Session Recording 2607 LTSR

> **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 2607-ltsr

Important note about upgrading to version 2607 LTSR:

To prevent session recording failures due to incomplete upgrades of Session Recording agents, follow these steps when upgrading to 2607 LTSR:

1. Upgrade each Session Recording server to version 2607 LTSR.
2. Enable remote access using .NET Remoting with the following command:

   ```
   <Session Recording server installation path>\Bin\SsRecUtils.exe -EnableBrokerRemoting
   ```

3. Upgrade each Session Recording agent to version 2607 LTSR.
4. After all Session Recording agents are upgraded, disable remote access using .NET Remoting with the following command:

   ```
   <Session Recording server installation path>\Bin\SsRecUtils.exe -DisableBrokerRemoting
   ```

Note on Upgrade Impact for the ICLFile Table

As part of the upgrade process, several indexes will be created on the ICLFile table. Depending on the volume of data, this operation may take up to 15 minutes to complete and will require approximately 60% additional storage relative to the current size of the table.

This change does not affect fresh installations.

This release includes the following new features...

Session event data export as JSON

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

For more information, see Session Recording file export.

Daily insights in AI-powered insights for session recording

Session Recording now supports three analysis scopes when analyzing recordings: a single recording file, an entire rollover session, or all recordings of a user on a selected day. The new daily insight option enables administrators to review a full day's activity in a single analysis.

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

Azure Managed Identity support for Azure SQL

Session Recording now supports Azure Managed Identity authentication for Azure SQL database connections.

For more information, see Install the Session Recording Administration components.

Site-level user activity reporting in the Session Recording web console

The Session Recording web console now includes a site-level user activity report, giving administrators a consolidated view of detected events across all recorded sessions. Events can be filtered by event type, session user, and client device for more targeted analysis.

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

Web console policy configuration

Administrators can now configure session recording, event detection, and event response policies directly in the Session Recording web console, in addition to using the Session Recording Policy Console. The web console also introduces a new Idle periods event type that logs user idle time within recorded sessions.

For more information, see Policies (web console).

What's new in earlier releases

For new features included in the releases that shipped after the 1912 Long Term Service Releases (LTSR) through the 2603 Releases, see What's new history.

Fixed issues

Compared with: Session Recording 2603

Session Recording 2607 LTSR adds the following fixes:

- Session Recording might fail to detect or log file transfer events when files are transferred through Client Drive Mapping (CDM) or USB devices.
- When applying search filters in the Session Recording Player, valid recordings that match the criteria might be randomly missing from the result list.
- Session recording might occasionally fail in lossy mode after multiple file rollovers when using SRMQ.
- Session Recording might fail to detect app start and app end events when the application is launched from a UNC path.
- Session Recording installation might fail in a multi-forest Active Directory environment.

Known issues

The following issues have been identified in this release:

- Audio recording might fail if the VDA and Session Recording Agent versions are mismatched.
- When the Session Recording Agent accesses the Session Recording Server through an F5 reverse proxy configured in L7 mode with TLS re-encryption, Session Recording may not work. Workaround: Add the following iRule to the F5 Virtual Server to strip the Expect header before the request reaches the backend:

  ```
  when HTTP_REQUEST {

      HTTP::header remove "Expect"

  }
  ```

- Session Recording Server installation might fail with the error "Database 'CitrixSessionRecording' already in use" (Error 1001 followed by Error 1603) when the SQL

Server model database contains user-defined tables. Workaround: Before installing Session Recording, verify that the SQL Server model database does not contain user-defined tables by running the following query: SELECT name FROM model.sys.tables. If any tables are present, work with your DBA to remove them from the model database, then retry the installation.

- When the client is:

  a. A **Windows 10** virtual machine

  b. Has **no** physical GPU

  c. **Only** has Microsoft's basic display drivers installed, such as Microsoft Basic Display Adapter, Microsoft Remote Display Adapter, Microsoft Hyper-V Video, etc., and no other third-party indirect display drivers or Citrix Indirect Display Driver installed

If any of the following operations are performed:

1. Connecting to RDP, then disconnecting and reconnecting
2. Changing the display resolution

Endpoint Recording will fail unexpectedly.

- 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.

- A **400 Bad Request** error might occur when a user attempts to replay recorded sessions using the Session Recording player or web player. The issue can occur when the user is a member of too many Active Directory user groups. To work around this issue, complete the following steps:

  a. Go to the IIS server machine where the Session Recording server is installed and add the **MaxFieldLength** and the **MaxRequestBytes** DWORD values under **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters**.

  b. Set the DWORD values to 65534 in decimal.

c. Restart the IIS server machine.

- Attempts to record Microphone audio fail when HDX™ audio is transmitted in Real-time Transport Protocol (RTP) mode on a Windows 10 or Windows 11 VDA.
- 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.
- Attempts to close unresponsive or dormant live recordings automatically or manually by using the ICLDB DORMANT command might fail. The issue occurs when you update Session Recording to 2308 instead of doing a fresh installation. To resolve the issue, run the following script in PowerShell on the Session Recording server machine and ensure that you have administrative access to the Session Recording database:

```
Add-Type -AssemblyName System.data

$registryKey =
[Microsoft.Win32.Registry]::LocalMachine.OpenSubKey("SOFTWARE\\Citrix\
\SmartAuditor\\Server")

$dbName = $registryKey.GetValue("DatabaseName")

$dbInstance = $registryKey.GetValue("SmAudDatabaseInstance")

write-host "Connecting to $dbInstance\$dbName"

# Connect db

$conn = New-Object System.Data.SqlClient.SqlConnection

$conn.ConnectionString = "workstation id=.;packet size=4096;integrated
security=SSPI;data source=$dbInstance;persist security
info=True;initial catalog=$dbName"

$conn.Open()

$cmd = $conn.CreateCommand()

$cmd.CommandText = "use [$dbName];if not exists(select * from [dbo].
[EndReason] where ID=5) begin insert [dbo].[EndReason] values (5,
'Dormant') end"
```

```
$cmd.ExecuteNonQuery()
```

- Session Recording doesn't capture file transfers between a native disk on the session host (VDA) and a disk that's mapped to the session from the client.
- When you upgrade Session Recording to the latest version, your **image resolution scaling** settings for lossy screen recording 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.
- Session Recording Server upgrades may fail if IIS HTTPS bindings include a specific hostname.
- You may experience screen distortion during playback using Session Recording Web Player if recordings use HDX super resolution feature.
- Audio recording may fail if the VDA and Session Recording Agent versions are mismatched.

Third party notices

Session Recording Version 2509 (PDF Download)

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

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 the Knowledge Center article.

Session Recording database

Supported operating systems:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows 11
- 64-bit Windows 10

Supported Microsoft SQL Server versions:

- Microsoft SQL Server 2025 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2022 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2019 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

Supported database collations:

- Collations ending with _CI_AS

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 2025
- Windows Server 2022
- Windows Server 2019

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 Microsoft Edge.

Session Recording policy console

Supported operating systems:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019

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 2025
- Windows Server 2022
- Windows Server 2019
- Windows 11
- Windows 10

Requirements:

- Citrix Virtual Apps and Desktops™ 7 2607 LTSR with Premium license
- Citrix Virtual Apps and Desktops™ 7 2507 LTSR CU1 with Premium license
- Citrix Virtual Apps™ and Desktops 7 2402 LTSR CU3 with Premium license
- .NET Framework 4.7.2
- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled and MSMQ HTTP support enabled or Session Recording message queue.

> **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 2025
- Windows Server 2022
- Windows Server 2019

- Windows 11
- 64-bit Windows 10

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, your machine's hardware specifications, and the fast seeking settings configured in Session Recording Agent Properties. For more information, see Enable fast seeking.

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.

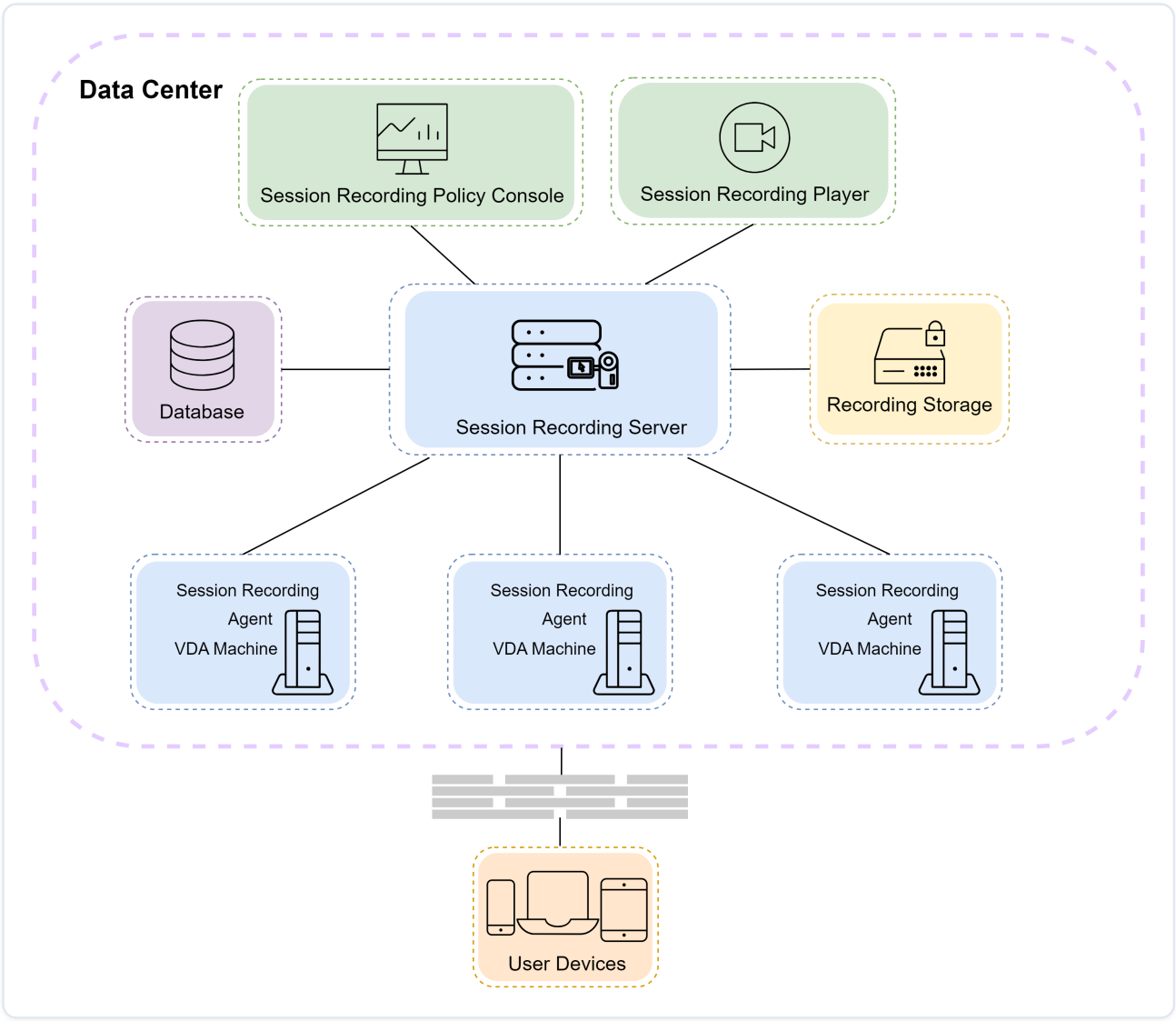
To install Session Recording or upgrade an existing installation, go to each machine where you are about to or have already installed the Session Recording components and then run the Citrix Virtual Apps™ and Desktops ISO.

> **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

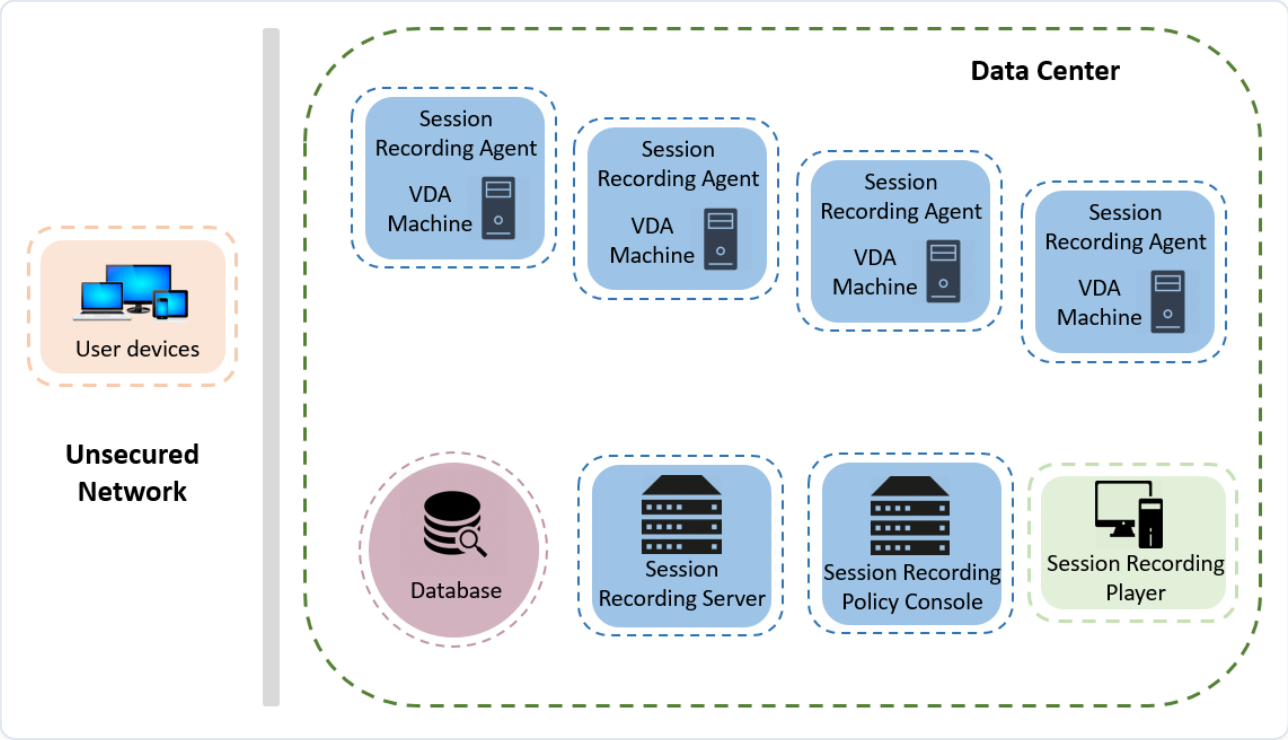
SOURCE	DESTINATION	TYPE	PORT	DETAILS
Virtual Delivery Agent	Session Recording server	TCP	80, 443	Communication between the Session Recording agent installed on Virtual Delivery Agent and the

SOURCE	DESTINATION	TYPE	PORT	DETAILS
				Session Recording server. Default installation uses HTTPS/SSL to secure communications. If SSL is not configured, use HTTP.
Virtual Delivery Agent	Session Recording server	TCP	1801	By default, Session Recording uses TCP as the communication protocol and thus MSMQ uses port 1801 for sending messages over TCP. Alternatively, MSMQ can use port 80 or 443 for sending messages over HTTP or HTTPS based on your protocol setting on the **Connections** tab of **Session Recording Agent Properties**.
Session Recording policy console	Session Recording server	TCP	80, 443	Communication between the server where

SOURCE	DESTINATION	TYPE	PORT	DETAILS
				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. 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`

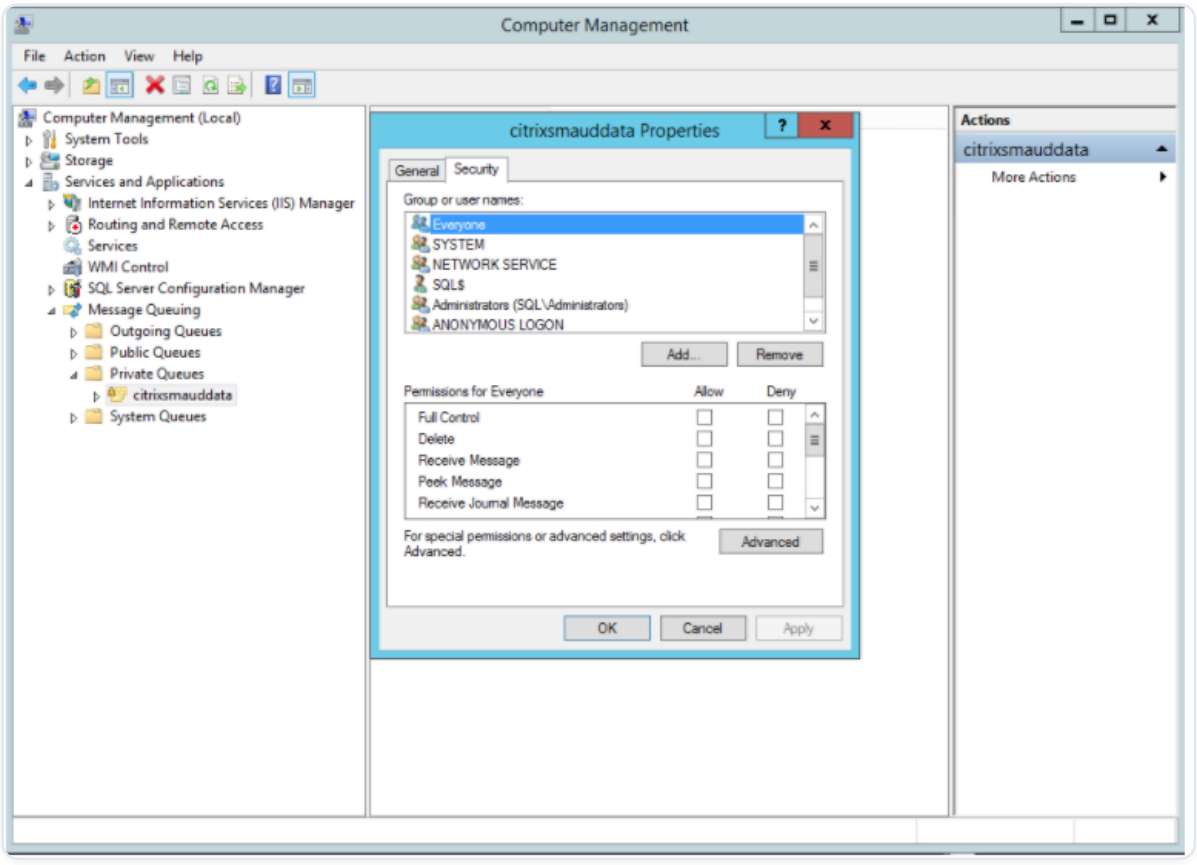
- As a security best practice, Citrix recommends using HTTPS on IIS.
- Set the access control list (ACL) for Message Queuing (MSMQ) on the Session Recording server to restrict VDA or VDI machines that can send MSMQ data to the Session Recording server and prevent unauthorized machines from sending data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

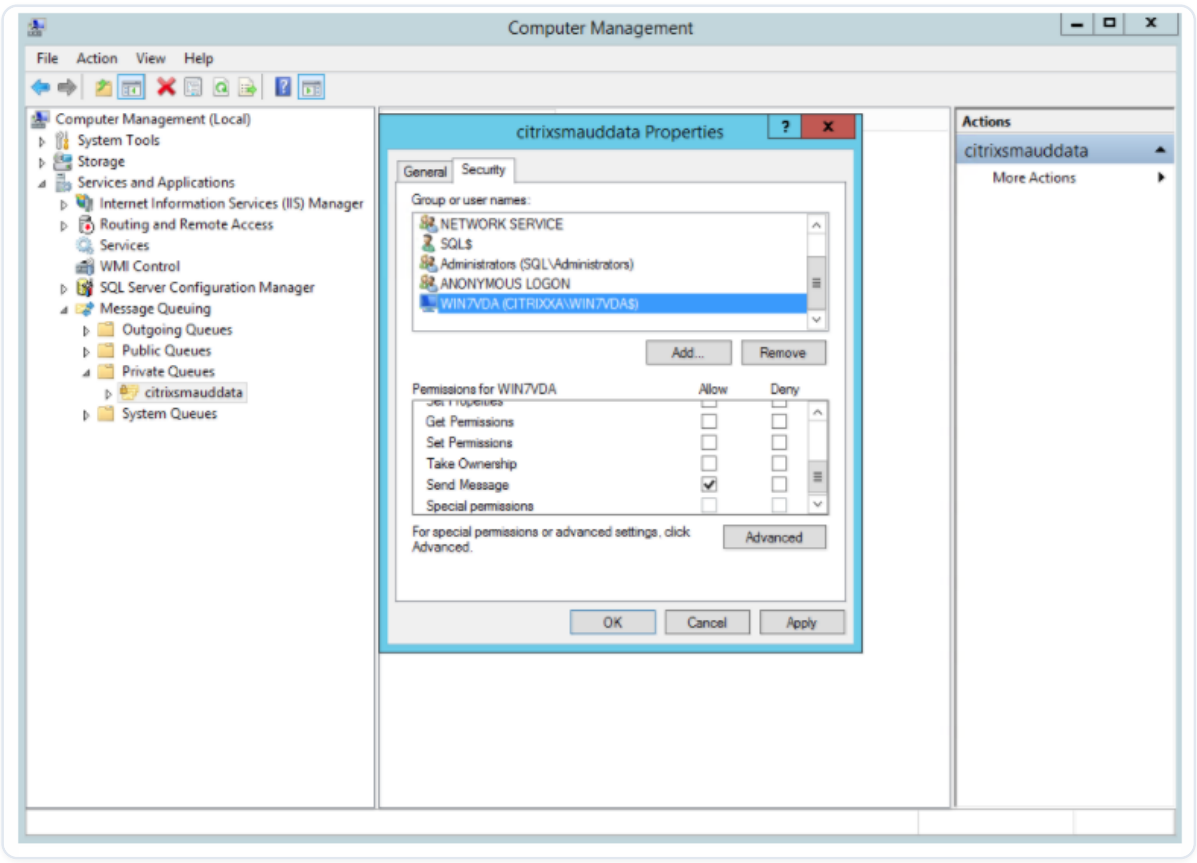
  b. From the Windows **Start** menu on each Session Recording server, open **Administrative Tools** \> **Computer Management**.

  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.

Enable enhanced message security for Session Recording

This feature introduces a message signature mechanism to validate the authenticity and integrity of incoming messages before they enter the Message Queuing (MSMQ) system. It is particularly critical for addressing security vulnerabilities in Azure Active Directory Joined (AADJ) Session Recording deployments.

To enable this feature, configure the registry keys on both the Session Recording server and the agent.

1. On the Session Recording server:

Add the `EnableMessageSignature` DWORD value and set it to `1` under the following registry key:

`HKEY_LOCAL_MACHINE\Software\Citrix\SmartAuditor\Server`

2. On the Session Recording agent:

   Add the `EnableMessageSignature` DWORD value and set it to `1` under the following registry key:

   `HKEY_LOCAL_MACHINE\Software\Citrix\SmartAuditor\Agent`

3. Restart services:

   For the changes to take effect, restart the Citrix Session Recording Storage Manager service on the server and the Citrix Session Recording Agent service on the agent.

> **Note:**
>
> To disable this feature, set the `EnableMessageSignature` DWORD value to `0` or delete the registry key on both the server and the agent, and then restart the respective services.

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

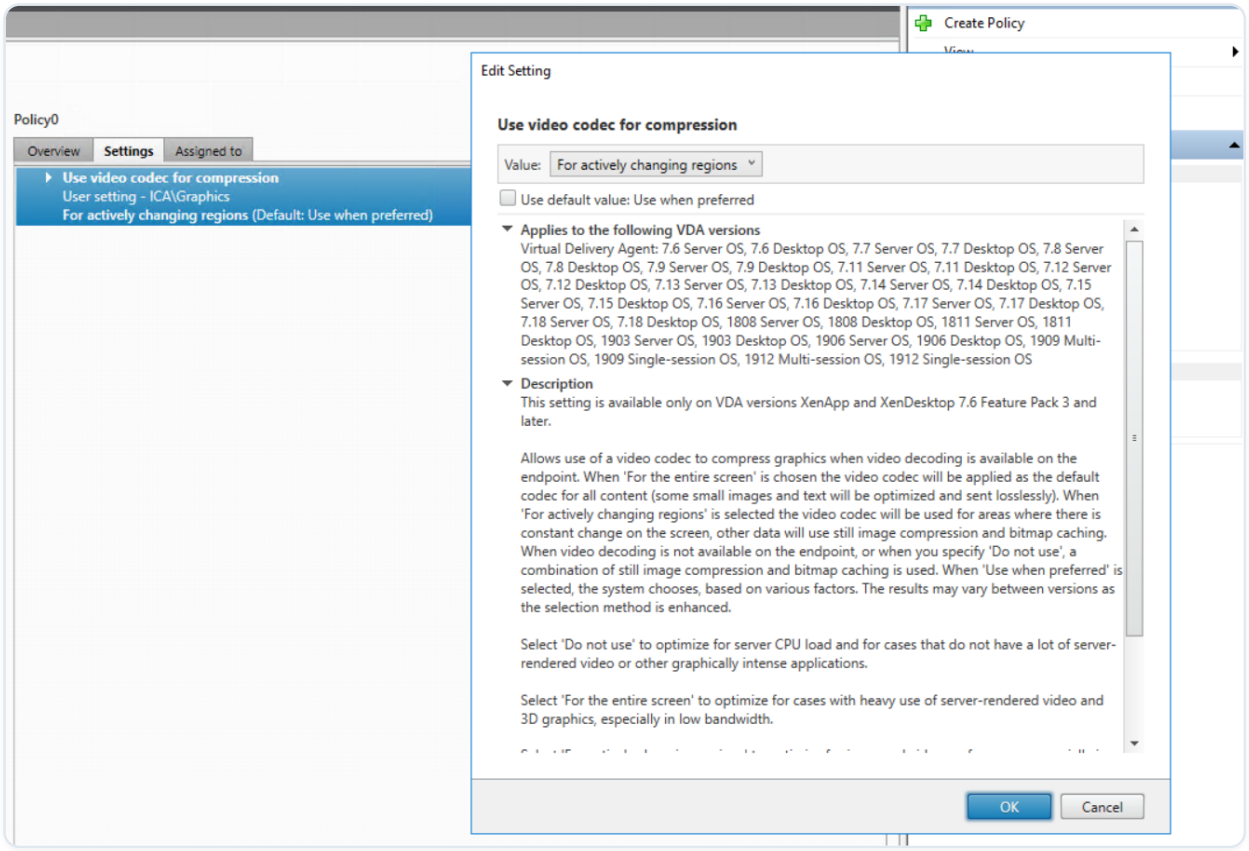
There are two major reasons that Session Recording scales well compared with competitive products:

- 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. **By default, recordings are 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**.

If lossless recordings are larger than your storage or network budget allows, you can enable lossy screen recording. Lossy screen recording encodes the session screen with a configurable frame rate, bit rate, I-frame interval, and image resolution scaling. It reduces the recording file size further, and it also speeds up fast forward and rewind during playback. The trade-off is image fidelity: text and fine detail are less sharp than in a lossless recording, so evaluate the compression options against your audit requirements before you deploy the feature broadly. Graphically intense workloads, such as CAD, mapping, or video applications, benefit the most, because they are also the workloads that produce the largest lossless recordings. You enable lossy screen recording through a session recording policy or an event response policy, and you tune the compression options on the **Lossy Screen** tab of Session Recording Agent Properties. For more information, see Enable or disable lossy screen recording.



- 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.

- Set the MSMQ message storage limit explicitly, and verify the value on every Session Recording server. If no limit is configured, MSMQ can consume all the physical memory that is available on the server before it starts queuing to disk. Size the limit for the burst and outage duration you want to tolerate, and keep it below half of the physical RAM, as described in Scaling up.
- Plan capacity on the system drive, not only on the message and recording drives. MSMQ tracks queued data with a mapping file on the system drive, and that file grows with the volume of data held in memory. A server that is backlogged for a long period consumes system drive space as well as memory and message-store space.

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.

Apply the same rule when you size a load-balanced pool, not only a single server. Divide your estimated data input rate by 50% of the processing rate of one server to get the number of servers that the pool needs to carry the steady-state load. Then add one more server, so that the pool still has spare capacity while one server is down for maintenance, upgrade, or a fault. For example, if your estimated input rate is 10 Mbps and one server can process 5.0 Mbps, target 2.5 Mbps per server. You therefore need four servers to carry the load, plus one for redundancy: five servers in total.

Sizing a pool at 100% of its aggregate capacity leaves nothing for the 9 o'clock rush, and it means that losing a single server pushes every remaining server into a permanent backlog. As described earlier in this article, a backlogged server triples its disk IOPS while the queues drain, so an under-sized pool recovers from a burst or an outage far more slowly than a simple capacity calculation suggests. For more information about deploying multiple Session Recording servers behind a load balancer, see Load balance Session Recording servers.

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

PERFORMANCE OBJECT	COUNTER NAME	DESCRIPTION
		maximum processing rate of the Storage Manager.
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`

PERFORMANCE OBJECT	COUNTER NAME	DESCRIPTION
		counter that measures the processing rate of data. If the network rate is greater than this value, messages build in the message queue.
Processor	`% Processor Time`	Worth monitoring even though CPU is unlikely to be a bottleneck.

Recognizing an overloaded server

On a healthy Session Recording server, the MSMQ counters show a store-and-flush pattern: Bytes in Queue and Messages in Queue rise during a burst and then fall back as the Storage Manager drains the queue. A sustained level with no downward trend means that the server is receiving data faster than it can process it. Note the following:

- In a well-sized deployment, Bytes in Queue does not exceed the MSMQ message storage limit that you configured.
- Bytes in Queue and available memory are directly related. As Bytes in Queue rises, available memory falls. When queued data cannot be flushed to disk fast enough, MSMQ also grows its mapping file on the system drive, so system drive usage rises at the same time.
- If the MSMQ message storage limit is reached, MSMQ logs Event ID 2183 in the Application log with the message “Machine MSMQ storage quota was exceeded or there is insufficient disk space. No more messages can be stored in user queues.” This event means that the server is receiving more data than it can handle. Raising the storage quota only defers the problem; add Session Recording servers instead. For more information, see Scaling out.

Size Session Recording servers on the maximum values you observe on each individual server, not on averages across the pool. Averages hide the bursts that actually cause data loss. Averages are useful for a different purpose: comparing the effect of a configuration change, such as moving to a different storage back end.

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.

CPU

For a high-performance Session Recording server, at least a dual CPU or dual core CPU is recommended. To let the Storage Manager use more than one core for incoming recorded data, enable the dual message queue.

The Session Recording server creates two data queues, and the Storage Manager runs a separate consumer thread for each of them. By default, every Session Recording agent sends to the first queue only, so the second consumer thread stays idle. When you enable the dual message queue, the agents spread their recorded data across both queues, the two consumer threads process it in parallel, and the server can use a second core productively. Adding CPU capacity beyond two cores helps only if the recorded data is spread across at least the same number of queues. The Session Recording server and agent must both be version 2507 or later. For more information, see Configure the dual message queue.

Processor architecture

64-bit processor architecture is recommended but an x86 processor type is also suitable.

Memory

8 GB of RAM is recommended for a Session Recording server. For a large-scale deployment, increase the RAM and the MSMQ message storage limit together. More message storage lets the server absorb a longer burst, fault, or maintenance window before recorded data is discarded, as described in Bursts and faults, and more RAM keeps that larger backlog manageable.

Keep the MSMQ message storage limit below half of the physical RAM on the server. If the storage limit approaches the size of the physical RAM, the server pages heavily at exactly the moment it is already backlogged, which slows the drain rate instead of improving it. To set the limit, open **Computer Management > Services and Applications > Message Queuing, right-click Message Queuing**, click **Properties**, and set **Limit message storage to (KB)** on the **General** tab. This is a computer-wide setting; the per-queue quotas of the Session Recording data queues are set to unlimited by the installer.

Memory and message storage absorb bursts. They do not raise the steady-state processing rate of a server. If the queues on a server stay high instead of draining between bursts, the server is receiving more data than it can process, and adding memory only lets it fall further behind before data is discarded. In that situation, add servers rather than memory. For more information, see Scaling out.

> **Note:**
>
> Configure your antivirus software for the Session Recording server before you benchmark it. Real time scanning of the MSMQ message store, the recording storage folders, and the Session Recording service processes can impose a significant performance cost on how quickly the Storage Manager processes data, and it can make an adequately sized server appear to be under-sized.

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.

Scale out in preference to scaling up. Each Session Recording server has a throughput limit that is usually reached in MSMQ, in how fast the Storage Manager can drain the queues to disk, rather than in the storage back end. Beyond that limit, a larger server does not process meaningfully more data; it only queues more of it. Several smaller Session Recording servers therefore handle a given load more efficiently than a smaller number of large ones, and they keep the queue depth on each server low. Scenarios in which scaling up resolves a Session Recording throughput problem are uncommon.

Size the load balancer as well as the servers. All recorded session data traverses it, so measure the throughput that your deployment generates and confirm that the load balancer, and its throughput licensing where that applies, can carry it. An under-sized load balancer becomes the bottleneck no matter how many Session Recording servers sit behind it.

For more information about deploying and configuring a load balanced pool, see Load balance Session Recording servers.

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 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 LEVEL	TYPE	MINIMUM NUMBER OF DISKS	DESCRIPTION
RAID 5	Striped set with distributed parity	3	Provides high read performance with redundancy but at the cost of slower write performance. 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.

Session recording events change this figure significantly. When you enable event logging in a session recording policy — for example, application starts and ends, file transfers, clipboard activity, web browsing activity, USB device usage, or RDP connections — each logged event is stored as its own row in the database, together with the event text and any associated event data. An active session can generate hundreds or thousands of events per hour, so the per-session database footprint grows from about 1 KB to well beyond it. In deployments that enable all event types for several hundred concurrent sessions, the database can grow by several GB.

Before you enable event logging at scale, do the following:

- Enable only the event types that your compliance or audit requirements actually need. Events that fire on ordinary user activity, such as application starts and ends and web browsing activity, generate by far the most rows.
- Run a pilot with a representative group of users, measure the growth of the database over several days, and extrapolate that growth to your full user count and your retention period.
- Size the database, its storage, and its retention policy for the measured growth, and review the sizing whenever you change which event types are logged.

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. The 4,000,000-session figure assumes that event logging is disabled. With event logging enabled, an Express Edition database can reach its 10 GB limit after far fewer sessions, so use a full edition of Microsoft SQL Server if you enable event logging beyond a pilot.

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 **write** load on the database is unlikely to be stressed. **For a deployment that records a moderate number of sessions and logs few or no events**, 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.

Host the Session Recording database on a separate SQL Server instance, preferably on a separate machine, when any of the following applies:

- The database holds a large number of recording records, because you record many sessions, you keep a long retention period, or both.
- You have enabled event logging broadly, so that the event table grows to millions of rows.
- Administrators frequently search recordings by event, in the Session Recording web player or through the REST API.

Searching recordings by event is a read-intensive query that runs on demand against a large table, and it competes for CPU, memory, and disk I/O with everything else on the same SQL Server instance. Where the Session Recording database shares an instance with the Citrix Virtual Apps and Desktops site database, this competition works in both directions: a heavy recording search can affect brokering and session launches, and a busy site database can make recording searches slow. Separating the two databases also lets you size, back up, and maintain each of them independently.

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.

You can install the Session Recording server and agent on an Azure AD joined machine and enable Azure AD support for them. Later when you configure various policies and playback permissions from the cloud, you can specify Azure AD users and groups who launch sessions from Azure AD joined machines. The **Enable Azure AD support** option is **not** available on the GUI when you install the Session Recording server using the Citrix Virtual Apps and Desktops™ installer.

This article contains the following sections:

Installation checklist

Use Citrix® scripts to install the Windows roles and features prerequisites

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 hardware and software requirements for the 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 the Citrix 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.

(Required only for msi installation) Use Citrix scripts to install the Windows roles and features prerequisites

For Session Recording to work properly, use the following Citrix scripts to install the necessary Windows roles and features prerequisites before installing Session Recording:

- `InstallPrereqsforSessionRecordingAdministration.ps1`

```
<#

.Synopsis

    Installs Prereqs for Session Recording Administration

.Description

    Supports Windows Server 2025, Windows Server 2022, Windows Server
2019.

    Install below windows feature on this machine:

    -Application Development

    -Security - Windows Authentication

    -Management Tools - IIS 6 Management Compatibility

        IIS 6 Metabase Compatibility
```

```
        IIS 6 WMI Compatibility

        IIS 6 Scripting Tools

        IIS 6 Management Console

    -Microsoft Message Queuing (MSMQ), with Active Directory
integration disabled, and MSMQ HTTP support enabled.

#>

function AddFeatures($featurename)

{

    try

    {

        $feature=Get-WindowsFeature | ? {$_.DisplayName -eq
$featurename -or $_.Name -eq $featurename}

        Add-WindowsFeature $feature

    }

    catch

    {

        Write-Host "Addition of Windows feature $featurename failed"

        Exit 1

    }

    Write-Host "Addition of Windows feature $featurename succeeded"

}



$system= gwmi win32_operatingSystem | select name
```

```
if (-not (($system -Like '*Microsoft Windows Server 2025*') -or
($system -Like '*Microsoft Windows Server 2022*') -or ($system -Like
'*Microsoft Windows Server 2019*')))

{

    Write-Host("This is not a supported server platform. Installation
aborted.")

    Exit

}



# Start to install Windows feature

Import-Module ServerManager



AddFeatures('Web-Asp-Net45') #ASP.NET 4.5

AddFeatures('Web-Mgmt-Console') #IIS Management Console

AddFeatures('Web-Windows-Auth') # Windows Authentication

AddFeatures('Web-Metabase') #IIS 6 Metabase Compatibility

AddFeatures('Web-WMI') #IIS 6 WMI Compatibility

AddFeatures('Web-Lgcy-Scripting')#IIS 6 Scripting Tools

if (($system -Like '*Microsoft Windows Server 2022*') -or ($system
-Like '*Microsoft Windows Server 2019*'))

{

    AddFeatures('Web-Lgcy-Mgmt-Console') #IIS 6 Management Console

}
```

```
AddFeatures('MSMQ-HTTP-Support') #MSMQ HTTP Support

AddFeatures('web-websockets') #IIS Web Sockets

AddFeatures('NET-WCF-HTTP-Activation45') #http activate

AddFeatures('Web-IP-Security')#IIS-IPSecurity
```

- `InstallPrereqsforSessionRecordingAgent.ps1`

```
<#

.Synopsis

    Installs Prereqs for Session Recording Agent

.Description

    Supports  Windows Server 2025, Windows Server 2022, Windows Server
2019, Windows Server 2016, windows 11, and Windows 10.

    Install below windows feature on this machine:

    -Microsoft Message Queuing (MSMQ), with Active Directory
integration disabled, and MSMQ HTTP support enabled.

#>

function AddFeatures($featurename)

{

    try

    {

        $feature=Get-WindowsFeature | ? {$_.DisplayName -eq
$featurename -or $_.Name -eq $featurename}

        Add-WindowsFeature $feature
```

```
    }
    catch
    {
        Write-Host "Addition of Windows feature $featurename failed"
        Exit 1
    }
    Write-Host "Addition of Windows feature $featurename succeeded"
}


# Start to install Windows feature


$system= gwmi win32_operatingSystem | select name


if (-not (($system -Like '*Microsoft Windows Server 2025*') -or
($system -Like '*Microsoft Windows Server 2022*') -or ($system -Like
'*Microsoft Windows Server 2019*') -or ($system -Like '*Microsoft
Windows Server 2016*') -or ($system -Like '*Microsoft Windows 11*') -or
($system -Like '*Microsoft Windows 10*')))
{
    Write-Host("This is not a supported platform. Installation
aborted.")
    Exit
}
```

```
if ($system -Like '*Microsoft Windows Server*')

{

    Import-Module ServerManager

    AddFeatures('MSMQ-Server') #Message Queuing

}

else

{

    try

    {

        dism /online /enable-feature /featurename:MSMQ-Server /all

    }

    catch

    {

        Write-Host "Addition of Windows feature MSMQ failed"

        Exit 1

    }

    write-Host "Addition of Windows feature MSMQ succeeded"

}
```

To install the Windows roles and features prerequisites, complete the following steps:

1. On the machine where you plan to install the Session Recording administration components:

    a. Make sure that the execution policy is set to **RemoteSigned** or **Unrestricted** in PowerShell.

```
Set-ExecutionPolicy RemoteSigned
```

b. Start a command prompt as an administrator and run the `powershell.exe -file InstallPrereqsforSessionRecordingAdministration.ps1` command.

   The script displays the features that are successfully added and then stops.

c. After the script runs, make sure that the execution policy is set to a proper value based on your company policy.

2. On the machine where you plan to install the Session Recording agent component:

a. Make sure that the execution policy is set to **RemoteSigned** or **Unrestricted** in PowerShell.

```
Set-ExecutionPolicy RemoteSigned
```

b. Start a command prompt as an administrator and run the `powershell.exe -file InstallPrereqsforSessionRecordingAgent.ps1` command.

   The script displays the features that are successfully added and then stops.

c. After the script runs, make sure that the execution policy is set to a proper value based on company policy.

Install Session Recording using the Citrix Virtual Apps and Desktops installer

Citrix Session Recording comprises the following components:

- Session Recording Administration (including the Session Recording database, Session Recording server, and Session Recording policy console)
- Session Recording agent
- Session Recording player
- Session Recording web player

While installing all the components on a single server is acceptable for a **proof of concept**, we recommend installing them on separate servers as follows:

- Install the Microsoft SQL Server on Machine A.

- Install the Session Recording server, Session Recording administrator logging, and Session Recording database on Machine B.

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

- Install the Session Recording policy console on Machine C.
- Install the Session Recording player on either Machine C or Machine D.
- Install the Session Recording agent on the VDA.

Install the Session Recording Administration components

Install the Session Recording agent

Install the Session Recording player

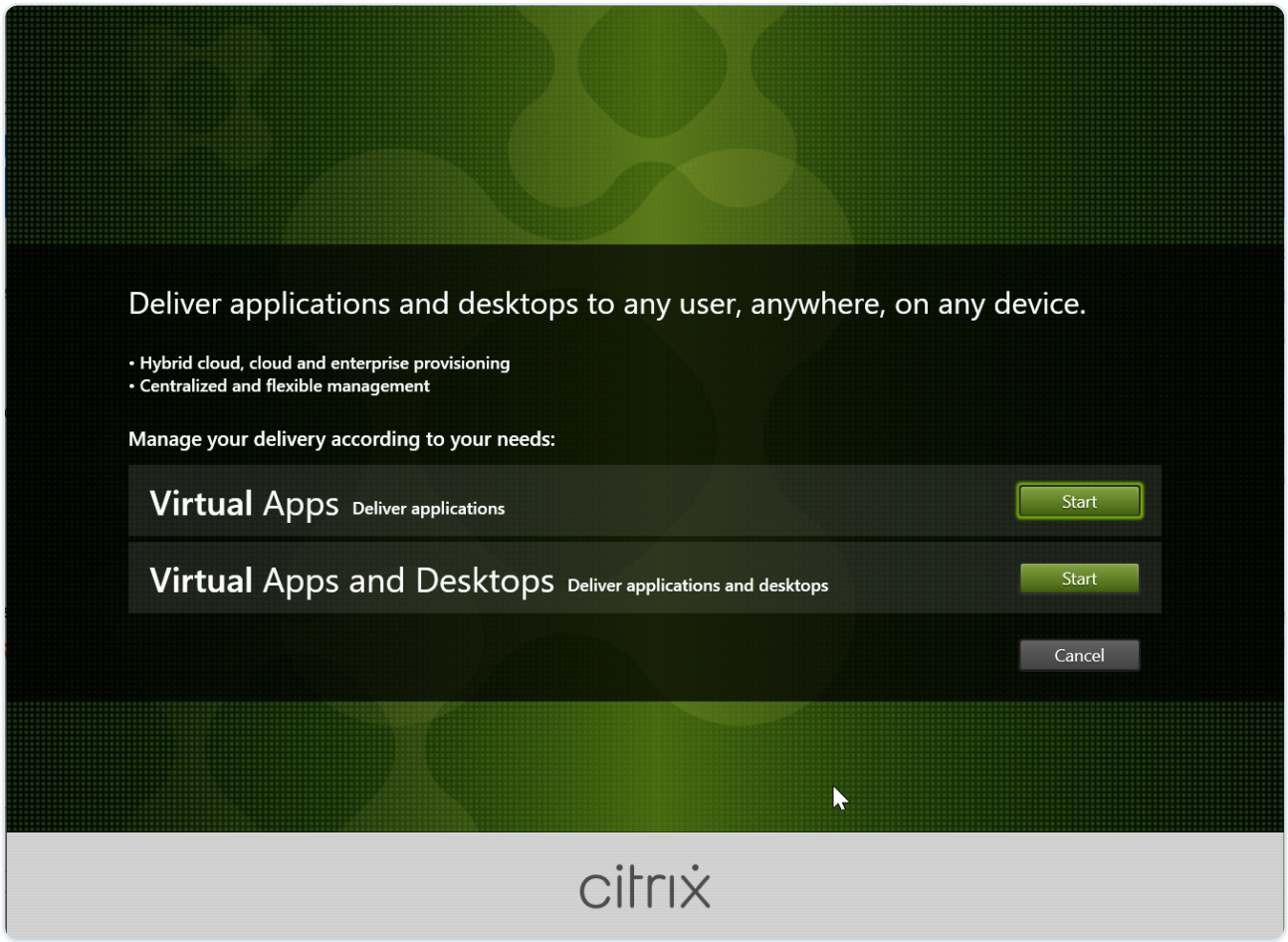
Install the Session Recording Administration components

> **Note:**
>
> By default, for secure, Session Recording work only on TLS enabled scenario, which means you need to bind a valid certificate on Session Recording IIS -> default web site. Do NOT specify hostname during binding.
>
> If you want to use http only for session recording, see Use HTTP as the communication protocol.
>
> 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

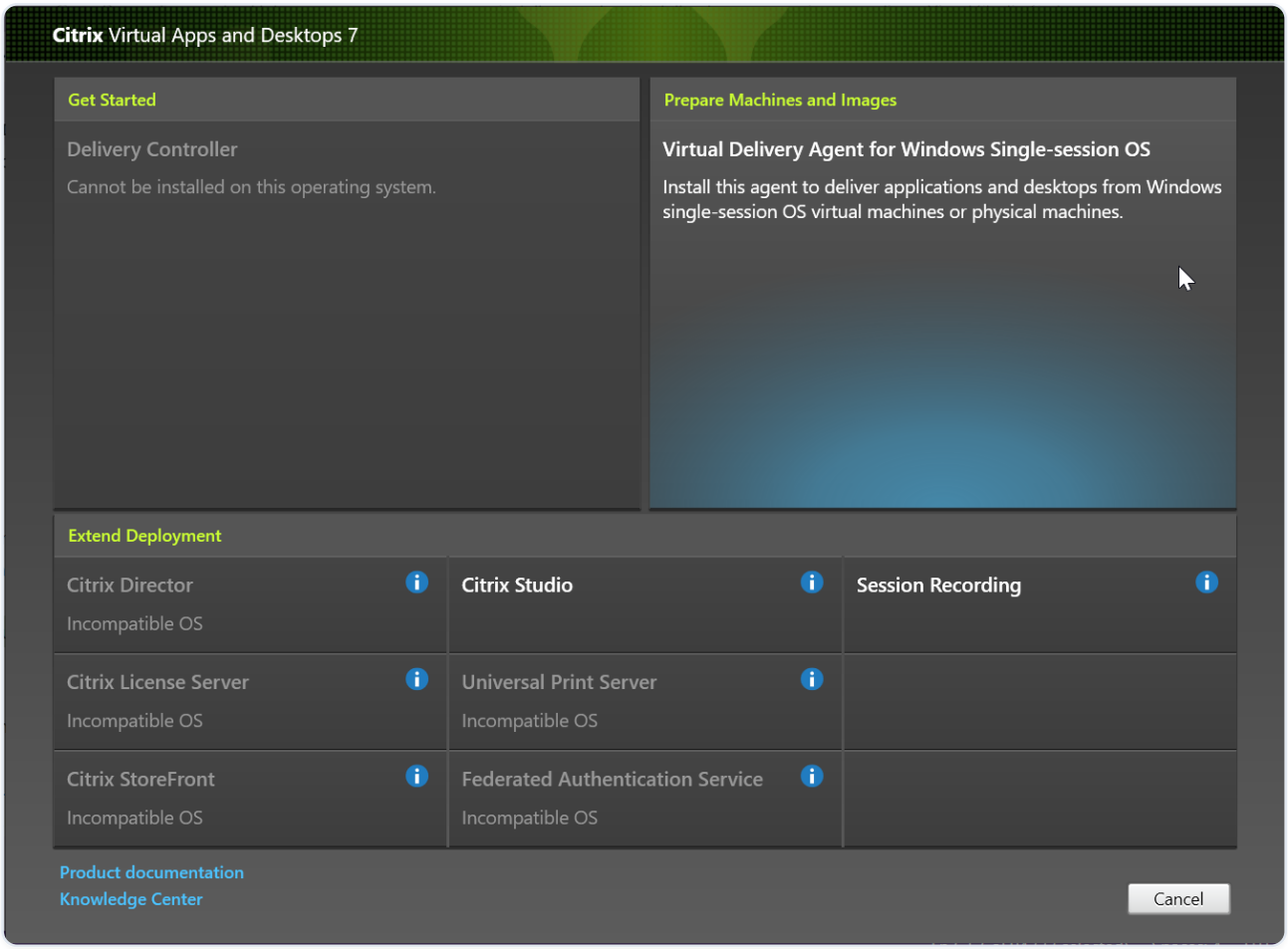
1. Use your Citrix account credentials to access the Citrix Virtual Apps and Desktops download page and download the product ISO file. Unzip the ISO file or burn a DVD of it.
2. Use a local administrator account to log on to the machine where you are installing the Session Recording Administration components. 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



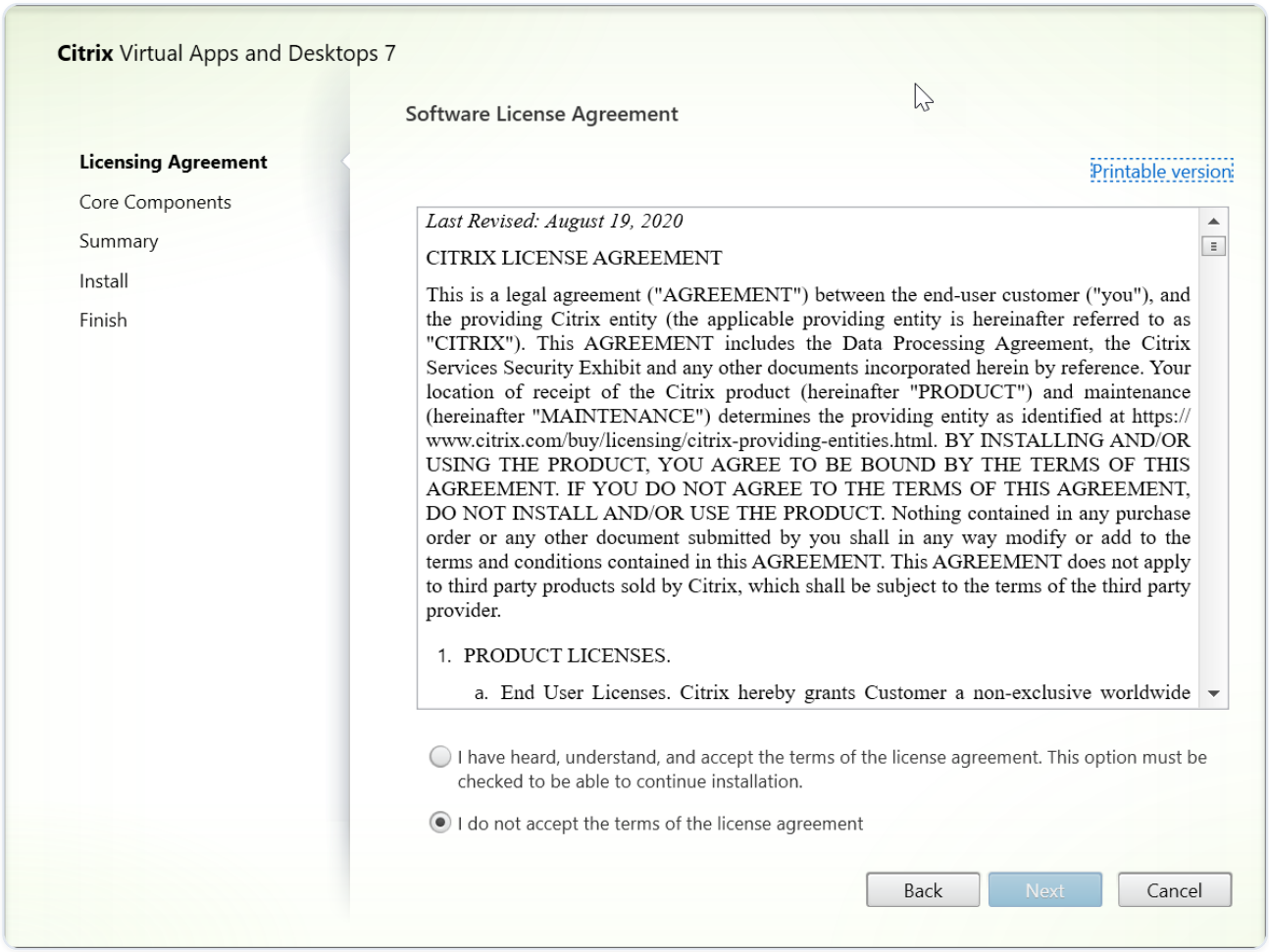
Click **Start** next to the product to install **Citrix Virtual Apps** or **Citrix Virtual Desktops™**.

Step 3: Select Session Recording



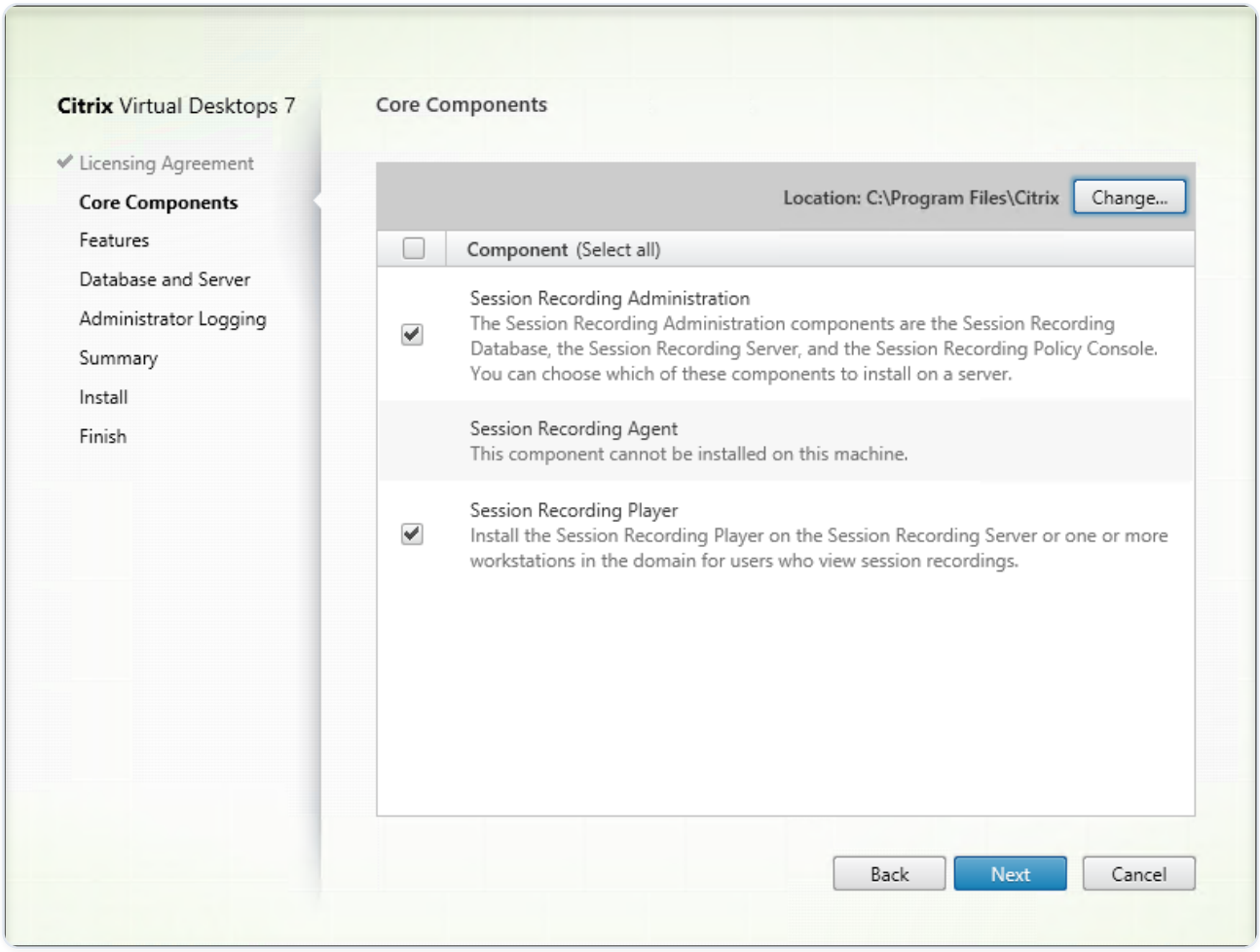
Select the **Session Recording** entry.

Step 4: Read and accept the license agreement



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

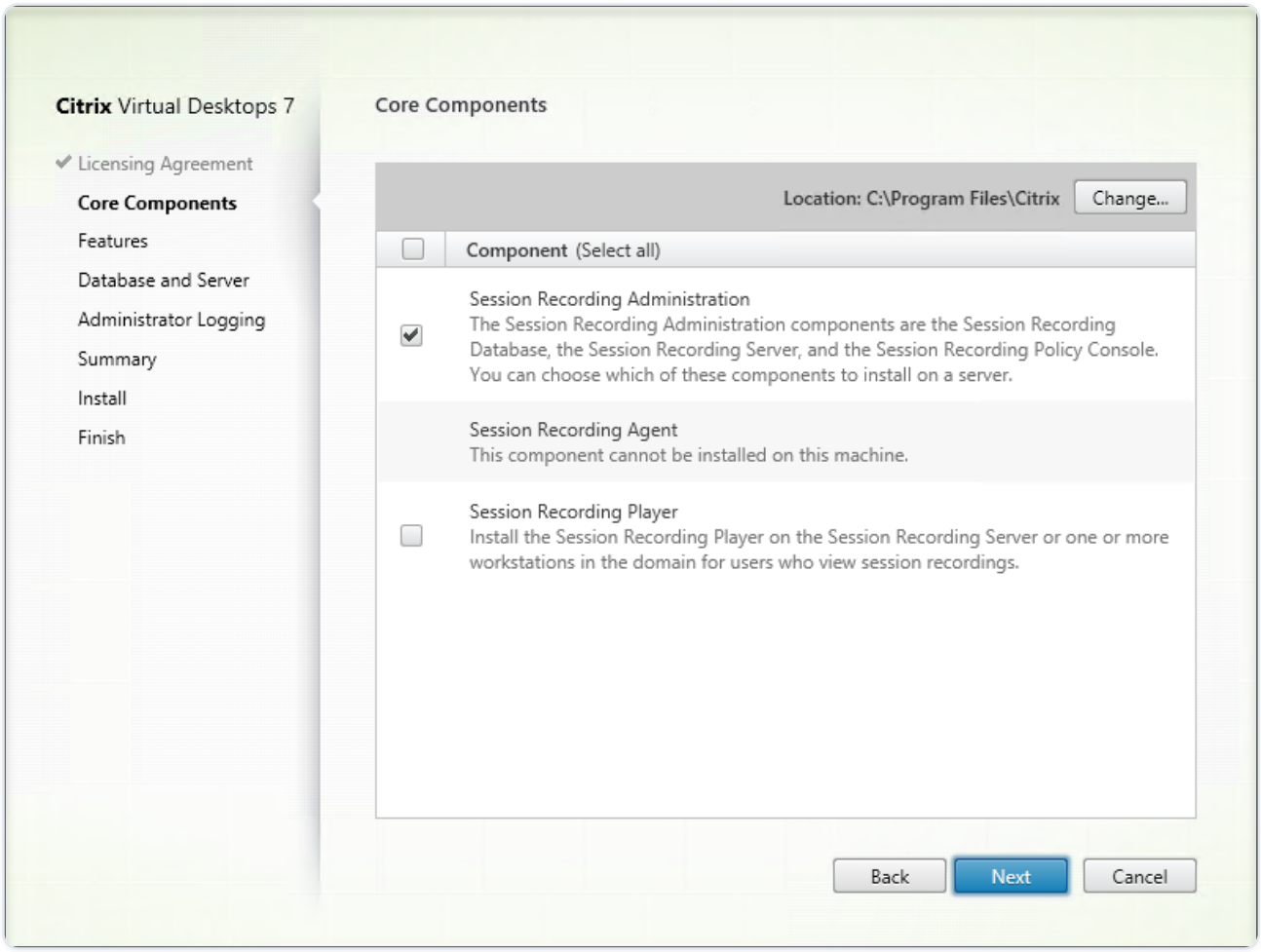
Step 5: Select the components to install and the installation location



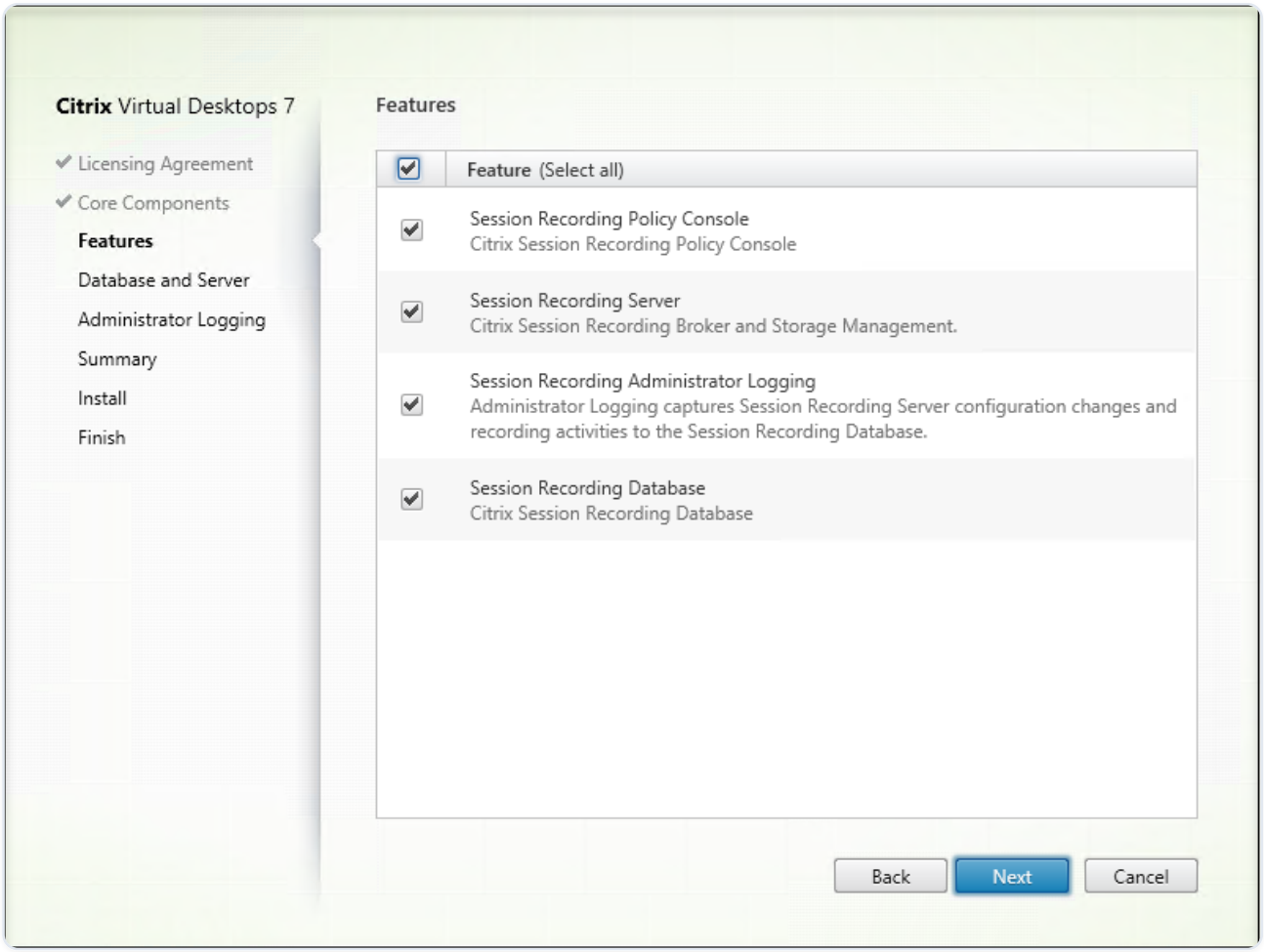
On the **Core Components** page:

- **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**.

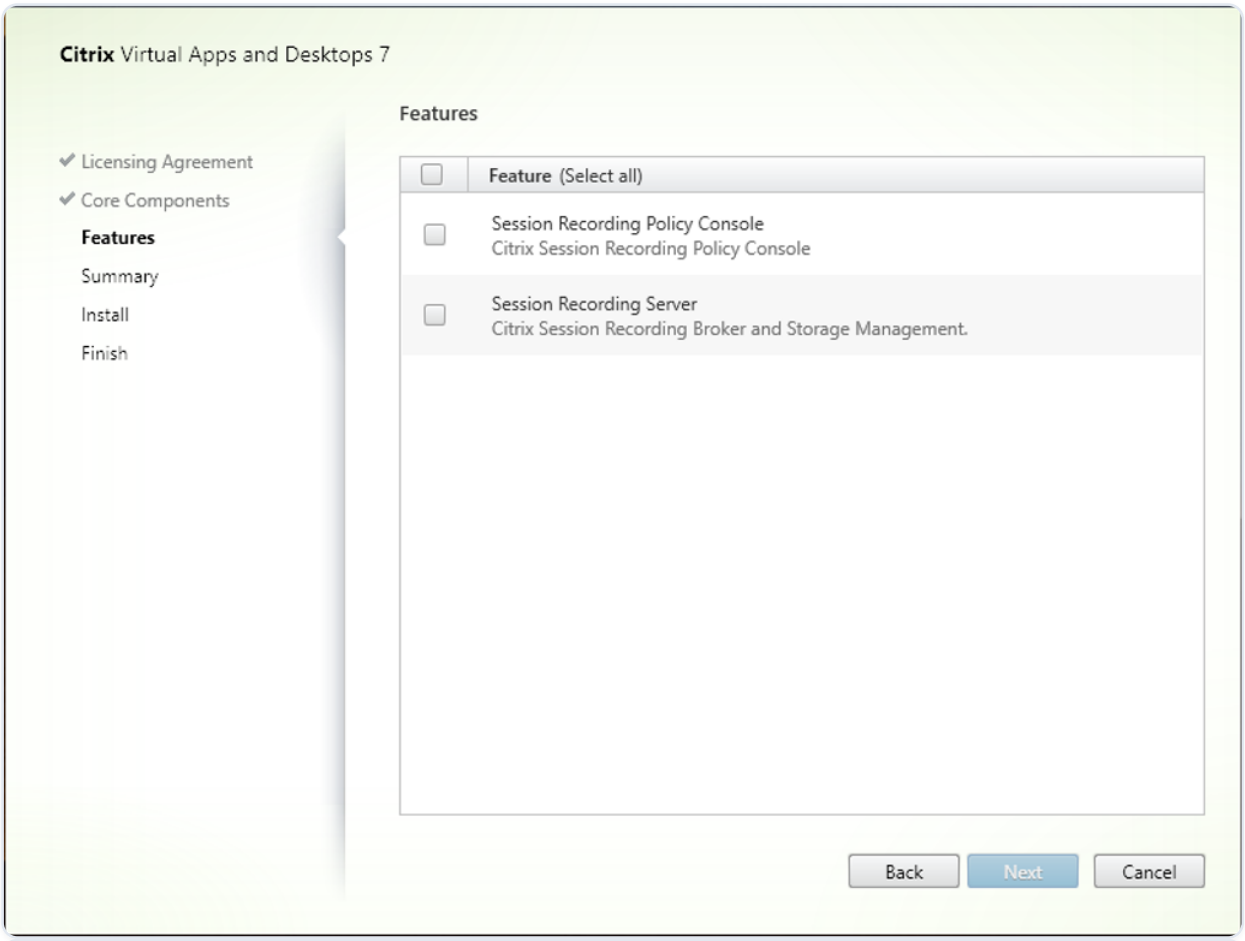

Citrix Virtual Desktops 7
Licensing Agreement
Core Components
Features
Database and Server
Administrator Logging
Summary
Install
Finish
Core Components
Location: C:\Program Files\Citrix
Change...
Component (Select all)
Session Recording Administration
The Session Recording Administration components are 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

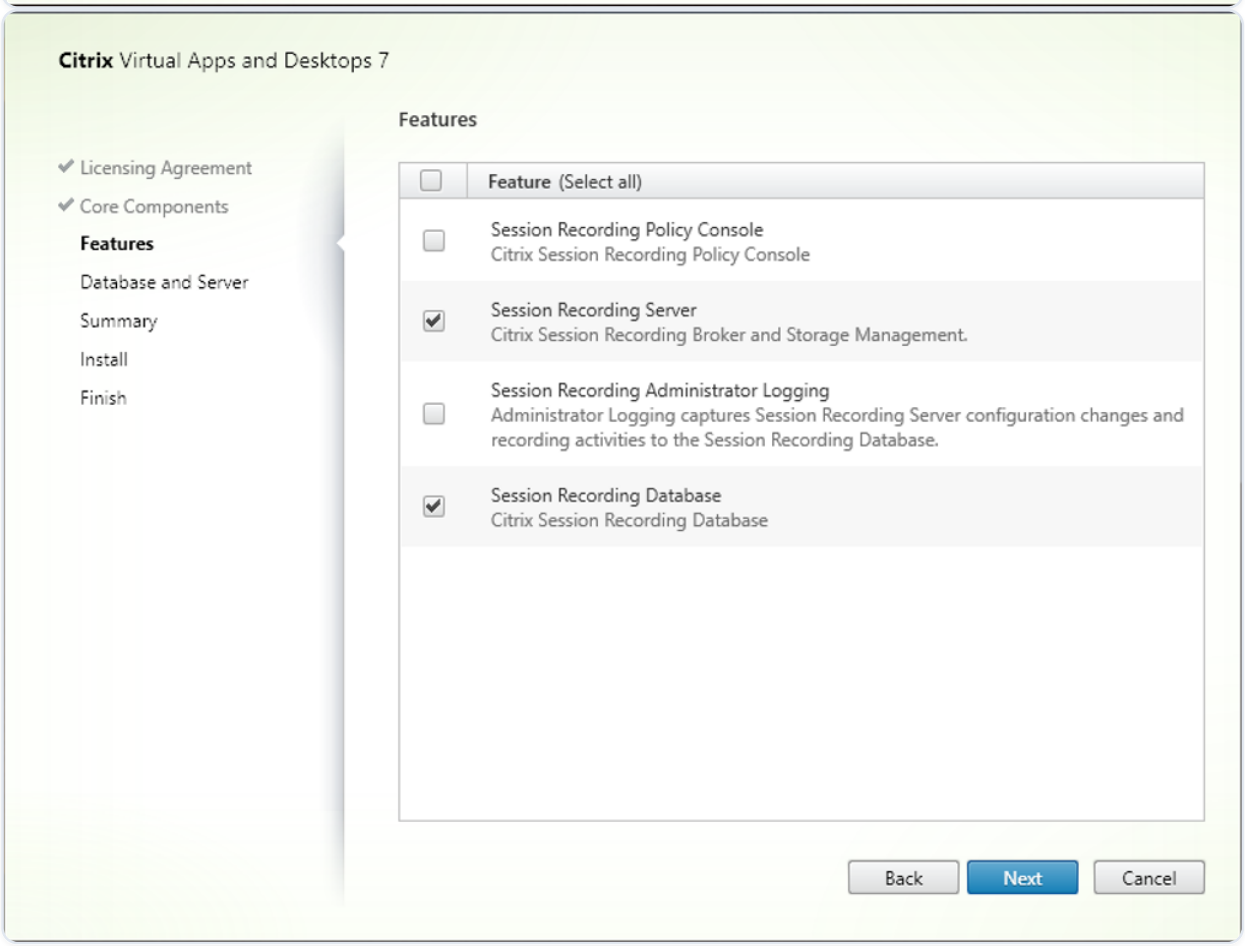
Step 6: Select the features to install



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. The Session Recording database is a mandatory subfeature of the Session Recording server. When the Session Recording server is selected for installation, the Session Recording database is also selected automatically and cannot be unselected.





- 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.
- **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.

- **Session Recording database**
  - 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
    - Google Cloud SQL Server
- **Session Recording admin 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.

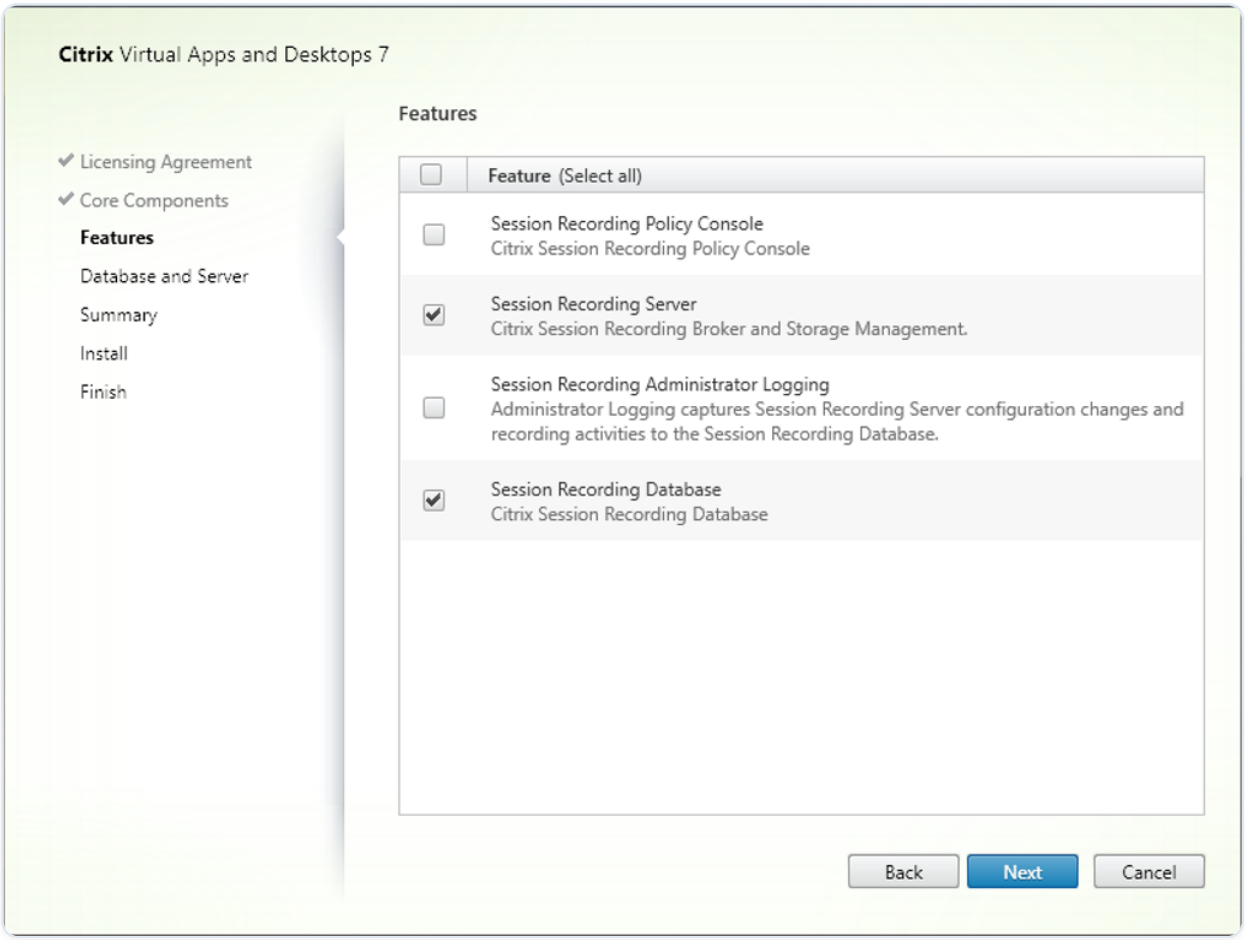
- **Session Recording policy console**

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

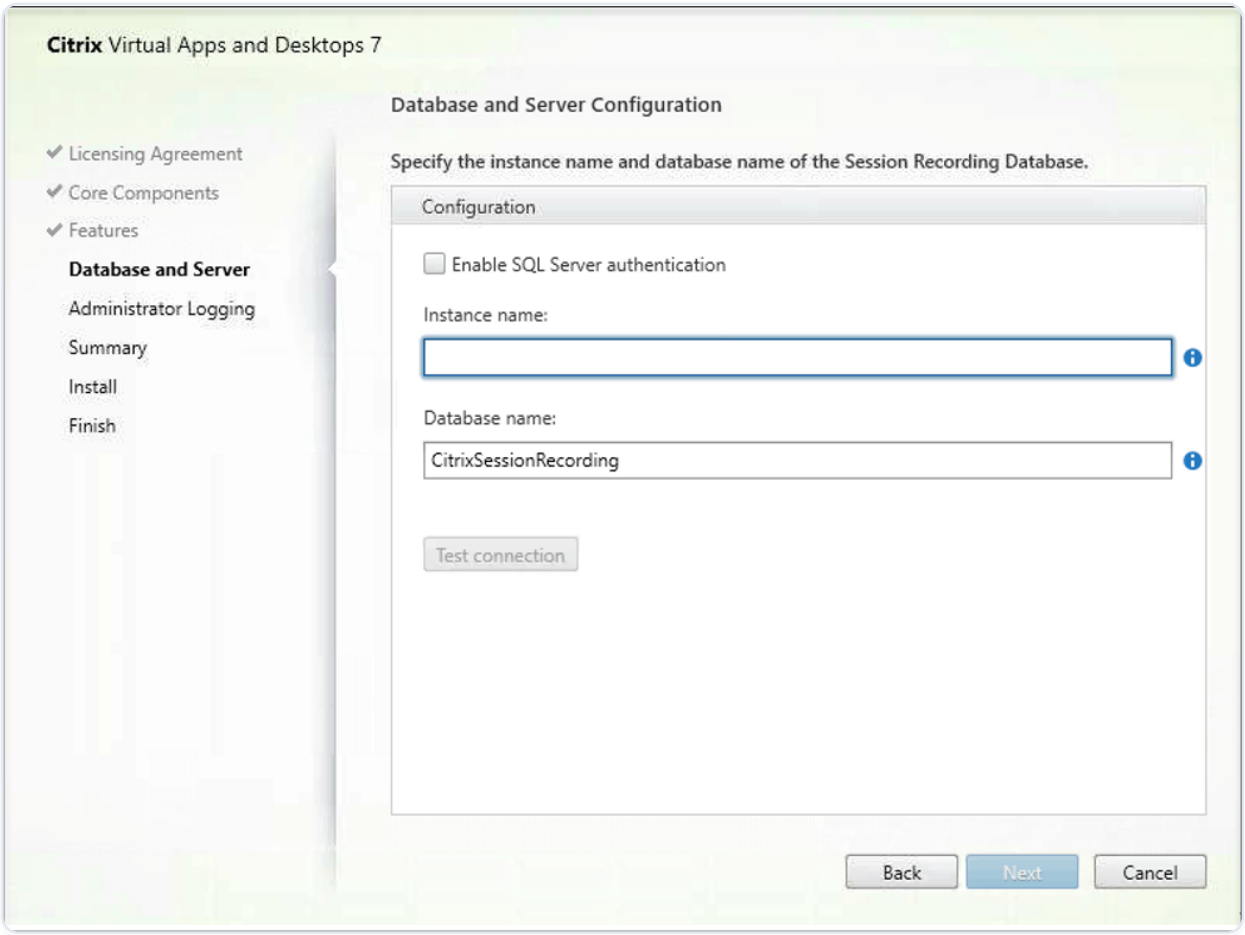
Step 6.1: Install the Session Recording server, database, and administrator logging

As described earlier, the Session Recording database is a mandatory subfeature of the Session Recording server and we recommend that you install the Session Recording administrator logging together with the Session Recording server at the same time. Therefore, this section walks you through installing the three components on the same machine.

1. On the **Features** page, select **Session Recording Server** and **Session Recording Administrator Logging**. With **Session Recording Server** selected, **Session Recording Database** is also selected automatically. Click **Next**.



2. On the **Database and Server Configuration** page, specify the instance name and database name of the Session Recording database, enable **SQL Server authentication** as needed, and click **Next**.

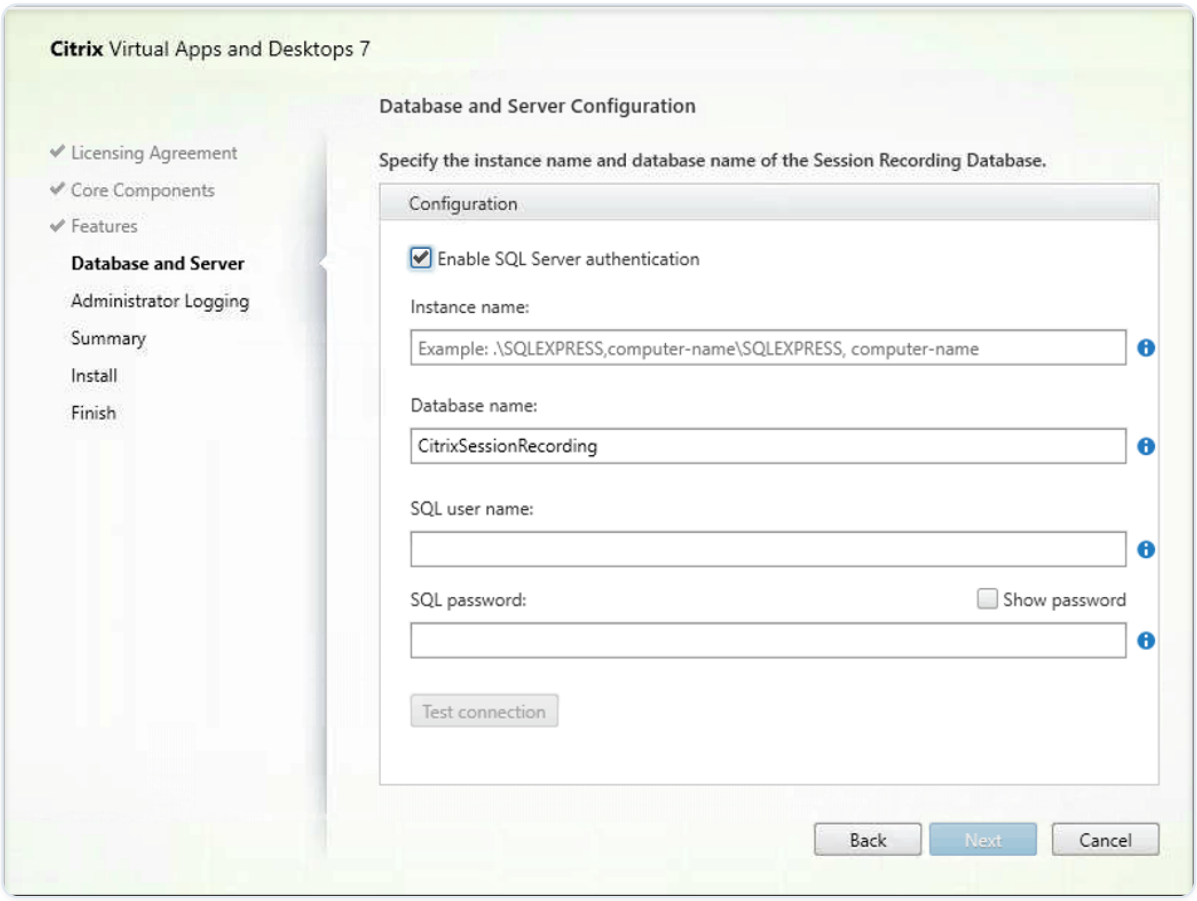


Note:

Starting with 2507, in addition to SQL Server authentication, Session Recording supports Entra ID (formerly Azure Active Directory) password and service principal authentication with Cloud Managed Entra id account. For more information, see Install the complete set of the Session Recording Administration components by using a single command.

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

- **Enable SQL Server authentication**: This option lets you connect to the Session Recording database using SQL Server authentication.



- **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 uses a custom port instead of the default 1433, append a comma and the custom port to the instance name. For example, type **DXSBC-SRD-1,2433** in the **Instance name** text box, where **2433** denotes the custom 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.

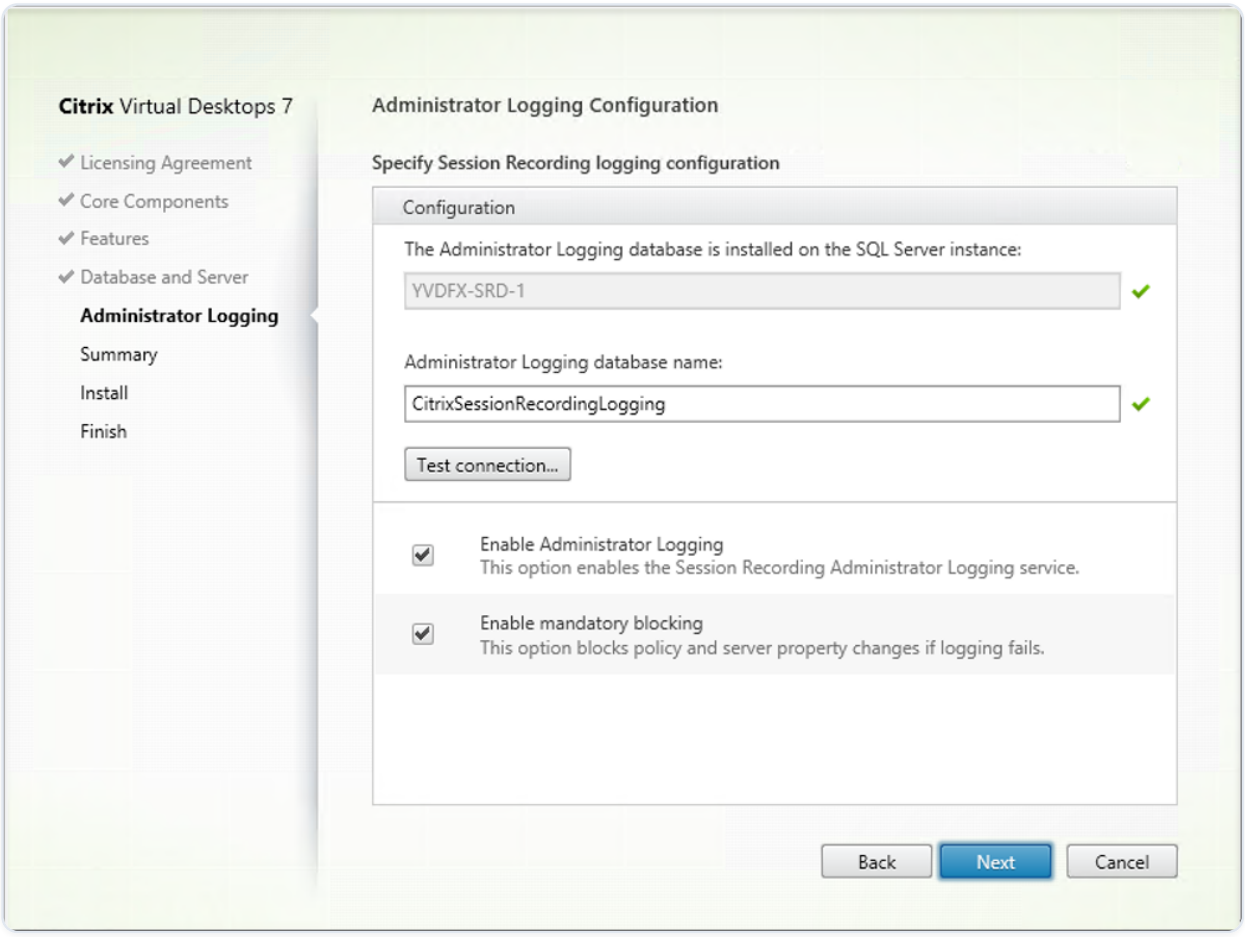
> **Note:**
>
> The Session Recording server default installation uses HTTPS/TLS to secure communications. If TLS is not configured in the default Internet Information Services (IIS) site of the Session Recording server, use HTTP. To do so, cancel the selection of SSL in the IIS Management Console by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

> **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 SQL Server instance. 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**.

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. Starting with the 2411 release, you can install the Session Recording admin logging database on a separate instance from the Session Recording database. To do so, complete the following steps before installing them:

  a. Go to the machine where you are going to install the Session Recording server.

  b. Open the Registry Editor.

  c. Modify the registry:

     - Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`.
     - Add the `SmAudDatabaseLoggingState` DWORD (32-bit) value and set the value data to `1`.
     - Add the `SmAudDatabaseLoggingInstance` value and set the value data to the instance name where you want to install the Session Recording admin logging database.

Later when you install the databases, the Session Recording admin logging database is installed on the separate instance specified by the `SmAudDatabaseLoggingInstance` registry value. You must configure the same authentication mode for both databases (SQL Server authentication, Windows authentication, or Microsoft Entra ID authentication) and grant identical user permissions.

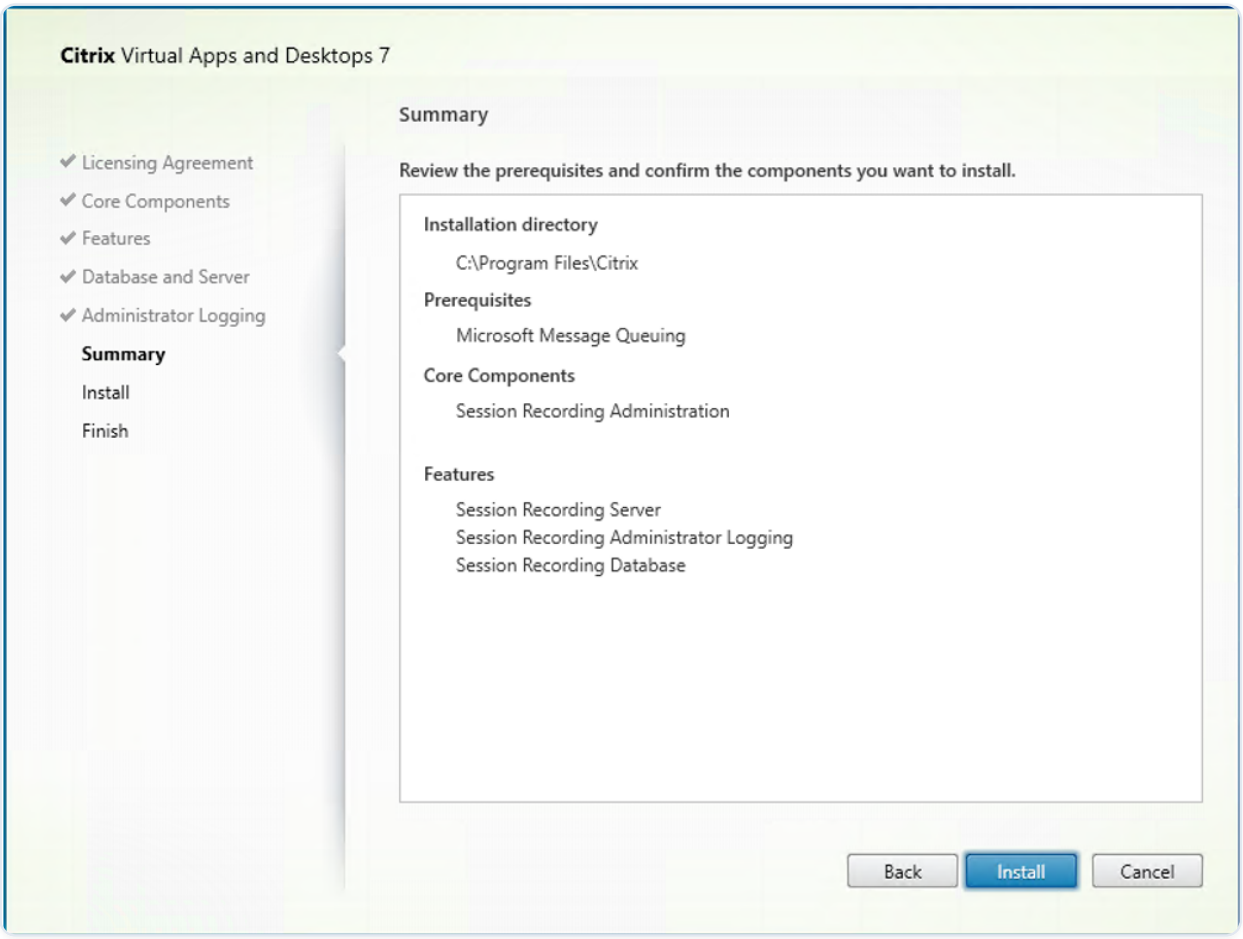
- **Administrator Logging database name**: To install the Session Recording administrator logging feature, type a custom database name for the administrator logging database in this text box or use the default database name **CitrixSessionRecordingLogging** that is preset in the text box.

  > **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.

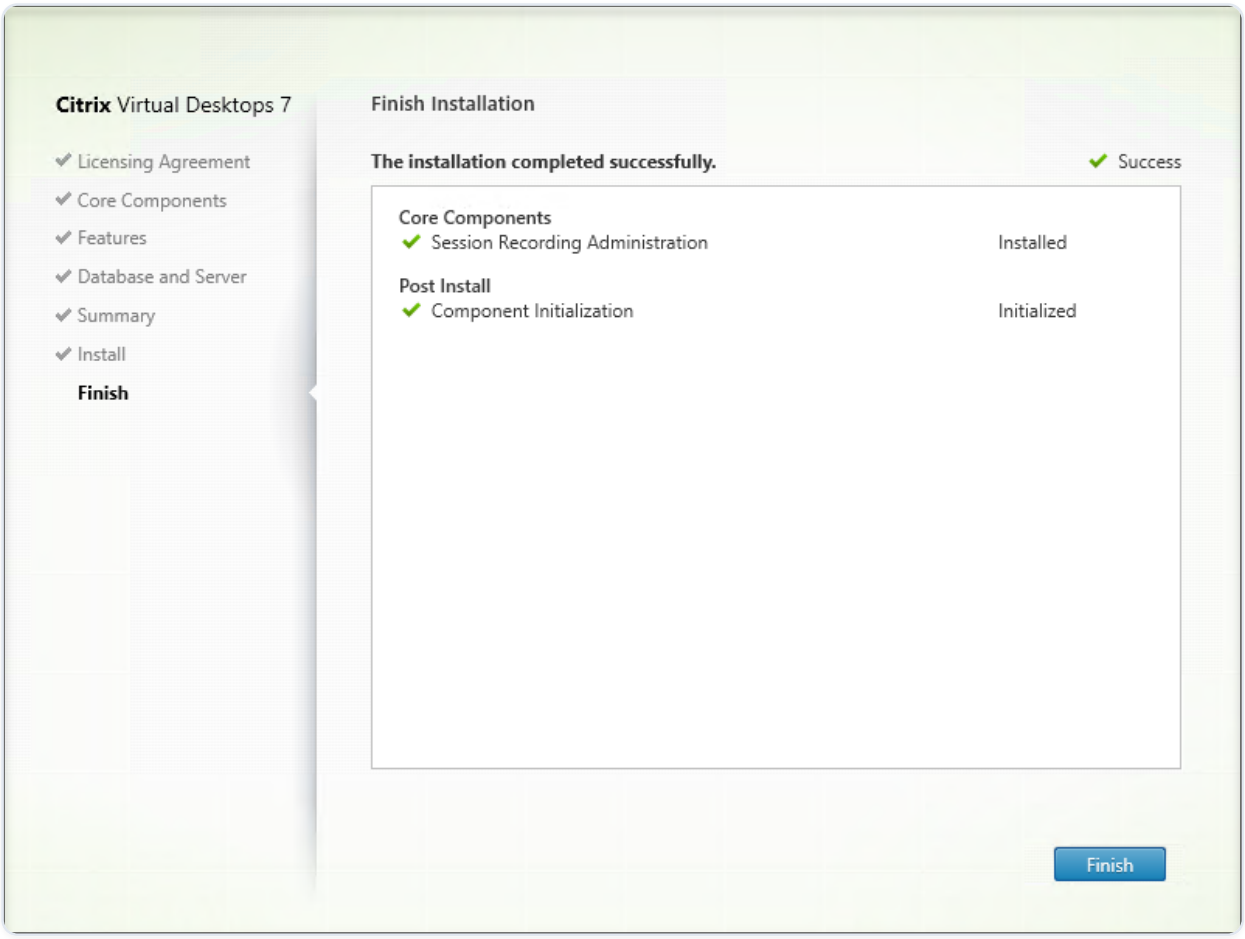
Click **Next** to continue the installation.

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.



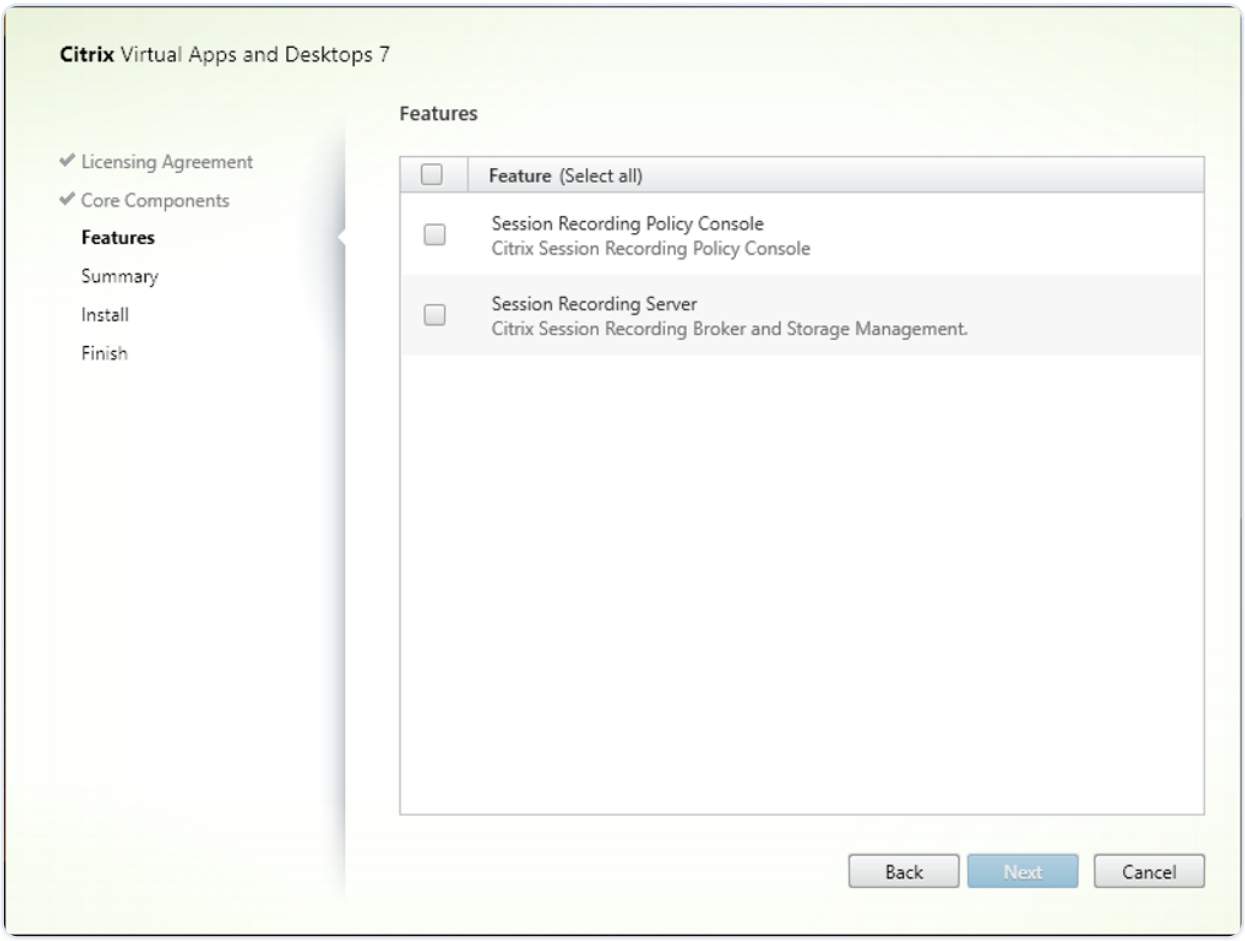
The **Finish Installation** page shows green check marks for all the prerequisites and components that have been installed and initialized successfully.

Click **Finish** to complete the installation of the Session Recording server, database, and administrator logging.

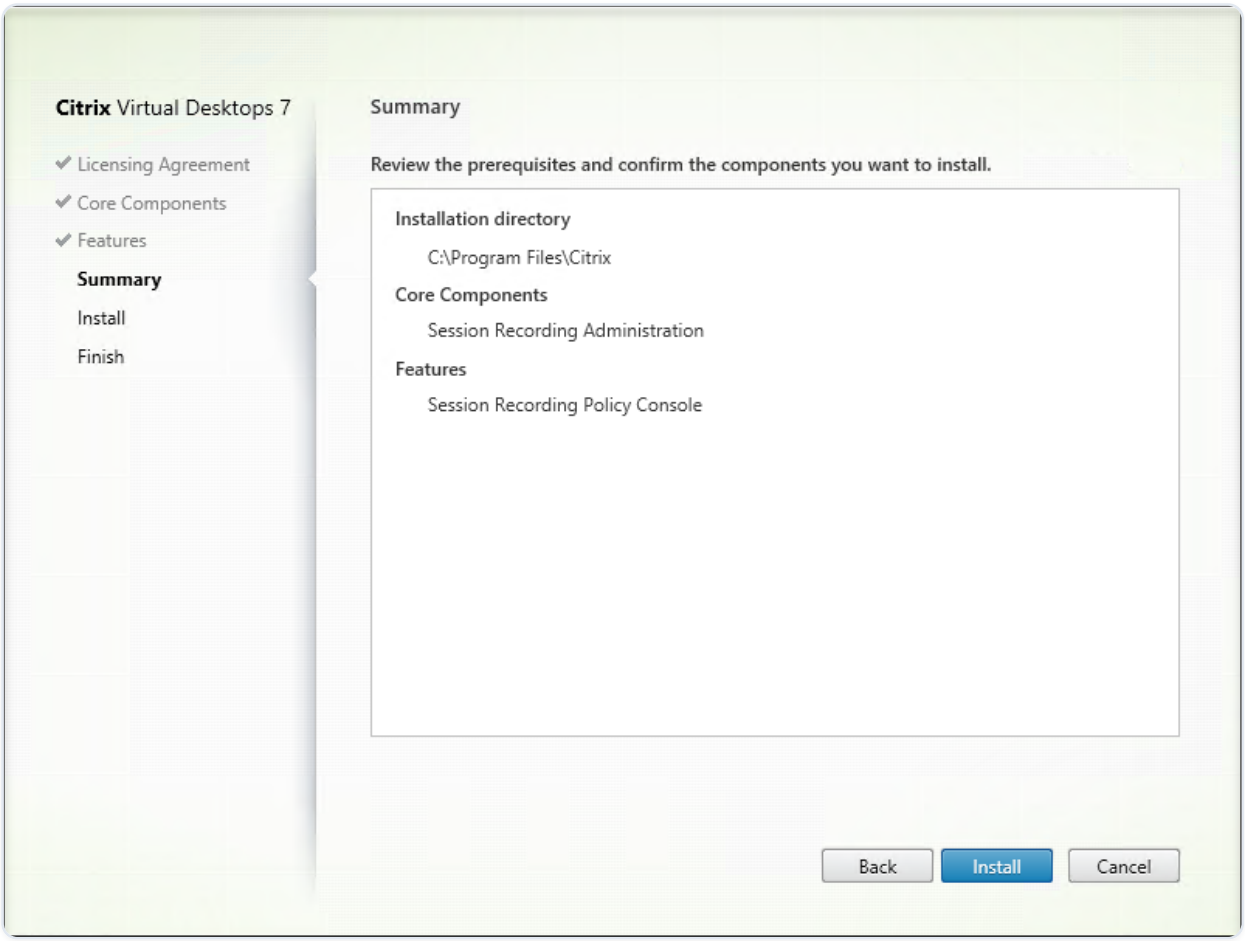
Step 6.2: Install the Session Recording policy console

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

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

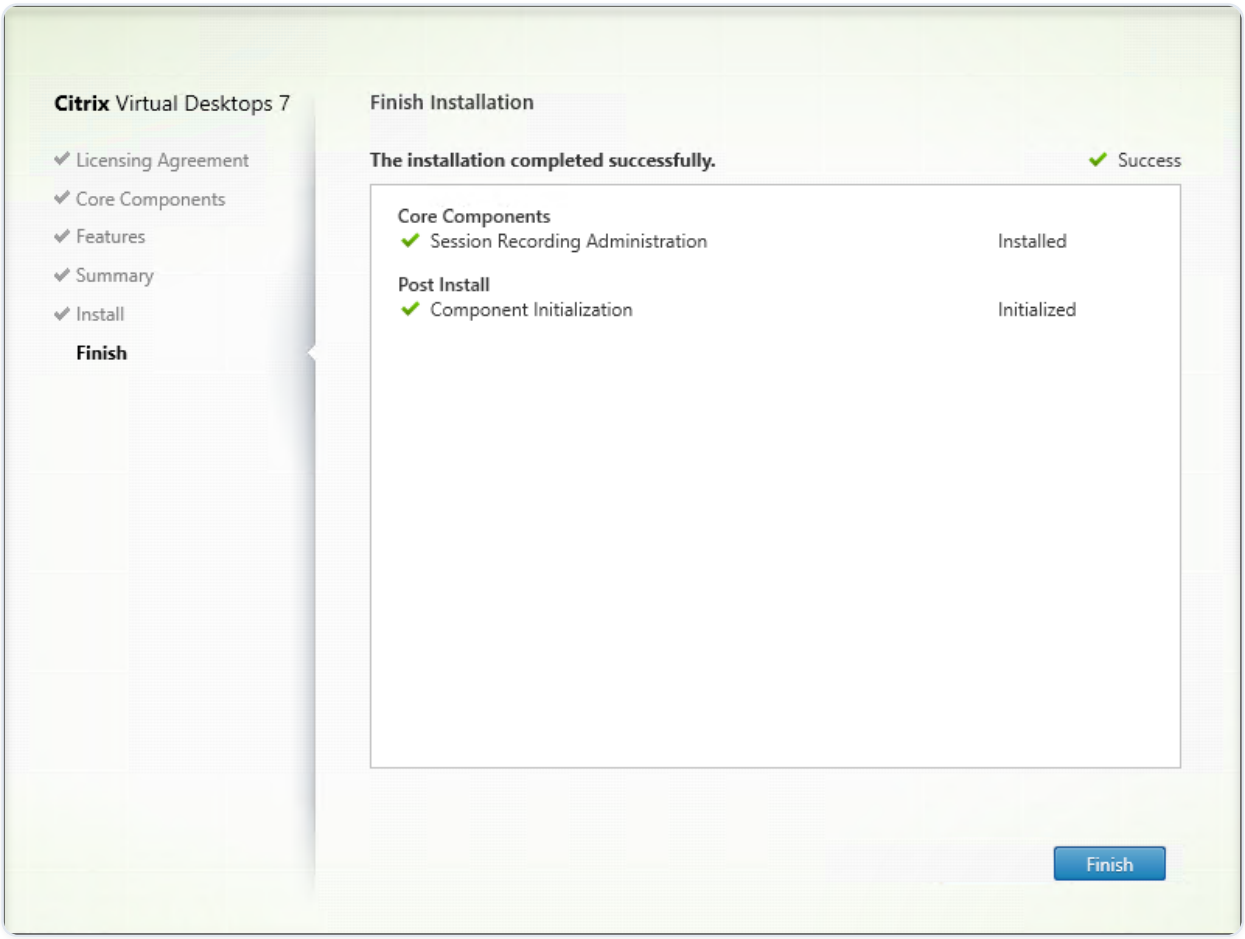


2. Review the prerequisites and confirm the installation.



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 components 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

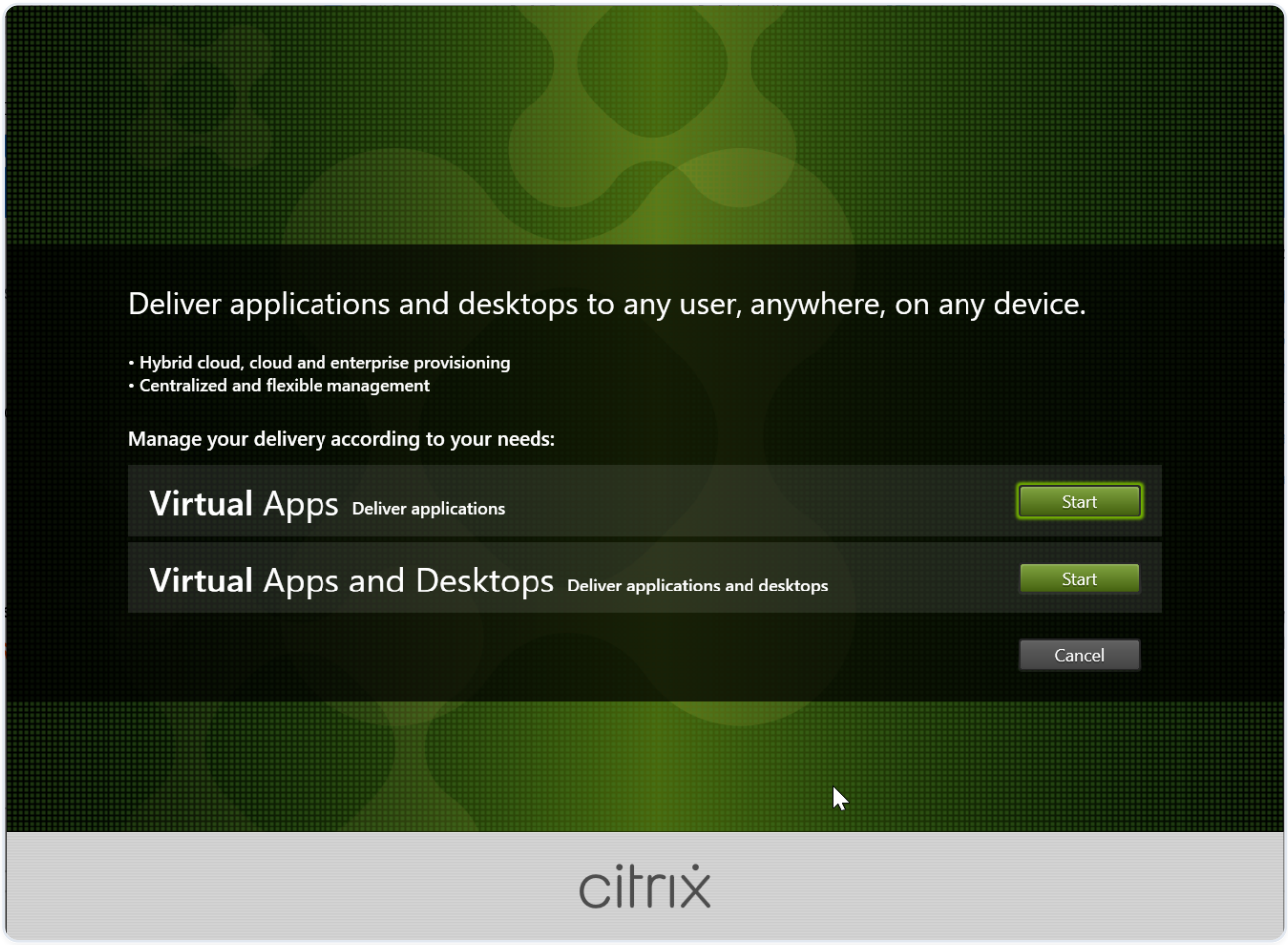
The Session Recording agent is a component installed on each VDA for multi-session OS or single-session OS to enable recording. It is responsible for recording session data.

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.

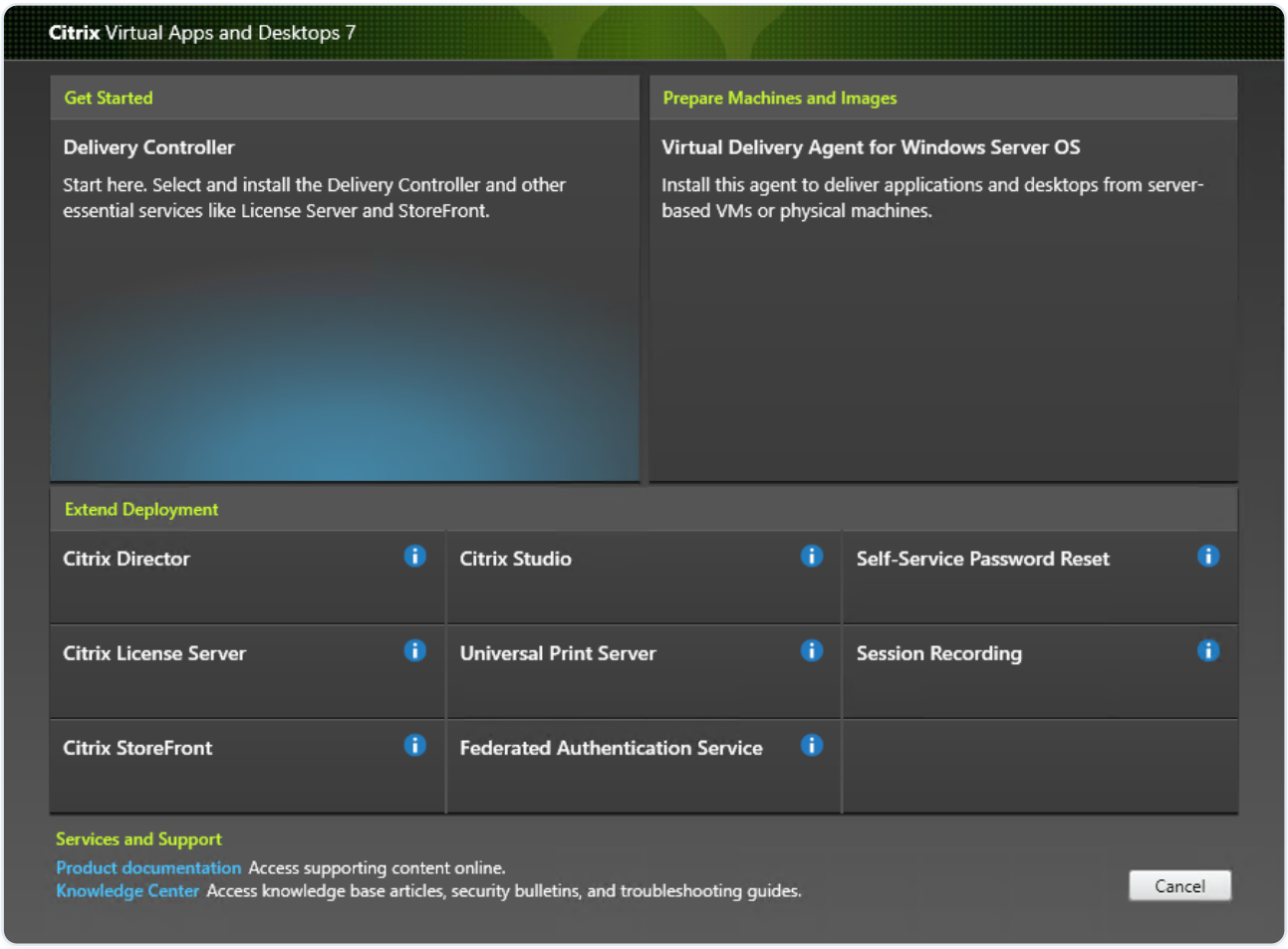
The installation wizard launches.

Step 2: Choose which product to install



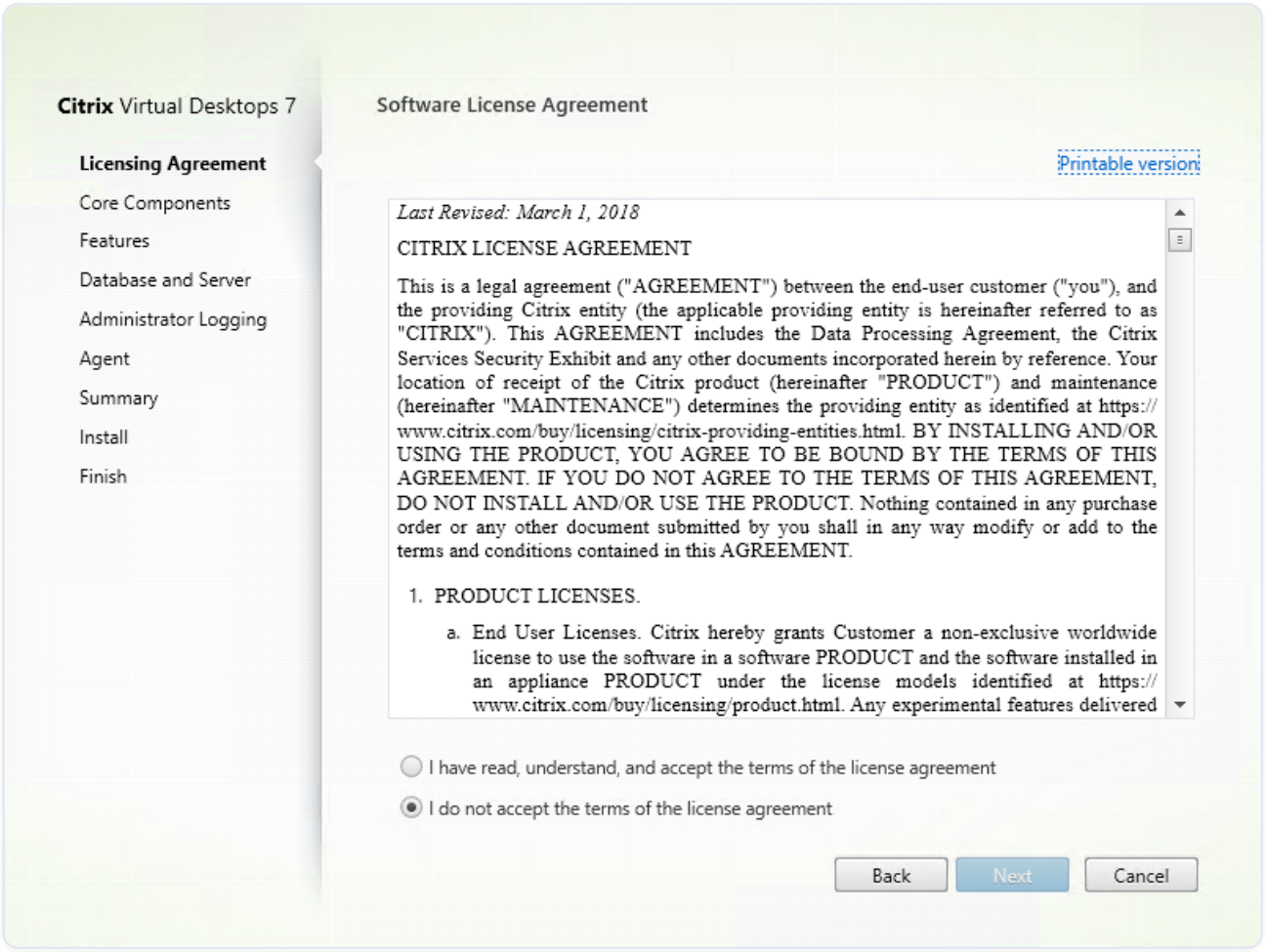
Click **Start** next to the product to install **Citrix Virtual Apps** or **Citrix Virtual Desktops**.

Step 3: Select Session Recording



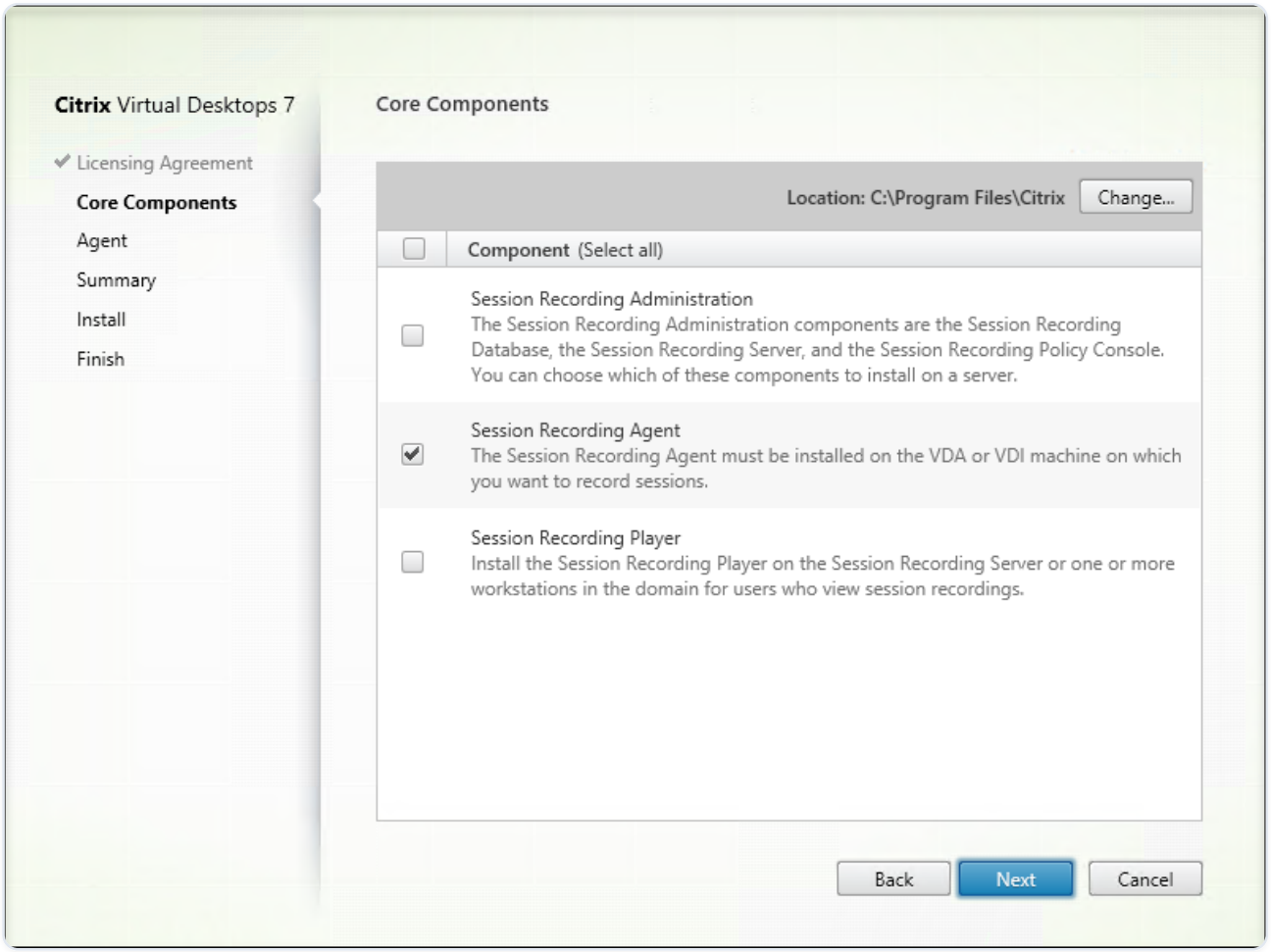
Select the **Session Recording** entry.

Step 4: Read and accept the license agreement



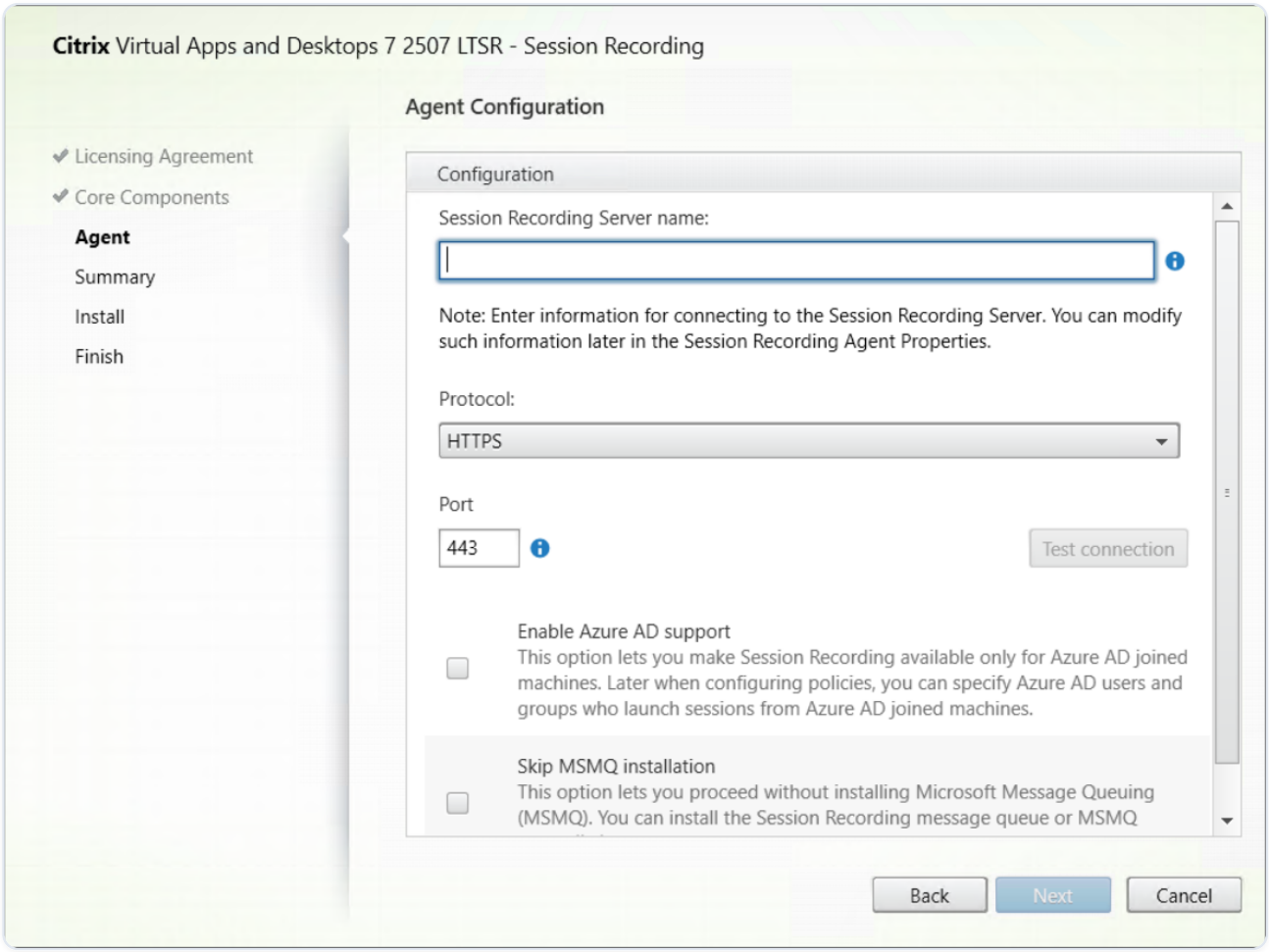
On the **Software License Agreement** page, read the license agreement, accept it, and then click **Next**

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, complete the following settings:

- 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**.
- If you want to install the Session Recording message queue or MSMQ manually later. You can check "Skip MSMQ installation". This option lets you proceed without installing Microsoft Message Queuing (MSMQ).
- If you are installing the Session Recording agent on an Azure AD joined machine, select **Enable Azure AD support**. To fully enable Azure AD identity support for configuring playback permissions and various Session Recording policies from the cloud, complete the following steps and then restart the VDA:

> **Note:**

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

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

- Use the MSI package to install the Session Recording server on an Azure AD joined machine as well. Select **Enable Azure AD support** during the MSI installation.

- Connect Citrix Cloud to Azure AD.
- Go to the home page for the Full Configuration interface and enable the **SessionRecordingSupportAAD** and **Send User Identity Info In Prepare Session** toggles under the **Preview features** section. To access the home page for the Full Configuration interface, complete the following steps:

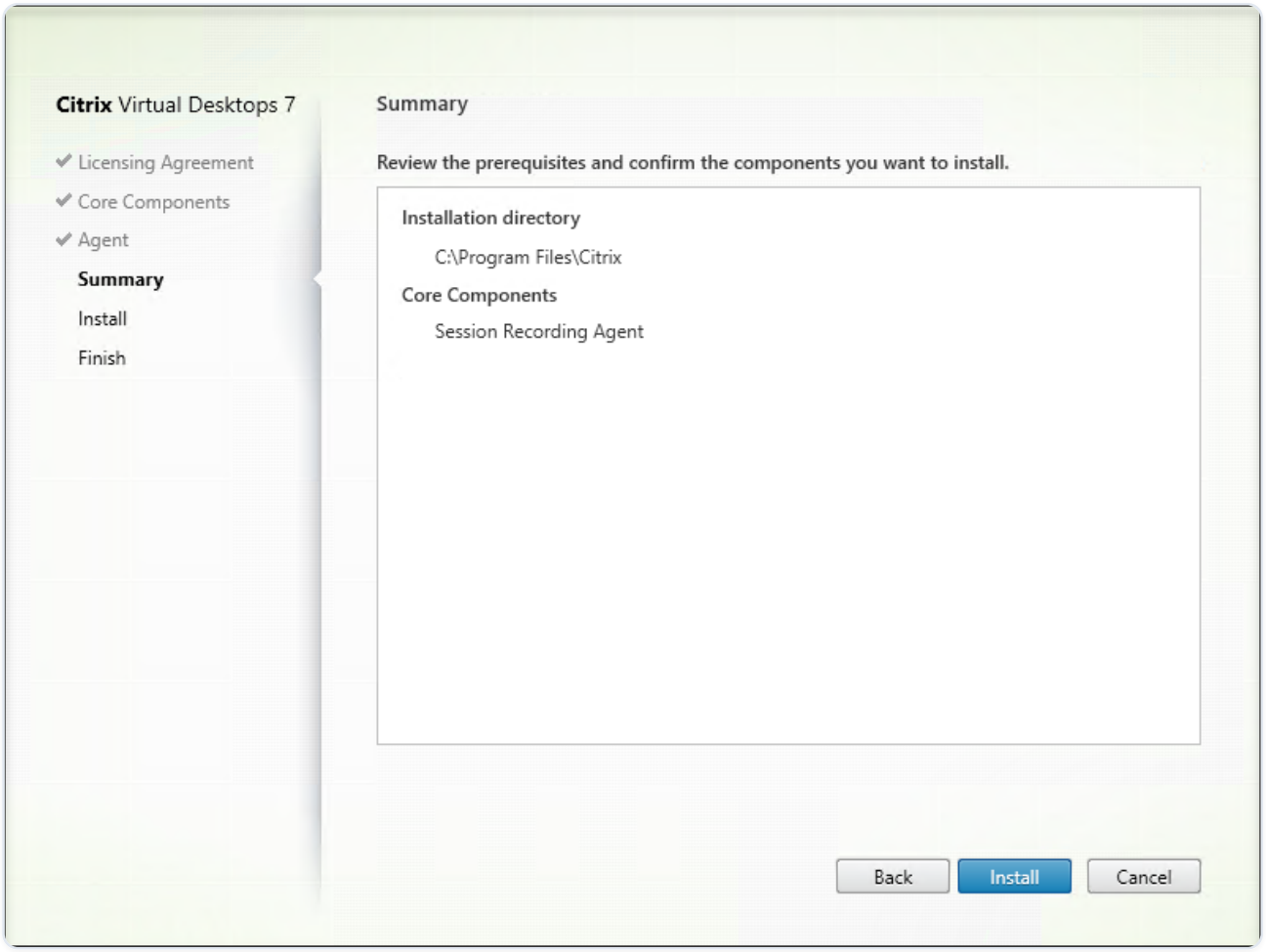
  a. Sign in to Citrix Cloud.

  b. In the upper left menu, select **My Services > DaaS**. By default, the home page for the Full Configuration interface appears.

Note:

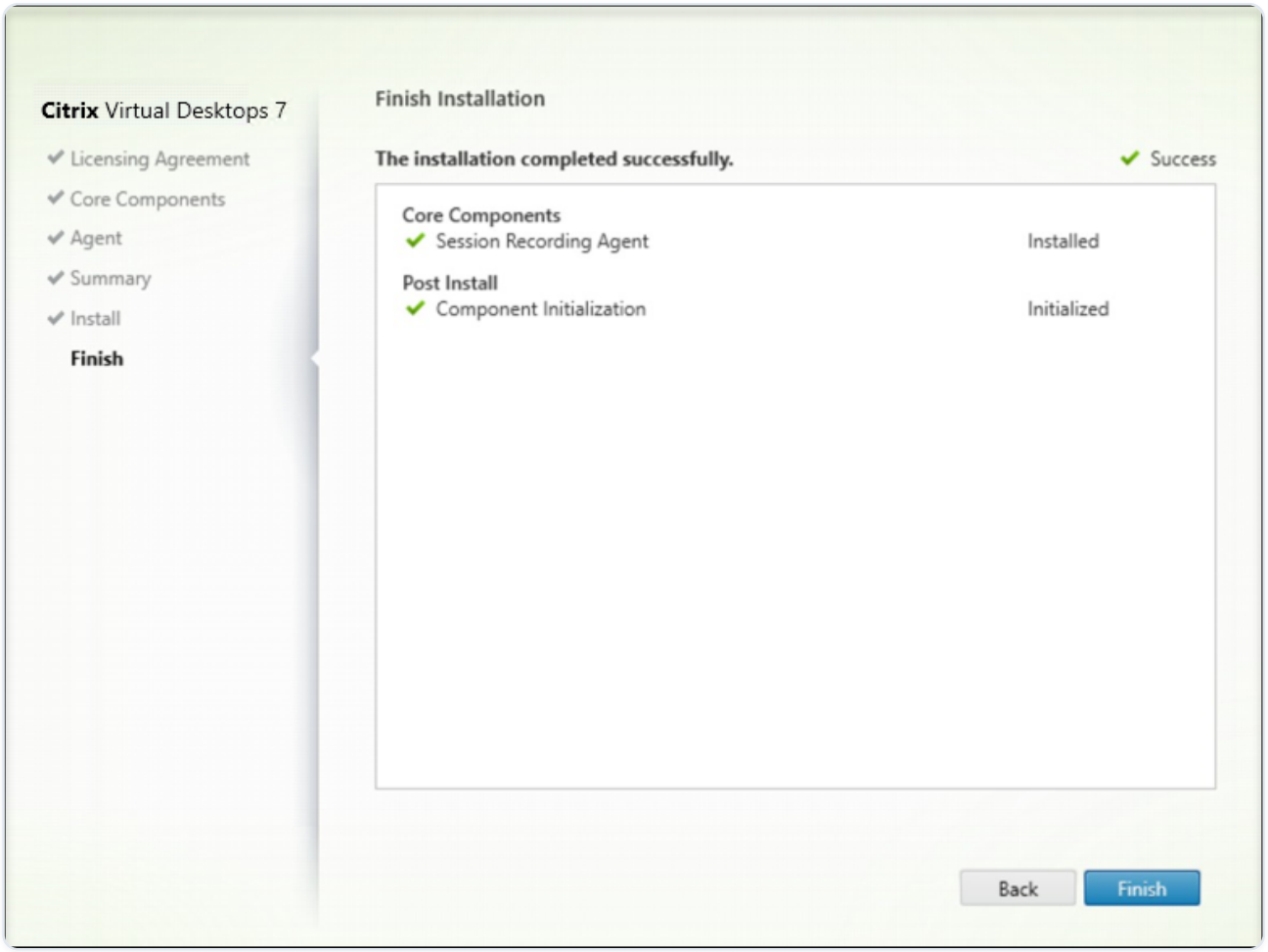
> There is a limitation with the test connection function of the installer. It does not support the "HTTPS requires TLS 1.2" scenario. If you use the installer in this scenario, the test connection fails but you can ignore the failure and click **Next** to continue the installation. It does not affect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

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.

Tip:

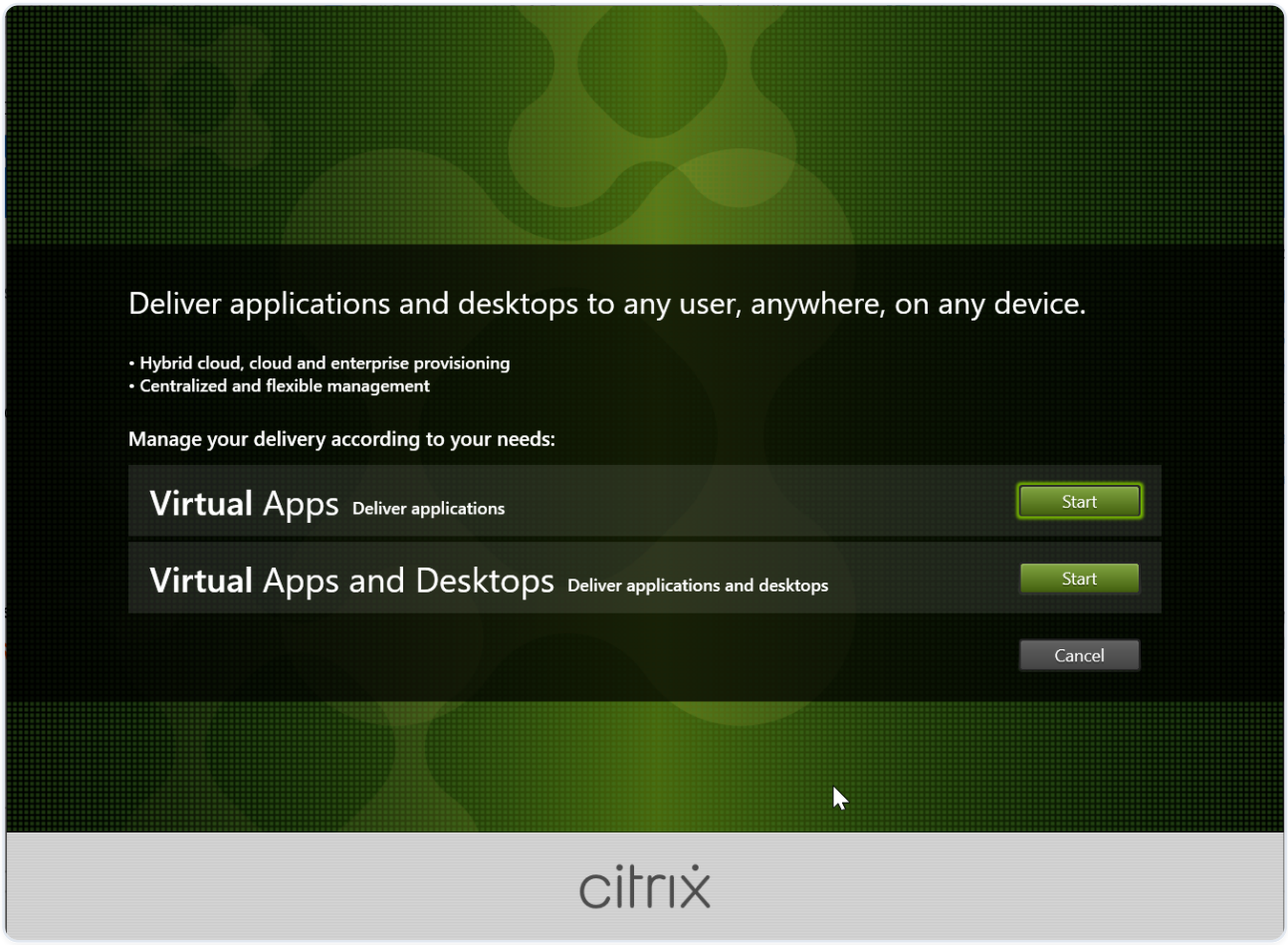
- Installing the Session Recording server lets you install the Session Recording web player automatically.
- Before or after you install the Session Recording player, install the Microsoft Visual C++ Redistributable package called **VC_redist.x86.exe**. You can find the package on the Citrix Virtual Apps and Desktops ISO under **\Support\VcRedist**.

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.

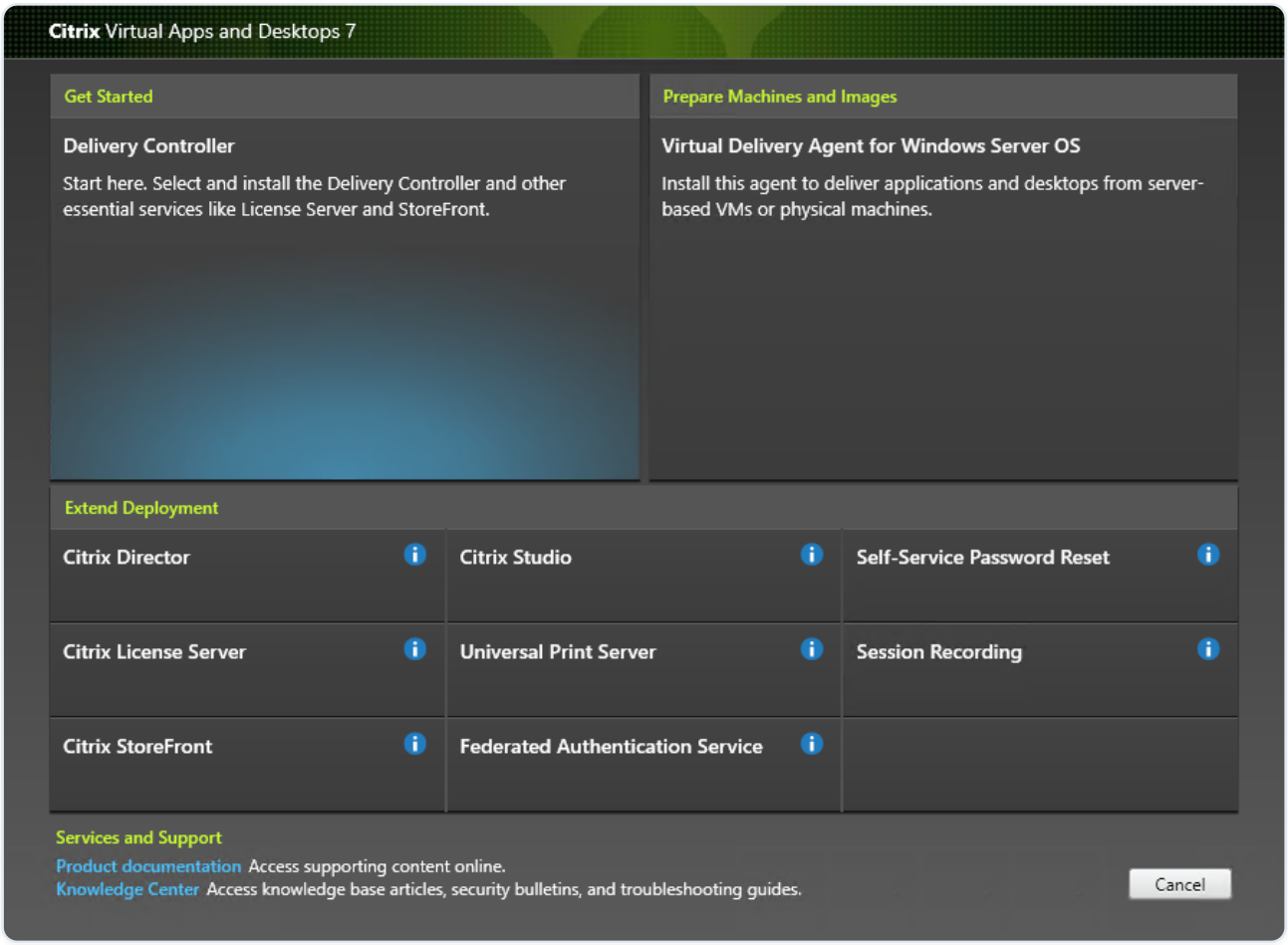
The installation wizard launches.

Step 2: Choose which product to install



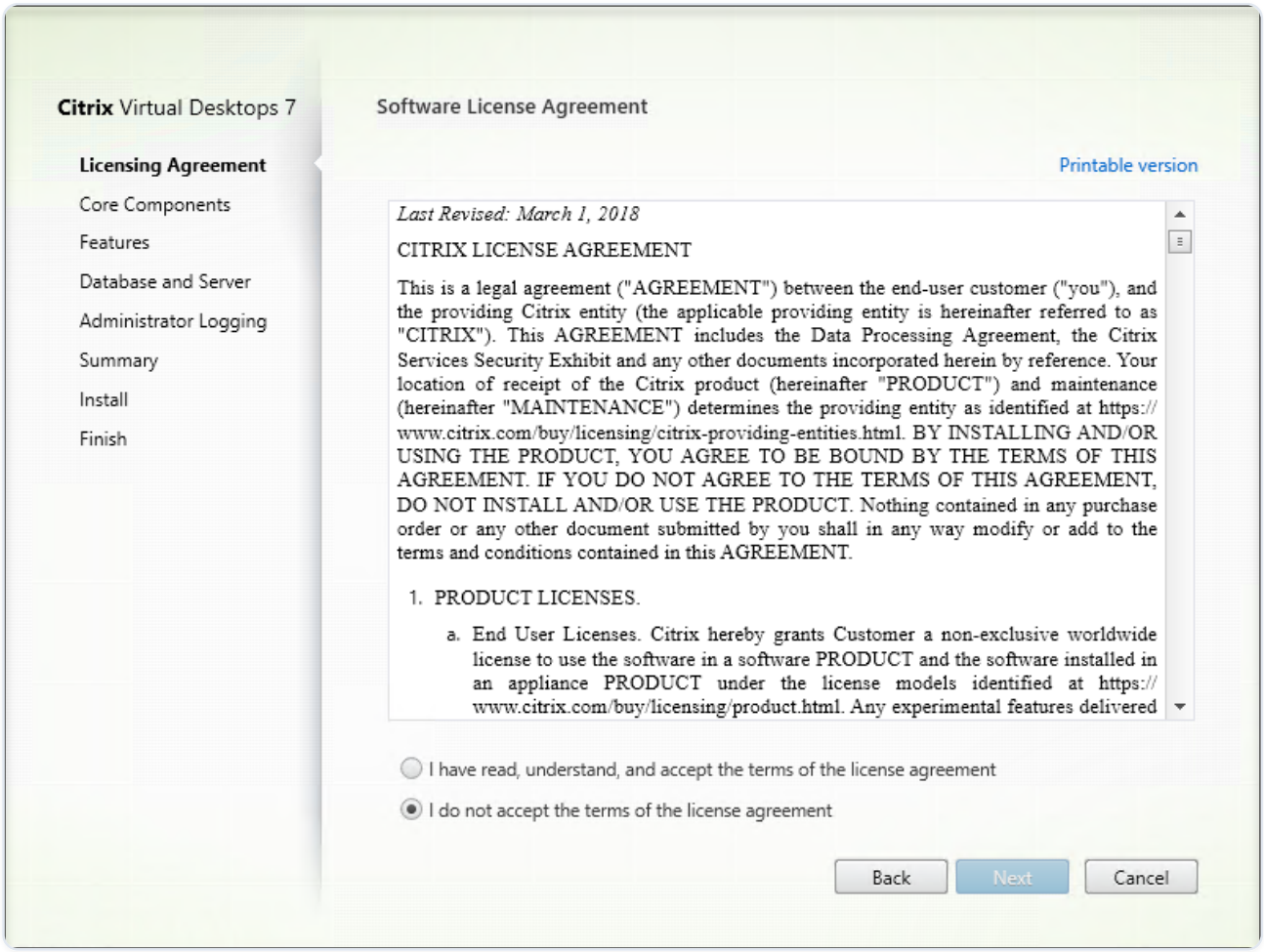
Click **Start** next to the product to install **Citrix Virtual Apps** or **Citrix Virtual Desktops**.

Step 3: Select Session Recording



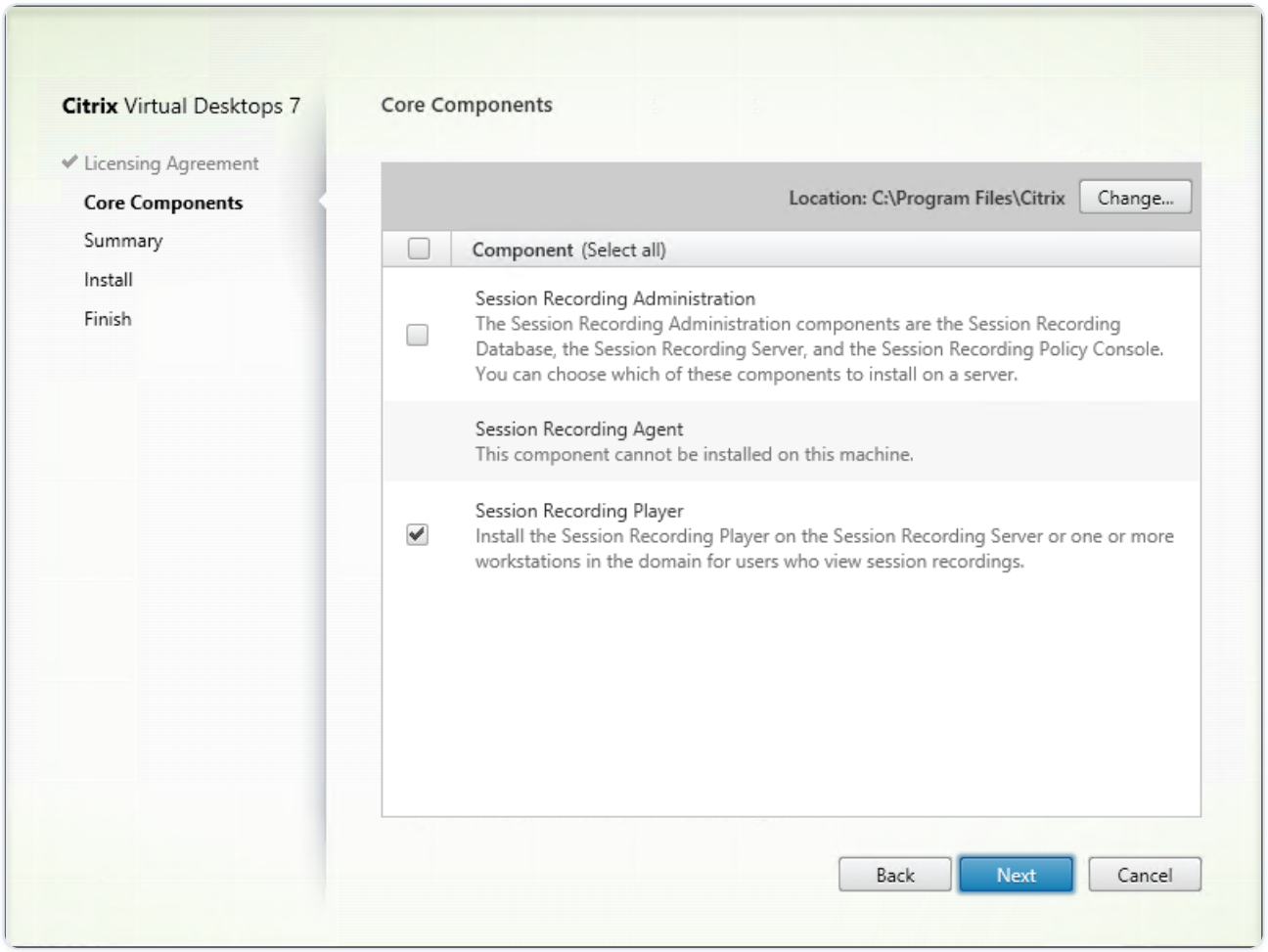
Select the **Session Recording** entry.

Step 4: Read and accept the license agreement



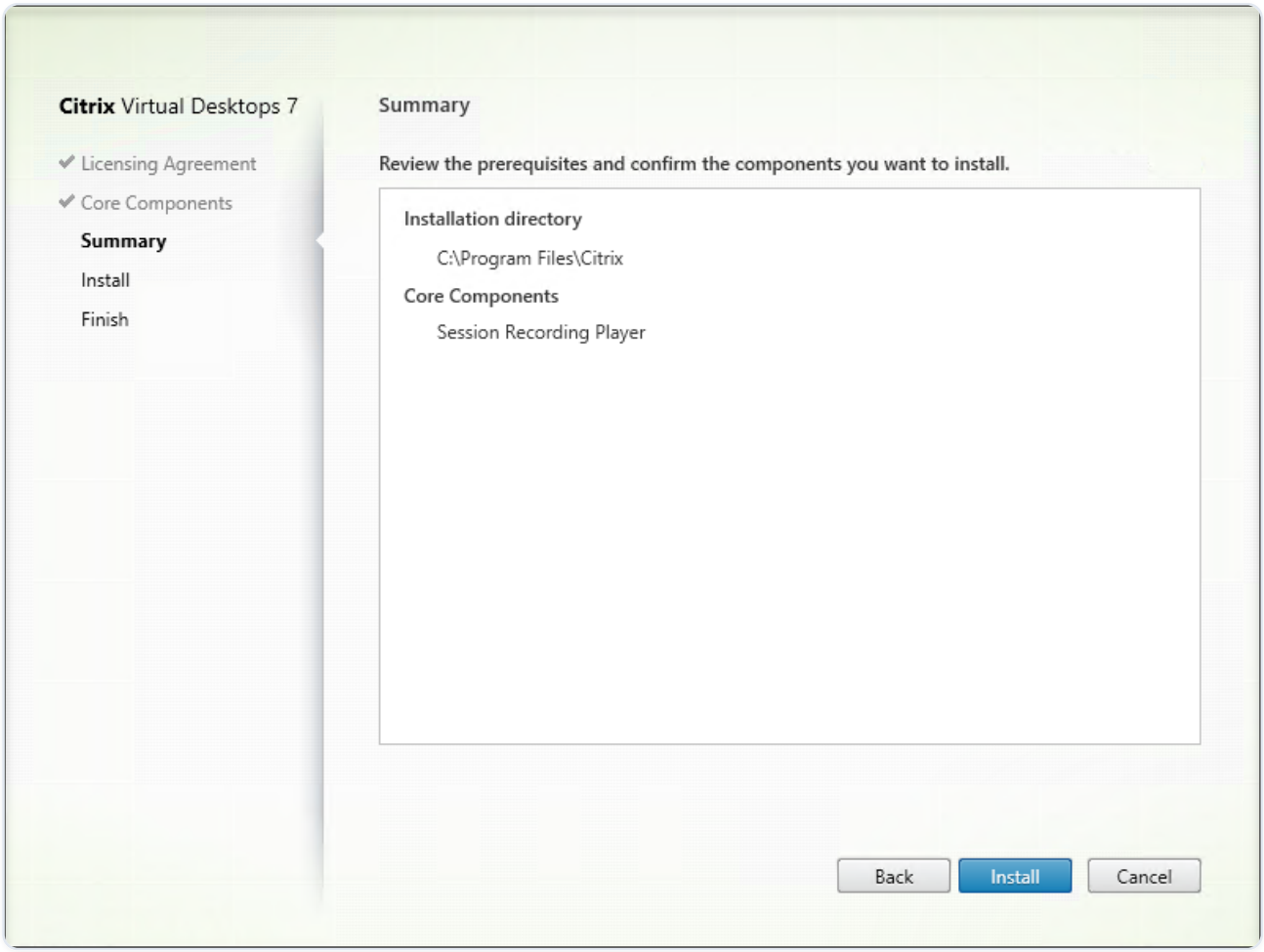
On the **Software License Agreement** page, read the license agreement, accept it, and then click **Next**.

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



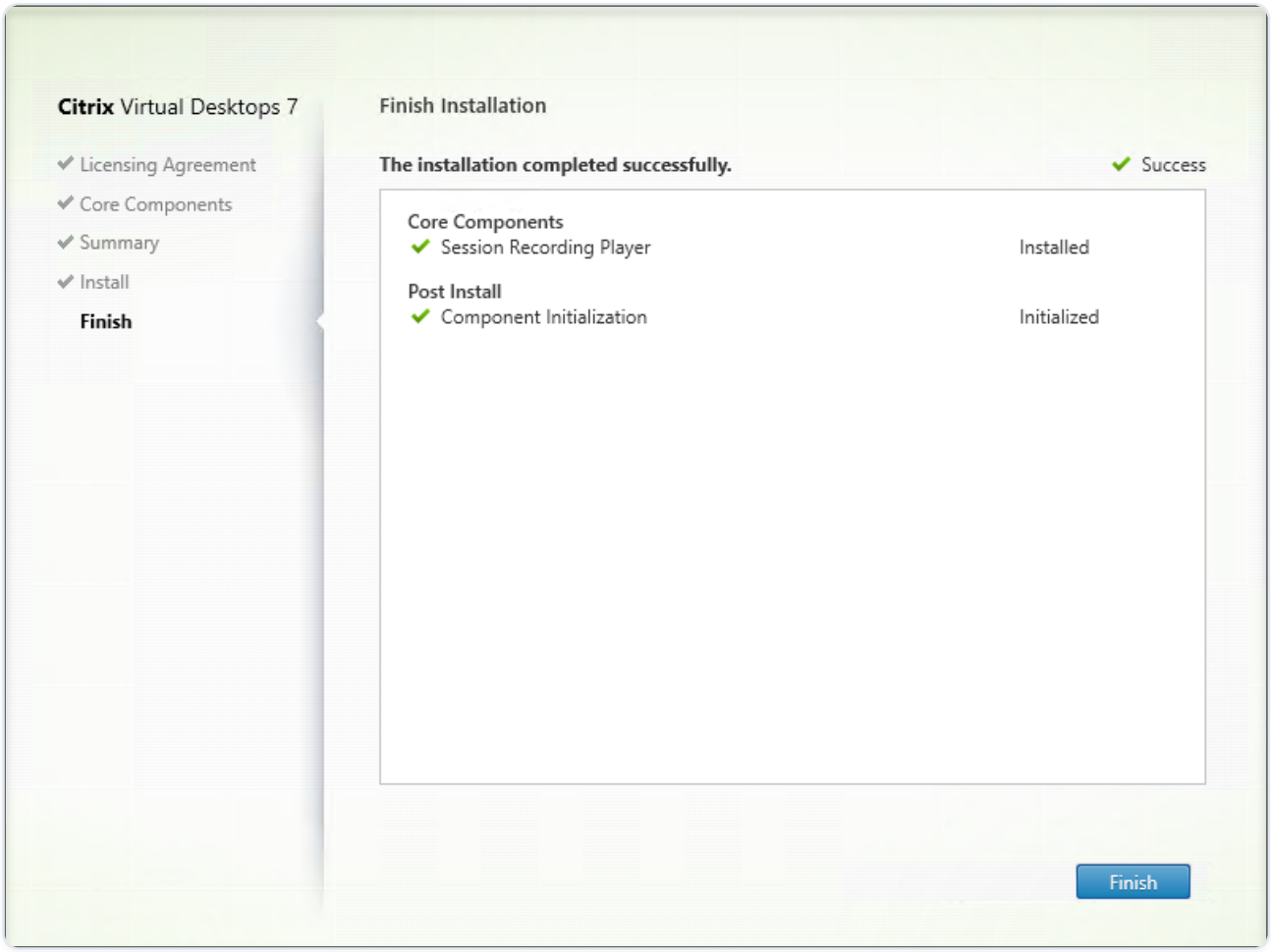
Select **Session Recording Player** and click **Next**.

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.

Choose the message queuing solution

The default message queue for Session Recording is Microsoft Message Queue (MSMQ). Session Recording offers the Session Recording message queue as an alternative to MSMQ. Its installation and configuration are described further in this section. The active message queue can be changed using registry settings.

MSMQ

It is recommended that users of MSMQ configure the Access Control List (ACL) following the Session Recording installation. For more information, see Security recommendations.

Session Recording message queue

The Session Recording message queue solution is designed to enhance Session Recording's capabilities by:

- **Supporting modern .NET environments**: Built on WebSocket and nats.io, it eliminates the dependency on the .NET Framework required by MSMQ.
- **Providing enhanced features**: Offers persistent storage, multiple authentication methods, SSL encryption, and various configuration options.
- **Improving authentication flexibility**: Supports better authentication choices for Azure AD or other non-AD scenarios.

Install and configure the Session Recording message queue

1. To proceed with the installation and configuration of the Session Recording message queue, ensure that the following prerequisites are met:

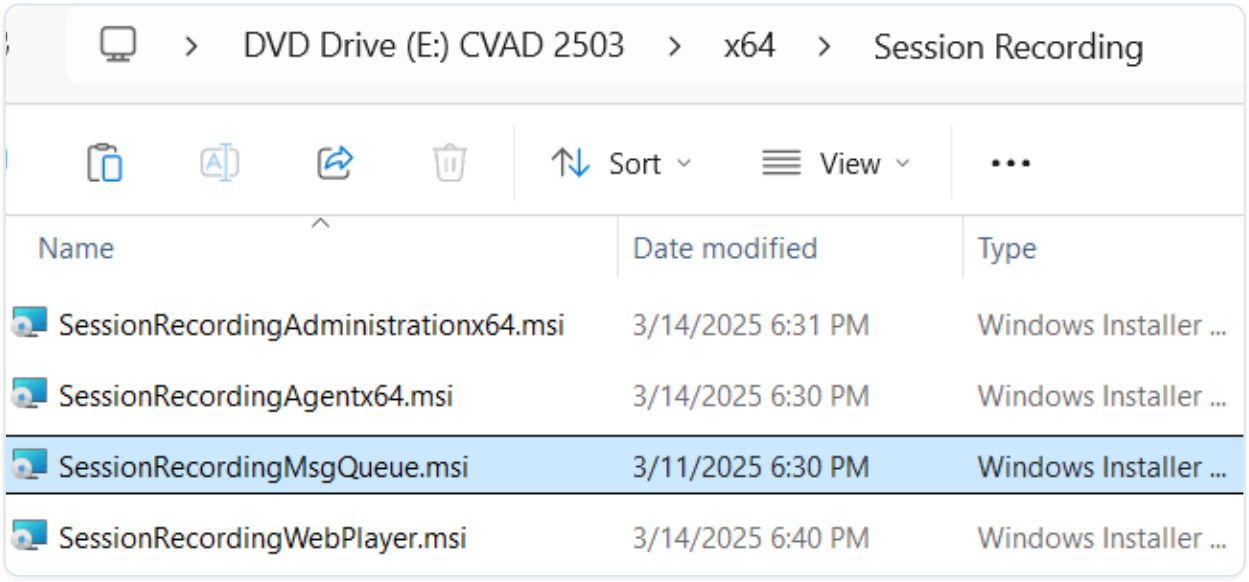
   - You must have administrator privileges.
   - .NET 8 Runtime must be installed from `<https://dotnet.microsoft.com/en-us/download/dotnet/8.0>` before you install the Session Recording message queue.

2. On the VDA, install the Session Recording agent using either the meta installer from the ISO file or by directly running SessionRecordingAgentx64.msi.

   If your environment uses only the Session Recording message queue and will not switch to MSMQ, you may select the "Skip MSMQ Installation" option during the Session Recording agent installation. This ensures that:

   - MSMQ will not be installed on the VDA by meta installer.
   - The Session Recording agent service is not configured with an MSMQ dependency.

   After completing the agent installation, deploy the Session Recording message queue by running SessionRecordingMsgQueue.msi from the ISO file.



3. Restart the VDA.
4. Configure the permissions, policies, and other settings for Session Recording. Recorded sessions can now be transmitted through the Session Recording message queue.

Optional configurations

Use SSL encryption

1. Configure the Agent:
    a. Open Session Recording Agent Properties from the Start menu.
    b. Navigate to the Connections tab.
    c. Under Session Recording Broker, change the Protocol to HTTPS.
    d. Click OK to save changes.
    e. Restart Citrix Session Recording Agent and Citrix Session Recording MsgQueue service.
2. Configure the Server:
    a. On the Session Recording Server, verify that a valid SSL certificate is bound to the Default Web Site in IIS.

Troubleshooting

Communication failure

1. Check whether the **IIS** and **CitrixSsRecStorageManager** services are in a running state on the Session Recording server.

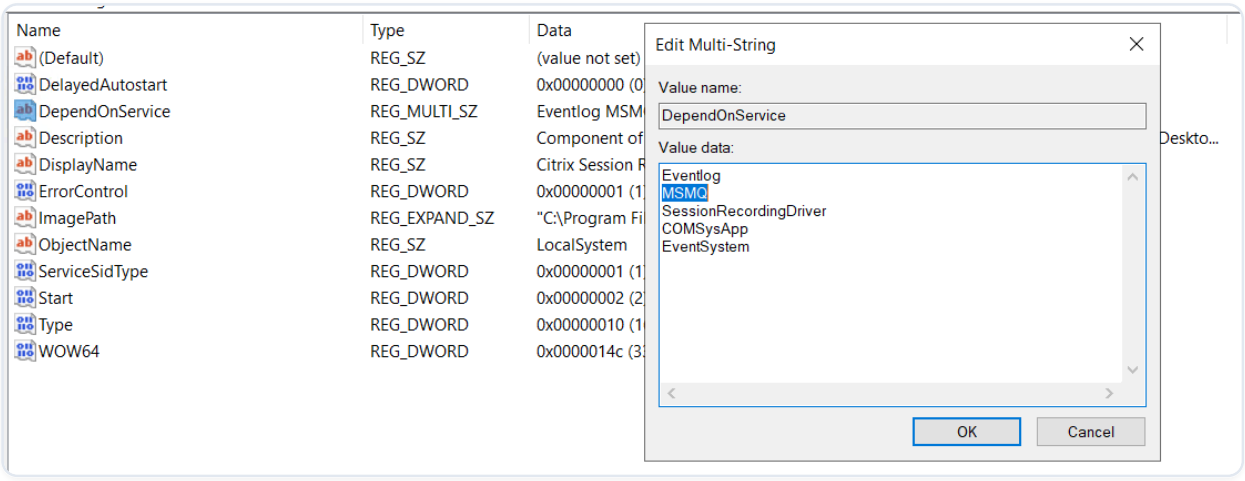
2. Check whether the **CitrixSmAudAgent**, **CitrixSmAudMsgQueue**, and **CitrixSmAudNatsServer** services are in a running state on the VDA.

The VDA's CitrixSmAudMsgQueue service fails to start

1. Check whether .NET 8 Runtime is installed on the VDA.
2. Check whether you have administrator privileges when installing SessionRecordingMsgQueue.msi.

Unable to stop the MSMQ service or disable the MSMQ feature

1. On the VDA, in the registry `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixSmAudAgent`, remove **MSMQ** from the **DependOnService** key, leave the rest unchanged, and click **OK** then restart VDA.



Automate installation

Session Recording supports silent installation with options.

Automate installation of the Session Recording Administration components

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

Session Recording now supports different types of SQL authentication. Refer to the following table for details:

SESSION RECORDING VERSION	SUPPORTED SQL SERVER TYPE	SUPPORTED SQL AUTHENTICATION METHOD	NOTES
< 2411	• On-Premises SQL Server • Azure SQL Database • Azure SQL Managed Instance • SQL Server on Azure VMs • AWS RDS • Google Cloud SQL Server	SQL Server Authentication	For more information, see Install the Session Recording database on cloud SQL database services
Starting from 2411	• On-Premises SQL Server • Azure SQL Database • Azure SQL Managed Instance • SQL Server on Azure VMs • AWS RDS	• SQL Server Authentication • Microsoft Entra ID Password Authentication with Cloud Managed Entra id account	Microsoft Entra ID Password Authentication only supported Azure SQL Database and Azure SQL Managed Instance. For more information, see Install the Session Recording database on Azure SQL Database and

SESSION RECORDING VERSION	SUPPORTED SQL SERVER TYPE	SUPPORTED SQL AUTHENTICATION METHOD	NOTES
	• Google Cloud SQL Server		Install the Session Recording database on Azure SQL Managed Instance or on AWS RDS.
Starting from 2507	• On-Premises SQL Server • Azure SQL Database • Azure SQL Managed Instance • SQL Server on Azure VMs • AWS RDS • Google Cloud SQL Server	• SQL Server Authentication • Microsoft Entra ID Password Authentication with Cloud Managed Entra id account • Microsoft Entra ID Service Principal Authentication with Cloud Managed Entra id account	• Microsoft Entra ID Password Authentication only supported Azure SQL Database and Azure SQL Managed Instance. • Microsoft Entra ID Service Principal Authentication only supported Azure SQL Managed Instance

SESSION RECORDING VERSION	SUPPORTED SQL SERVER TYPE	SUPPORTED SQL AUTHENTICATION METHOD	NOTES
Starting from 2607	• On-Premises SQL Server • Azure SQL Database • Azure SQL Managed Instance • SQL Server on Azure VMs • AWS RDS • Google Cloud SQL Server	• SQL Server Authentication • Microsoft Entra ID Password Authentication with Cloud Managed Entra id account • Microsoft Entra ID Service Principal Authentication with Cloud Managed Entra id account • Azure managed identity	• Microsoft Entra ID Password Authentication and Azure managed identity only supported Azure SQL Database and Azure SQL Managed Instance. • Microsoft Entra ID Service Principal Authentication only supported Azure SQL Managed Instance

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="DatabaseConnectionString"
DATABASENAME="CitrixSessionRecording"
LOGGINGDATABASENAME="CitrixSessionRecordingLogging"
AZURESQLSERVICESUPPORT="1" DATABASEUSER="localhost" CLOUDDBSUPPORT="0"
AZUREUSERNAME="SQLorEntraIDAdminName"
AZUREPASSWORD="SQLorEntraIDAdminPassword" AADPASSWORD="1"
SERVICEKEYAUTHENABLE="1" /qn+ /l*vx "yourinstallationlog"
```

```
msiexec /i "SessionRecordingAdministrationx64.msi"

ADDLOCAL="SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"

DATABASEINSTANCE="DatabaseConnectionString"
DATABASENAME="CitrixSessionRecording"
LOGGINGDATABASENAME="CitrixSessionRecordingLogging"
AZURESQLSERVICESUPPORT="1"

CLOUDDBSUPPORT="0"

AZUREUSERNAME="ServicePrincipalClientId"
AZUREPASSWORD="ServicePrincipalClientsecret"

AADPASSWORD="0"

AZURETENANTID="ServicePrincipalTenantId"

SERVICEPRINCIPAL="1" /qn+ /l*vx "yourinstallationlog "

AZUREMANAGEDIDENTITY="1"
AZUREMANAGEDIDENTITYCLIENTID="AzureManagedIdentityId"
```

Note:

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

Regardless of the instance specified by `DATABASEINSTANCE` here, starting with the 2411 release, you can also choose to install the Session Recording admin logging database on a separate instance from the Session Recording database. To do so, complete the following steps before running either of the commands to install them:

1. Go to the machine where you are going to install the Session Recording server.
2. Open the Registry Editor.
3. Modify the registry:
    - Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`.
    - Add the `SmAudDatabaseLoggingState` DWORD (32-bit) value and set the value data to `1`.
    - Add the `SmAudDatabaseLoggingInstance` value and set the value data to the instance name where you want to install the Session Recording admin logging database.

    Later when you install the databases, the Session Recording admin logging database is installed on the separate instance specified by the `SmAudDatabaseLoggingInstance` registry value. You must configure the same authentication mode for both databases (SQL Server authentication, Windows authentication, or Microsoft Entra ID authentication) and grant identical user permissions.

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. As described earlier, you can install the Session Recording database and the Session Recording admin logging database on the same instance or separate instances.
- **DATABASENAME** is the database name of the Session Recording database.
- **LOGGINGDATABASENAME** is the name of the administrator logging database.
- **AZURESQLSERVICESUPPORT** determines whether SQL Server authentication is supported. To use SQL Server authentication, set it to `1`.
- **DATABASEUSER** is the computer account of the Session Recording server.
- **CLOUDDBSUPPORT** determines whether Azure SQL Databases are supported.
- **AZUREUSERNAME** is the SQL Server or Microsoft Entra ID administrator name or Microsoft Entra ID ServicePrincipal client id(Application ID). To use Microsoft Entra ID authentication, complete the following steps:

  a. Make sure that Visual C++ Redistributable has been installed on the Session Recording server. Otherwise, download and install it from `<https://learn.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170>`.

  b. Make sure that the Microsoft ODBC Driver for SQL Server has been installed on the Session Recording server. Otherwise, download and install it from `<https://learn.microsoft.com/en-us/sql/connect/odbc/download-odbc-driver-for-sql-server?view=sql-server-ver16>`.

  c. Include the **AADPASSWORD** parameter and set it to 1 when running the database installation command.

  d. Create an Entra ID admin and grant it SQL Server administrative permissions. For more information, see the Microsoft documentation: `<https://learn.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?view=azuresql&tabs=azure-powershell>`.

- **AZUREPASSWORD** is the SQL Server or Microsoft Entra ID administrator password or Microsoft Entra ID ServicePrincipal client secret.
- **AADPASSWORD** determines whether Microsoft Entra ID authentication is supported. To use Microsoft Entra ID authentication, set it to 1.
- **AZURETENANTID** is Azure tenantid(Directory ID).

- **SERVICEPRINCIPAL** determines whether Microsoft Entra ID ServicePrincipal authentication is supported. To use Microsoft Entra ID ServicePrincipal authentication, set it to 1.
- **SERVICEKEYAUTHENABLE** enables the service key authentication between the Session Recording agent and the Session Recording server. This parameter is required only when you want to enable Azure AD support and you must set it to **1**. Otherwise, do not add this parameter.
- **/q** specifies quiet mode.
- **/l*v** specifies verbose logging.
- **yourinstallationlog** is the location of your installation log file.
- **AZUREMANAGEDIDENTITY** determines whether Azure ManagedIdentity authentication is supported. To use Azure ManagedIdentity authentication, set it to 1.
- **AZUREMANAGEDIDENTITYCLIENTID** is the ObjectId of Azure ManagedIdentity.

> **Note:**
>
> Session Recording supports only the user-assigned managed identity and not the system-assigned identity.

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.

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

SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol
SESSIONRECORDINGBROKERPORT=yourbrokerport
SESSIONRECORDINGAUTHENTICATION="Citrix Cloud™"
SESSIONRECORDINGRPC="Websocket" SESSIONRECORDINGIDP="IDP"
```

> **Note:**

> You can find `SessionRecordingAgentx64.msi` on the Citrix Virtual Apps and Desktops ISO under `\x64\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.
- **SESSIONRECORDINGAUTHENTICATION** is the authentication type between the Session Recording agent and the Session Recording server. This parameter is required only when you want to enable Azure AD support. To enable Azure AD support, add this parameter and set it to **Citrix Cloud**.
- **SESSIONRECORDINGRPC** is the communication method between the Session Recording agent and the Session Recording server. This parameter is required only when you want to enable Azure AD support. To enable Azure AD support, add this parameter and set it to **Websocket**.
- **SESSIONRECORDINGIDP** specifies the identity type. This parameter is required only when you want to enable Azure AD support. To enable Azure AD support, add this parameter and set it to **IDP**.
- **/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 is 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.

Important note about upgrading to version 2607 LTSR:

To prevent session recording failures due to incomplete upgrades of Session Recording agents, follow these steps when upgrading to 2607 LTSR:

1. Upgrade each Session Recording server to version 2607 LTSR.
2. Enable remote access using .NET Remoting with the following command:

   ```
   <SessionRecordingserverinstallationpath>\Bin\SsRecUtils.exe -EnableBrokerRemoting
   ```

3. Upgrade each Session Recording agent to version 2607 LTSR.
4. After all Session Recording agents are upgraded, disable remote access using .NET Remoting with the following command:

   ```
   <SessionRecordingserverinstallationpath>\Bin\SsRecUtils.exe -DisableBrokerRemoting
   ```

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
- SQL Server on Azure VMs
- AWS RDS
- Google Cloud SQL Server

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, Entra ID authentication, or both.
            - **Server admin login**: Enter a SQL Server or Microsoft Entra ID administrator name. Starting with 2411, Session Recording supports Entra ID authentication for cloud-based SQL databases including Azure SQL Database and Azure SQL Managed Instance. For more information about Microsoft Entra ID authentication, see the command parameter descriptions in this article.
            - **Password**: Enter a SQL Server or Microsoft Entra ID 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" DATABASEUSER="localhost" CLOUDDBSUPPORT="1"
AZUREUSERNAME="SQLorEntraIDAdminName"
AZUREPASSWORD="SQLorEntraIDAdminPassword" AADPASSWORD="1" /qn+ /l*vx
"yourinstallationlog"
```

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 SQL Server authentication is supported. To use SQL Server authentication, set it to 1.
- **CLOUDDBSUPPORT** determines whether Azure SQL Databases are supported.
- **DATABASEUSER** is the computer account of the Session Recording server.
- **AZUREUSERNAME** is the SQL Server or Microsoft Entra ID administrator name. Starting with 2411, Session Recording supports Entra ID authentication for cloud-based SQL databases including Azure SQL Database and Azure SQL Managed Instance. To use Microsoft Entra ID authentication, complete the following steps:

  a. Make sure that Visual C++ Redistributable has been installed on the Session Recording server. Otherwise, download and install it from `<https://learn.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170>`.

  b. Make sure that the Microsoft ODBC Driver for SQL Server has been installed on the Session Recording server. Otherwise, download and install it from `<https://learn.microsoft.com/en-us/sql/connect/odbc/download-odbc-driver-for-sql-server?view=sql-server-ver16>`.

  c. Include the **AADPASSWORD** parameter and set it to 1 when running the database installation command.

  d. Create an Entra ID admin and grant it SQL Server administrative permissions. For more information, see the Microsoft documentation: `<https://learn.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?view=azuresql&tabs=azure-powershell>`.

- **AZUREPASSWORD** is the SQL Server or Microsoft Entra ID administrator password.
- **AADPASSWORD** determines whether Microsoft Entra ID authentication is supported. To use Microsoft Entra ID authentication, set it to 1.
- **/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

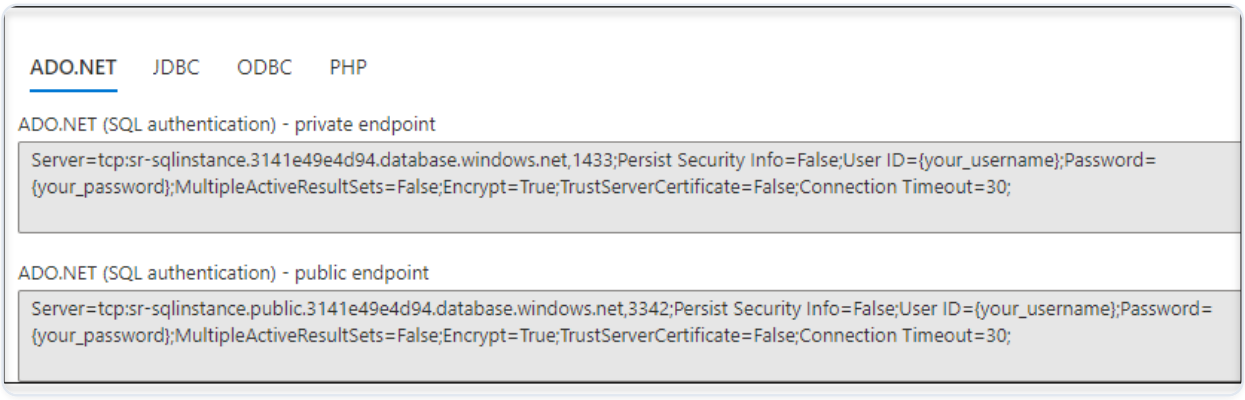
Tip:

On Azure SQL Managed Instance and on AWS RDS, you can install the Session Recording database by:

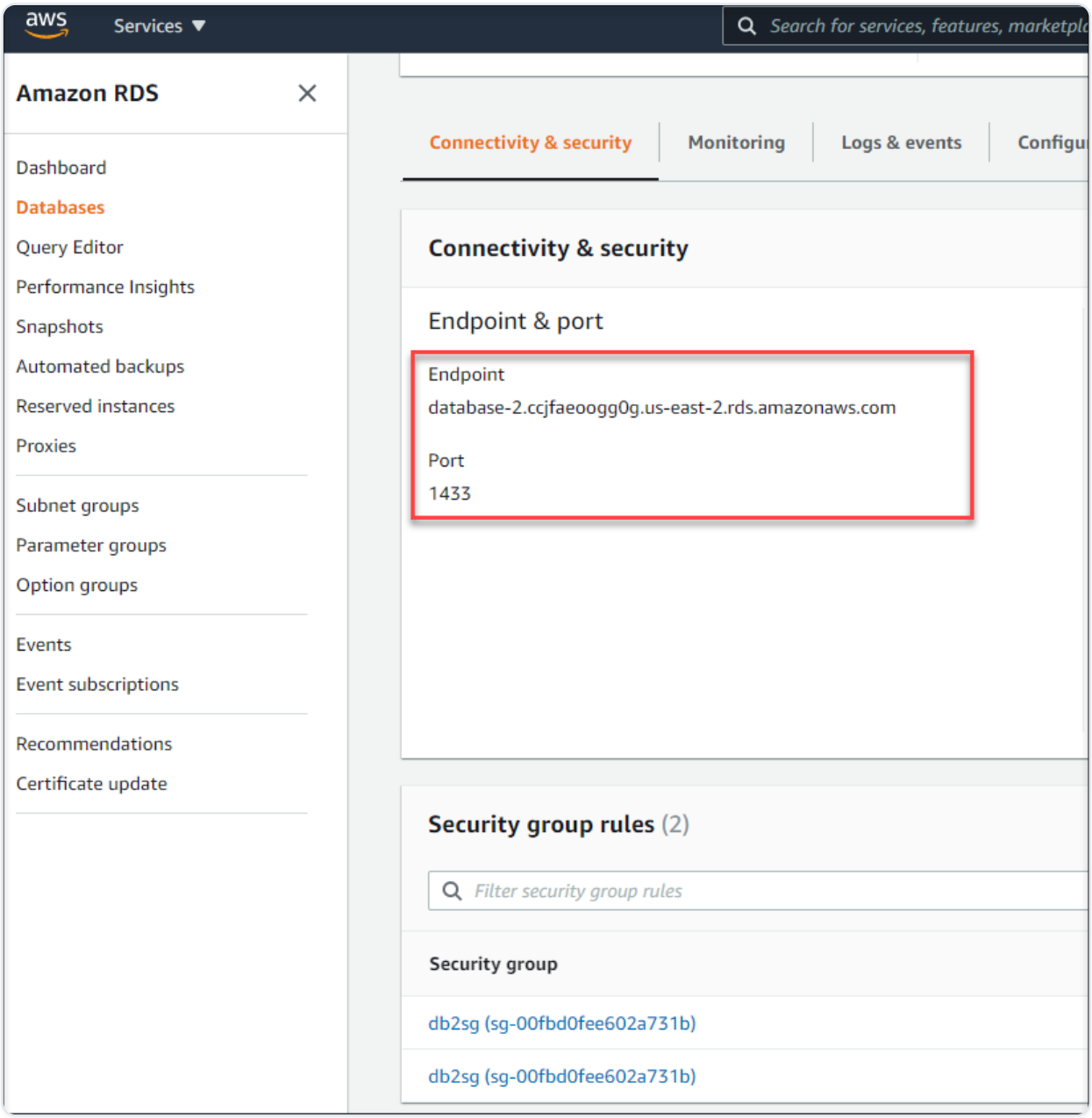
- Double-clicking and running the SessionRecordingAdministrationx64.msi package.
- Running a command similar to the following:

```
msiexec /i "SessionRecordingAdministrationx64.msi"
ADDLOCAL="SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
DATABASEINSTANCE="DatabaseConnectionString
"DATABASENAME="CitrixSessionRecording"
LOGGINGDATABASENAME="CitrixSessionRecordingLogging"
AZURESQLSERVICESUPPORT="1" CLOUDDBSUPPORT="1"
AZUREUSERNAME="SQLorEntraIDAdminName"
AZUREPASSWORD="SQLorEntraIDAdminPassword" AADPASSWORD="1"/qn+ /l*vx
"yourinstallationlog"
```

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.

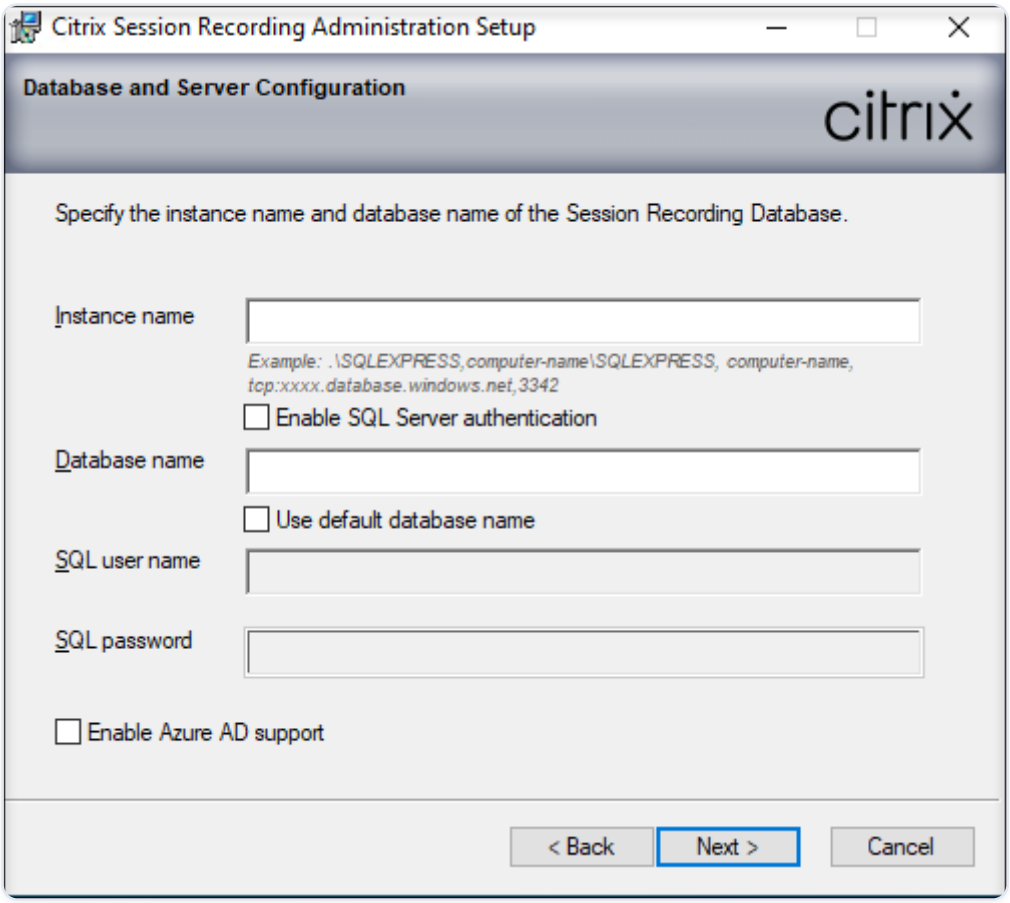


3. (For AWS RDS only) Keep a record of the **Endpoint** and **Port** information. We use it as the instance name of your database, in the format of **<Endpoint, Port>**.



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

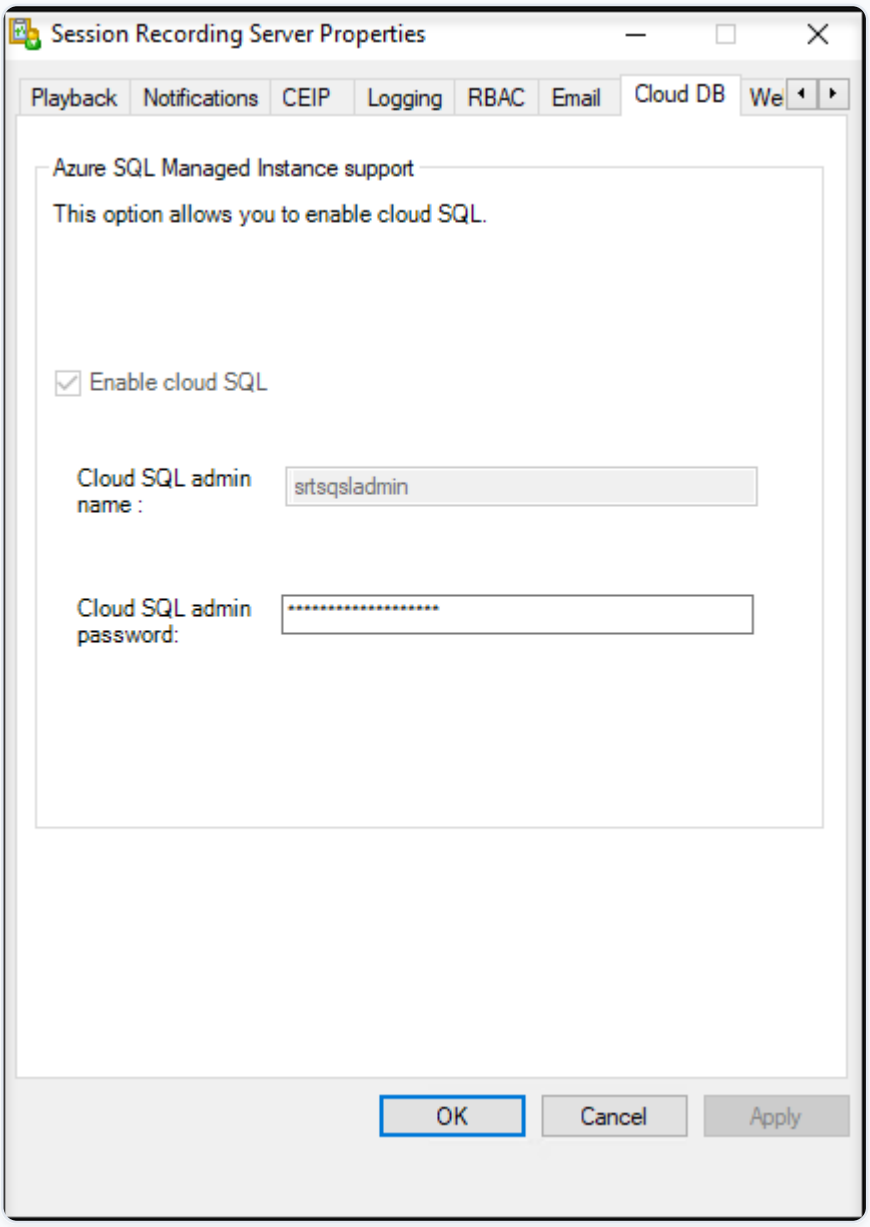
   Select the **Enable SQL Server authentication** check box and fill in the SQL Server administrator name and password. Make other required configurations.



Note:

- If you change the SQL Server administrator 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 SQL Server administrator password. Restart the Citrix Session Recording Analytics service, the Citrix Session Recording Storage

Manager service, and the IIS service.



- In addition to SQL Server authentication, Session Recording supports Entra ID (formerly Azure Active Directory) authentication for cloud-based SQL databases, including Azure SQL Database and Azure SQL Managed Instance. To use Microsoft Entra ID authentication, install the database through the command line and follow the instructions described earlier in this article.
- 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 SQL Server authentication** check box.

4. Follow the installation user interface to complete installing the Session Recording database.

Install the Session Recording database on Google Cloud SQL Server

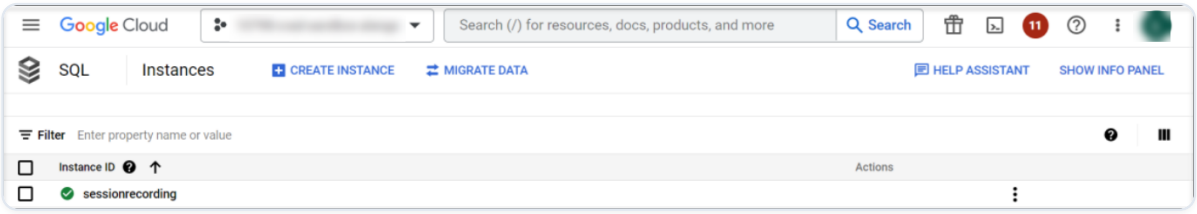
Tip:

On Google Cloud SQL Server, 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. For a description of the command parameters, see the preceding Automate installation section in this article.

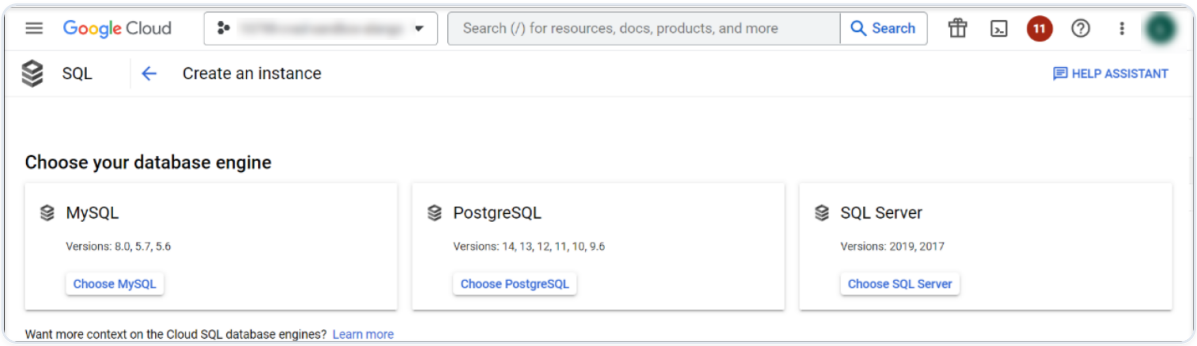
```
msiexec /i "SessionRecordingAdministrationx64.msi"
ADDLOCAL="SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
DATABASEINSTANCE="CloudSQL" DATABASENAME="CitrixSessionRecording"
LOGGINGDATABASENAME="CitrixSessionRecordingLogging"
AZURESQLSERVICESUPPORT="1" AZUREUSERNAME="CloudSQLAdminName"
AZUREPASSWORD="CloudSQLAdminPassword"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

This section details the installation method by using SessionRecordingAdministrationx64.msi that you can find on the Citrix Virtual Apps and Desktops ISO under **\x64\Session Recording**.

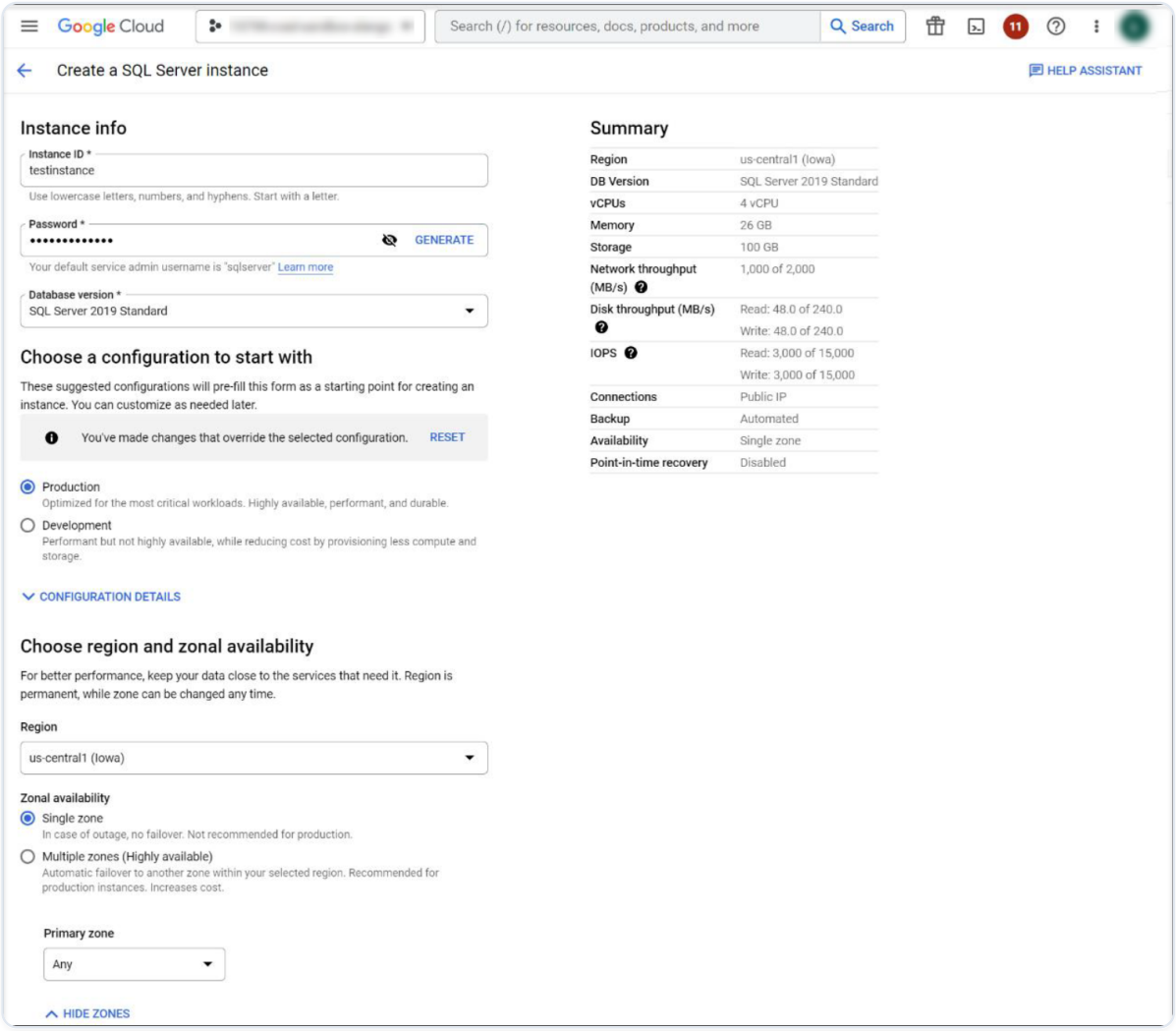
1. Create a SQL Server instance in Google Cloud.
   a. Go to the Google Cloud console and open the SQL instances page.
   b. Click **CREATE INSTANCE**. For example:



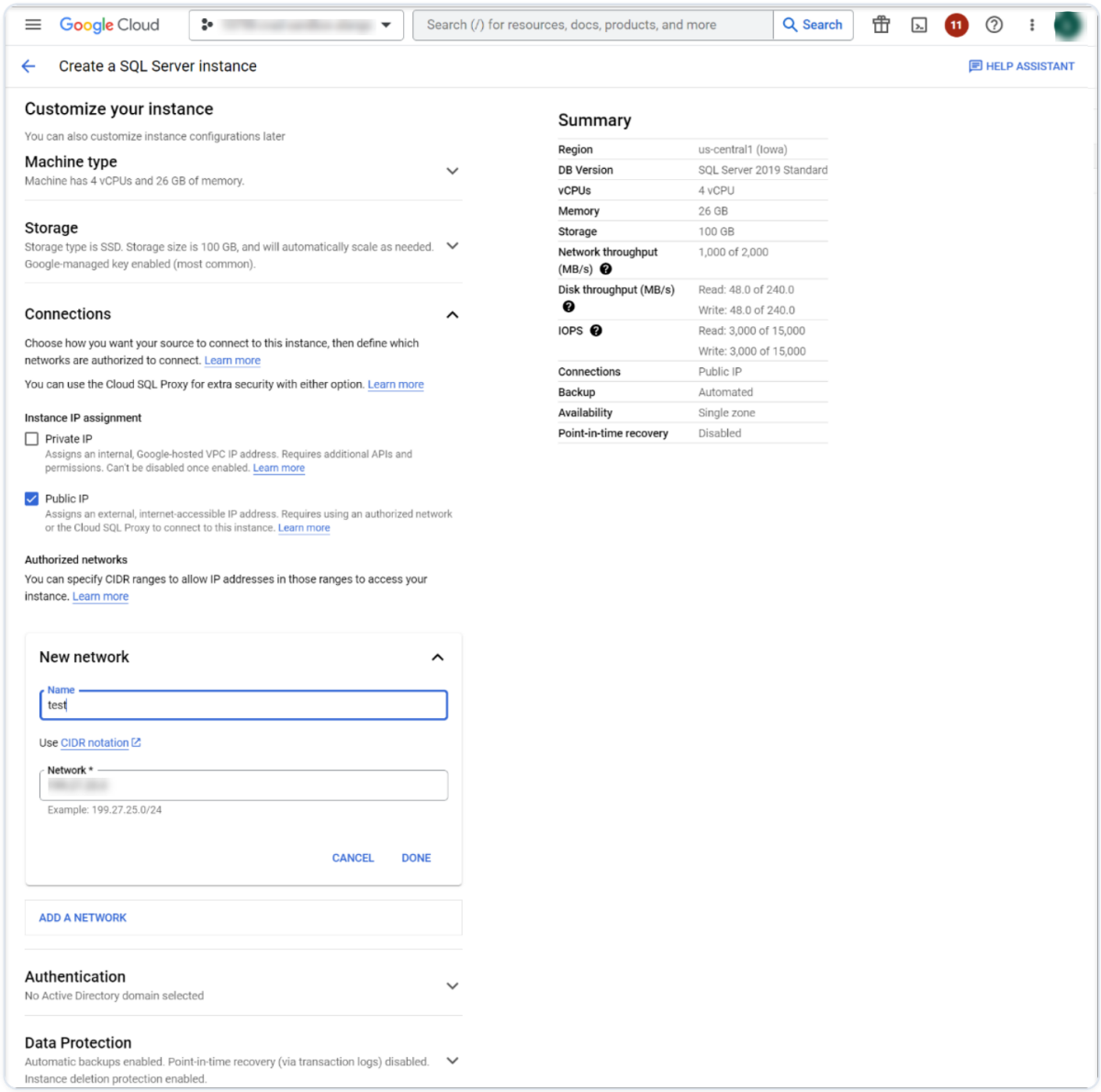
   c. Choose **SQL Server** as your database engine.



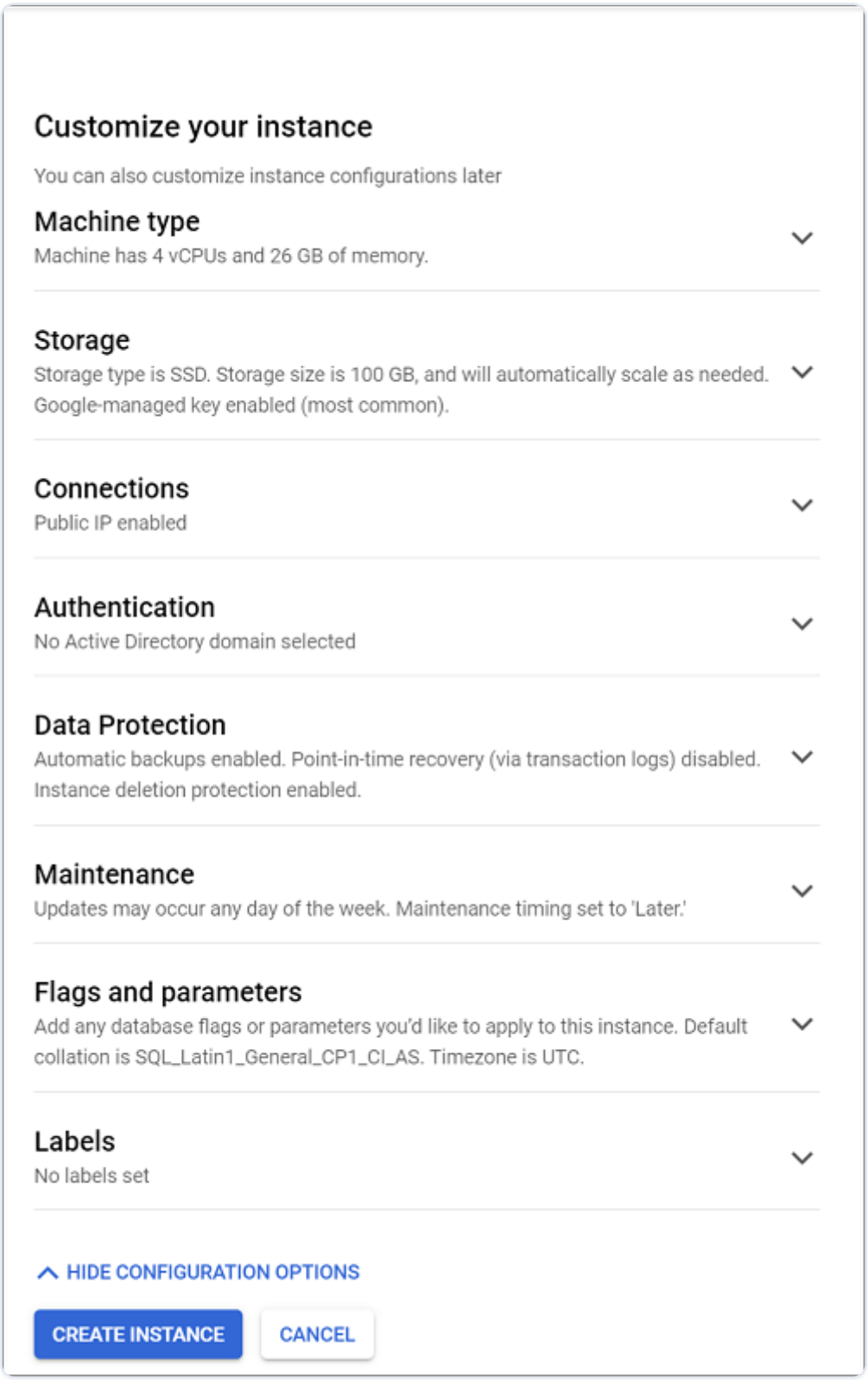
d. Fill in the **Instance ID** field and enter a password for the user. Keep a record of the password. Select a SQL Server version for your instance. Do other configurations as needed. For example:



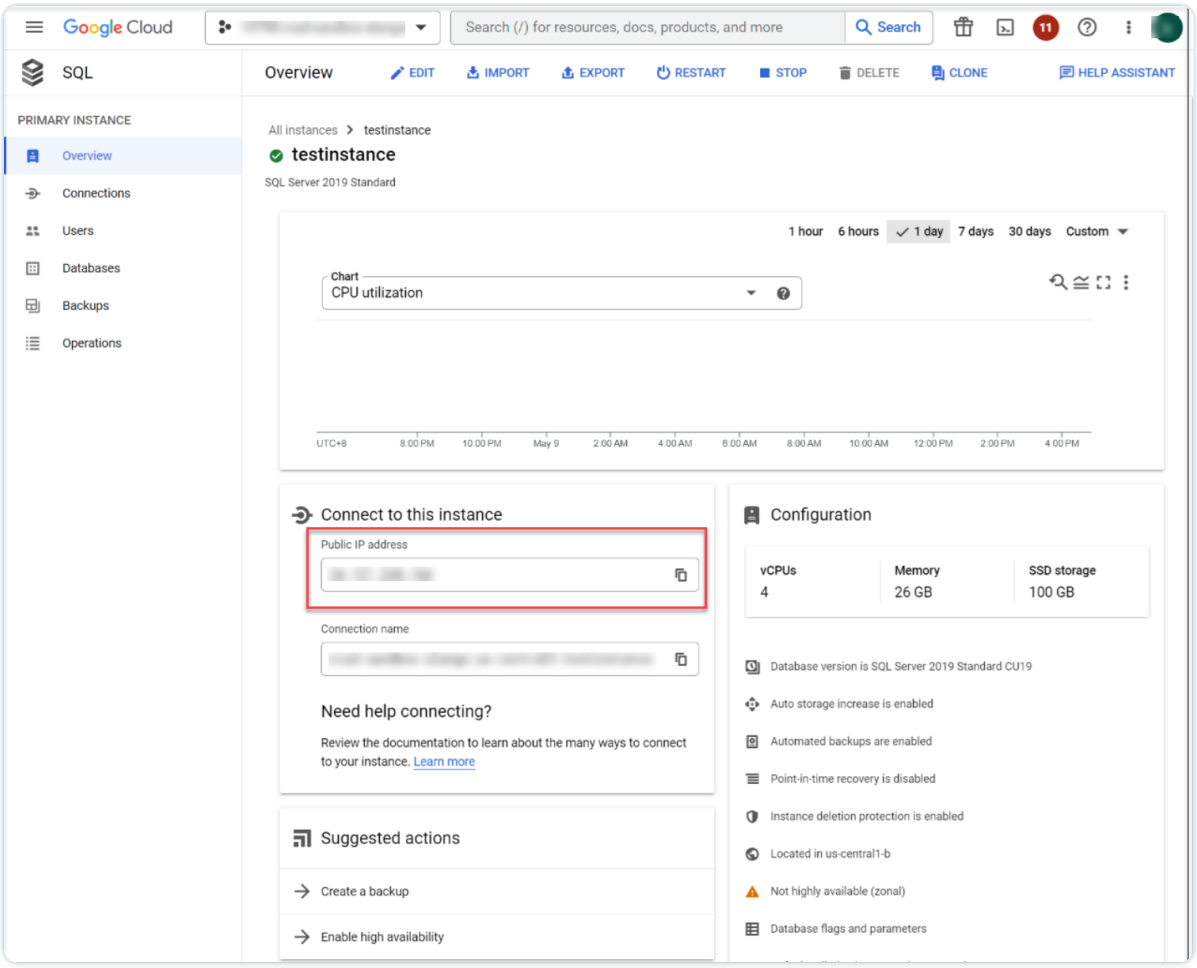
e. Assign the instance a public IP address and set an authorized network that can connect to the instance. In the **Network** field, enter the IP address of the machine where the Session Recording server is installed. For example:



f. Click **CREATE INSTANCE** and wait for a few minutes.



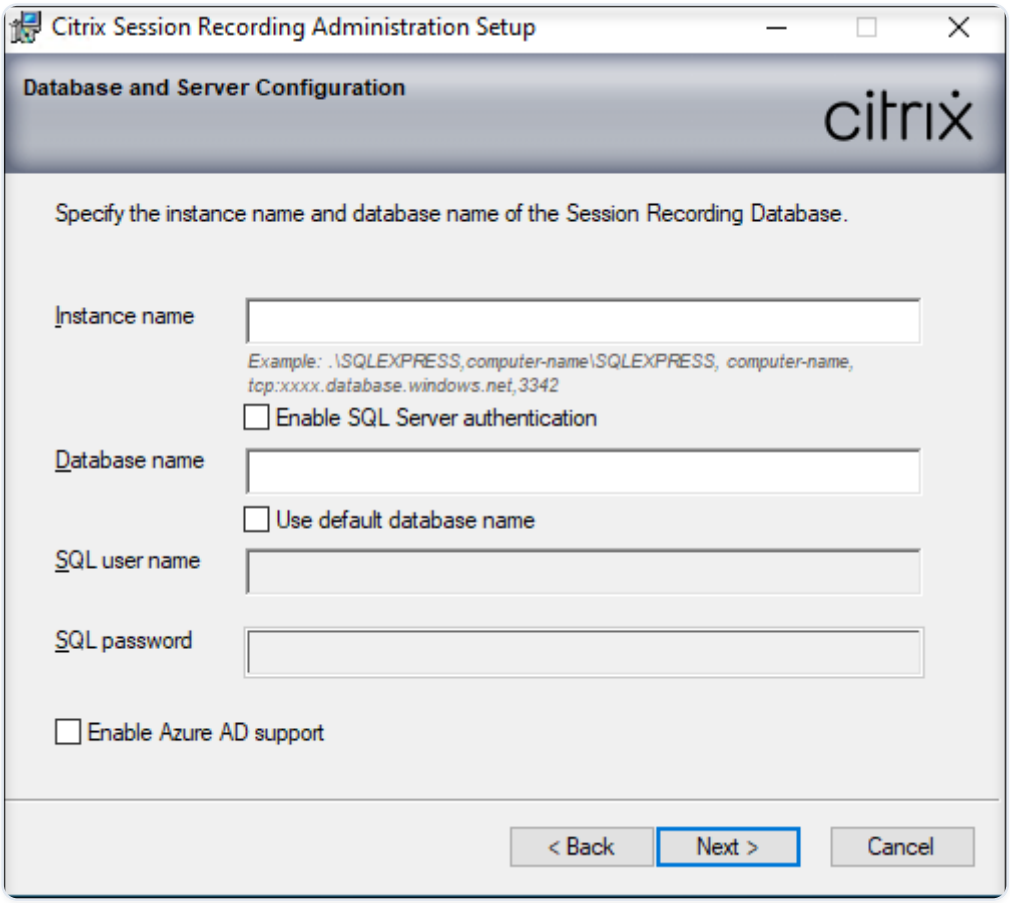
g. On the page of the newly created instance, find the public IP address and keep a record of it.



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

On the following page during the installation, make the following configurations:

- Select the **Enable SQL Server authentication** check box.
- In the **Instance name** field, enter the public IP address of the SQL Server instance that you created earlier.
- Fill in the SQL Server administrator name and password.



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:

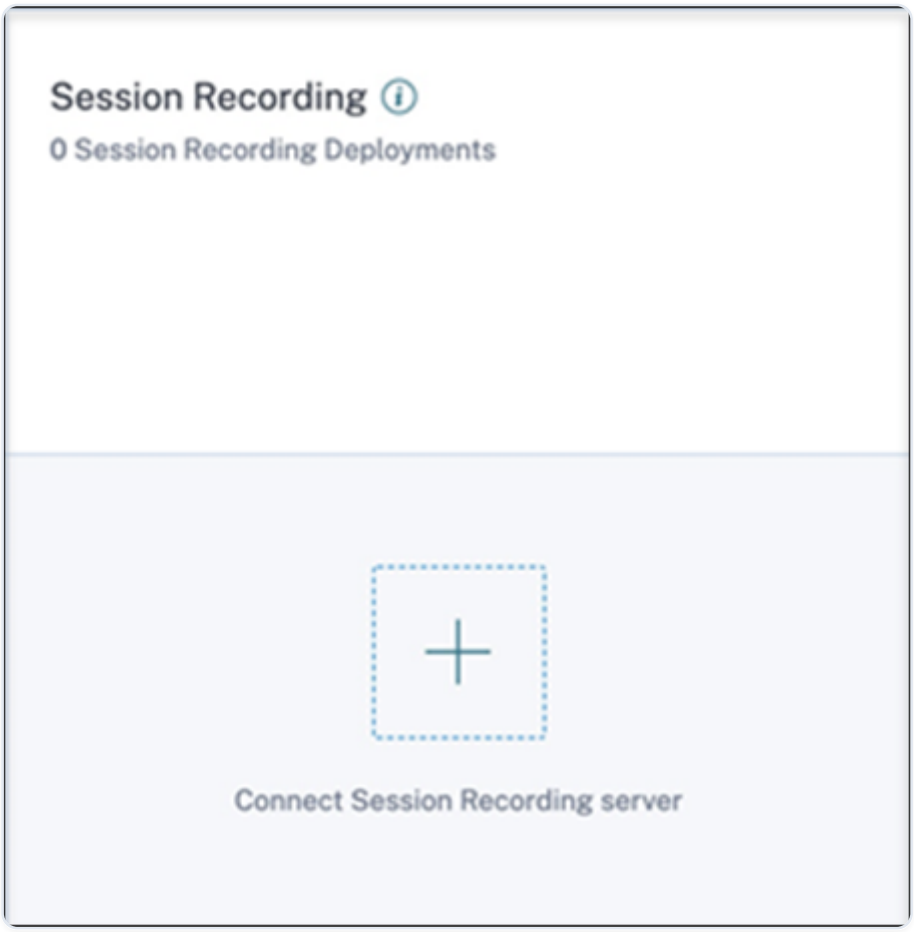
- The Session Recording server must be able to connect to the following addresses:

- `<https://*.cloud.com>`
- `<https://*.citrixdata.com>`
- `<https://api.analytics.cloud.com>`

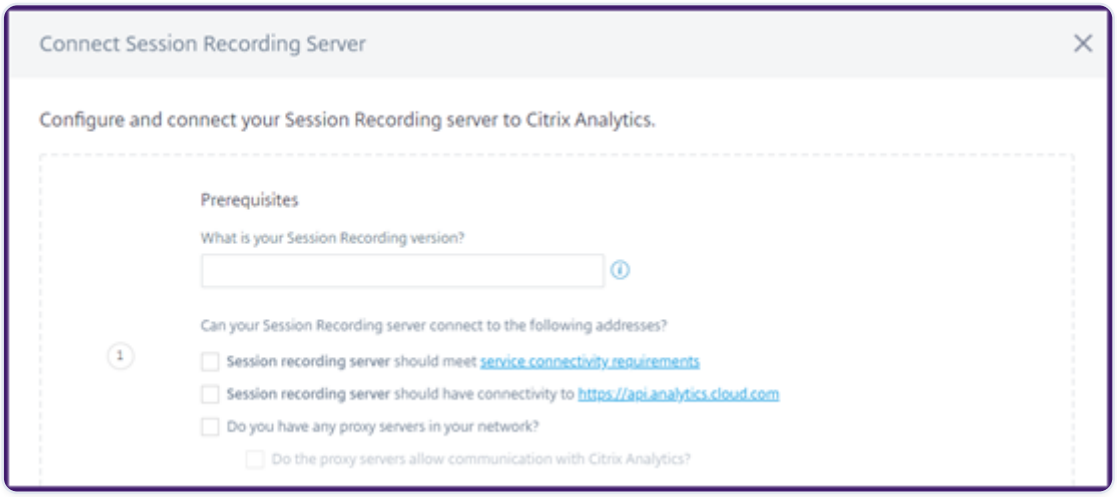
- The Session Recording deployment must have port 443 open for outbound internet connections. Any proxy servers on the network must allow this communication with Citrix Analytics for Security.
- If you are using Citrix Virtual Apps and Desktops 7 1912 LTSR, the supported Session Recording version is 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**.



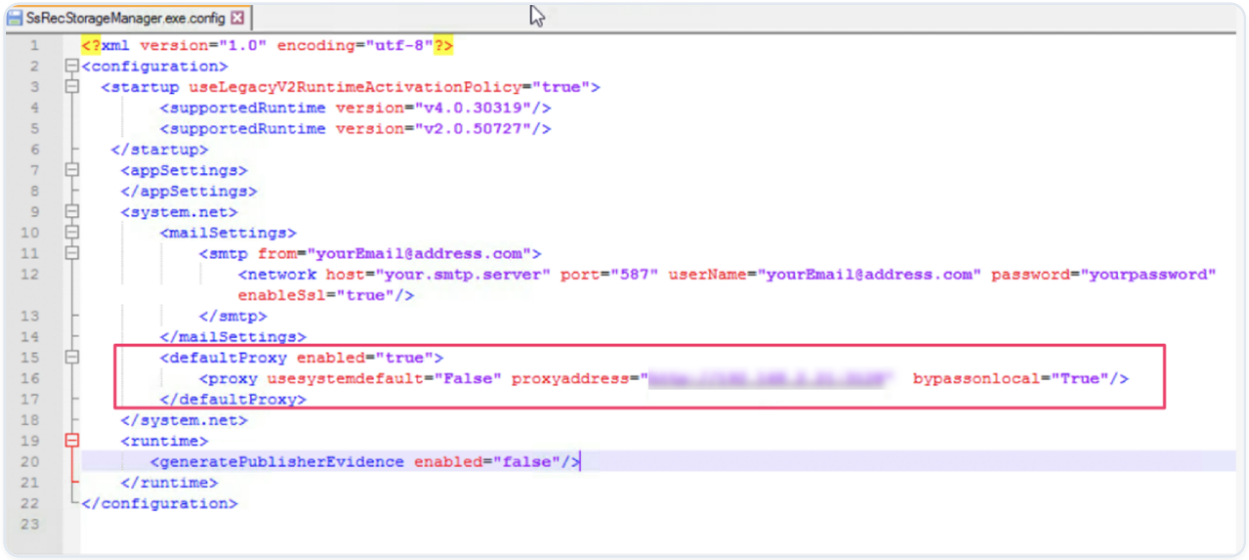
5. On the **Connect Session Recording Server** page, review the checklist, and select all the mandatory requirements. If you do not select a mandatory requirement, the **Download File** option is disabled.



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 `<SessionRecordingserverinstallationpath>\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:

```
<SessionRecordingserverinstallationpath>\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
```

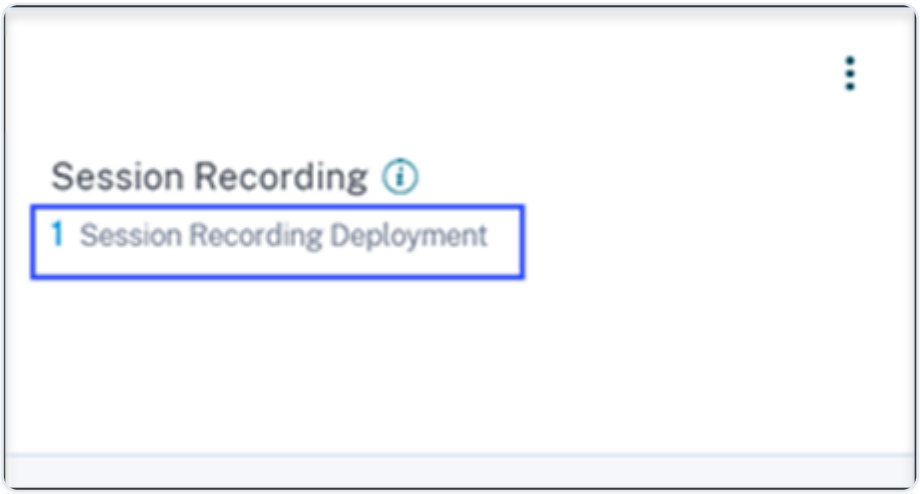
11. Restart the following services:
    - Citrix Session Recording Analytics Service
    - Citrix Session Recording Storage Manager
12. After configuration is successful, go to Citrix Analytics for Security to view the connected Session Recording server. Click **Turn On Data Processing** to allow Citrix 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.

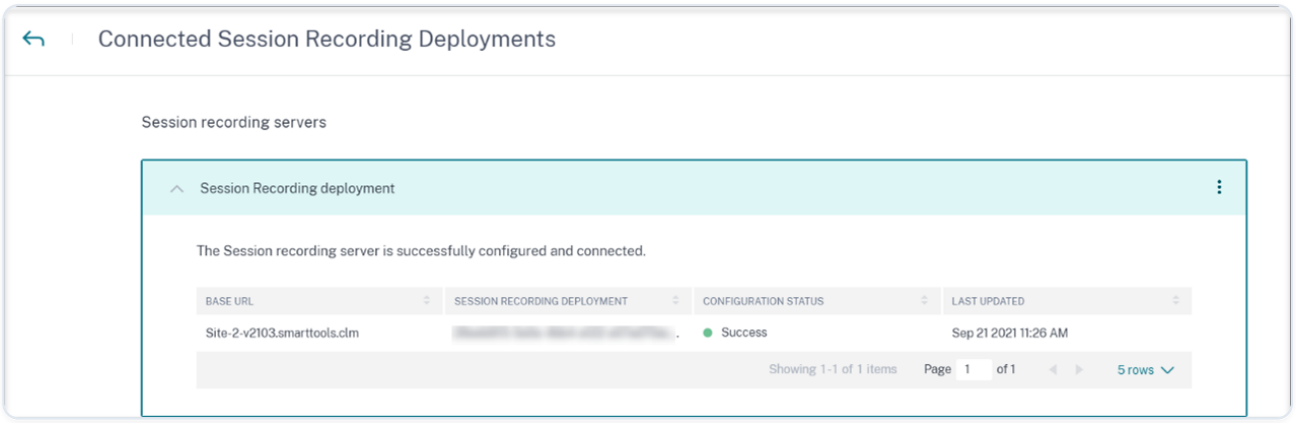
View the connected deployments

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.

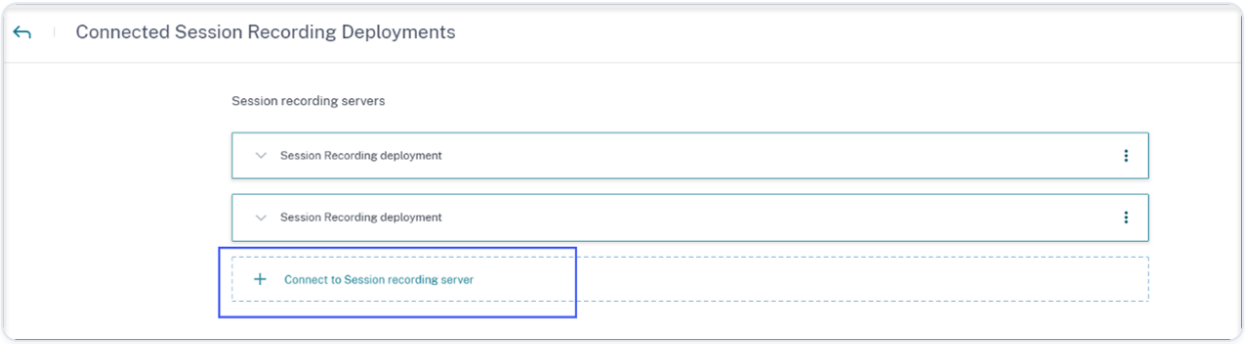
After you have enabled data processing, the site card might display the **No data received** status. This status appears for two reasons:

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.

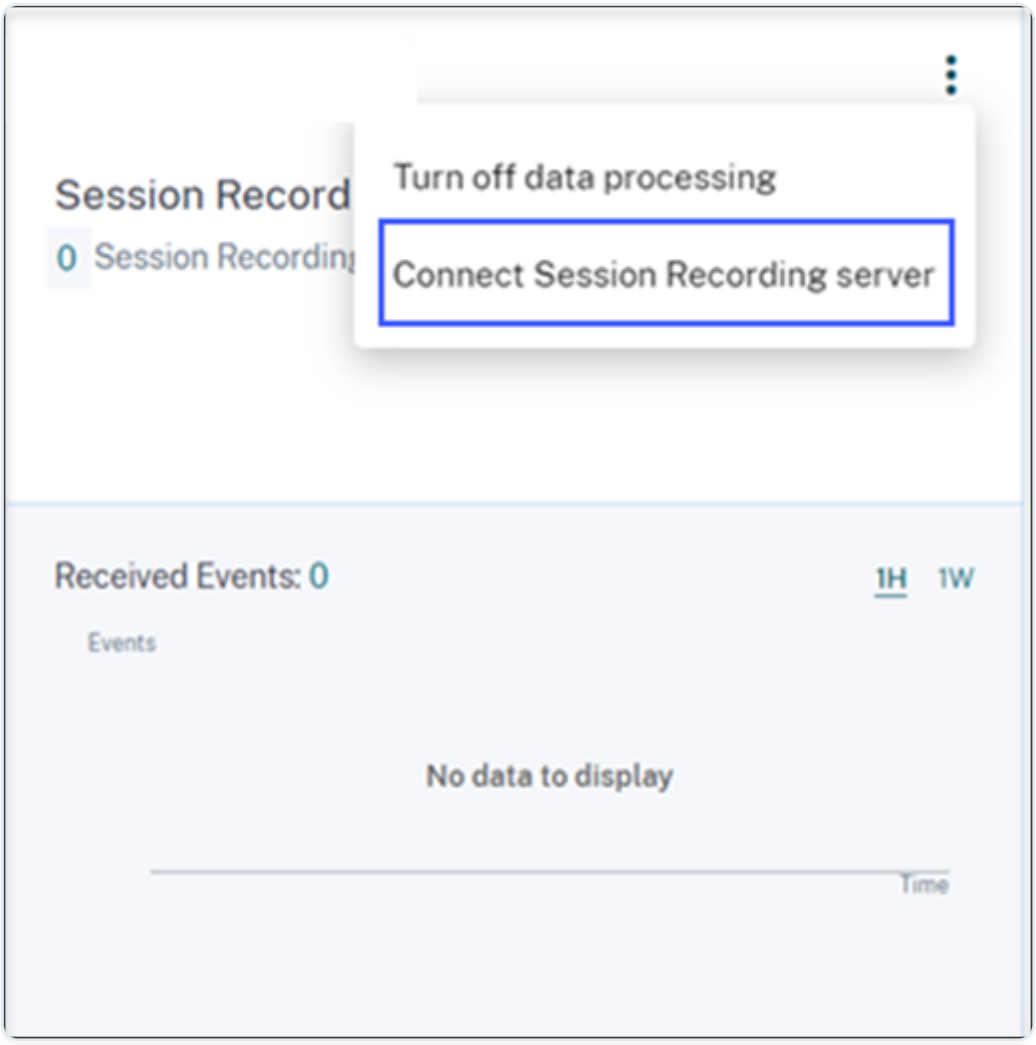
Add Session Recording servers

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**.

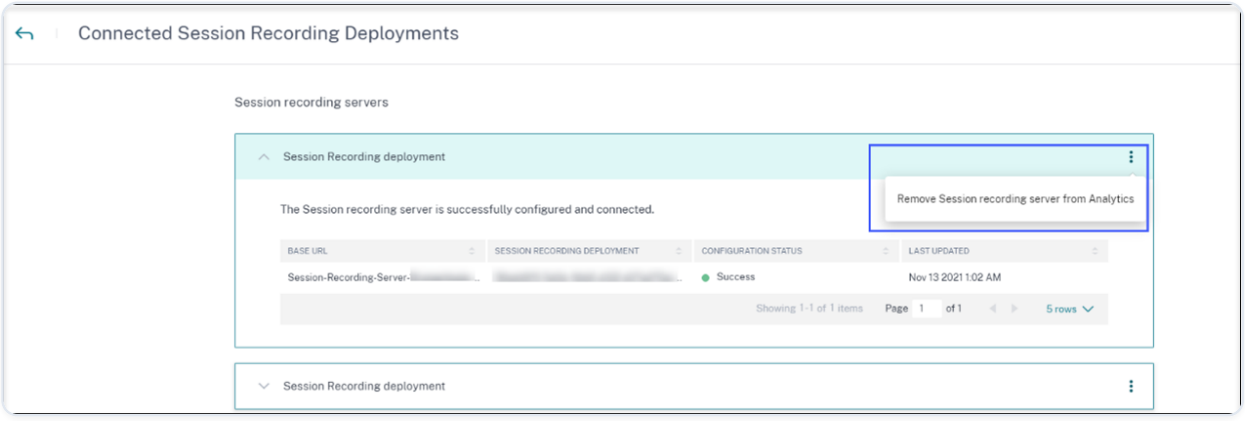


Follow the steps to download the configuration file and configure a Session Recording server.

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:

```
<SessionRecordingserverinstallationpath>\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.

REGISTRY NAME	REGISTRY PATH	KEY TYPE	VALUE
`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

Session recording for endpoint devices (preview)

In addition to recording activities within virtual app and desktop sessions (VDI), Citrix Session Recording also captures user actions on endpoint devices accessing Citrix-delivered web apps, virtual apps and desktops.

Citrix session recording for web apps relies on web apps being delivered through a Citrix infrastructure. The following are the fundamental on-premises Citrix components required for delivering web apps and using session recording for endpoint devices, ensuring that end users can see and launch the configured web apps successfully through Citrix Workspace™ app through NetScaler® Gateway.

- **Citrix Workspace app for Windows**: To use session recording for endpoint devices, ensure that Citrix Workspace app for Windows is installed, version 2503 or later.
- **Secure Private Access**: Secure Private Access enables secure delivery of web apps. Installing this component is a foundational step for making web apps available for recording.
- **StoreFront™**: The application store that users access to launch their web and SaaS apps.
- **NetScaler (ADC/Gateway)**: This component provides secure remote access, load balancing, and traffic management for StoreFront and the web apps.

  > **Note:**
  >
  > Use NetScaler firmware version 14.1 or later to use session recording for endpoint devices.

- **StoreFront and NetScaler (ADC/Gateway) integration**: The integration is key for session recording for endpoint devices to capture remote web app sessions. If the integration is misconfigured or not set up, users can’t launch web apps remotely, leaving no session to record. Refer to the following documentation for integration:
  - Integrate NetScaler Gateway with StoreFront (gateway side): Integrate NetScaler Gateway with StoreFront

- Configure Citrix Gateways (StoreFront side): Configure Citrix Gateways

> **Note:**
>
> This step can be skipped if you are using Citrix Cloud Workspace (cloud-hosted StoreFront).

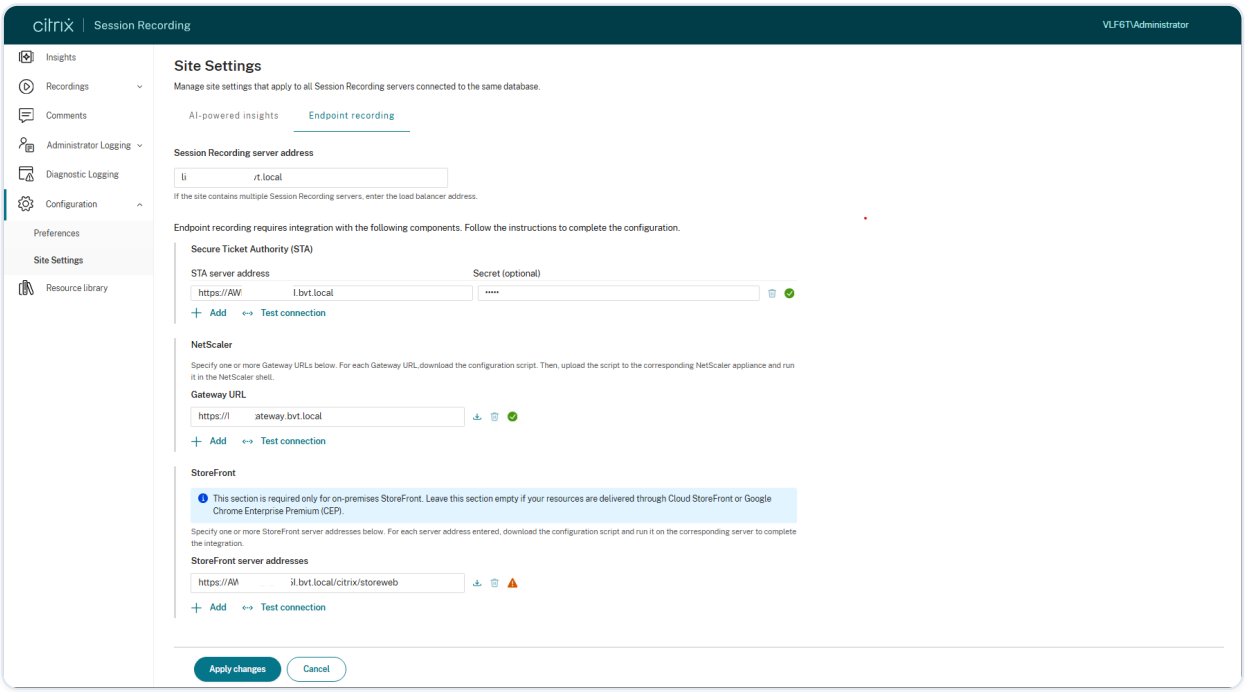
> **Note:**

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

> The procedure for configuring the session recording for endpoint devices feature involves the following steps.

Step 1: Configure settings in Site Setting

1. Open the Session Recording Web Console and navigate to Site Settings, enter the following details
   - Session Recording server address: e.g., https://SRServer.domain.com
   - STA server address: e.g., https://sta.domain.com
   - Gateway URL: e.g., https://gateway.domain.com
   - StoreFront server address: e.g., https://storefront.domain.com/citrix/store
2. Test connection for STA/Gateway/Storefront input.
3. Apply changes.



Step 2: Integrate the Session Recording server with StoreFront

> **Note:**
>
> This step can be skipped if you are using Citrix Cloud Workspace (cloud-hosted StoreFront).

> Perform the following steps to configure StoreFront manually.

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

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

   - No other parameters are required.

- The PowerShell script execution policy must be set to Unrestricted or Bypass to run the StoreFront script.
- The script also propagates the configuration to other StoreFront servers if StoreFront is configured as a cluster.

Step 3: Integrate the Session Recording server with Secure Ticket Authority

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

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

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

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

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

    b. Update Certificate Binding for New HTTPS Port.

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

Step 4: Integrate the Session Recording server with NetScaler

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

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

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

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

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

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

5. Run the uploaded script in the NetScaler shell.

```
root@Netscaler# ./ns_gateway_sessionrecording.sh

************ Gateway configuration ********************
configure session recording FQDN for virtual server
*****************************************************

Note:press Enter button to finish
Input the virtual server Name in Netscaler Gateway:       sg.    local
Input Session Recording FQDN(FQDN:PORT/IP:PORT):        22.    local:443^C
root@Netscaler#
root@Netscaler# ./ns_gateway_sessionrecording.sh

************ Gateway configuration ********************
configure session recording FQDN for virtual server
*****************************************************

Note:press Enter button to finish
Input the virtual server Name in Netscaler Gateway: _XD_10.147.210.44_443
Input Session Recording FQDN(FQDN:PORT/IP:PORT):          r.    local:443
Press Enter to quit, any key else to continue...
NetScaler Gateway creation script ns_gateway_sessionrecording created
Please copy it to NetScaler (e.g. /var/tmp folder) and run command:
batch -fileName /var/tmp/ns_gateway_sessionrecording -outfile /var/tmp/ns_gateway_sessionrecording_output
Check ns_gateway_sessionrecording_output file for output
root@Netscaler#
```

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

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

```
root@Netscaler# cat ns_gateway_sessionrecording
#############################################################################################################################
#1. Upload file to NetScaler (e.g. to /var/tmp)                                                                             #
#2. Run batch command (e.g. batch -fileName /var/tmp/ns_gateway_sessionrecording -outfile /var/tmp/ns_gateway_sessionrecording_output)    #
#3. Analyze output (e.g. cat /var/tmp/ns_gateway_sessionrecording_output)                                                   #
#############################################################################################################################
bind vpn vserver _XD_10.147.210.44_443 -sharefile          .bvt.local:443
save ns config
root@Netscaler#
```

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

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

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

8. Ensure that all commands were successfully completed.

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

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

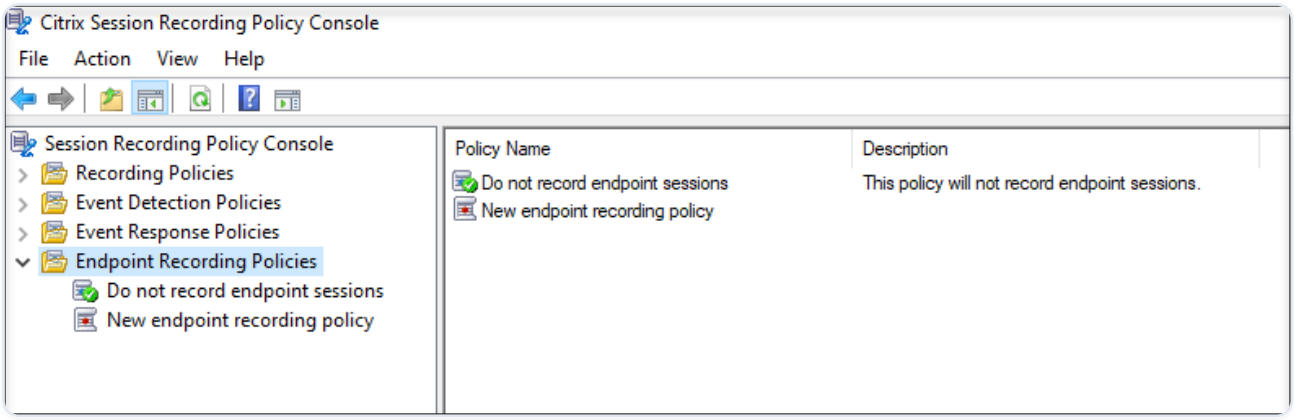
> **Note:**
>
> If you are using Citrix Workspace app for Windows version 2503, ensure that ICA® Proxy mode is set to OFF on the Citrix NetScaler Gateway to enable endpoint recording functionality.

> For detailed configuration steps, refer to the NetScaler command reference guide.

Step 5: Configure endpoint recording policies

System-defined endpoint recording policy

Session Recording provides a system-defined endpoint recording policy:



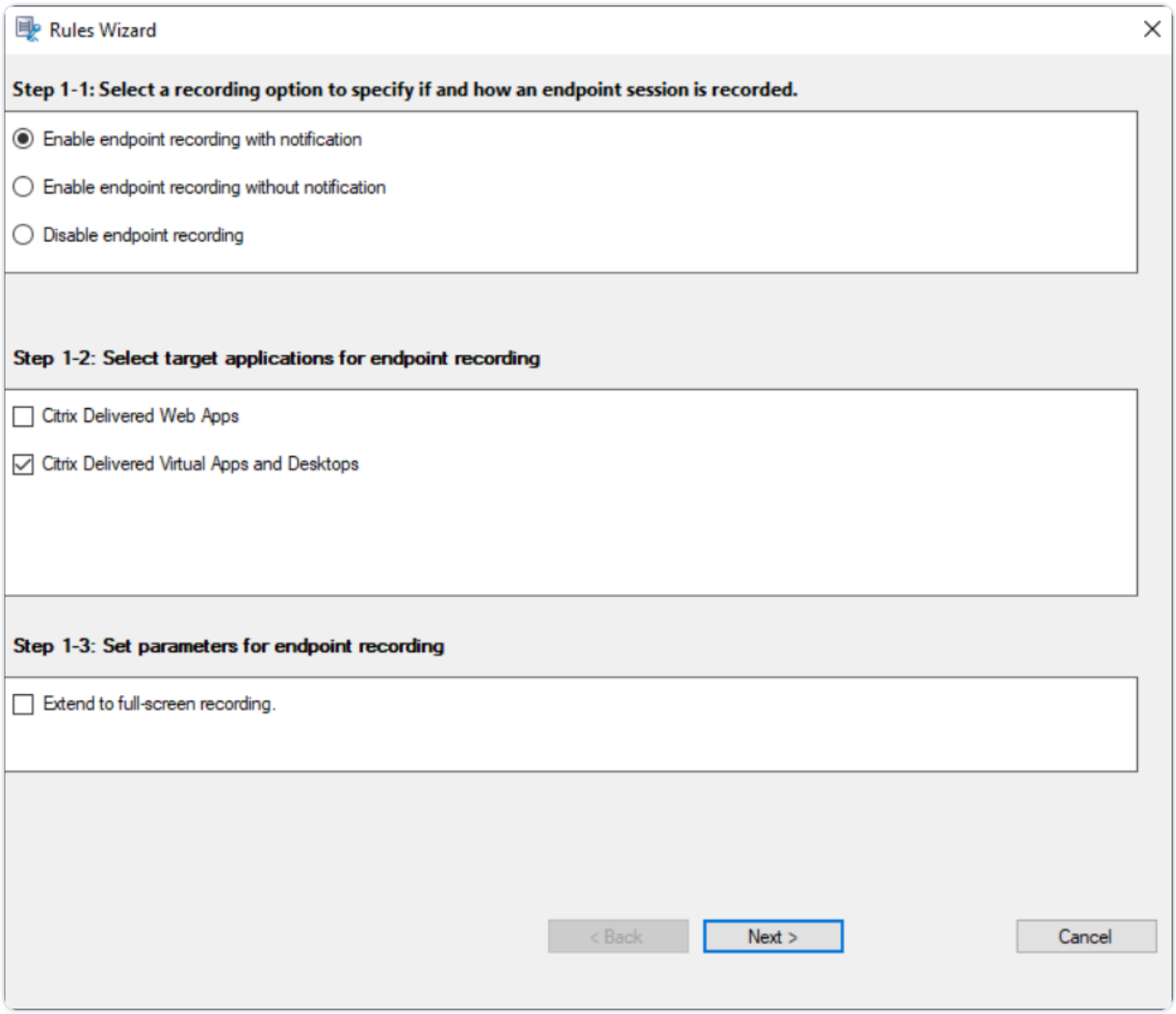
- **Do not record endpoint sessions**. The default policy. When it's active, Session Recording does not capture user actions on endpoint devices accessing Citrix-delivered web apps.

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

Create a custom endpoint recording policy

You can enable endpoint recording for specific users or groups. A wizard within the Session Recording policy console helps you create rules. For each rule you create, you specify a recording action and rule criteria. The recording action applies to sessions that meet the rule criteria.

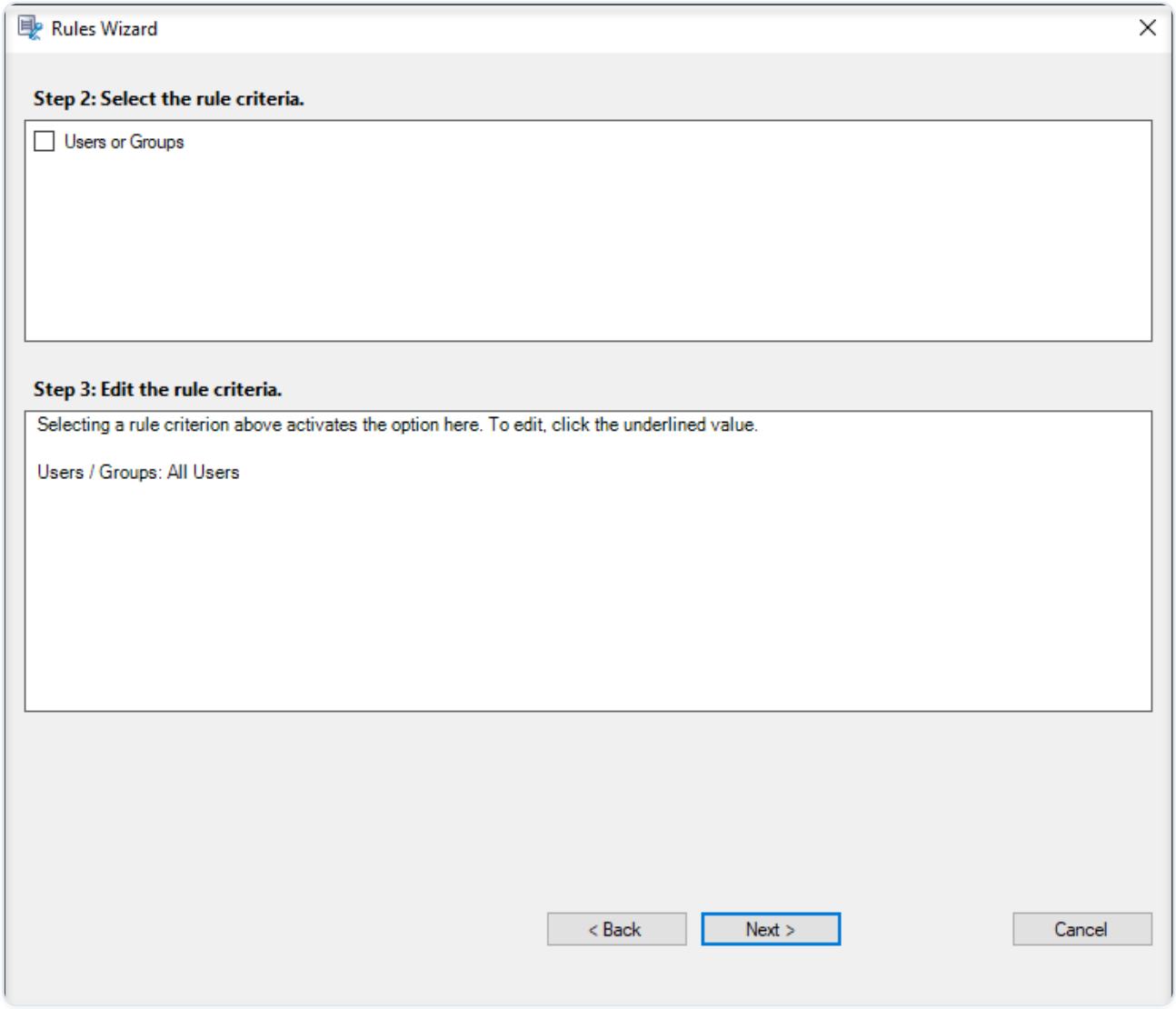
For each rule, choose one recording action:



- **Enable endpoint recording with notification**. This option records user actions on endpoint devices accessing Citrix-delivered web apps. Users receive recording notifications in advance.
- **Enable endpoint recording without notification**. This option records user actions on endpoint devices accessing Citrix-delivered web apps. Users do not receive recording notifications.
- **Disable endpoint recording**. This option means that no user actions on endpoint devices are recorded.
- **Citrix Delivered Web Apps**. This option lets you specify particular Citrix-delivered web apps for recording user actions on endpoint devices accessing these apps.
- **Citrix Delivered Virtual Apps and Desktops**. This option lets you specify particular Citrix-delivered virtual apps and desktops for recording user actions on endpoint devices accessing these apps.

- **Extend to full-screen recording**. This option lets you record the entire screen space, including any extended displays, of the endpoint devices accessing the specified Citrix-delivered web apps.

For each rule, create a list of users or groups to which the action of the rule applies:



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

The recording action of a rule determines its priority:

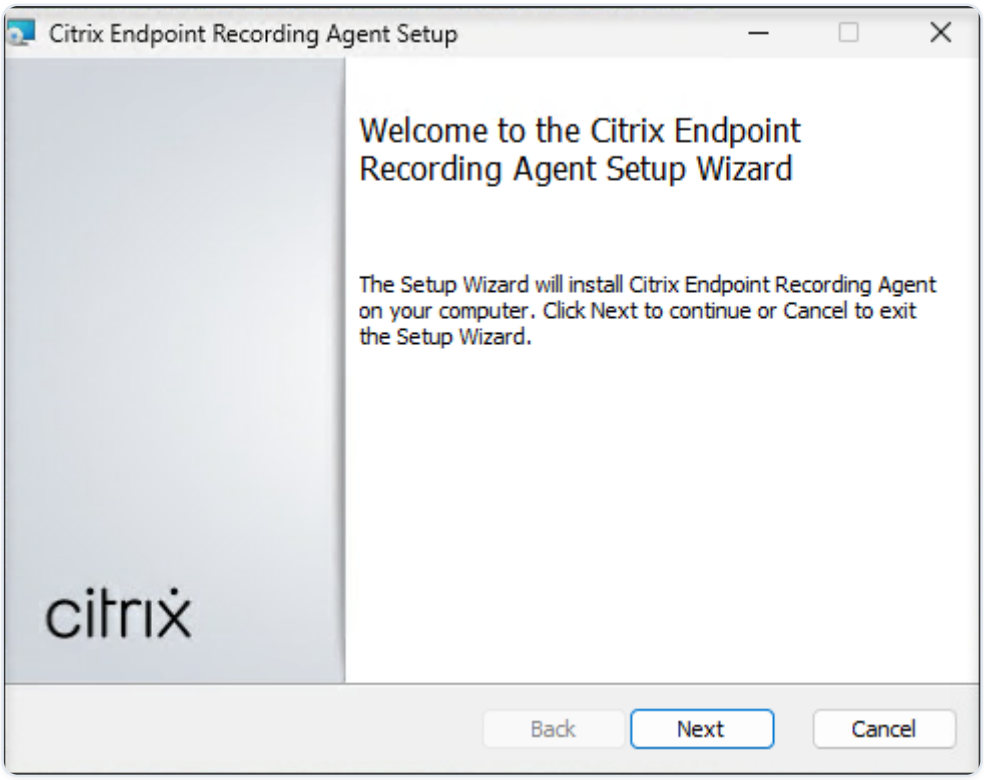
- Rules with the **Disable endpoint recording action** have the highest priority.
- Rules with the **Enable endpoint recording with notification** action have the second-to-highest priority.
- Rules with the **Enable endpoint recording without notification** action have the lowest priority.

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

Step 6: Install the Citrix session recording for endpoint devices agent

To enable session recording for endpoint devices, install the session recording agent for endpoint devices on each client where you install the Citrix Workspace app. To install the session recording agent for endpoint devices, follow these steps:

1. Ensure that Citrix Workspace app for Windows is installed, version 2503 or later.
2. Install the session recording agent for endpoint devices using either the GUI or the command prompt.



3. Exit Citrix Workspace app for Windows from the system tray, and then reopen it.

> **Note:**
>
> - Temporarily disable any anti-screen capture features when installing the session recording agent for endpoint devices.

- If using Citrix Workspace app authentication and the self-service plug-in:
  - Either disable the anti-screen capture feature entirely (see Configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in).
  - Or add the session recording agent for endpoint devices executable (SRGraphicsEngine.exe) to the screen capture allow list (see Configure Screen Capture Allow List).
- For web and SaaS apps, see Configure Anti-keylogging and Anti-screen capture for Web and SaaS apps for specific anti-keylogging and anti-screen capture configurations.
- For virtual apps and desktops, see Configure Anti-keylogging and Anti-screen capture for anti-screen capture configurations.

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.

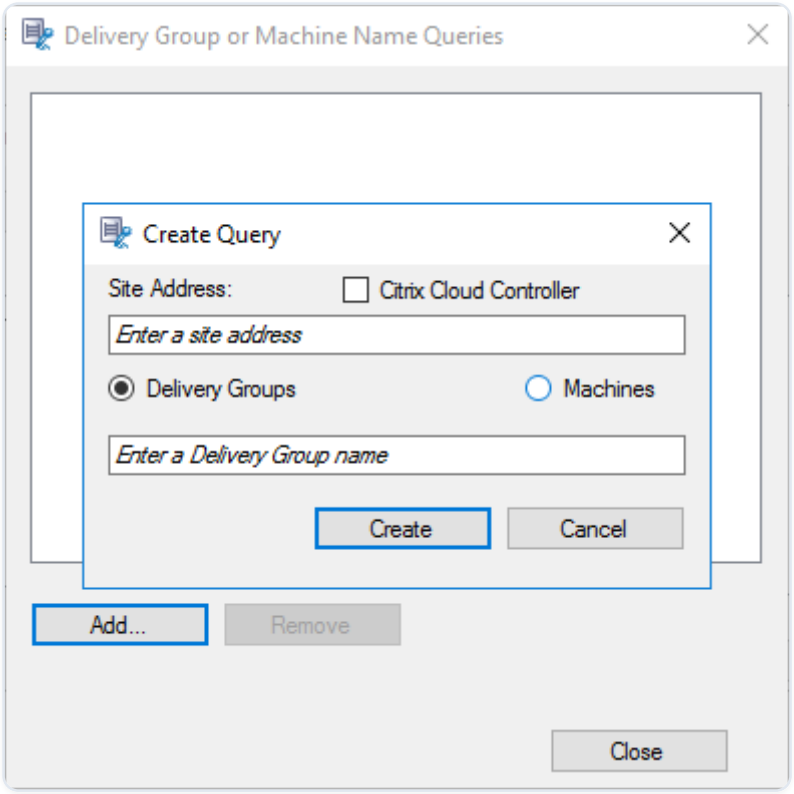
> **Warning:**

> 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

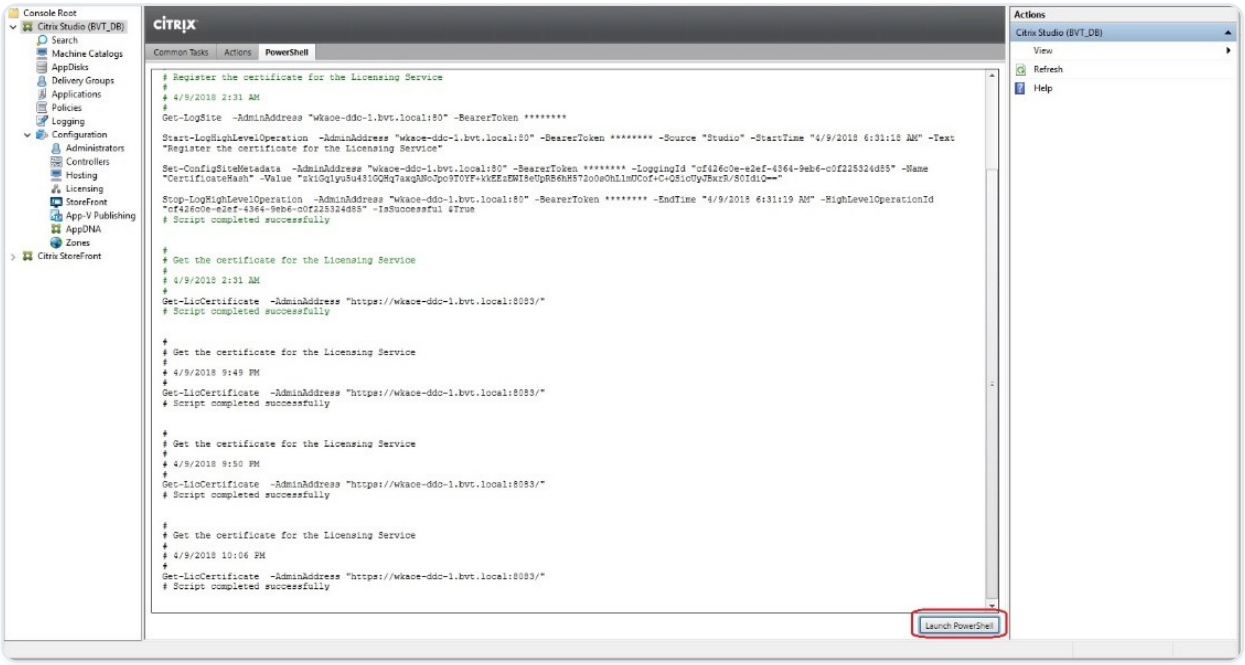
> the same resource location. We recommend that you do not run this SDK's cmdlets on Cloud Connectors. The SDK's operation does not involve the Cloud Connectors.

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

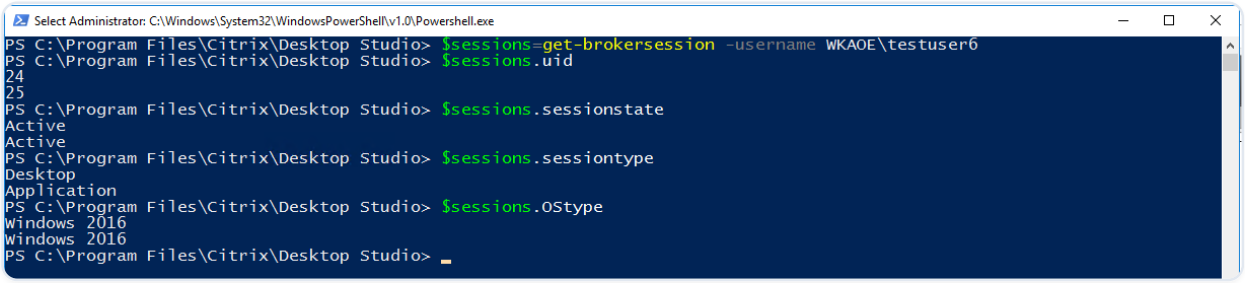
COMMAND	DESCRIPTION
Start-BrokerSessionRecording	Lets you start recording a specific active session, a list of active sessions, or sessions launched by a specific user. If a specific session is originally set up for an event-only recording according to policy settings, using this command allows you to start capturing the screen in addition to the target events. 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 recordings and proceed with the follow-up troubleshooting.

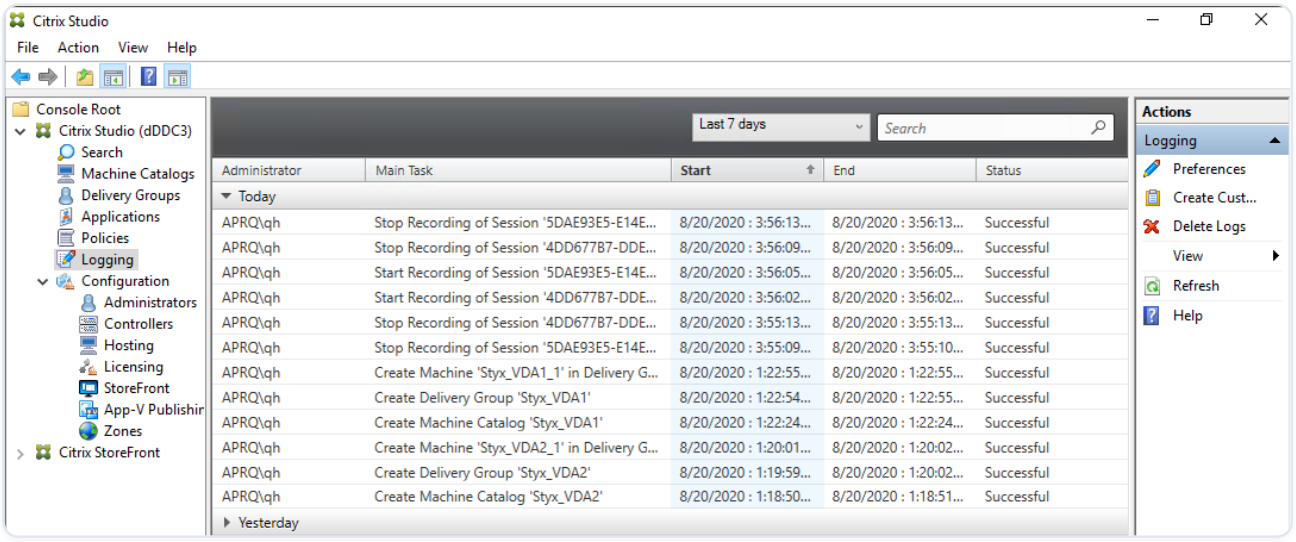
> **Note：**
>
> When you play a **Complete** recording by Session Recording Player ended by the `Stop-BrokerSessionRecording` command, the last section of the timeline on the player progress bar might show gray. And, the last section of the recorded session is idle. It is not obvious when the recorded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

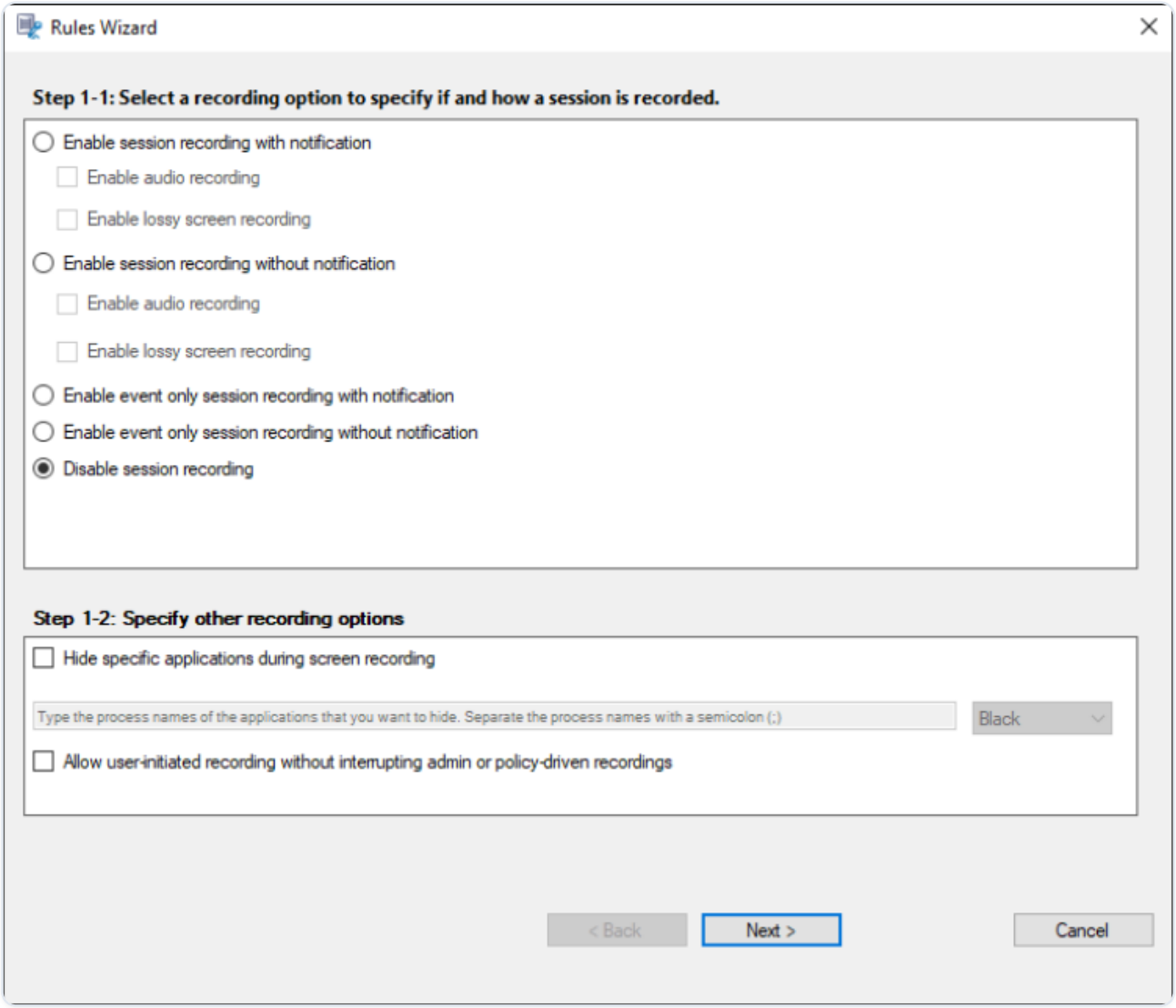


End-user triggered session recording

Previously, session recording started strictly based on the recording policies configured by administrators. Starting with the current release, Session Recording introduces the end-user triggered session recording feature. With this feature, end users can start or stop recording their own sessions at any time, providing greater flexibility for on-demand recording needs.

Enable end-user triggered recording

By default, end-user triggered recording is disabled. To enable this feature, you must configure a recording policy in the Session Recording Policy Console. For more information about how to configure the customized policy, see Create a custom recording policy.



Start or stop recording by using Citrix Virtual Desktop Assistant

The Citrix Virtual Desktop Assistant, installed by default in CVAD, provides a built-in Session Recording page that enables users to manually record their active virtual desktop sessions.

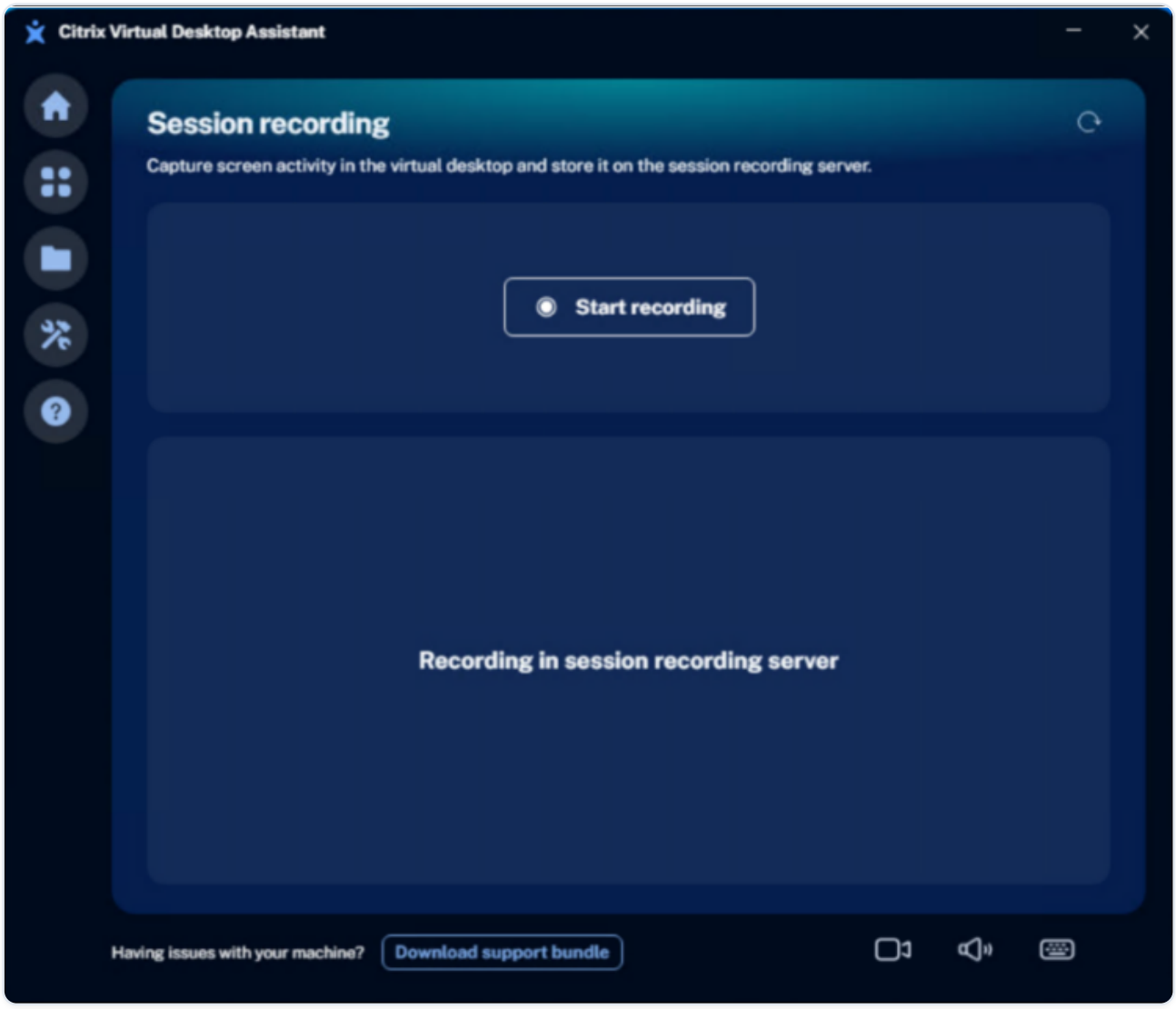


Start recording

Starts capturing the current session. A recording indicator is displayed to confirm that recording is in progress.

Stop recording

Stops the recording and automatically saves the recorded session to the Session Recording server.



Start or stop recording by using PowerShell commands

End users can trigger recording through PowerShell commands after importing the required model.

Import the Session Recording Module

Before running the recording commands, you must import the necessary module into the PowerShell session. Open PowerShell and Import the module by running:

```
Import-Module -DisableNameChecking 'C:\Program Files\Citrix\SessionRecording\Agent\Bin\EndUserInitiatedSRSnapin.dll'
```

Available Commands

The following table lists three PowerShell commands that provide for end user triggered session recording.

COMMAND	DESCRIPTION
Start-SessionRecording	Starts recording the active session in which the command is executed. To record a specific active session, use the `-SessionId <ID>` parameter (requires local administrator privileges). For more information, run `Get-Help Start-SessionRecording` to see the command online help.
Stop-SessionRecording	Stops recording the active session in which the command is executed. To stop recording a specific active session, use the `-SessionId <ID>` parameter (requires local administrator privileges). Note: Users can only stop recordings they initiated. They cannot stop recordings triggered by dynamic or policy-based recording. For more information, run `Get-Help Stop-SessionRecording` to see the command online help.
Get-SessionRecordingStatus	Retrieves the recording status of the active session in which the command is executed. To get the status of a specific active session, use the `-SessionId <ID>` parameter. For more information, run `Get-Help Get-SessionRecording` Status to see the command online help.

Scenario 1: End-user triggered recording

End users can trigger recordings for their current active session to capture operations dynamically (for example, for troubleshooting purposes).

The user can perform the following steps inside the session:

1. Launch PowerShell from the session desktop.
2. Import the module as described in the previous section.
3. Use the `Get-SessionRecordingStatus` command to check the recording status, ensure the session is not already being recorded.
4. Use the `Start-SessionRecording` command to start recording the session.

5. Use the `Get-SessionRecordingStatus` command to check the recording status, ensure the session is being recorded. The status is supposed to be **Recording**.
6. Reproduce the issue or perform the operations that need to be documented.
7. Use the `Stop-SessionRecording` command to stop recording once the operations are complete.
8. Inform the administrator to playback the **Live** or **Complete** recordings and proceed with the follow-up troubleshooting.

Scenario 2: Administrator-triggered recording

Administrators can trigger recordings for specific active sessions on the machine (for example, to assist a user with troubleshooting).

The administrator can perform the following steps on the machine hosting the session:

1. Launch PowerShell as an administrator.
2. Import the module as described in the previous section.
3. Get the `SessionID` of the target user session by using : query session \| find "Active".
4. Use the `Get-SessionRecordingStatus -SessionId <SessionID>` command to check the recording status, ensure the session is not already recorded.
5. Use the `Start-SessionRecording -SessionId <SessionID>` command to start recording the session.
6. Use the `Get-SessionRecordingStatus -SessionId <SessionID>` command to check the recording status, ensure the session is being recorded. The status is supposed to be **Recording**.
7. Instruct the user to reproduce the issue or perform the operations that need to be documented.
8. Use the `Stop-SessionRecording -SessionId <SessionID>` to stop recording once the operations are complete.
9. Playback the **Live** or **Complete** recordings and proceed with the follow-up troubleshooting.

Start or stop recording by using Hotkeys

End users can also control recording using shortcut keys (Hotkeys). By default, this feature is disabled.

Enable Hotkeys

To enable the hotkey functionality, add a **DWORD** value named `EnableHotKeys` under the registry path: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\EndUserRecording` Set the value to **1** on the VDA machine. This setting is applied **per machine** and will take effect for all **subsequent active sessions**.

Default Hotkeys

Once enabled, the default hotkeys are:

- **Start recording**: CTRL + SHIFT + F8
- **Stop recording**: CTRL + SHIFT + F9

Customize Hotkeys

If the default hotkeys conflict with other applications, add or modify the following REG_SZ values under:

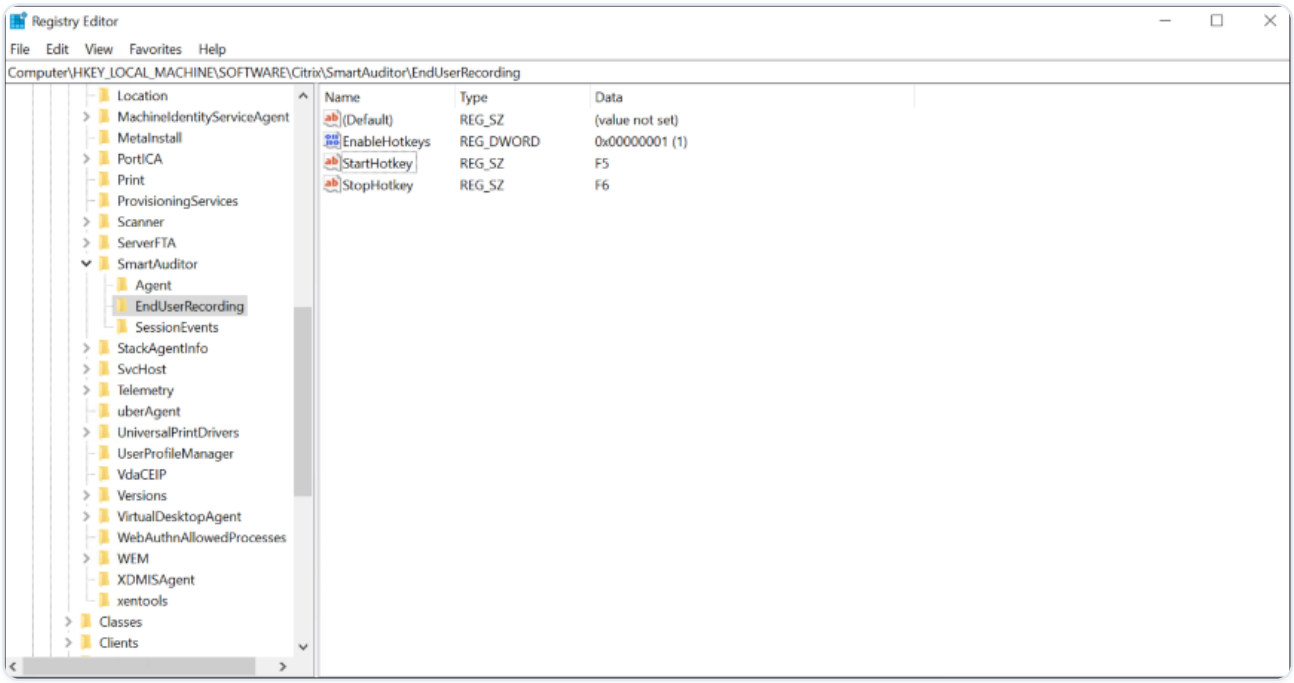
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\EndUserRecording`

- **StartHotkey** – specify the new hotkey for starting to record
- **StopHotkey** – specify the new hotkey for stopping to record

Hotkey rules

- Only **F1–F12** or **capital letters (A–Z)** can be used as the last key.
- You only define the **last key** in the combination. The CTRL + SHIFT prefix is mandatory and automatically applied.

Example: To set the start hotkey to **CTRL + SHIFT + F5**, set the value of **StartHotkey** to F5.


Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\EndUserRecording
Location
MachineIdentityServiceAgent
MetaInstall
PortICA
Print
ProvisioningServices
Scanner
ServerFTA
SmartAuditor
Agent
EndUserRecording
SessionEvents
StackAgentInfo
SvcHost
Telemetry
uberAgent
UniversalPrintDrivers
UserProfileManager
VdaCEIP
Versions
VirtualDesktopAgent
WebAuthnAllowedProcesses
WEM
XDMISAgent
xentools
Classes
Clients
Name Type Data
(Default) REG_SZ (value not set)
EnableHotkeys REG_DWORD 0x00000001 (1)
StartHotkey REG_SZ F5
StopHotkey REG_SZ F6

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 recording notification messages
  - Specify where recordings are stored
  - Specify file size for recordings
  - Enable or disable digital signing
  - CEIP and Google Analytics
- Policies (policy console)
  - Configure session recording policies
  - Configure recording viewing policies
  - Configure event detection policies
  - Configure event response policies
- Policies (web console)
  - Configure session recording policies
  - Configure event detection policies
  - Configure event response policies
  - Configure endpoint recording 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

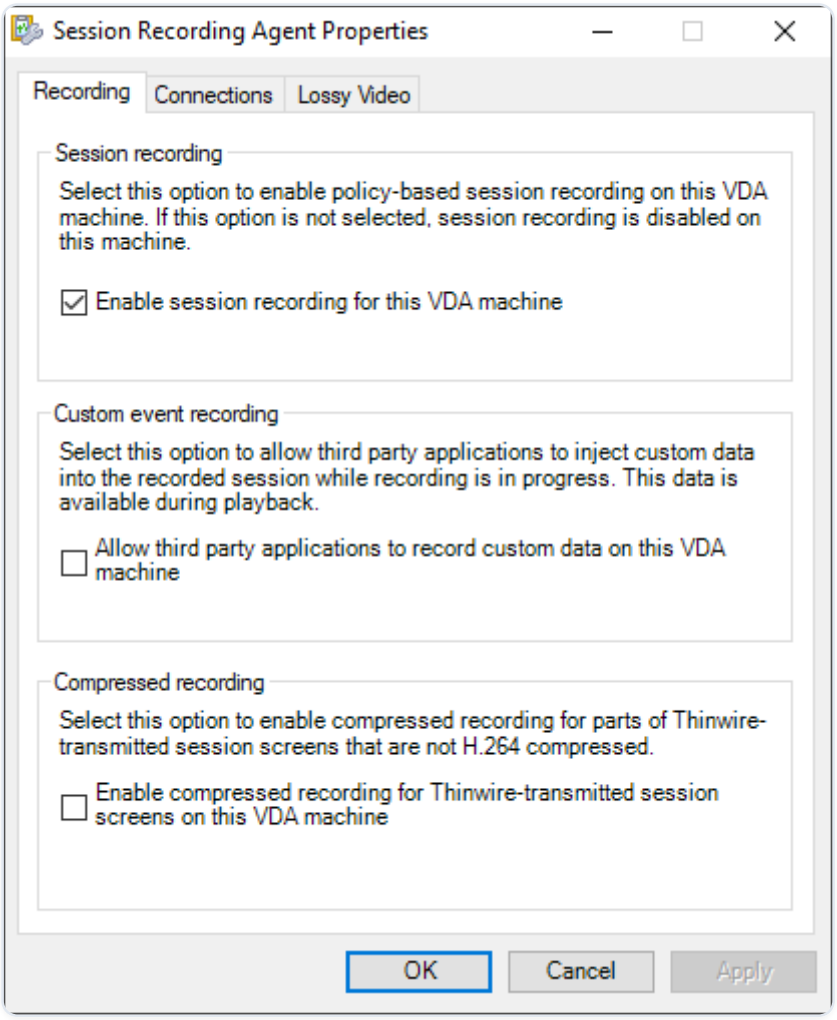
Enable or disable recording

You can install the Session Recording agent on both multi-session OS and single-session OS VDAs for recording sessions hosted on those VDAs. 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.

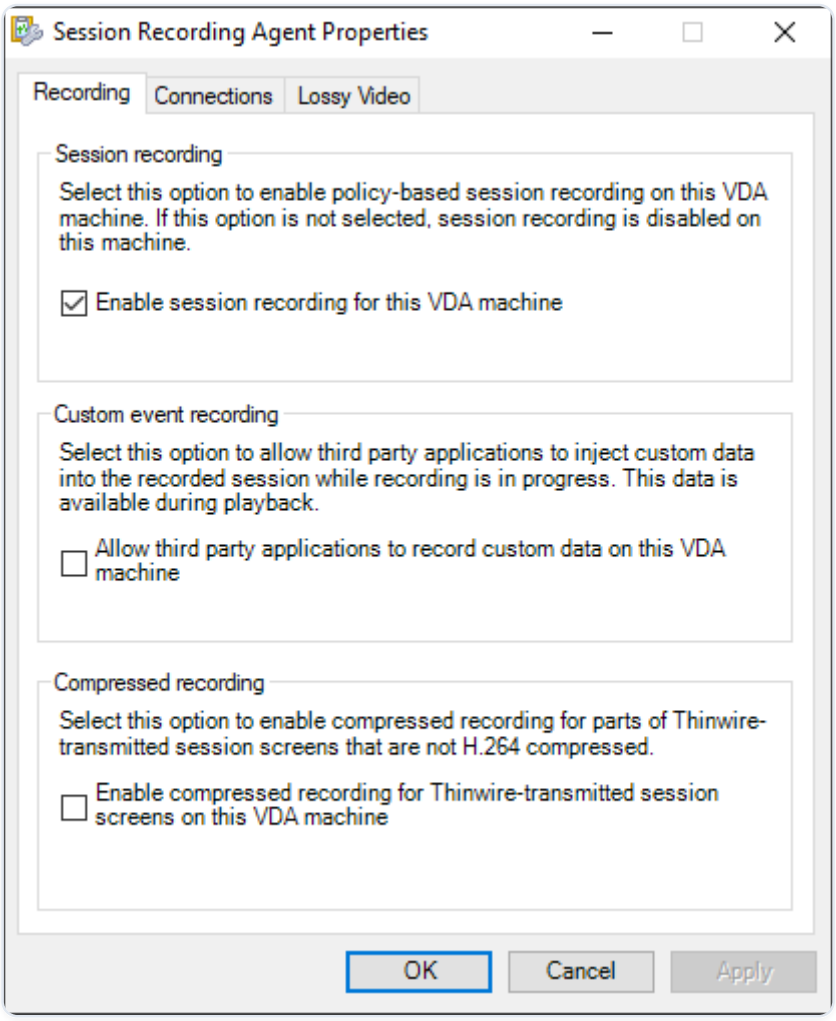
Enable compressed recording

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 screen recording

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

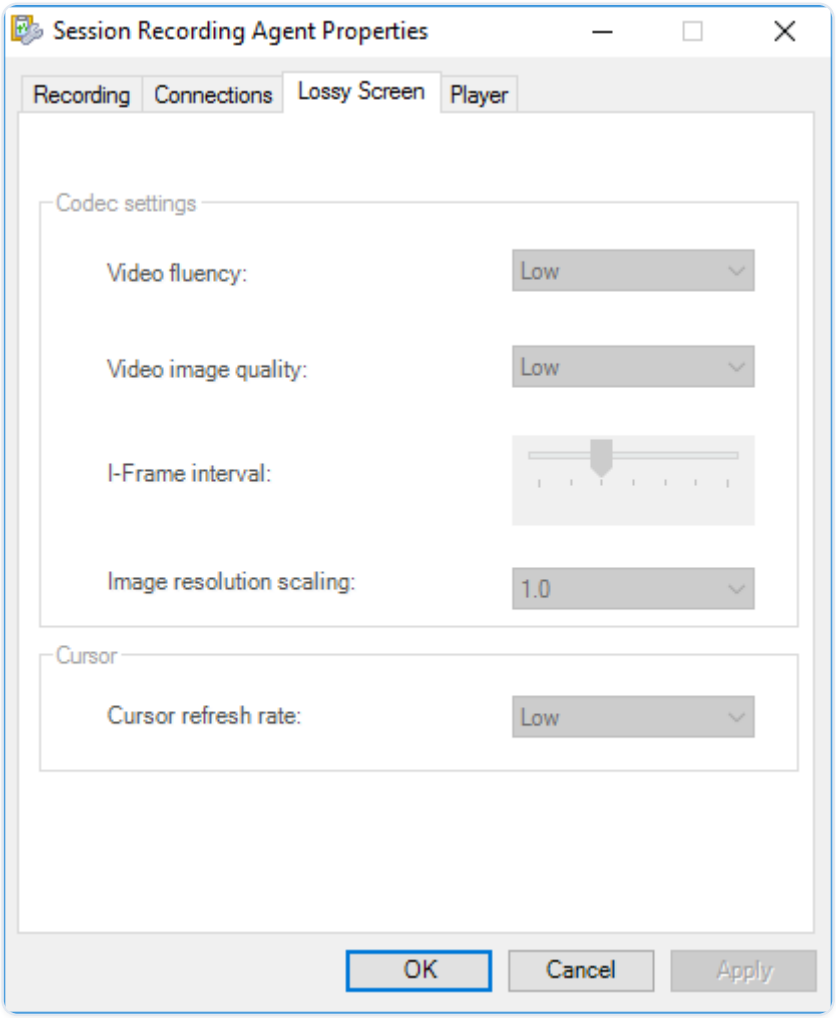
- the size of recording files per time unit is too large, or
- there is a lag while you fast forward or rewind during recording playback.

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

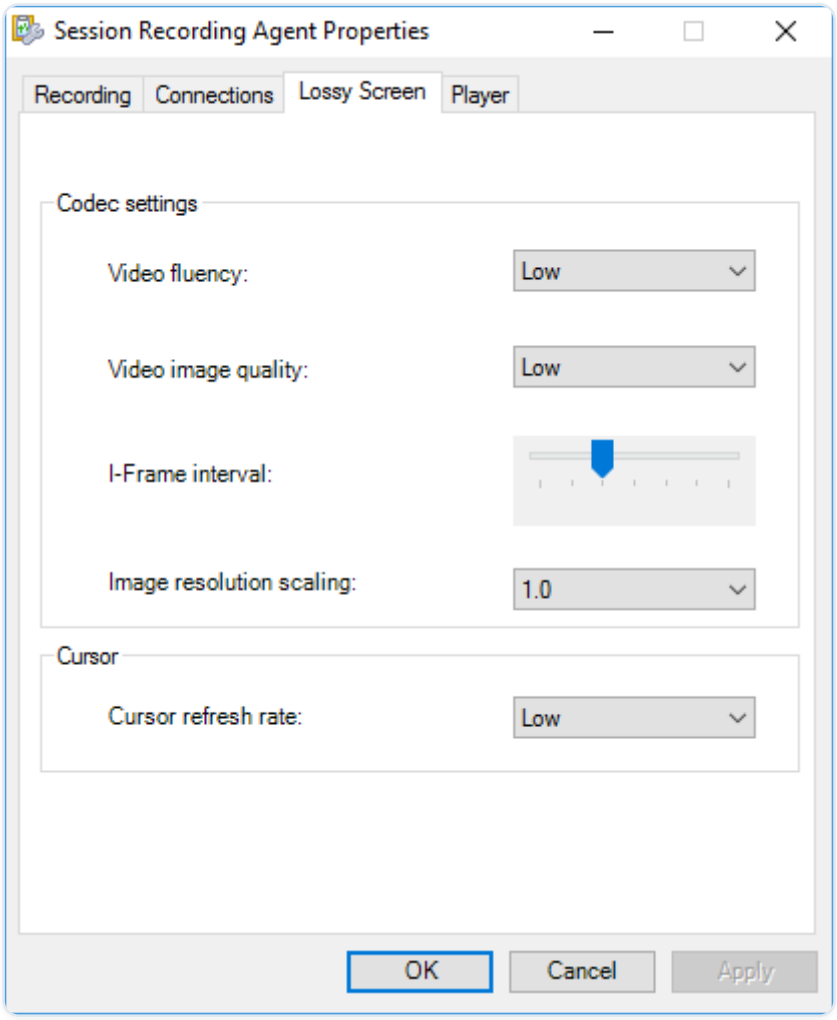
- Activate a system-defined session recording policy that has lossy screen recording enabled.
- Create and activate a custom session recording policy, and make sure to select **Enable lossy screen recording** when creating the custom policy.
- Select **Enable lossy screen recording** when configuring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

For more information, see Configure session recording policies and Configure event response policies.

When the active session recording or event response policy doesn't have lossy screen recording enabled, compression options are unavailable.



When the active session recording or event response policy has lossy screen recording enabled, compression options are available on the **Lossy Screen** tab of **Session Recording Agent Properties**.



You can 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**: 5; **High**: 10	**Low**	N/A
Video image quality	**Low**: `bitrate:140 (kbps)`; **Medium**: `bitrate:280 (kbps)`; **High**: bitrate: `420 (kbps)`	**Low**	Session Recording uses Average Bitrate (ABR) for video bitrate encoding. Higher values mean less compression. You can also set a custom value between 40 kbps

COMPRESSION OPTION	DESCRIPTION	DEFAULT VALUE	REMARKS
			and 80,000 kbps by editing the Registry at HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent\SRGraphicsX264Bitrate.
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**. You can also set the image resolution scaling by editing the Registry at HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent\SRGraphicsZoomFactor.

COMPRESSION OPTION	DESCRIPTION	DEFAULT VALUE	REMARKS
Cursor refresh rate (times per second)	**Low**: 3; **Medium**: 5; **High**: 10	**Low**	N/A

Enable fast seeking

Fast seeking allows to accelerate navigating ICA® screen recordings during playback. It significantly improves the playback seeking experience.

> **Note:**
>
> Fast seeking is valid only for the sessions that are recorded after the feature is enabled in **Session Recording Agent Properties**.

Enable fast seeking

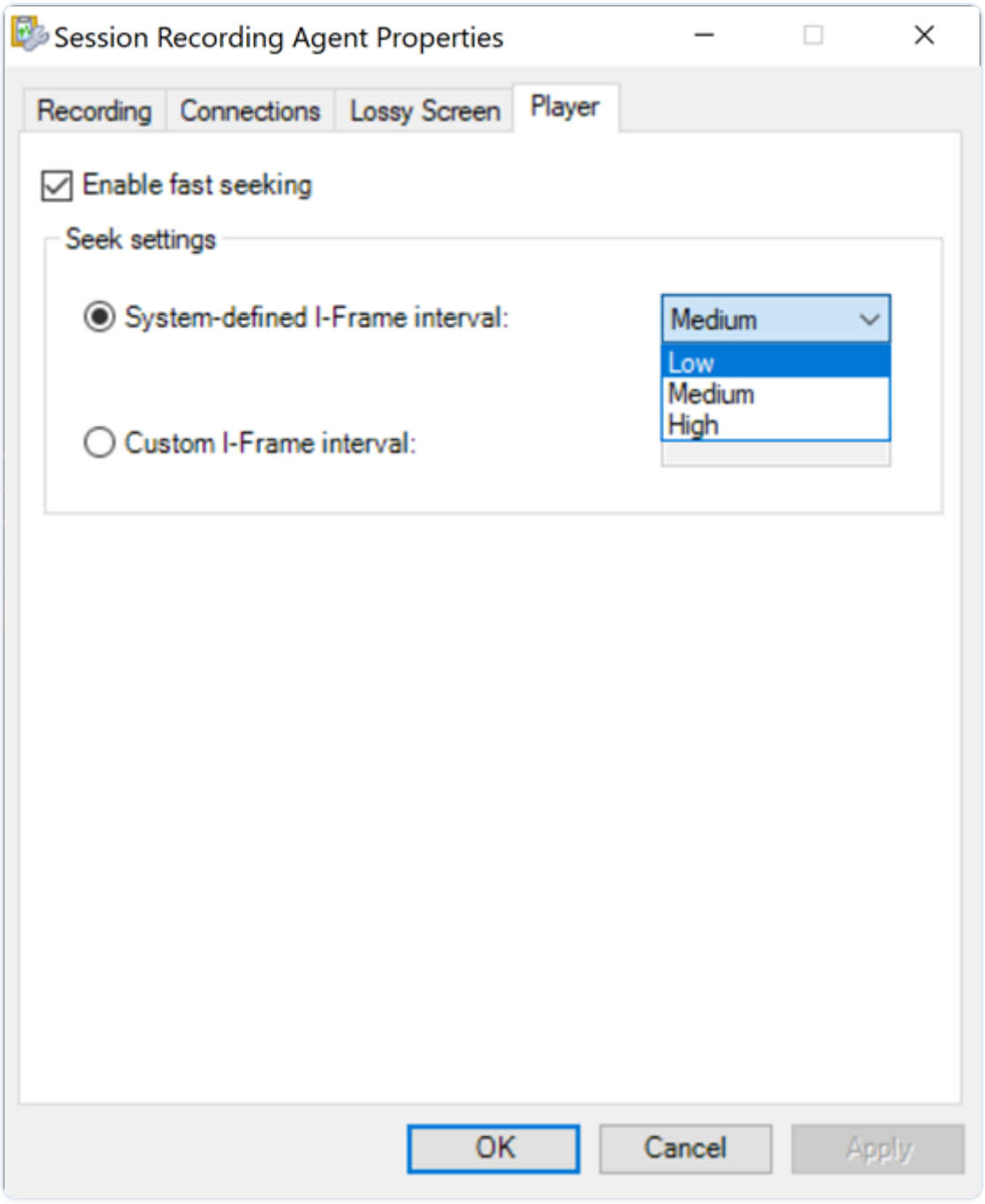
To enable fast seeking, complete the following steps:

1. Open the **Player** tab of **Session Recording Agent Properties**.
2. Select **Enable fast seeking** and configure how often an I-Frame is generated.

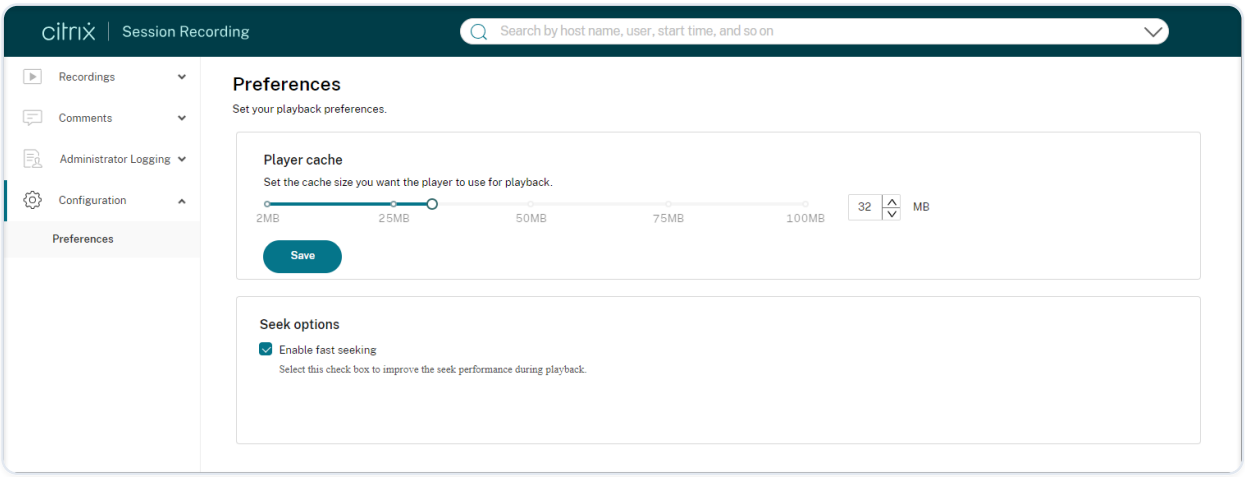
   You can select a system-defined I-Frame interval or configure a custom I-Frame (in seconds, ranging from 10 to 1,800 seconds). By default, the system-defined I-Frame interval **Medium** (60 seconds) is selected.

   For a description of the system-defined I-Frame intervals, see the following table:

SYSTEM-DEFINED I-FRAME INTERVAL	DESCRIPTION
Low	300 seconds
Medium	60 seconds
High	30 seconds



3. (Optional) If you also want to enable fast seeking for the Session Recording web player, navigate to **Configuration > Preferences** on the web player page and ensure that **Enable fast seeking** is selected.



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.

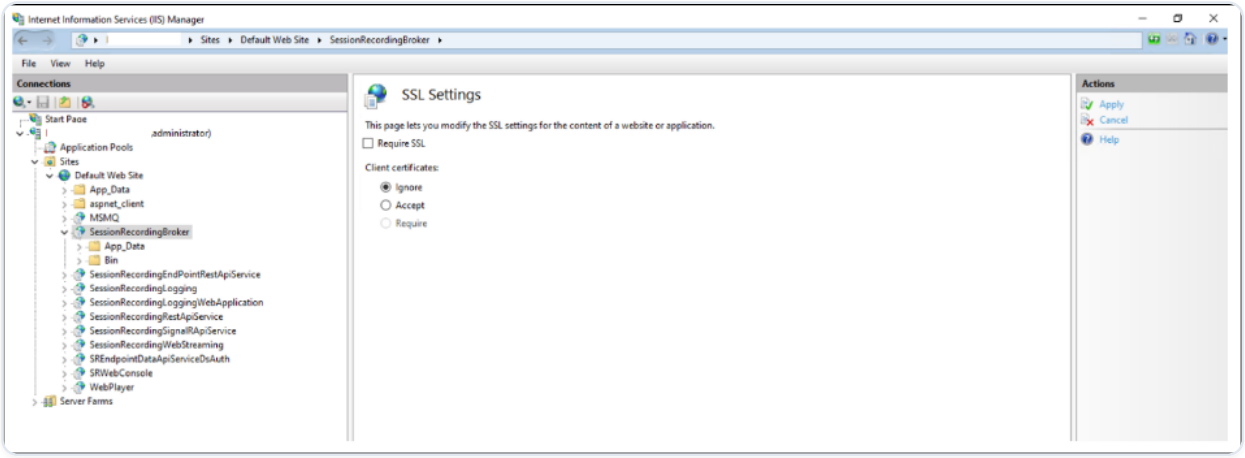
6. In the **Message life** field, accept the default 7,200 seconds (two hours) or type a new value for the number of seconds each message is retained in the queue if there is a communication failure. After this time elapses, the message is deleted and the file is playable until the point where the data 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. In IIS, navigate to Default Web Site, open each application, go to SSL Settings, and uncheck Require SSL.



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 the dual message queue

The dual message queue feature allows the Session Recording Server to use a second MSMQ queue for processing data streams from VDAs. Enabling this feature can improve performance and

scalability on multi-core Session Recording Servers, especially in environments with high recording traffic.

Enable the dual message queue

By default, this feature is disabled. To enable the dual message queue, complete the following steps:

1. Log on to the VDA where the Session Recording Agent is installed.
2. Open the Registry Editor.
3. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent`.
4. Create a DWORD value named `MsmqDataQueueCount` and set its value data to **2**.
5. Restart the Citrix Session Recording Agent service to make your changes take effect.

Disable the dual message queue

To disable the feature, either set the `MsmqDataQueueCount` value data to **1** or delete the registry value. A restart of the Citrix Session Recording Agent service is required for the change to take effect.

> **Note:**
>
> To use this feature, your Session Recording Server and Agent components must be version 2507 or later. Ensure you apply the registry change on all relevant VDAs for consistent performance enhancement.

Configure settings on the Session Recording server

This section guides you through the following settings:

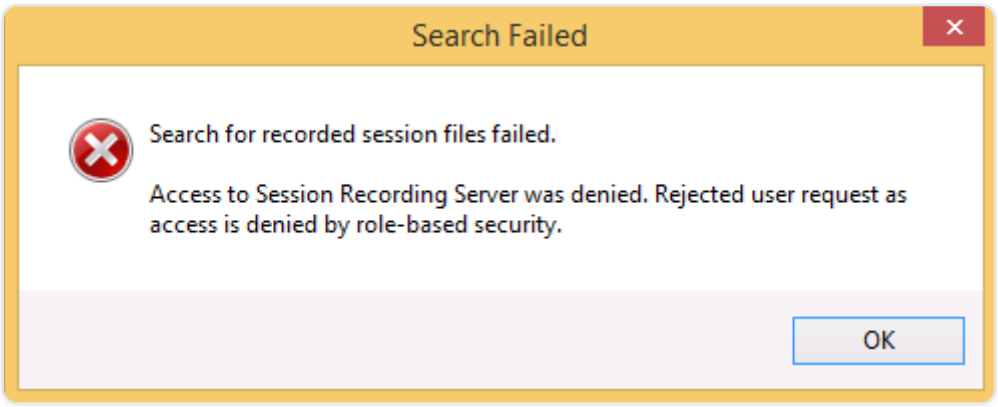
- Authorize users
- Customize recording notification messages
- Specify where recordings are stored
- Specify file size for recordings
- Enable or disable digital signing
- CEIP and Google Analytics

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.

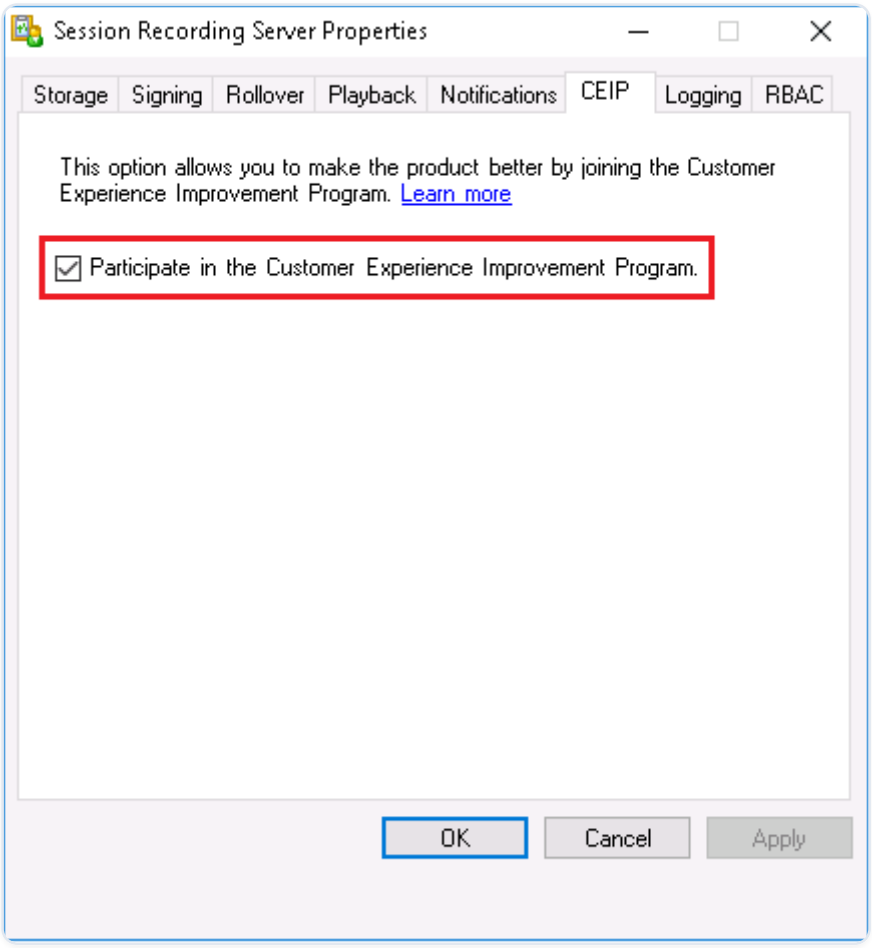
CEIP and Google Analytics

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.

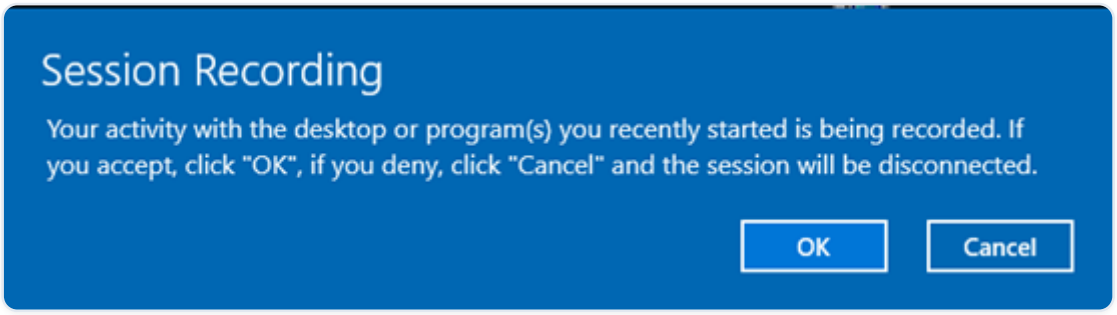
DATA POINT	KEY NAME	DESCRIPTION
		With Google Analytics enabled, heartbeat data is sent to Google Analytics regardless of whether CEIP is enabled.
Number of application recordings	`application-recording-number`	Integer denoting the number of application recording files. The data is sent when both Google 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 recording notification messages

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

- When **Allow end user to deny recording of their session** is enabled on the **Notifications** tab of the **Session Recording Server Properties**, the default notification message reads as follows:

  Allow end user to deny recording of their session. This feature forces end users to explicitly consent to the session recording disclaimer before they can continue with their session. If end users accept the disclaimer, their session continues with session recording enabled. If end users deny the disclaimer, their session is terminated.

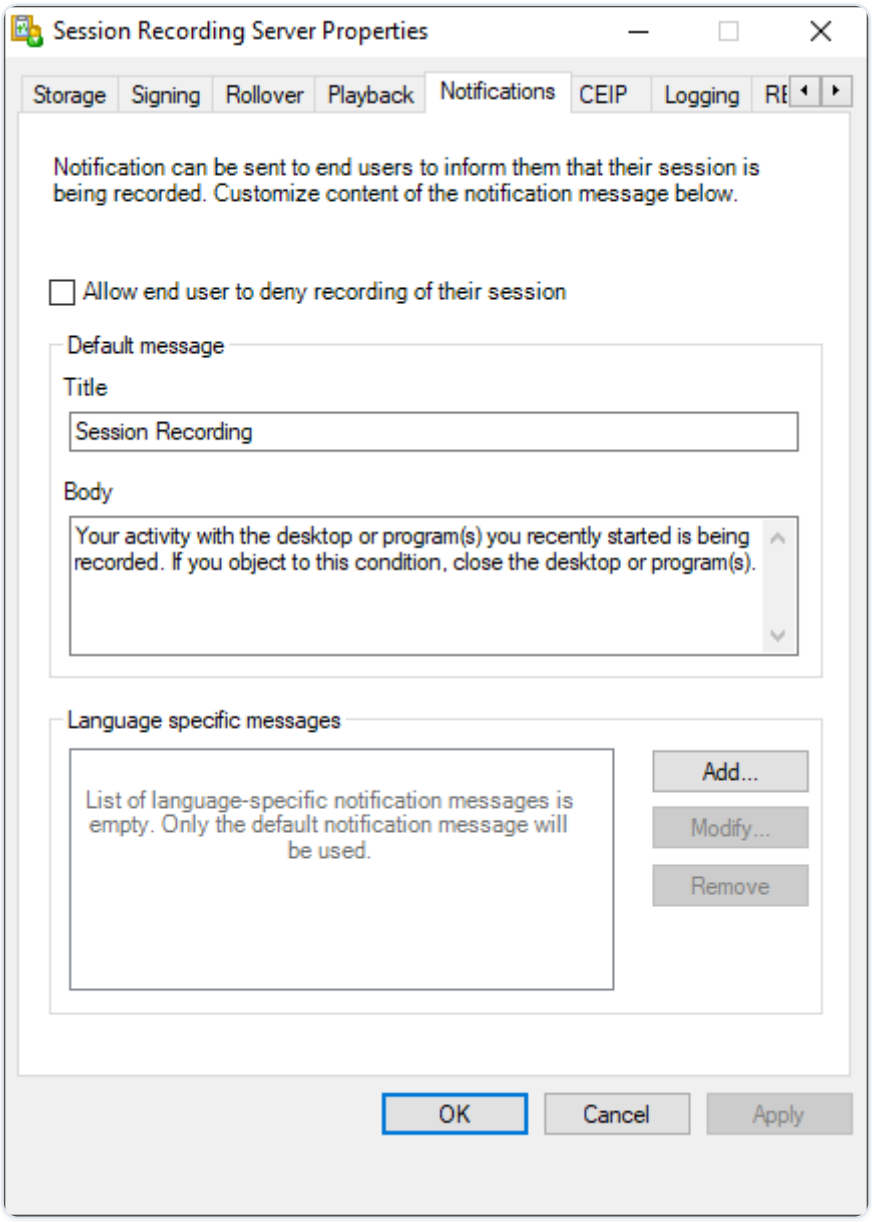
- When **Allow end user to deny recording of their session** is not enabled, the default notification message is **Your activity with the desktop or program(s) you recently started is being recorded. If you object to this condition, close the desktop or program(s)**. Users can click **OK** to dismiss the window and continue their sessions.

The default notification message appears in the language of the operating system on the VDA. You can change the default message title and message body as needed.

You can also create notification messages in specific languages that you choose. While doing so, you can customize the message title and message body too. You can have only one notification message for each language. Your users see notification messages in the languages of their preferred local settings. The language-specific notification messages take precedence over the default notification message.

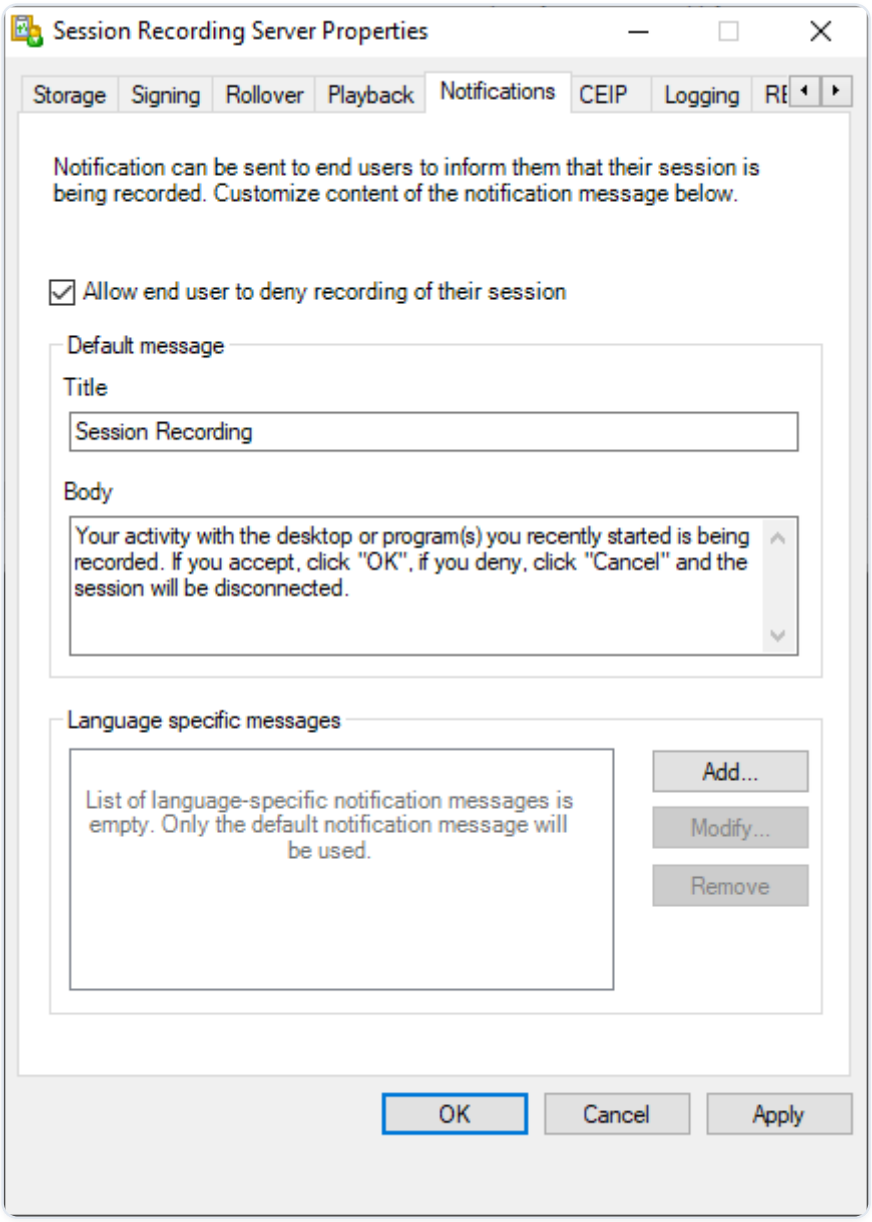
Customize recording notification messages

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.

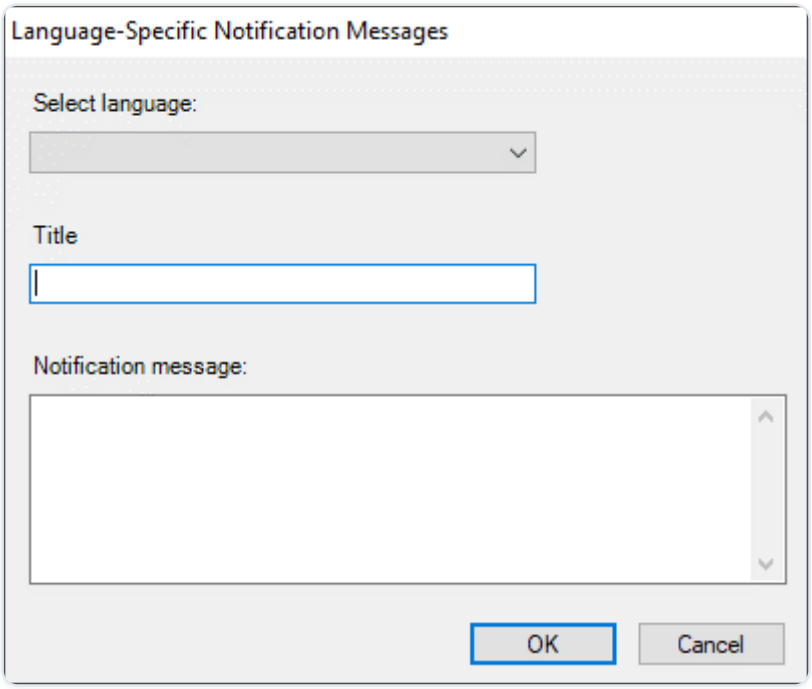


4. To enable explicit user consent before recording sessions, select **Allow end user to deny recording of their session**.

   After you select **Allow end user to deny recording of their session**, the default message body changes accordingly:



5. If you want to use the default notification message, change the default message title and message body as needed and then click **OK** to complete the settings. If you want to use a language-specific notification message, proceed to the following steps.
6. Click **Add** in the **Language specific messages** section.
7. Choose the language for the message and type the message title and message body. 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**.

Event response reports

Overview

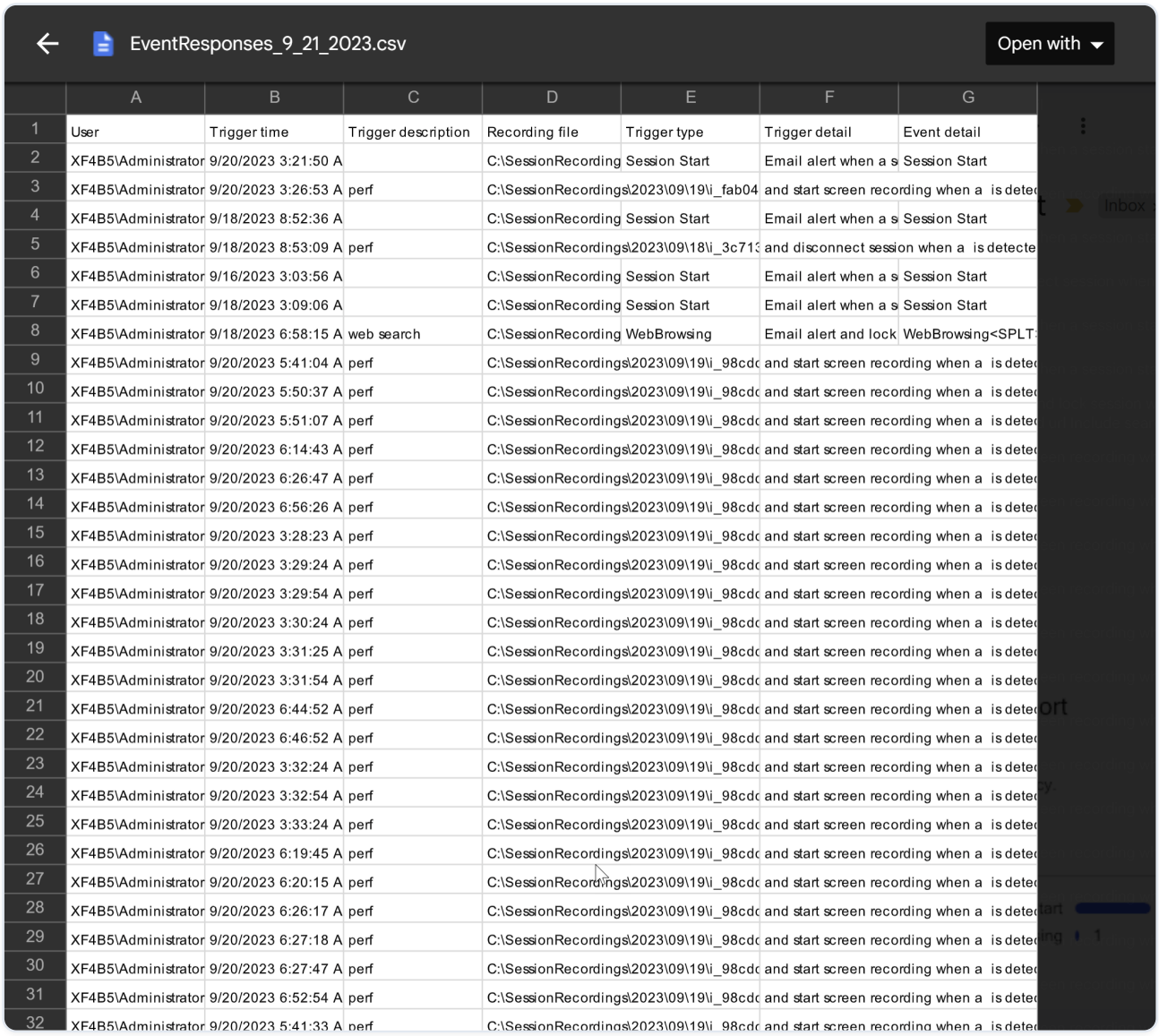
You can receive emailed event response reports on a daily or weekly basis. An event response report contains a digest chart as the email body and a csv file as the attachment. The csv file includes a full list of the events during the day or week that have triggered various event responses.

> **Note:**
>
> By selecting email notifications as the event response in your custom event response policy, you can still be notified about each **individual** occurrence. You can choose regular event response reports, individual notifications, or both.

> The following are example digest charts contained in a weekly and a daily event response report:

WEEKLY	DAILY
	

See the screen capture below for an example csv file that can be linked to an event response report:



EventResponses_9_21_2023.csv

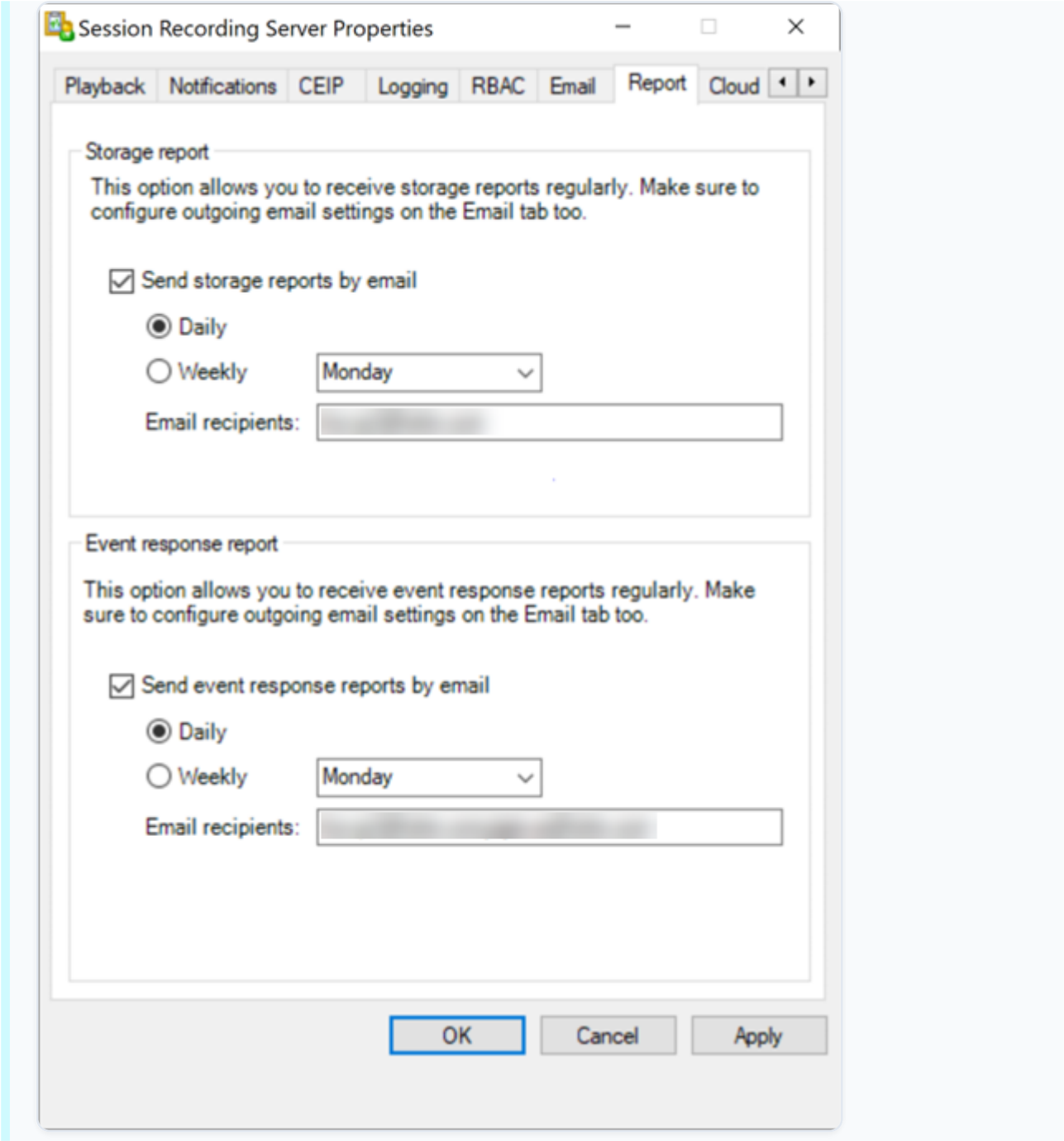
Open with

	A	B	C	D	E	F	G
1	User	Trigger time	Trigger description	Recording file	Trigger type	Trigger detail	Event detail
2	XF4B5\Administrator	9/20/2023 3:21:50 A		C:\SessionRecording	Session Start	Email alert when a s	Session Start
3	XF4B5\Administrator	9/20/2023 3:26:53 A	perf	C:\SessionRecordings\2023\09\19\i_fab04		and start screen recording when a	is detec
4	XF4B5\Administrator	9/18/2023 8:52:36 A		C:\SessionRecording	Session Start	Email alert when a s	Session Start
5	XF4B5\Administrator	9/18/2023 8:53:09 A	perf	C:\SessionRecordings\2023\09\18\i_3c71		and disconnect session when a	is detecte
6	XF4B5\Administrator	9/16/2023 3:03:56 A		C:\SessionRecording	Session Start	Email alert when a s	Session Start
7	XF4B5\Administrator	9/18/2023 3:09:06 A		C:\SessionRecording	Session Start	Email alert when a s	Session Start
8	XF4B5\Administrator	9/18/2023 6:58:15 A	web search	C:\SessionRecording	WebBrowsing	Email alert and lock	WebBrowsing<SPLT
9	XF4B5\Administrator	9/20/2023 5:41:04 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
10	XF4B5\Administrator	9/20/2023 5:50:37 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
11	XF4B5\Administrator	9/20/2023 5:51:07 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
12	XF4B5\Administrator	9/20/2023 6:14:43 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
13	XF4B5\Administrator	9/20/2023 6:26:47 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
14	XF4B5\Administrator	9/20/2023 6:56:26 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
15	XF4B5\Administrator	9/20/2023 3:28:23 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
16	XF4B5\Administrator	9/20/2023 3:29:24 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
17	XF4B5\Administrator	9/20/2023 3:29:54 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
18	XF4B5\Administrator	9/20/2023 3:30:24 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
19	XF4B5\Administrator	9/20/2023 3:31:25 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
20	XF4B5\Administrator	9/20/2023 3:31:54 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
21	XF4B5\Administrator	9/20/2023 6:44:52 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
22	XF4B5\Administrator	9/20/2023 6:46:52 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
23	XF4B5\Administrator	9/20/2023 3:32:24 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
24	XF4B5\Administrator	9/20/2023 3:32:54 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
25	XF4B5\Administrator	9/20/2023 3:33:24 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
26	XF4B5\Administrator	9/20/2023 6:19:45 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
27	XF4B5\Administrator	9/20/2023 6:20:15 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
28	XF4B5\Administrator	9/20/2023 6:26:17 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
29	XF4B5\Administrator	9/20/2023 6:27:18 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
30	XF4B5\Administrator	9/20/2023 6:27:47 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
31	XF4B5\Administrator	9/20/2023 6:52:54 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec
32	XF4B5\Administrator	9/20/2023 5:41:33 A	perf	C:\SessionRecordings\2023\09\19\i_98cdc		and start screen recording when a	is detec

Configuration

To receive emailed event response 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.



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:

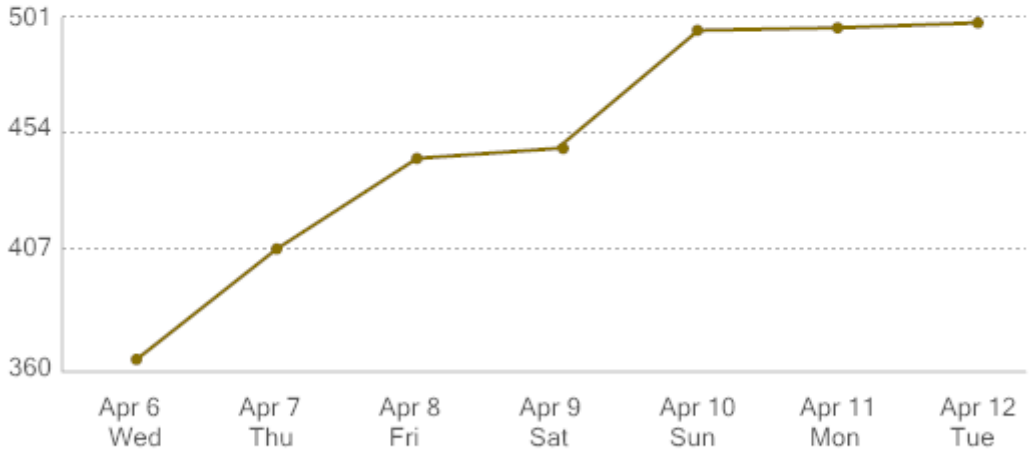
SERVER

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

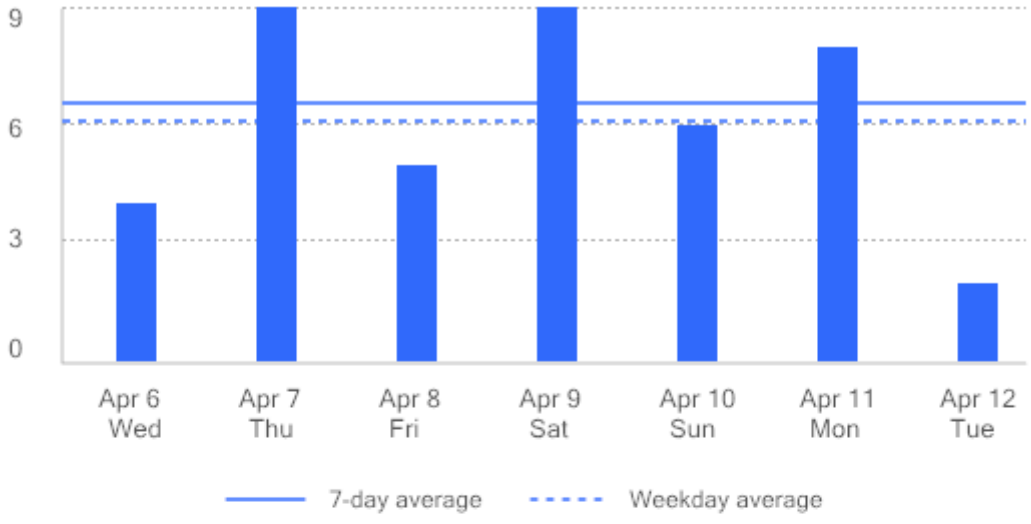
Total size of all recordings: 499.0 GB ▲ 4% over previous week

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

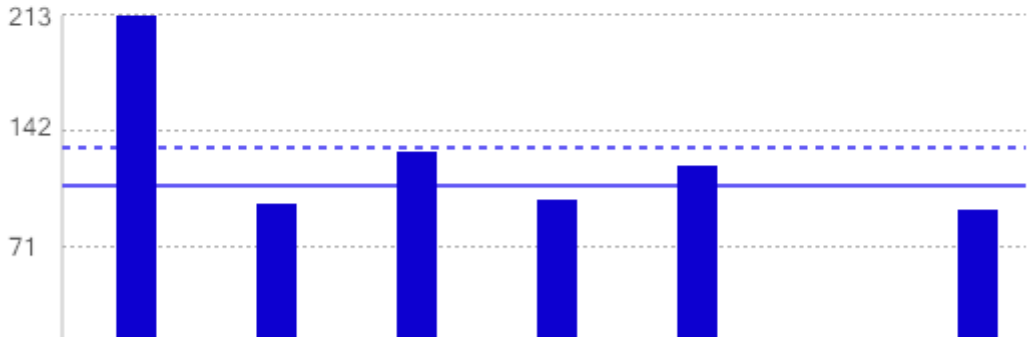
Total size of all recordings (GB)



Storage usage per day (GB)



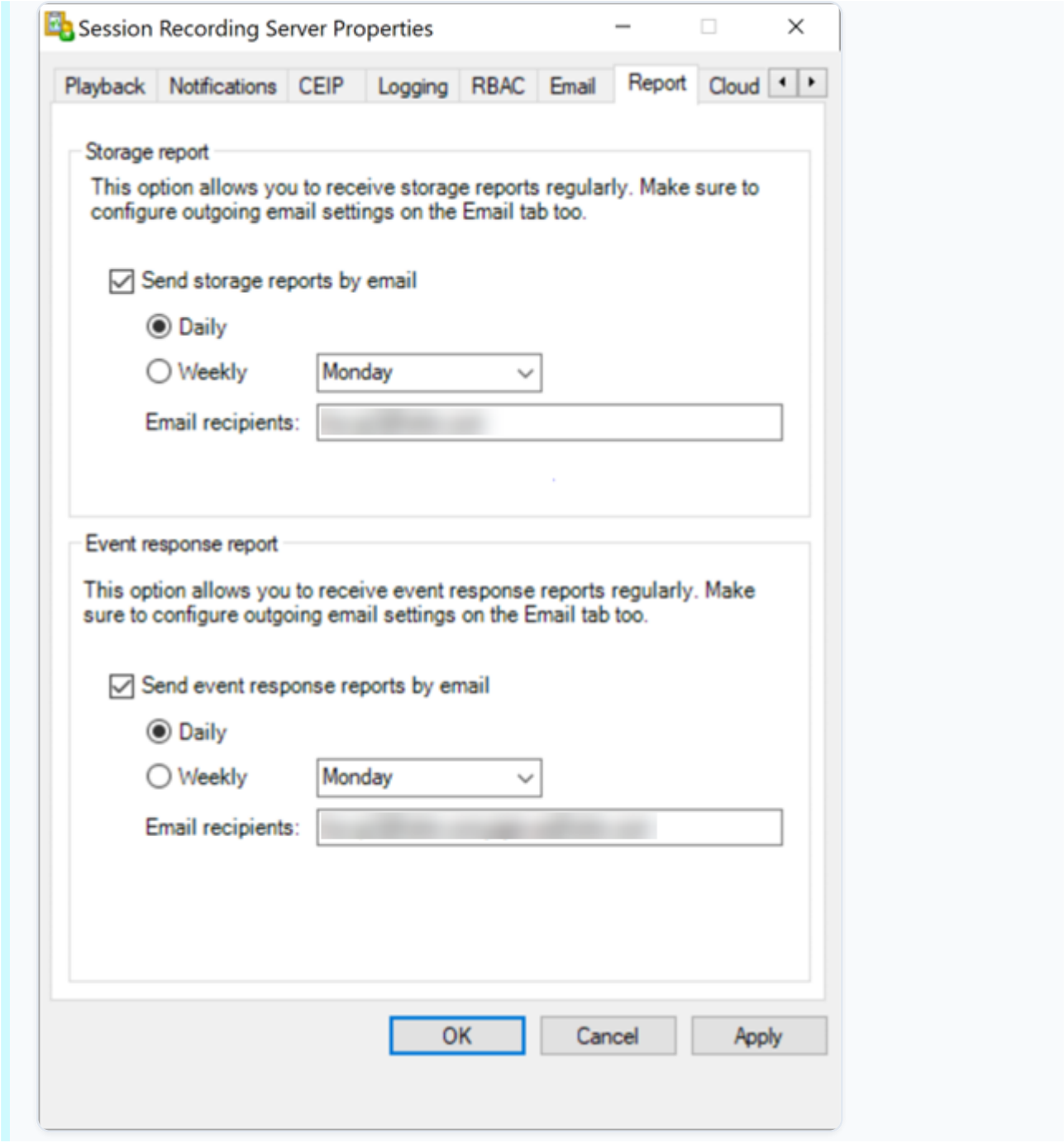
Number of sessions recorded per day



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.

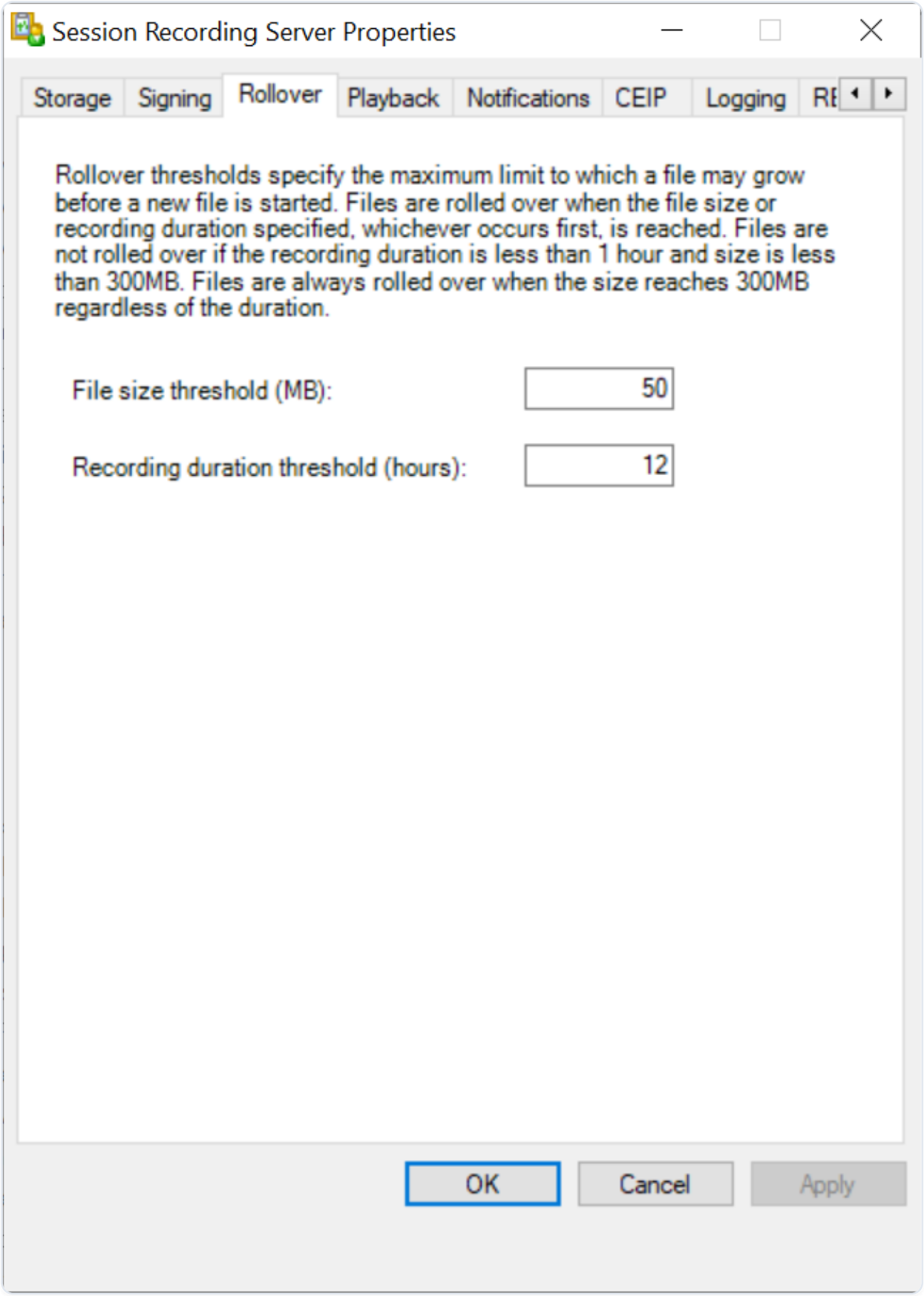
- **Duration.** When the duration is reached, the current file closes and a new file opens. By default, the rollover occurs when the session records for 12 hours. Supported values: 1-24.

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 recording storage locations

You can store recordings on a local drive, a SAN volume, and a location specified by a UNC network path. You can also store recordings in Azure file shares and Amazon Simple Storage Service (Amazon S3).

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 to avoid security implications and perform scale testing to ensure proper performance.
- To archive files or restore deleted files, use the ICLDB command.

This article walks you through the following procedures:

- Specify recording storage locations in Session Recording Server Properties
- Store recordings in an Azure file share
- Store recordings in Amazon S3
- Store recordings in a network shared folder

Specify recording storage locations in Session Recording Server Properties

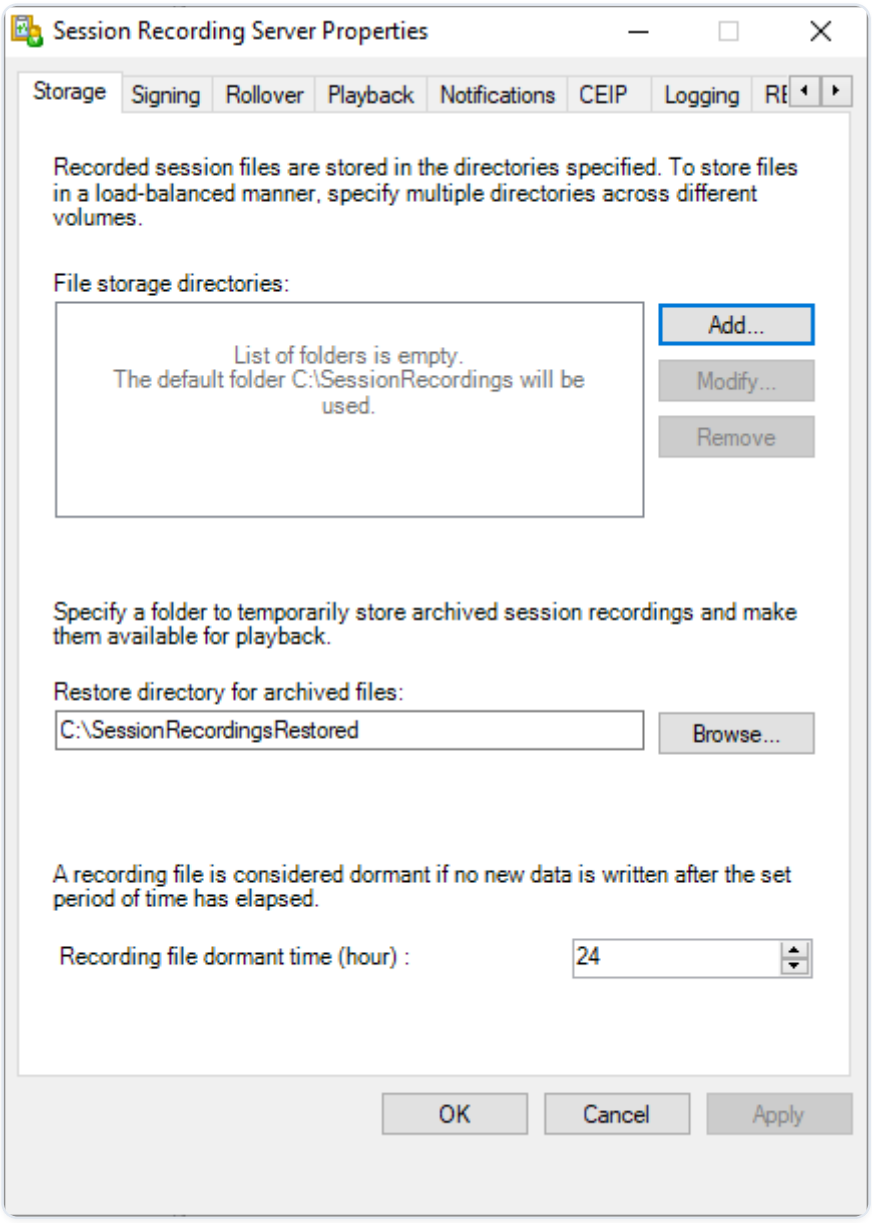
This section provides a general procedure for setting storage locations in Session Recording Server Properties.

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, specify a folder for restoring archived recordings. You can specify only one 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.

Store recordings in an Azure file share

To store recordings in an Azure file share, 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`.

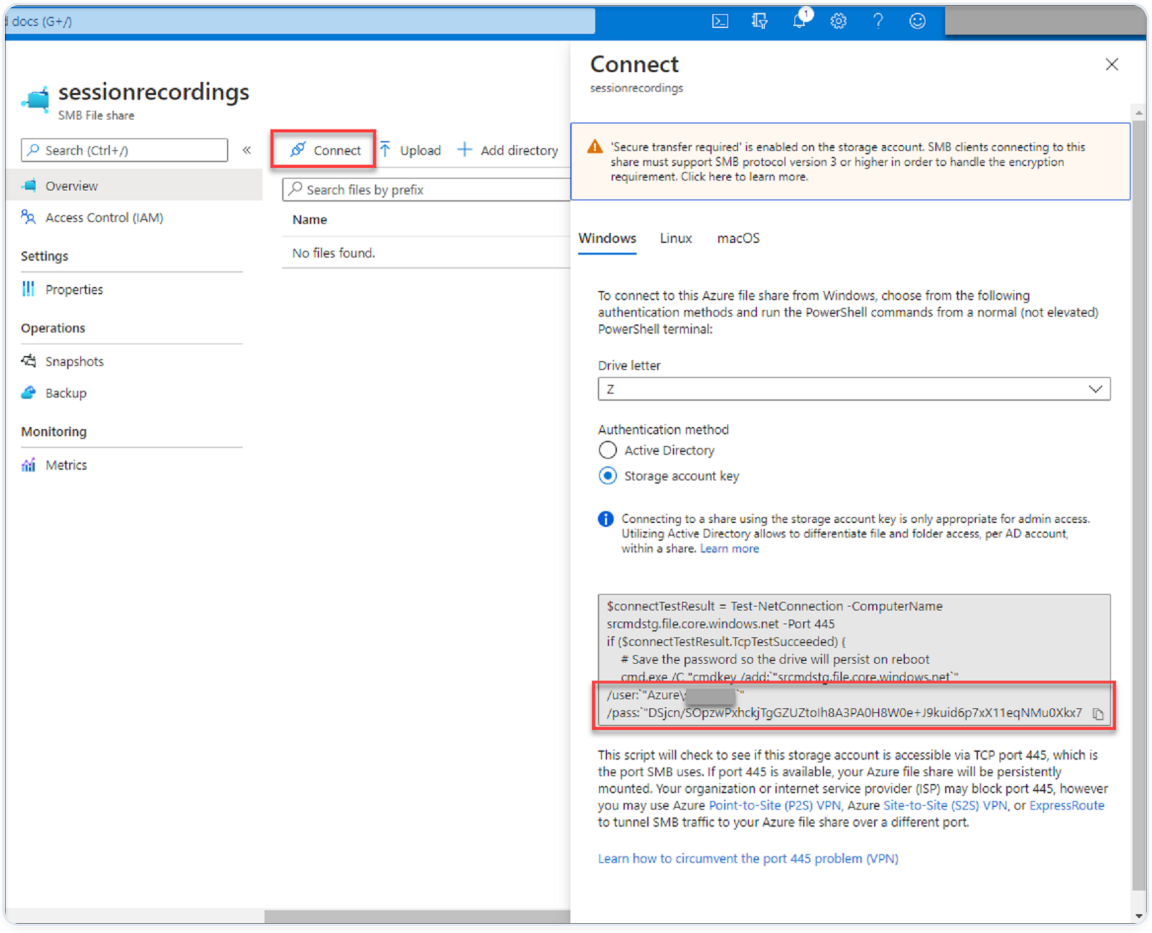
b. Run the **SsRecUtils.exe -AddAzureFiles <storageAccountName\> <fileShareName\> <accesskey\>** command.

Where,

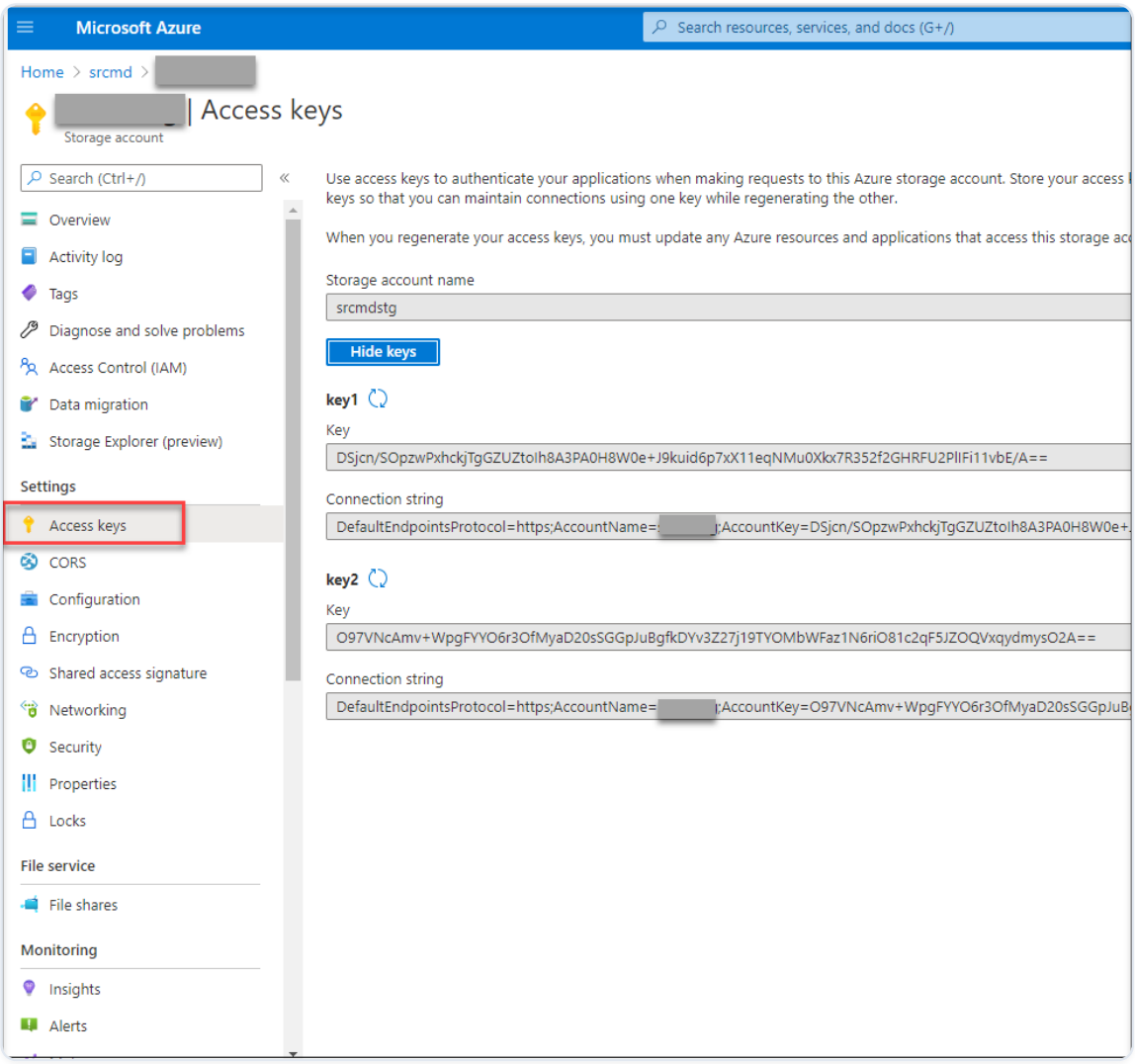
- **<storageaccountname\>** is the name of your storage account in Azure.
- **<filessharename\>** is the name of the file share contained within your storage account.
- **<accesskey\>** is your storage account key that can be used to access the file share.

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.



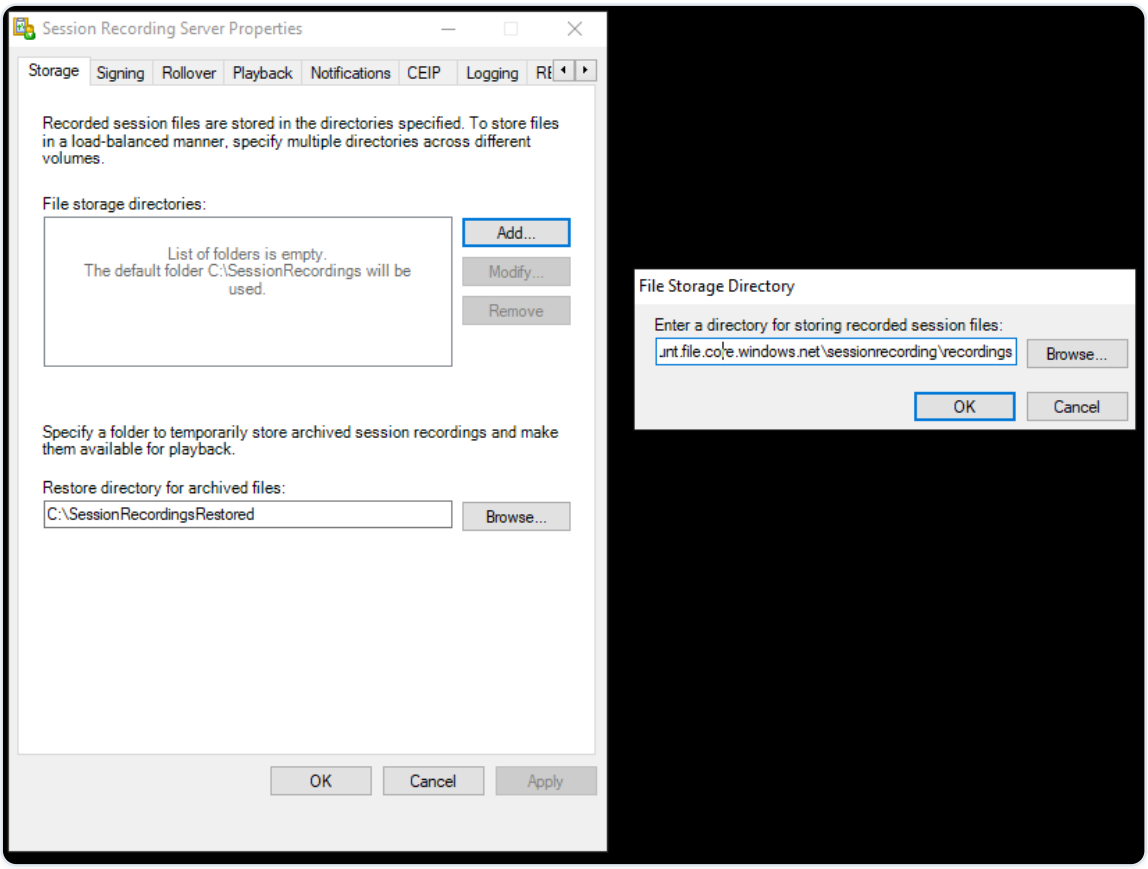
c. Mount the Azure file share to the host where you installed the Session Recording server.

   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.

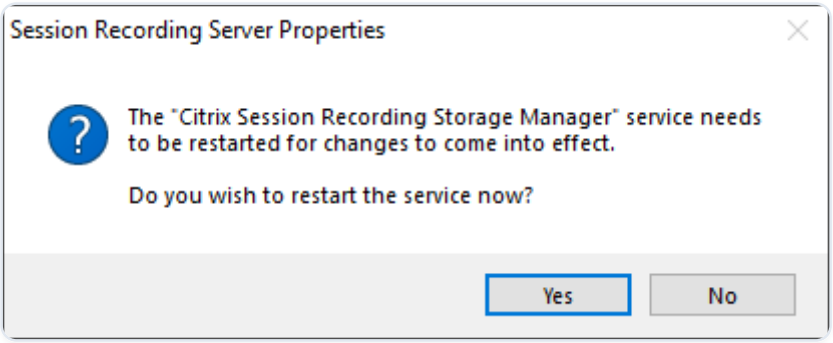


iv. Click **OK** in the **File Storage Directory** dialog box.

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

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

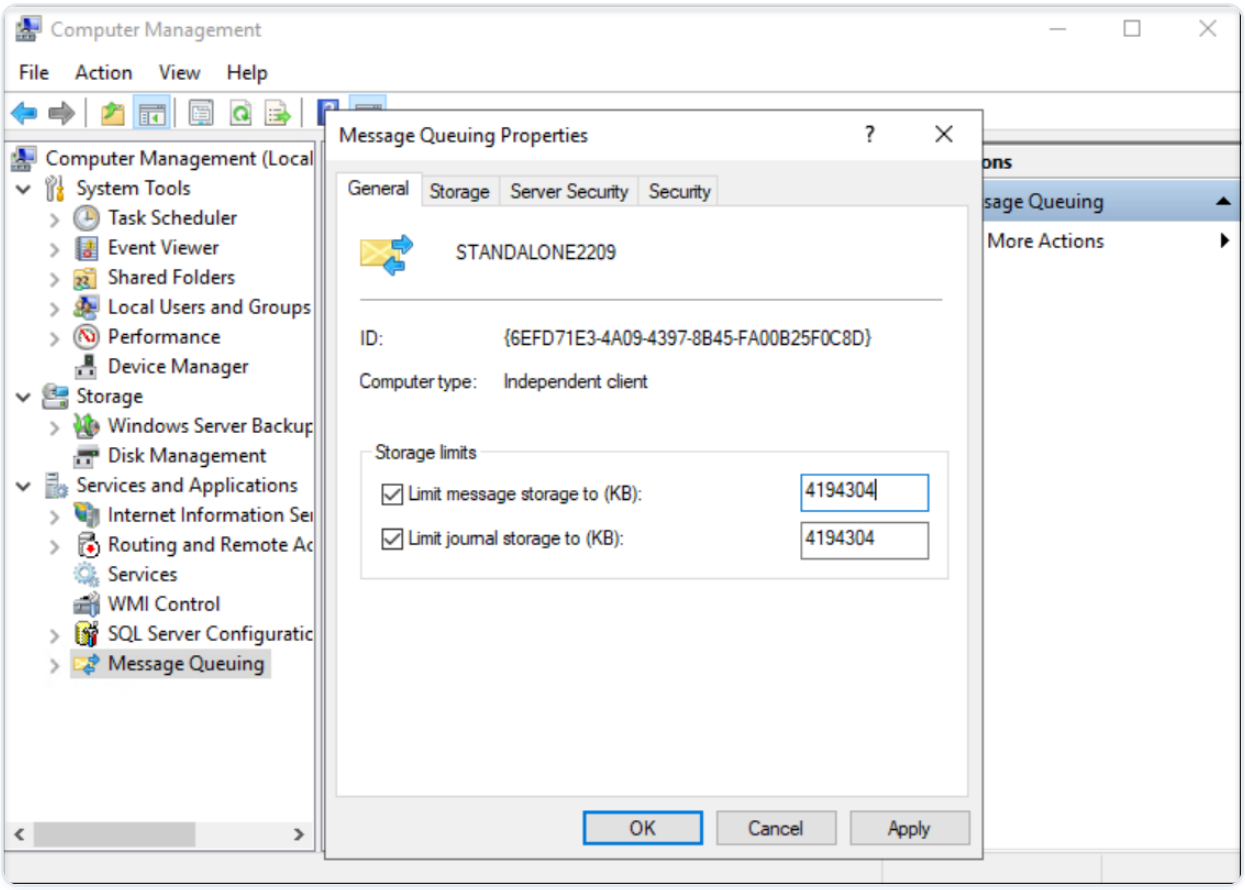
vii. Click **Yes** when you're prompted to restart the Session Recording Storage Manager service.



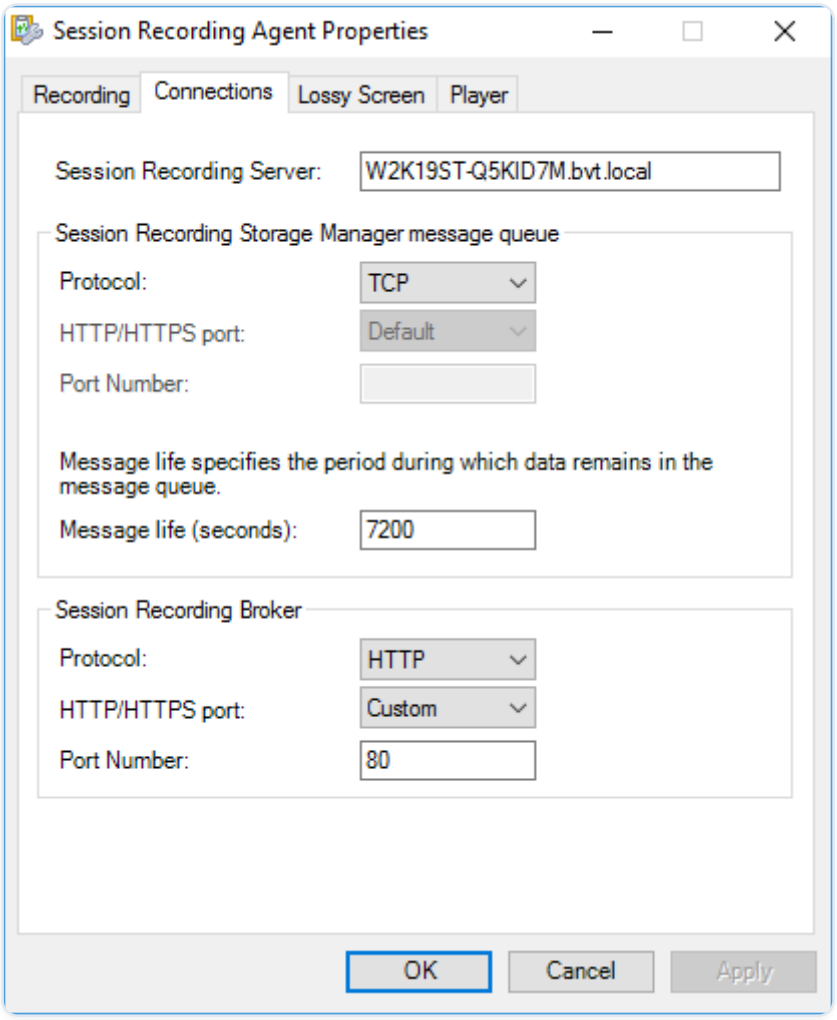
Store recordings in Amazon S3

Recommendations

1. Install the Session Recording server on t2.xlarge or other AWS EC2 instances with higher specifications.
2. Set the storage limit on Message Queues to a minimum of 4,194,304 KB (4 GB).



3. In Session Recording Agent Properties, set the lifetime of the messages on Message Queues to 14,400 seconds (4 hours).



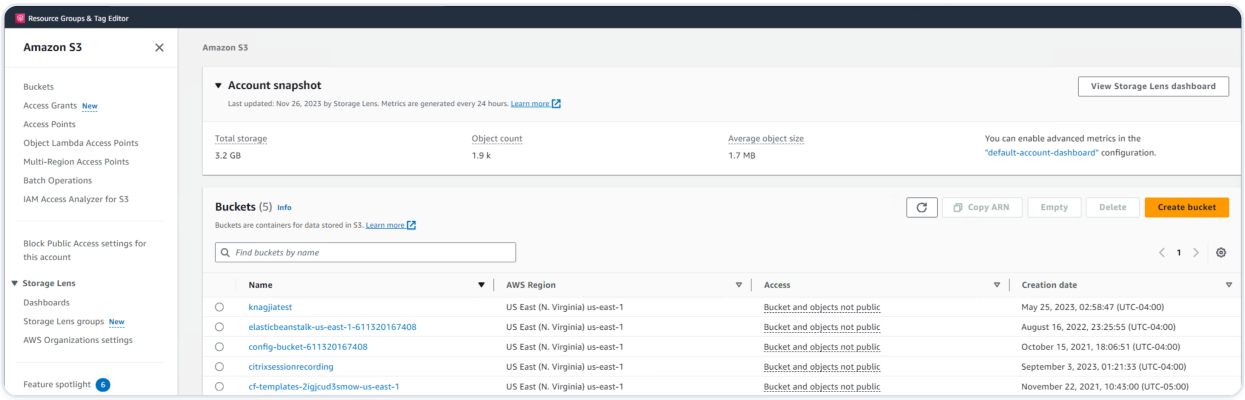
Note:

During the update or maintenance of the AWS Storage Gateway, recording files might not be saved from the Session Recording server to the file share. Data losses can occur.

Steps

To store recordings in Amazon S3, complete the following steps:

1. Create an Amazon S3 bucket. For more information, see the Amazon documentation Creating a bucket.



2. Create and activate an Amazon S3 File Gateway. Doing so enables data transfer to and from the Amazon S3 bucket created earlier.

   For step-by-step instructions, see the following Amazon documentation:

   - Create and activate an Amazon S3 File Gateway
   - Getting an activation key for your gateway

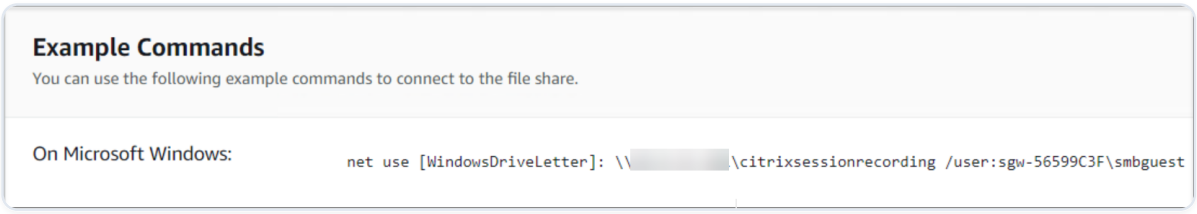
3. Create a file share with guest access. When creating the file share, select the Amazon S3 File Gateway that you created earlier and connect the file share to your Amazon S3 bucket. For more information, see the Amazon documentation Create a file share.
4. Go to the machine where you installed the Session Recording server and complete the following steps:

   a. Add the file share credentials to the Session Recording server. To do so, 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. Then run the **SsRecUtils.exe -AddAwsS3 <GatewayIPAddress\> <S3Path\> <GatewayID\> <Password\>** command.

      Where,

      - **<GatewayIPAddress\>** is the IP address of your Amazon S3 File Gateway.
      - **<S3Path\>** is the name of your Amazon S3 bucket.
      - **<GatewayID\>** is the ID of your Amazon S3 File Gateway.
      - **<Password\>** is the guest password that you set when creating the file share.

      All the information except for the guest password is available on the file share page similar to the following. As for the guest password, you must keep a careful record yourself.



b. Set the file share as the location for storing your recordings.

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

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

   iii. Enter the UNC path in the format of **\\\\<GatewayIPAddress\>\\<S3Path\>\\<subfolder\>**. Specify a subfolder under the file share to store your recording files. The Session Recording server then automatically creates the subfolder for you.

Store recordings in a network shared folder

> **Note:**
>
> - For an accessible network shared folder, the Session Recording server accesses it through SMB by default.
> - 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 to avoid security implications and perform scale testing to ensure proper performance.

Steps

To store recordings in a network shared folder, complete the following steps:

1. Create an account with read and write permissions for the network shared folder to be created later. To do so, use the Windows GUI or run a PowerShell command similar to the following:

   ```
   New-LocalUser -Name "YourUserName" -Password (ConvertTo-SecureString
   -String "YourPassword" -AsPlainText -Force)
   ```

2. Create a network shared folder and ensure that the shared folder is accessible to the Session Recording Server. To do so, use the Windows GUI or run the PowerShell commands similar to the following:

```
New-SmbShare -Name "YourShareName" -Path "YourSharePath" -FullAccess
"YourUserName"



Grant-SmbShareAccess -Name "YourShareName" -AccessRight Change
-AccountName "YourUserName"
```

3. Go to the machine where you installed the Session Recording server and complete the following steps:

   a. Add the credentials for the created account to the Session Recording server. To do so, 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. Then run the **SsRecUtils.exe -AddSharedFolder <IPAddress\> <ShareName\> <Protocol\> <Username\> <Password\>** command.

      Where,

      - **<IPAddress\>** is the IP address of the machine where the shared folder resides.
      - **<ShareName\>** is the share name.
      - **<Protocol\>** is fixed to SMB.
      - **<Username\>** is the user name that you set for the shared folder.
      - **<Password\>** is the password that you set for the shared folder.

      For example, if **\\\10.100.100.100\myshare** is your shared folder, you can run a command similar to **SsRecUtils -AddSharedFolder 10.100.100.100 myshare SMB myusername mypassword**.

   b. Set the shared folder as the location for storing your recordings.

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

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

      iii. Enter the UNC path in the format of **\\\\<IPAddress\>\\<ShareName\>\\<subfolder\>**. Specify a subfolder under the shared folder to store your recording files. The Session Recording server then automatically creates the subfolder for you.

Policies (policy console)

Note:

You can also configure policies in the Session Recording web console. For more information, see Policies (web console).

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.

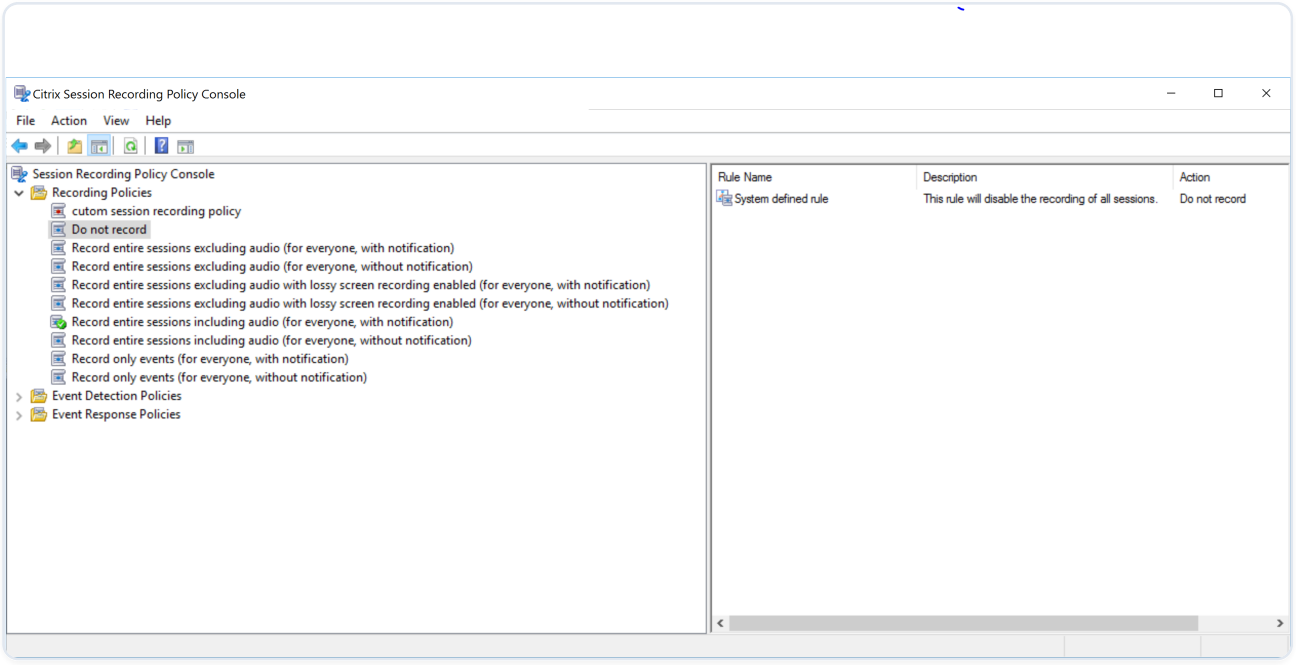
Configure session recording policies

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 entire sessions excluding audio (for everyone, with notification)**. This policy records entire sessions (including screens and events but excluding audio). Users receive recording notifications in advance.

- **Record entire sessions excluding audio (for everyone, without notification)**. This policy records entire sessions (including screens and events but excluding audio). Users do not receive recording notifications.
- **Record entire sessions excluding audio with lossy screen recording enabled (for everyone, with notification)**. This policy records entire sessions (including screens and events but excluding audio). Lossy screen recording is enabled to reduce the size of recording files. Users receive recording notifications in advance.
- **Record entire sessions excluding audio with lossy screen recording enabled (for everyone, without notification)**. This policy records entire sessions (including screens and events but excluding audio). Lossy screen recording is enabled to reduce the size of recording files. Users do not receive recording notifications.
- **Record entire sessions including audio (for everyone, with notification)**. This policy records entire sessions (including screens, events, and audio). Users receive recording notifications in advance. You can now enable audio recording for non-optimized HDX audio. The audio that is handled on the VDA and delivered to/from the client where the Citrix Workspace app is installed is referred to as non-optimized HDX audio. Unlike non-optimized HDX audio, optimized HDX audio has its processing offloaded to the client, as seen in the Browser Content Redirection (BCR) and Optimization for Microsoft Teams scenarios.
- **Record entire sessions including audio (for everyone, without notification)**. This policy records entire sessions (including screens, events, and audio). Users do not receive recording notifications.
- **Record only events (for everyone, with notification)**. This policy records only events that your event detection policy specifies. It does not record screens or audio. Users receive recording notifications in advance.
- **Record only events (for everyone, without notification)**. This policy records only events that your event detection policy specifies. It does not record screens or audio. Users do not receive recording notifications.

Note:

When upgrading Citrix Session Recording from version 1912 , existing policy names are retained (e.g., Record everyone with notification, Record everyone without notification).

However, fresh installations use updated policy names.

> This is expected behavior and does not affect policy functionality.

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

Create a custom recording policy

Considerations

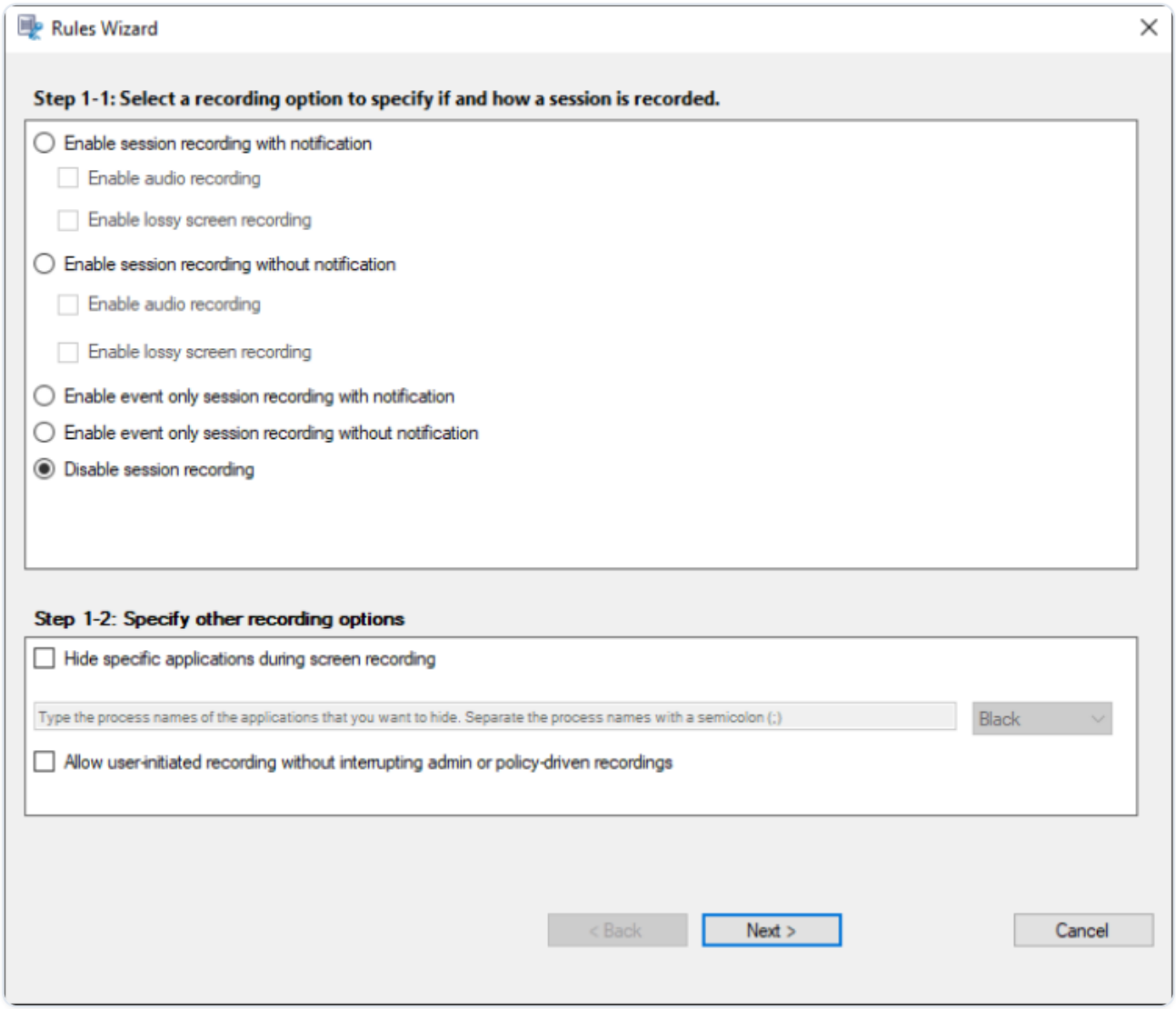
You can record sessions of specific users or groups, published applications or desktops, delivery groups or VDA machines, and Citrix Workspace™ app client IP addresses. To obtain the lists of published applications or desktops and delivery groups or VDA machines, you must have the **read** permission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

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

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

A wizard within the Session Recording policy console helps you create rules. 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:

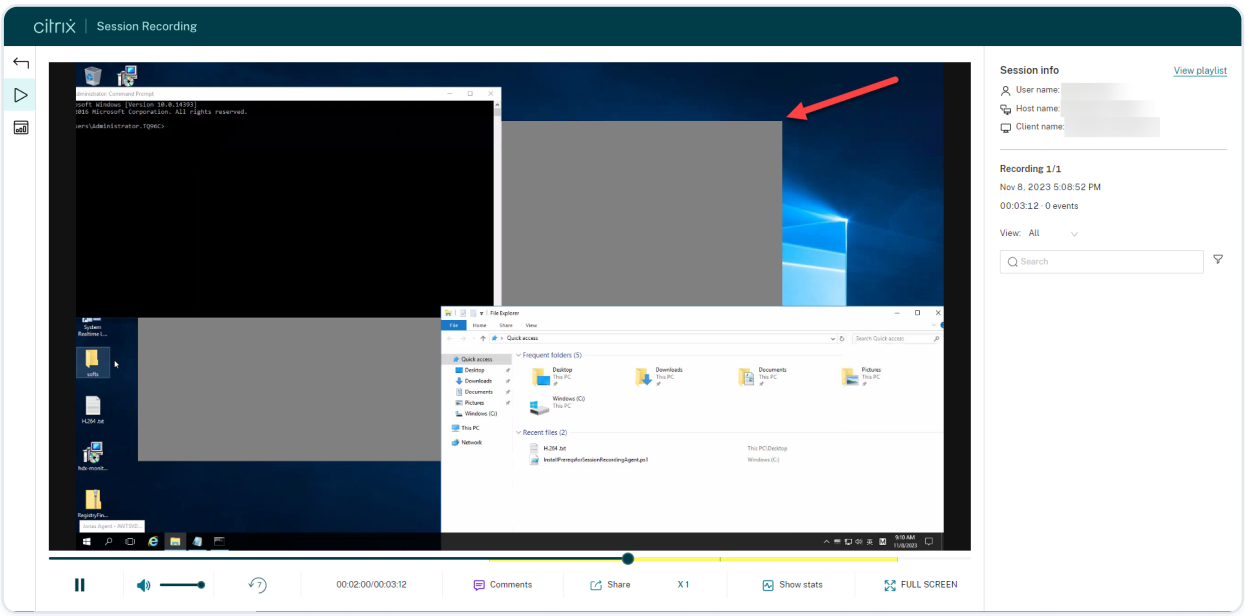


- **Enable session recording with notification**. This option records entire sessions (screens and events). Users receive recording notifications in advance. With this option selected, you can further select to enable audio recording or lossy screen recording. Additionally, you can choose to hide specific applications in screen recordings.
- **Enable session recording without notification**. This option records entire sessions (screens and events). Users do not receive recording notifications. With this option selected, you can further select to enable audio recording or lossy screen recording. Additionally, you can choose to hide specific applications in screen recordings.
- **Enable event only session recording with notification**. Recording only specific events helps to free up storage space. This option records throughout sessions only events that your event detection policy specifies. It does not record screens. Users receive recording notifications in advance.
- **Enable event only session recording without notification**. Recording only specific events helps to free up storage space. This option records throughout sessions only events that your

event detection policy specifies. It does not record screens. Users do not receive recording notifications.

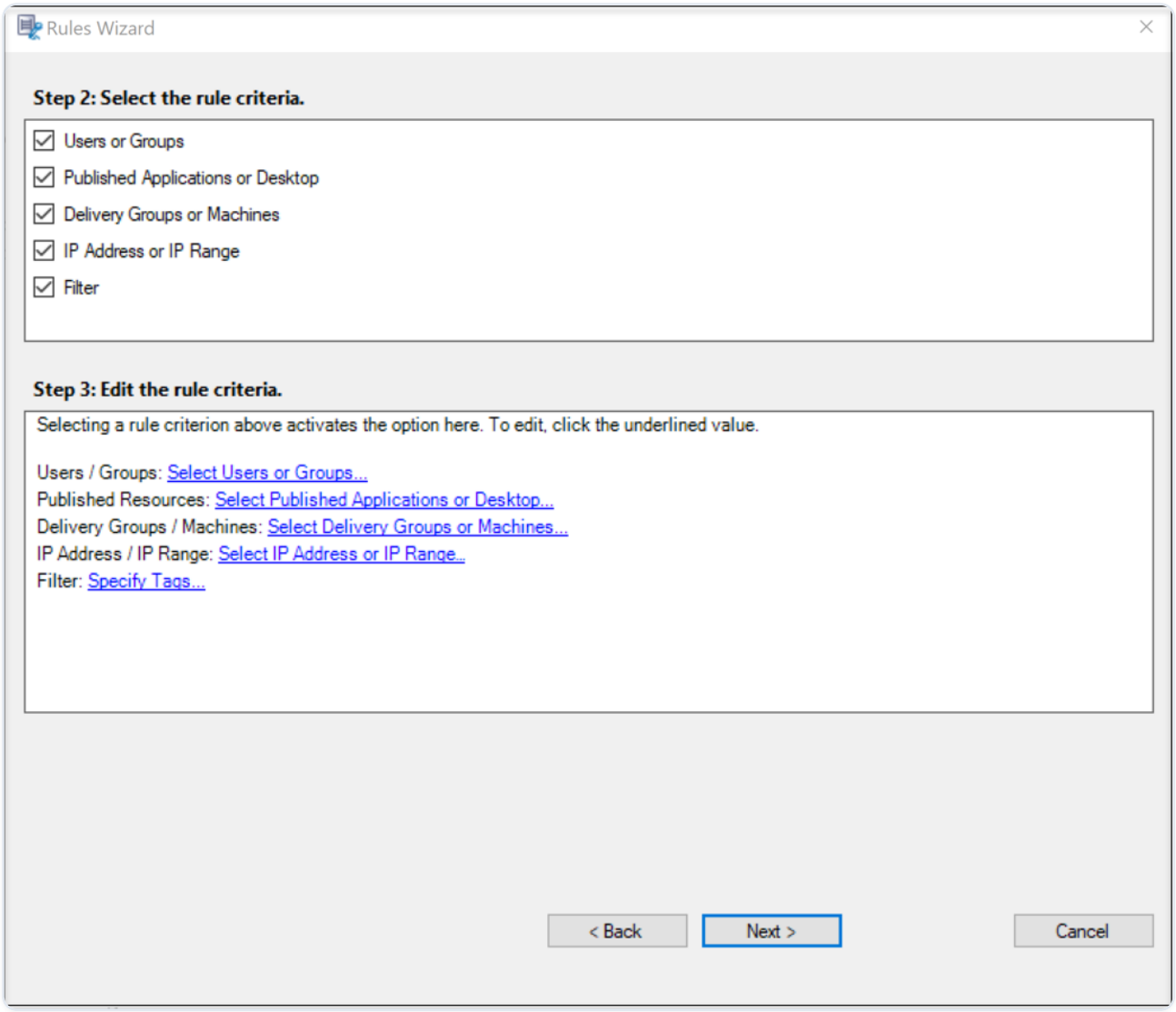
- **Disable session recording**. This option means that no sessions are recorded.
- **Hide specific applications during screen recording**. This feature lets you hide specific applications with a layer mask during screen recording. The color for the layer mask is configurable, which can be Black, Gray, or White.

  For example, you can see that an application is hidden during the recording playback:



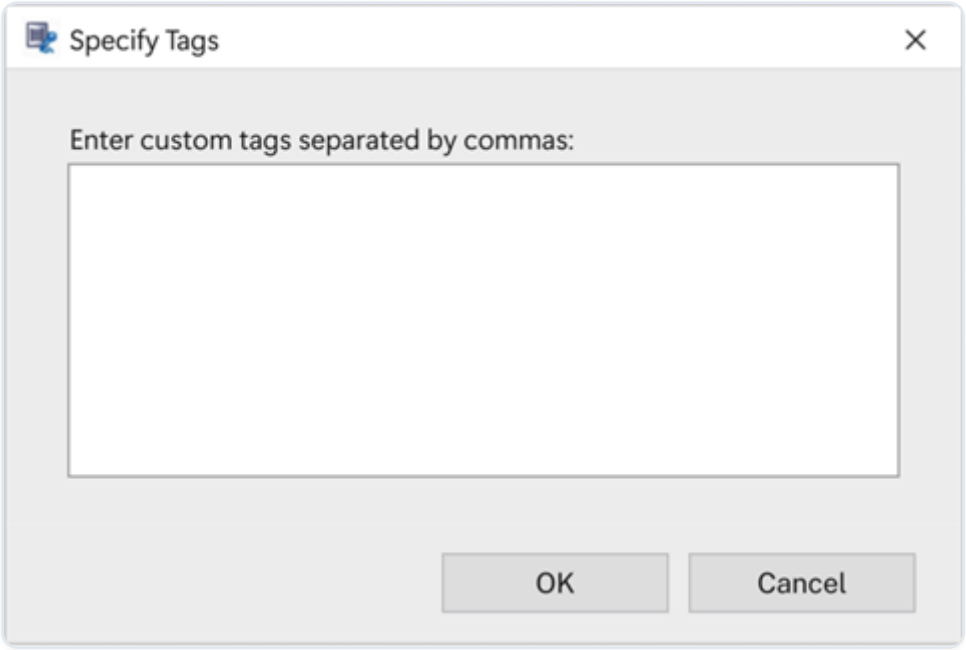
- **Allow user-initiated recording without interrupting admin or policy-driven recordings**. This feature lets end users start and stop recordings on demand. Administratorinitiated and policydriven recordings take precedence and are not interrupted by enduser triggered recordings.

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.

- **Filter**. Creates a list of smart access tags to which the action of the rule applies. You can configure contextual access (smart access) using smart access policies on Citrix NetScaler.



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 **Disable session recording** action have the highest priority.
- Rules with the **Enable session recording with notification** action have the second-to-highest priority.
- Rules with the **Enable session recording without notification** action have the second-to-lowest priority.

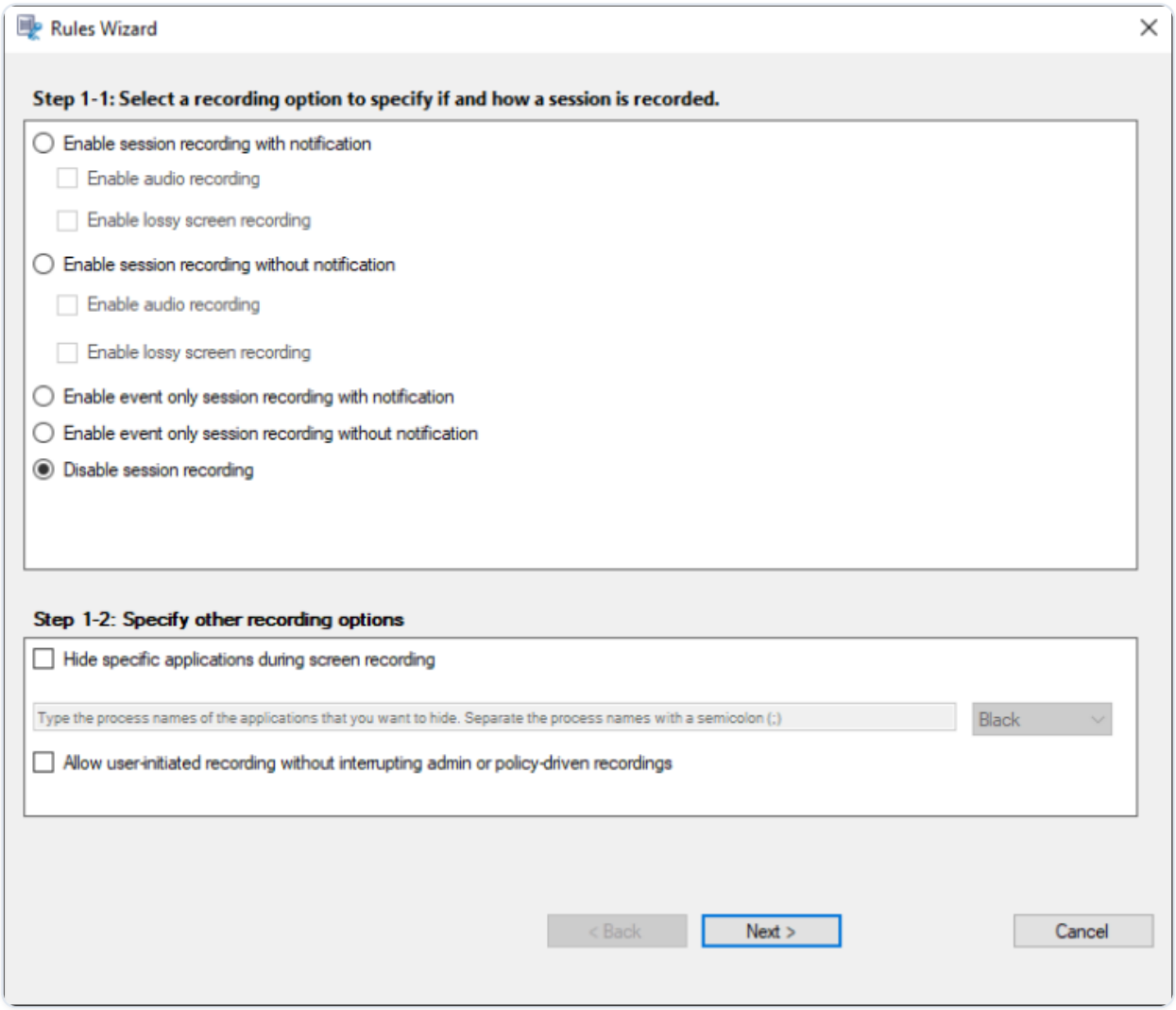
- Rules with the **Enable event only session recording with notification** action have the medium priority.
- Rules with the **Enable event only session recording without notification** action have the lowest priority.

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

Steps

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**.



When you select **Enable session recording with notification** or **Enable session recording without notification**, you can further select to enable audio recording or lossy screen recording.

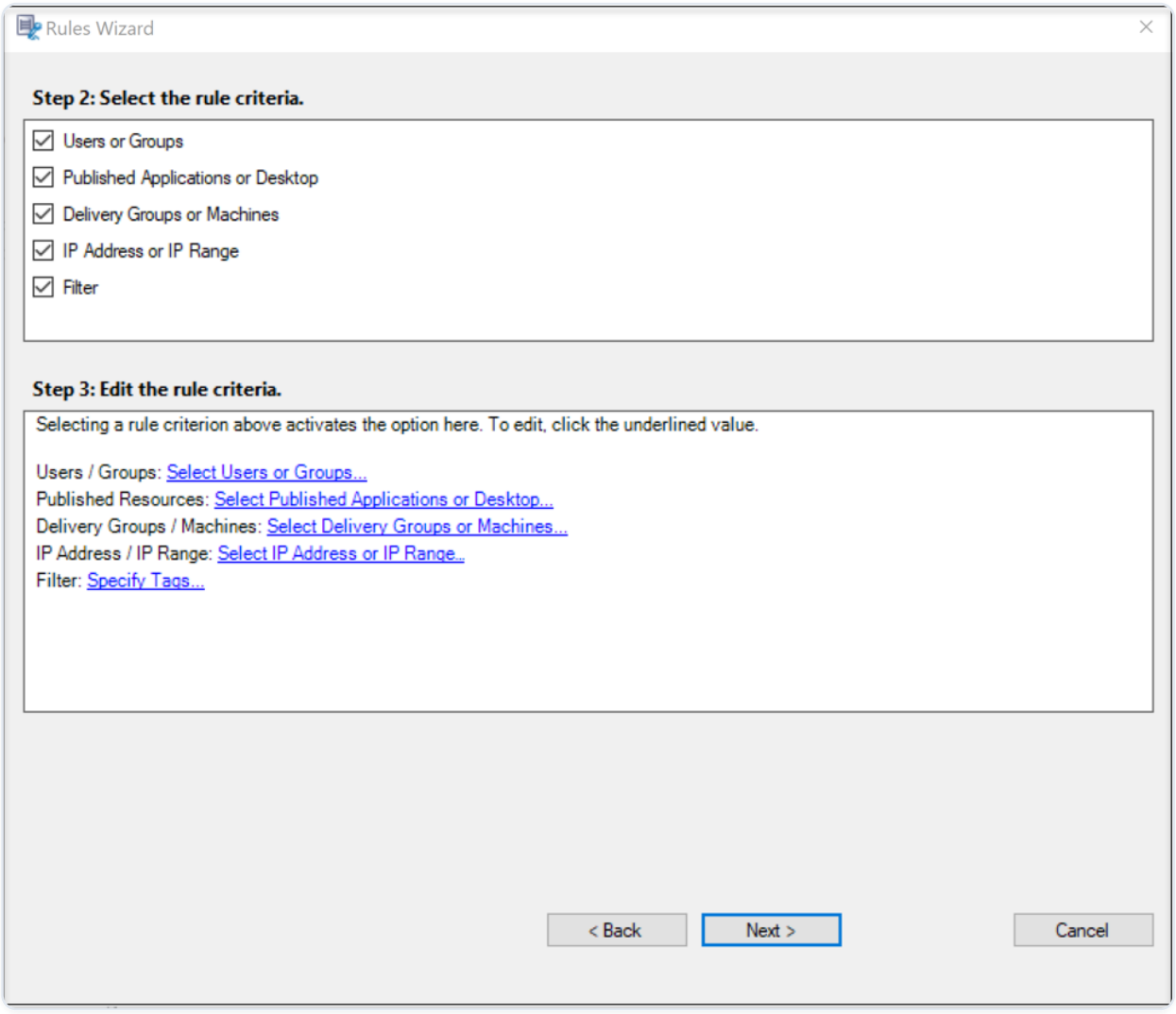
5. Select the rule criteria - You can choose one or more rule criteria:
    - **Users or Groups**
    - **Published Applications or Desktop**
    - **Delivery Groups or Machines**
    - **IP Address or IP Range**
    - **Filter**
6. Edit the rule criteria - To edit, click the underlined values. The values are underlined based on the criteria that you chose in the previous step.

> **Note:**

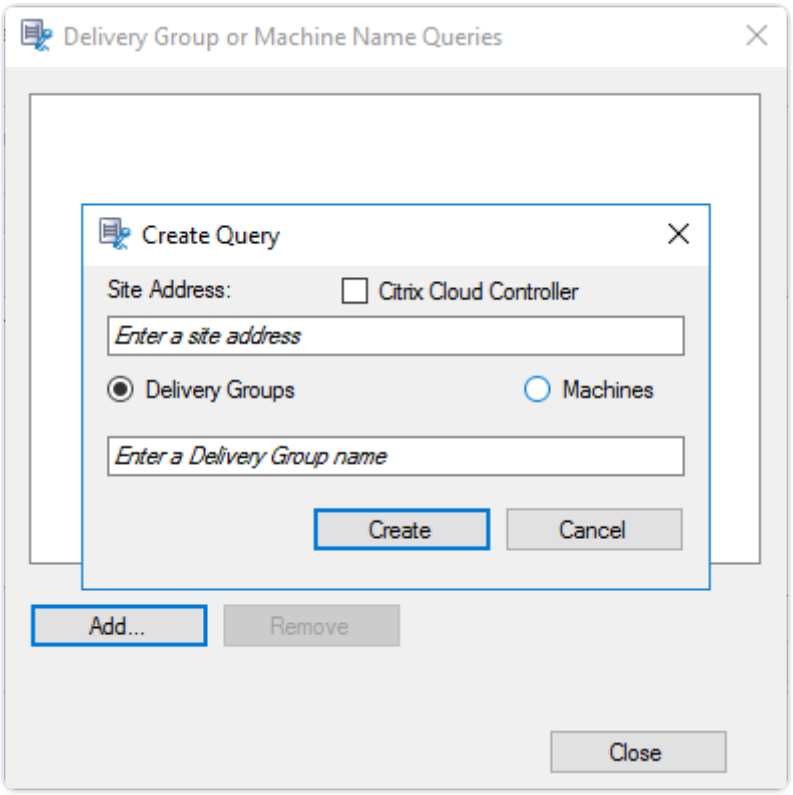
> If you choose the **Published Applications or Desktop** underlined value, the **Site Address** is the IP address, a URL, or a machine name if the Controller is on a local network. The **Name of Application** list shows the display name.

> 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 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.
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.

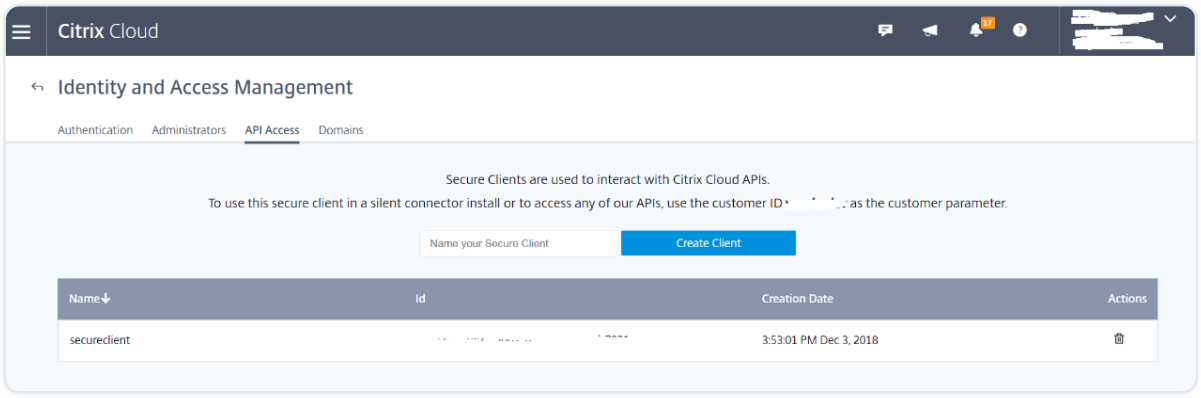
USE CASE	ACTION REQUIRED
	3. Clear the **Citrix Cloud Controller** check box.

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 the 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've reached the maximum size or recording duration. For more information about the rollover thresholds, see Specify file size for recordings.

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

IF THE PREVIOUS RECORDING POLICY WAS	AND THE NEW RECORDING POLICY IS	AFTER A ROLLOVER, THE RECORDING POLICY WILL BE
Do not record	Any other policy	No change. The new policy takes effect only when the user logs on to a new session.
Record without notification	Do not record	The recording stops.
Record without notification	Record with notification	Recording continues and a notification message appears.
Record with notification	Do not record	The recording stops.
Record with notification	Record without notification	Recording continues. No message appears the next time a user logs on.

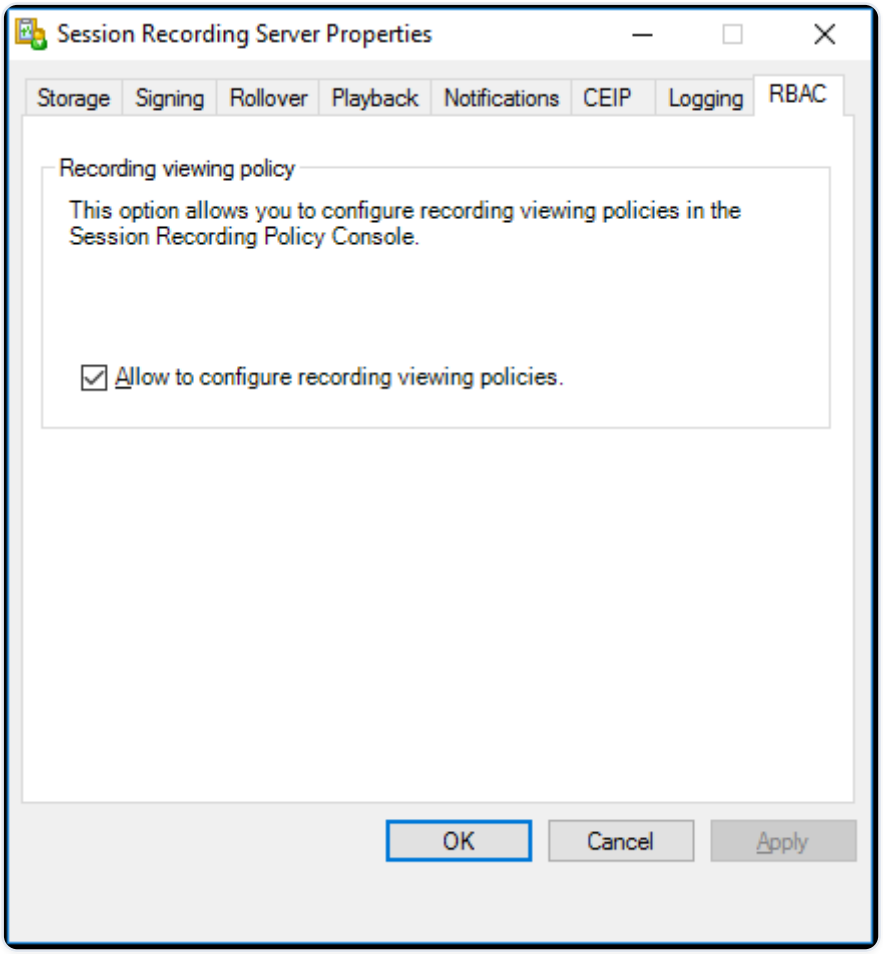
Configure recording viewing policies

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:

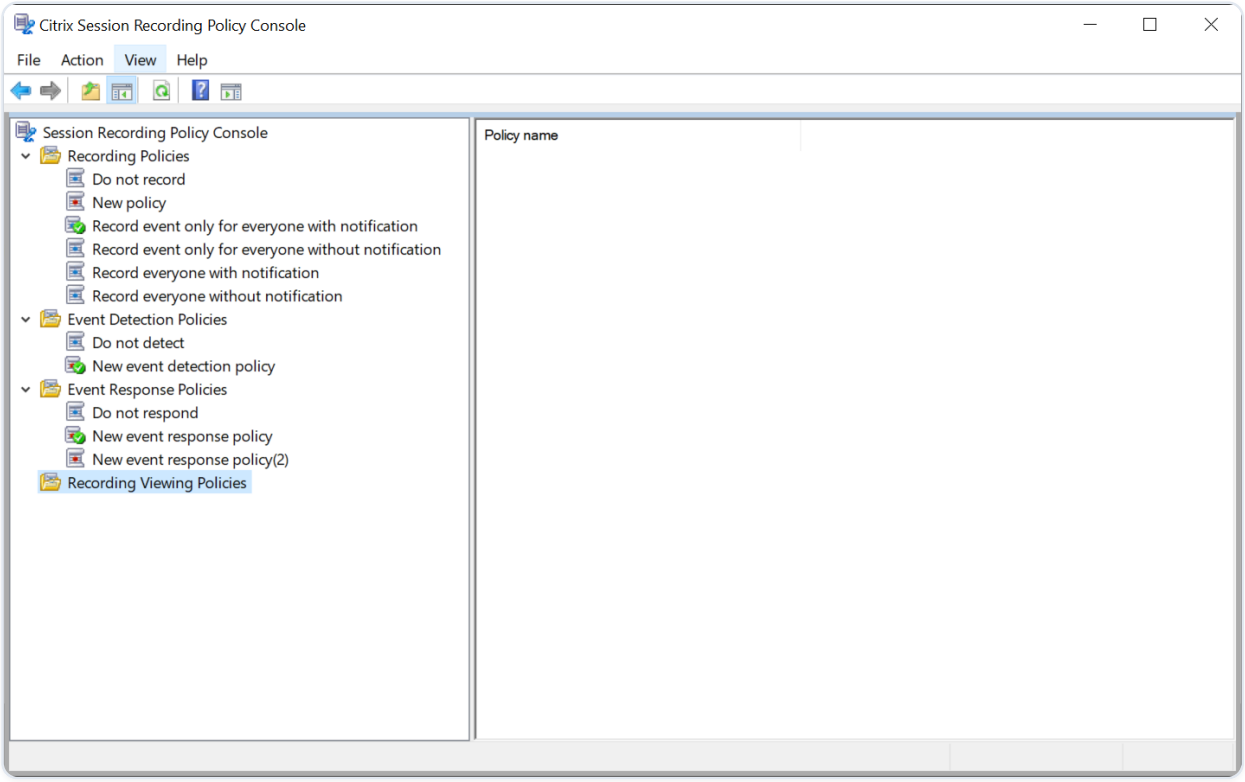
1. Log on to the machine hosting the Session Recording server.
2. From the **Start** menu, choose **Session Recording Server Properties**.
3. In **Session Recording Server Properties**, click the **RBAC** tab.
4. Select the **Allow to configure recording viewing policies** check box.



To create a custom recording viewing policy:

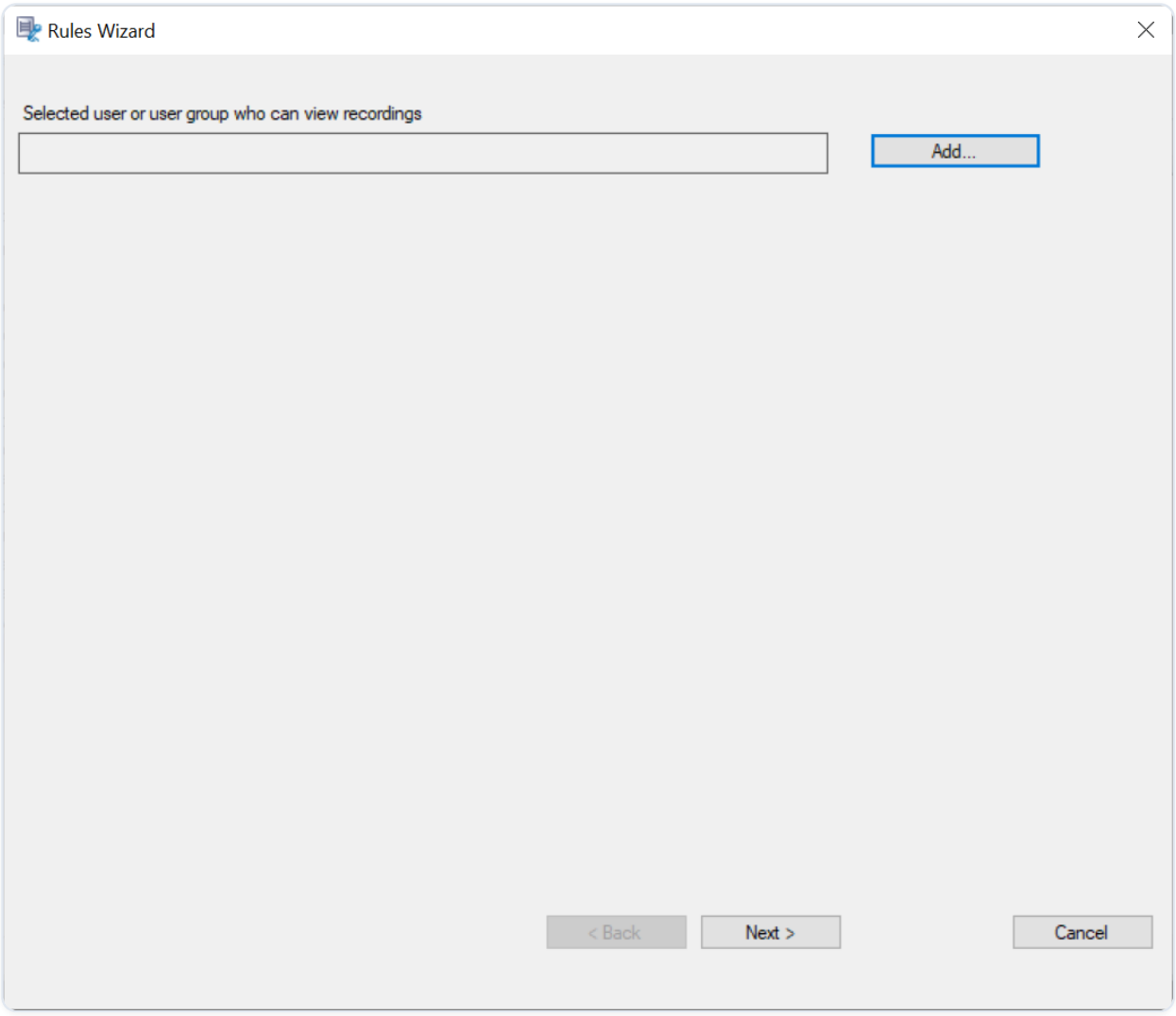
Note: Different from recording policies and event detection policies, a recording viewing policy (including all rules added within) is active immediately when it is created. You do not have to activate it.

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.



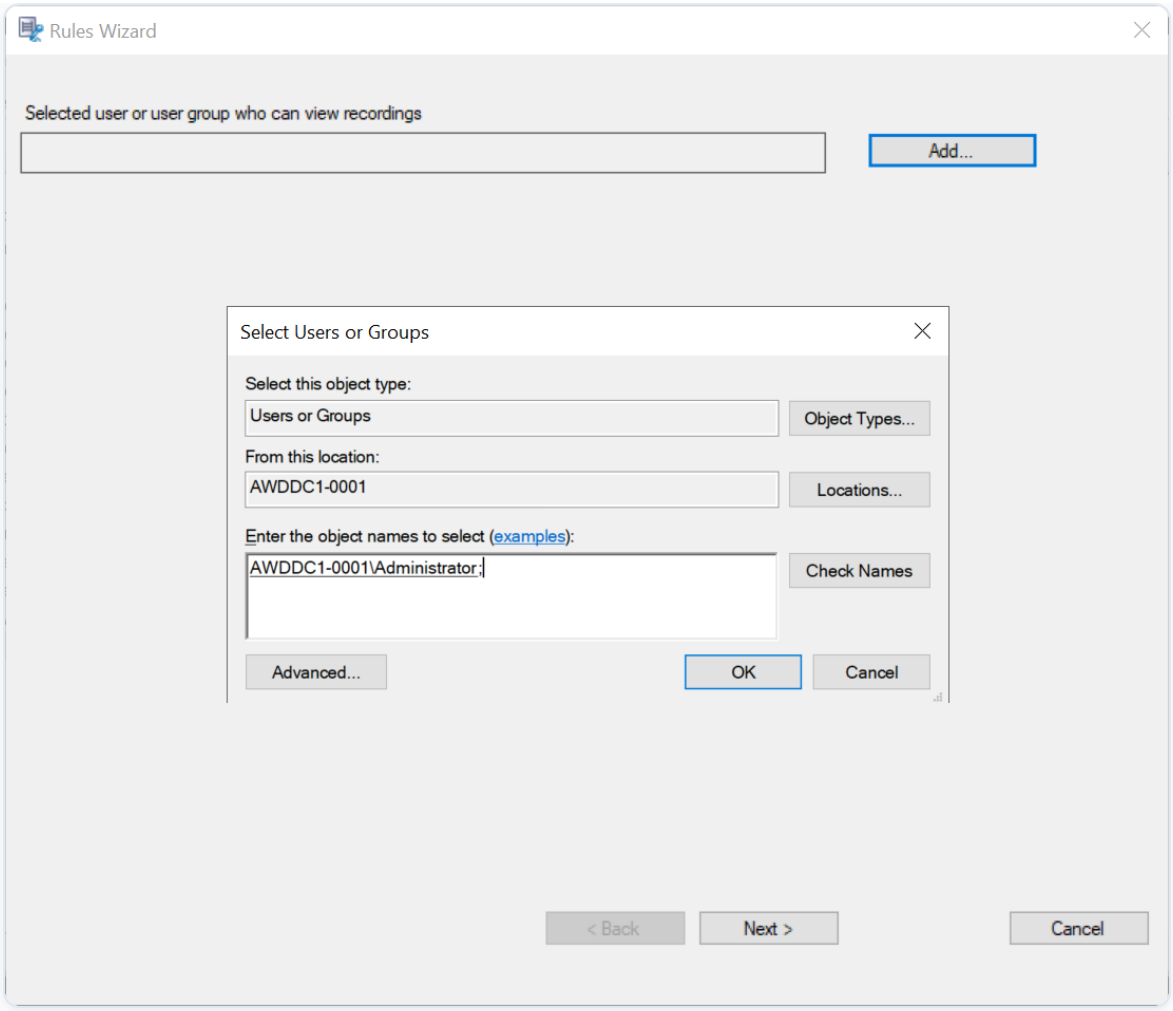
Note: To make **Recording Viewing Policies** available, enable the feature in **Session Recording Server Properties** first.

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.



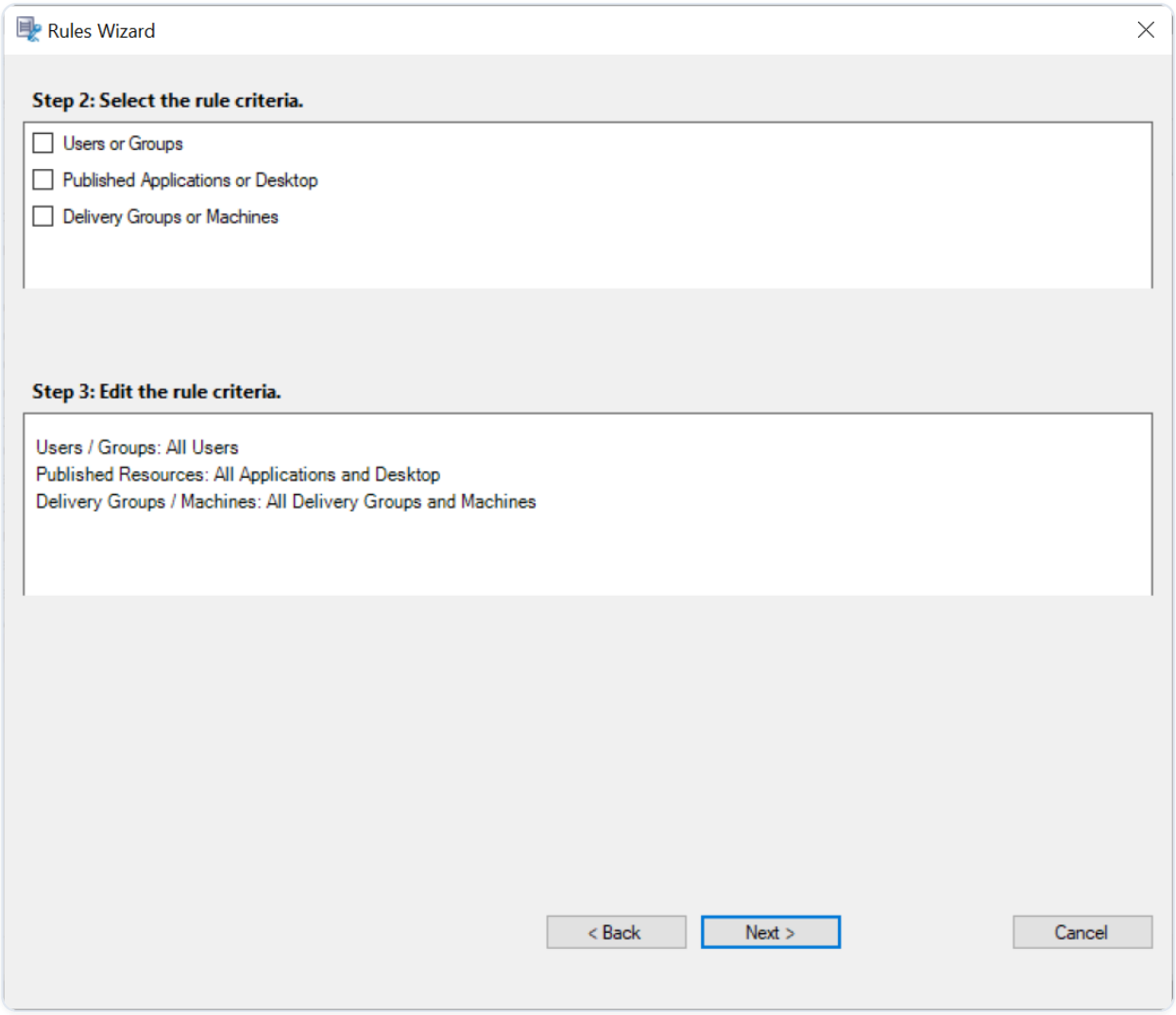
Note:

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**

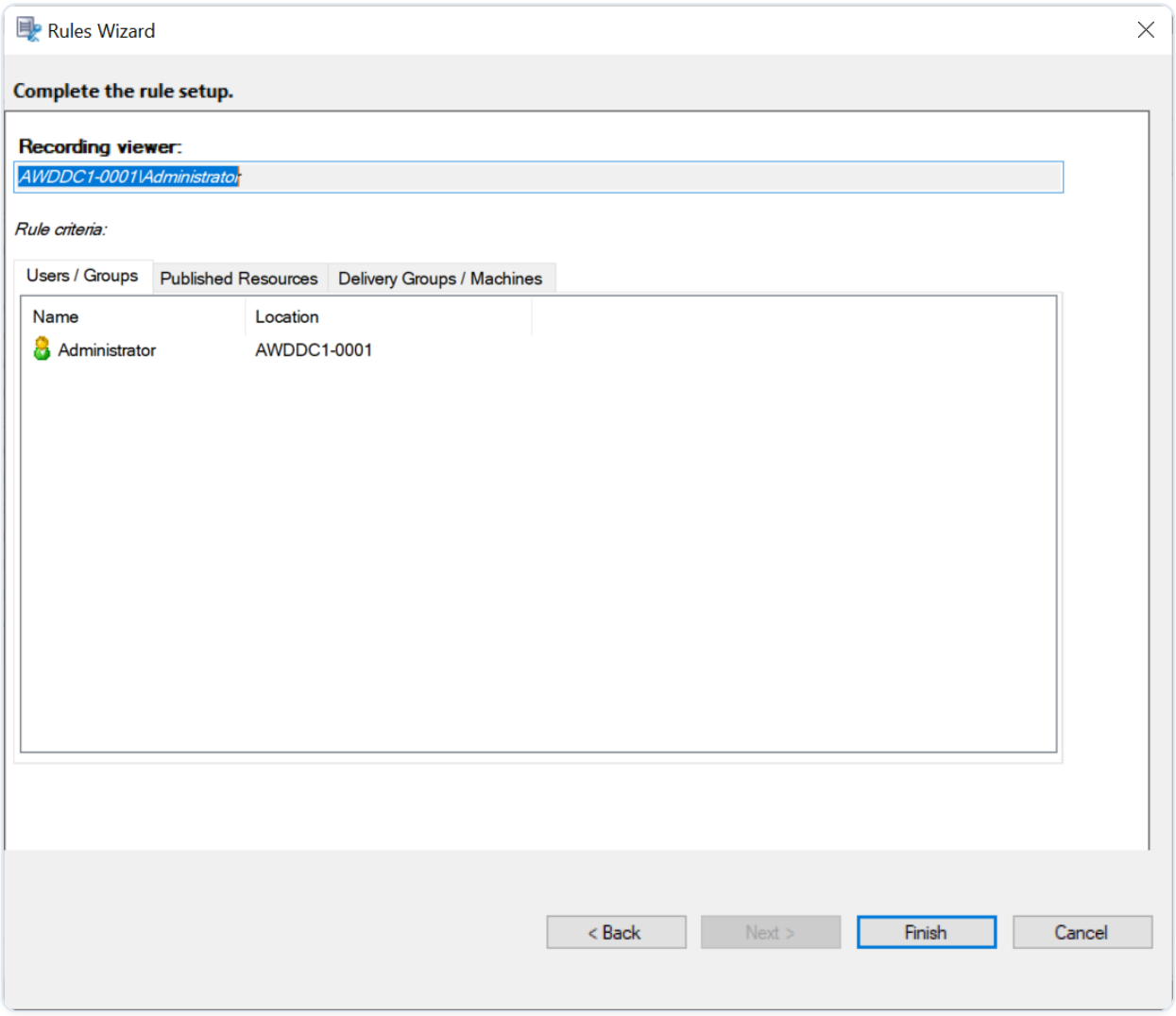
- **Published Applications or Desktop**
- **Delivery Groups or Machines**



> **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

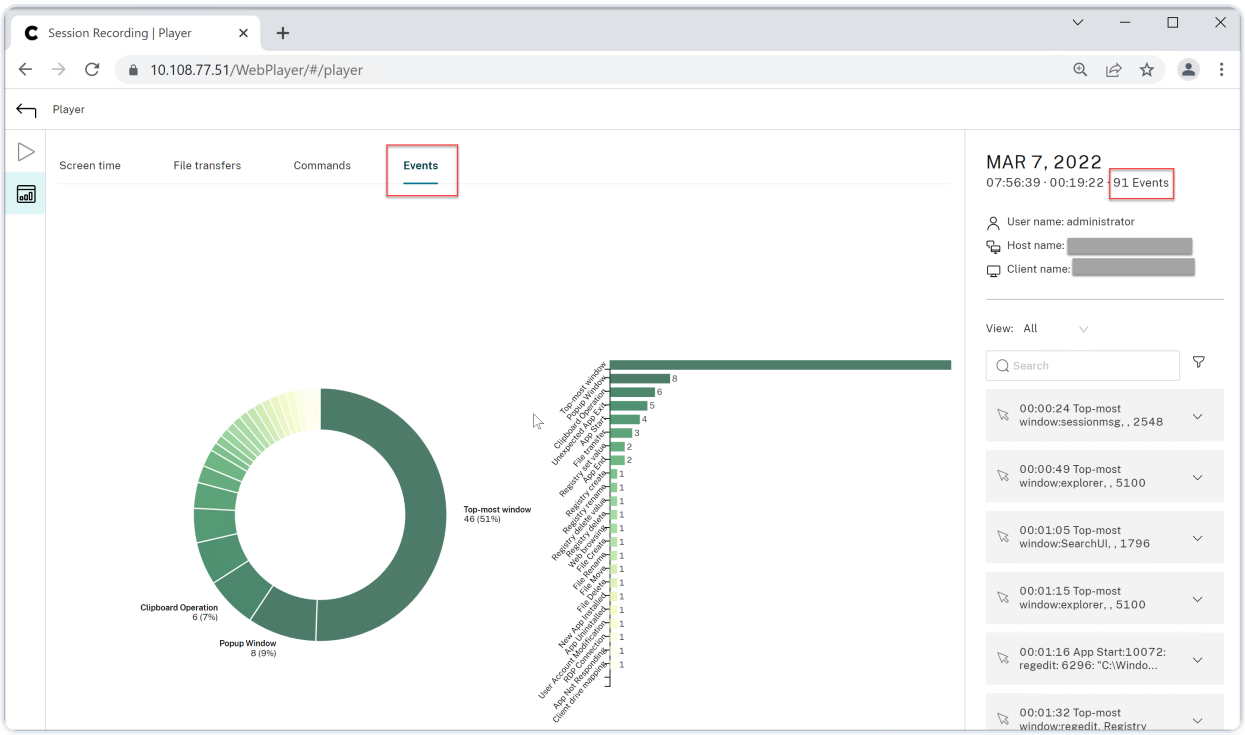
Session Recording can detect and log the following system-defined events that occur during recorded sessions:

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

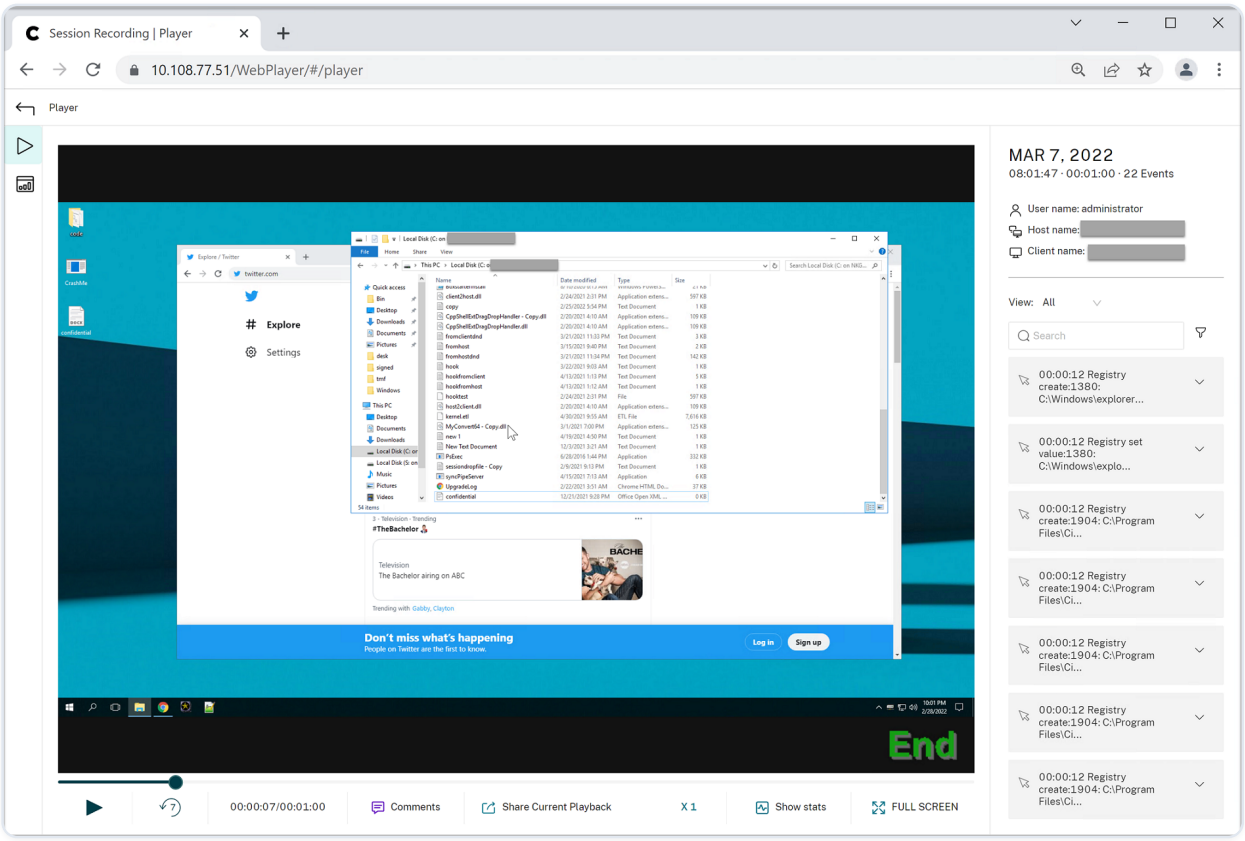
- App failures
- App installs and uninstalls
- File renaming, creation, deletion, and moving operations within sessions
- File transfers between session hosts (VDAs) and client devices (including mapped client drives and generic redirected mass storage devices)
- Web browsing activities
- Topmost window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

For example:

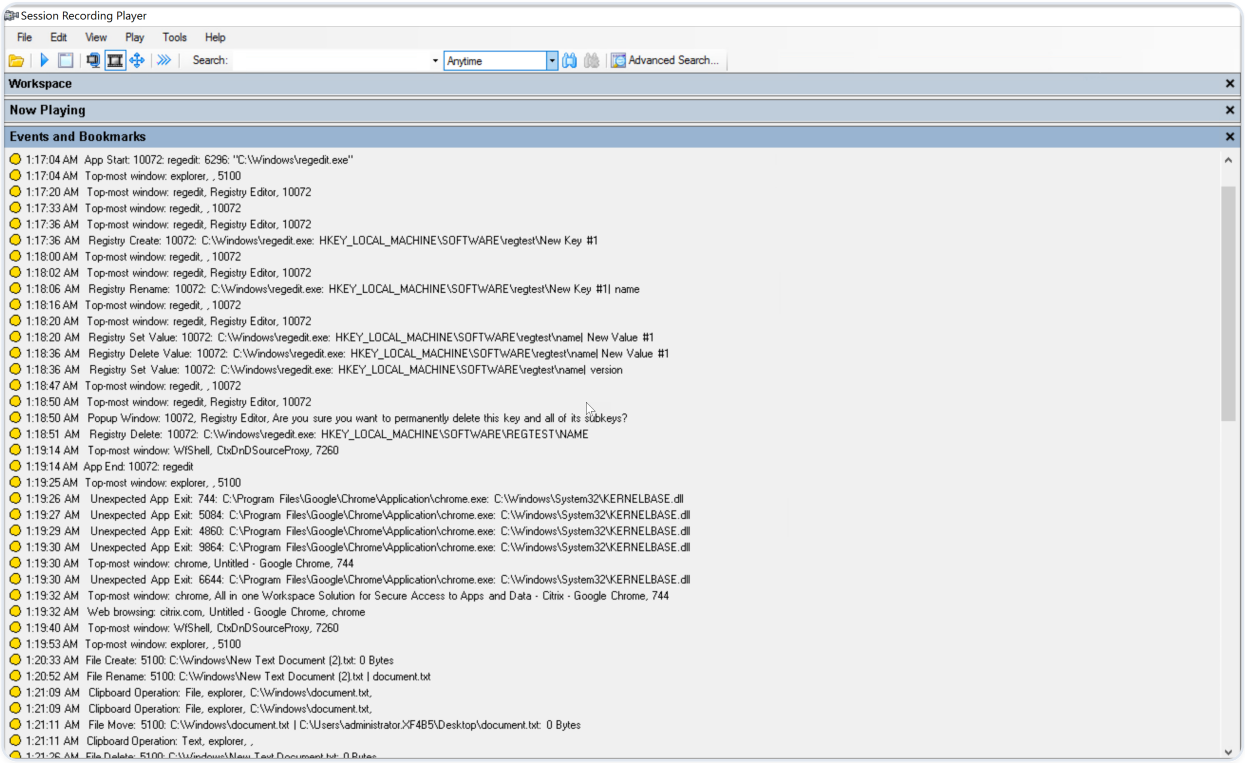
- Events in an event-only recording in the web player:



- Events in a screen recording in the web player:



- Events in the Session Recording player:



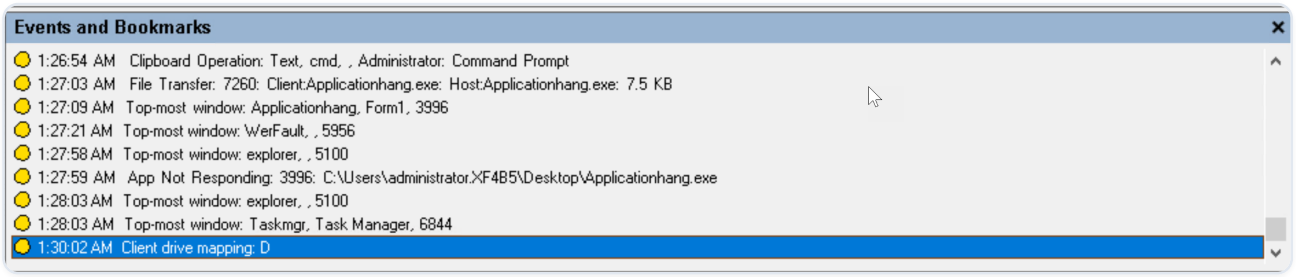
For more events in the Session Recording player, see the event descriptions later in this article.

> **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.

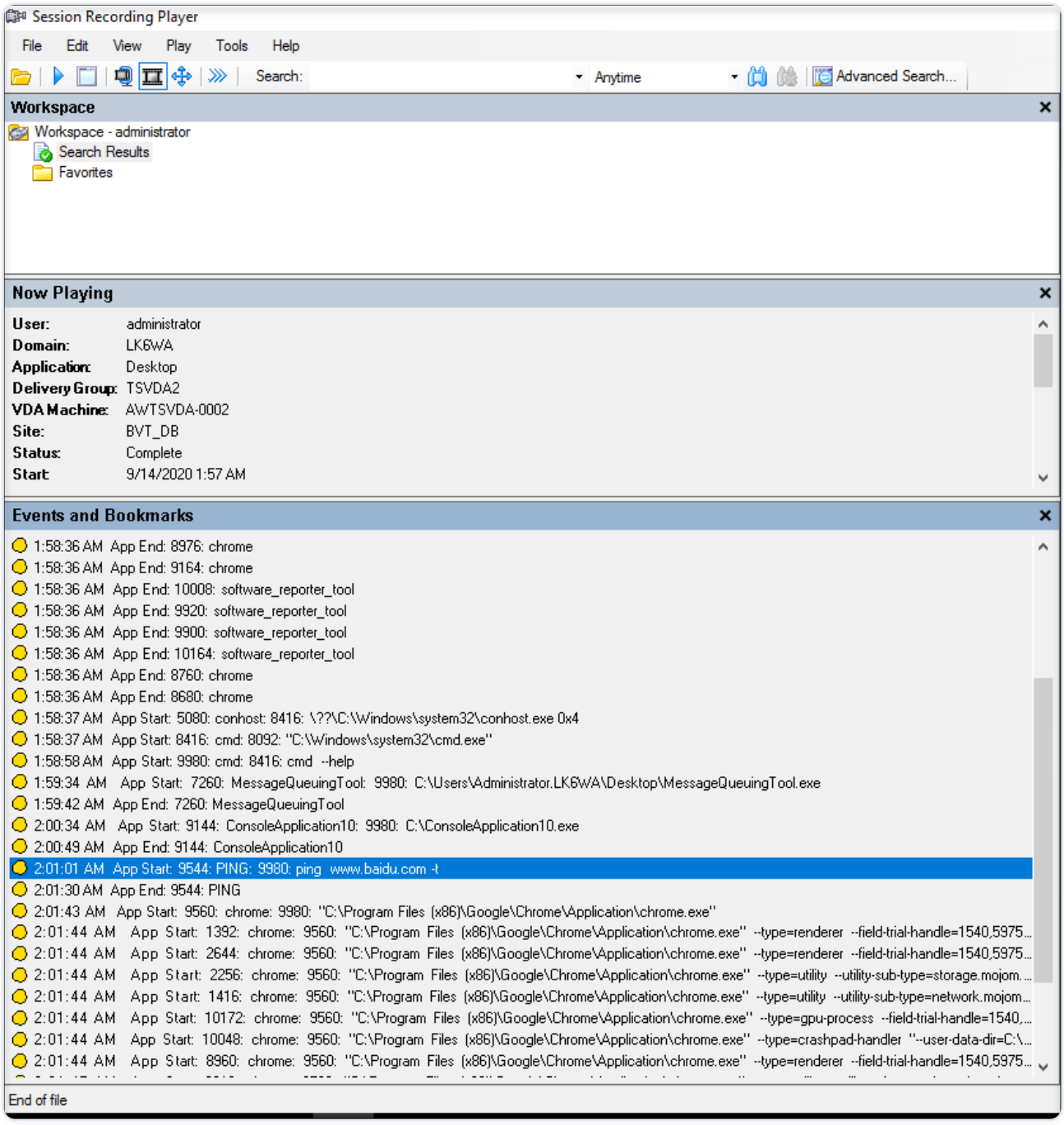
> Currently, only the insertion of USB mass storage devices (USB Class 08) can be detected.

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.



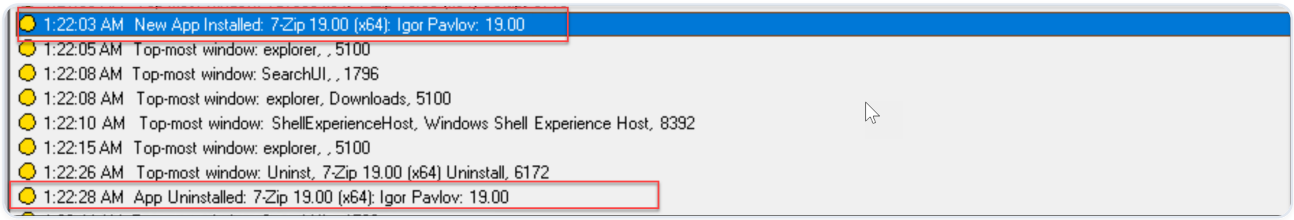
APPLICATION FAILURES

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.



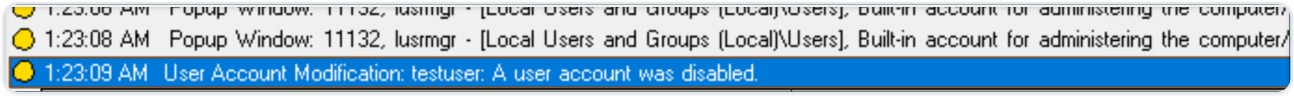
APP INSTALLS AND UNINSTALLS

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



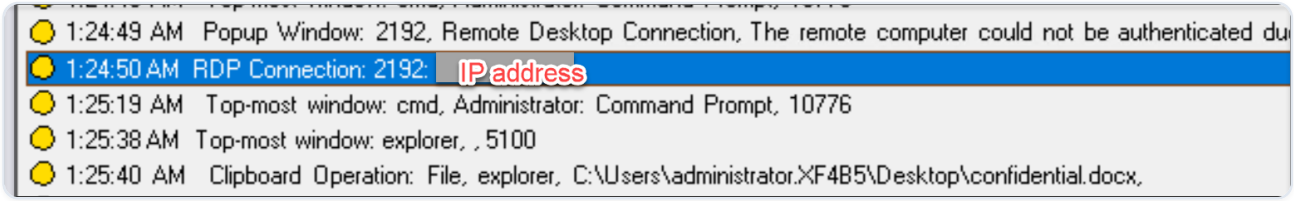
USER ACCOUNT MODIFICATIONS

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



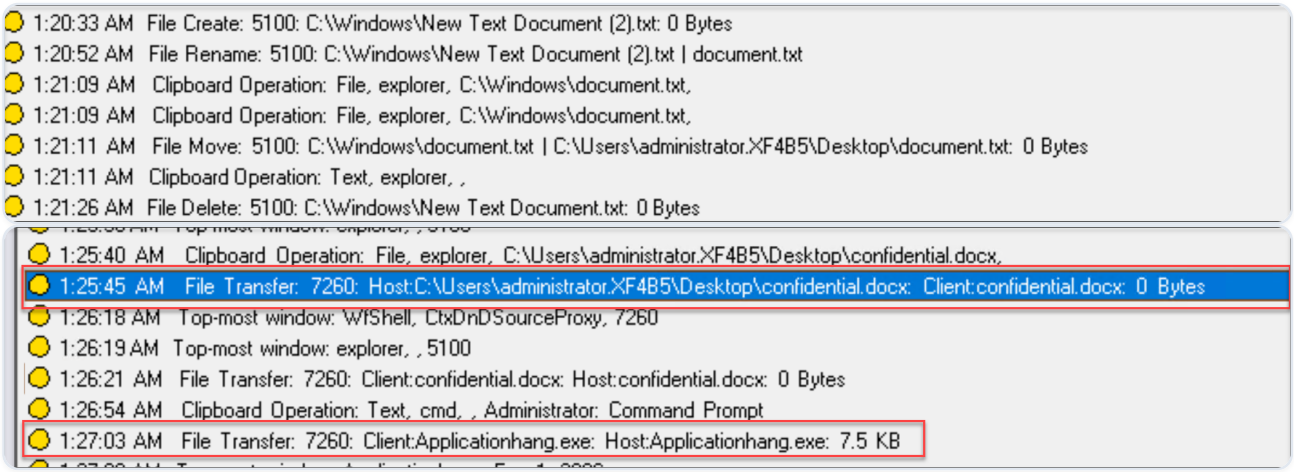
RDP CONNECTIONS

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.



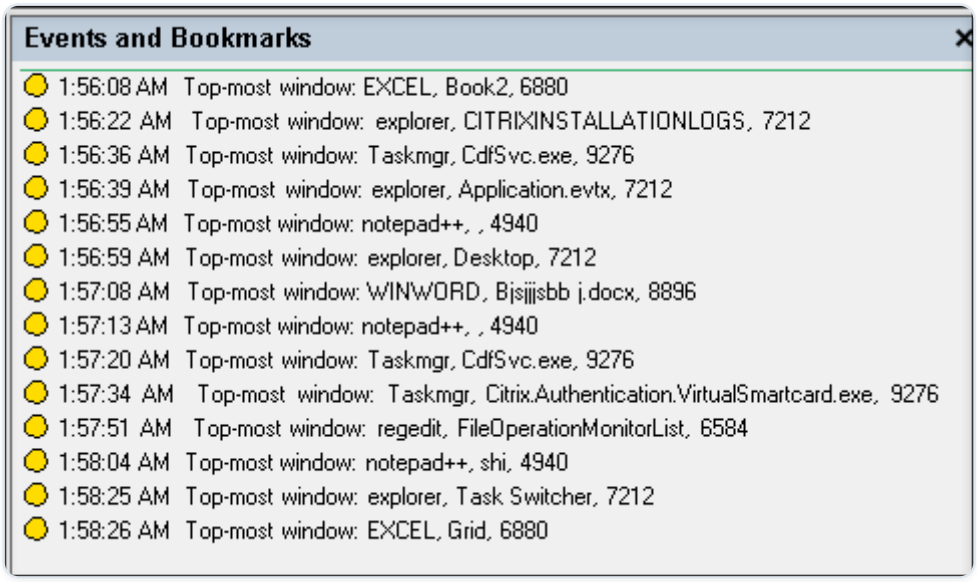
List of supported browsers:

- 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.

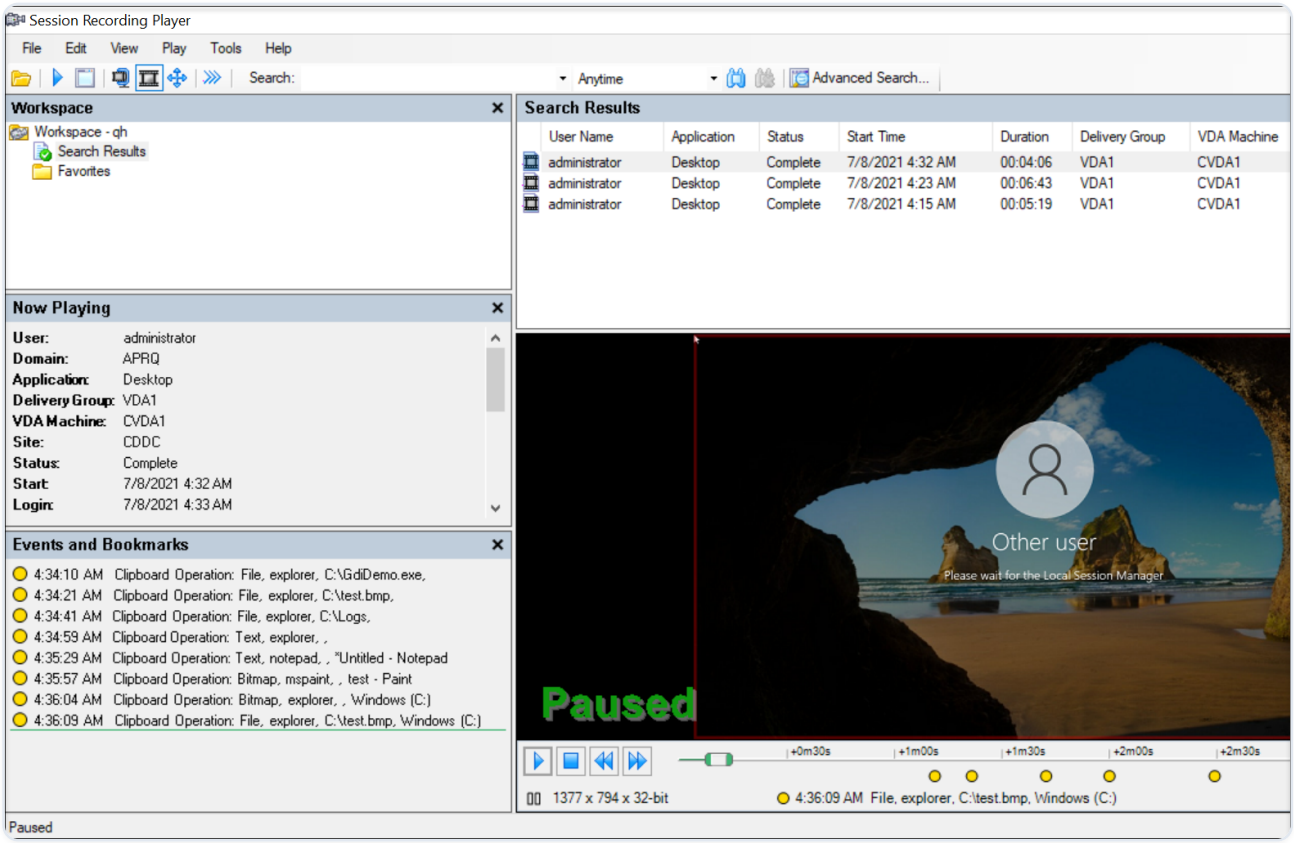


CLIPBOARD ACTIVITIES

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`).

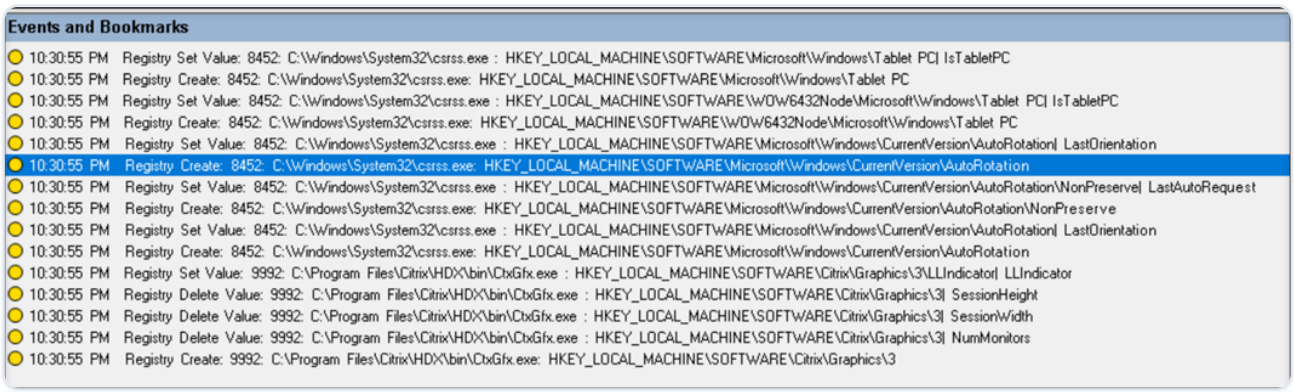


WINDOWS REGISTRY MODIFICATIONS

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:



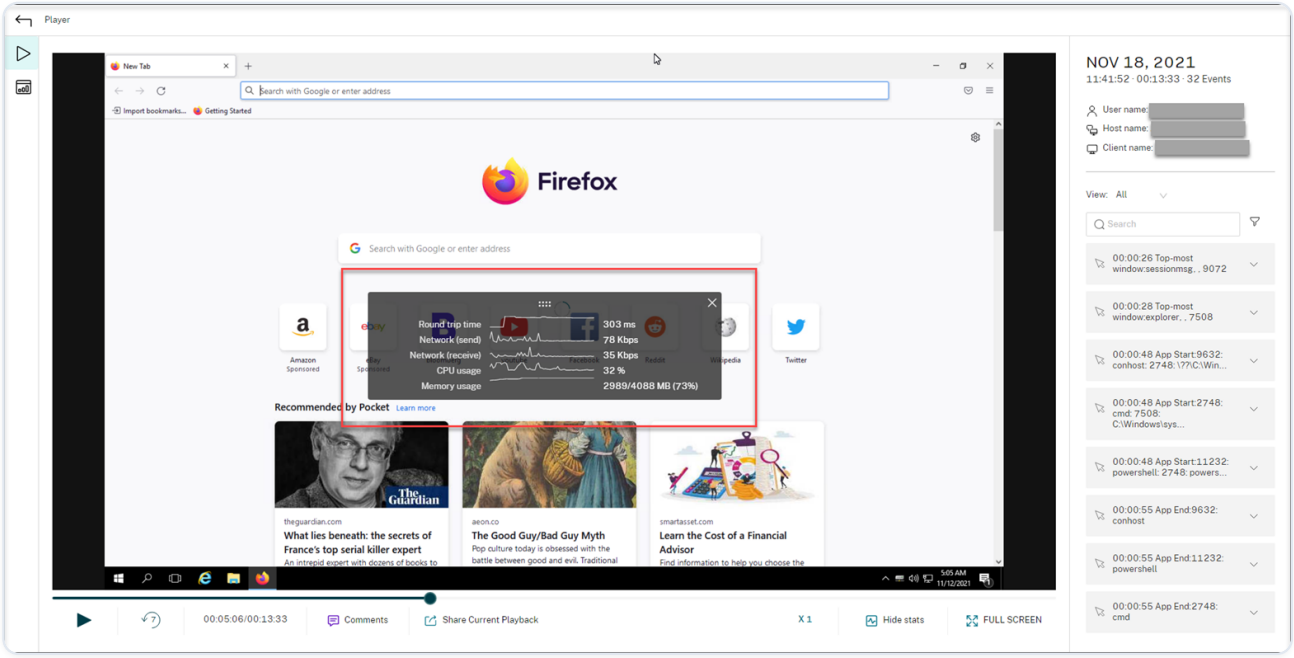
To enable this registry monitoring functionality, select the **Log registry modifications** option for your event detection policy.

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)

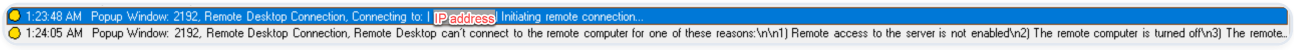
- Network (receive)
- CPU usage
- Memory usage



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.



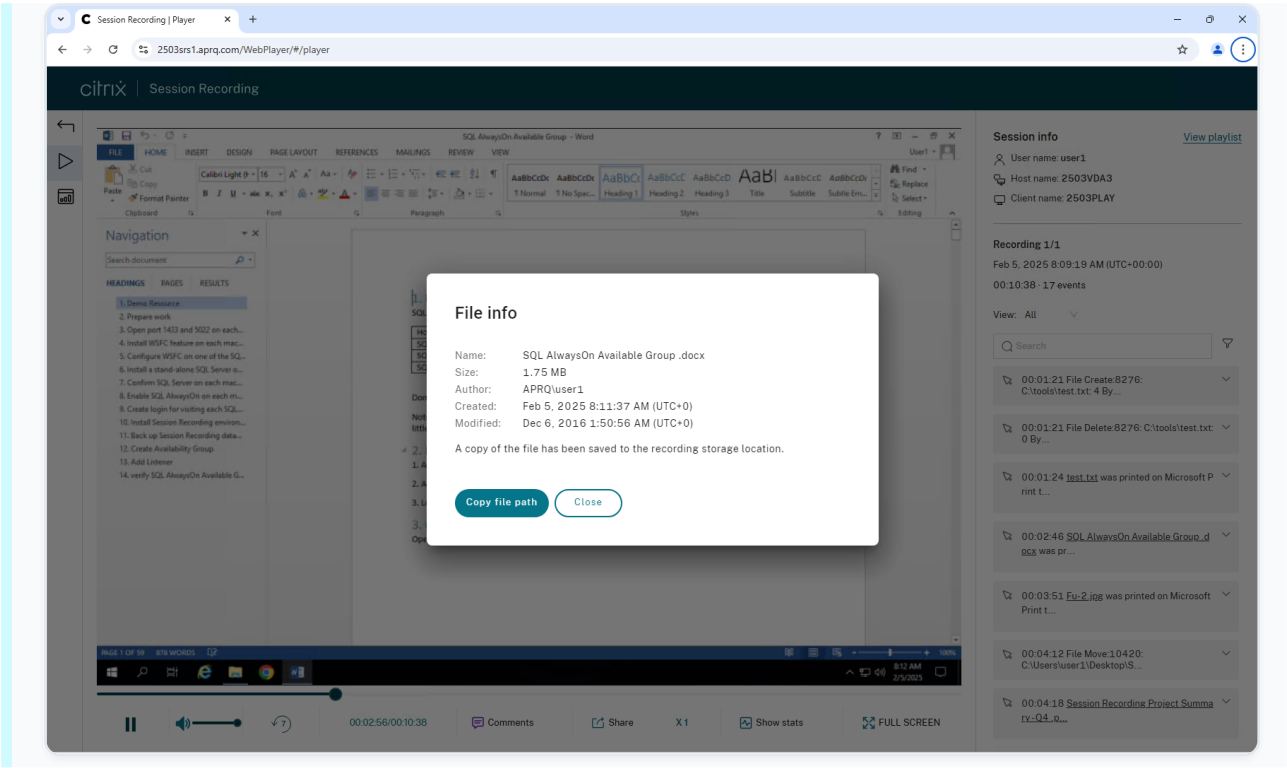
PRINTING ACTIVITIES

Session Recording monitors printing activities that occur during recorded sessions and tags them as events in recordings for later search and playback.

For an example printing activity event in the Session Recording web player, see the following screen capture:

> **Note:**

> Printing activity events file information are not displayed in the Session Recording player.



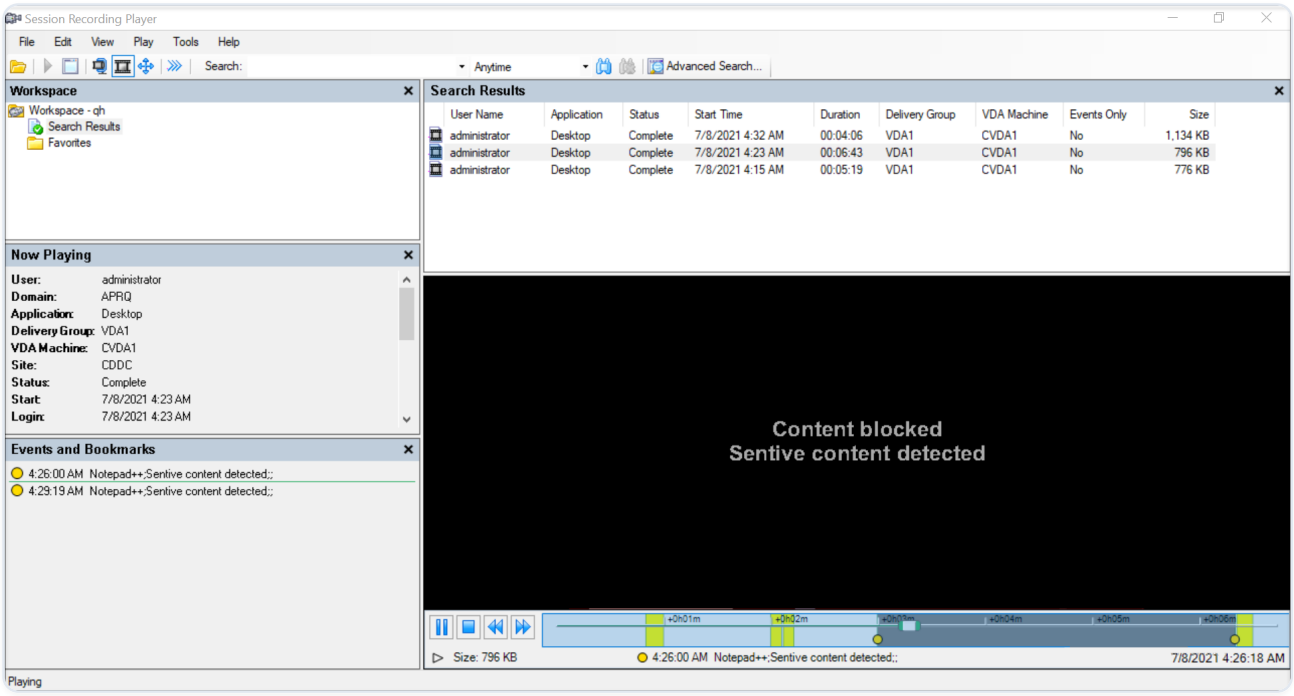
On the session replay interface, you can view printing events and click printed files in the right pane to access detailed file information.

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.

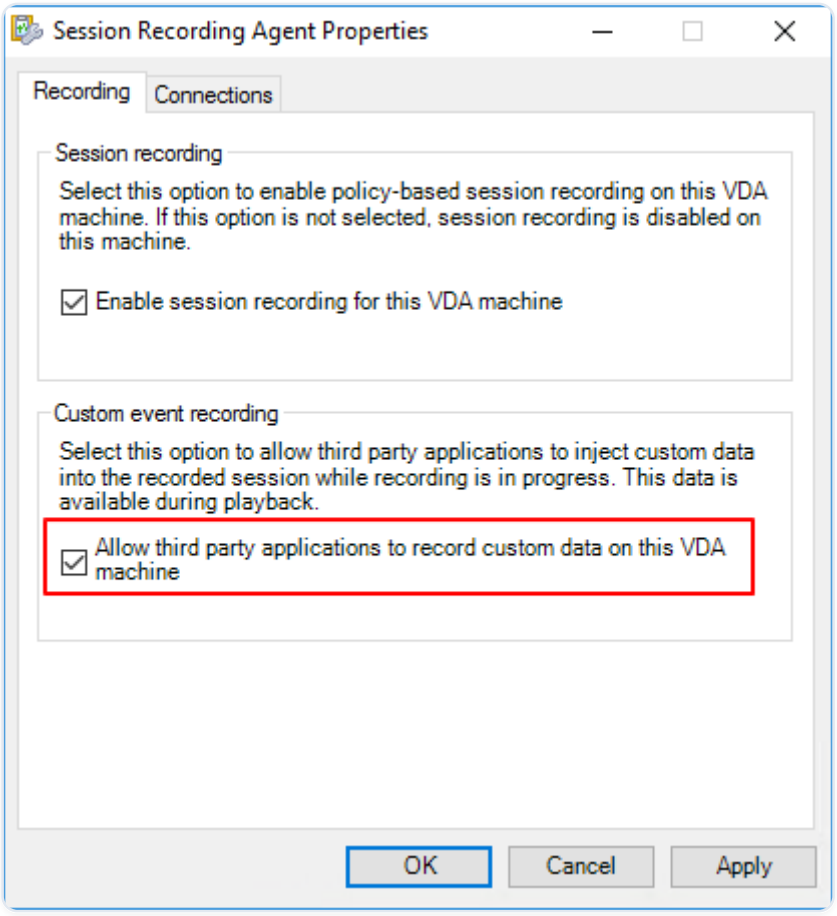
SENSITIVE INFORMATION BLOCKING

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**.

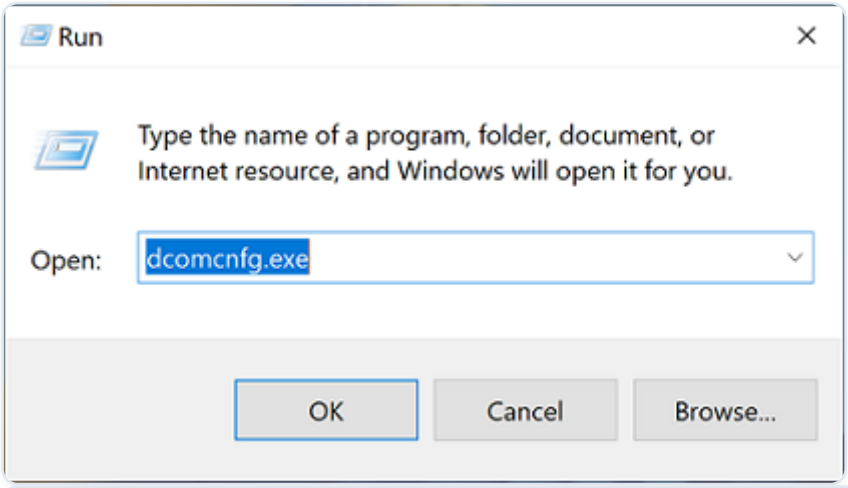


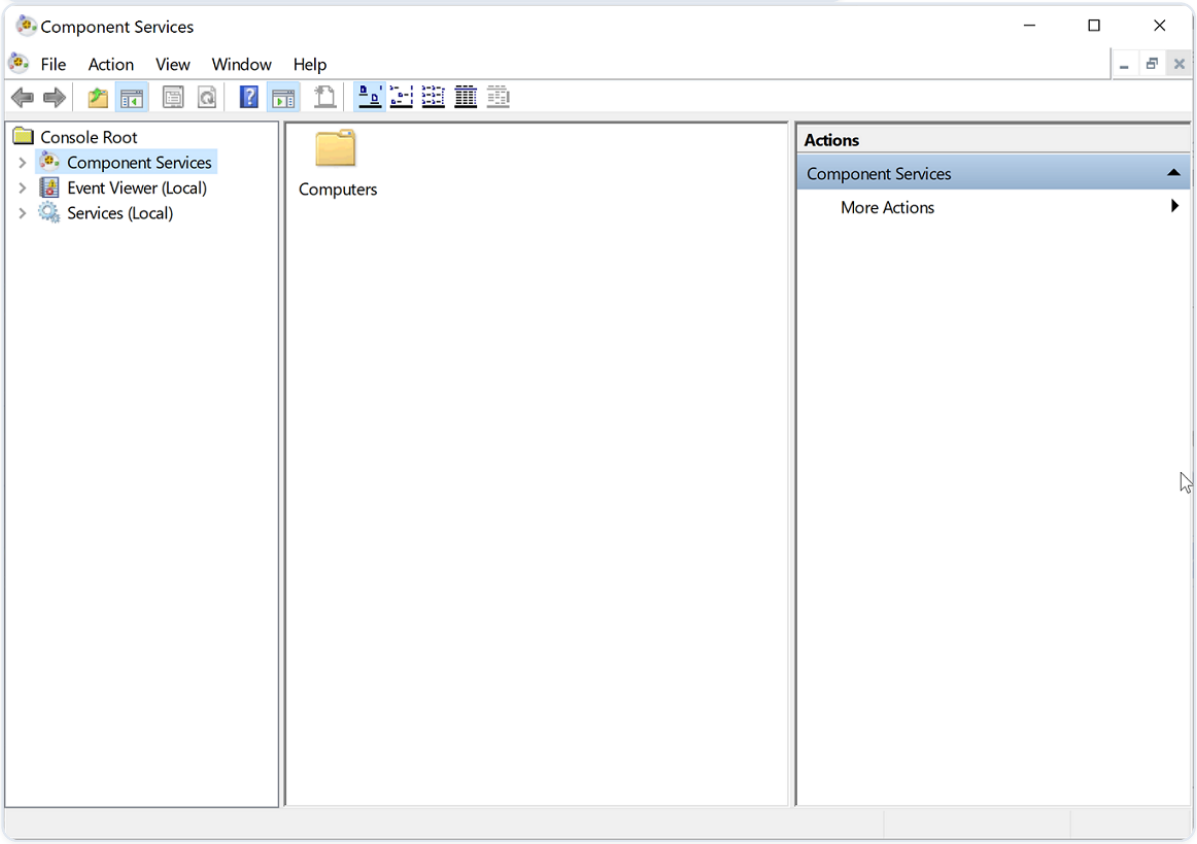
2. Grant users permission to invoke the Session Recording Event API (IUserApi COM interface).

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.

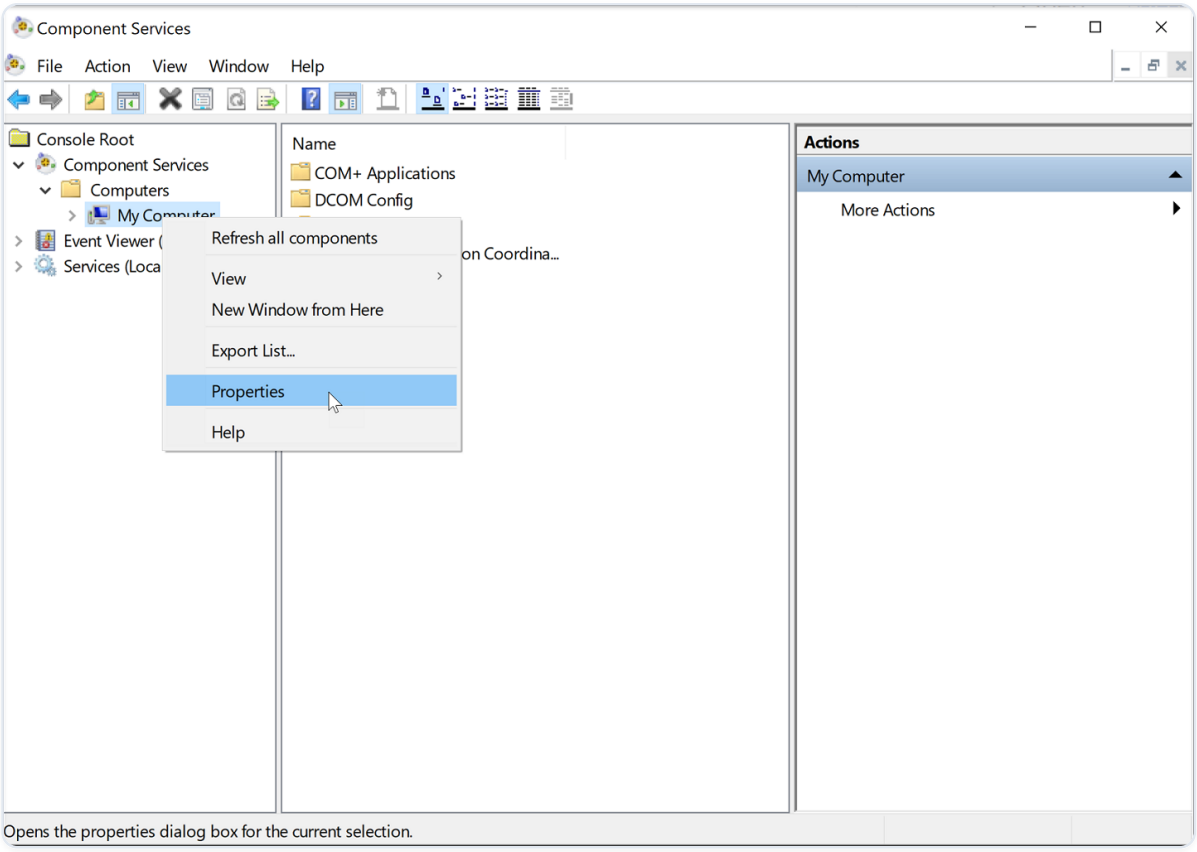




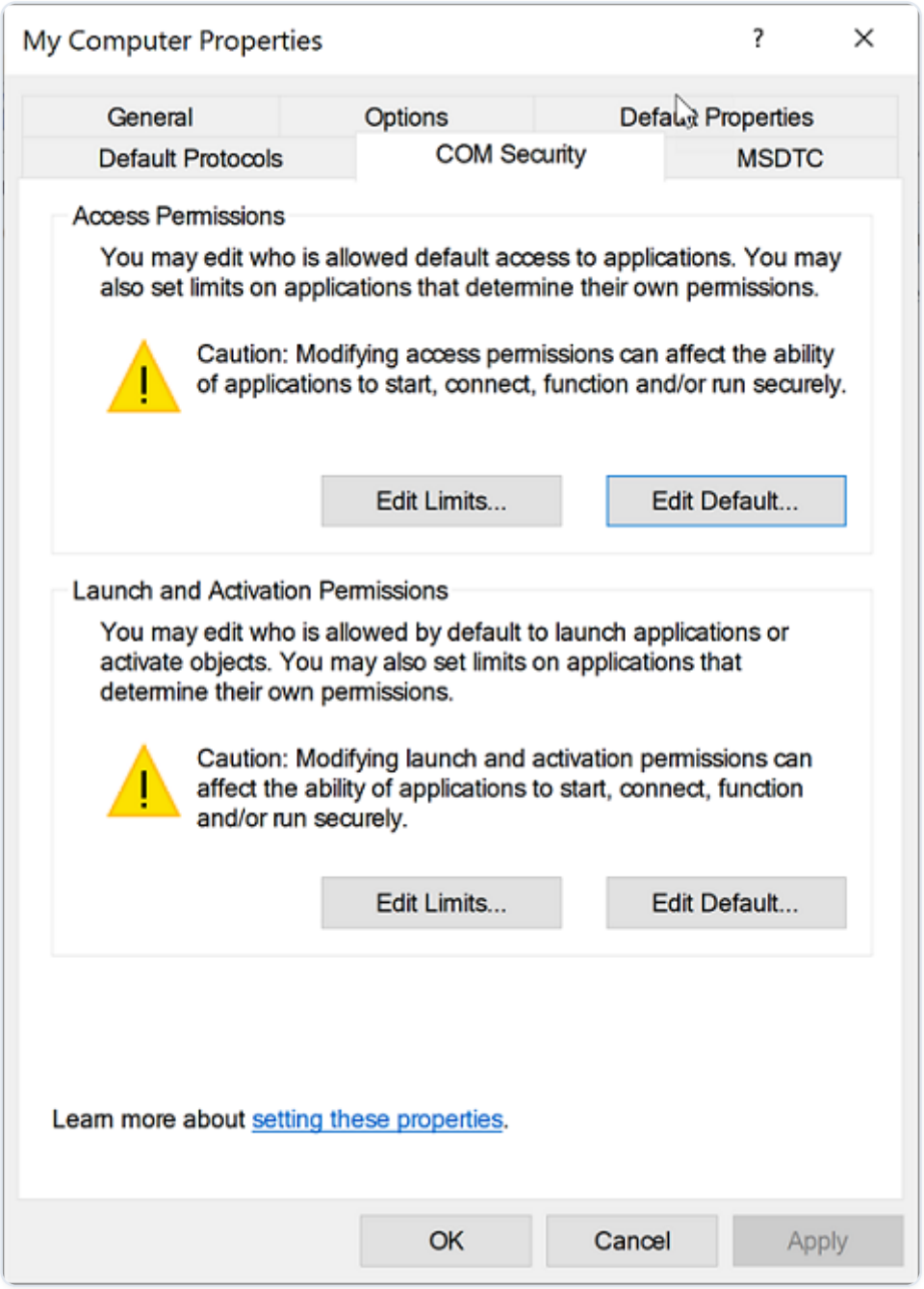
If you are granting permission to users who are not members of the domain administrator group and the Session Recording agent is running on Windows Server 2019 or later, or Windows 10 or later, proceed to step b. Otherwise, skip step b and go to step c directly.

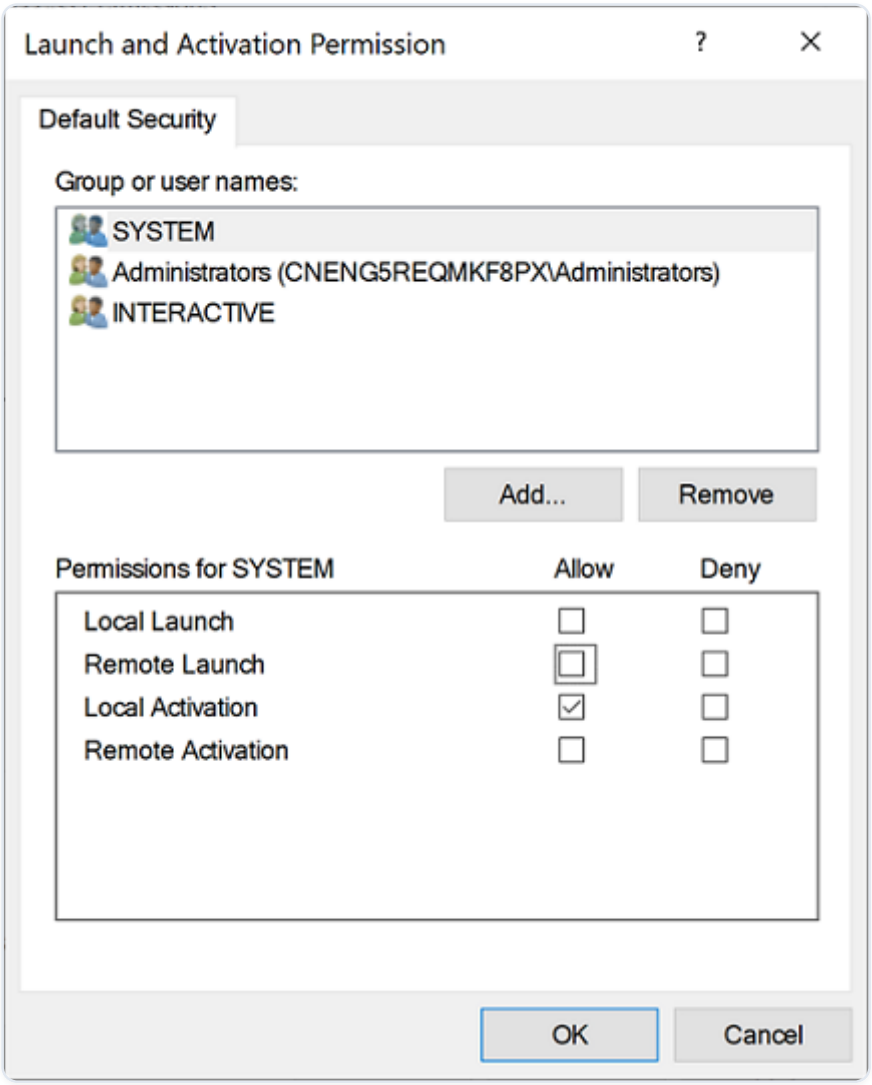
b. Select **Console Root > Component Services > Computers > My Computer** from the left navigation.

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

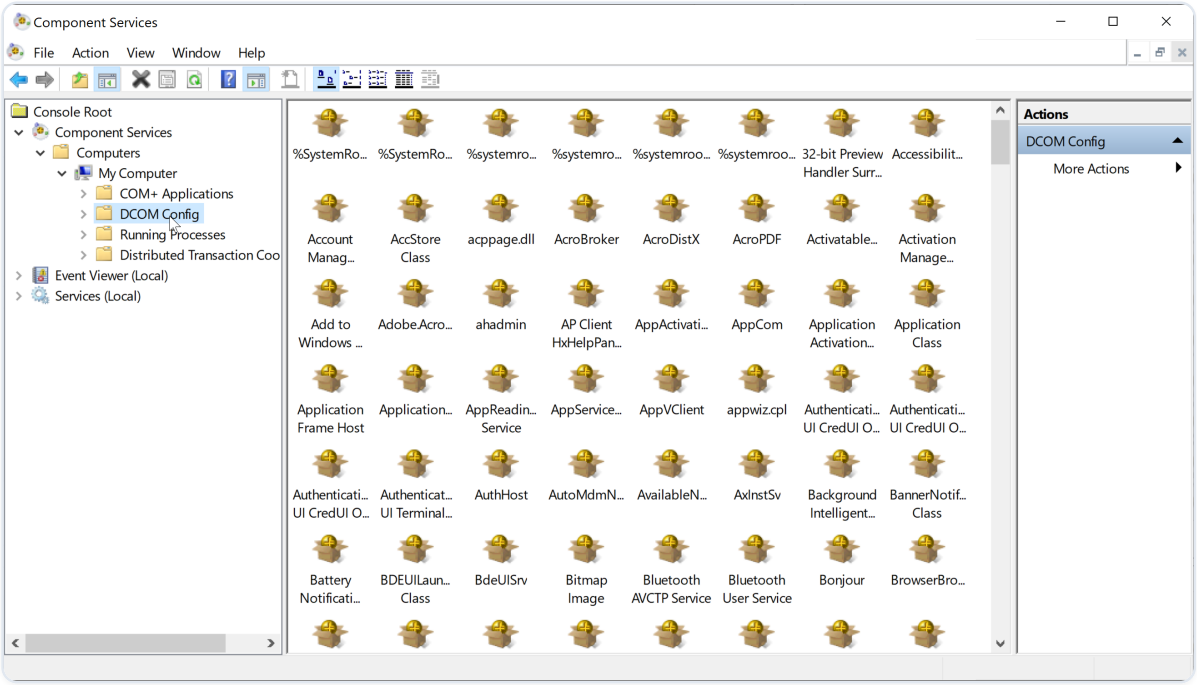


Select the **COM Security** tab, and then click **Edit Default** to add users with **Local Activation** permission in the **Launch and Activation Permissions** section.

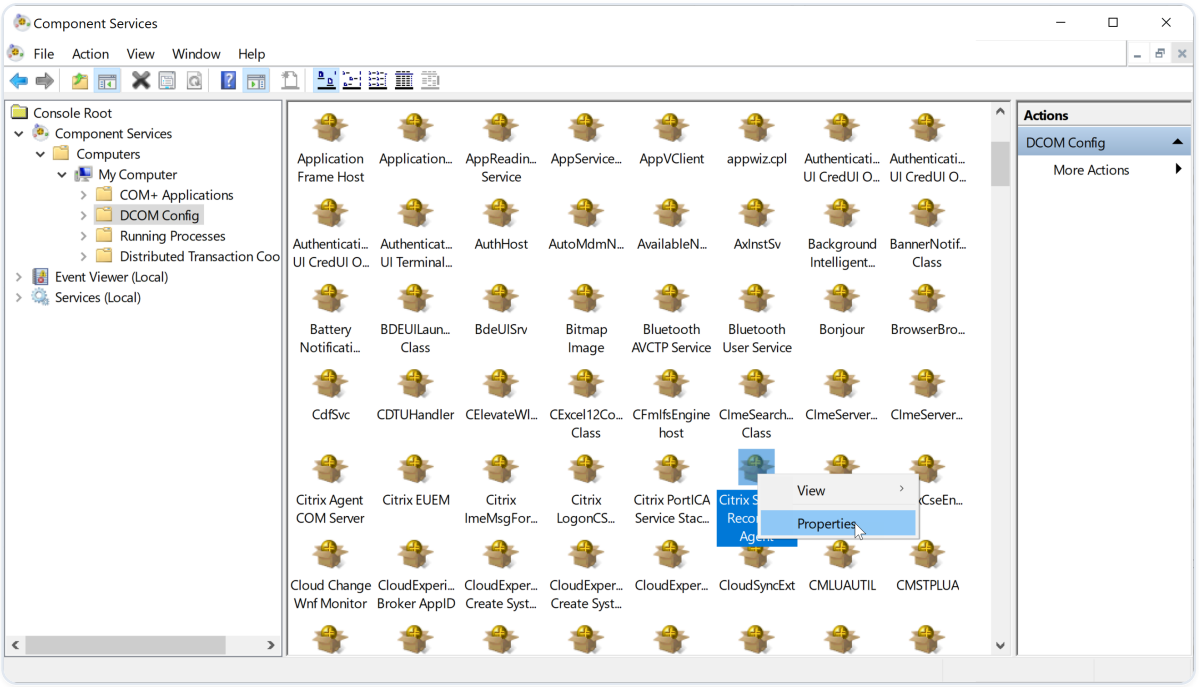

My Computer Properties
General
Options
Default Properties
Default Protocols
COM Security
MSDTC
Access Permissions
You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.
Caution: Modifying access permissions can affect 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



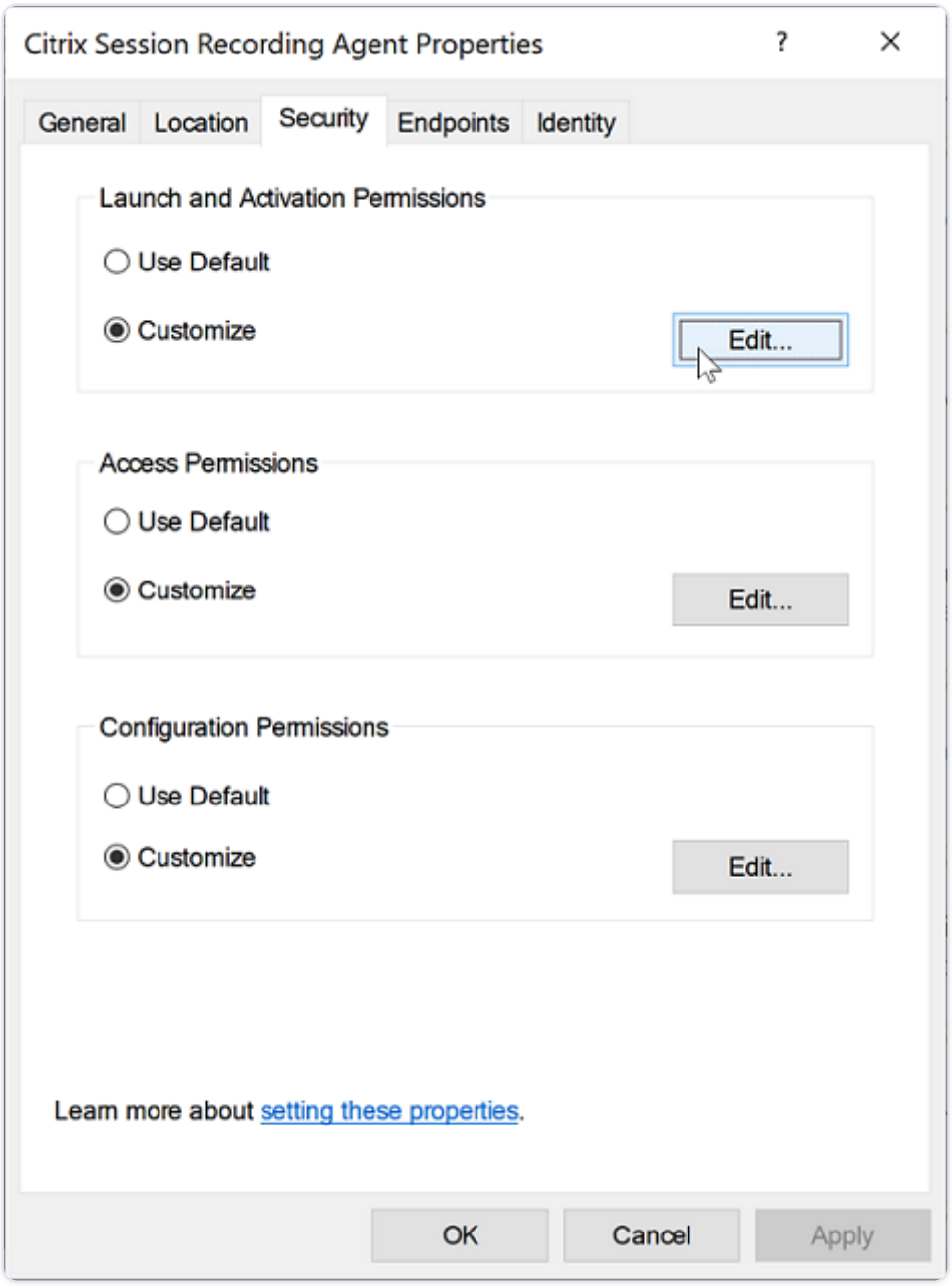
c. Select **Console Root > Component Services > Computers > My Computer > DCOM Config** from the left navigation.

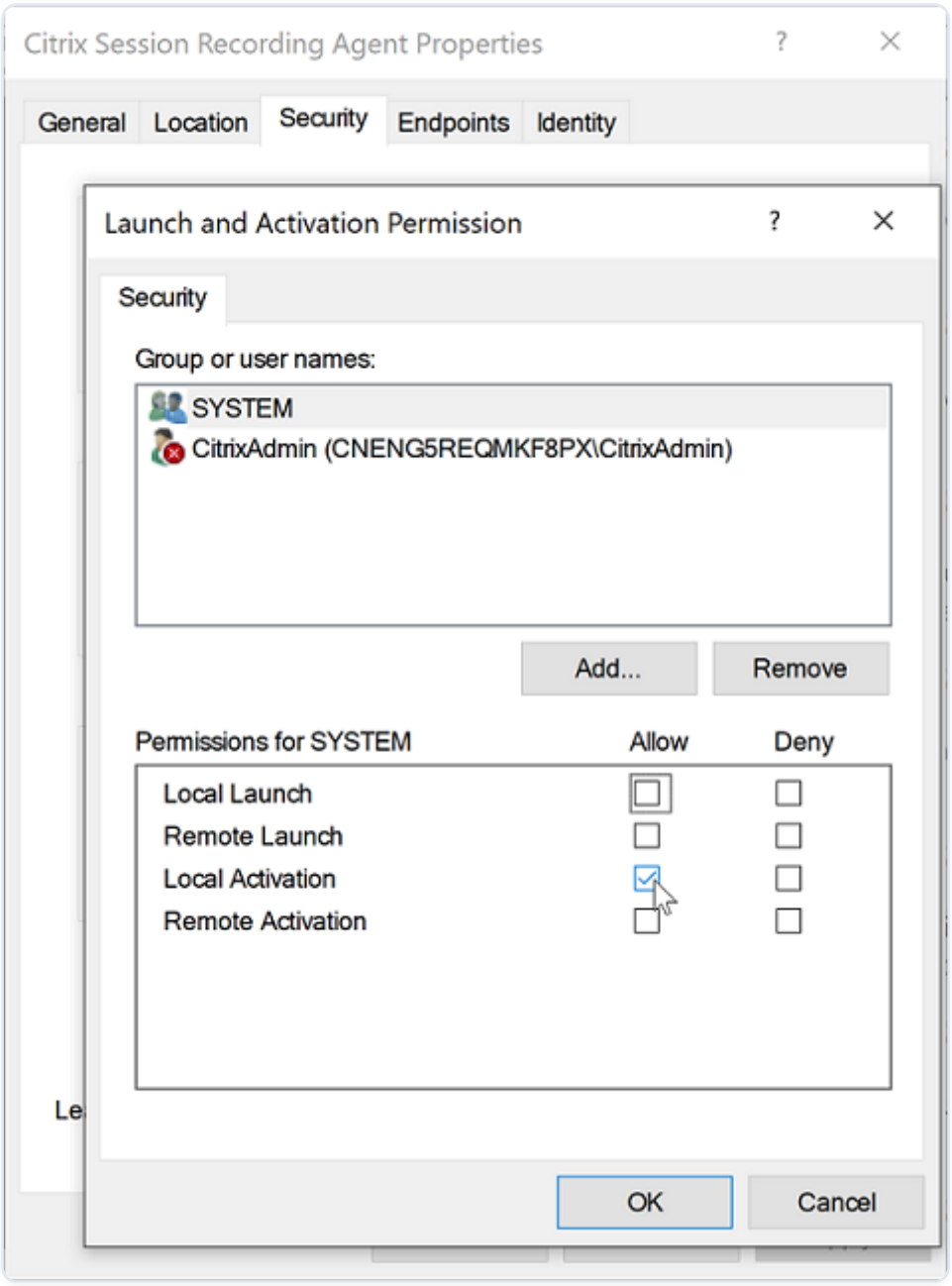


Right-click **Citrix Session Recording Agent** and choose **Properties**.



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

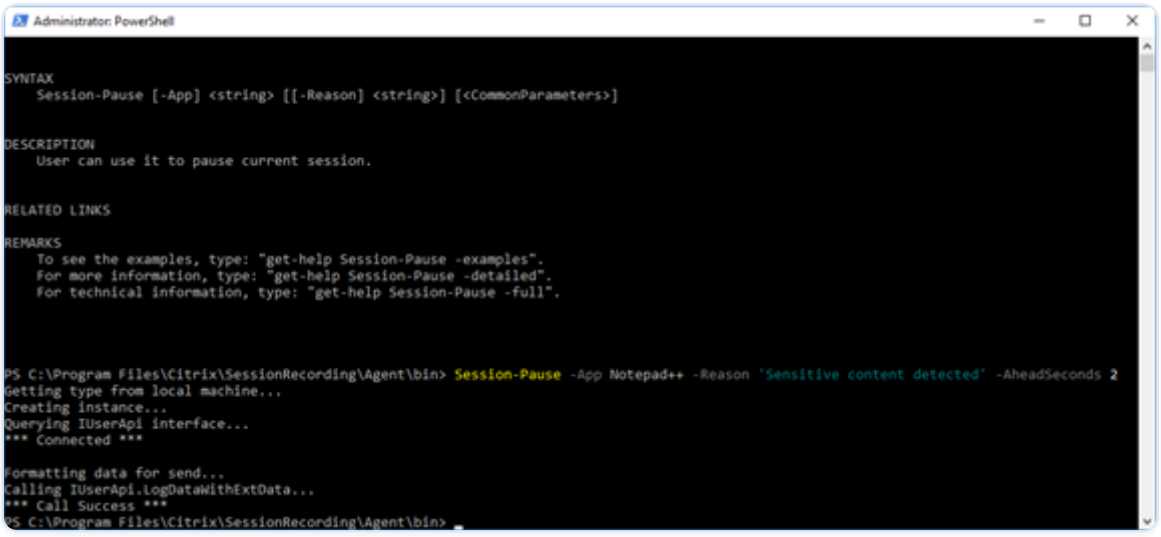


> **Note:**
>
> DCOM configuration takes effect immediately. There is no need to restart any services or the machine.

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:



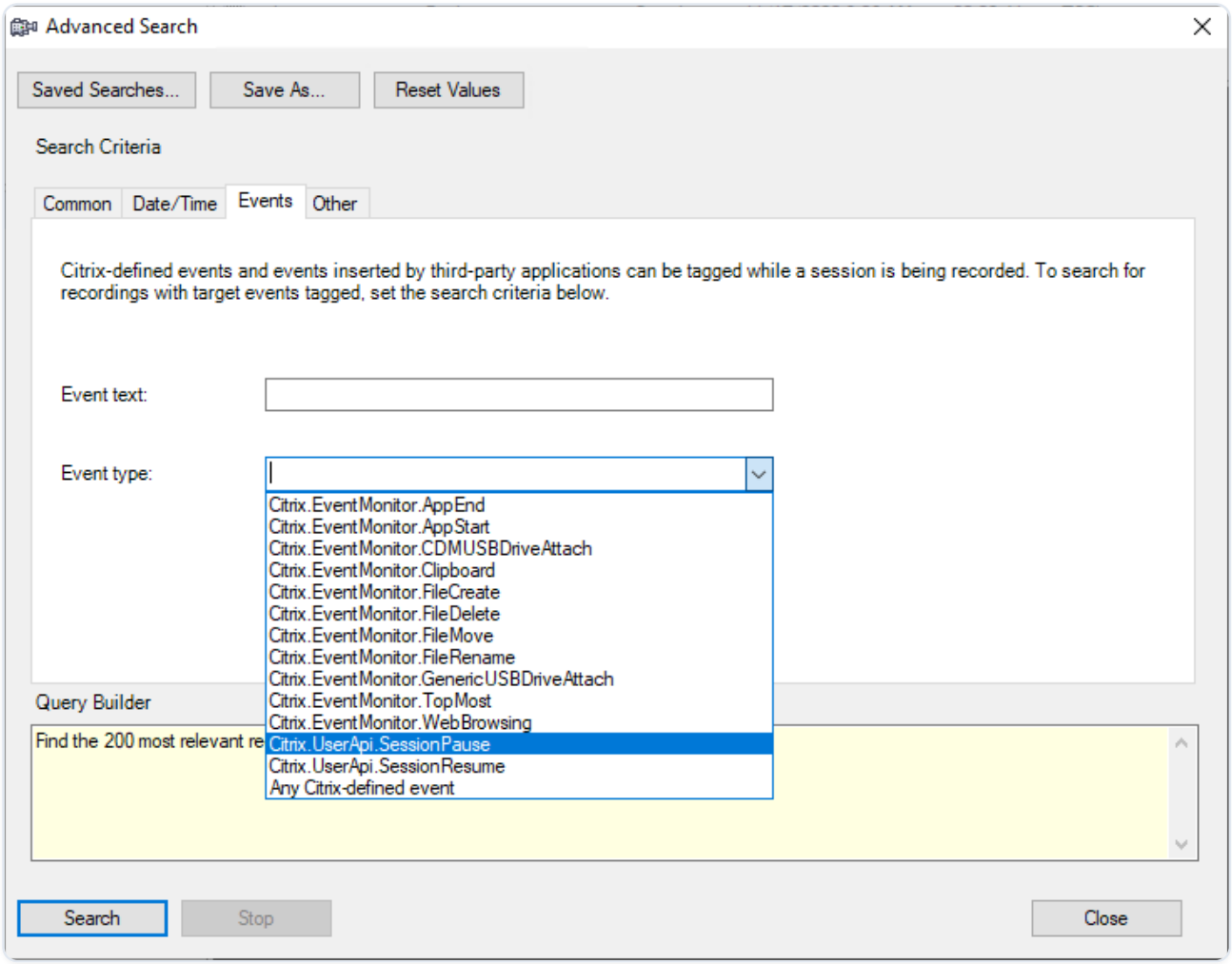
Search for and play back recordings with tagged events

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.



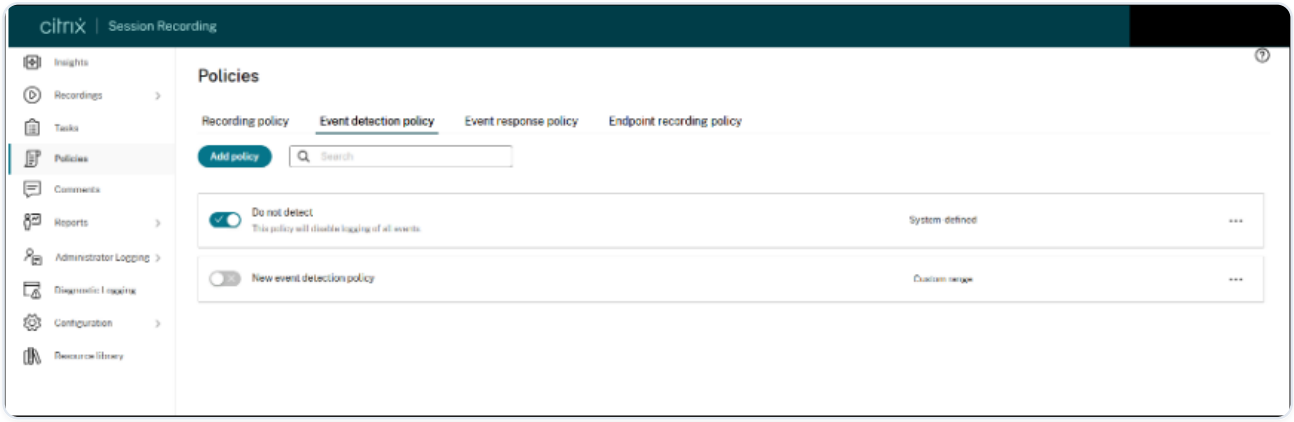
Note:

- 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.

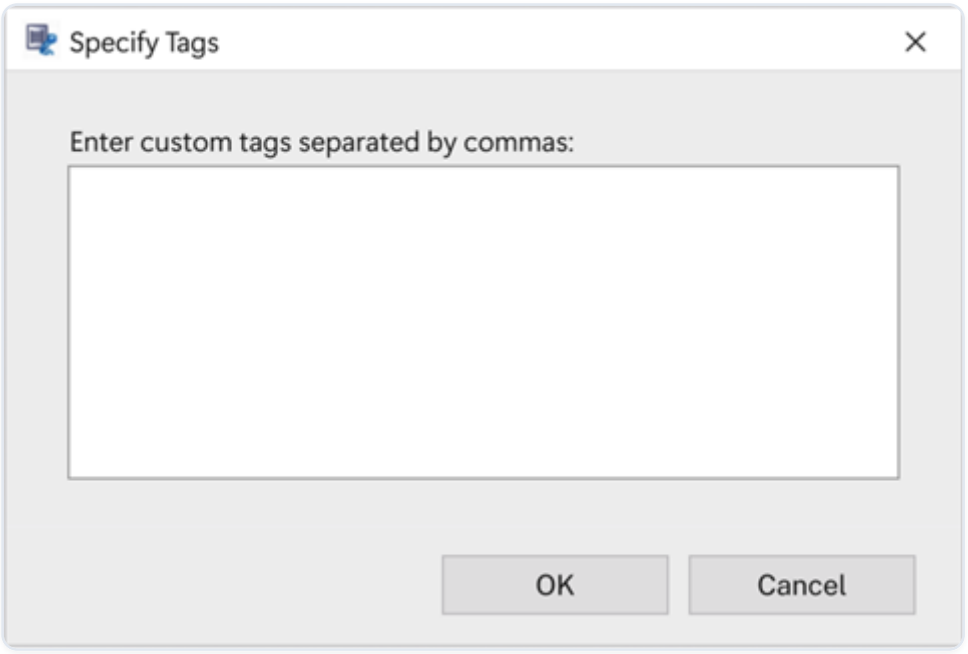
Create a custom event detection policy

Considerations

You can specify which events to log. A wizard within the Session Recording policy console helps you create rules. For each rule you create, you select the events to log and specify which sessions the rule applies to through the rule criteria settings.

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 rule applies.
- **Published Applications or Desktop**. Creates a list of published applications or desktops to which the rule applies.
- **Delivery Groups or Machines**. Creates a list of Delivery Groups or machines to which the rule applies.
- **IP Address or IP Range**. Creates a list of IP addresses or ranges of IP addresses to which the rule applies. The IP addresses mentioned here are the IP addresses of the Citrix Workspace apps.
- **Filter**. Creates a list of smart access tags to which the rule applies. You can configure contextual access (smart access) using smart access policies on Citrix NetScaler.



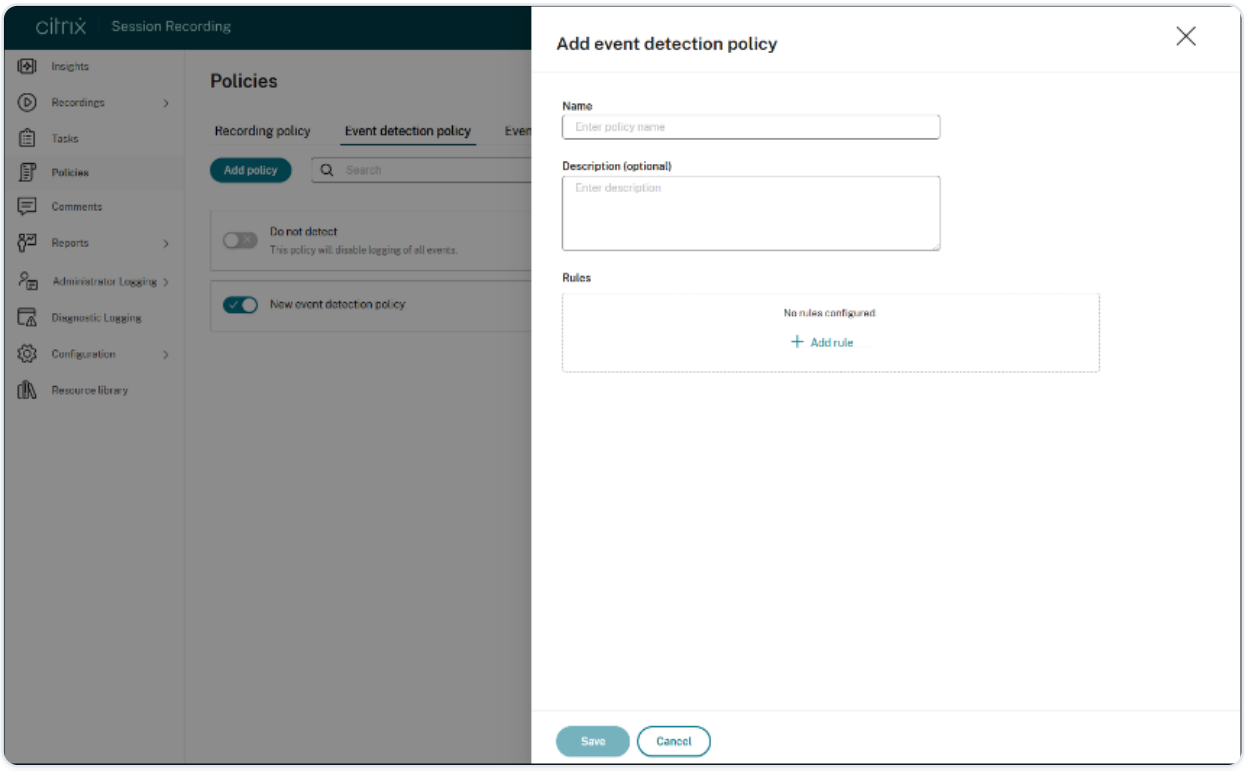
Contextual access (smart access) is available for Session Recording 2402 and later. It lets you apply policies based on the user access context including:

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

Steps

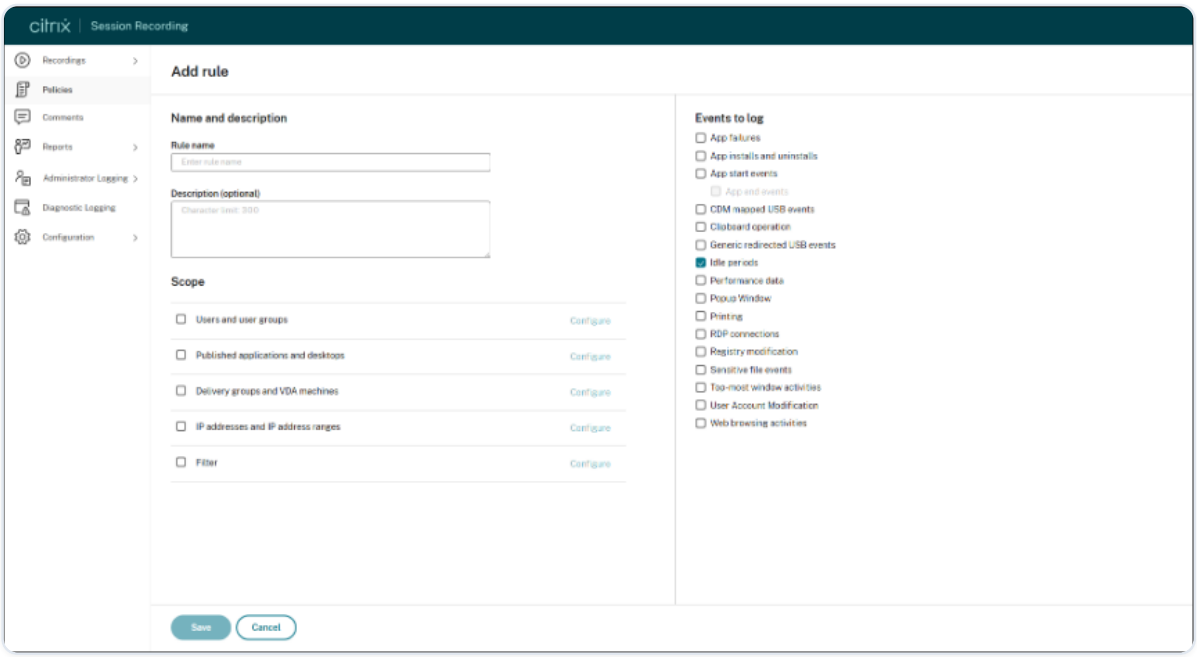
To create a custom event detection policy:

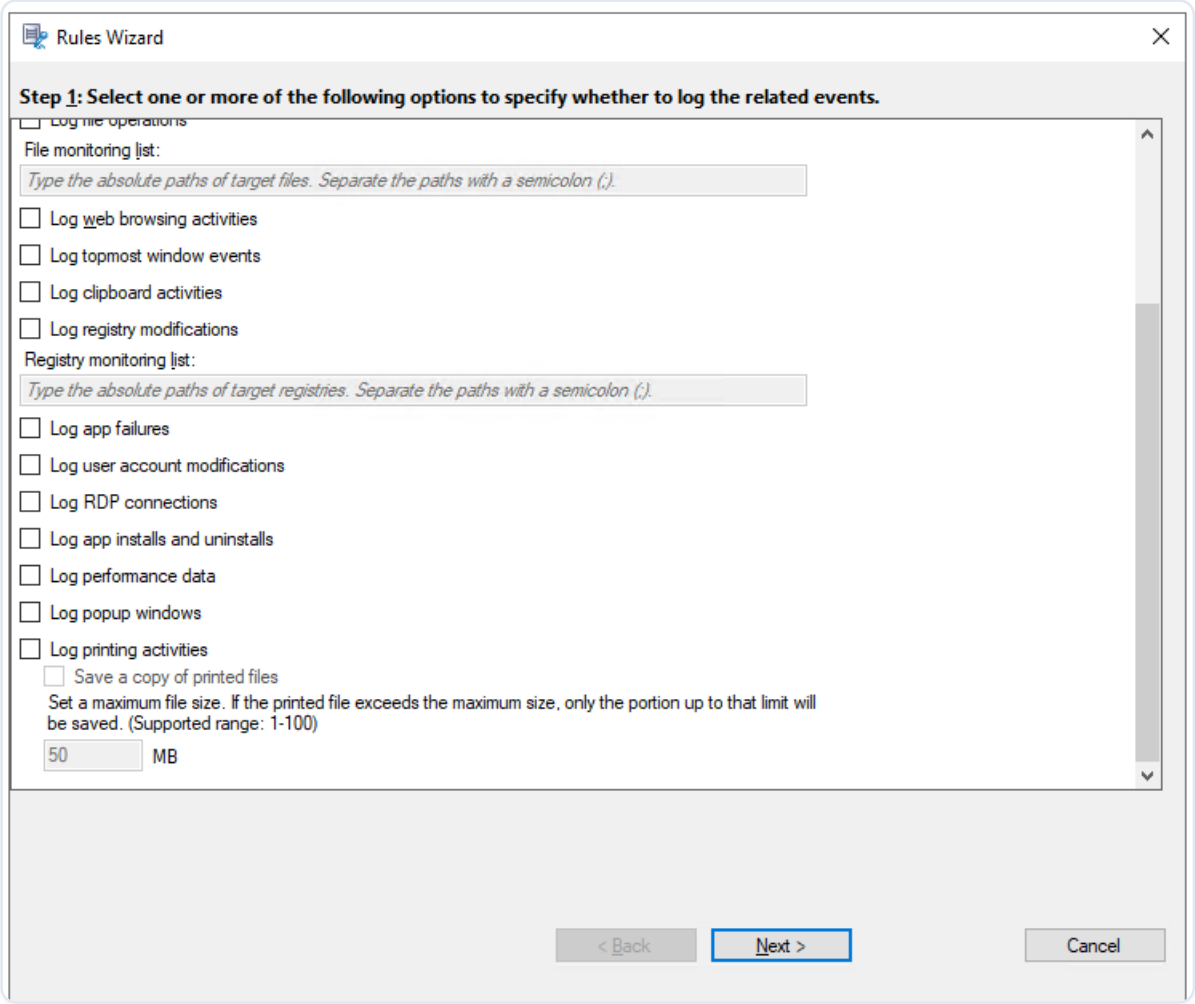
1. Log on as an authorized Policy Administrator to the server where the Session Recording policy console is installed.
2. Start the Session Recording policy console. By default, there is no active event detection policy.
3. Select **Event Detection Policies** in the left pane. From the menu bar, choose **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.





- **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.

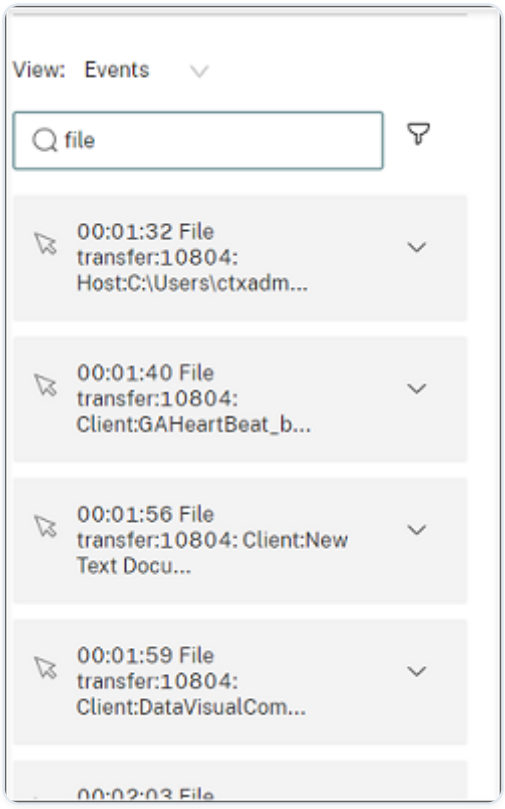
> **Note:**
>
> The **Log app end events** check box is grayed out before you select **Log app start events**.

- **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.

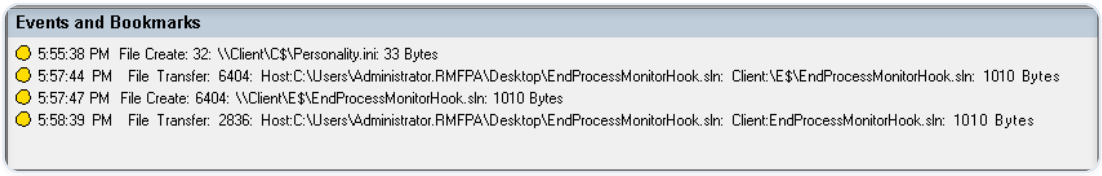
Note:

- 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.

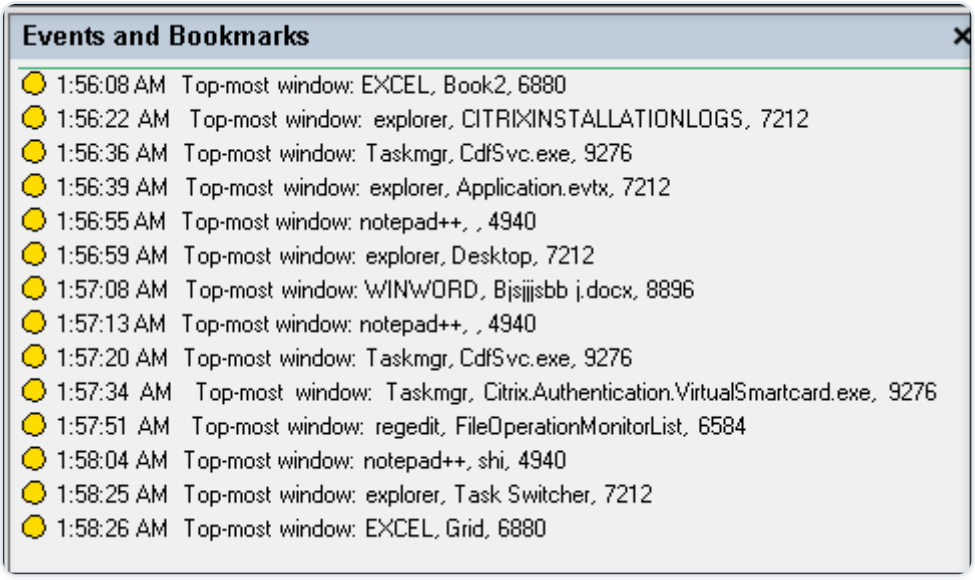
- **Log web browsing activities**: Logs user activities on supported browsers and tags the browser name, URL, and page title in the recording.



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.
- **Log printing activities**: Logs printing activities that occur during recorded sessions. Session Recording captures details about printed content, including file name, file size, author, printer name, timestamp, and more. You can choose to save a copy of the printed files along with the recordings for future reference and auditing. This feature allows for greater oversight and auditing of printing activity within recorded sessions.

b. Select and edit the rule criteria.

Similar to creating a custom recording policy, you can choose one or more rule criteria:

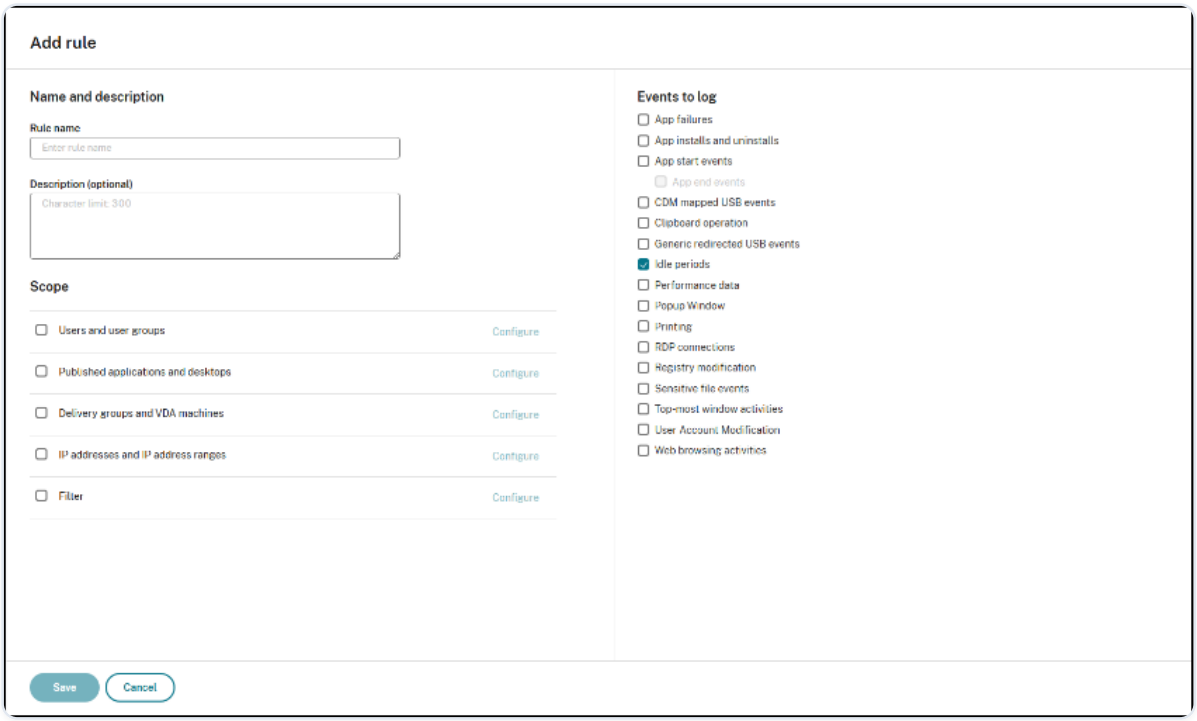
- **Users or Groups**
- **Published Applications or Desktop**
- **Delivery Groups or Machines**
- **IP Address or IP Range**
- **Filter**

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.

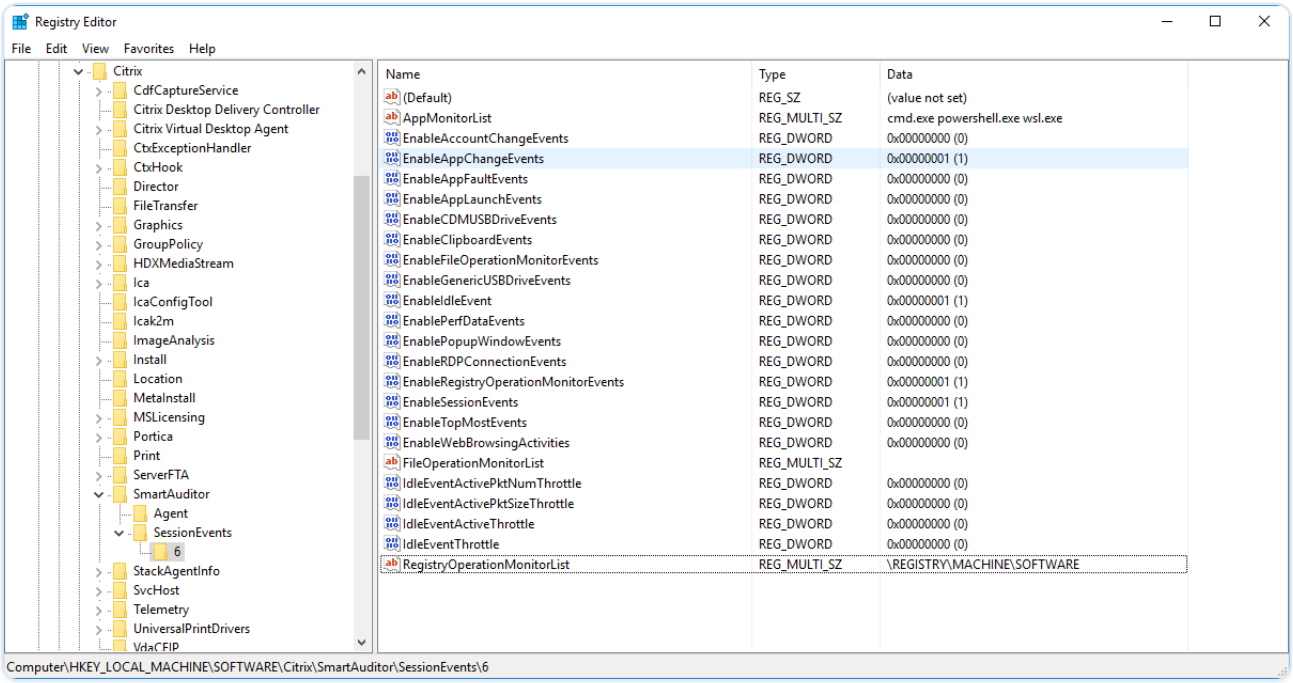
For more information, see the instructions in the Create a custom recording policy section.

> **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).
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).

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).**
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).
EnableRDPConnectionEvents	**1**: enables detecting RDP connections; **0**: disables detecting RDP connections (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).**
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).
EnablePrintingEvents	**1**: enables detecting printing activities; **0**: disables detecting printing 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 (with or without lossy screen recording enabled)
- Lock session
- Log off session
- Disconnect session

Note:

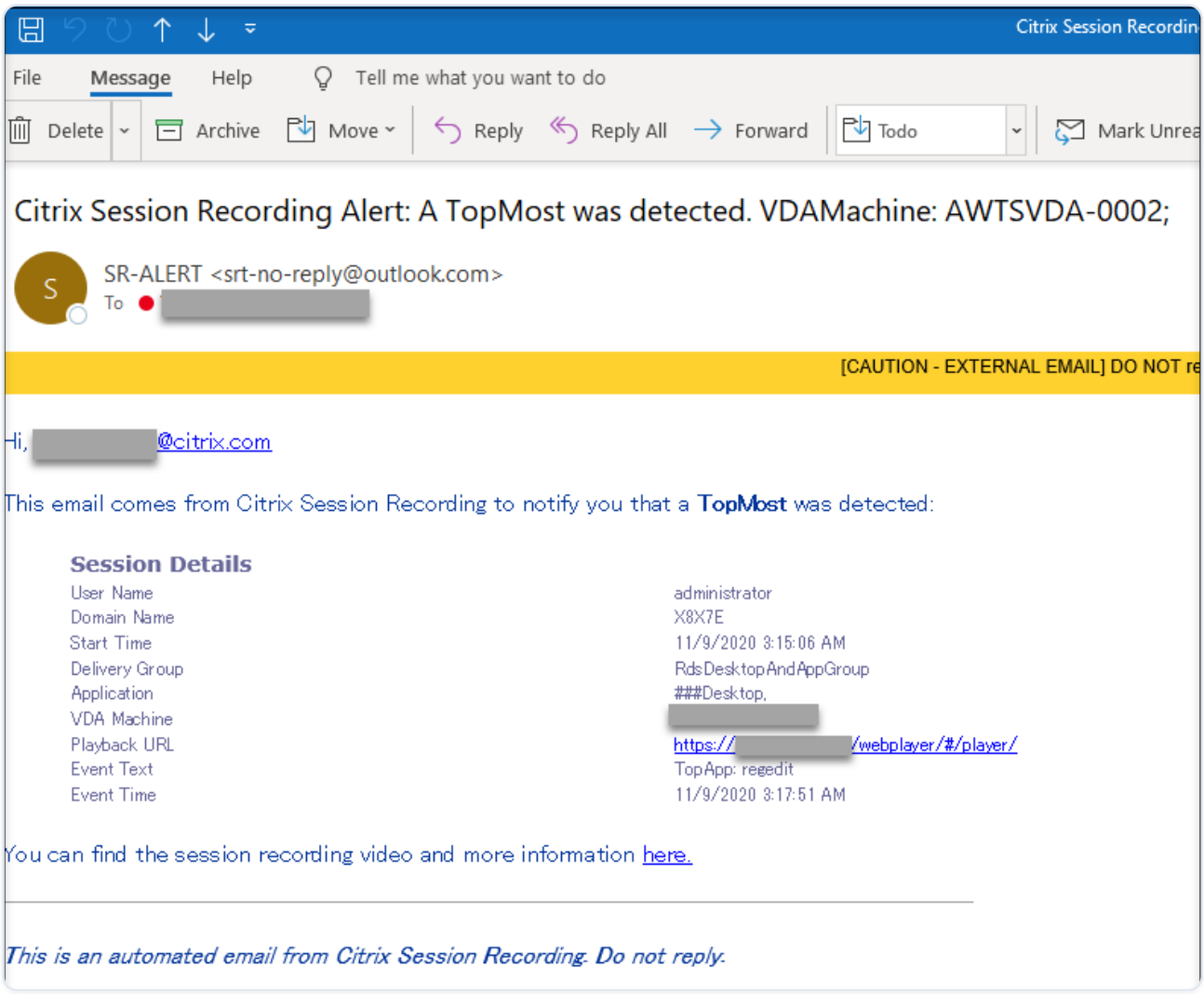
If the **Lock session** action doesn't work as expected, check the following registry keys on the VDA and ensure that there is no registry value under them or the value data is set to 0.

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System

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:



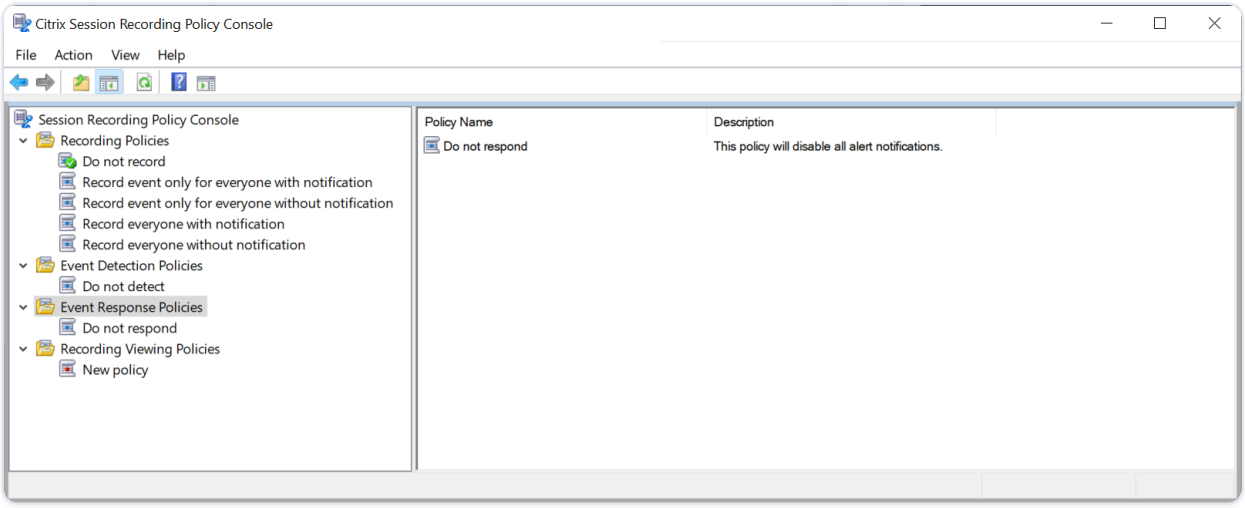
System-defined event response policy

Session Recording provides one system-defined event response policy:

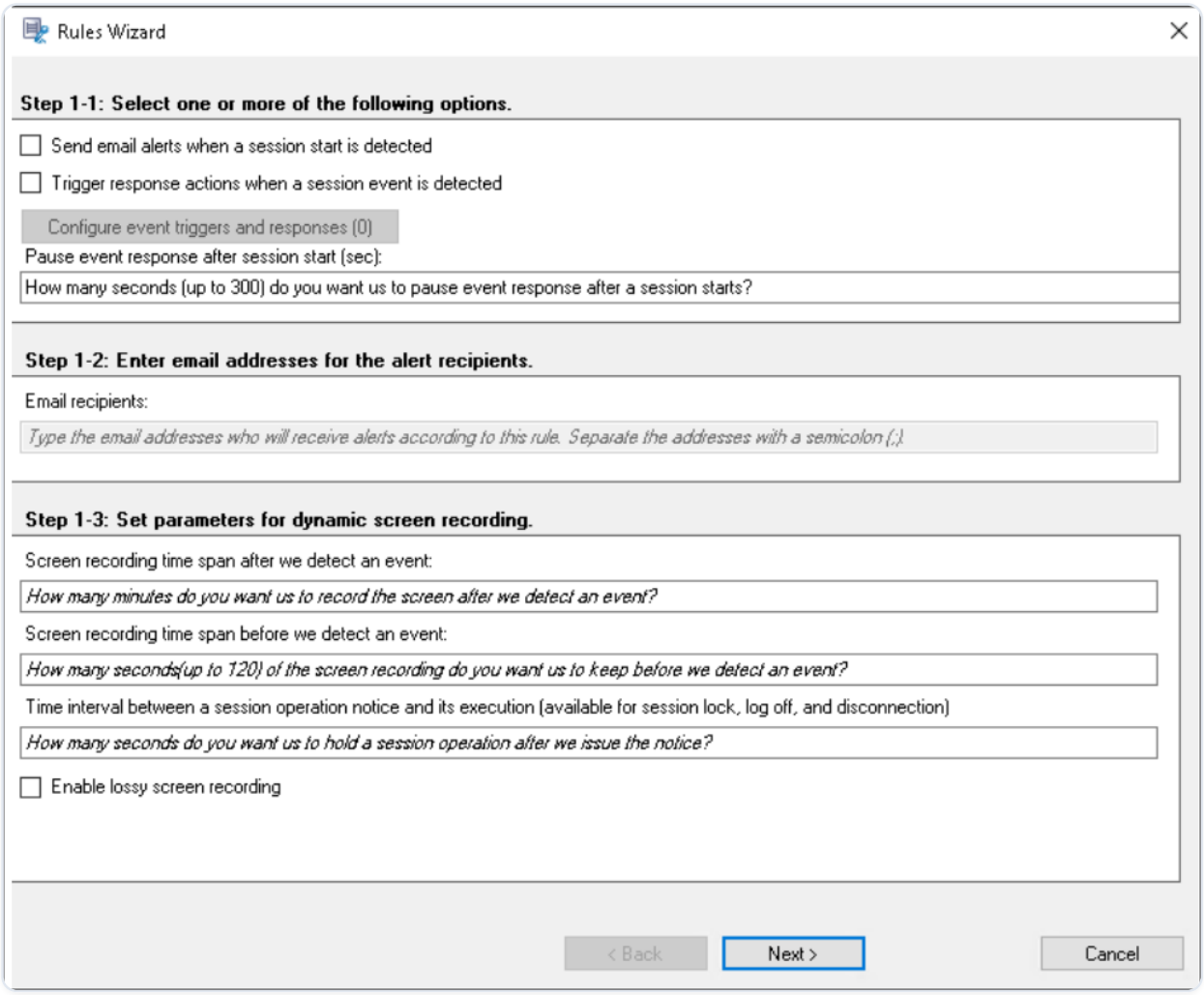
- **Do not respond**. By default, no action is taken in response to logged events in your recordings.

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.



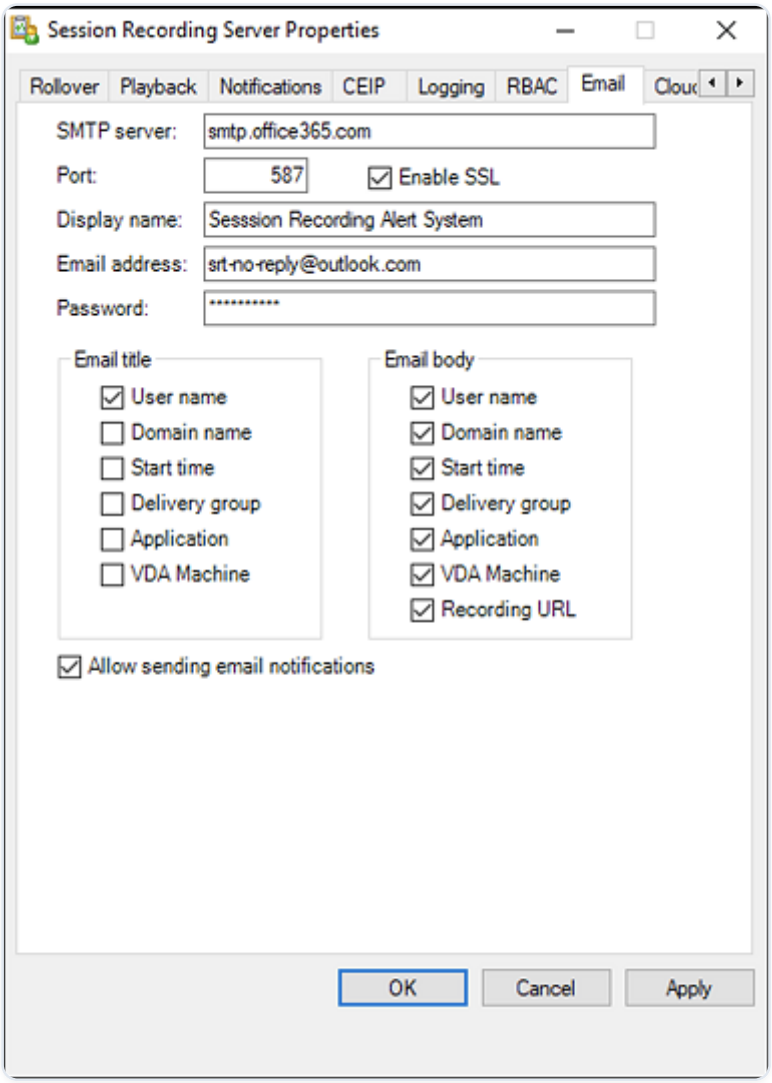
3. Select **Event Response Policies** in the left pane. From the menu bar, choose **Add New Policy**.
4. (Optional) Right-click the new event response policy and rename it.
5. Right-click the new event response policy and select **Add Rule**.
6. Select **Email alert when a session start is detected**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

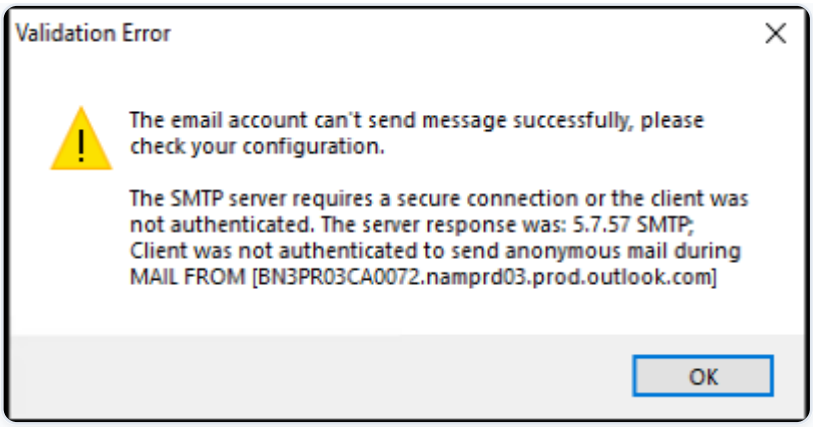
   a. Type the email addresses for the alert recipients in the **Rules** wizard.

   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 the 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.

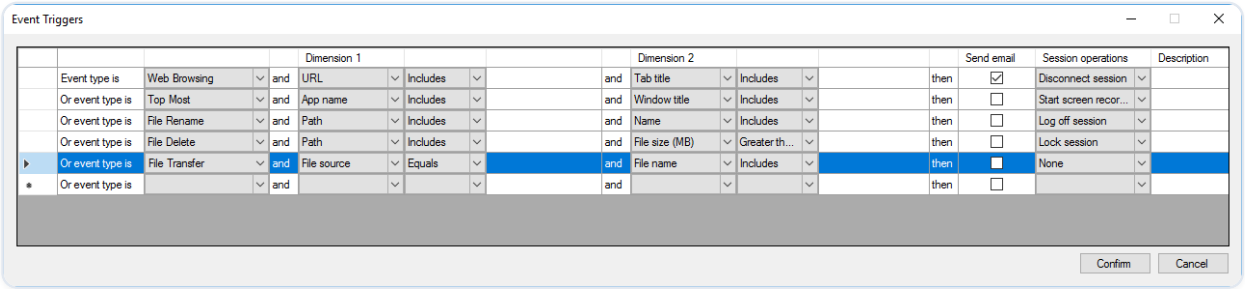
> **Note:**
>
> - Your email server might treat an email sending account as a spam bot and thus prevent it from sending emails. Before an account is allowed to send emails, an email client such as Outlook might request you to verify that the account is used by a human user.

- 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:

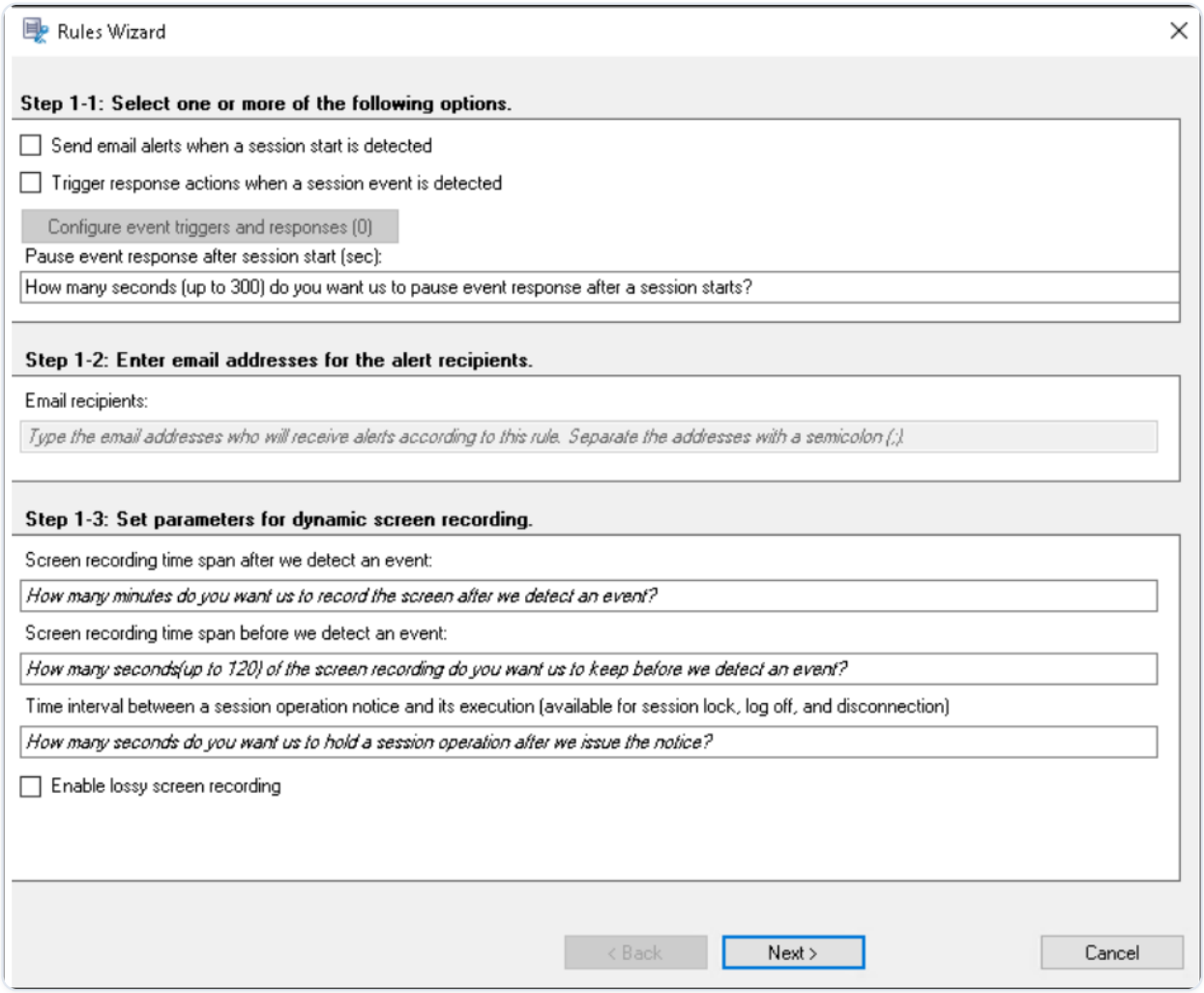
If your system language is German, French, or Spanish, ensure that the horizontal resolution of your machine is equal to or larger than 1,700 pixels. Otherwise, text truncation occurs and thus the columns of the **Event Triggers** table are not displayed completely.

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.

In the **Pause event response after session start (sec)** section, specify how many seconds (up to 300) you want to pause event response after a session starts.

You can enable lossy screen recording and set the time spans for dynamic screen recording:



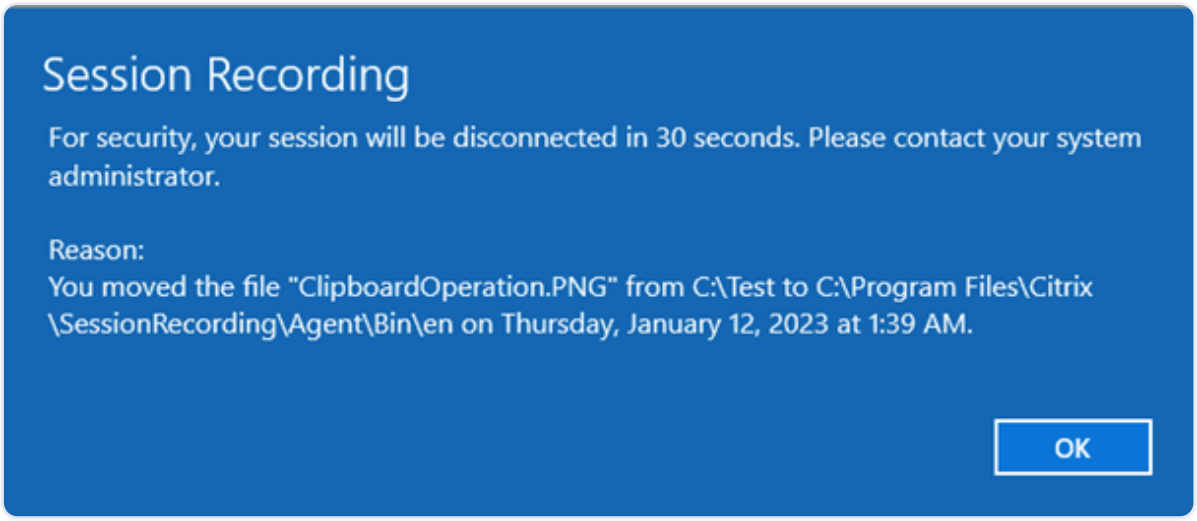
- **Screen recording time span after we detect an event**: You can configure how many minutes you want to record the screen after events are detected. If you leave the value unspecified, screen recording continues until the recorded sessions end.
- **Screen recording time span before we detect an event**: You can configure how many seconds of the screen recording you want to keep before events are detected. This feature

is available for both virtual desktop and app 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:



- **Enable Lossy screen recording**: Lossy screen recording lets you adjust compression options to reduce the size of recording files and to accelerate navigating recorded sessions during playback. For more information, see Enable or disable lossy screen recording.

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

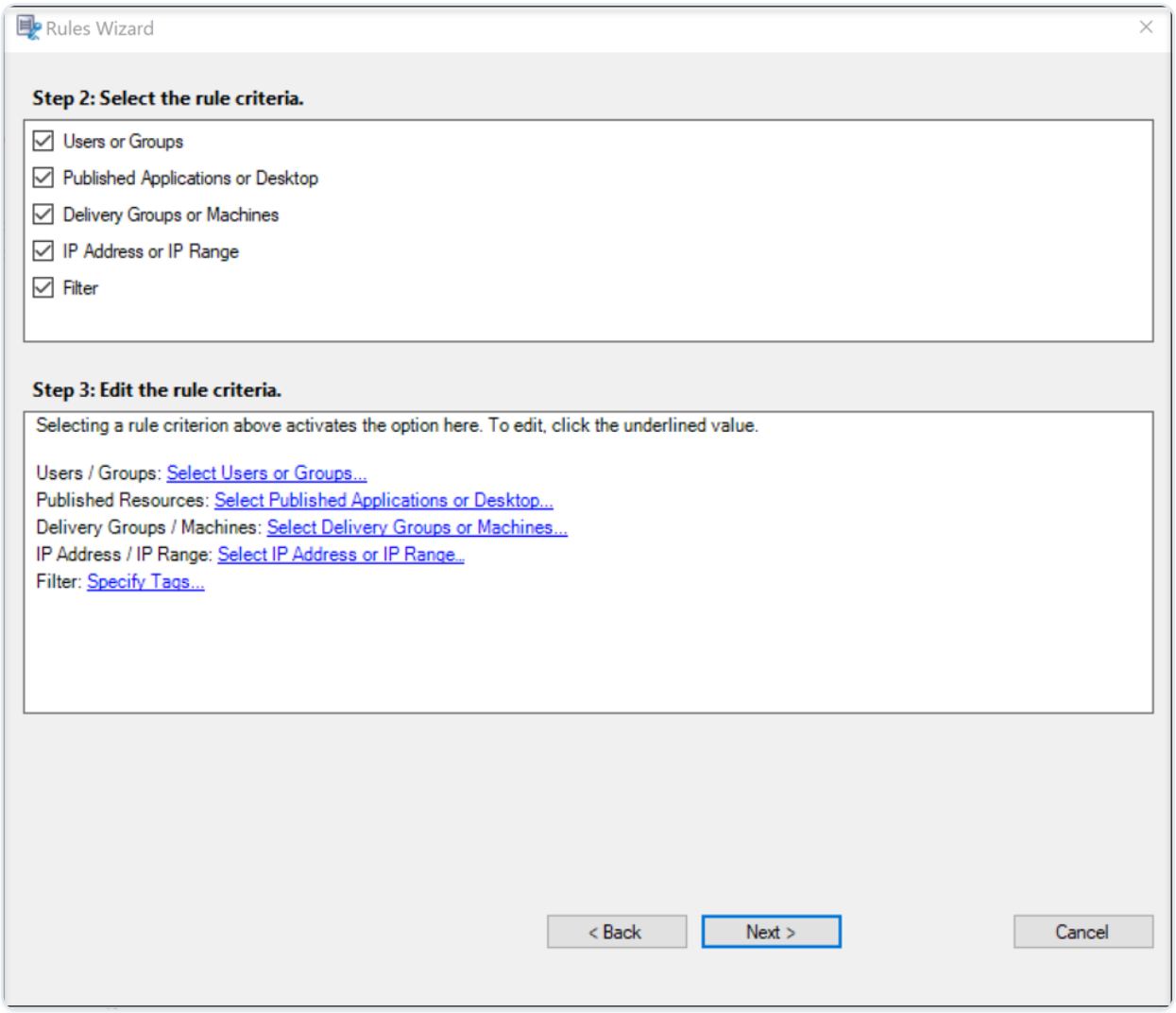
EVENT TYPE	DIMENSION	OPTION
App Start		
	App name	Includes, Equals, Matches
	Full command line	Includes, Equals, Matches
App End		
	App name	Includes, Equals, Matches
Top Most		
	App name	Includes, Equals, Matches
	Windows title	Includes, Equals, Matches
Web Browsing		
	URL	Includes, Equals, Matches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

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

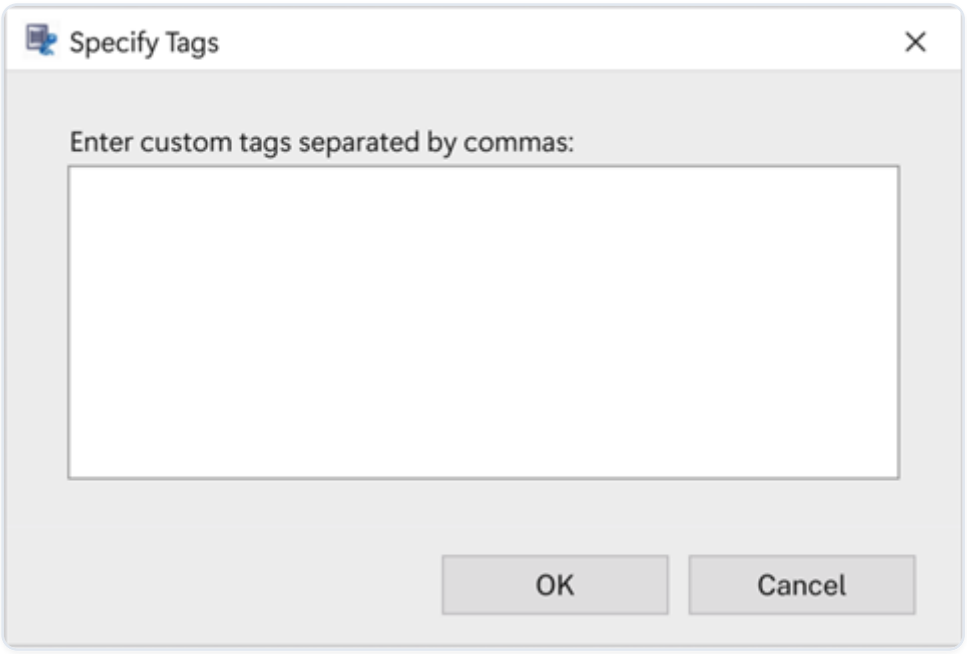
EVENT TYPE	DIMENSION	OPTION
	Value name	Includes, Equals, Matches
Registry Delete Value		
	Key name	Includes, Equals, Matches
	Value name	Includes, Equals, Matches
Registry Rename		
	Key name	Includes, Equals, Matches
User Account Modification		
	User name	Includes, Equals, Matches
Unexpected App Exit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

EVENT TYPE	DIMENSION	OPTION
Performance Data		
	CPU usage (%)	Greater than
	Memory usage (%)	Greater than
	Net send (MB)	Greater than
	Net receive (MB)	Greater than
	RTT (ms)	Greater than
Clipboard Operation		
	Data type	Equals (Text, File, Bitmap)
	Process name	Includes, Equals, Matches
	Content	Includes, Equals, Matches

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



- **Users or Groups**. Creates a list of users or groups to which the rule applies.
- **Published Applications or Desktop**. Creates a list of published applications or desktops to which the rule applies.
- **Delivery Groups or Machines**. Creates a list of Delivery Groups or machines to which the rule applies.
- **IP Address or IP Range**. Creates a list of IP addresses or ranges of IP addresses to which the rule applies. The IP addresses mentioned here are the IP addresses of the Citrix Workspace™ apps.
- **Filter**. Creates a list of smart access tags to which the rule applies. You can configure contextual access (smart access) using smart access policies on Citrix NetScaler.



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

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

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

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

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

Policies (web console)

The Session Recording web console provides a browser-based interface for creating and managing policies. The URL of the web console for policy configuration is `https:// <FQDN of Session Recording server>/SRWebConsole/#/policies`

The following policy types are available:

- Session recording policies specify which VDA sessions are recorded.
- Event detection policies specify which events are logged within recorded sessions.
- Event response policies specify actions to trigger automatically in response to detected events.
- Endpoint recording policies specify which endpoint sessions are recorded.

For more information, see:

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

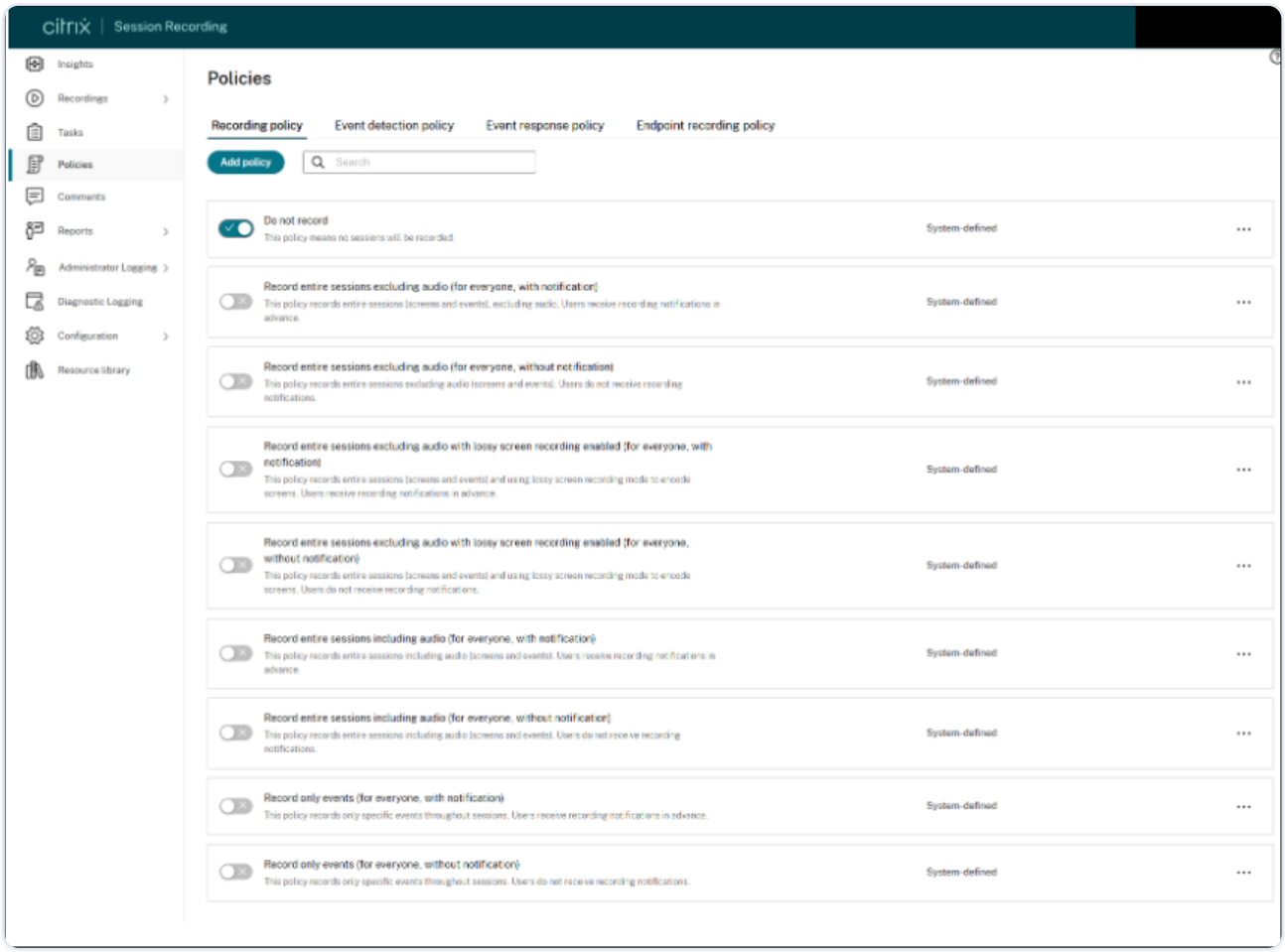
Configure session recording policies

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 entire sessions excluding audio (for everyone, with notification)**. This policy records entire sessions (including screens and events but excluding audio). Users receive recording notifications in advance.
- **Record entire sessions excluding audio (for everyone, without notification)**. This policy records entire sessions (including screens and events but excluding audio). Users do not receive recording notifications.
- **Record entire sessions excluding audio with lossy screen recording enabled (for everyone, with notification)**. This policy records entire sessions (including screens and events but excluding audio). Lossy screen recording is enabled to reduce the size of recording files. Users receive recording notifications in advance.
- **Record entire sessions excluding audio with lossy screen recording enabled (for everyone, without notification)**. This policy records entire sessions (including screens and events but excluding audio). Lossy screen recording is enabled to reduce the size of recording files. Users do not receive recording notifications.

- **Record entire sessions including audio (for everyone, with notification)**. This policy records entire sessions (including screens, events, and audio). Users receive recording notifications in advance. You can now enable audio recording for non-optimized HDX audio. The audio that is handled on the VDA and delivered to/from the client where the Citrix Workspace app is installed is referred to as non-optimized HDX audio. Unlike non-optimized HDX audio, optimized HDX audio has its processing offloaded to the client, as seen in the Browser Content Redirection (BCR) and Optimization for Microsoft Teams scenarios.
- **Record entire sessions including audio (for everyone, without notification)**. This policy records entire sessions (including screens, events, and audio). Users do not receive recording notifications.
- **Record only events (for everyone, with notification)**. This policy records only events that your event detection policy specifies. It does not record screens or audio. Users receive recording notifications in advance.
- **Record only events (for everyone, without notification)**. This policy records only events that your event detection policy specifies. It does not record screens or audio. Users do not receive recording notifications.

> **Note:**
>
> When upgrading Citrix Session Recording from version 1912 , existing policy names are retained (e.g., Record everyone with notification, Record everyone without notification).
>
> However, fresh installations use updated policy names.
>
> This is expected behavior and does not affect policy functionality.
>
> You can't modify or delete the system-defined recording policies.

Create a custom recording policy

Considerations

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

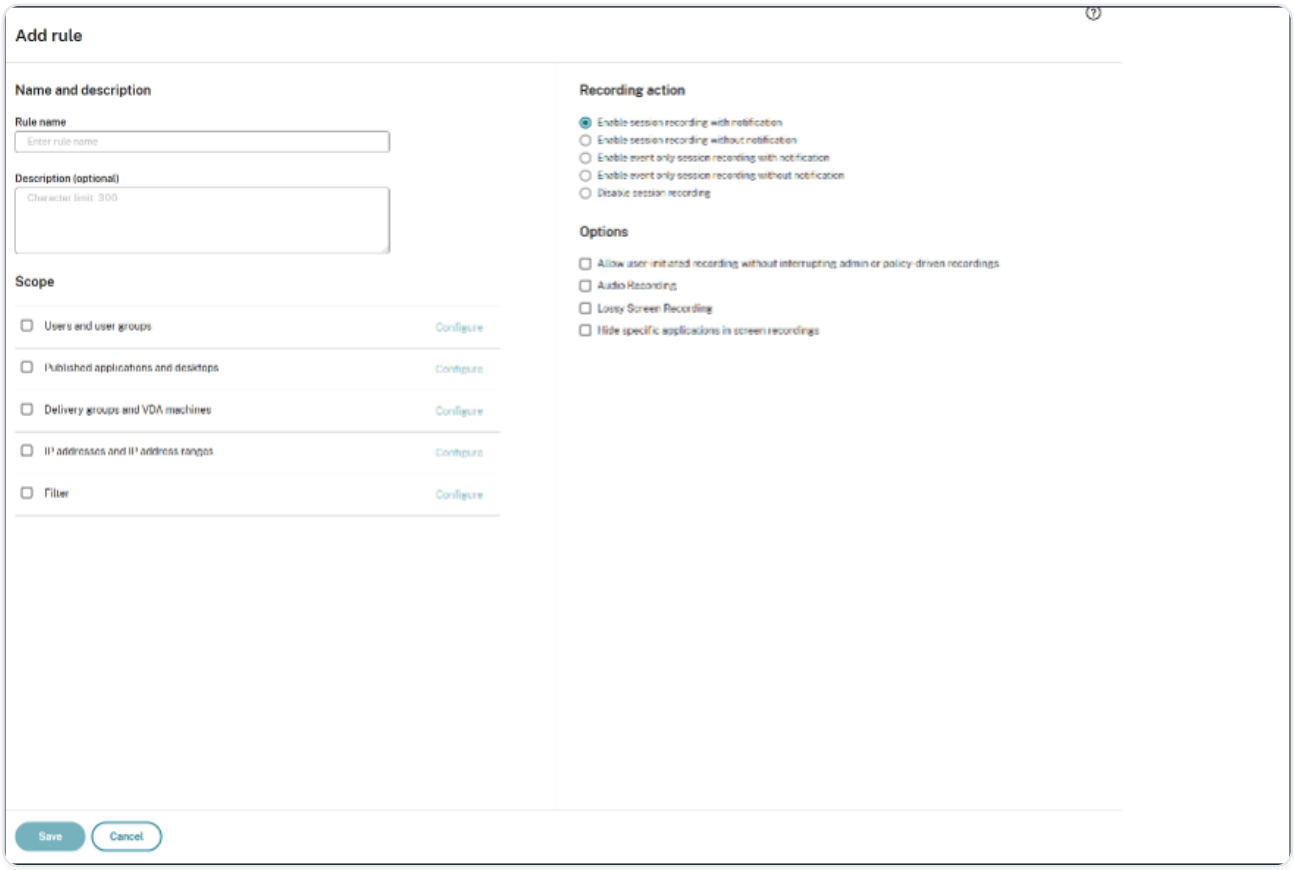
permission as a site administrator. Configure the administrator **read** permission on the Delivery Controller™ of the site.

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

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

A wizard within the Session Recording policy console helps you create rules. 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:

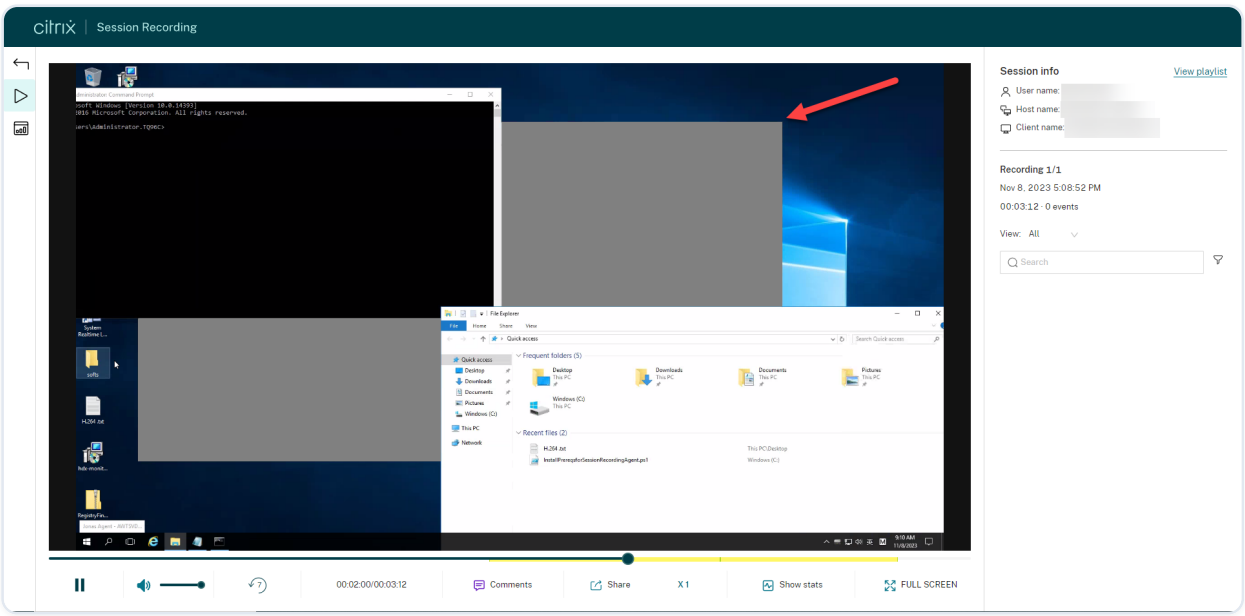


- **Enable session recording with notification**. This option records entire sessions (screens and events). Users receive recording notifications in advance. With this option selected, you can

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

- **Enable session recording without notification**. This option records entire sessions (screens and events). Users do not receive recording notifications. With this option selected, you can further select to enable audio recording or lossy screen recording. Additionally, you can choose to hide specific applications in screen recordings.
- **Enable event only session recording with notification**. Recording only specific events helps to free up storage space. This option records throughout sessions only events that your event detection policy specifies. It does not record screens. Users receive recording notifications in advance.
- **Enable event only session recording without notification**. Recording only specific events helps to free up storage space. This option records throughout sessions only events that your event detection policy specifies. It does not record screens. Users do not receive recording notifications.
- **Disable session recording**. This option means that no sessions are recorded.
- **Hide specific applications during screen recording**. This feature lets you hide specific applications with a layer mask during screen recording. The color for the layer mask is configurable, which can be Black, Gray, or White.

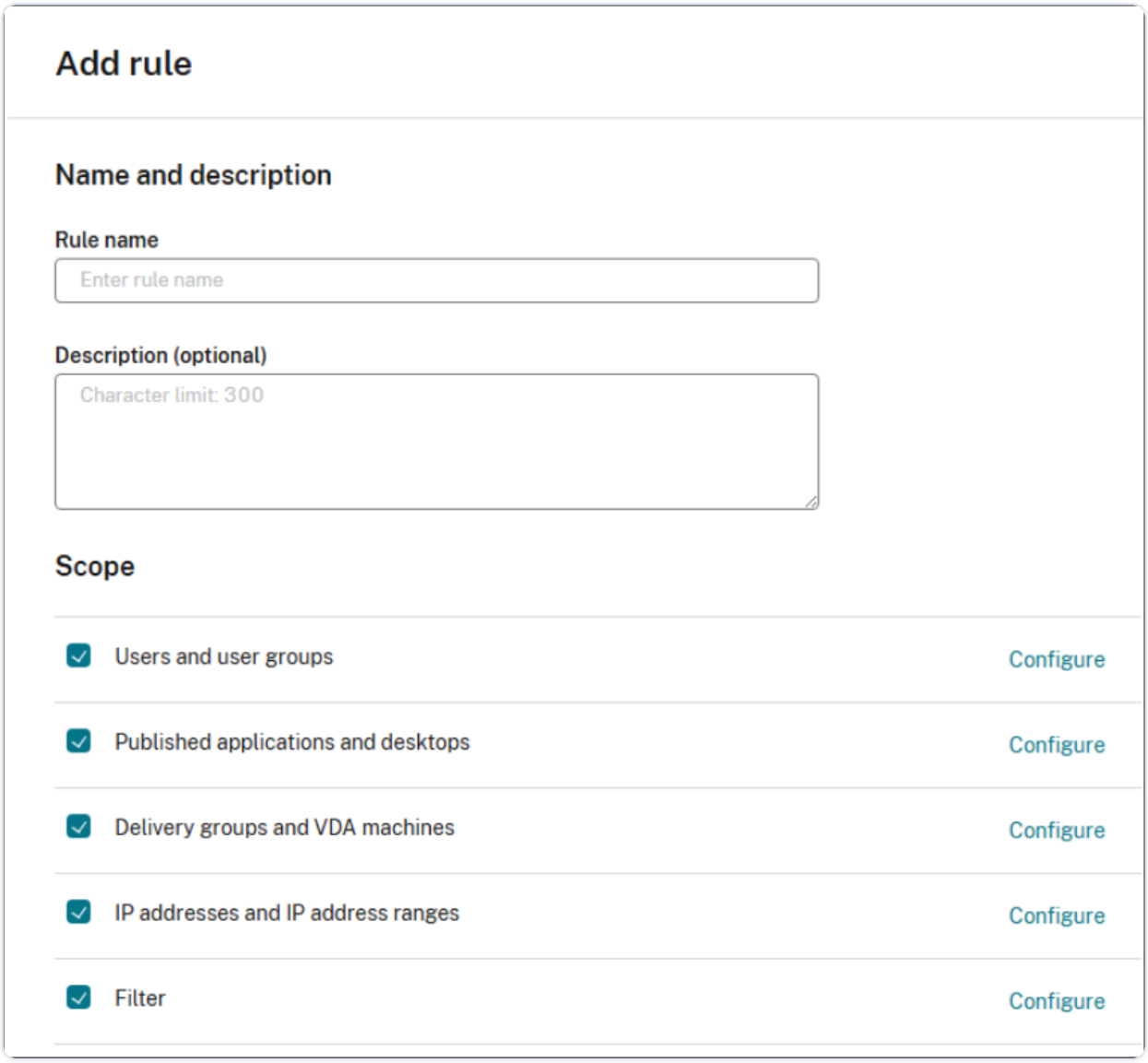
  For example, you can see that an application is hidden during the recording playback:



- **Allow user-initiated recording without interrupting admin or policy-driven recordings**. This feature lets end users start and stop recordings on demand. Administratorinitiated and

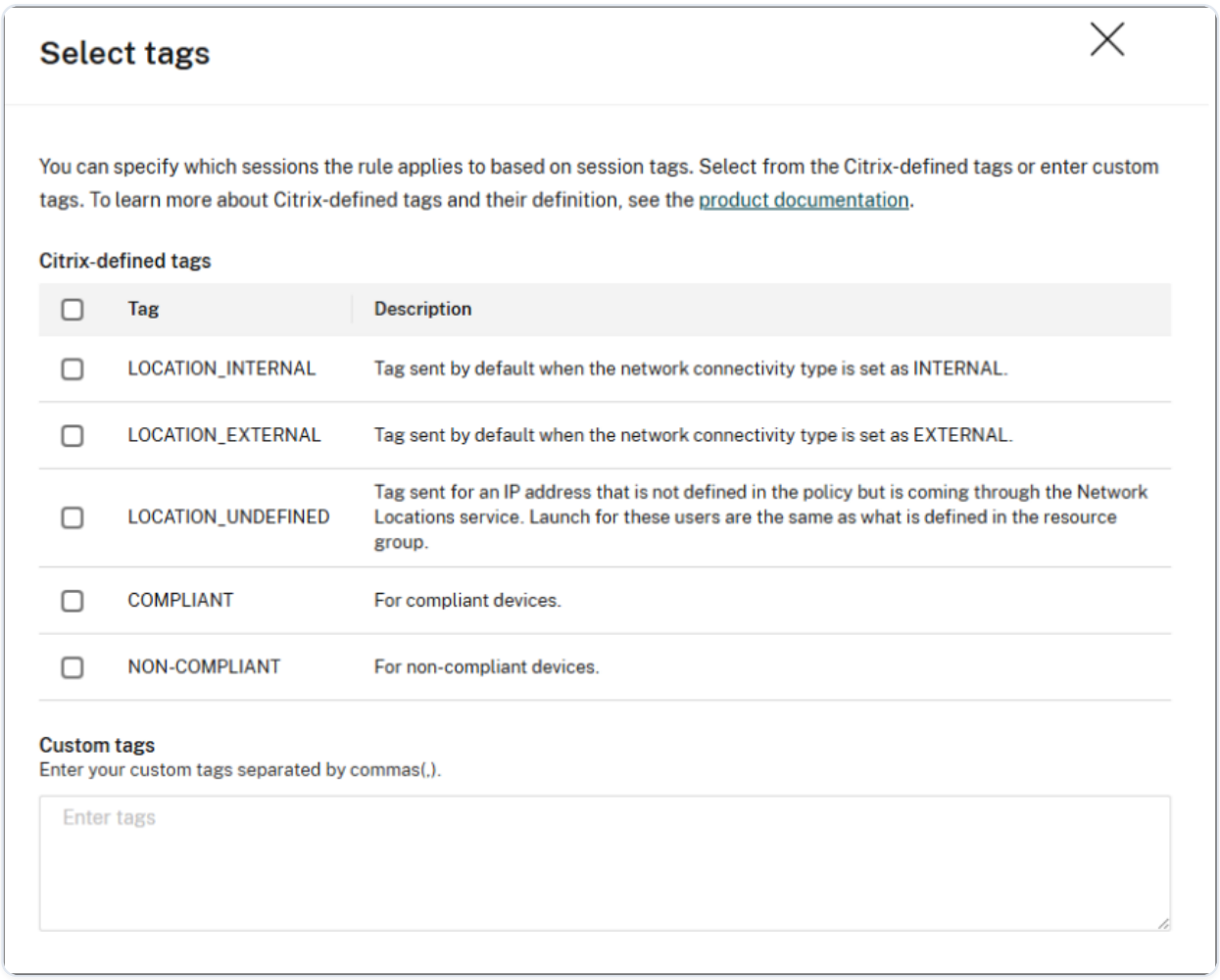
policydriven recordings take precedence and are not interrupted by enduser triggered recordings.

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



- **Users and user 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 and desktops**. 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 and VDA 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 and IP address ranges**. 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.
- **Filter**. Creates a list of smart access tags to which the action of the rule applies. You can configure contextual access (smart access) using smart access policies on Citrix NetScaler.



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 **Disable session recording** action have the highest priority.
- Rules with the **Enable session recording with notification** action have the second-to-highest priority.
- Rules with the **Enable session recording without notification** action have the second-to-lowest priority.
- Rules with the **Enable event only session recording with notification** action have the medium priority.
- Rules with the **Enable event only session recording without notification** action have the lowest priority.

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

Steps

To create a custom recording policy:

1. Log on as an authorized Policy Administrator to the Session Recording web console.
2. Select **Policies** from the left pane. The **Recording policy** tab is displayed by default.
3. Click **Add Policy**.
4. Enter a **name and description** for the new policy, and then click **Add rule**.
5. Enter a name and description for the rule. Specify a recording action and choose at least one of the following items to create the rule scope.

   For each rule, specify a recording action:

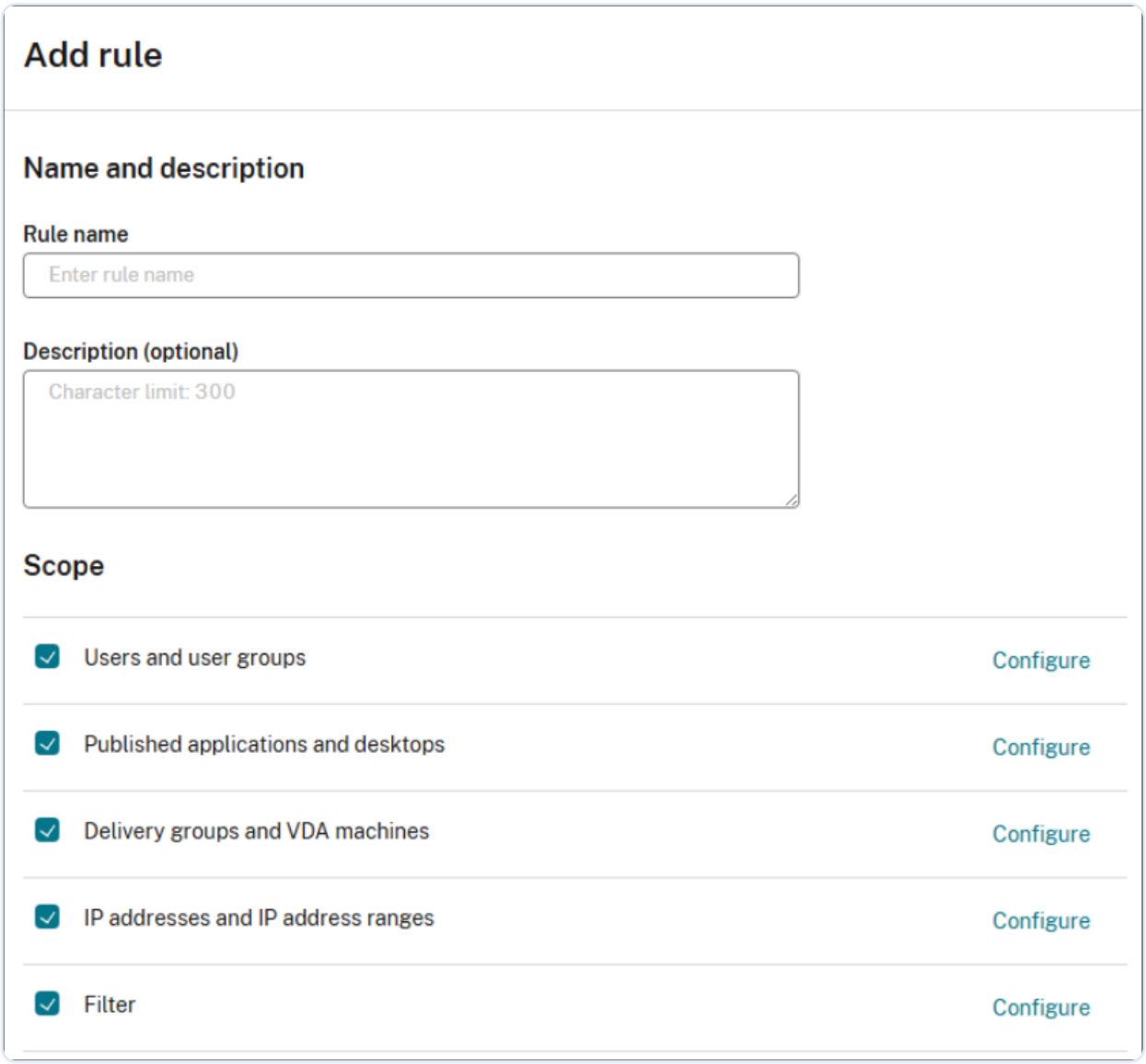
   - Enable session recording with notification
   - Enable session recording without notification
   - Enable event only session recording with notification
   - Enable event only session recording without notification
   - Disable session recording

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

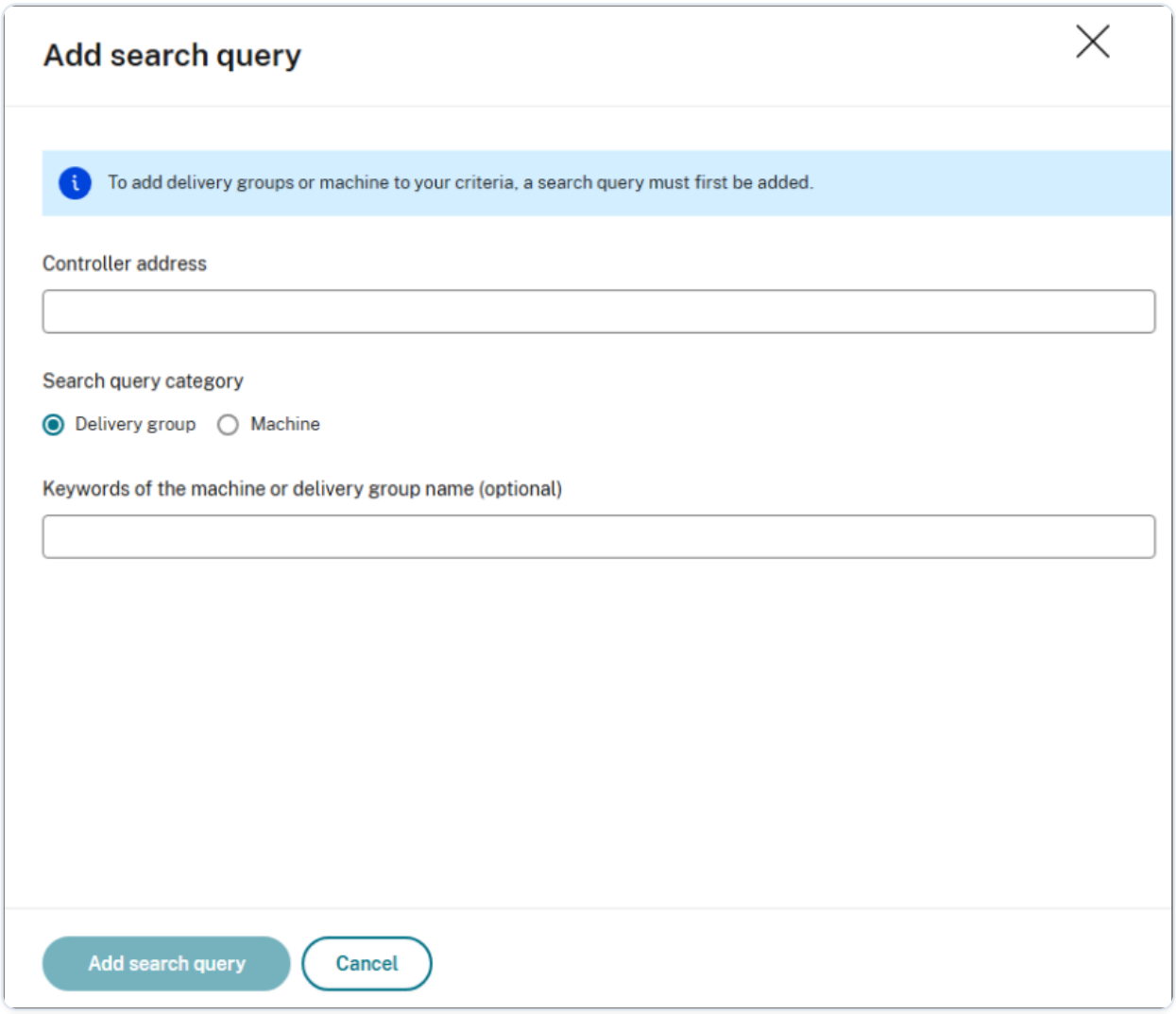
   - **Users and user groups**
   - **Published applications and desktops**
   - **Delivery groups and VDA Machines**
   - **IP Addresses and IP address ranges**
   - **Filter**

7. 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 and desktops** underlined value, the **Controller address** is the IP address, a URL, or a machine name if the Controller is on a local network. When choosing **Published applications and desktops** or **Delivery groups and VDA machines**, specify the Delivery Controller address 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 on-premises environments.



For example, when choosing **Delivery groups and VDA machines** , click the corresponding hyperlink in the preceding screenshot and click **Add search query** to add queries to the Controller.



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

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 the 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've reached the maximum size or recording duration. For more information about the rollover thresholds, see Specify file size for recordings.

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

IF THE PREVIOUS RECORDING POLICY WAS	AND THE NEW RECORDING POLICY IS	AFTER A ROLLOVER, THE RECORDING POLICY WILL BE
Do not record	Any other policy	No change. The new policy takes effect only when the user logs on to a new session.
Record without notification	Do not record	The recording stops.
Record without notification	Record with notification	Recording continues and a notification message appears.
Record with notification	Do not record	The recording stops.
Record with notification	Record without notification	Recording continues. No message appears the next time a user logs on.

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.

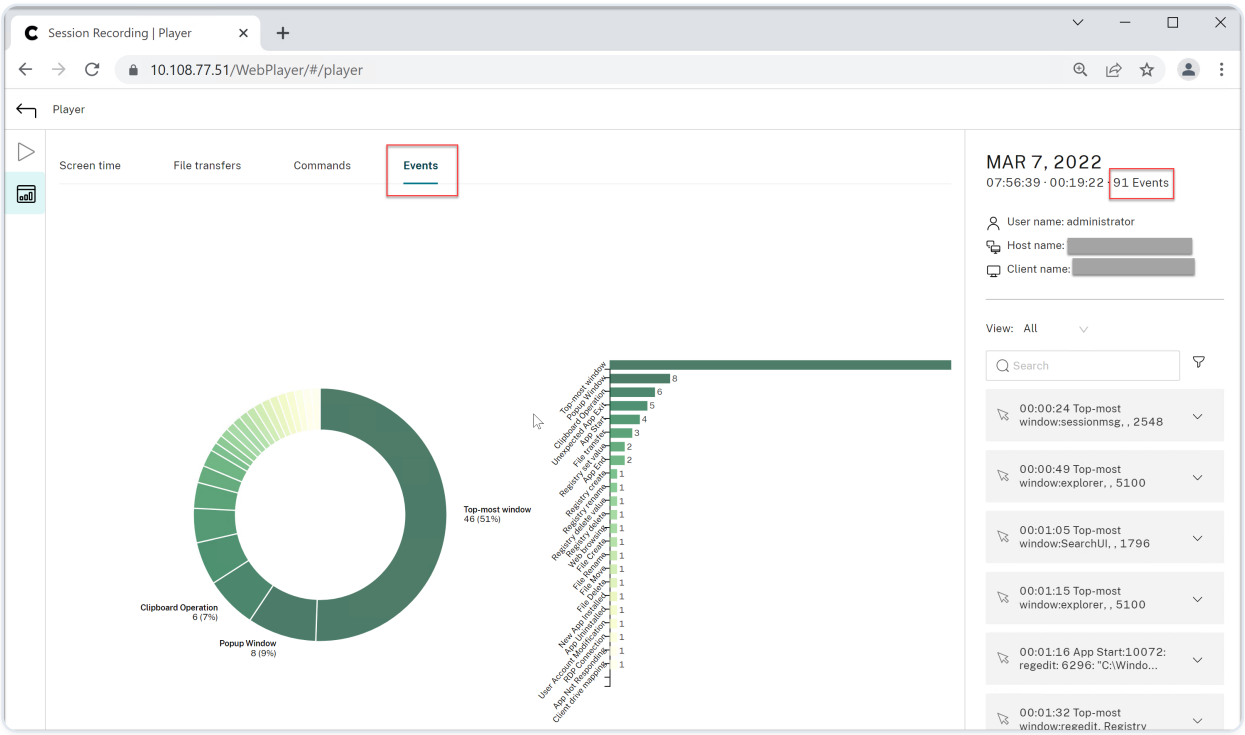
System-defined events

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

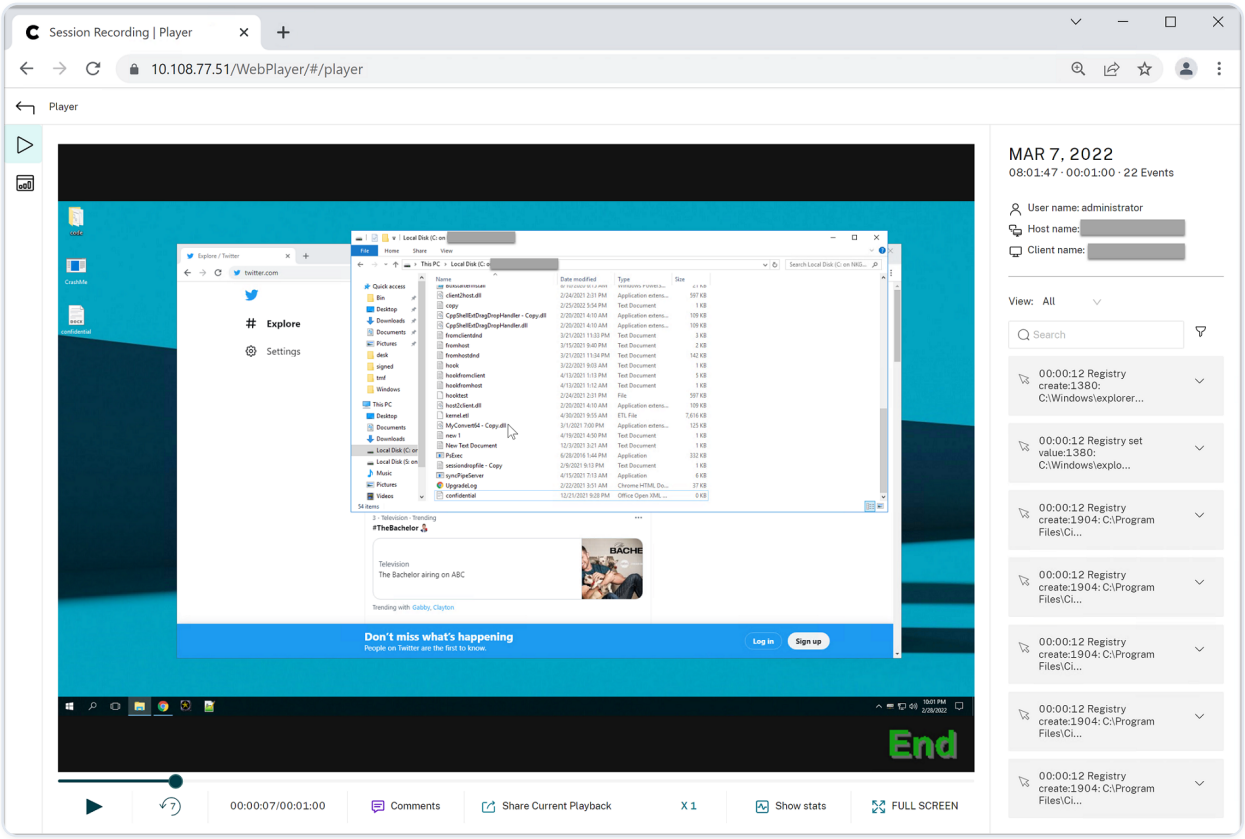
- Insertion of USB mass storage devices
- Application starts and ends
- App failures
- App installs and uninstalls
- File renaming, creation, deletion, and moving operations within sessions
- File transfers between session hosts (VDAs) and client devices (including mapped client drives and generic redirected 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
- Printing activities
- Idle periods

For example:

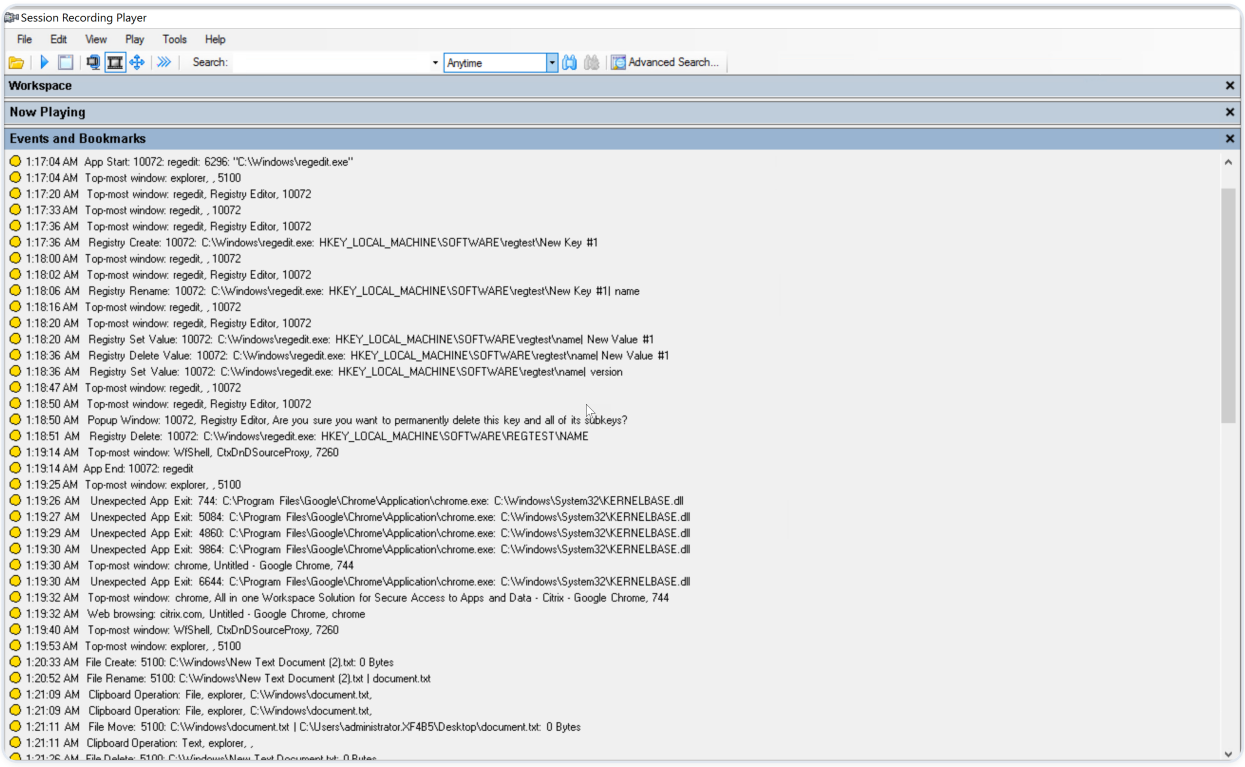
- Events in an event-only recording in the web player:



- Events in a screen recording in the web player:



- Events in the Session Recording player:

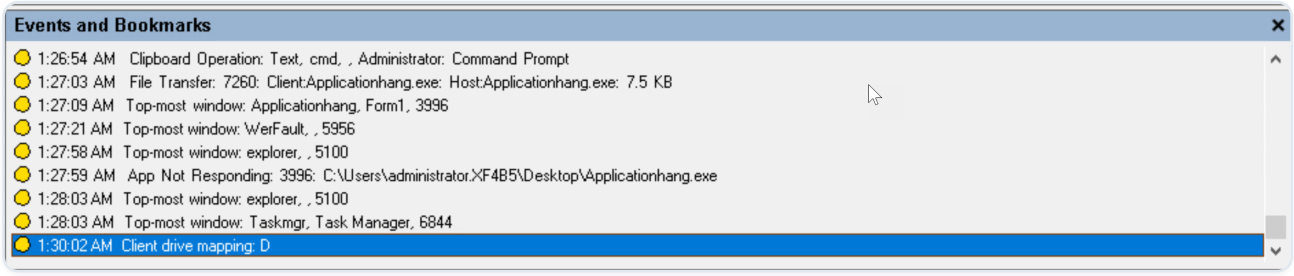


For more events in the Session Recording player, see the event descriptions later in this article.

> **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.

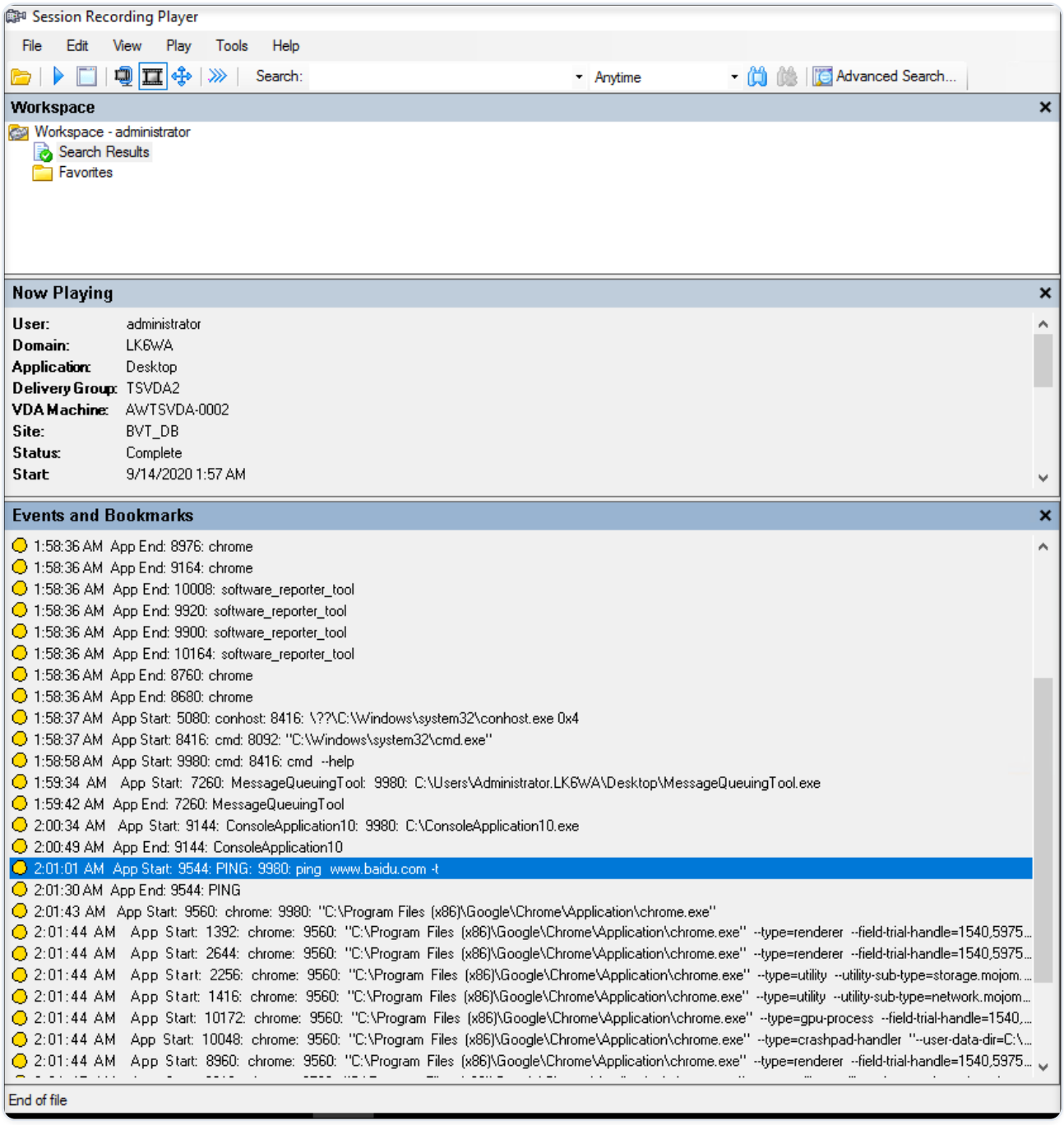
> Currently, only the insertion of USB mass storage devices (USB Class 08) can be detected.

APPLICATION STARTS AND ENDS

Session Recording supports detection of both application starts and ends. When you add a process to the **Monitored apps**, 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 **Monitored apps** by default. If you select **App start events** and **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 **Monitored apps**. The default process names are not visible on the **Monitored apps**.

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



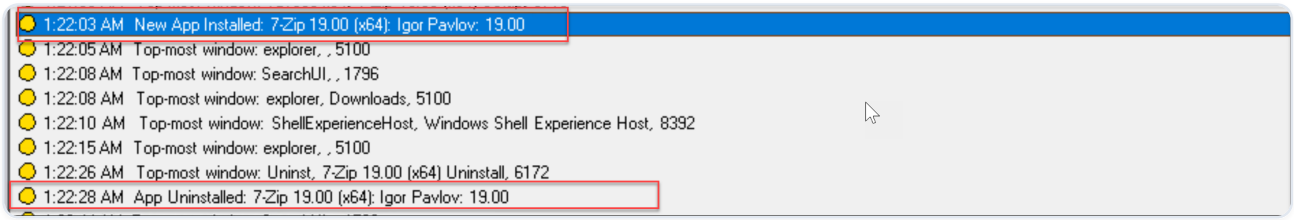
APPLICATION FAILURES

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



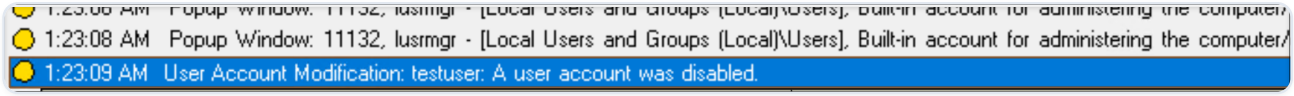
APP INSTALLS AND UNINSTALLS

The **App installs and uninstalls** rule applies to all apps.



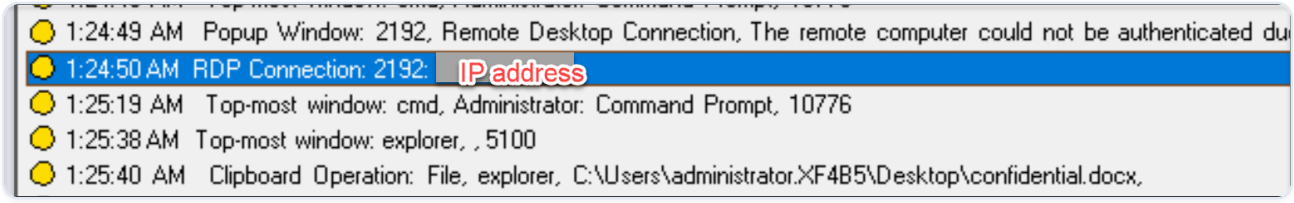
USER ACCOUNT MODIFICATIONS

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



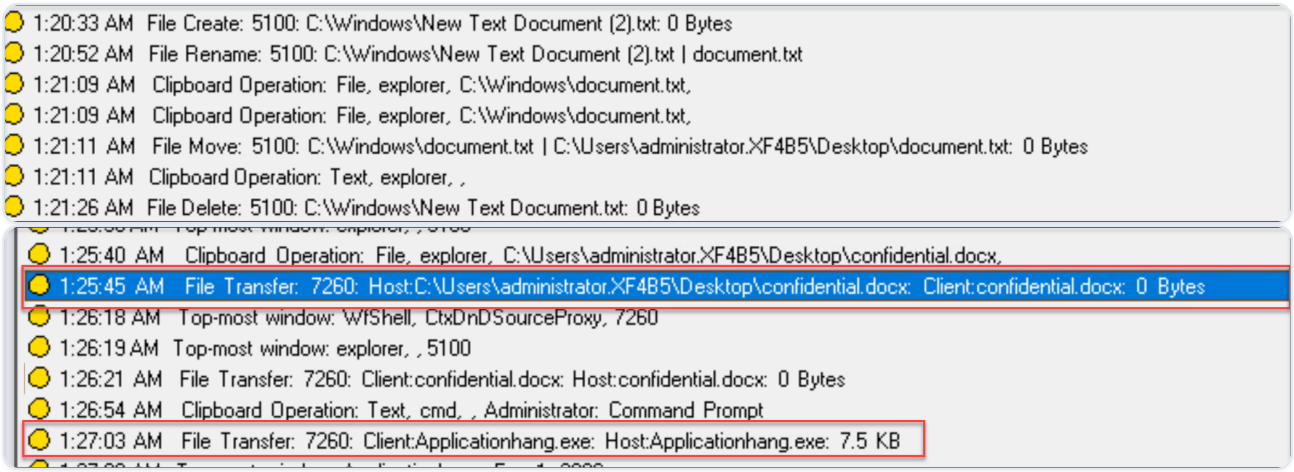
RDP CONNECTIONS

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 **Monitored files**. 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 **Sensitive file events** option triggers the detection of file transfers, no matter whether you specify the **Monitored files**.



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.



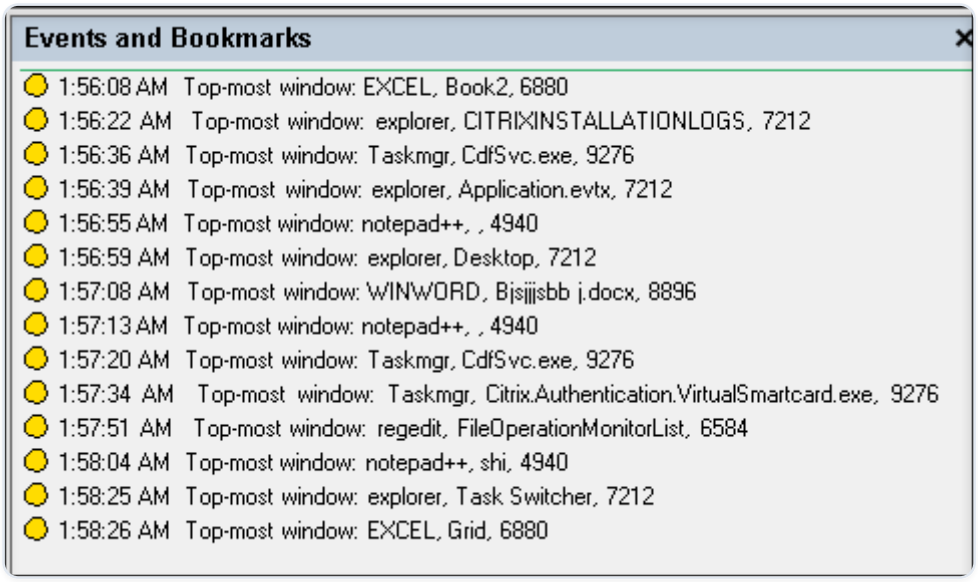
List of supported browsers:

- Google Chrome
- Microsoft Edge Chromium
- Mozilla Firefox

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

TOPMOST WINDOW EVENTS

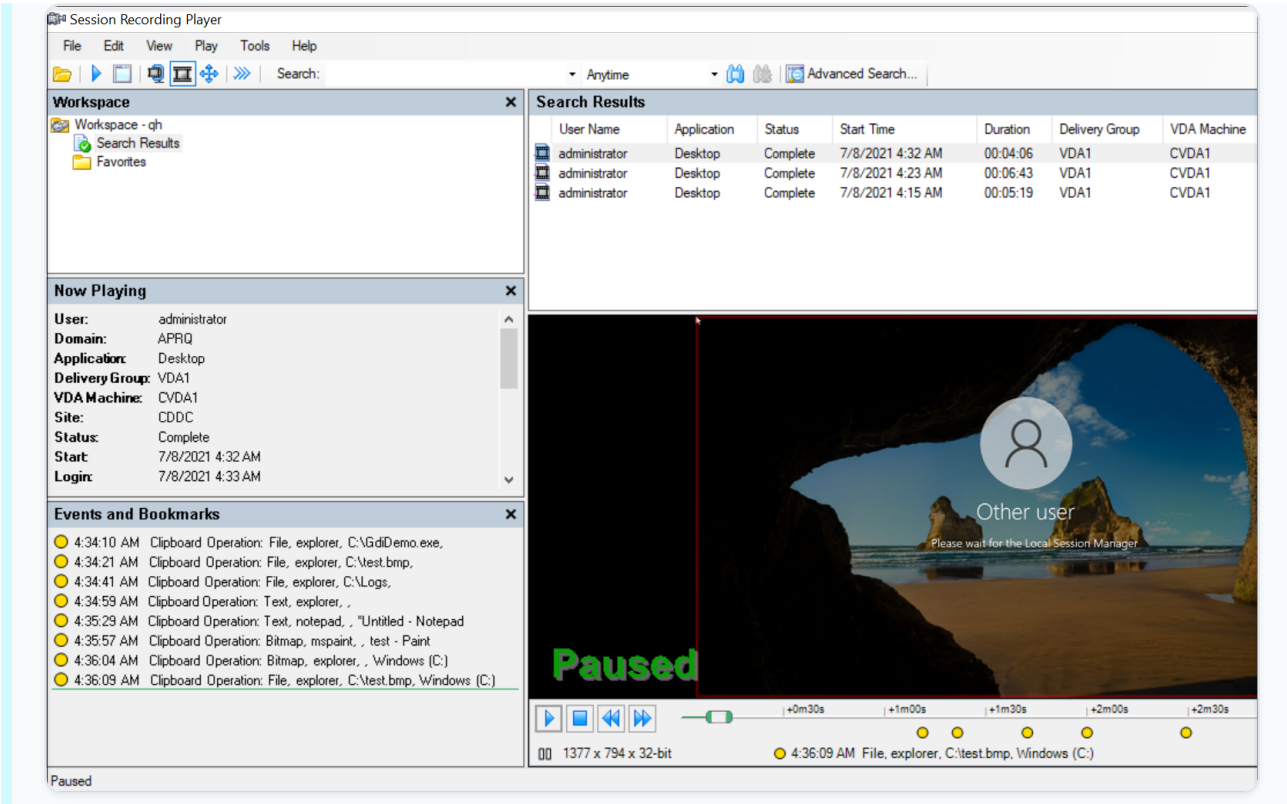
Session Recording can detect the events when the window of an app is on top of all others. The process name, title, and process number are logged.



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`).

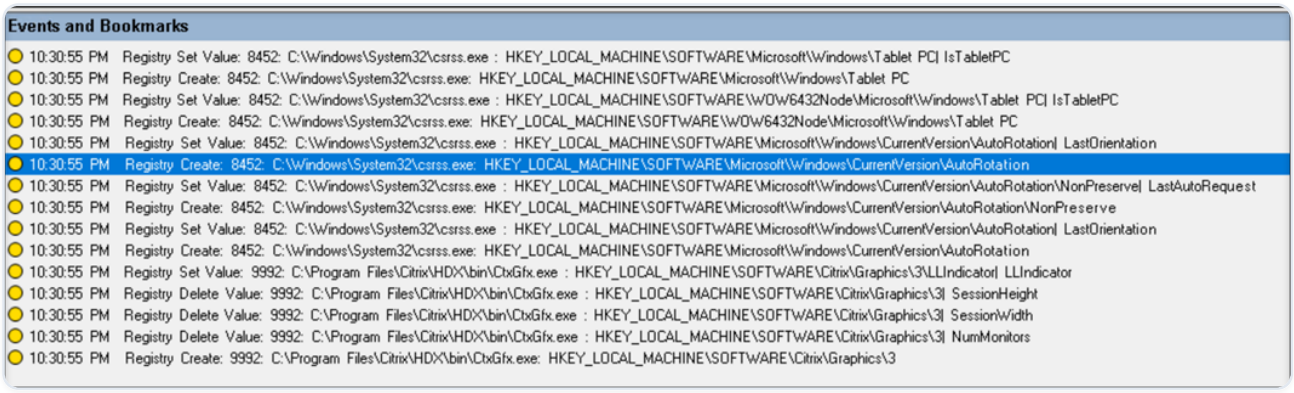


WINDOWS REGISTRY MODIFICATIONS

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:

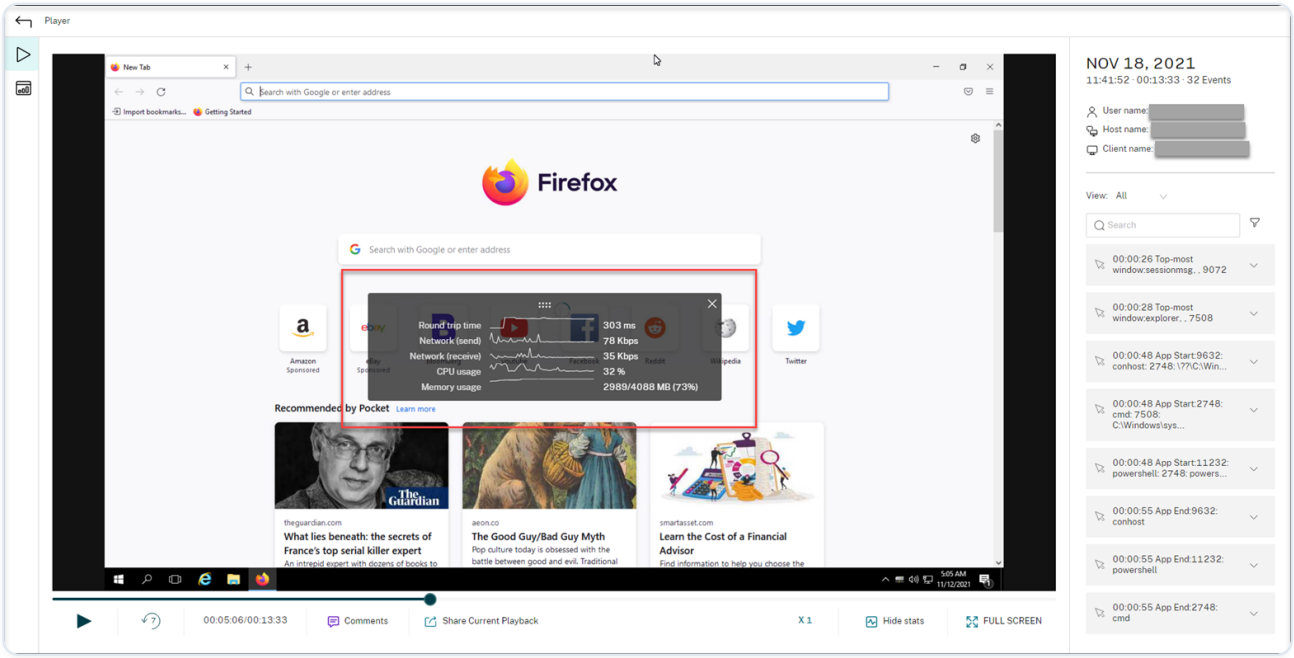


To enable this registry monitoring functionality, select the **Registry modification** option for your event detection policy.

PERFORMANCE DATA (DATA POINTS RELATED TO THE RECORDED SESSION)

When creating your event detection policy, select **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:

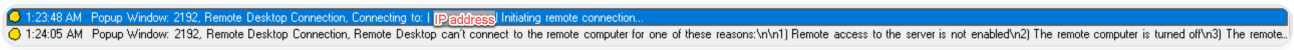
- Round trip time
- Network (send)
- Network (receive)
- CPU usage
- Memory usage



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.

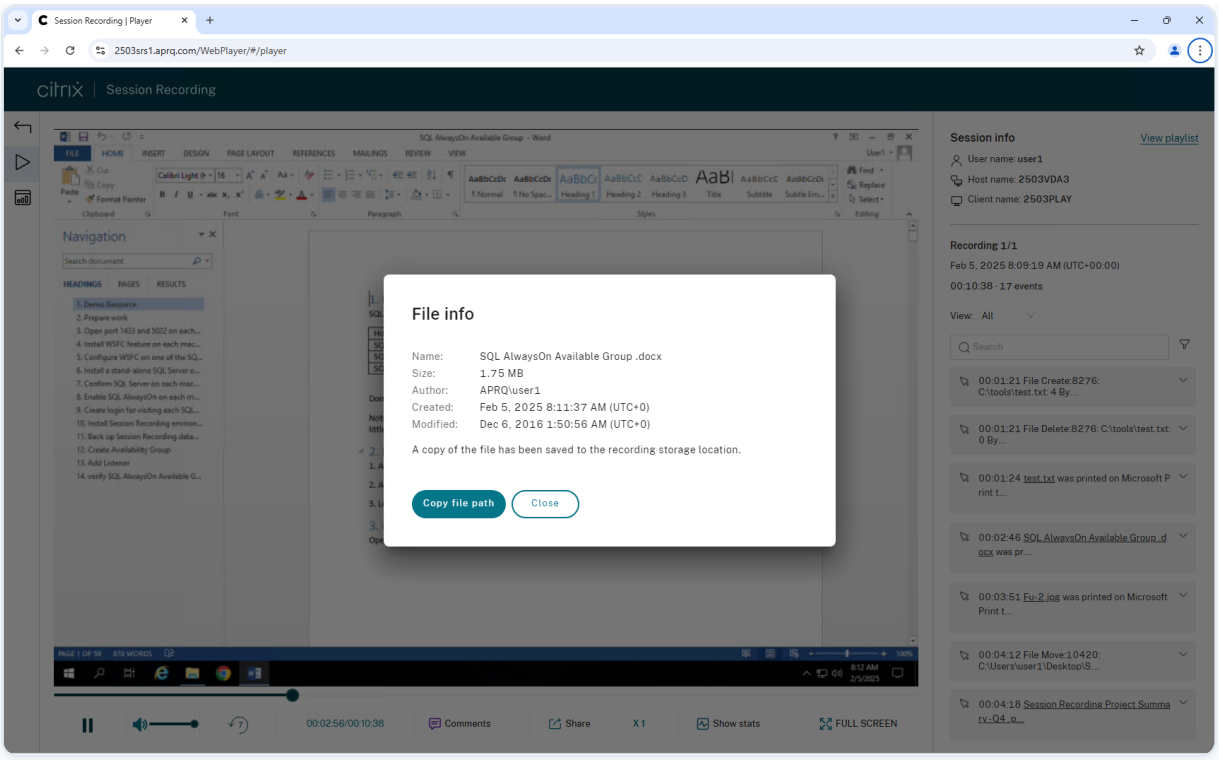


PRINTING ACTIVITIES

Session Recording monitors printing activities that occur during recorded sessions and tags them as events in recordings for later search and playback.

For an example printing activity event in the Session Recording web player, see the following screen capture:

> **Note:**
>
> Printing activity events file information are not displayed in the Session Recording player.



On the session replay interface, you can view printing events and click printed files in the right pane to access detailed file information.

IDLE PERIODS

Detects consecutive periods of user inactivity within a recorded session.

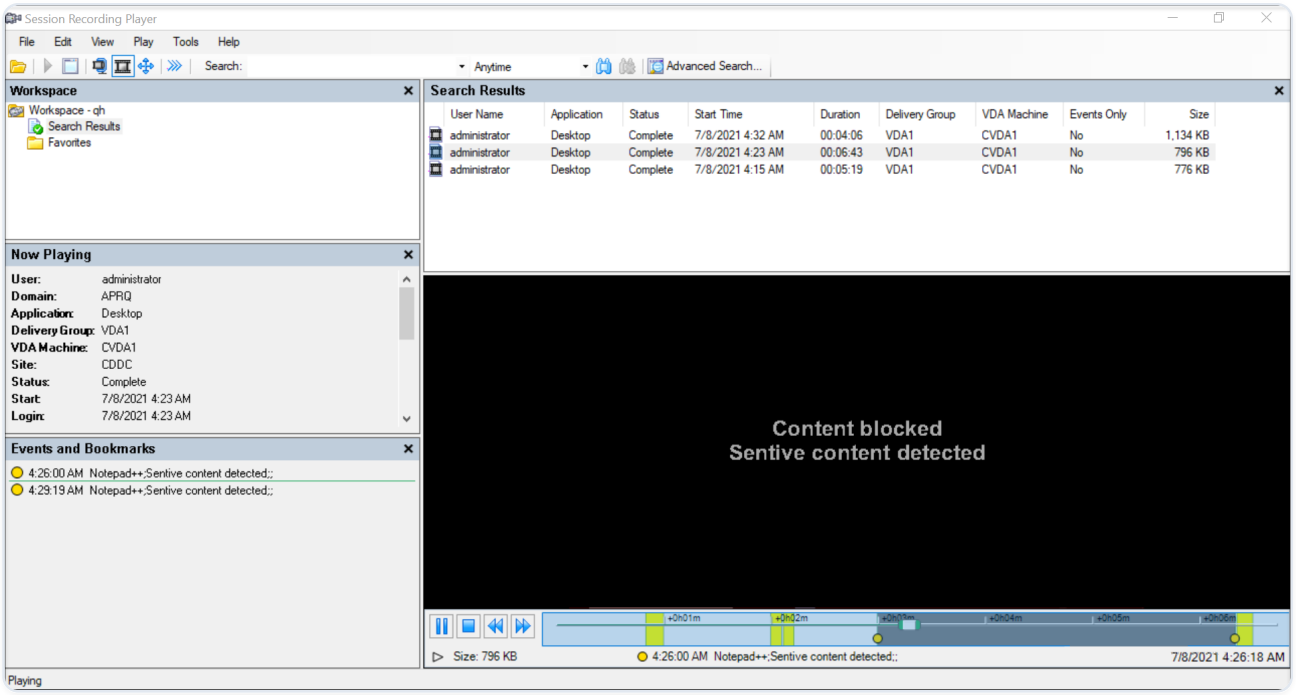
> **Note:**
>
> This feature requires Session Recording Version 2607 or later.

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.

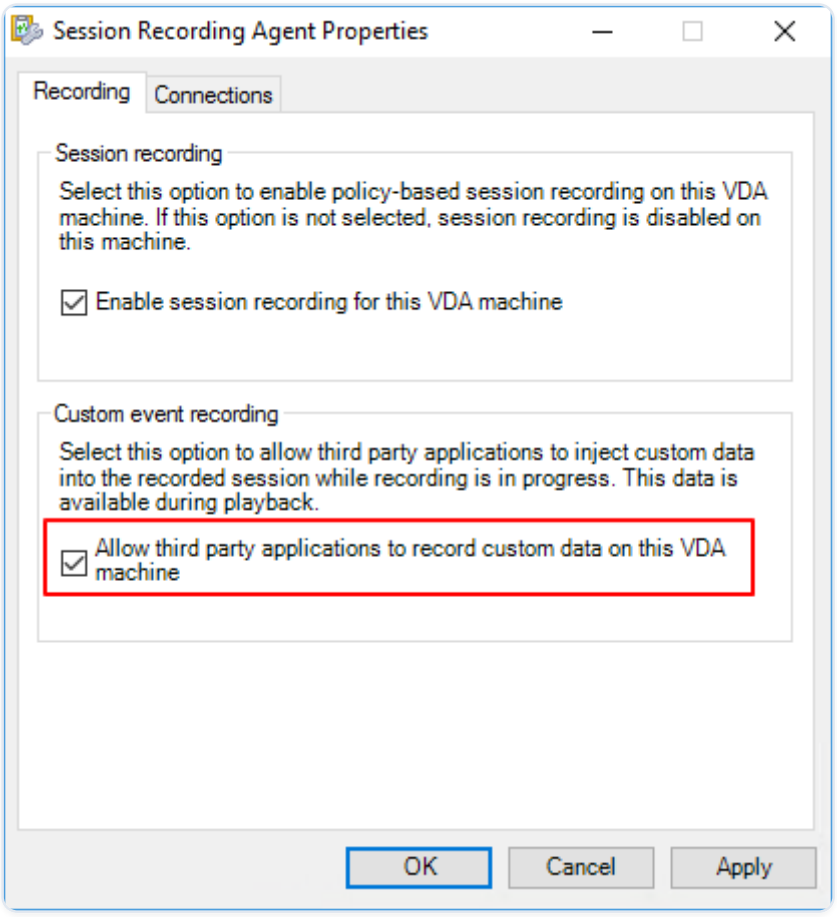
SENSITIVE INFORMATION BLOCKING

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**.

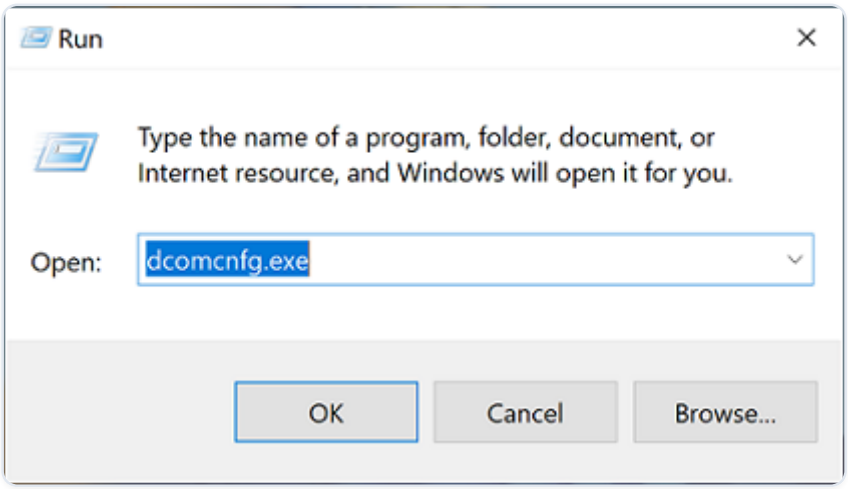


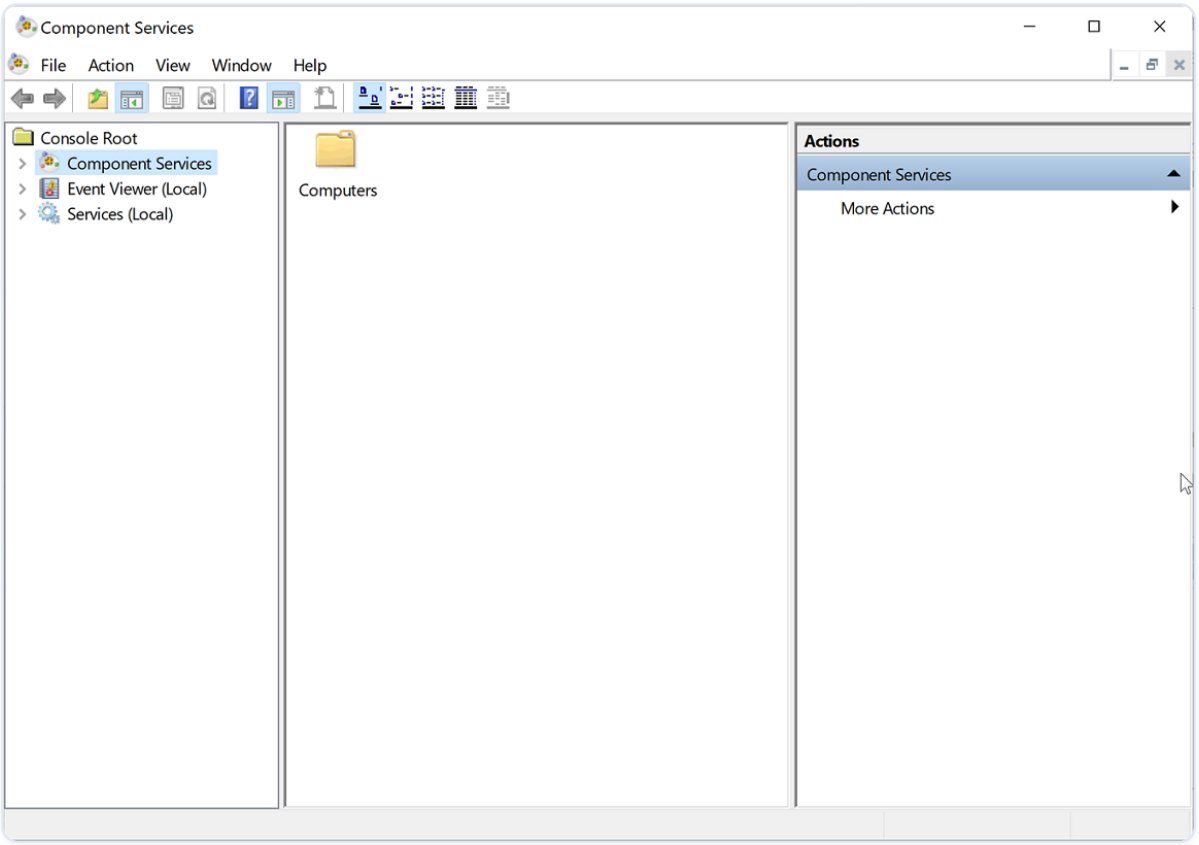
2. Grant users permission to invoke the Session Recording Event API (IUserApi COM interface).

   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.

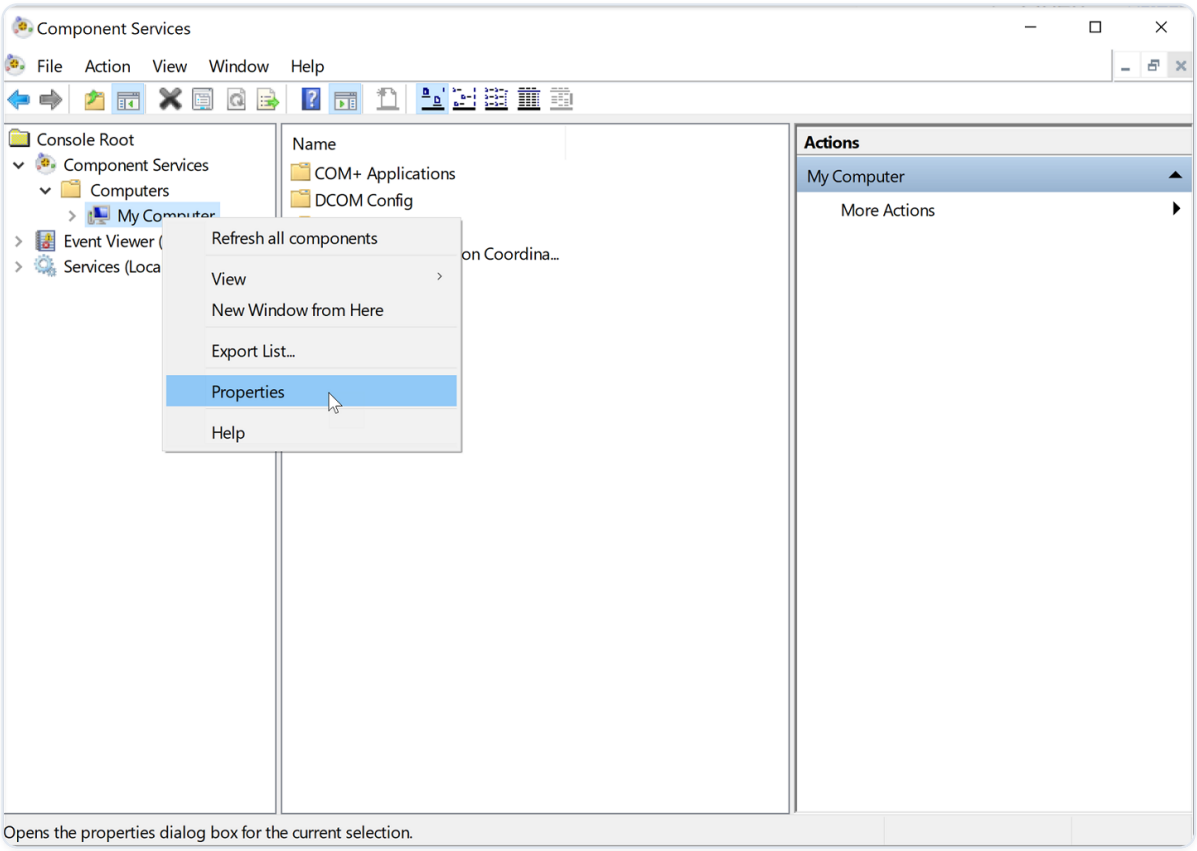




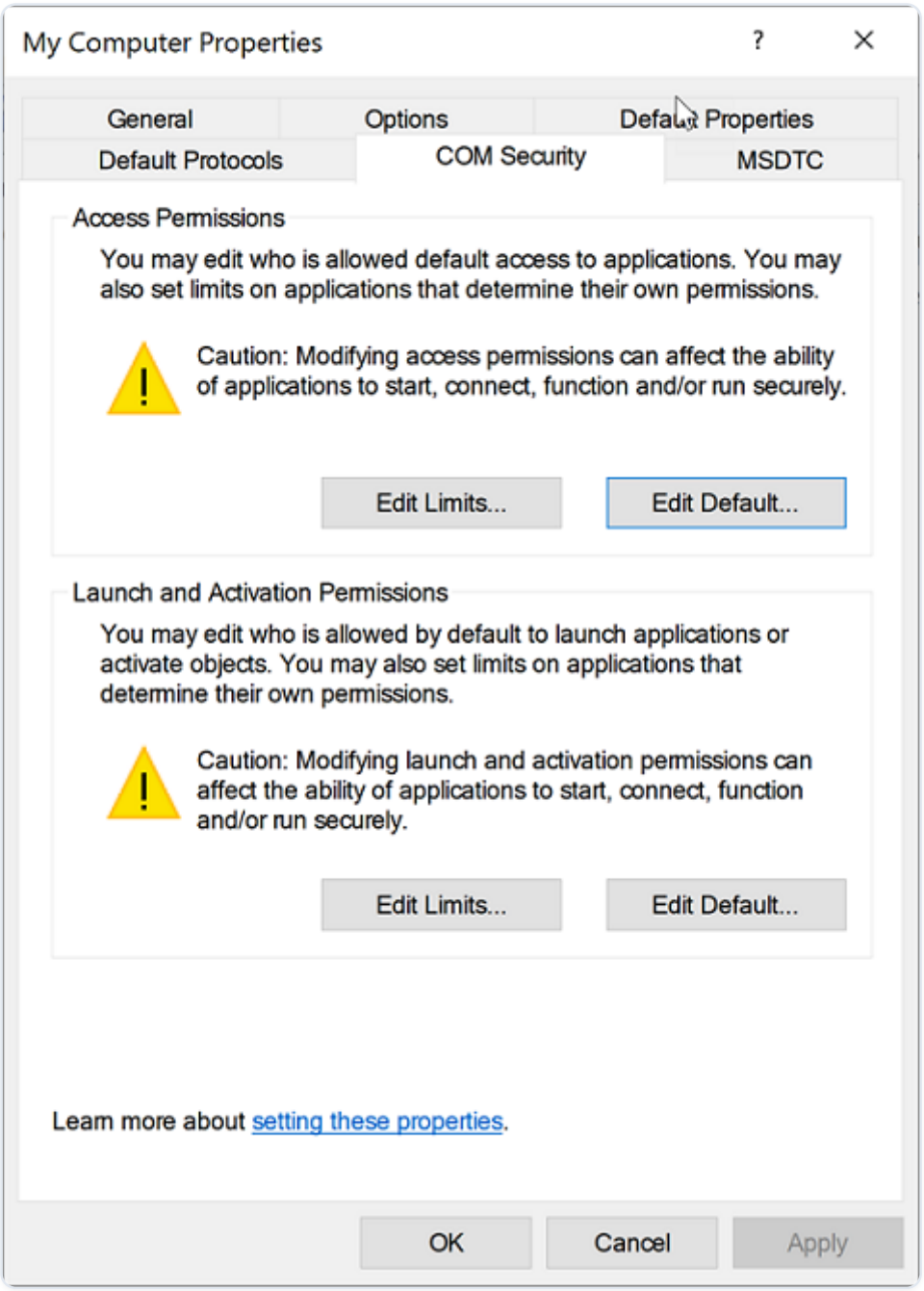
If you are granting permission to users who are not members of the domain administrator group and the Session Recording agent is running on Windows Server 2019 or later, or Windows 10 or later, proceed to step b. Otherwise, skip step b and go to step c directly.

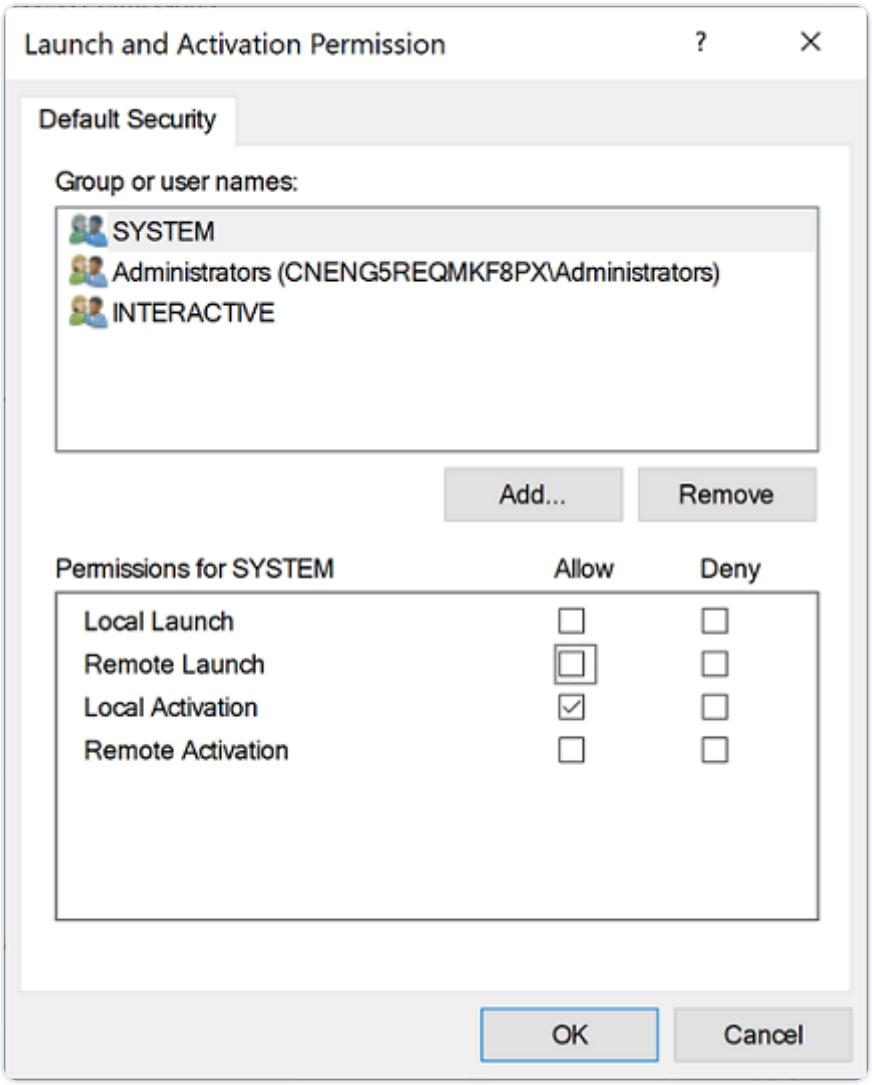
b. Select **Console Root > Component Services > Computers > My Computer** from the left navigation.

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

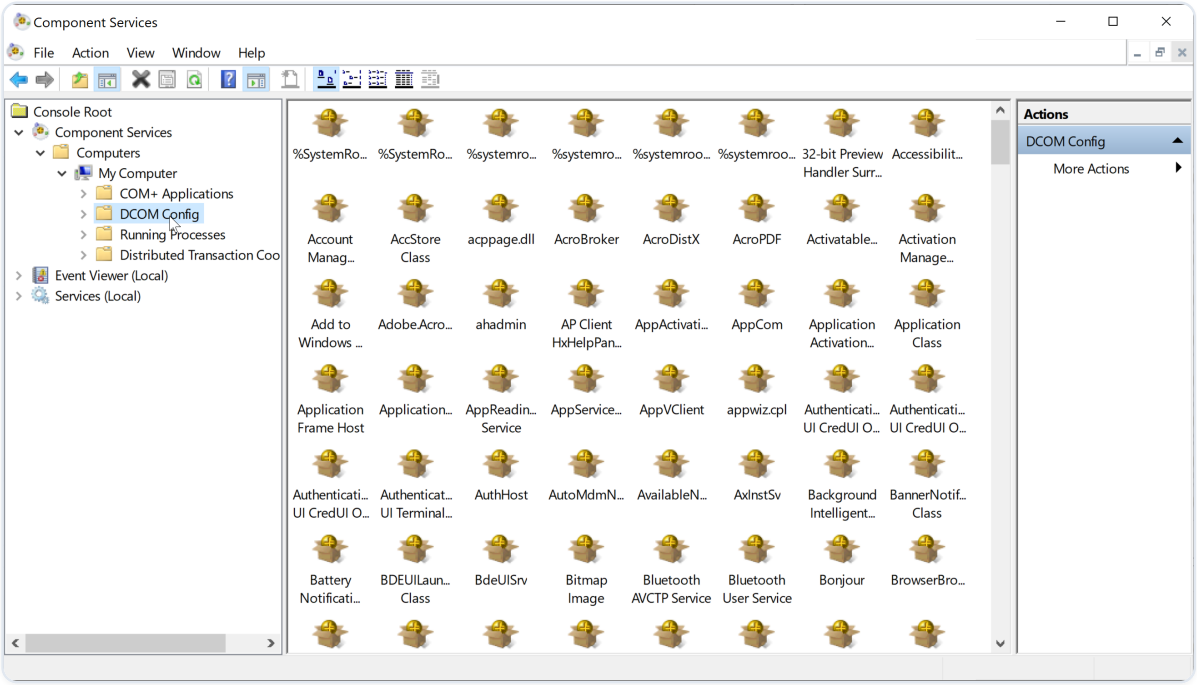


Select the **COM Security** tab, and then click **Edit Default** to add users with **Local Activation** permission in the **Launch and Activation Permissions** section.

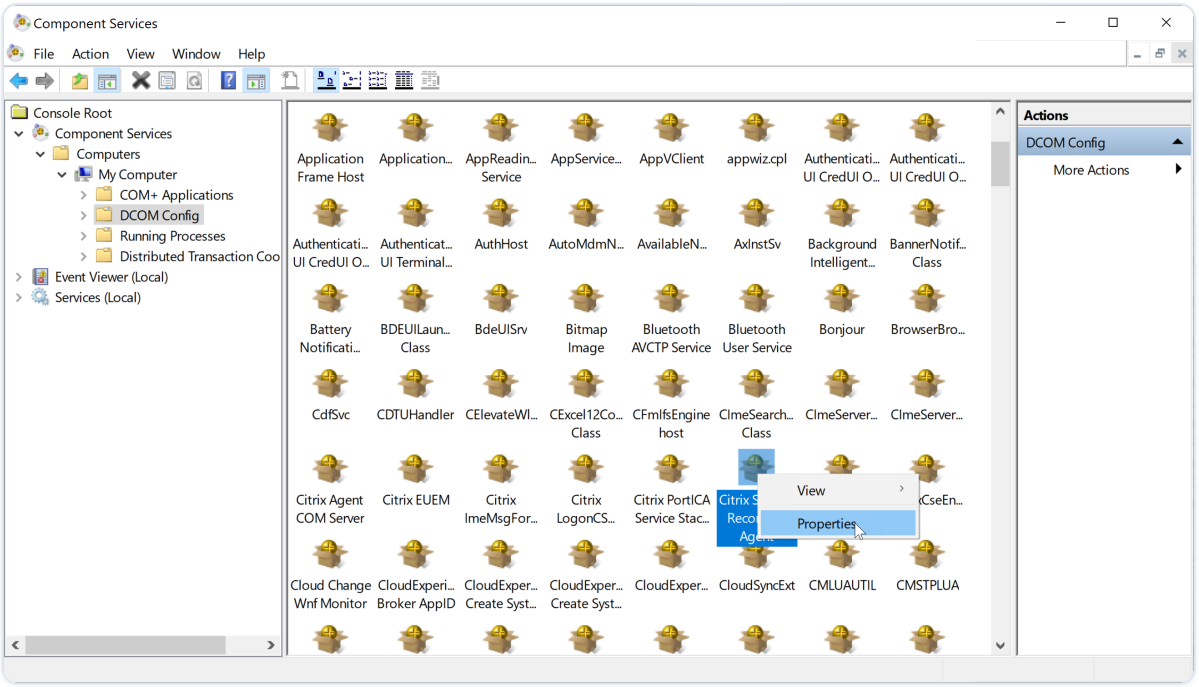

My Computer Properties
General
Options
Default Properties
Default Protocols
COM Security
MSDTC
Access Permissions
You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.
Caution: Modifying access permissions can affect 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



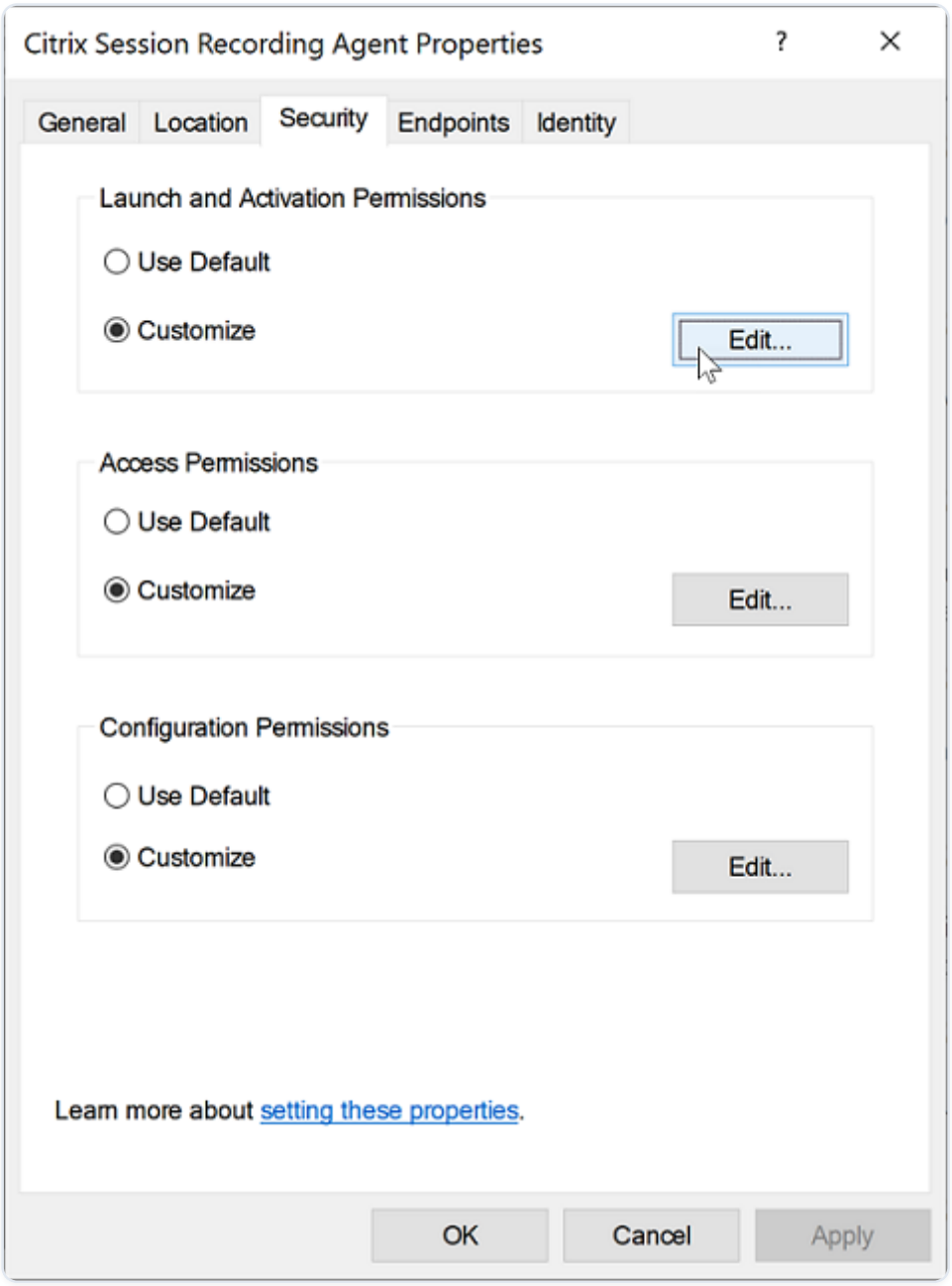
c. Select **Console Root > Component Services > Computers > My Computer > DCOM Config** from the left navigation.

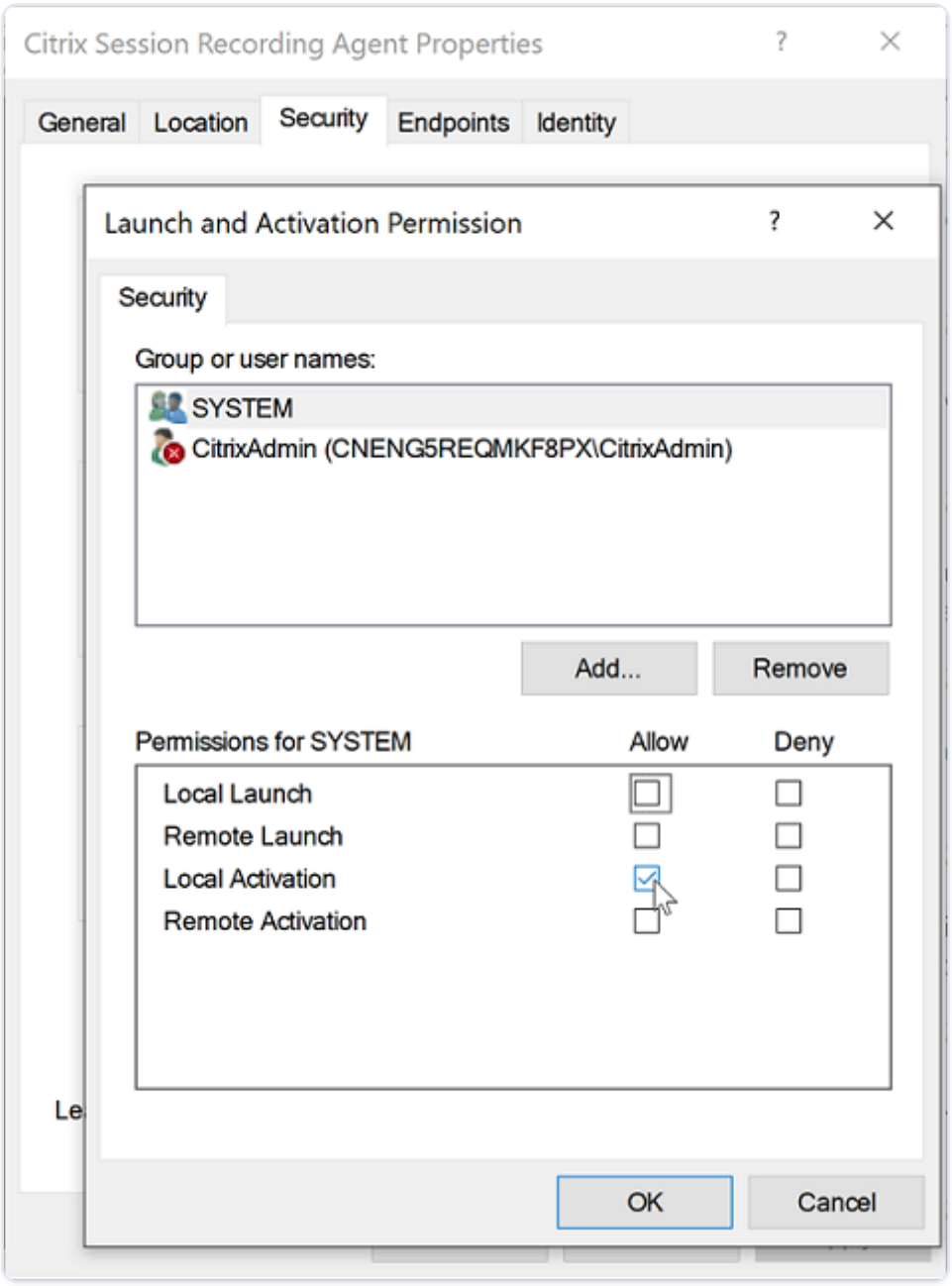


Right-click **Citrix Session Recording Agent** and choose **Properties**.



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

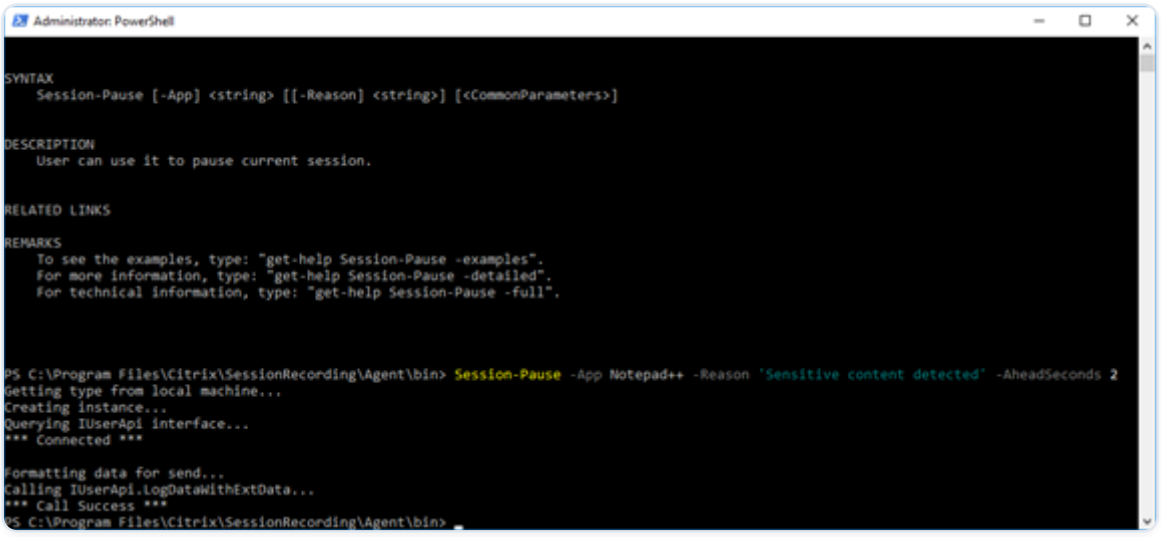


> **Note:**
>
> DCOM configuration takes effect immediately. There is no need to restart any services or the machine.

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:



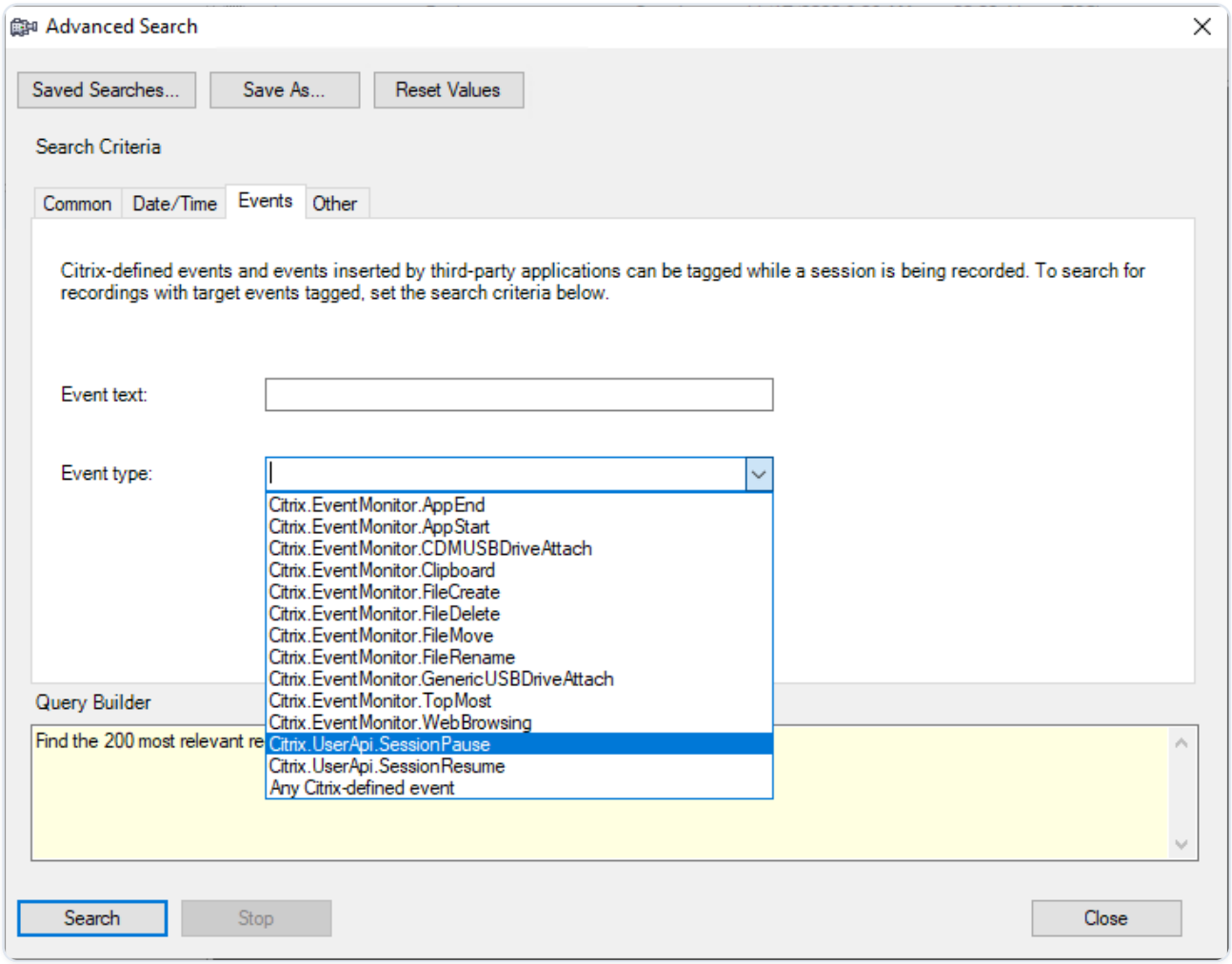
Search for and play back recordings with tagged events

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.



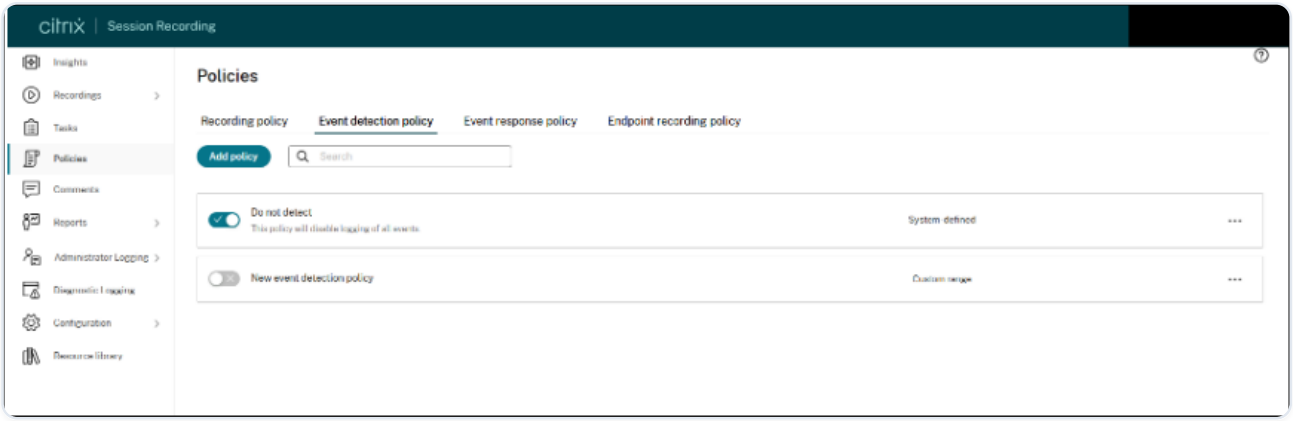
Note:

- 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.

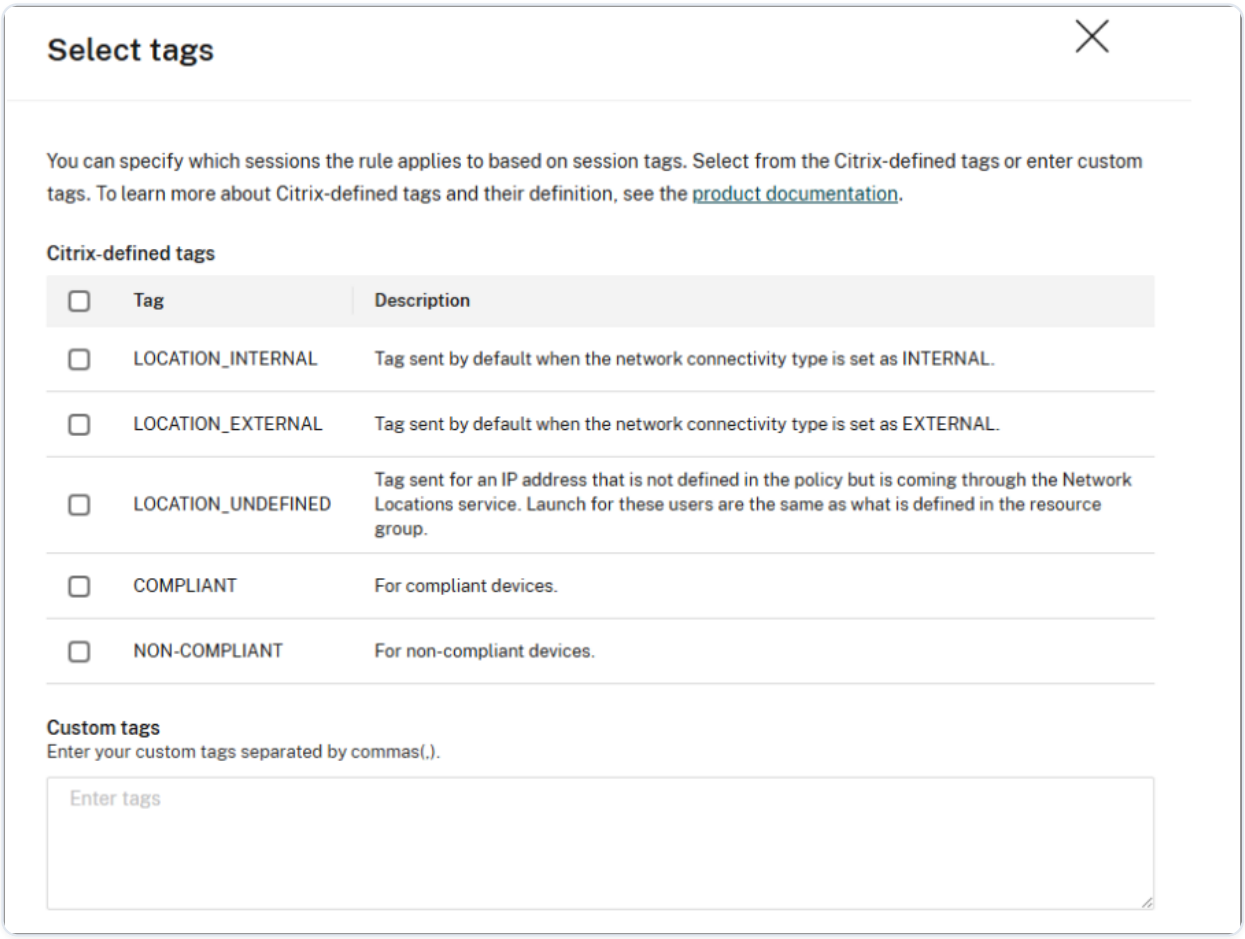
Create a custom event detection policy

Considerations

You can specify which events to log. A wizard within the Session Recording policy console helps you create rules. For each rule you create, you select the events to log and specify which sessions the rule applies to through the rule criteria settings.

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

- **Users and user groups**. Creates a list of users or groups to which the rule applies.
- **Published applications and desktops**. Creates a list of published applications or desktops to which the rule applies.
- **Delivery groups and VDA machines**. Creates a list of Delivery Groups or machines to which the rule applies.
- **IP addresses and IP address ranges**. Creates a list of IP addresses or ranges of IP addresses to which the rule applies. The IP addresses mentioned here are the IP addresses of the Citrix Workspace apps.
- **Filter**. Creates a list of smart access tags to which the rule applies. You can configure contextual access (smart access) using smart access policies on Citrix NetScaler.



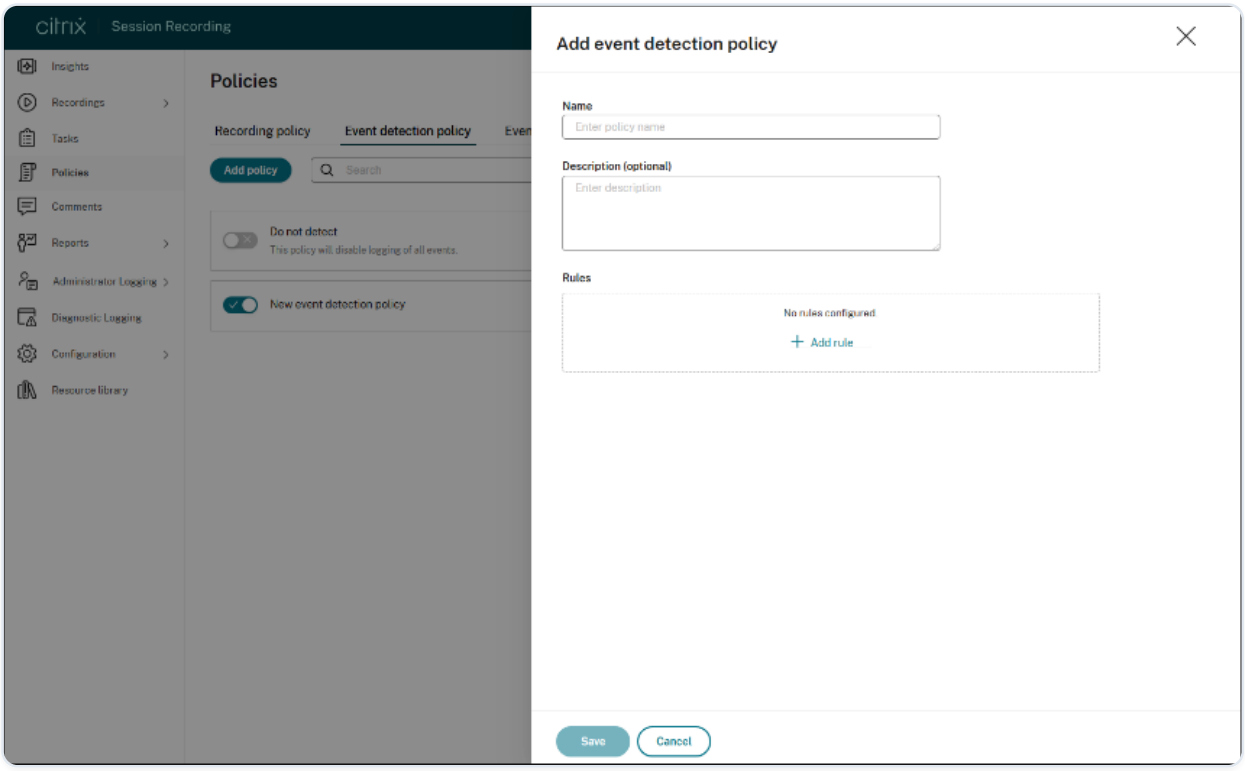
Contextual access (smart access) is available for Session Recording 2402 and later. It lets you apply policies based on the user access context including:

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

Steps

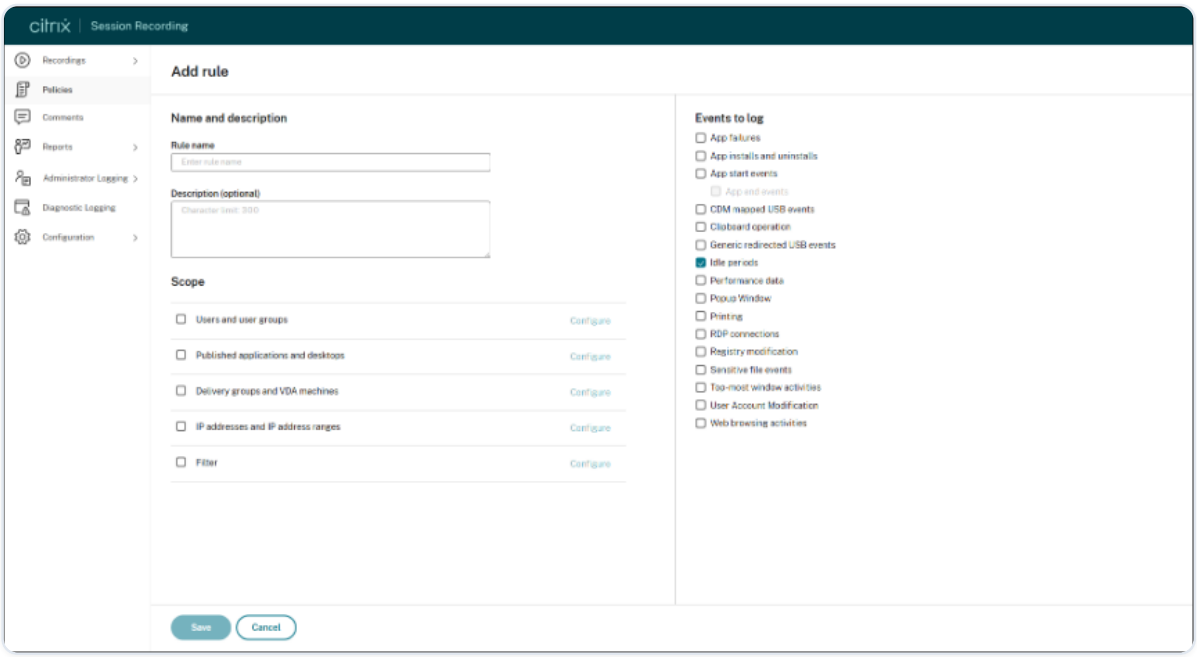
To create a custom event detection policy:

1. Log on as an authorized Policy Administrator to the Session Recording web console.
2. Select **Policies** from the left navigation.
3. Select **Event detection policy**.
4. Click **Add policy**.
5. Enter a name and description for the new policy, and then click **Add rule**.



6. Enter a name and description for the rule.

   a. Specify one or more target events to monitor by selecting the check box next to each event type.



   - **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.
   - **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.

- **App start events**: Logs the starts of target applications.
- **App end events**: Logs the ends of target applications.

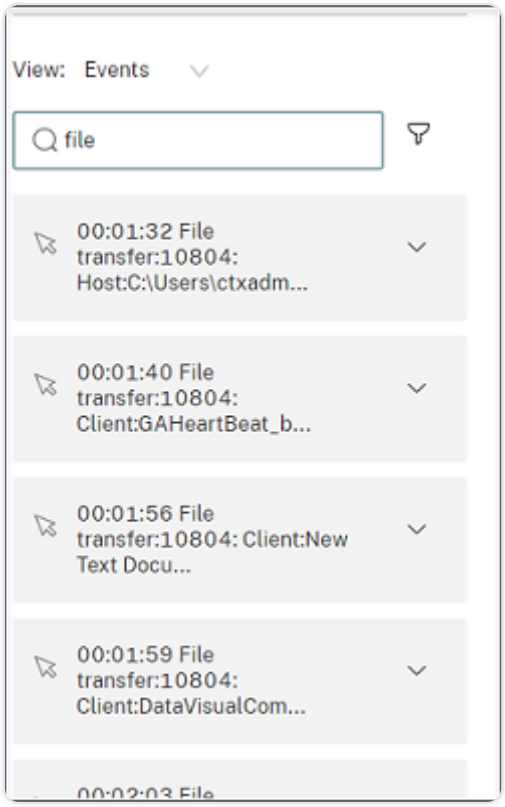
> **Note:**
>
> The **App end events** check box is grayed out before you select **App start events**.

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

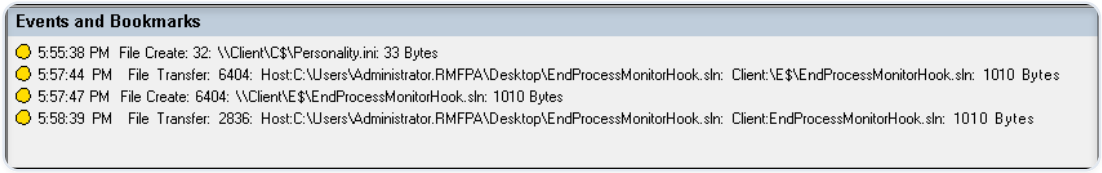
> **Note:**
>
> - To capture the start and end of an application, add the process name of the application in the **Monitored apps**. For example, to capture the start of Remote Desktop Connection, add the process name `mstsc.exe` to the **Monitored apps**. When you add a process to the **Monitored apps**, 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 **Monitored apps** by default. If you select **App start events** and **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 **Monitored apps**. The default process names aren't visible on the **Monitored apps**.
> - 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.

- **Sensitive file events**: Logs operations on target files in the **Monitored files** 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 **Monitored files** is specified.

  - File events presented in the web player



  - File events presented in the Session Recording Player



- **Monitored files**: When you select **Sensitive file events**, use the **Monitored files** 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 **Monitored files**. 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 **Monitored files**.

- 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 **Monitored files**.
- 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.

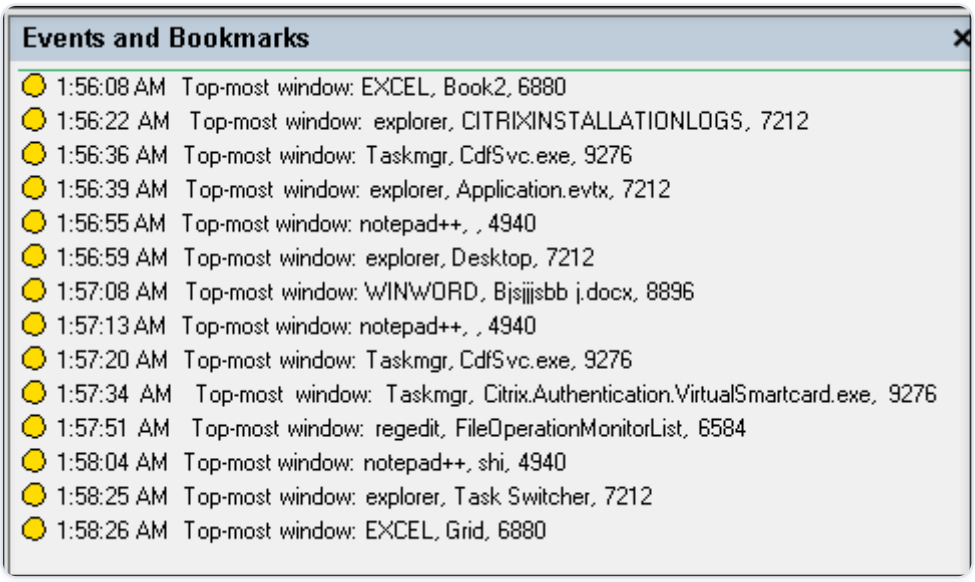
- **Web browsing activities**: Logs user activities on supported browsers and tags the browser name, URL, and page title in the recording.



List of supported browsers:

- Google Chrome
- Microsoft Edge Chromium
- Mozilla Firefox

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



- **Clipboard operation**: 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.
- **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.
- **Monitored registries**: When you select **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.
- **App failures**: Logs unexpected app exits and unresponsive apps. This rule applies to all apps.
- **User account modifications**: Logs the following user account modifications: account creation, enablement, disablement, deletion, lockout, name changes, and password modification attempts.
- **RDP connections**: Logs RDP connections initiated from the VDA hosting the recorded session.
- **App installs and uninstalls**: Logs app installs and uninstalls during the recorded session. This rule applies to all apps.
- **Performance data**: Enables the session data overlay feature. Select this check box to view data points related to the recorded session.
- **Popup window**: Logs popup windows that might appear when users open or close a confidential file or access a folder.

- **Printing**: Logs printing activities that occur during recorded sessions. Session Recording captures details about printed content, including file name, file size, author, printer name, timestamp, and more. You can choose to save a copy of the printed files along with the recordings for future reference and auditing. This feature allows for greater oversight and auditing of printing activity within recorded sessions.

b. Select and edit the rule criteria.

   Similar to creating a custom recording policy, you can choose one or more rule criteria:

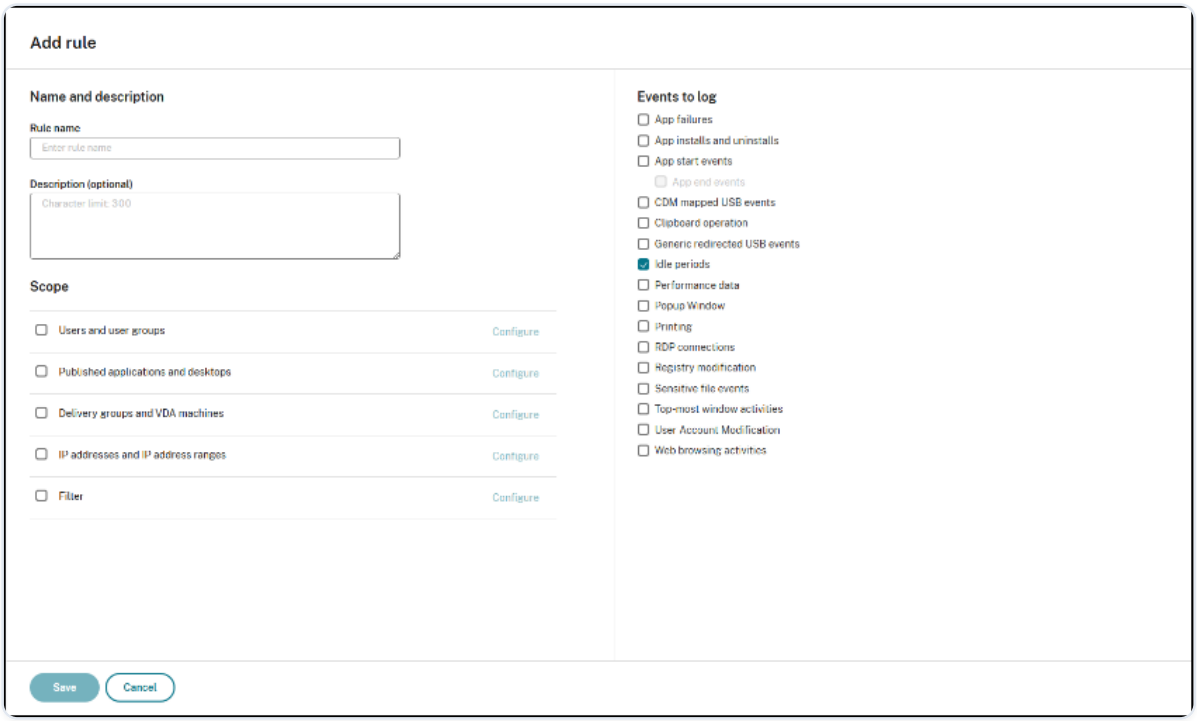
   - **Users and user groups**
   - **Published applications and desktops**
   - **Delivery groups and VDA machines**
   - **IP addresses and IP address ranges**
   - **Filter**

   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.

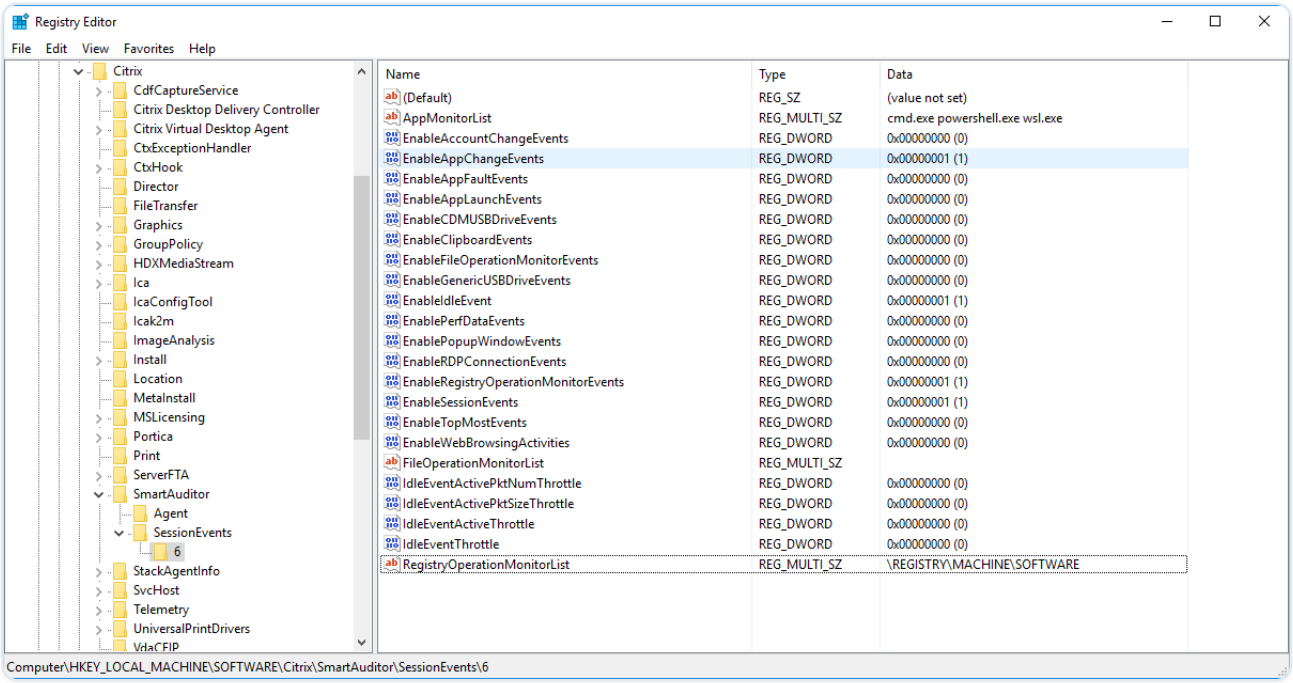
   For more information, see the instructions in the Create a custom recording policy section.

   > **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).
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).

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).**
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).
EnableRDPConnectionEvents	**1**: enables detecting RDP connections; **0**: disables detecting RDP connections (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).**
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).
EnablePrintingEvents	**1**: enables detecting printing activities; **0**: disables detecting printing 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

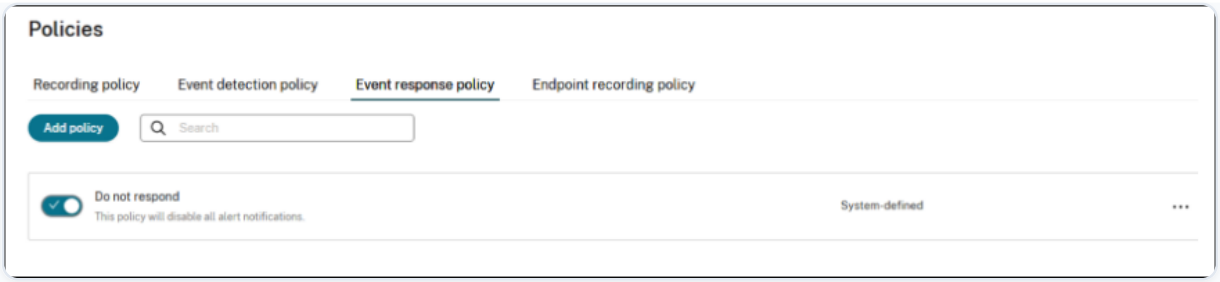
Event response policies let you configure event-triggered actions so that you can:

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

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

> **Note:**

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



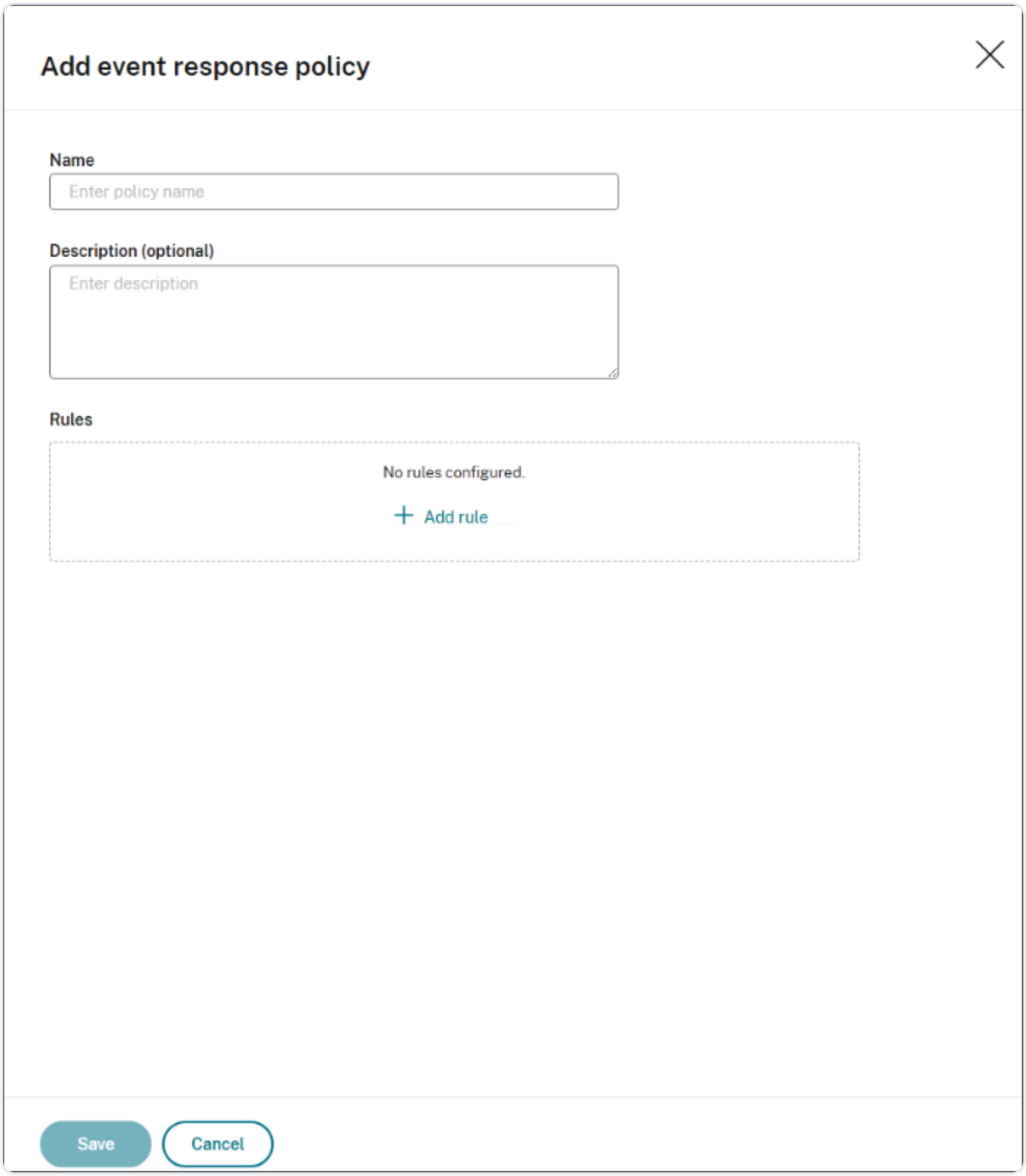
System-defined event response policy

Session Recording provides one system-defined event response policy:

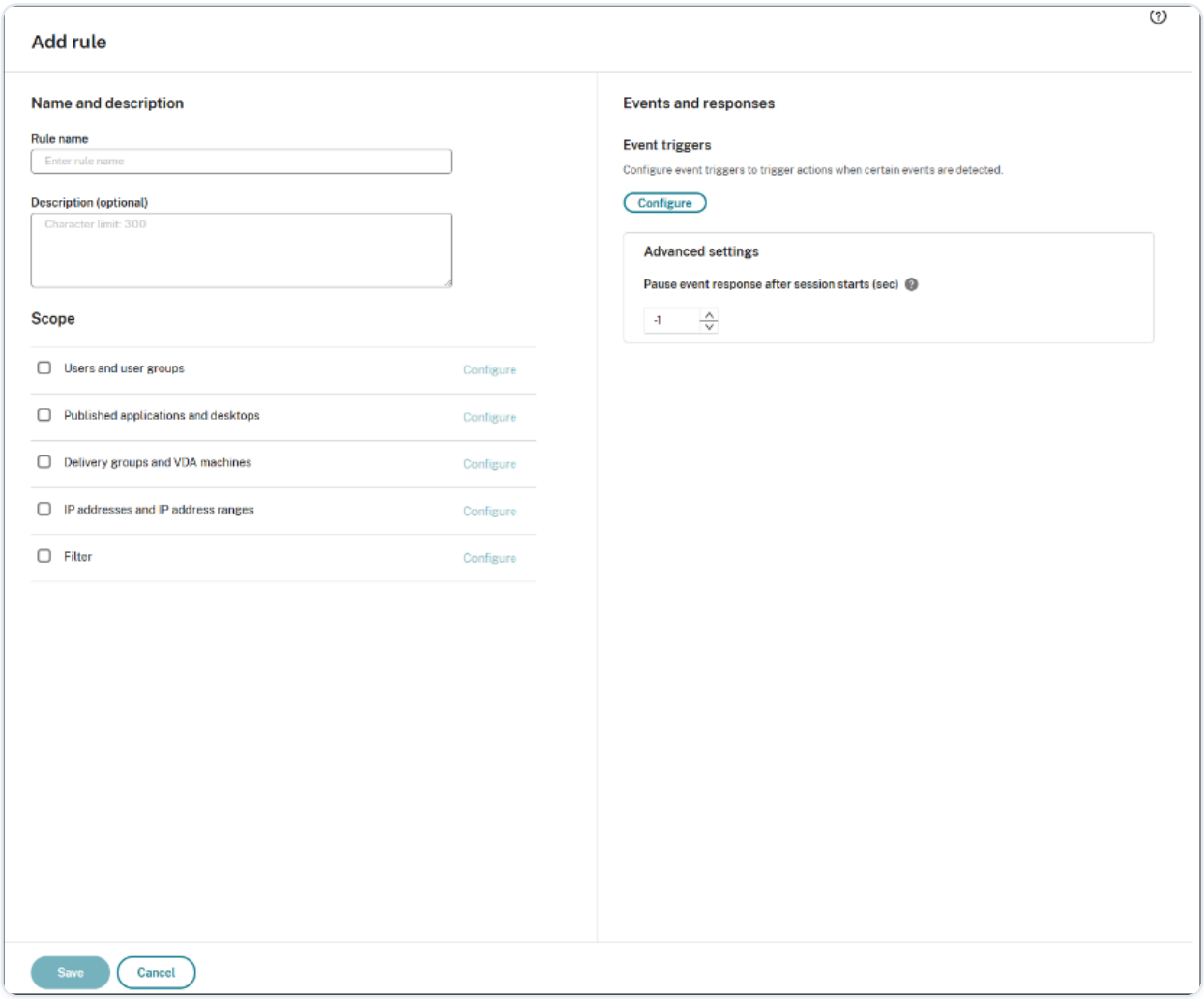
- **Do not respond**. By default, no action is taken in response to logged events in your recordings.

Create a custom event response policy

1. Click **Add policy**.
2. On the **Add event response policy** page, enter a name and description for your new policy.



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

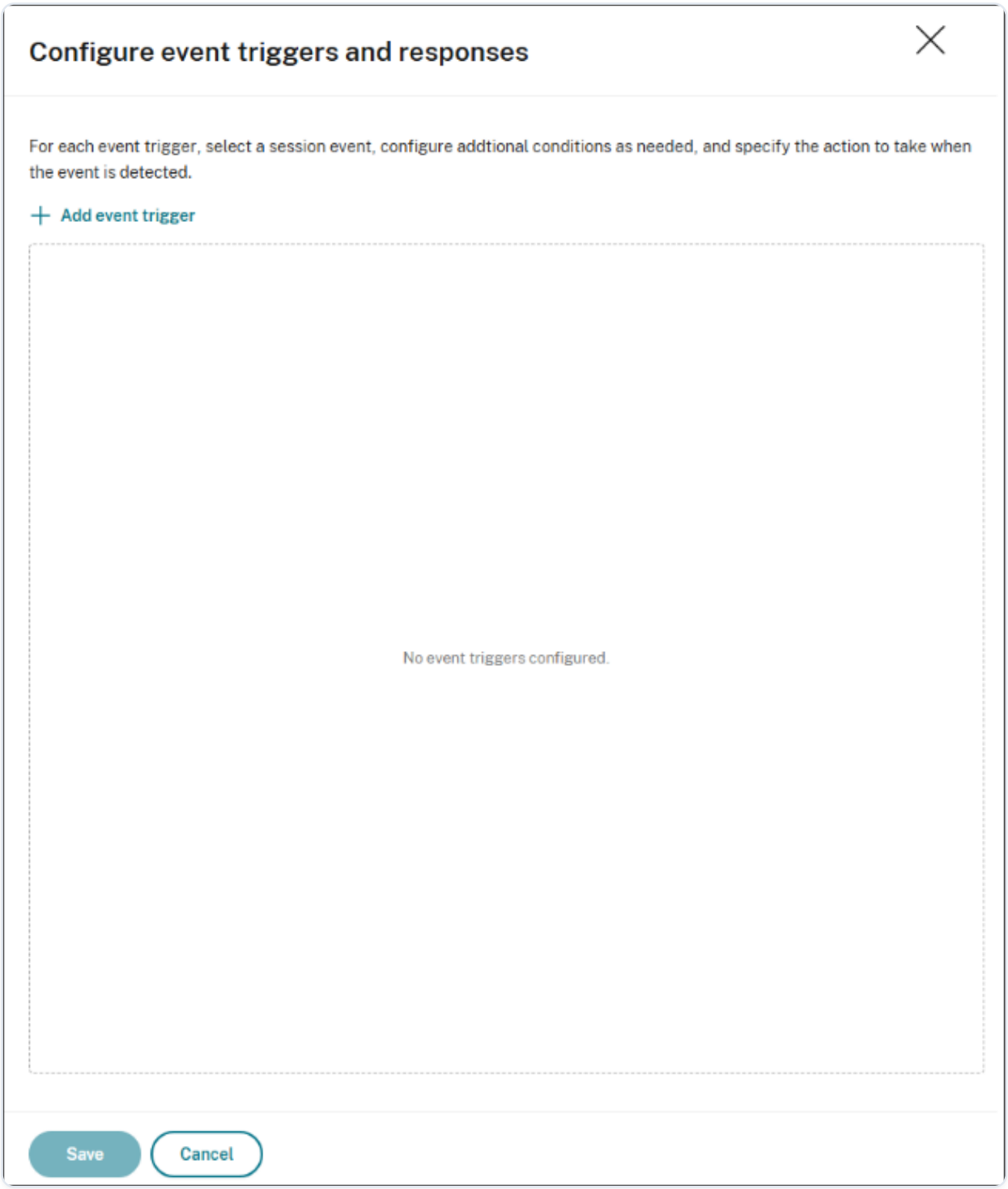


5. In the **Event triggers** section, click **Configure** to configure event-triggered actions so that you can:

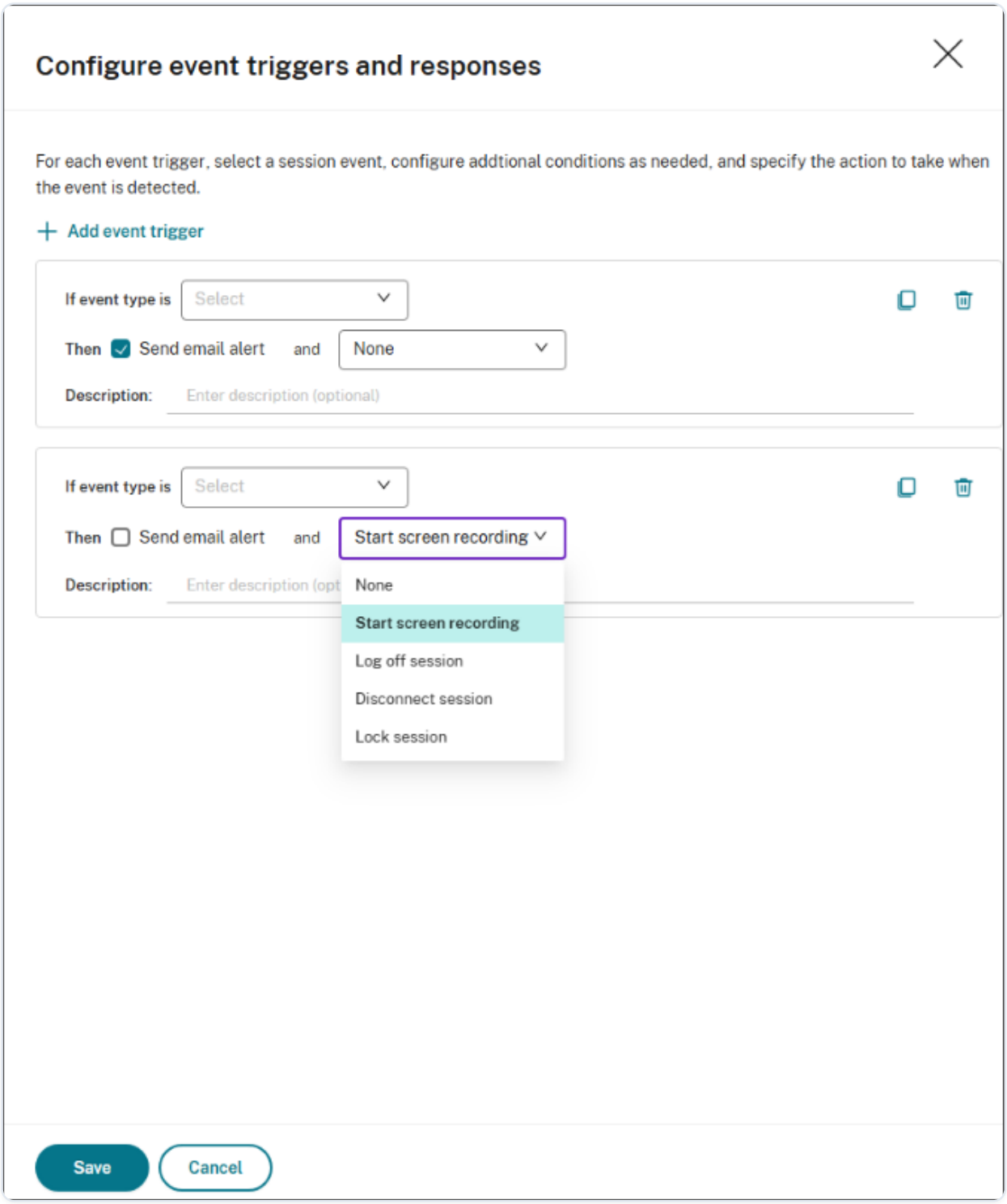
   - Send an email alert when a session start event is detected.
   - Take action (any combination of the following actions) when events are detected in recorded sessions

     - Send email alert
     - Start screen recording immediately (with or without lossy screen recording enabled)
     - Lock session
     - Log off session
     - Disconnect session

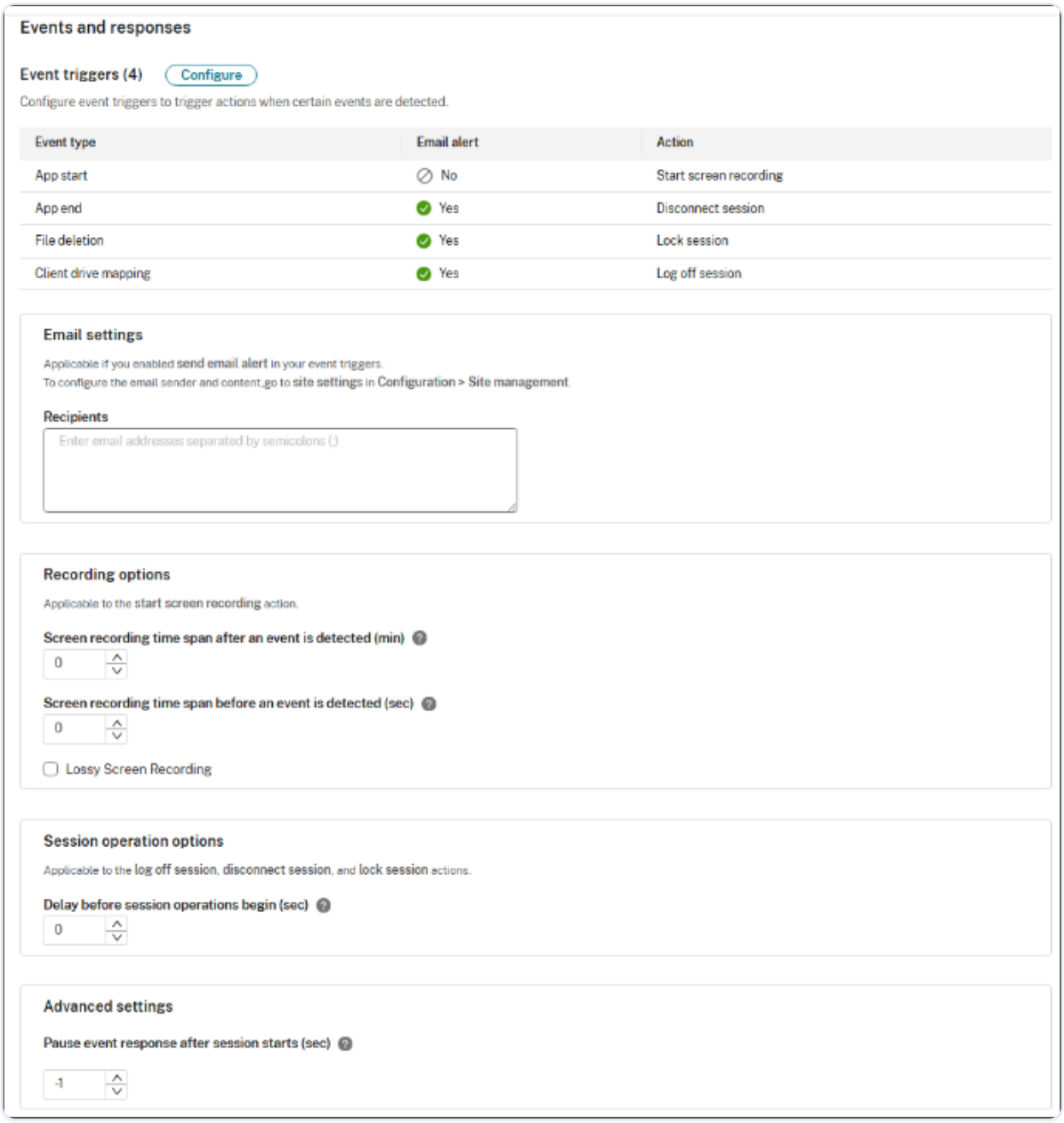
   Click **Add event triggers** to create event triggers from scratch. Or, click **Browse templates** to select existing event trigger templates to use directly or customize.



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



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



Note:

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

You can define your event triggers on the **Description** row or leave the row empty. Your defined description of an event trigger is provided in the alert emails if you have **Send email** selected and events of the type are logged. If you have **Start screen recording** selected, set the relevant parameters as illustrated later in this article. After that, dynamic

> screen recording automatically starts when certain events occur during an event-only recording.

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

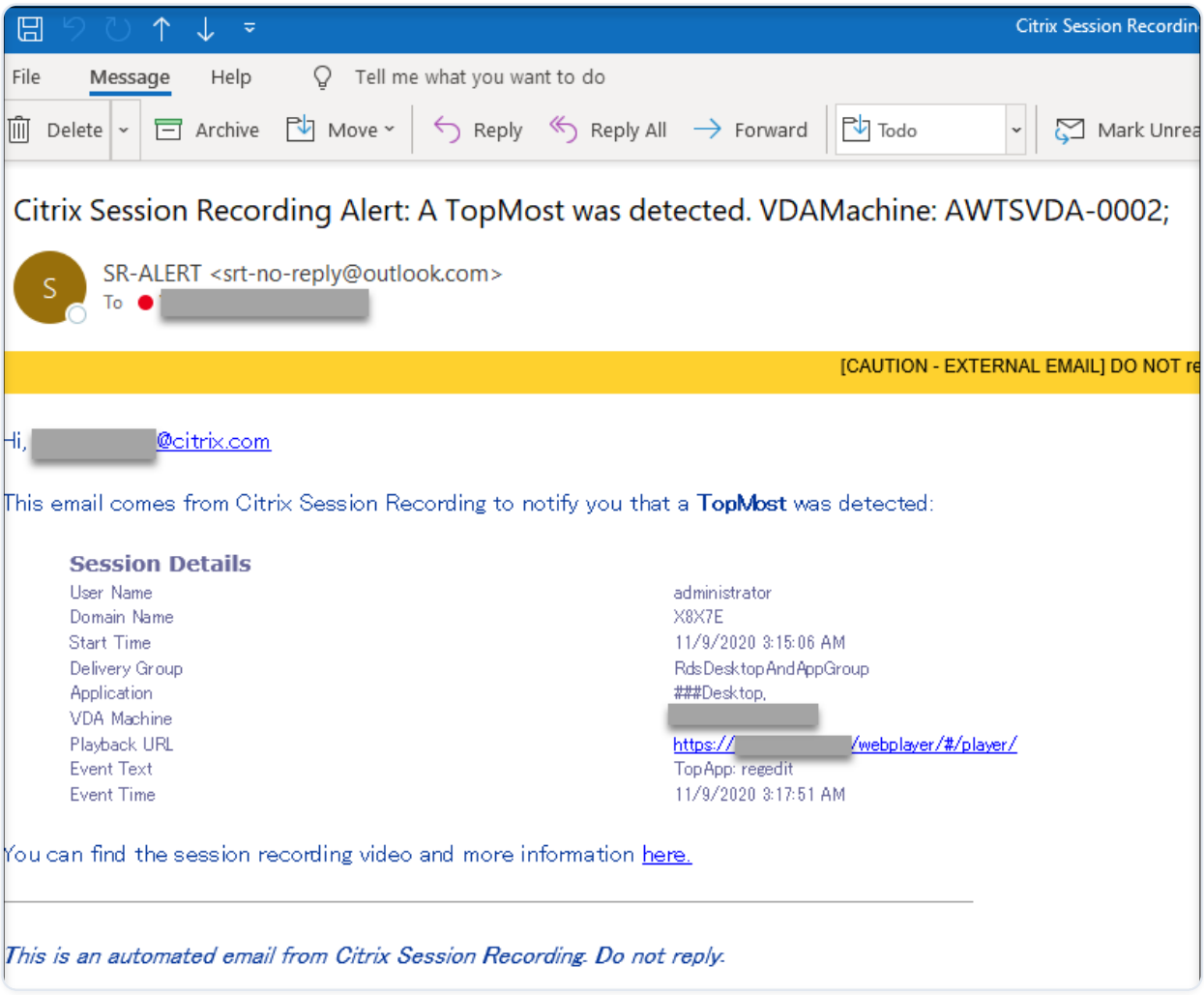
EVENT TYPE	DIMENSION	OPTION
App Start		
	App name	Includes, Equals, Matches
	Full command line	Includes, Equals, Matches
App End		
	App name	Includes, Equals, Matches
Top Most		
	App name	Includes, Equals, Matches
	Windows title	Includes, Equals, Matches
Web Browsing		
	URL	Includes, Equals, Matches
	Tab title	Includes, Equals, Matches
	Browser name	Includes, Equals, Matches
File Create		
	Path	Includes, Equals, Matches
	File size (MB)	Greater than, Between, Smaller than
File Rename		
	Path	Includes, Equals, Matches
	Name	Includes, Equals, Matches

EVENT TYPE	DIMENSION	OPTION
File Move		
	Source path	Includes, Equals, Matches
	Destination path	Includes, Equals, Matches
	File size (MB)	Greater than, Between, Smaller than
File Delete		
	Path	Includes, Equals, Matches
	File size (MB)	Greater than, Between, Smaller than
CDM USB		
	Drive letter	Equals
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		

EVENT TYPE	DIMENSION	OPTION
	Key name	Includes, Equals, Matches
Registry Set Value		
	Key name	Includes, Equals, Matches
	Value name	Includes, Equals, Matches
Registry Delete Value		
	Key name	Includes, Equals, Matches
	Value name	Includes, Equals, Matches
Registry Rename		
	Key name	Includes, Equals, Matches
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

EVENT TYPE	DIMENSION	OPTION
Popup Window		
	Process name	Includes, Matches
	Window content	Includes, Equals, Matches
Performance Data		
	CPU usage (%)	Greater than
	Memory usage (%)	Greater than
	Net send (MB)	Greater than
	Net receive (MB)	Greater than
	RTT (ms)	Greater than
Clipboard Operation		
	Data type	Equals (Text, File, Bitmap)
	Process name	Includes, Equals, Matches
	Content	Includes, Equals, Matches

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



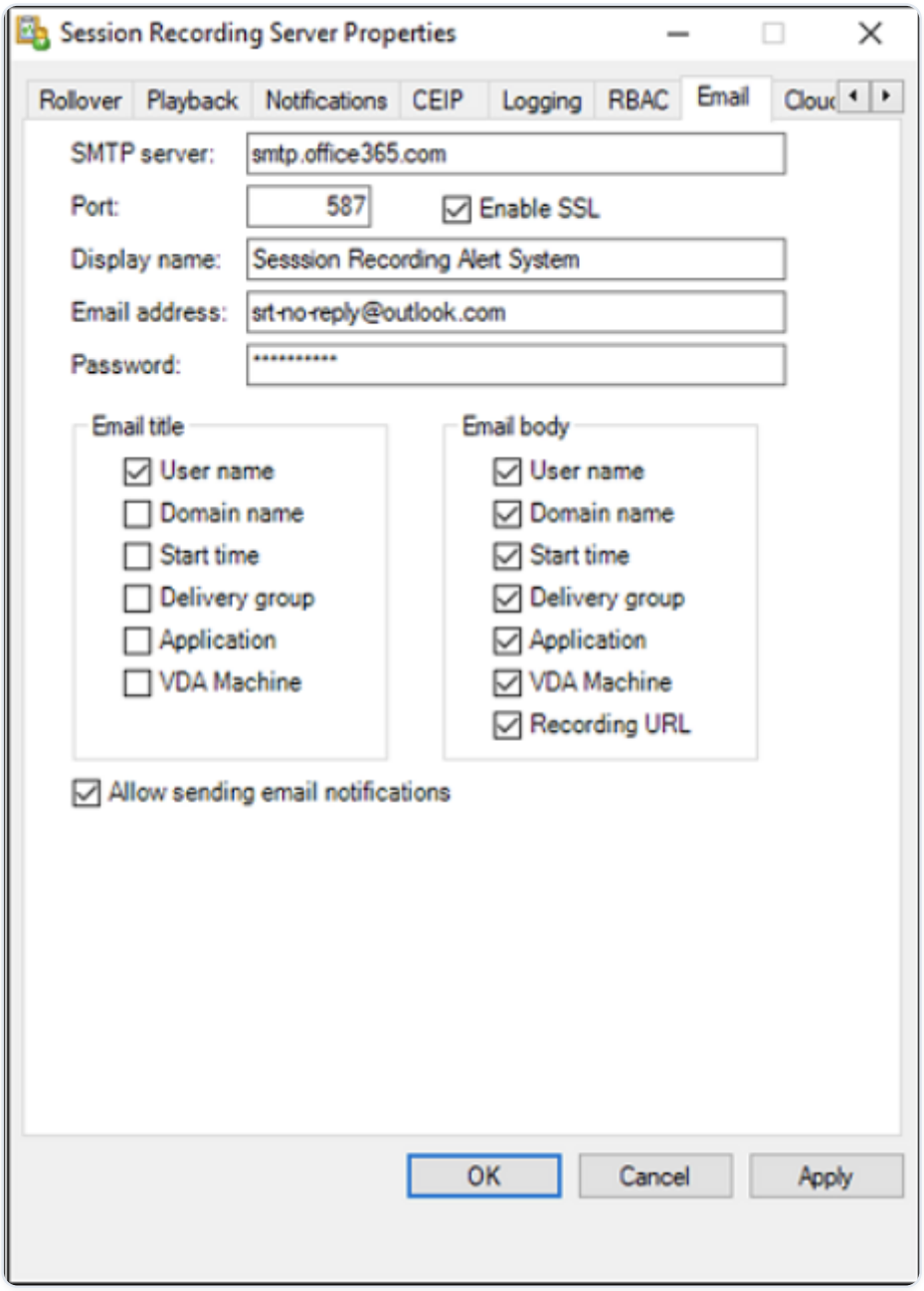
Tip:

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

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

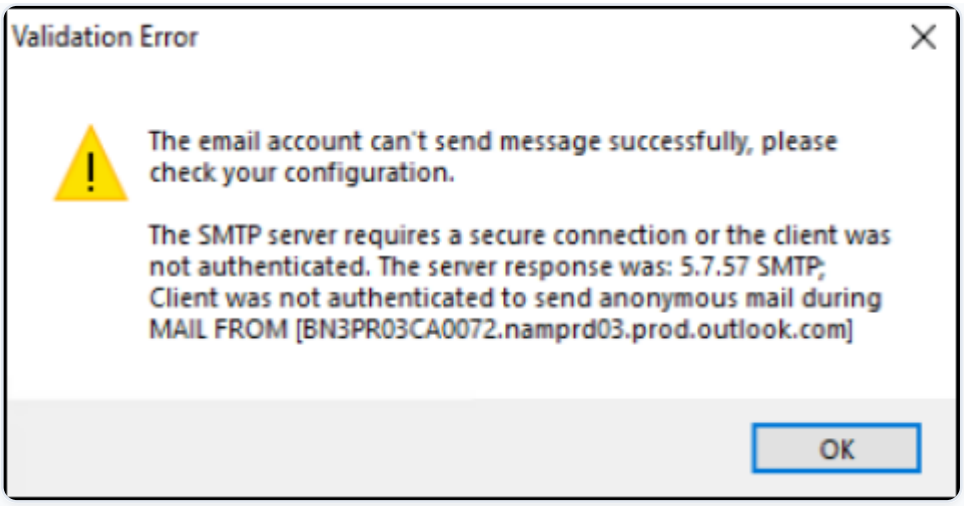
a. In the **Recipients** section of the **Events and responses** page, enter email addresses for the target recipients.

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

Note:

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

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

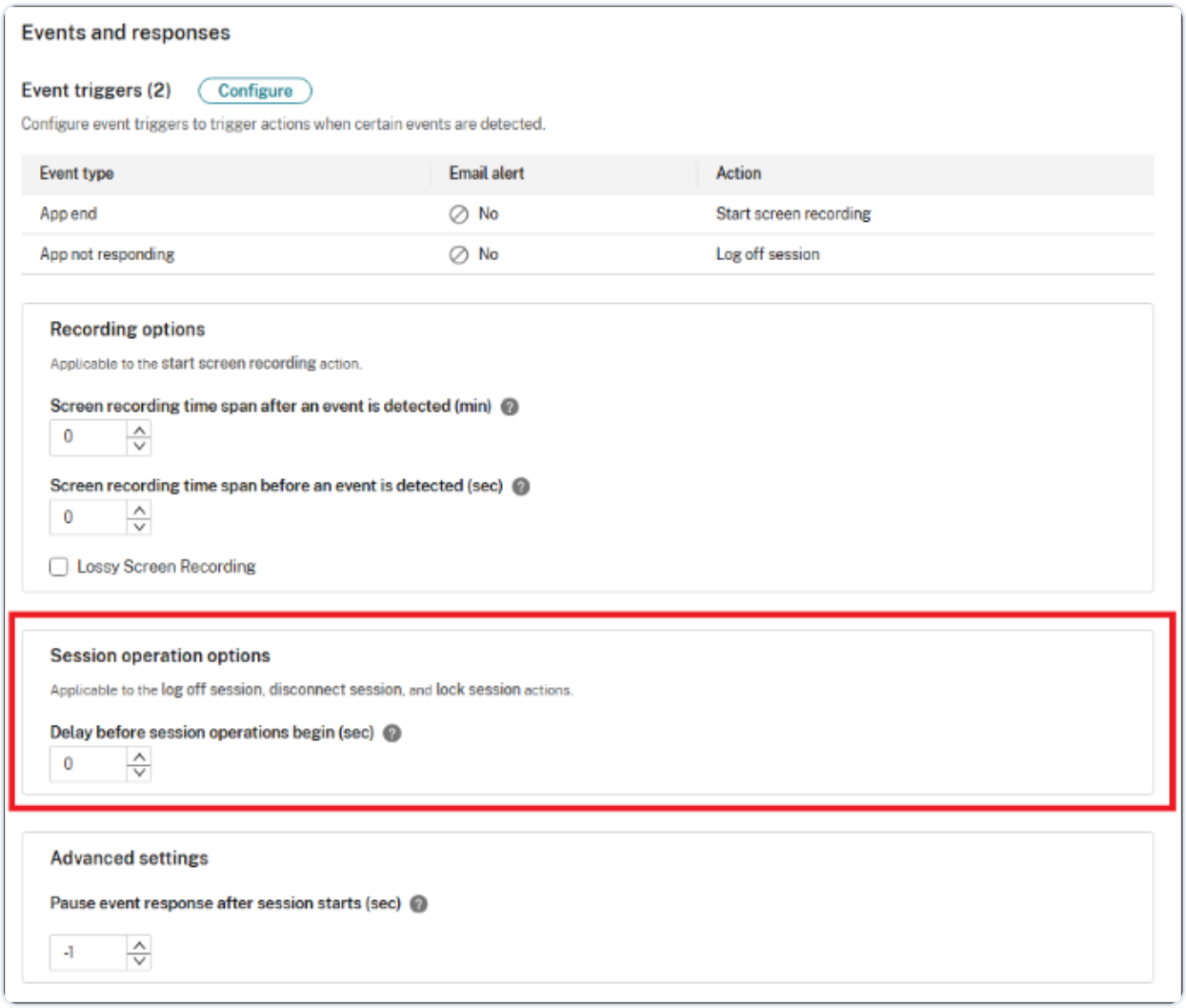
7. (Optional) To start screen recording immediately when certain events occur during an event-only recording, set the following options for dynamic screen recording in the **Recording options** section:

   - **Screen recording time span after an event is detected (min)**: You can configure the time duration (minutes) that you want to record the screen after events are detected. If you leave the value unspecified, screen recording continues until the recorded sessions end.
   - **Screen recording time span before an event is detected (sec)**: You can configure the time duration (seconds) of the screen recording you want to keep before events are detected. The value ranges from 1 to 120. Setting the value to any of 1 through 10 makes the value 10 effective. If you leave the value unspecified, the feature does not take effect. The actual length of the screen recording that Session Recording keeps might be a little longer than your configuration.
   - **Lossy screen recording**: You can specify whether to enable lossy screen recording when a session event is detected. Lossy screen recording lets you adjust compression options to reduce the size of recording files and to accelerate navigating recorded sessions during playback. This feature is available with Session Recording 2308 and later. For more information, see Enable or disable lossy screen recording.

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

   - Lock session
   - Log off session
   - Disconnect session

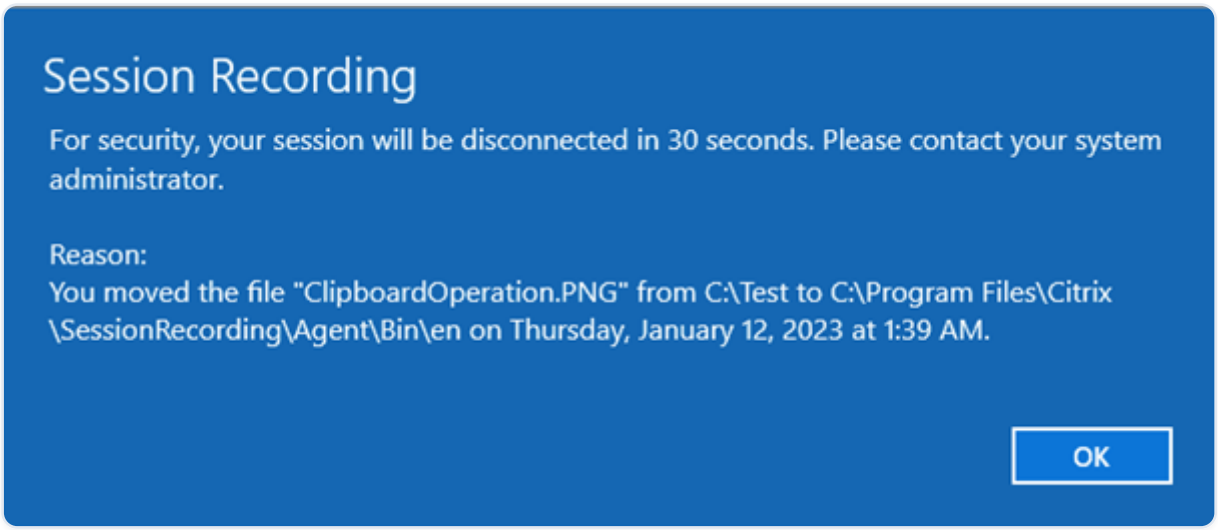
   For example:



Note:

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

For an example notice, see the following screen capture:



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

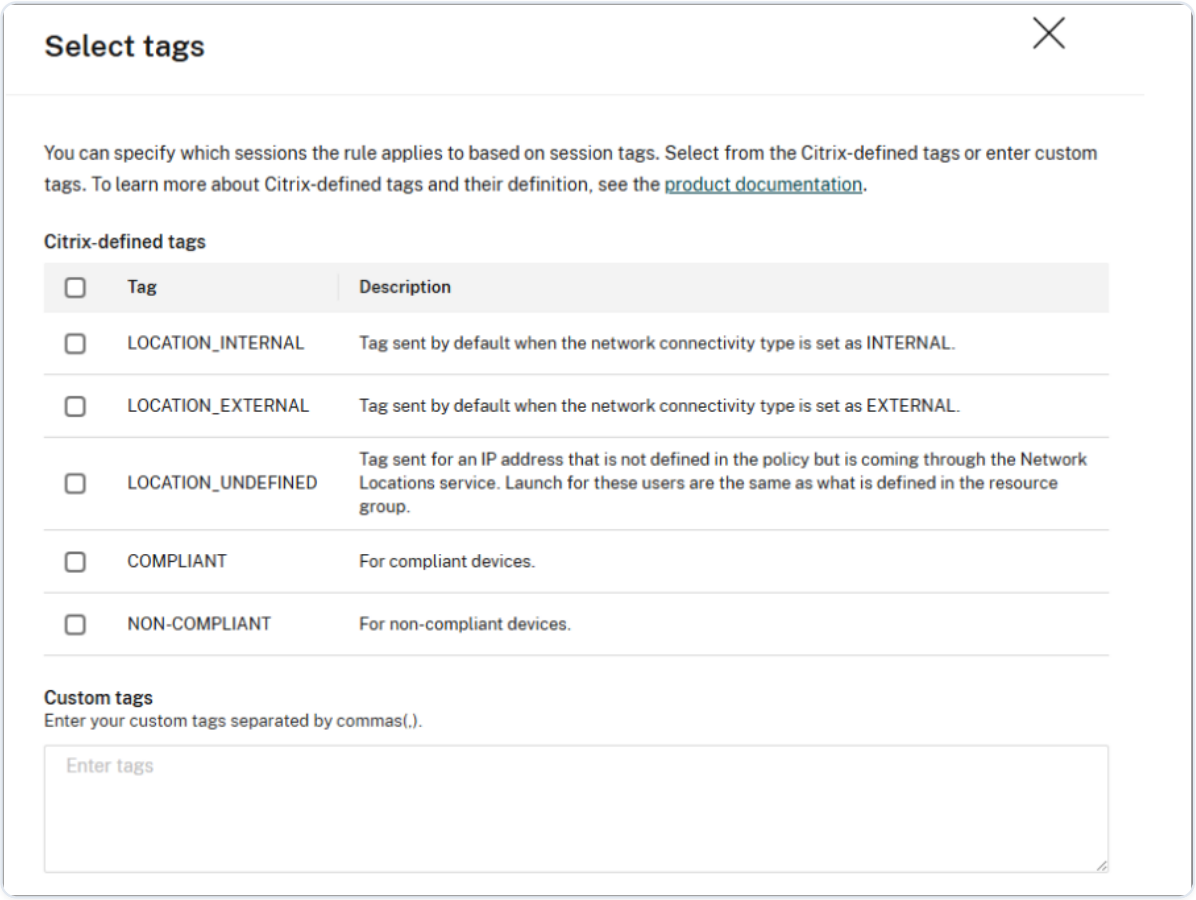
   Note:

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

10. Select and edit the rule scope.

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

    - **Users and user groups**. Creates a list of users and groups to which the responses of the rule apply.
    - **Published applications and desktops**. Creates a list of published applications and desktops to which the responses of the rule apply.
    - **Delivery groups and VDA machines**. Creates a list of delivery groups and VDA machines to which the responses of the rule apply.
    - **IP addresses and IP address ranges**. Creates a list of IP addresses and ranges of IP addresses to which the responses of the rule apply. The IP addresses mentioned here are the IP addresses of the Citrix Workspace™ apps.
    - **Filter**. Creates a list of smart access tags to which the rule applies. You can configure contextual access (smart access) using smart access policies on Citrix NetScaler.



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

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

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

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

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

Configure endpoint recording policies

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

Prerequisites

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

- Citrix Session Recording server version 2503 or later
- Citrix Workspace App version 2503 or later
- Proper integration with Citrix Gateway and StoreFront, see Site settings

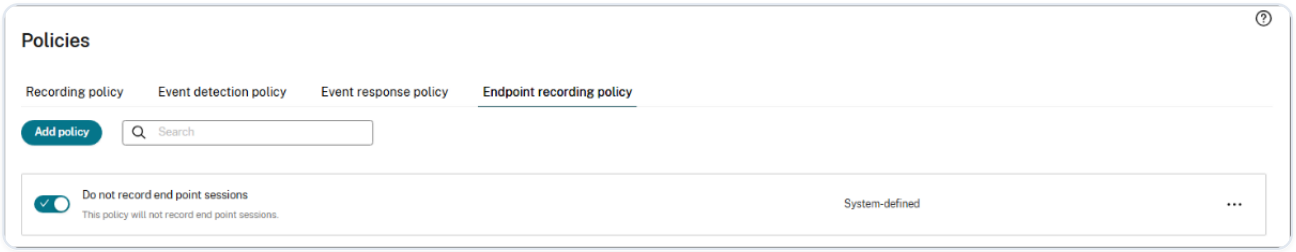
Configure endpoint recording policies

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

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

System-defined endpoint recording policies

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



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

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

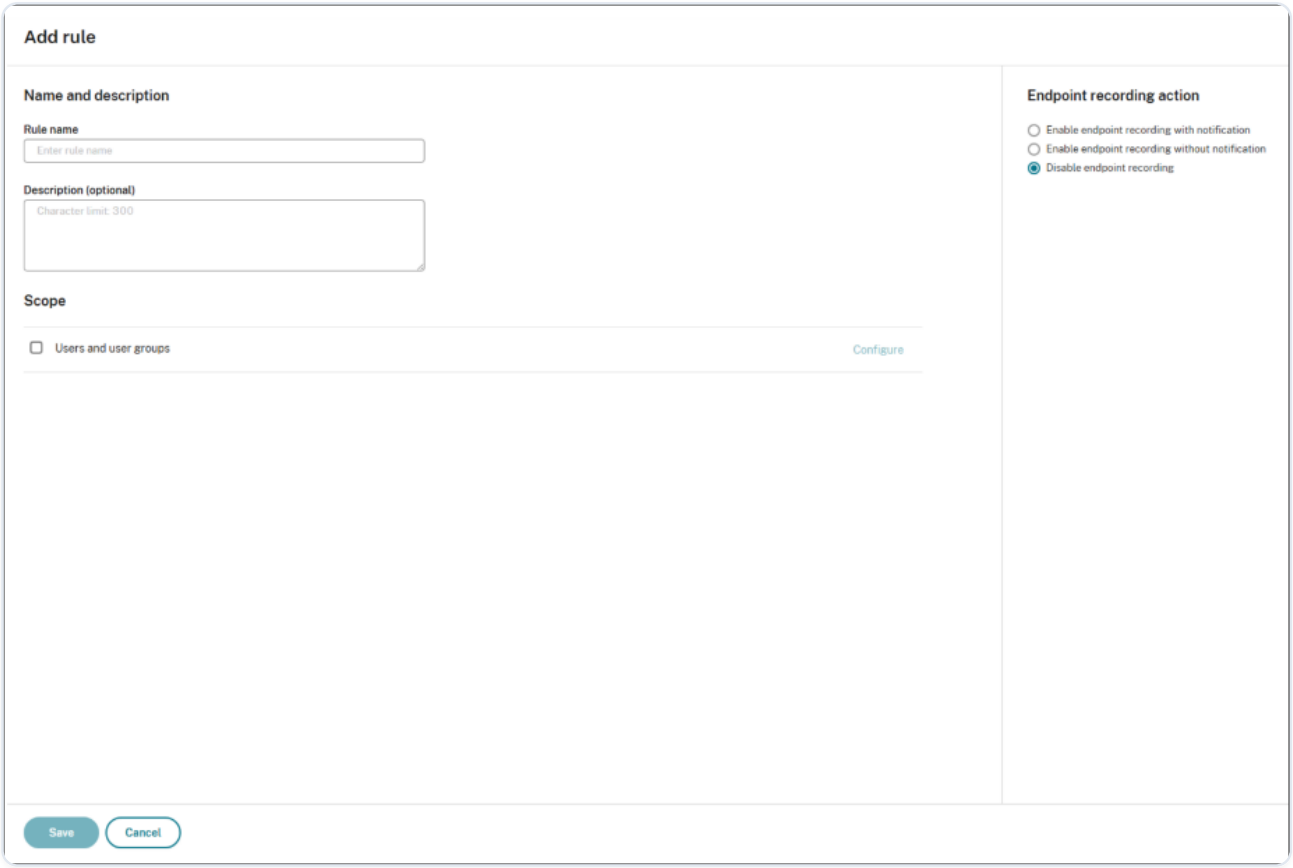
Create a customer endpoint recording policy

Considerations

You can record endpoint sessions of specific users or groups.

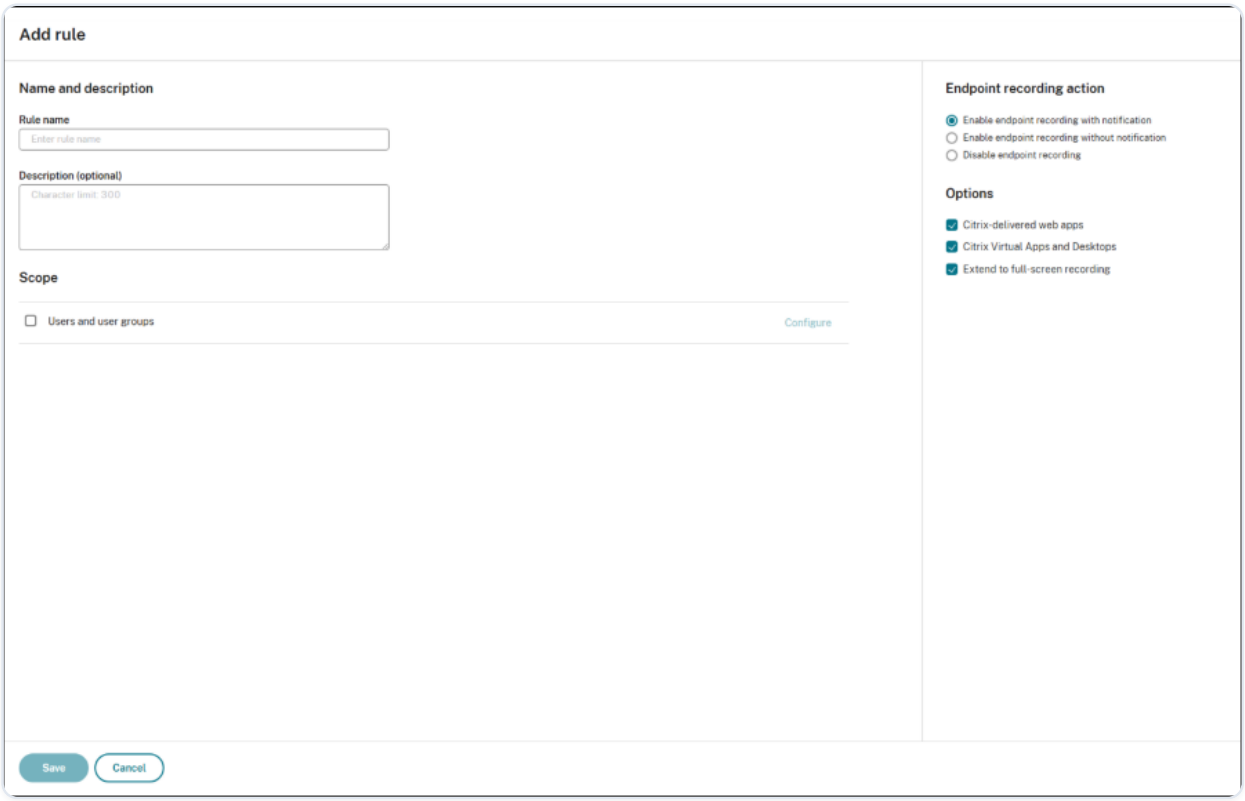
For each rule you create, you specify an endpoint recording action and a rule scope. The recording action applies to sessions that fall into the rule scope.

For each rule, choose one endpoint recording action:



- **Enable endpoint recording with notification**. This option records user actions on endpoint devices. Users receive recording notifications in advance. With this option selected, you can further select to enable recording for Citrix-delivered web apps or Citrix Virtual Apps and Desktops. Additionally, you can choose to extend to full-screen record in endpoint recording.
- **Enable endpoint recording without notification**. This option records user actions on endpoint. Users do not receive recording notifications. With this option selected, you can further select to enable recording for Citrix-delivered web apps or Citrix Virtual Apps and Desktops. Additionally, you can choose to extend to full-screen record in endpoint recording.
- **Disable endpoint recording**. This option means that no user actions on endpoint devices are recorded.

- **Citrix-delivered web apps**. This option lets you record user actions on endpoint devices accessing these apps.
- **Citrix Virtual Apps and Desktops**. This option lets record user actions on endpoint devices accessing these apps.
- **Extend to full-screen recording**. This option lets you record the entire screen space, including any extended displays.



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

Users and user groups. Creates a list of users and user groups to which the action of the rule applies.

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

The recording action of a rule determines its priority:

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

- Rules with the **Enable endpoint recording without notification** action have the lowest priority.

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

STEPS

1. Log on as an authorized Policy Administrator to the Session Recording web console.
2. Select **Policies** from the left navigation.
3. Select the **Endpoint recording policy**.
4. Click **Add policy**.
5. Enter a name and description for the new policy, and then click **Add rule**.
6. Enter a **name** and **description** for the rule. Specify an endpoint recording action and choose at least one of the following items to create the rule scope.

   For each rule, specify a recording action:

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

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

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

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

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 or FQDN 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 does not function as expected if the Session Recording database is stopped or in a state of failure. If the Session Recording Administrator Logging database is stopped or experiencing failure, the administrator logging feature becomes unavailable and this prevents you from being able to modify policies or change server properties when mandatory blocking is enabled. Therefore, it is advisable to implement a high availability (HA) mode for the databases.

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

You can 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 Virtual Delivery Agents (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:

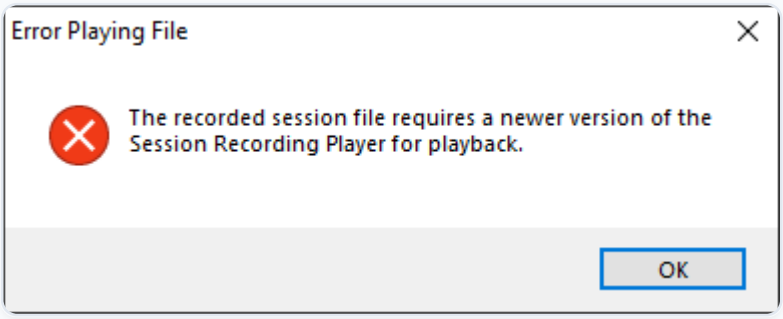
- Launch the Session Recording player
- Enable or disable live session playback
- Enable or disable playback protection
- Search for recordings
- Open and play recordings
- Cache recordings
- Highlight idle periods
- Use events and bookmarks

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.

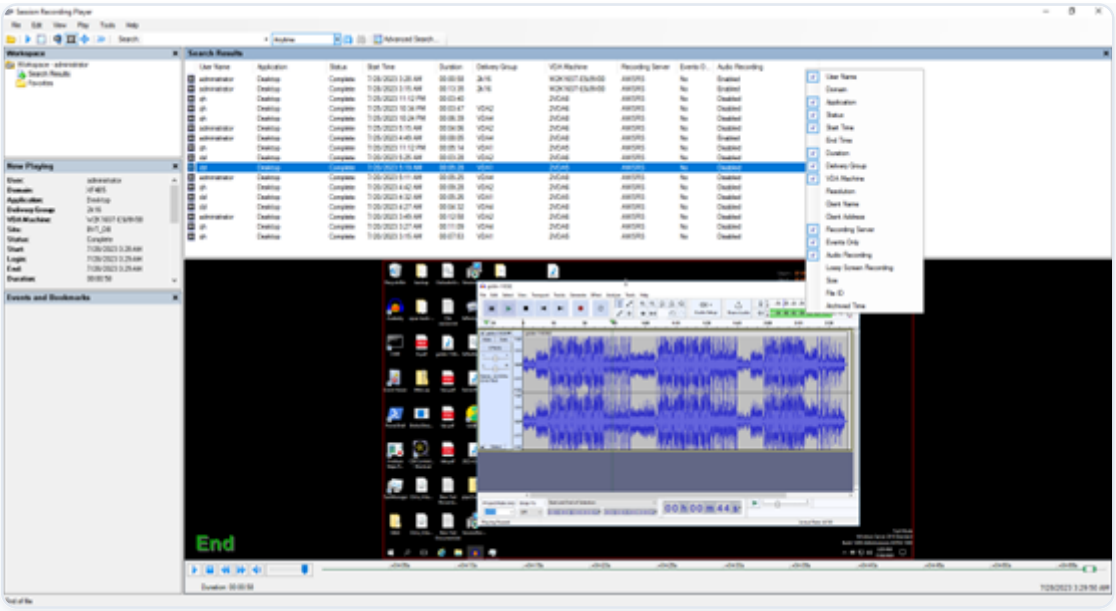


- If playback justification logging is enabled, each time you play a recording, a dialog box appears, asking you to enter a playback justification. For more information, see Playback logging.

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.

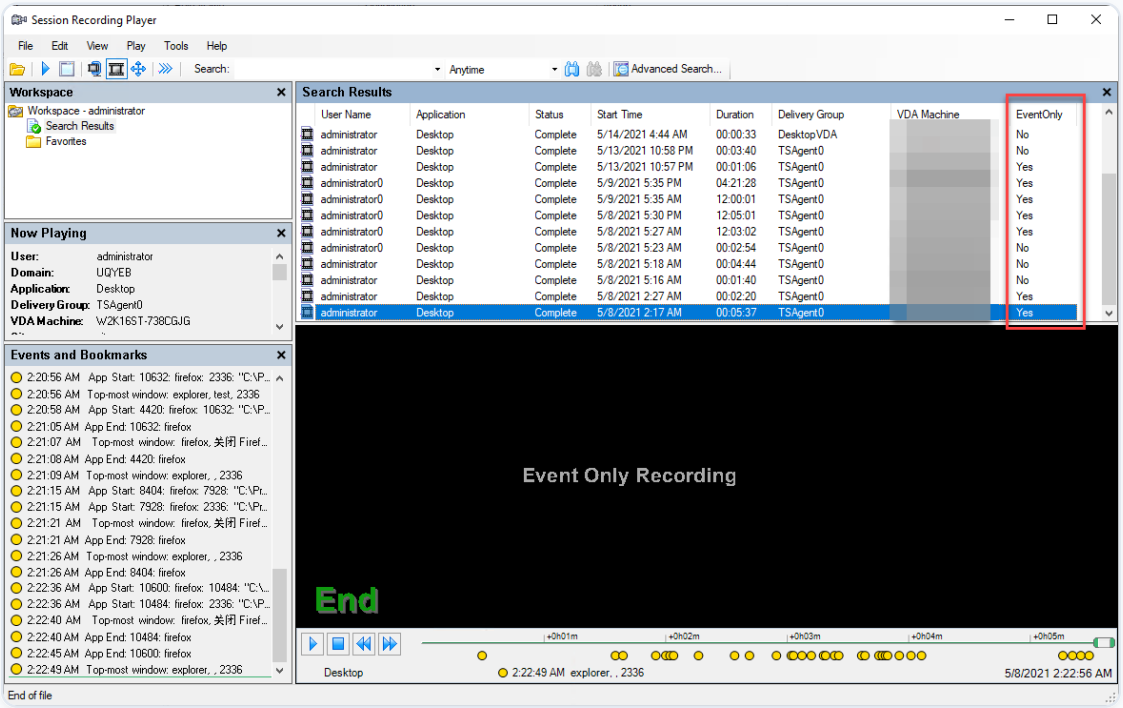
Tip:

- To customize columns to display, right-click the table header.

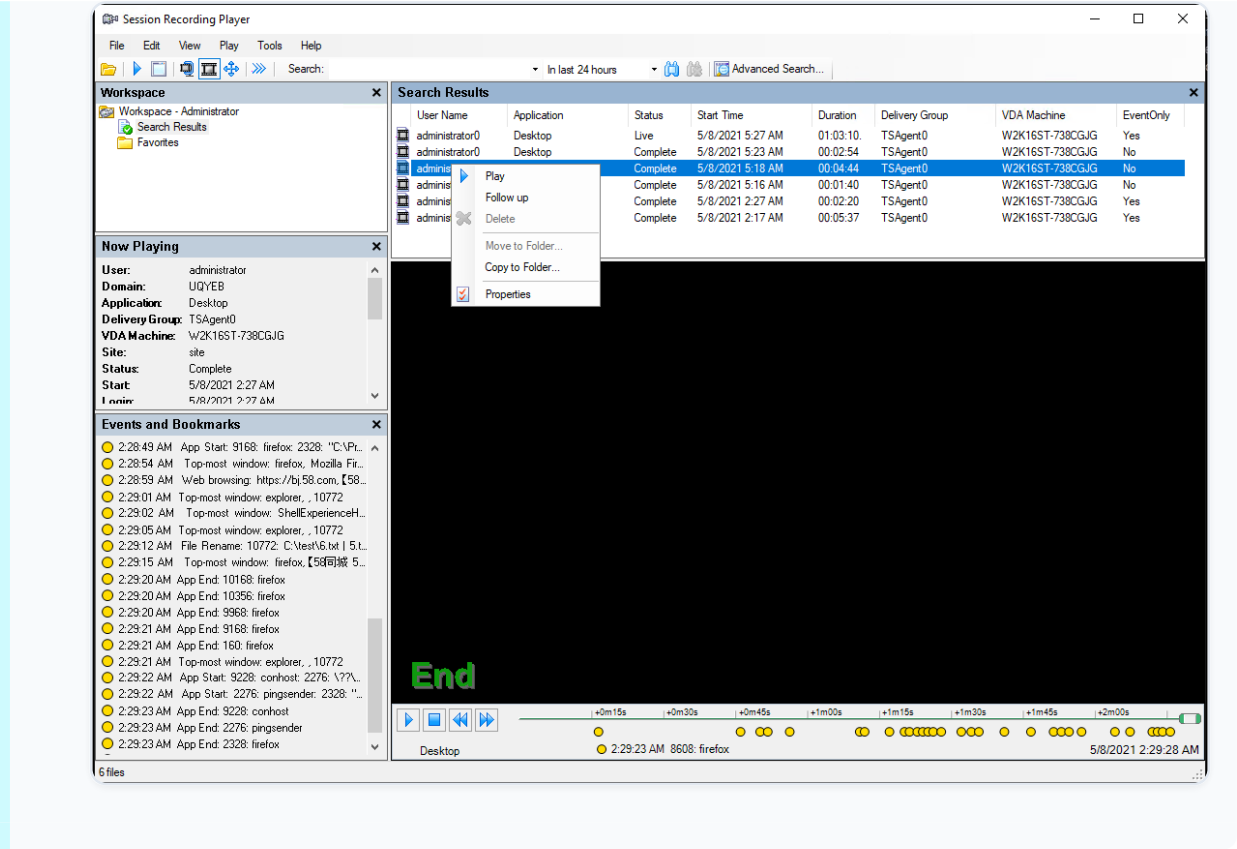


- The **Audio Recording** column indicates whether audio in the recorded session is available during playback.
- The **EventOnly** column indicates a screen recording or an event-only recording.

  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 the 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 the 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

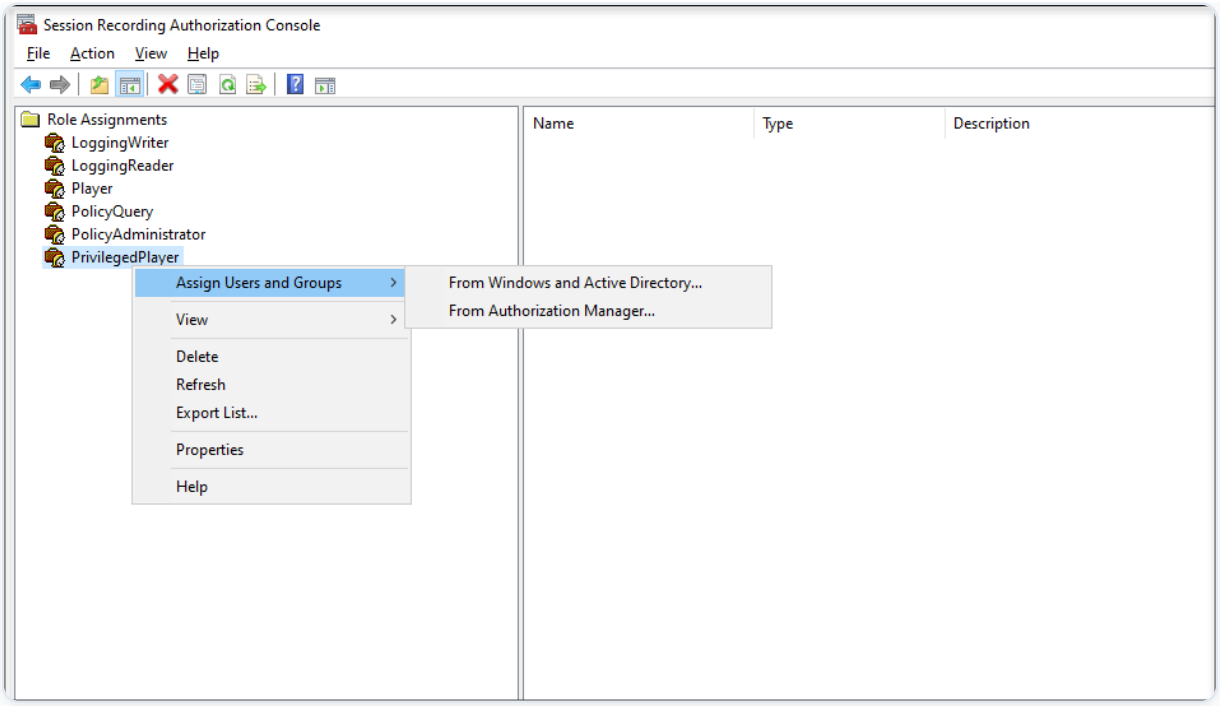
The Session Recording player search options allow you to limit the maximum number of session recordings that appear in search results and to specify whether search results include archived session files.

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.

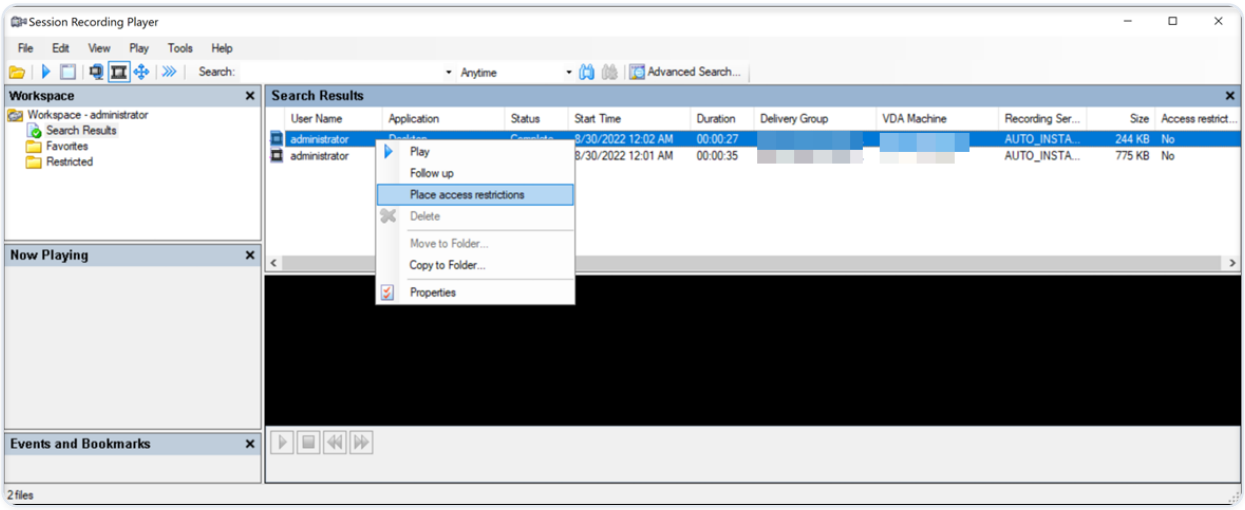


The following section walks you through the process of placing and removing access restrictions on target recordings.

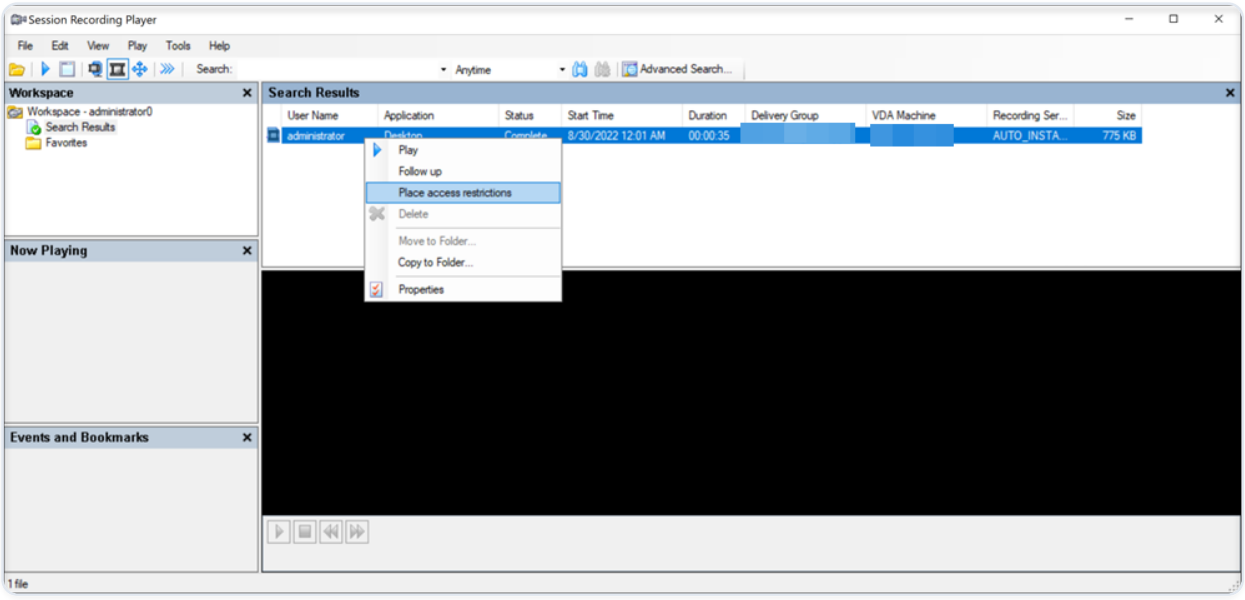
1. Log on to the machine where the Session Recording player is installed.
2. From the **Start** menu, choose **Session Recording Player**.
3. Select **Search Results** in the **Workspace** pane.
4. In the **Search Results** area, select one or more target recordings.
5. Right-click and select **Place 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.

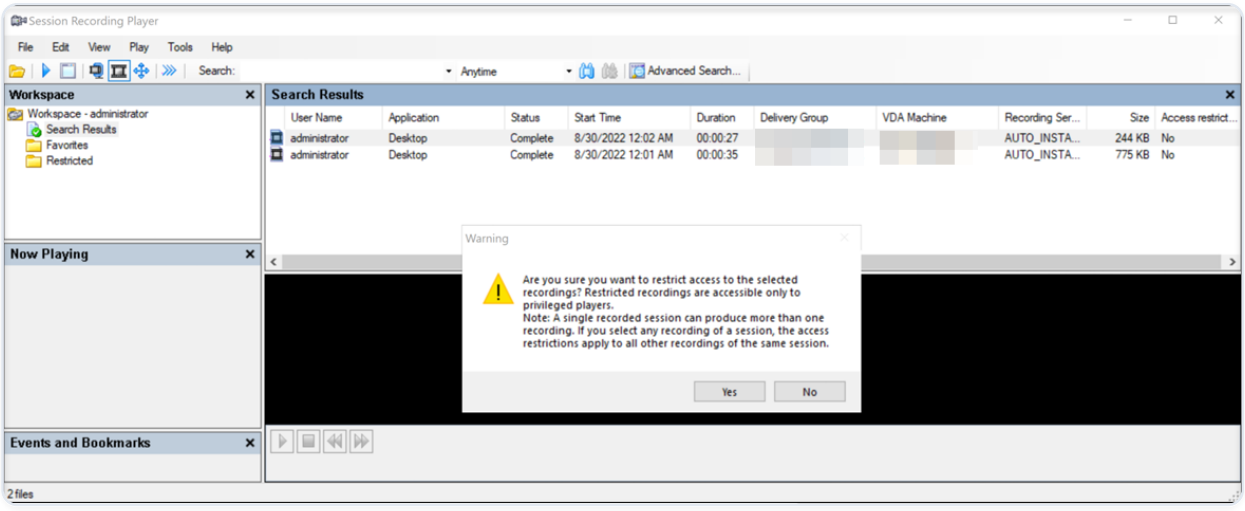
   View for the **PrivilegedPlayer** role:



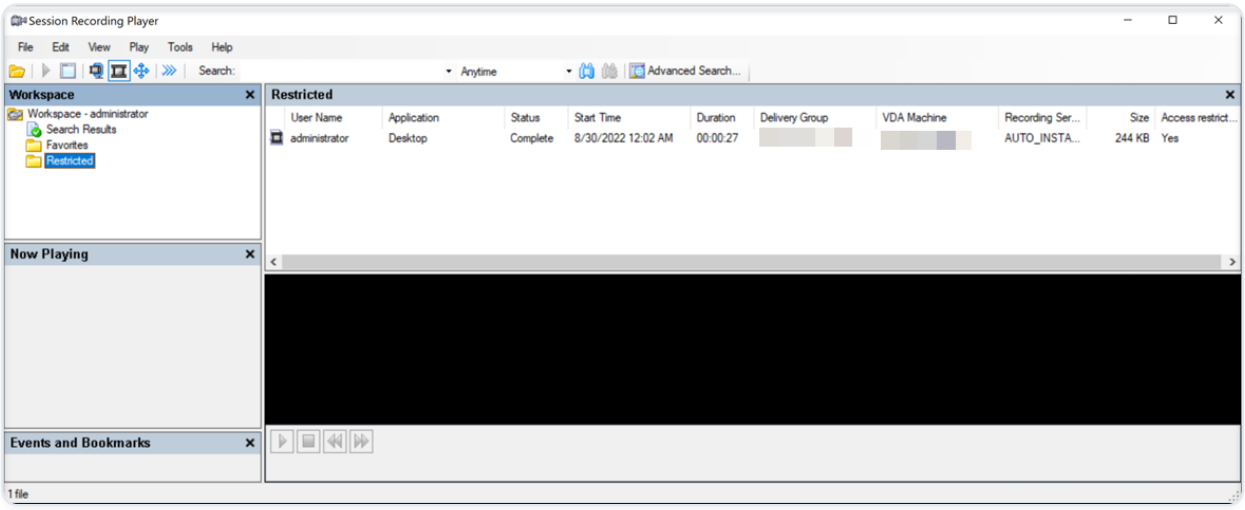
View for the **Player** role:



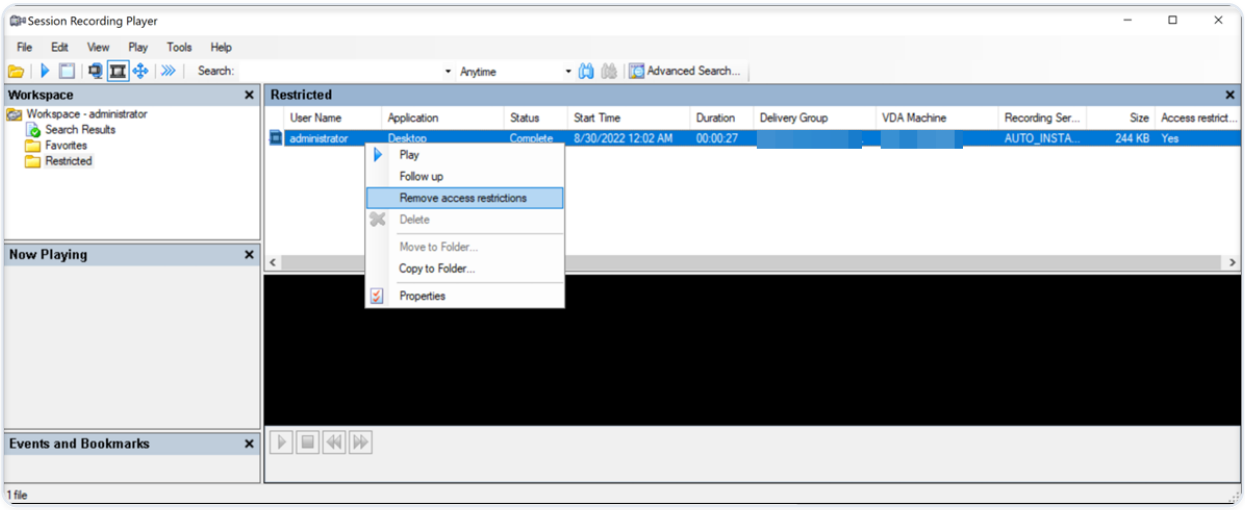
6. Click **Yes**.



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

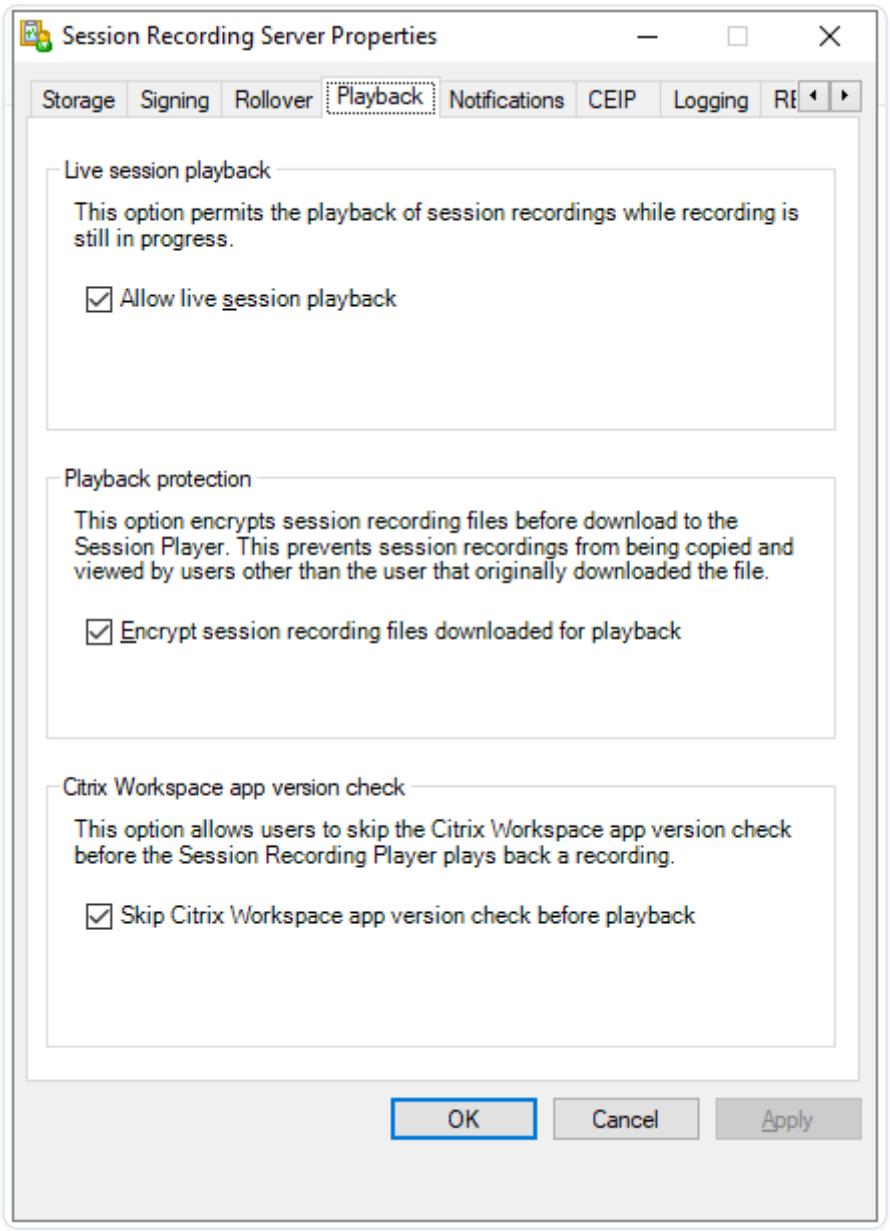
You can open session recordings in the Session Recording player in three ways:

- 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.

If playback justification logging is enabled, each time you play a recording, a dialog box appears, asking you to enter a playback justification. For more information, see Playback logging.

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 a severity for each comment.
- 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.

> **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.

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

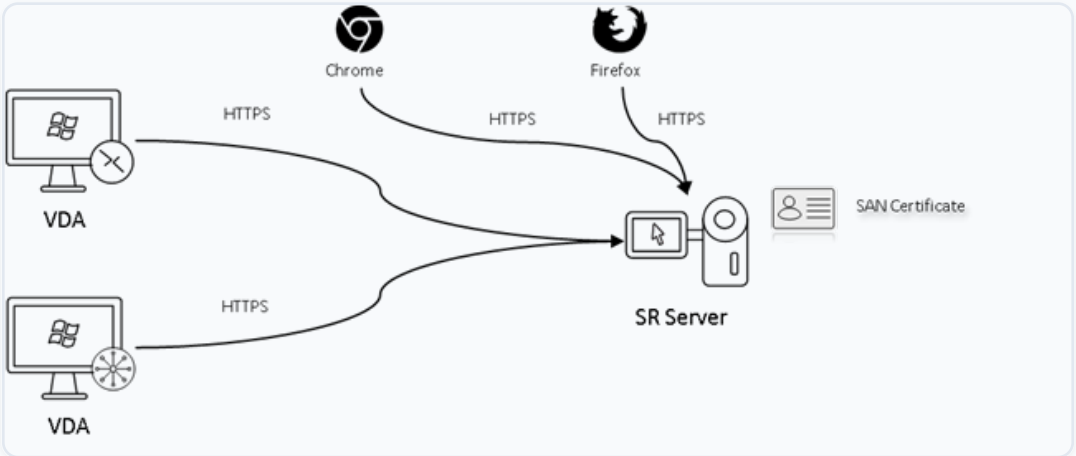
The URL of the web player website is `http(s)://<FQDN of Session Recording server>/WebPlayer`. To ensure the use of HTTPS, add an SSL binding to the website in IIS.

> **Note:**
>
> When logging on to the web player website, domain users do not need to enter credentials while non-domain users must.

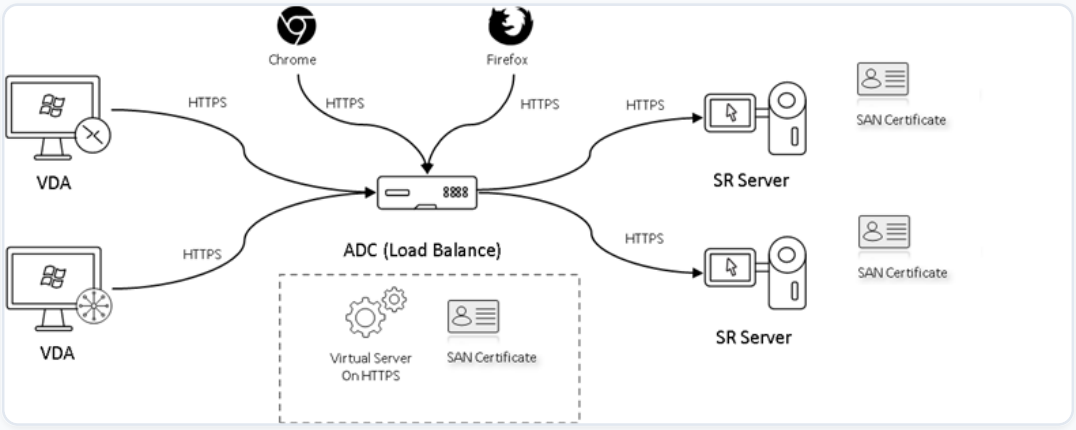
To use HTTPS to access the web player website, complete the following steps:

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.



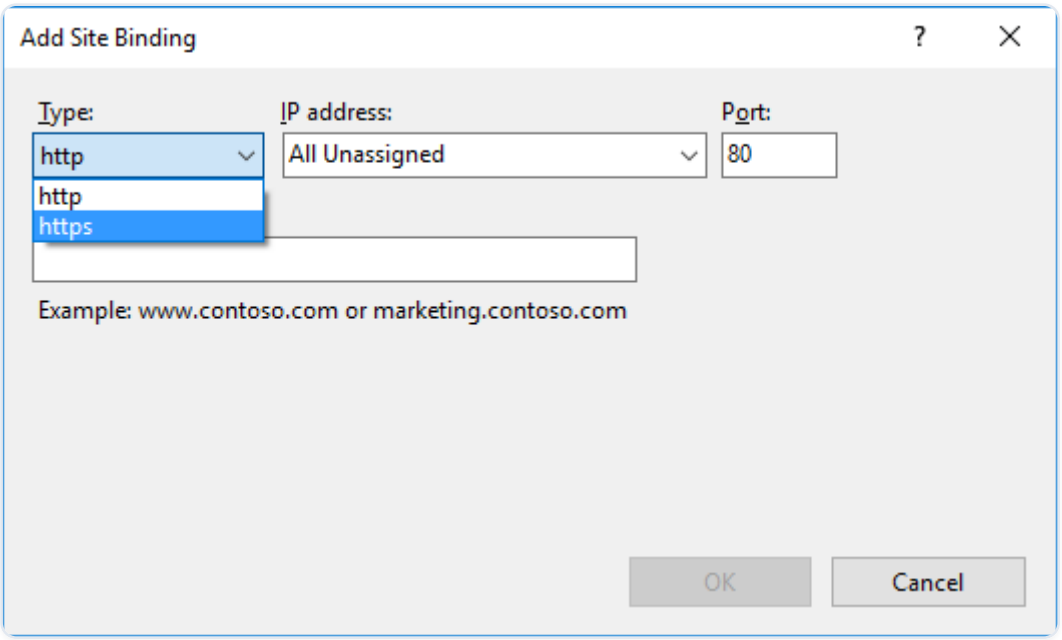
- When load balancing is in use, ensure that a SAN certificate is available both on Citrix ADC and on each Session Recording Server.

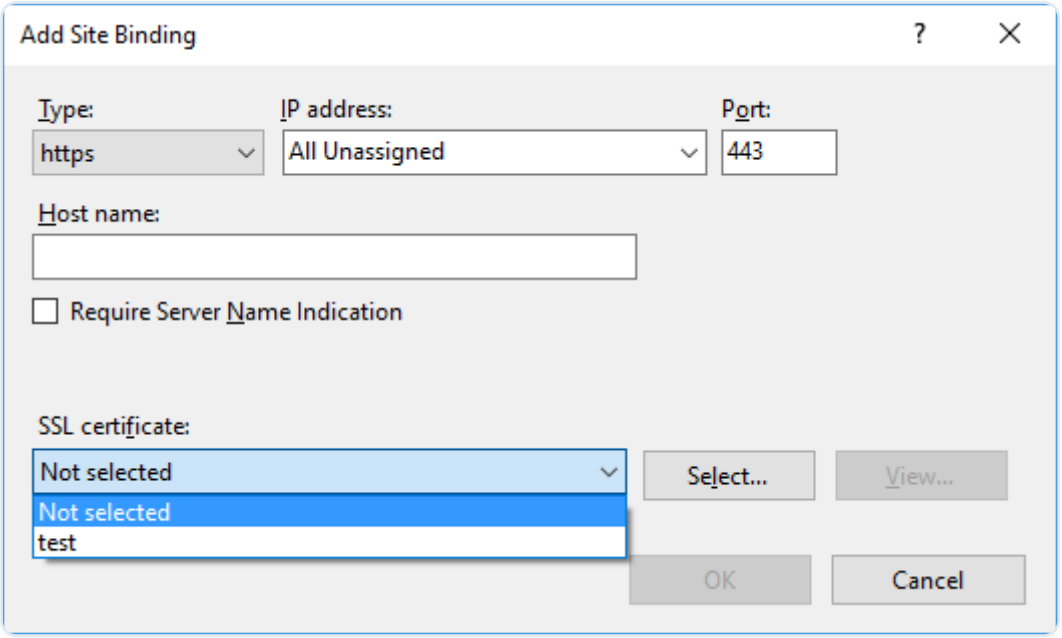


b. On IIS, right-click the website and select **Add Bindings**. The **Site Bindings** dialog box appears.

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.

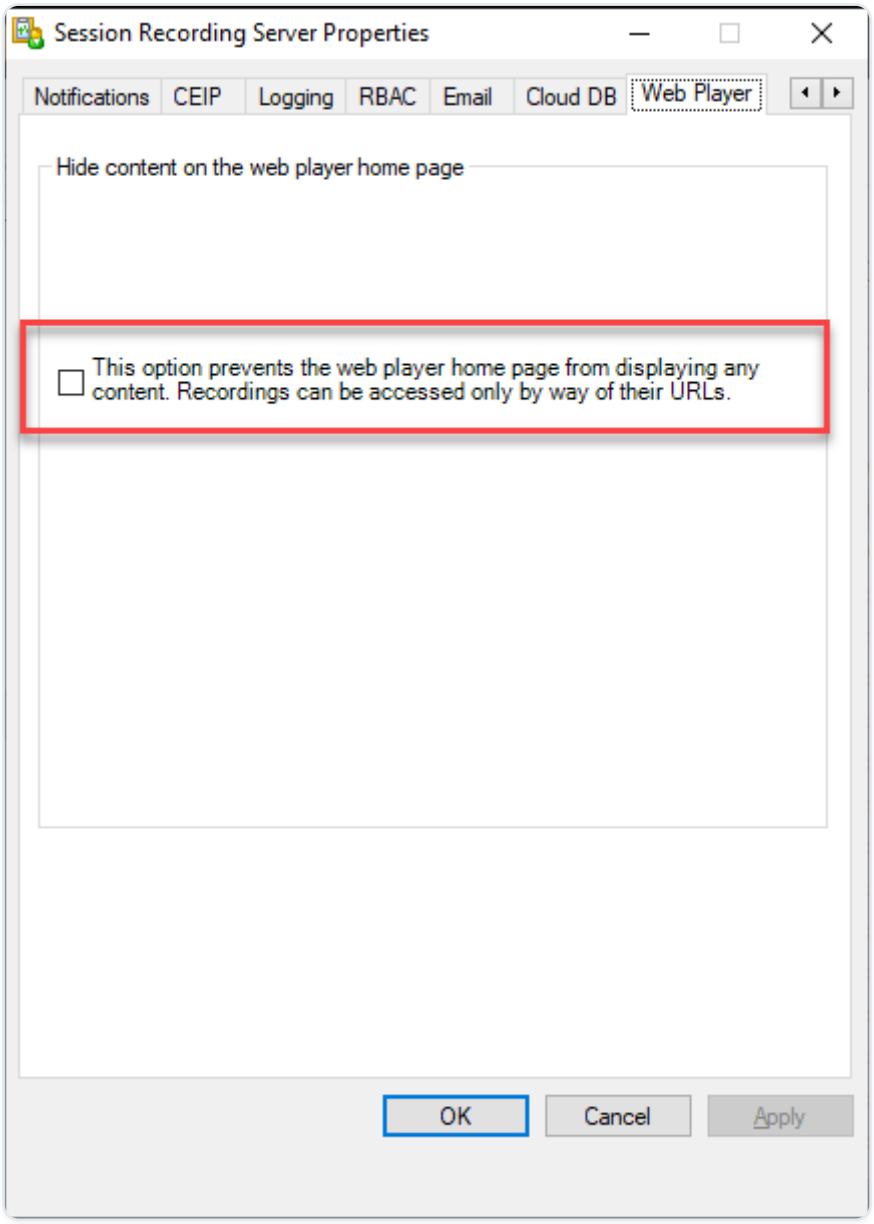




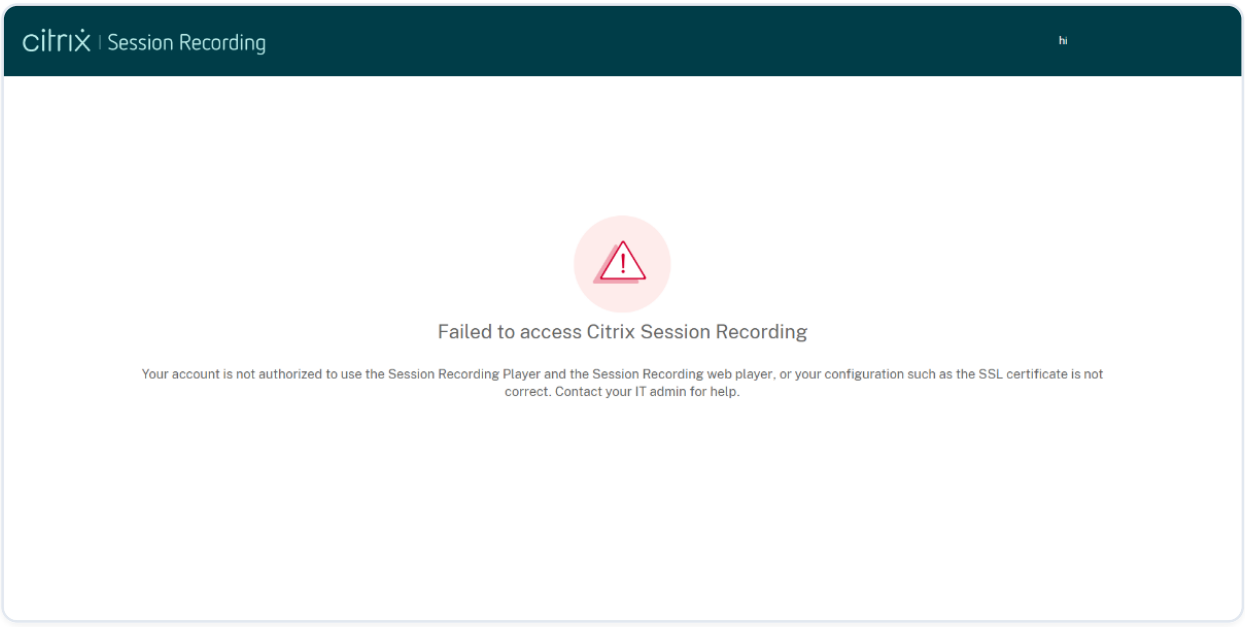
e. Click **OK**.

Hide or show content on the web player home page

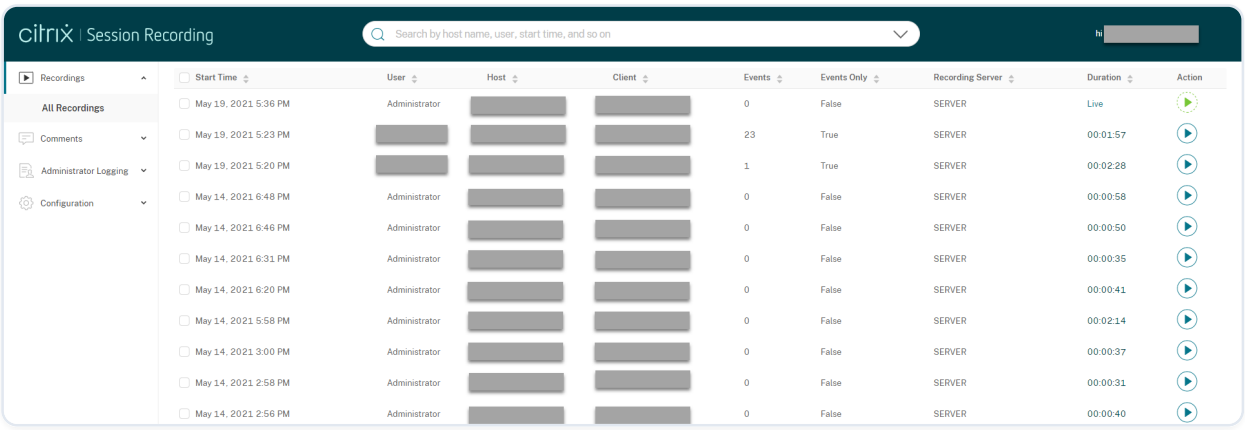
After you log on, the web player home page might hide or show content based on whether the following option is selected in **Session Recording Server Properties**.



- 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.



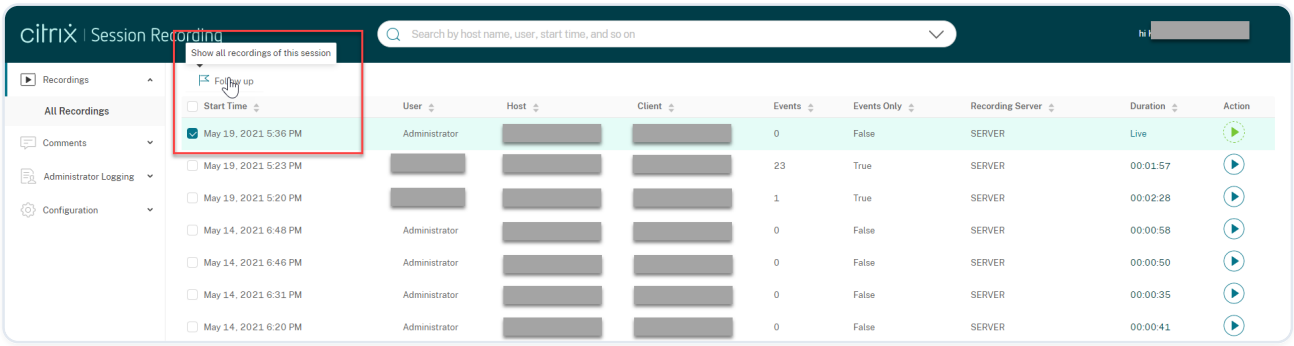
- With the option unselected, the web player home page shows content similar to the following screen capture. Click **All Recordings** in the left navigation to refresh the page and display new recordings if there are any. Scroll down the webpage to select recordings to view or use filters to customize your search results. For live recordings, the **Duration** column shows **Live** and the play button appears green.



Note:

Starting with 2411, the **Diagnostic Logging** menu is available in the left navigation. For more information, see View diagnostic logging.

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.

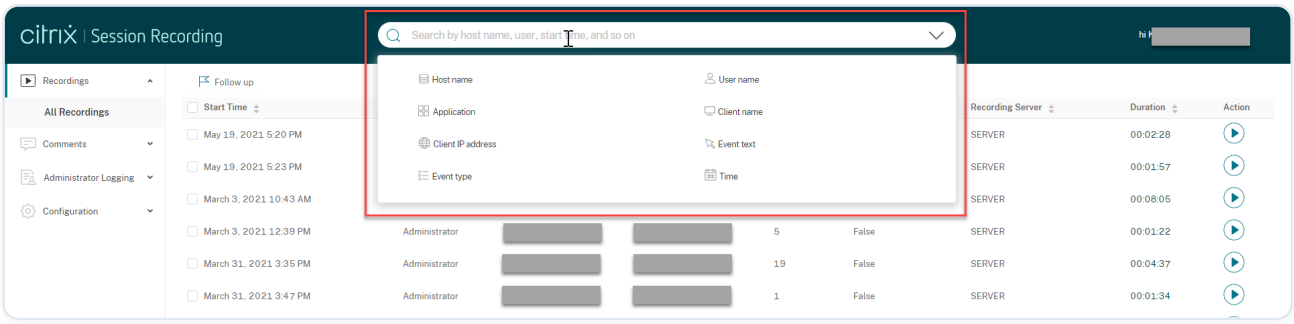
ITEM	DESCRIPTION
Start time	The recording start time. Click the up and down arrows to list recordings in chronological order.
User	The user whose session was recorded. Click the up and down arrows to concentrate recordings of a user on the list and arrange users in alphabetical order.
Host	The host name 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.

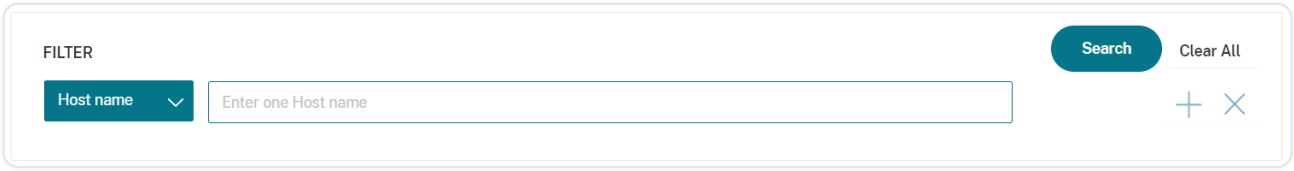
Search for recordings

Search for recordings by using filters

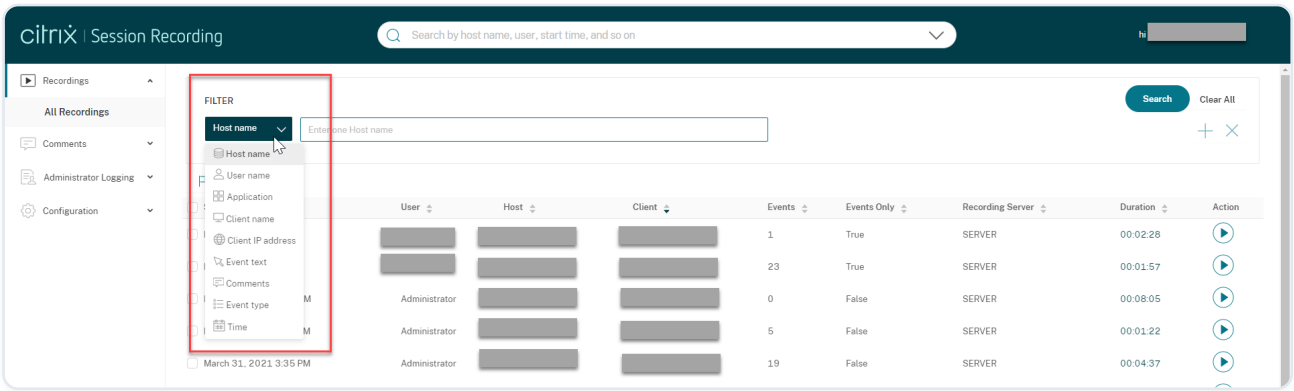
You can search for recordings by using filters in the web player. The available filters include host name, client name, user name, application, client IP address, event text, event type, and time.



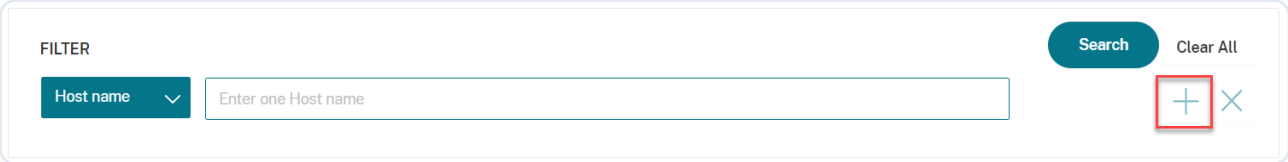
For example, after you select the host name filter, the following dialog box appears. Type in the host name (of the VDA where recorded sessions are hosted) and click **Search** to filter out irrelevant recordings and display only the relevant ones.



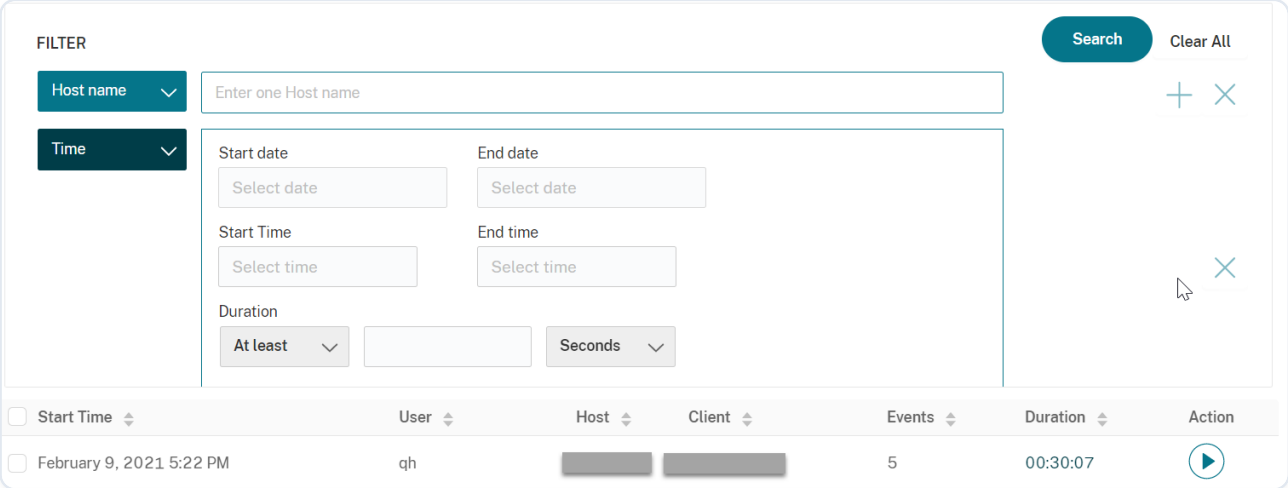
You can change to a different filter by clicking the currently selected **Host name**, as shown in the following screen capture. All filters are listed after you click **Host name**. Select a different filter as needed.



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.

Show all recordings of a session

There are two ways to show all recordings of a session in the Session Recording web player:

Method 1:

Select a recording and click the **Follow up** button to show all recordings of the recorded session.

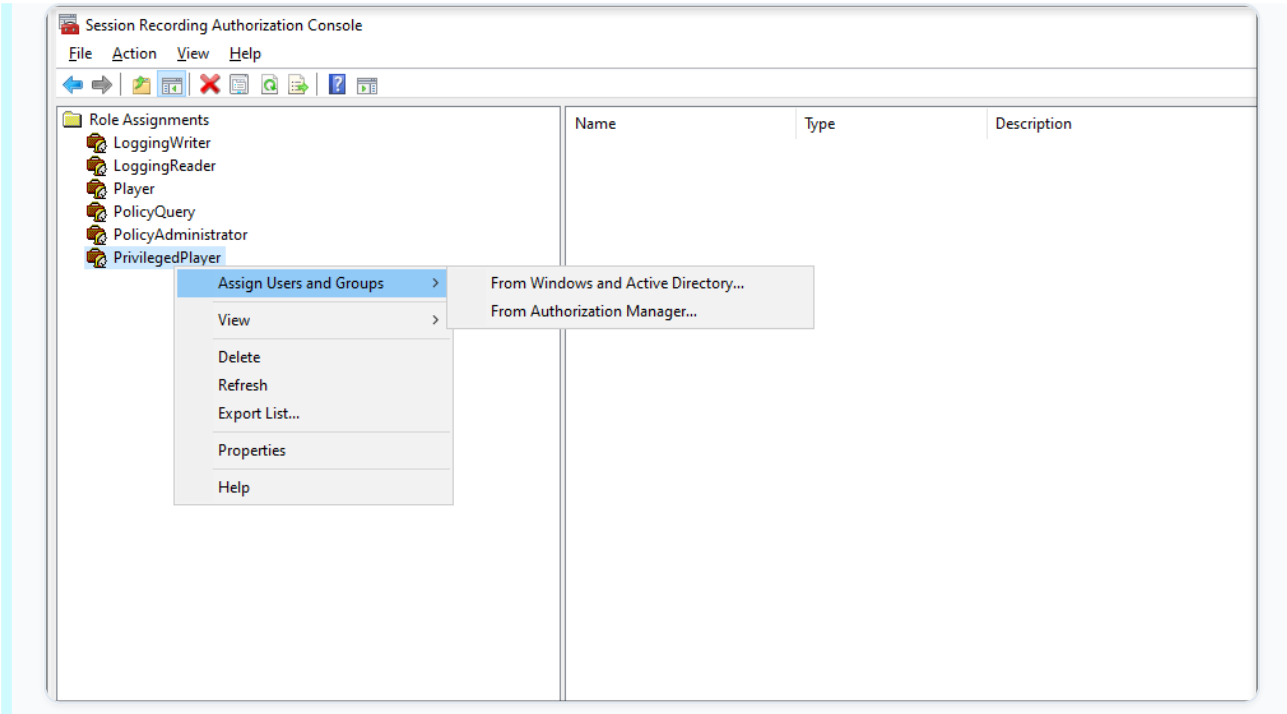
Method 2:

Select a recording to play and click **View playlist** in the upper right corner of the playback page.

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.

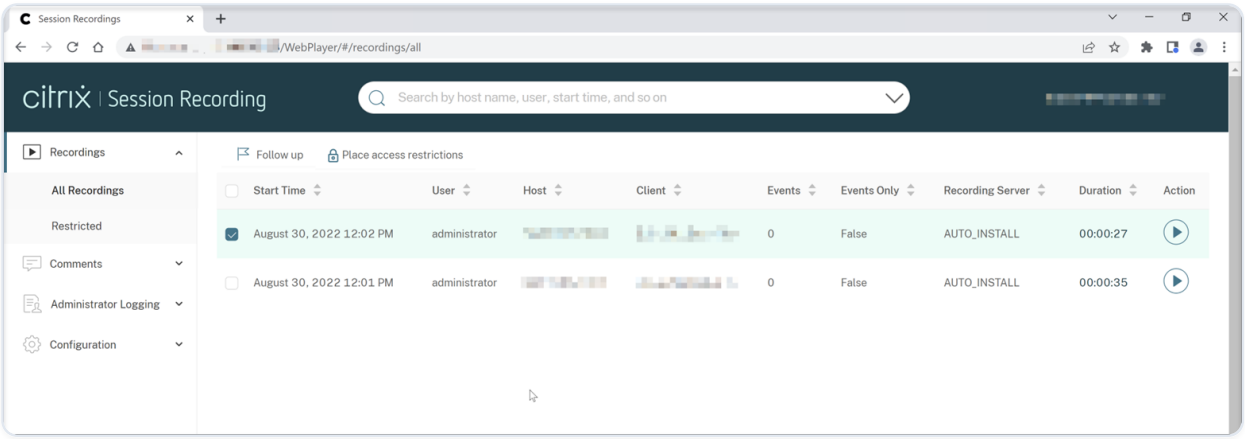
1. Enter the URL of your web player website in the address bar of a supported browser.

   The URL format is **http(s)://<FQDN of Session Recording server\>/WebPlayer**.

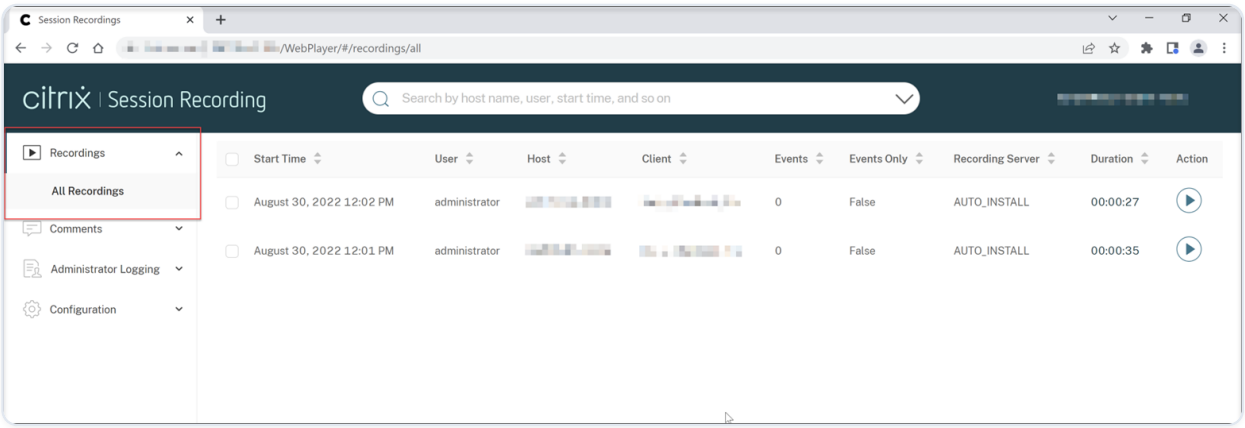
   Supported browsers include Google Chrome, Microsoft Edge, and Firefox.
2. In the left navigation of the web player page, expand the **Recordings** menu.
3. On the **All Recordings** page, select one or more target recordings.
4. Click the **Place access restrictions** icon on top of the recording list.

   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.

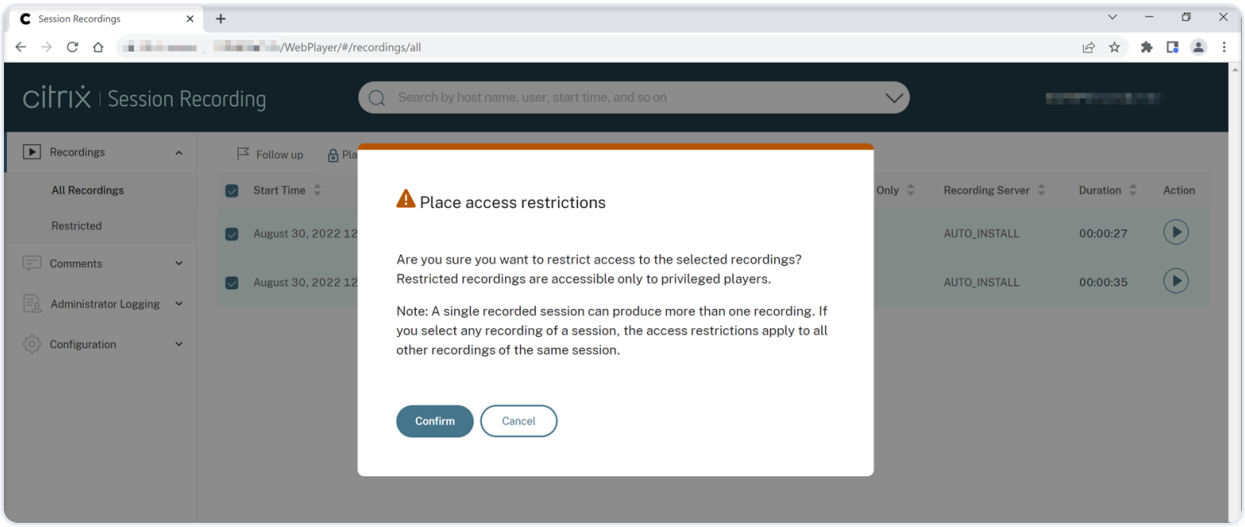
   View for the **PrivilegedPlayer** role:



View for the **Player** role:

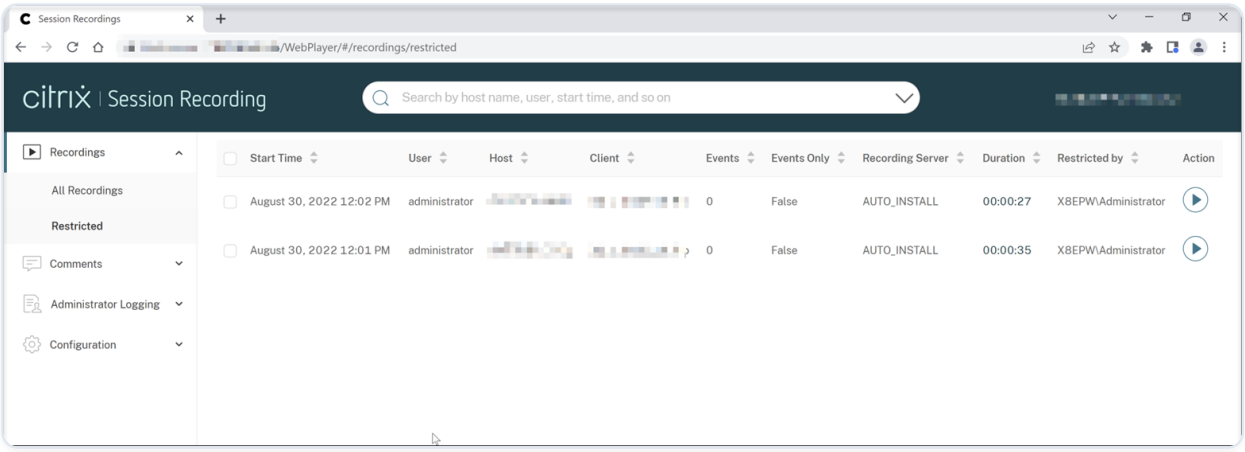


5. Click **Confirm**.

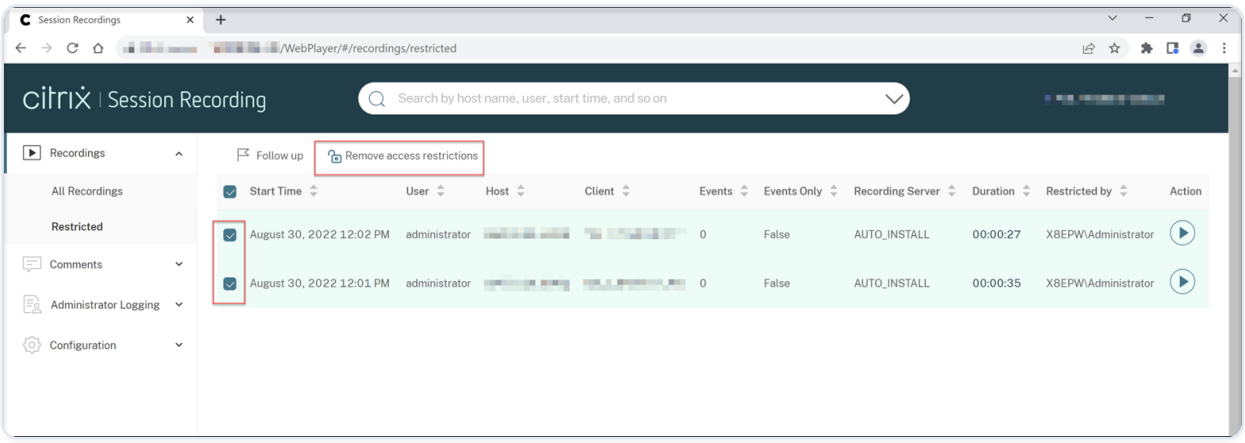


6. Verify that the selected recordings on which you placed access restrictions are moved from the **All Recordings** page to the **Restricted** page.

   The **Restricted by** column shows who placed access restrictions on the relevant recordings.

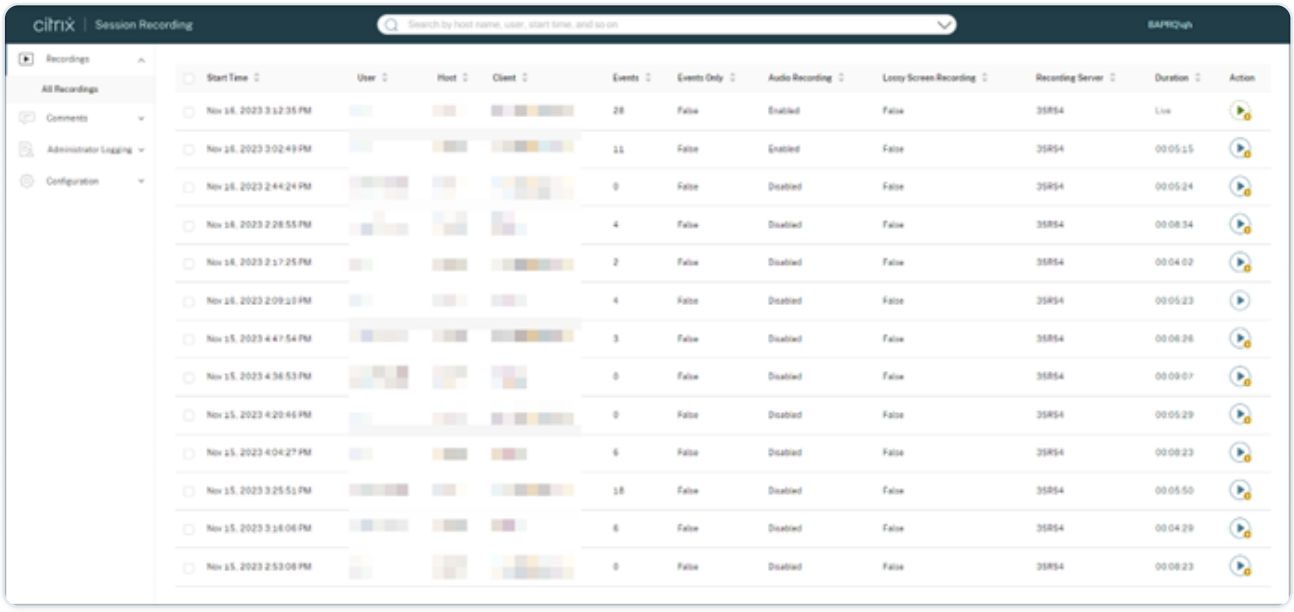


7. On the **Restricted** page, remove access restrictions as needed. With access restrictions removed, recordings are moved back to the **All Recordings** page.



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:**

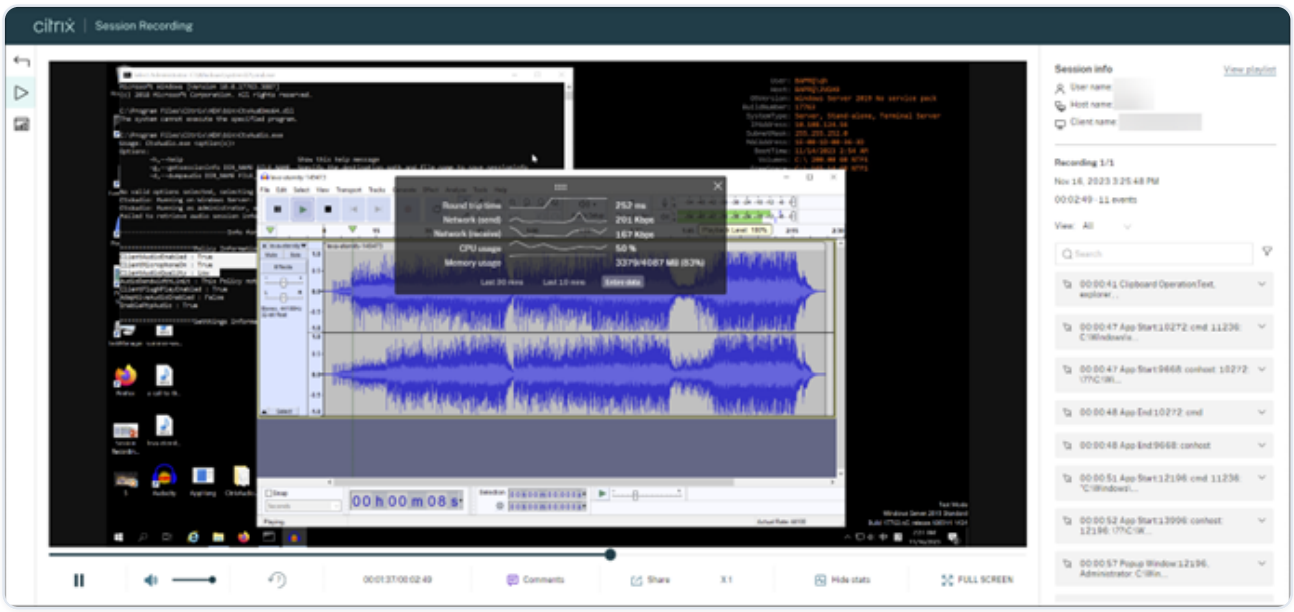
> For the **Player** role, the **Recordings** menu in the left navigation shows only the **All Recordings** submenu.

> For the **PrivilegedPlayer** role, the **Recordings** menu shows both the **All Recordings** and the **Restricted** submenus.

> Starting with 2411, the **Diagnostic Logging** menu is available in the left navigation. For more information, see View diagnostic logging.

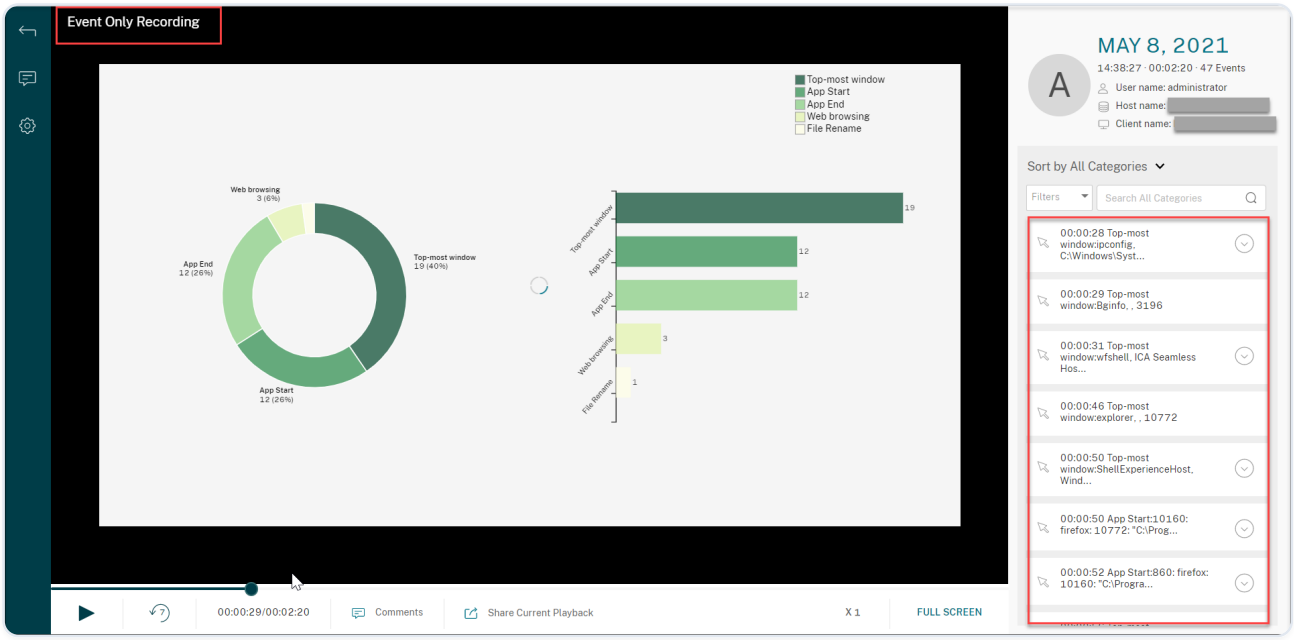
> Click the play button. The playback page appears. Playback starts after memory caching.

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:

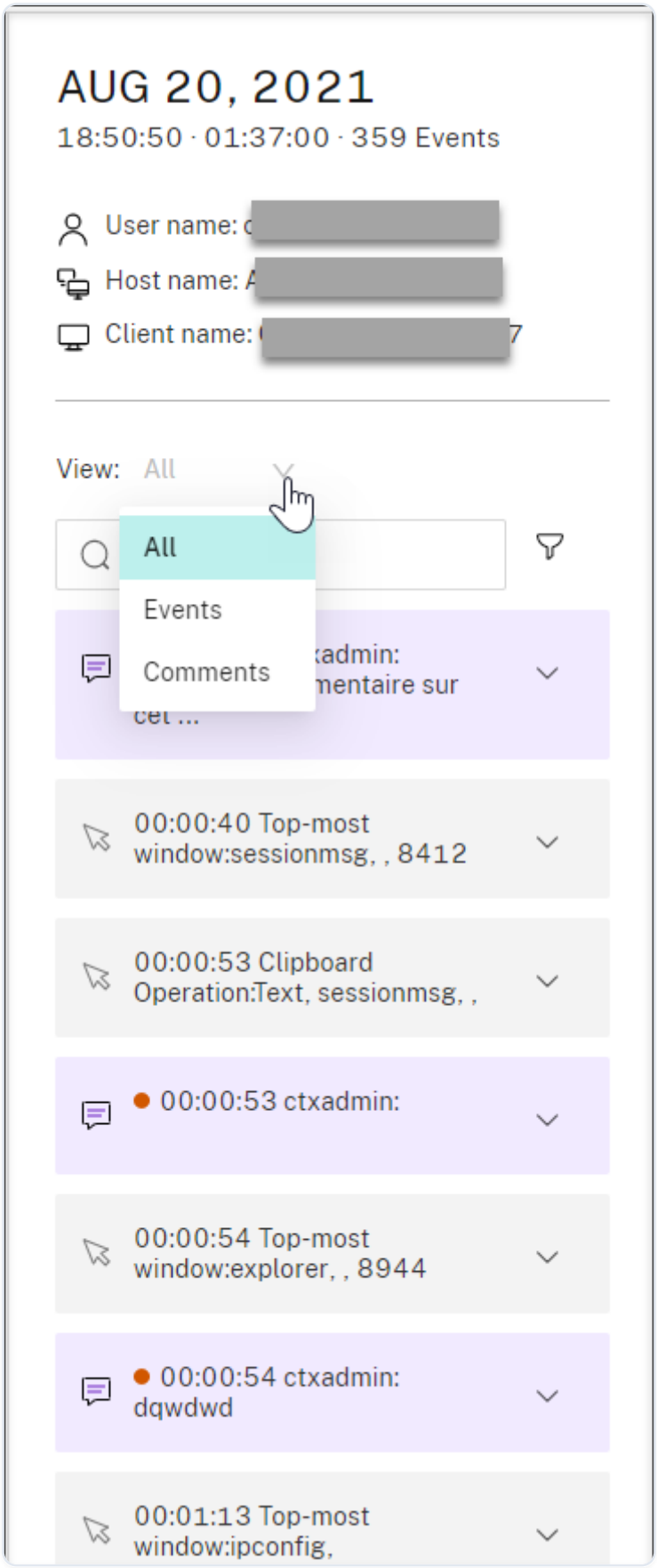
- Clicking the session progress time lets you switch to the absolute date and time the session was recorded.
- For an event-only recording, the play icon in the upper left corner is unavailable.

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

PLAYER CONTROL	DESCRIPTION
	Plays the selected recording file.
	Pauses playback.
	Mutes/unmutes audio playback and adjusts the volume using the slider.
	You can drag the progress bar during playback. Idle periods of recorded sessions are highlighted during playback.
	Seeks backward 7 seconds.

PLAYER CONTROL	DESCRIPTION
	Indicates the current position of the recording playback and the total recording duration. The time format is HH:MM:SS.
	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.
	Zoom in on the current playback area.

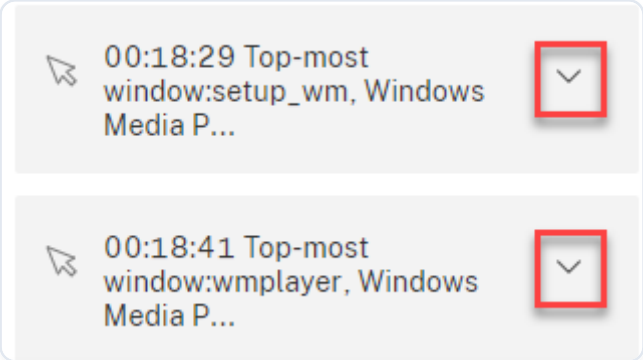
In the right pane of the playback page, the **Events** and **Comments** filters, quick search box, and some recording data are available, for example:



- 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.

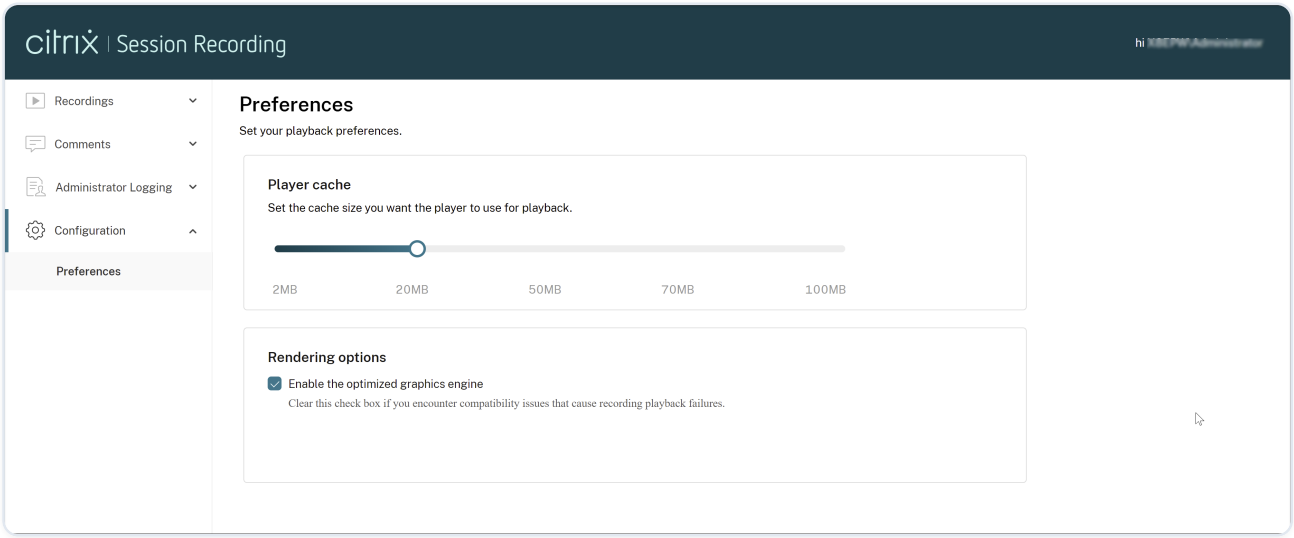
  Click the icon to expand the display of events. For example:



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

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:

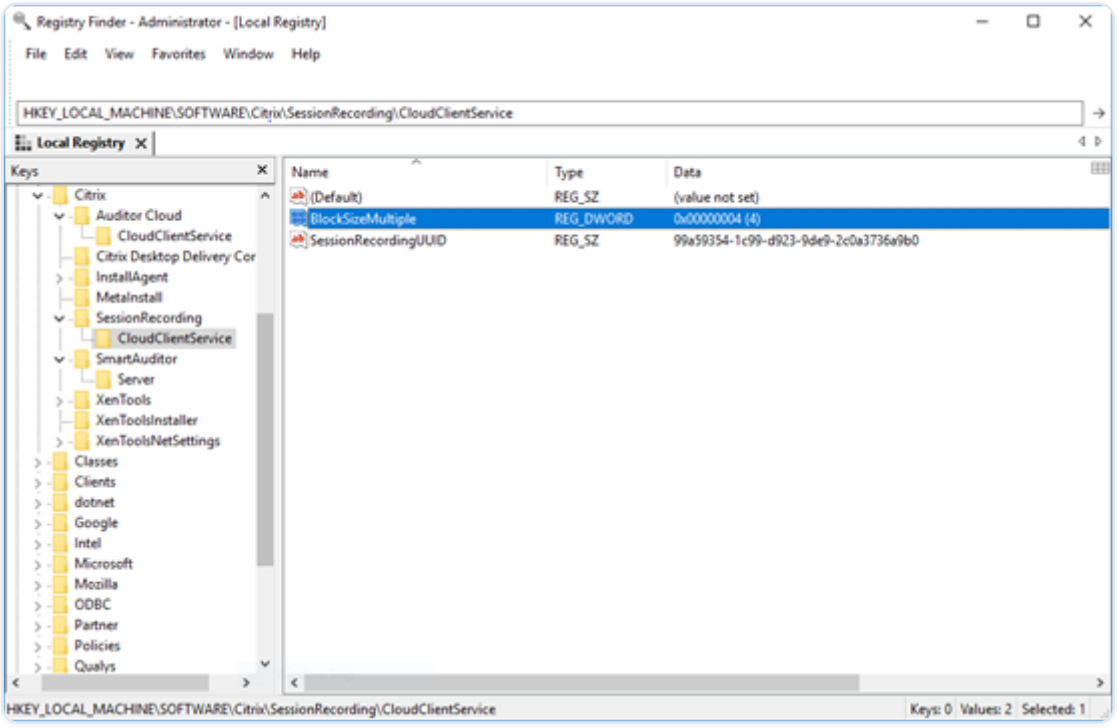
- **Player cache**. Drag the slider to set the cache size you want the player to use for playback.

- **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 periods of inactivity (idle periods) and visually represent them in the web player.

> **Tip:**

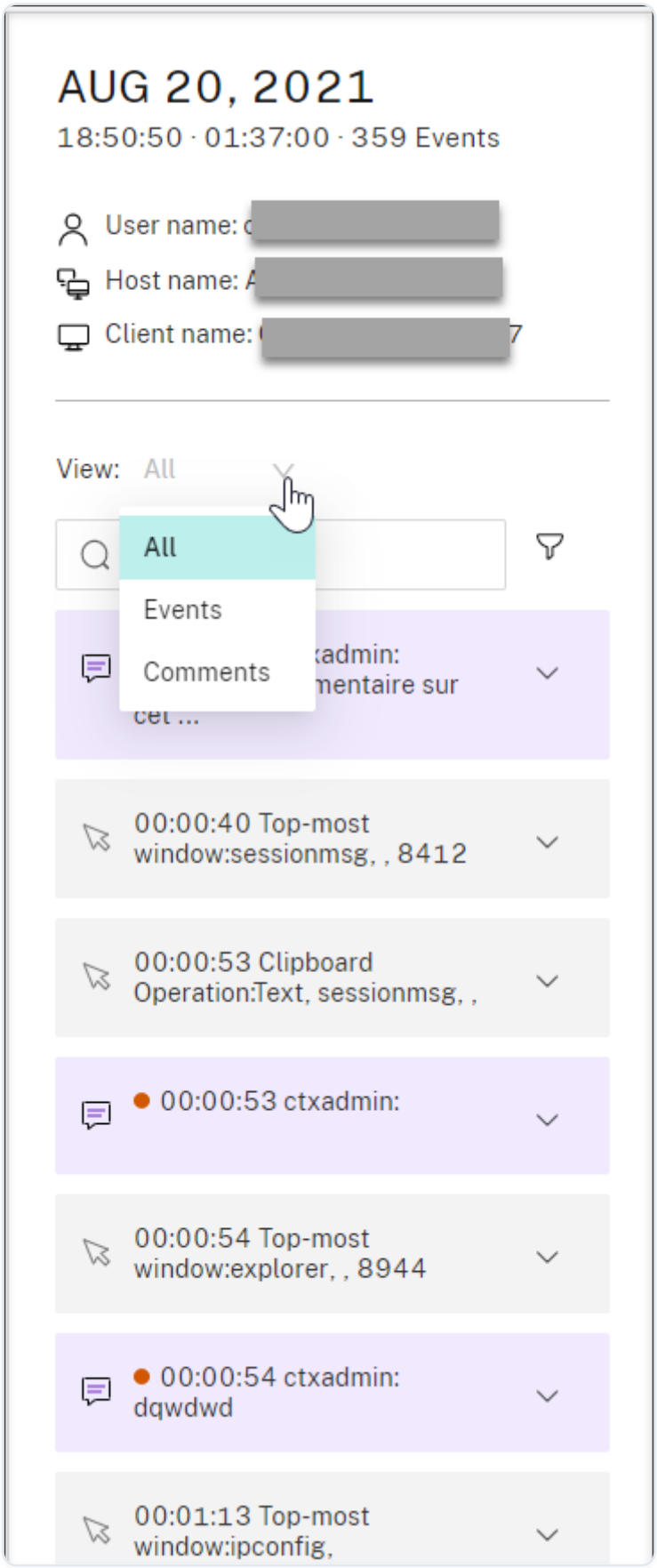
> Idle events are not visible in the Session Recording player because idle events are saved in the Session Recording database but not in the relevant recording files (`.icl` files).

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

REGISTRY KEY	DEFAULT VALUE	DESCRIPTION
EnableIdleEvent	1	To disable the idle event feature, set the value to **0**. To enable the idle event feature, set the value to **1**.
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.

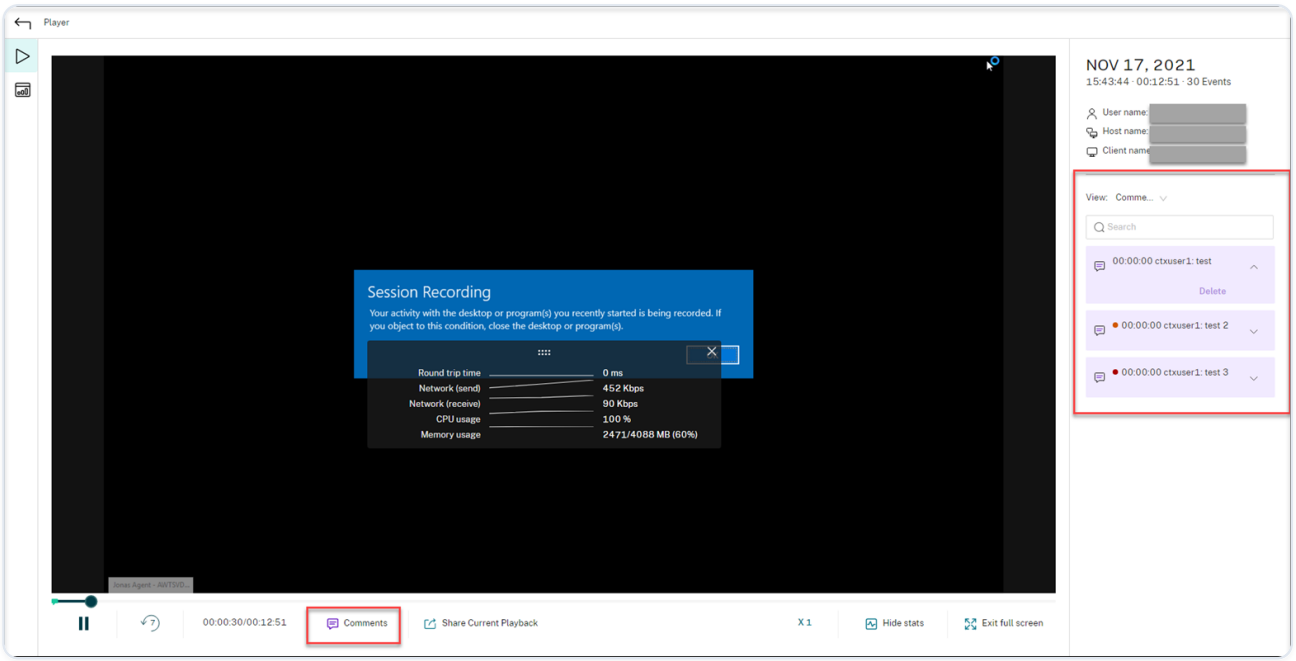
Use events and comments

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.

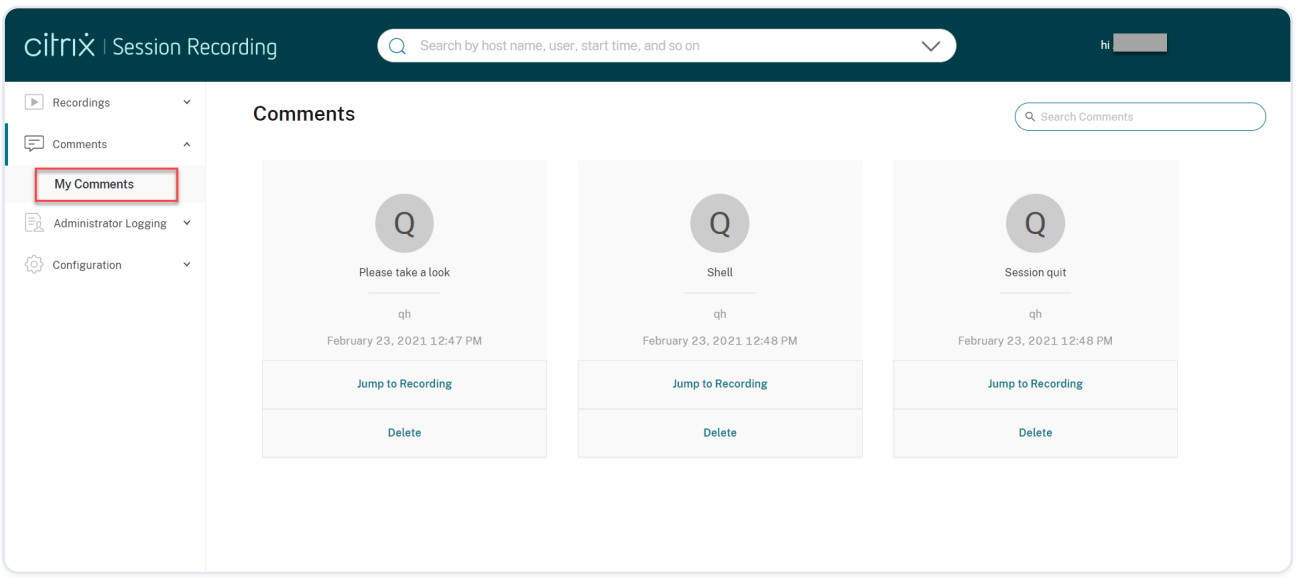

AUG 20, 2021
18:50:50 · 01:37:00 · 359 Events
User name:
Host name:
Client name:
View: All
All
Events
Comments
00:00:40 Top-most window:sessionmsg, , 8412
00:00:53 Clipboard Operation:Text, sessionmsg, ,
00:00:53 ctxadmin:
00:00:54 Top-most window:explorer, , 8944
00:00:54 ctxadmin: dqwdwd
00:01:13 Top-most 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**.

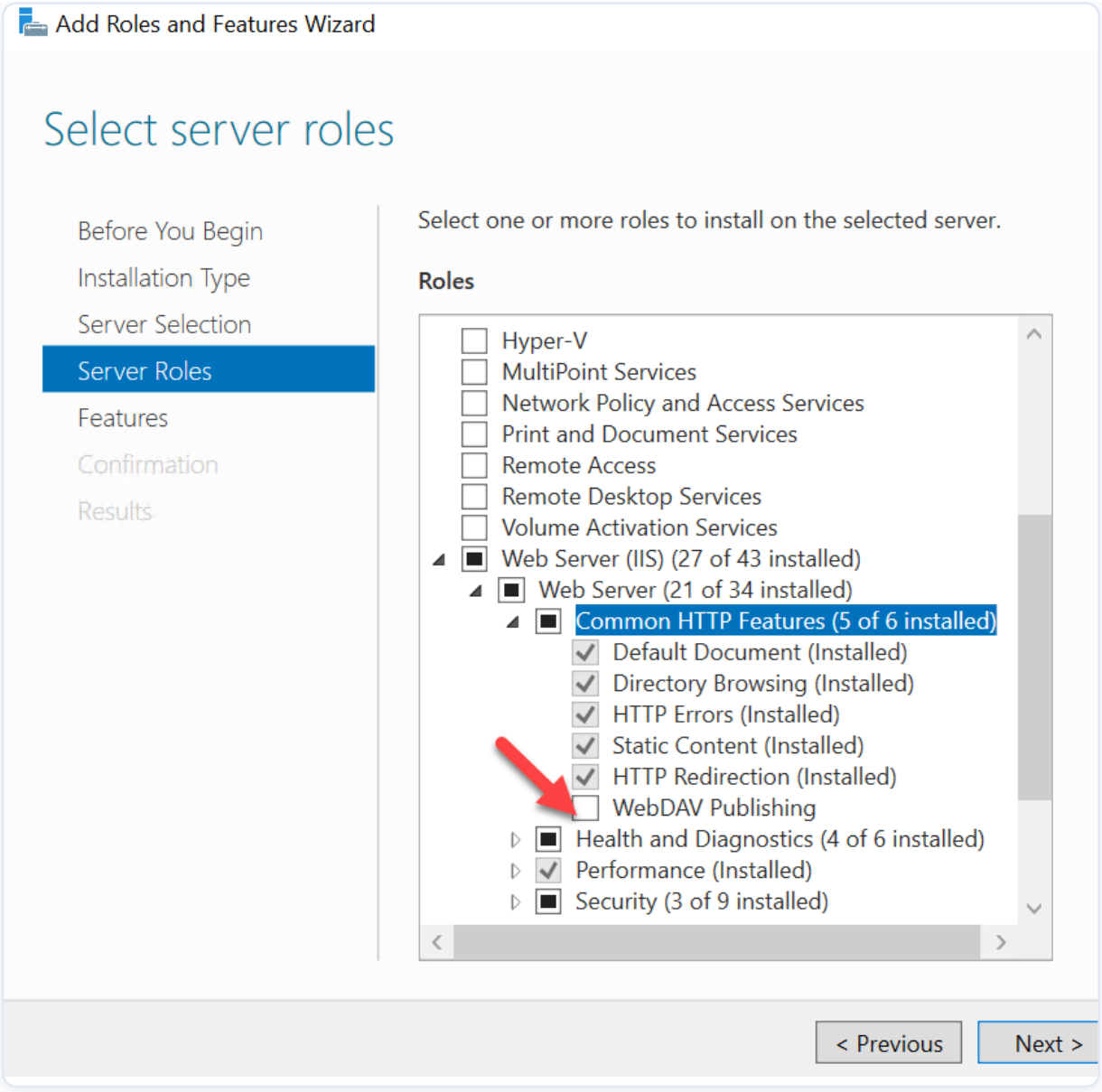


Clicking a comment lets you jump to the location where the comment was given. You can view all your comments on the **My comments** page.



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.

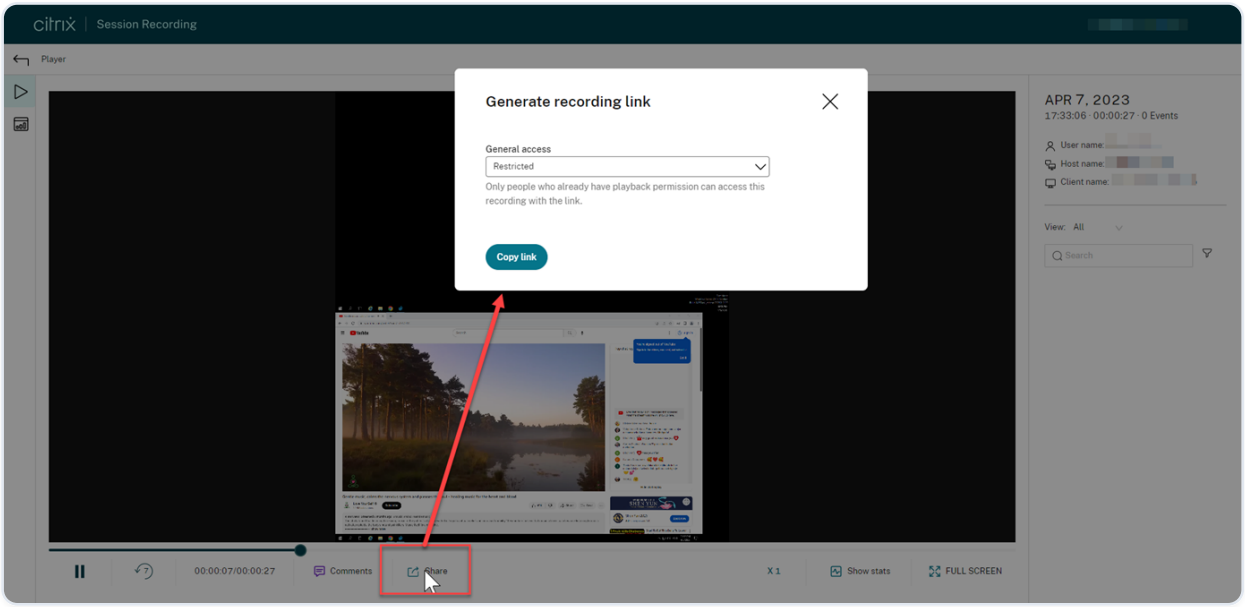
Note:

- 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.

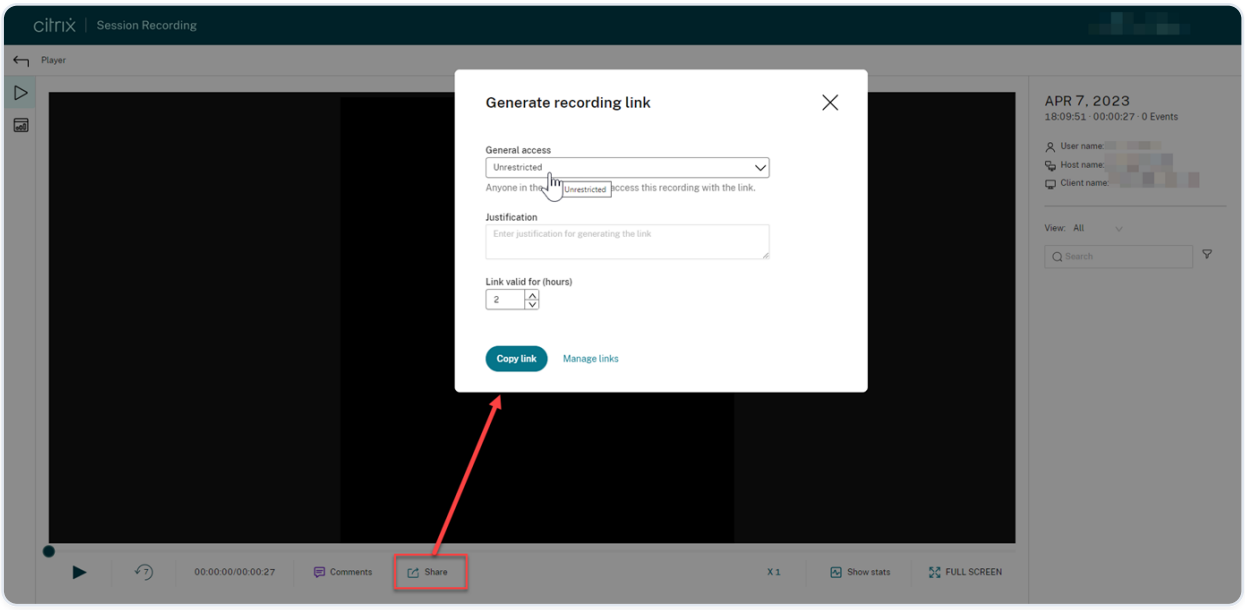
Share recordings as unrestricted links

> **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.

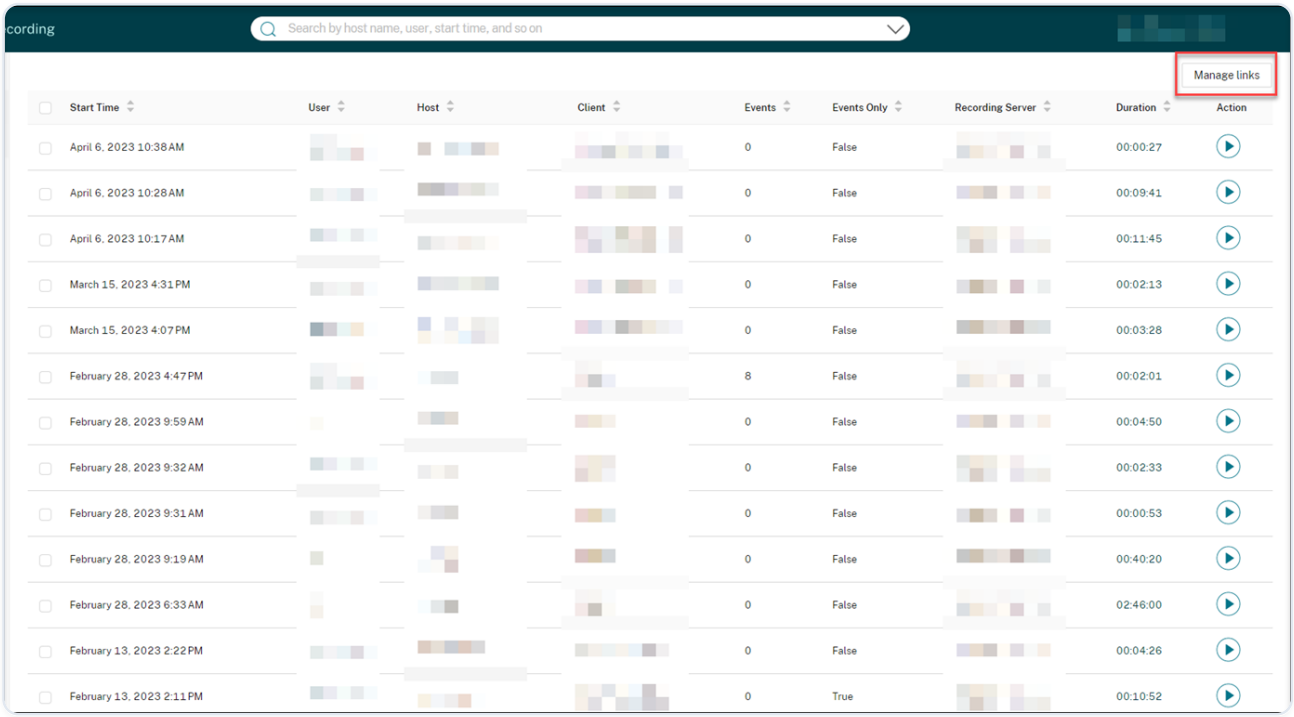
> **Note:**
>
> - To view a recording using an unrestricted link, users must enter a justification.
> - The actions of generating and accessing unrestricted links are logged under the playback logging sector of administrator logging.

Manage unrestricted links

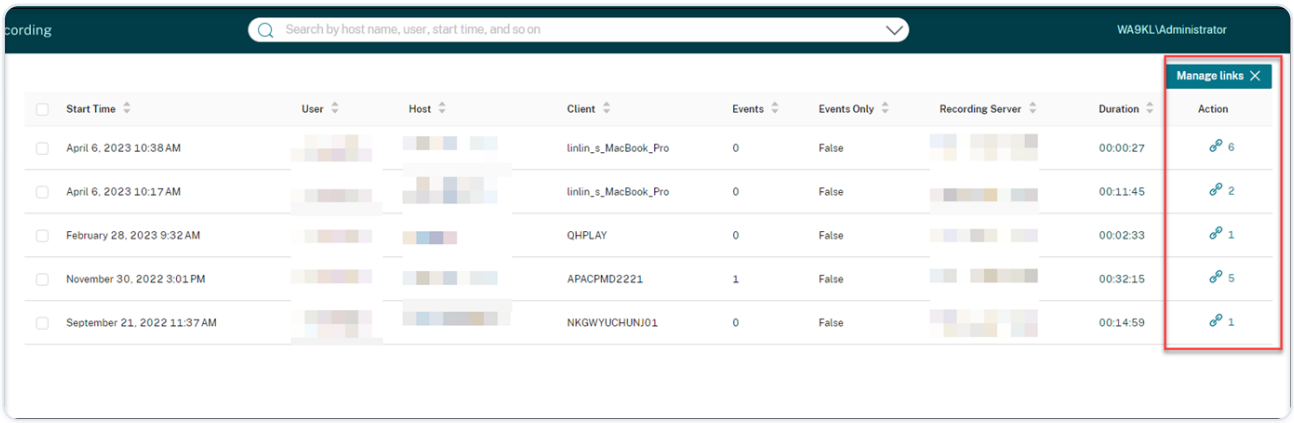
> **Note:**
>
> To manage unrestricted links, you must be assigned the **PrivilegedPlayer** role.

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.



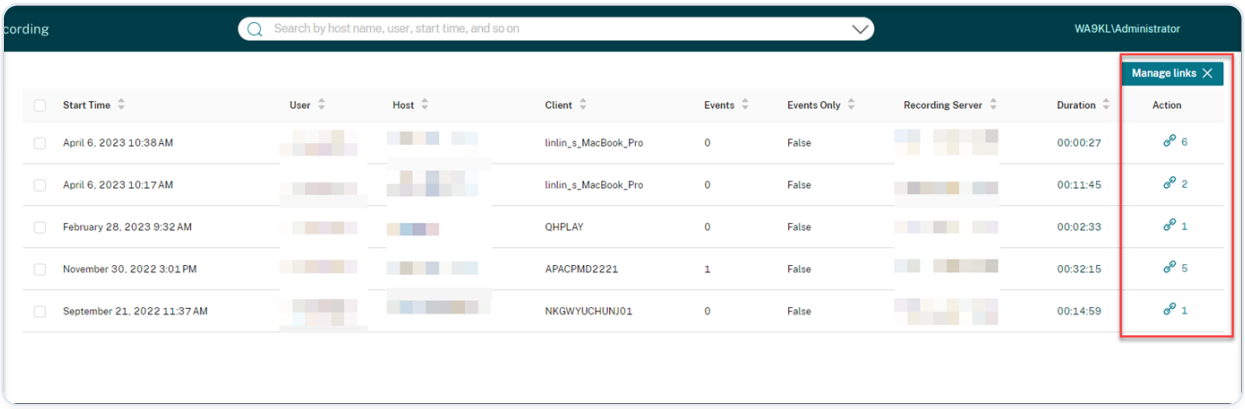
After you click **Manage Links**, only recordings that have been shared as unrestricted links are listed.



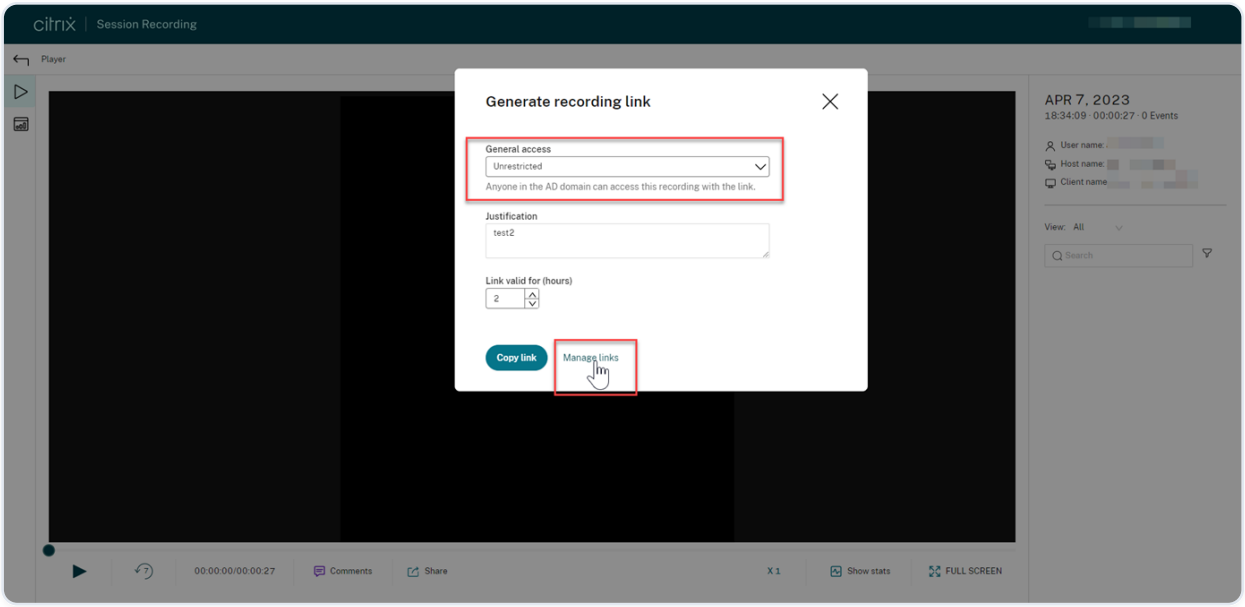
View and manage unrestricted links of a specific recording

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

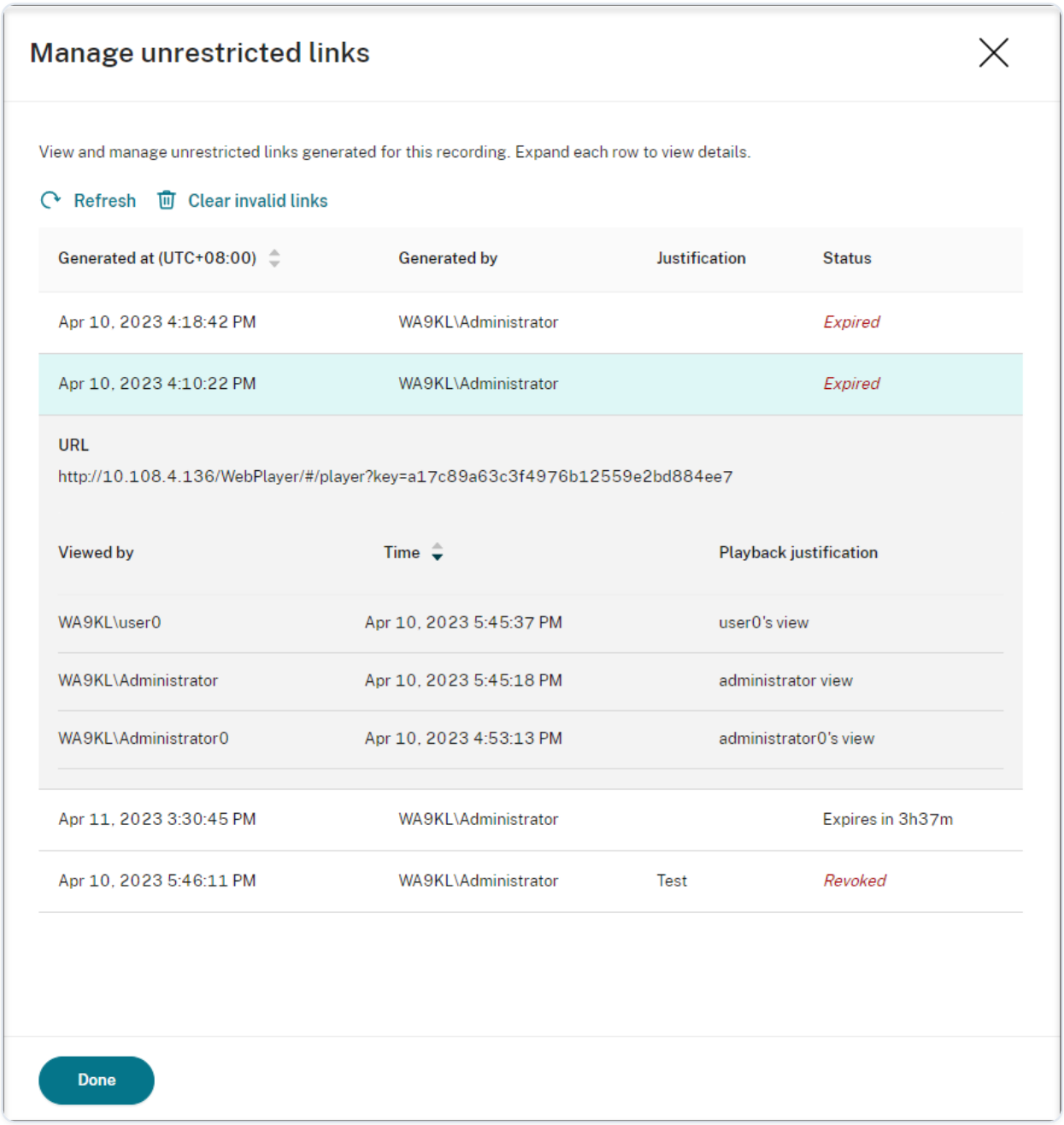
   Method 1: By clicking the link icon in the **Action** column on the **All Recordings** page



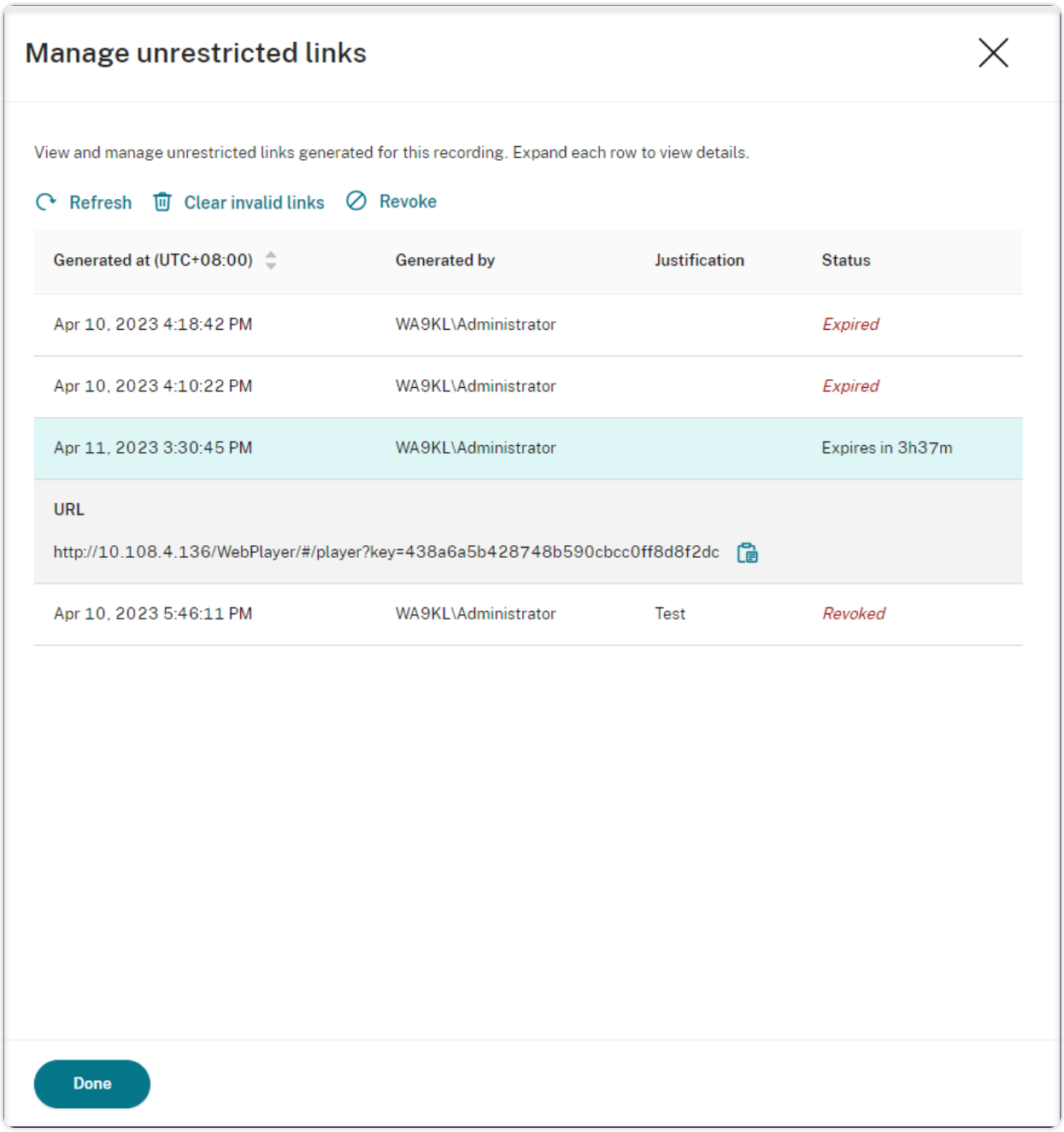
   Method 2: By clicking **Manage Links** in the **Generate recording link dialog**



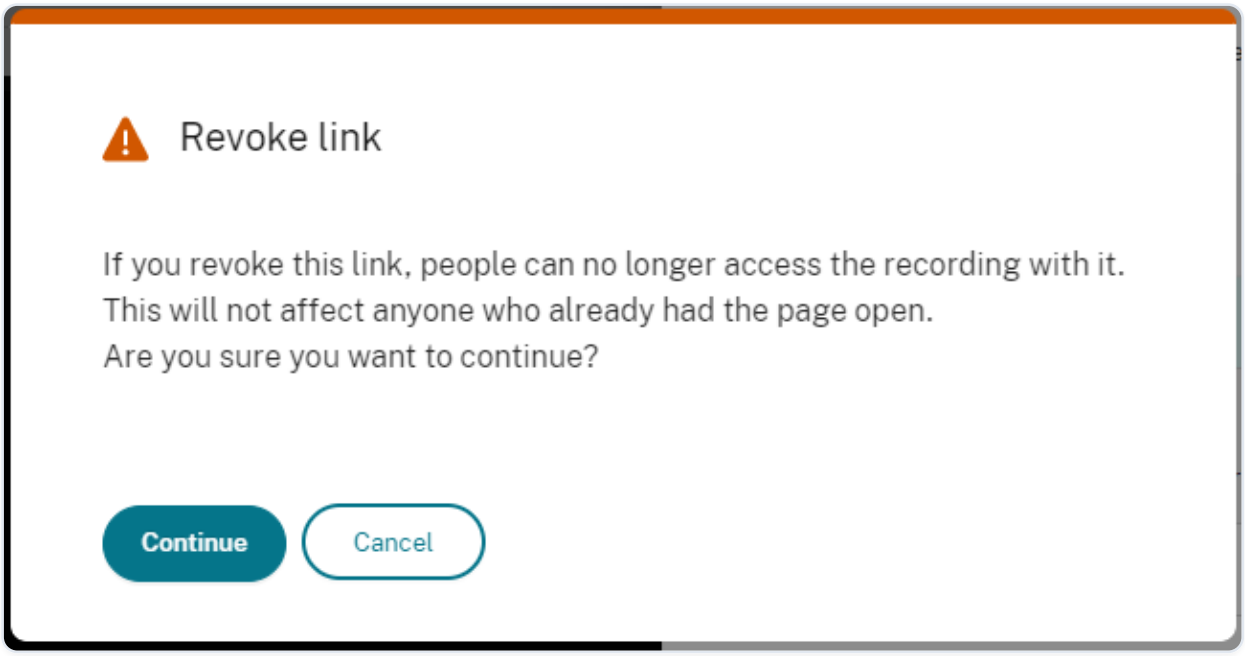
2. On the **Manage unrestricted links** page, expand each row to view details about the unrestricted links that are generated for the specific recording.



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.



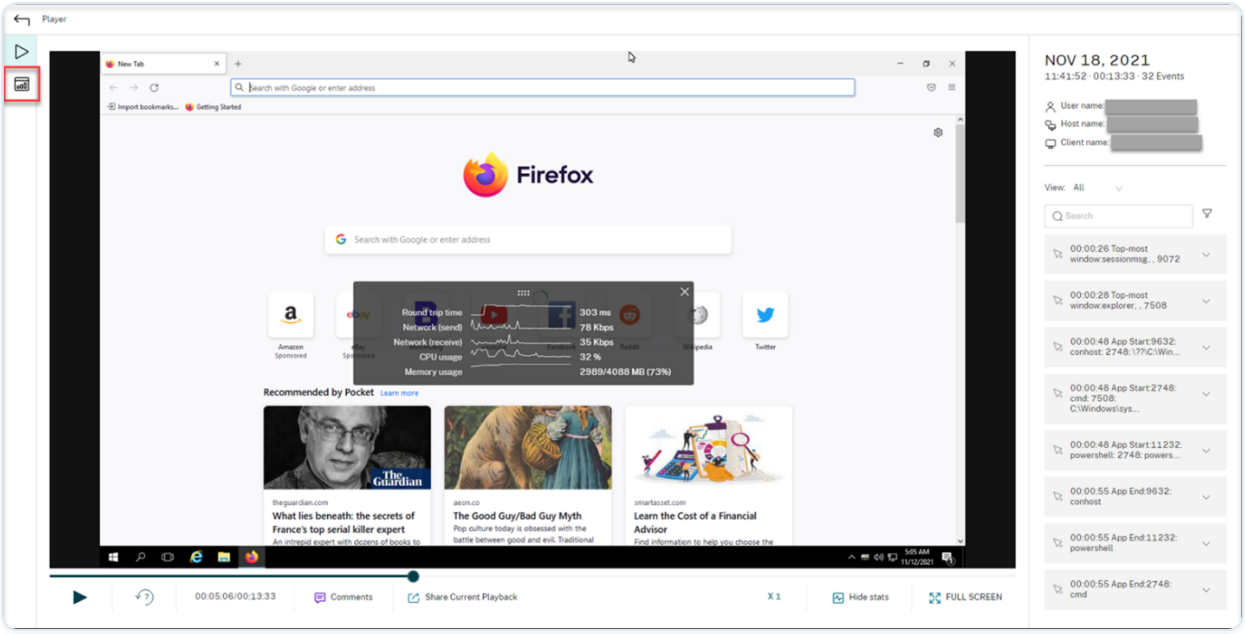
4. (Optional) To remove the links that have expired or revoked, click **Clear invalid links**.

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:

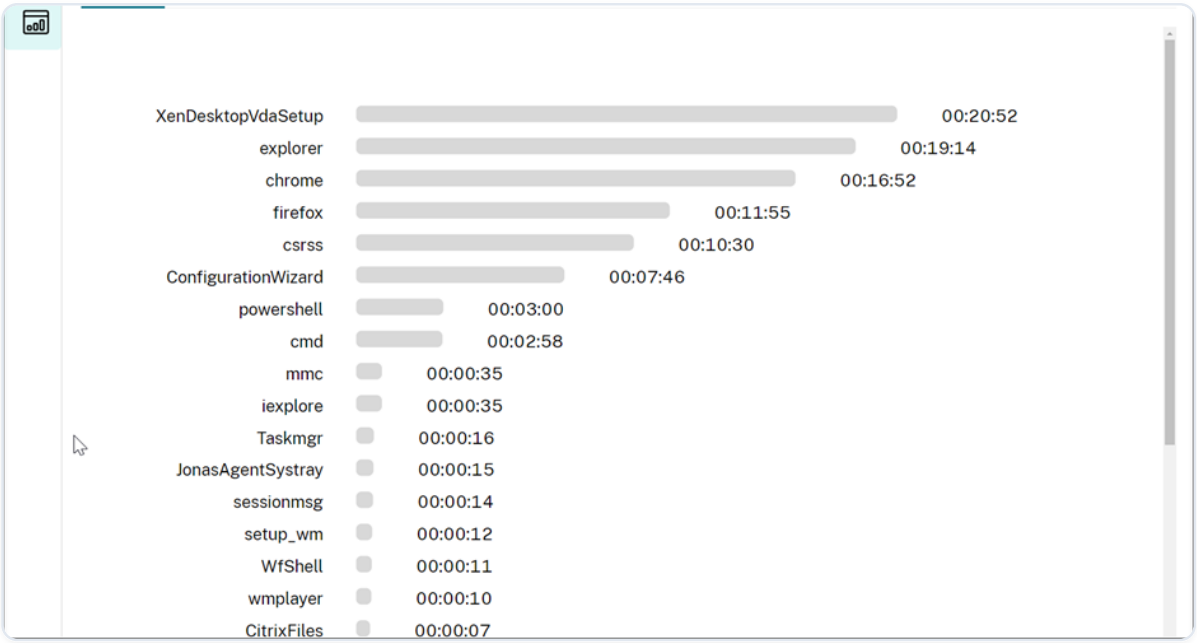
1. Open and play a recording.
2. In the upper left corner of the playback page, click the statistics icon.



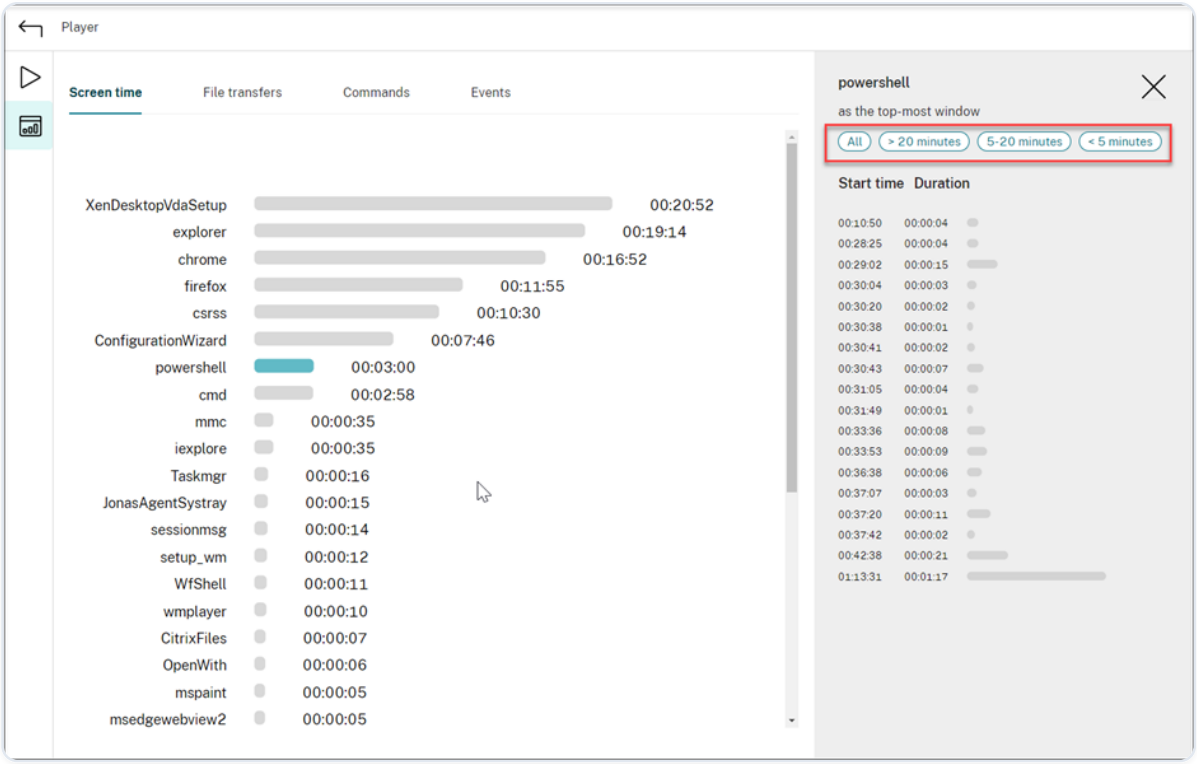
3. Switch between the **Screen time**, **File transfers**, **Commands**, **Printing**, and **Events** tabs to view statistics from different perspectives.

- **Screen time**

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



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

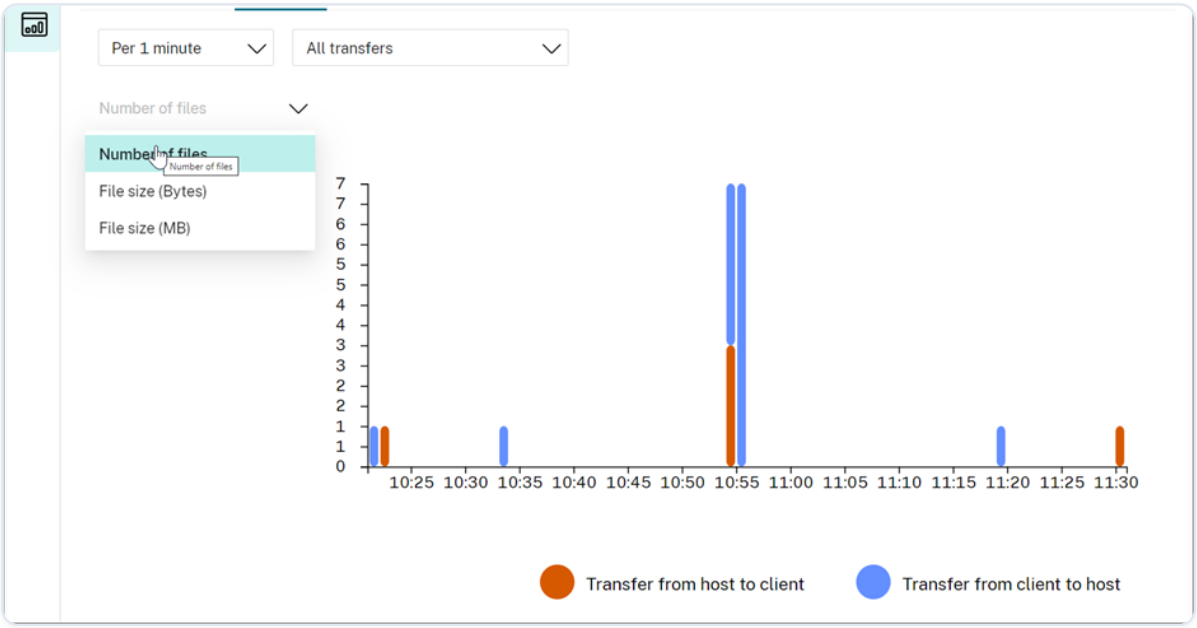


- **File transfers**

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

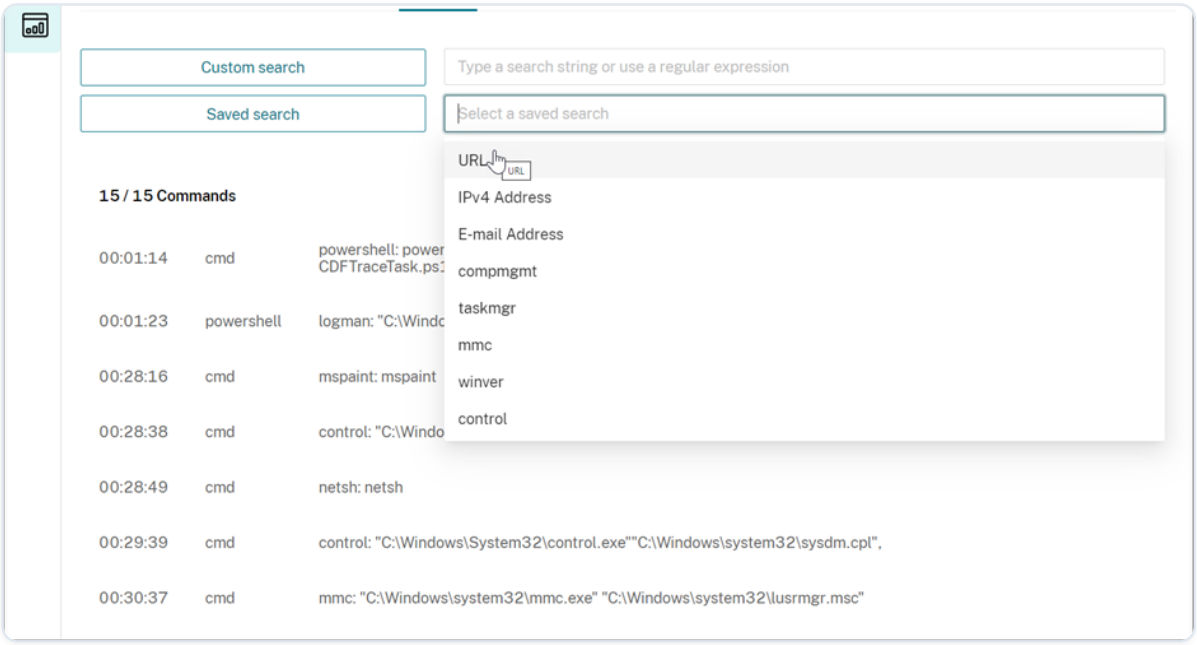
- Time granularity: **Per 1 minute**, **Per 10 minutes**, **Per hour**
- File transfer destination: **All transfers**, **Transfer from host to client**, **Transfer from client to host**
- Number or size (Bytes or MB) of transferred files

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



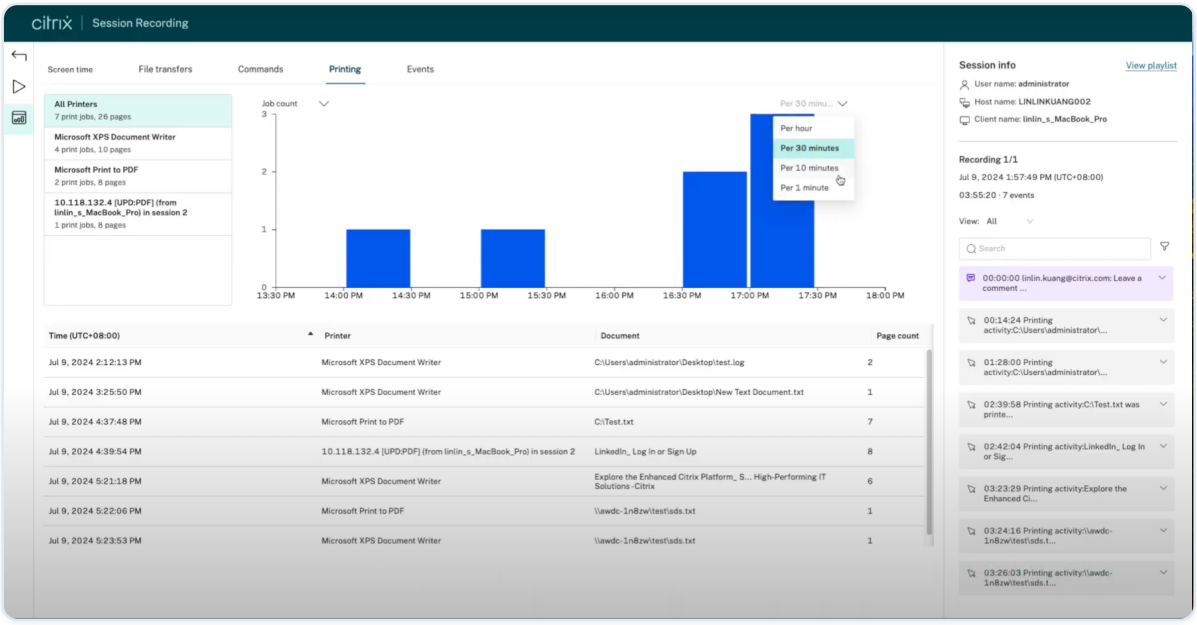
- **Commands**

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



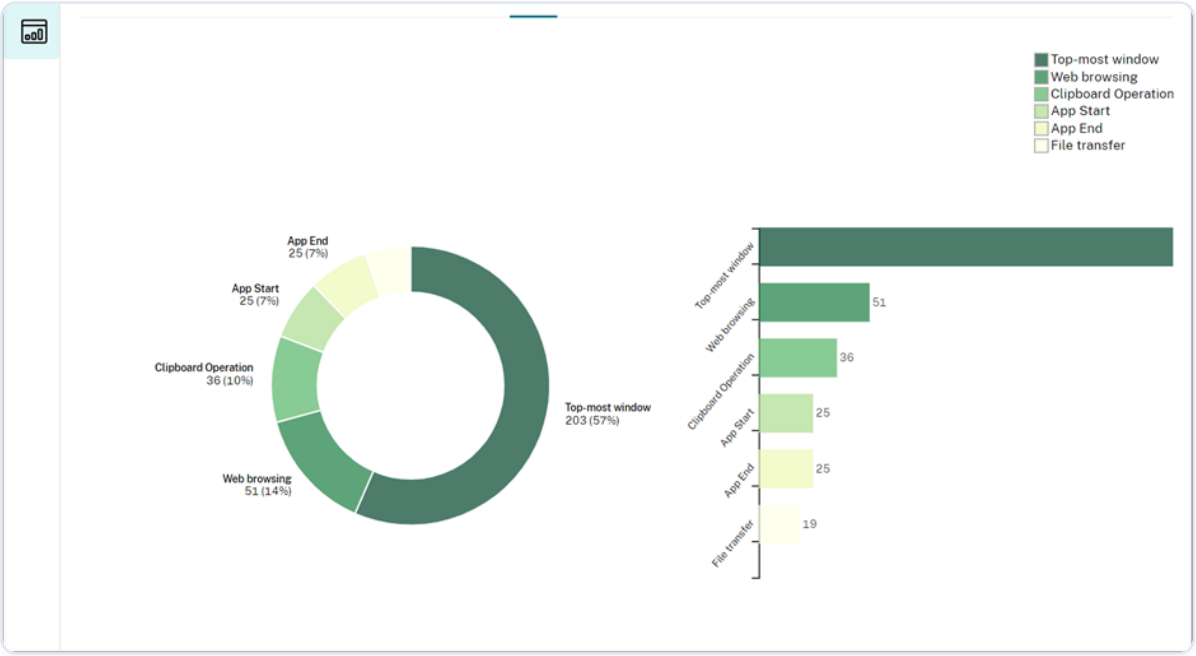
- **Printing**

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



- **Events**

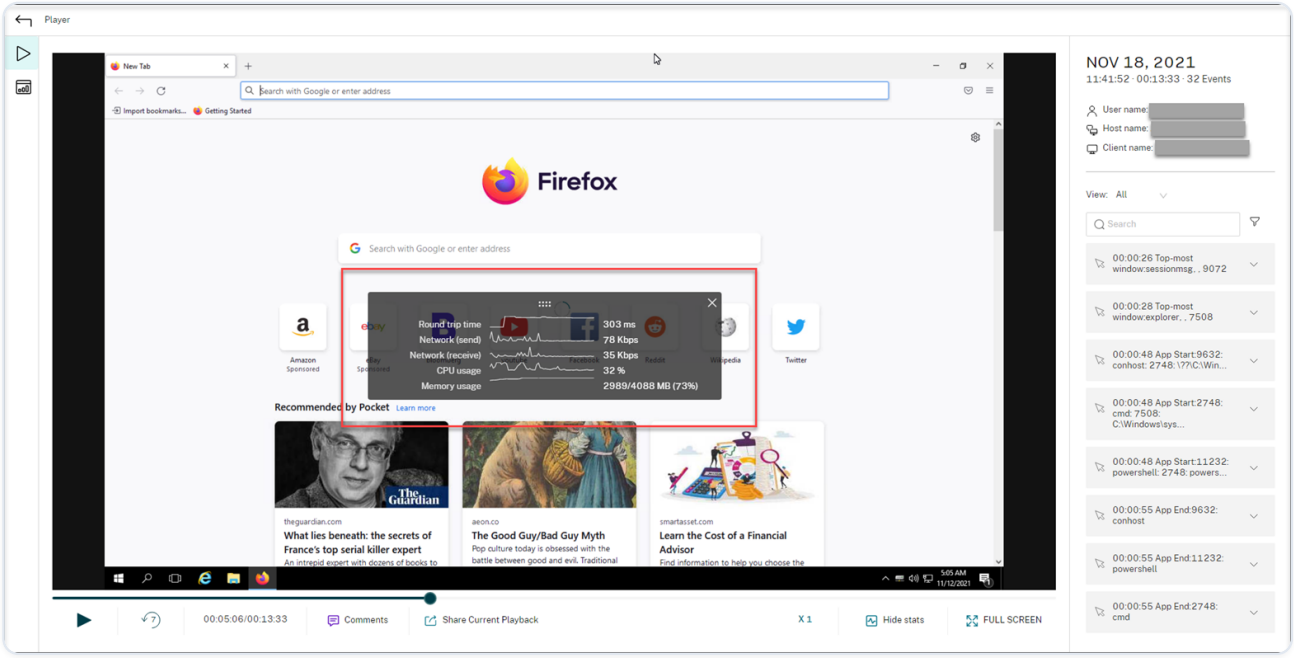
  The **Events** tab shows the proportions and numbers of all types of events in the recorded session.



View 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 time 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.

View diagnostic logging

Overview

Various diagnostic logs including message queue quota exceedance can be detected on the VDAs and sent to the Session Recording server for display in the Session Recording web player.

Message queue quota exceedance

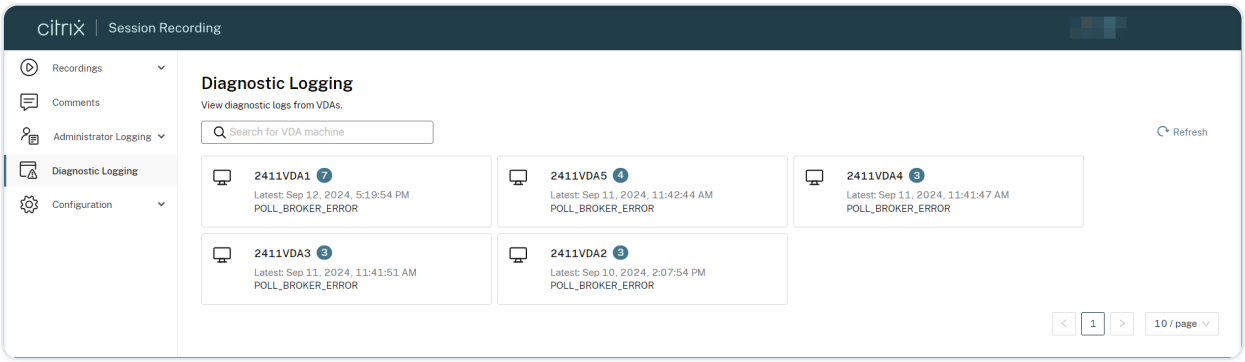
In any of the scenarios outlined below, there's a chance of exceeding the maximum size of the Microsoft Message Queuing (MSMQ) directory on a VDA, resulting in packet drops or pushback.

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

View diagnostic logging

1. Open the Session Recording web player, and click **Diagnostic Logging** in the left navigation. The **Diagnostic Logging** page appears.

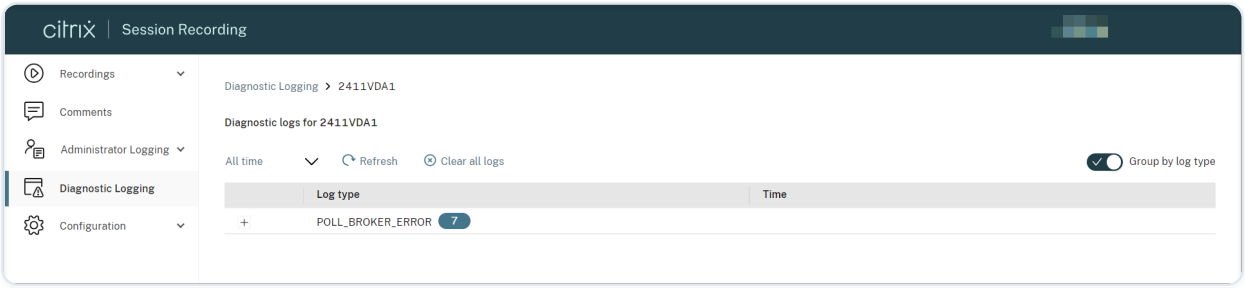
   For example:

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

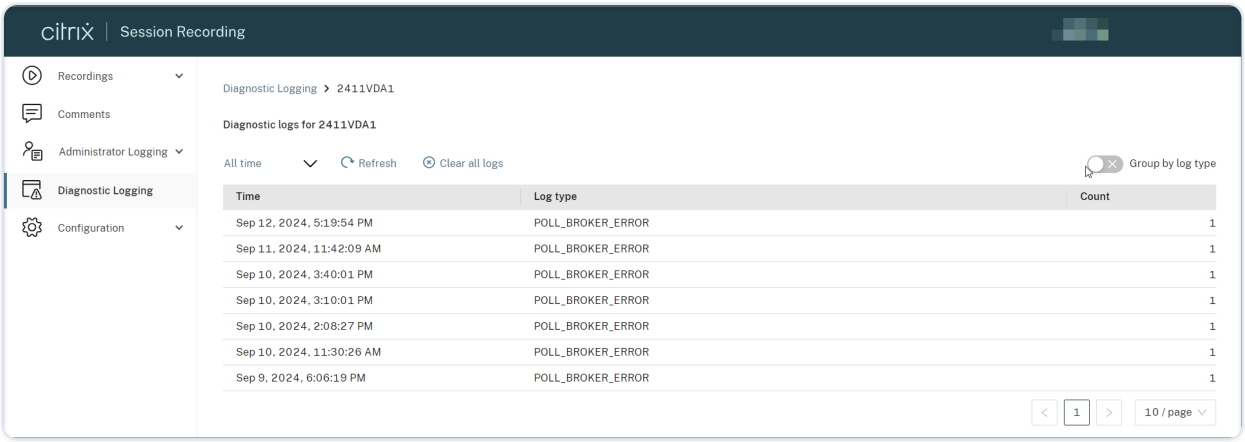
2. Click a target VDA to view its diagnostic logs.

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

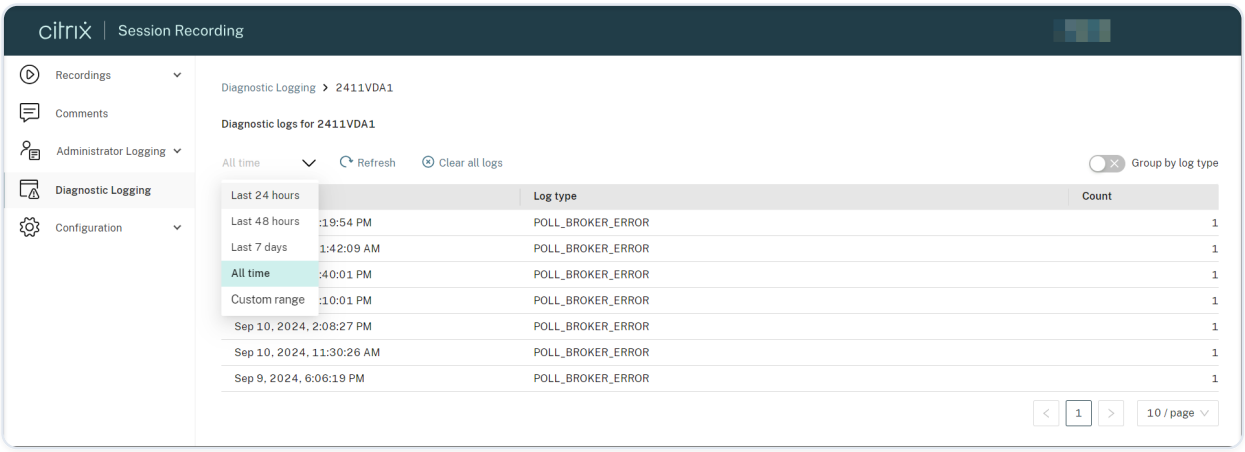
   

   You can disable log grouping by type and list all logs in chronological order instead.

   For example:

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



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

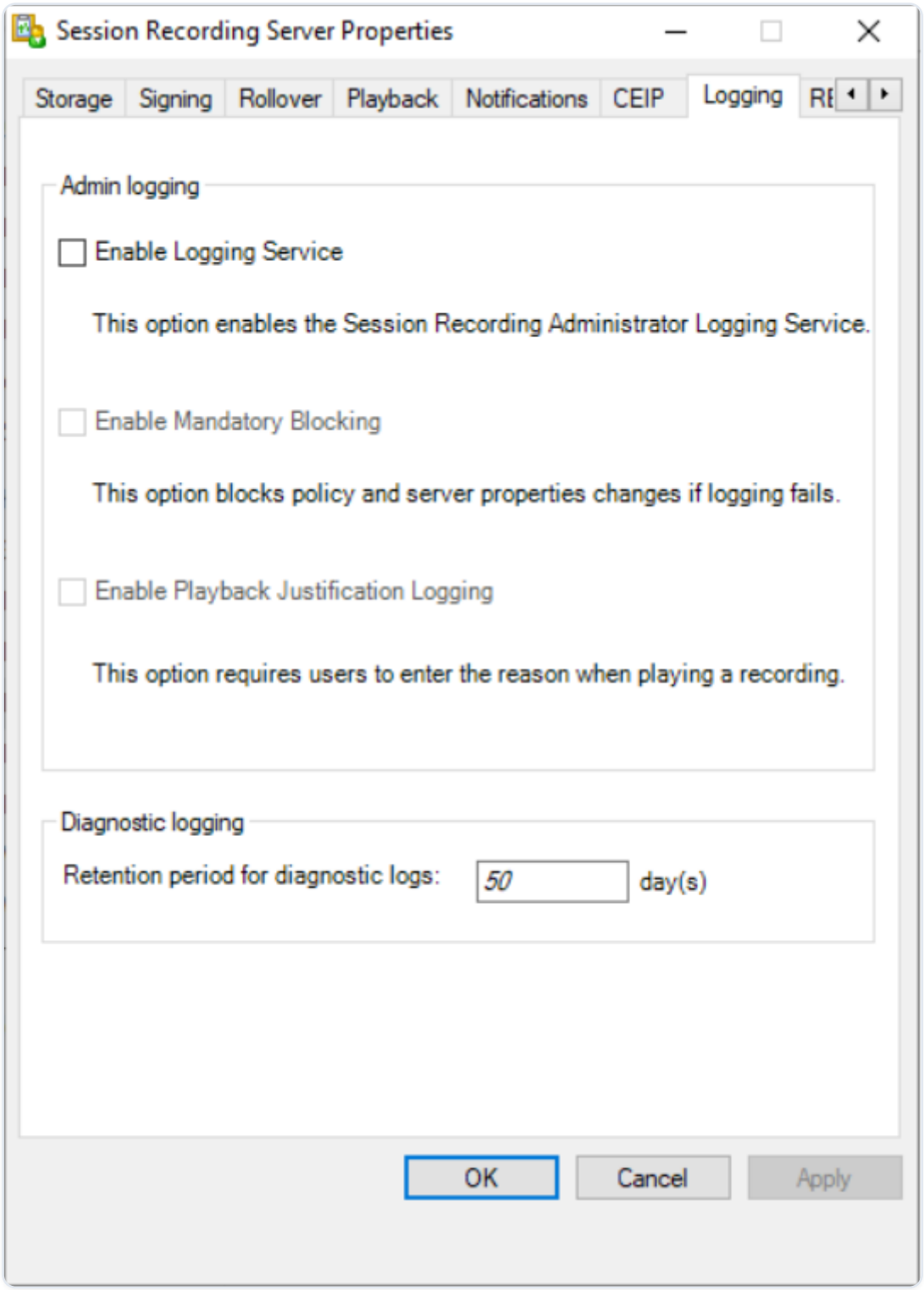
Configure diagnostic logging

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

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent\DiagnosticLoggingEnabled

Value data: 1 = enabled, 0 = disabled

You can also set how long these logs can be retained on the Session Recording database. To do so, go to the **Logging** tab of Session Recording Server Properties and configure the **Retention period for diagnostic logs**. The default value is 30 days.


Session Recording Server Properties
Storage
Signing
Rollover
Playback
Notifications
CEIP
Logging
RE
Admin logging
Enable Logging Service
This option enables the Session Recording Administrator Logging Service.
Enable Mandatory Blocking
This option blocks policy and server properties changes if logging fails.
Enable Playback Justification Logging
This option requires users to enter the reason when playing a recording.
Diagnostic logging
Retention period for diagnostic logs:
50
day(s)
OK
Cancel
Apply

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 | REPAIR] 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. You can specify a target session recording file to archive by using the FILEID parameter. You can also specify target session recording files by using the RETENTION parameter and the FILTER or RULES parameter. In the second case, 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`

COMMAND	DESCRIPTION
	`filter>] [/RULES:<advanced filters>] [/L] [/F] [/S] [/?]`
`DORMANT`	Displays or counts the live recording files that are considered dormant or unresponsive. A live recording is considered unresponsive or dormant when no new data is written to the recording file after a specified period of time has elapsed. You can specify a target session recording file by using the FILEID parameter. You can also 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. You can manually close unresponsive or dormant live recordings by appending the CLOSEFILES parameter. You can also set a time threshold on the **Storage** tab of **Session Recording Server Properties** to close unresponsive or dormant live recordings automatically when the threshold is exceeded. For more information, see Close unresponsive or dormant live recordings later in this article.
`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

COMMAND	DESCRIPTION
	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 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, you can either specify a target session recording file by using the FILEID parameter or specify target session recording files using the RETENTION parameter and the FILTER or RULES parameter. In the second case, 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 `?`

COMMAND	DESCRIPTION
	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 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.
`REPAIR`	Repairs recording files that are corrupted due to missing data in the file headers. Repaired files can be found at **%AppData%\Citrix\SessionRecording\Restore**.

COMMAND	DESCRIPTION
`/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.
- You must enclose each "**CONDITION**" item in double quotes (`""`) and separate two "**CONDITION**" items with 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 the 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 moving session recording files, the ICLDB utility moves them 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:

- **/FILEID:<id\>** - Lets you specify a target session recording file. You can check the ID of a session recording file in the Session Recording player (Windows). A recording file name can also be used as the file ID.
- **/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 the 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:

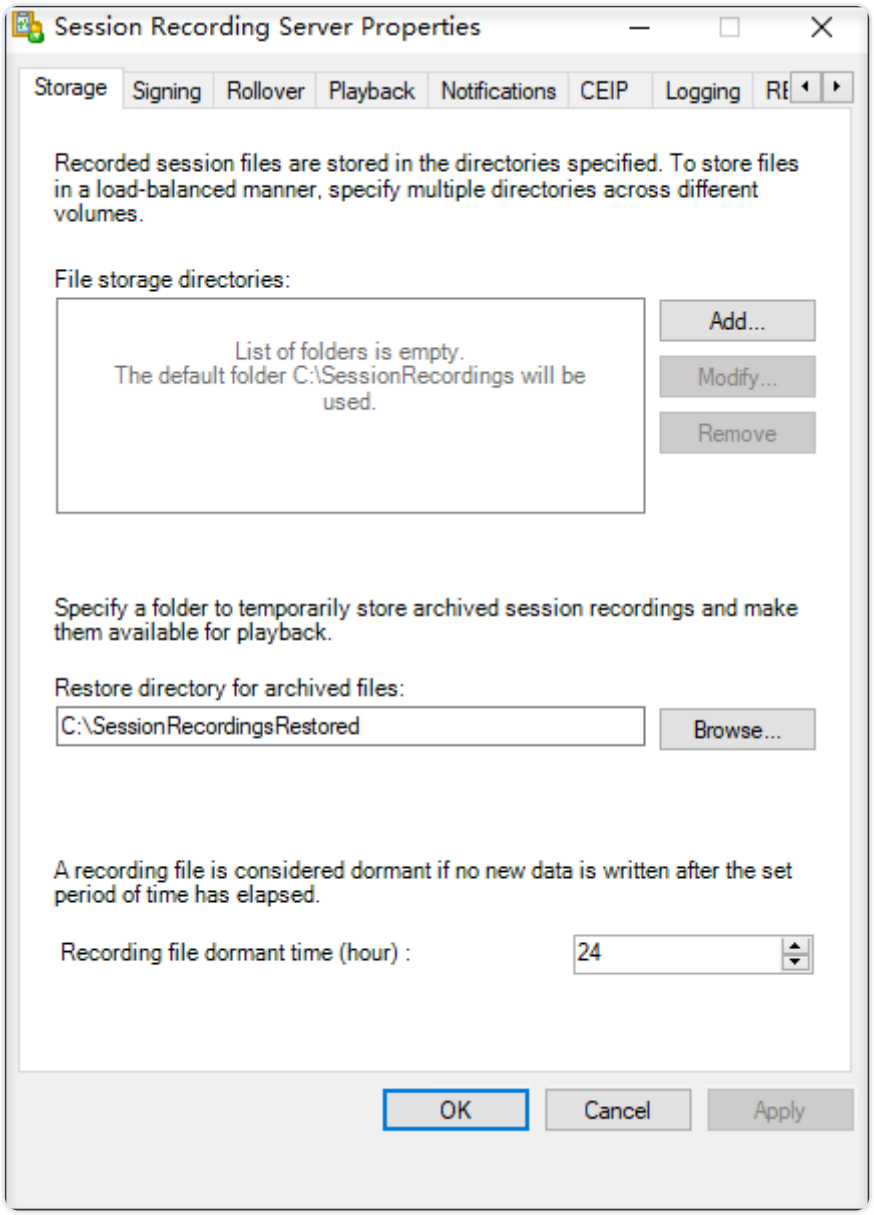
   - Run the `ICLDB IMPORT /LISTFILES /RECURSIVE /RELOCATE /L <directory>` command where **directory** is the name of one or more directories, separated by a space containing session recording files. Enter **Y** to confirm the import.
   - Run the `ICLDB IMPORT /LISTFILES /RELOCATE /L <file>` command where **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**.

Close unresponsive or dormant live recordings

By default, a live recording is considered unresponsive or dormant if no new data was written to the recording file for 24 hours. You can configure this time threshold on the **Storage** tab of **Session Recording Server Properties** to close unresponsive or dormant live recordings automatically when this threshold is exceeded. The minimum value that you can set is 12 (hours).



You can also manually close unresponsive or dormant live recordings by using the **ICLDB DORMANT** command, for example:

```
ICLDB DORMANT [/DAYS:<days> | /HOURS:<hours> | /MINUTES:<minutes> | /
FILEID:<id>] [/LISTFILES] [/CLOSEFILES] [/L] [/F] [/S] [/?]
```

The FILEID parameter lets you specify a target session recording file and the CLOSEFILES parameter lets you manually close unresponsive or dormant live recordings that you specify.

> **Tip:**
>
> You can check the ID of a session recording file in the Session Recording player (Windows). A recording file name can also be used as the file ID.

Session recording file export

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

Key capabilities of this feature include:

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

Prerequisites

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

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

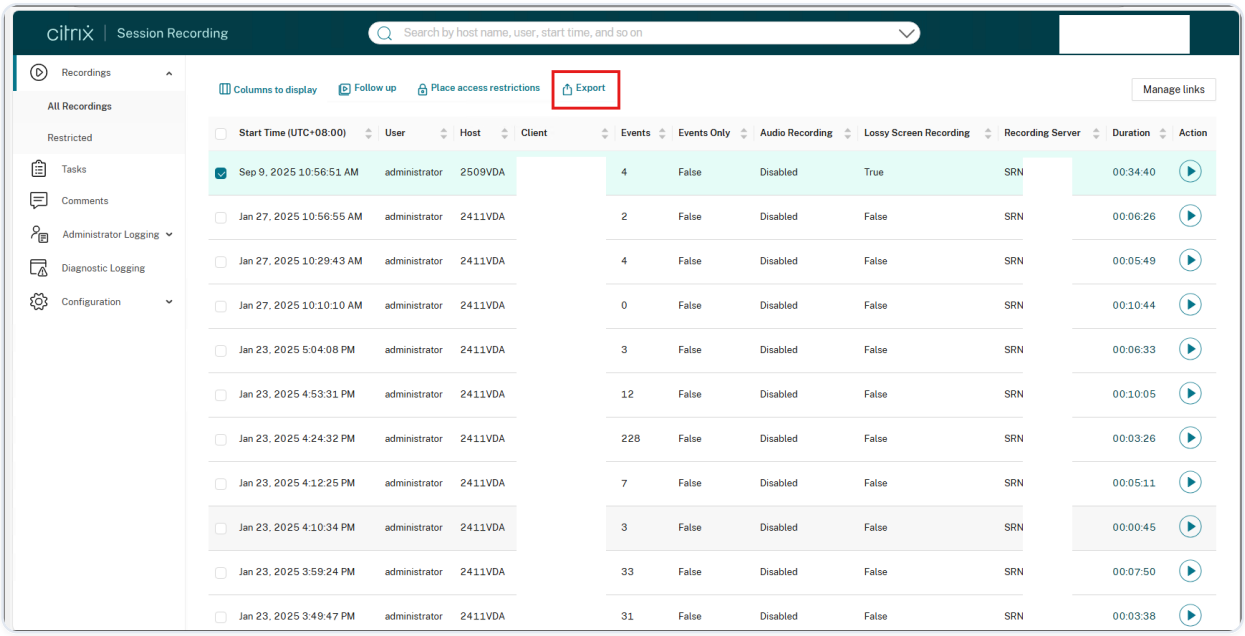
How to use recording file export

How to export Session Recording files

> **Note:**
>
> Only administrators who have been assigned both the `LoggingReader` and `PrivilegedPlayer` roles can perform export operations. You can assign roles to users in the **Session Recording Authorization Console**.

1. Log in to the Session Recording Web Player and navigate to the **All Recordings** page.
2. Select one or more recordings that you need to export.

3. Click the **Export** button located above the list.



4. Check the export files under the following folder on the machine running media task service: `%ProgramData%\Citrix\SessionRecording\SRTask\Cache`.

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

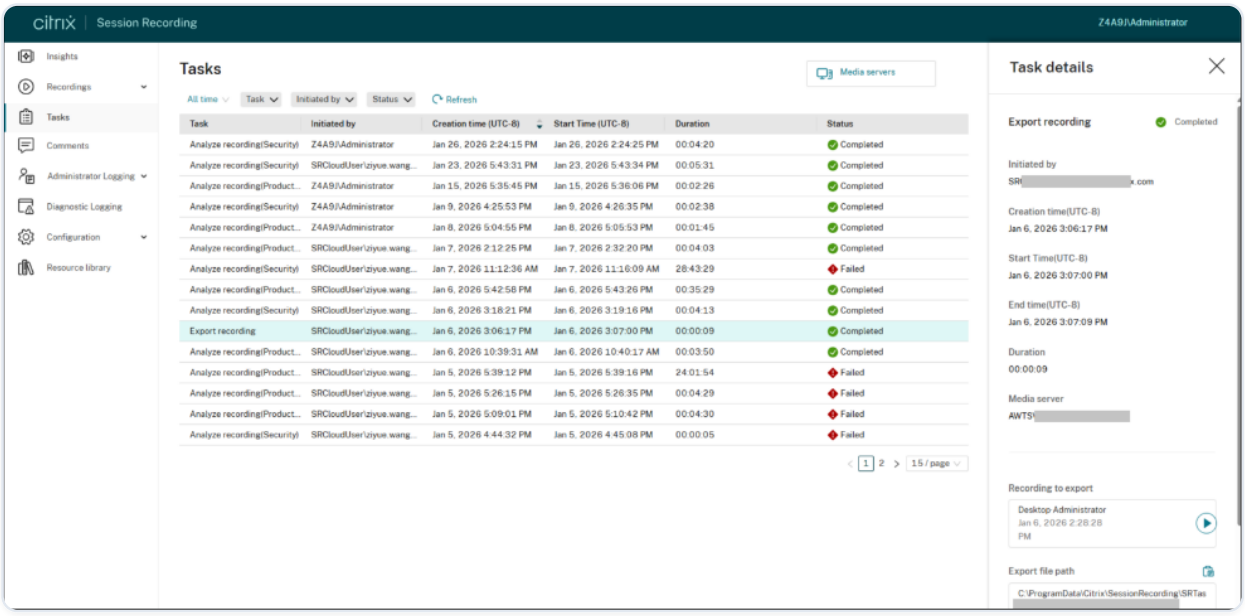
> **Note:**
>
> The sidecar JSON file is generated only when the Session Recording media task service is version 2607 or later.

How to monitor export tasks and audit logs

- To view export status:

  a. Click **Tasks** in the left navigation pane.

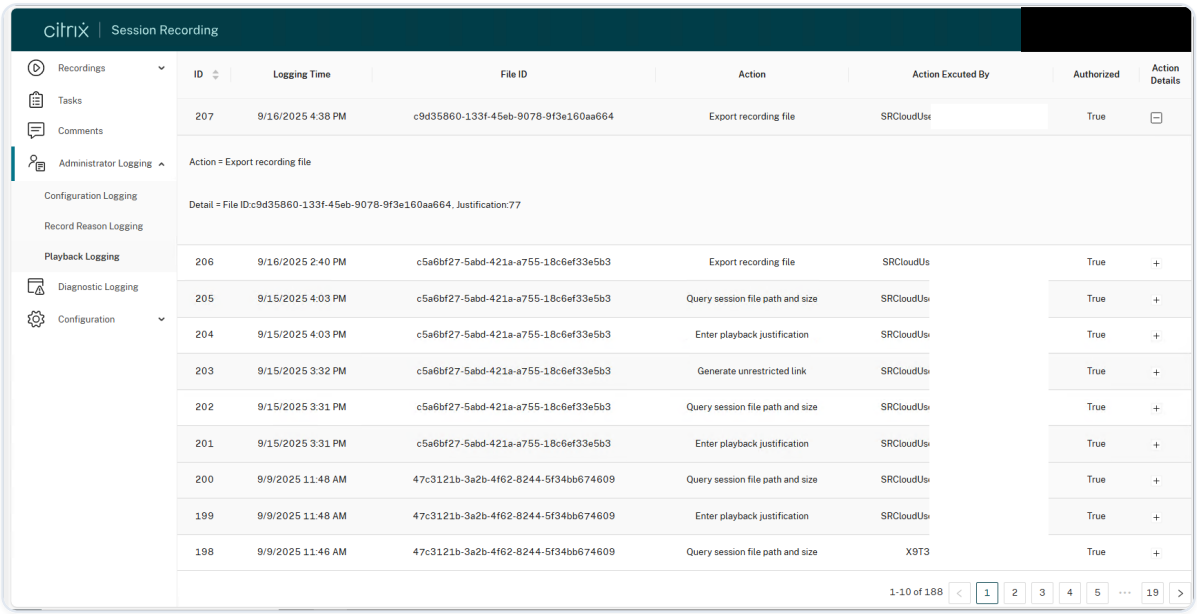
  b. This page displays the real-time status of all export tasks, including "In Progress," "Completed," "Pending," or "Failed."



- To audit export activities:

  a. In the left navigation pane, expand **Admin Logging** and click **Playback Logging**.

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



Session recording media task service

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

Prerequisites

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

- 8-core CPU
- 16 GB RAM

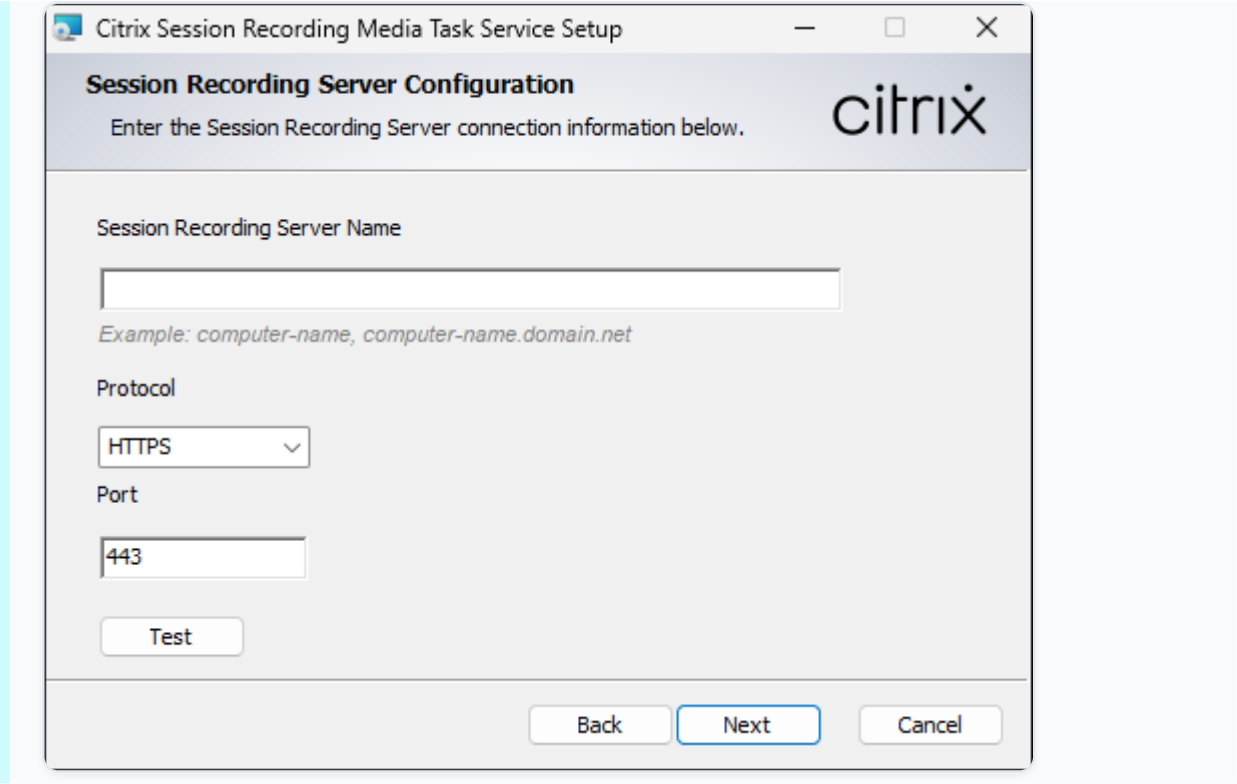
Installation and configuration

Follow the steps below to install and configure the Task.

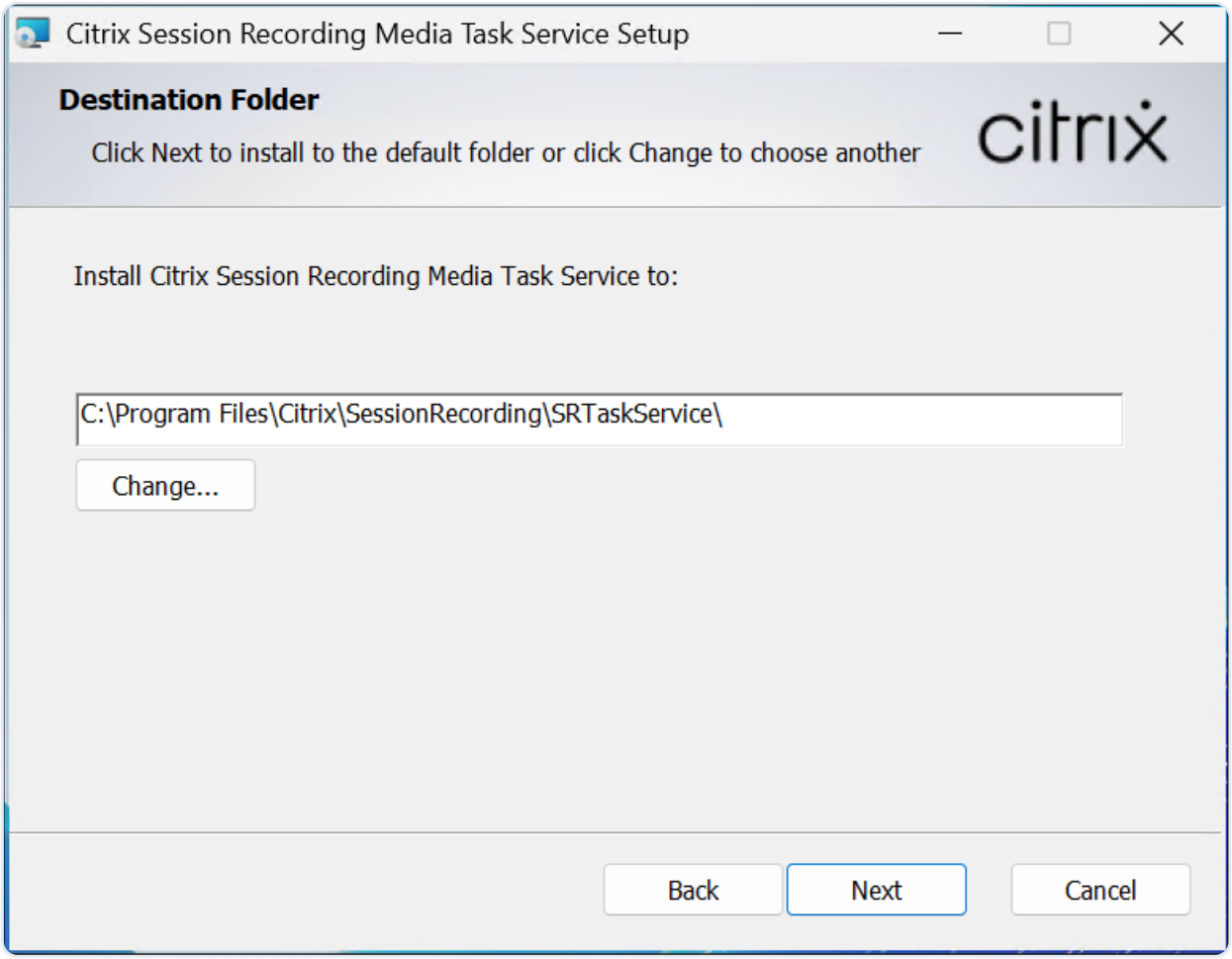
Step 1: Install the Session Recording media task service

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

> **Note:**
>
> When deploying in a load-balanced environment, enable session persistence on your load balancer and select SOURCEIP (or equivalent) as the persistence type.
>
> - For Citrix NetScaler/ADC, see (https://docs.netscaler.com/en-us/citrix-adc/2607 LTSR/getting-started-with-citrix-adc/load-balancing/configure-persistence-settings.html).
> - For Azure Load Balancer, see Session Persistence.

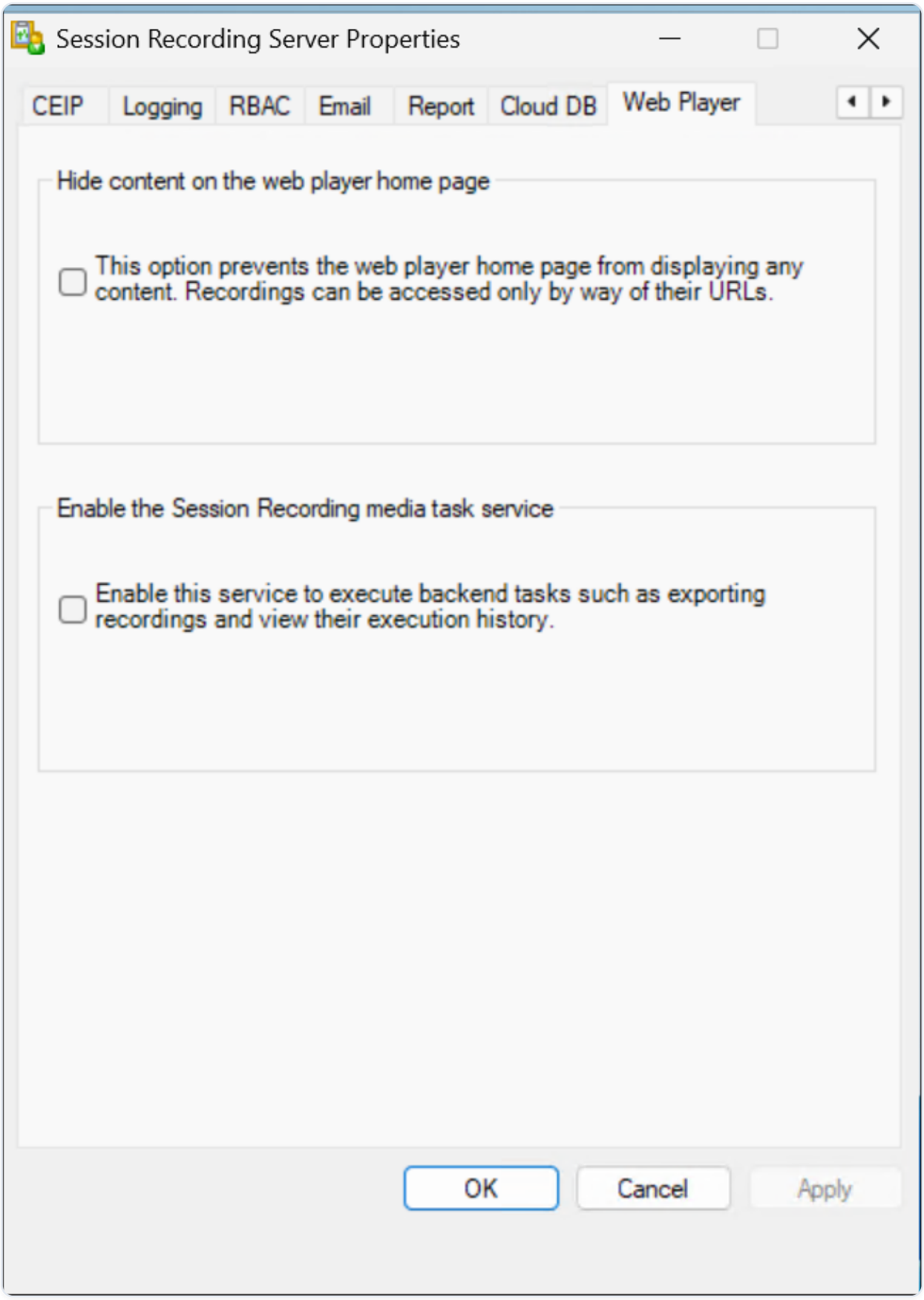


3. On the Destination Folder screen, confirm or change the installation path, and then complete the installation.



Step 2: Enable the media task service on the server

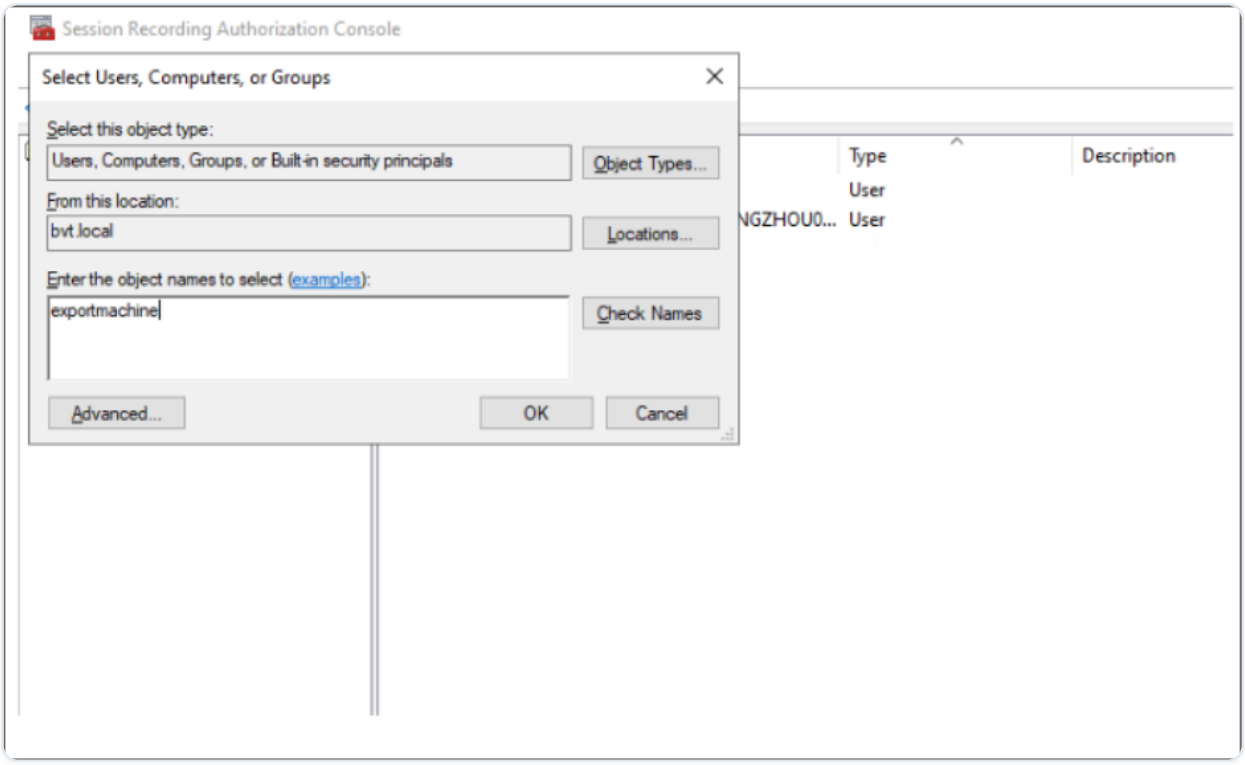
1. On the Session Recording Server, open Session Recording Server Properties.
2. Switch to the Web Player tab.
3. Check the Enable the Session Recording media task service checkbox.
4. Click Apply. This action allows the service to perform backend tasks, such as exporting recordings.



Step 3: Assign permissions for the media task service

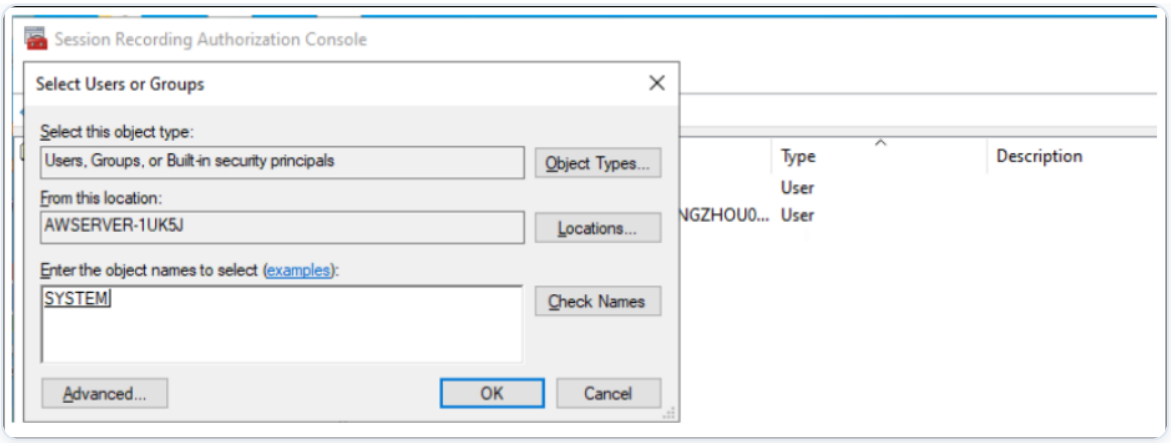
1. On the Session Recording Server, open the Session Recording Authorization Console.

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



Note:

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



Step 4 (Optional): Configure a custom export directory

Configure a custom path for exporting recordings by changing the registry key value for:

`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SRTaskService\SROutputDir`

AI-powered insights for session recording

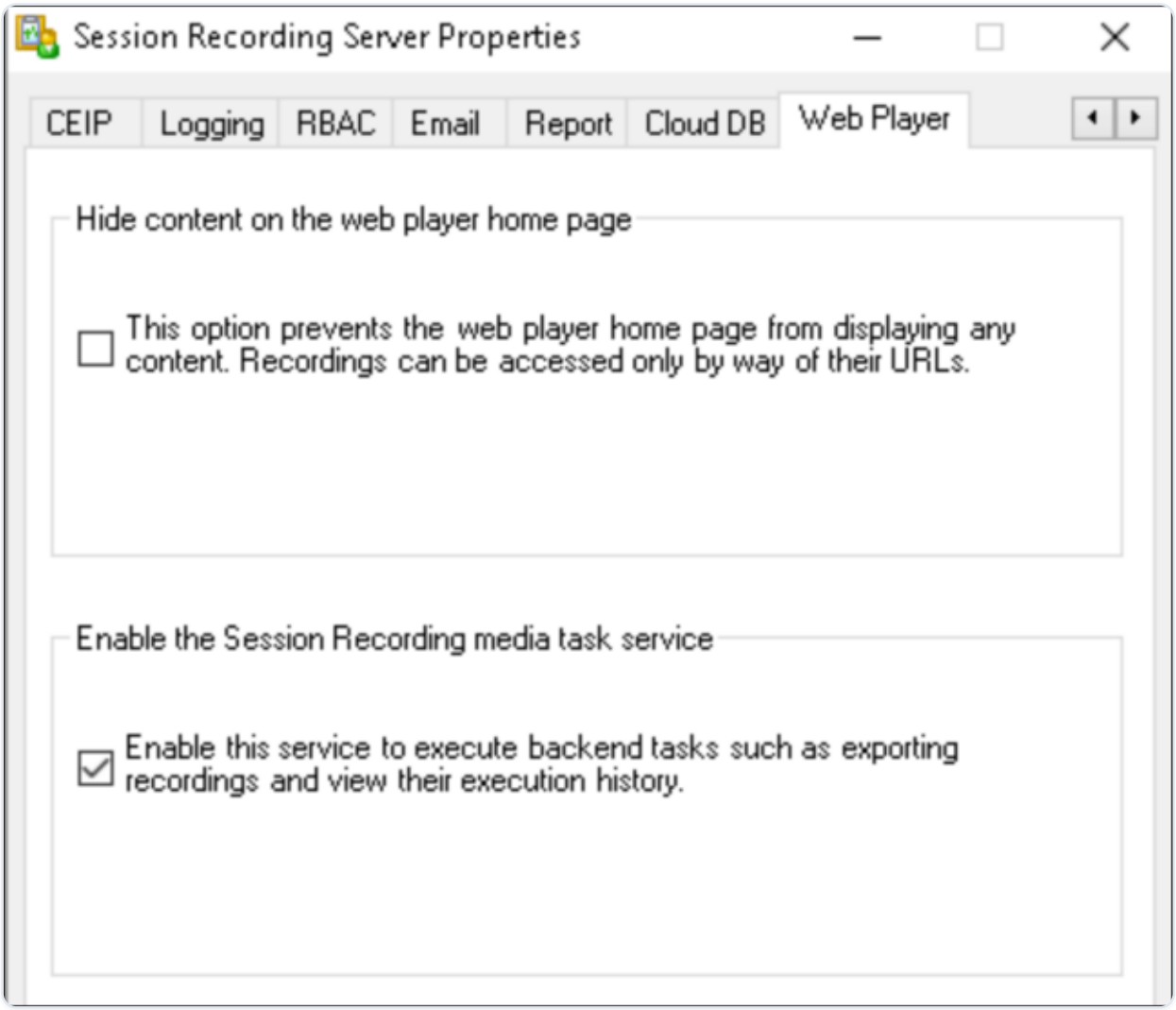
Overview

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

Prerequisites

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

- Citrix Session recording server version 2607 LTSR or later is installed.
- Session recording media task service version 2607 LTSR or later is installed. Refer to the official setup guide. Enable the media task service in Session Recording Server Properties:



Configuration

Session recording is properly configured and operational.

- Session recording web console (formerly Web Player) must use HTTPS.
- Access to an OpenAI-compatible API endpoint (e.g., Azure OpenAI) is available for AI analysis.
- Grant PriviledgedPlayer role in Session Recording Authorization Console.

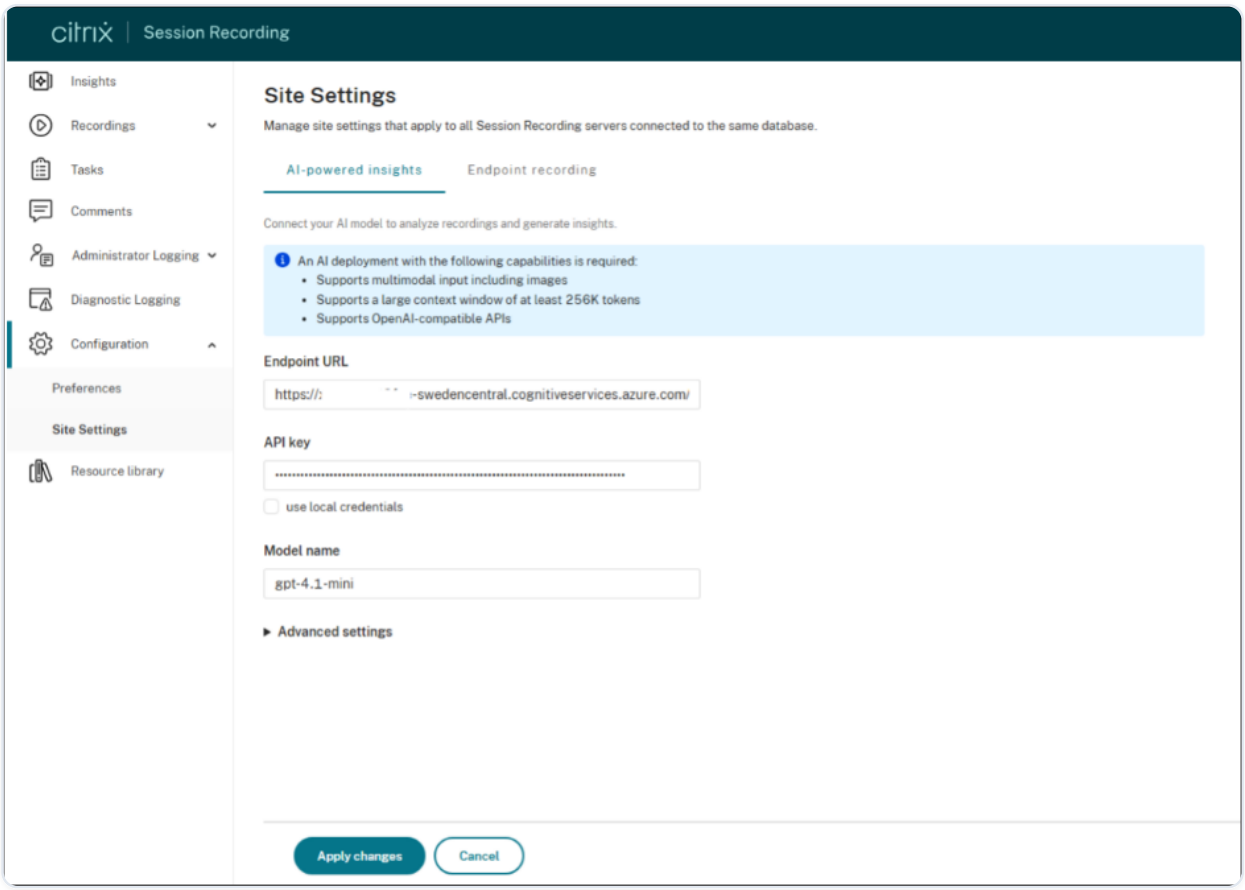


Get Started

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

Configure AI-Powered Insights in Site Settings

1. Open the **Session Recording Web Console** and navigate to **Site management**.
2. In the **Site Settings** panel, locate the **AI-powered insights** section.



3. Provide the following parameters:

- **Endpoint URL**: The API endpoint of your AI model (e.g., https://example.azure.com/openai/v1/).
- **API Key**: The authentication key for your AI service.

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

4. (Optional) Configure Advanced Settings:

- **Maximum number of analysis tasks per media server**: Defines how many AI analysis tasks can run simultaneously on a single media server (e.g., set to `2`).
- **Sample rate**: Determines how frequently video frames are analyzed.

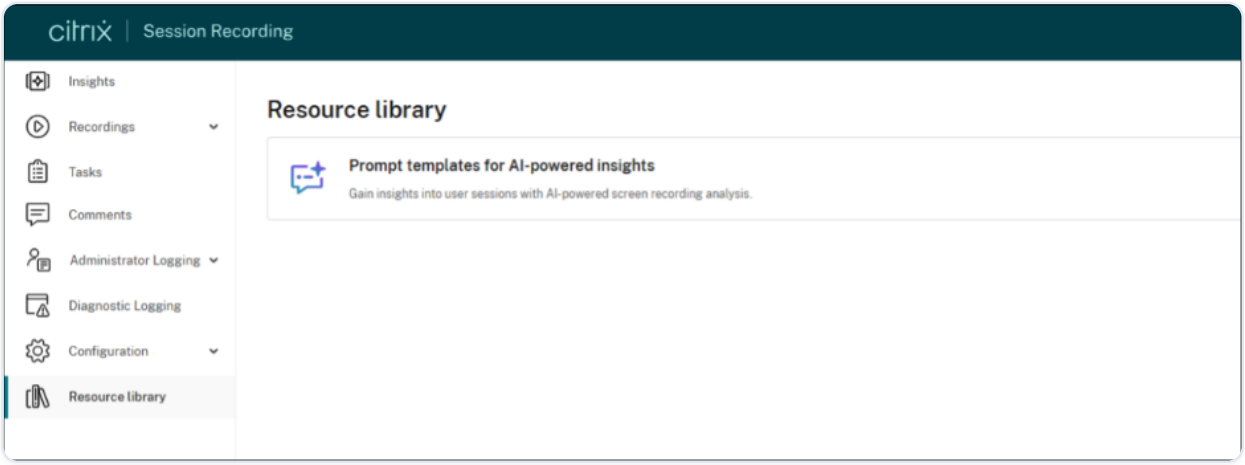
- **Frame difference threshold**: Sets the percentage of pixel changes required to consider a frame as "changed."
- **Batch size**: The number of frames sent to the AI model per batch.

5. Click **Apply changes** to save the configuration.

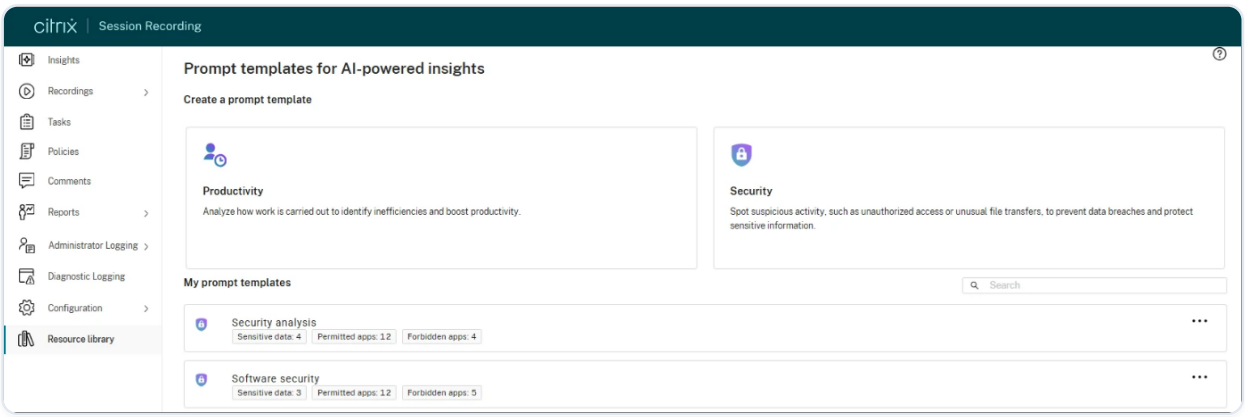
> **Note:**
>
> Session Recording will not collect your data that is sent to AI models.

Configure Prompt Templates

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



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



Productivity Prompt Template

When creating or editing a productivity prompt template, configure:

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

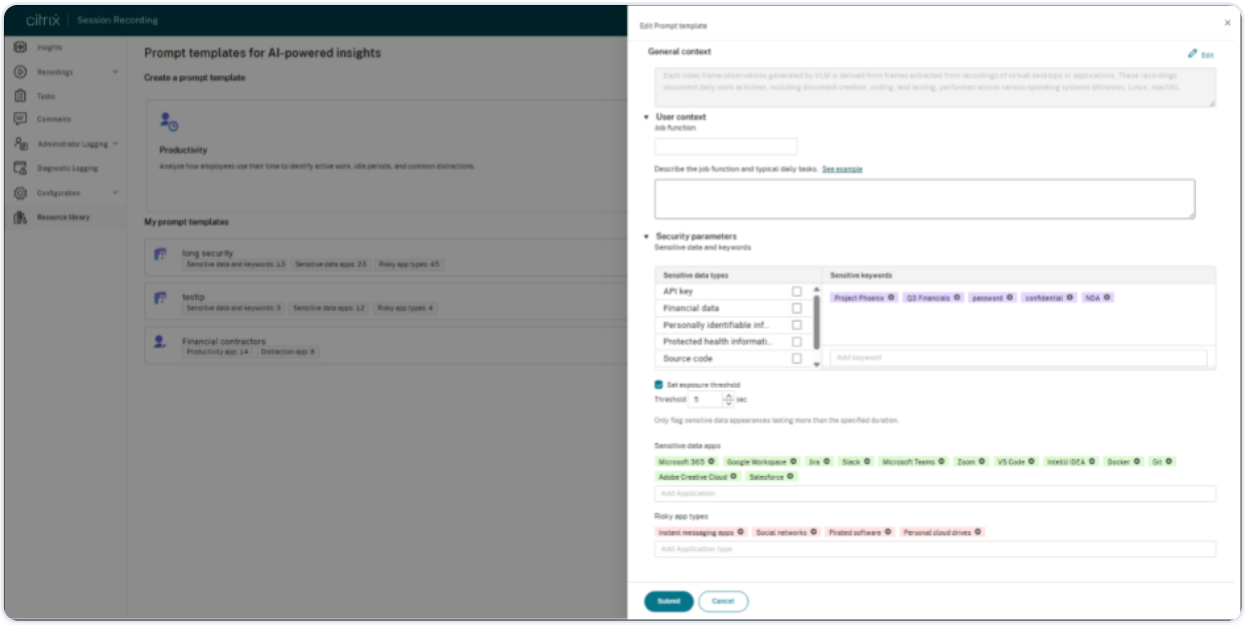


Security prompt template

When creating or editing a security prompt template, configure:

- **General context:** Explains the overall purpose of the template.
- User context
  - **Job function:** Enter the user's role.
  - **Describe the role and typical daily tasks:** Provide a short description of the responsibilities.
- Security parameters
  - **Sensitive datatypes:** Categories beyond keywords (e.g., Source code, Financial data).
  - **Sensitive Keywords:** Define keywords indicating sensitive data (For example, **password**, **credit card**).
  - **Set exposure threshold:** Minimum duration (in seconds) sensitive data must remain visible on screen before being flagged.

- **Sensitive data apps:** Apps where sensitive data is likely to appear (e.g., Microsoft Excel, Dynamics 365).
- **Risky app types:** High-risk categories (e.g., Social networks, Personal cloud drives).



Security Templates and Sensitive Data Definitions

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

Pre-defined Sensitive Data Categories

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

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

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

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

2. **Financial Information**

   Detects banking and payment-related data, including:

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

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

   Detects medical and health-related records, including:

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

4. **Source Code**

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

5. **API Keys**

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

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

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

> **Note on AI Contextual Analysis:**

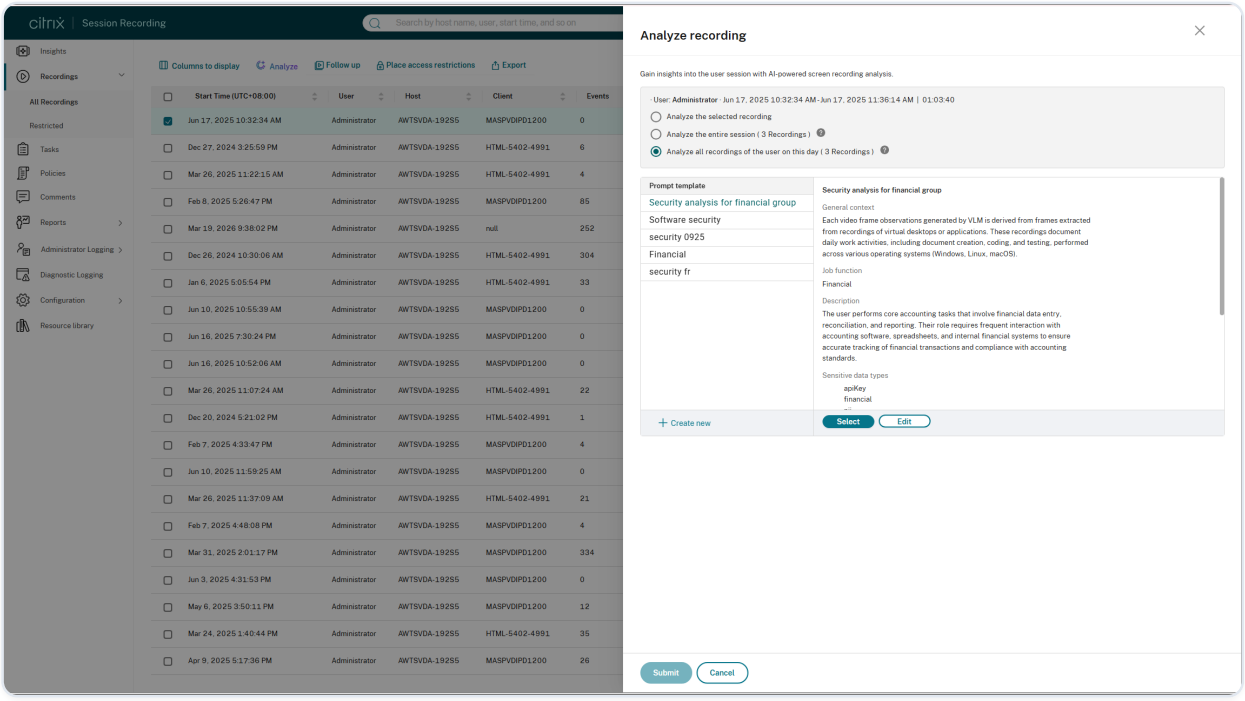
> In addition to keyword matching, the AI model leverages contextual information to improve judgment accuracy. This helps distinguish between sensitive data and non-sensitive text that may share similar formats.

Customizing Definitions

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

Select Recordings for Analysis

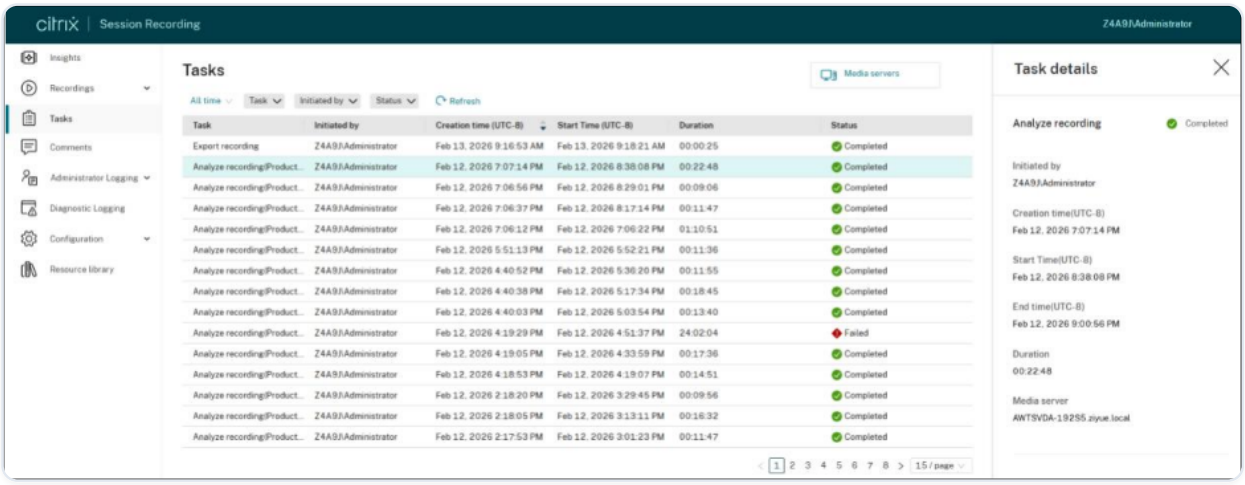
1. Navigate to **Recordings** in the **Session Recording Console**.
2. Use filters or search to locate the session(s) for analysis.
3. Select one or more video recordings, then click **Analyze**.
4. In the dialog:
    - Select a prompt template from the **Resource Library** or **Create new**.
    - Choose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



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

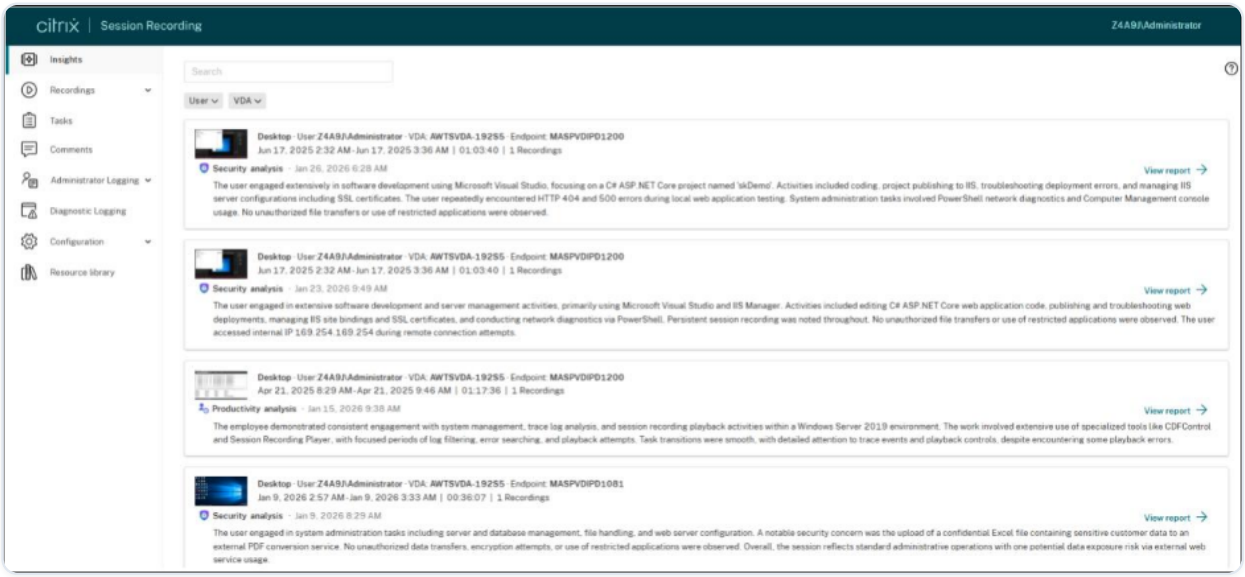
Monitor Task Progress

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



Review AI-Powered Insights

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

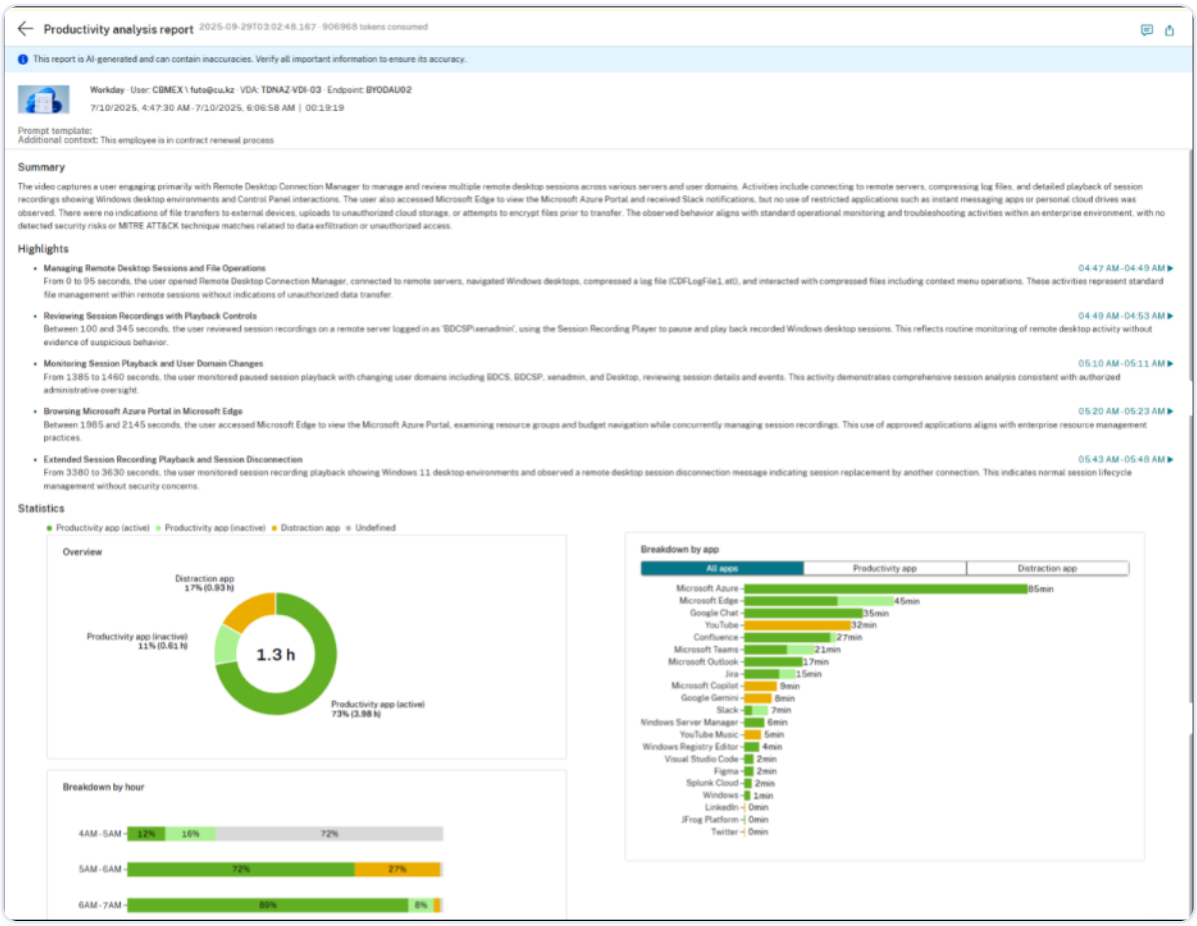


Detailed Reports

Productivity Analysis Report

Includes:

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

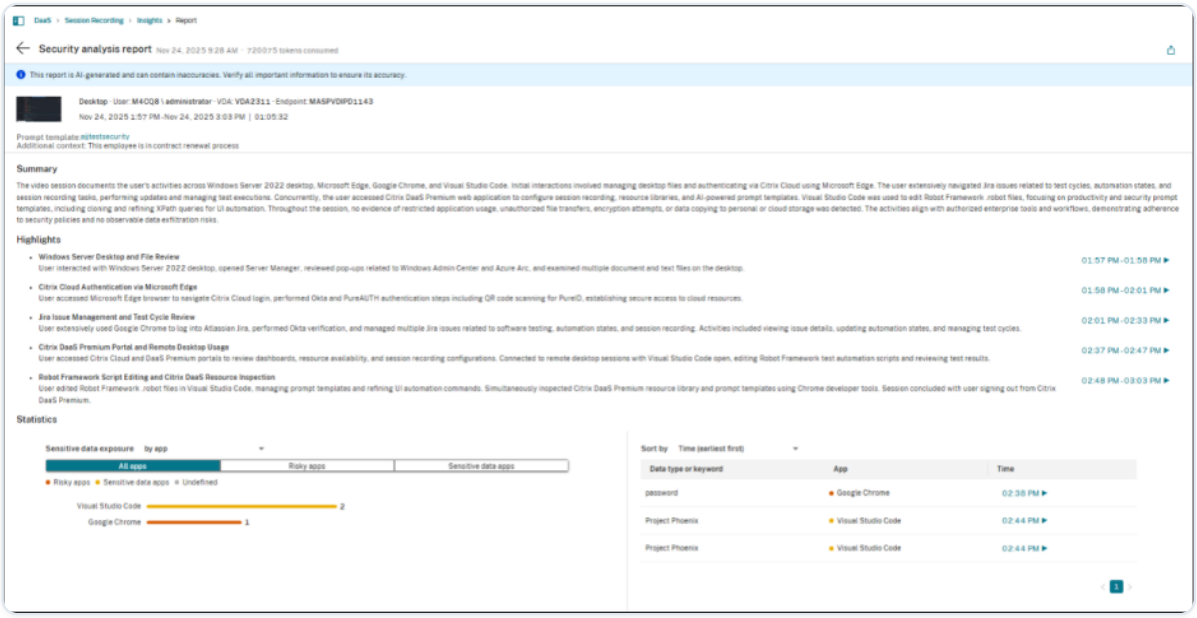


Security Analysis Report

Includes:

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

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



Limitations

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

Legal and Privacy Disclaimer

The AI Insights in Session Recording feature and its provided prompt templates as well as the outputs, reports and/or information that may be generated from utilizing this feature (“AI Insights”) are not intended to provide, legal, security, regulatory and/or technical advice or judgement to you in any form and all information created and derived from utilizing AI Insights is provided “As-Is”, with no warranties or representations, whether express or implied, regarding the AI Insights, including, without limitation, that the information is accurate, error-free or meets any conditions of merchantability or fitness for a particular purpose.

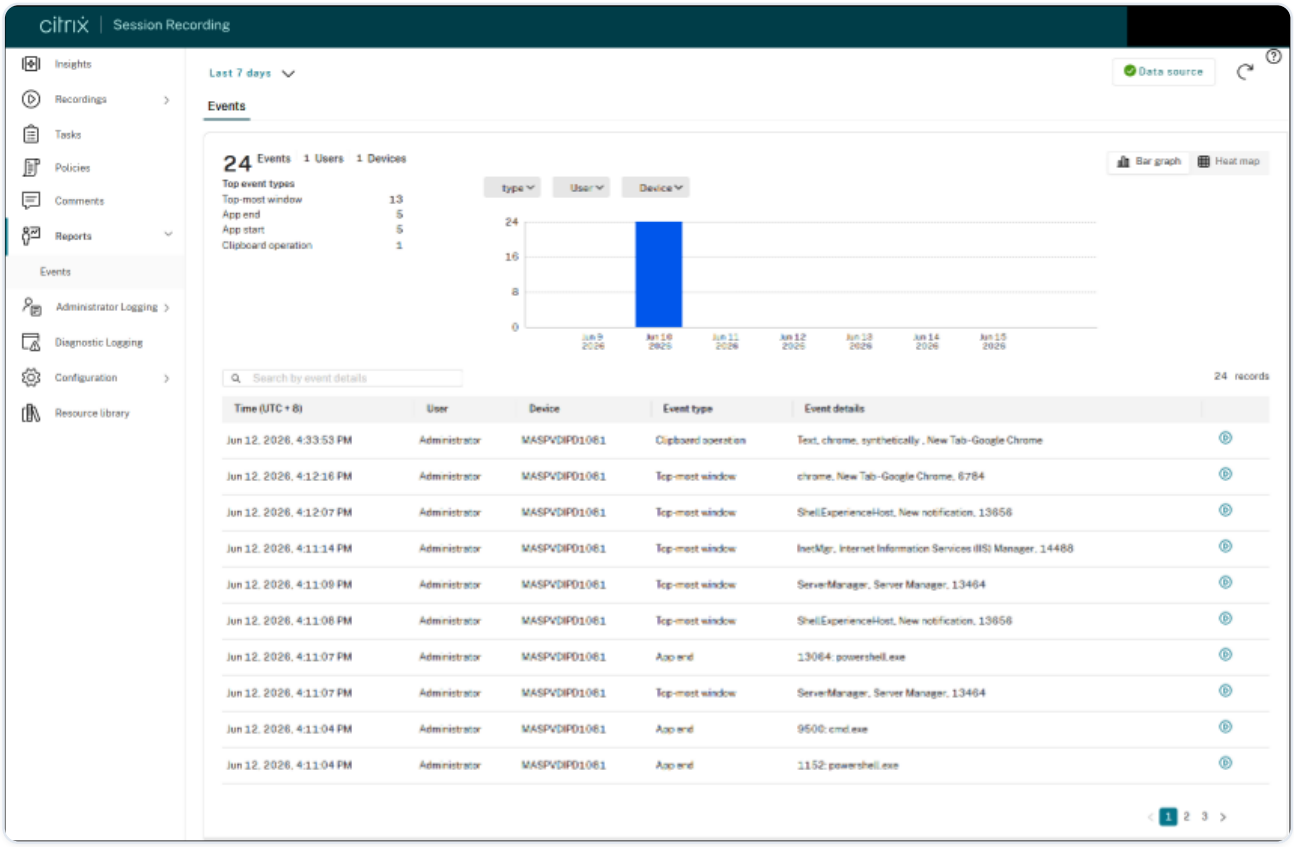
Customer is solely responsible for the legal and regulatory compliance of processing any personal data or sensitive information through utilizing this feature, including but not limited to balancing your internal data classification obligations, global data and/or AI regulatory compliance as well as

industry related compliance obligations related to your business or customer market. Customer is advised to consult their own designated subject matter expert before utilizing AI-Insights.

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

Site-level user activity reporting

Session Recording uses event detection in recorded sessions to display event data in the web console, offering a site-wide view of user activity.



With site-level user activity reporting, you can:

- Filter events by category to quickly locate specific activity
- Identify abnormal behavior across your site
- Gain a broader understanding of user activity patterns

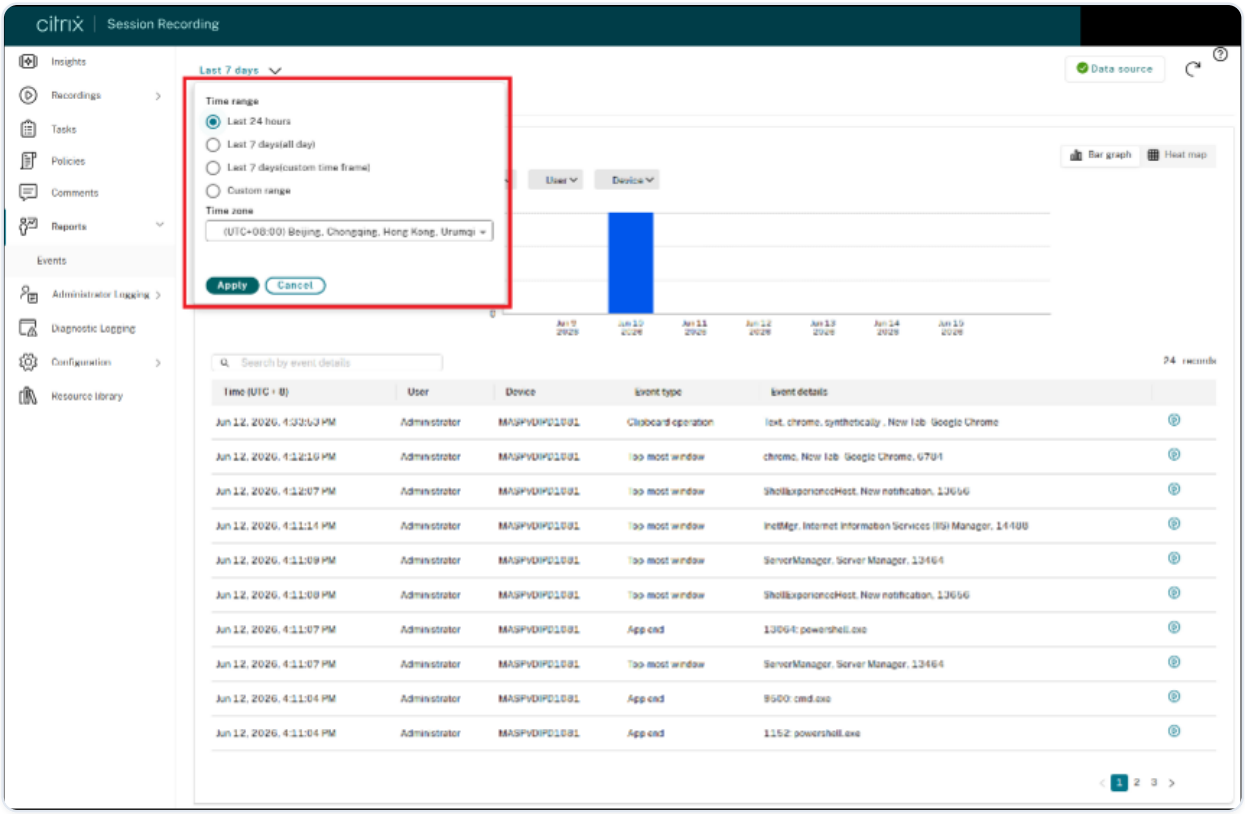
Prerequisites

- Session Recording 2607 LTSR or later
- A configured and active event detection policy that includes the event types you want to monitor

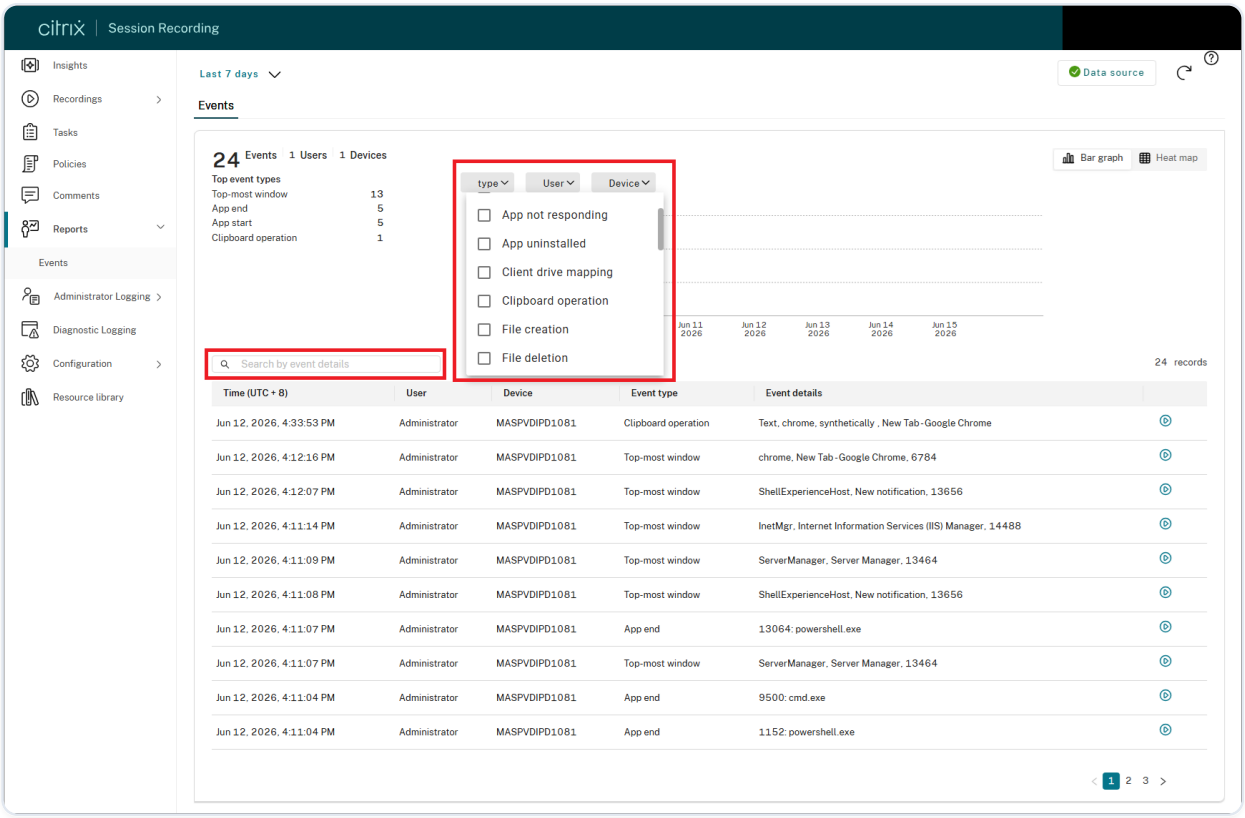
For more information, see Configure event detection policies.

View site-level event reports

1. In the Session Recording web console, select **Reports** from the left navigation pane.
2. Select **Events**.
3. Specify the time range and time zone.



4. Use the filters to narrow results by event type, session user, or client device. You can also use the search box to find events by keyword. Filters are combined using AND logic.



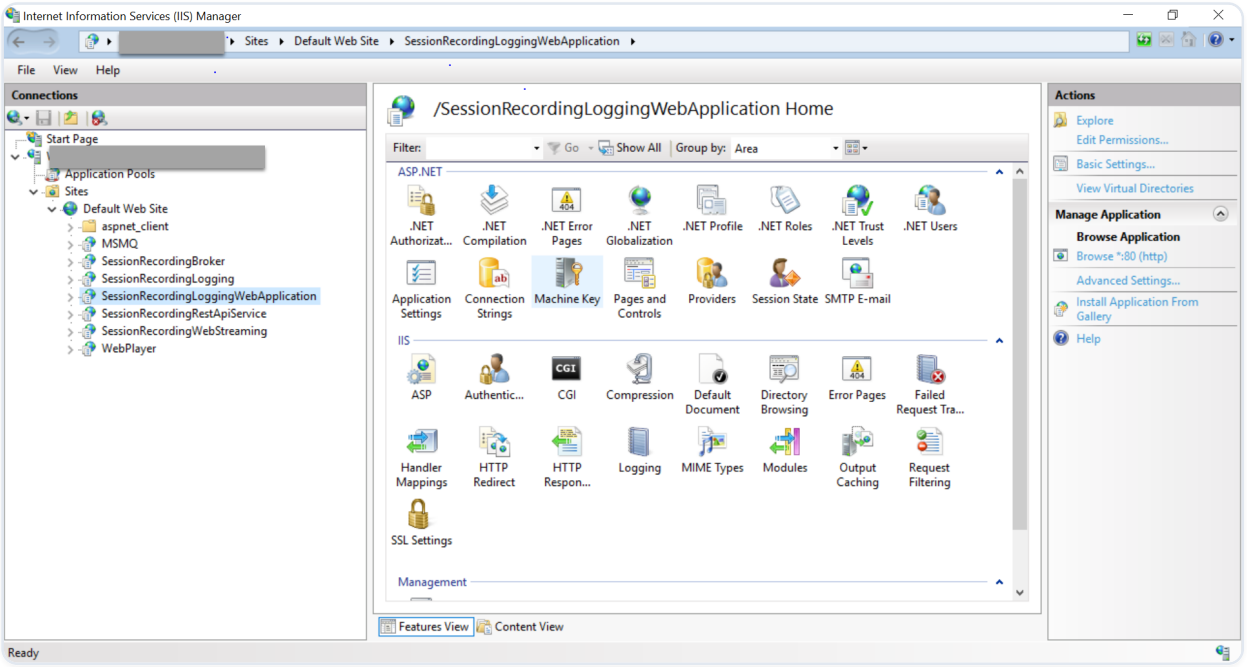
5. Click the play button next to an event to navigate to the recording playback page, where events and comments are shown in context.

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.



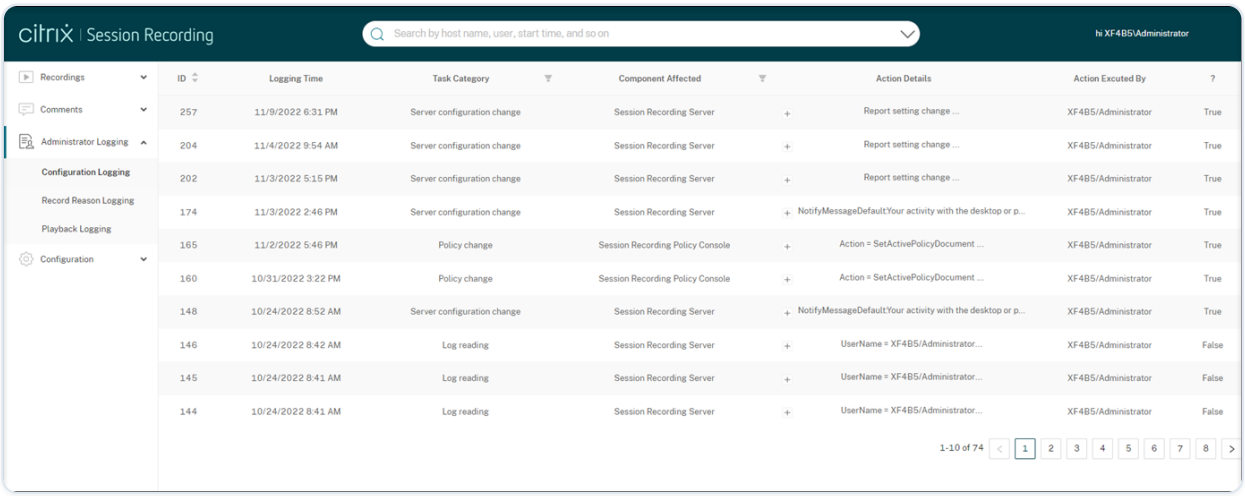
Steps

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

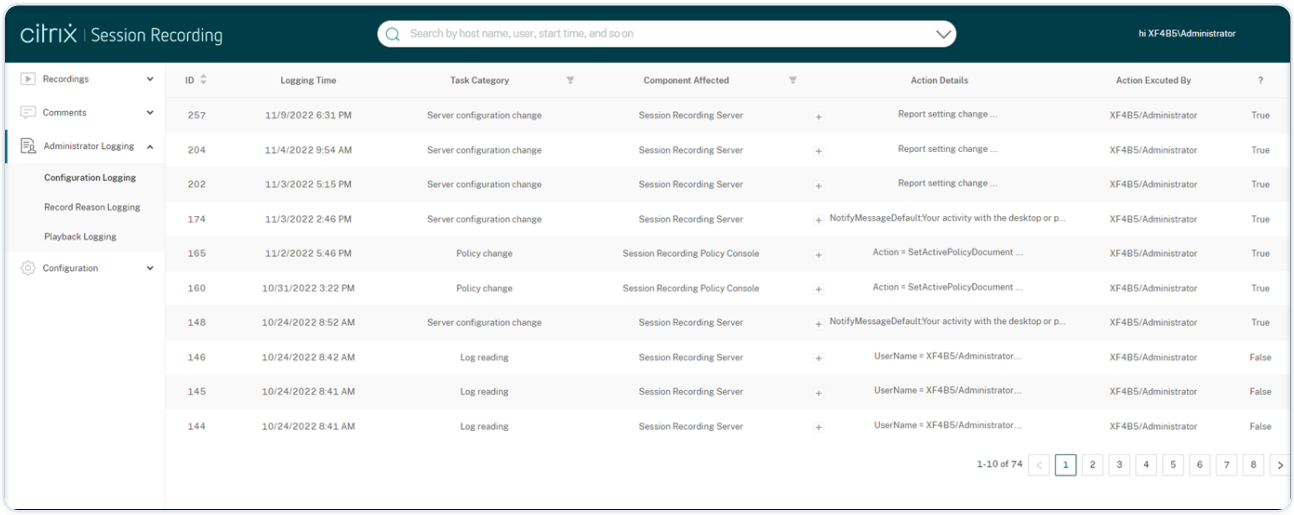
1. Open a web browser and visit the webpage for administrator logging.
   - **For HTTPS:** `https://servername/WebPlayer/#/logging/config` and `https://servername/WebPlayer/#/logging/record`, where `servername` is the name of the machine hosting the Session Recording server.
   - **For HTTP:** `http://servername/WebPlayer/#/logging/config` 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



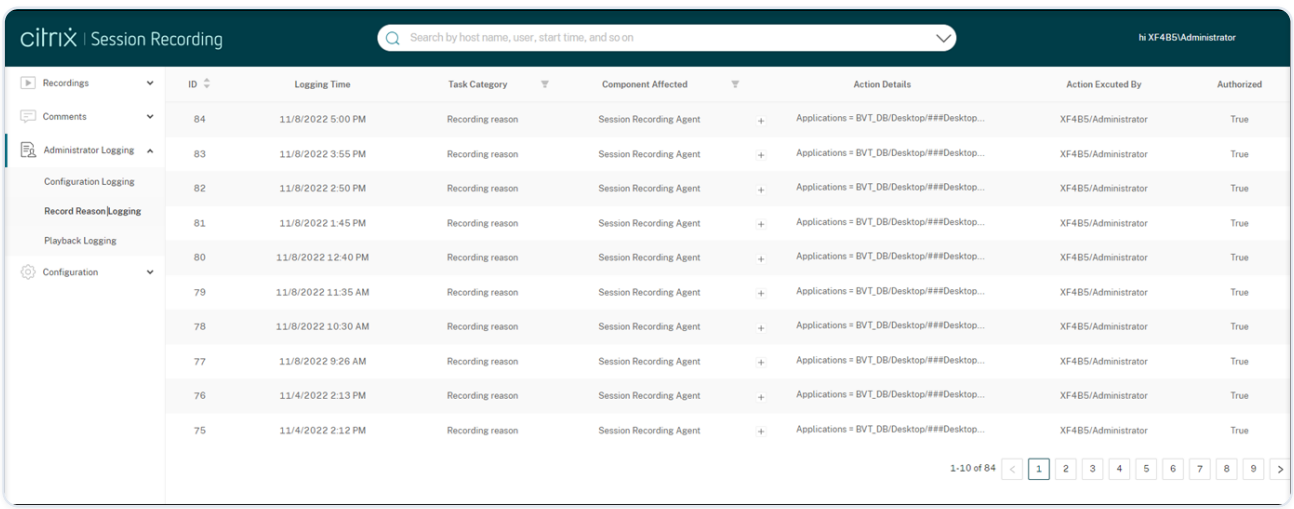
This part logs the following administrator activities:

- **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.

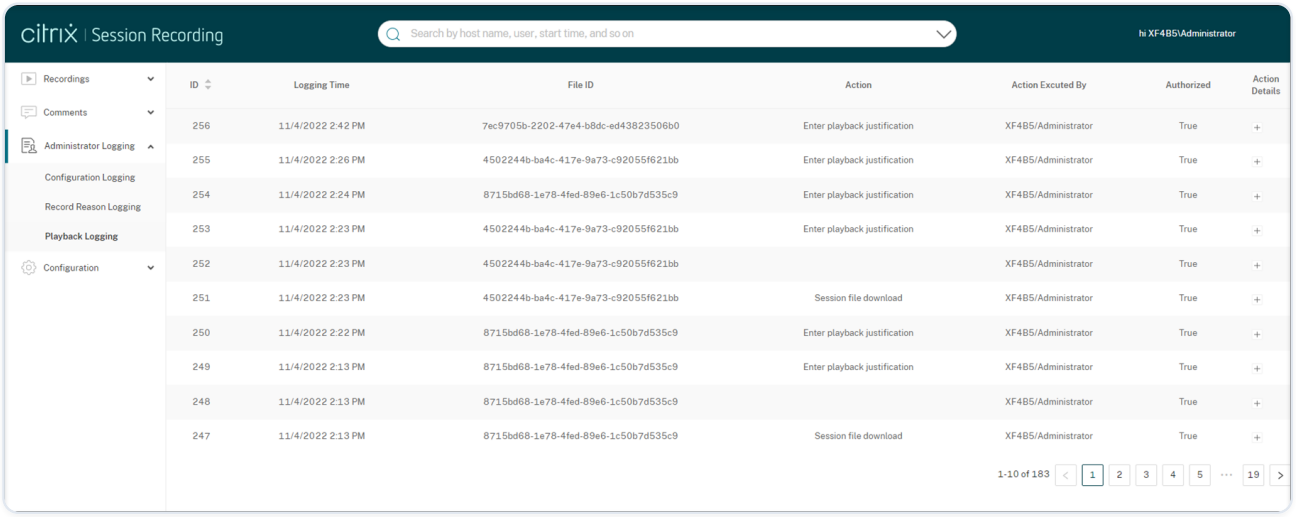
Recording reason logging



This part logs which policies have triggered recordings.

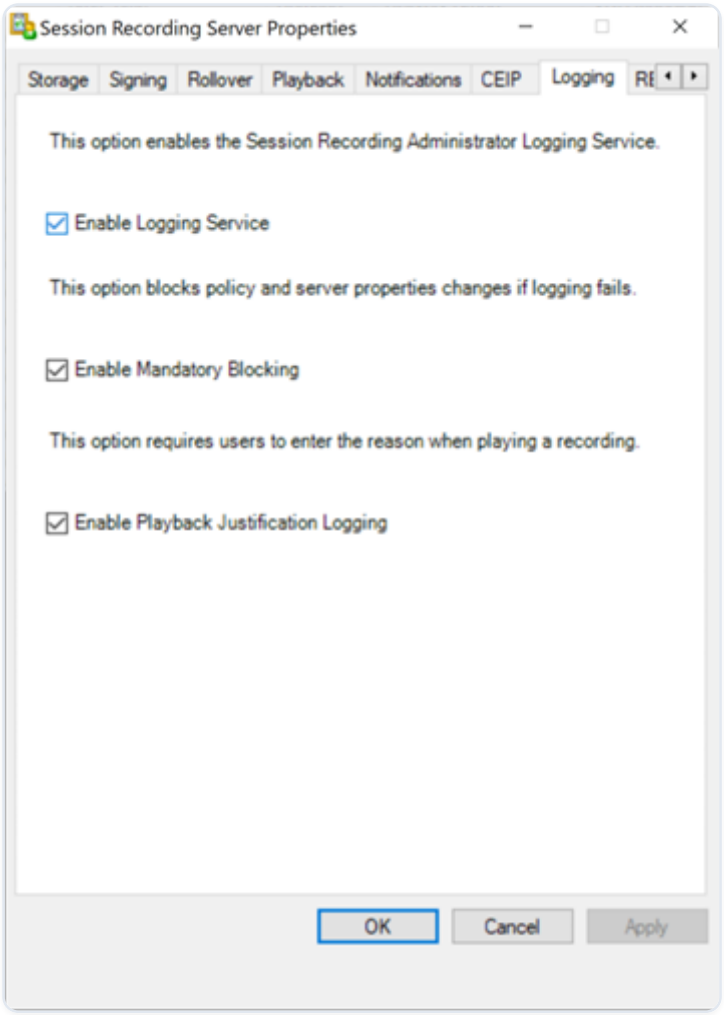
To enable recording reason logging, enable both administrator logging and recording reason logging on your Session Recording servers. If administrator logging is disabled, enabling recording reason logging does not take effect. For information about enabling recording reason logging, see Disable or enable the recording reason logging.

Playback logging



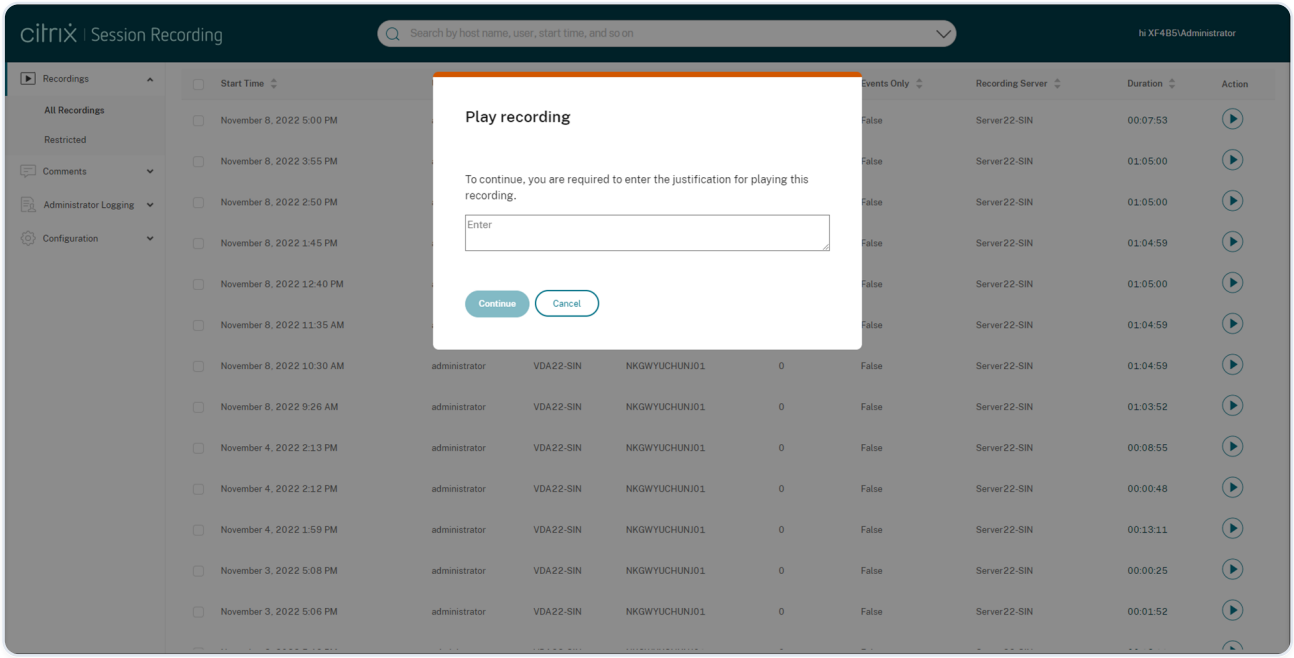
This part logs playback-related actions. For more information about each log record, click the plus sign (+) in the **Action Details** column.

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.

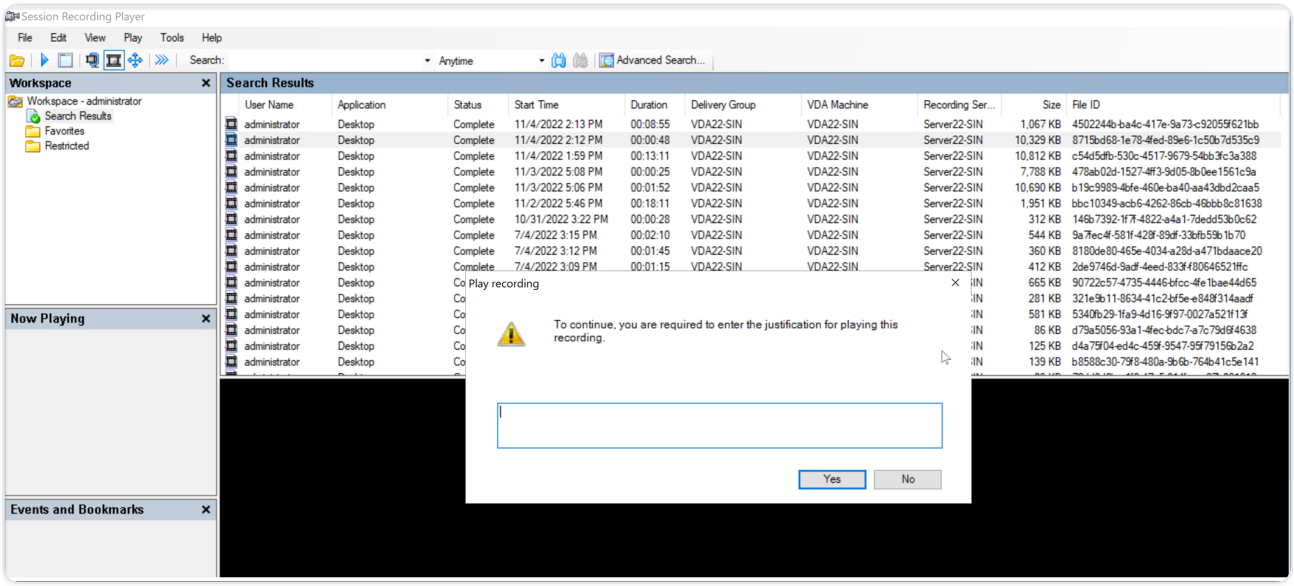


With playback justification logging enabled, each time you play a recording, a dialog box appears, asking you to enter a playback justification. For example, see the following screen captures:

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

Monitor Session Recording agents

All VDAs with Session Recording agents installed are monitored. You can run **SsRecUtils.exe** on the Session Recording server to:

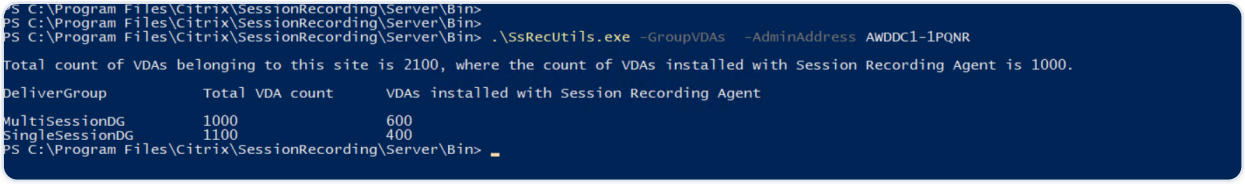
- Check the counts of VDAs with and without Session Recording agents installed.
- View the connection status of all Session Recording agents.

To check the counts of VDAs with and without Session Recording agents installed

1. Start a command prompt as an administrator and change the drive to the **<\Session Recording server installation path>\Bin** folder.
2. Run a command similar to the following:

   ```
   SsRecUtils.exe /GroupVDAs -AdminAddress AWDDC1-1PQNR
   ```

   The **AdminAddress** parameter specifies the FQDN of your Delivery Controller. It allows you to view the counts of VDAs in your site and the counts of VDAs installed with Session Recording agents. For an example output, see the following screen capture:



To View the connection status of all Session Recording agents

1. Start a command prompt as an administrator and change the drive to the **<\Session Recording server installation path>\Bin** folder.
2. Run a command similar to the following:

```
SsRecUtils.exe  /ListVDAs -AdminAddress AWDDC1-1PQNR -DeliverGroup
BVT_DG [-InstalledSRAgent True -MachineName  AWVDA-1PQNR
-MaxRecordCount 1000 -OffSet 0]
```

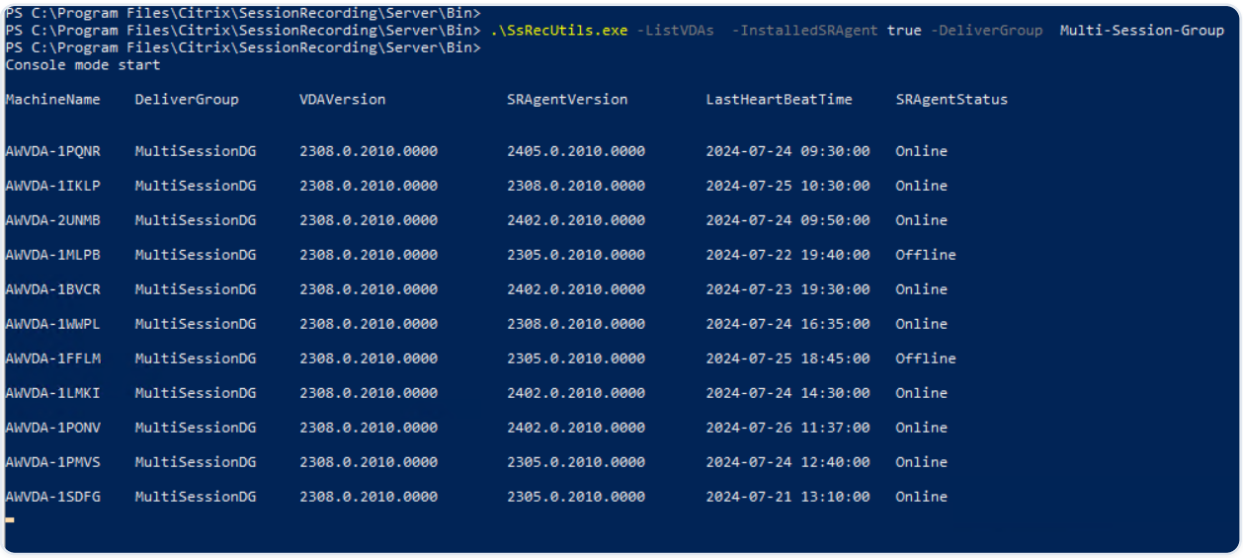
This command displays a detailed list of VDAs, sorted in ascending order based on when their Session Recording agent was registered (oldest to newest).

Where,

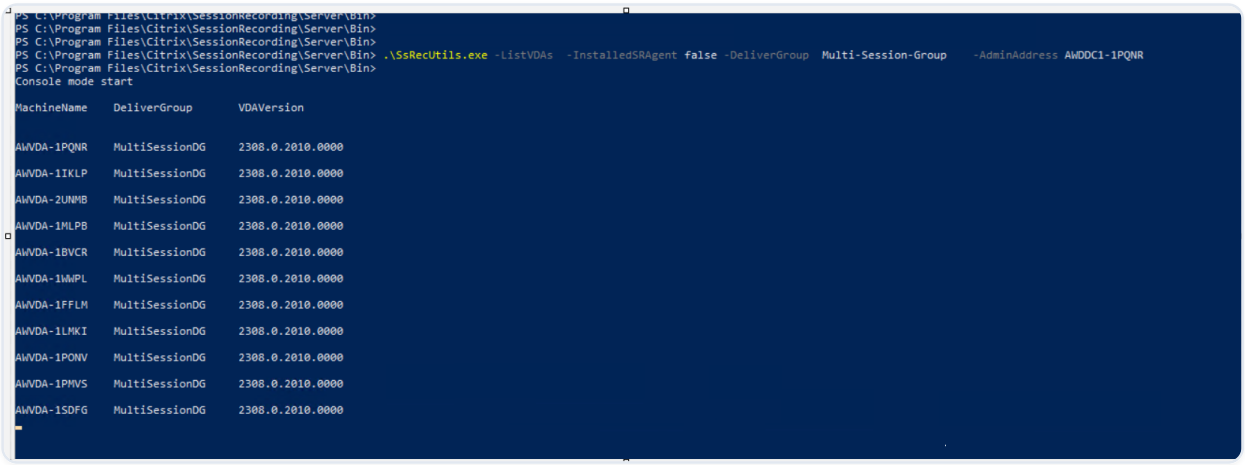
- **AdminAddress** (mandatory) specifies the FQDN of your Delivery Controller. It allows you to list VDAs in your site.
- **DeliverGroup** (mandatory) specifies a delivery group.
- **InstalledSRAgent** (optional, default: **True**) controls which VDAs to list. **True**: List only VDAs installed with the Session Recording agent. **False**: List only VDAs without the agent.
- **MachineName** (optional) specifies the machine name of a target VDA.
- **MaxRecordCount** (optional, default: 1000) limits the number of output records.
- **Offset** (optional, default: 0) specifies the starting point for data retrieval, skipping the first **Offset** items.

For example command outputs, see the following screen captures:

- Example output when **InstalledSRAgent** is set to **True**:



- Example output when **InstalledSRAgent** is set to **False**:


PS C:\Program Files\Citrix\SessionRecording\Server\Bin>
PS C:\Program Files\Citrix\SessionRecording\Server\Bin>
PS C:\Program Files\Citrix\SessionRecording\Server\Bin>
PS C:\Program Files\Citrix\SessionRecording\Server\Bin> .\SsRecUtils.exe -ListVDAs -InstalledSRAgent false -DeliverGroup Multi-Session-Group -AdminAddress AWDDC1-1PQNR
PS C:\Program Files\Citrix\SessionRecording\Server\Bin>
Console mode start
MachineName DeliverGroup VDAVersion
AWVDA-1PQNR MultiSessionDG 2308.0.2010.0000
AWVDA-1IKLP MultiSessionDG 2308.0.2010.0000
AWVDA-2UNMB MultiSessionDG 2308.0.2010.0000
AWVDA-1MLPB MultiSessionDG 2308.0.2010.0000
AWVDA-1BVCR MultiSessionDG 2308.0.2010.0000
AWVDA-1WWPL MultiSessionDG 2308.0.2010.0000
AWVDA-1FFLM MultiSessionDG 2308.0.2010.0000
AWVDA-1LMKI MultiSessionDG 2308.0.2010.0000
AWVDA-1PONV MultiSessionDG 2308.0.2010.0000
AWVDA-1PMVS MultiSessionDG 2308.0.2010.0000
AWVDA-1SDFG MultiSessionDG 2308.0.2010.0000

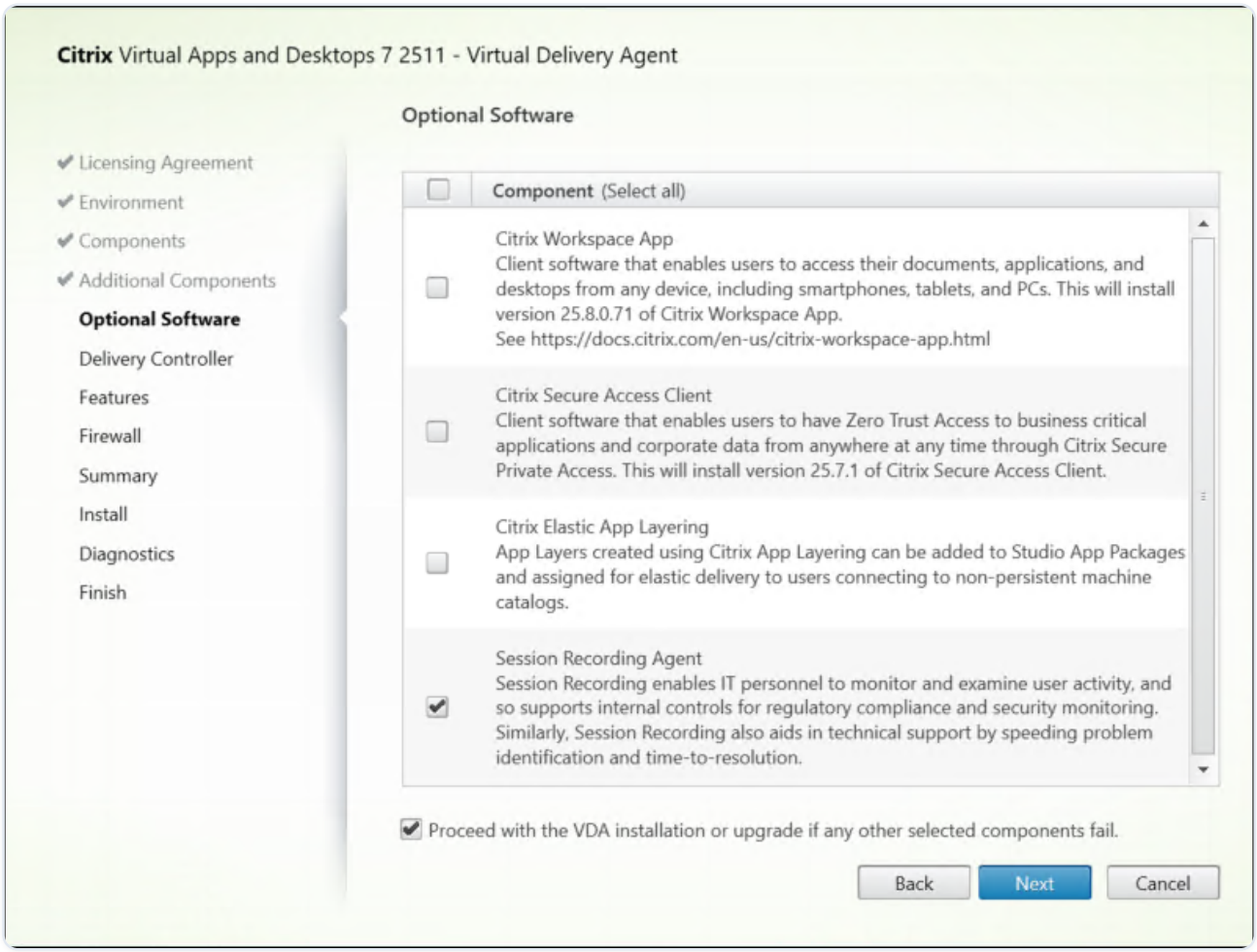
Manage basic deployment agents

You can use Session Recording to manage basic deployment agents. This feature provides a lightweight method to deploy Session Recording. You can use this deployment method for utilizing Session Recording basic functionalities--record active sessions to MP4 files without deploying the backend components such as Session Recording Servers, player, databases, and consoles.

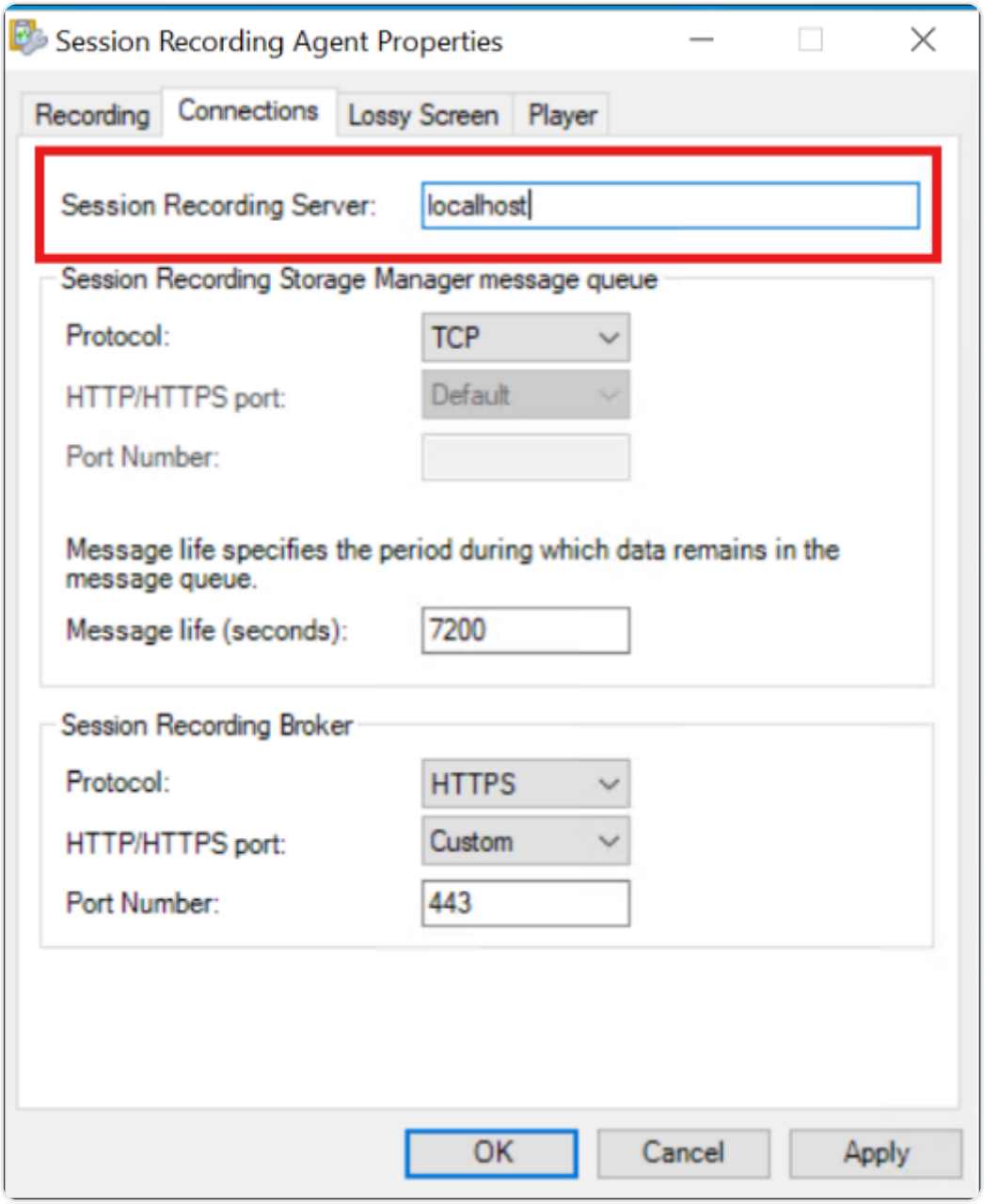
Installation

The Session Recording Agent is installed along with the Citrix Virtual Delivery Agent (VDA) by default.

- New installation: When installing or upgrading to VDA version 2511 or later, the Session Recording Agent is installed and works in deployment mode.



- Existing installation: If you already have a Session Recording agent installed, you can switch to the basic deployment mode by upgrading the agent to version 2511 or later and changing the Session Recording Server Address to localhost in the Session Recording Agent properties.



Use the basic deployment agent

In the basic deployment mode, recordings can be triggered manually by end users or administrators using the Citrix Virtual Desktop Assistant or PowerShell commands. They can also be triggered by hotkeys or dynamic recording.

Start or stop recording by using Citrix Virtual Desktop Assistant

Citrix Virtual Desktop Assistant is installed by default in CVAD. It includes a built-in Session Recording page that allows customers to manually record their active virtual desktop sessions. This feature enables customers to capture screen activity as MP4 video clips for troubleshooting, collaboration, and session review.

For more information, see, Citrix Virtual Desktop Assistant application.

Start or stop recording by using PowerShell commands

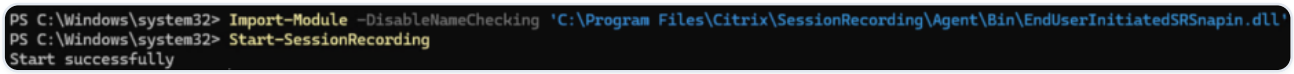
Both end users and administrators can use PowerShell commands to manage recordings.

Import the Session Recording module

Before running any commands, ensure the necessary module is imported.

Open PowerShell and Import the module by running:

```
Import-Module -DisableNameChecking 'C:\Program Files\Citrix\SessionRecording\Agent\Bin\EndUserInitiatedSRSnapin.dll'
```



Available Commands

The following table lists three PowerShell commands that provide for end user triggered session recording.

COMMAND	DESCRIPTION
Start-SessionRecording	Starts recording the active session in which the command is executed. To record a specific active session, use the `-SessionId <ID>` parameter (requires local administrator privileges). For more information, run `Get-Help Start-SessionRecording` to see the command online help.
Stop-SessionRecording	Stops recording the active session in which the command is executed. To stop recording a specific active session, use the `-SessionId <ID>` parameter (requires local administrator privileges). Note: Users can only stop

COMMAND	DESCRIPTION
	recordings they initiated. They cannot stop recordings triggered by dynamic or policy-based recording. For more information, run `Get-Help Stop-SessionRecording` to see the command online help.
Get-SessionRecordingStatus	Retrieves the recording status of the active session in which the command is executed. To get the status of a specific active session, use the `-SessionId <ID>` parameter. For more information, run `Get-Help Get-SessionRecording Status` to see the command online help.

Example 1: End-user triggered recording

End users can trigger recordings for their current active session to capture operations dynamically (for example, for troubleshooting purposes).

The user can perform the following steps inside the session:

1. Launch PowerShell from the session desktop.
2. Import the module as described in the previous section.
3. Use the `Get-SessionRecording Status` command to check the recording status, ensure the session is not already being recorded.
4. Use the `Start-SessionRecording` command to start recording the session.
5. Use the `Get-SessionRecordingStatus` command to check the recording status, ensure the session is being recorded. The status is supposed to be **Recording**.

```
PS C:\Program Files\Citrix\SessionRecording\Agent\Bin> Get-SessionRecordingStatus
--- Recording Status Details ---
  Status:              Recording
  Recording Location:  C:\Users\dzl\Videos\SessionRecordings\QHVDA5 OCT_dzl 2025-10-15 at 12.00.30 PM.mp4
  Size:                341048 Bytes
  Duration:            46 Seconds
  PrerecordingEnabled: True
--------------------------------------
```

6. Reproduce the issue or perform the operations that need to be documented.
7. Use the `Stop-SessionRecording` command to stop recording once the operations are complete.

8. Find the recording file and proceed with the follow-up troubleshooting. By default, the storage path is under: `% USE RPROFILE %\Videos\SessionRecordings`, this can be customized by Configurating the basic deployment agent settings.

> **Note:**

> The recording will automatically stop when the session duration reaches **30 minutes**, or the file size reaches **60 MB**.

> **Example 2:** Administrator-triggered recording

Administrators can trigger recordings for specific active sessions on the machine (for example, to assist a user with troubleshooting).

The administrator can perform the following steps on the machine hosting the session:

1. Launch PowerShell as an administrator.
2. Import the module as described in the previous section.
3. Get the SessionID of the target user session by using query session command. `query session | Select-String "Active"`

```
PS C:\Windows\system32> query session | Select-String "Active"

>console                 ctxuser                   3  Active
```

4. Use the `Get-SessionRecordingStatus -SessionId <SessionID>` command to check the recording status, ensure the session is not already being recorded. The status is supposed to be shown as below:

```
PS C:\Windows\system32> Get-SessionRecordingStatus
Get-SessionRecordingStatus Error: Session is not recorded now.
```

5. Use the `Start-SessionRecording -SessionId <SessionID>` command to start recording the session.
6. Use the `Get-SessionRecordingStatus -SessionId <SessionID>` command to check the recording status, ensure the session is being recorded. The status is supposed to be **Recording**.
7. Instruct the user to reproduce the issue or perform the operations that need to be documented.

8. Use the `Stop-SessionRecording -SessionId <SessionID>` to stop recording once the operations are complete.
9. Find the recording file under the target user profile, such as: `C:\Users\user0\Videos\SessionRecordings` and proceed with the follow-up troubleshooting.

Start or stop recording by using Hotkey

End users can also control recording using shortcut keys (Hotkeys). By default, this feature is disabled.

Enable Hotkeys

To enable hotkey functionality, on the VDA machine:

```
Set-SessionRecordingConfiguration -PerMachine -EnableHotkeys $true
```

This command requires a **local administrator account** to execute.

The setting is applied **per machine** and will take effect for subsequent active sessions.

Default Hotkeys

Once enabled, the default hotkeys are:

- Start recording: CTRL + SHIFT + F8
- Stop recording: CTRL + SHIFT + F9

> **Note:**

> By default, the storage path is under: `%USERPROFILE%\Videos\SessionRecordings`, this can be customized by Configurating the basic deployment agent settings.

> The recording will automatically stop when the session duration reaches **30 minutes**, or the file size reaches **60 MB**.

Customize Hotkeys

If the default hotkeys conflict with other applications, you can customize them using the following command:

`Set-SessionRecordingConfiguration -PerMachine -StartHotKey <hotkey> -StopHotKey <hotkey>`

Hotkey rules:

- Only **F1–F12** or **capital letters (A–Z)** can be used as the last key.
- You only define the **last key** in the combination. The **CTRL + SHIFT** prefix is mandatory and automatically applied.

Example: To set the start hotkey to **CTRL + SHIFT + F1**, you would enter **F1** as the \<hotkey>.

Start or stop recording by using Dynamic Recording

You can also trigger recordings using Dynamic Session Recording policies. For more information, see Dynamic Session Recording.

> **Note:**

> By default, the storage path is under: `%USERPROFILE%\Videos\SessionRecordings`, this can be customized by Configurating the basic deployment agent settings.

> The recording will automatically stop when the session duration reaches **30 minutes**, or the file size reaches **60 MB**.

Configurating the basic deployment agent settings

You can customize the settings for the basic deployment agent using PowerShell commands. These settings are applied at the machine or user level.

Prerequisites

Before configuring the settings, you must import the necessary module into the PowerShell session.

1. Open PowerShell and navigate to the agent installation folder: `<SessionRecordingAgent installation path>\Bin` folder.

   For example: `cd "C:\Program Files\Citrix\SessionRecording\Agent\Bin\"`
2. Import the module by running:

```
import-module -DisableNameChecking.\EndUserInitiatedSRSnapin.dll
```



PowerShell configuration commands

The following table lists the PowerShell commands for managing session recording configuration:

COMMAND	DESCRIPTION
Set-SessionRecordingConfiguration	Sets session recording configuration values at the machine or user level. For more information, run `Get-Help SetSessionRecordingConfiguration`
Get-SessionRecordingConfiguration	Gets the effective session recording configuration or queries raw values from specific registry scopes (Machine, User, or Session). For more information, run `Get-Help GetSessionRecordingConfiguration`
Clear-SessionRecordingConfiguration	Clears session recording configuration values at the machine or user level, reverting them to machine-level or default values. For more information, run `Get-Help ClearSessionRecordingConfiguration`.

Configuration settings

The settings available for the basic deployment mode are listed as follows. You can use the `Set-SessionRecordingConfiguration` cmdlet to configure them.

Add the `-PerMachine` switch parameter to apply the configuration at the machine. This requires administrator privileges. If specified, the settings apply to the machine level. If omitted, settings apply to the **user level**.

PROPERTY	TYPE	SETTING	SCOPE	DEFAULT	NOTE
-AllowUserTrigger	Boolean	Allow endusertrigg	Machine	True	Controls whether users can

PROPERTY	TYPE	SETTING	SCOPE	DEFAULT	NOTE
		ered recording			manually start/stop recordings
-StoragePath	String	Recording storage path	Machine, User, Session	%USERPROFILE%\Videos\Session Recordings	The directory where recording files are saved. This directory can be located on a local drive, a UNC network path, or a mounted drive.
-MaximumDurationInMinutes	Int	Maximum recording duration	Machine, User, Session	30	The session automatically stops recording after this duration (in minutes).
-MaximumSizeInMegabytes	Int	Maximum file size	Machine, User, Session	60	The session automatically stops recording after reaching this size (in MB).
-EnablePreRecording	Boolean	Enable prerecording	Machine	False	Enable pre-recording before

PROPERTY	TYPE	SETTING	SCOPE	DEFAULT	NOTE
					recording trigger.
-EnablePreRecording	Boolean	Enable prerecording	Machine	False	Enable pre-recording before recording trigger.
-PreRecordingDurationInSeconds	Int	Prerecording duration	Machine	30	The duration of the pre-recording buffer in seconds.
-EnableHotkeys	Boolean	Enable hotkeys	Machine	False	Enables hotkeys for start/stop recording
-StartHotkey	String	Start recording hotkey	Machine	F8	Default maps to CTRL + SHIFT + F8.
-StopHotkey	String	Stop recording hotkey	Machine	F9	Default maps to CTRL + SHIFT + F9.
-ScreenId	Int	The screen ID to record	Machine, User, Session	0	Use 0 for all screens.

Note:

If you customize these settings at multiple levels, the priority order is: Session > User > Machine.

Example Configuration

These examples illustrate how different users set configurations and how the agent determines the final, effective setting.

Example 1: Administrator Disabling User-Triggered Recording

A local administrator (e.g. LocalAdmin) can set a machine-wide policy to disable the ability for all standard users to start recordings manually.

```
Set-SessionRecordingConfiguration -PerMachine -AllowUserTrigger $false
```

Explanation: This command requires administrative privileges (`-PerMachine`) and prevents any user on this VDA from using `Start-SessionRecording`, regardless of their user-level settings.

Example 2: Administrator Setting Machine-Wide Defaults

The LocalAdmin sets the default storage location, maximum duration, and maximum size for all users on the VDA.

```
Set-SessionRecordingConfiguration -PerMachine -StoragePath "D:\SessionRecordings"-MaximumDurationInMinutes 120 - MaximumSizeInMegabytes 500
```

Explanation: This sets the configuration at the Machine level. For a standard user (e.g. User0), recordings will now default to D:\SessionRecordings and stop after 120 minutes or 500 MB, whichever comes first.

Example 3: Standard User Overriding Machine Defaults

The standard user (User0) prefers to save their files locally to the C: drive, overriding the administrator's Machine-level setting.

```
Set-SessionRecordingConfiguration -StoragePath "C:\Users\User0\SessionRecordings" -MaximumDurationInMinutes 60
```

Explanation: Since this command is run **without** the `-PerMachine` switch, it applies at the **User level**. Because User-level settings have a higher priority than Machine-level settings, User0's recordings will now be saved to C:\Users\User0\ SessionRecordings and stop after 60 minutes.

Example 4: Session-Specific Override

During a specific recording, User0 needs to temporarily save the file to a network share (\\ \fileshare\temp) and limit the duration to 15 minutes, overriding both User and Machine settings.

```
Start-SessionRecording -StoragePath "\\fileshare\temp" -
MaximumDurationInMinutes 15
```

Explanation: Parameters passed directly to `Start-SessionRecording` to create a **session-level override**, which has the absolute highest priority and is only valid for that single recording instance. The next recording session will revert to the User or Machine configuration.

Checking Configuration

Use the `Get-SessionRecordingConfiguration` commandlet to view the currently configured values and the final effective setting:

```
Get-SessionRecordingConfiguration
```

Explanation: This command shows the result of applying the hierarchy (Session > User > Machine), providing the settings currently in use for the user running the command.

Clearing Configuration

Use the `Clear-SessionRecordingConfiguration` commandlet to remove custom settings, allowing the agent to fall back to the next-highest priority configuration.

- Clear specific user settings:

  If User0 wants to stop saving files to C:\Users\User0\SessionRecordings and revert custom settings to the default setting, they would run:

  ```
  Clear-SessionRecordingConfiguration -StoragePath - MaximumDurationInMinutes
  ```

Explanation: This clears the `StoragePath` and `MaximumDurationInMinutes` values from the User scope.

- Clear all machine-level configurations (Requires Administrator Privileges):

  ```
  Clear-SessionRecordingConfiguration -PerMachine -ClearAll
  ```

Explanation: This command requires administrative privileges (`-PerMachine`) and clears all custom configurations set at the Machine level.

Switch the agent deployment type

The Session Recording agent supports two distinct deployment modes:

- **Basic deployment mode:** This provides a lightweight method to record active sessions locally as MP4 files without deploying backend components. This mode is active when the Session Recording Server address is set to **localhost**.
- **Standard deployment mode:** This is the traditional, centrally managed deployment where the agent connects to a Session Recording Server. This mode offers high scalability and advanced features. This mode is active when the Session Recording Server address is set to the **Fully Qualified Domain Name (FQDN)** of the server.

The operational mode is determined by the **Session Recording Server** value configured in the Session Recording Agent Properties or the Windows registry.

Method 1: Using the Session Recording Agent Properties

You can switch modes manually on a specific VDA.

1. Log on to the VDA where the Session Recording agent is installed.
2. From the **Start** menu, choose **Session Recording Agent Properties**.
3. Click the **Connections** tab.
4. Modify the value in the **Session Recording Server** field:
    a. **Basic deployment mode**: Enter localhost.
    b. **Standard deployment mode**: Enter the **FQDN** of your Session Recording Server.
5. Click **OK** to save the changes.

Method 2: Using the Windows Registry or Group Policy

For large-scale deployments, you can configure the setting directly in the Windows Registry, typically deployed via Group Policy Object (GPO).

- **Registry Key**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent\`
- **Value Name**: `SmAudServerName`
- **Value Data**:
    - **For basic deployment mode:** Set the value to localhost.
    - **For standard deployment mode:** Set the value to the **FQDN** of your Session Recording Server.

> **Note:**

> Key considerations for mode switching
>
> - The Session Recording agent reads the configuration value only at the **start of a session**. Any change to the deployment mode will take effect **on the next new session** launched on the VDA.
> - It is strongly recommended that you **do not switch modes** while there are active or in-progress recording sessions. Wait for all active recordings to stop to prevent data consistency issues.

Manage recording files

Session Recording provides a local tool, SRAgentTool.exe, to help you manage recording files. The tool offers the following capabilities:

- Recover corrupted MP4 recordings: Repairs MP4 files that are unplayable due to abnormal situations, such as an unexpected graphics process crash.
- Verify MP4 recording integrity: Checks whether a recording file has been tampered with to ensure its authenticity.

You can access the tool in the following directory: <`Session RecordingAgent installation path>\Bin`.

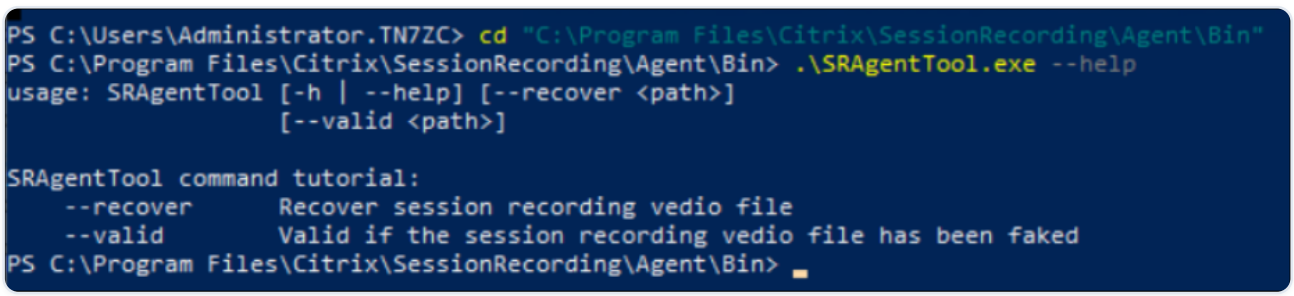
View usage instructions

To view the help information and usage instructions for the tool, run the following command in PowerShell or Command Prompt:

```
.\SRAgentTool.exe --help
```

Or

```
.\SRAgentTool.exe -h
```



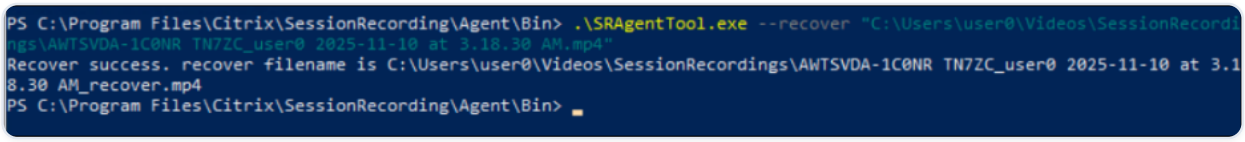
Recover corrupted recordings

If a recording file cannot be played, use the recovery command to attempt a repair. **Command:**

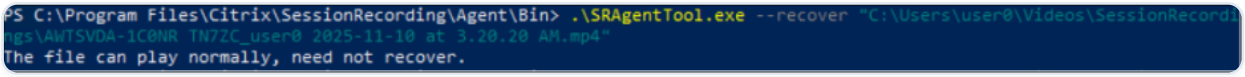
```
.\SRAgentTool.exe --recover <path_to_mp4>
```

Output:

- **Success**: The tool displays **Recover success** and shows the path of the newly recovered file (typically suffixed with _recover.mp4).



- **No recovery needed**: If the file is already playable, the tool displays **The file can play normally**, need not recover.



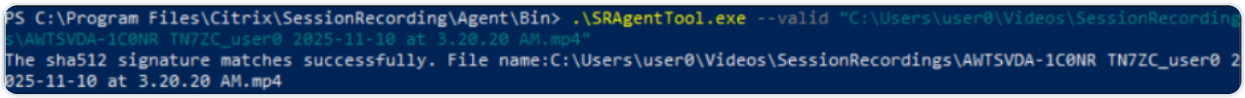
Verify recording integrity

To verify that a recording file has not been modified, use the validation command to check its SHA512 signature.

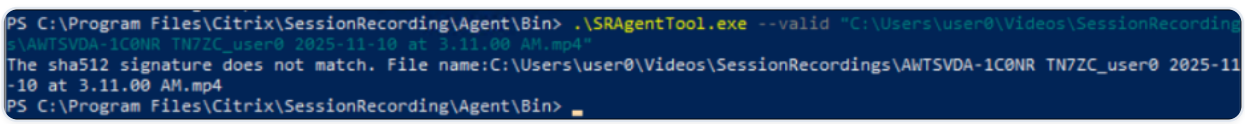
Command: `.\SRAgentTool.exe --valid <path_to_mp4>`

Output:

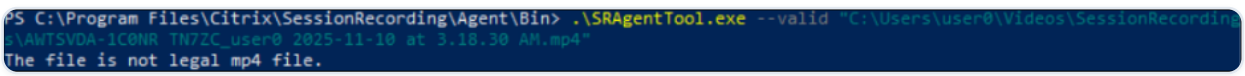
- Valid: The sha512 signature matches successfully.



- Tampered: The sha512 signature does not match.



- Invalid File: The file is not legal mp4 file.



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.

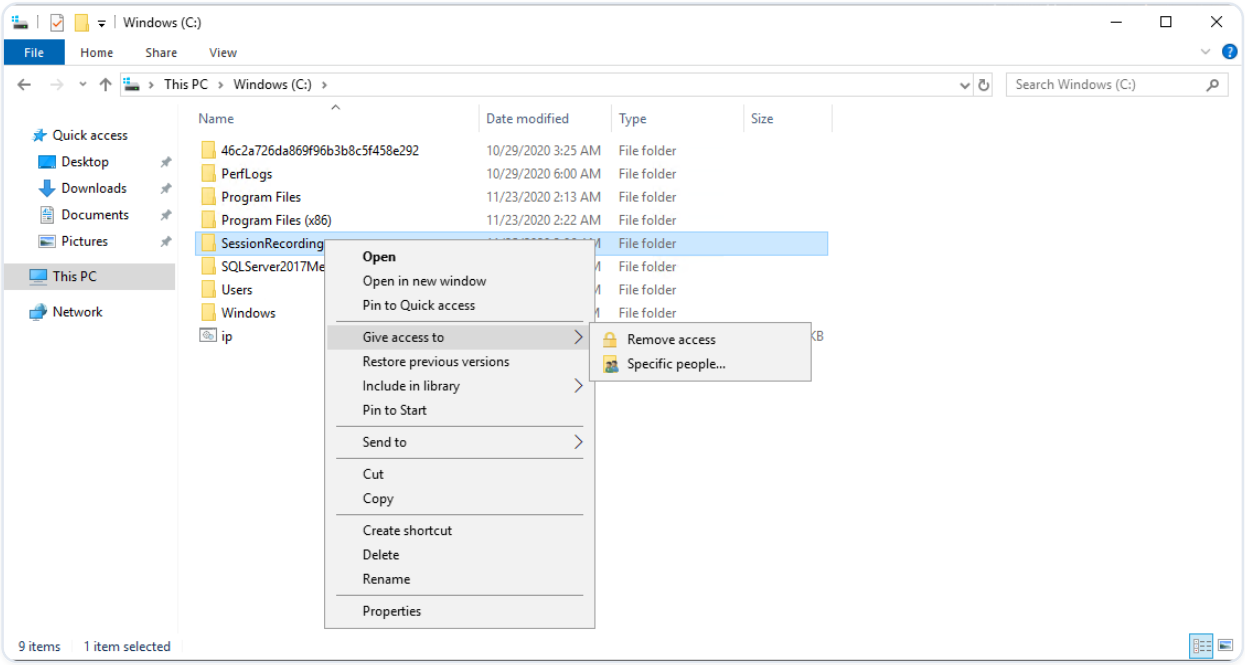
- Citrix ADC

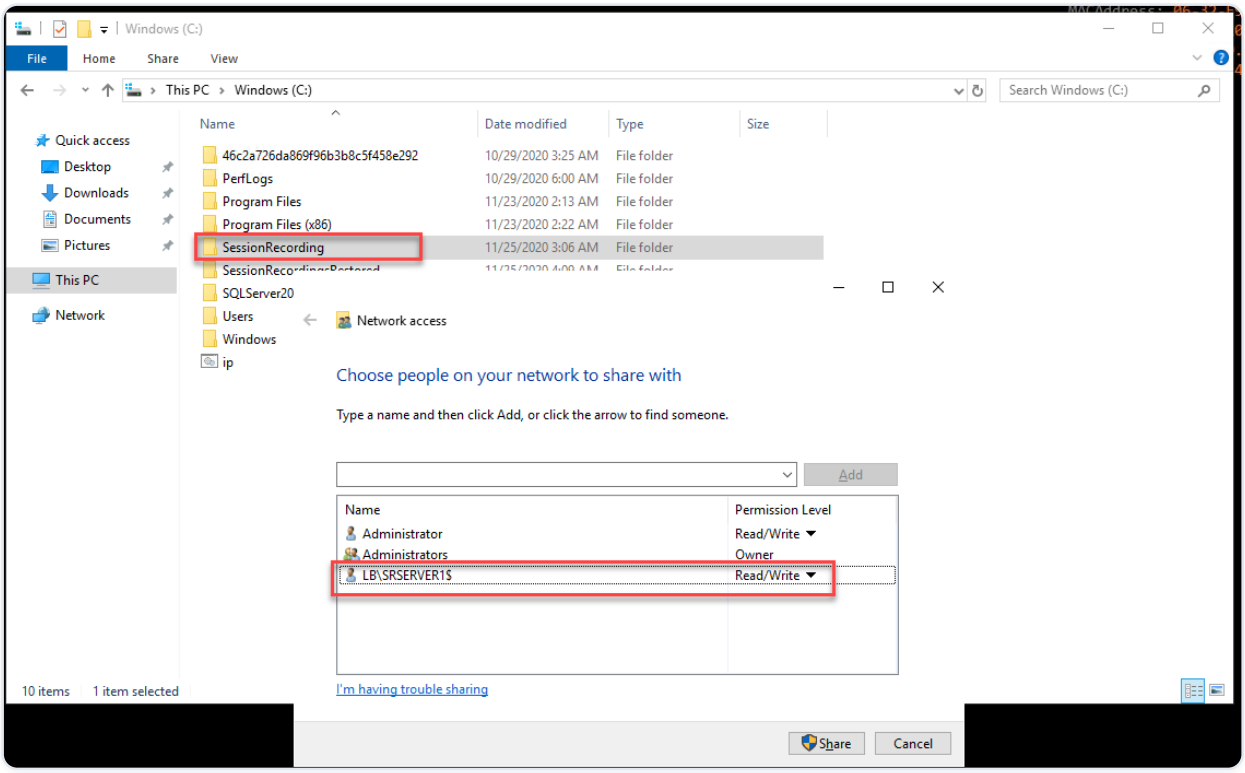
HOST NAME	SERVER ROLE	MANAGEMENT IP ADDRESS (NSIP)	SUBNET IP ADDRESS (SNIP)
Netscaler	Citrix ADC VPX instance	10.63.32.40	10.63.32.109

For more information, see (../../../citrix-adc/2607 LTSR/deploying-vpx.md).

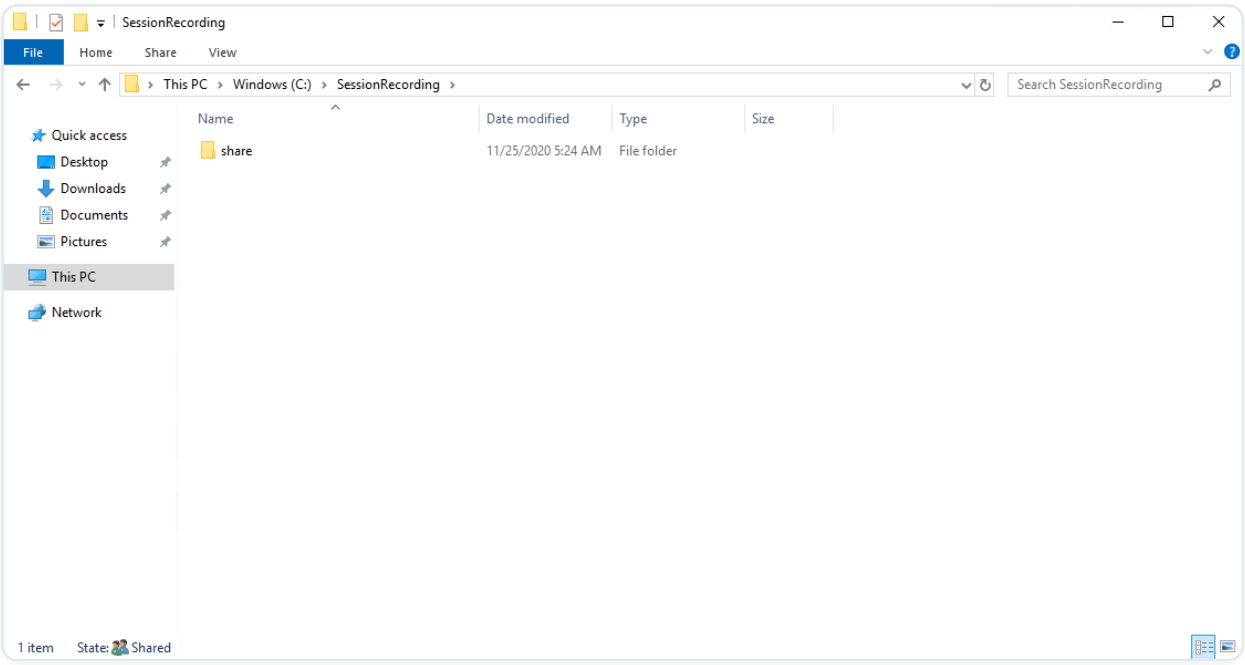
Step 1: Create shared folders on the file server

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`.



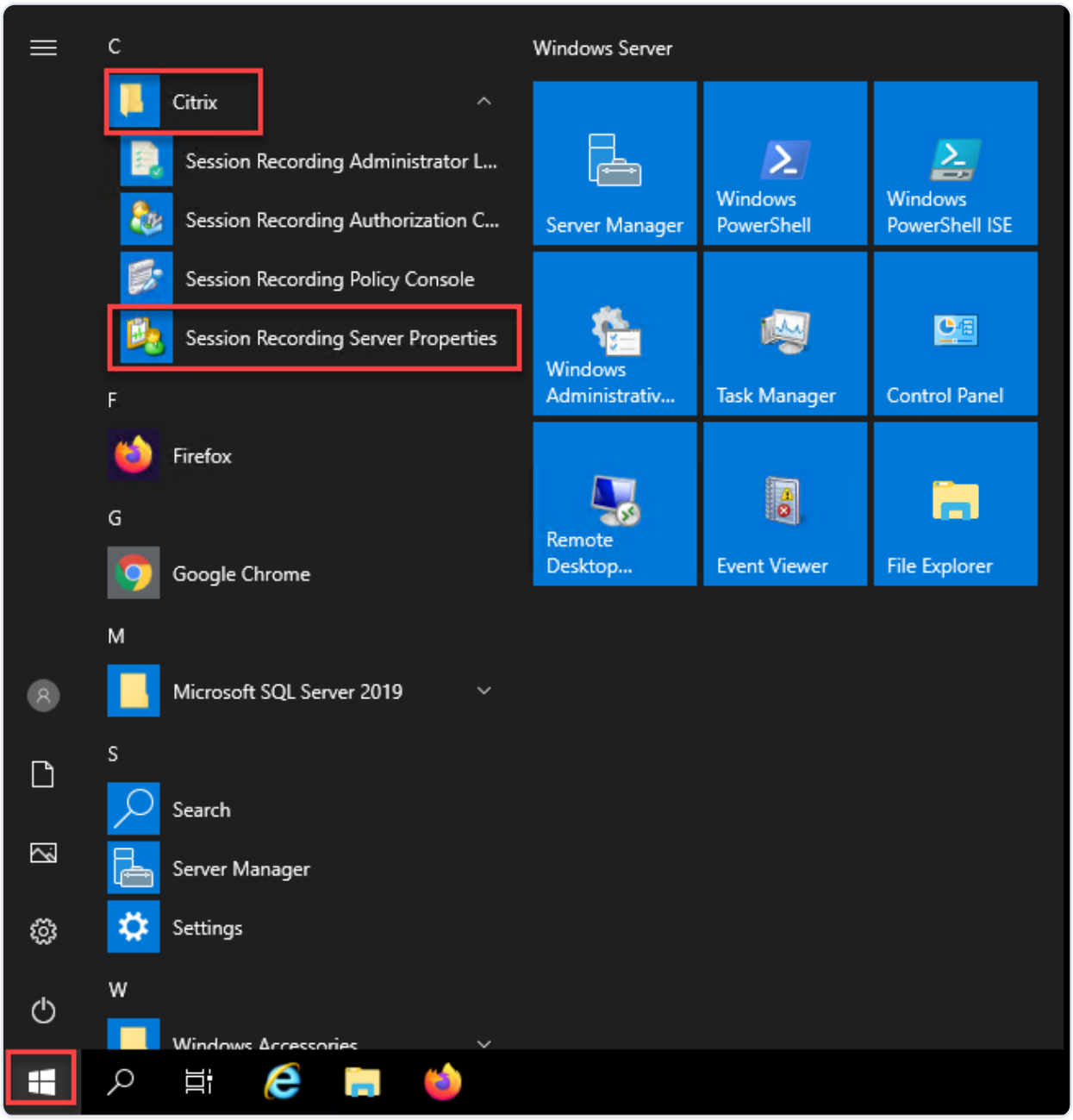
4. Create another folder to restore archived recordings and name the folder `SessionRecordingsRestored`, for example, `C:\ SessionRecordingsRestored`. Share the Read/Write permission of the folder with a Session Recording server. Using `SRServer1` as an example, type `LB\SRSERVER1$`. The dollar sign `$` 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.

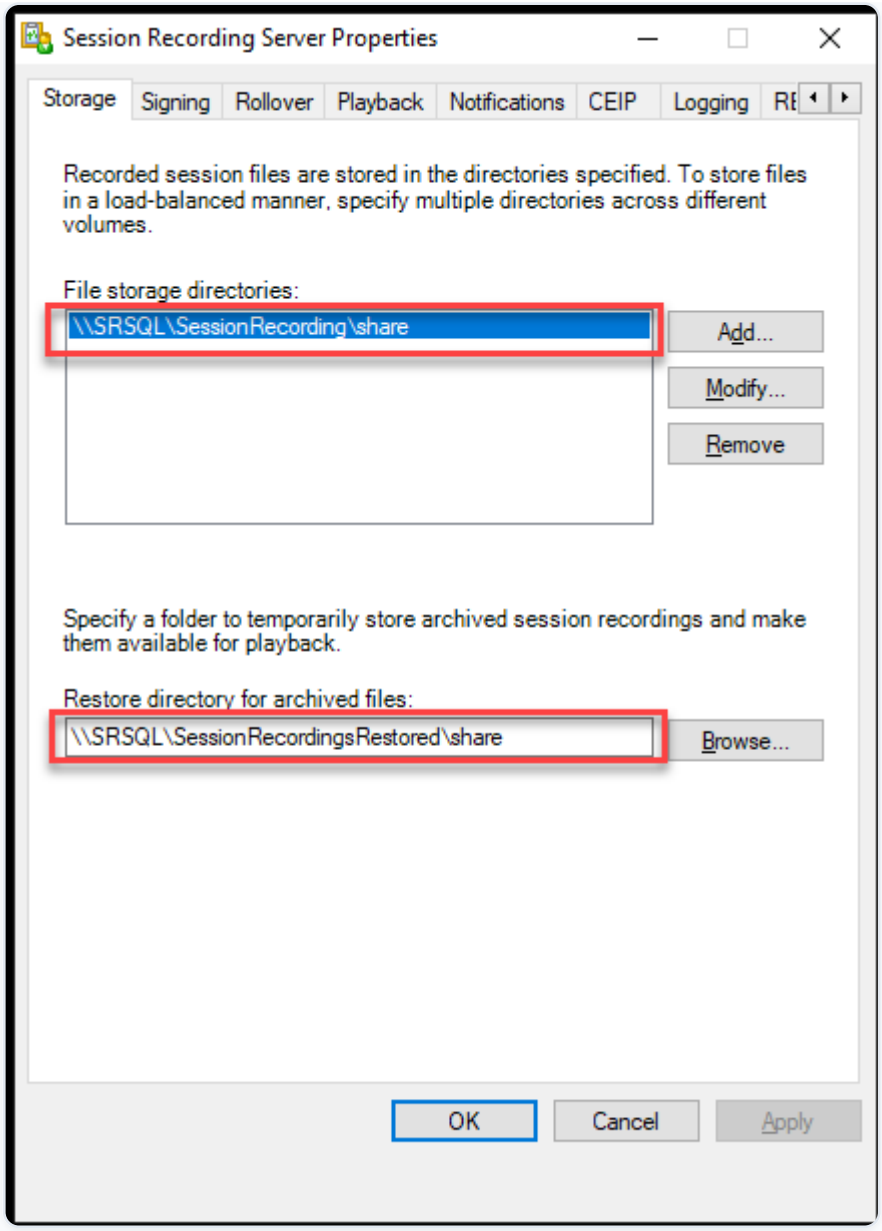
1. Log on to a Session Recording server by using a domain administrator account.
2. Open **Session Recording Server Properties**.



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.

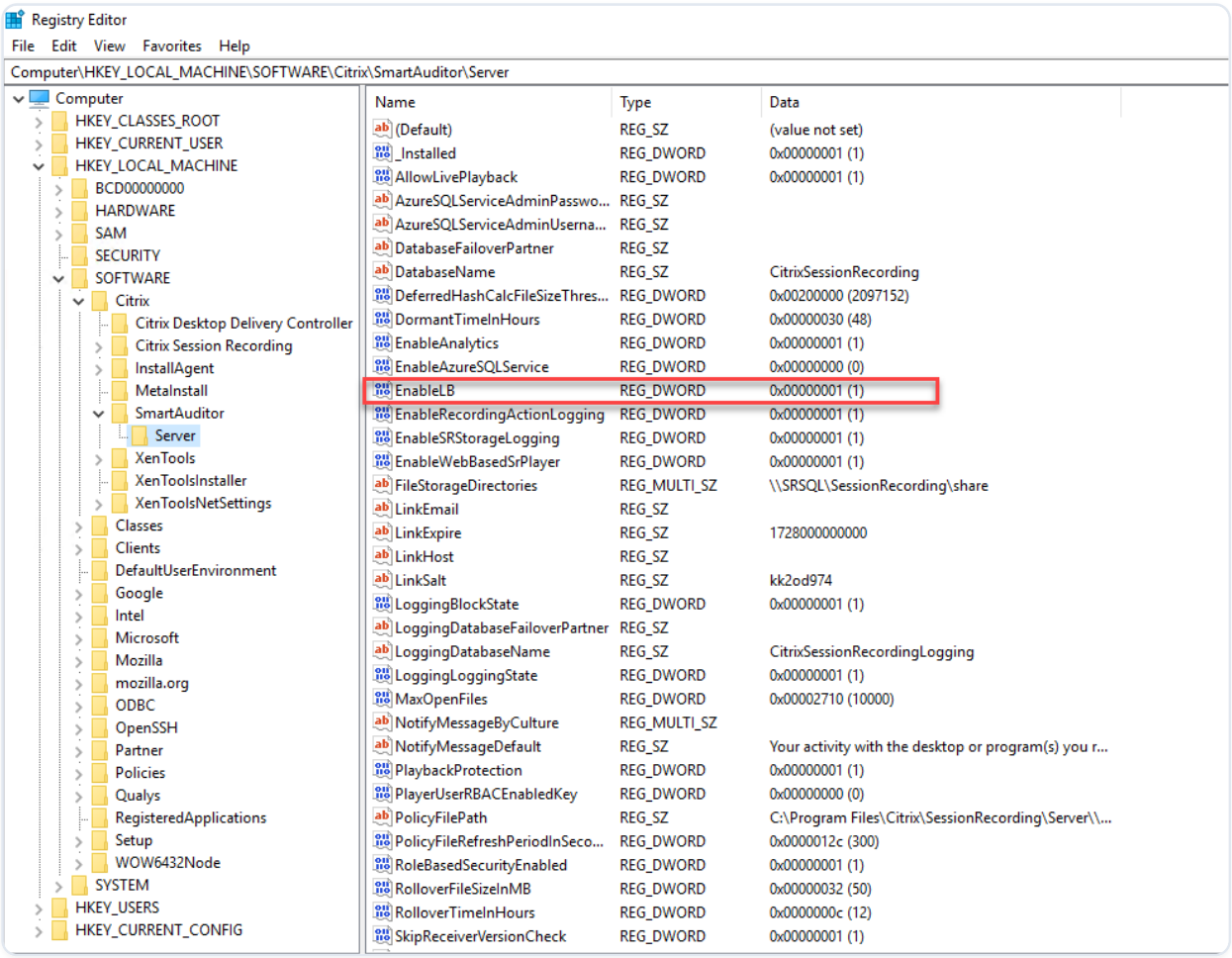
Note:

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.

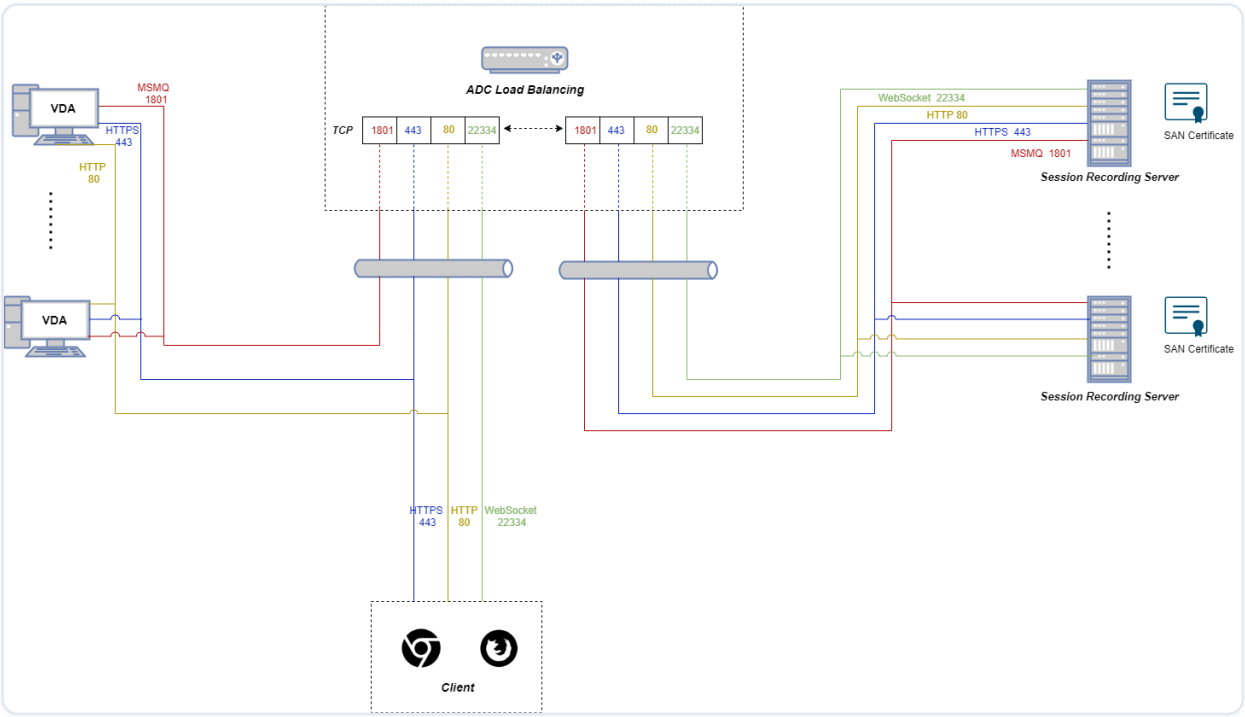
Step 3: Configure load balancing in Citrix ADC

There are two ways to configure load balancing in Citrix ADC - TCP passthrough and SSL offloading.

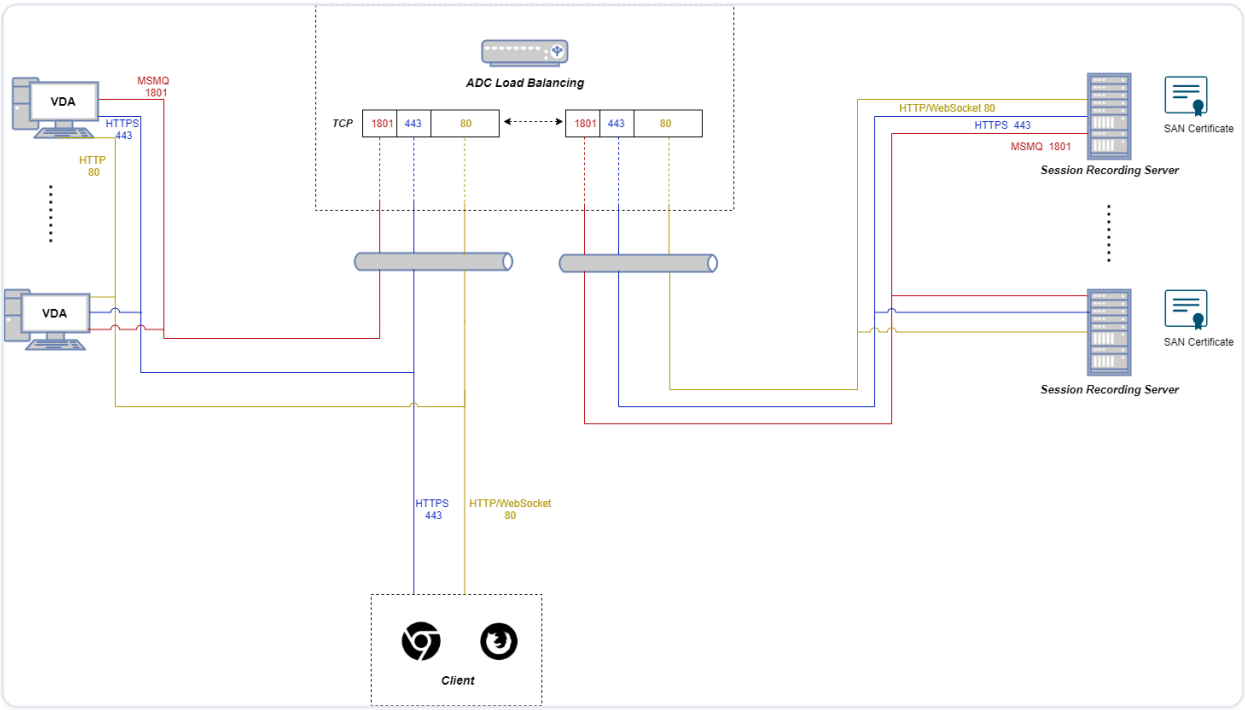
Configure load balancing through TCP passthrough

The following topologies show how to configure load balancing through **TCP passthrough**.

- If you are using the Python-based WebSocket server (Version 1.0):

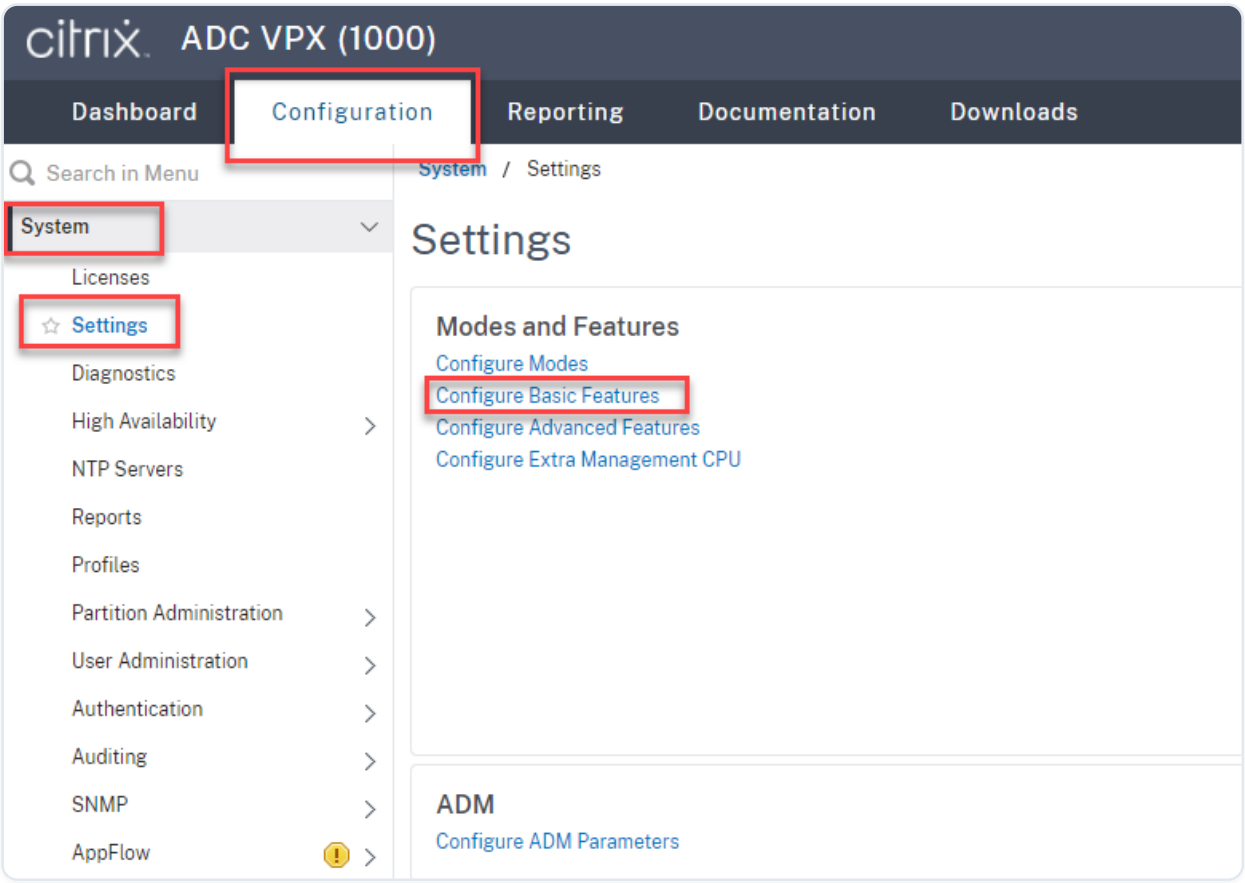


- If you are using the WebSocket server hosted in IIS (Version 2.0):

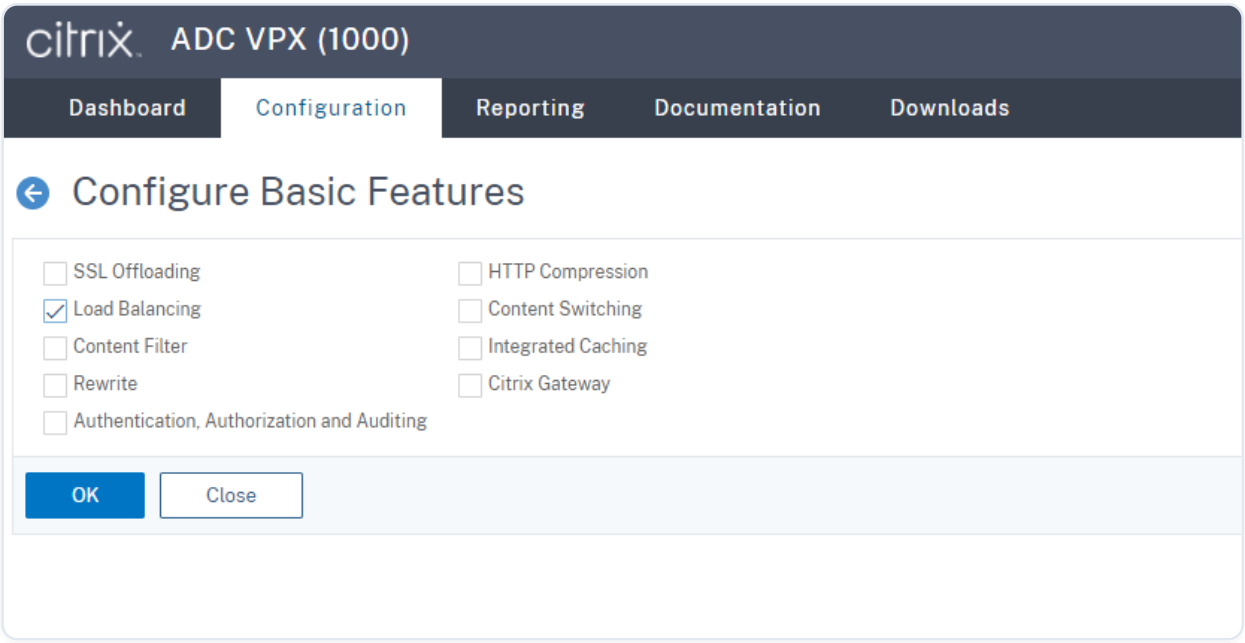


To configure load balancing through TCP passthrough, complete the following steps:

1. Log on to your Citrix ADC VPX instance.
2. Navigate to **Configuration > System > Settings > Configure Basic Features**.

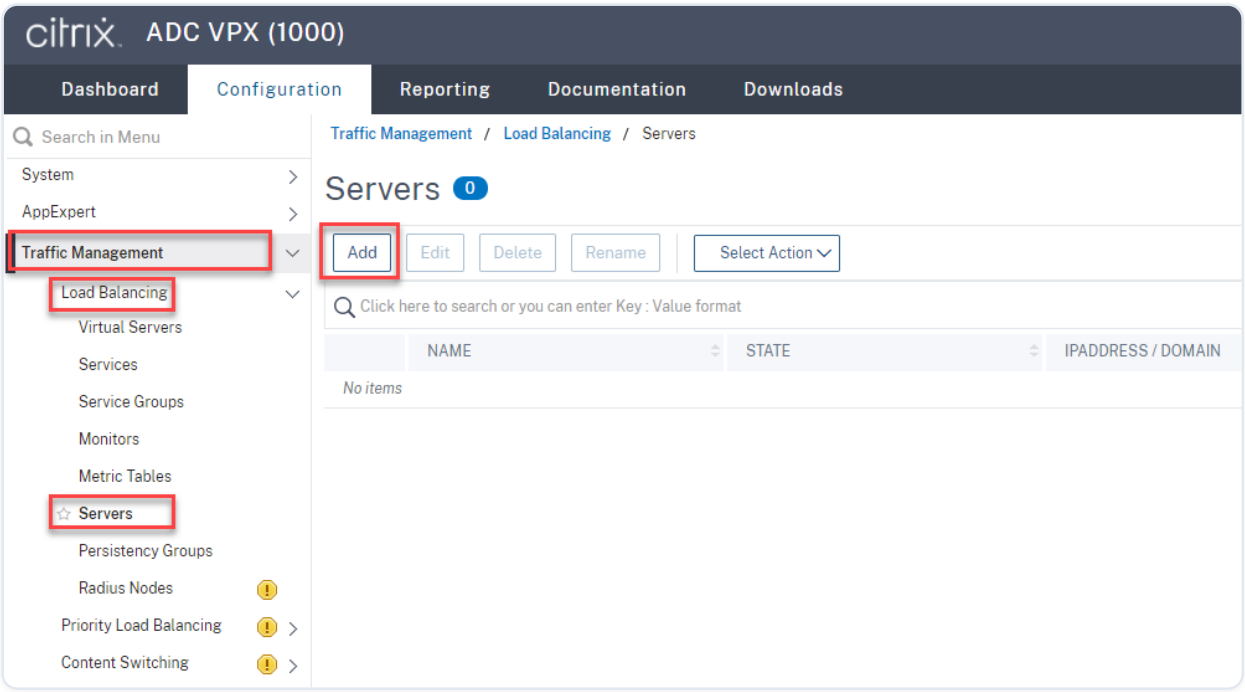


3. Select **Load Balancing** and click **OK**.

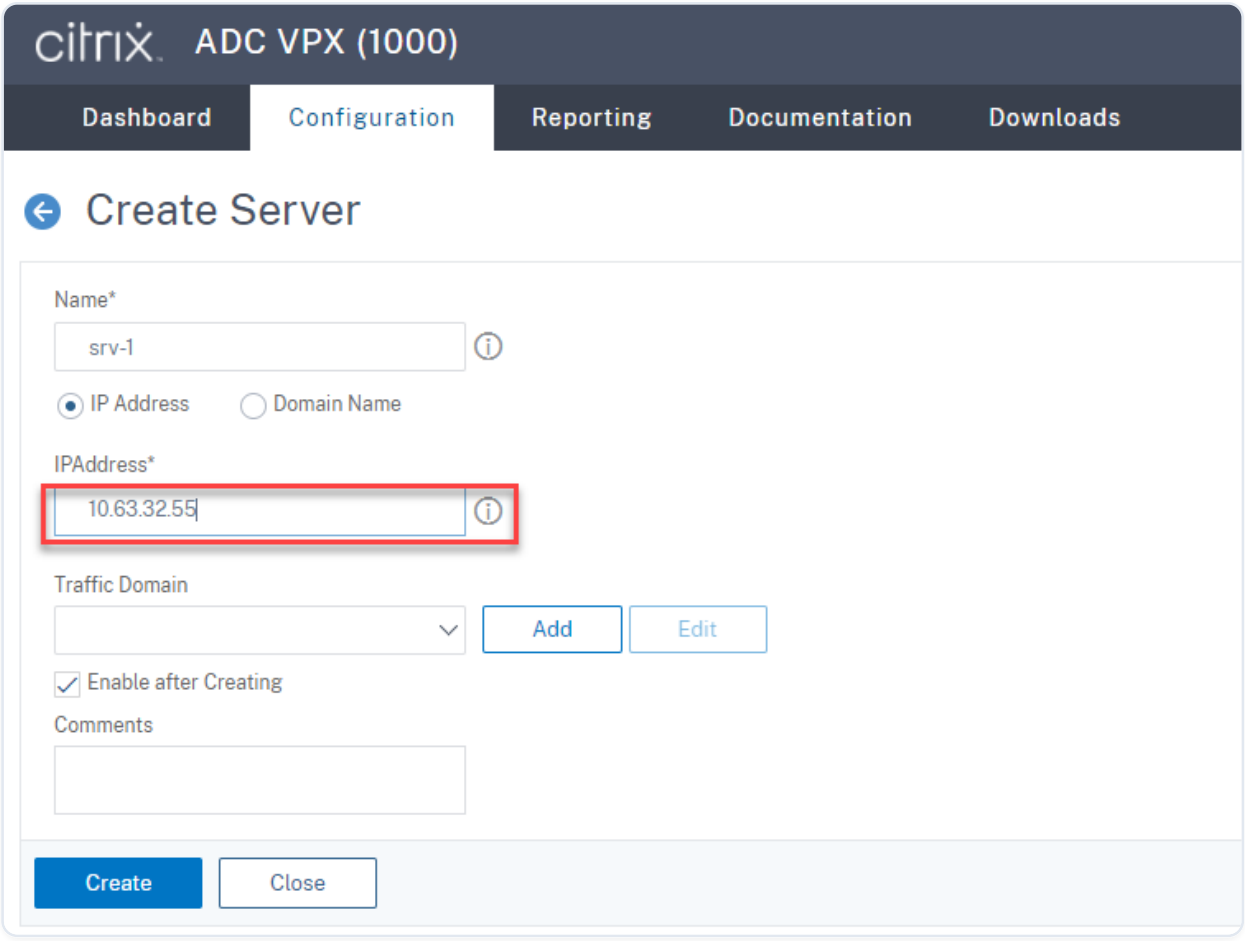


4. Add load balancing servers.

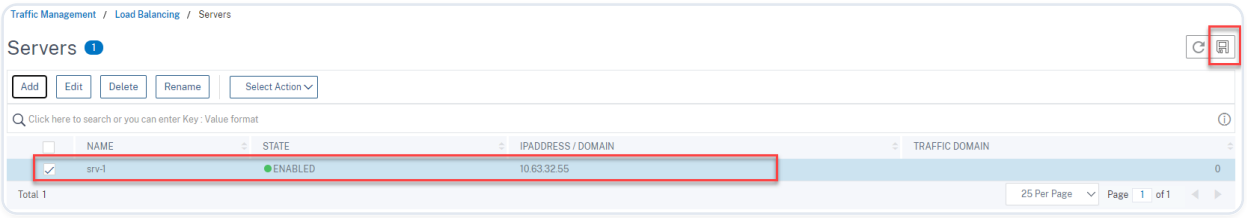
   Navigate to **Traffic Management > Load Balancing > Servers** and click **Add**.



Type the name and IP address of a Session Recording server and then click **Create**. For example:

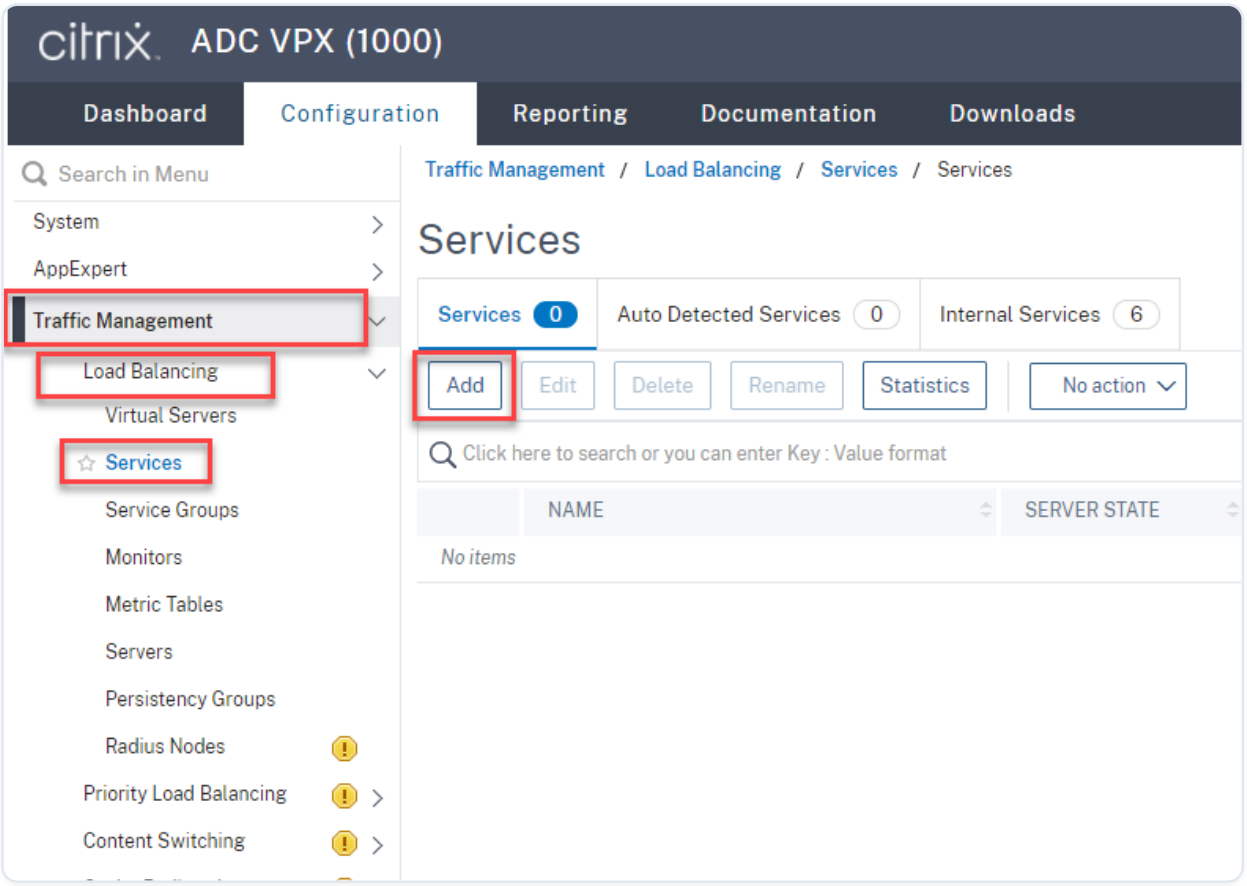


Click the save icon in the upper right corner to save your changes.

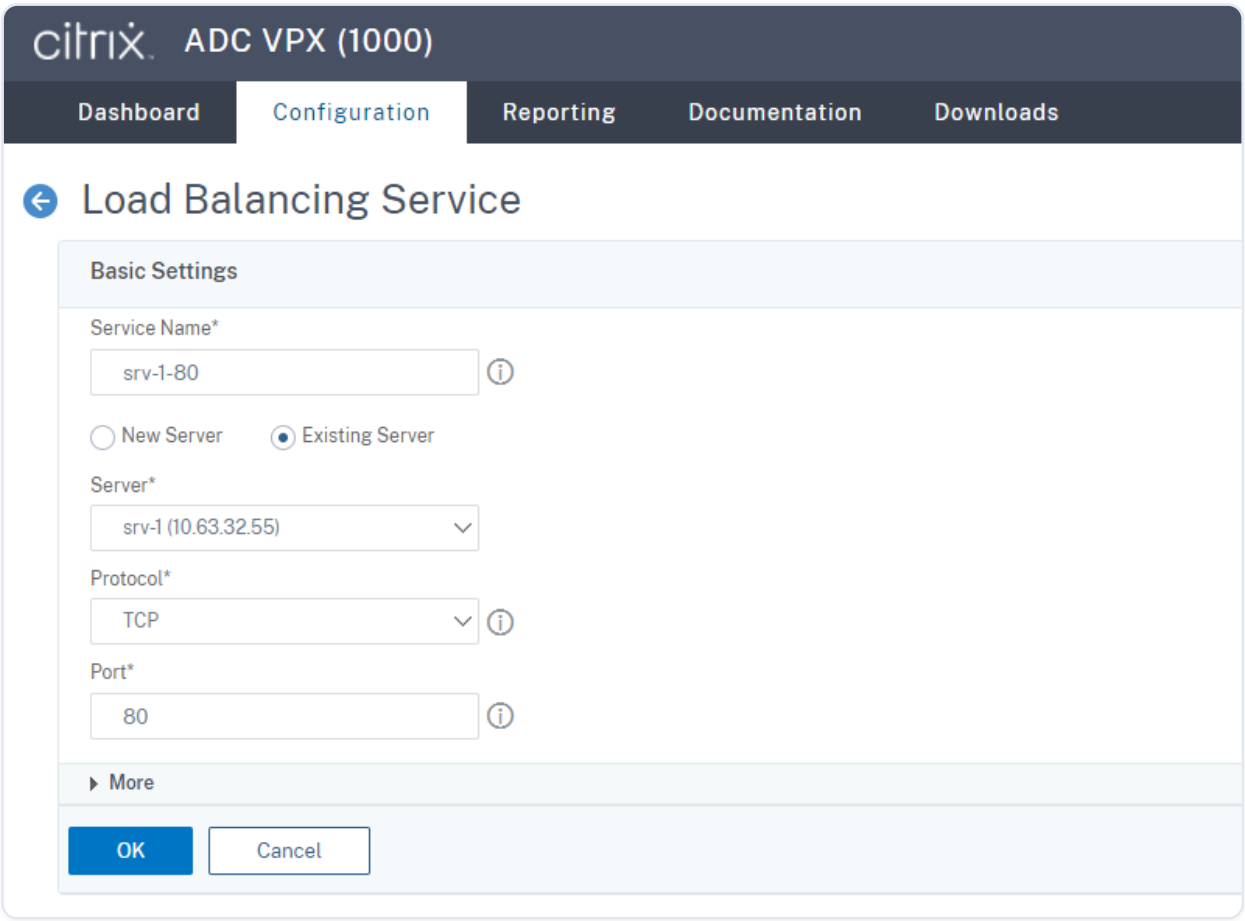


5. For WebSocket server Version 1.0, add **load balancing services** of ports 80, 1801, 22334, and 443 for each Session Recording server. For WebSocket server Version 2.0, add **load balancing services** of ports 80, 1801, and 443 for each Session Recording server.

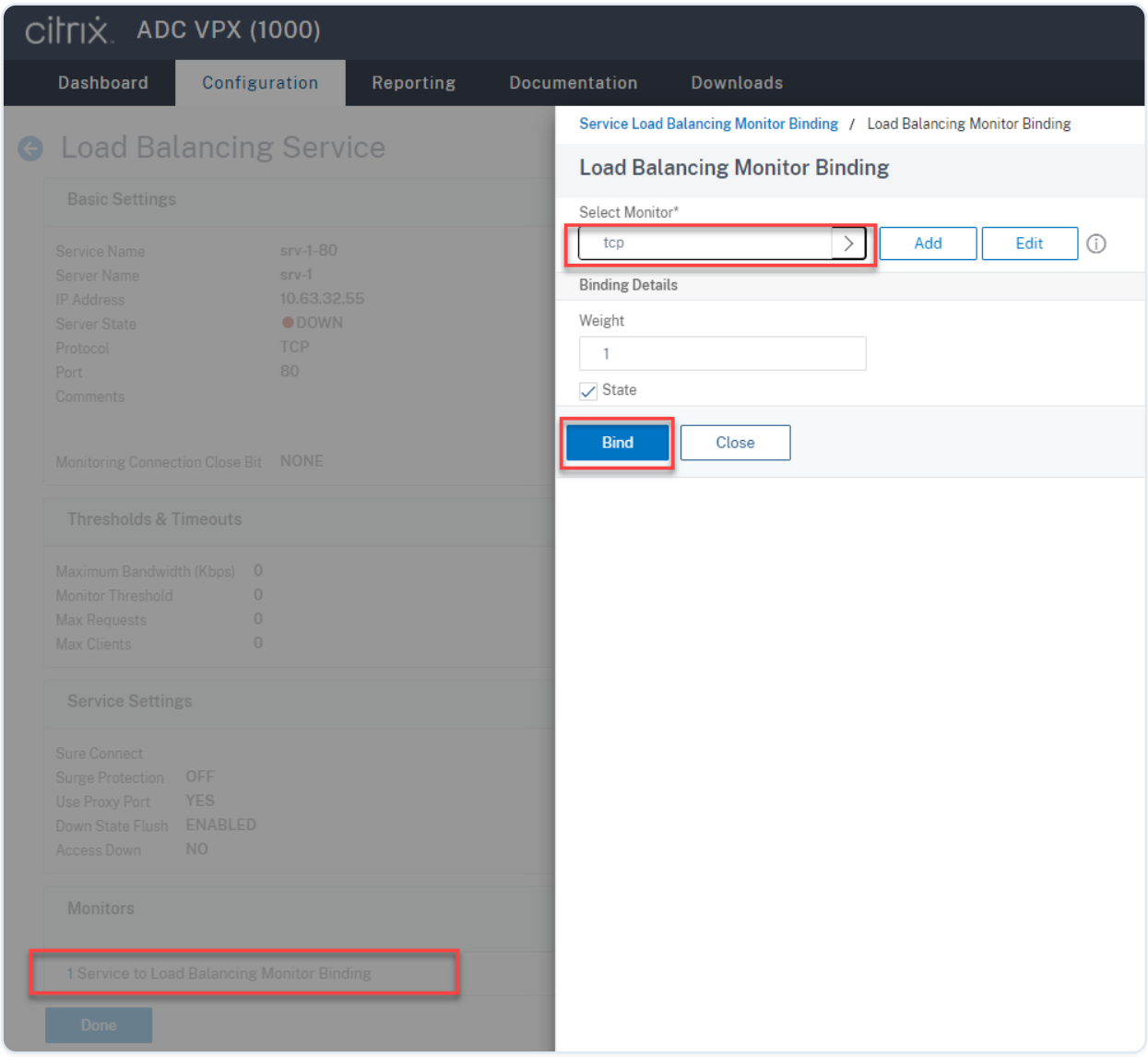
   Navigate to **Traffic Management > Load Balancing > Services** and click **Add**.



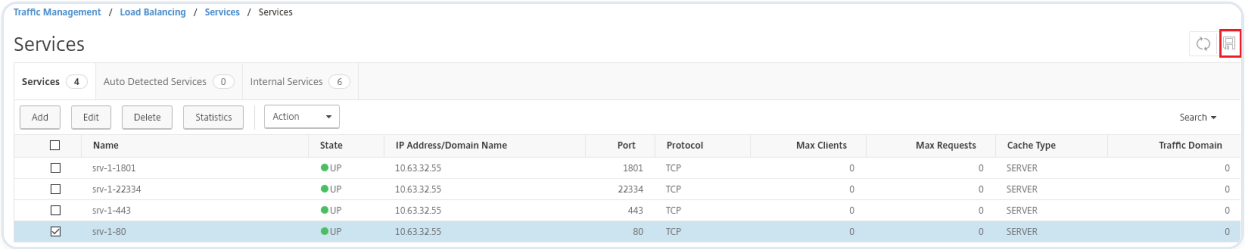
   Type a name for each **load balancing service** that you add. Choose **Existing Server**, select the IP address of your target Session Recording server, select **TCP** as the server protocol, and type a port number. Click **OK**.



Bind the TCP protocol monitor to each load balancing service.



Click the save icon in the upper right corner to save your changes.

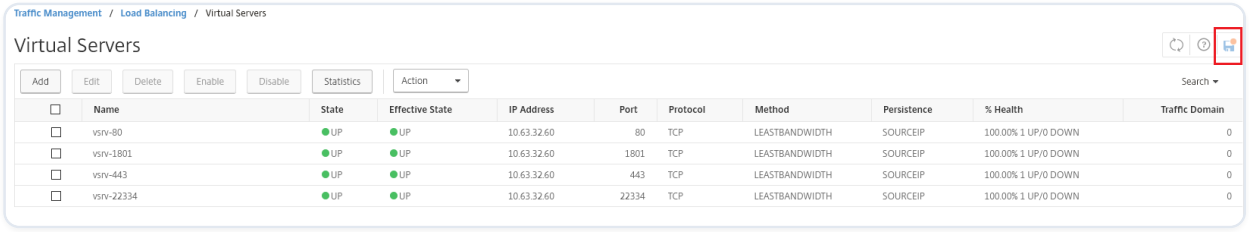


Tip:

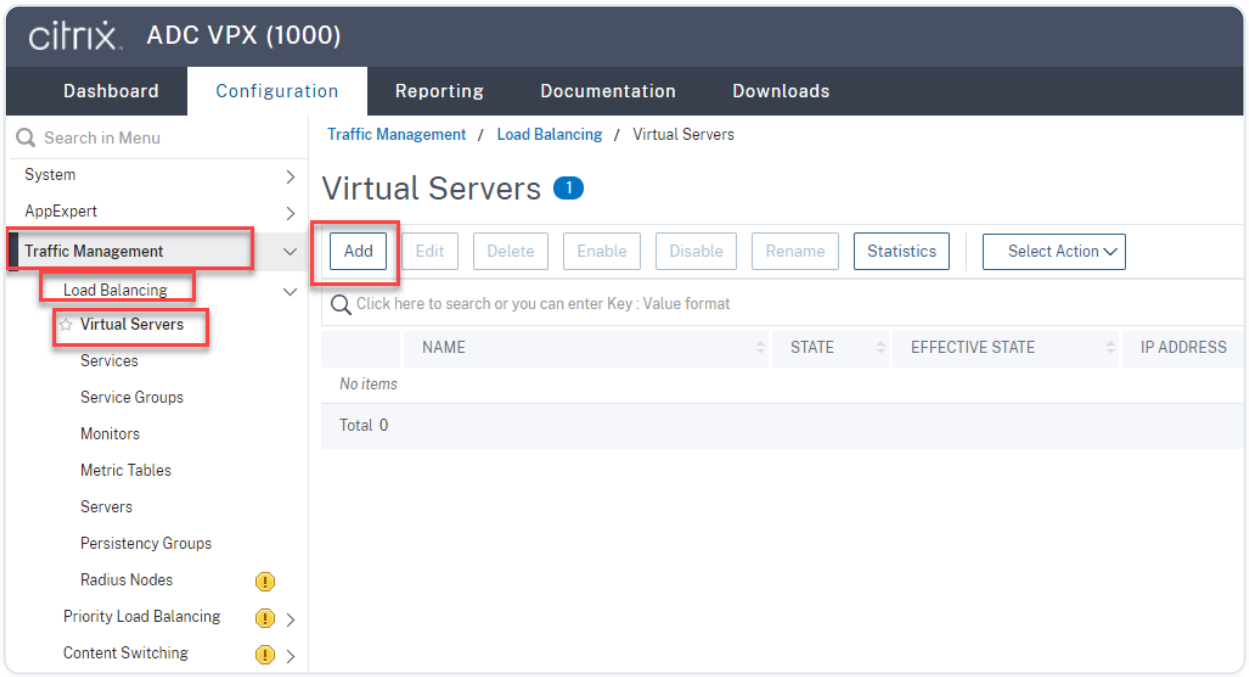
The **load balancing service** of port 22334 is required only for WebSocket server Version 1.0.

6. Add **load balancing virtual servers**.

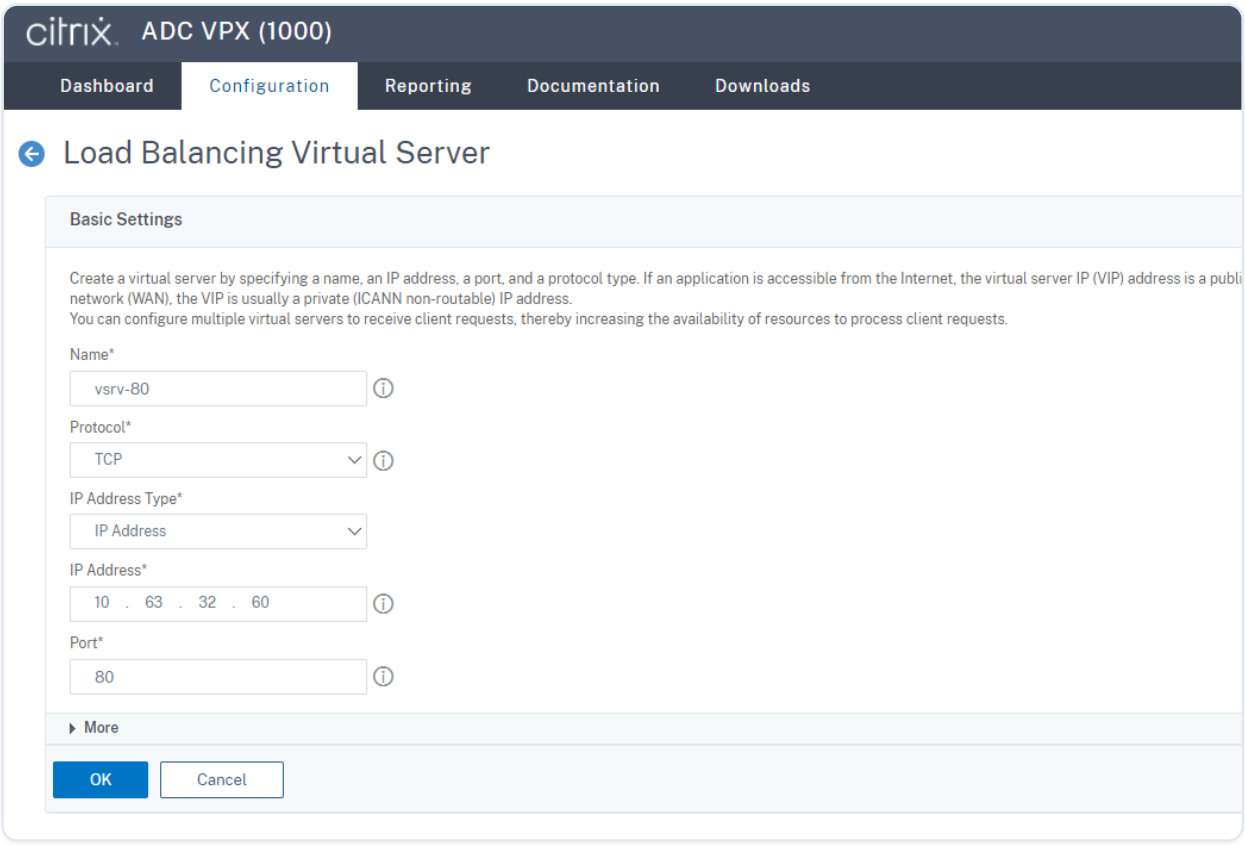
For WebSocket server Version 1.0, complete the following steps to add **load balancing virtual servers** of ports 80, 443, 1801, and 22334. For WebSocket server Version 2.0, add **load balancing virtual servers** of ports 80, 443, and 1801. For example:



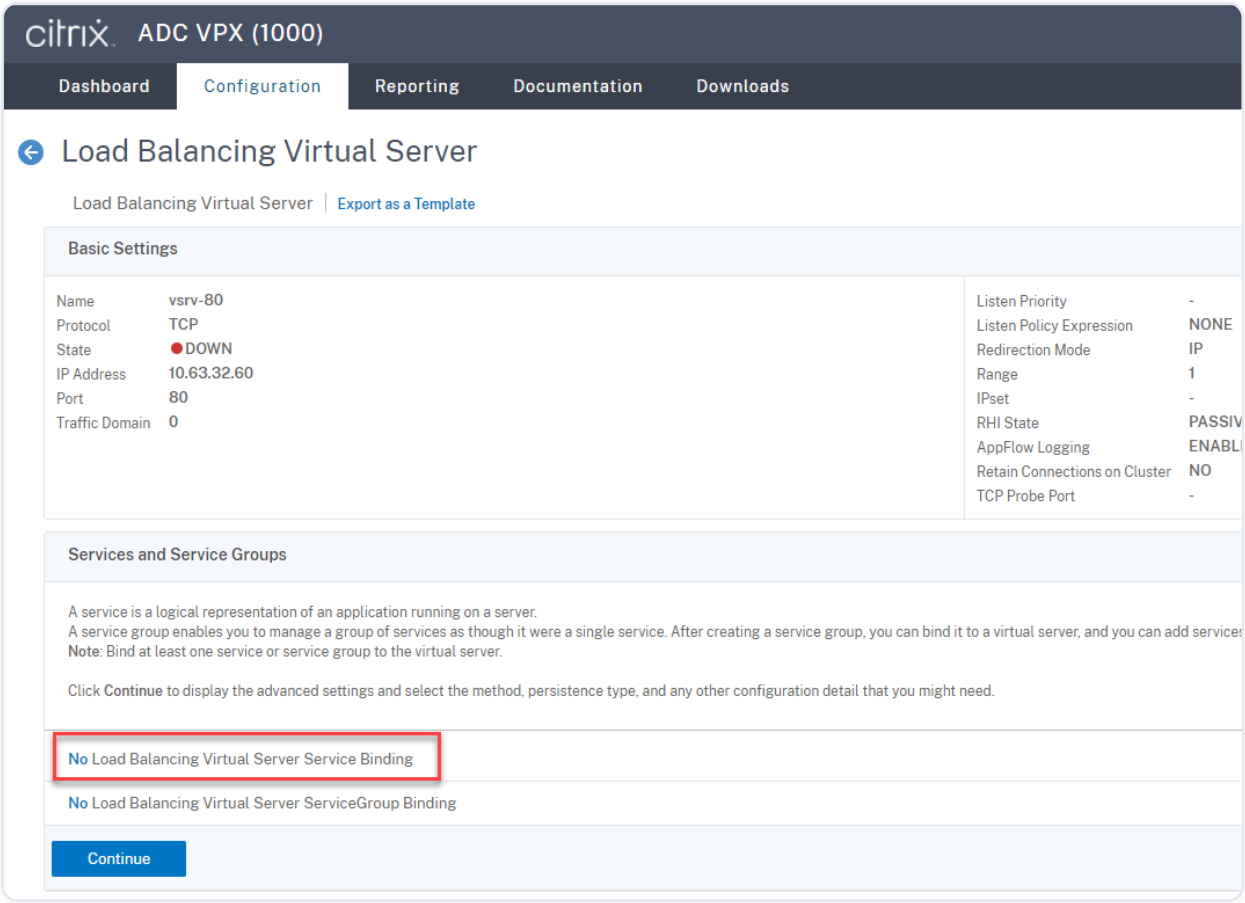
Navigate to **Traffic Management > Load Balancing > Virtual Servers** and click **Add**.

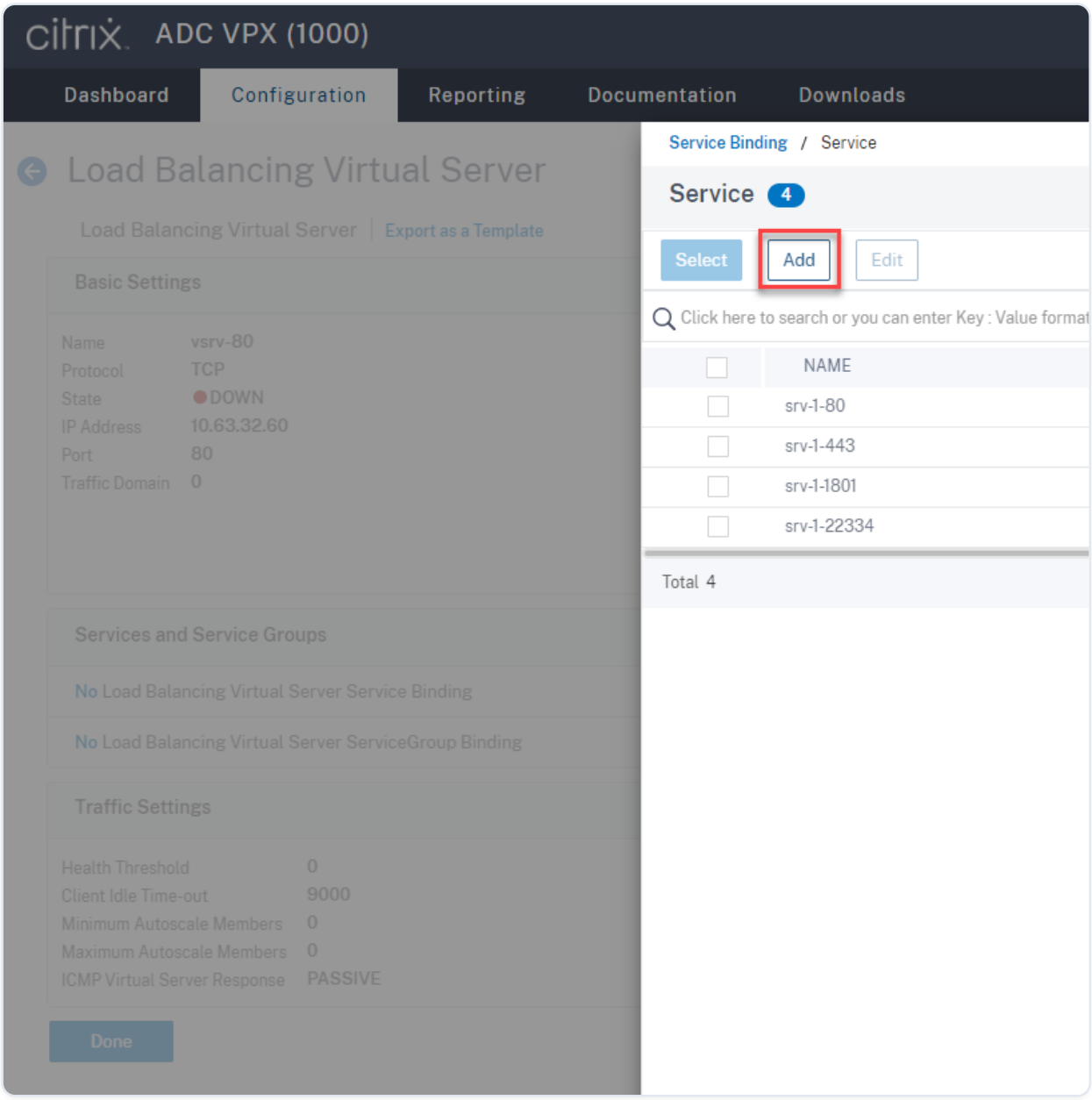


Add each virtual server with the Citrix ADC VIP address based on the TCP protocol.

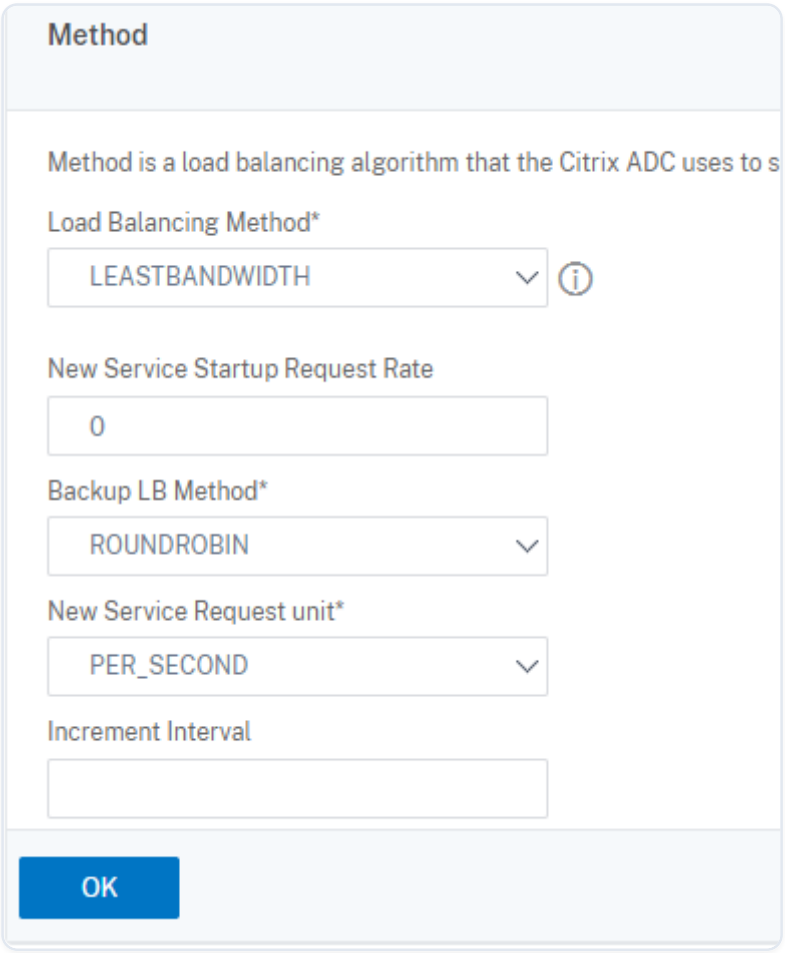


Bind each virtual server to the **load balancing service** of the same port. For example:

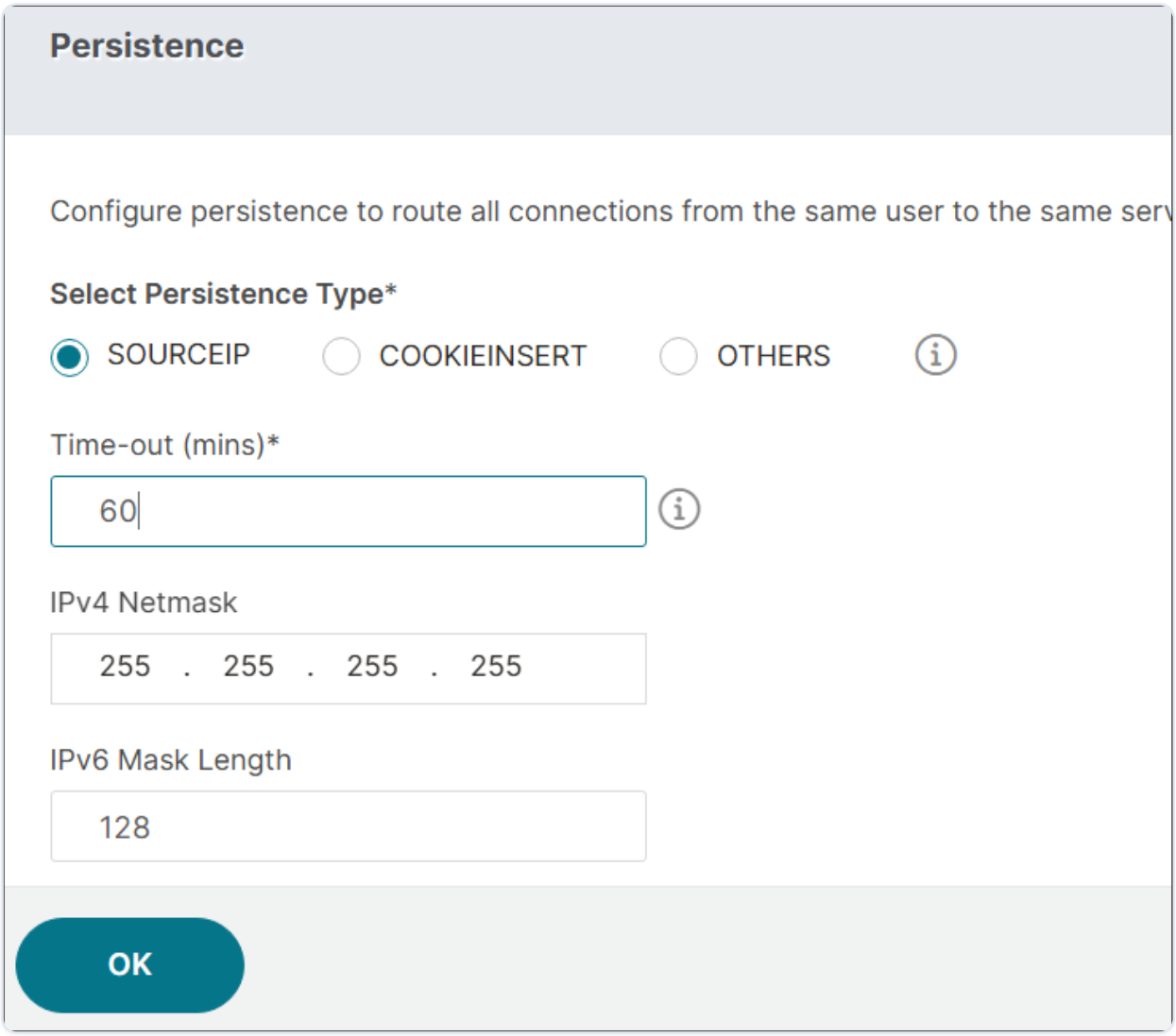




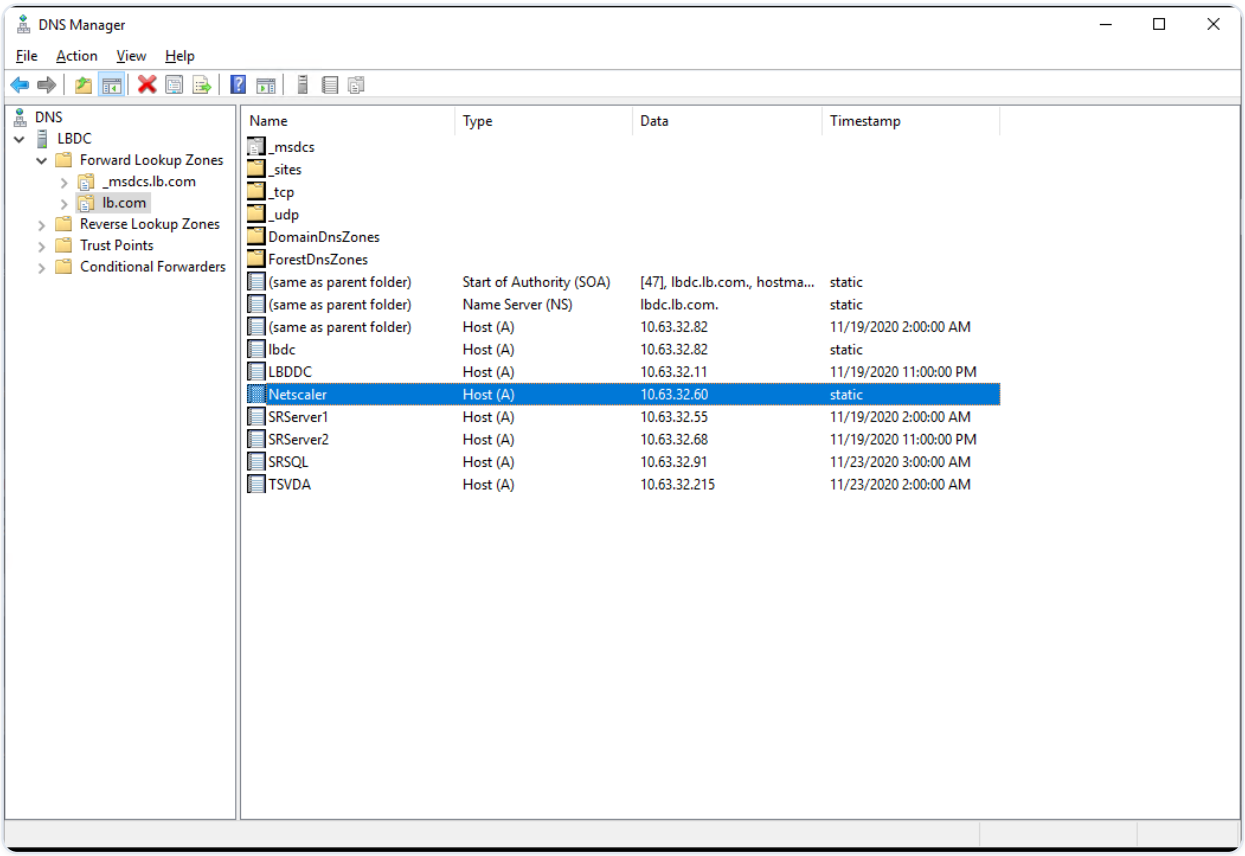
Choose a load balancing method.



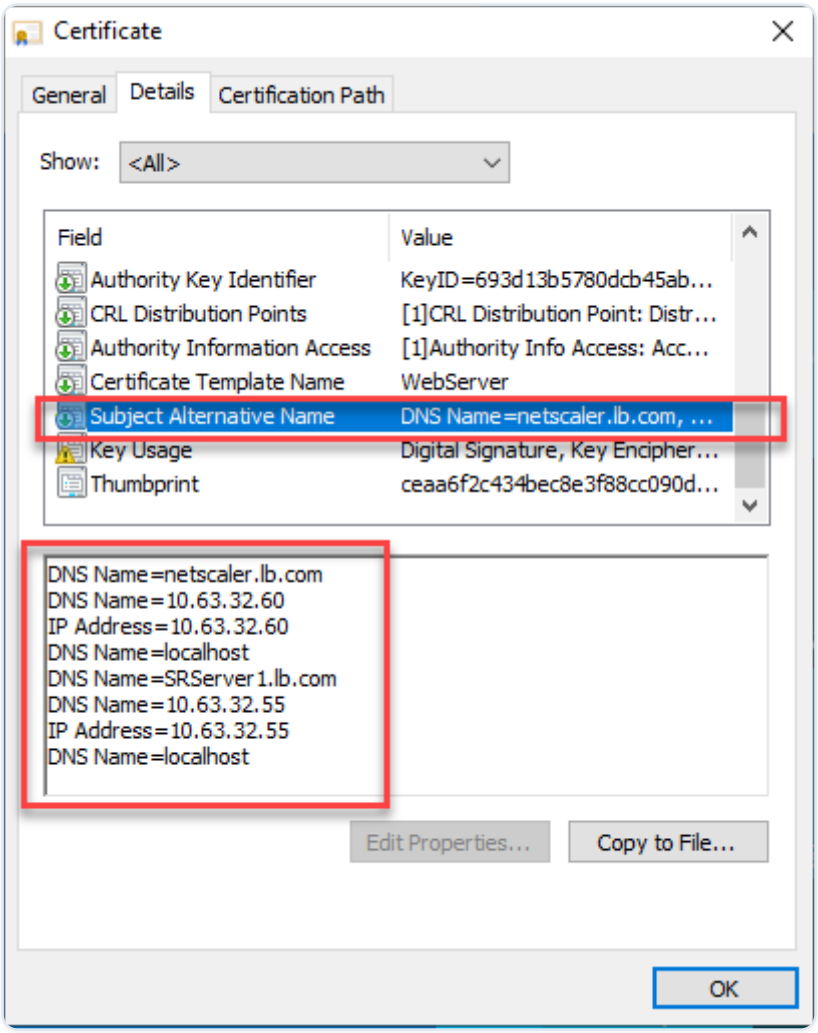
Configure persistence on each virtual server. We recommend you select **SOURCEIP** as the persistence type. For more information, see (../../../citrix-adc/2607 LTSR/getting-started-with-citrix-adc/load-balancing/configure-persistence-settings.md).



7. Create a host record for the Citrix ADC VIP address on the domain controller.



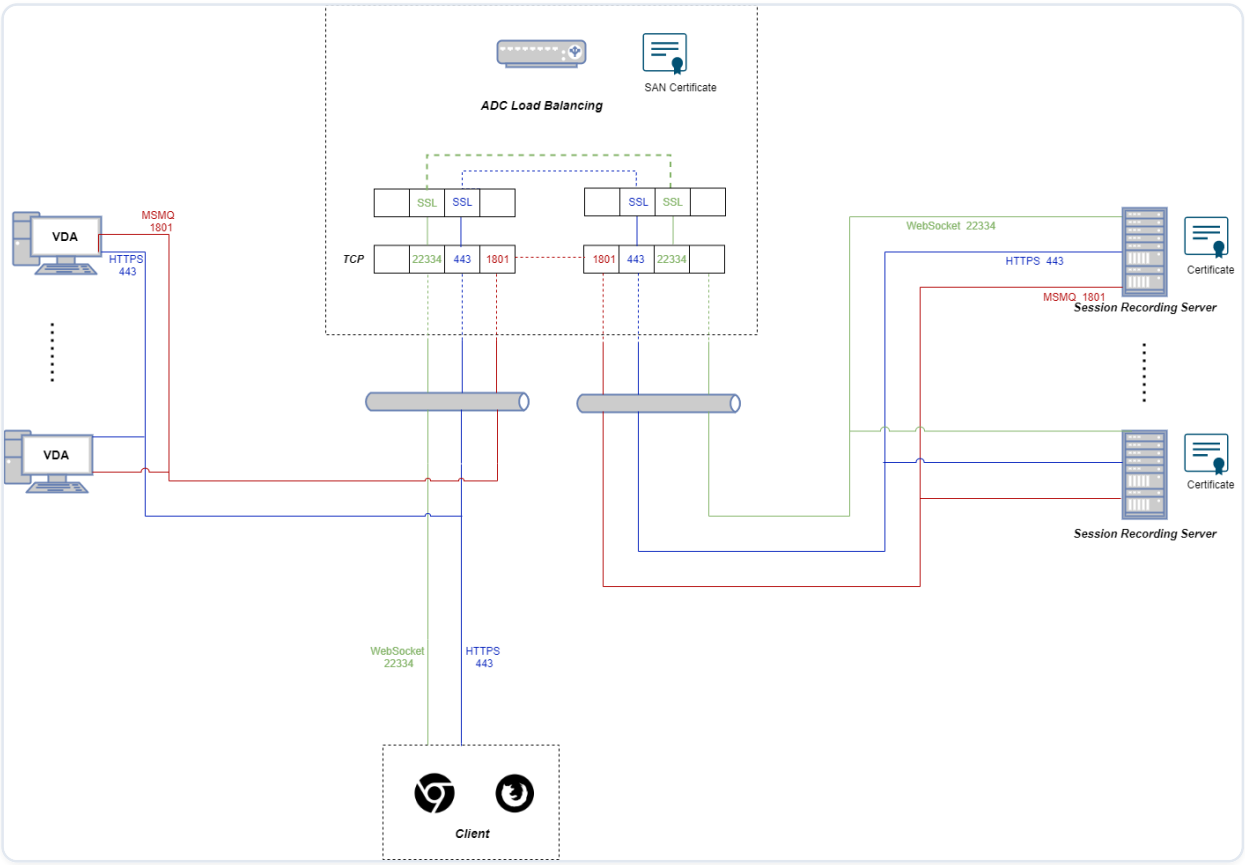
8. To access the web player over HTTPS, ensure that a SAN certificate is available both on Citrix ADC and on each Session Recording server. A SAN certificate contains the FQDNs of the Citrix ADC and of each Session Recording server.



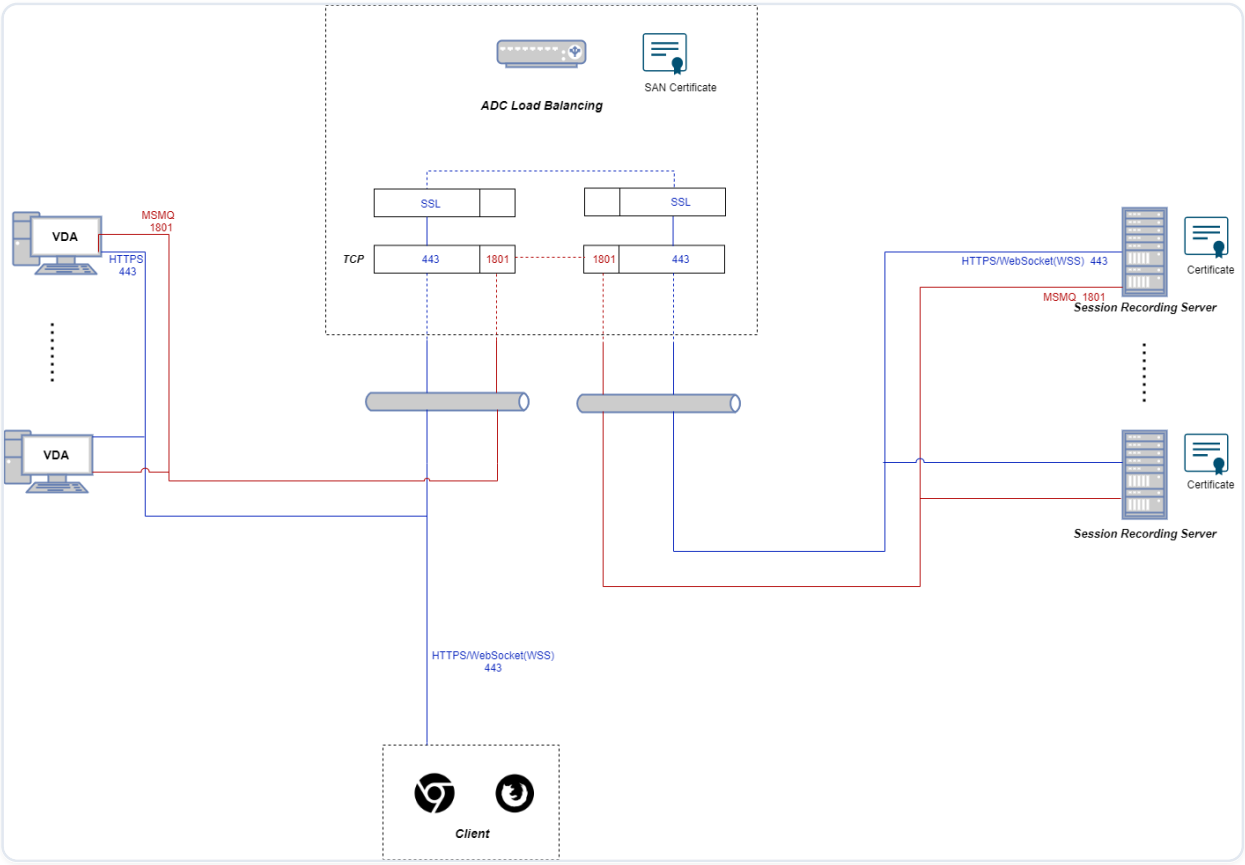
Configure load balancing through SSL offloading

The following topologies show how to configure load balancing through SSL offloading.

- If you are using the Python-based WebSocket server (Version 1.0):

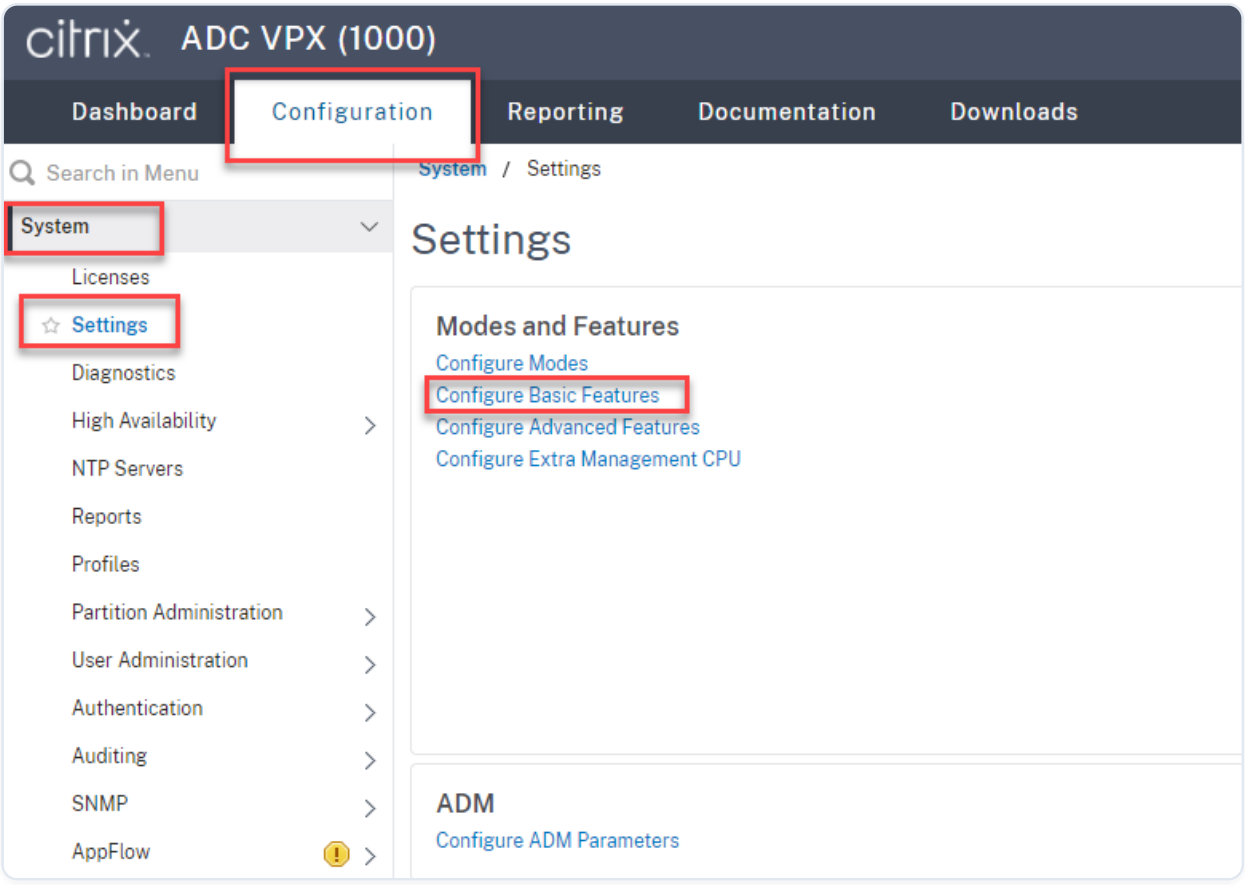


- If you are using the WebSocket server hosted in IIS (Version 2.0):

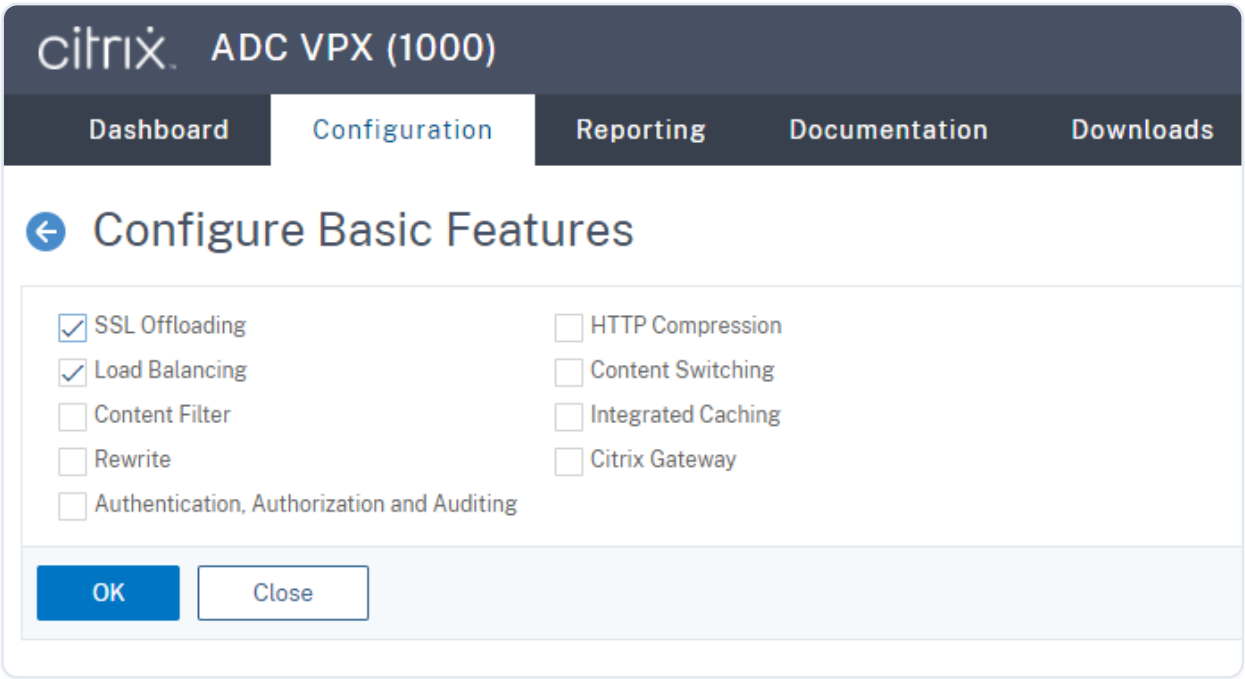


1. Log on to your Citrix ADC VPX instance.

2. Navigate to **Configuration > System > Settings > Configure Basic Features**.

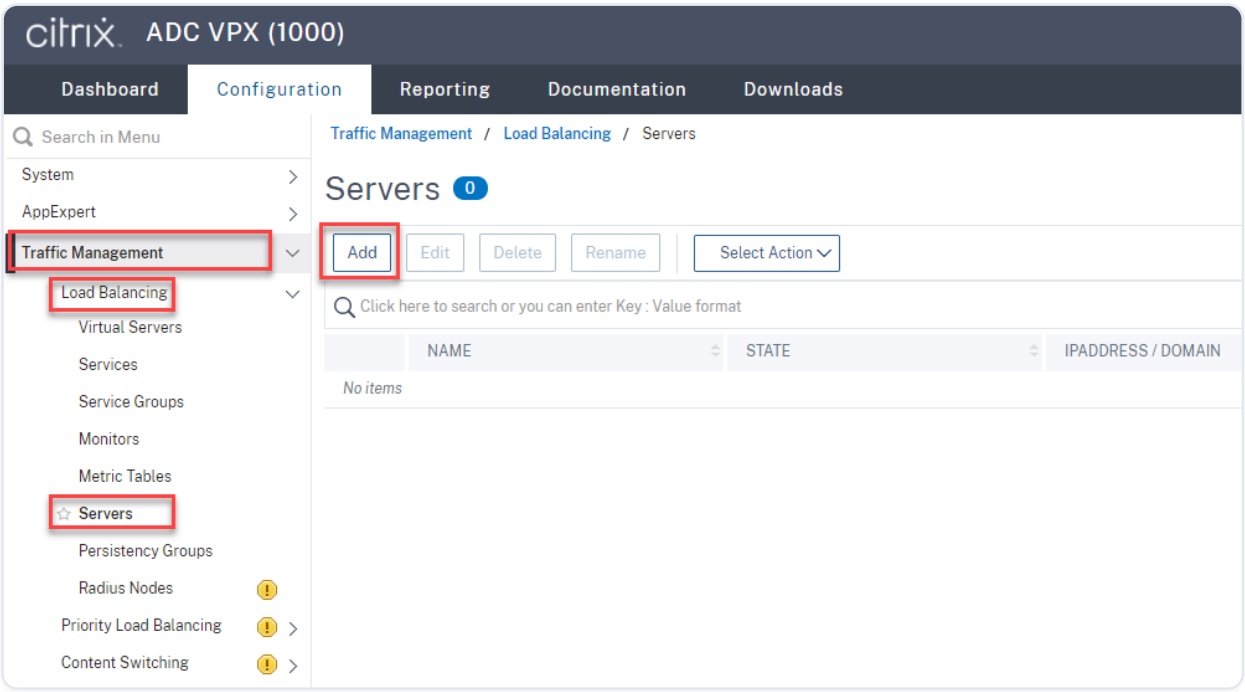


3. Select **SSL Offloading** and **Load Balancing** and click **OK**.

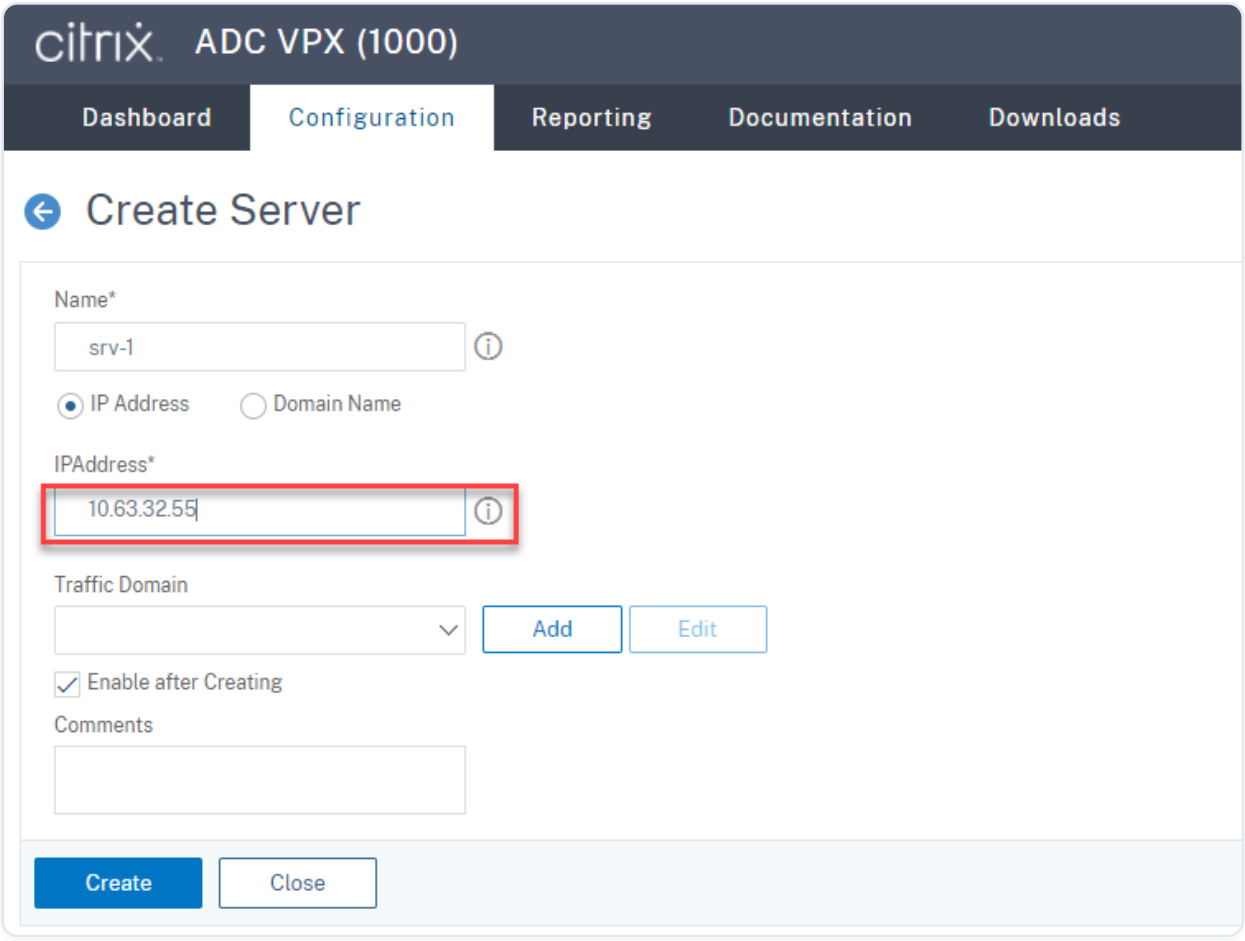


4. Add load balancing servers.

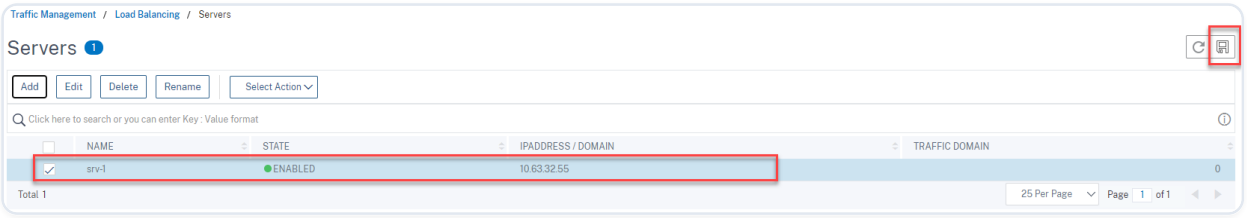
   Navigate to **Traffic Management > Load Balancing > Servers** and click **Add**.



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.

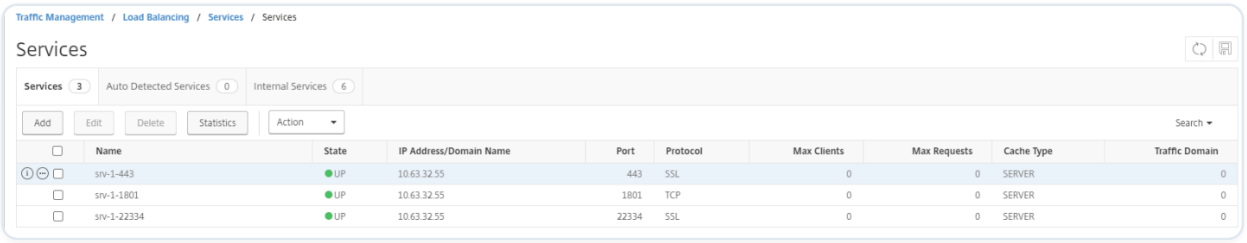


5. Add **load balancing services** for each Session Recording server that you added in the previous step.

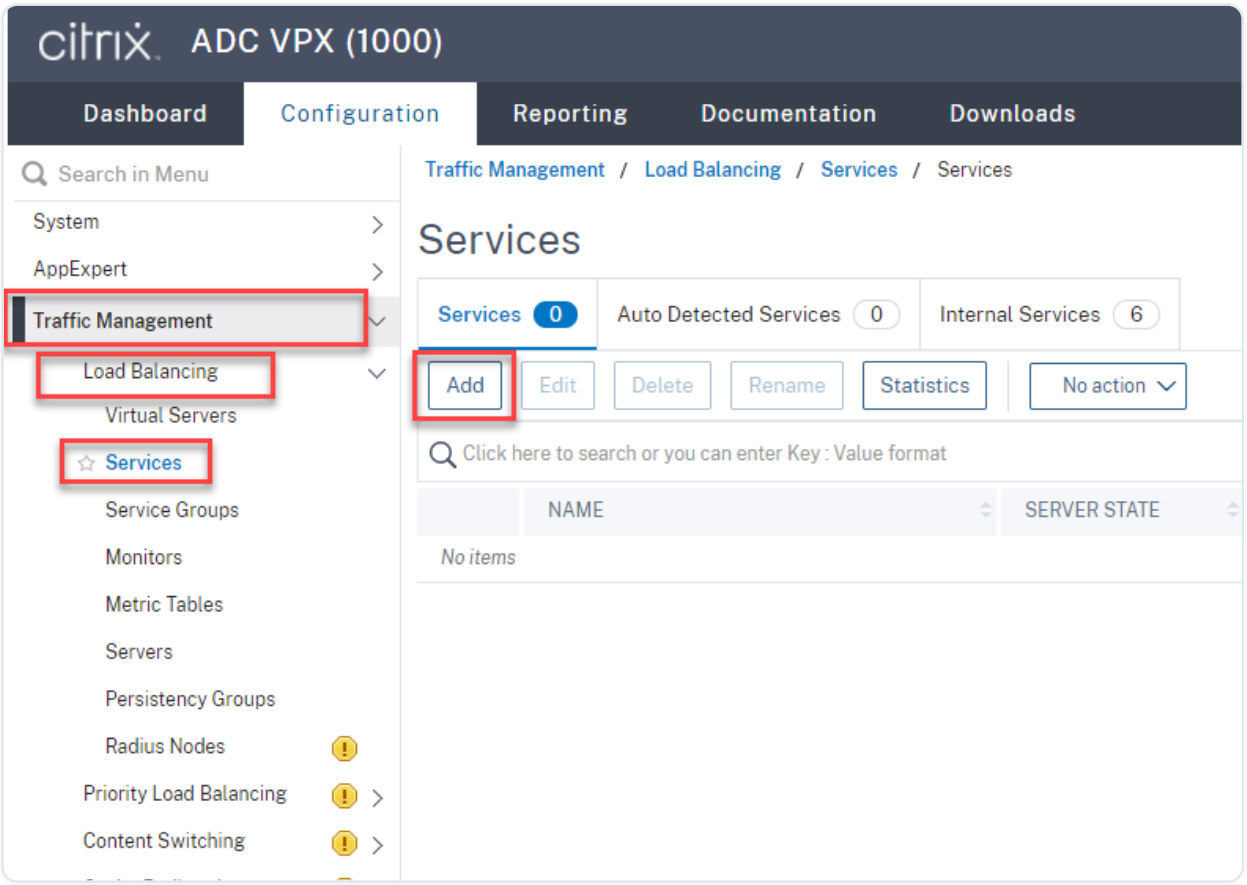
   Add the following **load balancing services** for each Session Recording server:

   - (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:

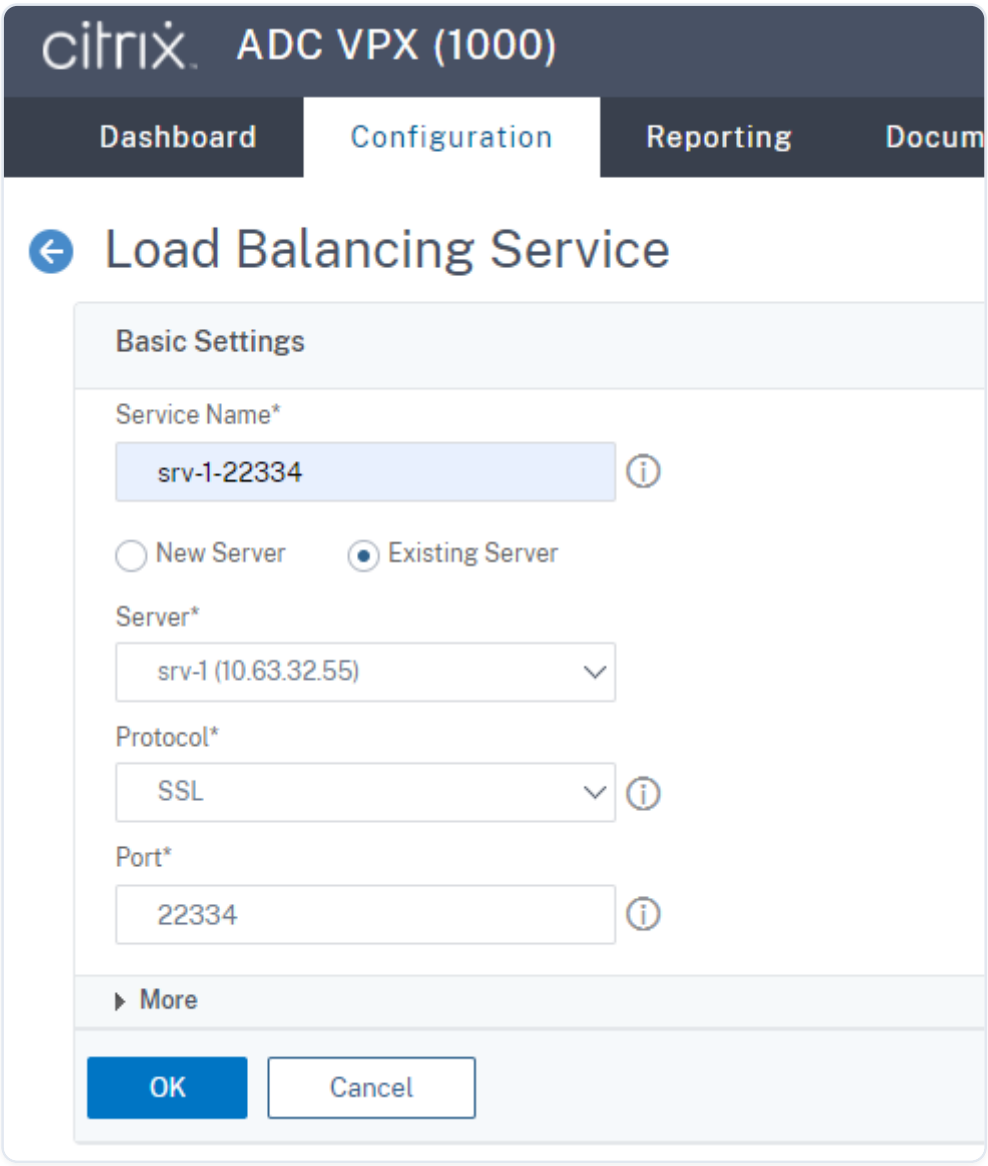


   Navigate to **Traffic Management > Load Balancing > Services** and click **Add**.

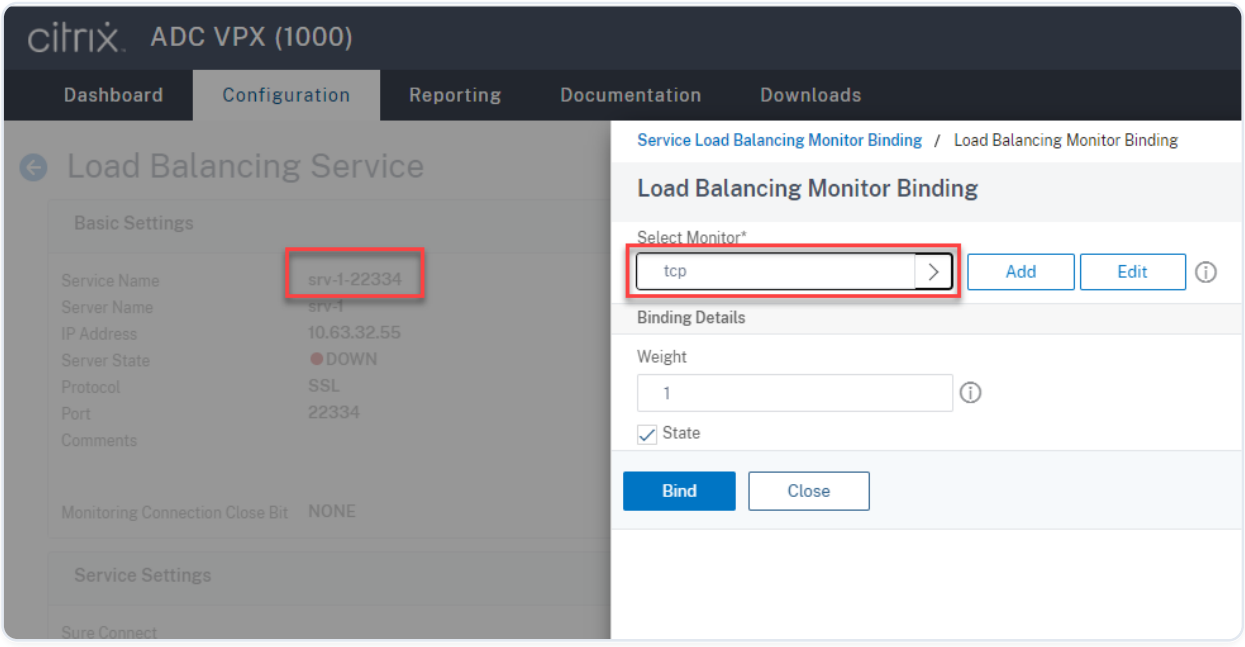


(Required only when you are using the WebSocket server Version 1.0) Add an SSL load balancing service of port 22334 for each Session Recording server. Type a name for the load balancing service, choose **Existing Server**, select the IP address of a Session Recording server, select **SSL** as the server protocol, type port number **22334**, and click **OK**.

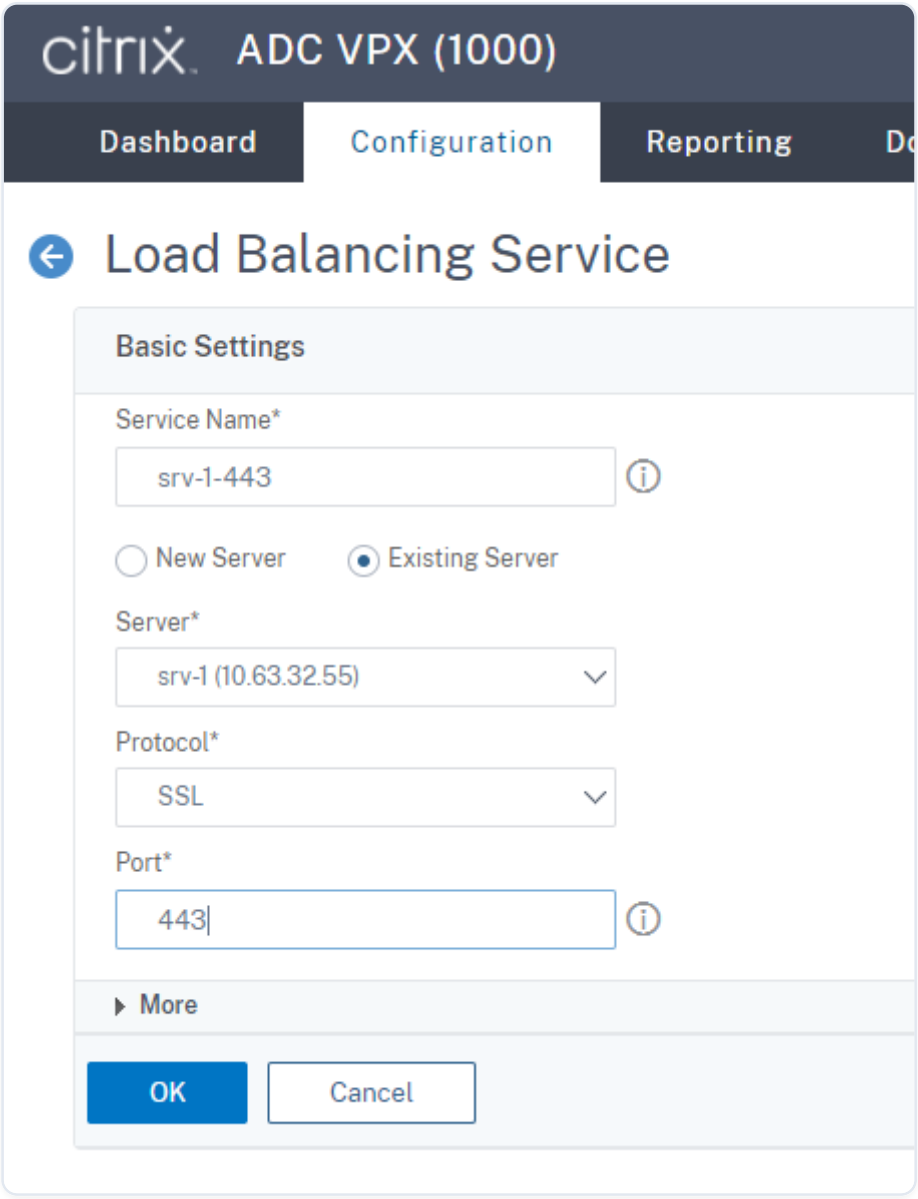
For example, see the following screen capture.



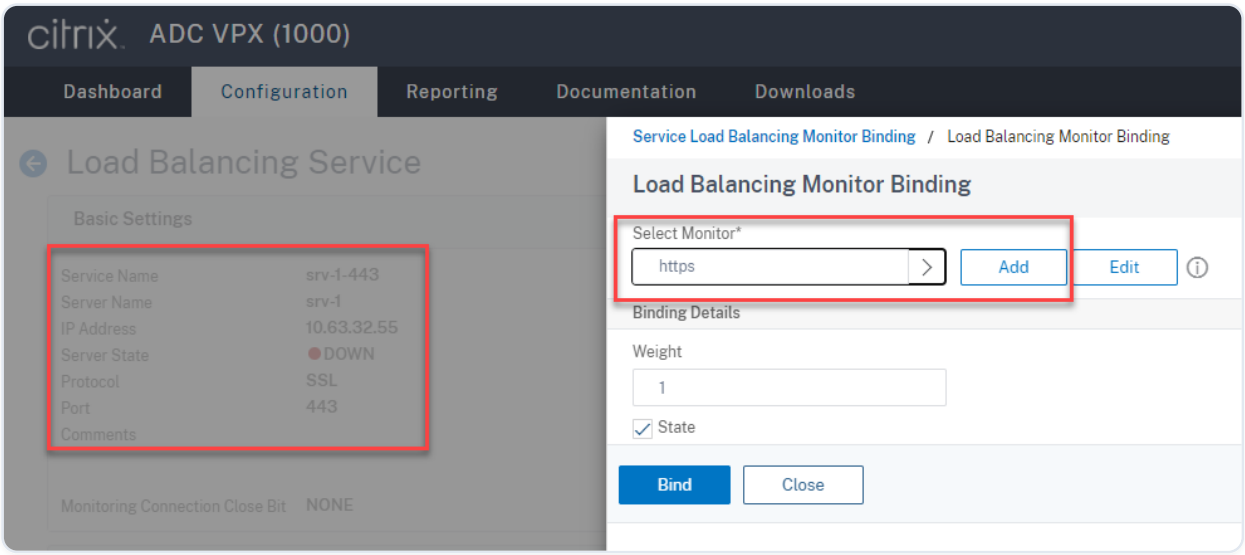
Bind the TCP monitor to the **SSL load balancing service** you just added.



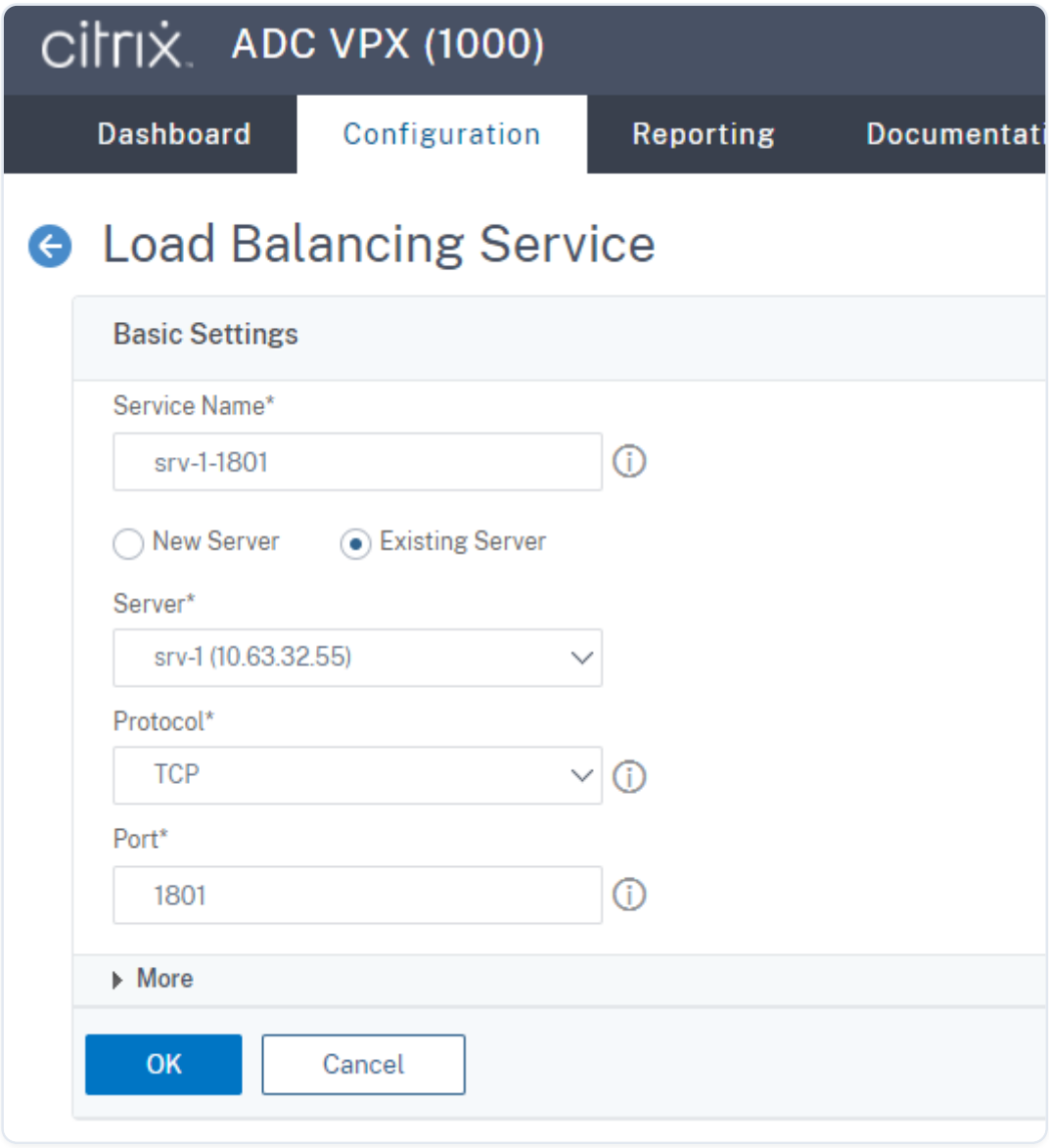
Add an SSL load balancing service of port 443 for each Session Recording server. Type a name for the load balancing service, choose **Existing Server**, select the IP address of a Session Recording server, select **SSL** as the server protocol, type port number 443, and click **OK**.



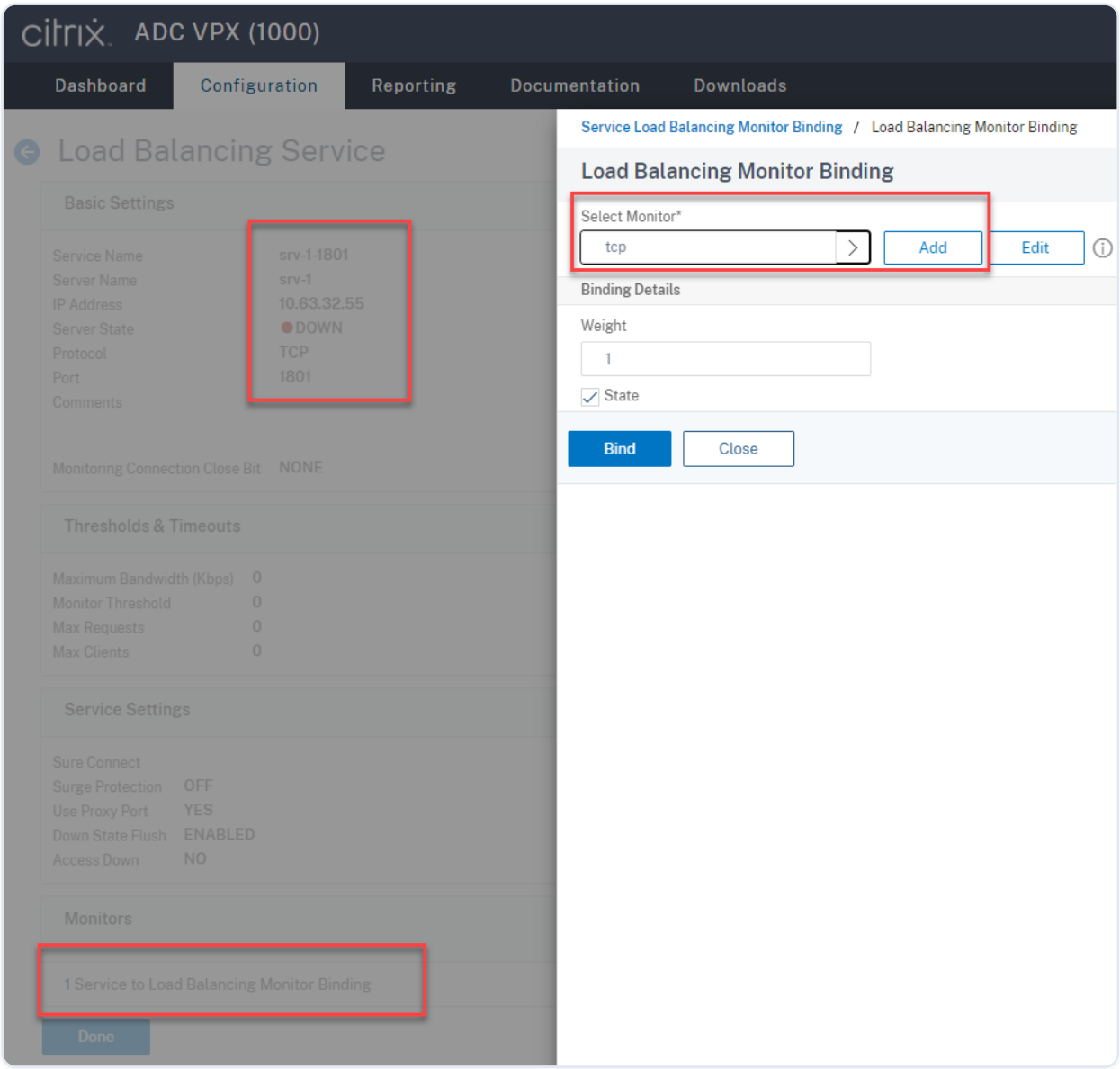
Bind the HTTPS monitor to the **SSL load balancing service** you just added.



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**.

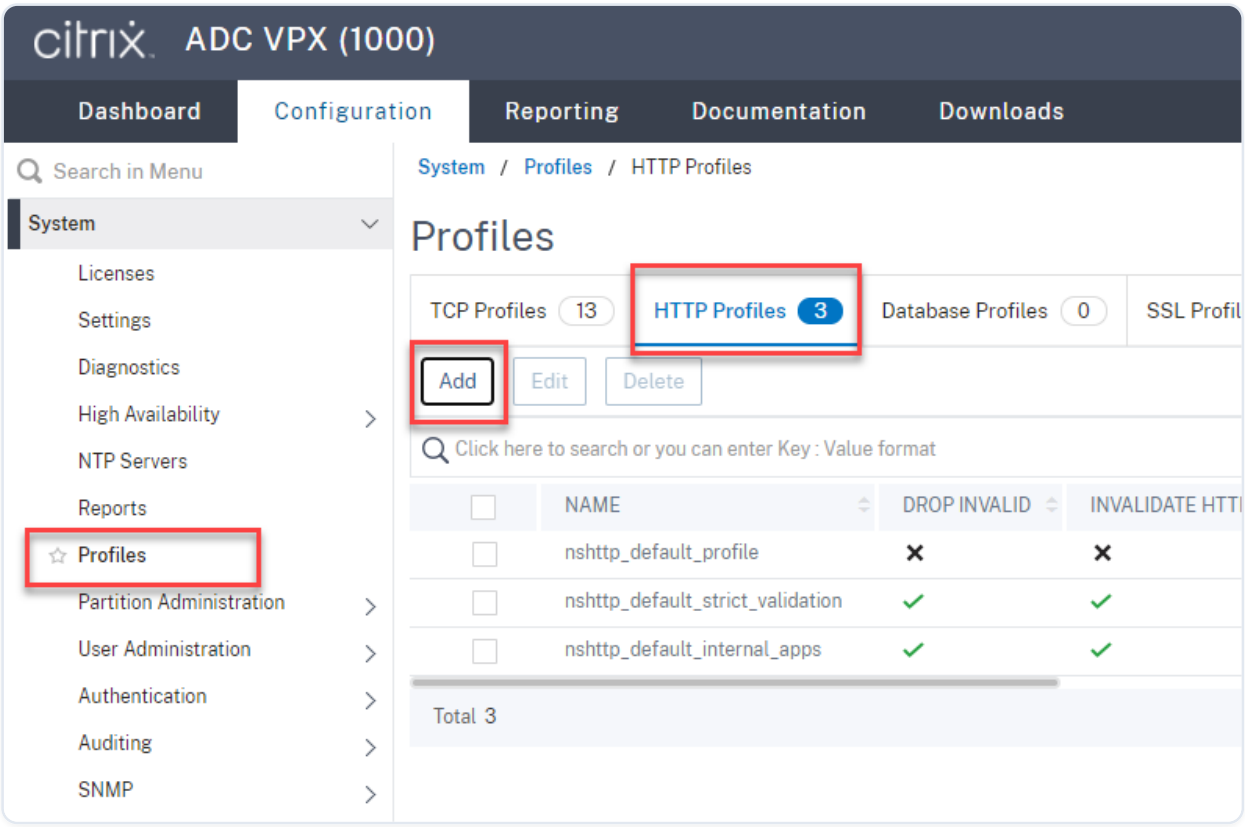


Bind the TCP monitor to the **TCP load balancing service** you just added.

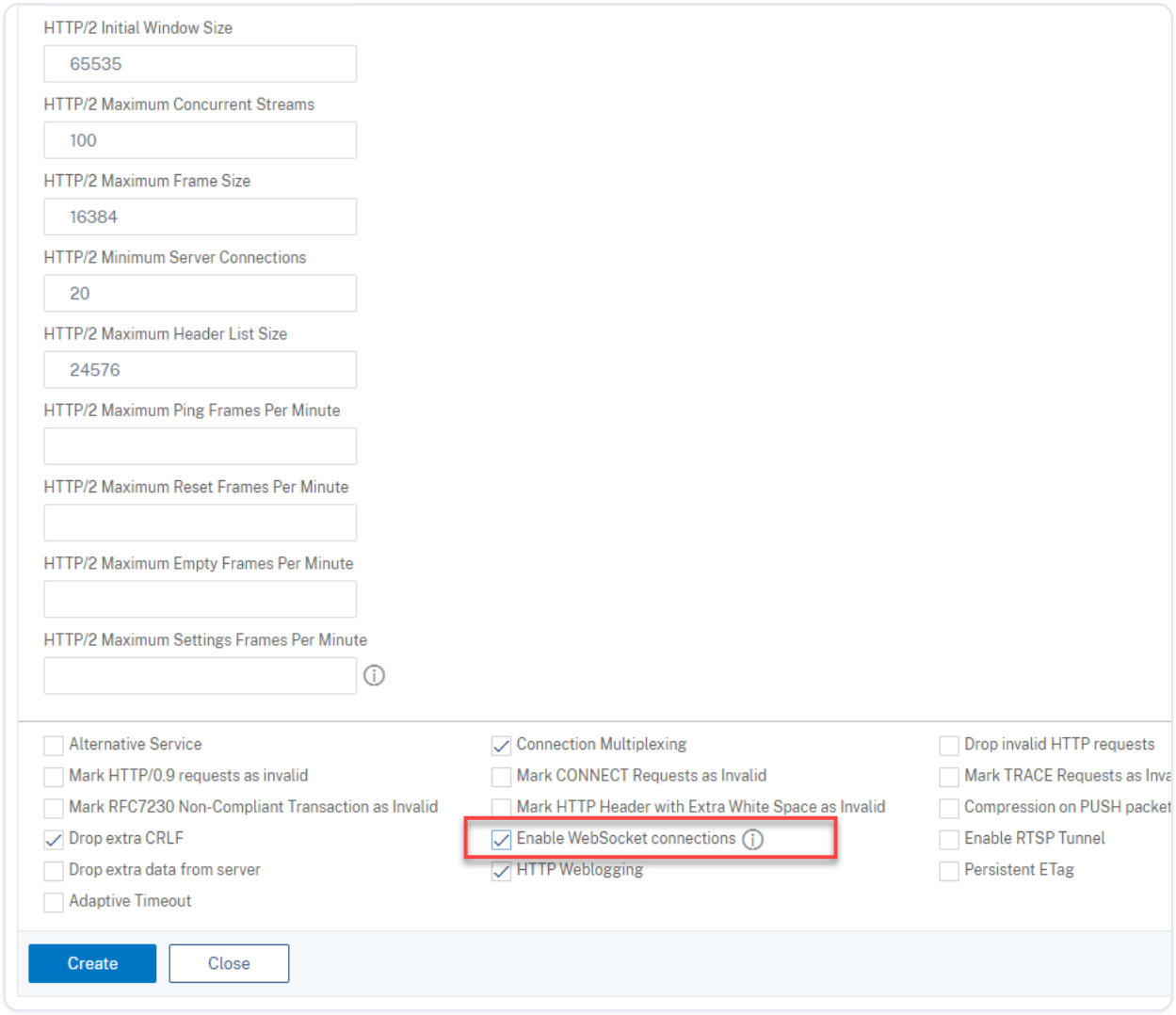


6. (Required only when you are using the WebSocket server Version 1.0) Add an HTTP profile for each **SSL load balancing service** of port 22334.

   Navigate to **System > Profiles > HTTP Profiles** and click **Add**.



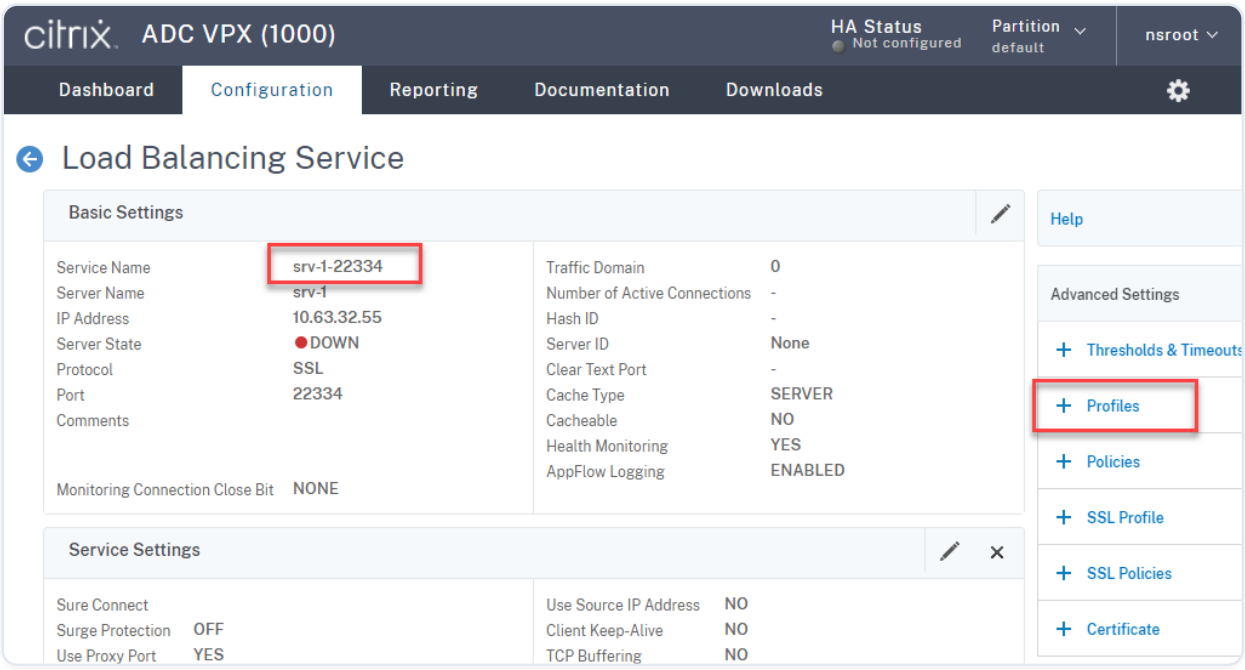
Select the **Enable WebSocket connections** check box and accept the other default settings.



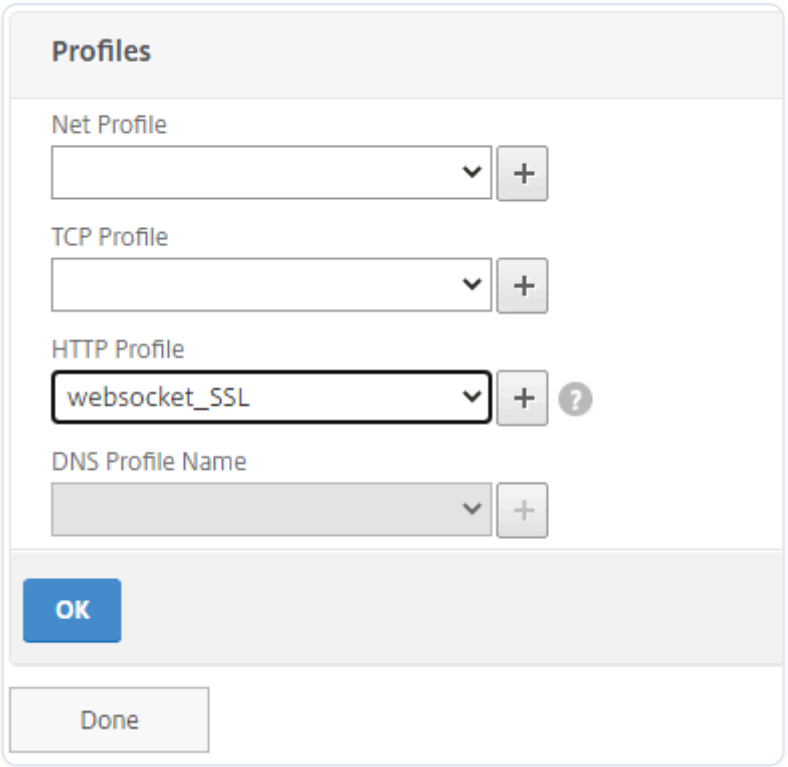
Type a name for the HTTP profile, for example, `websocket_SSL`.

Go back to each **SSL load balancing service** of port 22334, for example, `srv-1-22334`.

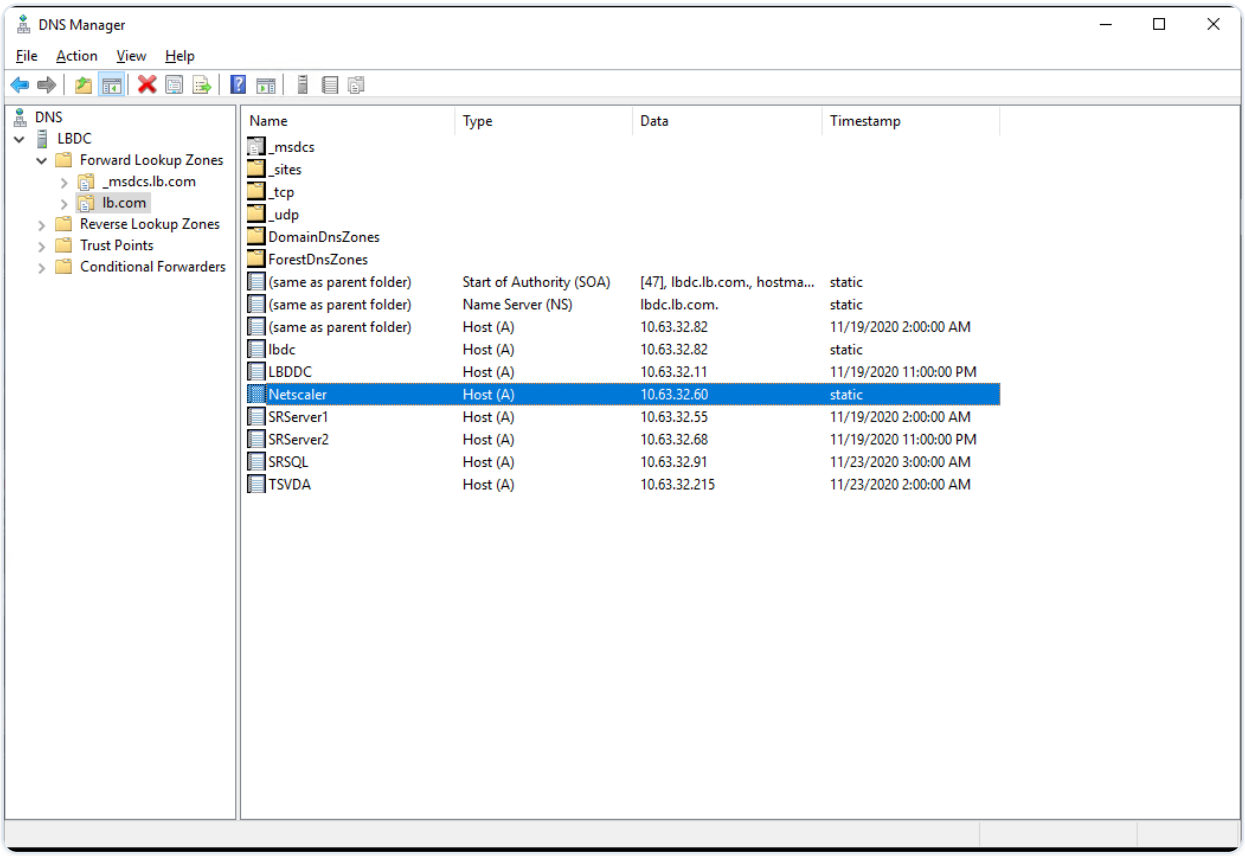
Click **+ Profiles**.



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.

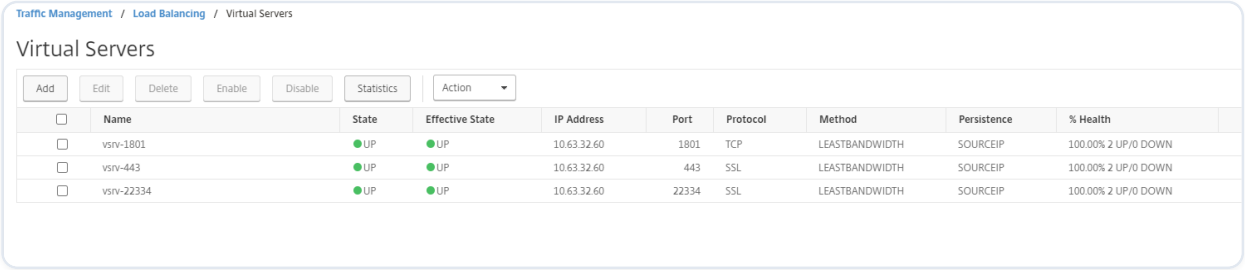


9. Add **load balancing virtual servers**.

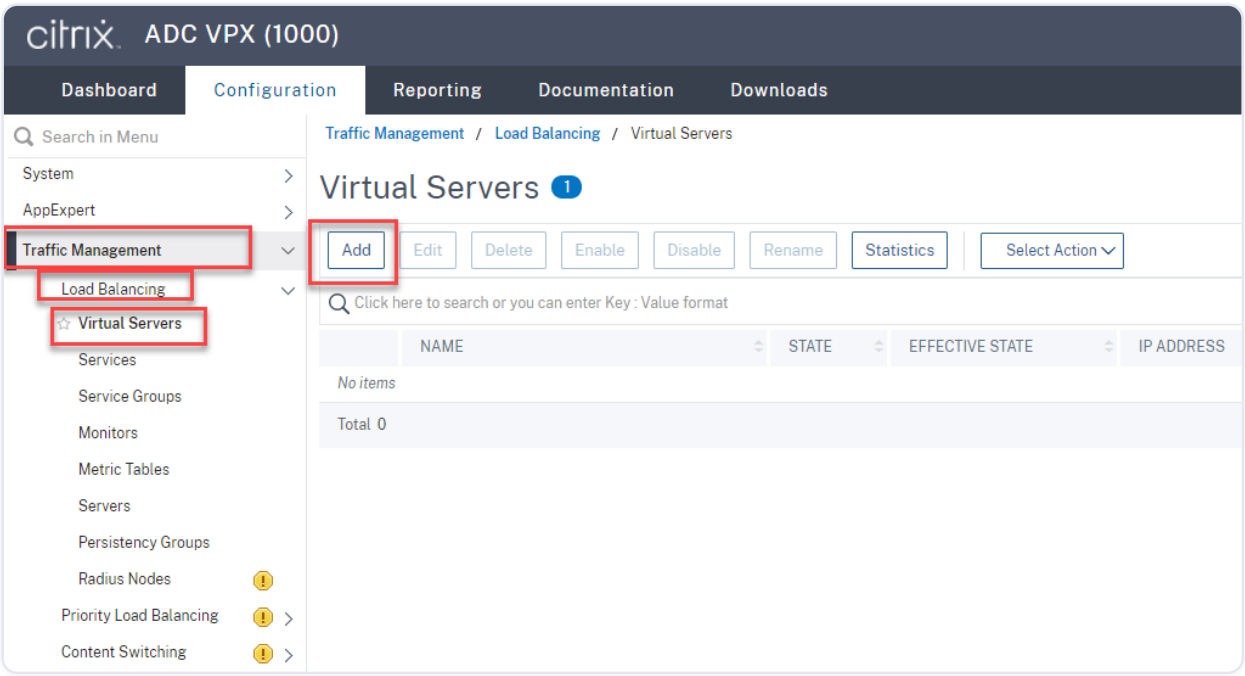
   Add the following **load balancing virtual servers** with the Citrix ADC VIP address.

   - (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

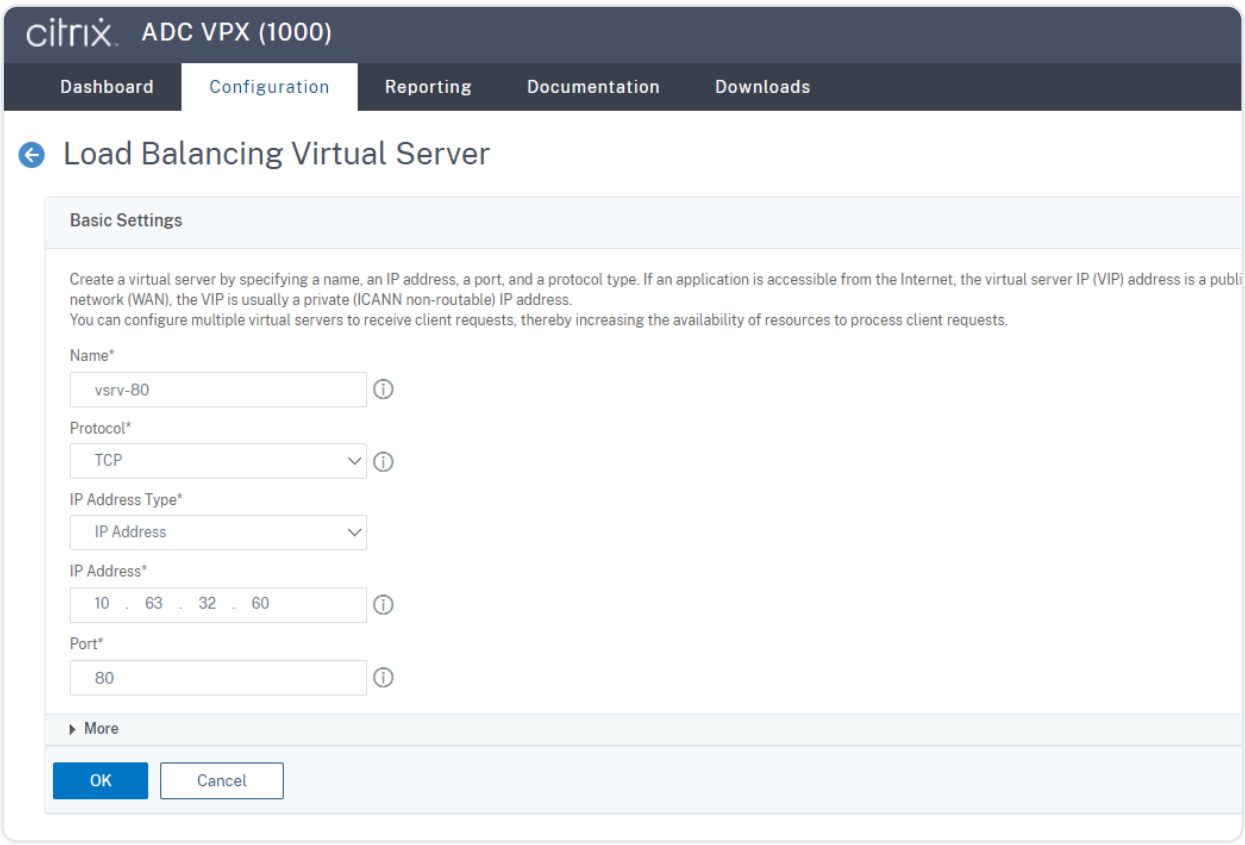
   For example, see the following screen capture.



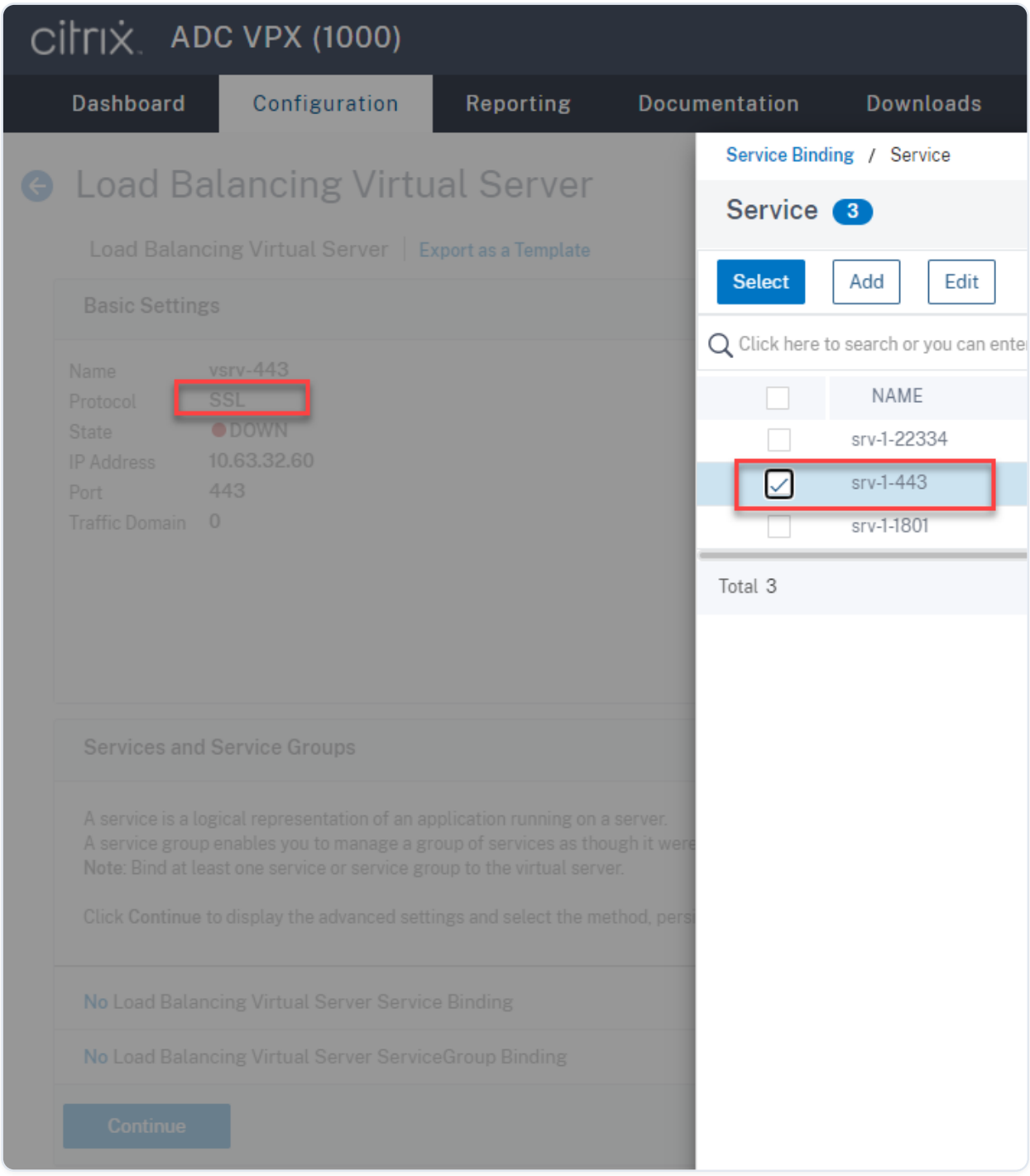
   Navigate to **Traffic Management > Load Balancing > Virtual Servers** and click **Add**.



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.



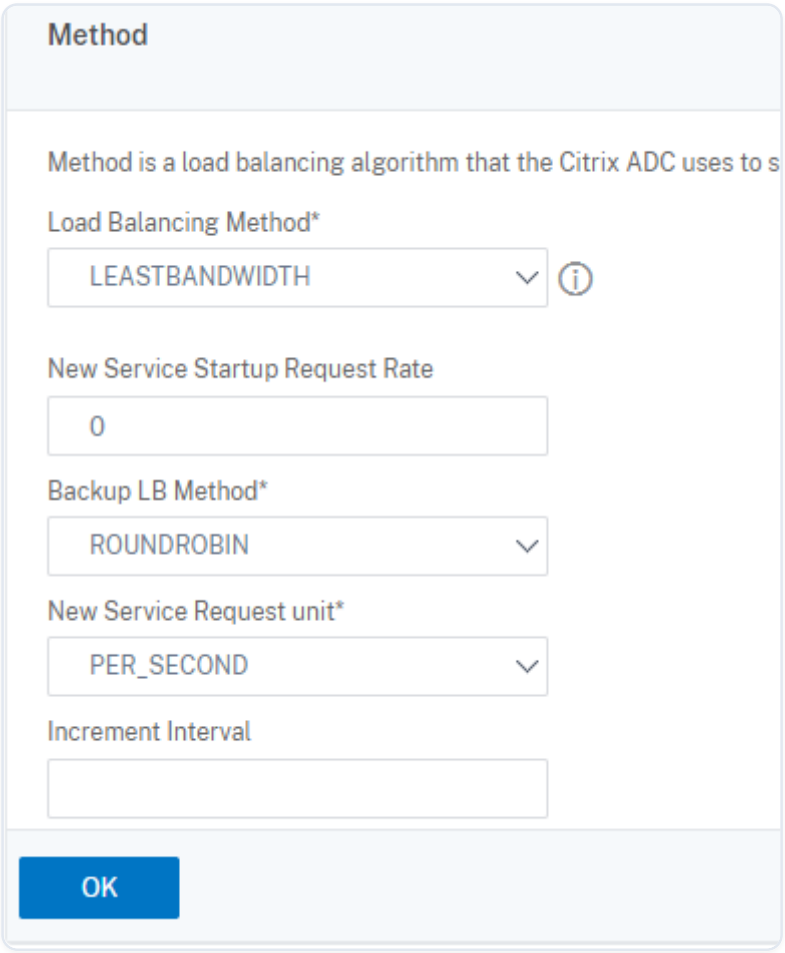
Bind each virtual server to the **load balancing service** of the same port. For example:



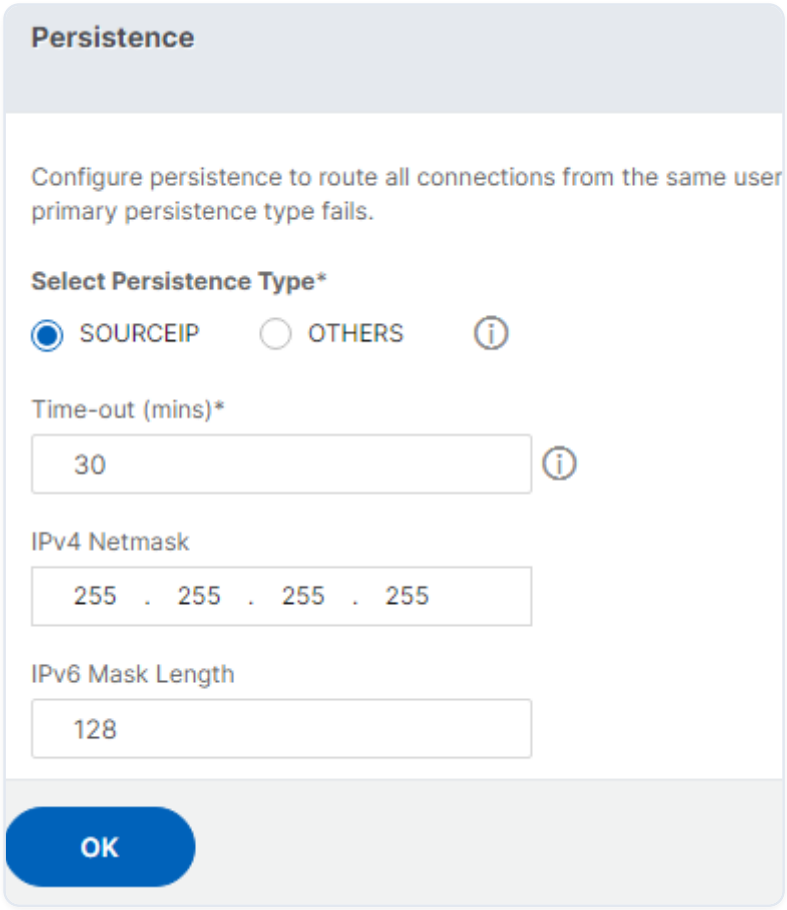
Tip:

The **load balancing service** of port 22334 is required only when you are using the WebSocket server Version 1.0.

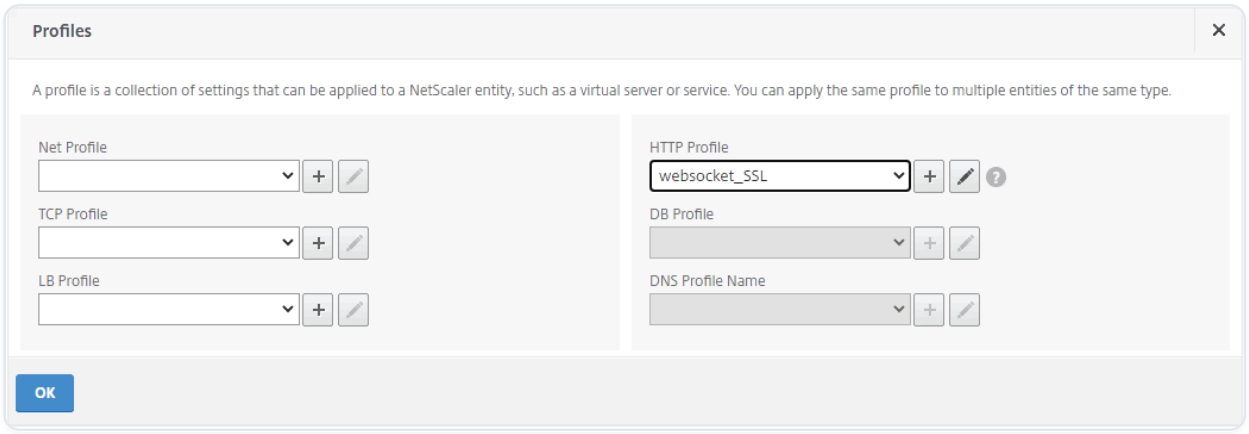
Choose a load balancing method.



Configure persistence on each virtual server. We recommend you select **SOURCEIP** as the persistence type. For more information, see (../../../citrix-adc/2607 LTSR/getting-started-with-citrix-adc/load-balancing/configure-persistence-settings.md).



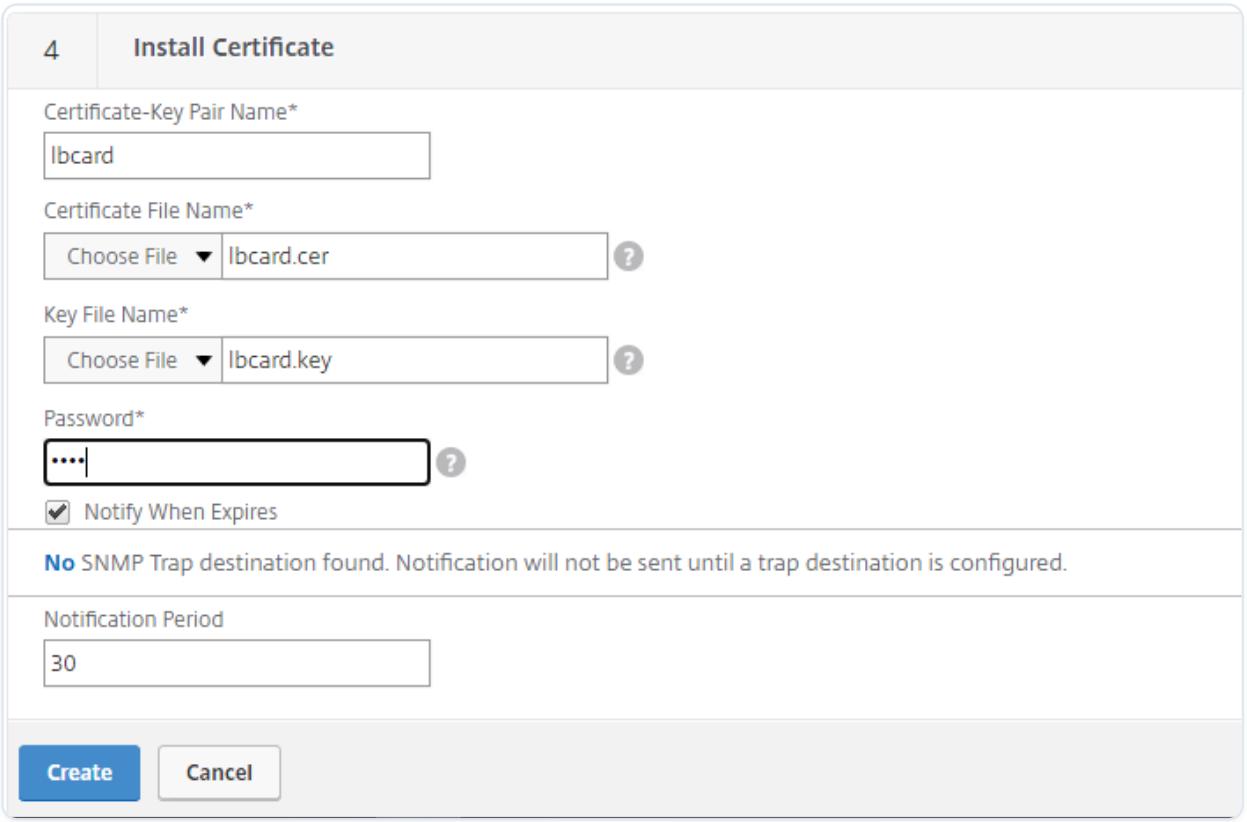
(Required only when you are using the WebSocket server Version 1.0) Add an HTTP profile for the load balancing virtual server of port 22334.



10. Install a Subject Alternative Name (SAN) certificate in Citrix ADC.

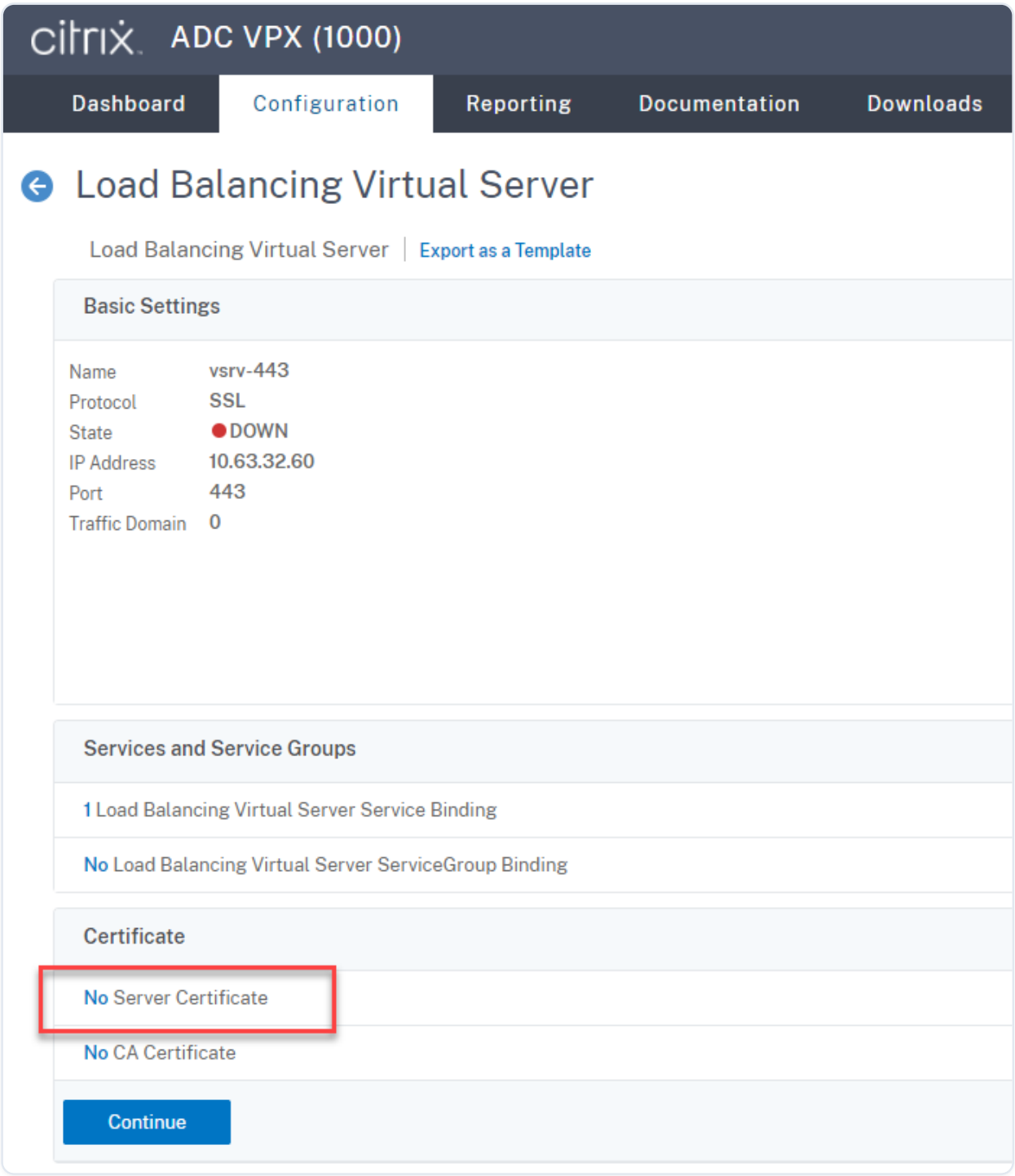
    Obtain a SAN certificate in PEM format from a trusted Certificate Authority (CA). Extract and upload the certificate and private key files in Citrix ADC by navigating to **Traffic Management > SSL > Server Certificate Wizard**.

    For more information, see (../../../citrix-adc/2607 LTSR/ssl/ssl-certificates.md).



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**.

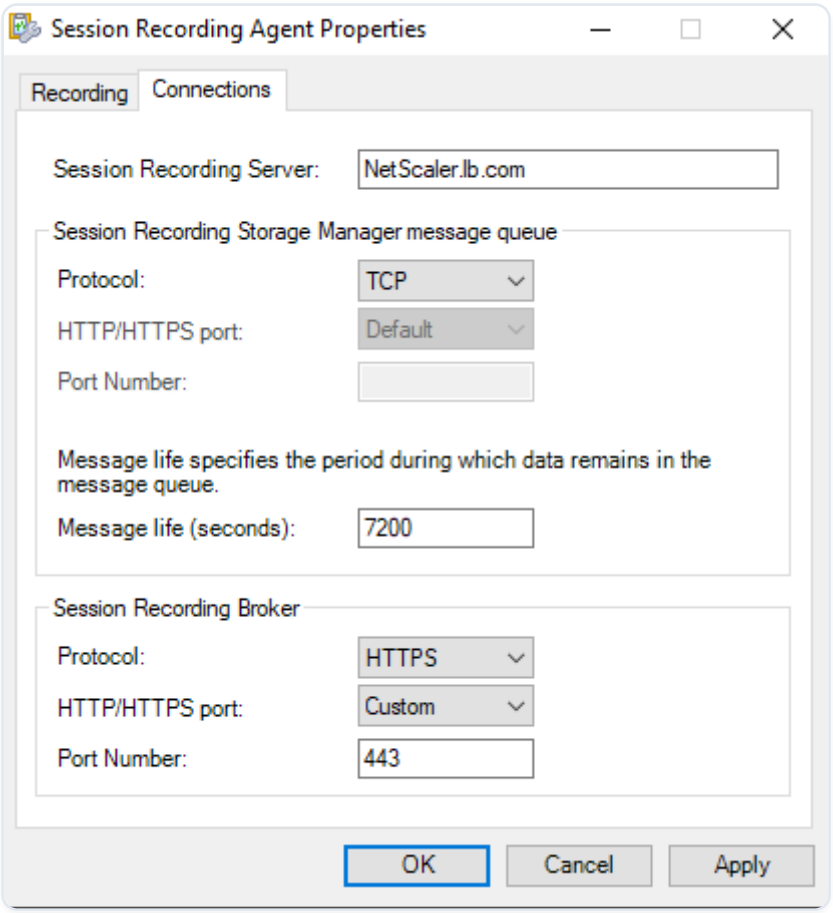


Add the previously mentioned SAN certificate and click **Bind**.

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.

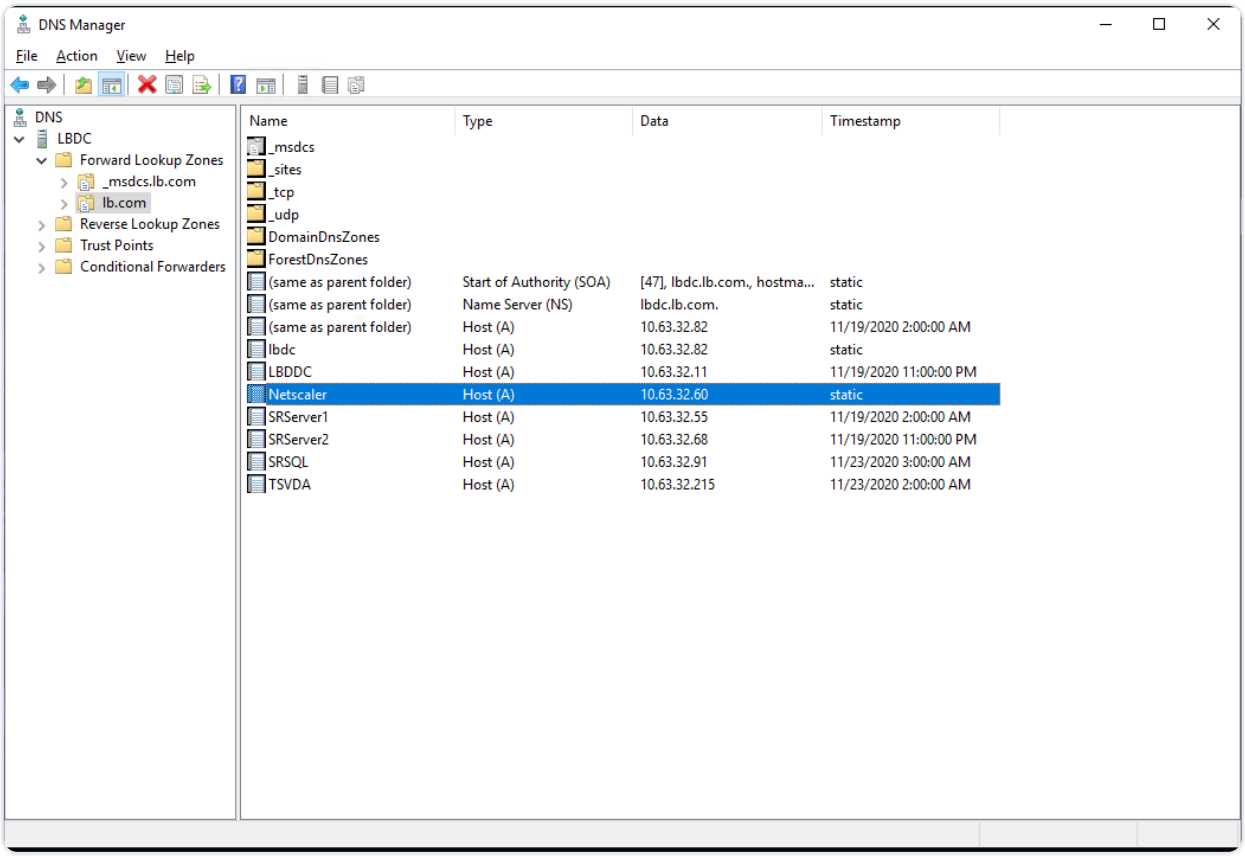
   Type your Citrix ADC VIP address or FQDN in the **Session Recording Server** box.



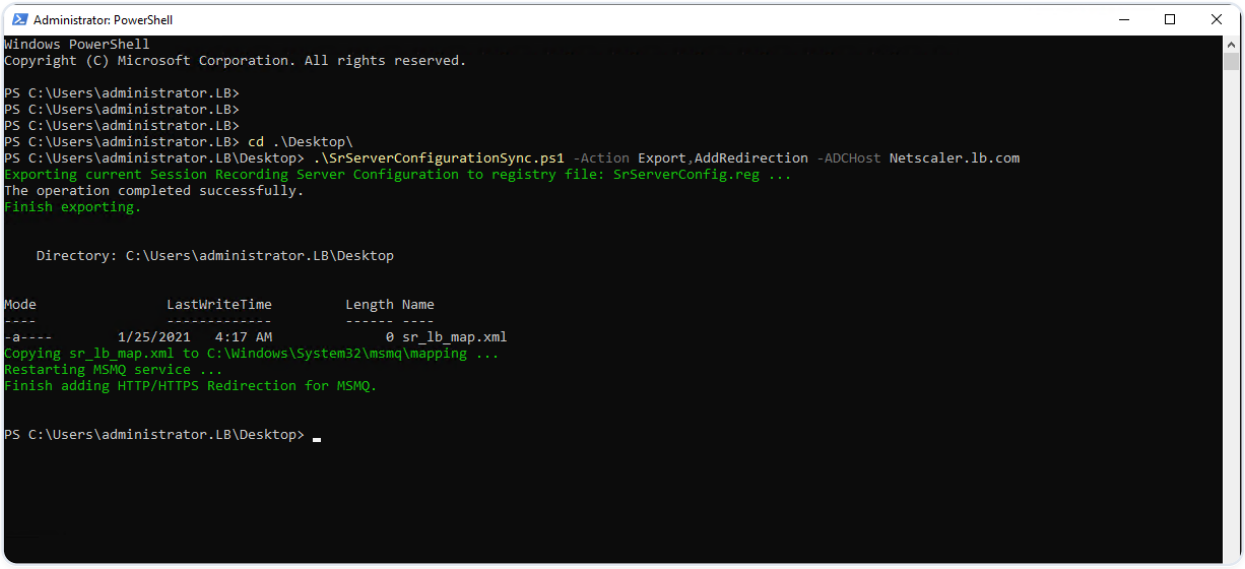
On each Session Recording server, add and set the `IgnoreOSNameValidation` DWORD value to `1` under `HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\MSMQ\Parameters`.

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.

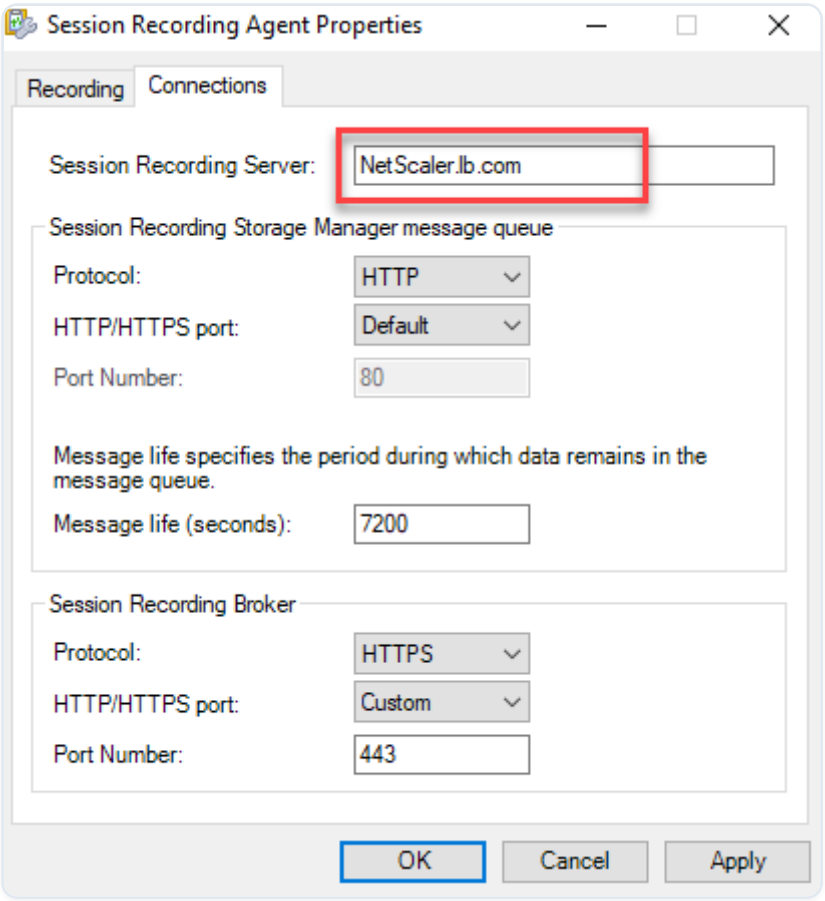


On each Session Recording server, run the `powershell.exe -file SrServerConfigurationSync.ps1 –Action AddRedirection – ADCHost <ADCHost>` command to add redirections from Citrix ADC to the local host. `<ADCHost>` is the FQDN of the Citrix ADC VIP address. A redirection file, for example, `sr_lb_map.xml` 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

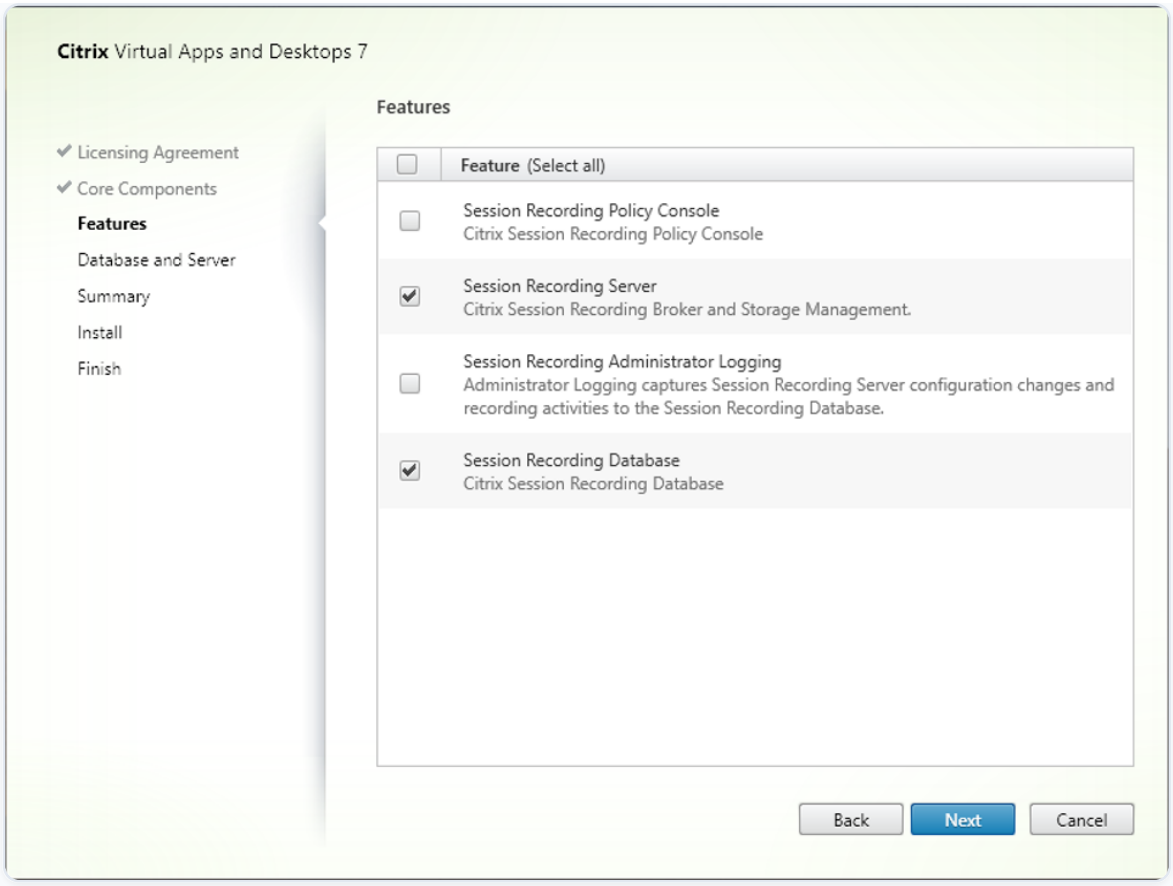
1. Launch a Citrix virtual session.
2. Check whether the session can be recorded.
3. Check whether the web player and the Session Recording player can play back the recording file.

Step 7: Add more Session Recording servers

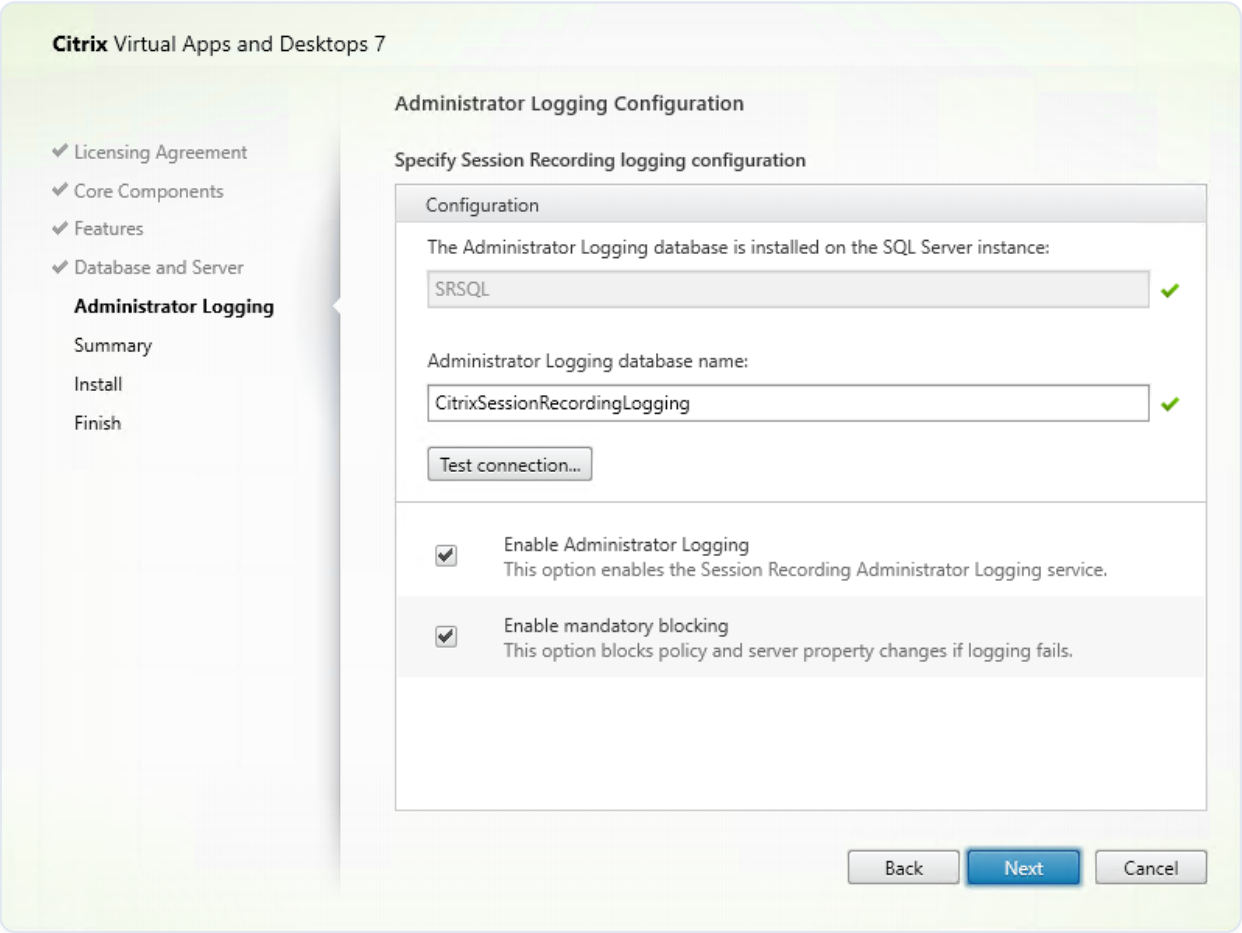
1. Prepare a machine in the same domain and install the Session Recording server, database, and administrator logging modules on the machine.

Note:

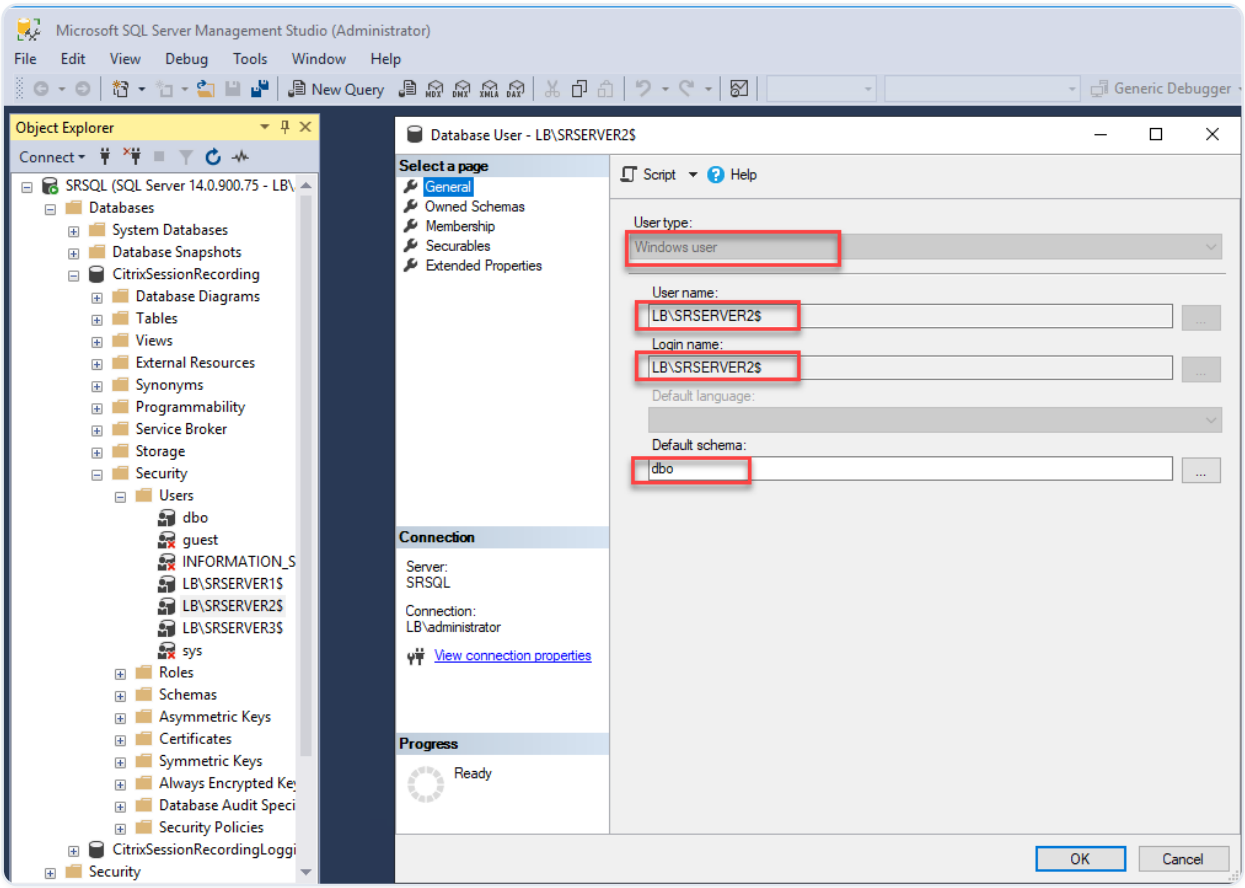
The Session Recording administrator logging is an optional subfeature of the Session Recording server. Select the Session Recording server before you can select the Session Recording administrator logging. The Session Recording database is a mandatory subfeature of the Session Recording server. When the Session Recording server is selected for installation, the Session Recording database is also selected automatically and cannot be unselected.

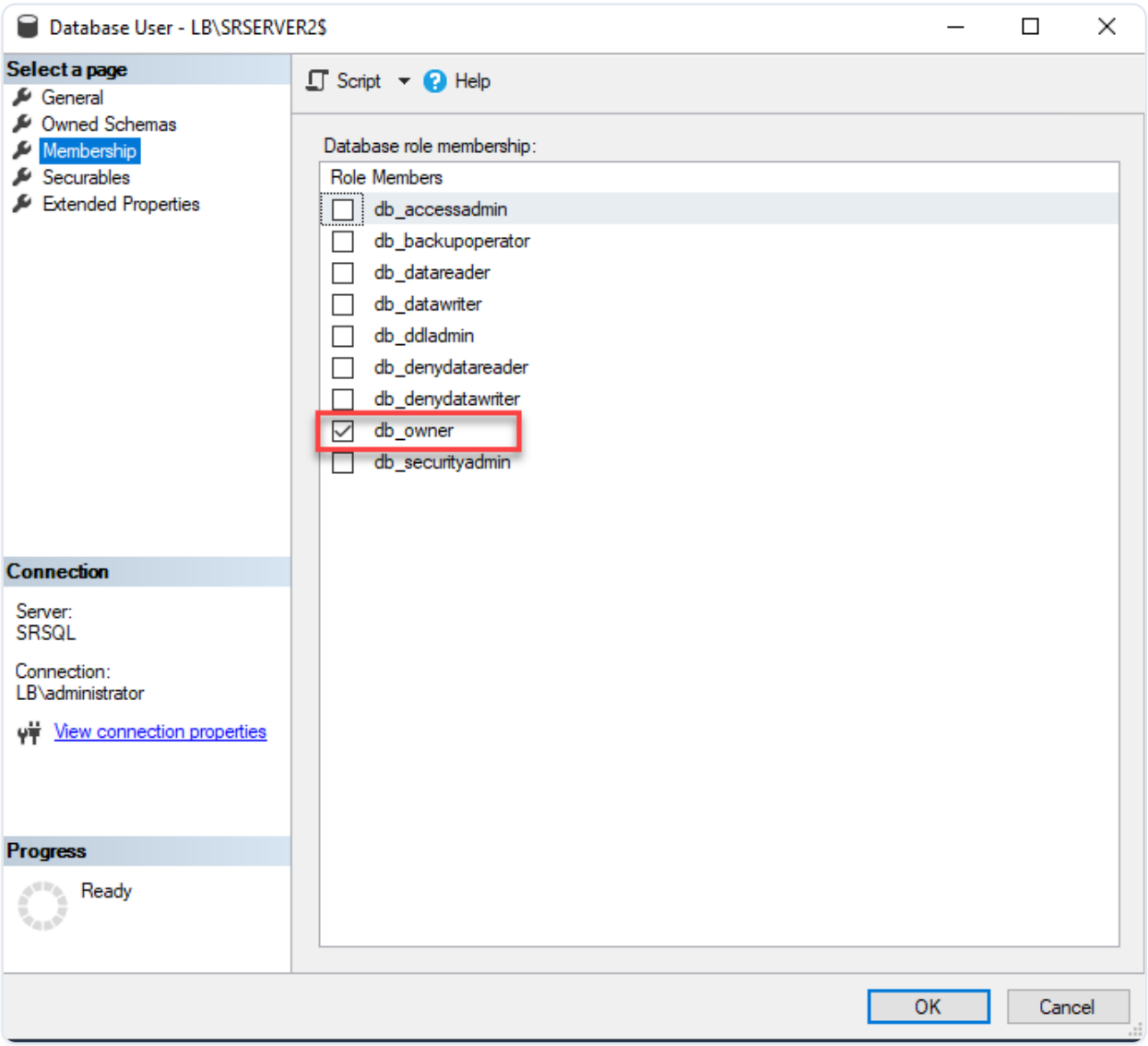


2. Use the same database names as the existing Session Recording server. For example:

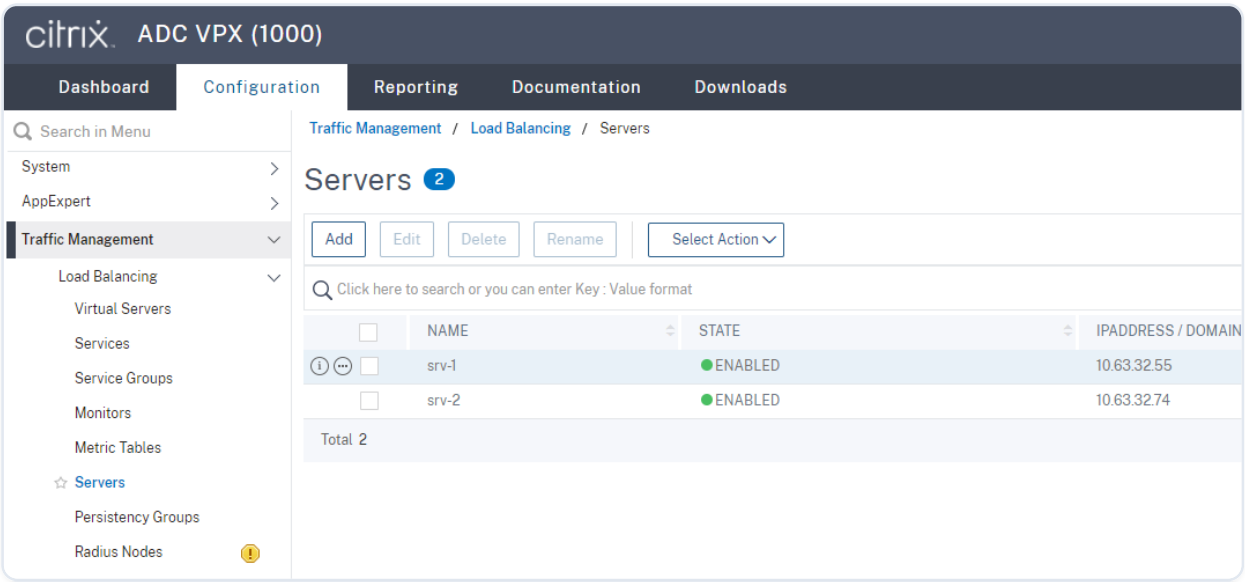


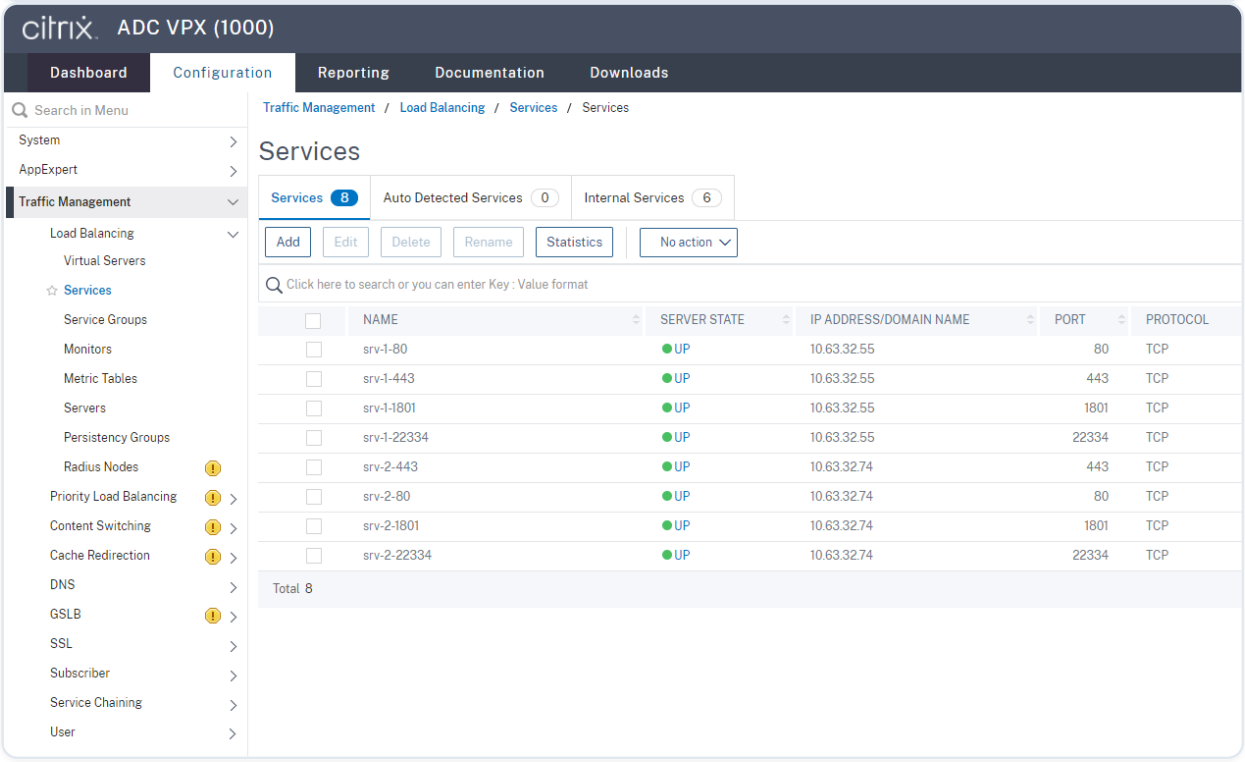
3. Disable the network firewall on the machine.
4. On the SQL Server where you installed the Session Recording database, add all the Session Recording server machine accounts to the shared Session Recording database and assign them with the `db_owner` permission. For example:

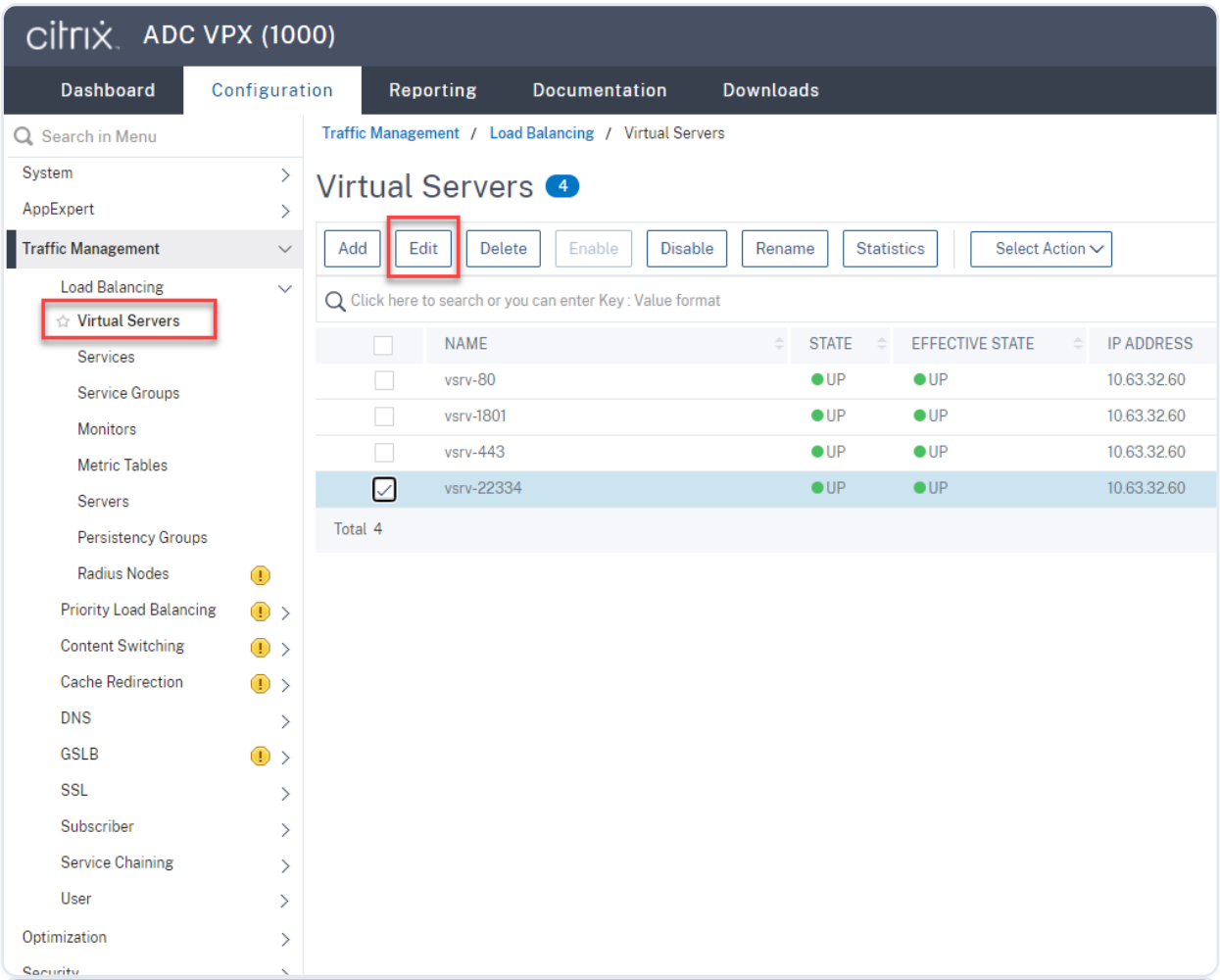

Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Generic Debugger
Object Explorer
Connect
SRSQL (SQL Server 14.0.900.75 - LB\
Databases
System Databases
Database Snapshots
CitrixSessionRecording
Database Diagrams
Tables
Views
External Resources
Synonyms
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

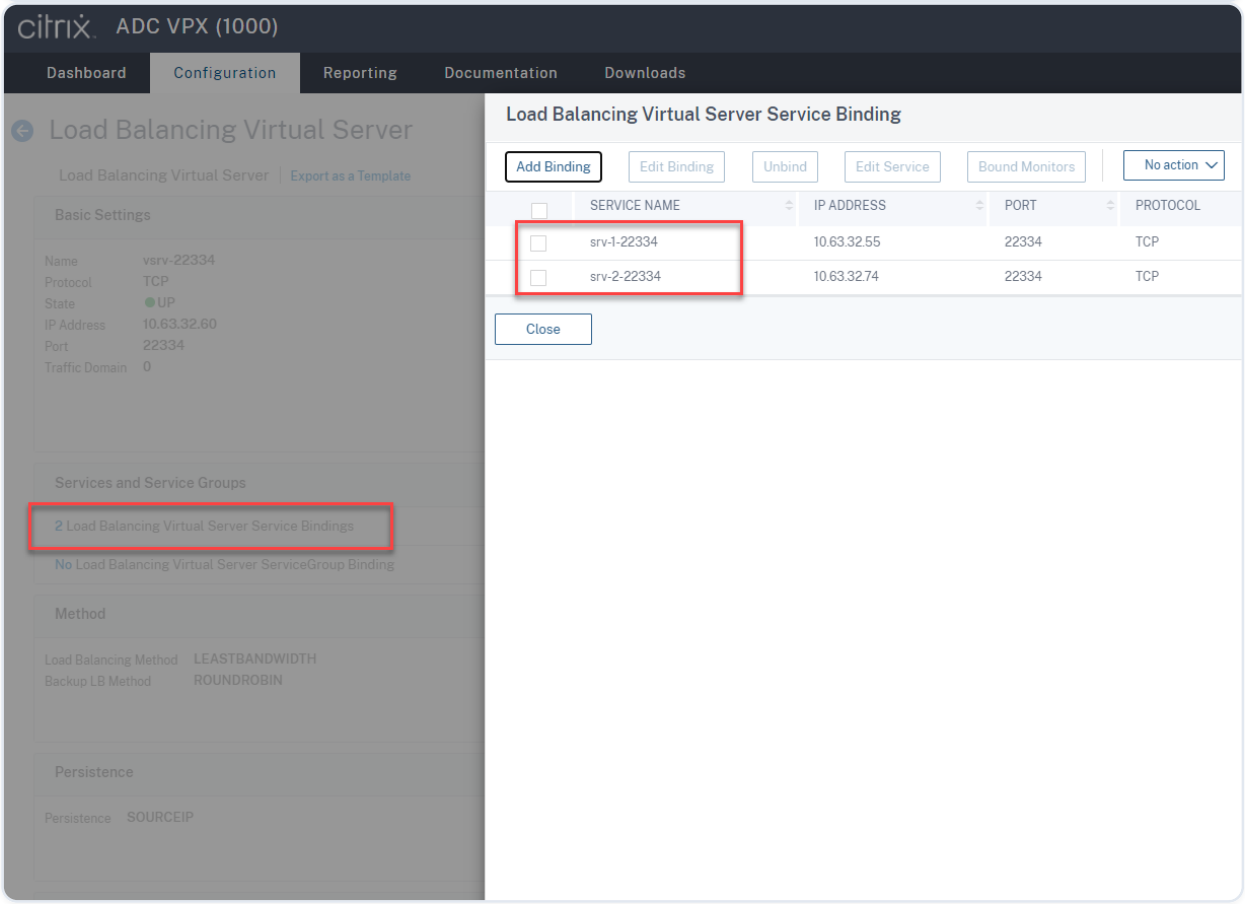


5. Share the Read/Write permission of the recording storage and restore folders, for example, `SessionRecording` and `SessionRecordingsRestored`, with the machine account of the new Session Recording server, for example, `LB\SRServer2$`. The dollar sign `$` is required.
6. Repeat Step 3 to add **load 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

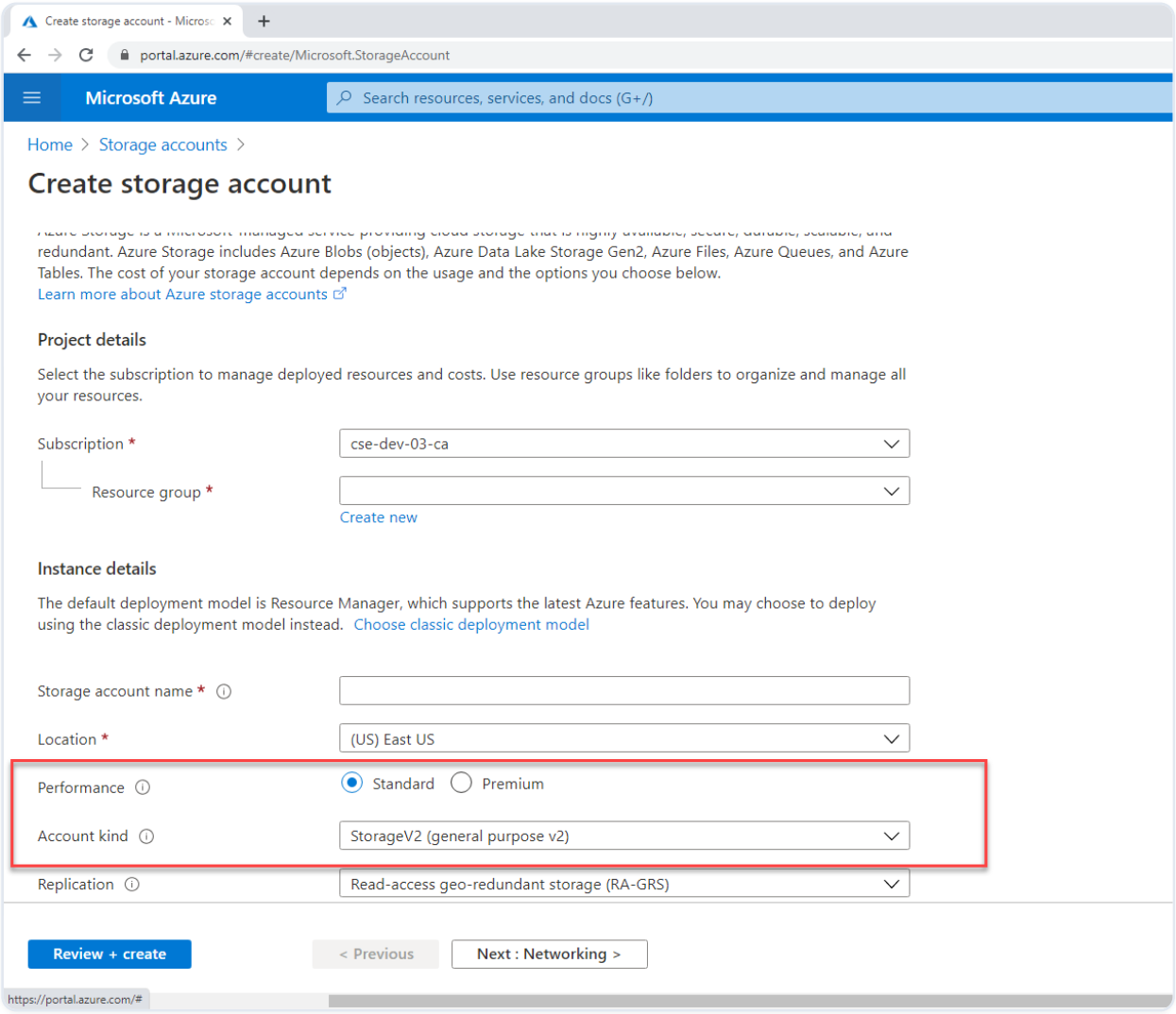
- You already have Citrix Virtual Apps and Desktops™ or Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) installed in Azure.
- You have an Azure account.

Step 1: Upload the Citrix Virtual Apps™ and Desktops installer to Azure

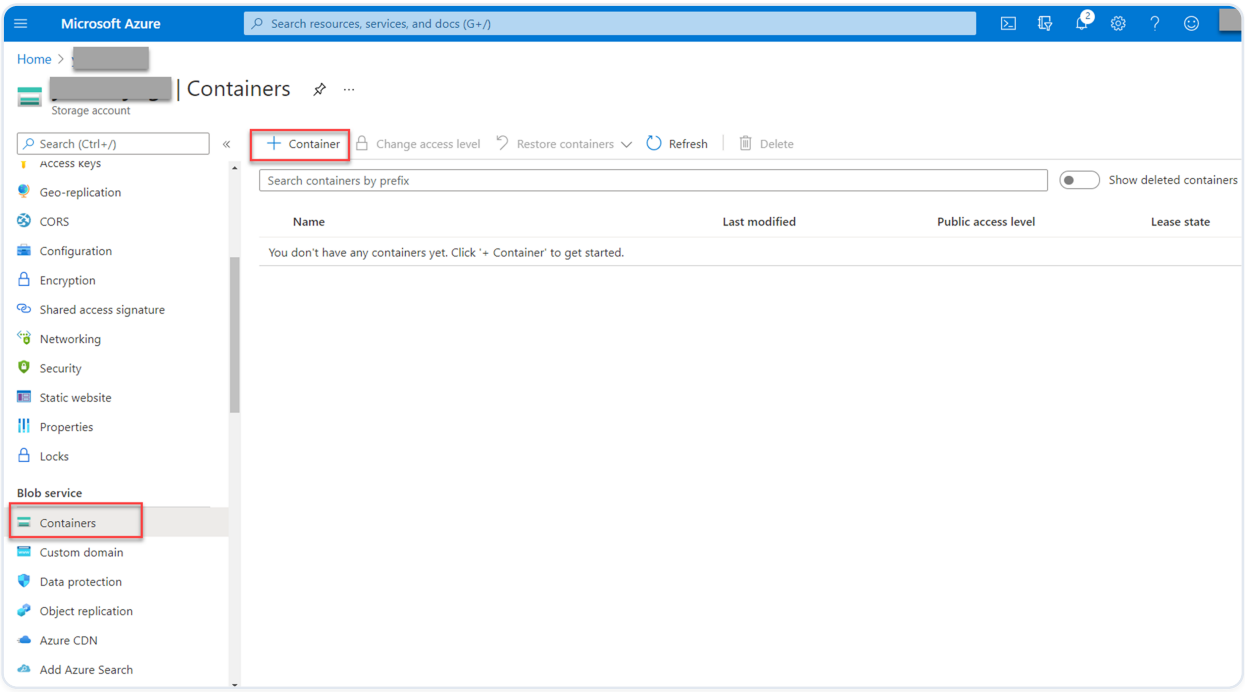
> **Note:**
>
> Skip Step 1 if you use your Citrix account credentials to access the Citrix Virtual Apps and Desktops download page and download the product ISO file to a VM in Azure.

1. In the Azure portal, create a **general-purpose v2** storage account and accept the default performance tier, **Standard**.

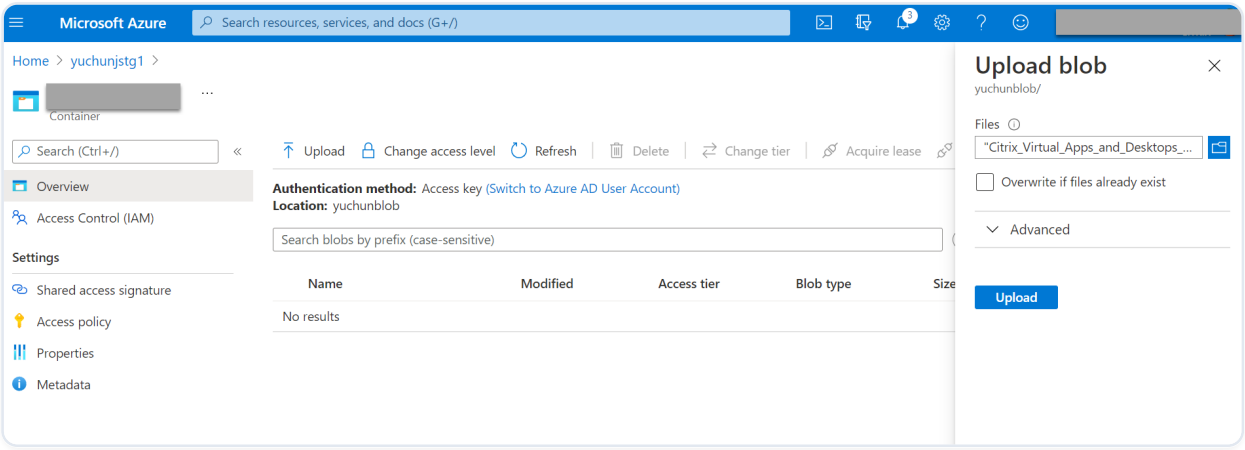
   All access to Azure Storage goes through a storage account.



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.

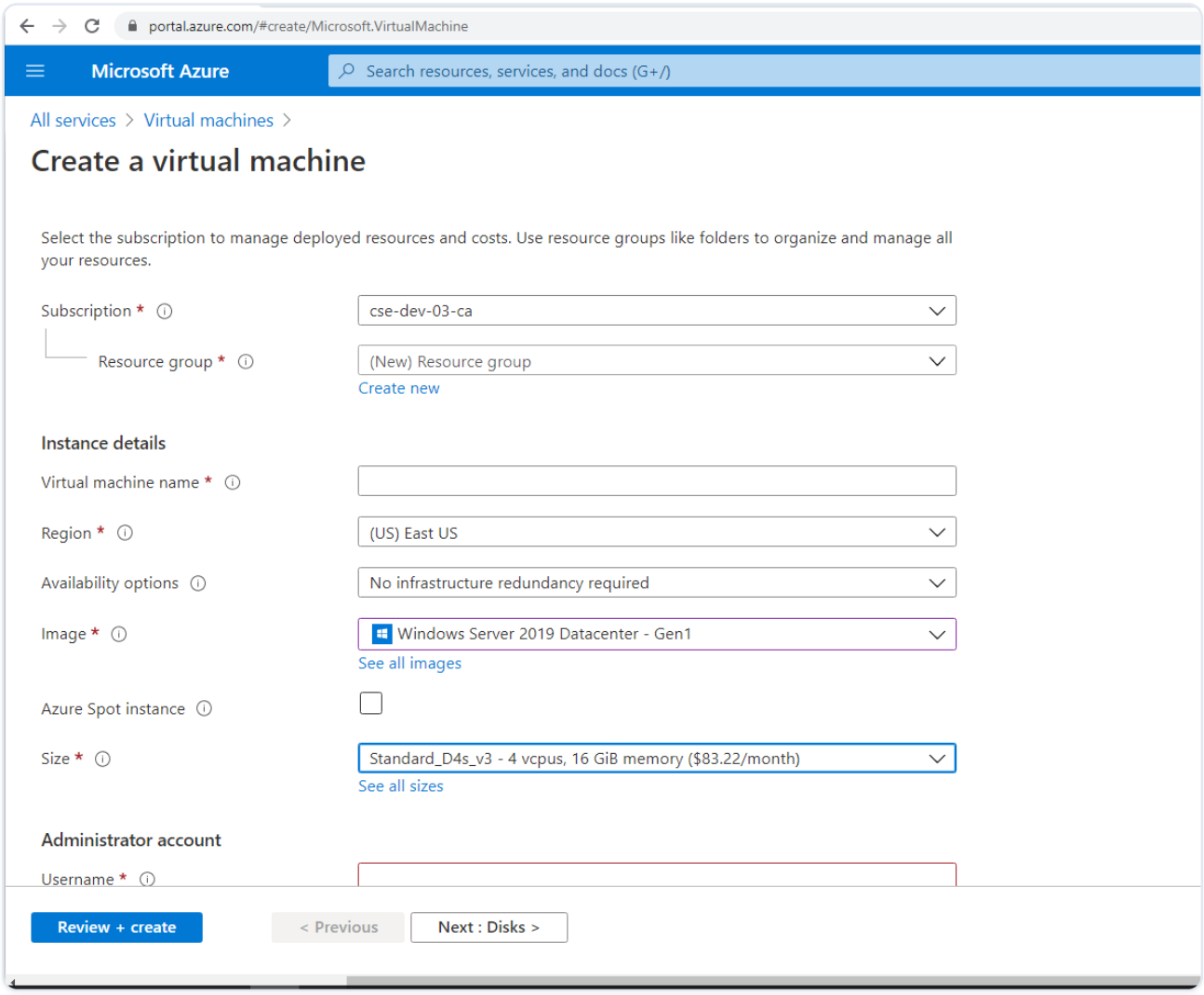


Step 2: Create a SQL managed instance in the Azure portal

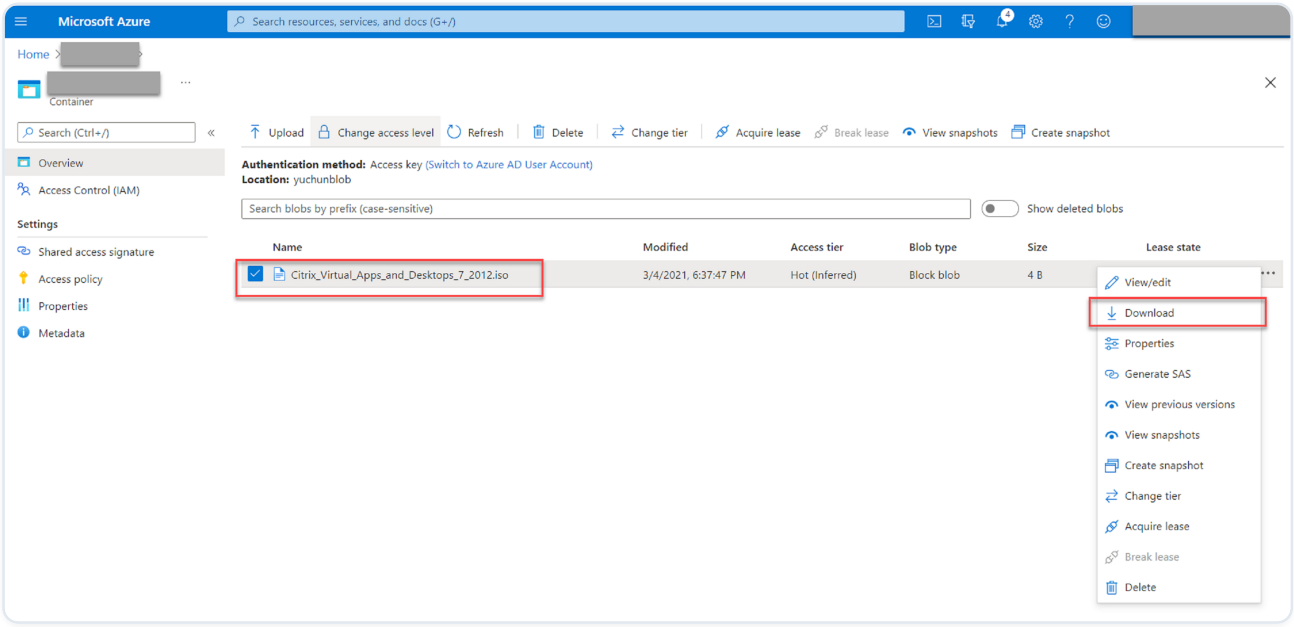
For more information, see Create an Azure SQL Managed Instance.

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.

Note:

- The recording sizes in the preceding table are examples, not product limits. The amount of data that a session generates varies greatly depending on what is being recorded. Screen resolution, color depth, graphics mode, and how graphically intense the published applications are all have an impact. A session in which a user runs CAD, mapping, or video applications can produce a recording that is several times larger than a session in which the user only sends and receives emails in Outlook. Whether you enable lossy screen recording also changes the figure significantly.
- Before you fix the share type and the quota, record a representative pilot group of your own users for a few days, measure the average MB/hour that your workloads actually produce, and size the file share from that measurement. Recalculate the quota whenever your published applications, session recording policies, or retention period change. A quota that is too small stops recordings from being stored; a quota that is too large costs more than it needs to. For more information about estimating your data rates, see Scalability considerations.

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`.

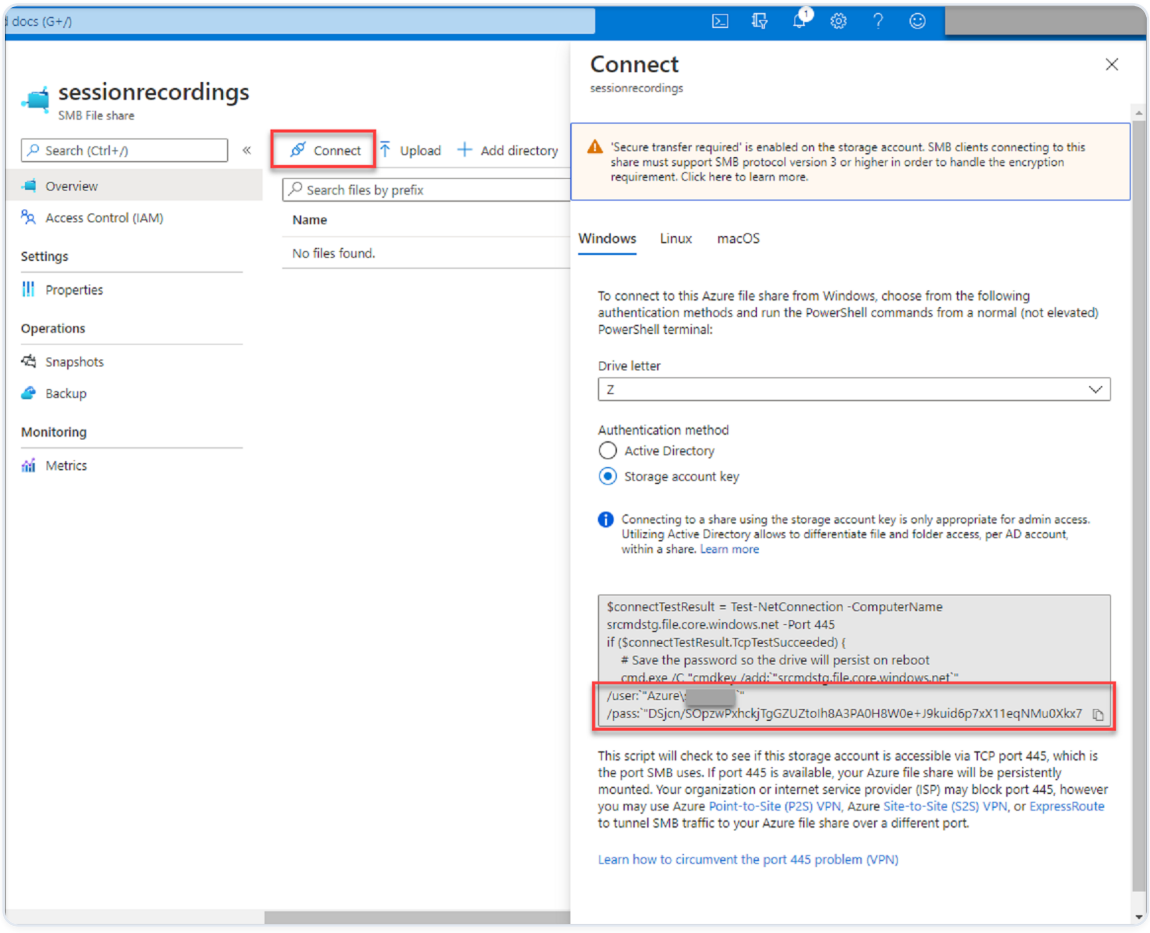
b. Run the **SsRecUtils.exe -AddAzureFiles <storageAccountName\> <fileShareName\> <accesskey\>** command.

Where,

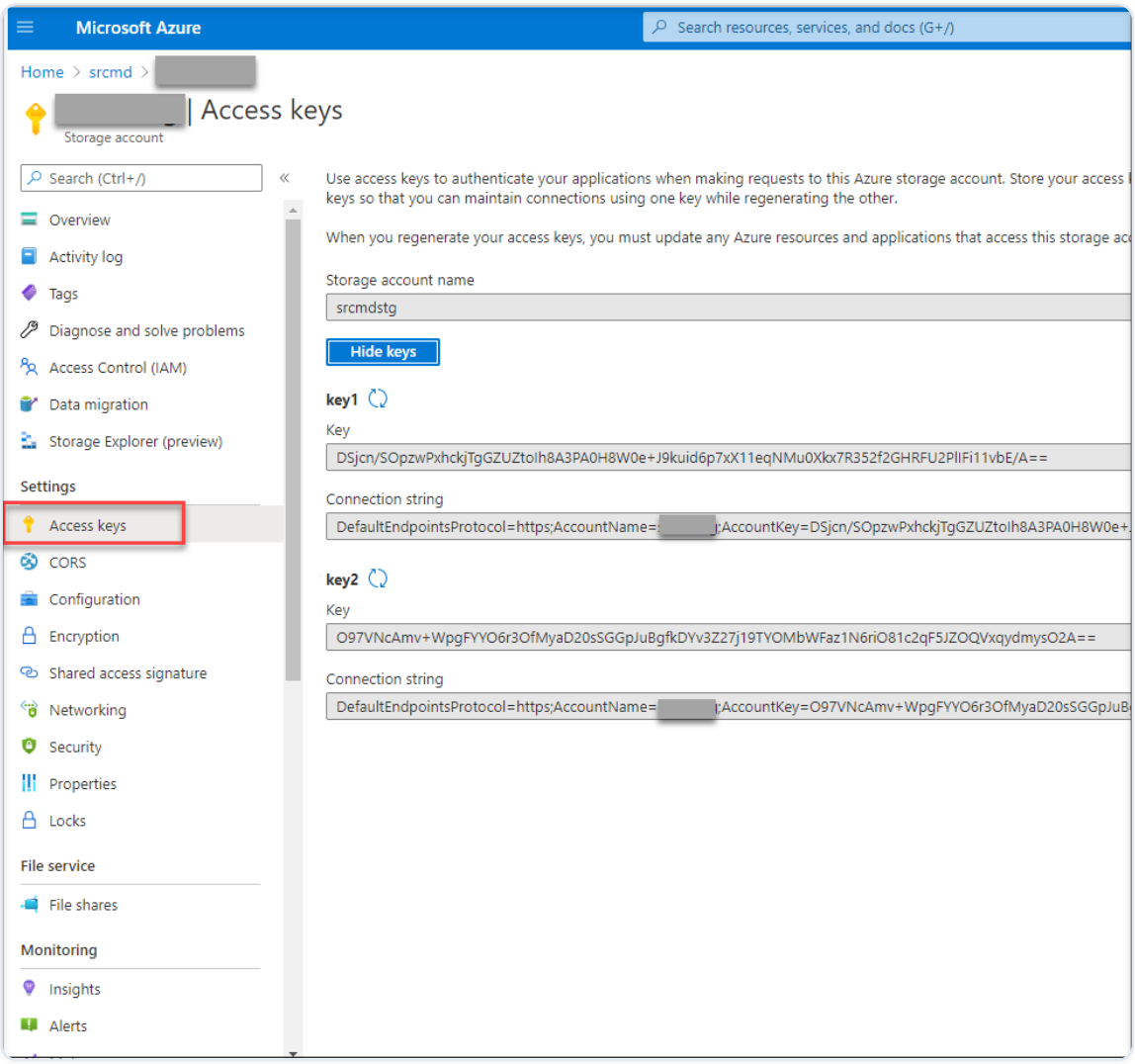
- **<storageaccountname\>** is the name of your storage account in Azure.
- **<filessharename\>** is the name of the file share contained within your storage account.
- **<accesskey\>** is your storage account key that can be used to access the file share.

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.



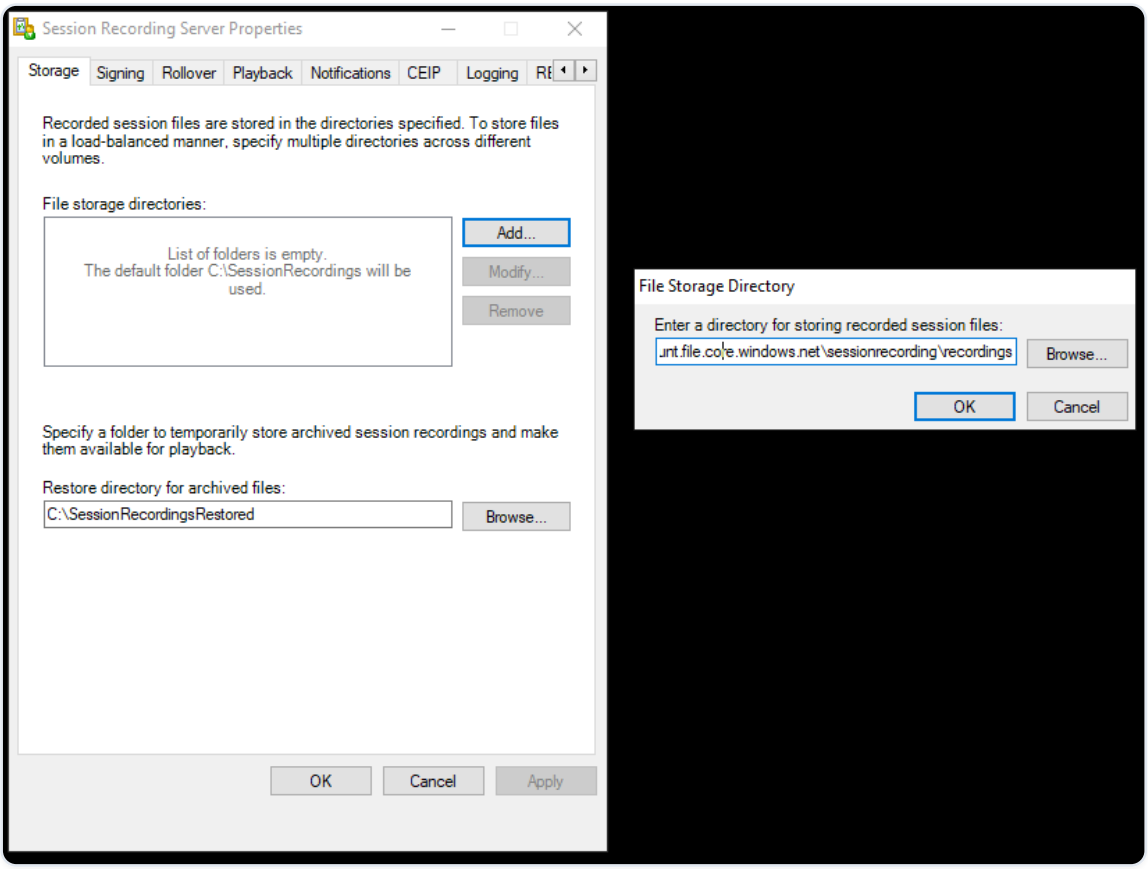
c. Mount the Azure file share to the host where you installed the Session Recording server.

   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.

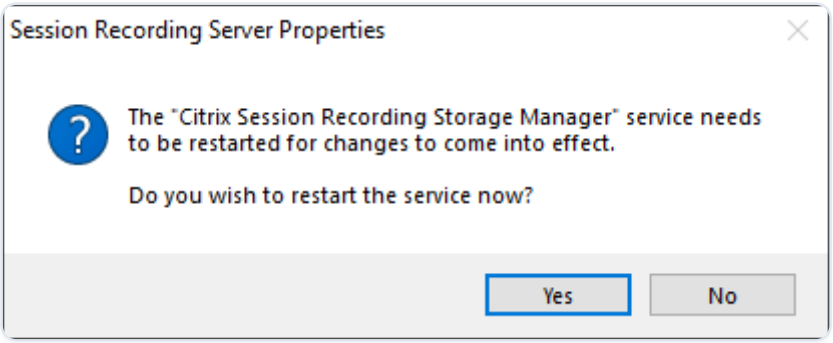


iv. Click **OK** in the **File Storage Directory** dialog box.

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.

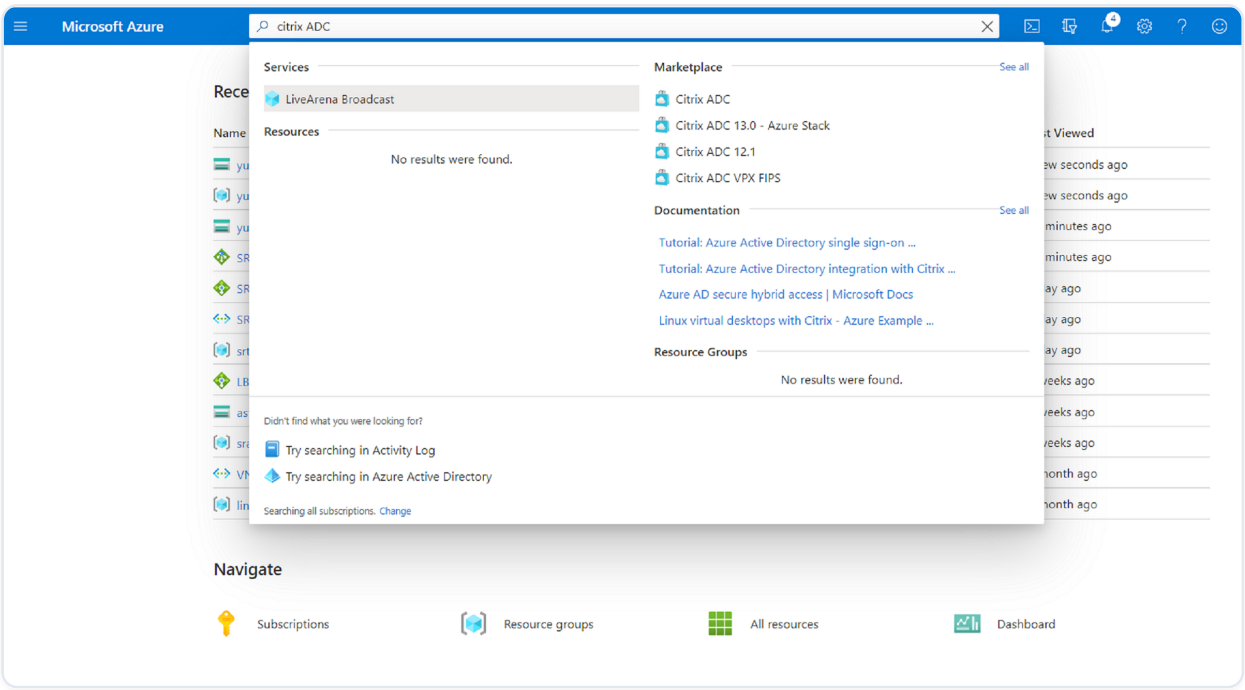


Step 7: Add a load balancer

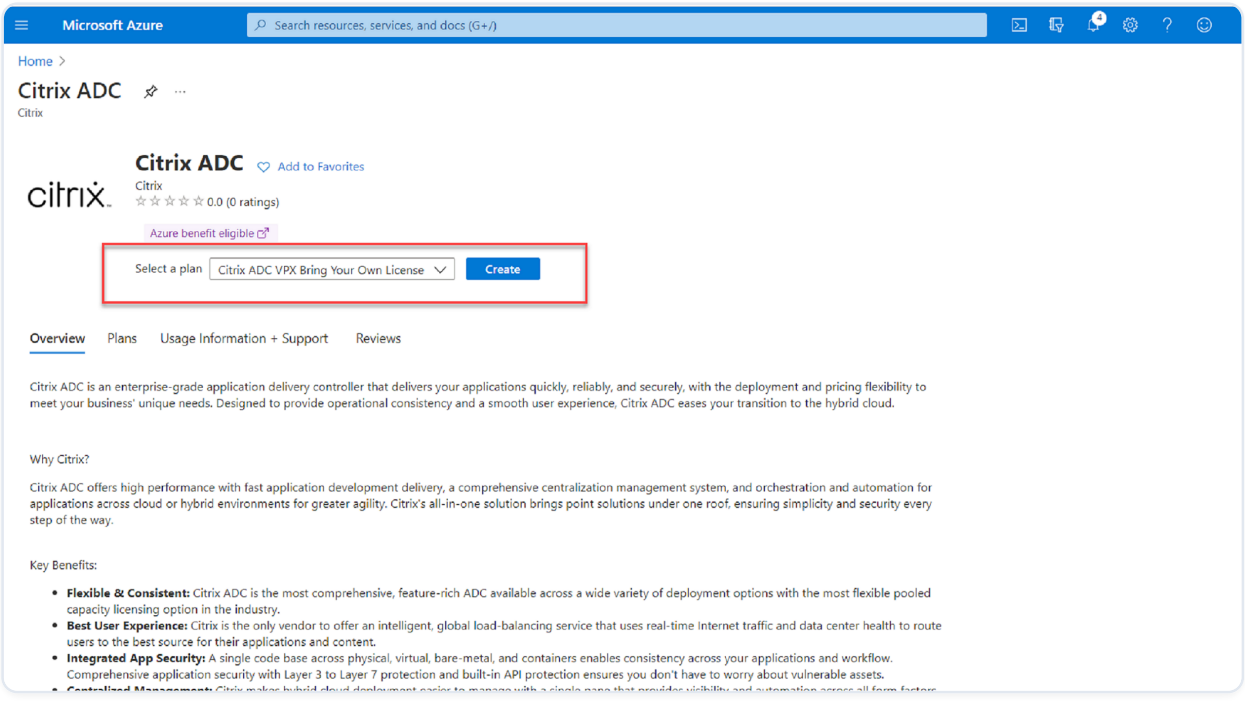
If there is more than one Session Recording server, we recommend you add a load balancer in front of them. Azure offers many options to load-balance traffic requests. This section walks you through the process of creating Citrix ADC, Azure Load Balancer, and Azure Application Gateway in Azure.

Option 1: Create a Citrix ADC VPX instance in Azure

1. In the Azure portal, type Citrix ADC in the search box.

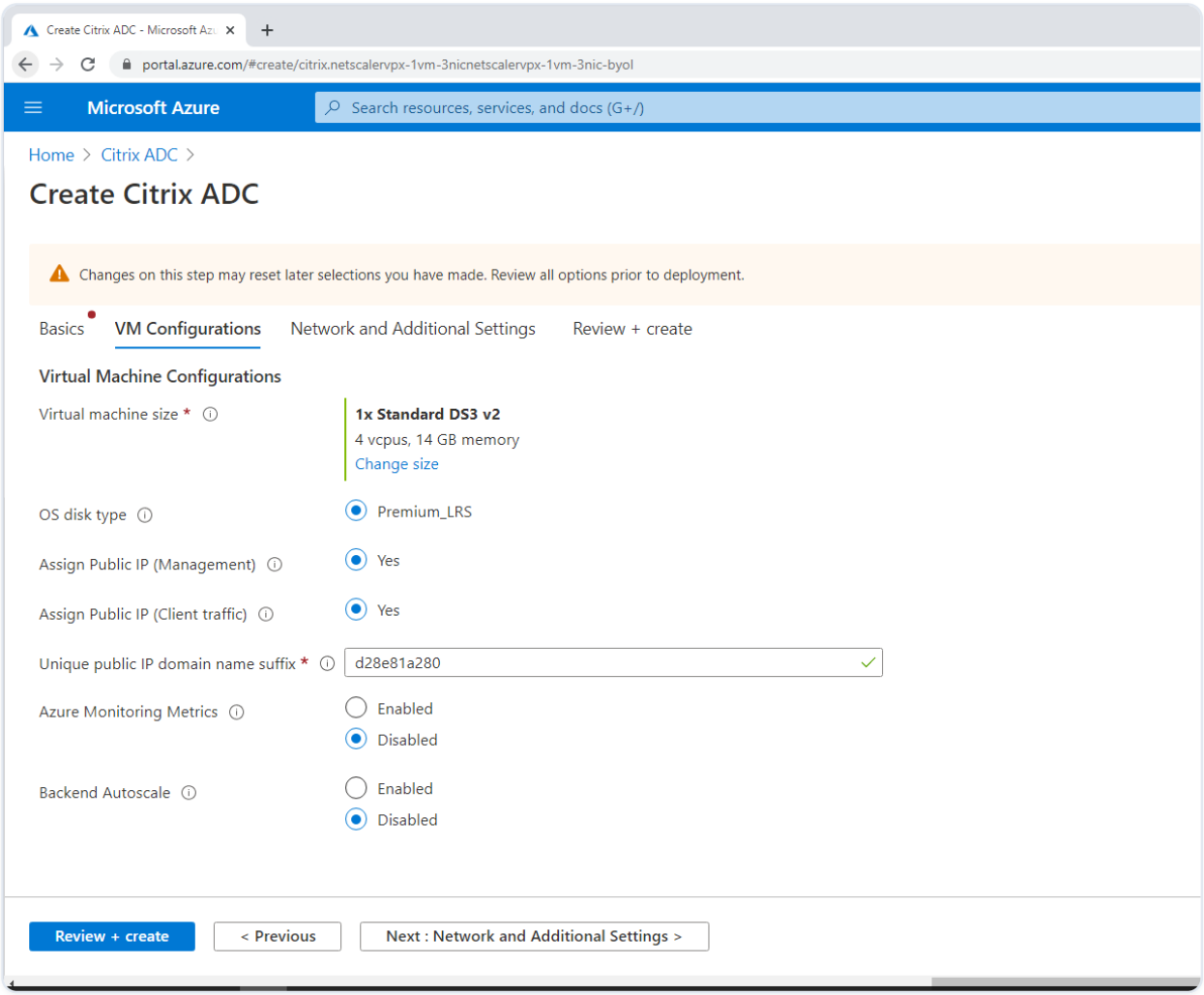


2. Choose the **Citrix ADC VPX Bring Your Own License** plan and then click **Create**.



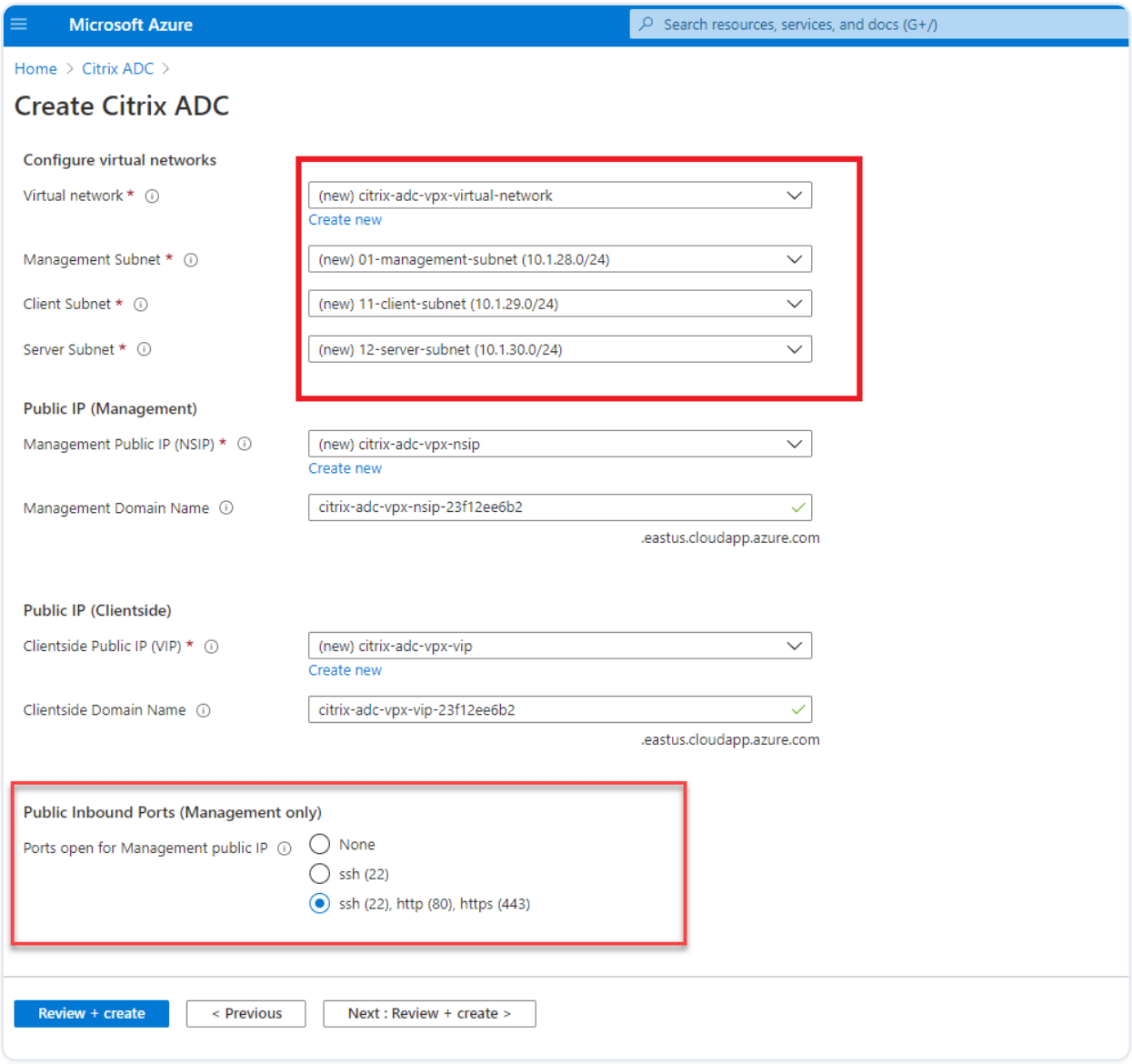
3. Select or create a resource group and set the other settings on the **Basics** tab.

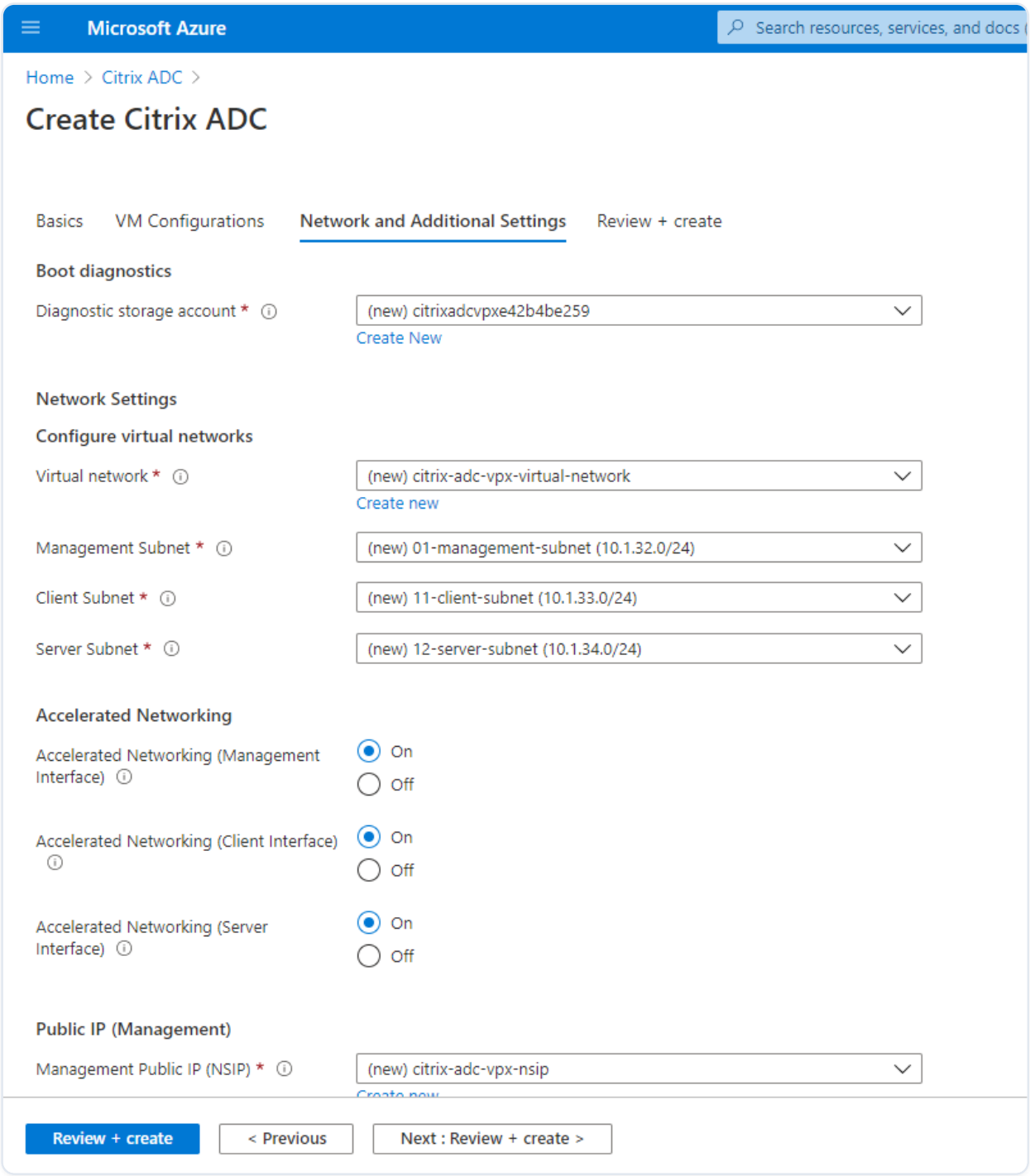
4. Set VM configurations.



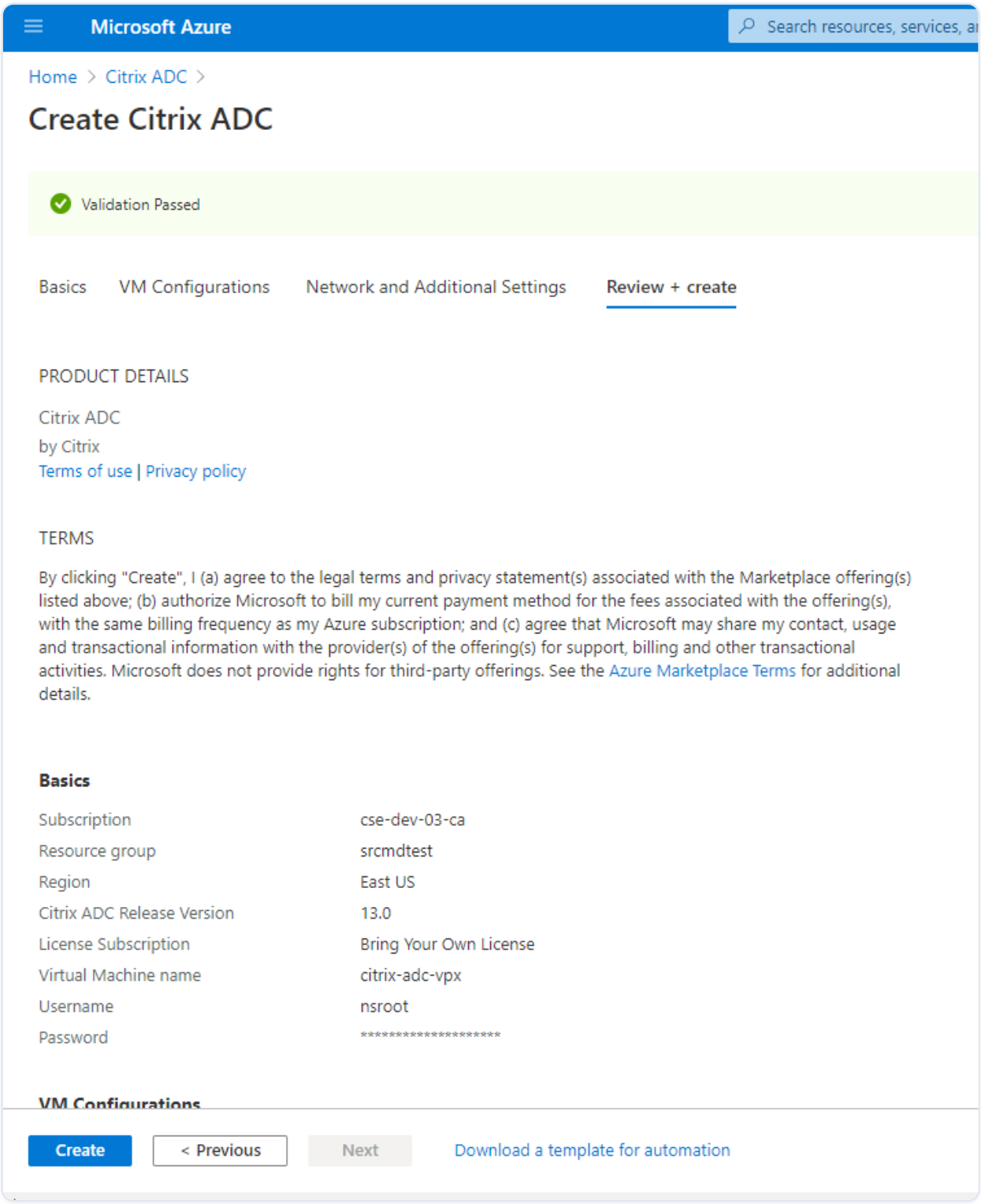
5. Check and modify network settings if necessary. Choose **ssh (22), http (80), https (443)** for public inbound ports.

   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.

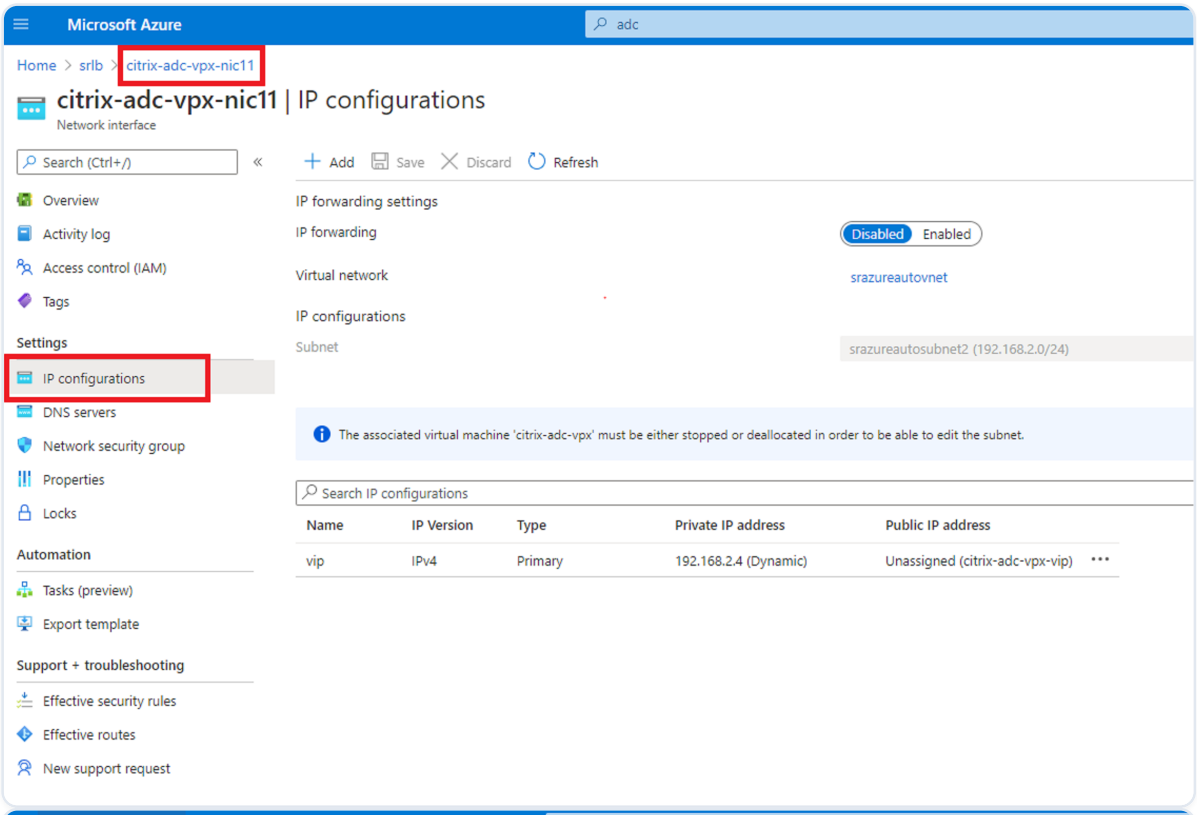


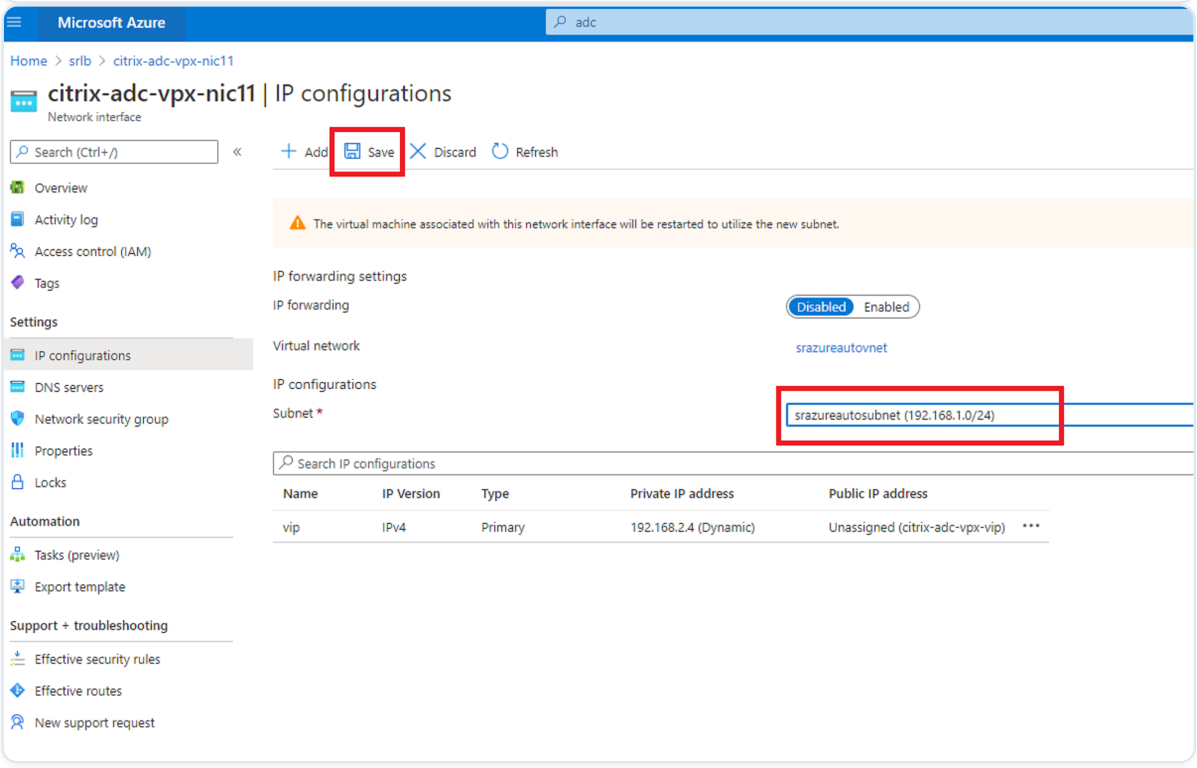
7. Set the subnet IP (SNIP) address and the Citrix ADC VIP address to be on the same subnet.

   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.

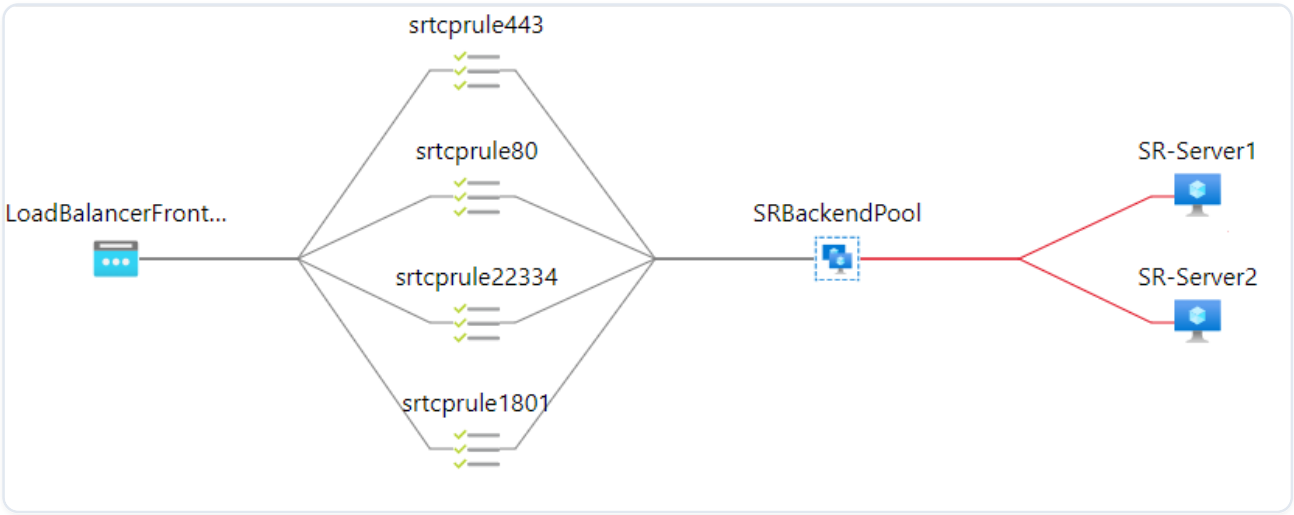




c. Start the **citrix-adc-vpx** virtual machine

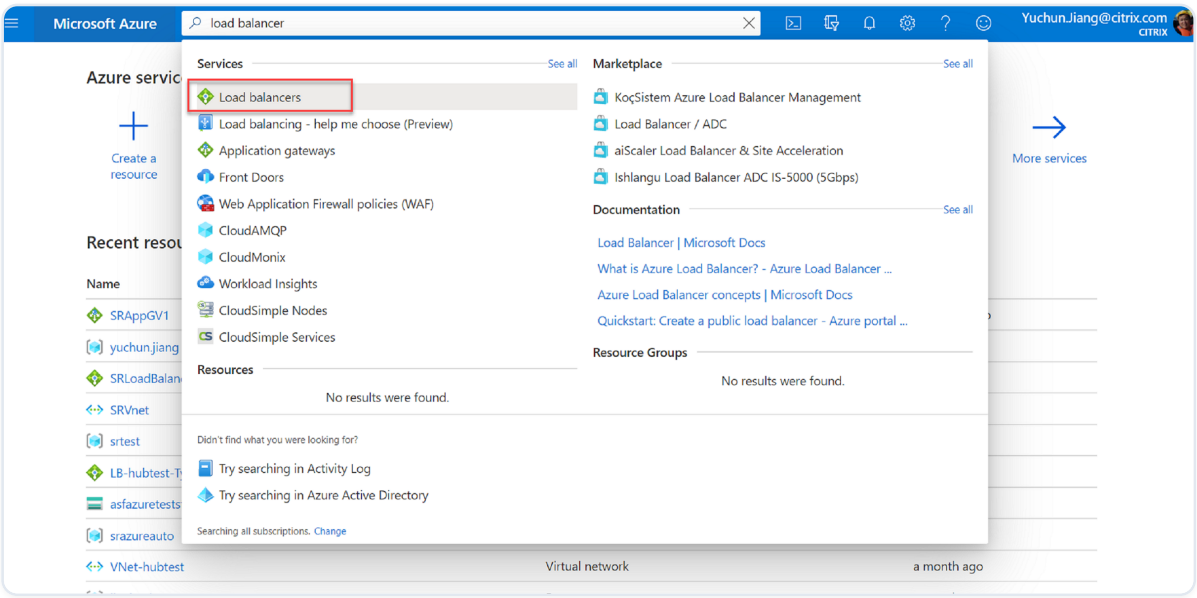
Option 2: Create an Azure load balancer

Azure Load Balancer is a TCP passthrough service. The following diagram shows load balancing through TCP passthrough.



1. Create an Azure load balancer.

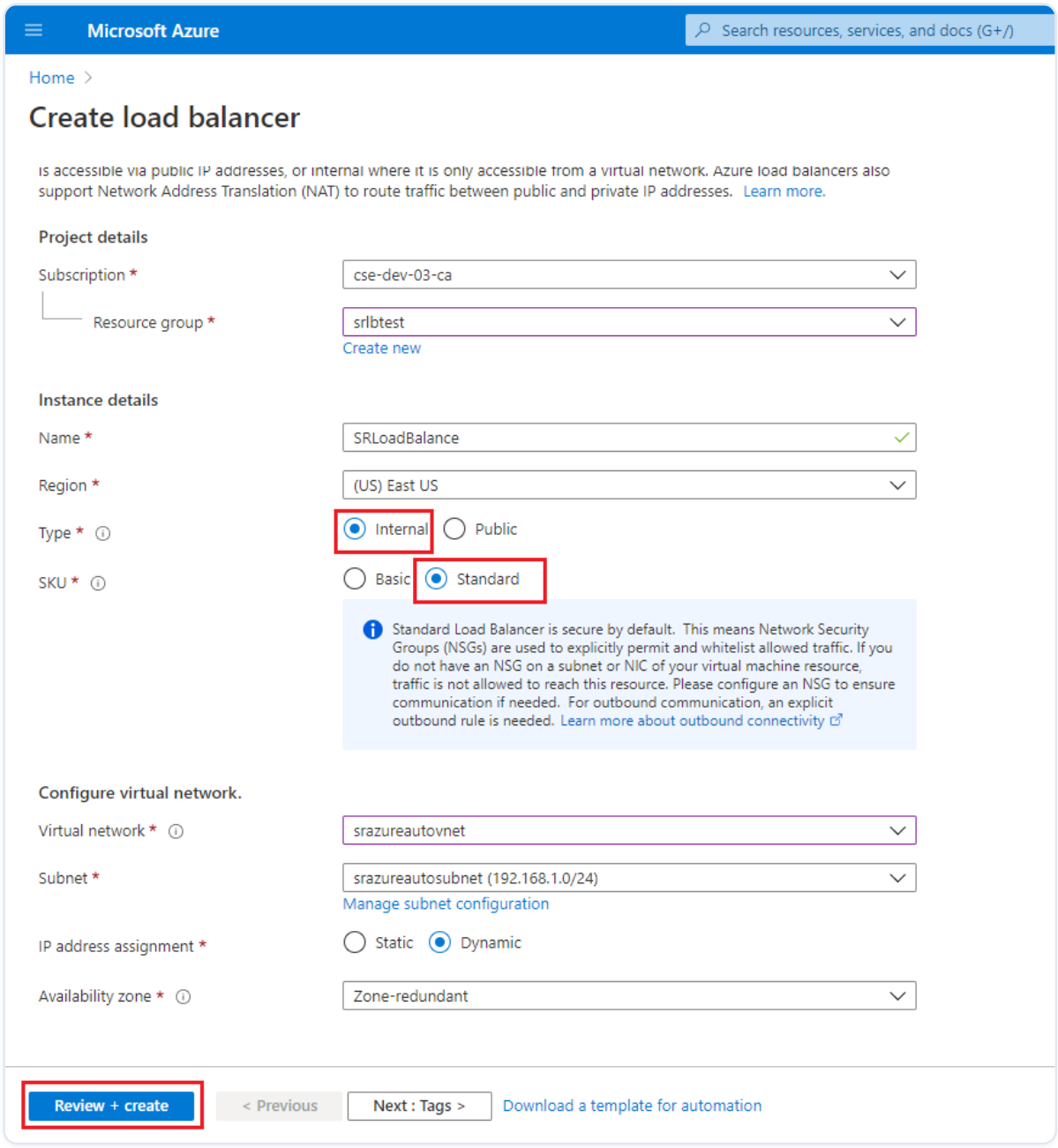
   a. Search in the Azure portal and select **Load Balancers** from the **Marketplace**.



   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**.

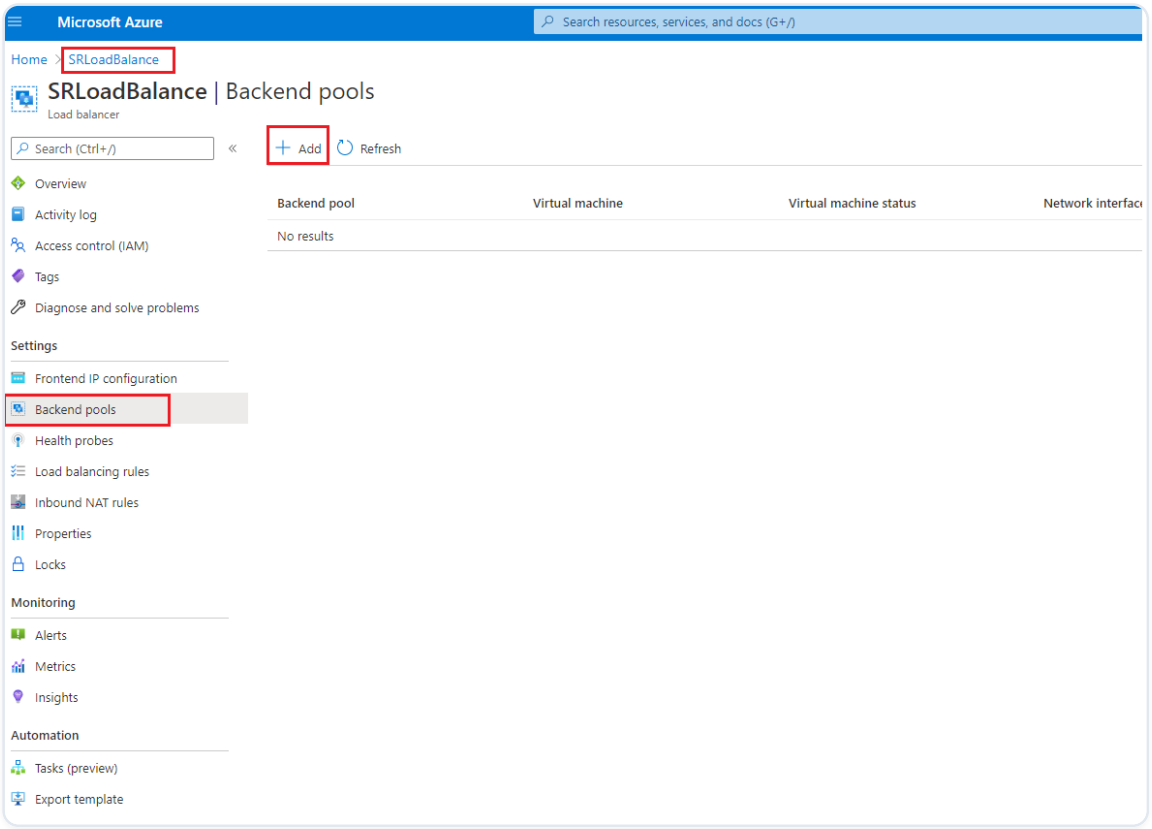
SETTING	VALUE
Type	Select **Internal**.
SKU	Select **Standard**
Virtual network	For example, select **srazureautovnet** created earlier.
Subnet	For example, select **srazureautosubnet** created earlier.
IP address assignment	Select **Dynamic**.
Availability zone	Select **Zone-redundant**.



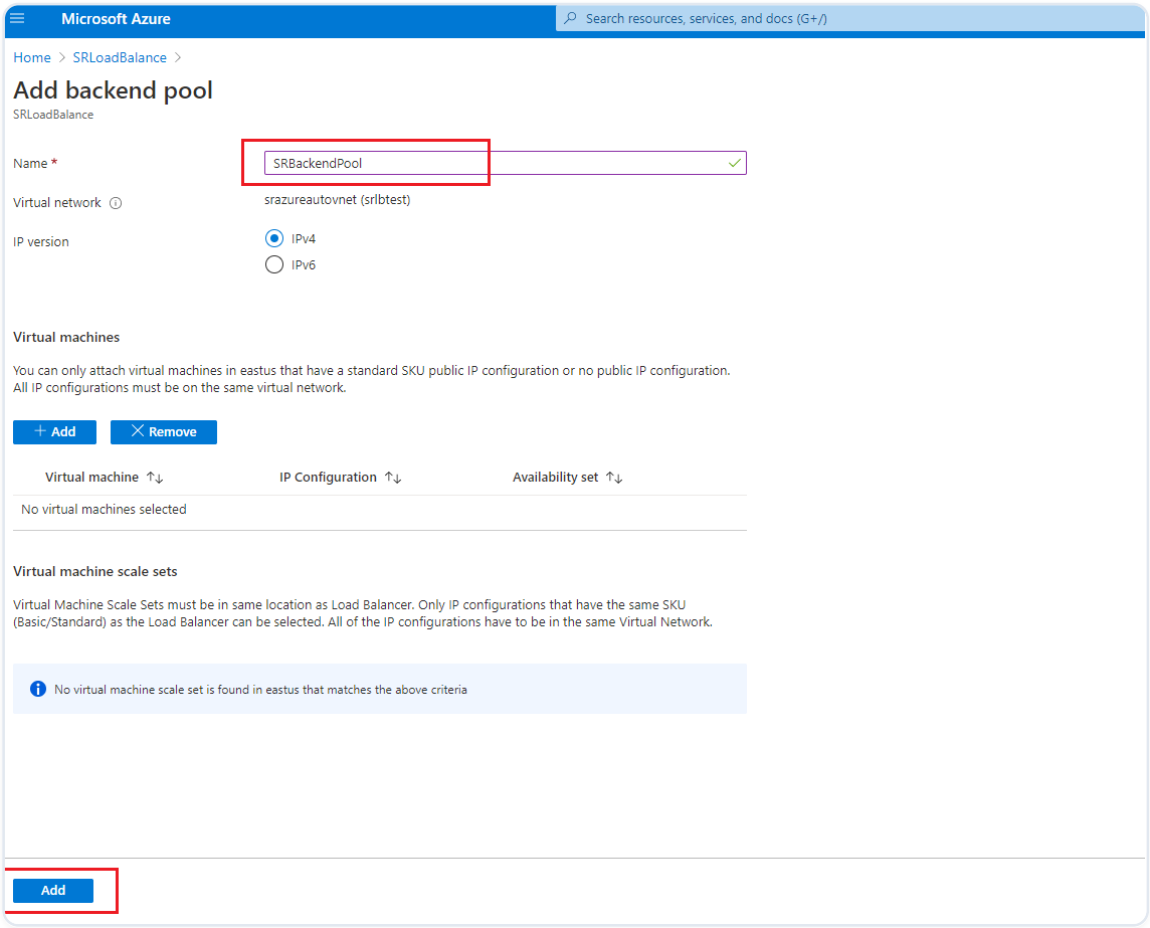
b. Add load balancer resources, including a back-end pool, health probes, and load balancing rules.

- 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.

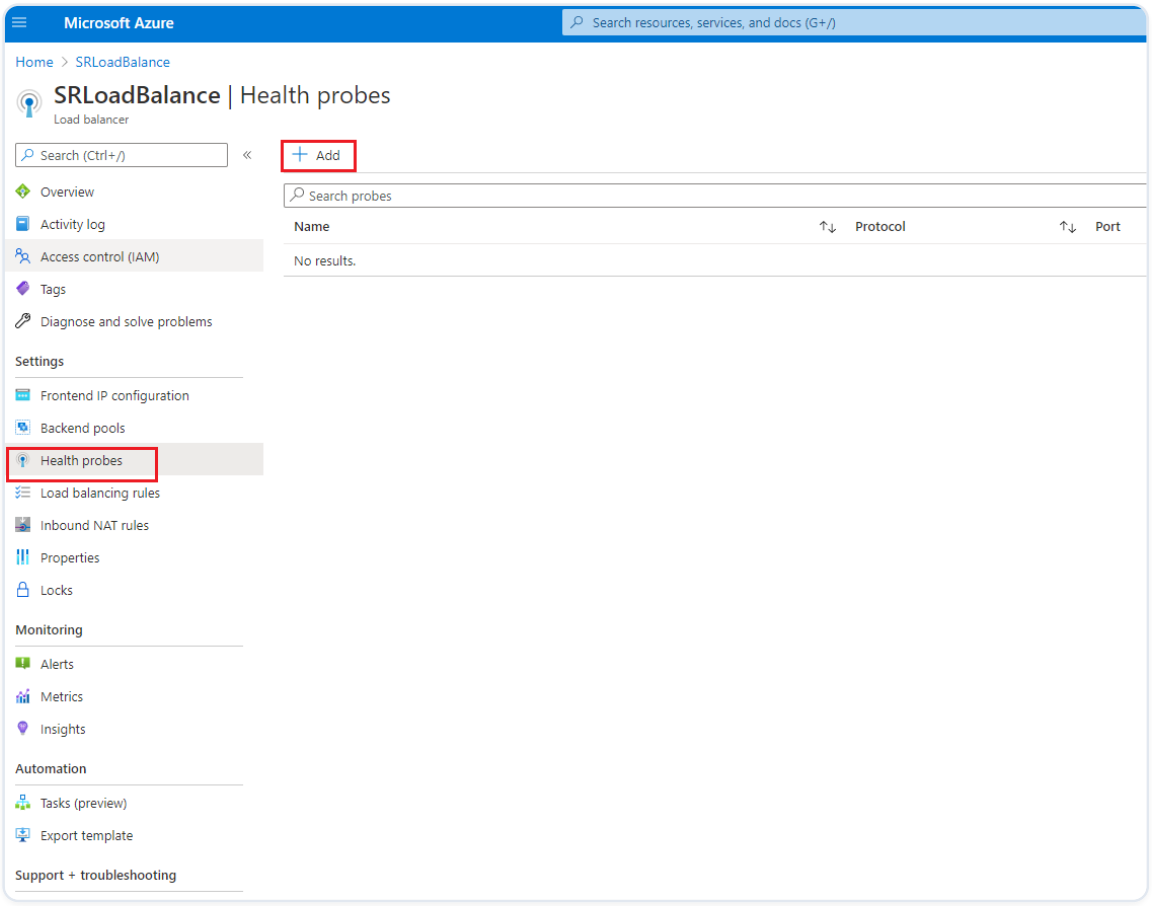


Enter a name for the new back-end pool and then click **Add**.

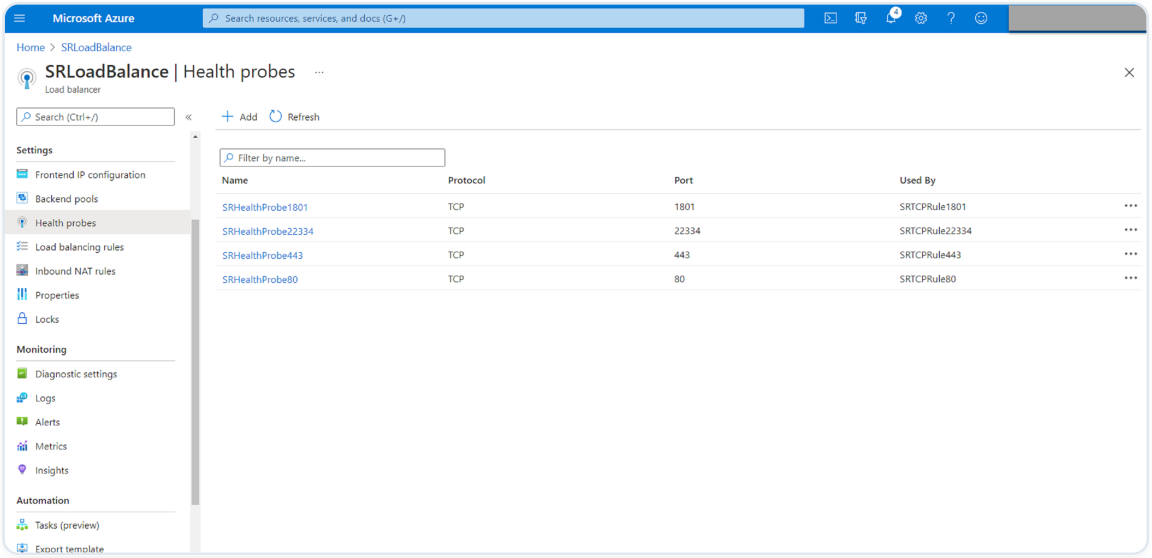


- Add health probes.

Select the load balancer you created from the resources list and then click **Health probes** in the left navigation.



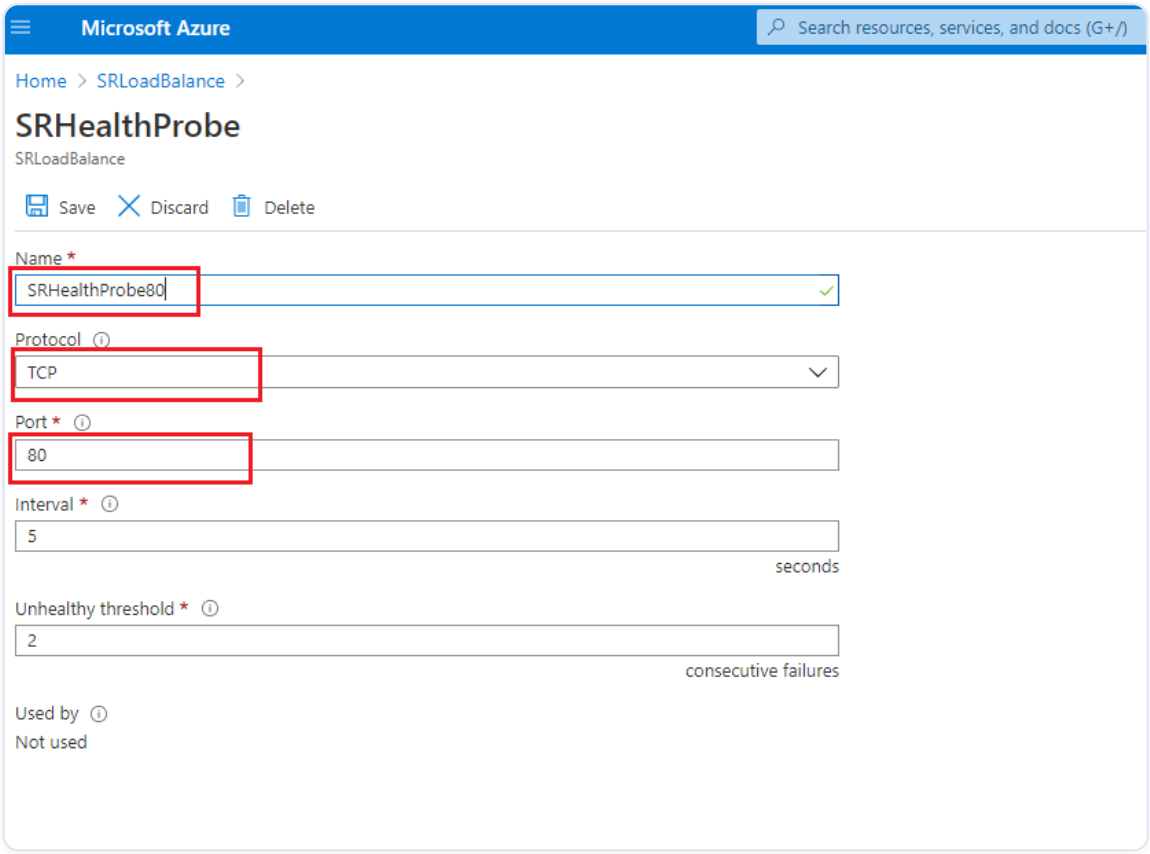
Click **Add** to add health probes on ports 80, 22334, 1801, and 443.



For example, use the following settings to create a health probe on port 80.

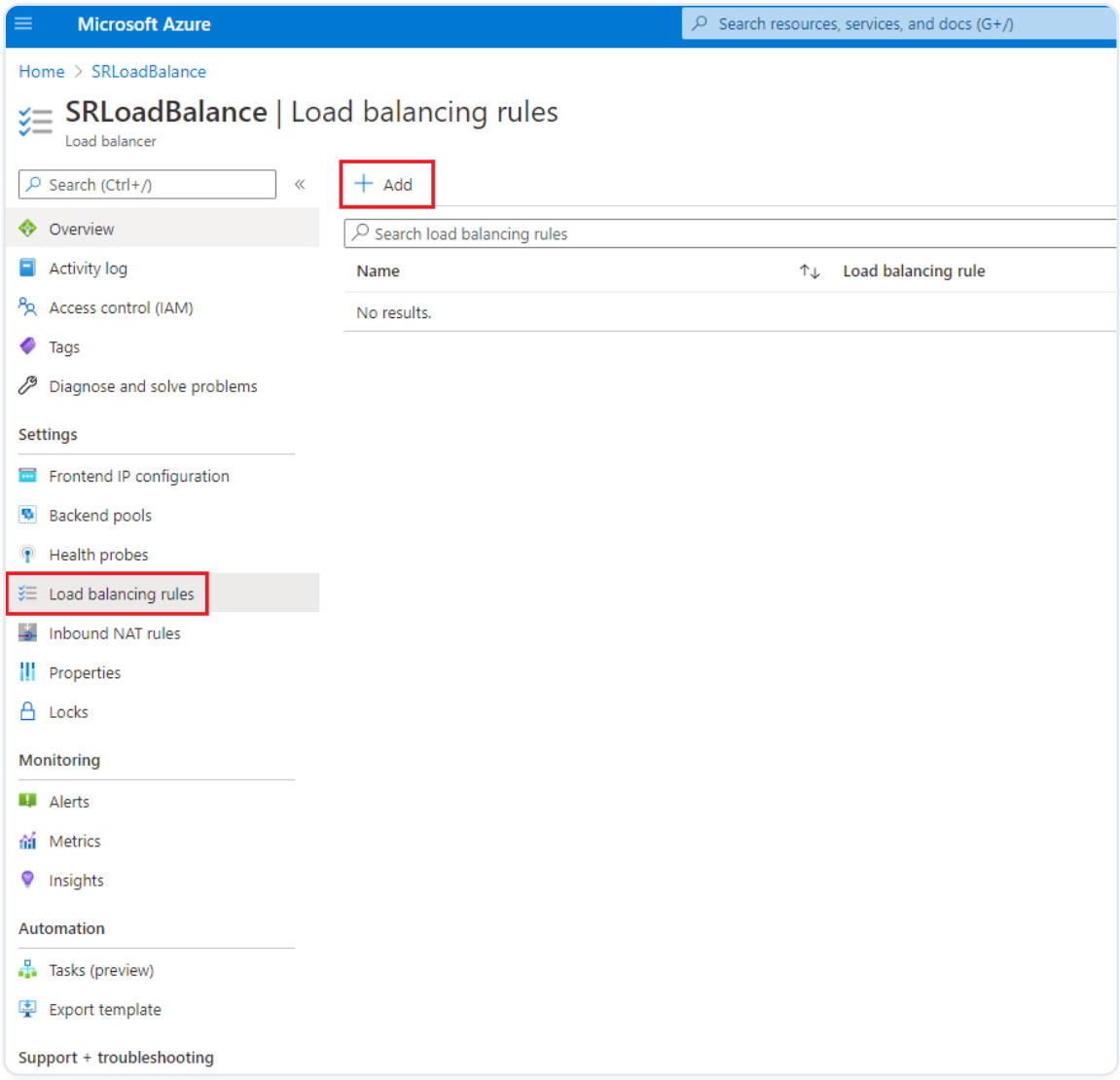
SETTING	VALUE
Name	Enter **SRHealthProbe80**.

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.

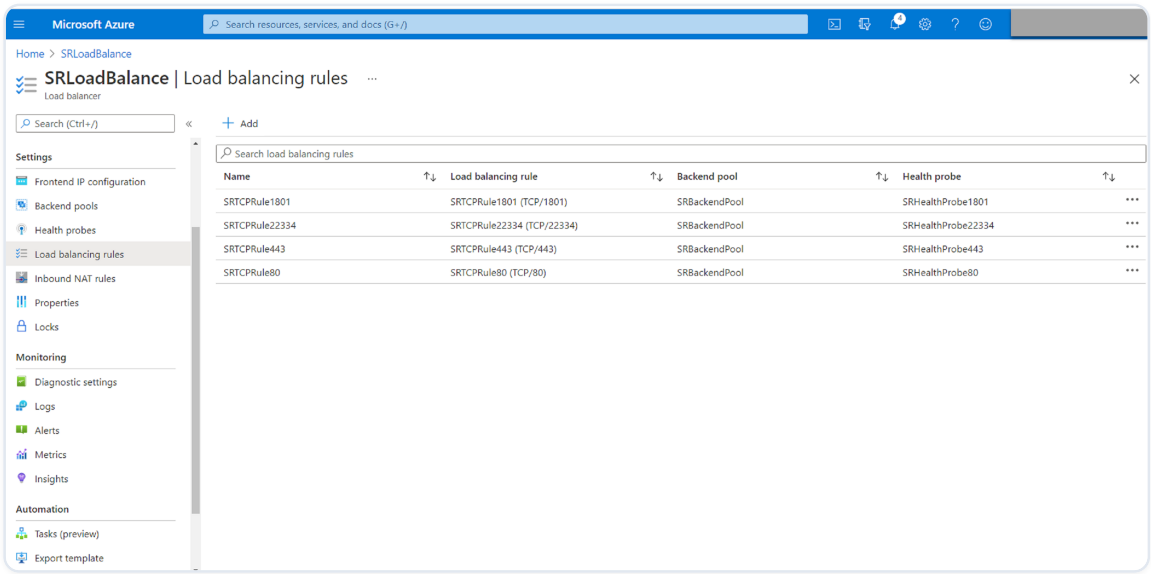


- Add a load balancing rule.

  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.

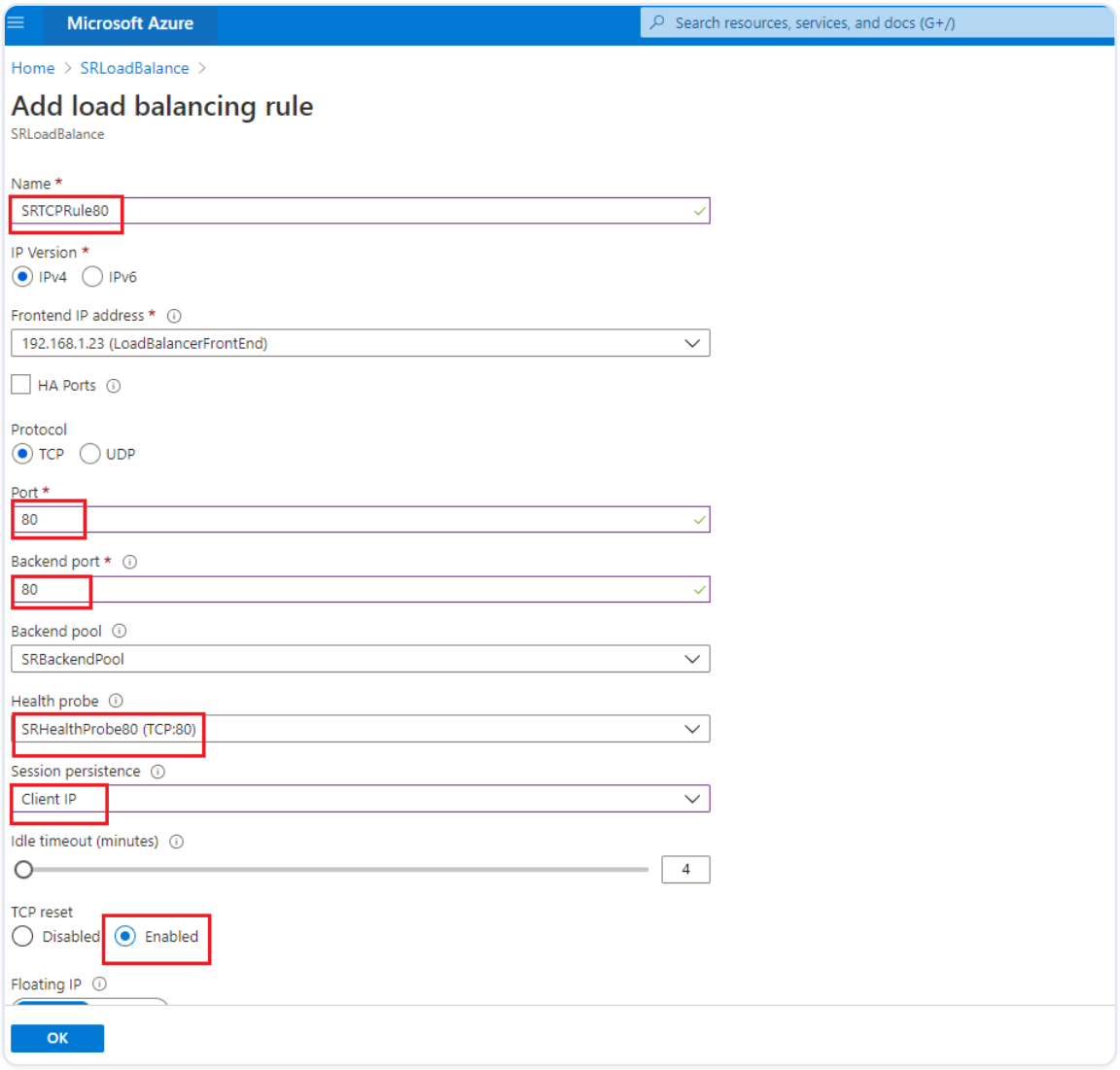


Click **Add** to add load balancing rules for ports 80, 22334, 1801, and 443.

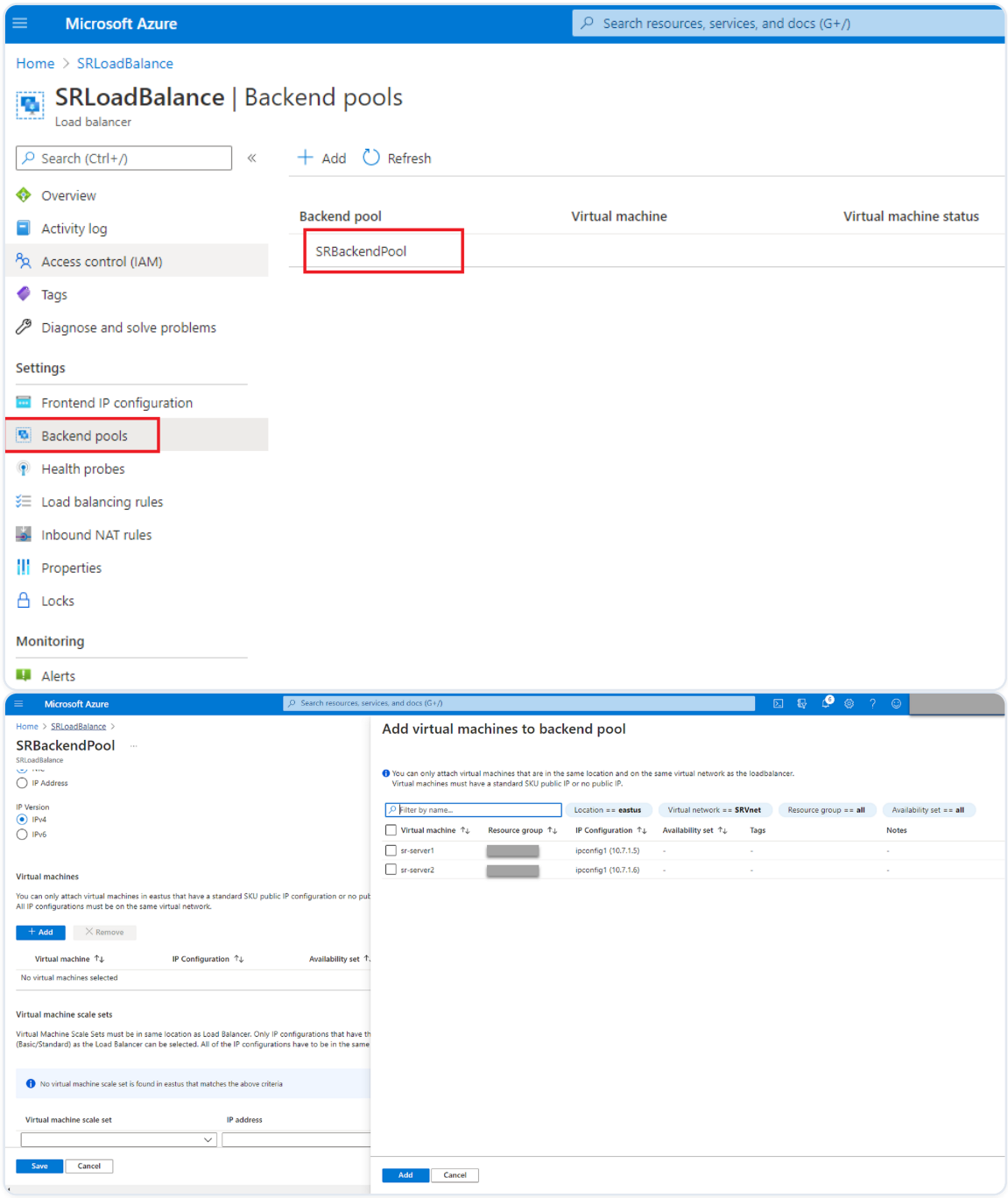


For example, use the following settings to create a load balancing rule for port 80.

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**.

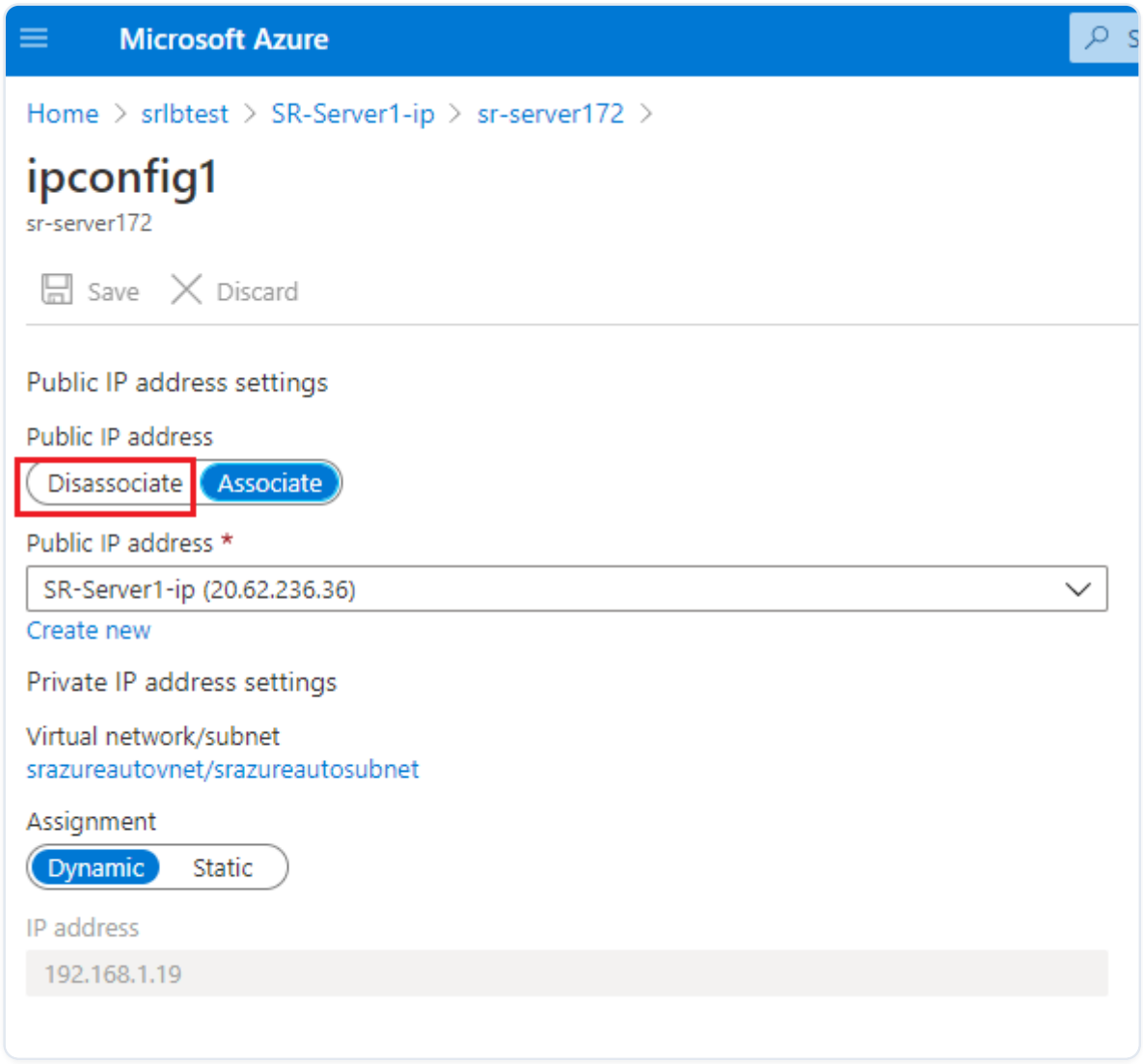


- Add the Azure VMs where the Session Recording server is installed to the back-end pool.



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:**

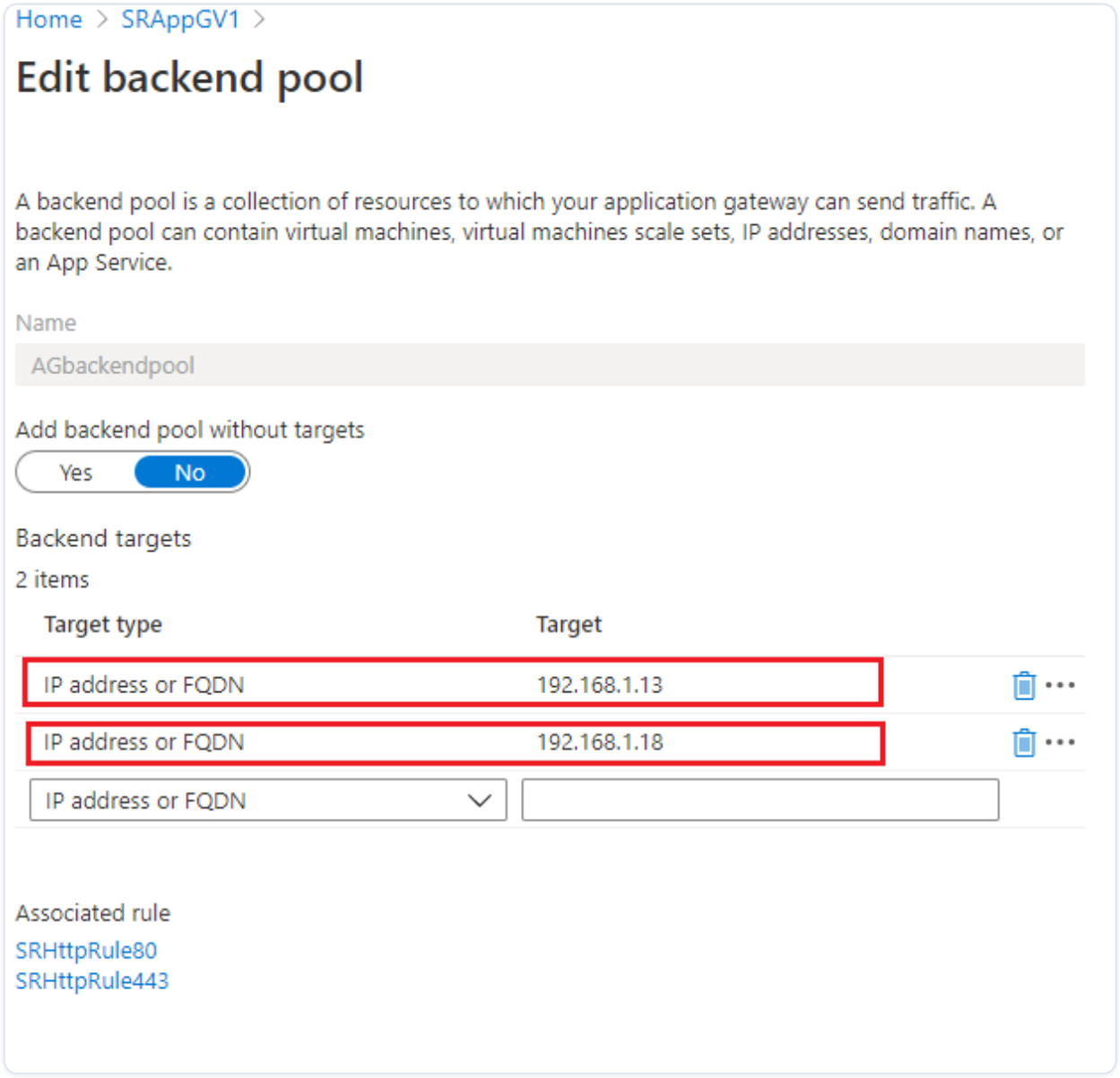
> Application Gateway V2 does not support routing requests through an NTLM-enabled proxy.

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.

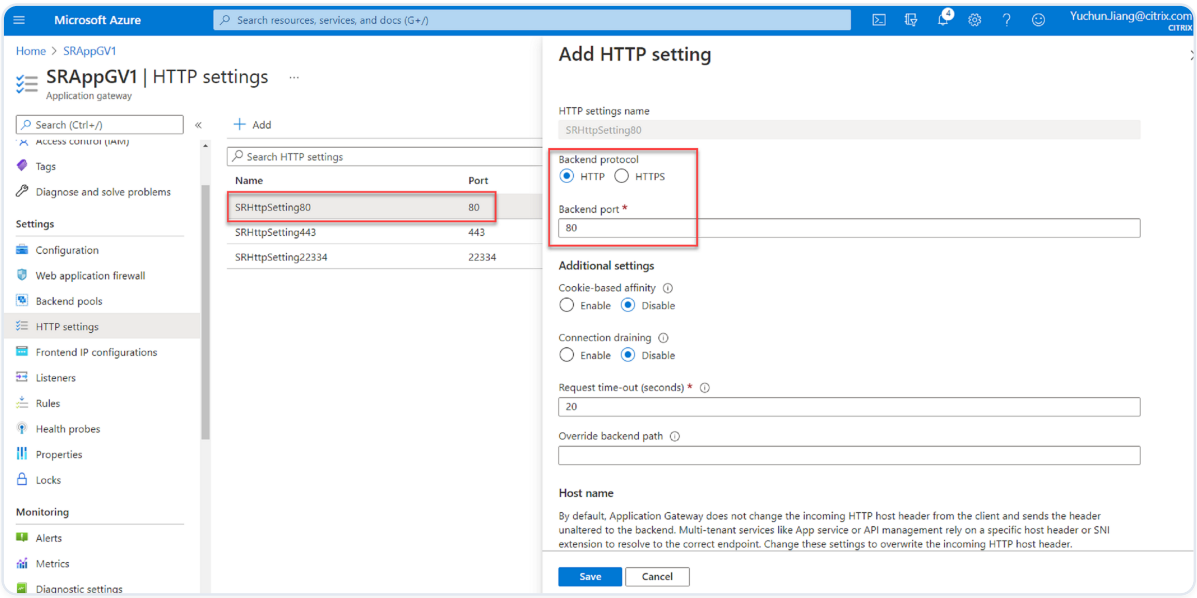
2. Add a back-end pool.



3. Create HTTP settings.

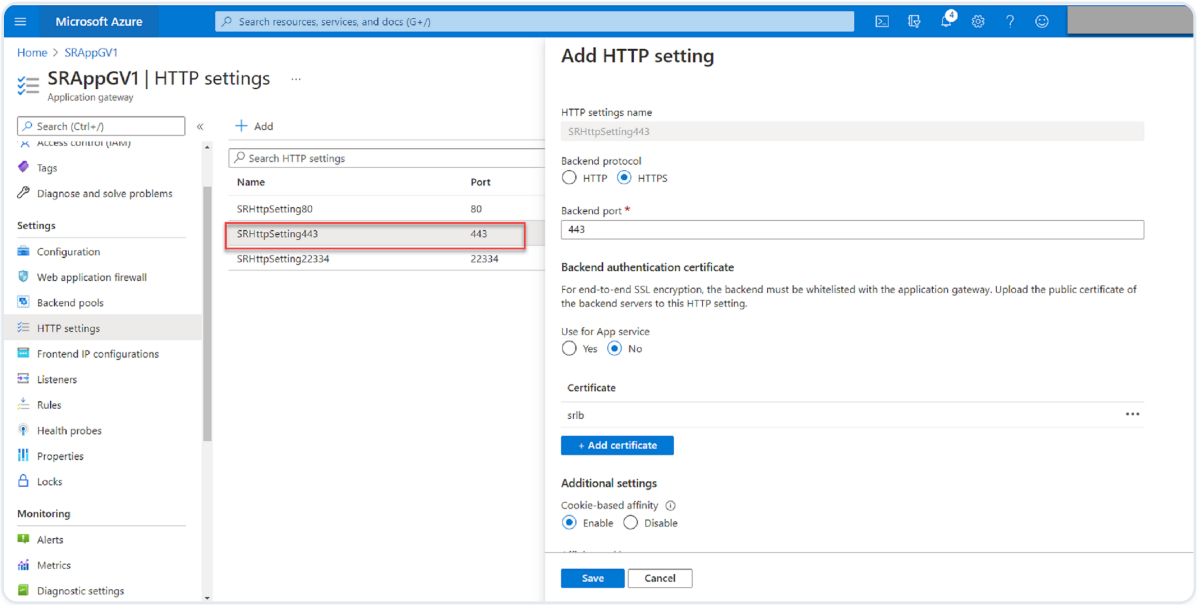
   Azure Application Gateway supports both HTTP and HTTPS for routing requests to back-end servers. Create HTTP settings for ports 80, 443, and 22334.

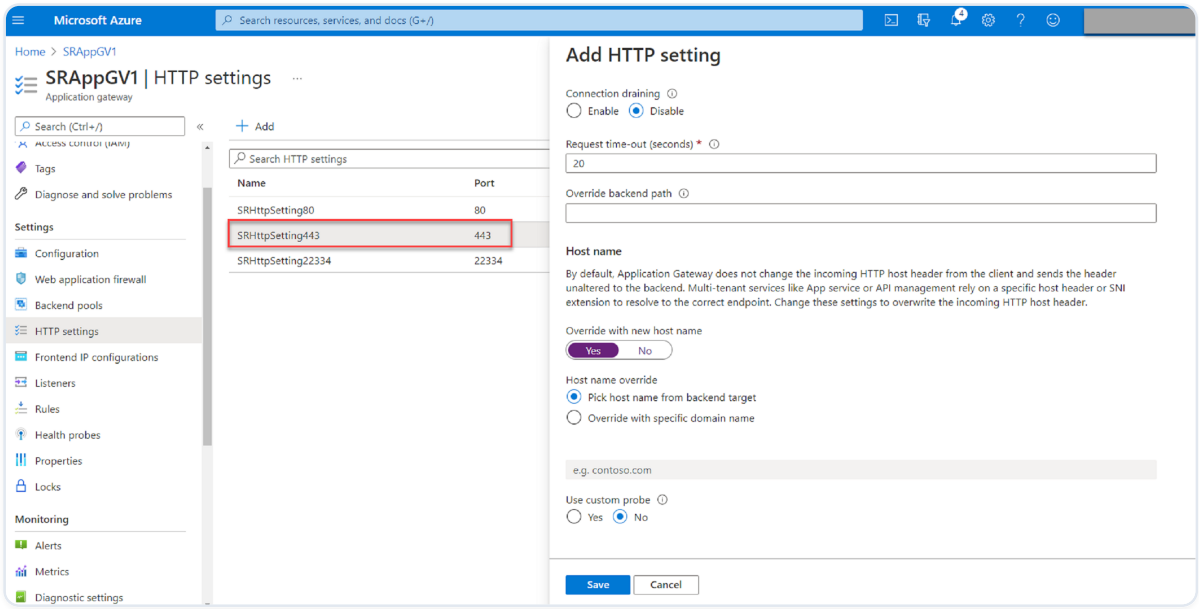
   - HTTP over port 80



- 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).

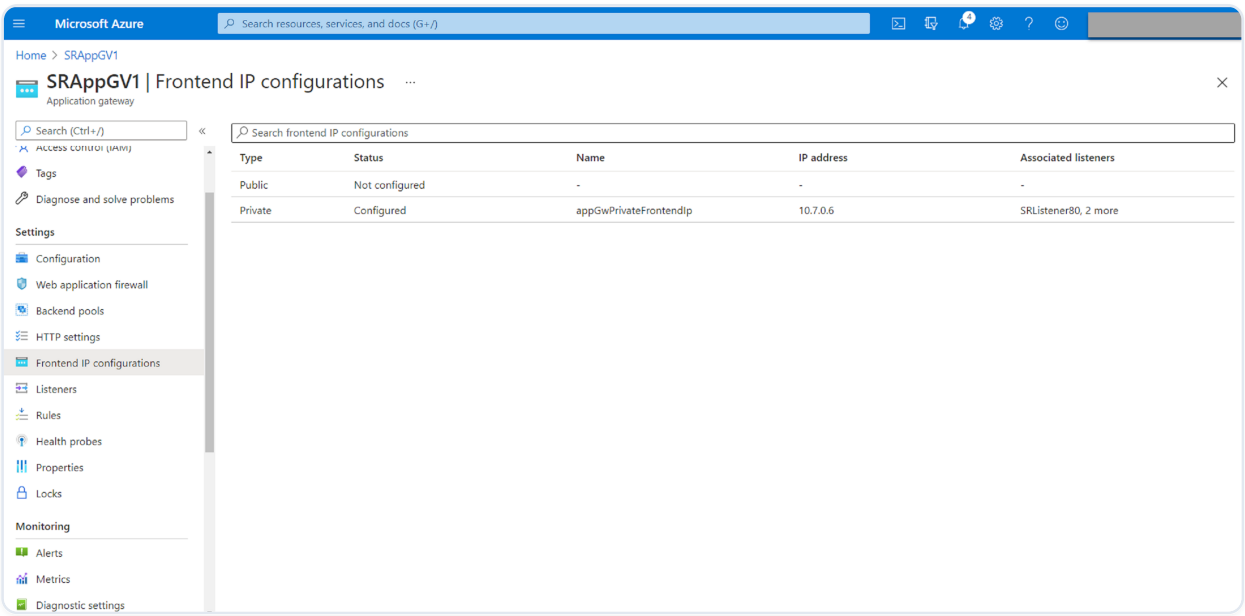




- HTTP or HTTPS over port 22334

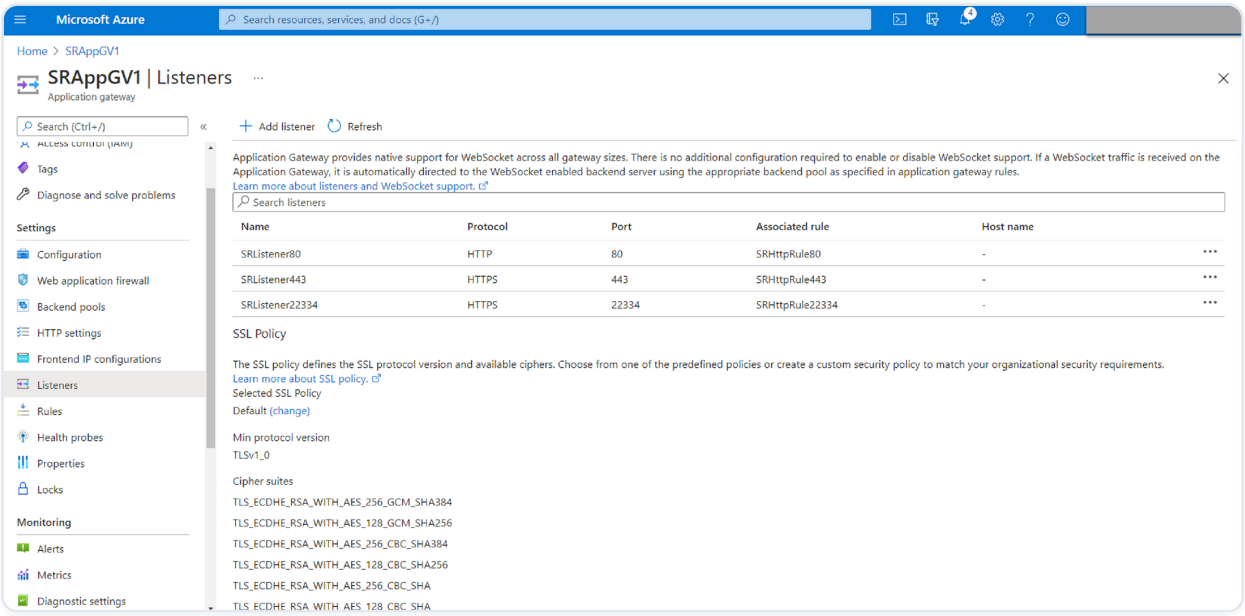
  If WebSocket uses HTTP, use the same setting as port 80. If WebSocket uses HTTPS, use the same setting as port 443.

4. Add a front-end IP address.

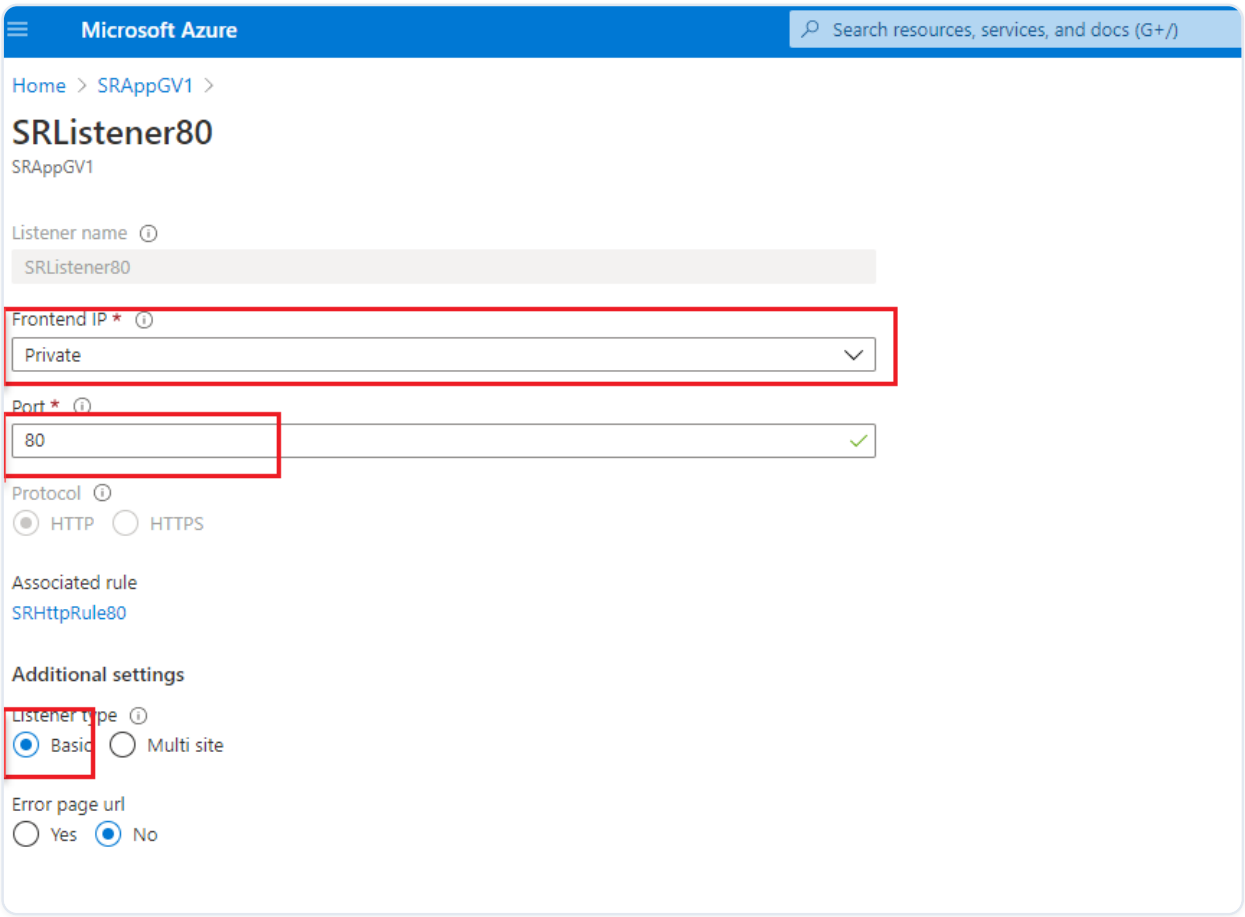


5. Add listeners.

   Add listeners on ports 80, 443, and 22334, for example:

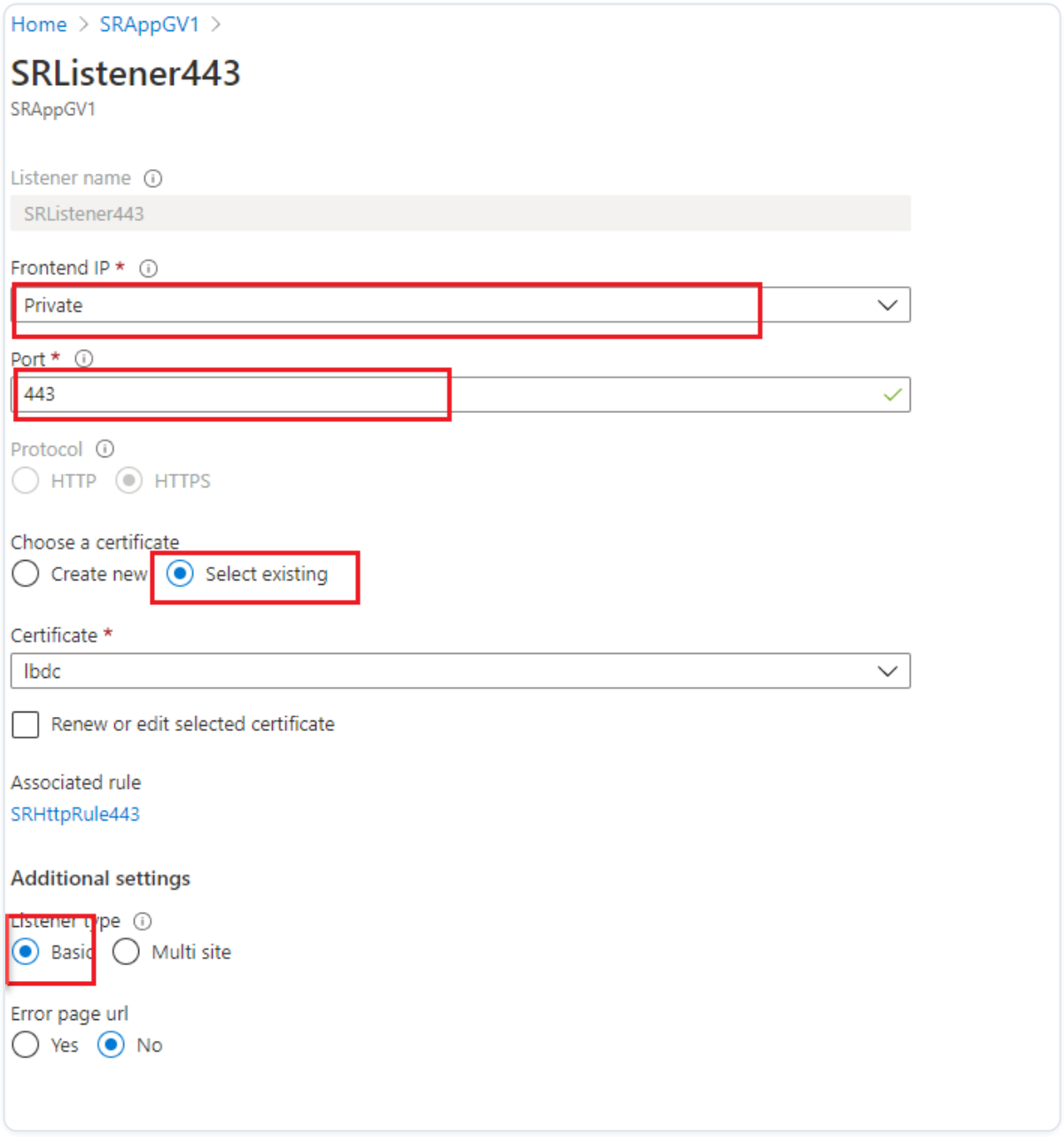


- Listener on port 80



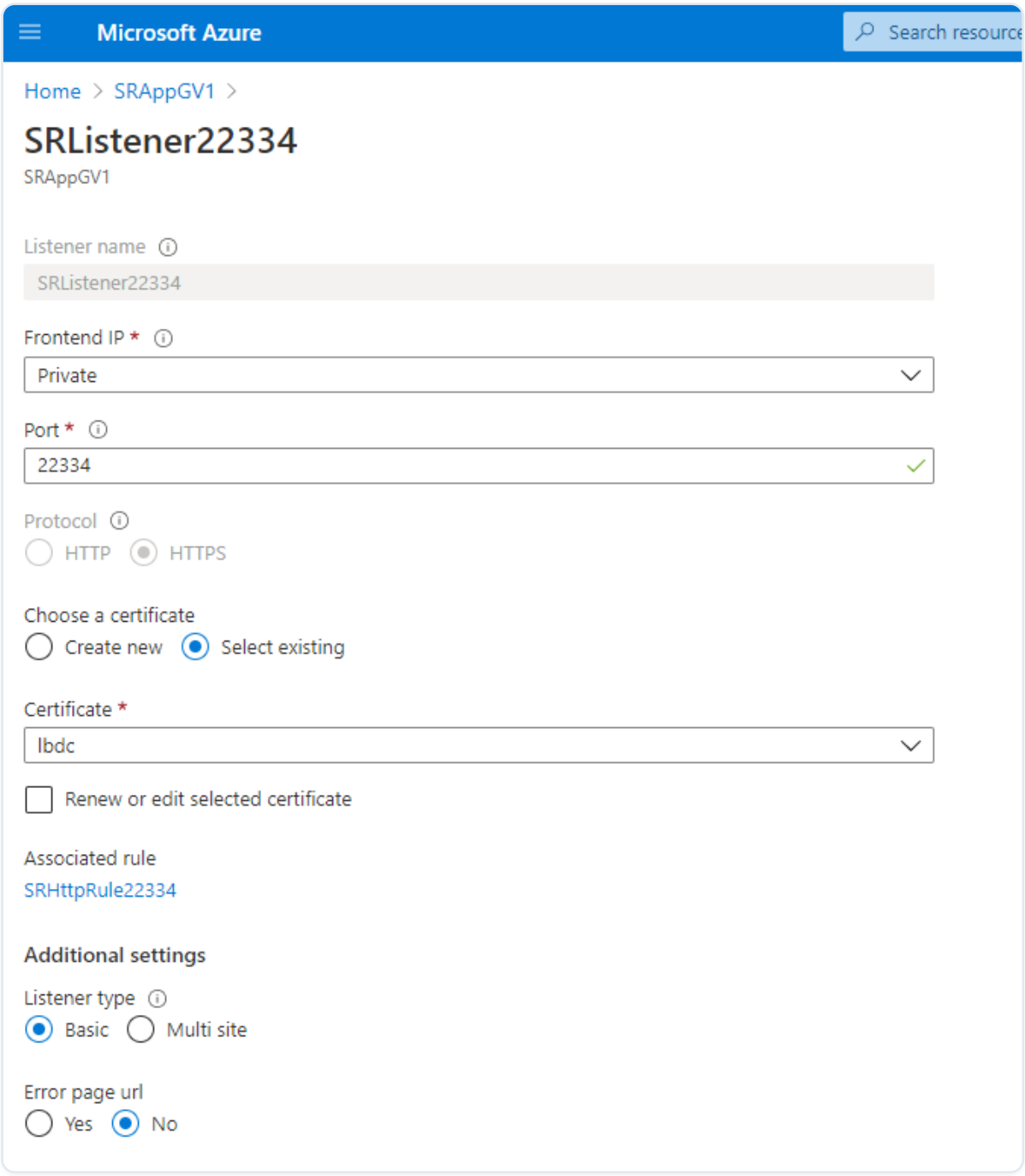
- Listener on port 443

  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.



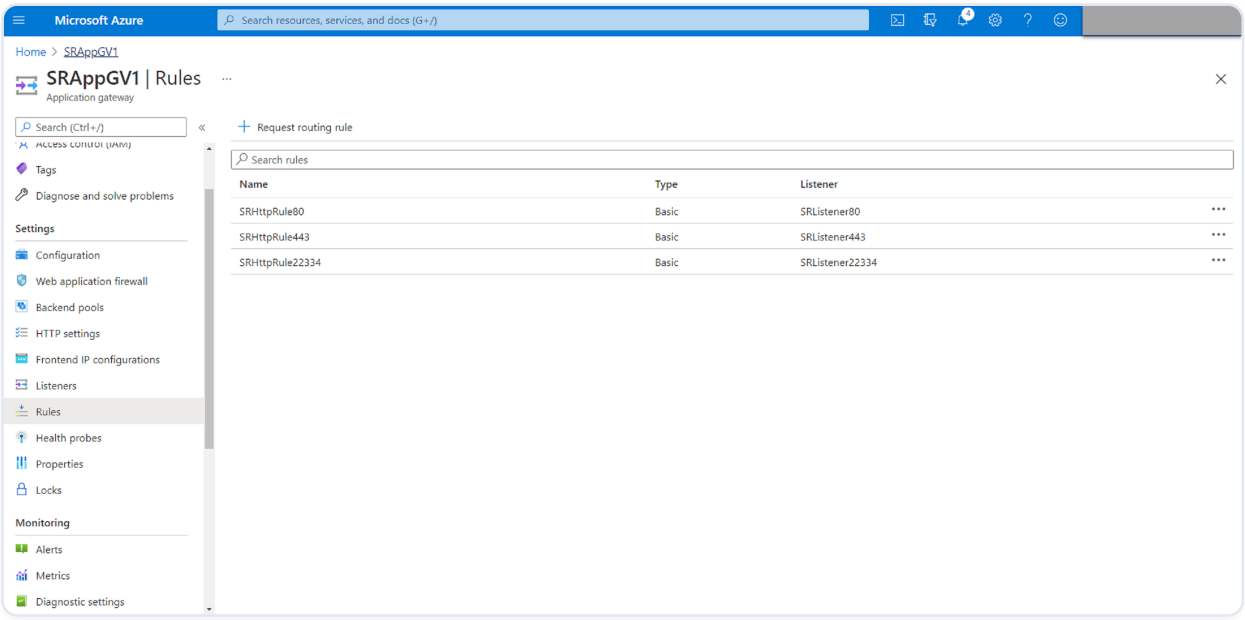
- Listener on port 22334

  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.

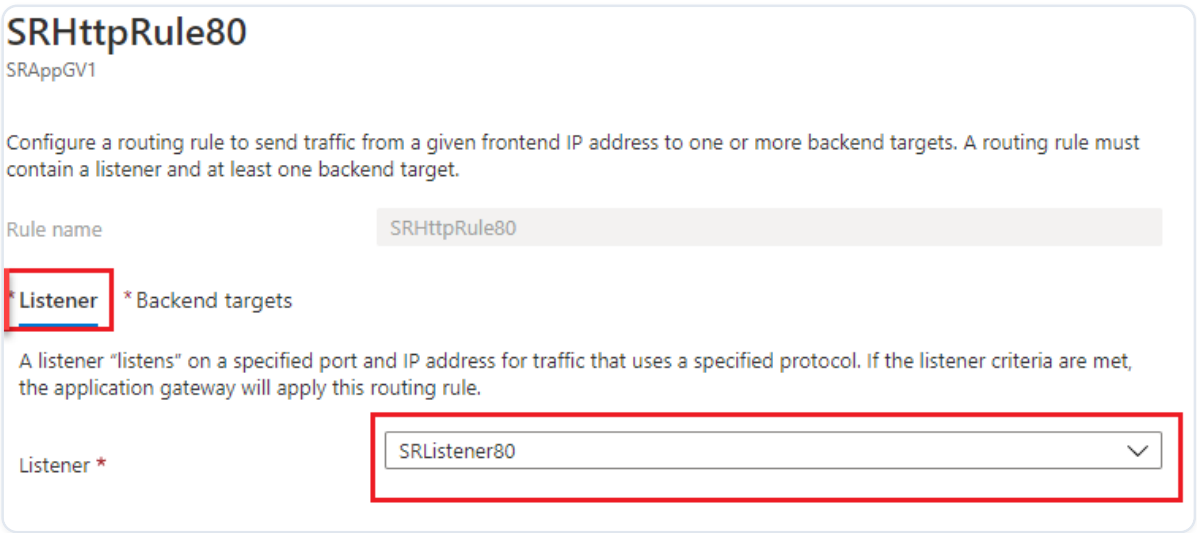


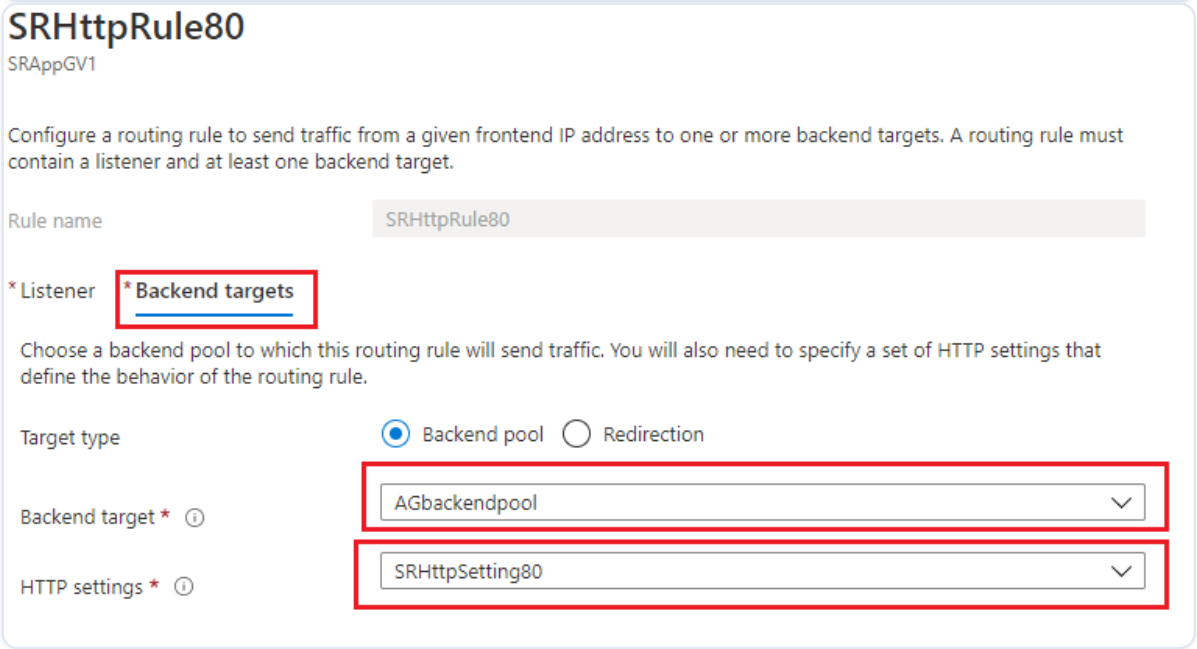
6. Create request routing rules.

   Create rules for ports 80, 443, and 22334, for example:

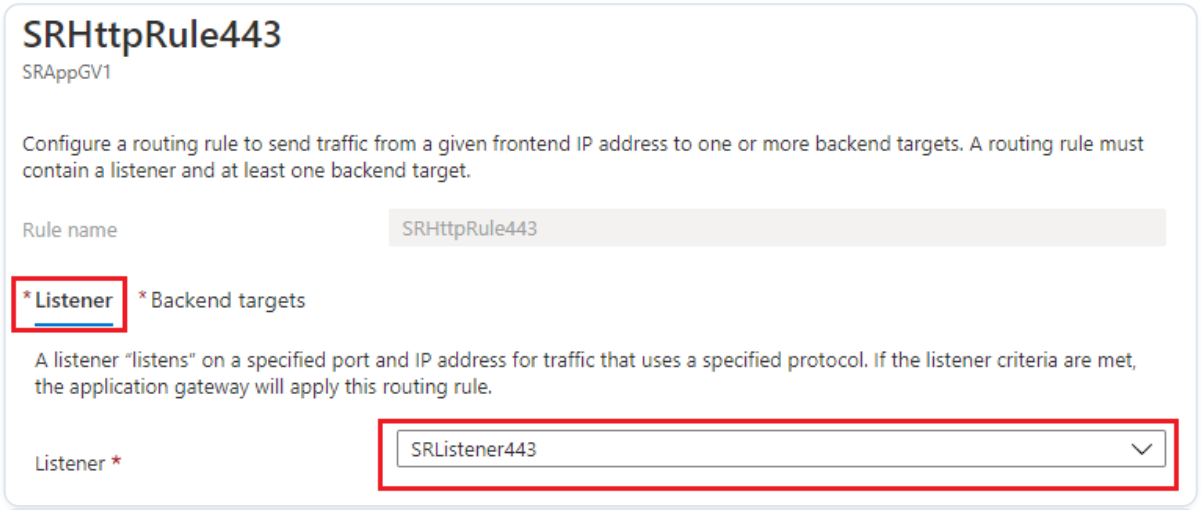


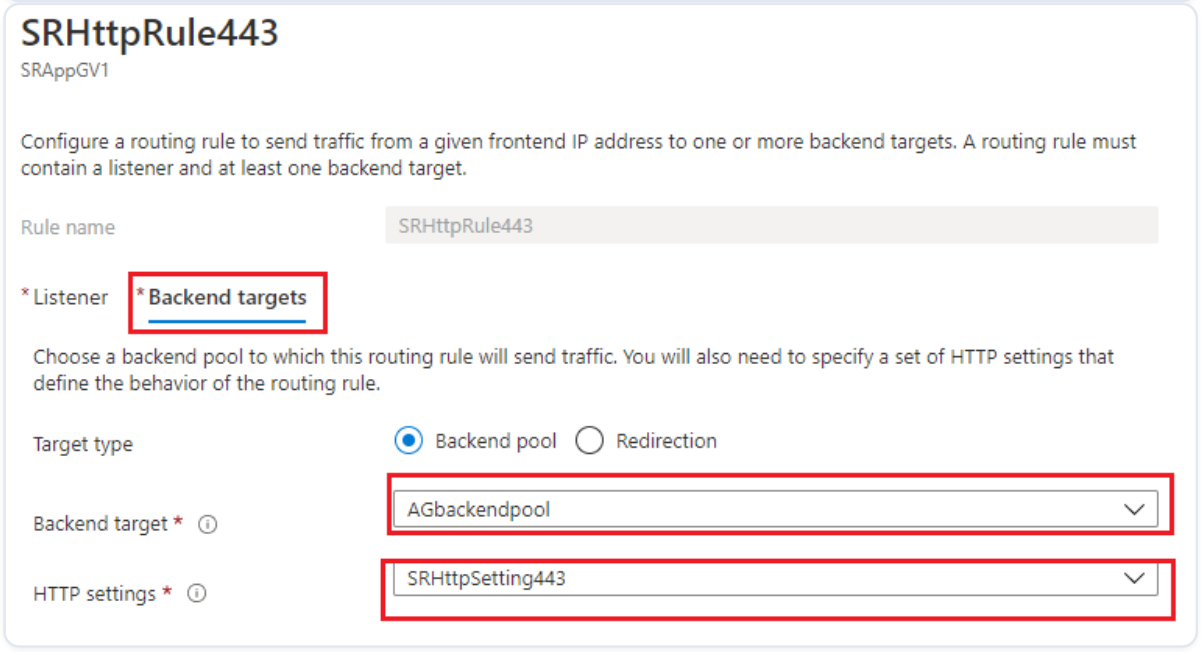
- Routing rule for port 80



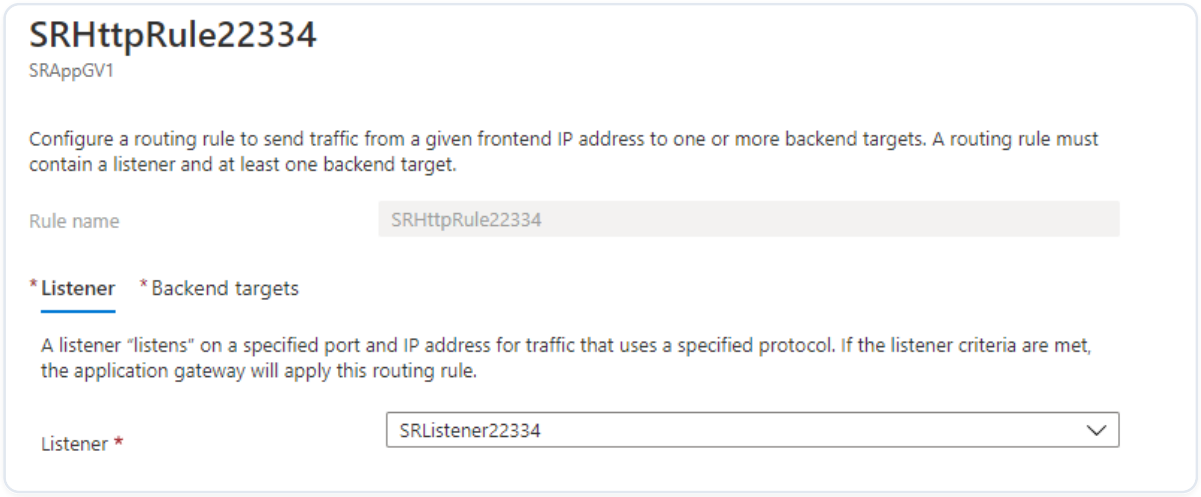


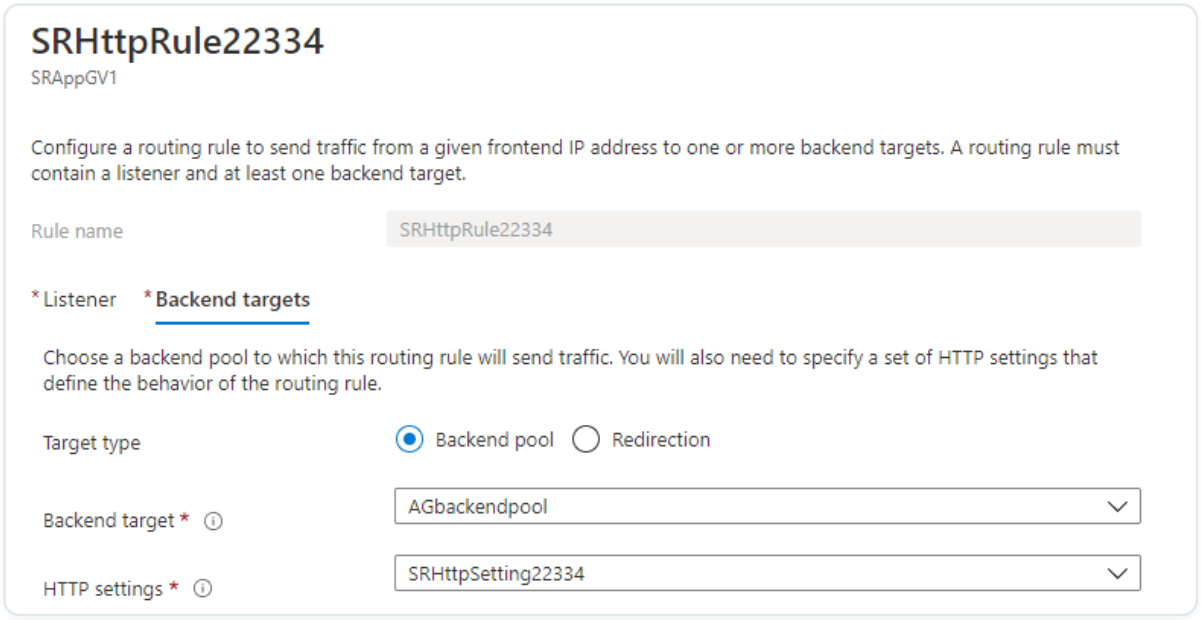
- Routing rule for port 443





- 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.
    - Step 1: Create shared folders on the file server
    - Step 2: Configure an existing Session Recording server to support load balancing

Configure Group Managed Service Account (gMSA) support for Session Recording

Session Recording supports Group Managed Service Accounts (gMSAs) to simplify service principal name (SPN) management for services running on multiple servers. This feature enhances security and simplifies the management of service accounts.

Step 1: Create a gMSA on the domain controller

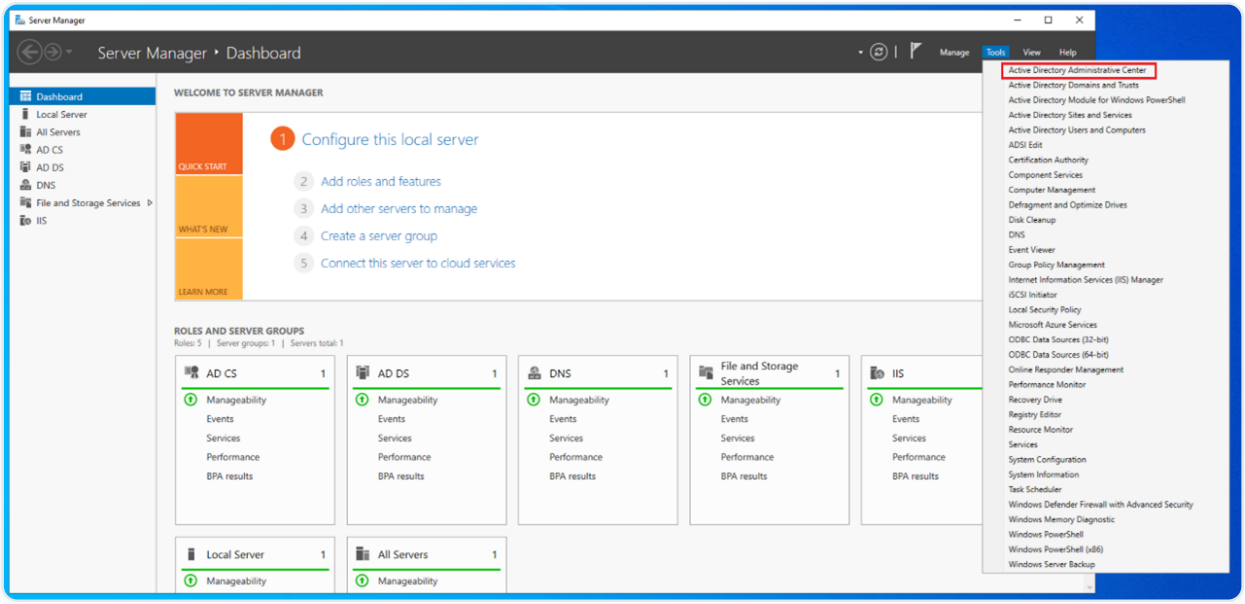
> **Note:**
>
> This section describes how to create a gMSA using Server Manager on the domain controller. Alternatively, you can run the following script to achieve the same purpose:
>
> ```
> Add-KdsRootKey -EffectiveImmediately
>
> Install-WindowsFeature -Name RSAT-AD-PowerShell
>
> NEW-ADGroup –name "gMSA"  –path "DC=ajj,DC=test" -GroupCategory
> Security -groupscope Global
> ```

```
Add-ADGroupMember "gMSA" -Members "Server-3$"(The dollar sign $ is must)

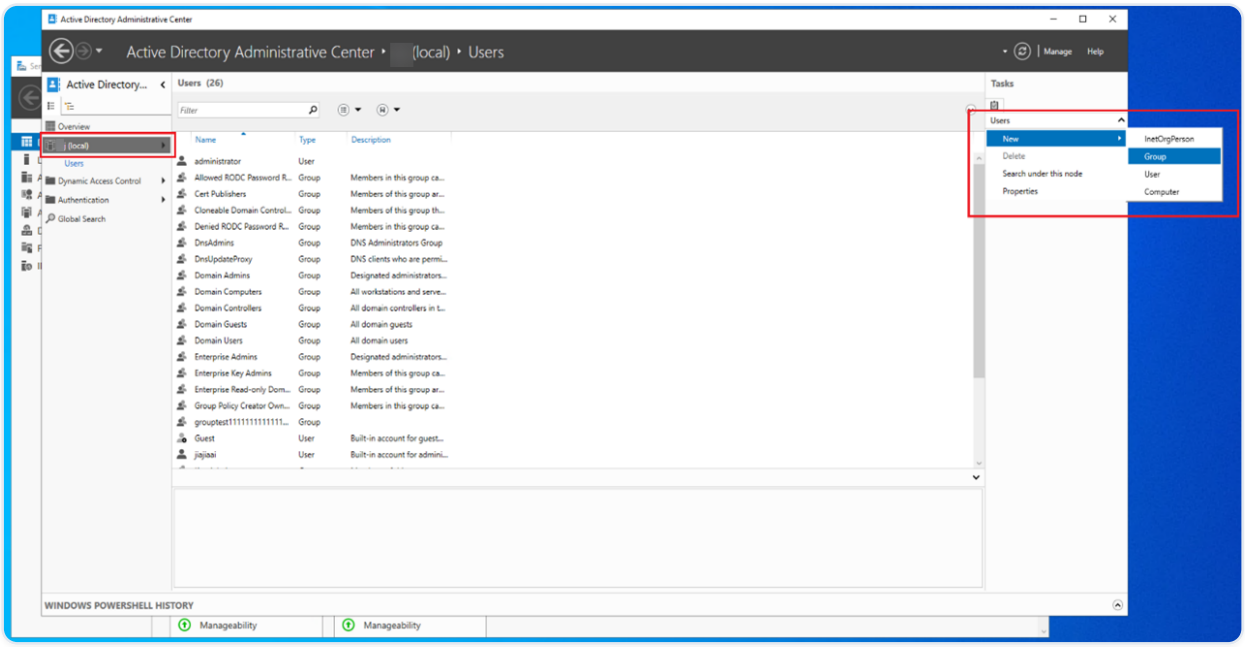
New-ADServiceAccount IIS1SvC -DNSHostName IIS1Svc.ajj.test -PrincipalsAllowedToRetrieveManagedPassword gMSA
```

The Effective time parameter allows time for keys to propagate to all domain controllers (DCs) before use. Using **Add-KdsRootKey -EffectiveImmediately** adds a root key to the target DC for immediate use by the Key Distribution Service (KDS) service. However, other domain controllers will not be able to use the root key until replication is complete.

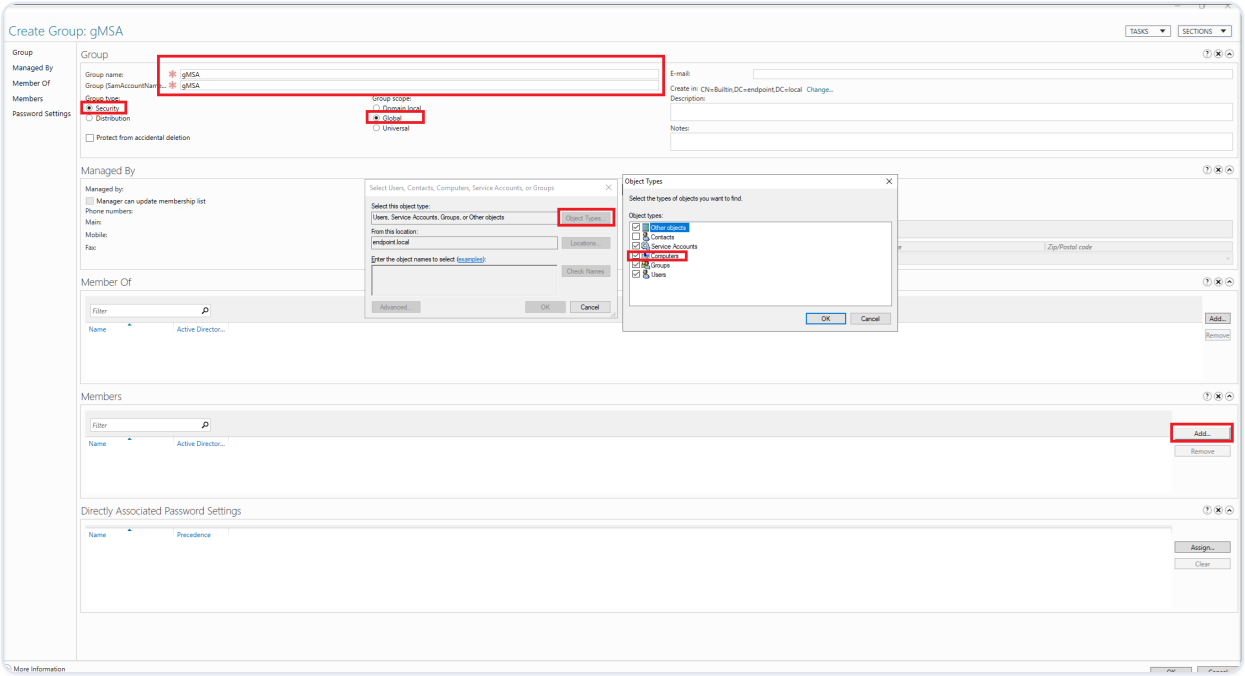
1. On the domain controller, open the Active Directory Administrative Center.



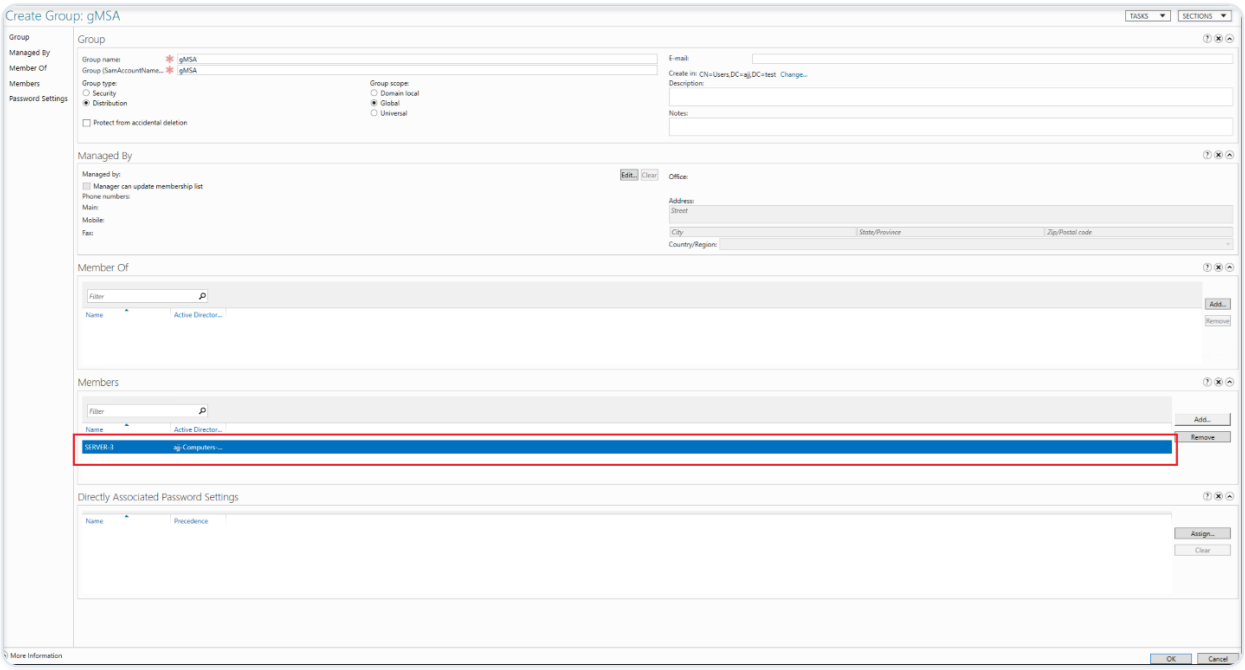
2. Select the domain and create a group.



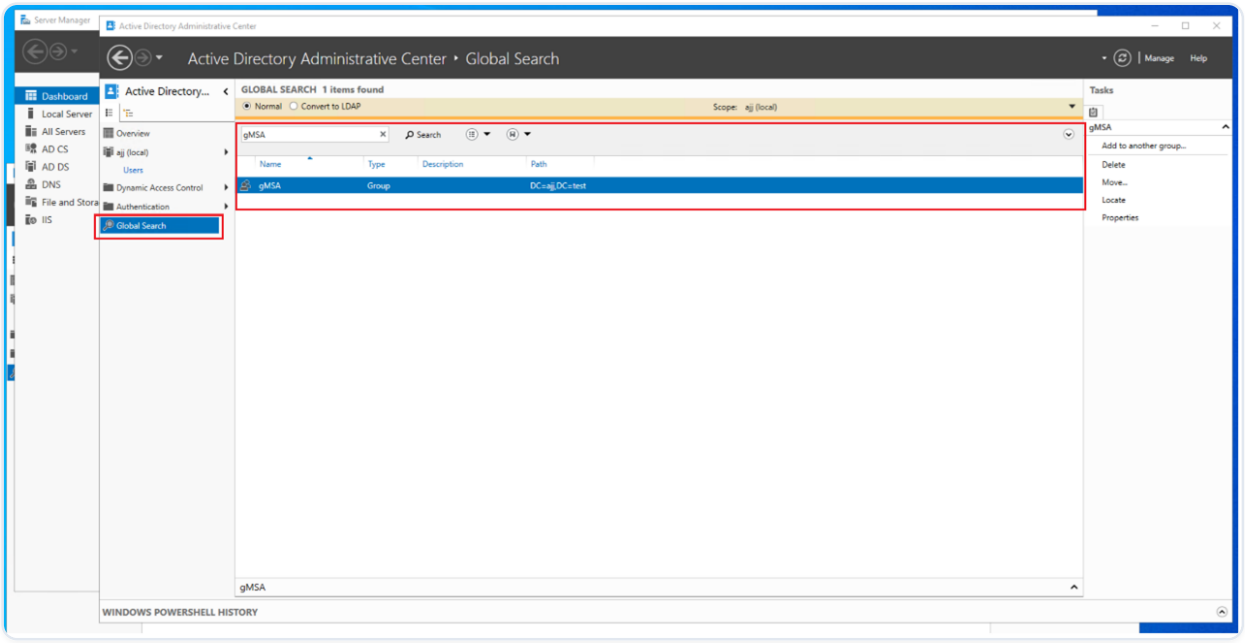
3. Name the group (using **gMSA** as an example). Set **Group type** to **Security** and **Group scope** to **Global**. Add member servers to it. The member servers include machines where the Session Recording servers and Session Recording database are installed.



For example, a group member is added as follows:



4. After successfully adding a security group, you can search for it using the global search in the Active Directory Administrative Center. You can view the member servers, and remember to restart all of them.



5. Create a gMSA account using the **New-ADServiceAccount** PowerShell cmdlet.

   On the domain controller, Open Windows PowerShell and run the following command to create a gMSA:

```
New-ADServiceAccount $serviceAccountName -DNSHostName $DNSHostName
-PrincipalsAllowedToRetrieveManagedPassword $groupName
```

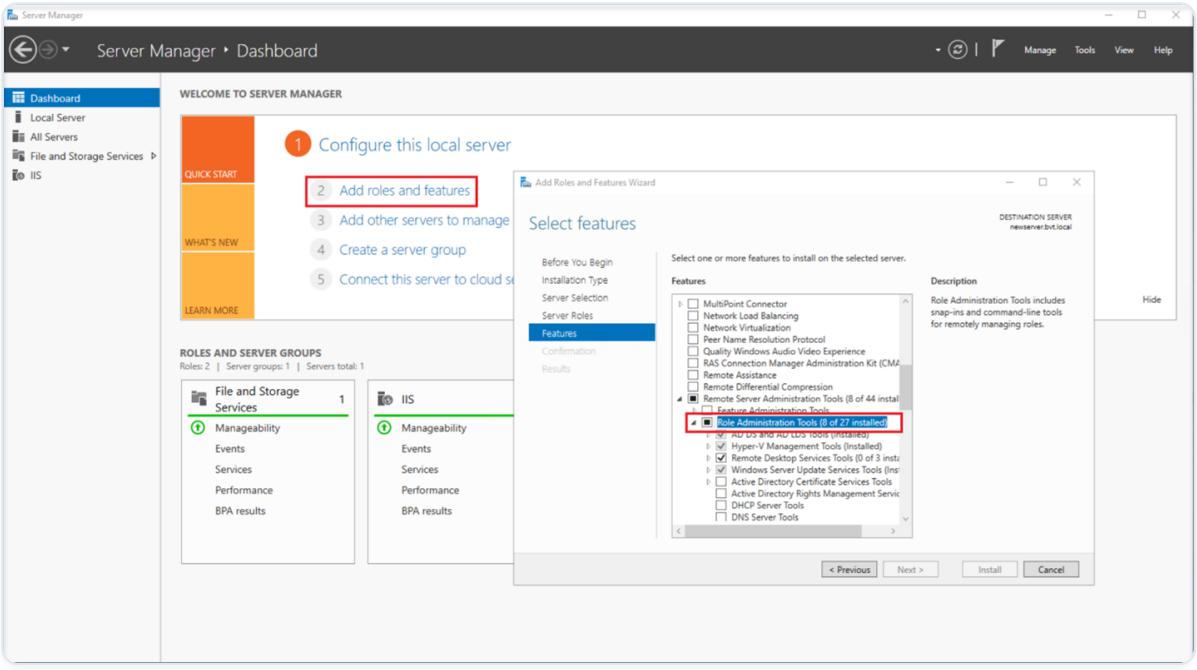
Where,

- **\$serviceAccountName** specifies the name of the gMSA. This article uses **IIS1SvC** as an example.
- **\$DNSHostName** specifies the DNS host name, in the format of **\$serviceAccountName** followed by the domain name of the domain controller.
- **\$groupName** specifies the group allowed to retrieve the managed password. This article uses **gMSA** as an example.

Step 2: Install the gMSA on each member server

You must install the gMSA on each server that will use it.

1. Install the Active Directory module for Windows PowerShell, using either the Server Manager or PowerShell with administrative privileges.
   - For an example of using the Server Manager:



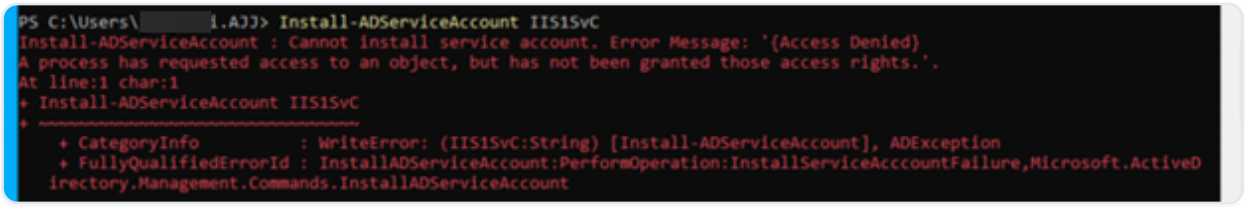
   - If you use PowerShell with administrative privileges, run the following command:

```
Install-WindowsFeature -Name RSAT-AD-PowerShell
```

2. Open Windows PowerShell and run a command similar to the following to install the gMSA.

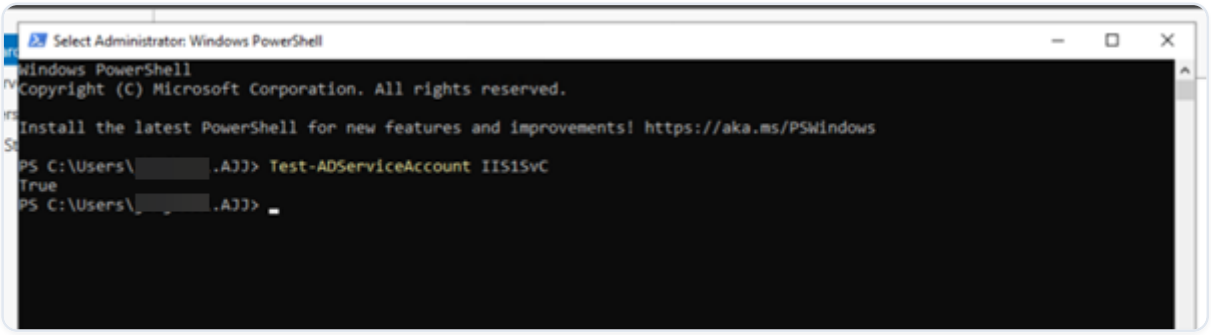
```
Install-ADServiceAccount IIS1SvC
```

If you encounter an "Access Denied" error similar to the following, make sure that the current member server has been added to the allow list of the gMSA and the server has been restarted afterwards.



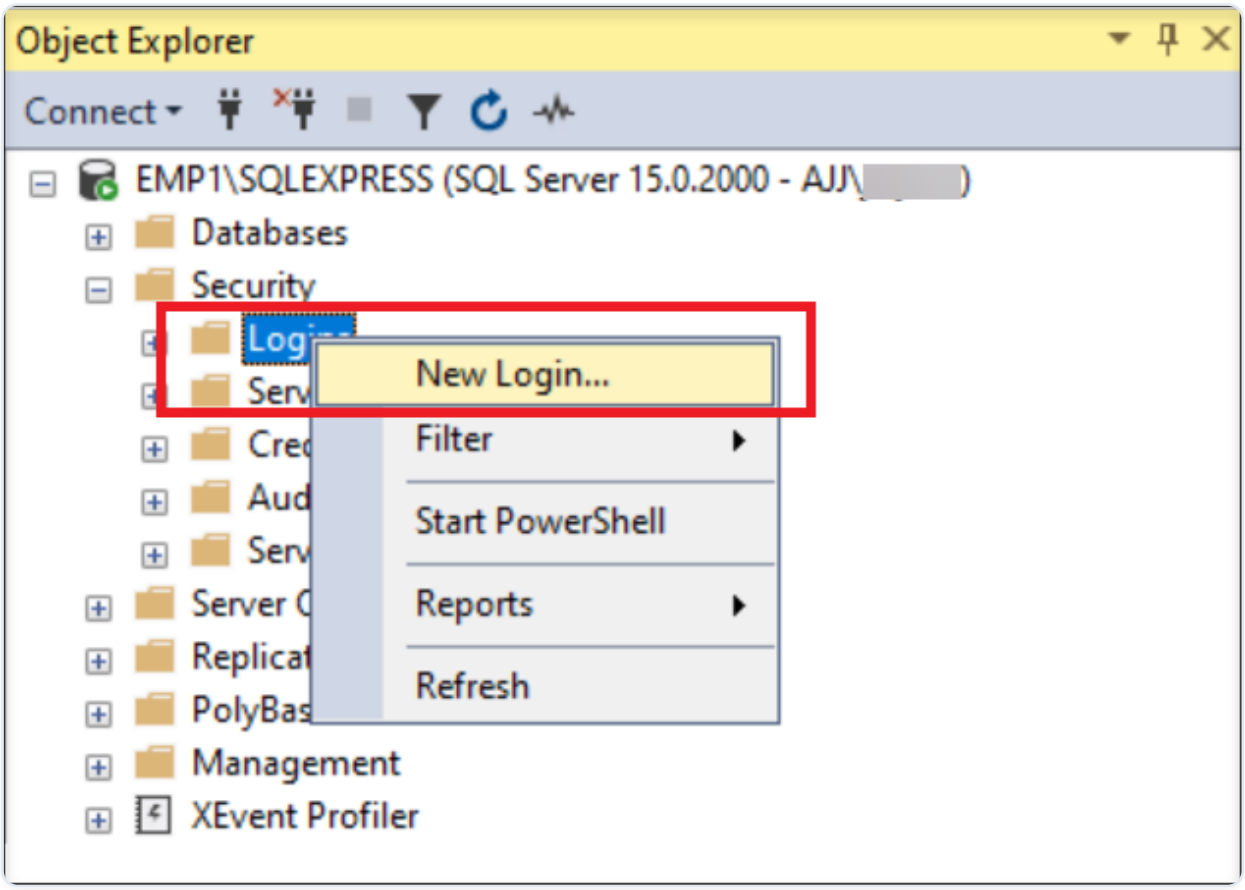
3. Verify that you have installed the gMSA successfully by running a command similar to the following in PowerShell. If the command returns **True**, the gMSA has been installed successfully.

```
Test-ADServiceAccount IIS1SvC
```

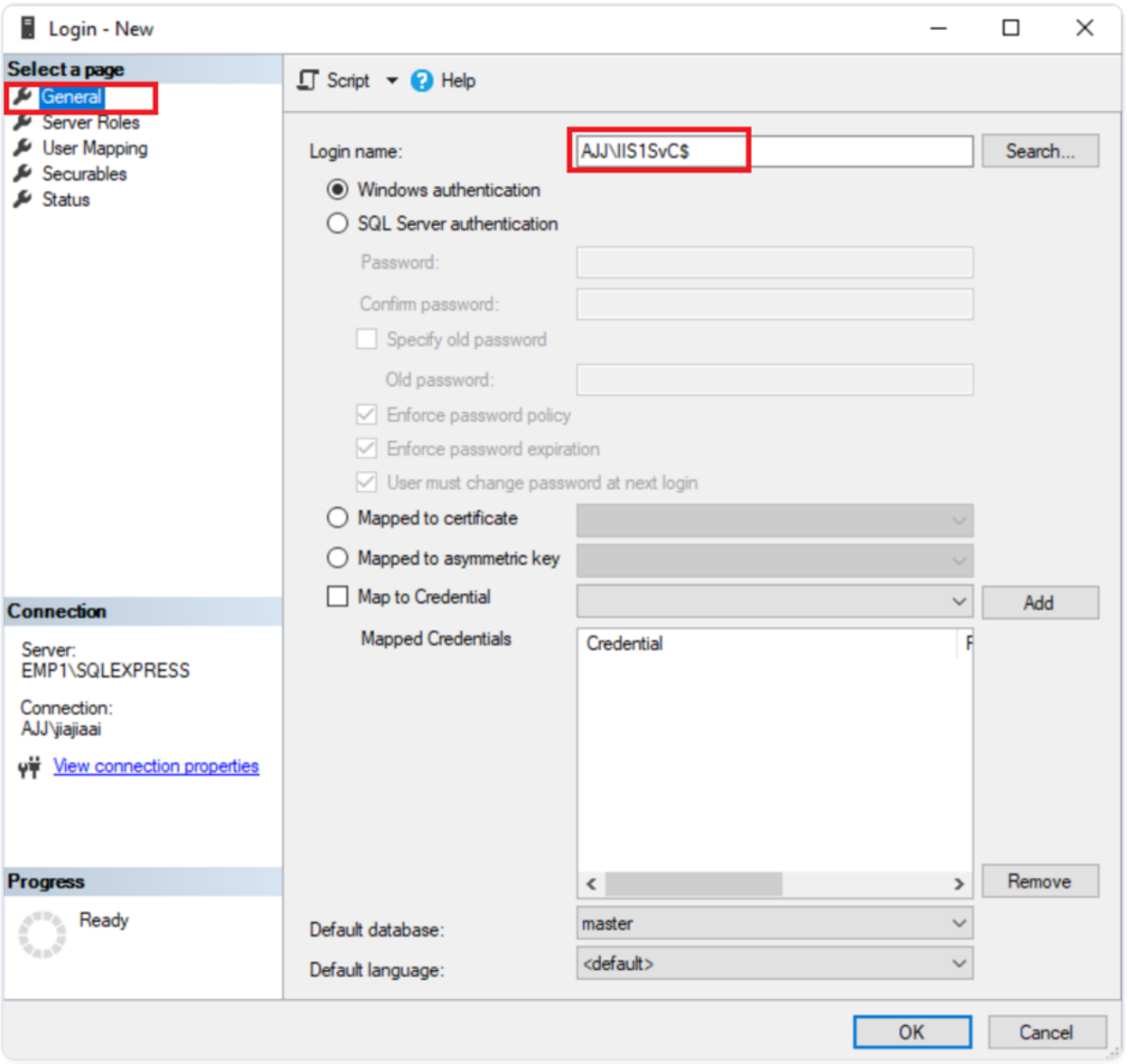


Step 3: Enable the gMSA to access the Session Recording database and Session Recording logging database

1. Create a login for the gMSA. Use the SQL Server Management Studio (SSMS) to connect to the SQL instance of the Session Recording database.

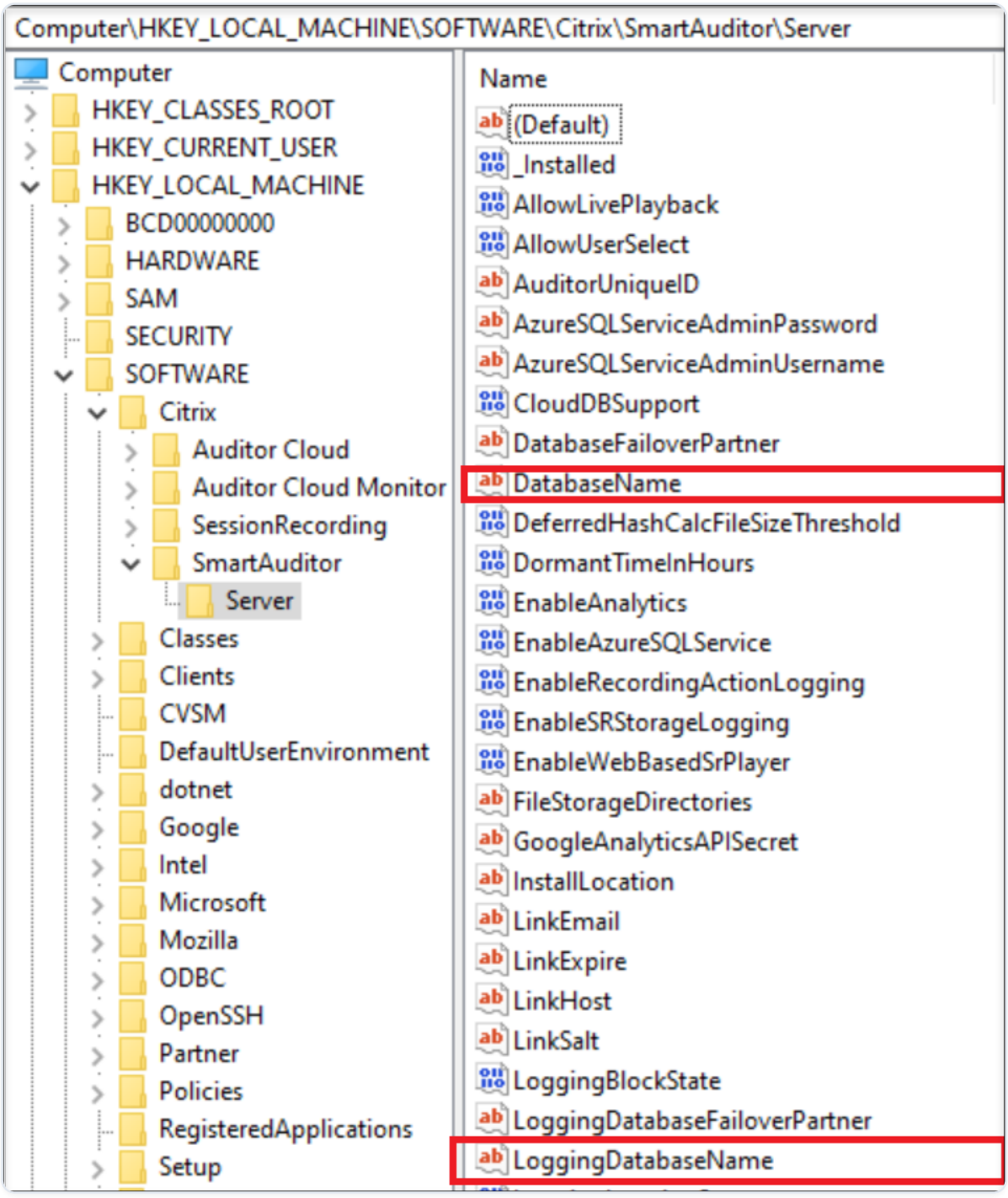


Name the new login in the format of **\<domain name of the domain controller>\\\<name of the gMSA>**. For example:

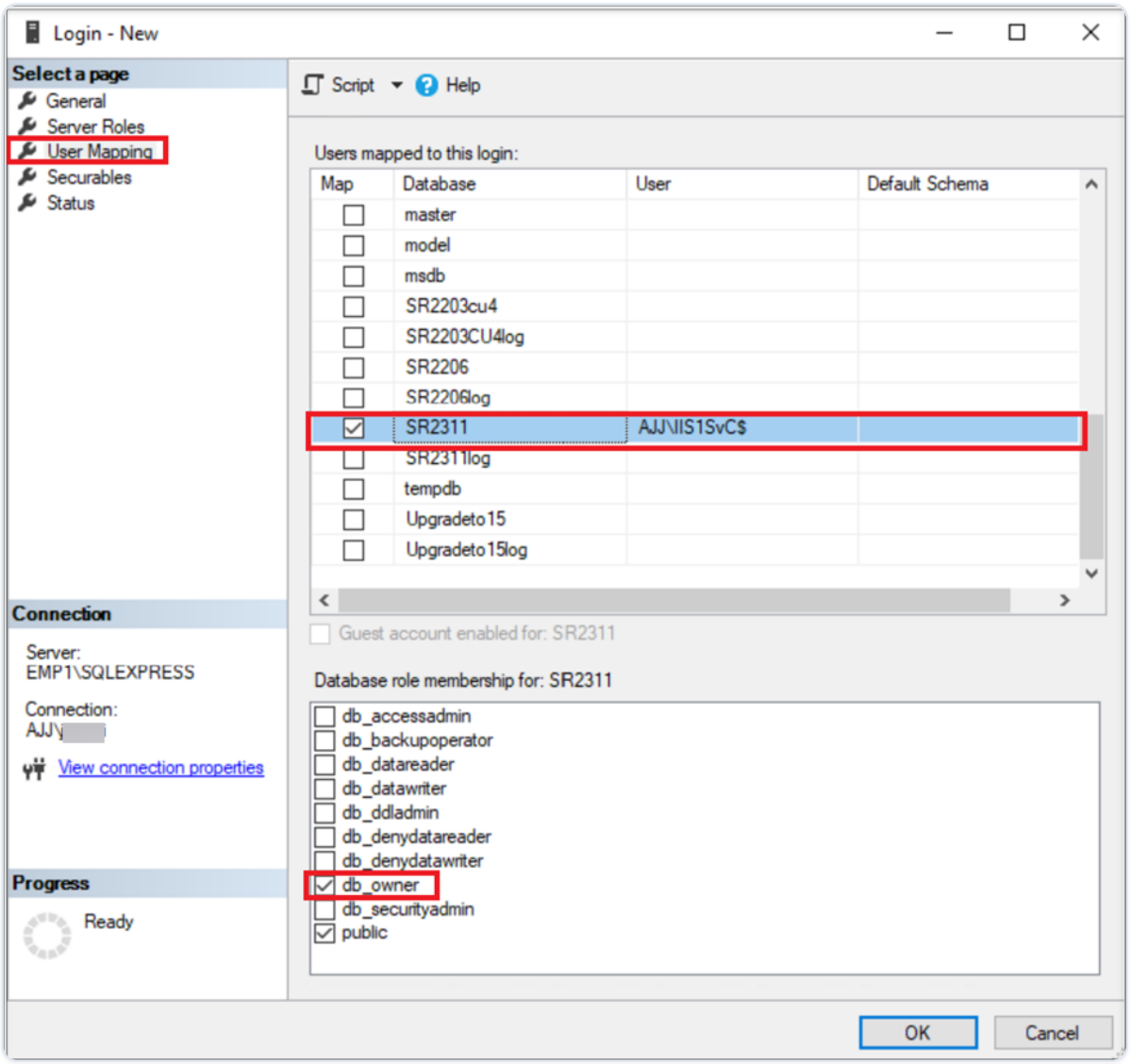


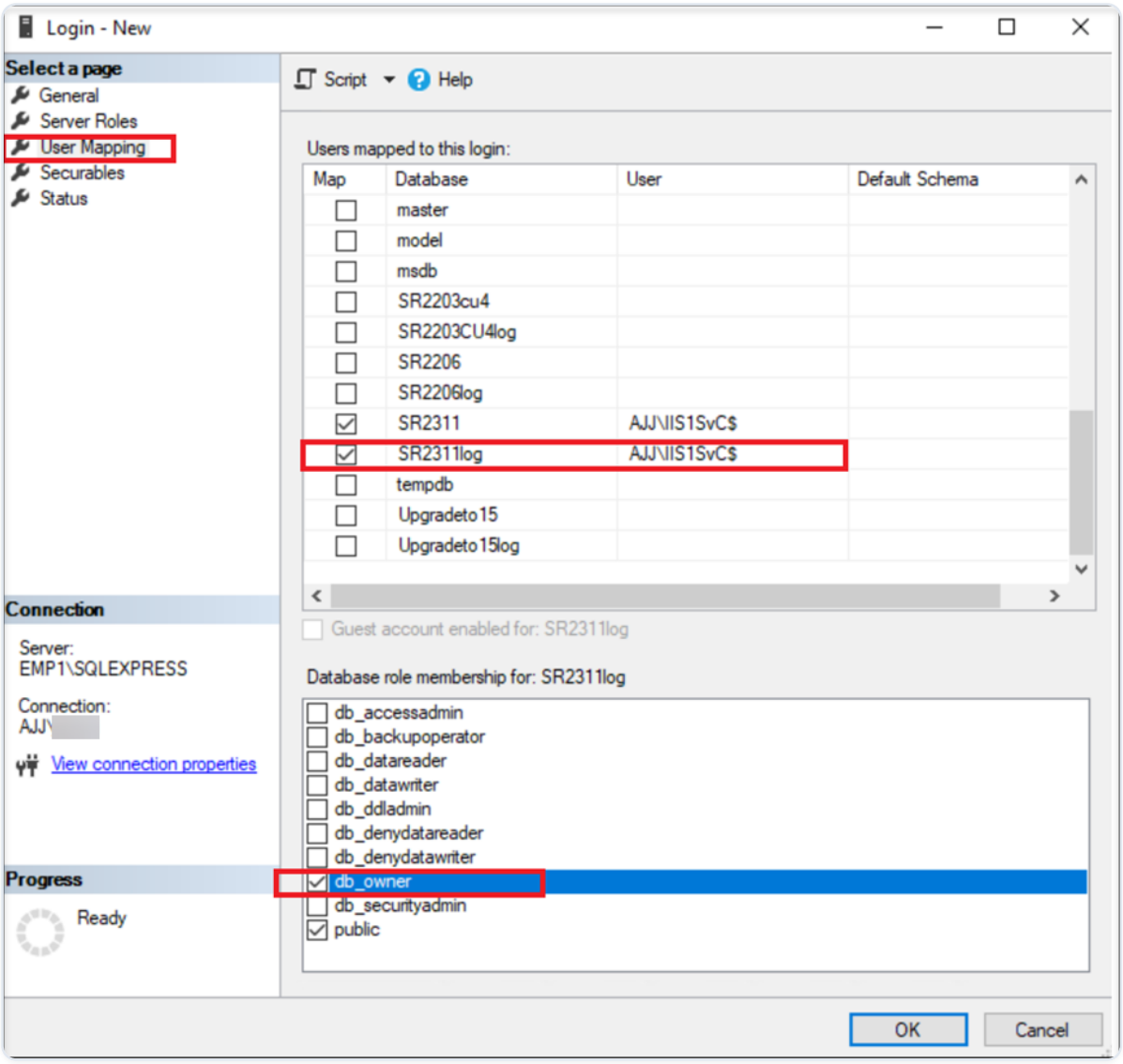
2. Enable the gMSA to access the Session Recording database and Session Recording logging database.

   a. Find the names of the Session Recording database and Session Recording logging database through the Registry. For example, double-click the following registry keys to get the value data.



b. Grant the **db_owner** permission of the Session Recording database and Session Recording logging database to the gMSA.


Login - New
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Users mapped to this login:
Map
Database
User
Default Schema
master
model
msdb
SR2203cu4
SR2203CU4log
SR2206
SR2206log
SR2311
AJJ\IIS1SvC$
SR2311log
tempdb
Upgradeto15
Upgradeto15log
Guest account enabled for: SR2311
Database role membership for: SR2311
db_accessadmin
db_backupoperator
db_datareader
db_datawriter
db_ddladmin
db_denydatareader
db_denydatawriter
db_owner
db_securityadmin
public
Connection
Server:
EMP1\SQLEXPRESS
Connection:
AJJ\
View connection properties
Progress
Ready
OK
Cancel



Note:

If you grant **db_datareader** and **db_datawriter** permissions instead of **db_owner** permission, you must also grant the execution permission on the databases to the gMSA. For example:

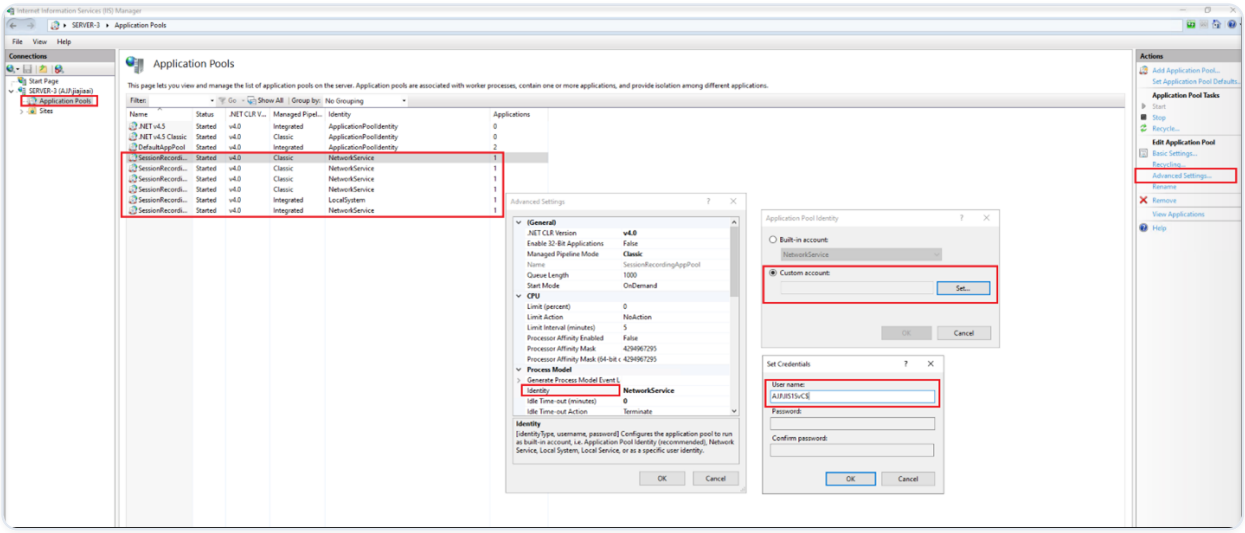
```
use SR2311 grant execute to [name of the login created earlier]

use SR2311log grant execute to [name of the login created earlier]
```

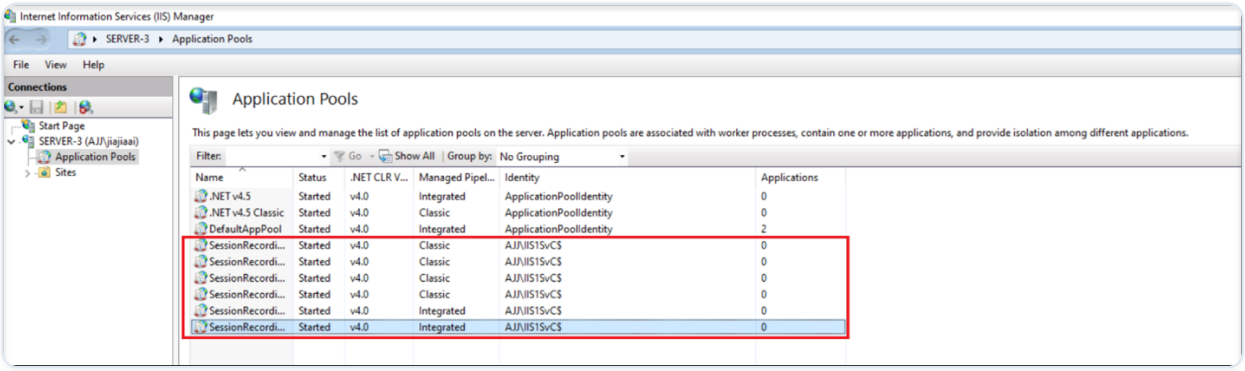
Step 3: Enable the gMSA to access the Session Recording servers

Complete the following steps on each Session Recording server:

1. Open Internet Information Services (IIS) Manager on the machine where the Session Recording server is installed, set the application pool identity to the gMSA, and the restart IIS.



For example, the following application pool identities have been set to the gMSA



Note:

Alternatively, you can set the application pool identity by running a command similar to the following using Windows PowerShell:

```
Import-Module WebAdministration -ErrorAction Stop

$webapps = Get-ChildItem -Path IIS:\AppPools

foreach ($webapp in $webapps) {

    if ($webapp.Name.Contains("SessionRecording")){

        $Pool = "IIS:\AppPools\" + $webapp.Name

        Write-Host $Pool
```

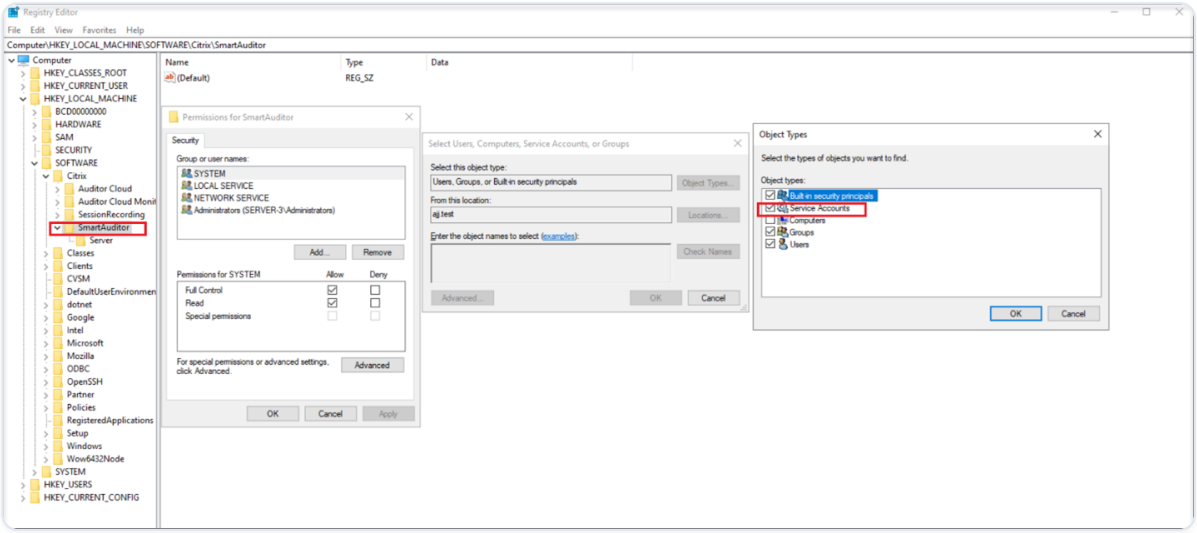
```
        Set-ItemProperty -Path $Pool -Name processModel -Value
@{userName="AJJ \IIS1SvC$";identitytype=3}

    }

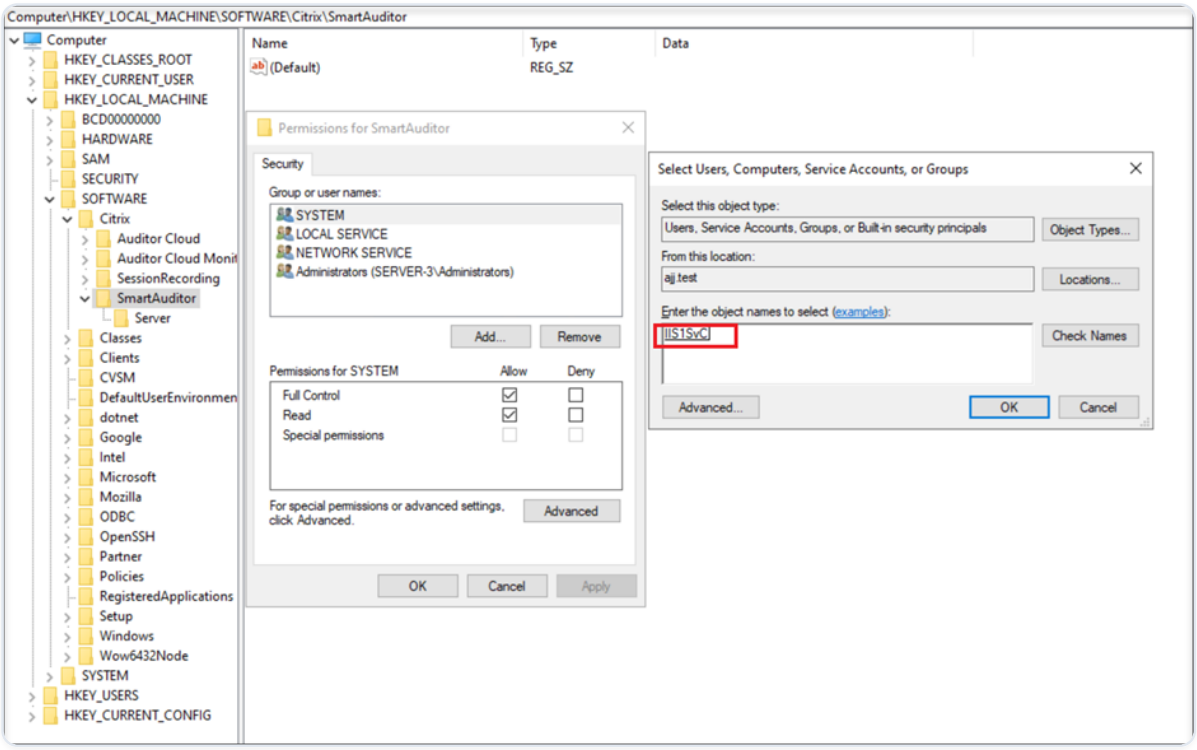
}
```

2. Open the Registry Editor on the machine where the Session Recording server is installed, and then grant Read permission on the Session Recording server to the gMSA.

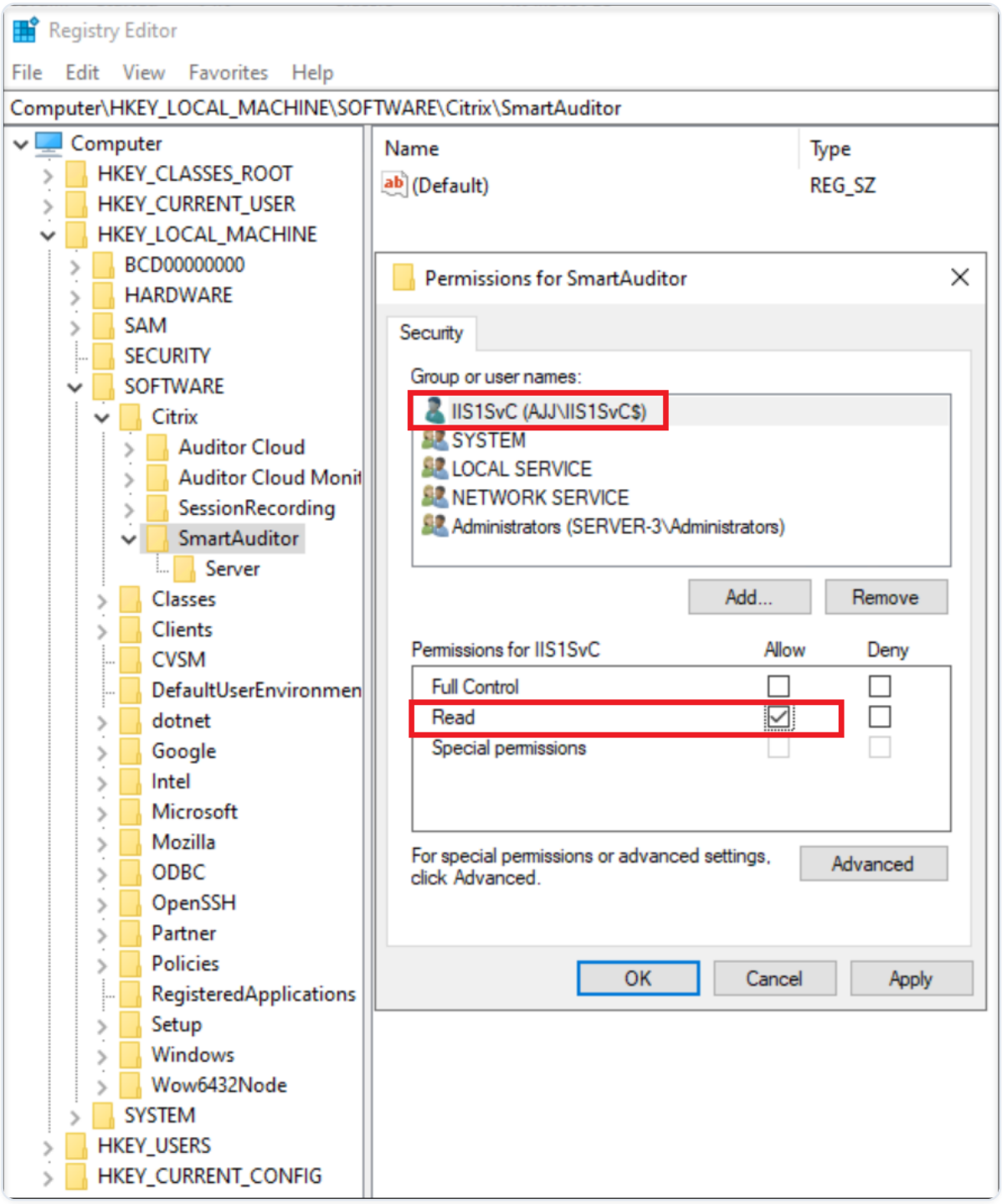
   a. Locate the service account object type.



   b. Enter the name of the gMSA.



c. Grant Read permission to the gMSA.



Note:

Alternatively, you can use a script similar to the following to grant Read permission on the Session Recording server to a gMSA:

```
$RegistryKey = "HKLM:\SOFTWARE\Citrix\SmartAuditor"

$NewAcl = Get-Acl -Path $RegistryKey
```

```
$identity = "pahl6\IIS1SvC$"

$RegistryKeyRights = "ReadPermissions"

$type = "Allow"

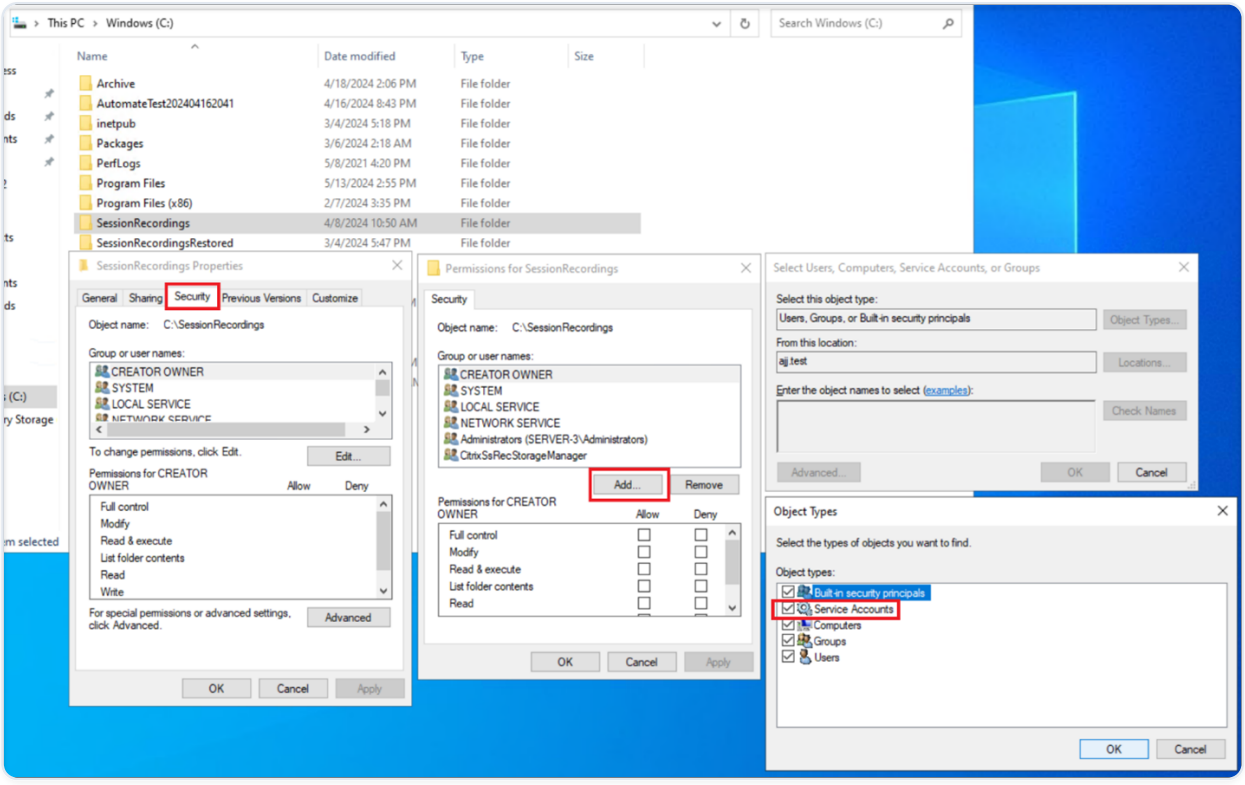
$RegistryKeyAccessRuleArgumentList = $identity, $RegistryKeyRights,
$type

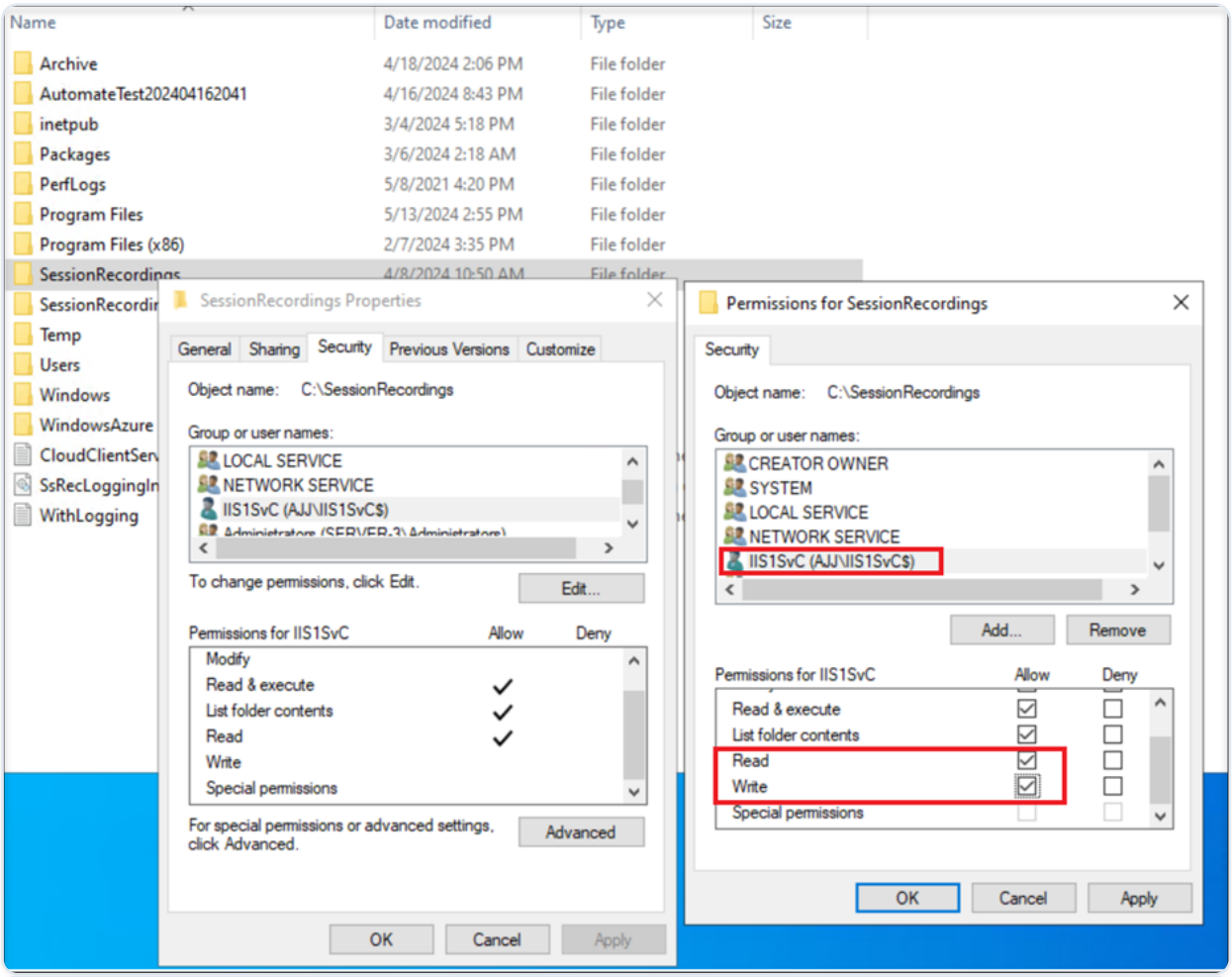
$RegistryKeyAccessRule = New-Object
System.Security.AccessControl.RegistryAccessRule -ArgumentList
$RegistryKeyAccessRuleArgumentList

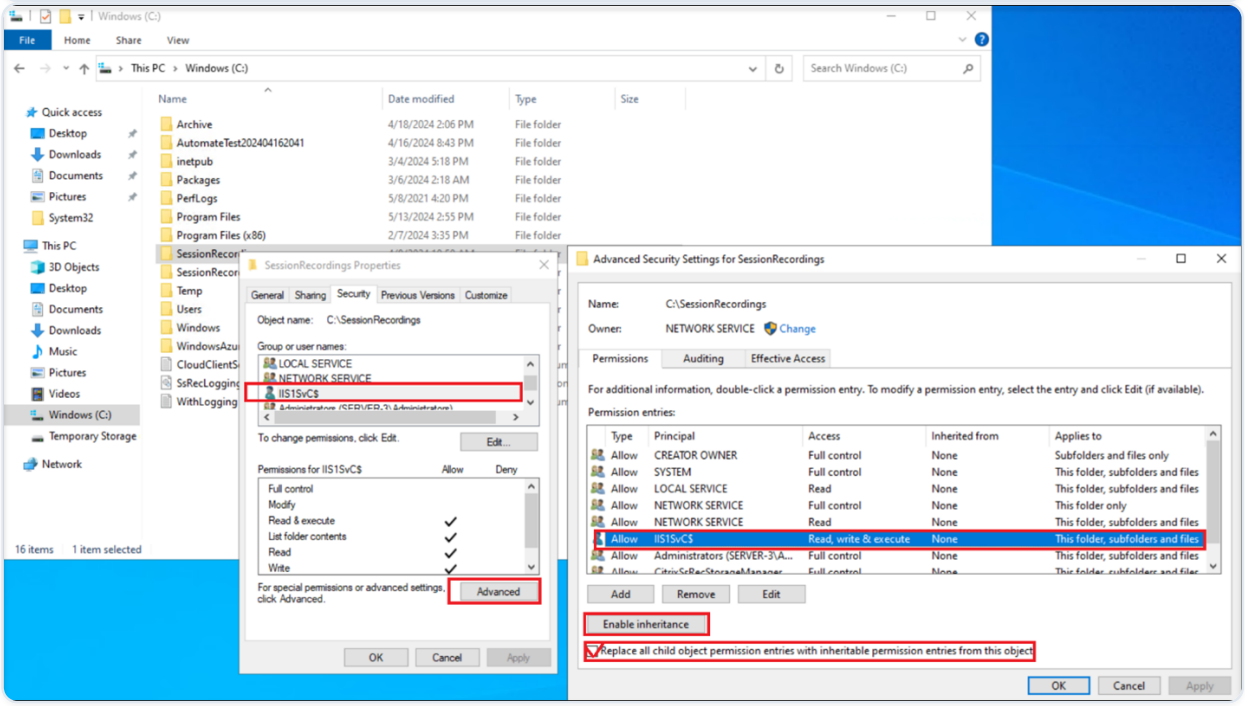
$NewAcl.SetAccessRule($RegistryKeyAccessRule)

Set-Acl -Path $RegistryKey -AclObject $NewAcl
```

3. Add the gMSA to the Session recording storage folder and grant it Read and Write permissions on the folder. After that, enable inheritance and select **Replace all child object permission entries with inheritable permission entries from this object**.




Name
Date modified
Type
Size
Archive
AutomateTest202404162041
inetpub
Packages
PerfLogs
Program Files
Program Files (x86)
SessionRecordings
Temp
Users
Windows
WindowsAzure
WithLogging
SessionRecordings Properties
General
Sharing
Security
Previous Versions
Customize
Object name: C:\SessionRecordings
Group or user names:
LOCAL SERVICE
NETWORK SERVICE
IIS1SvC (AJJ\IIS1SvC$)
To change permissions, click Edit.
Edit...
Permissions for IIS1SvC
Allow
Deny
Modify
Read & execute
List folder contents
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Permissions for SessionRecordings
Security
Object name: C:\SessionRecordings
Group or user names:
CREATOR OWNER
SYSTEM
LOCAL SERVICE
NETWORK SERVICE
IIS1SvC (AJJ\IIS1SvC$)
Add...
Remove
Permissions for IIS1SvC
Allow
Deny
Read & execute
List folder contents
Read
Write
Special permissions
OK
Cancel
Apply


Windows (C:)
File
Home
Share
View
This PC
Windows (C:)
Search Windows (C:)
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
Temporary Storage
Network
16 items
1 item selected
SessionRecordings Properties
Advanced Security Settings for SessionRecordings
Name: C:\SessionRecordings
Owner: NETWORK SERVICE
Change
Permissions
Auditing
Effective Access
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).
Permission entries:
Type
Principal
Access
Inherited from
Applies to
Add
Remove
Edit
Enable inheritance
Replace all child object permission entries with inheritable permission entries from this object
OK
Cancel
Apply

Note:

Alternatively, you can use a script similar to the following to grant Read and Write permissions on the Session recording storage folder to a gMSA and to enable inheritance:

```
$path = "C:\SessionRecordings"

$NewAcl = Get-Acl $path

# Set properties

$identity = "pahl6\IIS1SvC$"

$fileSystemRights = "Modify"

$type = "Allow"

# Create new rule

$fileSystemAccessRuleArgumentList = $identity, $fileSystemRights,
$type

$fileSystemAccessRule = New-Object -TypeName
System.Security.AccessControl.FileSystemAccessRule
 $fileSystemAccessRuleArgumentList

# Apply new rule

$NewAcl.SetAccessRule($fileSystemAccessRule)

# enable inherit

$isProtected = $false

$preserveInheritance = $false

$NewAcl.SetAccessRuleProtection($isProtected, $preserveInheritance)

Set-Acl -Path $path -AclObject $NewAcl
```

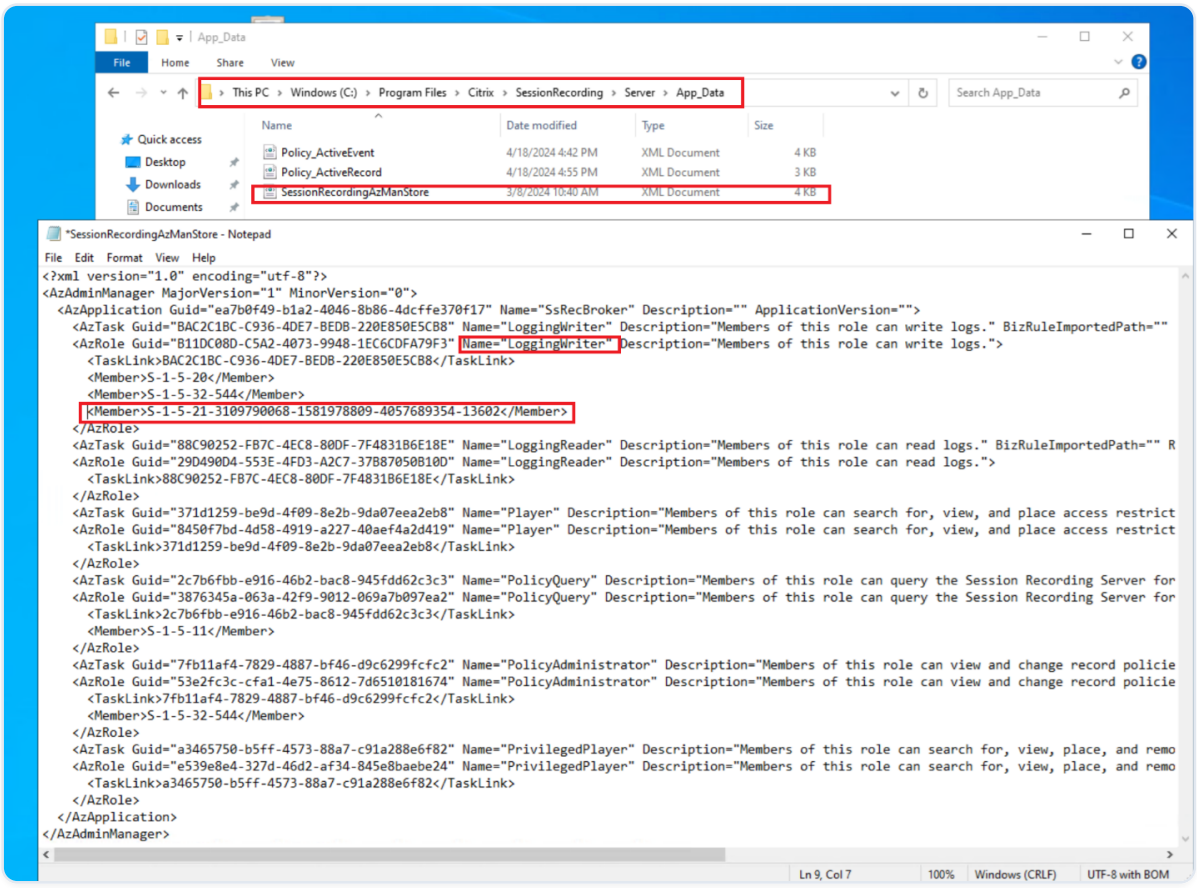
4. Add the gMSA to the Session Recording Authorization Console.

   a. Find the Security Identifier (SID) for the gMSA.

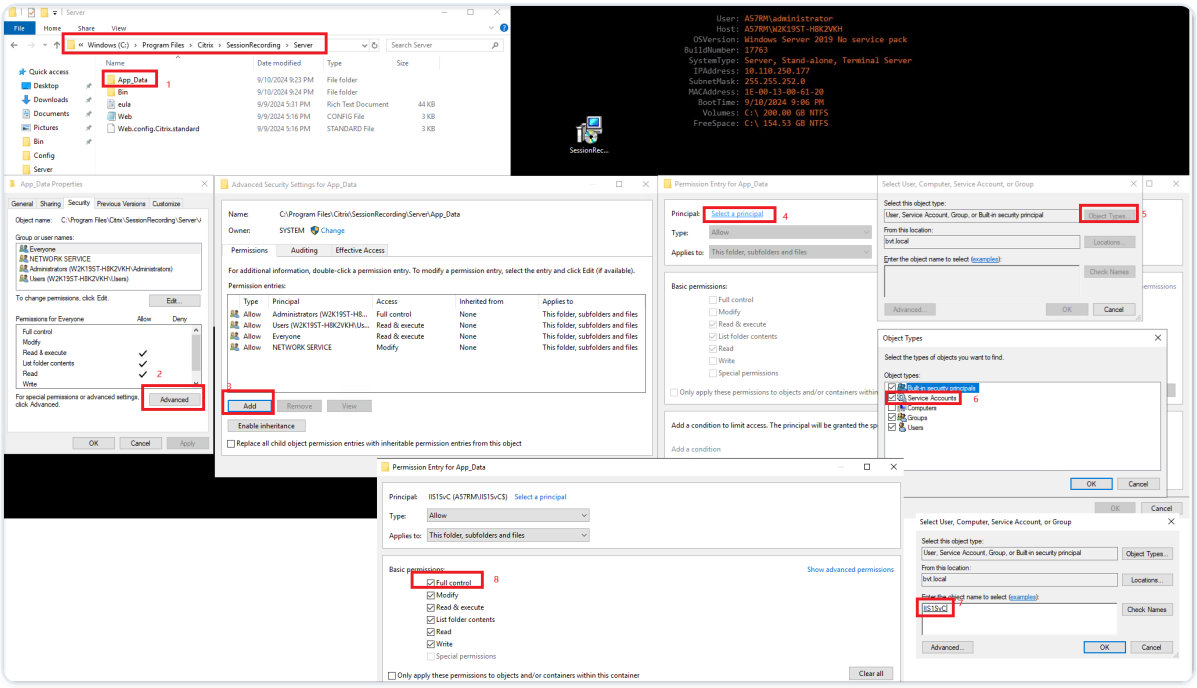
```
PS C:\Users\[redacted].AJJ> $account = "IIS1SvC"
PS C:\Users\[redacted].AJJ> Get-ADServiceAccount -Identity $account


DistinguishedName : CN=IIS1SvC,CN=Managed Service Accounts,DC=ajj,DC=test
Enabled           : True
Name              : IIS1SvC
ObjectClass       : msDS-GroupManagedServiceAccount
ObjectGUID        : 4f4a2eb2-81c7-438a-b054-68fcd915cdfc
SamAccountName    : IIS1SvC$
SID               : S-1-5-21-3109790068-1581978809-4057689354-13602
UserPrincipalName :
```

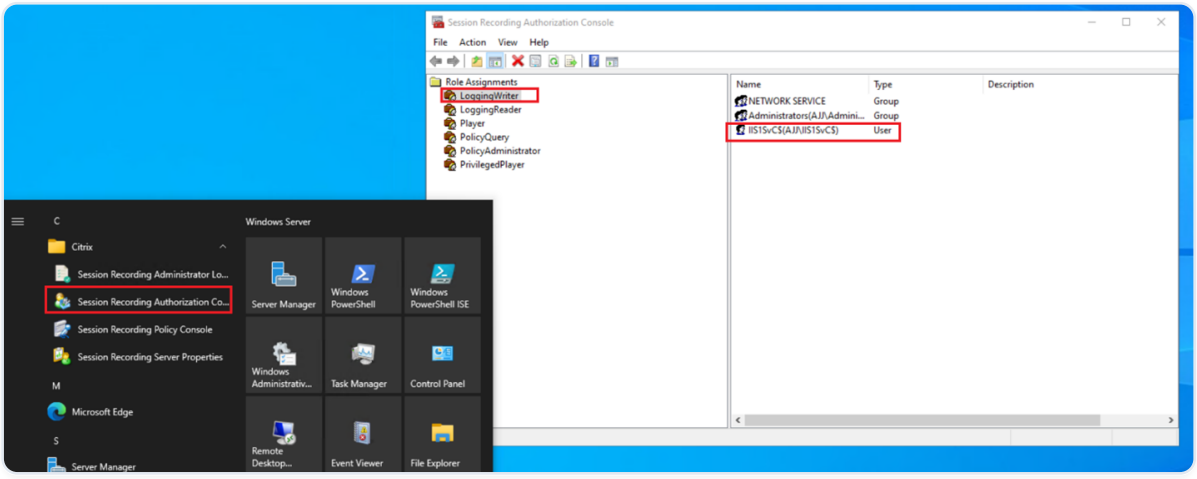
b. Write the SID to the **SessionRecordingAzManStore** file under **\<Session Recording server installation path>\App_Data**.



c. Grant full control permission on the **App-Data** folder to the gMSA.



d. Verify that the gMSA is successfully added to the Session Recording Authorization Console.



Note:

Alternatively, you can use a script similar to the following to add a gMSA to the Session Recording Authorization Console:

```
$account = "IIS1SvC"

$AccountDetail = Get-ADServiceAccount -Identity $account

$accountSid = $AccountDetail.SID.Value

write-host $accountSid
```

```
$path = "C:\Program
Files\Citrix\SessionRecording\Server\App_Data\SessionRecordingAzMan
Store.xml"

$doc = [xml](Get-Content $path)

$node = $doc.AzAdminManager.AzApplication.AzRole | Where-Object
{$_.Name -eq "LoggingWriter"}

$element = $doc.CreateElement("Member")

$element.InnerText = $accountSid

$node.AppendChild($element)

$doc.Save($path)
```

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.

Event ID table

The following table provides a quick reference for specific event IDs and their meanings. Each event ID includes a description and a severity level to help understand the nature of the event and the appropriate response. If any of these events occur, you can check them in the Windows Event Viewer. Event logs related to the Session Recording administration components can be viewed on the Session Recording server. Event logs generated by the Session Recording agent can be viewed on the VDA. Event logs generated by the Session Recording player can be viewed on the machine where the player is installed.

EVENT ID	DESCRIPTION	LEVEL
2001	Database Connection Established	Information
2002	Service Start Success	Information
2003	Service Stop Success	Information
2004	Error: Service Start Failure	Error
2005	Error: Data Lost For File	Error

EVENT ID	DESCRIPTION	LEVEL
2006	Warning: Certificate Approaching Expiry (Days)	Warning
2007	Warning: Certificate Approaching Expiry (Hours)	Warning
2008	Warning: Certificate Approaching Expiry (Minutes)	Warning
2009	Error: No Active Policy Document	Error
2010	Error: Unknown Active Policy Document	Error
2011	Error: Unsupported Active Policy Document Version	Error
2012	Error: Method Loading Active Policy Document	Error
2013	Error: Failed Verify Generated Signature	Error
2014	Error: Failed Verify CAS Configuration	Error
2015	Audit: Successful File Download	Audit
2016	Audit: Successful File Query	Audit
2017	Audit: Successful New Policy Document	Audit
2018	Audit: Successful Load Policy Document	Audit
2019	Audit: Successful Save Policy Document	Audit

EVENT ID	DESCRIPTION	LEVEL
2020	Audit: Successful Copy Policy Document	Audit
2021	Audit: Successful Rename Policy Document	Audit
2022	Audit: Successful Set Policy Document Description	Audit
2023	Audit: Successful Set Policy Document Read Only	Audit
2024	Audit: Successful Delete Policy Document	Audit
2025	Audit: Successful Set Active Policy Document	Audit
2026	Message Rejected User On Role Based Security	Information
2027	Error: Method Principal Access Check	Error
2028	Error: Method Setting Database Connection String	Error
2029	Error: Method Get Time Adjustment	Error
2030	Error: Method Searching Files	Error
2031	Error: Method Retrieving Live File Updates	Error
2032	Error: Method Opening For Encryption	Error
2033	Error: Method Opening For Reading	Error

EVENT ID	DESCRIPTION	LEVEL
2034	Error: Method Retrieving Encryption Percent Complete	Error
2035	Error: Method Reading File	Error
2036	Error: Method Querying File	Error
2037	Error: Method Closing File	Error
2038	Error: Method Enumerating Account Authorities	Error
2039	Error: Method Enumerating User Names	Error
2040	Error: Method Enumerating Group Names	Error
2041	Error: Method Enumerating Client Names	Error
2042	Error: Method Enumerating Client Addresses	Error
2043	Error: Method Enumerating Farm Names	Error
2044	Error: Method Enumerating Zone Names	Error
2045	Error: Method Enumerating Server Names For Farm	Error
2046	Error: Method Enumerating Server Names For Farm And Zone	Error
2047	Error: Method Enumerating Server Names For Farm And Delivery Group	Error

EVENT ID	DESCRIPTION	LEVEL
2048	Error: Method Enumerating Application Names	Error
2049	Error: Method Enumerating EventType Names	Error
2050	Error: Method Loading Policy Console Config File	Error
2051	Error: Method Saving Policy Console Config File	Error
2052	Error: Method Enumerating Policy Documents	Error
2053	Error: Method Getting Policy Document	Error
2054	Error: Method Creating New Policy Document	Error
2055	Error: Method Loading Policy Document	Error
2056	Error: Method Saving Policy Document	Error
2057	Error: Method Copying Policy Document	Error
2058	Error: Method Renaming Policy Document	Error
2059	Error: Method Setting Policy Document Description	Error
2060	Error: Method Deleting Policy Document	Error
2061	Error: Method Getting Active Policy Document	Error

EVENT ID	DESCRIPTION	LEVEL
2062	Error: Method Setting Active Policy Document	Error
2063	Error: Method Running Policy Document Test Query	Error
2064	Error: Method Processing Log Service Notification	Error
2065	Error: Method Encrypting	Error
2066	Error: Method Create Directory	Error
2067	Error: Method Receiving Message	Error
2068	Error: Method Create Recorded Session File Writer	Error
2069	Error: Method Reopen Recorded Session File Writer	Error
2070	Error: Method Creating File	Error
2071	Error: Method Open File For Append	Error
2072	Error: Method Removing LRU	Error
2073	Error: Method Getting File Details	Error
2074	Error: Method Removing Expired Readers	Error
2075	Error: Method Deleting File	Error
2076	Error: Method Writing File	Error
2077	Error: Method Writing Signature	Error

EVENT ID	DESCRIPTION	LEVEL
2078	Error: Method Opening Queue	Error
2079	Error: Method Receiving From Queue	Error
2080	Error: Method Establishing Database Connection	Error
2081	Error: Method Removing Message From Queue	Error
2082	Error: Method Load Active Cached Policy Document	Error
2083	Error: Method Init Policy Engine	Error
2084	Error: Method Enum Player User Policy Groups	Error
2085	Error: Method New Player User Policy Group	Error
2086	Error: Method Update Player User Policy Group	Error
2087	Error: Method Delete Player User Policy Group	Error
2088	Error: Method Enum Player User Role Policies	Error
2089	Error: Method New Player User Account Role Policy	Error
2090	Error: Method Delete Player User Account Role Policy	Error
2091	Error: Method Set File Hidden Attribute	Error

EVENT ID	DESCRIPTION	LEVEL
2092	MSMQ storage quota on VDA was exceeded	Error

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.

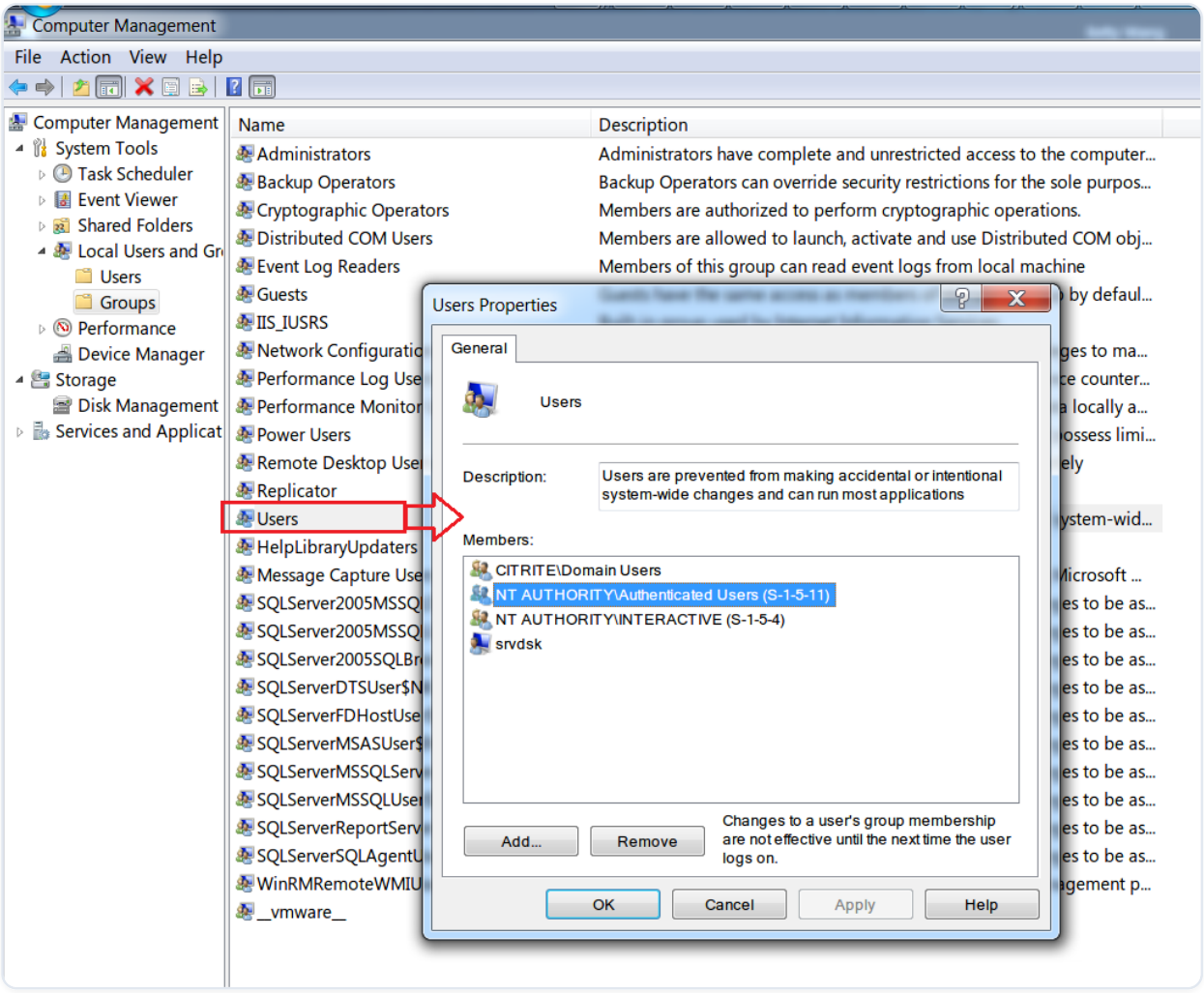
- **The underlying connection was closed. A connection that was expected to be kept alive was closed by the server.** This error means that the Session Recording server is down or unavailable to accept requests. The IIS might be offline or restarted, or the entire server might be offline.

  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.

Check the recording success rate

You can check the recording success rate to learn whether all sessions that match the active recording policy are recorded. The recording success rate is calculated as follows:

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

Prerequisites

- This feature requires the Session Recording server minimum version 2203.

- To obtain site configuration and session data for accurate calculation, you must install the Broker PowerShell Snap-in (Broker_PowerShellSnapIn_x64.msi). You can locate the snap-in on the Citrix Virtual Apps and Desktops ISO (\x64\Citrix Desktop Delivery Controller) and follow the instructions to install it.
- For an on-premises Delivery Controller, install and use the Citrix Virtual Apps and Desktops™ PowerShell SDK. For a Delivery Controller in Citrix Cloud, install and use the Citrix DaaS Remote PowerShell SDK. To determine which SDK to install and use, be aware of the Delivery Controller that you specified when you configured your recording policy.

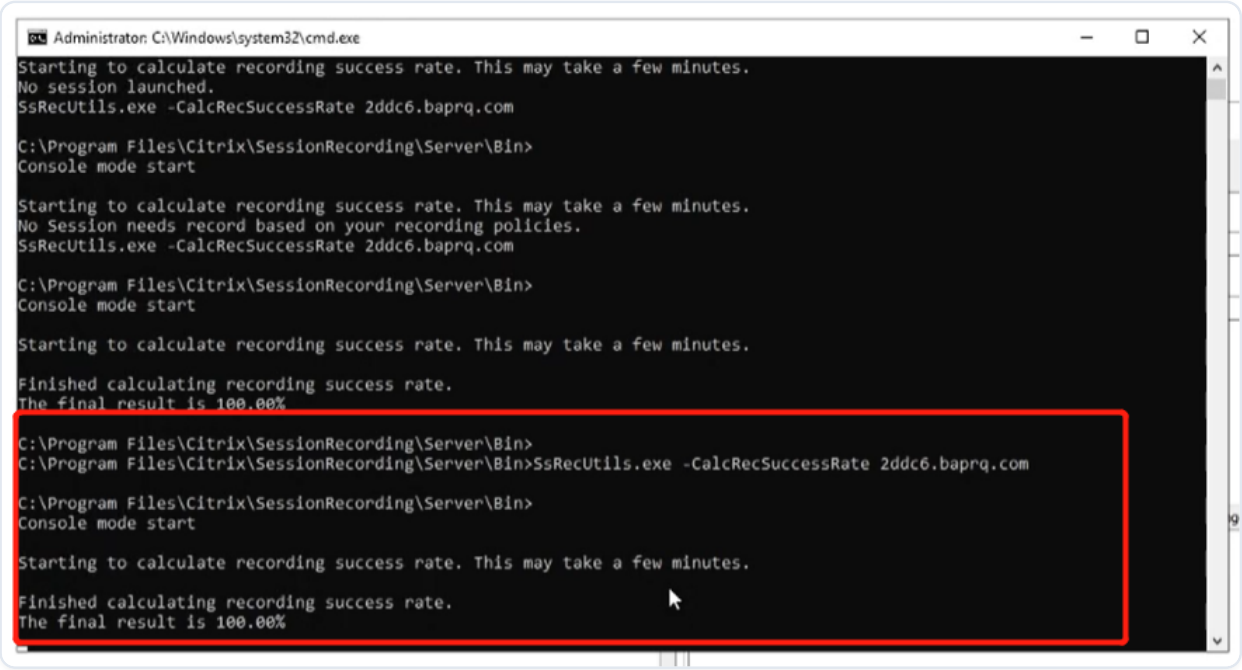
Steps

To check the recording success rate across your deployment, complete the following steps:

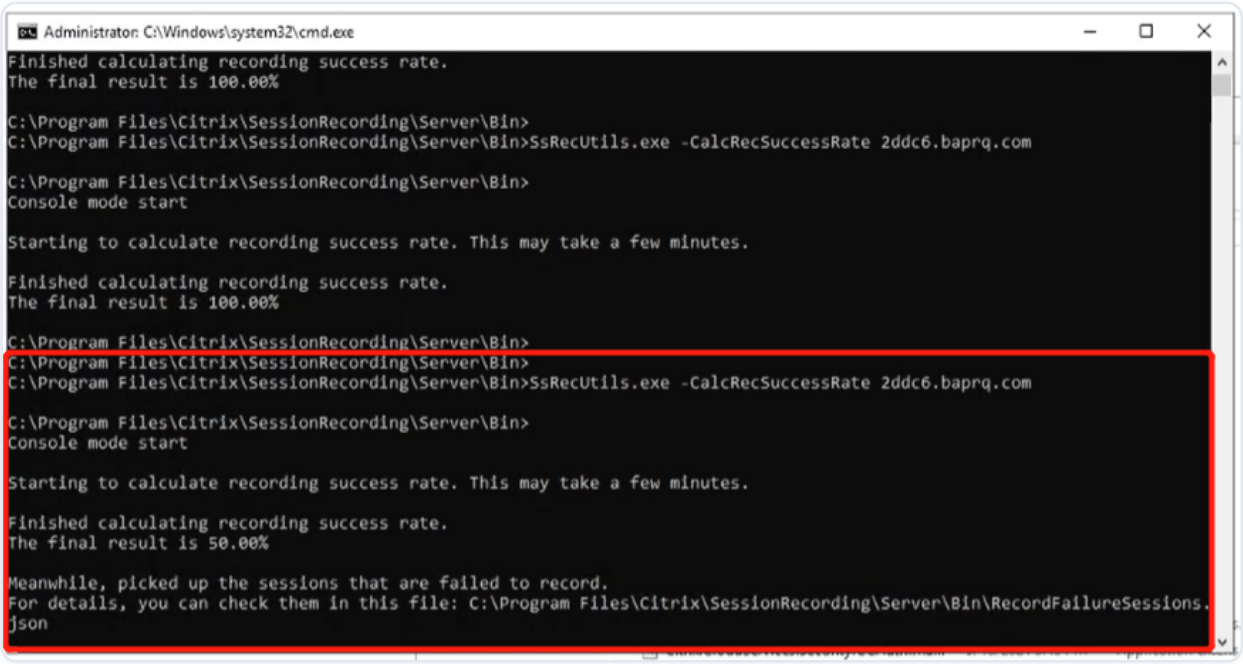
1. Use a domain user account with proper permission to log on to the machine where you have installed the Session Recording server.
2. Start PowerShell and change the current drive to the **<Session Recording server installation path\>\Bin** folder.
3. Run a command based on the type of your deployment:
    - For an on-premises Delivery Controller™, run either of the following commands as needed:
        - If the FQDN of the Session Recording server is the same with the FQDN in the certificate bound to the Session Recording server, run **SsRecUtils.exe -CalcRecSuccessRate <Delivery Controller address\>**.
        - If you have specified a custom domain name with the certificate binding, run **SsRecUtils.exe -CalcRecSuccessRate <Delivery Controller address\> -SRBrokerURL <custom domain name\>**.
    - For a Delivery Controller in Citrix Cloud™, run the following commands in sequence:
        - **Add-PSSnapin Citrix.Broker.Admin.V2**
        - **Set-XDCredentials -CustomerId "<Citrix Cloud customer ID\>" -SecureClientFile "<path to secure client file\>" -ProfileType CloudApi -StoreAs default**
        - **get-xdauthentication**
        - **SsRecUtils.exe -CalcRecSuccessRate CloudDDC**
4. Check the recording success rate. If all sessions that match the currently active recording policy are recorded, the recording success rate is 100%. Otherwise, the recording success rate

is lower than 100% and you are prompted to check failed recordings in a file where session details are provided. For example:

100% recording success rate



50% recording success rate



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-domain-joined machines**. Session Recording is designed to run in a domain environment. If you are not running in an Active Directory or Azure 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 or Azure 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.

Session Recording Data Loss

Event Description

Session Recording – Event 2005 in Event Viewer

Administrators may notice Event 2005 from Citrix Session Recording Storage Manager in the Event Viewer on the Session Recording server. The event message typically appears as:

"Data lost while recording file: VDA = XXX, CtxSessionId = YYY, path = ZZZ, NNN bytes missing."

If the administrator attempts to play the recording file located at the path specified in the event, the playback will indicate that the recording is **incomplete**.

Why did this occur?

There are several possible causes for this issue:

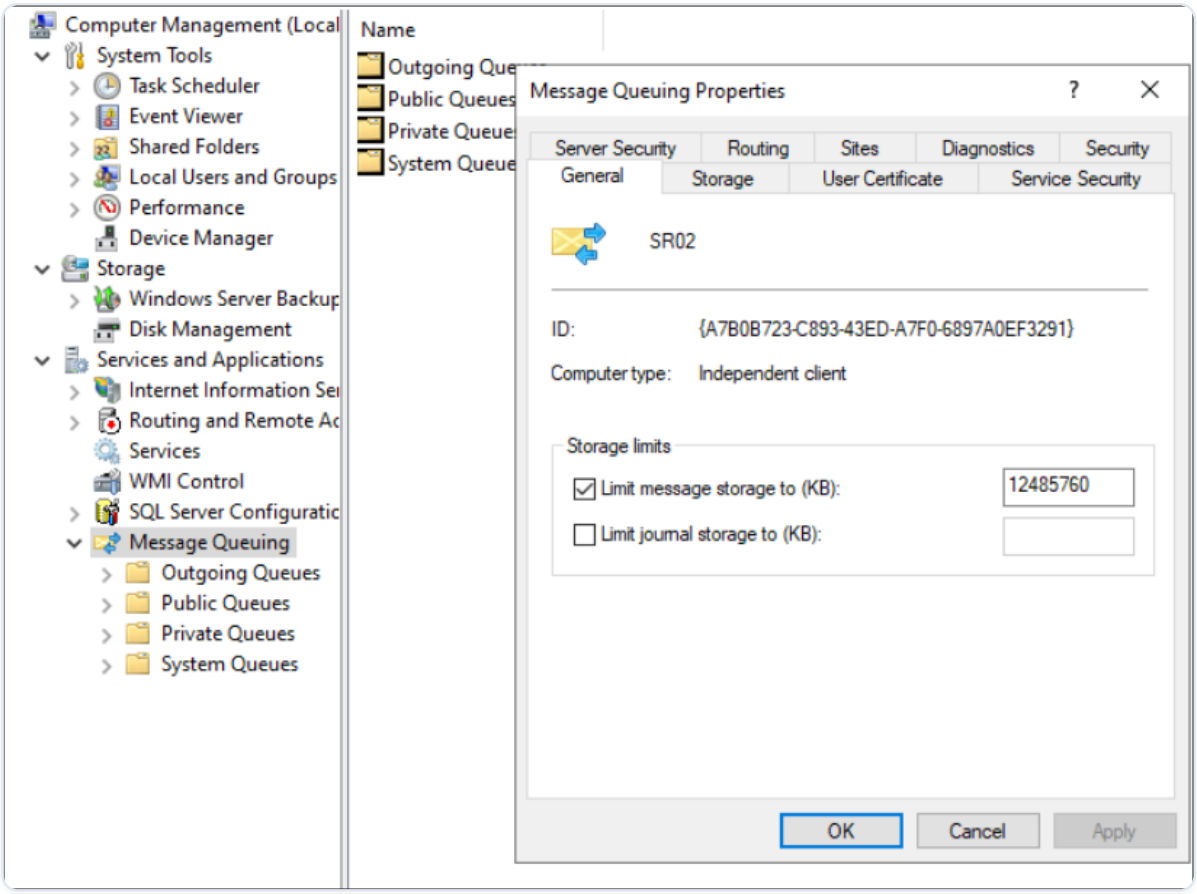
1. Two or more VDAs are configured with the same QMID for MSMQ, which can occur on both persistent and non-persistent VDAs.

2. The QMID on non-persistent VDAs remained unchanged after reboot, which can lead to conflicts.
3. The Session Recording Server is under heavy load and cannot efficiently process a large number of concurrent sessions.

How to identify the issue?

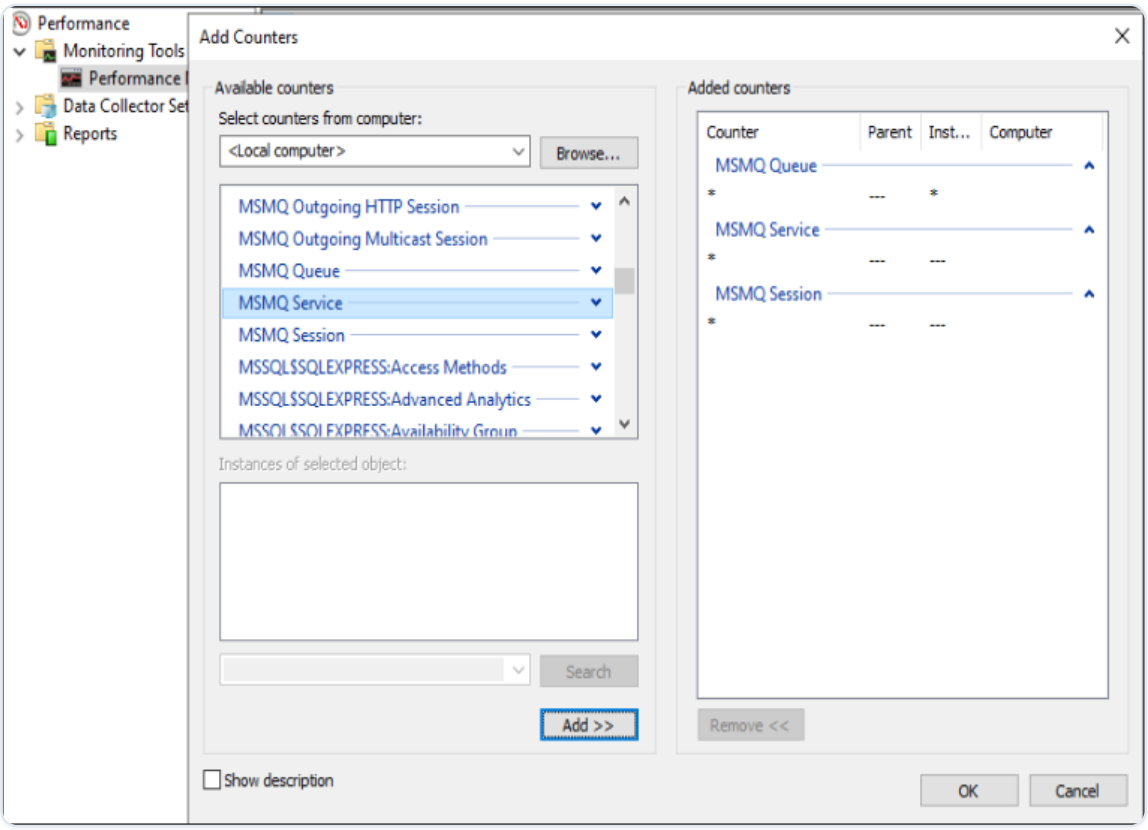
1. Verify the QMID configuration on the VDAs.
    a. For persistent VDAs
        i. check the registry on each machine to verify the QMID configuration.
        `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters\MachineCache\QMId`
        ii. Each VDA should have a unique QMID value to avoid conflicts.
    b. For Non-persistent VDAs
        i. Check the registry on the VDA to verify the QMID.
        ii. After rebooting the same VDA, check the registry again.
        iii. The QMID should be different after the reboot.
2. Verify whether the server is under heavy load.

a. Check the storage limits configured in the MSMQ properties on the Session Recording Server.

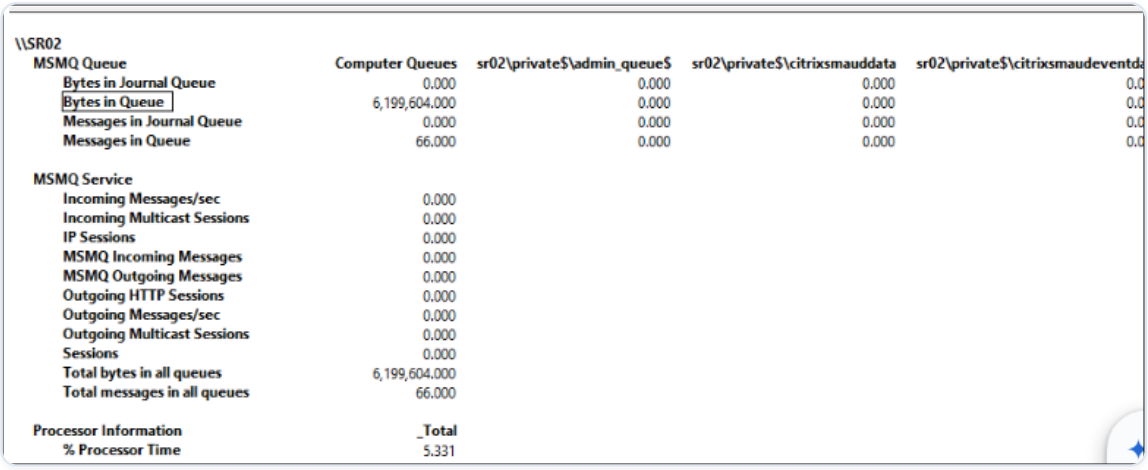


b. Monitor MSMQ resource usage using Performance Monitor.

i. Add the MSMQ counters in the Performance Monitor to track resource usage.



ii. Verify the current data usage within MSMQ.



\\SR02					
MSMQ Queue	Computer Queues	sr02\private$\admin_queue$	sr02\private$\citrixsmauddata	sr02\private$\citrixsmaudeventd	
Bytes in Journal Queue	0.000	0.000	0.000	0.0	
Bytes in Queue	6,199,604.000	0.000	0.000	0.0	
Messages in Journal Queue	0.000	0.000	0.000	0.0	
Messages in Queue	66.000	0.000	0.000	0.0	
MSMQ Service					
Incoming Messages/sec	0.000				
Incoming Multicast Sessions	0.000				
IP Sessions	0.000				
MSMQ Incoming Messages	0.000				
MSMQ Outgoing Messages	0.000				
Outgoing HTTP Sessions	0.000				
Outgoing Messages/sec	0.000				
Outgoing Multicast Sessions	0.000				
Sessions	0.000				
Total bytes in all queues	6,199,604.000				
Total messages in all queues	66.000				
Processor Information	_Total				
% Processor Time	5.331				

iii. Check whether the MSMQ data size is approaching the configured quota limit. If it is, the server may be overloaded.

How to solve it?

The following items outline how to resolve the issue.

1. All VDAs using the Session Recording Agent must be assigned distinct QMIDs for MSMQ.
    a. For persistent VDAs, the QMID for MSMQ only needs to be set once.
    b. For non-persistent VDAs, the QMID for MSMQ needs to be set during Windows startup

c. How to modify the QMID on a VDA

   i. Manually modify the QMID: Install, upgrade, and uninstall

   ii. The latest Citrix Provisioning Services automatically update the QMID for MSMQ on each VDA startup since CVAD 2511. Create machine catalogs

   iii. Image optimization tools or custom-defined scripts can be used to generate a new QMID for MSMQ during Windows startup.

d. Additionally, for non-persistent VDAs, set the startup type of both the **Session Recording Agent Service** and the **Citrix Session Recording Monitor Service to Automatic (Delayed Start)** in the Windows Services configuration.



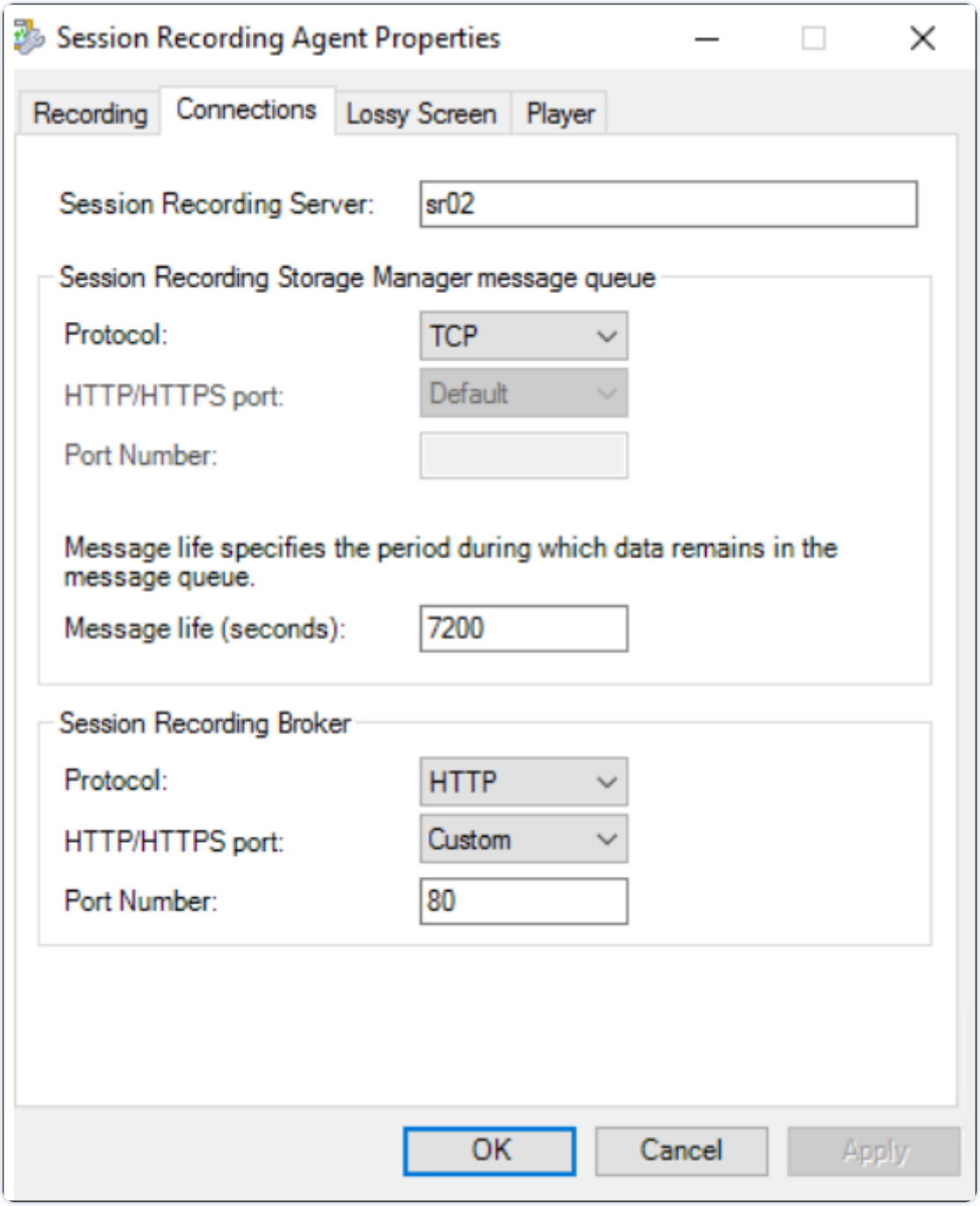
2. The Session Recording Server is overloaded. The supported session capacity of the Session Recording Server can vary significantly depending on the hardware configuration. By default, it can handle up to 2,000 concurrent sessions. However, if the server is equipped with more than 16 GB of RAM and SSD storage, the capacity can be higher. To help resolve overload issues:

   a. Increase the main memory quota on the machine, then raise the MSMQ storage limit.

      Ensure that the total available main memory is at least 1.5 times the configured MSMQ storage limit.

      > **Note:**
      >
      > The total MSMQ storage limit should always remain less than the total physical memory.
      >
      > After making changes, MSMQ on the Session Recording Server must be restarted. The Session Recording Service will restart automatically as a result.
      >
      > This process will not result in any loss of session data.

   b. Adjust the message lifetime in the Session Recording Agent properties. Consider doubling the current value to allow more time for message processing and reduce data loss risks.



You can configure this setting via the following registry key on the VDA:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent\MsmqMessageLifeInSeconds`

Set the value (in seconds) based on your environment's needs.

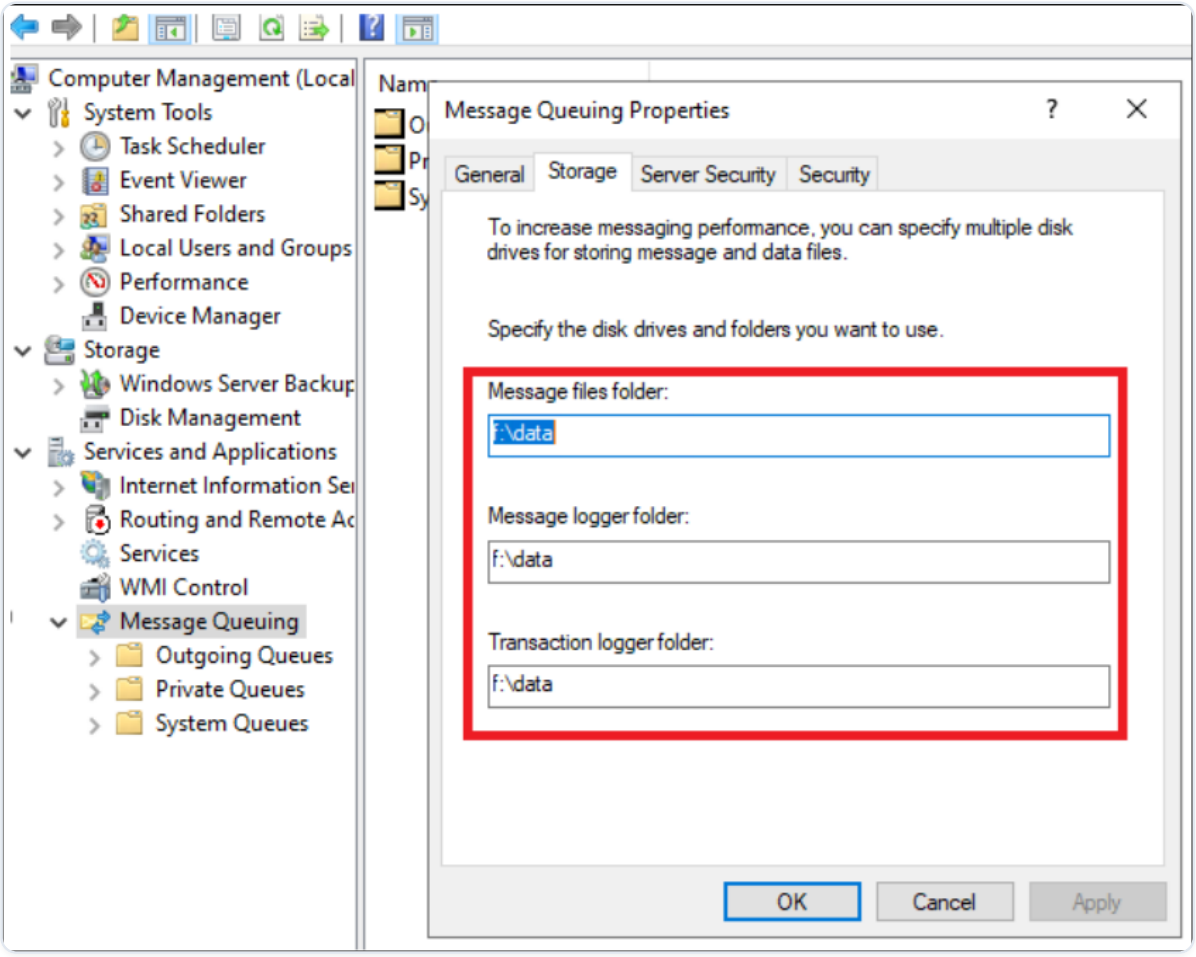
> **Note:**
>
> After making changes, the Session Recording Agent must be restarted.

> This action will result in loss of session data for any live session.

> Please ensure that this operation is scheduled during a maintenance window.

c. Change the Message folder to a different drive with a disk(SSD) IOPS capacity of more than 3000 for MSMQ on all Session Recording Server machines.

   This will help speed up processing and can improve performance by up to 50%.



   https://learn.microsoft.com/en-us/previous-versions/troubleshoot/msmq/optimize-message-queuing-performance

d. If the above steps do not resolve the issue, the recommended solution is to add an additional Session Recording Server to distribute the load.

   For guidance, refer to the official documentation on configuring load balancing in an existing deployment: Citrix Documentation – Configure Load Balancing

Configuring Always On Tracing (AOT) for Session Recording

The AOT Log Server acts as a centralized destination for collecting and storing Always On Tracing (AOT) logs from various Citrix components. For more information, see Citrix Always on Tracing.

To integrate and utilize AOT within Session Recording, you must configure the Session Recording Server. For more information, see Uploading the AOT logs from CVAD Core Components.

Record Linux sessions (preview)

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 (preview) 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 2511 documentation. To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	DESCRIPTION
29 Dec 2025	Session Recording 2511	For more information, see What's new.