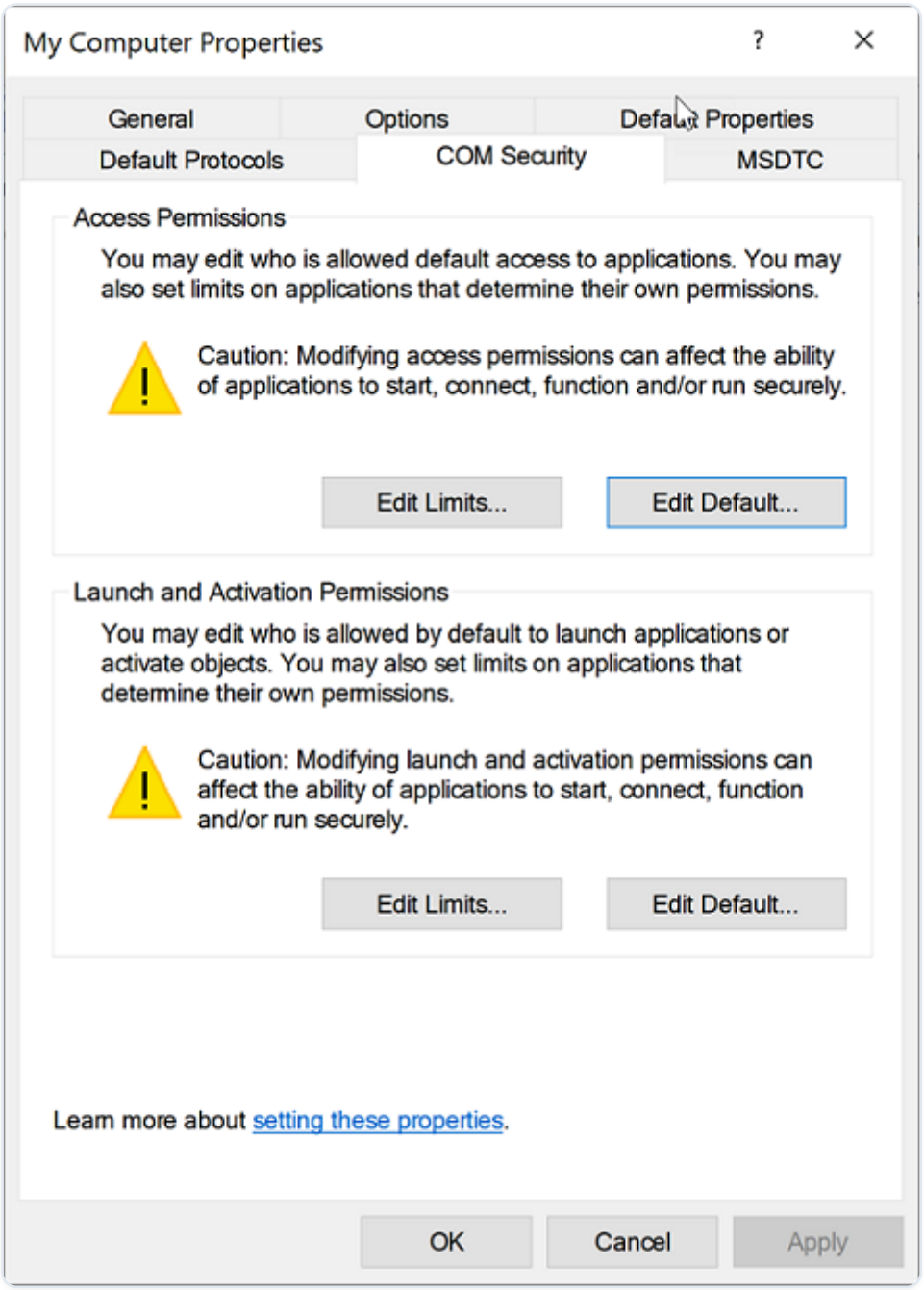
If you are granting permission to users who are not members of the domain administrator group and the Session Recording agent is running on Windows Server 2019 or later, or Windows 10 or later, proceed to step b. Otherwise, skip step b and go to step c directly.

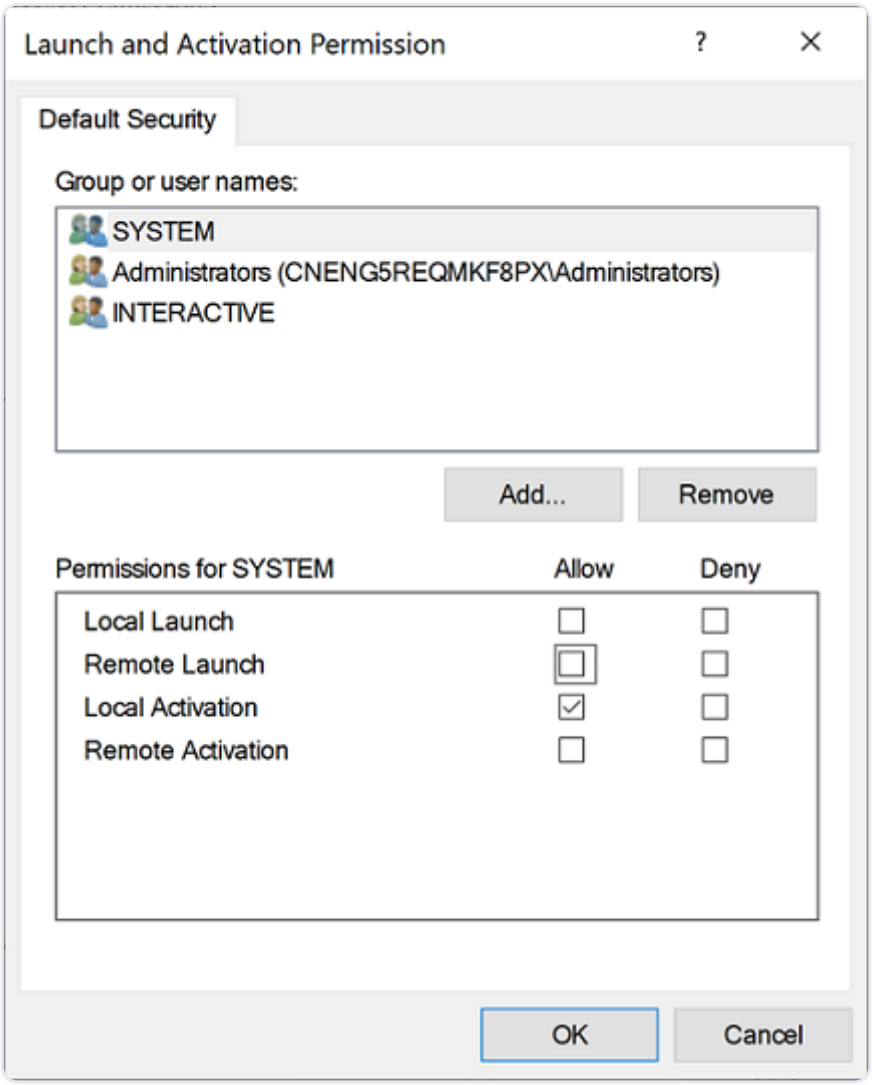
b. Select **Console Root > Component Services > Computers > My Computer** from the left navigation.

Right-click **My Computer** and select **Properties**.

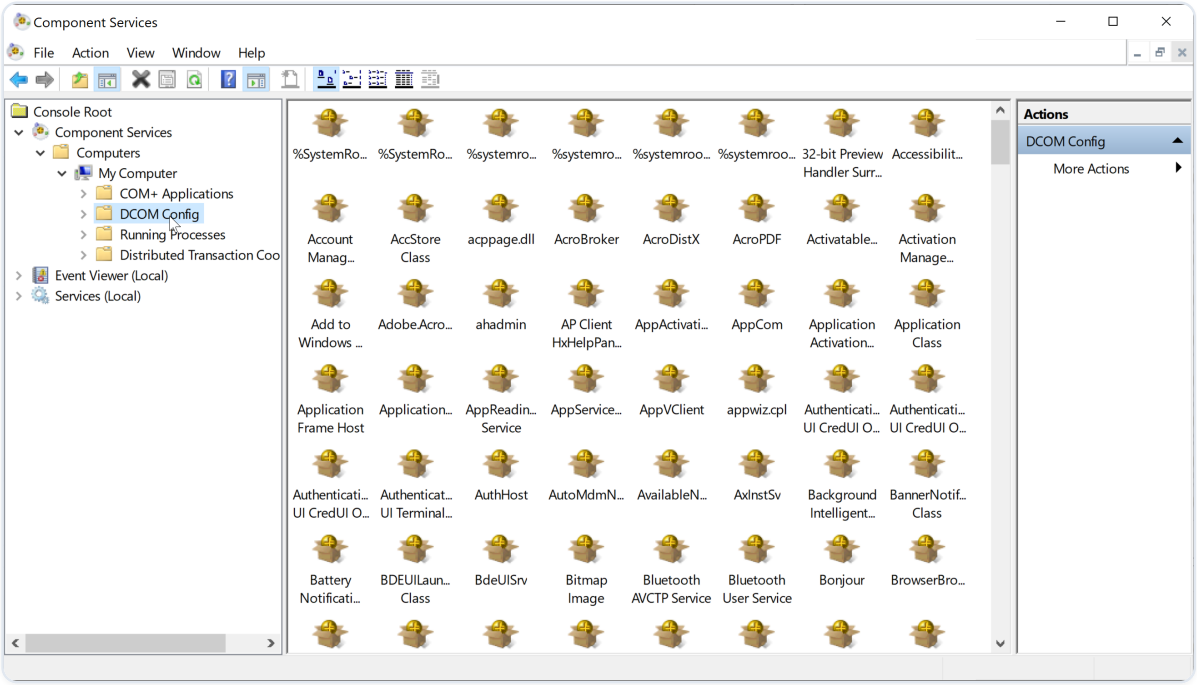


Select the **COM Security** tab, and then click **Edit Default** to add users with **Local Activation** permission in the **Launch and Activation Permissions** section.

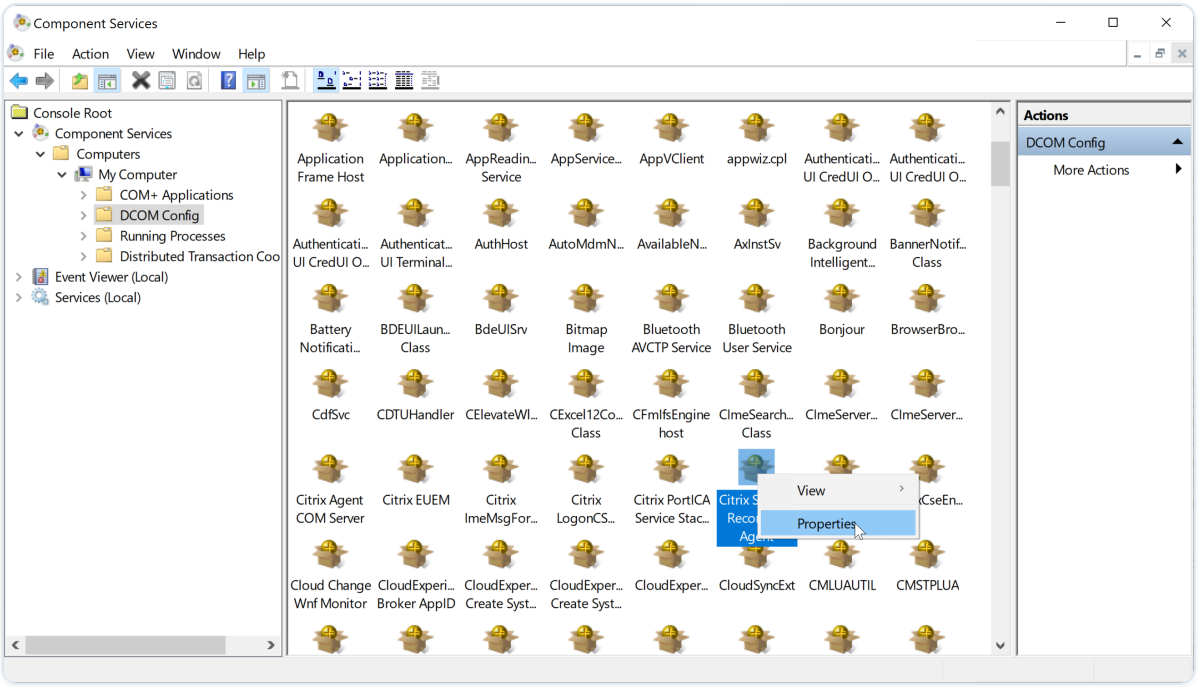

My Computer Properties
General
Options
Default Properties
Default Protocols
COM Security
MSDTC
Access Permissions
You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.
Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.
Edit Limits...
Edit Default...
Launch and Activation Permissions
You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.
Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.
Edit Limits...
Edit Default...
Learn more about setting these properties.
OK
Cancel
Apply



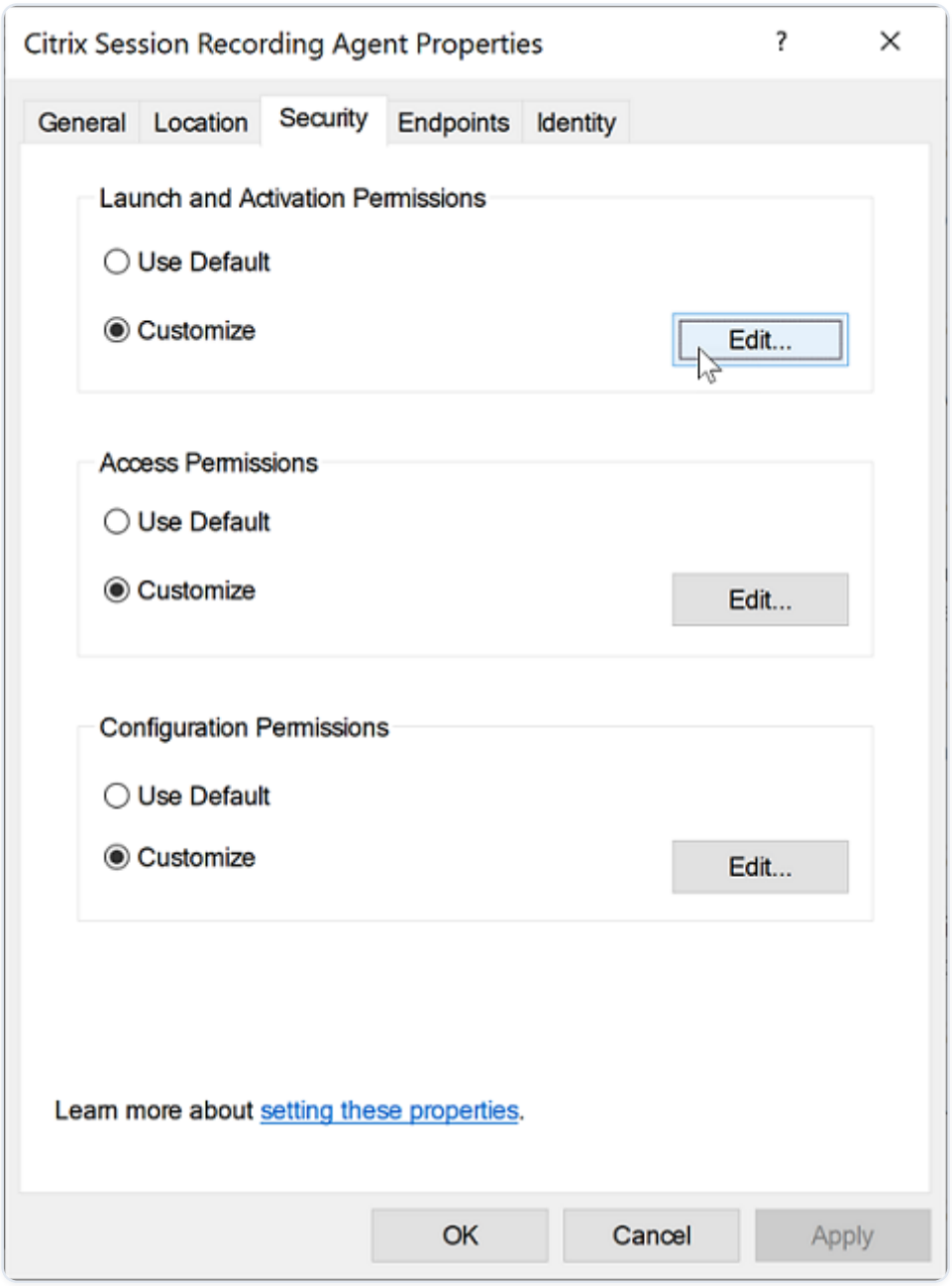
c. Select **Console Root > Component Services > Computers > My Computer > DCOM Config** from the left navigation.

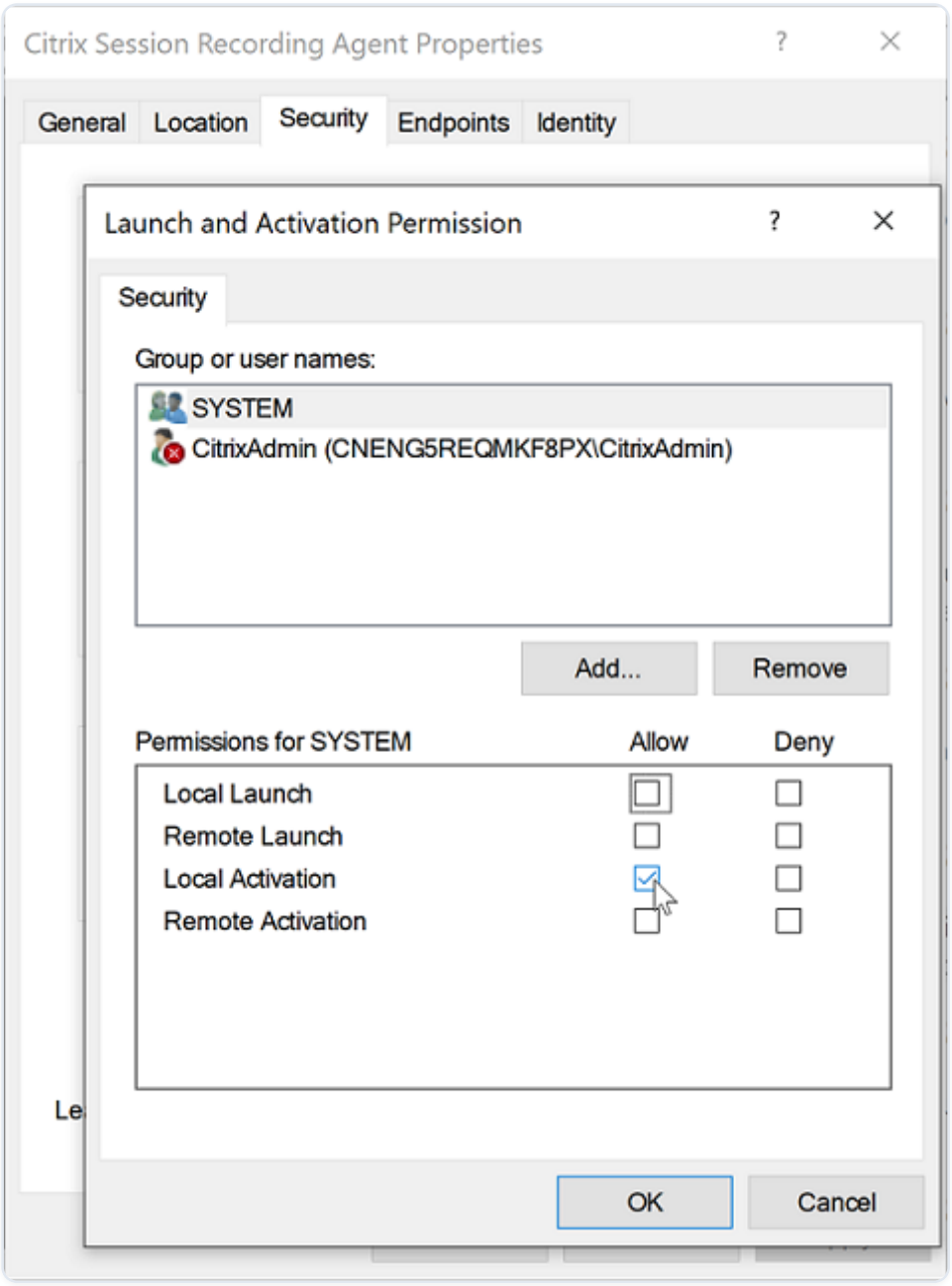


Right-click **Citrix Session Recording Agent** and choose **Properties**.



d. Select the **Security** tab, and then click **Edit** to add users with **Local Activation** permission in the **Launch and Activation Permissions** section.


Citrix Session Recording Agent Properties
General
Location
Security
Endpoints
Identity
Launch and Activation Permissions
Use Default
Customize
Edit...
Access Permissions
Use Default
Customize
Edit...
Configuration Permissions
Use Default
Customize
Edit...
Learn more about setting these properties.
OK
Cancel
Apply



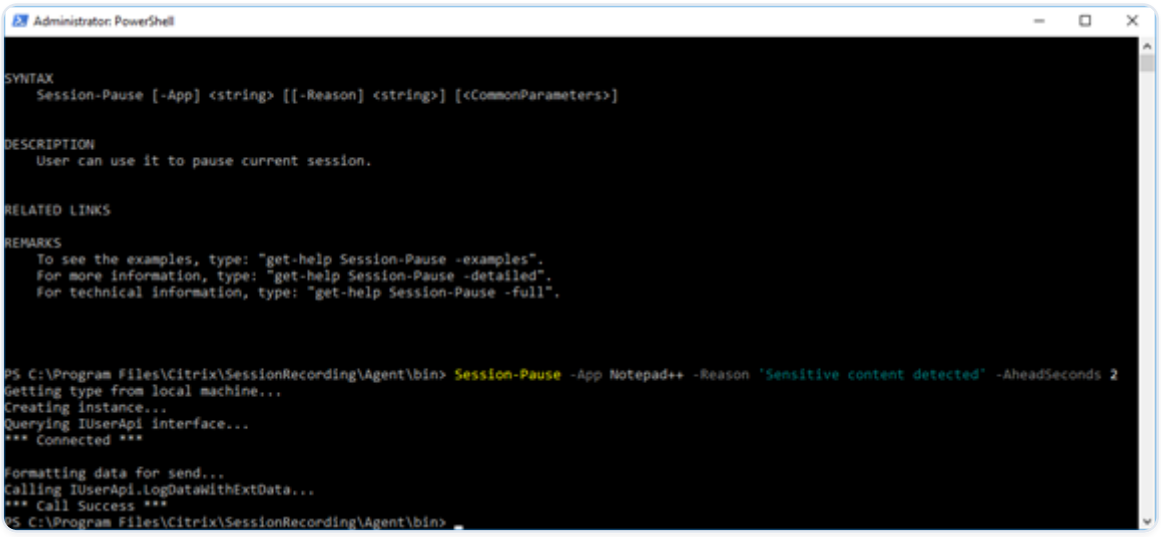
Note:

DCOM configuration takes effect immediately. There is no need to restart any services or the machine.

3. Start a Citrix virtual session.
4. Start PowerShell and change the current drive to the **<Session Recording agent installation path\>\Bin** folder to import the SRUserEventHelperSnapin.dll module.
5. Run the `Session-Pause` and `Session-Resume` cmdlets to set parameters for triggering sensitive information blocking.

PARAMETER	DESCRIPTION	REQUIRED OR OPTIONAL
`-APP`	The app name that calls the **Session-Pause** and **Session-Resume** cmdlets.	Required
`-Reason`	The reason that content is blocked. If you leave this parameter unspecified, the default setting shows, stating **Content Blocked** and **Sensitive information exists and is blocked**. If you set this parameter, the reason you specify shows when you navigate to the blocked period during session playback. This parameter is available for both the **Session-Pause** and **Session-Resume** cmdlets.	Optional
`-AheadSeconds`	This parameter is available for the **Session-Pause** cmdlet only. It lets you configure the amount of time of the screen recording you want to bypass before sensitive information is detected. The default value is 1 s.	Optional

For example, you can run **Session-Pause** similar to the following:



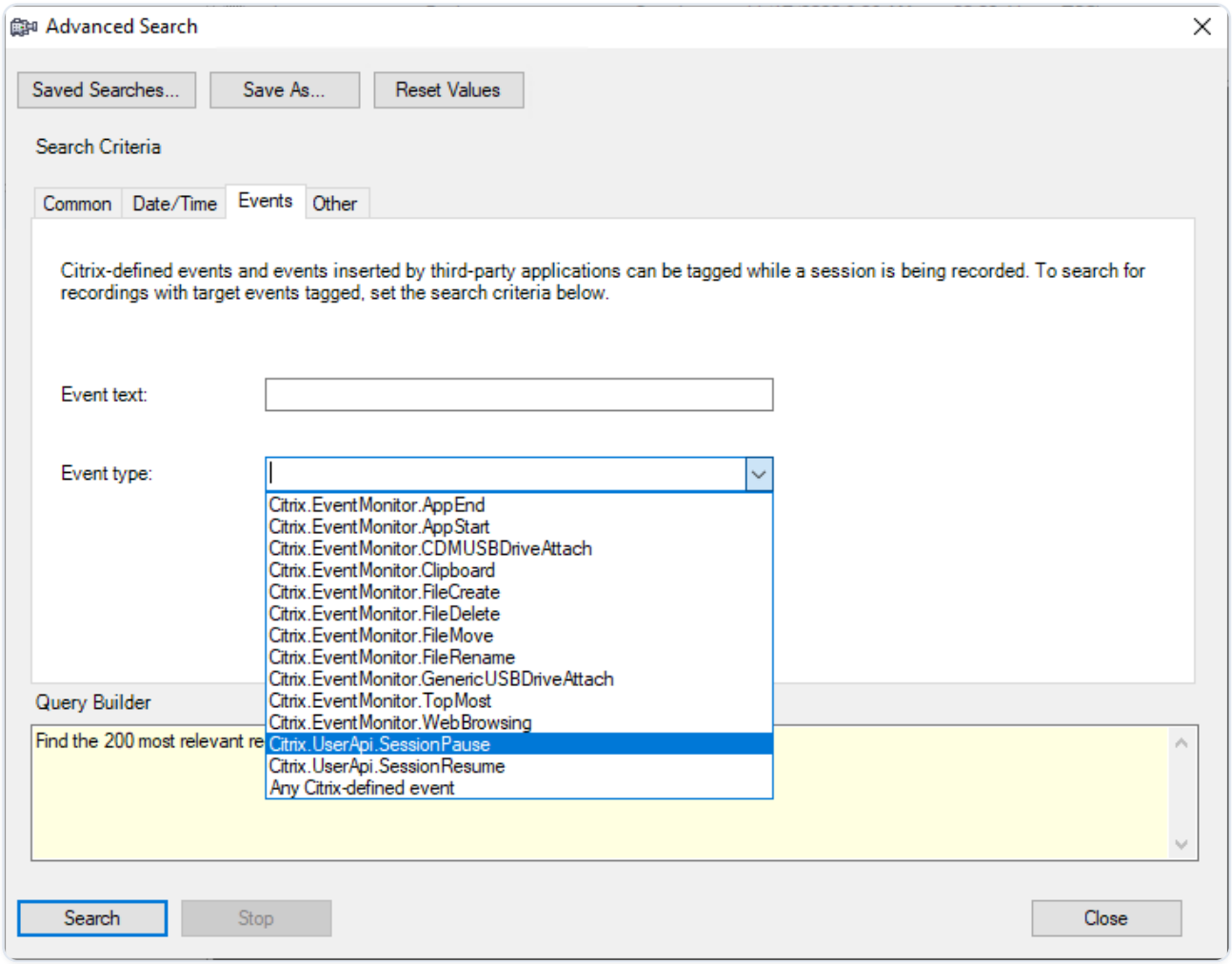
Search for and play back recordings with tagged events

SEARCH FOR RECORDINGS WITH TAGGED EVENTS

The Session Recording player allows you to perform advanced searches for recordings with tagged events.

1. In the Session Recording player, click **Advanced Search** on the tool bar or choose **Tools > Advanced Search**.
2. Define your search criteria in the **Advanced Search** dialog box.

The **Events** tab allows you to search for tagged events in sessions by **Event text** or **Event type** or both. You can use the **Events**, **Common**, **Data/Time**, and **Other** filters in combination to search for recordings that meet your criteria.



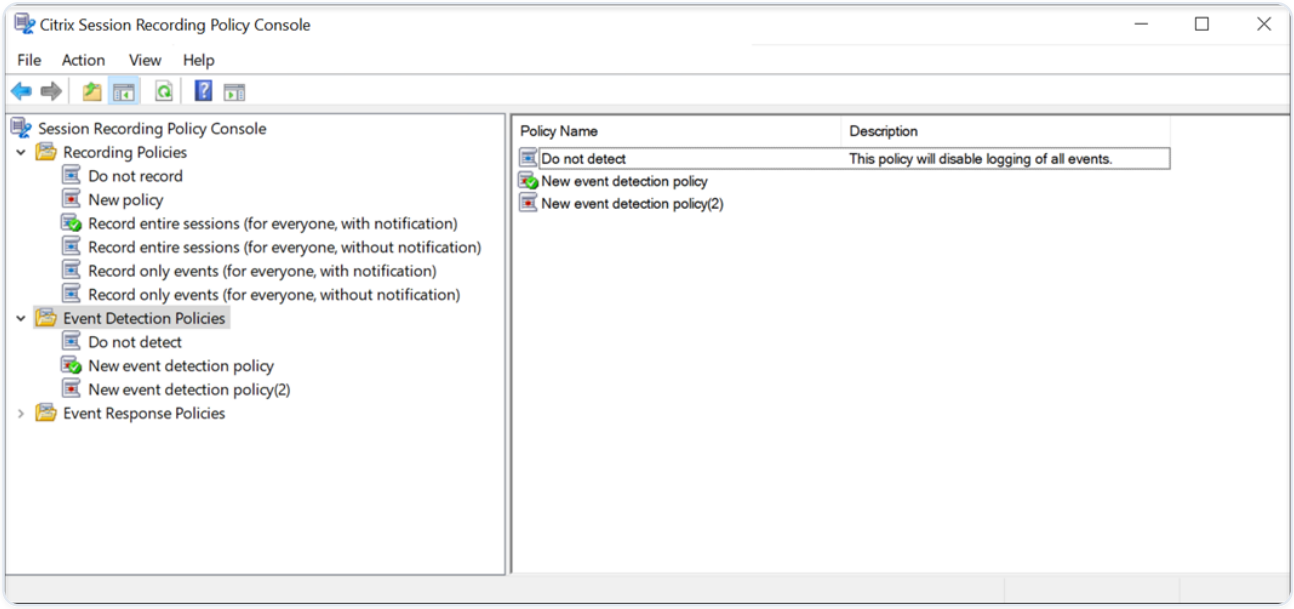
Note:

- The **Event type** list itemizes all event types. You can select an event type to search. Selecting **Any Citrix-defined event** means to search for all recordings with any type of events logged by Citrix Session Recording.
- The **Event text** filter supports partial match. Wildcards are not supported.
- The **Event text** filter is case-insensitive when matching.
- For the types of events, the words `App Start`, `App End`, `Client drive mapping`, and `File Rename` do not participate in matching when you search by **Event text**. Therefore, when you type `App Start`, `App End`, `Client drive mapping`, or `File Rename` in the **Event text** box, no result can be found.

You can use events to navigate through a recorded session, or skip to the points where the events are tagged.

System-defined event detection policy

The system-defined event detection policy is **Do not detect**. It's inactive by default. When it's active, no events are logged.

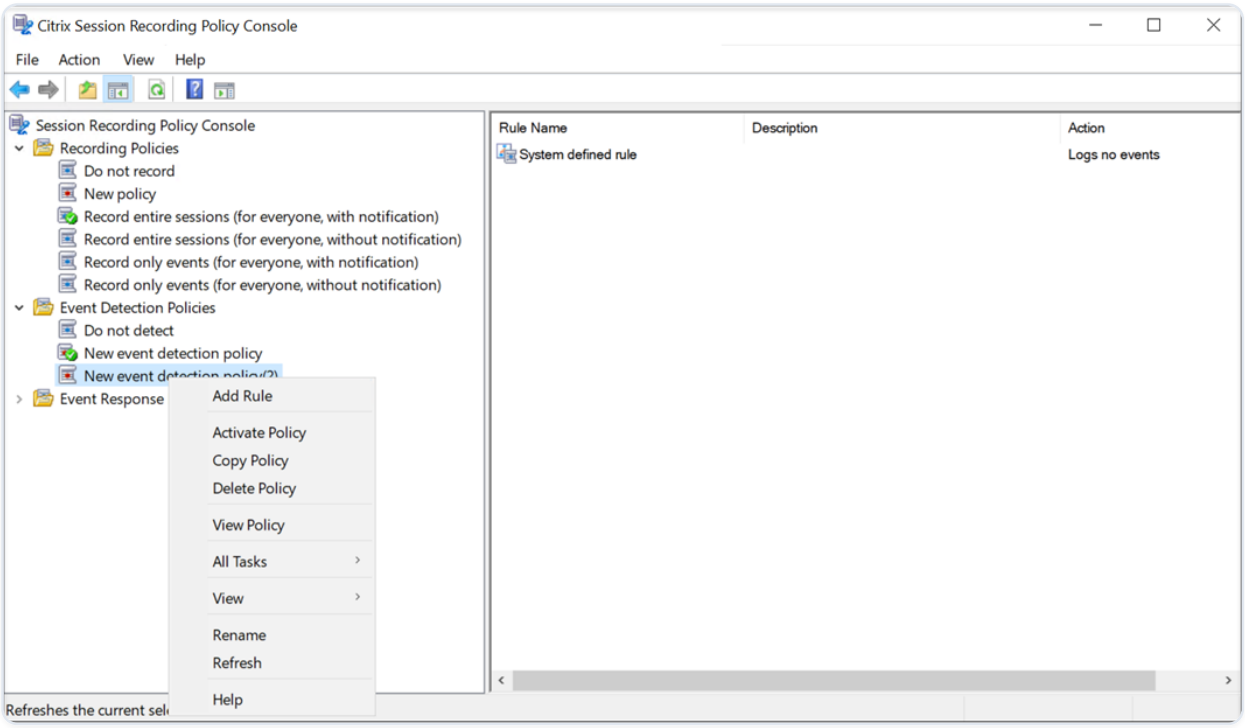


You cannot modify or delete the system-defined event detection policy.

Create a custom event detection policy

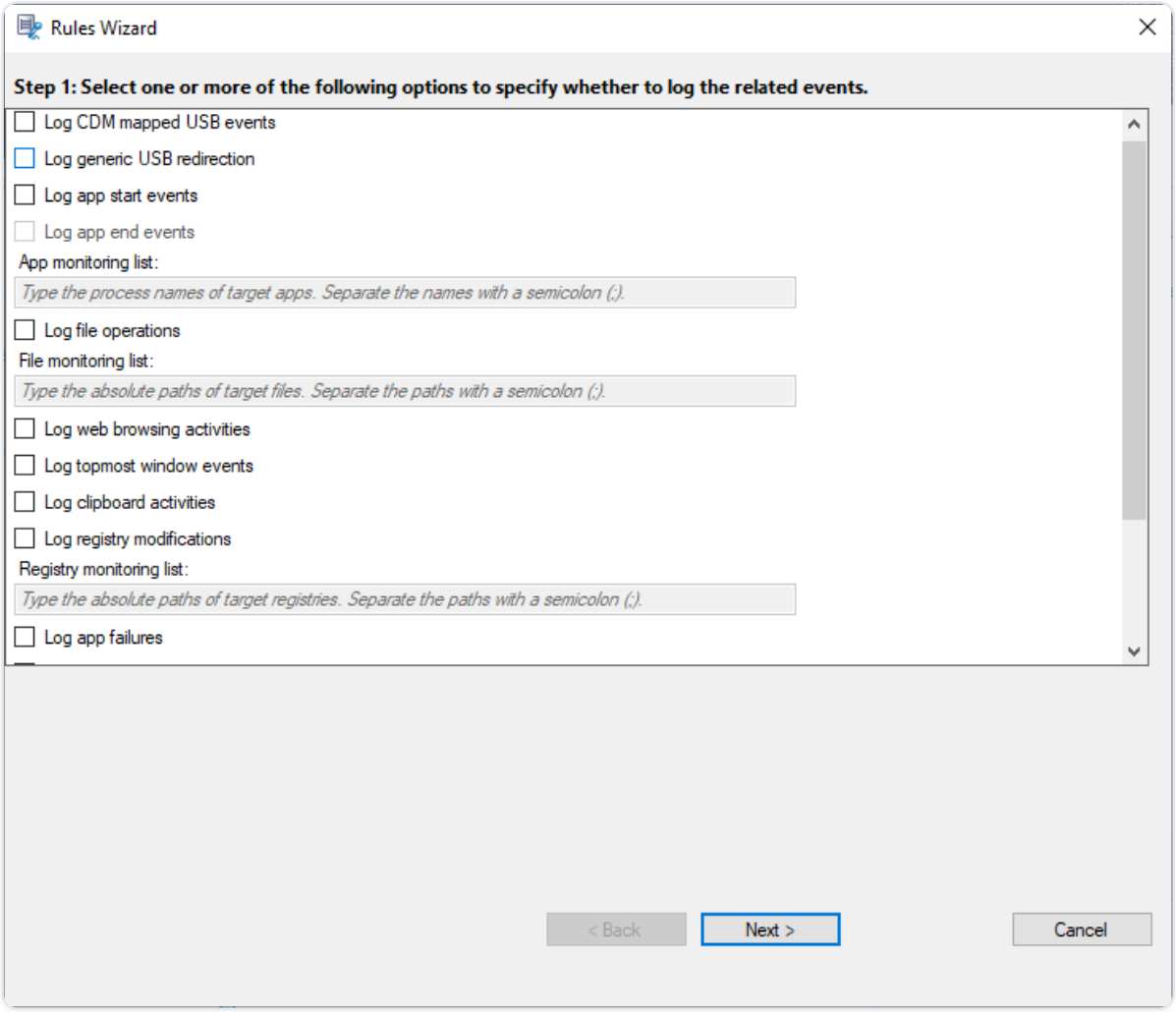
To create a custom event detection policy:

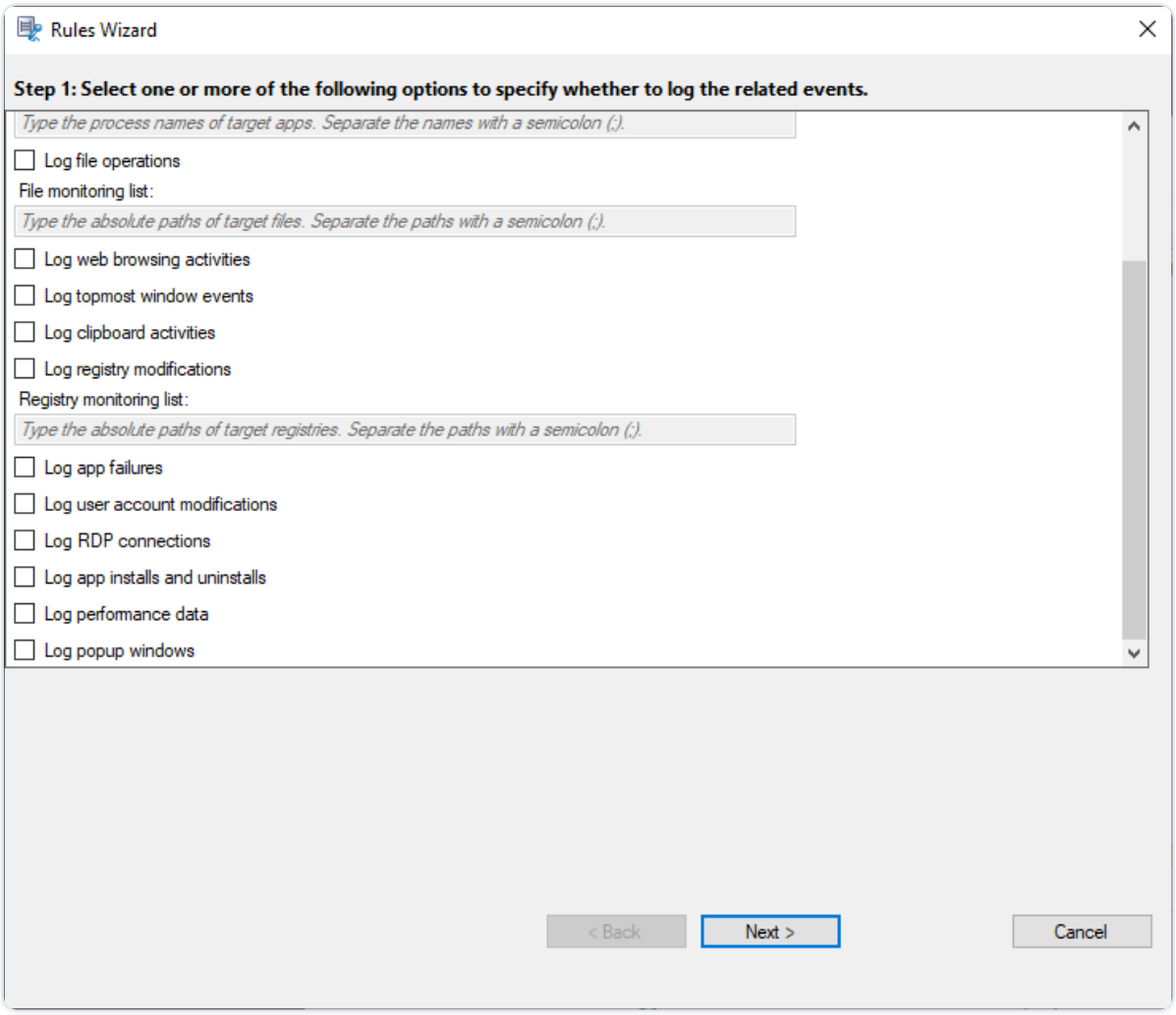
1. Log on as an authorized Policy Administrator to the server where the Session Recording policy console is installed.
2. Start the Session Recording policy console. By default, there is no active event detection policy.
3. Select **Event Detection Policies** in the left pane. From the menu bar, choose **Add New Policy** to create an event detection policy.
4. (Optional) Right-click the new event detection policy and rename it.



5. Right-click the new event detection policy and select **Add Rule**.

   a. Specify one or more target events to monitor by selecting the check box next to each event type. Scroll down the window to view all available event types.


Rules Wizard
Step 1: Select one or more of the following options to specify whether to log the related events.
Log CDM mapped USB events
Log generic USB redirection
Log app start events
Log app end events
App monitoring list:
Type the process names of target apps. Separate the names with a semicolon (;).
Log file operations
File monitoring list:
Type the absolute paths of target files. Separate the paths with a semicolon (;).
Log web browsing activities
Log topmost window events
Log clipboard activities
Log registry modifications
Registry monitoring list:
Type the absolute paths of target registries. Separate the paths with a semicolon (;).
Log app failures
< Back
Next >
Cancel



- **Log CDM mapped USB events**: Logs the insertion of a Client Drive Mapping (CDM) mapped mass storage device in a client where Citrix Workspace app for Windows or for Mac is installed.
- **Log generic USB redirection**: Logs the insertion of a generic redirected mass storage device in a client where Citrix Workspace app for Windows or for Mac is installed.
- **Log app start events**: Logs the starts of target applications.
- **Log app end events**: Logs the ends of target applications.

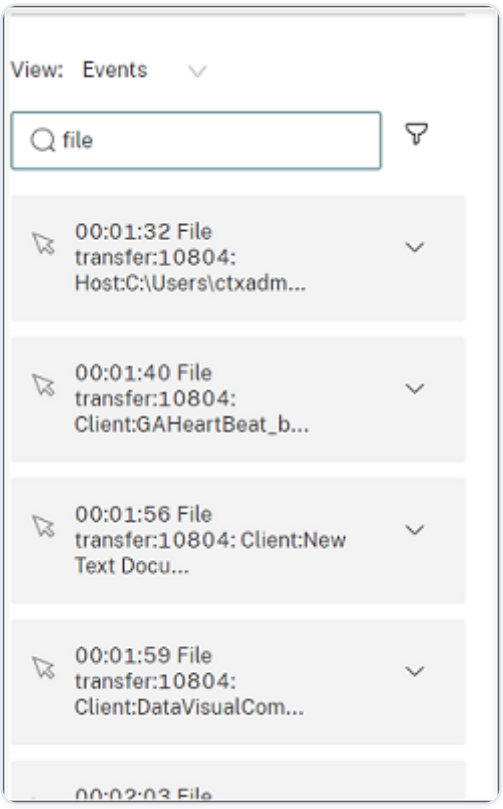
> **Note:**
>
> The **Log app end events** check box is grayed out before you select **Log app start events**.

- **App monitoring list**: When you select **Log app start events** and **Log app end events**, use the **App monitoring list** to specify target applications to monitor and to avoid an excessive number of events from flooding the recordings.

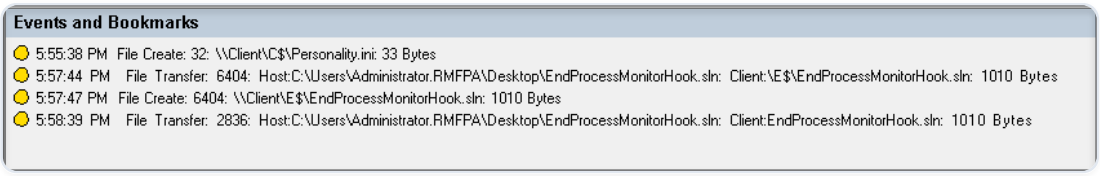
  > **Note:**
  >
  > - To capture the start and end of an application, add the process name of the application in the **App monitoring list**. For example, to capture the start of Remote Desktop Connection, add the process name `mstsc.exe` to the **App monitoring list**. When you add a process to the **App monitoring list**, applications driven by the added process and its child processes are monitored. Session Recording adds the process names, `cmd.exe`, `powershell.exe`, and `wsl.exe`, to the **App monitoring list** by default. If you select **Log app start events** and **Log app end events** for an event detection policy, the starts and ends of the Command Prompt, PowerShell, and Windows Subsystem for Linux (WSL) apps are logged regardless of whether you manually add their process names to the **App monitoring list**. The default process names aren't visible on the **App monitoring list**.
  > - Separate process names with a semicolon (;).
  > - Only the exact match is supported. Wildcards aren't supported.
  > - Process names you add are case-insensitive.
  > - To avoid an excessive number of events from flooding the recordings, do not add any system process names (for example, explorer.exe) and web browsers in the registry.

- **Log file operations**: Logs operations on target files in the **File monitoring list** and logs file transfers between session hosts (VDAs) and client devices (including mapped client drives and generic redirected mass storage devices). Selecting this option triggers the logging of file transfers, no matter whether the **File monitoring list** is specified.

  - File events presented in the web player



- File events presented in the Session Recording Player



- **File monitoring list**: When you select **Log file operations**, use the **File monitoring list** to specify target files to monitor. You can specify folders to capture all files within them. No file is specified by default, which means no file is captured by default.

> **Note:**
>
> - To capture renaming, creation, deletion, or moving operations on a file, add the path string of the file folder (not the file name or the root path of the file folder) in the **File monitoring list**. For example, to capture renaming, creation, deletion, and moving operations on the `sharing.ppt` file in `C:\User\File`, add the path string `C:\User\File` in the **File monitoring list**.
> - Both local file paths and remote shared folder paths are supported. For example, to capture operations on the RemoteDocument.txt file in the `\`

> `\remote.address\Documents` folder, add the path string `\\remote.address\Documents` in the **File monitoring list**.
>
> - Separate monitored paths with a semicolon (;).
> - Only exact matches are supported. Wildcards aren't supported.
> - Path strings are case-insensitive.

> Limitations:

- Copying files or folders from a monitored folder to an unmonitored folder isn't captured.
- When the length of a file or folder path including the file or folder name exceeds 260 characters, operations on the file or folder aren't captured.
- Pay attention to the database size. To prevent large numbers of events from being captured, back up or delete the "Event" table regularly.
- When large numbers of events are captured in a short time, the player displays and the database stores only one event for each type to avoid storage expansion.

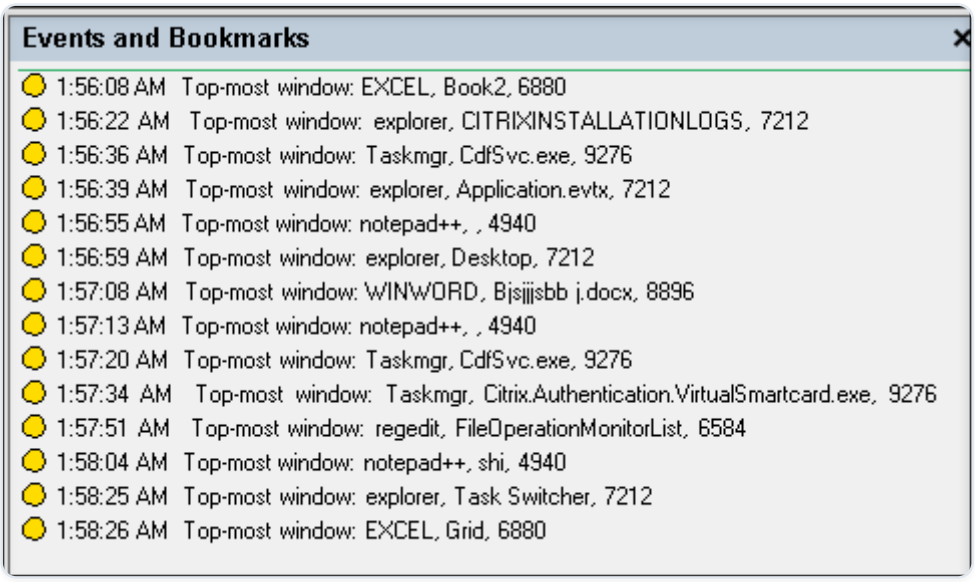
- **Log web browsing activities**: Logs user activities on supported browsers and tags the browser name, URL, and page title in the recording.



List of supported browsers:

- Google Chrome
- Microsoft Edge Chromium
- Mozilla Firefox

- **Log topmost window events**: Logs the topmost window events and tags the process name, title, and process number in the recording.



- **Log clipboard activities**: Logs copy operations of text, images, and files using the clipboard. The process name and file path are logged for a file copy. The process name and title are logged for a text copy. The process name is logged for an image copy.
- **Log registry modifications**: Logs the following Windows registry modifications: add a key or value, rename a key or value, change an existing value, and delete a key or value.
- **Registry monitoring list**: When you select **Log registry modifications**, type the absolute paths of the registries you want to monitor and separate the paths with a semicolon (;). Start a path with HKEY_USERS, HKEY_LOCAL_MACHINE, or HKEY_CLASSES_ROOT. For example, you can type `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows;HKEY_CLASSES_ROOT\GuestStateVDev`. If you leave this list unspecified, no registry modification is captured.
- **Log app failures**: Logs unexpected app exits and unresponsive apps. This rule applies to all apps.
- **Log user account modifications**: Logs the following user account modifications: account creation, enablement, disablement, deletion, lockout, name changes, and password modification attempts.
- **Log RDP connections**: Logs RDP connections initiated from the VDA hosting the recorded session.
- **Log app installs and uninstalls**: Logs app installs and uninstalls during the recorded session. This rule applies to all apps.
- **Log performance data**: Enables the session data overlay feature. Select this check box to view data points related to the recorded session.

- **Log popup windows**: Logs popup windows that might appear when users open or close a confidential file or access a folder.

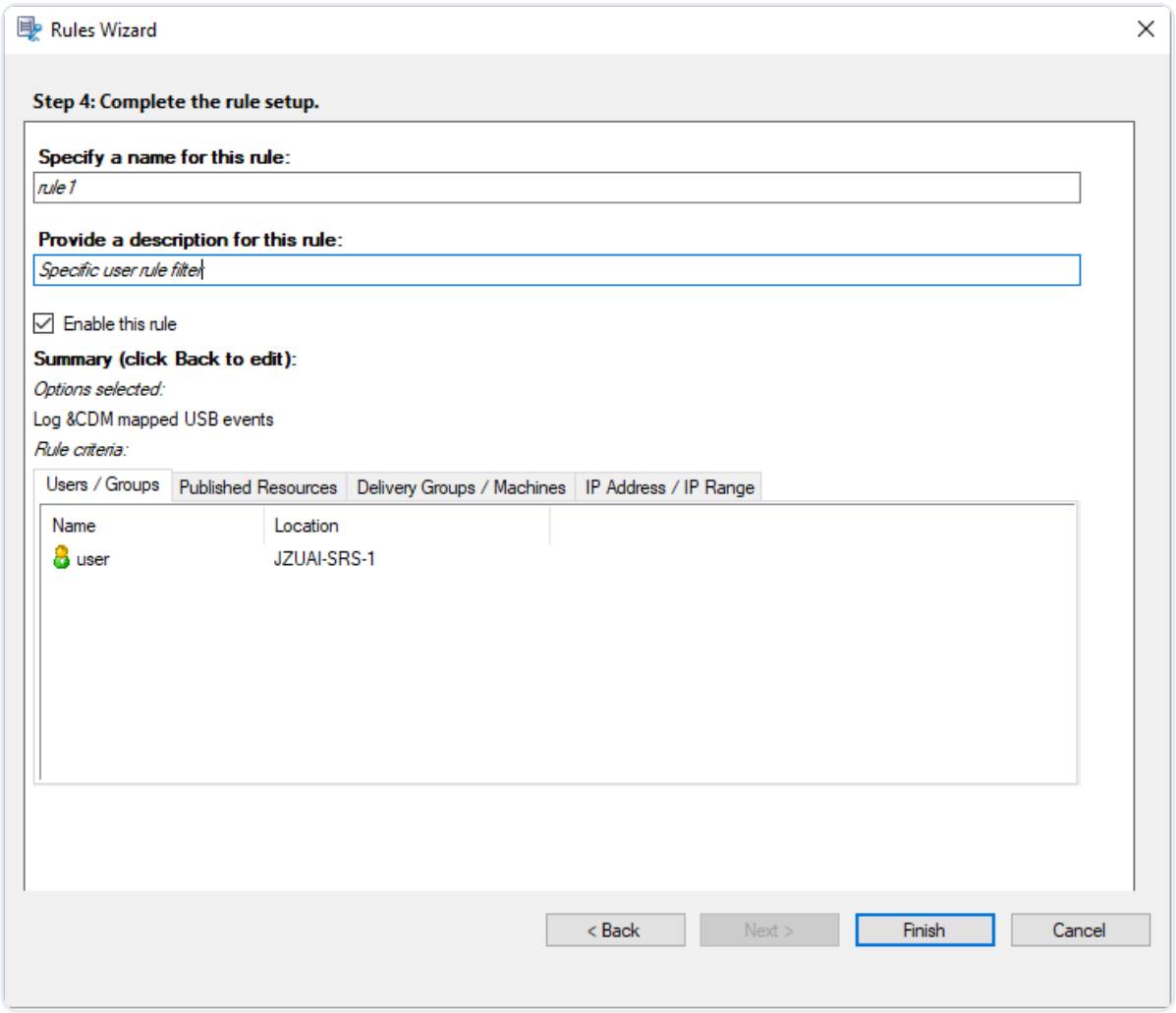
b. Select and edit the rule criteria.

   Similar to creating a custom recording policy, you can choose one or more rule criteria: **Users or Groups**, **Published Applications or Desktop**, **Delivery Groups or Machines**, and **IP Address or IP Range**. To obtain the lists of published applications or desktops and delivery groups or VDA machines, you must have the read permission as a site administrator. Configure the administrator read permission on the Delivery Controller™ of the site.

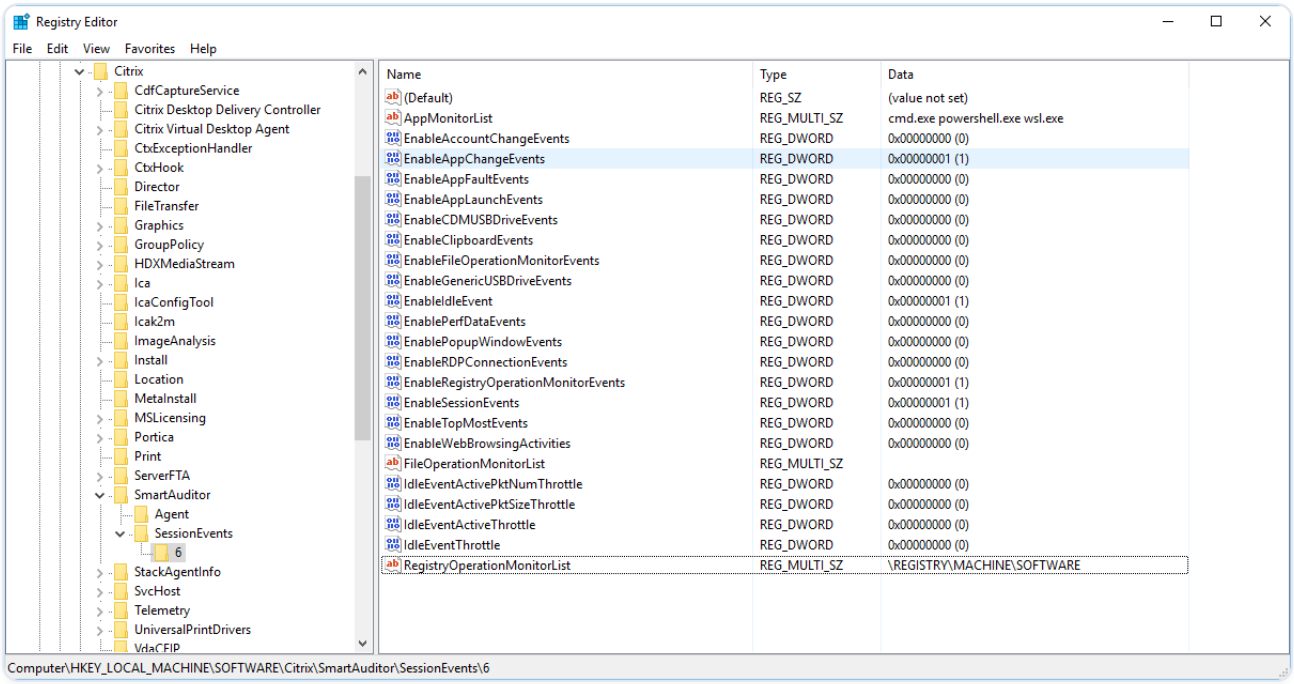
   For more information, see the instructions in the Create a custom recording policy section.

   > **Note:**
   >
   > Some sessions might not meet any rule criteria in an event detection policy. For these sessions, the action of the fallback rule applies, which is always **Do not detect**. You cannot modify or delete the fallback rule.

c. Follow the wizard to complete the configuration.



After a session that matches an event detection policy starts, the session ID and its event registry values appear in the Session Recording agent. For example:



Compatibility with registry configurations

When Session Recording is newly installed or upgraded, no active event detection policy is available by default. In this case, each Session Recording agent respects the registry values under `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SessionEvents` to determine whether to log specific events. For a description of the registry values, see the following table:

REGISTRY VALUE	DESCRIPTION
ENABLESESSIONEVENTS	1: ENABLES EVENT DETECTION GLOBALLY; 0: DISABLES EVENT DETECTION GLOBALLY (DEFAULT VALUE DATA).
ENABLEACCOUNTCHANGEEVENTS	1: ENABLES DETECTING USER ACCOUNT MODIFICATIONS; 0: DISABLES DETECTING USER ACCOUNT MODIFICATIONS (DEFAULT VALUE DATA).
ENABLEAPPCHANGEEVENTS	1: ENABLES DETECTING APP INSTALLS AND UNINSTALLS; 0: DISABLES DETECTING APP INSTALLS AND UNINSTALLS (DEFAULT VALUE DATA).
ENABLEAPPFAULTEVENTS	1: ENABLES DETECTING APP FAILURES; 0: DISABLES DETECTING APP FAILURES (DEFAULT VALUE DATA).
EnableAppLaunchEvents	**1**: enables detecting only app starts; **2**: enables detecting both app starts and ends; **0**: disables detecting app starts and ends (default value data).
AppMonitorList	Specifies target apps to monitor. No app is specified by default, which means no app is captured by default.
EnableCDMUSBDriveEvents	**1**: enables detecting the insertion of CDM mapped USB mass storage devices; **0**: disables detecting the insertion of CDM mapped USB mass storage devices (default value data).

REGISTRY VALUE	DESCRIPTION
ENABLESESSIONEVENTS	**1: ENABLES EVENT DETECTION GLOBALLY; 0: DISABLES EVENT DETECTION GLOBALLY (DEFAULT VALUE DATA).**
ENABLEACCOUNTCHANGEEVENTS	**1: ENABLES DETECTING USER ACCOUNT MODIFICATIONS; 0: DISABLES DETECTING USER ACCOUNT MODIFICATIONS (DEFAULT VALUE DATA).**
ENABLEAPPCHANGEEVENTS	**1: ENABLES DETECTING APP INSTALLS AND UNINSTALLS; 0: DISABLES DETECTING APP INSTALLS AND UNINSTALLS (DEFAULT VALUE DATA).**
ENABLEAPPFAULTEVENTS	**1: ENABLES DETECTING APP FAILURES; 0: DISABLES DETECTING APP FAILURES (DEFAULT VALUE DATA).**
EnableClipboardEvents	**1**: enables detecting clipboard activities; **0**: disables detecting clipboard activities (default value data).
EnableFileOperationMonitorEvents	**1**: enables detecting file operations; **0**: disables detecting file operations (default value data).
FileOperationMonitorList	Specifies target folders to monitor. No folder is specified by default, which means no file operation is captured by default.
EnableGenericUSBDriveEvents	**1**: enables detecting the insertion of generic redirected USB mass storage devices; **0**: disables detecting the insertion of generic redirected USB mass storage devices (default value data).
EnablePerfDataEvents	**1**: enables the session data overlay feature; **0**: disables the session data overlay feature (default value data).
EnablePopupWindowEvents	**1**: enables detecting popup window events; **0**: disables detecting popup window events (default value data).

REGISTRY VALUE	DESCRIPTION
ENABLESESSIONEVENTS	**1: ENABLES EVENT DETECTION GLOBALLY; 0: DISABLES EVENT DETECTION GLOBALLY (DEFAULT VALUE DATA).**
ENABLEACCOUNTCHANGEEVENTS	**1: ENABLES DETECTING USER ACCOUNT MODIFICATIONS; 0: DISABLES DETECTING USER ACCOUNT MODIFICATIONS (DEFAULT VALUE DATA).**
ENABLEAPPCHANGEEVENTS	**1: ENABLES DETECTING APP INSTALLS AND UNINSTALLS; 0: DISABLES DETECTING APP INSTALLS AND UNINSTALLS (DEFAULT VALUE DATA).**
ENABLEAPPFAULTEVENTS	**1: ENABLES DETECTING APP FAILURES; 0: DISABLES DETECTING APP FAILURES (DEFAULT VALUE DATA).**
EnableRDPConnectionEvents	**1**: enables detecting RDP connections; **0**: disables detecting RDP connections (default value data).
EnableRegistryOperationMonitorEvents	**1**: enables detecting Windows registry modifications; **0**: disables detecting Windows registry modifications (default value data).
RegistryOperationMonitorList	Specifies target registries to monitor. No registry is specified by default, which means no registry modification is captured by default.
EnableWebBrowsingActivities	**1**: enables detecting web browsing activities; **0**: disables detecting web browsing activities (default value data).

Here are some compatible scenarios:

- If your Session Recording is newly installed or upgraded from a release earlier than 1811 that doesn't support event detection (logging), the related registry values on each Session Recording agent are the default. Because there is no active event detection policy by default, no events are logged.

- If your Session Recording is upgraded from a release earlier than 1811 that supports event detection but has the feature disabled before your upgrade, the related registry values on each Session Recording agent remain the default. Because there is no active event detection policy by default, no events are logged.
- If your Session Recording is upgraded from a release earlier than 1811 that supports event detection and has the feature partially or fully enabled before your upgrade, the related registry values on each Session Recording agent remain the same. Because there is no active event detection policy by default, the event detection behavior remains the same.
- If your Session Recording is upgraded from 1811, the event detection (logging) policies configured in the policy console remain in use.

> **Caution:**
>
> Activating the system-defined or a custom event detection policy means to ignore the relevant registry settings on each Session Recording agent. If you do so, you can't use registry settings for event detection any more.

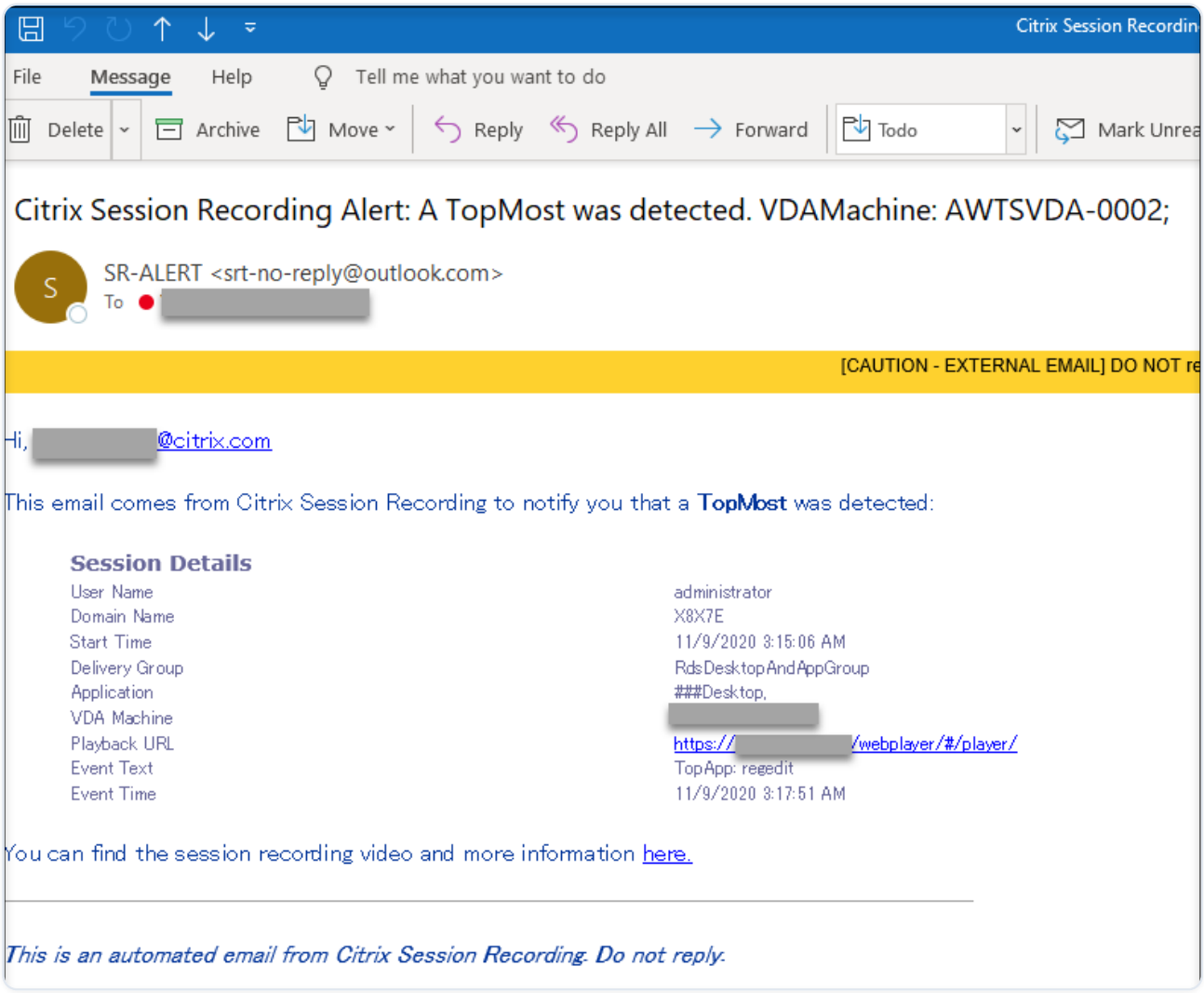
Configure event response policies

You can send an email alert when a session start is detected and take the following actions in response to logged events in recorded sessions:

- Send email alerts
- Start screen recording immediately
- 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.

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 web player. Clicking **here** opens the **All recordings** page in the web player.

Session Recording sends email alerts in the operating system language of your Session Recording server. However, if the operating system language of your Session Recording server is not one of the following languages that Session Recording supports, email alerts are sent in English by default:

- English
- French
- German
- Spanish

- Japanese
- Simplified Chinese

To customize a language to send email alerts in, find the email template called `template.en.html` under `<Session Recording server installation path>\Bin\templates`, and then change the plain text in the template to your preferred language. For example:



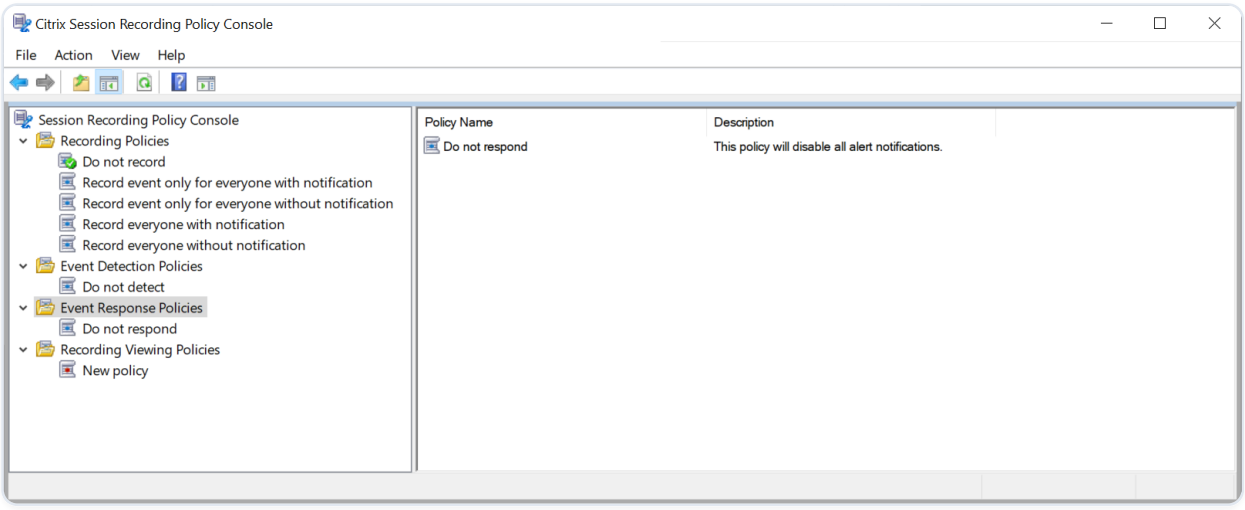
System-defined event response policy

Session Recording provides one system-defined event response policy:

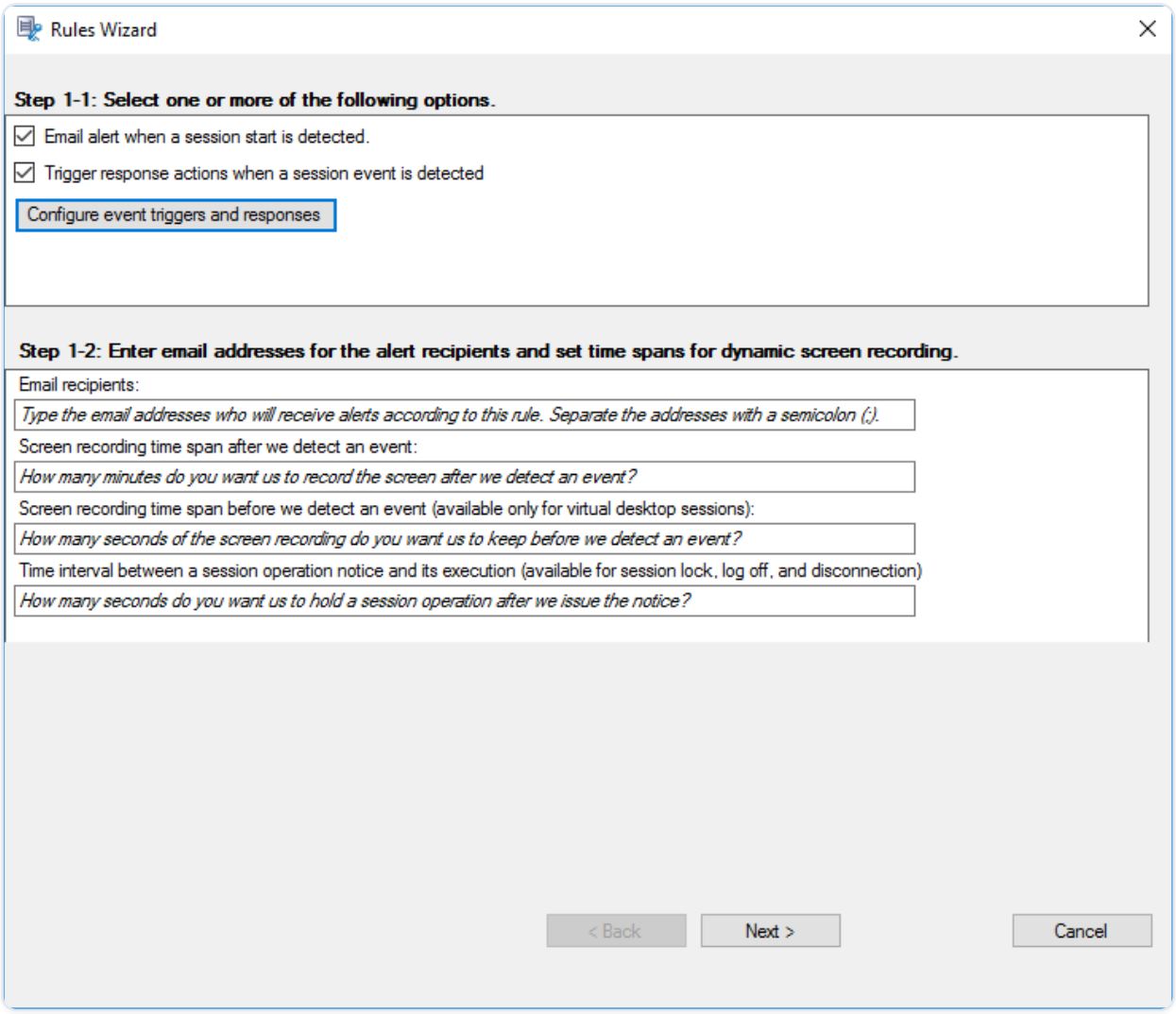
- **Do not respond**. By default, no action is taken in response to logged events in your recordings.

Create a custom event response policy

1. Log on as an authorized policy administrator to the server where the Session Recording policy console is installed.
2. Start the Session Recording policy console. By default, there is no active event response policy.



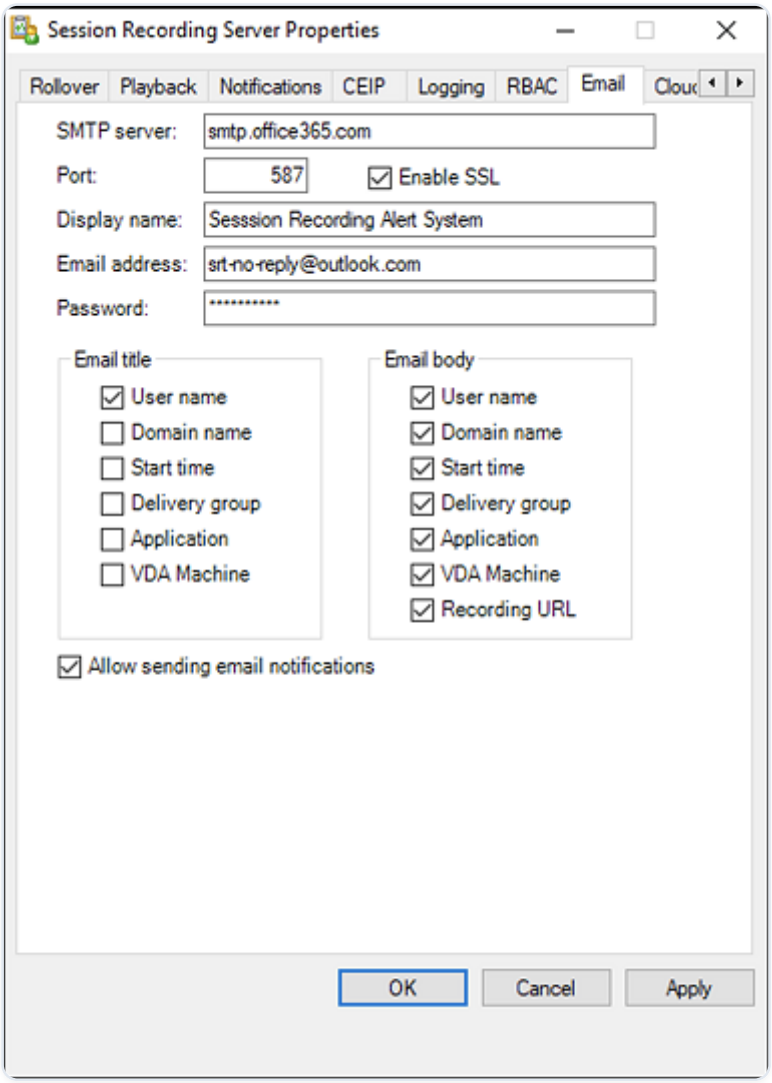
3. Select **Event Response Policies** in the left pane. From the menu bar, choose **Add New Policy**.
4. (Optional) Right-click the new event response policy and rename it.
5. Right-click the new event response policy and select **Add Rule**.
6. Select **Email alert when a session start is detected** and **Use event triggers to specify how to respond when a session event is detected** based on your needs.



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

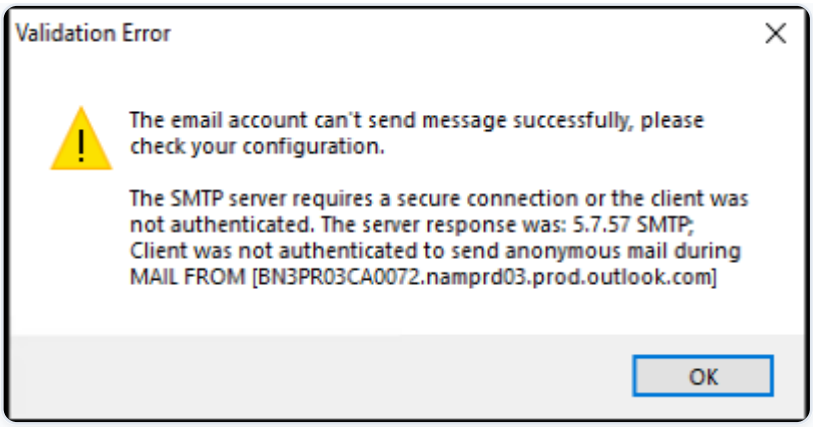
   a. Type the email addresses for the alert recipients in the **Rules** wizard.

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



Note:

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



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

c. Edit registry for accessing the 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 web player. For example, to access a web player at `https://example.com/webplayer/#/player/` , set the value data of **LinkHost** to `https://example.com` .
- Add a value, **EmailThreshold**, and set its value data to a number in the range of 1 through 100. The value data determines the maximum number of alert emails that an email sending account sends within a second. This setting helps slow down the number of emails that are being sent and thus reduces the CPU usage. If you leave the value data unspecified or set it to a number out of range, the value data falls back to 25.

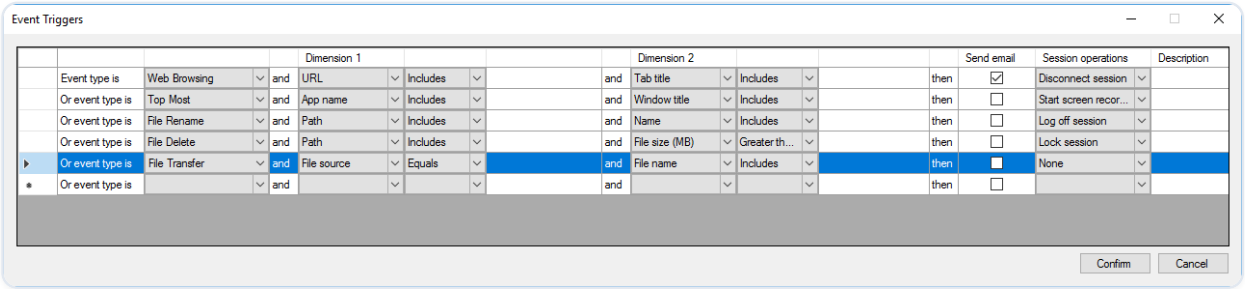
> **Note:**
>
> - Your email server might treat an email sending account as a spam bot and thus prevent it from sending emails. Before an account is allowed to send emails, an email client such as Outlook might request you to verify that the account is used by a human user.

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

8. (Optional) Configure event triggers and responses.

   After you select **Trigger response actions when a session event is detected**, the **Configure event triggers and responses** button becomes available. Click it to specify logged events that can trigger the following response actions:

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

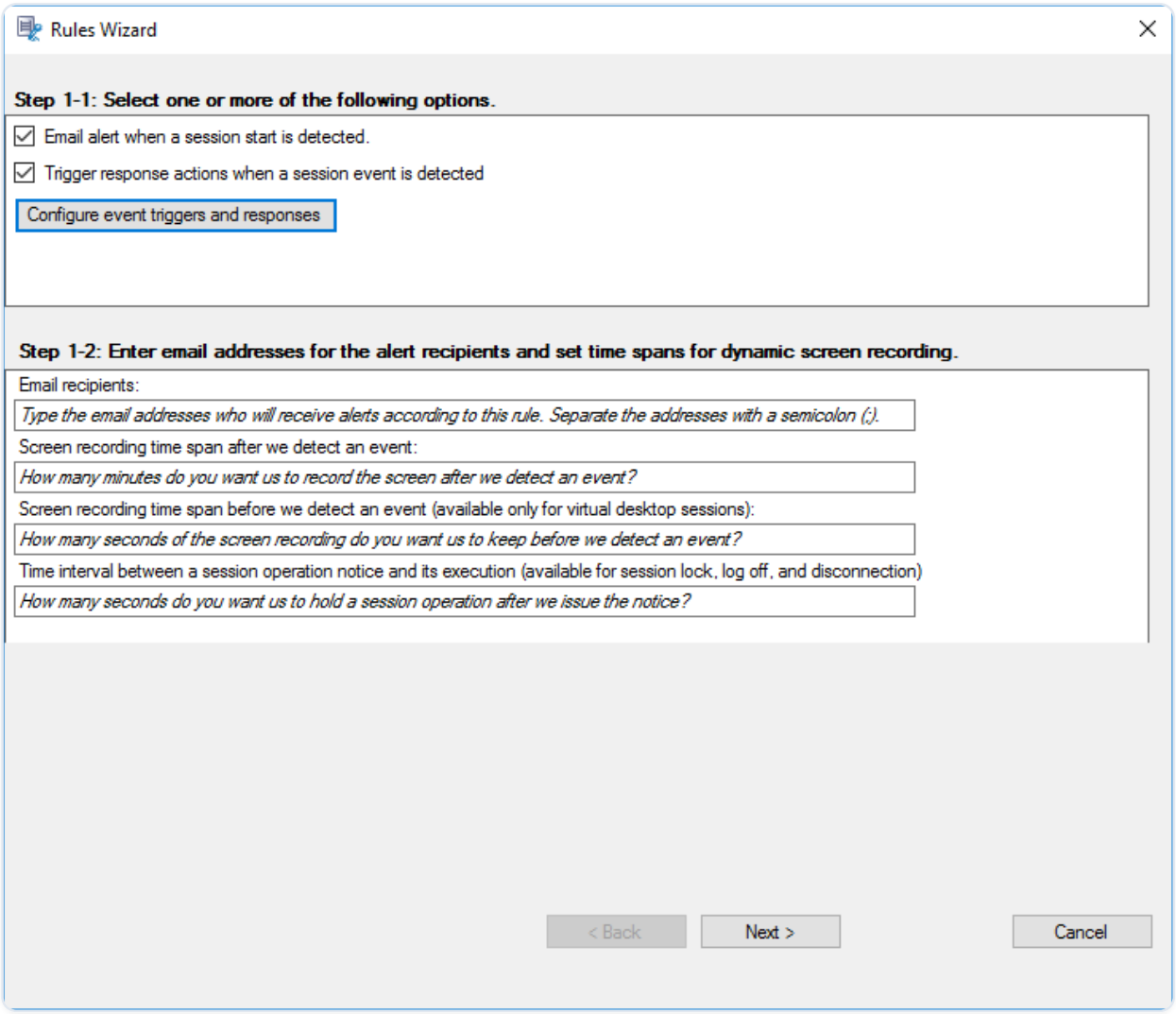


Note:

If your system language is German, French, or Spanish, ensure that the horizontal resolution of your machine is equal to or larger than 1,700 pixels. Otherwise, text truncation occurs and thus the columns of the **Event Triggers** table are not displayed completely.

You must select the event types that the active event detection policy logs. Click **Confirm** when you are finished.

Select event types from the drop-down list and set event rules through the two dimensions that are combined using the logical AND operator. You can set up to seven event triggers for each policy rule. You can also define your event triggers in the **Description** column or leave the column empty. Your defined description of an event trigger is provided in the alert emails if you have **Send email** selected and events of the type are logged. If you have **Start screen recording** selected, dynamic screen recording automatically starts when certain events occur during an event-only recording. You can set the time spans for dynamic screen recording:

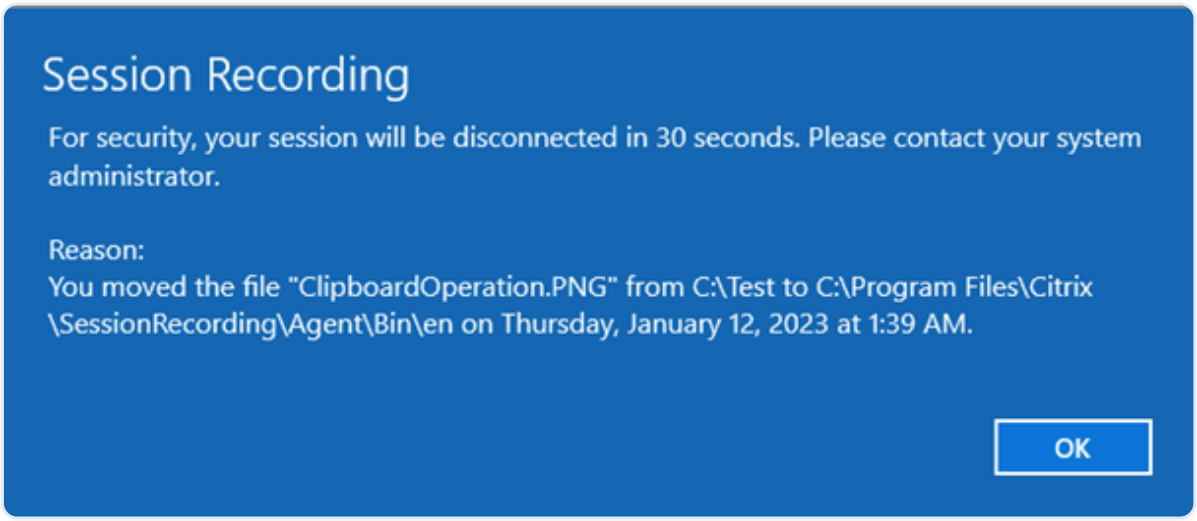


- **Screen recording time span after we detect an event**: You can configure how many minutes you want to record the screen after events are detected. If you leave the value unspecified, screen recording continues until the recorded sessions end.
- **Screen recording time span before we detect an event**: You can configure how many seconds of the screen recording you want to keep before events are detected. This feature is available only for virtual desktop sessions. The value ranges from 1 to 120. Setting the value to any of 1 through 10 makes the value 10 effective. If you leave the value

unspecified, the feature does not take effect. The actual length of the screen recording that Session Recording keeps might be a little longer than your configuration.

- If you specify any of the following actions in response to logged events in recorded sessions, you can notify users of the actions by filling the **Time interval between a session operation notice and its execution** field:
  - Lock session
  - Log off session
  - Disconnect session

> **Note:**
>
> The field value is 0 by default, which means users are not notified when you lock, log off, or disconnect them from their virtual sessions. To notify users, set an appropriate field value.
>
> For an example notice, see the following screen capture:



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

EVENT TYPE	DIMENSION	OPTION
App End		
	App name	Includes/Equals/Matches
Top Most		
	App name	Includes/Equals/Matches
	Windows title	Includes/Equals/Matches
Web Browsing		
	URL	Includes/Equals/Matches
	Tab title	Includes/Equals/Matches
	Browser name	Includes/Equals/Matches
File Create		
	Path	Includes/Equals/Matches
	File size (MB)	Greater than/Between/ Smaller than
File Rename		
	Path	Includes/Equals/Matches
	Name	Includes/Equals/Matches
File Move		
	Source path	Includes/Equals/Matches
	Destination path	Includes/Equals/Matches
	File size (MB)	Greater than/Between/ Smaller than
File Delete		

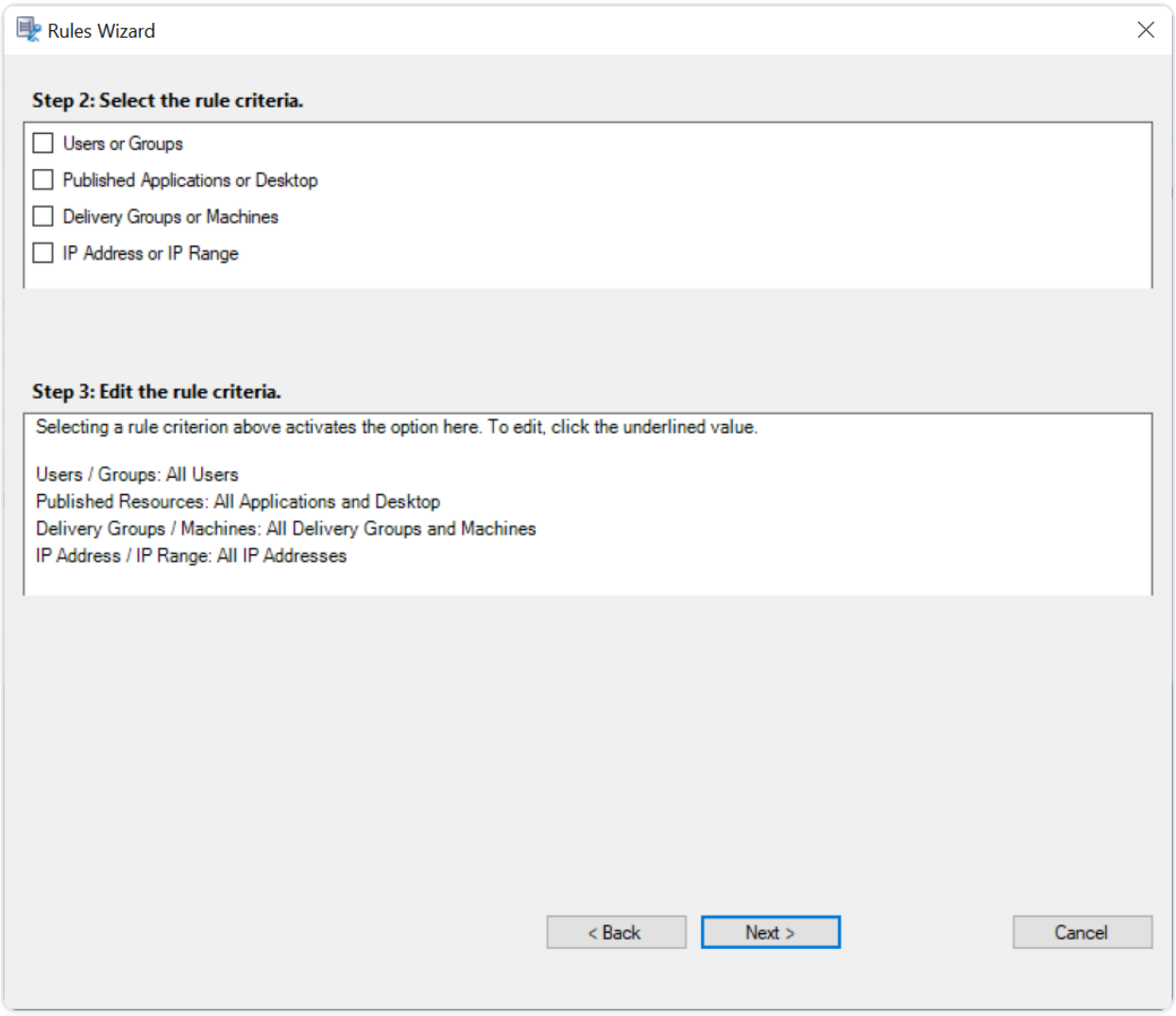
EVENT TYPE	DIMENSION	OPTION
	Path	Includes/Equals/Matches
	File size (MB)	Greater than/Between/ Smaller than
CDM USB		
	Drive letter	Equals
Generic USB		
	Device name	Includes/Equals/Matches
Idle		
	idle duration (Hrs)	Greater than
File Transfer		
	File source	Equals ("host" or "client")
	File size (MB)	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
	Value name	Includes/Equals/Matches
Registry Delete Value		
	Key name	Includes/Equals/Matches

EVENT TYPE	DIMENSION	OPTION
	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
Performance Data		
	CPU usage (%)	Greater than
	Memory usage (%	Greater than

EVENT TYPE	DIMENSION	OPTION
	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

9. Click **Next** to select and edit the rule criteria.

   Similar to when creating a custom recording policy, you can choose one or more rule criteria: **Users or Groups**, **Published Applications or Desktop**, **Delivery Groups or Machines**, and **IP Address or IP Range**. For more information, see the instructions in the Create a custom recording policy section.



Note:

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

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

High availability and load balancing

This section guides you through the following settings:

- Load balance Session Recording servers
- Configure database high availability

Load balance Session Recording servers

Session Recording supports **load balancing** across Session Recording servers. This article summarizes the **load balancing** configuration using the Citrix ADC as an example. For more information, see Configure load balancing in an existing deployment and Deploy and load balance Session Recording in Azure.

You can synchronize **load balancing** configurations among all Session Recording servers.

> **Note:**
>
> The **load balancing** feature requires Version 7.16 or later of the Session Recording server and Session Recording agent.

> **Changes to Session Recording in support of load balancing:**

- All Session Recording servers share one folder to store recording files.
- All Session Recording servers share one Session Recording Database.
- (Recommended) Install only one Session Recording policy console and all Session Recording servers share this console.

Configure load balancing

To use this feature, perform the following steps on Citrix ADC and on the various Session Recording components:

Configure load balancing (Citrix ADC part)

CONFIGURE LOAD BALANCING SERVERS

Add the Session Recording servers to the **load balancing servers** in Citrix ADC.

CONFIGURE LOAD BALANCING SERVICES

1. Add a l**oad balancing service** for each needed protocol on each Session Recording server.
2. (Recommended) Select the relevant protocol monitor to bind each service monitor.

CONFIGURE LOAD BALANCING VIRTUAL SERVERS

1. Create virtual servers with the same Citrix ADC VIP address based on the needed protocols and bind the virtual servers to the relevant **load balancing services**.
2. Configure persistence on each virtual server.

3. (Recommended) Choose LEASTBANDWITH or LEASTPACKETS as the **load balancing method** rather than the default method (LEASTCONNECTION).
4. Create a certificate to make the HTTPS virtual server UP.

Configure load balancing (Session Recording part)

ON EACH SERVER WHERE YOU INSTALLED THE SESSION RECORDING SERVER, DO THE FOLLOWING

1. (Recommended) Type the same Session Recording Database name during the Session Recording server installation.
2. If you choose the Administrator Logging feature, we recommend you type the same Administrator Logging Database name when you install each Session Recording server.
3. Share the Read/Write permission of the file storage folder with all Session Recording server machine accounts. After that, change to use the file storage folder as the shared folder in **Session Recording Server Properties**. For more information, see Specify where recordings are restored.
4. Add a value to the Session Recording server registry key at `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`.

   Value name: **EnableLB** Value data: **1** (DWORD, meaning enable)
5. If you choose the HTTP or the HTTPS protocol for the Session Recording Storage Manager message queue, create a host record for the Citrix ADC VIP address and add redirections in `C:\Windows\System32\msmq\Mapping\sample_map`. After that, restart the Message Queuing service.

   The redirection is similar to:

```
<redirections xmlns="msmq-queue-redirections.xml">

        <redirection>

                    <from>http://<ADCHost>/msmq/private$/
CitrixSmAudData</from>

                    <to>http://<LocalFqdn>/msmq/private$/
CitrixSmAudData</to>

        </redirection>
```

```
        <redirection>

                    <from>https://<ADCHost>/msmq/private$/
CitrixSmAudData</from>

                    <to>https://<LocalFqdn>/msmq/private$/
CitrixSmAudData</to>

        </redirection>

</redirections>
```

Where **\<ADCHost\>** is the created FQDN of the Citrix ADC VIP address, and **\<LocalFqdn\>** is the FQDN of the local host.

6. (Recommended) After configuring one Session Recording server registry, you can use the **<Session Recording Server installation path\>\Scripts\SrServerConfigurationSync.ps1** script to export configurations from this server registry and import the registry to the other Session Recording server registries. You can also use the **SrServerConfigurationSync.ps1** script to add redirection mapping for message queuing.

    a. On one Session Recording server, after configuring the **EnableLB** registry value, start a command prompt as an administrator and run the **powershell.exe -file SrServerConfigurationSync.ps1 –Action Export,AddRedirection –ADCHost \<ADCHost\>** command, where **\<ADCHost\>** is the created FQDN of the Citrix ADC VIP address.

    b. After the script runs, an exported registry file named **SrServerConfig.reg** is generated and an **sr_lb_map.xml** file is added to the **C:\\Windows\\System32\\msmq\\Mapping** path.

    c. On other Session Recording servers, copy **SrServerConfig.reg** generated in the preceding step, start a command prompt as an administrator, and run the **powershell.exe -file SrServerConfigurationSync.ps1 –Action Import,AddRedirection –ADCHost \<ADCHost\>** command, where **\<ADCHost\>** is the created FQDN of the Citrix ADC VIP address.

    d. After the script runs, the **EnableLB** value is added to the other Session Recording server registry keys and an **sr_lb_map.xml** file is added to the **C:\\Windows\\System32\\msmq\\Mapping** path.

ON THE MACHINE WHERE YOU INSTALLED THE SESSION RECORDING AGENT, DO THE FOLLOWING IN SESSION RECORDING AGENT PROPERTIES

- If you choose the HTTP or the HTTPS protocol for the Session Recording Storage Manager message queue, type the FQDN of the Citrix ADC VIP address in the **Session Recording Server** text box.
- If you choose the default TCP protocol for the Session Recording Storage Manager message queue, type the Citrix ADC VIP address in the **Session Recording Server** text box.

ON THE MACHINE WHERE YOU INSTALLED THE SESSION RECORDING PLAYER, DO THE FOLLOWING

Add the Citrix ADC VIP address or its FQDN as the connected Session Recording server.

ON THE SQL SERVER WHERE YOU INSTALLED THE SESSION RECORDING DATABASE, DO THE FOLLOWING

Add all the Session Recording server machine accounts to the shared Session Recording Database and assign them with the **db_owner** permission.

Configure database high availability

Session Recording supports the following solutions for database high availability based on the Microsoft SQL Server. Databases can automatically fail over when the hardware or software of a principal or primary SQL Server fails.

- Always On availability groups

  The Always On availability groups feature is a high availability and disaster-recovery solution that provides an enterprise-level alternative to database mirroring. It maximizes the availability of a set of user databases for an enterprise. It requires that the SQL Server instances reside on the Windows Server Failover Clustering (WSFC) nodes. For more information, see Always On availability groups: a high-availability and disaster-recovery solution.

- SQL Server clustering

  The Microsoft SQL clustering technology allows one server to automatically take over the tasks and responsibilities of the server that has failed. However, setting up this solution is complicated and the automatic failover is typically slower than alternatives such as SQL Server database mirroring. For more information, see Always On Failover Cluster Instances (SQL Server).

- SQL Server database mirroring

Database mirroring ensures that an automatic failover occurs in seconds if the active database server fails. This solution is more expensive than the other two solutions because full SQL Server licenses are required on each database server. You cannot use the SQL Server Express edition in a mirrored environment. For more information, see Database Mirroring (SQL Server).

Methods for configuring Session Recording with database high availability

To configure Session Recording with database high availability, do either of the following:

- Install the Session Recording Server components first and then configure database high availability for the created databases.

  You can install the Session Recording Administration components with databases configured to be installed on the prepared SQL Server instance. Then, configure database high availability for the created databases.

  - For Always On availability groups and clustering, change the SQL Server instance name to the name of the availability group listener or SQL Server network through `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\SmAudDatabaseInstance`.
  - For database mirroring, add the failover partners for databases through `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\DatabaseFailoverPartner` and `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\LoggingDatabaseFailoverPartne`

- Configure database high availability for empty databases first and then install the Session Recording Administration components.

  You can create two empty databases as the Session Recording Database and the Administrator Logging Database in the expected primary SQL Server instance and configure high availability. Then enter the SQL Server instance name when installing the Session Recording Server components:

  - To use the Always On availability groups solution, enter the name of your availability group listener.
  - To use the database mirroring solution, enter the name of your principal SQL Server.
  - To use the clustering solution, enter the network name of your SQL Server.

View recordings

Use the Session Recording player or the Session Recording web player to view, search, and bookmark recorded sessions.

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.

Session Recording player

The Session Recording player is a user interface that you access from a workstation to play recorded session files. This section provides instructions for you to:

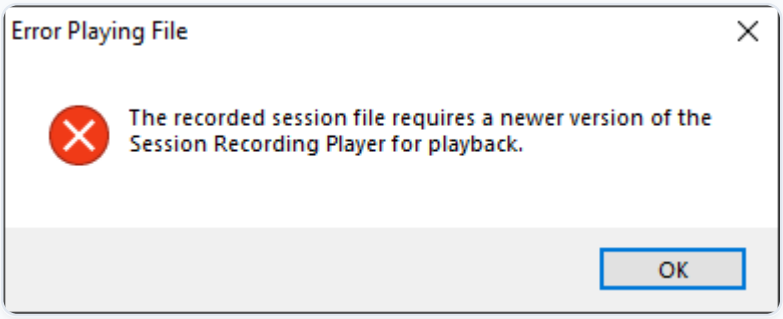
- Launch the Session Recording player
- Enable or disable live session playback
- Enable or disable playback protection
- Search for recordings
- Open and play recordings
- Cache recordings
- Highlight idle periods
- Use events and bookmarks

Launch the Session Recording Player

Launch the Session Recording player

Note:

- If a recording contains blocked content, Session Recording skips it. However, if you navigate to the blocked period, your playback shows a black screen and a message indicating that that content is blocked. To use this feature, use Session Recording 2012 and later.
- If you are using the Session Recording player 2009 and earlier to play back a recording, the following error message appears. The web player is not impacted.



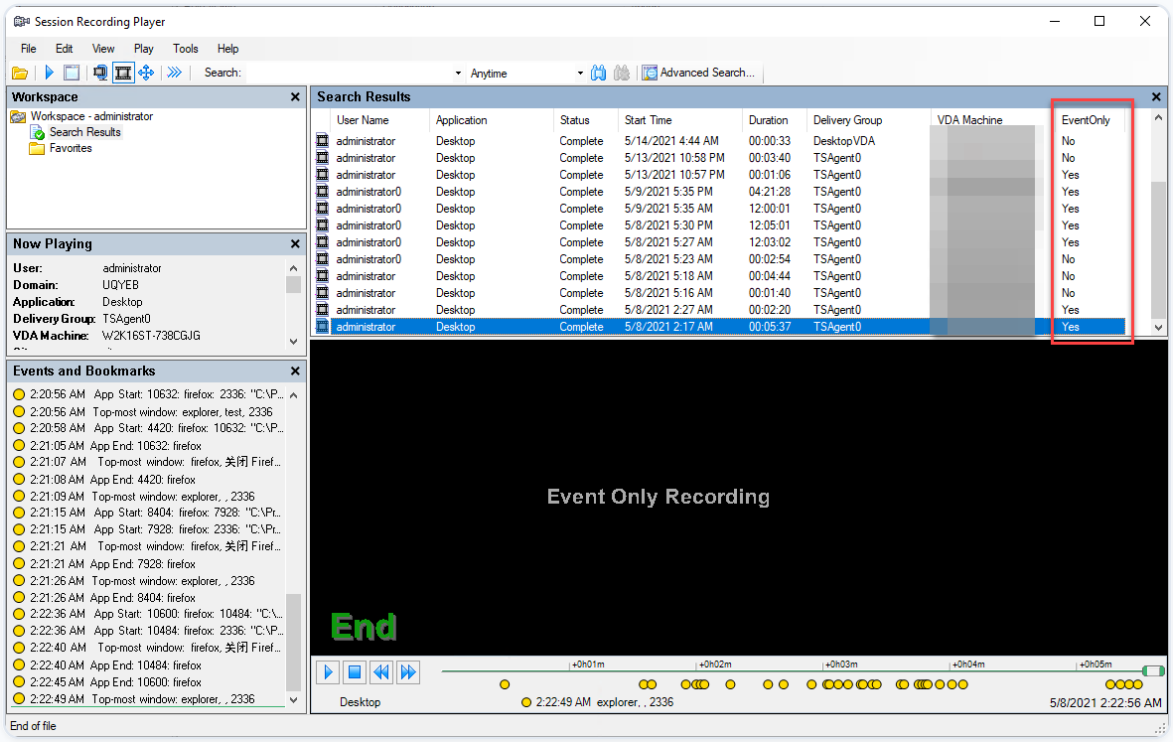
1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**. The Session Recording player appears.

Tip:

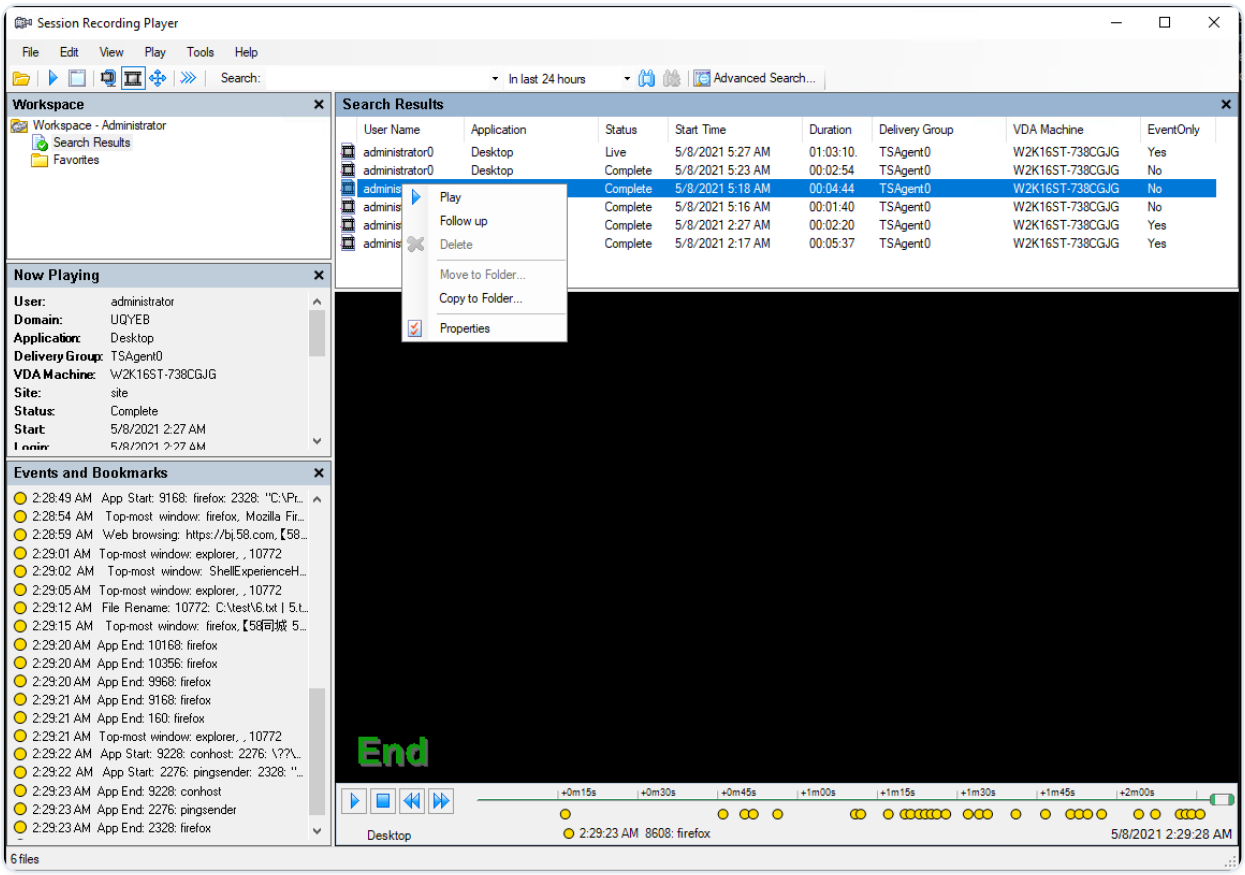
The **EventOnly** column indicates a screen recording or an event-only recording.

The following screen capture shows an example of an event-only recording being played in the Session Recording Player. All events are present in the **Events and Bookmarks**

panel and show as yellow dots in the lower part of the Session Recording Player.



To show all recording files of a recorded session, right-click a recording on the list and choose **Follow up**.



Display or hide window elements

The Session Recording player has window elements that toggle on and off.

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **View**.
4. Choose the elements that you want to display. Selecting an element causes it to appear immediately. A check mark indicates that the element is selected.

Connect to the desired Session Recording Server

You can set up your Session Recording player to connect to multiple Session Recording servers and then select a Session Recording server that it connects to. The Session Recording player can connect to only one Session Recording Server at a time.

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Tools > Options > Connections**.
4. Select the Session Recording server to which you want to connect.

Enable or disable live session playback

If sessions are recorded with the live playback feature enabled, you can view a session after or while it is being recorded. Viewing a session that is being recorded is similar to seeing actions happening live. However, there is actually a delay of 1-2 seconds when the data propagates from the VDA.

Some functionality is not available when you view live playback sessions:

- You can't assign a digital signature or view the certificate until recording is completed.
- Playback protection can't be applied until recording is complete. If playback protection is enabled, you can view live playback sessions. But they are not encrypted until the session is completed.
- You can't cache a file until recording is completed.

By default, live session playback is enabled.

1. Log on to the computer hosting the Session Recording server.
2. From the **Start** menu, choose **Session Recording Server Properties**.

3. In **Session Recording Server Properties**, click the **Playback** tab.
4. Select or clear the **Allow live session playback** check box.

Enable or disable playback protection

As a security precaution, Session Recording automatically encrypts recorded files that are downloaded for viewing in the player. Encrypted files can't be copied or played on another workstation or by another user. Encrypted files are identified with an `.icle` extension. Unencrypted files are identified with an `.icl` extension. The files remain encrypted while they reside in `%localAppData%\Citrix\SessionRecording\Player\Cache` on the player until an authorized user opens them.

We recommend that you use HTTPS to protect the transfer of data.

By default, playback protection is enabled.

1. Log on to the machine hosting the Session Recording Server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **Playback** tab.
4. Select or clear the **Encrypt session recording files downloaded for playback** check box.

Search for recordings

The Session Recording player allows you to perform quick and advanced searches and to specify options that apply to all searches. Results of searches appear in the search results area of the Session Recording player.

> **Note:**

> The player installation typically lets you set up a connection between the Session Recording player and a Session Recording server. If you fail to set up the connection, you are prompted to do so the first time you perform a search for files.

> To display all available recorded sessions, up to the maximum number of sessions that might appear in a search, perform a search without specifying any search parameters.

Perform a quick search

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Define your search criteria:
    - Enter a search criterion in the **Search** field.
    - Move the mouse pointer over the **Search** label to display a list of parameters to use as a guideline.
    - Click the arrow to the right of the **Search** field to display the text for the last 64 searches you performed.
    - Use the drop-down list to the right of the **Search** field to select a period or duration specifying when the session was recorded.
4. Click the binocular icon to the right of the drop-down list to start the search.

Perform an advanced search

Advanced searches might take up to 20 seconds to return results containing more than 150,000 entities. Citrix® recommends using more accurate search conditions such as a date range or user to reduce the result number.

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. In the **Session Recording Player** window, click **Advanced Search** on the tool bar or choose **Tools** \> **Advanced Search**.
4. Define your search criteria on the tabs of the **Advanced Search** dialog box:
    - **Common** allows you to search by domain or account authority, site, group, VDA for multi-session OS, application, or file ID.
    - **Date/Time** allows you to search date, day of week, and time of day.
    - **Events** allows you to search for Citrix-defined and custom events that are inserted to the sessions.
    - **Other** allows you to search by session name, client name, client address, and recording duration. It also allows you to specify, for this search, the maximum number of search results displayed and whether archived files are included in the search.

When you specify search criteria, the query you are creating appears in the pane at the bottom of the dialog box.

5. Click **Search** to start the search.

   You can save and retrieve advanced search queries. Click **Save** in the **Advanced Search** dialog box to save the current query. Click **Open** in the **Advanced Search** dialog box to retrieve a saved query. Queries are saved as files with an `.isq` extension.

Set search options

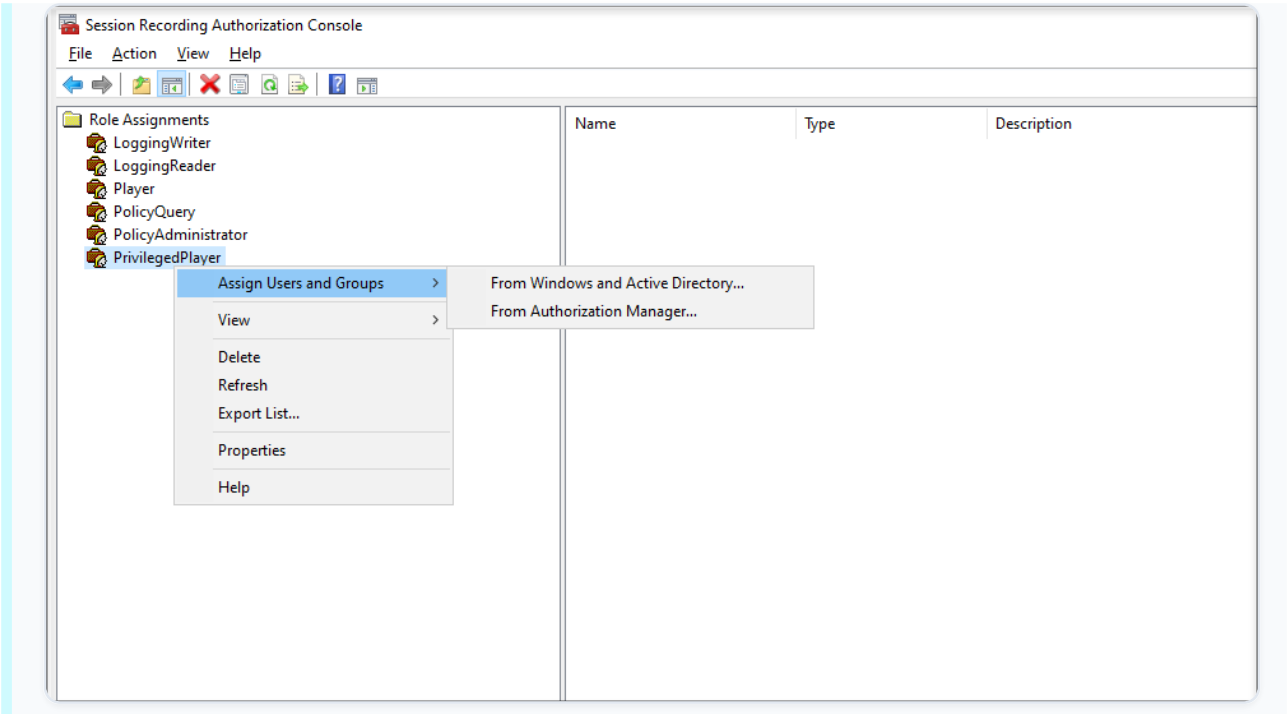
The Session Recording player search options allow you to limit the maximum number of session recordings that appear in search results and to specify whether search results include archived session files.

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Tools > Options > Search**.
4. In the **Maximum result to display** field, type the number of search results you want to display. A maximum of 500 results can be displayed.
5. To set whether archived files are included in searches, select or clear **Include archived files**.

Place access restrictions on recordings

You place access restrictions on target recordings in addition to role-based access control through recording viewing policies. Restricted recordings are accessible only to users and user groups that are assigned the **PrivilegedPlayer** role through the Session Recording Authorization Console.

> **Note:**
>
> Placing access restrictions on live recordings is not supported.

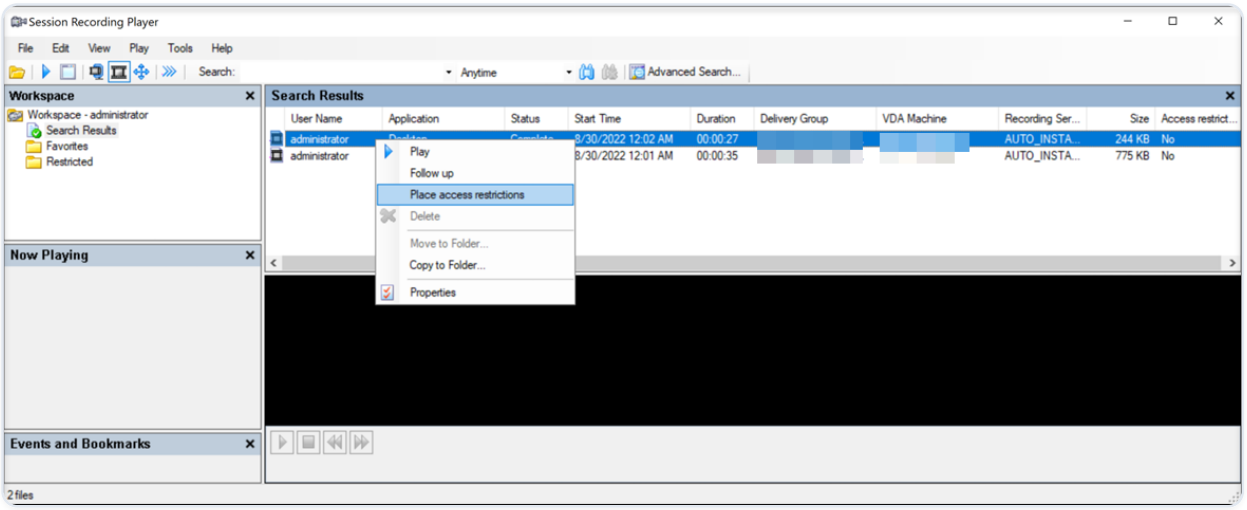


The following section walks you through the process of placing and removing access restrictions on target recordings.

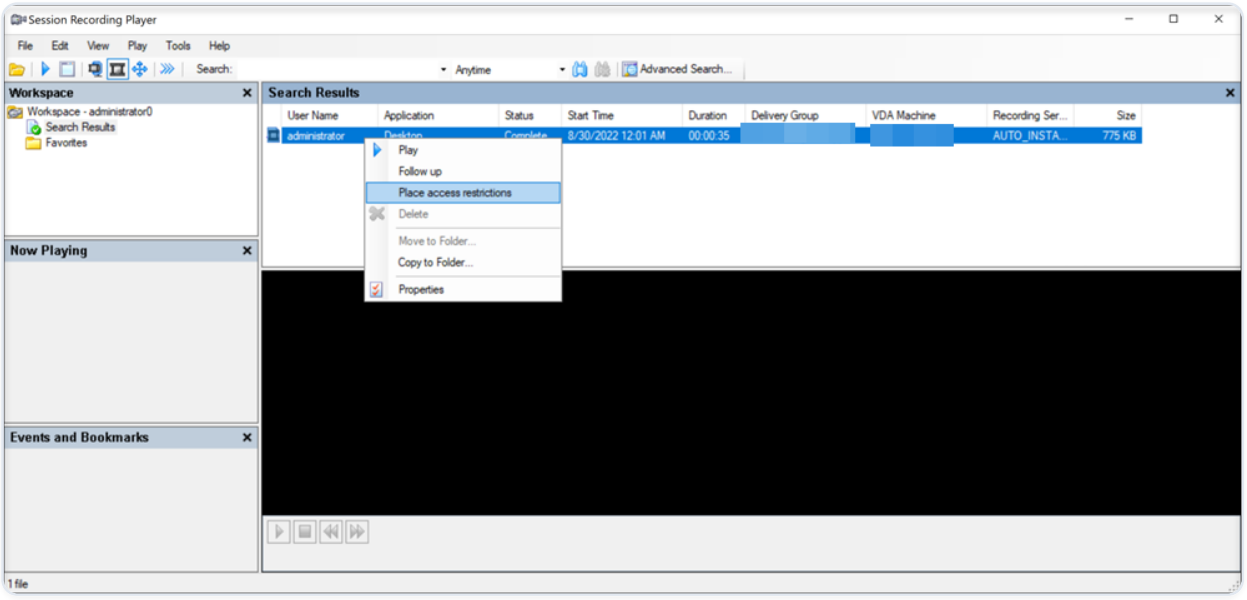
1. Log on to the machine where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Select **Search Results** in the **Workspace** pane.
4. In the **Search Results** area, select one or more target recordings.
5. Right-click and select **Place access restrictions**.

   Users and user groups, assigned either the **Player** or the **PrivilegedPlayer** role, are allowed to place access restrictions on recordings. The **Restricted** menu is available only for users and user groups assigned the **PrivilegedPlayer** role.

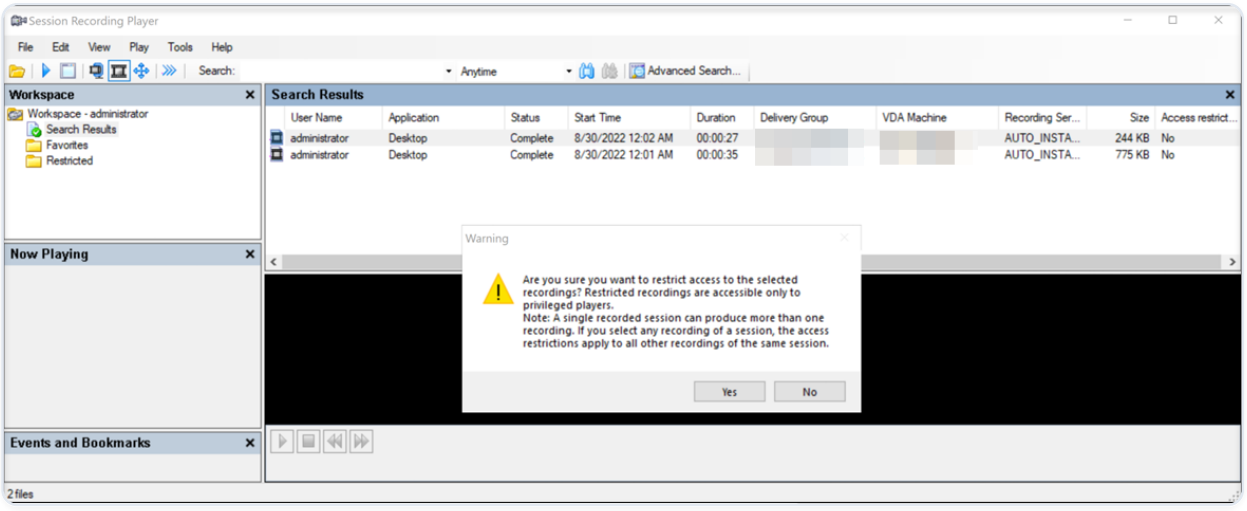
   View for the **PrivilegedPlayer** role:



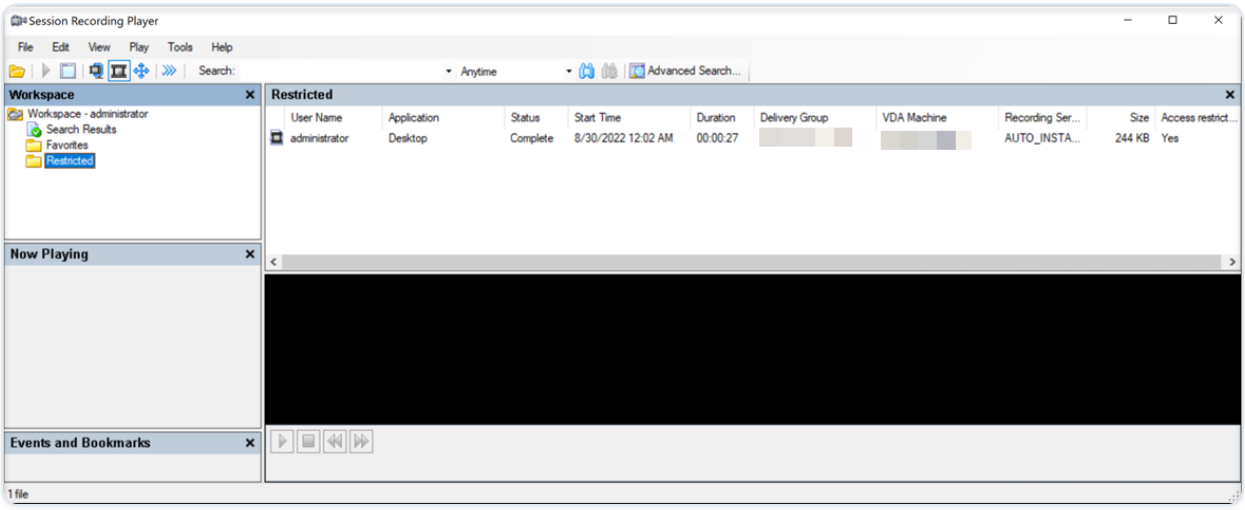
View for the **Player** role:



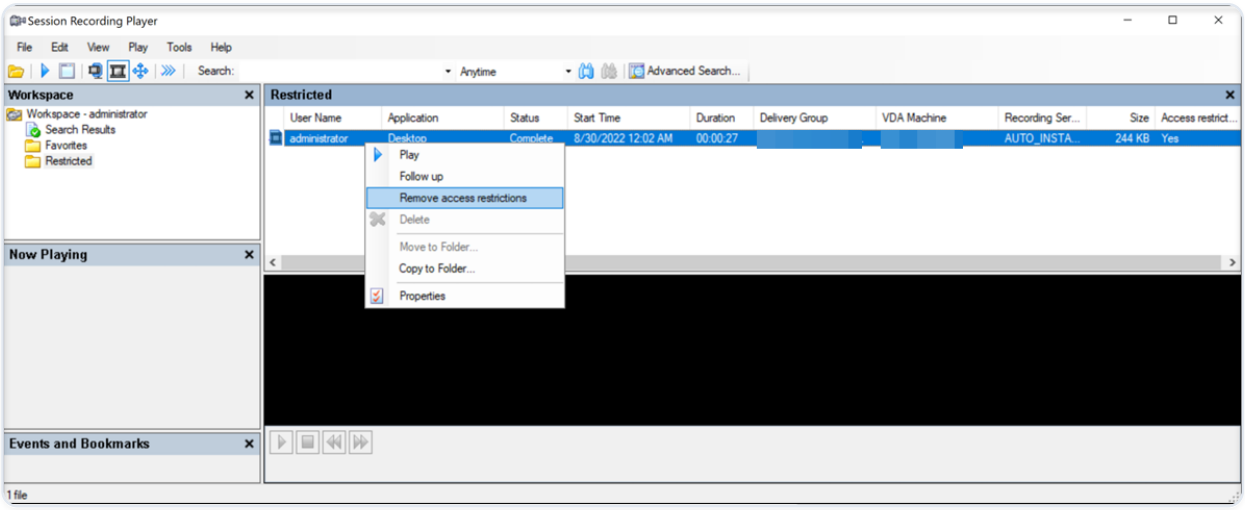
6. Click **Yes**.



7. Verify that the selected recordings on which you placed access restrictions are moved from the **Search Results** area to the **Restricted** area.



8. In the **Restricted** area, remove access restrictions as needed. With access restrictions removed, recordings are moved back to the **Search Results** area.



Open and play recordings

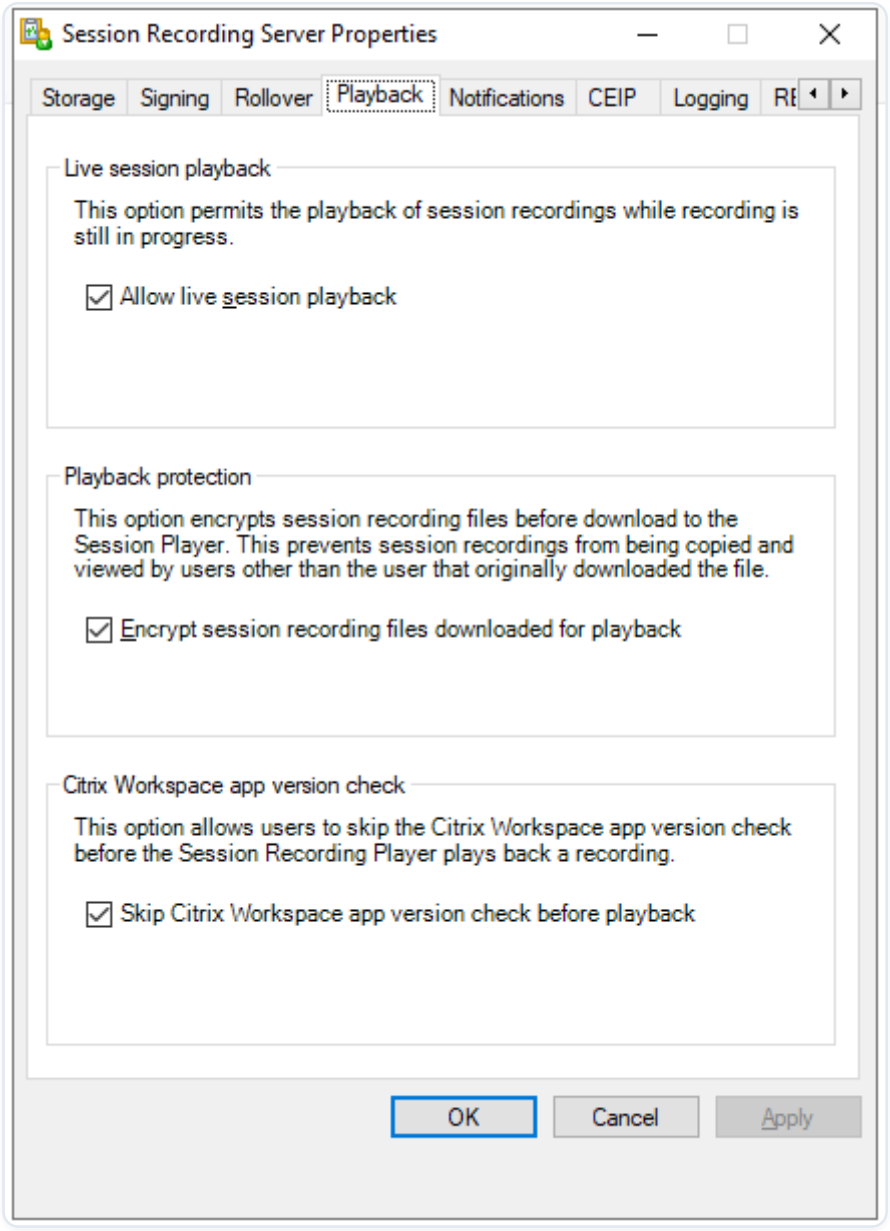
Open recordings

You can open session recordings in the Session Recording player in three ways:

- Perform a search using the Session Recording player. Recorded sessions that meet the search criteria appear in the search results area.
- Access recorded session files directly from your local disk drive or a shared drive.
- Access recorded session files from a Favorites folder.

When you open a file that was recorded without a digital signature, a warning message appears. It says that the origin and integrity of the file were not verified. If you are confident of the integrity of the file, click **Yes** in the warning window to open the file.

The Session Recording player checks the Citrix Workspace™ app version before playing back a recorded session. If the player doesn't support the Citrix Workspace app version, an error is returned. To eliminate the error, select **Skip Citrix Workspace app version check** in **Session Recording Server Properties**.



Note:

The Administrator Logging feature of Session Recording allows you to log the downloads of recordings in the Session Recording player. For more information, see Administrator Logging.

Open a recording in the search results area

1. Log on to the machine where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Perform a search.
4. If the search results area is not visible, select **Search Results** in the Workspace pane.
5. In the search results area, select the session you want to play.
6. Do any of the following:

   - Double-click the session.
   - Right-click and select **Play**.
   - From the **Session Recording Player** menu bar, choose **Play > Play**.

Open a recording by accessing the file

The name of a recording file begins with `i_`, followed by a unique alphanumeric file ID and then the `.icl` or `.icle` extension. The `.icl` extension denotes the recordings without playback protection applied. The `.icle` extension denotes the recordings with playback protection applied. Recorded session files are saved in a folder that incorporates the date the sessions were recorded. For example, the file for a session recorded on December 22, 2014, is saved in the folder path `2014\12\22`.

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Do any of the following:

   - From the **Session Recording Player** menu bar, choose **File > Open** and browse for the file.
   - Using Windows Explorer, navigate to the file and drag the file to the **Player** window.
   - Using Windows Explorer, navigate to and double-click the file.
   - If you created Favorites in the Workspace pane, select **Favorites** and open the file from the Favorites area in the same way you open files from the search results area.

Use favorites

Creating the **Favorites** folders allows you to quickly access recordings that you view frequently. These **Favorites** folders reference recorded session files that are stored on your workstation or on

a network drive. You can import and export these files to other workstations and share these folders with other Session Recording player users.

> **Note:**
>
> Only users with access rights to the Session Recording player can download the recorded session files associated with the **Favorites** folders. Contact your Session Recording administrator for the access rights.

To create a **Favorites** subfolder:

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. In the **Session Recording Player** window, select the **Favorites** folder in your Workspace pane.
4. From the menu bar, choose **File > Folder > New Folder**. A new folder appears under the **Favorites** folder.
5. Type the folder name, then press **Enter** or click anywhere to accept the new name.

Use the other options that appear in the **File > Folder** menu to delete, rename, move, copy, import, and export the folders.

Play recordings

After you open a recorded session in the Session Recording player, you can navigate through the recorded sessions using these methods:

- Use the player controls to play, stop, pause, and increase or decrease playback speed.
- Use the seek slider to move forward or backward.

You can also navigate through the recorded session by going to the inserted markers and custom events.

> **Note:**

- During playback of a recorded session, a second mouse pointer might appear. The second pointer appears at the point in the recording when the user navigated within Internet Explorer and clicked an image that was originally larger than the screen but was scaled down automatically by Internet Explorer. While only one pointer appears during the session, two might appear during playback.
- This version of Session Recording doesn't support SpeedScreen Multimedia Acceleration and the Flash quality adjustment policy setting. When this option is enabled, playback displays a black square.
- When you record a session with a resolution higher than or equal to 4096 x 4096, there might be fragments in the recording appearance.

Use the player controls

You can click the player controls in the lower part of the player window or access them by choosing **Play** from the **Session Recording Player** menu bar.

PLAYER CONTROL	FUNCTION
	Plays the selected session file.
	Pauses playback.
	Stops playback. If you click **Stop**, then **Play**, the recording restarts at the beginning of the file.
	Halves the current playback speed down to a minimum of one-quarter of the normal speed.
	Doubles the current playback speed up to a maximum of 32 times the normal speed.

Use the seek slider

Use the seek slider in the lower part of the player window to jump to a different position within the recorded session. You can drag the seek slider to the point in the recording you want to view or click anywhere on the slider bar to move to that location.

You can also use the following keyboard keys to control the seek slider:

KEYBOARD KEY	FUNCTION
Home	Seeks to the beginning.
End	Seeks to the end.
Right Arrow	Seeks forward five seconds.
Left Arrow	Seeks backward five seconds.
Move the mouse wheel one notch down	Seeks forward 15 seconds.
Move the mouse wheel one notch up	Seeks backward 15 seconds.
Ctrl + Right Arrow	Seeks forward 30 seconds.
Ctrl + Left Arrow	Seeks backward 30 seconds.
Page Down	Seeks forward one minute.
Page Up	Seeks backward one minute.
Ctrl + Move the mouse wheel one notch down	Seeks forward 90 seconds.
Ctrl + Move the mouse wheel one notch up	Seeks backward 90 seconds.
Ctrl + Page Down	Seeks forward six minutes.
Ctrl + Page Up	Seeks backward six minutes.

To adjust the speed of the seek slider: From the **Session Recording Player** menu bar, choose **Tools > Options > Player** and drag the slider to increase or decrease the seek response time. A faster response time requires more memory. The response might be slow depending on the size of the recordings and your machine's hardware.

Change the playback speed

You can set a playback speed in exponential increments from one-quarter normal playback speed to 32 times normal playback speed.

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Play > Play Speed**.

4. Choose a speed option.

The speed adjusts immediately. Text indicating the exponential rate appears briefly in green in the lower part of the player window.

Highlight the idle periods of recorded sessions

Idle periods of a recorded session are the portions in which no action takes place. The Session Recording player can highlight the idle periods of recorded sessions during playback. The option is **On** by default. For more information, see Highlight idle periods.

Skip over spaces where no action occurred

Fast review mode allows you to set the player to skip the portions of recorded sessions where no action takes place. This setting saves time for playback viewing. However, it doesn't skip animated sequences such as animated mouse pointers, flashing cursors, or displayed clocks with second hand movements.

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Play > Fast Review Mode**.

The option toggles on and off. Each time you choose it, its status appears briefly in green in the player window.

Change the playback display

You can do the folloing to change how recorded sessions appear in the player window:

- Pan and scale the image.
- Show playback in full screen
- Display the player window in a separate window
- Display a red border around the recorded session to differentiate it from the player window background.

DISPLAY THE PLAYER WINDOW IN FULL SCREEN

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **View > Player Full Screen**.
4. To return to the original size, press **Esc** or **F11**.

DISPLAY THE PLAYER WINDOW IN A SEPARATE WINDOW

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **View > Player in Separate Window**. A new window appears, containing the player window. You can drag and resize the window.
4. To embed the player window in the main window, choose **View > Player in Separate Window**, or press **F10**.

SCALE THE SESSION PLAYBACK TO FIT THE PLAYER WINDOW

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Play > Panning and Scaling > Scale to Fit**.

    - **Scale to Fit (Fast Rendering)** shrinks images while providing good quality. Images are drawn quicker than using the High Quality option but the images and texts are not sharp. Use this option if you are experiencing performance issues when using the High Quality mode.
    - **Scale to Fit (High Quality)** shrinks images while providing high quality. Using this option can cause the images to be drawn more slowly than the Fast Rendering option.

PAN THE IMAGE

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Play > Panning and Scaling > Panning**. The pointer changes to a hand. And a small representation of the screen appears in the top right of the player window.
4. Drag the image. The small representation indicates where you are in the image.
5. To stop panning, choose one of the scaling options.

DISPLAY A RED BORDER AROUND SESSION RECORDING

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Tools > Options > Player**.
4. Select the **Show border around session recording** check box.

If the **Show border around session recording** check box is not selected, you can temporarily view the red border by clicking and holding down the left mouse button while the pointer is in the player window.

Cache recordings

Each time you open a recorded session file, the Session Recording player downloads the file from the location where the recordings are stored. If you download the same files frequently, you can save download time by caching the files on your workstation. Cached files are stored on your workstation in this folder:

userprofile**AppData**Local**Citrix**SessionRecording**Player**Cache**

You can specify how much disk space is used for the cache. When the recordings fill the specified disk space, Session Recording deletes the oldest, least used recordings to make room for new recordings. You can empty the cache at any time to free up disk space.

Enable caching

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Tools > Options > Cache**.
4. Select the **Cache downloaded files on local machine** check box.
5. To limit the amount of disk space used for caching, select the **Limit amount of disk space to use** check box and specify the number of MB to be used for cache.
6. Click **OK**.

Empty caches

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **Tools > Options > Cache**.
4. Select the **Cache downloaded files on local machine** check box.
5. In the Session Recording player, choose **Tools > Options > Cache**.
6. Click **Purge Cache** and **OK** to confirm the action.

Highlight idle periods

Idle periods of a recorded session are the portions in which no action takes place. The Session Recording player can highlight the idle periods of recorded sessions during playback. The option is **On** by default.

Note: Idle periods are not highlighted when playing back live sessions with the Session Recording player.

To highlight the idle periods of recorded sessions, do the following:

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. From the **Session Recording Player** menu bar, choose **View** \> **Idle Periods** and select or clear the check box.

Use events and bookmarks

You can use events and bookmarks to help you navigate through recorded sessions.

Citrix-defined events are inserted to sessions while the sessions are recorded. You can also use the Event API and a third-party application to insert custom events. Events are saved as part of the session file. You cannot delete or alter them using the Session Recording player.

Bookmarks are markers that you insert in a recorded session during session playback using the Session Recording player. After insertion, bookmarks are associated with the recorded session until you delete them. However, they are not saved as part of the session file but stored as separate `.iclb` files in the **Bookmarks** cache folder on the Session Recording player, for example, C:\Users\SpecificUser\AppData\Local\Citrix\SessionRecording\Player\Bookmarks, with the same file name as the `.icl` recording file. To play back a recording using bookmarks on a different player, copy the `.iclb` files to the **Bookmarks** cache folder on that player. By default, each bookmark is labeled with the text "Bookmark," but you can change it to any text annotation up to 128 characters long.

Events appear as yellow dots and bookmarks appear as blue squares in the lower part of the player window. Moving the mouse over the dots and squares displays the text label associated with them. You can also display the events and bookmarks in the **Events and Bookmarks** list of the Session Recording player. They appear in this list with their text labels and the times in the recorded session at which they appear, in chronological order.

You can use events and bookmarks to help you navigate through recorded sessions. By going to an event or bookmark, you can skip to the point in the recorded session where the event or bookmark is inserted.

Display events and bookmarks in the list

The **Events and Bookmarks** list displays the events and bookmarks inserted in the recorded session that is currently playing. It can show events only, bookmarks only, or both.

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Move the mouse pointer to the **Events and Bookmarks** list area and right-click to display the menu.
4. Choose **Show Events Only**, **Show Bookmarks Only**, or **Show All**.

Insert a bookmark

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Begin playing the recorded session to which you want to add a bookmark.
4. Move the seek slider to the position where you want to insert the bookmark.
5. Move the mouse pointer to the player window area and right-click to display the menu.
6. Add a bookmark with the default **Bookmark** label or create an annotation:
    - To add a bookmark with the default **Bookmark** label, choose **Add Bookmark**.
    - To add a bookmark with a descriptive text label that you create, choose **Add Annotation**. Type the text label that you want to assign to the bookmark, up to 128 characters. Click **OK**.

Add or change an annotation

After a bookmark is created, you can add an annotation to it or change its annotation.

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Begin playing the recorded session containing the bookmark.
4. Ensure that the **Events and Bookmarks** list is displaying bookmarks.
5. Select the bookmark in the **Events and Bookmarks** list and right-click to display the menu.
6. Choose **Edit Annotation**.

7. In the window that appears, type the new annotation and click **OK**.

Delete a bookmark

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Begin playing the recorded session containing the bookmark.
4. Ensure that the **Events and Bookmarks** list is displaying bookmarks.
5. Select the bookmark in the **Events and Bookmarks** list and right-click to display the menu.
6. Choose **Delete**.

Go to an event or bookmark

Going to an event or bookmark causes the Session Recording player to go to the point in the recorded session where the event or bookmark is inserted.

1. Log on to the workstation where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Begin playing a session recording containing events or bookmarks.
4. Go to an event or bookmark:
    - In the lower part of the player window, click the dot or square representing the event or bookmark to go to the event or bookmark.
    - In the **Events and Bookmarks** list, double-click the event or bookmark to go to it. To go to the next event or bookmark, select any event or bookmark from the list, right-click to display the menu, and choose **Seek to Bookmark**.

Session Recording web player

The web player lets you use a web browser to view and play back recorded sessions. Using the web player, you can:

- Search for recordings by using filters.
- View and play back both live and completed recordings with tagged events listed in the right pane.
- configure cache memory for storing recordings during playback.
- Highlight idle periods.

- Leave comments about a recording and set comment severities.
- Share URLs of recordings.
- View graphical event statistics for each recording.
- View data points related to each recorded session.

Access the web player

The URL of the web player website is `http(s)://<FQDN of Session Recording server>/WebPlayer`. To ensure the use of HTTPS, add an SSL binding to the website in IIS and update the `SsRecWebSocketServer.config` configuration file.

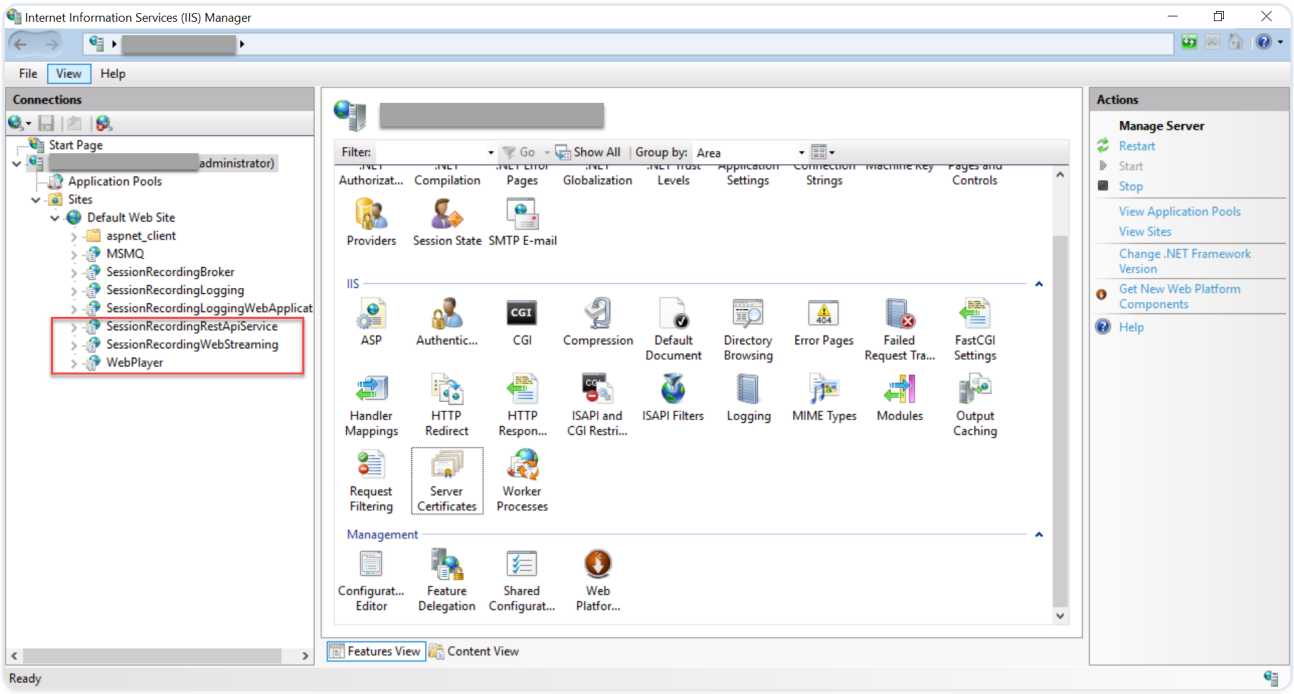
> **Note:**
>
> - When logging on to the web player website, domain users do not need to enter credentials while non-domain users must.
> - Supported browsers include Google Chrome, Microsoft Edge, and Firefox.
> - To have the web player function properly, make sure you enable WebGL in Firefox.

> This article guides you through the process of installing and enabling the web player and the process of configuring HTTPS.

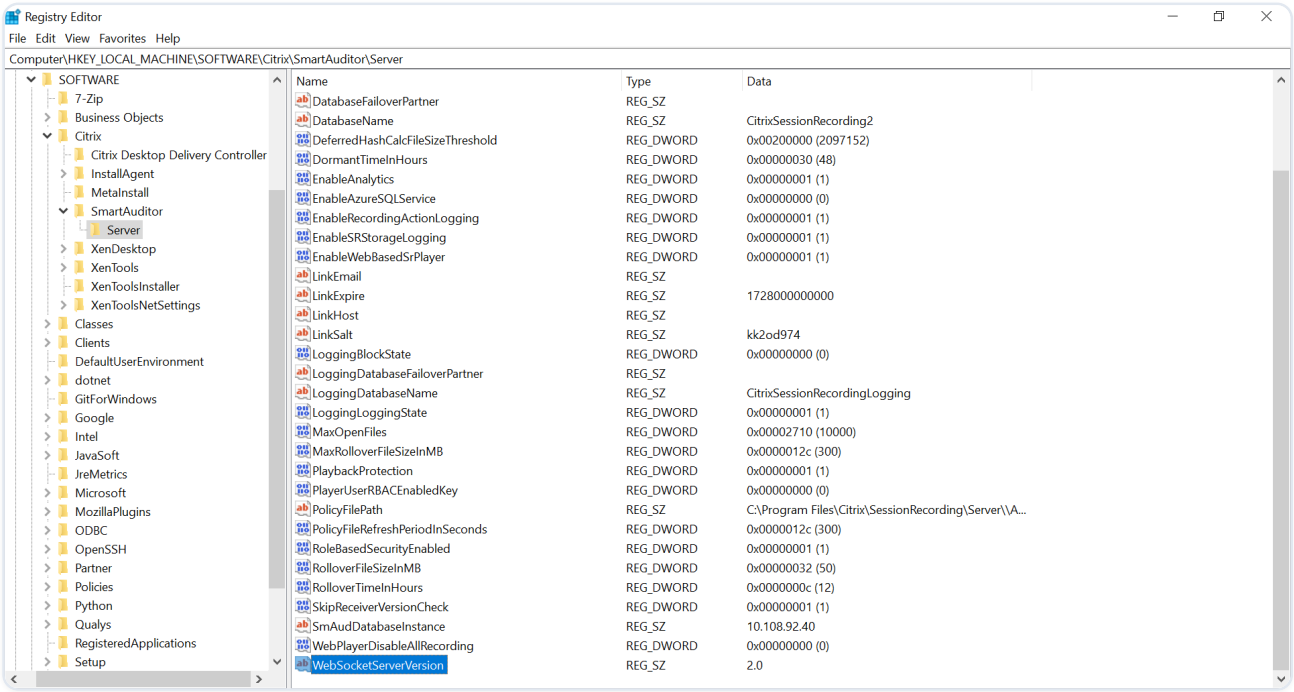
Install the web player

Install the web player on the Session Recording server only. Double-click SessionRecordingWebPlayer.msi and follow the instructions to complete your installation. For more information about installing Session Recording, see Install, upgrade, and uninstall.

Starting from Version 2103, Session Recording migrates the WebSocket server to IIS. With the web player installed, the **SessionRecordingRestApiService**, **SessionRecordingWebStreaming**, and **WebPlayer** applications appear in IIS.



A fresh installation of Session Recording 2103 and later connects your web browser to the WebSocket server hosted in IIS when you access the web player website. The WebSocket server hosted in IIS is versioned 2.0, as indicated by the registry value **WebSocketServerVersion** under the registry key at `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 WebSocket server. To connect to the WebSocket server hosted in IIS, run the **<Session Recording server installation path\>\Bin\SsRecUtils.exe -enablestreamingservice** command. To connect back to the Python-based WebSocket server, run the **<Session Recording server installation path\>\Bin\SsRecUtils.exe -disablestreamingservice** command. The Python-based WebSocket server is versioned 1.0.

Enable the web player

The web player is enabled by default.

- To disable the web player, start a Windows command prompt and run the `<Session Recording Server installation path>\Bin\SsRecUtils.exe –disablewebplayer` command.
- To enable the web player, start a Windows command prompt and run the `<Session Recording Server installation path>\Bin\SsRecUtils.exe -enablewebplayer` command.

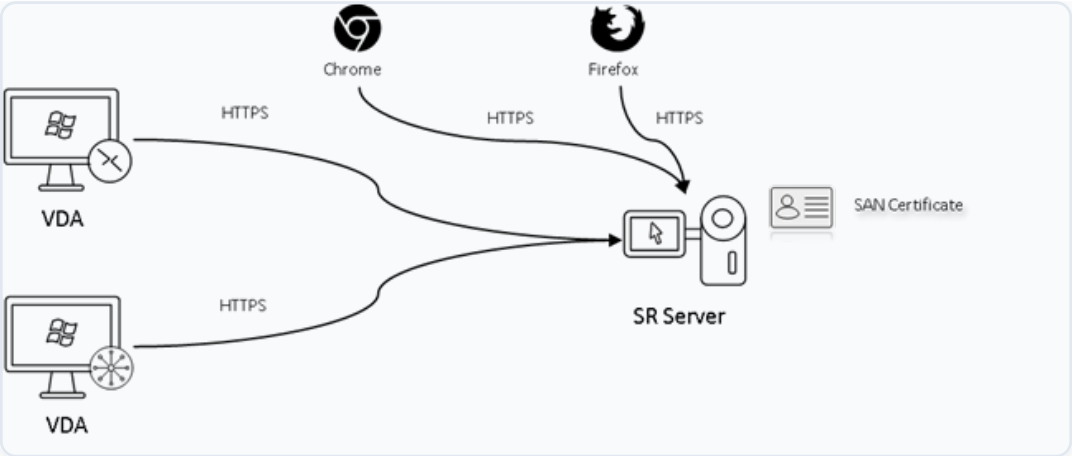
Configure HTTPS

The URL of the web player website is `http(s)://<FQDN of Session Recording server>/WebPlayer`. To ensure the use of HTTPS, add an SSL binding to the website in IIS and update the `SsRecWebSocketServer.config` configuration file.

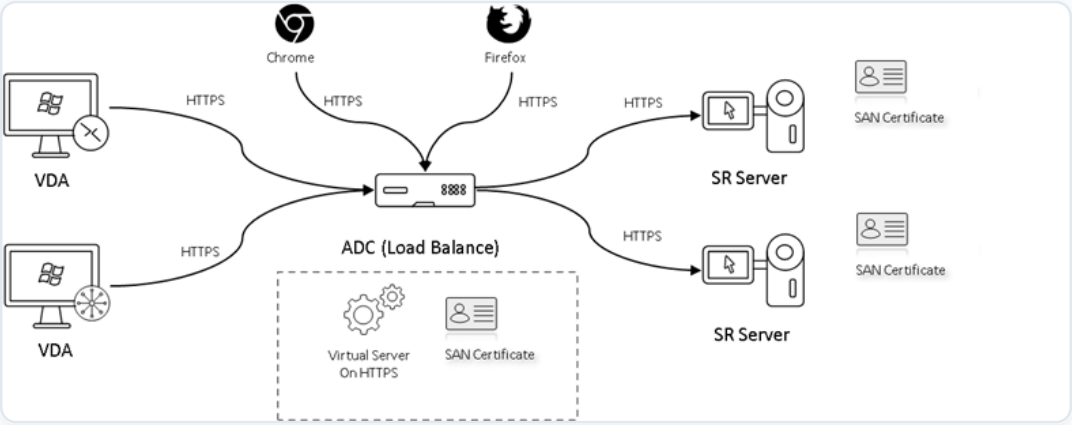
> **Note:**
>
> When logging on to the web player website, domain users do not need to enter credentials while non-domain users must.
>
> To use HTTPS to access the web player website, complete the following steps:

1. Add an SSL binding in IIS.
   a. Obtain an SSL certificate in PEM format from a trusted Certificate Authority (CA).

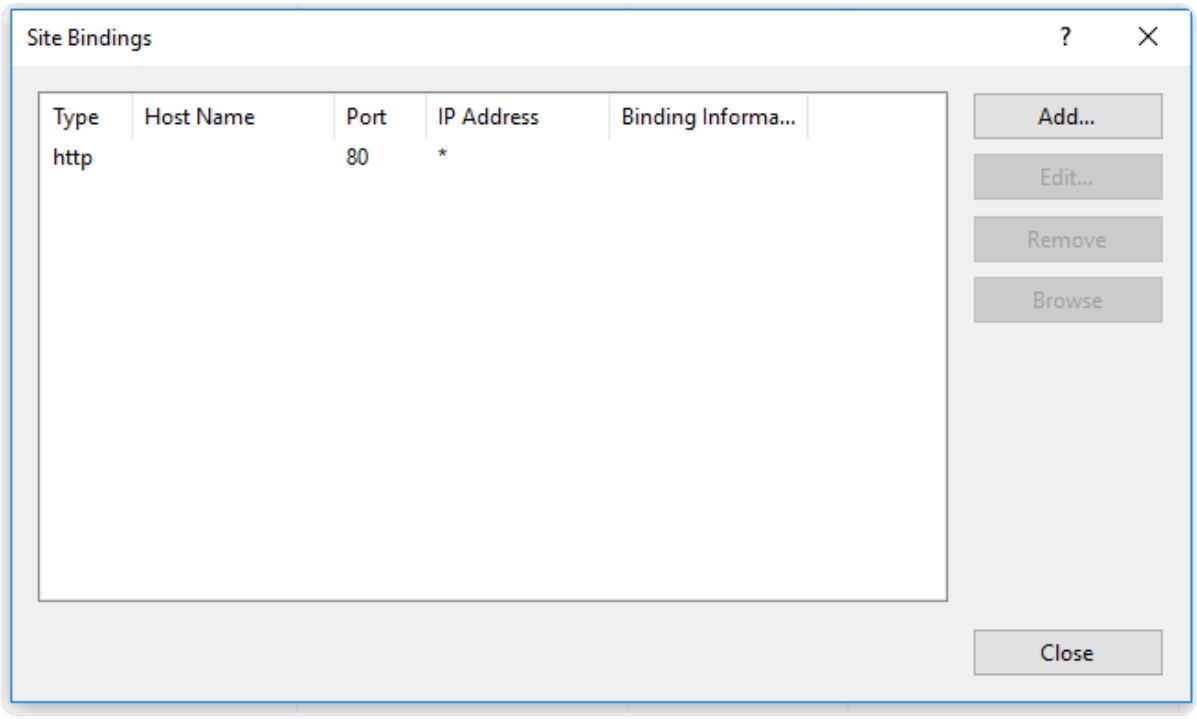
      > **Note:**
      >
      > Most popular browsers such as Google Chrome and Firefox no longer support the common name in a Certificate Signing Request (CSR). They enforce Subject Alternative Name (SAN) in all publicly trusted certificates. To use the web player over HTTPS, take the following actions accordingly:
      >
      > - When a single Session Recording Server is in use, update the certificate of the Session Recording Server to a SAN certificate.



- When load balancing is in use, ensure that a SAN certificate is available both on Citrix ADC and on each Session Recording Server.

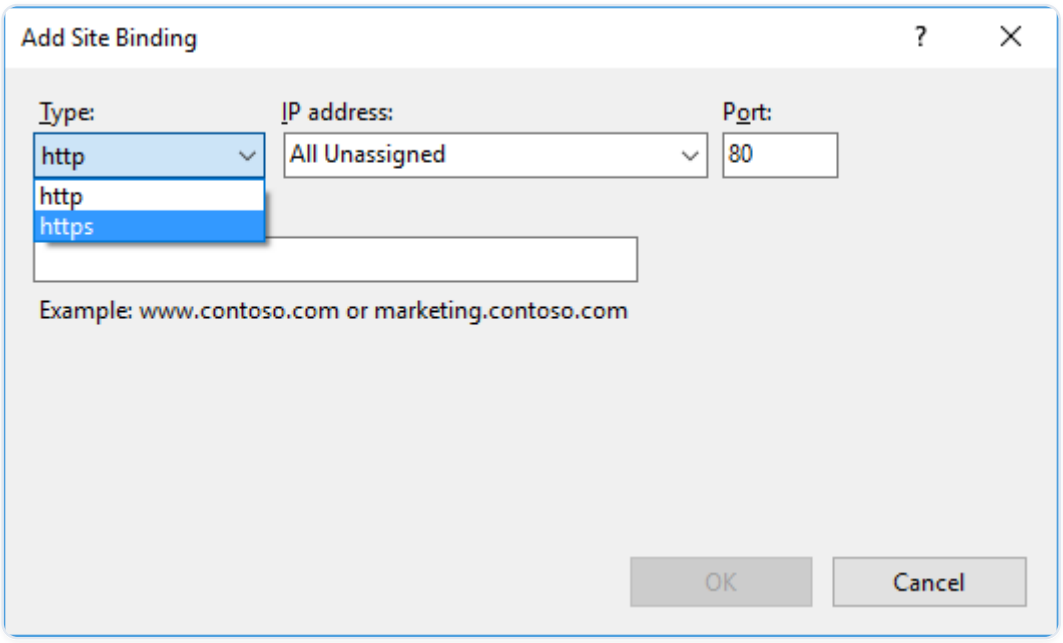


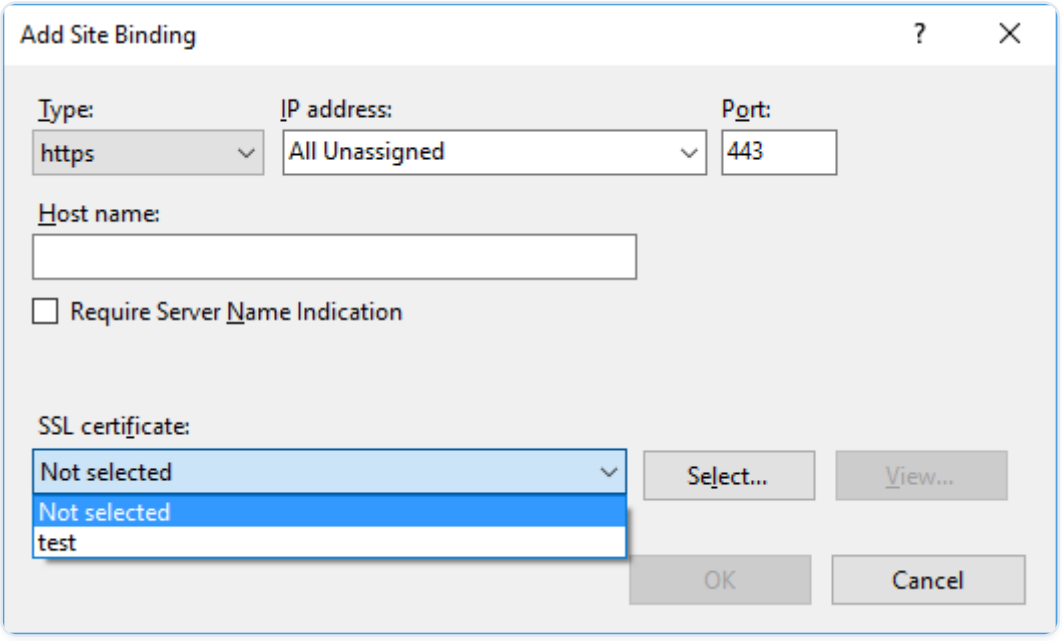
b. On IIS, right-click the website and select **Add Bindings**. The **Site Bindings** dialog box appears.



c. Click **Add** in the upper right corner. The **Add Site Binding** dialog box appears.

d. Select **https** from the **Type** list and select your SSL certificate.





e. Click **OK**.

2. Update the `SsRecWebSocketServer.config` configuration file.

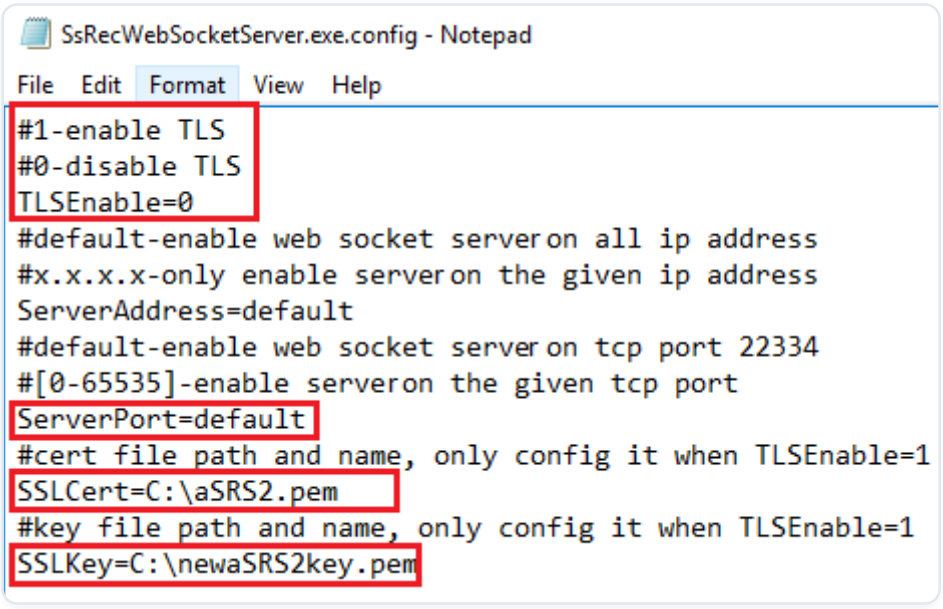
   a. Locate and open the `SsRecWebSocketServer.config` configuration file.

      The `SsRecWebSocketServer.config` configuration file is typically located in the `<Session Recording Server installation path>\Bin\` folder.

   b. (Optional) For Session Recording 2103 and later that host the WebSocket server in IIS, enable TLS by editing TLSEnable=1 and ignore the **ServerPort**, **SSLCert**, and **SSLKey** fields.

   c. (Optional) For Session Recording 2012 and earlier, enable TLS by editing TLSEnable=1, and fill in the paths to the SSL certificate and its key, respectively.

> **Note:**
>
> Only the PEM format of SSL certificates and key files is supported.
>
> \>The **ServerPort** field indicates the port number that the web player uses to collect recording files. In the following screen capture, it is set to the default value (22334).



To extract the separate certificate and key files used in the WebSocket server configuration:

i. Ensure that OpenSSL is installed on your Session Recording Server that contains the SSL certificate.

ii. Export the SSL certificate as a .pfx file. The .pfx file includes both the certificate and the private key.

iii. Open the command prompt and go to the folder that contains the .pfx file.

iv. Start OpenSSL from the OpenSSL\bin folder.

v. Run the following command to extract the certificate:

```
openssl pkcs12 -in [yourfile.pfx] -clcerts -nokeys -out
[aSRS2.pem]
```

Enter the import password that you created when exporting the .pfx file.

vi. Run the following command to extract the private key:

```
openssl pkcs12 -in [yourfile.pfx] -nocerts -out
[newaSRS2keyWithPassword.pem]
```

Enter the import password that you created when exporting the .pfx file. Provide a new password for protecting your key file when prompted for the PEM pass phrase.

vii. Run the following command to decrypt the private key:

```
openssl rsa -in [newaSRS2keyWithPassword.pem] -out
[newaSRS2key.pem]
```

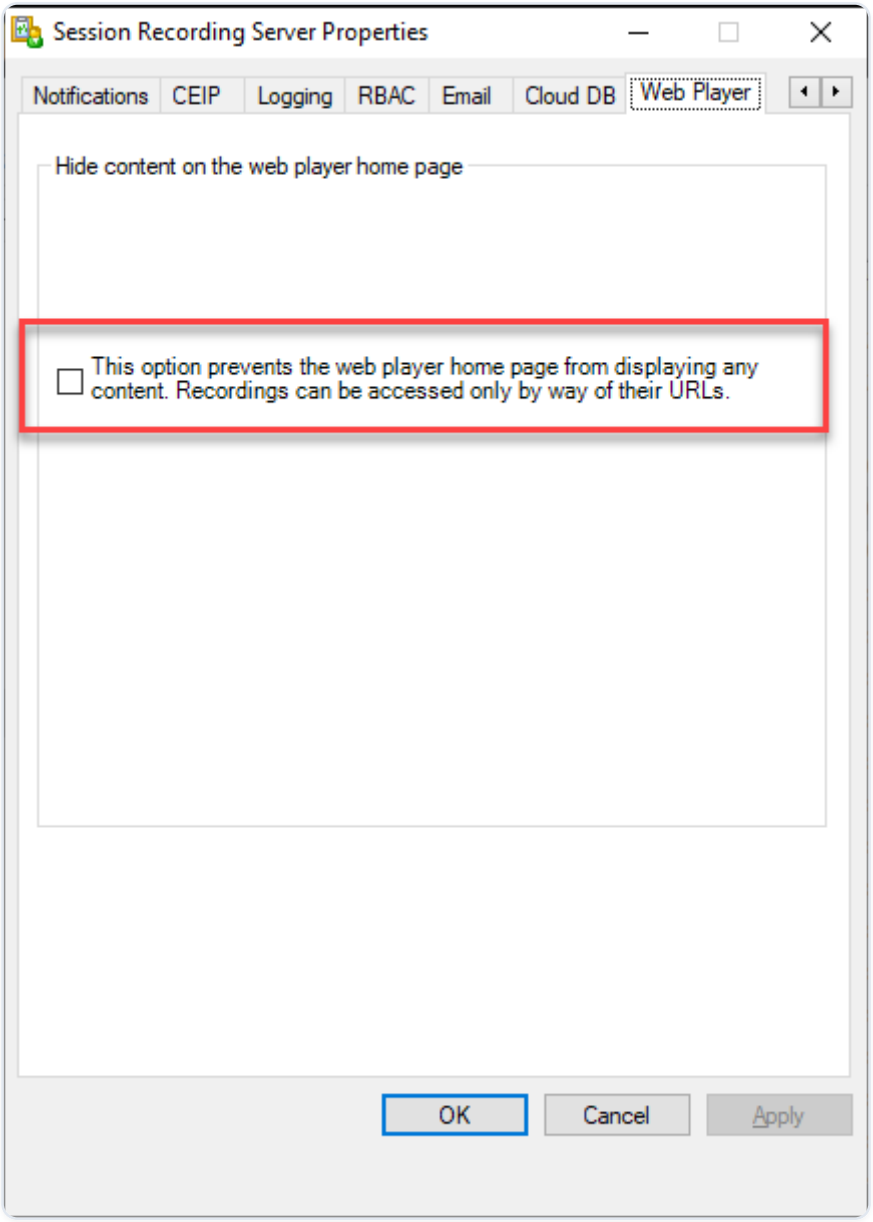
d. Save your changes.

e. Check your firewall settings. Allow SsRecWebSocketServer.exe to use the TCP port (22334 by default) and allow access to the web player URL.

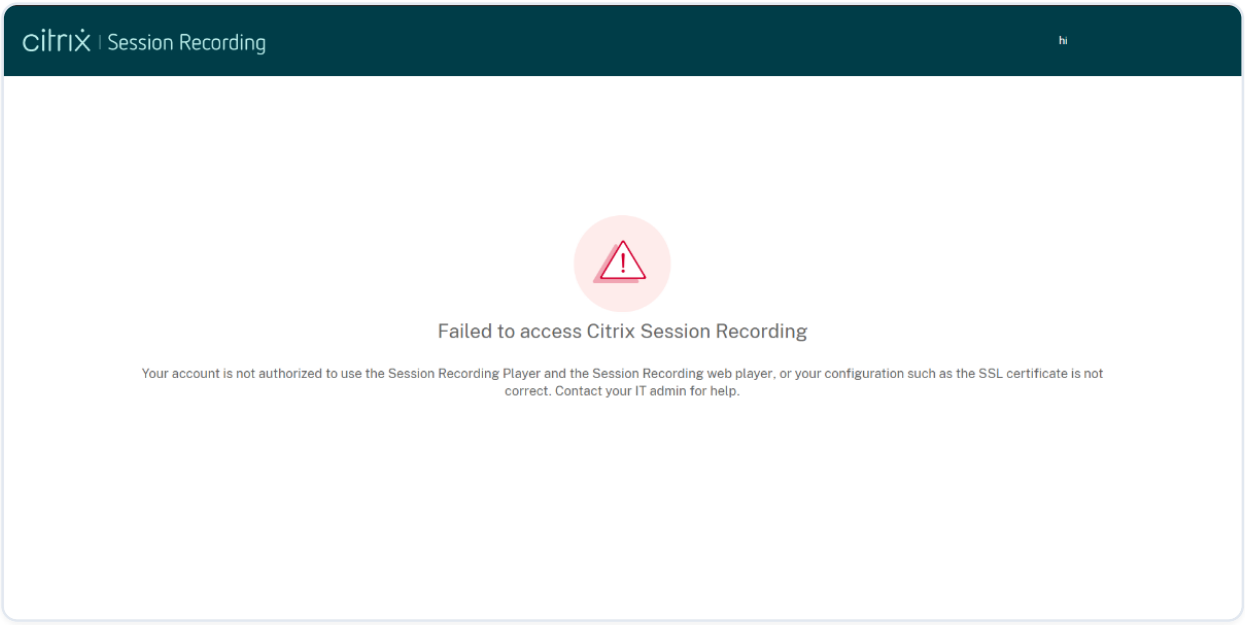
f. Run the `SsRecUtils –stopwebsocketserver` command.

Hide or show content on the web player home page

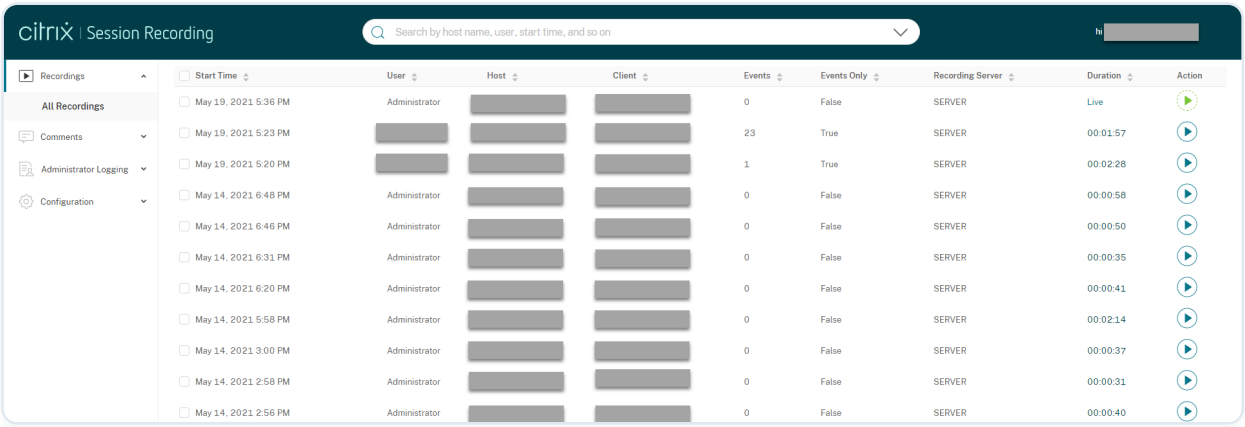
After you log on, the web player home page might hide or show content based on whether the following option is selected in **Session Recording Server Properties**.



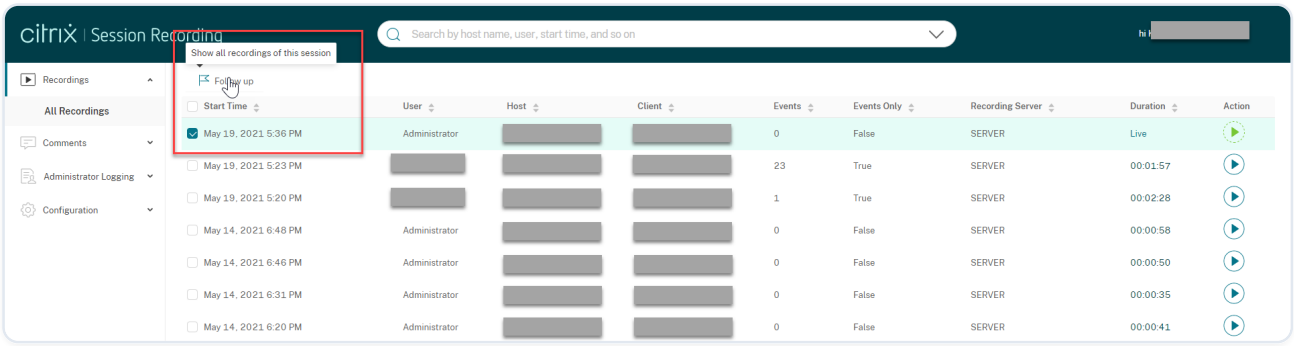
- With the option selected, the web player home page hides all content. Recordings can be accessed only by way of their URLs. Recording URLs are provided in email alerts that are sent to specified recipients. For information about email alerts, see Configure event response policies. You can also share recording URLs through the **Share Current Playback** control on recording playback pages. See descriptions later in this article.



- With the option unselected, the web player home page shows content similar to the following screen capture. Click **All Recordings** in the left navigation to refresh the page and display new recordings if there are any. Scroll down the webpage to select recordings to view or use filters to customize your search results. For live recordings, the **Duration** column shows **Live** and the play button appears green.



To show all recording files of a recorded session, select a recording on the list and click the **Follow up** icon. The **Follow up** icon is available only when a recording is selected.



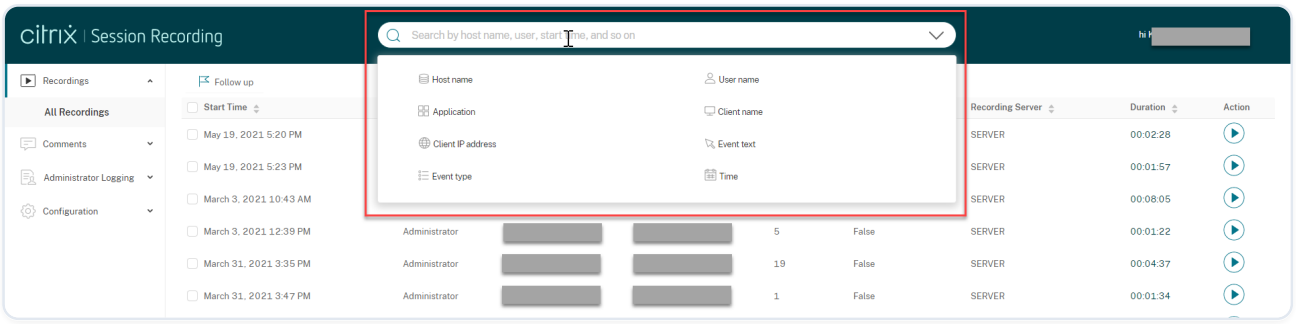
For a description of the recording items, see the following table.

ITEM	DESCRIPTION
Start time	The recording start time. Click the up and down arrows to list recordings in chronological order.
User	The user whose session was recorded. Click the up and down arrows to concentrate recordings of a user on the list and arrange users in alphabetical order.
Host	The host name of the VDA where the recorded session was hosted. Click the up and down arrows to arrange the VDA host names in alphabetical order.
Client	The name of the client device where the session was running. Click the up and down arrows to arrange the client host names in alphabetical order.
Events	The quantity of events in the recording. Click the up and down arrows to arrange recordings on the list by event quantity.
Events Only	Indicates a screen recording or an event-only recording. An event-only recording played in the web player contains an event statistics pie chart and histogram. The pie chart and histogram hold static throughout playback.
Recording Server	The Session Recording Server that processes recording data sent from VDAs.

ITEM	DESCRIPTION
Duration	The time length of the recording. Click the up and down arrows to arrange recordings on the list by time length.

Search for recordings

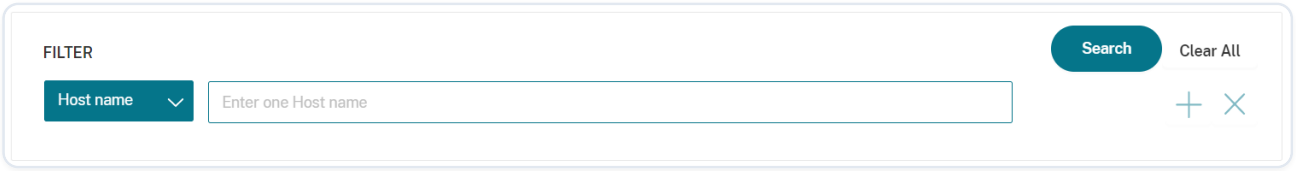
You can search for recordings by using filters in the web player. The available filters include host name, client name, user name, application, client IP address, event text, event type, and time.



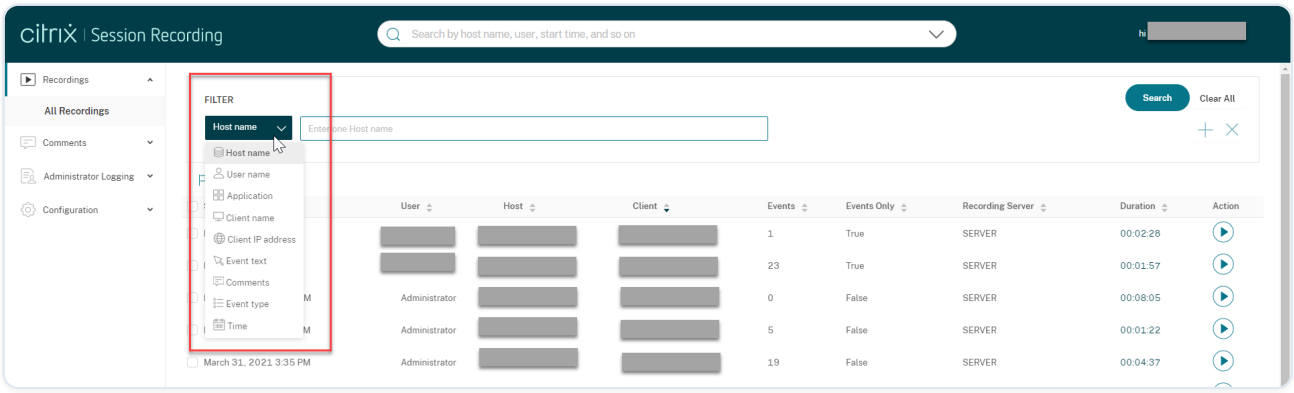
Tip:

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

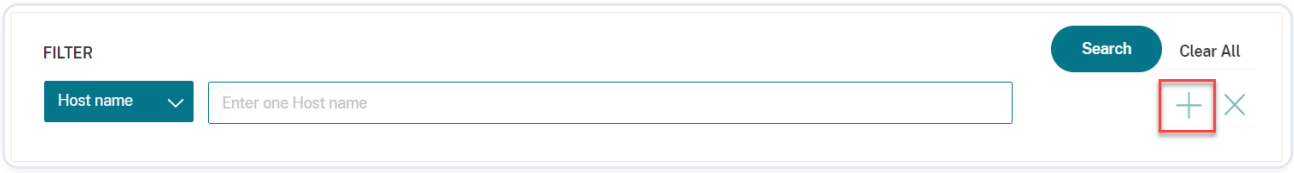
For example, after you select the host name filter, the following dialog box appears. Type in the host name (of the VDA where recorded sessions are hosted) and click **Search** to filter out irrelevant recordings and display only the relevant ones.



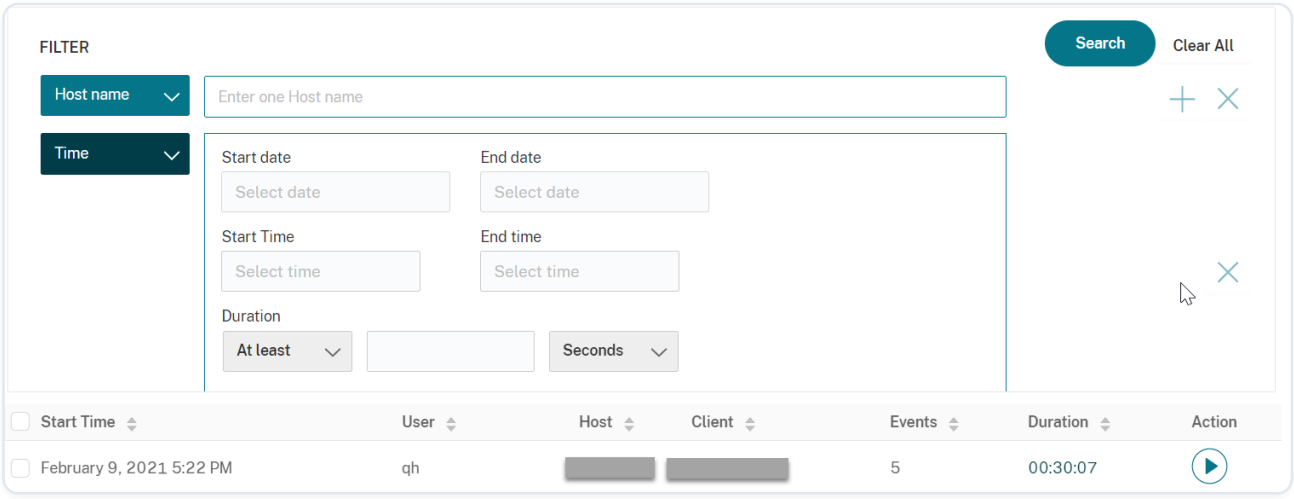
You can change to a different filter by clicking the currently selected **Host name**, as shown in the following screen capture. All filters are listed after you click **Host name**. Select a different filter as needed.



You can also click the **+** symbol to add filters.



For example, you can add the **Time** filter as shown in the following screen.

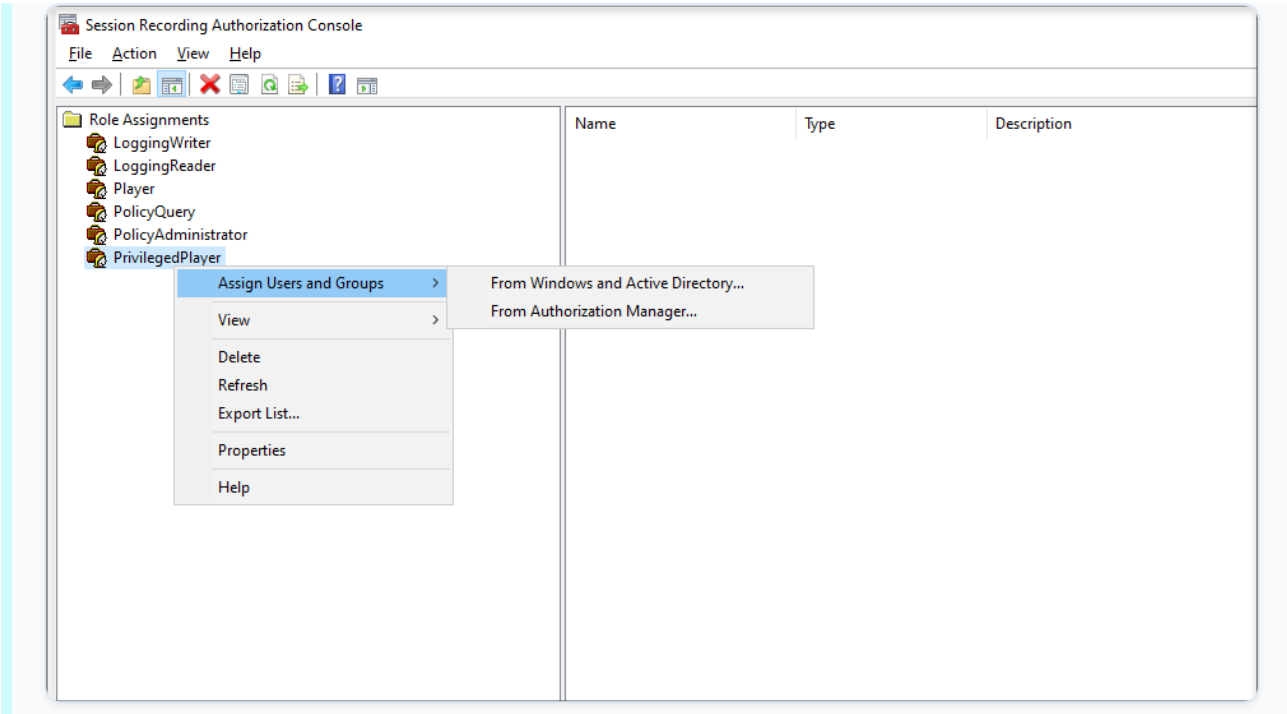


The **Time** filter consists of recording start date, start time, and duration.

Place access restrictions on recordings

You place access restrictions on target recordings in addition to role-based access control through recording viewing policies. Restricted recordings are accessible only to users and user groups that are assigned the **PrivilegedPlayer** role through the Session Recording Authorization Console.

> **Note:**
>
> Placing access restrictions on live recordings is not supported.



The following section walks you through the process of placing and removing access restrictions on target recordings.

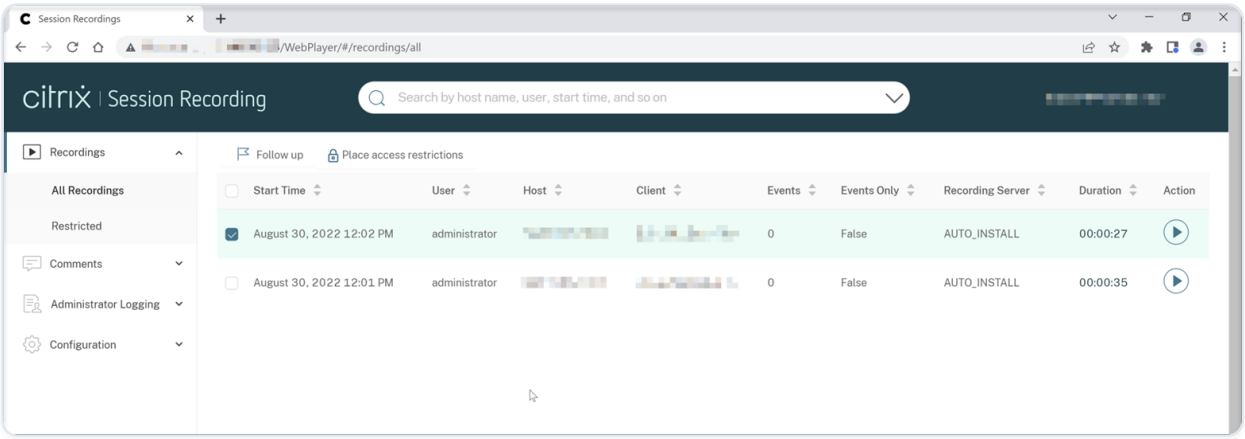
1. Enter the URL of your web player website in the address bar of a supported browser.

   The URL format is **http(s)://<FQDN of Session Recording server\>/WebPlayer**.

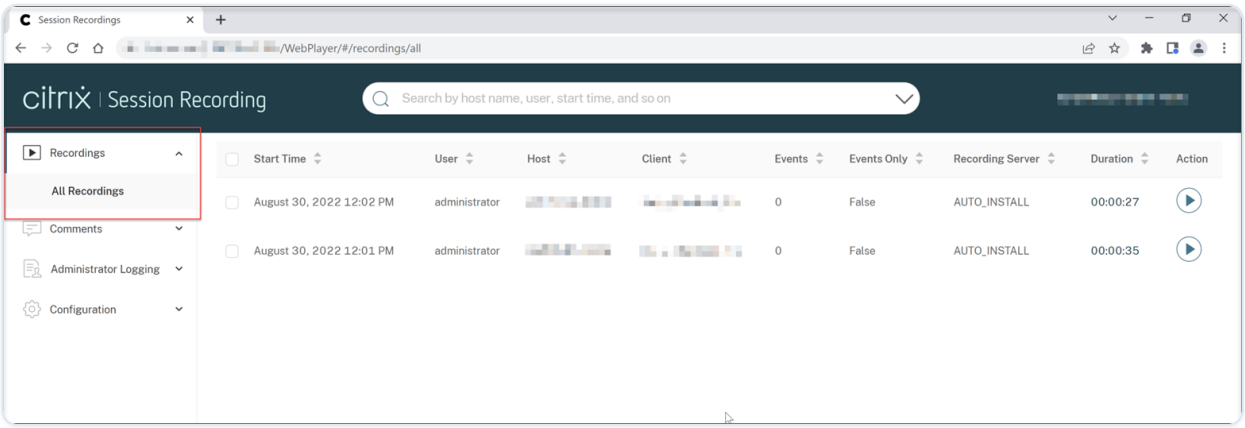
   Supported browsers include Google Chrome, Microsoft Edge, and Firefox.
2. In the left navigation of the web player page, expand the **Recordings** menu.
3. On the **All Recordings** page, select one or more target recordings.
4. Click the **Place access restrictions** icon on top of the recording list.

   Users and user groups, assigned either the **Player** or the **PrivilegedPlayer** role, are allowed to place access restrictions on recordings. The **Restricted** menu is available only for users and user groups assigned the **PrivilegedPlayer** role.

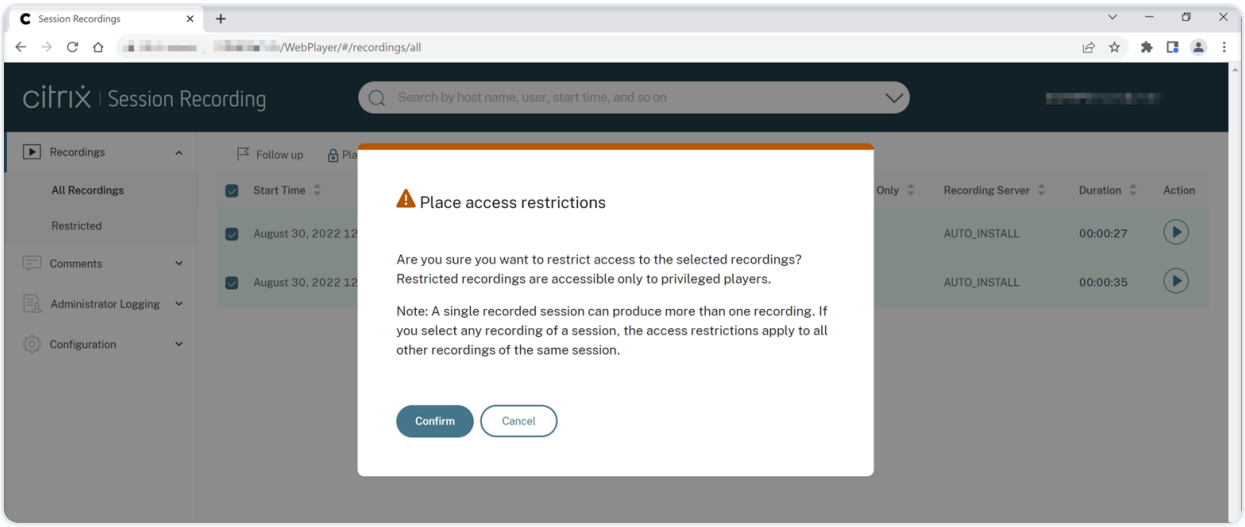
   View for the **PrivilegedPlayer** role:



View for the **Player** role:

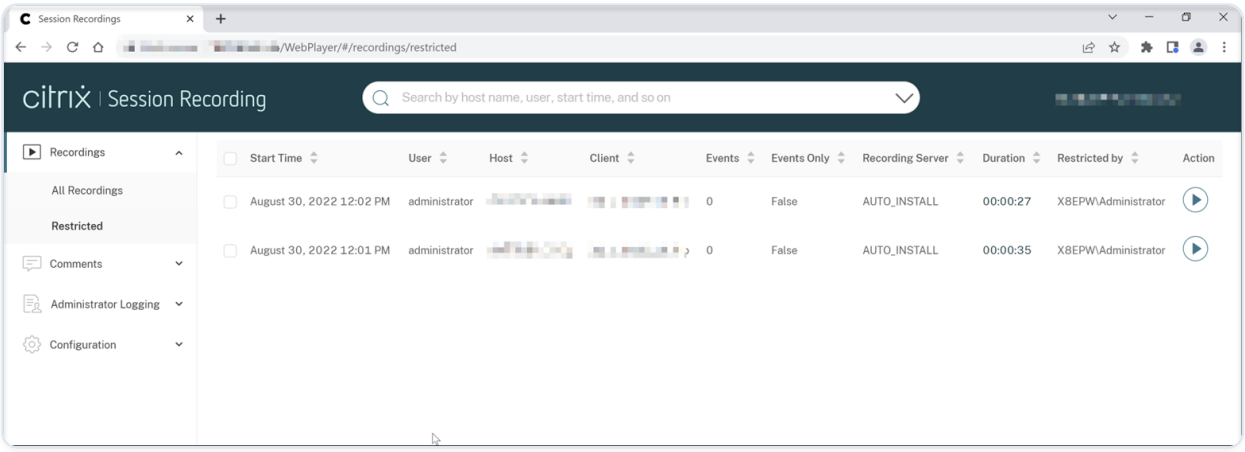


5. Click **Confirm**.

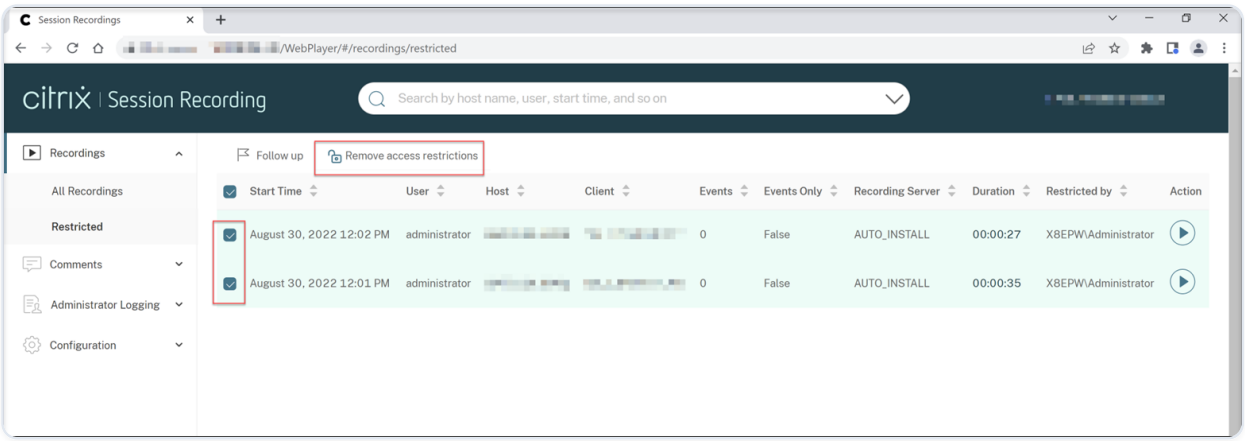


6. Verify that the selected recordings on which you placed access restrictions are moved from the **All Recordings** page to the **Restricted** page.

   The **Restricted by** column shows who placed access restrictions on the relevant recordings.

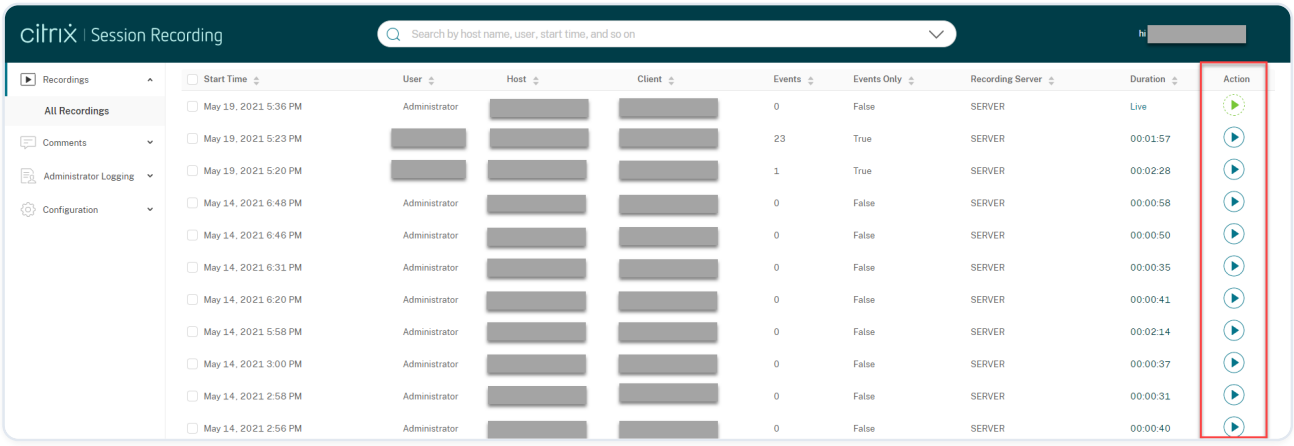


7. On the **Restricted** page, remove access restrictions as needed. With access restrictions removed, recordings are moved back to the **All Recordings** page.



Open and play recordings

You can play live and completed recordings in the web player. On the recordings page, each recording has a play button on the right side, next to the **Duration** item.



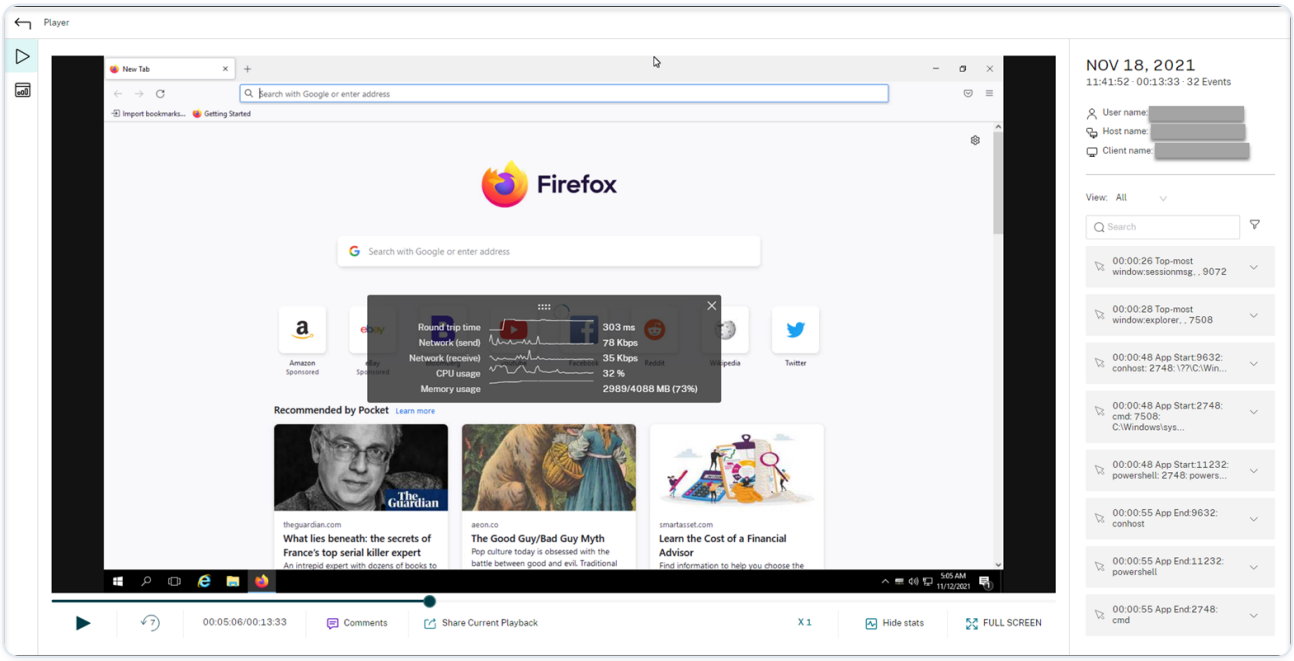
Tip:

For the **Player** role, the **Recordings** menu in the left navigation shows only the **All Recordings** submenu.

For the **PrivilegedPlayer** role, the **Recordings** menu shows both the **All Recordings** and the **Restricted** submenus.

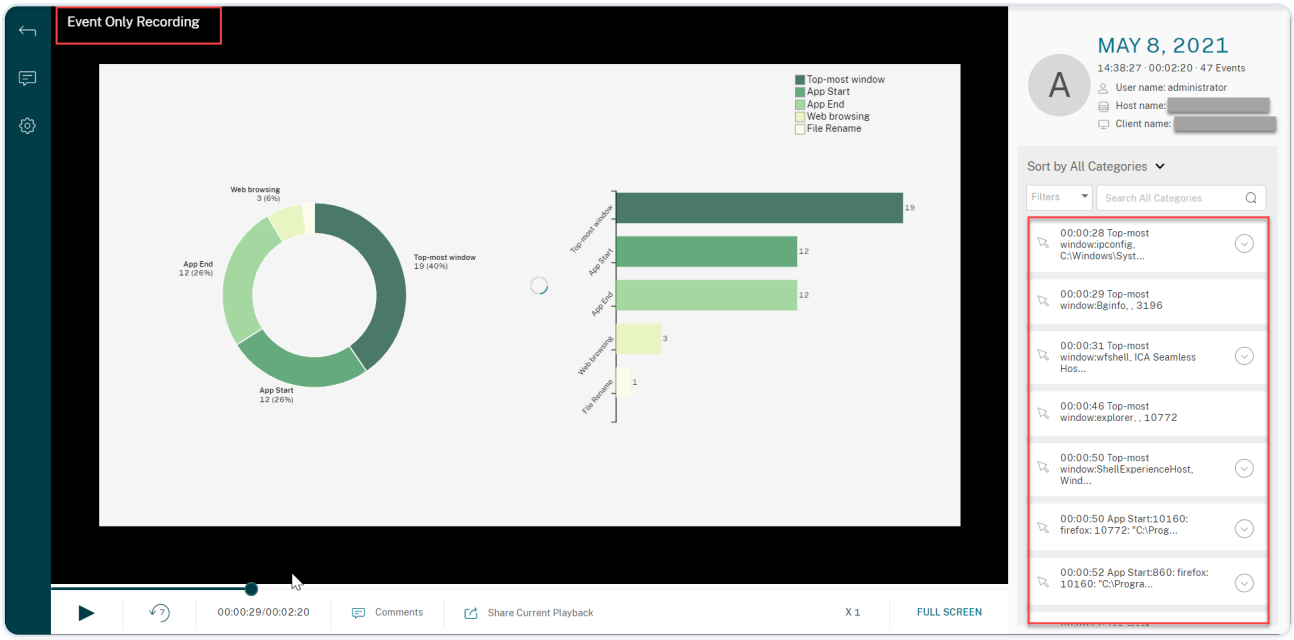
Click the play button. The playback page appears. Playback starts after memory caching.

Playback of a screen recording:



Playback of an event-only recording:

An event-only recording played in the web player contains an event statistics pie chart and histogram. The pie chart and histogram hold static throughout playback. You can navigate to a specific event from within the right pane.



Tip:

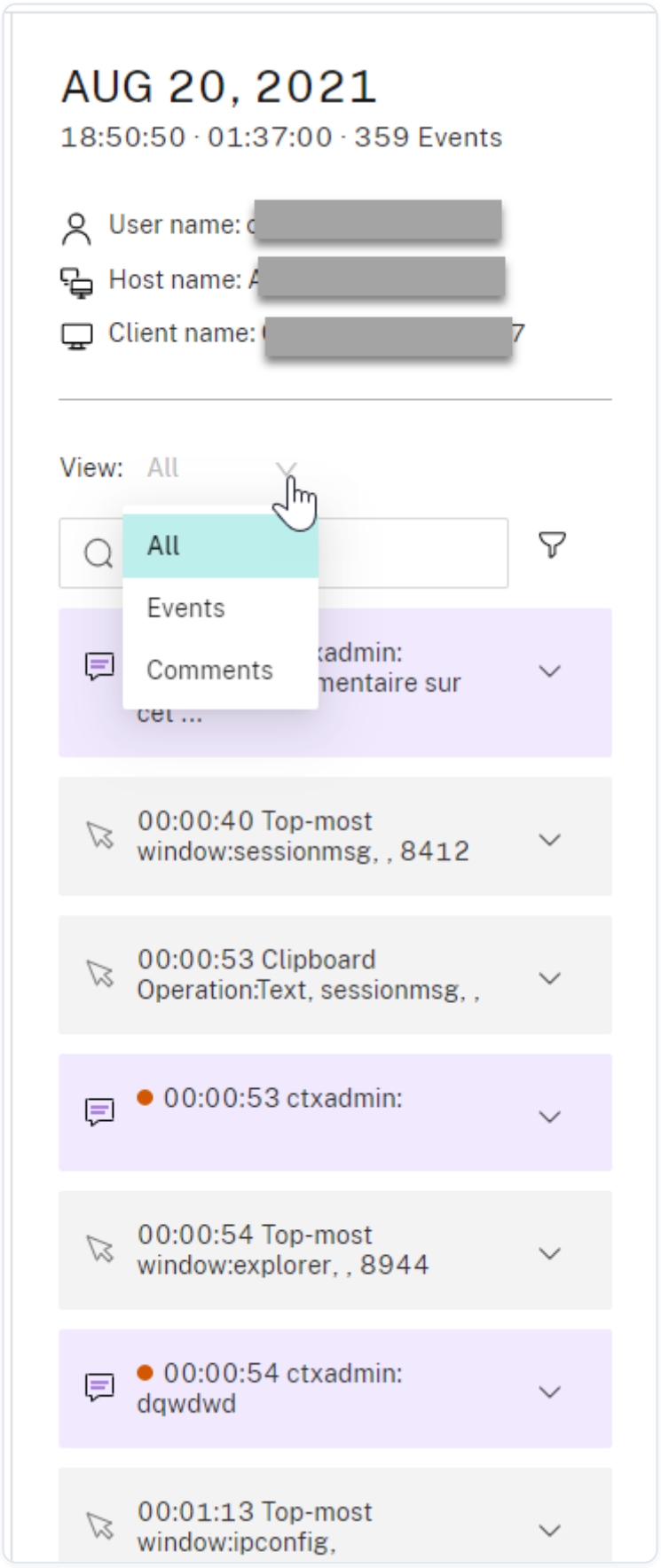
- Clicking the session progress time lets you switch to the absolute date and time the session was recorded.
- For an event-only recording, the play icon in the upper left corner is unavailable.

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

PLAYER CONTROL	DESCRIPTION
	Plays the selected recording file.
	Pauses playback.
	You can drag the progress bar during playback. Idle periods of recorded sessions are highlighted during playback.
	Seeks backward 7 seconds.
	Indicates the current position of the recording playback and the total recording duration. The time format is HH:MM:SS.

PLAYER CONTROL	DESCRIPTION
	Lets you click and leave a comment about the recording being played.
	Lets you click and copy the URL of the current recording to the clipboard.
	Shows the overlay that features data points related to the recorded session.
	Hides the session data overlay.
	Indicates the current speed of playback. Click the icon to switch between options including X0.5, X1, X2, and X4.
	Displays the playback in full screen.
	Displays the playback within the webpage.

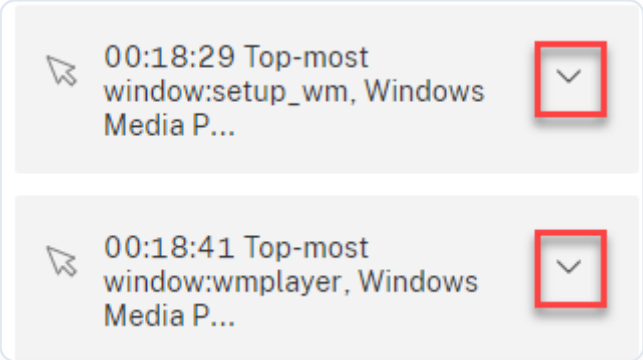
In the right pane of the playback page, the **Events** and **Comments** filters, quick search box, and some recording data are available:



- The date and time on the web player machine. In this example, **AUG 20, 2021** and **18:50:50**.
- The duration of the recording in playback. In this example, **01:37:00**.

- The number of events in the recording. In this example, **359 EVENTS**.
- The name of the user whose session was recorded.
- The host name of the VDA where the recorded session was hosted.
- The name of the client device where the session was running.
- Options for sorting search results: Select **All**, **Events**, or **Comments** to sort search results.
- Event filters. You can select more than one filter to search for events in the current recording.

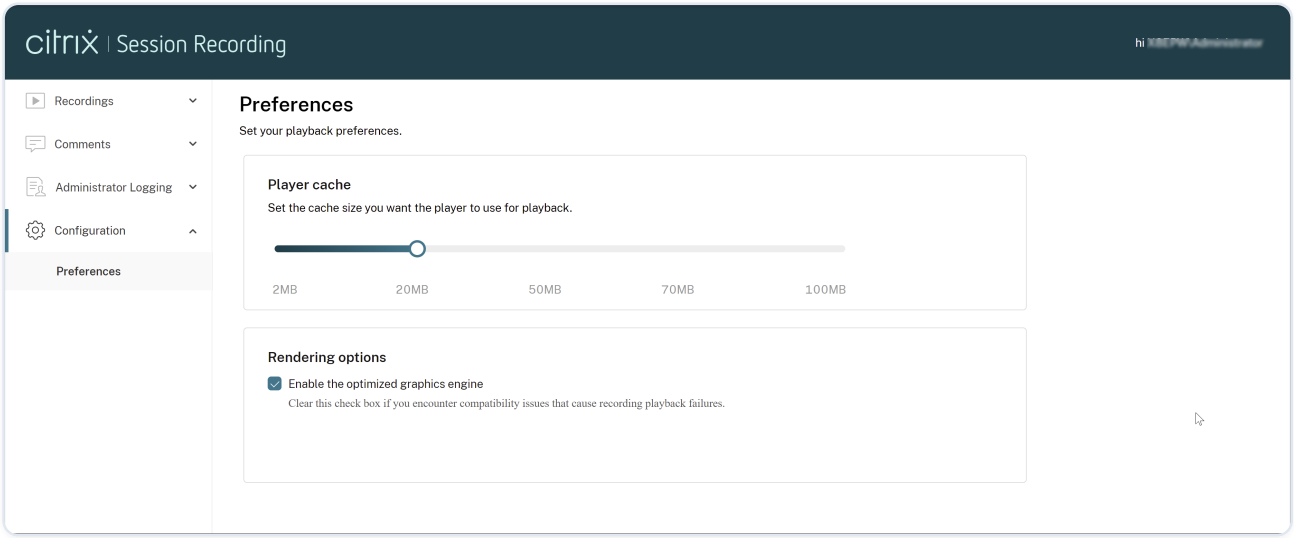
  Click the icon to expand displays of events. For example:



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

Configure preferences

To configure preferences for your web player, navigate to **Configuration > Preferences** on the web player page.



You can configure the following preferences for your web player:

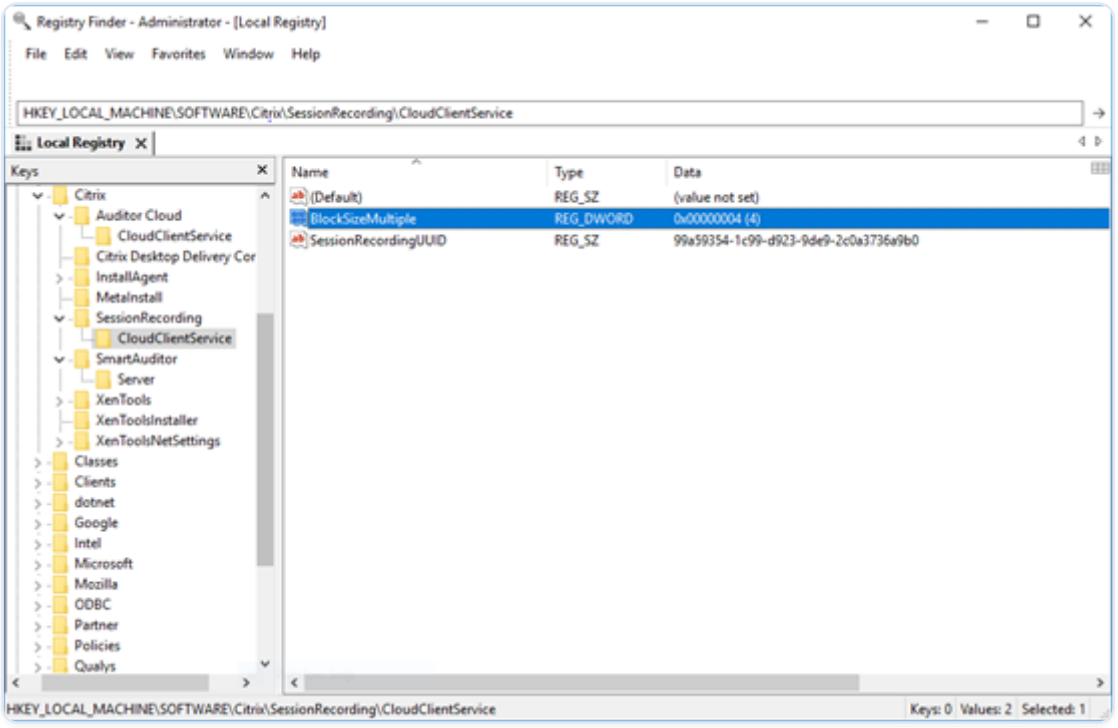
- **Player cache**. Drag the slider to set the cache size you want the player to use for playback.

- **Optimized graphics engine**. We have optimized the graphics engine to improve the performance of the web player. The optimized engine is enabled by default. If you encounter compatibility or other issues with the optimized engine, you can disable it by clearing the check box.

Increase the transport packet size for the web player

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

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



Highlight idle periods

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

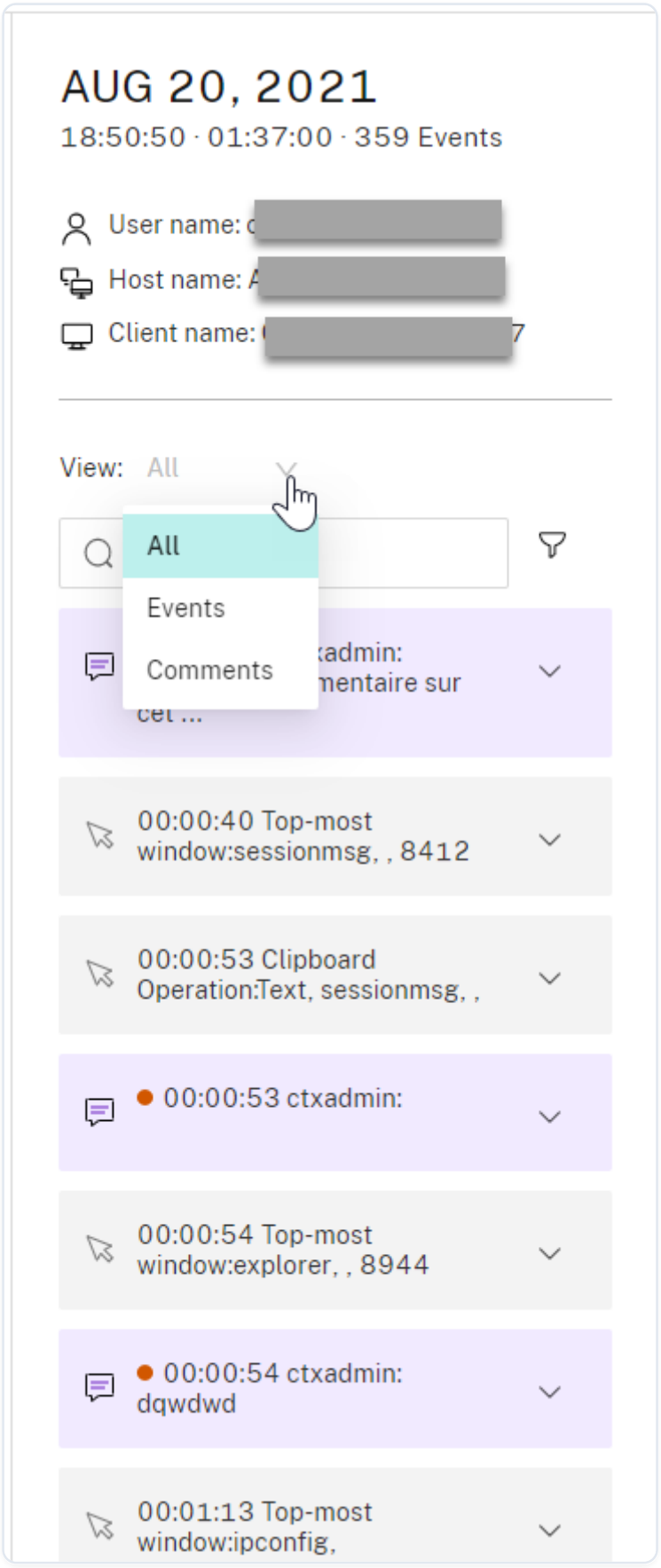
> **Tip:**
>
> Idle events are not visible in the Session Recording player because idle events are saved in the Session Recording database but not in the relevant recording files (`.icl` files).

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

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.

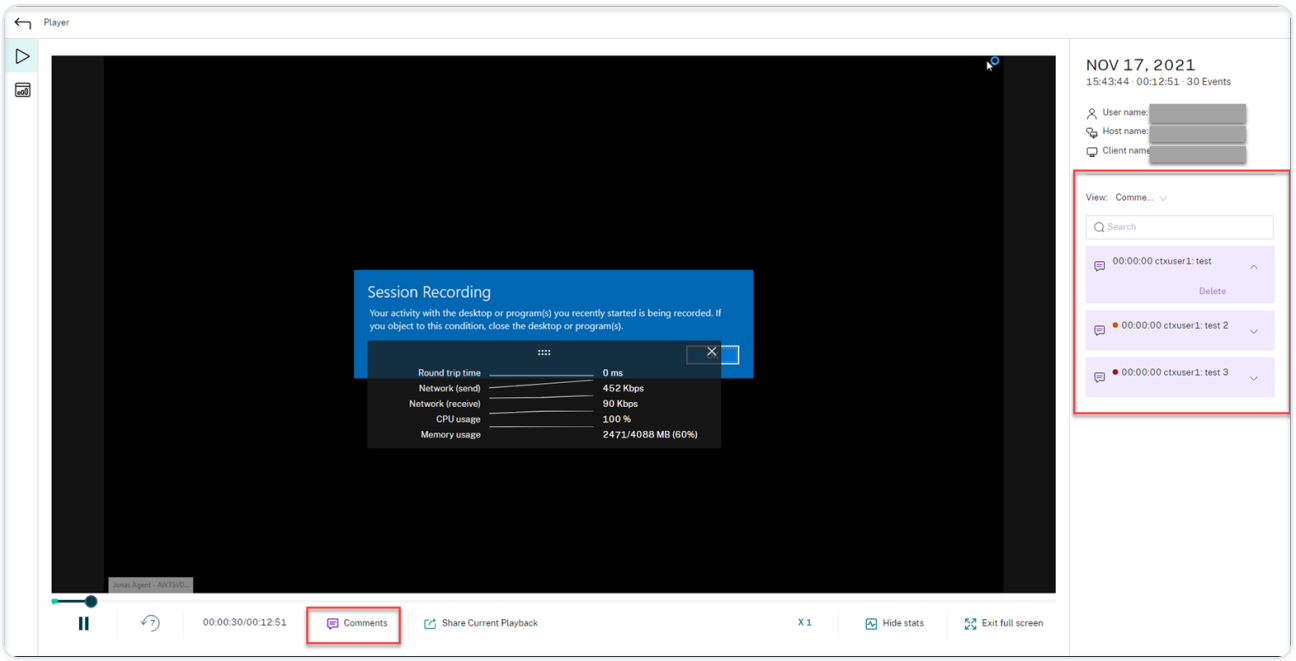
Use events and comments

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.

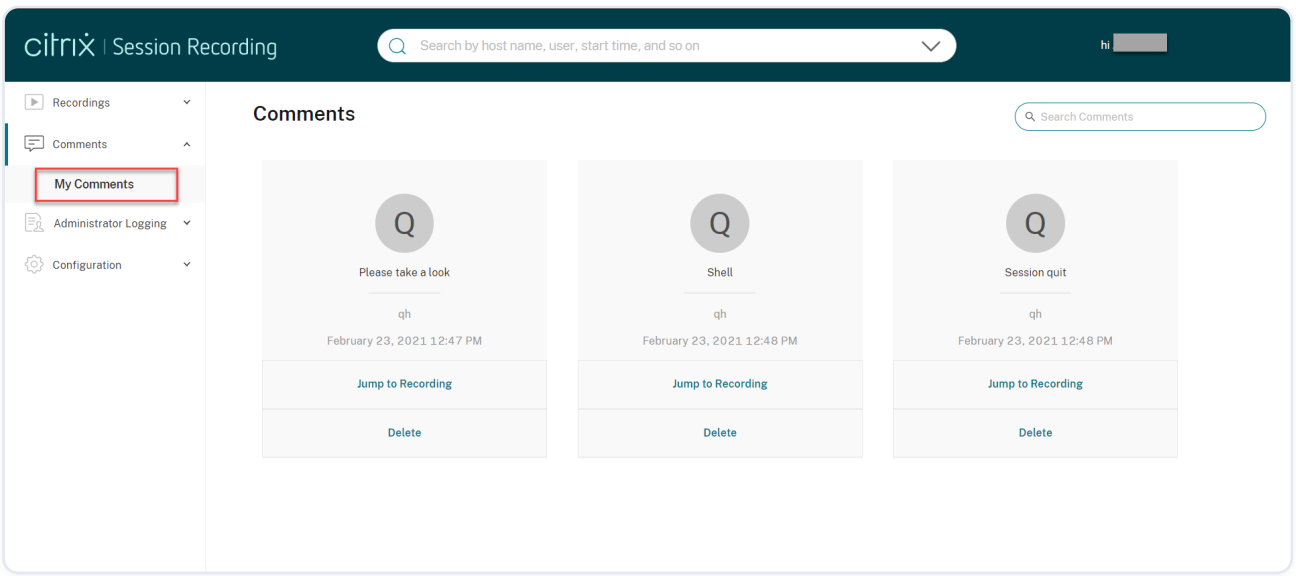

AUG 20, 2021
18:50:50 · 01:37:00 · 359 Events
User name:
Host name:
Client name:
View: All
All
Events
Comments
00:00:40 Top-most window:sessionmsg, , 8412
00:00:53 Clipboard Operation:Text, sessionmsg, ,
00:00:53 ctxadmin:
00:00:54 Top-most window:explorer, , 8944
00:00:54 ctxadmin: dqwdwd
00:01:13 Top-most window:ipconfig,

Comment on recordings

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

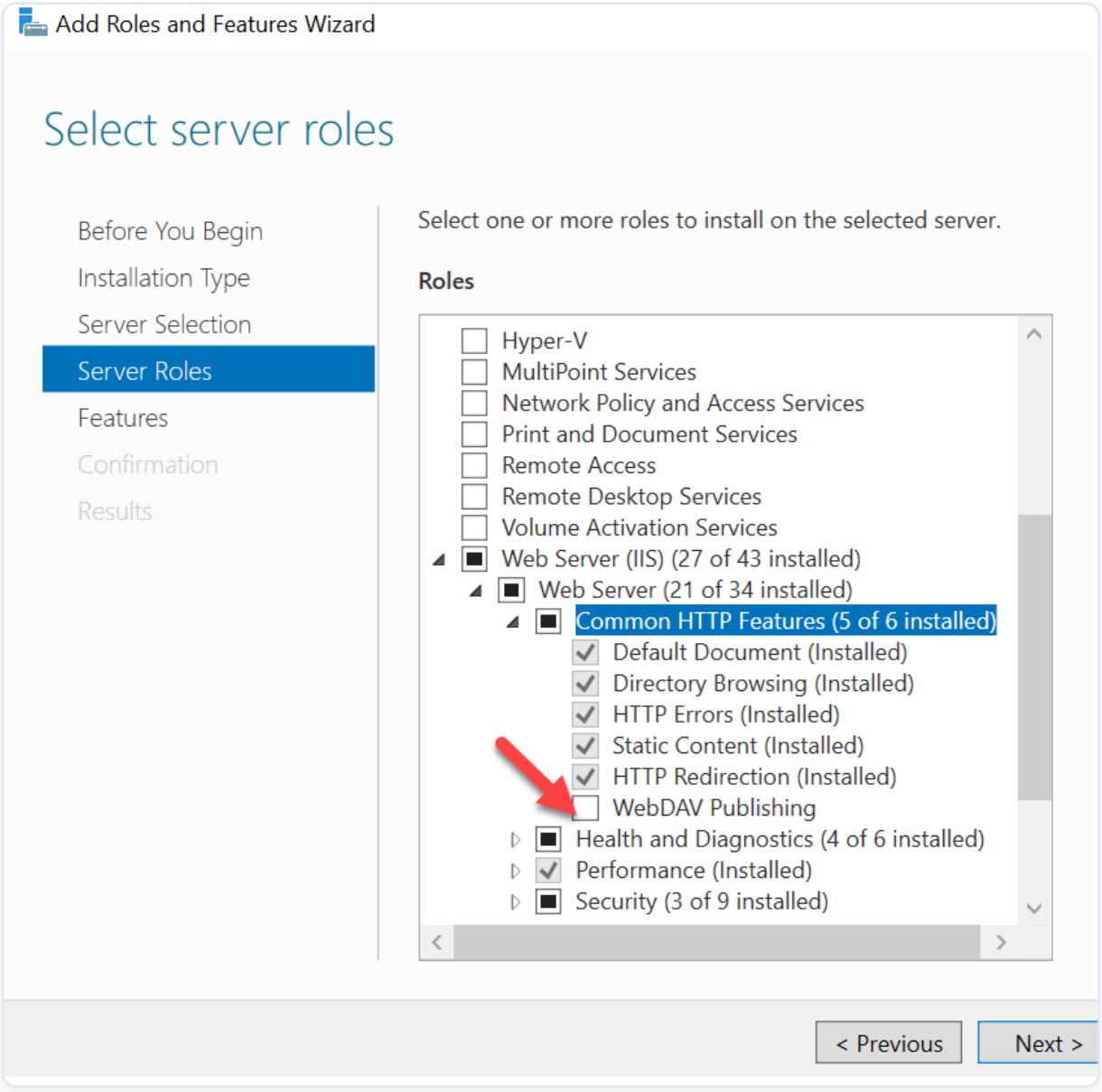


Clicking a comment lets you jump to the location where the comment was given. You can view all your comments on the **My comments** page.



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.



Share recordings as links

Overview

You can share recordings as links so that other users can access the recordings directly, without the need to search among many recordings. You can share recordings as restricted and unrestricted links. 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.

To facilitate managing unrestricted links, Session Recording 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.

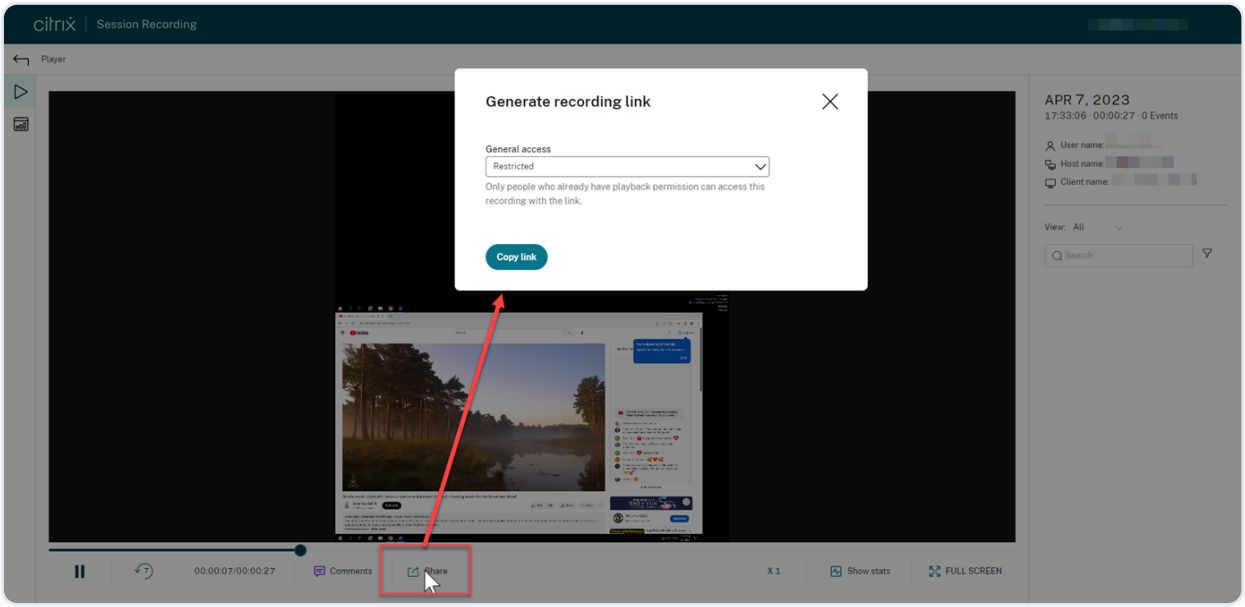
Note:

- To share recordings as unrestricted links and to manage unrestricted links, you must be assigned the **PrivilegedPlayer** role.
- 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 web player, open and play the recording that you want to share.
2. Click **Share** on the playback page of the recording. The **Generate recording link** dialog appears.



3. Select **Restricted** from the **General access** drop-down.

4. Click **Copy link**.

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

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

5. Apply secure sharing at the server level.

   To ensure secure sharing, set the following registry values under `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`:

REGISTRY VALUE	DESCRIPTION	DEFAULT VALUE	REMARKS
LinkExpire	Time span beyond which a generated URL link expires. Counted as timeticks in the unit of 10 microseconds.	1,728,000,000,000 (The default value equals 2 days.)	-
LinkSalt	A security method to encrypt the preceding URL expiration time	Kk2od974	Change the default value to an arbitrary string that preferably ends with digits.

6. 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.

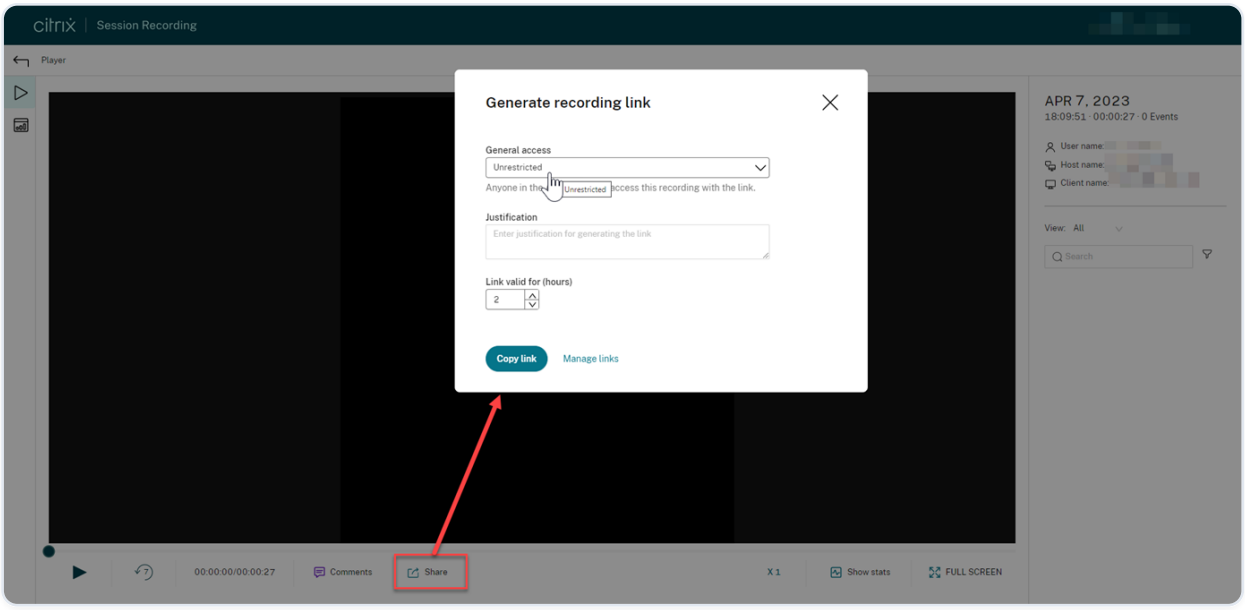
Share recordings as unrestricted links

> **Note:**
>
> To share recordings as unrestricted links, you must be assigned the **PrivilegedPlayer** role.

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

1. In the web player, open and play the recording that you want to share.

2. Click **Share** on the playback page of the recording. The **Generate recording link** dialog appears.
3. Select **Unrestricted** from the **General access** drop-down.



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

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

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

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

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

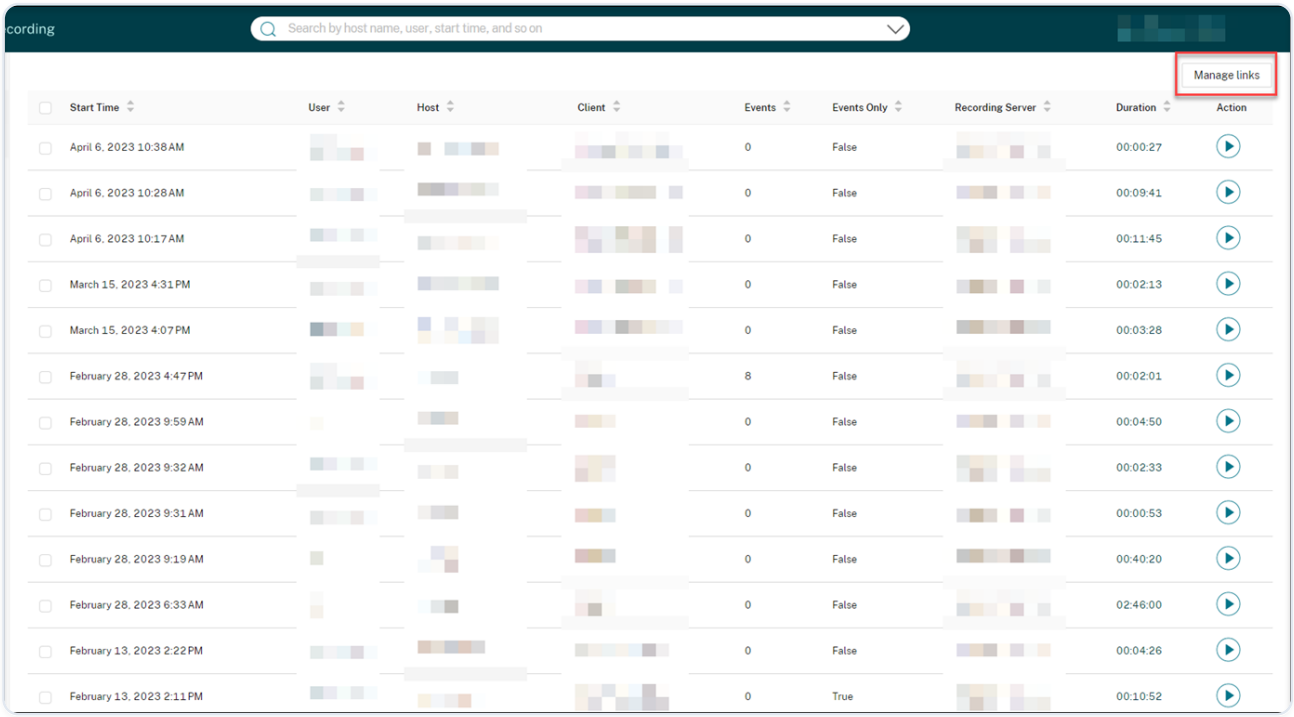
> **Note:**
>
> - To view a recording using an unrestricted link, users must enter a justification.
> - The actions of generating and accessing unrestricted links are logged under the playback logging sector of administrator logging.

Manage unrestricted links

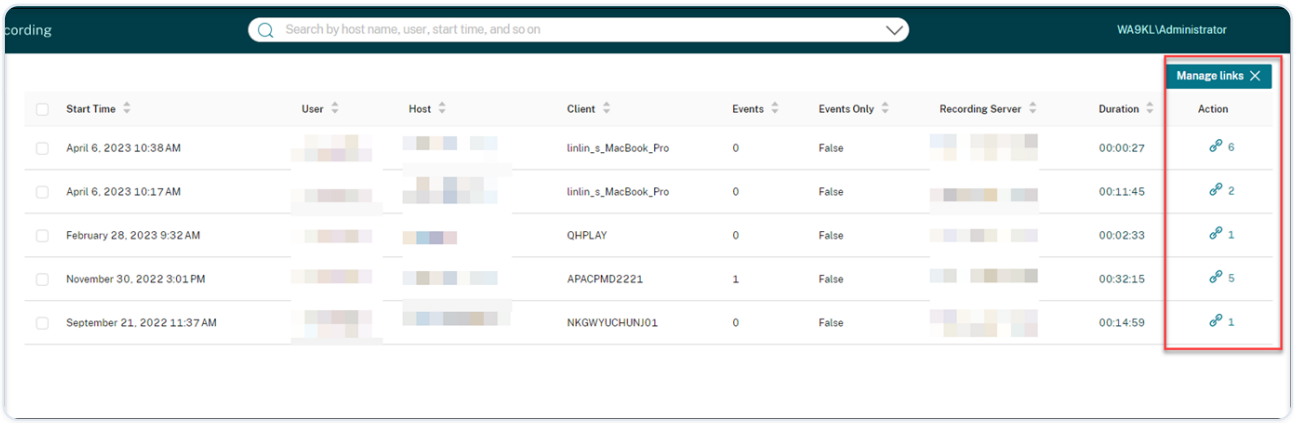
> **Note:**
>
> To manage unrestricted links, you must be assigned the **PrivilegedPlayer** role.

View which recordings have been shared as unrestricted links

To get an overview of which recordings have been shared as unrestricted links, click **Manage Links** in the upper right corner of the **All Recordings** page.



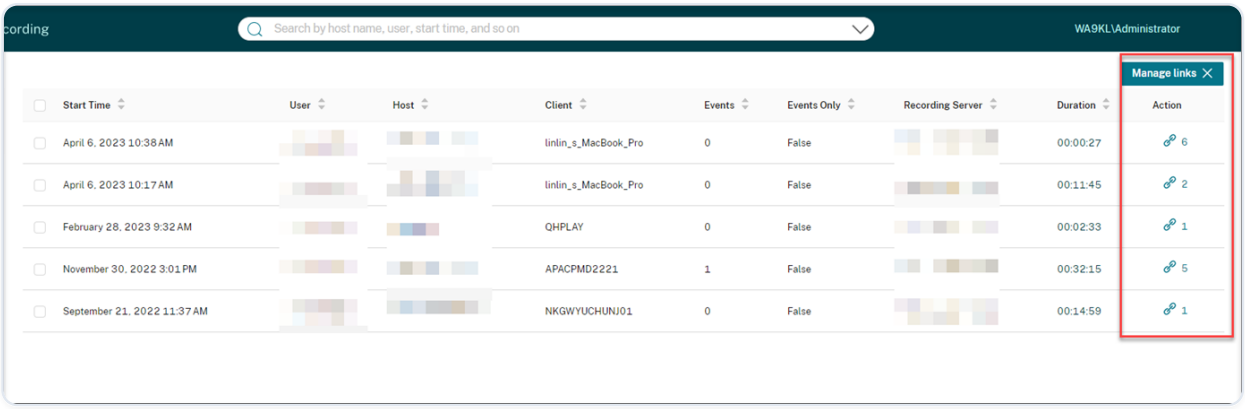
After you click **Manage Links**, only recordings that have been shared as unrestricted links are listed.



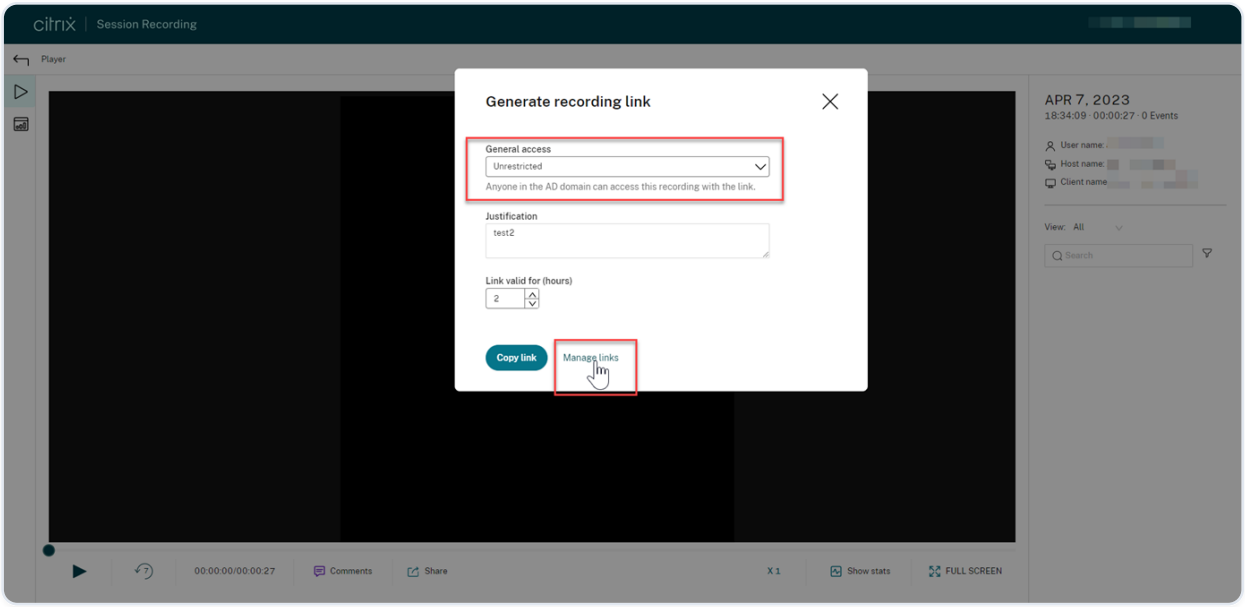
View and manage unrestricted links of a specific recording

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

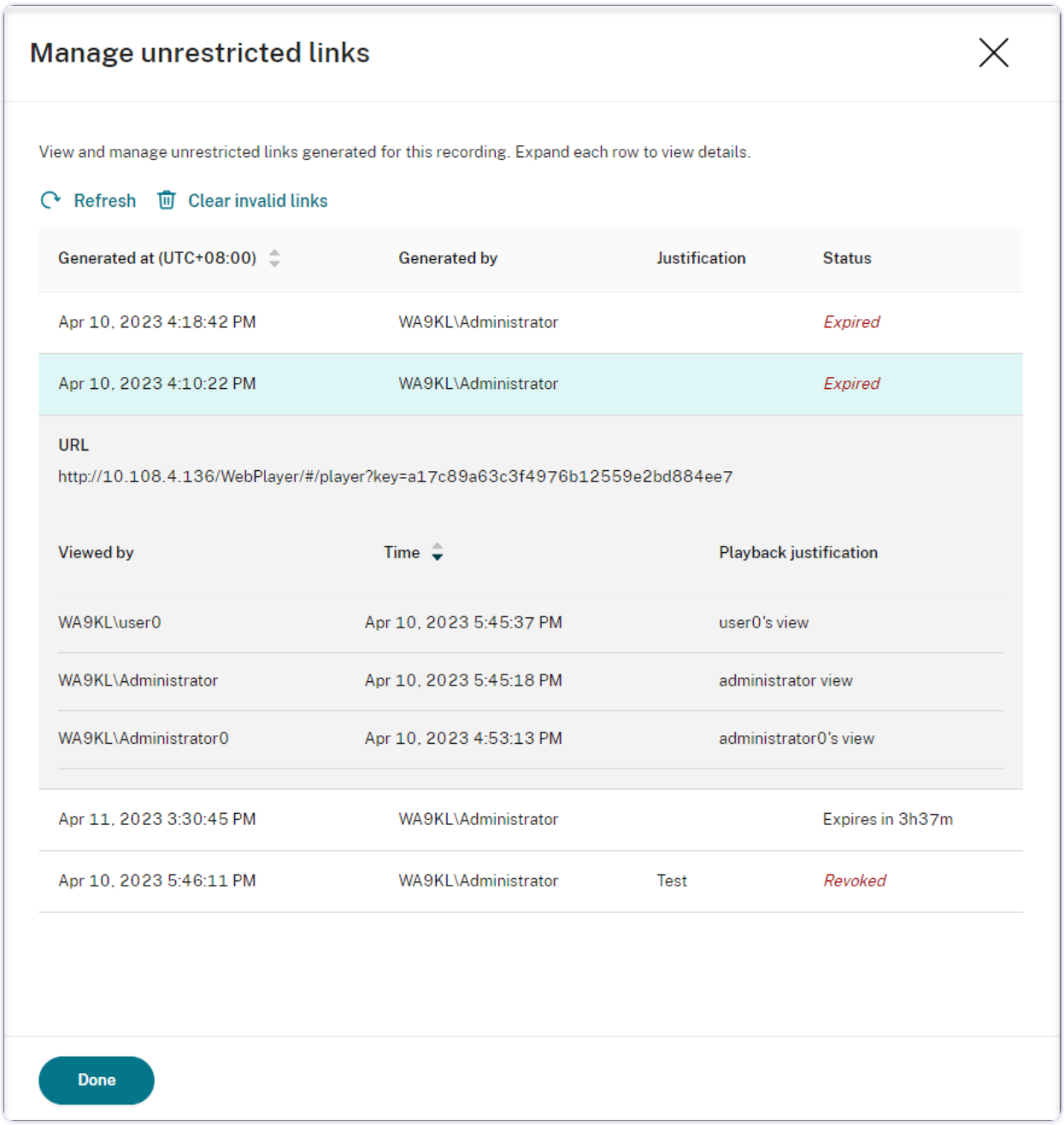
   Method 1: By clicking the link icon in the **Action** column on the **All Recordings** page



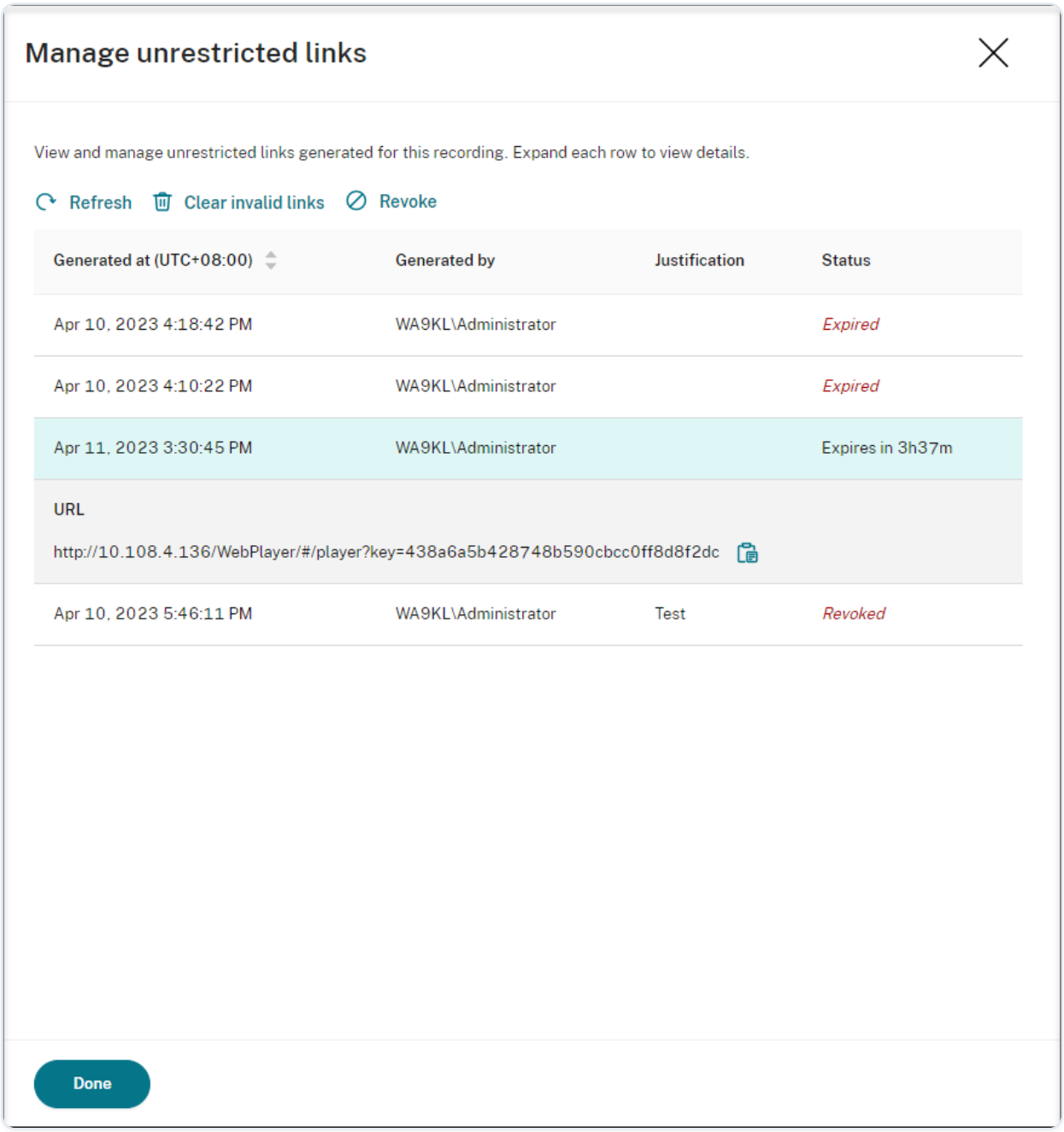
   Method 2: By clicking **Manage Links** in the **Generate recording link dialog**



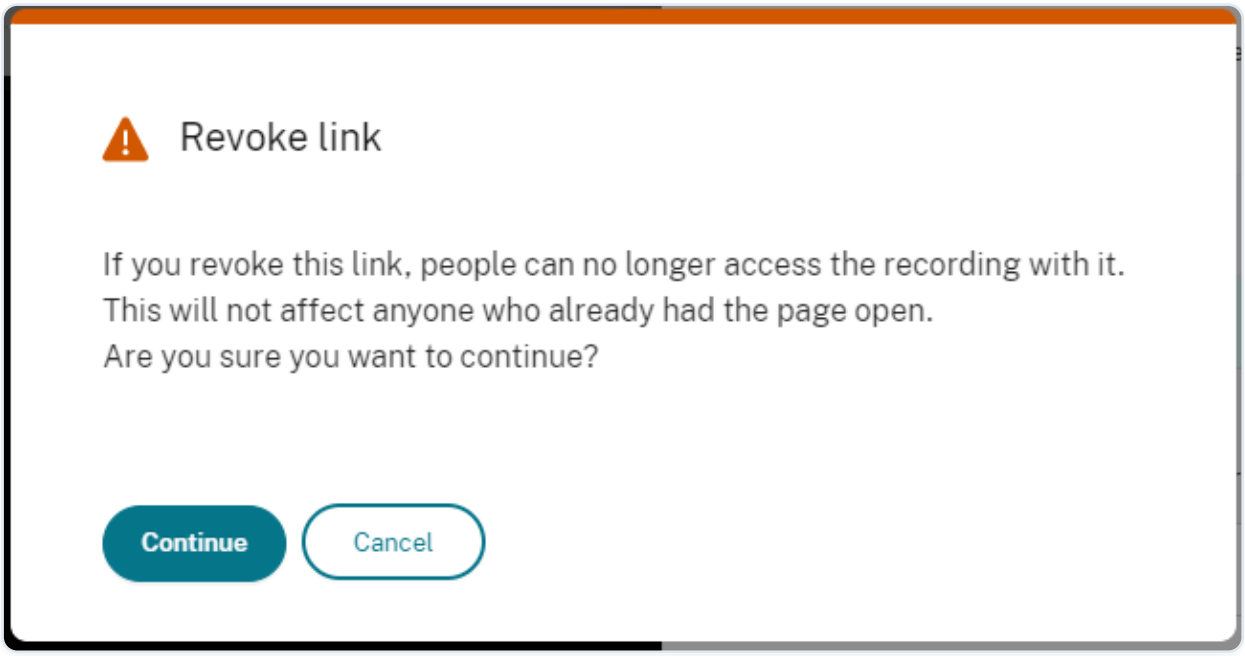
2. On the **Manage unrestricted links** page, expand each row to view details about the unrestricted links that are generated for the specific recording.



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.



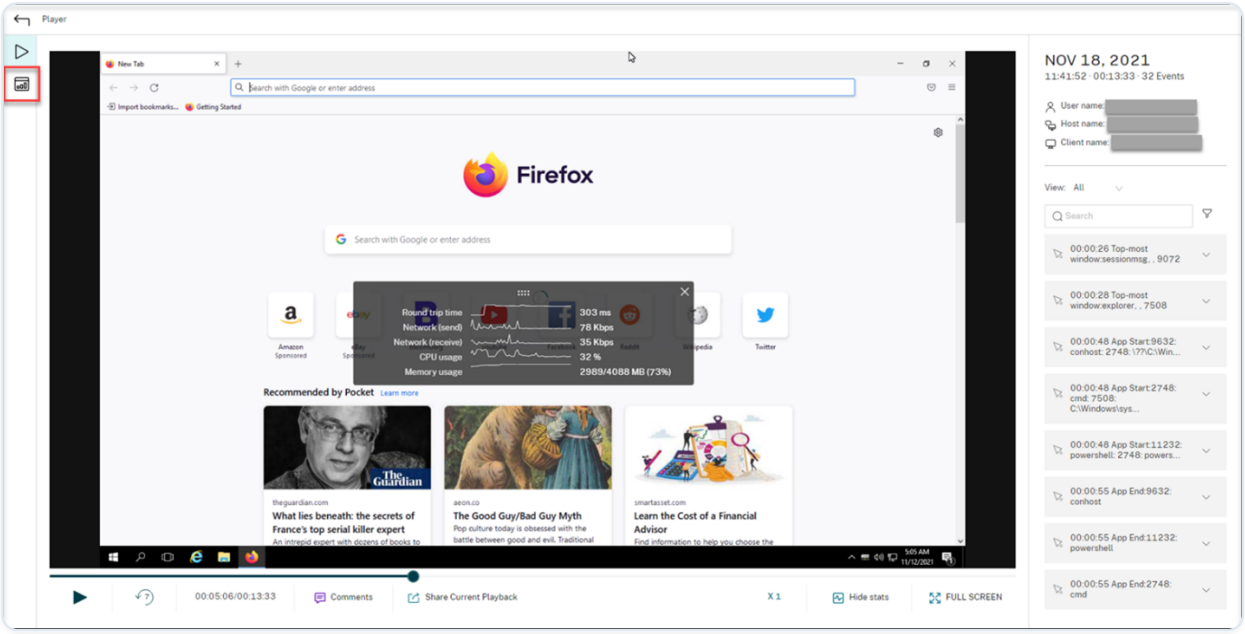
4. (Optional) To remove the links that have expired or revoked, click **Clear invalid links**.

View graphical event statistics for each recording

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

To view graphical event statistics, complete the following steps:

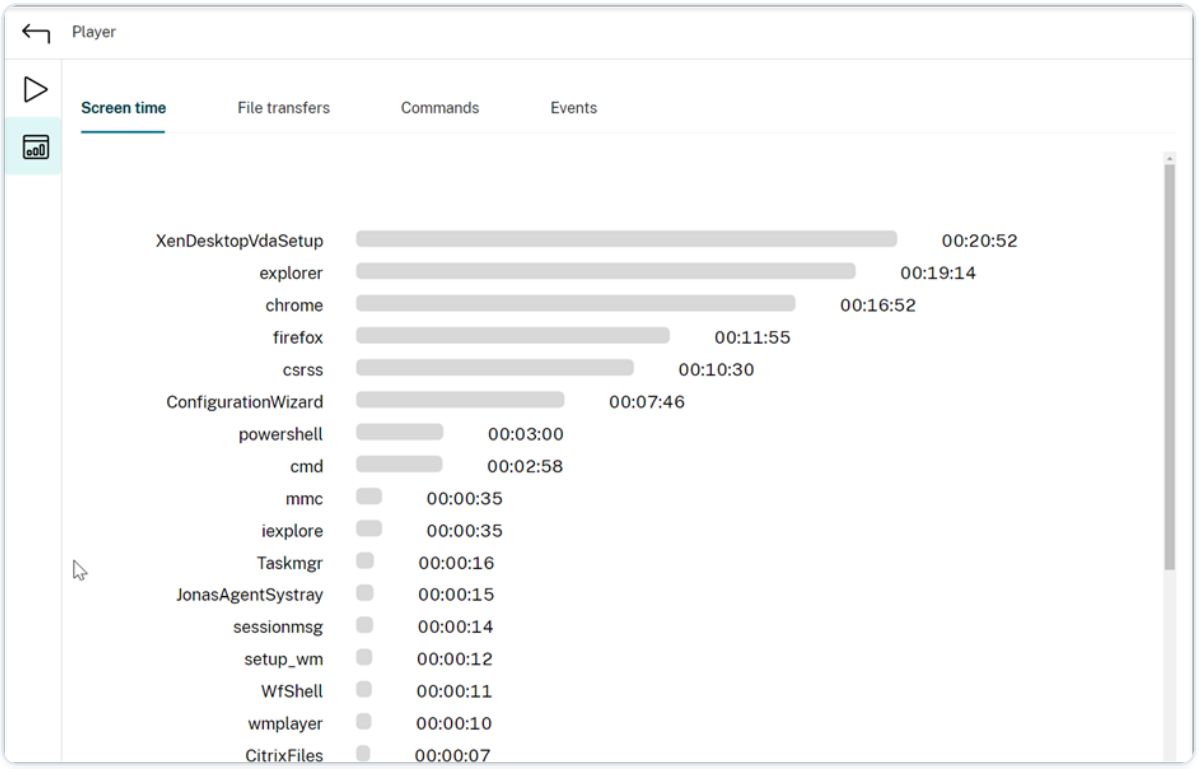
1. Open and play a recording.
2. In the upper left corner of the playback page, click the statistics icon.



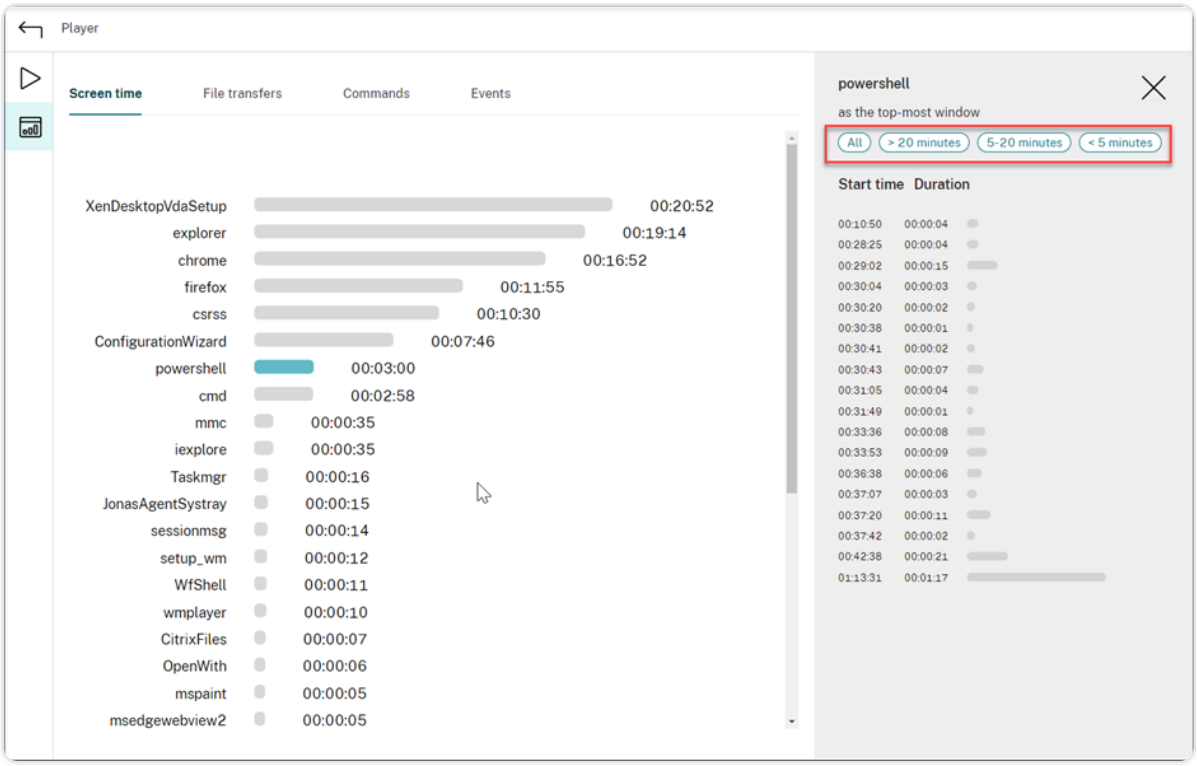
3. Switch between the **Screen time**, **File transfers**, **Commands**, and **Events** tabs to view statistics from different perspectives.

- **Screen time**

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



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

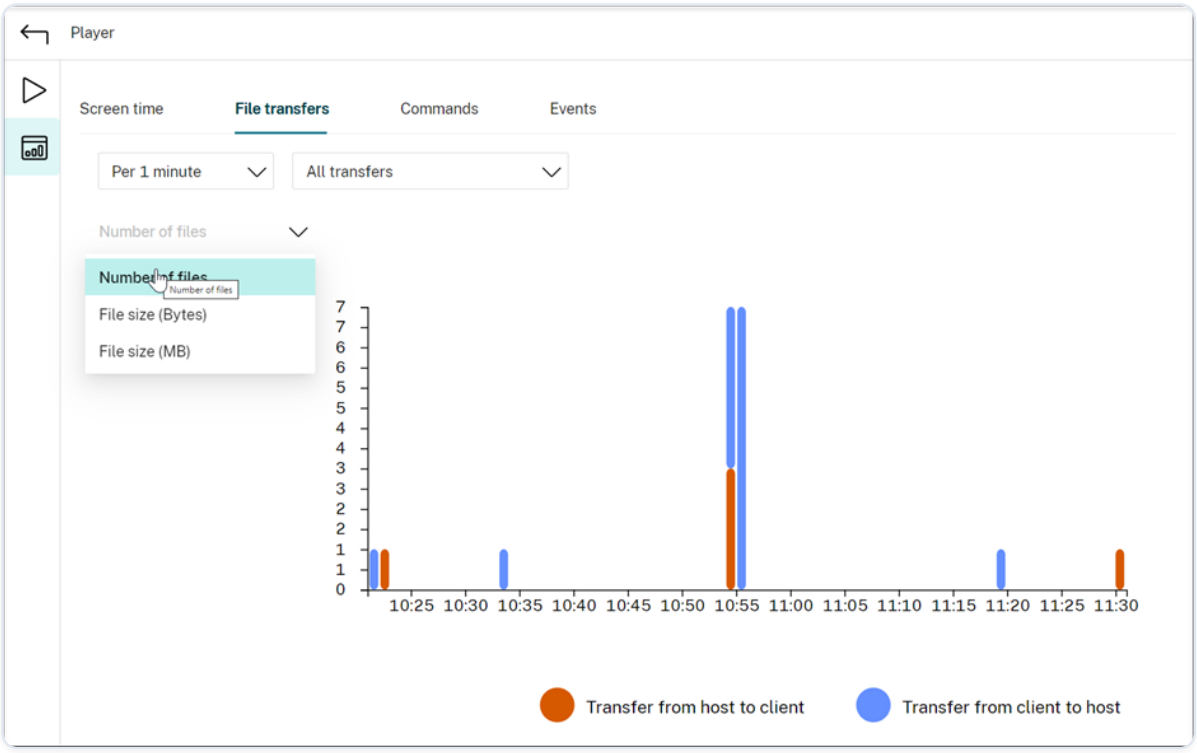


- **File transfers**

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

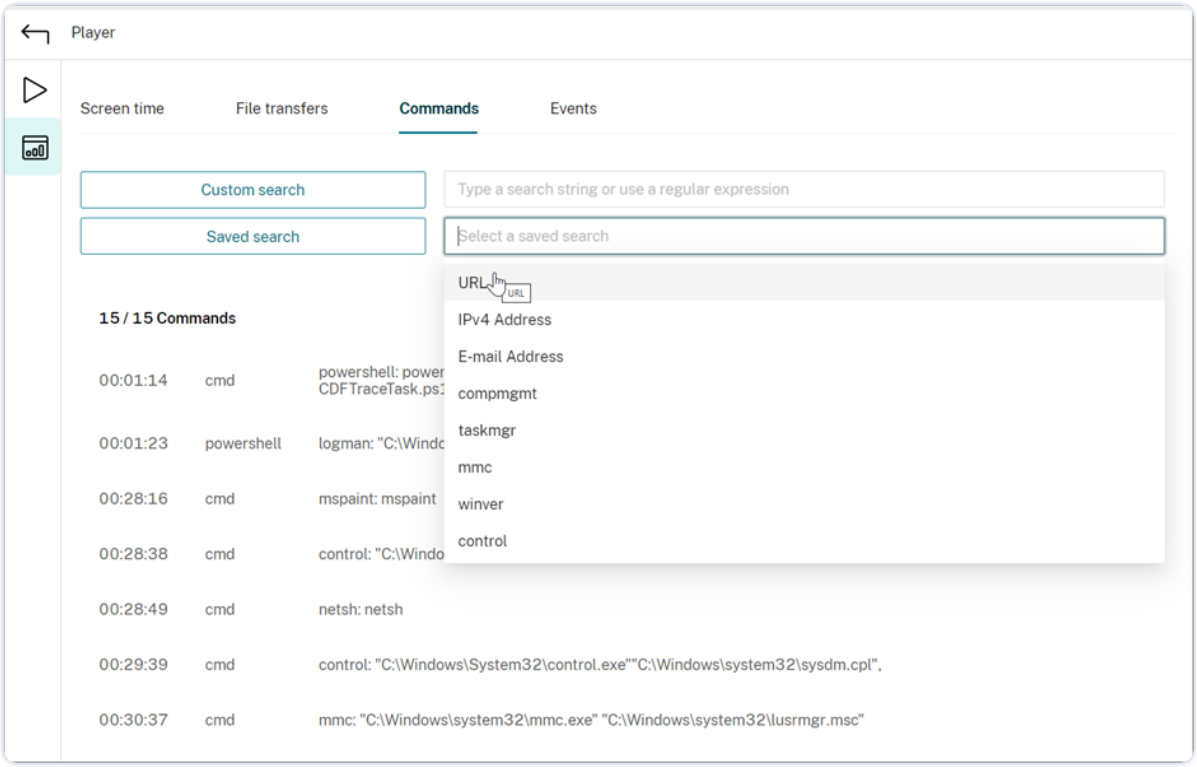
  - Time granularity: **Per 1 minute**, **Per 10 minutes**, **Per hour**
  - File transfer destination: **All transfers**, **Transfer from host to client**, **Transfer from client to host**
  - Number or size (Bytes or MB) of transferred files

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



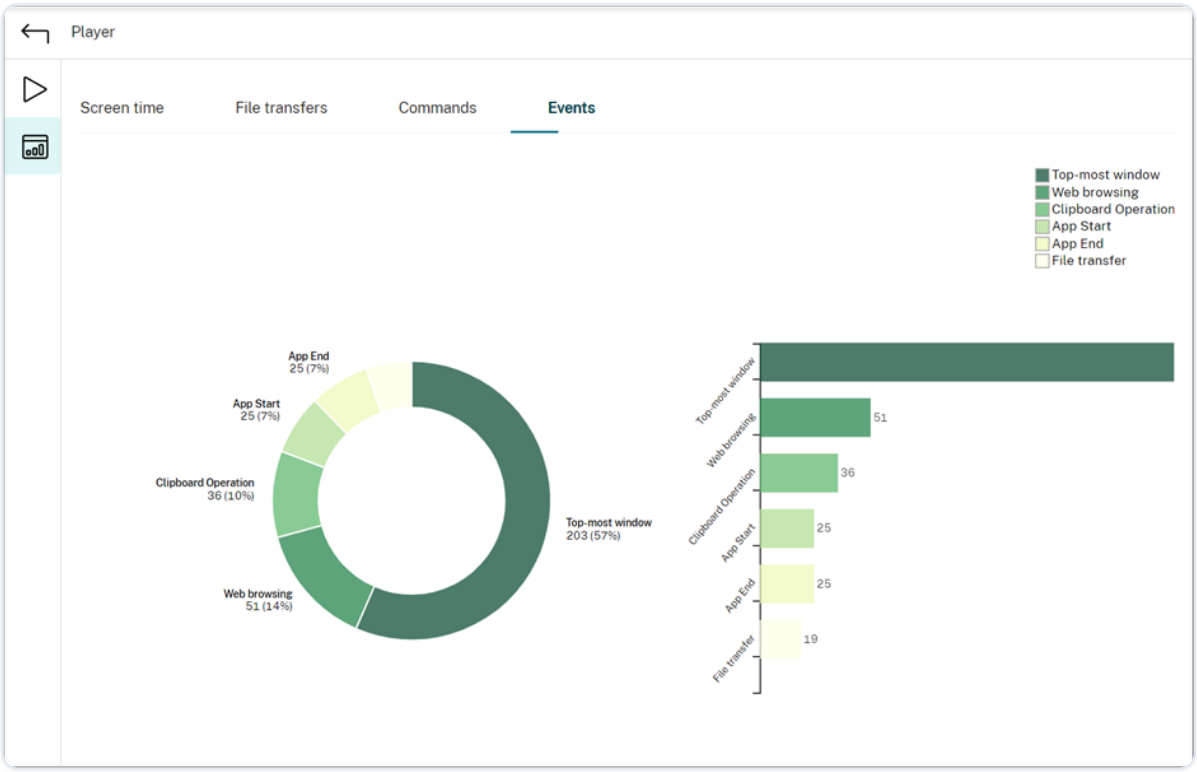
- **Commands**

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



- **Events**

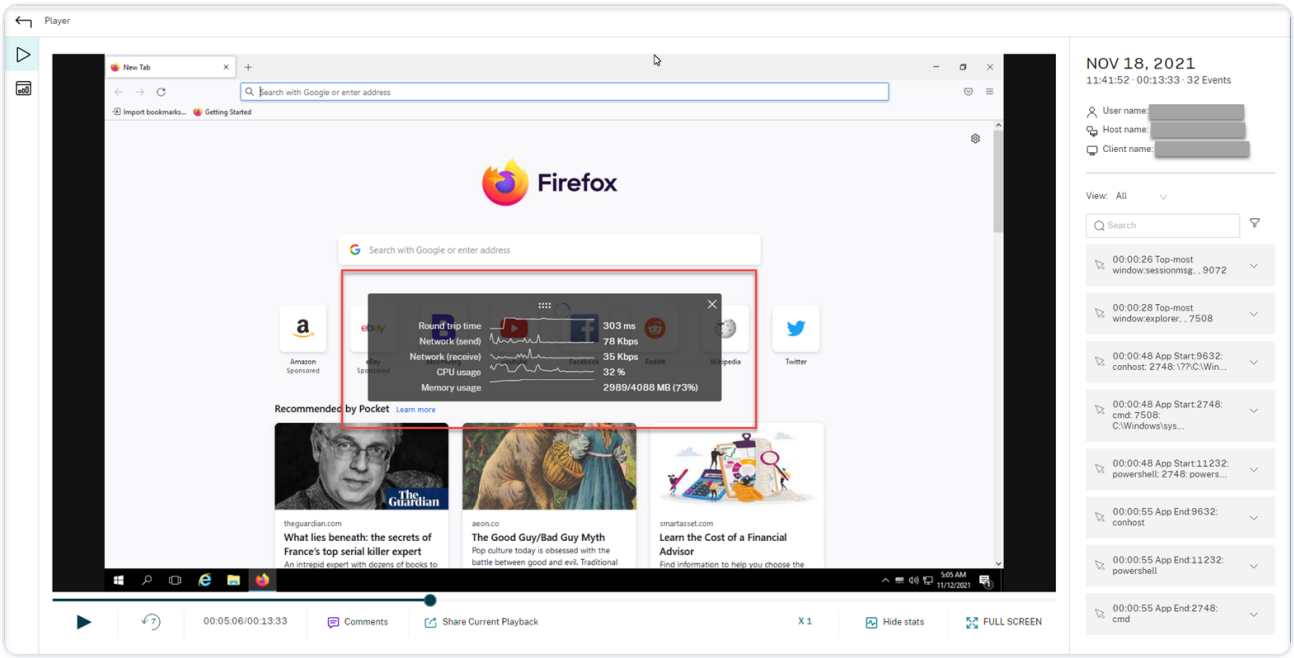
The **Events** tab shows the proportions and numbers of all types of events in the recorded session.



View data points related to each recorded session

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 **semi-transparent**. 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

ICA log database (ICLDB) is a database command-line utility used to manipulate the session recording database records. This utility is installed, during the Session Recording installation, to the `<Session Recording Server installation path>\Bin` folder on the server hosting the Session Recording server.

> **Note:**
>
> If you want to use ICLDB to manage session recording files stored in Azure file shares, run the `SsRecUtils.exe -MountAzureFiles` command. SsRecUtils.exe and ICLDB are in the same folder.

Quick reference chart

The following table lists the commands and options that are available for the ICLDB utility. Type the commands using the following format:

`ICLDB [VERSION | LOCATE | DORMANT | IMPORT | ARCHIVE | REMOVE | REMOVEALL] command-options [/L] [/F] [/S] [/?]`

> **Note:**
>
> More extensive instructions are available in the help associated with the utility. To access the help, from a command prompt, type the `\Program Files\Citrix\SessionRecording\Server\Bin` folder, and type `icldb /?`. To access help for specific commands, type `icldb <specific command> /?`.

COMMAND	DESCRIPTION
`ARCHIVE`	Archives the session recording files that you specify using the RETENTION parameter and the FILTER or RULES parameter. The RETENTION parameter is mandatory. It lets you manipulate session recording files older than the retention period specified. A valid retention period is 2 days at least. Therefore, set RETENTION to 2 or a greater value that suits your needs. The FILTER and RULES parameters are optional. The FILTER parameter lets you filter file paths by using the `*` and `?` wildcards. The RULES parameter sets advanced filters by combining multiple filters strictly in accordance with the `/RULES:FIELD-In-["CONDITION","CONDITION"];FIELD-NotIn-["CONDITION","CONDITION"];` format. For more information, see The RULES parameter for ICLDB ARCHIVE and ICLDB REMOVE commands following this table. The RULES parameter and the FILTER parameter cannot be used together. If you add the FILTER or RULES parameter, only session recording files meeting both RETENTION and FILTER or RULES are manipulated. You can archive both recordings and events in the recordings. The events are archived in the ArchivedEvent database table. Example ICLDB ARCHIVE command: `ICLDB ARCHIVE /RETENTION:<days> [/LISTFILES] [/MOVETO:<dir>] [/NOTE:<note>] [/FILTER:<file path filter>] [/RULES:<advanced filters>] [/L] [/F] [/S] [/?]`

COMMAND	DESCRIPTION
`DORMANT`	Displays or counts the session recording files that are considered dormant. Dormant files are session recordings that were not completed due to data loss. Use this command to verify if you suspect that you are losing data. You can check whether session recording files are becoming dormant for the entire database, or only recordings made within the specified number of days, hours, or minutes. Among the time parameters (DAYS, HOURS, and MINUTES), only one can be specified at a time.
`IMPORT`	Imports session recording files to the Session Recording database. Use this command to rebuild the database if you lose database records. Also, use this command to merge databases (if you have two databases, you can import the files from one of the databases). The 2303 release introduces the RELOCATE parameter to the **IMPORT** command. Without the RELOCATE parameter, the **IMPORT** command parses session recording files in their entirety, which takes time. With the RELOCATE parameter, the **IMPORT** command simply locates the database records of session recording files and updates their file paths directly. Example ICLDB IMPORT command: `ICLDB IMPORT [/LISTFILES] [/RECURSIVE] [/RELOCATE] [/L] [/F] [/S] [/?] [<file>] [<directory>]`
`LOCATE`	Locates and displays the full path to a session recording file using the file ID as the criteria. Use this command when you are looking for the storage location of a session recording file. It is also one way to verify if

COMMAND	DESCRIPTION
	the database is up-to-date with a specific file. Example ICLDB LOCATE command: `ICLDB LOCATE /FILEID:<id> [/L] [/F] [/S] [/?]`
`REMOVE`	Removes the references to session recording files from the database. Use this command (with caution) to clean up the database. You can also remove the associated physical files. When using the **REMOVE** command, specify target session recording files using the RETENTION parameter and the FILTER or RULES parameter. The RETENTION parameter is mandatory. It lets you manipulate session recording files older than the retention period specified. A valid retention period is 2 days at least. Therefore, set RETENTION to 2 or a greater value that suits your needs. The FILTER and RULES parameters are optional. The FILTER parameter lets you filter file paths by using the `*` and `?` wildcards. The RULES parameter sets advanced filters by combining multiple filters strictly in accordance with the `/RULES:FIELD-In-["CONDITION","CONDITION"];FIELD-NotIn-["CONDITION","CONDITION"];` format. For more information, see The RULES parameter for ICLDB ARCHIVE and ICLDB REMOVE commands following this table. The RULES parameter and the FILTER parameter cannot be used together. If you add the FILTER or RULES parameter, only session recording files meeting both RETENTION and FILTER or RULES are manipulated. Example ICLDB REMOVE command: `ICLDB REMOVE /RETENTION:<days> [/LISTFILES] [/DELETEFILES] [/FILTER:<file path`

COMMAND	DESCRIPTION
	`filter>] [/RULES:<advanced filters>] [/L] [/F] [/S] [/?]`
`REMOVEALL`	Removes all references to session recording files from the Session Recording database and returns the database to its original state. The actual physical files are not deleted; however, you cannot search for these files in the Session Recording player. Use this command (with caution) to clean up the database. Deleted references can be reversed only by restoring from your backup.
`VERSION`	Displays the Session Recording database schema version.
`/L`	Logs the results and errors to the Windows event log.
`/F`	Forces the command to run without prompts.
`/S`	Suppresses the copyright message.
`/?`	Displays help for the commands.

The RULES parameter for ICLDB ARCHIVE and ICLDB REMOVE commands

The RULES parameter sets advanced filters by combining multiple filters strictly in accordance with the `/RULES:FIELD-In-["CONDITION","CONDITION"];FIELD-NotIn-["CONDITION","CONDITION"];` format, where:

- "**FIELD**" sets a filter with a field, which can be "**path**", "**user**", "**group**", "**deliverygroup**", "**application**", "**server**", "**client**", or any other column in the database table called **dbo.ICLFile**.
- "**In**" means that at least one of the filter conditions in the brackets must be met for a recording file to be an operation object.

- "**NotIn**" means that recording files that meet any of the filter conditions in the brackets are excluded from the operation.
- "**CONDITION**" sets a filter condition with a record (or row) in the database table called dbo.ICLFile.
- User and group records must be entered in the format of `<domain>.<name>`.
- Path records can be filtered by using Windows wildcards.
- Each "**CONDITION**" item must be surrounded by double quotes (`""`), and two "**CONDITION**" items must be separated by a comma (`,`).
- Do not add spaces when entering "**CONDITION**" items unless a "**CONDITION**" item itself contains spaces.
- If a "**CONDITION**" item contains one or more commas, enclose the "**CONDITION**" item in double quotes that are followed by escaped double quotes `""" """`.
- Multiple filters can be used in various combinations. End each filter with a semicolon (`;`).
- The "AND" logical operator is used to compute the multiple filters. There is no limit to the number of filters, but the total length of RULES must not exceed 2,048 bytes.

Examples:

- `/RULES:group-In-["BUILTIN.Guests"];`
- `/RULES:path-In-["S:\SessionRecordings\2023*"];group-NotIn-["Mydomain.Suspicious","Mydomain.Persistence"];`
- `/RULES:deliverygroup-In-["RdsDesktopAndAppGroup"];user-In-["Mydomain.AdminA","""Mydomain.Admin,,,B"""];`
- `/RULES:EndReasonID-In-["1","2"];`

Archive session recording files

To maintain an adequate level of spare disk capacity in the recording storage locations, archive session recording files regularly. Depending on the amount of available disk space and typical size of recording files, archiving intervals differ. Session recording files must be older than two days from the start date before a session recording file can be archived. This rule is to prevent any live recordings from being archived before they become complete.

Two methods are available when you archive session recordings. The database record for a recording file can be updated to have a status of archived while the file remains in the recording storage location. This method can be used to reduce the search results in the player. The other

method is to update the database record for a recording file to the archived status and move the file from the recording storage location to another location for backup to alternative media. When the ICLDB utility moves session recording files, the files are moved to the specified directory where the original file folder structure of year/month/day no longer exists.

The session recording record in the Session Recording database contains two fields associated with archiving—the archive time and archive note. The archive time represents the current date and time that a recording was archived. The archive note is an optional text note that can be added during archiving. The two fields indicate that a recording has been archived and the time of archiving.

In the Session Recording player, archived session recordings show a status of Archived and the date and time of archiving. Session recordings that have been archived might still be played if the files have not been moved. If a session recording file was moved during archiving, a file not found error is displayed. The session recording file must be restored before the session can be played. To restore a session recording file, provide the File ID and Archive Time of the recording file. Restoring archived files is discussed further in the following Restore session recording files section.

The **ARCHIVE** command of the ICLDB utility has several parameters that are described as follows:

- **/RETENTION:<days\>** - The retention period in days for session recordings. Recordings older than the number of days specified are marked as archived in the Session Recording database. The retention period must be an integer number greater than or equal to 2 days.
- **/FILTER:<filter\>**: Lets you filter file paths by using the `*` and `?` wildcards. The FILTER parameter is optional. If you add the FILTER parameter, only those session recording files meeting both RETENTION and FILTER are archived.
- **/RULES:<advanced filters\>**: Sets advanced filters by combining multiple filters strictly in accordance with the `/RULES:FIELD-In-["CONDITION","CONDITION"];FIELD-NotIn-["CONDITION","CONDITION"];` format. The RULES parameter and the FILTER parameter cannot be used together. For more information, see the preceding The RULES parameter for ICLDB ARCHIVE and ICLDB REMOVE commands section in this article.
- **/LISTFILES** – Lists the full path and file name of session recording files as they are being archived. This parameter is optional.
- **/MOVETO:<directory\>** - The directory to which you physically move archived session recording files. The specified directory must exist. This parameter is optional. If no directory is specified, the files remain in their original storage location.

- **/NOTE:<note\>** - A text note that is added to the database record for each session recording archived. Ensure that the note is enclosed with double quotes. This parameter is optional.
- **/L** – Logs the results and errors to the Windows event log of the number of session recording files archived. This parameter is optional.
- **/F** – Forces the archive command to run without prompts. This parameter is optional.

To archive session recordings in the Session Recording database and physically move session recording files

1. Log on to the server where the Session Recording server is installed as a local administrator.
2. Start a command prompt.
3. Change from the current working directory to the Bin directory of the Session Recording server installation path (`<Session Recording server Installation Path>\Bin`).
4. Run the `ICLDB ARCHIVE /RETENTION:<days> [/LISTFILES] [/MOVETO:<dir>] [/NOTE:<note>] [/FILTER:<file path filter>] [/RULES:<advanced filters>] [/L] [/F] [/S] [/?]` command. The parameters in brackets are optional. Remove the brackets when running the command. The RULES parameter and the FILTER parameter cannot be used together. **days** is the retention period for session recording files, **directory** is the directory where archived session recording files are moved to, and **note** is the text note that is added to the database record for each session recording file being archived. Enter **Y** to confirm the archive.

To only archive session recordings in the Session Recording database

1. Log on to the server where the Session Recording server is installed as a local administrator.
2. Start a command prompt.
3. Change from the current working directory to the Bin directory of the Session Recording server installation path (<Session Recording server installation path\>\Bin).
4. Run the `ICLDB ARCHIVE /RETENTION:<days> [/LISTFILES] [/NOTE:<note>] [/FILTER:<file path filter>] [/RULES:<advanced filters>] [/L] [/F] [/S] [/?]` command. The parameters in brackets are optional. Remove the brackets when running the command. The RULES parameter and the FILTER parameter cannot be used together. **days** is the retention period for session recordings and **note** is the text note that is added to the database record for each session recording being archived. Enter **Y** to confirm the archive.

Restore session recording files

To view a recording file archived in the Session Recording database and moved from the recording storage location, restore it. Archived session recordings that were not moved from the recording storage location during archiving are still accessible in the player.

Two methods are available for restoring session recording files that have been moved. Copy the required session recording file to the restore directory for archived files. Or, import the required session recording file back to the Session Recording database by using the ICLDB utility. We recommend the first method for restoring archived session recording files. Remove archived files copied to the restore directory for archived files when you no longer need them.

The Session Recording Broker uses the **Restore directory for archived files** when a session recording file is not found in its original storage location. This case occurs when the player requests a session recording file for playback. The Session Recording Broker first attempts to find the session recording file in the original storage location. If the file is not found in the original storage location, the Session Recording Broker then checks the **Restore directory for archived files**. If the file is present in the restore directory, the Session Recording Broker sends the file to the player for playback. If the file is not found, the Session Recording Broker sends a file not found error to the player.

Importing an archived recording file updates the Session Recording database with the session recording information from the file, including a new storage path. Importing an archived session recording file doesn't move the file back to the original storage location when the session was recorded.

Note: An imported session recording file has the archive time and archive note cleared in the Session Recording database. The next time the **ICLDB ARCHIVE** command is run, the imported session recording file might become archived again.

The **ICLDB IMPORT** command is useful to import a large number of archived recording files. It can repair or update incorrect and missing session recording data in the Session Recording database. It is also useful to move session recording files from one storage location to another on the Session Recording server. You can use the **ICLDB IMPORT** command to repopulate the Session Recording database with session recordings after running the **ICLDB REMOVEALL** command.

The **IMPORT** command of the ICLDB utility has several parameters that you can use for restoring archived recording files:

- **/LISTFILES** – Lists the full path and file name of session recording files while they are being imported. This parameter is optional.

- **/RECURSIVE** – Searches all subdirectories for session recording files. This parameter is optional.
- **/RELOCATE** – Without the RELOCATE parameter, the IMPORT command parses session recording files in their entirety, which takes time. With the RELOCATE parameter, the IMPORT command simply locates the database records of session recording files and updates their file paths directly.
- **/L** – Logs the results and errors to the Windows event log the number of session recording files imported. This parameter is optional.
- **/F** – Forces the IMPORT command to run without prompts. This parameter is optional.

> **Note:**
>
> The IMPORT command of the ICLDB utility also provides an optional parameter, RELOCATE, that you can use for relocating recording files. For more information, see the Relocate session recording files section in this article.

Restore session recording files by using the restore directory for archived files

1. Log on as a local administrator to the server where the Session Recording server is installed.
2. In Session Recording Player Properties, determine the File ID and Archive Time of the archived session recording file.
3. Locate the session recording file in your backups using the File ID specified in Session Recording Player Properties. Each session recording has a file name of `i_<FileID>.icl`, where FileID is the ID of the session recording file.
4. Copy the session recording file from your backup to the restore directory for archived files. To determine the restore directory for archived files:
    a. From the **Start** menu, choose **Start** > **All Programs** > **Citrix®** > **Session Recording Server Properties**.
    b. In **Session Recording Server Properties**, select the **Storage** tab. The current restore directory appears in the **Restore directory for archived files** field.

Restore session recording files by using the ICLDB IMPORT command

1. Log on as a local administrator to the server where the Session Recording server is installed.

2. Start a command prompt.
3. Change from the current working directory to the Bin directory of the Session Recording server installation path (`<Session Recording server installation path>\Bin`).
4. Either:

   - Run the `ICLDB IMPORT /LISTFILES /RECURSIVE /L <directory>` command where **directory** is the name of one or more directories, separated by a space containing session recording files. Enter **Y** to confirm the import.
   - Run the `ICLDB IMPORT /LISTFILES /L <file>` command where **file** is the name of one or more session recording files, separated by a space. Wildcards might be used to specify session recording files. Enter **Y** to confirm the import.

Relocate session recording files

You can move session recording files to different storage paths for load balancing or other purposes. To ensure that the files can still be played, you must update their new paths to the Session Recording database. To do so, use the **ICLDB IMPORT** command. To accelerate the import process, append the RELOCATE parameter to the **ICLDB IMPORT** command.

> **Note:**
>
> The RELOCATE parameter is optional. Without the RELOCATE parameter, the ICLDB IMPORT command parses session recording files in their entirety, which takes time. With the RELOCATE parameter, the ICLDB IMPORT command simply locates the database records of session recording files and updates their file paths directly.

> The following steps illustrate how to use the RELOCATE parameter to update new file paths to the Session Recording database.

1. Move session recording files to different storage paths as needed.
2. Log on as a local administrator to the server where the Session Recording server is installed.
3. Start a command prompt.
4. Change from the current working directory to the Bin directory of the Session Recording server installation path (`<Session Recording server installation path>\Bin`).
5. Either:

- Run the `ICLDB IMPORT /LISTFILES /RECURSIVE /RELOCATE /L <directory>` command where **directory** is the name of one or more directories, separated by a space containing session recording files. Enter **Y** to confirm the import.
- Run the `ICLDB IMPORT /LISTFILES /RELOCATE /L <file>` command where **file** is the name of one or more session recording files, separated by a space. Wildcards might be used to specify session recording files. Enter **Y** to confirm the import.

Note:

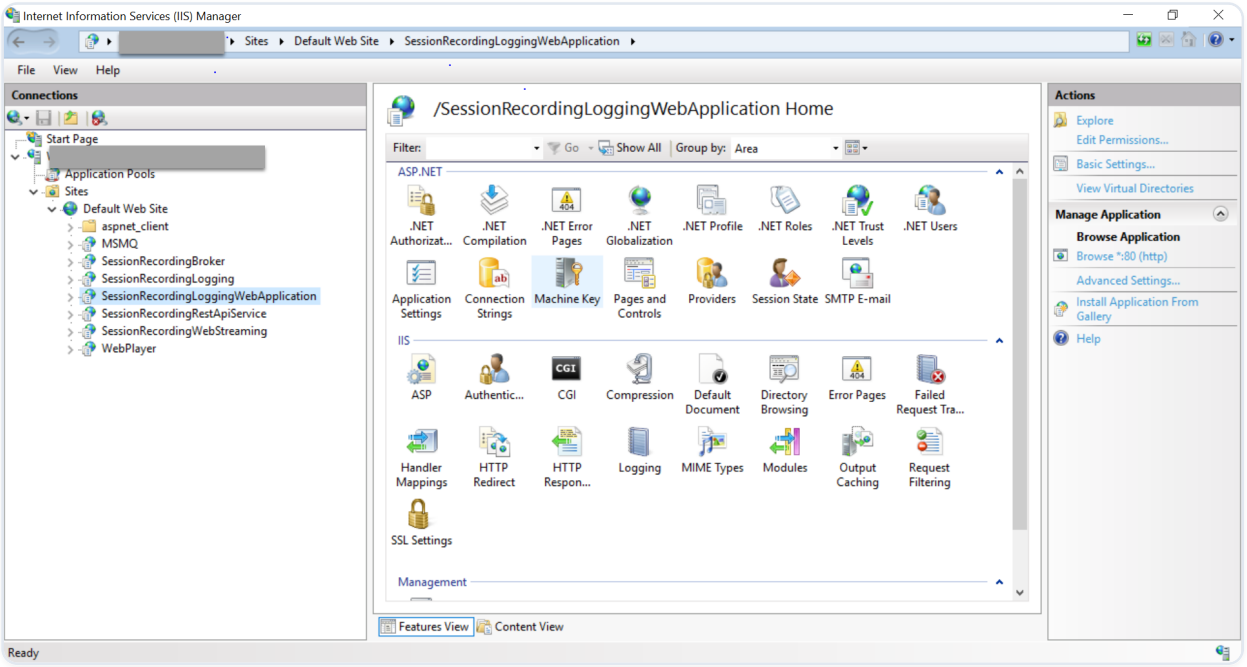
- The RELOCATE parameter assumes that there are already records of the session recording files in the Session Recording database.
- The session recording files must be playable before being moved. Otherwise, the RELOCATE parameter does not help.
- The new storage paths of the session recording files must be recognizable by the Session Recording server. You can try them on the **Storage** tab of **Session Recording Server Properties**.

Manage and query administrator logging

Query the administrator logging data

Requirements

- An administrator assigned to both the **LoggingReader** and the **Player** roles can view administrator logging. To assign users to the roles, go to the Session Recording Authorization Console.
- The administrator logging page is integrated with the web player. The web player must be installed for querying administrator logging. Otherwise, 404 (page not found) errors can occur.
- The language set for the web player browser must match the language you selected when you installed the Session Recording Administration components.
- Ensure that your SessionRecordingLoggingWebApplication site in IIS and the web player have the same SSL settings. Otherwise, 403 errors occur when you request to access the administrator logging data.



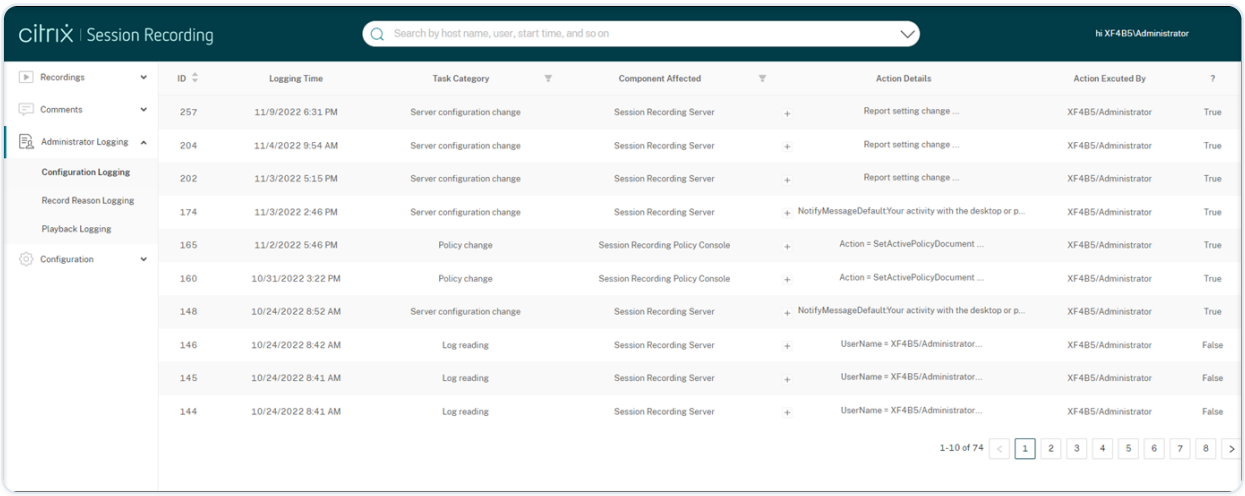
Steps

You can query administrator logging data about a Session Recording server both from the machine that hosts the server and from other machines:

On the machine hosting the target Session Recording server

1. From the **Start** menu, choose **Session Recording Administrator Logging**.
2. Type the credentials of a **LoggingReader** user.

   The administrator logging webpage integrated with the web player appears.



On other machines

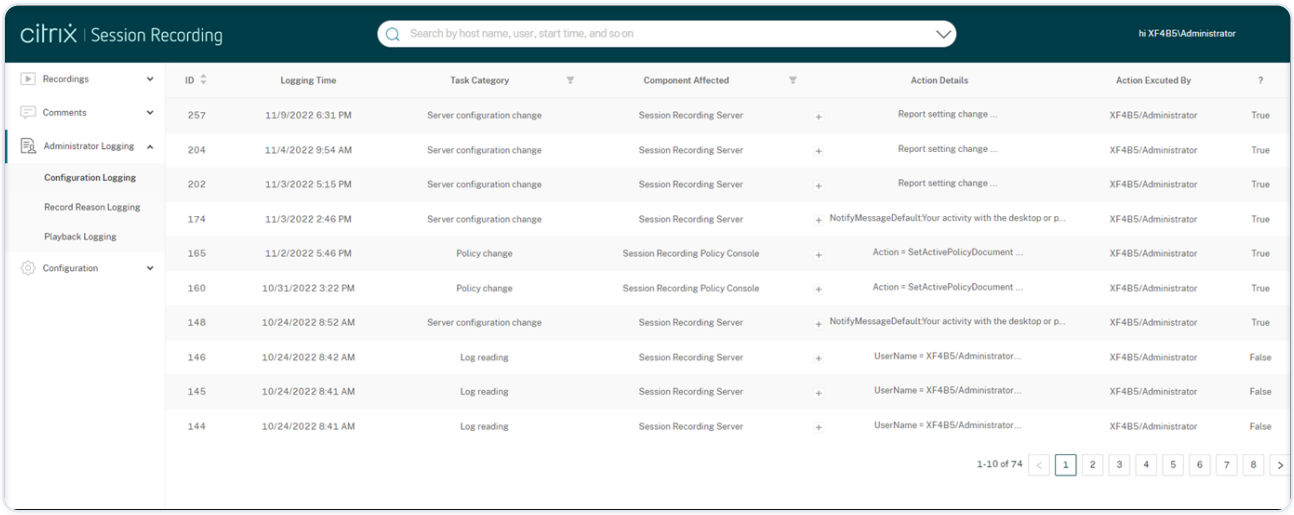
1. Open a web browser and visit the webpage for administrator logging.
   - **For HTTPS:** `https://servername/WebPlayer/#/logging/config` and `https://servername/WebPlayer/#/logging/record`, where `servername` is the name of the machine hosting the Session Recording server.
   - **For HTTP:** `http://servername/WebPlayer/#/logging/config` and `http://servername/WebPlayer/#/logging/record`, where `servername` is the name of the machine hosting the Session Recording server.
2. Type the credentials of a **LoggingReader** user.

Logging data overview

Administrator logging data consists of:

- Configuration logging
- Recording reason logging
- Playback logging.

Configuration logging



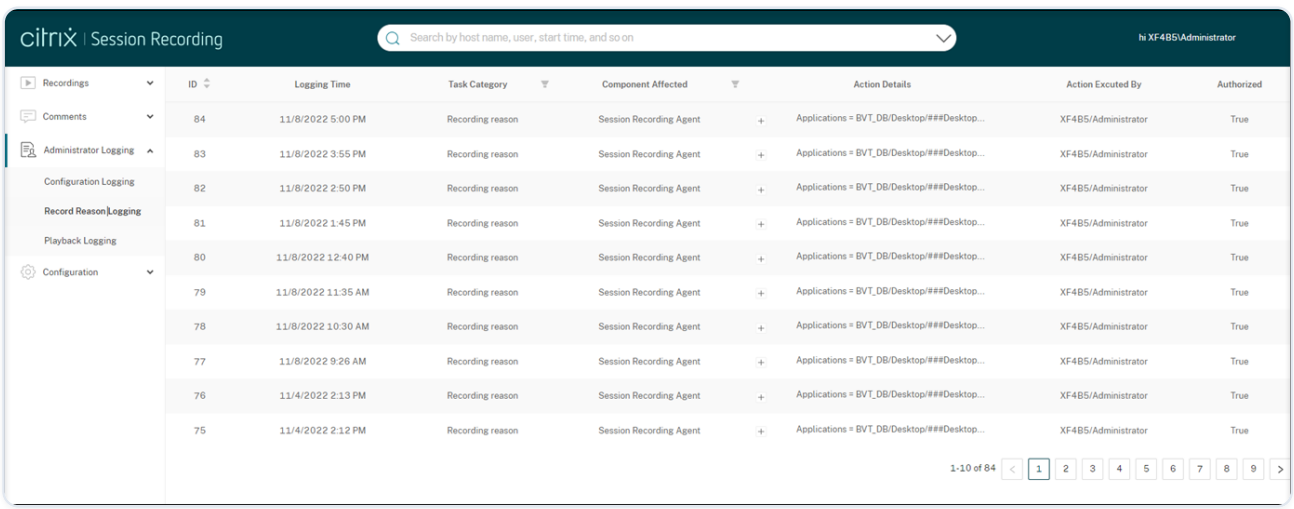
This part logs the following administrator activities:

- **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

To log administrator activities, enable administrator logging on your Session Recording servers. For more information, see Disable or enable administrator logging. To enhance security, you can also configure an administrator logging service account.

> **Tip:**
>
> You can enable administrator logging both through the Session Recording service and through Session Recording Server Properties.

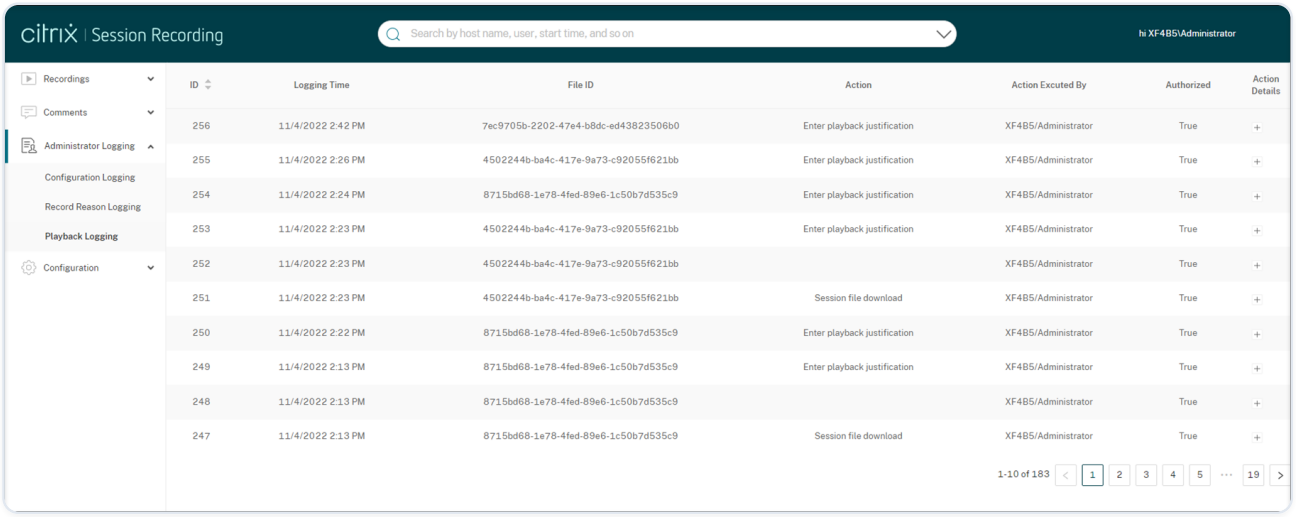
Recording reason logging



This part logs which policies have triggered recordings.

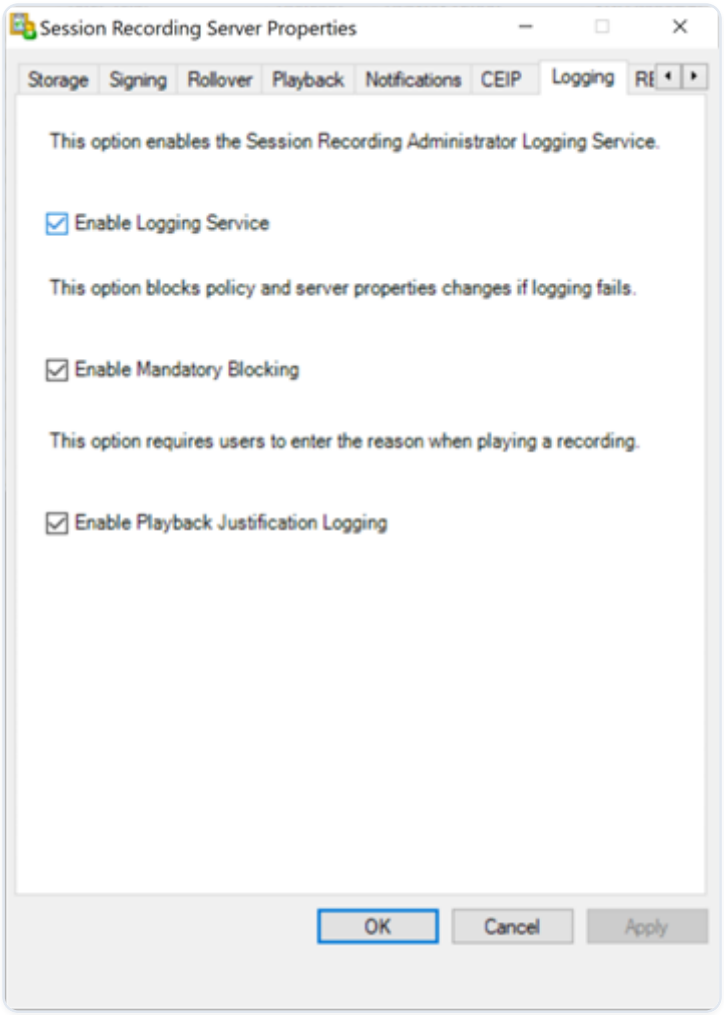
To enable recording reason logging, enable both administrator logging and recording reason logging on your Session Recording servers. If administrator logging is disabled, enabling recording reason logging does not take effect. For information about enabling recording reason logging, see Disable or enable the recording reason logging.

Playback logging



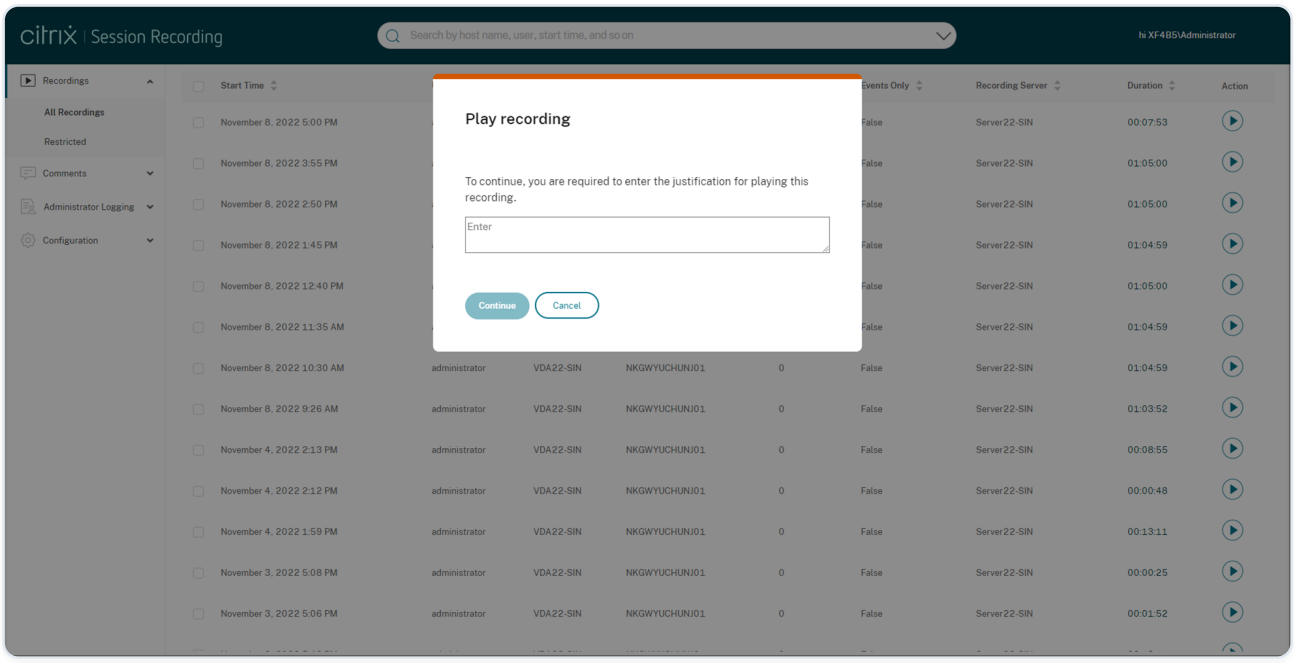
This part logs playback-related actions. For more information about each log record, click the plus sign (+) in the **Action Details** column.

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.

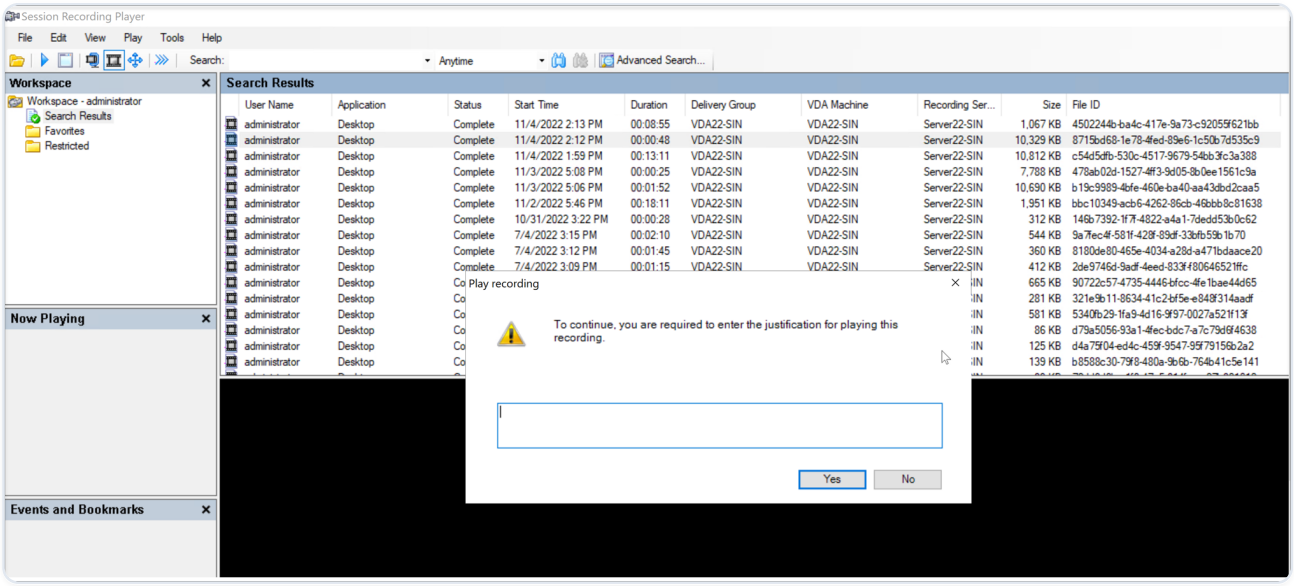


With playback justification logging enabled, each time a user plays a recording, a dialog box appears, asking the user to enter a playback justification. For example, see the following screen captures:

Justification required for playback in the web player:



Justification required for playback in the Session Recording player:



On the condition that playback justification logging is enabled on a Session Recording server, mind the following tips for using playback justifications:

- If you use a player that connects to a Session Recording server, a justification is required, even for recording files that you downloaded to a local path.
- A single session can generate multiple recordings because of file rollover. When you play back such a recorded session, you must enter a justification for each of its recordings.

Disable or enable administrator logging

After installation, you can disable or enable the Session Recording administrator logging feature in **Session Recording Server Properties**.

1. As an administrator, log on to the machine where Session Recording administrator logging is installed.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. Click the **Logging** tab.

When Session Recording administrator logging is disabled, no new activities are logged. You can query the existing logs from the web-based UI.

When **mandatory blocking** is enabled, the following activities are blocked if the 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.

Configure an administrator logging service account

By default, administrator logging is running as a web application in Internet Information Services (IIS), and its identity is Network Service. To enhance the security level, you can change the identity of this web application to a service account or a specific domain account.

1. As an administrator, log on to the machine hosting the Session Recording server.
2. In IIS Manager, click **Application Pools.**
3. In **Application Pools**, right-click **SessionRecordingLoggingAppPool** and choose **Advanced Settings**.
4. Change the attribute **identity** to the specific account that you want to use.
5. Grant the **db_owner** permission to the account for the database **CitrixSessionRecordingLogging** on the Microsoft SQL Server.
6. Grant the read permission to the account for the registry key at **HKEY_LOCAL_MACHINE\ \SOFTWARE\\Citrix\\SmartAuditor\\Server**.

> **Warning:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Disable or enable the recording reason logging

By default, administrator logging logs every recording reason after the policy query completes. This behavior might generate many logs. To improve the performance and save the storage, disable this kind of logging in the registry.

1. As an administrator, log on to the machine hosting the Session Recording server.
2. Open the Registry Editor.
3. Browse to **HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\SmartAuditor\\Server**.
4. Set the value of **EnableRecordingActionLogging** to:

0: disable the recording reason logging

1: enable the recording reason logging

Best practices

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

- Configure load balancing in an existing deployment
- Deploy and load-balance Session Recording in Azure

Configure load balancing in an existing deployment

You can add load balancing nodes using Citrix ADC in an existing Session Recording deployment. The following servers are used as an example. You can also deploy and load-balance Session Recording in Azure.

- Session Recording

HOST NAME	SERVER ROLE	OS	IP ADDRESS
SRServer1	Session Recording Server	Windows Server	10.63.32.55
LBDC	Domain controller	Windows Server	10.63.32.82
TSVDA	Session Recording Agent	Windows Server	10.63.32.215
SRSQL	Session Recording database and the file server	Windows Server	10.63.32.91

  All Session Recording components and the domain controller share a domain, for example, `lb.com`. The domain administrator account, for example, lb\administrator, is used for server logon.

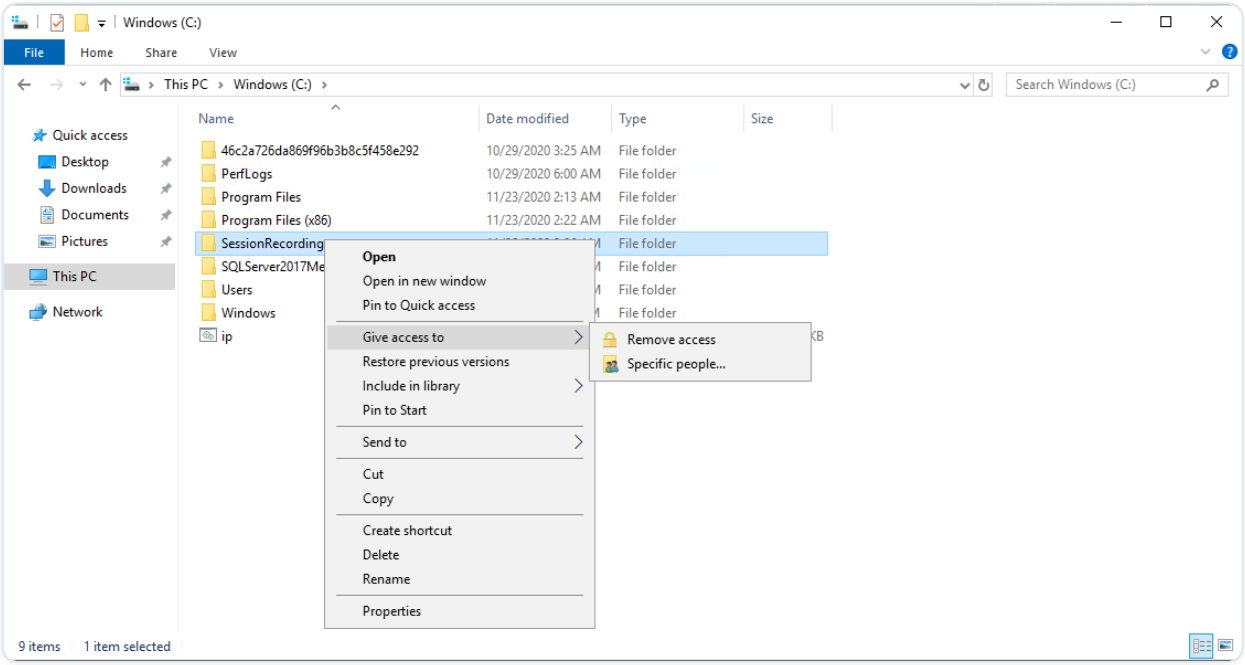
- Citrix ADC

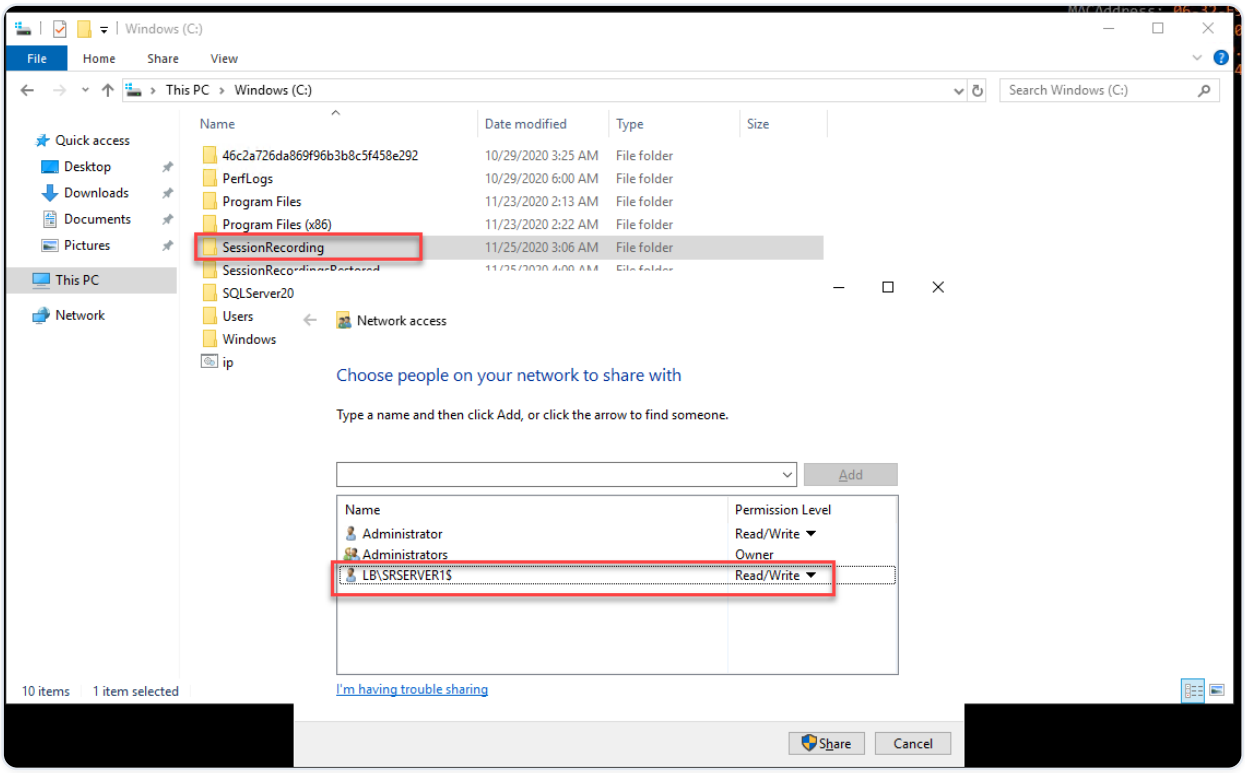
HOST NAME	SERVER ROLE	MANAGEMENT IP ADDRESS (NSIP)	SUBNET IP ADDRESS (SNIP)
Netscaler	Citrix ADC VPX instance	10.63.32.40	10.63.32.109

For more information, see Deploy a Citrix ADC VPX instance.

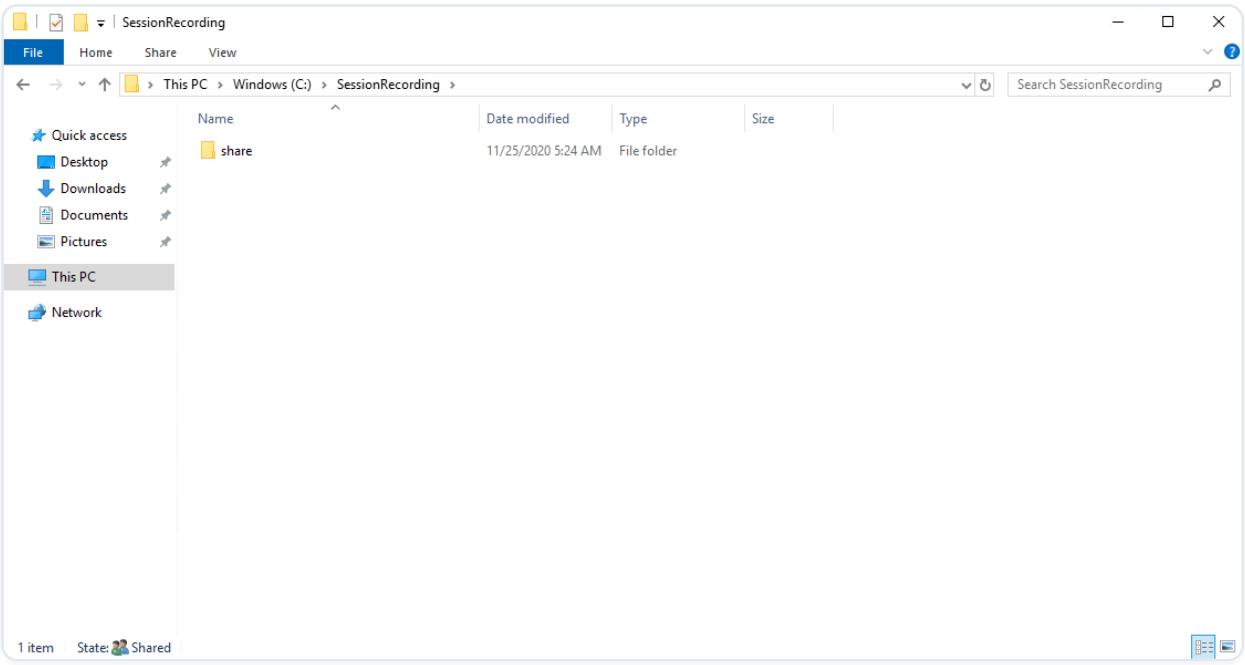
Step 1: Create shared folders on the file server

1. Log on to the file server by using a domain administrator account, for example, `lb\administrator`.
2. Create a folder to store recordings and name the folder `SessionRecording`, for example, `C:\SessionRecording`. Share the Read/Write permission of the folder with a Session Recording server. Using `SRServer1` as an example, type `LB\SRSERVER1$`. The dollar sign `$` is required.





3. Create a subfolder within the `SessionRecording` folder and name the subfolder `share`, for example, `C:\SessionRecording\share`.



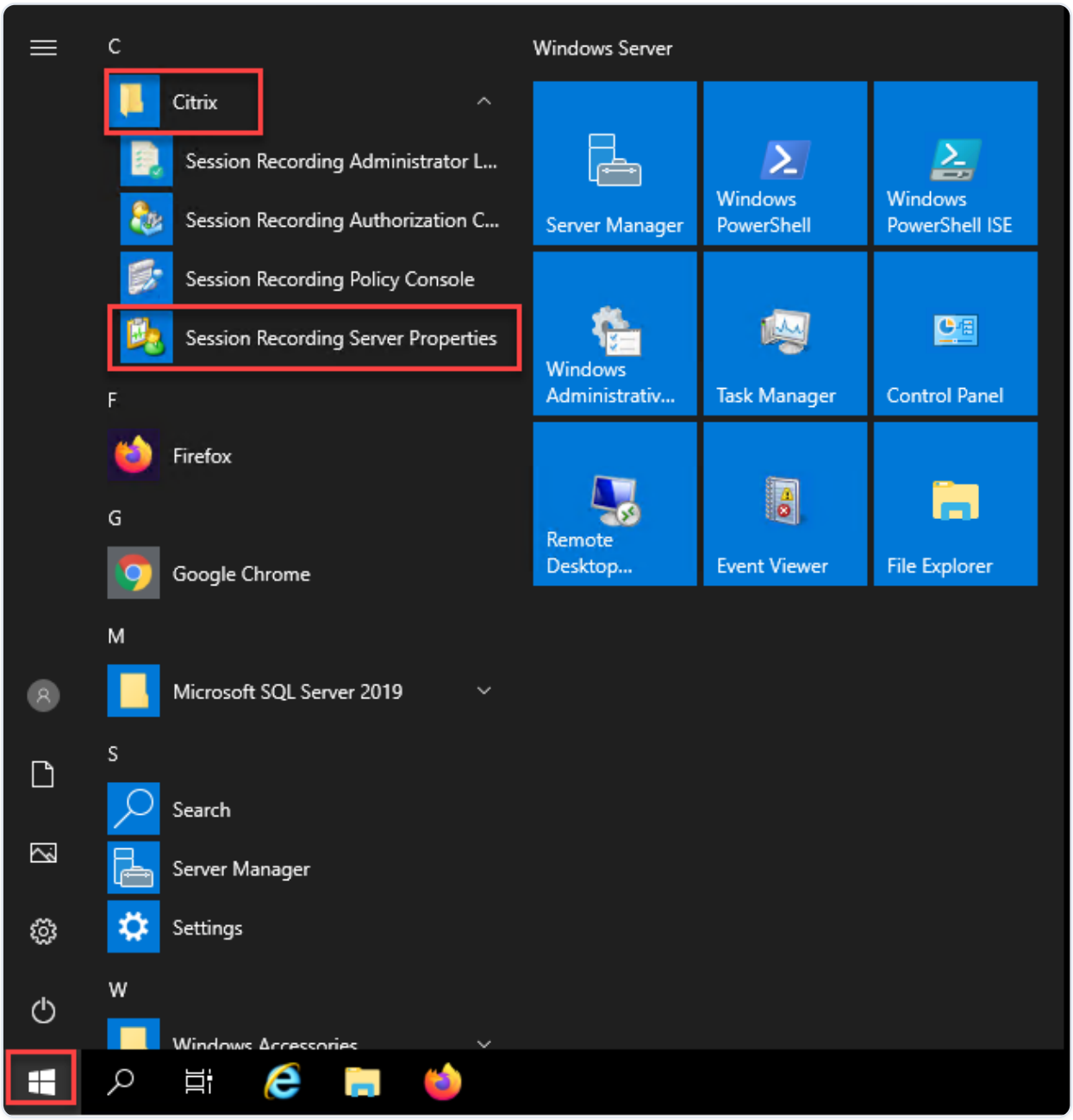
4. Create another folder to restore archived recordings and name the folder `SessionRecordingsRestored`, for example, `C:\ SessionRecordingsRestored`. Share the Read/Write permission of the folder with a Session Recording server. Using `SRServer1` as an example, type `LB\SRSERVER1$`. The dollar sign `$` is required.

5. Create a subfolder within the `SessionRecordingsRestored` folder and name the subfolder `share`, for example, C:\ `SessionRecordingsRestored\share`.

Step 2: Configure an existing Session Recording server to support load balancing

This step describes how to configure an existing Session Recording server to support load balancing. Step 7 details the procedure of adding more Session Recording servers to your existing deployment.

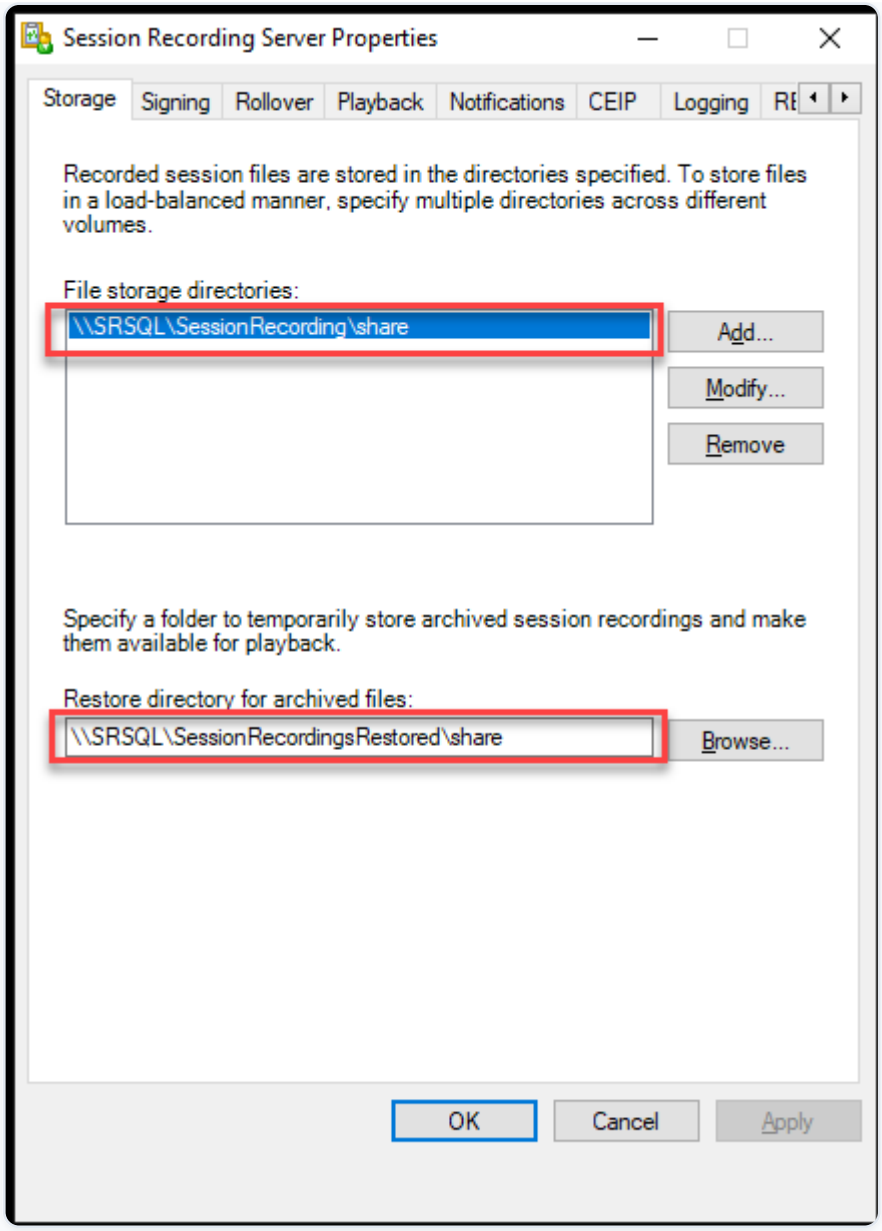
1. Log on to a Session Recording server by using a domain administrator account.
2. Open **Session Recording Server Properties**.



3. Add the Universal Naming Convention (UNC) paths created in Step 1 to store and restore recording files, in this example, `\\SRSQL\SessionRecording\share` and `\\SRSQL\SessionRecordingRestored\share`. `SRSQL` is the host name of the file server.

Note:

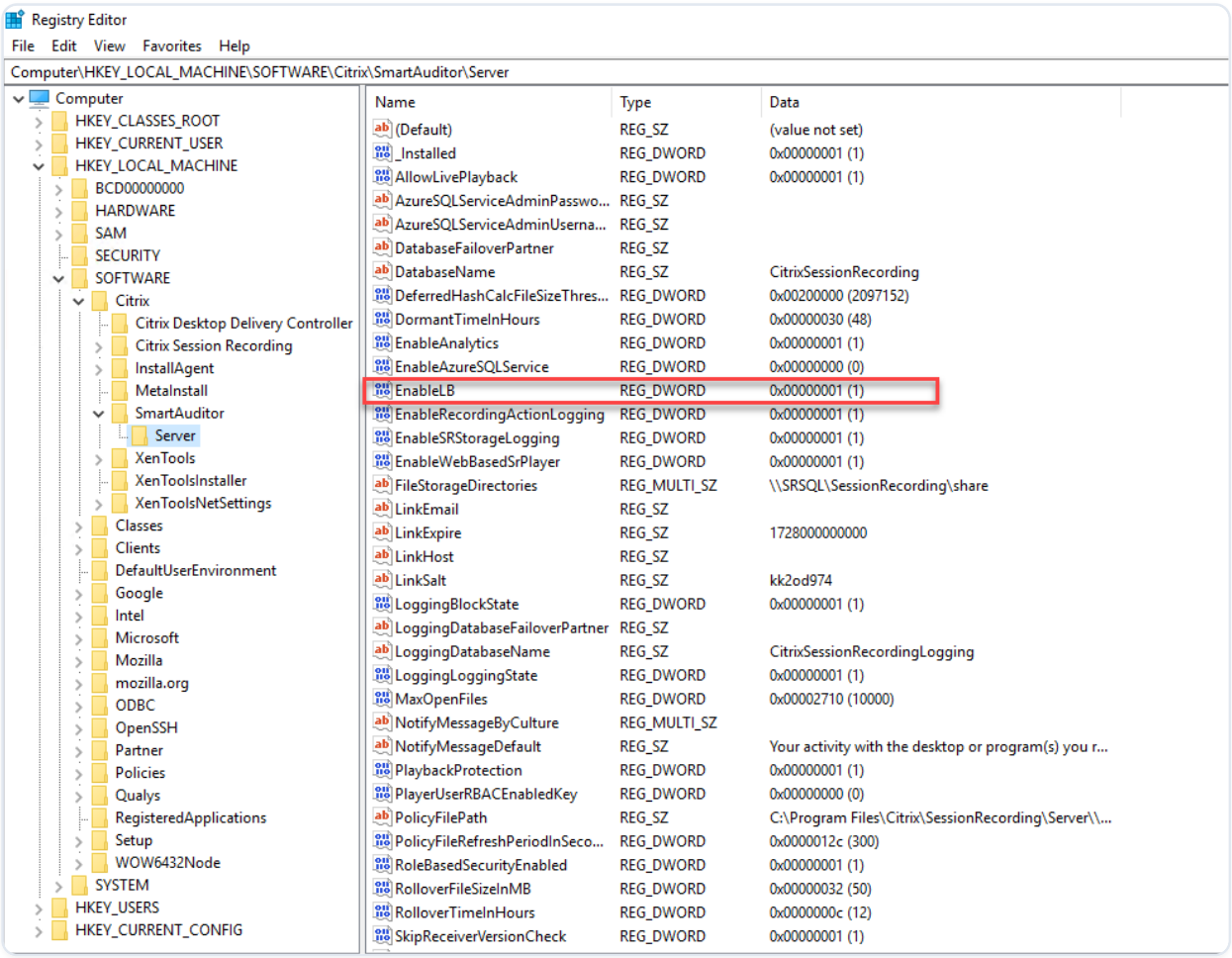
The Session Recording player cannot play files under a path that contains a drive letter or a dollar sign (`$`). The exception is that you install the player and the Session Recording server on the same machine.



4. Add a value to the Session Recording server registry key at `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`.

   Value name: EnableLB

   Value data: 1 (D_WORD, meaning enable)



5. Restart the Citrix Session Recording Storage Manager service.

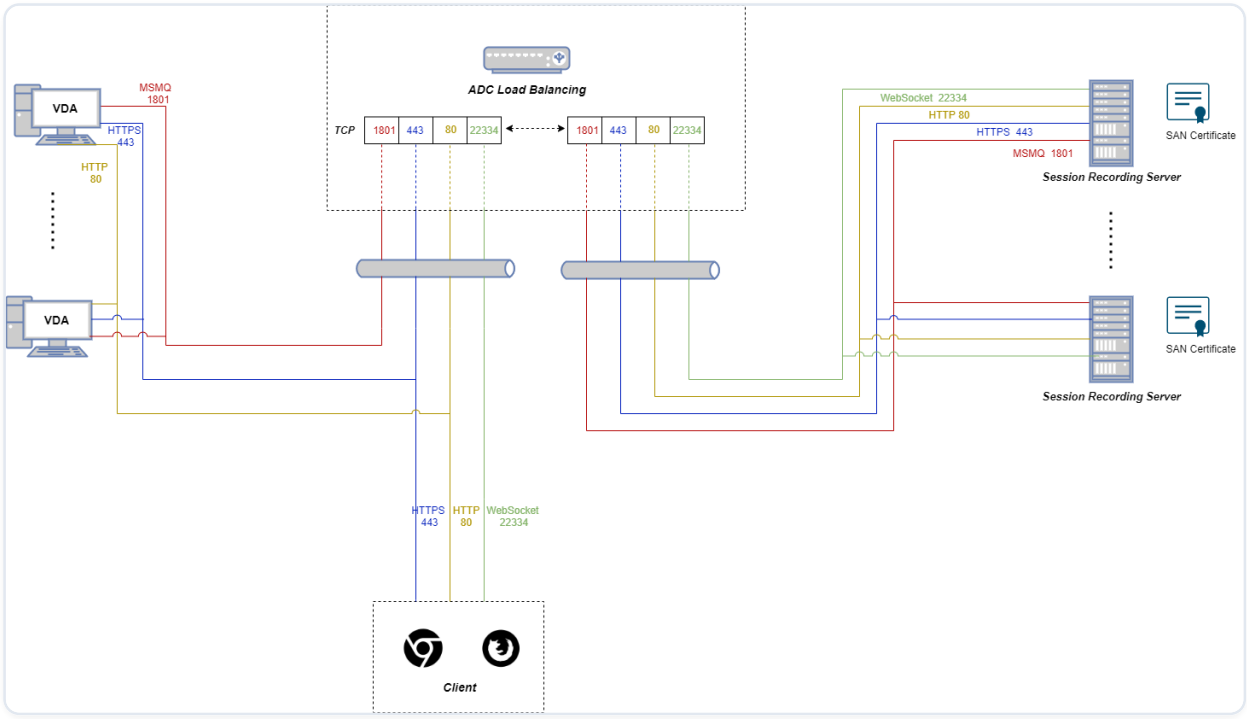
Step 3: Configure load balancing in Citrix ADC

There are two ways to configure load balancing in Citrix ADC - TCP passthrough and SSL offloading.

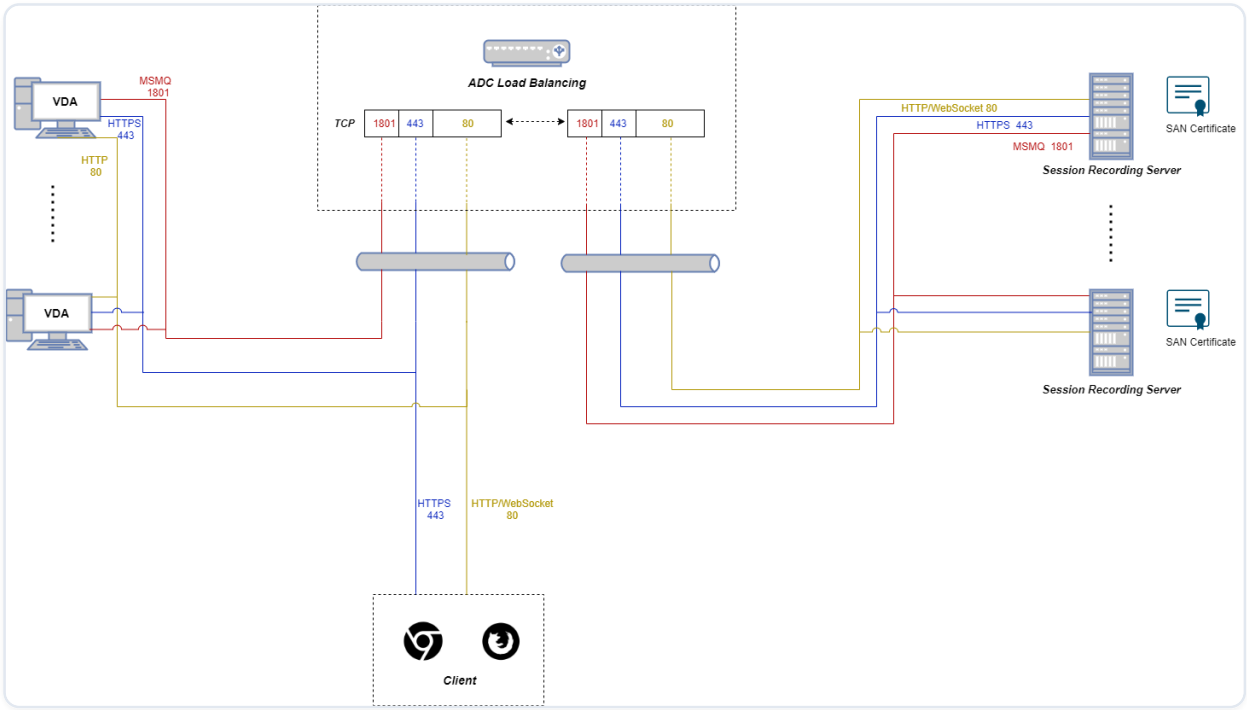
Configure load balancing through TCP passthrough

The following topologies show how to configure load balancing through **TCP passthrough**.

- If you are using the Python-based WebSocket server (Version 1.0):

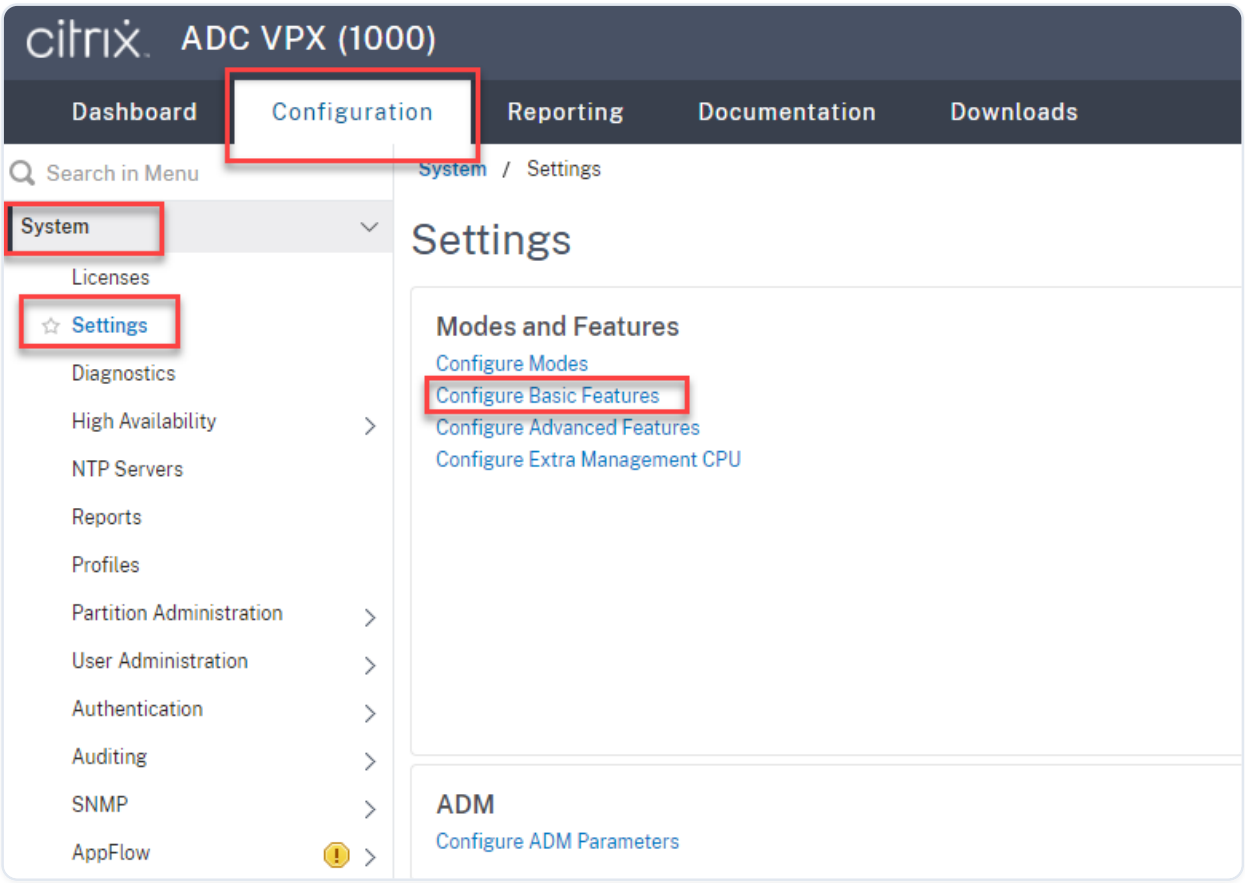


- If you are using the WebSocket server hosted in IIS (Version 2.0):

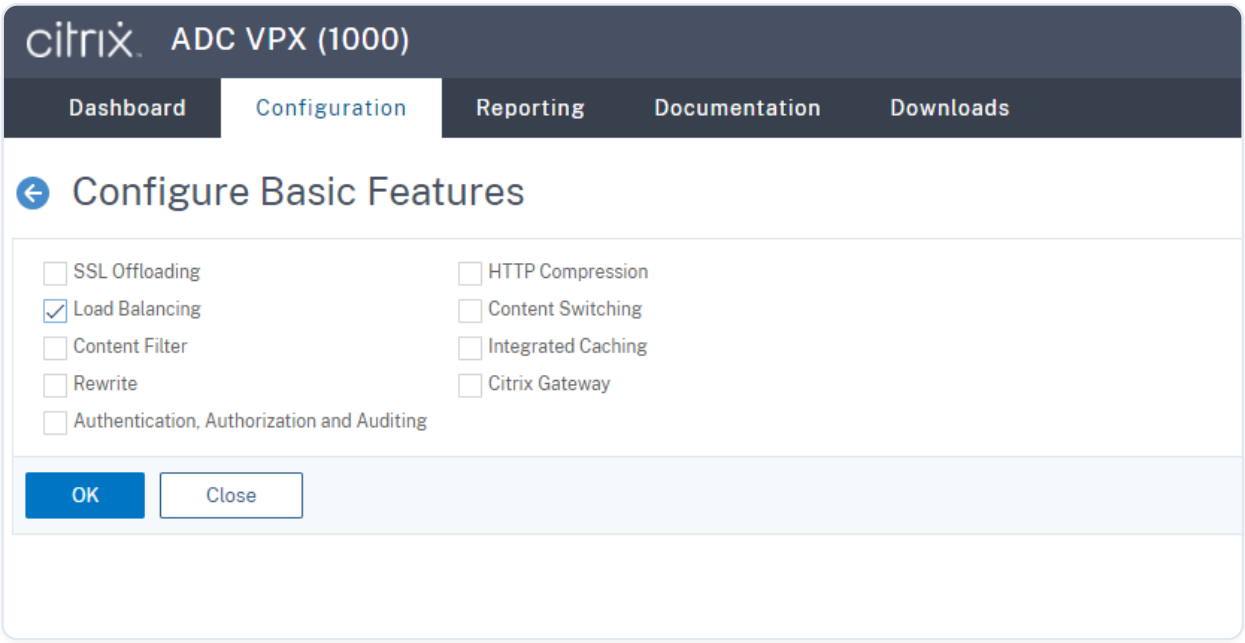


To configure load balancing through TCP passthrough, complete the following steps:

1. Log on to your Citrix ADC VPX instance.
2. Navigate to **Configuration > System > Settings > Configure Basic Features**.

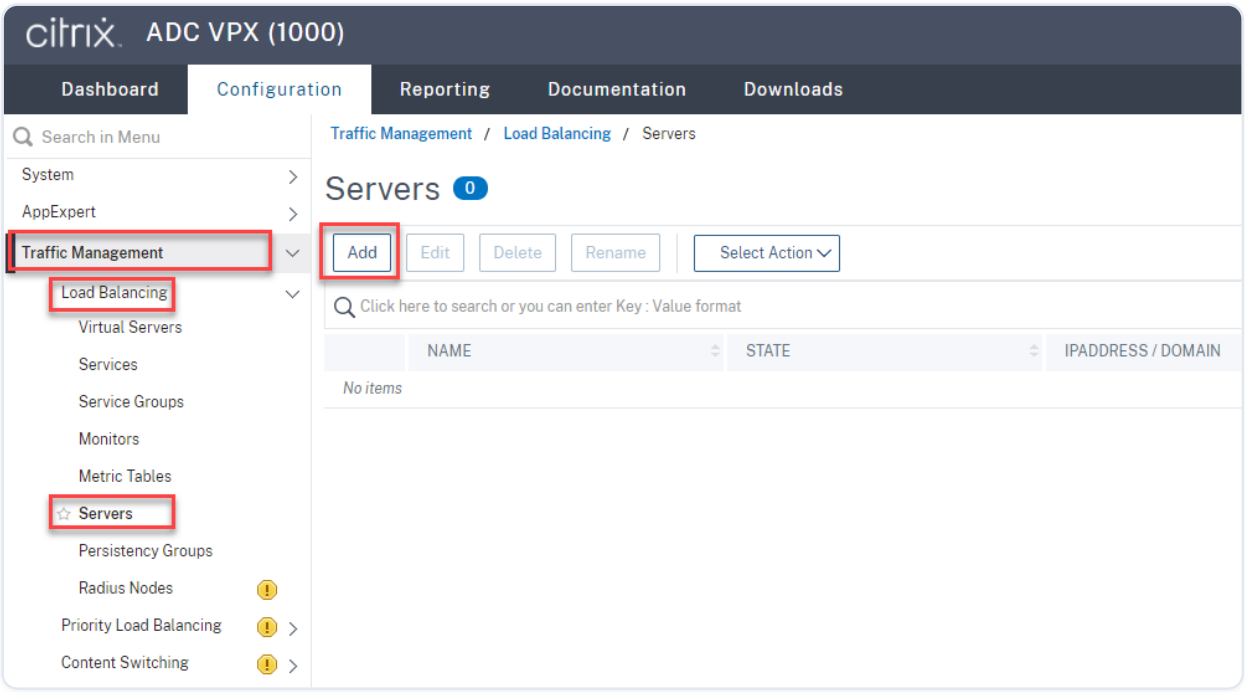


3. Select **Load Balancing** and click **OK**.

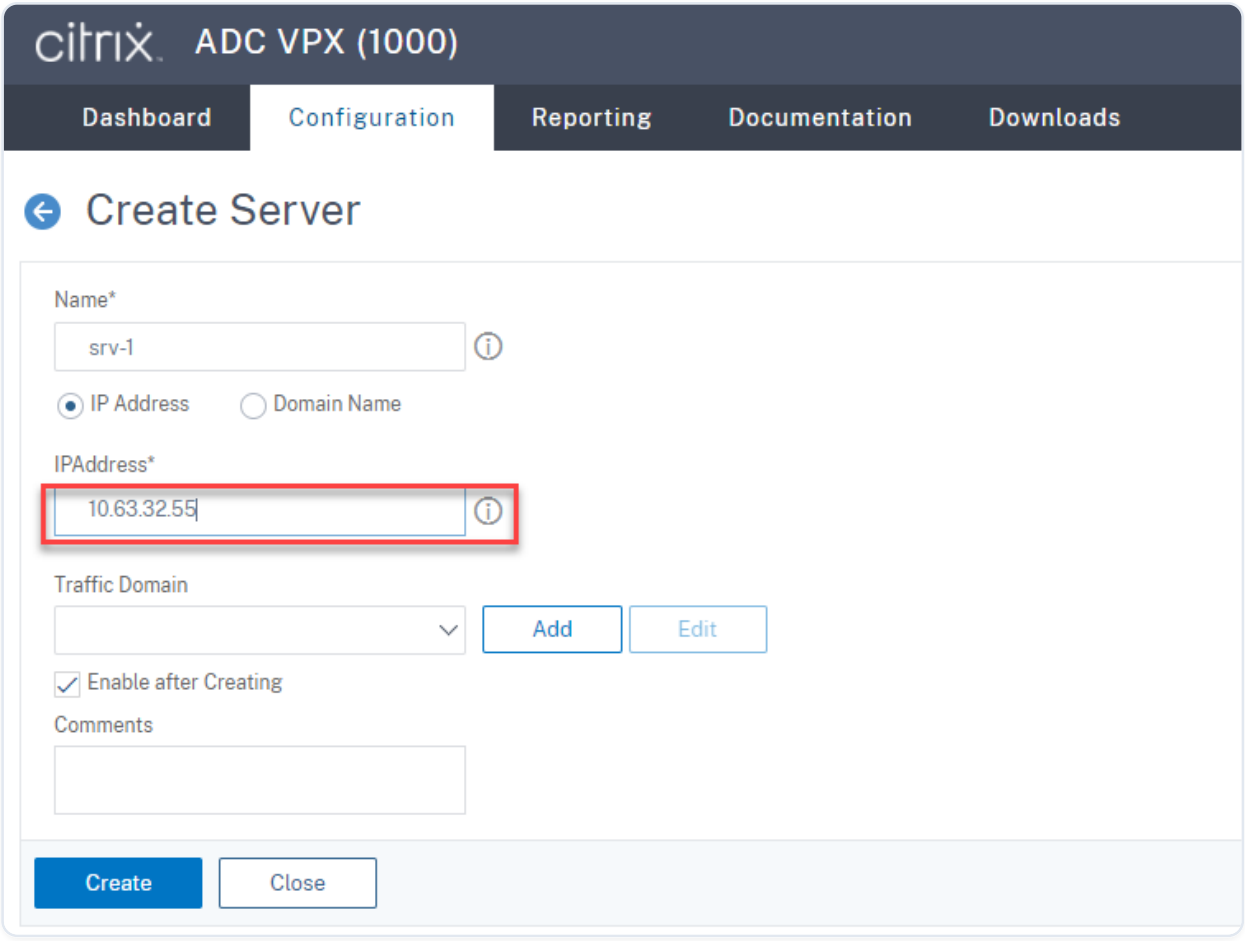


4. Add load balancing servers.

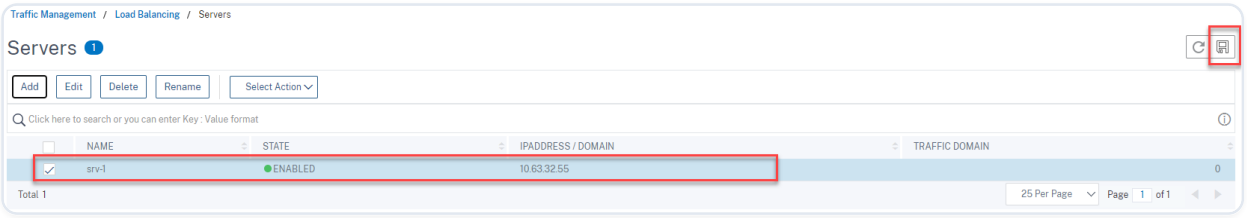
   Navigate to **Traffic Management > Load Balancing > Servers** and click **Add**.



Type the name and IP address of a Session Recording server and then click **Create**. For example:

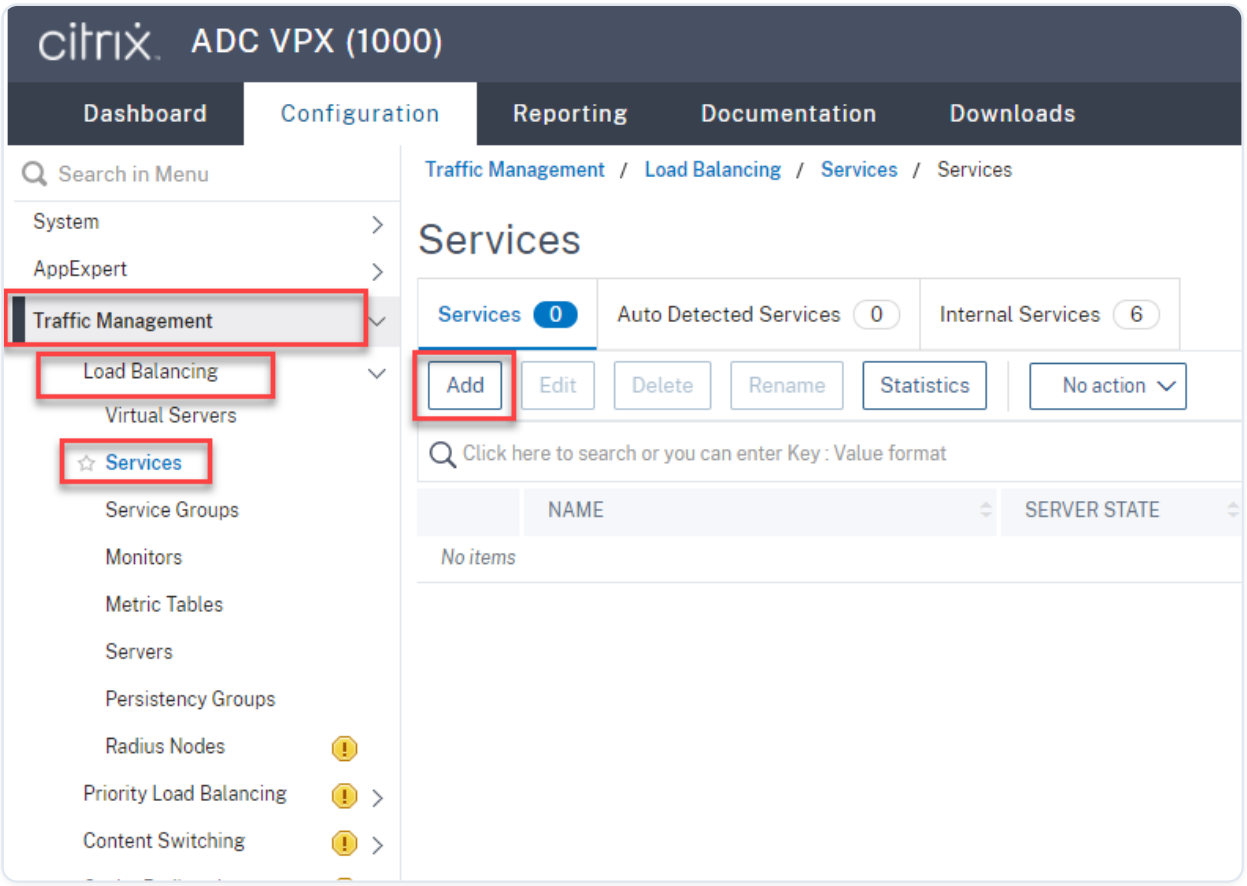


Click the save icon in the upper right corner to save your changes.

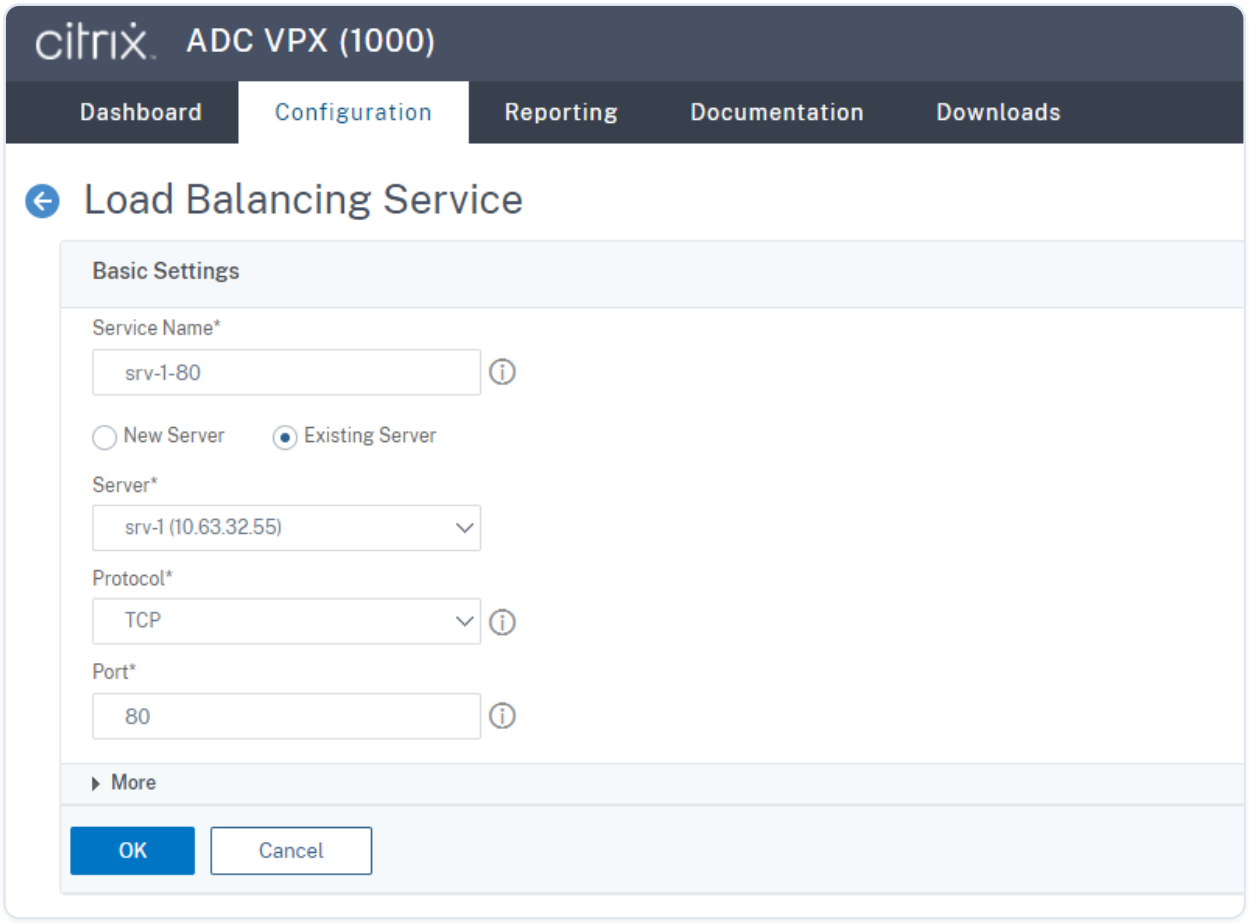


5. For WebSocket server Version 1.0, add **load balancing services** of ports 80, 1801, 22334, and 443 for each Session Recording server. For WebSocket server Version 2.0, add **load balancing services** of ports 80, 1801, and 443 for each Session Recording server.

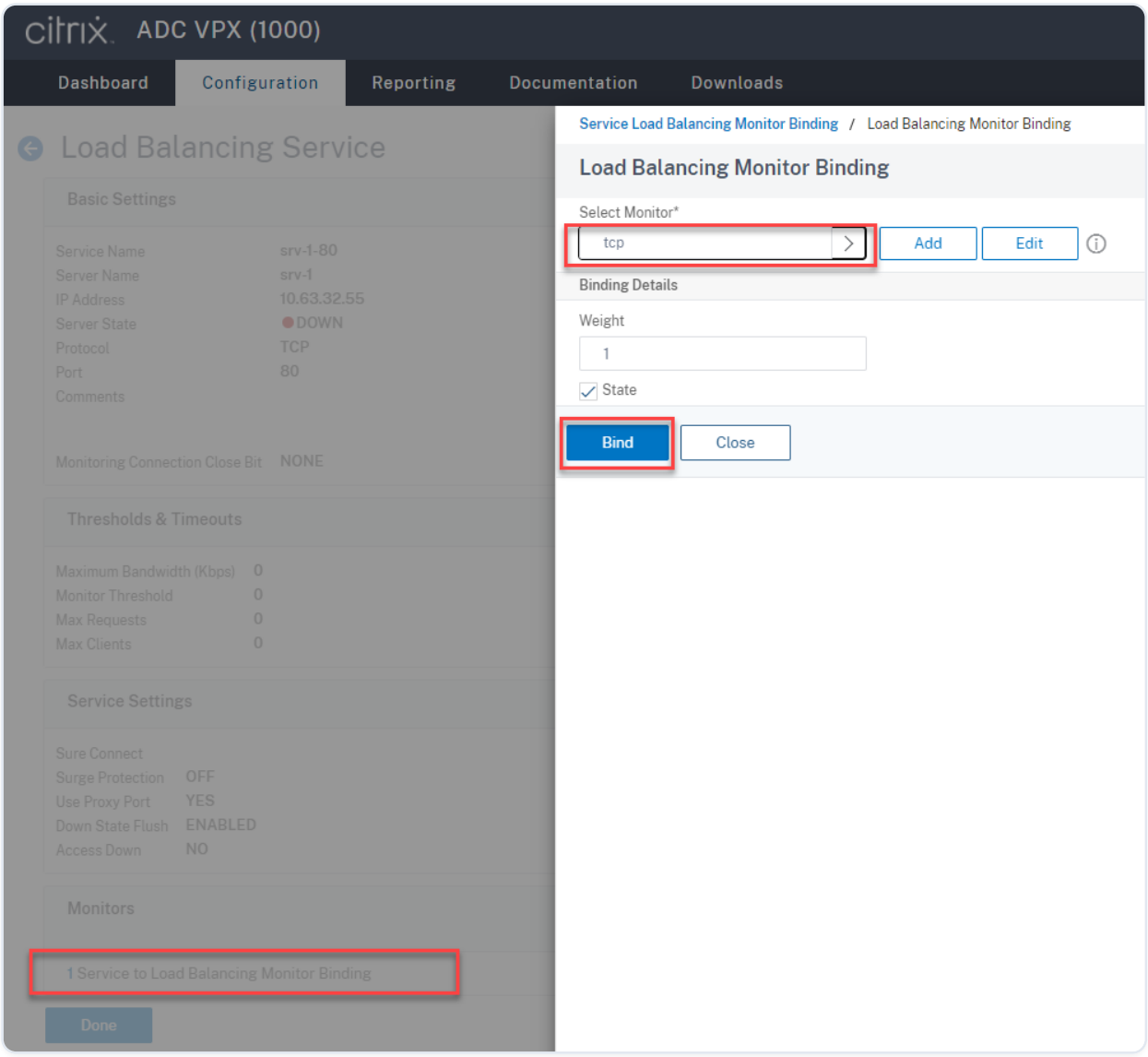
   Navigate to **Traffic Management > Load Balancing > Services** and click **Add**.



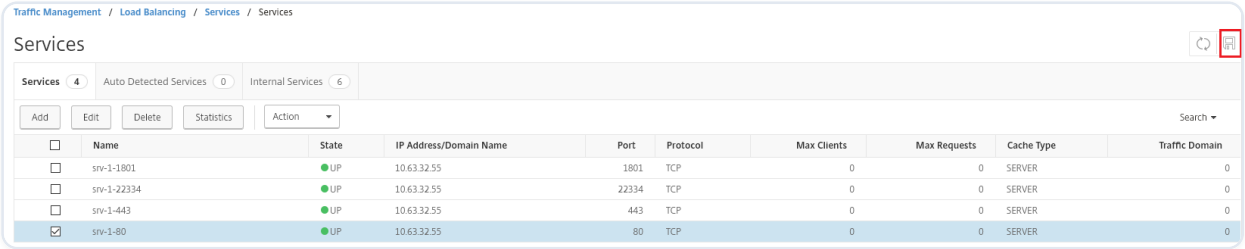
   Type a name for each **load balancing service** that you add. Choose **Existing Server**, select the IP address of your target Session Recording server, select **TCP** as the server protocol, and type a port number. Click **OK**.



Bind the TCP protocol monitor to each load balancing service.



Click the save icon in the upper right corner to save your changes.

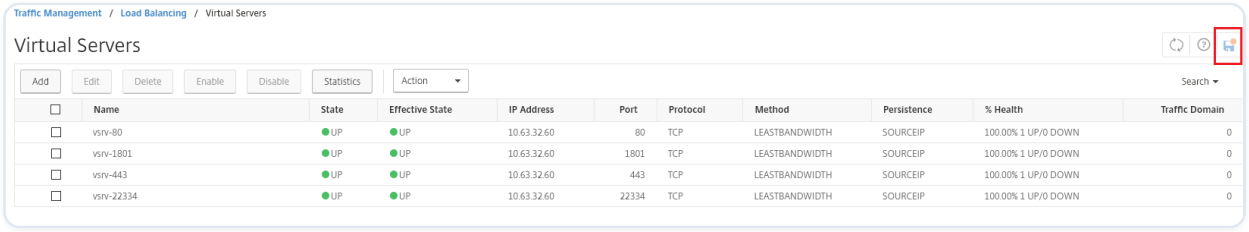


Tip:

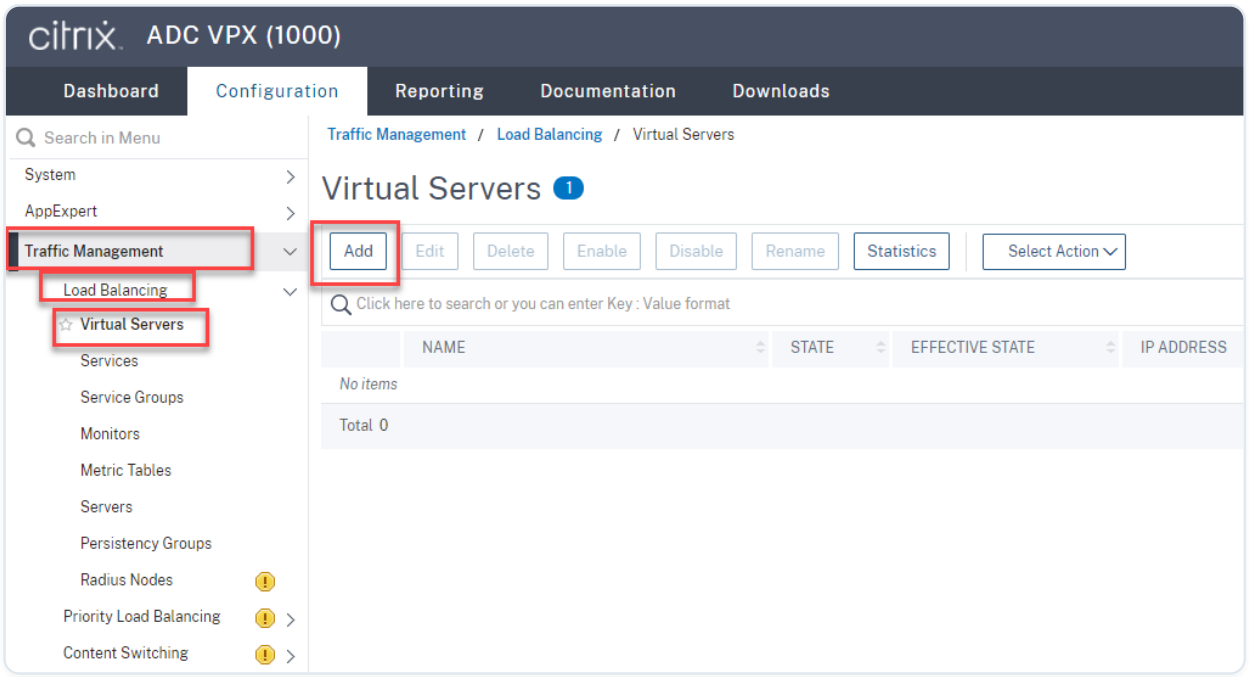
The **load balancing service** of port 22334 is required only for WebSocket server Version 1.0.

6. Add **load balancing virtual servers**.

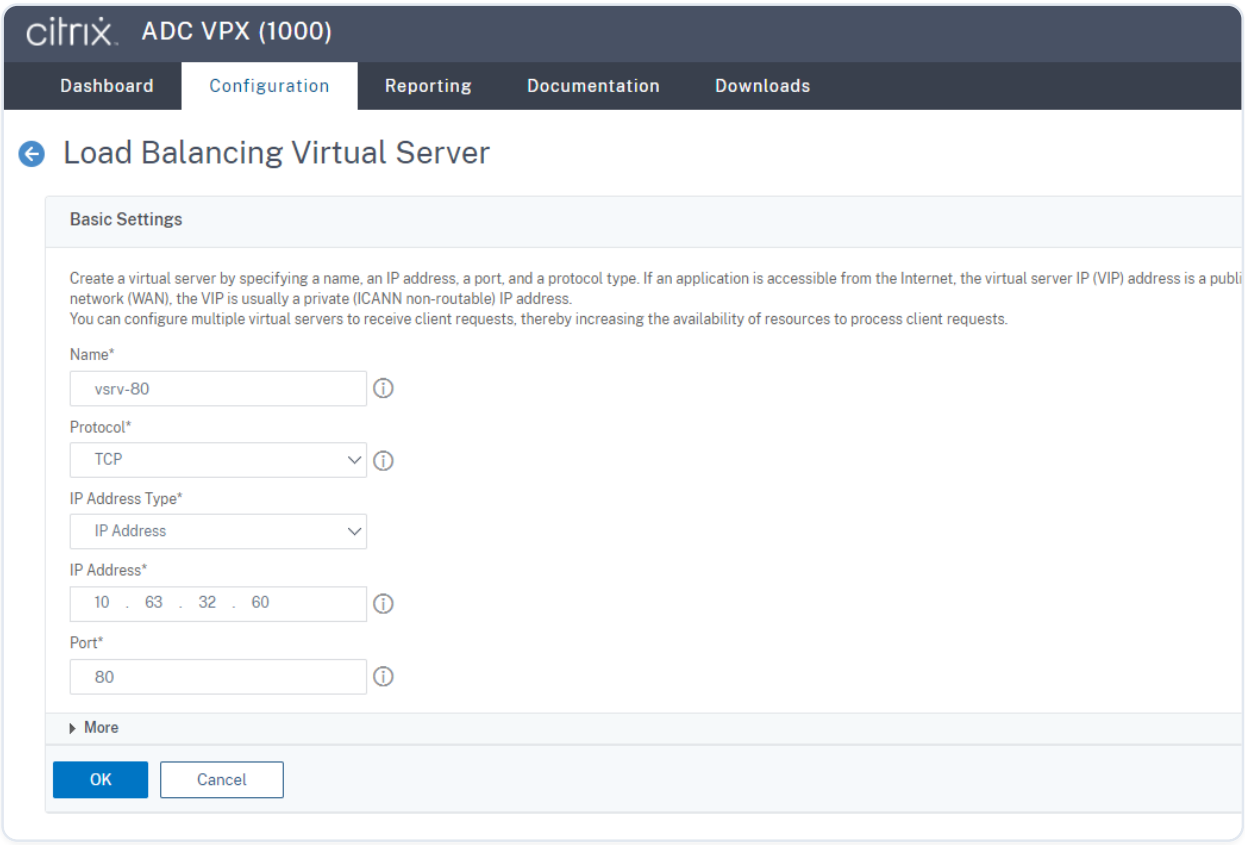
For WebSocket server Version 1.0, complete the following steps to add **load balancing virtual servers** of ports 80, 443, 1801, and 22334. For WebSocket server Version 2.0, add **load balancing virtual servers** of ports 80, 443, and 1801. For example:



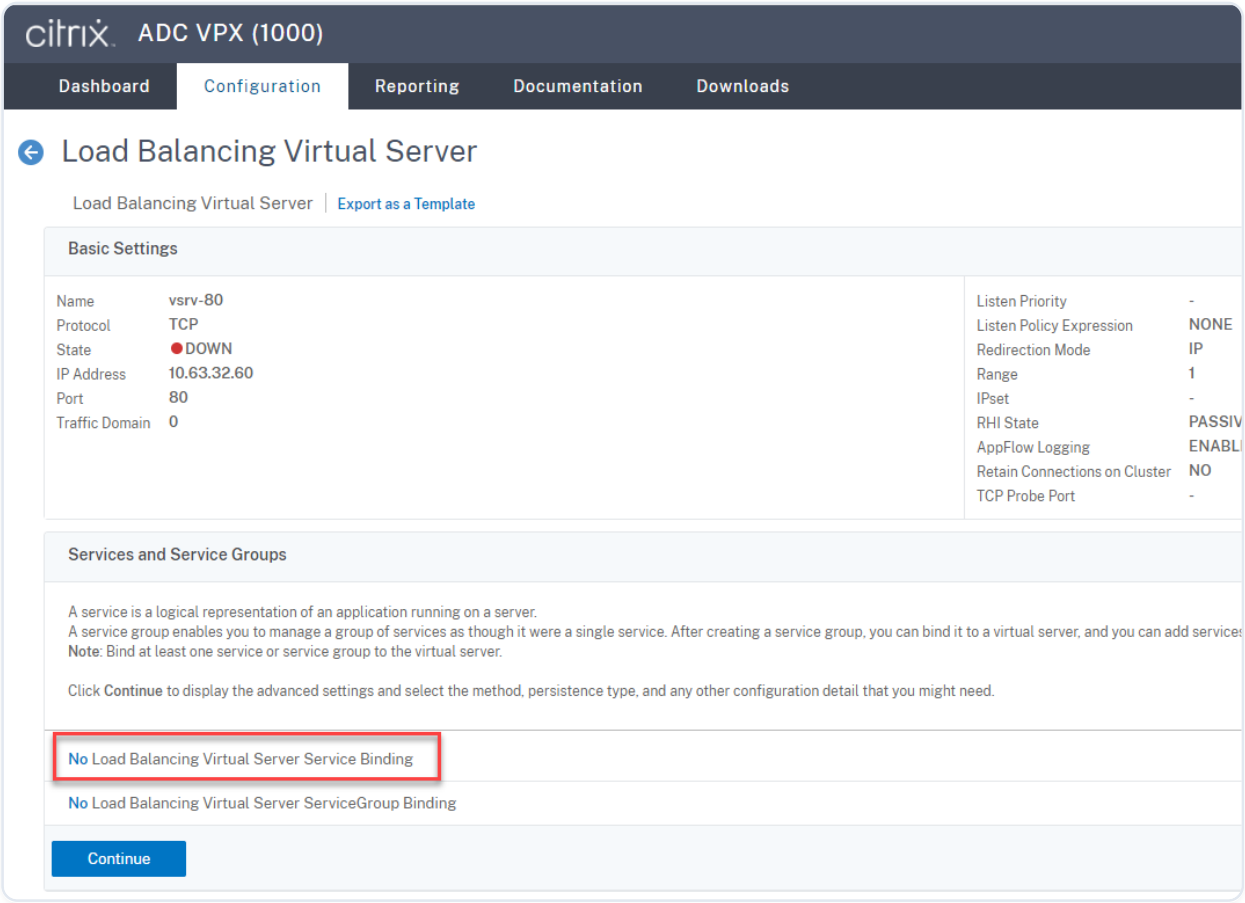
Navigate to **Traffic Management > Load Balancing > Virtual Servers** and click **Add**.

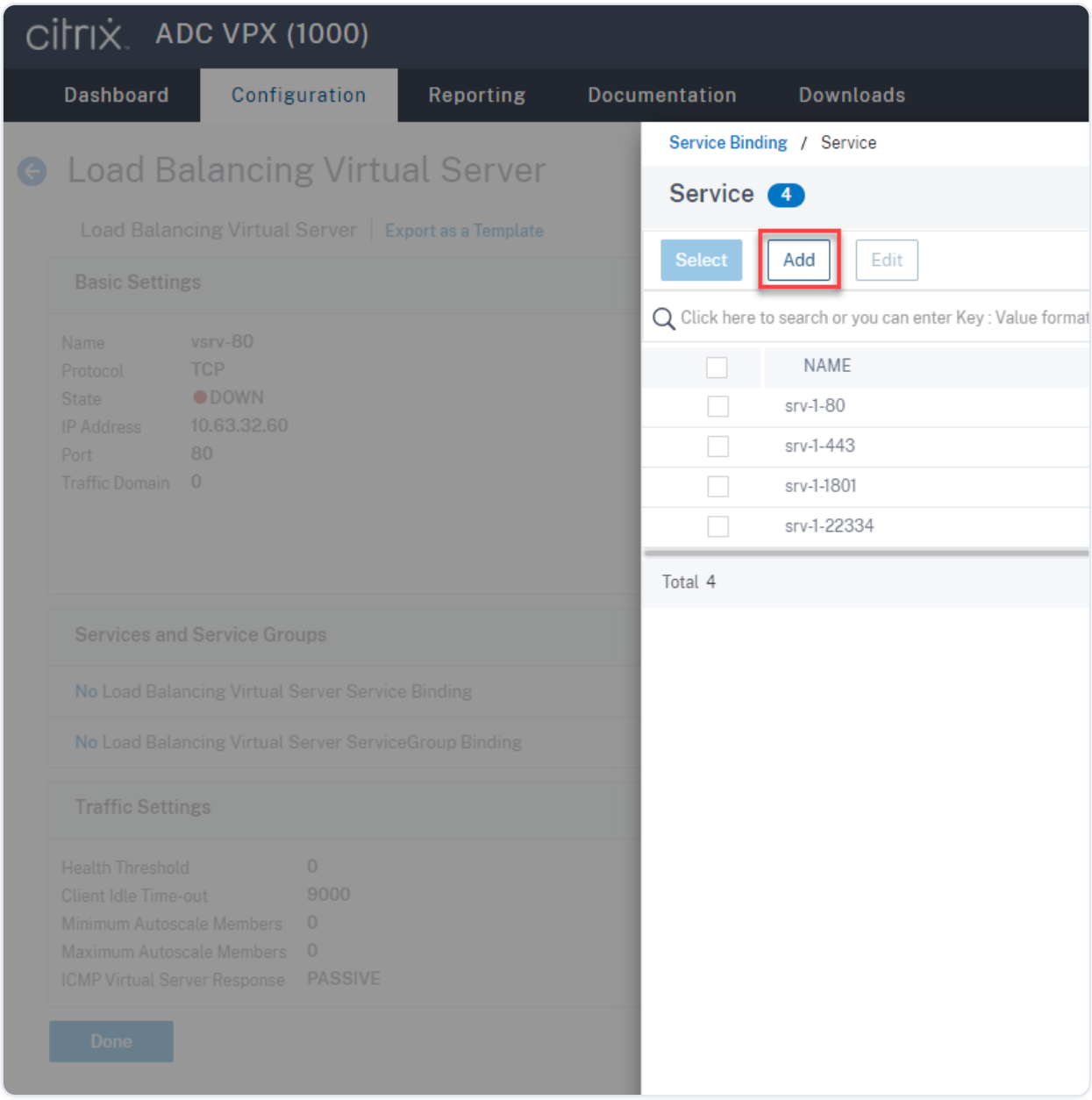


Add each virtual server with the Citrix ADC VIP address based on the TCP protocol.

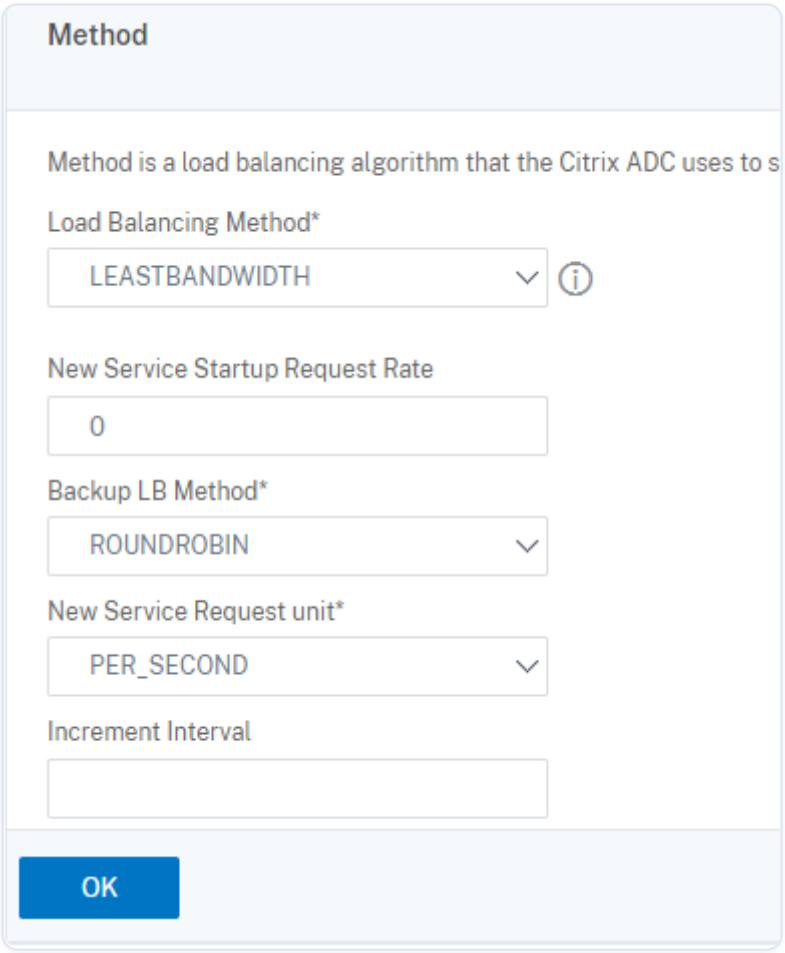


Bind each virtual server to the **load balancing service** of the same port. For example:

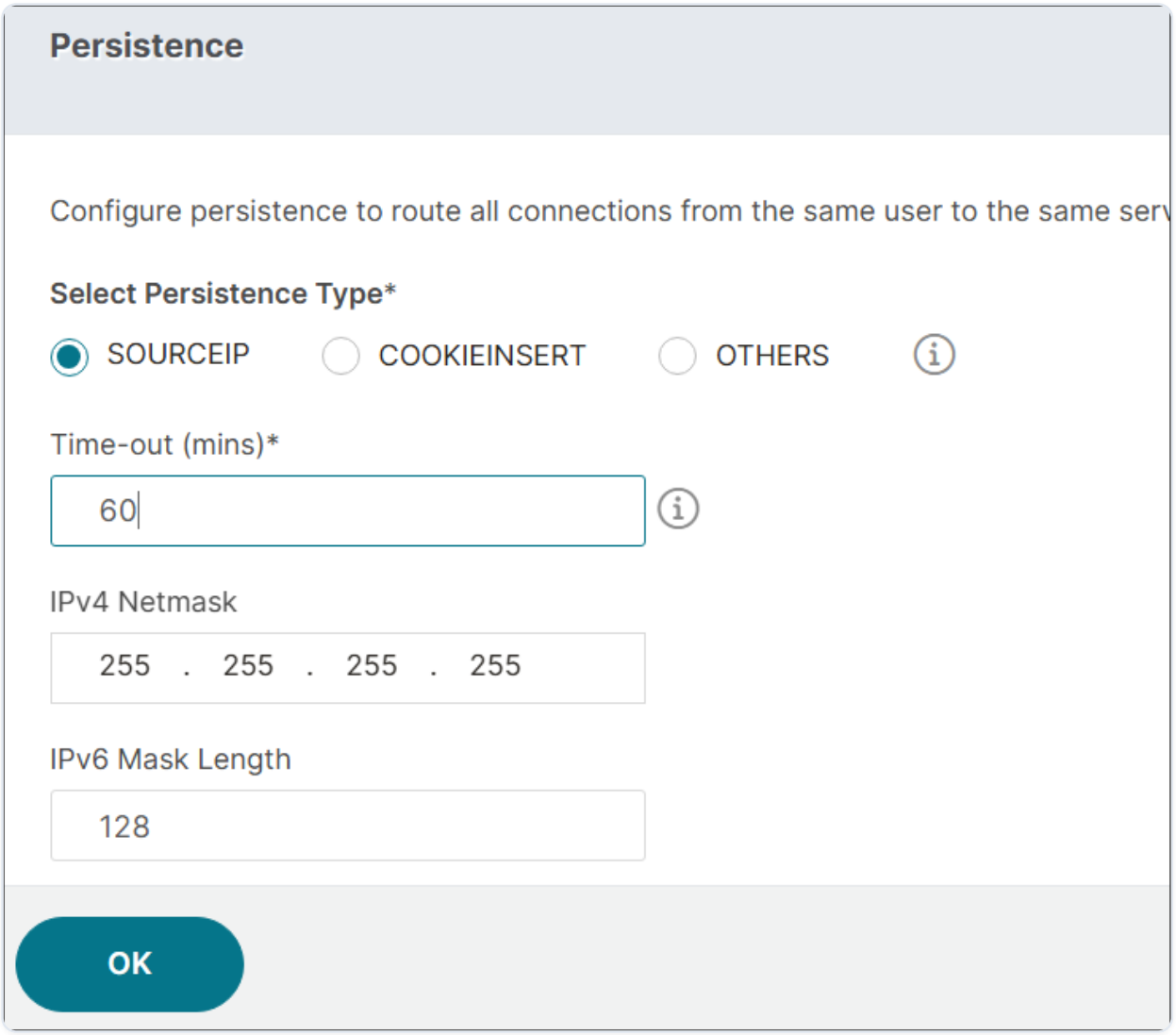




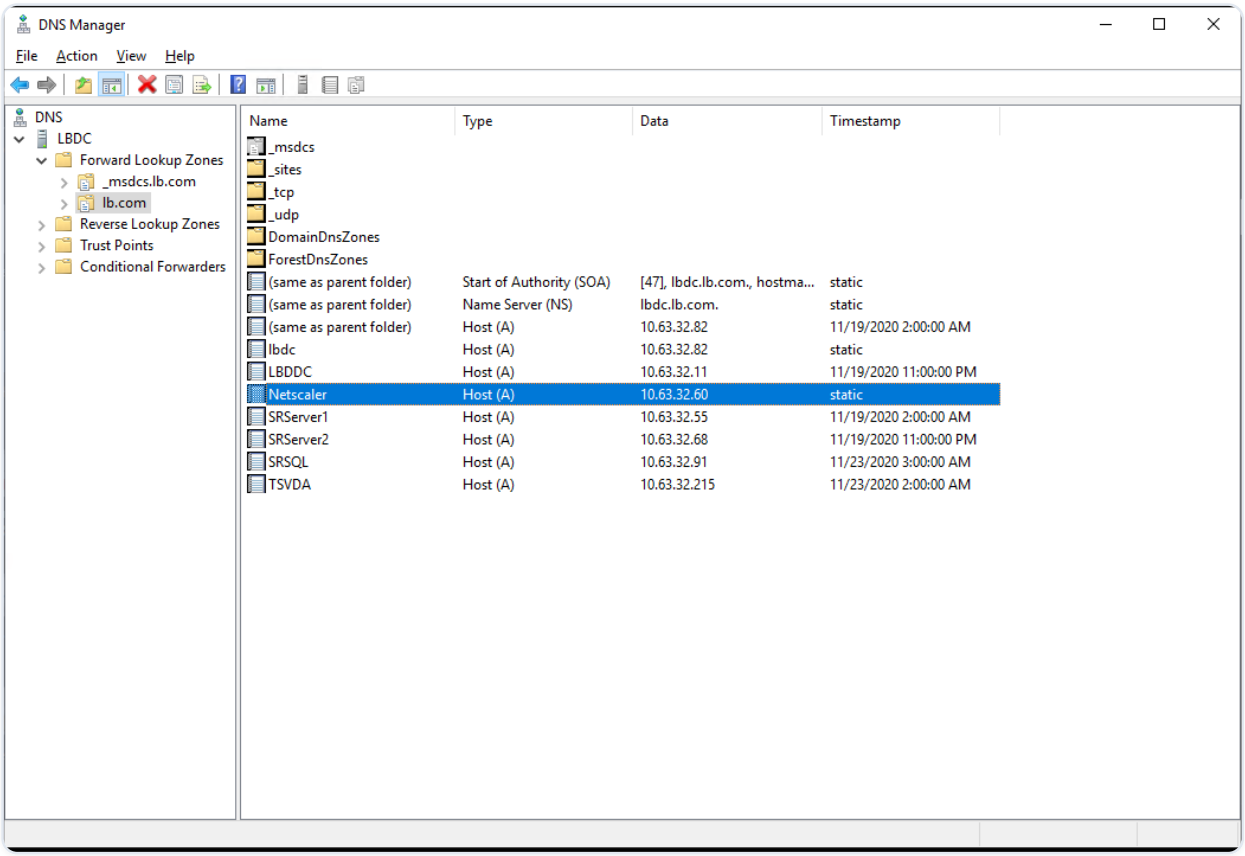
Choose a load balancing method.



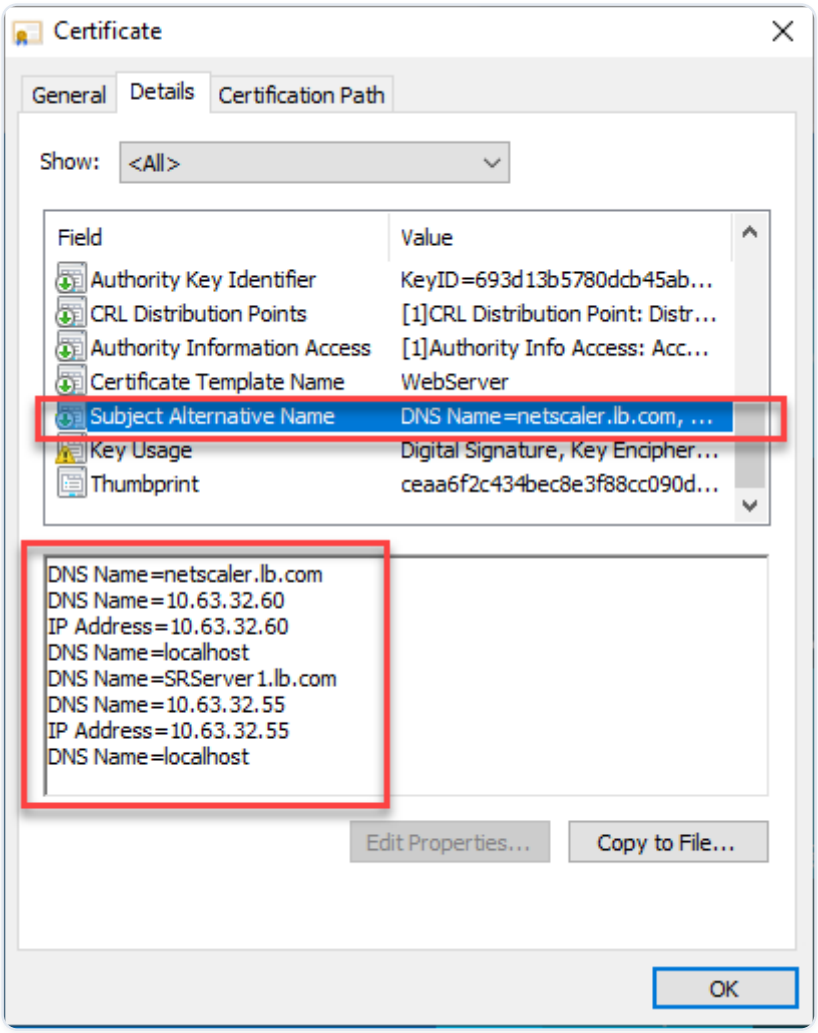
Configure persistence on each virtual server. We recommend you select **SOURCEIP** as the persistence type. For more information, see Persistence settings.



7. Create a host record for the Citrix ADC VIP address on the domain controller.



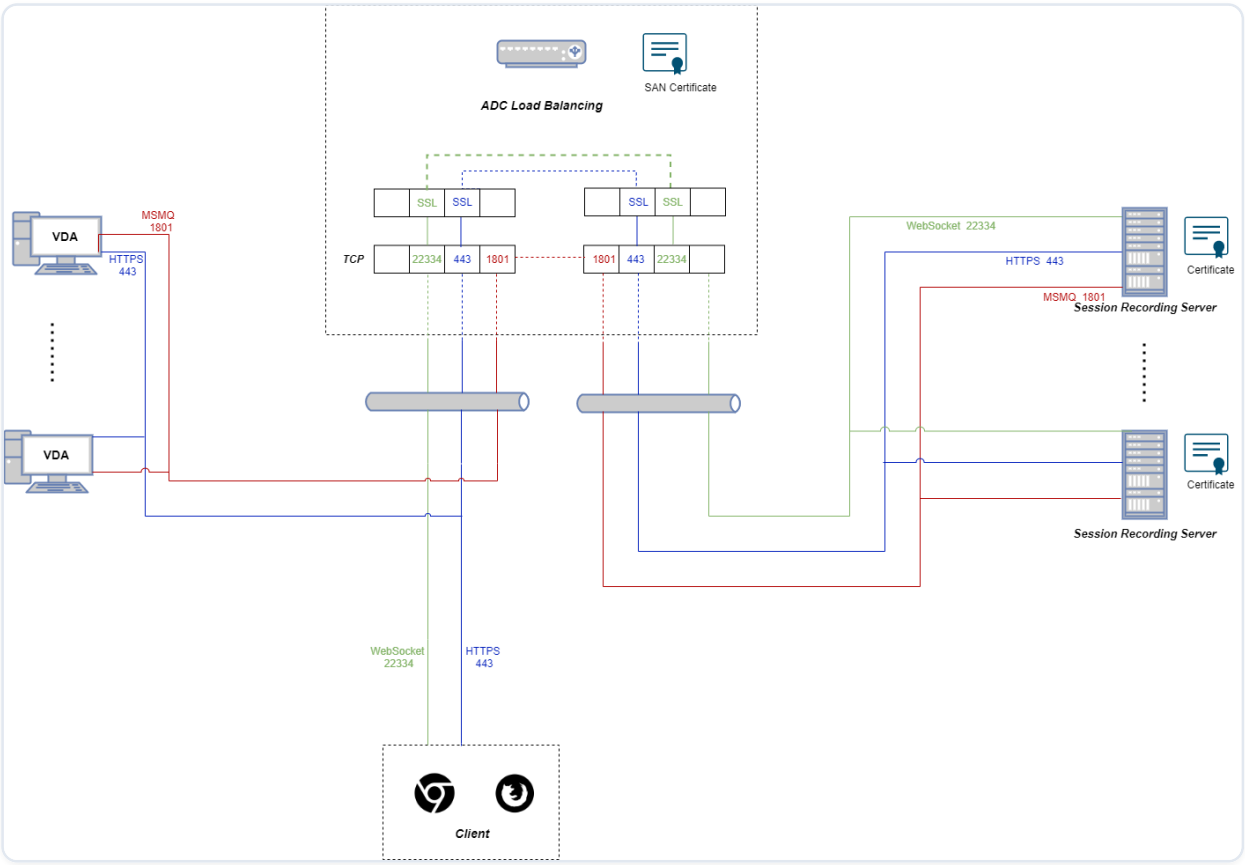
8. To access the web player over HTTPS, ensure that a SAN certificate is available both on Citrix ADC and on each Session Recording server. A SAN certificate contains the FQDNs of the Citrix ADC and of each Session Recording server.



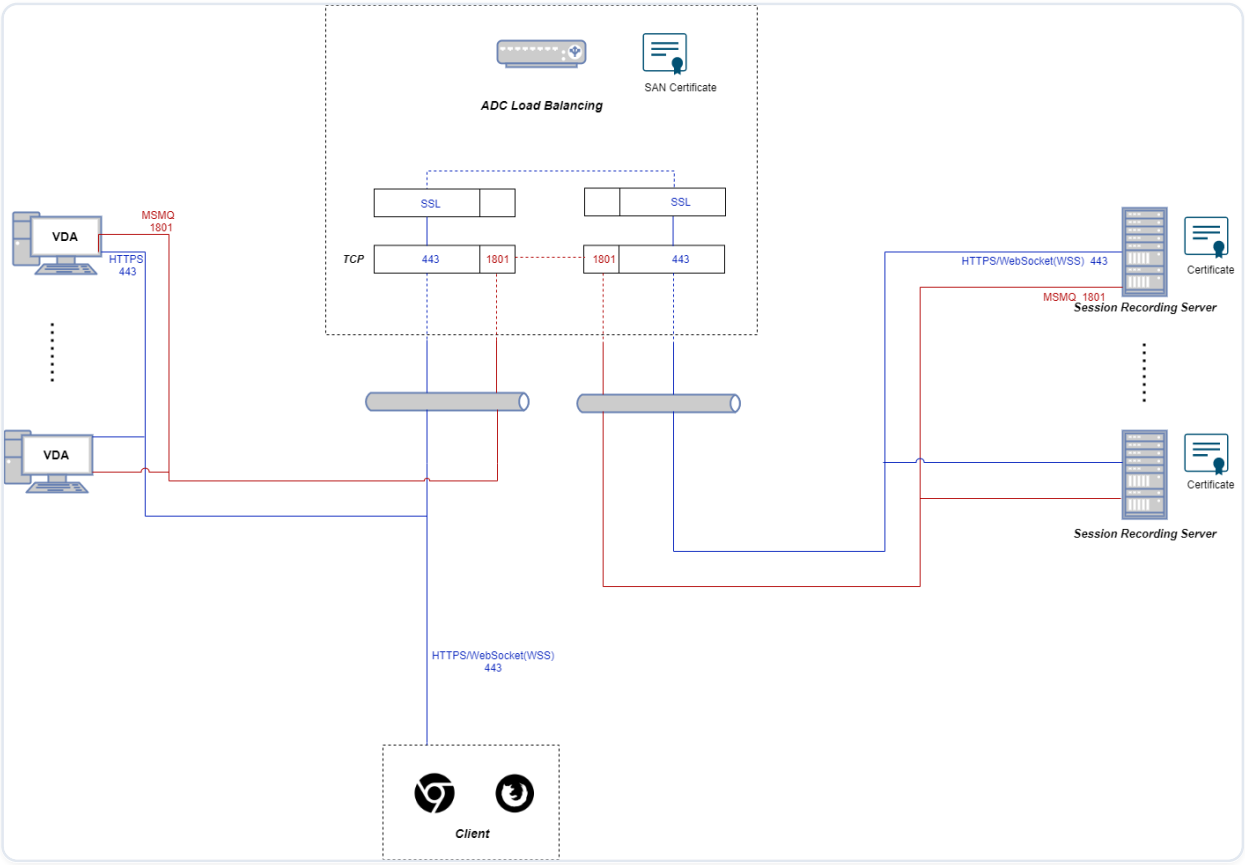
Configure load balancing through SSL offloading

The following topologies show how to configure load balancing through SSL offloading.

- If you are using the Python-based WebSocket server (Version 1.0):

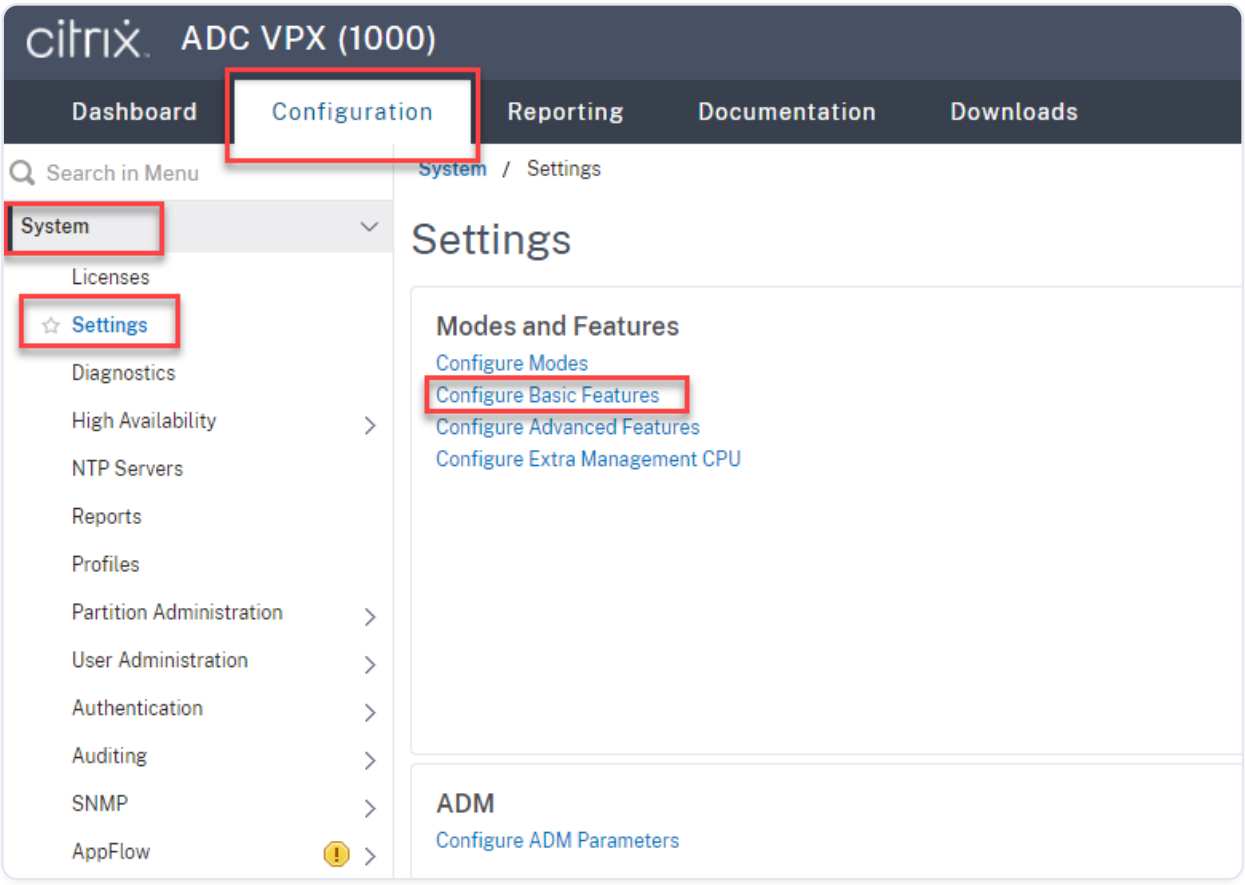


- If you are using the WebSocket server hosted in IIS (Version 2.0):

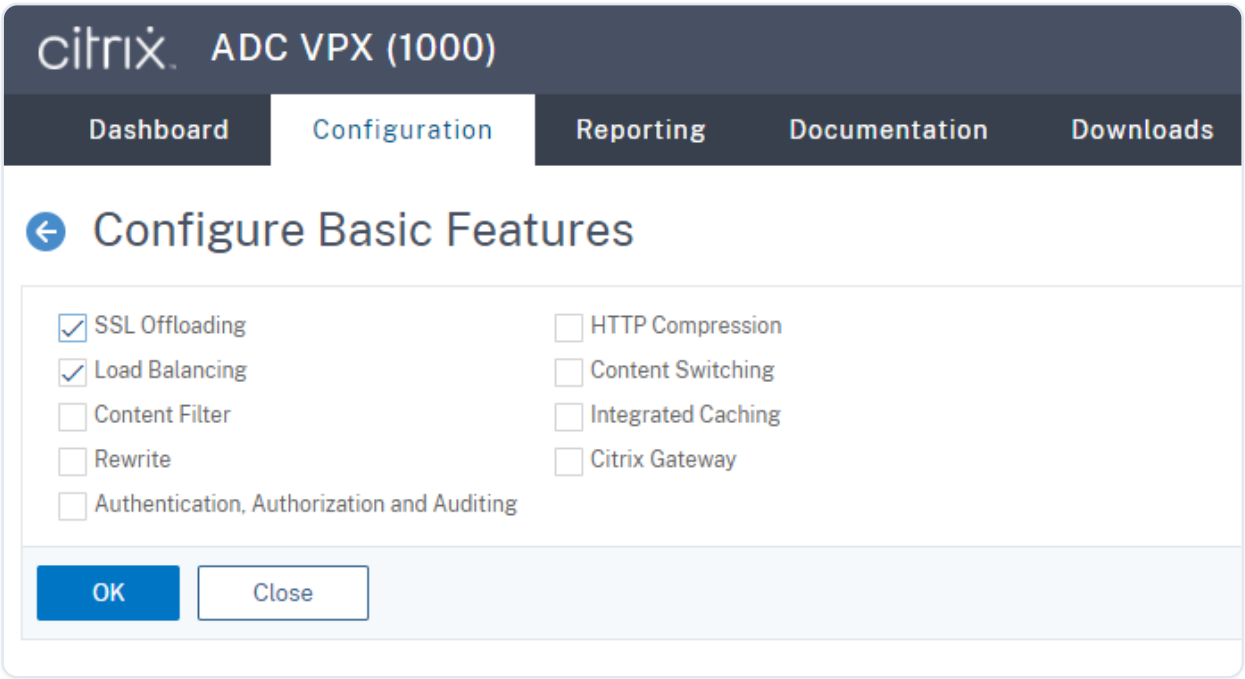


1. Log on to your Citrix ADC VPX instance.

2. Navigate to **Configuration > System > Settings > Configure Basic Features**.

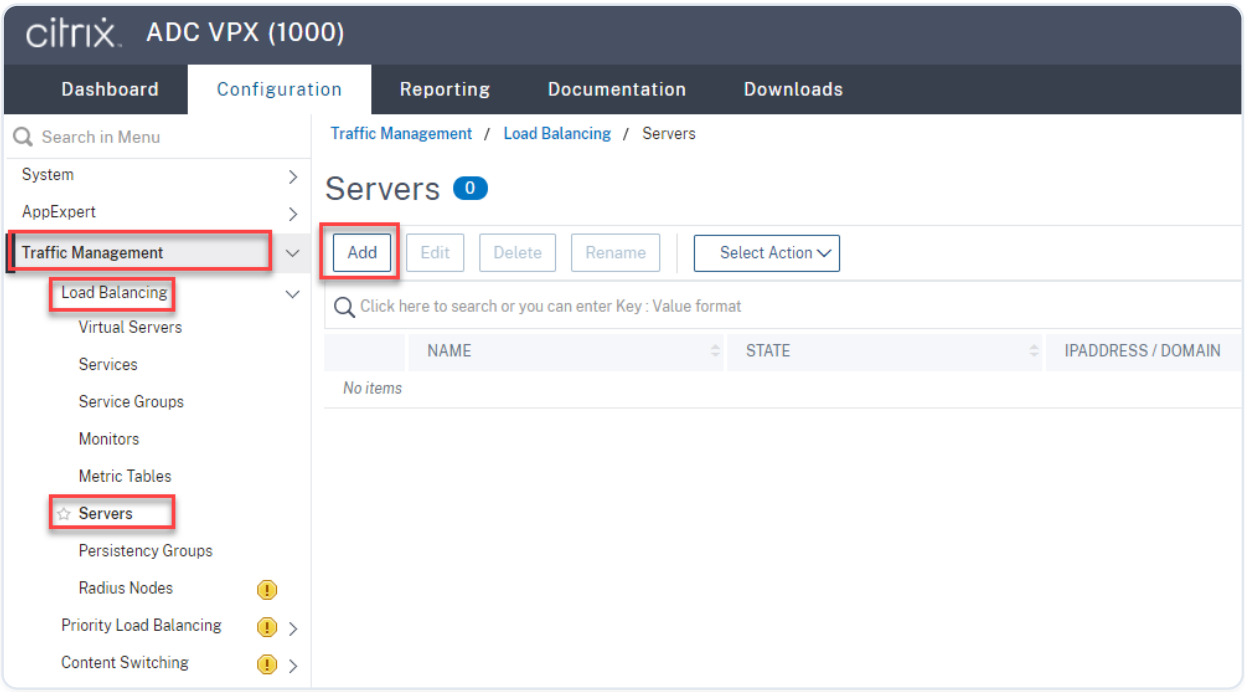


3. Select **SSL Offloading** and **Load Balancing** and click **OK**.

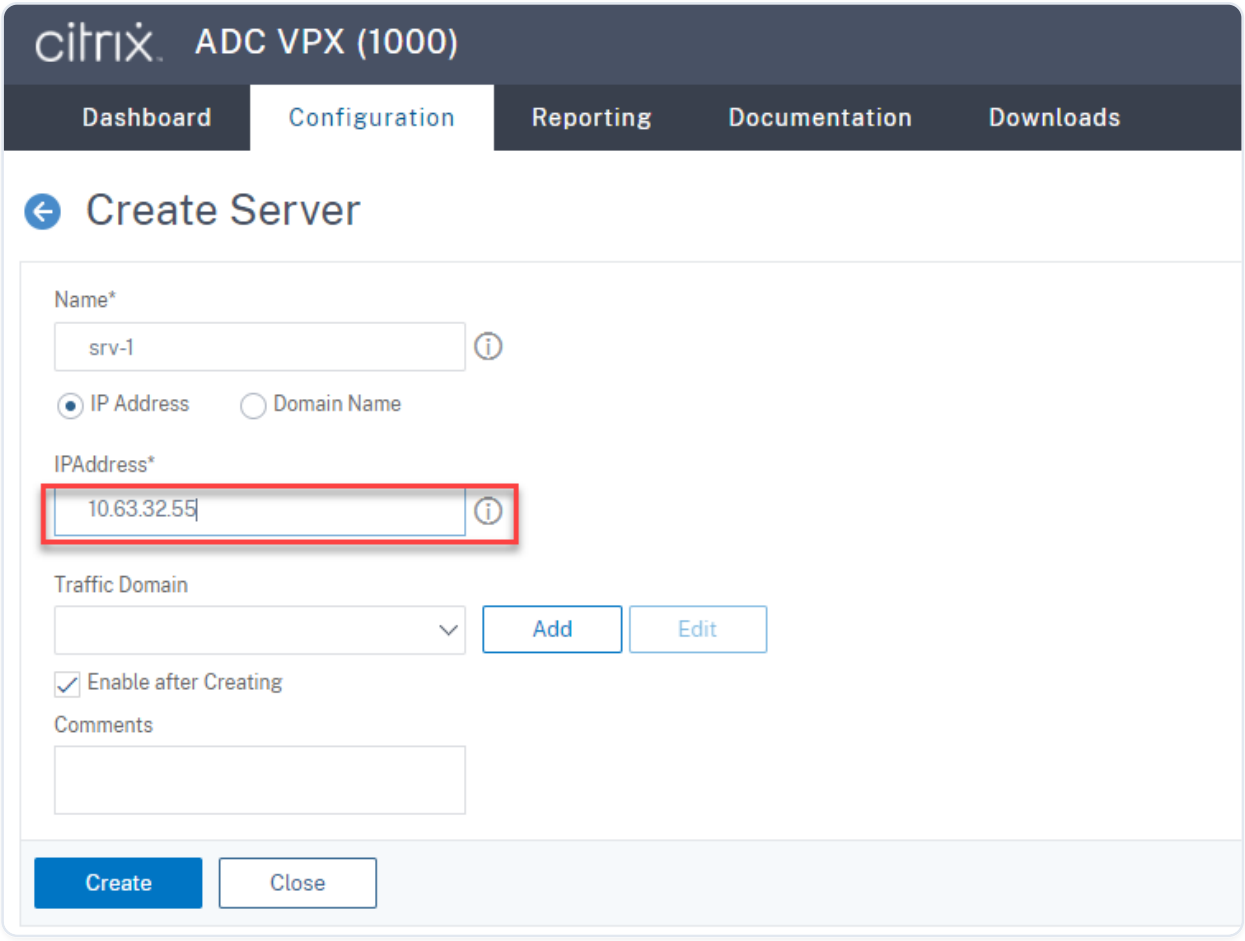


4. Add load balancing servers.

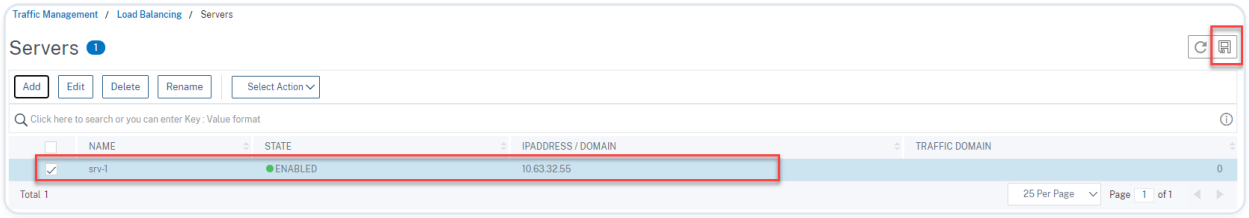
   Navigate to **Traffic Management > Load Balancing > Servers** and click **Add**.



Type the name and IP address of a Session Recording server and then click **Create**. For example:



Click the save icon in the upper right corner to save your changes.

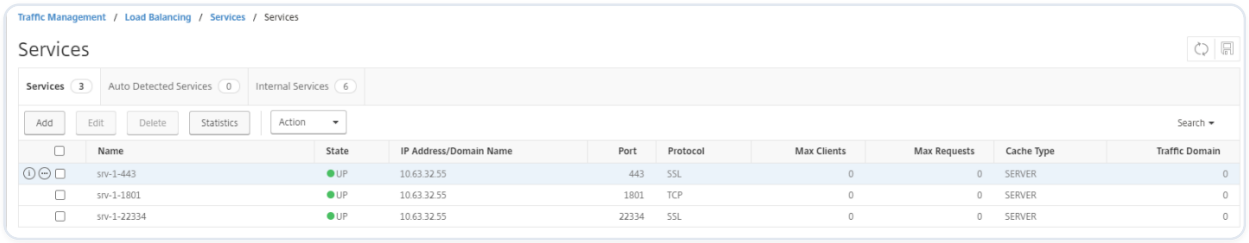


5. Add **load balancing services** for each Session Recording server that you added in the previous step.

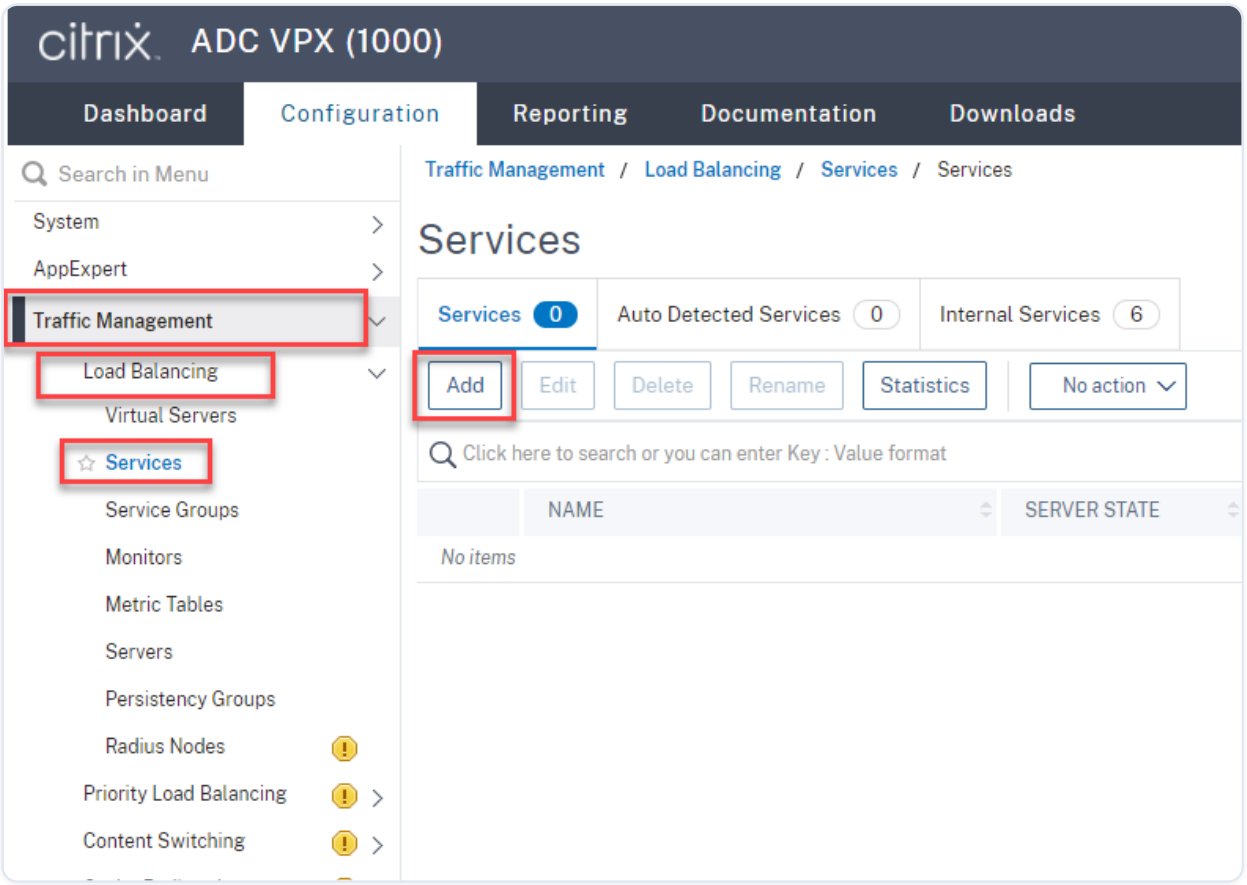
   Add the following **load balancing services** for each Session Recording server:

   - (Required only when you are using the WebSocket server Version 1.0) **SSL load balancing service** of port 22334 that binds to the TCP monitor
   - **SSL load balancing service** of port 443 that binds to the HTTPS monitor
   - **TCP load balancing service** of port 1801 that binds to the TCP monitor

   For example:

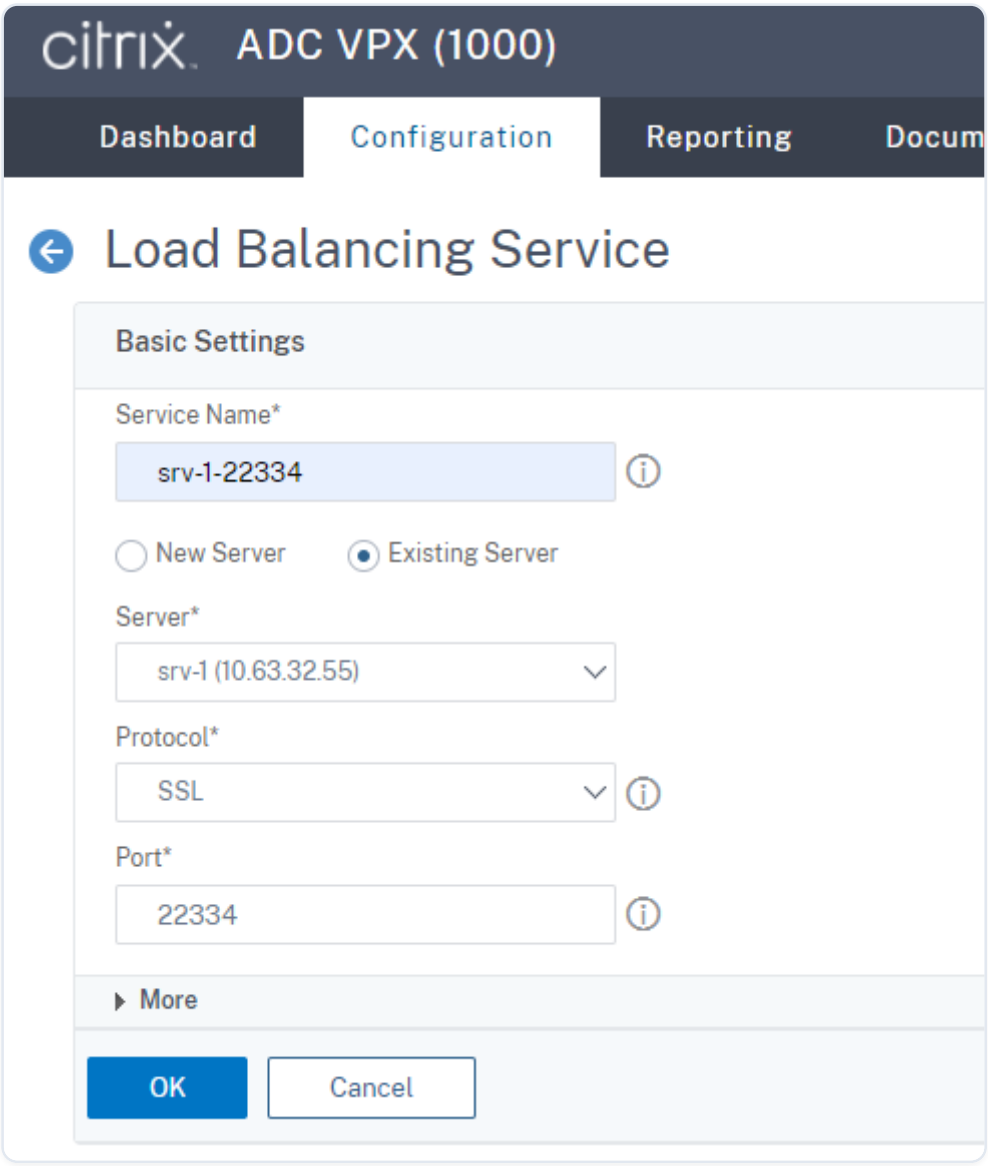


   Navigate to **Traffic Management > Load Balancing > Services** and click **Add**.

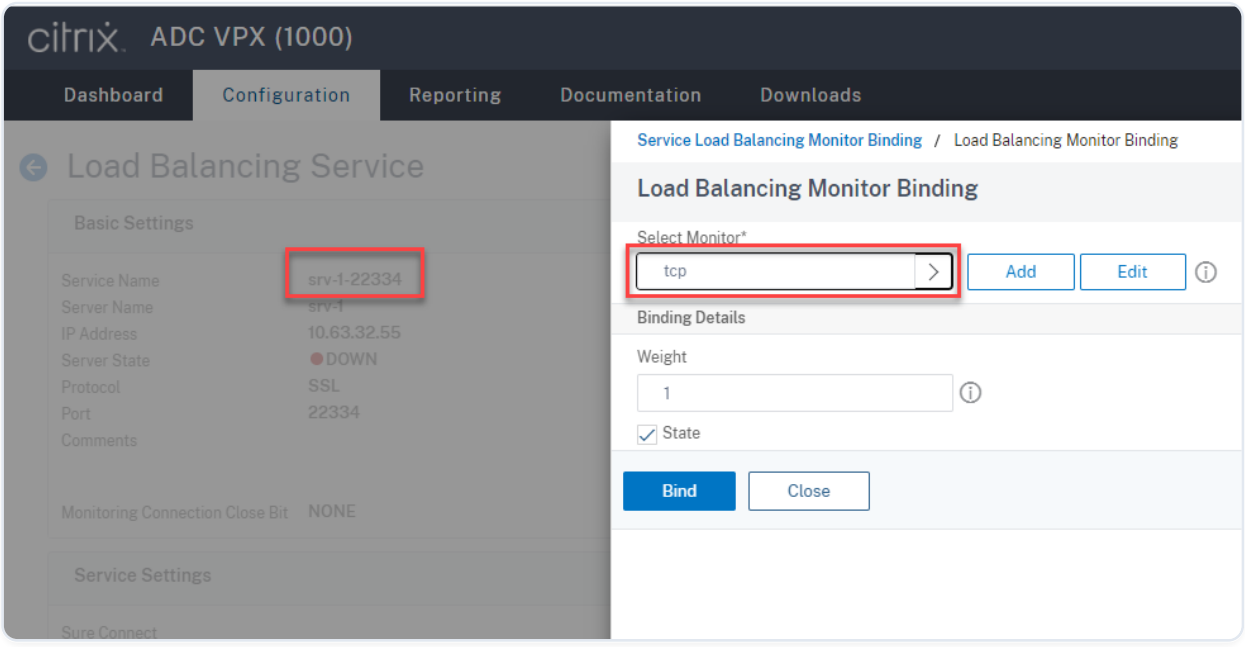


(Required only when you are using the WebSocket server Version 1.0) Add an SSL load balancing service of port 22334 for each Session Recording Server. Type a name for the load balancing service, choose **Existing Server**, select the IP address of a Session Recording server, select **SSL** as the server protocol, type port number **22334**, and click **OK**.

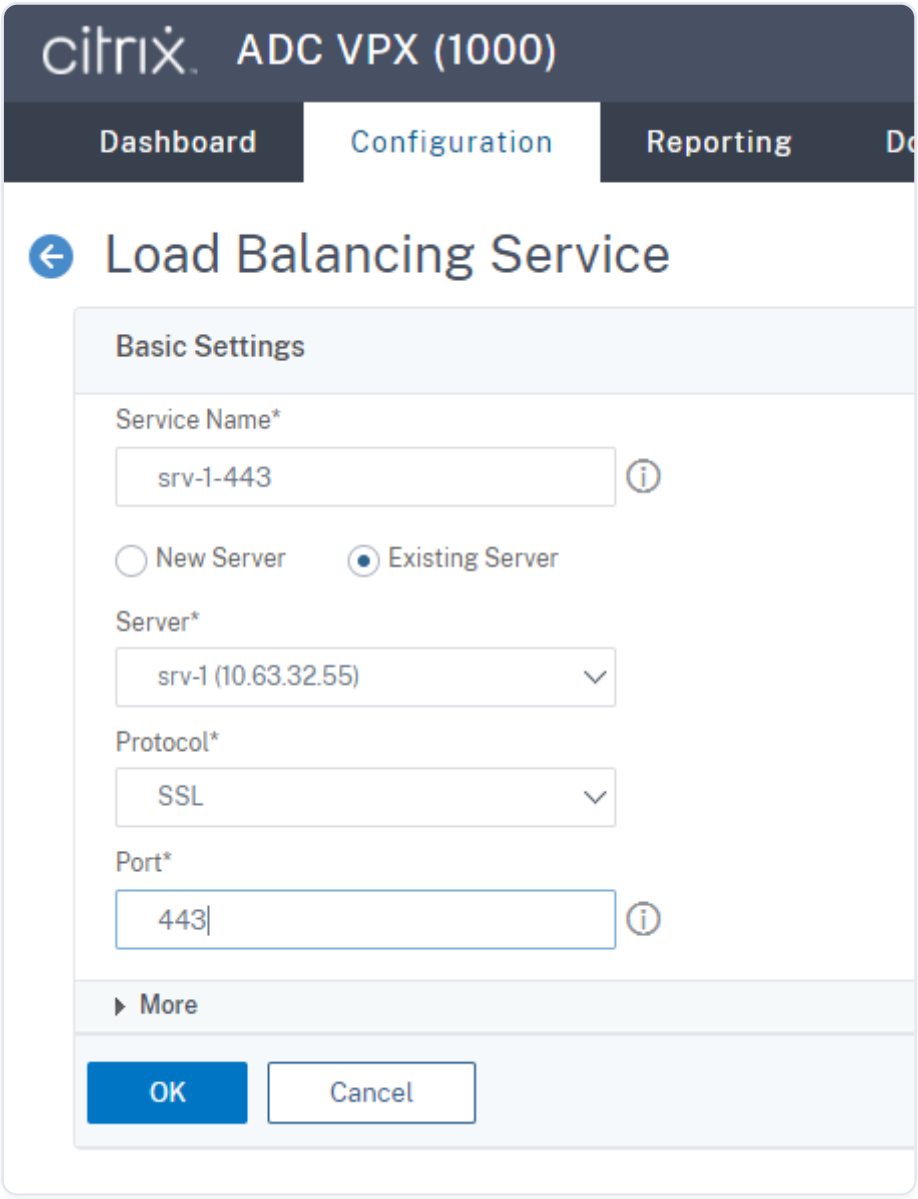
For example, see the following screen capture.



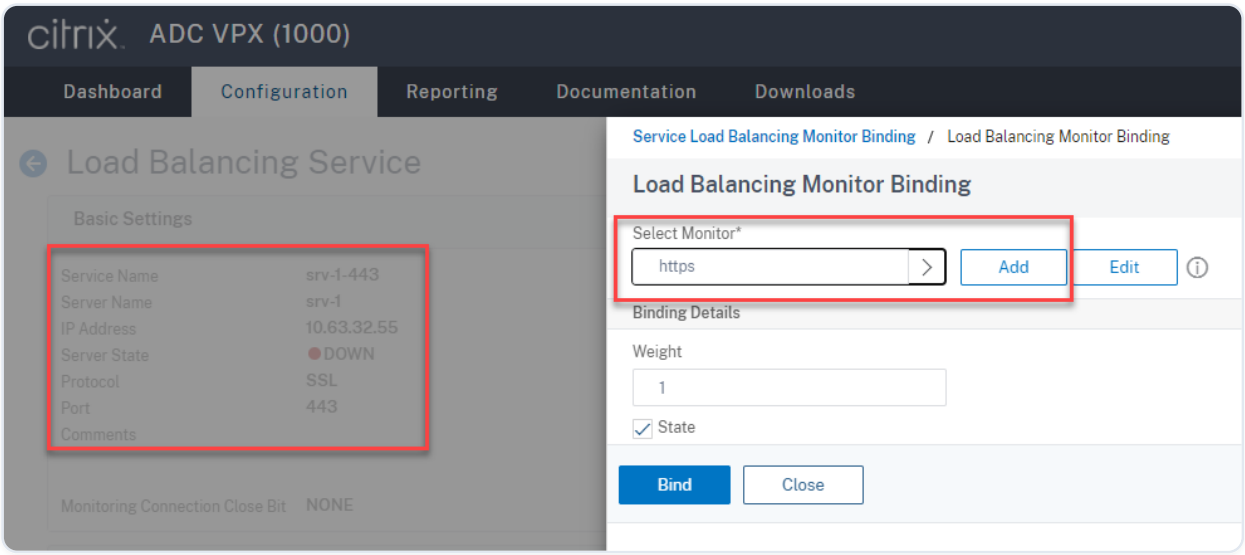
Bind the TCP monitor to the **SSL load balancing service** you just added.



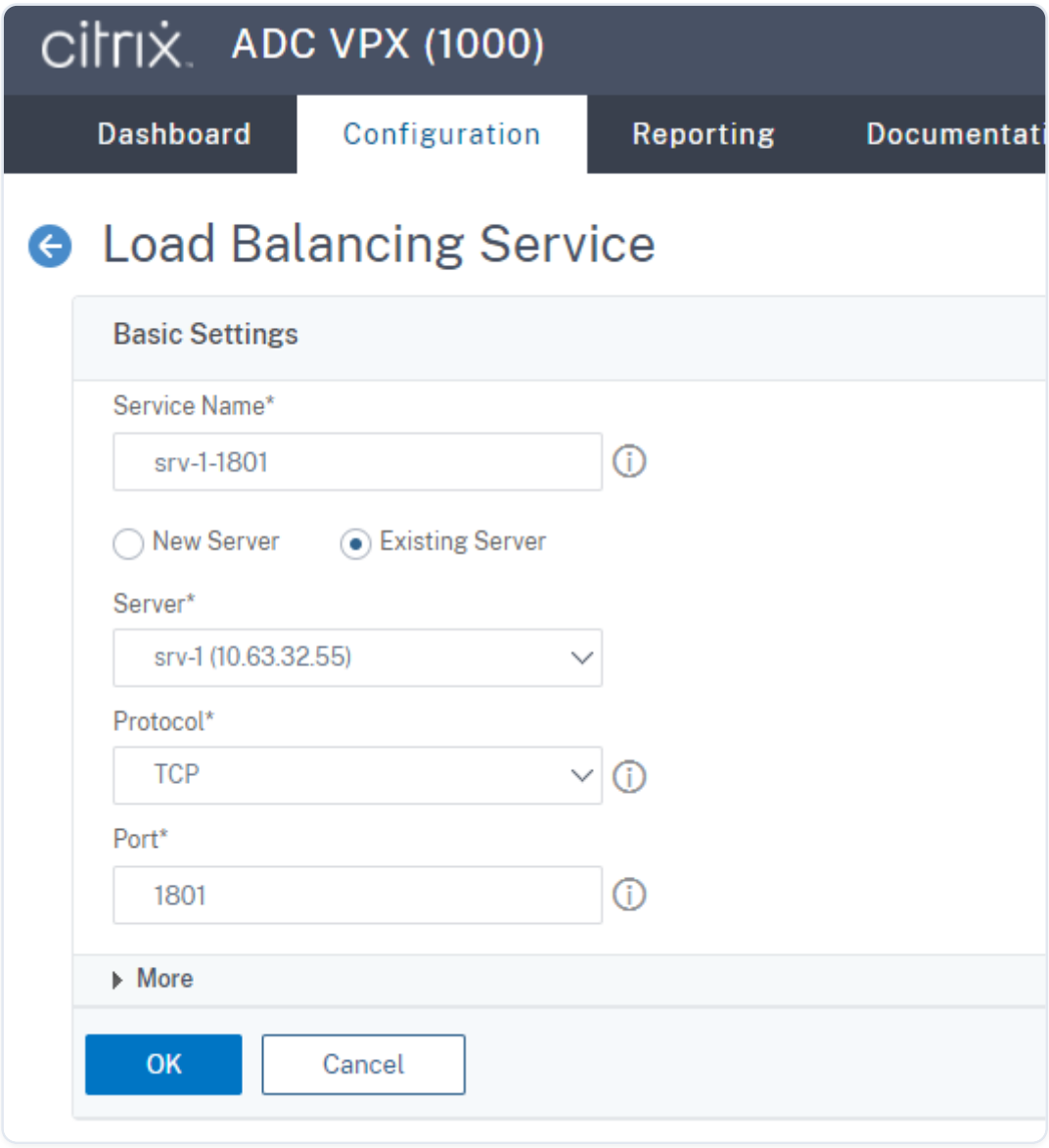
Add an SSL load balancing service of port 443 for each Session Recording Server. Type a name for the load balancing service, choose **Existing Server**, select the IP address of a Session Recording server, select **SSL** as the server protocol, type port number 443, and click **OK**.



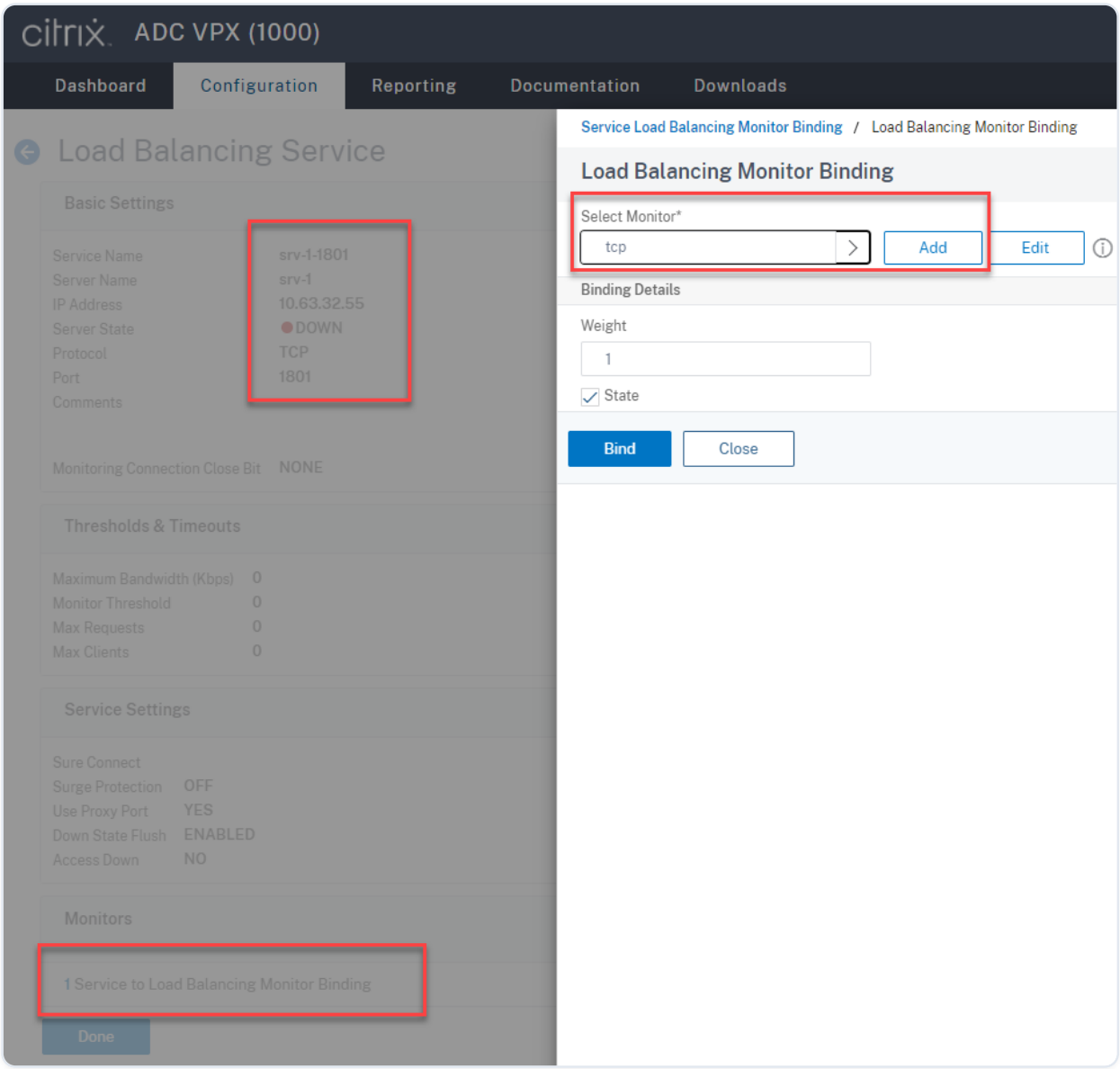
Bind the HTTPS monitor to the **SSL load balancing service** you just added.



Add a TCP load balancing service of port 1801 for each Session Recording Server. Type a name for the load balancing service, choose **Existing Server**, select the IP address of a Session Recording server, select **TCP** as the server protocol, type port number 1801, and click **OK**.

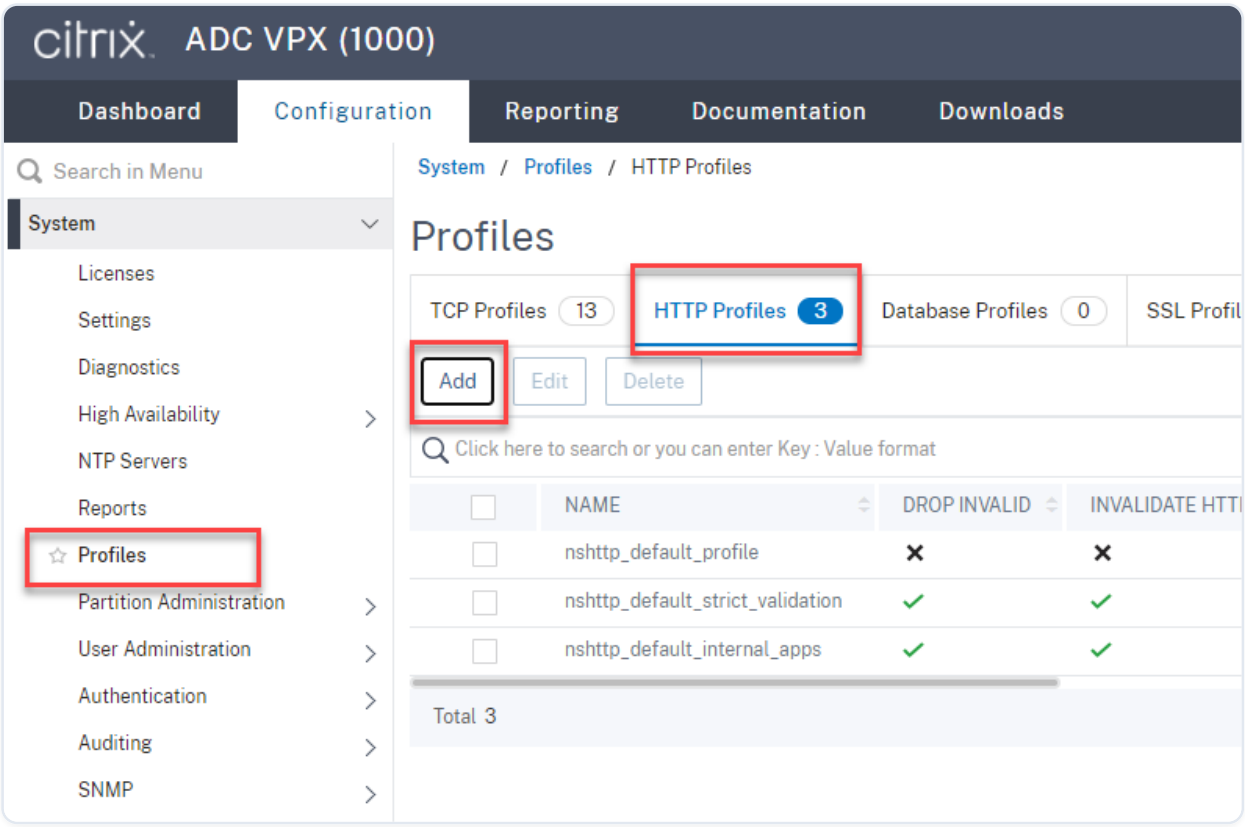


Bind the TCP monitor to the **TCP load balancing service** you just added.

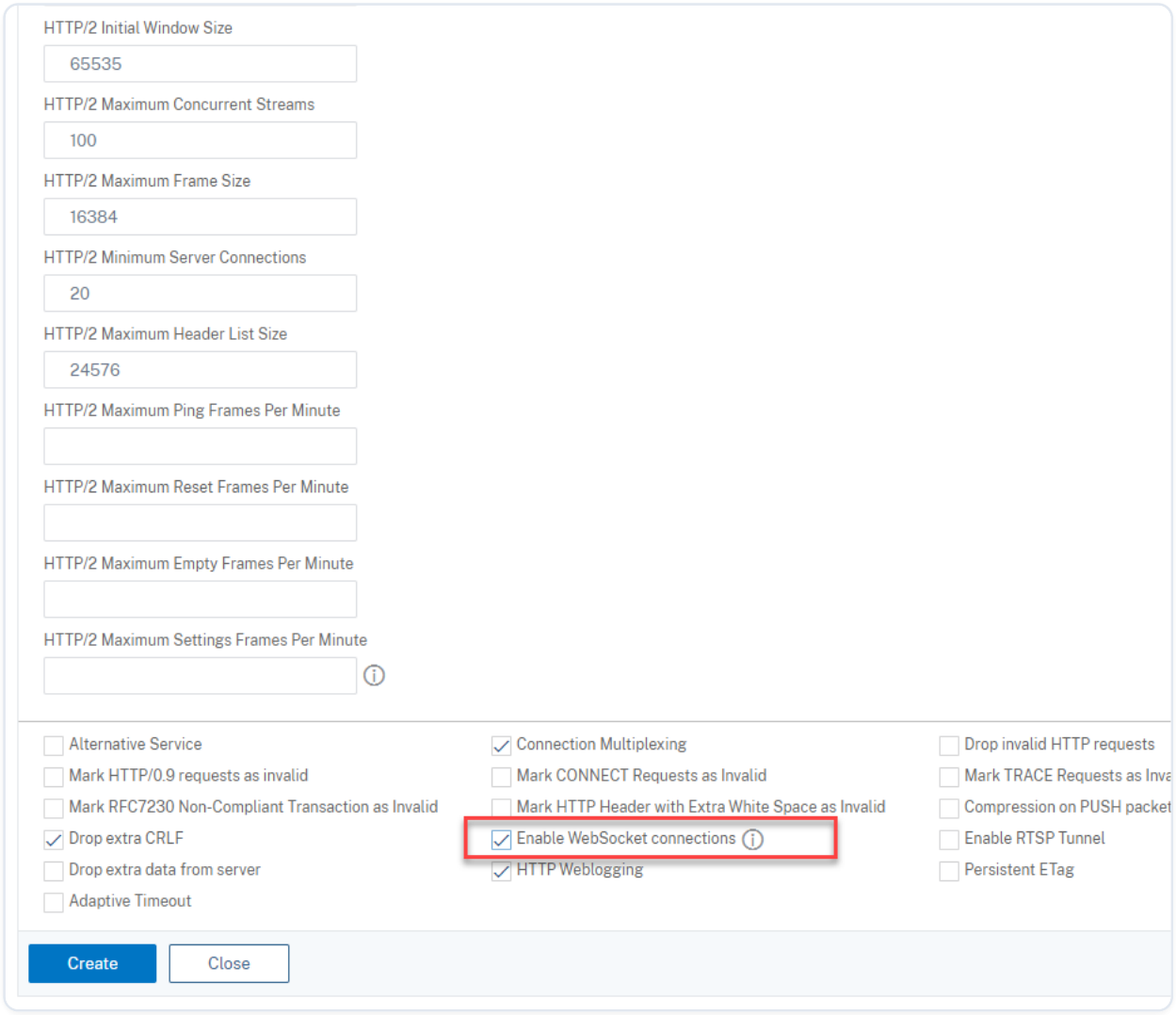


6. (Required only when you are using the WebSocket server Version 1.0) Add an HTTP profile for each **SSL load balancing service** of port 22334.

   Navigate to **System > Profiles > HTTP Profiles** and click **Add**.



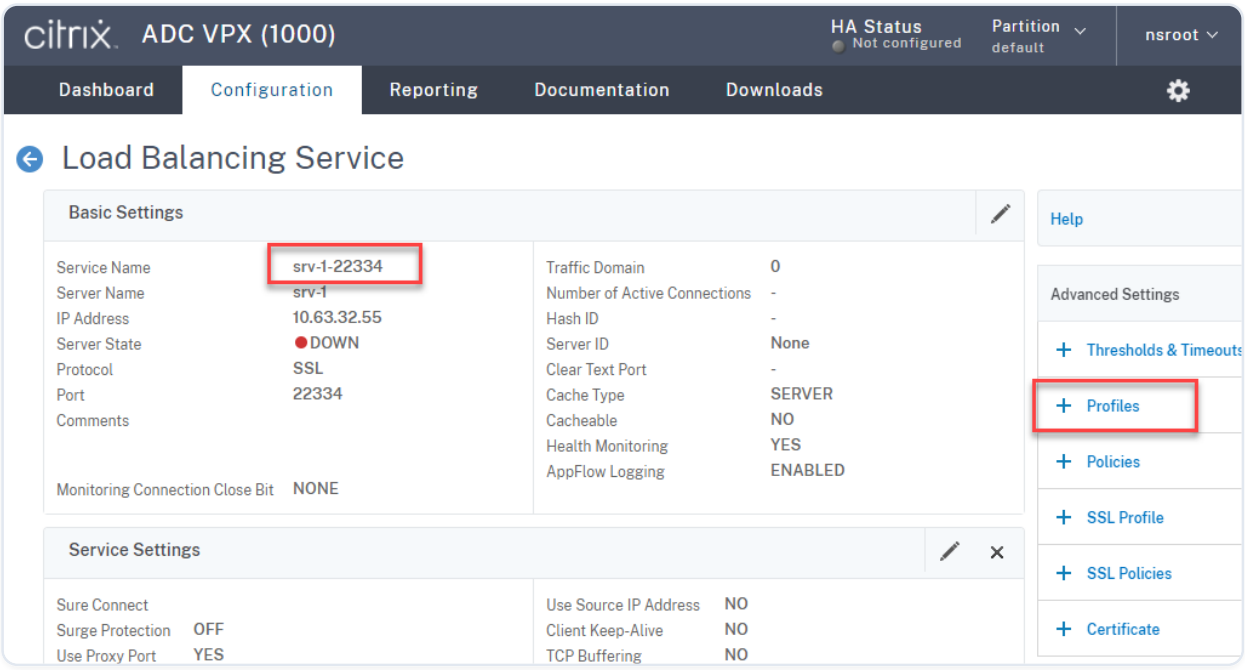
Select the **Enable WebSocket connections** check box and accept the other default settings.



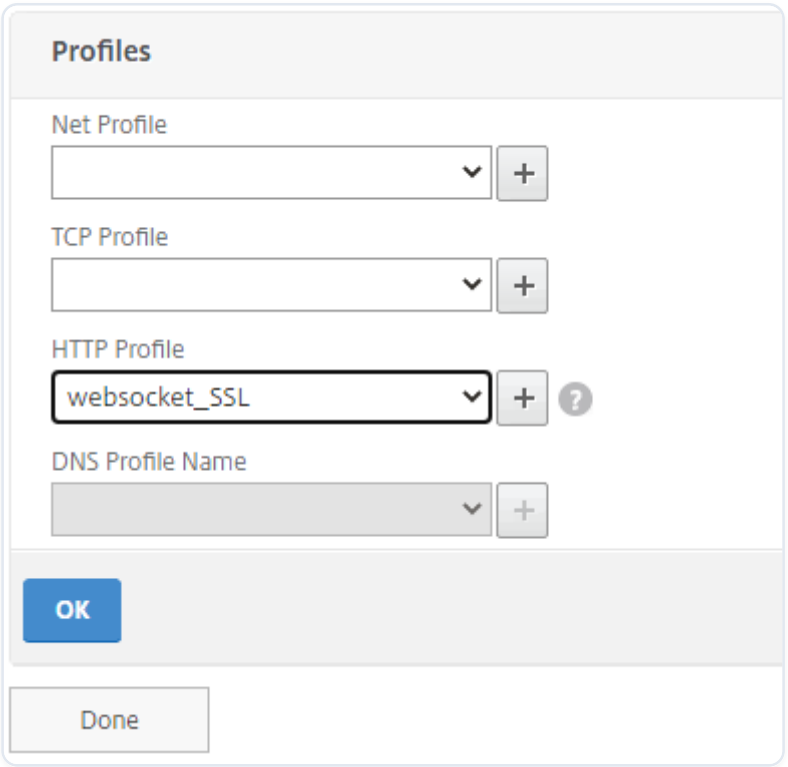
Type a name for the HTTP profile, for example, `websocket_SSL`.

Go back to each **SSL load balancing service** of port 22334, for example, `srv-1-22334`.

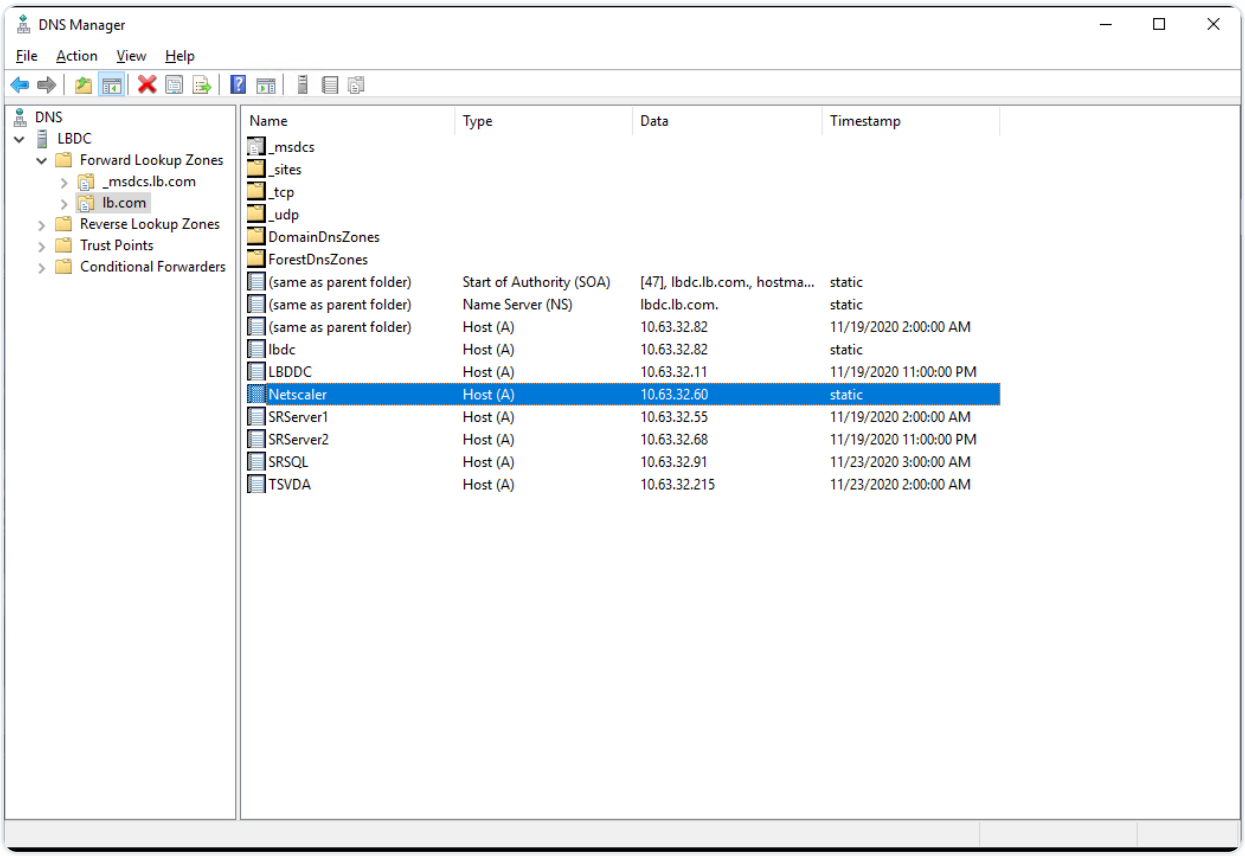
Click **+ Profiles**.



Select the HTTP profile, for example, `websocket_SSL`, and click **OK** and then **Done**.



7. (Required only when you are using the WebSocket server Version 2.0) Add an HTTP profile for each **SSL load balancing service** of port 443.
8. Create a host record for the Citrix ADC VIP address on the domain controller.

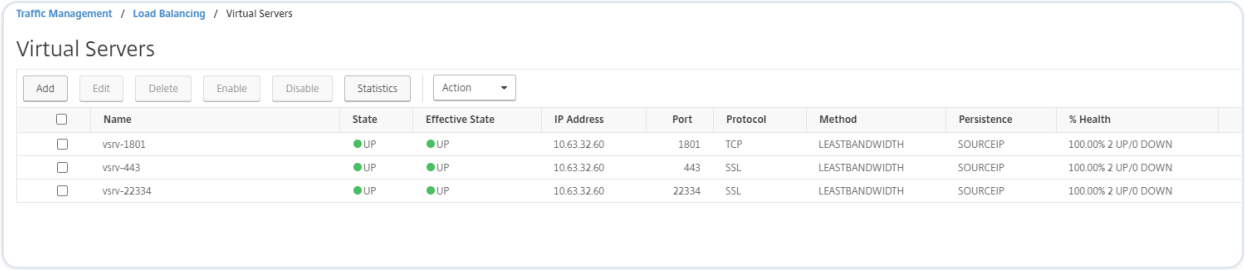


9. Add **load balancing virtual servers**.

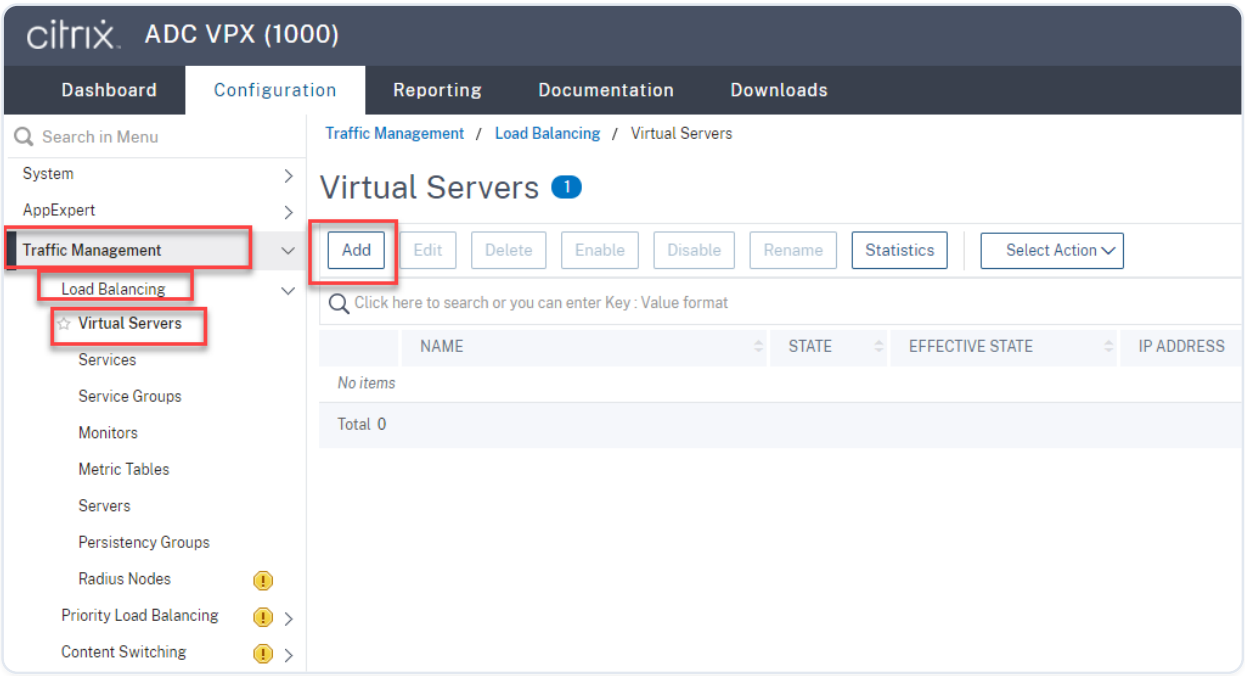
   Add the following **load balancing virtual servers** with the Citrix ADC VIP address.

   - (Required only when you are using the WebSocket server Version 1.0) **load balancing virtual server** of port 22334 based on SSL
   - **load balancing virtual server** of port 443 based on SSL
   - **load balancing virtual server** of port 1801 based on TCP

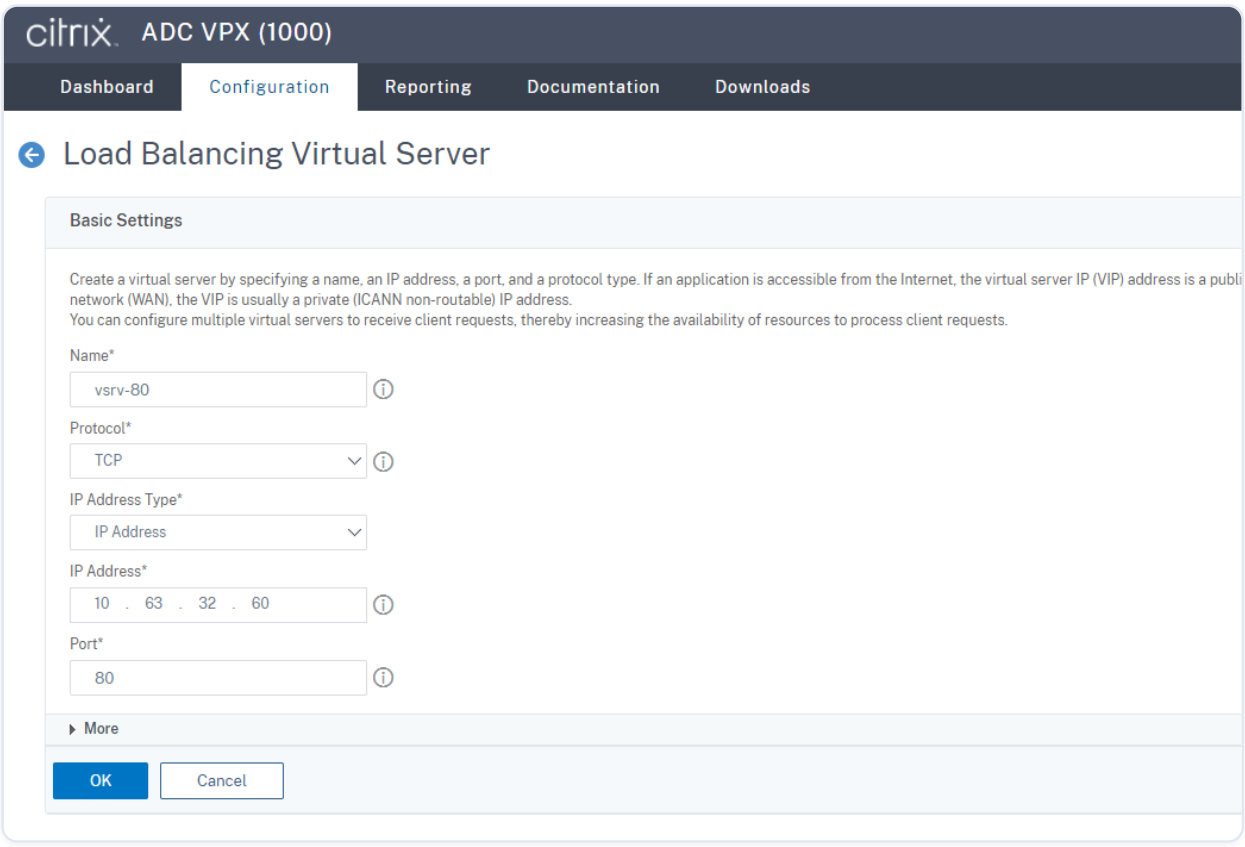
   For example, see the following screen capture.



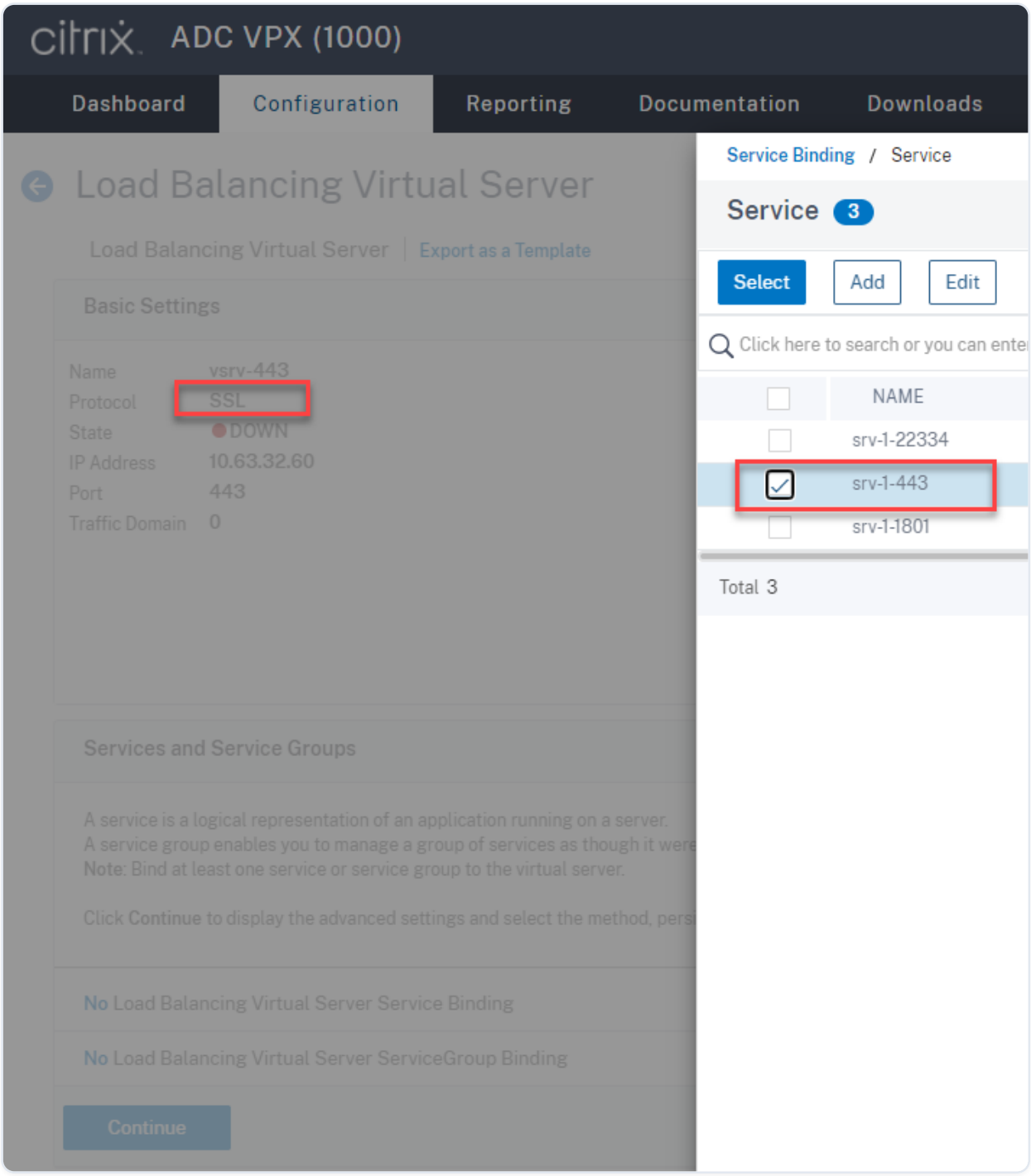
   Navigate to **Traffic Management > Load Balancing > Virtual Servers** and click **Add**.



Add each virtual server with the Citrix ADC VIP address. Type a server name, select **TCP** or **SSL**, and select the relevant port number as described earlier.



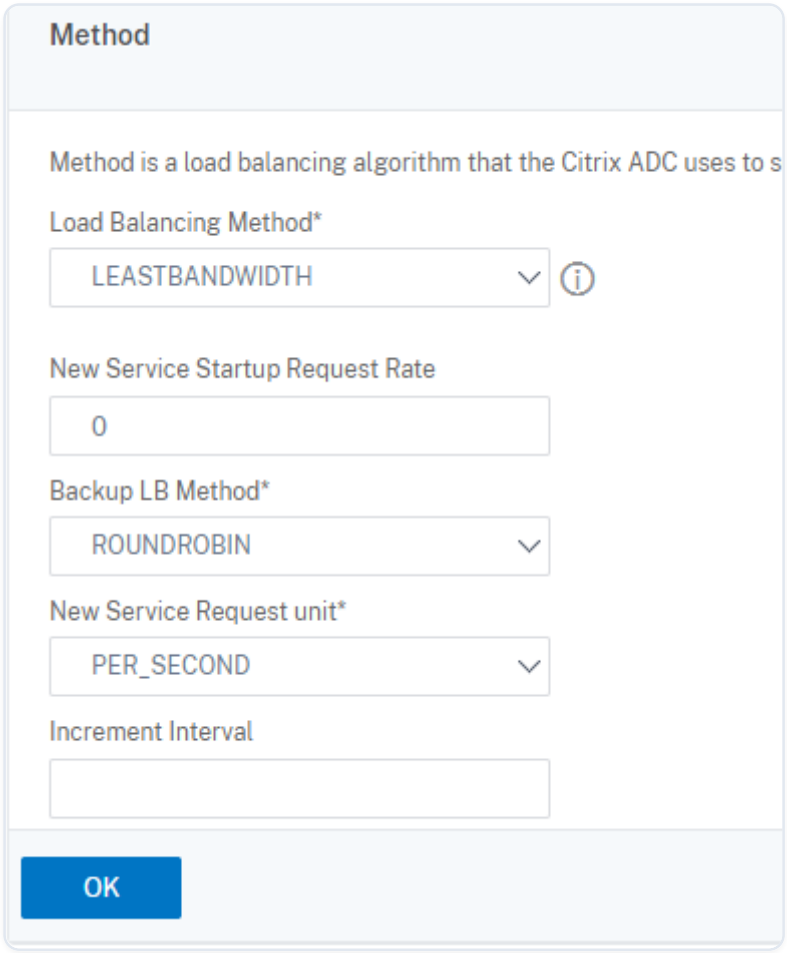
Bind each virtual server to the **load balancing service** of the same port. For example:



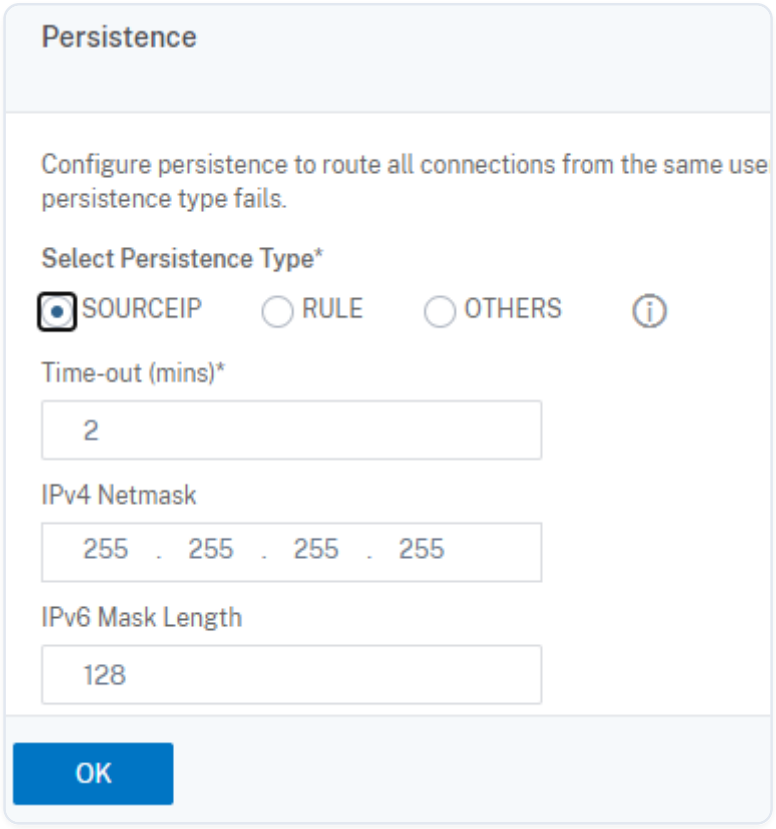
Tip:

The **load balancing service** of port 22334 is required only when you are using the WebSocket server Version 1.0.

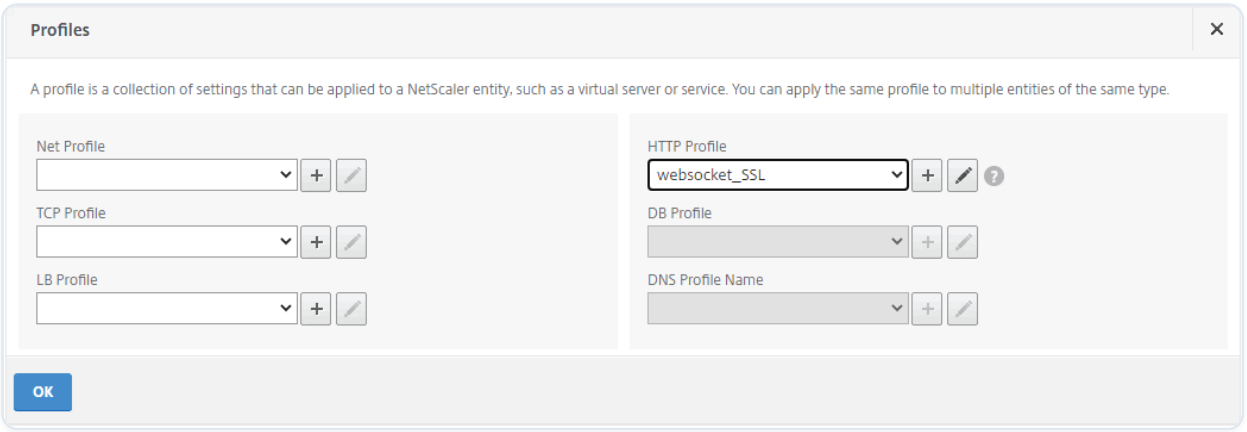
Choose a load balancing method.



Configure persistence on each virtual server. We recommend you select **SOURCEIP** as the persistence type. For more information, see Persistence settings.



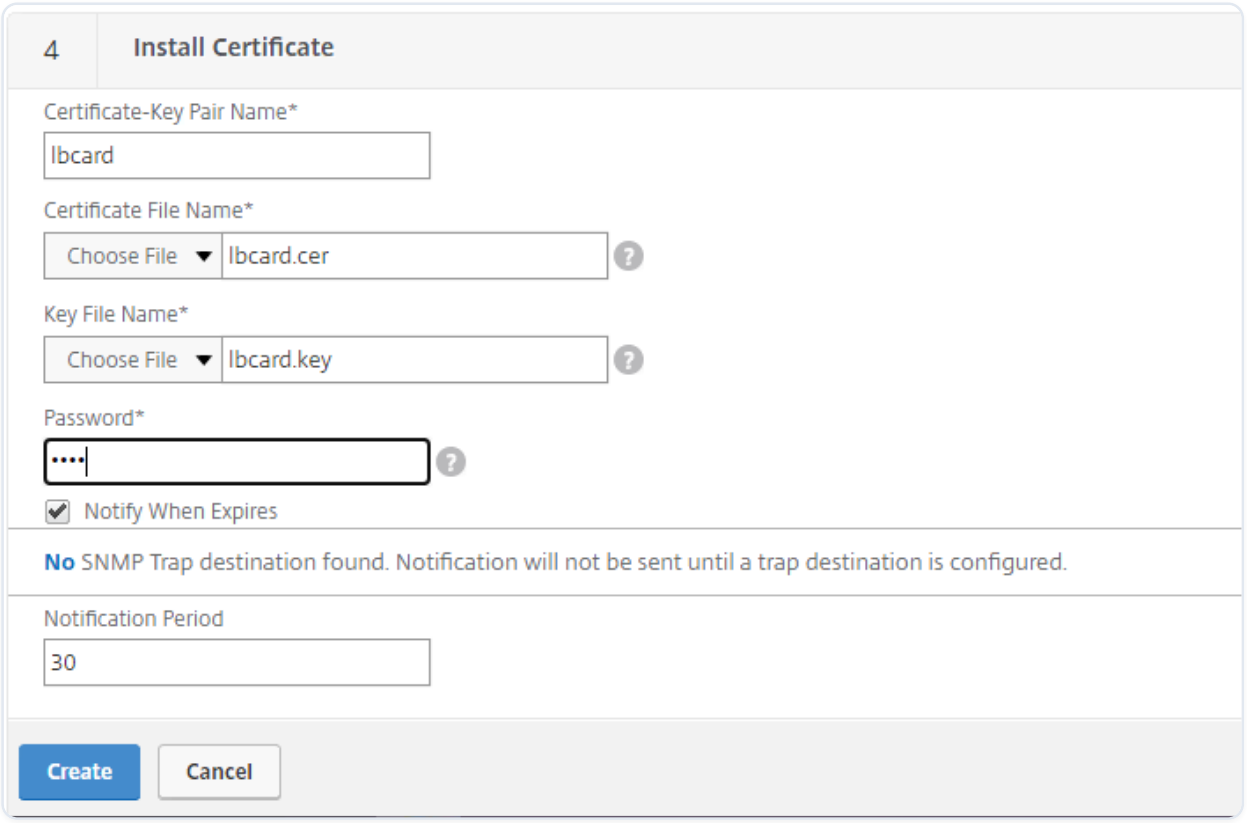
(Required only when you are using the WebSocket server Version 1.0) Add an HTTP profile for the load balancing virtual server of port 22334.



10. Install a Subject Alternative Name (SAN) certificate in Citrix ADC.

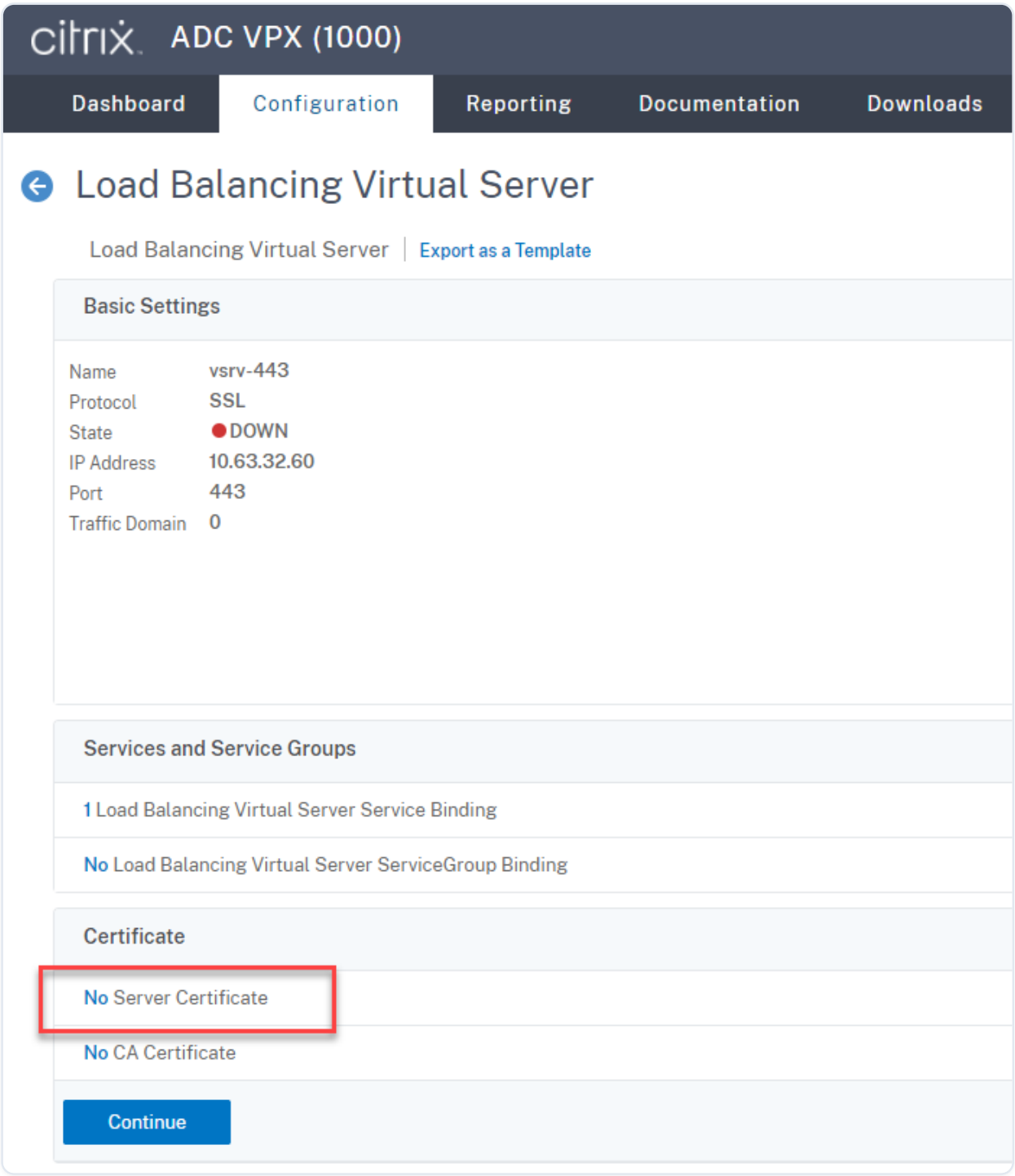
    Obtain a SAN certificate in PEM format from a trusted Certificate Authority (CA). Extract and upload the certificate and private key files in Citrix ADC by navigating to **Traffic Management > SSL > Server Certificate Wizard**.

    For more information, see SSL certificates.



11. Bind a SAN certificate to each SSL load balancing virtual server.

    Navigate to **Traffic Management > Load Balancing > Virtual Servers**, select an SSL load balancing virtual server, and click **Server Certificate**.

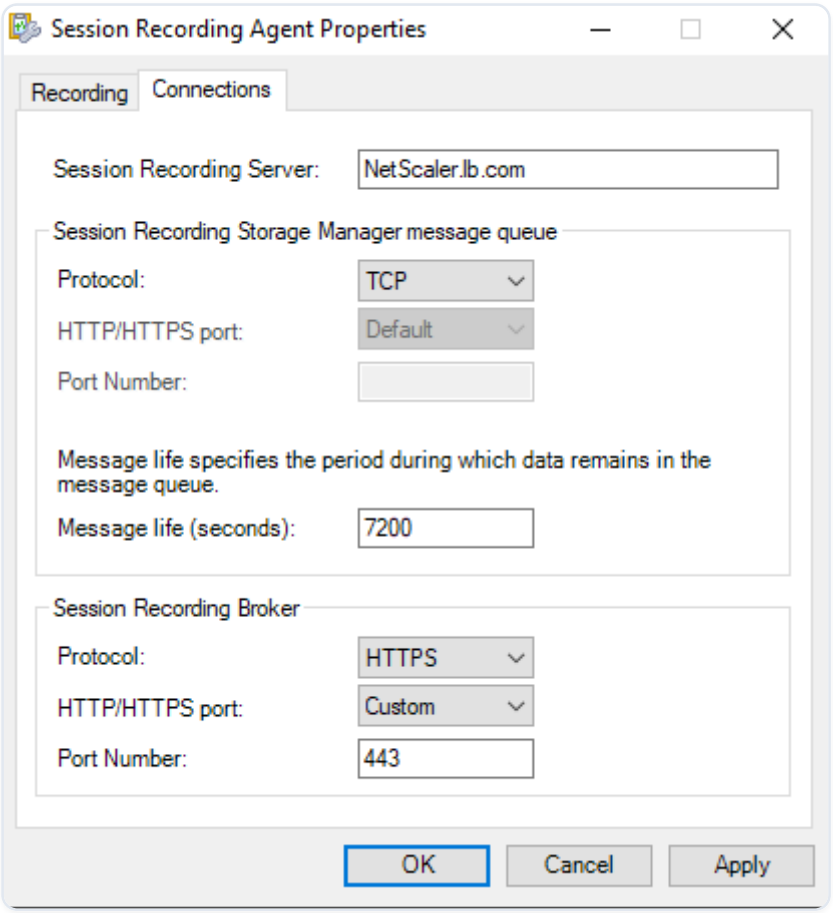


Add the previously mentioned SAN certificate and click **Bind**.

Step 4: Configure an existing Session Recording Agent to support load balancing

1. Log on to the Session Recording Agent by using a domain administrator account.
2. Open **Session Recording Agent Properties**.
3. Complete this step if you use Microsoft Message Queuing (MSMQ) over TCP.

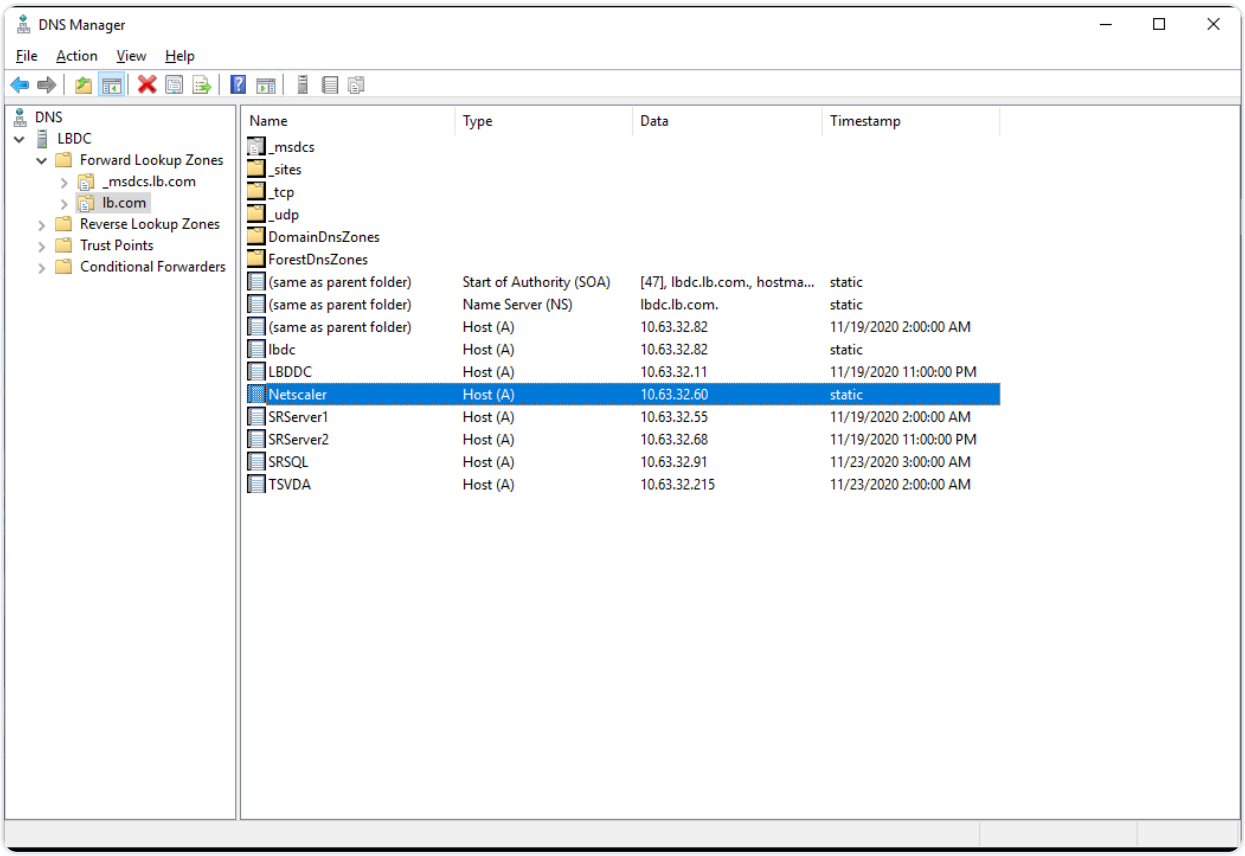
   Type the FQDN of your Citrix ADC VIP address in the **Session Recording Server** box.



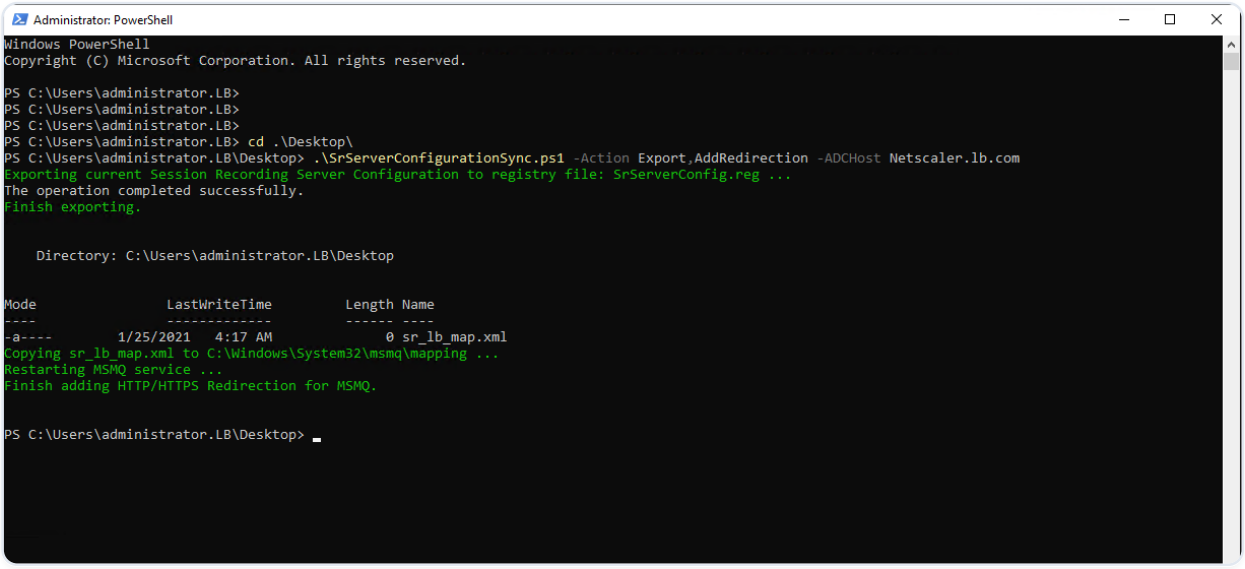
On each Session Recording server, add and set the `IgnoreOSNameValidation` DWORD value to `1` under `HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\MSMQ\Parameters`.

4. Complete this step if you use MSMQ over HTTP or HTTPS.

   (Skip if this step is done) Create a host record for the Citrix ADC VIP address on the domain controller.

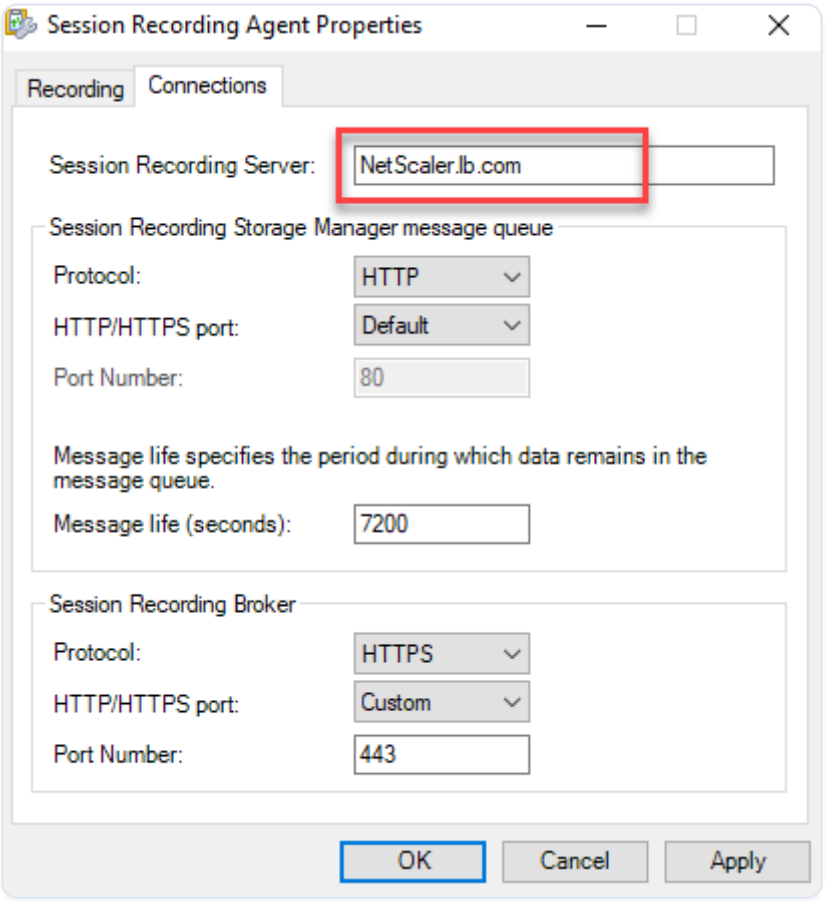


On each Session Recording server, run the `powershell.exe -file SrServerConfigurationSync.ps1 –Action AddRedirection – ADCHost <ADCHost>` command to add redirections from Citrix ADC to the local host. `<ADCHost>` is the FQDN of the Citrix ADC VIP address. A redirection file, for example, `sr_lb_map.xml` is generated under `C:\Windows\System32\msmq\Mapping`.



Note: Change to the folder where `SrServerConfigurationSync.ps1` resides when you run PowerShell.exe.

Type the FQDN of your Citrix ADC VIP address in the **Session Recording Server** box. For example:



Step 5: Configure an existing Session Recording player to support load balancing

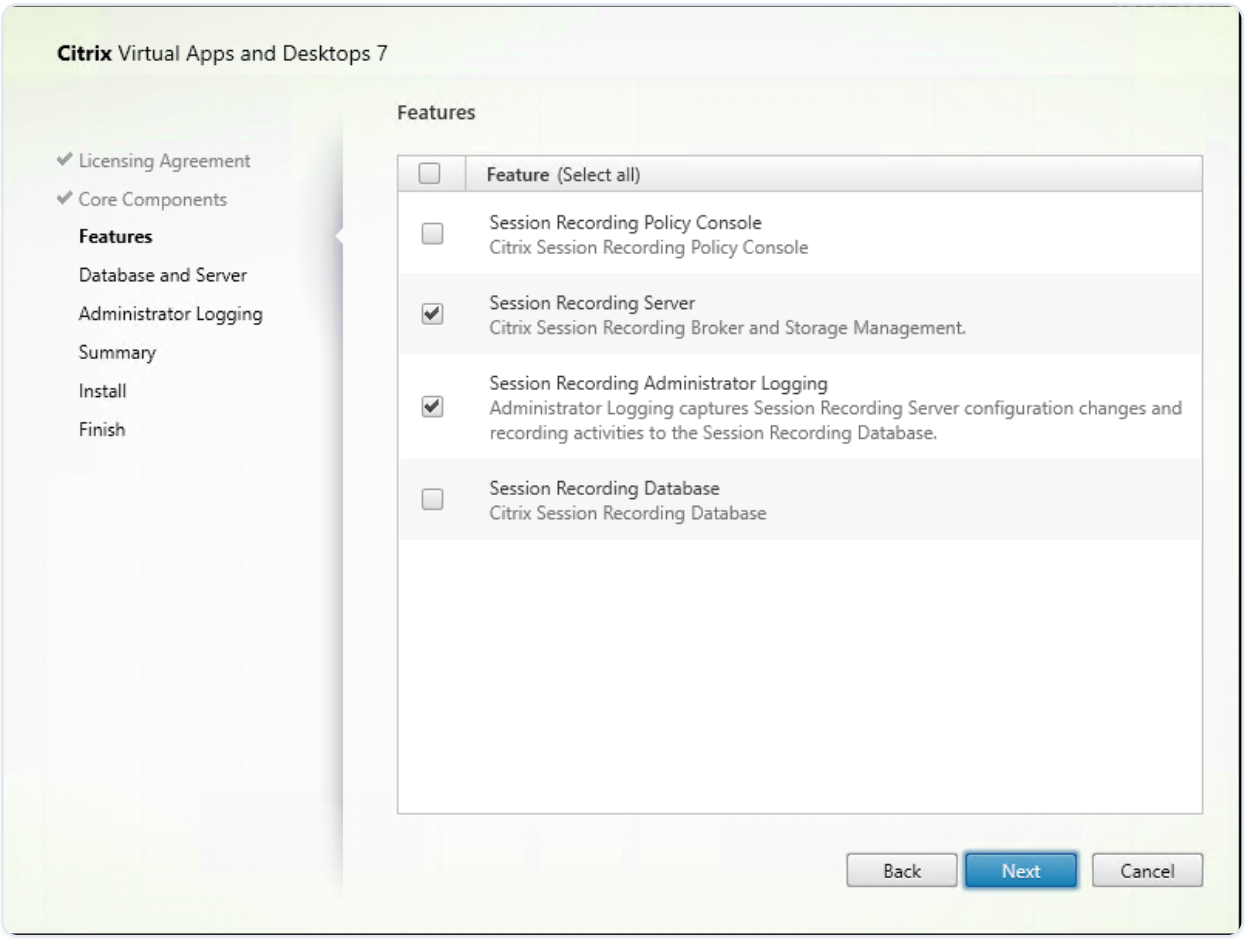
On each machine where you installed the Session Recording player component, add the Citrix ADC VIP address or its FQDN as the connected Session Recording server.

Step 6: Check whether load balancing works for the configured, existing Session Recording server

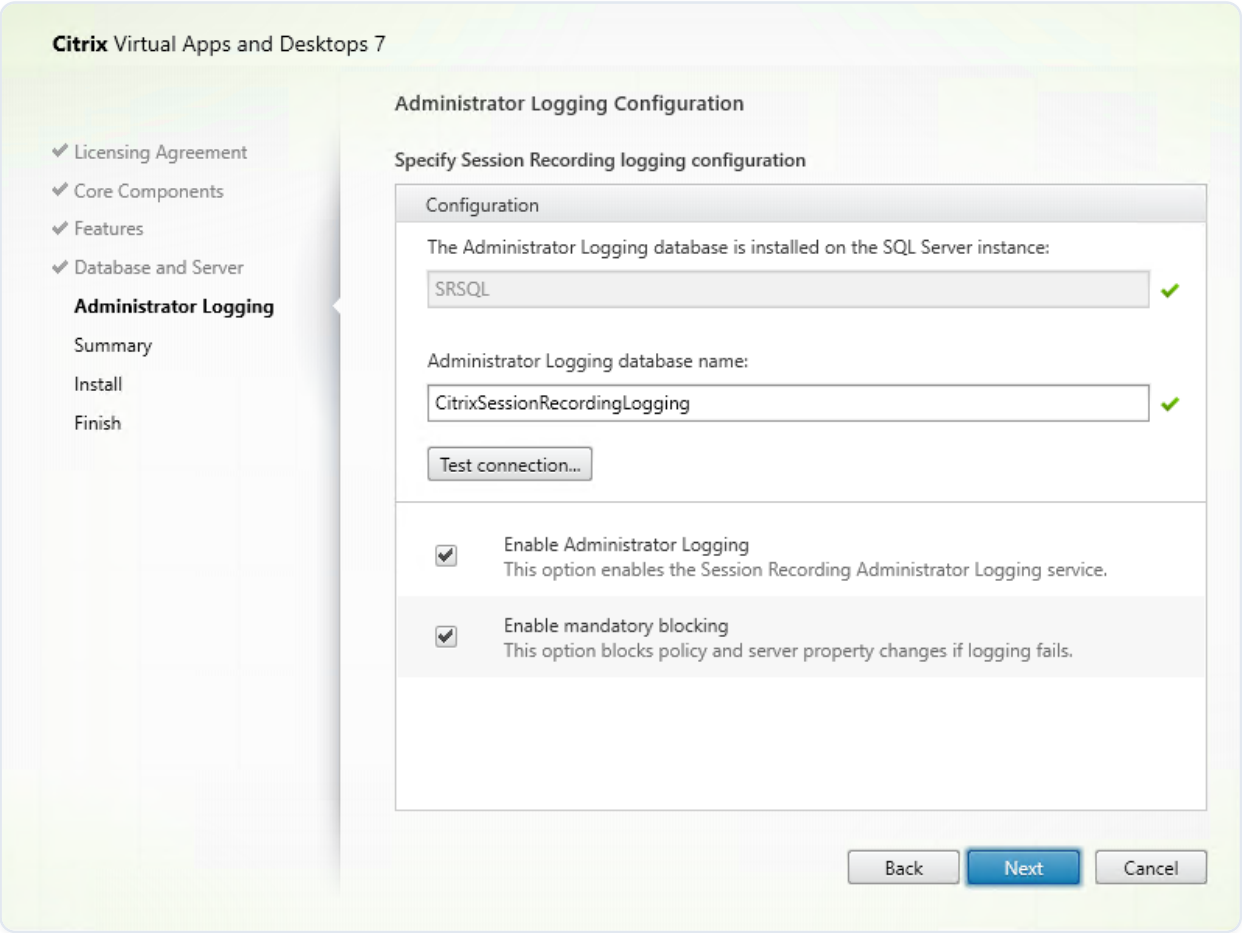
1. Launch a Citrix virtual session.
2. Check whether the session can be recorded.
3. Check whether the web player and the Session Recording player can play back the recording file.

Step 7: Add more Session Recording servers

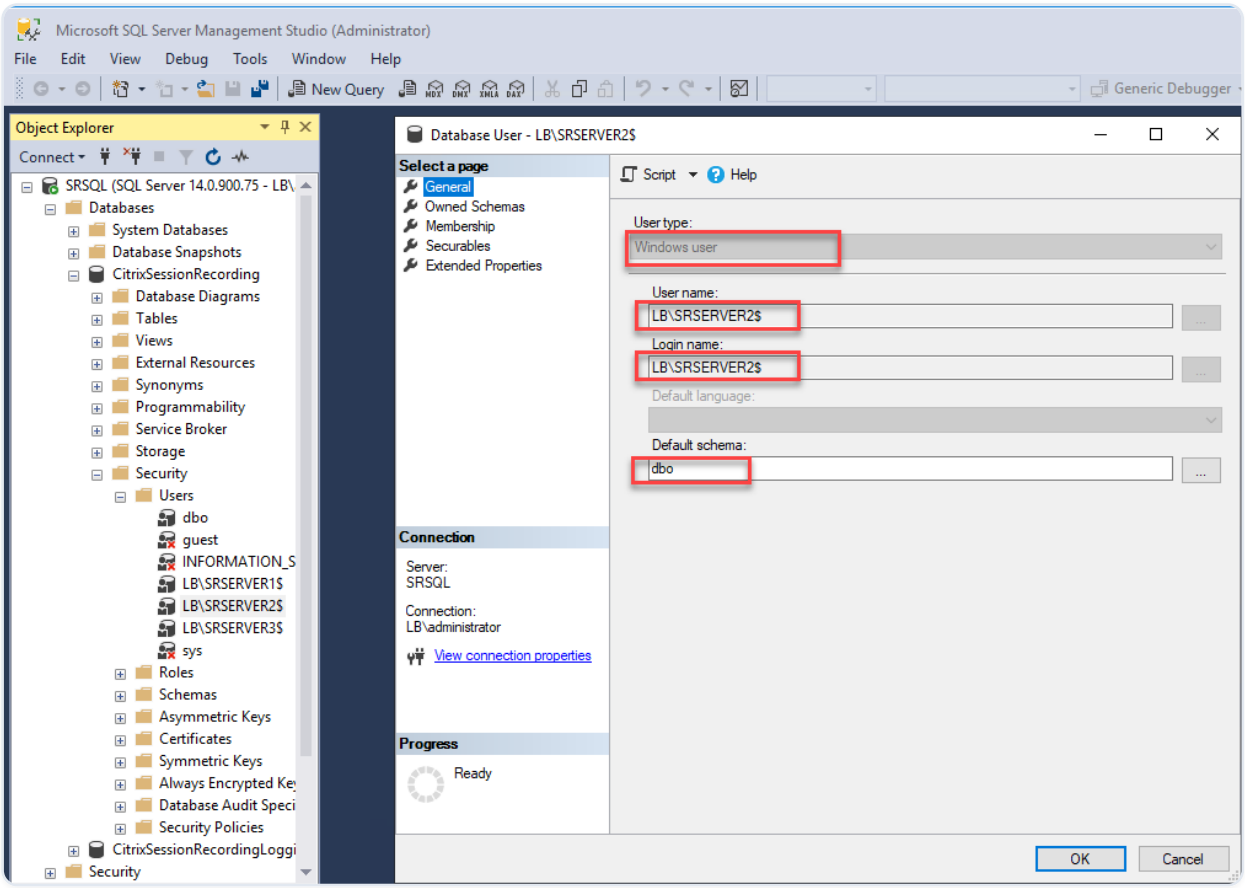
1. Prepare a machine in the same domain and install only the Session Recording server and Session Recording Administrator Logging modules on the machine.

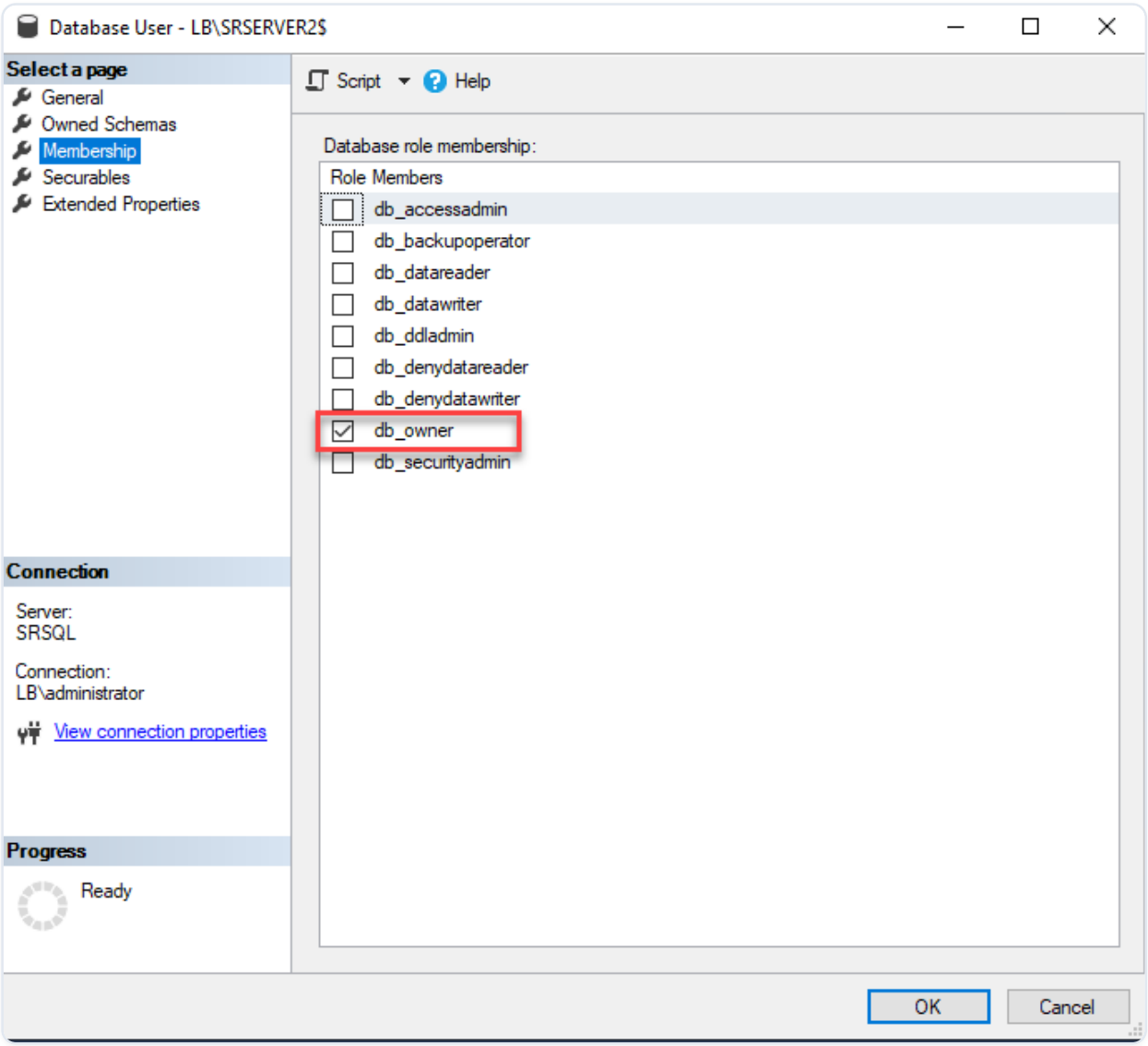


2. Use the same database names as the existing Session Recording server. For example:

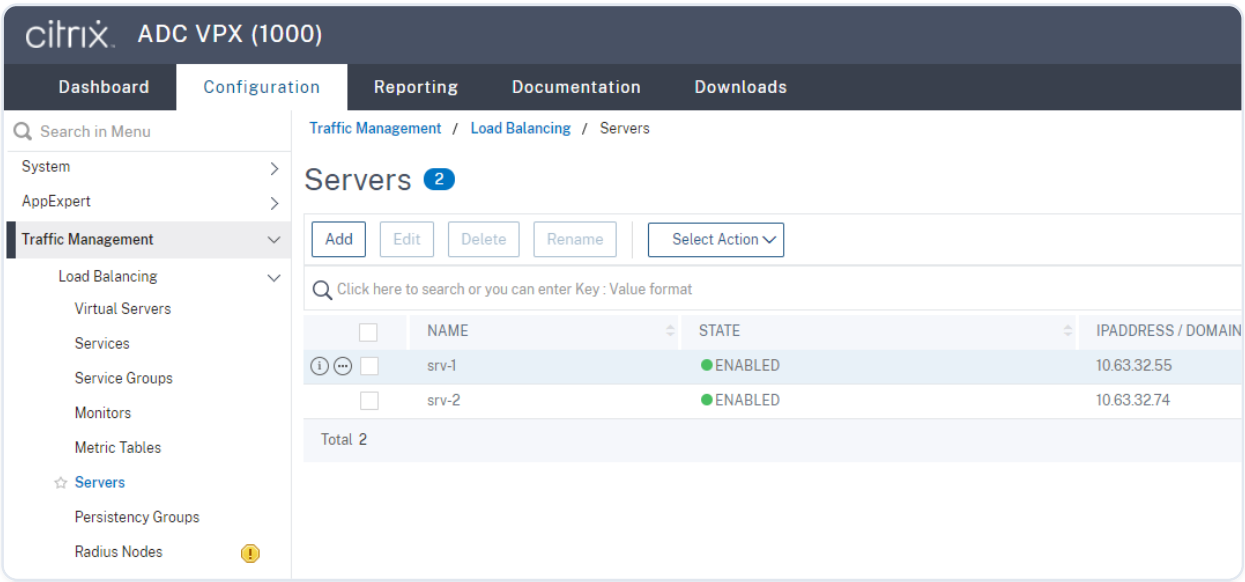


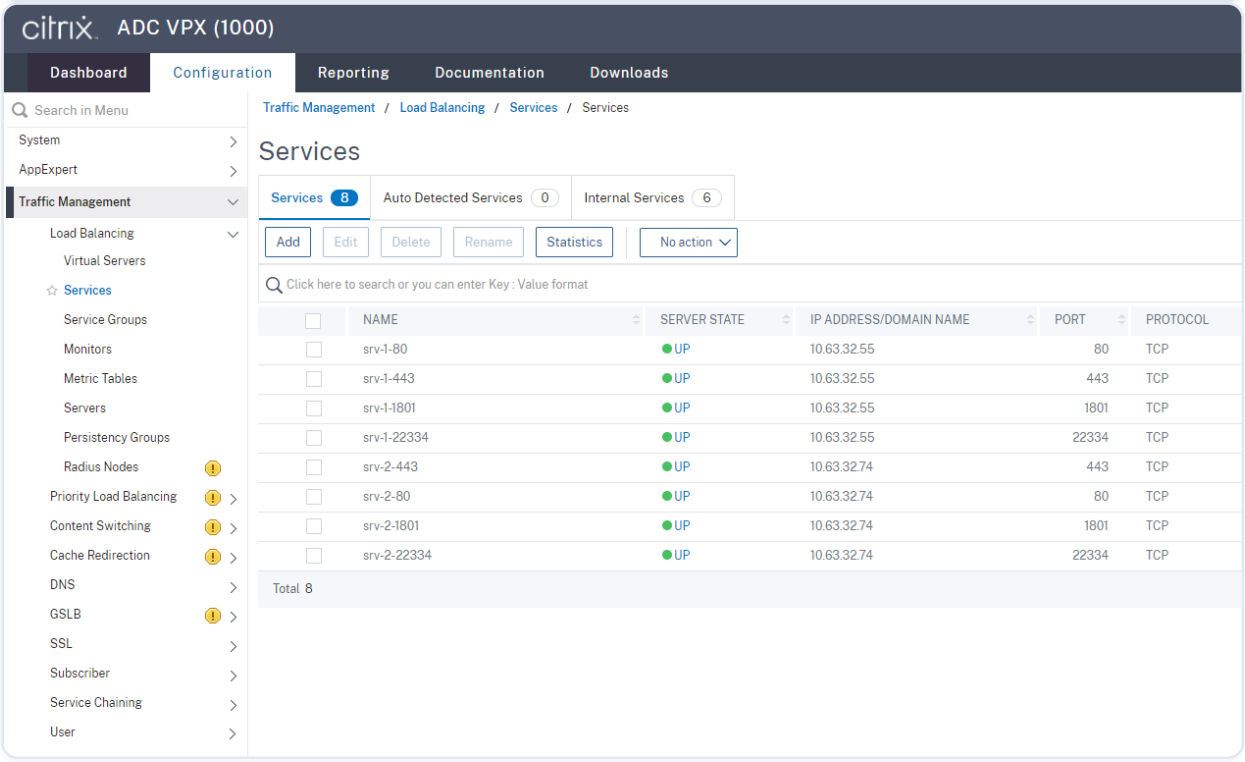
3. Disable the network firewall on the machine.
4. On the SQL Server where you installed the Session Recording database, add all the Session Recording server machine accounts to the shared Session Recording database and assign them with the `db_owner` permission. For example:

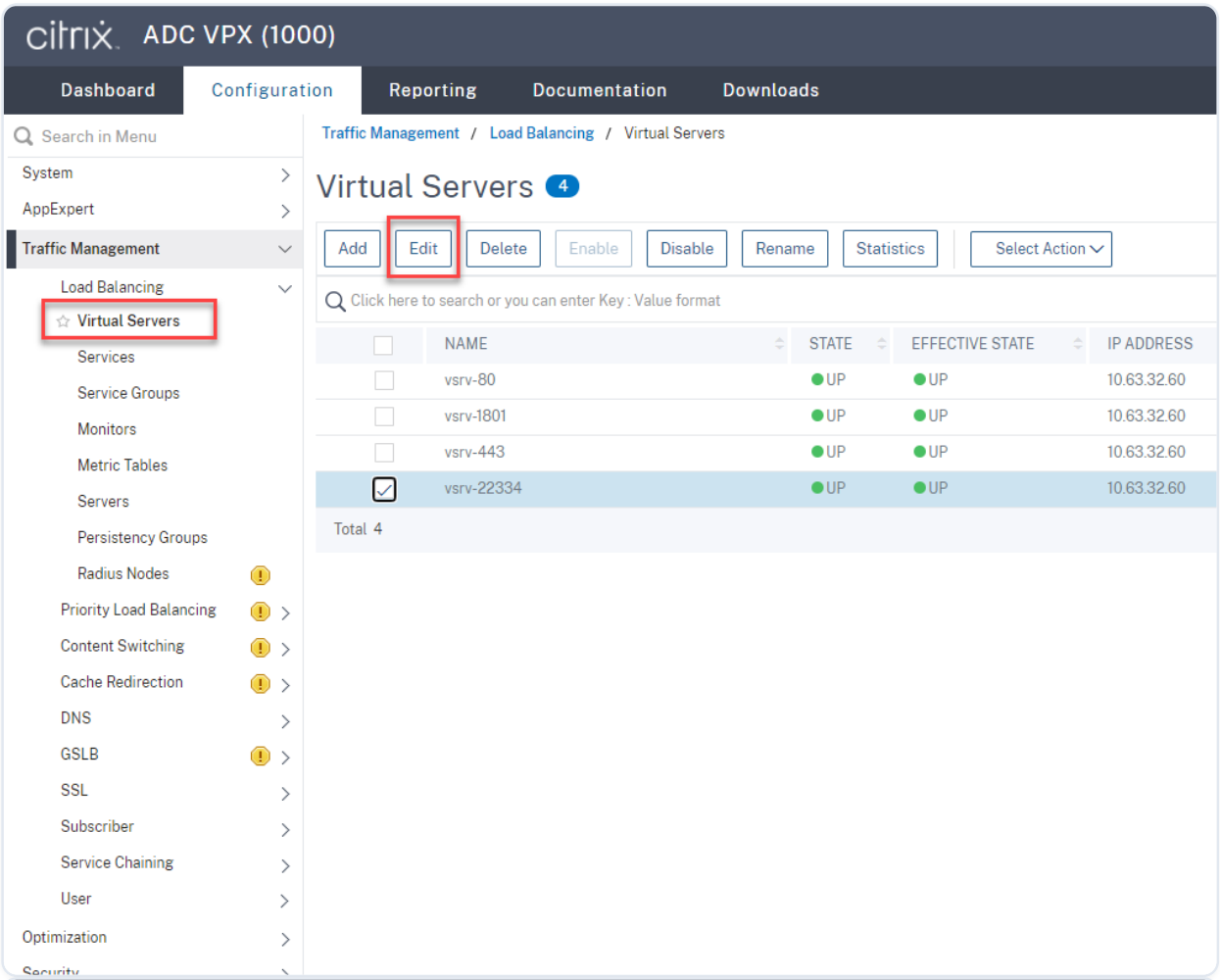

Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Generic Debugger
Object Explorer
Connect
SRSQL (SQL Server 14.0.900.75 - LB\
Databases
System Databases
Database Snapshots
CitrixSessionRecording
Database Diagrams
Tables
Views
External Resources
Synonyms
Programmability
Service Broker
Storage
Security
Users
dbo
guest
INFORMATION_S
LB\SRSERVER1$
LB\SRSERVER2$
LB\SRSERVER3$
sys
Roles
Schemas
Asymmetric Keys
Certificates
Symmetric Keys
Always Encrypted Ke
Database Audit Speci
Security Policies
CitrixSessionRecordingLoggi
Security
Database User - LB\SRSERVER2$
Select a page
General
Owned Schemas
Membership
Securables
Extended Properties
Script
Help
User type:
Windows user
User name:
LB\SRSERVER2$
Login name:
LB\SRSERVER2$
Default language:
Default schema:
dbo
Connection
Server:
SRSQL
Connection:
LB\administrator
View connection properties
Progress
Ready
OK
Cancel

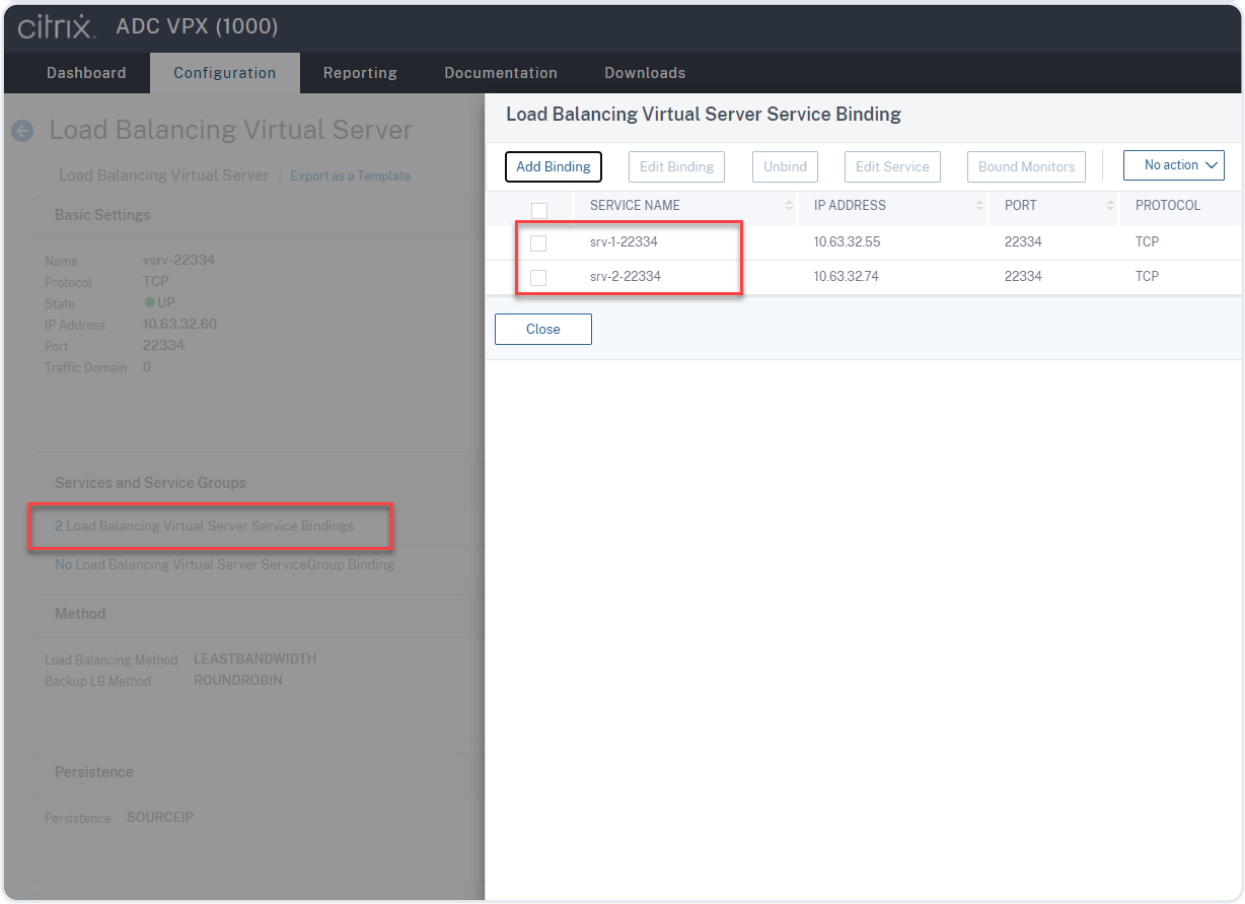


5. Share the Read/Write permission of the recording storage and restore folders, for example, `SessionRecording` and `SessionRecordingsRestored`, with the machine account of the new Session Recording server, for example, `LB\SRServer2$`. The dollar sign `$` is required.
6. Repeat Step 3 to add **load balancing services** for the new Session Recording server and edit existing virtual servers to add bindings to the load balancing services. There is no need to add more virtual servers. For example:


citrix ADC VPX (1000)
Dashboard
Configuration
Reporting
Documentation
Downloads
Search in Menu
System
AppExpert
Traffic Management
Load Balancing
Virtual Servers
Services
Service Groups
Monitors
Metric Tables
Servers
Persistency Groups
Radius Nodes
Traffic Management / Load Balancing / Servers
Servers 2
Add
Edit
Delete
Rename
Select Action
Click here to search or you can enter Key : Value format
NAME
STATE
IPADDRESS / DOMAIN
srv-1
ENABLED
10.63.32.55
srv-2
ENABLED
10.63.32.74
Total 2


citrix ADC VPX (1000)
Dashboard
Configuration
Reporting
Documentation
Downloads
Search in Menu
System
AppExpert
Traffic Management
Load Balancing
Virtual Servers
Services
Service Groups
Monitors
Metric Tables
Servers
Persistency Groups
Radius Nodes
Priority Load Balancing
Content Switching
Cache Redirection
DNS
GSLB
SSL
Subscriber
Service Chaining
User
Traffic Management / Load Balancing / Services / Services
Services
Services 8
Auto Detected Services 0
Internal Services 6
Add
Edit
Delete
Rename
Statistics
No action
Click here to search or you can enter Key : Value format
NAME
SERVER STATE
IP ADDRESS/DOMAIN NAME
PORT
PROTOCOL
srv-1-80 UP 10.63.32.55 80 TCP
srv-1-443 UP 10.63.32.55 443 TCP
srv-1-1801 UP 10.63.32.55 1801 TCP
srv-1-22334 UP 10.63.32.55 22334 TCP
srv-2-443 UP 10.63.32.74 443 TCP
srv-2-80 UP 10.63.32.74 80 TCP
srv-2-1801 UP 10.63.32.74 1801 TCP
srv-2-22334 UP 10.63.32.74 22334 TCP
Total 8


citrix ADC VPX (1000)
Dashboard
Configuration
Reporting
Documentation
Downloads
Search in Menu
System
AppExpert
Traffic Management
Load Balancing
Virtual Servers
Services
Service Groups
Monitors
Metric Tables
Servers
Persistency Groups
Radius Nodes
Priority Load Balancing
Content Switching
Cache Redirection
DNS
GSLB
SSL
Subscriber
Service Chaining
User
Optimization
Traffic Management / Load Balancing / Virtual Servers
Virtual Servers 4
Add
Edit
Delete
Enable
Disable
Rename
Statistics
Select Action
Click here to search or you can enter Key : Value format
NAME
STATE
EFFECTIVE STATE
IP ADDRESS
vsrv-80 UP UP 10.63.32.60
vsrv-1801 UP UP 10.63.32.60
vsrv-443 UP UP 10.63.32.60
vsrv-22334 UP UP 10.63.32.60
Total 4


citrix ADC VPX (1000)
Dashboard
Configuration
Reporting
Documentation
Downloads
Load Balancing Virtual Server
Load Balancing Virtual Server
Export as a Template
Basic Settings
Name vsrv-22334
Protocol TCP
State UP
IP Address 10.63.32.60
Port 22334
Traffic Domain 0
Services and Service Groups
2 Load Balancing Virtual Server Service Bindings
No Load Balancing Virtual Server ServiceGroup Binding
Method
Load Balancing Method LEASTBANDWIDTH
Backup LB Method ROUNDROBIN
Persistence
Persistence SOURCEIP
Load Balancing Virtual Server Service Binding
Add Binding
Edit Binding
Unbind
Edit Service
Bound Monitors
No action
SERVICE NAME
IP ADDRESS
PORT
PROTOCOL
srv-1-22334 10.63.32.55 22334 TCP
srv-2-22334 10.63.32.74 22334 TCP
Close

7. Copy the Session Recording Authorization Console configuration file, `SessionRecordingAzManStore.xml`, from the existing Session Recording server to the new Session Recording server. The file lives in `<Session Recording Server installation path>\App_Data`.
8. To use MSMQ over HTTP or HTTPS for the new Session Recording server, complete the following steps to import the registry settings of the currently functioning Session Recording server.

   On the existing Session Recording server, for example, `SRServer1`, run the `powershell.exe -file SrServerConfigurationSync.ps1 –Action Export – ADCHost <ADCHost >` command, where `<ADCHost>` is the FQDN of the Citrix ADC VIP address. An exported registry file, `SrServerConfig.reg`, is generated.

   Copy the `SrServerConfig.reg` file to the new Session Recording server and run the `powershell.exe -file SrServerConfigurationSync.ps1 –Action Import,AddRedirection – ADCHost <ADCHost>` command. The **EnableLB** value is added to the registry key of the new Session Recording Server at `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server` and a `sr_lb_map.xml` file is added under `C:\Windows\System32\msmq\Mapping`.
9. Repeat the procedure to add another Session Recording server.

Troubleshoot

- Sessions are not recording when you use a CNAME record or an ALIAS record for a Session Recording server. To address this issue, see the Microsoft documentation.
- Recording files can be stored locally but cannot be stored in a Universal Naming Convention (UNC) path. To address this issue, change the start mode of the Citrix Session Recording Storage Manager service to **Automatic (Delayed Start)**.

Deploy and load balance Session Recording in Azure

Prerequisites

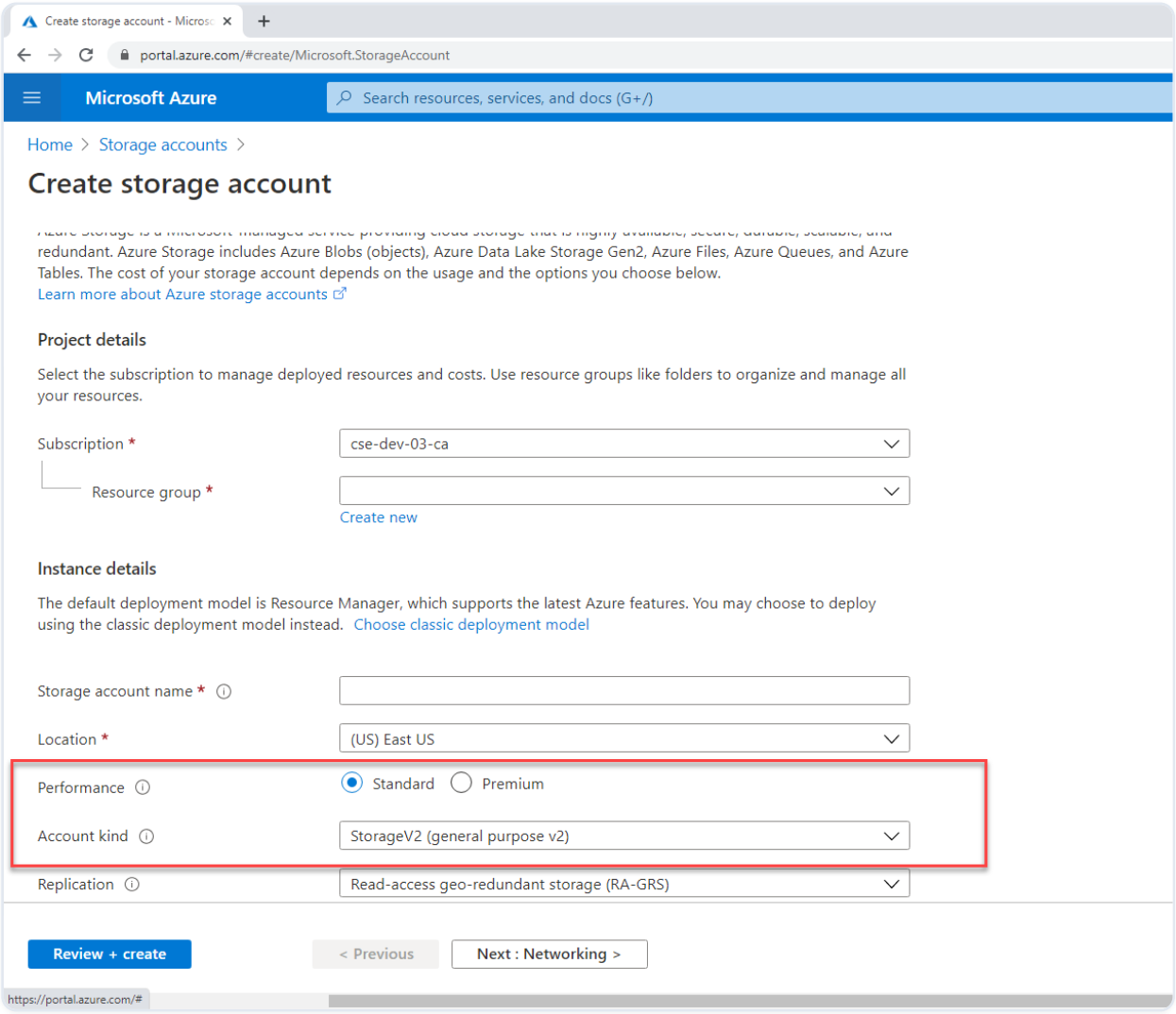
- You already have Citrix Virtual Apps and Desktops™ or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) installed in Azure.
- You have an Azure account.

Step 1: Upload the Citrix Virtual Apps™ and Desktops installer to Azure

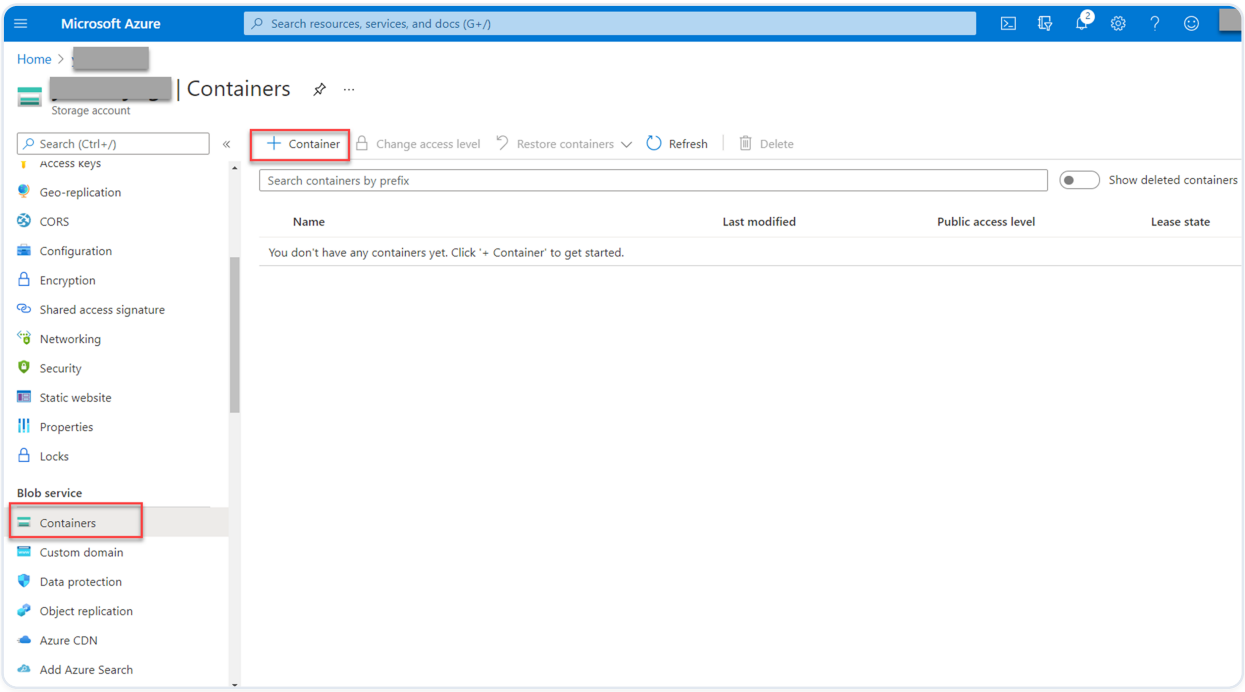
> **Note:**
>
> Skip Step 1 if you use your Citrix account credentials to access the Citrix Virtual Apps and Desktops download page and download the product ISO file to a VM in Azure.

1. In the Azure portal, create a **general-purpose v2** storage account and accept the default performance tier, **Standard**.

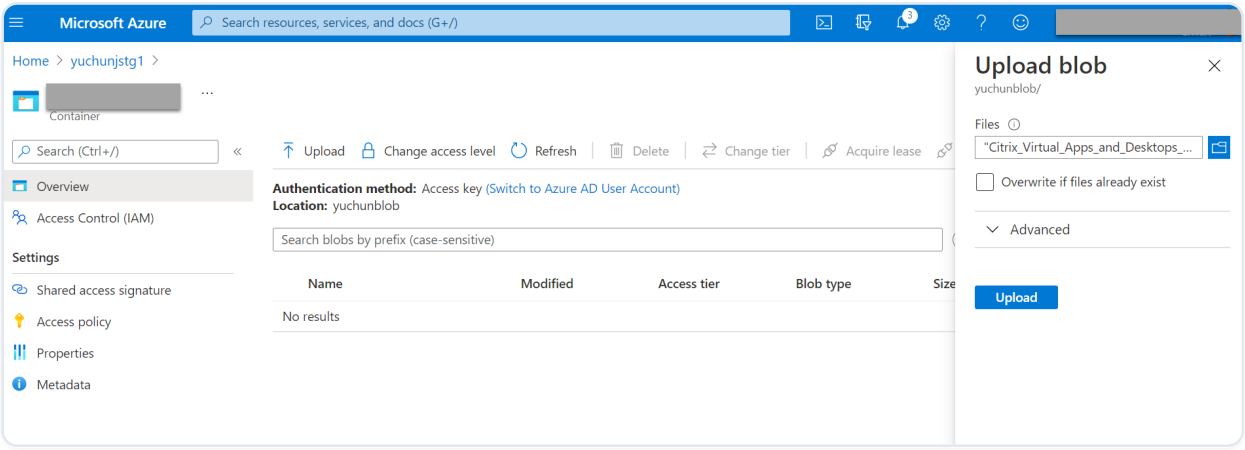
   All access to Azure Storage goes through a storage account.



2. Navigate to your new storage account and select **Containers** in the **Blob service** section to create a container.



3. Upload the Citrix Virtual Apps and Desktops installer to the container.

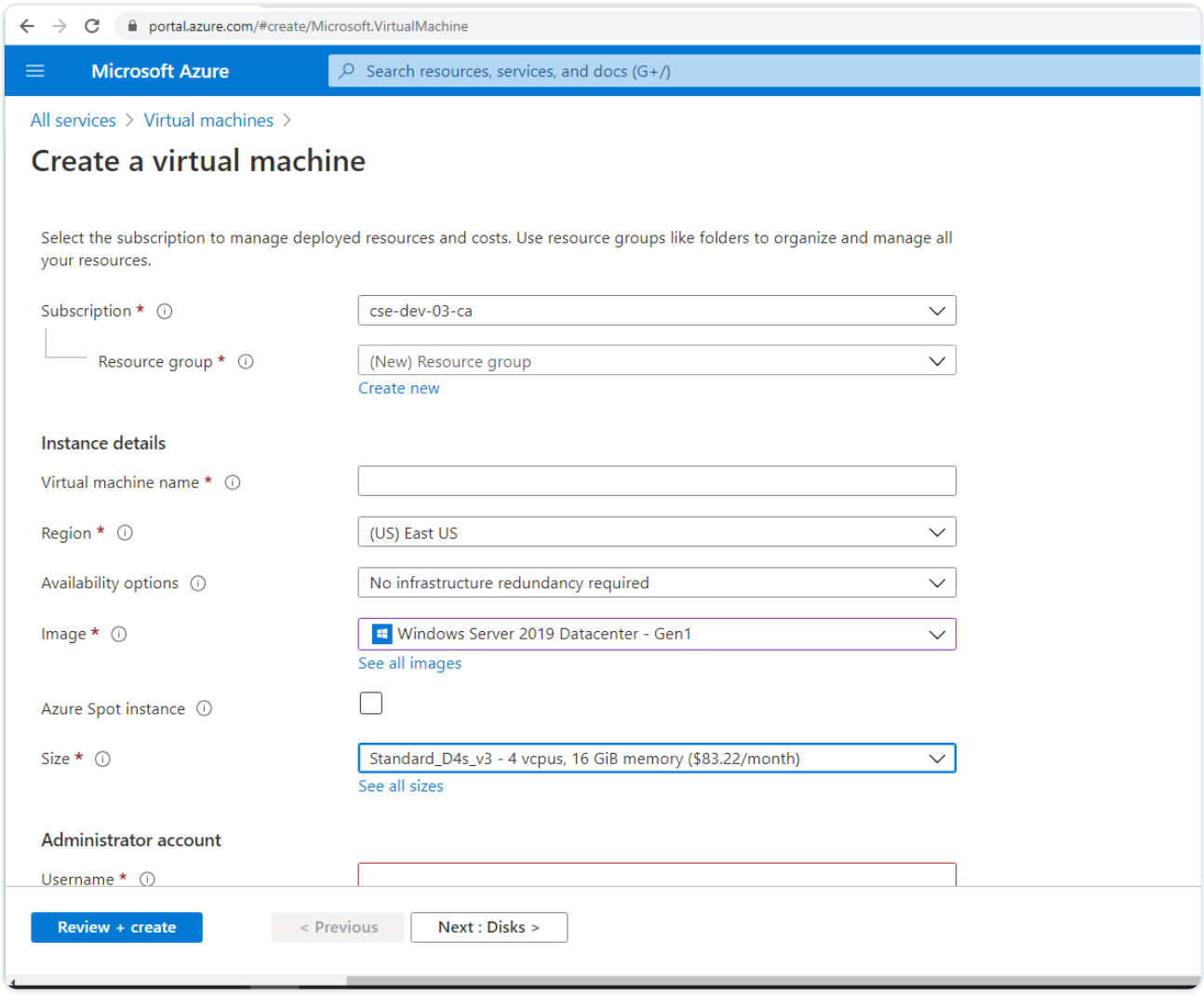


Step 2: Create a SQL managed instance in the Azure portal

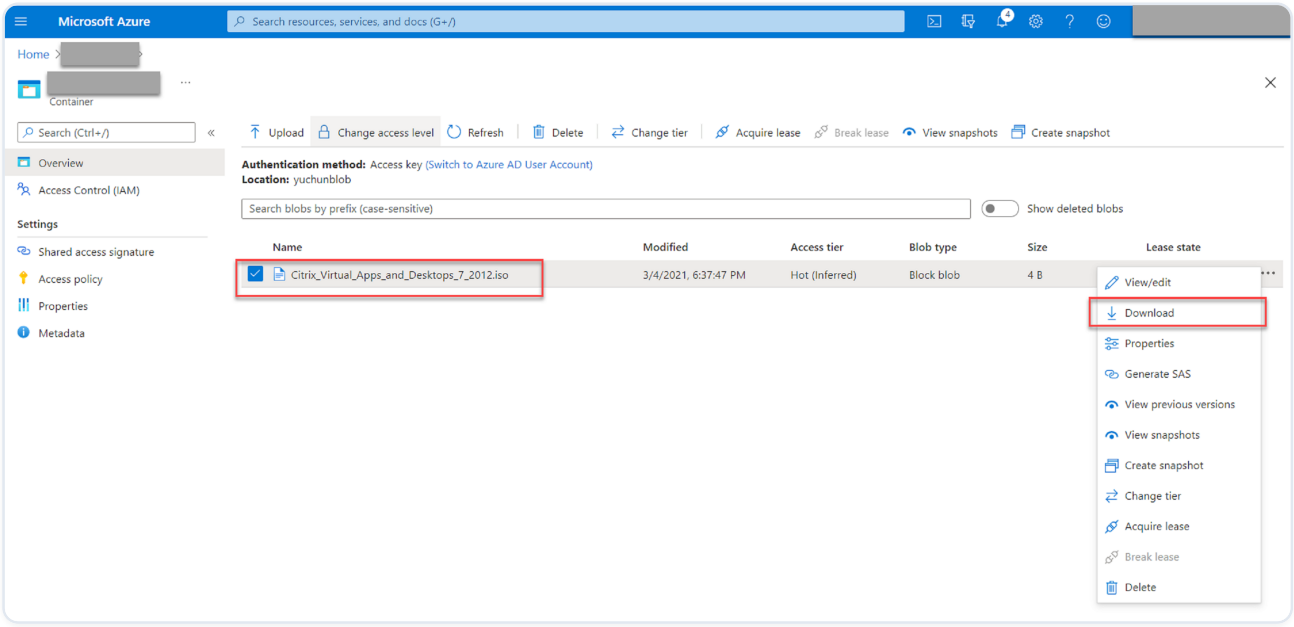
For more information, see Create an Azure SQL Managed Instance.

Step 3: Create Azure virtual machines (VMs)

Choose **Windows Server 2019 Datacenter – Gen1** for the image and **Standard_D4as_v4 – 4 vcpus, 16GiB memory** for the size. For more information, see Create a Windows virtual machine in the Azure portal.



Step 4: Remote desktop and download the Citrix Virtual Apps and Desktops installer to the Azure VMs



Step 5: Run the installer to install Session Recording components on the Azure VMs

For more information, see Install the Session Recording Administration components.

Step 6: Configure an Azure file share to store recordings

To create an Azure file share to store recordings, complete the following steps:

1. In the Azure portal, create a storage account and then create an Azure file share.

   For a quick start guide, see Create and manage Azure file shares with the Azure portal. The following table recommends configurations for your consideration.

RECORDING FILE SIZE MB/ HOUR	NUMBER OF RECORDED SESSIONS PER DAY	FILE SHARE TYPE	FILE SHARE QUOTA (TB)	SESSION RECORDING SERVER QUANTITY	SESSION RECORDING SERVER SIZE
< 6.37	< 1,000	HDD Standard (StorageV2)	2	1	Standard D4as_v4
< 6.37	1,000–2,000	SSD Premium	3	1	Standard D4as_v4
< 6.37	2,000–3,000	SSD Premium	5	1	Standard D4as_v4
< 6.37	3,000–4,000	SSD Premium	6	1	Standard D4as_v4
Approx.10	< 1,000	HDD Standard (StorageV2)	3	1	Standard D4as_v4
Approx.10	1,000–2,500	SSD Premium	6	1	Standard D4as_v4

RECORDING FILE SIZE MB/ HOUR	NUMBER OF RECORDED SESSIONS PER DAY	FILE SHARE TYPE	FILE SHARE QUOTA (TB)	SESSION RECORDING SERVER QUANTITY	SESSION RECORDING SERVER SIZE
Approx.10	2,500–4,000	SSD Premium	10	2	Standard D4as_v4

The file share quota is calculated based on eight hours per day, 23 working days per month, and a one-month retention period for each recording file.

2. Add the Azure file share credentials to the host where you installed the Session Recording server.

   a. Start a command prompt as an administrator and change the drive to the **<Session Recording server installation path\>\Bin** folder.

      By default, the Session Recording server is installed in `C:\Program Files\Citrix\SessionRecording\Server`.

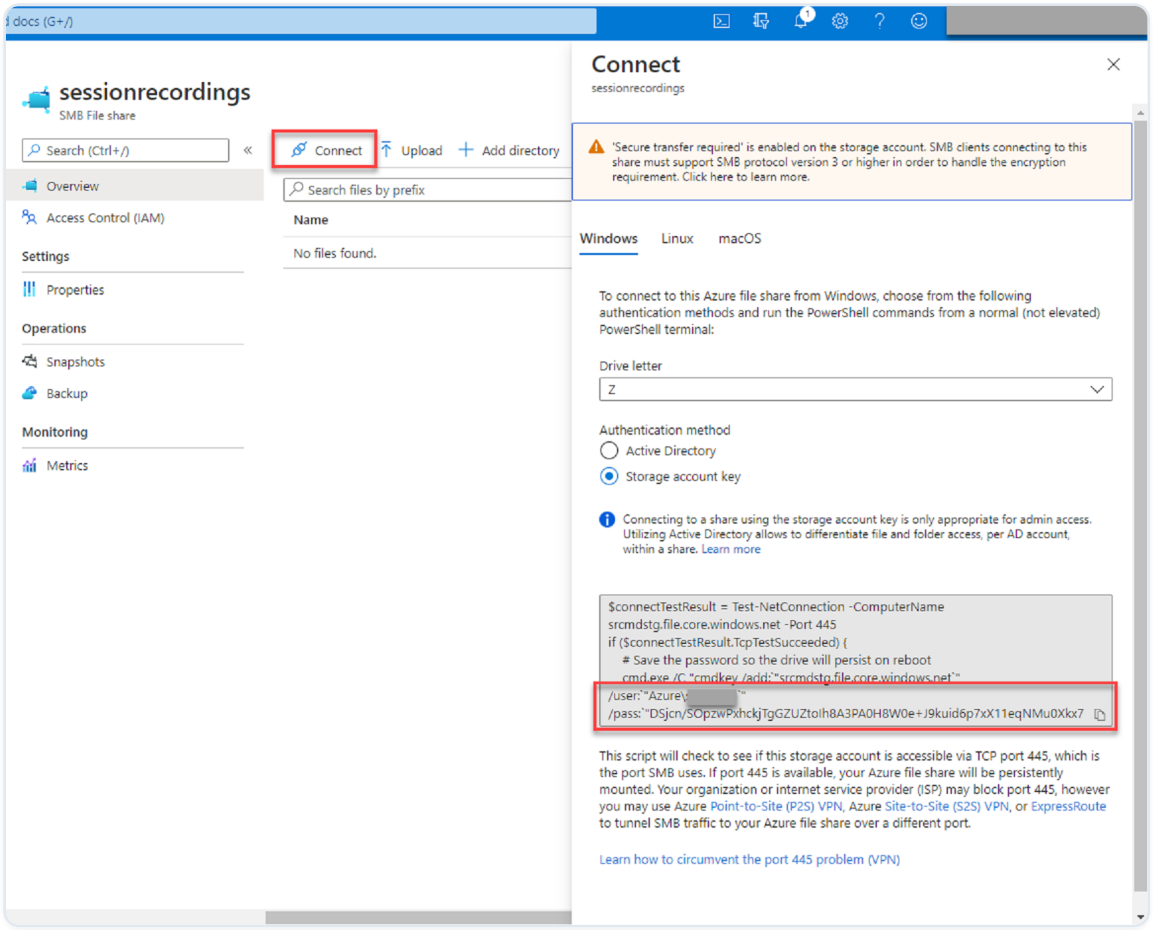
   b. Run the **SsRecUtils.exe -AddAzureFiles <storageAccountName\> <fileShareName\> <accesskey\>** command.

      Where,

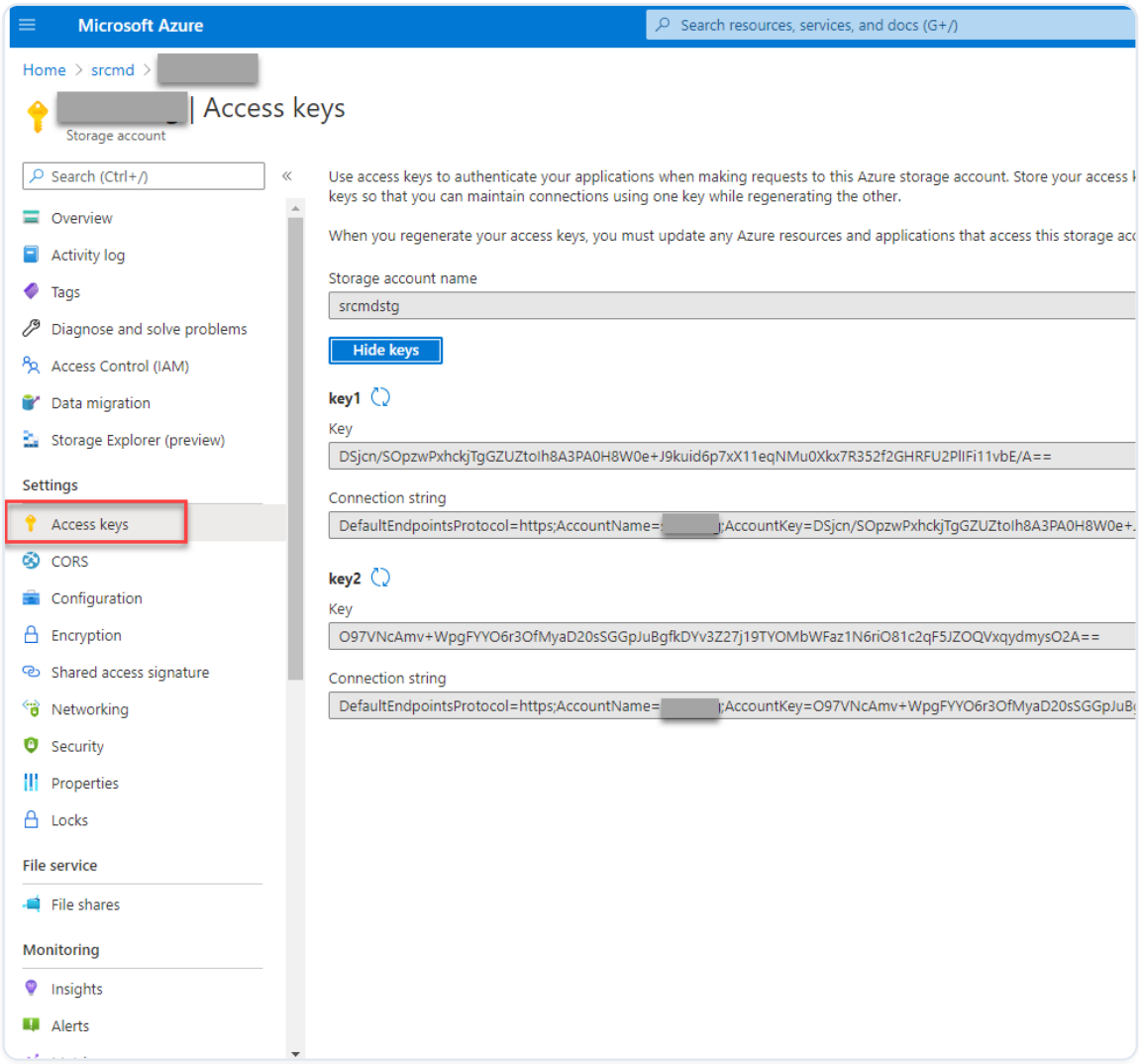
      - **<storageaccountname\>** is the name of your storage account in Azure.
      - **<filessharename\>** is the name of the file share contained within your storage account.
      - **<accesskey\>** is your storage account key that can be used to access the file share.

      There are two ways to obtain your storage account key:

      - You can obtain your storage account key from the connection string that appears when you click the **Connect** icon in your file share page.



- You can also obtain your storage account key by clicking **Access keys** in the left navigation of your storage account page.



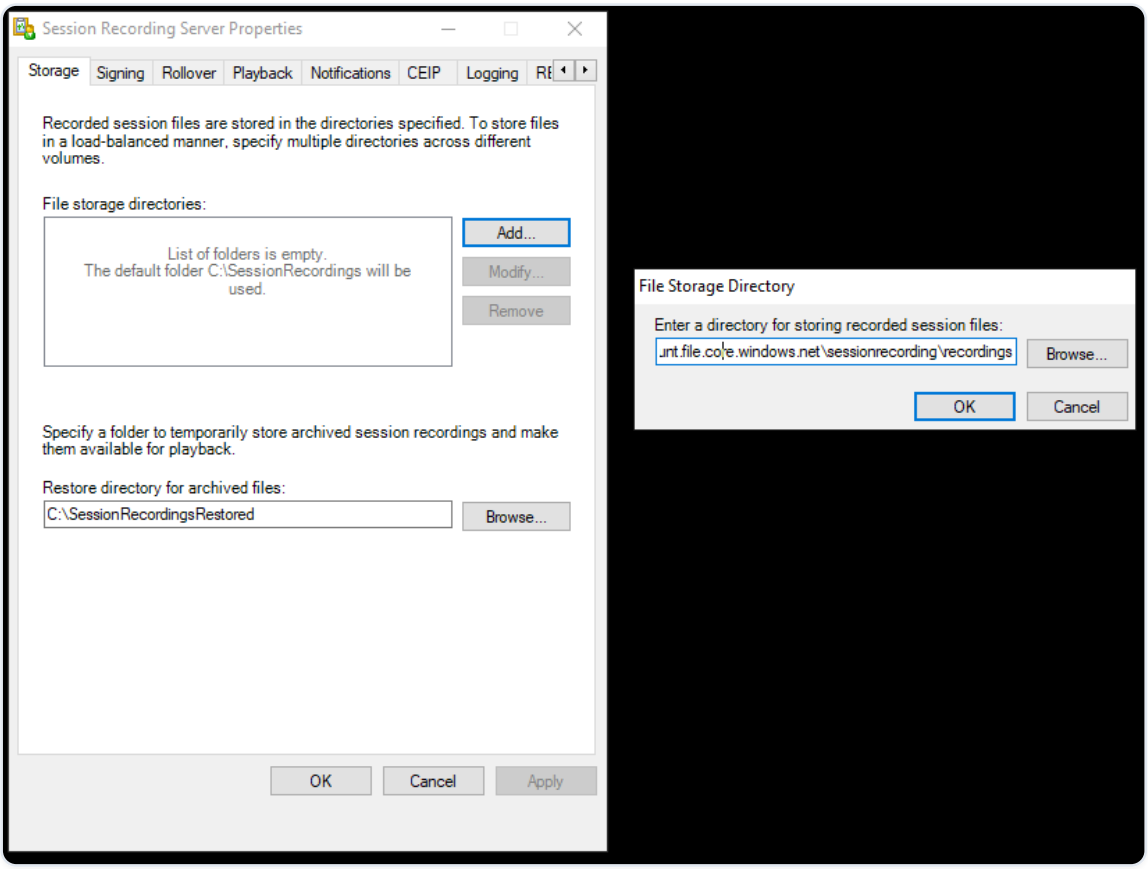
c. Mount the Azure file share to the host where you installed the Session Recording server.

   i. Open **Session Recording Server Properties**.

   ii. Click **Add** on the **Storage** tab.

   iii. Enter the UNC path in the format of **\\\\<storageaccountname\>.file.core.windows.net\\\<filessharename>\\<subfolder\>**.

   Specify a subfolder under the file share to store your recording files. The Session Recording server then automatically creates the subfolder for you.

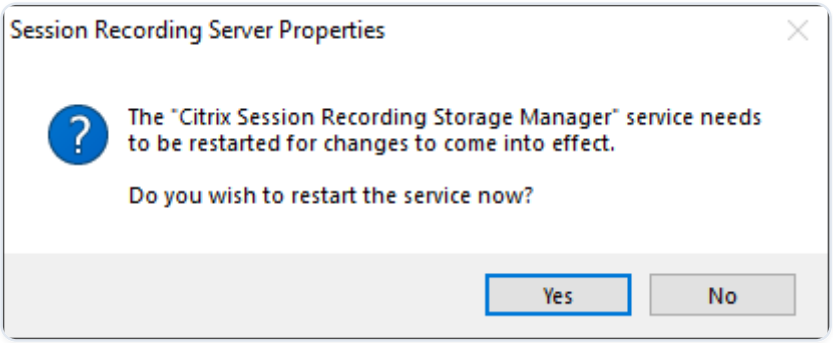


iv. Click **OK** in the **File Storage Directory** dialog box.

v. Click **Apply** in the **Session Recording Server Properties** window.

vi. Click **OK** after **Apply** becomes grayed out.

vii. Click **Yes** when you are prompted to restart the Session Recording Storage Manager service.

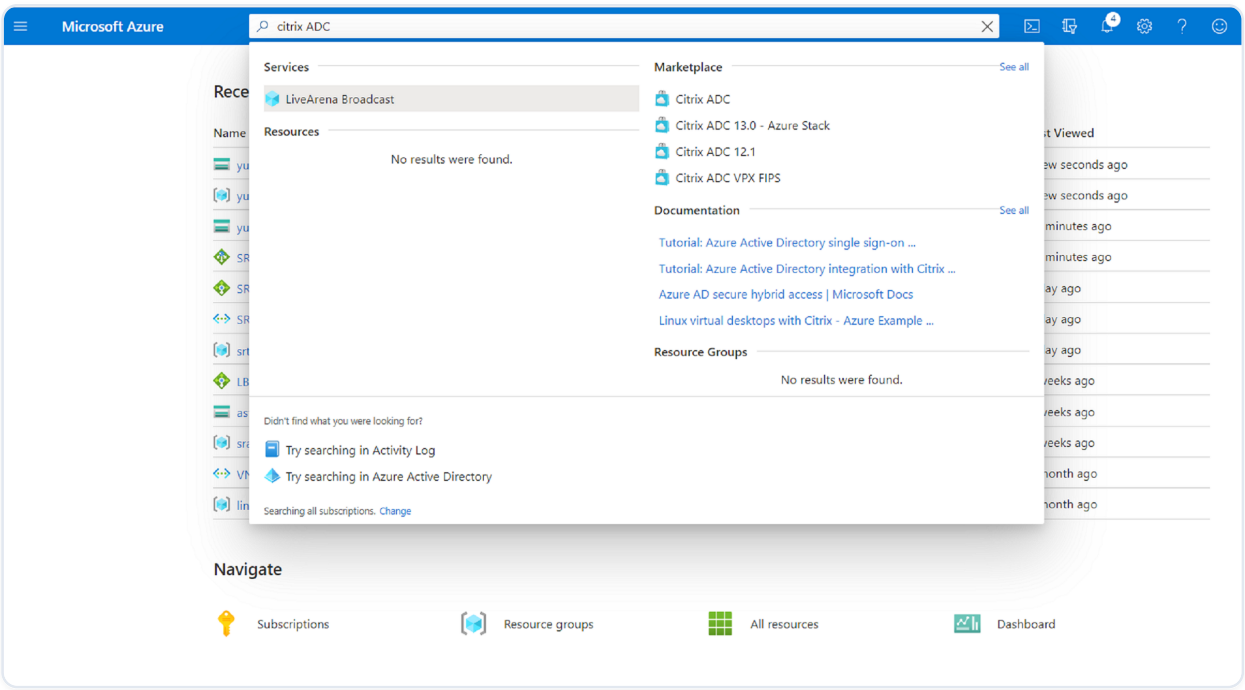


Step 7: Add a load balancer

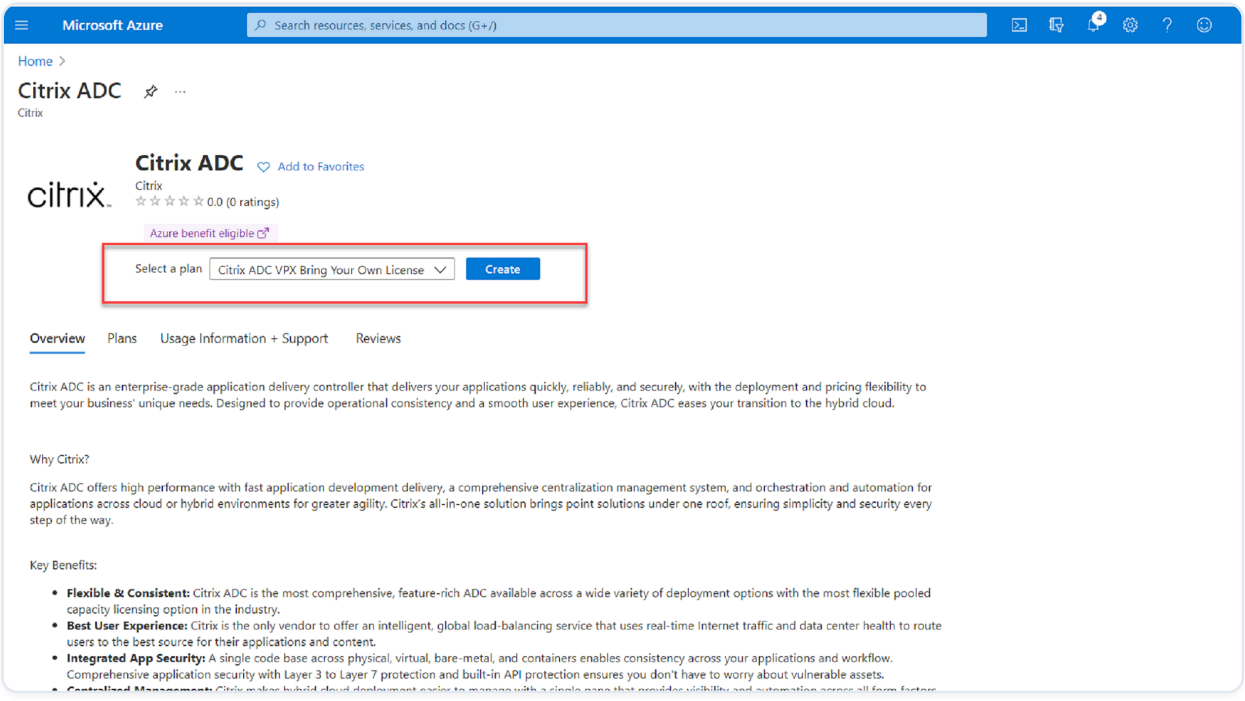
If there is more than one Session Recording server, we recommend you add a load balancer in front of them. Azure offers many options to load-balance traffic requests. This section walks you through the process of creating Citrix ADC, Azure Load Balancer, and Azure Application Gateway in Azure.

Option 1: Create a Citrix ADC VPX instance in Azure

1. In the Azure portal, type Citrix ADC in the search box.

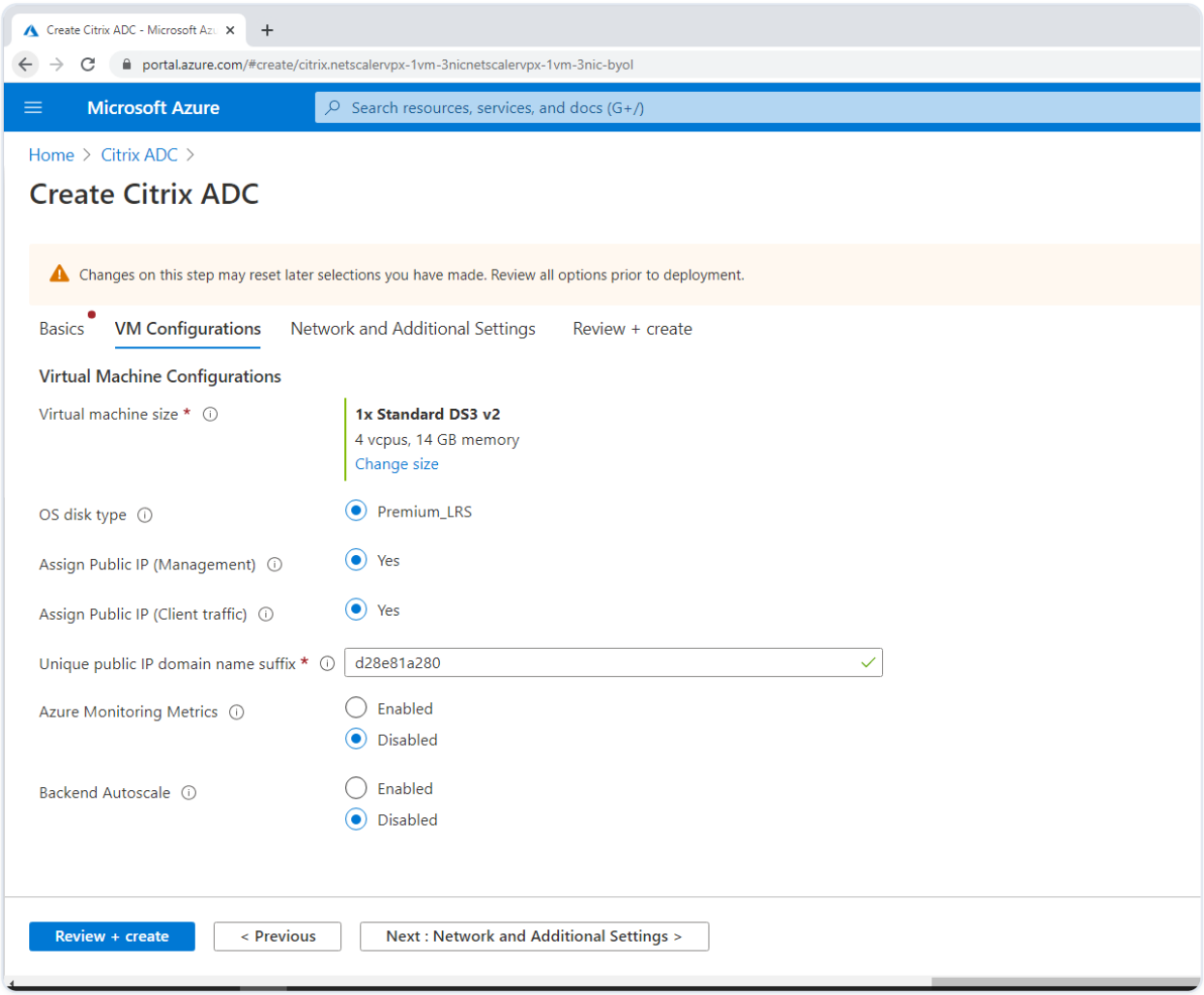


2. Choose the **Citrix ADC VPX Bring Your Own License** plan and then click **Create**.



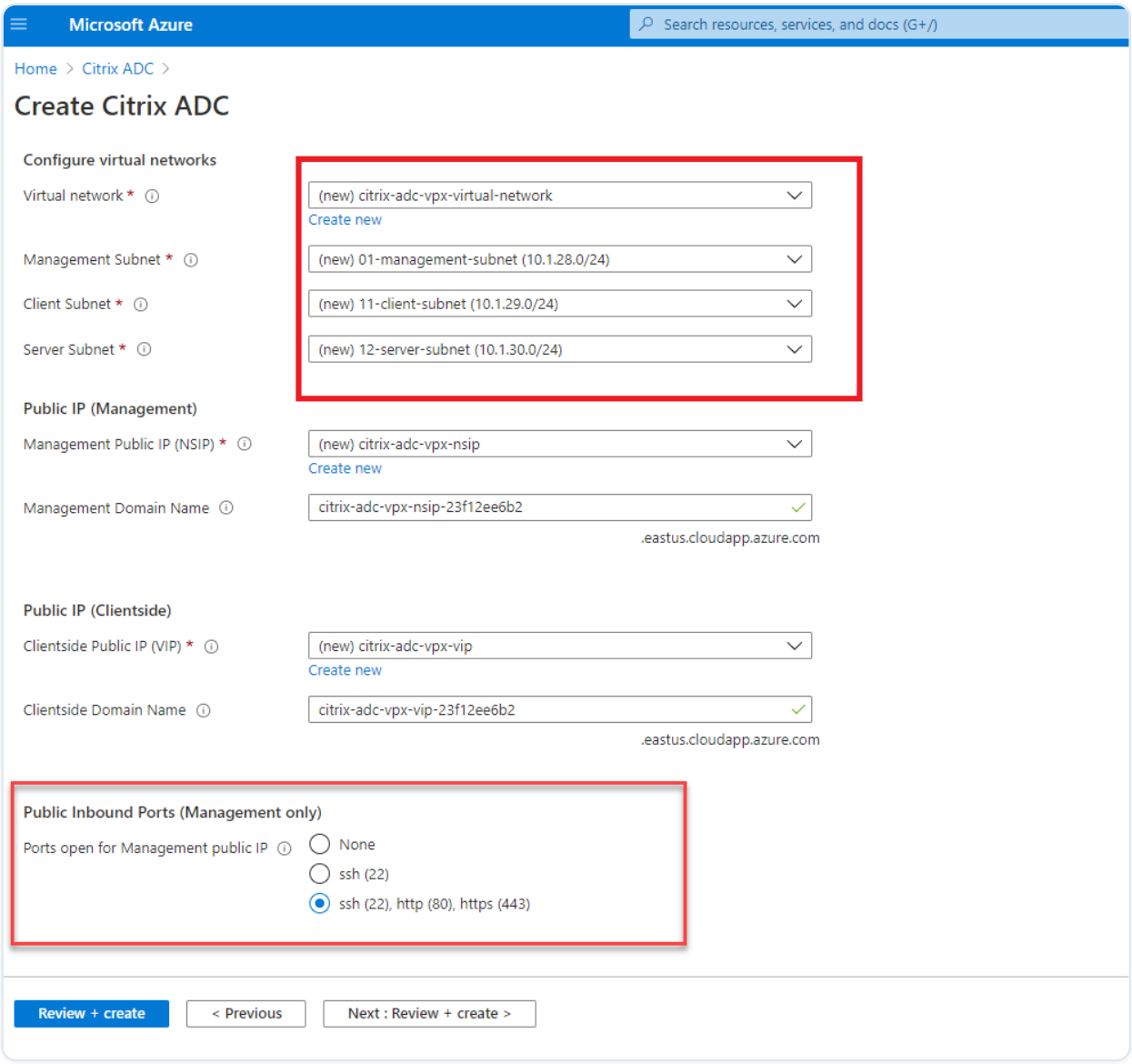
3. Select or create a resource group and set the other settings on the **Basics** tab.

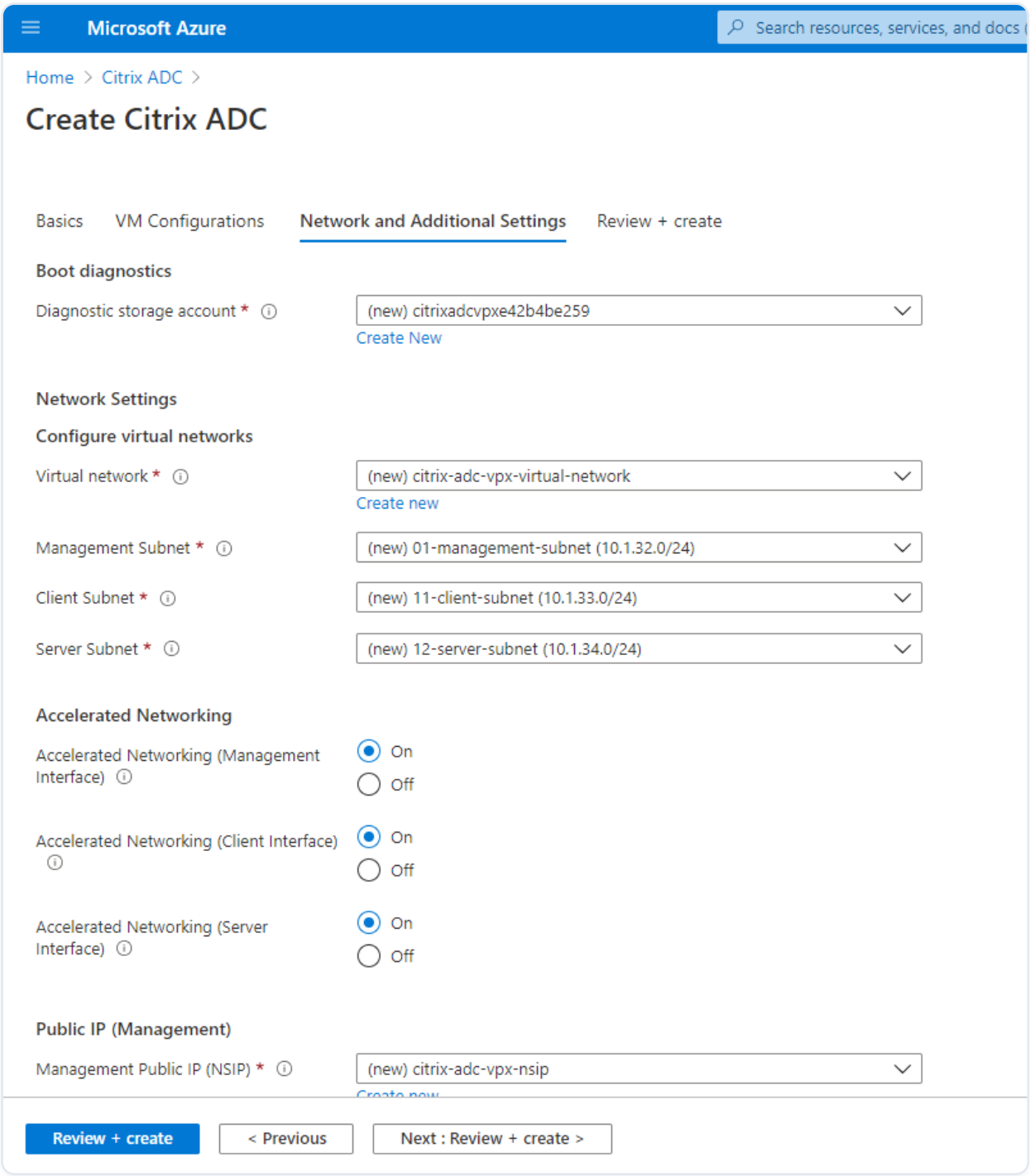
4. Set VM configurations.



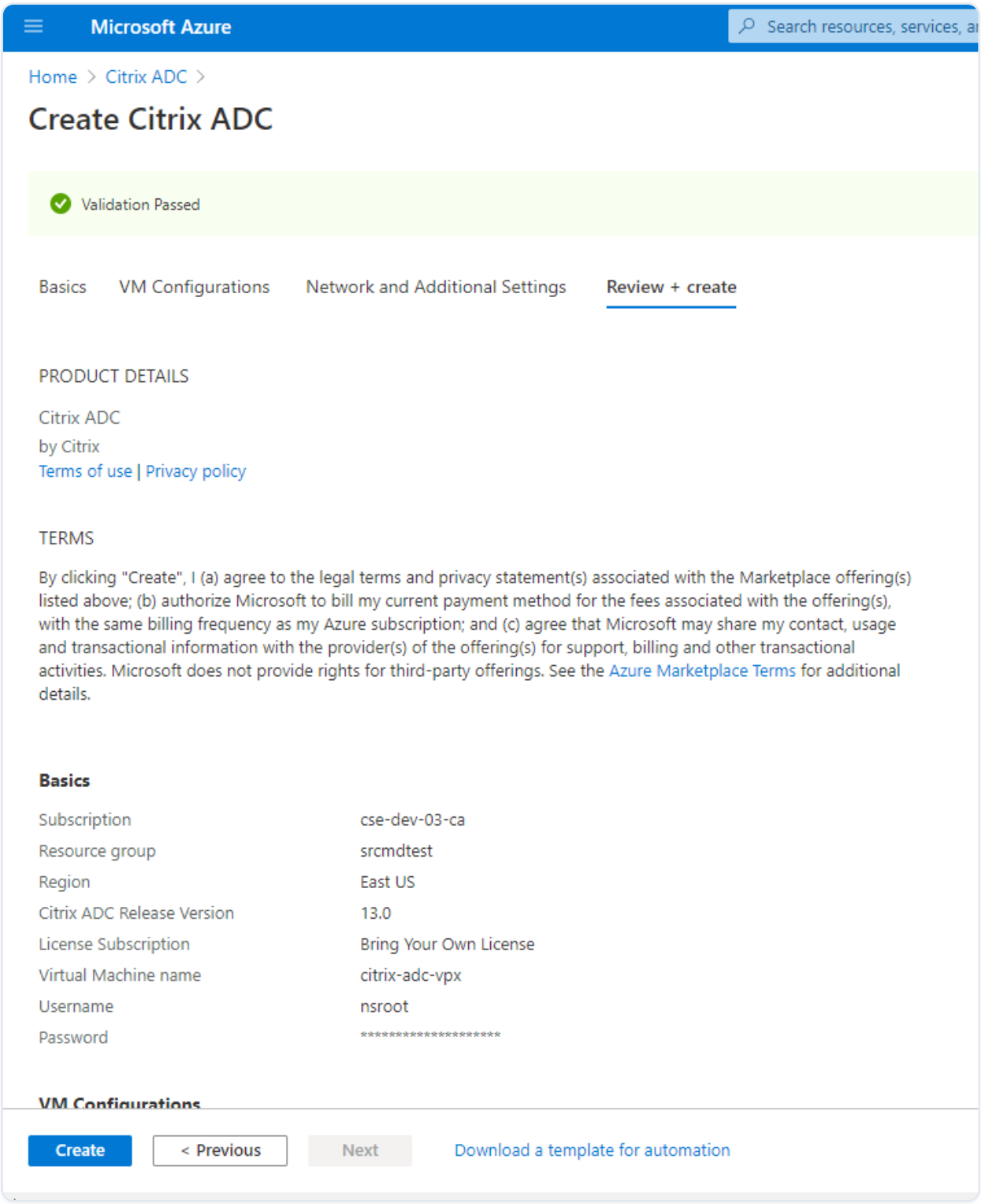
5. Check and modify network settings if necessary. Choose **ssh (22), http (80), https (443)** for public inbound ports.

   A virtual network is automatically created. If you already have a Session Recording environment installed, you can use its virtual network and server subnet settings.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Citrix ADC >
Create Citrix ADC
Configure virtual networks
Virtual network *
(new) citrix-adc-vpx-virtual-network
Create new
Management Subnet *
(new) 01-management-subnet (10.1.28.0/24)
Client Subnet *
(new) 11-client-subnet (10.1.29.0/24)
Server Subnet *
(new) 12-server-subnet (10.1.30.0/24)
Public IP (Management)
Management Public IP (NSIP) *
(new) citrix-adc-vpx-nsip
Create new
Management Domain Name
citrix-adc-vpx-nsip-23f12ee6b2
.eastus.cloudapp.azure.com
Public IP (Clientside)
Clientside Public IP (VIP) *
(new) citrix-adc-vpx-vip
Create new
Clientside Domain Name
citrix-adc-vpx-vip-23f12ee6b2
.eastus.cloudapp.azure.com
Public Inbound Ports (Management only)
Ports open for Management public IP
None
ssh (22)
ssh (22), http (80), https (443)
Review + create
< Previous
Next : Review + create >



6. Click **Next: Review + create** to create the Citrix ADC VPX instance and wait for the deployment to complete.

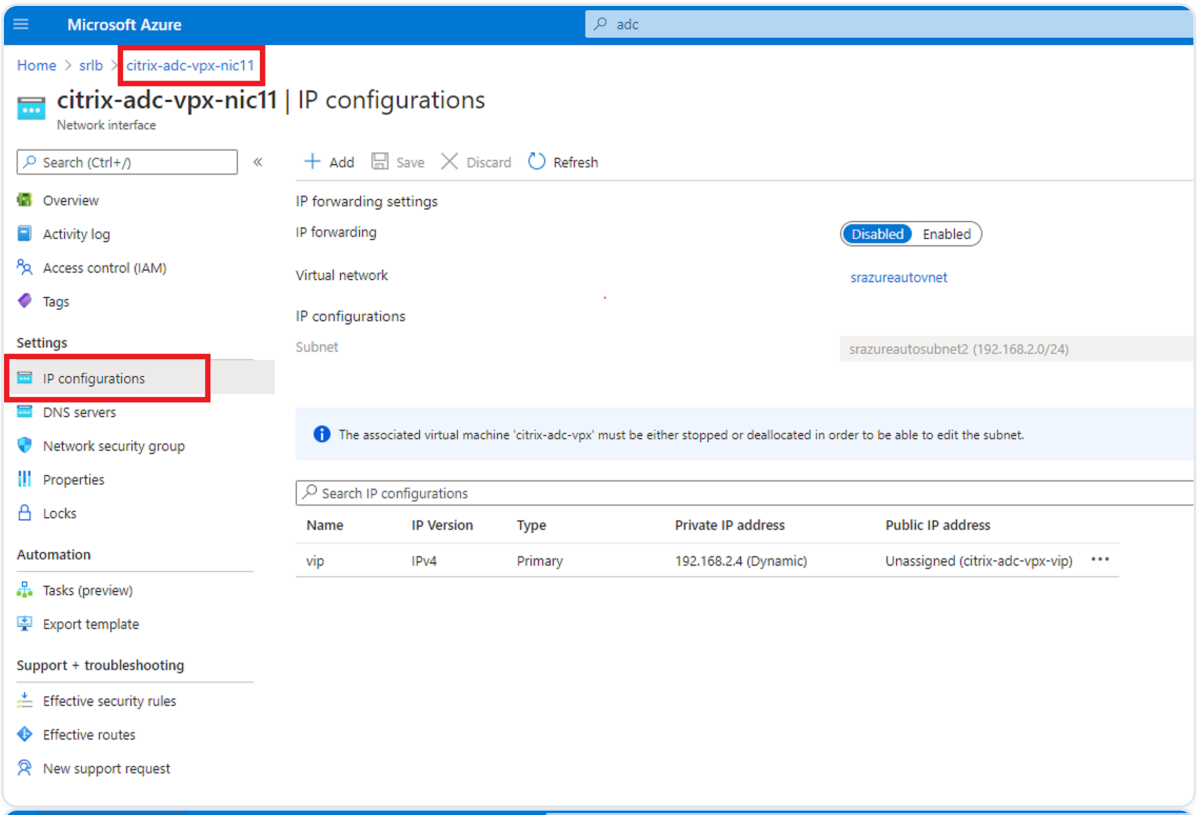


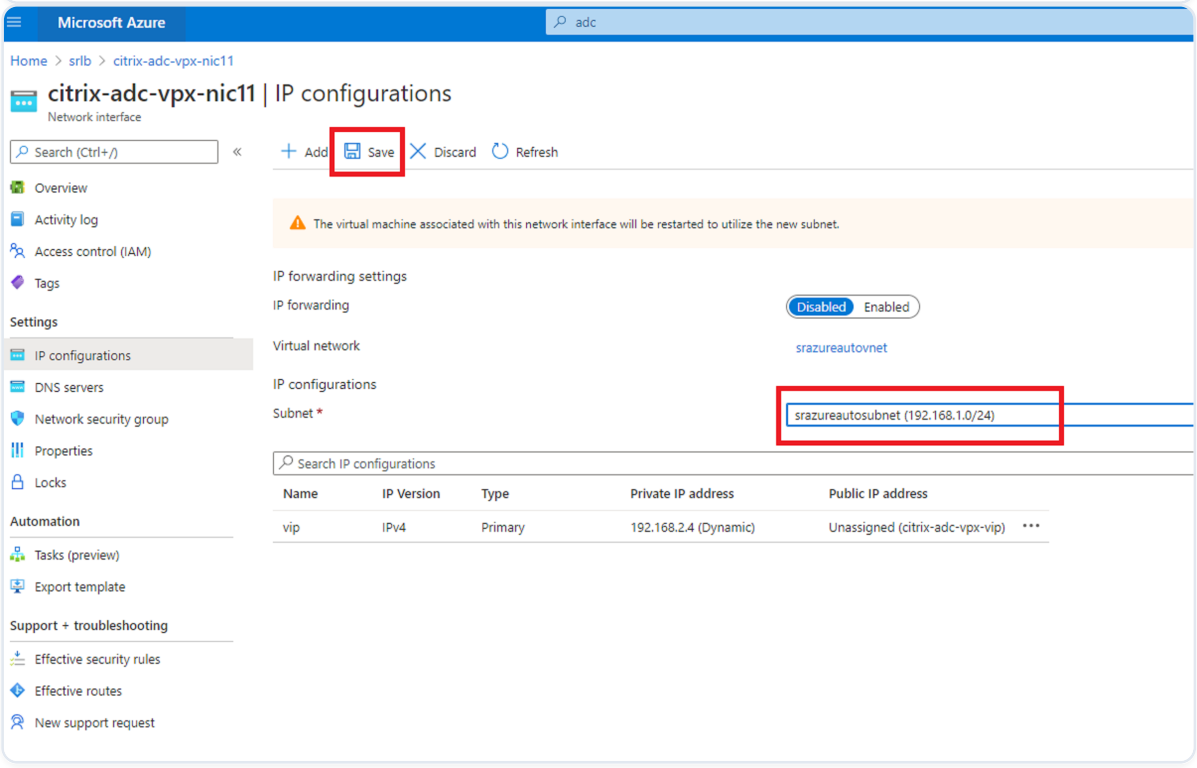
7. Set the subnet IP (SNIP) address and the Citrix ADC VIP address to be on the same subnet.

   The SNIP address and the VIP address must be on the same subnet. In this example, we set the VIP address to be on the subnet of the SNIP address.

   a. Stop the **citrix-adc-vpx** virtual machine.

   b. Change the subnet of the VIP address.

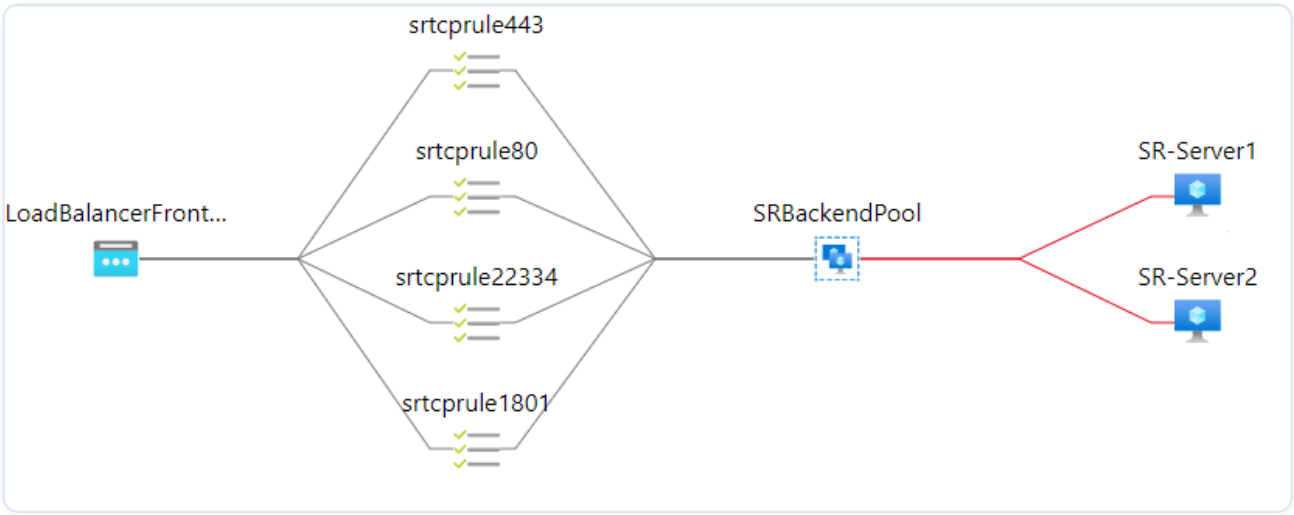




c. Start the **citrix-adc-vpx** virtual machine

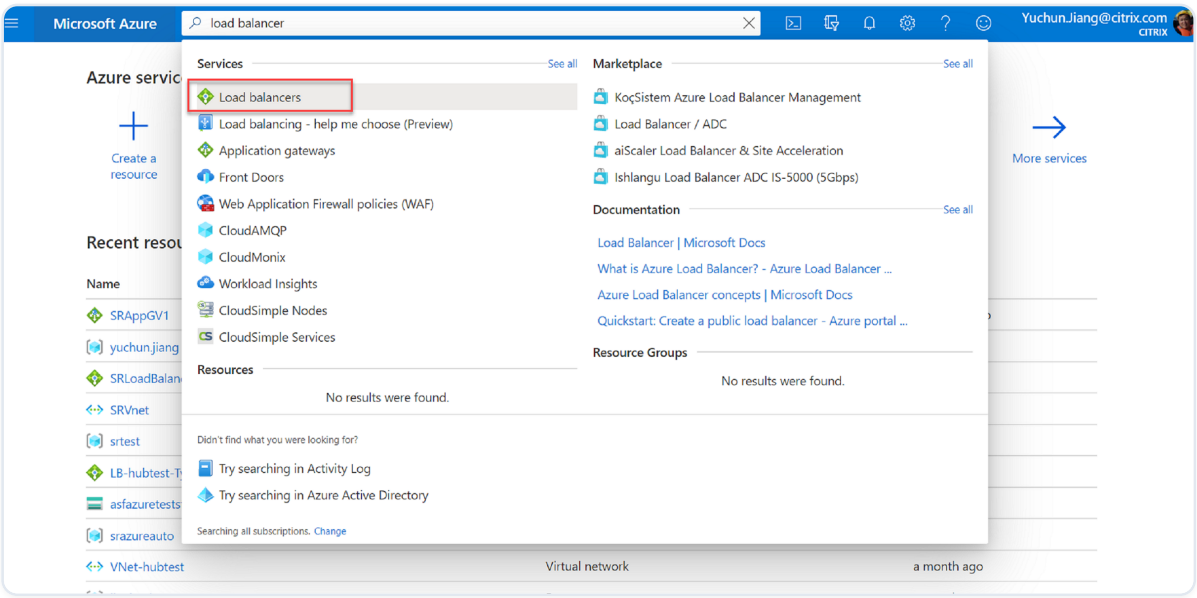
Option 2: Create an Azure load balancer

Azure Load Balancer is a TCP passthrough service. The following diagram shows load balancing through TCP passthrough.



1. Create an Azure load balancer.

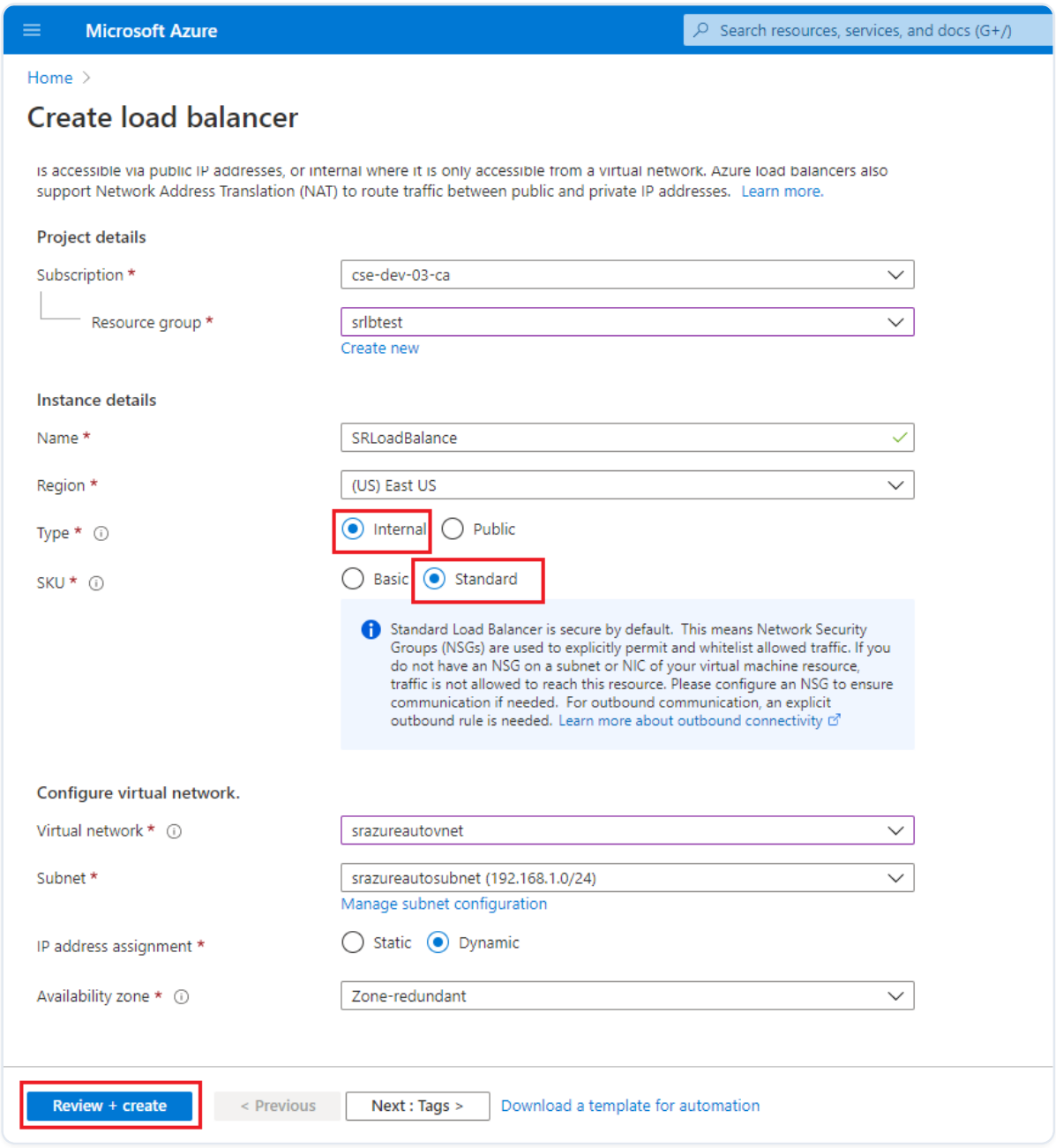
   a. Search in the Azure portal and select **Load Balancers** from the **Marketplace**.



   On the **Basics** tab of the **Create load balancer** page, configure settings as described in the following table:

SETTING	VALUE
Subscription	Select your subscription.
Resource group	For example, select **srlbtest** created earlier.
Name	Enter **SRLoadBalance**.
Region	Select **(US) East US**.

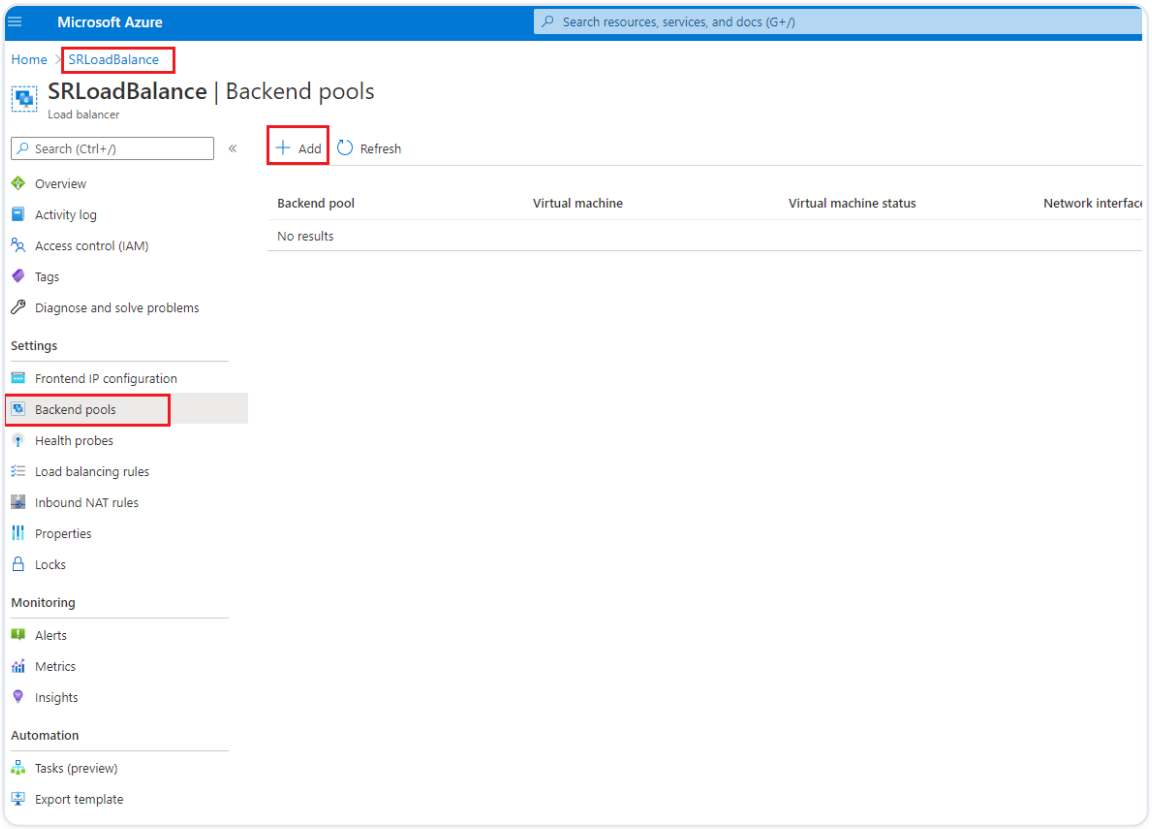
SETTING	VALUE
Type	Select **Internal**.
SKU	Select **Standard**
Virtual network	For example, select **srazureautovnet** created earlier.
Subnet	For example, select **srazureautosubnet** created earlier.
IP address assignment	Select **Dynamic**.
Availability zone	Select **Zone-redundant**.



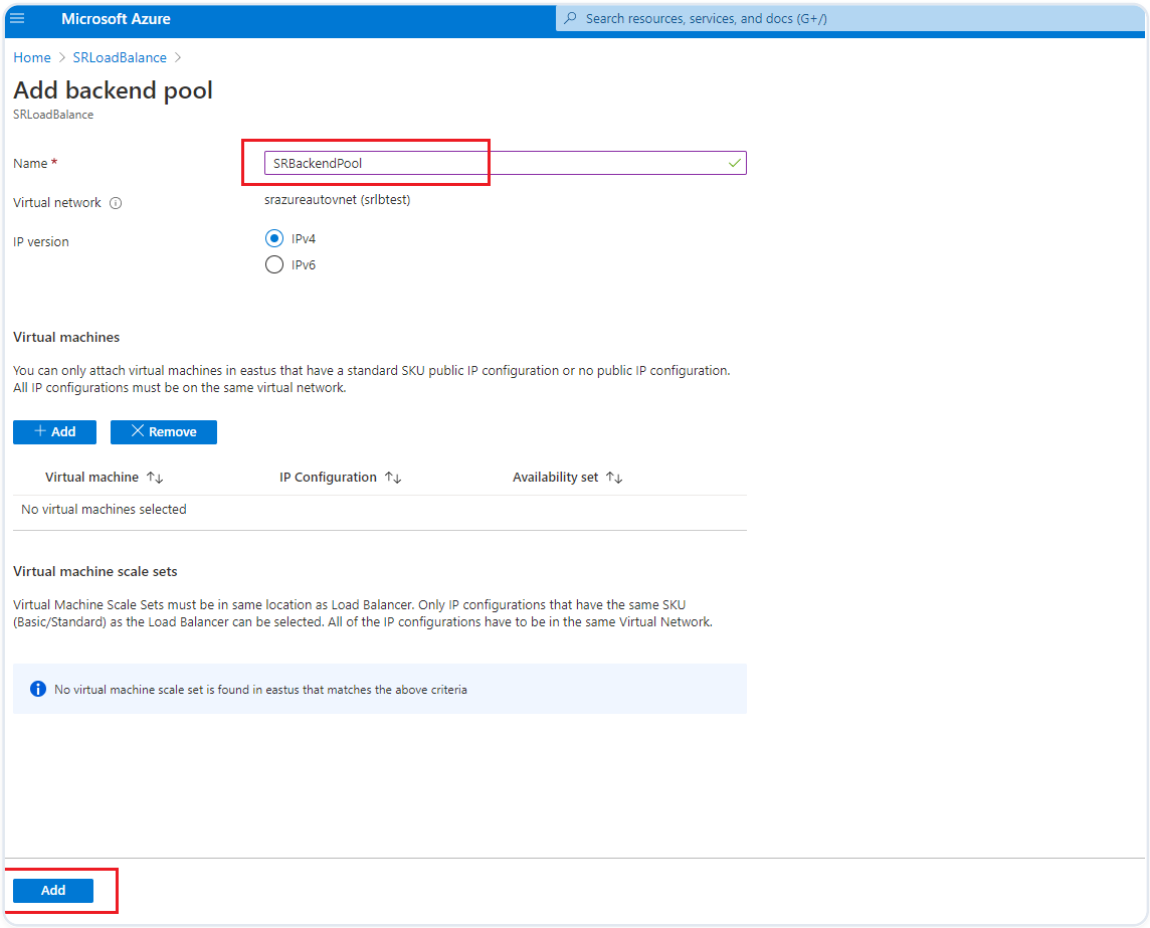
b. Add load balancer resources, including a back-end pool, health probes, and load balancing rules.

- Add a back-end pool.

  Select the load balancer you created from the resources list and click **Backend pools** in the left navigation. Click **Add** to add a back-end pool.

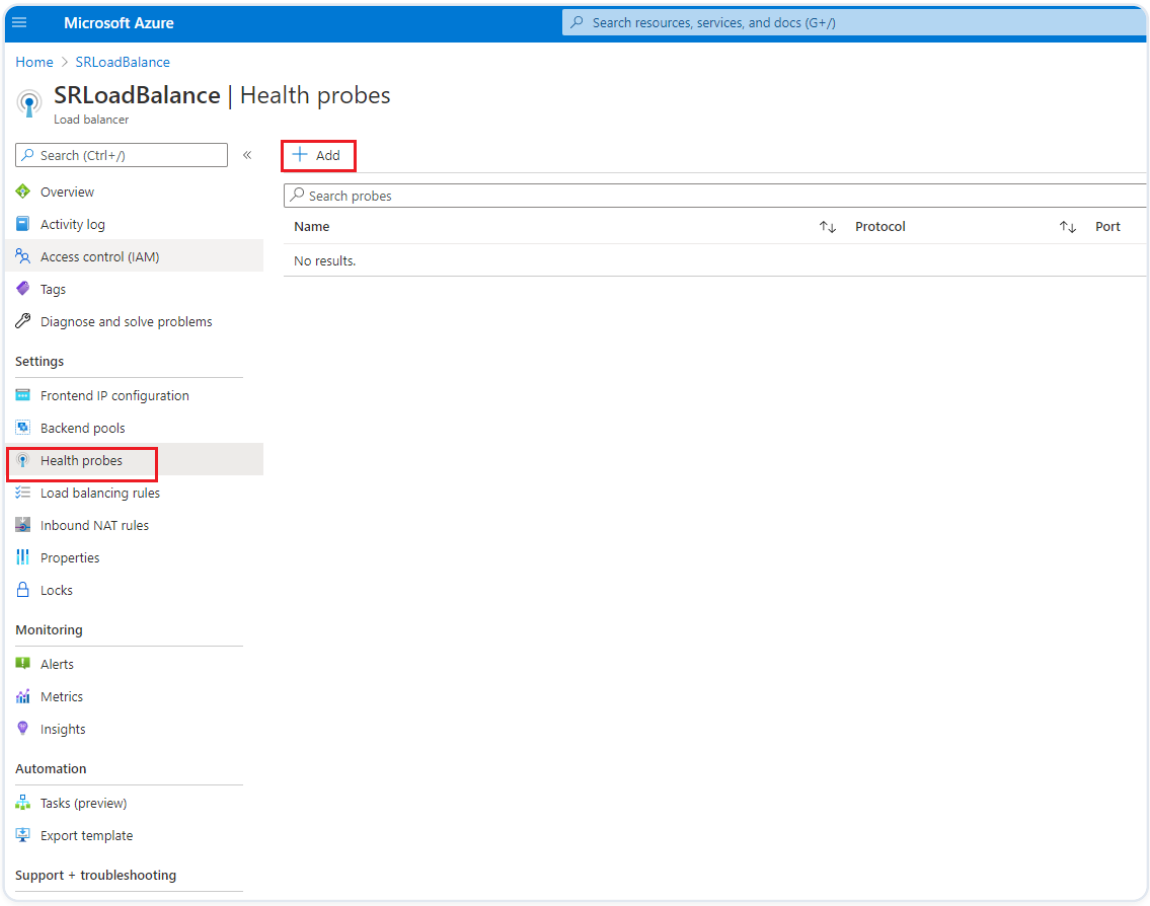


Enter a name for the new back-end pool and then click **Add**.

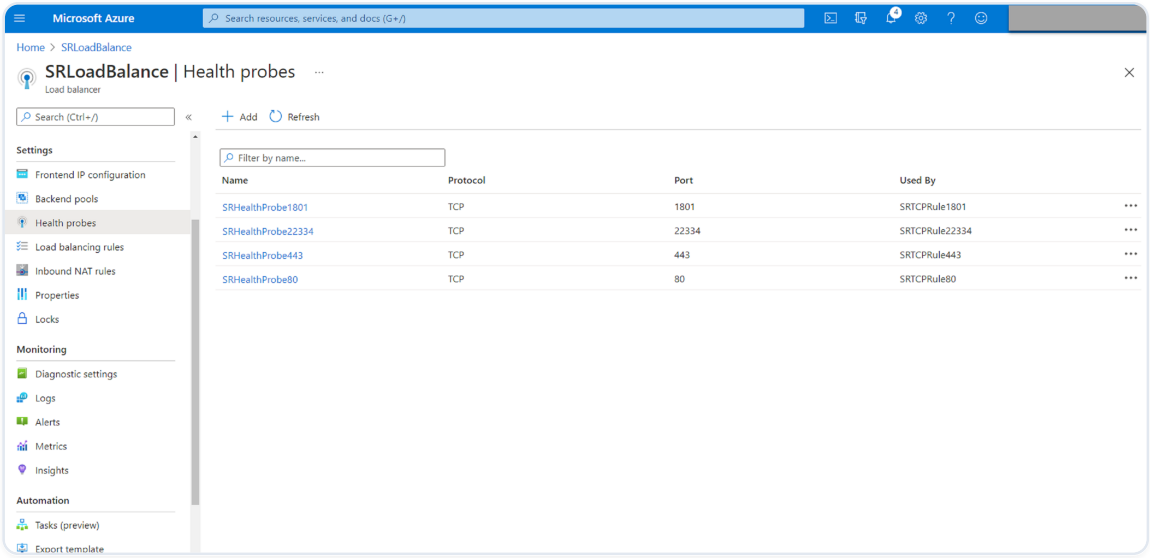


- Add health probes.

Select the load balancer you created from the resources list and then click **Health probes** in the left navigation.



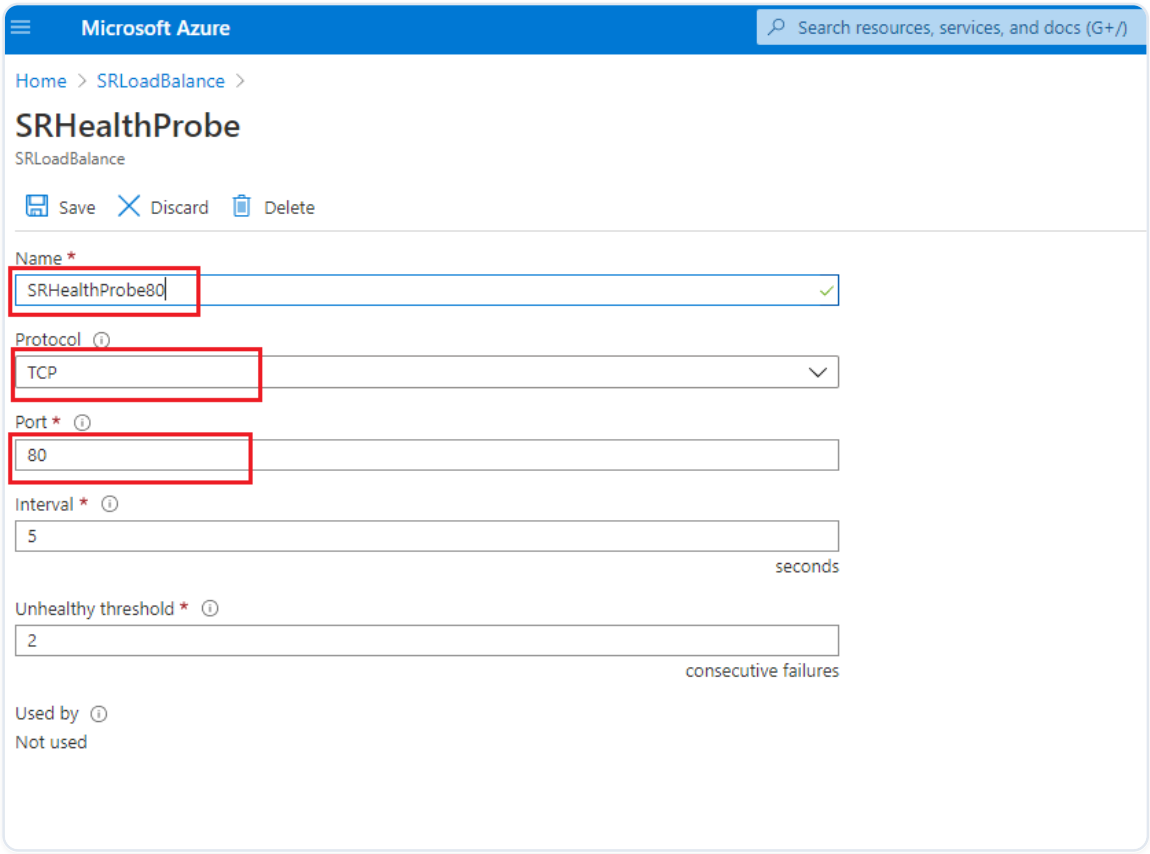
Click **Add** to add health probes on ports 80, 22334, 1801, and 443.



For example, use the following settings to create a health probe on port 80.

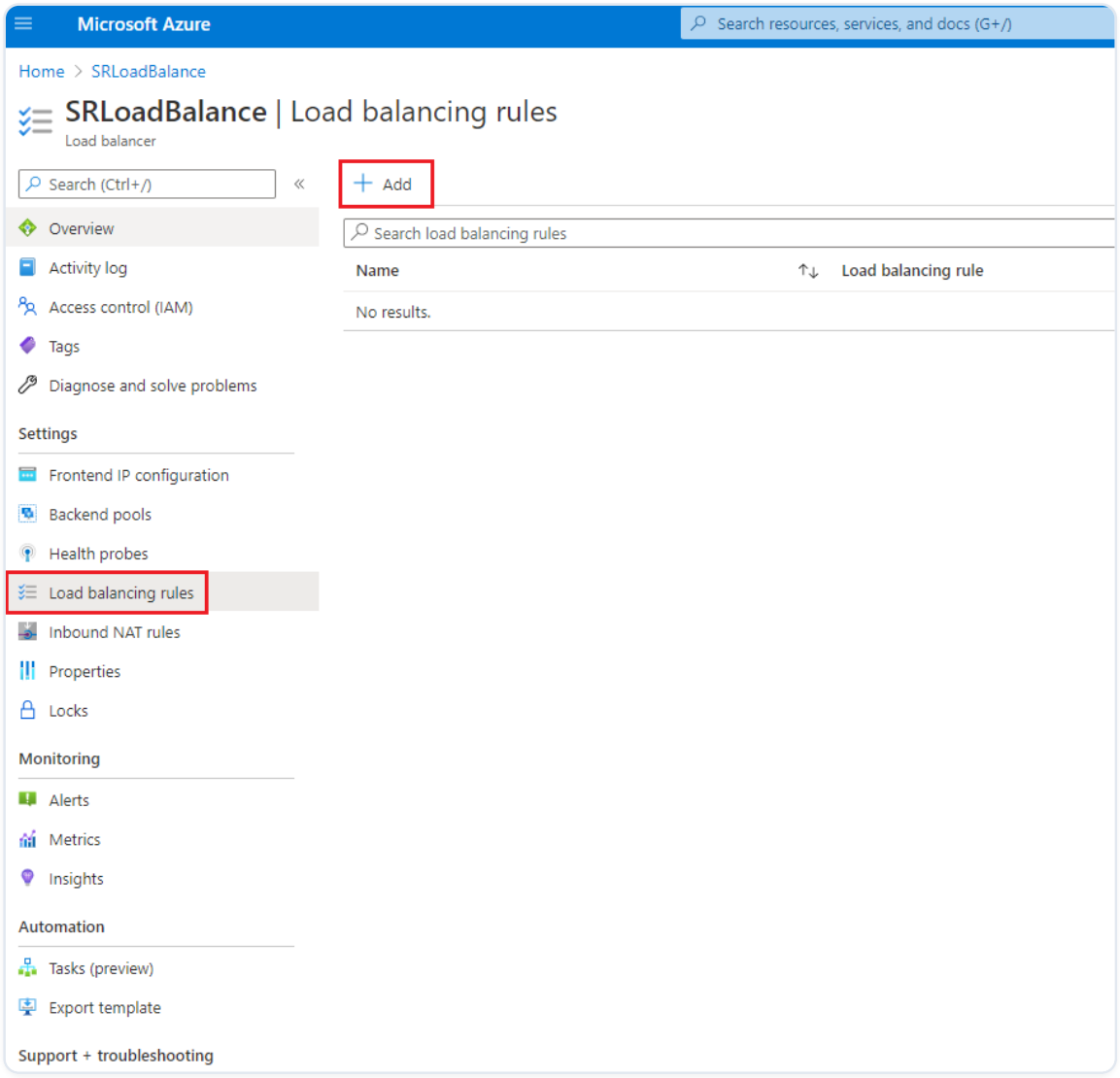
SETTING	VALUE
Name	Enter **SRHealthProbe80**.

SETTING	VALUE
Protocol	Select **TCP**.
Port	Enter **80**.
Interval	5
Unhealthy threshold	Select 2 for the number of unhealthy threshold or consecutive probe failures that must occur before a VM is considered unhealthy.

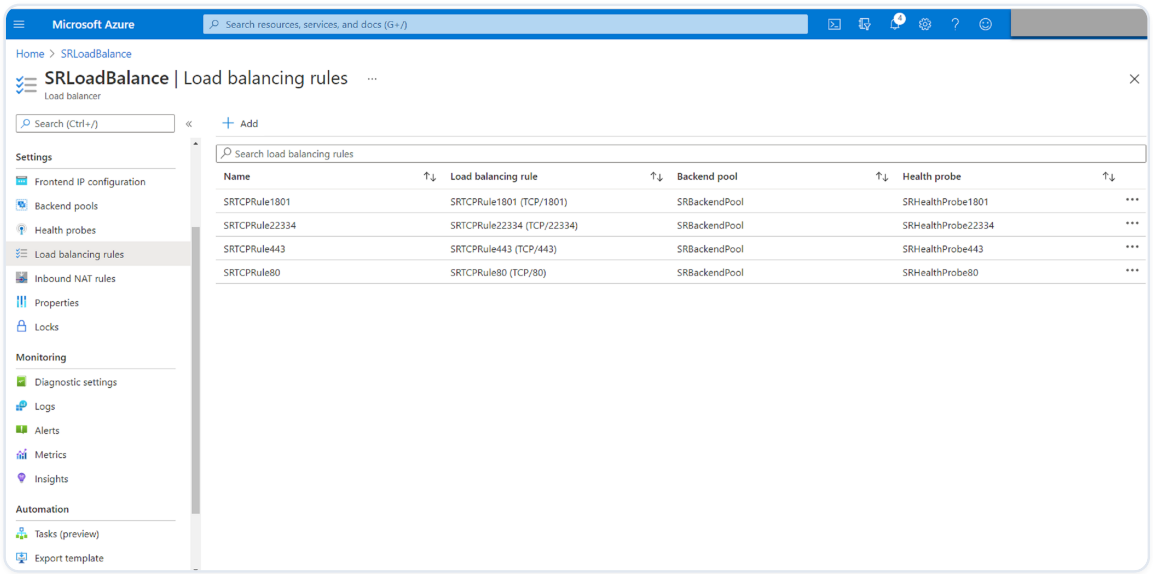


- Add a load balancing rule.

  Select the load balancer you created from the resources list and then click **Load balancing rules** in the left navigation. Click **Add** to add a load balancing rule.

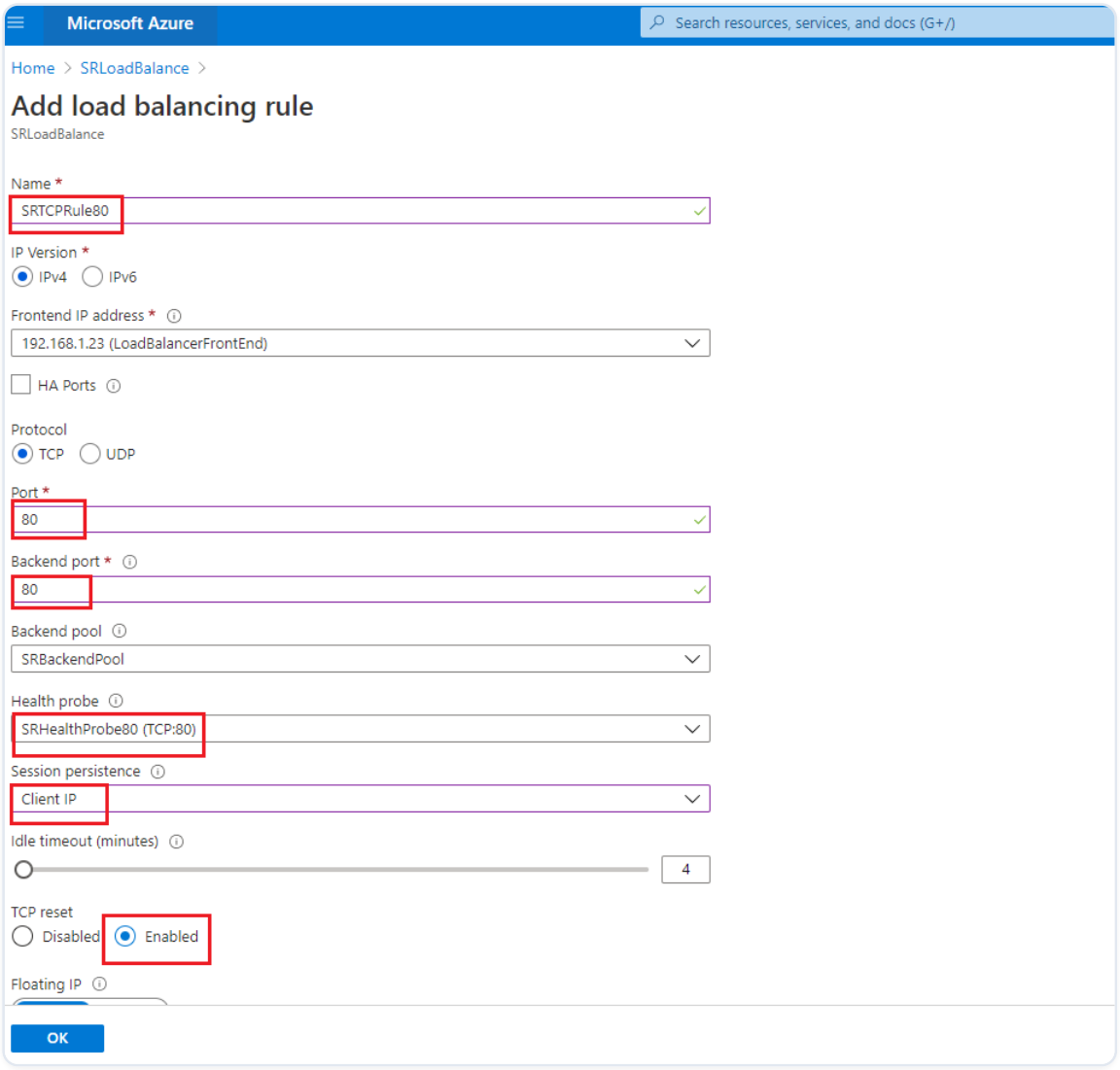


Click **Add** to add load balancing rules for ports 80, 22334, 1801, and 443.

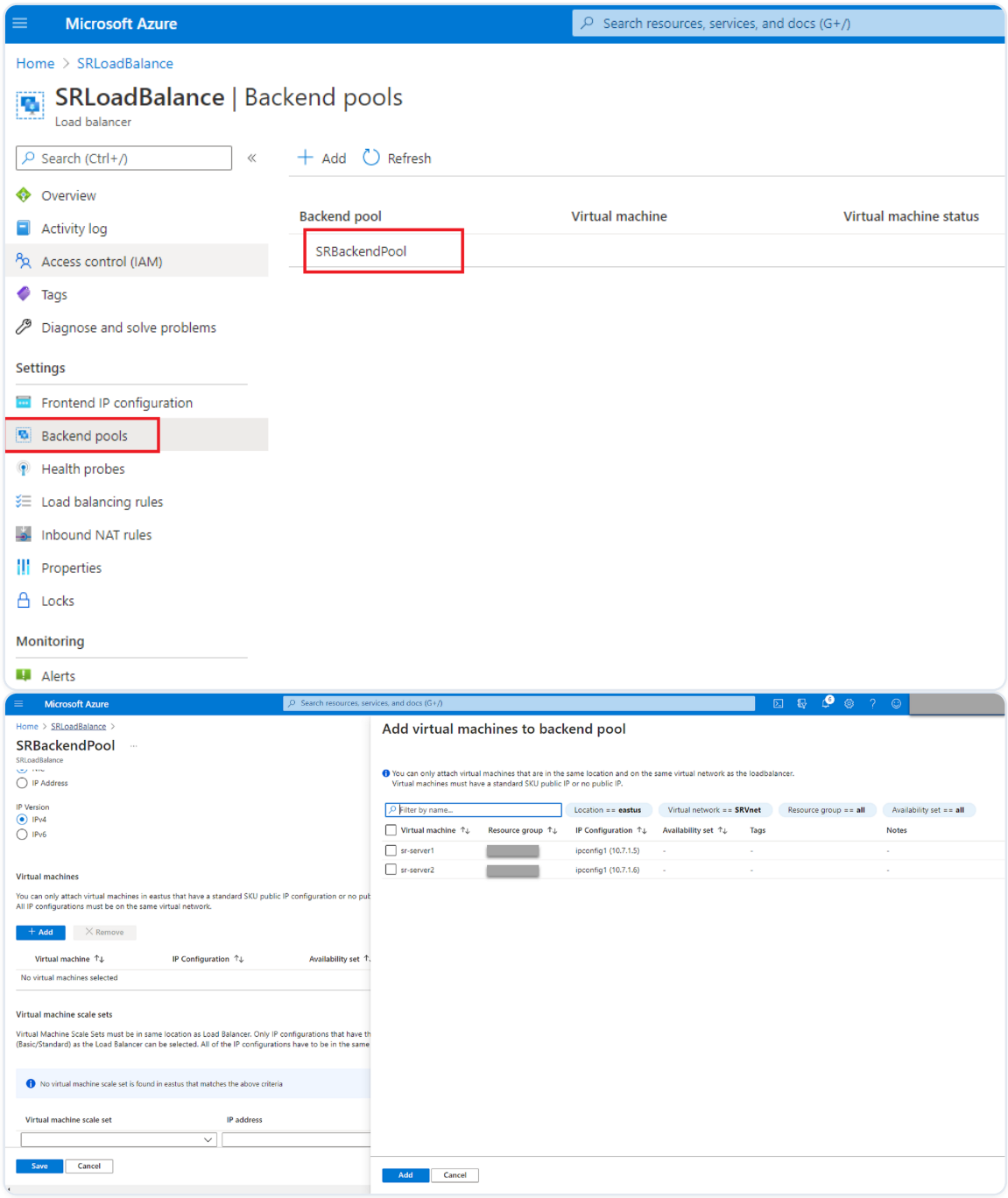


For example, use the following settings to create a load balancing rule for port 80.

SETTING	VALUE
Name	Enter a name, for example, **SRTCPRule80**.
IP Version	Select **IPv4**.
Frontend IP address	Select **LoadBalancerFrontEnd**.
Protocol	Select **TCP**.
Port	Enter **80**.
Backend port	Enter **80**.
Backend pool	Select **SRBackendPool**.
Health probe	Select **SRHealthProbe80**.
Session persistence	Select **Client IP**.
Idle timeout (minutes)	Accept the default setting.
TCP reset	Select **Enabled**.
Outbound source network address translation (SNAT)	Select **(Recommended) Use outbound rules to provide backend pool members access to the internet**.

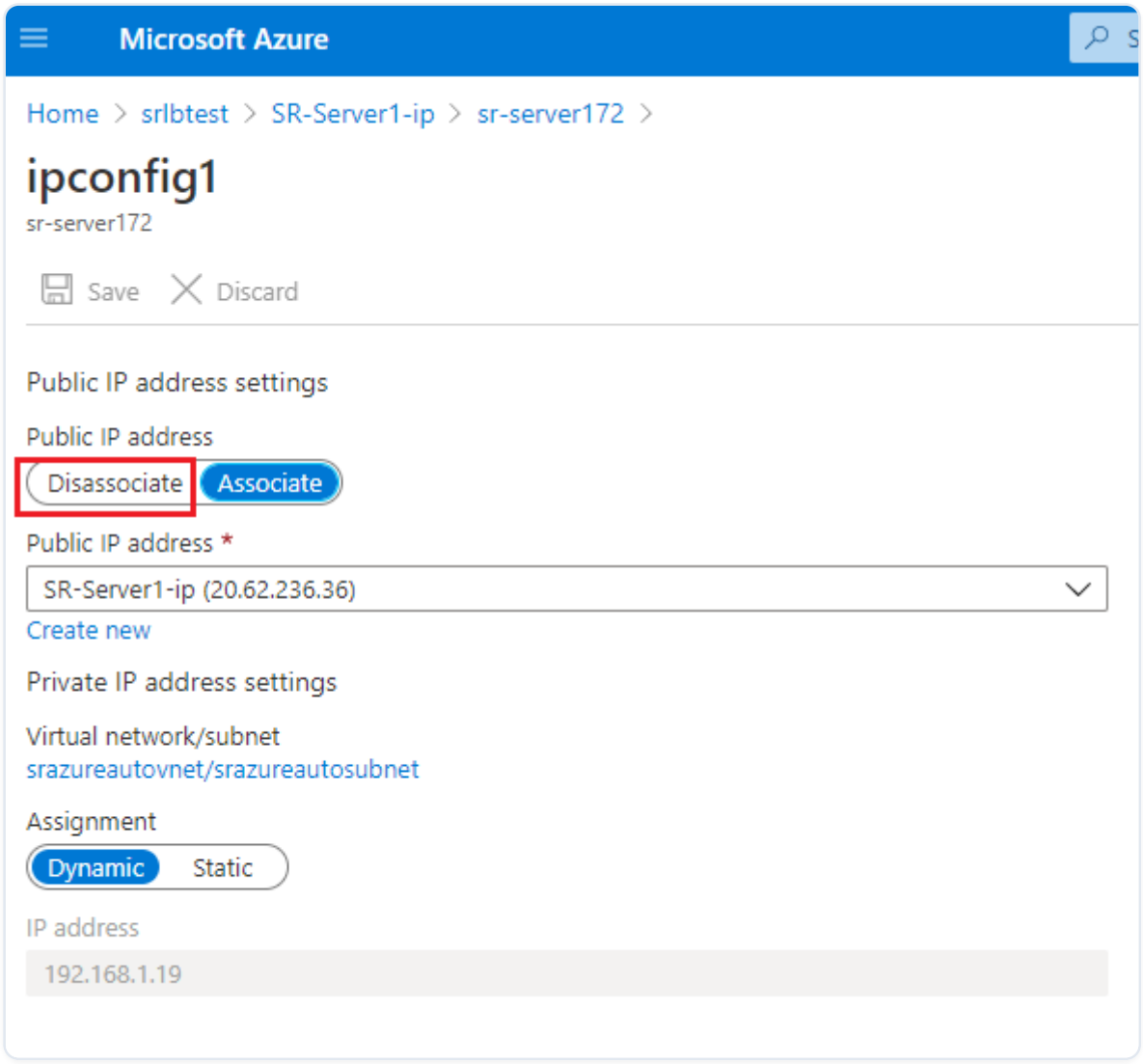


- Add the Azure VMs where the Session Recording server is installed to the back-end pool.



c. Test the Azure load balancer.

If you cannot add a server to the back-end pool and the following error message appears **NetworkInterfaceAndLoadBalancerAreInDifferentAvailabilitySets**, disassociate the public IP address of the server network interface.



Option 3: Create an Azure application gateway

> **Tip:**

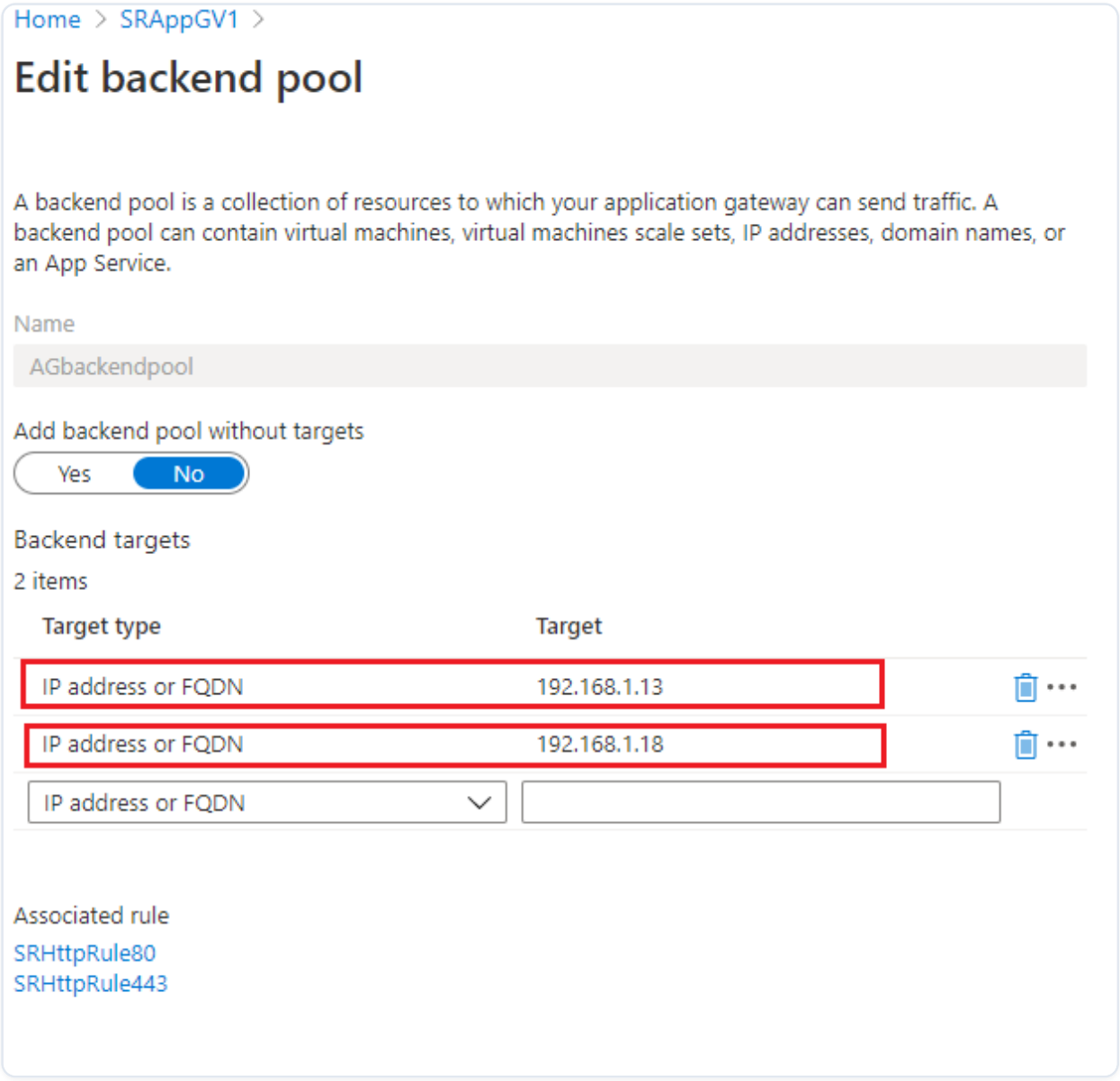
> Application Gateway V2 does not support routing requests through an NTLM-enabled proxy.

1. Create an Azure application gateway.

   Configure the following settings when you create an application gateway.

   - On the **Basics** tab, set **Tier** to **Standard**.
   - On the **Frontends** tab, set **Frontend IP address type** to **Private**. The new application gateway is used as an internal load balancer.

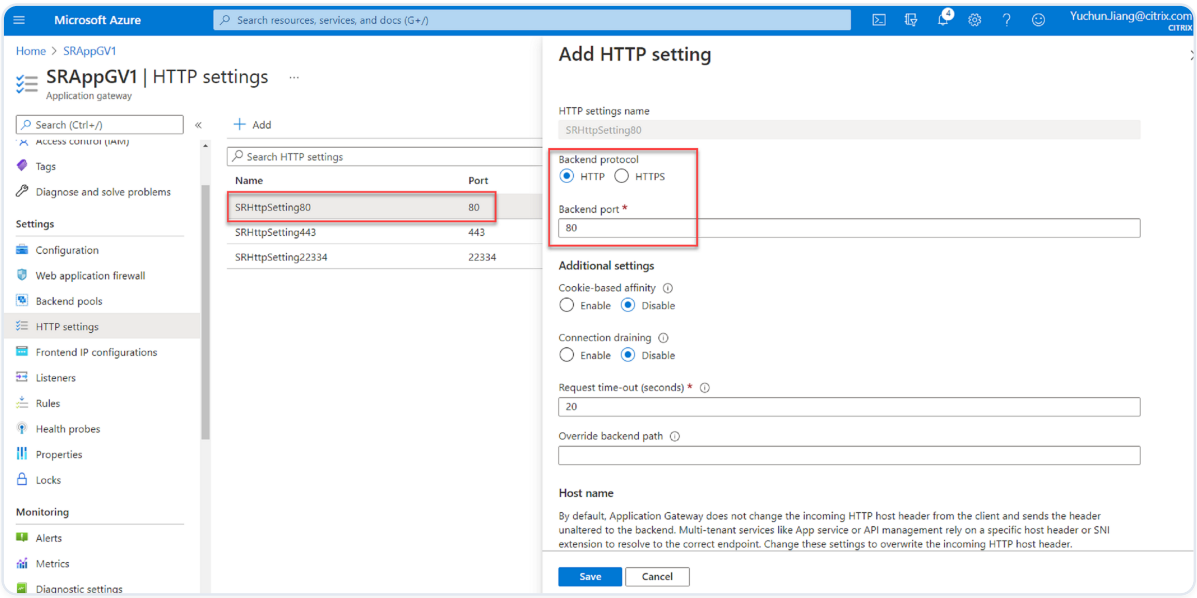
2. Add a back-end pool.



3. Create HTTP settings.

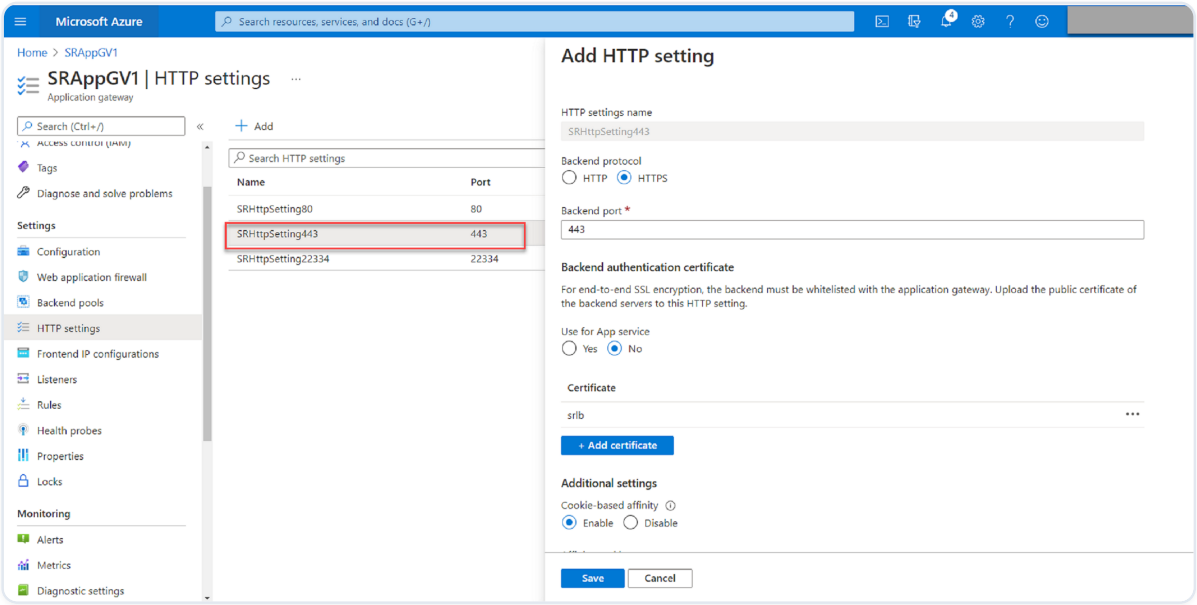
   Azure Application Gateway supports both HTTP and HTTPS for routing requests to back-end servers. Create HTTP settings for ports 80, 443, and 22334.

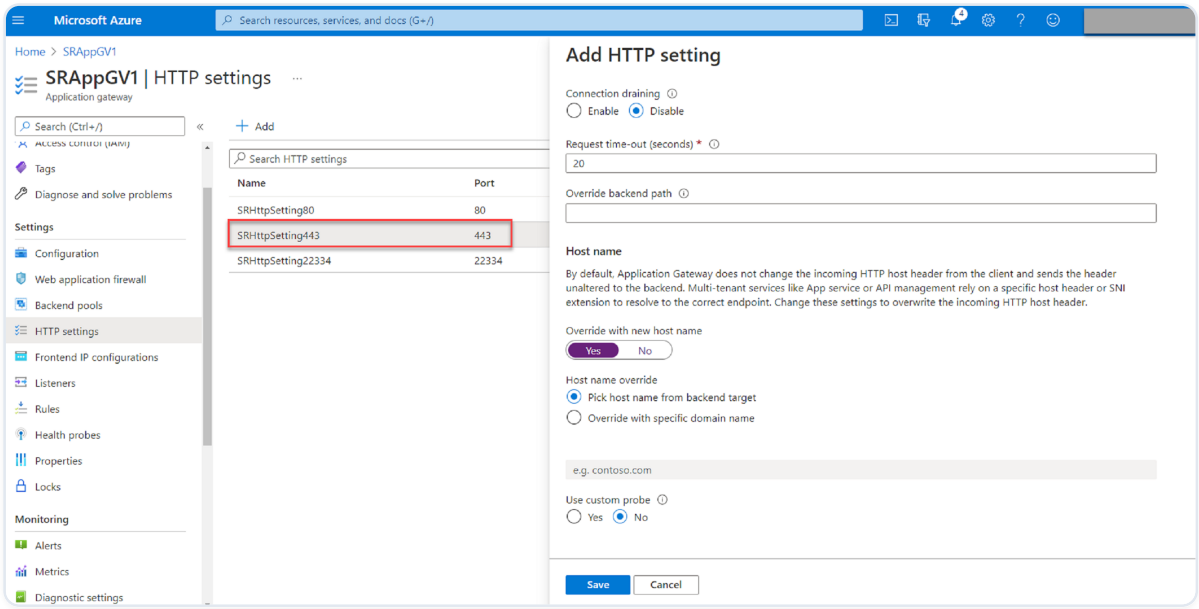
   - HTTP over port 80



- HTTP over port 443

An authentication certificate is required to allow back-end servers in Application Gateway V1. The authentication certificate is the public key of back-end server certificates in Base-64 encoded X.509(.CER) format. For information on how to export the public key from your TLS/SSL certificate, see Export authentication certificate (for v1 SKU).

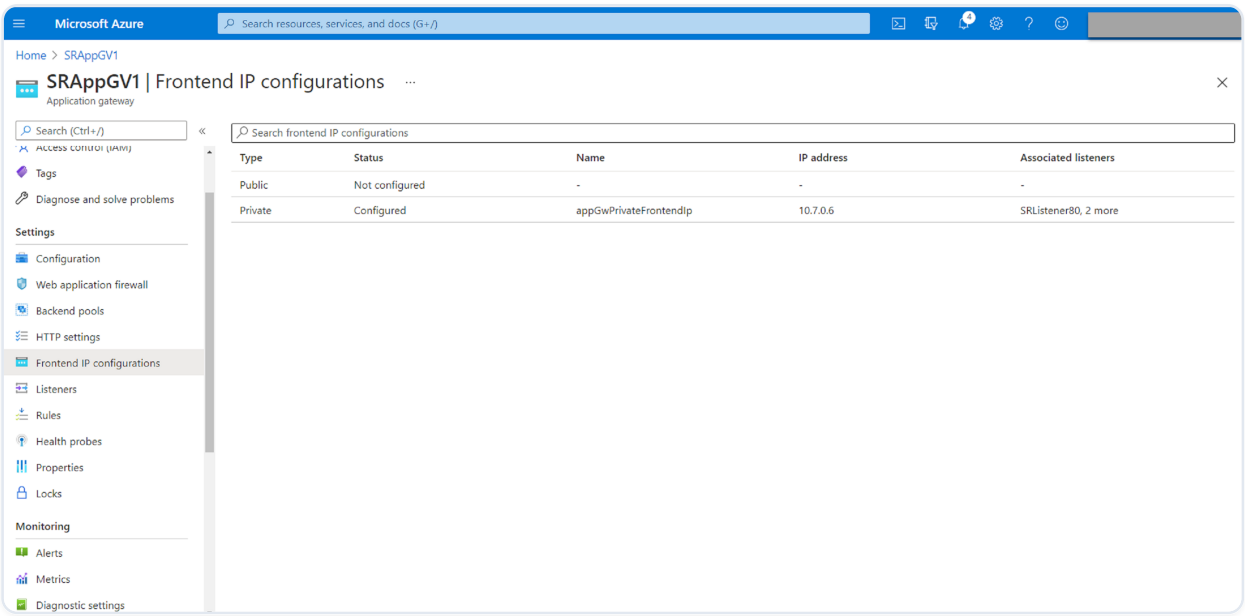




- HTTP or HTTPS over port 22334

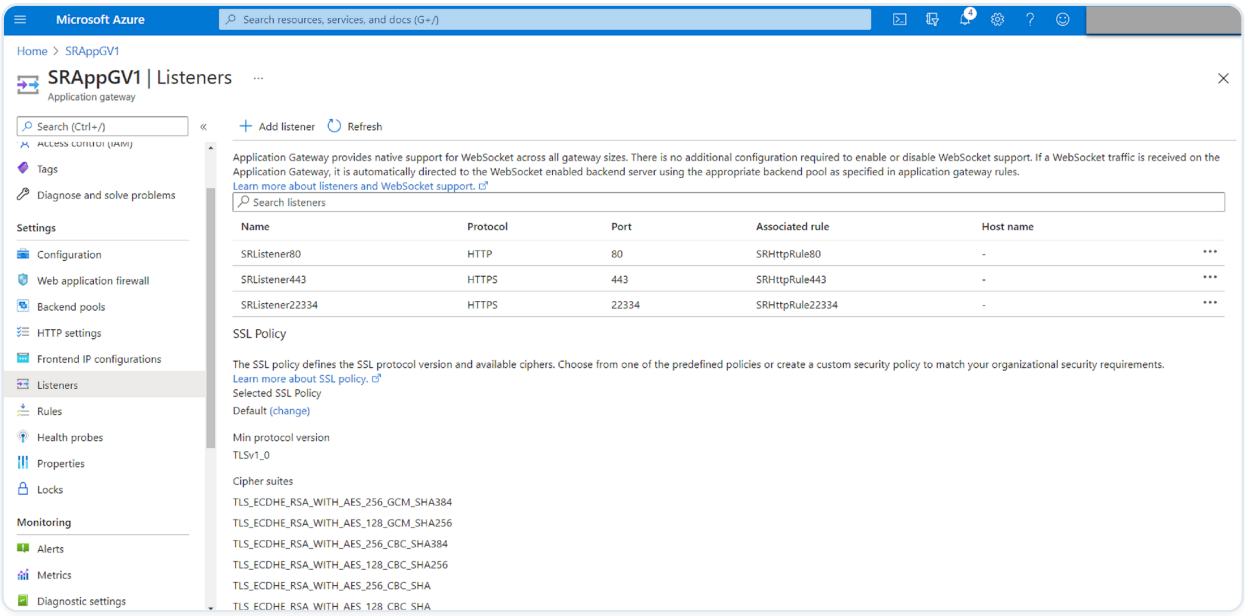
  If WebSocket uses HTTP, use the same setting as port 80. If WebSocket uses HTTPS, use the same setting as port 443.

4. Add a front-end IP address.

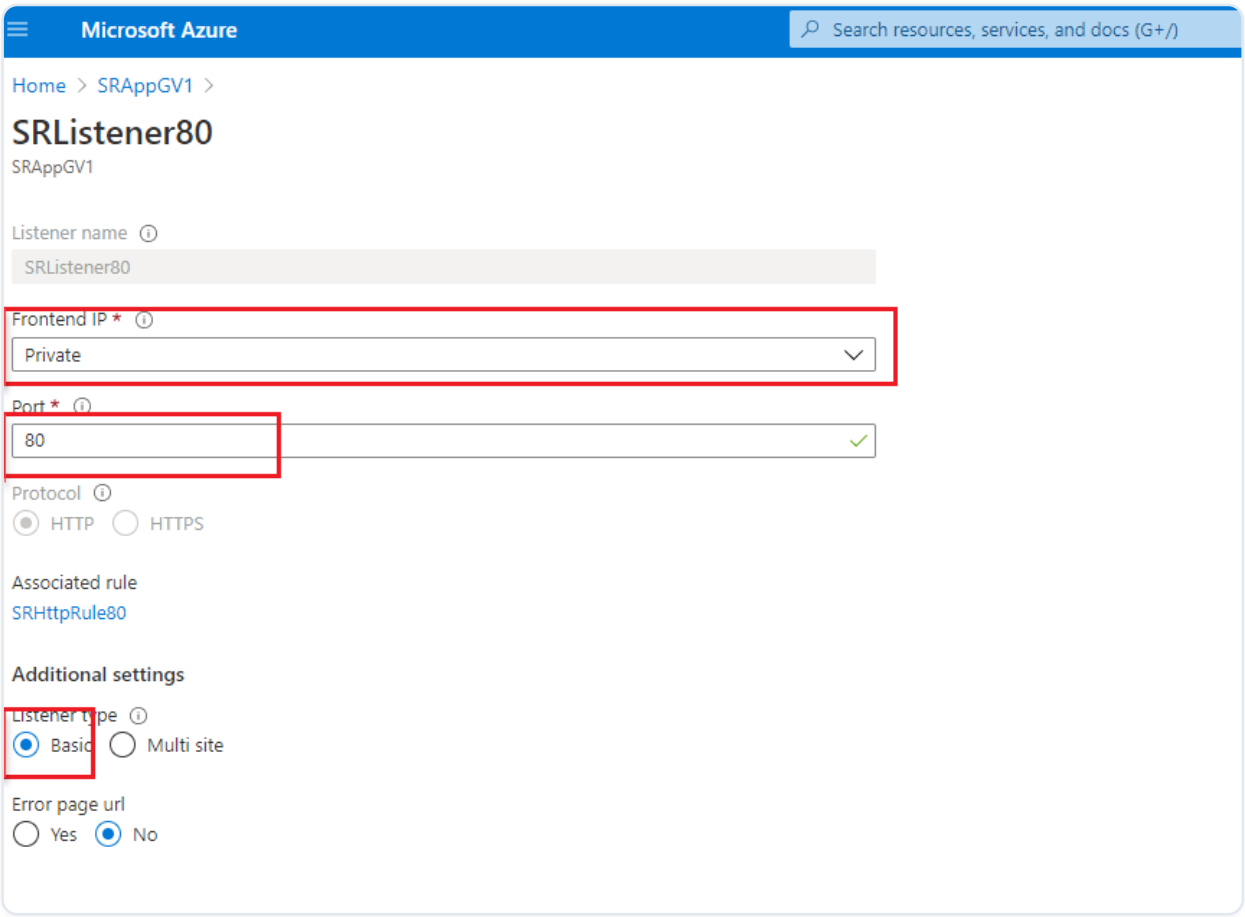


5. Add listeners.

   Add listeners on ports 80, 443, and 22334, for example:

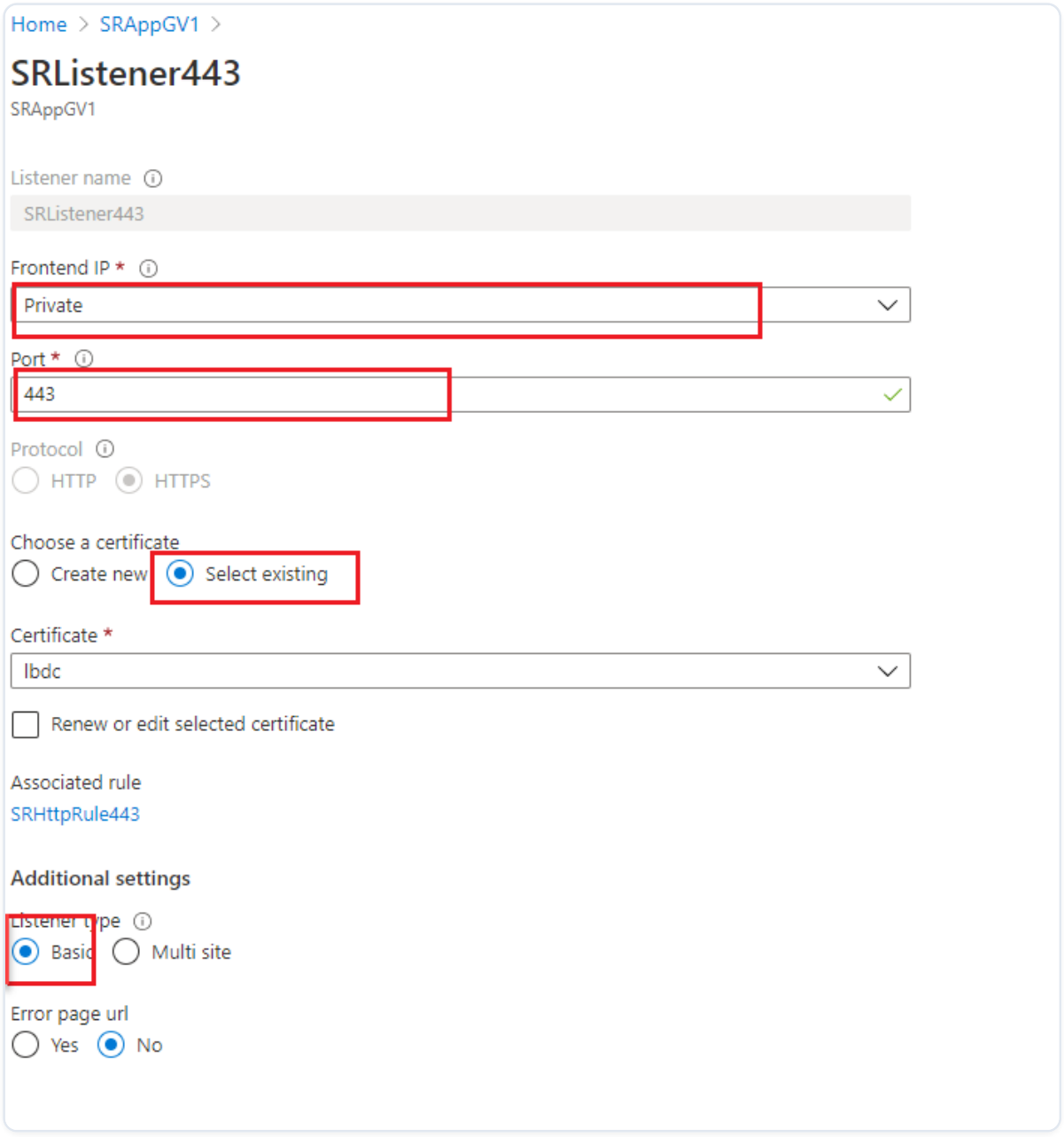


- Listener on port 80



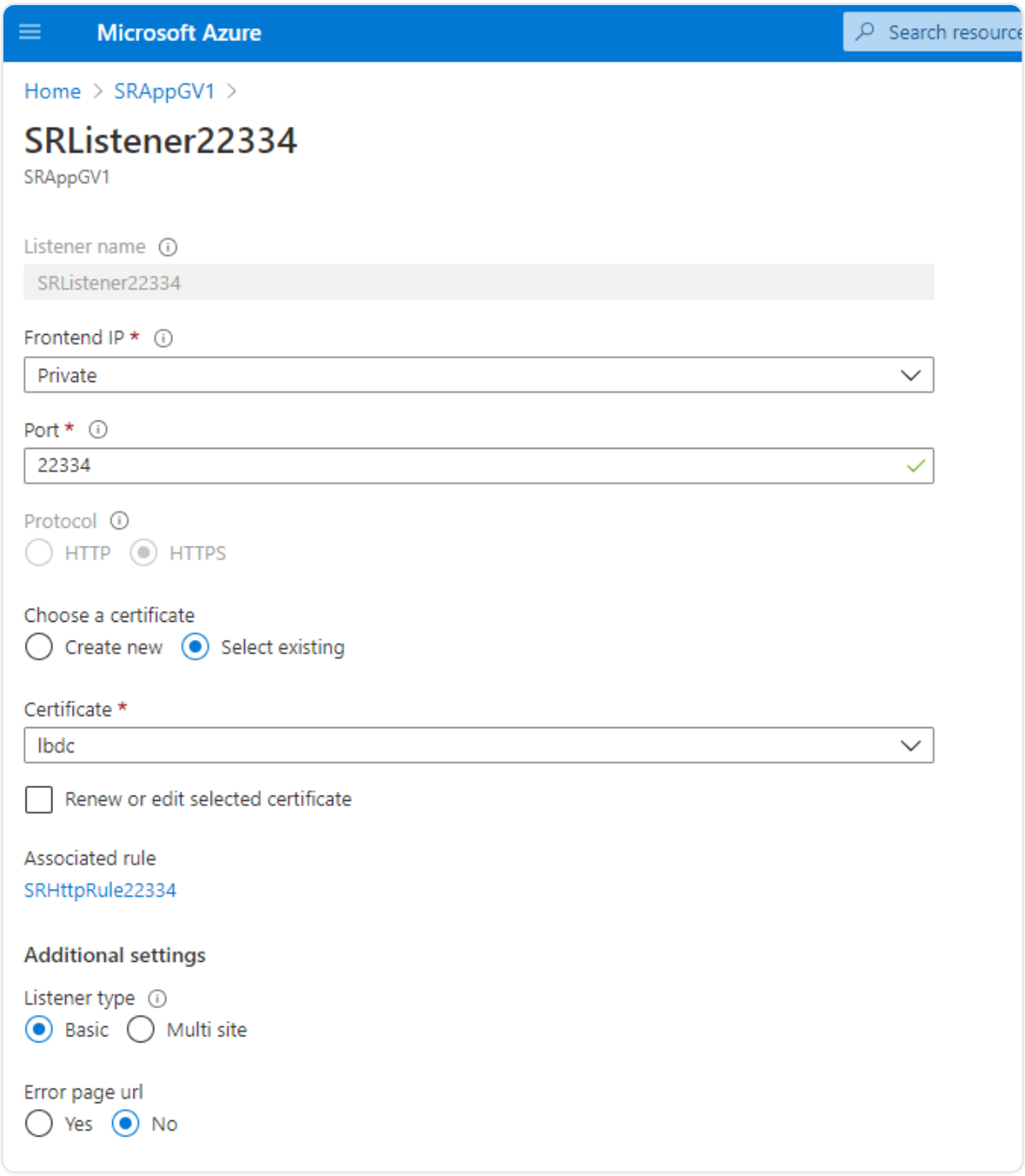
- Listener on port 443

Create a self-signed certificate and upload the certificate to the Azure portal when you create the HTTPS listener. For more information, see Certificates supported for TLS termination and Create a self-signed certificate.



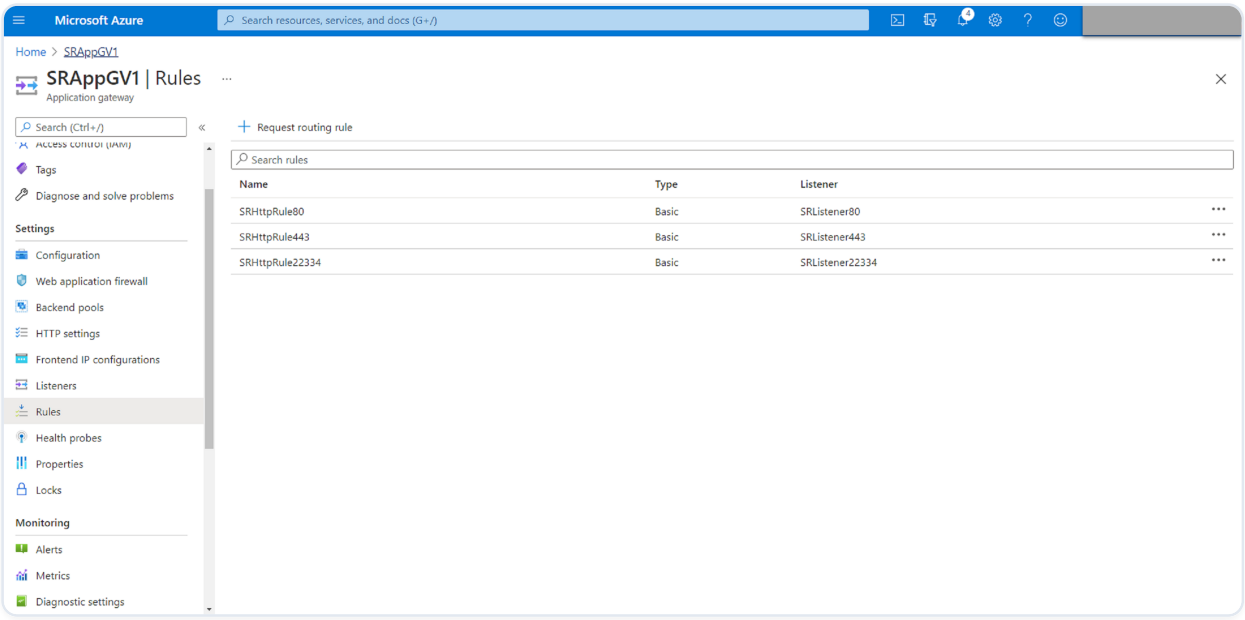
- Listener on port 22334

  If WebSocket uses HTTP, use the same setting as port 80. If WebSocket uses HTTPS, use the same setting as port 443. The following example shows the setting of an HTTPS listener on port 22334.

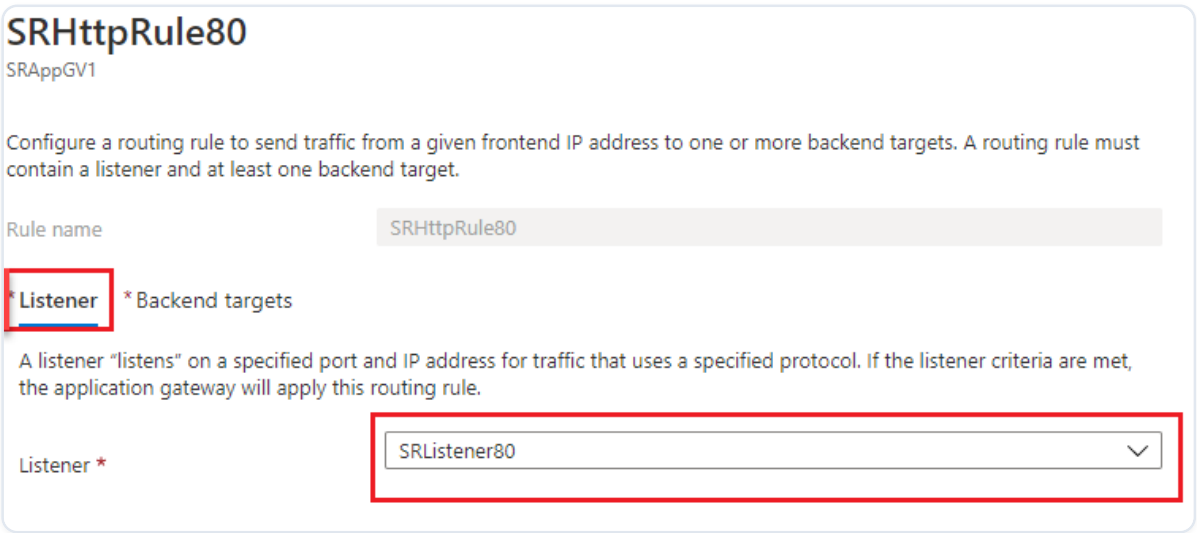


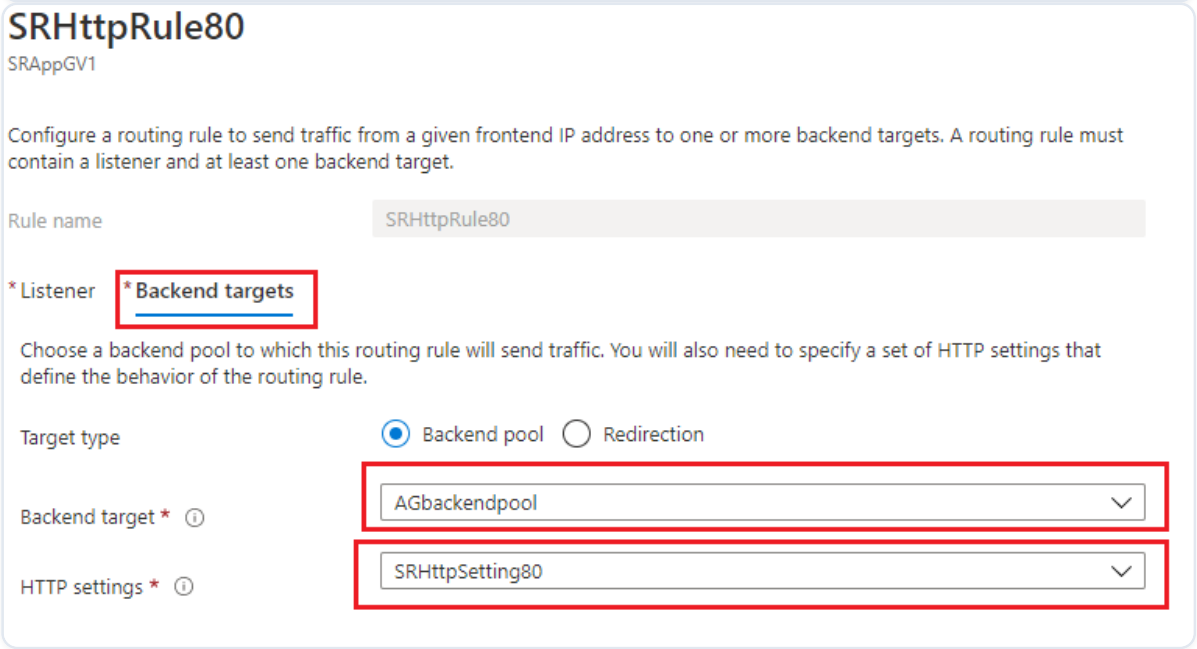
6. Create request routing rules.

   Create rules for ports 80, 443, and 22334, for example:

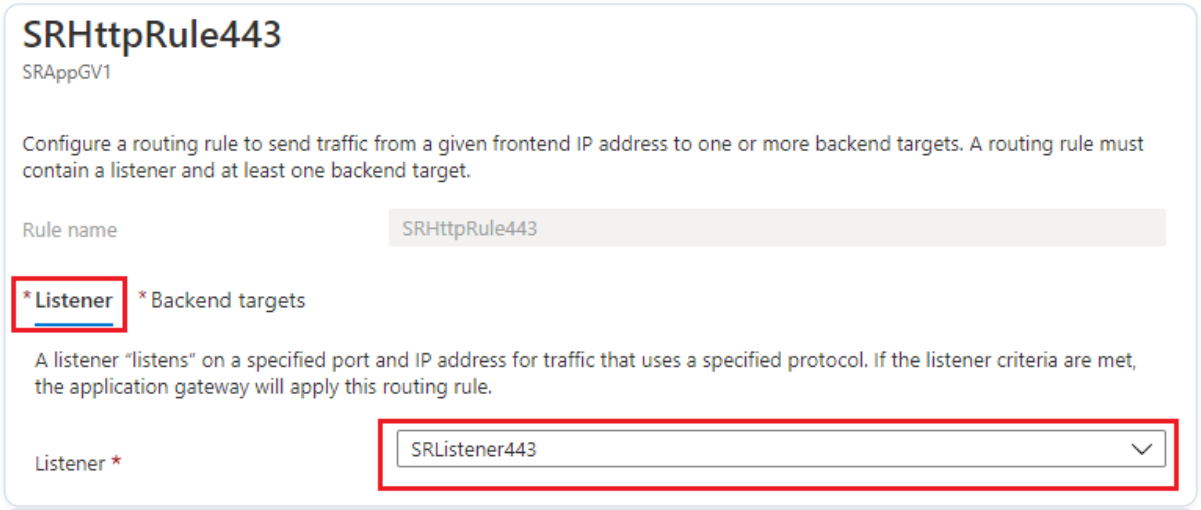


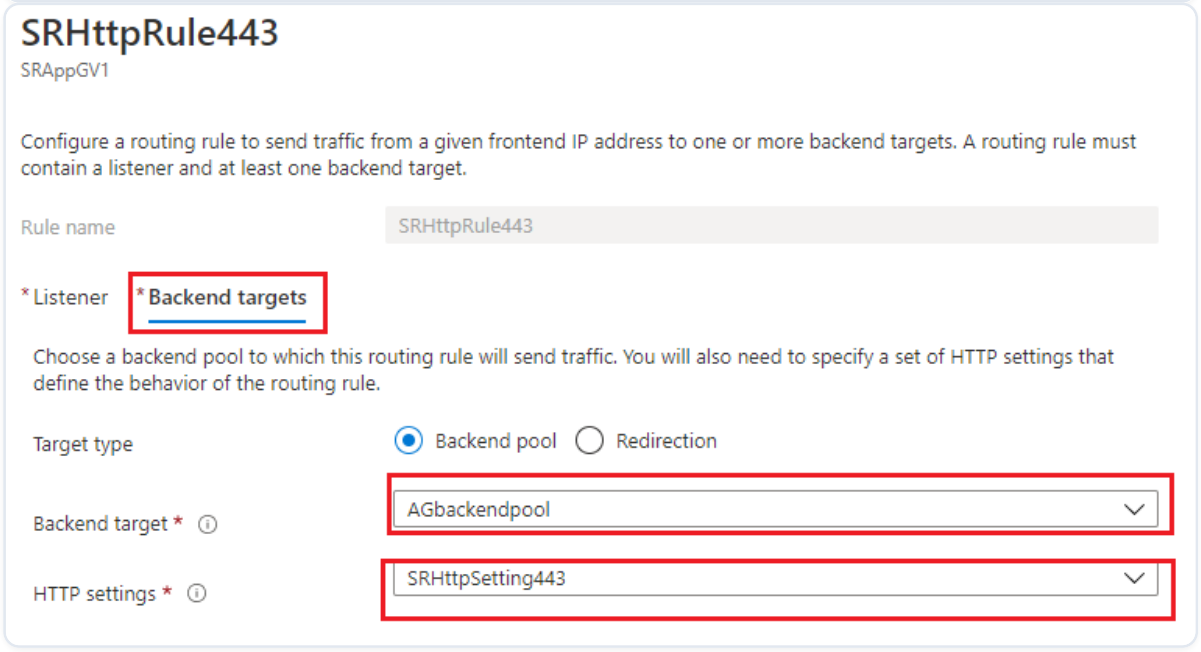
- Routing rule for port 80



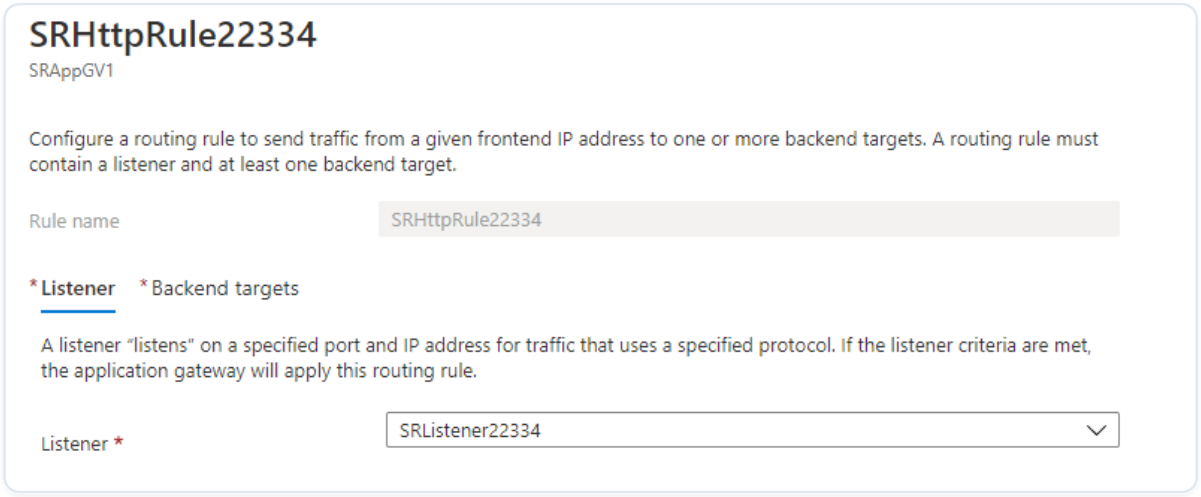


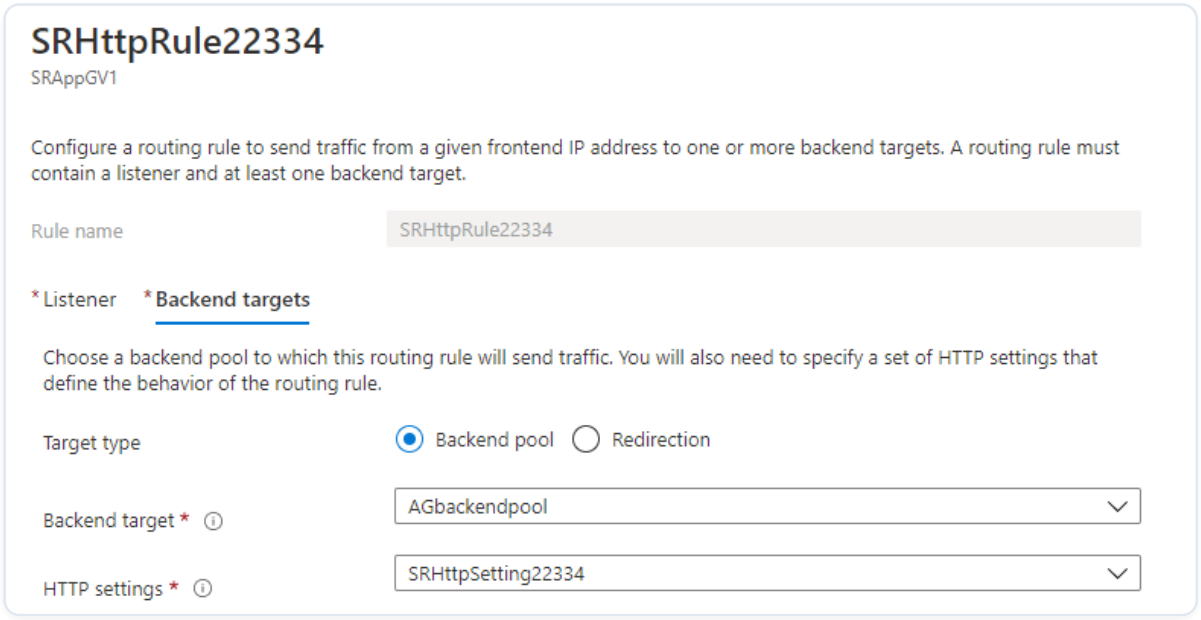
- Routing rule for port 443





- Routing rule for port 22334





7. Add the Azure VMs where the Session Recording server is installed to the back-end pool.
8. Configure Session Recording servers according to Knowledge Center article CTX230015.

Troubleshoot

The troubleshooting information contains solutions to some issues that you might encounter during or after installing the Session Recording components.

> **Warning:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix® cannot guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Installation of server components fails

The installation of the Session Recording server components fails with error codes 2503 and 2502. Resolution: Check the access control list (ACL) of folder C:\\windows\\Temp to ensure that the Local Users and Groups have write permission for this folder. If not, manually add write permission.

Test connection to the database fails during install

When you install the Session Recording database or the Session Recording server, the test connection fails with the error message **Database connection test failed. Please correct database instance name** even if the database instance name is correct.

In this case, ensure that the current user has the public SQL Server role permission to correct the permission limitation failure.

Agent cannot connect to the server

When the Session Recording agent cannot connect to the Session Recording server, the **Exception caught while sending poll messages to Session Recording Broker** event message is logged with an exception text. The exception text provides reasons why the connection failed. The reasons include:

- **The underlying connection was closed. Could not establish a trust relationship for the SSL/TLS secure channel.** This exception means that the Session Recording server is using a certificate signed by a CA that the server hosting the Session Recording agent does not trust or the server hosting the Session Recording agent does not have a CA certificate. Alternatively, the certificate might have expired or been revoked.

  Solution: Install a correct CA certificate on the server hosting the Session Recording agent. Use a CA that is trusted.

- **The remote server returned an error: (403) forbidden.** This standard HTTPS error occurs when you attempt to connect using HTTP that is unsecure. The machine hosting the Session Recording server rejects the connection because it accepts only secure connections.

  Solution: Use **Session Recording Agent Properties** to change the Session Recording Broker protocol to **HTTPS**.

- **The Session Recording Broker returned an unknown error while evaluating a record policy query. Error code 5 (Access Denied). For more information, see the Event log on the Session Recording server.** This error occurs when sessions are started and a request for a record policy evaluation is made. The error is a result of the Authenticated Users group (the default member) being removed from the Policy Query role of the Session Recording Authorization Console.

  Solution: Add the Authenticated Users group back to this role, or add each server hosting each Session Recording agent to the PolicyQuery role.

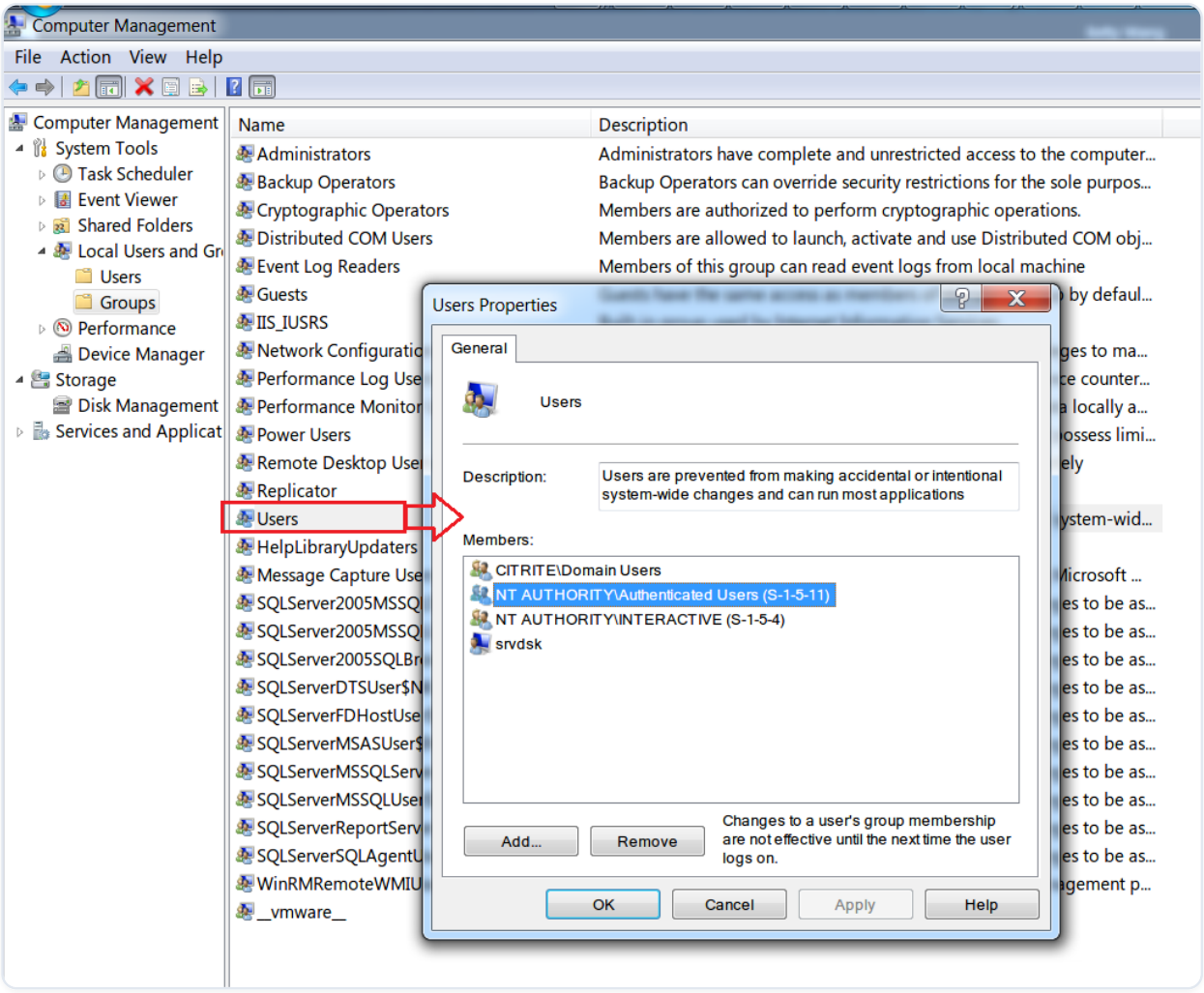
- **The underlying connection was closed. A connection that was expected to be kept alive was closed by the server.** This error means that the Session Recording server is down or unavailable to accept requests. The IIS might be offline or restarted, or the entire server might be offline.

  Solution: Verify that the Session Recording server is started and connected to the network. Make sure that IIS is running on the server.

- **The remote server returned an error: 401 (Unauthorized).** This error manifests itself in the following ways:

  - On startup of the Session Recording agent Service, an error describing the 401 error is recorded in the event log.
  - Policy query fails on the Session Recording agent.
  - Session recordings are not captured on the Session Recording agent.

Solution: Ensure that the **NT AUTHORITY\Authenticated Users** group is a member of the local **Users** group on the Session Recording agent.



Server cannot connect to the database

When the Session Recording server can't connect to the Session Recording database, you might see a message similar to one of the following:

Event Source:

A network-related or instance-specific error occurred while establishing a connection to SQL Server. This error appears in the applications event log with ID 2047. You can find the event log in the Event Viewer on the Session Recording server.

Citrix Session Recording Storage Manager Description: Exception caught while establishing database connection. This error appears in the applications event log in the Event Viewer of the Session Recording server.

Unable to connect to the Session Recording server. Ensure that the Session Recording server is running. This error message appears when you launch the Session Recording policy console.

Resolution:

- You installed Microsoft SQL Server on a stand-alone server and failed to configure the correct services or settings for Session Recording. The server must have the TCP/IP protocol enabled and the SQL Server Browser service running. See the Microsoft documentation for information about enabling these settings.
- During the Session Recording installation (administration portion), incorrect server/database information was given. Uninstall the Session Recording database and reinstall it, supplying the correct information.
- The Session Recording database server is down. Verify that the server has connectivity.
- The machine hosting the Session Recording server or the machine hosting the Session Recording database server cannot resolve the FQDN or NetBIOS name of the other. Use the ping command to verify that the names can be resolved.
- Check the firewall configuration on the Session Recording Database to ensure that the SQL Server connections are allowed. For more information, see the Microsoft article at `<https://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?redirectedfrom=MSDN&view=sql-server-ver15>`.

Logon failed for user 'NT_AUTHORITY\\ANONYMOUS LOGON'. This error message means that the services are logged on incorrectly as .\\administrator.

Resolution: Restart the services as local system user and restart the SQL services.

Sessions are not recording

If application sessions are not recording successfully, check the application event log in the Event Viewer on the Session Recording agent and Session Recording server. Doing so can provide valuable diagnostic information.

If sessions are not recording, the possible cause might be:

- **Component connectivity and certificates**. If the Session Recording components cannot communicate with each other, session recording can fail. To troubleshoot recording issues,

verify that all components are configured correctly to point to the correct machines and that all certificates are valid and correctly installed.

- **Non-Active Directory domain environments**. Session Recording is designed to run in a Microsoft Active Directory domain environment. If you are not running in an Active Directory environment, you might experience recording issues. Ensure that all Session Recording components are running on machines that are members of an Active Directory domain.
- **Session sharing conflicts with the active policy.** Session Recording matches the active policy with the first published application that a user opens. Subsequent applications opened during the same session continue to follow the policy that is in force for the first application. To prevent session sharing from conflicting with the active policy, publish the conflicting applications on separate multi-session OS VDAs.
- **Recording is not enabled.** By default, installing the Session Recording Agent on a multi-session OS VDA enables recording for the VDA. Recording does not occur until an active recording policy is configured to allow it.
- **The active recording policy does not permit recording.** A session can be recorded only when the session meets the rules of the active recording policy.
- **Session Recording services are not running.** For sessions to be recorded, the Session Recording Agent service must be running on a multi-session OS VDA and the Session Recording Storage Manager service must be running on the machine hosting the Session Recording Server.
- **MSMQ is not configured.** If MSMQ is not correctly configured on the server running the Session Recording Agent and the machine hosting the Session Recording Server, recording problems might occur.

Unable to view live session playback

If you experience difficulties when viewing recordings using the Session Recording player, the following error message might appear:

Download of recorded session file failed. Live session playback is not permitted. The server has been configured to disallow this feature. This error indicates that the server is configured to disallow the action.

Resolution: In **Session Recording Server Properties**, choose the **Playback** tab and select the **Allow live session playback** check box.

Recordings are corrupted or incomplete

- When you view corrupted or incomplete recordings in the player, you might also see warnings in the Event logs on the Session Recording server.

  Event Source: Citrix Session Recording Storage Manager

  Description: Data lost while recording file **\<icl file name\>**

  The issue occurs when MCS or PVS is used to create VDAs with a master image configured and Microsoft Message Queuing (MSMQ) installed. In this condition, the VDAs have the same `QMId` for MSMQ.

  As a workaround, create a unique `QMId` for each VDA. For more information, see Install, upgrade, and uninstall.

- The Session Recording player might report an internal error with the message - "**The file being played has reported that an internal system error (error code: 9) occurred during its original recording. The file can still be played up to the point that the recording error occurred**" when playing back a certain recording file.

  The issue occurs due to insufficient buffer size on the Session Recording Agent when graphic intensive sessions are recorded.

  As a workaround, change `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SmAudBufferSizeMB` to higher value data on the Session Recording agent, and then restart the machine.

Verify component connections

During the setup of Session Recording, the components might not connect to other components. All the components communicate with the Session Recording server (Broker). By default, the Broker (an IIS component) is secured using the IIS default website certificate. If one component can't connect to the Session Recording server, the other components might also fail when attempting to connect.

The Session Recording agent and the Session Recording server (Storage Manager and Broker) log connection errors in the applications event log. You can view the log in the Event Viewer of the machine hosting the Session Recording server. The Session Recording policy console and the Session Recording player display connection error messages on screen when they fail to connect.

Verify that the Session Recording agent is connected

1. Log on to the server where the Session Recording agent is installed.
2. From the **Start** menu, choose **Session Recording Agent Properties**.
3. In **Session Recording Agent Properties**, click **Connection**.
4. Verify that the correct FQDN is entered in the **Session Recording Server** field.
5. Verify that the server given as the value for the Session Recording server is accessible to your VDA for multi-session OS.

For more information, see Agent cannot connect to the server.

> **Note:**
>
> Check the application event log for errors and warnings.

Verify that the Session Recording server is connected

> **Caution:**
>
> Using the Registry Editor can cause serious problems that might require you to reinstall the operating system. Citrix® cannot guarantee that problems resulting from incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk.

1. Log on to the machine hosting the Session Recording server.
2. Open the Registry Editor.
3. Browse to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`.
4. Verify that the **SmAudDatabaseInstance** value correctly references the Session Recording database you installed on your SQL Server instance.

For more information, see Server cannot connect to the database.

Verify that the Session Recording database is connected

1. Using a SQL Management tool, open your SQL instance that contains the Session Recording database you installed.
2. Open the Security permissions of the Session Recording database.

3. Verify that the Session Recording Computer Account has access to the database. For example, if the machine hosting the Session Recording server is named **SsRecSrv** in the MIS domain, the computer account in your database must be configured as **MIS\\SsRecSrv$**. This value is configured during the Session Recording database installation.

Test IIS connectivity

You can test connections to the Session Recording server IIS site by using a Web browser to access the Session Recording Broker webpage. It can help you determine whether problems with communication between Session Recording components stem from misconfigured protocol configuration, certification issues, or problems starting Session Recording Broker.

To verify IIS connectivity for the Session Recording agent:

1. Log on to the server where the Session Recording Agent is installed.
2. Open a Web browser and type the following address:
   - For HTTPS: `https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl`, where `servername` is the name of the machine hosting the Session Recording server.
   - For HTTP: `http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl`, where `servername` is the name of the machine hosting the Session Recording server.
3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

To verify IIS connectivity for the Session Recording player:

1. Log on to the workstation where the Session Recording player is installed.
2. Open a Web browser and type the following address:
   - For HTTPS: `https://servername/SessionRecordingBroker/Player.rem?wsdl`, where `servername` is the name of the machine hosting the Session Recording server.
   - For HTTP: `http://servername/SessionRecordingBroker/Player.rem?wsdl`, where `servername` is the name of the machine hosting the Session Recording server.
3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

To verify IIS connectivity for the Session Recording policy console:

1. Log on to the server where the Session Recording policy console is installed.
2. Open a Web browser and type the following address:
    - For HTTPS: `https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`, where `servername` is the name of the machine hosting the Session Recording server.
    - For HTTP: `http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`, where `servername` is the name of the machine hosting the Session Recording server.
3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

If you see an XML document within your browser, it verifies that the Session Recording policy console is connected to the Session Recording server using the configured protocol.

Troubleshoot certificate issues

If you are using HTTPS as your communication protocol, the machine hosting the Session Recording server must be configured with a server certificate. All component connections to the Session Recording server must have root certificate authority (CA). Otherwise, attempted connections between the components fail.

You can test your certificates by accessing the Session Recording Broker webpage as you would when testing IIS connectivity. If you are able to access the XML page for each component, the certificates are configured correctly.

Here are some common ways certificate issues cause connections to fail:

- **Invalid or missing certificates.** If the server running the Session Recording agent does not have a root certificate to trust the server certificate and cannot trust and connect to the Session Recording server over HTTPS, causing connectivity to fail, verify that all components trust the server certificate on the Session Recording server.
- **Inconsistent naming.** If the server certificate assigned to the machine hosting the Session Recording server is created using an FQDN, all connecting components must use the FQDN when connecting to the Session Recording server. If a NetBIOS name is used, configure the components with a NetBIOS name for the Session Recording server.
- **Expired certificates.** If a server certificate expired, connectivity to the Session Recording server through HTTPS fails. Verify the server certificate assigned to the machine hosting the Session Recording server is valid and has not expired. If the same certificate is used for the

digital signing of session recordings, the event log of the Session Recording server provides error messages that the certificate expired or warning messages when it is about to expire.

Search for recordings using the player fails

If you experience difficulties when searching for recordings using the Session Recording player, the following error messages might appear:

- **Search for recorded session files failed. The remote server name could not be resolved: servername.** The **servername** is the name of the server to which the Session Recording player is attempting to connect. The Session Recording player cannot contact the Session Recording server. Two possible reasons are an incorrectly typed server name or that the DNS cannot resolve the server name.

  Resolution: From the player menu bar, choose **Tools > Options > Connections** and verify that the server name in the **Session Recording Servers** list is correct. If it is correct, from a command prompt, run the ping command to see if the name can be resolved. When the Session Recording server is down or offline, the search for recorded session files failed error message is **Unable to contact the remote server**.
- **Unable to contact the remote server.** This error occurs when the Session Recording server is down or offline.

  Resolution: Verify that the Session Recording server is connected.
- **Access denied.** An access denied error can occur if the user was not given permission to search for and download recorded session files.

  Resolution: Assign the user to the Player role using the Session Recording Authorization Console.
- **Access denied when the Player role is assigned.** This error occurs when you install the Session Recording player on the same machine with the Session Recording server, and you have enabled UAC. When you assign the Domain Admins or Administrators user group as the Player role, a non-built-in administrator user in that group might fail to pass the role-based check.

  Resolutions:

  - Run the Session Recording player as an administrator.
  - Assign specific users as the Player role rather than the entire group.

- Install the Session Recording player in a separate machine rather than the Session Recording server.

- **Search for recorded session files failed. The underlying connection was closed. Could not establish a trust relationship for the SSL/TLS secure channel.** The error occurs when the Session Recording server uses a certificate that is signed by a CA that the client device does not trust or have a CA certificate for.

  Resolution: Install the correct or trusted CA certificate workstation where the Session Recording player is installed.

- **The remote server returned an error: (403) forbidden.** This error is a standard HTTPS error that occurs when you attempt to connect using HTTP (nonsecure protocol). The server rejects the connection because, by default, it is configured to accept only secure connections.

  Resolution: From the **Session Recording Player** menu bar, choose **Tools** \> **Options** \> **Connections**. Select the server from the **Session Recording Servers** list, and click **Modify**. Change the protocol from **HTTP** to **HTTPS**.

Troubleshoot MSMQ

If a notification message is given but the viewer cannot find any recordings after a search in the Session Recording player, there is a problem with MSMQ. Verify that the queue is connected to the Session Recording server (Storage Manager). Use a Web browser to test for connection errors (if you are using HTTP or HTTPS as your MSMQ communication protocol).

To verify that the queue is connected:

1. Log on to the server hosting the Session Recording Agent and view the outgoing queues.
2. Verify that the queue to the machine hosting the Session Recording server has a connected state.
   - If the state is **waiting to connect**, there are messages in the queue, and the protocol is HTTP or HTTPS (corresponding to the protocol selected on the **Connections** tab in **Session Recording Agent Properties**), perform Step 3.
   - If the state is **connected** and there are no messages in the queue, there might be a problem with the server hosting the Session Recording server. Skip Step 3 and perform Step 4.
3. If there are messages in the queue, open a Web browser and type the following address:

- For HTTPS: `https://servername/msmq/private$/CitrixSmAudData`, where `servername` is the name of the machine hosting the Session Recording server.
- For HTTP: `http://servername/msmq/private$/CitrixSmAudData`, where `servername` is the name of the machine hosting the Session Recording server.

If the page returns an error such as **The server only accepts secure connections**, change the MSMQ protocol listed in **Session Recording Agent Properties** to HTTPS. If the page reports a problem with the website security certificate, there might be a problem with a trust relationship for the TLS secure channel. In that case, install the correct CA certificate or use a CA that is trusted.

4. If there are no messages in the queue, log on to the machine hosting the Session Recording server and view private queues. Select **citrixsmauddata**. If there are messages in the queue (Number of Messages Column), verify that the Session Recording StorageManager service is started. If it is not, restart the service.

Record Linux sessions (experimental)

As an experimental feature starting with the Linux VDA 2212, you can record and replay sessions hosted on a Linux VDA. For more information, see Session recording (experimental) in the Linux VDA documentation.

Note:

All the policies you set for recording Windows sessions don't apply to the Linux session recording.

Session Recording Document History

The following table describes important changes to the Session Recording 2305 documentation. To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	DESCRIPTION
31 May 2023	Initial release of Session Recording 2305	See What's new.