citrix

Session Recording 2411

Contents

Session Recording 2411	5
What's new	5
Fixed issues	8
Known issues	9
Third party notices	11
System requirements	11
Get started	14
Plan your deployment	16
Security recommendations	22
Scalability considerations	28
Install, upgrade, and uninstall	40
Dynamic session recording	104
Configure	109
Configure settings on the Session Recording agent	110
Enable or disable recording	110
Enable or disable lossy screen recording	115
Enable fast seeking	119
Configure the connection to the Session Recording server	121
Change your communication protocol	122
Configure settings on the Session Recording server	124
Authorize users	124
CEIP and Google Analytics	126
Customize recording notification messages	130

Enable or disable digital signing	134
Event response reports	135
Session recording storage reports	138
Specify file size for recordings	142
Specify recording storage locations	145
Policies	155
Configure session recording policies	157
Configure recording viewing policies	169
Configure event detection policies	174
Configure event response policies	206
High availability and load balancing	217
Load balance Session Recording servers	218
Configure database high availability	221
View recordings	222
Session Recording player	223
Launch the Session Recording Player	223
Enable or disable live session playback	226
Enable or disable playback protection	227
Search for recordings	227
Place access restrictions on recordings	229
Open and play recordings	232
Cache recordings	239
Highlight idle periods	240
Use events and bookmarks	241

Session Recording web player	243
Access the web player	243
Hide or show content on the web player home page	248
Search for recordings	251
Place access restrictions on recordings	252
Open and play recordings	255
Configure preferences	260
Increase the transport packet size for the web player	261
Highlight idle periods	261
Use events and comments	263
Share recordings as links	265
View graphical event statistics for each recording	271
View data points related to each recorded session	275
View diagnostic logging	276
Manage recordings	281
Manage and query administrator logging	293
Best practices	301
Configure load balancing in an existing deployment	301
Deploy and load balance Session Recording in Azure	349
Configure Group Service Managed Account (gMSA) support for Session Recording	382
Troubleshoot	399
Event ID table	400
Installation of server components fails	405
Test connection to the database fails during install	405

Agent cannot connect to the server	405
Server cannot connect to the database	407
Check the recording success rate	408
Sessions are not recording	410
Unable to view live session playback	411
Recordings are corrupted or incomplete	412
Verify component connections	412
Search for recordings using the player fails	415
Record Linux sessions (preview)	418

Session Recording 2411

November 11, 2024

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

December 4, 2024

What's new in 2411

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

Important note about upgrading to version 2411:

To prevent session recording failures due to incomplete upgrades of Session Recording agents, follow these steps when upgrading to 2411:

- 1. Upgrade each Session Recording server to version 2411.
- 2. Enable remote access using .NET Remoting with the following command:

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

- 3. Upgrade each Session Recording agent to version 2411.
- 4. After all Session Recording agents are upgraded, disable remote access using .NET Remoting with the following command:

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

Group Service Managed Account (gMSA) support for Session Recording

Session Recording now supports **Group Service Managed Account (gMSA)** to simplify service principal name (SPN) management for services running on multiple servers. This feature enhances security and simplifies the management of service accounts. For more information, see the best practice article: Configure Group Service Managed Accounts (gMSA) support for Session Recording.

Support for Microsoft Entra ID authentication

In addition to SQL Server authentication, Session Recording now supports Entra ID authentication for cloud-based SQL databases including Azure SQL Database and Azure SQL Managed Instance. To enable Entra ID authentication, include the AADPASSWORD parameter and set it to 1 when installing the Session Recording database through the command line. For more information, see Install, upgrade, and uninstall.

Support for installing databases on separate Instances

You can now install the Session Recording database and Session Recording admin logging database on separate instances. To enable this feature, complete the following steps before installing the data-

bases:

- 1. Go to the machine where the Session Recording server is installed.
- 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. 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 through either a GUI or command line, the admin logging database is installed on the separate instance specified by the SmAudDatabaseLoggingInstance registry value. For more information about Session Recording installation, see Install, upgrade, and uninstall.

Capturing printing activities in recorded sessions is now generally available

You can capture printing activities that occur during recorded sessions and tag them as events in recordings for later search and playback. The feature is now generally available and has been enhanced to capture the full paths of printed files. For more information, see Configure event detection policies.

Enhanced diagnostic logging

More types of diagnostic logs, beyond message queue quota exceedance, can now be detected on the Virtual Delivery Agents (VDAs) and sent to the Session Recording server. Previously, diagnostic logs were visible in the Windows Event Viewer, but they are now visible in the Session Recording web player. For more information, see View diagnostic logging.

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 2407 Current Releases (CR), see What's new history.

Fixed issues

October 25, 2024

Compared with: Session Recording 2407

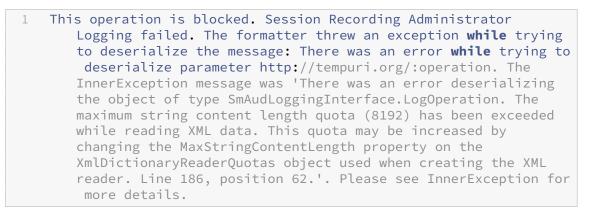
Session Recording 2411 adds the following fixes:

- The H.264 package dropping feature might not work as expected. [SRT-13478]
- You might encounter the error **USP_AddLoggingEventLogging is missing** in Windows Event Viewer after upgrading Session Recording from a version earlier than 2009. [SRT-12913]
- Attempts to install additional Session Recording servers and connect them to the same Session Recording database might fail when SQL server authentication is selected. The issue doesn't affect the first Session Recording server installed and connected to the Session Recording database, but it does affect subsequent Session Recording servers. To work around the issue, you can install the additional Session Recording servers using a command similar to the following:



[SRT-12976]

• Attempts to save the Session Recording policy settings might fail and you can obtain the following error message by using CDFControl:



[SRT-11791]

• When the DNS name differs from the domain name, the sr_lb_map.xml file generated using SrServerConfigurationSync.ps1 contains incorrect Fully Qualified Domain Names (FQDNs) for the redirection mapping of Microsoft Message Queuing (MSMQ) in load-balanced deployments. [SRT-13158]

When the SQL database reaches its saturation capacity, recording files become corrupted due to missing data in the file headers, resulting in the message "The file is not a recorded session file or is possibly corrupt." when played in the Session Recording player. This issue is fixed in the 2411 release. For corrupted files prior to 2411, you can run the ICLDB REPAIR [/LISTFILES] [/RECURSIVE] [/L] [/F] [/S] [/?] [<file>] [<directory>] command to repair them. Repaired files can be found at %AppData%\Citrix\SessionRecording\Restore. [SRT-12442]

Known issues

December 2, 2024

The following issues have been identified in this release:

- 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:
 - 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\C
 - 2. Set the DWORD values to 65534 in decimal.
 - 3. Restart the IIS server machine.

[SRT-13739]

- 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. [CVADHELP-26534]
- 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. [CVADHELP-24365]
- 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:

1 Add-Type -AssemblyName System.data

```
$registryKey = [Microsoft.Win32.Registry]::LocalMachine.
       OpenSubKey("SOFTWARE\\Citrix\\SmartAuditor\\Server")
    $dbName = $registryKey.GetValue("DatabaseName")
3
   $dbInstance = $registryKey.GetValue("SmAudDatabaseInstance")
4
   write-host "Connecting to $dbInstance\$dbName"
5
6
    # Connect db
    $conn = New-Object System.Data.SqlClient.SqlConnection
7
    $conn.ConnectionString = "workstation id=.;packet size=4096;
8
       integrated security=SSPI;data source=$dbInstance;persist
       security info=True; initial catalog=$dbName"
9
    $conn.0pen()
    $cmd = $conn.CreateCommand()
10
    $cmd.CommandText = "use [$dbName];if not exists(select * from [
11
       dbo].[EndReason] where ID=5) begin insert [dbo].[EndReason]
       values (5, 'Dormant') end"
12
    $cmd.ExecuteNonQuery()
```

[SRT-11119]

- 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. [SRT-10514]
- 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. [SRT-10130]
- 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. [SRT-5769]
- 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. [SRT-5624]
- 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. [SRT-4546]
- 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. [#528678]

Third party notices

October 10, 2024

Session Recording Version 2411 (PDF Download)

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

System requirements

December 4, 2024

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

Supported Microsoft SQL Server versions:

- Microsoft SQL Server 2022 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2019 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2017 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2016 SP2 Enterprise, Express, and Standard editions

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

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 Internet Explorer 11

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, minimum version 1607
- Windows 10 Enterprise for Virtual Desktops

Requirements:

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

Note:

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

Session Recording player

Supported operating systems:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows 11
- 64-bit Windows 10, minimum version 1607

Requirement: .NET Framework 4.7.2

Note:

On 32-bit Windows 10, you can install the player only by using the SessionRecordingPlayer.msi

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

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

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

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

Get started

June 21, 2024

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 singlesession 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.

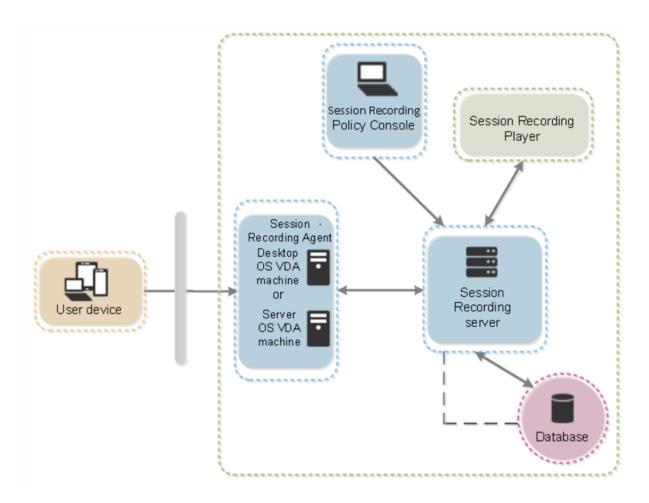
Tip:

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

November 13, 2024

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

Session Recording 2411

Source	Destination	Туре	Port	Details
Virtual Delivery	Session	ТСР	80, 443	Communication
Agent	Recording server			between the
				Session
				Recording agent
				installed on
				Virtual Delivery
				Agent and the
				Session
				Recording server
				Default
				installation uses
				HTTPS/SSL to
				secure
				communications
				If SSL is not
				configured, use
				HTTP.

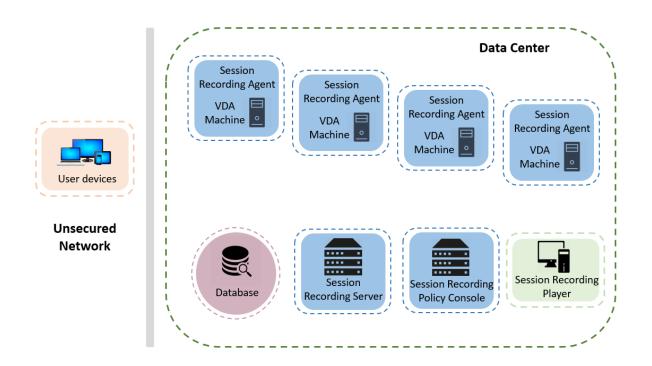
Session Recording 2411

Source	Destination	Туре	Port	Details
Virtual Delivery	Session	ТСР	1801	By default,
Agent	Recording server			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	Session	ТСР	80, 443	Communication
Recording policy	Recording server			between the
console				server where the
				Session
				Recording policy
				console is
				installed and the
				Session
				Recording server.

Source	Destination	Туре	Port	Details
Session	Session	TCP	80, 443	Communication
Recording player	Recording server			between the
				workstation
				where the
				Session
				Recording player
				is installed and
				the Session
				Recording server.
Session	Microsoft SQL	ТСР	1433	Connection to
Recording server	Server			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 Out-

look is running, Word also is recorded. Conversely, if the active policy doesn't specify to record Word and the user launches Word before Outlook, Outlook is not recorded.

- Though you can install the Session Recording server on a Delivery Controller, we don't recommend it because of performance issues.
- You can install the Session Recording Policy Console on a Delivery Controller.
- You can install both the Session Recording server and the Session Recording Policy Console on the same system.
- Ensure that the NetBIOS name of the Session Recording server does not exceed the limit of 15 characters. Microsoft has a 15-character limit on the host name length.
- PowerShell 5.1 or later is required for custom event logging. Upgrade PowerShell if you install the Session Recording agent on Windows Server 2012 R2 that has PowerShell 4.0 installed. Failure to comply can cause failed API calls.
- For step-by-step instructions on deploying and configuring the Citrix Session Recording and Citrix Session Recording service, see this Citrix Tech Zone article: POC Guide: Citrix Session Recording.

Security recommendations

November 20, 2024

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.

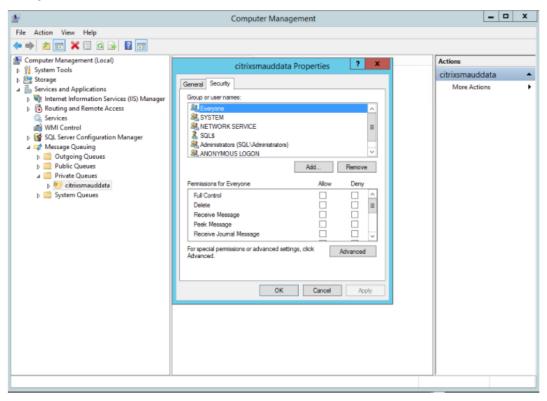
Tip:

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.

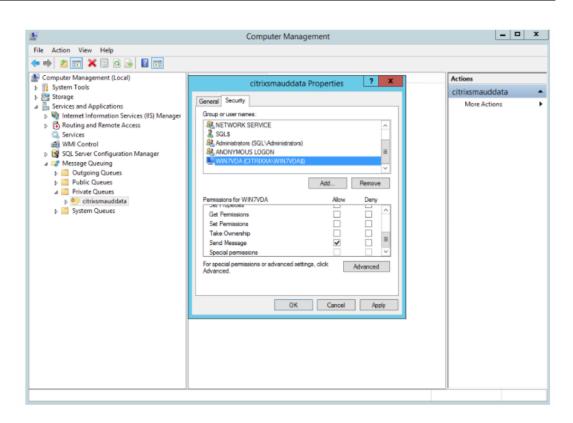
- Ensure that you properly isolate the different administrator roles in the corporate network, in the Session Recording system, or on individual machines. By not doing so, security threats that can impact the system functionality or abuse the system might occur. We recommend that you assign different 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:
 - 1. Right-click My Computer, and then select Properties.

- 2. Click the **Advanced** tab, and then under **Startup and Recovery**, click **Settings**.
- 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
 - $\cdot \ {\sf Registry values within {\sf HKEY_LOCAL_MACHINE}SOFTWARE} \\ {\sf Citrix} \\ {\sf SmartAuditor} \\ {\sf Server} \\ {\sf Server} \\ {\sf Supple and {\sf S$
 - * 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.
 - 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.

- From the Windows Start menu on each Session Recording server, open Administrative Tools > Computer Management.
- 3. Open Services and Applications > Message Queuing > Private Queues.
- 4. Click the private queue **citrixsmauddata** to open the **Properties** page and select the **Security** tab.



5. 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:
 - 1. Using the Microsoft Group Policy Editor, navigate to **Computer Configuration > Admin**istrative Templates > Network > SSL Configuration Settings.
 - 2. Set the **SSL Cipher Suite Order** policy to **Enabled**. By default, this policy is set to **Not Configured**.
 - 3. 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:

- 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\ and HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319.
 - e) Restart the machine.
- Log on to the machine hosting the Session Recording policy console. Apply the latest hotfix rollup of .NET Framework, and set strong cryptography for .NET Framework (version 4 or later). The method for setting strong cryptography is the same as substeps 1–4 and 1–5. You can omit these steps if you choose to install the Session Recording policy console on the same computer as the Session Recording server.

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

Scalability considerations

October 24, 2024

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

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

Why Session Recording scales well

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

• Small file size

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

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

	🗘 Create Policy
	Edit Setting
0 nview Settings Assigned to	Use video codec for compression
Use video codec for compression User setting - ICA\Graphics For actively changing regions (Default: Use when preferred)	Value: For actively changing regions * Use default value: Use when preferred
	★ Applies to the following VDA versions Virtual Delivery Agent: 7.6 Server OS, 7.6 Desktop OS, 7.7 Server OS, 7.7 Desktop OS, 7.8 Server OS, 7.8 Desktop OS, 7.9 Server OS, 7.9 Desktop OS, 7.11 Server OS, 7.11 Desktop OS, 7.12 Server OS, 7.12 Desktop OS, 7.13 Server OS, 7.10 Desktop OS, 7.14 Server OS, 7.14 Desktop OS, 7.15 Server OS, 7.15 Desktop OS, 7.16 Server OS, 7.16 Desktop OS, 7.17 Desktop OS, 7.15 Server OS, 7.18 Desktop OS, 7.16 Server OS, 7.16 Desktop OS, 7.17 Desktop OS, 7.17 Desktop OS, 7.18 Desktop OS, 1808 Server OS, 1808 Desktop OS, 1811 Server OS, 1811 Desktop OS, 1903 Single-session OS, 1902 Single-session OS
	 Description This setting is available only on VDA versions XenApp and XenDesktop 7.6 Feature Pack 3 and later.
	Allows use of a video codec to compress graphics when video decoding is available on the endpoint. When 'For the entire screen' is chosen the video codec will be applied as the default codec for all content (some small images and text will be optimized and sent (ossiessly). When 'For actively changing regions' is selected the video codec will be used for areas where there is constant change on the screen, other data will use still image compression and bitmap caching. When video decoding is not available on the endpoint, or when you specify 'Do not use', a combination of still image compression and bitmap caching is used. When 'Use when preferred' is selected, the system chooses, based on various factors. The results may vary between versions as the selection method is enhanced.
	Select 'Do not use' to optimize for server CPU load and for cases that do not have a lot of server- rendered video or other graphically intense applications.
	Select 'For the entire screen' to optimize for cases with heavy use of server-rendered video and 3D graphics, especially in low bandwidth.
	OK Cancel

• Low processing required to generate files

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

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

Estimate data input and processing rates

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

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

than the data input rate.

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

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

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

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

Bursts and faults

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

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

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

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

- Adding more disk space to each server, especially the Session Recording server, and making it available to MSMQ can increase the tolerance to bursts and faults.
- It is important to configure the Message Life setting for each Session Recording agent to an appropriate level (on the **Connections** tab in Session Recording agent Properties). The default value is 7,200 seconds (two hours). It means that each recorded data message has two hours to reach the Storage Manager before the Storage Manager discards it and damages the recording file. With more disk space available (or fewer sessions to record), you can choose to increase this value. The maximum value is 365 days.

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

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

Design for spare capacity

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

Backlogs and live playback

Live playback is when a reviewer opens a session recording for playback while the session is still active. During live playback, the responsible Session Recording agent switches to a streaming mode for that session. Recording data is sent immediately to the Storage Manager without internal buffering. Because the recording file is constantly updated, the player can continue to be fed with the latest data from the live session. However, data sent from the agent to the Storage Manager is through MSMQ, so the queuing rules described earlier apply. A problem can occur in this scenario. When MSMQ is backlogged, the new recorded data available for live playback is queued like all other data messages. The reviewer can still play the file, but viewing the latest live recorded data is delayed. If live playback is an important feature for reviewers, ensure a low probability of backlog. You can design spare capacity and fault tolerance into your deployment.

System scalability

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

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

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

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

Measuring throughput

You can measure the throughput of recorded session data from the sending VDA to the receiving Session Recording server. A simple and effective approach is to observe the size of recording files and the rate at which disk space on the Session Recording server is being consumed. The volume of data written to disk closely reflects the volume of network traffic being generated. The Windows Performance Monitor tool (perfmon.exe) has standard system counters that you can observe in addition to some counters provided by Session Recording. Counters can be used to measure throughput, and identify bottlenecks and system problems. The following table outlines some of the most useful performance counters.

Performance Object	Counter Name	Description
Citrix Session Recording Agent	Active Recording Count	The number of sessions that are currently being recorded on a particular VDA.
Citrix Session Recording Agent	Bytes read from the Session Recording Driver	The number of bytes read from the kernel components responsible for acquiring session data. Useful for determining how much data a single VDA generates for all sessions recorded on that server.
Citrix Session Recording Storage Manager	Active Recording Count	Similar to the Citrix Session Recording agent counter except for the Session Recording server. Indicates the total number of sessions currently being recorded for all servers.

Performance Object	Counter Name	Description
Citrix Session Recording Storage Manager	Message bytes/sec	The throughput of all recorded sessions. Can be used to determine the rate at which the Storage Manager is processing data. If MSMQ is backlogged with messages, the Storage Manager runs at full speed. This value can be used to indicate the maximum processing rate of the Storage Manager.
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.

Performance Object	Counter Name	Description
Network Interface	Bytes Total/sec	Can be used to measure on
		both sides of the link to
		observe how much data is
		generated when sessions are
		recorded. When measured on
		the Session Recording server,
		this counter indicates the rate
		at which incoming data is
		received. Contrasts with the
		Citrix Session Recording
		Storage Manager
		Message bytes/sec
		counter that measures the
		processing rate of data. If the
		network rate is greater than
		this value, messages build in
		the message queue.
Processor	% Processor Time	Worth monitoring even though
		CPU is unlikely to be a
		bottleneck.

Session Recording server hardware

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

Scaling up

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

Scaling out

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

Network capacity

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

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

Storage

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

Store data on a RAID or a SAN.

Note:

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

For a local drive setup, aim for a disk controller with built-in cache memory. Caching allows the controller to use elevator sorting during write-back. It minimizes disk head movement and ensures that write operations are completed without waiting for the physical disk operation to complete. It can improve write performance significantly at a minimal extra cost. Caching does however raise the problem of data loss after a power failure. To ensure the integrity of data and the file system, consider a battery backup facility for the caching disk controller. Consider using a suitable RAID storage solution. There are many RAID levels available depending on performance and redundancy requirements. The following table specifies each of the RAID levels and how applicable each standard is to Session Recording.

	-	Minimum Number of	_
RAID Level	Туре	Disks	Description
RAID 0	Striped set without	2	Provides high
	parity		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	2	No performance gain
	parity		over one disk, making
			it a relatively
			expensive solution.
			Use this solution only
			if a high level of
			redundancy is
			required.

Session Recording 2411

		Minimum Numbe	er of
RAID Level	Туре	Disks	Description
RAID 3	Striped set with	3	Provides high write
	dedicated parity		performance with
			redundancy
			characteristics simila
			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 i
			not common.
RAID 5	Striped set with	3	Provides high read
	distributed parity		performance with
			redundancy but at th
			cost of slower write
			performance. RAID 5
			the most common for
			general purpose
			usages. But due to th
			slow write
			performance, RAID 5
			not recommended for
			Session Recording.
			RAID 3 can be
			deployed at a similar
			cost but with better
			write performance.

		Minimum Numb	per of
RAID Level	Туре	Disks	Description
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 blocklevel disk access. To the Session Recording server, the disk array appears as a local drive. SANs are more expensive to set up, but as the disk array is shared, SANs do have the advantage of simplified and centralized management. There are two main types of SAN: Fibre Channel and iSCSI. iSCSI is essentially SCSI over TCP/IP and is gaining popularity over Fibre Channel since the introduction of Gb Ethernet.

Database scalability

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

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

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

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

Install, upgrade, and uninstall

December 17, 2024

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.

Step

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

```
<#
1
2
   .Synopsis
3
       Installs Prereqs for Session Recording Administration
4
   .Description
5
      Supports Windows Server 2025, Windows Server 2022, Windows
           Server 2019.
       Install below windows feature on this machine:
6
7
       -Application Development
       -Security - Windows Authentication
8
       -Management Tools - IIS 6 Management Compatibility
9
```

```
IIS 6 Metabase Compatibility
11
            IIS 6 WMI Compatibility
            IIS 6 Scripting Tools
12
            IIS 6 Management Console
13
14
        -Microsoft Message Queuing (MSMQ), with Active Directory
            integration disabled, and MSMQ HTTP support enabled.
15
    #>
    function AddFeatures($featurename)
16
17
    {
18
19
        try
20
        {
21
            $feature=Get-WindowsFeature | ? {
23
    $_.DisplayName -eq $featurename -or $_.Name -eq $featurename }
24
25
            Add-WindowsFeature $feature
         }
26
27
28
        catch
29
        {
31
            Write-Host "Addition of Windows feature $featurename
                failed"
            Exit 1
32
33
         }
34
        Write-Host "Addition of Windows feature $featurename
35
            succeeded"
     }
38
39
    $system= gwmi win32_operatingSystem | select name
40
    if (-not (($system -Like '*Microsoft Windows Server 2025*') -or (
41
        $system -Like '*Microsoft Windows Server 2022*') -or ($system
       -Like '*Microsoft Windows Server 2019*')))
    {
42
43
44
        Write-Host("This is not a supported server platform.
            Installation aborted.")
45
        Exit
46
     }
47
48
49
    # Start to install Windows feature
    Import-Module ServerManager
51
    AddFeatures('Web-Asp-Net45') #ASP.NET 4.5
52
53
    AddFeatures('Web-Mgmt-Console') #IIS Management Console
    AddFeatures('Web-Windows-Auth') # Windows Authentication
54
55
    AddFeatures('Web-Metabase') #IIS 6 Metabase Compatibility
    AddFeatures('Web-WMI') #IIS 6 WMI Compatibility
```

```
AddFeatures('Web-Lgcy-Scripting')#IIS 6 Scripting Tools
58
    if (($system -Like '*Microsoft Windows Server 2022*') -or (
        $system -Like '*Microsoft Windows Server 2019*'))
59
    {
60
61
        AddFeatures('Web-Lgcy-Mgmt-Console') #IIS 6 Management
            Console
62
     }
63
64
    AddFeatures('MSMQ-HTTP-Support') #MSMQ HTTP Support
    AddFeatures('web-websockets') #IIS Web Sockets
    AddFeatures('NET-WCF-HTTP-Activation45') #http activate
67
```

InstallPrereqsforSessionRecordingAgent.ps1

```
1
    <#
2
    .Synopsis
3
        Installs Prereqs for Session Recording Agent
4
    .Description
5
        Supports Windows Server 2025, Windows Server 2022, Windows
            Server 2019, windows 11, and Windows 10.
        Install below windows feature on this machine:
6
7
        -Microsoft Message Queuing (MSMQ), with Active Directory
            integration disabled, and MSMQ HTTP support enabled.
8
    #>
9
    function AddFeatures($featurename)
10
    ł
11
12
        try
13
        {
14
15
             $feature=Get-WindowsFeature | ? {
    $_.DisplayName -eq $featurename -or $_.Name -eq $featurename }
16
17
             Add-WindowsFeature $feature
18
19
         }
        catch
21
22
        {
23
            Write-Host "Addition of Windows feature $featurename
24
                failed"
25
             Exit 1
26
         }
27
        Write-Host "Addition of Windows feature $featurename
28
            succeeded"
29
     }
31
    # Start to install Windows feature
32
    $system= gwmi win32_operatingSystem | select name
```

```
34
    if (-not (($system -Like '*Microsoft Windows Server 2025*') -or (
        $system -Like '*Microsoft Windows Server 2022*') -or ($system
        -Like '*Microsoft Windows Server 2019*') -or ($system -Like '*
        Microsoft Windows 11*') -or ($system -Like '*Microsoft Windows
         10*')))
    {
37
        Write-Host("This is not a supported platform. Installation
            aborted.")
        Exit
40
     }
41
42
    if ($system -Like '*Microsoft Windows Server*')
43
44
    ł
45
46
        Import-Module ServerManager
47
        AddFeatures('MSMQ') #Message Queuing
        AddFeatures('MSMQ-HTTP-Support')#MSMQ HTTP Support
48
49
     }
50
51
    else
52
    {
53
54
        try
55
        {
56
57
             dism /online /enable-feature /featurename:MSMQ-HTTP /all
         }
        catch
61
        {
62
             Write-Host "Addition of Windows feature MSMQ HTTP Support
63
                 failed"
64
             Exit 1
         }
        write-Host "Addition of Windows feature MSMQ HTTP Support
67
            succeeded"
68
     }
```

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 Power-Shell.

1 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 Power-Shell.

1 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:

Before installing the Session Recording Administration components on Windows Server where TLS 1.0 is disabled and the version of the .NET Framework is earlier than 4.6, complete the following steps:

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

For more information, see Transport Layer Security (TLS) best practices with the .NET Framework.

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

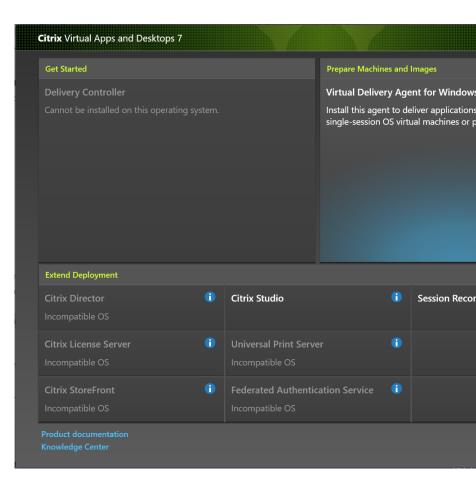
- 1. Use your Citrix account credentials to access the Citrix Virtual Apps and Desktops download page and download the product ISO file. Unzip the ISO file or burn a DVD of it.
- Use a local administrator account to log on to the machine where you are installing the Session Recording Administration components.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

• Hybi	iver applications and desktops to any user, anywhere rid cloud, cloud and enterprise provisioning ralized and flexible management
Mana	age your delivery according to your needs:
	irtual Apps Deliver applications
	citrix

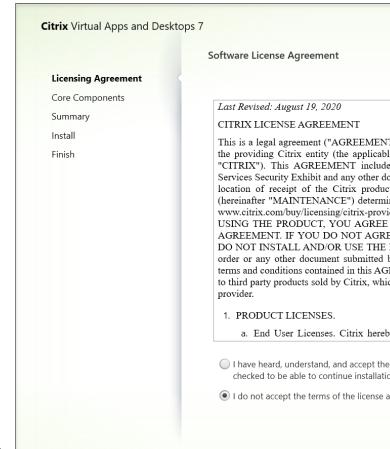
Step 2: Choose which product to install

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



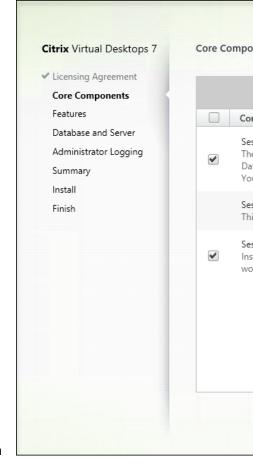
Step 3: Select Session Recording

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**.



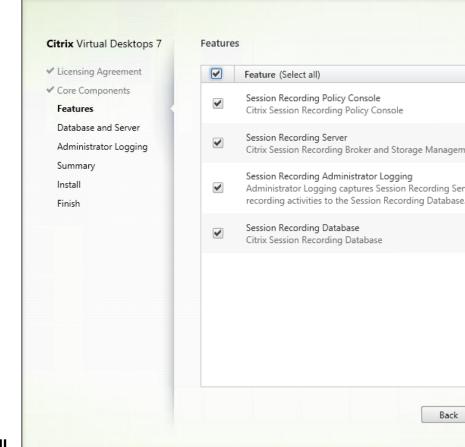
Step 5: Select the components to install and the installation location

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.

Licensing Agreement	
Core Components Features	Location: C:\Program Files\Citrix Change
	Component (Select all)
Database and Server Administrator Logging Summary Install	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.
Finish	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.



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.

	Features
Licensing Agreement	Feature (Select all)
Core Components	1
Features	Session Recording Policy Console Citrix Session Recording Policy Console
Summary	Session Recording Server
Install Finish	Citrix Session Recording Broker and Storage Management.
rmisn	
	Back Next Cancel
Citrix Virtual Apps and Deskto	Features
Core Components	Feature (Select all)
	Session Recording Policy Console Citrix Session Recording Policy Console
Features	
Features Database and Server Summary Install	Session Recording Server Citrix Session Recording Broker and Storage Management.
Database and Server Summary	Session Recording Server
Database and Server Summary Install	Session Recording Server Citrix Session Recording Broker and Storage Management. Session Recording Administrator Logging Administrator Logging captures Session Recording Server configuration changes and
Database and Server Summary Install	Session Recording Server Citrix Session Recording Broker and Storage Management. Session Recording Administrator Logging Administrator Logging captures Session Recording Server configuration changes and recording activities to the Session Recording Database. Session Recording Database

- 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

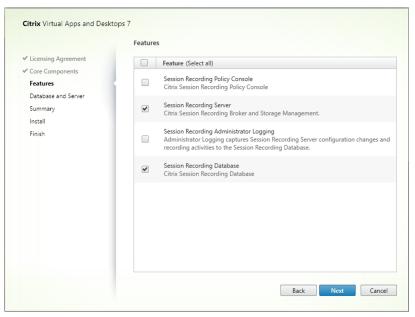
We recommend that you install the Session Recording administrator logging together with the Session Recording server at the same time. If you don't want the administrator logging feature to be enabled, you can disable it on a later page. However, if you choose not to install this feature at the beginning but want to add it later, you can only manually add it by using Session-RecordingAdministrationx64.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**.

	Database and Server Configuration	
✓ Licensing Agreement	Specify the instance name and database name of the Session Recording Database.	
 ✓ Core Components ✓ Features 	Configuration	
Database and Server	Enable SQL Server authentication	
Administrator Logging	Instance name:	
Summary		1
Install	Database name:	1
Finish	CitrixSessionRecording	1
		1
	Test connection	
	reat connection	

Note:

Starting with 2411, 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. For more information, see Install the Session Recording database on Azure SQL Database and Install the Session Recording database on Azure SQL Managed Instance or on AWS RDS.

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.

	Database and Server Configuration	
Licensing Agreement	Specify the instance name and database name of the Session Recording Databa	se.
Core Components	Configuration	
 Features Database and Server Administrator Logging 	Enable SQL Server authentication Instance name:	
Summary	Example: .\SQLEXPRESS,computer-name\SQLEXPRESS, computer-name	
Install Finish	Database name:	
	CitrixSessionRecording	
	SQL user name:	
	SQL password:	ow password
	Test connection	
	Back	Cancel

- 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.

Citrix Virtual Desktops 7	Administrator Logging Configuration
Licensing Agreement	Specify Session Recording logging configuration
Core Components	Configuration
	The Administrator Logging database is installed on the SQL Server instance:
Database and Server	VVDFX-SRD-1
Administrator Logging	
Summary	Administrator Logging database name:
Install	CitrixSessionRecordingLogging 🗸
Finish	Test connection Image: Second Se
	Enable mandatory blocking This option blocks policy and server property changes if logging fails.
	Back Next Cancel

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.

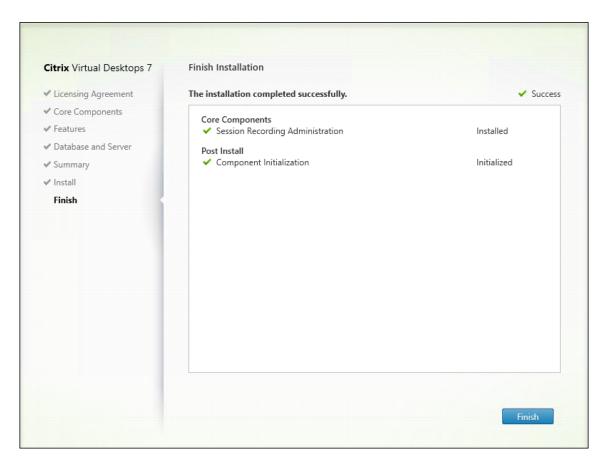
Click **Next** to continue the installation.

4. Review the prerequisites and confirm the installation.

Review the prerequisites and confirm the components you want to install.
Installation directory CAProgram Files/Citrix Prerequisites Microsoft Message Queuing Core Components Session Recording Administration Features Session Recording Server Session Recording Server Session Recording Database

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.

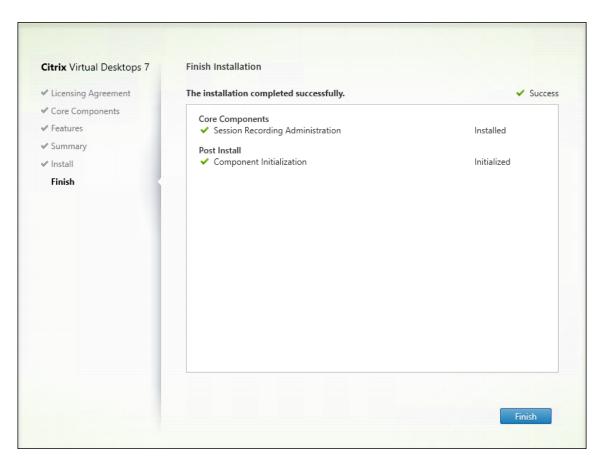
	Features
Licensing Agreement	Feature (Select all)
Core Components	Couries Describer Dellas Coursel
Features	Citrix Session Recording Policy Console
Summary	
Install	Session Recording Server Citrix Session Recording Broker and Storage Management.
Finish	

2. Review the prerequisites and confirm the installation.

Citrix Virtual Desktops 7	Summary
✓ Licensing Agreement	Review the prerequisites and confirm the components you want to install.
 Core Components Features Summary Install Finish 	Installation directory C:\Program Files\Citrix Core Components Session Recording Administration Features Session Recording Policy Console
	Back Install Cancel

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_PowerShellSna.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 singlesession 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.



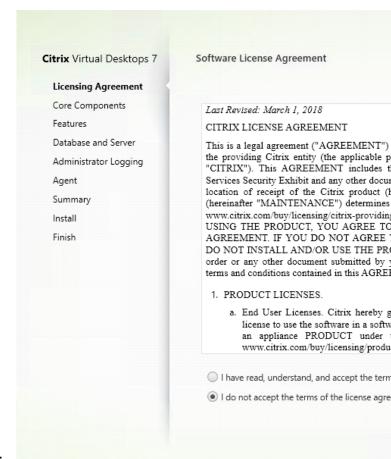
Step 2: Choose which product to install

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

Get Started			Prepare Machines and Images	
Delivery Controller			Virtual Delivery A	gent for Winde
Start here. Select and install the essential services like License Si			Install this agent to based VMs or physi	
Extend Deployment				
Extend Deployment Citrix Director	•	Citrix Studio	¢	Self-Servic
	•	Citrix Studio Universal Print Serve		

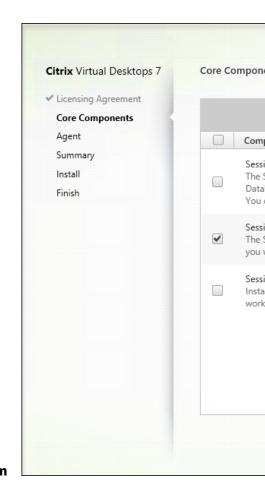
Step 3: Select Session Recording

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.

	Agent Configuration
 Licensing Agreement Core Components Agent Summary Install Finish 	Configuration Session Recording Server name: I Note: Enter information for connecting to the Sessis such information later in the Session Recording Age Protocol: HTTPS Port 443 © Enable Azure AD support This option lets you make Session Recording agroups who launch sessions from Azure A Test connection

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 Record-ing Agent Properties**.
- 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 permis sions 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.

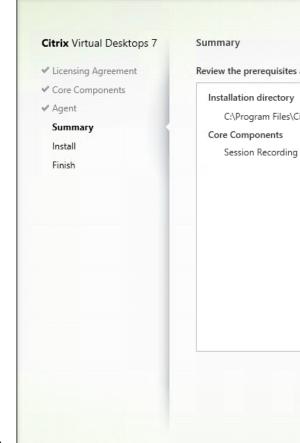
- Use the MSI package to install the Session Recording server on an Azure AD joined machine

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:
 - 1. Sign in to Citrix Cloud.
 - 2. In the upper left menu, select **My Services > DaaS**. By default, the home page for the Full Configuration interface appears.

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.

Citrix Virtual Desktops 7	Finish Installation
Citrix Virtual Desktops 7 Citrix Virtual Desktops 7 Licensing Agreement Core Components Agent Summary Install Finish	The installation completed successfully. Core Components Session Recording Agent Post Install Component Initialization

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:

```
1 # Remove old QMId from registry and set SysPrep flag for MSMQ
2
3 Remove-Itemproperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\
    MachineCache -Name QMId -Force
4
5 Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -
    Name "SysPrep" -Type DWord -Value 1
6
7 # Get dependent services
8
9 $depServices = Get-Service -name MSMQ -dependentservices | Select -
    Property Name
10
11 # Restart MSMQ to get a new QMId
12
13 Restart-Service -force MSMQ
```

```
15
   # Start dependent services
16
17 if ($depServices -ne $null) {
18
19
       foreach ($depService in $depServices) {
21
22
            $startMode = Get-WmiObject win32_service -filter "NAME = '$
23
       ($depService.Name)'" | Select -Property StartMode
24
25
             if ($startMode.StartMode -eq "Auto") {
26
27
                 Start-Service $depService.Name
28
29
              }
30
    }
32
34
    }
```

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.

	Deliver applications and desktops to any user, anywhere, • Hybrid cloud, cloud and enterprise provisioning • Centralized and flexible management
	Manage your delivery according to your needs:
	Virtual Apps Deliver applications
4	Virtual Apps and Desktops Deliver applications and desktops
	k k
	citrix

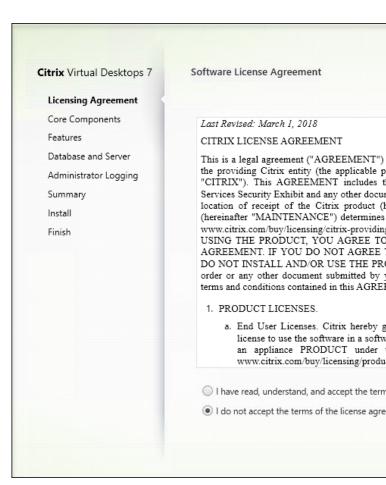
Step 2: Choose which product to install

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

		Prepare Machines		
Get Started		Prepare Machines	and	images
Delivery Controller	Virtual Delivery	Age	nt for Wind	
Start here. Select and install the essential services like License Se		Install this agent t based VMs or phy		
Extend Deployment				
	e		Ð	Self-Servio
Citrix Director	Citrix Studio			Self-Selfik
Citrix Director Citrix License Server	Universal Print Serve)	Session Re
		r (

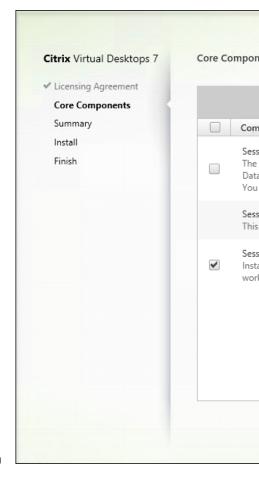
Step 3: Select Session Recording

Select the **Session Recording** entry.



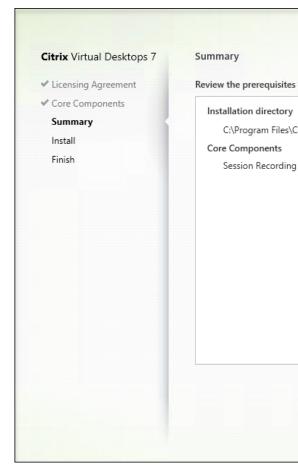
Step 4: Read and accept the license agreement

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



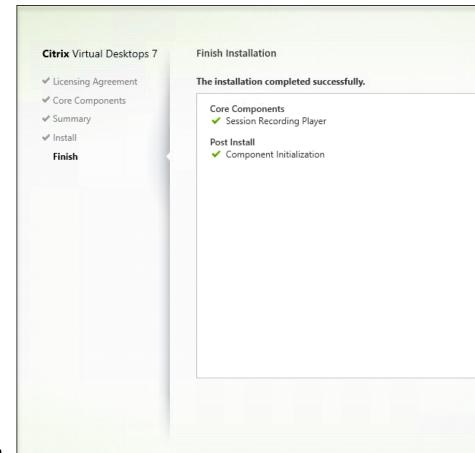
Step 5: Select the component to install and the installation location

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.

Set the access control list (ACL) for Message Queuing (MSMQ)

After installing Session Recording, it is recommended to configure the ACL for MSMQ. For more information, see Security recommendations.

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 singlecommandFor 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.

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

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. SsRec-Server 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. 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:
 - 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/c pp/windows/latest-supported-vc-redist?view=msvc-170.
 - 2. 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.
 - 3. Include the **AADPASSWORD** parameter and set it to 1 when running the database installation command.
 - 4. 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/azu re/azure-sql/database/authentication-aad-configure?view=azuresql&tabs=azurepowershell.
- 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.
- **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.

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:

```
1 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:

```
1 .\SsRecUtils.exe -modifydbconnectionpara DATABASEINSTANCE
DATABASENAME LOGGINGDATABASENAME
2
3 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:

1 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.

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

1 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.

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

2 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 x64Session 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.

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 cloudbased 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="0"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/enus/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.micr osoft.com/en-us/sql/connect/odbc/download-odbc-driver-for-sql-server?view=sqlserver-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/enus/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:

```
1 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>**.

aws Services ▼	Q Search for services, features, marketple
Amazon RDS ×	
Dashboard Databases Query Editor Performance Insights Snapshots Automated backups Reserved instances Proxies Subnet groups Parameter groups Option groups Events Event subscriptions	Connectivity & security Monitoring Logs & events Configu Connectivity & security Endpoint & port Endpoint database-2.ccjfaeoogg0g.us-east-2.rds.amazonaws.com Port 1433
Recommendations Certificate update	Security group rules (2) Q Filter security group rules Security group db2sg (sg-00fbd0fee602a731b) db2sg (sg-00fbd0fee602a731b)

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.

👹 Citrix Session Re	cording Administration Setup	-		×
Database and Serv	er Configuration		citr	ιż
Specify the instan	ce name and database name of the Session Record	ing Datab	ase.	
Instance name	Example: .\SQLEXPRESS, computer-name\SQLEXPRESS, top::coc. database. windows.net, 3342 Enable SQL Server authentication	computer-	name,	Ī
<u>D</u> atabase name	Use default database name			
SQL user name				
SQL password				
Enable Azure	AD support			
	< Back Ne	ext >	Cano	æl

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 US convice

		perties			- 🗆	×
Playback Notificati	ons CEIP	Logging	RBAC	Email	Cloud DB	We • •
Azure SQL Manag	ed Instance s	support				
This option allows	s you to enab	le cloud S	QL.			
Enable cloud	SQL					
Cloud SQL adn	nin _{srtsqs}	ladmin				
name :						
Cloud SQL adn	nin					
password:						-
		0	K	Can	cel	Apply

 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/datamigration/ or https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migratean-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 Session-RecordingAdministrationx64.msi package. For a description of the command parameters, see the preceding Automate installation section in this article.



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:

Google Cloud Search (/) for resources, docs, products, and more	Q Search 🛱 ⊾ 🚺 🖓 🗄 🌑
SQL Instances CREATE INSTANCE CREATE DATA	HELP ASSISTANT SHOW INFO PANEL
	Ø III
Instance ID 😧 🛧	Actions
Sessionrecording	i

c) Choose SQL Server as your database engine.

≡ Google Cloud :•	Search (/) for resources, docs, products, and more	Q Search	击	>	11 ?	- 0
SQL ← Create an instance					🖻 HELI	P ASSISTANT
Choose your database engine						
MySQL	PostgreSQL	SQL Server				
Versions: 8.0, 5.7, 5.6	Versions: 14, 13, 12, 11, 10, 9.6	Versions: 2019, 201	17			
Choose MySQL	Choose PostgreSQL	Choose SQL Ser	ver			
Want more context on the Cloud SQL database engines?	Learn more					

 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:

■ Google Cloud Search (/) for	resources, docs, products, and	more Q Search	÷ L		0	
Create a SQL Server instance				I	HELP A	SSISTAN
Instance info	Summary					
Instance ID *	Region	us-central1 (lowa)				
testinstance	DB Version	SQL Server 2019 Standard				
Use lowercase letters, numbers, and hyphens. Start with a letter.	vCPUs	4 vCPU				
Password *	Memory	26 GB				
GENERATE	Storage	100 GB				
Your default service admin username is "sqlserver" Learn more Database version *	Network throughput (MB/s)	1,000 of 2,000				
SQL Server 2019 Standard	Disk throughput (MB/s)	Read: 48.0 of 240.0				
	0	Write: 48.0 of 240.0				
Choose a configuration to start with	IOPS	Read: 3,000 of 15,000				
		Write: 3,000 of 15,000				
These suggested configurations will pre-fill this form as a starting point for creating an nstance. You can customize as needed later.	Connections	Public IP				
	Backup	Automated				
You've made changes that override the selected configuration. RESET	Availability	Single zone				
	Point-in-time recovery	Disabled				
CONFIGURATION DETAILS Choose region and zonal availability For better performance, keep your data close to the services that need it. Region is						
permanent, while zone can be changed any time.						
us-central1 (lowa)						
Zonal availability Single zone In case of outage, no failover. Not recommended for production.						
 Multiple zones (Highly available) Automatic failover to another zone within your selected region. Recommended for production instances. Increases cost. 						
Primary zone						
Any 👻						

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:

■ Google Cloud Search (/) for resources, docs, products, and	more Q S	earch	毌	>_	11	?	: (
Create a SQL Server instance						P	E HELP	ASSISTA
Customize your instance	Summary							
ou can also customize instance configurations later	Region	us-central1 (Iowa)						
Nachine type	DB Version	SQL Server 2019 Stand	ard					
fachine has 4 vCPUs and 26 GB of memory.	vCPUs	4 vCPU	uru					
	Memory	26 GB						
Storage	Storage	100 GB						
torage type is SSD. Storage size is 100 GB, and will automatically scale as needed. $$ $$	Network throughput	1,000 of 2,000						
oogle-managed key enabled (most common).	(MB/s) 😧							
	Disk throughput (MB/s)	Read: 48.0 of 240.0						
Connections ^	0	Write: 48.0 of 240.0						
hoose how you want your source to connect to this instance, then define which	IOPS	Read: 3,000 of 15,000						
etworks are authorized to connect. Learn more	0	Write: 3,000 of 15,000						
ou can use the Cloud SQL Proxy for extra security with either option. Learn more	Connections Backup	Public IP Automated						
	Availability	Single zone						
nstance IP assignment	Point-in-time recovery	Disabled						
Private IP Assigns an internal, Google-hosted VPC IP address. Requires additional APIs and	Point-in-time recovery	Disubicu						
New network								
< Name								
test								
Use <u>CIDR notation</u>								
Network *								
Example: 199.27.25.0/24								
CANCEL DONE								
ADD A NETWORK								
Authentication void the Directory domain selected								
Data Protection utomatic backups enabled. Point-in-time recovery (via transaction logs) disabled.								

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

Session Recording 2411

You can also customize instance configurations later	
Machine type Machine has 4 vCPUs and 26 GB of memory.	~
Storage Storage type is SSD. Storage size is 100 GB, and will automatically scale as neede 3oogle-managed key enabled (most common).	d. 🗸
Connections Public IP enabled	~
Authentication Vo Active Directory domain selected	~
Data Protection Mutomatic backups enabled. Point-in-time recovery (via transaction logs) disabled instance deletion protection enabled.	. ~
Maintenance Jpdates may occur any day of the week. Maintenance timing set to 'Later.'	~
Flags and parameters Add any database flags or parameters you'd like to apply to this instance. Default collation is SQL_Latin1_General_CP1_CLAS. Timezone is UTC.	~
Labels No labels set	~

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

=	Google Cloud	Search (/) for resources, docs, products, and more 🔍 Search 🗄 🗈 💶 🕐 ᠄
\$	SQL	Overview 🖍 Edit 👌 Import 🏦 Export 🕐 Restart 🔳 Stop 🍵 delete 🛱 Clone 💷 Help Assistant
PRIMA	ARY INSTANCE	All instances > testinstance
A	Overview	⊘ testinstance
÷	Connections	SQL Server 2019 Standard
**	Users	1 hour 6 hours 🗸 1 day 7 days 30 days Custom 💌
	Databases	Chart S ≅ C :
▣	Backups	CPU utilization 👻 🕢
i	Operations	
		UTC-8 8.00 PM May 9 2.00 AM 4.00 AM 8.00 AM 10.00 AM 12.00 PM 2.00 PM 4.00 PM Connect to this instance Image: Configuration Image: Configuration VCPUs Memory SSD storage Connection name Image: Configuration Image: Configuration Image: Configuration Image: Configuration Need help connecting? Image: Contract backups are enabled Image: Contract backups are enabled Image: Contract backups are enabled Image: Contract backups are enabled Image: Contract backups are enabled Image: Contract backups are enabled
		Image: Suggested actions Instance deletion protection is enabled Instance

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.

🚽 Citrix Session Re	cording Administration Setup	-		×
Database and Serv	er Configuration		citi	٦×
Specify the instan	ce name and database name of the Session Recordin	g Datab	ase.	
Instance name	Example: \SQLEXPRESS, computer-name\SQLEXPRESS, bpccocc.database.windows.net, 3342	computer-	name,	1
<u>D</u> atabase name	Use default database name			
<u>S</u> QL user name	Г			
SQL password				
Enable Azure /	AD support			
	< Back Nex	t >	Can	cel

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.

Session Recording (i) 0 Session Recording Deployments
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.

Connect Sess	ion Recording Server	×
Configure and	connect your Session Recording server to Citrix Analytics.	
1	Prerequisites What is your Session Recording version? Can your Session Recording server connect to the following addresses? Session recording server should meet <u>service connectivity requirements</u> Session recording server should have connectivity to <u>https://api.analytics.cloud.com</u> Do you have any proxy servers in your network? Do the proxy servers allow communication with Citrix Analytics?	

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

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

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



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

Note:

The file contains sensitive information. Keep the file in a safe and secure location.

- 8. Copy the file to the Session Recording server that you want to connect to Citrix Analytics for Security.
- 9. If you have multiple Session Recording servers in your deployment, you must copy the file in each server that you want to connect and follow the steps to configure each server.

10. On the Session Recording server, run the following command to import the settings:

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

For example:

```
1 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.

Session Recording 🛈	
1 Session Recording Deployment	

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.

← Conr	necte	ed Session Recording	De	ployments					
5	Sessio	n recording servers							
	^	Session Recording deployment							:
		The Session recording server is suc	cess	fully configured and connected.					
		BASE URL		SESSION RECORDING DEPLOYMENT	CONFIGURATION STATUS		LAST UPDATED		
		Site-2-v2103.smarttools.clm		Barriel 145, 851 at 17176.	Success		Sep 21 2021 11:26 AM		
					Showing 1-1 of 1 items	Pa	age 1 of 1 < 🕨	5 rows ∨	

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:

- 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**.

← Connected Session Recording Deployments						
	Session recording servers					
	Session Recording deployment					
	Session Recording deployment					
	+ 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.

Session Record O Session Recording	Turn off data processing Connect Session Recording server
Received Events: 0	<u>1H</u> 1W
	No data to display
	Time

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 (\square) and select **Remove Session Recording server from Analytics**.

Connected Sessio	n Recording Deployments	
	Session recording servers	
	∧ Session Recording deployment	:
	The Session recording server is successfully configured and connected.	Remove Session recording server from Analytics
	BASE URL © SESSION RECORDING DEPLOYMENT © CONFIGURATION STATUS	a LAST UPDATED 0
	Session-Recording-Server-	Nov 13 2021 1:02 AM
	Showing 1	1-1 of 1 items Page 1 of 1 <
	✓ Session Recording deployment	i

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

For example:

1 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):

1 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\	String	Enter your UUID.			
	HKEY_LOCAL_MACHINE					
	\SOFTWARE\					
	Citrix\					
	SmartAuditor\					
	Server\					
EnableCASUseAudi	to@ompiopterID	REG_DWORD	1			
	HKEY_LOCAL_MACH	IINE				
	/SOFTWARE/					
	Citrix/					
	SmartAuditor/					
	Server/					

- 3. Restart the following services:
 - Citrix Session Recording Analytics Service
 - Citrix Session Recording Storage Manager

Dynamic session recording

June 21, 2024

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
- 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.

🖳 Delivery Group or Machine Name Queries	\times
🖳 Create Query 🛛 🗙	1
Site Address: Citrix Cloud Controller	
Enter a site address	
Delivery Groups Machines	
Enter a Delivery Group name	
Create Cancel	
Add Remove	-
Close	

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.

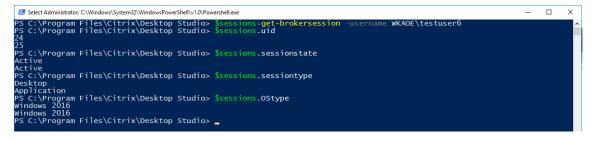
Command	Description
Stop-BrokerSessionRecording	Lets you stop recording a specific active session,
	a list of active sessions, or sessions launched by
	a specific user. For more information, run Get-
	Help Stop-BrokerSessionRecording
	to see the command online help.
Get-BrokerSessionRecordingStatus	Lets 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.

Console Root			Actions	
 Citrix Studio (BVT_DB) Search 	citrix		Citrix Studio (8VT_D8)	-
Machine Catalogs	Common Tacks Actions PowerShell		View	•
AppDisks		1.1	(d) Refresh	
B Delivery Groups	<pre># Register the certificate for the Licensing Service #</pre>	1	Help	
Applications	4/9/2018 2:31 AM			
Cogging	Get-LogSite -AdminAddress "wkace-ddc-1.bvt.local:80" -BearerToken *******			
 Configuration Administrators 	Start-LopHighlevelOperation -AdminAddress "wksoe-ddc-1.bvt.local:80" -BearerToken ******* -Source "Studio" -StartTime "4/9/2018 6:31:18 AM" -Text "Register the certificate for the Licensing Service"			
E Controllers Hosting	Set-ConfigSizeWetadata -AdminAddress "wkace-dds-1.bvt.lcom1:80" -BearerToken ******* -LoggingId "of42608-e2ef-4364-9eb6-off225324d55" -Name "CertificateMash" -Value "zkiGglyuSu43160Mq7xmgANoJpo9TOTF+kkErZMI5eUp85#AM57201e0hlimUCof-C+QSioUy25xF3/50Id10"	m.		
Creening StoreFront App-V Publishing ApoDNA	Stop-LogKiphLawsDopersionKanikdstess "wise-do-low.loalist" -BearerToken ****** -EadTime *4/9/2015 6:81:19 AMBiphLevelOpersionId *Tet4840Abt-434-496-00728324685" -ISGuccestal STrue # Script complement successful Strue			
Zones				
> 🗱 Citrix StoreFront	+ Get the certificate for the Licensing Service			
	# 4/9/2018 2:31 AM			
	* Get-LisCertificste = %dminddress "https://wRace=ddo=1.bvt.local:8085/* # Script completed successfully			
	# Get the certificate for the Licensing Service			
	+ 4/9/2018 9:49 FM			
	Get-LioCertificate -kdminkdiress "https://wkaoe-ddo-1.bvt.looal:8083/" # Script completed successfully	-		
	# Get the certificate for the Licensing Service			
	4/9/2018 9:50 PM			
	Get-LioCertificate -AdminAddress "https://wkace-ddo-1.bvt.local:6083/" # Script completed successfully			
	Get the certificate for the Licensing Service			
	# 4/9/2018 10:06 PM			
	* Get-LicCertificateAdminAddress "https://wkace-dds-1.bvt.local:0083/" # Script completed successfully			
		-	1	
	Laurch Power	ihel	J	

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



- 3. Use the Get-BrokerSessionRecordingStatus command to get the recording status of the specified session.
 - PS C:\Program Files\Citrix\Desktop Studio> Get-BrokerSessionRecordingStatus -Session 24 SessionNotRecorded PS C:\Program Files\Citrix\Desktop Studio> Get-BrokerSessionRecordingStatus -Session 25 SessionNotRecorded PS C:\Program Files\Citrix\Desktop Studio> _

Note:

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

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

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

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

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

Note 🗆

When you play a **Complete** recording ended by the Stop-BrokerSessionRecording command, the last section of the timeline on the player progress bar might show gray. And,

the last section of the recorded session is idle. It is not obvious when the recorded session has constant activities.

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

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.

The following table shows common ways of using this command:

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

Citrix Studio						-	٥	×
File Action View Help								
🏟 🞽 🖬 👔 🖬								
🚆 Console Root			10000			Acti	ons	
Citrix Studio (dDDC3)	_		Last 7 days	Search	م ا	Log	ging	
Search Machine Catalogs	Administrator	Main Task	Start +	End	Status		Preference	es
Delivery Groups	▼ Today						Create Cu	ust
Applications	APRQ\qh	Stop Recording of Session '5DAE93E5-E14E	8/20/2020 : 3:56:13	8/20/2020 : 3:56:13	Successful	x	Delete Lo	gs
Policies Policies	APRQ\qh	Stop Recording of Session '4DD677B7-DDE	8/20/2020 : 3:56:09	8/20/2020 : 3:56:09	Successful		View	-
V 🖗 Configuration	APRQ\qh	Start Recording of Session '5DAE93E5-E14E	8/20/2020 : 3:56:05	8/20/2020 : 3:56:05	Successful	a	Refresh	
Administrators	APRQ\qh	Start Recording of Session '4DD677B7-DDE	8/20/2020 : 3:56:02	8/20/2020 : 3:56:02	Successful			
Controllers	APRQ\qh	Stop Recording of Session '4DD677B7-DDE	8/20/2020 : 3:55:13	8/20/2020 : 3:55:13	Successful	?	Help	
💻 Hosting	APRQ\qh	Stop Recording of Session '5DAE93E5-E14E	8/20/2020 : 3:55:09	8/20/2020 : 3:55:10	Successful	I		
k Licensing	APRQ\qh	Create Machine 'Styx_VDA1_1' in Delivery G	8/20/2020 : 1:22:55	8/20/2020 : 1:22:55	Successful	I		
🖳 StoreFront 🔂 App-V Publishir	APRQ\qh	Create Delivery Group 'Styx_VDA1'	8/20/2020 : 1:22:54	8/20/2020 : 1:22:55	Successful	I		
Zones	APRQ\qh	Create Machine Catalog 'Styx_VDA1'	8/20/2020 : 1:22:24	8/20/2020 : 1:22:24	Successful	I		
Citrix StoreFront	APRQ\qh	Create Machine 'Styx_VDA2_1' in Delivery G	8/20/2020 : 1:20:01	8/20/2020 : 1:20:02	Successful	I		
	APRQ\qh	Create Delivery Group 'Styx_VDA2'	8/20/2020 : 1:19:59	8/20/2020 : 1:20:02	Successful			
	APRQ\qh	Create Machine Catalog 'Styx_VDA2'	8/20/2020 : 1:18:50	8/20/2020 : 1:18:51	Successful			
	Yesterday							

Configure

June 21, 2024

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
 - Configure session recording policies
 - Configure recording viewing policies
 - Configure event detection policies
 - Configure event response policies
- High availability and load balancing
 - Load balance Session Recording servers
 - Configure database high availability

Configure settings on the Session Recording agent

June 21, 2024

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

October 24, 2024

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.

🐼 Session Recording Agent Properties – 🗆 🗙
Recording Connections Lossy Video
Session recording
Select this option to enable policy-based session recording on this VDA machine. If this option is not selected, session recording is disabled on this machine.
Enable session recording for this VDA machine
Custom event recording
Select this option to allow third party applications to inject custom data into the recorded session while recording is in progress. This data is available during playback.
Allow third party applications to record custom data on this VDA machine
Compressed recording
Select this option to enable compressed recording for parts of Thinwire- transmitted session screens that are not H.264 compressed.
Enable compressed recording for Thinwire-transmitted session screens on this VDA machine
OK Cancel Apply

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 Thinwiretransmitted session screens on this VDA machine check box.

🖏 Session I	Recording Ag	ent Proper	ties		-		×
Recording	Connections	Lossy Vid	ео				
- Session r	-						
	is option to en . If this option hine.						
🗹 Enab	ole session rec	ording for t	his VDA ma	achine			
Custom e	vent recording						
into the r	iis option to all recorded sess e during playb	ion while re					a
Allov mac	v third party ap hine	oplications	to record cu	ustom da	ta on this	s VDA	
Compress	sed recording -						
	ted session so					Thinwir	·e-
	ole compresse ens on this VD			re-transn	nitted se	ssion	
			ОК	Can	icel	Ap	ply

Enable or disable lossy screen recording

July 31, 2024

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.

🚳 Session Recording Agent Prop	_		×	
Recording Connections Lossy So	creen Player	·		
Codec settings				
Video fluency:		Low	\sim	
Video image quality:		Low	\sim	
I-Frame interval:		1 1 1	1 1 1	
Image resolution scaling:		1.0	\sim	
Cursor				
Cursor refresh rate:		Low	\sim	
	ОК	Cancel	App	ly

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**.

🐵 Session Re	ecording Age	ent Properties		_		×
Recording	Connections	Lossy Screen	Player			
Codec sett	ings					
Video	fluency:			Low	~	
				1		
Video	o image qualit	ty:		Low	~	
I-Fra	me interval:			1 1	1 I I	
Image	e resolution s	caling:		1.0	~	
Cursor						
Curse	or refresh rat	e:		Low	~	
		0	<	Cancel	Арр	ly

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

Compression option	Description	Default value	Remarks
Video image quality	Low:bitrate:140	Low	Session Recording
	(kbps); Medium:		uses Average Bitrate
	bitrate:280 ((ABR) for video bitrate
	kbps); High :		encoding. Higher
	bitrate:420 (kbps)		values mean less
			compression. You can
			also set a custom
			value between 40 kbps
			and 80,000 kbps by
			editing the Registry at
			HKEY_LOCAL_MACHINE\SOFTWARE
I-Frame interval	60, 120, 300, 600,	600	The larger the I-Frame
(seconds)	1200, 1800, 3600		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	1.0, 0.9, 0.8, 0.7, 0.6,	1	You can downscale the
scaling	0.5, 0.4		resolution of recorded
C C			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
Cursor refresh rate	Low: 3; Medium: 5;	Low	N/A
(times per second)	High : 10		

Enable fast seeking

June 21, 2024

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

🕹 Session F	Recording Age	ent Properties		-		×
Recording	Connections	Lossy Screen	Player			
_	fast seeking					
Seek set	tings					
System	stem-defined I-	Frame interval:		Medium Low Medium	~	
⊖ Cu	stom I-Frame in	nterval:		High		
		OK		Cancel	Арр	ly

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.

CİTIX Session Rec	Cording Search by host name, user, start time, and so on
▶ Recordings ✓ ☐ Comments ✓	Preferences Set your playback preferences.
Administrator Logging Image: Configuration	Player cache Set the cache size you want the player to use for playback. 2MB 25MB 50MB 75MB 100MB 32 ♪ MB
Preferences	Since Sound Found Found Found Found

Configure the connection to the Session Recording server

June 21, 2024

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

June 21, 2024

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

Use HTTP as the communication protocol

- 1. Log on to the machine hosting the Session Recording server and disable secure connections for Session Recording Broker in IIS.
- 2. Change the protocol setting from HTTPS to HTTP in **Session Recording Agent Properties** on each server where the Session Recording agent is installed:
 - a) Log on to each server where the Session Recording agent is installed.
 - b) From the Start menu, choose Session Recording Agent Properties.
 - c) In Session Recording Agent Properties, choose the Connections tab.
 - d) In the **Session Recording Broker** area, select **HTTP** from the **Protocol** drop-down list and click **OK** to accept the change. If you are prompted to restart the service, click **Yes**.
- 3. Change the protocol setting from HTTPS to HTTP in the Session Recording Player settings:
 - a) Log on to each workstation where the Session Recording Player is installed.
 - b) From the Start menu, choose Session Recording Player.
 - c) From the **Session Recording Player** menu bar, choose **Tools** > **Options** > **Connections**, select the server, and choose **Modify**.
 - d) Select **HTTP** from the **Protocol** drop-down list and click **OK** twice to accept the change and exit the dialog box.
- 4. Change the protocol setting from HTTPS to HTTP in the Session Recording policy console:
 - a) Log on to the server where the Session Recording policy console is installed.
 - b) From the **Start** menu, choose **Session Recording Policy Console**.
 - c) Select **HTTP** from the **Protocol** drop-down list and click **OK** to connect. If the connection is successful, this setting is remembered the next time you start the Session Recording policy console.

Revert to HTTPS as the communication protocol

- 1. Log on to the machine hosting the Session Recording server and enable secure connections for the Session Recording Broker in IIS.
- 2. Change the protocol setting from HTTP to HTTPS in **Session Recording Agent Properties** on each server where the Session Recording agent is installed:
 - a) Log on to each server where the Session Recording agent is installed.
 - b) From the Start menu, choose Session Recording Agent Properties.
 - c) In Session Recording Agent Properties, choose the Connections tab.
 - d) In the **Session Recording Broker** area, select **HTTPS** from the **Protocol** drop-down list and click **OK** to accept the change. If you are prompted to restart the service, click **Yes**.
- 3. Change the protocol setting from HTTP to HTTPS in the Session Recording Player settings:

- a) Log on to each workstation where the Session Recording Player is installed.
- b) From the Start menu, choose Session Recording Player.
- c) From the **Session Recording Player** menu bar, choose **Tools** > **Options** > **Connections**, select the server, and choose **Modify**.
- d) Select **HTTPS** from the **Protocol** drop-down list and click **OK** twice to accept the change and exit the dialog box.
- 4. Change the protocol setting from HTTP to HTTPS in the Session Recording policy console:
 - a) Log on to the server where the Session Recording policy console is installed.
 - b) From the **Start** menu, choose **Session Recording Policy Console**.
 - c) Select **HTTPS** from the **Protocol** drop-down list and click **OK** to connect. If the connection is successful, this setting is remembered the next time you start the Session Recording policy console.

Configure settings on the Session Recording server

June 21, 2024

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

June 21, 2024

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

June 21, 2024

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.

🐴 Session Re	cording Server P	roperties	_		×
Storage Sig	ning Rollover F	Playback Notifications	CEIP	Logging	RBAC
		ke the product better b gram. <u>Learn more</u>	y joining I	the Custor	ner
🗹 Participa	ate in the Custom	er Experience Improve	ment Prog	gram.	
					4 1
		OK	Cancel		Apply

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
Operating System version	OS_version	whether CEIP is enabled. 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.

Data Point	Key Name	Description
Session Recording server version	SRS_version	Text string denoting the installed version of the Session Recording server. 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 Analytics and CEIP are enabled.

Data Point	Key Name	Description
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.

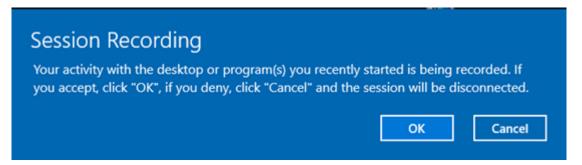
Customize recording notification messages

June 21, 2024

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.

	Intecoru	ing Server	Properties	;	_		×
torage	Signing	Rollover	Playback	Notifications	CEIP	Logging	RE
being r	ecorded.	Customize	content of	o inform them the notification f their session	n messag		S
- Defau	ult messag	e					
Title	-						
Sess	ion Recor	ding					
Body							
Langu	uage spec	ific messag	jes				~
List	t of langua	age-specifi the default	c notificatio	on messages is 1 message will		Add Modify Remov	····
List	t of langua	age-specifi the default	c notificatio			Modify	····

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:

	n Record	ing Server	Properties	i	_		×
itorage	Signing	Rollover	Playback	Notifications	CEIP	Logging	RI 1
being r	ecorded.	Customize	e content of	to inform them the notification f their session	n messag		8
Defau	ılt messag	e					
Title							
Sess	ion Recor	ding					
Body							
Langu	uage spec	ific messag	jes —				~
	_						
		the default		on messages is n message will		Add Modify Remov	····
		the default	t notification			Modify	····

- 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 languagespecific 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.

Language-Specific Notificatio	n Messages
Select language:	
	~
Title	
li internet	
Notification message:	
	^
	×
	OK Cancel

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

Enable or disable digital signing

June 21, 2024

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

June 21, 2024

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:

eekly		Daily
citrix.		citrix.
Session Recording Event Aug 7 – Aug 13, 2023 Statistics on responses triggered by yo Database instance name: sessionrecor	our event response policy.	Session Recording Event Response Report Aug 8, 2023 Statistics on responses triggered by your event response policy. Database instance name: sessionrecording-db
Email alerts 157	Web browsing 82 File deletion 35 Performance data 12 Other 28	Email alerts Web browsing 23 Performance data 7 File deletion 2 Other 2
Dynamic screen recordings	App start 33 Web browsing 30	Dynamic screen recordings App start 6 10
Session locked	App start 21 Web browsing 15 Popup window 11 Other 3	Session locked Popup window 5 19 Web browsing 1 Other 11
Sessions disconnected	File transfer 🛛 25	Sessions disconnected File transfer 🛑 1 1
Sessions logged off 45	Idle 22 USB drive insertion 15 Performance data 8	Sessions logged off O
You can find the full list of	of events and responses attached to this email.	You can find the full list of events and responses attached to this email
This is an automated email from Citrix	Session Recording. Do not reply.	This is an automated email from Citrix Session Recording. Do not reply.

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

÷	EventRes	sponses_9_21_2	023.csv				Oper	with 👻
	A	В	С	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	g Session Start	Email alert when a s	s Session Start	
3	XF4B5\Administrator	9/20/2023 3:26:53 A	perf	C:\SessionRecording	gs\2023\09\19\i_fab04	and start screen reco	ording when a is deteo	
1	XF4B5\Administrator	9/18/2023 8:52:36 A		C:\SessionRecording	g Session Start	Email alert when a s	s Session Start	
5	XF4B5\Administrator	9/18/2023 8:53:09 A	perf	C:\SessionRecording	gs\2023\09\18\i_3c71	and disconnect sess	ion when a is detecte	
3	XF4B5\Administrator	9/16/2023 3:03:56 A		C:\SessionRecording	g Session Start	Email alert when a s	s Session Start	
	XF4B5\Administrator	9/18/2023 3:09:06 A		C:\SessionRecording	g Session Start	Email alert when a s	s Session Start	
3	XF4B5\Administrator	9/18/2023 6:58:15 A	web search	C:\SessionRecording	gWebBrowsing	Email alert and lock	WebBrowsing <splt< td=""><td></td></splt<>	
)	XF4B5\Administrator	9/20/2023 5:41:04 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
0	XF4B5\Administrator	9/20/2023 5:50:37 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
	XF4B5\Administrator	9/20/2023 5:51:07 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
2	XF4B5\Administrator	9/20/2023 6:14:43 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
3	XF4B5\Administrator	9/20/2023 6:26:47 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
4	XF4B5\Administrator	9/20/2023 6:56:26 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
5	XF4B5\Administrator	9/20/2023 3:28:23 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
	XF4B5\Administrator	9/20/2023 3:29:24 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
7	XF4B5\Administrator	9/20/2023 3:29:54 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
8	XF4B5\Administrator	9/20/2023 3:30:24 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
9	XF4B5\Administrator	9/20/2023 3:31:25 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
0	XF4B5\Administrator	9/20/2023 3:31:54 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
1	XF4B5\Administrator	9/20/2023 6:44:52 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	ort
2	XF4B5\Administrator	9/20/2023 6:46:52 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
3	XF4B5\Administrator	9/20/2023 3:32:24 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
4	XF4B5\Administrator	9/20/2023 3:32:54 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
5	XF4B5\Administrator	9/20/2023 3:33:24 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
6	XF4B5\Administrator	9/20/2023 6:19:45 A	perf	C:\SessionRecording	s\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
7	XF4B5\Administrator	9/20/2023 6:20:15 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
8	XF4B5\Administrator	9/20/2023 6:26:17 A	perf	C:\SessionRecording	gs\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
9	XF4B5\Administrator	9/20/2023 6:27:18 A	perf	C:\SessionRecording	s\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	ing readra
0	XF4B5\Administrator	9/20/2023 6:27:47 A	perf	C:\SessionRecording	s\2023\09\19\i_98cd	and start screen reco	ording when a is deteo	
1	XF4B5\Administrator	9/20/2023 6:52:54 A	perf	C:\SessionRecording	as\2023\09\19\i 98cd	and start screen reco	ording when a is deteo	

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.

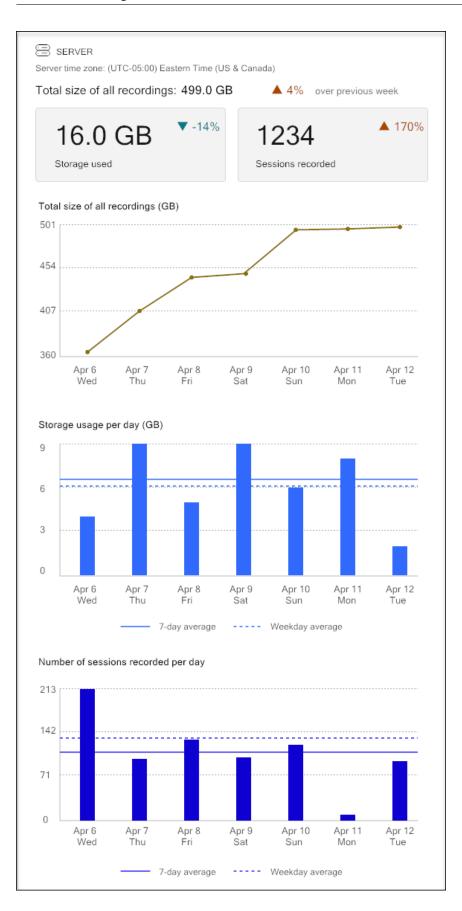
	Recording Se		sperdes					
Playback	Notifications	CEIP	Logging	RBAC	Email	Report	Cloud	•
Storage	report							
	ption allows you are outgoing en					rly. Make	sure to	
S S	end storage re	ports by	email					
(Daily							
(◯ Weekly	Mon	day	~]			
E	Email recipients	s:			-			
	-							_
	esponse report	to rece	ive event r	esponse	reports	regularly	Make	
This op sure to	esponse report tion allows you configure outgo end event resp	oing em	ail settings	on the E	reports mail tab	regularly too.	. Make	
This op sure to	tion allows you configure outgo	oing em	ail settings	on the E	reports mail tab	regularly too.	. Make	
This op sure to ∑ S	tion allows you configure outgo end event resp	oing em	ail settings ports by er	on the E	reports mail tab	regularly too.	. Make	
This op sure to ∑ S ((tion allows you configure outgo end event resp Daily	oonse re Mon	ail settings ports by er	on the E	reports mail tab	regularly too.	. Make	

Session recording storage reports

June 21, 2024

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:



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.

	necolulity be	erver Pro	operties			-		×
Playback	Notifications	CEIP	Logging	RBAC	Email	Report	Cloud	•
Storage	report							
	otion allows yo ire outgoing en					ly. Make	sure to	
√ S	end storage re	ports by	email					
(Daily							
(◯ Weekly	Mon	day	~				
E	mail recipients	s:			-			1
								_
This op	esponse report	to rece	ive event r	esponse	reports	regularly	. Make	
sure to		oing ema	ail settings	on the E	reports mail tab	regularly too.	. Make	
sure to	tion allows you configure outgo	oing ema	ail settings	on the E	reports mail tab	regularly too.	. Make	
sure to	tion allows you configure outgo end event resp	oing ema	ail settings ports by er	on the E	mail tab	regularly too.	. Make	
sure to	tion allows you configure outgo end event resp Daily	oonse re Mon	ail settings ports by er	on the E	mail tab	regularly too.	. Make]
sure to	tion allows you configure outgo end event resp Daily Weekly	oonse re Mon	ail settings ports by er	on the E	mail tab	regularly too.	. Make]

Specify file size for recordings

June 21, 2024

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.

🐴 Sessio	n Record	ing Server	Properties	;	_		×
Storage	Signing	Rollover	Playback	Notifications	CEIP	Logging	RE 1 +
before record not rol than 30	a new file ing duration led over if 00MB. File	is started on specifie the record	Files are r d, whicheve ling duration	num limit to w olled over wh er occurs first n is less than ver when the	en the file t, is reach 1 hour ar	e size or ned. Files a nd size is lo	are ess
File	size thres	hold (MB):			50		
Reco	ording dura	ation thres	hold (hours):	12		
				ОК	Cancel		Apply

- 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

December 11, 2024

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.

📴 Sessio	n Record	ing Server	Properties		_		×
Storage	Signing	Rollover	Playback	Notifications	CEIP	Logging	R[• •
	ad-balanc			he directories ultiple director			
File st	orage dire	ctories:					
	The defau		lders is em SessionRe used.	pty. cordings will t	be	Add. Modify Remo	·
them a	vailable for	or playback y for archiv	<. ved files:	rchived sessio	on record	-	
C:\Se	ssion Reco	rdingsRest	ored			Browse	e
period	of time ha	s consider is elapsed. lormant tim		t if no new data	a is writte 24	en after the	set
				ОК	Cancel		Apply

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.

	Connect	>
sessionrecordings	sessionrecordings	
Search (Ctrl+/) « 🖋	↑ Upload + Add directory Add directory Share must support SMB protocol version 3 of share must support 3 of share	
Overview	by prefix requirement. Click here to learn more.	
Access Control (IAM) Na	Westware Para and O	
ttings No	Windows Linux macOS	
Properties	To connect to this Azure file share from Win	
perations	authentication methods and run the PowerS PowerShell terminal:	hell commands from a normal (not elevated)
\$ Snapshots	Drive letter	
Backup	Z	~
onitoring	Authentication method	
Metrics	Active Directory Storage account key	
	Connecting to a share using the storage ac Utilizing Active Directory allows to different within a share. Learn more	count key is only appropriate for admin access. tiate file and folder access, per AD account,
	\$connectTestResult = Test-NetConnection srcmdstg.file.core.windows.net -Port 445 if (5connetTestResult.foreStsucceded)	
	# Save the password so the drive will pe mid exe /C "midkey /addi"strandstation	rsist on reboot
	/user: "Azure\: "	PAOH8W0e+J9kuid6p7xX11eqNMu0Xkx7
	the port SMB uses. If port 445 is available, y mounted. Your organization or internet serv	ice provider (ISP) may block port 445, howeve Azure Site-to-Site (S2S) VPN, or ExpressRoute
	Learn how to circumvent the port 445 probl	em (VPN)

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

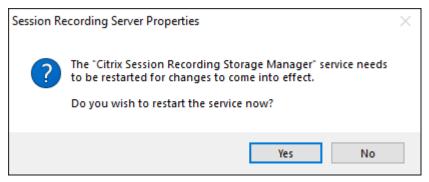
Home > srcmd >	
Access ke	
Storage account	·ys
	Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access
Cverview	keys so that you can maintain connections using one key while regenerating the other.
Activity log	When you regenerate your access keys, you must update any Azure resources and applications that access this storage ac
🔷 Tags	Storage account name srcmdstg
Diagnose and solve problems	Hide keys
Access Control (IAM)	
💕 Data migration	key1 ()
Storage Explorer (preview)	Key DSjcn/SOpzwPxhckjTgGZUZtolh8A3PA0H8W0e+J9kuid6p7xX11eqNMu0Xkx7R352f2GHRFU2PIIFi11vbE/A==
Settings	Connection string
📍 Access keys	DefaultEndpointsProtocol=https;AccountName=rAccountKey=DSjcn/SOpzwPxhckjTgGZUZtolh8A3PA0H8W0e+
S CORS	key2 🔿
Configuration	Key
A Encryption	O97VNcAmv+WpgFYYO6r3OfMyaD20sSGGpJuBgfkDYv3Z27j19TYOMbWFaz1N6riO81c2qF5JZOQVxqydmysO2A==
Shared access signature	Connection string
👸 Networking	DefaultEndpointsProtocol=https;AccountName= rAccountKey=O97VNcAmv+WpgFYYO6r3OfMyaD20sSGGpJuB
Security	
Properties	
File service	
- File shares	
Monitoring	
Insights	
Alerts	

- 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 \<filesshare

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

orage (Signing	Rollover	Playback	Notification	is CEIP	Logging	RE • •							
	l-balance				es specified tories acros									
File stor	age direc	ctories:												
Th	ne default	List of fo		pty. cordings wi	ll be	Add Modify			F 1 O 1	0.				
			used.			Remov	/e		File Stora	-	1			
									Enter a	directory	/ for storin	ng record	ed session files:	
												-	ed session files: cording\recordings	Browse
Specify a	a folder to	o tempora	rily store a	rchived ses	sion record	ings and m	nake	L				-		Browse
them ava	ailable for	r playbac	k.	rchived ses	sion record	ings and m	ake	l				-	cording \recordings	
them ava	a folder to ailable for directory sionRecor	r playbac for archi	k. ved files:	rchived ses	sion record	ings and m Browse		ŀ				-	cording \recordings	
them ava	ailable for directory	r playbac for archi	k. ved files:	rchived ses	sion record							-	cording \recordings	
them ava	ailable for directory	r playbac for archi	k. ved files:	rchived ses	sion record							-	cording \recordings	
them ava	ailable for directory	r playbac for archi	k. ved files:	rchived ses	sion record							-	cording \recordings	
them ava	ailable for directory	r playbac for archi	k. ved files:	rchived ses	sion record							-	cording \recordings	
them ava	ailable for directory	r playbac for archi	k. ved files:	rchived ses	sion record	Browse						-	cording \recordings	

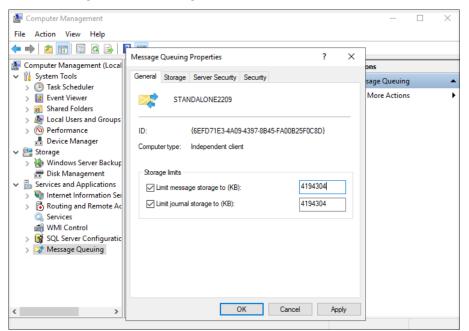
- iv. Click OK in the File Storage Directory dialog box.
- v. Click Apply in the Session Recording Server Properties window.
- vi. Click **OK** after **Apply** becomes grayed out.
- vii. Click **Yes** when you're prompted to restart the Session Recording Storage Manager service.



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).

🚳 Session Recording Agent Pro	perties	—		Х
Recording Connections Lossy	Screen Player			
Session Recording Server:	W2K19ST-Q5KID7	M.bvt.local		
- Session Recording Storage Mar	ager message queu	e		_
Protocol:	TCP ~			
HTTP/HTTPS port:	Default \vee			
Port Number:				
Message life specifies the per message queue. Message life (seconds):	iod during which da 7200	ta remains i	in the	
Session Recording Broker				
Protocol:	HTTP ~			
HTTP/HTTPS port:	Custom ~			
Port Number:	80			
L	ОК	Cancel	Арр	ly

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.

🖉 Resource Groups & Tag Editor										
Amazon S3	×	Amazon S3								
Buckets Access Grants New			unt snapshot dated: Nov 26, 2023 by Storage Lens. Metrics are generat	ed every 24 hou	rs. Learn more 🔀				View Storag	e Lens dashboard
Access Points Object Lambda Access Points Multi-Region Access Points		Total stor 3.2 GB	age	Object 1.9 k	count	Average object size 1.7 MB			enable advanced metrics in the account-dashboard [*] configurat	
Batch Operations IAM Access Analyzer for S3			5 (5) Info containers for data stored in S3. <u>Learn more</u>				C D c	opy ARN	Empty Delete	Create bucket
Block Public Access settings for this account		Q Find	buckets by name							< 1 > ©
▼ Storage Lens		N	lame	•	AWS Region			▼	Creation date	7
Dashboards		0 k	nagjiatest		US East (N. Virginia) us-east-1	Bucket and objects not public			May 25, 2023, 02:58:47 (UTC-0	4:00)
Storage Lens groups New		0 e	lasticbeanstalk-us-east-1-611320167408		US East (N. Virginia) us-east-1	Bucket and objects not public			August 16, 2022, 23:25:55 (UT	C-04:00)
AWS Organizations settings		0 0	onfig-bucket-611320167408		US East (N. Virginia) us-east-1	Bucket and objects not public			October 15, 2021, 18:06:51 (U	TC-04:00)
		0 0	itrixsessionrecording		US East (N. Virginia) us-east-1	Bucket and objects not public			September 3, 2023, 01:21:33 (UTC-04:00)
Feature spotlight 🜀		0 0	f-templates-2igjcud3smow-us-east-1		US East (N. Virginia) us-east-1	Bucket and objects not public			November 22, 2021, 10:43:00	UTC-05:00)

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.

Example Commands You can use the following example	commands to connect to the file share.	
On Microsoft Windows:	net use [WindowsDriveLetter]: \\ \\	ıser:sgw-56599C3F\smbguest

- 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:

```
1 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:

```
1 New-SmbShare -Name "YourShareName" -Path "YourSharePath" -
    FullAccess "YourUserName"
2
3 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 Record-** *ing Server installation path>\Bin* folder. By default, the Session Recording server is in stalled 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 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

June 21, 2024

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

August 15, 2024

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:

Citrix Session Recording Policy Console			
File Action View Help			
• • • 2 💼 2 🖬			
 Session Recording Policy Console Recording Policies cutom session recording policy Do not record Record entire sessions excluding audio (for everyone, with notification) Record entire sessions excluding audio with lossy screen recording enabled (for everyone, without notification) Record entire sessions excluding audio with lossy screen recording enabled (for everyone, without notification) Record entire sessions excluding audio (for everyone, without notification) Record entire sessions excluding audio (for everyone, without notification) Record entire sessions including audio (for everyone, without notification) Record entire sessions including audio (for everyone, without notification) Record only events (for everyone, with notification) Record only events (for everyone, without notification) Event Detection Policies Event Response Policies 	Rule Name	Description This rule will disable the recording of all sessions.	Action Do not record
	<		

- **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.

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:

Rules Wizard	×
	^
Step 1: Select a recording option to specify if and how a session is recorded.	
C Enable session recording with notification	
Enable audio recording	
Enable lossy screen recording	
O Enable session recording without notification	
Enable audio recording	
Enable lossy screen recording	
Enable event only session recording with notification	
O Enable event only session recording without notification	
Disable session recording	
Step 1-2: Set parameters for screen recording	
Hide specific applications during screen recording.	
Type the process names of the applications that you want to hide. Separate the process names with a semicolon (;) Black <	
< Back Next > Cance	

- **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:

CİTTIX Session Recording		
Constant of the state of t		Session info View playlist ≪ Urer name W Host name Client name Recording 1/1 No 8, 2023 50 852 PM 000312 Covents Vew: All V Q Search
Karana Rabara Karana Karana	Image: Second secon	
	ک او کی او کی او کی کی کی کی کی کی کی کی کی کی کی کی کی	R D 1804 D

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

🕎 Rules Wizard	×
Step 2: Select the rule criteria.	
Users or Groups	
☑ Published Applications or Desktop	
Delivery Groups or Machines	
☑ IP Address or IP Range	
☑ Fiter	
Step 3: Edit the rule criteria.	
Selecting a rule criterion above activates the option here. To edit, click the underlined value.	
Users / Groups: <u>Select Users or Groups</u>	
Published Resources: Select Published Applications or Desktop	
Delivery Groups / Machines: Select Delivery Groups or Machines	
IP Address / IP Range: Select IP Address or IP Range	
Filter: Specify Tags	
< Back Next >	Cancel
< DdUx IVEXL >	Cancel

- **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.

Specify Tags		×
Enter custom tags separa	ated by commas:	
	ОК	Cancel

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**.

Rules Wizard	×
Step 1: Select a recording option to specify if and how a session is recorded.	
O Enable session recording with notification	
Enable audio recording	
Enable lossy screen recording	
O Enable session recording without notification	
Enable audio recording	
Enable lossy screen recording	
O Enable event only session recording with notification	
Enable event only session recording without notification	
Disable session recording	
Step 1-2: Set parameters for screen recording	
Hide specific applications during screen recording.	
Type the process names of the applications that you want to hide. Separate the process names with a semicolon (;)	e
< Back Next > Canc	el

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.

🜉 Rules Wizard	×
Step 2: Select the rule criteria.	
Users or Groups	
Published Applications or Desktop	
Delivery Groups or Machines	
☑ IP Address or IP Range	
☑ Filter	
Step 3: Edit the rule criteria.	
Selecting a rule criterion above activates the option here. To edit, click the underlined value.	
Users / Groups: <u>Select Users or Groups</u>	
Published Resources: Select Published Applications or Desktop	
Delivery Groups / Machines: Select Delivery Groups or Machines	
IP Address / IP Range: <u>Select IP Address or IP Range.</u> Filter: <u>Specify Tags</u>	
< Back Next >	Cancel

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.

🖳 Delivery Group or Machine Name Queries	\times
	_
🖳 Create Query X	
Site Address: Citrix Cloud Controller	
Enter a site address	
Delivery Groups Machines	
Enter a Delivery Group name	
Create Cancel	
Add Remove	
Close	

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	 a) Install Broker_PowerShellSnapIn_x64.msi. 2. Clear the Citrix Cloud Controller check box. 		
Citrix Cloud Delivery Controller	a) Install the Citrix DaaS Remote PowerShell SDK. 2. Validate the Citrix Cloud account credentials. 3. Select the Citrix Cloud Controller check box.		

Use Case	Action Required
Switch from an on-premises Delivery Controller to a Citrix Cloud Delivery Controller	a) 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	 a) Uninstall the Citrix DaaS Remote PowerShell SDK and restart the machine. 2. Install Broker_PowerShellSnapIn_x64.msi. 3. Clear the Citrix Cloud Controller check box.

Validating the Citrix Cloud credentials

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

To do the manual validation:

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

Citrix Cloud		P 🛪 🖡	0 1
6 Identity and Access Management			
Authentication Administrators API Access Domains			
To use this secure client in a sile	Secure Clients are used to interact v nt connector install or to access any of our AF Name your Socure Client	Ath Citrix Cloud APIs. (s, use the customer ID • • • • as the customer paramete Create Client	r.
Name↓	ld	Creation Date	Actions
secureclient		3:53:01 PM Dec 3, 2018	

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

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 **Exec-utive**, 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.
- 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		After a rollover, the recording
was	And the new recording policy is	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

June 21, 2024

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:

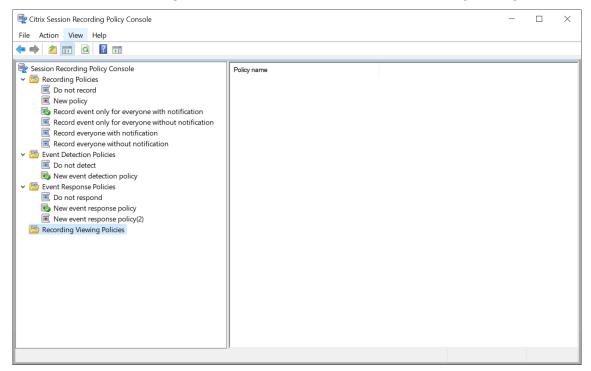
- 1. Log on to the machine hosting the Session Recording server.
- 2. From the Start menu, choose Session Recording Server Properties.
- 3. In Session Recording Server Properties, click the RBAC tab.
- 4. Select the **Allow to configure recording viewing policies** check box.

🐴 Sessio	n Record	ing Server	Properties		_		×
Storage	Signing	Rollover	Playback	Notifications	CEIP	Logging	RBAC
Record	ling viewir	ng policy —					
			configure re / Console.	ecording view	ing polici	ies in the	
		r.	r				
	Now to co	ontigure re	cording vie	wing policies			
				OK	Cancel		Apply

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**.

🖳 Rules Wizard			×
Selected user or user group who can view recordings		Add	
			_
	< Back Next >		Cancel

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.

📑 Rules Wizard					×
Selected user or user group who can v	iew recordings				
				Ado	d
Select Us	ers or Groups			×	
	s object type:				
Users or				Object Types	
From this AWDDC				Locations	
Enter the	object names to select (example	<u>s</u>):			
AWDDC	1-0001\Administrator;		[Check Names	
Adva	nced	[OK	Cancel	
				-11	
		< Back	Next >		Cancel

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

Rules Wizard	×
Step 2: Select the rule criteria.	
Users or Groups	
Published Applications or Desktop	
Delivery Groups or Machines	
Step 3: Edit the rule criteria.	
Users / Groups: All Users Published Resources: All Applications and Desktop Delivery Groups / Machines: All Delivery Groups and Machines	
< Bac	< Next > Cancel

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:

🖳 Rules Wizard	ł					×
Complete the r	ule setup.					
Recording view						
AWDDC1-000114	Administrator					
<i>Rule criteria:</i> Users / Groups	Published Resources	s Delivery Groups / Mac	hines			
Name	Location					
👌 Administrato	r AWDD	21-0001				
			< Back	Next >	Finish	Cancel

Configure event detection policies

December 6, 2024

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.

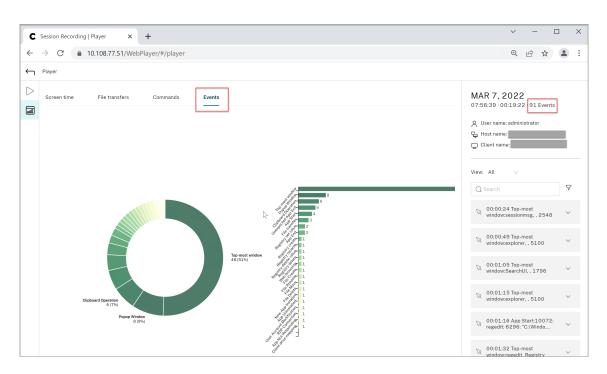
System-defined events

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:

C Session Recording Player × +		∽ — □ X
← → C	ŧ/player	• 🖻 🛧 🚨 🗄
Player		
		MAR 7, 2022 08:01:47 · 00:01:00 · 22 Events
add add	■ B v lood Ba Com Too Par Unv	Vser name: administrator GHost name: GLient name:
CastArk	Container Container	ordbaccowske, A View: Alt ∨
explore # Explore	Drammel P Cyclottel/Usycopended 2/2/2/14 (1400 M Applotest storm 191/3 Restr * Execution 2/2/2/21 (1400 M Applotest storm 191/3 Restr * Execution 2/2/21 (1400 M Applotest storm 191/3 Geht Execution 2/2/21 (1400 M Applotest storm 12/21 191/3 Geht Execution 2/2/21 (1400 M Applotest storm 12/21 191/3 12/21 Geht Execution 2/2/21 (1400 M Applotest storm 12/21 191/3 12/21 Geht Execution 2/2/21 (1400 M Applotest storm 12/21 12/21 12/21 Geht Execution 2/2/21 (1400 M Applotest storm 12/21 12/21 12/21 Geht Execution 2/21/21 14/21 12/21	Search Sea
	Windows Resolution 41/3/2011 52.64.1 Non Decument 108 Image: State of the state of the	Chealer 2500: C:Windowstexplorer
	Institution Institution Institution Institution Institution Institution Institution Institution Institution Institution Institution Institution Institution Institution Institution Institution Institution Institution Institution Institution Inst	v∾ value1380: C:Windows\explo
	I towards building Thefacter S Towards on S Thefacter Towards on S To	■ 00:00:12 Registry create:1904: C:\Program Files\C
	Hereinan The Buchetor along on ABC Fineding with Calding, Clayton	Co:00:12 Registry create:1904: C\Program Files\Cl ✓
	Don't miss what's happening Proye as Letter are the lot to box.	♥ 00:00:12 Registry create:1904: C:\Program Files\Ci
# P O A O A		► D 41 MINUTE End >> 00:00:12 Registry create:1904: C:Program >> Files:IC
► √7) 00:00:07/00:01:	00 戻 Comments 🖸 Share Current Playback X 1 🕞 Show st	ats 💱 FULL SCREEN

• Events in the Session Recording player:

Session Recording Player	
File Edit View Play Tools Help	
🖻 🕨 🔲 🗐 🏛 💠 🚿 Search: 🔹 Anytime 🔹 🛄 🎼 🦉 Advanced Search	
Norkspace	
Now Playing	
Events and Bookmarks	
1:17:04 AM App Start: 10072: regedit: 6296: "C:\Windows\regedit.exe"	
O 1:17:04 AM Top-most window: explorer 5100	
1:17:20 AM Top-most window: regedit, Registry Editor, 10072	
1:17:33 AM Top-most window: regedit, 10072	
1:17:36 AM Top-most window: regedit, Registry Editor, 10072	
1:17:36 AM Registry Create: 10072; C:\Windows\regedit.exe: HKEY_LOCAL_MACHINE\S0FTWARE\regtest\New Key #1	
1:18:00 AM Top-most window: regedit, , 10072	
1:18:02 AM Top-most window: regedit, Registry Editor, 10072	
1:18:06 AM Registry Rename: 10072: C:\Windows\regedit.exe: HKEY_LOCAL_MACHINE\SOFTWARE\regtest\New Key #1 name	
1:18:16 AM Top-most window: regedit, , 10072	
1:18:20 AM Top-most window: regedit, Registry Editor, 10072	
1:18:20 AM Registry Set Value: 10072: C:\\windows\regedit.exe: HKEY_LOCAL_MACHINE\S0FTWARE\regtest\name New Value #1	
1:18:36 AM Registry Delete Value: 10072: C:\Windows\vegedit.exe: HKEY_LOCAL_MACHINE\SOFTWARE\vegtest\name New Value #1	
1:18:36 AM Registry Set Value: 10072: C:\Windows\regedit.exe: HKEY_LOCAL_MACHINE\SOFTWARE\regtest\name version	
1:18:47 AM Top-most window: regedit, 10072	
1:18:50 AM Top-most window: regedit, Registry Editor, 10072	
🗦 1:18:50 AM : Popup Window: 10072, Registry Editor, Are you sure you want to permanently delete this key and all of its sübkeys?	
1:18:51 AM Registry Delete: 10072: C:\\Windows\regedit.exe: HKEY_LOCAL_MACHINE\SOFTWARE\REGTEST\NAME	
1:19:14 AM Top-most window: WiShell, CtxDnDSourceProxy, 7260	
1:19:14 AM App End: 10072: regedit	
1:19:25 AM Top-most window: explorer, , 5100	
🗦 1:19:26 AM - Unexpected App Exit: 744: C:\Program Files\Google\Chrome\Application\chrome.exe: C:\Windows\System32\KERNELBASE.dll	
1:19:27 AM Unexpected App Exit: 5084: C:\Program Files\Google\Chrome\Application\chrome.exe: C:\Windows\System32\KERNELBASE.dll	
1:19:29 AM Unexpected App Exit: 4860: C:\Program Files\Google\Chrome\Application\chrome.exe: C:\Windows\System32\KERNELBASE.dll	
1:19:30 AM Unexpected App Exit: 9864: C:\Program Files\Google\Chrome\Application\chrome.exe: C:\Windows\System32\KERNELBASE.dll	
1:19:30 AM Top-most window: chrome, Untitled - Google Chrome, 744	
1:19:30 AM Unexpected App Exit: 6644: C:\Program Files\Google\Chrome\Application\chrome.exe: C:\Windows\System32\KERNELBASE.dll	
1:19:32 AM Top-most window: chrome, All in one Workspace Solution for Secure Access to Apps and Data - Citrix - Google Chrome, 744	
1:19:32 AM Web browsing: citrix.com, Untitled - Google Chrome, chrome	
1:19:40 AM Top-most window: WiShell, CtxDnDSourceProxy, 7260	
1:19:53 AM Top-most window: explorer, , 5100	
2 1:20:33 AM File Create: 5100: C:\Windows\New Text Document (2).tx: 0 Bytes	
1:20:52 AM File Rename: 5100: C:\Windows\New Text Document (2).txt document.txt	
1:21:09 AM Clipboard Operation: File, explorer, C:\Windows\document.txt,	
■ 1:21:09 AM Clipboard Operation: File, explorer, C:\Windows\document.txt,	
1:21:11 AM File Move: 5100: C:\Windows\document.txt C:\Users\administrator.XF4B5\Desktop\document.txt 0 Bytes	
1:21:11 AM Clipboard Operation: Text, explorer, .	

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.

	rding Player			
File Edit V	iew Play Tools Help			
🔁 🕨 🛅 🕻	🕘 🎞 💠 湤 🛛 Search:	 Anytime 	- 💢 🕍 [🚺 Advanced Search	
Vorkspace				
🔄 Workspace - a	administrator			
👌 Search Re	esults			
🚞 Favorites				
Now Playing				
User:	administrator			
Domain:	LK6WA			i i
Application:	Desktop			
Application Delivery Group:				
	AWTSVDA-0002			
Site:	BVT DB			
Status:	Complete			
Start	9/14/2020 1:57 AM			
Events and Bo	ookmarks			
😑 1:58:36 AM A	pp End: 8976: chrome			
🗢 1:58:36 AM A	pp End: 9164: chrome			
😑 1:58:36 AM (A	vpp End: 10008: software_reporter_tool			
💛 1:58:36 AM (A	<pre>spp End: 9920: software_reporter_tool</pre>			
🔾 1:58:36 AM (A	<pre>spp End: 9900: software_reporter_tool</pre>			
🔾 1:58:36 AM A	vpp End: 10164: software_reporter_tool			
💛 1:58:36 AM (A	pp End: 8760: chrome			1.1
💛 1:58:36 AM A	pp End: 8680: chrome			
💛 1:58:37 AM A	.pp Start: 5080: conhost: 8416: \??\C:\Windows\system32\co	onhost.exe 0x4		
🔾 1:58:37 AM A	.pp Start: 8416: cmd: 8092: "C:\Windows\system32\cmd.exe"			
💛 1:58:58 AM A	pp Start: 9980: cmd: 8416: cmdhelp			
🔾 1:59:34 AM	App Start: 7260: MessageQueuingTool: 9980: C:\Users\Adi	ministrator.LK6WA\Desktop\Mes	ssageQueuingTool.exe	
💛 1:59:42 AM (A	.pp End: 7260: MessageQueuingTool			
💛 2:00:34 AM 🕖	App Start: 9144: ConsoleApplication10: 9980: C:\ConsoleApp	plication10.exe		
-	pp End: 9144: ConsoleApplication10			
	vpp Start: 9544: PING: 9980: ping_www.baidu.com -t			
_	pp End: 9544: PING			
	App Start: 9560: chrome: 9980: "C:\Program Files (x86)\Goo			
-	App Start: 1392: chrome: 9560: "C:\Program Files (x86)			
	App Start: 2644: chrome: 9560: "C:\Program Files (x86)			
-	App Start: 2256: chrome: 9560: "C:\Program Files (x86)			
-	App Start: 1416: chrome: 9560: "C:\Program Files (x86)			
-	App Start: 10172: chrome: 9560: "C:\Program Files (x86			
	App Start: 10048: chrome: 9560: "C:\Program Files (x86)			
	App Start: 8960: chrome: 9560: "C:\Program Files (x86)	\Google\Lhrome\Application\ch	rome.exe ^{***} type=rendererfield-trial-handle=1540,59,	1/5

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.

🔾 1:19:30 AM Unexpected App Exit: 6644: C:\Program Files\Google\Chrome\Application\chrome.exe: C:\Windows\System32\KERNELBASE.dll
🗢 1:19:32 AM Top-most window: chrome, All in one Workspace Solution for Secure Access to Apps and Data - Citrix - Google Chrome, 744
O 1:19:32 AM Web browsing: citrix.com, Untitled - Google Chrome, chrome
1:19:40 AM Top-most window: WfShell, CtxDnDSourceProxy, 7260

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

1:22:03 AM New App Installed: 7-Zip 19.00 (x64): Igor Pavlov: 19.00	
💛 1:22:05 AM Top-most window: explorer, , 5100	
O 1:22:08 AM Top-most window: SearchUI, , 1796	
O 1:22:08 AM Top-most window: explorer, Downloads, 5100	Ν
O 1:22:10 AM Top-most window: ShellExperienceHost, Windows Shell Experience Host, 8392	h ²
O 1:22:15 AM Top-most window: explorer, , 5100	
O 1:22:26 AM Top-most window: Uninst, 7-Zip 19.00 (x64) Uninstall, 6172	
1:22:28 AM App Uninstalled: 7-Zip 19.00 (x64): Igor Pavlov: 19.00	
 1:22:15 AM Top-most window: explorer, , 5100 1:22:26 AM Top-most window: Uninst, 7-Zip 19:00 (x64) Uninstall, 6172 	

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

T.23.00 AM Popup Window: TT32, lusting P [Local Osers and Groups (Local)/Osers], Built-in account for administering the computer/
 1:23:08 AM Popup Window: 11132, lusting P [Local Users and Groups (Local)/Users], Built-in account for administering the computer/
 1:23:09 AM User Account Modification: testuser: A user account was disabled.

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

1:24:49 AM Popup Window: 2192, Remote Desktop Connection, The remote computer could not be auther 0	nticated du
O 1:24:50 AM RDP Connection: 2192: IPaddress	
1:25:19 AM Top-most window: cmd, Administrator: Command Prompt, 10776	
🔾 1:25:38 AM Top-most window: explorer, , 5100	
🔾 1:25:40 AM Clipboard Operation: File, explorer, C:\Users\administrator.XF4B5\Desktop\confidential.docx,	

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**.

- 🔵 1:20:33 AM File Create: 5100: C:\Windows\New Text Document (2).txt: 0 Bytes -
- 🗢 1:20:52 AM | File Rename: 5100: C:\Windows\New Text Document (2).txt | document.txt |
- 1:21:09 AM Clipboard Operation: File, explorer, C:\Windows\document.txt,
- 1:21:09 AM Clipboard Operation: File, explorer, C:\Windows\document.txt,
- 🔁 1:21:11 AM File Move: 5100: C:\Windows\document.txt | C:\Users\administrator.XF4B5\Desktop\document.txt: 0 Bytes
- 🗢 1:21:11 AM Clipboard Operation: Text, explorer, ,
- 1:21:26 AM File Delete: 5100: C:\Windows\New Text Document.txt: 0 Bytes

		Top most mindow. explorer, , or ou
	1:25:40 AM	Clipboard Operation: File, explorer, C:\Users\administrator.XF485\Desktop\confidential.docx,
0	1:25:45 AM	File Transfer: 7260: Host:C:\Users\administrator.XF4B5\Desktop\confidential.docx: Client:confidential.docx: 0 Bytes
6	1:26:18 AM	Top-most window: WiShell, CtxDnDSourceProxy, 7260
$ \circ$	1:26:19 AM	Top-most window: explorer, , 5100
$ \circ$	1:26:21 AM	File Transfer: 7260: Client:confidential.docx: Host:confidential.docx: 0 Bytes
0	1:26:54 AM	Clipboard Operation: Text, cmd, , Administrator: Command Prompt
0	1:27:03 AM	Clipboard Operation: Text, cmd, , Administrator: Command Prompt File Transfer: 7260: Client:Applicationhang.exe: HostApplicationhang.exe: 7.5 KB
	4 07 00 444	

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.

Events and Bookmarks

😑 5:42:32 AM Web browsing: https://www.google.com, Google - Google Chrome, chrome -

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.

Events and Bookmarks

3:01:43 AM Web browsing: https://www.facebook.com, Facebook - Log In or Sign Up - Google Chrome, chrome 3:02:00 AM Web browsing: https://www.facebook.com, Facebook - Log In or Sign Up - Google Chrome

List of supported browsers:

- Google Chrome
- Microsoft Edge Chromium
- Mozilla Firefox

Note:

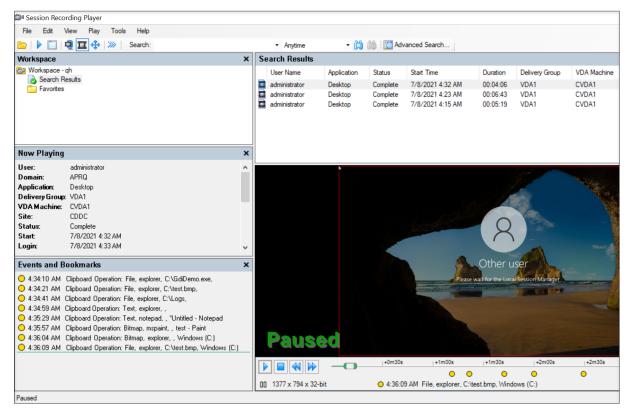
This feature requires Session Recording Version 1906 or later.

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.

Events and Bookmarks ×
1:56:08 AM Top-most window: EXCEL, Book2, 6880
○ 1:56:22 AM Top-most window: explorer, CITRIXINSTALLATIONLOGS, 7212
😑 1:56:36 AM Top-most window: Taskmgr, CdfSvc.exe, 9276
○ 1:56:39 AM Top-most window: explorer, Application.evtx, 7212
O 1:56:55 AM Top-most window: notepad++, , 4940
○ 1:56:59 AM Top-most window: explorer, Desktop, 7212
\Theta 1:57:08 AM Top-most window: WINWORD, Bisijisbb j.docx, 8896
O 1:57:13 AM Top-most window: notepad++, , 4940
○ 1:57:20 AM Top-most window: Taskmgr, CdfSvc.exe, 9276
O 1:57:34 AM Top-most window: Taskmgr, Citrix.Authentication.VirtualSmartcard.exe, 9276
○ 1:57:51 AM Top-most window: regedit, FileOperationMonitorList, 6584
O 1:58:04 AM Top-most window: notepad++, shi, 4940
○ 1:58:25 AM Top-most window: explorer, Task Switcher, 7212
1:58:26 AM Top-most window: EXCEL, Grid, 6880

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:

Events and Bo	nokmarks
10:30:55 PM	Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Tablet PC IsTabletPC
10:30:55 PM	Registry Create: 8452: C:\Windows\System32\csrss.exe: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Tablet PC
10:30:55 PM	Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\W0W6432Node\Microsoft\Windows\Tablet PC IsTabletPC
10:30:55 PM	Registry Create: 8452: C:\Windows\System32\csrss.exe: HKEY_LOCAL_MACHINE\S0FTWARE\W0W6432Node\Microsoft\Windows\Tablet PC
10:30:55 PM	Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation LastOrientation
O 10:30:55 PM	Registry Create: 8452: C:\Windows\System32\csrss.exe: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation
10:30:55 PM	Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation\NonPreserve LastAutoRequest
10:30:55 PM	Registry Create: 8452: C:\Windows\System32\csrss.exe: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation\NonPreserve
10:30:55 PM	Registry Set Value: 8452: C:\Windows\System32\csrss.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation LastOrientation
10:30:55 PM	Registry Create: 8452: C:\Windows\System32\csrss.exe: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AutoRotation
10:30:55 PM	Registry Set Value: 9992: C:\Program Files\Citrix\HDX\bin\CtxGfx.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\3\LLIndicator
10:30:55 PM	Registry Delete Value: 9992: C:\Program Files\Citrix\HDX\bin\CtxGfx.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\3 SessionHeight
10:30:55 PM	Registry Delete Value: 9992: C:\Program Files\Citrix\HDX\bin\CtxGfx.exe : HKEY_LOCAL_MACHINE\S0FTWARE\Citrix\Graphics\3] Session\Vidth
10:30:55 PM	Registry Delete Value: 9992: C:\Program Files\Citrix\HDX\bin\CtxGfx.exe : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\3 NumMonitors
10:30:55 PM	Registry Create: 9992: C:\Program Files\Citrix\HDX\bin\CtxGfx.exe: HKEY_LOCAL_MACHINE\S0FTWARE\Citrix\Graphics\3

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

÷	Player							
\triangleright		🔹 New Tab 🛛 🗙	+		۵	- a ×	NOV 18, 2021	
030		$\leftarrow \ \rightarrow \ G$	Q Search with Google or enter address				11:41:52 · 00:13:33 · 32 Events	
		🕀 Import bookmarks 👋 Getting St	inted				🖉 User name:	
				ۏ Firefox		© 	Host name: Client name: View: All	
						_	Q Search	8
			G Search with Google or enter a	lddress			© 00:00:26 Top-most window:sessionmsg., 9072	~
			a, ebay Round trip time Network (send)		• • •		00:00:28 Top-most window:explorer, , 7508	~
			Amazon Spensored Spensored CPU usage Memory usage	32%	Redde Weipedia Twitter 88 MB (73%)		© 00:00:48 App Start:9632: conhost: 2748: \??\C:\Win	~
			Recommended by Pocket Learn more				© 00:00:48 App Start:2748: cmd: 7508: C:\Windows\sys	~
			Gilifitian		Y A Se Se		00:00:48 App Start:11232: powershell: 2748: powers	~
			theguardian.com aed	n.co e Good Guy/Bad Guy Myth	smartasset.com Learn the Cost of a Financial		© 00:00:55 App End:9632: conhost	~
		: P ロ , é 🖡	France's top serial killer expert Pop An intrepid expert with dozens of books to bat	o culture today is obsessed with the tile between good and evil. Traditional	Advisor Find information to help you choose the		00:00:55 App End:11232: powershell	~
	•	√7) 00:05:0	6/00:13:33 🗐 Comments 🔀 Share Cur	rent Playback	Xı	Hide stats		~

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.

1:23:48 AM. Popup Window. 2132, Remote Desktop Connection. Connection to: 1 Paddress Initiating remote connection...
 1:24:05 AM. Popup Window. 2132, Remote Desktop Connection, Remote Desktop can't connect to the remote computer for one of these reasons: \n\n1] Remote access to the server is not enabled\n2] The remote computer is turned off\n3] The remote.

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 player, see the following screen capture:

	Events and Bookmarks	×
	9:57:23 AM Printing activity: C:\ttt.txt was printed on Micro	soft Print to PDF, pages printed: 1
i		

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, Ses-

sion 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.

Session Recording Player										- 0	×
File Edit View Play Tools Help											
눌 🕨 🛅 🗐 🧰 💠 ≫ 🛛 Search:		 Anytime 	- 🛍	🎼 🚺 Adv	anced Search						
Workspace >	× Sear	ch Results									×
Workspace - qh Search Results Favorites		ser Name	Application	Status	Start Time	Duration	Delivery Group	VDA Machine	Events Only	Size	
		ministrator	Desktop	Complete	7/8/2021 4:32 AM	00:04:06	VDA1	CVDA1	No	1,134 KB	
		ministrator	Desktop Desktop	Complete Complete	7/8/2021 4:23 AM 7/8/2021 4:15 AM	00:06:43 00:05:19	VDA1 VDA1	CVDA1 CVDA1	No No	796 KB 776 KB	
	1	Iministrator	Desktop	Complete	77072021 4.15 AM	00.05.15	VDAT	CVDAT	NO	776 ND	
Now Playing >	×										
User: administrator ADD ADD ADD ADD ADD ADD ADD ADD ADD AD											
Application: Desktop											
Delivery Group: VDA1 VDA Machine: CVDA1											
Site: CDDC											
Status: Complete											
Start 7/8/2021 4:23 AM											
Login: 7/8/2021 4:23 AM	- 1				Co	ntent b	locked				
Events and Bookmarks	×						nt detecte	ed			
4:26:00 AM Notepad++;Sentive content detected;;					BOILING						
4:29:13 AM Notepad++Sentive content detected;;											
				+0h	01m +0h02r	m	+0h02m	+0h04m	+0h05m	+0h06	
											•
	⊳ s	ize: 796 KB		0 4:26:0	0 AM Notepad++;Sentiv	e content dete	cted;;			7/8/2021 4	:26:18 AM
laying											

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.

🐝 Session	Recording Ag	jent Prop	oerties		—		×	
Recording	Connections							
Session recording Select this option to enable policy-based session recording on this VDA machine. If this option is not selected, session recording is disabled on this machine.								
Custom event recording Select this option to allow third party applications to inject custom data into the recorded session while recording is in progress. This data is available during playback.								
[™] machine								
			OK	Car	ncel	Ap	oply	

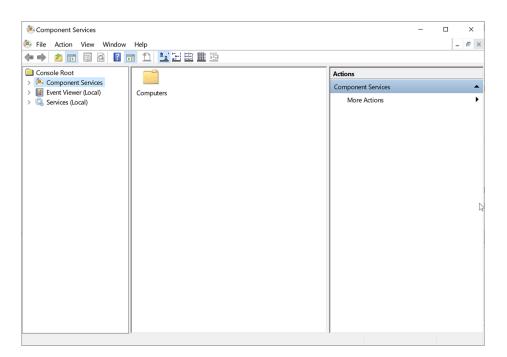
2. Grant users permission to invoke the Session Recording Event API (IUserApi COM interface).

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.

📨 Run				×
			ram, folder, docu /indows will open	
Open:	dcomcnfg.e	≥xe		~
		ОК	Cancel	Browse



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.

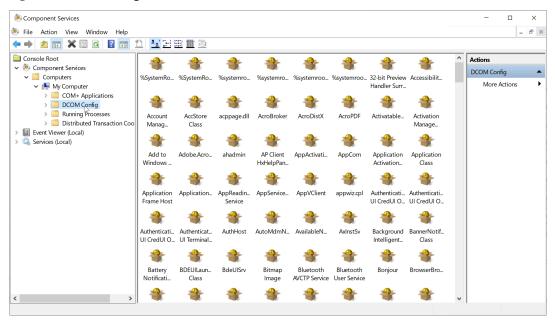
les Component Services		- 🗆 ×
🖲 File Action View Window I	Help	- <i>5</i> ×
	Name	Actions
 Component Services Computers 	COM+ Applications	My Computer
> Ny Computer	DCOM Config	More Actions
	components on Coordina	
> 🤹 Services (Loca View	>	
New Windo	ow from Here	
Export List		
Properties		
Help	10	
Opens the properties dialog box for the		

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

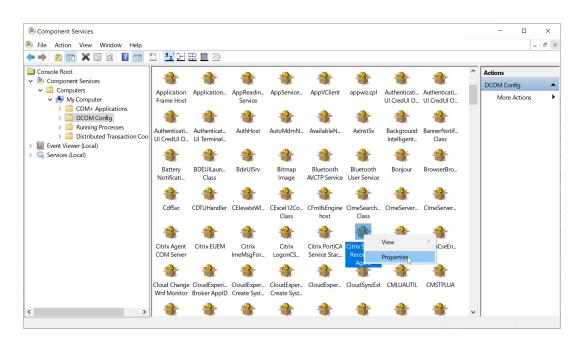
My Computer Propertie	s		?	×
General Default Protocols	Options COM Sea		Properties MSDT0	
also set limits on ap	s allowed default acce plications that determi Modifying access permi ions to start, connect, f Edit Limits	ne their own pe ssions can affe function and/or	rmissions	ity
activate objects. Yo determine their own	s allowed by default to u may also set limits o permissions. Modifying launch and a ability of applications to	n applications t	hat sions can	
	Edit Limits	Edit [Default	
Learn more about <u>settin</u>	g these properties.			
	ОК	Cancel	Ap	oply

aunch and Activation Permission	I	?	×
Default Security			
Group or user names:			
SYSTEM Administrators (CNENG5REC Manual Interactive	MKF8PX\Adminis	trators)	
	Add	Remove	
Permissions for SYSTEM	Allow	Deny	
Permissions for SYSTEM	Allow	Deny	1
	Allow		
Local Launch Remote Launch Local Activation	Allow		
Local Launch Remote Launch	Allow		

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 Reco	rding Age	nt Properti	es		?	×
General Location	Security	Endpoints	Identity			
Launch and A	ctivation Pe	rmissions				
⊖ Use Defau	lt					
 Customize 				E	dit	
Access Permis	sions					
⊖ Use Defau	lt					
Customize				E	dit	
Configuration	Permissions	5				
O Use Defau	lt					
Customize				E	dit	
Learn more about	setting the	se properties				
		ОК	C	ancel	App	bly

Session Recording 2411

			nt Properti				
eneral	Location	Security	Endpoints	Identity			
La	unch and a	Activation	Permission			?	×
s	ecurity						
	Group or us	er names:					
	SYST						
	CitrixA	dmin (CNE	NG5REQM	(F8PX\Citri	xAdmin)	
				Add		Remove	
				Add		Remove	
	Permission	s for SYSTI	EM		llow	Remove	,
-	Local La	unch	EM			Deny	
	Local La Remote	unch Launch	EM			Deny	
	Local La Remote Local Ac	unch Launch tivation	EM			Deny	
	Local La Remote Local Ac	unch Launch	EM			Deny	
	Local La Remote Local Ac	unch Launch tivation	EM			Deny	
	Local La Remote Local Ac	unch Launch tivation	EM			Deny	
	Local La Remote Local Ac	unch Launch tivation	EM			Deny	
	Local La Remote Local Ac	unch Launch tivation	EM			Deny	1
.e	Local La Remote Local Ac	unch Launch tivation	EM			Deny	

Note:

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

- 3. Start a Citrix virtual session.
- 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

Parameter	Description	Required or Optional
-Reason	The reason that content is	Optional
	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.	
-AheadSeconds	This parameter is available for	Optional
	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.	

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

23 Administrator: PowerShell	- 0	o x
SYNTAX Session-Pause [-App] <string> [[-Reason] <string>] [<commonparameters>]</commonparameters></string></string>		
DESCRIPTION User can use it to pause current session.		
RELATED LINKS		
REMARKS To see the examples, type: "get-help Session-Pause -examples". For more information, type: "get-help Session-Pause -full". For technical information, type: "get-help Session-Pause -full".		
PS C:\Program Files\Citrix\SessionRecording\Agent\bin> Session-Pause -App Notepad++ -Reason 'Sensitive content detected' -Ahe Getting type from local machine reating instance uperying TuserApi interface *** Connected ***		ds 2
Formatting data for send Calling IUserApi.LogDataWithExtData *** Call Success *** 5 C:Program Files/Citrix\SessionRecording\Agent\bin>		

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 > Ad-vanced 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.

🗊 Advanced Search		×
Saved Searches Save	As Reset Values	
Search Criteria		
Common Date/Time Events	Other	
	ents inserted by third-party applications can be tagged while s tagged, set the search criteria below.	a session is being recorded. To search for
Event text:		
Citu Citu Citu Citu Citu Citu Citu Citu	tx.EventMonitor.AppEnd tx.EventMonitor.AppStart tx.EventMonitor.CDMUSBDriveAttach tx.EventMonitor.Clipboard tx.EventMonitor.FileCreate tx.EventMonitor.FileDelete tx.EventMonitor.FileMove tx.EventMonitor.FileRename tx.EventMonitor.GenericUSBDriveAttach	
Query Builder Citr Citr Find the 200 most relevant re Citr Citr	ix.EventMonitor.TopMost	^ ~
Search Stop		Close

Note:

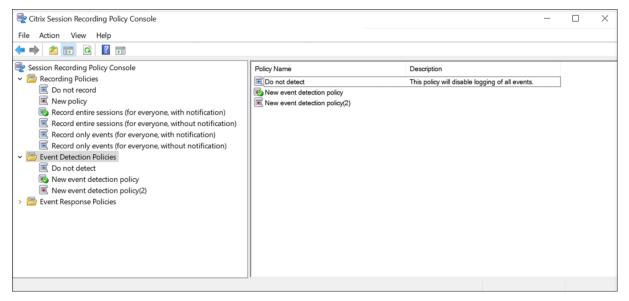
- The **Event type** list itemizes all event types. You can select an event type to search. Selecting **Any Citrix-defined event** means to search for all recordings with any type of events logged by Citrix Session Recording.
- The **Event text** filter supports partial match. Wildcards are not supported.

- 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

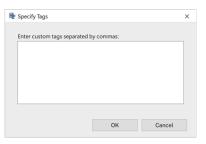
Considerations

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.



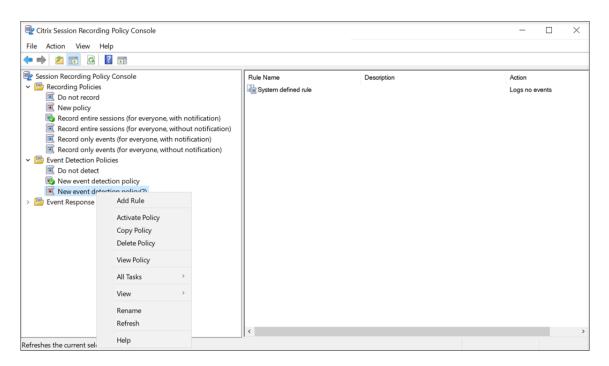
Contextual access (smart access) is available for Session Recording 2402 and later. It lets you apply policies based on the user access context including:

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



- 5. Right-click the new event detection policy and select Add Rule.
 - a) Specify one or more target events to monitor by selecting the check box next to each event type. Scroll down the window to view all available event types.

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

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

Note:

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

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

Note:

- To capture the start and end of an application, add the process name of the application in the App monitoring list. For example, to capture the start of Remote Desktop Connection, add the process name mstsc.exe to the App monitoring list. When you add a process to the App monitoring list, applications driven by the added process and its child processes are monitored. Session Recording adds the process names, cmd.exe, powershell.exe, and wsl.exe, to the App monitoring list by default. If you select Log app start events and Log app end events for an event detection policy, the starts and ends of the Command Prompt, PowerShell, and Windows Subsystem for Linux (WSL) apps are logged regardless of whether you manually add their process names to the App monitoring list. The default process names aren't visible on the App monitoring list.
- Separate process names with a semicolon (;).
- Only the exact match is supported. Wildcards aren't supported.
- Process names you add are case-insensitive.
- To avoid an excessive number of events from flooding the recordings, do not add any system process names (for example, explorer.exe) and web browsers in the registry.
- Log file operations: Logs operations on target files in the File monitoring list and logs file transfers between session hosts (VDAs) and client devices (including mapped client drives and generic redirected mass storage devices). Selecting this option triggers the logging of file transfers, no matter whether the File monitoring list is specified.
 - File events presented in the web player

Q file	8
© 00:01:32 File transfer:10804: Host:C:\Users\ctxa	
© 00:01:40 File transfer:10804: Client:GAHeartBea	۲_b
© 00:01:56 File transfer:10804: Cl Text Docu	ient:New 🗸
00:01:59 File transfer:10804: Client:DataVisualCo	~

- File events presented in the Session Recording Player

Events and Book	marks
O 5:57:44 PM File	Create: 32. \\Client\C\$\Personality.ini: 33 Bytes . Transfer: 6404: Host:C\Users\4dministrator.RMFPA\Desktop\EndProcessMonitorHook.sln: Client\E\$\EndProcessMonitorHook.sln: 1010 Bytes Create: 6404: \\Client\E\$\EndProcessMonitorHook.sln: 1010 Bytes
-	Transfer: 2836: Host:C:\Users\Administrator.RMFPA\Desktop\EndProcessMonitorHook.shr: Client:EndProcessMonitorHook.shr: 1010 Bytes

• 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.

Events and Bookmarks 5:42:32 AM Web browsing: https://www.google.com, Google - Google Chrome, chrome

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.

Events and Bookmarks ×
O 1:56:08 AM Top-most window: EXCEL, Book2, 6880
○ 1:56:22 AM Top-most window: explorer, CITRIXINSTALLATIONLOGS, 7212
○ 1:56:36 AM Top-most window: Taskmgr, CdfSvc.exe, 9276
O 1:56:39 AM Top-most window: explorer, Application.evtx, 7212
O 1:56:55 AM Top-most window: notepad++, , 4940
😑 1:56:59 AM Top-most window: explorer, Desktop, 7212
😑 1:57:08 AM Top-most window: WINWORD, Bisijjisbb j.docx, 8896
O 1:57:13 AM Top-most window: notepad++, , 4940
😑 1:57:20 AM Top-most window: Taskmgr, CdfSvc.exe, 9276
😑 1:57:34 AM Top-most window: Taskmgr, Citrix.Authentication.VirtualSmartcard.exe, 9276
😑 1:57:51 AM Top-most window: regedit, FileOperationMonitorList, 6584
😑 1:58:04 AM Top-most window: notepad++, shi, 4940
⊖ 1:58:25 AM Top-most window: explorer, Task Switcher, 7212
1:58:26 AM Top-most window: EXCEL, Grid, 6880

- 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.
- 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.

ule1		ıle:						
ule l								
Provide a desc	-	this rule:						
Specific user rule	filter							
Enable this rul	e							
ummary (click		dit):						
ptions selected:								
og &CDM mappe	d USB event	ts						
ule criteria:								
Users / Groups	Published F	Resources	Delivery Grou	ps / Machines	IP Address / IP	Range		
Name		Location						
Name		Location						
ame 🔒 user		JZUAI-SF	IS-1					
-			IS-1					
-			IS-1					
-			IS-1					
-			15-1					
-			15-1					
-			IS-1					
-			IS-1					
-			IS-1					

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:

gistry Editor				- 🗆
Edit View Favorites Help				
V Citrix	^ Name	Туре	Data	
> - CdfCaptureService	ab (Default)	REG_SZ	(value not set)	
Citrix Desktop Delivery Controller	ab AppMonitorList	REG_MULTI_SZ	cmd.exe powershell.exe wsl.exe	
> - Citrix Virtual Desktop Agent	EnableAccountChangeEvents	REG DWORD	0x00000000 (0)	
CtxExceptionHandler	Right EnableAppChangeEvents	REG_DWORD	0x00000001 (1)	
> - CtxHook	EnableAppFaultEvents	REG DWORD	0x00000000 (0)	
Director FileTransfer	Right EnableAppLaunchEvents	REG DWORD	0x00000000 (0)	
	EnableCDMUSBDriveEvents	REG DWORD	0x00000000 (0)	
> - GroupPolicy	EnableClipboardEvents	REG_DWORD	0x00000000 (0)	
- HDXMediaStream	EnableFileOperationMonitorEvents	REG DWORD	0x00000000 (0)	
	EnableGenericUSBDriveEvents	REG DWORD	0x00000000 (0)	
	EnableIdleEvent	REG DWORD	0x00000001 (1)	
lcak2m	Right EnablePerfDataEvents	REG DWORD	0x00000000 (0)	
ImageAnalysis	B EnablePopupWindowEvents	REG DWORD	0x00000000 (0)	
> - Install	ReableRDPConnectionEvents	REG_DWORD	0x00000000 (0)	
- Location	Bill EnableRegistryOperationMonitorEvents	REG_DWORD	0x00000001 (1)	
	W EnableSessionEvents	REG DWORD	0x00000001 (1)	
> - MSLicensing	Right EnableTopMostEvents	REG DWORD	0x00000000 (0)	
> Portica	Bill EnableWebBrowsingActivities	REG DWORD	0x00000000 (0)	
	ab FileOperationMonitorList	REG MULTI SZ		
> - ServerFTA	1016EventActivePktNumThrottle	REG_DWORD	0x00000000 (0)	
SmartAuditor	101eEventActivePktSizeThrottle	REG_DWORD	0x00000000 (0)	
Agent	101/2010 IdleEventActiveThrottle	REG DWORD	0x00000000 (0)	
SessionEvents	10 IdleEventThrottle	REG DWORD	0x00000000 (0)	
6	ab RegistryOperationMonitorList	REG MULTI SZ	\REGISTRY\MACHINE\SOFTWARE	
> - StackAgentInfo				
> - SvcHost				
> - UniversalPrintDrivers				
VdaCEIP	~			

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.

Registry Value	Description
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).
EnableFileOperationMonitorEver	nt 1 : enables detecting file operations; 0 : disables detecting file operations (default value data).
FileOperationMonitorList	Specifies target folders to monitor. No folder is specified by default, which means no file operation is captured by default.
EnableGenericUSBDriveEvents	 1: enables detecting the insertion of generic redirected USB mass storage devices; 0: disables detecting the insertion of generic redirected USB mass storage devices (default value data).
EnablePerfDataEvents	 1: enables the session data overlay feature; 0: disables the session data overlay feature (default value data).
EnablePopupWindowEvents	 1: enables detecting popup window events; 0: disables detecting popup window events (default value data).

Registry Value	Description
EnableRDPConnectionEvents	 1: enables detecting RDP connections; 0: disables detecting RDP connections (default value data).
EnableRegistryOperationMonito	orE leet tables 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

June 21, 2024

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:

∑ Mark Un 0A-0002;
A-0002.
A 0002,
MAIL] DO NO

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:



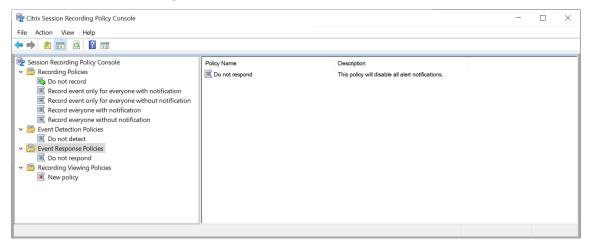
System-defined event response policy

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.

🗮 Rules Wizard	×
Step 1-1: Select one or more of the following options.	
Email alert when a session start is detected.	
Trigger response actions when a session event is detected	
Configure event triggers and responses	
Step 1-2: Enter email addresses for the alert recipients.	
Email recipients:	
Type the email addresses who will receive alerts according to this rule. Separate the addresses with a sem	sicolon (;).
Step 1-3: Set parameters for dynamic screen recording. Screen recording time span after we detect an event:	
How many minutes do you want us to record the screen after we detect an event?]
Screen recording time span before we detect an event:	,
How many seconds of the screen recording do you want us to keep before we detect an event?	
Time interval between a session operation notice and its execution (available for session lock, log off, and	disconnection)
How many seconds do you want us to hold a session operation after we issue the notice?	
Enable lossy screen recording	
< Back Next >	Cancel
C.SOUR	Call Incl

- 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.

Session Recording 2411

ollover	Playback	Notfications	CEIP	Logging	RBAC	Email	Cloux	• •	
SMTP server: smtp.office36		.com							
Port:		587	$\mathbf{\nabla}$	Enable S	SL.				
Display name: Session Rec		ording /							
Email address: srt-		srt-no-reply@o	rt-no-reply@outlook.com						
Passwo	rd:	•••••							
Email	title		- I	Email body					
	User na	me		User	rname				
	Domain	name		Dom 🗸	ain name				
	Start tim	e		Start	time				
	Delivery	group							
	Applicat	ion							
	VDA Ma	chine							
				Reci	ording UR	L			
Allo	w sendin	g email notifica	ations						
			_	ок	Cance		Appl		

Note:

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

Validation	Error	×
	The email account can't send message successfully, please check your configuration.	
	The SMTP server requires a secure connection or the client was not authenticated. The server response was: 5.7.57 SMTP; Client was not authenticated to send anonymous mail during MAIL FROM [BN3PR03CA0072.namprd03.prod.outlook.com]	
	OK	

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

					Dimension 1						Dimension 2					Send email	Session operations		Description
	Event type is	Web Browsing	\sim	and	URL	\sim	Includes	\sim	and	nd	Tab title	~	Includes \	/	then	\checkmark	Disconnect session	\sim	
	Or event type is	Top Most	\sim	and	App name	\sim	Includes	\sim	and	nd	Window title	~	Includes N	1	then		Start screen recor	\sim	
	Or event type is	File Rename	\sim	and	Path	\sim	Includes	\sim	and	nd	Name	~	Includes N	/	then		Log off session	\sim	
	Or event type is	File Delete	\sim	and	Path	\sim	Includes	\sim	and	nd	File size (MB)	~	Greater th	1	then		Lock session	\sim	
•	Or event type is	File Transfer	\sim	and	File source	\sim	Equals	\sim	and	nd	File name	~	Includes \	/	then		None	~	
	Or event type is		\sim	and		\sim		\sim	and	nd		~	×	/	then			~	

Note:

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

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

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

🕎 Rules Wizard	\times
Step 1-1: Select one or more of the following options.	_
Email alert when a session start is detected.	
Trigger response actions when a session event is detected	
Configure event triggers and responses	
Step 1-2: Enter email addresses for the alert recipients.	
Email recipients:	
Type the email addresses who will receive alerts according to this rule. Separate the addresses with a semicolon (.).	
Step 1-3: Set parameters for dynamic screen recording.	
Screen recording time span after we detect an event:	
How many minutes do you want us to record the screen after we detect an event?	
Screen recording time span before we detect an event:	
How many seconds of the screen recording do you want us to keep before we detect an event?	
Time interval between a session operation notice and its execution (available for session lock, log off, and disconnection)	
How many seconds do you want us to hold a session operation after we issue the notice?] [
Enable lossy screen recording	
< Back Next > Cancel	
	_

- 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

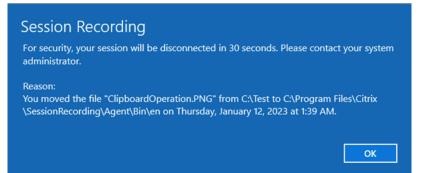
seconds of the screen recording you want to keep before events are detected. This feature is available for both virtual desktop and app sessions. The value ranges from 1 to 120. Setting the value to any of 1 through 10 makes the value 10 effective. If you leave the value unspecified, the feature does 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

Event type	Dimension	Option
	App name	Includes, Equals, Matches
Top Most		
	App name	Includes, Equals, Matches
	Windows title	Includes, Equals, Matches
Web Browsing		
	URL	Includes, Equals, Matches
	Tab title	Includes, Equals, Matches
	Browser name	Includes, Equals, Matches
File Create		
	Path	Includes, Equals, Matches
	File size (MB)	Greater than, Between, Smaller than
File Rename		
	Path	Includes, Equals, Matches
	Name	Includes, Equals, Matches
File Move		
	Source path	Includes, Equals, Matches
	Destination path	Includes, Equals, Matches
	File size (MB)	Greater than, Between, Smaller than
File Delete		
	Path	Includes, Equals, Matches
	File size (MB)	Greater than, Between, Smaller than
CDM USB		
	Drive letter	Equals
Generic USB		
	Device name	Includes, Equals, Matches
Idle		
	idle duration (Hrs)	Greater than

Event type	Dimension	Option
File Transfer		
	File source	Equals ("host"or "client")
	File size (MB)	Greater than
	File name	Includes, Equals, Matches
Registry Create		
	Key name	Includes, Equals, Matches
Registry Delete		
	Key name	Includes, Equals, Matches
Registry Set Value		
	Key name	Includes, Equals, Matches
	Value name	Includes, Equals, Matches
Registry Delete Value		
	Key name	Includes, Equals, Matches
	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		

Event type	Dimension	Option
	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

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

🖳 Rules Wizard	<
Step 2: Select the rule criteria.	
Users or Groups]
Published Applications or Desktop	
Delivery Groups or Machines	
☑ IP Address or IP Range	
☑ Filter	
Step 3: Edit the rule criteria.	
Selecting a rule criterion above activates the option here. To edit, click the underlined value.]
Users / Groups: Select Users or Groups	
Published Resources: Select Published Applications or Desktop	
Delivery Groups / Machines: <u>Select Delivery Groups or Machines</u> IP Address / IP Range: <u>Select IP Address or IP Range.</u>	
Filter: Specify Tags	
< Back Next > Cancel	1
	1

- 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.

Specify Tags		×
Enter custom tags separ	ated by commas:	
	,	

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.

High availability and load balancing

June 21, 2024

This section guides you through the following settings:

- Load balance Session Recording servers
- Configure database high availability

Load balance Session Recording servers

October 21, 2024

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 load 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.
- 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:

```
1
   <redirections xmlns="msmq-queue-redirections.xml">
2
           <redirection>
                        <from>http://<ADCHost>*/msmq/private$/
3
                           CitrixSmAudData</from>
                        <to>http://<LocalFqdn>/msmq/private$/
                           CitrixSmAudData</to>
           </redirection>
5
6
           <redirection>
                        <from>https://<ADCHost>*/msmq/private$/
7
                           CitrixSmAudData</from>
8
                        <to>https://<LocalFqdn>/msmq/private$/
                           CitrixSmAudData</to>
           </redirection>
10 </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 SrServerCon-figurationSync.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 <AD-CHost> command, where <ADCHost> is the created FQDN of the Citrix ADC VIP address.
 - d) After the script runs, the **EnableLB** value is added to the other Session Recording server registry keys and an **sr_lb_map.xml** file is added to the **C:\Windows\System32\msmq\Mapping** path.

On the machine where you installed the Session Recording agent, do the following in Session Recording Agent Properties

- If you choose the HTTP or the HTTPS protocol for the Session Recording Storage Manager message queue, type the FQDN of the Citrix ADC VIP address in the **Session Recording Server** text box.
- If you choose the default TCP protocol for the Session Recording Storage Manager message queue, type the Citrix ADC VIP address in the **Session Recording Server** text box.

On the machine where you installed the Session Recording Player, do the following Add the Citrix ADC VIP address or its FQDN as the connected Session Recording server.

On the SQL Server where you installed the Session Recording Database, do the following Add all the Session Recording server machine accounts to the shared Session Recording Database and assign them with the **db_owner** permission.

Configure database high availability

July 4, 2024

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\SmAudDatabaseIn
- 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\LoggingDatabaseFailoverPartner.
- 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

December 4, 2024

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

June 21, 2024

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

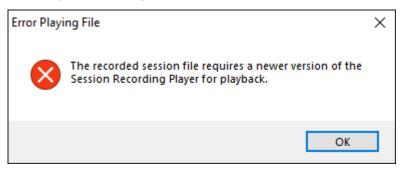
Launch the Session Recording Player

June 21, 2024

Launch the Session Recording player

Note:

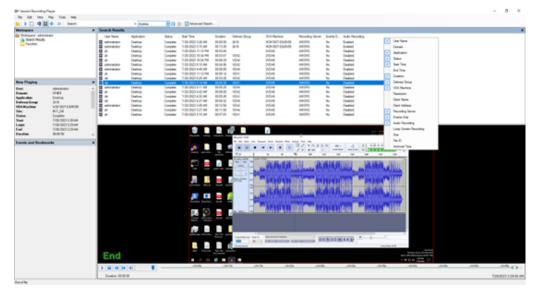
- If a recording contains blocked content, Session Recording skips it. However, if you navigate to the blocked period, your playback shows a black screen and a message indicating that that content is blocked. To use this feature, use Session Recording 2012 and later.
- If you are using the Session Recording 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.

№ Session Recording Player File Edit View Play Tools Help									- 0	×
File Edit View Play Tools Help P Image Teach (1990) Search:			 Anytime 	- 🛱	🚵 🛛 🛅 Advanced Sean	sh				
forkspace	×	Search Results							_	-
Workspace - administrator		User Name	Application	Status	Start Time	Duration	Delivery Group	VDA Machine	EventOnly	
Search Results		administrator	Desktop	Complete	5/14/2021 4:44 AM	00:00:33	DesktopVDA		No	1
Eavorites		administrator	Desktop	Complete	5/13/2021 10:58 PM	00:03:40	TSAgent0		No	
		administrator	Desktop	Complete	5/13/2021 10:57 PM	00:01:06	TSAgent0		Yes	
		administrator0	Desktop	Complete	5/9/2021 5:35 PM	04:21:28	TSAgent0		Yes	
		administrator0	Desktop	Complete	5/9/2021 5:35 AM	12:00:01	TSAgent0		Yes	
		administrator0	Desktop	Complete	5/8/2021 5:30 PM	12:05:01	TSAgent0		Yes	
ow Playing		administrator0	Desktop	Complete	5/8/2021 5:27 AM	12:03:02	TSAgent0		Yes	
		administrator0	Desktop	Complete	5/8/2021 5:23 AM	00:02:54	TSAgent0		No	
ser: administrator	^	administrator	Desktop	Complete	5/8/2021 5:18 AM	00:04:44	TSAgent0		No	
omain: UQYEB	- I.	administrator	Desktop	Complete	5/8/2021 5:16 AM	00:01:40	TSAgent0		No	
pplication: Desktop		administrator	Desktop	Complete	5/8/2021 2:27 AM	00:02:20	TSAgent0		Yes	н
elivery Group: TSAgent0 DA Machine: W2K16ST-738CGJG		dministrator	Desktop	Complete	5/8/2021 2:17 AM	00:05:37	TSAgent0		Yes	1
vents and Bookmarks	×									
2:20:56 AM App Start: 10632: firefox: 2336: "C:\P 2:20:56 AM Top-most window: explorer, test, 2336										
) 2:20:58 AM App Start: 4420: firefox: 10632: "C:\P) 2:21:05 AM App End: 10632: firefox) 2:21:07 AM Top-most window: firefox, 关闭 Firef.										
2:21:08 AM App End: 4420: firefox										
2:21:09 AM Top-most window: explorer, , 2336				Event	Only Record	lina				
2:21:15 AM App Start: 8404: firefox: 7928: "C:\Pt.						2				
2:21:15 AM App Start: 7928: firefox: 2336: "C:\Pt.										
) 2:21:21 AM Top-most window: firefox, 关闭 Firef										
2:21:21 AM App End: 7928: firefox										
2:21:26 AM Top-most window: explorer, , 2336										
2:21:26 AM App End: 8404: firefox										
2:22:36 AM App Start: 10600: firefox: 10484: "C:\.		Engl								
2:22:36 AM App Start: 10484: firefox: 2336: "C:\P		End								
) 2:22:40 AM Top-most window: firefox, 关闭 Firef.	•									
				+0h01m	+0h02m	00	+0h03m	+0h04m	+0h05m	-0

• To show all recording files of a recorded session, right-click a recording on the list and choose **Follow up**.

🕮 Session Rec													- 0	>
File Edit \	/iew Play Tools Help													
눧 🕨 🛄 I י	👰 🎞 💠 ≫ Search:				 In last 24 h 	iours	- 🛱 🕅	Advanced S	Search					
Workspace		×	Search I	Resu	lts									
Workspace - / Search Ri Favorites			User N adminis adminis adminis adminis adminis adminis	trator		Con Con Con	nplete nplete nplete nplete	Start Time 5/8/2021 5:27 AM 5/8/2021 5:23 AM 5/8/2021 5:18 AM 5/8/2021 5:16 AM 5/8/2021 2:27 AM 5/8/2021 2:17 AM	Duration 01:03:10 00:02:54 00:04:44 00:01:40 00:02:20 00:05:37	TSAgent0 TSAgent0 TSAgent0 TSAgent0	φ.	VDA Machine W2K16ST-738CG W2K16ST-738CG W2K16ST-738CG W2K16ST-738CG W2K16ST-738CG W2K16ST-738CG	JG No JG No JG No JG Yes)nly
New Playing		×			Move to Folder	-								
	W2K16ST-738CGJG	î		3	Copy to Folder Properties									
Site: Status: Start Login Events and B	site Complete 5/8/2021 2:27 AM 5/8/2021 2:27 AM	×												
 2:28:54 AM 2:29:01 AM 2:29:02 AM 2:29:02 AM 2:29:02 AM 2:29:12 AM 2:29:15 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:20 AM 2:29:21 AM 2:29:21 AM 2:29:21 AM 2:29:21 AM 	App Start 9168 firefox 2328: "C.VPL. Toomott window: firefox, Mozalle Fin. Web horwing: http://x195.com.[55: opmott window: explore, 1.0772 Toomott window: Shellipperincedt, Toomott window: Shellipperincedt, File Rename: 1072; C.Vearti& Htt 15: Rename: 1072; C.Vearti& Htt 15: pp End 10168: firefox upp End 1956; firefox upp End		En	ıd										
	pp End: 9228: conhost pp End: 2276: pingsender			•		+0m 15s	+0m30s		+1m00s	+1m15s	+1m30s	+1m45s	+2m00s	1
	opp End: 2276: pingsender opp End: 2328: firefox	-	Deskt			0 2:29:23	M 8608-	o 🚥 (• •		000	• • • • • • • • • • • • • • • • • • • •	5/8/2021 2:2	

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

June 21, 2024

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

June 21, 2024

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

June 21, 2024

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 multisession 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**.

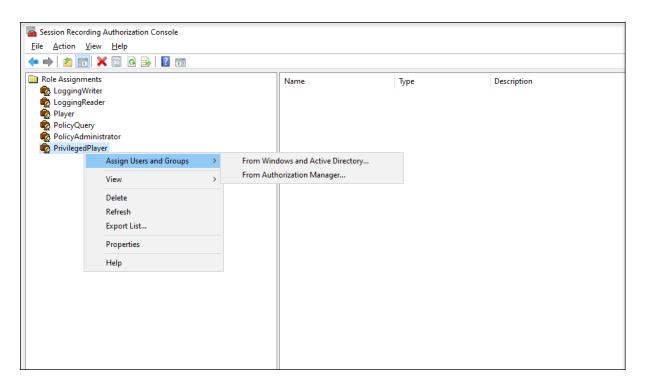
Place access restrictions on recordings

June 21, 2024

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:

Recording Player											-		×
File Edit View Play Tools Help													
📁 🕨 📋 💐 🎞 💠 ≫ Search:				 Anytime 		• 📖 🏨 🕎 Advance	d Search						
Workspace	x	Search Results											×
Workspace - administrator		User Name	Ap	plication	Status	Start Time	Duration	Delivery Group	VDA Machine	Recording Ser	Size	Access r	estrict
Search Results		administrator		addan .	Comoloto	8/30/2022 12:02 AM	00:00:27			AUTO_INSTA	244 KB		
Restricted		dministrator				B/30/2022 12:01 AM	00:00:35			AUTO_INSTA	775 KB	No	
				Follow up									
				Place access restric	tions								
			36	Delete									
				Move to Folder									
Now Playing	×	٢		Copy to Folder									>
			3	Properties									
Events and Bookmarks	×												
Events and Dookmarks	^												
2 files													

View for the **Player** role:

Session Recording Player									-	×
File Edit View Play Tools Help										
늘 🕨 📋 📮 🏛 💠 🔉 Search:		 Anytime 		- 💢 🎼 🔟 Advance	d Search					
	arch Results									×
		pplication	Status	Start Time	Duration	Delivery Group	VDA Machine	Recording Ser	Size	
Favorites			Complete	8/30/2022 12:01 AM	00:00:35			AUTO_INSTA	775 KB	
_		Play Follow up								
		Place access restriction								
	26	Delete	619							
		Move to Folder								
Now Playing ×		Copy to Folder								
	3	Properties								
Events and Bookmarks ×										
	لحدا لحد بد									
1 file										

6. Click Yes.

Ression Recording Player										
File Edit View Play Tools Help										
늘 🕨 🛅 💐 🎞 💠 ≫ 🛛 Search:		- A	nytime	- 🛗 🕼 🕎 Advanc	ed Search					
Workspace ×	Search Results									
Workspace - administrator	User Name	Application	Status	Start Time	Duration	Delivery Group	VDA Machine	Recording Ser	Size	Access restric
Search Results Favorites	administrator	Desktop	Complete	8/30/2022 12:02 AM	00:00:27			AUTO_INSTA	244 KB	
Restricted	administrator	Desktop	Complete	8/30/2022 12:01 AM	00:00:35			AUTO_INSTA	775 KB	No
Now Playing ×	1		Warning							
now ridying A	<									
				sure you want to restric ngs? Restricted recording						
			privileg	ed players. single recorded session		-				
			recordi	ng. If you select any reco	rding of a set	ssion, the access				
			restrict	ions apply to all other re-	ordings of th	he same session.				
					Yes	No				
Events and Bookmarks ×										

7. Verify that the selected recordings on which you placed access restrictions are moved from the **Search Results** area to the **Restricted** area.

Session Recording Player										-		×
File Edit View Play Tools Help												
늘 🕨 🛅 📮 🎞 💠 ≫ Search:			 Anytime 		- 🛗 📖 🕎 Advance	d Search						
Workspace	×	Restricted										×
Workspace - administrator Workspace - administrator Search Results Forces Feastrated Restricted		User Name administrator	Application Desktop	Status Complete	Start Time 8/30/2022 12:02 AM	Duration 00:00:27	Delivery Group	VDA Machine	Recording Ser AUTO_INSTA	Size 244 KB	Access re Yes	estrict
Now Playing	×	<						_				>
Events and Bookmarks	×											
1 file												

8. In the **Restricted** area, remove access restrictions as needed. With access restrictions removed, recordings are moved back to the **Search Results** area.

Session Recording Player									-		×
File Edit View Play Tools Help											
늘 🕨 📋 📮 🎞 💠 ≫ Search:		 Anytime 		- 📋 📖 🔀 Advanc	ed Search						
	K Restricted										×
Workspace - administrator Search Results	User Name	Application	Status	Start Time	Duration	Delivery Group	VDA Machine	Recording Ser		Access	estrict
Favorites	administrator	Desktop	Complete	8/30/2022 12:02 AM	00:00:27			AUTO_INSTA	244 KB	Yes	
Estricted		Play									
		Follow up Remove access restri	ations								
		Delete	CUUTIS	1							
Now Playing	«	Move to Folder									>
		Copy to Folder									
		Properties									
Events and Bookmarks		*									
1 file			_		_						

Open and play recordings

June 21, 2024

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**.

🔄 Session Recording Server Properties - 🗆 🗙
Storage Signing Rollover Playback Notifications CEIP Logging Rt
Live session playback This option permits the playback of session recordings while recording is still in progress. Allow live <u>s</u> ession playback
Playback protection This option encrypts session recording files before download to the Session Player. This prevents session recordings from being copied and viewed by users other than the user that originally downloaded the file. <u>Encrypt session recording files downloaded for playback</u>
Ctrix Workspace app version check This option allows users to skip the Citrix Workspace app version check before the Session Recording Player plays back a recording. Skip Citrix Workspace app version check before playback
OK Cancel Apply

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 .iclor.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.
- 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.
88	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.

Keyboard Key	Function
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.
- 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**.
- 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

June 21, 2024

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

June 21, 2024

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

June 21, 2024

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 using 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

June 21, 2024

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

June 21, 2024

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

Note:

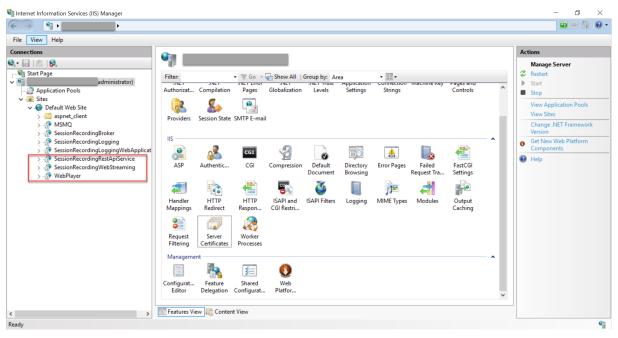
- When logging on to the web player website, domain users do not need to enter credentials while non-domain users must.
- Supported browsers include Google Chrome, Microsoft Edge, and Firefox.
- To have the web player function properly, make sure you enable WebGL in Firefox.

This article guides you through the process of installing and enabling the web player and the process of configuring HTTPS.

Install the web player

Install the web player on the Session Recording server only. Double-click SessionRecordingWeb-Player.msi and follow the instructions to complete your installation. For more information about installing Session Recording, see Install, upgrade, and uninstall.

Starting from Version 2103, Session Recording migrates the WebSocket server to IIS. With the web player installed, the **SessionRecordingRestApiService**, **SessionRecordingWebStreaming**, and **WebPlayer** applications appear in IIS.



A fresh installation of Session Recording 2103 and later connects your web browser to the WebSocket server hosted in IIS when you access the web player website. The WebSocket server hosted in IIS is versioned 2.0, as indicated by the registry value **WebSocketServerVersion** under the registry key at HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.

dit View Favorites Help				
uter\HKEY_LOCAL_MACHINE\SOFTWARE\Citr				
SOFTWARE		Type	Data	
- 📙 7-Zip	atabaseFailoverPartner	REG_SZ		
> Business Objects	ab DatabaseName	REG_SZ	CitrixSessionRecording2	
V Citrix	BeferredHashCalcFileSizeThreshold	REG_DWORD	0x00200000 (2097152)	
- Citrix Desktop Delivery Controller	20 DormantTimeInHours	REG_DWORD	0x00000030 (48)	
> InstallAgent	88 EnableAnalytics	REG_DWORD	0x00000001 (1)	
- MetaInstall	EnableAzureSQLService	REG_DWORD	0x00000000 (0)	
V SmartAuditor	EnableRecordingActionLogging	REG_DWORD	0x00000001 (1)	
Server	EnableSRStorageLogging	REG_DWORD	0x00000001 (1)	
XenDesktop XenTools	EnableWebBasedSrPlayer	REG_DWORD	0x00000001 (1)	
XenTools XenToolsInstaller	4 LinkEmail	REG_SZ		
	and LinkExpire	REG_SZ	172800000000	
XenToolsNetSettings Classes	a) LinkHost	REG_SZ		
Clients	at LinkSalt	REG_SZ	kk2od974	
DefaultUserEnvironment	88 LoggingBlockState	REG_DWORD	0x00000000 (0)	
> dotnet	a Logging Database Failover Partner	REG_SZ		
GitForWindows	a Logging Database Name	REG_SZ	CitrixSessionRecordingLogging	
> Google	88 LoggingLoggingState	REG DWORD	0x00000001 (1)	
> Intel	10 MaxOpenFiles	REG DWORD	0x00002710 (10000)	
> JavaSoft	38 MaxRolloverFileSizeInMB	REG DWORD	0x0000012c (300)	
	100 PlaybackProtection	REG DWORD	0x00000001 (1)	
> Microsoft	700 PlayerUserRBACEnabledKey	REG DWORD	0x00000000 (0)	
MozillaPlugins	ab PolicyFilePath	REG_SZ	C:\Program Files\Citrix\SessionRecording\Server\\A	
> ODBC	B PolicyFileRefreshPeriodInSeconds	REG DWORD	0x0000012c (300)	
> OpenSSH	100 RoleBasedSecurityEnabled	REG DWORD	0x00000001 (1)	
> Partner	BolloverFileSizeInMB	REG DWORD	0x00000032 (50)	
> Policies	BolloverTimeInHours	REG DWORD	0x000000c (12)	
> Python	20 SkipReceiverVersionCheck	REG DWORD	0x00000001 (1)	
> Qualys	ab SmAudDatabaseInstance	REG SZ	10.108.92.40	
RegisteredApplications	WebPlayerDisableAllRecording	REG DWORD	0x00000000 (0)	
> Setup	WebSocketServerVersion	REG SZ	2.0	

An upgrade installation from an earlier version to Session Recording 2103 and later connects your web browser to the Python-based WebSocket server. To connect to the WebSocket server hosted in IIS, run the **<Session Recording server installation path>\Bin\SsRecUtils.exe -enablestreamingservice** command. To connect back to the Python-based WebSocket server, run the **<Session Recording server installation path>\Bin\SsRecUtils.exe - disablestreamingservice** command. The Python-based WebSocket server, run the **Session Recording server installation path>\Bin\SsRecUtils.exe - disablestreamingservice** command. The Python-based WebSocket server is versioned 1.0.

Enable the web player

The web player is enabled by default.

- To disable the web player, start a Windows command prompt and run the <Session Recording Server installation path>\Bin\SsRecUtils.exe –disablewebplayer command.
- To enable the web player, start a Windows command prompt and run the <Session Recording Server installation path>\Bin\SsRecUtils.exe -enablewebplayer command.

Configure HTTPS

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

Note:

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

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

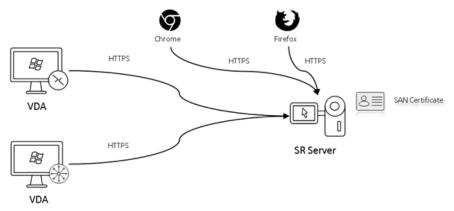
1. Add an SSL binding in IIS.

a) Obtain an SSL certificate in PEM format from a trusted Certificate Authority (CA).

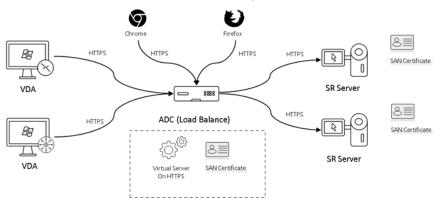
Note:

Most popular browsers such as Google Chrome and Firefox no longer support the common name in a Certificate Signing Request (CSR). They enforce Subject Alternative Name (SAN) in all publicly trusted certificates. To use the web player over HTTPS, take the following actions accordingly:

• When a single Session Recording Server is in use, update the certificate of the Session Recording Server to a SAN certificate.



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



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

pears.

- 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.

Add Site Binding		? ×
Ipe: IP address: http All Unassigned http All Unassigned https Example: www.contoso.com or marketing.contoso.com	P <u>o</u> rt: ~ 80]
Add Site Binding	ОК	Cancel
Add Site Binding		? ×
Ippe: IP address: https V	P <u>o</u> rt: √ 443	1
Host name:		
Require Server <u>N</u> ame Indication		
SSL certi <u>f</u> icate:		
Not selected ~	Se <u>l</u> ect	<u>V</u> iew
Not selected test		
	OK	Cancel

e) Click **OK**.

- 2. Update the SsRecWebSocketServer.config configuration file.
 - a) Locate and open the SsRecWebSocketServer.config configuration file.

The SsRecWebSocketServer.config configuration file is typically located in the <

Session Recording Server installation path>\Bin\folder.

- b) Enable TLS by editing TLSEnable=1 and ignore the **ServerPort**, **SSLCert**, and **SSLKey** fields.
- c) Save your changes.

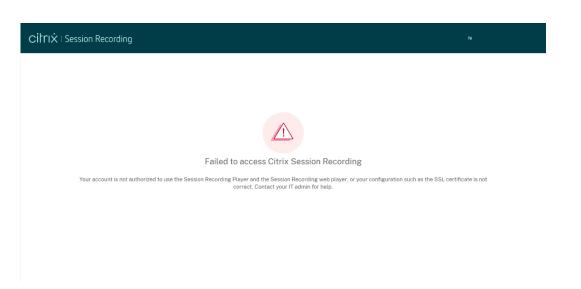
Hide or show content on the web player home page

September 14, 2024

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**.

🔄 Session Recording Server Properties —	×
Notifications CEIP Logging RBAC Email Cloud DB Web Player	• •
Hide content on the web player home page	
☐ This option prevents the web player home page from displaying any content. Recordings can be accessed only by way of their URLs.	
OK Cancel Apply	

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.

Cilrix Session	CITIX Session Recording		Q Search by host name, user, start time, and so on				\sim	~		N CONTRACTOR	
► Recordings	^	🗌 Start Time 👙	User 👙	Host 👙	Client 👙	Events 👙	Events Only 👙	Recording Server 👙	Duration 👙	Action	
All Recordings		May 19, 2021 5:36 PM	Administrator			0	False	SERVER	Live	۲	
Comments	÷	May 19, 2021 5:23 PM				23	True	SERVER	00:01:57	ightarrow	
Administrator Logging	÷	May 19, 2021 5:20 PM				1	True	SERVER	00:02:28	ightarrow	
Configuration	÷	May 14, 2021 6:48 PM	Administrator			0	False	SERVER	00:00:58	ightarrow	
		May 14, 2021 6:46 PM	Administrator			0	False	SERVER	00:00:50	ightarrow	
		May 14, 2021 6:31 PM	Administrator			0	False	SERVER	00:00:35	\mathbf{b}	
		May 14, 2021 6:20 PM	Administrator			0	False	SERVER	00:00:41	ightarrow	
		May 14, 2021 5:58 PM	Administrator			0	False	SERVER	00:02:14	ightarrow	
		May 14, 2021 3:00 PM	Administrator			0	False	SERVER	00:00:37	ightarrow	
		May 14, 2021 2:58 PM	Administrator			0	False	SERVER	00:00:31	ightarrow	
		May 14, 2021 2:56 PM	Administrator			0	False	SERVER	00:00:40	$\mathbf{\bullet}$	

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.

CitriX Session	Recording Show all recordings of this session		t name, user, start time, a	and so on		\sim		hi I	
▶ Recordings	► Folling up								
All Recordings	□ Start Time ≑	User 😄	Host 👙	Client 👙	Events 😄	Events Only 👙	Recording Server 👙	Duration 👙	Action
Comments	May 19, 2021 5:36 PM	Administrator			0	False	SERVER	Live	۲
Administrator Logging	May 19, 2021 5:23 PM				23	True	SERVER	00:01:57	ightarrow
Configuration	May 19, 2021 5:20 PM				1	True	SERVER	00:02:28	ightarrow
	May 14, 2021 6:48 PM	Administrator			0	False	SERVER	00:00:58	ightarrow
	May 14, 2021 6:46 PM	Administrator			0	False	SERVER	00:00:50	ightarrow
	May 14. 2021 6:31 PM	Administrator			0	False	SERVER	00:00:35	ightarrow
	May 14, 2021 6:20 PM	Administrator			0	False	SERVER	00:00:41	\mathbf{b}

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.
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

June 21, 2024

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.

CilriX Session Reco	ording	Q Search by host name, use	r, start <mark>T</mark> me, and so on			\sim		hi P	_
► Recordings	Follow up	🗟 Host name		🛆 User na	me				
All Recordings	□ Start Time 👙	28 Application		🖵 Client n	ame		Recording Server 👙	Duration 👙	Action
Comments V	May 19, 2021 5:20 PM	Client IP address		🗟 Event te	ext		SERVER	00:02:28	ightarrow
Administrator Logging V	May 19, 2021 5:23 PM	🔚 Event type		Time			SERVER	00:01:57	ightarrow
	March 3, 2021 10:43 AM						SERVER	00:08:05	ightarrow
	March 3, 2021 12:39 PM	Administrator			5	False	SERVER	00:01:22	\mathbf{b}
	March 31, 2021 3:35 PM	Administrator			19	False	SERVER	00:04:37	ightarrow
	March 31, 2021 3:47 PM	Administrator			1	False	SERVER	00:01:34	lacksquare

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 record-ings and display only the relevant ones.

FILTER		Search	Clear All
Host name 🗸 🗸	Enter one Host name		$+ \times$

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.

C il†rı ×∣Sessia	on Reco	ording	Q Search by hos	st name, user, start time, i	and so on		`	<u> </u>	hi	
Recordings	^	FILTER							Search	Clear All
All Recordings									Obarter	
Comments	~		ne Host name							$+ \times$
Administrator Logging	¥	F Suser name								
Configuration	~	Client name	User 🌲	Host 👙	Client 🖕	Events 👙	Events Only 👙	Recording Server 👙	Duration 👙	Action
		Client IP address				1	True	SERVER	00:02:28	\mathbf{b}
		□ ¹ Event text Comments				23	True	SERVER	00:01:57	ightarrow
		□ I ≣ Event type M	Administrator			0	False	SERVER	00:08:05	\mathbf{b}
		Time M	Administrator			5	False	SERVER	00:01:22	ightarrow
		March 31, 2021 3:35 PM	Administrator			19	False	SERVER	00:04:37	

You can also click the + symbol to add filters.

FILTER		Search Cle	ear All
Host name 🗸 🗸	Enter one Host name	+	· ×

For example, you can add the **Time** filter as shown in the following screen.

FILTER						Search	Clear All
Host name 🗸 🗸	Enter one Host name]	$+ \times$
Time 🗸	Start date	End d	ate				
	Select date	Sel	ect date				
	Start Time	End t	ime				
	Select time	Sel	ect time				\sim
	Duration						43
	At least 🛛 🤝		Seconds 🗸				
Start Time 🍦		User 🖕	Host 🍦	Client 🖕	Events 🌲	Duration 👙	Action
February 9, 2021 5:	22 PM	qh			5	00:30:07	

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

June 21, 2024

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.

👼 Session Recording Author	orization Console							
<u>File Action View H</u> e	elp							
🗢 🔿 🖄 📰 🗙 🖾								
Carl Role Assignments			Name	Туре	Description			
	🍖 LoggingReader							
Realized Player								
PolicyAdministrator	r							
nivilegedPlayer 😨								
Assi	gn Users and Groups		dows and Active Directory					
View	v	> From Auth	orization Manager					
Dele	te							
Refr	esh							
Expo	ort List							
Prop	perties							
Help	p							

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.

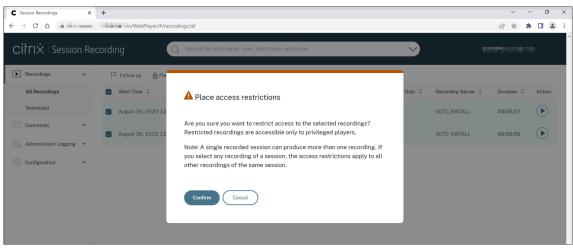
View for the **PrivilegedPlayer** role:

C Session Recordings	×	+							× -	- 0
← → C ☆ ▲		/WebPlayer/#/recordings/a							<i>È</i> ☆ \$	F 🖪 😩
Citri X Sessi	on Red	cording Q Se	arch by host nam	ne, user, start time, a	and so on		\checkmark			
Recordings	^	Follow up 🔒 Place access r	estrictions							
All Recordings		Start Time 🍦	User 🌲	Host ≑	Client 🌲	Events 🚔	Events Only $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	Recording Server $\buildrel {\buildrel {\ulldrel {\ulldrel {\buildrel {\ulldrel \ulll} \ulltrel {\ulldrel {\ulldrel \ulltrel \ulltrel \$	Duration 👙	Action
Restricted		August 30, 2022 12:02 PM	administrator	100000	$(1,1,2,1) \in \mathbb{C}^{n}$	0	False	AUTO_INSTALL	00:00:27	
Comments	v g v	August 30, 2022 12:01 PM	administrator			0	False	AUTO_INSTALL	00:00:35	∢
Ornfiguration	v			Ģ						

View for the **Player** role:

C Session Recordings	×	+								~ -	ø ×
< → C ☆		/WebPlay	yer/#/recordings/a							i ☆ 🛊	1 😩 E
Cilrix Session	n Re	cording	Q Se	arch by host nam	e, user, start time, a	nd so on		\sim	-		-
▶ Recordings	^	Start Time 🍦		User 崇	Host 崇	Client 崇	Events 🚔	Events Only 🍦	Recording Server 🍦	Duration 🌲	Action
All Recordings		August 30, 20)22 12:02 PM	administrator		$(a_1,a_2,\ldots,a_{n-1},a_n) \in \mathbb{R}$	0	False	AUTO_INSTALL	00:00:27	ightarrow
Comments	× ×	August 30, 20	02212:01 PM	administrator	-	11 - Artist 11	0	False	AUTO_INSTALL	00:00:35	∢
Onfiguration	v										
						Ν					

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.

C Session Recordings	×	+								~ -	
÷ → C ☆	-	/WebPlayer/#/recording	s/restricted							ici ☆ 🗰 🕻	1 (1)
CitriX Session	ı Rec	cording Q	Search by hos	t name, user, star	t time, and so on			\checkmark			
► Recordings	^	Start Time 🍦	User 🌲	Host 👙	Client 👙	Events 🚔	Events Only 🍦	Recording Server 👙	Duration $\stackrel{\scriptscriptstyle {\scriptscriptstyle \triangle}}{_{\scriptscriptstyle \nabla}}$	Restricted by 👙	Action
All Recordings		August 30, 2022 12:02 PM	administrator			0	False	AUTO_INSTALL	00:00:27	X8EPW\Administrator	lacksquare
Restricted		August 30, 2022 12:01 PM	administrator	-018-010	,	0	False	AUTO_INSTALL	00:00:35	X8EPW\Administrator	
Comments	ř										0
Administrator Logging	~										
Configuration	~										

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

C Session Recordings ×	+	~ -	o ×
← → ♂ ☆	WebPlayer/#/recordings/restricted	ie 🛧 🕈	🖪 😩 E
CİİTIX Session Re	cording Q Search by host name, user, start time, and so on		
► Recordings	Follow up BRemove access restrictions		
All Recordings	Start Time 🗘 User 🗘 Host 🗘 Client 🗘 Events 🗘 Events Only 🌵 Recording Server 🇘 Duration 🗘	Restricted by $\buildrel {\buildrel {\ulldrel {\ulldrel {\buildrel {\ulldrel \ulll} \ulltr$	Action
Restricted	August 30, 2022 12:02 PM administrator	X8EPW\Administrator	\mathbf{b}
Comments V	August 30, 2022 12:01 PM administrator 0 False AUTO_INSTALL 00:00:35	X8EPW\Administrator	∢
 Configuration 			

Open and play recordings

September 14, 2024

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.

Session Recording 2411

Cilrix Session Reco	ording	u -	aron ay nosi i	neme, user, start time, and	r 90 04			\sim		BAPRONAN	
Recordings At Recordings	StartTime 0	User 0	Het 0	Olent 0	Events 0	Events Only 0	Audio Recording 0	Lossy Screen Recording	Recording Server 0	Duration 0	Actio
Comments v	Nov 14, 2023 3 12:35 PM				28	False	Enabled	False	35854	Live	•
Administrator Legging 🛩	Nov 24, 2023 3:02:49 PM			100	11	False	Enabled	False	35R94	00.05.15	Þ
Configuration ~	Nov 24, 2023 2:44:24 PM					False	Disabled	False	35R54	00.05/24	B
	Nov 14, 2023 2,28.55 PM	100		100	4	False	Disabled	False	35854	00.08.34	Þ
	Nov 14, 2023 2:17:25 PM				2	False	Disabled	False	35854	00.04.02	Þ
	Nov 14, 2023 2:09:10 PM				4	False	Disabled	False	35R54	00.05/23	۲
	Nov 15, 2023 4 42:54 PM				3	False	Disabled	False	35R54	00.06.26	Ð
	 Nov 15, 2023 4:36:53 PM 	100			0	Faire	Disabled	false	35854	00.09.07	E
	Nov 15, 2023 4:20:46 PM					False	Disabled	False	35R54	00:05:29	Þ
	Nov 15, 2023 4:04:27 PM				6	False	Disabled	False	35R54	00.08.23	Ð
	Nov 15, 2023 3,25.51 PM				18	False	Disabled	Estre	35854	00.05.50	Ð
	Nov 15, 2023 3,14,04 PM			100	6	False	Disabled	False	35R54	00.04.29	Þ
	Nov 15, 2023 2:53:08 PM				•	False	Disabled	False	25854	00.08.23	Þ

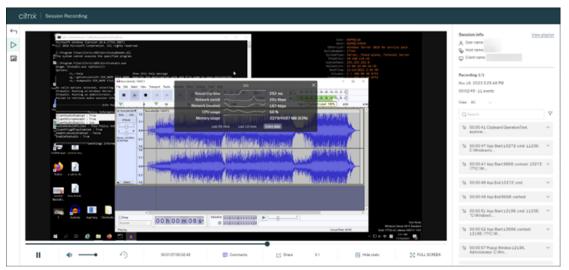
Tip:

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.

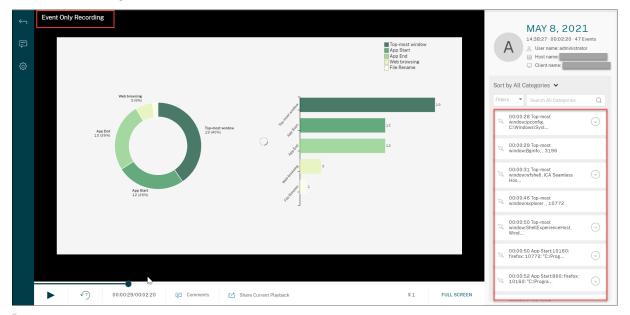


Playback of a screen recording:

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.

Player Control	Description
	Plays the selected recording file.
II	Pauses playback.
57 (1)	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.
√7)	Seeks backward 7 seconds.
00:05:06/00:13:33	Indicates the current position of the recording playback and the total recording duration. The time format is HH:MM:SS.

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

Player Control	Description
戻 Comments	
	Lets you click and leave a comment about the recording being played.
C Share Current Playback	Lets you click and copy the URL of the current recording to the clipboard.
\Lambda Show stats	
—	Shows the overlay that features data points
	related to the recorded session.
\Lambda Hide stats	
	Hides the session data overlay.
X 1	Indicates the current speed of playback. Click
	the icon to switch between options including
	X0.5, X1, X2, and X4.
FULL SCREEN	Displays the playback in full screen.
Exit full screen	Displays the playback within the webpage.

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

AUG 20, 2021 18:50:50 · 01:37:00 · 359 Events User name: d Host name: A Client name: (7
View: All	∇
Events Comments admin: cet	~
⋈ 00:00:40 Top-most window:sessionmsg, , 8412	~
© 00:00:53 Clipboard Operation:Text, sessionmsg, ,	\sim
₱ 00:00:53 ctxadmin:	\sim
© 00:00:54 Top-most window:explorer, , 8944	\sim
● 00:00:54 ctxadmin: dqwdwd	~
© 00:01:13 Top-most window:ipconfig,	~

- 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:

Session Recording 2411

ß	00:18:29 Top-most window:setup_wm, Windows Media P	~
	00:18:41 Top-most window:wmplayer, Windows Media P	~

- 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

June 21, 2024

To configure preferences for your web player, navigate to **Configuration > Preferences** on the web player page.

Citrix Session	Recording	hi wata ma
Recordings Comments Administrator Logging Onfiguration	 Preferences Set your playback preferences. Player cache Set the cache size you want the player to use for playback. 	
Preferences	2MB 20MB 100MB Rendering options Image: Solution of the problem of the prob	4

You can configure the following preferences for your web player:

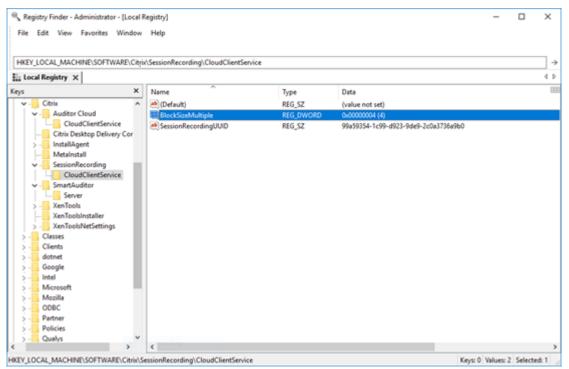
- Player cache. Drag the slider to set the cache size you want the player to use for playback.
- **Optimized graphics engine**. We have optimized the graphics engine to improve the performance of the web player. The optimized engine is enabled by default. If you encounter compatibility or other issues with the optimized engine, you can disable it by clearing the check box.

Increase the transport packet size for the web player

June 21, 2024

- 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

June 21, 2024

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

Tip:

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

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

Registry key	Default value	Description
DisableIdleEvent	0	To disable the idle event
		feature, set the value to 1 . To
		enable the idle event feature,
		set the value to 0 .
dleEventThrottle	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 o
		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 a
		user activities.
dleEventActivePktNumThrottle	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 a
		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

June 21, 2024

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 Q User name: c Lost name: <i>k</i> Client name: (7
View: All
Events Comments admin: cer
⋈ 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, ✓

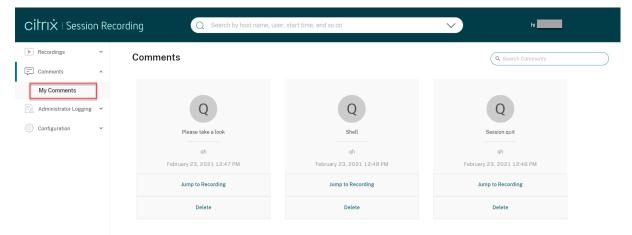
Comment on recordings

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

←	ר Player	
		NOV 17, 2021
		15:43:44 · 00:12:51 · 30 Events
ave.		♀ User name: ♀ Host name: ☐ Client name
		View: Comme V
		Q Search
		D0:00:00 ctxuser1: test
	Session Recording	Delete
	Your activity with the desktop or program(i) you recently started is being recorded. If you object to this condition, close the desktop or program(s).	🗩 • 00:00:00 ctxuser1: test 2 🗸
		• 00:00:00 ctxuser1: test 3
		L
	Jonar Ryent - ANTSYD -	
	1 47 00:00:30/00:12:51 C Comments C Share Current Playback X1 <table-cell> Hide stats 🔀 Exit full screen</table-cell>	
	you object to this condition, close the deductor or program(s). T T Round trip time 0 ms 452 K loss Network (send) 452 K loss CPU unage 2471/4088 MB (60%)	 • 000000 ctuser1 test 2 • 000000 ctuser1 test 3

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.

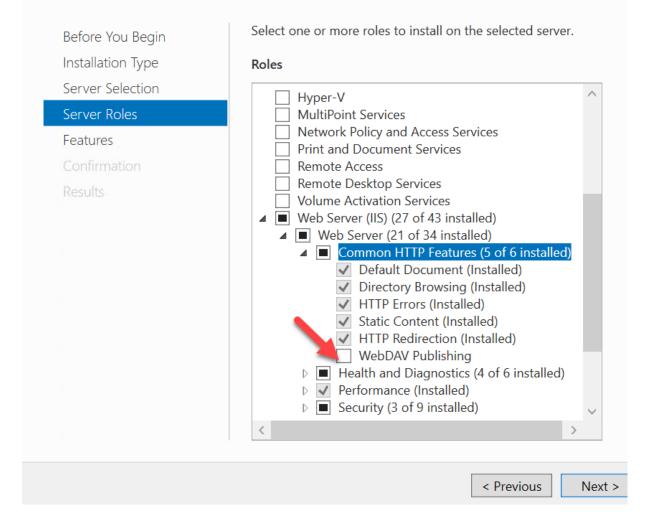


Note:

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.

📥 Add Roles and Features Wizard

Select server roles



Share recordings as links

June 21, 2024

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.

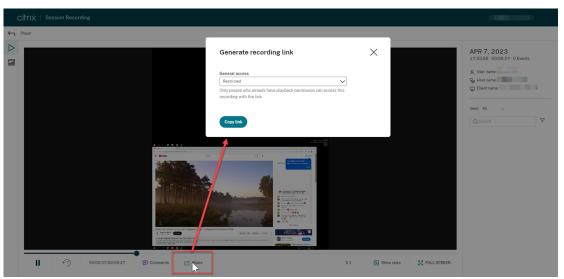
Note:

- 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.

CİİTIX │ Session Recording				- 10 - 10 - 10 - 10 - 10 - 10 - 10 - 10
← Player				
	Generate recording link	×	_	APR 7, 2023 18:09:51 · 00:00:27 · 0 Events
	General access Unrestricted Anyone in thu			 Q. User name: Q. Host name: Client name:
	Justification Enter justification for generating the link			View: All V
	Link valid for (hours)			
	Copy link Manage links			
	1			
► ⑦ 00.00.00.00.27	X1	Show stats	FULL SCREEN	

- 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.

ding	Q	Search by host name	e, user, start time, and so on			\checkmark			
	Start Time 🔶	User 🚔	Host 🚔	Client ≑	Events 🚔	Events Only 🗘	Recording Server 🍦	Duration 🗘	Manage links Action
	April 6, 2023 10:38 AM	1.00	1.000		0	False		00:00:27	►
	April 6, 2023 10:28 AM				0	False		00:09:41	►
	April 6, 2023 10:17 AM			10.00	0	False		00:11:45	►
	March 15, 2023 4:31PM				0	False		00:02:13	►
	March 15, 2023 4:07 PM		1.0		0	False		00:03:28	►
	February 28, 2023 4:47 PM			10 C	8	False		00:02:01	►
	February 28, 2023 9:59 AM				0	False		00:04:50	►
	February 28, 2023 9:32 AM				0	False		00:02:33	►
	February 28, 2023 9:31 AM				0	False		00:00:53	►
	February 28, 2023 9:19 AM				0	False		00:40:20	►
	February 28, 2023 6:33 AM			10 C	0	False	100.00	02:46:00	►
	February 13, 2023 2:22 PM				0	False		00:04:26	►
	February 13, 2023 2:11 PM			and the second se	0	True		00:10:52	►

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

								Manage links 🗲
Start Time 🗘	User 崇	Host 🚔	Client 🌻	Events 🌻	Events Only 🍦	Recording Server $\ \ \diamondsuit$	Duration \Rightarrow	Action
April 6, 2023 10:38 AM			linlin_s_MacBook_Pro	0	False		00:00:27	6 ⁹ 6
April 6, 2023 10:17 AM		1.00	linlin_s_MacBook_Pro	0	False		00:11:45	a ^p 2
February 28, 2023 9:32 AM			QHPLAY	0	False		00:02:33	° 1
November 30, 2022 3:01 PM			APACPMD2221	1	False		00:32:15	o ^p 5
September 21, 2022 11:37 AM			NKGWYUCHUNJ01	0	False		00:14:59	c [©] 1
							- 1	

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

ding	0	Search by host na	me, user, start time, and so c	n		\sim		WA9KL\Ad	dministrator
									Manage links $ imes$
Start Time ≑		User ≑	Host 🕆	Client 🗘	Events ≑	Events Only 👙	Recording Server 🍦	Duration \Rightarrow	Action
April 6, 2023 10:3	8 AM			linlin_s_MacBook_Pro	0	False		00:00:27	6 ¹⁰ 6
April 6, 2023 10:1	.7 AM		- 10 C	linlin_s_MacBook_Pro	0	False	1000	00:11:45	6 ⁰ 2
February 28, 2023	9:32 AM			QHPLAY	0	False		00:02:33	6 ⁰ 1
November 30, 202	2 3:01 PM			APACPMD2221	1	False		00:32:15	o ^p 5
September 21, 20	22 11:37 AM			NKGWYUCHUNJ01	0	False		00:14:59	8 ⁹ 1

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

CİİTIX │ Session Recording			
← Player			
	Generate recording link	×	APR 7, 2023 16:34:09:00:00:27:0 Events & User name.
	Unrestricted V Anyone in the AD domain can access this recording with the link.		😌 Host name:
	Justification test2		View: All View:
	Link valid for (hours)		
	Copy link Manage links		
► <7 00:00:00/00:00:27	x	1 🔥 Show stats	5 FULL SCREEN

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

Iew and manage unrestricted links generated at (UTC+08:00) ‡ Apr 10. 2023 4:18:42 PM Apr 10. 2023 4:10:22 PM URL http://10.108.4.136/WebPlayer/#/pl Viewed by	Generated by WA9KL\Administrator WA9KL\Administrator	Justification	Status Expired Expired					
Apr 10, 2023 4:18:42 PM Apr 10, 2023 4:10:22 PM URL http://10.108.4.136/WebPlayer/#/pl	WA9KL\Administrator WA9KL\Administrator		Expired					
Apr 10, 2023 4:10:22 PM URL http://10.108.4.136/WebPlayer/#/pl	WA9KL\Administrator	559e2bd884ee7						
URL http://10.108.4.136/WebPlayer/#/pl		559e2bd884ee7	Expired					
http://10.108.4.136/WebPlayer/#/pl	layer?key=a17c89a63c3f4976b12!	559e2bd884ee7						
Viewed by		URL http://10.108.4.136/WebPlayer/#/player?key=a17c89a63c3f4976b12559e2bd884ee7						
	Time 🗘	Playbac	k justification					
WA9KL\user0	Apr 10, 2023 5:45:37 PM	user0's	view					
WA9KL\Administrator	Apr 10, 2023 5:45:18 PM	adminis	trator view					
WA9KL\Administrator0	Apr 10, 2023 4:53:13 PM	adminis	trator0's view					
Apr 11, 2023 3:30:45 PM	WA9KL\Administrator		Expires in 3h37m					
Apr 10, 2023 5:46:11 PM	WA9KL\Administrator	Test	Revoked					

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

Manage unrestricted links X							
View and manage unrestricted links generated for this recording. Expand each row to view details.							
Generated at (UTC+08:00) 🍦	Generated by	Justification	Status				
Apr 10, 2023 4:18:42 PM	WA9KL\Administrator		Expired				
Apr 10, 2023 4:10:22 PM	WA9KL\Administrator		Expired				
Apr 11, 2023 3:30:45 PM	WA9KL\Administrator		Expires in 3h37m				
URL http://10.108.4.136/WebPlayer/#/player?key=438a6a5b428748b590cbcc0ff8d8f2dc							
Apr 10, 2023 5:46:11 PM	WA9KL\Administrator	Test	Revoked				
Done							

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

A Revoke link	
If you revoke this link, people can n This will not affect anyone who alre Are you sure you want to continue?	o longer access the recording with it. ady had the page open.
Continue	

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

View graphical event statistics for each recording

June 21, 2024

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.

÷	Player				
\triangleright					
_		🔹 New Tab 🛛 🗙	+	м – а ×	NOV 18, 2021 11:41:52 · 00:13:33 · 32 Events
		$\leftarrow \ \rightarrow \ \mathbf{C}$	Q. Search with Google or enter address		
		-1 Import bookmarks 👈 Getting Sta	ed	0	🖉 User name:
				*	G Client name:
			🝅 Firefox		View: All
					Q Search 🗸
			G Search with Google or enter address		∞ 00:00:26 Top-most window:sessionmsg9072 ~
			a. example a second trip time 303 ms Network (sand)		№ 00:00:28 Top-most window:explorer., 7508
			Amazon Sponsored Spon CPU usage32 % Memory usage32 %	³ Taulos Tailter 088 MB (73%)	© 00:00:48 App Start:9632: conhost: 2748: \??\C\Win ∨
			Recommended by Pocket Learn more	9	© 00:00:48 App Start:2748: cmd: 7508: C:\Windows\sys
			Gilittan		© 00.00:48 App Start11232: ∨ powershell: 2748: powers
			theguardian.com What lies beneath: the secrets of The Good Guy/Bad Guy Myth	smartasset.com Learn the Cost of a Financial	№ 00.00:55 App End:9632: conhost
		щ Р 🗆 🤗 🗖	France's top serial killer expert An intrepid expert with dozens of books to the battle between good and evil. Traditional	Advisor Find information to help you choose the 스 페 에 및 107,2021 평	№ 00:00:55 App End:11232: powershell
	•	√7) 00:05:00	00:13:33 Comments Share Current Playback	X1 Nide stats	EN 00:00:55 App End:2748: V

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).

0			
XenDesktopVdaSetup			00:20:52
explorer			00:19:14
chrome			00:16:52
firefox		00:11:55	
csrss		00:10:30	
ConfigurationWizard		00:07:46	
powershell	00:03:00		
cmd	00:02:58		
mmc	00:00:35		
iexplore	00:00:35		
Taskmgr	00:00:16		
JonasAgentSystray	00:00:15		
sessionmsg	00:00:14		
setup_wm	00:00:12		
WfShell	00:00:11		
wmplayer	00:00:10		
CitrixFiles	00:00:07		

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:

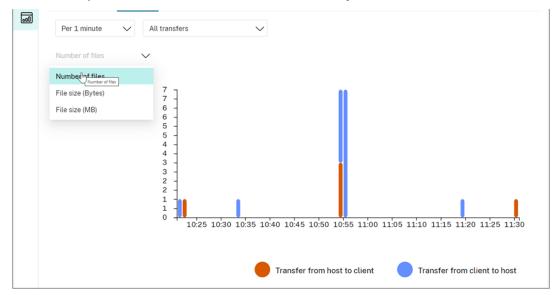
Screen time File tra	notoro	Commands	Events		powers	hell
Screen time File tra	Insters	Commands	Events		as the to	p-most window
					^ All	> 20 minutes) (5-20 minutes) (< 5 m
					Start ti	ne Duration
XenDesktopVdaSetup				00:20:52		
explorer				00:19:14	00:10:50 00:28:25	00:00:04
chrome				00:16:52	00:29:02	00:00:15
firefox			00:11:55		00:30:04	00:00:03
csrss			00:10:30		00:30:20	00:00:02
ConfigurationWizard	_		00:07:46		00:30:38	00:00:01 0
-	_				00:30:41	00:00:02
powershell		00:03:00			00:30:43	00:00:07
cmd		00:02:58			00:31:05 00:31:49	00:00:04
mmc		00:00:35			00:33:36	00:00:08
iexplore		00:00:35			00:33:53	00:00:09
Taskmgr		00:00:16			00:36:38	00:00:06
JonasAgentSystray		00:00:15	3		00:37:07	00:00:03
sessionmsg		00:00:14			00:37:20	00:00:11
					00:37:42 00:42:38	00:00:02
setup_wm		00:00:12			01:13:31	00:01:17
WfShell		00:00:11			0110.01	00.01.17
wmplayer		00:00:10				
CitrixFiles		00:00:07				
OpenWith		00:00:06				
mspaint		00:00:05				

• 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.

•0Ū				
		Custom search	ı	Type a search string or use a regular expression
		Saved search		Select a saved search
	15 / 15 Com	mands		IPv4 Address
	00:01:14	powers		
	00:01:14	cmd	CDFTraceTask.ps1	compmgmt
	00:01:23	00:01:23 powershell logman: "C:\Windo		taskmgr
	00:28:16	cmd	mspaint: mspaint	mmc
	00:28:10	ста	mspaint: mspaint	winver
	00:28:38	cmd	control: "C:\Windo	control
	00:28:49	cmd	netsh: netsh	
	00:29:39	cmd	control: "C:\Windo	ws\System32\control.exe""C:\Windows\system32\sysdm.cpl",
	00:30:37	cmd	mmc: "C:\Windows	s/system32/mmc.exe" "C:\Windows/system32/lusrmgr.msc"

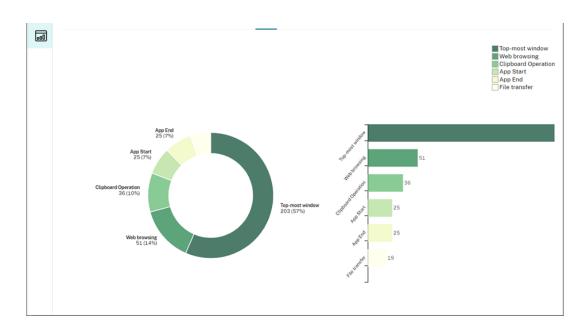
• Printing

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

Screen time File transfers	Commands	Printing Events			Session info View	play
All Printers 7 print jobs, 26 pages	Job count	~	Per 30 minu V		G Host name: LINLINKUANG002	
Microsoft XPS Document Writer 4 print jobs, 10 pages			Per nour Per 30 minutes		Recording 1/1	
Microsoft Print to PDF 2 print jobs, 8 pages	2 -		Per 10 minutes		Jul 9, 2024 1:57:49 PM (UTC+08:00)	
10.118.132.4 [UPD:PDF] (from linlin_s_MacBook_Pro) in session 2 1 print jobs, 8 pages	1 -				03:55:20 · 7 events View: All V	
					Q Search]
	0 13:30 PM	14:00 PM 14:30 PM 15:00 PM 15:30	PM 16:00 PM 16:30 PM 17:00 PM 17:30 PM	18:00 PM	 00:00:00 linlin.kuang@citrix.com: Leave a comment 	
Time (UTC+08:00)		* Printer	Document	Page count	© 00:14:24 Printing activity:C:\Users\administrator\	
Jul 9, 2024 2:12:13 PM		Microsoft XPS Document Writer	C:\Users\administrator\Desktop\test.log	2	01:28:00 Printing activity:C:\Users\administrator\	
Jul 9, 2024 3:25:50 PM		Microsoft XPS Document Writer	C:\Users\administrator\Desktop\New Text Document.txt	1	Q 02:39:58 Printing activity:C:\Test.txt was	
Jul 9, 2024 4:37:48 PM		Microsoft Print to PDF	C:\Test.txt	7	printe	
Jul 9, 2024 4:39:54 PM		10.118.132.4 [UPD:PDF] (from linlin_s_MacBook_Pro) in ses	ion 2 LinkedIn_Log In or Sign Up	8	Q 02:42:04 Printing activity:LinkedIn_ Log In or Sig	
Jul 9, 2024 5:21:18 PM		Microsoft XPS Document Writer	Explore the Enhanced Citrix Platform_ S High-Performing IT Solutions - Citrix	6	Q 03:23:29 Printing activity:Explore the Explored Printing activity:Explore the	
Jul 9, 2024 5:22:06 PM		Microsoft Print to PDF	\\awdc-1n8zw\test\sds.txt	1	Enhanced Ci	
			\\awdc-1n8zw\test\sds.txt	1	03:24:16 Printing activity:\\awdc- 1n8zw\test\sds.t	
Jul 9, 2024 5:23:53 PM		Microsoft XPS Document Writer	////www.thotw/rescisus.txt			

• Events

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



View data points related to each recorded session

June 21, 2024

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

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

_					
÷	Player				
\triangleright			Ν		
		单 New Tab 🛛 🗙	+ b	- a ×	NOV 18, 2021 11:41:52 · 00:13:33 · 32 Events
030		$\leftarrow \ \rightarrow \ \mathbf{G}$	Q. Bearch with Google or enter address		
		-🕣 Import bookmarks 👋 Getting Sta	ted		
				8	Client name:
			iirefox		View: All View: All View: All View: All View: All View: All View: All View: All View: View: All View:
			G Search with Google or enter address		№ 00:00:26 Top-most window:sessionmsg, , 9072
			a. Reading time and the first		∞ 00:00:28 Top-most window:explorer., 7508
			Amazon Spreamert Spreamert Metwork (Incerive) CPU using CPU	© 00:00:48 App Start:9632: conhost: 2748: \??\C:\Win	
			Recommended by Pocket Learn more		№ 00:00:48 App Start:2748: cmd: 7508: C:Windows\sys
					© 00:00:48 App Start:11232: v powershell: 2748: powers
			theguardian.com aeon.co smartasset.com What lies beneath: the secrets of The Good Guy/Bad Guy Myth Learn the Cost of a Financial		[∞] 00:00:55 App End:9632: [∞] [∞] [∞]
		# 2 @ @ #	France's top serial killer expert An intergial expert with dcars of books to battle between good and evit. Traditional Find information to help you choose the	== 40) 12 505 AM	∞ 00:00:55 App End:11232: powershell
	►	√7) 00:05:0	3001333 🕞 Comments 🗹 Share Current Playback X1 🛃 Hit	de stats	© 00:00:55 App End:2748: cmd ∨

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

October 23, 2024

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:

CİTIX Session Recording									
Image: Second lings ✓ Image: Second lings ✓ Image: Second lings ✓ Image: Second lings ✓	Diagnostic Logging View diagnostic logs from VDAs. Q Sarch for VDA machine	C• Refresh							
Diagnostic Logging	2411VDA1 ② 2411VDA5 ③ Latest: Sep 12, 2024, 519:54 PM DolL_BROKER_ERROR Latest: Sep 11, 2024, 11:42:44 AM DolL_BROKER_ERROR								
	2411VDA3 2 Latest: Sep 11.2024, 11:41:51 AM Latest: Sep 10.2024, 2:07:54 PM POLL_BROKER_ERROR POLL_BROKER_ERROR								
	٦	1 > 10/page v							

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:

CİTIX Session Recording									
🕑 Recordings 🗸 🗸	Diagnostic Logging > 2411VDA1								
Comments	Diagnostic logs for 2411VDA1								
P Administrator Logging ✓	All time 🗸 C ^e Refresh 🕲 Clear all logs		Group by log type						
Diagnostic Logging	Log type	Time							
ố옷 Configuration ~	+ POLL_BROKER_ERROR 7								

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

For example:

c	CİTTIX Session R	lecording		
Ø	Recordings ~	Diagnostic Logging > 2411VDA1 Diagnostic logs for 2411VDA1		
۶	Administrator Logging 🗸	All time 🗸 C Refresh 🛞 Clear all logs		Group by log type
	Diagnostic Logging	Time	Log type	Count
ផ្ល័រ	Configuration 🗸	Sep 12, 2024, 5:19:54 PM	POLL_BROKER_ERROR	1
-		Sep 11, 2024, 11:42:09 AM	POLL_BROKER_ERROR	1
		Sep 10, 2024, 3:40:01 PM	POLL_BROKER_ERROR	1
		Sep 10, 2024, 3:10:01 PM	POLL_BROKER_ERROR	1
		Sep 10, 2024, 2:08:27 PM	POLL_BROKER_ERROR	1
		Sep 10, 2024, 11:30:26 AM	POLL_BROKER_ERROR	1
		Sep 9, 2024, 6:06:19 PM	POLL_BROKER_ERROR	1
				< 1 > 10/page ∨

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

C	CİTIX Session Recording										
Ø	Recordings	×	Diagnostic Logging > 2411VDA1								
Ę	Comments		Diagnostic logs for	Diagnostic logs for 2411VDA1							
8₽	Administrator Logging	~	All time 🗸	All time V C Refresh S Clear all logs							
	Diagnostic Logging		Last 24 hours		Log type		Count				
ល្វ៊ែ	Configuration	~	Last 48 hours	:19:54 PM	POLL_BROKER_ERROR		1				
			Last 7 days	1:42:09 AM	POLL_BROKER_ERROR		1				
			All time	:40:01 PM	POLL_BROKER_ERROR		1				
			Custom range	:10:01 PM	POLL_BROKER_ERROR		1				
			Sep 10, 2024, 3	2:08:27 PM	POLL_BROKER_ERROR		1				
			Sep 10, 2024, 3	11:30:26 AM	POLL_BROKER_ERROR		1				
			Sep 9, 2024, 6:	06:19 PM	POLL_BROKER_ERROR		1				
							< 1 > 10/page ∨				

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.

📴 Sessio	n Record	ing Server	Properties	;	_		×			
Storage	Signing	Rollover	Playback	Notifications	CEIP	Logging	RE • •			
En:		ing Service		ecordina Admi	inistrator	Logging S	ervice.			
🗌 Ena	This option enables the Session Recording Administrator Logging Service. Enable Mandatory Blocking This option blocks policy and server properties changes if logging fails.									
	-		fication Log	ging r the reason wi	hen playi	ng a recor	ding.			
	ostic loggir		antia lana:	-	—					
Reten	tion period	d for diagn	ostic logs:	<i>50</i>	day(Apply			

Manage recordings

December 4, 2024

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
	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 grea
	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. Fo
	more information, see The RULES parameter f
	ICLDB ARCHIVE and ICLDB REMOVE command
	following this table. The RULES parameter and
	the FILTER parameter cannot be used togethe
	you add the FILTER or RULES parameter, only
	session recording files meeting both RETENTIC
	and FILTER or RULES are manipulated. You ca
	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></days>
	[/LISTFILES] [/MOVETO: <dir>] [/</dir>
	NOTE: <note>] [/FILTER:<file path<="" td=""></file></note>
	filter>] [/RULES: <advanced< td=""></advanced<>
	filters>] [/L] [/F] [/S] [/?]

Command	Description
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 ha
	elapsed. You can specify a target session
	recording file by using the FILEID parameter. Yo
	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.

Command	Description
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). Th
	2303 release introduces the RELOCATE
	parameter to the IMPORT command. Without
	the RELOCATE parameter, the IMPORT
	command parses session recording files in the
	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]
	<pre>[/S] [/?] [<file>] [<directory>]</directory></file></pre>
LOCATE	Locates and displays the full path to a session
	recording file using the file ID as the criteria. U
	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 /FILE
	: <id> [/L] [/F] [/S] [/?]</id>

Command	Description
Command REMOVE	Description Removes the references to session recording files from the database. Use this command (wit caution) to clean up the database. You can also remove the associated physical files. When usin 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, se RETENTION to 2 or a greater value that suits you needs. The FILTER and RULES parameters are optional. The FILTER parameter lets you filter fil paths by using the * and ? wildcards. The RULE parameter sets advanced filters by combining multiple filters strictly in accordance with the /RULES:FIELD-In-["CONDITION"," CONDITION"];FIELD-NotIn-[" CONDITION"]; FIELD-NotIn-[" CONDITION", "CONDITION"]; format. For more information, see The RULES parameter and the FILTER parameter cannot be used together. 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<="" td=""></file></days>

Command	Description
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 %App-
	Data%\Citrix\SessionRecording\Restore.
/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"]; 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 "**CONDI**-**TION**"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).

torage	Signing	Rollover	Playback	Notifications	CEIP	Logging	RE
Recor in a lo volum	ad-balanc	on files are ed manner	stored in t specify m	he directories ultiple director	specifie ries acro	d. To store ss differen	files t
File st	orage dire	ctories:					
		List of fo	lders is en	ntv		Add.	
	The defau	It folder C:	SessionRe	cordings will	be	Modify	y
			useu.			Remo	ve
Specif them a	iy a folder available fi	to tempora or playbac	rilystore a k.	rchived session	on record	dings and n	nake
them a Resto	ivailable fi re director	or playbac y for archi	k. [°] ved files:	rchived session	on record		
them a Resto	ivailable fi re director	or playbac	k. [°] ved files:	rchived session	on record	dings and n Brows	
Resto C:\Se	ivailable fi re director ssion Reco ording file i	or playbac y for archi indingsRest	k. [°] ored red dorman	rchived session		Brows	e
Resto C:\Se A reco	ivailable fi re director ssion Reco roding file i of time ha	or playbac y for archi indingsRest s consider	k. ' ored red dorman			Brows	e

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

```
1 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.

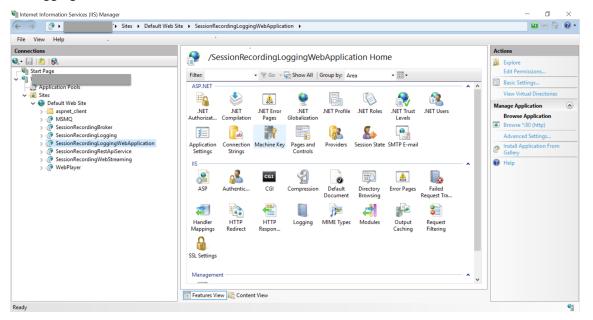
Manage and query administrator logging

June 21, 2024

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.

CilriX Session Re	cording		Search by host name, user, start time	e, and so on		\checkmark	hi XF4B5\Administrat	tor
▶ Recordings ✓	ID \$	Logging Time	Task Category	Component Affected	Ŧ	Action Details	Action Excuted By	?
Comments V	257	11/9/2022 6:31 PM	Server configuration change	Session Recording Server	+	Report setting change	XF4B5/Administrator	True
Eg Administrator Logging A	204	11/4/2022 9:54 AM	Server configuration change	Session Recording Server	+	Report setting change	XF4B5/Administrator	True
Configuration Logging	202	11/3/2022 5:15 PM	Server configuration change	Session Recording Server	+	Report setting change	XF4B5/Administrator	True
Record Reason Logging	174	11/3/2022 2:46 PM	Server configuration change	Session Recording Server	+ Noti	yMessageDefaultYour activity with the desktop or p	XF4B5/Administrator	True
Playback Logging	165	11/2/2022 5:46 PM	Policy change	Session Recording Policy Console	+	Action = SetActivePolicyDocument	XF4B5/Administrator	True
() company .	160	10/31/2022 3:22 PM	Policy change	Session Recording Policy Console	+	Action = SetActivePolicyDocument	XF4B5/Administrator	True
	148	10/24/2022 8:52 AM	Server configuration change	Session Recording Server	+ Noti	yMessageDefaultYour activity with the desktop or p	XF4B5/Administrator	True
	146	10/24/2022 8:42 AM	Log reading	Session Recording Server	+	UserName = XF4B5/Administrator	XF4B5/Administrator	False
	145	10/24/2022 8:41 AM	Log reading	Session Recording Server	+	UserName = XF4B5/Administrator	XF4B5/Administrator	False
	144	10/24/2022 8:41 AM	Log reading	Session Recording Server	+	UserName = XF4B5/Administrator	XF4B5/Administrator	False
						1-10 of 74 < 1	2 3 4 5 6 7	7 8

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.

C itrı × ∣Session I	Recording	ı (C Search by host name, user, start time,	and so on		\checkmark	hi XF4B5\Administr
▶ Recordings ✓	ID ‡	Logging Time	Task Category 👻	Component Affected	Ψ	Action Details	Action Excuted By
Comments •	257	11/9/2022 6:31 PM	Server configuration change	Session Recording Server	+	Report setting change	XF4B5/Administrator
Administrator Logging 🔺	204	11/4/2022 9:54 AM	Server configuration change	Session Recording Server	+	Report setting change	XF4B5/Administrator
Configuration Logging	202	11/3/2022 5:15 PM	Server configuration change	Session Recording Server	+	Report setting change	XF4B5/Administrator
Record Reason Logging	174	11/3/2022 2:46 PM	Server configuration change	Session Recording Server	+ Noti	fyMessageDefault.Your activity with the desktop or p	XF4B5/Administrator
Playback Logging	165	11/2/2022 5:46 PM	Policy change	Session Recording Policy Console	+	Action = SetActivePolicyDocument	XF4B5/Administrator
Configuration V	160	10/31/2022 3:22 PM	Policy change	Session Recording Policy Console	+	Action = SetActivePolicyDocument	XF4B5/Administrator
	148	10/24/2022 8:52 AM	Server configuration change	Session Recording Server	+ Noti	fyMessageDefault.Your activity with the desktop or p	XF4B5/Administrator
	146	10/24/2022 8:42 AM	Log reading	Session Recording Server	+	UserName = XF4B5/Administrator	XF4B5/Administrator
	145	10/24/2022 8:41 AM	Log reading	Session Recording Server	+	UserName = XF4B5/Administrator	XF4B5/Administrator
	144	10/24/2022 8:41 AM	Log reading	Session Recording Server	+	UserName = XF4B5/Administrator	XF4B5/Administrator
						1-10 of 74 < 1	2 3 4 5 6

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.

 Recordings 	ID \$	Logging Time	Task Category 🐨	Component Affected	Ŧ	Action Details	Action Excuted By
Comments 🗸	84	11/8/2022 5:00 PM	Recording reason	Session Recording Agent	+	Applications = BVT_DB/Desktop/###Desktop	XF4B5/Administrator
Administrator Logging 🖍	83	11/8/2022 3:55 PM	Recording reason	Session Recording Agent	+	Applications = BVT_DB/Desktop/###Desktop	XF4B5/Administrator
Configuration Logging	82	11/8/2022 2:50 PM	Recording reason	Session Recording Agent	+	Applications = BVT_DB/Desktop/###Desktop	XF4B5/Administrator
Record Reason Logging	81	11/8/2022 1:45 PM	Recording reason	Session Recording Agent	+	Applications = BVT_DB/Desktop/###Desktop	XF4B5/Administrator
Playback Logging	80	11/8/2022 12:40 PM	Recording reason	Session Recording Agent	+	Applications = BVT_DB/Desktop/###Desktop	XF4B5/Administrator
Configuration	79	11/8/2022 11:35 AM	Recording reason	Session Recording Agent	+	Applications = BVT_DB/Desktop/###Desktop	XF4B5/Administrator
	78	11/8/2022 10:30 AM	Recording reason	Session Recording Agent	+	Applications = BVT_DB/Desktop/###Desktop	XF4B5/Administrator
	77	11/8/2022 9:26 AM	Recording reason	Session Recording Agent	+	Applications = BVT_DB/Desktop/###Desktop	XF4B5/Administrator
	76	11/4/2022 2:13 PM	Recording reason	Session Recording Agent	+	Applications = BVT_DB/Desktop/###Desktop	XF4B5/Administrator
	75	11/4/2022 2:12 PM	Recording reason	Session Recording Agent	+	Applications = BVT_DB/Desktop/###Desktop	XF4B5/Administrator
						1-10 of 84	1 2 3 4 5

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

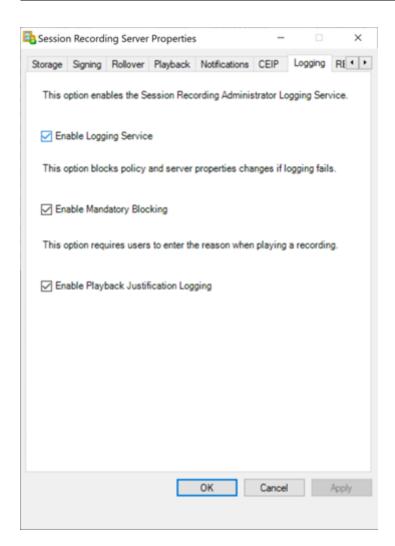
logging does not take effect. For information about enabling recording reason logging, see Disable or enable the recording reason logging.

ilri×∣Session Re	y					
Recordings 🗸	ID 🌩	Logging Time	File ID	Action	Action Excuted By	Aut
Comments 🗸	256	11/4/2022 2:42 PM	7ec9705b-2202-47e4-b8dc-ed43823506b0	Enter playback justification	XF4B5/Administrator	
Administrator Logging	255	11/4/2022 2:26 PM	4502244b-ba4c-417e-9a73-c92055f621bb	Enter playback justification	XF4B5/Administrator	
Configuration Logging	254	11/4/2022 2:24 PM	8715bd68-1e78-4fed-89e6-1c50b7d535c9	Enter playback justification	XF4B5/Administrator	
Playback Logging	253	11/4/2022 2:23 PM	4502244b-ba4c-417e-9a73-c92055f621bb	Enter playback justification	XF4B5/Administrator	
Configuration	252	11/4/2022 2:23 PM	4502244b-ba4c-417e-9a73-c92055f621bb		XF4B5/Administrator	
	251	11/4/2022 2:23 PM	4502244b-ba4c-417e-9a73-c92055f621bb	Session file download	XF4B5/Administrator	
	250	11/4/2022 2:22 PM	8715bd68-1e78-4fed-89e6-1c50b7d535c9	Enter playback justification	XF4B5/Administrator	
	249	11/4/2022 2:13 PM	8715bd68-1e78-4fed-89e6-1c50b7d535c9	Enter playback justification	XF4B5/Administrator	
	248	11/4/2022 2:13 PM	8715bd68-1e78-4fed-89e6-1c50b7d535c9		XF4B5/Administrator	
	247	11/4/2022 2:13 PM	8715bd68-1e78-4fed-89e6-1c50b7d535c9	Session file download	XF4B5/Administrator	
					1-10 of 183 < 1 2	3 4

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:

Session Recording 2411

C il⊓i X Session Re		Q Search by host name	e, user, start time, an	d so on		~	2		
Recordings	🗌 Start Time 🍦					Events Only 👙	Recording Server 🌲	Duration 🗘	Action
All Recordings	November 8, 2022 5:00	PM Play	recording			False	Server22-SIN	00:07:53	►
Restricted	November 8, 2022 3:55					False	Server 22-SIN	01:05:00	∢
Administrator Logging 🗸	November 8, 2022 2:50	record		ed to enter the justification	for playing this	False	Server22-SIN	01:05:00	►
Configuration 🗸	November 8, 2022 1/4	Enter :			A	False	Server 22-SIN	01:04:59	►
	November 8, 2022 12:4					False	Server 22-SIN	01:05:00	
	November 8, 2022 11:3	5 AM	Cancel			False	Server 22-SIN	01:04:59	►
	November 8, 2022 10:) AM administrator	VDA22-SIN	NKGWYUCHUNJ01	0	False	Server22-SIN	01:04:59	►
	November 8, 2022 9:20	AM administrator	VDA22-SIN	NKGWYUCHUNJ01	0	False	Server22-SIN	01:03:52	►
	November 4, 2022 2:13	PM administrator	VDA22-SIN	NKGWYUCHUNJ01	0	False	Server 22-SIN	00:08:55	►
	November 4, 2022 2:12	PM administrator	VDA22-SIN	NKGWYUCHUNJ01	0	False	Server22-SIN	00:00:48	
	November 4, 2022 1:55	PM administrator	VDA22-SIN	NKGWYUCHUNJO1	0	False	Server22-SIN	00:13:11	►
	November 3, 2022 5:08	PM administrator	VDA22-SIN	NKGWYUCHUNJ01	0	False	Server 22-SIN	00:00:25	
	November 3, 2022 5:06	PM administrator	VDA22-SIN	NKGWYUCHUNJ01	0	False	Server22-SIN	00:01:52	►

Justification required for playback in the Session Recording player:

Image: Image:	Session Recording Player											
Search Results Search Results Search Results Duration Delvey Grup VDA Machine Recording Ser. Size Fiel ID Search Results Log Status Search Results	File Edit View Play Too	ols Hel	p									
Uder Name Application Statu Start Time Duration Delivery Group VDA Machine Recording Ser Size Fie ID Beach Result Administrator Delivery Group VDA Machine Recording Ser Size Fie ID Administrator Delivery Group VDA22.SIN VDA22.SIN Server22SIN 1.067 KB 4502244-ba-6-417e-5a73-52039f22/bb/Sh253.358 Administrator Delivery Group VDA22.SIN VDA22.SIN VDA22.SIN Server22SIN 1.067 KB 4502244-ba-6-417e-5a73-52039f22/bb/Sh253.358 Administrator Delivery Group VDA22.SIN VVA22.SIN VVA22.SIN Server22SIN 1.017 KB 4502244-ba-6-417e-5a73-52039f27b-bb/Sh253.358 Administrator Delivery Group VDA22.SIN VVA22.SIN VVA22	👝 🕨 🛄 📮 🛄 🔛	Search	h:		 Anytime 	- 🛍 🛍 🔟	Advanced Sea	arch				
Operation Operation <t< th=""><th>Workspace</th><th>×</th><th>Search Results</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></t<>	Workspace	×	Search Results									
Parontes Parontes	Workspace - administrator		User Name	Application	Status	Start Time	Duration	Delivery Group	VDA Machine	Recording S	er Size	File ID
mexticad existicad existicad existicad existicad Server2251N 77381K F43ab02A1527-#339405-8bc-1537 Server2251N			administrator	Desktop	Complete	11/4/2022 2:13 PM	00:08:55	VDA22-SIN	VDA22-SIN	Server22-SI	1.067 KB	4502244b-ba4c-417e-9a73-c92055f621bb
ow Playing X Dexistop Complete 11/4/2022 159 PM 001311 VDA22-SIN Server22SIN 10121 KB c545db-530a-4577967554b-35a38 558cb-530a-4577967554b-35a38 558cb-530a-4577967554b-35a38 558cb-530a-4577967554b-35a38 558cb-530a-457795754b-35a38 558cb-530a-4577957554b-350a-457795754b-350a-4577957554b-350a-4577857554b-350a-457785754b-350a-457785754b-350a-457785754b-350a-457785754b-350a-457785754b-350a-457785754b-350a-457785754b-350a-457785754b-350a-457785754b-350a-457785754b-350a-457785754b-350a-457785754b-350a-457787554b-350a-457787554b-350a-457787554b-350a-457787554b-350a-457785754b-350a-457787554b-350a-457785754b-350a-457785754b-350a-457785754b-350a-457785754b-350a-457785754b-350a-457785754b-350a-4577856b-320-45787856b-320-45787866b-320-4587866b-378866b-378866b-378866b-378866b-378866b-378866b-3788			administrator	Desktop	Complete	11/4/2022 2:12 PM	00:00:48	VDA22-SIN	VDA22-SIN	Server22-SI	10,329 KB	8715bd68-1e78-4fed-89e6-1c50b7d535c9
ow Playing Administrator Desktop Complete 11/3/2022 50 F PM 00 01 52 VDA22 51N VDA22 51N Serve2251N 110 50 KE 115 89383 446r 460-440 454 4540 567 133 administrator Desktop Complete 11/3/2022 32 FM M0 010 12 VDA22 51N VDA22 51N Serve2251N 115 KB bb113453 446r 420 564r 4540 564 153 administrator Desktop Complete 11/3/2022 32 FM M0 010 22 VDA22 51N Serve2251N 312 KB 1467 7393 +174 4202 441 7664 450 564 153 administrator Desktop Complete 7/4/2022 315 FM 00 00 21 VDA22 51N Serve22 51N 544 KB 58 7766 458 H 423 693 430 456 201 h 203 426 471 b 436 493 430 456 201 h 203 426 471 b 436 494 126 964 447 956 447 340 4493 493 4493 494 447 969 447 447 964 447 447 964 447 447 964 447 447 447 447 4	Hestricted		administrator	Desktop	Complete	11/4/2022 1:59 PM	00:13:11	VDA22-SIN	VDA22-SIN	Server22-SI	10,812 KB	c54d5dfb-530c-4517-9679-54bb3fc3a388
owr Playing Administrator Desktop Complete 11/2/2022 54.6 PM 00.18.11 VDA22.51N Serve22.51N 1.55 1K8 bebr10343-ac6-4228-6bc-46bba8c1632 administrator Desktop Complete 7/4/2022 315 PM 00.02.10 VDA22.51N Serve22.51N 312 K8 9a Tre-425431-6bc356-0652 administrator Desktop Complete 7/4/2022 315 PM 00.02.10 VDA22.51N VDA22.51N Serve22.51N 301 K8 9a Tre-425431-6bc356-0652 administrator Desktop Complete 7/4/2022 315 PM 00.01.45 VDA22.51N VDA22.51N Serve22.51N 301 K8 9a Tre-425431-4234 s47 33dx153b 150 10 administrator Desktop Complete 7/4/2022 310 PM 00.01.45 VDA22.51N VDA22.51N Serve22.51N 112 bit 28 deshta64534 desdeset 428 438 desdeset 428 438 desdeset 428 438 desdee 438 438 desdee 438 438 desdee 438 438 desdee 438 438 desdee 448 438 desdee 448 438 438 desdee 448 438 desdee 448 438 438 desdee 448			administrator	Desktop	Complete	11/3/2022 5:08 PM	00:00:25	VDA22-SIN	VDA22-SIN	Server22-SI	7,788 KB	478ab02d-1527-4ff3-9d05-8b0ee1561c9a
ow Playing Administrator Desktop Complete 10/31/2022 32 PM 00:00.22 VDA22-SIN VDA22-SIN Serve22-SIN 312 K8 18/47:032 417-4620450-052 administrator Desktop Complete 7/4/2022 315 PM 00:00.15 VDA22-SIN VDA22-SIN Serve22-SIN 458 387-66-9874426343-ddad580-b127 administrator Desktop Complete 7/4/2022 315 PM 00:01:15 VDA22-SIN VDA22-SIN Serve22-SIN 448 387-66-9874426343-ddad580-b127 administrator Desktop Complete 7/4/2022 315 PM 00:01:15 VDA22-SIN VDA22-SIN Serve22-SIN 44164 387-66-46-46-657467 administrator Desktop Complete 7/4/2022 30.9 PM 00:01:15 VDA22-SIN VDA22-SIN 450-66 367-354-466/c6-76-46-545647 368 307-225-2548-466-68 367-664-46-465 368-66-76-46-76-46-46-46-46-46-46-46-46-46-46-46-46-46			administrator	Desktop	Complete	11/3/2022 5:06 PM	00:01:52	VDA22-SIN	VDA22-SIN	Server22-SI	10,690 KB	b19c9989-4bfe-460e-ba40-aa43dbd2caa5
ovr Playing Administrator Desktop Complete 7/4/2022 315 PM 000 02:10 VDA22-SIN VDA22-SIN Server22SIN 564 KB 837ecd-581+2378433db59b107 administrator Desktop Complete 7/4/2022 312 PM 000 02:15 VDA22-SIN VDA22-SIN Server22SIN 561 KB 5010x4554b107 3061 K554b107 3072 K574735444548b107 4581 K584b107 "><td></td><td></td><td>administrator</td><td>Desktop</td><td>Complete</td><td>11/2/2022 5:46 PM</td><td>00:18:11</td><td>VDA22-SIN</td><td>VDA22-SIN</td><td>Server22-SI</td><td>N 1,951 KB</td><td>bbc10349-acb6-4262-86cb-46bbb8c81638</td></t<>			administrator	Desktop	Complete	11/2/2022 5:46 PM	00:18:11	VDA22-SIN	VDA22-SIN	Server22-SI	N 1,951 KB	bbc10349-acb6-4262-86cb-46bbb8c81638
ow Playing Administrator Desktop Complete 7/4/2022 319 PM 00014 5 VDA22-SIN Server22SIN 360 K8 18106x80.456x-043.4284.4571/basc.465 administrator Desktop Complete 7/4/2022 309 PM 00011.5 VDA22-SIN VDA22-SIN Server22SIN 450 K8 18106x80.456x-043.4284.4571/basc.465 administrator Desktop Cop Play recording X IM 655 K8 90726.571735.4486456:00; 4F1 base.4465 administrator Desktop Cop Cop Cop Cop To continue, you are required to enter the justification for playing this IN 858 K8 7385056331-486-cbd7-78736443232113 administrator Desktop Cop Cop To continue, you are required to enter the justification for playing this IN 858 K8 7385056331-486-cbd7-7873644323 administrator Desktop Cop Cop V V VDA22-SIN VDA22-SIN VDA22-SIN VDA22-SIN VDA22-SIN VDA22-SIN VDA22-SIN VDA22-SIN VDA22-SIN VDA22-SIN VDA22-SIN VDA22-SIN VDA22-SIN VDA22-SIN			administrator	Desktop	Complete	10/31/2022 3:22 PM	00:00:28	VDA22-SIN	VDA22-SIN	Server22-SI	312 KB	146b7392-1f7f-4822-a4a1-7dedd53b0c62
Administrator Desktop Complete T-4/2022 3.09 PM 00.01.15 VDA22.SIN Serve22SIN 412 KB 24947864.9adf-4ee433480464552ff administrator Desktop Co Administrator Desktop Co A			administrator	Desktop	Complete	7/4/2022 3:15 PM	00:02:10	VDA22-SIN	VDA22-SIN	Server22-SI	N 544 KB	9a7fec4f-581f-428f-89df-33bfb59b1b70
Administrator Desktop Co Play recording administrator Desktop Co administrator		administrator	Desktop	Complete	7/4/2022 3:12 PM	00:01:45	VDA22-SIN	VDA22-SIN	Server22-SI	N 360 KB	8180de80-465e-4034-a28d-a471bdaace20	
ow Playing Administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co Image: To continue, you are required to enter the justification for playing this 1N 1N 125 KB 447904-eds-45947-9973155ba25 1N 1N 135 KB 55820-0784-80-666-764-1C6 H1 1N 1N 135 KB 55820-0784-80-666-764-1C6 H1 1N 1N 135 KB 55820-0784-80-666-764-1C6 H1 1N 1N 135 KB 55820-0784-80-666-764-1C6 H1 1N 1N 135 KB 55820-0784-80-966-764-1C6 H1 1N 1N 135 KB 55820-0			administrator	Desktop	Complete	7/4/2022 3:09 PM	00:01:15	VDA22-SIN	VDA22-SIN	Server22-SI	412 KB	2de9746d-9adf-4eed-833f-f80646521ffc
ow Playing administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co administrator Desktop Co Administrator Desktop Co Administrator Desktop Co Administrator Desktop Co Administrator Desktop Co Administrator Desktop Co Administrator Desktop Co Administrator Desktop Co Administrator Desktop Co Administrator Desktop Co Administrator Desktop Co Administrator De			administrator	Desktop	Co Play re-	cordina				× 11	N 665 KB	90722c57-4735-4446-bfcc-4fe1bae44d65
Administrator Desktop Co administrator Desk			administrator	Desktop		5				10	N 281 KB	321e9b11-8634-41c2-bf5e-e848f314aadf
administrator Desktop Co	low Playing	¥	administrator	Desktop	Co					11	N 581 KB	5340fb29-1fa9-4d16-9f97-0027a521f13f
Administrator Desitop Co administrator Desitop Co IN 125 KB 64379749809-806-7641-f5641 IN 135 KB 65838.00-798409-806-7641-f5641 IV 8588.00-798409-806-7641-f5641 IV 8588.00-798409-806-7641-f5641 IV 125 KB 647974-15641	now i laying	^	administrator	Desktop	Co		you are requ	uired to enter the just	stification for playing this	11	N 86 KB	d79a5056-93a1-4fec-bdc7-a7c79d6f4638
Yes No			administrator	Desktop	Co 4	recording.					N 125 KB	d4a75f04-ed4c-459f-9547-95f79156b2a2
l Yes No			administrator	Desktop						8 11	N 139 KB	b8588c30-79f8-480a-9b6b-764b41c5e141
					-							
					Γ							
					•							
vents and Bookmarks x									Yes N	10		
	Fronts and Realmerter	~										
	Events and DUOKMarks	×										

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\

Warning:

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

Disable or enable the recording reason logging

By default, administrator logging logs every recording reason after the policy query completes. This behavior might generate many logs. To improve the performance and save the storage, disable this kind of logging in the registry.

- 1. As an administrator, log on to the machine hosting the Session Recording server.
- 2. Open the Registry Editor.
- 3. Browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server**.
- 4. Set the value of EnableRecordingActionLogging to:
 - **0**: disable the recording reason logging
 - **1**: enable the recording reason logging

Best practices

June 21, 2024

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

- Configure load balancing in an existing deployment
- Deploy and load-balance Session Recording in Azure

Configure load balancing in an existing deployment

November 26, 2024

You can add load balancing nodes using Citrix ADC in an existing Session Recording deployment. The following servers are used as an example. You can also deploy and load-balance Session Recording in Azure.

Session Recording

Host Name	Server Role	OS	IP Address
SRServer1	Session Recording server	Windows Server	10.63.32.55
LBDC	Domain controller	Windows Server	10.63.32.82
TSVDA	Session Recording agent	Windows Server	10.63.32.215
SRSQL	Session Recording database and the file server	Windows Server	10.63.32.91

All Session Recording components and the domain controller share a domain, for example, lb. com. The domain administrator account, for example, lb\administrator, is used for server logon.

Citrix ADC

Host Name	Server Role	Management IP Address (NSIP)	Subnet IP Address (SNIP)
Netscaler	Citrix ADC VPX instance	10.63.32.40	10.63.32.109

For more information, see Deploy a Citrix ADC VPX instance.

Step 1: Create shared folders on the file server

- 1. Log on to the file server by using a domain administrator account, for example, lb\ administrator.
- 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 Record ing server. Using SRServer1 as an example, type LB\SRSERVER1\$. The dollar sign \$ is re quired.

🏪 🏹 📙 🖛 Window	vs (C:)								-		×
											~ 🕐
File Home Sha	re View										~ U
← → × ↑ 🐂 > '	「his PC → Wi	ndows (C:) ⇒						~ ē	Search Windows (C:)		Q
	Name		^	Date modified	Туре	Size					
📌 Quick access						5120					
Desktop 🔊			b3b8c5f458e292	10/29/2020 3:25 AN							
Downloads	PerfL	-		10/29/2020 6:00 AN							
	Prog	ram Files		11/23/2020 2:13 AN							
	Prog	ram Files (x86		11/23/2020 2:22 AN							
Fictures 🕫		onRecording			1 File folder						
💻 This PC		erver2017Me	Open in new windo	224	1 File folder						
_	Users		Pin to Quick access		1 File folder						
🥏 Network	- Wind	lows			1 File folder						
	💿 ip		Give access to	>	Remove access		KB				
			Restore previous ve		Specific people						
			Include in library	>							
			Pin to Start								
			Send to	>							
			Cut								
			Сору								
			Create shortcut								
			Delete								
			Rename								
			Properties								
			riopenies								_
9 items 1 item selected	1										800
									MACAddpor	06	22 60
🏪 📝 📑 🖛 Windov	vs (C:)								_		×
File Home Sha											~ 0
											4
$\leftarrow \rightarrow \checkmark \uparrow \blacksquare \flat$	This PC → Wi							~ Ū	Search Windows (C:)		P
	Name		^	Date modified	Туре	Size					
📌 Quick access		725 1 050000	1 21 0 55150 202								
Desktop 🤉	e =		b3b8c5f458e292	10/29/2020 3:25 AN 10/29/2020 6:00 AN							
👆 Downloads 🗦	PerfL	.ogs ram Files		11/23/2020 0:00 AIV							
Documents 🦻		ram Files (x86)	5	11/23/2020 2:22 AN							
Pictures 2		onRecording		11/25/2020 2:22 Alv 11/25/2020 3:06 Alv							
		onRecording		11/25/2020 3:00 AN							
💻 This PC		Gerver20					- 0	×			
💣 Network	Users		- N								
- Metholic	Wind		2 Network access								
	ip										
			Choose people on	your network to	share with						
			-								
			Type a name and then c	lick Add, or click the	arrow to find someone.						
						~	Add				
			Name			Permission		1			
			& Administrator			Read/Write					
			Administrator			Owner	•				
						Read/Write					
			LB\SRSERVER1\$			Read/Write					
						Read/Write					
						Read/Write					
						Read/Write					
10 items 1 item selecti	ed		LB\SRSERVER1\$	ng		Read/Write				E	
10 items 👘 1 item selecti	ed			ng		Read/Write					
10 items 1 item select	ed		LB\SRSERVER1\$	ng				Cancel			

3. Create a subfolder within the SessionRecording folder and name the subfolder share, for example, C:\SessionRecording\share.

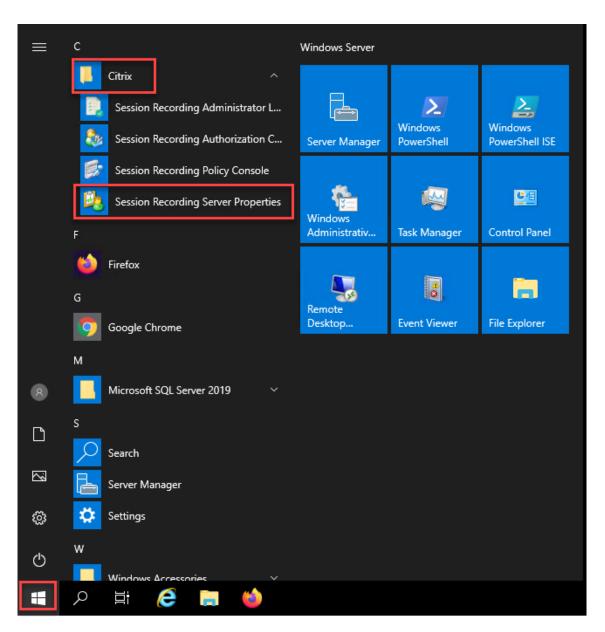
	Share	View							~ (
→ • ↑	> Thi	PC > Windows ((C:) > SessionRecord	ling >			~ Ū	Search SessionRecording	P
📌 Quick access		Name	^	Date modified	Туре	Size			
Desktop	*	share		11/25/2020 5:24 AM	File folder				
Downloads	*								
Documents	*								
Pictures	*								
This PC									
Network									

- 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.

Session Recording Server Properties —		×
Storage Signing Rollover Playback Notifications CEIP	Logging	RI
Recorded session files are stored in the directories specified in a load-balanced manner, specify multiple directories acros volumes.		
File storage directories:		_
\\SRSQL\SessionRecording\share	A <u>d</u> d.	
	<u>M</u> odify	
	Remo	ve
Specify a folder to temporarily store archived session record	inas and n	nake
them available for playback.		
Restore directory for archived files:		_
\\SRSQL\SessionRecordingsRestored\share	Browse	ə
OK Cancel		Apply
		2-2-0

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)

er\HK	EY_LOCAL_MACHINE\SOFTWARE\Citri	SmartAuditor\Server			
omput	ter	Name	Туре	Data	
HKEY_CLASSES_ROOT		(Default)	REG_SZ	(value not set)	
		installed	REG_DWORD	0x00000001 (1)	
·	Y_LOCAL_MACHINE	AllowLivePlayback	REG_DWORD	0x00000001 (1)	
	CD0000000	ab AzureSQLServiceAdminPasswo	-		
	ARDWARE	ab AzureSQLServiceAdminUserna	-		
	AM	ab DatabaseFailoverPartner	REG SZ		
_	ECURITY	ab DatabaseName	REG_SZ	CitrixSessionRecording	
-	OFTWARE	Bill DeferredHashCalcFileSizeThres	-	0x00200000 (2097152)	
Y	Citrix	B DormantTimeInHours	REG_DWORD	0x00000030 (48)	
	Citrix Desktop Delivery Controller	Big EnableAnalytics	REG_DWORD	0x00000001 (1)	
>	InstallAgent	EnableAzureSOLService	REG_DWORD	0x00000000 (0)	
>	MetaInstall	100 EnableLB	REG DWORD	0x00000001 (1)	
~	SmartAuditor	EnableRecordingActionLogging	REG_DWORD	0x00000001 (1)	
Ĩ	Server	EnableSRStorageLogging	REG DWORD	0x00000001 (1)	
	XenTools	EnableWebBasedSrPlayer	REG DWORD	0x00000001 (1)	
	XenToolsInstaller	ab FileStorageDirectories	REG MULTI SZ	\\SRSQL\SessionRecording\share	
5	XenToolsNetSettings	LinkEmail	REG SZ	(Shade Session Recording Share	
>	Classes	ab LinkExpire	REG SZ	172800000000	
3	Clients	LinkExpire LinkHost	REG_SZ	17200000000	
	DefaultUserEnvironment	ab LinkSalt	-	kk2od974	
>	Google		REG_SZ		
>	Intel	BLoggingBlockState	REG_DWORD	0x00000001 (1)	
>	Microsoft	LoggingDatabaseFailoverPartner	-		
>	Mozilla	ab LoggingDatabaseName	REG_SZ	CitrixSessionRecordingLogging	
>	mozilla.org	CoggingLoggingState	REG_DWORD	0x0000001 (1)	
>	ODBC	88 MaxOpenFiles	REG_DWORD	0x00002710 (10000)	
>	OpenSSH	ab NotifyMessageByCulture	REG_MULTI_SZ		
>	Partner	ab NotifyMessageDefault	REG_SZ	Your activity with the desktop or program(s) you r	
>	Policies	88 PlaybackProtection	REG_DWORD	0x00000001 (1)	
>	Qualys	8 PlayerUserRBACEnabledKey	REG_DWORD	0x00000000 (0)	
	RegisteredApplications	ab PolicyFilePath	REG_SZ	C:\Program Files\Citrix\SessionRecording\Server\\	
>	Setup	BolicyFileRefreshPeriodInSeco	REG_DWORD	0x0000012c (300)	
>	WOW6432Node	RoleBasedSecurityEnabled	REG_DWORD	0x00000001 (1)	
	YSTEM	RolloverFileSizeInMB	REG_DWORD	0x00000032 (50)	
	Y_USERS	RolloverTimeInHours	REG_DWORD	0x000000c (12)	
HKE	Y_CURRENT_CONFIG	8 SkipReceiverVersionCheck	REG_DWORD	0x00000001 (1)	

5. Restart the Citrix Session Recording Storage Manager service.

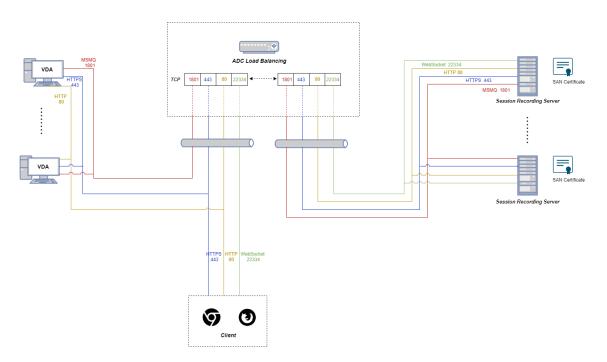
Step 3: Configure load balancing in Citrix ADC

There are two ways to configure load balancing in Citrix ADC - TCP passthrough and SSL offloading.

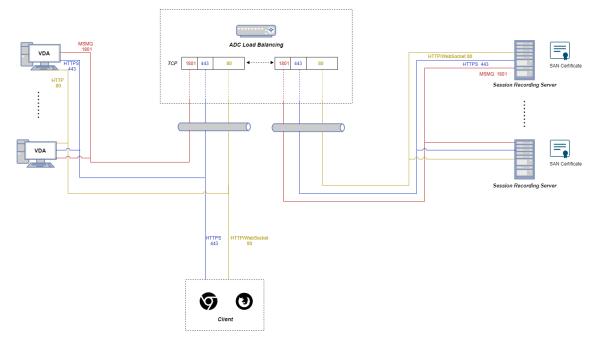
Configure load balancing through TCP passthrough

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 followings steps:

- 1. Log on to your Citrix ADC VPX instance.
- 2. Navigate to **Configuration > System > Settings > Configure Basic Features**.

	PX (100	0)
Dashboard C	onfigurati	on Reporting Documentation Downloads
Q Search in Menu		System / Settings
System	\sim	Settings
Licenses Settings Diagnostics High Availability	>	Modes and Features Configure Modes Configure Basic Features Configure Advanced Features
NTP Servers Reports Profiles		Configure Extra Management CPU
Partition Administration User Administration	>	
Authentication	>	
Auditing SNMP	>	ADM
AppFlow	• >	Configure ADM Parameters

3. Select Load Balancing and click OK.

citrix. Add										
Dashboard	Configuration	Reporting	Documentation	Downloads						
G Configur	e Basic Feat	ures								
SSL Offloading		HTTP Compression								
🗸 Load Balancing		Content Switching								
Content Filter		Integrated Caching								
Rewrite		Citrix Gateway								
Authentication, Au	thorization and Auditing									
ОК С	ose									

4. Add load balancing servers.

Navigate to **Traffic Management > Load Balancing > Servers** and click **Add**.

CİTIX. ADC VPX (1000)									
Dashboard	Configurat	tion R	eporting	Documentation	Downloads				
Q Search in Menu		Traffic Man	agement / Lo	ad Balancing / Servers					
System AppExpert	>	Serve	rs ០						
Traffic Management	~	Add	Edit Del	ete Rename	Select Action \checkmark				
Load Balancing Virtual Servers	~								
Services			NAME		STATE		IPADDRESS / DOMAIN		
Service Groups		No items							
Monitors									
Metric Tables									
☆ Servers Persistency Groups									
Radius Nodes	(!)								
Priority Load Balancin	g 🧵 >								
Content Switching	() >								

Type the name and IP address of a Session Recording server and then click **Create**. For example:

Dashboard	Configuration	Reporting	Documentation	Downloads						
Croate S	Croate Server									

Create Server

Name*	
srv-1	\bigcirc
IP Address Domain Name	
IPAddress*	
10.63.32.55	
Traffic Domain	
~	Add Edit
🗸 Enable after Creating	
Comments	
Create Close	

Click the save icon in the upper right corner to save your changes.

Traffic Management / Load Balancin	ng / Servers			_
Servers 1				CR
Add Edit Delete Re	ename Select Action V			
\mathbf{Q} Click here to search or you can enter	er Key : Value format			0
NAME	STATE	IPADDRESS / DOMAIN	TRAFFIC DOMAIN	
🗸 srv-1	ENABLED	10.63.32.55		0
Total 1				25 Per Page ∨ Page 1 of 1 ∢ ▶

 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.

CİİTIX. ADC VPX (1000)									
Dashboard	Configurat	tion Repor	ting D	ocumentation	Downloads				
Q Search in Menu		Traffic Managem	ent / Load Ba	alancing / Services ,	/ Services				
System AppExpert	>	Services							
Traffic Management	~	Services 0	Auto Dete	cted Services 0	Internal Services 6				
Load Balancing Virtual Servers	~	Add Edit	Delete	Rename	tistics No action 🗸				
Services		${f Q}$ Click here to search or you can enter Key : Value format							
Service Groups		NA	ME		♦ SERVER STATE				
Monitors		No items							
Metric Tables									
Servers									
Persistency Groups	;								
Radius Nodes									
Priority Load Balancin	g 🧵 >								
Content Switching	• >								

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**.

Dashboard	Configuration	Reporting	Documentation	Downloads
Load Bala	ancing Serv	ice		
Basic Settings				
Service Name*				
srv-1-80		()		
New Server	• Existing Server			
Server*				
srv-1 (10.63.32	55) 🗸			
Protocol*				
TCP	~	(i)		
Port*				
80		()		
More				

Bind the TCP protocol monitor to each load balancing service.

Dashboard	Configuration	Reporting	Documentation	Downloads
Load Bala				ad Balancing Monitor Binding / Load Balancing Monitor Binding
				alancing Monitor Binding
			Select Monit	hitor*
			Binding Deta	tails
	 DOWN 		Weight	
	ТСР		1	
			🗸 State	
			Bind	Close

Click the save icon in the upper right corner to save your changes.

Traffic Manage	ment / Load Balancing / Services	/ Services							
Service	5								Q 🗐
Services 4	Auto Detected Services 0	Internal Services 6							
Add	Edit Delete Statistics	Action 👻							Search 👻
	Name	State	IP Address/Domain Name	Port	Protocol	Max Clients	Max Requests	Cache Type	Traffic Domain
	srv-1-1801	• UP	10.63.32.55	1801	TCP	0	0	SERVER	0
	srv-1-22334	• UP	10.63.32.55	22334	TCP	0	0	SERVER	0
	srv-1-443	• UP	10.63.32.55	443	TCP	0	0	SERVER	0
	srv-1-80	• UP	10.63.32.55	80	TCP	0	0	SERVER	0

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 balanc-ing virtual servers** of ports 80, 443, and 1801. For example:

Traffic Manag	ement / Load Balancing / Virtual Servers									
Virtual	Servers									Q 💿 😭
Add Edit Delete Enable Disable Statistics Action									Search 💌	
	Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence	% Health	Traffic Domain
	vsrv-80	• UP	●UP	10.63.32.60	80	TCP	LEASTBANDWIDTH	SOURCEIP	100.00% 1 UP/0 DOWN	0
	vsrv-1801	• UP	●UP	10.63.32.60	1801	TCP	LEASTBANDWIDTH	SOURCEIP	100.00% 1 UP/0 DOWN	0
	vsrv-443	• UP	●UP	10.63.32.60	443	TCP	LEASTBANDWIDTH	SOURCEIP	100.00% 1 UP/0 DOWN	0
	vsrv-22334	• UP	●UP	10.63.32.60	22334	TCP	LEASTBANDWIDTH	SOURCEIP	100.00% 1 UP/0 DOWN	0

Navigate to Traffic Management > Load Balancing > Virtual Servers and click Add.

citrix. Add	VPX (100	00)							
Dashboard	Configurat	tion Re	porting	Documentatio	n Dov	vnloads			
Q Search in Menu		Traffic Mana	gement / Load	Balancing / Virtu	al Servers				
System	>	Virtua	Server	s 🚹					
AppExpert	>	VIIItuu		5					
Traffic Management	~	Add	Edit Delete	e Enable	Disable	Rename	Statistics	Select Action \checkmark	
Load Balancing	~	Q Click her	e to search or yo	u can enter Key : Val	ue format				
☆ Virtual Servers		~				07175	· · · · · · · · · · · · · · · · · · ·		10 4000500
Services			NAME			STATE	EFFECTIVE ST	TATE \diamond	IP ADDRESS
Service Groups		No items							
Monitors		Total 0							
Metric Tables									
Servers									
Persistency Groups									
Radius Nodes									
Priority Load Balancin	g 🧵 >								
Content Switching	<u> </u>								

Add each virtual server with the Citrix ADC VIP address based on the TCP protocol.

itriý ADC	VPX (1000)			
Dashboard	Configuration	Reporting	Documentation	Downloads
Load Bal	ancing Virtu	al Server		
Basic Settings				
network (WAN), th	e VIP is usually a private (ICANN non-routable)	IP address.	plication is accessible from the Internet, the virtual server IP (VIP) address is a publ ailability of resources to process client requests.
Name*				
vsrv-80		(j)		
Protocol*				
TCP		(i)		
IP Address Type*				
IP Address		·		
IP Address*				
10 . 63 .	32 . 60	(i)		
Port*				
80		(i)		
More				
ОК	Cancel			

Bind each virtual server to the **load balancing service** of the same port. For example:

С	itrix. AI	DC VPX (1000)										
	Dashboard	Configuration	Reporting	Documentation	Downloads							
€		alancing Virtu										
	Name Protocol State IP Address Port Traffic Domain	vsrv-80 TCP • DOWN 10.63.32.60 80 0				Lister Redir Rang IPset RHI S AppF Retai		- NONE IP 1 - PASSIV ENABL NO -				
	Services and	Services and Service Groups										
	A service grou Note: Bind at l	east one service or service g	roup of services as the roup to the virtual serv	ugh it were a single service er.	After creating a service group, y any other configuration detail th		tual server, and you can ac	ld service				
	No Load Bala	ncing Virtual Server Servio	ce Binding									
	No Load Bala	No Load Balancing Virtual Server ServiceGroup Binding										
	Continue											

citrix. Ad	C VPX (1000)		
Dashboard	Configuration	Reporting	Documentation Downloads
G Load Ba	lancing Virtu	ıal Server	Service Binding / Service Service 4
			Select Add Click here to search or you can enter Key : Value for NAME srv-1-80 srv-1-443 srv-1-1801 srv-1-22334

Choose a load balancing method.

Method is a load balancing algorit	hm that the Citrix ADC	uses to
Load Balancing Method*		
LEASTBANDWIDTH	~ (i)	
New Service Startup Request Rate	5	
0		
Backup LB Method*		
ROUNDROBIN	\sim	
New Service Request unit*		
PER_SECOND	\sim	
Increment Interval		

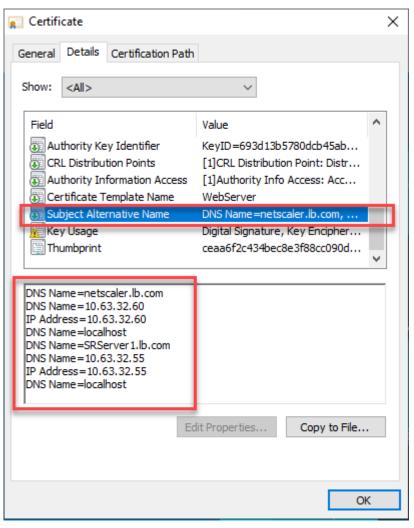
Configure persistence on each virtual server. We recommend you select **SOURCEIP** as the persistence type. For more information, see Persistence settings.

Persistence
Configure persistence to route all connections from the same use persistence type fails.
Select Persistence Type*
Time-out (mins)*
2
IPv4 Netmask
255 . 255 . 255 . 255
IPv6 Mask Length
128
ОК

7. Create a host record for the Citrix ADC VIP address on the domain controller.

Elle Action Yiew Help IBDC Image: Start of Authority (SOA) Image: Start of Authority (SOA) Image: Start of Authority (SOA) Ibbcm Image: Start of Authority (SOA) [47], lideLib.com, hostma. static Image: Start of Authority (SOA) [47], lideLib.com, hostma. static Image: Start of Authority (SOA) [47], lideLib.com, hostma. static Image: Start of Authority (SOA) [47], lideLib.com, hostma. static Image: Start of Authority (SOA) [47], lideLib.com, hostma. static Image: Start of Authority (SOA) [47], lideLib.com, hostma. static Image: Start of Authority (SOA) [47], lideLib.com, hostma. static Image: Start of Authority (SOA) [47], lideLib.com, hostma. static Image: Start of Authority (SOA) [47], lideLib.com, hostma. static Image: Start of Authority (SOA) [47], lideLib.com, hostma. static Image: Start of Authority (SOA) [47], lideLib.com, hostma. static Image: Start of Authority (SOA) [47], lideLib.com, hostma. static Image: Start of Authority (SOA) [40], 10.63.32.81 11/19/2020 1:00.00 PM Image: Start of A	🤱 DNS Manager					_		×		
▶ DNS ↓ LBDC ↓ Data Timestamp ↓ BDC	<u>File Action View H</u> elp	Eile Action View Help								
 LBDC Forward Lookup Zones Sites Ltcp Lbcom Trust Points Conditional Forwards Conditional Forwards Conditional Forwarders Conditional Forwarders Start of Authority (SOA) Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad Idad <liidad< li=""> Idad</liidad<>										
	LBDC LBDC Gamma Cookup Zones	sitestcpudpudpometainesforestDnsZonesforestDnsZones(same as parent folder)(same as parent folder)(same as parent folder)lbdclbdclbdDCsRServer1SRServer1SRServer2SRSQL	Start of Authority (SOA) Name Server (NS) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A)	[47], Ibdc.lb.com, hostma Ibdc.lb.com, 10.63.32.82 10.63.32.82 10.63.32.11 10.63.32.50 10.63.32.55 10.63.32.56 10.63.32.68	static static 11/19/2020 2:00:00 AM static 11/19/2020 11:00:00 PM static 11/19/2020 1:00:00 AM 11/19/2020 11:00:00 PM 11/23/2020 3:00:00 AM					

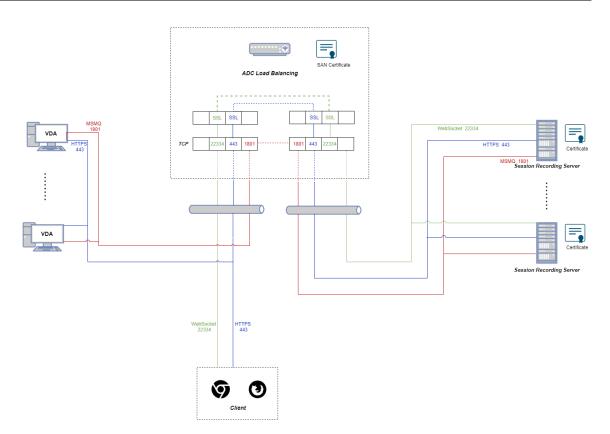
8. To access the web player over HTTPS, ensure that a SAN certificate is available both on Citrix ADC and on each Session Recording server. A SAN certificate contains the FQDNs of the Citrix ADC and of each Session Recording server.



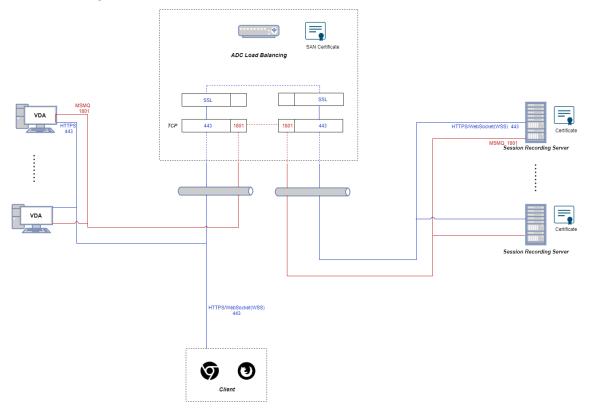
Configure load balancing through SSL offloading

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.

CITIX ADC VI	CİİTIX ADC VPX (1000)							
Dashboard Co	onfiguratio	on Reporting Documentation Downloads						
Q Search in Menu		System / Settings						
System Licenses	~	Settings						
☆ Settings Diagnostics High Availability	>	Modes and Features Configure Modes Configure Basic Features Configure Advanced Features						
NTP Servers Reports Profiles		Configure Extra Management CPU						
Partition Administration	>							
User Administration	>							
Authentication	>							
Auditing	>							
SNMP	>	ADM						
AppFlow	• >	Configure ADM Parameters						

2. Navigate to **Configuration > System > Settings > Configure Basic Features**.

3. Select SSL Offloading and Load Balancing and click OK.

CİTIX ADC VPX (1000)								
Dashboard	Configuration	Reporting	Documentation	Downloads				
Configure Basic Features								
SSL Offloading		HTTP Compres	sion					
✓ Load Balancing		Content Switching						
Content Filter		Integrated Caching						
Rewrite		Citrix Gateway						
Authentication, Authorization and Auditing								
ОК СІ	ose							

4. Add load balancing servers.

Navigate to Traffic Management > Load Balancing > Servers and click Add.

citrix. Add v	VPX (10)0)		_		
Dashboard	Configura	ion	Reporting	Documentation	Downloads	
Q Search in Menu		Traffic Ma	nagement / Lo	oad Balancing / Servers		
System AppExpert	>	Serve	ers 重			
Traffic Management	~	Add	Edit Del	lete Rename	Select Action \checkmark	
Load Balancing Virtual Servers	\sim	Q Click	nere to search or	you can enter Key : Value fo	rmat	
Services			NAME		STATE	IPADDRESS / DOMAIN
Service Groups		No items				
Monitors						
Metric Tables						
☆ Servers						
Persistency Groups						
Radius Nodes						
Priority Load Balancin	g ! >					
Content Switching	(!) >					

Type the name and IP address of a Session Recording server and then click **Create**. For example:

Dashboard	Configuration	Reporting	Documentation	Downloads			
Croate Server							

Create Server

Name*	
srv-1	\bigcirc
IP Address Domain Name	
IPAddress*	
10.63.32.55	
Traffic Domain	
~	Add Edit
🗸 Enable after Creating	
Comments	
Create Close	

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:

Traffic Manager	ment / Load Balancing / Services / Ser	vices							
Services	5								Q E
Services 3	Auto Detected Services 0 Inter	nal Services 6							
Add	Edit Delete Statistics	Action 👻							Search 🛩
	Name	State	IP Address/Domain Name	Port	Protocol	Max Clients	Max Requests	Cache Type	Traffic Domain
0	srv-1-443	• UP	10.63.32.55	443	SSL	0	0	SERVER	0
	srv-1-1801	• UP	10.63.32.55	1801	TCP	0	0	SERVER	0
	srv-1-22334	• UP	10.63.32.55	22334	SSL	0	0	SERVER	0

Navigate to Traffic Management > Load Balancing > Services and click Add.

citrix. Add v	VPX (100	00)							
Dashboard	Configurat	ion Re	eporting	Documentation	Dowr	nloads			
Q Search in Menu		Traffic Management / Load Balancing / Services / Services							
System > AppExpert >		Services							
Traffic Management	~	Services	0 Au	to Detected Services) Interna	l Services 6			
Load Balancing Virtual Servers	~	Add	Edit D	elete	Statistics	No action 🗸			
☆ Services	Q Click here to search or you can enter Key : Value format								
Service Groups			NAME		\$	SERVER STATE			
Monitors		No items							
Metric Tables									
Servers									
Persistency Groups									
Radius Nodes									
Priority Load Balancin	g 🧵 >								
Content Switching	• >								

(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.

citrix ada	C VPX (1000)		
Dashboard	Configuration	Reporting	Docum
🕒 Load Bal	ancing Serv	ice	
Basic Settings			
Service Name* srv-1-22334		()	
O New Server	• Existing Server		
Server*	2.55)		
Protocol*	-		
SSL	×	(i)	
Port*		(ī)	
► More		U III	
OK	Cancel		

Bind the TCP monitor to the **SSL load balancing service** you just added.

CİTIX. ADC VPX (1	000)	
Dashboard Configu	ration Reporting	Documentation Downloads
G Load Balancing	g Service	Service Load Balancing Monitor Binding / Load Balancing Monitor Binding
		Select Monitor*
Service Name Server Name IP Address	srv-1-22334 srv-1 10.63.32.55	tcp Add Edit () Binding Details
	• DOWN SSL 22334	Weight ()
		✓ State Bind Close
Sure Connect		

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**.

citrix. add	VPX (1000)	
Dashboard	Configuration	Reporting C
😔 Load Bal	ancing Ser	rvice
Basic Settings		
Service Name*		
srv-1-443		()
O New Server	• Existing Server	
Server*		
srv-1 (10.63.32	.55)	\sim
Protocol*		
SSL		\sim
Port*		
443		(j)
More		
ОК	Cancel	

Bind the HTTPS monitor to the **SSL load balancing service** you just added.

Dashboard	Configuration Reporting	Documentation Downloads
		Service Load Balancing Monitor Binding / Load Balancing Monitor Binding
Load Balar	ncing Service	Load Balancing Monitor Binding
		Select Monitor*
		https > Add Edit (
		Binding Details
	• DOWN	Weight
		1
		✓ State

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**.

citrix ado	C VPX (1000)		
Dashboard	Configuration	Reporting	Documentati
🕒 Load Bal	ancing Serv	vice	
Basic Settings			
Service Name* srv-1-1801		()	
New Server	• Existing Server		
srv-1 (10.63.32	2.55)	/	
Protocol*			
TCP		× ()	
Port* 1801		Ō	
► More			
ОК	Cancel		

Bind the TCP monitor to the **TCP load balancing service** you just added.

Dashboard	Configuration	Reporting	Documentation	Downloads	Notion (Lond Del	e Masitas Diadi
Load Bala	ancing Serv				Binding / Load Balancin	g Monitor Binding
				lancing Monit	or Binding	-
			Select Moni	tor*	Add	Edit
					7	
			Binding Det	ails		
	• DOWN		Weight			
			1			
			✓ State			
			Bind	Close		

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**.

citrix add	VPX (100	00)						
Dashboard	Configurat	ion Rep	oorting	Documentati	on	Downloads		
Q Search in Menu		System / Pr	ofiles / H	HTTP Profiles				
System	~	Profiles	5					
Licenses Settings		TCP Profiles		HTTP Profiles 3		Database Profiles	0	SSL Profil
Diagnostics High Availability	>	Add	dit D	elete				
NTP Servers	,	Q Click here	to search (or you can enter Key : Va	alue f	ormat		
Reports			NAME		\$	DROP INVALID 💠	INV	ALIDATE HTTI
🟫 Profiles			nshttp_c	lefault_profile		×	×	
Partition Administration	on >		nshttp_c	lefault_strict_validation	n	~	~	
User Administration	>		nshttp_c	lefault_internal_apps		~	~	
Authentication	>	Total 3			_			
Auditing	>	Total O						
SNMP	>							

Select the **Enable WebSocket connections** check box and accept the other default settings.

HTTP/2 Initial Window Size		
65535		
HTTP/2 Maximum Concurrent Streams		
100		
HTTP/2 Maximum Frame Size		
16384		
HTTP/2 Minimum Server Connections		
20		
HTTP/2 Maximum Header List Size		
24576		
HTTP/2 Maximum Ping Frames Per Minute		
HTTP/2 Maximum Reset Frames Per Minute		
HTTP/2 Maximum Empty Frames Per Minute		
HTTP/2 Maximum Settings Frames Per Minute		
0		
Alternative Service	Connection Multiplexing	Drop invalid HTTP requests
Mark HTTP/0.9 requests as invalid	Mark CONNECT Requests as Invalid	Mark TRACE Requests as Inva
Mark RFC7230 Non-Compliant Transaction as Invalid	Mark HTTP Header with Extra White Space as Invalid	Compression on PUSH packet
✓ Drop extra CRLF	Enable WebSocket connections (i)	Enable RTSP Tunnel
Drop extra data from server	✓ HTTP Weblogging	Persistent ETag
Adaptive Timeout		
Close		
Close		

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**.

С	itriż, adc vi	PX (1000)				HA Status Not configured	Parti defau	t ion 🗸 It	nsroot ∨
	Dashboard	onfiguration	Reporting	Documentation	Downloads	i			\$
¢	Load Balan	cing Servi	се						
	Basic Settings						/	Help	
	Service Name Server Name IP Address Server State Protocol Port Comments	srv-1-2233 srv-1 10.63.32.5 • DOWN SSL 22334		Traffic Domain Number of Active Connecti Hash ID Server ID Clear Text Port Cache Type Cacheable Health Monitoring AppFlow Logging	0 ons - - None - SERVE NO YES ENABL				
	Monitoring Connection Cl	lose Bit NONE		Approv COPPILS				+ SSL	Profile
	Service Settings					1	×	+ SSL	Policies
	Sure Connect Surge Protection OFF Use Proxy Port YES			Client Keep-Alive	NO NO NO			+ Cert	tificate

Select the HTTP profile, for example, websocket_SSL, and click **OK** and then **Done**.

Profiles	
Net Profile	
	✓ +
TCP Profile	
	✓ +
HTTP Profile	
websocket_SSL	✓ +
DNS Profile Name	
	✓ +
ОК	
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.

🛔 DNS Manager					-	×
<u>File</u> <u>Action</u> <u>V</u> iew <u>H</u> elp						
🗢 🄿 🙍 📆 🔀 🔤	? 🖬 🗄 🖬 🖬					
 DNS LBDC Forward Lookup Zones Simmatics.lb.com Reverse Lookup Zones Crust Points Conditional Forwarders 	Name Insdcs Insdcs Isites Ltcp DomainDnsZones ForestDnsZones (same as parent folder) (same as parent folder) Ibdc LBDDC NetsColer SRServer1 SRServer2 SRSQL TSVDA	Type Start of Authority (SOA) Name Server (NS) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A)	Data [47], Ibdc.lb.com, hostma Ibdc.lb.com. 10.63.32.82 10.63.32.82 10.63.32.60 10.63.32.55 10.63.32.55 10.63.32.91 10.63.32.91	Timestamp static static 11/19/2020 2:00:00 AM static 11/19/2020 11:00:00 PM static 11/19/2020 11:00:00 PM 11/23/2020 3:00:00 AM 11/23/2020 2:00:00 AM		

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.

Traffic Manage	ment / Load Balancing / Virtual Servers								
Virtual	Servers								
Add Edit Delete Enable Disable Statistics Action									
	Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence	% Health
	vsrv-1801	• UP	• UP	10.63.32.60	1801	TCP	LEASTBANDWIDTH	SOURCEIP	100.00% 2 UP/0 DOWN
	vsrv-443	• UP	• UP	10.63.32.60	443	SSL	LEASTBANDWIDTH	SOURCEIP	100.00% 2 UP/0 DOWN
	vsrv-22334	• UP	• UP	10.63.32.60	22334	SSL	LEASTBANDWIDTH	SOURCEIP	100.00% 2 UP/0 DOWN

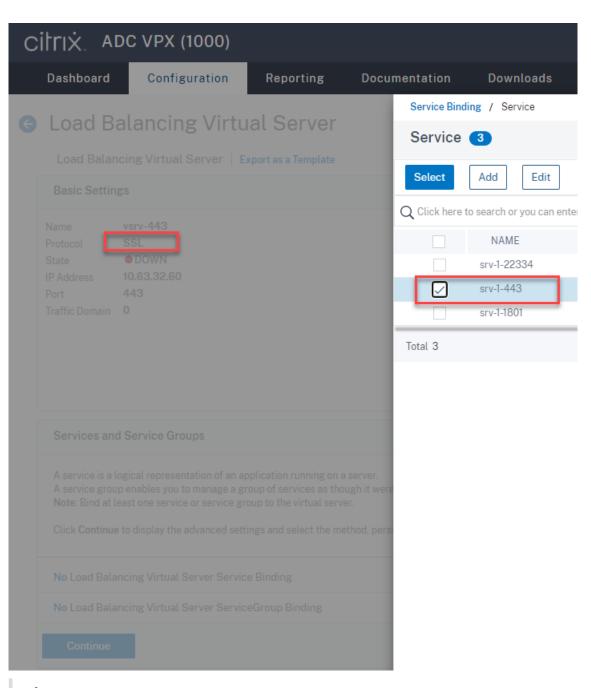
Navigate to Traffic Management > Load Balancing > Virtual Servers and click Add.

citrix add	VPX (100)0)				
Dashboard	Configurati	tion Reporting	Documentation	Downloads		
Q Search in Menu		Traffic Management / Lo	ad Balancing / Virtual Serve	ers		
System	>	Virtual Serve	rs በ			
AppExpert	>	virtual ocree				
Traffic Management	~	Add Edit Del	ete Enable Disable	e Rename	Statistics Select	Action 🗸
Load Balancing	~	Q Click here to search or	you can enter Key : Value form	at		
☆ Virtual Servers		NAME		STATE	EFFECTIVE STATE	IP ADDRESS
Services		No items		0.1112		, in Hobileou
Service Groups		No items				
Monitors		Total 0				
Metric Tables						
Servers						
Persistency Groups						
Radius Nodes						
Priority Load Balancin	g)					
Content Switching	() >					

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.

İİTIX. ADC VPX	(1000)		
Dashboard Conf	iguration Reporting	Documentation	Downloads
Load Balanci	ng Virtual Server		
Basic Settings			
network (WAN), the VIP is u You can configure multiple	sually a private (ICANN non-routable	e) IP address.	pplication is accessible from the Internet, the virtual server IP (VIP) address is a pu ailability of resources to process client requests.
Name*			
vsrv-80	(j)		
Protocol*			
TCP	~ (i)		
IP Address Type*			
IP Address	\sim		
IP Address*			
10 . 63 . 32 .	60 (j)		
Port*			
80	(j)		
► More			
OK Cancel			

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 Web-Socket server Version 1.0.

Choose a load balancing method.

Method is a load balancing algorit	hm that the Citrix ADO	Cuses to
Load Balancing Method*		
LEASTBANDWIDTH	~ (i)	
New Service Startup Request Rate	3	
0		
Backup LB Method*		
ROUNDROBIN	\sim	
New Service Request unit*		
PER_SECOND	\sim	
Increment Interval		

Configure persistence on each virtual server. We recommend you select **SOURCEIP** as the persistence type. For more information, see Persistence settings.

Persistence

Configure persistence to route all connections from the same user primary persistence type fails.

Select Persistence Type*	
● SOURCEIP ○ OTHERS (Ð
Time-out (mins)* 30	Ō
IPv4 Netmask	
255 . 255 . 255 . 255	
IPv6 Mask Length	
128	
ок	

(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.

Profiles	×	
A profile is a collection of settings that can be applied to a NetScaler entity, such as a virtual	server or service. You can apply the same profile to multiple entities of the same type.	
Net Profile TCP Profile LB Profile +	HTTP Profile websocket_SSL + 2 DB Profile + 2 DNS Profile Name + 2	
ОК		

10. Install a Subject Alternative Name (SAN) certificate in Citrix ADC.

Obtain a SAN certificate in PEM format from a trusted Certificate Authority (CA). Extract and upload the certificate and private key files in Citrix ADC by navigating to **Traffic Management > SSL > Server Certificate Wizard**.

For more information, see SSL certificates.

4 Install Certific	cate	
Certificate-Key Pair Name	*	
lbcard		
Certificate File Name*		
Choose File 🔻 Ibcard	l.cer	0
Key File Name*		
Choose File 🔻 Ibcard	l.key	0
Password*		
	0	
Notify When Expires		
No SNMP Trap destinati	ion found. Notification will not	be sent until a trap destination is configured.
Notification Period		
30		
Create Cancel		

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**.

С	itriż ai	DC VPX (1000)			
	Dashboard	Configuration	Reporting	Documentation	Downloads
¢	Load B	alancing Virtu	ıal Server		
	Load Balar	ncing Virtual Server E	xport as a Template		
	Basic Settin	gs			
	Protocol State IP Address	443			
	Services and	d Service Groups			
	1 Load Baland	cing Virtual Server Service	Binding		
	No Load Bala	ncing Virtual Server Servic	eGroup Binding		
	Certificate				
	No Server Ce	rtificate			
	No CA Certifi	cate			
	Continue				

Add the previously mentioned SAN certificate and click **Bind**.

Step 4: Configure an existing Session Recording agent to support load balancing

- 1. Log on to the Session Recording agent by using a domain administrator account.
- 2. Open Session Recording Agent Properties.
- 3. Complete this step if you use Microsoft Message Queuing (MSMQ) over TCP.

Type the FQDN of your Citrix ADC VIP address in the **Session Recording Server** box.

🐉 Session Recording Agent Pr	operties	—		\times
Recording Connections				
				_
Session Recording Server:	NetScaler.lb.com			
-Session Recording Storage Ma	anager message queue			_
Protocol:	TCP \sim			
HTTP/HTTPS port:	Default \sim			
Port Number:				
Message life specifies the pe message queue.	riod during which data	a remains	in the	
Message life (seconds):	7200			
Session Recording Broker				
Protocol:	HTTPS \sim			
HTTP/HTTPS port:	Custom \checkmark			
Port Number:	443			
	ОК С	ancel	Ap	ply

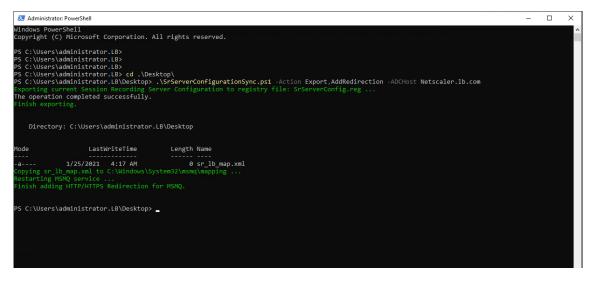
On each Session Recording server, add and set the IgnoreOSNameValidation DWORD value to 1 under HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\MSMQ\ Parameters. For more information, see Knowledge Center article CTX248554.

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.

🏝 DNS Manager					-	\times
<u>File Action View H</u> elp						
🗢 🔿 🙍 📅 🔀 📴 🛃						
DNS DNS DNS DNS DNS DNS Doward Lookup Zones Doward Lookup Zones Doward Lookup Zones Dowards Dowards Dowards Dowards Dowards Dowards Dowards Dowards	Vame	Type Start of Authority (SOA) Name Server (NS) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A)	Data [47], Ibdc.Ib.com, hostma [bdc.Ib.com. 10.63.32.82 10.63.32.82 10.63.32.60 10.63.32.55 10.63.32.55 10.63.32.68 10.63.32.91 10.63.32.215	Timestamp static static 11/19/2020 2:00:00 AM static 11/19/2020 11:00:00 PM 11/19/2020 2:00:00 AM 11/19/2020 2:00:00 AM 11/23/2020 2:00:00 AM		

On each Session Recording server, run the powershell.exe -file SrServerConfigurationSyn .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 exam-

ple:

🐉 Session Recording Agent P	roperties	-		×
Recording Connections				
Session Recording Server:	NetScaler.lb.com			
Session Recording Storage M	lanager message que	Je		
Protocol:	HTTP ~			
HTTP/HTTPS port:	Default \vee			
Port Number:	80			
Message life specifies the p message queue. Message life (seconds):	eriod during which d	ata remains	in the	
Session Recording Broker				
Protocol:	HTTPS ~			
HTTP/HTTPS port:	Custom ~			
Port Number:	443			
	ОК	Cancel	Ap	ply

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:

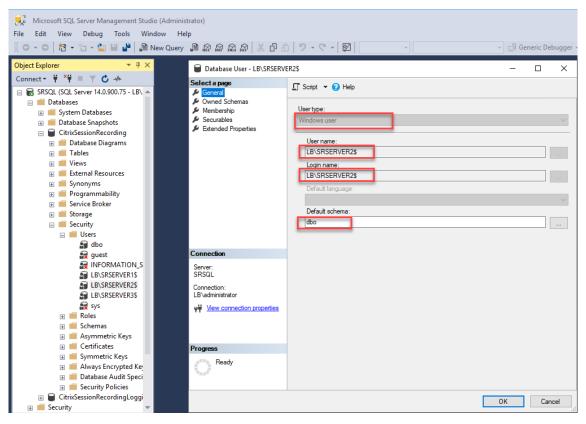
The Session Recording administrator logging is an optional subfeature of the Session Recording server. Select the Session Recording server before you can select the Session Recording administrator logging. The Session Recording database is a mandatory subfeature of the Session Recording server. When the Session Recording server is selected for installation, the Session Recording database is also selected automatically and cannot be unselected.

Core Components Features Core Components Features Citrix Session Recording Policy Console Citrix Session Recording Policy Console Summary Summary Install Finish Session Recording Broker and Storage Management. Session Recording Administrator Logging		Features
	Database and Server Summary Install	Session Recording Policy Console Citrix Session Recording Policy Console Citrix Session Recording Policy Console Session Recording Broker and Storage Management. Session Recording Administrator Logging Administrator Logging captures Session Recording Database. Session Recording Database

2. Use the same database names as the existing Session Recording server. For example:

	Administrator Logging Configuration
Licensing Agreement	Specify Session Recording logging configuration
Core Components	Configuration
 Features Database and Server 	The Administrator Logging database is installed on the SQL Server instance:
Administrator Logging	SRSQL
Summary Install Finish	Administrator Logging database name: CitrixSessionRecordingLogging Test connection
	 Enable Administrator togging This option enables the Session Recording Administrator Logging service. Enable mandatory blocking This option blocks policy and server property changes if logging fails.
	Back Next Cance

- 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:



🗑 Database User - LB\SRSERV	R2\$	_		×
Select a page General	🖵 Script 🔻 😮 Help			
 Øwned Schemas Membership Securables Extended Properties 	Database role membership: Role Members db_accessadmin db_backupoperator db_datareader db_datawriter db_ddladmin db_denydatareader db_denydatareader db_denydatareader db_denydatareader db_denydatareader db_denydatareader db_securityadmin			
Connection				
Server: SRSQL Connection: LB\administrator v# <u>View connection properties</u>				
Progress				
Ready				
		ОК	Can	cel

- 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 (100	0)			
Dashboard	Configurati	ion Reporting	Documentation	Downloads	
Q Search in Menu		Traffic Management / Lo	ad Balancing / Servers		
System AppExpert	>	Servers 2			
Traffic Management	\sim	Add Edit Del	ete Rename	Select Action \checkmark	
Load Balancing Virtual Servers	~	Q Click here to search or	you can enter Key : Value fo	rmat	
Services		NAME		STATE	IPADDRESS / DOMAIN
Service Groups		(i) 💬 👘 srv-1		ENABLED	10.63.32.55
Monitors		srv-2		ENABLED	10.63.32.74
Metric Tables		Total 2			
☆ Servers					
Persistency Group	s				
Radius Nodes					

	(1000))					
Dashboard Conf	figuratio	n Reporti	ng Documentation	Downloads			
Q Search in Menu	1	Traffic Managemen	t / Load Balancing / Services /	Services			
System AppExpert	> (Services					
Traffic Management	\sim	Services (8)	Auto Detected Services 0	Internal Services 6			
Load Balancing Virtual Servers	~	Add Edit	Delete Rename Stat	istics No action V			
☆ Services		Q Click here to se	arch or you can enter Key : Value for	nat			
Service Groups		N	AME	♦ SERVER STATE	IP ADDRESS/DOMAIN NAME	PORT 0	PROTOCOL
Monitors		SI	rv-1-80	• UP	10.63.32.55	80	TCP
Metric Tables		SI	rv-1-443	• UP	10.63.32.55	443	TCP
Servers		s	rv-1-1801	● UP	10.63.32.55	1801	TCP
Persistency Groups		SI	rv-1-22334	• UP	10.63.32.55	22334	TCP
Radius Nodes		SI	rv-2-443	• UP	10.63.32.74	443	TCP
Priority Load Balancing	• >	SI	rv-2-80	• UP	10.63.32.74	80	TCP
Content Switching	• >	SI	rv-2-1801	• UP	10.63.32.74	1801	TCP
Cache Redirection	• >	SI	rv-2-22334	• UP	10.63.32.74	22334	TCP
DNS	>	Total 8					
GSLB	• >						
SSL	>						
Subscriber	>						
Service Chaining	>						

>

User

Dashboard Co	onfiguration	Reporting	Documentation	Downloads		
Search in Menu	Traffic	Management / Load	Balancing / Virtual Serve	rs		
System AppExpert	> Virt	ual Server	S 4			
Traffic Management	~ Add	Edit Delet	e Enable Disable	Rename S	tatistics Select Acti	on 🗸
Load Balancing	~ Q CI	ick here to search or yo	u can enter Key : Value form	at		
Services		NAME		STATE	EFFECTIVE STATE	IP ADDRESS
Service Groups		vsrv-80		• UP	● UP	10.63.32.60
Monitors		vsrv-1801		• UP	• UP	10.63.32.60
Metric Tables	_	vsrv-443		• UP	• UP	10.63.32.60
Servers		vsrv-22334		• UP	• UP	10.63.32.60
Persistency Groups	Total	4				
Radius Nodes						
Priority Load Balancing	<u> </u>					
Content Switching	<u> </u>					
Cache Redirection	<u></u> >					
DNS	>					
GSLB	•					
SSL	>					
Subscriber	>					
Service Chaining	>					
User	>					
Optimization	>					

Dashboard Configuration Reporting	Documentation Downloads
Load Balancing Virtual Server	Load Balancing Virtual Server Service Binding
	Add Binding Edit Binding Unbind Edit Service Bound Monitors No action
	SERVICE NAME
	srv-2-22334 10.63.32.55 22334 TCP
	Close
Services and Service Groups	
Services and Service Groups 2 Load Balancing Virtual Server Service Bindings No Load Balancing Virtual Server ServiceGroup Binding	
2 Load Balancing Virtual Server Service Bindings	
2 Load Balancing Virtual Server Service Bindings No Load Balancing Virtual Server ServiceGroup Binding	

- 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. For more information, see Knowledge Center article CTX248554.
- 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

September 10, 2024

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.

▲ Create storage account - Microsc × +		
\leftrightarrow \rightarrow C $($ portal.azure.com/#create/Microso	ft.StorageAccount	
E Microsoft Azure	 Search resources, services, and docs (G+/) 	
Home > Storage accounts >		
Create storage account		
redundant. Azure Storage includes Azure Blo	bbs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azu pends on the usage and the options you choose below.	re
Project details		
Select the subscription to manage deployed your resources.	resources and costs. Use resource groups like folders to organize and manage a	11
Subscription *	cse-dev-03-ca	
Resource group *	~	/
	Create new	
Instance details		
The default deployment model is Resource to using the classic deployment model instead.	Vanager, which supports the latest Azure features. You may choose to deploy . Choose classic deployment model	
Storage account name * ①		
Location *	(US) East US	·
Performance ①	● Standard 🔿 Premium	
Account kind ①	StorageV2 (general purpose v2)	
Replication ①	Read-access geo-redundant storage (RA-GRS)	/
Review + create	< Previous Next : Networking >	

2. Navigate to your new storage account and select **Containers** in the **Blob service** section to create a container.

\equiv Microsoft Azure	, >>> Search resources, services, and docs (G+/)			🗳 🏟 ? 😊 📕
Home > 1				
Storage account	ainers 🖈 …			
Search (Ctrl+/) Access Keys		Restore containers 🗸 💍 Refresh 🛛 🔟 Delete		
Access keys Geo-replication	Search containers by prefix		(Show deleted containers
S CORS	Name	Last modified	Public access level	Lease state
Configuration	You don't have any containers yet. Click '+ Cont	tainer' to get started.		
🔒 Encryption				
Shared access signature				
👸 Networking				
Security				
📧 Static website				
Properties				
🔒 Locks				
Blob service				
🔤 Custom domain				
💎 Data protection				
Object replication				
📥 Azure CDN				
🗠 Add Azure Search				

3. Upload the Citrix Virtual Apps and Desktops installer to the container.

≡ Microsoft Azure	𝒫 Search	resources, services, and docs (C	ŝ+/)		D <table-cell></table-cell>	P 🔅	? 🙂		
Home > yuchunjstg1 >							Upload	blob	×
Container							yuchunblob/		
							Files 🛈		
Search (Ctrl+/)	«	🚹 Upload 💾 Change a	ccess level 💍 Refresh 🕴 🗓] Delete │ ⇄ Change	tier Ø Acquir	e lease 🖉	"Citrix_Virtua	al_Apps_and_Desktops	6
Overview			cess key (Switch to Azure AD Us	er Account)			Overwrite	e if files already exist	
Access Control (IAM)		Location: yuchunblob					✓ Advance	od	
Settings		Search blobs by prefix (case	-sensitive)			(✓ Auvance	.eu	
 Shared access signature 		Name	Modified	Access tier	Blob type	Size			
Access policy		No results					Upload		
Properties									
 Metadata 									

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.

Microsoft Azure	\mathcal{P} Search resources, services, and docs (G+/)	
services > Virtual machines >		
reate a virtual mac	hine	
elect the subscription to manage de our resources.	ployed resources and costs. Use resource groups like folders to or	ganize and manage all
Subscription * 🕕	cse-dev-03-ca	\checkmark
Resource group * 🛈	(New) Resource group	\checkmark
	Create new	
nstance details		
/irtual machine name * 🕕		
Region * 🕕	(US) East US	\sim
Availability options 🕕	No infrastructure redundancy required	\sim
mage * 🕕	Windows Server 2019 Datacenter - Gen1	\sim
	See all images	
Azure Spot instance ①		
iize * 🕕	Standard_D4s_v3 - 4 vcpus, 16 GiB memory (\$83.22/month	
	See all sizes	· ·
Administrator account		

Step 4: Remote desktop and download the Citrix Virtual Apps and Desktops installer to the Azure VMs

Microsoft Azure	>>> Search resources, services, and docs (G+/)			D 🗣	🗳 🐵 ?	©
ome > ···	≪ ↑ Upload 🔒 Change access level 🖒 Refresh 🗊 Delete		. đ			
9 Search (Ctrl+/) Overview Access Control (IAM)	Authentication method: Access key (Switch to Azure AD User Account Location: yuchunblob		re lease of Break lease			
ttings	Search blobs by prefix (case-sensitive)			•	Show delete	d blobs
Shared access signature	Name	Modified	Access tier	Blob type	Size	Lease state
Access policy	Citrix_Virtual_Apps_and_Desktops_7_2012.iso	3/4/2021, 6:37:47 PM	Hot (Inferred)	Block blob	4 B	🖉 View/edit
Properties						↓ Download
Metadata						2 Properties
						Cenerate SAS
						 View previous versions
						 View snapshots
						न Create snapshot
						💉 Acquire lease
						ග් Break lease
						Delete

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.

	Number of			Session	
	Recorded			Recording	Session
Recording File	Sessions Per	File Share	File Share	Server	Recording
Size MB/hour	Day	Туре	Quota (TB)	Quantity	Server Size
< 6.37	< 1,000	HDD Standard	2	1	Standard
		(StorageV2)			D4as_v4
< 6.37	1,000–2,000	SSD Premium	3	1	Standard
					D4as v4

	Number of			Session	
	Recorded			Recording	Session
Recording File	Sessions Per	File Share	File Share	Server	Recording
Size MB/hour	Day	Туре	Quota (TB)	Quantity	Server Size
< 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	3	1	Standard
		(StorageV2)			D4as_v4
Approx.10	1,000–2,500	SSD Premium	6	1	Standard
					D4as_v4
pprox.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.

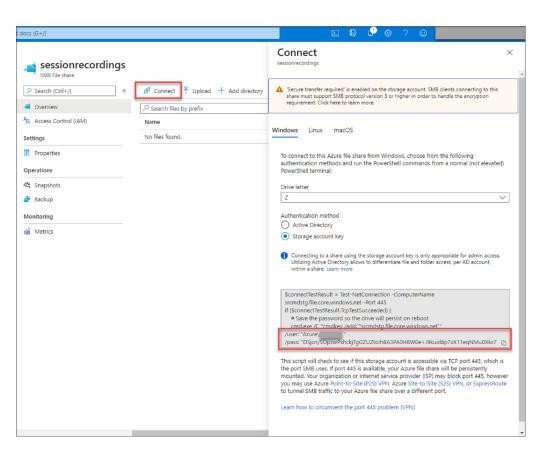
b) Run the SsRecUtils.exe -AddAzureFiles <storageAccountName> <fileShareName> <accesskey> command.

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.

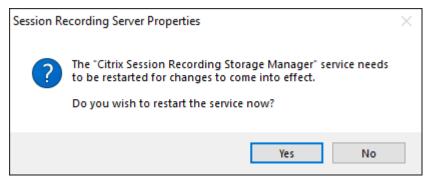
	𝒫 Search resources, services, and docs (G+/)
Home > srcmd >	
Storage account	eys
Search (Ctrl+/) « Overview	Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys so that you can maintain connections using one key while regenerating the other.
Activity log	When you regenerate your access keys, you must update any Azure resources and applications that access this storage acc
🗳 Tags	Storage account name srcmdstg
 Diagnose and solve problems Access Control (IAM) 	Hide keys
💕 Data migration	key1 💭 Key
Storage Explorer (preview)	Ney DSjcn/SOpzwPxhckjTgGZUZtolh8A3PA0H8W0e+J9kuid6p7xX11eqNMu0Xkx7R352f2GHRFU2PlIFi11vbE/A==
Settings	Connection string
📍 Access keys	DefaultEndpointsProtocol=https;AccountName=;AccountKey=DSjcn/SOpzwPxhckjTgGZUZtolh8A3PA0H8W0e+_
S CORS	key2 🗘
Encryption	Key O97VNcAmv+WpgFYYO6r3OffMyaD20sSGGpJuBgfkDYv3Z27j19TYOMbWFaz1N6riO81c2qF5JZOQVxqydmysO2A==
Shared access signature	Connection string
👻 Networking	DefaultEndpointsProtocol=https:/AccountName= AccountKey=O97VNcAmv+WpgFYYO6r3OfMyaD20sSGGpJuB
Security	
Properties	
🔒 Locks	
File service	
🛋 File shares	
Monitoring	
Insights	
Alerts	

- 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 \<filesshare

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

Storage	Signing	Rollover	Playback	Notifications	CEIP	Logging	RI • •	
	d-balance			ne directories ultiple directo				
File sto	orage direc	tories:					_	
Т	he default	folder C:\		pty. cordings will	be	Add Modify	_	
			used.		i	Remov	/e	File Storage Directory Enter a directory for storing recorded session files:
								unt.file.co/e.windows.net\sessionrecording\recordings Brow
Specify them a	v a folder ti vailable fo	o temporar r playback	rily store ar	chived sessi	on recordir	ngs and m	ake	OK Can
Restor	e directory	for archiv	ed files:					
C:\Ses	sionRecor	dingsResto	ored			Browse		
				ОК	Cancel		Apply	

- 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.

Microsoft Azure		₽ citrix ADC		X] 🕞 🗳 🎯 ?
		Services	Marketplace	See all	
	Rece Name	😝 LiveArena Broadcast	🙆 Citrix ADC		
		Resources	🐴 Citrix ADC 13.0 - Azure Stack		at Viewed
	🚍 yu	No results were found.	Citrix ADC 12.1		ew seconds ago
	() yu		👌 Citrix ADC VPX FIPS		ew seconds ago
			Documentation	See all	
	📰 yu 🗇 SR 🔇 SR		Tutorial: Azure Active Directory single sign-on		minutes ago
	SR		Tutorial: Azure Active Directory integration with Citrix		minutes ago
			Azure AD secure hybrid access Microsoft Docs		ay ago
	<↔> SR			ay ago	
	💌 srt		Resource Groups		ay ago
	🚸 LB		No results were found.		veeks ago
	as Didn't find what you were looking for?		veeks ago		
	🧐 sra	Try searching in Activity Log			veeks ago
	VY Vy			nonth ago	
	💌 lin	Searching all subscriptions. Change			nonth ago
	Navig ?	ate	os 🖬 All resources 🛛	Dashbo	pard

2. Choose the **Citrix ADC VPX Bring Your Own License** plan and then click **Create**.

		Σ	Ŗ	. ч ча	
Home⇒ Citrix ADC 🛷 …					
Citrix					
Citrix	ADC 👳 Add to Favorites				
citrix_ citrix	☆ 0.0 (0 ratings)				
Azure be	nefit eligible (3°				
Select a pla	n Citrix ADC VPX Bring Your Own License 🗸 Create				
	Information + Support Reviews				
Overview Plans Usage					
Overview Plans Usage	momaton + support interiews				
Citrix ADC is an enterprise-grac	 Je application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to				
Citrix ADC is an enterprise-grac					
Citrix ADC is an enterprise-grac meet your business' unique nee	 Je application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to				
Citrix ADC is an enterprise-grac meet your business' unique nee Why Citrix?	te application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to eds. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud.				
Citrix ADC is an enterprise-grac meet your business' unique nee Why Citrix? Citrix ADC offers high performa	 Je application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to				
Citrix ADC is an enterprise-grac meet your business' unique net Why Citrix? Citrix ADC offers high perform applications across cloud or hyl step of the way.	te application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to eds. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud.				
Clirki ADC is an enterprise-grac meet your business' unique nee Why Clirki? Clirki ADC offers high performs applications across cloud or hyl step of the way. Key Benefits:	te application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to eds. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud. Ince with fast application development delivery, a comprehensive centralization management system, and orchestration and automation for brid environments for greater agility. Citrix's all-in-one solution brings point solutions under one root, ensuring simplicity and security every				
Clitrix ADC is an enterprise-grac meet your business' unique neer Why Clitrix? Clitrix ADC offers high performa applications across cloud or hyl step of the way. Key Benefits: • Flexible & Consistent: capacity licensing option	te application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to eds. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud. Ince with fast application development delivery, a comprehensive centralization management system, and orchestration and automation for brid environments for greater agility. Citrix's all-in-one solution brings point solutions under one root, ensuring simplicity and security every Citrix ADC is the most comprehensive, feature-rich ADC available across a wide variety of deployment options with the most flexible pooled in the industry.				
Citrix ADC is an enterprise-grac meet your business' unique net Why Citrix? Citrix ADC offers high perform applications across cloud or hyl step of the way. Key Benefits: • Flexible & Consistent: capacity licensing optior • Best User Experience : users to the best source	te application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to ds. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud. Ince with fast application development delivery, a comprehensive centralization management system, and orchestration and automation for brid environments for greater agility. Citrix's all-in-one solution brings point solutions under one roof, ensuring simplicity and security every Citrix ADC is the most comprehensive, feature-rich ADC available across a wide variety of deployment options with the most flexible pooled in the industry. Citrix the only vendor to offer an intelligent, global load-balancing service that uses real-time internet traffic and data center health to route for their applications and content.				
Citrix ADC is an enterprise-grac meet your business' unique ner Why Citrix? Citrix ADC offers high performs applications across cloud or hyl step of the way. Key Benefits: • Flexible & Consistent: capacity licensing optior • Best User Experience users to the best source • Integrated App Security	e application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to ds. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud.				
Citrix ADC is an enterprise-grac meet your business' unique net Why Citrix? Citrix ADC offers high performa applications across cloud or hyl step of the way. Key Benefits: • Flexible & Consistent: capacity licensing option • Best User Experience: C users to the best source • Integrated App Securit Comprehensive applications	te application delivery controller that delivers your applications quickly, reliably, and securely, with the deployment and pricing flexibility to eds. Designed to provide operational consistency and a smooth user experience, Citrix ADC eases your transition to the hybrid cloud.				

4. Set VM configurations.

▲ Create Citrix ADC - Microsoft Az∪ × +	
← → C	etscalervpx-1vm-3nicnetscalervpx-1vm-3nic-byol
\equiv Microsoft Azure	Search resources, services, and docs (G+/)
Home > Citrix ADC >	
Create Citrix ADC	
▲ Changes on this step may reset later sel	ections you have made. Review all options prior to deployment.
Basics VM Configurations Netwo	ork and Additional Settings Review + create
Virtual Machine Configurations	
Virtual machine size * ①	1x Standard DS3 v2
	4 vcpus, 14 GB memory
	Change size
OS disk type ①	Premium_LRS
Assign Public IP (Management) 🕕	• Yes
Assign Public IP (Client traffic) 🕕	• Yes
Unique public IP domain name suffix * ①	d28e81a280 ✓
Azure Monitoring Metrics 🕕	Enabled Disabled
Backend Autoscale 🛈	Enabled Isabled
Review + create < Previous	Next : Network and Additional Settings >

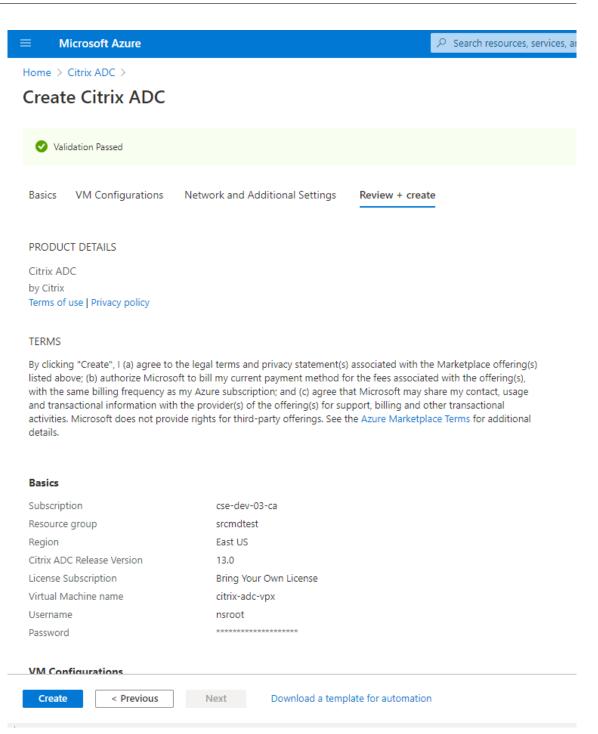
5. Check and modify network settings if necessary. Choose **ssh (22), http (80), https (443)** for public inbound ports.

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		$\mathcal P$ Search resources, services, an	d docs (G+/)
Home > Citrix ADC >			
Create Citrix ADC			
Configure virtual networks			1
Virtual network * 🕡	(new) citrix-adc-vpx-virtual-network Create new	\checkmark	
Management Subnet * 🛈	(new) 01-management-subnet (10.1.28.0/24)	\checkmark	
Client Subnet *	(new) 11-client-subnet (10.1.29.0/24)	\checkmark	
Server Subnet * 🛈	(new) 12-server-subnet (10.1.30.0/24)	\checkmark	
Public IP (Management)			I
Management Public IP (NSIP) * 🛈	(new) citrix-adc-vpx-nsip Create new	\checkmark	
Management Domain Name 🛈	citrix-adc-vpx-nsip-23f12ee6b2	~	
		.eastus.cloudapp.azure.com	
Public IP (Clientside)			
Clientside Public IP (VIP) * ()	(new) citrix-adc-vpx-vip	\checkmark	
Clientside Domain Name 🕕	Create new citrix-adc-vpx-vip-23f12ee6b2	<u> </u>	
		.eastus.cloudapp.azure.com	
Public Inbound Ports (Management of	aniv)		
Ports open for Management public IP ①			
	 ssh (22) ssh (22), http (80), https (443) 		
L			
Review + create < Previous	Next : Review + create >		

		$\mathcal P$ Search resources, services, and docs (
Home > Citrix ADC >		
Create Citrix ADC		
Basics VM Configurations Netwo	ork and Additional Settings Review + create	2
Boot diagnostics		
Diagnostic storage account * 🕕	(new) citrixadcvpxe42b4be259	\checkmark
	Create New	
Network Settings		
Configure virtual networks		
Virtual network * 🕕	(new) citrix-adc-vpx-virtual-network	\checkmark
	Create new	
Management Subnet * 🔋	(new) 01-management-subnet (10.1.32.0/24)	\checkmark
Client Subnet * 🥡	(new) 11-client-subnet (10.1.33.0/24)	\checkmark
Server Subnet * 🛈	(new) 12-server-subnet (10.1.34.0/24)	\checkmark
A sector to d Nature data a		
Accelerated Networking	On	
Accelerated Networking (Management Interface) ③	O off	
Accelerated Networking (Client Interface)	On Off	
Accelerated Networking (Server Interface) ()	On Off	
-		
Public IP (Management)		
Management Public IP (NSIP) * 🛈	(new) citrix-adc-vpx-nsip	\sim
	Croate new	
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.

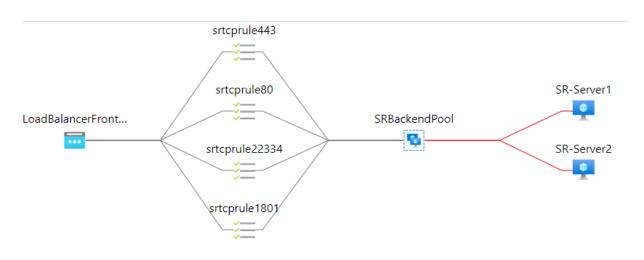
- a) Stop the citrix-adc-vpx virtual machine.
- b) Change the subnet of the VIP address.

■ Microsoft Azure			فر	adc	
ome > srlb > citrix-adc-vpx-nic	11				
🚽 citrix-adc-vpx-n	ic11 IP conf	igurations			
Network interface					
Search (Ctrl+/)	« 🕂 Add [🖫 Save 🗙 Disc	ard 🕐 Refresh		
Verview	IP forwardin	ig settings			
Activity log	IP forwarding	9			Disabled Enabled
Access control (IAM)	Virtual netwo	ork			srazureautovnet
Tags	IP configura	tions			
ettings	Subnet				srazureautosubnet2 (192.168.2.0/24)
IP configurations					
DNS servers					
Network security group	1 The as	sociated virtual mach	nine 'citrix-adc-vpx' mi	ust be either stopped or deallocated in	order to be able to edit the subnet.
Properties	O count in				
Locks	Name	P configurations	Type	Private IP address	Public IP address
utomation			Туре		
Tasks (preview)	vip	IPv4	Primary	192.168.2.4 (Dynamic)	Unassigned (citrix-adc-vpx-vip) ***
Export template					
upport + troubleshooting					
Effective security rules					
Effective security rules Effective routes New support request					
 Effective security rules Effective routes New support request Microsoft Azure 	_		,∕⊃ adc		
Effective security rules Effective routes New support request Microsoft Azure ome > srlb > citrix-adc-vpx-nic11	11 LD configu	wations	,₽ adc		
 Effective security rules Effective routes New support request Microsoft Azure 	11 IP configu	urations	₽ adc		
Effective security rules Effective routes New support request Microsoft Azure ome > srlb > citrix-adc-vpx-nic11 citrix-adc-vpx-nic2 Network interface	11 IP configu	-	오 adc		
Effective security rules Effective routes Merrosoft Azure Microsoft Azure me > srlb > citrix-adc-vpx-nic11 citrix-adc-vpx-nic2 Network interface > Search (Ctrl+/)		-			
Effective security rules Effective routes Merrosoft Azure Microsoft Azure me > srlb > citrix-adc-vpx-nic11 citrix-adc-vpx-nic2 Network interface > Search (Ctrl+/)	< + Add 🗔 s	Save X Discard	🕐 Refresh	e will be restarted to utilize the new subn	et.
Effective security rules Effective routes Ketwork request Microsoft Azure Microsoft Azure citrix-adc-vpx-nic1 citrix-adc-vpx-nic1 citrix-adc-vpx-nic2 Network interface Search (Ctrl+/) Verview Activity log	< + Add 🗔 s	Save X Discard	🕐 Refresh	e will be restarted to utilize the new subm	et
Effective security rules Effective routes New support request Microsoft Azure met > srlb > citrix-adc-vpx-nic1 citrix-adc-vpx-nic1 Network interface > search (Ctrl+/) « Overview Activity log Access control (IAM)	Add S S	ave X Discard	🕐 Refresh	_	
Effective security rules Effective routes Microsoft Azure Microsoft Azure Microsoft Azure Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic Network interface Search (ctrl+/) Cverview Activity log Access control (IAM) Tags	Add 🔚 S	ave X Discard	🕐 Refresh	e will be restarted to utilize the new subm	
Effective security rules Effective routes Ketwork interface Search (Ctrl+/) Overview Activity log Access control (IAM) Tags Effective security rules Effective routes Effective routes Microsoft Azure	Add S S	ave X Discard	🕐 Refresh	Disab	
	Add 🔄 s	Discard with associated with things	🕐 Refresh	Disab	ied Enabled
Effective security rules Effective routes Ketwork interface Search (Ctrl+/) Coverview Activity log Access control (IAM) Tags ttings P configurations Effective routes Effective routes Coverview Co	Add S S The virtual a IP forwarding set IP forwarding Virtual network	Discard with associated with things	🕐 Refresh	Disat srazu	ied Enabled
Effective security rules Effective routes Effective routes Microsoft Azure Microsoft Azure Come > srlb > citrix-adc-vpx-nic1 Ci	 Add s The virtual a IP forwarding set IP forwarding Virtual network IP configurations Subnet * 	Tave Discard	🕐 Refresh	Disat srazu	reautovnet
Effective security rules Effective routes Ffective routes Microsoft Azure Microsoft Azure Microsoft Azure Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Coverview Activity log Access control (IAM) Tags Titings Ponfigurations DNS servers Network security group Properties	 Add S S A The virtual a IP forwarding set IP forwarding Virtual network IP configurations 	Tings	Refresh th this network interface	Disab srazur Srazur	reautovnet
Effective security rules Effective routes Iffective route	 Add s The virtual The virtual IP forwarding set IP forwarding Virtual network IP configurations Subnet * 	Tigurations IP Version Ty	🕐 Refresh	Dicab srazu srazu Private IP address	reautovnet reautosubnet (192.168.1.0/24)
Effective security rules Effective routes Effective routes Microsoft Azure Microsoft Azure me Sufb > citrix-adc-vpx-nic1 citrix-ad	 Add S s A The virtual a IP forwarding set IP forwarding Virtual network IP configurations Subnet * Search IP con Name 	Tigurations IP Version Ty	C Refresh	Dicab srazu srazu Private IP address	reautovnet reautosubnet (192.168.1.0/24) Public IP address
Effective security rules Effective routes Effective routes Microsoft Azure microsoft Azure microsoft Azure microsoft Azure microsoft Azure microsoft Azure microsoft Azure microsoft Azure microsoft Azure microsoft	 Add S s A The virtual a IP forwarding set IP forwarding Virtual network IP configurations Subnet * Search IP con Name 	Tigurations IP Version Ty	C Refresh	Dicab srazu srazu Private IP address	reautovnet reautosubnet (192.168.1.0/24) Public IP address
Effective security rules Effective routes Effective routes Effective routes Microsoft Azure Microsoft Azure metabolic security rules intra-adc-vpx-nic1 citrix-a	 Add S s A The virtual a IP forwarding set IP forwarding Virtual network IP configurations Subnet * Search IP con Name 	Tigurations IP Version Ty	C Refresh	Dicab srazu srazu Private IP address	reautovnet reautosubnet (192.168.1.0/24) Public IP address
Effective security rules Effective routes Effective routes Microsoft Azure Microsoft Azure Microsoft Azure Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Overview Activity log Access control (IAM) Tags I P configurations I PNS servers Network security group Properties Locks tomation Tasks (preview) Export template pport + troubleshooting Effective routes Effective routes Effective routes Effective routes Effective routes Microsoft Azure Microsoft Azure Microsoft Azure Microsoft Azure Microsoft Azure Citrix-adc-vpx-nic1 Microsoft Azure Second (IAM) Tags Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Citrix-adc-vpx-nic1 Properties Locks Citrix-adc-vpx-nic1 Citrix-adc-vpx-n	 Add S s A The virtual a IP forwarding set IP forwarding Virtual network IP configurations Subnet * Search IP con Name 	Tigurations IP Version Ty	C Refresh	Dicab srazu srazu Private IP address	reautovnet reautosubnet (192.168.1.0/24) Public IP address
Effective security rules Effective routes Keffective routes New support request Microsoft Azure come > srlb > citrix-adc-vpx-nic1 citrix-adc-vpx-nic1 citrix-adc-vpx-nic1 vetwork interface Search (Ctrl+/) Vetwork interface Search (Ctrl+/) Vetwork interface Activity log Access control (IAM) Tags Poonfigurations DNS servers	 Add S s A The virtual a IP forwarding set IP forwarding Virtual network IP configurations Subnet * Search IP con Name 	Tigurations IP Version Ty	C Refresh	Dicab srazu srazu Private IP address	reautovnet reautosubnet (192.168.1.0/24) Public IP 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**.

crosoft Azure	ho load balancer	× 🛛 🗣 🗘 🔅	? ©	Yuchun.Jiang@citrix.com
Azure servic	Services See all	Marketplace	See all	
Create a resource		Load Balancer / ADC aiScaler Load Balancer & Site Acceleration ishlangu Load Balancer ADC IS-5000 (5Gbps)		More services
Recent resou	CloudAMQP CloudAMQP CloudAMQF CloudAMQF CloudAMQF CloudAmix Workload Insights	Documentation Load Balancer Microsoft Docs What is Azure Load Balancer? - Azure Load Balancer Azure Load Balancer concepts Microsoft Docs	See all	
SRAppGV1	CloudSimple Nodes CloudSimple Services Resources	Quickstart: Create a public load balancer - Azure portal Resource Groups		,
 ♦ SRLoadBalan ♦ SRVnet 	No results were found.	No results were found.		
 srtest LB-hubtest-T asfazuretests 	Dicht find what you were looking for? Try searching in Activity Log Try searching in Azure Active Directory			
💓 srazureauto	Searching all subscriptions. Change			
↔ VNet-hubtest	Virtual	network a	a month ago	

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.
Туре	Select Internal.
SKU	Select Standard

Setting	Value
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 .

	s, or internal where it is only accessible from a virtual network. Azure on (NAT) to route traffic between public and private IP addresses. Le	
Project details		
Subscription *	cse-dev-03-ca	\checkmark
Resource group *	srlbtest Create new	\checkmark
Instance details		
Name *	SRLoadBalance	~
Region *	(US) East US	\checkmark
Type * 🕡	Internal Public	
SKU * 🕡	 Basic Standard Standard Load Balancer is secure by default. This means Groups (NSGs) are used to explicitly permit and whitelist do not have an NSG on a subnet or NIC of your virtual m traffic is not allowed to reach this resource. Please config communication if needed. For outbound communication outbound rule is needed. Learn more about outbound component 	t allowed traffic. If you nachine resource, gure an NSG to ensure n, an explicit
Configure virtual network.		
Virtual network * 🕡	srazureautovnet	\sim
Subnet *	srazureautosubnet (192.168.1.0/24) Manage subnet configuration	\checkmark
IP address assignment *	🔵 Static 💿 Dynamic	
Availability zone * 🕕	Zone-redundant	\sim

- 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.

		$\mathcal P$ Search resources, services, and docs (G	+/)	
Home > SRLoadBalance				
SRLoadBalance Bac	kend pools			
	+ Add 💍 Refresh			
Overview				
Activity log	Backend pool	Virtual machine	Virtual machine status	Network interface
Access control (IAM)	No results			
🗳 Tags				
Diagnose and solve problems				
Settings				
Frontend IP configuration				
Backend pools				
Health probes				
≆ Load balancing rules				
Inbound NAT rules				
Properties				
🔒 Locks				
Monitoring				
Alerts				
mi Metrics				
Insights				
Automation				
🖧 Tasks (preview)				
Export template				

Enter a name for the new back-end pool and then click **Add**.

■ Microsoft Azure		$\mathcal P$ Search resources, services,
Home > SRLoadBalance > Add backend pool SRLoadBalance		
Name * Virtual network () IP version	SRBackendPool srazureautovnet (sribtest) IPv4 IPv6	~
All IP configurations must be on the sam	e virtual network.	onfiguration or no public IP configuration.
Virtual machine ↑↓ No virtual machines selected	IP Configuration ↑↓	Availability set ↑↓
	me location as Load Balancer. Only IP conf n be selected. All of the IP configurations h	
1 No virtual machine scale set is found	d in eastus that matches the above criteria	

Add

• Add health probes.

Select the load balancer you created from the resources list and then click **Health probes** in the left navigation.

E Microsoft Azure		
Iome > SRLoadBalance		
SRLoadBalance Health probes		
Overview Overview Search probes		
Activity log Name	↑↓ Protocol	↑↓ Port
Access control (IAM) No results.		
Tags		
Diagnose and solve problems		
Settings		
Frontend IP configuration		
Backend pools		
🕐 Health probes		
E Load balancing rules		
Inbound NAT rules		
Properties		
Locks		
Monitoring		
Alerts		
Metrics		
Insights		
Automation		
🔓 Tasks (preview)		
🛃 Export template		
upport + troubleshooting		

Click Add to add health probes on ports 80, 22334, 1801, and 443.

Microsoft Azure	🔎 Search resources, services, and docs (G+/) 💿 💀 🚱 ? 😳				
Home > SRLoadBalance					
SRLoadBalance	Health probes				
✓ Search (Ctrl+/)	« 🕂 Add 💍 Refresh				
Settings	Filter by name				
Frontend IP configuration	Name	Protocol	Port	Used By	
Backend pools	SRHealthProbe1801	TCP	1801	SRTCPRule1801	
Health probes	SRHealthProbe22334	TCP	22334	SRTCPRule22334	
Load balancing rules	SRHealthProbe443	TCP	443	SRTCPRule443	
Inbound NAT rules	SRHealthProbe80	TCP	80	SRTCPRule80	
Properties					
Locks					
Monitoring					
Diagnostic settings					
📍 Logs					
Alerts					
d Metrics					
Insights					
Automation	1				
Tasks (preview)					
Export template					

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.

	${\cal P}$ Search resources, services, and docs (G+/)
Home > SRLoadBalance >	
SRHealthProbe SRLoadBalance	
🔚 Save 🗙 Discard 直 Delete	
Name *	
SRHealthProbe80	\checkmark
Protocol (i)	
тср	\sim
Port* ①	
80	
Interval * ① 5	
5	seconds
Unhealthy threshold * ①	
2	
cons	ecutive failures
Used by ①	
Not used	

• 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.

■ Microsoft Azure		${\cal P}$ Search resources, services, and docs (G+/)
Home > SRLoadBalance		
SRLoadBalance Loa	d balancing rules	
P Search (Ctrl+/) ≪	+ Add	
💠 Overview	✓ Search load balancing rules	
Activity log	Name	↑↓ Load balancing rule
Access control (IAM)	No results.	
🗳 Tags		
Diagnose and solve problems		
Settings		
Frontend IP configuration		
Backend pools		
Health probes		
š≡ Load balancing rules		
🕌 Inbound NAT rules		
Properties		
🔒 Locks		
Monitoring		
Alerts		
Metrics		
Insights		
Automation		
📇 Tasks (preview)		
😫 Export template		
Support + troubleshooting		

Click **Add** to add load balancing rules for ports 80, 22334, 1801, and 443.

■ Microsoft Azure		D Search resources, services, and docs (G	+/)				🗆 🛛 🖗 🖉 🎯 ? 💿	
Home > SRLoadBalance								
	Loa	d balancing rules 🦷						×
	«	+ Add						
Settings	^							
Frontend IP configuration		Name	↑↓	Load balancing rule	↑↓	Backend pool	1↓ Health probe	↑↓
Backend pools		SRTCPRule1801		SRTCPRule1801 (TCP/1801)		SRBackendPool	SRHealthProbe1801	
Health probes	11	SRTCPRule22334		SRTCPRule22334 (TCP/22334)		SRBackendPool	SRHealthProbe22334	
		SRTCPRule443		SRTCPRule443 (TCP/443)		SRBackendPool	SRHealthProbe443	
Inbound NAT rules	п.	SRTCPRule80		SRTCPRule80 (TCP/80)		SRBackendPool	SRHealthProbe80	
Properties								
🔒 Locks								
Monitoring								
Diagnostic settings								
🗭 Logs								
Alerts								
Metrics								
Insights								
Automation								
🔓 Tasks (preview)								
Export template								

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.

■ Microsoft Azure	${\cal P}$ Search resources, services, and docs (G+/)
Home > SRLoadBalance >	
Add load balancing rule	
SRLoadBalance	
Name *	
SRTCPRule80	
IP Version *	
● IPv4 ○ IPv6	
Frontend IP address * 🕕	
192.168.1.23 (LoadBalancerFrontEnd)	~
HA Ports 🗊	
Protocol	
● TCP ○ UDP	
Port *	
80	\checkmark
Backend port * ①	
80	\checkmark
Backend pool ①	
SRBackendPool	~
Health probe ① SRHealthProbe80 (TCP:80)	~
	V
Session persistence ① Client IP	~
Idle timeout (minutes) ①	4
TCP reset Disabled Enabled	
Floating IP	
ок	

• Add the Azure VMs where the Session Recording server is installed to the back-end pool.

		ices and docs (G+A
	y - Scaler resources, serv	
Home > SRLoadBalance		
SRLoadBalance Backend po	ols	
) Refresh	
Overview		
Activity log Backend po	ol Virtual machine	Virtual machine status
Access control (IAM)	ndPool	
Tags		
Diagnose and solve problems		
Settings		
Frontend IP configuration		
Backend pools		
P Health probes		
ž≡ Load balancing rules		
Inbound NAT rules		
Properties		
🔒 Locks		
Monitoring		
Alerts		
Microsoft Azure P Search resources, se	rvices, and docs (G+/)	N R 🗳 🕸 ? 💿
Home > <u>SRLoadBalance</u> >	Add virtual machines to backend pool	
SRBackendPool ··· SRDadBalnee		
IP Address	You can only attach virtual machines that are in the same location and on the same virtual network a Virtual machines must have a standard SKU public IP or no public IP.	s the loadbalancer.
IP Version		SRVnet Resource group == all Availability set == all
O IPv6	□ Virtual machine ↑↓ Resource group ↑↓ IP Configuration ↑↓ Availability set ↑↓ □ sr-server1 ipconfig1 (10.7.1.5) -	Tags Notes
Virtual machines	ipconfig1 (10.7.1.6)	
You can inscrime? You can only attach virtual machines in eastus that have a standard SKU public IP configuration or no pul All IP configurations must be on the same virtual network.		
+ Add X Remove		
Virtual machine ↑↓ IP Configuration ↑↓ Availability set ↑		
No virtual machines selected		
Virtual machine scale sets		
Virtual Machine Scale Sets must be in same location as Load Balancer. Only IP configurations that have th (Basic/Standard) as the Load Balancer can be selected. All of the IP configurations have to be in the same		
No virtual machine scale set is found in eastus that matches the above criteria		
Virtual machine scale set IP address		
Save Cancel		

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.

■ Microsoft Azure	و م
Home > srlbtest > SR-Server1-ip > sr-server172 >	
ipconfig1 sr-server172	
🖫 Save 🗙 Discard	
Public IP address settings	
Public IP address	
Disassociate Associate	
Public IP address *	
SR-Server1-ip (20.62.236.36)	\sim
Create new	
Private IP address settings	
Virtual network/subnet srazureautovnet/srazureautosubnet	
Assignment	
Dynamic Static	
IP address	
192.168.1.19	

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.

Home > SRAppGV1 > Edit backend pool

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machines scale sets, IP addresses, domain names, or an App Service.

Name		
AGbackendpool		
Add backend pool without targets		
Backend targets		
2 items		
Target type	Target	
IP address or FQDN	192.168.1.13	Ē ···
IP address or FQDN	192.168.1.18	<u>i</u>
IP address or FQDN	×]	

Associated rule SRHttpRule80 SRHttpRule443

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

	\mathcal{P} Search resources, services, and docs (G+/)		🖉 🎯 ?	Yuchun.Jiang@citrix.com crrex
Home > SRAppGV1 SRAppGV1 HTTP s	settings		Add HTTP setting		;
Search (Ctrl+/) « Access control (IAM)	+ Add		HTTP settings name SRHttpSetting80		
🔷 Tags	Name	Port	Backend protocol HTTP HTTPS		
Diagnose and solve problems	SRHttpSetting80	80	Parland and		
Settings	SRHttpSetting443	443	Backend port * 80		
Configuration	SRHttpSetting22334	22334			
Web application firewall			Additional settings		
🤨 Backend pools			Cookie-based affinity ① O Enable • Disable		
SE HTTP settings			Connection draining ①		
Frontend IP configurations			Connection draming () Enable O Disable		
🗄 Listeners			Request time-out (seconds) * ①		
📩 Rules			20		
Health probes			Override backend path ①		
Properties					
🔒 Locks			Host name		
Monitoring			By default, Application Gateway does not change the i		
💶 Alerts			unaltered to the backend. Multi-tenant services like Ap extension to resolve to the correct endpoint. Change t		
mi Metrics			Save Cancel		
Diagnostic settings			Cancer		

• 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).

■ Microsoft Azure	\mathcal{P} Search resources, services, and doc	s (G+/)	N 📭 🗳 🛞 ? 😊 🔜
Home > SRAppGV1	settings		Add HTTP setting
Application gateway Application gateway Application (Ctrl+/) « Access control (MMM) Access control (MMM) Access control (MMM)	+ Add Search HTTP settings Name	Port	HTTP settings name SRHttp:Setting443 Backend protocol O HTTP
Diagnose and solve problems Settings	SRHttpSetting80 SRHttpSetting443	80	Backend port *
 Configuration Web application firewall 	SRHttpSetting22334	22334	Backend authentication certificate
 Backend pools HTTP settings 			For end-to-end SSL encyption, the backend must be whitelisted with the application gateway. Upload the public certificate of the backend servers to this HTTP setting.
Frontend IP configurations			Ves No
Rules Health probes			Certificate srib ····
Properties			Add certificate Additional settings
Monitoring			Cookie-based difnity ⊙ ● Enable ◯ Disable
 Alerts Metrics Diagnostic settings 			Save Cancel

	♀ Search resources, services, and docs ((G+/)	2 6 9 0 0
Microsoft Axure Home > SRAppGV1 HTTP s SRAppGV1 HTTP s Accuse tourno (wm) Tags Diagnose and solve problems Settings Configuration Web application firewall Backend pools HTTP settings Itheres Itales Health probes Ith probes		Port 80 443 22334	▶ • P
 Alerts Metrics Diagnostic settings 			Save Cancel

• 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.

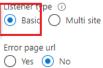
ome > SRAppGV1					
SRAppGV1 Front	end IP config	gurations			
Search (Ctrl+/) Access control (IAW)	/* bearen none	end IP configurations			
Tags	Туре	Status	Name	IP address	Associated listeners
Diagnose and solve problems	Public	Not configured			-
	Private	Configured	appGwPrivateFrontendIp	10.7.0.6	SRListener80, 2 more
ettings					
Configuration					
Web application firewall					
Backend pools					
HTTP settings					
Frontend IP configurations					
Elisteners					
Rules					
Health probes					
Properties					
Locks					
Aonitoring					
Alerts					
Metrics					

5. Add listeners.

Add listeners on ports 80, 443, and 22334, for example:

Home > SRAppGV1						
SRAppGV1 Liste	ners					
Application gateway	illers					
Search (Ctrl+/)	Add listener Add listener Refresh					
 Access control (IAIM) 						
Tags				litional configuration required to enable or appropriate backend pool as specified in a	disable WebSocket support. If a WebSocket tra pplication gateway rules.	ffic is received on the
Diagnose and solve problems	Learn more about listeners and WebS	Socket support. 🖒				
ettings	Name	Protocol	Port	Associated rule	Host name	
	SRListener80	HTTP	80	SRHttpRule80		
Configuration					· .	
Web application firewall	SRListener443	HTTPS	443	SRHttpRule443		
Backend pools	SRListener22334	HTTPS	22334	SRHttpRule22334		
HTTP settings	SSL Policy					
Frontend IP configurations		ol version and available ciphers.	Choose from one of the prede	fined policies or create a custom security po	licy to match your organizational security requ	irements.
Listeners	Learn more about SSL policy. Selected SSL Policy					
Rules	Default (change)					
Health probes	Min protocol version					
Properties	TLSv1_0					
Locks	Cipher suites					
	TLS_ECDHE_RSA_WITH_AES_256_GCM					
onitoring	TLS_ECDHE_RSA_WITH_AES_128_GCM TLS_ECDHE_RSA_WITH_AES_256_CBC					
Alerts	TLS_ECDHE_RSA_WITH_AES_230_CBC					
Metrics	TLS_ECDHE_RSA_WITH_AES_256_CBC					
Diagnostic settings	TLS ECDHE RSA WITH AES 128 CBC	SHA				
Listener	-			<i>P</i> Search re	esources, services, and doc	s (G+/)
Microsoft A						
	\					
	>					
ome > SRAppGV1						
ome > SRAppGV1						
ome > SRAppGV1						
ome > SRAppGV1						
ome > SRAppGV1 RListener8 RAppGV1						
ome > SRAppGV1 RListener8 AppGV1 stener name ①						
ome > SRAppGV1 RListener8						

Frontend IP * ①						
Private	~					
Port * 🛈						
80	✓					
Protocol 🛈						
HTTP HTTPS						
Associated rule						
SRHttpRule80						
Additional settings						



• 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.

Home > SRAppGV1 >	
SRAppGV1	
Listener name ① SRListener443	
Frontend IP * 🕕	
Private	\sim
Port * ①	
443	~
Protocol ⁽¹⁾ HTTP ⁽¹⁾ HTTPS	
Choose a certificate Create new Select existing	
Certificate *	
Ibdc	\sim
Renew or edit selected certificate	
Associated rule SRHttpRule443	
Additional settings	
Error page url Yes ONO	

• 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.

≡ Microsoft Azure	𝒫 Searce	h resource
Home > SRAppGV1 >		
SRListener22334 SRAppGV1		
Listener name 🛈		
SRListener22334		
Frontend IP * ()		
Private	\sim	
Port * (i)		
22334	~	
Protocol ① O HTTP HTTPS		
Choose a certificate O Create new O Select existing		
Certificate *		
Ibdc	\sim	
Renew or edit selected certificate		
Associated rule SRHttpRule22334		
Additional settings		
Listener type ① Basic O Multi site		
Error page url Ves No		

6. Create request routing rules.

Create rules for ports 80, 443, and 22334, for example:

Microsoft Azure	, P Search resources, services, and docs (G+/)		📃 🛛 🗣 🖨 🎯 ? C	
ome > <u>SRAppGV1</u>				
SRAppGV1 Rule	2S			
Search (Ctrl+/) Access control (IAM)	« + Request routing rule			
Tags	>> Search rules			
Diagnose and solve problems	Name	Туре	Listener	
tings	SRHttpRule80	Basic	SRListener80	
	SRHttpRule443	Basic	SRListener443	
Configuration	SRHttpRule22334	Basic	SRListener22334	
Web application firewall				
Backend pools				
HTTP settings				
Frontend IP configurations				
Listeners				
Rules				
Health probes				
Properties				
Locks				
nitoring				
Alerts				
Metrics				
Diagnostic settings				

• Routing rule for port 80

SRHttpRule80

SRAppGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name	SRHttpRule80					
Listener *Backend targets A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.						
Listener *	SRListener80 V					

SRHttpRule80

SRAppGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name	SRHttpRule80							
* Listener * Backend targets								
	Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.							
Target type 💿 Backend pool 🔘 Redirection								
Backend target * 🕡	AGbackendpool V							
HTTP settings * ①	SRHttpSetting80 V							

• Routing rule for port 443

SRHttpRule443 SRAppGV1 Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target. Rule name *Listener *Backend targets A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule. Listener *

SRHttpRule443

SRAppGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name	SRHttpRule443
* Listener * Backend targets	
Choose a backend pool to which this ro define the behavior of the routing rule.	outing rule will send traffic. You will also need to specify a set of HTTP settings that
Target type	Backend pool Redirection
Backend target * 🕡	AGbackendpool V
HTTP settings * 🗊	SRHttpSetting443

• Routing rule for port 22334

SRHttpRule2	2334
	to send traffic from a given frontend IP address to one or more backend targets. A routing rule must east one backend target.
Rule name	SRHttpRule22334
	argets specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, will apply this routing rule.
Listener *	SRListener22334 V

SRHttpRule22334

SRAppGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name	SRHttpRule22334
* Listener * Backend targets	
Choose a backend pool to which define the behavior of the routing	this routing rule will send traffic. You will also need to specify a set of HTTP settings that g rule.
Target type	Backend pool Redirection
Backend target * 🕕	AGbackendpool V
HTTP settings * 🕕	SRHttpSetting22334 V

- 7. Add the Azure VMs where the Session Recording server is installed to the back-end pool.
- 8. Configure Session Recording servers according to Knowledge Center article CTX230015.

Configure Group Service Managed Account (gMSA) support for Session Recording

September 14, 2024

Session Recording supports Group Service Managed Account (gMSA) 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 - EffectiveTime ((get-date).addhours(-10))
    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
```

1. On the domain controller, open the Active Directory Administrative Center.

📠 Server Manager				- 🗆 X				
Server Manager + Dashboard • (2) 1 Marage Total Vew Help								
Doubbased Local Server Mark JS Servers Mark JS Servers Mark JS Servers AD LS AD DS AD DS Mark JS Servers Mark JS Serverses Port IS	WELCOME TO SERVER MANAGER OCCCSM	ces						
	ROLES AND SERVER GROUPS Roles 1 Servers total 1 Roles And SERVER GROUPS AD CS 1 Manageability Events Services Performance BPA results Imageability Imageability Events Services Performance BPA results Imageability Imageability Imageability Imageability Imageability Imageability Imageability Imageability Imageability Imageability	DNS 1 Imageability Imageability Events Imageability Services Performance BPA results BPA results	IIS Manageability Events Services Performance BPA results	Lead Security Policy Microsoft Auras Services COEC Close Sources (23-bit) COEC Close Sources (24-bit) Colice Responses (84-bit) Colice Responses (84-bit) Responses (84-bit) Response (84-bit) R				

2. Select the domain and create a group.

	🗈 Active Directory Administrative Center - 🗆 X								
ĒL S	€ S - Active	Directory Administra	ative (Center • (local) • Use	rs			• 🗊 Manage Help	
G	🔺 Active Directory 🔇	Users (26)						Tasks	
\leq	H 12	Filter	0	(i) • (ii) •				自	
	Overview	riner	~	0.0.			1	Users ^	
		Name	Туре	Description				New 🔸	InetOrgPerson
1	L Users	administrator	User				^	Delete	Group
10	A Dynamic Access Control	Allowed RODC Password R	Group	Members in this group ca				Search under this node	User
12	A Authentication	🖆 Cert Publishers	Group	Members of this group ar				Properties	Computer
¥	P Global Search	Loneable Domain Control	Group	Members of this group th					
2	C Global search	Denied RODC Password R	Group	Members in this group ca					
ig.	F		Group	DNS Administrators Group					
ĒD			Group	DNS clients who are permi					
			Group	Designated administrators					
			Group	All workstations and serve All domain controllers in t					
		-	Group	All domain quests					
			Group	All domain users					
			Group	Designated administrators					
			Group	Members of this group ca					
		A Enterprise Read-only Dom	Group	Members of this group ar					
		Sroup Policy Creator Own	Group	Members in this group ca					
			Group						
			User	Built-in account for guest					
		🚨 jiajiaai	User	Built-in account for admini			~		
		A					~		
	WINDOWS POWERSHELL HIS	TORY						۲	
		Manageability		Manageability					
		C	_					×	

 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.

				- 6 .							
Create Group	p: gMSA										
	Group			280							
Managed By	Group name: * gMSA		E-mail								
Member Of	Group (SamAccountName * gMSA		Create in: CN=Builtin,DC=endpoint,DC=local Charge								
Members	Group type:	Group scope:	Description:								
Password Settings	Security	O Domein Incel									
Passinonu setonga	O Distribution	Global Universal	Notes								
	Protect from accidental deletion	O Universal	NODEL								
	Managed By										
	Managed by:	Select Users, Contacts, Computers, Service Accounts, or Groups X	Ibject Types X								
	Manager can update membership list		Select the types of objects you want to find.								
	Phone numbers	Select this object type:									
	Main	Users, Service Accounts, Groups, or Other objects Object Types	Object types:								
	Mobile:	From this location:	Contexts								
	Fac										
		Enter the object names to select (<u>examples</u>):	121 W Concident	~							
		Check Names	₩ May Groups ② & Usen								
	Member Of			280							
	Filter P	Advanced OK Cancel	OK Cancel	Add							
	Name * Active Director.										
				Remove							
	Members			280							
	Memoers										
	Filter P										
				Add							
	Name Active Director			Remove							
				Remove							
	Directly Associated Password Settings			280							
	Name Precedence										
				Assign							
				Clear							

For example, a group member is added as follows:

Create Group	z: gMSA							TASKS V SECTIONS V
	Group							280
Managed By Member Of	Group name: * gMSA Group (SamAccountName* gMSA			E-mail: Create in: C	N=Users,DC=ajj,DC=test	Change		
Members Password Settings	Group type: Security (*) Distribution	Group scope O Domain local C Global		Description				
	Protect from accidental deletion	O Universal		Notes				
	Managed By							? × 0
	Managed by: Manager can update membership list Phone numbers:	<u>Edi</u>	t., Clear	Office:				
	Main: Mobile:			Street				
	Fax			City Country/Re	gion	State, Province	Zip,₽ostal code	~
	Member Of							280
	Filter P							Add
	Name Active Director							Remove
	Members							?⊗⊙
	Filter D							Add
Г	Name Active Director SERVER-3 ağ-Computers							Remove
L								
	Directly Associated Password Settings							280
	Narre * Precedence							Assign Clear
More Information								OK Cancel

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.

er Manager 🖪 Active Directory Administrative Center		- 0
		• 🕝 Manage Help
Active Directory c GLOBAL SEARCH 1 items found		Tasks
cal Server E T TE Convert to LDAP Scope: aj (local)	•	ė
I Servers ■ Overview ØMSA X Ø Search ③ ▼ ④ ▼	۲	gMSA
D CS III aj (soul) Name Type Description Path		Add to another group Delete
Users Users		Move
NS Ma Dynamic Access Control D E MAA Group DCing/DCitest		Locate
		Properties
9MSA	^	
WINDOWS POWERSHELL HISTORY		

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:

1 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.
- 6. Use Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10)) to enable the gMSA globally on domain of the domain controller.

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:

Local Server All Servers Configure this local server	Help
A find and storage services Concestant	Hide

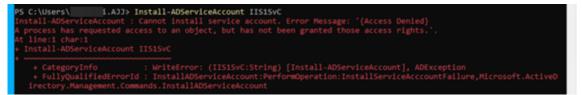
• If you use PowerShell with administrative privileges, run the following command:

1 Install-WindowsFeature -Name RSAT-AD-PowerShell

2. Open Windows PowerShell and run a command similar to the following to install the gMSA.

```
1 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.

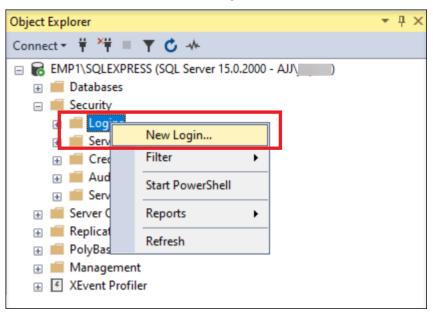


3. Verify that you have installed the gMSA successfully by running a command similar to the following in PowerShell. If the command returns **True**, the gMSA has been installed successfully.



Step 3: Enable the gMSA to access the Session Recording database and Session Recording logging database

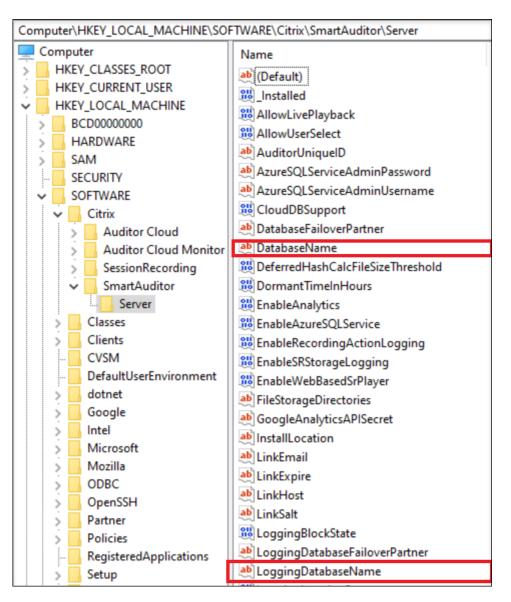
1. Create a login for the gMSA. Use the SQL Server Management Studio (SSMS) to connect to the SQL instance of the Session Recording database.



Name the new login in the format of **<domain name of the domain controller>\<name of the gMSA>**. For example:

Login - New			-	-		×
Select a page	🖵 Script 🔻 🕜 Help					
 Server Roles User Mapping Securables 		AJJ\IIS1SvC\$			Search	h
🖌 Status	 Windows authentication SQL Server authentication 					
	Password:					
	Confirm password:					
	Specify old password					
	Old password: Enforce password policy					
	Enforce password expira					
	User must change pass Mapped to certificate	word at next login				
	Mapped to certificate Mapped to asymmetric key			~		
Connection	Map to Credential			~	Add	
Server: EMP1\SQLEXPRESS	Mapped Credentials	Credential		F		
Connection: AJJ\jiajiaai						
View connection properties						
Progress		<		>	Remo	ve
Ready	Default database:	master		\sim		
48*	Default language:	<default></default>		\sim		
			OK		Cano	cel

- 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				- 0	×
Select a page	Script	🕶 🕜 Help			
 Server Roles User Mapping 	Users ma	apped to this login:			
Securables	Мар	Database	User	Default Schema	^
🔎 Status		master			
		model			
		msdb			
		SR2203cu4			
		SR2203CU4log			
		SR2206			
		SR2206log			
		SR2311	AJJ\IIS1SvC\$		
		SR2311log			_
		tempdb			
		Upgradeto 15			
		Upgradeto 15log			
					~
Connection	<				>
Server:	Gues	t account enabled for: SR2	2311		
EMP1\SQLEXPRESS	Databas	e role membership for: SR2	211		
Connection:		ccessadmin			
AJJ		ackupoperator			
View connection properties		latareader			
		latawriter			
		Idladmin			
		lenydatareader lenydatawriter			
Progress	db_o				
Ready	db_s ✓ publi	ecurityadmin c			
				OK	Cancel

Login - New					
Selectapage Ø General	Script	🔻 😮 Help			
General Server Roles					
User Mapping	Users ma	apped to this login:			
Securables	Мар	Database	User	Default Schema	^
👂 Status		master			
		model			
		msdb			
		SR2203cu4			
		SR2203CU4log			
		SR2205C0-H0g			
		SR2206log			
		SR2311	AJJ\IIS1SvC\$		- 6
		SR2311log	AJJ\IIS1SvC\$	_	
		tempdb	700 (1010/04		
		Upgradeto 15			
		Upgradeto 15			
		Opgradeto Tolog			~
· · · · · · · · · · · · · · · · · · ·	<				>
Connection	Gues	st account enabled for: SR	2311log		
Server:			-		
EMP1\SQLEXPRESS	Databas	e role membership for: SR	2311log		
Connection: AJJ		accessadmin			
		packupoperator			
View connection properties		latareader latawriter			
		dladmin			
		denydatareader			
		denydatawriter			
Progress					
		securityadmin			
Ready	2 publi	C			
Ready	🗹 publi	ic			

Note:

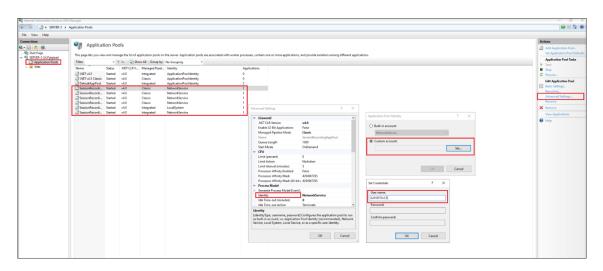
If you grant **db_datareader** and **db_datawriter** permissions instead of **db_owner** permission, you must also grant the execution permission on the databases to the gMSA. For example:

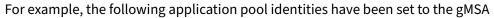
```
    use SR2311 grant execute to [name of the login created earlier]
    use SR2311log grant execute to [name of the login created earlier]
```

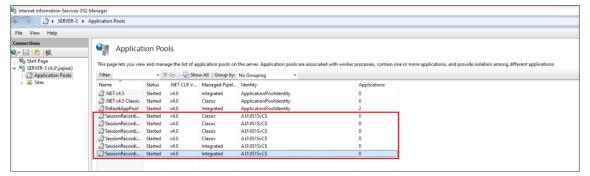
Step 3: Enable the gMSA to access the Session Recording servers

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.







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
1
2
   $webapps = Get-ChildItem -Path IIS:\AppPools
   foreach ($webapp in $webapps) {
3
4
5
       if ($webapp.Name.Contains("SessionRecording")){
6
           $Pool = "IIS:\AppPools\" + $webapp.Name
7
           Write-Host $Pool
8
9
          Set-ItemProperty -Path $Pool -Name processModel -Value
              6{
    userName="AJJ \IIS1SvC$";identitytype=3 }
11
       }
12
14
    }
```

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.

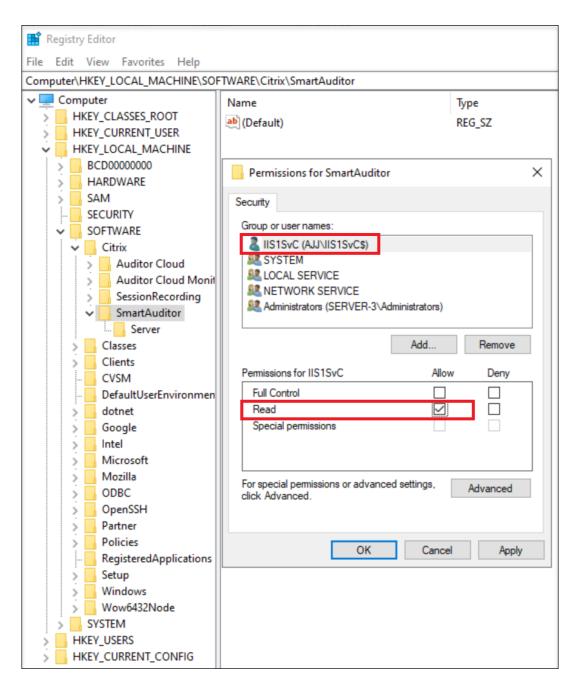
a) Locate the service account object type.

📑 Registry Editor						- 🗆 X
File Edit View Favorites Help						
Computer\HKEY_LOCAL_MACHINE\SOF	TWARE\Citrix\SmartAuditor					
V Computer	Name	Туре	Data			
HKEY_CLASSES_ROOT	e) (Default)	REG_SZ				
HKEY_LOCAL_MACHINE						
> BCD0000000	Permissions for SmartAuditor	×				
HARDWARE					Object Types	×
SAM SECURITY	Security		Select Users, Computers, Service Accounts, or Groups	×		
SOFTWARE	Group or user names:		Select this object type:		Select the types of objects you want to find.	
Citrix	SYSTEM Stocal Service		Users, Groups, or Built-in security principals	Object Types	Object types:	
Auditor Cloud Monit	SE NETWORK SERVICE		From this location:		Built-in security principals	
> SessionRecording	Administrators (SERVER-3\Administrators)		ajitest	Locations		
 SmartAuditor 			Enter the object names to select (examples):		C R Groups	
Classes	Add	Remove	B and a state of the state of t	Check Names	Users	
> Clients						
- CVSM	Permissions for SYSTEM Allo		1			
DefaultUserEnvironmen	Full Control		Advanced	OK Cancel		
Google	Special permissions			11		OK Cancel
> Intel						
> Microsoft						
> Mozilia > ODBC	For special permissions or advanced settings, click Advanced.	Advanced				
> OpenSSH	cick Advanced.					
> Partner						
> Policies RegisteredApplications	OK Cano	el Apply				
> Setup						
> Windows						
> Wow6432Node > SYSTEM						
HKEY USERS						
HKEY_CURRENT_CONFIG						

b) Enter the name of the gMSA.

Computer	Name	Туре	Data	
HKEY_CLASSES_ROOT	(Default) REG_SZ			
HKEY_CURRENT_USER				
HKEY_LOCAL_MACHINE			1	
> BCD0000000	Permissions for SmartAuditor	\times		
SAM				
SECURITY	Security		Select Users, Computers, Service Accounts, or Groups	×
SOFTWARE	Group or user names:			
V Citrix	SYSTEM		Select this object type:	
> Auditor Cloud	Second Service		Users, Service Accounts, Groups, or Built-in security principals	Object Types
Auditor Cloud Mon	it SERVICE		From this location:	
SessionRecording	Administrators (SERVER-3\Administrators)	ajitest	Locations
SmartAuditor				
Server			Enter the object names to select (examples):	
> Classes	Add	Remove	IIS1SvC	Check Names
> Clients	Permissions for SYSTEM A	low Deny		
- CVSM			1	
- DefaultUserEnvironme			Advanced OK	Cancel
> dotnet	Read			
> Google	Special permissions			
> Intel				
> Microsoft				
> ODBC	For special permissions or advanced settings,	Advanced		
> OpenSSH	click Advanced.			
Partner				
Policies				
- RegisteredApplication	S OK Can	cel Apply		
> Setup			2	
> Windows				
> Wow6432Node				
> SYSTEM				
HKEY_USERS				
HKEY_CURRENT_CONFIG				

c) Grant Read permission to the gMSA.



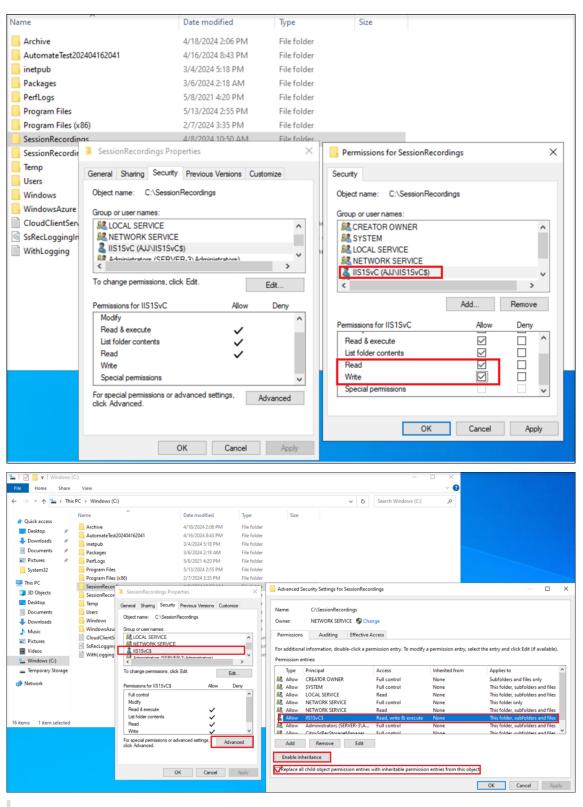
Note:

Alternatively, you can use a script similar to the following to grant Read permission on the Session Recording server to a gMSA:

```
1 $RegistryKey = "HKLM:\SOFTWARE\Citrix\SmartAuditor"
2 $NewAcl = Get-Acl -Path $RegistryKey
3 $identity = "pahl6\IIS1SvC$"
4 $RegistryKeyRights = "ReadPermissions"
5 $type = "Allow"
6 $RegistryKeyAccessRuleArgumentList = $identity,
```

- \$RegistryKeyRights, \$type
 7 \$RegistryKeyAccessRule = New-Object System.Security.
 AccessControl.RegistryAccessRule -ArgumentList
 \$RegistryKeyAccessRuleArgumentList
 8 \$NewAcl.SetAccessRule(\$RegistryKeyAccessRule)
 9 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**.

🖢 > This	PC → Windows (C:)			ٽ ~	Search Windows (C:)	
	<u>^</u>	modified Type	Size			
ess * ds * hts * ts ts ds ((Cs) ry Storage	Archive 4/18/ AutomateTest202404162041 4/16/ Interbub 3/4/2 Packages 3/6/2 PerfLogs 5/8/2 Program Files 5/1/3 Program Files (x86) 2/7/2 SessionRecordings 4/02	2024 2:06 PM File folder 2024 2:06 PM File folder 2024 2:18 PM File folder 2024 2:18 AM File folder 2024 2:25 PM File folder 2024 2:25 PM File folder 2024 2:25 PM File folder 224 1:050 AM File folder 224 1:050 AM File folder 224 1:050 AM File folder 224 2:07 PM File folder 225 Pm File folder	SessionRecordings SessionRecordings I: NER CE	×	Select Users, Computers, Service Accounts, or Groups Select this object type: Users, Groups, or Built in security principals From this location: agitest Epiter the object names to select (<u>examples</u>):	X Object Types Locations Direck Names
m selected	C Edt To change permissions, click Edt. Edt Permissions for CREATOR Allow OWNER Allow D Full control Mody Read Write Vivre For special permissions or advanced settings, click Advanced. OK Cancel	eny Permissions for CRE OWNER Ful control Modify Read 8 execute Lat folder content Read	Ator Ald	Remove Deny	Advanced. Object Types Select the types of objects you want to find. Object types: Object types: Object types: Object Type: Object Type:	OK Cancel X
						OK Cancel



Note:

Alternatively, you can use a script similar to the following to grant Read and Write permis-

sions on the Session recording storage folder to a gMSA and to enable inheritance:

```
1 $path = "C:\SessionRecordings"
2 $NewAcl = Get-Acl $path
3 # Set properties
4 $identity = "pahl6\IIS1SvC$"
5 $fileSystemRights = "Modify"
6 $type = "Allow"
7 # Create new rule
8 $fileSystemAccessRuleArgumentList = $identity,
      $fileSystemRights, $type
9 $fileSystemAccessRule = New-Object -TypeName System.Security.
      AccessControl.FileSystemAccessRule
      $fileSystemAccessRuleArgumentList
10 # Apply new rule
11 $NewAcl.SetAccessRule($fileSystemAccessRule)
12 # enable inherit
13 $isProtected = $false
14 $preserveInheritance = $false
15 $NewAcl.SetAccessRuleProtection($isProtected,
      $preserveInheritance)
16 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\		AJJ> \$account = "IIS1SvC"
PS C:\Users\		.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.

File Home S	_Data ihare View							- 0	× ~ ?
← → * ↑	> This PC > Windo	ws (C:) > Program Files	> Citrix > SessionRecording >	Server > App_Data		~	ල් Search App	p_Data	م
✤ Quick access ■ Desktop ↓ Downloads	Name Policy_A Policy_A Policy_A Session		Date modified 4/18/2024 4:42 PM 4/18/2024 4:55 PM 3/8/2024 10:40 AM	Type XML Document XML Document XML Document	Size 4 KB 3 KB 4 KB				
SessionRecordingAzManStore	*								
<aztask 1"="" guid="BAC2C1</th><th>sion=" minor<br="">a7b0f49-b1a2-4 BC-C936-4DE7-4 8D-C5A2-4073-9</aztask>	rVersion="0"> 4046-8b86-4dcffe37 3EDB-220E850E5CB8" 9948-1EC6CDFA79F3"	70f17" Name="SsRecBroke ' Name="LoggingWriter" ' Name="LoggingWriter" faskLink>	Description="Mem	bers of this ro	le can w	rite logs." B	izRuleImpor	tedPath=	
<azrole <br="" guid="29D490
<TaskLink>88C90252
</AzRole></th><th>109790068-158
52-FB7C-4EC8-4
D4-553E-4FD3-7
-FB7C-4EC8-80</th><th>80DF-7F4831B6E18E">A2C7-37B87050B10D" DF-7F4831B6E18E<!--7</th--><td>' Name="LoggingReader" ' Name="LoggingReader"</td><td>Description="Mem</td><td>bers of this ro</td><td>le can r</td><td>ead logs."></td><td></td><td></td></azrole>	' Name="LoggingReader" ' Name="LoggingReader"	Description="Mem	bers of this ro	le can r	ead logs.">				
<azrole 2c7b6f<br="" guid="8450f7
<TaskLink>371d1259
</AzRole>
<AzTask Guid="><azrole <br="" guid="387634
<TaskLink>2c7b6fbb
<Member>5-1-5-11</</th><th>/bd-4d58-4919-4
 -be9d-4f09-8e2
 bb-e916-46b2-
 5a-063a-42f9-9
 -e916-46b2-baa</th><th>a227-40aef4a2d419">2b-9da07eea2eb8<!--7<br-->bac8-945fdd62c3c3" 9012-069a7b097ea2"</azrole></azrole>	' Name="Player" Descrip FaskLink> ' Name="PolicyQuery" De ' Name="PolicyQuery" De	otion="Members of escription="Membe	this role can	search fo	or, view, and ry the Sessio	n Recording	ss restr Server		
<azrole <br="" guid="53e2fc
<TaskLink>7fb11af4</th><th>3c-cfa1-4e75-8
-7829-4887-bf4</th><th>8612-7d6510181674">46-d9c6299fcfc2<!--7</th--><td></td><td>rator" Descriptio</td><td>n="Members of t</td><td>his role</td><td>can view and</td><td>change rec</td><td>ord poli</td></azrole>		rator" Descriptio	n="Members of t	his role	can view and	change rec	ord poli		
<member>S-1-5-32-5 <aztask a34657<="" guid="a34657</th><th>50-b5ff-4573-</th><th></th><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><th></AzRole>
<AzTask Guid=" th=""><th>e4-327d-46d2-a</th><th>af34-845e8baebe24"</th><td>'Name="PrivilegedPlaye</td><td></td><td></td><td></td><td></td><td>view, plac</td><td>e, and r</td></aztask></member>	e4-327d-46d2-a	af34-845e8baebe24"	'Name="PrivilegedPlaye					view, plac	e, and r

c) Grant full control permission on the **App-Data** folder to the gMSA.

Image: Second	esterRecording > Server 0 0 Differ modified 7 type 81/02/024 921 PM F4E folder 91/02/024 921 PM F4E folder 91/02/024 921 PM F4E folder 91/02/024 921 PM F4E folder 91/02/024 910 PM 51AH0ARD F4E	- □ × ✓ ● Search Sener	Session Pet-	User: AC709LadicListrator Net: AC709LadicListrator OVersative Hild Handborn Versa System Jper: Server, Stand Janes, Fredan Dederess: Server, Stand Janes, Fredan Dederess: Server, Stand Janes, Fredan Dederess: Server, Stand Janes, Stand Market, Stand Janes, Stand Kottime, V18/2023 File, Server Volumes: Ci, V30,00 G MTS Freedpace: Ci, V55,53 G MTS	
Servel Starry Month (Head Network Cutom) Cold one are: Charge The Cale Charge Network (Server) Cold one are: Charge The Cale Charge Network (Server) Cold Cold Server Cold Cold Cold Cold Cold Cold Cold Cold	Allow Administrators (W2K195T-H8 Ful Allow Users (W2K195T-H8K2VKH/Us Rei Allow Everyone Rei	on extry. To modify a permission entry, solicit The come behavior from the solicit The the X model The Second The The Second The Second The A model The Second The The Second Th		Premiant hoty for Age, Sate Project	Sene User, Computer, Senera Accord, et alling 2 2 2 2 Select Transport, Senera Accord, et alling works prevand The Transport, Senera, Balan works prevand The Transport, Senera, Balan works prevand The Transport, Senera, Balan works prevand The Transport, Senera, Balan works prevand The Transport, Senera
	,	Revealant Body for App, Data Revealant Body for App, Data Revealant Body for App, Data Revealant Body (Second S	v v	Add a condition	Mixed Location

d) Verify that the gMSA is successfully added to the Session Recording Authorization Console.

				Session Re	cording Authorization Console				- 0	×
				File Action	View Help					
				(+ +) 🖄	🗊 🗙 🗊 @ 🕞 📓 🗊					
				🗎 Role Assign		Name	Type	Description		
				🕼 Loggin		RETWORK SERVICE	Group	best poor		
				🗞 Loggin	gReader	Administrators(AJJ\Admini				
				PolicyC	Query	IIS1SvC\$(AJJ\IIS1SvC\$)	User			
					dministrator					
				nivileg	edPlayer					
=		Windows Server								
	Citrix ^									
	Session Recording Administrator Lo	–	\geq	2						
			Windows	Windows						
	Session Recording Authorization Co	Server Manager	PowerShell	PowerShell ISE						
	Session Recording Policy Console									
	-	*	-							
	Session Recording Server Properties	. 1	- 19	<u>e</u> e						
	м	Windows Administrativ	Task Manager	Control Panel						
	Nicrosoft Edge	_	_			<				>
			8							
	- Server Manager	Remote Desktop	Event Viewer	File Explorer						

Note:

Alternatively, you can use a script similar to the following to add a gMSA to the Session Recording Authorization Console:



Troubleshoot

June 21, 2024

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

August 15, 2024

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
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

Event ID	Description	Level
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
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

Encryption2033Error: Method Opening For ReadingError Reading2034Error: Method Retrieving Encryption Percent CompleteError2035Error: Method Reading FileError2036Error: Method Querying FileError2037Error: Method Closing FileError2038Error: Method Enumerating User NamesError2040Error: Method Enumerating Group NamesError2041Error: Method Enumerating Group NamesError2042Error: Method Enumerating Group NamesError2043Error: Method Enumerating Group NamesError2044Error: Method Enumerating Group NamesError2045Error: Method Enumerating FrorError2046Error: Method Enumerating FrorError2047Error: Method Enumerating FrorError2046Error: Method Enumerating Server Names For FarmError2047Error: Method Enumerating Server Names For Farm And Delivery GroupError2048Error: Method Enumerating Server Names For Farm And Delivery GroupError2049Error: Method Enumerating Server MamesError2049Error: Method Enumerating Server NamesError2049Error: Method Enumerating Server NamesError2049Error: Method Enumerating Server NamesError2049Error: Method Enumerating Server NamesError2049Error: Method Enumerating Server NamesError <th>Event ID</th> <th>Description</th> <th>Level</th>	Event ID	Description	Level
Reading2034Error: Method Retrieving Encryption Percent Complete2035Error: Method Reading FileError2036Error: Method Querying FileError2037Error: Method Closing FileError2038Error: Method Enumerating Account AuthoritiesError2039Error: Method Enumerating User NamesError2040Error: Method Enumerating Group NamesError2041Error: Method Enumerating Group NamesError2042Error: Method Enumerating Client NamesError2043Error: Method Enumerating ErrorError2044Error: Method Enumerating Client AddressesError2045Error: Method Enumerating ErrorError2046Error: Method Enumerating ZoneError2047Error: Method Enumerating Server Names For FarmError2048Error: Method Enumerating Server Names For Farm And Delivery GroupError2048Error: Method Enumerating Server Names For Farm And Delivery GroupError2048Error: Method Enumerating Server Names For Farm And Delivery GroupError2049Error: Method Enumerating Server NamesError2049Error: Method Enumerating Server NamesError2050Error: Method Enumerating Server NamesError2050Error: Method Enumerating Server NamesError2050Error: Method Enumerating Server NamesError	2032		Error
Encryption Percent Complete Encryption Percent Complete Error Error: Method Reading File Error Error: Method Querying File Error Error: Method Closing File Error Method Enumerating Error Account Authorities Error Account Authorities Error Method Enumerating Error User Names User Names Error Group Names Error Client Names Error Client Names Error Client Addresses Error Client Addresses Error Error Error: Method Enumerating Error Client Addresses Error Error Error: Method Enumerating Error Error Error: Method Enumerating Error Error Error: Method Enumerating Error Error Server Names Error Server Names For Farm Add Zone Error: Method Enumerating Error Server Names For Farm And Zone Error: Method Enumerating Error Server Names For Farm And Zone Error Server Names For Farm And Delivery Group Error Server Names For Farm And Delivery Group Error Server Names Error Server Names For Farm And Zone Error Server Names For Farm And Zone Error Server Names For Farm And Delivery Group Error Server Names Error Server Names For Farm And Zone Error Server Names For Farm And Zone Error Server Names For Farm And Delivery Group Error Server Names Error Er	2033		Error
2036Error: Method Querying FileError2037Error: Method Closing FileError2038Error: Method EnumeratingError2039Error: Method EnumeratingError2039Error: Method EnumeratingError2040Error: Method EnumeratingError2040Error: Method EnumeratingError2041Error: Method EnumeratingError2042Error: Method EnumeratingError2043Error: Method EnumeratingError2044Error: Method EnumeratingError2045Error: Method EnumeratingError2046Error: Method EnumeratingError2047Error: Method EnumeratingError2048Error: Method EnumeratingError2047Error: Method EnumeratingError2048Error: Method EnumeratingError2049Error: Method EnumeratingError2049Error: Method EnumeratingError2040Error: Method EnumeratingError2041Error: Method EnumeratingError2042Error: Method EnumeratingError2043Error: Method EnumeratingError2044Error: Method EnumeratingError2045Error: Method EnumeratingError2046Error: Method EnumeratingError2047Error: Method EnumeratingError2048Error: Method EnumeratingError2049Error: Method EnumeratingError<	2034	Ũ	Error
2037Error: Method Closing FileError2038Error: Method Enumerating Account AuthoritiesError2039Error: Method Enumerating User NamesError2040Error: Method Enumerating Group NamesError2041Error: Method Enumerating Group NamesError2042Error: Method Enumerating Client NamesError2043Error: Method Enumerating Client AddressesError2044Error: Method Enumerating Client AddressesError2045Error: Method Enumerating Farm NamesError2046Error: Method Enumerating Farm Server Names For FarmError2047Error: Method Enumerating Server Names For Farm And ZoneError2048Error: Method Enumerating Server Names For Farm And Delivery GroupError2049Error: Method Enumerating Server Names For Farm And Delivery GroupError2049Error: Method Enumerating Server Names For Farm And Delivery GroupError2040Error: Method Enumerating Server Names For Farm And Delivery GroupError2048Error: Method Enumerating Application NamesError2049Error: Method Enumerating ErrorError2050Error: Method Loading Policy ErrorError	2035	Error: Method Reading File	Error
2038Error: Method Enumerating Account AuthoritiesError2039Error: Method Enumerating User NamesError2040Error: Method Enumerating Group NamesError2041Error: Method Enumerating Group NamesError2041Error: Method Enumerating Client NamesError2042Error: Method Enumerating Client AddressesError2043Error: Method Enumerating Farm NamesError2044Error: Method Enumerating Farm NamesError2045Error: Method Enumerating Farm NamesError2046Error: Method Enumerating Zone Names For FarmError2047Error: Method Enumerating Server Names For Farm And ZoneError2048Error: Method Enumerating Application NamesError2049Error: Method Enumerating ErrorError2050Error: Method Enumerating ErrorError2050Error: Method Enumerating ErrorError	2036	Error: Method Querying File	Error
Account Authorities Error: Method Enumerating Error User Names 2040 Error: Method Enumerating Error Group Names 2041 Error: Method Enumerating Error Client Names 2042 Error: Method Enumerating Error Client Addresses 2043 Error: Method Enumerating Error Farm Names 2044 Error: Method Enumerating Error Farm Names 2044 Error: Method Enumerating Error 2046 Error: Method Enumerating Error 2046 Error: Method Enumerating Error 2047 Error: Method Enumerating Error 2048 Error: Method Enumerating Error 2046 Error: Method Enumerating Error 2047 Error: Method Enumerating Error 2048 Error: Method Enumerating Error 2047 Error: Method Enumerating Error 2048 Error: Method Enumerating Error 2048 Error: Method Enumerating Error 2048 Error: Method Enumerating Error 2048 Error: Method Enumerating Error 2048 Error: Method Enumerating Error 2049 Error: Method Enumerating Error 2049 Error: Method Enumerating Error	2037	Error: Method Closing File	Error
User Names2040Error: Method Enumerating Group NamesError2041Error: Method Enumerating Client NamesError2042Error: Method Enumerating Client AddressesError2043Error: Method Enumerating Farm NamesError2044Error: Method Enumerating Farm NamesError2045Error: Method Enumerating Farm NamesError2046Error: Method Enumerating Server Names For FarmError2046Error: Method Enumerating Server Names For FarmError2047Error: Method Enumerating Server Names For Farm And ZoneError2048Error: Method Enumerating Server Names For Farm And Delivery GroupError2048Error: Method Enumerating Server Names For Farm And Delivery GroupError2049Error: Method Enumerating Application NamesError2049Error: Method Enumerating Application NamesError2050Error: Method Loading Policy ErrorError	2038	0	Error
Group Names2041Error: Method Enumerating Client NamesError2042Error: Method Enumerating Client AddressesError2043Error: Method Enumerating Farm NamesError2044Error: Method Enumerating Farm NamesError2045Error: Method Enumerating Zone NamesError2046Error: Method Enumerating Zone Names For FarmError2047Error: Method Enumerating Server Names For Farm And ZoneError2047Error: Method Enumerating Server Names For Farm And Delivery GroupError2048Error: Method Enumerating Server Names For Farm And Delivery GroupError2049Error: Method Enumerating Server NamesError2049Error: Method Enumerating Server NamesError2049Error: Method Enumerating Server NamesError2050Error: Method Enumerating Server NamesError	2039	User Names	Error
Client Names 2042 Error: Method Enumerating Error Client Addresses 2043 Error: Method Enumerating Error Farm Names 2044 Error: Method Enumerating Error Zone Names 2045 Error: Method Enumerating Error Server Names For Farm 2046 Error: Method Enumerating Error Server Names For Farm And Zone 2047 Error: Method Enumerating Error Server Names For Farm And Delivery Group 2048 Error: Method Enumerating Error Server Names For Farm And Delivery Group 2048 Error: Method Enumerating Error Application Names 2049 Error: Method Enumerating Error 2049 Error: Method Enumerating Error 2049 Error: Method Enumerating Error 2049 Error: Method Enumerating Error 2049 Error: Method Enumerating Error 2049 Error: Method Enumerating Error 2049 Error: Method Enumerating Error 2049 Error: Method Enumerating Error 2049 Error: Method Enumerating Error 2049 Error: Method Enumerating Error	2040	-	Error
Client Addresses2043Error: Method Enumerating Farm NamesError2044Error: Method Enumerating Zone NamesError2045Error: Method Enumerating Server Names For FarmError2046Error: Method Enumerating Server Names For FarmError2047Error: Method Enumerating Server Names For Farm And Delivery GroupError2048Error: Method Enumerating Server Names For Farm And Delivery GroupError2049Error: Method Enumerating Server NamesError2049Error: Method Enumerating Server Type NamesError2050Error: Method Loading PolicyError	2041	v	Error
Farm Names Error: Method Enumerating Error Zone Names 2045 Error: Method Enumerating Error Server Names For Farm 2046 Error: Method Enumerating Error Server Names For Farm And Zone 2047 Error: Method Enumerating Error Server Names For Farm And Delivery Group 2048 Error: Method Enumerating Error Application Names 2049 Error: Method Enumerating Error Application Names	2042		Error
2045Zone Names2045Error: Method EnumeratingError2046Error: Method EnumeratingError2046Error: Method EnumeratingError2047Error: Method EnumeratingError2047Error: Method EnumeratingError2048Error: Method EnumeratingError2048Error: Method EnumeratingError2049Error: Method EnumeratingError2049Error: Method EnumeratingError2050Error: Method Loading PolicyError	2043	-	Error
Server Names For Farm Error: Method Enumerating Error Server Names For Farm And Zone Error: Method Enumerating Error Server Names For Farm And Delivery Group 2048 Error: Method Enumerating Error Application Names 2049 Error: Method Enumerating Error EventType Names	2044	-	Error
Server Names For Farm And Zone Error: Method Enumerating Server Names For Farm And Delivery Group 2048 Error: Method Enumerating Application Names 2049 Error: Method Enumerating EventType Names	2045	Server Names For Farm	Error
2047 Error: Method Enumerating Error Server Names For Farm And Delivery Group 2048 Error: Method Enumerating Error Application Names 2049 Error: Method Enumerating Error EventType Names 2050 Error: Method Loading Policy Error	2046	Server Names For Farm And	Error
Application Names 2049 Error: Method Enumerating Error EventType Names 2050 Error: Method Loading Policy Error	2047	Error: Method Enumerating Server Names For Farm And	Error
EventType Names Error: Method Loading Policy Error	2048	-	Error
	2049		Error
	2050		Error

Event ID	Description	Level
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
057	Error: Method Copying Policy Document	Error
058	Error: Method Renaming Policy Document	Error
059	Error: Method Setting Policy Document Description	Error
2060	Error: Method Deleting Policy Document	Error
061	Error: Method Getting Active Policy Document	Error
062	Error: Method Setting Active Policy Document	Error
063	Error: Method Running Policy Document Test Query	Error
064	Error: Method Processing Log Service Notification	Error
065	Error: Method Encrypting	Error
066	Error: Method Create Directory	Error
067	Error: Method Receiving Message	Error
068	Error: Method Create Recorded Session File Writer	Error
069	Error: Method Reopen Recorded Session File Writer	Error
070	Error: Method Creating File	Error

Event ID	Description	Level
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
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

Event ID	Description	Level
2091	Error: Method Set File Hidden Attribute	Error
2092	MSMQ storage quota on VDA was exceeded	Error

Installation of server components fails

June 21, 2024

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

June 21, 2024

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

June 21, 2024

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.

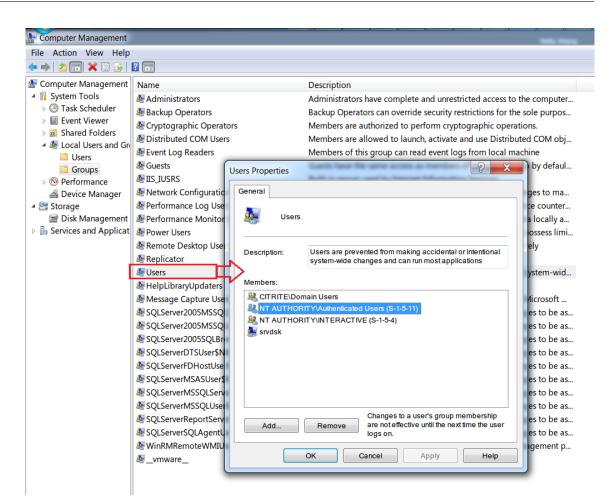
Solution: Add the Authenticated Users group back to this role, or add each server hosting each Session Recording agent to the PolicyQuery role.

• 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

June 21, 2024

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-sqlserver-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

June 21, 2024

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

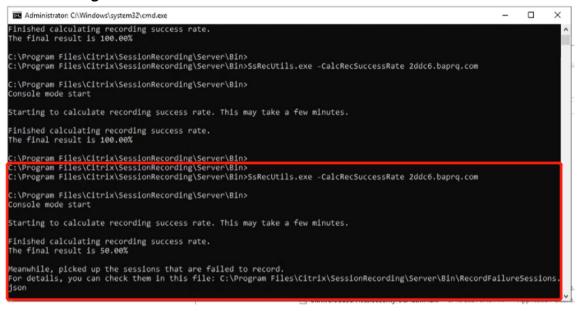
To check the recording success rate across your deployment, complete the following steps:

- 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
 Oelivery 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

Administrator: C:\Windows\system32\cmd.exe	-	×	7
Starting to calculate recording success rate. This may take a few minutes. No session launched. SsRecUtils.exe -CalcRecSuccessRate 2ddc6.baprq.com		ŕ	•
C:\Program Files\Citrix\SessionRecording\Server\Bin> Console mode start			
Starting to calculate recording success rate. This may take a few minutes. No Session needs record based on your recording policies. SsRecUtils.exe -CalcRecSuccessRate 2ddc6.baprq.com			
C:\Program Files\Citrix\SessionRecording\Server\Bin> Console mode start			
Starting to calculate recording success rate. This may take a few minutes.			
Finished calculating recording success rate. The final result is 100.00%			
C:\Program Files\Citrix\SessionRecording\Server\Bin> C:\Program Files\Citrix\SessionRecording\Server\Bin>SsRecUtils.exe -CalcRecSuccessRate 2ddc6.baprq.com			
C:\Program Files\Citrix\SessionRecording\Server\Bin> Console mode start			
Starting to calculate recording success rate. This may take a few minutes.			
Finished calculating recording success rate.			
			-

50% recording success rate



Sessions are not recording

June 21, 2024

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

June 21, 2024

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

June 21, 2024

• 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

June 21, 2024

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.

- ForHTTP: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

June 21, 2024

If you experience difficulties when searching for recordings using the Session Recording player, the following error messages might appear:

• Search for recorded session files failed. The remote server name could not be resolved: servername. The servername is the name of the server to which the Session Recording player is attempting to connect. The Session Recording player cannot contact the Session Recording server. Two possible reasons are an incorrectly typed server name or that the DNS cannot resolve the server name.

Resolution: From the player menu bar, choose **Tools > Options > Connections** and verify that the server name in the **Session Recording Servers** list is correct. If it is correct, from a command prompt, run the ping command to see if the name can be resolved. When the Session Recording server is down or offline, the search for recorded session files failed error message is **Unable to contact the remote server**.

• Unable to contact the remote server. This error occurs when the Session Recording server is down or offline.

Resolution: Verify that the Session Recording server is connected.

• Access denied. An access denied error can occur if the user was not given permission to search for and download recorded session files.

Resolution: Assign the user to the Player role using the Session Recording Authorization Console.

• Access denied when the Player role is assigned. This error occurs when you install the Session Recording player on the same machine with the Session Recording server, and you have enabled UAC. When you assign the Domain Admins or Administrators user group as the Player role, a non-built-in administrator user in that group might fail to pass the role-based check.

Resolutions:

- Run the Session Recording player as an administrator.
- Assign specific users as the Player role rather than the entire group.
- Install the Session Recording player in a separate machine rather than the Session Recording server.
- Search for recorded session files failed. The underlying connection was closed. Could not establish a trust relationship for the SSL/TLS secure channel. The error occurs when the Session Recording server uses a certificate that is signed by a CA that the client device does not trust or have a CA certificate for.

Resolution: Install the correct or trusted CA certificate workstation where the Session Recording player is installed.

• The remote server returned an error: (403) forbidden. This error is a standard HTTPS error that occurs when you attempt to connect using HTTP (nonsecure protocol). The server rejects the connection because, by default, it is configured to accept only secure connections.

Resolution: From the **Session Recording Player** menu bar, choose **Tools** > **Options** > **Connections**. Select the server from the **Session Recording Servers** list, and click **Modify**. Change the protocol from **HTTP** to **HTTPS**.

Troubleshoot MSMQ

If a notification message is given but the viewer cannot find any recordings after a search in the Session Recording player, there is a problem with MSMQ. Verify that the queue is connected to the Session Recording server (Storage Manager). Use a Web browser to test for connection errors (if you are using HTTP or HTTPS as your MSMQ communication protocol).

To verify that the queue is connected:

- 1. Log on to the server hosting the Session Recording Agent and view the outgoing queues.
- 2. Verify that the queue to the machine hosting the Session Recording server has a connected state.
 - If the state is **waiting to connect**, there are messages in the queue, and the protocol is HTTP or HTTPS (corresponding to the protocol selected on the **Connections** tab in **Session Recording Agent Properties**), perform Step 3.
 - If the state is **connected** and there are no messages in the queue, there might be a problem with the server hosting the Session Recording server. Skip Step 3 and perform Step 4.
- 3. If there are messages in the queue, open a Web browser and type the following address:
 - For HTTPS: https://servername/msmq/private\$/CitrixSmAudData, where servername is the name of the machine hosting the Session Recording server.
 - For HTTP: http://servername/msmq/private\$/CitrixSmAudData, where servername is the name of the machine hosting the Session Recording server.

If the page returns an error such as **The server only accepts secure connections**, change the MSMQ protocol listed in **Session Recording Agent Properties** to HTTPS. If the page reports a problem with the website security certificate, there might be a problem with a trust relationship for the TLS secure channel. In that case, install the correct CA certificate or use a CA that is trusted.

4. If there are no messages in the queue, log on to the machine hosting the Session Recording server and view private queues. Select **citrixsmauddata**. If there are messages in the queue

(Number of Messages Column), verify that the Session Recording StorageManager service is started. If it is not, restart the service.

Record Linux sessions (preview)

June 21, 2024

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.

citrix

© 2024 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.

 $\ensuremath{\mathbb{C}}$ 1999–2024 Cloud Software Group, Inc. All rights reserved.